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 4

Харків
Харківський національний
університет радіоелектроніки
2021

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 № 3/3-3 від 09.04.2021.

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

МЕТОДИ ТА МОДЕЛІ КРИПТОГРАФІЧНОГО АНАЛІЗУ ТА КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

А.М. Олексійчук Узагальнений диференціально-лінійний криптоаналіз блокових шифрів 5

М.В. Єсіна, С.О. Кандій, Є.В. Острянська, І.Д. Горбенко Генерація загальносистемних параметрів для схеми електронного підпису Rainbow для 384 та 512 біт безпеки 16

І.Д. Горбенко, О.В. Потій, О.А. Замула Концепція синтезу одного класу самосинхронізуючих дискретних сигналів 24

В.І. Єсін, С.Г. Рассомахін, В.В. Вілігура Аналіз формальних моделей забезпечення цілісності даних і їх застосовність для баз даних (*рос.*) 30

М.В. Єсіна, Б.С. Шахов Дослідження та аналіз реалізацій кандидатів другого раунду конкурсу NIST PQC, що орієнтовані на сімейства FPGA Xilinx 40

С.О. Кандій, Г.А. Малєєва Аналіз складності атак на мультиваріативні криптографічні перетворення з використанням алгебраїчної структури поля 59

Є.В. Котух, О.В. Северинов, А.В. Власов, А.О. Теницька, Е. О. Зарудна Деякі результати розробки схем криптографічних перетворень з використанням неабелевих груп (*рос*.) 66

РАДІОТЕХНІЧНІ ТА ТЕЛЕКОМУНІКАЦІЙНІ МЕРЕЖІ ТА СИСТЕМИ

Ю.Ю. Коляденко, О.В. Коляденко, Б.П. Муляр Метод оптимізації розподілу частотного ресурсу з повторним використанням частот для систем когнітивного радіо 73

М.О. Єрмошин, А.А Побережний, О.С. Онопрієнко, М.П. Шурига Архітектура сітьової бази знань складної системи воєнного призначення (*англ.*) 80

О.В. Рязанцев, С.В. Марченко, М.В. Кулик Про ефект Доплера в радіолокації (*рос.*) 93

В.Г. Крижановський, С.П. Сергієнко, Д.В. Чернов, В.В. Крижановський Підслуховування NFC-зв'язку на частотах вищих гармонік 99

ФІЗИКА ПРИЛАДІВ ТА СИСТЕМ

В.М. Борщов, О.М. Лістратенко, М.А. Проценко, І.Т. Тимчук, О.В. Кравченко, О.В. Суддя, М.І. Сліпченко, Б.М. Чічков Дисперсія наночасток в оптично прозорі полімерні матриці (*рос.*) 105

Б.В. Жуков, А.В. Одновол Контроль різниці рівнів рідини в суміжних резервуарах (*рос.*) 115

РАДІОТЕХНІЧНІ ПРИСТРОЇ ТА ЗАСОБИ ТЕЛЕКОМУНІКАЦІЙ

Д.Г. Макаров, Д.В. Чернов, В.В. Крижановський, Ю.В. Рассохіна, В.Г. Крижановський, А. Грєбєнніков Дослідження підсилювача класу E/F3 з паралельним контуром 120

ПІДГОТОВКА СПЕЦІАЛІСТІВ В ОБЛАСТІ РАДІОТЕХНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ

І.О. Мощенко, О.М. Нікітенко, Ю.В. Козлов Можливості застосування СМК Maple для дослідження законів розподілу випадкових величин (*англ.*) 128

РЕФЕРАТИ 135

CONTENT

METHODS AND MODELS OF CRYPTOGRAPHIC ANALYSIS AND CRYPTOGRAPHIC TRANSFORMATIONS

A.N. Alekseychuk Generalized differential-linear cryptanalysis of block ciphers 5

M.V. Yesina, S.O. Kandiy, E.V. Ostryanska, I.D. Gorbenko Generation of general system parameters for Rainbow electronic signature scheme for 384 and 512 security bits 16

I.D. Gorbenko, O.V. Potii, A.A. Zamula The concept of synthesis of one class of self-synchronizing discrete 24

V.I. Yesin, S.G. Rassomakhin, V.V. Vilihura Analysis of formal models for ensuring data integrity and their applicability to databases 30

M.V. Yesina, B.S. Shahov Research and analysis of implementations of the NIST PQC competition second round candidates focused on the Xilinx FPGA family 40

S. Kandiy, G. Maleeva Analysis of the complexity of attacks on multivariate cryptographic transformations using algebraic field structure 59

E.V. Kotukh, O.V. Severinov, A.V. Vlasov, A.O. Tenytska, E.O. Zarudna Towards results of cryptographic transformations schemes development with application of nonabelian groups 66

RADIO AND TELECOMMUNICATION NETWORKS AND SYSTEMS

Yu.Yu. Kolyadenko, O.B. Kolyadenko, B.P. Mulyar Method for optimization of frequency resource allocation with frequency reuse for cognitive radio systems 73

M. Yermoshyn, A. Poberezhnyi, O. Onopriyenko, M. Shuryha Architecture of network knowledge base of a complex military system 80

O.V. Ryazantsev, S.V. Marchenko, M.V. Kulik On the Doppler effect in radar 93

V.G. Kryzhanovskyi, S.P. Serhiienko, D.V. Chernov, V.V. Kryzhanovskyi Listening to NFC at higher harmonic frequencies 99

PHYSICS OF INSTRUMENTS AND SYSTEMS

V.M. Borshchov, O.M. Listratenko, M.A. Protsenko, I.T. Tymchuk, O.V. Kravchenko, O.V. Syddia, M.I. Slipchenko, B.M. Chichkov Dispersion of nanoparticles in optically transparent polymer matrices 105

B.V. Zhukov, A.V. Odnovol Monitoring the difference in liquid levels in adjacent tanks 115

RADIO ENGINEERING DEVICES AND TELECOMMUNICATIONS MEANS

D.G. Makarov, D.V. Chernov, V.V. Kryzhanovskyi, Yu.V. Rassokhina, V.G. Kryzhanovskyi, A. Grebennikov Investigation into Class E/F3 with Parallel Network 120

TRAINING OF SPECIALISTS IN THE FIELD OF RADIO AND TELECOMMUNICATIONS

I. Moshchenko, O. Nikitenko, Yu.V. Kozlov Possibility of using CMS Maple to study laws of distribution of random variables 128

ABSTRACTS 135

МЕТОДИ ТА МОДЕЛІ КРИПТОГРАФІЧНОГО АНАЛІЗУ ТА КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

УДК 621.391:519.2 **DOI:10.30837/rt.2021.1.204.01**

А.М. ОЛЕКСІЙЧУК, д-р техн. наук

УЗАГАЛЬНЕНИЙ ДИФЕРЕНЦІАЛЬНО-ЛІНІЙНИЙ КРИПТОАНАЛІЗ БЛОКОВИХ ШИФРІВ

Вступ

Диференціально-лінійний метод криптоаналізу блокових шифрів запропоновано в 1994 р. [1]. Його сутність полягає у сумісному застосуванні для побудови атаки на шифр високоймовірного диференціалу для перших раундів та високоймовірної лінійної апроксимації для останніх раундів шифрування. Зазначений метод виявляється більш ефективним в порівнянні з (окремо) диференціальним та лінійним методами при застосуванні до багатьох блокових шифрів (див. [1 – 5]), проте його наукове обґрунтування залишається предметом подальших досліджень.

Відомо декілька публікацій [2 – 5], присвячених формалізації диференціально-лінійного методу та з'ясуванню умов, за яких його трудомісткість може бути оцінено математично строго. Певний прогрес в цьому напрямі зроблено протягом останніх років [4, 5], але проблема обґрунтування диференціально-лінійного методу в повному обсязі залишається не вирішеною. Мета статті – викласти перші результати, отримані автором у напрямі вирішення цієї проблеми.

В п. 1 розширюється клас диференціально-лінійних атак на блокові шифри. А саме, розглядаються як розрізнювальні атаки, так і атаки, спрямовані на відновлення одного біту інформації про ключ. При цьому не робиться жодних припущень (як у відомих публікаціях [1 – 5]) про можливість представлення шифру у вигляді певних двох компонент. За допомогою окремих результатів роботи [6] отримано нижні оцінки інформаційної складності зазначених атак, вирази яких залежать від усереднених (за ключами) значень квадратів елементів узагальненої автокореляційної таблиці шифрувального перетворення [7]. На відміну від відомих [1, 2, 4], отримані оцінки інформаційної складності диференціально-лінійних атак не базуються на жодних евристичних припущеннях відносно блокових шифрів, що досліджуються, та є справедливими для більш широкого класу атак в порівнянні з традиційною диференціально-лінійною атакою. Для порівняння викладено також евристичний підхід до побудови оцінок інформаційної складності узагальненої диференціально-лінійної атаки, який є загальновизнаним у випадку звичайної розрізнювальної атаки.

В п. 2 у важливому окремому випадку отримано явний вираз середнього значення параметра, який фігурує в зазначених вище оцінках, для випадкової рівноймовірної підстановки на множині повідомлень, що шифруються. Аналогічно диференціальному або лінійному методам криптоаналізу цей результат надає можливість порівнювати диференціально-лінійні властивості бієктивних булевих відображень з аналогічними властивостями "ідеального" криптографічного відображення, тобто випадкової рівноймовірної підстановки.

В п. 3 наведено співвідношення, які встановлюють взаємозв'язок між, відповідно, диференціальними, лінійними та диференціально-лінійними властивостями бієктивних булевих відображень. На відміну від відомих робіт [4, 6, 8], використовується матрична форма запису співвідношень, що дозволяє краще з'ясувати їх сутність та спростити доведення. Отримано також нове співвідношення для елементів узагальненої автокореляційної таблиці шифрувального перетворення добутку двох блокових шифрів, яке може бути корисним в подальших дослідженнях. Наприкінці статті сформульовано стислі висновки.

1. Узагальнені диференціально-лінійні атаки на блокові шифри

Для будь-якого натурального n позначимо $\sigma(V_n)$ симетричну групу підстановок на множині $V_n = \{0,1\}^n$. Для будь-яких $\alpha = (\alpha_1,...,\alpha_n)$, $\beta = (\beta_1,...,\beta_n) \in V_n$ покладемо $\alpha\beta = \alpha_1\beta_1 \oplus \cdots \oplus \alpha_n\beta_n$, $\alpha \oplus \beta = (\alpha_1 \oplus \beta_1, \dots, \alpha_n \oplus \beta_n)$.

