МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ
УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

РАДІОТЕХНІКА

Всеукраїнський
міжвідомчий науково-технічний збірник

Засновано в 1965 р.

В И П У С К 2 0 2

Харків
Харківський національний
університет радіоелектроніки
2020

УДК 621.3

Збірник включено до Переліку наукових фахових видань України, категорія "Б", технічні та фізико-математичні науки (затверджено наказами МОНУ від 17.03.2020 № 409; від 02.07.2020 № 886; від 24.09.2020 № 1188) за спеціальностями: 171 – Електроніка; 172 – Телекомунікації та радіотехніка; 173 – Авіоніка; 125 – Кібербезпека; 151 – Автоматизація та комп'ютерно-інтегровані технології; 152 – Метрологія та інформаційно-вимірювальна техніка; 153 – Мікро- та наносистемна техніка; 163 – Біомедична інженерія; 105 – Прикладна фізика та наноматеріали.

Сборник включен в Перечень научных профессиональных изданий Украины, категория «Б», технические и физико-математические науки (утверждено приказами МОНУ от 17.03.2020 № 409, от 02.07.2020 № 886, от 24.09.2020 № 1188) по специальностям: 171 – Электроника; 172 – Телекоммуникации и радиотехника; 173 – Авионика; 125 – Кибербезопасность; 151 – Автоматизация и компьютерно-интегрированные технологии; 152 – Метрология и информационно-измерительная техника; 153 – Микро- и наносистемная техника; 163 – Биомедицинская инженерия; 105 – Прикладная физика и наноматериалы.

The collection is included in the List of scientific professional publications of Ukraine, category «Б», technical and physical-mathematical sciences (approved by orders of the Ministry of Education and Science from 17.03.2020 № 409; from 02.07.2020 № 886; from 24.09.2020 № 1188) by specialties: 171 – Electronics; 172 – Telecommunications and Radio Engineering; 173 – Avionics; 125 – Cybersecurity; 151 – Automation and Computer-Integrated Technologies; 152 – Metrology and Information-Measuring Equipment; 153 – Micro- and Nanosystem Technology; 163 – Biomedical Engineering; 105 – Applied Physics and Nanomaterials.

Сайт: rt.nure.ua

Реєстраційне свідоцтво КВ № 12098-969 ПР від 14. 12. 2006.

За зміст статті відповідальні автори.

Відповідальні випускові: *І.Д. Горбенко, д-р техн. наук, проф.,*
А.І. Лучанінов, д-р фіз.-мат. наук, проф.
Технічний секретар *О.С. Полякова.*

Рекомендовано Вченою радою Харківського національного університету радіоелектроніки, протокол № 7/11-1 від 16.09.2020.

Адреса редакційної колегії: Харківський національний університет радіоелектроніки (ХНУРЕ), просп. Науки, 14, Харків, 61166, тел. (0572) 7021-397.

Збірник «Радіотехніка» включено до Каталогу передплатних видань України, передплатний індекс ***08391.***

ЗМІСТ

ПЕРСПЕКТИВНІ МЕТОДИ ТА ЗАСОБИ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОММУНІКАЦІЙНИХ СИСТЕМАХ

ОБРОБКА СИГНАЛІВ В РАДІОТЕХНІЧНИХ СИСТЕМАХ

ПРИСТРОЇ РАДІОТЕХНІКИ ТА ЗАСОБИ ТЕЛЕКОМУНІКАЦІЙ

ФІЗИКА ПРИСТРОЇВ ТА СИСТЕМ

CONTENT

PROSPECTIVE METHODS AND MEANS OF CRYPTOGRAPHIC TRANSFORMATIONS

PROTECTION OF INFORMATION IN INFORMATION AND COMMUNICATION SYSTEMS

SIGNAL PROCESSING IN RADIO ENGINEERING SYSTEMS

RADIO ENGINEERING DEVICES AND MEANS OF TELECOMMUNICATIONS

PHYSICS OF DEVICES AND SYSTEMS

ПЕРСПЕКТИВНІ МЕТОДИ ТА ЗАСОБИ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

УДК 004.056.55 **DOI:10.30837/rt.2020.3.202.01**

І.Д. ГОРБЕНКО, д-р техн. наук, А.М. ОЛЕКСІЙЧУК, д-р техн. наук,
О.Г. КАЧКО, канд. техн. наук, Ю.І. ГОРБЕНКО, канд. техн. наук,
М.В. ЄСІНА, канд. техн. наук, С.О. КАНДІЙ

МЕТОДИ ОБЧИСЛЕННЯ СИСТЕМНИХ ПАРАМЕТРІВ ДЛЯ ЕЛЕКТРОННОГО ПІДПИСУ «CRYSTALS-DILITHIUM» 128, 256, 384 ТА 512 БІТ РІВНІВ БЕЗПЕКИ

Вступ

Наразі спостерігається стійкий прогрес у створенні квантових комп'ютерів різних призначень та можливостей, одним із основних призначень є здійснення криптоаналізу існуючих асиметричних криптосистем [1, 3]. Практично завершується створення математичних основ та програмного забезпечення для таких квантових комп'ютерів [4 – 11]. Особлива увага приділяється розробці великомасштабних квантових комп'ютерів, що призначаються для криптоаналізу існуючих стандартизованих криптосистем з відкритим ключем – електронних підписів, асиметричних шифрів та криптографічних протоколів різного призначення [9, 11]. Залишаються певні сумніви щодо симетричних криптоперетворень типу гешування, блокового та потокового симетричного шифрування. Але, як показують дослідження, збільшення при їх використанні розмірів параметрів та ключів згідно з нинішніми поглядами дозволяє забезпечити криптографічний захист на далеку перспективу. Зважаючи на можливості зламу існуючих асиметричних криптосистем, Національний інститут стандартів і технологій (NIST) США прийняв рішення у вигляді проєкту стандарту NIST 8309 щодо другого раунду конкурсу на перспективні стандартні алгоритми електронного (цифрового) підпису (ЕП) [2, 3].

Прийняті нові стандартизовані алгоритми ЕП дозволять реалізувати системи ЕП, що будуть здатні захистити конфіденційну інформацію уряду США в доступному для огляду майбутньому, в тому числі після появи квантових комп'ютерів. Таким чином, однією з основних проблем сучасної криптографії на міжнародному рівні є створення стандартизованих криптографічних систем (схем), які були б безпечними у постквантовий період. Таким чином, на світовому рівні зусилля значного числа криптологів, математиків та криптологів-практиків зосереджені на відкритому конкурсі NIST PQC [1 – 4, 12 – 18], одним із основних завдань якого є розробка та прийняття постквантового чи постквантових стандартів ЕП. Його підсумком є визначення фіналістів другого етапу конкурсу у вигляді проєктів CRYSTALS-DILITHIUM, FALCON та Rainbow [2, 3]. Окрім цього, були визначені три альтернативних кандидати, які потребують більш детальних досліджень уже на четвертому етапі конкурсу – GeMSS, Picnic та SPHINCS+[2].

Аналіз показує, що в Україні є розуміння існування загроз стандартизованим існуючим асиметричним криптоперетворенням. Так, розроблено та прийнято національний стандарт «Алгоритми асиметричного шифрування та інкапсуляції ключів» [2, 3], що побудований на основі застосування алгебраїчних решіток. Особливістю цього стандарту (ДСТУ 8961-2019) [12] є суттєве підвищення криптографічної стійкості асиметричного шифрування та інкапсуляції ключів у перехідний та постквантовий період. На відміну від пропозицій та можливостей, що затверджені та прийняті NIST 8309 [2], є можливість використовувати його з рівнями безпеки 384 та 512 бітів. Найвищий рівень безпеки проєктів CRYSTALS-DILITHIUM, FALCON та Rainbow 256 бітів проти класичного та 128 бітів квантового криптоаналізу.

В той же час наші дослідження показали, що з урахування можливостей щодо забезпечення безпеки з використанням уже прийнятих в Україні симетричних криптоперетворень ДСТУ 7564-2014, ДСТУ 7624-2014 та ДСТУ 8845-2019 [12], національні стандарти ЕП повинні забезпечити в перспективі до 512 біт класичної та 256 біт квантової безпеки.

Аналіз показав [2, 17, 18], що серед схем ЕП на решітках суттєві переваги надано проєктам ЕП CRYSTALS – DILITHIUM та FALCON, вони рекомендовані для подальшого дослідження та стандартизації в процесі третього етапу конкурсу. Причому кращими визначено як математичні основи, так і алгоритми ЕП CRYSTALS – DILITHIUM [3, 16 – 18]. ЕП CRYSTALS-DILITHIUM досліджувався у другому раунді як один із трьох проєктів ЕП на основі решітки. Його безпека грунтується на складності MLWE задачі криптоаналізу та задачі модульного короткого цілого рішення (MSIS) [17, 18]. Основою побудови алгоритму ЕП CRYSTALS–DILITHIUM є використання алгоритму Fiat-Shamir [17] з перериваннями. В ньому використовуються один і той же модуль і кільце поліномів для всіх наборів параметрів, а ентропія забезпечується за допомогою рівномірного розподілу. Це призводить, у порівнянні з гаусовим розподілом проєкту ЕП FALCON, до більш простої реалізації.

Загалом DILITHIUM має високі, збалансовані показники щодо розміру ключів та підписів, а також щодо ефективності алгоритмів генерації ключів, підпису та перевірки. DILITHIUM добре працює в реальних експериментах. Також у другому раунді до реалізації DILITHIUM додано опцію випадкової генерації підпису, що заснована на використанні AES. Це дало майбутні переваги при апаратних реалізаціях інструкцій ЕП. Крім того, було опубліковано нове дослідження безпеки в QROM [45], яке стосується DILITHIUM.

NIST рекомендував розробникам ЕП DILITHIUM додати набір параметрів 5-го рівня безпеки (5-й – за нашою класифікацією це 1-й рівень безпеки із 4-х рівнів). Також необхідні додаткові дослідження розуміння конкретної безпеки, оскільки DILITHIUM має найнижчий набір параметрів безпеки CoreSVP [2, 3] з усіх схем на основі решітки, які все ще знаходяться в процесі досліджень та порівняння. В той же час NIST вибрав DILITHIUM як фіналіста і очікує, що або DILITHIUM, або FALCON будуть стандартизовані як основна схема постквантового підпису в кінці третього раунду.

Необхідно відмітити, що в процесі формування вимог до ЕП NIST у рамках конкурсу був зацікавлений тільки в наборах загальносистемних параметрів до 256 біт класичної безпеки включно. Проте, на нашу думку, на перспективу доцільним є використання в DILITHIUM, 384 і 512 біт безпеки проти класичного криптоаналізу та 192 та 256 біт безпеки проти квантового криптоаналізу. Але, як показали дослідження, як з точки зору теорії так і практики, генерація загальносистемних параметрів для використання 256, 384 і 512 біт безпеки проти класичного криптоаналізу та 128, 192 та 256 біт безпеки проти квантового криптоаналізу, які в фіналісті CRYSTALS-DILITHIUM не реалізовано. Будемо також вважати, що відносно побудування ЕП CRYSTALS-DILITHIUM для 128 класично та 64 біт квантової стійкості проблем немає [3, 16].

Під час ухвалення рішення стосовно фіналістів на прийняття стандарту ЕП в третьому раунді кращими та отримали рекомендації визначені проєкти ЕП CRYSTALS-DILITHIUM та FALCON. В оцінці NIST ці проєкти на основі структурованої решітки представляються найбільш перспективними та універсальними алгоритмами для електронного підпису, асиметричного шифрування та протоколу інкапсуляціє ключів [2, 12 – 18].

Метою статті є обгрунтування моделі безпеки, класифікація, первинний аналіз та оцінка відомих атак на криптосистему ЕП CRYSTALS–DILITHIUM, встановлення обмежень та розробка практичних алгоритмів обчислення (генерації) загальносистемних параметрів для за-

безпечення 128, 256, 384 і 512 біт безпеки проти класичного та 64, 128, 192 та 256 біт проти квантового криптоаналізу.

1. Сутність криптографічних перетворень фіналіста ЕП конкурсу NIST США «CRYSTALS-DILITHIUM»

У [2, 3, 16] наведено пропозиції та результати досліджень щодо сутності, властивостей та умов застосування кандидата на постквантовий стандарт ЕП Crystals-Dilithium (в подальшому Dilithium), що були сформовані та подані на конкурс NIST. На першому етапі досліджень в 2018 р. виявлені певні проблемні питання, щодо яких авторами проєкту стандарту були обґрунтовані та запропоновані певні удосконалення механізму ЕП Dilithium [3]. У цьому розділі розглянемо сутність та основні математичні та криптографічні положення Dilithium, що будуть потрібні для оцінки криптографічної стійкості. Причому, особливу увагу звернемо на рівні криптографічної стійкості, тобто 1 – 5 рівні стійкості [1, 2], що рекомендуються та можуть бути реалізованими поки ще в проєкті стандарту ЕП Dilithium. Відмітимо, що одним із основних проблемних питань, будемо мати на увазі обґрунтування необхідності та розробки удосконаленої версії ЕП Dilithium, що може забезпечувати в постквантовий період 128, 256, 384 і 512 біт безпеки проти класичного та 64, 128, 192 та 256 біт проти квантового криптоаналізу від найбільш загрозливих атак [2, 16 – 18].

Метод (схема) ЕП Dilithium ґрунтується на підході, що отримав назву "Fiat-Shamir з перериваннями" [3, 17]. Він в певній мірі схожий на схему, що запропонована з послідовним удосконаленням в [16, 17]. Для спрощеного та узагальненого подання механізму розглянемо спрощену його версію на рис. 1 [3, 16], на якому наведено алгоритми генерації ключа, вироблення та перевірки ЕП. Основні положення та вирішення задачі обчислення (генерування) системних параметрів удосконаленого ЕП Dilithium наведені у параграфі 4 статі.

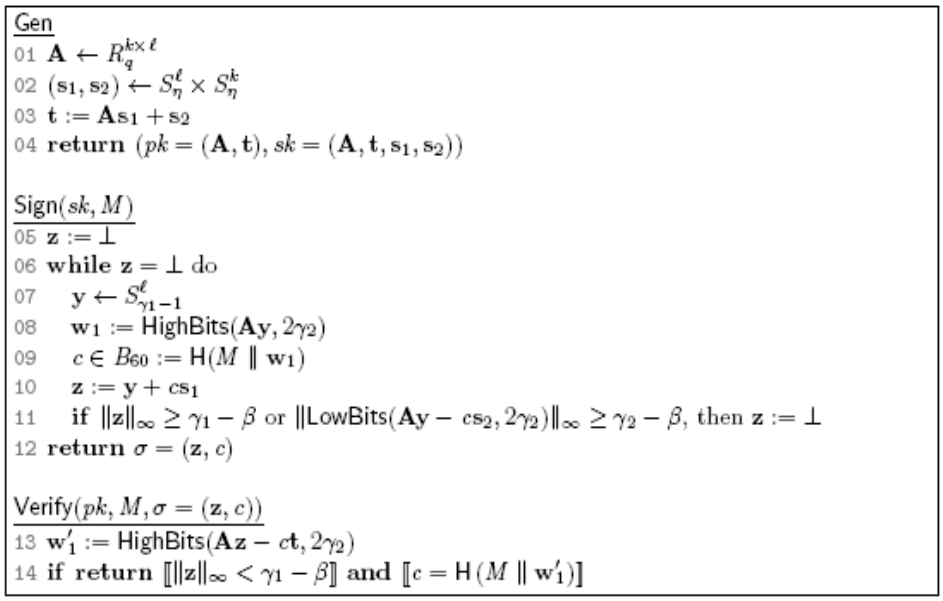


Рис. 1. Шаблон для механізму ЕП без стиснення відкритого ключа

1.1. Генерація основних складових ключа

Спочатку (рядок 01, рис. 1) генерується матриця поліномів **A** розміру $k \times \ell$, кожен з елементів якої є поліномом у кільці $R_q = \square_q[X]/(X^n + 1)$. В процесі попереднього розгляду будемо вважати, що модуль q=2^{23}–2^{13}+1, а степінь полінома n=256. Потім генеруються

(обчислюються) випадкові вектори, тобто множини поліномів секретного ключа $\mathbf{s}_1$ і $\mathbf{s}_2$ (рядок 02) відповідно з числом поліномів k та l. Коефіцієнти цих векторів (поліномів) є елементами поля R_η, тобто з (малими) коефіцієнтами з розміром не більше η (від $-\eta$ до η). Далі з використанням матриці $\mathbf{A}$ та секретного ключа $\mathbf{s}_1$ і $\mathbf{s}_2$ обчислюється друга частина відкритого ключа $\mathbf{t}=\mathbf{A}\mathbf{s}_1+\mathbf{s}_2$ (рядок 03), а перша частина відкритого ключа задається значенням ρ. Всі алгебраїчні операції з поліномами в механізмі виконуються над кільцем полінома $R_q = \mathbb{Z}_q[X]/(X^n+1)$. Четвертий рядок показує вихідні значення відкритого P_k та секретного S_k ключів. Детально алгоритм генерації ключа наводиться в [3].

1.2. Узагальнений алгоритм вироблення ЕП

В алгоритм перевірки ЕП вводяться значення секретного ключа S_k та повідомлення M, що підписується. Далі обчислюється вектор поліномів маскування $\mathbf{y}$ з коефіцієнтами, що є меншими, ніж γ_1 (рядок 07), а також обчислюється значення вектора поліномів $\mathbf{A}\mathbf{y}$. На основі отриманого значення $\mathbf{A}\mathbf{y}$ обчислюються старші біти $\mathbf{w}_1$ ("біти високого порядку") коефіцієнтів у цьому векторі поліномів (строчка 08); $\mathbf{w}_1$ є вектором, що містить всі поліноми w_1. Потім обчислюється поліном (рядок 09) c, що є поліномом у полі R_q з точно 60 символами ±1, а решта 0. Безпосередньо ЕП обчислюється у вигляді вектора поліномів $\mathbf{z}=\mathbf{y}+c\mathbf{s}_1$.

Якщо значення ЕП $\mathbf{z}$ вивести безпосередньо після його обчислення (рядок 10), то механізм ЕП Dilithium не буде безпечним через те, що при певних значеннях секретний ключ може бути компрометований. Щоб уникнути залежності $\mathbf{z}$ від секретного ключа та його витоку, використовується відхилення вибірки. Для цього встановлюється значення параметру β як максимально можливий коефіцієнт $c\mathbf{s}_i$. Оскільки c має значення 60 ±1, а максимальний коефіцієнт в $\mathbf{s}_i$ дорівнює $\mathbf{s}_i$, то легко побачити, що $\beta \le 60\eta$. Якщо будь-який коефіцієнт $\mathbf{z}$ перевищує $\gamma_1 - \beta$, то процес ЕП відхиляється, а процедура ЕП повторюється. Також, якщо коефіцієнт бітів низького порядку вектора $\mathbf{A}\mathbf{z}-c\mathbf{t}$ більше, ніж $\gamma_2 - \beta$, то процес ЕП відхиляється, а процедура ЕП знову повторюється (рядок 11). Перша перевірка необхідна для безпеки ЕП, а інша – для його безпеки та правильності. Таким чином, процес ЕП повторюється, доти не будуть виконані дві наведені умови. Необхідно відмітити, що параметри β та γ_1 і γ_2 повинні бути вибрані, щоб очікувана кількість повторень ЕП була не надто висока (наприклад, від 4 до 7). Детально алгоритм ЕП наводиться в [3].

1.3. Узагальнений алгоритм перевірки ЕП

При перевірці ЕП перевірник обчислює $\mathbf{w}'_1$ як біти високого порядку вектора $\mathbf{A}\mathbf{z}-c\mathbf{t}$. Далі ЕП приймається, якщо всі коефіцієнти $\mathbf{z}$ менше, ніж $\gamma_1 - \beta$ і якщо c є геш-значенням повідомлення M, що перевіряється, та значення $\mathbf{w}'_1$ (рядок 13). Перевірка спрацьовує за умов, якщо

$$\text{HighBits}(\mathbf{A}\mathbf{z}-c\mathbf{t},\, 2\gamma_2) = \text{HighBits}(\mathbf{A}\mathbf{y},\, 2\gamma_2) \qquad (1)$$

Дійсно, причиною цього є те, що для дійсного ЕП буде завжди виконуватись умова

$$\|\text{LowBits}(\mathbf{A}\mathbf{y}-c\mathbf{s}_2,\, 2\gamma_2)\|_\infty < \gamma_2 - \beta. \qquad (2)$$

А так як коефіцієнти $c\mathbf{s}_2$ менше, ніж β, то додавання $c\mathbf{s}_2$ недостатньо для того, щоб викликати будь-які перенесення, збільшивши будь-який коефіцієнт низького порядку до величини, щонайменше γ_2. Таким чином, рівняння (1) є правильним, і ЕП перевіряється правильно. Детальніше ця умова розглядається нижче в розд. 4.

1.4. Загальні оцінки щодо рівня безпеки ЕП Dilithium

Якщо дотримуватись основного підходу, що викладений в [16 – 18], то безпеку механізму ЦП, що наведено на рис. 1, можна довести в моделі випадкового оракула (ROM), ґрунтуючись на складності двох проблем. Перша – це стандартна задача LWE (над кільцями поліномів), в якій пропонується відрізняти (A, t:=As_1+s_2) від (A, u), де u рівномірно випадкове. Інша проблема полягає в тому, що в [3, 18] було названо проблемою SelfTargetMSIS, тобто проблемою пошуку вектора

$$\begin{bmatrix} \mathrm{z} \\ c \\ \mathrm{v} \end{bmatrix} \tag{3}$$

з малими коефіцієнтами і повідомлення (дайджесту) μ, що задовольняє умові

$$\mathrm{H}\left(\mu \| \left[\mathrm{A} \,|\, \mathrm{t} \,|\, \mathrm{I} \right] \cdot \begin{bmatrix} \mathrm{z} \\ c \\ \mathrm{v} \end{bmatrix} \right) = c, \tag{4}$$

де A і t рівномірно випадкові, а I – одинична матриця. У ROM можна отримати (не жорстке) скорочення, використовуючи розгалужену лему [3.16] зі звичайної задачі SIS знаходження z' з малими коефіцієнтами, що задовольняють Az'=0, до SelfTargetMSIS. Можна дотримуватися цього точного підходу, щоб довести безпеку Dilithium в ROM на основі складності LWE та SIS.

У моделі квантового випадкового оракула (QROM), де зловмисник може запитувати H у суперпозиції, ситуація дещо інша. У [3, 18] було показано, що Dilithium все ще базується на LWE та SelfTargetMSIS у QROM, навіть при жорсткому скороченні, коли механізм є детермінованим. Але більше не можна безпосередньо використовувати розгалужену лему (оскільки це інший тип розгляду), щоб дати квантове скорочення від SIS до SelfTargetMSIS. Є ще вагомі підстави вважати, що задача SelfTargetMSIS, а отже, і Dilithium, є безпечною в QROM. По-перше, не існує «природних» механізмів ЕП, побудованих із Σ-протоколів, що використовують перетворення Fiat-Shamir[17], які безпечні в ROM і не безпечні в QROM. Крім того, можна встановити параметри Dilithium (залишивши структуру механізму незмінною), щоб проблема SelfTargetMSIS стала інформаційно-теоретично складною, що робить цю версію Dilithium безпечною в QROM на основі тільки LWE. Також зовсім недавно дві нові роботи ще більше звузили розрив між безпекою в ROM та QROM. Так, у [3] показано, що якщо покладений в основу Σ-протокол *руйнується*, але відрізняється особливою надійністю, то його перетворення Фіата – Шаміра є безпечним підписом в QROM.

2. Модель безпеки щодо ЕП на основі фіналіста ЕП «DILITHIUM»

Введемо поняття комплексної моделі безпеки криптографічних перетворень типу ЕП, орієнтуючись на[19 – 23]. Приймемо в якості часткових складових комплексної моделі безпеки щодо асиметричних криптоперетворень типу ЕП такі приватні моделі:

- порушника щодо асиметричних криптоперетворень типу ЕП;
- загроз щодо асиметричних криптоперетворень типу ЕП;
- безпеки щодо асиметричних криптоперетворень типу ЕП.

Нижче наводяться результати обгрунтування вказаних моделей безпеки щодо перспективних асиметричних криптоперетворень типу ЕП «DILITHIUM».

2.1. Сутність моделі порушника щодо перспективного ЕП

Побудова моделі порушника необхідна для того, щоб розробити комплекс заходів із забезпечення захищеності алгоритму. Така модель може бути побудована з урахування різних критеріїв.

По суті модель порушника – це опис можливих дій порушника, який формується на основі аналізу типу зловмисника, рівня його повноважень, знань, теоретичних та практичних можливостей. У якості порушника розглядається особа, що може отримати доступ до роботи з включеними до складу відповідної комп'ютерної системи засобами.

Порушники класифікуються за рівнем можливостей, що надаються їм штатними засобами КС. Виділяються чотири рівні таких можливостей. Класифікація є ієрархічною – кожний наступний рівень включає в себе функціональні можливості попереднього [24].

Вважатимемо, що порушник використовує усі доступні йому ресурси – найпотужніші комп'ютери і необмежний час.

Таким чином, у найгіршому випадку – порушник знає все про метод синтезу перспективного ЕП та про всі механізми безпеки, що виконуються під час синтезу та застосування, виключенням є те що криптоаналітик не знає особистого ключа чи відповідним чином обґрунтовану частину особистого ключа. У найкращому випадку порушник не знає нічого про системні параметри та ключі. У нашому випадку це рівноімовірні варіанти.

2.2. Обгрунтування та сутність моделі загроз щодо ЕП

Модель загроз ЕП (далі – Модель загроз) повинна бути документом, яким закріплено найбільш повний перелік загроз щодо існуючих та перспективних ЕП. Відповідно до Законів інформація у основних інформаційних ресурсах поділяється на відкриту і конфіденційну. Інформація у підтримуючих інформаційних ресурсах є технологічною інформацією.

При застосуванні ЕП, незалежно від видів додатків, використовуються асиметричні пари ключів, для кожної пари особистий та відкритий [3, 29, 30]. В подальшому при реальному застосуванні ЕП відкритий ключ, як правило, є сертифікатом відкритого ключа та є доступним усім користувачам інфраструктури відкритого ключа (ІВК).

Оскільки сертифікат відкритого ключа є відкритою інформацією, то під час обробки згідно з [1 – 3, 29] він повинен зберігати цілісність, справжність, доступність, неспростовність та бути захищеним від несанкціонованих дій, які можуть привести до випадкової чи умисної модифікації, нав'язування хибного чи знищення. Усім користувачам, наприклад ІВК, має бути забезпечений доступ до ознайомлення з відкритою інформацією, в даному випадку у вигляді сертифіката відкритого ключа [29, 30].

Під час обробки (застосування) конфіденційна інформація, в нашому випадку особистий ключ, вона повинна зберігати цілісність, справжність, доступність, неспростовність та бути захищеною від несанкціонованих дій, має бути практично забезпечений її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання та поширення. Тобто, безумовно має бути забезпечена конфіденційність особистого ключа кожного користувача. Також, технологічна інформація повинна бути відома тільки авторизованим на це особам та зберігати цілісність.

Таким чином, в усіх відомих додатках, у яких використовується ЕП, стосовно відкритого ключа ЕП повинне бути можливість забезпечувати його цілісність, справжність, доступність, неспростовність та бути захищеною від несанкціонованих дій, які можуть привести до випадкової чи умисної модифікації, нав'язування хибного чи знищення. Стосовно особистого ключа мають бути забезпеченими його цілісність, справжність, доступність, неспростовність та бути захищеною від несанкціонованих дій, а також повинен бути забезпеченим його захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання та поширення, тобто конфіденційність.

Тобто, як існуючі ЕП, так і перспективні ЕП, повинні дозволяти гарантовано захищати їх асиметричні пари ключів у відповідності із вказаними вище вимогами, незалежно від їх

подання при використанні – в апаратному, програмному чи апаратно-програмному вигляді. Причому, незалежно від виду їх обробки, реалізація загроз, що спрямовані на вказані ресурси, може призводити до порушення вимог безпеки первинних інформаційних ресурсів, вплинути на інше ПЗ, що підписується, та, в окремих випадках, на функціонування апаратних ресурсів.

2.3. Загальні загрози щодо ЕП

Перелік можливих загроз безпеці застосування існуючих та перспективних ЕП був сформований з числа загроз, наявних у IT-Grundschutz Catalogues з урахуванням апаратних, програмних та апаратно-програмних ресурсів, технологій обробки даних та механізмів криптографічного захисту при застосуванні ЕП.

За результатами аналізу IT-Grundschutz Catalogues щодо методів синтезу та застосування системи визначено такі загрози: атака "Людина посередині"; атака Clickjacking; викрадення даних за допомогою мобільних носіїв інформації; викрадення пристроїв, носіїв чутливої інформації та документів; витік каналами побічних електромагнітних випромінювань і наведень; відмова від дій; відмова криптомодулю; відсутнє або недостатнє оповіщення при виникненні інцидентів безпеки; відсутність дозволів для обробки персональних даних; відсутність прозорості для особи, що зацікавлена та уповноважена контролювати захист даних; відсутня або неповна документація; втрата цілісності інформації, яка повинна бути захищена; старіння криптографічних методів; зловживання повноваженнями; зловживання правами адміністратора; зловживання правами користувачів; компрометація криптографічних ключів; крадіжка чутливих даних; не виявлені інциденти інформаційної безпеки; невірне тлумачення події інформаційної безпеки; недооцінювання актуальності виправлень і змін; неналежне зберігання носіїв інформації в разі виникнення надзвичайної ситуації; необережне знищення обладнання або даних; неправильне використання криптомодулів; несанкціоноване використання криптомодулів; несанкціоноване використання прав; нестійкі криптографічні алгоритми; неякісна або відсутня автентифікація; підробні сертифікати; порушення законів або правил; проблеми при автоматизації поширення виправлень і змін; розголошення чутливої інформації; систематичний перебір паролів; троянський кінь; уразливості або помилки ПЗ; шкідливе програмне забезпечення. При синтезі та застосуванні перспективних ЕП повинне бути зроблено перекриття названих загроз.

2.4. Обгрунтування та сутність моделі безпеки щодо ЕП

В якості моделі безпеки стосовно асиметричних постквантових криптоперетворень ЕП пропонується застосовувати EUF-CMA модель [19 – 23]. EUF-CMA модель визначає екзистенційну непідроблюваність від атак на основі адаптивно вибраних повідомлень. Зокрема, безпека в сенсі EUF-CMA не дозволяє криптоаналітику (зловмиснику) виробляти ЕП для повідомлень, що залежать від ключів, наприклад ЕП, при застосуванні особистого sk ключа. По суті, при застосуванні механізму безпечного ЕП, згідно з моделлю EUF-CMA ще є безпечною для EUF-CMA у випадку, коли не застосовуються запити повідомлення. Але при наявності хоча б одного запиту повідомлення, що залежить від ключів, безпека механізму ЕП порушується.

Існує два загальних формальних визначення для забезпечення безпеки схеми ЕП. Кожне з цих визначень представлено як "гра", або експеримент, який виконується між атакуючим (attacker) та деяким чесним претендентом (challenger).

Неформально експеримент EUF-CMA (екзистенційна непідроблюваність при атаці на основі підібраних повідомлень) виконується так:

1. Претендент генерує дійсну пару ключів (pk, sk) і надає pk атакуючому.

2. Атакуючий тепер може повторно запросити підписи на підібраних(вибраних) повідомленнях (M1,..., Mq) за своїм вибором, і отримує дійсні підписи (σ1,...., σq) у відповідь.

3. По завершенню експерименту зловмисник повинен вивести повідомлення та підпис M*, σ* такі, що одне повідомлення було не одним із повідомлень, які вимагали попереднього кроку (1), і (2) повідомлення/підпис перевіряється правильно з відкритим ключем.

Схема вважається безпечною, якщо жоден (ефективний) зловмисник не має ні найменшої переваги у виконанні зазначених умов. Зазвичай кількість повідомлень q обмежується лише часом дій атакуючого, однак для спеціального випадку одноразових ЕП, зловмисник обмежується запитом лише одного підпису на кроці (2).

Це визначення досить сильне, але не настільки сильне, наскільки це можливо. Дещо сильнішим визначенням є визначення та відповідна вимога SUF-CMA.

Неформально, експеримент SUF-CMA (Сильна екзистенційна непідроблюваність при атаці на основі підібраних(вибраних) повідомлень виконується так:

1. Те саме, що і в попередньому експерименті.

2. Те саме, що і в попередньому експерименті.

3. Після завершення експерименту атакуючий повинен вивести повідомлення та підпис M*, σ* такі, що (1) пара (M*, σ*) не була одним із запитаних повідомлень, а підпис повернувся на попередньому кроці, (2) повідомлення/підпис перевіряється правильно з відкритим ключем.

Атакуючий виграє, якщо вона задовольняє наведеним умовам.

1. Головна відмінність полягає в тому, що це більш сильне визначення гарантує, що атакуючий не зможе підібрати підпис. Наприклад, схема, в якій атакуючий може повторно рандомізувати дійсний підпис, щоб він залишався дійсним, але виглядав інакше, ніж вихідне значення, не задовольнила би SUF-CMA [19, 22, 23].

2. Вищезгадане визначення безпеки EUF-CMA здійснюється одноразовими схемами підпису в очевидний спосіб – єдиною модифікацією є те, що Aeuf може запитувати оракул підпису OS лише один раз. Зокрема, безпека в сенсі EUF-CMA не дозволяє зловмиснику отримувати підписи повідомлень, залежних від ключів, як підпис на повному секретному ключі sk. Фактично, враховуючи EUF-CMA-безпечну схему ЕП, легко скласти схему підписів, яка все ще є EUF-CMA-безпечною, але один запит на повідомлення, залежного від ключів, порушує безпеку схеми.

3. Огляд та аналіз атак щодо стійкості ЕП «DILITHIUM»

3.1. Класифікація атак та загальна оцінка стійкості ЕП «DILITHIUM»

В постквантовій криптології актуальними є завданнями забезпечення криптографічної стійкості щодо класичних та квантових атак. Проблема зводиться до навчання з помилками (LWE), сутність якої у наступному.

Нехай n, q є деякими натуральними числами, χ – деякий ймовірнісний розподіл над $\mathbf{Z}$ та s – секретний вектор (множина поліномів) у $\mathbf{Z}_q^n$. Ймовірнісний розподіл $L_{s,\chi}$ над $\mathbf{Z}_q^n \times \mathbf{Z}_q$ отримується обчисленням [3, 16]

$$(a,c) = (a, \langle a, s \rangle + e) \in \mathbf{Z}_q^n \times \mathbf{Z}_q, \tag{5}$$

де $a \in \mathbf{Z}_q^n$ отримується з рівномірного розподілу та $e \in \mathbf{Z}$ з розподілу χ. Атака Decision-LWE полягає у тому, щоб визначити, чи отримана пара $(a,c) \in \mathbf{Z}_q^n \times \mathbf{Z}_q$ з розподілу $L_{s,\chi}$ або рівномірного розподілу. Її Search-LWE складова полягає у знаходженні s з пари $(a,c) \in \mathbf{Z}_q^n \times \mathbf{Z}_q$. Вважається, що як проблема Decision-LWE, так і Search-LWE [3, 16] з точки зору складності є еквівалентними та можуть бути зведені одна до одної за поліноміальний час і фактично є різними поглядами на одну і ту ж задачу. Розподіл χ для цих задач зазви-

чай є дискретним нормальним розподілом над кінцевим полем з математичним очікуванням рівним 0 та дисперсією, що характеризується параметром α. При цьому більшість атак на LWE полягають у знаходженні деякого вектора v з певною нормою на решітці L з фіксованим об'ємом $vol(L)$, але з різною розмірністю m, яка фактично характеризує оптимальну кількість пар $(a_i, c_i) \in \mathbf{Z}_q^n \times \mathbf{Z}_q$ необхідних для атаки.

Аналіз показав, що складність проблеми навчання з помилками точно знайдена лише асимптотичне. Так, доведено [31, 32], що за певних умов складність вирішення LWE в просторі розмірності n становить щонайменше $2^{O(n)}$. Цей результат зручно використовувати для оцінки загальносистемних параметрів, проте конкретні оцінки складності криптостійкості досі не відомі. Таке пов'язано з тим, що атаки на LWE зводяться в кінцевому випадку до редукції решіток.

За останні 10 років помітний суттєвий прогрес у цьому напрямку, що призводить до постійного уточнення та зміни оцінок. Він стосується більшості сучасних криптосистем, у яких використовуються варіанти LWE над поліноміальними кільцями (PR-LWE), тобто розподіл розглядається не над $\mathbf{Z}_q$, а над $\mathbf{Z}_q[X]/(f(x))$. При аналізі криптоперетворень засобом множення використовується поліном виду $f(x) = x^{2^n} + 1$ і відповідне поле $R_q = \mathbf{Z}_q[X]/(x^{2^n} + 1)$. Причому, якщо $(a_i, c_i) \in R_q \times R_q$, то задача має назву R-LWE. Коли $(a_i, c_i) \in R_q^d \times R_q$ – M-LWE відповідно.

Відмітимо, що поліном $f(x) = x^{2^n} + 1$ обраний невипадково. Його властивості дозволяють здійснити доказ про стан захищеності асиметричного криптоперетворення щодо квантових атак. Також його властивості дозволяють використати для операцій множення поліномів швидке NTT перетворення і, як наслідок, створювати швидкодіючі реалізації криптоперетворень. Однак з теорії Галуа відомо [3, 5, 7], що поле $R_q = \mathbf{Z}_q[X]/(x^{2^n} + 1)$ має складну структуру підполів, що може бути використано для здійснення криптоаналізу. Проте, на нинішній час на практиці такі атаки носять більше обмежений теоретичний характер, ніж практичний. Фактично сучасними криптологами ігноруються додаткові можливості, а R-LWE та M-LWE розглядаються як LWE. Це пояснюється тим, що для полінома $f(x) = x^{2^n} + 1$ доведено, що R-LWE та M-LWE є складнішими за LWE атаки.

На основі аналізу визначено [33 – 41], що стосовно атак на LWE можливо виділити та необхідно розглядати наступні:

1) атака грубої сили, тобто повного перебору;
2) традиційна атака зустріч посередині;
3) атака на основі алгоритму Arora-Ge;
4) BKW, коли LWE зводиться до SIS атаки;
5) диференційні атаки на помилки на детермінований ЕП на решітках;
6) Primal attack (Search-LWE зводиться до BDD атаки);
7) Dual attack (Decision-LWE зводиться до SIS);
8) зведення до uSVP атаки пошуку короткого вектора.

Розглянемо детальніше вказані атаки та зробимо їх оцінки та порівняння. Відмітимо, що атаки 1) – 4) наведеного переліку є експоненційно складними, аналіз їх складності та можливості застосування у загальному виді наведено в [33 – 39]. Попередні оцінки дозволили зробити висновки про неможливість їх використання, оскільки їх часова та просторова складності є експоненційно складними (для випадку застосування обґрунтовано вибраних розмірах системних параметрів та ключів).

В [42] запропоновано диференційні атаки на помилки на детермінований ЕП на решітках. По суті вони зводяться до розширення застосування диференційних атак на помилки на криптографію на основі решітки. Показано, чи вразливі до таких атак дві детерміновані схеми ЕП на основі решітки – Dilithium та qTESLA. Показано, що одиничні випадкові помилки можуть спричинити сценарій повторного використання початкового стана (нонсу), який дозволяє відновити ключ. Також, зроблено розширення до атак викликаних помилками з частковим повторним використанням нонсу, які не пошкоджують дійсність обчислених ЕП тому їх важче виявити.

Використовуючи лінійну алгебру та методи зведення базису решітки, зловмисник після успішного внесення помилки може отримати один із елементів секретного ключа. Деякі інші частини ключа неможливо відновити, але показано, що алгоритм підпису з підробленим підписом все ще може успішно підписувати будь-яке повідомлення. В цій же роботі зроблено експериментальні перевірки наведених атак, наприклад виконуючи збої годинника на мікроконтролері ARM Cortex-M4 [42]. Зокрема, показано, що до 65,2 % часу виконання Dilithium вразливе до непрофільованої атаки, де випадкова помилка вводиться в будь-якому місці під час процедури підпису і все ще призводить до успішного відновлення ключа. Але, віднесемо ці можливості зловмисника до атак сторонніми каналами, їх аналіз є окремою задачею досліджень.

3.2. Атаки на основі решіток

В цьому підрозділі розглядаються такі основні атаки на основі решіток:
- із застосуванням зведення LWE до BDD атаки;
- Dual Attack зі зведенням LWE до SIS атаки;
- Primal Attack виду (LWE->uSVP);
- на основі алгоритму SIS.

3.2.1. Атака зі застосуванням зведення LWE до BDD

Сутність атаки у наступному. Припускається, що відомі m пар

$$(a_i, c_i) = (a_i, \langle a_i, s_i \rangle + e_i) \in \mathbf{Z}_q^n \times \mathbf{Z}_q .$$

Зробимо запис наведеного у більш зручному вигляді

$$(A, c) = (A, A^* s + e) \in \mathbf{Z}_q^{m \times n} \times \mathbf{Z}_q^{m \times 1} . \quad (6)$$

Для (6) побудуємо решітку

$$L = \{ Ax \bmod q : x \in \mathbf{Z}_q^m \}.$$

Очевидно, що s є вектором на решітці та є найближчим до вектора $As + e$. Задача знаходження найближчого вектора на решітці до деякого довільного вектора має назву BDD та вирішується за допомогою алгоритму Бабаї [33]. Алгоритм є поліноміально складним, він працює за поліноміальний час, проте рішення знаходиться тільки з деякою ймовірністю. Для LWE цю ймовірність можна оцінити як

$$\prod_{i=0}^{m-1} erf\left(\frac{\left\| b_i^* \right\| \sqrt{\pi}}{2\alpha q} \right), \quad (7)$$

де $\left\| b_i^* \right\|$ – норми ортогоналізованих за Граммом – Шмідтом векторів базису решітки (тобто столбців матриці A). Для того щоб ймовірність вирішення BDD була близька до одиниці, потрібно зменшити $\left\| b_i^* \right\|$, тобто редукувати базис. Одним з найкращих алгоритмів для редук-

ції базиса є алгоритм блочної редукції Коркіна – Золотарьова (BKZ) та його модифікаціїї (BKZ 2.0) [38, 3]. Фактор Ерміта δ_0 для редукції можливо отримати з співвідношення

$$\begin{aligned} \left\| b_0 \right\|_2 &= \delta_0^n q^{\frac{1}{n}} \\ \left\| b_i^* \right\|_2 &\approx \delta_0^{-2i+n} * q^{\frac{1}{n}}. \end{aligned} \tag{8}$$

Алгоритм BKZ 2.0 залежить від натуральних параметрів β і m, що позначають так звані довжину блоку та кількість ітерацій відповідно, і дозволяє будувати редукований за Коркіним – Золотарьовим базис повної решітки вимірності n за $2^{E(\beta, m, n)}$ операцій, де

$$E(\beta, m, n) = 0,000784314\,\beta^2 + 0,366078\,\beta + \log((n)m) + 0,875. \tag{9}$$

В [37] описано симулятор алгоритму BKZ 2.0, який дозволяє обчислювати за вхідним параметром $\delta_0 > 1$ такі значення параметрів β і m, що застосування алгоритму BKZ 2.0 з цими параметрами до будь-якого вхідного базису повної решітки вимірності n та приводить до її редукованого базису з кореневим фактором Ерміта δ_0.

3.2.2. Dual Attack зі зведенням LWE до SIS

Існують атаки на дуальній решітці засобом зведення LWE до SIS задачі. Сутність зведення у наступному. Побудуємо спочатку решітку $L = \{x \in \mathbf{Z}_q^m \mid A^* x = 0 \bmod q\}$. Задача SIS полягає у знаходженні такого найменшого цілого $x \in \mathbf{Z}^n$, щоб $A^* x = 0$. Припустимо, що такий вектор знайдений, тоді можна вирішити задачу Decision-LWE. Нехай дано m пар $(A, c) = (A, A^* s + e) \in \mathbf{Z}_q^{m \times n} \times \mathbf{Z}_q^{m \times 1}$. Обчислимо скалярний добуток $\langle x, c \rangle$:

$$\langle x, c \rangle = x^* a^* s + x^* e = 0^* s + x^* e = x^* e = \langle x, e \rangle. \tag{10}$$

Оскільки вектор $x \in \mathbf{Z}^n$ відомий, то з цієї рівності можна знайти значення вектора помилок *e*, проте простір помилок залишається досить великим. У [40] показано, що, якщо вектор *x* має норму

$$\left\| x \right\|_2 = \frac{1}{\alpha} * \sqrt{\frac{\ln(\frac{1}{\varepsilon})}{\pi}}, \tag{11}$$

то з ймовірністю близькою до 1 можливо вирішити цю задачу, при цьому знадобиться $\frac{1}{\varepsilon^2}$ запусків вирішувача SIS. Вирішувач фактично знаходить достатньо малий вектор на решітці, тобто вирішує задачу SVP. У [33] було показано, що при цьому фактор Ерміта δ_0 має бути не більше

$$\log \delta_0 = \frac{\log^2(\frac{1}{\alpha}\sqrt{\frac{\ln(\frac{1}{\varepsilon})}{\pi}})}{4 * n \log q}. \tag{12}$$

Атаки такого типу називаються Dual Attack. Точна оцінка атаки потребує вибрати певний вирішувач. У якості вирішувача можливо взяти BKZ 2.0 і виконати оцінку як для атаки на BDD.

3.2.3. Primal Attack (LWE->uSVP)

Нехай в атаці, що розглядається, решітка містить вектор *s*. Сутність Primal Attack полягає у тому, щоб побудувати таку решітку, на якій буде лежати вектор $(s,e,1)$ і він буде найменшим унікальним вектором, тобто, вона зводиться до задачі uSVP [3]. Такою решіткою буде

$$\Lambda = \{x \in \mathbf{Z}^{m+n+1} : (A \mid I_m \mid -c) * x = 0 \bmod q\}.$$

Для пошуку вектора можливо скористатися вирішувачем BKZ 2.0 і редукувати решітку, як наслідок b_0 буде рішенням, що шукається. Далі, для вдалої редукції оцінити фактор Ерміта можливо виразом [33, 40]

$$\log \delta_0 = \frac{1}{4n^2 \ln^2 q}\left(W\left((-2n\ln q) * (\sqrt{n \log q}) * \frac{(\tau\alpha)^2}{2\pi}\right)\right)^2. \quad (13)$$

3.2.4. Зауваження стосовно алгоритму SIS

Як вище вказувалось, задачу SIS можливо звести до пошуку найменшого вектора на дуальній решітці, тобто у вигляді

$$v \approx \gamma\lambda_1(L), L = \{x \in \mathbf{Z}_q^m \mid A * x = 0 \bmod q\}. \quad (14)$$

Проте, автори Dilithium запропонували інший підхід – шукати рішення як найменший вектор на решітці з обмеженням на коефіцієнти

$$v \approx \gamma\lambda_1(L), \|\gamma\lambda_1(L)\|_\infty < \beta, L = \{Ax \bmod q : x \in \mathbf{Z}_q^m\}. \quad (15)$$

Але автори не вказують, чому вони вважають такий підхід є кращим за класичний підхід.

3.3. Аналіз атаки щодо SUF-CMA безпеки

Згідно з [43] схема підпису забезпечує SUF-CMA безпеку, яка може бути визначена як

$$Adv_{Dilithium}^{SUF-CMA}(A) \le Adv_{k,l,D}^{MLWE}(B) + Adv_{H,k,l+1,\xi}^{SelfTargetMSIS}(C) + Adv_{k,l,\xi'}^{MSIS}(D) + 2^{-254}, \quad (16)$$

де D є рівномірним розподілом над відповідним полем значень,

$$\xi = \max(\gamma_1 - \beta, 2 * \gamma_2 + 1 + 2^{d-1} * h)$$

$$\xi' = \max\left(2 * [\![(\gamma]\!]_1 - \beta\right), 4 * \gamma_2 + 2),$$

тож безпека залежить від трьох атак: MLWE, SelfTargetMSIS та MSIS.

Захист від MLWE потрібен для захисту від атак на відтворення ключа. Атаки SelfTargetMSIS та MSIS направлені на підробку повідомлення. Варто зазначити, що до MLWE є дуальна атака, яка іноді може мати кращі результати. Таким чином, для удосконаленого ЕП «DILITHIUM» потрібно знайти параметри, що є стійкими до атак Primal MLWE, Dual MLWE, SelfTargetMSIS та MSIS.

У [43, 44] для оцінки безпеки застосовувалася методика “core SVP hardness”. Вона базується на тому факті, що досі не знайдено ефективних методів експлуатації структури модульних решіток, тож можна звести MLWE та MSIS до LWE та SIS без втрати точності аналізу.

Безпеку останніх можна звести до проблеми SVP, яка є добре вивченою (порівняно з іншими проблемами на решітках). Проте з кожним роком з'являються нові більш ефективні алгоритми для вирішення цієї проблеми. Найкращим відомим алгоритмом для редукції решіток є BKZ. Він мінімізує кожен вектор решітки у ортогональному підпросторі розмірності *b*. Найкраща відома складність атаки для класичних комп'ютерів складає

$$O(2^{0.292b}) \text{ та } O(2^{0.265b}) \quad (17)$$

для квантових. Під час роботи BKZ викликає "оракула" для мінімізації у ортогональному підпросторі. Найкраща відома складність оракула складає $O(2^{0.2075b})$.

3.3.1. Аналіз атаки Primal Attack

Проблема $MLWE_{k,l,D}$ зводиться до $LWE_{nk,nl,D}$, яку у свою чергу можна звести до *unique-SVP* на решітці розмірності $d = n * l + n * k + 1$. В ній норму найменшого вектора можна оцінити як $\lambda \approx \xi * \sqrt{d}$, де ξ є середньоквадратичним відхиленням для розподілу, що використовується. Оскільки в Dilithium використовується рівномірний розподіл, то $\xi = sqrt\left(\frac{\sum i^2}{2 * \eta + 1}\right)$.

Атака вважається успішною, якщо була знайдена довжина блока, для якої проекція найменшого вектора *v* у векторний простір, натягнутий на останні *b* вектори Грамма – Шмідта, коротше ніж b^*_{d-b}. Довжину вектора *v* можна оцінити як $\delta^{2*b-d-1} * q^{\frac{m}{d}}$, де $\delta = \left((\pi * b)^{\frac{1}{b}} * \frac{b}{2 * pi * e}\right)^{\frac{1}{2(b-1)}}$, а норму проекції як $\xi\sqrt{b} \le \delta^{2*b-d-1} * q^{\frac{m}{d}}$.

Алгоритм 3.1 реалізації Primal Attack наведено нижче.

Алгоритм 3.1. Primal Attack
Вхідні данні: n, q, η, l, k
Вихідні данні: криптобезпека λ_1.

bestcost = $+\infty$
for dim $\in [5, n*k]$, $b \in [50, n*k+n*l]$ {
$d = n * l + dim + 1$
$\delta = \left((\pi * b)^{\frac{1}{b}} * \frac{b}{2 * pi * e}\right)^{\frac{1}{2(b-1)}}$
$l = \delta^{2*b-d-1} * q^{\frac{m}{d}}$
$\xi = sqrt\left(\frac{\sum i^2}{2 * \eta + 1}\right)$
Якщо $\xi\sqrt{b} \le l$ та 0.296*b <bestcost, тоді bestcost = 0.296*b
}
Return bestcost

3.3.2. Аналіз атаки Dual attack

Атака Dual attack полягає у вирішенні decision–LWE на дуальній решітці. Нехай знайдено певний вектор. Якщо рішення належить до LWE, то його коефіцієнти мають мати нормальний розподіл, інакше матиме рівномірний розподіл. Відстань між нормальним та рівномірним розподілом можна оцінити як

$$\epsilon = 4\exp\left(-2*\pi^2*\left(l*\frac{\xi}{q}\right)^2\right),$$

де l – довжина вектора, ξ – середньоквадратичне відхилення. Це значення можна трактувати як ймовірність успіху. Нажаль, вона досить мала. Для успішної атаки потрібно атаку виконати щонайменше $R = \max\left(\frac{1{,}1}{2^{(0.2075*b)\epsilon^2}}\right)$ разів. Довжину вектора можна оцінити як $\delta^{d-1}*q^{\frac{n*l}{d}}$, де d – розмірність підрешітки, що обрана для атаки.

Алгоритм 3.2 реалізації Dual attack наведено нижче.

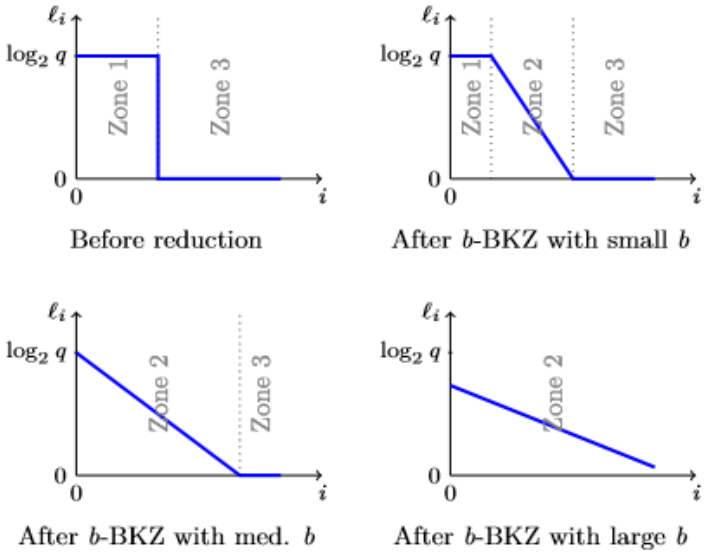
Алгоритм 3.2. Dual Attack
Вхідні параметри: n, q, k, l, η
Вихідні параметри: криптостійкість λ_2

bestcost = $+\infty$
for dim $\in [5, n*k]$, $b \in [50, n*k+n*l]$ {
$d = n*l+dim+1$
$\delta = \left((\pi*b)^{\frac{1}{b}}*\frac{b}{2*pi*e}\right)^{\frac{1}{2(b-1)}}$
$l = \delta^{d-1}*q^{\frac{n*l}{d}}$
$\xi = sqrt\left(\frac{\sum i^2}{2*\eta+1}\right)$
$\epsilon = 4\exp\left(-2*\pi^2*\left(l*\frac{\xi}{q}\right)^2\right)$
$R = \max\left(\frac{1{,}1}{2^{(0.2075*b)\epsilon^2}}\right)$
Якщо $\log_2\left(R*2^{0.2075b}\right)$<bestcost, тоді bestcost = $\log_2\left(R*2^{0.2075b}\right)$
}
Return bestcost

3.3.3. Результати застосування SIS та SelfTargetMSIS до ЕП «DILITHIUM»

У [43] було показано, що SelfTargetMSIS можна звести до MSIS, а відповідну проблему вирішення MSIS – до вирішення SIS. Задача SIS полягає у знаходженні вектору цілих чисел, які мають досить малу норму || ||. Автори пропонують шукати такий вектор за допомогою BKZ (у якому використовується $||\ ||_2$ норма). Згідно з [3, 43] після редукції решітки, що асоційована з криптосистемою ЕП «DILITHIUM», в векторах умовно можна виділити три зони. У першій зоні коефіцієнти будуть розподілені рівномірно за модулем q. У другій зоні коефі-

цієнти матимуть нормальний розподіл, а у третій зоні усі коефіцієнти дорівнюють 0. Криптостійкістю є обернена величина до добутку ймовірності того, що усі коефіцієнти менші за певне значення (що є параметром атаки) на час роботи підпроцедури, що виконує редукцію в ортогональному підпросторі із застосуванням алгоритму BKZ. Для виявлення меж зон *i, j* використовується ряд евристичних міркувань. До редукції перші вектори матимуть евклідову норму q, а останні 1. Після редукції з'явиться певний "схил". Довжина цього схили і визначатиме межі другої зони:



Згідно з [43] "крутизну схилу" можна обчислити як

$$slope(b) = -\frac{1}{b-1}\left((\pi * b)^{\frac{1}{b}} * \frac{b}{2 * pi * e}\right)$$

Алгоритм 3.3 обчислення меж зон наведено нижче.

Алгоритм 3.3. Обчислення меж зон
Вхідні данні: $b, q, q_{count}, zero_{count}$
Вихідні данні: i – кінець першої зони. j – кінець другої зони. l – довжина найбільшого вектору "на схилі".
$slope = \frac{1}{b-1}\left((\pi * b)^{\frac{1}{b}} * \frac{b}{2 * pi * e}\right)$ slope_count = $\frac{\log_2 q}{slope}$ slope_sum=slope_count*log(q)-slope*slope_count*(slope_count+1)/2 I = floor((q_count*log(q)-slope_sum)/log(q) diff = log(q)*q_count-slope_sum – i*log(q) L = log(q) +log_slope + 1.0*diff/slope_count j = i + slope_count return (i,j,L)

У [2] сказано, що рандомізація базису дозволяє зменшити складність атаки. На практиці це означає, що i=0 у алгоритмі 3.4.

Алгоритм 3.4. SIS attack
Вхідні данні: криптостійкість λ_3
Вихідні данні:
$\sigma = \frac{L}{\sqrt{J - I + 1}}$ *return* $\log_2\left(\frac{1}{p_1 * p_2 * 2^{0.207 sb}}\right)$

В розд. 4 наведено результати обчислення (генерації) системних параметрів щодо удосконаленого ЕП DILITHIUM для 128, 256, 384, 512 біт стійкості

4. Генерація загальносистемних параметрів ЕП DILITHIUM для 128, 256, 384, 512 біт стійкості

4.1. Загальні положення

Для генерації системних параметрів удосконаленого ЕП DILITHIUM використаємо результати аналізу відомих атак на криптосистему, що наведені в розд. 3, та встановимо умови, за яких забезпечується захист від них. Найочевиднішим підходом атаки криптосистеми є відновлення особистого ключа на основі використання значення відкритого ключа.

4.1.1. Атака відновлення особистого ключа на основі відкритого ключа

Як показано вище, в криптосистемі ЕП DILITHIUM вирішення цієї задачі зводиться до задачі MLWE (Module learning with errors) [43]. В літературі для аналізу MLWE використовується стратегія зведення до проблеми LWE [3, 43, 44]. З однієї сторони, це полегшує аналіз, але з іншої – залишає простір для оптимізацій. Проблема LWE може бути вирішена різними шляхами. До першого можливо віднести комбінаторні атаки, такі як BKW, Arora-Ge та зустріч посередині. Ці атаки іноді є ефективними, коли коефіцієнти полінома, що є особистим ключем, належать до деякої невеликої множини (наприклад $\{-1,0,1\}$). Як правило, їх розгляд має сенс тільки у разі гомоморфних криптосистем [3, 43]. Для ЕП DILITHIUM вони значно поступаються в ефективності і надалі розглядатися не будуть. До другої категорії належать атаки через редукцію решіток. Розглядають атаки на решітці та дуальній до неї [43]. У першому випадку будується решітка

$$\Lambda = \{x \in \mathbf{Z}^{m+n+1} : (A \mid I_m \mid -c) * x = 0 \bmod q\}. \tag{18}$$

Далі за допомогою алгоритмів редукції базису знаходиться найменший унікальний вектор (фактично задача зводиться до USVP) [44]. Для оцінки стійкості до цієї атаки зазвичай використовується підхід, що був запропонований в роботі тільки в [43]. Фактично виконується пошук найменшого розміру блоку β для BKZ, такого, що виконується умова

$$\sigma\sqrt{\beta} \le \delta_0^{2\beta-d-1} q^{\frac{n}{d}},$$

де σ, q – загальносистемні параметри, d – розмірність решітки, δ_0 – максимальне значення фактора Ерміта, за яким решітка буде достатньо редукованою. Причому δ_0 можливо вирази-

ти через β як $\delta \approx ((\pi\beta)^{\frac{1}{\beta}} * \beta / 2\pi e)^{1/2(\beta-1)}$. Таким чином, маємо нелінійне діофантове рівняння. Вирішувати його можливо повним перебором, або більш оптимізованими шляхами.

Для дуальної атаки будується решітка

$$L = \{(x, y) \in \mathbf{Z}_q^m \times \mathbf{Z}_q^n \mid A^* x = y \bmod q\} \ . \tag{19}$$

Для неї задача криптоаналітика полягає у тому, щоб визначити, чи буде знайдений після редукції вектор на цій решітці належати до розподілу, з якого отримано ключ, чи рівномірного розподілу. Згідно з [43] статистична відстань між цими двома розподілами складає $\varepsilon = 4\exp(-2\pi^2\left(\frac{l\sigma}{q}\right)^2)$, де l – довжина найменшого вектора. Відповідно, потрібно перебрати $1/\varepsilon^2$ для вдалої атаки таких векторів. Нехай вирішувач працює за час T, тоді кількість спроб можливо розрахувати як $R = \max(1, \frac{1}{T * \varepsilon^2})$. Оскільки довжина вектора l залежить від фактора Ерміта як $\delta_0^{d-1} q^{\frac{n}{d}}$, а той може бути виражений через розмір блока як

$$\delta \approx ((\pi\beta)^{\frac{1}{\beta}} * \beta / 2\pi e)^{1/2(\beta-1)},$$

то задача знову зводиться до перебору значень параметра β .

Деталізовані вище дві атаки вище називаються Primal Attack і Dual Attack відповідно і складають основу для оцінки складності криптосистем на основі LWE (та його різновидів) [43, 44]. Всі інші покращення як правило є еврістиками.

4.1.2. Атаки засобом підробки ЕП·

Іншим шляхом здійснення зловмисником атаки є підробка ЕП. У цьому разі атака здійснюється шляхом вирішення задачі SIS. Візьмемо до уваги, що дуальна атака фактично є вирішенням SIS [43, 44]. Проте автори ЕП DILITHIUM запропонували інший підхід до вирішення цієї задачі. В SIS потрібно знайти вектор, всі елементи якого менші за певну величину. Автори Dilithium пропонують шукати малі вектори на решітці до тих пір, доки всі елементи такого малого вектора не будуть менші за задану величину в задачі SIS. Нехай T – час роботи вирішувача, $p-$ ймовірність знаходження такого вектора. Тоді ймовірність атаки можливо оцінити як $\frac{1}{T * p}$. Відповідно, повторивши обчислення декілька разів, ця ймовірність зросте до потрібного рівня. Недоліком такого підходу є використання великої кількості евристичних міркувань. Проте складність оцінки криптостійкості виявляються меншою, ніж при використанні дуальної атаки. Далі, після редукції решітки в векторах умовно можна виділити, як показано вище в п. 3.3.3, три зони. У першій зоні довжини норм Грамма – Шмідта будуть розподілені рівномірно за модулем q, у другій довжини норм Грамма – Шмідта матимуть нормальний розподіл, а у третій зоні усі довжини норм Грамма – Шмідта дорівнюють 0. Якщо рандомізувати базис решітки перед редукцією, то перша зона зникає і редукція відбувається швидше.

Таким чином, потрібно, щоб перші j довжини норм Грамма – Шмідта (які розподілені за нормальним розподілом) були менші за задане значення ζ . Ймовірність цього складає

$$p = \Phi\left(\frac{\zeta}{\sigma\sqrt{2}}\right)^{j+1} \tag{20}$$

Головна проблема полягає у знаходженні необхідного значення j.

Варто окремо згадати про алгебраїчні атаки. При достатньо малих σ та достатньо великих q існують алгебраїчні атаки на LWE [45]. Для значень σ та q, що використовуються в Dilithium ці атаки не можуть бути здійснені.

4.2. Обчислення основних параметрів для удосконаленого ЕП DILITHIUM

Основні параметри для реалізації LWE та SIS атак представлені табл. 1.

Таблиця 1

Основні параметри ЕП DILITHIUM

Параметри	Значення
(N,q)	Степінь та модуль коефіцієнтів поліномів.
(k,l)	Кількість поліномів в матриці.
η	Значення коефіцієнтів особистих ключів s (знаходяться в межах $[-\eta,\eta]$.
(γ_1,γ_2)	Обмеження на максимальні значення коефіцієнтів під час вироблення підпису. Сильно впливають на стійкість до атак на підробку підпису.
β	Також впливає на максимальне значення коефіцієнтів, проте впливає не стільки на стійкість, скільки на розмір підпису. Фактично дозволяє знаходити баланс між стійкістю та техніко-економічними показниками.
d	Впливає на стійкість до атак до підробки підпису.
h	Визначає об'єм простору з якого обирається challenge
w	Впливає тільки на розмір підпису. Знаходиться з практичних міркувань.

Враховано, що чим менше N, тим швидше працюватиме схема. Автори ЕП DLILITHIUM використовують $N=256$. Збільшуючи кількість поліномів через параметри (k,l) можливо досягти будь-якого рівня стійкості до MLWE, проте для забезпечення стійкості до інших атак при використанні $N=256$ вже для рівня стійкості 384 біт не існує стійких параметрів, тому для $\lambda\in\{384,512\}$ потрібно збільшити N до 512.

Параметр q сильно впливає на стійкість. Він повинен бути простим числом. Для створення ефективних реалізацій з використанням NTT повинно виконуватися співвідношення $q\equiv 1 \bmod 2N$. Автори Dilithium використовували $q=8389417$. При збільшенні q буде знижуватися криптостійкість, немає сенсу збільшувати його значення, оскільки умова $q\equiv 1 \bmod 2N$ виконується для 256, 384, 512 біт безпеки.

Для обчислення параметрів (γ_1,γ_2) автори використовували формули

$$\gamma_1=(q-1)/16,\ \gamma_2=\gamma_1/2 \tag{21}$$

При такому виборі стійкість до всіх можливих атак буде приблизно однаковою. Такий вибір має сенс і при генерації параметрів для 256, 384, 512 біт безпеки.

Параметр h визначає кількість ненульових елементів в поліномі c. Для стійкості λ кількість можливих поліномів повинна бути не меншою за 2^λ. Тож, має виконуватися нерівність

$$2^h\binom{n}{h}\geq 2^\lambda. \tag{22}$$

Атаки на LWE можуть бути задані трьома параметрами: n, q, σ, де n – розмірність решітки (у випадку Dilithium $n = N*l+1+m, m \in \{0, N*k\}$), q – найбільше значення елементів векторів. Співпадає з значенням q в загальносистемних параметрах. σ – середньоквадратичне відхилення для розподілу, з якого отримується секретний ключ. Для ЕП DILITHIUM це значення обчислюється як

$$\sigma = \sqrt{\frac{\sum_{i=1}^{\eta} i^2}{2\eta + 1}} \tag{23}$$

Атаки на SIS параметризовано трьома параметрами: x, y, ς. Для ЕП DILITHIUM $x = N*k, y = N*l$. Параметр ζ є обмеженням на максимальне значення елементів векторів. Для ЕП DILITHIUM є дві атаки, що зводяться до SIS, тому відповідно два різних значення ζ

$$\begin{aligned} \zeta_1 &= \max(\gamma_1 - \beta, 2\gamma_2 + 1 + 2^{d-1}h) \\ \zeta_2 &= \max(2(\gamma_2 - \beta), 4\gamma_2 + 2) \end{aligned} \tag{24}$$

Якщо встановити обмеження $2^{d-1}h + 1 \le 2\gamma_2$ і врахувати що $\gamma_2 = \gamma_1/2$, то маємо:

$$\begin{aligned} \zeta_1 &\le 4\gamma_2 \\ \zeta_2 &\le 4\gamma_2 + 2 \end{aligned}. \tag{25}$$

Параметр β визначає максимальне значення коефіцієнтів поліномів $c*s_i$. Враховуючи обмеження вище, максимальне значення яке може бути отримане це $\beta = \eta h$. При такому виборі забезпечуватиметься максимальний захист від атак SIS, проте параметр β при всіх можливих значеннях майже не впливає на безпеку, тож його вплив можливо не враховувати. Проте, параметр β сильно впливає на ймовірність повтору циклу. Ця ймовірність становить

$$\approx \exp(-N\beta(\frac{l}{\gamma_1} + \frac{k}{\gamma_2})) \tag{26}$$

Тож, саме ця ймовірність є критерієм вибору параметра β.

Параметр w не впливає на криптостійкість, проте дозволяє зменшити розмір підпису ціною повтору циклу. Практичні експерименти показали, що при значенні $w = 0.08nk$ отримуються гарні результати, проте можливі подальші оптимізації.

Враховуючи приведені критерії, алгоритм генерації загальносистемних параметрів виглядає наступним чином:

1. Визначити потрібний рівень безпеки $\lambda \in \{256, 384, 512\}$;
2. Обрати значення N. Якщо $\lambda = 256$, то $N = 256$, інакше $N = 512$;
3. Обрати значення q. $q = 8389417$;
4. Обчислити γ_1 та γ_2 за формулами $\gamma_1 = (q-1)/16$, $\gamma_2 = \gamma_1/2$;
5. Обчислити значення η. За замовченням встановити $\eta = 2$. На наступних кроках значення буде уточнене;
6. Встановити значення $(k, l) = (2, 1)$;
7. Обчислити λ_1-стійкість до Primal Attack (Додаток А, алгоритм 1). Якщо стійкість менша за λ, то оновити параметри $(k, l) = (k+1, l+1)$ та повернутися до кроку 7 або збільшити η та повернутися до кроку 7;

8. Обчислити λ_2-стійкість до Dual Attack (Додаток А, алгоритм 2). Якщо стійкість менша за λ, то оновити параметри $(k,l)=(k+1,l+1)$ та повернутися до кроку 7 або збільшити η та повернутися до кроку 7;
9. Обчислити λ_3-стійкість до SIS з ζ_1 (Додаток А, алгоритм 3). Якщо стійкість менша за λ, то оновити параметри $(k,l)=(k+1,l+1)$ та повернутися до кроку 7 або збільшити $k=k+1$ та повернутися до кроку 7;
10. Обчислити λ_4-стійкість до SIS з ζ_2 (Додаток А, алгоритм 3). Якщо стійкість менша за λ, то оновити параметри $(k,l)=(k+1,l+1)$ та повернутися до кроку 7 або збільшити $k=k+1$ та повернутися до кроку 7;
11. Обчислити h як найбільше ціле, для якого виконується нерівність $2^h\binom{n}{h}\geq 2^{\lambda}$;
12. Обчислити d як найбільше ціле, для якого виконується нерівність $2^{d-1}h+1\leq 2\gamma_2$;
13. Встановити $\beta=\eta h$ та зменшувати β, щоб ймовірність повтору циклу була достатньо малою;
14. Обчислити $w=0.08nk$ (цей крок не впливає на криптостійкість та його можливо оптимізувати).

В табл. 2 наведено значення параметрів для удосконаленого ЕП DILITHIUM.

Таблиця 2

Значення параметрів для 256, 384, 512 біт стійкості

Набір	N,q	γ_1	γ_2	k,l	η	β	d	h	ω
256	(256,8380417)	523776	261888	(9,8)	2	144	14	60	184
384	(512, 8380417)	523776	261888	(7,5)	5	100	13	77	286
512	(512, 8380417)	523776	261888	(9,8)	2	74	13	118	368

Ймовірність повтору циклу при цьому складає для 256 біт – 0,15442678312246608, для 384 біт – 0,15609624568669475 і для 512 біт – 0,15247678668181552

Результати оцінки криптостійкості для удосконаленого ЕП DILITHIUM (в бітах) з використанням параметрів з табл. 2 наведено в табл. 3.

Таблиця 3

Оцінки криптостійкості для удосконаленого ЕП DILITHIUM

Набір	Primal Attack (класичний)	Primal Attack (квантовий)	Dual Attack (класичний)	Dual Attack (квантовий)	SIS (класичний)	SIS (квантовий)
256	298	270	296	269	293	266
384	440	399	438	397	503	456
512	582	527	579	525	590	535

Висновки

1. Наразі спостерігається стійкий прогрес у створенні квантових комп'ютерів. Практично завершується створення математичних основ та програмного забезпечення для таких квантових комп’ютерів. Розробляються квантові комп'ютери, що призначаються для криптоаналізу

існуючих стандартизованих криптосистем з відкритим ключем – електронних підписів, асиметричних шифрів та криптографічних протоколів різного призначення. Національний інститут стандартів і технологій (NIST) США закінчив та прийняв рішення у вигляді проєкту стандарту NIST 8309 щодо 2-го раунду конкурсу на перспективні стандартні алгоритми електронного (цифрового) підпису (ЕП). Його підсумком є визначення фіналістів другого етапу конкурсу у вигляді проєктів CRYSTALS-DILITHIUM, FALCON та Rainbow [2, 3]. Також визначені три альтернативних кандидатів, які потребують більш детальних досліджень уже на четвертому етапі конкурсу – GeMSS, Picnic та SPHINCS+.

2. Одним із основних проблемних питань, що потрібно вирішувати є обґрунтування необхідності та розробки удосконаленої версії ЕП Dilithium, що може забезпечувати в постквантовий період 128, 256, 384 і 512 біт безпеки проти класичного та 64, 128, 192 та 256 біт проти квантового криптоаналізу від найбільш загрозливих атак [2, 16 – 18].

3. Метод (схема) ЕП Dilithium ґрунтується на підході, що отримав назву "Fiat-Shamir з перериваннями. Він в певній мірі схожий на схему, що запропонована з послідовним удосконаленням в [16, 17]. В перспективі необхідно вирішувати проблему обчислення (генерування) системних параметрів для удосконаленого ЕП Dilithium.

4. В якості часткових складових комплексної моделі безпеки щодо асиметричних криптоперетворень типу ЕП прийнято та визначено такі приватні моделі:

- модель порушника щодо асиметричних криптоперетворень типу ЕП;
- модель загроз щодо асиметричних криптоперетворень типу ЕП;
- модель безпеки щодо асиметричних криптоперетворень типу ЕП.

5. Отримані результати дозволяють зробити висновок, що атаки на LWE можливо розділити на два великі класи – атаки, що ґрунтуються на переборі, та атаки, що ґрунтуються на редукції решіток. До першого класу належать атаки повного перебору, зустріч посередині та Arora-Ge. Підхід, що використаний в атаці Arora-Ge, є цікавим та перспективним, але він поки що поступається атакам на решітках.

6. Попередній аналіз дозволяє зробити висновок, що сучасні варіанти механізмів LWE ґрунтуються на поліноміальних кільцях, зокрема на $R_q = \mathbf{Z}_q[X]/(x^{2^n}+1)$. Властивості поліномів кільця дозволяють довести ряд теоретичних тверджень щодо стійкості криптосистеми і розробляти ефективні програмні реалізації. Проте, такі кільця мають нетривіальні підполя, що теоретично може використовуватися для криптоаналізу, проте на практиці атак, що застосовують ці додаткові структури, не було знайдено, або ці атаки знаходяться в незавершеному вигляді досліджень.

7. Проблеми криптоаналізу RLWE та MLWE по суті зводяться до LWE проблеми. Таке зведення можливо для $R_q = \mathbf{Z}_q[X]/(x^{2^n}+1)$, оскільки доведено, що RLWE є не менш стійким, ніж LWE. Проте, при такому підході внутрішня структура кільця ігнорується.

8. Атаки на решітках полягають у зведенні проблеми LWE до достатньо вивчених теоретичних проблем в теорії решіток. Існують три основні підходи: зведення LWE до BDD, зведення LWE до SIS, зведення LWE до SVP. Кожен з цих підходів в кінцевому випадку зводиться до задачі пошуку достатньо малого вектора на решітці, для чого використовується алгоритм BKZ та його варіації.

9. Точні оцінки для BKZ та його варіацій невідомі. При практичній оцінці використовується ряд евристичних підходів та екстраполяція результатів, що отримані на решітках меншої розмірності. Це становить основну проблему при оцінці криптостійкості систем подібних Dilithium, оскільки немає гарантії, що не з'явиться кращий спосіб редукції решіток, або оцінка виявиться недопустимо неточною.

10. Для генерації системних параметрів удосконаленого ЕП DILITHIUM використаємо результати аналізу відомих атак на криптосистему, що наведені в розд. 3, та встановимо умо-

ви, за яких забезпечується захист від них. Найочевиднішим підходом атаки криптосистеми є відновлення особистого ключа на основі використання значення відкритого ключа.

11. Деталізовані дві атаки називаються Primal Attack і Dual Attack відповідно і складають основу для оцінки складності криптосистем на основі LWE (та його різновидів) [43, 44]. Всі інші покращення як правило є евристиками.

12. Атака підробки ЕП· здійснюється шляхом вирішення задачі SIS. Візьмемо до уваги, що дуальна атака фактично є вирішенням SIS. Проте автори ЕП DILITHIUM запропонували інший підхід до вирішення цієї задачі. В SIS потрібно знайти вектор, всі елементи якого менші за певну величину. Автори Dilithium пропонують шукати малі вектори на решітці до тих пір, доки всі елементи такого малого вектора не будуть менші за задану величину в задачі SIS.

13. Враховано, що чим менше N, тим швидше працюватиме схема. Автори ЕП DLILITHIUM використовують $N = 256$. Збільшуючи кількість поліномів через параметри, (k,l), можливо досягти будь-якого рівня стійкості до MLWE, проте для забезпечення стійкості до інших атак при використанні $N = 256$ вже для рівня стійкості 384 біт не існує стійких параметрів, тому для $\lambda \in \{384,512\}$ потрібно збільшити N до 512.

14. В табл. 2, 3 наведені значення параметрів та оцінки криптостійкості для удосконаленого ЕП DILITHIUM з рівнями безпеки 256, 384, 512 біт.

Список літератури:

1. Chen L, Jordan S, Liu Y-K, Moody D, Peralta R, Perlner RA, Smith-Tone D (2016) Report on Post-Quantum Cryptography. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8105. https://doi.org/10.6028/NIST.IR.8105.
2. Gorjan Alagic Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. NISTIR 8309 / Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone // 22 July 2020. Режим доступу: https://doi.org/10.6028/NIST.IR.8309.
3. ЕП Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler and Damien Stehlé CRYSTALS-Dilithium: Algorithm Specifications and Supporting Documentation. Access mode: https://pq-crystals.org/dilithium/data/dilithium-specification.pdf.
4. Post-Quantum Cryptography. Round 2 Submissions. [Електронний ресурс]. Режим доступу: https://csrc.nist.gov/Projects/post-quantum-cryptography/round-2-submissions.
5. Горбенко Ю. І. Аналіз можливостей квантових комп'ютерів та квантових обчислень для криптоаналізу сучасних криптосистем / Ю. І. Горбенко, Р. С. Ганзя // Східно-європейський журнал передових технологій. 2014. № 1/9 (67). С. 8–15.
6. ISCI'2019: Information Security in Critical Infrastructures. Collective monograph. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov. ASC Academic Publishing, USA, 2019. 445 p.
7. Gorbenko Ivan The problem of cryptographic transformations standardization and the state of its solution / Ivan Gorbenko, Olena Kachko, Oleksandr Kuznetsov, Yurii Gorbenko, Maryna Yesina // VII Міжнар. наук.-техн. конф. "Захист інформації і безпека інформаційних систем" : Праці Науково-технічної конференції, 30–31 травня 2019 р. Львів : Нац. ун-т "Львівська політехніка", 2019. С. 84-85.
8. Горбенко І. Д. Порівняння, оцінювання, дослідження можливості використання та переваг постквантових алгоритмів / І. Д. Горбенко, В. А. Пономар, М. В. Єсіна // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Київ : Нац. техн. ун-т України "Київський політехнічний інститут імені Ігоря Сікорського", 2017. Вип. 2(34). С. 9-32.
9. Горбенко Ю. І. Аналіз можливостей квантових комп'ютерів та квантових обчислень для криптоаналізу сучасних криптосистем / Ю. І. Горбенко, Р. С. Ганзя // Східно-європейський журнал передових технологій. 2014. № 1/9 (67). С. 8–15.
10. Квантовые компьютеры. [Електронний ресурс]. Режим доступу: http://www.nkj.ru/archive/articles/5309/.
11. Горбенко І. Д., Постквантова криптографія та механізми її реалізації / І. Д. Горбенко, О. О. Кузнецов, О. В. Потій, Ю. І. Горбенко, Р. С., Ганзя, В. А. Пономар // Радиотехника. 2017. Вып. 186. С. 32–52.
12. ДСТУ 8961:2019 Інформаційні технології. Криптографічний захист інформації. Алгоритми асиметричного шифрування та інкапсуляції ключів. [Електронний ресурс]. Режим доступу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=88056.
13. Vadim Lyubashevsky. Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures. In ASIACRYPT, pages 598–616, 2009.

14. Vadim Lyubashevsky. Lattice signatures without trapdoors. In EUROCRYPT, pages 738–755, 2012.
15. Tim Güneysu, Vadim Lyubashevsky, and Thomas Pöppelmann. Practical lattice-based cryptography: A signature scheme for embedded systems. In CHES, pages 530–547, 2012.
16. Eike Kiltz, Vadim Lyubashevsky, and Christian Schaffner. A concrete treatment of Fiat-Shamir signatures in the quantum random-oracle model. Cryptology ePrint Archive, Report 2017/916, 2017. Access mode: https://eprint.iacr.org/2017/916.
17. Lyubashevsly V (2009) Fiat-Shamir with aborts: Applications to Lattice and Factoring-Based Signatures. International Conference on the Theory and Application of Cryptology and Information Security – ASIACRYPT (Springer), pp. 598-616. https://doi.org/10.1007/978-3-642-10366-7_35.
18. Don J, Fehr S, Majenz C, Schaffner C (2019) Security of the Fiat-Shamir Transformation in the Quantum Random-Oracle Model. Annual International Cryptology Conference – CRYPTO (Springer), p. 356-383. https://doi.org/10.1007/978-3-030-26951-7_13.
19. Єсіна М. В. Моделі безпеки постквантових криптографічних примітивів / М. В. Єсіна // Міжнародний науковий симпозіум "Питання оптимізації обчислень (ПОО-XLVI)", 2019 р. Математичне на комп'ютерне моделювання. Серія: Технічні науки. Вип. 19. С. 49-55.
20. V. Shoup On Formal Models for Secure Key Exchange, Theory of Cryptography Library, 1999. [Електронний ресурс]. Режим доступу: http://philby.ucsd.edu/cryptolib/1999/9912.html.
21. M. Bellare, R. Canetti, H. Krawczyk A modular approach to the design and analysis of authentication and key-exchange protocols. 30th STOC 1998.
22. Privacy for Code-Based Encryption in the Standard Model. In: Lange T., Takagi T. (eds) Post-Quantum Cryptography. PQCrypto 2017. Lecture Notes in Computer Science, vol 10346. Springer, Cham.
23. M. Bellare, A. Boldyreva, A. Desai, D. Pointcheval Key-privacy in public-key encryption. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248. P. 566–582. Springer, Heidelberg (2001). doi:10.1007/3-540-45682-1.
24. Державна служба спеціального зв'язку та захисту інформації України. Наказ від 20.07.2007 №141 «Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної та відкритої інформації з використанням електронного цифрового підпису» № 862/14129.
25. Закон України «Про основні засади забезпечення кібербезпеки України» // Відомості Верховної Ради (ВВР). 2017. № 45. Ст. 403.
26. Закон України «Про електронні довірчі послуги» // Відомості Верховної Ради (ВВР), 2017. № 45. Ст. 400).
27. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах".
28. Закон України "Про захист персональних даних.
29. Горбенко Ю. І. Методи побудування та аналізу криптографічних систем : монографія. Харків : Форт, 2015. 959 с.
30. Горбенко І. Д. Прикладна криптологія: Монографія / Горбенко І. Д., Горбенко Ю. І. 2-ге вид. Харків : Форт, 2012. 868 с.
31. Albrecht M.R., Goepfert F., Virdia F., Wunderer T. Revisiting the expected cost of solwing uSVP and applications to LWE // Cryptology ePrint Archive, Report 2017/815. Access mode: http://eprint.iacr.org/2017/815.
32. Albrecht M.R., Player R., Scott S. On the concrete hardness of learning with errors // Cryptology ePrint Archive, Report 2015/046. Access mode: http://eprint.iacr.org/2015/046.
33. Rachel Player Parameter selection in lattice-based cryptography. Access mode: https://pure.royalholloway.ac.uk/portal/files/29983580/2018playerrphd.pdf.
34. Gottfried Herold, Elena Kirshanova and Alexander May. On the asymptotic complexity of solving LWE // Designs, Codes and Cryptography, Jan 2017.
35. Shi Bai and Steven D. Galbraith. Lattice decoding attacks on binary LWE // Willy Susilo and Yi Mu, editors, ACISP 14, vol. 8544 of LNCS, pages 322–337. Springer, Heidelberg, July 2011.
36. Sanjeev Arora and Rong Ge. New algorithms for learning in presence of errors // Luca Aceto, Monika Henzinger, and Jiri Sgall, editors, ICALP 2011, Part I, vol. 6755 of LNCS, pages 403–415. Springer, Heidelberg, July 2011.
37. Martin R. Albrecht, Carlos Cid, Jean-Charles Faugère, and Ludovic Perret. Algebraic algorithms for LWE. Cryptology ePrint Archive, Report 2014/1018, 2014. Access mode: http://eprint.iacr.org/2014/1018.
38. Martin R. Albrecht, Carlos Cid, Jean-Charles Faugère, Robert Fitzpatrick, and Ludovic Perret. On the complexity of the BKW algorithm on LWE // Designs, Codes and Cryptography, 74:325–354, 2015.
39. Martin R. Albrecht, Jean-Charles Faugère, Robert Fitzpatrick, and Ludovic Perret. Lazy modulus switching for the BKW algorithm on LWE // Hugo Krawczyk, editor, PKC 2014, vol. 8383 of LNCS, pages 429–445. Springer, Heidelberg, March 2014.
40. Richard Lindner and Chris Peikert. Better key sizes (and attacks) for LWE-based encryption // Aggelos Kiayias, editor, CT-RSA 2011, vol. 6558 of LNCS, pages 319–339. Springer, Heidelberg, February 2011.
41. Avrim Blum, Adam Kalai, and Hal Wasserman. Noise-tolerant learning, the parity problem, and the statistical query model // Journal of the ACM, 50(4): 506–519, July 2003.
42. Leon Groot Bruinderink1 and Peter Pessl2 . Differential Fault Attacks on Deterministic Lattice Signatures.

43. Lyubachevsky V., Ducas L., Kiltz E. [et all]. CRYSTALS–Dilithium. Techn. rep. NIST (2017). [Electronic resource]. Access mode: https://crc.nist.gov./projects/post-quantum-cryptogtraphy/ round-1-submissions.

44. Albrecht M.R., Goepfert F., Virdia F., Wunderer T. Revisiting the expected cost of solwing uSVP and applications to LWE // Cryptology ePrint Archive, Report 2017/815. Access mode: http://eprint.iacr.org/2017/815.

45. Peikert C., How (not) to instanaite Ring-LWE // Cryptology ePrintAchive 2016/351, 2016.

46. Горбенко І. Д. Особливості побудування та аналіз електронних підписів 5 рівня безпеки для постквантового періоду на основі алгебраїчних решіток / І. Д. Горбенко, О. Г. Качко, А. М. Олексійчук, Ю. І. Горбенко, В. П. Звєрєв, М. В. Єсіна, В. А. Пономар // Прикладная радиоэлектроника. Харьков : ХНУРЭ, 2019. Т. 18, № 3, 4. С. 123–136.

Надійшла до редколегії 05.08.2020

Відомості про авторів:

Горбенко Іван Дмитрович – д-р техн. наук, професор, Харківський національний університет імені В.Н. Каразіна, професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, головний конструктор АТ «Інститут інформаційних технологій», Україна, e-mail: GorbenkoI@iit.kharkov.ua, ORCID: https://orcid.org/0000-0003-4616-3449

Олексійчук Антон Миколайович – д-р техн. наук, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "КПІ", професор спеціальної кафедри №1, Україна, ORCID: https://orcid.org/0000-0003-4385-4631

Качко Олена Григорівна – канд. техн. наук, Харківський національний університет радіоелектроніки, професор кафедри програмної інженерії, начальник відділу програмування АТ «Інститут інформаційних технологій», Україна, e-mail: iit@iit.kharkov.ua, ORCID: https://orcid.org/0000-0001-9249-0497

Горбенко Юрій Іванович – канд. техн. наук, АТ «інститут інформаційних технологій», перший заступник головного конструктора, Україна, e-mail: gorbenkou@iit.kharkov.ua, ORCID: https://orcid.org/0000-0003-0073-9107

Єсіна Марина Віталіївна – канд. техн. наук, Харківський національний університет імені В. Н. Каразіна, старший викладач кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Україна, e-mail: rinayes20@gmail.com, ORCID: https://orcid.org/0000-0002-1252-7606

Кандій Сергій Олександрович - Харківський національний університет імені В.Н. Каразіна, студент кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Україна, e-mail: kandy.sergey@yandex.ua

УДК 004.056.55 **DOI:10.30837/rt.2020.3.202.02**

Ю.І. ГОРБЕНКО, канд. техн. наук, О.В. ПОТІЙ, д-р техн. наук,
В.В. ОНОПРІЄНКО, канд. техн. наук, М.В. ЄСІНА, канд. техн. наук, Г.А. МАЛЄЄВА

ОСНОВНІ ПОЛОЖЕННЯ ЩОДО МОДЕЛІ БЕЗПЕКИ ДЛЯ АСИМЕТРИЧНИХ ПЕРЕТВОРЕНЬ ТИПУ ЕП З УРАХУВАННЯМ ВИМОГ ТА ЗАГРОЗ ПОСТКВАНТОВОГО ПЕРІОДУ

Вступ

Стосовно криптографічної стійкості (безпеки) асиметричних криптоперетворень, як і симетричних криптоперетворень, для оцінки використовуються існуючі методи, методики та різні системи криптоаналізу. Такий вузький підхід при аналізі стійкості залишає без необхідного врахування можливі моделі порушника, моделі загроз, а також не дає можливих варіантів протидії. На наш погляд, продуктивним може бути введення та використання узагальненої (комплексної) моделі криптографічної стійкості. Приймемо в якості складових комплексної моделі безпеки щодо асиметричних криптоперетворень типу ЕП такі часткові моделі:

- порушника щодо асиметричних криптоперетворень типу ЕП;
- загроз щодо асиметричних криптоперетворень типу ЕП;
- безпеки щодо асиметричних криптоперетворень типу ЕП.

При викладенні сутності, призначення, можливостей застосування та обмежень щодо такої комплексної моделі будемо орієнтуватись та використовувати результати теоретичного обґрунтування та розробки вказаних часткових моделей безпеки та комплексної моделі безпеки у цілому. Метою цієї статі є обґрунтування та розробка пропозицій щодо побудування комплексної моделі безпеки стосовно асиметричних криптоперетворень типу перспективний ЕП, що може та повинен застосовуватись в постквантовий період.

1. Визначення моделей порушника, загроз та безпеки щодо перспективного ЕП

Побудова моделі порушника необхідна для того, щоб розробити комплекс заходів із забезпечення захищеності механізмів ЕП, в тому числі з урахуванням вимог та умов їх застосування в постквантовий період. Така модель порушника може бути побудована з урахування різних критеріїв.

Звичайно модель порушника розробляється з метою отримання відповідей на наступні питання:

- від кого необхідно захищати інформацію?
- якою є мета порушника?
- якими знаннями володіє порушник?
- які повноваження в системі має потенційний порушник?
- які методи, системи та засоби використовує порушник?

По суті модель порушника – це опис можливих дій порушника, який формується на основі аналізу типу зловмисника, рівня його повноважень, знань, теоретичних та практичних можливостей. У якості порушника розглядається особа, що може отримати доступ до роботи з включеними до складу відповідної комп'ютерної системи (КС) засобами.

Модель загроз ЕП (далі – модель загроз) повинна бути документом, яким закріплено найбільш повний перелік загроз щодо існуючих та перспективних ЕП, що може застосовуватись в постквантовий період. Відповідно до Законів України "Про захист інформації в інформаційно-телекомунікаційних системах", "Про електронні довірчі послуги" та "Про захист персональних даних". Перелік можливих загроз безпеці застосування існуючих та перспективних ЕП сформований з числа загроз, наявних у IT-Grundschutz Catalogues [10] з урахуванням апаратних, програмних та апаратно-програмних ресурсів, технологій обробки даних та механізмів криптографічного захисту при застосуванні ЕП, в тому числі з урахуванням вимог та умов синтезу перспективних ЕП та застосування ЕП в постквантовий період.

Основними загрозами (атаками) з застосуванням квантових математичних методів, які можуть бути реалізованими на квантовому комп'ютері (звичайно, якщо він буде побудований та доступний для застосування), є такі:

- квантовий алгоритм факторизації Шора;
- квантовий алгоритм Гровера;
- квантовий алгоритм Шора вирішення дискретного логарифму в полі;
- квантовий алгоритм Шора вирішення дискретного логарифму в групі точок еліптичної кривої;
- квантовий алгоритм криптоаналізу для перетворень в фактор-кільці тощо.

Стосовно перспективного ЕП можливо виділити та необхідно, як мінімум, розглядати наступні атаки (загрози):

1. Атака грубої сили, тобто повного перебору.
2. Традиційна атака зустріч посередині.
3. Атака на основі алгоритму Arora-Ge.
4. Диференційні атаки.
5. BKW, коли LWE зводиться до SIS атаки.
6. Primal attack (Search-LWE зводиться до BDD атаки).
7. Dual attack (Decision-LWE зводиться до SIS).
8. Зведення до uSVP атаки пошуку короткого вектора.

Для однозначного розуміння та використання також введемо поняття щодо моделі безпеки (криптографічної стійкості) стандартизованих криптографічних примітивів ЕП. Модель безпеки (криптографічної стійкості) криптографічних примітивів (в тому числі типу ЕП) – це сукупність організаційно-технічних, програмно-технічних та логічних механізмів (методів) та заходів, законодавчих та нормативно-правових норм та правил, що визначають вимоги до методів синтезу, оцінки криптографічної стійкості та застосування стандартизованих криптографічних примітивів (типу ЕП), з урахуванням умов їх реалізації при інтенсивній протидії порушника 4-го рівня [8, 9] із застосуванням методів, систем та засобів класичного та квантового криптоаналізу.

Аналіз показує, що NIST США планує стандартизувати один чи декілька стандартизованих криптопримітивів типу ЕП, що будуть забезпечувати екзистенційну стійкість ЕП щодо атак на основі адаптивно підібраного повідомлення. Така безпека позначається в науковій літературі як EUF-CMA безпека [1, 2]. Представлені кандидати ЕП оцінюються на підставі того, наскільки такі можливості існують для кандидата на постквантовий стандарт, щоб забезпечити таку його властивість. Але така вимога не є обов'язковою, заявники не зобов'язані надавати докази безпеки щодо атаки на основі адаптивно підібраного повідомлення, хоча такі докази вже розглядаються та розглядатимуться при подальших дослідженнях, якщо вони будуть наявні (доступні).

Важливим є те, що у якості апріорних даних запропоновано вважати, що зловмисник має доступ не більш, ніж до 2^{64} обраних повідомлень. Проте, атаки за умови більшої кількості повідомлень також можуть розглядатись. Крім того, скоріше всього NIST розглядає як класичні, так і квантові атаки.

2. Загальні положення щодо моделі безпеки перспективного ЕП

Модель безпеки EUF-CMA визначає екзистенційну непідроблюваність від атак на основі адаптивно вибраних повідомлень [1, 2, 5]. Зокрема, безпека в сенсі EUF-CMA повинна протидіяти порушнику 4-го рівня виробляти ЕП для повідомлень, що залежать від ключів (застосуванні особистого sk ключа). По суті, при застосуванні механізму безпечного ЕП, згідно моделі EUF-CMA, вона є безпечною для EUF-CMA у випадку, коли не застосовуються запити повідомлення. Але, при наявності хоча б одного запиту повідомлення, що залежить від ключів, безпека механізму ЕП порушується.

Існує два загальних формальних визначення для забезпечення безпеки схеми ЕП [7]. Кожне з цих визначень представлено як експеримент, який виконується між атакуючим (attacker) та деяким чесним претендентом (challenger).

Експеримент щодо моделі EUF-CMA (екзистенційна непідроблюваність при атаці на основі підібраних повідомлень) виконується у такій послідовності:

1. Претендент генерує дійсну пару ключів (pk, sk) і надає pk атакуючому.

2. Далі атакуючий може повторно запросити підписи на підібраних (вибраних) повідомленнях (M_1,...,M_q) за своїм вибором, і отримує дійсні підписи (σ_1,...., σ_q) у відповідь.

3. По завершенню експерименту зловмисник повинен вивести повідомлення та підпис M*, σ* такі, що одне повідомлення було не одним із повідомлень, які вимагали попереднього кроку (1), і (2) повідомлення/підпис перевіряється правильно з відкритим ключем.

Така схема вважається безпечною, якщо жоден (ефективний) зловмисник не має ні найменшої переваги у виконанні вищезазначених умов. Зазвичай кількість повідомлень q обмежується лише часом дій атакуючого, однак для спеціального випадку одноразових ЕП, зловмисник обмежується запитом лише одного підпису на кроці (2).

Така властивість є досить сильною, але не настільки як можливо. Дещо сильнішим визначенням є визначення моделі безпеки SUF-CMA [7].

Експеримент із застосуванням моделі SUF-CMA (сильна екзистенційна непідроблюваність при атаці на основі підібраних) повідомлень) виконується у такій послідовності:

1. Те саме, що і в попередньому експерименті.

2. Те саме, що і в попередньому експерименті.

3. Після завершення п. 2 експерименту, атакуючий повинен вивести повідомлення та підпис M*, σ* такі, що (1) пара (M*, σ*) не була одним із запитаних повідомлень, а підпис повернувся на попередньому кроці, (2) повідомлення/підпис перевіряється правильно з відкритим ключем.

Атакуючий виграє, якщо вона задовольняє вищенаведеним умовам.

Головна відмінність моделі SUF-CMA полягає в тому, що це більш сильне визначення гарантує, що атакуючий не зможе підібрати підпис. Так, схема, в якій атакуючий може повторно рандомізувати дійсний підпис, щоб він залишався дійсним, але виглядав інакше, ніж вихідне значення, не задовольнила би умові SUF-CMA.

Введемо визначення 1 гри між зловмисником та схемою підпису використовуючи [7].

Нехай EUF–CMA–GAME(Gen, Sign, Ver, A, n), причому виконуються пункти 1 – 7.

1. Gen(1n) (sk, vk);

2. A отримує vk;

3. A створює повідомлення m;

4. A отримує s Sign(sk, m);

5. A повторює кроки 3 та 4, якщо це необхідно;

6. A виводить (m*, s*);

7. A виграє, якщо Ver(vk, m*, s*)=accept та m* не було раніше підписано Sign.

Тоді дійсним є визначення 1.

Визначення 1. Схема підпису є EUF-CMA безпечною, якщо для будь-якого зловмисника A, що виконується за поліноміальний час, ймовірність виграшу EUF-CMA-GAME є незначною.

3. Попередні дані та визначення

Як вже зазначалося і як буде показано далі, для цілей безпеки вкрай важливо допустити алгоритм підпису з відслідковуванням стану (stateful).

Це забезпечується на основі використання та врахування наступного:

- KDM – повідомлення, залежне від ключа;
- KD – залежність від ключа;
- KDS – підписи, залежні від ключів;

- EUF-CMA – екзистенційна непідроблюваність при атаці на основі адаптивно підібраних (вибраних) повідомлень;
- Aeuf – зловмисник (імовірнісний алгоритм поліноміального часу) при EUF-CMA
- Akds – зловмисник (імовірнісний алгоритм поліноміального часу) при KDS-CMA;
- Akd – зловмисник (імовірнісний алгоритм поліноміального часу) при KD-EUF;
  OS – оракул підпису при Aeuf.
- безпека розглядається в сенсі KDS-CMA означає безпеку в сенсі EUF-CMA;
- CMA – атака на основі адаптивно підібраних (вибраних) повідомлень.

Також використовується «пряма» секретність (forward security, forward secrecy), як властивість криптосистем зберігати конфіденційність минулих сеансових ключів при компрометації довгострокового ключа.

Також застосовується досконала пряма секретність (perfect forward secrecy (PFS)), яка означає, що сеансовий ключ, який генерується з використанням довгострокових ключів, не буде скомпрометований при умові, якщо один або декілька з цих довгострокових ключів будуть скомпрометовані у майбутньому.

Аналіз показав [6, 7], що моделі безпеки щодо підписів засновуються на принципах та понятті теорії ігор. Поняття теорії ігор може використовуватись у такому змісті.

Теорія ігор – це теорія математичних моделей прийняття оптимальних рішень в умовах конфлікту. Оскільки сторони, що беруть участь в більшості конфліктів, зацікавлені в тому, щоб приховати від супротивника власні наміри, прийняття рішень в умовах конфлікту, зазвичай, відбувається в умовах невизначеності. Фактор невизначеності можна інтерпретувати як противника суб'єкта, який приймає рішення. Логічною основою теорії ігор є формалізація трьох понять, які входять в її визначення і є фундаментальними для всієї теорії: конфлікт; приймання рішення у конфлікті; оптимальність прийнятого рішення.

4. Аналіз схем підписів та екзистенційна непідроблюваність

Подальший аналіз можна провести засобом використання визначень 2 та 3 із [7].

Визначення 2 [7] (Схема підпису). Схема підпису S є трійкою поліноміальних алгоритмів S=(K, S, V):

K − імовірнісний алгоритм генерації ключа, який при введенні параметру безпеки 1k повертає пару (sk, pk) ключів − відкритий ключ перевірки pk з відповідним секретним ключем підпису sk {0,1}*. У випадку підписувача з відслідковуванням стану (stateful) sk інтерпретуємо як початковий стан підписувача, тобто вся секретна інформація підписувача є частиною його стану;

S − імовірнісний алгоритм підпису, який при введенні повідомлення M {0,1}* та стану sk − який у випадку підписувача без стану (stateless) є лише секретним ключем − повертає підпис σ {0,1}* на M або символ помилки. Крім того, оновлюється стан значення sk;

V − це детерміністичний алгоритм перевірки, який при введенні відкритого ключа pk, повідомлення M та підпису кандидата σ для M повертає true або false, вказуючи, чи є σ дійсним підписом для M при відкритому ключі pk.

Далі, для пар ключа (sk, pk), що виводяться за допомогою K, вимагаємо, щоб із переважною ймовірністю мала місце очевидна умова правильності – для всіх повідомлень M маємо Vpk(M, Ssk(M))=true.

Стандартна вимога до безпеки для схем підписів – EUF-CMA, що означає екзистенційну непідроблюваність при атаці адаптивно підібраних повідомлень.

Визначення 3 [7]. (EUF-CMA). Нехай S=(K, S, V) буде схемою підпису, і Aeuf – імовірнісним алгоритмом, що виконується за поліноміальний час. Сценарій атаки буде такий:

1. Обчислити пару ключів (sk, pk) K(1k) та pk як вхідні дані Aeuf.