Розглянемо блоковий шифр $\Im$ з множиною відкритих (шифрованих) повідомлень $X = V_n$, множиною ключів $K = V_m$ та сім'єю шифрувальних перетворень $(F_k : k \in K)$.

Узагальнена диференціально-лінійна атака на шифр $\Im$ визначається за допомогою ненульових векторів $a, \alpha, \beta \in V_n$, комутативної групової операції $+$ на множині V_n та зрівноваженої функції $\psi : K \to \{0,1\}$. Вважається, що при проведенні атаки супротивник має доступ до оракула F_k з невідомим (вибраним випадково рівноймовірно з множини K) ключем k. Супротивник генерує незалежні в сукупності випадкові рівноймовірні відкриті тексти $X_1, \dots, X_t \in V_n$ та обчислює за відповідними шифротекстами $F_k(X_i), F_k(X_i \oplus a)$ значення $\nu_i = \alpha F_k(X_i) \oplus \beta F_k(X_i + a)$, $i \in \overline{1,t}$. Мета атаки полягає в тому, щоб відновити значення $\psi(k)$ за послідовністю $\nu_1, \dots, \nu_t$.

Зауважимо, що для побудови ефективних диференціально-лінійних атак слід вибирати вектори a, α, β, операцію $+$ та функцію ψ, виходячи з особливостей будови блокового шифру так, щоб випадкова послідовність $\nu_1, \dots, \nu_t$ містила якомога більше інформації про значення $\psi(k)$. Поряд з тим, для обґрунтування стійкості блокових шифрів відносно диференціально-лінійного методу криптоаналізу можна використовувати нижню оцінку інформаційної складності наведеної атаки, яка не накладає жодних додаткових обмежень на вектори a, α, β, операцію $+$ та функцію ψ. Для того щоб навести зазначену оцінку, розглянемо більш загальну атаку на шифр $\Im$, описану в [6], та скористаємося доведеним там твердженням 1.

Загальна атака (d-го порядку, $d = 1, 2, \dots$) на шифр $\Im$ будується на основі пари відображень $\varphi : X^d \times X^d \to Z$, $\psi : K \to S'$, де Z, S' – скінченні множини, відображення φ є відмінним від константи, а відображення ψ задовольняє умові $|\psi^{-1}(s')| = |K| \cdot |S'|^{-1}$ для будь-якого $s' \in S'$. Вважається, що на множині K задано рівномірний розподіл ймовірностей, а на множині X^d – певний розподіл $P^{(d)}$. При проведенні атаки супротивник має доступ до оракула F_k з невідомим (вибраним випадково рівноймовірно з множини K) ключем k. Супротивник генерує незалежні в сукупності набори відкритих повідомлень $X_i = (X_{i,1}, \dots, X_{i,d})$, кожен з яких розподілений за законом $P^{(d)}$, отримує набори $F_k(X_i) = (F_k(X_{i,1}), \dots, F_k(X_{i,d}))$ та обчислює значення $Z_i = \varphi(X_i, F_k(X_i))$, $i \in \overline{1,t}$. Мета супротивника – відновити значення $\psi(k)$ за відомою послідовністю $Z^{(t)} = Z_1, \dots, Z_t$.

Наступна лема дозволяє оцінити інформаційну складність наведеної атаки.

Лема 1 [6]. Найменший обсяг даних, необхідних для проведення описаної загальної атаки з імовірністю помилки не більше ніж $\delta \in (0, 1/2)$, задовольняє нерівності

$$t \geq \frac{(1-\delta)\log|S'| - h(\delta)}{|K|^{-1} \sum_{k \in K} \Delta(P_k)} \ln 2, \qquad (1)$$

де

$$\Delta(P_k) = |Z|^{-1} \sum_{z \in Z} (|Z| P^{(d)}\{\varphi(X, F_k(X)) = z\} - 1)^2, \qquad (2)$$

$h(\delta) = -\delta \log \delta - (1-\delta)\log(1-\delta)$, а $X = (X_1, \dots, X_d)$ є випадковим вектором, розподіленим на множині X^d за законом $P^{(d)}$, $F_k(X) = (F_k(X_1), \dots, F_k(X_d))$, $k \in K$.

Доведемо зараз наступне твердження.

Твердження 1. Найменший обсяг даних, необхідних для проведення на шифр $\Im$ диференціально-лінійної атаки (на основі векторів a, α, β, операції $+$ та функції ψ) з імовірністю

помилки не більше ніж $\delta \in (0, 1/2)$, задовольняє нерівності

$$t \geq \frac{(1-\delta-h(\delta))\ln 2}{|K|^{-1}\sum\limits_{k\in K}(2\mathbf{P}_X\{\alpha F_k(X)=\beta F_k(X+a)\}-1)^2}, \tag{3}$$

де X – випадковий вектор з рівномірним розподілом ймовірностей на множині V_n.

Доведення. Помітимо, що диференціально-лінійна атака на шифр $\Im$ є окремим випадком наведеної вище загальної атаки при $d=2$, $S'=Z=\{0,1\}$, $\varphi((x,x'),(y,y'))=\alpha y \oplus \beta y'$, $x,x',y,y' \in V_n$ та розподілі ймовірностей $P^{(d)}$, що є рівномірним на множині $\{(x, x+a): x \in V_n\}$. Оскільки при цьому

$$\Delta(P_k)=|Z|^{-1}\sum_{z\in Z}(|Z|P^{(d)}\{\varphi(X, F_k(X))=z\}-1)^2 =$$

$$=(2\mathbf{P}_X\{\alpha F_k(X)=\beta F_k(X+a)\}-1)^2,$$

то нерівність (3) є безпосереднім наслідком нерівності (1). Твердження доведено.

Поряд із наведеною вище диференціально-лінійною атакою, спрямованою на відновлення значення $\psi(k)$ (тобто одного біту інформації про ключ) за випадковою послідовністю $\nu_i = \alpha F_k(X_i) \oplus \beta F_k(X_i + a)$, $i \in \overline{1,t}$, розглянемо також розрізнювальну атаку на шифр $\Im$, яка має за мету відрізнити цей шифр від суто випадкової підстановки на множині V_n шляхом аналізу послідовності ν_i, $i \in \overline{1,t}$. Зауважимо, що саме такі атаки (в окремому випадку $\alpha = \beta$) розглядаються в переважній більшості робіт, присвячених диференціально-лінійному криптоаналізу (див., наприклад, [2, 4, 5]).

Для того щоб навести нижню оцінку інформаційної складності розрізнювальної диференціально-лінійної атаки, розглянемо спочатку більш загальну атаку на шифр $\Im$, описану в [6].

Нехай Φ – випадкове відображення, яке з ймовірністю $1/2$ є випадковою рівноймовірною підстановкою на множині $X = V_n$ (гіпотеза H_0) або випадковим рівноймовірним шифрувальним перетворенням шифру $\Im$ (гіпотеза H_1). Розрізнювальна атака на шифр $\Im$ будується на основі відмінної від константи функції $\varphi: X^d \times X^d \to Z$ та розподілу ймовірностей $P^{(d)}$ на множині X^d і спрямована на те, щоб розрізнити гіпотези H_0 та H_1 за відомою реалізацією випадкової послідовності $Z^{(t)} = Z_1, \ldots, Z_t$, де $Z_i = \varphi(X_i, \Phi(X_i))$, а $X_i = (X_{i,1}, \ldots, X_{i,d})$ є незалежними наборами відкритих повідомлень, кожен з яких розподілений за законом $P^{(d)}$, $\Phi(X_i) = (\Phi(X_{i,1}), \ldots, \Phi(X_{i,d}))$, $i \in \overline{1,t}$.

Наступна лема містить нижню оцінку інформаційної складності цієї атаки.

Лема 2 [6]**.** Найменший обсяг даних, необхідних для проведення зазначеної розрізнювальної атаки з імовірністю помилки не більше ніж $\delta \in (0, 1/2)$, задовольняє нерівності

$$t \geq \frac{2(1-h(\delta))\ln 2}{|K|^{-1}\sum\limits_{k\in K}\Delta(P_k)+|\sigma(V_n)|^{-1}\sum\limits_{F\in\sigma(V_n)}\Delta(P_F)}, \tag{4}$$

де $\Delta(P_k)$ визначається за формулою (2), а $\Delta(P_F)$ – за аналогічною формулою, яка отримується з формули (2) шляхом заміни у ній F_k на $F \in \sigma(V_n)$.

Вважаючи у формулюванні леми 2 $d=2$, $Z=\{0,1\}$, $\varphi((x,x'),(y,y'))=\alpha y \oplus \beta y'$, $x,x',y,y' \in V_n$, та визначаючи $P^{(d)}$ як рівномірний розподіл ймовірностей на множині

$\{(x, x+a): x \in V_n\}$, отримаємо наступне твердження, яке встановлює нижню межу інформаційної складності розрізнювальної диференціально-лінійної атаки, що будується на основі ненульових векторів $a, \alpha, \beta \in V_n$ та операції $+$.

Твердження 2. Найменший обсяг даних, необхідних для проведення на шифр $\Im$ диференціально-лінійної атаки з імовірністю помилки не більше ніж $\delta \in (0, 1/2)$, задовольняє нерівності (4), де

$$\Delta(P_k) = (2\mathbf{P}_X\{\alpha F_k(X) = \beta F_k(X+a)\} - 1)^2, \tag{5}$$

$$\Delta(P_F) = (2\mathbf{P}_X\{\alpha F(X) = \beta F(X+a)\} - 1)^2, \tag{6}$$

а X є випадковим вектором із рівномірним розподілом ймовірностей на множині V_n.

На завершення цього пункту розглянемо традиційну розрізнювальну диференціально-лінійну атаку на шифр $\Im$, яка будується на основі ненульових векторів a, α, β, що задовольняють умові

$$\mathbf{P}_{x,k}\{\alpha F_k(x) = \beta F_k(x+a)\} \geq 1/2 \cdot (1+\varepsilon), \tag{7}$$

де x і k є незалежними випадковими векторами з рівномірними розподілами ймовірностей на множинах X і K відповідно, $\varepsilon \in (0, 1/2)$. Вважається, що при проведенні атаки супротивник має доступ до оракула F, який з імовірністю $1/2$ є реалізацією випадкової рівноймовірної підстановки на множині V_n (гіпотеза H_0) і з такою ж ймовірністю співпадає з шифрувальним перетворенням F_k шифру $\Im$ при невідомому ключі k, вибраному випадково рівноймовірно з множини K (гіпотеза H_1). Мета атаки полягає в тому, щоб розрізнити зазначені гіпотези. Для цього супротивник генерує незалежні в сукупності випадкові рівноймовірні вхідні повідомлення $X_1, \ldots, X_t \in V_n$, обчислює за відповідними вихідними повідомленнями $F(X_i), F(X_i + a)$ значення $\nu_i = \alpha F(X_i) \oplus \beta F(X_i + a)$, $i \in \overline{1,t}$, та перевіряє умову $\nu_1 + \cdots + \nu_t > C$ (для заздалегідь визначеної величини $C > 0$). Якщо ця умова виконується, то приймається гіпотеза H_0; інакше приймається гіпотеза H_1.

Визначимо умови, за яких наведена атака є успішною, та оцінимо її трудомісткість. Перш за все, доведемо таку лему.

Лема 3. Середнє значення ймовірності $\mathbf{P}_x\{\alpha F(x) = \beta F(x+a)\}$ за всіма підстановками $F \in \sigma(V_n)$ дорівнює $1/2$, якщо $\alpha \neq \beta$ та $1/2 \cdot (1 - (2^n - 1)^{-1})$, якщо $\alpha = \beta$.

Доведення. Помітимо, що

$$\frac{2}{2^n!}\sum_{F \in \sigma(V_n)} \mathbf{P}_x\{\alpha F(x) = \beta F(x+a)\} - 1 = \frac{1}{2^n!}\sum_{F \in \sigma(V_n)} 2^{-n} \sum_{x \in V_n} (-1)^{\alpha F(x) \oplus \beta F(x+a)} =$$

$$= \frac{1}{2^n!} 2^{-n} \sum_{x \in V_n} \sum_{\substack{y,z \in V_n: \\ y \neq z}} |\{F \in \sigma(V_n): F(x) = y, F(x+a) = z\}| (-1)^{\alpha y \oplus \beta z} =$$

$$= \frac{1}{2^n(2^n - 1)} \sum_{\substack{y,z \in V_n: \\ y \neq z}} (-1)^{\alpha y \oplus \beta z} = \frac{1}{2^n(2^n - 1)} \left(0 - \sum_{y \in V_n} (-1)^{(\alpha \oplus \beta) y} \right).$$

При цьому останній вираз дорівнює 0, якщо $\alpha \neq \beta$ та $-(2^n - 1)^{-1}$, якщо $\alpha = \beta$. Лему доведено.

З опису наведеної атаки випливає, що випадкова послідовність $\nu_i = \alpha F(X_i) \oplus \beta F(X_i + a)$, $i \in \overline{1,t}$, яку спостерігає супротивник, є схемою Бернуллі з ймовір-

ністю успіху $p_F = 1 - \mathbf{P}_x\{\alpha F(x) = \beta F(x+a)\}$. При цьому на підставі леми 3 число $\frac{1}{2^n!}\sum_{F\in\sigma(V_n)} p_F$ майже не відрізняється від $1/2$ (при $n \geq 64$), в той час як за умови (7) число $\frac{1}{|K|}\sum_{k\in K} p_{F_k}$ не перевищує $1/2\cdot(1-\varepsilon)$. Зазначений факт дозволяє прийняти такі припущення, аналогічні відомим гіпотезам про розрізненість та, відповідно, стохастичну еквівалентність ключів у статистичних атаках на блокові шифри (див., наприклад, [9, 10]).

Припущення 1. За умови справедливості гіпотези H_0 для кожного $F \in \sigma(V_n)$ виконується рівність $p_F = 1/2$.

Припущення 2. За умови справедливості гіпотези H_1 для кожного $k \in K$ виконується нерівність $p_{F_k} \leq 1/2\cdot(1-\varepsilon)$.

Використовуючи стандартні міркування із застосуванням нерівності Гефдінга [11], отримаємо наступне твердження, яке встановлює оцінку трудомісткості наведеної атаки.

Твердження 3. Нехай виконуються умова (7) та припущення 1 і 2. Тоді при $C = t/2\cdot(1+\varepsilon/2)$, $t = \left\lceil 8\varepsilon^{-2}\ln(\delta^{-1})\right\rceil$, $\delta \in (0,\, 1/2)$ наведена атака дозволяє відрізнити блоковий шифр $\mathfrak{I}$ від випадкової рівноймовірної підстановки на множині V_n із середньою ймовірністю помилки не вище ніж δ за $O(t)$ операцій.

Зауважимо, що твердження 3 встановлює верхню оцінку трудомісткості описаної розрізнювальної атаки на шифр $\mathfrak{I}$ за умови припущень 1 і 2, в той час як твердження 2 визначає нижню оцінку трудомісткості будь-якої розрізнювальної диференціально-лінійної атаки на шифр $\mathfrak{I}$ без жодного евристичного припущення. Згідно з твердженням 3 трудомісткість наведеної атаки обернено пропорційна параметру $(2\mathbf{P}_{x,k}\{\alpha F_k(x) = \beta F_k(x+a)\} - 1)^2$, який не перевищує середнє арифметичне значення чисел (5) за всіма $k \in K$.

2. Аналітичний вираз середнього значення параметра, що характеризує диференціально-лінійні властивості випадкової рівноймовірної підстановки

Розглянемо практично важливий випадок, в якому операція $+$ співпадає з покоординатним булевим додаванням $\oplus$ на множині V_n, та отримаємо в цьому випадку явний вираз параметра $\overline{\Delta}_a(\alpha,\beta) = |\sigma(V_n)|^{-1}\sum_{F\in\sigma(V_n)}\Delta(P_F)$, де $\Delta(P_F)$ визначається за формулою (6). Доведемо наступне твердження.

Твердження 4. Справедливі рівності

$$\overline{\Delta}_a(\alpha,\beta) = 2^{1-n} + \frac{(3\cdot 2^n - 6)}{2^n(2^n-1)(2^n-3)}, \text{ якщо } \alpha = \beta; \tag{8}$$

$$\overline{\Delta}_a(\alpha,\beta) = 2^{-n} - \frac{1}{2^n(2^n-1)} + \frac{2^n-6}{2^n(2^n-1)(2^n-3)}, \text{ якщо } \alpha \neq \beta. \tag{9}$$

Доведення. На підставі формули (6)

$$\Delta(P_F) = \left(2^{-n}\sum_{x\in V_n}(-1)^{\alpha F(x)\oplus\beta F(x\oplus a)}\right)^2 =$$

$$= 2^{-2n}\sum_{(x,\,x')\in V_n\times V_n}(-1)^{\alpha(F(x)\oplus F(x'))\oplus\beta(F(x\oplus a)\oplus F(x'\oplus a))} = S_1 + S_2 + S_3,$$

де S_1, S_2 та S_3 позначають суми зазначених виразів за всіма парами (x, x'), що належать множинам $M_1 = \{(x, x') \in V_n \times V_n : x' = x\}$, $M_2 = \{(x, x') \in V_n \times V_n : x' = x \oplus a\}$ та $M_3 = \{(x, x') \in V_n \times V_n : x' \notin \{x, x \oplus a\}\}$ відповідно.

Позначимо $\overline{S}_l$ середнє значення суми S_l за всіма підстановками $F \in \sigma(V_n)$, $l = 1, 2, 3$. Тоді

$$\overline{\Delta}_a(\alpha, \beta) = \overline{S}_1 + \overline{S}_2 + \overline{S}_3. \tag{10}$$

При цьому

$$\overline{S}_1 = 2^{-n}, \tag{11}$$

$$\overline{S}_2 = 2^{-2n} \sum_{x \in V_n} |\sigma(V_n)|^{-1} \sum_{F \in \sigma(V_n)} (-1)^{(\alpha \oplus \beta)(F(x) \oplus F(x \oplus a))} = 2^{-n}, \text{ якщо } \alpha = \beta.$$

Нехай $\alpha \neq \beta$. Тоді

$$|\sigma(V_n)|^{-1} \sum_{F \in \sigma(V_n)} (-1)^{(\alpha \oplus \beta)(F(x) \oplus F(x \oplus a))} =$$

$$= \frac{1}{2^n!} \sum_{\substack{(y,z) \in V_n \times V_n: \\ y \neq z}} \sum_{\substack{F \in \sigma(V_n): \\ F(x)=y, \\ F(x \oplus a)=z}} (-1)^{(\alpha \oplus \beta)(y \oplus z)} =$$

$$= \frac{1}{2^n(2^n - 1)} \sum_{\substack{(y,z) \in V_n \times V_n: \\ y \neq z}} (-1)^{(\alpha \oplus \beta)(y \oplus z)} = -\frac{1}{2^n - 1},$$

де остання рівність випливає зі співвідношення ортогональності для характерів (див., наприклад, [12]). Отже, у випадку, що розглядається, маємо $\overline{S}_2 = 2^{-2n} \sum_{x \in V_n} \frac{-1}{2^n - 1} = -\frac{1}{2^n(2^n - 1)}$.

Таким чином, отримаємо кінцевий вираз:

$$\overline{S}_2 = 2^{-n}, \text{ якщо } \alpha = \beta; \ \overline{S}_2 = -\frac{1}{2^n(2^n - 1)}, \text{ якщо } \alpha \neq \beta. \tag{12}$$

Обчислимо зараз значення суми

$$\overline{S}_3 = 2^{-2n} \sum_{(x, x') \in M_3} |\sigma(V_n)|^{-1} \sum_{F \in \sigma(V_n)} (-1)^{\alpha(F(x) \oplus F(x')) \oplus \beta(F(x \oplus a) \oplus F(x' \oplus a))}.$$

З означення множини M_3 випливає, що

$$T \stackrel{\text{def}}{=} |\sigma(V_n)|^{-1} \sum_{F \in \sigma(V_n)} (-1)^{\alpha(F(x) \oplus F(x')) \oplus \beta(F(x \oplus a) \oplus F(x' \oplus a))} =$$

$$= \frac{1}{2^n(2^n - 1)(2^n - 2)(2^n - 3)} \sum_{(y_1, y_2, y_3, y_4) \in R_n} (-1)^{\alpha(y_1 \oplus y_2) \oplus \beta(y_3 \oplus y_4)},$$

де R_n позначає множину, що складається з усіх четвірок попарно різних двійкових векторів довжини n.