2. Зловмиснику Aeuf надається необмежений доступ до оракулу підпису OS для виконання Ssk( ).

3. Зрештою, Aeuf виводить повідомлення M та підпис σ.

Зауваження 1. Вищезгадане визначення безпеки EUF-CMA є дійсними одноразовими схемами підпису в очевидний спосіб – єдиною модифікацією є те, що Aeuf може запитувати оракул підпису OS лише один раз.

Зокрема, безпека в сенсі EUF-CMA не дозволяє зловмиснику отримувати підписи повідомлень, залежних від ключів, як підпис на повному секретному ключі (стані) sk. Фактично, враховуючи EUF-CMA-безпечну схему підпису, легко скласти схему підписів, яка все ще є EUF-CMA-безпечною, але один запит на повідомлення, залежного від ключів, порушує безпеку схеми.

5. Аналіз безпеки за наявності підписів, залежних від ключів

В ряді випадків схема підпису S=(K, S, V) називається KDS-CMA-безпечною, якщо вона є захищеною, незважаючи на здатність зловмисника отримувати підписи на довільних (таких, що ефективно обчислюються) функціях g стану sk підписувача. Зокрема, g має доступ до секретного ключа, що зберігається під час підписування.

Визначення 4 [7] (KDS-CMA). Нехай трійка S=(K, S, V) буде схемою підпису, і Akds – це імовірнісний алгоритм поліноміального часу. Нехай реалізується такий сценарій атаки:

1. Обчислити пару ключів (sk, pk) K(1k) та pk – як вхідні дані до Akds.

2. Зловмисник Akds отримує необмежений доступ до оракула підпису. Оракул приймає як вхідну функцію g, представлену як логічна схема поліноміального розміру, і виконує алгоритм підпису S із поточним станом sk і повідомлення g(sk) як вхідними даними (у моделі випадкового оракула g може викликати випадковий оракул).

3. Зрештою, Akds виводить повідомлення M {0,1}* і підпис σ.

Необхідно відмітити, що оцінка ефективності моделі безпеки KDS-CMA в сенсі KDS-CMA означає безпеку в сенсі EUF-CMA, і виникає питання, чи/як може бути досягнута безпека в сенсі *Визначення* 3.

6. Неможливість KDS-CMA з алгоритмом підпису без стану (stateless)

Як перший (негативний) результат необхідно відмітити, що жодна схема підпису з алгоритмом підписування без стану не може відповідати цілі безпеки KDS-CMA-безпечності.

Зауваження 2[7]. Нехай S=(K, S, V) буде схемою підпису з алгоритмом підписування без стану S, тобто секретний ключ підпису sk не змінюється шляхом виконання S. Тоді схема підпису S не є безпечною в сенсі KDS-CMA.

Незважаючи на свою простоту, атака в доказі зауваження 2[7] є досить руйнівною, і це може виявитися незрозумілим.

Як правило для моделі прямої безпеки розглядаються так звані схеми підпису з ключами, що розвиваються, та компрометація поточного секретного ключа не дозволяє зловмиснику підроблювати попередні підписи. Підписи для повідомлень, підписаних раніше при фіксованому відкритому ключі, дійсні, навіть, якщо поточний секретний ключ розкрито. Крім того, зловмисник не може підробити підпис з "датою" перед розголошенням ключа.

7. Схеми підпису з ключами, що розвиваються, та пряма безпека

Визначення 5. Схема підпису з ключем, що модифікується. Схема підпису з ключем, що «розвивається». Така схема Sf є кортежем з чотирьох елементів поліноміальних алгоритмів S=(Kf, Uf, Sf, Vf):

1. Kf – імовірнісний алгоритм генерації ключа, у якому при введенні параметра безпеки 1k, загальна кількість періодів часу T (і, можливо, інші параметри) повертає пару (sk0, pk) ключів – відкритий ключ перевірки pk з відповідним (базовим) секретним ключем підпису sk0.

2. Uf – детермінований алгоритм оновлення секретного ключа, який приймає в якості вхідних даних секретний ключ підпису sk_{j-1} попереднього періоду j−1 і повертає секретний ключ підпису sk_j для періоду j.

3. Sf – імовірнісний алгоритм підпису, у якого вхідними даними є повідомлення M {0, 1}* та секретний ключ підпису sk_j поточного періоду часу j повертає підпис для M для періоду j або повертає символ помилки.

4. Vf – це детермінований алгоритм перевірки, у якого вхідними даними є відкритий ключ pk, повідомлення M і підпис, повертає true або false, що вказує на те, що підпис прийнято або відхилено відповідно.

Можна припустити, що sk_j зберігає саме значення j для періоду j {1,...,T}, а також загальне число T періодів часу. Далі, приймається рішення про те, що skT+1 – це порожній рядок і, що Uf(skT) повертає skT+1. І поточний період часу j, і загальна кількість періодів T є загальновідомими та доступними для зловмисника Afwd разом із атакованим відкритим ключем pk. Фактична гра атаки, яка використовується для визначення прямої безпеки схеми підпису з ключем, що «розвивається», включає в себе три етапи – етап атаки підібраного повідомлення (cma), етап розриву (breakin) та етап підробки (forge).

Визначення 6 (FWD-CMA – пряма безпека). Нехай Sf=(Kf, Uf, Sf, Vf) – це схема підпису з ключем, що розвивається, і нехай Afwd – це імовірнісний поліноміальний алгоритм. Тоді важливим для рішення є сценарій.

1. CMA стадія

Встановити j←0, і згенерувати пару ключів (sk0, pk) Kf(1k,...,T). (Тут '...' вказує, що додаткові вхідні параметри можуть бути присутніми).

repeat
  j←j+1; skj←Uf(skj−1)
 (cma, pk)
until (d = breakin) or (j = T)
if d ≠ breakin and j = T
 then j = T + 1
end if

2. Breakin стадія

Зловмиснику Afwd передається поточний секретний ключ sk_j.

3. Forge стадія

Зрештою, Afwd виводить повідомлення M та підпис з b<j.

Нехай QueriedEarlier – це подія, що Afwd виводить повідомлення M, яке вже було запитано до оракула підпису.

Процес у *визначенні* 5 суворо упорядкований тим, що як тільки зловмисник відмовляється від оракула підпису для sk_j, він не може знову отримати доступ до цього оракула. У якийсь момент зловмисник Afwd вирішує скористатися своїм привілеєм розриву, і повертає поточний секретний ключ sk_j. Щоб бути успішним Afwd повинен підробити підпис з sk_b для деяких b<j і нового повідомлення M.

Зауваження 3 [7]. За визначенням безпечна схема FWD-CMA дозволяє зловмиснику Afwd подавати поліноміальну кількість запитів до його оракула підпису протягом одного часового періоду j. Таким чином, за наявності повідомлень залежних від ключів, атака, як показано в доказі *зауваження* 2, може розкрити повний секретний ключ, перед тим як з'явиться оновлення секретного ключа. Іншими словами, безпека у сенсі FWD-CMA не передбачає сильних гарантій безпеки при наявності повідомлень залежних від ключів.

На противагу вищезазначеному негативному твердженню після застосування деяких технічних модифікацій для отримання синтаксично правильної схеми підпису з ключем, що «розвивається», компілятор (який був розроблений для забезпечення безпеки KDS-CMA) може бути використаний для безпеки EUF-CMA одноразової схеми підпису S, включно до прямої безпеки схеми підпису з ключем, що розвивається, Sf.

Висновки

1. В результаті проведених досліджень визнано, що продуктивним може бути введення та використання узагальненої (комплексної) моделі криптографічної стійкості ЕП.

2. В якості складових узагальненої (комплексної) моделі криптографічної стійкості асиметричних криптоперетворень типу ЕП обґрунтовані та визначені такі часткові моделі:

- порушника щодо асиметричних криптоперетворень типу ЕП;
- загроз щодо асиметричних криптоперетворень типу ЕП;
- безпеки щодо асиметричних криптоперетворень типу ЕП.

3. Побудова моделі порушника необхідна для того, щоб розробити комплекс заходів із забезпечення захищеності механізмів ЕП, в тому числі з урахуванням вимог та умов їх застосування в постквантовий період. Така модель порушника може бути побудована з урахування різних критеріїв.

4. Порушники класифікуються за рівнем можливостей, що надаються їм штатними засобами КС, в тому числі для класичного та квантового криптоаналізу. Виділяються чотири рівні таких можливостей. Класифікація є ієрархічною – кожний наступний рівень включає в себе функціональні можливості попереднього рівня [5]. Прийнято, що щодо перспективного ЕП для постквантового періоду безпека повинна бути забезпечена в умовах протидії порушнику 4 рівня.

5. У найгіршому випадку безпека повинна бути забезпечена проти криптоаналітика 4-го рівня можливостей, він знає все про метод синтезу перспективного ЕП, криптографічні властивості методу ЕП, а також всі механізми безпеки, що виконуються під час синтезу та застосування. Виключенням є те, що криптоаналітик не знає особистого ключа чи відповідним чином обґрунтовану частину особистого ключа. У найкращому випадку порушник не знає нічого про системні параметри та ключі. У нашому випадку можливі варіанти є рівноймовірними.

6. Модель загроз щодо криптоперетворення ЕП повинна бути документом, яким закріплено найбільш повний перелік загроз щодо існуючих та перспективних ЕП. Відповідно до Законів України інформація у основних інформаційних ресурсах поділяється на відкриту і конфіденційну. Інформація у підтримуючих інформаційних ресурсах є технологічною інформацією.

7. При застосуванні ЕП, незалежно від видів додатків, використовуються асиметричні пари ключів, для кожної пари особистий та відкритий. В подальшому при реальному застосуванні ЕП відкритий ключ, як правило, є сертифікатом відкритого ключа та є доступним усім користувачам інфраструктури відкритого ключа.

8. Стосовно відкритого ключа ЕП повинна бути можливість забезпечення його цілісності, справжності, доступності, неспростовності та захист від несанкціонованих дій, які можуть привести до випадкової чи умисної модифікації, нав’язування хибного чи знищення.

9. Стосовно особистого ключа повинна забезпечуватись його цілісність, справжність, доступність, неспростовність та захист від несанкціонованих дій, а також його захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання та поширення, тобто конфіденційність.

10. Перелік можливих загроз безпеці застосування існуючих та перспективних ЕП сформований з числа загроз, що визначені у IT-Grundschutz Catalogues Германії з урахуванням апаратних, програмних та апаратно-програмних ресурсів, технологій обробки даних та механізмів криптографічного захисту при застосуванні ЕП, в тому числі з урахуванням вимог та умов синтезу перспективних та застосуванні ЕП в постквантовий період.

11. Безумовно, що щодо обґрунтованої та вибраної на основі IT-Grundschutz Catalogues бази Германії моделі загроз, при синтезі та застосуванні існуючих стандартизованих та перспективних ЕП, повинне бути зроблено перекриття названих загроз з необхідною якістю. Для цього, у залежності від механізмів та засобів, що застосовуються для протидії, повинні бути розробленими відповідні нормативно-правові документи.

12. Детально загрози щодо застосування класичного криптоаналізу при синтезі та застосуванні ЕП розглянуті в [1 - 9]. Їх перекриття повинне бути зроблене на всіх етапах синтезу та застосування перспективних ЕП. Вказані загрози з точки зору застосування математичних

методів синтезу та застосування перспективних методів ЕП залежать від математичних методів, що застосовуються, та умов їх функціонування.

13. Загрози (атаки) сторонніми каналами є виділеним класом атак, основною особливістю яких є спрямованість на вразливості практичної реалізації криптосистем, тобто, на відміну від теоретичного криптоаналізу. Загрозою такого класу атак над традиційними є менша потужність та більш висока дієвість.

14. Загрози (атаки) сторонніми каналами є надзвичайно небезпечними, якщо їх не перекривати. Концепція цих атак існує доволі тривалий час, але реалізація захищеності від них вимагає знань не лише у сфері криптографії, а й у сферах технічного характеру. Тому переважна більшість перспективних ЕП розрахована на використання у пристроях, які не можуть захистити від сторонніх атак, бо не мають відповідних програмних рішень щодо захисту від витоку сторонніми каналами.

15. Основними загрозами (атаками) з застосуванням квантових математичних методів, які можуть бути реалізованими на квантовому комп'ютерові (звичайно, якщо він буде побудований), є такі: квантовий алгоритм факторизації Шора; квантовий алгоритм Гровера; квантовий алгоритм Шора вирішення дискретного логарифму в полі; квантовий алгоритм Шора вирішення дискретного логарифму в групі точок еліптичної кривої; квантовий алгоритм криптоаналізу для перетворень в фактор кільці.

16. У залежності від математичних методів, що застосовуються для синтезу та застосування ЕП, можуть застосовуватись різні методи, системи та засоби. Наприклад, для криптоперетворень на алгебраїчних решітках необхідно вирішувати проблему навчання з помилками (LWE).

17. Наразі в постквантовій криптології актуальними є завданнями забезпечення криптографічної стійкості щодо квантових атак.

18. Стосовно атак на LWE можливо виділити та необхідно розглядати наступні атаки (загрози): атаки грубої сили, тобто повного перебору; традиційні атаки зустріч посередині; атаки на основі алгоритму Arora-Ge; BKW, коли LWE зводиться до SIS атаки; Primal attack (Search-LWE зводиться до BDD атаки); Dual attack (Decision-LWE зводиться до SIS); зведення до uSVP атаки пошуку короткого вектора.

19. Для однозначного розуміння та використання пропонується ввести та використовувати нове поняття щодо моделі безпеки (криптографічної стійкості) стандартизованих криптографічних примітивів.

20. Модель безпеки (криптографічної стійкості) криптографічних примітивів (в тому числі типу ЕП) – це сукупність організаційно-технічних, програмно-технічних та логічних механізмів (методів) та заходів, законодавчих та нормативно-правових норм та правил, що визначають вимоги до методів синтезу, оцінки криптографічної стійкості та застосування стандартизованих криптографічних примітивів (типу ЕП), з урахуванням умов їх реалізації при інтенсивній протидії порушника 4-го рівня із застосування методів, систем та засобів класичного та квантового криптоаналізу.

21. Модель безпеки EUF-CMA визначає екзистенційну непідроблюваність від атак на основі адаптивно вибраних повідомлень [7]. Зокрема, безпека в сенсі EUF-CMA повинна протидіяти порушнику 4-го рівня виробляти ЕП для повідомлень, що залежать від ключів (застосуванні особистого sk ключа). По суті, при застосуванні механізму безпечного ЕП, згідно моделі EUF-CMA, вона є безпечною для EUF-CMA випадку.

22. Головна відмінність моделі SUF-CMA полягає в тому, що це більш сильне визначення гарантує, що атакуючий не зможе підібрати підпис. Так, схема, в якій атакуючий може повторно рандомізувати дійсний підпис, щоб він залишався дійсним, але виглядав інакше, ніж вихідне значення, не задовольнила би умові SUF-CMA.

23. В ряді випадків схема підпису S=(K, S, V) називається KDS-CMA-безпечною, якщо вона є захищеною, незважаючи на здатність зловмисника отримувати підписи на довільних

(таких, що ефективно обчислюються) функціях g стану sk підписувача. Зокрема, g має доступ до секретного ключа, що зберігається під час підписування.

24. Оцінка ефективності моделі безпеки KDS-CMA в сенсі KDS-CMA означає безпеку в сенсі EUF-CMA, і виникає питання, чи може бути досягнута за цих умов безпека.

25. Після застосування деяких технічних модифікацій для отримання синтаксично правильної схеми підпису з ключем, що «розвивається», компілятор може бути використаний для безпеки EUF-CMA одноразової схеми підпису S, включно до «прямої» безпеки схеми підпису з ключем, що розвивається, Sf.

Список літератури:

1. Lily Chen Report on Post-Quatum Cryptography. NISTIR 8105 (DRAFT) / Lili Chen, Stephen Jordan, Yi-Kai-Liu, Dustin Moody, Rene Peralta, Ray Perlner, Daniel Smith-Tone // Access mode: http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf.
2. Moody D. Post-Quntum Cryptography: NIST's Plan for the Future. The Seventh International Conference on Post-Quntum Cryptography [Електронний ресурс] // Moody. 2016. Режим доступу: https://pqcrypto2016.jp/data/pqc2016_nist_announcement.pdf.
3. ETSI GR QSC 001 V.1.1.1 (2016-07). Quantum-Safe Cryptography (QSC); Quantum-safe algorithmic framework. Режим доступу: https://www.etsi.org/deliver/etsi_gr/QSC/001_099/001/01.01.01_60/gr_QSC001v010101p.pdf.
4. ETSI Quantum safe cryptography and security // White Paper №8, 2015. Режим доступу: https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf.
5. NIST. Post-Quantum Cryptography Standardization. National Institute of Standards and Technology Internal, Report 8105 [Електронний ресурс] // NIST Режим доступу: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization.
6. Gorbenko I., Ponomar V. Examining a possibility to use and the benefits of post-quantum algorithms dependent on the conditions of their application // Eastern-European Journal of Enterprise Technologies. 2017. Vol. 2 NO 9 (86). P.21–32. Available at: http://journals.uran.ua/
7. EUF-CMA and SUF-CMA. [Електронний ресурс]. Режим доступу: https://blog.cryptographyengineering.com/euf-cma-and-suf-cma/.
8. Горбенко І. Д., Кузнєцов О. О., Олійников Р. В., Горбенко Ю. І., Ганзя Р. С., Пономар В. А. Аналіз проблем криптографічного захисту інформації у постквантовий період та можливі шляхи їх вирішення // V Міжнар. Наук.-техн. конф. "Захист інформації і безпека інформаційних систем" : Праці Наук.-техн. конф., 02–03 червня 2016 р. Львів : Нац. ун-т "Львівська політехніка", 2016. С. 110-111.
9. Горбенко Ю.І. Методи побудування та аналізу, стандартизація та застосування криптографічних систем ; за заг. ред.. І.Д. Горбенка. Харків : Форт, 2015. 959 с.
10. IT-Grundschutz Catalogues. [Електронний ресурс]. Режим доступу: https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ITGrundschutzCatalogues/itgrundschutzcatalogues_node.html.

Надійшла до редколегії 07.08.2020

Відомості про авторів:

Горбенко Юрій Іванович – канд. техн. наук, АТ «Інститут інформаційних технологій», перший заступник головного конструктора, Україна, e-mail: gorbenkou@iit.kharkov.ua, ORCID: https://orcid.org/0000-0003-0073-9107

Потій Олександр Володимирович – д-р техн. наук., професор, заступник Голови Державної служби спеціального зв'язку та захисту інформації України, e-mail: potav@ua.fm, ORCID: https://orcid.org/0000-0002-2366-0541

Онопрієнко Віктор Васильович – канд. техн. наук, генеральний директор АТ «Інститут інформаційних технологій», Україна.

Єсіна Марина Віталіївна – канд. техн. наук, Харківський національний університет імені В. Н. Каразіна, доцент кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Україна, e-mail: rinayes20@gmail.com, ORCID: https://orcid.org/0000-0002-1252-7606

Малєєва Ганна Андріївна – Харківський національний університет радіоелектроніки, аспірант кафедри безпеки інформаційних технологій, Україна, e-mail: hanna.malieieva@nure.ua

УДК 004.056.55 **DOI:10.30837/rt.2020.3.202.03**

Є.Ю. КАПТЬОЛ, І.Д. ГОРБЕНКО, д-р техн. наук

АНАЛІЗ МОЖЛИВОСТЕЙ ТА ОСОБЛИВОСТІ ПРОГРАМУВАННЯ ЗАДАЧ КРИПТОЛОГІЇ НА КВАНТОВОМУ КОМП'ЮТЕРІ

Вступ

Обґрунтовано вважається, що застосування квантового комп'ютера при вирішенні задач криптоаналізу щодо існуючих криптоперетворень асиметричного типу скоріше всього приведе до їх зламу. Але для цього ще потрібно розробити та виготовити квантові комп'ютери відповідної кубічної розрядності та розробити відповідне математичне та програмне забезпечення. Тому питання програмування задач взагалі криптології, особливо криптоаналізу, з орієнтацією на квантовий комп'ютер, стає все більш актуальним. Такі можливості появились завдяки успіхам у справі створення робочого варіанту екземпляру квантового комп'ютера [1 – 3]. Але, як виявилось, як математичне так і програмне забезпечення квантового комп'ютера є суттєво специфічними і не вкладаються в наші звичні рамки. В той же час, необхідність вирішення задач криптоаналізу на квантовому комп'ютері пояснюється його суттєвою перевагою перед класичним у швидкодії. Така перевага здебільшого базується на використанні квантовими комп'ютерами квантових властивостей, що є недоступними для класичних комп'ютерів. Наприклад, завдяки квантовим властивостям існує можливість розглядати одразу весь регістр замість одного елемента, як це робиться в класичному комп'ютері. Вказане дає суттєву перевагу в швидкодії обчислень.

Для загального доступу з використанням хмарних сервісів доступними є квантові комп'ютери компанії IBM на 5 та 15 кубітів та квантового симулятору (до 32 кубітів) [6]. Вони виконують квантові операції та можуть реалізовувати квантові гейти. Слід помітити, що ці гейти однокубітні та двохкубітні, а один з них трикубітний. Робоча реалізація методу Гровера в свою чергу потребує наявності квантових гейтів, що діяли б на більшу кількість кубітів одночасно. Тому багатокубітні гейти доводиться розкладати на послідовності гейтів, що є в наявності серед універсальних. Враховуючи вказане, необхідно виробити три схеми застосування методу Гровера на квантовому комп'ютері для квантового регістру з чотирьох кубітів для отримання квантового регістру.

Мета статі – обгрунтування підходів до аналізу можливостей та вивчення особливостей програмування задач криптоаналізу на квантових комп'ютерах, а також оцінка сучасного стану можливостей його реалізації на однокубітних, двохкубітних та трикубітному гейті.

1. Особливості та можливості квантового комп'ютера

Квантові комп'ютери, як показує аналіз, суттєво відрізняються від класичних самими принципами роботи. В них використовується специфічна квантова інформатика. Вона цілком базується на властивостях квантових об'єктів [1 – 3]: В першу чергу на здатності квантової частки приймати одночасно декілька станів завдяки квантової суперпозиції станів. Також суттєвими є здатність систем, що складаються з декількох квантових часток перебувати в переплутаних (корельованих) станах та нелокальність, що є їх наслідком. Важливим є вплив процесу вимірювання на стан вимірюваного об'єкта аж до його знищення, а також практична неможливість здійснити клонування квантових станів квантових часток.

Наведені вище властивості слідують з властивостей квантової фізики, вони є підґрунтям для квантової інформатики. Причому квантова фізика є складною в розумінні та відрізняється від класичної на принциповому рівні.

На основі квантових властивостей квантових об'єктів розроблено специфічну квантову математику, яку покладено в основу квантових алгоритмів криптоаналізу. Основні з них [4]:

- алгоритм Шора для здійснення факторизації надвеликих цілих чисел;
- алгоритми вирішення задач дискретного логарифму в скінченному полі;
- алгоритми дискретного логарифмування в групі точок еліптичних кривих;

- алгоритм пошуку в несортованій базі (Гровера);
- алгоритми криптоаналізу перетворень в кільцях поліномів та фактор-кільцях тощо.

Як правило, вказані алгоритми забезпечують вирішення задач, що є або неможливими для вирішення за допомогою класичних комп'ютерів, або нерентабельно складними з точки зору обчислювального ресурсу, що необхідний для отримання практичного результату [1 – 4]. Однією з властивостей квантових алгоритмів є те, що вони мають ймовірнісну природу, тобто результат можна отримати тільки з певною ймовірністю. Тобто проблемність вирішення задачі криптоаналізу в необхідності отримання, при вимірюванні стану квантового регістру після завершення роботи алгоритму, результату з необхідною ймовірністю.

Як теоретично, так і практично підтверджено, що застосування квантових алгоритмів на класичному комп'ютері не тільки не дає переваги, а є дуже невигідним з точки зору швидкодії [5]. Так, наприклад, реалізація методу Гровера на класичному комп'ютері є невигідною через те, що сам алгоритм передбачає для отримання потрібного результату при вимірюванні стану квантового регістру, багаторазового повторення терації Гровера. Тоді як на квантовому комп'ютері повтори покращують результат, а квантові властивості нівелюють затрати на повтори, в той час як на класичному комп'ютері ці повтори не є потрібними, а лише зайвими. Щодо властивостей, що нівелюють для квантового комп'ютера проведення повторів, то вони пояснюються тим, що квантовий комп'ютер дозволяє переглядати весь результат в регістрі всього однією операцією, в той час, як на класичному комп'ютері перегляд регістру здійснюється по одному елементу за одну операцію.

Необхідно зазначити, що поява квантового комп'ютера, регістр котрого матиме для здійснення квантового криптоаналізу достатню кількість кубітів, є суттєво необхідною умовою зламу існуючих асиметричних криптоалгоритмів з обмеженими розмірами системних параметрів. Достатність умови в тому, що окрім власне квантового комп'ютера необхідним ще є наявність відповідного математичного та програмного забезпечення, а також ще й реалізації на квантовому комп'ютері безпосередньо алгоритмів, з використанням котрих можна провести криптоаналіз. Хоча, без сумнівів, створення квантового комп'ютера призведе до появи значної загрози для сучасних криптографічних систем з боку вже розроблених квантових алгоритмів, таких як алгоритми Гровера та Шора тощо.

2. Аналіз можливостей та наявності забезпечень для вирішення задач криптоаналізу

Таким чином, завдяки сучасним успіхам в створенні квантового комп'ютера існує можливість доступу до програмування квантового комп'ютера за допомогою хмарних сервісів. Так, для загального доступу з використанням хмарних сервісів доступними є квантові комп'ютери компанії IBM на 1, 5 та 15 кубітів [1, 6]. Вони виконують квантові операції та можуть реалізовувати квантові гейти. Також можна скористатися квантовим симулятором (до 32 кубітів) [1, 6].

Наш практичний аналіз показав, що загальнодоступними для використання є однокубітні та двохкубітні, та один з них трикубітний гейти. Але робочі реалізації, наприклад методу Гровера, потребують наявності квантових гейтів, що діяли б на більшу кількість кубітів одночасно. Тому багатокубітні гейти доводиться розкладати на послідовності гейтів, що є в наявності, тобто універсальних.

Наш пошук показав[1, 6], що серед доступних для загального доступу квантових комп'ютерів наявні: $ibmq\_16\_melbourne$ (15 кубітів), $ibmq\_london$ (5 кубітів), $ibmq\_burlington$ (5 кубітів), $ibmq\_essex$ (5 кубітів), $ibmq\_ourense$ (5 кубітів), $ibmq\_vigo$ (5 кубітів), $ibmq\_5\_yorktown - ibmqx2$ (5 кубітів), $ibmq\_armonk$ (1 кубіт). Квантовий симулятор $ibmq\_qasm\_simulator$ може використовуватись для реалізації алгоритмів, що передбачають використання регістрів з довжиною до 32 кубітів.

3. Особливість квантового програмування для методу Гровера

Одним з основних квантових методів, що є необхідними для вирішення задач криптології є метод Гровера. Розглянемо його детальніше.

Алгоритм Гровера будується з використанням методу Гровера, він є квантовим алгоритмом, що призначений для проведення вичерпного пошуку унікального елементу в несортованій базі даних, що містить $N = 2^n$ елементів, де n позначає довжину задіяного для представлення пошукового простору квантового регістру (кількість кубітів в ньому), а N є розміром пошукового простору [2, 5].

Особливість алгоритму Гровера полягає в тому, що, завдяки квантовим властивостям та використанню функції «чорної скриньки» (у вигляді квантового оракула), він потребує лише $O(\sqrt{N})$ групових операцій замість $O(N)$ у класичних алгоритмів. Квадратичне прискорення у порівнянні з класичними алгоритмами досягається завдяки використанню квантових властивостей, таких як квантова суперпозиція станів.

Хоча інші квантові алгоритми при порівнянні з класичними аналогами можуть забезпечити експоненційне прискорення, а алгоритм Гровера може забезпечити лише квадратичне прискорення, слід зауважити, що навіть таке прискорення є дуже значним та його значущість збільшується зі зростанням N. Для прикладу, методом Гровера 128-бітний криптографічний ключ можна зламати приблизно за 2^{64} звернень до функції «чорної скриньки», що можна визначити як 2^{64} звернень до ітерації Гровера, а отже 2^{64} ітерацій методу. В той же час як 256-бітний криптографічний ключ можна зламати за, приблизно, 2^{128} ітерацій. Виходячи саме з цього твердження для збільшення стійкості проти квантових атак іноді пропонують збільшувати довжину криптографічних ключів в два рази [3].

Метод Гровера, як і більшість квантових методів, є ймовірнісним, тобто правильна відповідь може бути виміряна з квантового регістру з певною ймовірністю, яка не повинна перевищувати 1. Також слід зауважити, що при виконанні більшого числа ітерацій, чим потрібно, ймовірність виміру правильного результату зменшується, тому це потрібно відповідним чином відслідковувати [5].

Метод Гровера має ряд можливостей для застосування, одним з котрих є реалізація його як алгоритму криптоаналізу симетричних перетворень, функцій гешування, асиметричного шифру в кільці поліномів тощо у зв'язку з його можливим узагальненим використанням [1, 5]. Для криптоаналізу симетричних блокових перетворень метод можна звести до алгоритму пошуку сеансового чи довгострокового ключа тощо. У випадку функцій гешування метод можна застосувати для пошуку колізій тощо. Метод Гровера має значні потенційні можливості, котрі беруться в розрахунок з огляду на сучасний стан розробки квантового комп'ютера.

4. Сутність та застосування методу Гровера

Для розуміння методу Гровера необхідно визначити квантову суперпозицію станів [1, 5]. Нехай $|\psi\rangle$ – суперпозиція всіх станів (згідно нотації Дірака):

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle.$$

З урахуванням цього алгоритм приймає такий вигляд:

1) Встановлення системи в стан суперпозиції $|\psi\rangle$.

2) Виконання «ітерації Гровера» (або ж G) $\frac{\pi}{4}\sqrt{N}$ разів, де $N = 2^n$ та N становить розмір пошукового простору, а n – розмір квантового регістру, що використовується для представлення пошукового простору. При цьому G включає в себе два етапи:

- застосування квантового оракула (O);
- застосування оператора дифузії, що здійснює «інверсію щодо середнього» та має вигляд $2|0\rangle\langle 0|-I$.

3) Виконання класичних вимірювань регістру для отримання результату роботи алгоритму, що з ймовірністю близькою до 1 буде вірним.

Практичний приклад

З метою демонстрації дії методу Гровера на практиці розглянемо приклад використання алгоритму пошуку несортованою базою даних з невеликим розміром пошукового простору, як було зроблено в [5].

Приклад [5]. Припустимо, що система може приймати $N = 72057594037927936 = 2^{56}$ станів, що означає, що база для пошуку складається з 72057594037927936 елементів. Також припустимо, що стан системи, котрий ми хочемо отримати в результаті пошуку, x_0, має індекс 234.

1) Для опису системи необхідно $n = 56$ кубітів. Згідно з алгоритмом Гровера ініціалізуємо квантовий регістр, що складатиметься з $n = 56$ кубітів, що є необхідною умовою для представлення пошукового простору, що має розмір $N = 2^{56}$, встановивши регістр у початковий стан, що має наступний вигляд:

$$|\psi_0\rangle = |000...000\rangle,$$

де кількість нулів дорівнює 56.

2) Проведемо перетворення Адамара, що дозволяє встановити систему в стан квантової суперпозиції, що робить значення амплітуди, що пов'язана з кожним станом, таким, щоб ймовірність перебування в кожному з 2^{56} можливих станів була рівною. Цей крок матиме наступний вигляд:

$$|\psi\rangle = H^{\otimes 56}|000...000\rangle = (H|0\rangle)^{\otimes 56} = \frac{1}{268435456}\sum_{i=0}^{2^{56}}|i\rangle$$

Таким чином, маємо квантовий регістр, встановлений в стан суперпозиції, що геометрично можна представити як наведено на рис. 1.

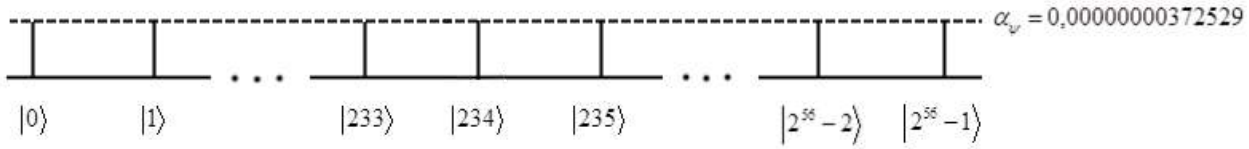


Рис. 1. Геометричне представлення регістру з 256 кубітів в стані суперпозиції

3) Визначаємо кількість потрібних ітерацій G:

$$\frac{\pi}{4}\sqrt{2^n} = \frac{\pi}{4}\sqrt{2^{56}} = \frac{2^{28}\pi}{4} \approx 210828714{,}133156$$

Далі для використання в розрахунках округлимо число ітерацій до 210828714 у зв'язку з округленням вниз.

4) Після цього визначимо

$$|u\rangle = \frac{1}{\sqrt{2^{56}-1}}\sum_{\substack{i=0\\ i\neq 301}}^{2^{56}-1}|i\rangle = \frac{|0\rangle+|1\rangle+...+|2^{56}-2\rangle+|2^{56}-1\rangle}{\sqrt{2^{56}-1}}.$$

Також маємо, що

$$|\psi\rangle = \frac{\sqrt{2^{56}-1}}{2^{28}}|u\rangle + \frac{1}{2^{28}}|234\rangle.$$

5) Далі, зі здійснення звернення до оракула починається перша ітерація. Після застосування оракула маємо

$$|\psi_1\rangle = |\psi\rangle - \frac{1}{2*2^{28}}|234\rangle = |\psi\rangle - \frac{1}{536870912}|234\rangle.$$

Стан даного регістру після застосування оракула під час першої ітерації Гровера має геометричне відображення, що наведено на рис. 2.

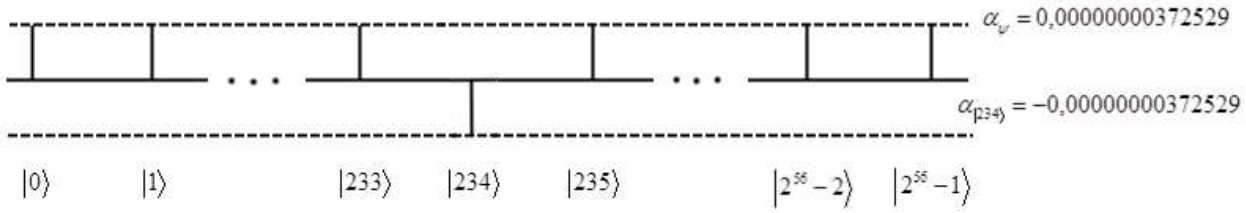


Рис. 2. Геометричне відображення стану регістру після застосування оракула під час першої ітерації G

Далі відбувається виконання оператора дифузії, в результаті чого отримуємо:

$$|\psi_2\rangle = (2|\psi\rangle\langle\psi| - I)|\psi_1\rangle = 0{,}9999999999999999861|\psi\rangle + 0{,}0000000018626|234\rangle;$$

Геометричне відображення стану регістру після першої ітерації зображено на рис. 3.

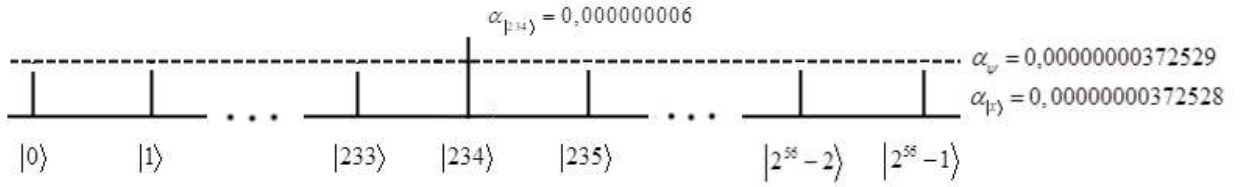


Рис. 3. Геометричне представлення стану квантового регістру після проведення першої ітерації G.

Далі аналогічним чином проводиться ще 210828713 ітерацій.

Під час проведення останньої, 210828714-й ітерації маємо в результаті застосування оракула:

$$|\psi_{421657427}\rangle = 0{,}00000000000003|\psi\rangle - 0{,}9999999999999841|234\rangle.$$

Стан даного регістру після застосування оракула під час останньої ітерації Гровера має геометричне відображення, що наведено на рис. 4.

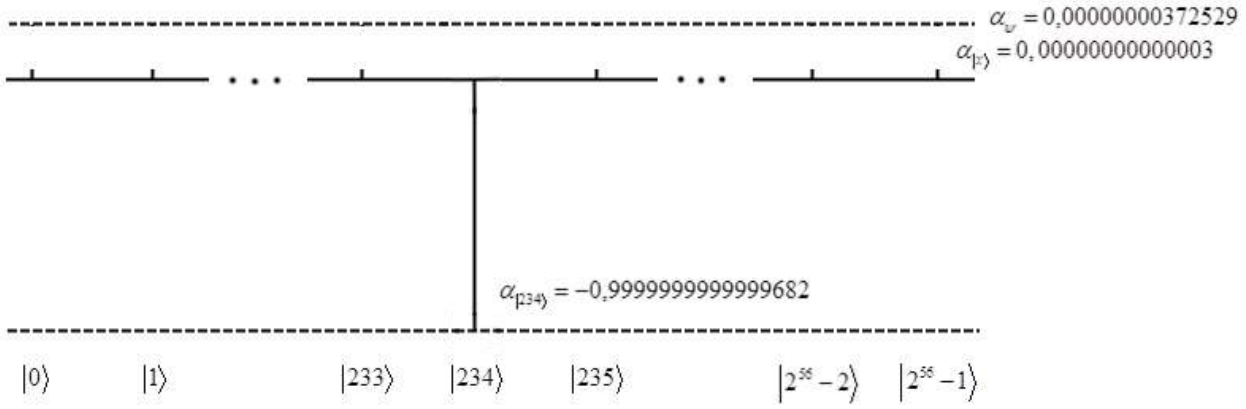


Рис. 4. Геометричне відображення стану регістру після застосування оракула під час останньої ітерації G

Після застосування оператора дифузії під час останньої ітерації маємо:

$$|\psi_{421657428}\rangle = (2|\psi\rangle\langle\psi| - I)|\psi_{421657427}\rangle = -0{,}00000000000001|\psi\rangle + 0{,}9999999999999841|234\rangle$$

Геометричне представлення результатів останньої ітерації наведено на рис. 5.

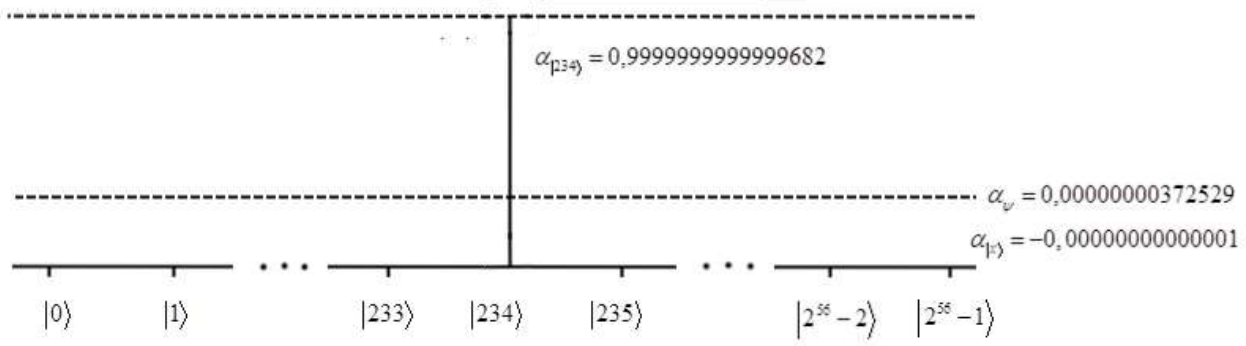


Рис. 5. Геометричне представлення стану квантового регістру після проведення останньої ітерації G

Ймовірність отримання потрібного елементу в результаті вимірювання регістру після проведення дванадцяти ітерацій становить:

$$P \approx |0{,}9999999999999841|^2 \approx 0{,}9999999999999682 \approx 99{,}99999999999682\%.$$

Таким чином, на цьому прикладі, враховуючи попередні, можна побачити, що зі зростанням N похибка дійсно стає незначною.

Також слід зазначити, що приклад було розраховано з використанням програмної моделі проведення пошуку методом Гровера, що була модернізована на швидкодію. В загальному вигляді програмна модель, використана для розрахунків, відповідає загальній програмній моделі методу Гровера, але відрізняється тим, що оракул було спрощено до елементарної функції пошуку, що також проводилася повністю лише в частині відповідальній за ініціалізацію. Така побудова моделі дозволила провести розрахунки без вирішення складної задачі пошуку, але зі збереженням достовірності результатів розрахунків на рівні, що відповідає рівню достовірності результатів програмної моделі, що проводить виконання складної задачі пошуку.

5. Схеми застосування методу Гровера на квантовому комп'ютері для квантових регістрів з використанням хмарних сервісів

Для загального доступу з використанням хмарних сервісів доступними є квантові комп'ютери компанії IBM на 5 та 15 кубітів та квантового симулятору (до 32 кубітів) [6].

Вони виконують квантові операції та можуть реалізовувати квантові гейти. Слід помітити, що ці гейти однокубітні та двохкубітні, а один з них трикубітний. Робоча реалізація методу Гровера в свою чергу потребує наявності квантових гейтів, що діяли б на більшу кількість кубітів одночасно. Тому багатокубітні гейти доводиться розкладати на послідовності гейтів, що є в наявності серед універсальних.

З урахуванням наведеного було вироблено три схеми застосування методу Гровера на квантовому комп'ютері для квантового регістру з чотирьох кубітів для отримання результату «0», що може бути представлено рядком бітів $|0000\rangle$, та три схеми для отримання результату 4, що може бути представлено рядком бітів $|0100\rangle$. Схеми відрізняються кількістю застосування ітерацій Гровера. Так, в перших схемах застосовується одна ітерація Гровера, в других – дві ітерації, в третіх – три ітерації. Ці схеми було випробувано на доступних для загального доступу тестових квантових комп'ютерах компанії IBM та доступному через той же сервіс квантовому симуляторі [6]. Серед квантових комп'ютерів, що використані в дослідженні, були: $ibmq\_16\_melbourne$, $ibmqx2$ (він же $ibmq\_5\_yorktown - ibmqx2$), $ibmq\_burlington$. Квантовий симулятор $ibmq\_qasm\_simulator$ може розраховувати схеми, що передбачає використання до 32 кубітів.

Як вже було зазначено, особливості реалізації метода Гровера для квантового регістру, що складається з чотирьох кубітів на квантовому комп'ютері, включають в себе необхідність застосування 3-кубітних квантових гейтів. В той же час інструментарій для взаємодії з доступними квантовими комп'ютерами не включає в себе квантові гейти, що оперують над потрібною кількістю кубітів. Потрібні квантові гейти можна замінити сукупностями наявних в інструментарії квантових гейтів, що дають той самий ефект.

Результати виконаних випробувань можуть вказувати як на недосконаліть методів, використаних для представлення багатокубітних гейтів у вигляді сукупності одно- та двокубітних гейтів, так і на недосконаліть розроблених квантових комп'ютерів, що має бути перевірено в майбутніх дослідженнях.

Результати застосування методу Гровера з однією ітерацією для отримання $|0000\rangle$ показали значні розбіжності між реальними результатами та отриманими за допомогою квантового симулятора. Так, симулятор вказував на те, що ймовірність отримання $|0000\rangle$ становить 46,875 %, в той час як при проведенні реальних вимірювань цей результат було отримано лише 6,152% разів на $ibmq\_burlington$, 7,52 % – на $ibmqx2$ та 8,789 % – на $ibmq\_16\_melbourne$ квантових комп'ютерах.

Результати застосування методу Гровера з двома ітераціями для отримання $|0000\rangle$ показали ще більші розбіжності між очікуваними та реальними результатами. Так, на симуляторі ймовірність отримання $|0000\rangle$ становила 91,211 %, в той час як насправді було отримано лише 6,543 % на $ibmq\_burlington$, 8,398 % на $ibmqx2$ та 10,156 % на $ibmq\_16\_melbourne$ квантових комп'ютерах.

Результати застосування методу Гровера з трьома ітераціями (що є остаточною кількістю ітерацій для регістру цього розміру) для отримання $|0000\rangle$ підтвердили розбіжності, отримані на попередньому кроці. Так, Симулятор спрогнозував ймовірність отримання $|0000\rangle$ в 96,387 %, в той час як на реальних квантових комп'ютерах було отримано потрібний результат значно меншу кількість разів: 7,227 % – на $ibmq\_burlington$, 8,301 % – на $ibmqx2$, 9,961 % – на $ibmq\_16\_melbourne$ квантовому комп'ютері.

Результати застосування методу Гровера з однією ітерацією для отримання $|0100\rangle$ показали значні розбіжності між реальними результатами та отриманими за допомогою квантового симулятора. Так, симулятор вказував на те, що ймовірність отримання $|0100\rangle$ становить

46,387 %, в той час як при проведенні реальних вимірювань цей результат було отримано лише 5,469 % разів на *ibmq_burlington*, 10,547 % – на *ibmqx*2 та 6,506 % – на *ibmq_16_melbourne* квантових комп'ютерах.

Результати застосування методу Гровера з двома ітераціями для отримання $|0100\rangle$ показали ще більші розбіжності між очікуваними та реальними результатами. Так, на симуляторі ймовірність отримання $|0100\rangle$ становила 90,259 %, в той час як насправді було отримано лише 6,006 % на *ibmq_burlington*, 6,982 % на *ibmqx*2 та 6,897 % на *ibmq_16_melbourne* квантових комп'ютерах.

Результати застосування методу Гровера з трьома ітераціями для отримання $|0100\rangle$ підтвердили розбіжності, отримані на попередньому кроці. Так, Симулятор спрогнозував ймовірність отримання $|0100\rangle$ в 96,436 %, в той час як на реальних квантових комп'ютерах було отримано потрібний результат за значно меншу кількість разів: 6,299 % – на Бурлінгтонському, 6,152 % – на Йорктаунському, 7,837 % на Мельбурнському квантовому комп'ютері.

Детальніше результати випробувань розроблених схем на квантових комп'ютерах наведено в табл. 1 – 6.

Таблиця 1

Результати застосування методу Гровера з однією ітерацією для отримання $|0000\rangle$

Значення	Симулятор (1024 повтори), %	Бурлінгтон (1024 повтори), %	Йорктаун (1024 повтори), %	Мельбурн (1024 повтори), %
0000	46,875	6,152	7,52	8,789
0001	4,395	6,543	6,934	6,25
0010	2,832	6,738	5,566	7,031
0011	3,809	5,664	8,691	5,664
0100	3,613	8,594	6,445	5,566
0101	2,637	5,957	4,688	6,836
0110	3,125	6,543	4,004	4,98
0111	3,906	5,176	10,742	6,348
1000	2,539	7,422	7,422	7,52
1001	4,199	6,738	4,688	7,031
1010	2,832	7,031	4,59	6,641
1011	2,637	5,371	7,715	5,957
1100	5,566	6,934	4,199	5,273
1101	3,809	5,762	4,492	5,957
1110	3,223	3,906	4,883	5,566
1111	4,004	5,469	7,422	4,59

Таблиця 2

Результати застосування методу Гровера з двома ітераціями для отримання $|0000\rangle$

Значення	Симулятор (1024 повтори), %	Бурлінгтон (1024 повтори), %	Йорктаун (1024 повтори), %	Мельбурн (1024 повтори), %
0000	91,211	6,543	8,398	10,156
0001	0,781	6,25	6,152	6,641
0010	0,391	6,25	5,371	6,348
0011	0,391	8,398	8,008	5,566
0100	0,684	5,762	8,594	7,227
0101	0,586	6,641	5,176	7,422
0110	0,488	6,152	4,98	5,762
0111	0,586	7,324	7,813	4,395
1000	0,195	6,445	6,348	6,738
1001	0,586	6,152	4,004	6,641
1010	0,684	5,273	4,492	5,273
1011	0,586	5,957	7,715	4,102
1100	0,684	5,273	6,738	7,422
1101	0,879	6,152	3,906	5,664
1110	0,488	5,566	5,664	6,348
1111	0,781	5,859	6,641	4,297

Таблиця 3

Результати застосування методу Гровера з трьома ітераціями для отримання $|0000\rangle$

Значення	Симулятор (1024 повтори), %	Бурлінгтон (1024 повтори), %	Йорктаун (1024 повтори), %	Мельбурн (1024 повтори), %
0000	96,387	7,227	8,301	9,961
0001	0,391	7,91	2,93	5,371
0010	0,098	6,836	6,641	8,496
0011	0,586	6,836	6,641	5,664
0100	0,195	5,664	7,715	5,859
0101	0,098	6,738	3,613	6,641
0110	0,098	6,543	7,031	5,762
0111	0,195	6,055	7,422	6,348
1000	0,195	5,859	8,594	10,742
1001	0,293	4,98	3,613	4,59
1010	0,098	5,371	5,566	6,641
1011	0,391	7,617	8,105	3,613
1100	0,098	5,566	7,227	5,859
1101	0,195	5,957	3,223	5,469
1110	0,391	5,078	6,445	4,395
1111	0,293	5,762	6,934	4,59

Таблиця 4

Результати застосування методу Гровера з однією ітерацією для отримання $|0100\rangle$

Значення	Симулятор (4096 повторів), %	Бурлінгтон (4096 повтори), %	Йорктаун (4096 повтори), %
0000	3,589	8,691	7,666
0001	3,247	6,909	6,348
0010	4,053	5,859	5,811
0011	3,003	5,151	4,541
0100	46,387	5,469	10,547
0101	3,125	5,322	8,398
0110	3,076	5,957	7,666
0111	3,906	6,567	7,153
1000	3,955	9,839	3,687
1001	4,321	6,47	6,274
1010	3,516	6,03	2,881
1011	3,198	5,151	6,396
1100	3,296	5,859	4,321
1101	3,54	5,005	8,252
1110	4,175	5,591	3,296
1111	3,613	6,128	6,763

Таблиця 5

Результати застосування методу Гровера з двома ітераціями для отримання $|0100\rangle$

Значення	Симулятор (4096 повтори), %	Бурлінгтон (4096 повтори), %	Йорктаун (4096 повтори), %
0000	0,537	7,861	6,738
0001	0,537	5,981	6,982
0010	0,635	8,179	3,711
0011	0,659	6,934	3,54
0100	90,259	6,006	6,982
0101	0,464	5,64	7,495
0110	0,684	6,616	4,175
0111	0,586	5,981	3,833
1000	0,781	7,3	5,688
1001	0,61	5,884	5,908
1010	0,659	5,688	8,862
1011	0,732	6,274	7,446
1100	0,659	5,493	6,03
1101	0,708	5,566	6,03
1110	0,757	5,396	8,423
1111	0,732	5,2	8,154

Таблиця 6

Результати застосування методу Гровера з трьома ітераціями для отримання $|0100\rangle$

Значення	Симулятор (4096 повтори), %	Бурлінгтон (4096 повтори), %	Йорктаун (4096 повтори), %
0000	0,22	7,52	6,299
0001	0,244	6,152	6,177
0010	0,244	6,519	3,784
0011	0,122	5,859	9,131
0100	96,436	6,299	6,152
0101	0,244	6,543	6,323
0110	0,22	6,152	3,467
0111	0,171	5,249	7,91
1000	0,391	6,738	5,762
1001	0,244	6,177	5,957
1010	0,269	5,615	3,711
1011	0,22	6,909	8,862
1100	0,195	6,641	6,738
1101	0,269	6,47	6,055
1110	0,269	5,615	3,76
1111	0,244	5,542	9,912

Висновки

1. Подальший розвиток вимагає вдосконалення представлення багатокубітних гейтів шляхом використання одно- та двокубітних гейтів, а також вдосконалення оснастки для роботи з квантовими комп'ютерами та розробки багатокубітних гейтів та впровадження їх у діючі зразки квантових комп'ютерів.

2. Хоча квантовий симулятор вказує на те, що схеми повинні надавати правильний результат із ймовірністю близькою до максимальної, результати реальних експериментів не є навіть близько такими вдалими.

3. Реалізація методу Гровера на класичному комп'ютері є невигідною через те, що сам алгоритм передбачає для отримання потрібного результату при вимірюванні стану квантового регістру, багаторазового повторення терації Гровера. Тоді як на квантовому комп'ютері повтори покращують результат, а квантові властивості нівелюють затрати на повтори, в той час як на класичному комп'ютері ці повтори не є потрібними, а лише зайвими.

4. Щодо властивостей, що нівелюють для квантового комп'ютера проведення повторів, то вони пояснюються тим, що квантовий комп'ютер дозволяє переглядати весь результат в регістрі всього однією операцією, в той час, як на класичному комп'ютері перегляд регістру здійснюється по одному елементу за одну операцію.

5. Необхідно також зазначити, що поява квантового комп'ютера, регістр котрого матиме для здійснення квантового криптоаналізу достатню кількість кубітів, є суттєво необхідною умовою зламу існуючих асиметричних криптоалгоритмів з обмеженими розмірами системних параметрів.

6. Достатність умови в тому, що окрім власне квантового комп'ютера, необхідним ще є наявність відповідного математичного та програмного забезпечень, а також ще й реалізації на квантовому комп'ютері безпосередньо алгоритмів, з використанням котрих можна провести криптоаналіз.

7. Можна стверджувати, що створення квантового комп'ютера призведе до появи значної загрози для сучасних криптографічних систем з боку вже розроблених квантових алгоритмів, таких як алгоритми Гровера та Шора тощо.

8. Питання програмування задач взагалі криптології, особливо криптоаналізу, з орієнтацією на квантовий комп'ютер, стає все більш актуальним. Такі можливості появились завдяки успіхам у справі створення робочого варіанту екземпляру квантового комп'ютера [1 – 4, 6].

9. З метою демонстрації дії методу Гровера на практиці розглянемо приклад використання алгоритму пошуку несортованою базою даних з невеликим розміром пошукового простору, як було зроблено в [1, 5].

10. Але, як виявилось, як математичне так і програмне забезпечення квантового комп'ютера є суттєво специфічними і не вкладаються в наші звичні рамки. В той же час, необхідність вирішення задач криптоаналізу на квантовому комп'ютерові пояснюється його суттєвою перевагою перед класичним у швидкодії

11. З отриманих результатів можна зробити висновок, що нинішні квантові комп'ютери ще не здатні на повноцінне контрольоване відтворення всіх квантових властивостей. Хоча можливо з більшою кількістю кубітів метод Гровера і даватиме кращий результат, що буде перевірено подальшими дослідженнями.

13. Причини таких результатів та можливість отримання кращих результатів підлягають подальшим дослідженням.

Список літератури:

1. Квантовые компьютеры. [Електронний ресурс]. Режим доступу: http://www.nkj.ru/archive/articles/5309/.
2. Lov K. Grover. A fast quantum mechanical algorithm for database search, 1996. URL: https://arxiv.org/pdf/quant-ph/9605043.pdf
3. Feyman R. P. Quantum mechanical computers // Opt. News. 1985. February, 11. pp. 11-39.
4. Горбенко І. Д. Прикладна криптологія / І. Д. Горбенко, Ю. І. Горбенко. Харків : Форт, 2012. 868 с.
5. Сутність та особливості реалізації методу Гровера на класичному комп'ютері для симетричного криптоаналізу / Ю. І. Горбенко, Є. Ю. Каптьол // Радіотехніка. 2018. Вип. 195. С. 89-100.
6. IBM Quantum Experience Dashboard. [Електронний ресурс]. Режим доступу: https://quantum-computing.ibm.com/

Надійшла до редколегії 11.08.2020

Відомості про авторів:

Каптьол Євген Юрійович – Харківський національний університет імені В.Н. Каразіна, аспірант кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Україна

Горбенко Іван Дмитрович – д-р техн. наук, професор, Харківський національний університет імені В.Н. Каразіна, професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Україна, e-mail: gorbenkoivan03@gmail.com, ORCID: https://orcid.org/0000-0003-4616-3449

УДК 004.056.55 **DOI:10.30837/rt.2020.3.202.04**

Ю.І. ГОРБЕНКО, канд. техн. наук, О.С. ДРОЗДОВА

АНАЛІЗ СТІЙКОСТІ ПОСТКВАНТОВОГО ЕЛЕКТРОННОГО ПІДПИСУ DILITHIUM ДО АТАК НА ПОМИЛКИ

Вступ

На сьогодні поряд із задачею стандартизації постквантових алгоритмів стоїть задача поступового заміщення класичних алгоритмів, які використовуються у реальних додатках та пристроях на квантовостійкі. Критичною задачею у цьому процесі переходу є забезпечення відповідного рівня доказової стійкості та захищеності від атак не тільки в теорії, але і від атак на реалізацію та атак по стороннім каналам. Ця стаття присвячена дослідженню саме такої, практичної, стійкості Dilithium до атак на помилки.

Схема ЕП Dilithium [1] пройшла до третього раунду процесу постквантової стандартизації NIST в якості одного з трьох фіналістів. Статус «фіналіст» означає, що дана схема придатна до застосування у багатьох додатках,та випадках використання [2]. Характерними рисами Dilithium є маленькі розміри ключів та підпису, достатня швидкість, простота та гнучкість(адаптація до різних рівнів стійкості).

Очікується що незабаром після закінчення третього раунду відбудеться процес стандартизації одного з двох фіналістів ЕП (Dilithium або Falcon, обидві схеми засновані на математиці алгебраїчних решіток).

1. Основні відомості про стійкість Dilithium

Доцільно сказати, що теоретична та практична стійкість повинні доповнювати одна іншу, тому спочатку наведемо рівні доказової стійкості для України та сумісність з ними Dilithium.

Для використання в Україні пропонуються наступні чотири рівні доказової стійкості (класична / квантова):

0-й рівень – 128 біт / 64 біт

1-й рівень – 256 біт / 128 біт

2-й рівень – 384 біт / 192 біт

3-й рівень – 512 біт / 256 біт

Dilithium забезпечує 1й(AES128), 2й(SHA256/ SHA3-256) та 3й(AES192) рівні стійкості згідно NIST. Наприклад стійкість AES128 означає, що зламати схему так само важко як зламати 128-бітний AES повним перебором.

Важливо розуміти можливості таких атак на помилки на алгоритми ЕП, але до того як буде прийнято рішення щодо стандартизації постквантового ЕП в Україні, щоб забезпечити їх безпечне впровадження у перехідний та постквантовий періоди.

Стійкість Dilithium заснована на складності задачі Модульного навчання з помилками (MLWE) та Модульного короткого цілого рішення (MSIS). Схема підпису Dilithium використовує структуру Фіат – Шаміра з перериваннями. Структура Фіат – Шаміра потребує використання нонсу (одноразового випадкового значення), через це вона має добре відому вразливість – при використанні однакового нонсу для різних повідомлень, стає можливим відновити особистий ключ. Автори Dilithium запропонували контр захід до цієї атаки – вироблення нонсу шляхом гешування повідомлення та ключа, тож кожен раз нонс є унікальним. Таке рішення забезпечує детермінованість схеми ЕП, однак воно не стає у нагоді, коли зловмисник застосовує атаку на помилки. Він може ввести обчислювальну помилку в одному з підписів, тож два повідомлення будуть мати однаковий нонс.

2. Параметри Dilithium

Спершу наведемо основні параметри Dilithium, які знадобляться при описі атаки на помилки, причому c, h, z – частини підпису, де:

- c – значення після застосування гешування;
- σ – цифровий підпис;
- s – малий елемент особистого ключа;
- y – шум(компонент маскування;
- tr – геш-значення відкритого ключ.

Функція XOF у підписі Dilithium застосовується для детерміновано розширення початкового значення матриці A, використовуючи функцію розширюваного виводу SHAKE128. Ця функція зменшує розміри відкритого та особистого ключів, оскільки потрібно зберігати тільки ρ замість повного значення матриці A .

3. Сутність атаки на помилки

Атаки на помилки вперше були представлені в 1996 р. Боне та ін. [3] для реалізації атаки на RSA-CRT, а незабаром Біхам і Шамір описали диференціальну атаку на помилки стосовно шифру DESblock [4]. Атаки на помилки – це розповсюджений метод криптоаналізу, який полягає у внесенні помилок на будь-якому етапі дії електронної схеми, у нашому випадку, схеми ЕП Dilithium. Даний тип атак належить до атак по стороннім каналам.

Атаки на помилки на електронні системи вивчалися більше 40 років. Відтоді до реального обладнання застосовувались різні форми внесення помилок, такі як зміна напруги, подача високих температур на апаратні засоби, використання рентгенівських променів тощо [5]. Через необхідність фізичного доступу до пристрою внесення помилок в основному загрожували захищеному відмовостійкому апаратному забезпеченню, як смарт-картки, так і жорстким апаратним модулям безпеки. Це змінилося з появою апаратної помилки Rowhammer, що впливає на основну пам'ять комп'ютера [6]. У 2014 р. Кім та інші показали, що зловмисне програмне забезпечення може використовувати пошкодження пам'яті, щоб викликати обернення бітів у сусідніх областях пам'яті, минаючи захист пам'яті обладнання [6]. За допомогою Rowhammer помилки стало можливо вносити дистанційно і за допомогою лише програмного забезпечення. Такий спосіб став потужною можливістю внесення помилки.

Сутність диференційної атаки на помилки на схему Dilithium заключається у наступному. Зловмисник створює таку ситуацію, в якій жертва двічі підписує одне і те ж повідомлення, але в одному з підписів внесена обчислювальна помилка (наприклад, за рахунок збоїв годинника). Це призводить до того, що різні підписи використовують однаковий нонс, таким чином стає можливим відновити особистий ключ. При диференційних атаках на помилки різниця між помилковим та правильним виводом використовується для визначення інформації про особистий ключ.

4. Можливості здійснення атаки на помилки

Спочатку визначимо якою може бути помилка. Помилкою може бути пропуск інструкцій, арифметична помилка, збій у сховищі тощо. Помилки можуть застосовуватися протягом великого періоду часу виконання, а не лише у конкретних операціях.

Коротко проведення атаки можна описати наступним чином. Підписувач двічі виконує підписання одного повідомлення M. Перший раз помилка не вноситься, та отримуємо дійсний і коректний підпис $\sigma = (\mathrm{z}, \mathrm{h}, c)$. Другий раз вноситься помилка (змінні при підписі з помилкою позначаються рискою $'$). Більш точно, помилка вноситься така, що за рахунок детермінованості y' є непорушеним та дорівнює y, проте $c' \neq c$, таким чином $\mathrm{z}' = \mathrm{y} + c'\mathrm{s}_1$.

Однак структура Фіат – Шаміра з перериванням створює додаткові перешкоди для здійснення атаки. Існує вимога, щоб обчислення як дійсного, так і помилкового підпису закінчу-

валось однаковою ітерацією циклу переривання. Іншими словами, коли k_f позначає кінцеве значення лічильника циклу k, потрібно, щоб $\Delta k_f = k_f - k'_f = 0$. Зауважимо, що в алгоритмі підпису лічильник циклу k вводиться до детермінованої вибірки. Отже, щоб виконувалась тотожність $y = y'$ постає вимога $\Delta k_f = 0$. Через проміжні помилки та вплив тестів відхилення це, очевидно, не гарантується.

Далі описуються можливі сценарії здійснення атаки на помилки.

4.1. Випадкова помилка при зверненні до геш-функції

При даному способі внесення помилки до обчислення $c \in B_{60} := \mathrm{H}(\mu \| \mathrm{w}_1)$ вводиться випадкова помилка. Наприклад, можна використати один із входів μ, w_1 безпосередньо перед їх використанням у H, або внести помилку безпосередньо у саму геш-функцію H.

У [7] показано, що зловмисник може ввести помилку в правильну ітерацію k_f, тобто в останню при обчисленні помилки. Якщо крок відхилення проходить з різним c', секретний елемент s_1 може бути відновлений.

Атака відбулась успішно, якщо відновлений елемент особистого ключа s_1 є малим, а Δc є оборотним. Це вірно з дуже високою ймовірністю. Частка оборотних поліномів у R_q дорівнює $(1-1/q)^n$ [8], що для параметрів Dilithium приблизно становить $1-2^{-15}$. Знаючи s за допомогою лінійної алгебри можна відновити повний секретний ключ. Також можна використати малу норму $c\mathrm{s}$ обчислюючи $\|\Delta \mathrm{z}\|_2$ (або $\|\Delta \mathrm{z}\|_2$) і перевірити, чи вона не нижче певного порогу.

4.2. Випадкова помилка у множенні поліномів геш-функції

Ця помилка зводиться до зміни складової підпису $c := \mathrm{H}(\mu, \mathrm{w}_1)$ у геш-значенні H, яке використовується при обчислення її вхідних параметрів μ, w_1. Геш-значення повідомлення або відкритого ключа μ також використовується як початкове значення (seed) для детермінованої вибірки, отже, помилки в обчисленні $\mu := \mathrm{CRH}(tr \| M)$ не можна використати. Але можна використати помилки в обчисленні $\mathrm{w} := \mathrm{Ay}$, які призводять до неправильного w_1. Необхідні множення поліномів у q можна ефективно реалізувати за допомогою теоретико-числового перетворення (NTT). Тим не менш, час множення є більше, ніж час гешування, тому множення може підходити для атак на помилки. Варто зазначити, що зменшення кількості коефіцієнтів помилки збільшує ймовірність успіху оскільки непорушені коефіцієнти w чітко проходять відхилення, а одного зміненого достатньо для досягнення $\Delta c \neq 0$. Таким чином, на відміну від інших сценаріїв з [7], таке застосування помилки має набагато сильніший вплив.

Більш імовірно, що атака буде успішною якщо вносити помилку не у прямий NTT від y, а у зворотній, застосований до w, у цьому випадку порушені лише два коефіцієнти. Однак однокоефіцієнтні помилки трохи рідше призводять до успішного відновлення ключів. Це пов'язано з тим, що коефіцієнт помилки w' може округлиться до правильного $w'_1 = w_1$, що призводить до $\Delta c = 0$ і помилку не можна використати.

4.3. Випадкова помилка при завантаженні особистого ключа та розширенні початкового значення

Сутність даної помилки – виконати розширення початкового значення ρ до матриці A. Дана операція є привабливою з трьох причин:

- помилка вноситься перед входом у цикл переривання і, таким чином, завжди виконується за один час;

- розширення до A дає головний внеск до загального часу виконання;

- A має більший слід (20 кБ у Dilithium-III), ніж інші змінні, і потенційно зберігається в пам'яті протягом тривалого часу. Тому, при обчисленні його кеш-значення не потрібно повторно запускати ExpandA для кожної операції підпису. Також існує атака на пам’ять Rowhamer, яка має схожий принцип дії.

Різниці (диференціали) у матриці A можна досягти, використовуючи початкове значення ρ, наприклад, під час завантаження особистого ключа, або вносячи помилку у розширення $A \in R_q^{k \times l} := \text{ExpandA}(\rho)$. У першому випадку поліноми $k \cdot l$, що містять A, створюються за допомогою незалежних викликів SHAKE у методі розширення ρ до A. І помилка у перестановці SHAKE призводить до лише одного полінома з помилкою. Отже, після множення матриці на вектор Ay маємо n різних коефіцієнтів w. У другому випадку, помилка вводиться напряму у ρ під час імпорту або при зберіганні значення, що призводить до зовсім іншого значення A і, таким чином до w. Цей тип помилок варто застосовувати, якщо використовуються контр заходи, такі як подвійне обчислення, тому що у цьому разі помилку складно виявити. Хоча ймовірність успіху другого методу менше у порівнянні з першим [7].

4.4. Повторне використання нонсу

Задача даної атаки – створити сценарій повторного використання нонсу з використанням помилок для генерації екземпляру LWE який буде мати тривіальне розв’язання. Спільною рисою ряду схем (NewHope, Frodo, Dilithium, Kyber) на основі LWE є процедура вибірки помилок.

Логіка атаки: У процедурі генерації ключів як компонент помилки, так і компонент секрету екземпляру LWE генеруються з використанням початкових значень (seed), які відрізняються один від одного лише одним значенням нонсу. Ці початкові значення далі вводяться до функції вибірки, яка генерує необхідні поліноми за рахунок використання функцій XOF з родини SHA3. Найбільш важливим спостереженням є те, що початкові значення відрізняються лише значенням нонсу, щоб згенерувати компоненти секрету та помилки екземпляру LWE. Спосіб виконання даної атаки полягає у тому щоб пересвідчитись, що використовуються однакові нонси як для генерації секрету, так і помилки. А робиться це за допомогою внесення відповідних помилок.

Далі показано, як знайдені вразливості можуть призвести до атак відновлення особистого ключа Dilithium.

У [9] було досліджено можливість здійснення атаки по відновлення ключа на Dilithium, на схему, яка виконує операції з модулями (матрицями/векторами/поліномами у кільці). Атака націлена на процедуру генерації ключів.

Визначимо екземпляр LWE t як тип LWE_{PK}. Кратні поліноми у відповідних компонентах секрету та помилки створюються з використанням дуже схожих початкових значень (seed), які відрізняються лише значенням нонсу, яке детерміновано збільшується. Якщо до реалізації повторного використання нонсу, при генерації компонентів секрету і помилки, можна внести кратні помилки, то $\mathbf{t}$ зводиться до множини визначених лінійних рівнянь ($k \times n$ невідомих оскільки $k > l$).

Існує достатньо специфічна але істотна відмінність щодо розкриття екземплярів LWE у схемі Dilithium. Відкритий ключ розкриває лише $\mathbf{t}_1$, d верхніх біт $\mathbf{t}$, тоді як $\mathbf{t}_0$ (компонент нижнього порядку) є частиною особистого ключа. Навіть при повторному використанні нонсу не має можливості тривіально отримати секретне значення s з помилкового відкритого ключа. Але відзначимо, що аналіз стійкості підпису Dilithium робиться за припущення, що усе $\mathbf{t}$ можна відновити лише при перегляді декількох підписів, які були генеровані на одному ключі. Таким чином доцільно припустити, що після успішного внесення помилок до

процедури генерації ключів, це призводить до успішної атаки відновлення ключа у схемі підпису Dilithium.

4.5. Часткове повторне використання нонсу

Даний спосіб атаки спершу застосовувався до підписів на еліптичній кривій [10], потім був перенесений на схеми на решітках та для Dilithium було отримано 100 % ймовірність успіху атаки [7].

Алгоритм атаки:

1) Внести помилку $\mathrm{y}' \in S^{l}_{\gamma_1-1}$, але таку, що лише один коефіцієнт $\left(\underline{y'}_u\right)_v \in \mathrm{y}$ (з індексом $u \in \{0,...,l-1\}$) та $v \in \{0,...,n-1\}$ змінюється на випадкове значення. Це все ще призводить до зовсім іншого w_1, а отже, до різного c' та $\mathrm{z}' = \mathrm{y}' + c'\mathrm{s}_1$.

2) Обчислити $\mathrm{s}_1 = \Delta c^{-1} \cdot \Delta \mathrm{z}$.

3) Визначити u, просто використовуючи один індекс для яких $s_{1,u} \notin S_\eta$. Для всіх $i \neq u$ маємо, що $\Delta y_i = 0$, таким чином вдається відновлення цих поліномів ключа.

4) Встановити поріг $\delta = 60\eta$, такий щоб $\|c\mathrm{s}_1\|_\infty \le \delta$ виконується для будь-яких c і s_1.

5) Визначити індекс v і далі положення помилки допомогою індексу максимального $|\Delta z_u|$. Оскільки введена помилка $\left(\underline{y'}_u\right)_v$ може спричинити будь-яку різницю від значення, але в середньому вона буде великою. Як очікувалось $\left|\left(\underline{y'}_u\right)_v - \left(\underline{y}_u\right)_v\right|$ буде $\frac{2_{\gamma_1}-1}{3}$, оскільки обидва ці коефіцієнти є випадковими значеннями в $\left[-(\gamma_1-1),(\gamma_1-1)\right]$ (за припущенням).

6) Відновити $s_{1,u}$. Для цього потрібно видалити рядок v лінійної системи $s_{1,u} = \Delta c^{-1} \cdot \Delta z_u$, відгадати значення $\left(\underline{s}_{1,u}\right)_v$ (вичерпним пошуком), розв'язати для повного $s_{1,u}$ і перевірити чи є він у S_η.

5. Заходи щодо протидії можливим атакам

Після аналізу ряду джерел було знайдено п’ять заходів протидії атакам на помилки. Далі наведено сутність заходів, їх переваги та недоліки.

5.1. Повторне обчислення підпису

Для того щоб виявити помилку у підписі, можна виконати його повторне обчислення та порівняти два підписи. Але якщо внести помилку двічі, або помилка є постійною (якщо внести її при завантаженні особистого ключа), то цей захід не захистить від атаки. Також його недоліком є подвійний час виконання.

5.2. Перевірка після підпису

Більшість способів атаки призводять до того, що підписи є недійсними. Таким чином, якщо перевірити підпис, то буде виявлено помилку підпису, що є ефективним заходом протидії. При чому, час перевірки приблизно у три рази менше часу вироблення підпису [11], тому цей варіант є більш ефективним ніж повторне обчислення підпису. Але недоліком є те, що даний захід не може виявити помилки, внесені до вибірки y, оскільки при цьому виробляються дійсні підписи.

5.3. Додаткова випадковість

Ще одним контрзаходом є внесення додаткової випадковості до детермінованої вибірки шуму $\mathbf{y}$. Можна просто взяти вибірку випадкового $r \leftarrow 0,1^{256}$, а потім викликати $\mathbf{y} := \text{DeterministicSample}(K \| \mu \| \kappa \| r)$. Це ефективно пом'якшує диференційну атаку на помилки, оскільки виклик помилки до алгоритму підпису використовує різні $\mathbf{y}$ і, отже $\| \mathbf{y} \neq 0$.

Більше того, цей метод також може перешкодити подальшим атакам по стороннім каналам, що стають побічним ефектом детермінізму. Як зазначають [12, 13], змішування відомого повідомлення μ з таємним початковим значенням K у геш-функції (у Dilithium це SHAKE у DeterministicSample) відкриває двері для DPA-подібних атак. Функції гешування важко захистити від таких атак; використання додаткового випадкового значення може бути альтернативою. Додатковими перевагами цього контрзаходу є його простота та незначна тривалість виконання. Крім того, на відміну від прямих реалізацій двох попередніх контрзаходів, він є однопрохідним і тому не потребує збереження копії повідомлення в пам'яті. Наприклад, автори qTESLA вимагають використовувати цей контрзахід через наявність зазначених вище атак.

Недоліком даного заходу протидії є його ймовірнісний характер, та необхідність у генераторі випадкових чисел. Такий генератор може бути доступний не на всіх пристроях, особливо малоресурсних. Також, введення цього контрзаходу скасовує гарантії стійкості, хоча конкретні атаки невідомі. Автори Dilithium "все ще рекомендують використовувати детерміновані підписи, за винятком середовищ, які можуть бути вразливими до вищезгаданих атак по стороннім каналам" [11]. Однак визначити, чи є вразливим середовище чи ні, непросто, як це чітко показано помилкою Rowhammer.

5.4. Перевірка значення нонсу

Щодо атаки повторного використання нонсів у еталонній реалізації, Dilithium може стати легкою мішенню за рахунок атак на помилки. Основна причина, однак, пов'язана з використанням початкових значень (seed) для створення компонентів секрету та помилки, які змінюються лише на один або два байти через нонс. Значення нонсу насамперед визначає різницю між компонентами секрету та помилки. Таким чином, важливо провести перевірку значення нонсу, що може унеможливити атаку. Існує маса відомих вразливостей задачі LWE, в [7] реалізували одну із вразливостей за допомогою помилок. Таким чином, проведення простих перевірок секретних та помилкових компонентів екземплярів LWE на предмет відомих тривіальних слабкостей також може бути потенційним контрзаходом проти даної атаки.

5.5. Обчислення середнього значення та дисперсії вибірки

Наступний захід протидії, запропонований у [7], обчислює середнє значення вибірки та дисперсію вибірки, одночасно перевіряючи наявність повторень. Перевірка дисперсії вибірки є особливо важливою, оскільки цей параметр пов’язаний зі складністю задачі LWE криптографічної схеми. Зменшення дисперсії вибірки помилок може спростити вирішення екземплярів LWE. Ці контрзаходи також виявляють помилки у вибірці та будь-які зловмисні реалізації. В апаратному забезпеченні цей тест буде обчислюватися після обсягу вибірки в два рази, тому не має необхідності явно обчислювати розподіл. Це зручно для такої схеми як Dilithium, яка вимагає $n = 256$ для кожного підпису.

Обчисливши середнє значення та дисперсію, можна провести статистичні тести, щоб побачити, чи ці значення є допустимими. Для середнього значення проводиться t-тест, щоб побачити, чи середнє значення цієї вибірки знаходиться в допустимих межах (попередньо

розрахованих). Для дисперсії проводиться тест хі-квадрата, щоб побачити, чи дисперсія вибірки знаходиться в межах допустимого заздалегідь визначеного значення.

Даний контрзахід додає приблизно 44 % необхідних ресурсів до вибірки CDT. Однак він має фіксовану вартість, та необхідності у додаткових апаратних ресурсах не буде, якщо дискретизатор помилок був повільнішим чи більшим. Цей контрзахід також має мінімальний вплив на продуктивність, оскільки більшість розрахунків обчислюються в паралельному розподілі помилок. В цілому для завершення обчислень потрібен лише один додатковий такт після того, як розподіл помилок завершить генерацію n вибірок.

Висновки

1. Із наведеного можна зробити висновок, що диференційні атаки на помилки становлять загрозу сучасним та перспективним схемам електронного підпису. це стосується і фіналіста конкурсу на постквантовий стандарт Dilithium.

2. Слабкими властивостями схеми Dilithium щодо атаки на помилки є геш-функція (можливо внести випадкову помилку при зверненні до геш-функції та в операцію множення поліномів), а також функція розширення початкового значення та стадія завантаження особистого ключа. Також з'являється вразливість через використання нонсу – порушник може використати двічі однакове значення нонсу (частково чи повністю).

3. Основними методами захисту від вказаних атак можуть бути:

- повторне обчислення підпису;
- перевірка підпису після підписання, що є втричі швидшим ніж попередній метод;
- внесення додаткової випадковості до детермінованої вибірки шуму;
- перевірка значення секретних та помилкових компонентів (нонсу);
- обчислення середнього значення та дисперсії вибірки, та перевірка на приналежність заданому діапазону.

Так, наприклад, зменшення дисперсії свідчить про те, що варіант LWE, на якому заснована стійкість Dilithium, значно простіше вирішити.

4. Тому розробникам постквантових схем ЕП доцільно врахувати знайдені вразливості для забезпечення стійкості до атак на помилки та застосувати знайдені рішення щодо захисту від даних атак.

5. Потрібно взяти до уваги можливі побічні ефекти після застосування контрзаходів, такі як збільшення необхідних ресурсів, порушення вимоги детермінованості схеми, зменшення ефективності.

Список літератури:

1. CRYSTALS-Dilithium. Algorithm Specifications and Supporting Documentation. Access mode https://pq-crystals.org/dilithium/data/dilithium-specification-round2.pdf

2. Відео-конференція NIST. Режим доступу: https://icmconference.org/?page_id=14324

3. Dan Boneh, Richard A. DeMillo, and Richard J. Lipton. On the Importance of CheckingCryptographic Protocols for Faults (Extended Abstract). InEUROCRYPT, Lecture Notesin Computer Science, pages 37–51. Springer, 1997.

4. Eli Biham and Adi Shamir. Differential Fault Analysis of Secret Key Cryptosystems. InCRYPTO, Lecture Notes in Computer Science, pages 513–525. Springer, 1997.

5. H. Bar-El, H. Choukri, D. Naccache, M. Tunstall, and C. Whelan. The sorcerer's apprentice guide to fault attacks // Proceedings of the IEEE, vol. 94, no. 2, pp. 370–382, 2006.

6. Y. Kim, R. Daly, J. Kim, C. Fallin, J. H. Lee, D. Lee, C. Wilkerson, K. Lai, and O. Mutlu. Flipping bits in memorywithout accessing them: An experimental study of dram disturbance errors // SIGARCH Comput. Archit. News, vol. 42,no. 3, pp. 361–372, Jun. 2014. Access mode: http://doi.acm.org/10.1145/2678373.2665726

7. Leon Groot Bruinderink and Peter Pessl. Differential Fault Attacks on Deterministic Lattice Signatures // Access mode: https://eprint.iacr.org/2018/355.pdf

8. Vadim Lyubashevsky, Chris Peikert and Oded Regev. A Toolkit for Ring-LWE Cryptography. // EUROCRYPT, volume 7881 ofLecture Notes inComputer Science, pages 35–54. Springer, 2013.

9. Prasanna Ravi1, Debapriya Basu Roy, Shivam Bhasin, Anupam Chattopadhyay, and Debdeep Mukhopadhyay. Number "Not Used" Once – Practical fault attack on pqm4 implementations of NIST candidates. Access mode: https://eprint.iacr.org/2018/211.pdf

10. Christopher Ambrose, Joppe W. Bos, Björn Fay, Marc Joye, Manfred Lochter, and Bruce Murray. Differential Attacks on Deterministic Signatures // CT-RSA, volume 10808 of LNCS, pages 339–353. Springer, 2018.

11. Vadim Lyubashevsky, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Peter Schwabe, Gregor Seiler and Damien Stehlé // CRYSTALS-Dilithium. Submission to the NIST Post-Quantum Cryptography Standardization [NIS], 2017. Access mode: https://pq-crystals.org/dilithium.

12. Hermann Seuschek, Johann Heyszl, and Fabrizio De Santis. A Cautionary Note: Side-Channel Leakage Implications of Deterministic Signature Schemes // CS2@HiPEAC, pages 7–12. ACM, 2016.

13. Niels Samwel, Lejla Batina, Guido Bertoni, Joan Daemen, and Ruggero Susella. Breaking Ed25519 in WolfSSL // CT-RSA, volume 10808 of Lecture Notes in Computer Science, pages 1–20. Springer, 2018.

14. James Howe, Ayesha Khalidy, Marco Martinoli, Francesco Regazzoniz and Elisabeth Oswald. Fault Attack Countermeasures for Error Samplers // Lattice-Based Cryptography. Access mode: https://eprint.iacr.org/2019/206.pdf

Надійшла до редколегії 02.09.2020

Відомості про авторів:

Горбенко Юрій Іванович – канд. техн. наук, АТ «інститут інформаційних технологій», перший заступник головного конструктора, e-mail: gorbenkou@iit.kharkov.ua, ORCID: https://orcid.org/0000-0003-0073-9107

Дроздова Ольга Сергіївна – АТ «інститут інформаційних технологій», аналітик з систем захисту інформації, Україна, e-mail: 4akolzinaolga@gmail.com

УДК 004.056.55 **DOI:10.30837/rt.2020.3.202.05**

І.Д. ГОРБЕНКО, д-р техн. наук, С.О. КАНДІЙ, М.В. ЕСІНА, канд. техн. наук, Є.В. ОСТРЯНСЬКА

ГЕНЕРАЦІЯ ЗАГАЛЬНОСИСТЕМНИХ ПАРАМЕТРІВ ДЛЯ КРИПТОСИСТЕМИ FALCON ДЛЯ 256, 384, 512 БІТ БЕЗПЕКИ

Вступ

В останнє десятиріччя спостерігається практично завершальне створення математичних основ та програмного забезпечення квантового комп'ютера [1]. Також спостерігається стійкий прогрес у створенні безпосередньо квантових комп'ютерів різного призначення та різних можливостей [2]. При цьому особлива увага приділяється реалізації великомасштабних квантових комп'ютерів, що призначаються для криптоаналізу існуючих криптосистем з відкритим ключем – електронних підписів, асиметричних шифрів та криптографічних протоколів різного призначення [1 – 3]. Певні сумніви є і щодо симетричних криптоперетворень блокового та потокового шифрування, але збільшення при їх використанні розмірів параметрів та ключів за нинішніх поглядів дозволяє забезпечити криптографічний захист на далеку перспективу. Зважаючи на вказане, Національний інститут стандартів і технологій (NIST) США знаходиться в процесі вибору криптографічних алгоритмів з відкритим ключем через проведення відкритого конкурсу. Прийняті в майбутньому нові стандарти криптографії з відкритим ключем визначатимуть один або кілька додаткових алгоритмів для цифрових підписів, асиметричного шифрування та встановлення ключів. Вважається, що ці стандартизовані алгоритми будуть здатні захистити конфіденційну інформацію уряду США в доступному для огляду майбутньому, в тому числі після появи квантових комп'ютерів. Таким чином, однією з основних проблем сучасної криптографії є створення стандартизованих криптографічних схем, які були б безпечними у постквантовий період.

На світовому рівні зусилля значного числа теоретичних криптологів, математиків та криптологів-практиків зосереджені на відкритому конкурсі NIST PQC [2]. Одним із основних завдань конкурсу є розробка та прийняття постквантового чи постквантових стандартів електронного (цифрового) підпису (ЕП). Фіналістами другого етапу конкурсу NIST стали три механізми ЕП – CRYSTALS-DILITHIUM, FALCON та Rainbow. Окрім цього, були визначені три альтернативних кандидати, які потребують більш детальних досліджень. У цілому всебічний аналіз фіналістів є важливою задачею для криптологів світової криптоспільноти. Причому, безпека, тобто доведення криптографічної стійкості двох кандидатів-фіналістів, на стандарт ЕП – CRYSTALS-DILITHIUM та FALCON, ґрунтується на проблемах з теорії та практики алгебраїчних решіток [1, 3].

Дослідження показали, що серед схем ЕП на решітках дещо відрізняється від інших кандидатів та має перспективи щодо прийняття в якості стандарту FALCON [1, 4]. Основним та домінуючим підходом до проєктування механізму ЕП FALCON є використання перетворення Фіата – Шаміра з перериваннями [5, 6]. Його перевагою є доказова стійкість в межах моделі квантового випадкового оракула. Але його аналізу присвячено значно менше робіт, ніж, наприклад, щодо CRYSTALS-DILITHIUM. Крім того, при проєктуванні ЕП FALCON були прийняті обмеження щодо рівнів безпеки, максимально 256 біт проти класичного та 128 біт проти квантового криптоаналізу. Ці обмеження, на наш погляд, пов'язані зі складністю обчислення загальносистемних параметрів, а також з суттєвим впливом їх збільшення параметрів на швидкодію ЕП. Тобто, для безпечного використання ЕП FALCON повинні бути знайдені набори загальносистемних параметрів, за яких забезпечується стійкість до всіх відомих та потенційних атак. В процесі формування вимог до ЕП NIST у рамках конкурсу був зацікавлений тільки в наборах загальносистемних параметрів до 256 біт класичної безпеки включно. Проте, на нашу думку, на перспективу доцільним є забезпечення не менше 384 і 512 біт безпеки проти класичного криптоаналізу та не менше 192 та 256 біт безпеки проти квантово-

го криптоаналізу. Але, як показали дослідження, як з точки зору теорії так і практики, генерація загальносистемних параметрів для використання 384 і 512 біт безпеки проти класичного криптоаналізу та 192 та 256 біт безпеки проти квантового криптоаналізу.

Метою статті є класифікація та первинний аналіз відомих атак на криптосистему ЕП FALCON, встановлення обмежень та розробка практичних алгоритмів обчислення (генерації) загальносистемних параметрів для забезпечення не менше 256, 384 і 512 біт безпеки проти класичного та не менше 128, 192 та 256 біт проти квантового криптоаналізу.

1. Сутність механізму ЕП FALCON

Проєкт ЕП FALCON [1, 4] у цілому є механізмом (схемою) ЕП на алгебраїчних решітках. Вважається, що безпека ЕП FALCON ґрунтується на складності проблеми SIS (коротке ціле рішення) над решітками NTRU, а докази безпеки наведені як у випадковій моделі оракула (ROM), так і в моделі QROM [5]. Як показують дослідження, механізм ЕП FALCON є складнішим для впровадження, наприклад ніж DILITHIUM[1]. Він вимагає використання деревних структур даних, операцій з плаваючою крапкою та випадкової вибірки з декількох дискретних гауссових розподілів.

Однією з основних переваг FALCON є те, що він забезпечує у порівнянні з ЕП CRYSTALS-DILITHIUM та Rainbow найменші розміри відкритого ключа та ЕП. Безпосередньо ЕП FALCON також ефективний, хоча генерація ключів відбувається повільніше [1]. Також ЕП FALCON можуть легко вводитись існуючі стандартизовані криптографічні протоколи та програми, що в середньому забезпечує хороші загальні показники.

В основу механізму ЕП FALCON покладено перетворення фреймворк GPV [7], в якому відкритим ключем є базис $A \in \mathbb{Z}_q^{n \times m}$ решітки Λ. У якості особистого (закритого) ключа використовується редукований базис $B \in \mathbb{Z}_q^{m \times m}$ дуальної решітки $\Lambda^{\perp}$. В механізмі ЕП FALCON використовуються NTRU решітки виду [4]:

$$A = \begin{bmatrix} 1 & h \\ 0 & q \end{bmatrix}, B = \begin{bmatrix} f & g \\ F & G \end{bmatrix}, \quad (1)$$

де ключові дані f, g, h, F, G є поліномами у кільці поліномів $\mathbb{Z}_q[X]/(\phi(X))$. Щодо них виконується порівняння

$$fG - gF = q \bmod \phi. \quad (2)$$

Якщо f, g є малими поліномами, то задача вирішення рівняння (2) стає складною. Використання структурованих решіток дає змогу зменшити розмір ключів та передавати не всю матрицю базису, а лише поліноми, що її формують.

При виробленні ЕП для повідомлення m застосовується пара поліномів (s_1, s_2), для якої виконується рівність

$$s_1 + s_2 h = H(r \| m) \quad (3)$$

де r – сіль(початкова ентропія) ключа, H – деяка криптографічна геш-функція, що відображає бінарні данні на вектори. Таких (s_1, s_2) існує багато і знайти їх неважко, проте якщо ввести обмеження $\|s\| < \beta$, де β має достатньо мале значення, то задача стає важкою і зводиться до проблеми *SIS*. Таким чином, основною проблемою, на якій ґрунтується безпека механізму ЕП FALCON, є SIS на NTRU-решітках, тобто знаходження короткого цілого рішення (Short Integer Solution).

2. Аналіз атак на ЕП FALCON

Перетворення GPV [7], яке застосовується в ЕП FALCON**,** вимагає щоб геш-функція H була захищена від колізій. Це означає, що розмір солі в бітах повинен бути не меншим за 2λ, де λ – рівень безпеки, що вимагається. Проте, за умовами конкурсу NIST [8] кількість запитів на вироблення ЕП (signature queries) є не більшою за $q_s = 2^{64}$, що дає розмір $\lambda + \log_2(q_s)$. Тобто, для 5-7 рівнів безпеки це дає значення, що наведені в табл. 1.

Таблиця 1

Розмір в бітах солі r

Безпека	Розмір r	Розмір r з врахуванням вимог NIST
256	512	320
384	768	448
512	1024	576

Аналіз показав, що основними атаками ЕП FALCON є атаки на відновлення особистого (секретного) ключ з відкритого ключа та атаки на підробку ЕП. Розглянемо ці атаки.

2.1. Атаки на відновлення особистого (секретного) ключа з відкритого ключа

Атаки на відновлення особистого (секретного) ключа з відкритого ключа можуть зводиться до вирішення проблеми NTRU [4]. У ряді схем, стійкість яких ґрунтуються на проблемі NTRU, поліноми f, g мають коефіцієнти з множини значень $\{0,1,-1\}$. Це робить можливим реалізувати різні комбінаторні атаки. Наприклад, для ДСТУ 8961:2019 «Скеля» найефективнішою атакою є гібридна атака, яка знаходить частину вектора комбінаторними шляхами. Для Falcon такі атаки неможливі, оскільки поліноми f, g змінюються (точніше, семплуються) згідно з нормальним розподілом з заданими параметрами. За даного перетворення простір можливих значень поліномів збільшується настільки, що застосування комбінаторних методів стає неефективним. Залишається прямий шлях відновлення особистого ключа з відкритого засобом редукції базису решітки. При цьому, чим менші значення має норма найменшого вектора (f, g), тим більша криптостійкість системи. В криптосистемі Falcon поліноми генеруються над полем

$$\mathbb{Z}_q[X]/(\phi(x)), \deg(\phi) = n$$

з математичним очікуванням рівним 0. Перетворення спираються на результати роботи [12] , у якій детально досліджувалися можливості застосування алгоритмів семплування нормально розподілених величин. В [12] було показано, що алгоритм семплування Клейна може давати вектори розміру $\approx \sqrt{\frac{qe}{2}}$, що є дуже близьким до теоретичного мінімуму $\sqrt{q}$. Відповідно, щоб отримати такий розмір, кожний коефіцієнт отримується з розподілу з середньоквадратичним відхиленням

$$\sigma' = \sqrt{\frac{qe}{2}} * \frac{1}{\sqrt{2n}}.$$

Згідно з [9] найменший вектор може бути знайдений, якщо його проекція на простір, що натягнутий на перші B векторів $b_1^*, b_2^*, ..., b_B^*$ буде менша за b_{2n-B}^*. Згідно з [9, 12] ця проекція може бути оцінена як

$$\sqrt{\gamma_B} * \det(\Lambda_{[b_1^*,...,b_B^*]}) \approx \sqrt{\frac{3}{4}} * \sigma' \sqrt{B} = \sqrt{\frac{3}{4}} * \sqrt{\frac{qe}{2}} * \frac{1}{\sqrt{2n}} * \sqrt{B} \quad (4)$$

Водночас, згідно з [9, 12] b_{2n-B}^* може бути оцінений як

$$\left\|b^*_{2n-B}\right\| \approx GH(B)^{\frac{2n+1-2(2n-B)}{2(B-1)}} \det(\Lambda)^{\frac{1}{2n}} = GH(B)^{\frac{2B-2n+1}{2B-2}} \sqrt{q} = \left(\frac{B}{2\pi e}\right)^{\frac{2B-2n+1}{2B-2}} \sqrt{q} \quad (5)$$

Таким чином, маємо умову щоб:

$$\left(\frac{B}{2\pi e}\right)^{\frac{2B-2n+1}{2B-2}} \sqrt{q} < \sqrt{\frac{3eB}{8n}} * \sqrt{q}\,. \quad (6)$$

Далі, завдяки вибору $\sigma' = \sqrt{\frac{qe}{2}} * \frac{1}{\sqrt{2n}}$ з обох сторін рівняння маємо множник $\sqrt{q}$, який можна скоротити. Тому умова захисту від атак на відновлення особистого ключа з відкритого шляхом редукції виглядає наступним чином:

$$\left(\frac{B}{2\pi e}\right)^{\frac{2B-2n+1}{2B-2}} < \sqrt{\frac{3eB}{8n}} \quad (7)$$

2.2. Атаки на підробку ЕП

Атаки на безпосередньо підробку ЕП можуть бути найбільш загрозливими. Тому іншим вектором атаки є атака підробки ЕП. При реалізації такої атаки потрібно знайти достатньо короткий вектор s. Відповідно, це можливо зробити, редукувавши базис так, щоб виконувалася умова

$$\left\|b^*_1\right\| < \beta \quad (8)$$

Причому оцінити $\left\|b^*_1\right\|$ можливо таким же чином, що і у попередньому випадку, тобто у такій послідовності:

$$\left\|b^*_1\right\| \approx GH(B)^{\frac{2n+1-2}{2(B-1)}} \det(\Lambda)^{\frac{1}{2n}} = GH(B)^{\frac{2n-1}{2B-2}} \sqrt{q} = \left(\frac{B}{2\pi e}\right)^{\frac{2n-1}{2B-2}} \sqrt{q}\,. \quad (9)$$

Отримуємо, що умовою захисту від атак на підробку підпису є

$$\left(\frac{B}{2\pi e}\right)^{\frac{2n-1}{2B-2}} \sqrt{q} < \beta \quad (10)$$

Для практичного прийняття рішення необхідно визначитись щодо того, як обирати параметр β. Розробники ЕП Falcon пропонують використовувати значення $\sigma = 1.55\sqrt{q}$ для полінома $\phi = x^n + 1$ і $\sigma = 1.32 * 2^{1/4} * \sqrt{q}$ для полінома $\phi = x^n - x^{n/2} - 1$. Такий вибір σ базується на результатах роботи [10] і параметр β для полінома $\phi = x^n + 1$ обчислюється як:

$$\beta = 1.2 * \sigma \sqrt{2nq}\,. \quad (11)$$

Для полінома $x^n - x^{n/2} - 1$ β обчислюється таким чином:

$$\beta^2 = \frac{\left(1.2 * \sigma * 2n\sqrt{q}\right)^2}{n}. \quad (12)$$

Формули відрізняються тому, що для полінома $x^n - x^{n/2} - 1$ замість L2 норми обчислення виконуються за допомогою embedding norm під час генерації ключів та підпису.

Якщо підставити значення β у рівняння для оцінки захищеності від атак на підробку підпису, то також обидві сторони будуть пропорційні значенню $\sqrt{q}$. Таким чином, середньоквадратичні відхилиння при семплуванні поліномів з нормального розподілу підібрані таким чином, щоб від q складність атаки не залежала. Проте на параметр q існує безліч інших обмежень, які впливають на його вибір.

Параметр q обирається згідно наступних міркувань [4]:

- для захисту від алгебраїчних атак q має бути простим числом;

- якщо q буде занадто малим (порядку $q \approx n$), то будуть можливі BKW атаки;

- якщо q буде занадто великим ($q \approx n^{2.83}$), то будуть можливі атаки на підполе;

- якщо використовується поле $x^n + 1$, то для реалізації ефективного множення повинне виконуватися рівняння $q \equiv 1 \bmod 2n$;

- якщо використовується поле $x^n - x^{n/2} - 1$, то для реалізації ефективного множення повинне виконуватися рівняння $q \equiv 1 \bmod 3n$.

Примітка: Стійкість найкращого алгоритму пошуку найменшого вектору оцінюється як 2 ^ 0.292B, де B – розмір блоку при редукції. Якщо при криптоаналізі застосовувати алгоритм Гровера, то нижня оцінка класичної стійкості в 256 біт складає 2 ^ 0.265B квантової стійкості (при класичній стійкості в 256 біт. Тому, для ЕП на решітках квантова стійкість при класичній стійкості 256 біт набагато більше ніж 128 біт.

2.3. Точність арифметики з плаваючою крапкою

Останнім невизначеним параметром, який необхідно вибрати для забезпечення рівнів стійкості 384 та 512 біт, є необхідна точність виконання операцій у арифметиці з плаваючою крапкою. Розробники Falcon для теоретичної оцінки використовували роботу [10], проте точність обиралася з практичних експериментів. З роботи [10] видно, що рівень безпеки λ слабо впливає на потрібну точність. Основний вплив має кількість запитів на підпис $q_s = 2^{64}$, тому є надія, що 64 бітів буде достатньо. Проте, це питання виходить за межі даної статті і є предметом подальшого дослідження.

Також до проблемного питання щодо недоліку ЕП FALCON необхідно віднести використання арифметики з плаваючою крапкою. Разом з використанням деревоподібних структур це ускладнює аналіз схеми до атак по стороннім каналам. Іншою проблемою є складність реалізації на малоресурсних пристроях.

3. Генерація параметрів для 256, 384, 512 біт стійкості

У цілому, якщо підсумувати наведене вище, то знайти параметри n, q, β можна з системи нерівностей (13) та умов (1) – (5):

$$\begin{cases} \left(\frac{B}{2\pi e}\right)^{\frac{2n-1}{2B-2}} \sqrt{q} < \beta \\ \left(\frac{B}{2\pi e}\right)^{\frac{2B-2n+1}{2B-2}} < \sqrt{\frac{3eB}{8n}} \end{cases} \tag{13}$$

де параметр β визначається як $\beta = 1.2 * \sigma \sqrt{2nq}$, якщо використовується поліном $x^n + 1$ і $\beta^2 = \frac{\left(1.2 * \sigma * 2n\sqrt{q}\right)^2}{n}$, якщо використовується поліном $x^n - x^{n/2} - 1$.

На основі (13) розроблено програмне забезпечення, з використанням якого були обчислені параметри n, q та β^2 ЕП FALCON для відповідних поліномів для 256, 384, 512 біт безпеки, що наведені в табл. 2.

Таблиця 2

Основні загальносистемні параметри
для 256, 384, 512 біт безпеки

Безпека	$\phi(x)$	n	q	β^2
256	x^n+1	1024	12289	87070769
384	$x^n-x^{n/2}-1$	1536	18433	174141539
512	x^n+1	2048	12289	200928983

4. Отриману криптостійкість наведено в табл. 3. Криптостійкість наведено у форматі «стійкість» λ /розмір блоку.

Таблиця 3

Криптостійкість до атак на основі редукції решіток

Безпека	Стійкість до відновлення ключа (класична)	Стійкість до відновлення ключа (квантова)	Стійкість до підробки підпису (класична)	Стійкість до підробки підпису (квантова)
256	273/936	248/936	269/922	244/922
384	413/1417	375/1417	430/1474	390/1474
512	554/1899	503/1899	599/2053	544/2053

Оцінки криптостійкості отримувалися з розміру блоку як 0,265B та 0,292B. Такий підхід вважається класичним і використовувався авторами Dilithium і авторами Falcon. Проте, оцінки є досить грубими. Якщо використати підхід як в qTesla, то значення криптостійкості при тих же самих параметрах буде суттєво більшим. В табл. 3 для квантових атак для 256 і 512 sn отримані значення є трохи меншими за необхідні, проте через грубість оцінки можна вважати, що вони досягають потрібного порога. Для 256 біт згенеровані параметри співпадають із параметрами, згенерованими авторами Falcon для 256 біт рівня криптостійкості.

Висновки

1. Одним із основних завдань конкурсу NIST США є розробка та прийняття постквантового чи постквантових стандартів ЕП. Фіналістами другого етапу конкурсу NIST стали три механізми ЕП – CRYSTALS-DILITHIUM, FALCON та Rainbow. Причому, подальше вирішення проблеми безпеки, тобто доведення криптографічної стійкості двох кандидатів-фіналістів, на стандарт ЕП FALCON, може ґрунтується на проблемах теорії та практики алгебраїчних решіток.

2. Схеми цифрового підпису на решітках є основними претендентами на перемогу в конкурсі NIST PQC. Тому, їх подальший детальний аналіз та порівняння щодо основних характеристик стійкості є першочерговою задачею. Схема FALCON, як фіналіст другого етапу, потребує особливої уваги, оскільки має нетиповий дизайн, що використовує арифметику з плаваючою крапкою.

3. Криптостійкість ЕП FALCON залежить від двох добре вивчених – NTRU та SIS – проблем. Завдяки використанню семплування особистих ключів застосуванням нормального розподілу, гібридні атаки для зламу недоцільні, а NTRU атаки можуть зводиться до прямої атаки редукцією решітки. Також SIS проблема, в свою чергу, може вирішуватись за допомогою редукції решітки.

4. Завдяки використанню циклотомічних поліномів розробники проєкту FALCON досягли гарної швидкодії вироблення та перевірки ЕП з використанням бінарних та тернарних дерев. Проте недоліком такого підходу є недостатня гнучкість при генерації загальносистемних параметрів. Криптостійкість здебільшого залежить від параметра n, який має або бути ступенем двійки, або невеликим кратним до ступеня двійки. Можливі значення параметра лежать у невеликій множині, що сильно обмежує вибір параметрів.

5. Криптостійкість FALCON сильно залежить від того, наскільки малі вектори можливо семплувати з нормального розподілу. Розробники FALCON детально вивчили відомі алгоритми та обрали алгоритм Клейна, оскільки він у порівнянні з іншими алгоритмами дає найменші вектори. У подальшому дослідження та розробка нових алгоритмів семплування можуть дати можливість зменшити розміри ЕП та підвищити швидкодію.

6. До основного проблемного питання щодо недоліку ЕП FALCON необхідно віднести використання арифметики з плаваючою крапкою. Разом з використанням деревоподібних структур це ускладнює аналіз схеми до атак по стороннім каналам. Іншою проблемою є складність реалізації на малоресурсних пристроях.

7. Основним результатом, що отриманий в процесі досліджень та наведений у цій статті, є співвідношення (13), з використанням якого були обчислені та запропоновані набори загальносистемних параметрів для рівнів безпеки 256, 384, 512 біт.

8. Необхідно відмітити, що для безпеки 256 біт результат збігається з запропонованим розробниками проєкту ЕП FALCON.

9. Для отримання оцінок щодо складності задачі SIS та NTRU було використано зведення проблеми до редукції решіток. Причому через недостатню гнучкість схеми для 384 біт класичної стійкості був використаний поліном $x^n - x^{n/2} - 1$.

Список літератури:

1. *Gorjan Alagic* Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. NISTIR 8309 / Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone // 22 July 2020. Режим доступу: https://doi.org/10.6028/NIST.IR.8309.
2. Cryptography Standardization Process. Electronic resource]. Access mode: http://www.nist.gov/pqcrypto.
3. Post-Quantum Cryptography. Round 2 Submissions. [Electronic resource]. Access mode: https://csrc.nist.gov/Projects/post-quantum-cryptography/round-2-submissions.
4. Falcon. [Electronic resource]. Access mode: https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions.
5. Eike Kiltz, Vadim Lyubashevsky, and Christian Schaffner. A concrete treatment of fiat-shamir signatures in the quantum random-oracle model. Cryptology ePrint Archive, Report 2017/916, 2017. [Electronic resource]. Access mode: http://eprint.iacr.org/2017/916.
6. Dominique Unruh. Post-quantum security of fiat-shamir // IACR Cryptology ePrintArchive, 2017:398, 2017.
7. Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and newcryptographic constructions // Richard E. Ladner and Cynthia Dwork, editors,40th ACM STOC,pages 197–206. ACM Press, May 2008.
8. PQC Standardization Process: Third Round Candidate Announcement. July 22, 2020. [Electronic resource]. Access mode: https://csrc.nist.gov/News/2020/pqc-third-round-candidate-announcement
9. Daniele Micciancio and Michael Walter. Practical, predictable lattice basis reduction // Marc Fischlin and Jean-Sébastien Coron, editors,EUROCRYPT 2016, Part I, volume9665 ofLNCS, pages 820–849, Vienna, Austria, May 8–12, 2016. Springer, Heidelberg,Germany.
10. Thomas Prest. Sharper bounds in lattice-based cryptography using the Rényi divergence // Takagiand Peyrin [TP17], pages 347–374.
11. Martin R. Albrecht, Shi Bai, and Léo Ducas. A subfield lattice attack on overstretchedNTRU assumptions – cryptanalysis of some FHE and graded encoding schemes // Matthew Robshaw and Jonathan Katz, editors,CRYPTO 2016, Part I, volume 9814 ofLNCS, pages 153–178, Santa Barbara, CA, USA, August 14–18, 2016. Springer, Heidelberg, Germany.
12. Thomas Prest.Gaussian Sampling in Lattice-Based Cryptography // Theses, École NormaleSupérieure, December 2015

Надійшла до редколегії 14.08.2020

Відомості про авторів

Горбенко Іван Дмитрович – д-р техн. наук, професор, Харківський національний університет імені В. Н. Каразіна, професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Україна, e-mail: GorbenkoI@iit.kharkov.ua, ORCID: https://orcid.org/0000-0003-4616-3449

Кандій Сергій Олександрович – Харківський національний університет імені В. Н. Каразіна, студент кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Україна, e-mail: kandy.sergey@yandex.ua

Єсіна Марина Віталіївна – канд. техн. наук, Харківський національний університет імені В. Н. Каразіна, старший викладач кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Україна, e-mail: rinayes20@gmail.com, ORCID: https://orcid.org/0000-0002-1252-7606

Острянська Єлизавета Вадимівна – Харківський національний університет імені В. Н. Каразіна, студент кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Україна, e-mail: antelizza@gmail.com

УДК 004.056.55 **DOI:10.30837/rt.2020.3.202.06**

В.А. КУЛІБАБА

ПРОЦЕСИ ТА МЕТОДИ ВИБОРУ ЗАГАЛЬНОСИСТЕМНИХ ПАРАМЕТРІВ ПЕРСПЕКТИВНОГО АЛГОРИТМУ ЕЛЕКТРОННОГО ПІДПИСУ НА ОСНОВІ АЛГЕБРАЇЧНИХ РЕШІТОК

Вступ

У липні 2020 р. NIST США оголосив фіналістів другого раунду конкурсу постквантових криптографічних примітивів [1], а також оголосив про старт третього раунду. Серед 26 кандидатів другого раунду для проходження у третій раунд у якості основних кандидатів на стандартизацію будо обрано сім механізмів, чотири – асиметричного шифрування та інкапсуляції ключів, а також три електронних підписи.

Аналіз показав, що складність проблеми навчання з помилками точно знайдена лише асимптотично [2], тому важливим моментом є розгляд конкретних значень загальносистемних параметрів алгоритму ЕП Dilithium в контексті відомих атак на алгоритми, що базуються на проблемі LWE.

Серед обраних кандидатів на стандарт ЕП два із трьох алгоритмів засновані на алгебраїчних решітках, це CRYSTALS-DILITHIUM (далі Dilithium) та FALCON.

У звіті NIST зазначено, що Dilithium використовує один і той же модуль і кільце для всіх наборів параметрів і вибірок за допомогою рівномірного розподілу, що призводить до більш простої реалізації, ніж у його основного конкурента, FALCON. Проте, зважаючи, що обидва алгоритми базуються на решітках, скоріше за все, за заявою NIST, стандартизовано буде лише один із них.

У [3, 4, 14] наведено сутність та результати досліджень щодо властивостей та умов застосування кандидата на постквантовий стандарт ЕП Dilithium, що були сформовані та подані на конкурс постквантових криптографічних стандартів NIST. На першому етапі конкурсу [5] були виявлені певні проблемні питання, а на другому етапі уточнені вимоги щодо деяких властивостей алгоритмів, зокрема стійкості до атак сторонніми каналами, щодо яких авторами проєкту стандарту були обґрунтовані та запропоновані удосконалення алгоритму ЕП Dilithium та оптимізована реалізація AVX2.

В звіті [1] NIST явно рекомендував команді Dilithium додати набір параметрів категорії 5, тобто рівня стійкості 512 бітів класичної безпеки та 256 бітів квантової безпеки.

Метою даної статті є:

- попередній аналіз криптографічної стійкості алгоритму ЕП Dilithium від класичних та квантових атак типу «груба сила» та атак на решітках у перехідний та постквантовий періоди;
- обґрунтування та розробка пропозицій щодо генерування та застосування загальносистемних параметрів алгоритму ЕП Dilithium рівня стійкості 512 бітів класичної безпеки та 256 бітів квантової безпеки;
- експериментальний аналіз захищеності ЕП Dilithium від атак сторонніми каналами, зокрема від атаки на основі різної складності множення поліномів.

1. Основні атаки на алгоритми ЕП, що базуються на алгебраїчних решітках

На основі аналізу визначено [6 – 10], що стосовно атак на LWE можна виділити наступні:

1. Атака грубої сили, тобто повного перебору.
2. Атака зустріч посередині.
3. Атака на основі алгоритму Arora-Ge.
4. Атака типу BKW, коли LWE зводиться до SIS атаки.
5. Атака зведення Search-LWE до BDD.

6. Дуальна атака (Decision-LWE зводиться до SIS).

7. Primal attack. Зведення до uSVP атаки пошуку короткого вектору.

8. Диференційна атака.

У роботі [8] доведено, що для вирішення задачі Search-LWE з параметрами n, q, α та з ймовірністю ε потрібно

$$\Theta(2^{n*\log(2*t*\alpha*q+1)+\log(n)+1+\log(m)})$$

операцій у Z_q, де

$$m = \frac{\log(1-\varepsilon) - n\log(2t\alpha q+1)}{\log(2t\alpha)}, t = \omega(\sqrt{\log(n)}) \tag{1}$$

Для вдалої атаки потрібно не менше, ніж $n+m$ пар $(a,c) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$.

Атаки типу зустріч посередині були реально застосовані та позитивно себе показали при криптоаналізі NTRU-подібних систем. В роботі [5] запропоновано ідею застосування цього підходу стосовно криптосистем на основі LWE та доведено, що атака для деякого параметра $t = \omega(\sqrt{\log(n)})$ буде з ненульовою ймовірністю вирішувати задачу Search-LWE за час

$$\Theta((2t\alpha q+1)^{n/2} * (m*n + \log(n/2) + \\ + \log(\log(t\alpha q)) + n/2 * \log(2t\alpha q+1))) \tag{2}$$

Алгоритм Arora-Ge [7] фактично є оптимізацією алгоритму повного перебору та вирішує Search-LWE. Головна ідея алгоритму полягає у побудові системи нелінійних рівнянь, рішенням якої є секретний поліном s. Система вирішується шляхом лінеаризації рівнянь. Було доведено, що, якщо $D_{GA} \in o(n)$ де $D_{GA} = 8(\alpha q)^2 \log(n) + 1$, то рішення системи буде знайдено зі складністю

$$\Theta(2^{w*D_{GA}\log(n/D_{GA})*(\alpha q)*q*\log(q)}). \tag{3}$$

Визначено також, що якщо $\alpha q \approx \sqrt{n}$, то атака буде успішною з ймовірністю

$$\varepsilon = \frac{3}{\log(\log(n))}.$$

У роботі [8] запропоновано вдосконалення алгоритму Arora-Ge, яке потребує $\Theta(2^{2.35wn+1.13n)})$ часу та пам'яті.

Атака на основі алгоритму BKW [9, 10].

Ідея алгоритму BKW полягає у зведенні задачі LWE до задачі SIS у підрешітках меншої розмірності. В алгоритмі розділення на підрешітки здійснюється шляхом розбиття матриці

$$A = \begin{pmatrix} a_1 \\ (\dots) \\ a_m \end{pmatrix} \in \mathbf{Z}_q^{n \times m}$$

на b матриць виду $a_1^{'}, \dots, a_b^{'}$, кожна з яких належить простору $\mathbf{Z}_q^{\eta \times m}$. Далі кожна з матриць $a_1^{'}, \dots, a_b^{'}$ використовується для вирішення SIS у відповідному підпросторі. Основною перевагою такого алгоритму є можливість суттєво розпаралелити обчислення. Для вирішення задачі Decision-LWE алгоритм потребує часу, що можна оцінити таким виразом

$$\Theta((\frac{q^b-1}{2}) * (\frac{\eta(\eta-1)}{2} * (n+1) - \frac{b\eta(\eta-1)}{4}) - \\ - \frac{b}{6}(\frac{q^b-1}{2})((\eta-1)^3 + \frac{3}{2}(\eta-1)^2 + \frac{1}{2}(\eta-1))) \tag{4}$$

Атака зі застосуванням зведення LWE до BDD. Припускається, що дано m пар.

$$(a_i, c_i) = (a_i, \langle a_i, s_i \rangle + e_i) \in \mathbf{Z}_q^n \times \mathbf{Z}_q.$$

Або у іншому вигляді:

$$(A, c) = (A, A^* s + e) \in \mathbf{Z}_q^{m \times n} \times \mathbf{Z}_q^{m \times 1}.$$

Можливо побудувати решітку

$$L = \{Ax \bmod q : x \in \mathbf{Z}_q^m\}.$$

Очевидно, що s є вектором на решітці та є найближчим до вектору $As + e$. Задача знаходження найближчого вектору на решітці до деякого довільного вектору має назву BDD та вирішується за допомогою алгоритму Бабаї [5 – 7]. Алгоритм працює за поліноміальний час, проте знаходить рішення з деякою ймовірністю. Для LWE цю ймовірність можливо оцінити як

$$\prod_{i=0}^{m-1} erf\left(\frac{\|b_i^*\|\sqrt{\pi}}{2\alpha q}\right),$$

де $\|b_i^*\|$ – норми ортогоналізованих за Граммом – Шмідтом векторів базису решітки (тобто стовбців матриці A). Для того щоб ймовірність вирішення BDD була близька до одиниці, потрібно зменшити $\|b_i^*\|$, тобто редукувати базис. Фактор Ерміта δ_0 для редукції отримаємо з співвідношення

$$\|b_0\|_2 = \delta_0^n q^{\frac{1}{n}}$$

$$\|b_i^*\|_2 \approx \delta_0^{-2i+n} * q^{\frac{1}{n}}$$

Алгоритм BKZ 2.0 залежить від натуральних параметрів β і m, що позначають довжину блоку та кількість ітерацій відповідно, і дозволяє будувати редукований за Коркіним – Золотарьовим [8] базис повної решітки вимірності n за $2^{E(\beta, m, n)}$ операцій, де

$$E(\beta, m, n) = 0,000784314\,\beta^2 + \\ +0,366078\,\beta + \log((n)m) + 0,875. \qquad (5)$$

Атаки на дуальній решітці засобом зведення LWE до SIS. Будується спочатку решітка $L = \{x \in \mathbf{Z}_q^m \mid A^* x = 0 \bmod q\}$. Задача SIS полягає у знаходженні такого найменшого $x \in \mathbf{Z}^n$, щоб $A^* x = 0$. Припустимо, що такий вектор знайдений, тоді можна вирішити задачу Decision-LWE. Нехай дано m пар

$$(A, c) = (A, A^* s + e) \in \mathbf{Z}_q^{m \times n} \times \mathbf{Z}_q^{m \times 1}$$

Обчислюється скалярний добуток $\langle x, c \rangle$:

$$\langle x, c \rangle = x^* a^* s + x^* e = 0^* s + x^* e = x^* e = \langle x, e \rangle$$

Оскільки вектор $x \in \mathbf{Z}^n$ відомий, то з цієї рівності можна знайти значення вектору помилок e, проте простір помилок залишається досить великим. В роботі [9] доведено, що якщо вектор x має норму

$$\|x\|_2 = \frac{1}{\alpha} * \sqrt{\frac{\ln(\frac{1}{\varepsilon})}{\pi}},$$

то з ймовірністю близькою до 1 можливо вирішити задачу, при цьому знадобиться $\frac{1}{\varepsilon^2}$ запусків вирішувача SIS. Вирішувач знаходить достатньо малий вектор на решітці, тобто вирішує задачу SVP. У роботі [6] було показано, що при цьому фактор Ерміта δ_0 має бути не більше

$$\log \delta_0 = \frac{\log^2(\frac{1}{\alpha}\sqrt{\frac{\ln(\frac{1}{\varepsilon})}{\pi}})}{4*n\log q}.. \tag{6}$$

Подальша оцінка атаки потребує вибрати певний вирішувач, наприклад алгоритм BKZ, та проведення експериментальних досліджень з різними параметрами.

У Primal Attack припускають, що решітка містить вектор s. Сутність атаки полягає у тому, щоб побудувати таку решітку, на якій буде лежати вектор $(s,e,1)$ і він буде найменшим унікальним вектором, тобто, вона зводиться до задачі uSVP [4]. Такою решіткою буде

$$\Lambda = \{x \in \mathbf{Z}^{m+n+1} : (A \mid I_m \mid -c) * x = 0 \bmod q\}.$$

Для пошуку вектору можливо скористатися вирішувачем BKZ 2.0 і редукувати решітку, як наслідок b_0 буде рішенням, що необхідно знайти. Далі, для вдалої редукції оцінити фактор Ерміта можливо виразом [6]

$$\log \delta_0 = \frac{1}{4n^2 \ln^2 q}\left(W\left((-2n\ln q) * (\sqrt{n\log q}) * \frac{(\tau\alpha)^2}{2\pi}\right)\right)^2. \tag{7}$$

Атаки на LWE можливо розділити на два великі класи – атаки типу груба сила та атаки, що базуються на редукції решіток. До першого класу належать атаки зустріч посередині, повного перебору та Arora-Ge. Атаки на решітках полягають у зведенні проблеми LWE до достатньо відомих проблем (задач) на решітках: зведення LWE до BDD, зведення LWE до SIS, зведення LWE до uSVP. Кожен з цих підкласів задач зводиться до задачі пошуку достатньо малого вектору на решітці, для чого використовується алгоритм BKZ та його варіації. Проте, точні оцінки для BKZ та його варіацій невідомі, або ще не опубліковані. Це є проблемним питанням при оцінці криптографічної стійкості систем, що базуються на проблемі LWE та темою для подальших досліджень.

2. Загальносистемні параметри алгоритму ЕП Dilithium, що впливають на стійкість

Як і в більшості алгоритмів електронного підпису, алгоритм Dilithium має набір загальносистемних параметрів, частина з яких є постійною. В табл. 1 наведено постійні параметри та їх значення, що пропонуються до застосування авторами проєкту стандарту.

Таблиця 1

Постійні параметри алгоритму Dilithium, запропоновані авторами

Позначення	Сутність
N=256	Степінь поліному
q=8380417	Усі обчислення виконуються модулем q
SEEDBYTES=32	Довжина seed (байт)
d=14	Параметр, який використовується при виділенні старшої і молодшої частини
BITS_IN_BYTE=8	Кількість бітів в байті
HASHBYTES=64	Довжина початкового значення розгортання ключа

Параметри, які можуть змінюватися, задано в табл. 2 для всіх чотирьох режимів роботи, що наводяться авторами стандарту.

Таблиця 2

Параметри, що можуть змінюватись в ЦП Dilithium

Рівень стійкості	k	l	H	η	β	ω
1	3	2	7	4	375	64
2	4	3	6	4	325	80
3	5	4	5	4	275	96
4	6	5	3	3	175	120

Довжина блоку залежить тільки від значень *k, l,* η, *n, q* і розраховується окремо для кожної з двох задач (SIS та LWE) та двох атак (прямої та дуальної) на кожну з них згідно з методикою, наведеною в [2,3] Для кожної з них зазначені параметри обчислюються за формулами

$$\text{Best Known Classical bit-cost} = 0{,}292b \qquad (8)$$
$$\text{Best Known Quantum bit-cost} = 0{,}265b$$

де b є довжиною блоку (BKZ bock-size b для зламу SIS або LWE [1]). В ролі кінцевої оцінки стійкості використовується найменше з двох значень, обчислених для b, що є довжиною блоку для задачі SIS та задачі LWE відповідно.

У [8 – 13] наводиться детальний аналіз алгоритмів оцінювання довжини блоку b для задачі LWE для прямої і дуальної атаки. Як доведено, достатньою умовою стійкості на рівні λ бітів відносно прямої атаки є нерівність $0{,}292b_*^{(1)} \geq \lambda$, яка при $\lambda = 256$ рівносильно нерівності $b_*^{(1)} \geq 877$, а для дуальної атаки умовою стійкості на рівні λ бітів є нерівність

$$0{,}292b_*^{(2)} + 2c \geq \lambda. \qquad (9)$$

В загальному випадку, пряма атака потребує менше часу в порівнянні з дуальною.

Пояснення кожного параметру наведено в табл. 3.

Таблиця 3

Параметри, що можуть змінюватися та впливають на стійкість алгоритму Dilithium

Параметр	Визначення
q	Більший модуль перетворення коефіцієнтів поліномів
k	Кількість поліномів, визначають кількість рядків матриці A
l	Кількість поліномів, визначають кількість стовбців матриці A
η	Значення коефіцієнтів секретного полінома s, які знаходяться в інтервалі $[-\eta, \eta]$, основа алфавіту ключових даних
(γ_1, γ_2)	Обмеження на максимальні значення коефіцієнтів під час вироблення підпису.
h	Елемент матриці h [i][j] встановлюється в 1, якщо tmp [i][j]$_{high}$ не співпадає з (ct$_{low}$+tmp) [i][j]$_{high}$ і 0, якщо вони співпадають
ω	Цей параметр визначається як верхній поріг для числа одиниць у векторі *h*, який обчислюється на кроці 21 алгоритму формування підпису. Впливає на ймовірність повтору циклу(швидкодію алгоритму підпису) та на розмір підпису. Знаходиться з практичних міркувань.
β	Параметр β вибирається, виходячи з такої умови: ймовірність $p = \mathbf{P}\{\| cs_2 \|_\infty \geq \beta\}$ де s_2 є випадковим вектором з рівномірним розподілом на множині S_η^k, а $c \in B_h$, є достатньо малим числом. Також впливає на максимальне значення коефіцієнтів, проте впливає не стільки на стійкість, скільки на розмір підпису.
d	Цей параметр визначається як найбільше натуральне *d*, що задовольняє умові $2^{d-1}h + 1 \leq 2\gamma_2$.

3. Параметри алгоритму ЕП Dilithium для рівнів 512/256 бітів класичної та квантової стійкості

Питання генерування параметрів більш високого рівня стійкості 512 бітів, є актуальним для алгоритму ЕП Dilithium, так як авторами кандидату не будо запропоновано загальносистемних параметрів для рівнів безпеки вище, ніж 256 бітів, а лише дані загальні рекомендації щодо їх генерування. NIST США для третього раунду конкурсу рекомендував авторам надати набір параметрів 5-го рівня, що, враховуючи ряд проблемних питань в описі відповідних алгоритмів, є актуальною задачею досліджень.

Попередні оцінки стійкості наведено в підрозд. 3 та в [15] для довжини блоку *b* BKZ у вигляді нижніх оцінок. Також для параметра *n* необхідно використовувати $n = 256$, якщо $\lambda = 256$; або $n = 512$, якщо $\lambda \geq 256$

В проєкті стандарту[4] авторами наводяться параметри тільки до 4-го рівня стійкості NIST (принаймні так важко зламати, як AES256 (вичерпний перебір ключів). Проте існує задача генерування параметрів більш високого рівня стійкості 512 бітів класичної та 256 бітів квантової стійкості.

Алгоритм обчислення параметрів рівня стійкості 512/256:

1. Нехай $\lambda \in 512$, $\eta = 2$
2. Обрати значення N. Так як $\lambda \geq 256$, то $N = 512$
3. $\gamma_1 = (q-1)/16 = 523776$, $\gamma_2 = \gamma_1/2 = 261888$
4. Встановити початкові значення за замовчанням $k = 2$ та $l = 1$
5. Обчислити $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ – стійкість до Primal Attack, Dual Attack, стійкість до SIS з $\zeta_1 = \max(\gamma_1 - \beta, 2\gamma_2 + 1 + 2^{d-1}h)$, стійкість до SIS з $\zeta_2 = \max(2(\gamma_2 - \beta), 4\gamma_2 + 2)$ згідно [4 – 6].
6. Якщо

$$\lambda_1 < 512 \square \lambda_2 < 512 \square \lambda_3 < 512 \square \lambda_4 < 512 \tag{10}$$

тобто стійкість до будь-якої з атак менша за необхідне значення $\lambda = 512$, то збільшити *k* та *l,* і повернутися до кроку 5

7. Обчислити h як найбільше ціле, для якого виконується нерівність

$$2^h \binom{n}{h} \geq 2^{\lambda}$$

$$2^h \binom{n}{h} \geq 2^{512} \tag{11}$$

$$h = 118$$

8. Обчислити d як найбільше ціле, для якого виконується нерівність

$$2^{d-1}h + 1 \leq 2\gamma_2$$

$$2^{d-1} \square 118 + 1 \leq 2 \square 261888 \tag{12}$$

$$d = 13$$

9. Обчислити $w = \lfloor 0.08nk \rfloor = 0.08 \square 9 \square 512 = 368.64 = 368$

Зведені значення параметрів для $\lambda = 512$ наведено в табл. 4.

В табл. 5 наведено значення загальносистемних параметрів рівня стійкості 512/256 при $k = 9$ та $l = 8$.

Таблиця 4

Значення загальносистемних параметрів для рівня стійкості 512/256

Стійкість	N	γ_1	γ_2	η	β	d	h	ω
$\lambda = 512$	512	523776	261888	2	76	13	118	368

4. Захищеність алгоритму ЕП від атак сторонніми каналами

В процесі проведення конкурсу на другому етапі була висунута особлива вимога до захищеності кандидату на стандарт ЕП від атак сторонніми каналами.

Дослідження стосовно алгоритму ЕП Dilithium було проведено за такими параметрами [15]:

$$\text{BKZ bock-size to break SIS} = 475;$$
$$\text{BKZ bock-size to break LWE} = 485;$$
$$k = 5; l = 4; \eta = 5; \zeta = 4; \beta = 275; \omega = 96 .$$

Для проведення експерименту було згенеровано 10000 ключів та виконано 10000 підписів. Результат залежності часу підпису від номеру ключа наведено на рис. 1, Для 10000 ключів максимальне відхилення від нормалізованого середнього (дисперсія) усіх вимірів часу підпису повинно знаходитися в інтервалі $-5.19676 <= d <= 6.62797(\%)$, щоб вважати, що час підпису практично не залежить від ключа. Номери ключів, для яких було отримано мінімальне та максимальне значення при повтореннях вимірів не повинні співпадати.

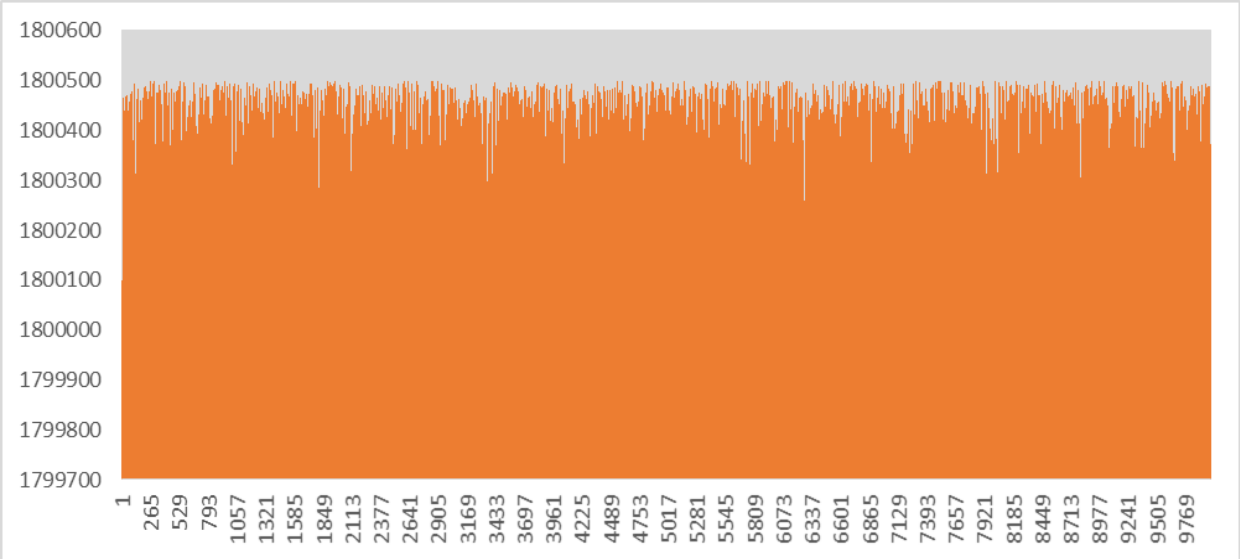


Рис. 1. Залежність часу підпису (у тактах процесору) від номеру ключа

Значення дисперсії $d \approx 2\%$, що свідчить про практично (враховуючи можливі відхилення при роботі операційної системи) статистичну незалежність часу підпису від ключа, що є важливим з точки зору захищеності від атак сторонніми каналами на основі різної складності множення поліномів тощо.

Висновки

1. Другий етап конкурсу NIST PQC завершився прийняттям для подальшого розгляду трьох основних алгоритмів електронного підпису [1]: Rainbow, CRYSTALUS-DILITHIUM та FALCON. Причому, з останніх двох скоріше за все буде обрано один, так як вони обидва ґрунтуються на проблемі LWE.

2. Алгоритм ЕП Dilithium з параметрами, наведеними в [4, 5], забезпечує тільки 1-4 рівні безпеки за класифікацією NIST. NIST ставить питання про генерацію параметрів рівня стійкості 5 та вище, що є перспективним напрямком подальших досліджень в контексті впливу параметрів більш високих рівнів стійкості на техніко-експлуатаційні характеристики, такі як швидкодія.

3. Генерування параметрів для більш високих рівнів безпеки є проблемним питанням через те, що не всі алгоритми детально описані і потребують подальших досліджень.

4. В алгоритмі Dilithium при генеруванні загальних параметрів використовуються засоби з рівноймовірним розподілом, що було доведено в [5, 11 – 13], а також перевірено практично. Також такі операції, як множення поліномів та їх округлення реалізовані з однаковою часо-

вою складністю. Це забезпечує захист від атак сторонніми каналами на основі різної складності множення поліномів тощо.

5. Аналіз показав, що складність проблеми навчання з помилками знайдена лише асимптотично. Так, доведено [2], що за певних умов складність вирішення LWE в просторі розмірності n становить щонайменше $2^{O(n)}$

6. На основі аналізу визначено [9 – 13], що стосовно атак на LWE можливо виділити та необхідно розглядати такі атаки як: атака грубої сили, тобто повного перебору; традиційна атака зустріч посередині; атака на основі алгоритму Arora-Ge; BKW, коли LWE зводиться до SIS атаки; primal attack (Search-LWE зводиться до BDD атаки); Dual attack (Decision-LWE зводиться до SIS); зведення до uSVP атаки пошуку короткого вектора

7. Як видно з табл. 3, нижня оцінка довжини блоку, потрібної для успішної реалізації дуальної атаки, є помітно вище в порівнянні зі значенням цього параметру для прямої атаки.

Знаходження довжини блоку b за параметрами k, l, η – найбільш нетривіальна частина алгоритму вибору параметрів. Довжина блоку залежить від значень k, l, η, n, q і розраховується для кожної з двох задач (SIS та LWE) та двох можливих атак (прямої та дуальної) на кожну з них згідно з методикою, наведеною в [8, 9] (таким чином, для обчислення b слід застосувати чотири різні алгоритми та взяти найменше з отриманих значень – п. 6 алгоритму вибору параметрів у підрозд. 3).

Список літератури:

1. NISTIR 8309 / Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper,Quynh Dang,John Kelsey,Yi-Kai Liu,Carl Miller,Dustin Moody,Rene Peralta,Ray Perlner,Angela Robinson,Daniel Smith-Tone. Access mode: http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf.

2. *Gottfried Herold, Elena Kirshanova, and Alexander May*. On the asymptotic complexity of solving LWE // Designs, Codes and Cryptography, Jan 2017.

3. *Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler and Damien Stehlé* CRYSTALS-Dilithium: Algorithm Specifications and Supporting Documentation. Access mode: https://pq-crystals.org/dilithium/data/dilithium-specification.pdf.

4. Post-Quantum Cryptography. Round 2 Submissions. Electronic resource. Access mode: https://csrc.nist.gov/Projects/post-quantum-cryptography/round-2-submissions.

5. *Lyubachevsky V., Ducas L., Kiltz E.* et all. CRYSTALS–Dilithium. Techn. rep. NIST (2017). Electronic resource. Access mode: https://crc.nist.gov./projects/post-quantum-cryptogtraphy/ round-1-submissions.

6. *Rachel Player*. Parameter selection in lattice-based cryptography. Access mode: https://pure.royalholloway.ac.uk/portal/files/29983580/2018playerrphd.pdf.

7. *Sanjeev Arora and Rong Ge*. New algorithms for learning in presence of errors. In Luca Aceto, Monika Henzinger, and Jiri Sgall, editors, ICALP 2011, Part I, volume 6755 of LNCS, pages 403–415. Springer, Heidelberg, July 2011.

8. *Martin R. Albrecht, Carlos Cid, Jean-Charles Faugère, and Ludovic Perret*. Algebraic algorithms for LWE. Cryptology ePrint Archive, Report 2014/1018, 2014. Access mode: http://eprint.iacr.org/2014/1018.

9. *Martin R. Albrecht, Carlos Cid, Jean-Charles Faugère, Robert Fitzpatrick, and Ludovic Perret*. On the complexity of the BKW algorithm on LWE // Designs, Codes and Cryptography, 74:325–354, 2015.

10. *Martin R. Albrecht, Jean-Charles Faugère, Robert Fitzpatrick, and Ludovic Perret*. Lazy modulus switching for the BKW algorithm on LWE // Hugo Krawczyk, editor, PKC 2014, volume 8383 of LNCS, pages 429–445. Springer, Heidelberg, March 2014.

11. *Vadim Lyubashevsky*. Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures // ASIACRYPT, pages 598–616, 2009.

12. *Vadim Lyubashevsky*. Lattice signatures without trapdoors. In EUROCRYPT, pages 738–755, 2012.

13. *Tim Güneysu, Vadim Lyubashevsky, and Thomas Pöppelmann*. Practical lattice-based cryptography: A signature scheme for embedded systems. In CHES, pages 530–547, 2012.

14. *Горбенко І. Д.*, Постквантова криптографія та механізми її реалізації / І. Д. Горбенко, О. О. Кузнецов, О. В. Потій, Ю. І. Горбенко, Р. С., Ганзя, В. А. Пономар // Радиотехника. 2017. Вип. 186. С. 32–52.

15. *Кулібаба В.А.*, Перспективні методи та системи критптографічного захисту інформації / О.М. Олексійчук, В.А. Кулібаба, М.В. Єсіна, С. О. Кандій, Є.В. Острянська, І.Д. Горбенко // Радіотехніка. 2020. Вип. 200. С. 5-13.

Надійшла до редколегії 05.09.2020

Відомості про авторів:

Кулібаба Владислав Андрійович – Харківський національний університет імені В.Н. Каразіна, аспірант кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Україна, E-mail: vlad.kulibaba1994@gmail.com.

УДК 004.056.55 **DOI:10.30837/rt.2020.3.202.07**

Ю.І. ГОРБЕНКО, канд. техн. наук, М.В. ЄСІНА, канд. техн. наук,
В.В. ОНОПРІЄНКО, канд. техн. наук, Г.А. МАЛЄЄВА

МОДЕЛІ ЗАГРОЗ ЩОДО АСИМЕТРИЧНИХ КРИПТОПЕРЕТВОРЕНЬ ПЕРСПЕКТИВНОГО ЕЛЕКТРОННОГО ПІДПИСУ

Вступ

Модель загроз ЕП (далі – Модель загроз) повинна бути документом, яким закріплено найбільш повний перелік загроз щодо існуючих та перспективних ЕП, що може застосовуватись в постквантовий період. Відповідно до Законів України "Про захист інформації в інформаційно-телекомунікаційних системах", "Про електронні довірчі послуги" та "Про захист персональних даних", інформація в основних інформаційних ресурсах поділяється на відкриту і конфіденційну. Інформація у підтримуючих інформаційних ресурсах є технологічною інформацією [1 – 4].

При застосуванні ЕП, незалежно від видів додатків, використовуються асиметричні пари ключів, для кожної пари особистий та відкритий [1, 3 – 5]. В подальшому при реальному застосуванні ЕП відкритий ключ, як правило, є сертифікатом відкритого ключа та є доступним усім користувачам інфраструктури відкритого ключа (ІВК).

Оскільки сертифікат відкритого ключа є відкритою інформацією, то під час обробки згідно з [2, 5] він повинен зберігати цілісність, справжність, доступність, неспростовність та бути захищеним від несанкціонованих дій, які можуть привести до випадкової чи умисної модифікації, нав’язування хибного чи знищення. Усім користувачам, наприклад ІВК, повинен бути забезпечений доступ до ознайомлення з відкритою інформацією, в даному випадку у вигляді сертифіката відкритого ключа [1, 3, 4].

Під час обробки (застосування) конфіденційної інформації, в нашому випадку особистого ключа, вона повинна зберігати цілісність, справжність, доступність, неспростовність та бути захищеною від несанкціонованих дій, а також практично повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання та поширення. Тобто, безумовно повинна бути забезпечена конфіденційність особистого ключа кожного користувача. Також, згідно з [1 – 3] технологічна інформація повинна бути відома тільки авторизованим на це особам та зберігати цілісність.

Таким чином, в усіх відомих додатках, у яких використовується ЕП, стосовно відкритого ключа ЕП повинна бути можливість забезпечення його цілісності, справжності, доступності, неспростовності та захист від несанкціонованих дій, які можуть привести до випадкової чи умисної модифікації, нав’язування хибного чи знищення. Стосовно особистого ключа повинна забезпечуватись його цілісність, справжність, доступність, неспростовність та захист від несанкціонованих дій, а також його захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання та поширення, тобто конфіденційність.

Тобто як існуючі ЕП, так і перспективні ЕП повинні дозволяти гарантовано захищати їх асиметричні пари ключів у відповідності із вказаними вище вимогами, незалежно від їх подання при використанні в апаратному, програмному чи апаратно-програмному вигляді. Причому, незалежно від виду їх обробки, реалізація загроз, що спрямовані на вказані ресурси, може призводити до порушення вимог безпеки первинних інформаційних ресурсів, вплинути на інше програмне забезпечення (ПЗ), що підписується, та, в окремих випадках, на функціонування апаратних ресурсів.

Метою цієї статі є обґрунтування та розробка пропозицій щодо побудування моделі загроз стосовно асиметричних криптоперетворень типу перспективний ЕП, що може застосовуватись в постквантовий період.

Загальні загрози щодо перспективних ЕП та їх оцінка

На наш погляд повний перелік можливих загроз безпеці застосування існуючих та перспективних ЕП, що сформований з числа загроз, наявних у IT-Grundschutz Catalogues з урахуванням апаратних, програмних та апаратно-програмних ресурсів, технологій обробки даних та механізмів криптографічного захисту при застосуванні ЕП, в тому числі з урахуванням вимог та умов синтезу перспективних ЕП та застосуванні ЕП в постквантовий період, може бути прийнятий таким, що наведений нижче.

Загрози, пов'язані з апаратним, програмним забезпеченням та технологіями обробки, що використовуються в ІВК та системі Блокчейн (БЧ), мають розглядатись додатково [4, 8].

У цілому за результатами аналізу щодо методів синтезу та застосування відомих та перспективних ЕП визначено такі загрози:

- закладення вразливостей в алгоритми синтезу та застосування ЕП;
- застосування криптоаналітичних систем щодо аналізу чутливих даних ЕП;
- викрадення чутливих даних ЕП за допомогою мобільних носіїв інформації;
- викрадення пристроїв, носіїв чутливої інформації та документів з чутливими даними ЕП;
- витік чутливих даних ЕП каналами побічних електромагнітних випромінювань і наведень;
- відмова від дій проти загроз щодо чутливих даних ЕП;
- відмова криптомодулю з чутливими даними ЕП;
- відсутнє або недостатнє оповіщення при виникненні інцидентів компрометації чутливих даних ЕП;
- відсутність прозорості для особи, що зацікавлена та уповноважена контролювати захист чутливих даних ЕП;
- відсутня або неповна документація щодо чутливих даних ЕП;
- втрата цілісності інформації, яка повинна бути захищена (чутливих даних та програмного забезпечення ЕП);
- старіння чутливих даних та криптографічних методів ЕП;
- зловживання повноваженнями щодо чутливих даних ЕП;
- зловживання правами адміністратора щодо чутливих даних ЕП;
- зловживання правами користувачів щодо чутливих даних ЕП;
- компрометація асиметричних пар криптографічних ключів ЕП;
- крадіжка чутливих даних ЕП;
- не виявлені інциденти інформаційної безпеки щодо чутливих даних ЕП;
- невірне тлумачення події інформаційної безпеки щодо чутливих даних ЕП;
- недооцінення актуальності виправлень і змін щодо чутливих даних ЕП;
- неналежне зберігання носіїв інформації з чутливими даними в разі виникнення надзвичайної ситуації ЕП;
- неправильне використання криптомодулів з чутливими даними ЕП;
- несанкціоноване використання криптомодулів ЕП;
- несанкціоноване використання прав адміністраторів та користувачів ЕП;
- нестійкі криптографічні алгоритми ЕП;
- неякісна або відсутня автентифікація щодо чутливих даних ЕП;
- підробні сертифікати відкритих ключів ЕП;
- порушення законів або правил щодо чутливих даних при синтезі та застосуванні ЕП;
- проблеми при автоматизації поширення виправлень і змін щодо ЕП;
- розголошення чутливої інформації щодо синтезу та застосування ЕП;
- систематичний перебір паролів доступу до ЕП;
- троянський кінь щодо чутливих даних ЕП при синтезі та застосуванні ЕП;
- уразливості або помилки ПЗ щодо ЕП;

- атака "Людина посередині";
- атака Clickjacking (буквально – натискання);
- шкідливе програмне забезпечення при синтезі та застосуванні ЕП.

Безумовно, що щодо обґрунтованої та вибраної на основі IT-Grundschutz Catalogues бази Германії моделі загроз, при синтезі та застосуванні існуючих стандартизованих та перспективних ЕП, повинне бути зроблено перекриття названих загроз з необхідною якістю. Для цього, у залежності від механізмів та засобів, що застосовуються для протидії, повинні бути розроблені відповідні нормативно-правові документи.

Моделі загроз щодо ЕП при застосуванні методів та засобів класичного криптоаналізу

Детально загрози щодо застосування класичного криптоаналізу при синтезі та застосуванні ЕП повинні бути визначеними безумовно. Їх перекриття повинне бути зроблене на всіх етапах синтезу та застосування перспективних ЕП. Вказані загрози з точки зору застосування математичних методів синтезу та застосування перспективних методів ЕП залежить від математичних методів, що застосовуються, та умов їх функціонування. Детально ці особливості розглянуті в [3-5], наприклад, для математичних методів, що визначені в якості кандидатів на постквантові стандарти ЕП.

Основними загрозами (методами) класичного криптоаналізу, що повинні бути врахованими, є наступні:

- атаки типу «повне розкриття», загальною можливістю яких є компрометація чутливих параметрів та ключів при відомих відкритих даних;
- атаки «повне розкриття» на основі підписаних даних, призначенням яких є спроба компрометації ключових даних при наявності множини підписаних даних;
- атаки типу «екзистенційна підробка», що можуть бути застосованими за наявності слабкостей у функції гешування, яка використовується при виробленні ЕП;
- атак типу «селективна підробка», яка полягає в тому, що при невідомому особистому ключі для заздалегідь обраних даних можна обчислити ЕП;
- атаки щодо ЕП на «зв'язаних» ключах, особливістю яких є те, що при генеруванні асиметричних пар ключів закладається вразливість;
- атаки на програмну реалізацію ЕП, особливістю яких є те, що при генеруванні асиметричних пар ключів закладається вразливість тощо.

Моделі загроз при синтезі та застосуванні ЕП сторонніми каналами

Загрози (атаки) сторонніми каналами є виділеним класом атак, основною особливістю яких є спрямованість на вразливості практичної реалізації криптосистем, тобто, на відміну від теоретичного криптоаналізу. Загрозливістю такого класу атак над традиційними є менша потужність та більш висока дієвість [4].

Атаки сторонніми каналами націлені на використання інформації про фізичні процеси у технічних пристроях, в тому числі на основі таких:

1) Час виконання операцій вироблення та перевірки ЕП та управління ключами;
2) Спожита енергія (потужність) під час вироблення та перевірки ЕП та управління ключами;
3) Акустичні звуки та сигнали під час вироблення та перевірки ЕП та управління ключами;
4) Електромагнітні випромінювання під час синтезу та застосування ЕП тощо;

Основними видами атак сторонніми каналами є такі [4]:

- атаки за часом (timing attack) – найбільш відомий вид атак стосовно ЕП;
- атаки зондування (probing attack) – один з різновидів простої пасивної атаки;
- атаки на основі помилок обчислень (fault-induction attack) – різновид активної атаки;

Загрози сторонніми каналами можуть бути реалізовані такими методами:

- впливи змінним магнітним полем або лазерними променями;
- порушення контактів у засобі криптографічного перетворення або зміна його тактової частоти;
- зміна напруги живлення системи (сильно перевищені значення норм можуть призвести до помилок на деяких етапах);
- переміщення пристрою до локації з сильним електромагнітним полем;
- підвищення температури усієї системи або ж лише криптографічної частини тощо.

Атаки сторонніми каналами є надзвичайно небезпечними, якщо їх не перекривати. Концепція цих атак існує вже доволі тривалий час, але реалізація захищеності від них вимагає знань не лише у сфері криптографії, а й у сферах технічного характеру. Тому переважна більшість перспективних ЕП розрахована на використання у пристроях, які не можуть захистити від сторонніх атак, бо не мають відповідних програмних рішень щодо захисту від витоку сторонніми каналами.

Моделі загроз при синтезі та застосуванні ЕП при використанні квантових комп'ютерів та оцінки при їх застосуванні

Основними загрозами (атаками) із застосуванням квантових математичних методів, які можуть бути реалізовані на квантовому комп'ютері (звичайно, якщо він буде побудований), є такі [4, 6 – 8, 10 – 12]:

- квантовий алгоритм факторизації Шора;
- квантовий алгоритм Гровера;
- квантовий алгоритм Шора вирішення дискретного логарифму в полі;
- квантовий алгоритм Шора вирішення дискретного логарифму в групі точок еліптичної кривої;
- квантовий алгоритм криптоаналізу для перетворень в фактор кільці тощо.

Порівняльний аналіз складності факторизації для класичного та квантового алгоритмів наведено у табл. 1 [4].

Таблиця 1

Порівняльний аналіз класичного та квантового алгоритмів факторизації (RSA)

Розмір модуля N, бітів	Кількість необхідних кубітів $2n$	Складність квантового алгоритму $4n^3$	Складність класичного алгоритму
512	1024	$0.54 \cdot 10^9$	$1.6 \cdot 10^{19}$
3072	6144	$12 \cdot 10^{10}$	$5 \cdot 10^{41}$
15360	30720	$1.5 \cdot 10^{13}$	$9.2 \cdot 10^{80}$

Порівняльний аналіз складності алгоритму дискретного логарифмування в скінченому полі на основі решета числового поля та алгоритму Шора наведено в табл. 2.

Таблиця 2

Порівняльний аналіз класичного і квантового алгоритму дискретного логарифмування в скінченому полі

Розмір модуля перетворення (бітів)	Кількість необхідних кубітів $\approx 3n$	Час квантового алгоритму $\approx n^3$	Час класичного алгоритму
1024	3072	$0.1 \cdot 10^{10}$	$3.3 \cdot 10^{20}$
3072	9216	$2.9 \cdot 10^{10}$	$1.4 \cdot 10^{31}$
15360	46080	$3.6 \cdot 10^{12}$	$5.9 \cdot 10^{56}$

Деякі оцінки та результати порівняльного аналізу класичних алгоритмів та квантового алгоритму Шора наведений у табл. 3.

Таблиця 3

Порівняльний аналіз складності класичного і квантового алгоритмів дискретного логарифмування групі точок еліптичної кривої (ECC)

Алгоритм розв'язку дискретного логарифмічного рівняння			
Розмір порядку базової точки, бітів	Кількість необхідних кубітів $f(n) = 7n + 4\log_2 n + 10$	Складність квантового алгоритму $360n^3$	Складність класичного алгоритму
163	1210	$1.6 \cdot 10^9$	$3.4 \cdot 10^{24}$
256	1834	$6 \cdot 10^9$	$3.4 \cdot 10^{38}$
571	4016	$6.7 \cdot 10^{10}$	$8.8 \cdot 10^{85}$
1024	7218	$3.8 \cdot 10^{11}$	$1.3 \cdot 10^{154}$

Аналіз даних табл. 1 – 3 дозволяє зробити висновок, що збільшення розміру порядку базової точки при криптоаналізі з використанням квантового алгоритму не дає суттєвого збільшення криптографічної стійкості криптографічної системи на еліптичних кривих. Також видно, що при збільшенні модуля складність дискретного логарифмування класичними методами в групі точок еліптичної кривої зі збільшенням порядку базової точки збільшується суттєво. Але потрібно взяти до уваги, що реалізація квантового алгоритму пов'язана зі застосуванням регістрів з великою кількістю кубітів, яка необхідна для проведення квантової атаки. Наприклад, для базової точки з порядком 2^{571} необхідно використовувати реєстр з довжиною 4016 кубітів. Вважається, що така велика кількість кубітів, ще певний час буде не реалізованою.

Моделі загроз при синтезі та застосуванні ЕП постквантового періоду

У залежності від математичних методів, що застосовуються для синтезу та застосування ЕП, можуть застосовуватись різні методи, системи та засоби.

Розглянемо загрози (атаки) на прикладі проблеми стійкості криптоперетворень на основі навчання з помилками (LWE) [6, 7].

Наразі в постквантовій криптології актуальними є завданнями забезпечення криптографічної стійкості щодо квантових атак.

Стосовно атак на LWE можливо виділити та необхідно розглядати наступні атаки (загрози) [6 – 8, 12]:

1. Атака грубої сили, тобто повного перебору.
2. Традиційної атаки зустріч посередині.
3. Атака на основі алгоритму Arora-Ge.
4. BKW, коли LWE зводиться до SIS атаки.
5. Primal attack (Search-LWE зводиться до BDD атаки).
6. Dual attack (Decision-LWE зводиться до SIS).
7. Зведення до uSVP атаки пошуку короткого вектора.
8. Диференційні атаки.

У цілому атаки на LWE можливо розділити на два великі класи – атаки, що ґрунтуються на переборі, та атаки, що ґрунтуються на редукції решіток. До першого класу належать атаки повного перебору, зустріч посередині та Arora-Ge. Підхід, що використаний в атаці Arora-Ge, є цікавим та перспективним, але він поки що поступається атакам на решітках.

Попередній аналіз дозволяє зробити висновок, що сучасні варіанти механізмів LWE ґрунтуються на поліноміальних кільцях, зокрема на $R_q = \mathbf{Z}_q[X]/(x^{2^n}+1)$. Властивості полі-

номів кільця дозволяють довести ряд теоретичних тверджень щодо стійкості криптосистеми і розробляти ефективні програмні реалізації. Проте, такі кільця мають нетривіальні підполя, що теоретично може використовуватися для криптоаналізу, проте на практиці атак, що застосовують ці додаткові структури, не було знайдено, або ці атаки знаходяться в незавершеному вигляді досліджень.

Проблеми криптоаналізу RLWE та MLWE по суті зводяться до LWE проблеми. Таке зведення можливо для $R_q = \mathbf{Z}_q[X]/(x^{2^n}+1)$, оскільки доведено, що RLWE є не менш стійким, ніж LWE. Проте, при такому підході внутрішня структура кільця ігнорується.

Атаки на решітках, що полягають у зведенні проблеми LWE, відносяться до достатньо вивчених теоретичних проблем в теорії решіток. Існують три основні підходи: зведення LWE до BDD, зведення LWE до SIS, зведення LWE до uSVP. Кожен з цих підходів в кінцевому випадку зводиться до задачі пошуку достатньо малого вектора на решітці, для чого використовується алгоритм BKZ та його варіації.

Точні оцінки для BKZ та його варіацій невідомі. При практичній оцінці використовується ряд евристичних підходів та екстраполяція результатів, що отримані на решітках меншої розмірності. Це становить основну проблему при оцінці криптостійкості систем подібних Dilithium, оскільки немає гарантії, що не з'явиться кращого способу редукції решіток, або оцінка виявиться недопустимо неточною.

Висновки

1. Модель загроз щодо криптоперетворення ЕП повинна бути документом, яким закріплено найбільш повний перелік загроз щодо існуючих та перспективних ЕП.
2. Відповідно до Законів України інформація у основних інформаційних ресурсах поділяється на відкриту і конфіденційну. Інформація у підтримуючих інформаційних ресурсах є технологічною інформацією.
3. При застосуванні ЕП, незалежно від видів додатків, використовуються асиметричні пари ключів, для кожної пари особистий та відкритий. В подальшому при реальному застосуванні ЕП відкритий ключ, як правило, є сертифікатом відкритого ключа та є доступним усім користувачам ІВК.
4. Стосовно відкритого ключа ЕП повинна бути можливість забезпечення його цілісності, справжності, доступності, неспростовності та захист від несанкціонованих дій, які можуть привести до випадкової чи умисної модифікації, нав'язування хибного чи знищення.
5. Стосовно особистого ключа повинна забезпечуватись його цілісність, справжність, доступність, неспростовність та захист від несанкціонованих дій, а також його захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання та поширення, тобто конфіденційність.
6. Перелік можливих загроз безпеці застосування існуючих та перспективних ЕП сформований з числа загроз, що визначені у IT-Grundschutz Catalogues Германії з урахуванням апаратних, програмних та апаратно-програмних ресурсів, технологій обробки даних та механізмів криптографічного захисту при застосуванні ЕП, в тому числі з урахуванням вимог та умов синтезу перспективних та застосуванні ЕП в постквантовий період.
7. Безумовно, що щодо обґрунтованої та вибраної на основі IT-Grundschutz Catalogues бази Германії моделі загроз, при синтезі та застосуванні існуючих стандартизованих та перспективних ЕП повинне бути зроблено перекриття названих загроз з необхідною якістю. Для цього, у залежності від механізмів та засобів, що застосовуються для протидії, повинні бути розробленими відповідні нормативно-правові документи.
8. Загрози (атаки) сторонніми каналами є виділеним класом атак, основною особливістю яких є спрямованість на вразливості практичної реалізації криптосистем, тобто, на відміну від теоретичного криптоаналізу. Загрозою такого класу атак над традиційними є менша потужність та більш висока дієвість.

9. Загрози (атаки) сторонніми каналами є надзвичайно небезпечними, якщо їх не перекривати. Концепція цих атак існує вже доволі тривалий час, але реалізація захищеності від них вимагає знань не лише у сфері криптографії, а й у сферах технічного характеру. Тому переважна більшість перспективних ЕП розрахована на використання у пристроях, які не можуть захистити від сторонніх атак, бо не мають відповідних програмних рішень щодо захисту від витоку сторонніми каналами.

10. Основними загрозами (атаками) з застосуванням квантових математичних методів, які можуть бути реалізованими на квантовому комп'ютері (звичайно, якщо він буде побудований), є такі:

- квантовий алгоритм факторизації Шора;
- квантовий алгоритм Гровера;
- квантовий алгоритм Шора вирішення дискретного логарифму в полі;
- квантовий алгоритм Шора вирішення дискретного логарифму в групі точок еліптичної кривої;
- квантовий алгоритм криптоаналізу для перетворень в фактор кільці.

Список літератури:

1. Наказ від 20.07.2007 №141 «Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної та відкритої інформації з використанням електронного цифрового підпису» № 862/14129.
2. Закон України «Про основні засади забезпечення кібербезпеки України» // Відомості Верховної Ради (ВВР). 2017. № 45, ст. 403.
3. Закон України «Про електронні довірчі послуги» // Відомості Верховної Ради (ВВР). 2017. № 45, ст. 400.
4. Горбенко Ю. І. Методи побудування та аналізу криптографічних систем. Харків : Форт, 2015. 959 с.
5. Горбенко І. Д. Прикладна криптологія : монографія / І. Д. Горбенко, Ю. І. Горбенко. 2-ге вид. Харків : Форт, 2012. 868 с.
6. Gorjan Alagic Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. NISTIR 8309 / Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone // 22 July 2020.Режим доступу: https://doi.org/10.6028/NIST.IR.8309.
7. ЕП Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler and Damien Stehlé CRYSTALS-Dilithium: Algorithm Specifications and Supporting Documentation.Access mode: https://pq-crystals.org/dilithium/data/dilithium-specification.pdf.
8. Горбенко І. Д. Особливості побудування та аналіз електронних підписів 5 рівня безпеки для постквантового періоду на основі алгебраїчних решіток / І. Д. Горбенко, О. Г. Качко, А. М. Олексійчук, Ю. І. Горбенко, В. П. Звєрєв, М. В. Єсіна, В. А. Пономар // Прикладная радиоэлектроника. Харьков : ХНУРЭ, 2019.Т. 18, № 3, 4. С. 123–136.
9. Горбенко Ю. І. Аналіз можливостей квантових комп'ютерів та квантових обчислень для криптоаналізу сучасних криптосистем / Ю. І. Горбенко, Р. С. Ганзя. // Східно-європейський журнал передових технологій. 2014. № 1/9 (67). С. 8–15.
10. Квантовые компьютеры. [Електронний ресурс].Режим доступу: http://www.nkj.ru/archive/articles/5309/.
11. Горбенко І. Д., Постквантова криптографія та механізми її реалізації / І. Д. Горбенко, О. О. Кузнецов, О. В. Потій, Ю. І. Горбенко, Р. Ганзя, В. А. Пономар // Радиотехника. 2017. Вып. 186.С. 32–52.
12. Yesina Maryna Comparative Analysis of Key Encapsulation Mechanisms / Maryna Yesina, Mikolaj Karpinski, Volodymyr Ponomar, Yurij Gorbenko, Tomasz Gancarczyk, Uliana Iatsykovska // Proceedings of the 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). September 18-21.

Надійшла до редколегії 10.09.2020

Відомості про авторів:

Горбенко Юрій Іванович – канд. техн. наук, АТ «інститут інформаційних технологій», перший заступник головного конструктора, Україна, e-mail: gorbenkou@iit.kharkov.ua, ORCID: https://orcid.org/0000-0003-0073-9107

Єсіна Марина Віталіївна – канд. техн. наук, Харківський національний університет імені В. Н. Каразіна, доцент кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Україна, e-mail: rinayes20@gmail.com, ORCID: https://orcid.org/0000-0002-1252-7606

Онопрієнко Віктор Васильович – канд. техн. наук, генеральний директор АТ «Інститут інформаційних технологій», Україна.

Малєєва Ганна Андріївна – Харківський національний університет радіоелектроніки, аспірант кафедри безпеки інформаційних технологій, Україна, e-mail: hanna.malieieva@nure.ua

УДК 004.056.55 **DOI:10.30837/rt.2020.3.202.08**

В.І. РУЖЕНЦЕВ, д-р техн. наук

ПОРІВНЯЛЬНИЙ АНАЛІЗ ARX СХЕМ ШИФРУВАННЯ

Вступ

Базовим елементом для багатьох сучасних систем захисту інформації є блоковий симетричний шифр (БСШ). З 2000 р. по теперішній час найбільш розповсюдженим в світі БСШ може вважатися AES (FIPS-197). Відомо, що цей алгоритм орієнтований на використання у 32-бітних платформах. Приблизно з 2005 р. зрозумілою стала актуальність розроблення шифру, який би був більш швидким та потребував би значно менших ресурсів на широкому спектрі сучасних обчислювальних систем, – так званого малоресурсного шифру (lightweight cryptography). На думку багатьох вчених, саме такі шифри мають використовуватися у системах Internet of Things (IoT).

В якості базових перетворень до малоресурсного БСШ перспективними сьогодні вважаються перетворення групи ARX – addition, rotation, xor. З використанням лише цих трьох типів перетворень за останній час було створено багато алгоритмів шифрування. До таких алгоритмів можна віднести шифри сімейства RC. Початком сучасного етапу розвитку ARX криптоагоритмів можна вважати роботи [1, 2], в яких запропоновано клас ARX потокових включно з алгоритмами Salsa та Chacha. Фіналісти конкурса SHA-3 Skein [3] та Blake [4] також є ARX алгоритмами. Пізніше запропоновані алгоритми шифрування Chaskey-cipher [5], Sparx [8], LAX [8], Американським агентством безпеки (American National Security Agency) запропоновано шифр Speck [6], південно-корейські вчені розробили lea [7].

ARX перетворення швидкі, ефективно реалізуються багатьма сучасними процесорами, легко масштабуються. Головна проблема пов’язана із доведенням криптографічних властивостей таких алгоритмів.

Найбільш ефективними криптоаналітичними атаками на ARX алгоритми вважаються диференційний та лінійний криптоаналіз [9 – 12], алгебраїчні атаки, атака «зсуву»(rotational cryptanalysis), атака зустріч у середині» (meet-in-the-middle) [9, 13], інтегральний криптоаналіз [14] та його варіант, що отримав назву «division» криптоаналіз [15, 16], атака нездійснених диференціалів [17] та інші.

Оцінювання стійкості до відомих криптоаналітичних атак є одним з найбільш важливих і, разом з тим, складних етапів створення сучасного блокового симетричного шифру. Існує декілька пояснень складності цього етапу. По-перше, існує багато видів криптоаналітичних атак, які постійно вдосконалюються, також з’являються нові види атак. По-друге, складність прямої перевірки стійкості шифру до багатьох атак є занадто великою для того, щоб здійснити таку перевірку за прийнятний час навіть з використанням дуже потужних обчислювальних систем. По-третє, багато з існуючих методів оцінювання стійкості не надають гарантій того, що шифр буде захищеним від даної атаки. По-четверте, розмір блока симетричних шифрів постійно збільшується і, якщо деякий метод оцінювання стійкості пов’язаний з вирішенням задач переборного типу для частини блока або ключа, то він може виявитись занадто складним для роботи з шифрами зі збільшеним блоком. Важливо також, що недостатня точність методів оцінювання стійкості може привести або до вразливостей криптографічного алгоритму, або до його низької швидкості.

При цьому відомо, що однією з переваг ARX структур є можливість їх масштабування. Тому можна розраховувати, що зменшена модель таких перетворень збереже криптографічні властивості повномасштабного прообразу. Підхід з аналізом зменшених моделей використовувався і в інших наших роботах [18].

Загальною метою роботи є обрання або запропонування найкращої з точки зору ефективність-стійкість структури ARX-перетворення.

Для досягнення мети на початковому етапі дослідження на прикладі аналізу опису відомих ARX-криптоалгоритмів планується виділити декілька найбільш вдалих рішень. Для обраних варіантів розробити зменшені програмні моделі (моделі зі значно зменшеним розміром блоку та ключа, для яких можливо, застосувавши «силові» методи, оцінити криптоаналітичні властивості), за допомогою яких проаналізувати такі властивості, як швидкість та ефективність реалізації, стійкість до найбільш потужних криптоаналітичних атак, серед яких диференційний та лінійний криптоаналіз, алгебраїчні атаки та інші.

На наступному етапі, використовуючи зменшені моделі, планується проаналізувати вплив таких параметрів шифруючого перетворення, як кількість та розмір підблоків, кількість окремих базових перетворень (модульне додавання, зсув, XOR-додавання), на стійкість цього перетворення до основних криптоаналітичних атак. Зробити спробу формалізувати залежність стійкості кінцевого перетворення від властивостей та кількості базових перетворень. Якщо така залежність буде знайдена, то вона може бути використана і для визначення стійкості повнорозмірного ARX-перетворення.

1. Зменшені ARX моделі

Перша ARX-схема QR – це quarter-round потокового алгоритму Chacha 2 [1] зі зменшеним розміром підблоків. 16-бітовий блок схеми QR складається з чотирьох 4-бітових підблоків (рис. 1).

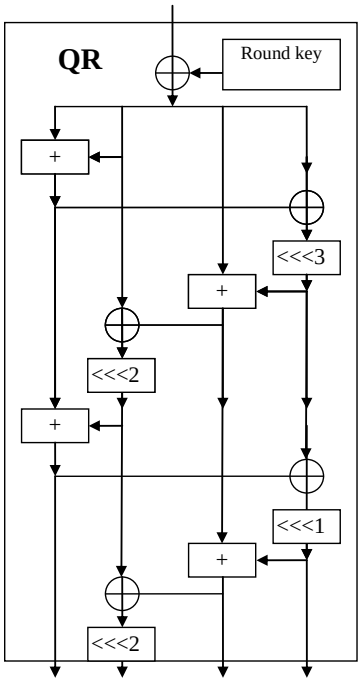


Рис. 1. QR схема

Подібна схема перетворень використовується і в блоковому алгоритмі шифрування Cypress [19].

Друга ARX-схема HR – це спрощена схема алгоритму Speckey. Спрощення полягає у відсутності двох операцій циклічного зсуву, які в оригінальному варіанті передували операціям модульного додавання. 16-бітовий блок схеми HR складається з двох 8-бітових підблоків (рис. 2).

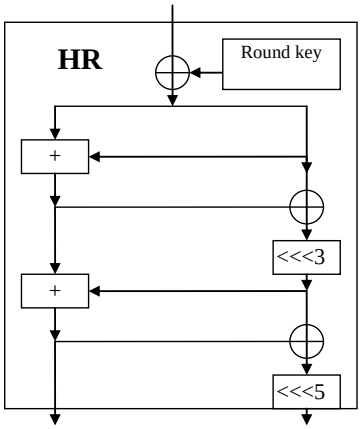


Рис.2. HR схема

Зменшена модель циклу алгоритму Simon представлена на рис. 3.

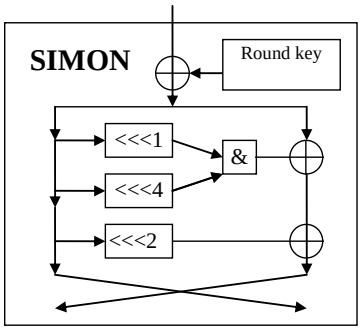
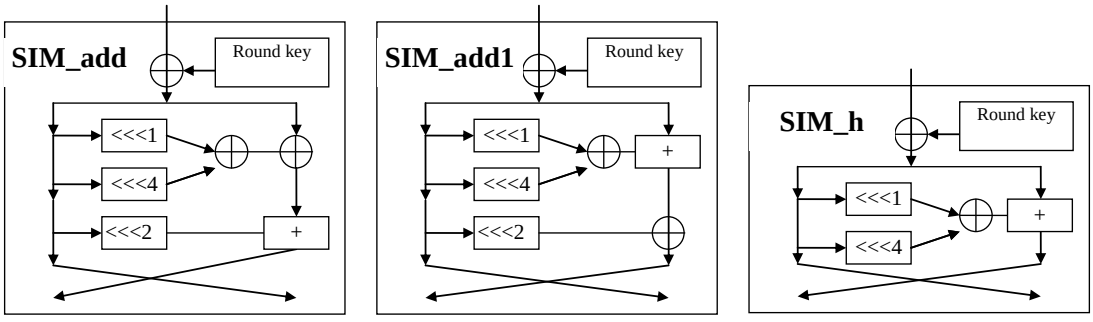


Рис. 3. Схема циклової функції шифру Simon

Як виявилося пізніше, в такому вигляді алгоритм навіть при великій кількості циклів не виходить на показники випадкової підстановки, отже в роботі також розглядалися модифікації Sim_add, Sim_add1, Sim_h, які представлено на рис. 4, *а – в* та які замість операції AND та деяких операцій XOR використовують модульне додавання.



а *б* *в*

Рис. 4. Модифікації циклової функції шифру Simon

Наступна ARX-схема – це зменшена схема алгоритму Chaskey. 16-бітовий блок схеми Chaskey складається з чотирьох 4-бітових підблоків (рис. 5).

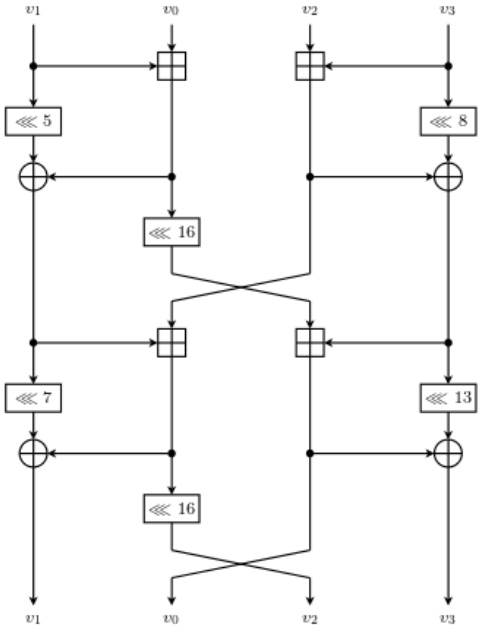


Рис. 5. Схема циклової функції шифру Chaskey

У табл. 1 представлені кількість і формат операцій для розглянутих вище схем.

Таблиця 1

Кількість та формат операцій в одному циклі шифруючих перетворень (без додавання ключа)

Шифруючі схеми	Модульне додавання (Addition)	Циклічний зсув (Rotation)	XOR
HR	2*8 bit	2*8 bit	2*8 bit
QR	4*4 bit	4*4 bit	4*4 bit
Simon	1*8 bit	3*8 bit	1*8 bit +1 AND
Sim_add	1*8 bit	3*8 bit	2*8 bit
Sim_add1	1*8 bit	3*8 bit	2*8 bit
Sim_h	1*8 bit	2*8 bit	1*8 bit
Chaskey	4*4 bit	4*4 bit	4*4 bit

Серед схем, які обрано для аналізу, є такі, що працюють з 4-бітними блоками (QR та Chaskey), та такі, що працюють з 8-бітними блоками (HR та варіанти алгоритму Simon). Кожна операція додавання (модульна або XOR), що працює з 8-бітними блоками, майже еквівалентна двом 4-бітним ідентичним операціям. Виконання 8-бітного циклічного зсуву потребує більших ресурсів ніж дві ідентичні 4-бітові операції. Але все одно, при порівнянні 4-бітних та 8-бітних схем можна вважати, що кожна 8-бітна операція еквівалентна двом таким 4-бітним операціям. Наприклад, схема HR містить у два рази менше операцій, чим QR, але формат операцій у два рази більше, ніж у схемі QR. Тому з погляду на швидкість або продуктивність ці схеми можна вважати еквівалентними при реалізації на 4-бітному процесорі, але на 8-бітному процесорі HR буде майже удвічі швидшою.

2. Аналіз криптографічної стійкості

Найбільш вагомими криптографічними показниками шифруючої функції є:

- максимальна імовірність проходження різниці (визначає стійкість шифру до атак диференціального криптоаналіза);

- максимальна імовірність лінійної апроксимації (визначає стійкість шифру до атак лінійного криптоаналіза);

- нелінійний порядок (визначає стійкість шифру до атак інтерполяційного, алгебраїчного криптоаналіза).

Для зменшених моделей шифруючих функцій є можливість визначити ці показники. Подібний підхід використовувався, наприклад, в роботі [18].

2.1. Стійкість до диференційних атак

Для обчислення максимальної імовірності проходження різниці через *n*-бітну функцію необхідно попередньо побудувати таблицю різниці, що складається зі значень

$$e_s(a, b) = \#\{x \in GF(2^n) \mid S(x \oplus a) \oplus S(x) = b\}$$

для всіх варіантів вхідної та вихідної різниць $a, b \in GF(2^n)$.

Максимальна імовірність проходження різниці через функцію $p_{D\ \max}$ визначається як усереднене для всіх ключів значення

$$p_{D\max} = \frac{\max\limits_{a\neq 0; b} e_s(a,b)}{2^n}.$$

Відомо, що для випадкової підстановки 16 в 16 бітів $p_{D\max} = 20/2^{-16} = 2^{-11,7}$.

З використанням вичерпного перебору вхідних різниць було здійснено пошук диференціалів, що володіють максимальною імовірністю, для розглянутих ARX схем. В ході пошуку використовувалися 64 випадково обраних ключі. Результати наведено у табл. 2.

Таблиця 2

Ймовірності диференціалів (для 64 випадкових ключів)

Шифруючі схеми	Кількість циклів							
	1	2	3	4	5	6	7	8
HR	1	2^{-2}	$2^{-4,6}$	$2^{-9,1}$	$2^{-11,7}$	$2^{-11,7}$	$2^{-11,7}$	$2^{-11,7}$
QR	1	2^{-2}	2^{-5}	$2^{-10,2}$	$2^{-11,7}$	$2^{-11,7}$	$2^{-11,7}$	$2^{-11,7}$
Simon	-	-	-	2^{-3}	-	$2^{-6,6}$	-	$2^{-7,9}$
Sim_add	1	$2^{-0,8}$	$2^{-1,7}$	2^{-4}	$2^{-5,9}$	$2^{-9,8}$	$2^{-11,5}$	$2^{-11,5}$
Sim_add1	1	2^{-2}	$2^{-3,8}$	$2^{-5,8}$	$2^{-8,9}$	$2^{-11,8}$	$2^{-11,8}$	$2^{-11,8}$
Sim_h	1	2^{-2}	$2^{-2,5}$	$2^{-4,4}$	2^{-6}	$2^{-8,3}$	2^{-10}	$2^{-11,7}$
Chaskey	1	2^{-3}	$2^{-8,7}$	$2^{-11,1}$	$2^{-11,8}$	$2^{-11,8}$	$2^{-11,8}$	$2^{-11,7}$

Отримані результати демонструють, що моделі приходять до стабільного значення $2^{-11,7}$ при використанні деякої кількості циклів. HR, QR та Chaskey потребують для цього п’ять циклів, Sim_add – 7 циклів, Sim_add1 – 6 циклів, Sim_h – вісім циклів.

Алгоритм Simon, навпаки, не виходить на показники випадкової підстановки при будь-якій кількості циклів. При однаковій кількості операцій в циклі алгоритм Sim_add1 демонструє кращі показники стійкості ніж Sim_add. З подальшого аналізу виключено алгоритми Simon та Sim_add.

2.2. Стійкість до лінійних атак

Для обчислення максимальної імовірності лінійної апроксимації функції необхідно попередньо побудувати таблицю лінійних апроксимацій, що складається зі значень

$$c_s(a,b) = \#\{x \in GF(2^n) \mid (W(x \,\&\, a) + W(S(x) \,\&\, b)) \bmod 2 = 0\} - 2^{n-1}$$

для всіх варіантів $a, b \in GF(2^n)$, де & – побітова кон’юнкція, $W(x)$ – вага Хемінга вектора x (кількість одиничних бітів у цьому векторі), mod 2 – операція взяття по модулю 2.

Максимальна імовірність лінійної апроксимації функції $p_{L\max}$ визначається як усереднене для всіх ключів значення

$$p_{L\max} = \frac{\left| \max\limits_{a\neq 0, b\neq 0} c_S(a,b) \right|}{2^{n-1}}.$$

Для випадкової підстановки 16 в 16 бітів $p_{L\max} = 2^{-6,4}$.

Для аналізу стійкості розглянутих ARX моделей виконувався пошук лінійної апроксимації, що володіє максимальною імовірністю, для перших п'яти варіантів вхідної маски і для випадково обраних п’яти ключів. Результати представлено в табл. 3.

Таблиця 3

Ймовірності лінійних апроксимацій (для 5 випадкових ключів)

Шифруючі схеми	Кількість циклів							
	1	2	3	4	5	6	7	8
HR	-	$2^{-3,6}$	2^{-6}	$2^{-6,3}$	$2^{-5,9}$	$2^{-8,1}$	$2^{-6,4}$	$2^{-6,4}$
QR	-	2^{-4}	$2^{-4,3}$	2^{-5}	$2^{-5,8}$	$2^{-6,5}$	$2^{-6,6}$	$2^{-8,1}$
Sim_add1	-	$2^{-2,7}$	$2^{-3,7}$	$2^{-5,6}$	$2^{-6,6}$	$2^{-6,5}$	$2^{-6,6}$	$2^{-6,6}$
Sim_h	-	2^{-2}	$2^{-3,7}$	$2^{-5,2}$	$2^{-5,4}$	$2^{-5,4}$	2^{-7}	$2^{-6,6}$
Chaskey	$2^{-0,7}$	$2^{-5,3}$	$2^{-5,2}$	$2^{-5,7}$	$2^{-6,6}$	$2^{-6,6}$	$2^{-8,1}$	$2^{-6,6}$

Отримані результати демонструють, що моделі приходять до стабільного значення $2^{-6,4}$ при збільшенні кількості циклів. Відхилення від цього значення пов'язано з розглядом сильно обмеженої безлічі вхідних масок (5 з 65536).

2.3. Стійкість до алгебраїчних атак

Для оцінки нелінійного порядку n-бітної функції $GF(2^n)\rightarrow GF(2^n)$ варто представити підстановку у вигляді n булевих функцій s_i, $0 \le i \le n-1$, кожна з яких задає відображення $GF(2)^n\rightarrow GF(2)$. Кожна з цих булевих функцій може бути представлена у вигляді суми над $GF(2)$ добутків її аргументів ступеня не вище n-1. Таке представлення булевої функції має назву алгебраїчна нормальна форма. Ступінь нелінійності булевої функції – це максимальний ступінь доданка в алгебраїчній нормальній формі цієї функції. Ступінь нелінійності (чи нелінійний порядок) усієї підстановки – це мінімальний ступінь нелінійності серед усіх складових її булевих функцій s_i, $0 \le i \le n-1$.

Нелінійний порядок для випадкової підстановки 16 в 16 бітів дорівнює 15. При аналізі зменшених моделей використовувався метод [20]. Усі моделі приходять до цього значення при використанні трьох та більше циклів.

3. Порівняльний аналіз ARX схем

Маючи для кожної з розглянутих схем показники стійкості (табл. 2, 3), можна визначити скільки операцій додавання та зсуву потрібно для забезпечення показників випадкової підстановки. У табл. 4, 5 наведена кількість операцій, відповідно, для 8-бітних та 4-бітних схем, яка потрібна для забезпечення показників випадкової підстановки.

Таблиця 4

Кількість 8-бітних операцій для забезпечення стійкості
проти диференційних, лінійних та алгебраїчних атак

Шифруючі схеми	Мінімальна кількість циклів	Кількість 8-бітних операцій			
		Addition	Rotation	Xor	Всього
HR	6	12	12	12	36
Sim_add1	6	6	18	12	36
Sim_h	8	8	16	8	32

Таблиця 5

Кількість 4-бітних операцій для забезпечення стійкості проти диференційних, лінійних та алгебраїчних атак

Шифруючі схеми	Мінімальна кількість циклів	Кількість 4-бітних операцій			
		Addition	Rotation	Xor	Всього
QR	6	24	24	24	72
Chaskey	5	20	20	20	60

Представлені у табл. 4, 5 результати демонструють, що найбільш ефективною 4-бітовою конструкцією можна вважати Chaskey, а найбільш ефективною 8-бітовою – схему Sim_h.

Стосовно схеми Sim_h важливим є те, що операція додавання підблоків (див. рис. 4, *в*) є відмінною від операції введення секретності (додавання з ключем). Якщо в цій схеми поміняти місцями операцію модульного додавання та XOR, то схема не виходить на диференційні показники випадкової підстановки навіть при великій кількості циклів.

Висновки

1. Проведено аналіз показників криптографічної стійкості зменшених моделей (16 бітний блок та ключ) відомих сьогодні ARX алгоритмів шифрування: Salsa, Chacha, Cypress, Speckey, Simon, Chaskey та їх модифікації. Продемонстровано, що для більшості з них можливо отримати показники випадкової підстановки при використанні певної кількості циклів. Виявлено, що схема алгоритму Simon не дозволяє отримати ці показники навіть при великій кількості циклів, що, на наш погляд, свідчить про вразливості цього алгоритму.

2. Показано, що потенційно ARX схеми з більшим форматом операцій є більш гнучкими та ефективними, оскільки, за нашими результатами, потребують приблизно вдвічі меншої кількості операцій для забезпечення криптографічних показників випадкової підстановки. З огляду на це, можливо більш ефективно було б запропонувати ARX схему, яка б працювала з 16-бітними блоками та виходила на показники випадкової підстановки, але поки що цього не вдалось зробити. Можливо це буде метою подальших досліджень.

3. За результатами табл. 4, 5 найбільш ефективною 4-бітовою конструкцією є зменшена модель Chaskey, а найбільш ефективною 8-бітовою – запропонована в роботі схема Sim_h (рис. 4, *в*). При цьому реалізація на 8-бітному процесорі Sim_h потребує майже вдвічі меншої кількості операції ніж Chaskey.

Список літератури:

1. Daniel J. Bernstein. Chacha, a variant of Salsa20. SASC 2008 –the State of the Art in Stream Ciphers. See also https://cr.yp.to/chacha.html, 2008.

2. Daniel J. Bernstein. The salsa20 family of stream ciphers. In Matthew Robshaw and Olivier Billet, editors, New Stream Cipher Designs: The eSTREAM Finalists, volume 4986 of Lecture Notes in Computer Science, pages 84–97, Berlin, Heidelberg, 2008.

3. Ferguson Niels, Stefan Lucks, Bruce Schneier, Doug Whiting, Mihir Bellare, Tadayoshi Kohno, Jon Callas, and Jesse Walker. The Skein hash function family. Submission to NIST, (round 3), 2010.

4. Jean-Philippe Aumasson, Luca Henzen, Willi Meier, and Raphael C.-W. Phan.SHA-3 proposal BLAKE: Submission to NIST (Round 3). http: //ehash.iaik.tugraz.at/wiki/BLAKE, 2010.

5. Nicky Mouha, Bart Mennink, Anthony Van Herrewege, Dai Watanabe, Bart Preneel, and Ingrid Verbauwhede. Chaskey: An effcient MAC algorithm for 32-bit microcontrollers. In Antoine Joux and Amr M. Youssef, editors, SAC 2014: 21st Annual International Workshop on Selected Areas in Cryptography, volume 8781 of Lecture Notes in Computer Science, pages 306–323. Springer, Heidelberg, August 2014. Doi:10.1007/978-3-319-13051-4_19

6. Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers. The SIMON and SPECK families of lightweight block ciphers. Cryptology ePrint Archive, Report 2013/404, 2013. http://eprint.iacr.org/2013/404.

7. Deukjo Hong, Jung-Keun Lee, Dong-Chan Kim, Daesung Kwon, Kwon Ho Ryu, and Dong-Geon Lee. LEA: A 128-bit block cipher for fast encryption on common processors. In Yongdae Kim, Heejo Lee, and Adrian Perrig, editors, WISA 13: 14th International Workshop on Information Security Applications, volume 8267 of Lecture Notes in Computer Science, pages 3–27. Springer, Heidelberg, August 2014. Doi:10.1007/978-3-319-05149-9_1

8. Daniel Dinu, Léo Perrin, Aleksei Udovenko, Vesselin Velichkov, Johann Großschädl, and Alex Biryukov. Design strategies for ARX with provable bounds: Sparx and LAX. In Jung Hee Cheon and Tsuyoshi Takagi, editors,

Advances in Cryptology – ASIACRYPT 2016, Part I, volume 10031 of Lecture Notes in Computer Science, pages 484–513. Springer, Heidelberg, December 2016. Doi:10.1007/978-3-662-53887-6_18

9. Alex Biryukov, Patrick Derbez, and Léo Perrin. Differential analysis and meet-in-the-middle attack against round-reduced TWINE. In Gregor Leander, editor, Fast Software Encryption – FSE 2015, volume 9054 of Lecture Notes in Computer Science, pages 3–27. Springer, Heidelberg, March 2015. Doi:10.1007/978-3-662-48116-5_1

10. Alex Biryukov, Vesselin Velichkov, and Yann Le Corre. Automatic Search for the Best Trails in ARX: Application to Block Cipher Speck. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 9783, 2016. P. 289-310. Doi:10.1007/978-3-662-52993-5_15

11. An Improved Automatic Search Method for Differential Trails in TEA Cipher. International Journal of Network Security, Vol.18, No.4, 2016. PP.644-649.

12. Alex Biryukov, Arnab Roy, and Vesselin Velichkov. Differential Analysis of Block Ciphers SIMON and SPECK. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 8540, 2015. P. 546-570. Doi:10.1007/978-3-662-46706-0_28

13. Patrick Derbez and Léo Perrin. Meet-in-the-middle attacks and structural analysis of round reduced PRINCE. In Gregor Leander, editor, Fast Software Encryption – FSE 2015, volume 9054 of Lecture Notes in Computer Science, pages 190–216. Springer, Heidelberg, March 2015. Doi:10.1007/978-3-662-48116-5_10

14. L. Wen and M. Wang. Integral zero-correlation distinguisher for ARX block cipher, with application to shacal-2," in Information Security and Privacy, pp. 454-461, Springer, 2014. Doi:10.1007/978-3-319-08344-5_32

15. Yosuke Todo. Structural evaluation by generalized integral property. In Elisabeth Oswald and Marc Fischlin, editors, Advances in Cryptology – EUROCRYPT 2015, Part I, volume 9056 of Lecture Notes in Computer Science, pages 287–314. Springer, Heidelberg, April 2015.

16. Christina Boura and Anne Canteaut. Another view of the division property. In Matthew Robshaw and Jonathan Katz, editors, Advances in Cryptology – CRYPTO 2016, Part I, volume 9814 of Lecture Notes in Computer Science, pages 654–682. Springer, Heidelberg, August 2016.

17. Xuexin Zheng and Keting Jia. Impossible differential attack on reduced-round TWINE. In Hyang-Sook Lee and Dong-Guk Han, editors, ICISC 13: 16th International Conference on Information Security and Cryptology, volume 8565 of Lecture Notes in Computer Science, pages 123–143. Springer, Heidelberg, November 2014.

18. Долгов В.И. Анализ циклических свойств блочных шифров / В.И. Долгов, И.В. Лисицкая, В.И. Руженцев // Прикладная радиоэлектроника. 2007. Т. 6, №2. С. 257-263.

19. Малоресурсний симетричний блоковий шифр "Кипарис" – сутність та основні властивості / М.Ю. Родінко // Математичне та комп'ютерне моделювання. Серія: Технічні науки : зб. наук. пр. Кам'янець-Подільський : Кам'янець-Подільськ. нац. ун-т, 2017. Вип. 15. С. 203-208.

20. Knudsen L. R. Truncated and Higher Order Differentials [Text] / L. R. Knudsen // Fast Software Encryption : proceedings of the Second International Workshop, Leuven, Belgium, December 14–16, 1994. Berlin ; Heidelberg : Springer-Verlag, 1995. P. 196–211. (Lecture Notes in Computer Science ; vol. 1008).

Надійшла до редколегії 04.09.2020

Відомості про авторів:

Руженцев Віктор Ігорович – д-р техн. наук, Харківський національний університет радіоелектроніки, професор кафедри безпеки інформаційних технологій, Україна, e-mail: viktor.ruzhentsev@nure.ua, ORCID: https://orcid.org/0000-0002-1007-6530

ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОММУНІКАЦІЙНИХ СИСТЕМАХ

УДК 681.3.06:519.248.681 **DOI:10.30837/rt.2020.3.202.09**

І.Д. ГОРБЕНКО, д-р техн. наук, Е.А. СЕМЕНКО, О.А. ЗАМУЛА, д-р техн. наук

МЕТОДИ ТА ЗАСОБИ СИНТЕЗУ І ГЕНЕРАЦІЇ СИГНАЛІВ – ФІЗИЧНИХ ПЕРЕНОСНИКІВ ДАНИХ У СУЧАСНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Вступ

Сучасні радіолокаційні, супутникові радіонавігаційні і інформаційно-комунікаційні системи (ІКС) виконують різноманітні завдання, основним з яких є пошук, виявлення, класифікація, обмін, обробка, цілевказівки, зберігання даних, освоюють все більшу кількість функцій, при цьому намітилися наступні тенденції:

- постійне зростання кількості корпоративних, індивідуальних і мобільних абонентів;
- зростання трафіку;
- обмежена кількість радіоканалів;
- обмежена пропускна здатність;
- великий час зчитування, запису та доставки інформації споживачеві;
- низька завадозахищеність, інформаційна і кібербезпека і ін.

Для вирішення цих та інших проблем приймаються такі технічні рішення:

- впровадження складних видів модуляції, кодування, шифрування даних;
- застосування технологій багаторівневого ущільнення інформаційних потоків;
- збільшення бази, об’єму сигналу і каналу;
- застосування адаптивних систем комплексного використання методів розділення сигналів, трас поширення та інформаційних каналів.

Однією зі складних проблем створення ІКС залишається синтез системи сигналів – фізичних переносників даних. При цьому повинна бути визначена необхідність та способи реалізації синхронізації, оцінені завадостійкість, скритність, інформаційна безпека при дії різних перешкод і впливів зловмисника, синтезовано структуру передавальної, приймальної апаратури, здійснено розподіл функції між програмної та апаратної частинами і інше [1].

Ключові технології побудови перспективних ІКС включають такі:

- застосування вузько-, широко- і понадширокосмугових сигналів;
- модернізація методів поділу каналів;
- побудова приймачів і антенних решіток з малим рівнем власних і взаємних шумів;
- розширення теорії ортогональних інформаційних просторів;
- побудова методів багатоетапного оборотного перетворення сигналів;
- стандартизація та уніфікація транспортних протоколів обміну на всіх рівнях системи;
- розробка методів управління точністю вимірювання параметрів;
- застосування бортового обладнання супутників зв’язку і космічних апаратів для побудови мереж з розподіленою обробкою інформації;
- поєднання в системі технологій радіо- та інших діапазонів, форм сигналів, в тому числі і неенергетичних;
- розробка технологій міжсупутникових ліній зв'язку, електромагнітних, оптичних та інших;
- підвищення надійності функціонування за рахунок адаптації системи інформаційного обміну в реальних умовах.

Аналіз наведених інформаційних технологій показує актуальність розробки нових і вдосконалення існуючих способів і засобів їх реалізації в сучасних ІКС. Зокрема, в теорії

сигналів накопичений величезний потенціал інформаційних технологій, однак на практиці використовується обмежений набір традиційних методів і технічних рішень.

Пошук нових систем сигналів повинен бути заснований на законі синергії, завдяки якому стає можливим отримання ефектів, що перевищують просту суму властивостей явищ, що входять в систему сигналів. Потрібно узагальнити накопичений потенціал, визначити закони, принципи та методи їх застосування. Для цього слід провести системну класифікацію та уніфікацію інформаційних потоків для вирішення завдань формування та обробки інформації в ІКС, систематизацію моделей, методів, технічних і програмних засобів їх реалізації. Принципи побудови нових технологій в області ІКС повинні охоплювати весь спектр перетворень інформації в комплексі, від джерела до споживача. І повинні бути засновані не тільки на ефективній передачі інформації, але і на забезпеченні скритності, електромагнітної та іншої сумісності, екології, інформаційної безпеки, захищеності від нав'язування (введення в систему) помилкових даних і інше.

Мета статті – представлення та аналіз моделей, методів і засобів генерації і обробки одного з класів сигналів з розширенням спектру, що є фізичному переносником даних в ІКС.

1. Аналіз сигналів – фізичних переносників даних у сучасних інформаційно-комунікаційних системах

Розвиток технологій бездротових комунікацій постійно формувався на основі досліджень форм сигналів. Як приклад можна навести використання технології мультиплексування сигналів з ортогональним частотним розділенням каналів (Orthogonal frequency – division multiplexing, далі – OFDM) в сучасних бездротових системах зв'язку широкосмугового доступу (WiMAX, WiFi, LTE та ін.). Застосування такої технології дозволяє підвищити інформаційну ємність системи при обмеженій смузі пропускання, швидкість прийому-передачі даних, наблизивши її до пропускної здатності каналу, збільшити скритність передачі і стійкість перед перешкодами прийому сигналів, і, як наслідок, забезпечити постійно зростаючі потреби користувачів мереж в високошвидкісних з'єднаннях і мультимедійних сервісах [2, 3].

По суті OFDM – це схема модуляції, що використовує множину несучих. Канал ділиться на кілька субканалів. В OFDM високошвидкісний потік даних конвертується в кілька паралельних бітових потоків меншої швидкості, кожен з яких модулюється своєю окремою несучою. Вся ця множина несучих передається одночасно. Одна з переваг OFDM полягає в тому, що тривалість символу в допоміжній несучій значно більше в порівнянні з затримкою поширення, ніж в традиційних схемах модуляції. Це робить OFDM набагато стійкішою до між символьної інтерференції.

Аналітично OFDM сигнал може бути представлений у вигляді [2]:

$$S(t) = \sum_{k=0}^{N-1} S_k(t) = \sum_{k=0}^{N-1} A_k \, e^{j2\pi kf/T}, 0 \le t \le T, \quad (1)$$

де k – індекс піднесучої, $S_k(t)$ – сигнал на k-піднесучий, A_k – амплітудна складова послідовності інформаційних символів, N – кількість піднесучих, T – тривалість інформаційного символу.

Основна ідея OFDM полягає в тому, що для досягнення високої швидкості передачі в частотної області застосовується розподіл повного діапазону частот сигналу на деяке число частотних підканалів з меншими швидкостями. При цьому кожен підканал (піднесуча) модулюється окремим символом, потім ці канали мультиплексуються за частотою і дані передаються паралельно по ортогональних підканалах. У порівнянні з передачею з однієї несучої цей підхід забезпечує підвищену стійкість до вузькополосної інтерференції і спотворень в каналі. Більш того, з цього випливає високий рівень гнучкості системи, так як параметри модуляції, такі як розмір сузір'я, швидкість кодування, можуть бути незалежно вибрані для кожного з підканалів.

Структура OFDM сигналу може бути досить складною, оскільки складається з множини компонентів:

- структура частотно-часового розподілу, що задана початковою частотою, кроком сітки частот, кількістю піднесучих;
- за часовими слотами, що задані тривалістю символу, тривалістю захисного інтервалу;
- вид маніпуляції: фазова (BPSK, QPSK, 8-PSK) або амплітудно-фазова квадратурна модуляція (QAM);
- дискретні послідовності, які визначають закон (правило) маніпуляції фази високочастотної несучої і задаються розмірністю сигнального простору;
- вид символьної синхронізації;
- наявність і вид завадостійкого кодування (код Ріда – Соломона, код Боуза – Чоудхурі Хоквінгема, турбокод і ін.);
- наявність і вид перемеження даних і ін.

Наведені особливості структури OFDM сигналу можуть бути використані при побудові ІКС, для яких вимоги забезпечення заданих показників захищеності від введення (нав'язування) неправдивих повідомлень, фальсифікації повідомлень, порушення цілісності даних, конфіденційності, завадостійкості прийому, скритності функціонування є визначальними.

Численні дослідження показали, що поліпшення якісних показників, зокрема завадозахищеності та інформаційної безпеки ІКС і мереж, може бути досягнутий, в тому числі, шляхом розробки методів синтезу, формування і обробки складних дискретних сигналів-фізичних переносників даних з необхідними ансамблевими, структурними і кореляційними властивостями [4 – 6].

Ряд досліджень [7, 8] показали, що подальше поліпшення основних якісних показників деяких додатків радіоканалів може бути досягнуто на основі використання сигналів з лінійною частотною модуляцією (ЛЧМ), ФМ ЛЧМ і в загальному випадку складових нерівномірних за тривалістю ЛЧМ сигналів з внутрішньоімпульсною ФМ (СНЛЧМ-ФМ) сигналів.

Аналітичне представлення СНЛЧМ-ФМ сигнали має вигляд

$$S^{(p)}(t) = S_0{}^{(p)} \sum_{n=1}^{N} \sum_{l=1}^{Q} V_e{}^{(p)} \operatorname{rect}\left(\frac{t - \sum_{r=0}^{n-1} T_r}{T_n} \right) \operatorname{rect}\left(\frac{t - (l-1)\tau_э}{\tau_э} \right) \times$$

$$\times \exp\left(j \left(\omega_n \left(t - \sum_{r=0}^{n-1} T_r \right) + \frac{\mu_n}{2} \left(t - \sum_{r=0}^{n-1} T_r \right)^2 + \varphi_n \right) \right), \qquad (2)$$

де $S_0{}^{(p)}$ – амплітуда огибаючої сигналу; N – число радіоімпульсів, що складають СНЛЧМ – ФМ сигнал; Q – число елементів двійкової маніпулюючої послідовності; $V_e{}^{(p)}$- символ p-й маніпулюючої послідовності, причому $V_l^{(p)} \in \{1, -1\}$; $\operatorname{rect}(x)$ – є функція, що має вигляд

$$\operatorname{rect}(x) = \begin{cases} 1 \text{ при } 0 \le x \le 1, \\ 0 \text{ при } x < 0, x > 1 \end{cases}; \qquad (3)$$

$\tau_э$ – тривалість елемента маніпулюючої послідовності; ω_n, φ_n – несуча частота і початкова фаза n-го ЛЧМ радіоімпульсу; μ_n – коефіцієнт нахилу маніпулюючої характеристики n-го ЛЧМ радіоімпульсу, що пов'язаний з девіацією частоти ΔF_n і тривалістю T_n співвідношенням $\mu_n = \pm 2\pi \Delta F_n / T_n$.

Одним з головних напрямків розвитку ІКС є впровадження складних, широкосмугових, шумоподібних сигналів [4 – 6], зокрема сигналів, отриманих шляхом зміни фази гармонійного коливання в дискретні моменти часу за законом псевдовипадкових кодових послідовностей. Застосування широкосмугових і досить протяжних в часі сигналів, як правило з внутрішньоімпульсною модуляцією, в сукупності з ефективними алгоритмами їх обробки дозволяє підвищити завадостійкість прийому сигналів при впливі навмисних і ненавмисних перешкод, енергетичну скритність сигналів від радіотехнічної розвідки, дає можливість реалізувати кодове розділення каналів при багатостанційному доступі, вимірювати час приходу сигналів з великою точністю і високою роздільною здатністю, встановлювати надійний зв'язок в каналах при наявності багатопроменевого характеру поширення радіохвиль і ін. Безліч таких сигналів має володіти хорошими кореляційними властивостями. Кожен з таких сигналів повинен відрізнятися від своєї зрушеною в часі копії і від будь-якого іншого сигналу цієї множини з довільним тимчасовим зрушенням.

Множинний доступ з кодовим поділом абонентів в багатокористувачевих інформаційно-комунікаційних системах (ІКС) здійснюється через використання при розширенні спектру специфічних дискретних послідовностей (ДП). При цьому кореляційні, структурні, ансамблеві та енергетичні властивості дискретних сигналів ототожнюють з відповідними властивостями ДП, які застосовують для утворення таких сигналів, і саме ДП, значною мірою визначають показники завадостійкості і скритності функціонування ТКС, а також інформаційної безпеки таких систем [4]. Тому розробка ефективних методів синтезу ДП (за законом яких маніпулюють параметри інформаційних бітів даних) з визначеними структурними, ансамблевими, кореляційними та іншими властивостями є актуальним завданням.

Авторами вперше сформульовано і у загальному вигляді вирішено задачу синтезу нового класу нелінійних дискретних складних сигналів – криптографічних дискретних сигналів (КДС).

Під КДС пропонується розуміти сукупності послідовностей (векторів) символів певного алфавіту, які обов’язково володіють необхідними (заданими) структурними, ансамблевими та кореляційними властивостями, часовою та просторовою складністю відтворення та мають можливість формування їх на основі ключів [9]. Правила побудови КДС грунтуються на використанні випадкових чи псевдовипадкових процесах, вони повинні відповідати вимогам випадковості, незворотності, непомітності, непередбачуваності та іншим [10 – 12]. Такі сигнали мають покращені, у порівнянні з іншими відомими класами сигналів, кореляційними і ансамблевих властивостями, і які обмежені значеннями «щільної упаковки».

2. Постановка і вирішення в загальному вигляді задачі синтезу криптографічних дискретних сигналів (КДС)

Під задачею побудування (синтезу) будемо розуміти задачу побудови підмножин дискретних послідовностей $(W_l^q), q = \overline{1,N}, l = \overline{1,L}$, сукупність яких утворює систему дискретних сигналів заданого алфавіту розмірності $M_k = N \times L$, таких, що в кожній із підмножин (словнику) виконуються умови, що висуваються до підмножини КДС в частині структурних, ансамблевих, кореляційних властивостей, просторової та часової складності їх генерування [13].

Побудова КДС грунтується на основі аналізу та використанні періодичних та аперіодичних функцій кореляції та зводиться до наступних етапів.

1. Забезпечення умов виконання вимог до структурних та ансамблевих властивостей, можливостей формування підмножини КДС з допустимою часовою та просторовою складністю, в тому числі з використанням ключів.

2. Побудова КДС W^q, періодична функція автокореляції (ПФАК) кожного з яких, задовольняє системі нелінійних параметричних нерівностей (НПН):

$$R^q_{a_1}(l) \le \sum_{i=1}^{L} W_i^q (W_{i+l}^q)^* \le R^q_{a_2}(l),\ l=\overline{1,L-1},\ q=\overline{1,N}, \tag{4a}$$

де $R^q_{a_1}(l)$ і $R^q_{a_2}(l)$ – задані значення реалізації ПФАК, а індекси обчислюються за модулем $(i+l)\ mod\ L$.

При $l=L$ для усіх $q=\overline{1,N}$ (1a) дає згортку зі значенням L:

$$\sum_{i=1}^{L} W_i^q W_{i+L}{}^q = \sum_{i=1}^{L} W_i^q W_i^q = L, q=\overline{1,N},\ . \tag{4b}$$

3. Побудова пар КДС W^q та W^p, функції взаємної кореляції (ФВК) яких задовольняють вимогам, що визначаються сукупністю систем НПН (5a), а також задовольняють вимогам до стикових функцій взаємної кореляції (СФВК) пар КДС W^q та W^p зі стиковими дискретними словами W^{qp} і W^{pq} (5b – 5d):

$$R^{qp}_{b_{1,1}}(l) \le \sum_{i=0}^{L-K} W_i^q \times (W_{i+l}^p)^* + \sum_{i=L-K+1}^{L-1} W_i^q \times (W_{i-l+K}^p)^* \le R^{qp}_{b_{2,1}}(l); \tag{5a}$$

$$R^{qp}_{b_{1,2}}(l) \le \sum_{i=0}^{L-K} W_i^q \times (W_{i+l}^q)^* + \sum_{i=L-K+1}^{L-1} W_i^q \times (W_{i-l+K}^p)^* \le R^{qp}_{b_{2,2}}(l); \tag{5b}$$

$$R^{qp}_{b_{1,3}}(l) \le \sum_{i=0}^{L-K} W_i^q \times (W_{i+l}^p)^* + \sum_{i=L-K+1}^{L-1} W_i^q \times (W_{i-l+K}^q)^* \le R^{qp}_{b_{2,3}}(l); \tag{5c}$$

$$R^{qp}_{b_{1,4}}(l) \le \sum_{i=0}^{L-K} W_i^p \times (W_{i+l}^p)^* + \sum_{i=L-K+1}^{L-1} W_i^p \times (W_{i-l+K}^q)^* \le R^{qp}_{b_{2,4}}(l); \tag{5d}$$

$$R^{qp}_{b_{1,5}}(l) \le \sum_{i=0}^{L-K} W_i^p \times (W_{i+l}^q)^* + \sum_{i=L-K+1}^{L-1} W_i^p \times (W_{i-l+K}^p)^* \le R^{qp}_{b_{2,5}}(l); \tag{5e}$$

причому $l=\overline{1,L-1}$ для всіляких поєднань q і p, $q=\overline{1,N}$, $p=\overline{1,N}$, $q\ne p$, де $R^{qp}_{b_{1,j}}(l)$ і $R^{qp}_{b_{2,j}}(l)$, задані (необхідні) реалізації ПФВК і СФВК відповідно, $j=\overline{1,5}$.