Для знаходження виразу параметра T скористаємося методом включення-виключення [13]. На множині "предметів" V_n^4 задамо властивості $\{i, j\}$, де $1 \le i < j \le 4$. За означенням "предмет" $y = (y_1, y_2, y_3, y_4) \in V_n^4$ володіє властивістю $\{i, j\}$, якщо $y_i = y_j$. Позначимо також $\omega(y) = (-1)^{\alpha(y_1 \oplus y_2) \oplus \beta(y_3 \oplus y_4)}$ вагу "предмету" y. Тоді значення T є пропорційним сумарній

вазі “предметів”, які не володіють жодною із зазначених властивостей. Отже, на підставі формули включення-виключення маємо

$$T = \frac{1}{2^n(2^n-1)(2^n-2)(2^n-3)} \sum_{k=0}^{6} (-1)^k T_k , \qquad (13)$$

де

$$T_0 = \sum_{y \in V_n^4} \omega(y) , \; T_k = \sum_{\{i_1, j_1\}, \ldots, \{i_k, j_k\}} M(A_{i_1, j_1}, \ldots, A_{i_k, j_k}) ,$$

і в останній формулі підсумування відбувається за всіма сполученнями з k властивостей $\{i_1, j_1\}, \ldots, \{i_k, j_k\}$, а $M(A_{i_1, j_1}, \ldots, A_{i_k, j_k})$ позначає сумарну вагу “предметів”, які володіють цими властивостями, $1 \le k \le 6$.

Для обчислення значення T за формулою (13) розглянемо декілька випадків.

Випадок 1: $k = 0$. Згідно із співвідношенням ортогональності для характерів маємо $T_0 = \sum_{y \in V_n^4} \omega(y) = \sum_{y \in V_n^4} (-1)^{\alpha(y_1 \oplus y_2) \oplus \beta(y_3 \oplus y_4)} = 0$.

Випадок 2: $k = 1$. Тоді для будь-якої властивості $\{i, j\}$ справедлива рівність $M(A_{i,j}) = \sum_{\substack{y \in V_n^4: \\ y_i = y_j}} (-1)^{\alpha(y_1 \oplus y_2) \oplus \beta(y_3 \oplus y_4)} = 0$, в чому неважко переконатися, розглядаючи усі можливі значення i та j. Звідси випливає, що $T_1 = 0$.

Випадок 3: $k = 2$. Існує тільки три сполучення $\{\{i_1, j_1\}, \{i_2, j_2\}\}$ таких, що $M(A_{i_1, j_1}, A_{i_2, j_2})$ може бути відмінним від нуля, а саме, $\{\{i_1, j_1\}, \{i_2, j_2\}\} = \{\{1, 2\}, \{3, 4\}\}$, $\{\{i_1, j_1\}, \{i_2, j_2\}\} = \{\{1, 3\}, \{2, 4\}\}$, $\{\{i_1, j_1\}, \{i_2, j_2\}\} = \{\{1, 4\}, \{2, 3\}\}$. При цьому, як показує безпосередня перевірка, $M(A_{1,2}, A_{3,4}) = 2^{2n}$, $M(A_{1,3}, A_{2,4}) = M(A_{1,4}, A_{2,3}) = 2^{2n}$, якщо $\alpha = \beta$; $M(A_{1,3}, A_{2,4}) = M(A_{1,4}, A_{2,3}) = 0$, якщо $\alpha \ne \beta$. Звідси випливає, що $T_2 = 3 \cdot 2^{2n}$, якщо $\alpha = \beta$ та $T_2 = 2^{2n}$, якщо $\alpha \ne \beta$.

Випадок 4: $k = 3$. В цьому випадку існує точно 4 сполучення $\{\{i_1, j_1\}, \{i_2, j_2\}, \{i_3, j_3\}\}$ таких, що $M(A_{i_1, j_1}, A_{i_2, j_2}, A_{i_3, j_3}) = 0$, а саме, $\{\{1, 2\}, \{1, 3\}, \{2, 3\}\}$, $\{\{1, 2\}, \{1, 4\}, \{2, 4\}\}$, $\{\{1, 3\}, \{1, 4\}, \{3, 4\}\}$, $\{\{2, 3\}, \{2, 4\}, \{3, 4\}\}$. Для решти сполучень по k кожен “предмет” $y = (y_1, y_2, y_3, y_4)$, що володіє властивістю, яка визначається цим сполученням, задовольняє умові $y_1 = y_2 = y_3 = y_4$. Звідси випливає, що для такого сполучення $M(A_{i_1, j_1}, A_{i_2, j_2}, A_{i_3, j_3}) = 2^n$. Таким чином, $T_3 = 2^n \left(\binom{6}{3} - 4 \right) = 16 \cdot 2^n$.

Випадок 5: $k \in \{4, 5, 6\}$. В цьому випадку для будь-якого “предмету”, що володіє властивостями $\{i_1, j_1\}, \ldots, \{i_k, j_k\}$, виконуються рівності $y_1 = y_2 = y_3 = y_4$. Отже, $M(A_{i_1, j_1}, \ldots, A_{i_k, j_k}) = 2^n$ і $\sum_{k=4}^{6} (-1)^k T_k = 2^n \left(\binom{6}{4} - \binom{6}{5} + \binom{6}{6} \right) = 10 \cdot 2^n$.

Підставляючи вирази, отримані у випадках 1 – 5, у формулу (13), знайдемо, що

$$T = \frac{3 \cdot 2^{2n} - 6 \cdot 2^n}{2^n(2^n-1)(2^n-2)(2^n-3)} , \text{ якщо } \alpha = \beta ;$$

$$T = \frac{2^{2n} - 6 \cdot 2^n}{2^n(2^n-1)(2^n-2)(2^n-3)} , \text{ якщо } \alpha \ne \beta .$$

Звідси, використовуючи формулу $\overline{S}_3 = 2^{-2n} \sum_{(x,\,x')\,\in M_3} T$, отримаємо кінцевий вираз:

$$\overline{S}_3 = \frac{(3\cdot 2^n - 6)}{2^n(2^n-1)(2^n-3)}, \text{ якщо } \alpha = \beta;\ \overline{S}_3 = \frac{2^n - 6}{2^n(2^n-1)(2^n-3)}, \text{ якщо } \alpha \neq \beta. \qquad (14)$$

Нарешті, використовуючи формули (10) – (12), (15), отримаємо формули (8), (9). Твердження доведено.

3. Співвідношення між параметрами, що характеризують диференціальні, лінійні та диференціально-лінійні властивості блокових шифрів

Для будь-якої комутативної групової операції $+$ на множині V_n та довільної підстановки $f \in \sigma(V_n)$ визначимо матриці $C_f = (C_f(\alpha,\beta))_{\alpha,\beta\in V_n}$, $L_f = (L_f(\alpha,\beta))_{\alpha,\beta\in V_n}$, $D_{f,+} = (D_{f,+}(\alpha,\beta))_{\alpha,\beta\in V_n}$ та $A_{f,+} = (A_{f,+}(\alpha,\beta))_{\alpha,\beta\in V_n}$, вважаючи

$$C_f(\alpha,\beta) = 2^{-n}\sum_{x\in V_n}(-1)^{\alpha f(x)\oplus\beta x},\ \alpha,\beta\in V_n, \qquad (15)$$

$$L_f(\alpha,\beta) = (2\mathbf{P}_X\{\alpha X = \beta f(X)\} - 1)^2,\ \alpha,\beta\in V_n, \qquad (16)$$

$$D_{f,+}(\alpha,\beta) = \mathbf{P}_X\{f(X+\alpha)\oplus f(X) = \beta\},\ \alpha,\beta\in V_n, \qquad (17)$$

$$A_{f,+}(\alpha,\beta) = 2^{-n}\sum_{x\in V_n}(-1)^{\beta(f(x+\alpha)\oplus f(x))},\ \alpha,\beta\in V_n, \qquad (18)$$

де у виразах (16) і (17) X позначає випадковий вектор з рівномірним законом розподілу на множині V_n. Матриці (15) і (16) співпадають (з точністю до нормуючих множників) з кореляційною матрицею [14] і таблицею розподілу кореляційної імунності [15] підстановки f відповідно, а матриці (17) і (18) (у випадку, коли $+ = \oplus$) – відповідно з таблицею розподілу різниць і таблицею розподілу автокореляції підстановки f [15]. (Декілька інша термінологія використовується в [4, 7], де матриця (2), з точністю до співмножника 2^{-n}, називається таблицею лінійних апроксимацій, а матриця (5) – автокореляційною таблицею підстановки f).

Нехай $\mathfrak{I}$ – блоковий шифр з множиною відкритих (шифрованих) повідомлень V_n, множиною ключів K та сім'єю шифрувальних перетворень $(F_k : k \in K)$. Тоді матриці $C_{\mathfrak{I}}$, $L_{\mathfrak{I}}$, $D_{\mathfrak{I},+}$ та $A_{\mathfrak{I},+}$ визначаються як середні арифметичні за всіма $k\in K$ значення матриць C_{F_k}, L_{F_k}, $D_{F_k,+}$ та $A_{F_k,+}$ відповідно.

Загальновідомо, що максимальні елементи матриць $L_{\mathfrak{I}}$ та $D_{\mathfrak{I},+}$, що містяться в їх рядках та стовпцях з ненульовими номерами, характеризують стійкість шифру $\mathfrak{I}$ відносно лінійного та диференціального методів криптоаналізу відповідно. При цьому на підставі твердження 3 спроможність цього шифру протистояти наведеній вище диференціально-лінійній атаці (у випадку $\alpha = \beta$) характеризується максимальним значенням квадратів елементів матриці $A_{\mathfrak{I},+}$, які містяться у її рядках та стовпцях з ненульовими номерами.

Відзначимо взаємозв'язок між матрицями (15) – (18).

Перш за все, безпосередньо з формул (15), (16) випливає рівність

$$L_f(\alpha,\beta) = C_f(\beta,\alpha)^2,\ \alpha,\beta\in V_n. \qquad (19)$$

Далі, позначимо $H_n = ((-1)^{\alpha\beta})_{\alpha,\beta\in V_n}$ матрицю Адамара абелевої групи $(V_n,\oplus)$, $\Pi_f = (\delta(f(\alpha),\beta))_{\alpha,\beta\in V_n}$ – підстановочну матрицю, що відповідає підстановці $f\in\sigma(V_n)$ (тут і

далі δ позначає символ Кронекера: $\delta(f(\alpha),\beta)=1$, якщо $f(\alpha)=\beta$; $\delta(f(\alpha),\beta)=0$ – у протилежному випадку). Справедливі такі рівності:

$$C_f = 2^{-n} H_n \Pi_f^{\,T} H_n,\ D_{f,\oplus} = 2^{-n} H_n L_f H_n, \tag{20}$$

перше з яких випливає безпосередньо з наведених означень, а друге – доведено в [16]. З першої формули (20) випливає, що матриця C_f є ортогональною. Отже, на підставі рівностей (17) та (19) матриці L_f та D_f є двічі стохастичними.