В системах нелінійних параметричних нерівностей (4a) – (4b) та (5a) – (5e) W_i^q та W_i^p є невідомими значеннями випадкових чи псевдовипадкових символів КДС W^q та W^p, $q=\overline{1,N}$, що належать визначенню в процесі їх побудування. В подальшому системи (4a)– (4b), (5a) – (5e) та квадратичне рівняння (5h) будемо називати моделлю підмножини (словника) КДС.

Проведемо аналіз систем нелінійних параметричних квадратичних нерівностей (далі систем) (4a) – (4b) та (5a) – (5e), використовуючи введену модель.

Системи (5b) та (5d) при $l=L$ для усіх $q=\overline{1,N}$ повинні дати повну згортку зі значенням L, тобто (5b)

$$\sum_{i=1}^{L} W_i^q W_{i+L}{}^q = \sum_{i=1}^{L} W_i^q W_i^q = L, q=\overline{1,N}, \tag{5f}$$

а (5d) дає

$$\sum_{i=1}^{L} W_i^p W_{i+L}{}^p = \sum_{i=1}^{L} W_i^p W_i^p = L, p=\overline{1,N},. \tag{5g}$$

Системи (5a), (5c) та (5e) при $l=L$ для усіх пар W^q та W^p дають значення функції взаємної кореляції при нульовому значенні зсуву відповідно виду

$$\sum_{i=1}^{L} W_i^q W_{i+L}{}^p = \sum_{i=1}^{L} W_i^q W_i^p = R^{qp}(0); q, p=\overline{1,N}, \tag{5h}$$

$$\sum_{i=1}^{L} W_i^q W_{i+L}{}^p = \sum_{i=1}^{L} W_i^q W_i^p = R^{qp}(0), q, p = \overline{1, N}, \tag{5i}$$

$$\sum_{i=1}^{L} W_i^p W_{i+L}{}^q = \sum_{i=1}^{L} W_i^p W_i^q = R^{pq}(0), p, q = \overline{1, N}, . \tag{5j}$$

Проведемо аналіз систем (4a) – (4b) на предмет існування рішень та незалежності. Безпосередньо із (4a) маємо, що щодо кожного із q КДС W^q є L невідомих – $W_1^q, W_2^q \cdots W_L^q$. Для їх знаходження згідно з (4a) можна скласти систему із L – 1 незалежних НПН. Далі, використовуючи (4b), отримуємо ще один вираз, але уже рівняння. Особливістю системи (4) є те, що вона дає згортку кожного із q КДС зі значенням L. На основі (4a) та (4b) при побудові кожної N підмножини КДС можна скласти N незалежних систем квадратичних НПН, кожна з яких буде містити L-1 квадратичних нерівностей виду (4a) і формально одне рівняння, тобто всього їх буде L.

Також проведемо аналіз сукупності систем параметричних нерівностей (5a) – (5e), з урахуванням (5f) – (5j), на предмет існування рішень та незалежності систем та окремих рівнянь. Системи (5a) – (5e) визначають допустимі взаємно кореляційні властивості відносно ПФВК та СФВК кожної пари КДС – W^q та W^p . Вони визначають вимоги відносно ПФВК та СФВК конкретно тільки двох КДС – W^q та W^p . При побудові трьох КДС будемо мати 3!/2 систем виду (5), а при N КДС відповідно – N!/2 систем виду (5). Таким чином, з ростом N число систем виду (5) збільшується експоненційно (за факторіалом).

Для N = 2 серед (5f) – (5j) систем НПН є збиткові нелінійні квадратичні рівняння. Рівняння (4b) співпадає з (5f) та (5g), тому останні два уже входять у систему (1b), є залежними, тому не можуть бути використаними. Далі, рівняння (5h) та (5i) співпадають, а рівняння (5j) є симетричним в частині кореляційної функції по відношенню до рівнянь (5h) та (5i). Тому для кожної пари p та q незалежним є (5h).

На основі аналізу маємо, що усі (5a) – (5e) системи НПН визначають різні реалізації ПФВК та СФВК конкретно тільки двох КДС – W^q та W^p. Тому математична модель побудови двох КДС W^q та W^p однозначно визначається п’ятьма системами НПН у вигляді (5a) – (5e) та, як уже було обґрунтовано, рівнянням (5h).

Наведені вище результати аналізу дозволяють визначити складність моделі та на її основі складність побудування підмножини із N КДС.

1. При побудуванні одного КДС необхідно, у залежності від допустимих значень $R_{a_1}^q(l)$ і $R_{a_2}^q(l)$, що визначаються межами щільної упаковки, розглянути $\upsilon \geq k$ систем виду (4).

2. При побудуванні двох КДС необхідно розглянути $\upsilon_2 \geq K_2$ систем виду (5), де K_2 визначається $R_{b_{1,j}}^{qp}(l)$ та $R_{b_{2,j}}^{qp}(l)$.

3. При побудуванні N КДС необхідно розглянути $\upsilon \geq K_N$ систем виду (5), де K_N визначається $R_{a_1}^q(l)$ і $R_{a_2}^q(l)$ та $R_{b_{1,j}}^{qp}(l)$ і $R_{b_{2,j}}^{qp}(l)$ допустимими значеннями.

Таким чином, на основі врахування меж фізичної упаковки підмножини КДС [1] існують можливості побудови підмножин КДС згідно (4) та (5).

Аналогічно (4) та (5) задається модель підмножини (словника) КДС через аперіодичні функції автокореляції (АФАК). В даному випадку можливі спрощення. Так, систему (4) за аналогією можна подати у вигляді системи НПН на основі аперіодичних функцій кореляції, тобто

$$r_{a_1}^q(l) \leq \sum_{i=1}^{L-m} W_i^q \left(W_{i+1}^q\right)^* \leq r_{a_2}^q(l), \; l = \overline{1, L}, \quad m = \overline{1, L}, \tag{6}$$

де $r_{a_1}^q(l)$ і $r_{a_2}^q(l)$ – задані, але допустимі реалізації з точки зору щільної упаковки.

Далі системи (4) та (5) також можна подати через аперіодичні функції взаємної кореляції (АФВК) у вигляді системи нелінійних параметричних нерівностей

$$r_{b_{1,1}}^{qp}(l) \le \frac{1}{L-m}\sum_{i=0}^{L-m} W_i^q \left(W_{i+1}^q\right)^* \le r_{b_{1,2}}^{qp}(l); \tag{7a}$$

$$l=\overline{1,L},\quad m=\overline{1,L},$$

$$r_{b_{2,1}}^{qp}(l) \le \frac{1}{L-m}\sum_{i=0}^{L-m} W_i^p \left(W_{i+1}^q\right)^* \le r_{b_{2,2}}^{pq}(l); \tag{7b}$$

$$l=\overline{1,L},\ m=\overline{1,L},$$

де $r_{b_{1,1}}{}^{qp}, r_{b_{1,2}}{}^{qp}, r_{b_{2,1}}{}^{qp}, r_{b_{2,2}}{}^{qp}$ – допустимі, з точки зору щільної упаковки, значення АФАК та АФВК.

Побудування (синтез) підмножини КДС ґрунтується на застосуванні ключових даних блокового симетричного алгоритму або на використанні випадкових чи псевдовипадкових дискретних послідовностей (наприклад, алгоритм AES з міжнародного стандарту ISO/IEC 18033 [1]). З урахуванням необхідності забезпечення криптографічної стійкості та структурної скритності пар чи підмножин КДС в якості джерела дискретних послідовностей може бути застосовано алгоритми блокового симетричного перетворення, які є стійкими у постквантовий період, або інше джерело випадкових чи псевдовипадкових послідовностей (наприклад, алгоритм AES з міжнародного стандарту ISO/IEC 18033).

Вказаний клас задач синтезу КДС може розв’язуватись при застосуванні методу «гілок і меж» і може бути зведений до реалізації таких етапів [13]:

1.Формування випадкових чи псевдовипадкових дискретних послідовностей.

2. Оцінка статистичних властивостей потенційних КДС.

3. Побудова необхідного числа потенційних КДС W^q згідно з системою (4) та ключовими даними.

4. Знаходження пар чи підмножин КДС W^q та W^p, які задовольняють вимогам (5a) – (5d), з застосуванням методу «гілок та меж».

5. Побудова матриці станів взаємно-кореляційних функцій всіх можливих пар потенційних КДС, які пройшли відбір за результатами попереднього кроку та мають усі необхідні властивості.

6. Аналіз матриці станів та формування необхідного числа підмножин чи пар КДС згідно з (1) та (2) та відбір в підмножину лише тих, що задовольняють вимогам.

3. Принципи побудови і загальна характеристика програмно-апаратного комплексу для синтезу, дослідження властивостей, генерації та обробки сигналів – фізичних переносників даних у сучасних ІКС

Наявність власного комплексу для розробки, аналізу та тестування запропонованих математичних моделей і теоретичних даних є важливою складовою. Крім того, практична реалізація запропонованої теоретичної моделі дозволяє оцінити якість досліджень та підтвердити теорію реальними даними. Саме для цього протягом декількох років ведеться розробка програмних засобів, що поєднують усі запропоновані принципи формування сигналів різних типів та різних конфігурацій у одному програмному засобі.

На початковому етапі було побудовано декілька окремих та незалежних модулів, які дозволяли проводити необхідні маніпуляції, а саме:

- комплексний програмний засіб для генерації/синтезу сигналів за заданими параметрами згідно із наявними закладеними моделями (доступні моделі побудови закладені на етапі програмування, змінними є лише параметри конфігурації). Даний засіб поєднував декілька наробок у сфері моделювання сигналів та декілька принципів побудови, що робило його доволі багаторазовим та цікавим з точки зору його варіаційних можливостей та повної незалежності. Результатом роботи цього засобу були згенеровані файли із дискретними

послідовностями (ДП), які у подальшому можна використовувати для проведення аналізу або для впровадження у налагоджену ІКС (систему зв'язку), як основу для утворення сигналів – фізичних переносників даних;

- комплексний програмний засіб для проведення аналізу сигналів щодо підтвердження (чи спростування) очікуваних властивостей послідовностей, що синтезуються. Даний засіб використовувався для аналізу статистичних, кореляційних, ансамблевих та криптографічних властивостей послідовностей, що синтезуються. Особливу увагу приділено аналізу криптографічних властивостей ДП, задля якого використовуються тести NIST. Як результат роботи – комплекс генерує вихідні файли, що у подальшому можуть бути використані для графічного відображення результатів у виді 2D та 3D графіків та для аналізу запропонованої моделі побудови;
- програмний засіб для побудови графічного відображення результатів досліджень.

У якості вихідних даних можна було використовувати як вихідні файли комплексного програмного засобу для генерації/синтезу сигналів, так і вихідні файли комплексного програмного засобу для проведення аналізу сигналів. Користувач отримував у якості результату побудовані зображення різноманітних видів кореляційних функцій, таблиці, що містять результати розрахунків (досліджень) статистичних, кореляційних, ансамблевих та криптографічних властивостей сигналів – фізичних переносників даних.

Усі результати генеруються із збереженням вихідних даних та параметрів системи, що дозволяє у будь-який момент відтворити отриманий результат.

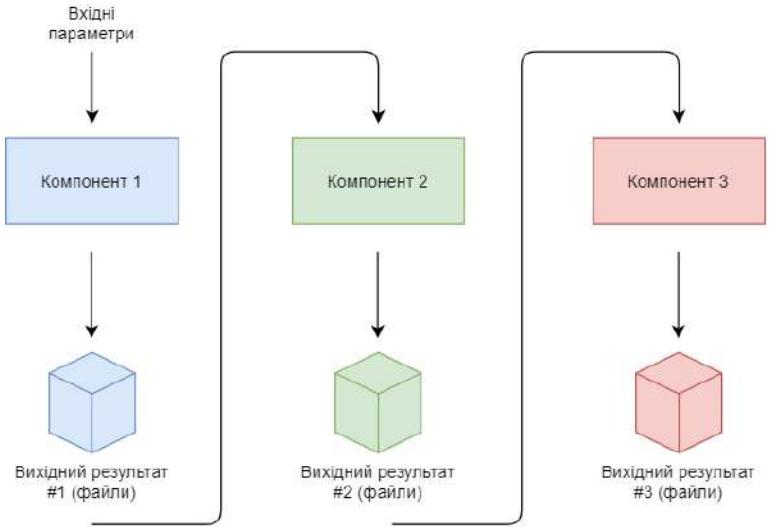


Рис. 1. Схема роботи та взаємодії між компонентами першої версії програмного рішення

Зазначені компоненти активно використовувалися у минулих дослідженнях. Проте, попри доведені властивості швидкодії та якості отриманих результатів досліджень, побудовані засоби мали низку якостей, а саме: 1) необхідність розуміння принципів налаштування та роботи, 2) необхідність знання однієї з використаних при розробці мов програмування, 3) необхідність наявності навичок роботі із декількома різними засобами для редагування зображень та інші, що значно ускладнювали та інколи унеможливлювали роботу із засобом для нових користувачів. Через це було прийнято рішення уніфікувати та поєднати зазначені компоненти у єдиний веб-сервіс. Основною ідеєю стала розробка доступного інтерфейсу користувача, що дозволяв би навіть користувачу, що не має знань у сфері побудови та аналізу сигналів ,за декілька кроків згенерувати послідовність, подаючи на вхід лише бажані параметри, отримати вихідний результат у прийнятній формі, а також провести аналіз із графічним відображенням результатів (2D/3D графіки та діаграми). На рис. 1 наведено приклад схеми взаємодії компонентів, яка була використана у першій версії імплементації, де Компонент 1 – модуль генерації послідовностей, Компонент 2 – модуль

аналізу, та Компонент 3 – це модуль графічної побудови результатів або сторонні програмні засоби, наприклад MathCad, MatLab при необхідності обробки вхідних даних, або Grafana.

Вихідні результати Компонентів 1 та 2 представлені у вигляді текстових файлів, а на виході Компоненту 3 користувач отримує графічні зображення.

Структурна схема нової версії програмного рішення наведена на рис. 2.

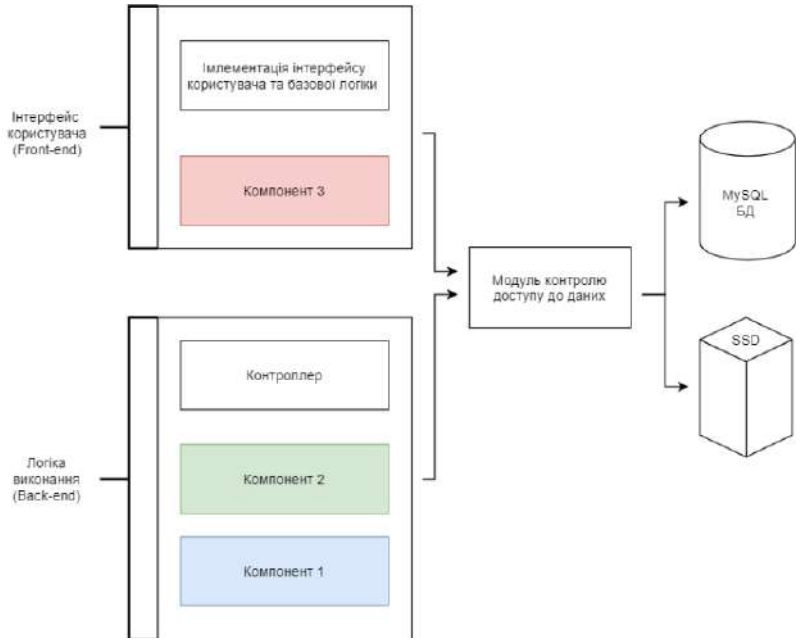


Рис. 2. Схема роботи та взаємодії між компонентами обраної архітектури веб-сервісу (оновлена версія програмного рішення)

Компоненти 1 – 3, які були використані раніше, знайшли місце у оновленій архітектурі, крім того, було розроблено окремий модуль для контролю доступу до даних (БД та системний диск). Рішення проводити дуплікацію отриманих результатів пов'язане з бажанням мінімізувати ризик втрати даних, а також мати декілька джерел. Той факт, що від сталого рішення без багатокористувачевого доступу ми змінюємо вектор на веб-сервіс із можливістю одночасного використання багатьма користувачами також мав вплив на наявну архітектуру. Було розроблено систему автентифікації та авторизації за логіком/паролем і токенами сесії, що дозволяє користувачам одночасно працювати без перешкод, отримувати доступ до своїх результатів, та ставити «задачі» на генерацію, які після завершення будуть відправляти листа на електронну пошту користувача із отриманими результатами.

Генерація послідовностей та сигналів проходить у відповідності із наведеними у теоретичній частині моделями. Наразі комплекс знаходиться на фінальній стадії розробки. Закладено можливість побудови та аналізу декількох досліджуваних типів послідовностей (М-послідовності, характеристичні дискретні сигнали, криптографічні дискретні сигнали (КДС), OFDM-сигнали). Увагу було приділено варіативності та розширенню можливостей з генерації КДС, оскільки цікавою частиною є методологія генерації криптографічного ключа. Якщо на початкових стадіях та у першій версії комплексу ми не мали змоги змінювати «на льоту» постачальника криптографічної бібліотеки, яка імплементує той чи інший алгоритм, у другій версії користувачу надано можливість обирати бібліотеку, алгоритм, вводити бажану довжину ДП, що генерується, а також особистий ключ, і все це – без втручання до програмного коду. Також однією з особливостей комплексу є модульність та відкритість до розширення новими типами сигналів і новими засобами для аналізу. Наявність інтерфейсу користувача дозволила розширити можливості з фільтрації отриманого результату без необхідності внесення змін до програмного коду, а також у декілька разів пришвидшила

загальний час роботи із комплексом. Тепер користувач має змогу візуалізувати отриманий результат та моментально перезапустити генерацію у разі необхідності. На фінальній стадії буде також запроваджено переклад порядку роботи з комплексом на три мови: російська, українська, англійська.

Апаратні характеристики робочої машини, що використовується для побудови та аналізу (вказано лише параметри, що мають прямий вплив на швидкість роботи комплексу та збереження отриманих результатів):

- центральний процесор: Intel iCore i7, 7^{th} Gen (2.9 – 3.4 GHz);
- оперативна пам'ять: 16 Gb;
- тип носія: SSD Kingston (до 550 Mb/s на запис та до 520 Mb/s зчитування);

Програмні особливості побудованого комплексу (мови програмування, деталі побудови інтерфейсу):

- мова програмування back-end частини: Java 8 (із використанням останніх особливостей для паралельної обробки);
- додаткові бібліотеки та залежності (back-end): Spring Boot, Spring Security, BouncyCastle security lib;
- мова програмування front-end (UI) частини: JavaScript, TypeScript, HTML, SCSS;
- додаткові бібліотеки та залежності (front-end): Angular 8;
- компоненти для побудови графічних елементів (графіки, діаграми): елементи, побудовані із використанням засобів та модулів Angular Framework, Grafana;
- зберігання результатів: файлова система (для вихідних файлів) + дублювання у MySQL database.

Для підвищення швидкодії під час генерації сигналів та їх аналізу використано адаптивний алгоритм конфігурації кількості одночасних потоків на центральному процесорі. Цей підхід дозволяє підвищити рівень загальної швидкості роботи програмного рішення в залежності від того, на якому апаратному комплексі він запущений.

У подальшому планується повна міграція із локальної машини до хмари (Amazon AWS, MS Azure чи Google Cloud), що дозволить, по-перше, підвищити швидкодію та, по-друге – надати повний доступ зацікавленим користувачам, які зможуть протестувати запропоновані моделі генерації та допомогти у виявленні недоліків чи запропонувати потенційні шляхи до покращення.

Крім того, ми впевнені, що завдяки відмові від власних компонентів візуалізації на користь всесвітньо визнаних засобів ми зможемо підвищити якість результатів та їх відображення, а також підвищити рівень відтворюваності отриманого результату. За бажанням кожен зможе використати запропонований комплекс для проведення власного аналізу і підтвердити достовірність наведених результатів, що є важливим для кожного дослідника.

Висновки

Авторами отримано метод синтезу нелінійних складних криптографічних дискретних сигналів (КДС) для застосування у ІКС в якості фізичного переносника даних, який використовує випадкові (псевдовипадкові) процеси і дозволяє створювати сигнали з необхідними ансамблевими, структурними і кореляційними властивостями, що дає можливість поліпшити показники ефективності інформаційно-телекомунікаційних систем, що функціонують в умовах зовнішніх і внутрішніх впливів, обумовлених, з одного боку, дією природних перешкод, перешкод від інших радіотехнічних систем, що функціонують на близьких частотах або в спільній ділянці діапазону частот, з іншого боку – навмисних перешкод, створених з метою радіоелектронного придушення діючих систем, станціями протидії. Поліпшення зазначених показників ефективності досягається, зокрема, за рахунок можливості формування із застосуванням отриманого методу великих ансамблів дискретних послідовностей практично будь-якого періоду з необхідними (для тих чи інших додатків

системи) значеннями бічних пелюсток функцій авто взаємної і стикової функцій кореляції в періодичному і аперіодичному режимах роботи, а так само статистичними характеристиками кореляційних функцій (КФ), які не поступаються аналогічним характеристикам кращих, з точки зору КФ, лінійних класів сигналів. Зазначене дає можливість підвищити завадостійкість прийому сигналів. КДС мають поліпшені в порівнянні з лінійними класами сигналів ансамблевими властивостями. Так, для періоду послідовності N=1023 обсяг системи, складений з КДС, більш ніж в 15 разів перевищує обсяг системи сигналів з трирівневою функцією взаємної кореляції, і більш ніж в 1200 разів обсяг системи, складеної з M-послідовностей. За рахунок поліпшених ансамблевих властивостей КДС і динамічної зміни відповідності біт повідомлення – складний сигнал з'являється можливість поліпшити показники інформаційної безпеки, насамперед, захищеності від нав'язування (вводу у систему) хибних повідомлень. Крім того, синтезовані з використанням розробленого методу сигнали, як показали результати тестування, за своїми статистичними властивостями близькі до властивостей випадкових послідовностей, тобто мають практично ідеальну структурну скритність, що дозволяє збільшити скритність функціонування системи.

Розроблено комплекс програмних засобів, який реалізує методи синтезу і дослідження властивостей нових класів складних нелінійних дискретних сигналів. Такий комплекс дозволяє: генерувати нелінійні КДС, нелінійні послідовності символів в кінцевих полях Галуа [14, 15], M-послідовності, OFDM-сигнали практично будь-якої тривалості; визначати значення мінімальних і максимальних бічних викидів різних КФ; порівнювати отримані значення з відомими, потенційно досяжними границями для відповідних КФ; синтезувати на основі КДС і ортогональних систем сигналів похідні системи сигналів із заданими властивостями; визначити синтезованим послідовностям унікальні ідентифікатори (спеціальні радіодані), які необхідні для оптимальної обробки даних; визначати і досліджувати статистичні, ансамблеві характеристики синтезованих нелінійних сигналів. Програмне та математичне забезпечення методів синтезу, формування, обробки і дослідження властивостей систем нелінійних сигналів, практично готове до можливого застосування в складі дослідних зразків і елементів цифрових комунікаційних засобів сучасних ІКС.

Можливості отриманого програмно-апаратного комплексу із застосуванням додаткового відповідного математичного апарату дозволяють здійснювати синтез та аналіз безлічі класів сигналів, у тому числі й тих, які наведено у даній публікації.

Список літератури:

1. Gorbenko I.D., Zamula A. A., Morozov V. L. Information security and noise immunity of telecommunication systems under conditions of various internal and external impacts // Telecommunications and Radio Engineering Volume 76, 2017 Issue 19, pages 1705-1717 DOI: 10.1615/TelecomRadEng.v76.i19.30.

2. Gorbenko I.D., Zamula A. A., Morozov V. L., Rodionov S.V. Mathematical model of orthogonal frequency distribution and multiplexing (OFDM) signals // Радіотехніка. 2019. Вип. 198. С. 32 44.

3. Замула О.А. Технологии формирования OFDM сигналов в современных информационно-коммуникационных системах // Радіотехніка. 2018. Вип. 193. С. 152 159.

4. Sarvate D.V. Crosleration Properties of Pseudorandom and Related Sequences // IEEE Trans. Commun. 1980. Vol. Com 68. P. 59–90.

5. Варакин Л. Е. Системы связи с шумоподобными сигналами. Москва : Сов. радио, 1985. 384 с.

6. Ipatov Valery P. Spread Spectrum and CDMA. Principles and Applications / University of Turku, Finland and St. Petersburg Electrotechnical University 'LETI', Russia. John Wiley & Sons Ltd. The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England. 2005. 385 p.

7. Горбенко І.Д., Замула О.А. Вдовенко С.Г. Аналіз функції невизначеності і структури спектрів ЛЧМ-сигналів // Вісник інженерної академії України. 2018. Вип.2. С.52-56.

8. Горбенко І.Д., Замула О.А. Дослідження структури спектрів сигналів з лінійною частотною модуляцією // Радіотехніка. 2018. Вип. 193. С.192 -199.

9. Gorbenko I.D., Zamula A. A. Cryptographic signals: requirements, methods of synthesis, properties, application in telecommunication systems // Telecommunications and Radio Engineering Vol. 76, 2017. Issue 12, pages 1079-1100. DOI: 10.1615/TelecomRadEng.v76.i12.50.

10. Gorbenko I.D., Zamula A.A., Semenko Ye.A. Ensemble and correlation properties of cryptographic signals for telecommunication system and network applications // Telecommunications and Radio Engineering. Vol. 75, 2016 Issue 2. Pages 169-178. DOI: 10.1615/TelecomRadEng.v75.i2.60.

11. Methods for implementing communications in info-communication systems based on signal structures with specified properties / Gorbenko I., Zamula A., Morozov V. // 2017 4th International Scientific-Practical Conference Problems of Info communications Science and Technology, PIC S and T 2017 Proceedings. DOI: 10.1109/INFOCOMMST.2017.8246359.

12. Gorbenko I. D., Zamula A. A., Semenko A. E., Morozov V. L. Method for complex improvement of characteristics of orthogonal ensembles based on multiplicative combining of signals of different classes // Telecommunications and Radio Engineering Vol. 76, 2017 Issue 18, pages 1581-1594. DOI: 10.1615/TelecomRadEng.v76.i18.10.

13. Горбенко І.Д., Замула О.А., Хо Чі Лик Оптимізація пошуку дискретних складних сигналів з необхідними властивостями для застосування у сучасних інформаційно-комунікаційних системах // Математичне та комп'ютерне моделювання. Серія: Технічні науки : зб. наук. праць / Інститут кібернетики імені В.М. Глушкова Національної академії наук України, 2019. Вип. 19. 160 с.

14. Свердлик М.Б. Оптимальные дискретные сигналы. Москва : Сов. радио, 1975. 200 с.

15. Gorbenko Ivan, Zamula Alexander, Morozov Vladyslav. Information and communication systems based on signal systems with improved properties building concept // Workshop Proceedings 2019 CEUR.

16. Замула А.А., Семенко Е.А Перспективы применения нелинейных дискретных сигналов в современных телекоммуникационных системах и сетях // Системи обробки інформації. Харків : ХУПС, 2015.

Надійшла до редколегії 03.09.2020

Відомості про авторів:

Горбенко Іван Дмитрович – д-р техн. наук, професор, Харківський національний університет імені В.Н. Каразіна, професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, головний конструктор АТ «Інститут інформаційних технологій», Україна, e-mail: GorbenkoI@iit.kharkov.ua, ORCID: https://orcid.org/0000-0003-4616-3449

Семенко Евген Олександрович – Харківський національний університет імені В.Н. Каразіна, пошукач наукового ступеня «кандидат технічних наук», кафедра безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Україна.

Замула Олександр Андрійович – д-р техн. наук, професор, Харківський національний університет імені В.Н. Каразіна, професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Україна, e-mail: zamylaaa@gmail.com, ORCID: http://orcid.org/0000-0002-8973-6190

УДК 681.3.067+621.396.626:537.87 **DOI:10.30837/rt.2020.3.202.10**

В.Р. ВОРОНОВ, канд. техн. наук, В.І. ЗАБОЛОТНИЙ, канд. техн. наук, В.І. ЛИСКО

ВРАХУВАННЯ ІНТЕРФЕРЕНЦІЙНОЇ СКЛАДОВОЇ У ТЕХНІЧНОМУ КАНАЛІ ВИТОКУ ІНФОРМАЦІЇ ПОБІЧНИМИ ЕЛЕКТРОМАГНІТНИМИ ВИПРОМІНЮВАННЯМИ ВІДЕОТРАКТУ ПРИ РОЗНЕСЕНОМУ ПРИЙОМІ

Вступ

Національними стандартами України [1, 2], іншими нормативно-правовими документами системи технічного захисту (ТЗІ) передбачається здійснювати аналіз об’єктів електронно-обчислювальної техніки (ЕОТ), ситуаційного плану, умов функціонування підприємства, установи, організації, оцінювати ймовірність прояву загроз інформації, підготовлювати засадничі дані для побудови окремої моделі загроз. До числа технічних каналів витоку інформації (ТКВІ) можна віднести ведення зацікавленою стороною рознесеного радіоприйому з метою покращання одержання слабких сигналів побічних електромагнітних випромінювань (ПЕМВ) [3]. Оцінка можливостей ведення такої розвідки, як показує практика, може мати певні особливості, які, на думку авторів, необхідно враховувати при побудові окремої моделі загроз інформації.

Задля якісного аналізу і проектування комплексу ТЗІ необхідне математичне моделювання процесів ведення розвідки-захисту інформації на окремих імітаційних моделях, розробка яких базується на розробленій якісній моделі.

Мета статті – обґрунтування необхідності урахування інтерференційної складової, яка впливає на поширення енергії побічних електромагнітних випромінювань відеотрактів засобів ЕОТ при їх рознесеному прийомі засобами розвідки.

Якісна модель ТКВІ ПЕМВ відеотракту при рознесеному прийомі

Дослідження процесів ведення розвідки-захисту для оцінки можливості витоку інформації технічними каналами доцільно розпочинати зі створення якісної моделі із визначенням структури, функціонального призначення і опису окремих елементів. Якісний опис у подальшому формалізується у математичні моделі елементів структури з метою їх всебічного дослідження.

Нехай об’єкт ЕОТ, який планується створювати, буде розташований у виділеному приміщенні певної споруди на певному поверсі. До складу об’єкту ЕОТ входить пристрій візуалізації з типовим відеотрактом, режим роботи якого можна встановлювати необхідним чином (роздільні характеристики, частота оновлення екрану тощо). Місце розташування і орієнтація монітору, з’єднувальні кабелі, системний блок, інші складові ЕОТ обрані за технічними умовами, зручними та необхідними для використання. Орієнтація вектора поляризації ПЕМВ у просторі невизначена і може бути розкладена на вертикальну і горизонтальну складові. ПЕМВ малоспрямовані у просторі.

Місце розташування ЗС відоме. Споруда ЗС може спостерігатися зовні практично безперешкодно. Споруди, інші місцеві предмети, що перешкоджають розповсюдженню ПЕМВ від об’єкту ЕОТ до ЗС, відсутні. Територія споруди ЗС недоступна для власника об’єкту ЕОТ.

Обмежень на характеристики обладнання радіо-, радіотехнічної розвідки (РРТР) для перехоплення ПЕМВ: антен, радіоприймачів, апаратури обробки і аналізу немає.

Орієнтація антен пристрою РРТР може адаптуватися під орієнтацію поляризації поля ПЕМВ для найкращого прийому.

Природно, що ЗС приховує факт ведення розвідки ПЕМВ. Тобто, наявність і розташування розвідувальних антен ЗС приховується. Приховане розташування антен, з мінімізацією ослаблення сигналу ПЕМВ конструкціями споруди ЗС, скоріш за все, може здійснюватися у віконних отворах приміщень ЗС. Можна припустити, що для виключення впливу розвідува-

льних антен ЗС одна на іншу вони рознесені на відстань не менш ніж відстань до сусіднього вікна.

Власник об'єкту ЕОТ не виключає можливості ведення ЗС рознесеного радіоприйому з метою покращання одержання слабких сигналів ПЕМВ [3].

При проектуванні комплексу ТЗІ об'єкту ЕОТ виставлені умови урахування можливості ведення перехоплення ПЕМВ відеотракту зацікавленою стороною (ЗС).

Модель джерела ПЕМВ відеотракту

У якості моделі джерела ПЕМВ обрано модель відеотракту [3], яка призначена для оцінювання рівнів ПЕМВ моніторів ЕОТ і базується на використанні тестових сигналах типу «меандр». Величина довжини імпульсу τ обирається з мінімальним значенням – розміром одного пікселю на екрані монітору. Період повторення тестового імпульсу – 2τ.

З прийнятих умов мінімальна ширина спектру, необхідного для відтворення інформаційного сигналу, визначається як $\Delta f_\tau = 1/\tau$.

Наведене дає змогу визначити параметри тестових сигналів, а саме їх гармонік в ОТЗ за відомим виразом рядом Фур'є:

$$G_i = A\ |sin(\pi i/2)/(\pi i/2)|\ *\ C_s,, \qquad (1)$$

де A – амплітуда імпульсу; i – номер гармоніки тестового сигналу монітору (i=1, 2, …, I); G_i – амплітуда i-ї гармоніки тестового сигналу; C_s – коефіцієнт впливу форми фронтів і спадів імпульсів на спектр ПЕМВ.

Підхід до визначення C_s, що наведений у [4], враховує вплив форми та довжини фронтів і спадів на величину гармонік спектру тестового сигналу ПЕМВ особливо з великими номерами i. Короткі і різкі переходи від нульового до максимального рівня сприяють збільшенню амплітуд гармонік високих номерів, а протяжні і плавні переходи – зменшенню.

Діаграма спрямованості ПЕМВ – малоспрямована. У подальшому значення нормованих діаграм спрямованості на різних гармоніках у різних кутах місця та азимутах прийняті за 1. Таке припущення підтверджується практикою діяльності вимірювань рівнів ПЕМВ у обмежених секторах кутів розповсюдження сигналів у напрямі до ЗС.

Модель розповсюдження ПЕМВ від об'єкту ЕОТ до ЗС

Ситуація захисту ПЕМВ малої потужності, у зоні прямої видимості, коли відстань до місця можливого розташування апаратури РРТР мала і кривизною Землі можна зневажити, приводить до випадку оцінки поширення електромагнітної хвилі над плоскою поверхнею [5]. Доцільність розгляду такої ситуації показана в [6]. Суть цього лежить у явищі складання прямого випромінювання від ЕОТ з відбитим від земної поверхні. Різниця довжин шляхів проходження цих сигналів може привести, у крайніх випадках, як до складання гармонік сигналів у фазі, що підвищує їх рівень, так і у профазі, яке приводить до зменшення сумарного сигналу. Це викривляє вихідний спектр сигналу на вході антен РРТР за рахунок інтерференції сигналів. До речі, наведене явище також приводить і до зміни спектру сигналу перешкод засобів активного захисту (ЗАЗ) від РРТР, яке необхідно враховувати при оцінці ефективності таких перешкод.

Таким чином, до моделі зменшення рівня сигналу ПЕМВ за законом $1/r$ додається інтерференційний множник V, величина якого може обмежуватися значеннями від 0 до 2. Це важливо враховувати як для небезпечного сигналу ПЕМВ, так і для створюваних перешкод ЗАЗ.

Вихідна для аналізу ситуація представлена на рис. 1.

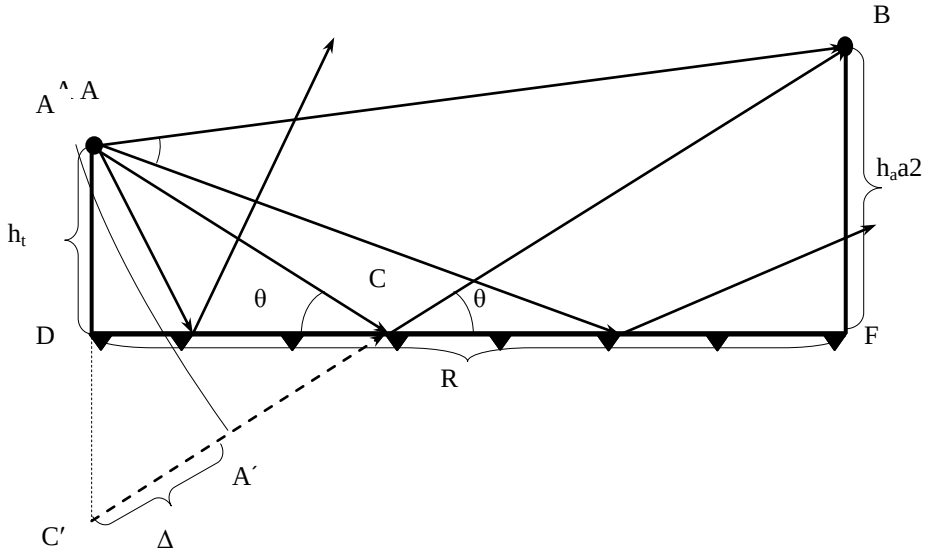


Рис.1. До визначення впливу плоскої Землі на дальність РРТР

Направленість ПЕМВ невисока. Рівень прямого сигналу і сигналу, що спрямований на область відбиття на землі на антену РРТР, вважається однаковим. В залежності від значення кута падіння θ і електродинамічних характеристик ґрунту модуль коефіцієнту відбиття Φ і його фаза β може приймати певні значення, які відповідним чином встановлюються у довідковій літературі.

В точку В приходять дві хвилі: пряма хвиля, яка розповсюджується по шляху АВ, і хвиля, яка віддзеркалена від земної поверхні. В точці С (рис. 1) обидві хвилі складаються. Таким чином, складові гармонік ПЕМВ інтерферують (як збільшуються, так і зменшуються) в точках розташування антени РРТР. Це явище можна характеризувати інтерференційним множником V.

В [5] наведено докладний вивід величин інтерференційного множника послаблення V хвиль:

$$V = \sqrt{1+|\Phi|^2+2|\Phi|\cos\left(2\pi\frac{\Delta}{\lambda}+\beta\right)} \tag{2}$$

Φ – коефіцієнт відбивання хвилі; β – фаза коефіцієнту відбивання; Δ – різниця шляхів проходження прямої та відбитої хвилі.

Даний вираз має два аргументи Φ та β, які можуть бути суттєво різні для горизонтальної та вертикальної поляризації полів ПЕМВ.

Оскільки поляризація ПЕМВ не визначена, то доцільно розглядати дві ортогональні поляризації і, відповідно, два інтерференційних множники $V_г$ та $V_в$:

$$V_в = \sqrt{1+|\Phi_в|^2+2|\Phi_в|\cos\left(2\pi\frac{\Delta}{\lambda}+\beta_в\right)}, \tag{3а}$$

$$V_г = \sqrt{1+|\Phi_г|^2+2|\Phi_г|\cos\left(2\pi\frac{\Delta}{\lambda}+\beta_г\right)}. \tag{3б}$$

Тоді узагальнений множник V через ортогональності полів складових можна представити у вигляді

$$V = \sqrt{V_г^2+V_в^2}. \tag{4}$$

Значення величин $\Phi_г, \beta_г, \Phi_в, \beta_в$ залежать від кутів відбиття θ, електричних параметрів земної поверхні. В свою чергу, згадані величини залежать від температури, вологості тощо.

На рис. 2 наведені графіки, які ілюструють величини $\Phi_г, \beta_г, \Phi_в, \beta_в$ для різних ґрунтів.

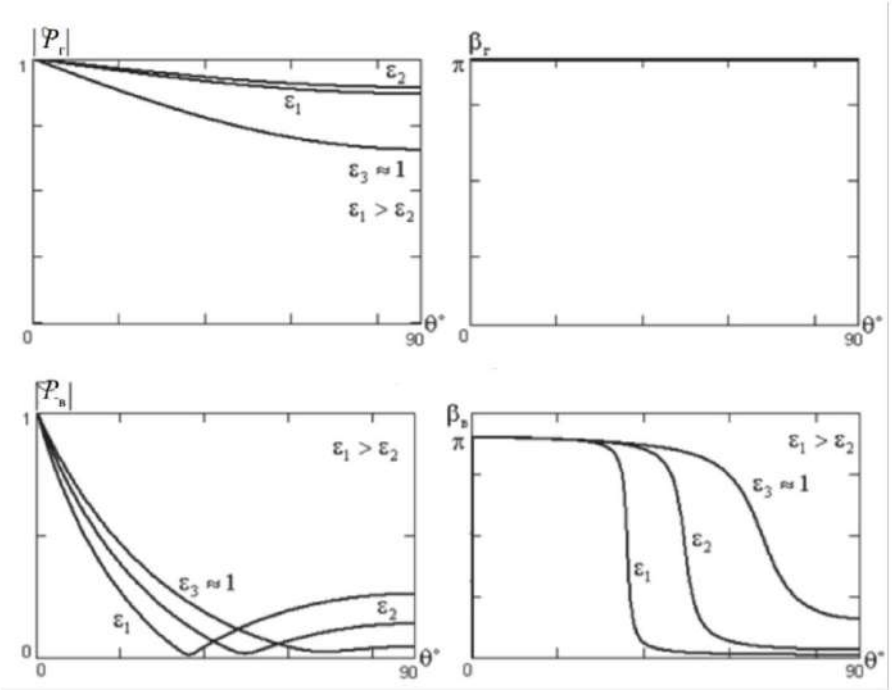


Рис. 2. Графічне представлення $\Phi_г, \beta_г, \Phi_в, \beta_в$ від кута відбиття θ та стану поверхні, що відбиває.

Модель розташування антен РРТР на об'єкті ЗС

Місце розташування кожної антени РРТР на об'єкті ЗС, як зазначено вище, суттєво впливає на рівень прийнятого сигналу.

По-перше, в залежності від різниць фаз прямого і відбитого сигналів. Різниця фаз залежить від співвідношення різниці шляхів проходження прямої та відбитої хвилі та довжини хвилі гармоніки тестового сигналу.

По-друге, від значення величини модуля коефіцієнта відбиття *Ф*. Ця величина визначається величиною поглинання енергії електромагнітного поля речовиною поверхні, що відбиває.

І, по-третє, від кута коефіцієнта відбиття *β*. Це значення визначається реактивною складовою коефіцієнта відбиття *Ф*.

Означене дає підставу для обов'язкового дослідження величин можливих значень інтерференційного множника *V* при оцінці рівня як небезпечного сигналу, так і рівня сигналу перешкод засобів активного захисту.

Завдання моделі – визначити різницю хода прямого і відбитого променів Δ та кут відбиття θ.

Модель базується на очевидних геометричних співвідношеннях взаємного положення джерела ПЕМВ і антени РРТР.

Для практичного моделювання характеристик середовища розповсюдження можна використовувати їх графічне представлення (рис. 2).

Діапазон можливих значень кутів відбиття θ, для обрання області моделювання можна визначити з очевидного виразу $\theta=arctg((h_t+h_a)/R)$. Реально це діапазон кутів $1 – 60^0$.

Для багатьох випадків, що трапляються у практиці ТЗІ, антени РРТР можуть розташовуватися у вікнах фасадної або бічної сторони споруди ЗС. Нескладно, за наявності (фотографічного) зображення відповідної сторони споруди ЗС визначити висоти нижніх і верхніх

частин вікон (з певною точністю, що може бути і не досить критично), розташування рядів вікон одне над одним та їх ширину.

Надалі припускається, що антена РРТР може бути розташована у будь-якій точці площині вікна. Таким чином, можна визначити можливу висоту розташування антени, проекцію відстані між ЗОТ і антеною, кут відбиття ПЕМВ.

В роботі пропонується один із варіантів аналітичних виразів, за якими можна проводити означені розрахунки. Вихідні дані для цього:

R_t – відстань від ЗОТ до площини стіни (до точки T), що співпадає з фасадом (бічною стіною) споруди ЗС, де можуть бути розташовані антени;

x_w – відстань до середини w-го вікна від точки T;

w – номер вікна у поверсі (w = 1, …, W);

b – ширина віконного отвору;

h_a – висота вікна a-го поверху (a = 1, …, A) над поверхнею землі;

s – висота віконного отвору;

a – номер поверху.

Таким чином, можна визначити проекцію відстані між ЗОТ і антеною РРТР w-го вікна:

$$R_w = \sqrt{R_t^2 + (x_w + b(\xi - 1))^2}\,, \tag{5}$$

де ξ – випадкова величина в межах 0 – 1.

Висота розташування антени на a-му поверсі може бути визначена за виразом

$$h_{ra} = h_a + \xi s \tag{6}$$

Ілюстрація ситуації для визначення місця розташування антен РРТР наведена на рис. 3

Рис. 3. Схема врахування розташування об’єкту ЕОТ та ЗС

Означене дозволяє провести розрахунки кута відбиття θ для відповідної антени, розташованої на a-му поверсі у w-му вікні як

$$\vartheta_{aw} = arctg\frac{h_t + h_{ra}}{R_w}\,. \tag{7}$$

Різницю ходу прямого і відбитого променів Δ для відповідної антени, розташованої на a-му поверсі у w-му вікні, можна визначити за виразом

$$\Delta_{aw} = R_w\left(\sqrt{1+\left(\frac{h_t + h_{ra}}{R_w}\right)^2} - \sqrt{1+\left(\frac{h_t - h_{ra}}{R_w}\right)^2}\right). \tag{8}$$

Розрахунок інтерференційного множника ПЕМВ

Одержані вирази дозволяють запропонувати алгоритм оцінки можливих значень інтерференційного множника V.

1. Визначається точка розташування ЗОТ (висота h_t).
2. Визначається положення антени РРТР за висотою h_a (за номером поверху a, розташуванням антени у вікні за висотою – формула (6)).
3. Визначається проекція відстані від ЗОТ до антени РРТР в горизонтальному напрямі (за номером вікна w, положенням антени у вікні по горизонталі – формула (5)).
4. Визначається значення кута відбиття θ_{aw} для відповідної антени, розташованої на a-му поверсі у w-му вікні за формулою (7).
5. За графіками рис. 2 визначаються величини $\Phi_г, \beta_г, \Phi_в, \beta_в$.
6. За формулою (8) обчислюється величина Δ_{aw}.
7. За формулами (3а), (3б) розраховуються два інтерференційних множники $V_г$ та $V_в$ для відповідної антени.
8. За формулою (4) визначається узагальнений множник V для відповідної антени.
9. Подальше прийняття рішення щодо захисту ПЕМВ від розвідки здійснюється за результатами розрахунків для вільного простору, де поле ПЕМВ змінюється за зворотною залежністю від відстані, з урахуванням впливу узагальненого множника V.

За наведеним алгоритмом і даними в якості приклада проведено моделювання значень множника V. При моделюванні використано метод Монте-Карло [7]. Для зручності аналізу одержаних даних величини множника V надані у дБ (рис. 4).

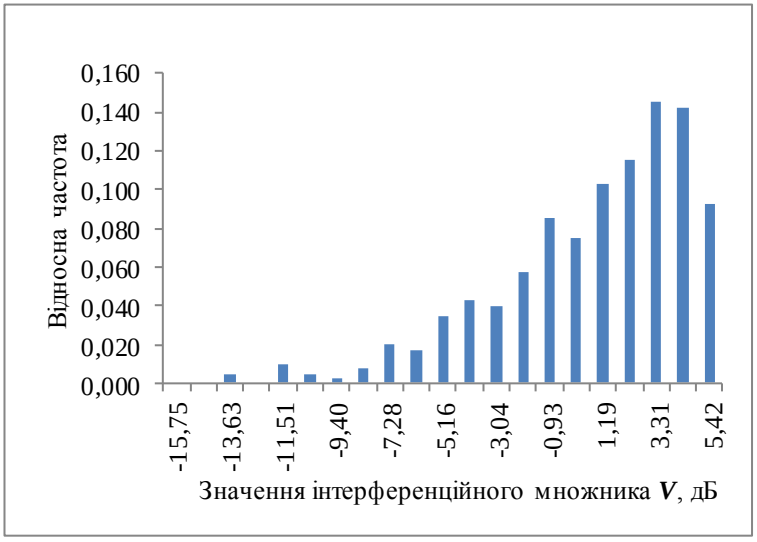


Рис. 4. Можливі значення інтерференційного множника при моделюванні методом Монте-Карло

Одержані значення мають розкид порядку 15 дБ. Така ситуація повинна обов'язково враховуватися при подальших діях з планування заходів захисту.

Оцінка впливу інтерференційного множника розповсюдження ПЕМВ при рознесеному прийомі

Можна запропонувати наступну схему дослідження впливу інтерференційного множника розповсюдження ПЕМВ при рознесеному прийомі.

На рівень сигналу, що сприймає кожна з антен РРТР, впливають ослаблення рівня сигналу за рахунок відстані між ЗОТ і антеною РРТР та інтерференційний множник, величина якого залежить від відстані, висот ЗОТ і антен РРТР над поверхнею землі та електродинамічних характеристик земної поверхні.

Оскільки прийнято, що місце розташування ЗС відоме та фіксоване, то на рівень прийнятого сигналу впливає лише інтерференційний множник V, що приведе до зміни відношення сигнал/шум Δ – у кожному каналі засобу РРТР зміниться у V раз.

При врахуванні можливості ведення ЗС рознесеного радіоприйому з метою покращення одержання слабких сигналів ПЕМВ [3] вираз загального відношення сигнал/шум Δ_Σ можна записати як

$$\Delta_\Sigma = \frac{\sum_i \sum_j \Delta_{ji} V_{ji}}{\sqrt{J}}, \tag{9}$$

де Δ_{ji} – відношення сигнал/шум на j-му каналі на i-й гармоніці прийому; V_{ji} – інтерференційний множник j-го каналу на i-й гармоніці прийому; J – число можливих каналів прийому апаратури РРТР ЗС.

Висновки

Вплив інтерференційного множника приводить до суттєвої невизначеності дальності розповсюдження ПЕМВ засобів ЕОТ. Застосування рознесеного прийому зацікавленою стороною дозволяє покращити розвідку ПЕМВ і збільшити ймовірність успішного рішення задачі перехоплення. Це підтверджує необхідність враховувати технічний канал витоку інформації за рахунок застосування рознесеного прийому зацікавленою стороною.

Запропоновано моделі елементів середовища поширення сигналу у ТКВІ для кількісної оцінки можливості розвідки ПЕМВ в умовах прояву інтерференції.

Визначено підхід для оцінки загального відношення сигнал/шум у ТКВІ рознесеного радіоприйому ПЕМВ засобів ЕОТ.

Запропоновано підхід з визначення обмежень кількості каналів рознесеного прийому, які доцільно враховувати при моделюванні дії засобів розвідки.

Список літератури:

1. ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ Захист інформації. Технічний захист інформації. Основні положення. ДСТУ 3396.0-96.
2. ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96.
3. Воронов В.Р., Заболотний В.І., Лиско В.І. Модель технічного каналу витоку інформації побічними електромагнітними випромінюваннями відеотракту при рознесеному прийомі // Прикладна радіоелектроніка. 2019. Т. 18. №3,4. С. 208-213.
4. Заболотний В.І., Герасименко Є.В., Перепадя В.І. Дослідження змін форми сигналу у каналі побічних електромагнітних випромінювань монітору // Радиотехника. 2014. Вып. 176. С. 116-121.
5. Никольский В.В., Никольская Т.И. Электродинамика и распространение радиоволн: учеб. пособие. 3-е изд. Москва : Наука, 1989. 543с.
6. Заболотний В.І., Ясиновий С.Ю. Дослідження спектрів побічних електромагнітних випромінювань дискретних імпульсів сигналів в умовах впливу навколишнього середовища // Прикладна радіоелектроніка. 2009. Т. 8. №3. С. 359-365.
7. Соболь И. М. Численные методы Монте-Карло. М. : Наука, 1973. 312 с.

Надійшла до редколегії 07.09.2020

Відомості про авторів:

Воронов Віктор Романович – канд. техн. наук, Департамент захисту інформації Адміністрації Держспецзв'язку, e-mail: dzi@dsszzi.gov.ua.

Заболотний Володимир Ілліч – канд. техн. наук, Харківський національний університет радіоелектроніки, професор кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії, Україна, e-mail: volodymyr.zabolotnyi@nure.ua.

Лиско Віктор Іванович – Харківський національний університет радіоелектроніки, магістрант, кафедра безпеки інформаційних технологій, факультет комп'ютерної інженерії, Україна, e-mail: viktor.lysko@nure.ua.

УДК 621.391 **DOI:10.30837/rt.2020.3.202.11**

І.Д. ГОРБЕНКО, д-р техн. наук, О.А. ЗАМУЛА, д-р техн. наук, Хо Чі Лик

КОМПЛЕКСНЕ ВИРІШЕННЯ ПРОБЛЕМИ ЕЛЕКТРОМАГНІТНОЇ СУМІСНОСТІ СУЧАСНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

Вступ

Більшість сучасних інформаційно-комунікаційних систем (ІКС), у тому числі бездротові мобільні системи зв'язку, системи радіонавігації, радіоуправління відносяться до систем, розрахованих на багато користувачів. У таких системах безліч каналів розміщуються в межах загального частотно-часового ресурсу, так що кожен абонент із впровадженням методів дистанційного доступу має можливість передавати і приймати інформацію одночасно з іншими абонентами і незалежно від них. При проектуванні таких систем основною проблемою є вибір способу множинного доступу, тобто можливості одночасного використання багатьма абонентами каналу зв'язку з мінімальним взаємним впливом. При необхідності обслуговування великої кількості абонентів частотно-часовий ресурс повинен бути значним. Одним з методів підвищення ефективності використання діапазону частот є застосування кодового поділу каналів (абонентів), які працюють в загальній смузі частот (CDMA). При такому методі передачі інформації кожному абоненту виділяється широкосмуговий сигнал (ШСС) з безлічі сигналів, і кожен сигнал займає всю смугу і весь часовий інтервал. Безумовно, саме для таких бездротових ІКС проблема електромагнітної сумісності є однією з найбільш пріоритетних. Електромагнітна сумісність (ЕМС) має на увазі безконфліктне існування різних радіотехнічних систем (в тому числі ІКС) в умовах, коли кожна з цих систем має можливість приймати свої сигнали і сигнали інших систем. Завданням розробника (користувача) системи (наприклад, ІКС) є вилучення або зведення до допустимого рівня негативного впливу системи (наприклад, випромінювання електромагнітних хвиль) на інші системи. До числа методів забезпечення ЕМС відносять: частотне планування у відповідності до вимог міжнародних і національних нормативних документів, контроль за дотриманням яких здійснюють відповідні інституції (служби); застосування антен з вузькою направленістю; ретельна розробка високочастотних вузлів та ін. На наш погляд, проблема ЕМС для сучасних бездротових ІКС може бути вирішена завдяки впровадженню технології розподіленого спектру.

Основні результати досліджень

Основними напрямками побудови ІКС з багатостанційним доступом на основі технології розподіленого спектру, на наш погляд, є: синтез та вибір ансамблів сигналів та сигнально-кодових конструкцій на їх основі в залежності від умов функціонування ІКС; розробка оптимальних і квазіоптимальних алгоритмів і пристроїв їх обробки, які забезпечують виявлення, пошук, оцінювання параметрів сигналів в умовах різного роду параметричної і непараметричної апріорної невизначеності відносно статистичних характеристик сигналів, каналів на фоні усієї сукупності можливих завад; синтез алгоритмів і пристроїв слідкування за часовим зміщенням, частотою і фазою складних ШСС. Крім того, не менш важливим напрямом підвищення ефективності ІКС з багатостанційним доступом на основі кодового поділу каналів є підвищення точності синхронізації ШСС за часом і частотою у сукупності з кодовою адресацією безлічі абонентів. При цьому об'єм ансамблів сигналів і бази ШСС повинні бути значними. Це дозволить підвищити пропускну здатність багатопроміневих каналів на основі виміру з високою точністю параметрів ШСС в умовах багатостанційного доступу при роботі у загальній смузі частот одночасно безлічі абонентів.

Застосування ШСС (з метою синхронізації, а також як фізичних переносників даних) в ІКС дозволяє забезпечити високоефективне використання смуги частот, високу завадостійкість пристроїв обробки сигналів, скритність і конфіденційність передачі інформації при впливі всієї сукупності шумових, структурних, зосереджених, вузькосмугових, імпульсних,

імітаційних, ретрансляційних і інших завад при наявності завмирань в радіоканалах, які обумовлені як умовами розповсюдження сигналів, так і багатопроміневістю каналів зв'язку.

При асинхронному способі множинного доступу абонентів до інформаційних ресурсів ІКС затримки різних сигналів на вході приймального пристрою можуть змінюватися в широкому діапазоні. В цьому випадку процедура синхронізації ШСС (сигнатур) стає проблематичною. Зазначене обумовлено тим фактом, що сигнатури різних абонентів володіють спектрами, що перекриваються, і тому не можуть залишатися ортогональними в широкому діапазоні взаємних затримок. Наслідком зазначеного є виникнення завад множинного доступу, проявом яких служить ненульовий відклик приймача, який налаштовано на *i*-го абонента, від сигналів інших абонентів. Для додатків ІКС, в яких використовується асинхронний метод з CDMA, вибір сигналів необхідно здійснювати таким чином, щоб мінімізувати взаємні перешкоди, тобто забезпечити електромагнітну сумісність.

При вивченні проблеми ЕМС будемо вважати, що в процесі інформаційного обміну беруть участь дві сторони. Перша з них – це система, що здійснює передачу даних (назвемо її «система, що аналізується»). Друга – це система, що наближена до першої («стороння» система»). Для системи, що аналізується, сигнали сторонньої системи можуть трактуватися як завади (вузькосмугові, загороджувальні шумові, внутрішні, структурні, ретрансляційні і ін.). Так само будемо вважати, що в каналі діє найбільш характерний вид завади, що описується гаусівським випадковим процесом, спектр якого збігається зі спектром сигналу. При такому підході ймовірність помилки залежить тільки від відношення потужності сигналу до потужності загального впливу, що заважає.

Характерною ситуацією для практики впливу на нормальне функціонування ІКС, є вузькосмугова завада. Причому даний тип завад може бути реалізовано як станцією протидії з метою порушення роботи системи, так і сусідніми станціями, що створюють перешкоди внаслідок свого звичайного функціонування.

Розглянемо два випадки. По перше, припустимо, що ІКС не впроваджує заходів щодо протидії заваді за виключенням вибору відповідного класу сигналів, тобто система не є адаптованою і у ній не запроваджуються заходи щодо вибору закону модуляції або алгоритму обробки сигналу відповідно до існуючої завадової обстановки. Тоді відношення q_i^2 потужності сигналу до завадового впливу на виході узгодженого фільтру може бути визначено як [1]

$$q_i^2 = 2 \cdot E / (N_0 + P_j / F), \qquad (1)$$

де E – енергія сигналу; F – смуга частот, яку займає сигнал; P_j – потужність сигналу; N_0 – спектральна щільність потужності шуму.

Аналіз останнього виразу свідчить, що не дивлячись на те, що вузькосмугова завада має відповідне значення смуги F_j, відношення q_i^2 приймає таке ж значення, якби потужність завади була рівномірно розподілена у смузі F сигналу, утворюючи додатковий абелевий білий гаусів шум (АБГШ) зі спектральною щільністю P_j / F.

Ішим варіантом є пристосування приймального пристрою до вузькосмугової завади. При такому варіанті оптимальною процедурою обробки є фільтрація, яка враховує завадовий вплив із урахуванням вузькосмугової завади. Така обробка по суті еквівалентна видаленню смуги частот, у якій зосереджена завада. Але при цьому виявляється видаленими і компоненти сигналу, які знаходяться у межах тієї ж смуги частот завади. У такому разі енергія сигналу (оскільки сигнал займає тільки частину полоси F, яка вільна від завади) дорівнює $E \cdot (1 - F_j / F)$, де F_j – смуга частот, яку займає завада. Тоді узгоджений фільтр забезпечує відношення сигнал шум у вигляді

$$q_j^2 = 2 \cdot E \cdot (1 - F_j / F) / N_0 = q^2 \cdot (1 - F_j / F), \qquad (2)$$

де $q^2 = 2 \cdot E / N_0$ – відношення потужностей сигналу та шуму на виході узгодженого фільтру при відсутності завади.

Аналіз відношень (1) – (2) показує, що чим ширше смуга сигналу F у порівнянні з полосою завади F_j, тим менша додаткова спектральна щільність у першому випадку та енергетичні втрати – у другому і, відповідно, більше q^2 і q_j^2.

Таким чином, досягнення високої завадостійкості прийому сигналів при впливі вузькосмугової завади, не вдаючись до збільшення енергії сигналу або пікової потужності сигналу, можливо тільки при розширенні спектру сигналу незалежно від його тривалості. Зазначене безумовно має велике значення для вирішення проблеми електромагнітної сумісності при функціонуванні широкосмугової ІКС і системи, що займає смугу частот, яка менша смуги ІКС і є області, де спектр сигналу не схильний до спотворення завадою.

Можливим сценарієм, який не може бути залишеним без уваги (якщо проводиться аналіз проблеми електромагнітної сумісності ІКС, розрахованих на багато користувачів), є функціонування сторонньої (по відношенню до системи, яка аналізується) системи, спектр якої покриває (без проміжку) спектр системи. Така завада (назвемо її «загороджувальна шумова завада») впливає на сигнал як додатковий АБГШ зі спектральною щільністю потужності, що дорівнює $N_j = P_j / F$. Тому відношення сигнал-завада на виході узгодженого фільтру системи, яка аналізується, буде визначатися як

$$q_j^2 = 2 \cdot E \cdot (N_0 + N_j) = 2 \cdot E / (N_0 + P_j / F). \quad (3)$$

При розгляді сценарію впливу загороджувальної завади як окремий випадок можна припустити, що відношення P_j/F буде суттєво перевищувати спектральну щільність потужності шуму N_0. Такий випадок є цілком припустимим, якщо мати на увазі, що стороння система буде прагнути здійснити ефект придушення, що істотно більший, ніж це можливо при впливі білого шуму. Тоді відношення (3) набирає вигляду

$$q_j^2 = 2 \cdot E \cdot F = 2 \cdot P \cdot (F \cdot T) / P_j. \quad (4)$$

Аналіз (4) показує, що при накладенні обмежень на пікову потужність сигналу системи, що аналізується, та потужність сигналу сторонньої системи, єдиним шляхом вирішення проблеми ЕМС систем при впливі з боку однієї з систем шумової загороджувальної завади є застосування сигналів з великим значенням частотно-часового добутку $F \cdot T$, тобто ШСС (технології розподіленого спектру).

Результати, що наведені вище, справедливі для випадку, коли завада є нормальним випадковим процесом і має рівномірну спектральну щільність. Стороння система може в процесі інформаційного обміну використовувати сигнали, подібні (з точки зору закону маніпуляції) тим, які використовує система, яка аналізується, створюючи так звані структурні взаємні завади з нерівномірним спектром. В таких умовах, внаслідок роботи великого числа абонентів в загальному частотному діапазоні, показники завадостійкості прийому сигналів в ІКС в значній мірі визначаються подібністю (відмінністю) структур сигналу і перешкоди, тобто тим, як придушуються окремі елементи сигналу завадою.

Розглянемо вплив взаємної завади на завадостійкість прийому даних в ІКС.

Нехай ширина загальної смуги частот системи дорівнює F. Припустимо, що ширина спектра всіх сигналів в ТКС дорівнює ширині загальної смуги частот і всі активні абоненти l створюють на вході *k*-го приймача сигнали однакової потужності P_C. У цьому випадку потужність взаємної перешкоди, яка утворюються l абонентами, буде дорівнювати $l \cdot P_C$. Припустимо, що спектральна щільність потужності Nv взаємної завади постійна в межах загальної смуги частот:

$$Nv = \frac{l \cdot P_C}{F}, \tag{5}$$

і взаємна заваду (за своїми статистичними властивостями) наближається до нормального випадкового процесу. Таким чином, зроблені припущення дозволяють вважати взаємну заваду нормальним випадковим процесом з рівномірною спектральною щільністю потужності. Неважко переконатися, що відношення сигнал – шум на вході вирішального пристрою приймача визначається з виразу

$$q^2 = \frac{B}{l} = F \cdot R / l, \tag{6}$$

де R – швидкість передавання інформації.

З (6) випливає, що при заданому числі активних абонентів l збільшення завадостійкості можливо тільки за рахунок збільшення бази (B) сигналів. Це пояснюється тим, що зі збільшенням бази (зі збільшенням ширини спектра сигналів при постійній швидкості передачі інформації R) зменшується спектральна щільність потужності завади $N_П$.

У практиці роботи ІКС можливі випадки, коли потужність одного або декількох сигналів, що заважають у багато разів більше потужності корисного сигналу. Яким чином в цих умовах забезпечити необхідну завадозахищеність.

Нехай потужність корисного сигналу P_C, а потужність сигналу сторонньої станції $P_П$ Потужність сигнальної складової на виході узгодженого фільтра в момент прийняття рішення пропорційна P_C, а потужність складової, що викликана дією завади – $P_П \cdot R_{jk}^2(\tau)$, де $R_{jk}(\tau)$ – взаємнокореляційна функція (ВКФ) корисного *k*-го сигналу і *j*-го сигналу, що заважає. Величина τ визначається зміщенням ВКФ щодо моменту відліку. Відношення сигнал/перешкода на виході пристрою оптимального прийому визначається співвідношенням [2]:

$$q^2(\tau) = \frac{P_C}{P_П \cdot R_{jk}^2(\tau)}, \tag{7}$$

Найменше відношення сигнал/завада

$$q^2(\tau) = \frac{P_C}{P_П \cdot R_{max}^2(\tau)}, \tag{8}$$

де R_{max} – є максимальне значення $R_{jk}(\tau)$.

З (8) стає очевидним, що для підвищення завадозахищеності ІКС необхідно вибирати сигнали, у яких максимальні піки ВКФ мінімальні.

Якщо максимальні піки ВКФ зменшені до середньоквадратичного рівня складає $\sigma_{j,k} = \sigma^2$, то відношення сигнал/завада дорівнюватиме

$$q^2(\tau) = \frac{P_C}{P_П} \cdot \sigma^2. \tag{9}$$

Наприклад, якщо $\sigma^2 = \frac{1}{2 \cdot F \cdot T}$, то

$$q^2(\tau) = \frac{P_C}{P_П} \cdot F \cdot T. \tag{10}$$

Для дискретних фазоманіпульованих широкосмугових сигналів (ФМШПС) $\sigma^2 = \frac{1}{2 \cdot N}$ (де N – число елементів сигналу). Для такого класу сигналів відношення сигнал/завада визначається з виразу

$$q^2(\tau) = \frac{P_C}{P_П} 2 \cdot N . \qquad (11)$$

З виразів (10) – (11) випливає, що збільшення бази сигналу призводить до збільшення q^2 (а значить, до збільшення завадостійкості прийому сигналів в системі) і може компенсувати зменшення відношення $\frac{P_C}{P_П}$ в разі, коли стороння станція вибере стратегію збільшення потужності завади ($P_П$).

Для реалізації вимог ЕМС різних додатків ІКС задача полягає у отриманні такого виграшу від обробки сигналу, який би гарантував достатньо низький рівень спектральної щільності сигналу, що використовується відносно спектральної інтенсивності природнього шуму на вході приймального пристрою сторонньої системи. Застосування широкосмугових сигналів (ШСС) дозволяє поліпшити показники завадостійкості прийому сигналів в ІКС при впливі вузькосмугових, структурних (взаємних), ретрансльованих і організованих завад. При цьому реальна завадостійкість буде нижчою за потенційну. Причинами зниження завадостійкості при входженні в синхронізм і при розрізненні сигналів є наявність бічних піків кореляційних функцій (КФ).

Як критерій вибору класу дискретних сигналів, які використовуються в системах, розрахованих на багато користувачів, як правило, орієнтуються на критерій мінімуму взаємних завад (мінімаксний критерій). Такий критерій має передбачає побудову ансамблів сигналів обсягу K, маніпульованих ДП, як можна помітніше відрізняються один від одного. Причому типовим для теорії зв'язку є підхід, що полягає у використанні безлічі сигналів, що володіють щонайменше однією з наступних властивостей:

1) кожен з сигналів даної безлічі легко відрізнити від своєї зрушеною за часом копії;

2) кожен з сигналів даної безлічі легко відрізнити від будь-якого іншого (в тому числі, зрушеного в часі) сигналу цієї множини.

Перша властивість важлива для радіолокаційних систем, систем синхронізації, а також для широкосмугових систем зв'язку, друга – для систем, розрахованих на багато користувачів, з кодовим поділом абонентів. Найчастіше використовуваним критерієм розрізнення є середньоквадратична відстань. Критерій полягає в тому, що два сигнали, що легко розрізнюються, тоді і тільки тоді, коли середньоквадратична відстань між ними значна. Будемо вимагати також, щоб сигнал $Y(t)$ відрізнявся не тільки від сигналу $X(t)$, але і від $-X(t)$. Необхідність спільного розгляду $Y(t)$ і $X(t)$ виникає при використанні маніпуляції, наприклад в тих випадках, коли сигнал модулюється двійковою послідовністю або коли їм самим модулюється деяка несуча. Таким чином, в якості запобіжного розрізнення сигналів будемо використовувати величину [3]:

$$T^{-1}\int_0^T \left[Y(t) \pm X(t) \right]^2 = -T^{-1}\left\{ \int_0^T \left[Y^2(t) + X^2 \right] dt \pm 2\int_0^T X(t) \cdot Y(t) dt \right\}, \qquad (12)$$

де T – період сигналів $X(t)$ и $Y(t)$.

Перший інтеграл в правій частині (12) є сума енергій сигналів $X(t)$ і $Y(t)$, $0 \le t \le T$. Отже, при фіксованих енергіях сигнал $Y(t)$ сильно відрізняється як від сигналу $X(t)$, так і від сигналу $-X(t)$ тільки в тому випадку, коли параметр

$$r = \int_0^T X(t) \cdot Y(t) dt \tag{13}$$

малий. Параметр r в системах зв'язку, які використовують узгоджену фільтрацію або кореляційний прийом, має сенс відгуку узгодженого з сигналом $Y(t)$ фільтра на вхідний сигнал $X(t)$. Наприклад, якщо в системі зв'язку з багатостанційним доступом сигнали $Y(t)$ і $X(t)$ виділені двом різним станціям, то параметр r є мірою рівня взаємних завад, які створюються кожним із сигналів прийому іншого.

У виразі (12) сигнали $X(t)$ і $Y(t)$ вважалися дійсними. Для переходу до комплексно-значної форми представлення сигналів досить замінити $Y(t)$ комплексно-поєднаним сигналом. У більшості додатків практичний інтерес представляють сигнали, які є послідовностями елементарних імпульсів кінцевої тривалості. Такий сигнал можна записати у вигляді

$$X(t) = \sum_{n=-\infty}^{\infty} x_n \cdot a(t - n \cdot T_c), \tag{14}$$

де $a(t)$ – функціональний вид елементарного імпульсу, T_c – його тривалість.

Якщо умова (14) виконується для всіх t, то період T повинен бути кратний T_c, а послідовність повинна бути з періодом, який дорівнює $N = T / T_c$. Якщо $X(t)$ і $Y(t)$ – періодичні сигнали, і $X(t)$ задається виразом (14), а $Y(t)$ має вигляд

$$Y(t) = \sum_{n=-\infty}^{\infty} Y_n \cdot a \cdot (t - n \cdot T_c), \tag{15}$$

то, у такому випадку, вираз (13) для параметра r зводиться до виду

$$r = \lambda \cdot \sum_{n}^{N-1} X_n \cdot Y_n, \tag{16}$$

$$\text{де} \quad \lambda = \int_0^{T_c} a^2(t) dt. \tag{17}$$

Якщо $a(t) = P \cdot T_c(t)$ – прямокутний імпульс одиничної амплітуди і тривалості T_c, $\lambda = T_c$. Згідно з (16) скалярний добуток двох періодичних сигналів з безперервним часом пропорційний скалярному добутку відповідних дискретних векторів $(x_0, x_1, x_2, ..., x_{N-1})$ і $(x_0, x_1, x_2, ..., x_{N-1})$. Узагальнивши (16) на випадок $r = l \cdot T_c$, отримаємо

$$r_{x,y}(r) = \lambda \cdot \sum_{n=0}^{N-1} X_n \cdot Y_{n+1} \tag{18}$$

що дорівнює скалярному добутку векторів $(x_0, x_1, x_2, ..., x_{N-1})$ і $(y_0, y_1, y_2, ..., y_{N-1})$, помноженому на постійну λ (17).

Наведені міркування є достатньою мотивацією для розгляду періодичної функції взаємної кореляції (ПФВК) послідовностей (X_n) і (Y_n), яка визначається співвідношенням

$$\theta_{x,y}(l) = \sum_{N=0}^{N-1} X_n \cdot Y_{n+1}. \tag{19}$$

З (18) слід, що при $r = l \cdot T_c$, $r_{x,y}(r) = \lambda \cdot \theta_{x,y}(l)$.

При довільних r значення $r_{x,y}(r)$ також визначається ПФВК. Наприклад, якщо $a(t) = P \cdot T_c(t)$, то при любому $0 \le r \le T$

$$r_{x,y}(r) = T_c \cdot \theta_{x,y}(l') + (r - l'T_c) \cdot \left[\theta_{x,y}(l'+1) - \theta_{x,y}(l') \right], \tag{20}$$

де l – найбільше ціле, таке, що $l \cdot T_c \le r$. Відзначимо також, що незалежно від функціонального виду імпульсу $a(t)$

$$\max \left\{ \left| r_{x,y}(r) \right| : 0 \le r \le T \right\} = \lambda_{max} \left\{ \left| \theta_{x,y}(t) \right| : 0 \le l \le N-1 \right\}. \tag{21}$$

Оскільки періодичні кореляційні параметри сигналів (14) і (15) з безперервним часом повністю визначаються взаємно-кореляційною функцією (ВКФ) відповідних послідовностей, завдання синтезу сигналів зводиться до пошуку множин періодичних послідовностей з наступними властивостями:

для будь-якої послідовності $X = (x_n)$ функція $\left| \theta_{x,y}(l) \right|$ мала при всіх $1 \le l \le N-1$;

для будь-якої пари послідовностей $X = (x_n)$ и $Y = (y_n)$ функція $\left| \theta_{x,y}(l) \right|$ мала при всіх 1.

В [3] отримано границі для середньоквадратичних і максимальних (пікових) значень авто- і ВКФ. Пікове значення ВКФ θ_c можна представити у вигляді

$$\theta_c = \max\{ \left| \theta_{x,y}(l) \right| : 0 \le l \le N-1,\ x \in X, y \in X, x \ne y \}, \tag{22}$$

де X _ безліч періодичних дискретних послідовностей.

Максимальне значення бокового піку (пелюстки) автокореляційної функції представимо у вигляді

$$\theta_a = \max\{ \left| \theta_x(l) \right| : 1 \le l \le N-1, x \in X \}, \tag{23}$$

Якщо X – це ансамбль, який складається з K послідовностей, то

$$\left(\frac{\theta_c^2}{N} \right) + \frac{N-1}{N \cdot (K-1)} \left(\frac{\theta_a^2}{N} \right) \ge 1. \tag{24}$$

З (24) слід:

$$\theta_{max} \overset{\Delta}{=} \max\{\theta_a, \theta_c\} \ge N \cdot \left[\frac{K-1}{N \cdot K - 1} \right]^{1/2}. \tag{25}$$

В [4] вказані принципово досяжні значення максимальних бічних піків періодичної функції автокореляції (межі «щільної упаковки») для заданого періоду послідовності N:

$$\theta_{a_{max}} \ge \begin{cases} 0, \text{если } N \equiv 0 \pmod 4 \\ 1, \text{если } N \ne 1 \pmod 4 \\ 2, \text{если } N \equiv 2 \pmod 4 \\ -1, \text{если } N \ne 3 \pmod 4 \end{cases}. \tag{26}$$

Дані значення можуть бути досягнуті для ряду класів дискретних послідовностей: *m*-послідовності, характеристичні коди, багатофазні послідовності (коди Чу, коди Франка), трійчасті послідовності і ін. В [1, 2, 4] запропоновано методи формування і результати дослідження властивостей зазначених сигналів.

Границі (24) задовольняють деякі пари m-послідовностей (кращі пари), що володіють трирівневою функцією взаємної кореляції. Однак для більшості додатків, зокрема, для широкосмугових систем з багатостанційним доступом, інтерес представляють не пари, а великі безлічі послідовностей з хорошими взаємно-кореляційними властивостями. У деяких системах число одночасно використовуваних послідовностей може перевищувати сотні тисяч. Відомі періодичні послідовності (безлічі Касамі, Голда), що володіють покращеними (у порівнянні з *m*-послідовностями) взаємно-кореляційними і ансамблевими властивостями. При цьому правила побудови зазначених класів послідовностей обумовлюють їх низьку структурну скритність, і отже, сигналів, що формуються на їх основі, і які є фізичними переносниками даних у ІКС. Під структурною скритністю розуміється складність визначення сторонньою системою (станцією протидії) правила (закону) побудови дискретної послідовності, що використовується для утворення широкосмугового сигналу.

Дослідження [5, 6] показали, що дискретні послідовності (ДП), які розширюють спектр, повинні бути засновані на нелінійних правилах побудови і мати покращені кореляційні, ансамблеві і структурні властивості. Зокрема, при використанні таких сигналів як фізичного переносника інформації або сигналів синхронізації, часові витрати на розкриття структури використовуваних сигналів зростають і постановка «оптимальних», з точки зору станції протидії, завад стає проблематичною.

В [6, 7] сформульовано у загальному вигляді і вирішено задачу синтезу нового класу сигналів-фізичних переносників даних для застосування у сучасних ІКС, – нелінійних складних дискретних криптографічних сигналів (КС). Під КС пропонується розуміти сукупність послідовностей (векторів) символів певного алфавіту, які мають необхідні (задані) структурні, ансамблеві і кореляційні властивості, часову і просторову складності. Правила побудови КС ґрунтуються на використанні випадкових або псевдовипадкових процесів (в тому числі, із застосуванням алгоритмів криптографічного перетворення інформації), які повинні відповідати вимогам випадковості, незворотності, непередбачуваності і ін. [8]. Необхідно відзначити особливу властивість систем КС: можливість їх відновлення в просторі і в часі із застосуванням ключів. Закон формування кожного з КС визначається ключем, причому довжина ключа може бути суттєво менше періоду (тривалості) самого сигналу. У табл. 1, 2 наведені результати досліджень ансамблевих і кореляційних властивостей різних класів, в тому числі криптографічних сигналів, що дозволяють проілюструвати можливість застосування КС для ряду додатків ІКС [9, 10]. Так, в табл. 1 представлено результати синтезу дискретних послідовностей для деяких значень періоду дискретних послідовності (ДП), зокрема, наведені: граничні значення для максимальних викидів кореляційних функцій (границі «щільної упаковки» [2]); кількість пар послідовностей, що складає повний ансамбль сигналів; кількість сигналів, які за своїми кореляційними властивостями відповідають граничним значенням. У табл. 2 наведені дані щодо числа пар послідовностей різного класу (*m*-послідовності, послідовності з трирівневою функцією взаємної кореляції – ПФВКТ, криптографічні послідовності (КП)), які відповідають граничним значенням («щільній упаковці») для відповідного числа елементів послідовності.

Таблиця 1

Число елементів ДП	Граничні значення ПФВК («щільної упаковки»)	Загальне число пар ДП	Число пар ДП, ПФВК яких задовольняє границі «щільної упаковки»	Найменше значення $R_{бmax}$
64	17	45 553 512	5 451 589	10
63	17	59 056 712	12 214 869	11
127	25	23 106 402	1 266 098	19
127	27	50 060 018	9 006 648	19
511	63	29 353 122	2 666 671	51
1 023	100	36 235 584	5 293 538	81
1 024	90	2 439 840	26 638	82

Таблиця 2

Клас сигналів	Число елементів ДП	Досяжне значення ПФВК для відповідного класу сигналів (границя «щільної упаковки»)	Число пар ДП, ПФВК яких задовольняє границі «щільної упаковки»
m-послідовності	31	9	3
ПФВКТ	31	9	495
КП	31	9	1465137
m-послідовності	127	27	36
ПФВКТ	127	17	11610
КП	127	23	47 053
m-послідовності	255	36	28
ПФВКТ	_	_	_
КП	255	36	17599
m-послідовності	511	63	276
ПФВКТ	511	33	147500
КП	511	63	2666671
m-послідовності	1023	100	435
ПФВКТ	1023	65	338000
КП	1023	100	5293538

Аналіз даних табл. 1, 2 показує, що запропонований метод синтезу криптографічних сигналів [7] дозволяє формувати великі ансамблі дискретних послідовностей практично будь-якого періоду з заданими, але фізично реалізованими, обмеженими границями «щільної упаковки» (24), (25) значеннями бічних пелюсток авто -, взаємної і стикової функцій кореляції в періодичному і аперіодичному режимах роботи, а також статистичними характеристиками кореляційних функцій, які не поступаються аналогічним характеристикам кращих лінійних класів сигналів. Так, для періоду послідовності $N=63$ число пар криптографічних ДП, які відповідають відомому граничному значенню максимальних бічних пелюсток ПФВК – 17, становить 12 214 869. Для представника класу лінійних послідовностей – послідовностей з трирівневою функцією взаємної кореляції (наприклад, безлічі Голда, які є оптимальними з точки зору ФВК [2]), число пар сигналів, які відповідають даній границі, становить – 975. Перевищення обсягу криптографічних сигналів над ансамблем, складеним з *m*-послідовностей, становить більш ніж 10^7 разів. Для періоду послідовності 1023 елементи, число пар криптографічних ДП, що задовольняють встановленому граничному значенню для бічних пелюсток ФВК – 100, становить 5293538, тоді як для *m*-послідовностей число пар, які відповідають даній границі, становить – 435 , тобто перевищення обсягу системи КС становить більш ніж 10^5 разів. Особливості процесів синтезу КС дозволяють варіювати пріоритетністю у досягненні необхідних (для відповідних додатків ІКС) показників ефективності функціонування таких систем. Це обумовлено, насамперед, можливістю проводити синтез КС для будь-якого числа елементів ДП і встановлювати при цьому необхідне граничне значення максимальних бокових пелюсток ФВК, яке у свою чергу визначає фактичні показники завадостійкості прийому сигналів. При незначному зниженні вимог до граничного значення максимального бічного піку ВКФ, відповідно до якого здійснюється відбір сигналів як фізичних переносників даних (по суті, зниження завадостійкості прийому), можуть бути суттєво поліпшені показники захищеності від нав'язування (вводу) хибних даних, режимів роботи ІКС тощо. Саме показники захищеності від імітації, нав'язування, порушення цілісності даних суттєво залежать від ансамблевих властивостей (об'єму ансамблю) застосовуваних систем сигналів. Так, для періоду послідовності $N = 127$ збільшення значення границі допустимих максимальних бокових піків ФВК на 1,2 дБ відносно границі «щільної упаковки» ($R_{б\max} = 17$), дозволить збільшити об'єм ансамблю з $M = 11610$ до 9 006 648 сигналів, тобто в 776 разів.

Виконані розрахунки і проведене імітаційне моделювання свідчить про те, що значення максимальних бічних викидів кореляційних функцій КС, а також статистичні характеристики даного класу сигналів не поступаються відповідним характеристикам лінійних *m*-послідовностей [9].

Висновки

Комплексне вирішення проблем забезпечення електромагнітної сумісності (ЕМС), завадозахищеності та інформаційної безпеки функціонування ІКС, розрахованих на багато користувачів, може бути досягнуто, в тому числі, на основі використання в якості фізичних переносників даних нелінійних дискретних широкосмугових систем сигналів. Пропоновані в роботі нелінійні дискретні криптографічні сигнали, на відміну від відомих класів сигналів, використовуваних в різних додатках ІКС, формуються на основі випадкових (псевдовипадкових) процесів, в тому числі із застосуванням алгоритмів криптографічного перетворення даних, і можуть бути синтезовані для будь-яких значень періоду дискретних сигналів. Системи КС мають структурні властивості, які притаманні аналогічним властивостям випадкових (псевдовипадкових) послідовностей. Синтез даного класу сигналів ґрунтується на обмеженнях, пов'язаних з граничними значеннями функцій авто- і взаємної кореляції сигналів в періодичному і аперіодичному режимах передачі інформації. Характеристики авто – і взаємних функцій кореляції таких сигналів не поступаються характеристикам кращих, з точки зору кореляційних властивостей, лінійних дискретних послідовностей. Обсяг системи нелінійних КС визначається, по-перше, вимогами, зумовленими сферою застосування даного класу сигналів і, по-друге, – вимогами, що пред'являються до системи, з точки зору таких показників ефективності функціонування ІКС, як ЕМС, завадостійкість прийому сигналів, інформаційна безпека системи. Показано, що варіюючи граничними значеннями рівня бічних пелюсток відповідної функції кореляції, в залежності від вимог, що висуваються до ІКС, можна вирішити завдання досягнення необхідних значень показників завадостійкості прийому сигналів і інформаційної безпеки ІКС.

Список літератури:

1. Ipatov, Valery P. Spread Spectrum and CDMA.Principles and Applications / Valery P. Ipatov. University of Turku, Finland and St. Petersburg Electrotechnical University ‘LETI’, Russia. John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England. 2005. 385 p.

2. Варакин Л. Е. Системы связи с шумоподобными сигналами. 1985. 384 с.

3. Sarvate D.V. Crosleration Properties of Pseudorandom and Related Sequences / D.V. Sarvate, M.V. Pursley // IEEE Trans. Commun, 1980. Vol. Com 68 P. 59–90.

4. Свердлик М. Б. Оптимальные дискретные сигналы. Москва : Радио и связь, 1975. 200 с.

5. Gorbenko I., Zamula A., Morozov V. Information and communication systems based on signal systems with improved properties building concept systems with improved properties building concept 2019 CEUR Workshop Proceedings.

6. Горбенко І.Д., Замула О.А., Хо Чі Лик Оптимізація пошуку дискретних складних сигналів з необхідними властивостями для застосування у сучасних інформаційно-комунікаційних системах // Математичне та комп’ютерне моделювання. Серія: Технічні науки : Зб. наук. праць / Інститут кібернетики імені В.М. Глушкова Національної академії наук України, 2019. Вип. 19. 160 с.

7. Gorbenko I., Zamula A. Cryptographic signals: requirements, methods of synthesis, properties, application in telecommunication systems // Telecommunications and Radio Engineering Volume 76, 2017. Issue 12, pages 1079-1100. DOI: 10.1615/TelecomRadEng.v76.i12.50.

8. Application Notes and Interpretation of the Scheme (AIS) 31. Functionality classes and evaluation methodology for physical random number generators. Certification body of the BSI in context of certification scheme. BSI, 2001.

9. Gorbenko I.D., Zamula A.A., Semenko Ye.A. Ensemble and correlation properties of cryptographic signals for telecommunication system and network applications // Telecommunications and Radio Engineering. Volume 75, 2016 Issue 2. pages 169-178.

10. D. Gorbenko, A. A. Zamula, Ho Tri Luk. Synthesis of derivatives of complex signals based on nonlinear discrete sequences with improved correlation properties // Радиотехника. 2019. Вып. 199. С. 110-120.

Надійшла до редколегії 06.09.2020

Відомості про авторів:

Горбенко Іван Дмитрович – д-р техн. наук, професор, Харківський національний університет імені В.Н. Каразіна, професор кафедри безпеки інформаційних систем і технологій, факультет комп’ютерних наук, Україна, email: gorbenkoivan03@gmail.com, ORCID: https://orcid.org/0000-0003-4616-3449

Замула Олександр Андрійович – д-р техн. наук, професор, Харківський національний університет імені В.Н. Каразіна, професор кафедри безпеки інформаційних систем і технологій, факультет комп’ютерних наук, Україна, email: zamylaaa@gmail.com, ORCID: http://orcid.org/0000-0002-8973-6190

Хо Чі Лик – Харківський національний університет імені В.Н. Каразіна, магістрант кафедри безпеки інформаційних систем і технологій, факультет комп’ютерних наук, Україна.

УДК 681.3.06 **DOI:10.30837/rt.2020.3.202.12**

К.Е. ЛИСИЦКИЙ, И.В. ЛИСИЦКАЯ, канд. техн. наук

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ СЛУЧАЙНОЙ ПОДСТАНОВКИ

Введение

Самые современные традиционные ключевые криптосистемы базируются на идее произведения (product) шифров, которые представляют класс криптосистем, многократно повторяющих сложную операцию, отображающую преобразование плайнтекста в шифртекст. Каждое такое повторение (итерация) известно как цикл шифра. Сложная (составная) операция, выполняющаяся в каждом цикле, является обычно комбинацией из набора примитивных операций, таких как сдвиг, линейное преобразование, модульное сложение и подстановка. В частности, комбинация перестановочных и подстановочных операций может привести к криптографически сильному нелинейному преобразованию, если оно применяется достаточное число раз. Подстановочные операции во многих шифрах выступают при этом как основной нелинейный элемент циклового преобразования (нелинейный элемент замены). Поэтому значительные усилия исследователей направлены на изучение подходов к построению подстановок с высокими криптографическими показателями [1 – 6] и многие другие.

Наиболее разработанным и наиболее популярным математическим аппаратом оценки криптографических свойств нелинейных элементов замены (S-блоков) стал аппарат линейной алгебры и, в частности, аппарат булевых функций. Его развитию и применению посвящено большое число публикаций [7 – 10 и др.]. Предложено и используется множество критериев и показателей оценки свойств как самих булевых (компонентных) функций S-блоков, так и критериев и показателей криптографических свойств S-блоков в целом. В их числе такие: сбалансированность булевой функции, нелинейность N_f, корреляционный иммунитет, критерий распространения (строгий лавинный критерий) $KP(k)$, алгебраическая степень булевой функции $\deg(f)$, а также соответствующие характеристики S-блоков – критерий битовой независимости (*BIC*), критерий нелинейности, максимальный порядок строгого лавинного критерия (*MOSAC*), максимальное значение линейной аппроксимационной таблицы, δ-гладкость (δ-равномерность) XOR-таблицы S-блока [11 и др.].

Следует отметить также предложенный в свое время подход к отбору подстановок [12 – 14], строящийся на основе оценки показателей их случайности (значений числа циклов, возрастаний и инверсий), дополненных ограничениями на максимально допустимые значения таблиц дифференциальных разностей и линейных аппроксимаций. Здесь и в дальнейшем будут сделаны ссылки в основном на наши публикации, так как это направление не привлекло внимание зарубежных исследователей. Можно лишь отметить работы, посвященные использованию подстановок для построения ключей шифрования [15 и др.].

Отмеченный подход нашел продолжение в работах [15, 16 и др.], выполненных, с участием авторов этой работы. Основное внимание в этих публикациях сосредоточено на разработке дополнительных критериев отбора случайных подстановок, построенных на использовании законов распределения переходов XOR таблиц и смещений таблиц линейных аппроксимаций случайных подстановок. Было предложено два (дополнительных к комбинаторным) критерия отбора, основанных на оценке близости дифференциальных и линейных законов распределения вероятностей подстановок к теоретически полученным законам [16]. Напомним здесь кратко их суть, следуя [16].

Критерий 4. *Подстановка удовлетворяет критерию случайности* 4*, если закон распределения однотипных переходов* $\Pr(\Lambda_\pi(\Delta X,\Delta Y)) = 2k,\ k = 0,1,...,k*$*, ее таблицы XOR разностей для входов, приписываемых к ненулевым характеристикам, соответствует по критерию согласия Колмогорова теоретическому закону распределения переходов случайной подста-*

новки, т.е. наибольшее значение модуля разности теоретического и эмпирического законов распределения вероятностей удовлетворяет условию $|F_{\mathrm{T}}(x_k) - F(x_k)| \le b$.

Здесь граничный параметр b подлежит уточнению по результатам экспериментов.

Критерий 5. *Подстановка удовлетворяет критерию случайности* 5*, если закон распределения однотипных переходов* $\Pr(\lambda^*(\alpha,\beta)) = 2k),\ k = 0,1,...,k^*$*, ее таблица линейных аппроксимаций соответствует по критерию согласия Колмогорова теоретическому закону распределения переходов случайной подстановки, т.е. наибольшее значение модуля разности теоретического и эмпирического законов распределения вероятностей удовлетворяет условию* $|F_{\mathrm{T}}(x_k) - F(x_k)| \le c$.

Здесь параметр c также подлежит уточнению по результатам экспериментов.

В последующей работе [17] рассмотрено установление границ (значений параметров b и c) при использовании критерия Колмогорова для оценки близости законов распределения переходов дифференциальных и линейных таблиц подстановок теоретическим (мы их назвали ″эталонными″), на основе результатов которых принимается решение, можно ли отнести проверяемую подстановку к случайной или нет.

Ожидалось, что подстановки, отобранные по предлагаемой системе критериев, будут более предпочтительными, чем известные конструкции. Однако, с одной стороны, формируемые в этом случае подстановки, как показал анализ, не имеют заметных преимуществ в сравнении с известными. С другой – применение представленных выше критериев для практического отбора случайных подстановок встретило определенные затруднения, так как неясной стала сама стратегия применения этих критериев. Вроде бы мы порождаем случайные подстановки, а потом начинаем их фильтровать. Не ясно, какие же показатели отбора являются предпочтительными.

В этой работе мы хотим изменить позицию к определению показателей случайности. Мы хотим ответить на вопросы, а какими свойствами будет обладать выборка случайно порождаемых подстановок? С какими подстановками в этом случае реально мы имеем дело? Как они соотносятся с приведенными критериями отбора?

В работе будут изучаться показатели последовательности байтовых подстановок, порождаемых случайным генератором. Итогом их изучения станет усовершенствованная модель случайной подстановки, отличающаяся от известных использованием свойств выборки случайных подстановок, что позволило существенно упростить правила отбора случайных подстановок (а практически использовать подстановки, порождаемые генератором случайных подстановок без каких-либо ограничений). Для недоверчивых можно лишь выполнять проверку поцикловых значений максимумов таблиц XOR разностей и смещений таблиц линейных аппроксимаций.

Задача практически сводится к определению законов распределения выборки, составленной из максимумов таблиц XOR разностей и максимумов смещений таблиц линейных аппроксимаций случайных подстановок.

Математические аспекты этой задачи рассмотрены в приложении работы [18]. В ней изучаются случаи, когда все значения выборки имеют одно и то же распределение и их плотности уменьшаются с ростом переменной x экспоненциально. Но это как раз и есть наши случаи.

Далее приведем краткое изложение сути этой методики с нашими исправлениями [19], затем применим ее для построения законов распределения максимумов переходов таблиц XOR разностей и максимумов смещений таблиц ЛАТ байтовых подстановок.

Суть методики определения законов распределения максимумов для больших по объему выборок независимых одинаково распределенных случайных величин

Нас будут интересовать два случая.

1-й случай, когда выборка состоит из случайных значений переходов XOR таблиц случайных подстановок. Как известно [20], в этом случае распределение вероятностей переходов подчиняется пуассоновскому закону:

$$\Pr\left(\Lambda_\pi(\Delta X,\Delta Y)=2k\right)=e^{-1/2}\cdot\frac{1}{2^k\cdot k!} \tag{1}$$

Здесь $\Pr\left(\Lambda_\pi(\Delta X,\Delta Y)=2k\right)$ – вероятность, что значение дифференциальной таблицы случайно взятой подстановки π порядка 2^n для перехода входной разности ΔX в соответствующую выходную разность ΔY будет равна $2k$.

2-й случай, когда выборка состоит из случайных значений, являющихся смещениями таблиц линейных аппроксимаций случайных подстановок, подчиняющихся нормальному закону распределения. Как показано в [18], в этом случае справедливо утверждение.

Утверждение. *Для случайной n-битовой подстановки, с* $n \geq 5$ *дисбаланс* Imb(v,*u*) *аппроксимации является случайным значением с распределением, которое может быть аппроксимировано в виде*

$$\Pr(\mathrm{Imb}(v,u)=z)\approx 2Z\left(\frac{z}{2^{(n-2)/2}}\right) \tag{2}$$

для z четного и ноль – для z нечетного.

В наших обозначениях дисбаланс Imb(*v*, u) = *z* при $z = 2k$ как раз соответствует значению смещения таблицы линейных аппроксимаций.

В работе [18] отмечается, что распределение максимумов больших по объему выборок независимых одинаково распределенных случайных величин хорошо изучено в теории вероятностей и описывается распределением экстремальных значений Фишера – Типпета или log-Вейбула в виде

$$D_{\max}(X)\approx e^{-e^{\frac{a-X}{b}}}.$$

Это распределение имеет математическое ожидание $\mu(X) = a + b\gamma$ с $\gamma \approx 0{,}58$ и среднеквадратическое отклонение $\frac{\pi}{\sqrt{6}}b \approx 1{,}3b$. Параметр *a* является решением уравнения

$$\ln(2)Y=-\ln f(X), \tag{3}$$

а *b* является единицей, деленной на производную функции – ln*f*(*x*) в точке *a* (здесь используется линейная аппроксимация функции – ln*f*(*x*) в точке *a*).

В работе [18] также показано, что решение уравнения (3) для выборки из 2^Y случайных значений, распределенных по пуассоновскому закону, имеет вид

$$i=\frac{\ln(2)y-\frac{1}{2}\ln(2\pi i)-\lambda}{\ln\left(\frac{i}{\lambda}\right)-1}. \tag{4}$$

Это уравнение может быть решено итеративно. Производная – ln*f*(*x*) определяется по формуле

$$\ln\left(\frac{i}{\lambda}\right)+\frac{1}{2i}. \tag{5}$$

Определив *a* и используя условие $a >> \lambda$, имеем

$$b=\frac{1}{\ln\left(\frac{a}{\lambda}\right)}.$$

Для нормального распределения (2) параметр a_s (подстрочный индекс *s* для стандарта) является решением уравнения

$$a_s = \sqrt{2\ln(2)y - \ln(2\pi) - 2\ln(a_s)}, \tag{6}$$

которое может быть найдено итеративным путем, без учета правого члена в первой итерации. Производная $f(x)$ определяется по формуле

$$x + \frac{1}{x}, \tag{7}$$

и, следовательно,

$$b_s = \frac{a_s}{a_s^2 + 1} \approx \frac{1}{a_s}. \tag{8}$$

Грубо говоря, максимум имеет распределение со средним значением $1{,}17\sqrt{y}$ и стандартным отклонением $1{,}11/\sqrt{y}$. Авторы работы [7] отмечают, что можно найти значения *a* и *b* для любого нормального распределения со средним значением $\mu(X)$ и стандартным отклонением σ заменив *x* на $\frac{X - \mu(X)}{\sigma}$. Это дает

$$\begin{aligned} a &= \sigma a_s - \mu(X), \\ b &= \sigma b_s \end{aligned} \tag{9}$$

Распределение максимумов XOR таблиц и смещений таблиц линейных аппроксимаций выборки из байтовых подстановок

Мы здесь будем рассматривать выборку размера 2^n, $n = 8$. Для $n = 8$ из (4) имеем:

Таблица 1

i	$\frac{\ln(2)\cdot 16 - \frac{1}{2}\ln(2\pi i) - \frac{1}{2}}{\ln(2i) - 1}$
5	6,8
5,5	6,3
5,9	5,98
6	5.9
7	5,3

И, следовательно, решением уравнения (4) является значение $i = a$ близкое к числу 6. Соответственно $b = \frac{1}{\ln(12)} = 0{,}4$. Но заметим здесь, что формула (4), по которой мы определяли значение *a*, работает с половинным значением перехода дифференциальной таблицы. Поэтому при подсчете действительного среднего значения мы должны полученный результат удвоить.

И тогда

$$\mu(X) = 2\cdot 6 + 2\cdot 0{,}4\cdot 0{,}58 = 12{,}4.$$

Если ориентироваться на результаты реального эксперимента, то среднее значение максимума должно быть близким к 11,55. Поэтому мы скорректируем наше значение до $a = 5$.

Это значение хорошо согласуется с результатами расчетов и экспериментов, представленными в работах [21 и др.].

Выше отмечалось, что поскольку распределение максимумов дискретное, то малая величина стандартного отклонения $b = \frac{1}{\ln(12)} = 0{,}4$ приводит к тому, что распределение сосредоточено в двух целочисленных значениях вблизи $\mu(X) \approx 2a$. В наших экспериментах с байтовыми подстановками это два значения 10 и 12.

Расчет далее предлагается вести для распределения

$$D_{\max}(X) \approx e^{-e^{\frac{10-2\cdot X}{0{,}87}}}, \qquad (10)$$

где использовано значение $a = 5$ (формула записана с учетом реального удвоения значений переходов XOR таблицы).

В табл. 2 приведено распределение значений максимумов для 256-битовых подстановок, рассчитанных по выражению (10), и результаты эксперимента.

Решение уравнения (6) способом подбора для байтовой подстановки приведено в табл. 3. Для ориентировочного выбора начальных значений, используемых в переборе, вполне можно опираться на результаты расчетов и экспериментов, приведенные в [21].

Таблица 2

k^* (X_1,X_2)	Pr(k^*)	Расчетное значение	Эксперимент
8	0,00004	0,01	0
10 (10,8)	0,368 – 0,00004 = 0,368	94	92
12 (12,10)	0,905 – 0,368 = 0,537	137	147
14 (14, 12)	0,9901 – 0,905 = 0,008	22	14
16 (16,14)	0,9967 – 0,9901 = 0,0066	1,71	3
18 (18,16)	0,9999– 0,9967 = 0,0032	0,819	0

Таблица 3

a_S	$\sqrt{\ln(2)32 - \ln(2\pi) - 2\ln(a_s)}$
4	4,19
5	4.13
6	4,09
8	4

Мы и в этом случае сделали небольшую коррекцию результата, ориентируясь на данные экспериментов. В качестве значения a_S рассматривалось значение $a_S = 4$ и соответственно

$$b_s = \frac{a_s}{a_s^2 + 1} \approx \frac{1}{a_s} = \frac{1}{4} = 0{,}25 \qquad (11)$$

(здесь уже учитываем результаты выполненных экспериментов, представленных в табл. 3). Для подстановок степени 2^8 имеем $\sigma = 2^{\frac{8-4}{2}} = 2^2$ и тогда $a = \sigma a_s + \mu(X) = 4\cdot 4 + 0 = 16$ и в соответствии с (21)

$$b = 4\cdot 0{,}25 = 1$$

и приходим к интегральному закону распределения максимумов полных дифференциалов уменьшенной 16-битной модели шифра в виде

$$D_{\max}(X) \approx e^{-e^{\frac{16-X}{1}}}, \quad (12)$$

или с учетом реального удвоения результатов смещений таблицы линейных аппроксимаций:

$$D_{\max}(X) \approx e^{-e^{\frac{32-X}{2}}}. \quad (13)$$

В табл. 4 представлены результаты расчетов по определению распределения значений максимумов линейных корпусов на основе интегрального закона распределения вероятностей (13).

Заметим, что по результатам ранее выполненной теоретической и экспериментальной оценки значения максимума смещения линейной аппроксимационной таблицы случайной подстановки степени $_2{}^8$ равны 32 (расчет) и 34 (эксперимент) [22].

Видно, что и в этом случае результаты экспериментов практически повторяют результаты расчетов.

Таблица 4

$k^*(X_1,X_2)$	Pr(k^*)	Число значений	Эксперимент
< 26	$3.41\ 10^{-7}$	0	0
28 (28,26)	$5{,}6\ 10^{-4} - 3{,}4110^{-7} = 5{,}6\ 10^{-4}$	0,14	0
30 (30,28)	$0{,}064 - 5{,}6\ 10^{-4} = 0{,}0638$	16	10
32 (32,30)	0,368–0,064 = 0,304	78	86
34 (34,32)	0,692 – 0,304 = 0,388	99	98
36 (36,34)	0,874 – 0,692 = 0,181	46	46
38(38,36)	0,9518 – 0,874 = 0,078	19	10
40 (40,38)	0,9821 – 0,9518 = 0,03	8	6
42 (42,40)	0,9933 – 0,9821 = 0,011	3	0
44 (44,42)	0,9975 – 0,9973 = 0,00028	0,07	0

Из расчетов следует, что вероятность получить подстановку со смещением равным 30 уже менее шести сотых, а получить значение, большее 38, – меньше семи сотых, т.е. с большой вероятностью случайно взятая байтовая подстановка будет иметь значение смещения, близкое к 34 (чаще всего встречаемое).

Таким образом, значения дифференциальных и линейных переходов (смещений) соответствующих таблиц байтовых случайных подстановок имеют ярко выраженные прогнозируемые максимумы, которые в два раза больше предельных значений (таких, например, как у AES-x S-блоков).

Подводя итог, можно в соответствии с представленными результатами ввести и более практичное определение случайной подстановки.

В частности, байтовая подстановка является случайной, если:

1) значение максимума ее XOR таблицы принимает значения 10,12;

2) значения максимумов смещений ее таблицы линейных аппроксимаций имеют значения в диапазоне 32 – 38.

Этими определениями мы уточняем критерии 4 и 5, введенные ранее. Уточнение касается наложения (выполнения) ограничений лишь на максимальные значения переходов XOR таблиц и смещений таблиц линейных аппроксимаций.

На самом деле, поскольку случайные подстановки с большой вероятностью будут давать максимальные значения дифференциальных и линейных вероятностей, то приведенные ограничения можно рассматривать лишь как проверочные.

И если для 128-битного шифра Rijndael с родными S-блоками минимальное число активизируемых S-блоков для прихода шифра к состоянию случайной подстановки по дифференциальным показателям равно 21, то для шифра со случайными подстановками потребуется активизировать минимум 32 S-блоков [23].

Это значит, что 128-битный шифр Rijndael с родными S-блоками приходит к состоянию случайной подстановки за три цикла, а шифр со случайными подстановками – за четыре [23].

256-битный шифр Rijndael приходит к состоянию случайной постановки с родными S-блоками по дифференциальным показателям при активизации минимум 42 S-блоков, а шифр со случайными S-блоками требует для прихода к случайной подстановке при активизации минимум 48 S-блоков [23].

256-битный шифр с родными S-блоками приходит к состоянию случайной подстановки по линейным показателям при активизации минимум 50 S-блоков, а шифр со случайными S-блоками требует для прихода к случайной подстановке активизации минимум 65 S-блоков [23].

Это значит, что 256-битный Rijndael приходит к состоянию случайной подстановки по линейным показателям за четыре цикла, а шифр со случайными подстановками – за пять [23].

По линейным показателям 128-битный шифр Rijndael с родными S-блоками приходит к состоянию случайной подстановки за три цикла, а шифр со случайными подстановками – за четыре [23].

Таким образом, использование случайных S-блоков увеличивает на один цикл минимальное число циклов прихода шифра к состоянию случайной подстановки.

Но, как показали эксперименты, именно случайные подстановки, сформированные без всяких ограничений, с очень большой вероятностью оказались подходящими, с точки зрения криптографических приложений, в предложенных новых конструкциях блочных симметричных шифров [23], цикловые функции которых строятся с использованием управляемых подстановок. Использование цикловых функций с управляемыми подстановками (по крайней мере, на первых циклах шифрования) позволяет увеличить минимальное число активизируемых S-блоков на этих циклах, что дает возможность реализовать динамические показатели выхода шифров к асимптотическим показателям случайных подстановок, не уступающие считающимся лучшими (отобранными по специальным методикам) S-блокам практически всех современных шифров [11 – 23].

Выводы

Таким образом, результатом выполненных исследований является уточненное определение случайной подстановки (уточненная математическая модель случайной подстановки), строящееся на свойствах выборки случайных подстановок. Теперь появилось полное понимание о том, с какими подстановками мы имеем дело при их случайном формировании. Как оказалось, с очень большой вероятностью будут получаться подстановки, для которых значения максимумов дифференциальных таблиц и значения максимумов смещений таблиц линейных аппроксимаций принимают существенно ограниченное число возможных значений. Все они концентрируются вокруг теоретических значений максимумов случайных подстановок соответствующей степени.

Как показывают эксперименты [24], случайные подстановки, взятые с выхода генератора случайных подстановок без всяких ограничений, вполне могут конкурировать с лучшими

известными конструкциями S-блоков, используемыми в современных шифрах. Увеличенные по сравнению с предельными значениями максимумов, к которым стремятся авторы большинства работ по поиску S-блоков с улучшенными показателями, могут быть компенсированы использованием в шифрах цикловых функций с увеличенным числом активизируемых S-блоков на первых циклах [24].

Список литературы:

1. Adams C. M. and Tavares S.E. The Structured design of cryptographically good S-boxes // Journal of Cryptology**,** 3(1): 27-41, 1990.

2. Forré R. Methods and instruments for designing S-boxes // Journal of Cryptology, 2(3): 115-130, 1990.

3. Nyberg K. Perfect nonlinear S-boxes // Advances in cryptology -EUROCRYPT91, volume 547, Lecture Notes in Computer Science, pp. 378-386. Springer-Verlag, Berlin, Heidelberg, New York, 1991.

4. Nyberg K. On the construction of highly nonlinear permutations // Advances in cryptology – Proceedings of EUROCRYPT'92 (1993) vol. 740, Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York pp. 92-98.

5. Nyberg K. Differentially uniform mappings for cryptography // Advances in cryptology – Proceedings of EUROCRYPT'93 (1994) vol. 765, Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York, pp. 55-65.

6. Claudia Peerez Ruisanchez A NEW ALGORITHM TO CONSTRUCT S-BOXES WITH HIGH DIFFUSION // International Journal of Soft Computing, Mathematics and Control (IJSCMC). Vol. 4, No. 3, August 2015. DOI : 10.14810/ijscmc.2015.4303 41.

7**.** Seberry J., Zhang X.-S. and Zheng Y. Nonlinearity and Propagation Characteristics of Balanced Boolean Functions // Inforsation and Cosputation. Vol. 119, No 1, pp. 1-13, 1995.

8. Pasalic E., Johansson T., Saitra S., Sarkar P. New constructions of resilient and correlation immune Boolean functions achieving upper bounds of nonlinearity // Workshop of Coding and Cryptography, Electronic Notes in Discrete Mathematics. Elsevier, January 2001.

9. Xiao G-Z and Massey J.L. A Spectral Characterization of Correlation-Immune Combining Functions // IEEE Transaction on Information Theory. Vol. 34, №.3 (1988), pp. 569-571.

10. Clark J., Jacob J., Stepney S., Saitra S. and Sillan W. Evolving of Boolean functions satisfying sultiple criteria", proceedings of INDOCRYPT'02, LNCS vol 2551, pages 246-259, Springer, 2002.

11. Yücel M.D. IAM501-Introduction to Cryptography. Institute of Applied Mathematics METU, Ankara, Turkey (9700501), 2002, p. 1-28.

12. Лисицкая И.В. К вопросу построения долговременных ключей для алгоритма ГОСТ 28147-89 // Информационно-управляющие системы на железнодорожном транспорте. 1997. № 3. С. 54–57.

13. Lysytska I.V., Koriak A.S., Golovashich S.A., Oleshko O.I., Oleinik R.V. The selection criteria of random substitution tables for symmetric enciphering algorithms // Abstracts of XXVIth General Assembly. Toronto, Ontario Canada, August 13-21, 1999. P. 204.

14. Горбенко И.Д., Лисицкая И.В. Критерии отбора случайных таблиц подстановок для алгоритма шифрования по ГОСТ 28147-89 //. Радиотехника. 1997. Вып 103. С. 121–130.

15. Лисицкая И.В. Оценка числа случайных подстановок с заданным распределением парных разностей XOR таблиц и смещений таблиц линейных аппроксимаций / И.В. Лисицкая, А.В. Широков, Е.Д. Мельничук, К.Е. Лисицкий // Прикладная радиоэлектроника. Харьков : ХНУРЭ, 2010. Т. 9, № 3. С. 341-345.

16. Долгов В.И. Случайные подстановки в криптографии / В.И. Долгов, И.В. Лисицкая, К.Е. Лисицкий // Радіоелектронні та комп'ютерні системи. 2010. № 5 (46). С. 79-85.

17. Лисицька І.В. Экспериментальная проверка работоспособности новых критериев отбора случайных подстановок / І.В. Лисицька, К.Є. Лисицкий, А.В. Широков, Е.Д. Мельничук // Радіоелектронні та комп'ютерні системи. 2010. № 6 (47). С. 87-93.

18. Joan Daemen, Vincent Rijmen. Probability distributions of Correlation and Differentials in Block Ciphers. April 13, 2006, pp. 1–38.

19. Лисицкий К.Е. О методике оценки законов распределения вероятностей максимумов полных дифференциалов и смещений линейных оболочек блочных симметричных шифров // Прикладная радиоэлектроника. Харьков : ХНУРЭ, 2015. Т. 14, № 4. С. 335-338.

20. Лисицкая И.В. Свойства законов распределения XOR таблиц и таблиц линейных аппроксимаций случайных подстановок // Вісник Харк. нац. ун-ту ім. В.Н. Каразіна. 2011. №960, Вип.16. С. 196-206.

21. Олейников Р.В. Дифференциальные свойства подстановок / Р.В. Олейников, О.И. Олешко, К.Е. Лисицкий, А.Д. Тевяшев // Прикладная радиоэлектроника. 2010. Т.9. № 3. С. 326-333.

22. Долгов В.И. Свойства таблиц линейных аппроксимаций случайных подстановок / В.И. Долгов, И.В. Лисицкая, О.И. Олешко // Прикладная радиоэлектроника. Харьков : ХНУРЭ, 2010. Т. 9, № 3. С. 334-340.

23. Долгов В.И. S-блоки для современных шифров. / В.И. Долгов, Е.В. Мельничук // Радиотехника. 2012. Вып.171. С. 121-133.

24. Dolgov V.I. The new concept of block symmetric ciphers design / V.I. Dolgov, I.V. Lisitska, K.Ye. Lisitskyi // Telecom RadEng. v. 76, 2017, i. 2. pages 157-184. DOI: 10.1615.

Поступила в редколлегию 08.09.2020

Сведения об авторах:

Лисицкий Константин Евгеньевич – Харьковский национальный университет имени В.Н. Каразина, аспирант кафедры безопасности информационных систем и технологий, факультет компьютерных наук, Украина, e-mail: konstantin.lisickiy@mail.ru

Лисицкая Ирина Викторовна – канд. техн. наук, Харьковский национальный университет имени В.Н. Каразина, профессор кафедры безопасности информационных систем и технологий, факультет компьютерных наук, Украина, e-mail: konstantin.lisickiy@mail.ru

ОБРОБКА СИГНАЛІВ В РАДІОТЕХНІЧНИХ СИСТЕМАХ

УДК 621.397 **DOI:10.30837/rt.2020.3.202.13**

И.В. КОРЫТЦЕВ, канд. техн. .наук, С.А. ШЕЙКО, канд. техн. наук,
В.М. КАРТАШОВ, д-р техн. наук, О.В. ЗУБКОВ, канд. техн. наук,
В.Н. ОЛЕЙНИКОВ, канд. техн. наук, С.И. БАБКИН, канд. техн. наук, И.С. СЕЛЕЗНЕВ

ОБРАБОТКА СИГНАЛОВ ПРИ ПЕЛЕНГАЦИИ И ОПРЕДЕЛЕНИИ ДАЛЬНОСТИ ДО МАЛОРАЗМЕРНЫХ БПЛА В ОПТИЧЕСКОМ И ИНФРАКРАСНОМ ДИАПАЗОНАХ

Введение

В настоящее время количество сфер применения малоразмерных беспилотных летательных аппаратов (БПЛА) стремительно растет, многие из них стали доступными для обычных пользователей. Обнаружение и оценка координат БПЛА имеет решающее значение для защиты от их несанкционированного применения в охраняемых зонах, для предотвращения столкновения БПЛА с другими летательными аппаратами, в случаях навигации нескольких БПЛА при выполнении экологического мониторинга, наблюдения и ландшафтной разведки.

Для обнаружения и пеленгации БПЛА используют радиолокационные, радиочастотные, акустические и оптико-электронные методы, а также их комплексирование [1]. Среди оптико-электронных методов определения координат объектов выделяют лазерное сканирование, структурированное освещение и пассивные стерео-бинокулярные системы [2]. Пассивные оптико-электронные системы по сравнению с активными обеспечивают следующие преимущества: скрытность измерений, значительно меньшее энергопотребление и низкая себестоимость за счет отсутствия мощного дорогостоящего лазера, возможность распознавания объектов по анализу их изображений, возможность измерения расстояний до удаленных объектов или объектов с малым коэффициентом отражения [3, 4].

Стерео-бинокулярные системы могут быть реализованы как в оптическом (видимом) [5 – 7], так и в инфракрасном (ИК) [8] диапазонах. Они применяются для автоматизации посадки больших БПЛА или навигации малых БПЛА в условиях ограниченного пространства.

Существуют пассивные оптико-электронные системы определения местоположения объектов с применением одной камеры [9, 10]. Однако для измерения расстояния они должны оперировать серией кадров, сделанных камерой при разных значениях фокусного расстояния [9] либо при ее пространственном смещении [10]. Очевидно, что в случае наблюдения движущихся БПЛА применение таких методов не представляется возможным.

Прогресс в развитии матричной видеотехники высокого разрешения открывает новые возможности для обнаружения воздушных объектов малых размеров, измерения их координат, а также их распознавания. Применение современных светочувствительных матриц позволяет расширить возможности системы стереовидеонаблюдения (СВН) на ближний и дальний ИК диапазоны [8, 11]. Использование оптико-электронного метода СВН в сочетании с акустическим методом выявления воздушных объектов [12 – 15] позволит в значительной степени повысить эффективность аппаратурного комплекса для противодействия дронам.

Существует множество алгоритмов обработки стереоизображений для измерения дальности [16 – 19]. Количество этапов обработки, содержание этих этапов и их параметры зависят от конкретной задачи: от вида, структуры, размера наблюдаемого объекта; от условий наблюдения – освещенности объекта, его контраста с фоном, отношения сигнал/шум; от наличия или отсутствия предварительного целеуказания и т.д.

В данной работе рассматривается задача выбора алгоритма обработки видеоизображений стереопары, полученных в видимом, ближнем или дальнем ИК диапазонах, определение параметров этого алгоритма, обеспечивающих надежное определение дальности до малых

БПЛА, их последующее автосопровождение и оценку параметров движения. При этом предполагается, что различие в обработке сигналов в оптическом, ближнем и дальнем ИК диапазонах проявляется на этапе обнаружения БПЛА. Это обусловлено различием портретов БПЛА в указанных диапазонах, что требует отдельной процедуры обучения нейронной сети на серии портретов в соответствующем диапазоне наблюдения.

Метод пеленгации и измерения дальности

Рассмотрим возможности оптического метода двуканального СВН. На рис. 1 изображена схема формирования световых образов объекта T на светочувствительных матрицах VM_1, VM_2 видеокамер с фокусным расстоянием F. Схема показывает лишь основные принципы формирования оптических проекций, а все абсолютные их значения и угловые величины показаны условно, т.к. реальная дальность до объекта D значительно больше расстояния O_1O_2 между оптическими осями z_1 и z_2 объективами видеокамер – стереобазы b. Угол обзора β определяется углами обзора объективов, полагаем $\beta = \beta_1 = \beta_2$. На бесконечно большой дальности до объекта угол параллакса α будет равен нулю, и при нахождении объекта на оси его световые образы формируются в центрах матриц.

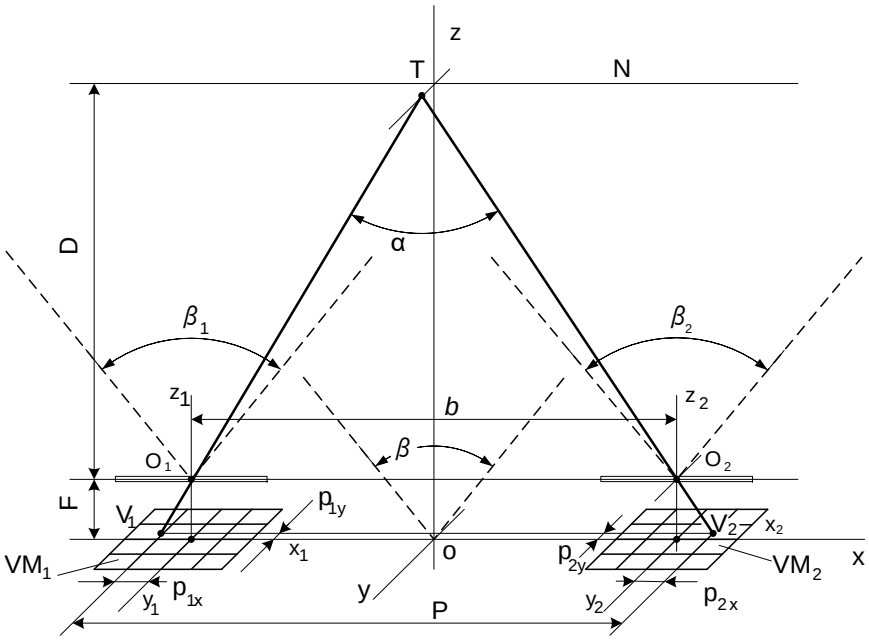


Рис. 1. Формирование световых образов
на светочувствительных матрицах системы СВН

При уменьшении дальности и возможном смещении объекта от оси z угол параллакса увеличивается; на матрицах наблюдаются отклонения образов (точки V_1, V_2) от центров матриц как по горизонтали ось x) p_{1x}, p_{2x} – это величины соответствующих линейных параллаксов с определенными знаками, так и по вертикали (ось y) p_{1y}, p_{2y} – это за счет смещения объекта вдоль оси y относительно оси z. Суммарную величину линейного параллакса p можно определить из подобия треугольников O_1TO_2 и V_1TV_2

$$p = \frac{bF}{D}, \tag{1}$$

где $p = p_{2x} - p_{1x}$.

Таким образом, дальность до объекта определяется базой системы, одинаковым фокусным расстоянием объективов и суммарным линейным параллаксом:

$$D = \frac{bF}{(p_{2x} - p_{1x})} = \frac{bF}{w_x(n_{2x} - n_{1x})}, \quad (2)$$

где n_{1x}, n_{2x} – количество пикселей в линейных параллаксах, взятые с соответствующими знаками – (-) если линейный параллакс наблюдается на отрицательной полуоси x, (+) – если на положительной полуоси x видеоматриц VM_1 и VM_2 соответственно левой и правой видеокамер; w_x – размер зерна пикселей по горизонтали.

Суммарный линейный параллакс одинаков для всех положений точки T объекта на плоскости, проходящей через линию N параллельно плоскости измерений XY. В то же время линейные параллаксы на матрицах видеокамер изменяются и по величине, и по знаку в своих системах координат $x_1y_1z_1$ и $x_2y_2z_2$, привязанных к центрам матриц, с плоскостями x_1y_1 и x_2y_2, совпадающими с плоскостью XY. Как видно из рис. 1, если точка T находится на главной оси z системы СВН или смещена лишь по оси y, то $|p_{1x}| = |p_{2x}|$, и их разность $\Delta p_x = 0$. При смещении объекта вправо от оси z по горизонтали (вдоль оси x) $|p_{1x}| > |p_{2x}|$, появляется положительная разность в величинах модулей линейных параллаксов

$$\Delta p_x = |p_{1x}| - |p_{2x}| > 0,$$

а при смещении объекта влево от оси z эта разность становится отрицательной

$$\Delta p_x = |p_{1x}| - |p_{2x}| < 0.$$

Появляется возможность сформировать сигнал управления поворотным устройством оптической системы для перемещения ее оси z по горизонтали в направлении перемещения объекта на угол $\Delta\gamma_x = \pm m_x \cdot \Delta p_x$ или до выполнения условия $\Delta p_x = 0$; здесь m_x – коэффициент пропорциональности по горизонтали с размерностью град/пикс.

Ортогональные смещения световых образов p_{1y}, p_{2y} являются также знакопеременными, и после выполнения перемещения главной оси по горизонтали они становятся равными, а их знак соответствует направлению перемещения объекта по оси y. Так, отрицательные значения смещений соответствуют перемещению объекта вверх по оси y, а положительные – вниз. Поворотное устройство системы должно отработать команду соответственно на увеличение или уменьшение угла места главной оси системы на величину $\Delta\gamma_y = \pm m_y \cdot (p_{1y} + p_{2y})/2$ либо до выполнения условия $p_{1y} + p_{2y} = 0$; здесь m_y – коэффициент пропорциональности по вертикали. Смещения p_{1y} и p_{2y} должны быть одинаковыми как по знаку, так и по величине. Их возможное неравенство указывает на неправильную юстировку видеокамер.

Механико-электрическое сопровождение объекта выполняется эпизодически с целью, чтобы объект не вышел из поля зрения оптической системы. Вся вторичная обработка сигналов, связанная с распознаванием дронов, на фоне помех и определения параметров их движения осуществляется при непрерывном электронном автосопровождении.

Экспериментальная установка СВН, ее калибровка и оценка погрешностей

Экспериментальная установка включала в себя две IP камеры Dahua DH-IPC-HFW2431RP-ZAS-IRE6 разрешением 2688(H) x 1520(V), разнесенных по горизонтали на величину базы 1 м.

IP камеры подключались по LAN интерфейсу к сетевому роутеру TP-Link TL-WR841N, а затем по WAN интерфейсу – к ноутбуку с программным обеспечением Smart PSS для записи видеопотоков с видеокамер. Системные часы IP камер предварительно программно синхронизировались. Старт и окончание процессов записи производились путем одновременной подачи аппаратного сигнала "тревоги" на обе камеры.

Горизонтальное поле зрения обеих камер через веб-интерфейс устанавливалось одинаковым $\beta = 60^{o}$ и контролировалось по изображению специальной мерной таблицы, установленной на расстоянии 1 м по оптической оси каждой камеры.

Структурная схема экспериментальной установки показана на рис. 2, а внешний вид – на рис. 3. Схема стереоскопической системы и приведенная формула (2) предполагают, что оптические оси объективов параллельны и фотоприемные матрицы находятся на одной прямой, параллельной оси x. Однако в реальной экспериментальной установке это реализовать достаточно трудно. Вторым источником ошибок измерения являются искажения объективов камер, главным образом – дисторсия. В этом случае коэффициент линейного увеличения изменяется по полю зрения объектива, нарушая геометрическое подобие между объектом и его изображением.

Таким образом, для оценивания трехмерных координат объекта по стереопаре необходимо: знать внутренние параметры камер (задача калибровки), знать параметры взаимного расположения камер (задача взаимной калибровки), определить на изображениях координаты соответствующих точек объекта (задача поиска сопряженных точек).

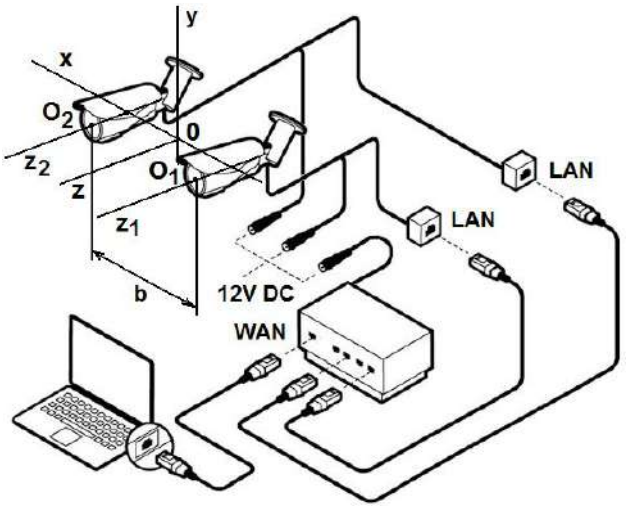


Рис. 2. Структурная схема экспериментальной установки

Рис. 3. Внешний вид экспериментальной установки

Задача калибровки каждой камеры, составляющей стереопару, заключается в нахождении матрицы $\mathbf{C}$, которая в случае линейной модели содержит только параметры объектива и светочувствительной матрицы [2]:

$$\mathbf{C} = \begin{bmatrix} F/w_x & 0 & u_0 \\ 0 & F/w_y & v_0 \\ 0 & 0 & 1 \end{bmatrix},$$

где w_x и w_y – шаг пикселей вдоль осей x и y соответственно; u_0 и v_0 – координаты главной точки относительно начала координат светочувствительной матрицы.

В нелинейной модели камеры матрица $\mathbf{C}$ учитывает также дисторсию.

Задача взаимной калибровки решается путем нахождения внешних параметров стереоскопической системы, которые описываются матрицей поворота $\mathbf{R}$ и вектором переноса $\mathbf{t}$:

$$\mathbf{R} = \mathbf{R}_\alpha \cdot \mathbf{R}_\beta \cdot \mathbf{R}_\gamma,$$

$$\mathbf{t} = (t_x, t_y, t_z)^T,$$

где $\mathbf{R}_\alpha, \mathbf{R}_\beta, \mathbf{R}_\gamma$ – матрицы поворота вокруг осей x, y, z на углы α, β, γ соответственно; t_x, t_y, t_z – значения переноса вдоль осей x, y, z; T – знак транспонирования.

Для определения матриц $\mathbf{C}$, $\mathbf{R}$ и вектора $\mathbf{t}$ существует много различных моделей и подходов [2, 3, 16]. Широко распространены методы, использующие в качестве объекта калибровки набор точек с известными пространственными координатами, например калибровочного щита [20]. Эти методы дают высокую точность калибровки стереопары, однако требуют сложной и точной системы крепления и перемещения щита для его съемки с различных ракурсов.

Существуют методы, которые используют для калибровки некоторые геометрические свойства сцены, например, линии схождения [21]. По понятным причинам, такие методы имеют недостаточную для наших целей точность.

В последнее время получили развитие методы самокалибровки [3, 9]. В качестве объекта съемки они используют калибровочную таблицу в виде сетчатого или шахматного поля известных размеров, снимаемую в различных положениях. Трех кадров достаточно, чтобы определить все внутренние и внешние параметры камеры. При малом числе снимков такие методы менее устойчивы и точны, чем при использовании точек с известными пространственными координатами, однако при большом количестве снимков (20 и более) их точность сопоставима.

Поскольку в нашем случае используются недорогие IP камеры и угол поля зрения объективов достаточно широк, необходимо производить калибровку с учетом нелинейных искажений. Для нелинейной модели камеры обычно используются смешанные двухшаговые методы калибровки. Сначала проводится линейная оценка параметров, которая затем используется в итеративной оптимизации как начальное приближение. В качестве минимизируемого функционала ошибки берется среднеквадратическая ошибка проецирования всех калибровочных точек на плоскость изображения. Основные различия в калибровке у различных авторов заключаются в способе вычисления начального приближения. Эти методы калибровки подробно описаны, например, в работах [22, 23].

При проведении калибровки мы руководствовались следующими главными принципами: простота изготовления испытательной таблицы и точность измерения пространственных координат. Для устойчивой и точной калибровки необходимо достаточно большое количество калибровочных точек, в процессе калибровки различные положения таблицы должны заполнять как можно большую часть рабочей области стереозрения, а ее изображения – как можно большую часть площади кадра. Поэтому мы стремились, чтобы на каждом кадре калибровочная таблица покрывала максимальную область изображения.

Одним из подходов может служить большой щит с сеткой, который снимается из разных положений передвигающейся стереопарой. Однако при перемещении стереопары можно нарушить взаимное расположение камер, что приведет к ошибкам калибровки. Поэтому в нашем случае использовалась жестко закрепленная стереопара, изменялось положение калибровочной таблицы.

Изготовленная нами калибровочная таблица представляет собой фанерный щит с наклеенной на него калибровочной сеткой в виде шахматного поля с количеством квадратов 9 х 6. Углы квадратов сетки служат калибровочными точками. Размер таблицы 0,9 м х 0,60 м позволяет производить калибровочные снимки на расстоянии 1 м и более. При этом таблица

полностью попадает в кадр при горизонтальном угле поля зрения 60° и находится дальше, чем ближняя граница зоны резко изображаемого пространства.

Калибровка камер осуществлялась в OpenCV при помощи функции, основанной на методах Zhang [22] и Bouguet [23]. Для оценки погрешности определения дальности после калибровки экспериментальной установки были сформированы 30 изображений калибровочной таблицы в разных позициях на расстояниях 1 – 2 м от камер. Для видеопотоков IP камер при этом устанавливалось минимальное сжатие. Пример одного такого изображения с найденными калибровочными точками показан на рис. 4.

Погрешность калибровки оценивалась при фиксированных значениях базы $b = 0{,}5$ м и 1 м. Маркер дальности устанавливался вдоль оси z при $y = 0$ (по оси системы) и по осям, отклоненным от оси z на ±25°. Диапазон дальностей до маркера от 5 м до 100 м, шаг – 5 м (рис. 5). Расстояния от центра системы СВН до маркера были измерены с помощью лазерного дальномера Bosh GLM 250 с типовой точностью измерений ±1 мм. Маркер представлял собой таблицу, изготовленную аналогично калибровочной, но с изображением креста в центре. Определение точки пересечения линий креста на изображении производилось в автоматическом режиме. На каждом расстоянии производилось 10 измерений дальности по 10 произвольным парам кадров системы СВН.

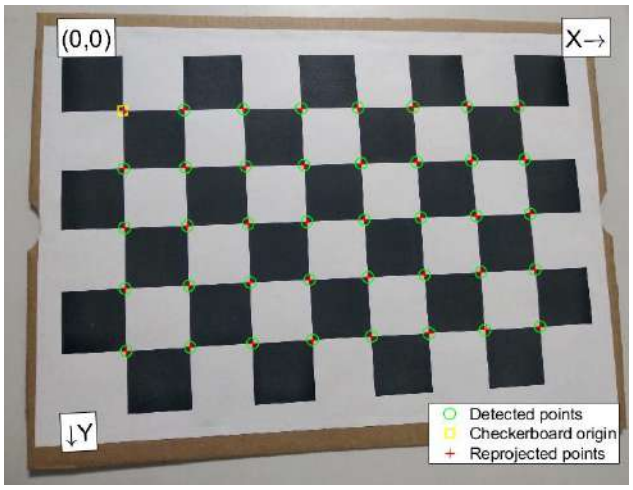


Рис. 4. Пример изображения калибровочной таблицы с найденными калибровочными точками

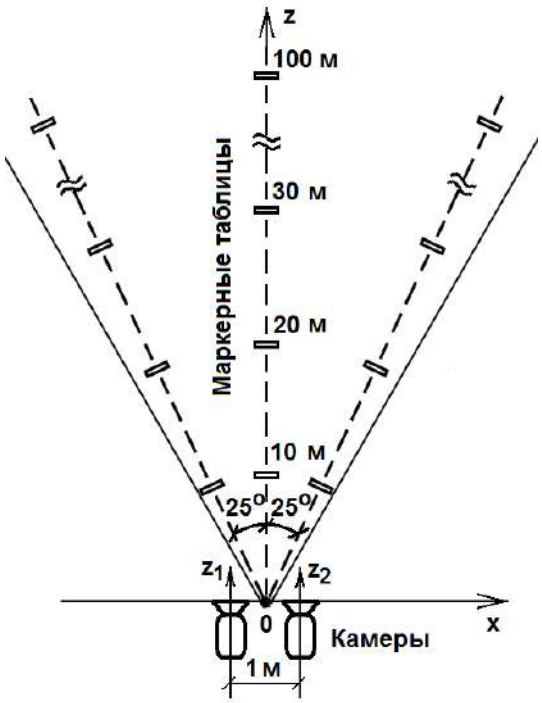


Рис. 5. К оценке погрешностей системы СВН

Определение дальности производилось по формуле (2), приведенной к виду, куда вместо фокусного расстояния F и шага пикселей w_x входят угол обзора β и разрешение по горизонтали M_x светочувствительной матрицы. Фокусное расстояние F можно выразить через угол обзора β камеры

$$F = \frac{W}{2 \cdot tg(\beta / 2)}, \tag{3}$$

где W – ширина светочувствительной матрицы.

Подставляя (3) в выражение (2) и учитывая, что $W / w_x = M_x$, получаем

$$D = \frac{bM_x}{2 \cdot tg(\beta / 2)[n_{2x} - n_{1x}]}. \tag{4}$$

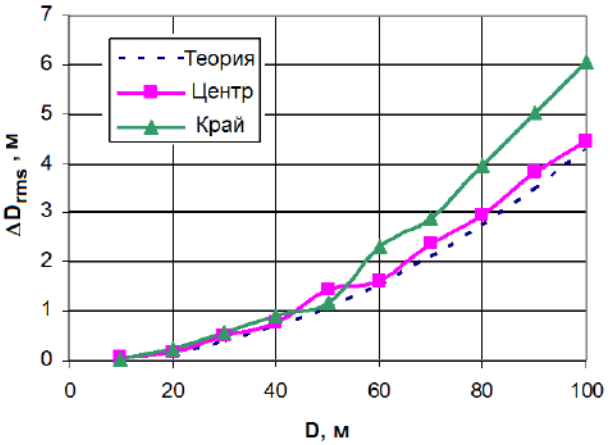


Рис. 6. Результаты испытаний откалиброванной системы СВН

Результаты испытаний откалиброванной установки СВН определения дальности по выражению (4) для откалиброванной установки СВН показаны на рис. 6.

Для каждого расстояния приведены значения среднеквадратической (по 10 измерениям) ошибки измерения дальности ΔD_{rms}. Пунктирной линией показаны значения максимальной абсолютной ошибки определения дальности, рассчитанные по формуле, учитывающей разрешающую способность СВН

$$\Delta D = \pm \frac{bFw_x D^2}{(bF)^2 - (w_x \cdot D)^2}. \qquad (5)$$

Входящие в формулу (5) величины, соответствующие условиям эксперимента: $F = 6{,}38$ мм с учетом $\beta = 60°$ и диагонали матрицы (1/3)", $w_x = 2{,}74$ мкм при горизонтальном разрешении 2688. Как следует из рис. 6, экспериментальная ошибка измерения дальности не превышает 4,5 % по центру и 6 % по краям горизонтального поля наблюдения

Экспериментальное определение координат БПЛА

Эксперимент по измерению координат БПЛА с помощью системы СВН проводился в полевых условиях в Харьковской области, Украина. Измерения осуществлялись 20.01.2020 г. с 14.00 до 16.00 в пасмурную погоду. Освещенность на вертикальной плоскости составляла 450 – 650 лк. Измерение освещенности проводилось люксметром Wintact WT81.

В эксперименте использовался квадрокоптер DJI Phantom 3 SE с горизонтальным размером 0,35 м. Тестовые полеты происходили на расстоянии до 200 м.

Координаты квадрокоптера (широта, долгота и высота), полученные стандартным GPS приемником квадрокоптера, использовались для сравнения с координатами БПЛА, полученными с помощью системы СВН. Для этого географические координаты квадрокоптера преобразовывались в декартовые, а затем путем поворота и смещения оси координат совмещались с системой координат системы СВН. Местоположение квадрокоптера описывается относительно начала отсчета в декартовых координатах.

В данной работе приводятся результаты измерений по двум тестовым полетам БПЛА. Трек 1 – пролет вдоль оси z с зависанием на высоте 5 м над точками, удаленными на 3 м, 25 м, 50 м, 100 м, 150 м, 200 м. Трек 2 – поднимающаяся спираль с диаметром витка 50 м на высоту 30 м с центром, удаленным по оси z на 100 м, 3 витка.

Алгоритм обработки изображений системы СВН для обнаружения и распознавания БПЛА подробно описан в [24]. Он включал в себя следующие этапы:

– преобразование цветного изображения в оттенки серого и выполнение нормализации его яркости для уменьшения влияния изменений интенсивности освещения;

– выделение движущихся фрагментов изображения в текущем видеокадре на неподвижном фоне методом MOG, MOG2 или KNN;

– применение ко всем фрагментам изображения, в которых обнаружено движение, алгоритма истории движения для уменьшения количества ложных тревог;

– распознавание изображения БПЛА при помощи нейронной сети.

Данный алгоритм позволяет обнаруживать и распознавать БПЛА при минимальном размере изображения 5x5 пикселов с вероятностью более 90 %. При разрешении видеокамеры 2688x1520 расстояние до квадрокоптера DJI Phantom 3 SE, при котором размер его изображения равен 5x5 писелов, будет составлять 166 м. Это максимальная дальность системы СВН, ограниченная надежностью обнаружения и распознавания БПЛА.

Алгоритм обработки изображений для пеленгации БПЛА показан на рис. 7.

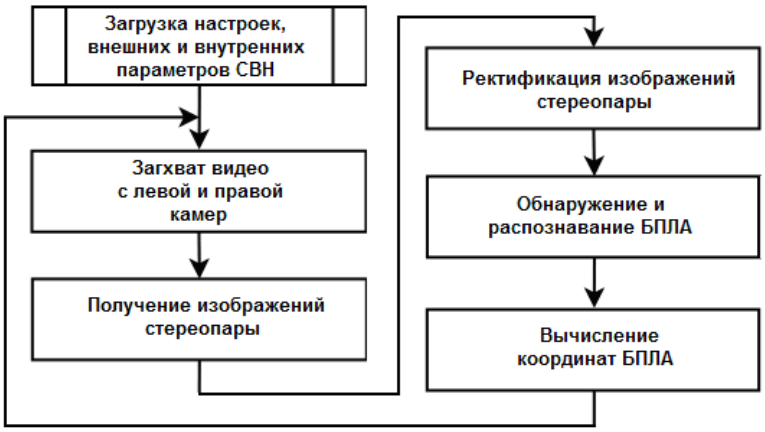


Рис. 7. Алгоритм обработки сигналов для определения координат

В качестве сопряженных точек изображения БПЛА использовались координаты центра $V(x, y)$ области, выделенной на этапе обнаружения и распознавания (рис.8).

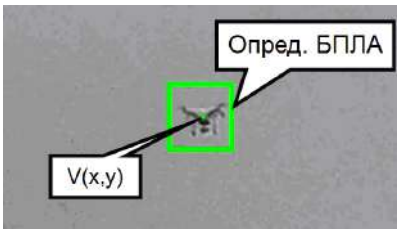


Рис. 8. Нахождение координат БПЛА на изображении

Азимут и угол места БПЛА вычислялись как

$$\varphi_{az} = \frac{\beta \cdot x}{M_x},\ \varphi_{el} = \frac{\beta \cdot y}{k \cdot M_y},$$

где M_x, M_y – разрешение матрицы по вертикали, k – формат кадра (16/9).

Результирующие значения азимута и угла места вычислялись как среднее по результатам измерений двумя камерами.

На рис. 9, 10 показаны результаты сравнения GPS координат БПЛА и результатов измерений системы СВН. Рис. 9 соответствует треку 1, рис. 10 – треку 2. Графики построены в координатах: *а* – азимут-время; *б* – угол места – время; *в* – дальность – время.

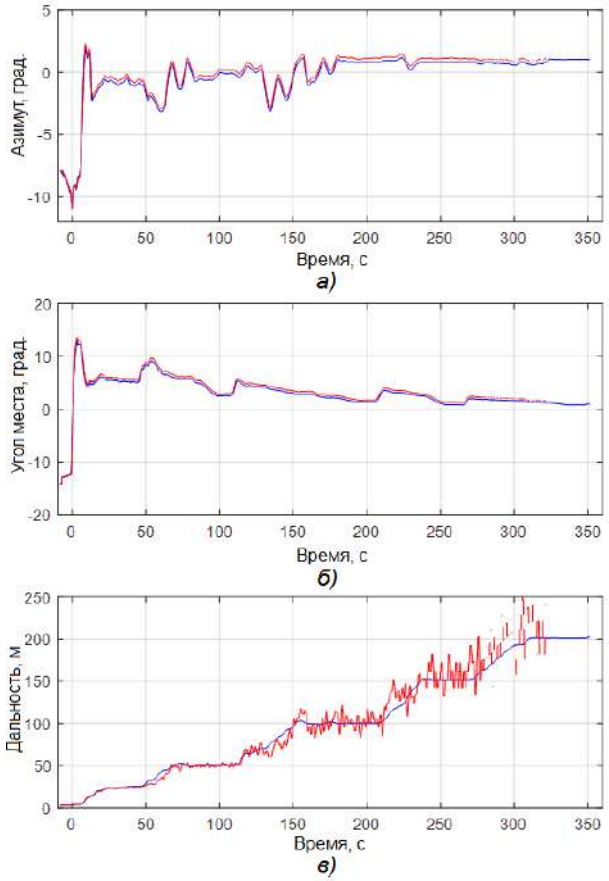


Рис. 9. Определение координат БПЛА (трек 1)

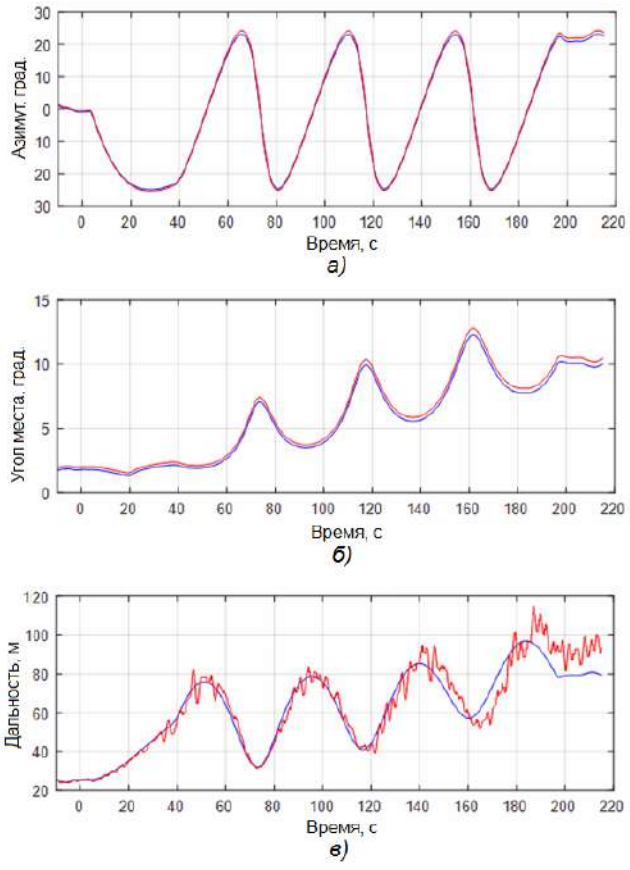


Рис. 10. Определение координат БПЛА (трек 2)

Анализируя графики на рис. 9, 10, можно отметить, что измерения азимута и угла места БПЛА системой СВН точно совпадают с данными GPS приемника. Это объясняется высокой разрешающей способностью камер и достаточно точной калибровкой их внутренних параметров. Для измерений по треку 1 среднеквадратическое отклонение относительной ошибки измерения дальности составило $\Delta D_{rms} = 9{,}6$ %, максимальная относительная ошибка измерений $\Delta D_{\max} = 26{,}4$ %. Для измерений по треку 2 – $\Delta D_{rms} = 7{,}8$ %, $\Delta D_{\max} = 24{,}8$ %.

При дальностях более 160 м на рис. 9 наблюдаются сбои в системе обнаружения и распознавания БПЛА, связанные с тем, что размер изображения объекта становится менее чем 5x5 пикселов. Этот процесс сопровождается заметным увеличением абсолютной ошибки измерения дальности. Наибольшая среднеквадратическая ошибка измерений дальности наблюдается в среднем диапазоне расстояний действия системы СВН 70 – 120 м. Как показал анализ, причиной этого является одновременное действие двух факторов: первый – ухудшение разрешающей способности системы СВН по дальности с увеличением дальности (рис. 6), второй – невысокая точность метода определения сопряженных точек как координат центров $V(x, y)$ областей обнаружения БПЛА (рис. 9). Причем, второй фактор дает бóльшие ошибки на меньших дальностях до объекта.

На графике рис.10, *в* заметно влияние недостаточно точной ректификации системы СВН, что проявляется в увеличении ошибки измерения дальности при больших азимутах и углах места. При этом влияние ошибок неточной ректификации сравнимо с влиянием ошибок определения сопряженных точек.

Выводы

Проведенный теоретический анализ и экспериментальные исследования показали:

1. Основной вклад в ошибку определения местоположения БПЛА с помощью системы СВН принадлежит измерению дальности. Измерения азимута и угла места при этом достаточно точны при высокой разрешающей способности камер и достаточно точной компенсации их нелинейных искажений.

2. Очевидными путями для увеличения точности измерения дальности системой СВН, а также увеличения дальности обнаружения объекта, является увеличение разрешающей способности камер. Однако для обнаружения, распознавания и пеленгации БПЛА в реальном времени в этом случае понадобятся значительные вычислительные ресурсы. Увеличение четкости изображения в два раза приводит к увеличению вычислительной сложности в четыре раза на каждом этапе обработки.

3. Уменьшение угла обзора камер при прочих равных условиях увеличивает разрешающую способность системы СВН по азимуту, углу места и дальности. Уменьшение поля зрения системы при этом необходимо компенсировать введением пространственного механико-электического сканирования, а после обнаружения БПЛА – эпизодическим трекингом объекта, чтобы он не вышел из поля зрения.

4. Определение сопряженных точек как координат центров $V(x, y)$ областей, выделенных на этапе обнаружения и распознавания БПЛА, дает недостаточно хороший результат на малых дальностях до объекта. Поэтому полагается целесообразным уточнять местоположение сопряженных точек корреляционным методом с размером окна, равным или несколько больше размера области $V(x, y)$.

5. Точность ректификации системы СВН существенно влияет на результат измерения дальности, поэтому к процессу калибровки нужно подходить тщательным образом. Необходимо использовать таблицы с как можно наибольшим числом калибровочных точек, в процессе калибровки различные положения таблицы должны заполнять как можно большую часть рабочей области стереозрения, а ее изображения – как можно большую часть площади кадра.

6. Для уменьшения максимальных ошибок целесообразно проводить усреднение во времени результатов измерений дальности с учетом радиальной скорости перемещения БПЛА.

Список литературы:

1. Farlik J., Kratky M, Casar J, Stary V. Multispectral Detection of Commercial Unmanned Aerial Vehicles // Sensors. 2019. Vol. 19 (7). P.1517–1545.

2. Shapiro L., Stockman G. Computer Vision. Prentice Hall, 2001. 617 p.

3. Computer Vision. CCF Chineese conf. CCCV 2015. Proseedings, Part II / Editors Zha H., Chen X., Wang L., Miao Q. Xi'an, China. September, 2015. 471 p.

4. Mrovlje J., Vrancic D. Distance measuring based on stereoscopic pictures // Proc. 9th International PhD Workshop on Systems and Control. Izola, Slovenia. 2008. 6 p.

5. Gökçe F, Üçoluk G, Şahin E, Kalkan S. Vision-Based Detection and Distance Estimation of Micro Unmanned Aerial Vehicles // Sensors. 2015. Vol. 15 (9). P. 23805–23846.

6. Ma Z., Hu T., Shen L. Stereo Vision Guiding for the Autonomous Landing of Fixed-Wing UAVs: A Saliency-Inspired Approach // International Journal of Advanced Robotic Systems. March, 2016. 13 p.

7. Mustafah Y. M., Azman A. W., Akbar F. Indoor UAV positioning using stereo vision sensor // Procedia Engineering. 2012. Vol. 41. P. 575–579.

8. Kong W., Zhang D., Wang X., Xian Z., J. Zhang. Autonomous landing of an UAV with a ground-based actuated infrared stereo vision system // 2013 IEEE/RSJ International Conference on Intelligent Robots and Systems. Tokyo, 2013. P. 2963–2970.

9. Chaudhuri S., Rajagopalan A.N. Depth from Defocus: A Real Aperture Imaging Approach. Washington: Springer, 1999. 172 p.

10. Патент RU2568335C1. Способ измерения дальности до объектов по их изображениям преимущественно в космосе / Смирнов А.И. Заявл. 22.05.2014; опубл. 20.11.2015, бюл. № 32. 10 с.

11. Andraši P., Radišić T., Muštra M., Ivošević J. Night-time Detection of UAVs using Thermal Infrared Camera // Transportation Research Procedia. Vol. 28. 2017. P. 183–190.

12. Kartashov V., Oleynikov V., Koryttsev I., Zubkov O., Babkin S., Sheiko S. Processing and Recognition of Small Unmanned Vehicles Sound Signals // International Scientific-Practical Conference on Problems of Infocommunications – Science and Technology, PICS&T 2018 – Proceedings. P. 392–396.

13. Oleynikov V.N., Zubkov O.V., Kartashov V.M., Korytsev I.V., Babkin S.I., Sheiko S.A. Investigation of detection and recognition efficiency of small unmanned aerial vehicles on their acoustic radiation // Telecommunications and Radio Engineering. 2019. Vol. 78 (9). P. 759–770.

14. Oleynikov V., Zubkov O., Kartashov V., Koryttsev I., Sheiko S., Babkin S. Experimental estimation of direction finding to unmanned air vehicles algorithms efficiency by their acoustic emission // 2019 International Scientific-Practical Conference on Problems of Infocommunications – Science and Technology, PIC S&T 2019 – Proceedings. P. 175–178.

15. Kartashov V.M., Oleynikov V.N, Sheyko S.A., Babkin S.I., Koryttsev I.V., Zubkov O.V., Anokhin M.A. Information characteristics of sound radiation of small unmanned aerial vehicles // Telecommunications and Radio Engineering. 2018. Vol. 77 (10). P. 915–924.

16. Szeliski R. Computer Vision: Algorithms and Applications. Washington: Springer, 2011. 812 p.

17. Zaarane A., Slimani I., Al Okaishi W., Atouf I., Hamdoun A. Distance measurement system for autonomous vehicles using stereo camera // Array. 2020. Vol. 5. P. 100016–100023.

18. Kusworo A. Distance measurement with a stereo camera // International Journal of Innovative Research in Advanced Engineering. 2017. Vol. 4 (11). P. 24–27.

19. Hou A.L., Cui X., Geng,Y., Yuan J., Hou J. Measurement of Safe Driving Distance based on Stereo Vision // Sixth International Conference on Image and Graphics (ICIG). Hefei, Anhui, China. 2011. P. 902–907.

20. Tsai R.Y. A versatile camera calibration technique for high-accuracy 3D machine vision metrology using off-the-shelf TV cameras and lenses // IEEE Int. Journal on Robotics and Automation. 1987. Vol. 3. P. 323–344.

21. Cipolla R., Drummond T., Robertson D. Camera calibration from vanishing points in images of architectural scenes // BMVC. September, 1999. P. 382–391.

22. Zhang Z. Flexible New Technique for Camera Calibration // IEEE Transaction on Pattern Analysis and Machine Intelligence. 2000. Vol. 22 (11). P. 1330–1334.

23. Bouguet J.Y. MATLAB calibration tool // http://www.vision.caltech.edu/bouguetj/calib_doc.

24. Kartashov V., Oleynikov V., Zubkov O., Sheiko S. Optical detection of unmanned air vehicles on a video stream in a real-time // The Fourth International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo'2019). Odessa, Ukraine. 9–13 September 2019. 4 p.

Поступила в редколлегию 00.00.2020

Сведения об авторах:

Корытцев Игорь Васильевич – канд. техн. наук, доцент, Харьковский национальный университет радиоэлектроники, профессор кафедры медиаинженерии и информационных радиоэлектронных систем, Украина, e-mail: igor.koryttsev@nure.ua, ORCID: https://orcid.org/0000-0003-1875-5534

Шейко Сергей Александрович – канд. техн. наук, доцент, Харьковский национальный университет радиоэлектроники, доцент кафедры медиаинженерии и информационных радиоэлектронных систем, Украина, e-mail: sergiy.sheiko@nure.ua, ORCID: https://orcid.org/0000-0003-1638-4478

Карташов Владимир Михайлович – д-р техн. наук, профессор, Харьковский национальный университет радиоэлектроники, заведующий кафедрой медиаинженерии и информационных радиоэлектронных систем, Украина, e-mail: volodymyr.kartashov@nure.ua, ORCID: https://orcid.org/0000-0001-8335-5373

Зубков Олег Викторович – канд. техн. наук, доцент, Харьковский национальный университет радиоэлектроники, доцент кафедры медиаинженерии и информационных радиоэлектронных систем, Украина, e-mail: Oleh.zubkov@nure.ua, ORCID: https://orcid.org/0000-0002-8528-6540

Олейников Владимир Николаевич – канд. техн. наук, доцент, Харьковский национальный университет радиоэлектроники, профессор кафедры медиаинженерии и информационных радиоэлектронных систем, Украина, e-mail: vladimir.oleinikov@nure.ua, ORCID: https://orcid.org/0000-0001-7197-9760

Бабкин Станислав Иванович – канд. техн. наук, Харьковский национальный университет радиоэлектроники, старший научный сотрудник кафедры медиаинженерии и информационных радиоэлектронных систем, Украина, e-mail: prl.res@nure.ua, ORCID: https://orcid.org/0000-0003-4903-3551

Селезнев Иван Сергеевич – Харьковский национальный университет радиоэлектроники, аспирант кафедры медиаинженерии и информационных радиоэлектронных систем, Украина, ORCID: https://orcid.org/0000-0002-0731-7540

УДК 629.7.022 **DOI:10.30837/rt.2020.3.202.14**

О.В. ЗУБКОВ, канд. техн. наук, С.А. ШЕЙКО канд. техн. наук,
В.Н. ОЛЕЙНИКОВ, канд. техн. наук, В.М. КАРТАШОВ, д-р техн. наук,
И.В. КОРЫТЦЕВ, канд. техн. наук, С.И. БАБКИН, канд. техн. наук

ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ ДЕТЕКТИРОВАНИЯ И РАСПОЗНАВАНИЯ ИЗОБРАЖЕНИЙ ДРОНОВ ПО ВИДЕОПОТОКУ

Введение

В Европе и других странах мира постепенно ужесточаются ограничения на зоны полета дронов. К зонам, в которых запрещены полеты, относятся: военные объекты, аэродромы, места скопления людей, автомагистрали, тюрьмы, промышленные предприятия [1, 2]. Эти ограничения связаны с обеспечением безопасности людей и конфиденциальностью информации. Поэтому растет спрос на современные электронные системы обнаружения и классификации дронов для контроля периметров охраняемых территориях [3]. Одним из вариантов подобных систем являются системы анализа видеоизображения охранных камер видеонаблюдения. Данная статья посвящена исследованию эффективности обнаружения дронов по видеопотоку стационарной видеокамеры. При обработке видеопотока возможно применение двух основных подходов: анализ всего изображения с использованием нейронной сети и анализ фрагментов изображения, в которых обнаружено движение объектов. Первый подход реализован в алгоритме YOLO на базе нейронной сети DarkNet [4]. Для его применения требуется подготовка обучающей базы изображений с дронами и другими движущимися объектами, обучение и тестирование сети. Однако анализ возможностей данного алгоритма говорит о ряде его ограничений. Первое ограничение – это сложность математической обработки, что делает невозможным реализацию обработки изображений в реальном масштабе времени на базе компьютерных процессоров с малым количеством ядер. При применении процессора i7 в сочетании с библиотекой OpenCV и операционной системой Linux предельная скорость обработки – до четырех кадров в секунду. Для обработки видеопотока в реальном масштабе времени необходимо применение высокопроизводительных GPU типа NVIDIA GeForce 1080 [5]. Однако при обнаружении дронов основным является второе ограничение алгоритма YOLO. Перед подачей на нейронную сеть любое изображение с видеокамеры должно быть пересчитано во входное, соответствующее нейронной сети с максимальным разрешением 416x416 пикселей [6]. Размер обнаруживаемого на этом изображении объекта не должен быть меньше 7x7 пикселей. Например, при горизонтальном размере квадрокоптера DJI Phantom 3 0,35м, угле обзора видеокамеры наблюдения 60° и ширине изображения 416 пикселов на входе сети для алгоритма YOLO можно оценить значение предельного расстояния обнаружения. Оно не превышает 18 м. В зонах с запретом на полеты дронов такой дальности обнаружения недостаточно, так как эти зоны занимают значительные площади. Для таких зон дальность обнаружения должна быть не менее 50 – 100м. Некоторым исследователям [6] удалось повысить входное разрешение алгоритма YOLO до 832x832 пиксела. Однако это увеличение нельзя считать существенным и оно требует значительного увеличения быстродействия устройства обработки изображения. Анализ существующих алгоритмов обнаружения и классификации объектов по видеопотоку камеры позволил сформулировать ряд задач для исследования, решение которых позволит создать недорогую систему обнаружения и классификации дронов на значительных расстояниях. К ним относятся: обнаружение дронов на расстояниях не менее 50 – 100 м и возможность применения недорогих вычислительных устройств или блоков для обработки изображения видеокамеры. Для решения сформулированных задач исследований авторами был разработан алгоритм, сочетающий высокую производительность, эффективность распознавания и возможность обработки изображений с любым разрешением.

Алгоритм обнаружения и классификации движущихся объектов

Разработанный алгоритм обнаружения и классификации движущихся объектов состоит из двух этапов: 1) обнаружение на текущем кадре всех фрагментов изображения, в которых выявлено движение; 2) подача массива этих фрагментов на вход обученной нейронной сети для их классификации.

Первый этап обработки изображения состоит из следующих шагов:

1) Преобразование цветного изображения в оттенки серого, и выполнение нормализации его яркости для уменьшения влияния изменений интенсивности освещения под действием суточных и погодных факторов. Нормализация яркости выполнялась по формуле [7]

$$G_{i,j} = 255\frac{P_{i,j} - I_{\min}}{I_{\max} - I_{\min}}, \quad (1)$$

где – яркость пикселей исходного изображения; i = 1,2, ..., H; i = 1,2, ..., W; H и W – высота и ширина изображения соответственно; $I_{\min}$ – минимальное значение исходной яркости изображения; $I_{\max}$ – максимальное значение исходной яркости изображения; $G_{i,j}$ – пиксель изображения с нормализованной гистограммой.

2) Выделение всех движущихся фрагментов изображения в текущем видеокадре на неподвижном фоне. На этом шаге исследований была проанализирована эффективность работы адаптивних моделей заднего фона изображений, таких как MOG, MOG2, KNN, GMG, CNT, GSOC, LSBP [13 – 20]. Результатом работы этих методов является черно-белое изображение, в котором черным цветом отображается неподвижный фон, а белые фрагменты изображения соответствуют областям движения (рис. 1).

Критериями эффективности являются: быстродействие работы модели и количество ложных контуров движущихся объектов в видеокадре.

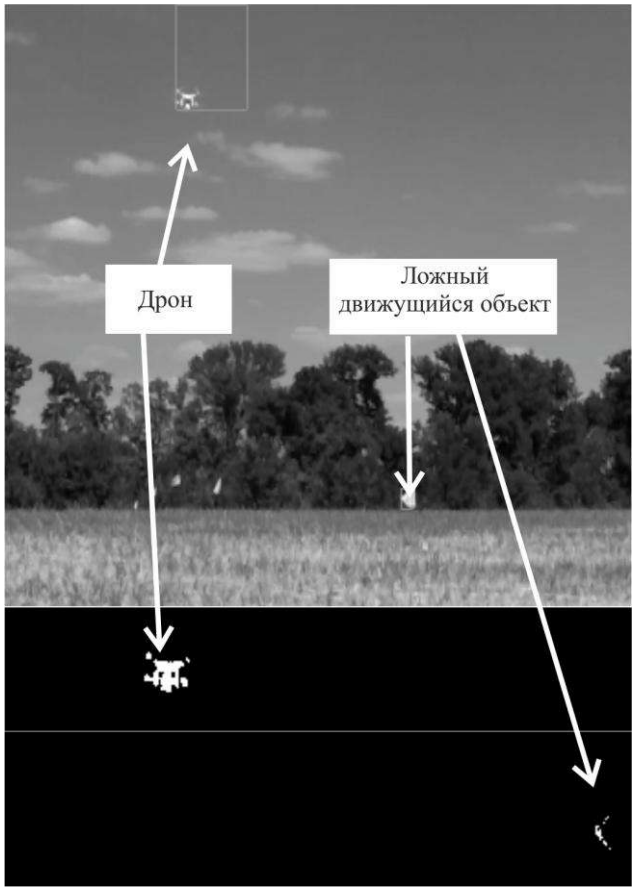


Рис. 1. Пример результата выделения на неподвижном фоне движущихся объектов: квадрокоптера и флажка

3) Применение ко всем фрагментам изображения, в которых обнаружено движение, алгоритма истории движения. Одной из наших приоритетных задач является обнаружение дрона на значительных расстояниях – до 100 м и более. При таких дальностях фрагмент изображения, содержащий дрон, очень мал. Например, при разрешении видеокамеры 1920x1080, угле ее обзора 60° на расстоянии 116 м изображение DJI Phantom 3 имеет размеры 5x5 пикселов. Столь малый фрагмент соизмерим с фрагментами, в которых обнаруживается движение под действием колебаний листвы деревьев, травы и т.д. Поэтому анализ движения производится на некотором интервале времени. Для этого создается фоновое изображение в оттенках серого с тем же разрешением, что и исходное.

На него накладывается результат работы одного из алгоритмов MOG, GMG, MOG2, KNN, CNT, GSOC, LSBP после обработки каждого кадра с видеокамеры. Перед наложением интенсивность каждого пиксела фонового изображения уменьшается на величину

$$\Delta I = \frac{255}{\Delta t \cdot FPS} \tag{2}$$

где 255 – предельная интенсивность пикселов; Δt – интервал анализа истории движения, с; FPS – частота кадров в секунду. В результате на фоновом изображении происходит наложение контуров движущихся объектов в группе кадров за интервал Δt и движущийся объект представляется результирующим контуром со значительно большей площадью, чем в одиночном кадре (рис. 2).

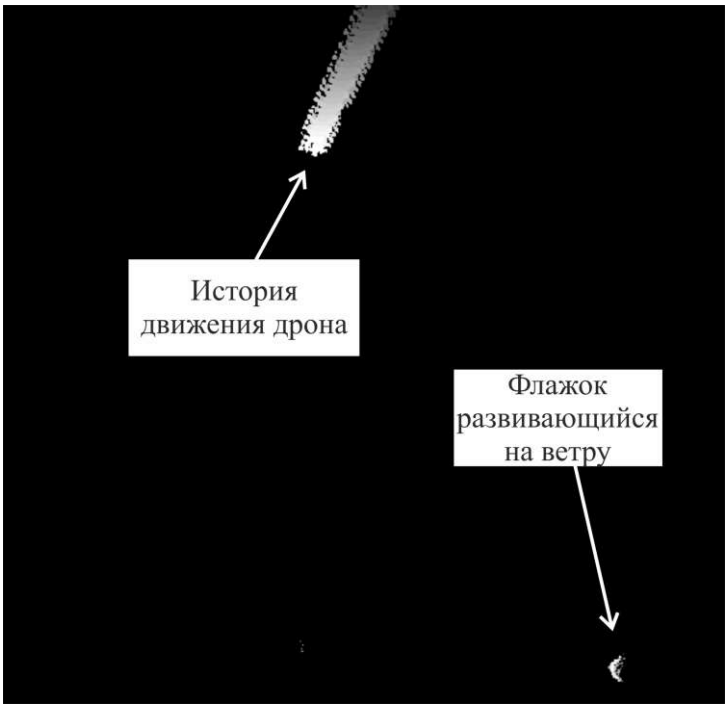


Рис. 2. Изображение, которое содержит историю движения двух объектов:
квадрокоптера DJI Phantom 3 и флажка

4) Для дальнейшего анализа выбираются контуры с площадью, превышающей заданное пороговое значение, то есть происходит частичное отсечение колебаний листвы деревьев и травы. Все контуры, удовлетворяющие этому критерию, будем считать контурами условно движущихся объектов. Также для каждого условно движущегося объекта в текущем кадре вычисляются его координаты для его локализации в полном изображении и вырезка изображений этих объектов с целью подачи на вход нейронной сети.

Второй этап обработки изображений заключается в классификации фрагментов изображений, соответствующих областям движения, с применением нейронных сетей. Сначала был проанализирован перечень подвижных объектов, которые могут оказаться в зоне видимости

видеокамеры. К ним относятся: дроны, люди, домашние животные, птицы, насекомые, легковые и грузовые автомобили, лошади, лодки и корабли, самолеты, фрагменты движущихся облаков, фрагменты качающихся ветвей деревьев и травы. Всего для исследований использовалось 12 классов объектов. После этого были созданы модели классических и сверточных нейронных сетей, проведено их обучение и экспериментальная проверка.

Проведение экспериментов

Для экспериментальной проверки эффективности разработанного алгоритма на протяжении трех сезонов (лето, осень, зима) проводились видеозаписи полетов дронов. Для записи видео использовалась видеокамера Dahua DH-IPC-HFW2431RP-ZAS-IRE6 с разрешением 2688(H)x1520(V). Камера была настроена с разрешением 1920x1080 и углом обзора 60°. Запись видео производилась при различных погодных условиях в дневное и вечернее время на территории города и в пригородной зоне. В экспериментах использовались две модели квадрокоптеров: DJI Phantom 4 и Hubsan x4 air h501m. Для определения расстояния от видеокамеры до квадрокоптера во время полета дрона проводилась запись его GPS координат с последующей привязкой момента начала полета к видеозаписи стационарной видеокамеры. Пример одной из рассчитанных траекторий приведен на рис. 3.

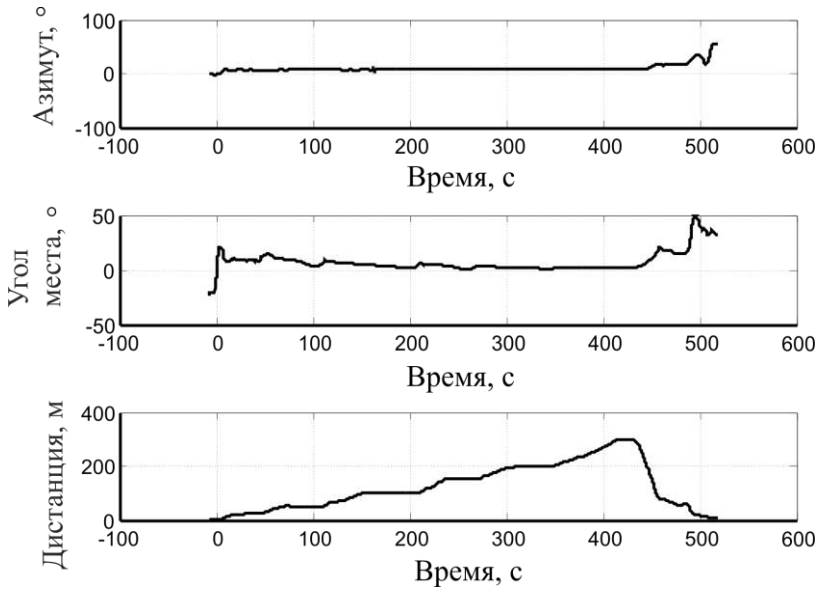


Рис. 3. Пример траектории движения квадрокоптера,
вычисленный по результатам логирования GPS координат квадрокоптера

Подготовка баз данных для обучения и тестирования нейронных сетей

Для обучения и тестирования моделей нейронных сетей авторами статьи были созданы наборы данных изображений с четырьмя классами объектов: дроны, насекомые, фрагмены листвы деревьев и травы, фрагменты неба с облаками. Для составления набора данных изображений с дронами с ресурса YouTube было скачано порядка 300 видеороликов с полетами порядка 14 модификаций различных дронов. Авторами статьи был разработан специальный видеоредактор на языке Python в среде PyCharmCommunity. С его помощью из видеокадров вырезаны 5000 изображений дронов, и каждое изображение автоматически сохранено с разрешениями: 5x5, 9x9, 13x13, 27x27, 49x49, 64x64, 128x128 пикселов. Также эти видео использованы для создания наборов данных изображений с фрагментами деревьев, облаков и травы. 4000 изображений использовались на этапе обучения нейронных сетей, а 1000 изображений – для их тестирования после окончания обучения (рис. 4).

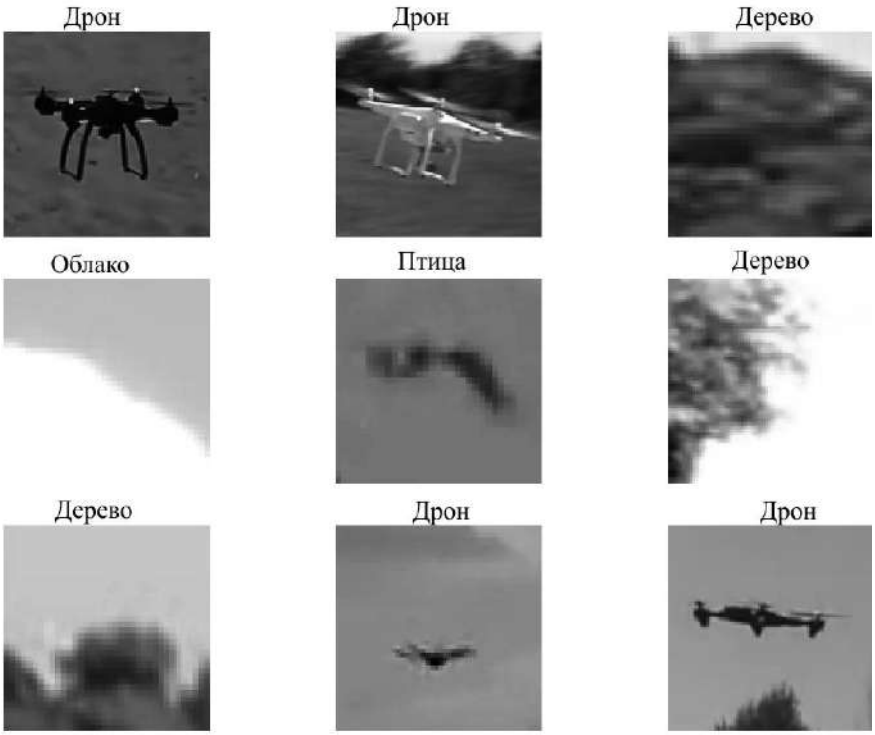


Рис. 4. Примеры изображений дронов, фрагментов облаков, листвы деревьев и травы из созданных наборов данных

Аналогично был разработан набор данных изображений насекомых.

Наборы данных для таких классов объектов, как: легковые и грузовые автомобили, животные, птицы, люди, самолеты, лодки и корабли были взяты из готовых наборов данных CIFAR-10 с сайта https://www.cs.toronto.edu/~kriz/cifar.html. Набор данных каждого класса содержит 4500 цветных изображений с разрешением 32x32 пиксела. Данный сетевой ресурс также содержит набор данных для тестирования обученной сети.

Результаты экспериментальных исследований выделения движущих объектов на неподвижном фоне

Обработка видеофайлов проводилась с использованием программного обеспечения MiniConda и PyCharmCommunity, а также с применением библиотеки компьютерного зрения OpenCV v4.

При анализе эффективности работы алгоритма MOG мы изменяли его параметры: количество кадров, на основании которых рассчитывается модель фона, количество гауссовых смесей, коэффициент шума и уровень шума. Диапазон значений оптимального количества кадров для построения модели фона находится в пределах 80 – 130, что соответствует временному интервалу порядка 3,2 – 5,2с при частоте кадров видеокамеры 25 кадров/с. При уменьшении этого числа наблюдается ухудшение выделения объекта и его дробление на группу более мелких частей. С увеличением числа кадров, по которому строится модель, существенно увеличивается время адаптации модели, что негативно сказывается в ситуациях изменения глобальной освещенности пространства (например, в момент, когда туча закрывает солнце или сильный ветер образует облако пыли). По нашим оценкам, метод позволяет обрабатывать до 10 – 11 кадров/с при разрешении камеры 1920x1080 пикселов. Под обработкой подразумевается не только работа самого алгоритма MOG, но и построение истории движения по 100 кадрам, а также детектирование контуров всех условно движущихся объектов, которые выделены на неподвижном фоне. Оптимальным диапазоном значений параметра “уровень шума” модели MOG является диапазон величин 20 – 25, он соответствует обнаружению летящего дрона до расстояния 120 – 140м. При уменьшении этого параметра вдвое

наблюдается значительное увеличение количества контуров условно движущихся объектов до 2 – 3 раз при отсутствии изменений общей интенсивности освещенности и без движения крупных объектов. При резких изменениях общей освещенности или движении крупных объектов количество контуров возрастает в 3 – 8 раз. С увеличением значения параметра “уровень шума” вдвое количество контуров сокращается, но снижается дальность обнаружения дрона до 50 – 60м. Диапазон оптимальных значений параметра “количество гауссовых смесей” находится в пределах 4 – 8. С двукратным увеличением значения этого параметра снижается скорость обработки кадров до 8 – 9 кадров/с. При двукратном уменьшении значения этого параметра количество условно движущихся объектов увеличивается в 1,2 раза. Значение параметра “коэффициент шума” слабо влияет на результат обнаружения движущихся объектов.

При исследовании эффективности работы алгоритма MOG2 мы анализировали влияние количество кадров, на основании которых рассчитывается модель фона и порог на квадрате расстояния Махаланобиса между пикселем и моделью. Значения первого параметра следует выбирать из диапазона 100 – 140, что соответствует скорости обработки до 11 – 13 кадров/с. Увеличение этого значения приводит к существенному снижению скорости обработки до 3 – 4 кадров/с в моменты резкого изменения общей освещенности и до 9 – 10 кадров/с – при отсутствии глобальных изменений в видеокадре. Значения второго параметра следует выбирать из диапазона 100 – 150. Уменьшение величины этого параметра вдвое приводит к увеличению числа условно движущихся объектов в 2 -6 раз, а увеличение величины этого параметра свыше 160 приводит к снижению дальности обнаружения дрона. Так, при величине этого параметра порядка 200 дальность снижается до 90 м.

При реализации алгоритма KNN было проанализировано влияние количества кадров, по которому рассчитывается модель и порога на квадрате расстояния между пикселем и образцом. Диапазон рабочих значений первого параметра находится в диапазоне 100 – 200. При этом достигается скорость обработки видеопотока 11 – 12 кадров/с. Дальнейшее увеличение величины этого параметра приводит к значительному повышению числа обнаруживаемых условно движущихся объектов. Оптимальный для нашей задачи диапазон значений второго параметра в пределах от 5000 до 10000. Уменьшение значения этого параметра приводит к существенному увеличению числа обнаруживаемых условно движущихся объектов, а увеличение значения этого параметра приводит к уменьшению дальности обнаружения ниже 120 м и разделение крупных объектов на группу более мелких.

Тестирование алгоритма GMG показало его высокую чувствительность к движению облаков, листвы деревьев, травы и чрезвычайно низкую скорость работы – порядка 1 – 3 кадров/с. Аналогичными недостатками обладает алгоритм CNT.

Применение алгоритма GSOC позволяет достичь скорости обработки видеопотока до 5 – 6 кадров/с и дальности обнаружения дрона до 90 м.

Итогом анализа стал выбор моделей MOG, MOG2, KNN для реализации алгоритма выделения движущихся объектов на неподвижном фоне для их дальнейшей классификации с применением нейронных сетей.

Результаты экспериментальных исследований обнаружения дронов с применением нейронных сетей

Для проведения исследований была выбрана популярная открытая библиотека машинного обучения Keras, совместимая с TensorFlow. Она была подключена к платформе MiniConda, и для написания программ обучения сетей и их тестирования использовался язык программирования Python. Для обучения сетей и тестирования их эффективности применялись описанные выше наборы данных, часть из которых была создана авторами статьи, а часть – загружена из открытых баз данных. Основными критериями анализа были: скорость обработки данных, вероятность правильного распознавания и вероятность ложного обнаружения дрона.

С точки зрения достижения высоких скоростей обработки данных целесообразно использовать простые последовательные полносвязные модели сети. Дополнительный прирост производительности обеспечивает преобразование цветного изображения объекта распознавания в оттенки серого и его дальнейшая классификация нейронной сетью. Вторым широко распространенным в практических задачах классом нейросетей являются сверточные сети. Эти сети прекрасно зарекомендовали себя в алгоритмах, подобных YOLO, и обладают возможностью распараллеливания операций обработки, инвариантны к повороту изображения, что актуально для различных ракурсов наблюдения дрона и его кренов во время полета. Основным недостатком таких сетей является сложность настройки параметров сети, так как их количество велико, а процесс обучения длителен.

Для исследования эффективности простых полносвязных сетей были выбраны три модели. Первая модель состоит их входного слоя (нормированных значений яркостей пикселов изображения), одного промежуточного слоя из 1024 нейронов и выходного слоя с 12 выходами, соответствующими 12 классам объектов классификации. Во второй модели добавлен еще один промежуточный слой из 256 нейронов, а в третьей – два промежуточных слоя из 256 и 120 нейронов соответственно. На вход сети подавались изображения в градациях серого с разрешением 27x27 пикселов. Графики зависимостей точности обучения и потерь от количества эпох обучения приведены на рис. 5.

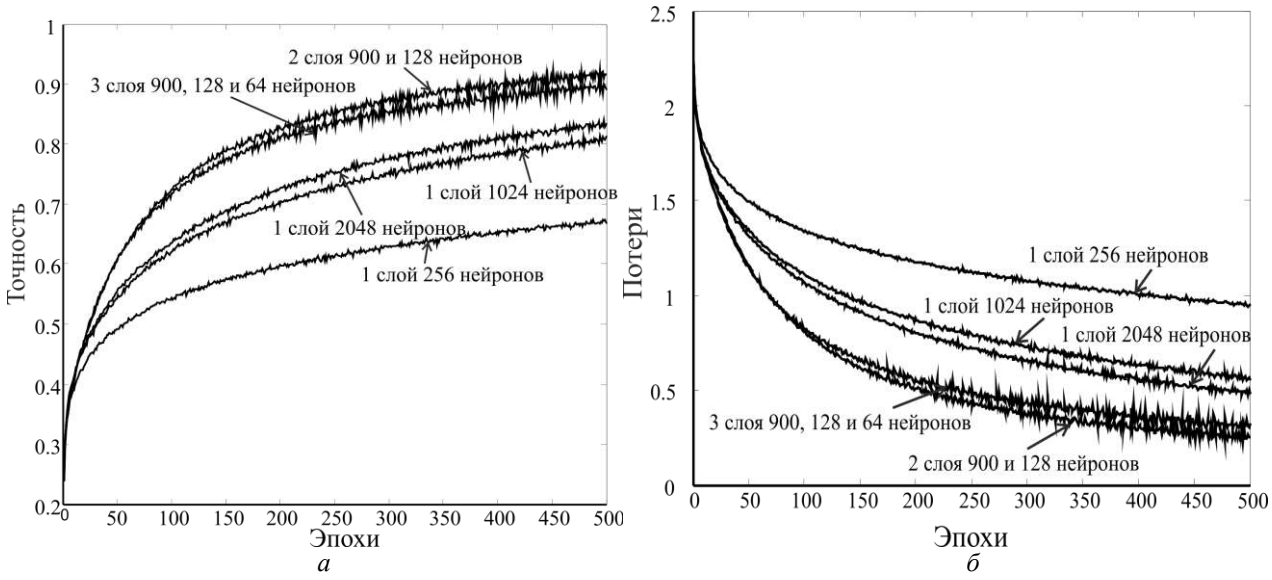


Рис. 5. Зависимости точности обучения (*а*) и потерь (*б*) полносвязных нейронных сетей от количества эпох обучения

Анализ зависимостей, приведенных на рис. 5, показывает: 1) для сетей с одним промежуточным слоем целесообразно использовать не менее 1000 нейронов в этом слое; 2) при увеличении количества промежуточных слоев свыше двух точность обучения начинает снижаться.

Тестирование обученной нейронной сети проводилась двумя способами. Первый – классический способ, при реализации которого используются тестовые наборы данных, состоящие из 1000 изображений дронов и от 500 до 1000 изображений на каждый из остальных классов.

Второй способ – тестирование при обработке снятых нами видеороликов с полетами дронов. Этот способ заключается в следующей последовательности действий:

- после окончания формирования модели заднего фона с применением алгоритмов MOG, MOG2 или KNN для каждого кадра потокового видео выделяются контуры условно движущихся объектов;

- каждый контур аппроксимируется квадратом со стороной, равной наибольшему из продольных размеров контуров;

- из общего изображения вырезается фрагмент, соответствующий координатам этого квадрата;

- разрешение фрагмента изображения пересчитывается в соответствующее обученной нейронной сети и преобразуется в оттенки серого;

- после обработки фрагмента изображения нейронной сетью принимается решение об обнаружении дрона. Критерий обнаружения – максимальное значение вероятности, соответствующее классу дрона из имеющихся классов объектов;

- по окончании обработки фрагмента видео с полетом дрона на расстояниях до 60 м формируются результирующие оценки вероятности верной классификации дронов p_t и вероятности ложного принятия решения p_f о наличии дрона.

Значения точности распознавания для тестовых наборов данных приведены в табл. 1.

Таблица 1

Значение	Тестовые наборы	Обработка видео	
	Accuracy	p_t	p_f
1 layer 256 neurons	0,5	0,23	0,09
1 layer 1024 neurons	0,81	0,63	0,051
1 layer 2048 neurons	0,78	0,58	0,059
2 layers 900 and 128 neurons	0,83	0,66	0,043
3 layers 900, 128 and 64 neurons	0,81	0,65	0,045

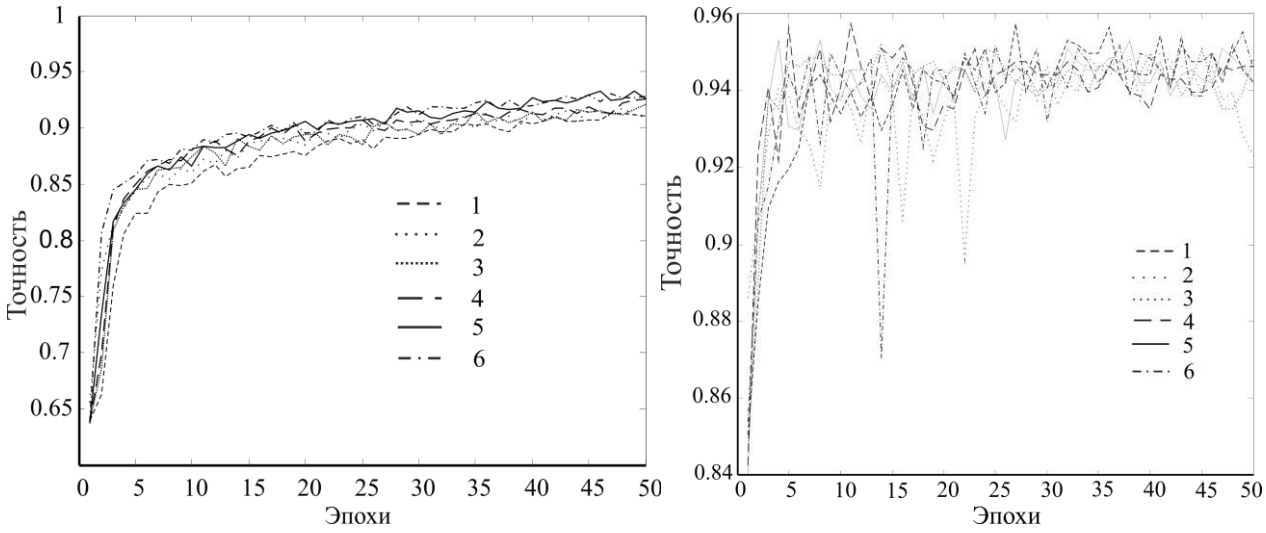
На основании результатов тестирования и экспериментальной проверки моделей полносвязных сетей был сделан вывод об их низкой эффективности для решения поставленной задачи. Поэтому было решено проанализировать эффективность работы сверточных сетей.

Для обучения сверточных нейронных сетей использовались ранее созданные наборы данных, содержащие 12 классов объектов. Однако при обучении сетей и их тестировании использовались цветные изображения, а не преобразованные в оттенки серого. Мы также решили увеличить объем базы для обучения за счет добавления в обучающие наборы копий исходных изображений, к которым были применены несколько аффинных преобразований: поворот изображения на угол 45°, зеркальное горизонтальное отражение. Первое преобразование позволяет смоделировать крены при полете дрона, второе преобразование связано с особенностями конструкции дронов. Дроны имеют, как правило, симметричную конструкцию, а большинство других объектов, таких как птицы, автомобили, кошки, собаки при виде сбоку не обладают симметрией. Для исследований использовались сети, состоящие из нескольких сверточных, одного полносвязного промежуточного и выходного слоев. К результатам сверток применялась функция MaxPool. Обучение проводилось в течение 50 эпох. Характеристики проанализированных сетей представлены в виде табл. 2.

Таблица 2

Номер модели	Количество сверток в сверточных слоях				Число нейронов в полносвязном слое
1	16	32			512
2	16	32			1024
3	16	32	64		512
4	16	32	64		1024
5	32	64	128		512
6	32	64	128	256	512

Графики зависимостей точности обучения и обнаружения дронов на тестовом наборе данных от количества эпох обучения приведены на рис. 6.



а *б*

Рис. 6. *а* – график зависимостей точности обучения от количества эпох обучения; *б* – график зависимостей точности обнаружения дронов на тестовом наборе данных от количества эпох обучения

Анализ полученных зависимостей позволил сделать следующие выводы:

- значения точности проанализированных моделей сверточных сетей отличаются несущественно в пределах 3 %;
- точность на обучающем наборе данных ниже, чем на тестовом, что объясняется дополнением исходного набора изображений копиями этих изображений, к которым применялись аффинные преобразования;
- наилучшие результаты показали 5-я и 6-я модели сверточных сетей;
- использование в полносвязном слое свыше 512 нейронов не повышает точности.

Дополнительные исследования, результаты которых не приведены на рис. 6, показали, что снижение количества нейронов в полносвязном слое ниже 256 негативно сказывается на результирующей точности. Также дополнительные исследования с сетями, содержащими пять сверточных слоев, показали, что эти сети не позволяют повысить точность в сравнении с моделями 5 и 6.

Эффективность работы сверточных сетей также была проанализирована на совокупности снятых видеороликов. Результаты этих исследований приведены в табл. 3.

Таблица 3

Номер модели	p_t	p_f
1	0,85	0,01
2	0,85	0,008
3	0,87	0,007
4	0,88	0,006
5	0,88	0,005
6	0,89	0,007

Для обученной сети с номером 3 были проведены исследования достоверности обнаружения в зависимости от расстояния до объекта. Чтобы оценить достоверность мы использовали созданные ранее наборы данных в разных разрешениях от 5x5 до 128x128 пикселов. Разрешение каждого из изображений перед подачей на вход сети пересчитывалось в формат 32x32 пикселов. Для каждого из разрешений рассчитывалось соответствующее значение рас-

стояния исходя из угла зрения видеокамеры 60° и разрешения видеокамеры 1920x1080 пикселов. Результат исследований представлен на рис. 7.

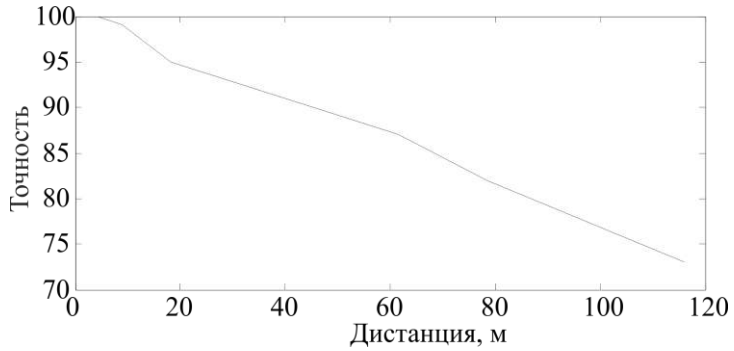


Рис. 7. Зависимость точности обнаружения от расстояния до дрона

Выводы

Разработан и экспериментально протестирован алгоритм обработки видеопотока стационарной видеокамеры наблюдения, позволяющий обнаруживать дроны на значительных расстояниях. Алгоритм разделен на два основных этапа: обнаружение всех движущихся объектов и их дальнейшая классификация. В сравнении с существующими алгоритмами, такими как YOLO, у алгоритма нет ограничений на разрешение обрабатываемого изображения. Поэтому для камер высокого разрешения (4K, 8K и т.д.) можно повысить дальность обнаружения дронов пропорционально увеличению разрешения камеры. Дополнительным преимуществом является возможность классификации не только дронов, но и других движущихся объектов, таких как: автомобили, люди, животные, что актуально для охранных систем. Эту возможность обеспечивает нейронная сеть, классифицирующая 12 типов подвижных объектов. Экспериментальная проверка предложенного алгоритма доказала его работоспособность и высокую скорость обработки видеопотока (не ниже 8 кадров/с) без использования GPU аналогичных NVIDIA GeForce 1080. Применение моделей простых полносвязных нейронных сетей для классификации движущихся объектов оказалось неэффективным при обработке видеопотока камеры, так как точность классификации на реальных видопотоках значительно ниже, чем на обучающем и тестовом наборах данных. Тестирование моделей сверточных сетей доказало их эффективность для поставленной задачи, так как результаты экспериментальной обработки видеопотоков идентичны результатам обучения и тестирования на наборах данных.

Предложенный алгоритм позволяет обнаруживать и распознавать движущиеся объекты с разрешением не ниже, чем 5x5 пикселов, что соответствует дальностям до 120 м при разрешении камеры FullHD и угле обзора 60°. Полученное значение точности распознавания порядка 89 %, на наш взгляд, может быть повышено благодаря дальнейшему совершенствованию обучающих баз для выбранных нейронных сетей и выбору более оптимальной модели сети. Планируется продолжение исследований в этом направлении.

Список литературы:

1. https://dronerules.eu/en/recreational/regulations

2. BBC (2018) Charges over drone drug smuggling into prisons. https://www.bbc.com/news/uk-england-43413134.

3. Jean-Paul Yaacoub, Hassan Noura, Ola Salman, Ali Chehab. Security analysis of drones systems // Attacks, limitations, and recommendations: Internet of Things. Volume 11, pages 1-39, 2020.

4. Kartashov V. M., Oleynikov V. N., Sheyko S. A., Koryttsev I. V., Babkin S.I., Zubkov O.V. Peculiarities of small-sized unmanned aerial vehicles detection and recognition // Telecommunications and Radio Engineering. Volume 78, Issue 9, pages 771-781, 2019.

5. Deep Learning on Multi Sensor Data for Counter UAV Applications – A Systematic Review. Stamatios Samaras, Eleni Diamantidou, Dimitrios Ataloglou, Nikos Sakellariou, Anastasios Vafeiadis, Vasilis Magoulianitis, Antonios

Lalas, Anastasios Dimou, Dimitrios Zarpalas, Konstantinos Votis, Petros Daras, Dimitrios Tzovaras. Sensors (Basel) 2019 Nov; 19(22): 4837. Published online 2019. Nov 6. doi: 10.3390/s19224837.

6. Redmon J., Divvala S., Girshick R. and Farhadi A. You Only Look Once: Unified, Real-Time Object Detection // 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Las Vegas, NV, pages 779-788, 2016, doi: 10.1109/CVPR.2016.91.

7. Hao Liu1, Fangchao Qu1, Yingjian Liu1, Wei Zhao1, Yitong Chen A drone detection with aircraft classification based on a camera array IOP // Conf. Series: Materials Science and Engineering 322 (2018).

8. Ammar A., Koubaa A., Ahmed M., Saad A. Aerial Images Processing for Car Detection using Convolutional Neural Networks: Comparison between Faster R-CNN and YoloV3. Preprints 2019, 2019100195 (doi: 10.20944/preprints201910.0195.v1).

9. Song Han, W. Shen, Z. Liu Deep Drone: Object Detection and Tracking for Smart Drones on Embedded System // Computer Science, 2016.

10. Wen Shao, Rei Kawakami,Ryota Yoshihashi, Shaodi You, Hidemichi Kawase &Takeshi Naemura Cattle detection and counting in UAV images based on convolutional neural networks // International Journal of Remote Sensing Volume 41- NO 1, pages 31-52, 2020.

11. Unlu E., Zenou E., Riviere N. et al. Deep learning-based strategies for the detection and tracking of drones using several cameras // IPSJ T Comput Vis Appl Vol. 11, 2019.

12. Marcin Kociołeka, Michał Strzeleckia, Rafał Obuchowicz. Does image normalization and intensity resolution impact texture classification? // Computerized Medical Imaging and GraphicsVolume 81, 2020.

13. Tomasz Hyla, Natalia Wawrzyniak. Automatic Ship Detection on Inland Waters: Problems and a Preliminary Solution // ICONS 2019: The Fourteenth International Conference on Systems, pages 56-60.

14. T. Trnovszký, P. Sýkora, R. Hudec. Comparison of Background Subtraction Methods on Near Infra-Red Spectrum Video Sequences // Procedia Engineering Volume 192, pages 887-892, 2017.

15. Yao G., Lei T., Zhong J., Jiang, P., Jia, W. Comparative Evaluation of Background Subtraction Algorithms in Remote Scene Videos Captured by MWIR Sensors // Sensors 2017, Vol. 17, pages 19-45.

16. Marcomini L. A., Cunha A. L. A Comparison between Background Modelling Methods for Vehicle Segmentation in Highway Traffic Videos. // Computer Vision and Pattern Recognition, 2018.

17. Kartashov V., Oleynikov V., Zubkov O., Sheiko S. Optical detection of unmanned air vehicles on a video stream in a real-time // The Fourth International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo'2019), 9–13 September 2019, Odessa, Ukraine, 4 p.

18. Moulay A. Akhloufi, Sebastien Arola, Alexandre Bonnet. Drones Chasing Drones: Reinforcement Learning and Deep Search Area Proposal. Drones, Vol. 58, No.3, 2019.

19. Yamashita R., Nishio M., Do R.K.G. et al. Convolutional neural networks: an overview and application in radiology // Insights Imaging Vol. 9, pages 611–629, 2018.

20. Vivienne Sze, Yu-Hsin Chen, Tien-Ju Yang, Joel Emer Efficient Processing of Deep Neural Networks: A Tutorial and Survey Computer Science, 2017.

Поступила в редколлегию 29.09.2020

Сведения об авторах:

Зубков Олег Викторович – канд. техн. наук, доцент, Харьковский национальный университет радиоэлектроники, доцент кафедры медиаинженерии и информационных радиоэлектронных систем, Украина, e-mail: Oleh.zubkov@nure.ua, ORCID: https://orcid.org/0000-0002-8528-6540

Шейко Сергей Александрович – канд. техн. наук, доцент, Харьковский национальный университет радиоэлектроники, доцент кафедры медиаинженерии и информационных радиоэлектронных систем, Украина, e-mail: sergiy.sheiko@nure.ua, ORCID: https://orcid.org/0000-0003-1638-4478

Олейников Владимир Николаевич – канд. техн. наук, доцент, Харьковский национальный университет радиоэлектроники, профессор кафедры медиаинженерии и информационных радиоэлектронных систем, Украина, e-mail: vladimir.oleinikov@nure.ua, ORCID: https://orcid.org/0000-0001-7197-9760

Карташов Владимир Михайлович – д-р техн. наук, профессор, Харьковский национальный университет радиоэлектроники, заведующий кафедрой медиаинженерии и информационных радиоэлектронных систем, Украина, e-mail: volodymyr.kartashov@nure.ua, ORCID: https://orcid.org/0000-0001-8335-5373

Корытцев Игорь Васильевич – канд. техн. наук, доцент, Харьковский национальный университет радиоэлектроники, профессор кафедры медиаинженерии и информационных радиоэлектронных систем, Украина, e-mail: igor.koryttsev@nure.ua, ORCID: https://orcid.org/0000-0003-1875-5534

Бабкин Станислав Иванович – канд. техн. наук, Харьковский национальный университет радиоэлектроники, старший научный сотрудник кафедры медиаинженерии и информационных радиоэлектронных систем, Украина, e-mail: prl.res@nure.ua, ORCID: https://orcid.org/0000-0003-4903-3551

УДК 551.501.7 **DOI:10.30837/rt.2020.3.202.15**

В.И. ЛЕОНИДОВ, канд. техн. наук, В.В. СЕМЕНЕЦ, д-р техн. наук

АНАЛИЗ ЧАСТОТНО-ВРЕМЕННОЙ СТРУКТУРЫ АКУСТИЧЕСКИХ ШУМОВ МАЛЫХ АВТОМАТИЧЕСКИХ АЭРОСИСТЕМ

Введение

Область применения современных малых автоматических аэросистем (МАА) непрерывно расширяется. Исследование акустического шума, создаваемого МАА, началось практически одновременно с их созданием. Стимулом к проведению этих исследований служит область практического применения МАА [1 – 3].

Шум МАА изучают при их использовании в биологии для наблюдения за поведением животных и насекомых в различных ситуациях, так как при этом шум дронов может оказывать влияние на исследуемые виды фауны [4, 5]. Похожие явления возникают при использовании дронов в сельском хозяйстве и в проблемах экологии [6, 7].

Кроме того, МАА могут использоваться для несанкционированного мониторинга различных объектов [8, 9]. В связи с этим возникает также задача разработки правил своевременного обнаружения МАА.

Использование известных методов обнаружения воздушных целей для обнаружения МАА имеет ряд особенностей.

Для радиолокационных средств обнаружения, работающих в сантиметровом и миллиметровом диапазонах электромагнитных волн, МАА являются малозаметными целями, так как для их изготовления, как правило, используются радиопрозрачные материалы и, следовательно, эти объекты имеют малую эффективную поверхность рассеивания (ЭПР).

Обнаружение МАА в диапазоне видимого света с помощью видеокамер ограничено дневным временем суток или требует дополнительной подсветки с помощью прожекторов. Этот метод не может быть использован также и в условиях возникновения тумана.

В большинстве случаев МАА являются очень слабыми источниками инфракрасного излучения, поэтому их обнаружение с помощью средств пассивной локации в инфракрасном диапазоне электромагнитных волн также является малоперспективным.

Обнаружение этих объектов по сигналам их связи с командным пунктом может оказаться возможным только в том случае, если в системе не используется полностью автономный режим выполнения полетного задания с однократным режимом передачи полученных данных в конце полета.

Одним из направлений решения задачи обнаружения МАА может быть регистрация акустического сигнала (шума), создаваемого их силовыми установками. Однако при использовании этого метода следует учитывать ряд особенностей.

Внешние по отношению к МАА акустические поля, которые создаются турбулентностью атмосферы и различными техническими средствами, относятся к нестационарным случайным процессам и по мощности могут значительно превышать мощность акустического сигнала, генерируемого МАА. При этом временная амплитудно-частотная структура сигналов МАА не является заданной априори (в отличие от радиолокации).

Обнаружение акустических сигналов МАА должно осуществляться в непрерывном режиме методом пассивной акустической локации. В этом случае задача обнаружения нестационарного случайного процесса, к которым относится сигнал МАА, на фоне нестационарного фонового шума становится в общем случае неопределенной.

В связи с приведенными особенностями для решения задачи обнаружения МАА необходимо учитывать два положения:

- энергетическое обнаружение цели возможно только при наличии информация о мощности только фонового шума в реальном времени;

- свести задачу обнаружения к обнаружению известного сигнала возможно только при известной временной амплитудно-частотной структуре акустического сигнала МАА.

В данном случае понятие «фоновый шум» означает композицию любых источников акустических сигналов за исключением шума дронов. В общем случае фоновый шум есть процесс нестационарный, поэтому использование априорных данных об уровне фонового шума, полученных при гарантированном отсутствии шума МАА, для решения задачи обнаружения в реальном времени приводит к неопределенности, так как рассчитанный по априорным данным пороговый уровень сигнала может быть превышен любым случайно включившимся источником.

Следовательно, в данном случае решение задачи обнаружения сигналов МАА сводится к решению задачи распознавания сигналов.

Цель работы – выявление информативных признаков временной амплитудно-частотной структуры сигналов МАА (дронов), которые характеризуются устойчивой повторяемостью от опыта к опыту, и, следовательно, могут быть использованы для надежного распознавания объектов МАА.

Основные положения

Очевидно, что при пилотировании дрона диапазон девиации частоты каждой группы двигатель – пропеллер есть близкие по значению величины, различие между которыми при неограниченном увеличении времени наблюдения стремится к нулю. Однако в пределах каждого малого фиксированного интервала времени разность частот этих сигналов есть случайная величина, зависящая от заданного режима движения и турбулентного процесса в атмосфере.

Анализ известных работ показывает, что причиной, создающей особенности временной амплитудно-частотной характеристики поля акустических волн, генерируемых МАА, являются флуктуации тягового усилия каждой из двигательных установок в системе двигатель – пропеллер в общей группе двигательных установок устройства.

Следовательно, модель акустического сигнала дрона можно представить как суперпозицию нескольких (по числу двигателей и воздушных винтов) частотных составляющих – гармоник, каждая из которых модулирована по частоте сигналом управления, что обеспечивает поддержку заданного режима движения в условиях случайных (турбулентных) атмосферных возмущений, воздействующих на дрон.