Справедливі також наступні рівності, що пов'язують між собою матриці (3), (4) та (5) у випадку $+=\oplus$ [15]:

$$A_{f,\oplus} = D_{f,\oplus} H_n = H_n L_f. \tag{21}$$

У загальному випадку справедлива рівність

$$A_{f,+} = D_{f,+} H_n, \tag{22}$$

яка доводиться шляхом безпосередньої перевірки.

Безпосередньо з формул (21), (22) випливає наступна лема.

Лема 4. Нехай $\mathfrak{I}$ є блоковим шифром з множиною відкритих (шифрованих) повідомлень V_n. Тоді $A_{\mathfrak{I},+} = D_{\mathfrak{I},+} H_n$ і $A_{\mathfrak{I},\oplus} = D_{\mathfrak{I},\oplus} H_n = H_n L_{\mathfrak{I}}$.

Матричні співвідношення (8) дозволяють швидко отримати один з основних результатів роботи [4], оригінальне доведення якого є більш складним.

Для будь-яких підстановок $f, g \in \sigma(V_n)$ позначимо $f \circ g$ їх композицію: $(f \circ g)(x) = f(g(x))$, $x \in V_n$. Слідуючи [4], назвемо ці підстановки диференціально (лінійно) незалежними, якщо $D_{f\circ g} = D_g D_f$ ($L_{f\circ g} = L_g L_f$). Зауважимо, що на підставі другої рівності (21) диференціальна незалежність підстановок на множині V_n рівносильна їх лінійній незалежності (див. твердження 2 в [4]).

Наступна лема є матричним аналогом теореми 2 в [4].

Лема 5. Якщо підстановки $f, g \in \sigma(V_n)$ є диференціально (лінійно) незалежними, то $A_{f\circ g} = A_g L_f$.

Доведення. Дійсно, $A_{f\circ g} = D_{f\circ g} H_n = D_g D_f H_n = D_g H_n (2^{-n} H_n) D_f H_n = A_g L_f$. Лему доведено.

За означенням [9] блоковий шифр $\mathfrak{I}$ називається марковським (відносно операції $\oplus$), якщо для будь-яких $x, \alpha, \beta \in V_n$ виконується рівність $D_{f,\oplus}(\alpha,\beta) = \mathbf{P}_k\{F_k(x\oplus\alpha) \oplus F_k(x) = \beta\}$.

Якщо $\mathfrak{I}_1$ і $\mathfrak{I}_2$ – блокові шифри з множиною відкритих (шифрованих) повідомлень V_n та сім'ями шифрувальних перетворень $(F'_{k'} : k' \in K')$ і $(F''_{k''} : k'' \in K'')$ відповідно, то їх добуток $\mathfrak{I} = \mathfrak{I}_1 \mathfrak{I}_2$ визначається як блоковий шифр з сім'ю шифрувальних перетворень $(F_k : k \in K)$, де $K = K' \times K''$, $F_k(x) = F''_{k''}(F'_{k'}(x))$, $x \in V_n$, $k = (k', k'') \in K$.

Твердження 5. Нехай $\mathfrak{I} = \mathfrak{I}_1 \mathfrak{I}_2$, де $\mathfrak{I}_2$ є марковським шифром. Тоді $A_{\mathfrak{I},+} = A_{\mathfrak{I}_1,+} L_{\mathfrak{I}_2}$.

Доведення. З марковості шифру $\mathfrak{I}_2$ випливає рівність $D_{\mathfrak{I},+} = D_{\mathfrak{I}_1,+} D_{\mathfrak{I}_2,\oplus}$. Звідси, використовуючи лему 2, отримаємо, що

$$A_{\mathfrak{I},+} = D_{\mathfrak{I},+} H_n = D_{\mathfrak{I}_1,+} D_{\mathfrak{I}_2,\oplus} H_n = (D_{\mathfrak{I}_1,+} H_n)(2^{-n} H_n D_{\mathfrak{I}_2,\oplus} H_n) = A_{\mathfrak{I}_1,+} L_{\mathfrak{I}_2}.$$

Твердження доведено.

Розглянемо більш загальні (в порівнянні з числами (18)) параметри, введені в [7], які визначають стійкість блокових шифрів відносно диференціально-лінійного методу криптоаналізу. А саме, для будь-яких $f \in \sigma(V_n)$, $a \in V_n$ позначимо $\Delta_{f,+,a}$ матрицю з елементами

$$\Delta_{f,+,a}(\alpha,\beta)=2^{-n}\sum_{x\in V_n}(-1)^{\alpha f(x)\oplus\beta f(x+a)},\ \alpha,\beta\in V_n. \qquad (23)$$

Зауважимо, що $\Delta_{f,+,a}(\alpha,\alpha)=A_{f,+}(a,\alpha)$. В роботі [7] набір, що складається з чисел (23) за всіма $a\in V_n$ (для випадку $+=\oplus$), названо узагальненою автокореляційною таблицею підстановки f.

Якщо $\mathfrak{I}$ – блоковий шифр з множиною відкритих (шифрованих) повідомлень V_n та сім'єю шифрувальних перетворень $(F_k: k\in K)$, то на підставі твердження 3 його стійкість відносно наведеної в п. 1 диференціально-лінійної атаки визначається параметром

$$(2\mathbf{P}_{x,k}\{\alpha F_k(x)=\beta F_k(x+a)\}-1)^2=\left(|K|^{-1}\sum_{k\in K}(\Delta_{F_k,+,a}(\alpha,\beta))^2\right).$$

Отримаємо представлення цього параметра для шифру $\mathfrak{I}$, що є добутком двох довільних шифрів.

Твердження 6. Нехай $\mathfrak{I}=\mathfrak{I}_1\mathfrak{I}_2$, де $\mathfrak{I}_1$ і $\mathfrak{I}_2$ – блокові шифри з множиною відкритих (шифрованих) повідомлень V_n та сім'ями шифрувальних перетворень $(F'_{k'}: k'\in K')$ і $(F''_{k''}: k''\in K'')$ відповідно. Тоді для будь-яких $a\in V_n$, $k=(k',k'')\in K'\times K''$ справедлива рівність $\Delta_{F_k,+,a}=C_{F''_{k''}}\Delta_{F'_{k'},+,a}(C_{F''_{k''}})^T$, де матриця $C_{F''_{k''}}$ визначається згідно з формулою (15).

Доведення. Для будь-яких підстановок $f_1, f_2\in\sigma(V_n)$ має місце рівність

$$C_{f_2\circ f_1}=C_{f_2}C_{f_1}, \qquad (24)$$

справедливість якої випливає з формули $\Pi_{f_2\circ f_1}=\Pi_{f_1}\Pi_{f_2}$ та першої рівності (20).

Покладемо $f_1=F'_{k'}$, $f_2=F''_{k''}$, $f=F_k=F''_{k''}\circ F'_{k'}$ та позначимо T_a підстановку, що реалізує зсув на вектор a: $T_a(x)=x+a$, $x\in V_n$. Використовуючи у формулі (23) заміну змінних $x=f^{-1}(y)$, отримаємо, що

$$\Delta_{f,+,a}(\alpha,\beta)=2^{-n}\sum_{y\in V_n}(-1)^{\alpha y\oplus\beta f(f^{-1}(y)+a)}=2^{-n}\sum_{y\in V_n}(-1)^{\alpha y\oplus\beta(f\circ T_a\circ f^{-1})(y)}=C_{f\circ T_a\circ f^{-1}}(\beta,\alpha).$$

Аналогічно отримаємо, що $\Delta_{f_1,+,a}(\alpha,\beta)=C_{f_1\circ T_a\circ f_1^{-1}}(\beta,\alpha)$. Звідси, використовуючи формулу (24), отримаємо рівності:

$$\Delta_{f,+,a}(\alpha,\beta)=(C_{f_2}(C_{f_1}C_{T_a}C_{f_1}^{-1})C_{f_2}^{-1})(\beta,\alpha)=(C_{f_2}\Delta_{f_1,+,a}C_{f_2}^{-1})(\beta,\alpha)=C_{f_2}\Delta_{f_1,+,a}(C_{f_2})^T(\beta,\alpha),$$

з яких на підставі симетричності матриць $\Delta_{f,+,a}$, $\Delta_{f_1,+,a}$ випливає формула (24).

Твердження доведено.

Зауважимо, що отримане твердження надає явний вираз параметра вигляду (23) (а отже, й параметрів вигляду (18)) для довільного блокового шифру $\mathfrak{I}$ в термінах кореляційних матриць перетворень його співмножників $\mathfrak{I}_1$ і $\mathfrak{I}_2$, не використовуючи при цьому жодних додаткових припущень про шифр (на кшталт тих, що робляться в [1 – 5]).

Висновки

1. В роботі отримано нижні оцінки інформаційної складності двох видів диференціально-лінійних атак на блокові шифри, а саме, розрізнювальних атак і атак, спрямованих на відновлення одного біту інформації про ключ. Отримані вирази зазначених оцінок залежать від усереднених (за ключами) значень квадратів елементів узагальнених автокореляційних таблиць шифрувальних перетворень. На відміну від відомих [1, 2, 4], отримані оцінки не базуються на жодних евристичних припущеннях відносно блокових шифрів, що досліджуються,

та є справедливими для більш широкого класу атак в порівнянні з традиційною диференціально-лінійною атакою.

2. У важливому окремому випадку отримано явний вираз середнього значення параметра, який фігурує в зазначених вище оцінках, для випадкової рівноймовірної підстановки на множині повідомлень, що шифруються. Аналогічно диференціальному або лінійному методам криптоаналізу цей результат надає можливість порівнювати диференціально-лінійні властивості бієктивних булевих відображень з аналогічними властивостями "ідеального" криптографічного відображення, тобто випадкової рівноймовірної підстановки.

3. Наведено співвідношення, які встановлюють взаємозв'язок між, відповідно, диференціальними, лінійними та диференціально-лінійними властивостями бієктивних булевих відображень. На відміну від відомих робіт [4, 6, 8], використовується матрична форма запису співвідношень, що дозволяє краще з'ясувати їх сутність та спростити доведення. Отримано також нове співвідношення для елементів узагальненої автокореляційної таблиці блокового шифру, що є добутком двох довільних шифрів. Це співвідношення не базується на жодних додаткових припущеннях про шифр (на кшталт таких, що робляться в [1 – 5]) та може бути корисним в подальших дослідженнях ефективності диференціально-лінійного методу криптоаналізу.