Можно предположить существование еще одной составляющей акустического сигнала дрона. Это комбинационные частоты, возникающие в результате нелинейных процессов распространения вибраций вдоль конструкции дрона, которые возбуждаются работой систем двигатель – пропеллер. Интенсивность этой составляющей определяется резонансными свойствами конструкции МАА, а частота – суммой и разностью частот, генерируемых установленными системами двигатель – пропеллер.

В [10 – 12] рассмотрен один из возможных подходов к анализу комбинационных сигналов, при котором используется анализ зависимостей изменения периодов, то есть анализ на малых интервалах времени, при которых длительность периода гармоник не успевает существенно измениться. В этом случае сигнал, который анализируется, можно представить как аддитивную смесь ряда дискретных гармоник.

Распределение по длительностям периода характеризует диапазон изменения режимов работы устройства в целом и, таким образом, дает «портреты», индивидуальные для каждого из источников шума.

Следовательно, для выявления информативных признаков акустических сигналов дрона целесообразно сопоставить акустический сигнал дрона и фоновый акустический шум, существующий в среде мегаполиса.

Результаты обработки и анализа данных экспериментальных наблюдений

Натурные исследования, проведенные авторами, позволили получить обширный экспериментальный материал по акустическим сигналам МАА.

На рис.1, 2 приведены примеры результатов модельно-корреляционной обработки сигналов МАА и фонового шума, полученные в виде трехмерной модельно-корреляционной структуры периодов акустического сигнала. Обработка выполнена по методике, приведенной в [10 – 12].

Задачей анализа сигналов является проверка гипотезы, состоящей в том, что разработка системы информативных признаков на основе временного анализа позволит создать более надежную систему распознавания сигналов МАА.

В связи с этим положением цель обработки состоит в приведении выборок сигналов к виду, удобному для исследования флуктуации периода акустического сигнала МАА на малых интервалах времени. Исходя из поставленной цели, методика обработки акустических шумоподобных сигналов состоит в записи выборки S_v акустического сигнала МАА длительностью t_v, последовательном выявлении присутствия в исследуемой выборки коротких фрагментов синусоидального сигнала:

$$S_{ai} = \sin\left(\frac{x \cdot 2\pi}{T_{ai}}\right)$$

где T_{ai} – период искомой составляющей сигнала, $t_{pi} = pT_{ai}$ – длительность фрагмента, $x = [0 : (p \cdot T_i)]$, где p – целое число периодов в модели фрагмента сигнала, $p = 10$ согласно [11].

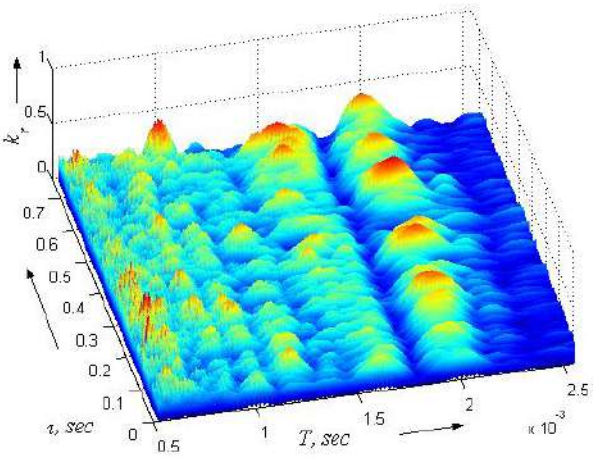


Рис. 1. Модельно-корреляционная структура периодов акустического сигнала МАА

Искомые фрагменты сигнала при выбранном периоде T_i выявляются путем расчета коэффициента корреляции k_r между моделью S_{Mi} фрагмента сигнала $S_{Mi} = \sin\left(\frac{x \cdot 2\pi}{T_{Mi}}\right)$, с установленными периодом T_{Mi} и длительностью $t_{Mi} = t_{pi}$, и фрагментом записанного сигнала $S_{ai}(x)$, причем коэффициенты корреляции вычисляются последовательно при сдвиге модели S_{Mi} сигнала вдоль временной оси τ на величину $\Delta\tau$ при $T_{Mi} = const$, при этом выполняется условие: $t_M << t_в$ длительность модели много меньше длительности записанной выборки.

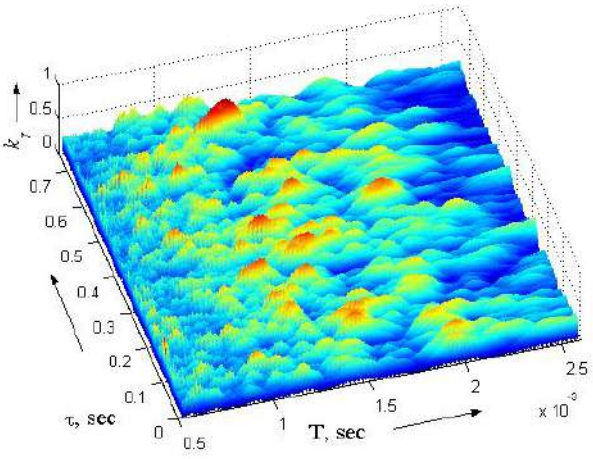


Рис. 2. Модельно-корреляционная структура периодов фонового шума

Операция расчета k_r производится для каждого значения T_M из заранее установленного ряда дискретных значений $T_M(i) = T_0 + i \cdot \Delta t$ при $i = (1 \ldots n)$, где $T_0 = 0{,}52 \cdot 10^{-3} s$ или эквивалент частоты $F_s = [385 \ldots 2000]\,Гц$ при $\Delta t = 2{,}083 \cdot 10^{-5} s$ и $n = 100$. Следовательно, за одну

операцию полного сдвига выявляется наличие одной компоненты искомой составляющей сигнала при одном из заданных значений периода модели T_{Mi}, при этом число операций полного сдвига модели вдоль выборки сигнала равно числу заданных значений T_{Mi} периода модели (в данном случае $n=100$).

В результате получаем ряд зависимостей, $k_{ri}(\tau, T_{Mi})$ которые организуются в $(m\times n)$ матрицу M_{kr}. При этом принимается условие, если $k_r \geq k_{st}$ – искомый фрагмент присутствует в сигнале МАА, при $k_r < k_{st}$ принимается альтернативное решение.

Члены матрицы M_{kr} вдоль столбцов есть коэффициенты корреляции k_{ri}, полученные при одном из заданных значений периода модели T_{Mi} и рассчитанные в зависимости от сдвига модели вдоль оси времени выборки.

Члены вдоль строк есть значения коэффициентов корреляции, полученные при одной и той же величине сдвига модели вдоль оси времени выборки, то есть каждая строка есть зависимость коэффициента корреляции от периода модели при данном сдвиге.

Визуальный анализ рис. 1 показывает, что сигнал МАА на малых интервалах времени $t_M = 10T_M$ представлен явно выделяющимся рядом дискретных составляющих при $T_M = [2;\ 1{,}5; 1{,}25; 1]ms$. Видно также, что амплитуда этих составляющих существенно флуктуирует.

Компоненты при $T_M < 1ms$ слабо различимы как дискретные составляющие. Их амплитуда существенно снижена по отношению к составляющим при $T_M = [2;\ 1{,}5]ms$.

Как следует из рис. 2, в структуре «период – время» сигналов фонового шума полностью отсутствует устойчивая повторяемость, то есть сигналы имеют чисто случайный характер.

Для формализации визуального анализа на рис. 3 приведены зависимости нормированного коэффициента корреляции в диапазоне периодов модели $T_M = [0{,}5\ldots 2{,}5]\cdot 10^{-3}c$ (эквивалентные частоты $F_{se} = [400\ldots 2000]Гц$) в структуре сигнала дрона и фонового шума. Эти зависимости получены путем усреднения значений матрицы M_{kr} вдоль столбцов.

Зависимость, представленная сплошной линией, получена из матрицы сигнала МАА, две другие (пунктир) получены аналогичным расчетом по двум выборкам из одной записи развитого шума улиц мегаполиса.

Как следует из приведенных графиков, в двух реализациях сигнала фонового шума отсутствуют области сосредоточенных устойчиво повторяющихся областей гармонических составляющих. Эти зависимости формализуют чисто случайный характер наблюдаемого процесса.

Зависимость, полученная из сигналов МАА, позволяет определить число гармоник и диапазон флуктуации их периодов. Вид этой зависимости формализует свойство структурированности периодов сигнала МАА. На этой зависимости наблюдаются две области, разделенные глубокими минимумами при периоде $T_M = 1{,}3мс$ и $T_M = 1{,}83мс$, что свидетельствует о существовании двух основных процессов генерации акустического сигнала.

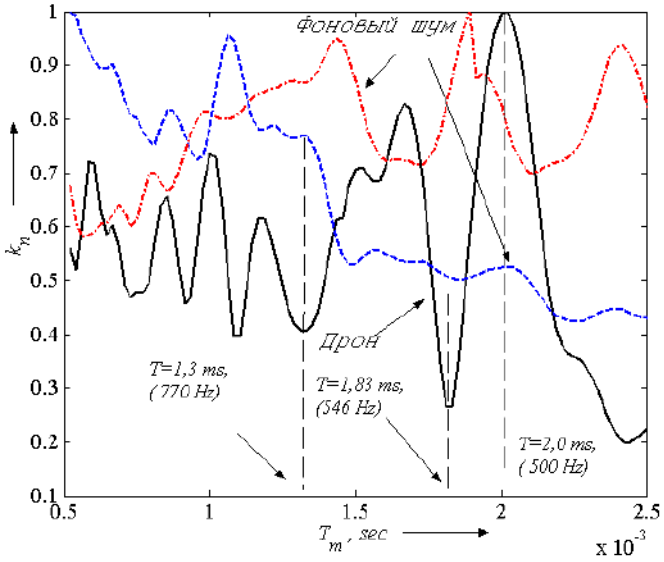


Рис. 3. Зависимости нормированного коэффициента корреляции от периода модели в структуре сигнала дрона и фонового шума улицы

Полученная структура рис. 1 – 3 позволяет выдвинуть предположение о существовании корреляционной связи между строками полученной матрицы M_{kr} коэффициентов корреляции.

На рис. 4 приведены графики зависимостей коэффициентов корреляции между строками матрицы M_{kr}, причем расчет коэффициентов корреляции ведется между начальной строкой N_{0str} и всеми последующими строками, включая начальную строку.

Номера начальных строк в данном случае устанавливаются из ряда $N_{0str} = [1,\ 100, 200, 300, 400, 500, 600]$. Величина $N_{str\max} = 600$ выбрана из условия $\Delta\tau_{N_{\max}} \geq 0{,}01s$.

В результате каждой итерации N_{0str} имеем последовательность коэффициентов корреляции $k_{rNi} = [k_{ri} \ldots k_{rm}]$, где $i = N_i \ldots m$, где m – число строк M_{kr}. Каждое значение зависимостей на рис. 4 получено путем усреднения рассчитанных последовательностей $k_{rNi} = [k_{ri} \ldots k_{rm}]$.

На рис.4 приведены две зависимости. Первая получена из сигналов МАА (обозначено *drone*), вторая – из сигналов фонового шума улицы мегаполиса (обозначено *Street Noise).*

Из полученного результата следует, что зависимости на рис. 4 не пересекаются, между их значениями имеется существенное и устойчивое отличие. Следовательно, полученный результат позволяет ввести классифицирующий признак в виде условия:

$$\begin{aligned} H &= 1 \quad при \quad k_r > k_{cl} \\ H &= 0 \quad при \quad k_r < k_{cl} \end{aligned}, \qquad (1)$$

где H – событие, определяющее принадлежность анализируемого сигнала, значение "1" – означает, что событие H состоит в правильном обнаружении сигнала МАА, значение "0" – означает, что событие H состоит в обнаружении сигнала фонового шума, k_{cl} – граничное значение классифицирующего признака, в данном случае можно принять $k_{cl} = 0{,}3$.

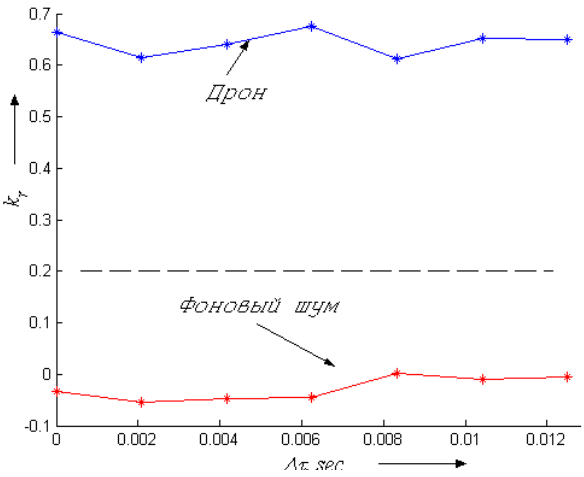


Рис. 4. Зависимости коэффициента корреляции между строками матриц коэффициентов корреляции сигналов МАА и фонового шума

Выводы

Основным результатом работы является обоснование целесообразности использования анализа «время – период» на малых интервалах времени. Показано, что этот подход позволяет получить классифицирующий признак для распознавания акустических сигналов МАА на фоне внешних шумов.

Сформулирована постановка задачи обнаружения МАА по регистрации и анализу акустических сигналов, которые генерируются МАА в процессе полета, определены факторы, влияющие на временную структуру флуктуаций периода сигналов МАА.

Список литературы:

1. Kloet N., et al. Acoustic signature measurement of small multi-rotor unmanned aircraft systems // International Journal of Micro Air Vehicles. 2017. 9(1). P.3–14.

2. Stimpson A., et al. Small UAV Noise Analysis. Humans and Autonomy Laboratory, Duke University, Durham, NC, USA. 2017. April 26, 12 pp. Available at https://hal.pratt.duke.edu/sites/hal.pratt.duke.edu/files/u24/Small_UAV_Noise_Analysis_rqi.pdf.

3. Leslie A. et al. Broadband noise reduction on a mini-UAV propeller // 14th AIAA/CEAS aeroacoustic conference, Geelong, Victoria, Australia, 2008. Available at https://www.semanticscholar.org/paper/Broadband-Noise-reduction-from-a-mini-UAV-propeller-Auld-Leslie/aa8f1514d96bd711bea00880afdb8050800037bc.

4. Brown J. What Is A Drone: Main Features and Applications of Today's Drones. Available at https://www.mydronelab.com/blog/what-is-a-drone.html.

5. King E., et al. Bee threat elicits alarm call in African elephants // PLoS One. 2010. vol. 5, no. 4. P. e10346. Available at https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0010346.

6. Anderson, K., and Gaston, K. Lightweight unmanned aerial vehicles will revolutionize spatial ecology // Frontiers in Ecology and the Environment. 2013. vol. 11, no. 3. P. 138146.

7. Feight, J. (2017). Characterization of a Multi-Rotor SUAS as a First Step Towards Detection and Identification via Acoust. Available at https://shareok.org/handle/11244/300026.

8. Карташов В. М. Информационные характеристики звукового излучения малых беспилотных летательных аппаратов / В.М. Карташов, С.А. Шейко, С.И. Бабкин, И.В. Корытцев, О.В. Зубков // Радиотехника. 2017. Вып. 191. С. 181-187.

9. Козерук С. О., Коржик О. В. Виявлення малих літальних апаратів за акустичним випромінюванням // Visnyk NTUU KPI Seriia – Radiotekhnika Radioaparatobuduvannia. 2019. Iss. 76. P. 15–20.

10. Semenetz V.V., Leonidov V.I. Model-structural analysis of combination interference in the problems acoustic sounding of the atmosphere // Telecommunications and Radio Engineering. 2019. Vol. 78, Issue 12. pages 1078-1095. DOI: 10.1615/TelecomRadEng.v78.i12.60 pages 1087-1095, 2019.

11. Леонидов В.И., Семенец В.В. Особенности амплитудно-временной структуры помех в системах акустического зондирования атмосферы // Радиотехника: 2019. Вып. 197. С. 93 – 99.

12. Leonidov V.I. Analysis of the models and structure of echo signals of the atmospheric acoustic sounding // Telecommunications and Radio Engineering. 2014. 73(16). P. 1497-1502.

Поступила в редколлегию 05.09.2020

Сведения об авторах:

Леонидов Владимир Иванович – канд. техн. наук, Харьковский национальный университет радиоэлектроники, с. н. с. кафедры биомедицинской инженерии, Украина, e-mail:volodymyr.leonidov@nure.ua, ORCID: https://orcid.org/0000-0001-5218-3177

Семенец Валерий Васильевич – д-р техн. наук, проф., Харьковский национальный университет радиоэлектроники, ректор, Украина, e-mail: valery.semenets@nure.ua, ORCID: https://orcid.org/0000-0001-8969-2143

УДК 629.7.022 **DOI:10.30837/rt.2020.3.202.16**

В.М. КАРТАШОВ, д-р техн. наук, И.В. КОРЫТЦЕВ, канд. техн. наук,
С.А. ШЕЙКО, канд. техн. наук, В.Н. ОЛЕЙНИКОВ, канд. техн. наук,
О.В. ЗУБКОВ, канд. техн. наук, С.И. БАБКИН, канд. техн. наук

ОПТИКО-ЭЛЕКТРОННЫЕ МЕТОДЫ ОБНАРУЖЕНИЯ ВОЗДУШНЫХ ОБЪЕКТОВ И ИЗМЕРЕНИЯ ИХ КООРДИНАТ

Введение

Оптико-электронные обнаружители воздушных объектов обеспечивают возможность распознавания этих объектов на фоне различных оптических засветок, точного измерения дальности до объектов и определения угловых координат. Перспективными являются пассивные проективные методы, базирующиеся на применении видео камер с фоточувствительными матрицами дневного, ночного и теплового видения.

Оптико-электронные методы (ОЭМ) в режимах измерений характеризуются высокой точностью, что обусловливает их успешную интеграцию с радиоэлектронными комплексами разного назначения. Данный анализ проведен с целью выбрать и исследовать ОЭМ, способный решать задачи обнаружения и определения координат малых беспилотных летательных аппаратов. Интерес представляют методы, позволяющие автоматизировать процессы обнаружения воздушных объектов и измерения их координат. Для конкретики рассмотрим различные ОЭМ измерения дальности до объектов. Эти ОЭМ можно классифицировать по физическому принципу следующим образом (рис. 1):

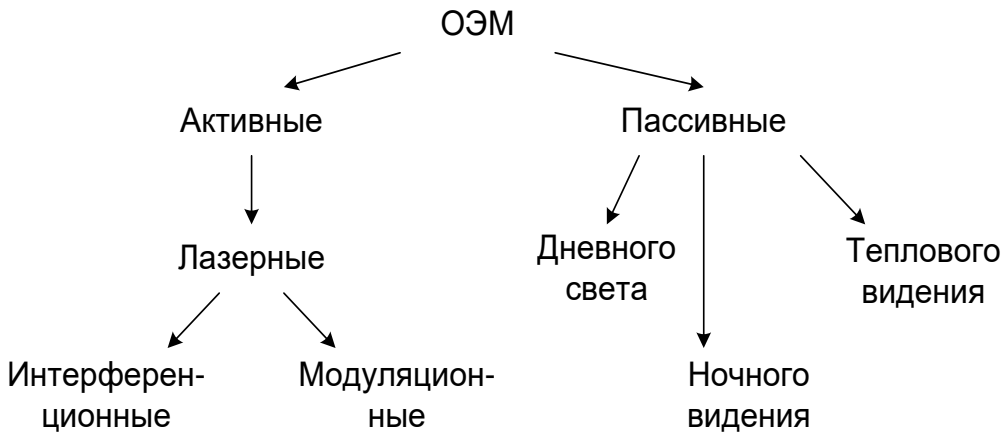


Рис. 1. Классификация ОЭМ по физическому принципу

1. Активные ОЭМ измерения дальности

Активные ОЭМ представляются, в основном, большой группой лазерных методов. Активные светолучевые методы уступают лазерным по всем показателям и более не используются. Лазерные ОЭМ оперируют с направляемым на объект лазерным лучом или с лучом, сканирующим пространство по определенному закону [1 – 3]. Отраженный объектом принимаемый сигнал позволяет обнаружить объект и по своему запаздыванию определить дальность до него.

Интерференционные методы измерения дальности D базируются на подсчете числа целых фазовых циклов N и дробной части цикла Δ в принимаемом сигнале [4, 5]

$$D = \lambda(N + \Delta)/2\,, \tag{1}$$

где λ – длина волны излучения.

Измерения проводят дискретно специальными счетчиками фазовых циклов [6, 7]. Системы, реализующие интерференционные методы, обладают высокой точностью, необходимостью создания опорного оптического канала, их максимальная дальность действия составляет всего несколько десятков метров. Для ее увеличения применяют многочастотные лазеры [8].

Модуляционные ОЭМ используют импульсную, частотную либо фазовую модуляцию лазерного излучения.

В *импульсных* дальномерах излучение является прерывистым, применяют твердотельные рубиновые и неодимовые лазеры. Дальность определяется путем измерения времени t, затраченного излученным импульсом на прохождение двойного расстояния:

$$D = ct/2n \approx cm/2nf_{ки}, \quad (2)$$

где c – скорость света; n – показатель преломления среды; m и $f_{ки}$ – число калибровочных временных импульсов, зарегистрированных в мерном интервале t, и их частота следования.

Для повышения точности и дальности измерений используют некогерентное накопление принимаемых сигналов [9, 10]. Максимальная дальность действия импульсных лазерных дальномеров может составлять, в условиях ясного неба, 20 – 30 км при абсолютной погрешности ±0,5 м.

Частотная модуляция лазерного излучения реализуется путем изменения параметров оптического резонатора лазера [11] по симметричному пилообразному закону, при этом формируется непрерывный лазерный луч постоянной интенсивности, но с изменяющейся по такому же закону частотой. Отраженный объектом сигнал детектируется, усиливается, подвергается частотному анализу на каждом полупериоде модулирующего сигнала с периодом T_m и сравнивается в частотном плане с текущим модулирующим сигналом [12, 13]. Появление разностной частоты f_p обусловлено наличием цели на определенной дальности, и сигнал приходит от нее с определенным значением частоты, преодолев двойную дальность. Наличие нескольких разностных частот указывает на присутствие нескольких объектов на соответствующих дальностях

$$D = cT_m f_p /4n(f_{max} - f_{min}), \quad (3)$$

где f_{max} и f_{min} – соответственно максимальная и минимальная частоты модулирующего сигнала.

Совместная суммарно-разностная обработка разностных сигналов по полупериодам позволяет раздельно оценить дальности до целей и их радиальные скорости. Однозначное измерение дальности и скорости возможно в интервале

$$\Delta D = c\, T_m / 8. \quad (4)$$

В фазовых лазерных дальномерах используется метод сравнения фаз принимаемого и излучаемого световых потоков:

$$D = c\varphi /4\pi f_m, \quad (5)$$

где φ – разность фаз; f_m – частота модуляции.

Разность фаз должна быть меньше 180^o для устранения неоднозначности оценки дальности, что обеспечивается надлежащим выбором частоты модуляции. Обычно используют несколько модулирующих частот [8, 14]. Однозначная оценка дальности может быть также получена подсчетом полных циклов N изменения фазы модулирующего сигнала и дробной части цикла Δ на интервале запаздывания отраженного сигнала:

$$D = c(N + \Delta)/2nf_m. \quad (6)$$

Количество циклов определяют, в основном, методом кратных частот, когда при сравнении фаз используется не одно модулирующее колебание, а несколько с кратными убывающими частотами [15, 16].

Частотный и фазовый методы лазерного измерения дальности обладают высокой точностью, абсолютная погрешность измерения не хуже $\pm 10^{-2}$м. Дальность действия обычно не превышает 1 км.

Рассмотренные активные методы обладают высокой точностью, но требуют значительных энергетических затрат и не обеспечивают скрытность работы.

2. Пассивные ОЭМ измерения дальности

2.1. Особенности матричных фоточувствительных сенсоров

Особый интерес представляют методы, не требующие участия зрительного аппарата человека в снятии измерительных отсчетов и обеспечивающие полную автоматизацию принятия решения [17]. Этому способствует прогресс в технологиях создания фоточувствительных сенсоров в виде матриц, чувствительных в области дневного света 0,4 – 0,7 мкм [18 – 20], ночного видения 0,7 – 1,4 мкм – это диапазон ближнего инфракрасного (ИК) света [21 – 23] и теплового видения 1 – 20 мкм [24, 25]. Объективом проецируется изображение объекта на фоточувствительную матрицу, отображающую его конфигурацию и являющуюся, дополнительно, точным двумерным цифровым устройством для определения линейных размеров объекта. Наибольшее применение находят ПЗС (приборы с зарядовой связью) и микроболометрические матрицы; КМОП-матрицы (комплементарный металл-оксид-полупроводник) обладают высоким уровнем шума, поэтому в оптических обнаружителях объектов и измерителях их координат они не используются.

В диапазоне белого света эффективно работают кремниевые ПЗС-матрицы, максимум их спектральной характеристики находится в области 1,1 мкм. Поэтому они находят применение, как в оптических измерительных системах дневного света, так и системах ночного видения в ближнем ИК диапазоне [22, 23]. Системы очень чувствительные, и в системах дневного света перед ПЗС матрицей устанавливается оптический фильтр, отсекающий излучения с длинами волн более 0,7 мкм.

В системах ночного видения ближнего ИК диапазона применяют кремниевые ПЗС-матрицы с ИК-подсветкой объекта, что делает систему уже активной, либо кремниевые ПЗС-матрицы с электронными умножителями. При кратности умножения выходного сигнала 10^3 система обнаруживает воздушный объект при его освещенности естественным светом ночного звездного неба $5 \cdot 10^{-4}$ лк [23]. Разрешение ПЗС матриц уже превышает величину, определяемую стандартом 4К, что наряду с высоким качеством изображения и точностью измерения линейных размеров объектов вызывает также необходимость передачи и обработки высокоскоростных информационных потоков.

Микроболометрические матрицы включают в себя активные элементы, сопротивление которых изменяется под действием тепла слабого оптического излучения [26, 27]. Особый интерес представляют матрицы диапазона 7 – 14 мкм, совпадающего с окном прозрачности в нижней атмосфере и с максимумом излучательной способности воздушных объектов в диапазоне температур от -50 ^{o}C до +500 ^{o}C. Температурная чувствительность матриц уже ниже 10 мК, а количество элементов разрешения достигло 1024 х 768. Эти матрицы могут обеспечить работу оптико-электронных систем во всех диапазонах дневной и ночной освещенностей и даже в условиях тумана, дымки, а также при постановке искусственных помех – засветок, задымления [28].

Рассмотренные фоточувствительные сенсоры, выявляющие воздушные объекты, как днем, так и ночью имеют матричную структуру и могут быть интегрированы в единую оптико-электронную систему обнаружения и измерения дальности.

2.2. ОЭМ измерения дальности с использованием матричных сенсоров

ОЭМ с матричными сенсорами подразделяются на однокамерные и стереоскопические.

Однокамерные ОЭМ. Метод измерения дальности до объектов по их изображениям, рассмотренный в работе [29], предполагает получение оптического изображения движущегося воздушного объекта из одной точки измерений, его преобразование в цифровое, распознавание объекта по оцифрованному изображению и определение дальности до движущегося объекта по формуле

$$D = FL/l, \tag{7}$$

где F – фокусное расстояние оптической системы, L – фактический линейный размер распознанного объекта по базе данных, l – соответствующий линейный размер изображения движущегося воздушного объекта на фоточувствительной матрице с учетом проекционных искажений.

Этот метод обладает низкой точностью, так как используется фактический линейный размер объекта, определяемого по распознаванию, а объект может быть не распознан, распознан ошибочно либо распознан правильно, но с другой модификацией. К тому же, учет проекционных искажений соответствующего линейного размера изображения требует знания многих параметров полета объекта (азимут, высота и углы тангажа, крена, рыскания), что делает задачу трудновыполнимой и решаемой с большим приближением.

Способ измерения дальности до объекта по его изображениям из двух точек [30] одной камерой с фокусным расстоянием объектива F включает измерение размеров A_1 изображения объекта и координат его центра X_1, Y_1 в 1-й точке, перемещение средства наблюдения под углом к оптической оси на определенное расстояние S, измерение размеров изображения объекта A_2 и координат центра изображения объекта X_2, Y_2 во второй точке, в процессе перемещения ориентацию камеры не меняют, а после перемещения измеряют сдвиг изображения B по выражению

$$B = [(Y_1 - Y_2)^2 + (X_1 - X_2)^2]^{\frac{1}{2}}. \tag{8}$$

Затем сравнивают сдвиг изображения B и изменения размеров изображения объекта $\Delta A=A_2-A_1$, и в случае, если отсутствуют условия для измерения угла между направлением перемещения камеры и оптической осью, дальность D определяют по выражению

$$D = S/(1 - K\cos\alpha + K^2)^{1/2}, \tag{9}$$

где $K=A_1/A_2$; α – угол визирования объекта ($\alpha=\mathrm{arctg}(B/F)$; S – величина перемещения камеры.

Стереоскопические ОЭМ. Эти методы связаны с построением более сложных оптико-электронных систем, обеспечивающих более высокую точность измерения дальности при меньших временных затратах.

Стереоскопический ОЭМ измерения дальности с использованием матричных сенсоров приведен в работе [31]. Метод базируется на использовании двух цифровых камер, разнесенных в пространстве по горизонтали на известное расстояние. Дальность до объекта вычисляется путем определения сдвига между изображениями по положению максимального значения двухмерной нормированной корреляционной функции в субпиксельном диапазоне. При этом левая и правая камеры установлены на внутренних рамах своих кардановых подвесов, каждый из которых содержит внешнюю и внутреннюю рамы, на осях которых установлены датчики угла поворота рам подвеса. Кроме того, левая и правая камеры, а также датчики угла поворота рам подвеса выполнены с возможностью передачи в вычислительный блок видеоданных и данных о текущей пространственной ориентации камер. Дальность до выделенной области объекта определяют из выражения, учитывающего отклонение от горизонтальной линии положения двух цифровых фотокамер:

$$D = \frac{fB}{\Delta l_z}\cos\left(arctg\frac{\Delta l_z}{\Delta l_e}\right), \tag{10}$$

где B – расстояние между точками съемки в пространстве, f – фокусное расстояние фотокамер, Δl_{Γ} _ сдвиг между изображениями объекта по горизонтальной оси, $\Delta l_{\text{В}}$ – сдвиг между изображениями объекта по вертикальной оси. Вычислительный блок содержит обрабатывающую систему, являющуюся удаленным компьютером, таким как ноутбук или персональный компьютер (рабочая станция), и пользовательский интерфейс, обеспечивающий выбор пользователем изображений и ввод команд обработки. Технический результат заключается в возможности изменения параметров рабочей зоны и в уменьшении суммарного времени на предварительную настройку дальномера и процесс измерений. Однако взаимная двухмерная корреляционная обработка областей изображений, занимаемых объектом, требует значительных массивов данных и становится невозможной для малых удаленных объектов. К тому же требование присутствия оператора также не является положительным фактором метода.

В работе [32] представлен метод определения дальностей до объектов в пассивных системах оптического, инфракрасного и теплового видения предназначенных для наблюдения за малоразмерными объектами. В системах оптического и инфракрасного диапазонов сигналы отражения и излучения от объектов проходят через оптические линзы, преобразуются в уровни амплитуды и отображаются на матрицах двух камер, взаимно удаленных в пространстве и образующих стереопары кадров изображений объекта. Полученные изображения объектов в k-х матрицах (k=1, 2) сегментируются выделением однородных по амплитуде подобластей с помощью известных операций сегментации, например [33], и каждый сегмент представляется вектором параметров, включающим координаты центра сегмента, среднюю амплитуду и геометрические характеристики. Для измерения дальности до объекта рассматривается пара сопряженных точек $V_{\text{k}}=(x_{\text{k}},y_{\text{k}},1)$, k=1, 2 – центров сегментов, отображающих центр объекта в прямоугольных координатах двух матриц оптического изображения (единица замещает неизвестную третью координату). Для известных матриц внутренних параметров камер A_{k}, k=1, 2, зависящих от фокусных расстояний f_{k}, устанавливается связь $Z_{\text{k}}V_{\text{k}}=A_{\text{k}}M_{\text{k}}$ [1], где M_{k} – центр объекта в прямоугольной системе k-й камеры, совмещенной с ее оптическим центром. Для найденных центров m сегментов определяют орты $a_1(i)$ векторов i-х направлений на центры объектов первой камеры и орты $a_2(j)$ векторов j-х направлений на центры объектов второй камеры, затем для всех m вариантов соединения ортов $a_1(i)$ и $a_2(j_{\text{i}})$ в m неповторяющихся сопряженных парах, где $j_{\text{i}} \in \{1, 2, \ldots, m\}$ находят оценки дальностей $r_1(i)$ и $r_2(j_{\text{i}})$ по критерию минимума квадрата евклидовой нормы вектора e_{i} ошибок сопряжения ортов:

$$J\left(r_1(i), r_2(j_i)\right) = \|e\|^2 = \|r_1(i)a_1(i) - r_2(j_i)Pa_2(j_i) - b\|^2, \tag{11}$$

на этапе расчетов выполняют операции минимизации функции $J(r_1, r_2)$ в (11) по r_1 и $r_{2.}$

Из m вариантов соединения ортов в m неповторяющихся пар $a_1(i)$ и $a_2(j_{\text{i}})$, $j_{\text{i}} \in \{1, 2, \ldots, \text{m}\}$ выбирают вариант с наименьшим значением показателя правильности сопряжения.

При этом получают оценки дальностей

$$\hat{r}_1(i) \text{ и } \hat{r}_2(j_i), \; i = 1 \ldots m. \tag{12}$$

Затем вычисляют оценки пространственных координат m объектов в системах координат двух камер

$$\widehat{M}_1(i) = \hat{r}_1(i)a_1(i), \; \widehat{M}_2(j_i) = \hat{r}_2(j_i)a_2(j_i), \; i = 1 \ldots m. \tag{13}$$

Рассмотренный метод позволяет обрабатывать изображения множества воздушных объектов, получаемых двумя неидентичными видеокамерами, разнесенными на определенное расстояние друг от друга и без жесткой связи между ними, но требуется предварительное определение внутренней и внешней матриц параметров камер с высокой точностью, поскольку они неоднократно участвуют в вычислительной процедуре. Этот метод является также очень вычислительноемким, дважды используется критериальный

подход к определению промежуточных величин – при выборе сопряженных точек и оценок дальностей до объекта. Не показано, как это влияет на точность определения дальности и на оперативность работы систем.

Выводы

ОЭМ измерения дальности до воздушных целей являются очень эффективными, обеспечивая измерения максимальной дальности от 100 – 200 м до 20 – 30 км с абсолютной погрешностью измерений от $\pm 10^{-2}$ м до 0,5 м соответственно.

Наибольшие значения максимальной дальности обеспечиваются импульсными лазерными дальномерами, а в области средних и малых дальностей широко используются частотные и фазовые методы лазерной дальнометрии. Для выполнения конкретных задач лазерные дальномеры хорошо интегрируются с радиоэлектронными комплексами обнаружения и распознавания воздушных целей.

Ограничивающими факторами использования лазерных методов являются наличие низкой облачности, тумана и осадков, а также низкая степень скрытности работы измерительных систем.

Пассивная область оптических безокулярных дальномеров развивается на основе использования матриц дневного, ночного и теплового видения. При этом используются изощренные алгоритмы обработки цифровых изображений, что требует увеличения времени для принятия решений.

Достоинством матричных ОЭМ является возможность одновременного использования всех трех датчиков дневного, ночного и теплового видения, что позволит проводить надежное обнаружение, распознавание и измерение координат малых воздушных объектов.

Список литературы:

1. Аснис Л.А., Васильев В.П. и др. Лазерная дальнометрия. Москва : Радио и связь, 1995. 256с.
2. Бокшанский В.Б., Бондаренко Д.А. и др. Лазерные приборы и методы измерения дальности. Москва : Издательство МГТУ им. Н.Э. Баумана, 2012. 92 с.
3. Hammer M., Hebel M., Laurenzis M., Arens M. Lidar-based detection and tracking of small UAVs // International Society for Optics and photonics, 2018. Vol. 10799. P. 107990.
4. Evenson K., Wells J., Speed of light from direct frequency and wavelength measurement of the methane stabilized laser // Phyls Rev.Lett. 1972. Vol. 29, No. 19. P. 1346–1349.
5. Коломийцов Ю.В. Интерферометры. Ланинград : Машиностроение, 1976. 296 с.
6. Bercovich G., Shafir E. Optical methods for distance and displacement measurements // Adv. Opt. Photonic. 2012. P. 441–473.
7. Wu H., Zhang F., Liu T., Absolute distance measurements by chirped pulse interferometry using a femtosecond pulse laser // Opt.Express. 2015. Vol. 23, No.24. P. 31582–31593.
8. Baumann E., Comb-calibrated frequency-modulated continuous wave lidar for absolute distance measurements // Opt. Lett. 2013. Vol. 38, No.12. P. 2026 – 2028.
9. Вильнер В., Лаврюшин А.,Рудь Е. Оценка возможностей светолокационного измерителя дальности с накоплением // Фотоника. 2007. С. 22–26.
10. Фуфаев А.В., Фёдорцев Р.В. Повышение точности измерения дистанции в дальномерном канале прибора наблюдения с использованием полупроводникового лазера // Приборы и методы измерений. 2013. №2. С. 95-102.
12. Власов В.Г., Лазнева Э.В. Метод гетеродинного приема излучения, амплитудно-модулированного в диапазоне 5 – 50 МГц, с помощью фотодиода // Опт.- мех. пром. 1968. №10. С. 5 – 8.
13. Попов Ю.В., Утенков Б.И. Методы управления режимом работы фотоэлектронных умножителей // Опт.- мех. пром. 1976. №2. С. 65–71.
14. Zhang W. Comb-referenced frequency sweeping interferometry for precisely measuring large stepped structures // Appl. Opt.2018. Vol. 57,No.5. C. 1247–1253.
15. Shihua Zhang, Zheyi Xu, Benyong Chen, Liping Yan, and Jiandong Xie. Shihua Zhang Sinusoidal phase modulating absolute distance interferometer combining frequency sweeping and multiwavelength intrferometry // Optics Express . Vol. 26. Issue 7. Pp. 9273-9284.
16. Gunnar Arisholm . Combined range ambiguity resolution and noise reduction in lidar signal processing // Opt. Eng. 2018. Vol. 57, No.7. P.73 – 103.
17. Медведев А.В., Гринкевич А.В., Князева С.Н. Современные подходы к созданию пассивных дальномеров // Фотоника. 2017. №8/68. С.30 – 37.

18. Juan Luis Nieves Multispectral synthesis of daylight using a commercial digital CCD // Appl. Opt. 2005. Vol.44, No.27. P. 5696 – 5703.

19. Ямбаев Х.К., Староверов С.З. Особенности фоточувствительных приемников с зарядовой связью и их возможности в геодезии и метрологии // Интерэкспо Гео-Сибирь. 2017.

20. Donald E. Groom. Recent progress on CCDs for astronomical imaging // Optical and IR Telescope Instrumentation and Detectors. 2000. Proc.Vol. 4008.

20. Волков В.Г. Высокочувствительные телевизионные камеры для обеспечения безопасности // Системы управления, связи и безопасности. 2016. №3. С.66 – 94.

21. Night vision technologies handbook. Homeland security. 2013. 34 p.

22. Рева В.П. и др. ПЗС-фотоматрицы с электронным умножением // Технология и конструирование в электронной аппаратуре. 2017. № 1-2. С.33 – 37.

23. Сизов Ф.Ф., Чувствительность матриц ПЗС с электронным умножением // Технология и конструирование в электронной аппаратуре. 2018. № 2. С.9 – 14.

24. Стафеев В.И., Болтарь К.О., Бурлаков И.Д., Акимов В.М. и др. Матричные фотоприемные устройства среднего и дальнего инфракрасных диапазонов спектра на основе фотодиодов из CdxHg1−xTe // Физика и техника полупроводников. 2005. Т. 39, вып. 10. С. 1257-1265.

25. Lohrmann D., Littleton R., Reese C. et al. Uncooled long-wave infrared small pixel focal plane array and system challenges // Opt. Eng. 2013. Vol.52, No.6. 061305.

26. Иванов С. Д., Косцов Э. Г. Автометрия. Тепловые приемники неохлаждаемых многоразмерных тепловизионных матриц. 2015. Т. 51, № 6. С.79-88.

27. Masafumi Kimata. Uncooled infrared focal plane arrays //wiley.com/doi/full/10.1002/tee. 22563. 2017.

28. Волков В.Г. Тепловизионные приборы для спецтехники //bnti.ru/showart.asp. 2012.

29. Патент RU2680265. Способ определения дальности до движущегося воздушного объекта методом пассивной локации / А.И. Стучилин, заявитель и патентообладатель. 2019.

30. Патент RU 2568335C1. Способ измерения дальности до объекта по его изображениям преимущественно в космосе / А.И. Смирнов, заявитель и патентообладатель. 2015.

31. Патент RU 0002579532 .Оптико-электронный стереоскопический дальномер / А.В. Зубарь, заявитель и патентообладатель. 2016.

32. Патент RU 2681518 Способ определения дальностей до объектов в пассивных системах видения / В.К. Клочко, Нгуен Конг Хоай – авторы. Патентообладатель – Федеральное государственное бюджетное образовательное учреждение высшего образования "Рязанский государственный радиотехнический университет". 2019.

Поступила в редколлегию 16.08.2020

Сведения об авторах:

Карташов Владимир Михайлович – д-р техн. наук, профессор, Харьковский национальный университет радиоэлектроники, заведующий кафедрой медиаинженерии и информационных радиоэлектронных систем, Украина, e-mail: volodymyr.kartashov@nure.ua, ORCID: https://orcid.org/0000-0001-8335-5373

Корытцев Игорь Васильевич – канд. техн. наук, доцент, Харьковский национальный университет радиоэлектроники, профессор кафедры медиаинженерии и информационных радиоэлектронных систем, Украина, e-mail: igor.koryttsev@nure.ua, ORCID: https://orcid.org/0000-0003-1875-5534

Шейко Сергей Александрович – канд. техн. наук, доцент, Харьковский национальный университет радиоэлектроники, доцент кафедры медиаинженерии и информационных радиоэлектронных систем, Украина, e-mail: sergiy.sheiko@nure.ua, ORCID: https://orcid.org/0000-0003-1638-4478

Олейников Владимир Николаевич – канд. техн. наук, доцент, Харьковский национальный университет радиоэлектроники, профессор кафедры медиаинженерии и информационных радиоэлектронных систем, Украина, e-mail: vladimir.oleinikov@nure.ua, ORCID: https://orcid.org/0000-0001-7197-9760

Зубков Олег Викторович – канд. техн. наук, доцент, Харьковский национальный университет радиоэлектроники, доцент кафедры медиаинженерии и информационных радиоэлектронных систем, Украина, e-mail: Oleh.zubkov@nure.ua, ORCID: https://orcid.org/0000-0002-8528-6540

Бабкин Станислав Иванович – канд. техн. наук, Харьковский национальный университет радиоэлектроники, старший научный сотрудник кафедры медиаинженерии и информационных радиоэлектронных систем, Украина, e-mail: prl.res@nure.ua, ORCID: https://orcid.org/0000-0003-4903-3551

УДК 621391: 629.052.3: 551.510.535 **DOI:10.30837/rt.2020.3.202.17**

Е.В. РОГОЖКИН, д-р физ.-мат. наук, Ю.И. ПОДЪЯЧИЙ, канд. физ.-мат. наук,
Л.Я. ЕМЕЛЬЯНОВ, канд. физ.-мат. наук

ОСОБЕННОСТИ ПРИМЕНЕНИЯ ТЕОРЕМЫ ОТСЧЕТОВ ПРИ ОБРАБОТКЕ УЗКОПОЛОСНЫХ РАДИОСИГНАЛОВ С ИЗВЕСТНОЙ ЦЕНТРАЛЬНОЙ ЧАСТОТОЙ СПЕКТРА

Введение

Эффективное применение информационно-вычислительных систем для обработки и анализа радиосигналов требует их преобразования в цифровой формат. При этом основным условием использования такой процедуры является исключение необратимых потерь информации. Например, при исследованиях ионосферы с использованием радиолокаторов некогерентного рассеяния необходимо выделять связанный с вертикальным дрейфом плазмы доплеровский сдвиг. Величина сдвига не превышает 1/100 от ширины спектра рассеяния, что при обработке на видеочастоте усложняет аппаратуру: как и в РЛС приходится использовать два квадратурных канала обработки [1, 2]. Кроме того, в высотном профиле скорости дрейфа плазмы есть области изменения знака скорости (изменение направления движения плазмы). Это при отношениях $P_s/P_n < 1$ серьезно ужесточает требования к идентичности и стабильности характеристик используемых каналов, так как в окрестности высоты изменения знака скорости доплеровский сдвиг имеет предельно низкие значения.

Согласно теореме Котельникова – Шеннона преобразование аналоговых сигналов в дискретную форму должно осуществляться с частотой не меньше удвоенной наивысшей частоты спектра преобразуемого сигнала. Если преобразование радиолокационного сигнала осуществляется на относительно высокой промежуточной частоте, то возникают проблемы с выбором вычислительного устройства достаточно высокой производительности. Один из вариантов решения проблемы заключается в поиске способов цифрового преобразования, позволяющих значительно уменьшить объем вычислительных операций без существенных потерь информации об огибающей и несущей [3].

Цель работы – уменьшение объема процедуры цифрового преобразования и обработки радиосигналов для получения информации о радиолокационных объектах в реальном времени.

Способ увеличения периода следования отсчетов

В когерентных РЛС при преобразовании аналогового сигнала в цифровой формат непосредственно на промежуточной частоте существует техническая возможность осуществлять отсчеты, синхронизируя их сигналом опорной частоты f [4 – 7], которая равна промежуточной в отсутствие доплеровского сдвига. Период следования отсчетов $u_0, u_1, \ldots, u_k, u_{k+1}, u_{k+2}, \ldots, u_{k+n}$ может быть выбран и кратно меньше [5], и кратно больше периода сигнала опорной частоты [8].

В отсутствие доплеровского сдвига каждый из отсчетов сигнала $u(t) = a\cos(2\pi ft + \alpha)$ можно представить комплексными амплитудами:

$$\dot{a}_0, \dot{a}_1, \ldots, \dot{a}_k, \dot{a}_{k+1}, \dot{a}_{k+2}, \ldots, \dot{a}_{k+n-1} = a\left(e^{i\alpha},\ e^{i(\alpha+\delta)},\ e^{i(\alpha+2\delta)}, \ldots,\ e^{i[\alpha+\delta(n-1)]}\right),$$

где δ – шаг отсчетов по углу, n – число отсчетов на интервале $T=1/f$.

На рис. 1 приведена векторная диаграмма, иллюстрирующая вариант дискретизации для случая $n=3$ и $\alpha = \pi/3$. Здесь отсчеты представлены единичными векторами ($\boldsymbol{u_1}$, $\boldsymbol{u_2}$, $\boldsymbol{u_3}$), исходящими из центра окружности, который совмещен с началом произвольно ориентированной системы декартовых координат:

$$x_1 + x_2 + x_3 = 0; \quad y_1 + y_2 + y_3 = 0.$$

Можно показать, что в общем случае при количестве отсчетов $n \geq 3$ суммы вещественных и мнимых частей комплексных амплитуд при угловом шаге отсчетов $\delta=2\pi/n$ и $\delta=4\pi/n$ тождественно равны нулю:

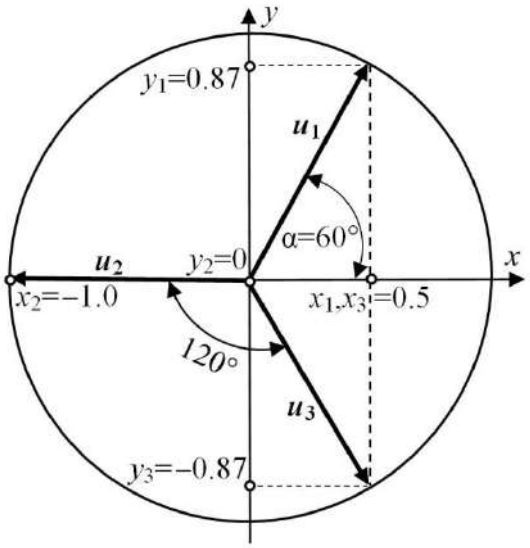


Рис. 1. Векторная диаграмма отсчетов для *n*=3; α=π/3

$$a[\cos\alpha+\cos(\alpha+\delta)+\cos(\alpha+2\delta)+\cdots+\cos(\alpha+(n-1)\delta)]=0;$$
$$ia[\sin\alpha+\sin(\alpha+\delta)+\sin(\alpha+2\delta)+\cdots+\sin(\alpha+(n-1)\delta)]=0. \quad (1)$$

Сумму квадратов отсчетов можно получить, используя уравнения (1) и известные тригонометрические формулы $\cos^2 x=(1+\cos 2x)/2$; $\sin^2 x=(1-\cos 2x)/2$:

$$a^2[\cos^2\alpha+\cos^2(\alpha+\delta)+\cos^2(\alpha+4\delta)+\cdots+\cos^2(\alpha+(n-1)2\delta)]=a^2n/2;$$
$$a^2[\sin^2\alpha+\sin^2(\alpha+\delta)+\sin^2(\alpha+4\delta)+\cdots+\sin^2(\alpha+(n-1)2\delta)]=a^2n/2. \quad (2)$$

Если амплитуда *a*=1, то сумма квадратов отсчетов, приходящихся на период синусоидального сигнала, определяется только количеством отсчетов.

Уравнения (2) для *n*=3, *n*=4, *a*=1 принимают вид:

$$\cos^2\alpha+\cos^2(\alpha+2\pi/3)+\cos^2(\alpha+4\pi/3)=3/2;$$
$$\sin^2\alpha+\sin^2(\alpha+2\pi/3)+\sin^2(\alpha+4\pi/3)=3/2; \quad (3,\ a)$$
$$\cos^2\alpha+\cos^2(\alpha+\pi/2)+\cos^2(\alpha+\pi)+\cos^2(\alpha+3\pi/2)=4/2;$$
$$\sin^2\alpha+\sin^2(\alpha+\pi/2)+\sin^2(\alpha+\pi)+\sin^2(\alpha+3\pi/2)=4/2. \quad (3,\ б)$$

Вывод можно сформулировать так: *если на интервал, равный периоду синусоидального сигнала T*=1/*f с единичной амплитудой приходится* n *отсчетов, следующих с шагом по углу* 2π/n, *то при* n>2 *независимо от фазы первого отсчета их сумма равна нулю, а сумма их квадратов равна* n/2.

В уравнениях (3, *б*) каждая пара соседних отсчетов квадратурно связана:

$$\cos^2\alpha+\cos^2(\alpha+\pi/2)=1;$$
$$\cos^2(\alpha+\pi/2)+\cos^2(\alpha+\pi)=1;$$
$$\cos^2(\alpha+\pi)+\cos^2(\alpha+3\pi/2)=1.$$

Первый и четвертый отсчеты также образуют «квадратуру»:

$$\cos^2\alpha+\cos^2(\alpha+3\pi/2)=1.$$

Для второго уравнения (3, *б*) аналогично.

Образование смежных «квадратур» позволяет определять фазу, на которую приходится отсчет, и амплитуду [8]. Это позволяет составлять такие ряды отсчетов, в которых любые соседние пары будут образовывать «квадратуры». Например, при n=4 ряд отсчетов на временном промежутке, равном длительности N периодов, имеет вид:

$$\cos\alpha, \cos(\alpha+\delta), \cos(\alpha+2\delta), \cos(\alpha+3\delta), \ldots;\ \delta = \pi N/2,\ N = 1,3,5,7,9,\ldots \qquad (4)$$

Из сказанного следует: если на интервал в N периодов синусоиды с единичной амплитудой приходится n отсчетов, следующих с шагом по углу $2\pi N/n$, то при n >2 сумма их квадратов равна $n/2$. Это означает, что и в этом случае (n=4) независимо от фазы первого отсчета имеется полная информация о сигнале (о фазе и амплитуде). Такой результат согласуется с теоремой отсчетов для огибающей.

Из (4) следует, что полную информацию об амплитуде и фазе синусоиды с периодом колебаний T можно получать и в случае, когда период следования отсчетов T_o больше периода синусоиды, то есть T_o=5T/4, 7T/4, 9T/4, … .

Аналогичные выводы можно сделать и для варианта n=3, с той лишь разницей, что N должно быть четным и не кратным трем (N=4, 8, 10,…), то есть T_o=4T/3, 8T/3, 10T/3, … .

Практические результаты предлагаемого способа

Пусть реальный аналоговый сигнал описывается выражением

$$u(t) = a(t)\ cos\ [2\pi(f+F)t + \alpha]. \qquad (5)$$

Здесь F=2V_r / λ – доплеровский сдвиг, который определяется радиальной скоростью объекта V_r и длиной рабочей волны λ. Известны значения f и максимальная частота f_{max} в спектре модулирующей функции $a(t)$ принятого сигнала. Отношение сигнал/шум P_s/P_n >>1.

Если доплеровский сдвиг пренебрежимо мал, то ориентируясь на характеристики $a(t)$ и теорему отсчетов, можно выбирать и формировать период следования отсчетов T_o способом, который определяет выражение (4). В результате при сохранении информации об амплитуде и фазе несущей и модулирующей функции $a(t)$ имеем кратное сокращение подлежащих обработке числа отсчетов, что увеличивает время для выполнения всего комплекса операций в режиме on-line [8].

Оценка погрешностей при наличии доплеровского сдвига

Доплеровский сдвиг F в радиолокационных наблюдениях приводит к нарушению квадратурных соотношений в уравнениях (2). Естественно, в этом случае использование предлагаемого способа цифрового преобразования аналогового радиолокационного сигнала вызывает погрешности в определении амплитуды и фазы. Погрешность зависит от числа периодов N, на общей длительности которых осуществляется n отсчетов, опорной частоты сигнала f, длины зондирующей волны λ, фазы первого отсчета α и радиальной скорости объекта V_r. Идеальный случай радиолокационного сигнала – зондирование прямоугольными радиоимпульсами большой длительности.

Результаты расчета относительных погрешностей определения амплитуды сигнала для радара с N=1, f=1 МГц, λ=1 м приведены в таблице. (Для удобства погрешность дана в промилле.) Скорость 1 км/с соответствует максимальным скоростям современных истребителей.

Если используются другие значения λ, f и N, погрешность, приведенную в таблице, можно пересчитать, умножая ее на величину $a = 10N/(\lambda\ f)$, где размерность λ [м], а f [МГц]. Для приведенных характеристик радара относительные погрешности при радиальных скоростях объектов меньше 1 км/с ничтожно малы. Например, для радара с характеристиками N=1, λ=2 м, f =1 МГц для скоростей меньше 1 км/с погрешность не превышает 0,3 %.

N=1, λ=1м, f=10 МГц									
α°	$-V_r$, км/с				$+V_r$, км/с				α°
	8	**4**	**2**	**1**	**1**	**2**	**4**	**8**	
0	–0,1	–0,02	–0,003	0,0	0,0	0,003	0,02	0,1	0
45	–5,0	–2,6	–1,3	–0,6	0,6	1,3	2,6	5,0	45
90	0,1	0,02	0,003	0,0	0,0	–0,003	–0,02	–0,1	90
135	5,0	2,6	1,3	0,6	–0,6	–1,3	–2,6	–5,0	135
180	–0,1	–0,02	–0,003	0,0	0,0	0,003	0,02	0,1	180
225	–5,0	–2,6	–1,3	–0,6	0,6	1,3	2,6	5,0	225

Свести к минимуму влияние ошибки при больших N и иных характеристиках радара можно либо разработав корректирующие алгоритмы, либо сформировав последовательность (4) с применением сдвоенных отсчетов с интервалом $T/4$ (рис. 2). Если амплитуда определяется с использованием сдвоенных отсчетов, то такая последовательность существенно смягчает требования к узкополосности, доплеровский сдвиг и изменения огибающей сказываются меньше (возможные интервалы T/4 или 3T/4, или 5T/4 в зависимости от промежуточной частоты).

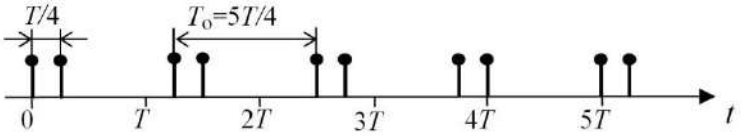


Рис. 2. Диаграмма следования отсчетов (вариант n=4; N=5)

Выводы

Предлагаемое преобразование в цифровой формат узкополосных радиосигналов с известной центральной частотой спектра позволяет существенно снизить объем выполняемых операций и может быть применимо при обработке сигналов некогерентного рассеяния, сигналов радиовещательных каналов с амплитудной модуляцией, а также и при обработке радиолокационных сигналов с фазовой (0, π) манипуляцией, если длительность элементов кода существенно больше периода сигнала опорной частоты.

Список литературы:

1. Skolnik M.I. Introduction to RADAR Systems. Second Ed. Singapore : McGraw Hill Publications, 1981.

2. Ziomek C., Corredoura P. Digital I/Q demodulator // Proceedings Particle Accelerator Conference 1-5 May 1995 USA, IEEE 2002. DOI: 10.1109/PAC.1995.505652.

3. Niranjan R.K., Rajendra Naik B. Approach of Pulse Parameters Measurement Using Digital IQ Method // International Journal of Information and Electronics Engineering. 2014. Vol. 4, No. 1. P. 31-35. DOI: 10.7763/IJIEE.2014.

4. Taran V.I., Rogozhkin E.V., Grigorenko E.I, Gridin A.N., Golobin V.I., Liokumovich V.I., Chernyaev S.V. Specialized measurement system of the Khar'kov Polytechnic Institute for investigating the ionosphere by the incoherent-scattering method // Radiophysics and Quantum Electronics. 1975. Vol. 18, Iss. 9, P. 1026-1027. DOI: 10.1007/BF01038201.

5. Рогожкин Е.В., Маенко Ф.А. Цифровой коррелометр для исследований сигналов с известной центральной частотой спектра // Вестник ХПИ. Сер. “Автоматика и приборостроение”. Харьков, 1975. №103 (2). С. 70-74.

6. Рогожкин Е.В., Белозеров Д.П., Еремин А.Н. Информационные возможности цифровой обработки радиосигналов при известной несущей частоте // Вестник Нац. техн. ун-та “ХПИ”: сб. науч. тр. темат. вып. : Радиофизика и ионосфера. Харьков : НТУ “ХПИ”, 2003. № 7, т. 4. С. 81-88.

7. Емельянов Л.Я., Лялюк А.И., Рогожкин Е.В. Особенности обработки сигналов некогерентного рассеяния на радаре Института ионосферы // Радиотехника. 2015. Вып. 182. С. 29-33.

8. Рогожкин Е.В., Подъячий Ю.И., Емельянов Л.Я. Модификация цифрового представления радиолокационных сигналов // Радиотехника. 2019. Вып. 196. С. 69-75.

Поступила в редколлегию 26.08.2020

Сведения об авторах:

Рогожкин Евгений Васильевич – д-р физ.-мат. наук, Национальный технический университет «Харьковский Политехнический Институт», заведующий кафедрой «Радиоэлектроника», Украина, e-mail: rogojkiner@ukr.net, ORCID: http://orcid.org/0000-0001-5310-3319

Подъячий Юрий Иванович – канд. физ.-мат. наук, Национальный технический университет «Харьковский Политехнический Институт», профессор кафедры «Радиоэлектроника», Украина, e-mail: yuivpod@gmail.com, ORCID: http://orcid.org/0000-0002-4848-947X

Емельянов Леонид Яковлевич – канд. физ.-мат. наук, Институт ионосферы НАН и МОН Украины, зав. отделом, Украина, e-mail: leonid.ya.emelyanov@gmail.com, ORCID: http://orcid.org/0000-0002-2117-2675

УДК 004.89: 621.396 **DOI:10.30837/rt.2020.3.202.18**

С.В. СОЛОНСКАЯ, канд. техн. наук, В.В. ЖИРНОВ, канд. техн. наук

ПРЕДИКАТНАЯ МОДЕЛЬ ПРОЦЕССНЫХ ЗНАНИЙ ПРИ ОБНАРУЖЕНИИ И РАСПОЗНАВАНИИ ПРОТЯЖЕННЫХ ОБЪЕКТОВ ТИПА ОБЛАКА, ТУЧИ, «АНГЕЛ-ЭХО» В ОБЗОРНЫХ РЛС

Введение

В статье рассмотрены актуальные вопросы разработки предикатной модели процессных знаний при обнаружении и распознавании радиолокационных сигналов протяженных объектов и метод принятия решений, основанный на прецедентах. Предложен метод обработки процессных знаний как инструмент для создания универсальных алгоритмов межпериодной обработки сигнальной информации для обеспечения эффективного обнаружения и распознавания сигналов от разных протяженных объектов, в том числе слабых сигналов от атмосферных неоднородностей тип «ангел-эхо». На основе анализа возможных сетей связей в предикатной модели выбраны классифицирующие и функциональные сети, где используются элементы логических и сетевых моделей. Из логических моделей заимствована идея правил вывода или решающего правила, а из сетевых моделей – описание знаний в виде семантической нейронной сети. В этой комбинированной модели явно выделена процедурная информация. Вместо логического вывода появляется вывод или решающее правило на знаниях.

В известных информационных системах контроля воздушного пространства [1] анализируется динамика межпериодных изменений первичных картин сигнальной обстановки. При этом, если воздушный объект протяженный, то из принятых сигналов формируется картина этого объекта, например, облака, стай птиц, локальных атмосферных неоднородностей типа «ангел-эхо». Из анализа публикаций следует [2 – 4], что интеллектуальными считают системы, которые могут решать задачи, выполняемые человеком-оператором. Эффективным математическим средством описания деятельность человека-оператора является алгебра предикатов и предикатных операций.

В информационных системах контроля подвижных объектов на воздушном и наземном транспорте используют методы обнаружения и распознавания сигналов [5 – 7]. При обнаружении радиолокационных целей задать вероятность прихода полезного сигнала или сигнала помехи очень сложно. При распознавании можно использовать не только энергетические признаки объектов.

Цель и задачи исследования

Цель: разработка предикатной модели процессных знаний при обнаружении и распознавании символьной модели радиолокационных сигналов протяженных воздушных объектов и метода принятия решений, основанного на прецедентах.

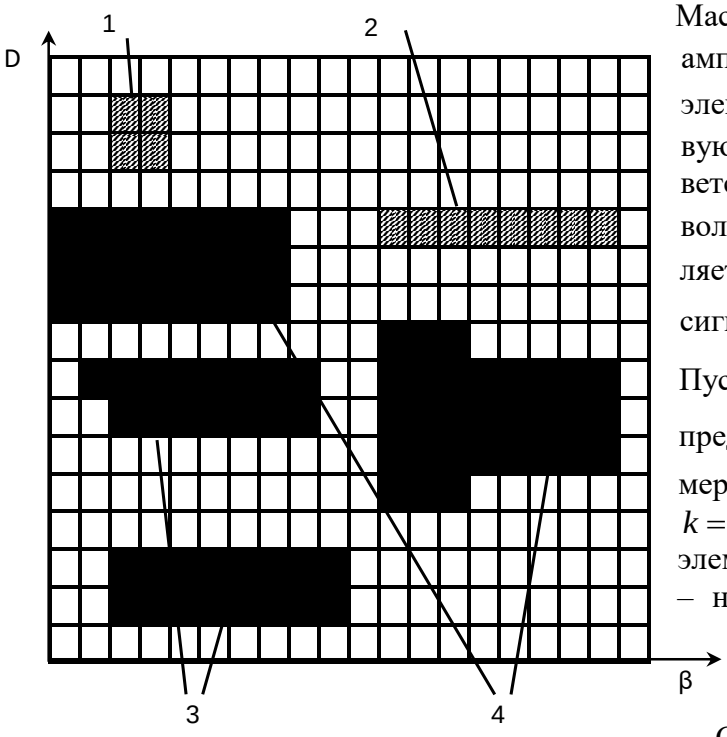
Задачи исследований: исходя из анализа возможных сетей связей в предикатной модели, выбрать классифицирующие и функциональные сети, где используются элементы логических и сетевых моделей. Из логических моделей взять правила вывода или решающего правила, а из сетевых моделей – описание знаний в виде семантической нейронной сети. Показать, как этот подход может использоваться для автоматизации процесса обнаружения и распознавания неподвижных и малоподвижных протяженных объектов типа облака, тучи, атмосферных неоднородностей типа «ангел-эхо».

Предикатные модели процессных знаний при обнаружении и распознавании протяженных объектов типа облака, тучи и «ангел-эхо»

В разработанную технологию входят процедуры формализации и анализа символьной модели наблюдаемых объектов на основе алгебры предикатов [8 – 13] и операций, предна-

значенных для создания предикатной модели процессных знаний получения решений о наблюдаемых объектах или обнаружении и распознавании протяженных объектов.

Символьная модель наблюдаемых протяженных объектов формируется из набора радиолокационных сигналов N информационных ячеек от каждого элемента зоны обзора. Обычно из полученных сигналов формируется карта или матрица данных. В нашем случае формируется символьная модель сигнальных отметок протяженных объектов типа облака, тучи и «ангел-эхо» (рис.1). Таким образом, обычная база данных превращается в базу знаний, в результате анализа которой можно и нужно получить требуемое решение.



1 –импульсная помеха; 2 – точечный объект;
3 – «ангел-эхо»; 4 – протяженные объекты.

Рис. 1 Символьные модели сигнальных отметок протяженных объектов

Массив данных представляет собой матрицу амплитуд $\|A\|$ размером $M \times N$. Каждый элемент матрицы i, j связан с соответствующим элементом зоны обзора РЛС соответственно. При этом формирование символьного массива амплитуд $\|A\|$ осуществляется запоминанием величины амплитуды сигнала q_{ij} на длительность T обзора РЛС. Пусть $M = \{q_{11}, q_{12}, ..., q_{ij}, ..., q_{mn}\}$ множество, представляющее собой матрицу $\|A\|$ размерностью $M \times N$, состоящее из элементов $k = m \times n$ – значений амплитуд сигналов в элементах обработки зоны обзора РЛС, а B – некоторое из его подмножеств $B \subseteq M$, амплитуды сигналов которого q_{ij} превышают пороговые значения V_{ij}. Составляем набор логических элементов t_{ij} по следующему принципу: если $q_{ij} \in B$, то $t_{ij} = 1$; если $q_{ij} \notin B$, то $t_{ij} = 0$, $i = \overline{1,m}$, $j = \overline{1,n}$.

Предикат $A(x)$ на множестве M, соответствующий множеству B элементов обработки, превысивших порог, с характеристикой $(t_{11}, t_{12}, \cdots, t_{ij}, \cdots, t_{mn})$, запишется формулой

$$A(x) = t_{11}x^{q_{11}} \vee ... \vee t_{mn}x^{q_{mn}} = \bigvee_{i=1,\, j=1}^{mn} t_{ij}x^{q_{ij}}. \quad (1)$$

Здесь выражение $x^{q_{ij}}$ – форма узнавания события. Когда $x = q_{ij}$, то $x^{q_{ij}} = 1$.

Предикатная модель процессных знаний о наблюдаемых воздушных или наземных объектов в общем виде – это система n унарных и бинарных предикатов Z_j:

$$M = \{Z_j, \ \ j = 1...n\}. \quad (2)$$

Такая система предикатов позволяет описать ситуацию вокруг анализируемой в данный момент информационной ячейки и позволяет формализовать процесс формирования символьного изображения отметки из $A(x)$ в течение ряда циклов зондирований РЛС. Их еще называют атрибутами или предикатными признаками процесса. Например, для радиолокационных систем обзора пространства это могут быть:

– унарный предикат Z_{pij} присутствия или наличия сигнала в a_{ij} информационной ячейке; i, j – номера элементов зоны обзора РЛС;

– бинарный предикат Z_{dij} ухода сигнала a_{ij} в соседнюю по дальности информационную ячейку;

– бинарный предикат Z_{aij} перехода сигнала в смежную по азимуту или соседнюю информационную ячейку, прилегающую к рассматриваемой ячейке.

При таких исходных условиях эти предикатные признаки формируются по следующим правилам:

$$Z_{pij} = 1, \text{ при } A_{ij} > 0 \tag{3}$$

$$Z_{dij} = 1, \text{ при } A_{i-1j} > 0 \wedge Z_{pij} = 1 \tag{4}$$

$$Z_{aij} = 1, \text{ при } Z_{pij} = 1 \wedge A_{ij-1} > 0, \tag{5}$$

где A_{ij} – предикат события наличия-отсутствия сигнала в соответствующем элементе анализа.

Предикатная модель процессных знаний о наблюдаемых объектах локации, адаптированная на обнаружение разных протяженных объектов, имеет следующий вид:

$$M^o = \{Z_j \mid \forall Z_j \in M \; \exists O_k \in O, k, \; j = 1...n\}, \tag{6}$$

где O – предметная область, O_k – объекты предметной области.

Разработана в общем виде иерархичная предикатная модель процессных знаний межпериодной обработки обзорной радиолокационной системы (рис. 3.), что позволяет представить "горизонтальный" процесс в виде "вертикальной" структуры в аналитической предикатной форме.

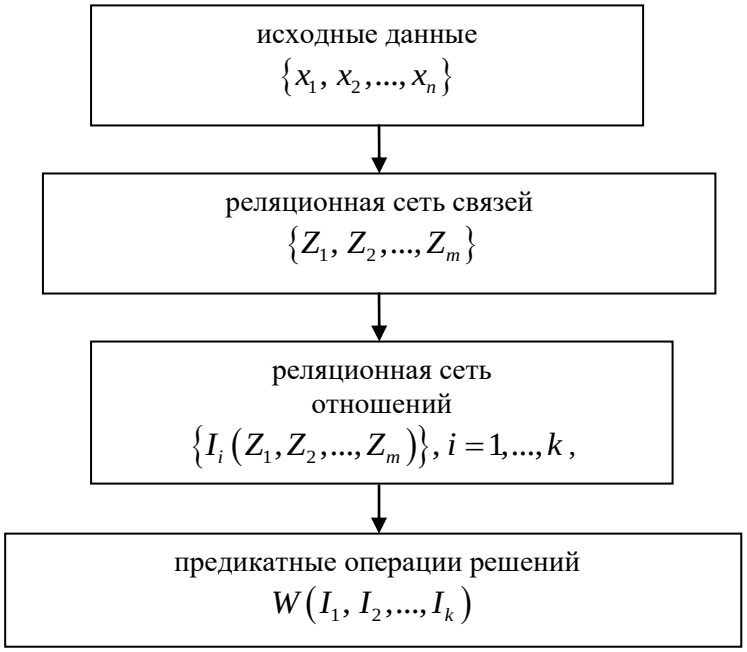


Рис. 2. Предикатная модель обработки процессных знаний

Первый уровень модели – это полученные в результате наблюдений данные $\{x_1, x_2, ..., x_n\}$, которые не всегда имеют удобный для использования формат. На втором уровне реляционная сеть $\{Z_1, Z_2, ..., Z_m\}$ задает связи между данными, которые определяют структуру информации.

На третьем уровне накопление знаний на основе данных и информации представляется как добавление новых реляционных сетей (отношений) $\{I_i(Z_1, Z_2, ..., Z_m)\}, i = 1, ..., k$, заданных на множестве начальных данных $\{x_1, x_2, ..., x_n\}$.

Четвертый уровень метазнаний объединяет все предыдущие уровни, позволяя находить новое понимание существующего знания. Формально уровень метазнаний имеет вид преди-

катной операции $W(I_1, I_2, ..., I_k)$, который задан на множестве $\{ I_1, I_2, ..., I_k \}$, связывает всю полученную информацию и в процессе ее обработки получает новую информацию.

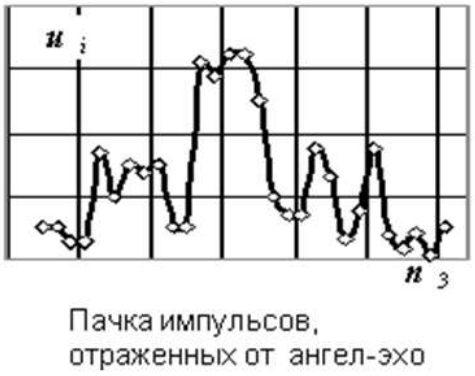


Рис. 3. Пачка сигналов от «ангел-эхо»

На рис. 3 приведена реальная, экспериментально полученная пачка импульсов, отраженных от «ангел-эхо». Здесь между информационными единицами предусмотрена возможность построения связей различного типа. Прежде всего, эти связи характеризуют отношения между информационными единицами. Семантика отношений носит и декларативный, и процедурный характер. С другой стороны процесс, как правило, описывается как функциональными связями, так и отношениями между информационными ячейками. Имея предикатные признаки, мы можем формализовать процессные знания получения символьных моделей сигнальных отметок для протяженных объектов типа облака, тучи, атмосферные образования типа «ангел-эхо».

Здесь две информационные единицы связаны отношением "причина – следствие": отношением появления сигнала в a_{ij} ячейке (это предикатный признак Z_{pij}^{k} присутствия сигнала); отношением ухода сигнала из a_{ij} ячейки (это предикатный признак $Z_{d\,ij}$ ухода (departure) сигнала); и отношением "соседней ячейки" (это предикатный признак $Z_{a\,ij}$ перехода сигнала в смежную по азимуту информационную ячейку). Приведенные отношения характеризуют декларативные знания.

Если между двумя информационными единицами установлено отношение "аргумент – функция", то оно характеризует процессное знание, связанное с вычислением определенных предикатных функций. Исследуем возможные операции.

На первом шаге составляем предикатные уравнения возможных состояний и путем их решения определяем номера $k = k_1$ и $l = l_1$ рядом расположенных элементов обработки с предикатными признаками $Z_{d\,ij}$ и $Z_{a\,ij}$ соседнего элемента обработки. Определяем также, с какими из этих признаков работать. Для этого при появлении предиката $Z_{p\,ij}$ наличия сигнала в a_{ij} информационной ячейке составляем предикатные уравнения для проверки возможности формирования бинарного предиката $Z_{d\,ij}$ (прихода сигнала из соседней по дальности $a_{i-1\,j}$ ячейки) и бинарного предиката $Z_{a\,ij}$ (перехода сигнала из смежной по азимуту a_{ij-1} ячейки), полученные из условий (4) и (5):

$$\begin{matrix} (A_{i-1\,j} > 0 \wedge Z_{p\,ij} = 1) = 1 \\ (Z_{p\,ij} = 1 \wedge A_{ij-1} > 0) = 1 \end{matrix} . \qquad (7)$$

Из анализа вариантов решений уравнений (7) можно сделать следующие выводы:

1. Если выполняется первое уравнение, то формируется бинарный предикат $Z_{d\,ij}$. Это означает, что сигнал в исследуемую ячейку переходит из соседней по дальности $a_{i-1\,j}$ ячейки и начинает формироваться новая символьная модель сигнальных отметок для протяженных неподвижных объектов типа облака, тучи или атмосферной неоднородности типа «ангел-эхо»;

2. Если выполняется второе уравнение, то формируется бинарный предикат $Z_{a\,ij}$. Это означает, что сигнал в исследуемую ячейку переходит из соседней по азимуту a_{ij-1} ячейки и начинает формироваться новая символьная модель (пачка) сигнальных отметок для точечных подвижных и малоподвижных летательных аппаратов типа самолет, вертолет, БПЛА;

3. Если выполняются первое и второе уравнение, то формируются бинарные предикаты $Z_{d\,ij}$ и $Z_{a\,ij}$. Это означает, что сигнал в исследуемую ячейку переходит и из соседней по дальности $a_{i-1\,j}$ ячейки и из соседней по азимуту a_{ij-1} ячейки. При этом начинает формироваться новая символьная модель сигнальных отметок для протяженных неподвижных объектов типа облака, тучи или атмосферной неоднородности типа «ангел-эхо»;

Более детально изучим процессные знания формирования символьной модели протяженных объектов. Для начала определим номер $k = k_1$ и $l = l_1$ рядом расположенных элементов обработки с предикатными признаками $Z_{d\,ij}$ и $Z_{a\,ij}$ соседнего элемента обработки. Здесь k_1 и l_1 – номера начала столбца и начала пачки символьных моделей сигнальных отметок для протяженных неподвижных объектов и точечных подвижных объектов. Для первого шага начала формирования символьных моделей определяем значения $k_1=0$, $l_1=0$. Исходя из анализа вариантов решений уравнений (7) и с учетом анализа структурных элементов процессной модели знаний по обнаружению и распознаванию протяженных объектов определяем очередность последующих процедур (шагов) обработки процессных знаний.

Далее, для нахождения следующего номера $k = k_2$ и $l = l_2$ элемента обработки с подобным предикатным признаком учитываем обозначившееся на первом шаге направление $(a_{ij}, a_{i+k_1, j+l_1})$ формирования возможных символьных моделей. Направление определяется с помощью анализа возможного (прогнозного) изменения номеров k_1, l_1 согласно анализу вариантов решений уравнений (7). При изменении номера по одной из координат (k_1 или l_1) направление поиска совпадает с направлением вдоль осей координат i или j (вниз или вправо). Анализ структурных элементов процессной модели знаний при межпериодной обработке сигнальной информации в обзорных РЛС показывает, что сначала идет заполнение информационных ячеек по дальности i, а затем уже идет заполнение информационных ячеек по азимуту j.

Таким образом, если имеется предикатный признак $Z_{d\,i+k_1 j}$ соседней ячейки по дальности, то в следующем шаге обработки проверяется наличие предикатного признака $Z_{d\,i+k_2 j}$ в информационной ячейке $a_{i+k_2 j}$.

$$Z_{d\,i+k_2 j}=(A_{ij}>0 \wedge Z_{p\,i+k_2 j}=1)=1 \tag{8}$$

На *n*-м шаге предикатное уравнение имеет вид:

$$Z_{d\,i+k_n j}=(A_{i+k_{n-1} j}>0 \wedge Z_{p\,i+k_n j}=1)=1 \tag{9}$$

В результате решения системы *n* предикатных уравнений (8), (9) находим все значения $k_1 \cdots k_n$ и запишем форму (вид) столбца символьной модели протяженного объекта в виде предикатного уравнения:

$$Z_{cdij}=\bigwedge_{k_1}^{k_n} Z_{di+k_n,j}=Z_{di+k_1,j}\wedge Z_{di+k_2,j}\wedge\cdots$$
$$\cdots\wedge Z_{di+(k_{n-1}),j}\wedge Z_{di+k_n,j}=1 \qquad (10)$$

Если выполняется первое и второе уравнение условий формулы (7), то одновременно формируются бинарные предикаты $Z_{d\,ij}$ и $Z_{a\,ij}$. Это означает, что сигнал в исследуемую ячейку переходит и из соседней по дальности $a_{i-1\,j}$ ячейки, и из соседней по азимуту a_{ij-1} ячейки. При этом начинает формироваться предикатный признак Z_{bij} символьной модели протяженных объектов типа облака, тучи или атмосферной неоднородности типа «ангел-эхо». В этом случае в следующем шаге обработки проверяется наличие столбца символьной модели протяженного объекта Z_{cdij} в информационной ячейке $a_{i+k_2,\,j+l_2}$ следующего по номеру $j+l_2$ зондирования РЛС:

$$Z_{d\,i+k_2,\,j+l_2}=(A_{ij+l_2}>0\wedge Z_{p\,i+k_2\,j+l_2}=1)=1. \qquad (11)$$

На *n*-м шаге предикатное уравнение имеет вид:

$$Z_{d\,i+k_n,\,j+l_2}=(A_{i+k_{n-1},\,j+l_2}>0\wedge Z_{p\,i+k_n,\,j+l_2}=1)=1. \qquad (12)$$

В результате решения системы *n* предикатных уравнений (11), (12) находим все значения $k_1\cdots k_n$ и запишем форму (вид) столбца символьной модели протяженного объекта в виде предикатного уравнения:

$$Z_{cdij+l_2}=\bigwedge_{k_1}^{k_n} Z_{di+k_n,j+l_2}=Z_{di+k_1,j+l_2}\wedge Z_{di+k_2,j+l_2}\wedge\cdots$$
$$\cdots\wedge Z_{di+(k_{n-1}),j+l_2}\wedge Z_{di+k_n,j+l_2}=1 \qquad (13)$$

В результате решения систем предикатных уравнений, подобных уравнениям (11) – (13), находим все возможные значения параметров столбцов символьной модели протяженного объекта Z_{cdij} для $j+l_1\cdots j+l_n$ азимутальных направлений и значение предикатного признака Z_{bij} символьной модели неподвижного протяженного объекта как решение предикатного уравнения

$$Z_{bij}=\left(\bigwedge_{l_1,k_1}^{l_n,k_n} Z_{cdi+k,\,j+l}=1\right)=\bigwedge_{l_1}^{l_n}\left(\bigwedge_{k_1}^{k_n} Z_{cdi+k,\,j+l}=1\right)=1 \qquad . \qquad (14)$$

Мы составили систему предикатных уравнений (8) – (14) моделей обработки процессных знаний при обнаружении и распознавании протяженных неподвижных объектов типа облака, тучи и «ангел-эхо». Путем решения этих уравнений можно составить структуру и перечень процедурных и семантических операций процессных моделей знаний.

Вид структуры и перечень процедурных и семантических операций обработки процессных знаний следует из анализа вариантов решений уравнений (7).

Если выполняется первое уравнение, то формируется бинарный предикат $Z_{d\,ij}$. Это означает, что сигнал в исследуемую ячейку перешел из соседней по дальности $a_{i-1\,j}$ ячейки и сформировался столбец новой символьной модели сигнальных отметок для протяженных

неподвижных объектов типа облака, тучи или атмосферной неоднородности типа «ангел-эхо». В результате решения системы *n* предикатных уравнений (8), (9) находим все значения $k_1 \cdots k_n$ и запишем форму (вид) столбца символьной модели протяженного объекта в виде предикатного уравнения (10).

Если выполняются первое и второе уравнение, то формируются бинарные предикаты $Z_{d\,ij}$ и $Z_{a\,ij}$. Это означает, что сигнал в исследуемую ячейку переходит и из соседней по дальности $a_{i-1\,j}$ ячейки и из соседней по азимуту a_{ij-1} ячейки. При этом начинает формироваться предикатный признак Z_{bij} символьной модели сигнальных отметок для протяженных неподвижных объектов типа облака, тучи или атмосферной неоднородности типа «ангел-эхо». В результате решения системы *n* предикатных уравнений (8), (9) находим все значения $k_1 \cdots k_n$ и запишем форму (вид) столбца символьной модели протяженного объекта в виде предикатного уравнения (10), а в результате решения систем предикатных уравнений, подобных уравнениям (11), (12), находим все возможные значения Z_{cdij} столбцов символьной модели протяженного объекта для $j+l_1 \cdots j+l_n$ азимутальных направлений и вид, и значение предикатного признака Z_{bij} символьной модели неподвижного протяженного объекта в виде предикатного уравнения (14).

Метод принятия решений, основанный на известных прецедентах

На основе разработанной модели процессных знаний при обнаружении и распознавании протяженных объектов разработан метод принятия решений, основанный на прецедентах. В зависимости от типов связей, используемых в модели, различают классифицирующие и функциональные сети [3]. Для наших целей наиболее применимы продукционные или комбинированные сети. В моделях этого типа используются некоторые элементы логических и сетевых моделей [8]. Из логических моделей заимствована идея правил вывода или решающего правила, а из сетевых моделей – описание знаний в виде семантической нейронной сети (рис. 4).

В методе явно выделена процедурная информация, которая описывается иными средствами, чем декларативная информация. Вместо логического вывода появляется вывод или решающее правило на знаниях. Формализация процессных знаний получения и обработки символьных моделей включает систему предикатных уравнений (8) – (14). Путем решения этих уравнений можно составить вид структуры и перечень процедурных и семантических операций обработки процессных этих моделей знаний. На рис. 4 иерархическая схема принятия решения.

Для оценки энергетического признака символьной модели протяженных объектов введено понятие накопленной энергии [12]. Она определяется как сумма амплитуд (предикатов) сигналов информационных ячеек символа протяженного объекта в направлениях, определяемых векторами (k_n, l_n) согласно предикатному уравнению:

$$I_{b2} = \sum_{k_1,l_1}^{k_n,l_n} q_{i+k_n,\,j+l_n} Z_{cdi+k,\,j+l} \qquad (15)$$

Матрица данных $M = \{q_{11}, q_{12}, ..., q_{ij}, ..., q_{mn}\}$

Первый уровень

Матрица предиката событий $A = \{A_{11}, A_{12}, ..., A_{ij}, ..., A_{mn}\}$

Второй уровень

Система унарных и бинарных предикатов $\{Z_{11}, Z_{12}, ...Z_{ij}, ..., Z_{mn}\}$:

– унарный предикат Z_{pij} присутствия в a_{ij} информационной ячейке $Z_{pij} = 1$, при $A_{ij} > 0$ (i, j – номера элементов зоны обзора РЛС);

– бинарный предикат Z_{dij} ухода сигнала a_{ij} в соседнюю по дальности информационную ячейку $Z_{dij} = 1$, при $A_{i-1j} > 0 \wedge Z_{pij} = 1$;

– бинарный предикат Z_{aij} перехода сигнала в смежную по азимуту или соседнюю информационную ячейку $Z_{aij} = 1$, при $Z_{pij} = 1 \wedge A_{ij-1} > 0$,

Третий уровень

Добавление новых реляционных сетей $\{I_i(Z_1, Z_2, ..., Z_m)\}$, $i = 1, ..., k$ заданных на множестве начальных данных $A = \{A_{11}, A_{12}, ..., A_{ij}, ..., A_{mn}\}$:

– предикатный признак символьной модели неподвижных протяженных объектов:

$$I_{b1} = Z_{bij} = (\bigwedge_{l_1, k_1}^{l_n, k_n} Z_{cdi+k, j+l} = 1) = \bigwedge_{l_1}^{l_n} (\bigwedge_{k_1}^{k_n} Z_{cdi+k, j+l} = 1) = 1;$$

– энергетический признак символьной модели неподвижных протяженных объектов:

$$I_{b2} = \sum_{k_1, l_1}^{k_n, l_n} q_{i+k_n, j+l_n} Z_{cdi+k, j+l}$$

где k, l – номера элементов символьных моделей объектов, начиная с текущего.

Четвертый уровень

объединяет все предыдущие уровни, имеет вид предикатной операции $W(I_1, I_2, ..., I_k)$.

Возможная иерархическая схема принятия решения

Неподвижный протяженный воздушный объект

$$O_b = W(I_{b1}, I_{b2})$$

Рис. 4. Иерархическая схема принятия решения

По виду предикатного признака символьной модели сигнальных отметок для протяженных неподвижных объектов, найденного из системы предикатных уравнений (8) – (14), и по энергетическому признаку символьной модели, определенному как суммарная амплитуда в виде (15), осуществляется процедура распознавания протяженных неподвижных воздушных объектов типа облака, тучи или атмосферной неоднородности типа «ангел-эхо».

Заключение

Разработаны предикатные модели процессных знаний при обнаружении и распознавании радиолокационных сигналов протяженных объектов и метод принятия решений, основанный на прецедентах. Предложен метод обработки процессных знаний как инструмент для создания универсальных алгоритмов межпериодной обработки сигнальной информации для обеспечения эффективного обнаружения и распознавания сигналов от разных протяженных объектов, в том числе слабых сигналов от атмосферных неоднородностей тип «ангел-эхо». В разработанную технологию входят процедуры формализации и анализа символьной модели наблюдаемых объектов на основе алгебры предикатов и операций обработки процессных знаний для получения решений о протяженных объектах.

Список литературы:

1. Сколник М.И. Справочник по радиолокации : в 2 т. ; пер. с англ. под ред. В.С. Вербы. Москва : Техносфера, 2014. 672 с.
2. Иванилов А.А. Реляционные алгебры и алгебры предикатов / А. А. Иванилов, Ю.П. Шабанов-Кушнаренко // Восточно-Европейский журнал передовых технологий. 2007. № 4/2. С. 43–48.
3. Russel S. Artificial intelligence. A modern approach, Second Edition / S. Russel, P. Norvig. Williams, 2006. 1410 p.
4. Бондаренко М. Ф. Теория интеллекта : учебник / М. Ф. Бондаренко, Ю. П. Шабанов-Кушнаренко. Харьков : изд-во СМИТ, 2007. 576 с.
5. Горелик А. Л. Методы распознавания / А. Л. Горелик, В. А. Скрипкин. Москва : Высш. шк, 2004. 261 с.
6. Журавлев Ю. И. Об алгебраическом подходе к решению задач распознавания или классификации // Проблемы кибернетики. 2005. Вып. 33. С. 5–68.
7. Жирнов В.В., Солонская С.В. Предикатная модель процессных знаний о наблюдаемых объектах в многоканальных интеллектуальных системах мониторинга // Радиотехника. 2019. Вып. 199. С. 67 – 74.
8. Solonskaya S. V., Zhirnov, V. V. Intelligent analysis of radar data based on fuzzy transforms // Telecommunications and Radio Engineering (English translation of Elektrosvyaz and Radio-tekhnika). 2018. 77 (15). P. 1321-1329.
9. Shubin I., Snisar S., Zhyrnov V., Slavhorodskyi V. Practical Application of Formal Representation of nformation for Intelligent Radar Systems // 5th International Scientific-Practical Conference “Problems of Infocommunications. Science and Technology (PIC S&T)”, 2018, 9-12 October, Pages 433-436.
10. Solonskaya S.V., Zhirnov V.V. Signal processing in the intelligence systems of detecting low-observable and low-doppler aerial targets/ Telecommunications and Radio Engineering. 2018. Vol. 77, Issue 20. P. 1827-1835.
11. Zhirnov V.V., Solonskaya S.V., Zima I.I. Magnetic and electric aspects of genesis of the radar angel clutters and their virtual imaging // Telecommunications and Radio Engineering (English translation of Elektrosvyaz and Radiotekhnika). 2016. 75 (15). P. 1331-1341.
12. Solonska S., Zhyrnov V., Holovin O. Semantic Processing of Radar Spectral Information for Air Object Recognition // 2019 IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019 – Proceedings.
13. Shubin I., Solonska S., Snisar S., Slavhorodskyi V., Skovorodnikova V. Semantic Radar Technology for Detecting and Recognizing Low-Visible Air Objects // 2019 IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019 – Proceedings.

Поступила в редколлегию 12.09.2020

Сведения об авторах:

Жирнов Владимир Витальевич – к.т.н., Харьковский национальный университет радиоэлектроники, в.н.с. НИЦ интегрированных радиоэлектронных систем и технологий, Украина, e-mail: nauka123@ukr.net

Солонская Светлана Владимировна – к.т.н., Харьковский национальный автомобильно-дорожный университет, доцент кафедры естественных и гуманитарных наук, Украина, e-mail: solonskaya@ukr.net, ORCID: https://orcid.org/0000-0002-8841-7825

УДК 621.397.48:004.932.2 **DOI:10.30837/rt.2020.3.202.19**

В.М. КАРТАШОВ, д-р техн. наук, В.Н. ОЛЕЙНИКОВ, канд. техн. наук,
В.П. РЯБУХА, канд. техн. наук, С.И. БАБКИН, канд. техн. наук,
В.В. ВОРОНИН, канд. техн. наук, А.И. КАПУСТА, И.С. СЕЛЕЗНЕВ

МЕТОДЫ КОМПЛЕКСНОЙ ОБРАБОТКИ И ИНТЕРПРЕТАЦИИ РАДИОЛОКАЦИОННЫХ, АКУСТИЧЕСКИХ, ОПТИЧЕСКИХ И ИНФРАКРАСНЫХ СИГНАЛОВ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Введение

В настоящее время известно большое количество различных типов беспилотных летательных аппаратов (БПЛА), способных выполнять широкий спектр полезных функций, а с другой стороны, способных нести потенциальную угрозу для различных областей деятельности человека – хозяйственной, повседневной и военной [1]. Трудности их обнаружения и наблюдения с использованием современных технических средств, а также сравнительно невысокая стоимость беспилотных аппаратов приводят к повышению безнаказанности и массовости противоправных действий с использованием БПЛА [2 – 5]. В соответствии с этим – задача защиты разнообразных объектов от воздействия БПЛА представляет собой одну из актуальных задач современности.

С целью обнаружения, распознавания и измерения координат беспилотных летательных аппаратов используют, прежде всего, радиолокационные, акустические, оптические и инфракрасные методы и средства [6 – 12].

Каждый из используемых методов обладает определенными достоинствами, недостатками и ограничениями. При этом каждый из методов характеризуется собственной областью возможностей, которая определяется множеством измеряемых информационных параметров сигнала с соответствующими показателями качества, диапазоном дальностей, пространственно-временным разрешением и т. д.

Поскольку области возможностей различных методов не совпадают, то появляется предпосылка совместного использования систем различного вида для расширения набора измеряемых параметров, диапазона наблюдаемых дальностей и повышения информативности получаемых данных путем совместной (комплексной) их обработки [13 – 19].

Во всех информационных каналах операции измерения координат БПЛА предшествует задача обнаружения. Хорошо разработанные методы энергетического обнаружения сигналов в данном случае не показывают достаточной эффективности [20, 21, 34, 35]. Это обусловлено тем, что обнаружение искомого объекта реализуется на фоне помех, имеющих определенные сходства с сигналом БПЛА, чаще всего, на фоне помех, формируемых птицами. Поэтому обнаружение дрона при наличии подобных ему объектов в используемых информационных каналах на практике реализуют как задачу «обнаружение-распознавание». Вследствие этого решение задачи обнаружения сопровождается анализом наличия некоторых дополнительных признаков у принимаемого сигнала.

Комплексная обработка сигналов различных информационных каналов может осуществляться как на этапе обнаружения, так и на этапе измерения координат. Причем, на этапе обнаружения она будет наиболее востребована в силу сложности задачи обнаружения-распознавания.

Рассмотрим известные в литературе системы комплексной обработки информации, используемые для обнаружения БПЛА. Целью публикации [22] является изучение работы мультисенсорных систем, предназначенных для решения задач обнаружения БПЛА, определения их пространственных координат, а также изучение различных схем объединения данных используемых информационных каналов. Система содержит радиолокационный, оптический и радиочастотный каналы. Обработка информации включала такие этапы: сопоставление данных, обнаружение целей и измерение их пространственных координат. Вначале

выполнялось обнаружение целей отдельно в различных информационных каналах, затем осуществлялось сопоставление и совмещение результатов обнаружения по принадлежности к определенной цели. На этом этапе выявлялось, какие решения соответствуют целям, а какие – представляют собой ложную тревогу, определялся также вклад каждого канала в обнаружение. Далее реализовывался алгоритм слияния данных в процессе комплексного измерения пространственных координат объектов.

В [23] рассмотрено объединение информации, поступающей по радиолокационному, акустическому и оптическому каналам с целью обнаружения, классификации наблюдаемых БПЛА и определения их местоположения. Комплексная система обеспечивает погрешности измерения угловых координат – азимута и угла места соответственно 1,5 и 2,5 град. Пеленгование по акустическому каналу осуществляется с использованием алгоритма MUSIC-MULIC.

Комплексирование радиолокационного и акустического каналов позволило существенно уменьшить вероятность ложных тревог, а комплексирование изображений видимого и инфракрасного диапазонов (последнее получено в коротковолновом инфракрасном диапазоне (SWIR)) позволило обеспечить более быстрое и достоверное обнаружение БПЛА при наличии помех, дыма и плотного фона на изображениях.

Обнаружение и отслеживание БПЛА в городской черте [24] осуществлялось с использованием статических и мобильных пунктов, которые включали радиолокационные, акустические, оптические средства наблюдения и лазерный локатор – лидар. Пеленгация и определение местоположения осуществлялось с использованием многоканальной акустической системы и метода триангуляции. Система позволяет обнаруживать дрон и определять его местоположение со средней ошибкой в 6 м.

В ряде работ рассмотрено объединение данных различных информационных каналов, предназначенных для обнаружения БПЛА, с использованием средств искусственного интеллекта.

В [25] предварительное обнаружение БПЛА осуществлялось с помощью радиолокационной станции. Совокупность акустических датчиков, информация с которых подавалась на предварительно обученный алгоритм глубокого обучения, состоящий из трех MLP, использовалась для выявления БПЛА. Система продемонстрировала успешное решение задач по обнаружению БПЛА в полевых условиях при малой вероятности ложных тревог. Стоимость такой комплексной системы достаточно мала, однако дальность обнаружения дронов составляет всего 50 м.

Недорогое оборудование, включающее радиолокационный, акустический, видимый и инфракрасный каналы, использовалось в комплексной системе [26]. Для объединения информации указанных каналов использовался фильтр Калмана, с которого информация подавалась на классификатор ближайшего соседа для вынесения решения. Система позволяла отслеживать воздушные транспортные средства на расстоянии до 800 м.

В системе [27] использовался комплекс из 30 видеокамер и трех микрофонов. В оптическом и акустическом каналах использовались классификаторы SVM, обученные соответственно по изображениям беспилотников и акустическим сигналам, порождаемым БПЛА. Система показала успешную работу при полетах различных видов БПЛА на высотах до 100 м и на удалении до 200 м.

Число публикаций, в которых рассматриваются методы и системы, предназначенные для обнаружения и наблюдения БПЛА на фоне разнообразных помех и различных объектов, постоянно увеличивается. Определенное внимание в литературе уделяется и комплексным системам, построенным с использованием различных физических датчиков – мультисенсорным системам. Рассматриваются различные методы приема, обработки сигналов, их последующего интеллектуального анализа. Однако эффективность функционирования систем с комплексной обработкой сигналов на практике является недостаточной.

Авторы многих публикаций не вполне осознают сложность задачи обнаружения и противодействия БПЛА, рассматривают только отдельные, частные аспекты этой проблематики, не обладая сведениями о реальных возможностях существующих технических средств и комплексов. Вместе с тем, проблема эффективного наблюдения и противодействия БПЛА (особенно малым БПЛА) до настоящего времени не имеет удовлетворительного решения, является сложной, многогранной и требует комплексного, системного подхода при ее решении.

Статья посвящена анализу возможностей систем с комплексной обработкой информации, получаемой по каждому из используемых каналов, а также разработке новых более эффективных методов комплексирования радиолокационных, акустических, оптических и инфракрасных информационных каналов комплексных систем обнаружения и измерения координат БПЛА.

Стратегии и методы объединения информации многоканальных систем

Увеличение числа используемых в комплексной системе измерителей, работающих как на одних, так и на различных физических принципах, позволяет улучшить показатели качества системы [28].

Дублирование даже однотипных измерителей, определяющих одни и те же параметры (координаты), приводит к структурной избыточности, что повышает надежность системы, поскольку выход из строя одного из измерителей не приводит к отказу всей комплексной системы в целом. Объединение различных измерителей, особенно работающих на разных физических принципах (например, радиолокационных и акустических), повышает помехозащищенность системы, так как каждый из каналов подвержен воздействию различных помех [28, 29].

Создание структурной избыточности сопровождается появлением информационной избыточности. В этом случае один и тот же параметр измеряется в различных каналах, что обеспечивает получение большего количества информации. В результате обработки полученной информации становится возможным уменьшить погрешности результатов измерений и повысить точность показателей качества системы.

Таким образом, под комплексированием каналов получения информации понимается их объединение в комплексную систему, реализующую совместную обработку полученной информации и обеспечивающую повышение основных показателей качества системы – помехозащищенности, надежности, точности измерений, вероятности правильного обнаружения и классификации (распознавания) целей [30].

В литературе также говорят о многомодальном объединении, обеспечивающем синергетическое использование информации, полученной из разных информационных каналов (модальностей). Термин «многомодальная интеграция/многомодальное объединение» может соответствовать любой стадии процесса интеграции, где присутствует совместное использование информации, полученной от различных источников. Объединение данных имеет смысл в том случае, когда используемые данные составляют избыточную и взаимно дополняющую информацию [31]. Интеграция в итоге уменьшает общую неопределенность и обеспечивает повышению точности, с которой признаки оцениваются системой. Избыточность информации также служит цели повышения надежности системы в случае появления аномальных ошибок, промахов или сбоев в каналах. Очень важно, что дополнительная информация из нескольких модальностей позволяет использовать признаки, которые невозможно однозначно воспринять и интерпретировать, имея лишь информацию от каждой модальности в отдельности. Также благодаря возможности реализовать параллельную обработку данных в используемых каналах несколько модальностей обеспечивают предоставление более оперативной информации.

Обобщенная структурная схема системы комплексной обработки сигналов информационных каналов, используемых при обнаружении БПЛА, приведена на рис. 1.

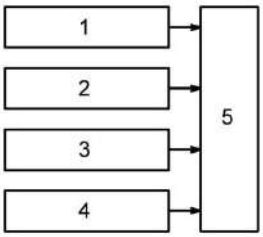


Рис. 1. Обобщенная структурная схема системы комплексной обработки сигналов, используемых при обнаружении БПЛА:
1 – радиолокационный канал, 2 – акустический канал, 3 – оптический канал, 4 – инфракрасный канал, 5 – устройство обработки и принятия решения

Объединение информации в комплексной системе возможно на уровне сигналов, на уровне признаков и на уровне решений.

*Стратегии объединения данных***,** получаемых с использованием различных каналов и датчиков получения входной информации об изучаемом объекте, разделяют на основные группы [28]:

- раннего объединения, реализуемые на уровне сигналов;
- раннего объединения, реализуемые на уровне признаков описания;
- позднего объединения, реализуемые на семантическом уровне принятия решения;
- гибридного объединения.

При раннем объединении информационные признаки формируются с использованием сигналов, поступающих по используемым информационным каналам (с использованием сигналов разных модальностей). Затем образованный вектор признаков $\vec{P} = [p_1, ...p_i, ...p_n]$ подается в устройство обработки-распознавания и принятия решения R. Стратегия раннего объединения многомодальной информации в комплексной системе обнаружения БПЛА на уровне признаков представлена на рис. 2.

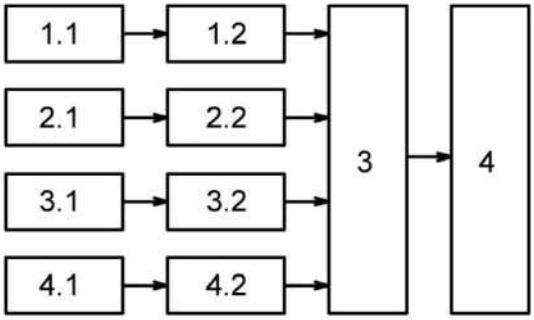


Рис. 2. Стратегия раннего объединения многомодальной информации на уровне признаков:
1.1, 2.1, 3.1, 4.1 – формирователи радиолокационного, акустического, оптического и инфракрасного сигналов (изображений), 1.2, 2.2, 3.2, 4.2 – формирователи признаков, 3 – объединение признаков (формирование вектора признаков), 4 – устройство принятия решения

Стратегия раннего объединения многомодальной информации в комплексной системе обнаружения БПЛА на уровне сигналов и признаков представлена на рис. 3. Здесь в каналах 1 и 2 объединение реализовано на уровне признаков, а в каналах 3 и 4 – на уровне физических сигналов (изображений).