Список літератури:

1. Langford S., Hellman M. Differential-linear cryptanalysis // Advanced in Cryptology – Crypto 1994, LNCS. Vol. 839. 1994. P. 17 – 25.
2. Biham E., Dunkelman O., Keller N. Enhancing differential-linear cryptanalysis // Advanced in Cryptology – ASIACRYPT 2002, LNCS. Vol. 2401. 2002. P. 254 – 266.
3. Lu J. A methodology for differential-linear cryptanalysis and its applications // Designs, Codes and Cryptography. 2015. Vol. 77. № 1. P. 11 – 48.
4. Blondeau C., Leander G., Nyberg K. Differential-linear cryptanalysis revisited // J. Cryptology. 2017. Vol. 30. № 3. P. 859 – 888.
5. Bar-On A., Dunkelman O., Keller N., Weizman A. DLCT: a new tool for differential-linear cryptanalysis // Cryptology ePrint Archive, Report 2019/256. http://eprint.iacr.org/2019/256.
6. Алексейчук А.Н. Неасимптотические нижние границы информационной сложности статистических атак на симметричные криптосистемы // Кибернетика и системный анализ. 2018. Т. 54. № 1. С. 93 – 104.
7. Nyberg K. The extended autocorrelation and boomerang tables and links between nonlinearity properties of vectorial Boolean functions // Cryptology ePrint Archive, Report 2019/1381. http://eprint.iacr.org/2019/1381.
8. Canteuat A., Koelsch L., Li Ch. [et al.] On the differential-linear connectivity table of vectorial Boolean function // CoRR, abs/190807455. 2019.
9. Lai X., Massey J.L., Murphy S. Markov ciphers and differential cryptanalysis // Advances in Cryptology – EUROCRYPT'91, Proceedings. – Springer Verlag, 1991. P. 17 – 38.
10. Harpes C., Kramer G.G., Massey J.L. A generalisation of linear cryptoanalysis and the applicability of Matsui's piling-up lemma // Advances in Cryptology – EUROCRYPT'95, Proceedings. – Springer Verlag, 1995. P. 24 – 38.
11. Hoeffding W. Probability inequalities for sums of bounded random variables // J. Amer. Statist. Assoc. 1963. Vol. 58. № 301. P. 13 – 30.
12. Логачев О.А., Сальников А.А., Ященко В.В. Булевы функции в теории кодирования и криптологии. Москва : МЦНМО, 2004. 470 с.
13. Сачков В.Н. Введение в комбинаторные методы дискретной математики. Москва : Наука, 1982. 384 с.
14. Daemen J., Govards R., Vandervalle J. Correlation matrices // Fast Software Encryption – FSE'94, LNCS. Vol. 1008. 1994. P. 275 – 285.
15. Zhang X.-M., Zheng J., Imai H. Relating differential distribution tables to other properties of substitution boxes // Des. Codes Cryptography. 2000. Vol. 19. № 1. P. 45 – 63.
16. Chabaud F., Vaudenay S. Links between differential and linear cryptanalysis // Advanced in Cryptology – EUROCRYPT'94, LNCS. Vol. 950. 1994. P. 356 – 365.

Надійшла до редколегії 03.02.2021

Відомості про автора:

Олексійчук Антон Миколайович – д-р техн. наук, доцент, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "КПІ", професор кафедри Кібербезпеки; Україна; e-mail: alex-dtn@ukr.ne

УДК 004.056.55 **DOI:10.30837/rt.2021.1.204.02**

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

ГЕНЕРАЦІЯ ЗАГАЛЬНОСИСТЕМНИХ ПАРАМЕТРІВ ДЛЯ СХЕМИ ЕЛЕКТРОННОГО ПІДПИСУ RAINBOW ДЛЯ 384 ТА 512 БІТ БЕЗПЕКИ

Вступ

Наразі спостерігається стрімкий прогрес у створенні квантових комп'ютерів щодо вирішення різних обчислювально складних задач та для різних цілей. При цьому особливі зусилля докладаються до створення такого квантового комп'ютера, що зможе вирішувати задачі криптоаналізу існуючих криптосистем – асиметричних шифрів, протоколів інкапсуляції ключів, електронних підписів тощо. Попередження таких загроз може бути досягнуто засобом розробки таких криптографічних систем, що будуть захищені як від квантових, так і від класичних атак, а також зможуть взаємодіяти з протоколами і мережами зв'язку, що вже існують. Також є суттєва необхідність захисту від атак сторонніми каналами.

На даний момент значні зусилля криптологів зосереджені на відкритому конкурсі NIST PQC [1]. Основною ідеєю конкурсу є визначення математичних методів, на основі яких можуть бути розроблені стандарти на асиметричні криптоперетворення, в першу чергу електронного підпису (ЕП), а також асиметричні шифри та протоколи інкапсуляції ключів. За підсумками другого етапу фіналістами третього етапу конкурсу NIST PQC стали три схеми ЕП – Crystals-Dilithium, Falcon та Rainbow [1]. Наразі всесторонній аналіз фіналістів є важливою задачею для усієї світової криптоспільноти. Переважна більшість схем, що стали фіналістами, ґрунтується на проблемах з теорії алгебраїчних решіток [2 – 4]. Також особлива увага була приділена схемі ЕП Rainbow, що ґрунтується на основі багатовимірних перетворень [1].

Схема ЕП Rainbow значно відрізняється від інших кандидатів конкурсу NIST, оскільки заснована на багатовимірних перетвореннях. Вона є узагальненням структури UOV [5], що забезпечує ефективну параметризацію алгоритму ЕП за рахунок додаткової алгебраїчної структури. Теоретична безпека Rainbow ґрунтується на тому, що вирішення набору випадкових багатовимірних квадратичних систем є NP-складною проблемою [6]. Авторами методу Rainbow заявлено досягнення EUF-CMA моделі безпеки, що засновано на використанні геш-конструкції з випадковим чи псевдовипадковим ключем сеансу (сіллю). Також запропоновано дуже малі ЕП, буквально лише в кілька сотень бітів (лише 528 біт (66 байт) для I рівня безпеки NIST). У порівнянні з іншими кандидатами конкурсу NIST на постквантову схему ЕП вони є набагато коротшими. Крім того, оскільки Rainbow використовує лише прості операції над невеликими скінченими полями, то процеси вироблення та перевірки підпису є надзвичайно ефективними [6]. Крім того, спектр параметрів Rainbow дозволяє оптимізувати їх застосування у широкому діапазоні випадків. Схема ЕП Rainbow також вивчалась в інших контекстах та має певні переваги, у тому числі, наприклад, у малоресурсних додатках.

Показано, що для гарантованого забезпечення криптографічної стійкості ЕП Rainbow необхідно обґрунтувати вимоги та побудувати набори загальносистемних параметрів, за яких забезпечується стійкість до класичних і квантових атак. При визначенні вимог до системних параметрів схеми Rainbow NIST у рамках конкурсу зупинився на загальносистемних параметрах, що забезпечать 256 біт стійкості проти класичного та до 128 біт проти квантового криптоаналізу. Дані обмеження, на нашу думку, в тому числі пов'язані зі складністю обчислення загальносистемних параметрів, а також із суттєвим впливом їх збільшення на швидкодію електронного підпису. Проте, зважаючи на нинішнє застосування симетричних криптоперетворень на рівні стійкості у 512 біт, вважаємо, що уже наразі необхідно розглянути та реалізувати на основі схеми Rainbow ЕП зі стійкістю включно до 512 бітів. Але для цього необхідно обґрунтувати основні положення та вимоги до загальносистемних параметрів таких довжин, а також безпосередньо їх побудувати. При цьому повинна бути забезпечена

криптографічна стійкість від класичних та квантових атак відповідних значень, а також захист від атак сторонніми каналами.

Метою цієї статі є попередній аналіз існуючих атак щодо перспективного електронного підпису Rainbow, визначення вимог до загальносистемних параметрів для забезпечення криптографічної стійкості включно не менше 512 біт проти класичного та 256 біт проти квантового криптоаналізу, а також розроблення та практична реалізація щодо Rainbow алгоритмів генерації загальносистемних параметрів для 512 біт проти класичного та 256 біт проти квантового криптоаналізу.

1. Сутність механізму ЕП Rainbow

Розглянемо основні складові перетворень Rainbow – генерування загальносистемних параметрів та безпосередньо криптоперетворення. Схема ЕП Rainbow заснована на багатовимірних перетвореннях. Для багатовимірних схем з відкритим ключем відкритий ключ задається набором нелінійних багатовимірних поліномів над скінченим полем. Загалом, ключ багатовимірної криптосистеми з відкритим ключем – це система багатовимірних квадратичних поліномів з *n* змінними та *m* рівняннями [6, 7]:

$$\begin{aligned} p^{(1)}\left(x_1,\ldots,x_n\right) &= \sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij}^{(1)}\cdot x_i x_j + \sum_{i=1}^{n} p_i^{(1)}\cdot x_i + p_0^{(1)} \\ p^{(2)}\left(x_1,\ldots,x_n\right) &= \sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij}^{(2)}\cdot x_i x_j + \sum_{i=1}^{n} p_i^{(2)}\cdot x_i + p_0^{(2)} \\ &\vdots \\ p^{(m)}\left(x_1,\ldots,x_n\right) &= \sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij}^{(m)}\cdot x_i x_j + \sum_{i=1}^{n} p_i^{(m)}\cdot x_i + p_0^{(m)} \end{aligned} . \tag{1}$$

Усі коефіцієнти та змінні походять з F_q – скінченого поля з q елементами. По суті сукупність загальновідомих поліномів

$$\mathrm{P}\left(x_1,\ldots,x_n\right) = \left(p^{(1)}\left(x_1,\ldots,x_n\right),\ldots,p^{(m)}\left(x_1,\ldots,x_n\right)\right) \tag{2}$$

математично являє собою відображення F_q^n до F_q^m. Операції зашифрування повідомлення або верифікації підпису полягають у простому оцінюванні $\mathrm{P}\left(x_1,\ldots,x_n\right)$ з використанням відкритого ключа. Процес розшифрування зашифрованого тексту, а також вироблення ЕП зводиться до здійснення «інверсії» відображення $\mathrm{P}\left(x_1,\ldots,x_n\right)$ з використанням секретного (особистого) ключа. Ці складові еквівалентні вирішенню проблеми стійкості MQ-перетворення.

Схему ЕП Rainbow [7] з u рівнями можна описати наступним чином. Нехай F_q – скінчене поле з q елементами, а $\upsilon_1 < \upsilon_2 < \cdots < \upsilon_u < \upsilon_{u+1} = n$ – цілі числа. Обираємо $V_i = \{1,\ldots,\upsilon_i\}$, $o_i = \upsilon_{i+1} - \upsilon_i$ та $O_i = \{\upsilon_i,\ldots,\upsilon_{i+1}\}$, де $(i = 1,\ldots,u)$. Таким чином отримаємо $|V_i| = \upsilon_i$ і $|O_i| = o_i$, де $(i = 1,\ldots,u)$.

Центральне відображення F Rainbow складається з $m = n - \upsilon_1$ багатовимірних квадратичних поліномів $f^{(\upsilon_1+1)},\ldots,f^{(n)}$ виду

$$f^{(k)}(\mathbf{x}) = \sum_{i,j\in V_\ell} \alpha_{ij}^{(k)} x_i x_j + \sum_{i\in V_\ell,\, j\in O_\ell} \beta_{ij}^{(k)} x_i x_j + \sum_{i\in V_\ell\cup O_\ell} \gamma_i^{(k)} x_i + \eta^{(k)}, \tag{3}$$

де $\ell \in \{1,\ldots,u\}$ – єдине ціле число, таке, що $k \in O_\ell$.

Зауважимо, що в кожному поліномі $f^{(k)}$ при $k \in O_\ell$ немає квадратного члена $x_i x_j$, де i та j знаходяться в O_ℓ. Цей факт використаний авторами [7] для вироблення ЕП. Такі поліноми називали поліномами Oil-Vinegar, коли пропонувались схеми OV [5].

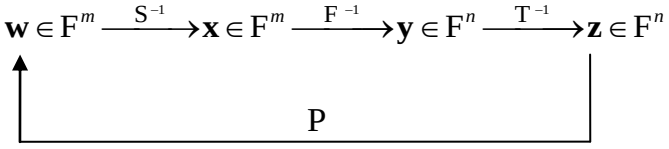
Щоб приховати структуру F у відкритому ключі, його складають з двома оберненими афінними або лінійними відображеннями $S : F^m \to F^m$ та $T : F^n \to F^n$. Отже, відкритий ключ Rainbow має вигляд $P = S \circ F \circ T : F^n \to F^m$, секретний ключ складається з трьох відображень S, F і T, а, отже, дозволяє інвертувати відображення відкритого ключа.

Щоб виконати ЕП для повідомлення $\mathbf{w} \in F^m$, необхідно виконати наступні три кроки.

1. Обчислити $\mathbf{x} = S^{-1}(\mathbf{w}) \in F^m$.
2. Обчислити попереднє відображення $\mathbf{y}$ з $\mathbf{x}$ під центральним відображенням F, використовуючи алгоритм інверсії, тобто $\mathbf{y} = F^{-1}(\mathbf{x}) \in F^n$.
3. Обчислити підпис $\mathbf{z} \in F^n$, $\mathbf{z} = T^{-1}(\mathbf{y})$.

Для підтвердження того, що $\mathbf{z} \in F^n$ є дійсним підписом для повідомлення $\mathbf{w} \in F^m$, необхідно обчислити $\mathbf{w}' = P(\mathbf{z})$. Якщо виконується рівність $\mathbf{w}' = \mathbf{w}$, підпис є дійсним. Процес генерації підпису та верифікації зображено на рис. 1.

Генерація підпису



Верифікація підпису

Рис. 1. Процес генерації та верифікації підпису Rainbow

2. Атаки на Rainbow

Нижче розглянуто низку атак на схему ЕП Rainbow, а саме пряму атаку, атаку MinRank та HighRank, атаку UOV та атаку «Rainbow Band Separation» (RBS) [1].

Хоча атаки прямої та грубої сили є атаками підробки підпису, які потрібно виконувати для кожного повідомлення окремо, атаки RBS та UOV є ключовими атаками відновлення. Після відновлення секретного ключа Rainbow за допомогою однієї з цих атак криптоаналітик може виробляти підписи так само, як законний користувач.

2.1. Прямі атаки

Найбільш прямолінійною атакою на багатовимірну схему Rainbow є пряма алгебраїчна атака, в якій загальновідоме рівняння $P(\mathbf{z}) = \mathbf{h}$ розглядається як проблема MQ. Оскільки Rainbow – це невизначена система з $n \approx 1.5 \cdot m$ рівнянь, найефективнішим способом вирішення цієї системи є фіксація *n–m* змінних для створення детермінованої системи. Можна очікувати, що отримана детермінована система має рівно одне рішення. У деяких випадках отримують ще кращі результати, коли відгадують додаткові змінні перед вирішенням системи (гібридний підхід) [8]. Складність вирішення такої системи з *m* квадратних рівнянь у *m* змінних можна оцінити за допомогою рівності (4):

$$\text{Complexity}_{\text{direct;classical}} = \min_k \left(q^k \cdot 3 \cdot \binom{m-k+d_{reg}}{d_{reg}}^2 \cdot \binom{m-k}{2} \right) \tag{4}$$

множень у полі, де d_{reg} – це так званий ступінь регулярності системи.

Ступінь регулярності системи можна оцінити як найменше ціле число d, для якого коефіцієнт t^d в

$$\frac{\left(1-t^2\right)^m}{\left(1-t\right)^{m-k}} \tag{5}$$

не є додатним.

За наявності квантових комп'ютерів додатковий крок вгадування гібридного підходу може бути прискорений алгоритмом Гровера. Застосовуючи такий підхід, можливо оцінити складність квантової прямої атаки наступним чином.

$$\text{Complexity}_{\text{direct;quantum}} = \min_k \left(q^{k/2} \cdot 3 \cdot \binom{m-k+d_{reg}}{d_{reg}}^2 \cdot \binom{m-k}{2} \right) \tag{6}$$

множень у полі.

2.2. MinRank атака

Під час атаки MinRank криптоаналітик намагається знайти лінійну комбінацію загальновідомих поліномів мінімального рангу. У випадку з Rainbow така лінійна комбінація рангу υ_2 відповідає лінійній комбінації центральних поліномів першого рівня. Таким чином, знаходячи o_1 цих лінійних комбінацій низького рангу, можна ідентифікувати центральні поліноми першого рівня та відновити еквівалентний секретний ключ Rainbow.

На сьогодні найбільш ефективний метод вирішення проблеми MinRank було запропонований у [9]. У цьому варіанті розглядається розкладання матриці низького рангу Q на $Q = S \cdot C$, де S – це $n \times r$, а C – це $r \times n$ матриці, що представляють простір рядків матриці Q. Визначається матриця $C'_j = \begin{pmatrix} r_j \\ C \end{pmatrix}$ і приймаються за нуль $r+1$ мінорів цих C_j матриць. Оскільки отримана система має набагато більше рівнянь, ніж змінних, ми можемо вирішити її шляхом лінеаризації за допомогою алгоритму Відемана.

Зокрема, кількість рівнянь у системі задається як $m \cdot \binom{n}{r+1}$, де $\binom{n}{r+1}$ – це кількість $r+1$ мінорів матриці C'_j. Кількість змінних у системі дорівнює $\left(o_2+1\right) \cdot \binom{n}{r}$. Отже, якщо нерівність

$$\left(o_2+1\right) \cdot \binom{n}{r+1} \geq \left(o_2+1\right) \cdot \binom{n}{r} - 1 \tag{7}$$

справедлива, то можливо розв’язати систему за допомогою алгоритму Відемана. Тому складність вирішення цієї системи задається як

$$\text{Complexity}_{\text{MinRank}} = 3 \cdot \left(\left(\left(o_2+1\right) \cdot \binom{n'}{r} \right)^2 \cdot \left(r+1\right) \cdot \left(o_2+1\right) \right). \tag{8}$$

Ретельний аналіз показав, що не потрібно розглядати всі *n* рядків матриці C'_j, щоб мати можливість вирішити систему. Число n' у (8) позначає найменше число, для якого виконується нерівність (7).

2.3. Атака HighRank

Метою атаки HighRank [10] є виявлення (у лінійному представленні) змінних, що з'являються найменшу кількість разів у центральних поліномах (вони відповідають Oil-змінним останнього рівня Rainbow, тобто змінним x_i з $i \in O_u$).

Складність цієї атаки можна оцінити як

$$\text{Complexity}_{\text{HighRank; classical}} = q^{o_u} \cdot \frac{n^3}{6}. \tag{9}$$

За наявності квантових комп'ютерів можна прискорити крок пошуку за допомогою алгоритму Гровера. Таким чином отримаємо

$$\text{Complexity}_{\text{HighRank; quantum}} = q^{o_u/2} \cdot \frac{n^3}{6} \tag{10}$$

множень у полі.

2.4. UOV атака

Оскільки Rainbow можна розглядати як продовження добре відомої схеми підпису Oil та Vinegar [5], її можна атакувати, використовуючи всі відомі атаки UOV [11].

Можна розглядати Rainbow як екземпляр UOV з $\upsilon = \upsilon_1 + o_1$ та $o = o_2$. Метою даної атаки є пошук попереднього відображення так званого Oil підпростору O афінного перетворення T, де $\mathrm{O} = \left\{ \mathbf{x} \in \mathrm{F}^n : x_1 = \cdots = x_\upsilon = 0 \right\}$. Знаходження цього простору дозволяє відокремити Oil від змінних Vinegar та відновити закритий ключ.

Складність цієї атаки можна оцінити як

$$\text{Complexity}_{\text{UOV-Attack; classical}} = q^{n-2o_2-1} \cdot o_2^4 \tag{11}$$

множень у полі. Використовуючи алгоритм Гровера, цю складність можна зменшити до

$$\text{Complexity}_{\text{UOV-Attack; quantum}} = q^{\frac{n-2o_2-1}{2}} \cdot o_2^4 \tag{12}$$

множень у полі.

2.5. Атака RBS

Атака RBS [12] спрямована на пошук лінійних відображень S і T, що перетворюють загальновідомі поліноми в поліноми форми Rainbow (тобто значення $\mathrm{Oil} \times \mathrm{Oil}$ повинні бути нульовими). Для цього криптоаналітик повинен вирішити кілька нелінійних багатовимірних систем. Складність цього кроку визначається складністю вирішення першої (і найбільшої) з цих систем, яка складається з $n + m - 1$ квадратних рівнянь з n змінними. Однак поліноми в цій системі не є випадковими квадратичними поліномами, але існують дві групи змінних X і Y, такі, що поліноми є білінійними в X і Y.