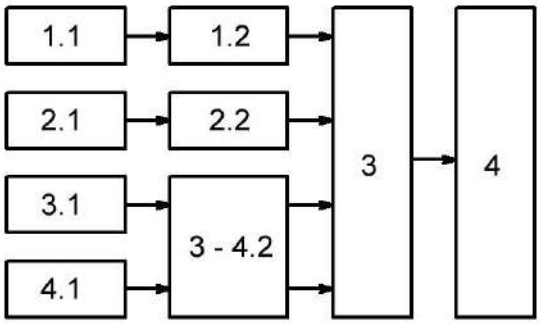


Рис. 3. Стратегия раннего объединеия многомодальной информации на уровне сигналов и признаков:
1.1, 2.1, 3.1, 4.1 – формирователи радиолокационного, акустического, оптического и инфракрасного сигналов (изображений), 1.2, 2.2 – формирователи признаков, 3-4.2 – объединение сигналов и формирование признаков, 3 – объединение признаков (формирование вектора признаков), 4 – устройство принятия решения

В методе позднего объединения канальные устройства обработки выносят частные решения в используемых информационных каналах, образуя вектор канальных решений $\vec{R} = [r_1, ...r_i, ...r_n]$ на основе соответствующих канальных признаков. Полученные решения интегрируются в вектор частных решений, с использованием которого формируется далее результирующее решение R (рис. 4.).

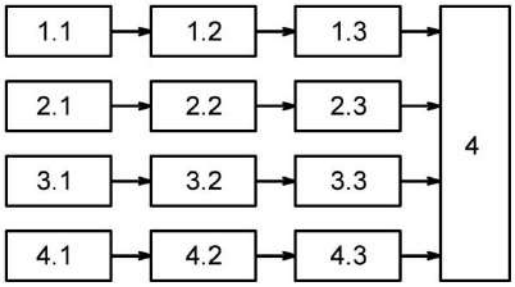
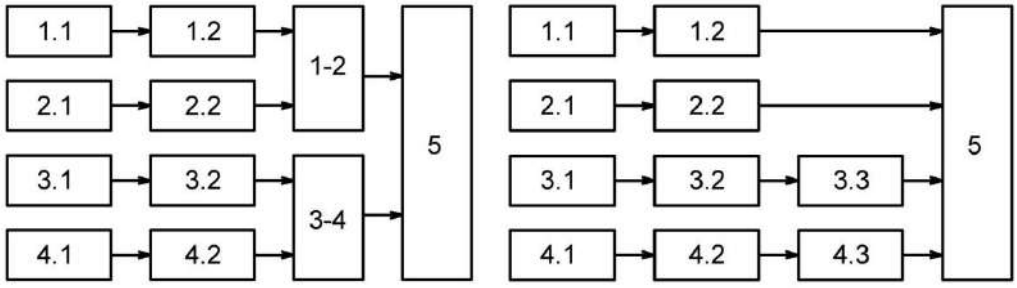


Рис. 4. Стратегия позднего объединеия многомодальной информации на уровне решений:
1.1, 2.1, 3.1, 4.1 – формирователи радиолокационного, акустического, оптического и инфракрасного сигналов (изображений), 1.2, 2.2, 3.2, 4.2 – формирователи признаков, 1.3, 2.3, 3.3, 4.3 – устройства принятия канальных решений, 4 – устройство формирования итогового решения

Стратегия гибридного объединения позволяет обеспечивать более гибкую комплексную обработку информации, поступающей по имеющимся каналам, с последующим принятием итогового решения. Она может быть реализована в различных видах, с использованием различных схем, некоторые из них представлены на рис. 5, *а, б.*



а *б*

Рис. 5. Различные стратегии гибридного объединеия многомодальной информации:
1.1, 2.1, 3.1, 4.1 – формирователи радиолокационного, акустического, оптического и инфракрасного сигналов (изображений) ,1.2, 2.2, 3.2, 4.2 – формирователи признаков,1-2, 3-4 – устройства объединение признаков, 3.3, 4.3 – устройства принятия частных решений, 5 – устройство принятия итогового решения

Стратегия гибридного объединения многомодальных сигналов информационных каналов комплексной системы позволит осуществлять эффективную обработку и объединение информации с учетом специфики решаемых задач и возможностей имеющихся технических средств.

При использовании классических подходов принятие, вынесение решения по имеющимся входным данным сопровождается потерей, разрушением значительной части информации, имеющейся во входных данных. И далее в процессе обработки участвует только информация, перешедшая в принятое решение (например, об обнаружении) или перешедшая в вынесенную оценку (оценку дальности до объекта) [31].

Использование современных математических средств (алгоритмов машинного обучения, нейронных сетей), а также современных технических средств (аппаратных и программных) позволяет более полноценно использовать информацию, содержащуюся во входных сигналах информационных каналов комплексных систем, осуществляя грамотное ее объединение с использованием рассмотренных подходов.

Методы объединения многомодальной (канальной) информации подразделяются на три основные группы: методы, основанные на правилах; основанные на классификации и методы, основанные на оценках [32].

Методы, основанные на правилах, включают линейное взвешенное объединение, мажоритарное правило и методы, определенные исследователем.

Методы, основанные на классификации, используют методы опорных векторов, байесовский вывод, теорию Дампстера – Шафера, динамические байесовские сети, нейронные сети, модель максимальной энтропии.

Методы, основанные на оценках, включают фильтр Калмана, расширенный фильтр Калмана, фракционный фильтр.

Существенное значение при объединении информации различных информационных каналов имеет корреляция между данными в различных каналах – кроссмодальная корреляция. Корреляция может определяться на различных уровнях объединения информации и использоваться в случае реализации различных методов [32].

В то же время, во внимание может приниматься не только корреляция между отдельными модальностями, но также и их независимость, что в ряде случаев позволяет достичь выигрыша при принятии решений.

Сигналы используемых информационных каналов обычно поступают в разных физических представлениях, обрабатываются с использованием различных методов, записываются и фиксируются с различной скоростью и в различных форматах. В соответствии с этим при их совместной обработке и принятии решений возникает необходимость в их синхронизации.

В случае синхронизации на уровне признаков происходит объединение признаков, сформированных в различных информационных каналах, которые получены в течение некоторого времени анализа от разнородных, но связанных и коррелированных между собой модальностей. Синхронизация на уровне принятия решений также нуждается в формировании временных меток, которые будут сопровождать происходящие события и принимаемые решения.

Методы объединения канальной информации при использовании нейронных сетей имеют ряд особенностей. В частности, объединение информационных каналов здесь осуществляется не на уровне признаков, формируемых в униполярных концептах, а путем объединения в мультимодальное семантическое представление (мультимодальную функцию) [32].

Результаты униполярного анализа при использовании нейронных сетей (НС) и раннего объединения сливаются до того, как соответствующие канальные представления изучены и сформированы соответствующие признаки. При использовании позднего слияния изучается канальная информация с помощью НС, при которой полученные оценки унимодальных

функций образуют вектор оценок мультимодальных функций, которые являются входными данными для системы машинного обучения.

В настоящее время сформулированы основные технические задачи, которые возникают при мультиспектральном объединении изображений, видео и звука [33]. Это представление, трансформация, выравнивание, слияние и совместное обучение. Представление определяет собой метод, который направлен на объединение унимодальных сигналов в общее пространство представлений. Трансформация – изменение формы представляемых данных. В процессе выравнивания определяются существующие связи между элементами различных модальностей. Слияние – объединение информации нескольких источников, совместное обучение – этап, на котором знания извлекаются из существующих модальностей.

Комплексирование информационных каналов с позиций статистической теории радиосистем

С позиций теории статистической теории радиосистем имеется два основных подхода к комплексированию информационных средств [34 – 36]. В соответствии с первым из них задача комплексирования решается на этапе первичной обработки информации, в соответствии со вторым – на этапе вторичной обработки (на этапе объединения решений). Вторичной принято называть обработку, при которой используются результаты вынесенных оценок и решений после соответствующей обработки поступающих входных сигналов (фильтрации, детектирования). При вторичной обработке решается задача обнаружения и сглаживания, например траекторий летательных аппаратов и т.д. В процессе третичной обработки с помощью математических методов уточняется и дополняется полученная информация, достигается повышение полноты данных и устойчивости сопровождения целей, а также оптимизируется группировка радиолокационных средств для получения радиолокационной информации (РЛИ) максимального качества при минимальным расходе ресурсов с учетом имеющихся обстановки и средств. Входной для третичной обработки является информация о трасах целей, полученных в результате вторичной обработки от различных радиолокационных станций (РЛС), координаты источников РЛИ и их характеристики. Выход третичной обработки – трассы целей, полученные с учётом передачи цели от одной РЛС к другой, точностные показатели разных источников и т. д.

При первом подходе к комплексированию в рамках статистической теории радиосистем по результатам наблюдения векторного процесса, компоненты которого представляют собой входные сигналы информационных каналов, осуществляется оптимальный синтез устройств первичной обработки сигналов в каждом канале, а также объединение информации, получаемой в каждом из каналов [35, 37]. Такой подход позволяет синтезировать оптимальную (в соответствии с выбранным критерием качества) комплексную систему обработку информации (КСОИ), обеспечивающую получение максимального количества информации из векторного процесса, наблюдаемого на входах информационных каналов.

При втором подходе компоненты наблюдаемого векторного процесса будут представлять собой выходные данные устройств первичной обработки сигналов. Это будут принятые решения об обнаружении, результаты оценивания координат объекта и т.д. В этом случае осуществляется синтез комплексной системы вторичной обработки информации (КСВОИ). Поскольку синтез КСВОИ осуществляется при имеющихся ограничениях на структуру и параметры устройств первичной обработки, которые заданы и физически реализованы, то качество получаемой информации на выходе КСВОИ может оказаться более низким, по сравнению с качеством выходных результатов КСОИ. Снижение качества обусловлено принятыми ограничениями на структуру системы.

Несмотря на некоторый проигрыш КСВОИ в сравнении с КСОИ использование оптимизации на этапе вторичной обработки (этапе решений) во многих случаях оказывается целесообразным на практике, поскольку опирается на использование того оборудования (устройств

первичной обработки сигналов), которые имеются в распоряжении разработчика и используются им для построения соответствующих информационных каналов.

Математические методы статистической теории радиосистем позволяют осуществить оптимальный синтез комплексных систем обнаружения и измерения параметров БПЛА при использовании различных информационных каналов и технических средств.

Выводы

1. Проанализированы известные комплексные системы обнаружения БПЛА, реализованные в виде совокупности информационных каналов, используемых в них системотехнических и технических решений, методы обработки многомодальных сигналов и изображений. Показано, что известные системы и методы обработки информации не позволяют решать задачи с необходимой эффективностью, и требуется их дальнейшее совершенствование.

Проблема эффективного наблюдения и противодействия БПЛА (особенно малым БПЛА) до настоящего времени не имеет удовлетворительного решения, является сложной, многогранной и требует комплексного, системного подхода при ее решении.

2. Обобщены известные и предложены новые стратегии и методы обработки и объединения (интеграции) многомодальной информации, получаемой с использованием информационных каналов, применяемых при наблюдении БПЛА. Показаны особенности объединения многомодальной информации с использованием нейросетевых технологий.

В частности, объединение информационных каналов при раннем объединении осуществляется не на уровне признаков, формируемых в униполярных концептах, а путем объединения в мультимодальное семантическое представление (мультимодальную функцию). При использовании позднего слияния изучается канальная информации с помощью НС, полученные оценки унимодальных функций образуют вектор оценок мультимодальных функций, которые являются входными данными для системы машинного обучения.

3. Проанализированы возможности объединения многомодальной информации комплексных систем обнаружения БПЛА с использованием статистической теории радиосистем (стохастической теории нелинейной фильтрации). Показано, что стохастическая теория нелинейной фильтрации может быть использована для оптимизации комплексных систем обнаружения БПЛА. С ее использованием осуществляется оптимальный синтез устройств первичной обработки сигналов в каждом канале, а также объединяется информация, получаемая в каждом из каналов. Такой подход позволяет синтезировать оптимальную (в соответствии с выбранным критерием качества) комплексную систему обработки информации – КСОИ, обеспечивающую получение максимального количества информации из векторного процесса, наблюдаемого на входах информационных каналов.

4. Использование разработанных подходов, стратегий и методов обработки и объединения многомодальной информации в комплексных системах наблюдения БПЛА позволит осуществлять гибкое объединение разнородной информации, получаемой по используемым каналам, с учетом специфики решаемых задач и возможностей используемых технических средств.

Список литературы:

1. Кошкин Р.П. Беспилотные авиационные системы. Москва : Стратегические приоритеты, 2016. 676 с.

2. Макаренко С. И., Тимошенко А. В., Васильченко А. С. Анализ средств и способов противодействия беспилотным летательным аппаратам. Ч. 1. Беспилотный летательный аппарат как объект обнаружения и поражения / Системы управления, связи и безопасности. 2020. № 1. С. 109-146. DOI: 10.24411/2410-9916-2020-10105.

3. Kartashov V.M., Oleynikov V.N, Sheyko S.A., Koryttsev I.V., Babkin S.I., Zubkov O.V. Peculiarities of small unmanned aerial vehicles detection and recognition // Telecommunications and Radio Engineering. 2019. Vol. 78, Issue 9. P. 771–781.

4. Kartashov V. M., Oleynikov V. N., Sheyko S. A., Babkin S. I., Koryttsev I. V., Zubkov O. V., Anokhin M. A. Information characteristics of sound radiation of small unmanned aerial vehicles // Telecommunications and Radio Engineering. 2018. Vol. 77., Iss. 10. P. 915–924.

5. Карташов В.М., Олейников В.Н., Шейко С.А., Бабкин С.И., Корытцев И.В., Зубков О.В., Анохин М.А. Информационные характеристики звукового излучения малых беспилотных летательных аппаратов// Радиотехника. 2017. Вып. 191. С. 181–193.

6. Kartashov V., Oleynikov V., Zubkov O., Sheiko S. Optical detection of unmanned air vehicles on a video stream in a real-time // The Fourth International Conferenceon Information and Telecommunication Technologies and Radio Electronics (UkrMiCo'2019), 9-13 September 2019, Odessa, Ukraine. 4 p.

7. Oleksandr Sotnikov, Vladimir Kartashov, Oleksandr Tymochko, Oleg Sergiyenko, Vera Tyrsa, Paolo Mercorelli, Wendy Flores-Fuentes. Methods for Ensuring the Accuracy of Radiometric and Optoelectronic Navigation Systems of Flying Robots in a Developed Infrastructure. Chapter 16 // Machine Vision and Navigation; Editors: Sergiyenko**,** Oleg, Flores-Fuentes**,** Wendy**,** Mercorelli**,** Paolo. P.537–578.

8. Oleynikov V. N , Zubkov O. V., Kartashov V. M., Korytsev I. V., Babkin S. I., Sheiko S. A. Investigation of detection and recognition efficiency of small unmanned aerial vehicles on their acoustic emission // Telecommunications and Radio Engineering. 2019. Vol. 78, Issue 9. P. 759–770.

9. Kartashov V., Oleynikov V., Koryttsev I., Zubkov O., Babkin S., Sheiko S. Processing and Recognition of Small Unmanned Vehicles Sound Signals // 2018 International Scientific-Practical Conference on Problems of Infocommunications. Science and Technology (PIC S and T 2018). Proceedings, 31 January 2019. P. 392–396.

10. Kartashov V., Oleynikov V., Koryttsev I., Sheyko S., Zubkov O., Babkin S., Selieznov I. Use of Acoustic Signature for Detection, Recognition and Direction Finding of Small Unmanned Aerial Vehicles // 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), 25-29 Feb. 2020. P. 1–4.

11. Kartashov V.M., Oleynikov V.N, Zubkov O.V., Korytsev I.V., Babkin S. I., Sheiko S.A., Kolendovskaya M.M. Spatial-temporal Processing of acoustic Signals of Unmanned Aerial Vehicles // Telecommunications and Radio Engineering. 2020. Vol. 79, Iss. 9. P. 769–780.

12. Oleynikov V., Zubkov O., Kartashov V., Koryttsev I., Sheiko S., Babkin S. Experimental estimation of direction finding to unmanned air vehicles algorithms efficiency by their acoustic emission // 2019 International Scientific-Practical Conference: Problems of Infocommunications. Science and Technology (PIC S and T 2019). Proceeding, 2019. P. 175–178.

13. Kartashov V. M., Tikhonov V. A., Voronin V. V. Features of Construction and Application of Complex Systems for the Atmosphere Remote Sounding // Telecommunications and Radio Engineering. 2017. Vol. 78, Issue 8. P.743–749.

14. Карташов В.М., Олейников В.Н., Колендовская М.М., Тимошенко Л.П., Капуста А.И., Рыбников Н.В. Комплексирование изображений при обнаружении беспилотных летательных аппаратов // Радиотехника. 2020. Вып. 201. С.120–129.

15. Kartashov V.M., Tikhonov V.A., Voronin V.V., Tymoshenko L.P. Complex model of random signal in problems of acoustic sounding of atmosphere // Telecommunications and Radio Engineering. 2016. Vol. 75, Iss. 20. P. 1885–1892.

16. Developing and Applying Optoelectronics in Machine Vision / Oleg Sergiyenko and Julio C. Rodriguez-Quiñonez; 2016. IGI Global. 341 p.

17. Sytnik O., KartashovV. Methods and Algorithms for Technical Visionin Radar Introscopy. Chapter 13 // Optoelectronics in Machine Vision-Based Theories and Applications. IGI Global, 2019. P. 373–391.

18. Дистанционные методы и средства исследования процессов в атмосфере Земли ; под ред. Б.Л. Кащеева, Е.Г. Прошкина, М.Ф. Лагутина. Харьков : Бизнес Информ, 2002. 426 с.

19. Карташов В.М. Модели и методы обработки сигналов систем радиоакустического и акустического зондирования атмосферы. Харьков : ХНУРЭ, 2011. 234 с.

20. Сосулин Ю.Г. Тероретические основы радиолокации и радионавигации : учеб. пособие для вузов. Москва : Радио и связь, 1992. 304 с.

21. Карташов В.М. и др. Обработка сигналов в радиоэлектронных системах дистанционного мониторинга атмосферы. Харьков : ХНУРЭ, 2014. 312 с.

22. Koch W., Koller J., Ulmke M. Ground target tracking and road map extraction // ISPRS J. Photogramm. Remote Sens. 2006; 61:197–208. doi: 10.1016/j.isprsjprs.2006.09.013.

23. Hengy S., Laurenzis M., Schertzer S., Hommes A., Kloeppel F., Shoykhetbrod A., Geibig T., Johannes W., Rassy O., Christnacher F. Multimodal UAV detection: Study of various intrusion scenarios // Proceedings of the Electro-Optical Remote Sensing XI International Society for Optics and Photonics; Warsaw, Poland. 11–14 September 2017. P. 104340P.

24. Laurenzis M., Hengy S., Hammer M., Hommes A., Johannes W., Giovanneschi F., Rassy O., Bacher E., Schertzer S., Poyet J.M. An adaptive sensing approach for the detection of small UAV: First investigation of static sensor network and moving sensor platform // Proceedings of the Signal Processing, Sensor/Information Fusion, and Target Recognition XXVII International Society for Optics and Photonics; Orlando, FL, USA. 16–19 April 2018. P. 106460S.

25. Park S., Shin S., Kim Y., Matson E.T., Lee K., Kolodzy P.J., Slater J.C., Scherreik M., Sam M., Gallagher J.C., et al. Combination of radar and audio sensors for identification of rotor-type unmanned aerial vehicles // Proceedings of the 2015 IEEE SENSORS; Busan, Korea. 1–4 November 2015. P. 1–4.

26. Charvat G.L., Fenn A.J., Perry B.T. The MIT IAP radar course: Build a small radar system capable of sensing range, Doppler, and synthetic aperture (SAR) imaging // Proceedings of the 2012 IEEE Radar Conference; Atlanta, GA, USA. 7–11 May 2012; pp. 0138–0144.

27. Liu H., Wei Z., Chen Y., Pan J., Lin L., Ren Y. Drone detection based on an audio-assisted camera array // Proceedings of the 2017 IEEE Third International Conference on Multimedia Big Data (BigMM); Laguna Hills, CA, USA. 19–21 April 2017; pp. 402–406.

28. Басов О.О., Карпов А.А. Анализ стратегий и методов объединения многомодальной информации // Обработка информации и управления. 2015. №2. С.7–14.

29. Atrey P. K., Hossain M. A., Kankanhalli M. S. Multimoda Fusion for Multimedia Analysis: a Survey // Multimedia Systems. 2010. Vol. 16. Iss. 6. P. 345–379.

30. Wu K., Lin C. K., Chang E., Smith J. R. Multimodal Information Fusion for Video Concept Detection // Proceedings IEEE Intern. Conf. on Image Processing, Singapore, 2004. P. 2391–2394.

31. Bendjebbour A., et al. Multisensor Image Segmentation Using Dempster–Shafer Fusion in Markov FieldsContext // IEEE Transactions on Geoscience and Remote Sensing. 2001. Vol. 39(8). P. 1789–1798.

32. Nefian A. V., Liang L., Pi X., Liu X., Murphye K. Dynamic Bayesian Networks for Audio-visual Speech Recognition // EURASIP Journal on Advances in Signal Processing. 2002. N 11. P. 1–15.

33. Town C. Multi-sensory and Multi-modal Fusion for Sentient Computing // Intern. Journal of ComputerVision. 2007. Vol. 71. P. 235–253.

34. Tikhonov V.I. Optimal reception of signals. Москва : Radio and communications, 1983. 320 p.

35.Falkovich S. E., Khomyakov E. N. Statistical theory of measuring radio systems. Москва : Radio and communications, 1981. 288 p.

36. Ситнік О.В., Карташов В.М. Радіотехнічні системи : навч. посібник. Харків : Сміт, 2009. 448 с.

37. Shirman Y.D., Manzhos V.N. The theory and technique of processing radar information against the background of interference. Москва : Radio and communications, 1981. 416 p.

Поступила в редколлегию 02.10.2020

Сведения об авторах:

Карташов Владимир Михайлович – д-р техн. наук, профессор, Харьковский национальный университет радиоэлектроники, заведующий кафедрой медиаинженерии и информационных радиоэлектронных систем, Украина, e-mail: volodymyr.kartashov@nure.ua, ORCID: https://orcid.org/0000-0001-8335-5373

Олейников Владимир Николаевич – канд. техн. наук, доцент, Харьковский национальный университет радиоэлектроники, профессор кафедры медиаинженерии и информационных радиоэлектронных систем, Украина, e-mail: vladimir.oleinikov@nure.ua, ORCID: https://orcid.org/0000-0001-7197-9760

Рябуха Вячеслав Петрович – канд. техн. наук, доцент, Харьковский национальный университет радиоэлектроники, ведущий научный сотрудник ПНИЛ радиолокационных систем наблюдения, Украина, e-mail: viacheslav.riabukha@nure.ua, ORCID: https://orcid.org/0000-0002-8607-9551

Бабкин Станислав Иванович – канд. техн. наук, Харьковский национальный университет радиоэлектроники, старший научный сотрудник кафедры медиаинженерии и информационных радиоэлектронных систем, Украина, e-mail: prl.res@nure.ua, ORCID: https://orcid.org/0000-0003-4903-3551

Воронин Виталий Валериевич – канд. техн. наук, преподаватель радиотехнических дисциплин, Светловодский политехнический колледж Центральноукраинского национального технического университета, Украина, e-mail: vvvoronin2016@gmail.com, ORCID: https://orcid.org/0000-0002-4495-9024

Капуста Анастасія Ігорівна – Харьковский национальный университет радиоэлектроники, аспирант кафедры медиаинженерии и информационных радиоэлектронных систем, Украина, e-mail: anastasiia.kapusta@nure.ua, ORCID: https://orcid.org/0000-0003-2206-1552

Селезнёв Иван Сергеевич – Харьковский национальный университет радиоэлектроники, аспирант кафедры медиаинженерии и информационных радиоэлектронных систем, Украина, e-mail: ivan.seleznov@nure.ua, ORCID: https://orcid.org/0000-0002-0731-7540

ПРИСТРОЇ РАДІОТЕХНІКИ ТА ЗАСОБИ ТЕЛЕКОМУНІКАЦІЙ

УДК 621.375.4 **DOI:10.30837/rt.2020.3.202.20**

В.Г. КРИЖАНОВСЬКИЙ, д-р техн. наук

ФАЗОВІ ХАРАКТЕРИСТИКИ ПІДСИЛЮВАЧА КЛАСУ Е З РІЗНИМИ ВИХІДНИМИ ЛАНКАМИ

Вступ

Нині продовжує зростати інтерес до використання високоефективних підсилювачів потужності класу Е в системах бездротової передачі енергії та інформації, а також і до побудови на їх основі потужних автогенераторів [1 – 4]. Триває розробка нових конструкцій автогенераторів класу Е [5 – 8], що потребує детального вивчення фазових характеристик режиму класу Е. Навіть в найпростіших схемах підсилювачів і автогенераторів ВЧ класу Е на фазові характеристики впливають нелінійність ємностей транзистора, паразитні елементи схеми і варіація параметрів елементів схеми [3]. Питання залежності зсуву фази (від входу підсилювача до його виходу загалом) у схемах з ускладненою вихідною ланкою ще не розглядалося. У НВЧ підсилювачах слід враховувати додатковий зсув фаз на паразитних елементах транзистора і залежність зсуву фаз від вихідної потужності (амплітудно-фазова конверсія) [9].

Мета роботи – розрахунок і експериментальне вивчення залежності зсуву фази від частоти в каскаді ВЧ підсилювача класу Е в схемі з конденсатором, що шунтує, з метою використання отриманих залежностей для проектування автогенераторів класу Е і оцінки посилення сигналів з розвиненим спектром в таких підсилювачах.

Цікавим є питання зміни зсуву фаз в пристроях класів E/F та інших, в яких формування напруги на стоці відбувається за участю іншого амплітудно-фазового розподілу вищих гармонік сигналу, наприклад автогенератори E/F_3 і інші [5, 7, 10]. Також треба розглянути зсув фаз в субоптимальному режимі класу Е, з урахуванням впливу антипаралельного діоду, який присутній в структурі потужних МОН транзисторів, оскільки такий режим роботи з'являється при зміні частоти в підсилювачах і автогенераторах [11 – 13].

В роботі [3] проаналізований зсув фаз в схемі потужного автогенератора класу Е, але розгляд виконаний тільки на одній частоті і для оптимального режиму настройки вихідної узгоджувальної ланки, тому для зсуву фаз на транзисторі використовується тільки одне значення.

Розрахунок зсуву фаз на ключі

Оскільки ми розглядаємо випадок зміни робочої частоти підсилювача класу Е, то вимагати виконання умов класу Е – нульового значення напруги і нульову похідну напруги в кінці періоду «Вимк» – неможна. Тому розрахунок форми напруги на ключі треба вести без цієї умови. Разом з тим висока добротність вихідної ланки дозволяє, як і раніше, вважати струм у навантаженні синусоїдальним.

На рис. 1 показана еквівалентна схема підсилювача класу Е, в якій у припущенні високої добротності навантажувальної ланки змінний струм у навантаженні на основній частоті можна представити генератором струму I_R. Зважаючи на велику індуктивність дроселя у колі стоку струм живлення буде постійним і відповідатиме генератору струму I_0.

Відповідно до рис. 1 [11, 12],

$$i_S + i_C = I_0 + i_R = I_0 + I_m \sin(\omega t + \phi).$$

Для інтервалу $0 < \omega t \le \pi$, ключ замкнений, і тому $i_C = 0$. Відповідно струм через ключ набуде вигляду

$$i_S = \begin{cases} I_0 + I_m \sin\left(\omega t + \phi\right), & \text{for } 0 < \omega t \le \pi, \\ 0, & \text{for } \pi < \omega t \le 2\pi \end{cases}$$

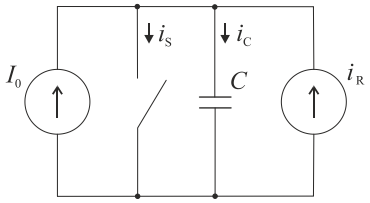


Рис. 1

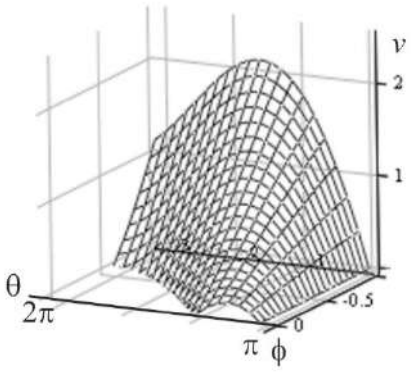


Рис. 2

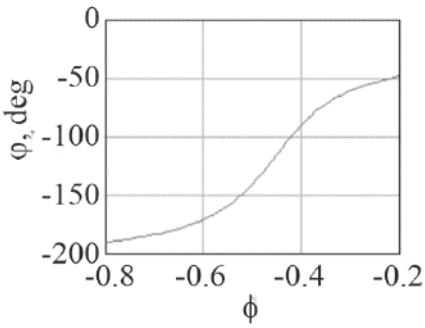


Рис. 3

На інтервалі $\pi < \omega t \le 2\pi$ ключ розімкнений, що дає $i_S = 0$. Отже, струм через ємність, що шунтує, *C* буде

$$i_C = \begin{cases} 0 & , \text{for} \, 0 < \omega t \le \pi, \\ I_I + I_m \sin\left(\omega t + \phi\right), & \text{for} \, \pi < \omega t \le 2\pi \end{cases}$$

Напруга на ключі та ємності *C* буде дорівнювати, позначаючи $\theta = \omega t$:

$$v_S = \frac{1}{\omega C}\int_{\pi}^{\theta} i_C d\theta = \frac{1}{\omega C}\int_{\pi}^{\theta}\left[I_0 + I_m \sin\left(\theta + \phi\right)\right]d\theta =$$

$$= \begin{cases} 0, & \text{for } 0 < \theta \le \pi \\ \dfrac{1}{\omega C}\left\{I_0\left(\theta - \pi\right) + I_m\left[\cos\left(\theta + \phi\right) + \cos\phi\right]\right\}, & \text{for } \pi < \theta \le 2\pi \end{cases} \quad (1)$$

Знайдемо Фур'є компоненти першої гармоніки:

$$A_1 = \frac{1}{\pi}\int_{\pi}^{2\pi} v(\omega t)\cos(\omega t)d(\omega t) \;\; ; \quad B_1 = \frac{1}{\pi}\int_{\pi}^{2\pi} v(\omega t)\sin(\omega t)d(\omega t).$$

І визначимо фазу

$$\varphi_1 = \arctan\left(B_1/A_1\right). \quad (2)$$

Виконуючи перетворення, отримаємо

$$\varphi_1 = \arctan\left(\frac{4I_m\cos\left(\phi\right) - 2\pi I_0 + \pi I_m \sin\left(\phi\right)}{4I_0 - \pi I_m \cos\left(\phi\right)}\right) \quad (3)$$

Видно, що фаза першої гармоніки залежить від кута ϕ і амплітуд струмів I_m і I_0. Для номінального режиму між ними існує зв'язок $I_0 = -I_m \sin\left(\phi\right)$, і при виконанні умов класу Е кут $\phi = \phi_0 = \arctan(-2/\pi) = -32.48°$ [11]. Тоді вираз (3) спроститься:

$$\varphi_1 = \arctan\left(\frac{4\cos\left(\phi\right) + 3\pi\sin\left(\phi\right)}{4\sin\left(\phi\right) + \pi\cos\left(\phi\right)}\right), \quad (4)$$

Арктангенс треба обчислювати з урахуванням знаку (функції atan2(x,y) або $\arg(x + jy)$ для обчислення кута). Тоді отримаємо значення $\varphi_1 = 4.423$ рад або $\varphi_1 = 253.42°$. У той же час відоме значення зсуву фаз для цього випадку 196,6 ° або -163.4° (знак може змінюватися у залежності від напрямку відліку фаз). Відомо, що ряд Фур'є можна записати двома способа-

ми – через формулу косинуса різниці або синус суми аргументів, обидва способи рівноправні, але фаза гармоніки буде в першому випадку записуватися через $\arctan(A_1/B_1)$, на відміну від формули (2). При цьому треба враховувати співвідношення $\arctan(x)+\arctan\left(\frac{1}{x}\right)=\begin{cases}\pi/2 \text{ if } x>0\\ -\pi/2 \text{ if } x<0\end{cases}$. Із урахуванням квадранта значення фази

$$\varphi_1=\arctan\left(\frac{4\sin(\phi_0)+\pi\cos\phi_0}{4\cos(\phi_0)+3\pi\sin(\phi_0)}\right)+\pi=163.4(^\circ). \qquad (5)$$

Отриманий фізично точний результат в точці оптимальної роботи підсилювача класу Е дозволяє оцінити зміну фази першої гармоніки напруги на ключі (ємності C) у залежності від початкової фази струму у вихідній ланці. Оскільки залежність (5) для фази отримана за умови виконання умов перемикання при нульовій напрузі на ключі, а кут φ_0 при нульовій похідній напруги [11], то форми напруги на ключі в залежності від ϕ можна отримати з (1).

Форма напруги на ключі у залежності від зміни параметрів в (1) показана на рис. 2, залежність напруги від фази θ (безрозмірного часу) – це перетин показаної поверхні при заданому ϕ. Якщо побудувати графік фази напруги за формулою (5) (рис. 3), то можна побачити, що поблизу точки $\phi_0=-32.48^\circ$ залежність відповідає фізиці процесу. Практично цікава частотна залежність зсуву фаз між затвором і стоком транзистора, але проведений розгляд не дає можливості її розрахувати, а вказує лише на простий факт, що фаза першої гармоніки залежить від форми імпульсу напруги на ключі в стані «Вимк». Природно, що залежності в реальній схемі будуть складнішими, тому розглянемо дві схеми вихідних ланок підсилювачів класу Е з ємністю, що шунтує, (рис. 4 і 5). На рис. 4 показана класична ланка з послідовним резонансним контуром, на основі якої побудовані автогенератори [3, 4], а на рис. 5 – ланка з дворазовим виконанням умов класу Е в смузі частот, яка використовується в автогенераторах [8].

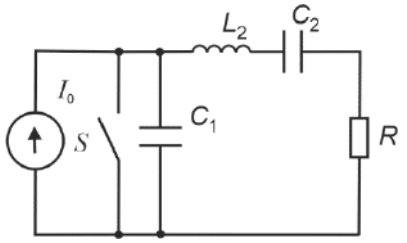


Рис. 4

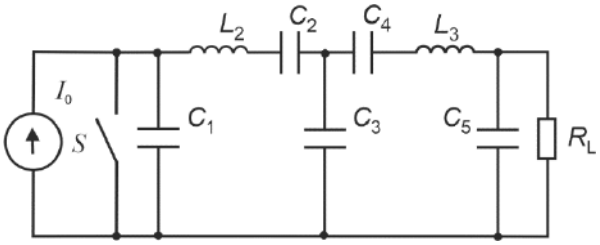
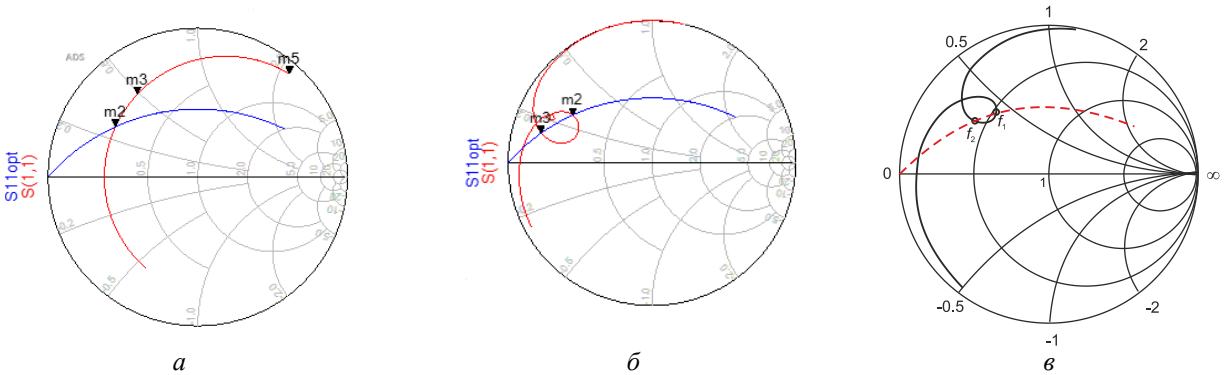


Рис. 5

Схеми відрізняються годографом навантажувального імпедансу, на рис. 6, *а* показана залежність вхідного імпедансу праворуч від ємності для класичної схеми (рис. 4), на рис. 6, *б* для схеми з «петлею» (рис. 5), на рис. 6, *в* представлений годограф експериментального макета. Лінія $S11\text{opt}$ показує значення навантажувального імпедансу, при якому забезпечується виконання умов класу Е [1, 8]. Частотні мітки відповідають $m2$ = 4,48 МГц, $m3$ = 4,98 МГц, $f_1=4.7$ МГц, $f_2=5.05$ МГц. Видно, що годограф рис. 6, *б* формально забезпечує умови роботи підсилювача класу Е на двох частотах, не враховуючи того факту, що ємність повинна мати різні значення на різних частотах [11 – 13]. Для створення автогенератора класу Е важливо знати, як на цих частотах зміниться зсув фази на транзисторі. Також величина цього зсуву фаз цікава для роботи підсилювача класу Е при посиленні сигналу зі змінною частотою (розширеним спектром), наприклад BPSK сигналу. Елементи схем підсилювачів зведені у таблицю:

Схема рис. 4	C_1 = 307 pF	L_2 = 2.07 uH	C_2 = 819 pF	R = 12 Ohm
Схема рис. 5	C_1 = 307 pF	L_2 = 1.25 uH	C_2 = 2.68 nF	C_3 = 3 nF
	L_3 = 2.18 uH	C_4 = 987 pH	C_5 = 1.5 nF	R_L = 50 Ohm

Роботу підсилювачів розглянемо за допомогою методу гармонічного балансу, що дозволяє аналізувати нелінійні кола і знаходити амплітуди і фази сигналів в різних точках схеми.



а *б* *в*

Рис. 6

Для врахування впливу антипаралельного діоду, який вбудований в МОН транзистор, схеми рис. 4 і 5 були змінені як показано на рис. 7. Форми напруги на ключі, які отримані при моделюванні на зазначених частотах, показані на рис. 8 для класичної ланки (*а*) і на двох частотах для схеми рис. 8 (*b* і *c*). Відрізки синусоїди показують моменти перемикання ключа (вхідний сигнал) для кожної форми напруги на ключі. Якщо асоціювати фазу першої гармоніки напруги на ключі (стоці транзистора) з «центром мас» умовної фігури, обмеженою формою напруги і віссю абсцис, то видно, що між фазами для випадків *a*, *b* і *c* будуть помітні відмінності.

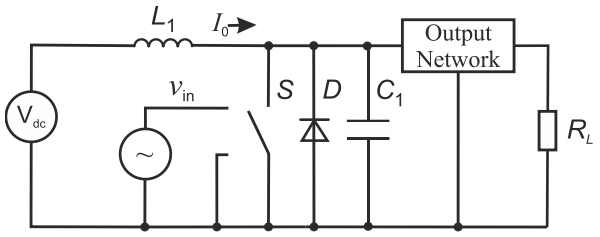


Рис. 7

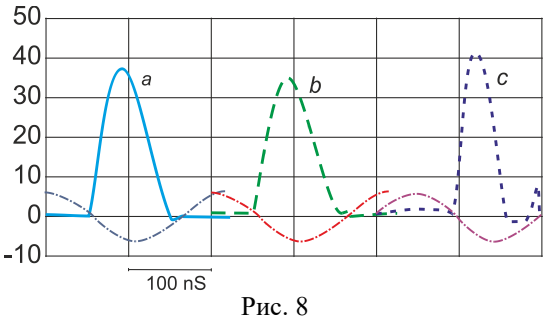


Рис. 8

На рис. 9 показані залежності зсуву фази на ділянці вхід-вихід ключа для схеми з годографом навантажувального імпедансу, відповідним рис. 6, *б* (крива 1). Для експериментального визначення зсуву фаз використовувався наступний метод. Записувалися форми напруги на затворі і стоці підсилювача класу Е, при навантажувальному імпедансі на рис. 6, *в*. Приклади форм напруги, записаних за допомогою цифрового осцилографа, показані на рис. 10. Потім за цими формами за допомогою швидкого перетворення Фур'є обчислювалися фази першої гармоніки вхідної та вихідної напруги. Фактично ця методика використовується в методі гармонічного балансу. Експериментальний зсув фаз показаний на рис. 9, крива 2. Зсув мінімуму кривої можна пов'язати зі зміною імпедансів в експериментальному макеті (рис. 6, *в*), але відмінність за абсолютними значеннями склала близько 30 градусів. Для пояснення цього факту проведемо моделювання підсилювача на ключі з урахуванням вхідної та перехідної ємностей (ємності Міллера), рис. 11. У схемі на рис. 11 також враховано вихідний опір генератора вхідного сигналу (вхідній узгоджувальній ланки). Отриманий графік представлений кривою 3. Видно, що результат більше схожий на експериментальний. Облік точних значень елементів, нелінійності ємностей має ще більше наблизити результати розрахунку до експерименту, але це не входило у мету роботи. Для порівняння кривими 4 (моделювання) та 5 (експеримент) показано залежності зсуву фази на ключі для класичної навантажувальної ланки. Аналіз залежностей дозволяє зробити висновок, що хід зсуву фаз на ключі в значній

мірі визначається фазовим кутом навантажувального імпедансу вихідної узгоджувальної ланки. Наявність «петлі» на годографі імпедансу, при якій фаза має локальні екстремуми, приводить до появи локальних екстремумів на залежності зсуву фаз на ключі. Це зрозуміло, бо фазовий кут навантаження практично визначає фазу струму ϕ у рівнянні (4).

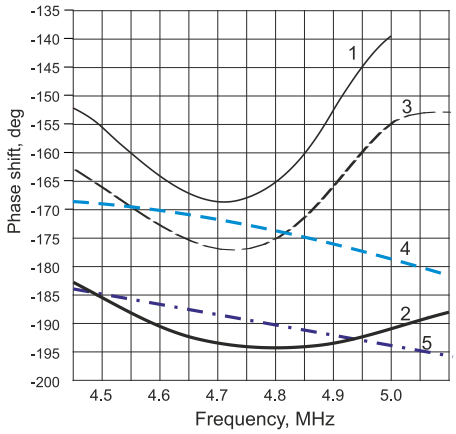


Рис. 9

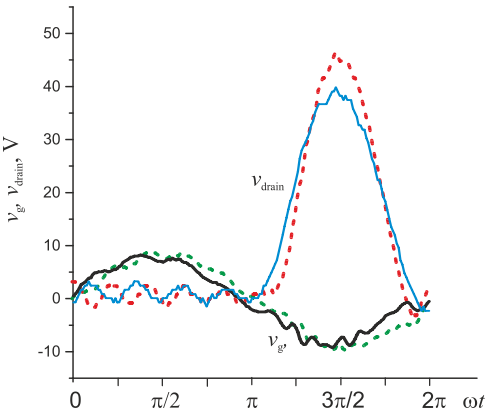


Рис. 10

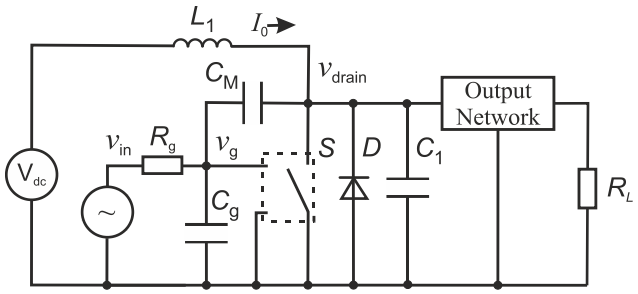


Рис. 11

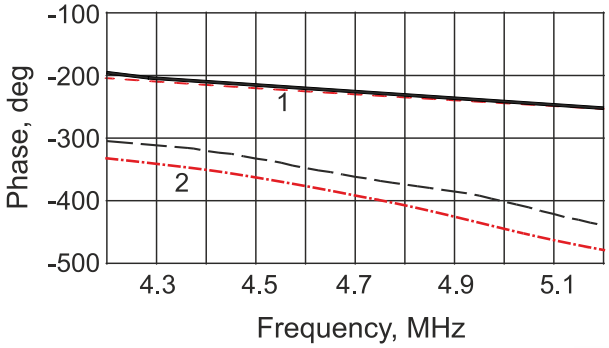


Рис. 12

Зсув фаз для підсилювача цілком, від затвора транзистору до опору навантаження показаний на рис. 12: цифра 1 відповідає підсилювачу з класичною ланкою, 2 – підсилювачу з розвиненою вихідною ланкою, верхні лінії в групі – теорія, нижні – експеримент. Зазначимо, що на цих кривих спостерігається монотонна залежність фази від частоти, що пов'язано зі значно більшою швидкістю зміни фази від частоти у навантажувальній ланці. І це ж пояснює близькість теорії і експерименту, оскільки моделювати пасивну ланку можна досить точно.

Вивчення фазових характеристик класу Е раніше проводилося для вивчення впливу нелінійностей і режиму роботи [14, 15], так само як і вивчення зсуву фаз у польових транзисторах [16]. Однак залежностей, схожих із залежностями на рис. 9, раніше не було отримано. У деяких роботах вимірювався зсув фаз у підсилювачі класу Е, але фаза визначалася за моментом перетину напруги з нулем, що не у всіх випадках справедливо. У даній роботі вивчена залежність зсуву фаз на ключі при зміні частоти в схемі з дворазовим виконанням умов класу Е. Важливою обставиною, що витікає з результату дослідження, є можливість отримання однакового зсуву фаз на різних частотах, що може спростити побудову автогенератора класу Е зі змінною частотою у широкому діапазоні частот. Знаючи залежність зсуву фаз на ключовому елементі, можна поставити задачу оптимізації конструкції двочастотного автогенератора класу Е [17] та розробити нові конструкції автогенераторів, схожих на [2, 3, 17], і побудувати для них метод проектування, аналогічний [18].

Висновки

Теоретично промодельована і експериментально виміряна залежність зсуву фаз від частоти між входом і виходом ключового активного елементу в підсилювачі класу Е з різними

навантажувальними ланками, з одноразовим і дворазовим виконанням умов на імпеданс навантажувальної ланки.

Список літератури:

1. Крижановський В.Г., Макаров Д. Г., Чернов Д. В., Крижановський В. В. Автогенератори класу Е. ; за ред. В. Г. Крижановського / ДонНУ імені Василя Стуса. Вінниця : Нілан-ЛТД, 2017. 220 с.
2. Laskovski A. N., Yuce M. R. Class-E Oscillators as Wireless Power Transmitters for Biomedical Implants // 3rd Int. Symp. on Applied Sciences in Biomedical and Communication Technologies (ISABEL), 2010 Rome, 7-10 Nov. 2010. P. 1-5.
3. Ahmadi M. M., Salehi-Sirzar M. A Self-Tuned Class-E Power Oscillator // IEEE Transactions on Power Electronics. Vol. 34, Issue 5, May 2019, Page(s): 4434 – 4449.
4. Mikołajewski M. A self-oscillating h.f. power generator with a Class E resonant amplifier // Bulletin of The Polish Academy of Sciences Technical Sciences. 2013. V. 61, № 2. P. 527- 534
5. Apperley T., Nielsen J., Okoniewski M. A Class E/Fodd Power Oscillator Incorporating a Distributed Active Transformer // IEEE Transactions on Microwave Theory and Techniques. Vol. 68, No. 6, June 2020. P. 2409-2418.
6. Ahmadi M. M. and Pezeshkpour S. A Self-Starting Class-E Power Oscillator with an Inverting Gate Driver // IEEE Transactions on Industrial Electronics, doi: 10.1109/TIE.2019.2949533.
7. Inaba T., Koizumi H., Class E/F3 Tuned Power Oscillator // IEEE Transactions on Power Electronics. 2018; Vol. 33, No. 2. pp. 1420-1427.
8. Kryzhanovskyi V. G. Class-E Self-Excited Oscillator with Expanded Tuning Bandwidth // Telecommunications and Radio Engineering. Vol. 73, 2014 Issue 15. P. 1387-1395.
9. Krizhanovskii V.G., Printsovskii V.A. Class-E microwave Oscillator // Radioelectronics and Communication Systems. 2006. Vol. 49, No. 11, pp. 30-35.
10. Krizhanovski V.G., Chernov D.V., Grebennikov Andrei Low-Voltage Class E/F_3 High Frequency Oscillator // 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering. Lviv-Slavske, Ukraine 2018. P: 607 – 611.
11. Grebennikov A., Sokal N. O. and M. J. Franco. Switchmode RF and Microwave Power Amplifiers, 2nd ed. Orlando, FL, USA: Academic, 2012, 667 p.
12. Kazimierczuk M. K. RF Power Amplifiers. 2nd ed. 2015 John Wiley & Sons Ltd. 686 p.
13. Raab F. H. Suboptimum operation of class-E RF power amplifiers // Proc. RF Technology Expo '89, Santa Clara, CA, pp. 85 – 98, Feb. 14 – 16, 1989.
14. Hayati M., Abbasi H., Kazimierczuk M. K. Sekiya, H. Analysis and Study of the Duty Ratio Effects on the Class-EM Power Amplifier Including MOSFET Nonlinear Gate-to-Drain and Drain-to-Source Capacitances // IEEE Transactions on Power Electronics, 1-1. doi:10.1109/tpel.2018.2810218.
15. Nagashima T., Wei X., Tanaka H.-A., Sekiya H. Locking Range Derivations for Injection-Locked Class-E Oscillator Applying Phase Reduction Theory // IEEE Trans. on Circuits and Systems-I: Regular Papers, Vol. 61, No. 10, Oct. 2014, p. 2904-2911.
16. Ishizaki T., Ikeda H., Yoshikawa Y., Uwano T. Analysis of phase characteristics of a GaAs FET power amplifier for digital cellular portable telephones // Electronics and Communications in Japan (Part II: Electronics). V.77, No. 4, April 1994. P. 1-9.
17. Krizhanovski V., Krizhanovski V., Grebennikov A. Class E oscillator with two switchable frequencies // 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET – 2020). Lviv-Slavske, Ukraine, February 25 – 29, 2020.
18. Kazimierczuk M. K., Krizhanovski V. G., Rassokhina Ju. V., Chernov D. V., Class-E MOSFET Tuned Power Oscillator Design Procedure // IEEE Trans. On Circuits and Systems I. Regular Papers. V. 52, No. 6. June 2005.P.1138-1147.

Надійшла до редколегії 06.09.2020

Відомості про авторів:

Крижановський Володимир Григорович – д-р техн. наук, Донецький національний університет імені Василя Стуса, проф. кафедри радіофізики та кібербезпеки, Україна, e-mail: v.krizhanovski@donnu.edu.ua ORCID: https://orcid.org/0000-0002-2685-9740

УДК 53.082.52 **DOI:10.30837/rt.2020.3.202.21**

А.Н. АНДРЕЕВ, канд. физ.-мат. наук, О.Н. АНДРЕЕВА, канд. физ.-мат. наук

ИССЛЕДОВАНИЕ ИНЕРЦИОННЫХ ХАРАКТЕРИСТИК ФОТОРЕЗИСТОРОВ В ФИЗИЧЕСКОМ ПРАКТИКУМЕ

Введение

Полупроводниковые фоторезисторы находят широкое применение в различных устройствах фотопреобразователей [1 – 4], особенно там, где необходим широкий диапазон спектральной чувствительности и/или значительная мощность рассеивания. Одной из основных характеристик, влияющей на инерционность и фоточувствительность фоторезисторов, является среднее время жизни неравновесных носителей заряда, возникающих под действием света. Определение данного параметра в требуемом диапазоне освещенностей для каждого конкретного фоторезистора необходимо при регистрации переменных световых потоков [5 – 7].

С точки зрения фундаментальной науки, экспериментальное изучение фотопроводимости позволяет студентам инженерных специальностей понять основы зонной теории и физические процессы, возникающие при взаимодействии электромагнитного излучения с полупроводником [8 – 10]. Традиционно, для исследования фотопроводимости используется осциллограф и модулированный по амплитуде световой поток, что не позволяет автоматизировать процесс измерения и требует дополнительных габаритных элементов для формирования переменного светового потока (генераторы или прерыватели). Поэтому создание современной компактной автоматизированной установки для индивидуального изучения явления фотопроводимости в физическом практикуме является актуальным.

Краткая теория фотопроводимости

При освещении собственного полупроводника фотонами с энергией не меньше ширины запрещенной зоны (или энергией ионизации примесных атомов для примесного полупроводника), его электропроводность возрастает:

$$\sigma = \sigma_0 + \Delta\sigma = e\left(n_0\mu_n + p_0\mu_p\right) + e\left(\Delta n\mu_n + \Delta p\mu_p\right), \quad (1)$$

где σ_0 – электрическая проводимость полупроводника при отсутствии освещенности (темновая электропроводность), определяется равновесной концентрацией электронов (n_0) и дырок (p_0) при данной температуре и их подвижностью μ_n, μ_p; $\Delta\sigma$ – фотопроводимость, обусловленная генерацией неравновесных носителей концентрацией Δn, Δp под действием света; e – заряд электрона.

Если интенсивность падающего излучения невелика, то концентрация неравновесных носителей заряда значительно меньше концентрации равновесных зарядов в полупроводнике $\left(\Delta n, \Delta p << n_0, p_0\right)$. Изменение Δn в единицу времени при освещении определяется разностью скоростей генерации и рекомбинацией неравновесных носителей. Скорость генерации избыточных носителей пропорциональна числу фотонов N, падающих на полупроводник за одну секунду:

$$G = \alpha\beta N = \alpha\beta\frac{JS}{h\nu}, \quad (2)$$

где α – коэффициент поглощения света; β – квантовый выход; J – интенсивность света;

v – частота света; h – постоянная Планка; S – площадь освещаемой поверхности полупроводника.

Скорость рекомбинации при низкой освещенности пропорциональна концентрации избыточных зарядов (линейная рекомбинация):

$$R = \frac{\Delta n}{\tau}, \tag{3}$$

где Δn – концентрация неравновесных носителей; τ – время жизни неравновесных носителей.

Таким образом, скорость изменения концентрации неравновесных носителей, с учетом соотношений (2) и (3), при отсутствии электрического тока будет:

$$\frac{d(\Delta n)}{dt} = G - \frac{\Delta n}{\tau}. \tag{4}$$

Решая уравнение (4) для нулевых начальных условий $(\Delta n(0) = 0)$, получаем:

$$\Delta n = G\tau\left(1 - e^{-\frac{t}{\tau}}\right) = \Delta n_0\left(1 - e^{-\frac{t}{\tau}}\right), \tag{5}$$

где t – время после начала освещения; $\Delta n_0 = G\tau$ – стационарное значение концентрации избыточных носителей заряда (при $t \to \infty$).

При выключении источника света генерация неравновесных носителей прекращается $(G = 0)$. Принимая во внимание начальные условия $\Delta n(0) = \Delta n_0$, находим частное решение уравнения (4):

$$\Delta n = \Delta n_0 e^{-\frac{t}{\tau}}. \tag{6}$$

Из (5) и (6) следует, что при низком уровне освещенности полупроводника $(\sigma_0 >> \Delta\sigma)$ нарастание и спад фотопроводимости определяется средним временем жизни неравновесных носителей.

Если темновое сопротивление полупроводника большое и/или интенсивность падающего излучения велика, то концентрация неравновесных носителей окажется значительно больше, чем равновесных $(\Delta n, \Delta p >> n, p)$. В этом случае рекомбинация происходит по квадратичному закону:

$$R = \gamma\Delta n^2, \tag{7}$$

где γ – коэффициент, характеризующий вероятность рекомбинации.

Решая уравнения (4) для квадратичной рекомбинации с учетом начальных условий, получим изменение концентрации неравновесных носителей:

при освещении:

$$\Delta n = \sqrt{\frac{G}{\gamma}}th\left(\sqrt{G\gamma}t\right) = \Delta n_0 th\left(\gamma\Delta n_0 t\right) = \Delta n_0 th\left(\frac{t}{\tau}\right), \tag{8}$$

при затемнении:

$$\Delta n = \frac{\sqrt{G\gamma^{-1}}}{1 + \sqrt{G\gamma}t} = \frac{\Delta n_0}{1 + t\gamma\Delta n_0} = \frac{\Delta n_0}{1 + \frac{t}{\tau}}. \tag{9}$$

При $\Delta\sigma >> \sigma_0$ нарастание и спад Δn происходят по разным законам (гиперболический тангенс и гипербола), поэтому время нарастания и спада фотопроводимости различно. Кроме

того, среднее время жизни $\left(\tau = \left(\gamma \Delta n_0\right)^{-1}\right)$ неравновесных носителей зависит от интенсивности падающего света.

Из соотношений (5) и (8), видно, что при линейной рекомбинации стационарная концентрация неравновесных носителей является линейной функцией интенсивности: $\Delta n_0 = \tau \alpha \beta JS$, а при квадратичной нелинейной – $\Delta n_0 = \sqrt{\alpha \beta \gamma^{-1} JS}$.

Экспериментальная установка

Для исследования инерционных характеристик фоторезисторов была разработана и изготовлена лабораторная установка на базе 32-разрядного микроконтроллера STM32F103VET6 (рис.1).

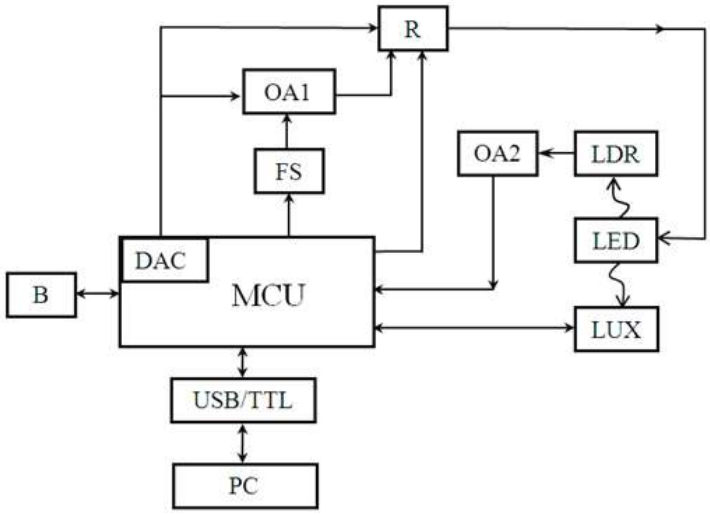


Рис. 1. Функциональная схема установки

Исследуемый фоторезистор (LDR) соединяется последовательно с сопротивлением нагрузки и источником постоянного напряжения. Сигнал, совпадающий по форме с фототоком, снимается с нагрузочного сопротивления и поступает на вход быстродействующего операционного усилителя (OA2) с регулируемым коэффициентом усиления. Регулировка коэффициента усиления OA2 выполняется микроконтроллером (MCU) путем переключения резистора в цепи обратной связи при помощи аналогового мультиплексора (на схеме не указан). Выходное напряжение усилителя оцифровывается встроенным 12-битным аналого-цифровым преобразователем (АЦП) микроконтроллера, и полученные значения сохраняются в оперативной памяти микроконтроллера. Оцифрованные значения сигнала сохраняются в оперативной памяти микроконтроллера и затем через USB-UART преобразователь передаются на персональный компьютер (PC).

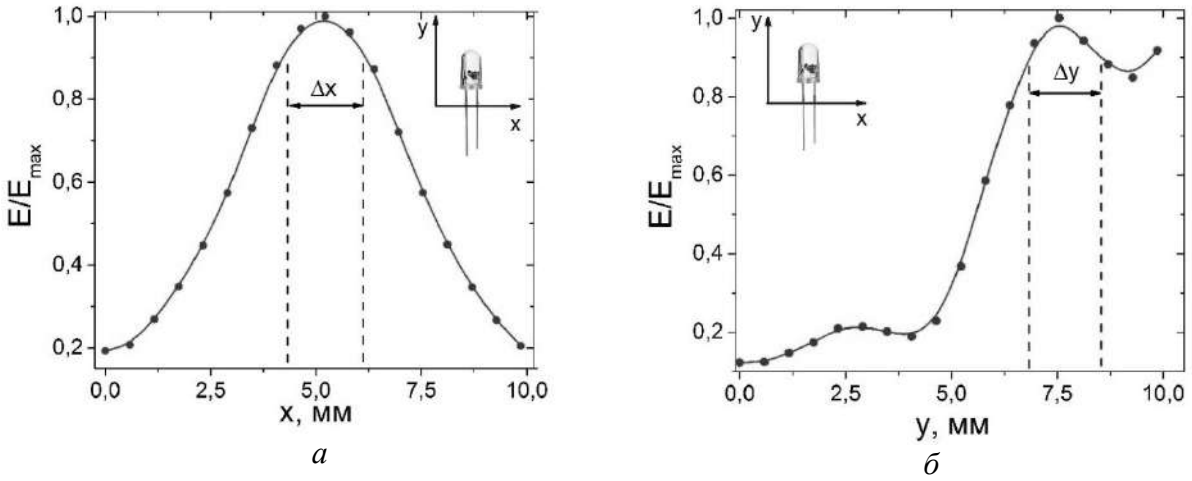
Для освещения фоторезистора в установке используется светодиод (LED) с цветовой температурой 2850 – 3000 К, на анод которого подается постоянное или переменное напряжение. Включение светодиода происходит в момент подачи с микроконтроллера цифрового сигнала низкого уровня на катод светодиода. Выбор источника питания светодиода осуществляется микроконтроллером путем переключения электромагнитного реле (R). Постоянное напряжение через буферный усилитель (на схеме не указан) поступает со встроенного 12-битного цифро-аналогового преобразователя (ЦАП) микроконтроллера (DAC). Переменное синусоидальное напряжение формируется синтезатором частоты (FS) на базе микросхемы AD9833 и инвертирующим усилителем с регулируемым коэффициентом усиления (OA1). Усиление может изменяться как дискретно (аналоговый мультиплексор и набор резисторов), так и плавно (цифровой потенциометр). Смещение гармонического сигнала осуществляется вторым встроенным ЦАП микроконтроллера. Измерение освещенности фоторезистора осуществляется цифровым датчиком освещенности BH1750 (LUX), который «общается» с микроконтроллером по шине I^2C.

Для сопряжения лабораторной установки со смартфоном используется блютуз модуль (B), подключенный к последовательному порту (UART) микроконтроллера. Это дает возможность проводить измерения в автономном режиме (без компьютера). Также на печатной плате установки находится разъем для подключения к микроконтроллеру Wi-Fi модуля на базе микроконтроллера ESP8266 для дистанционного режима измерений.

Измерительная установка может работать в следующих режимах: 1) определение люкс-амперной характеристики фоторезистора; 2) исследование нарастания и спада фототока при разных уровнях освещенности; 3) измерение частотной характеристики фоторезистора.

Результаты и их обсуждение

В установке светодиод одновременно освещает фоторезистор и цифровой датчик BH1750, расположенные с противоположных сторон от светодиода, но на одинаковом расстоянии от него. Поскольку размеры рабочей поверхности цифрового датчика значительно меньше освещаемой поверхности фоторезистора, то, первоначально, были проведены измерения освещенности в области предполагаемого размещения фоторезистора. Датчик BH1750 закреплен на подложке, которая перемещалась шаговым двигателем перпендикулярно (рис. 2, *а*) и параллельно (рис. 2, *б*) электродам светодиода (фоторезистора). В результате, вблизи максимума освещенности были установлены пространственные границы (Δx, Δy), в которых отклонение освещенности от среднего значения не превышает 5 %.



а *б*

Рис. 2. Исследование диаграммы направленности светодиода: *а* - зависимость относительной освещенности при перемещении поперек электродов светодиода; *б* - зависимость относительной освещенности при перемещении вдоль электродов светодиода

Поскольку спектральные характеристики фоторезистора и датчика освещенности похожи, а диаграмма направленности светодиода симметрична относительно прямой соединяющей, фоторезистор и BH1750, то отличие освещенности фоторезистора от значений, измеренных датчиком, не превысит 5 % при ограничении рабочей поверхности фоторезистора, путем размещения специально изготовленной круглой диафрагмы диаметром 1,8 мм, которая фиксировалась вблизи его поверхности.

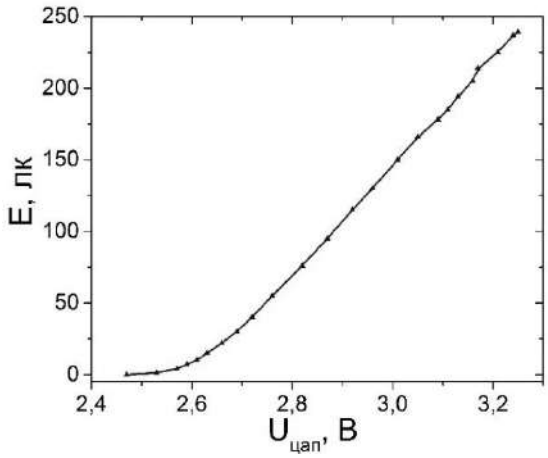


Рис. 3. Зависимость освещенности фоторезистора от напряжения питания светодиода

Уровень освещения фоторезистора определяется напряжением питания светодиода (рис. 3), которое поступает с ЦАП микроконтроллера с шагом 0,8 мВ, что позволяет плавно изменять уровень освещенности исследуемого фоторезистора и исследовать его люкс-амперную характеристику (рис. 4). Значение освещенности и число точек усреднения (фототока и освещенности) задаются в программе управления установкой в

режиме измерения люкс-амперной характеристики. Из рис. 4 видно, что люкс-амперная характеристика фоторезистора при освещенности более 10 лк становится нелинейной, что говорит о квадратичном законе рекомбинации избыточных носителей.

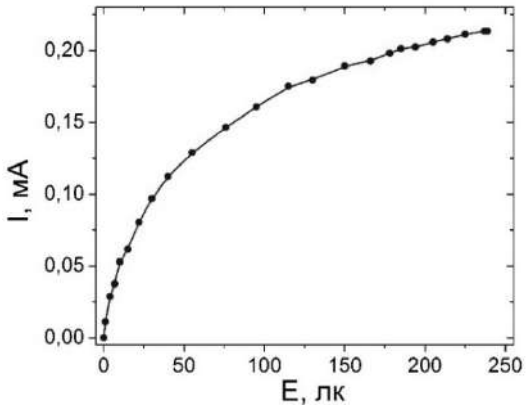


Рис. 4. Люкс-амперная характеристика фоторезистора

Фототок I на рис.4 представляет собой разность токов при освещении и затемнении фоторезистора. Применяя закон Ома в дифференциальной форме, а также учитывая соотношение (1) и однородность электрического поля, получим:

$$I = e\Delta n\left(\mu_n + \mu_p\right)\frac{U}{L}S, \qquad (10)$$

где S, L – площадь поперечного сечения и длина полупроводника в направлении электрического поля соответственно; U – напряжение на фоторезисторе.

В установке сопротивление фоторезистора значительно больше сопротивления нагрузки во всем диапазоне измерений, поэтому U в процессе освещения изменяется незначительно. Это позволяет определить в программе обработки некоторые характеристики (k, δ) фоторезистора путем аппроксимации люкс-амперной характеристики функцией вида

$$I = kUE^{\delta}, \qquad (11)$$

где k – константа, зависящая от свойств материала; δ – коэффициент нелинейности; E – освещенность.

Основным режимом работы установки является изучение инерционных характеристик фоторезистора. В программе управления задаются значения: освещенности фоторезистора; коэффициента усиления усилителя; частоты дискретизации АЦП. В соответствующем окне программы на экране монитора выводится осциллограммы фототока (рис. 5) в момент освещения и затемнения фоторезистора (верхняя кривая) и при затемнении в логарифмическом масштабе (нижняя кривая). Если выполняется линейный закон рекомбинации, то нижний график на рис. 5 будет прямой линией. Длительность импульса питающего напряжения светодиода устанавливается такой, чтобы фототок достиг своего стационарного значения.

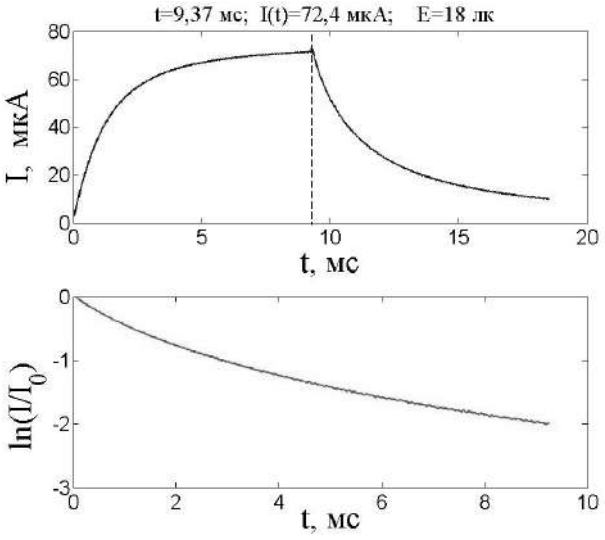


Рис. 5. Осциллограммы фототока

При квадратичной рекомбинации избыточных носителей, фототок согласно (8) и (9):

при освещении

$$I = e\Delta n_0\left(\mu_n + \mu_p\right)S\frac{U}{L}th\left(\gamma\Delta n_0 t\right) = I_0 th\left(\frac{t}{\tau}\right), \qquad (12)$$

при затемнении

$$I = I_0\left(1+\frac{t}{\tau}\right)^{-1}, \qquad (13)$$

где I_0 – установившееся значение фототока при данном уровне освещения фоторезистора.

При высокой инжекции время жизни неравновесных носителей является переменной величиной, зависящей от уровня освещенности фоторезистора и соответственно от концентрации избыточных носителей. Поэтому на практике пользуются понятием мгновенного времени жизни [8].

Выбирая на осциллограмме нарастания или спада фототока (рис. 5, *а*) с помощью вертикального маркера соответствующие точки, можно вычислить время жизни при данном уровне освещения фоторезистора, используя соотношения (12) и (13). Для уменьшения погрешности определения τ выполняется усреднение по десяти измерениям. Относительная погрешность измерений не превышает 2 %.

Если уменьшить уровень освещенности фоторезистора, то согласно (5) и (6) законы нарастания

$$I = I_0\left(1-e^{-\frac{t}{\tau}}\right), \tag{14}$$

и спада фототока

$$I = I_0 e^{-\frac{t}{\tau}}, \tag{15}$$

становятся экспоненциальными.

С помощью маркера на осциллограмме выбираются необходимые значения фототока, которые автоматически нормируются согласно выражениям (14) или (15), а затем логарифмируются.

Затем выполняется линейная аппроксимация (рис. 6) по методу наименьших квадратов. Котангенс угла наклона прямой к оси абсцисс равен времени жизни неравновесных носителей. Погрешность измерений не превышает 3 %.

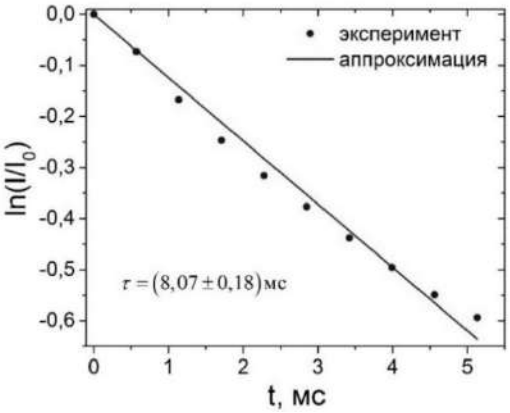


Рис. 6. Определение времени жизни неравновесных носителей заряда при затемнении фоторезистора

Третьим режимом работы установки является режим измерения частотной характеристики фоторезистора путем освещения его световым излучением синусоидальной формы. В этом случае для питания светодиода используется сигнал, формируемый синтезатором частоты и усилителем ОА1 (рис. 1). В программе управления задается глубина модуляции и частота светового сигнала, а также число точек усреднения при измерении фототока. На экран выводится осциллограмма фототока (рис. 7).

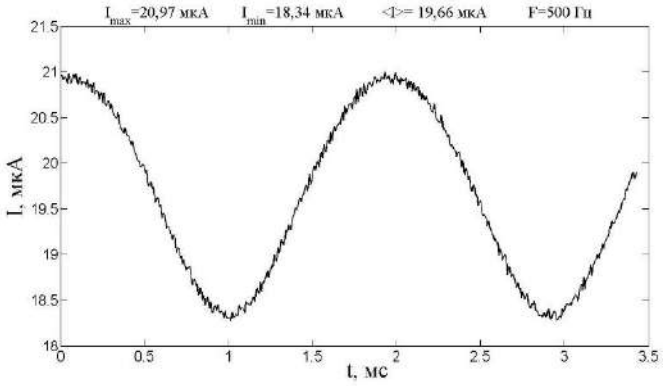


Рис. 7. Осциллограмма фототока при низком уровне освещенности

Если интенсивность падающего излучения изменяется по гармоническому закону $\left(J \sim \left(1+\cos\omega t\right)\right)$, то переменная составляющая фототока

$$I_{\sim} = \frac{I_{\max 0}}{\sqrt{1+\left(\omega\tau\right)^2}}\cos\left(\omega t-\phi\right), \tag{16}$$

где ω – циклическая частота падающего излучения; $\phi = arctg\left(\omega\tau\right)$ – разность фаз между фототоком и падающим световым потоком; $I_{\max 0}$ – амплитудное значение фототока при частоте, близкой к нулевой.

Из соотношения (16) следует, что амплитудное значение фототока зависит от произведения частоты модуляции светового потока на время жизни избыточных носителей. При воз-

растании частоты наблюдается уменьшение максимального значения переменной составляющей: $I_{max} = \frac{I_{max\,0}}{\sqrt{1+(\omega\tau)^2}}$. Частота, при которой амплитуда фототока уменьшается в $\sqrt{2}$ раз, называется частотой среза:

$$\omega_0 = \frac{1}{\tau}. \qquad (17)$$

Таким образом, измеряя экспериментально (рис.8) зависимость амплитуды переменной составляющей фототока от частоты падающего светового потока, можно не только исследовать отклик фоторезистора на переменный световой сигнал, но и определить время жизни избыточных носителей заряда по частоте среза.

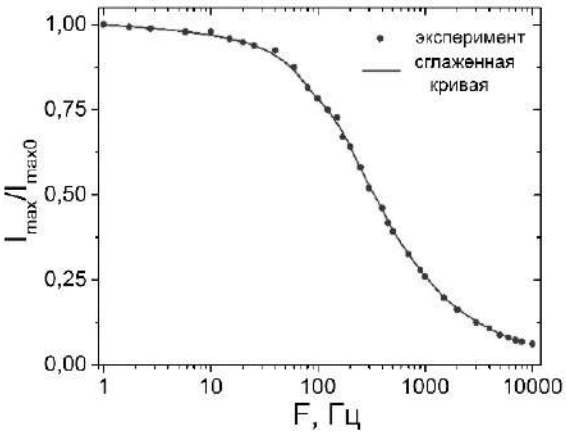


Рис. 8. Частотная характеристика фоторезистора

В заключение отметим, что фоторезистор и сопротивление нагрузки фиксируются на печатной плате измерительной установки с помощью винтовых клемм. Это позволяет, при необходимости, легко изменять их номиналы. Изменяя сопротивление нагрузки, можно исследовать зависимость времени нарастания и спада фототока от сопротивления нагрузки или реализовать согласованный режим работы, когда сопротивление нагрузки равно темновому сопротивлению фоторезистора.

Выводы

Разработана и протестирована компактная и низкобюджетная (себестоимость комплектующих 20 $) автоматизированная измерительная установка для исследования закономерностей фотопроводимости при разном уровне освещенности и не требующая применения цифрового осциллографа и генератора сигналов.

Список литературы:

1. Marinho F. Measuring light with light-dependent resistors: an easy approach for optics experiments / F. Marinho, C.M. Carvalho, F.R. Apolinário, L. Paulucci // European Journal of Physics. 2019. Vol.40, No.3.P. 035801–035814.
2. Jana A.K. An optical probe for liquid–liquid two-phase flows / A.K. Jana, T.K. Mandal, D.P. Chakrabarti, G. Das, P.K. Das // Measurement Science and Technology. 2007. Vol.18, No.5. P. 1563–1575.
3. Xiao-Yuan W. Implementation of an analogue model of a memristor based on a light-dependent resistor / W. Xiao-Yuan, A.L Fitch, H.H.C. Iu, V. Sreeram, W.G. Qi // Chinese Physics B. 2012. Vol. 21, No.10. P. 108501-1–108501-8.
4. Богданов Э.О. Фоторезисторы и их применение. Ленинград : Энергия, 1978. 144 с.
5. Sanga R. Design and development of a quasi-digital sensor and instrument for water turbidity measurement / R. Sanga, M. Sivaramakrishna, G.P. Rao // Measurement Science and Technology. 2019. Vol.30, No.11. P.115106.
6. Flores-Fuentes W. Comparison between Different Types of Sensors Used in the Real Operational Environment Based on Optical Scanning System / W. Flores-Fuentes, J.E. Miranda-Vega, M. Rivas-Lopez, O. Sergiyenko, J.C. Rodríguez-Quiñonez // Sensors. 2018. Vol.18, issue 6. P.1684–1689.
7. Yunianto M. Fiber optic sensor based on reflectivity configurations to detect heart rate / M. Yunianto, A. Marzuki, R. Riyatun, D. Lestari // Journal of Physics: Conference Series. 2016. Vol.776. P. 012110–012116.
8. Готра З.Ю. Фізичні основи електронної техніки / З.Ю. Готра, І.Є. Лопатинський, Б.А. Лукіянець та ін. Львів : Бескид Біт, 2004. 880 с.
9. Епифанов Г.И. Твердотельная электроника / Г.И. Епифанов, Ю.А. Мома. Москва : Высш. шк., 1986. 304 с.
10. Шалимова К.В. Физика полупроводников. Москва : Энергия, 1991. 416с.

Поступила в редколлегию 15.09.2020

Сведения об авторах:

Андреев Александр Николаевич – канд. физ.-мат. наук, Национальный технический университет «Харьковский Политехнический Институт», доцент кафедры физики, Украина, e-mail: andreievom@gmail.com

Андреева Ольга Николаевна – канд. физ.-мат. наук, Национальный технический университет «Харьковский Политехнический Институт», доцент кафедры физики, Украина, e-mail: Olga.Andreieva@khpi.edu.ua

ПЕРСПЕКТИВНІ МЕТОДИ ТА ЗАСОБИ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ
ПЕРСПЕКТИВНЫЕ МЕТОДЫ И СПОСОБЫ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ
PROSPECTIVE METHODS AND MEANS OF CRYPTOGRAPHIC TRANSFORMATIONS

УДК 004.056.55

Методи обчислення системних параметрів для електронного підпису «Crystals-Dilithium» 128, 256, 384 та 512 біт рівнів безпеки / *І.Д. Горбенко, А.М. Олексійчук, О.Г. Качко, Ю.І. Горбенко, М.В. Єсіна, С.О. Кандій* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 5 – 28.

На світовому рівні зусилля значного числа криптологів-теоретиків, математиків та криптологів-практиків зосереджені на відкритому конкурсі NIST PQC. Одним із основних завдань конкурсу є розробка та прийняття постквантового чи постквантових стандартів ЕП. Фіналістами другого етапу конкурсу NIST стали три механізми ЕП – CRYSTALS-DILITHIUM, Falcon та Rainbow. Окрім цього були визначені три альтернативні кандидати, які потребують більш детального дослідження. Всесторонній аналіз фіналістів є важливою задачею для криптологів світової криптоспільноти. Причому, безпека, тобто доведення криптографічної стійкості двох кандидатів-фіналістів на стандарт ЕП – CRYSTALS-DILITHIUM та Falcon, ґрунтується на проблемах з теорії та практики алгебраїчних решіток. Метод (схема) ЕП Dilithium ґрунтується на підході, що отримав назву "Fiat-Shamir з перериваннями". У статті розглядається сутність алгоритму ЕП CRYSTALS-DILITHIUM. Також проводиться детальний аналіз можливих атак на алгоритм та механізми їх реалізації. Розглядаються та аналізуються моделі порушника, загроз та безпеки. Надаються основні визначення щодо моделей безпеки ЕП. Описуються основні елементи конструкції механізму перспективного постквантового ЕП Dilithium в узагальненому вигляді. Наводяться загальні оцінки щодо рівня безпеки ЕП Dilithium. Приводиться обґрунтування та сутність моделей загроз, порушника та безпеки. Досліджується стійкість алгоритму ЕП Dilithium. Метою статті є обґрунтування моделі безпеки, класифікація, первинний аналіз та оцінка відомих атак на криптосистему ЕП CRYSTALS-DILITHIUM, встановлення обмежень та розробка практичних алгоритмів обчислення (генерації) загальносистемних параметрів для забезпечення 128, 256, 384 і 512 біт безпеки щодо класичного та 64, 128, 192 та 256 біт щодо квантового криптоаналізу.

Ключові слова: алгебраїчні решітки; атаки; безпека; загальносистемні параметри; модель безпеки; модель загроз; модель порушника; підпис; поліном; Dilithium.

Табл. 3. Іл. 1. Бібліогр.: 46 назв.

УДК 004.056.55

Методы вычисления системных параметров для электронной подписи «Crystals-Dilithium» 128, 256, 384 и 512 бит уровней безопасности / *И.Д. Горбенко, А.Н. Алексейчук, Е.Г. Качко, Ю.И. Горбенко, М.В. Есина, С.А. Кандий* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 5 – 28.

На мировом уровне усилия криптологов-теоретиков, математиков и криптологов-практиков сосредоточены на открытом конкурсе NIST PQC. Одной из основных задач конкурса является разработка и принятие постквантового или постквантовых стандартов ЭП. Финалистами второго этапа конкурса NIST стали три механизма ЭП – CRYSTALS-DILITHIUM, Falcon и Rainbow. Кроме этого были определены три альтернативных кандидата, которые требуют более детального исследования. Всесторонний анализ финалистов является важной задачей для криптологов мирового криптосообщества. Причем, безопасность, то есть доведение криптографической стойкости двух кандидатов-финалистов на стандарт ЭП – CRYSTALS-DILITHIUM и Falcon, основывается на проблемах по теории и практике алгебраических решеток. Метод (схема) ЭП Dilithium основывается на подходе, получившем название "Fiat-Shamir с прерываниями". В статье рассматривается суть алгоритма ЭП CRYSTALS-DILITHIUM. Также проводится детальный анализ возможных атак на алгоритм и механизмы их реализации. Даются основные определения относительно моделей безопасности ЭП. Описываются основные элементы конструкции механизма перспективного постквантового ЭП Dilithium в обобщенном виде. Приводятся общие оценки по уровню безопасности ЭП Dilithium. Приводится обоснование и сущность моделей угроз, нарушителя и безопасности. Исследуется стойкость алгоритма ЭП Dilithium. Цель статьи – обоснование модели безопасности, классификация, первичный анализ и оценка известных атак на криптосистему ЭП CRYSTALS-DILITHIUM, установление ограничений и разработка практических алгоритмов вычисления (генерации) общесистемных параметров для обеспечения 128, 256, 384 и 512 бит безопасности относительно классического и 64, 128, 192 и 256 бит относительно квантового криптоанализа.

Ключевые слова: алгебраические решетки; атаки; безопасность; общесистемные параметры; модель безопасности; модель угроз; модель нарушителя; подпись; полином; Dilithium.

Табл. 3. Ил. 1. Библиогр.: 46 назв.

UDC 004.056.55

Methods for calculating system parameters for electronic signature "Crystals-Dilithium" 128, 256, 384 and 512 bits of security levels / *I.D. Gorbenko, A.M. Aleksiychuk, O.G. Kachko, Yu.I. Gorbenko, M.V. Yesina, S.O. Kandiy* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 5 – 28.

Globally, the efforts of a significant number of crypto-theorists, mathematicians and cryptologists-practitioners are focused on the NIST PQC open competition. One of the main tasks of the competition consists in development and adoption of a post-quantum ES standard or standards. The finalists of the second stage of the NIST competition were three ES mechanisms – CRYSTALS-DILITHIUM, Falcon and Rainbow. In addition, three alternative candidates were identified that require more detailed research. In general, a comprehensive analysis of the finalists is an important task for cryptologists in the global cryptocommunity. Moreover, security, i.e. bringing the cryptographic stability of two finalist candidates, to the ES standard – CRYSTALS-DILITHIUM and Falcon, is based on problems in the theory and practice of algebraic lattices. The EP Dilithium method (scheme) is based on the approach called "Fiat-Shamir Interruptions". The essence of the CRYSTALS-DILITHIUM ES algorithm is considered in the article. A detailed analysis of possible attacks on the algorithm and the mechanisms of their implementation is also carried out. Models of violator, threats and security are considered and analyzed. The main definitions of ES security models are provided. The main design elements of the mechanism of perspective post-quantum ES Dilithium are described in the generalized form. General estimations of the ES Dilithium security level are given. The substantiation and essence of models of threats, violator and security are given. The stability of the ES Dilithium algorithm is investigated. The purpose of the article is to substantiate a security model, classification, primary analysis and assessment of known attacks on the CRYSTALS-DILITHIUM EP cryptosystem, to establish restrictions and develop practical algorithms for calculating (generating) system-wide parameters to ensure 128, 256, 384 and 512 bits of security relative to classical and 64, 128, 192 and 256 bits relative to quantum cryptanalysis..

Key words: algebraic lattice; attacks; security; system-wide parameters; security model; threat model; violator model; signature; polynomial; Dilithium.

3 tab. 1 fig. Ref: 46 items.

УДК 004.056.55

Основні положення щодо моделі безпеки для асиметричних перетворень типу ЕП з урахуванням вимог та загроз постквантового періоду / *Ю.І. Горбенко, О.В. Потій, В.В. Онопрієнко, М.В. Єсіна, Г.А. Малєєва* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 29 – 36.

Наведено результати обґрунтування та розробка пропозицій щодо побудування моделі загроз щодо асиметричних криптоперетворень типу перспективний електронний підпис (ЕП), що може застосовуватись в постквантовий період. Викладено деталізовано узагальнені моделі загроз щодо перспективних ЕП та надається їх оцінка. Запропоновано моделі загроз щодо перспективних ЕП при застосуванні методів та засобів класичного та квантового криптоаналізу, моделі загроз при синтезі та застосуванні ЕП взагалі, а також моделі загроз при синтезі та застосуванні ЕП в постквантовий період. Формулюються пропозиції до переліку загроз, щодо яких повинен бути забезпечений захист. Перелік можливих загроз безпеці застосування існуючих та перспективних ЕП формується з числа загроз, наявних у IT-Grundschutz Catalogues з урахуванням апаратних, програмних та апаратно-програмних ресурсів, технологій обробки даних та механізмів криптографічного захисту при застосуванні ЕП, в тому числі з урахуванням вимог та умов синтезу перспективних ЕП, та застосуванні ЕП в постквантовий період. Розглядаються поняття EUF-CMA та SUF-CMA безпеки. Наводяться алгоритми роботи кожної із цих схем. Вводиться поняття комплексної моделі безпеки та наводяться її складові. Розглядається модель порушника та її суть. Наводяться основні загрози (атаки) із застосуванням квантових математичних методів, які можуть бути реалізованими на квантовому комп'ютері (звичайно, якщо він буде побудований та доступний для застосування). Наводяться та розглядаються атаки (загрози) стосовно перспективного ЕП. Проводиться аналіз схем підписів на відповідність необхідним моделям безпеки. Надаються основні поняття та визначення (поняття в термінології теорії ігор і т.д.). Вводяться та використовуються поняття «пряма секретність» та «досконала пряма секретність». Проводиться аналіз схем підпису, що є EUF-CMA та SUF-CMA безпечними. Розглядаються схеми підпису, що є залежними від ключів, з ключами, що розвиваються, з точки зору відповідності моделі безпеки EUF-CMA чи SUF-CMA. Також розглядається алгоритм підпису без стану. Наводяться алгоритми роботи таких схем підпису.

Ключові слова: асиметричний ЕП; класичний та квантовий криптоаналіз; модель загроз при синтезі ЕП; модель загроз при застосуванні ЕП; перелік загроз ЕП; постквантовий період.

Бібліогр.: 10 назв.

УДК 004.056.55

Основные положения по модели безопасности для асимметричных преобразований типа ЭП с учетом требований и угроз постквантового периода / *Ю.И. Горбенко, А.В. Потий, В.В. Ониприенко, М.В. Есина, А.А. Малеева* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 29 – 36.

Приведены результаты, обоснование и разработка предложений по построению модели угроз относительно асимметричных криптопреобразования типа перспективная электронная подпись (ЭП), что может применяться в постквантовый период. Изложены обобщенные модели угроз по перспективным ЭП и дана их оценка. Предложены модели угроз по перспективным ЭП при применении методов и средств классического и квантового криптоанализа, модели угроз при синтезе и применении ЭП вообще, а также модели угроз при синтезе и применении ЭП в постквантовый период. Формулируются предложения по перечню угроз, в отношении которых должна быть обеспечена защита. Перечень возможных угроз безопасности применения существующих и

перспективных ЭП формируется из числа угроз, имеющихся в IT-Grundschutz Catalogues с учетом аппаратных, программных и аппаратно-программных ресурсов, технологий обработки данных и механизмов криптографической защиты при применении ЭП, в том числе с учетом требований и условий синтеза перспективных ЭП, и применении ЭП в постквантовый период. Рассматриваются понятие EUF-CMA и SUF-CMA безопасности. Приводятся алгоритмы работы каждой из этих схем. Вводится понятие комплексной модели безопасности и приводятся ее составляющие. Рассматривается модель нарушителя и его суть. Приводятся основные угрозы (атаки) с применением квантовых математических методов, которые могут быть реализованы на квантовом компьютере (конечно, если он будет построен и доступен для применения). Приводятся и рассматриваются атаки (угрозы) относительно перспективной ЭП. Проводится анализ схем подписей в соответствии с необходимыми моделями безопасности. Представляются основные понятия и определения (понятие в терминологии теории игр и т.д.). Вводятся и используются понятия «прямая секретность» и «совершенная прямая секретность». Проводится анализ схем подписи, которые являются EUF-CMA и SUF-CMA безопасными. Рассматриваются схемы подписи, которые являются зависимыми от ключей, с развивающимися ключами, с точки зрения соответствия модели безопасности EUF-CMA или SUF-CMA. Также рассматривается алгоритм подписи без состояния. Приводятся алгоритмы работы таких схем подписи.

Ключевые слова: асимметричная ЭП; классический и квантовый криптоанализ; модель угроз при синтезе ЭП; модель угроз при применении ЭП; перечень угроз ЭП; постквантовый период.

Библиогр.: 10 назв.

UDC 004.056.55

Basic statements on the security model for asymmetric transformations of the ES type taking into account the requirements and threats of the post-quantum period / *Yu.I. Gorbenko, O.V. Potii, V.V. Onoprienko, M.V. Yesina, G.A. Maleeva* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 29 – 36.

The paper presents the results of substantiation and development of proposals for building a threat model for asymmetric cryptotransformations such as a promising electronic signature (ES), which can be used in the post-quantum period. The generalized models of threats concerning perspective ES are stated in detail and their estimation is given. Threat models for promising ES using classical and quantum cryptanalysis methods and tools, threat models for synthesis and application of ES in general, as well as threat models for synthesis and application of ES in the post-quantum period are proposed. Proposals are formulated for a list of threats for which protection should be provided. The list of possible security threats to existing and future ES is formed from the number of threats available in IT-Grundschutz Catalogs, taking into account hardware, software and hardware-software resources, data processing technologies and cryptographic protection mechanisms in the use of ES, including requirements and conditions of synthesis of promising ES and application of ES in the post-quantum period. The concepts of EUF-CMA and SUF-CMA security are considered. Algorithms of work of each of these schemes are given. The concept of a comprehensive security model is introduced and its components are presented. The model of the violator and its essence are considered. The main threats (attacks) are given using quantum mathematical methods that can be implemented on a quantum computer (of course, if it is built and available for use). Attacks (threats) against a promising ES are presented and considered. The analysis of signature schemes for compliance with the required security models is performed. The terms "forward secrecy" and "perfect forward secrecy" are introduced and used. An analysis of signature schemes that are EUF-CMA and SUF-CMA secure is performed. Signature schemes, that are key-dependent, with evolving keys, are considered in terms of compliance with the EUF-CMA or SUF-CMA security model. The stateless signature algorithm is also considered. Algorithms of operation of such signature schemes are given.

Key words: asymmetric ES; classical and quantum cryptanalysis; model of threats in the synthesis of ES; model of threats in the use of ES; list of threats of ES; postquantum period.

Ref: 10 items.

УДК 004.056.55

Аналіз можливостей та особливості програмування задач криптології на квантовому комп'ютері / *Є.Ю. Каптьол, І.Д. Горбенко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 37 – 48.

Стаття присвячена деталізації можливостей та особливостей застосування квантового комп'ютера для програмування криптологічних задач, їх демонстрації, обгрунтуванню підходів до аналізу можливостей та вивчення особливостей програмування задач криптоаналізу на квантових комп'ютерах. Проаналізовано можливості та наявність забезпечення для вирішення задач криптоаналізу квантовими методами, а також визначено існуючі обмеження щодо їх використання. Розглянуто особливості та можливості квантового комп'ютера та програмування на квантовому комп'ютері. Також розглянуто можливості застосування квантового комп'ютера для криптоаналізу на прикладі методу Гровера. Наведено сутність методу Гровера та особливості його застосування для криптоаналізу. Наведено приклад його застосування для пошукового простору, що представлений квантовим регістром з 56 кубітів. Розглянуто застосування методу Гровера на квантовому комп'ютері, доступному через хмарний сервіс. Розроблено схеми проведення пошуку методом Гровера для застосування на квантовому комп'ютері, що містять різну кількість ітерацій Гровера для дослідження необхідності проведення повного циклу, можливості зупинки та оцінки результатів пошуку на певному етапі. Розроблені схеми перевірено на квантових комп'ютерах з різною архітектурою та на квантовому симуляторі, що наданий для аналізу схем, призна-

чених для запуску на квантовому комп'ютері. Наведено порівняння очікуваних та отриманих результатів застосування методу Гровера на різних етапах проведення пошуку на квантовому комп'ютері.

Ключові слова: квантовий комп'ютер; програмування на квантовому комп'ютері; метод Гровера; алгоритм Гровера; пошук несортованою базою даних; практичний приклад пошуку; приклади пошуку на квантовому комп'ютері.

Табл. 6. Іл. 5. Бібліогр.: 6 назв.

УДК 004.056.55

Анализ возможностей и особенностей программирования задач криптологии на квантовом компьютере / *Е.Ю. Каптел, И.Д. Горбенко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 37 – 48.

Статья посвящена детализации возможностей и особенностей применения квантового компьютера для программирования криптологических задач, их демонстрации, обоснованию подходов к анализу возможностей и изучения особенностей программирования задач криптоанализа на квантовых компьютерах. Проанализированы возможности и наличие обеспечения для решения задач криптоанализа квантовыми методами, а также определены существующие ограничения по их использованию. Рассмотрены особенности и возможности квантового компьютера и программирования на квантовом компьютере. Также рассмотрены возможности применения квантового компьютера для криптоанализа на примере метода Гровера. Приведены суть метода Гровера и особенности его применения для криптоанализа. Также приведен пример его применения для поискового пространства, представленного квантовым регистром из 56 кубитов. Рассмотрено применение метода Гровера на квантовом компьютере, доступном через облачный сервис. Разработаны схемы проведения поиска методом Гровера для применения на квантовом компьютере, содержащие разное количество итераций Гровера для исследования необходимости проведения полного цикла, возможности остановки и оценки результатов поиска на определенном этапе. Разработанные схемы проверены на квантовых компьютерах с разной архитектурой и на квантовом симуляторе, предоставленном для анализа схем, предназначенных для запуска на квантовом компьютере. Приведено сравнение ожидаемых и полученных результатов применения метода Гровера на разных этапах проведения поиска на квантовом компьютере.

Ключевые слова: квантовый компьютер; программирование на квантовом компьютере; метод Гровера; алгоритм Гровера; поиск в несортированной базе данных; практический пример поиска; примеры поиска на квантовом компьютере.

Табл. 6. Ил. 5. Библиогр.: 6 назв.

UDC 004.056.55

Analysis of the possibilities and peculiarities of programming cryptology problems on a quantum computer / *Ye.Yu. Kaptol, I.D. Gorbenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 37 – 48.

This paper is devoted to detailing the possibilities and features of quantum computer use for cryptological problems, their demonstration, justification of approaches to the possibilities analysis and studying features of cryptanalysis problems programming on quantum computers. The possibilities and availability of hardware for solving cryptanalysis problems through quantum methods are analyzed and existing restrictions of their use are determined. The quantum computer and quantum computer programming features are considered. The possibilities of quantum computer use for cryptanalysis are also considered with the Grover's method example. The essence of Grover's method and features of its application for cryptanalysis are given. An example of its application to the search space which is represented by a quantum register of 56 qubits is given as well. The quantum computer application of Grover's method on quantum computer accessible through a loud service is considered. Schemes for conducting a search by Grover's method for quantum computer application are developed, containing a different number of Grover iterations to study the need for executing a full cycle, the possibility to stop and evaluate search results at a certain stage. The developed circuits are tested on quantum computers with different architectures and on a quantum simulator provided for the analysis of circuits intended to run on a quantum computer. The comparison of the expected and obtained results of the Grover's method application at different search stages on quantum computer is given.

Key words: quantum computer; quantum computer programming; Grover's method; Grover's algorithm; unsorted database search; practical search example; examples of search on a quantum computer.

6 tab. 5 fig. Ref: 6 items.

УДК 004.056.55

Аналіз стійкості постквантового електронного підпису Dilithium до атак на помилки / *Ю.І. Горбенко, О.С. Дроздова* // Радіотехника : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 49 – 56.

Проведено аналіз перспективного варіанту постквантового електронного підпису на основі алгебраїчних решіток Dilithium. Головною задачею аналізу є дослідження стійкості до атак на помилки, зокрема диференційних. Спочатку наводяться відомості про саму схему ЕП та її стійкість, атаки на помилки, їх розвиток до диференційних атак на помилки. Розглядаються можливості проведення цих атак та критерії їх успішного виконання. Було виявлено місця алгоритму ЕП, які потребують захисту від атак на помилки, такими є геш-функція (момент звернення та операція множення поліномів), етап завантаження особистого ключа, функція розширення початкового значення. Також повторне використання нонсу та часткове повторне використання нонсу при ге-

нерації ключів становить суттєву загрозу; провівши таку атаку, порушник може повністю відновити довгостроковий особистий ключ Dilithium. Сформовано заходи протидії на основі аналізу джерел, наведено їх переваги та негативні ефекти. Методами захисту від таких атак є: повторне обчислення підпису; перевірка підпису після підписання, що є втричі швидшим ніж попередній метод; внесення додаткової випадковості до детермінованої вибірки шуму; перевірка значення секретних та помилкових компонентів (нонсу); обчислення середнього значення та дисперсії вибірки, та їх перевірка на приналежність заданому діапазону. Результати роботи дають дослідникам орієнтир для розробки захищених схем постквантового електронного підпису.

Ключові слова: електронний підпис; постквантова криптографія; стійкість; диференційні атаки на помилки; заходи протидії.

Бібліогр.: 14 назв.

УДК 004.056.55

Анализ стойкости постквантовой электронной подписи Dilithium к атакам на ошибки / *Ю.И. Горбенко, О.С. Дроздова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 49 – 56.

Проведен анализ перспективного варианта постквантовой электронной подписи на основе алгебраических решеток Dilithium. Основной задачей анализа является исследование стойкости Dilithium к атакам на ошибки, в частности дифференциальных. Сначала приводятся сведения о самой схеме ЭП и ее стойкости, далее – атаки на ошибки и их развитие в дифференциальные атаки на ошибки. Рассматриваются возможности проведения этих атак и критерии их успешного выполнения. Были обнаружены места алгоритма ЭП, которые нуждаются в защите от атак на ошибки такие как, хеш-функция (момент обращения к ней и операция умножения полиномов), этап загрузки закрытого ключа, функция расширения начального значения. Также повторное использование нонсов и частичное повторное использование нонсов при генерации ключей составляет существенную угрозу, проведя такую атаку, нарушитель может полностью восстановить долгосрочный закрытый ключ Dilithium. Сформированны меры противодействия атакам на основе анализа источников, приведены их преимущества и побочные негативные эффекты. Методами защиты от таких атак являются: повторное вычисление подписи; проверка подписи после подписания, что в три раза быстрее чем предыдущий метод, внесение дополнительной случайности к детерминированной выборке шума; проверка значения секретных и ошибочных компонентов (нонсов) вычисления среднего значения и дисперсии выборки и их проверка на принадлежность заданному диапазону. Результаты работы дают исследователям ориентир для разработки защищенных схем постквантовой электронной подписи.

Ключевые слова: электронная подпись; постквантовая криптография; стойкость; дифференциальные атаки на ошибки; меры противодействия.

Библиогр.: 14 назв.

UDC 004.056.55

Analysis of Dilithium post-quantum electronic signature resistance to fault attacks / *U.I. Gorbenko, O.S. Drozdova* // // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 49 – 56.

Analysis of a perspective variant of post-quantum electronic signature based on algebraic lattices of Dilithium is carried out. The central task of the analysis is to study the resistance of Dilithium to fault attacks, in particular differential ones. First, information is given about the ES scheme itself and its security, fault attacks, their development to differential fault attacks. Possibilities of carrying out these attacks and criteria of their successful execution are considered. The places of the ES algorithm that need protection against fault attacks were identified, such as hash function (the moment of access to it and operation of polynomials multiplying), the stage of loading the private key, the function of expanding seed. Also, nonce reuse and partial nonce reuse when generating keys poses a significant threat, and by carrying out such an attack, the attacker can fully recover the long-term Dilithium private key. Attacks countermeasures are formed based on the sources analysis, their advantages and negative effects are presented. Methods of protection against such attacks are: re-calculation of the signature; verification of signature after signing, which is three times faster than the previous method; introducing additional randomness to the deterministic noise sampling; checking the value of secret and false components (nonce); calculating the average value and variance of the sample, and checking them for belonging to a given range. The results of this work provide researchers with a guide for the development of secure post-quantum electronic signature schemes.

Key words: electronic signature, post-quantum cryptography, security, differential fault attack, countermeasures.

Ref.: 14 items.

УДК 004.056.55

Генерація загальносистемних параметрів для криптосистеми Falcon для 256, 384, 512 біт безпеки / *І.Д. Горбенко, С.О. Кандій, М.В. Єсіна, Є.В. Острянська* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 57 – 63.

На світовому рівні зусилля криптологів-теоретиків, математиків та криптологів-практиків зосереджені на відкритому конкурсі NIST PQC. Одним із основних завдань конкурсу є розробка та прийняття постквантового чи постквантових стандартів ЕП. Фіналістами другого етапу конкурсу NIST стали три механізми ЕП – CRYSTALS-DILITHIUM, Falcon та Rainbow. Окрім цього, були визначені три альтернативні кандидати, які потребують більш детального дослідження. Всесторонній аналіз фіналістів є важливою задачею для криптологів

світової криптоспільноти. Причому, безпека, тобто доведення криптографічної стійкості двох кандидатів-фіналістів на стандарт ЕП – CRYSTALS-DILITHIUM та Falcon ґрунтується на проблемах з теорії та практики алгебраїчних решіток. Дослідження показують, що серед схем ЕП на решітках дещо відрізняється від інших кандидатів та має перспективи щодо прийняття в якості стандарту алгоритм Falcon. Основним та домінуючим підходом до проєктування механізму ЕП Falcon є використання перетворення Фіата – Шаміра з перериваннями. Для безпечного використання ЕП Falcon повинні бути знайдені набори загальносистемних параметрів, за яких забезпечується стійкість до всіх відомих та потенційних атак. В процесі формування вимог до ЕП NIST у рамках конкурсу був зацікавлений тільки в наборах загальносистемних параметрів до 256 біт класичної безпеки включно. Проте, на думку авторів, на перспективу доцільним є забезпечення не менше 384 і 512 біт безпеки щодо класичного криптоаналізу та не менше 192 та 256 біт безпеки щодо квантового криптоаналізу. У статті коротко розглядається сутність алгоритму ЕП Falcon. Також проводиться аналіз можливих атак на алгоритм та механізми їх реалізації. Розглядається процес генерації загальносистемних параметрів для 256, 384, 512 біт стійкості. Наводяться висновки та рекомендації. Метою роботи є класифікація та первинний аналіз відомих атак на криптосистему ЕП Falcon, встановлення обмежень та розробка практичних алгоритмів обчислення (генерації) загальносистемних параметрів для забезпечення не менше, ніж 256, 384 і 512 біт безпеки щодо класичного та не менше, ніж 128, 192 та 256 біт безпеки щодо квантового криптоаналізу.

Ключові слова: алгебраїчні решітки; атаки; безпека; загальносистемні параметри; підпис; поліном; Falcon.

Табл. 3. Бібліогр.: 12 назв.

УДК 004.056.55

Генерация общесистемных параметров для криптосистемы Falcon для 256, 384, 512 бит безопасности / *И.Д. Горбенко, С.А. Кандий, М.В. Есина, Е.В. Острянская* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 57 – 63.

На мировом уровне усилия криптологов-теоретиков, математиков и криптологов-практиков сосредоточены на открытом конкурсе NIST PQC. Одной из основных задач конкурса является разработка и принятие постквантового или постквантовых стандартов ЭП. Финалистами второго этапа конкурса NIST стали три механизма ЭП – CRYSTALS-DILITHIUM, Falcon и Rainbow. Кроме этого, были определены три альтернативных кандидата, которые требуют более детального исследования. В целом всесторонний анализ финалистов является важной задачей для криптологов мирового криптосообщества. Причем, безопасность, то есть доведение криптографической стойкости двух кандидатов-финалистов, на стандарт ЭП – CRYSTALS-DILITHIUM и Falcon, основывается на проблемах по теории и практике алгебраических решеток. Исследования показывают, что среди схем ЭП на решетках несколько отличается от других кандидатов и имеет перспективы для принятия в качестве стандарта алгоритм Falcon. Основным и доминирующим подходом к проектированию механизма ЭП Falcon является использование преобразования Фиата – Шамира с прерываниями. Для безопасного использования ЭП Falcon должны быть найдены наборы общесистемных параметров, при которых обеспечивается устойчивость ко всем известным и потенциальным атакам. В процессе формирования требований к ЭП NIST в рамках конкурса был заинтересован только в наборах общесистемных параметров до 256 бит классической безопасности включительно. Однако, по мнению авторов, на перспективу целесообразно обеспечить не менее 384 и 512 бит безопасности по классическому криптоанализу и не менее 192 и 256 бит безопасности – по квантовому криптоанализу. В статье кратко рассматривается сущность алгоритма ЭП Falcon. Также проводится анализ возможных атак на алгоритм и механизмы их реализации. Рассматривается процесс генерации общесистемных параметров для 256, 384, 512 бит стойкости. Приводятся выводы и рекомендации. Цель работы – классификация и первичный анализ известных атак на криптосистему ЭП Falcon, установление ограничений и разработка практических алгоритмов вычисления (генерации) общесистемных параметров для обеспечения не менее 256, 384 и 512 бит безопасности относительно классического и не менее 128, 192 и 256 бит безопасности относительно квантового криптоанализа.

Ключевые слова: алгебраические решетки; атаки; безопасность; общесистемные параметры; подпись; полином; Falcon.

Табл. 3. Библиогр.: 12 назв.

UDC 004.056.55

Generation of system-wide parameters for Falcon cryptosystem for 256, 384, 512 bits of security / *I.D. Gorbenko, S.O. Kandiy, M.V. Yesina, E.V. Ostryanska* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 57 – 63.

Globally, the efforts of a significant number of crypto-theorists, mathematicians and cryptologists-practitioners are focused on the NIST PQC open competition. One of the main tasks of the competition consists in development and adoption of a post-quantum ES standard or standards. The finalists of the second stage of the NIST competition were three ES mechanisms – CRYSTALS-DILITHIUM, Falcon and Rainbow. In addition, three alternative candidates were identified that require more detailed research. In general, a comprehensive analysis of the finalists is an important task for cryptologists in the global cryptocommunity. Moreover, security, i.e. brining the cryptographic stability of two finalist candidates, to the ES standard – CRYSTALS-DILITHIUM and Falcon, is based on problems in the theory and practice of algebraic lattices. Studies show that among the ES schemes on lattices it differs slightly from other candidates and has prospects for the adoption as the Falcon algorithm standard. The main and dominant approach to the design of the Falcon ES mechanism is the use of the Fiat-Shamir transformation with interruptions. The sets of system-wide pa-

rameters that ensure resistance to all known and potential attacks should be found for the safe use of the Falcon ES. In the process of forming the requirements for ES within the competition, the NIST was interested only in sets of system-wide parameters up to 256 bits of classical security inclusive. However, according to the authors of this work, in the future it is advisable to provide at least 384 and 512 bits of security for classical cryptanalysis and at least 192 and 256 bits of security for quantum cryptanalysis. The article briefly considers the essence of the Falcon electronic signature (ES) algorithm. An analysis of possible attacks on the algorithm and the mechanisms of their implementation is also performed. The process of generating system-wide parameters for 256, 384, 512 stability bits is considered. Conclusions and recommendations are given. The objective of the work is the classification and initial analysis of known attacks on the ES Falcon cryptosystem, setting limits and developing practical algorithms for calculating (generating) system-wide parameters to provide not less than 256, 384 and 512 security bits for classical and not less than 128, 192 and 256 security bits for quantum cryptanalysis.

Key words: algebraic lattice; attacks; security; system-wide parameters; signature; polynomial; Falcon.
3 tab. Ref: 12 items.

УДК 004.056.55

Процеси та методи вибору загальносистемних параметрів перспективного алгоритму електронного підпису на основі алгебраїчних решіток / *В.А Кулібаба* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 64 – 71.

Важливою особливістю перехідного та постквантового періоду є застосування нових математичних методів для протидії квантовому криптоаналізу. Особливу увагу світове криптографічне співтовариство приділяє відкритому конкурсу на постквантовий стандарт електронного підпису. Проблемним питанням є доведення стійкості нових математичних методів синтезу перетворень типу електронний підпис, зокрема з використанням алгебраїчних решіток. Проаналізовано існуючі алгоритми електронного підпису 2-го етапу конкурсу NIST. Серед обраних кандидатів на стандарт ЕП два із трьох алгоритмів засновані на алгебраїчних решітках, це CRYSTALS-DILITHIUM та FALCON. NIST випустив заяву про те, що скоріше за все буде обрано один із алгоритмів через однакому математичну базу, що застосовується в обох алгоритмах. Розглядаються основні атаки на алгоритми електронного підпису, засновані на проблемі навчання з помилками, а також параметри алгоритму ЕП Dilithium, що впливають на стійкість та складність перетворень. Розглядаються методи генерування загальносистемних параметрів рівнів стійкості 512 біт класичної та 256 біт квантової безпеки, а також захищеність алгоритму від атак сторонніми каналами. Проаналізовано залежність часу вироблення електронного підпису від ключів. Подано результати обчислень параметрів для рівня стійкості 512/256, а також надано рекомендації щодо вибору загальносистемних параметрів. Розглянуто результати 2-го етапу конкурсу постквантових криптоалгоритмів NIST, а також перспективи стандартизації перетворень типу електронний підпис на 3-му етапі. Зроблено висновки про необхідність більш детального вивчення атак на алгоритми, засновані на проблемі навчання з помилками, а також про важливість генерування загальносистемних параметрів більш високих порядків.

Ключові слова: загальносистемні параметри; алгоритми постквантового електронного підпису; алгебраїчні решітки; функції хешування; криптографічна стійкість.
Табл. 4. Іл. 1. Бібліогр.: 15 назв.

УДК 004.056.55

Процессы и методы выбора общесистемных параметров перспективного алгоритма электронной подписи на основе алгебраических решеток / *В.А Кулибаба* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 64 – 71.

Важной особенностью переходного и постквантового периода является применение новых математических методов для противодействия квантовому криптоанализу. Особое внимание мировое криптографическое сообщество уделяет открытому конкурсу на постквантовый стандарт электронной подписи. Проблемным вопросом является доказательство стойкости новых математических методов синтеза преобразований типа электронной подписи, в том числе с использованием алгебраических решеток. Проанализированы существующие алгоритмы электронной подписи 2-го этапа конкурса NIST. Среди выбранных кандидатов на стандарт ЭП два из трех алгоритмов основаны на алгебраических решетках, это CRYSTALS-DILITHIUM и FALCON. NIST выпустил заявление о том, что, скорее всего, будет выбран один из алгоритмов ввиду одинаковой математической базы, которая применяется в обоих алгоритмах. Рассматриваются основные атаки на алгоритмы электронной подписи, основанные на проблеме обучения с ошибками, а также параметры алгоритма ЭП Dilithium, влияющие на стойкость и сложность преобразований. Рассматриваются методы генерирования общесистемных параметров уровней стойкости 512 бит классической и 256 бит квантовой безопасности, а также защищенность алгоритма от атак посторонними каналами. Проанализирована зависимость времени генерации электронной подписи от ключей. Представлены результаты вычислений параметров для уровня стойкости 512/256, а также даны рекомендации по выбору общесистемных параметров. Рассмотрены результаты 2-го этапа конкурса постквантовых криптоалгоритмов NIST, а также перспективы стандартизации преобразований типа электронной подписи на 3-м этапе. Сделаны выводы о необходимости более детального изучения атак на алгоритмы, основанные

на проблеме обучения с ошибками, а также о важности генерирования общесистемных параметров более высоких порядков.

Ключевые слова: общесистемные параметры; алгоритмы постквантового электронной подписи; алгебраические решетки; функции хеширования; криптографическая стойкость.

Табл. 4. Ил. 1. Библиогр.: 15 назв.

UDC 004.056.55

Processes and methods of selection of system-wide parameters of perspective algorithm of electronic signature based on algebraic lattices / *V.A. Kulibaba* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 64 – 71.

An important feature of the transition and post-quantum period is the application of new mathematical methods to counteract quantum cryptanalysis. The world cryptographic community pays special attention to the open competition for the post-quantum standard of electronic signature. The problem is to prove the stability of new mathematical methods for the synthesis of transformations such as electronic signature, in particular with the use of algebraic lattices. The existing algorithms of electronic signature of the 2nd stage of the NIST competition are analyzed. Among the selected candidates for the EP 2 standard, 3 of the 3 algorithms are based on algebraic lattices, CRYSTALS-DILITHIUM and FALCON. The NIST has issued a statement saying that it is most likely that one of the algorithms will be chosen due to the same mathematical basis used in both algorithms. The main attacks on electronic signature algorithms based on the problem of learning with errors, as well as the parameters of the EP Dilithium algorithm, which affect the stability and complexity of transformations, are considered. Methods for generating system-wide parameters of stability levels of 512 bits of classical and 256 bits of quantum security, as well as the protection of the algorithm againstfrom attacks by third-party channels are considered. The dependence of the time of electronic signature production on the keys is analyzed. The results of calculations for the level of stability 512/256 are given, and also recommendations on the choice of system-wide parameters are given. The results of the 2nd stage of the NIST competition of post quantum cryptographic algorithms, as well as the prospects of standardization of transformations such as electronic signature at the 3rd stage are considered. Conclusions are made about the need for a more detailed study of attacks on algorithms based on the problem of learning with errors, as well as the importance of generating system-wide parameters of higher levels.

Key words: system-wide parameters; post-quantum electronic signature algorithms; algebraic lattices; hashing functions; cryptographic stability.

4 tab. 1 fig. Ref: 15 items.

УДК 004.056.55

Моделі загроз щодо асиметричних криптоперетворень перспективного електронного підпису / *Ю.І. Горбенко, М.В. Єсіна, В.В. Оноприєнко, Г.А. Малєєва* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 72 – 78.

Розглядається поняття моделі загроз, наводяться результати обґрунтування та розробка пропозицій щодо побудування моделі загроз стосовно асиметричних криптоперетворень типу перспективний електронний підпис (ЕП), що може застосовуватись в постквантовий період. Викладені узагальнені моделі загроз щодо перспективних ЕП та дається їх оцінка. Запропоновано моделі загроз щодо перспективних ЕП при застосуванні методів та засобів класичного та квантового криптоаналізу, моделі загроз при синтезі та застосуванні ЕП взагалі, а також моделі загроз при синтезі та застосуванні ЕП в постквантовий період. За результатами аналізу щодо методів синтезу та застосування відомих та перспективних ЕП визначено перелік загроз. Формулюються пропозиції щодо переліку загроз, щодо яких повинен бути забезпечений захист. Перелік загроз визначається за допомогою використання IT-Grundschutz Catalogues бази Германії, і на основі цього формується модель загроз. Визначається, що детально загрози щодо застосування класичного криптоаналізу при синтезі та застосуванні ЕП повинні бути визначеними безумовно. Визначено основні загрози (методи) класичного криптоаналізу, що повинні бути враховані. Розглядаються можливі варіанти атак сторонніми каналами. Наведено основні загрози (атаки) із застосуванням квантових математичних методів, які можуть бути реалізовані на квантовому комп'ютері (звичайно, якщо він буде побудований). Наводиться порівняльний аналіз складності факторизації для класичного та квантового алгоритмів, а також порівняльний аналіз складності алгоритму дискретного логарифмування в скінченому полі на основі решета числового поля та алгоритму Шора. Розглядаються загрози (атаки) на прикладі проблеми стійкості криптоперетворень на основі навчання з помилками (LWE). У цілому атаки на LWE можливо розділити на два великі класи – атаки, що ґрунтуються на переборі та атаки, що ґрунтуються на зведенні решіток. Попередній аналіз дозволяє зробити висновок, що сучасні варіанти механізмів LWE ґрунтуються на поліноміальних кільцях.

Ключові слова: асиметричний ЕП; класичний та квантовий криптоаналіз; модель загроз при синтезі ЕП; модель загроз при застосуванні ЕП; перелік загроз ЕП; постквантовий період.

Табл. 3. Бібліогр.: 12 назв.

УДК 004.056.55

Модели угроз для асимметричных криптопреобразований перспективной электронной подписи / *Ю.И. Горбенко, М.В. Есина, В.В. Оноприенко, А.А. Малеева* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 72 – 78.

Рассматривается понятие модели угроз, приводятся результаты обоснование и разработка предложений по построению модели угроз относительно асимметричных криптопреобразований типа перспективная электронная подпись (ЭП), что может применяться в постквантовый период. Изложены обобщенные модели угроз для перспективных ЭП и дается их оценка. Предложены модели угроз по перспективным ЭП при применении методов и средств классического и квантового криптоанализа, модели угроз при синтезе и применении ЭП вообще, а также модели угроз при синтезе и применении ЭП в постквантовый период. По результатам анализа по методам синтеза и применению известных и перспективных ЭП определен перечень угроз. Формулируются предложения относительно перечня угроз, в отношении которых должна быть обеспечена защита. Перечень угроз определялся с помощью использования IT-Grundschutz Catalogues базы Германии, и на основе этого формируется модель угроз. Определяется, что подробно угрозы по применению классического криптоанализа при синтезе и применении ЭП должны быть определены безусловно. Определены основные угрозы (методы) классического криптоанализа, которые должны быть учтены. Рассматриваются возможные варианты атак сторонними каналами. Приведены основные угрозы (атаки) с применением квантовых математических методов, которые могут быть реализованы на квантовом компьютере (конечно, если он будет построен). Приводится сравнительный анализ сложности факторизации для классического и квантового алгоритмов, а также сравнительный анализ сложности алгоритма дискретного логарифмирования в конечных полях на основе решета числового поля и алгоритма Шора. Рассматриваются угрозы (атаки) на примере проблемы устойчивости криптопреобразования на основе обучения с ошибками (LWE). В целом атаки на LWE можно разделить на два больших класса – атаки, основанные на переборе и атаки, основанные на приведении решеток. Предварительный анализ позволяет сделать вывод, что современные варианты механизмов LWE основываются на полиномиальных кольцах.

Ключевые слова: асимметричная ЭП; классический и квантовый криптоанализ; модель угроз при синтезе ЭП; модель угроз при применении ЭП; перечень угроз ЭП; постквантовый период.

Табл. 3. Библиогр.: 12 назв.

UDC 004.056.55

Threat models for asymmetric cryptotransformations of the promising electronic signature / *Yu.I. Gorbenko, M.V. Yesina, V.V. Onoprienko, G.A. Maleeva* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 72 – 78.

The paper considers the concept of a threat model, presents the results of substantiation and development of proposals for building a threat model for asymmetric cryptotransformations such as a promising electronic signature (ES), which can be used in the post-quantum period. The generalized models of threats concerning perspective ES are stated in detail and their estimation is given. Threat models for promising ES using classical and quantum cryptanalysis methods and tools, threat models for synthesis and application of ES in general, as well as threat models for synthesis and application of ES in the post-quantum period are proposed. A list of threats is identified based on the results of the analysis of the methods of synthesis and application of known and promising ES. Proposals are formulated for a list of threats for which protection should be provided. The list of threats is determined using the IT-Grundschutz Catalogues of the German database, and based on this a threat model is formed. It is determined that the threats to the use of classical cryptanalysis in the synthesis and application of EP must be identified in detail unconditionally. The main threats (methods) of classical cryptanalysis that must be taken into account are identified. Possible variants of side channel attacks are considered. The main threats (attacks) using quantum mathematical methods that can be implemented on a quantum computer (of course, if it is built). A comparative analysis of the complexity of factorization for classical and quantum algorithms, as well as a comparative analysis of the complexity of the algorithm of discrete logarithm in a finite field based on the sieve of a numerical field and the Shore algorithm are given. Threats (attacks) are considered on the example of the problem of stability of cryptotransformations based on learning with errors (LWE). In general, attacks on LWE can be divided into 2 major classes – attacks based on bust and attacks based on lattice reduce. Preliminary analysis allows us to conclude that modern versions of LWE mechanisms are based on polynomial rings.

Key words: asymmetric ES; classical and quantum cryptanalysis; threat model in ES synthesis; threat model in ES application; list of ES threats; post-quantum period.

3 tab. Ref: 12 items.

УДК 004.056.55

Порівняльний аналіз ARX схем шифрування / *В.І. Руженцев* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 79 – 86.

Аналізуються ARX алгоритми шифрування, тобто такі, що використовують лише три операції: модульне додавання, XOR додавання та циклічний зсув. Розробляються 16-бітні зменшені моделі найбільш відомих алгоритмів цього класу. Серед цих алгоритмів Salsa, Chacha, Cypress, Speckey, Simon, Chaskey. Деякі з них оперують 4-бітними словами, інші – 8-бітними словами. Шляхом вичерпного пошуку для моделей цих алгоритмів визначаються такі криптографічні показники, як максимальна імовірність проходження різниці (визначає стійкість шифру до атак диференціального криптоаналіза); максимальна імовірність лінійної апроксимації (визначає стійкість шифру до атак лінійного криптоаналіза); нелінійний порядок (визначає стійкість шифру до атак інтерполяційного, алгебраїчного криптоаналіза). Демонструється, що більшість моделей зі збільшенням кількості

циклів наближаються за цими показниками до параметрів випадкових підстановок. Визначено, що модель алгоритму Simon не володіє цією властивістю. Запропоновано декілька модифікацій цього алгоритму. Зіставляння кількості потрібних операцій для досягнення показників випадкової підстановки визначило найбільш вдалі ARX схеми. Найбільш ефективною 4-бітовою конструкцією є зменшена модель Chaskey, а найбільш ефективною 8-бітовою – запропонована в роботі модифікація схеми Simon. Показано, що, потенційно ARX схеми з більшим форматом операцій є більш гнучкими та ефективними, оскільки потребують приблизно вдвічі меншої кількості операцій для забезпечення криптографічних показників випадкової підстановки.

Ключові слова: криптоаналіз; стійкість; ARX-алгоритм; модульне додавання; циклічний зсув; диференційний криптоаналіз; різність; лінійний криптоаналіз; алгебраічний криптоаналіз; випадкова підстановка.

Табл. 5. Іл. 5. Бібліогр.: 20 назв.

УДК 004.056.55

Сравнительный анализ ARX схем шифрования / *В.И. Руженцев* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 79 – 86.

Анализируются ARX алгоритмы шифрования, то есть такие, которые используют лишь три операции: модульное сложение, XOR сложение и циклический сдвиг. Разрабатываются 16-битные уменьшенные модели наиболее известных алгоритмов этого класса. Среди этих алгоритмов Salsa, Chacha, Cypress, Speckey, Simon, Chaskey. Некоторые из них оперируют 4-битными словами, другие – 8-битными словами. Путем исчерпывающего поиска для моделей этих алгоритмов определяются такие криптографические показатели, как максимальная вероятность прохождение разности (определяет стойкость шифра к атакам дифференциального криптоанализа); максимальная вероятность линейной аппроксимации (определяет стойкость шифра к атакам линейного криптоанализа); нелинейный порядок (определяет стойкость шифра к атакам интерполяционного, алгебраического криптоанализа). Демонстрируется, что большинство моделей с увеличением количества циклов приближаются по этим показателями к параметрам случайных подстановок. Определено, что модель алгоритма Simon не владеет этим свойством. Предложено несколько модификаций этого алгоритма. Сравнение количества нужных операций для достижения показателей случайной подстановки определило наиболее удачные ARX схемы. Наиболее эффективной 4-битовой конструкцией оказалась уменьшенная модель Chaskey, а наиболее эффективной 8-битовой – предложенная в работе модификация схемы Simon. Показано, что, потенциально, ARX схемы с большим форматом операций являются более гибкими и эффективными, поскольку требуют приблизительно вдвое меньшего количества операций для обеспечения криптографических показателей случайной подстановки.

Ключевые слова: криптоанализ; стойкость; ARX-алгоритм; модульное сложение; циклический сдвиг; дифференциальный криптоанализ; разность; линейный криптоанализ; алгебраический криптоанализ; случайная подстановка.

Табл. 5. Ил. 5. Библиогр.: 20 назв.

UDC 004.056.55

Comparative analysis of ARX encryption schemes / *V.I. Ruzhentsev* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 79 – 86.

ARX encryption algorithms are analyzed, that is, those that use only three operations: modular addition, XOR addition and cyclic shift. 16-bit reduced models of the most famous algorithms of this class are being developed. Among these algorithms are Salsa, Chacha, Cypress, Speckey, Simon, Chaskey. Some of them operate with 4-bit words, others with 8-bit words. By an exhaustive search for models of these algorithms some cryptographic parameters are determined. These parameters are the maximum probability of passing the difference (determines the resistance of the cipher to attacks of differential cryptanalysis); maximum probability of linear approximation (determines the resistance of the cipher to attacks of linear cryptanalysis); non-linear order (determines the resistance of the cipher to interpolation attacks, algebraic cryptanalysis). It is demonstrated that most models with an increase in the number of rounds come to the parameters of random permutations. It is determined that the Simon algorithm model does not possess this property. Several modifications of this algorithm are proposed. Comparing the number of necessary operations to achieve random substitution performance, the most successful ARX schemes were determined. The most efficient 4-bit scheme is the reduced Chaskey model, and the most effective 8-bit one is the modification of the Simon scheme which was proposed in this work. It is shown that, potentially, ARX schemes with a large format of operations are more flexible and efficient, since they require approximately half the number of operations to provide cryptographic parameters of random substitution.

Key words: cryptanalysis; strength; ARX algorithm; modular addition; cyclic shift; differential cryptanalysis; difference; linear cryptanalysis; algebraic cryptanalysis; random substitution.

5 tab. 5 fig. Re

ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОММУНІКАЦІЙНИХ СИСТЕМАХ
ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМАХ
PROTECTION OF INFORMATION IN INFORMATION AND COMMUNICATION SYSTEMS

УДК 681.3.06:519.248.681

Методи та засоби синтезу і генерації сигналів – фізичних переносників даних у сучасних інформаційно-комунікаційних системах / *І.Д. Горбенко, Є.А. Семенко, О.А. Замула* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 87 – 98.

Функціонування низки сучасних інформаційно-комунікаційних систем (ІКС) здійснюється в умовах зовнішніх і внутрішніх впливів, обумовлених, з одного боку, дією природних перешкод, перешкод від інших радіотехнічних систем, що функціонують на близьких частотах або в спільній ділянці діапазону частот, з іншого боку, – навмисних завад, створюваних станціями протидії з метою радіоелектронного подавлення діючих систем. До ІКС, особливо, критичного призначення, пред'являються все більш жорсткі вимоги щодо забезпечення ефективності їх функціонування: достовірності і швидкості передачі інформації, живучості, завадозахищеності, інформаційної безпеки. У таких умовах особливого значення набуває наявність і застосування захищених інформаційно-комунікаційних систем. Під захищеністю систем розуміють, перш за все, їх здатність забезпечувати необхідні показники з завадозахищеності, імітостійкості, інформаційної, енергетичної і структурної скритності, швидкості передавання інформації, частотної і енергетичної ефективності. Необхідність застосування захищених радіоканалів змушує дослідників по-новому подивитися на режими функціонування захищених радіоканалів і на аспекти формування і застосування складних сигналів – фізичних переносників даних для таких систем. У роботі представлено концептуальні положення щодо побудови захищених ІКС, які визначають необхідність проведення системної класифікації та уніфікацію інформаційних потоків для вирішення завдань формування та обробки інформації в ІКС, систематизацію моделей, методів, технічних і програмних засобів їх реалізації. Принципи побудови нових технологій в області ІКС повинні охоплювати весь спектр перетворень інформації в комплексі, від джерела до споживача, і повинні бути засновані не тільки на ефективній передачі інформації, але і на забезпеченні скритності, електромагнітної та іншої сумісності, екології, інформаційної безпеки, захищеності від нав'язування (введення в систему) помилкових даних і інше. Показано, що однією зі складних проблем створення захищених ІКС, є синтез системи сигналів – фізичних переносників даних. Наведено аналіз низки систем сигналів (OFDM-сигналів, сигналів з лінійною частотною модуляцією (ЛЧМ), складних нелінійних дискретних сигналів), застосування яких дозволяє поліпшити показники ефективності сучасних ІКС (завадостійкості прийому, інформаційної безпеки, скритності функціонування, захищеності від введення (нав'язування) неправдивих повідомлень, фальсифікації повідомлень; забезпечення цілісності даних, стійкості до міжсимвольної інтерференції, інформаційної ємності системи при обмеженій смузі пропускання, швидкості прийому-передачі даних тощо). У даній роботі на основі дослідження алгебраїчної структури систем нелінійних параметричних нерівностей сформульовані і у загальному виді вирішені задачі синтезу одного з нових класів складних нелінійних дискретних сигналів із заданими кореляційними, ансамблевими і структурними властивостями, – криптографічних сигналів. Представлено принципи побудови і загальна характеристика створеного програмно-апаратного комплексу для синтезу, дослідження властивостей, генерації, обробки та тестування математичних моделей низки класів сигналів-фізичних переносників даних у сучасних ІКС.

Ключові слова: завадостійкість прийому; скритність; інформаційна безпека; дискретні послідовності; складні системи сигналів; синтез систем сигналів; комплексний програмний засіб; інтерфейс користувача; шумоподібний сигнал.

Іл. 2. Бібліогр.: 16 назв.

УДК 681.3.06:519.248.681

Методы и средства синтеза и генерации сигналов – физических переносчиков данных в современных информационно-коммуникационных системах / *И.Д. Горбенко, Е.А. Семенко, А.А. Замула* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 87 – 98.

Функционирование ряда современных информационно-коммуникационных систем (ИКС) осуществляется в условиях внешних и внутренних воздействий, обусловленных, с одной стороны, действием естественных помех, помех от других радиотехнических систем, функционирующих на близких частотах или в общем участке диапазона частот, с другой стороны, – помех, создаваемых станциями противодействия с целью радиоэлектронного подавления действующих систем. К ИКС, особенно критического назначения, предъявляются все более жесткие требования по обеспечению эффективности их функционирования: достоверности и скорости передачи информации, живучести, помехозащищенности, информационной безопасности. В таких условиях особое значение приобретает наличие и применение защищенных информационно-коммуникационных систем. Под защищенностью систем понимают, прежде всего, их способность обеспечивать необходимые показатели по помехозащищенности, имитостойкости, информационной, энергетической и структурной скрытности, скорости передачи информации, частотной и энергетической эффективности. Необходимость применения защищенных радиоканалов заставляет исследователей по-новому посмотреть на режимы функционирования защищенных радиоканалов и на аспекты формирования и применения сложных сигналов – физических переносчиков данных для таких систем. В работе представлены концептуальные положения по построению защищенных ИКС, которые определяют необходимость проведения системной классификации и унификации информацион-

ных потоков для решения задач формирования и обработки информации в ИКС, систематизацию моделей, методов, технических и программных средств их реализации. Принципы построения новых технологий в области ИКС должны охватывать весь спектр преобразований информации в комплексе – от источника к потребителю, должны быть основаны не только на эффективной передачи информации, но и на обеспечении скрытности, электромагнитной и другой совместимости, экологии, информационной безопасности, защищенности от навязывания (введение в систему) ошибочных данных и прочее. Показано, что одной из сложных проблем создания, защищенных ИКС является синтез системы сигналов – физических переносчиков данных. Проведен анализ ряда систем сигналов (OFDM-сигналов, сигналов с линейной частотной модуляцией (ЛЧМ), сложных нелинейных дискретных сигналов), применение которых позволяет улучшить показатели эффективности современных ИКС (помехоустойчивости приема, информационной безопасности, скрытности функционирования, защищенности от введения (навязывания) ложных сообщений фальсификации сообщений, обеспечения целостности данных, устойчивости к межсимвольной интерференции, информационной емкости системы при ограниченной полосе пропускания, скорости приема-передачи данных и т.д.). В работе на основе исследования алгебраической структуры систем нелинейных параметрических неравенств сформулирована и в общем виде решена задача синтеза одного из новых классов сложных нелинейных дискретных сигналов с заданными корреляционными, ансамблевыми и структурными свойствами, – криптографических сигналов. Представлены принципы построения и общая характеристика созданного программно-аппаратного комплекса для синтеза, исследования свойств, генерации, обработки и тестирования математических моделей ряда классов сигналов – физических переносчиков данных в современных ИКС.

Ключевые слова: помехоустойчивость приема; скрытность; информационная безопасность; дискретные последовательности; сложные системы сигналов; синтез систем сигналов; комплексное программное средство; интерфейс пользователя; шумоподобный сигнал.

Ил. 2. Библиогр.: 16 назв.

UDC 681.3.06:519.248.681

Methods and means of synthesis and generation of signals – physical carriers of data in modern information and communication systems / *I.D. Gorbenko, E.A. Semenko, A.A. Zamula* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 87 – 98.

The functioning of a number of modern information and communication systems (ICS) is carried out under conditions of external and internal influences caused, on the one hand, by the action of natural interference, interference from other radio systems operating at close frequencies or in a common part of the frequency range, on the other hand , interference created by counteraction stations for the purpose of electronic suppression of existing systems. Increasingly stringent requirements are imposed on the ICS, especially for critical purposes, to ensure the efficiency of their functioning: the reliability and rate of information transfer, survivability, noise immunity, information security. In such conditions, the availability and use of secure information and communication systems is of particular importance. Under the security of systems is understood, first of all, their ability to provide the necessary indicators for noise immunity, imitation resistance, information, energy and structural secrecy, information transfer rate, frequency and energy efficiency. The need to use secure radio channels forces researchers to look in a new way, both at the modes of functioning of secure radio channels, and at the aspects of the formation and use of complex signals – physical data carriers for such systems. The paper presents conceptual provisions for the construction of secure ICS, which determine the need for a system classification and unification of information flows to solve the problems of information formation and processing in ICS, systematization of models, methods, hardware and software for their implementation. The principles of building new technologies in the field of ICS should cover the entire spectrum of information transformations in a complex, from a source to a consumer, and should be based not only on the effective transfer of information, but also on ensuring secrecy, electromagnetic and other compatibility, ecology, information security, protection from imposing (introduction into the system) of erroneous data and so on. It is shown that one of the complex problems of creating protected ICS is the synthesis of a system of signals – physical data carriers. The paper gives the analysis of a number of signal systems (OFDM – signals, signals with linear frequency modulation (LFM), complex nonlinear discrete signals), the use of which makes it possible to improve the efficiency indicators of modern ICS (reception noise immunity, information security, secrecy of functioning, protection from the introduction (imposition) of false messages, falsification of messages, ensuring data integrity, resistance to intersymbol interference, information capacity of the system with limited bandwidth, data transmission speed, etc.). In this paper, based on the study of the algebraic structure of systems of nonlinear parametric inequalities, the problem of synthesizing one of the new classes of complex nonlinear discrete signals with given correlation, ensemble and structural properties, cryptographic signals, is formulated and solved in a general form. The principles of construction and general characteristics of the created software and hardware complex for the synthesis, study of properties, generation, processing and testing of mathematical models of a number of classes of signals – physical data carriers in modern ICS.

Key words: reception immunity; secrecy; information security; discrete sequences; complex signal systems; synthesis of signal systems; complex software tool; user interface; noise-like signal.

2 fig. Ref: 16 items.

УДК 681.3.067+621.396.626:537.87

Врахування інтерференційної складової в технічному каналі витоку інформації побічного електромагнітного випромінювання відеотракту при рознесених прийомі / *В.Р. Воронов, В.І. Заболотний, В.І. Лиско* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 99 – 105.

Національними стандартами України, іншими нормативно-правовими документами системи технічного захисту інформації пропонується здійснювати захист відомостей, що становлять державну та іншу таємницю на об'єктах інформаційної діяльності організацій і установ всіх форм власності. Одним з небезпечних технічних каналів витоку інформації є канал побічних електромагнітних випромінювань відеотракту засобів електронно-обчислювальної техніки. Важливим елементом такого каналу є засоби радіо-, радіотехнічної розвідки, що використовуються зацікавленою стороною для перехоплення побічних електромагнітних випромінювань. Одним із напрямів удосконалення застосування засобів розвідки є рознесений прийом побічних електромагнітних випромінювань. При оцінці можливостей рознесеного прийому необхідно враховувати явища інтерференції відбитого від поверхні землі сигналу з сигналом прямого поширення від засобу електронно-обчислювальної техніки до прийомних антен розвідки.

Стаття присвячена аналізу необхідності врахування інтерференційного множника поширення електромагнітних полів при оцінці можливості ведення розвідки побічних електромагнітних випромінювань при рознесеному прийомі. Визначено підходи для врахування чинників впливу на інтерференцію ПЕМВ. Запропоновано складові частини кількісної моделі технічного каналу витоку інформації, що дозволяють проводити врахування факторів, що впливають на співвідношення сигнал/шум сигналу, що сприймається апаратурою розвідки.

Ключові слова: побічні електромагнітні випромінювання; інтерференція радіосигналів; рознесений прийом; сигнал / шум.

Іл. 4. Бібліогр.: 7 назв.

УДК 681.3.067+621.396.626:537.87

Учет интерференционной составляющей в техническом канале утечки информации побочного электромагнитного излучения видеотракта при разнесенном приеме / *В.Р. Воронов, В.И. Заболотный, В.И. Лыско* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 99 – 105.

Национальными стандартам Украины, другими нормативно-правовыми документами системы технической защиты информации предписывается осуществлять защиту сведений, составляющих государственную и другую тайну на объектах информационной деятельности организаций и учреждений всех форм собственности. Одним из опасных технических каналов утечки информации является канал побочных электромагнитных излучений видеотракта средств электронно-вычислительной техники. Важным элементом такого канала являются средства радио-, радиотехнической разведки, используемые заинтересованной стороной для перехвата побочных электромагнитных излучений. Одним из направлений совершенствования применения средств разведки является разнесенный прием побочных электромагнитных излучений. При оценке возможностей разнесенного приема необходимо учитывать также явления интерференции отраженного от поверхности земли сигнала с сигналом прямого распространения от средства электронно-вычислительной техники к приемным антеннам разведки.

Статья посвящена анализу необходимости учета интерференционного множителя распространения электромагнитных полей при оценке возможности ведения разведки побочных электромагнитных излучений при разнесенном приеме. Определены подходы для учета факторов влияния на интерференцию ПЭМВ. Предложены составные части количественной модели технического канала утечки информации, позволяющие проводить учет факторов, влияющих на соотношение сигнал/шум разведываемого сигнала в аппаратуре разведки.

Ключевые слова: побочные электромагнитные излучения; интерференция радиосигналов; разнесенный прием; сигнал/шум,

Ил. 4. Библиогр.: 7 назв.

UDC 681.3.067+621.396.626:537.87

Accounting for the interference component in the technical channel of information leakage of spurious electromagnetic radiation in the video path with diversity reception / *V.R. Voronov, V.I. Zabolotny, V.I. Lysko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 99 – 105.

National standards of Ukraine, other legal documents of the system of technical protection of information propose to protect information that is a state and other secret on the objects of information activities of organizations and institutions of all forms of ownership. One of the dangerous technical channels of information leakage is the channel of incidental electromagnetic radiation of the video path of electronic computing equipment. An important element of such a channel is the means of radio and radio intelligence used by the stakeholder to intercept spurious electromagnetic radiation. Intelligence tools are evolving and improving. One of the ways to improve the use of intelligence is the remote reception of incidental electromagnetic radiation. When assessing the possibilities of spaced reception, it is also necessary to take into account the phenomena of interference of the signal reflected from the earth's surface with the signal of direct propagation from the computer to the reconnaissance antennas.

The article is devoted to the analysis of the need to take into account the interference multiplier of electromagnetic field propagation when estimating the possibility of conducting reconnaissance of incidental electromagnetic radiation at spaced reception. Approaches to take into account the factors influencing the interference of PEMV are identified.

The components of the quantitative model of the technical channel of information leakage are proposed, which allow taking into account the factors influencing the signal/noise ratio of the signal perceived by the intelligence equipment.

Key words: spurious electromagnetic radiation; interference of radio signals; spaced reception; signal/noise.

4 fig. Ref: 7 items.

УДК 621.391

Комплексне вирішення проблеми електромагнітної сумісності сучасних інформаційно-комунікаційних систем / *І.Д. Горбенко, О.А. Замула, Хо Чі Лик* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 106 – 115.

Проаналізовано проблематику електромагнітної сумісності (ЕМС) інформаційно-комунікаційних систем (ІКС), розрахованих на багато користувачів, що використовують в якості способу надання доступу безлічі абонентів до ресурсів системи кодове розділення, при якому кожен абонент займає всю частотну смугу і весь часовий інтервал. Показано, що проблема електромагнітної сумісності ІКС як можливість безконфліктного існування різних бездротових ІКС в умовах, коли кожна з цих систем має можливість приймати свої сигнали і сигнали інших систем, є однією з найбільш пріоритетних при проєктуванні і експлуатації таких систем. Показана можливість реалізації вимог ЕМС на основі застосування широкосмугових шумоподібних сигналів (ШСС) в якості сигналів синхронізації і сигналів – фізичних переносників даних в умовах різних впливів, що заважають, в тому числі: вузькосмугових, широкосмугових загороджувальних, внутрішньосистемних (імітаційних, ретрансльованих) та інших завад, що створюються сусідніми станціями. Така можливість забезпечується завдяки застосуванню сигналів з великим значенням частотно-часового добутку (бази сигналу) без збільшення тривалості сигналу і пікової потужності випромінювання. На основі використання критерію розрізнення сигналів – мінімуму середньоквадратичної відстані між сигналами (векторами), сформульовані вимоги до синтезу і вибору класів ШСС, що забезпечують виконання вимог ЕМС бездротових систем зв'язку, розрахованих на багато користувачів. В якості сигналів-переносників даних і сигналів синхронізації запропоновано новий клас складних нелінійних дискретних криптографічних сигналів. Показано, що використання таких сигналів внаслідок того, що вони мають поліпшені ансамблеві, кореляційні, структурні властивості, дозволить здійснити комплексне вирішення проблеми ЕМС сучасних ІКС.

Ключові слова: електромагнітна сумісність; функція кореляції; дискретні послідовності; синтез систем сигналів; шумоподібний сигнал, оцінка параметрів сигналу; завадостійкість прийому сигналів; криптографічний сигнал; база сигналу; спектр частот.

Табл. 2. Бібліогр.: 10 назв.

УДК 621.391

Комплексное решение проблемы электромагнитной совместимости современных информационно-коммуникационных систем / *И.Д. Горбенко, А.А. Замула, Хо Чи Лык* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 106 – 115.

Проведен анализ проблематики электромагнитной совместимости (ЭМС) многопользовательских информационно-коммуникационных систем (ИКС), использующих в качестве способа предоставления доступа множества абонентов к ресурсам системы кодовое разделение, при котором каждый абонент занимает всю частотную полосу и весь временной интервал. Показано, что проблема электромагнитной совместимости ИКС как возможность бесконфликтного существования различных беспроводных ИКС в условиях, когда каждая из этих систем имеет возможность принимать свои сигналы и сигналы других систем, является одной из наиболее приоритетных при проектировании и эксплуатации таких систем. Показана возможность реализации требований ЭМС на основе применения широкополосных шумоподобных сигналов (ШШС) в качестве сигналов синхронизации и сигналов – физических переносчиков данных в условиях различных мешающих воздействий, в том числе: узкополосных, широкополосных заградительных, внутрисистемных (имитационных, ретранслированных) и других помех, создаваемыми соседствующими станциями. Такая возможность обеспечивается благодаря применению сигналов с большим значением частотно-временного произведения (базы сигнала) без увеличения длительности сигнала и пиковой мощности излучения. На основе использования критерия различимости сигналов – минимума среднеквадратического расстояния между сигналами (векторами) сформулированы требования к синтезу и выбору классов ШШС, обеспечивающих выполнение требований ЭМС многопользовательских беспроводных систем связи. Предложен, в качестве сигналов-переносчиков данных и сигналов синхронизации, новый класс сложных нелинейных дискретных криптографических сигналов. Показано, что использование таких сигналов вследствие того, что они обладают улучшенными ансамблевыми, корреляционными, структурными свойствами, позволит осуществить комплексное решение проблемы ЭМС современных ИКС.

Ключевые слова: электромагнитная совместимость; функция корреляции; дискретные последовательности; синтез систем сигналов; шумоподобный сигнал, оценка параметров сигнала; помехоустойчивость приема сигналов; криптографический сигнал; база сигнала; спектр частот.

Табл. 2. Библиогр.: 10 назв.

UDC 621.391

Comprehensive solution to the problem of electromagnetic compatibility of modern information and communication systems / *I.D. Gorbenko, A.A. Zamula, Ho Tri Luc* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 106 – 115.

The analysis of the problems of electromagnetic compatibility (EMC) of multi-user information and communication systems (ICS), using code division as a way of providing multiple subscribers access to system resources, in which each subscriber occupies the entire frequency band and the entire time interval. It is shown that the problem of electromagnetic compatibility of ICS as the possibility of a conflict-free existence of various wireless ICS in the conditions when each of these systems has the ability to receive its signals and signals of other systems is one of the highest priorities in the design and operation of such systems. It is shown that EMC requirements can be realized through the use of broadband noise-like signals (BNLS) as synchronization signals and signals – physical data carriers under various interfering influences, including narrow-band, wide-band obstruction, intrasystem (imitated, relayed) and other interferences caused by neighboring stations. This possibility is provided due to the use of signals with a large value of the time-frequency product (signal base) without increasing the signal duration and peak radiation power. Based on the use of the criterion of distinguishability of the signals of the minimum root mean square distance between the signals (vectors), the requirements for the synthesis and selection of the BNLS classes are formulated to ensure that the EMC requirements of multi-user wireless communication systems are met. A new class of complex nonlinear discrete cryptographic signals is proposed as data carrier signals and synchronization signals. It is shown that the use of such signals, due to the fact that they have improved ensemble, correlation, and structural properties, will allow for a comprehensive solution to the EMC problem of modern ICS.

Key words: electromagnetic compatibility; correlation function; discrete sequences; synthesis of signal systems; noise-like signal, estimation of signal parameters; noise immunity of signal reception; cryptographic signal; signal base; frequency spectrum.

2 tab. Ref: 10 items.

УДК 681.3.06

Математична модель випадкової підстановки / *К.Є. Лисицький, І.В. Лисицька* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 116 – 124.

Обговорюються підходи до відбору випадкових підстановок, засновані на застосуванні системи критеріїв, побудованих з використанням оцінок близькості законів розподілу XOR таблиць і таблиць зміщень лінійних апроксимацій підстановок теоретичним законам, притаманним випадковим підстановкам. Відзначається їх неконструктивність. Неясно, які ж показники відбору є кращими.

Викладається сутність уточненої нами методики визначення законів розподілу максимумів для великих за обсягом вибірок незалежних однаково розподілених випадкових величин. Відзначається, що розподіл максимумів великих за обсягом вибірок незалежних однаково розподілених випадкових величин добре вивчено в теорії ймовірностей і описується розподілом екстремальних значень Фішера – Тіппета або log-Вейбула. Методика застосовується для визначення законів розподілів максимумів XOR таблиць і максимумів зсувів таблиць лінійних апроксимацій вибірки з байтових випадкових підстановок. Результати розрахунків порівнюються з результатами експериментів. Результати розрахунків і експериментів свідчать про те, що в обох випадках розподілу концентруються навколо досить виражених максимумів з цілком певними одними і тими ж найбільш ймовірними значеннями, що дозволяють вважати, що випадково згенеровані підстановки з великою ймовірністю будуть за значеннями максимумів мало відрізнятися один від одного.

На основі отриманих результатів пропонується уточнене визначення випадкової підстановки, яке будується на властивостях вибірки випадкових підстановок.

Відзначається, що застосування випадкових підстановок призводить до збільшення числа циклів приходу шифрів до стану випадкової підстановки на один цикл.

Робиться висновок, що випадкові підстановки, взяті з виходу генератора випадкових підстановок без всяких обмежень, цілком можуть конкурувати з кращими відомими конструкціями S-блоків, що використовуються в сучасних шифрах. Збільшені в порівнянні з граничними значення максимумів, до яких прагнуть автори більшості робіт з пошуку S-блоків з поліпшеними показниками, можуть бути компенсовані використанням в шифрі циклових функцій зі збільшеним числом S-блоків, що активізуються, на перших циклах.

Ключові слова: симетричний шифр; алгебраїчний імунітет; нелінійний вузол заміни; булева функція; закон розподілу максимумів; модель випадкової підстановки.

Табл. 4. Бібліогр.: 24 назв.

УДК 681.3.06

Математическая модель случайной подстановки / *К.Е. Лисицкий, И.В. Лисицкая* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 116 – 124.

Обсуждаются подходы к отбору случайных подстановок, основанные на применении системы критериев, построенных с использованием оценок близости законов распределения XOR таблиц и таблиц смещений линейных аппроксимаций подстановок теоретическим законам, присущим случайным подстановкам. Отмечается их неконструктивность. Неясно, какие же показатели отбора являются предпочтительными.

Излагается сущность уточненной нами методики определения законов распределения максимумов для больших по объему выборок независимых одинаково распределенных случайных величин. Отмечается, что распределение максимумов больших по объему выборок независимых одинаково распределенных случайных величин хорошо изучено в теории вероятностей и описывается распределением экстремальных значений Фишера – Типпета или log-Вейбула. Методика применяется для определения законов распределений максимумов XOR таблиц и максимумов смещений таблиц линейных аппроксимаций выборки из байтовых случайных подстановок. Результаты расчетов сравниваются с результатами экспериментов. Результаты расчетов и экспериментов свидетельствуют о том, что в обоих случаях распределения концентрируются вокруг достаточно выраженных максимумов с вполне определенными одними и теми же наиболее вероятными значениями, позволяющими считать, что случайно генерируемые подстановки с большой вероятностью будут по значениям максимумов мало отличаться друг от друга.

На основе полученных результатов предлагается уточненное определение случайной подстановки, которое строится на свойствах выборки случайных подстановок.

Отмечается, что применение случайных подстановок приводит к увеличению числа циклов прихода шифров к состоянию случайной подстановки на один цикл.

Делается вывод, что случайные подстановки, взятые с выхода генератора случайных подстановок без всяких ограничений, вполне могут конкурировать с лучшими известными конструкциями S-блоков, используемыми в современных шифрах. Увеличенные по сравнению с предельными значения максимумов, к которым стремятся авторы большинства работ по поиску S-блоков с улучшенными показателями, могут быть компенсированы использованием в шифрах цикловых функций с увеличенным числом активизируемых S-блоков на первых циклах.

Ключевые слова: симметричный шифр; алгебраический иммунитет; нелинейный узел замены; булева функция; закон распределения максимумов; модель случайной подстановки.

Табл. 4. Библиогр.: 24 назв.

UDC 681.3.06

Mathematical model of random substitution / *K. Lisitsky, I.V. Lysitskya* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 116 – 124.

Approaches to the selection of random substitutions based on the application of a system of criteria constructed using estimates of the proximity of distribution laws of XOR tables and tables of displacements of linear approximations of substitutions to theoretical laws inherent in random substitutions are discussed. Their non-constructiveness is noted. It is not clear which selection rates are preferred.

The essence of our refined methodology for determining the laws of distribution of maxima for large samples of independent identically distributed random variables is stated. It is noted that the distribution of the maxima of large samples of independent identically distributed random variables is well studied in probability theory and is described by the distribution of Fisher-Tippett or log-Weibull extreme values. The technique is used to determine the laws of distribution of the maximums of XOR tables and the maximum of displacements of tables of linear approximations of a sample from byte random substitutions. The calculation results are compared with the experimental results. The results of calculations and experiments indicate that, in both cases, the distributions are concentrated around sufficiently pronounced maxima with quite definite and the same most probable values, which make it possible to assume that randomly generated substitutions with a high probability will differ little from each other in the values of the maxima.

Based on the results obtained, a refined definition of random substitution is proposed, which is based on the properties of a sample of random substitutions.

It is noted that the use of random substitutions leads to an increase in the number of cycles of arrival of ciphers to the state of random substitution by one cycle.

It is concluded that random substitutions taken from the output of a random substitution generator without any restrictions can compete with the best known S-box constructions used in modern ciphers. The maxima that are increased in comparison with the limiting values, which the authors of most works on the search for S-boxes with improved indicators strive for, can be compensated for by using cyclic functions in ciphers with an increased number of activated S-boxes in the first cycles.

Key words: symmetric cipher; algebraic immunity; non-linear replacement node; boolean function; distribution law of maxima; random substitution model.

4 tab. Ref: 24 items.

ОБРОБКА СИГНАЛІВ В РАДІОТЕХНІЧНИХ СИСТЕМАХ
ОБРАБОТКА СИГНАЛОВ В РАДИОТЕХНИЧЕСКИХ СИСТЕМАХ
SIGNAL PROCESSING IN RADIO ENGINEERING SYSTEMS

УДК 621.397

Обробка сигналів при пеленгації і визначенні дальності до малорозмірних БПЛА в оптичному і інфрачервоному діапазонах / *І.В. Корытцев, С.О. Шейко, В.М. Карташов, О.В. Зубков, В.М. Олейніков, С.І. Бабкін, І.С. Селезньов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 125 – 135.

Виявлення та оцінка координат БПЛА має вирішальне значення для захисту від їх несанкціонованого застосування в охоронюваних зонах. В роботі розглядається задача вибору алгоритму і параметрів обробки відеозображень стереопари в видимому, ближньому або дальньому інфрачервоному діапазонах для надійного визначення координат малих БПЛА, їх подальшого автосупроводу і оцінки параметрів руху. Проведено теоретичний аналіз можливостей оптичного методу двоканального стереовідеоспостереження. Представлено результати натурних експериментів з визначення координат малого БПЛА DJI Phantom 4 за допомогою системи стереовідеоспостереження на основі IP камер. Проведено калібрування зовнішніх і внутрішніх параметрів системи стереовідеоспостереження з урахуванням нелінійних спотворень об'єктивів. Калібрування камер здійснювалася в OpenCV за допомогою функції, заснованої на методах Zhang і Bouguet. Визначено теоретичні та практичні похибки вимірювання дальності до тестових об'єктів при їх різних положеннях. Описано алгоритм обробки зображень системи стереовідеоспостереження для виявлення, розпізнавання і вимірювання координат БПЛА. Наведено результати вимірювань координат БПЛА у двох тестових польотах. Вимірювання істинних координат БПЛА здійснювалося за даними бортового GPS приймача. Результати вимірювання азимута і кута місця БПЛА системою стереовідеоспостереження добре збігаються з даними GPS приймача. Це пояснюється високою роздільною здатністю камер і точним калібруванням їх внутрішніх параметрів. Середньоквадратична відносна похибка вимірювання дальності склала близько 10 %. Вказано шляхи для поліпшення точностних показників систем стереовідеоспостереження БПЛА.

Ключові слова: БПЛА; відеокамера; дальність; дрон; координати; виявлення; розпізнавання; ректифікація; стереобачення; трекінг.

Іл. 10. Бібліогр.: 24 назв.

УДК 621.397

Обработка сигналов при пеленгации и определении дальности до малоразмерных БПЛА в оптическом и инфракрасном диапазонах / *И.В. Корытцев, С.А. Шейко, В.М. Карташов, О.В. Зубков, В.Н. Олейников, С.И. Бабкин, И.С. Селезнев* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 125 – 135.

Обнаружение и оценка координат БПЛА имеет решающее значение для защиты от их несанкционированного применения в охраняемых зонах. В работе рассматривается задача выбора алгоритма и параметров обработки видеоизображений стереопары в видимом, ближнем или дальнем инфракрасном диапазонах для надежного определения координат малых БПЛА, их последующего автосопровождения и оценки параметров движения. Проведен теоретический анализ возможностей оптического метода двуканального стереовидеонаблюдения. Представлены результаты натурных экспериментов по определению координат малого БПЛА DJI Phantom 4 с помощью системы стереовидеонаблюдения на основе IP камер. Проведена калибровка внешних и внутренних параметров системы стереовидеонаблюдения с учетом нелинейных искажений объективов. Калибровка камер осуществлялась в OpenCV при помощи функции, основанной на методах Zhang и Bouguet. Определены теоретические и практические погрешности измерения дальности до тестовых объектов при различных их положениях. Описан алгоритм обработки изображений системы стереовидеонаблюдения для обнаружения, распознавания и измерения координат БПЛА. Приведены результаты измерений координат БПЛА по двум тестовым полетам. Измерение истинных координат БПЛА осуществлялось по данным бортового GPS приемника. Результаты измерения азимута и угла места БПЛА системой стереовидеонаблюдения хорошо совпадают с данными GPS приемника. Это объясняется высокой разрешающей способностью камер и точной калибровкой их внутренних параметров. Среднеквадратическая относительная ошибка измерения дальности составила около 10 %. Указаны пути для улучшения точностных показателей систем стереовидеонаблюдения БПЛА.

Ключевые слова: БПЛА; видеокамера; дальность; дрон; координаты; обнаружение; распознавание; ректификация; стереовидение; трекинг.

Ил. 10. Библиогр.: 24 назв.

UDC 621.397

Signal processing for direction finding and range determining to small UAVs in the optical and infrared ranges / *I.V. Koryttsev, S.O. Sheiko, V.M. Kartashov, O.V. Zubkov, V.M. Oleynikov, S.I. Babkin, I.S. Selieznov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 125 – 135.

Detection and assessment of UAV coordinates is critical to protect against their unauthorized use in protected areas. The paper considers the problem of choosing the algorithm and parameters of stereo pair video processing in the visible, near-infrared and far-infrared ranges for reliable determination of small UAVs coordinates, further tracking of them and evaluation of UAVs motion parameters. Theoretical analysis of the optical method possibilities for two-channel stereo-video observation is carried out. The paper presents the results of field experiments aimed to determine the coordinates of a small UAV DJI Phantom 4 using a stereo-video observation system based on IP cameras. The external and internal parameters of the stereo-video observation system were calibrated taking into account the nonlinear distortions of the lenses. The cameras were calibrated in OpenCV using a function based on Zhang and Bouguet methods. The theoretical and practical errors in measuring the range to test objects at their different positions were determined. An algorithm for image processing of a stereo-video observation system for detection, recognition and measurement of UAV coordinates is described. The results of measurements of UAV coordinates for two test flights are presented. The measurement of the true coordinates of the UAV was carried out according to the data of the onboard GPS receiver. The results of measuring the azimuth and elevation of the UAV by the stereo-video observation system were matched with the data of the GPS receiver. This fact can be explained by high resolution of the cameras and the precise

calibration of their internal parameters. The root-mean-square relative error in measuring the range was about 10%. Ways for improving the accuracy of UAV stereo-video observation systems are shown.

Key words: UAV; video camera; range; drone; coordinates; detection; recognition; rectification; stereo vision; tracking.

10 fig. Ref: 24 items.

УДК 629.7.022

Дослідженнефективності детектування та розпізнавання зображень дронів за відеопотоком / *О.В. Зубков, С.О. Шейко, В.М. Олейніков, В.М. Карташов, І.В. Коритцев, С.І. Бабкін* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 136 – 146.

Розроблено та експериментально протестовано алгоритм обробки відеопотоку стаціонарної відеокамери. Він складається з етапів виявлення рухомих об'єктів і класифікації цих об'єктів з використанням нейронної мережі. Для виявлення рухомих об'єктів використано методи виділення рухомих об'єктів на нерухомому фоні і аналізу історії руху. На підставі експериментальних даних проаналізовано ефективність застосування моделей заднього фону зображень MOG, MOG2, KNN, GMG, CNT, GSOC, LSBP для вирішення поставленого завдання. Сформульовано рекомендації щодо вибору параметрів цих моделей. Критеріями вибору були: забезпечення високої швидкодії і низький рівень шумів. Для класифікації рухомих об'єктів створено і навченомоделі повнозв'язних і згортальних нейронних мереж, що дозволяють класифікувати 12 типів рухомих об'єктів. Для навчання нейронних мереж створено набори зображень: дронів, фрагментів листя дерев, трави, хмар і комах. На підставі результатів навчання та тестування мереж надано рекомендації до числа шарів мереж, числу нейронів в шарі, кількості згорток для досягнення максимальної швидкодії і точності розпізнавання. Порівняльний аналіз точності класифікації дронів із застосуванням повнозв'язних і згортальних мереж при обробці експериментальних даних довів ефективність застосування згортальних мереж. Побудовано залежність точності виявлення дрона від розміру зображення і, відповідно, від дальності до цього дрона.

Ключові слова: дослідження; ефективність; детектування; розпізнавання; зображення; дрон; відеопотік.

Табл. 3. Іл. 7. Бібліогр.: 20 назв.

УДК 629.7.022

Исследование эффективности детектированияи распознавания изображений дронов по видеопотоку / *О.В. Зубков, С.А. Шейко, В.Н. Олейников, В.М. Карташов, И.В. Корытцев, С.И. Бабкин* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 136 – 146.

Разработан и экспериментально протестирован алгоритм обработки видеопотока стационарной видеокамеры. Он состоит из этапов обнаружения движущихся объектов и классификации этих объектов с использованием нейронной сети. Для обнаружения движущихся объектов использованы методы выделения движущихся объектов на неподвижном фоне и анализа истории движения. На основании экспериментальных данных проанализирована эффективность применения моделей заднего фона изображений MOG, MOG2, KNN, GMG, CNT, GSOC, LSBP для решения поставленной задачи. Сформулированы рекомендации по выбору параметров этих моделей. Критерии выбора: обеспечение высокого быстродействия и низкий уровень шумов. Для классификации движущихся объектов созданы и обучены модели полносвязных и сверточных нейронных сетей, позволяющие классифицировать 12 типов подвижных объектов. Для обучения нейронных сетей созданы наборы изображений: дронов, фрагментов листвы деревьев, травы, облаков и насекомых. На основании результатов обучения и тестирования сетей даны рекомендации к числу слоев сетей, числу нейронов в слое, количеству сверток для достижения максимального быстродействия и точности распознавания. Сравнительный анализ точности классификации дронов с применением полносвязных и сверточных сетей при обработке экспериментальных данных доказал эффективность применения сверточных сетей. Построена зависимость точности обнаружения дрона от размера изображения и, соответственно, от дальности до этого дрона.

Ключевые слова: исследование; эффективность; детектирование; распознавание; изображение; дрон, видеопоток.

Табл. 3. Ил. 7. Библиогр.: 20 назв.

UDC 629.7.022

Study of the efficiency of detecting and recognizing drone images from a video stream / *O.V. Zubkov, S.A. Sheyko, V.N. Oleynikov, V.M. Kartashov, I.V. Korytsev, S.I. Babkin* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 136 – 146.

The authors have developed and experimentally tested an algorithm for processing a video stream of a stationary video camera. It consists of the stages of detecting moving objects and classifying these objects using a neural network. To detect moving objects, the methods of identifying moving objects against a stationary background and analyzing the history of motion were used. Based on the experimental data, the effectiveness of using the models of the background images of MOG, MOG2, KNN, GMG, CNT, GSOC, LSBP for solving the problem was analyzed. Recommendations for the choice of the parameters of these models were formulated. The selection criteria were as follows: high performance and low noise. Models of fully connected and convolutional neural networks were created and trained making it possible to classify 12 types of moving objects. Sets of images were created to train neural networks: drones, fragments of tree foliage, grass, clouds and insects. Based on the results of training and testing networks, recommendations are

given for the number of network layers, the number of neurons in a layer, the number of convolutions to achieve maximum performance and recognition accuracy. Comparative analysis of the accuracy of drone classification using fully connected and convolutional networks when processing experimental data has proven the effectiveness of using convolutional networks. The dependence of the drone detection accuracy on the image size and, accordingly, on the distance to this drone is plotted.

Key words: research; efficiency; detection; recognition; image; drone; video stream.

3 tab. 7 fig. Ref: 20 items.

УДК 551.501.7

Аналіз частотно-часової структури акустичних шумів малих автоматичних аеросистем / *В.І. Леонідов, В.В. Семенець* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 147 – 152.

Формулюється постановка завдання виявлення малих автоматичних аеросистем (дронов), обґрунтовується доцільність побудови системи виявлення дронів на принципі прийому й аналізу акустичних сигналів, що випромінюються дронами під час виконання ними польотного завдання.

Дослідження часових флуктуацій періоду акустичних сигналів дрона проводиться методом модельно-кореляційного аналізу, у результаті якого формуються тривимірні структури: час – період – коефіцієнт кореляції акустичного сигналу з моделлю у вигляді обмеженої в часі синусоїдальної функції.

Отримані структури формуються у вигляді матриць значень коефіцієнта кореляції.

Члени, які розташовуються уздовж стовпців, розраховані при часовому зрушенні модельної функції уздовж вибірки сигналу. Члени в кожному стовпці розраховані при постійному, заданому з ряду значень, періоді модельної функції.

Показано, що коефіцієнти кореляції між рядками матриць, розрахованих по сигналах дрона значно більше, ніж ті ж значення, що отримані по вимірах фонового шуму. Функції, що показують зміну в часі коефіцієнтів кореляції між рядками матриць структур час – період для сигналів дрона й фонового шуму, не перетинаються й показують стійко більшу різницю коефіцієнтів кореляції, що дозволяє використати коефіцієнт кореляції як ознака що класифікує при розпізнаванні сигналів дрона.

Ключові слова: автоматичні аеросистеми; акустичний шум; кореляційний аналіз; модель сигналу; ознака.

Іл. 4. Бібліогр.: 12 назв.

УДК 551.501.7

Анализ частотно-временной структуры акустических шумов малых автоматических аэросистем / *В.И. Леонидов, В.В. Семенец* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 147 – 152.

Формулируется постановка задачи обнаружения малых автоматических аэросистем (дронов), обосновывается целесообразность построения системы обнаружения дронов на принципе приема и анализа акустических сигналов, излучаемых дронами во время выполнения ими полетного задания.

Исследование временных флуктуаций периода акустических сигналов дрона проводится методом модельно-корреляционного анализа, в результате которого формируются трехмерные структуры время – период – коэффициент корреляции акустического сигнала с моделью в виде ограниченной во времени синусоидальной функции.

Полученные структуры формируются в виде матриц значений коэффициента корреляции.

Члены, которые располагаются вдоль столбцов, рассчитаны при временном сдвиге модельной функции вдоль выборки сигнала. Члены в каждом столбце рассчитаны при постоянном, заданном из ряда значений, периоде модельной функции.

Показано, что коэффициенты корреляции между строками матриц, рассчитанных по сигналам дрона, значительно больше, чем те же значения, полученные по измерениям фонового шума. Функции, показывающие изменение во времени коэффициентов корреляции между строками матриц структур время – период для сигналов дрона и фонового шума, не пересекаются и показывают устойчиво большую разность коэффициентов корреляции, что позволяет использовать коэффициент корреляции в качестве классифицирующего признака при распознавании сигналов дрона.

Ключевые слова: автоматические аэросистемы; акустический шум; корреляционный анализ; модель сигнала; классифицирующий признак.

Ил. 4. Библиогр.: 12 назв.

UDC 551.501.7

Analysis of frequency-time structure of acoustic noise of small automatic air systems / *V.I. Leonidov, V.V. Semenets* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 147 – 152.

The statement of the problem of detecting small automatic air systems (drones) is formulated, the expediency of building a drone detection system on the principle of receiving and analyzing acoustic signals emitted by drones during their flight mission is substantiated.

The study of temporal fluctuations of the period of the acoustic signals of the drone is carried out by the method of model-correlation analysis, as a result of which three-dimensional structures are formed: time – period – the correlation coefficient of the acoustic signal with the model in the form of a sinusoidal function limited in time.

The resulting structures are formed as matrices of correlation coefficient values.

The members located along the columns are calculated with the time shift of the model function along the signal sample. The members in each column are calculated for a constant period of the model function set from a number of values.

It is shown that the correlation coefficients between the matrix rows calculated from the drone signals are significantly higher than the same values obtained from the background noise measurements. The functions showing the change in time of the correlation coefficients between the rows of the matrices of the time – period structures for drone signals and background noise do not intersect and show a consistently large difference in the correlation coefficients, which allows the correlation coefficient to be used as a classifying feature when recognizing drone signals.

Key words: automatic air systems; acoustic noise; correlation analysis; signal model; classifying feature.

4 fig. Ref: 12 items.

УДК 629.7.022

Оптико-електронні методи виявлення повітряних об’єктів та вимірювання їхніх координат / *В.М. Карташов, І.В. Коритцев, С. О. Шейко, В.М. Олейніков, О.В. Зубков, С.І. Бабкін* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 153 – 159.

Проведено аналіз оптико-електронних методів (ОЕМ) з метою вибору і дослідження ОЕМ, здатного вирішувати завдання виявлення і визначення координат малих безпілотних літальних апаратів. Для даного застосування розглянуто різні ОЕМ вимірювання дальності до об'єктів. Оптико-електронні методи (ОЕМ) в режимах вимірювань характеризуються високою точністю, що обумовлює їх успішну інтеграцію з радіоелектронними комплексами різного призначення. Авторами запропоновано класифікувати ОЕМ за фізичним принципом на дві великі групи: активні і пасивні ОЕМ вимірювання дальності. Оцінено інтерференційні і модуляційні методи. Розглянуті активні методи мають високу точність, але вимагають значних енергетичних витрат і не забезпечують скритність роботи. Більш глибоко розглянуто пасивні ОЕМ вимірювання дальності. ОЕМ з матричними сенсорами поділяються на однокамерні і стереоскопічні. Особливий інтерес представляють методи, які не потребують участі зорового апарату людини в знятті вимірювальних відліків і забезпечують повну автоматизацію прийняття рішення. Розглянуті фоточутливі сенсори, що виявляють повітряні об'єкти, як вдень, так і вночі, мають матричну структуру і можуть бути інтегровані в єдину оптико-електронну систему виявлення і вимірювання дальності. Перевагою матричних ОЕМ є можливість одночасного використання всіх трьох датчиків денного, нічного та теплового бачення, що дозволить проводити надійне виявлення, розпізнавання та вимірювання координат малих повітряних об'єктів.

Ключові слова: оптика; електрон; метод; виявлення; повітря; об’єкт; вимірювання; координата.

Іл. 1. Бібліогр.: 32 назв.

УДК 629.7.022

Оптико-электронные методы обнаружения воздушных объектов и измерения их координат / *В.М. Карташов, И.В. Корытцев, С. А. Шейко, В.Н. Олейников, О.В. Зубков, С.И. Бабкин* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 153 – 159.

Проведен анализ оптико-электронных методов (ОЭМ) с целью выбора и исследования ОЭМ, способного решать задачи обнаружения и определения координат малых беспилотных летательных аппаратов. Для данного применения рассмотрены различные ОЭМ измерения дальности до объектов. Оптико-электронные методы (ОЭМ) в режимах измерений характеризуются высокой точностью, что обусловливает их успешную интеграцию с радиоэлектронными комплексами разного назначения. Авторами предложено классифицировать ОЭМ по физическому принципу на две большие группы: активные и пассивные ОЭМ измерения дальности. Оценены интерференционные и модуляционные методы. Рассмотренные активные методы обладают высокой точностью, но требуют значительных энергетических затрат и не обеспечивают скрытность работы. Более глубоко рассмотрены пассивные ОЭМ измерения дальности. ОЭМ с матричными сенсорами подразделяются на однокамерные и стереоскопические. Особый интерес представляют методы, не требующие участия зрительного аппарата человека в снятии измерительных отсчетов и обеспечивающие полную автоматизацию принятия решения. Рассмотренные фоточувствительные сенсоры, выявляющие воздушные объекты, как днем, так и ночью, имеют матричную структуру и могут быть интегрированы в единую оптико-электронную систему обнаружения и измерения дальности. Достоинством матричных ОЭМ является возможность одновременного использования всех трех датчиков дневного, ночного и теплового видения, что позволит проводить надежное обнаружение, распознавание и измерение координат малых воздушных объектов.

Ключевые слова: оптика; электрон; метод; обнаружение; воздух; объект; измерение; координата.

Ил. 1. Библиогр.: 32 назв.

UDC 629.7.022

Optoelectronic methods for detecting air objects and measuring their coordinates / *V.M. Kartashov, I.V. Korytsev, S.A. Sheyko, V.N. Oleynikov, O.V. Zubkov, S.I. Babkin* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 153 – 159.

The analysis of optical-electronic methods (OEM) is carried out in order to select and study an OEM capable of solving the problems of detecting and determining the coordinates of small unmanned aerial vehicles. With this aim in view, various OEM measurements of distance to objects are considered. Optoelectronic methods (OEM) in the meas-

urement modes are characterized by high accuracy, which leads to their successful integration with electronic complexes for various purposes. The authors proposed to classify the OEM according to the physical principle into two large groups: active and passive OEM for measuring range. Interference and modulation methods are evaluated. The considered active methods are highly accurate, but require significant energy consumption and do not provide secrecy of work. Passive OEM range measurements are considered in more depth. The OEM with matrix sensors are subdivided into single-chamber and stereoscopic. Methods, that do not require the participation of the human visual apparatus in taking measurement readings and provide complete automation of decision-making, are of particular interest. The considered photosensitive sensors that detect air objects, both day and night, have a matrix structure and can be integrated into a single optoelectronic system for detecting and measuring range. The advantage of the matrix OEM is the ability to use simultaneously all three sensors for day, night and thermal vision, which will allow reliable detection, recognition and measurement of coordinates of small air objects.

Key words: optics; electron; method; detection; air; object; measurement; coordinate.
1 fig. Ref: 32 items.

УДК 621391: 629.052.3: 551.510.535

Особливості застосування теореми відліків при обробці вузькосмугових радіосигналів з відомою центральною частотою спектра / *Є.В. Рогожкін, Ю.І. Под'ячий, Л.Я. Ємельянов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 160 – 163.

Представлено варіант дискретизації вузькосмугових радіосигналів з відомою центральною частотою спектра, який дозволяє значно зменшити обсяг обчислювальних операцій при обробці таких сигналів без істотних втрат інформації про їхні параметри. У даному випадку вузькосмужність визначається співвідношенням ширини спектру прийнятого радіолокаційного сигналу та робочої частоти підсилювача проміжної частоти, з виходу якого сигнал надходить до аналого-цифрового перетворювача (АЦП). Проведено дослідження запропонованого способу дискретизації, в якому частота слідування опитувальних імпульсів АЦП визначається частотою опорного сигналу задаючої системи когерентної РЛС і вибирається за величиною кратно нижче робочої частоти підсилювача проміжної частоти. Синхронізація опитувальних імпульсів АЦП організована так, що будь-які два сусідніх відліки є квадратурно пов'язаними. Така процедура дозволяє визначити амплітуду і фазу сигналу, що відповідають кожному відліку. Тим самим створюються умови для визначення доплерівського зсуву і параметрів огинаючої сигналу. Наведено результати розрахунку відносної похибки визначення амплітуди сигналу, яка утворюється в результаті незбігу частоти прийнятого сигналу з частотою опорного сигналу. Для реальних випадків вона не перевищує 1 % і залежить від характеристик РЛС (довжина зондуючої хвилі, кратність між значенням проміжної частоти, на якій ведеться обробка, і значенням частоти відліків), а також від величини радіальної швидкості об'єкта і початкової різниці фаз між сигналом на виході підсилювача проміжної частоти й опорним сигналом. Показано, що такий підхід до перетворення сигналу в цифровий формат може бути застосований і для сигналів з фазовою $(0, \pi)$ маніпуляцією, якщо тривалість елементів коду суттєво більше періоду опорної частоти.

Ключові слова: обробка радіолокаційних сигналів; синхронне детектування; аналого-цифрове перетворення; дискретизація сигналу; доплерівський зсув.
Табл. 1. Іл. 2. Бібліогр.: 8 назв.

УДК 621391: 629.052.3: 551.510.535

Особенности применения теоремы отсчетов при обработке узкополосных радиосигналов с известной центральной частотой спектра / *Е.В. Рогожкин, Ю.И. Подъячий, Л.Я. Емельянов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 160 – 163.

Представлен вариант дискретизации узкополосных радиосигналов с известной центральной частотой спектра, который позволяет значительно уменьшить объем вычислительных операций при обработке таких сигналов без существенных потерь информации об их параметрах. В рассматриваемом случае узкополосность определяется соотношением ширины спектра принимаемого радиолокационного сигнала и рабочей частоты усилителя промежуточной частоты, с выхода которого сигнал поступает на аналого-цифровой преобразователь (АЦП). Исследован предложенный способ дискретизации, в котором частота следования опросных импульсов АЦП определяется частотой опорного сигнала задающей системы когерентной РЛС и выбирается по величине кратно ниже рабочей частоты усилителя промежуточной частоты. Синхронизация опросных импульсов АЦП организована так, что любые два соседних отсчета квадратурно связаны. Такая процедура позволяет определить амплитуду и фазу принимаемого сигнала, соответствующие каждому отсчету. Тем самым создаются условия для определения доплеровского сдвига и параметров огибающей сигнала. Приведены результаты расчета относительной погрешности определения амплитуды сигнала, которая образуется в результате несовпадения частоты принятого сигнала с частотой опорного сигнала. Для реальных случаев она не превышает 1 % и зависит от характеристик РЛС (длина зондирующей волны, кратность между значением промежуточной частоты, на которой ведется обработка, и значеним частоты отсчетов), а также от величины радиальной скорости объекта и начальной разности фаз между сигналом на выходе усилителя промежуточной частоты и опорным сигналом. Показано, что такой подход к преобразованию сигнала в цифровой формат применим и для сигналов с фазовой $(0, \pi)$ манипуляцией, если длительность элементов кода существенно больше периода опорного сигнала.

Ключевые слова: обработка радиолокационных сигналов; синхронное детектирование; аналого-цифровое преобразование; дискретизация сигнала; доплеровский сдвиг.

Табл. 1. Ил. 2. Библиогр.: 8 назв.

UDC 621391: 629.052.3: 551.510.535

Features of application of the sampling theorem when processing narrow-band radio signals with known center frequency of the spectrum / *E.V. Rogozhkin, Yu.I. Podyachiy, L.Ya. Emelyanov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 160 – 163.

An option is presented for sampling narrow-band radio signals with a known center frequency of the spectrum, which can significantly reduce the amount of computational operations when processing such signals without significant loss of information about their parameters. In this case, narrowband is determined by the ratio of the spectrum width of the received radar signal and the operating frequency of the intermediate frequency amplifier, from the output of which the signal is fed to an analog-to-digital converter (ADC). A study of the proposed method of discretization is carried out, in which the repetition rate of the ADC interrogation pulses is determined by the frequency of the reference signal of the master system of a coherent radar and is selected multiple times lower than the operating frequency of the intermediate frequency amplifier. The synchronization of the ADC interrogation pulses is organized in such a way that any two adjacent samples are quadrature connected. This procedure allows you to determine the amplitude and phase of the received signal corresponding to each sample. This creates the conditions for determining the Doppler shift and envelope parameters of the signal. The results of calculating the relative error in determining the amplitude of the signal, which appears as a result of a mismatch in the frequency of the received signal with the frequency of the reference signal, are presented. For real cases, it does not exceed 1% and depends on the radar characteristics (sounding wavelength, multiplicity between the value of the intermediate frequency at which the processing is carried out, and the value of the sampling frequency), as well as on the magnitude of the object radial velocity and the initial phase difference between the output signal of the intermediate frequency amplifier and the reference signal. It is shown that this approach to converting the signal into a digital format is also applicable to signals with phase (0, π) manipulation if the duration of the code elements is significantly longer than the period of the reference signal.

Key words: processing of radar signals; synchronous detection; analog-to-digital conversion; signal sampling; Doppler shift.

1 tab. 2 fig. Ref: 8 items.

УДК 004.89: 621.396

Предикатна модель процесних знань при виявленні і розпізнаванні протяжних об'єктів типу хмари, «ангел-луна» в оглядових РЛС / *С.В. Солонська, В.В. Жирнов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 164 – 172.

Розроблено предикатну модель процесних знань міжперіодної обробки радіолокаційних сигналів при виявленні і розпізнаванні протяжних об'єктів і метод прийняття рішень, заснований на прецедентах. Наведено основні особливості і структурні елементи моделі процесних знань. Показано, що переваги даної моделі пов'язані з можливостями конфігурації і ієрархічного представлення процесу з вивчення можливих структур одиночних або груп імпульсних сигналів в межах однієї зони огляду РЛС на основі інтелектуального аналізу сигналів з використанням алгебри кінцевих предикатів. Показано, як цей підхід може використовуватися для автоматизації процесу виявлення і розпізнавання протяжних об'єктів типу хмари, атмосферні неоднорідності типу «ангел-луна». Розроблено метод обробки процесних знань як інструмент для створення універсальних алгоритмів міжперіодной обробки сигнальної інформації для забезпечення ефективного виявлення і розпізнавання різних протяжних об'єктів, в тому числі атмосферних неоднорідностей типу «ангел-луна», за рахунок накопичення як сигнальної (енергетичної), так і логічної інформації в комірці, що аналізується, та в її околу. В розроблену технологію входять процедури формалізації та аналізу символьної моделі спостережуваних об'єктів для прийняття рішень, заснованих на прецедентах. Залежно від типів зв'язків, які використовуються в моделі, розрізняють класифіковані і функціональні мережі, де використовуються деякі елементи логічних і мережевих моделей. З логічних моделей запозичена ідея правил виведення або вирішального правила, а з мережевих моделей – опис знань у вигляді семантичної нейронної мережі. У цієї комбінованої моделі явно виділена процедурна інформація. Замість логічного висновку з'являється висновок або вирішальне правило на знаннях. В результаті рішення системи предикатних рівнянь процесних знань знаходимо місце, геометричні розміри і вид символьної моделі протяжного об'єкта.

Ключові слова: модель процесних знань; прийняття рішень; рухомий об’єкт; виявлення; розпізнавання; інтелектуальна система; символьна модель сигнальних відміток.

Іл. 4. Бібліогр.: 13 назв.

УДК 004.89: 621.396

Предикатная модель процессных знаний при обнаружении и распознавании протяженных объектов типа облака, тучи, «ангел-эхо» в обзорных РЛС / *С.В. Солонская, В.В. Жирнов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 164 – 172.

Разработана предикатная модель процессных знаний межпериодной обработки радиолокационных сигналов при обнаружении и распознавании протяженных объектов и метод принятия решений, основанный на

прецедентах. Приведены основные особенности и структурные элементы модели процессных знаний. Показано, что преимущества данной модели связаны с возможностями конфигурирования и иерархического представления процесса по изучению возможных структур одиночных или групп импульсных сигналов в пределах одной зоны обзора РЛС на основе интеллектуального анализа сигналов с использованием алгебры конечных предикатов. Показано, как этот подход может использоваться для автоматизации процесса обнаружения и распознавания протяженных объектов типа облака, тучи, атмосферные неоднородности типа «ангел-эхо». Разработан метод обработки процессных знаний как инструмент для создания универсальных алгоритмов межпериодной обработки сигнальной информации для обеспечения эффективного обнаружения и распознавания разных протяженных объектов, в том числе атмосферных неоднородностей типа «ангел-эхо», за счет накопления как сигнальной (энергетической), так и логической информации в анализируемой ячейке и в ее окрестности. В разработанную технологию входят процедуры формализации и анализа символьной модели наблюдаемых объектов для принятия решений, основанных на прецедентах. В зависимости от типов связей, используемых в модели, различают классифицирующие и функциональные сети, где используются некоторые элементы логических и сетевых моделей. Из логических моделей заимствована идея правил вывода или решающего правила, а из сетевых моделей – описание знаний в виде семантической нейронной сети. В этой комбинированной модели явно выделена процедурная информация. Вместо логического вывода появляется вывод или решающее правило на знаниях. В результате решения системы предикатных уравнений процессных знаний находим место, геометрические размеры и вид символьной модели протяженного объекта.

Ключевые слова: модель процессных знаний; принятия решений; протяженный объект; обнаружение; распознавание; интеллектуальная система; символьная модель.

Ил. 4. Библиогр.: 13 назв.

UDC 004.89: 621.396

Predicate model of process knowledge when detecting and recognizing extended objects such as clouds, angel-echoes in surveillance radars / *S. Solonskaya, V. Zhyrnov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 164 – 172.

A predicate model of the process knowledge of inter-period processing of radar signals in the detection and recognition of extended objects and a decision-making method based on precedents have been developed. The main features and structural elements of the process knowledge model are presented. It is shown that the advantages of this model are related to the configuration and hierarchical representation of the process for studying the possible structures of single or groups of impulse signals within the same radar field of view based on the intelligent analysis of signals using the algebra of finite predicates. It is shown how this approach can be used to automate the process of detecting and recognizing extended objects such as clouds, atmospheric inhomogeneities of the angel-echo type. A method for processing process knowledge has been developed as a tool for creating universal algorithms for inter-period processing of signal information to ensure effective detection and recognition of various extended objects, including atmospheric inhomogeneities of the angel-echo type, by accumulating both signal (energy) and logical information in the analyzed cell and in its vicinity. The developed technology includes procedures for formalizing and analyzing the symbolic model of observed objects for making decisions based on precedents. Depending on the types of connections used in the model, classifying and functional networks are distinguished, where some elements of logical and network models are used. The idea of inference rules or decision rules is borrowed from logical models, and the description of knowledge in the form of a semantic neural network is borrowed from network models. In this combined model, procedural information is clearly highlighted. Instead of a logical conclusion, a conclusion or a decisive rule on knowledge appears. As a result of solving the system of predicate equations of process knowledge, we find the place, geometric dimensions and type of the symbolic model of an extended object.

Key words: model of process knowledge; decision making; moving object; detection; recognition; intelligent system.

4 fig. Ref: 13 items.

УДК 621.397.48:004.932.2

Методи комплексної обробки та інтерпретації радіолокаційних, акустичних, оптичних і інфрачервоних сигналів безпілотних літальних апаратів / *В.М. Карташов, В.Н. Олейніков, В.П. Рябуха, С.И. Бабкін, В.В. Воронін, А.И. Капуста, И.С. Селєзнев* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 173 – 182.

Безпілотні літальні апарати (БПЛА) знаходять широке застосування при вирішенні широкого спектра корисних завдань, а з іншого боку, вони здатні нести активну або пасивну потенційну загрозу для різних областей діяльності людини – господарській, повсякденній і військовій. З метою виявлення та вимірювання координат безпілотних літальних апаратів використовують радіолокаційні, акустичні, інфрачервоні і оптичні засоби.

Оскільки області можливостей різних методів не збігаються, то з'являється передумова спільного використання систем різного виду для розширення набору вимірюваних параметрів, діапазону спостережуваних діяльностей і підвищення інформативності одержуваних даних шляхом сумісній (комплексній) їх обробки. Комплексна обробка сигналів різних інформаційних каналів може здійснюватися як на етапі виявлення, так і на етапі

вимірювання координат. Причому на етапі виявлення вона найбільш затребувана в силу складності завдання виявлення-розпізнавання.

Число публікацій в даній області постійно збільшується, приділяється увага і комплексним системам, побудованим з використанням різних фізичних сенсорів. Однак ефективність функціонування систем з комплексною обробкою сигналів на практиці є недостатньою.

Стаття присвячена аналізу можливостей комплексних систем з обробкою многомодальної інформації, одержуваної по кожному з використовуваних каналів, а також розробці нових більш ефективних методів комплексування радіолокаційних, оптичних, інфрачервоних і акустичних каналів комплексних систем виявлення і вимірювання координат БПЛА.

Ключові слова: безпілотний літальний апарат; виявлення; розпізнавання; радіолокаційна станція; содар; відеокамера; комплексна система; обробка сигналів.

Іл. 5. Бібліогр.: 37 назв.

УДК 621.397.48:004.932.2

Методы комплексной обработки и интерпретации радиолокационных, акустических, оптических и инфракрасных сигналов беспилотных летательных аппаратов / *В.М. Карташов, В.Н. Олейников, В.П. Рябуха, С.И. Бабкин, В.В. Воронин, А.И. Капуста, И.С. Селезнев* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 173 – 182.

Беспилотные летательные аппараты (БПЛА) находят широкое применение при решении широкого спектра полезных задач, а с другой стороны, они способны нести активную или пассивную потенциальную угрозу для различных областей деятельности человека – хозяйственной, повседневной и военной. С целью обнаружения и измерения координат беспилотных летательных аппаратов в настоящее время используют радиолокационные, акустические, инфракрасные и оптические средства.

Поскольку области возможностей различных методов не совпадают, то появляется предпосылка совместного использования систем различного вида для расширения набора измеряемых параметров, диапазона наблюдаемых дальностей и повышения информативности получаемых данных путем совместной (комплексной) их обработки. Комплексная обработка сигналов различных информационных каналов может осуществляться как на этапе обнаружения, так и на этапе измерения координат. Причем на этапе обнаружения она наиболее востребована в силу сложности задачи обнаружения-распознавания.

Число публикаций в данной области постоянно увеличивается, уделяется внимание и комплексным системам, построенным с использованием различных физических сенсоров. Однако эффективность функционирования систем с комплексной обработкой сигналов на практике является недостаточной.

Статья посвящена анализу возможностей комплексных систем с обработкой многомодальной информации, получаемой по каждому из используемых каналов, а также разработке новых более эффективных методов комплексирования радиолокационных, оптических, инфракрасных и акустических каналов комплексных систем обнаружения и измерения координат БПЛА.

Ключевые слова: беспилотный летательный аппарат; обнаружение; распознавание; радиолокационная станция; содар; видеокамера; комплексная система; обработка сигналов.

Ил. 5. Библиогр.: 37 назв.

UDC 621.397.48:004.932.2

Methods for complex processing and interpretation of radar, acoustic, optical and infrared signals from unmanned aerial vehicles / *V.M. Kartashov, V.M. Oleinikov, V.P. Ryabukha, S.I. Babkin, V.V. Voronin, A.I. Kapusta, I.S. Selezniov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 173 – 182.

Unmanned aerial vehicles (UAVs) are currently widely used in solving a wide range of useful tasks, and on the other hand, they are capable of carrying an active or passive potential threat to various areas of human activity, namely, economic, daily and military. Radar, acoustic, infrared and optical means are currently used to detect and measure the coordinates of unmanned aerial vehicles.

Since the areas of capabilities of different methods do not coincide, the prerequisite for the joint use of systems of various types appears to expand the set of measured parameters, the range of observed distances and increase the information content of the obtained data by joint (complex) processing. Complex processing of signals of various information channels can be carried out both at the stage of detection and at the stage of measuring coordinates. Moreover, at the detection stage, it is most in demand due to the complexity of the detection-recognition task.

The number of publications in this area is constantly increasing; attention is also paid to complex systems built using various physical sensors. However, the efficiency of functioning of the systems with complex signal processing in practice is not sufficient.

The article is devoted to the analysis of the capabilities of integrated systems with the processing of multimodal information obtained from each of the channels used, as well as the development of new more efficient methods for integrating radar, optical, infrared and acoustic channels of integrated systems for the detection and measurement of UAV coordinates.

Key words: unmanned aerial vehicle; detection; recognition; radar station; sodar; video camera; integrated system; signal processing.

5 fig. Ref: 37 items.

ПРИСТРОЇ РАДІОТЕХНІКИ ТА ЗАСОБИ ТЕЛЕКОМУНІКАЦІЙ
УСТРОЙСТВА РАДИОТЕХНИКИ И СРЕДСТВА ТЕЛЕКОММУНИКАЦИЙ
RADIO ENGINEERING DEVICES AND MEANS OF TELECOMMUNICATIONS

УДК 621.375.4

Фазові характеристики підсилювача класу Е з різними вихідними ланками / *В.Г. Крижановський* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 183 – 188.

Моделюванням та експериментально досліджено залежності зсуву фази від частоти у підсилювачах класу Е з класичною вихідною ланкою та вихідною ланкою з двократним виконанням умов класу Е на навантажувальний імпеданс. Аналітично розглянуто залежність зсуву фази на ключі в номінальному режимі. Досліджено зсув фаз на ключі у субоптимальному режимі роботи підсилювача класу Е, що виникає при зміні робочої частоти. Моделювання проведено методом гармонічного балансу на основі моделі ключа з урахуванням структури потужного польового транзистора – наявність вбудованого антипаралельного діоду, який змінює форму імпульсу напруги на ключі. Враховувались вхідна та перехідна ємності транзистора. Експериментальне вимірювання зсуву фаз проводилось на основі записаних оцифрованих форм напруги на вході та на виході ключа шляхом обчислення фаз перших гармонік напруги за допомогою швидкого перетворення Фурье. Встановлено залежність характеру зміни фази на виході ключа та підсилювача в цілому від виду навантажувальної ланки. Показаний зв'язок зсуву фази на ключі в залежності від годографу навантажувального імпедансу. Для ланки з двократним виконанням умов класу Е, що має петлю на годографі навантажувального імпедансу, залежність зсуву фази на ключі має екстремум, що потенційно надає можливість отримати однаковий зсув фаз на двох частотах робочого діапазону. Це дозволяє управляти фазочастотною характеристикою та груповим часом затримки підсилювача. Знання залежності зсуву фази від частоти дозволяє спростити умови визначення зсуву фази у колі зворотного зв'язку. Отримані результати будуть корисні для проєктування автогенераторів класу Е зі зміною частоти у широкому діапазоні.

Ключові слова: фазочастотна характеристика; підсилювач класу Е; автогенератор класу Е; МОН транзистор; умови класу Е.

Табл. 1. Іл. 12. Бібліогр.: 18 назв.

УДК 621.375.4

Фазовые характеристики усилителя класса Е с различными выходными цепями / *В.Г. Крыжановский* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 183 – 188.

Моделированием и экспериментально исследованы зависимости сдвига фазы от частоты в усилителях класса Е с классической выходной цепью и цепью с двукратным выполнением условий класса Е на погрузочный импеданс. Аналитически рассмотрена зависимость сдвига фазы на ключе в номинальном режиме. Исследован сдвиг фаз на ключе в субоптимальном режиме работы усилителя класса Е, возникающим при изменении рабочей частоты. Моделирование проведено методом гармонического баланса на основе модели ключа с учетом структуры мощного полевого транзистора – наличия встроенного антипараллельного диода, который изменяет форму импульса напряжения на ключе. Учитывались входная и переходная емкости транзистора. Экспериментальное измерение сдвига фаз проводилось на основе записанных оцифрованных форм напряжения на входе и на выходе ключа путем вычисления фаз первых гармоник напряжения с помощью быстрого преобразования Фурье. Установлена зависимость изменения фазы на выходе ключа и усилителя в целом от вида нагрузочной цепи. Показана связь сдвига фазы на ключе с формой годографа нагрузочного импеданса. Для звена с двукратным выполнением условий класса Е, с петлей на годографе нагрузочного импеданса, зависимость сдвига фазы на ключе от частоты имеет экстремум, что позволяет получить одинаковый сдвиг фаз на двух частотах рабочего диапазона. Это позволяет управлять фазочастотной характеристикой и групповым временем запаздывания усилителя. Знание зависимости сдвига фазы от частоты позволяет упростить условия определения сдвига фазы в цепи обратной связи. Полученные результаты могут быть полезными при проектировании автогенераторов класса Е с перестройкой частоты в широком диапазоне.

Ключевые слова: фазочастотная характеристика; усилитель класса Е; автогенератор класса Е; МОП транзистор; условия класса Е.

Табл. 1. Ил. 12. Библиогр.: 18 назв.

UDC 621.375.4

Phase characteristics of E class amplifier with various output networks / *V.G. Krizhanovski* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 183 – 188.

Phase shift of E class amplifiers with classical output network and output network that satisfies E class loading impedance conditions twice in the frequency band were studied by simulation and experimentally. The phase shift across switch in nominal operation mode was investigated analytically. The phase shift across switch in suboptimal class E operation mode that occurs while altering the operation frequency was investigated as well. The simulation method was the harmonic balance analysis using the switch model that considers the structure of power MOSFET device, namely, the existence of antiparallel diode pair that alters the switch current waveform. The input and transition capacitances of the transistor were considered. Experimental measurement of the phase shift was performed utilizing the recorded digitized waveforms of the switch input and output voltages by computing the phases of the voltages' first harmonics with the help of Fast Fourier Transform. It was observed that characteristics of phase shift at switch output

and amplifier output are dependent on the kind of load network. The relationship between the phase shift at the switch and hodograph of the loading impedance was demonstrated. For the network with double fulfilment of class E conditions that has a loop in the loading impedance hodograph the switch phase shift dependency has an extremum, which provides an opportunity to obtain the same phase shift at two frequencies within the operating frequency band. That facilitates control of the phase-frequency characteristic and the group delay of the amplifier. Knowledge of the phase-frequency dependency simplifies the conditions for calculation of the phase shift in the feedback network. The obtained results are useful for design of class E oscillator operating in a wide frequency band.

Key words: phase frequency response; E class amplifier; E class oscillator; MOSFET; E class condition.

1 tab. 12 fig. Ref: 18 items.

ФІЗИКА ПРИСТРОЇВ ТА СИСТЕМ
ФИЗИКА ПРИБОРОВ И СИСТЕМ
PHYSICS OF DEVICES AND SYSTEMS

УДК 53.082.52

Дослідження інерційних характеристик фоторезисторів у фізичному практикумі / *О.М. Андреєв, О.М. Андреєва* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 189 – 195.

Описано вимірювальний комплекс на базі 32-розрядного мікроконтролера STM32F103VET6 для дослідження люкс-амперної (світлової), частотної та інерційної характеристик фоторезистора при різних законах рекомбінації нерівноважних носіїв заряду, що виникають під дією світла. Розроблена установка підключається до персонального комп'ютера (смартфона) та дозволяє аналізувати фронти наростання і спаду струму фоторезистора, а також визначати час життя надлишкових носіїв заряду при різних рівнях освітленості. На відміну від традиційних методів вимірювання параметрів фоторезисторів, що працюють в динамічному режимі, в запропонованій установці не використовуються осцилограф і окремий модулятор світлового потоку (генератор або переривник), це дозволило істотно зменшити габаритні розміри та собівартість комплексу, а також автоматизувати процес вимірювання. Для визначення частотної характеристики фоторезистора запропоновано використовувати синтезатор частоти, який дозволяє разом з цифро-аналоговим перетворювачем мікроконтролера сформувати амплітудно-модульований світловий потік необхідної частоти і глибини модуляції. Описаний комплекс може бути підключений до мережі інтернет за допомогою Wi-Fi модуля на базі мікроконтролера ESP8266, що дозволяє проводити дослідження в дистанційному режимі. Також передбачена можливість визначати параметри фоторезистора при різних значеннях опору навантаження.

Ключові слова: фоторезистор; фотопровідність; внутрішній фотоефект; фоторезистивний ефект; нерівноважні носії; час життя; люкс-амперна характеристика; мікроконтролер; синтезатор частоти.

Іл. 8. Бібліогр.: 10 назв.

УДК 53.082.52

Исследование инерционных характеристик фоторезисторов в физическом практикуме / *А.Н. Андреев, О.Н. Андреева* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 189 – 195.

Описан измерительный комплекс на базе 32-разрядного микроконтроллера STM32F103VET6 для исследования люкс-амперной (световой), частотной и инерционной характеристик фоторезистора при разных законах рекомбинации неравновесных носителей заряда, возникающих под действием света. Разработанная установка подключается к персональному компьютеру (смартфону) и позволяет анализировать фронты нарастания и спада тока фоторезистора, а также определять время жизни избыточных носителей заряда при разных уровнях освещенности. В отличие от традиционных методов измерения параметров фоторезисторов, работающих в динамическом режиме, в предложенной установке не используются осциллограф и отдельный модулятор светового потока (генератор или прерыватель), это позволило существенно уменьшить габаритные размеры и себестоимость комплекса, а также автоматизировать процесс измерения. Для определения частотной характеристики фоторезистора предложено использовать синтезатор частоты, который позволяет вместе с цифро-аналоговым преобразователем микроконтроллера сформировать амплитудно-модулированный световой поток требуемой частоты и глубины модуляции. Описанный комплекс может быть подключен к сети интернет при помощи Wi-Fi модуля на базе микроконтроллера ESP8266, что позволяет проводить исследования в дистанционном режиме. Также предусмотрена возможность определять параметры фоторезистора при разных значениях сопротивления нагрузки.

Ключевые слова: фоторезистор; фотопроводимость; внутренний фотоэффект; фоторезистивный эффект неравновесные носители; время жизни; люкс-амперная характеристика; микроконтроллер; синтезатор частоты.

Ил. 8. Библиогр.: 10 назв.

UDC 53.082.52

Study on inertial characteristics of photoresistors in a physical workshop / O.*M. Andreiev, O.M. Andreieva* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. № 202. P. 189 – 195.

The article describes a measuring complex based on the 32-bit STM32F103VET6 microcontroller for studying the lux-ampere (light), frequency and inertial characteristics of a photoresistor with different laws of recombination of nonequilibrium charge carriers arising under the influence of light. The developed complex is connected to a personal computer (smartphone) and allows to analyze the rise and fall edges of the photoresistor current, as well as to determine the lifetime of excess charge carriers at different illumination levels. Unlike traditional methods for measuring the pa-

rameters of photoresistors operating in a dynamic mode, the proposed measuring complex does not use an oscilloscope and a separate modulator of the luminous flux (generator or light interrupter), this made it possible to significantly reduce the size and cost of the complex, as well as automate the measurement process. To determine the frequency response of the photoresistor, it is proposed to use a frequency synthesizer, which allows, together with a digital-to-analog converter of the microcontroller, to form an amplitude-modulated light flux of the required frequency and modulation depth. The complex described in the work can be connected to the Internet using a Wi-Fi module based on an ESP8266 microcontroller, which allows conducting research in a remote mode. It is also possible to determine the parameters of the photoresistor at different values of the load resistance.

Key words: photoresistor; photoconductivity; internal photoelectric effect; photoresistive effect nonequilibrium carriers; lifetime; lux-ampere characteristic; microcontroller; frequency synthesizer.

8 fig. Ref: 10 items.

ЗБІРНИК НАУКОВИХ ПРАЦЬ
РАДІОТЕХНІКА
Випуск 202
Українською, російською, та англійською мовами

СБОРНИК НАУЧНЫХ ТРУДОВ
РАДИОТЕХНИКА
Выпуск 202
На украинском, русском и английском языках

COLLECTION OF SCIENTIFIC PAPERS
RADIOTEKHNIKA
Issue 202
In Ukrainian, Russian and English

Коректор Л.І. Сащенко

Підп. до друку 30.09.2020. Формат 60x90/8. Папір офсет. Гарнітура Таймс. Друк. ризограф.
Ум. друк. арк. 12,4. Обл.-вид. арк. 11,3. Тираж 300 прим. Зам. № 341. Ціна договір.

Харківський національний університет радіоелектроніки (ХНУРЕ)
Просп. Науки, 14, Харків, 61166.

Оригінал-макет підготовлено і збірник надруковано у ПФ „Колегіум”, тел. (057) 703-53-74.
Свідоцтво про внесення суб’єкта видавничої діяльності до Державного реєстру видавців.
Сер. ДК №1722 від 23.03.2004.