Зокрема, отримуємо два набори змінних X та Y розміром $|X| = n_x = \upsilon_1 + o_1$ та $|Y| = n_y = o_2$. Маємо $m_x = x$ поліномів, які є квадратичними у змінних X, а $m_y = n - 1$ рівняння білінійні у змінних X та Y. Отже, складність атаки RBS можна оцінити як

$$Compl_{RBS} = \min_{\alpha,\beta} 3 \cdot \mathrm{M}_{\alpha,\beta}(t,s)^2 \cdot (n_x + 1) \cdot (n_y + 1), \tag{13}$$

де $\mathrm{M}_{\alpha,\beta}$ позначає кількість одночленів (α, β).

3. Генерація параметрів для 384, 512 біт стійкості

У цьому підрозділі наведено вибір (генерацію) параметрів для 384 та 512 біт стійкості над полем GF(256). Під час вибору параметрів керувалися такими умовами:

– кількість рівнянь, що нам необхідна, залежить від складності прямої атаки та атаки на геш-функцію;
– кількість змінних залежить від складності атак RBS, UOV та HighRank.

Тож, якщо підсумувати сказане вище, то знайти параметри υ_1, o_1, o_2 при $q = 256$, тобто $GF(q) = GF(256)$, можливо з умов (4) – (13). На основі цього було розроблене програмне забезпечення, з використанням якого було згенеровано параметри υ_1, o_1 та o_2 для ЕП Rainbow для 384 та 512 біт безпеки, що наведені в табл. 1.

Таблиця 1

Основні загальносистемні параметри Rainbow
для 384, 512 біт безпеки

Безпека	υ_1	o_1	o_2	$GF(q)$
384	192	48	136	$GF(256)$
512	272	120	128	$GF(256)$

При таких параметрах отримуємо наступні розміри ключів, гешування та підписів для трьох версій Rainbow: класичної (Classic), циклічної (CZ-Rainbow), та стисненої (Compressed), що наведені в табл. 2 – 4 відповідно.

Таблиця 2

Розміри ключів та підписів Classic Rainbow

Безпека	Набір параметрів $(\mathrm{F}, \upsilon_1, o_1, o_2)$	Розмір відкритого ключа (байтів)	Розмір закритого ключа (байтів)	Розмір гешу (байтів)	Розмір підпису (байтів)
384	$(GF(256), 192, 48, 136)$	13041184	9752288	64	392
512	$(GF(256), 272, 120, 128)$	33594080	24752480	64	536

Таблиця 3

Розміри ключів та підписів CZ-Rainbow

Безпека	Набір параметрів $(\mathrm{F}, \upsilon_1, o_1, o_2)$	Розмір відкритого ключа (байтів)	Розмір закритого ключа (байтів)	Розмір гешу (байтів)	Розмір підпису (байтів)
384	$(GF(256), 192, 48, 136)$	3337344	9752288	64	392
512	$(GF(256), 272, 120, 128)$	8939840	24752480	64	536

Таблиця 4

Розміри ключів та підписів Compressed Rainbow

Безпека	Набір параметрів $(\mathrm{F}, \upsilon_1, o_1, o_2)$	Розмір відкритого ключа (байтів)	Розмір закритого ключа (байтів)	Розмір гешу (байтів)	Розмір підпису (байтів)
384	$(GF(256), 192, 48, 136)$	3337344	64	64	392
512	$(GF(256), 272, 120, 128)$	8939840	64	64	536

Швидкодія при заданих параметрах для трьох версій Rainbow, що представлена в тактах процесора, наведена в табл. 5 – 7 відповідно.

Таблиця 5

Швидкодія Classic Rainbow

Набір параметрів	Генерація ключів	Генерація підпису	Верифікація підпису
384	4658727146	16484356	2645458
512	16999329532	43986312	8165628

Таблиця 6

Швидкодія CZ-Rainbow

Набір параметрів	Генерація ключів	Генерація підпису	Верифікація підпису
384	4658375168	16799206	2927814
512	16900406374	52017328	10617618

Таблиця 7

Швидкодія Compressed Rainbow

Набір параметрів	Генерація ключів	Генерація підпису	Верифікація підпису
384	4631048528	16288184	2398794
512	16694833556	44923458	7611730

Висновки

1. Однією із важливих проблем сучасної криптографії є створення стандартів асиметричних криптографічних перетворень ЕП, які були б безпечними у постквантовий період. Вирішення цієї проблеми здійснюється в процесі міжнародного конкурсу NIST США, завданням якого є розробка такого механізму ЕП, який би був стійким як до квантових, так і до класичних атак.

2. Фіналістами конкурсу NIST США на схему ЕП стали: Crystals-Dilithium, Falcon та Rainbow. Переважна більшість схем, що стали фіналістами, ґрунтується на проблемах з теорії алгебраїчних решіток. Також особлива увага була приділена схемі електронного підпису Rainbow, що ґрунтується на основі багатовимірних перетворень.

3. Схема електронного підпису Rainbow значно відрізняється від інших кандидатів конкурсу NIST, оскільки заснована на багатовимірних перетвореннях. Вона є узагальненням структури UOV, що забезпечує ефективну параметризацію за рахунок додаткової алгебраїчної структури. Теоретична безпека Rainbow базується на тому, що вирішення набору випадкових багатовимірних квадратичних систем є NP-складною проблемою. Щодо проекту Rainbow заявлено EUF-CMA безпечність, вказане досягається на основі використання гешконструкції з випадковим ключем сеансу (сіллю).

4. Процес вироблення ЕП Rainbow складається з простих операцій лінійної алгебри, таких як множення матричних векторів та вирішення лінійних систем над малими скінченими полями. Також Rainbow забезпечує малі, у порівнянні з іншими підписи, по суті лише в кілька сотень бітів.

5. Основним недоліком ЕП Rainbow є великий розмір відкритих ключів. Тому його застосування рекомендується у системах, де можуть бути використаними відкриті ключі значних розмірів. Розміри загальносистемних параметрів та ключів для випадку забезпечення 384 та 512 біт безпеки наведені в табл. 2 – 4.

6. Також із табл. 5 – 7 видно, що процес верифікації ЕП CZ-Rainbow значно повільніший, ніж у стандартній схемі Rainbow. Однак необхідно зазначити, що це спричинене використанням криптографічно захищеного PRNG на базі AES, що постачається OpenSSL (що є таким самим, що і у NIST), для створення «фіксованих» частин відкритого ключа. Використовуючи швидший потоковий шифр або навіть генеруючи відкритий ключ, використовуючи регістр лінійного зворотного зсуву (LFSR), цього уповільнення можна уникнути майже повністю.

7. Було розглянуто низку атак на схему ЕП Rainbow, а саме – пряму атаку, атаку MinRank та HighRank, атаку UOV та атаку «Rainbow Band Separation» (RBS). Хоча пряма атака є атакою підробки підпису, яка повинна виконуватися для кожного повідомлення окремо, атаки MinRank, HighRank, UOV та RBS є ключовими атаками відновлення. Після відновлення секретного ключа Rainbow за допомогою однієї з цих атак криптоаналітик може виробляти підписи так само, як законний користувач.

Обґрунтовані та обчислені загальносистемні параметри можуть бути використані для забезпечення підвищених рівнів безпеки ЕП Rainbow включно до 384 та 512 біт безпеки відпо-

відно з параметрами, що в цій статті обґрунтовані, а саме: $(GF(256),192,48,136)$ та $(GF(256),272,120,128)$ відповідно.

Список літератури:

1. 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.

2. Craig Gentry, Chris Peikert, Vinod Vaikuntanathan Trapdoors for hard lattices and new cryptographic constructions // Richard E. Ladner and Cynthia Dwork, editors, 40th ACM STOC, pages 197–206. ACM Press, May 2008.

3. Damien Stehlé, Ron Steinfeld Making NTRU as secure as worst-case problems over ideal lattices // Kenneth G. Paterson, editor, EUROCRYPT 2011, volume 6632 of LNCS, pages 27–47, Tallinn, Estonia, May 15–19, 2011. Springer, Heidelberg, Germany.

4. Thomas Prest Gaussian Sampling in Lattice-Based Cryptography. Theses, École Normale Supérieure, December 2015.

5. A. Kipnis, J. Patarin, L. Goubin Unbalanced Oil and Vinegar schemes // EUROCRYPT 1999, LNCS vol. 1592, pp. 206-222. Springer, 1999.

6. Rainbow Signature / Ding J. and other.2020. P. 16-22. Access mode: https://www.pqcrainbow.org/.

7. J. Ding, D. Schmidt Rainbow, a new multivariable polynomial signature scheme // ACNS 2005, LNCS vol. 3531, pp. 164-175. Springer, 2005.

8. J. Bonneau, I. Mironov Cache-Collision Timing Attacks Against AES. CHES 2006, LNCS vol. 4249, pp. 201-215. Springer, 2006.

9. Magali Bardet, Maxime Bros, Daniel Cabarcas, Philippe Gaborit, Ray A. Perlner, Daniel Smith-Tone, Jean-Pierre Tillich, Javier A. Verbel Algebraic attacks for solving the Rank Decoding and MinRank problems without Groebner basis. CoRR abs/2002.08322 (2020).

10. D. Coppersmith, J. Stern, S. Vaudenay Attacks on the birational signature scheme. CRYPTO 1994, LNCS vol. 773, pp. 435-443. Springer, 1994.

11. A. Kipnis, A. Shamir Cryptanalysis of the Oil and Vinegar signature scheme. CRYPTO 1998, LNCS vol. 1462, pp. 257-266. Springer, 1998.

12. J. Ding, B.-Y. Yang, C.-H. O. Chen, M.-S. Che, C.-M. Cheng: New differential-algebraic attacks and reparametrization of Rainbow // ACNS 2008, LNCS vol. 5037, pp. 242-257. Springer, 2008.

13. J. Ding, Z. Zhang, J. Deaton, K. Schmidt, F. Visakha New attacks on lifted unbalanced oil vinegar. The 2nd NIST PQC Standardization Conference, 2019.

14. A. Kipnis, A. Shamir Cryptanalysis of the Oil and Vinegar signature scheme. CRYPTO 1998, LNCS vol. 1462, pp. 257-266. Springer, 1998.

15. A. Petzoldt, S. Bulygin, J. Buchmann Cyclic Rainbow – a Multivariate Signature Scheme with a Partially Cyclic Public Key. INDOCRYPT 2010, LNCS vol. 6498, pp. 33 – 48. Springer, 2010.

16. A. Petzoldt: Efficient Key Generation for the Rainbow Signature Scheme. PQCrypto 2020.

17. E. Thomae C. Wolf: Solving Underdetermined Systems of Multivariate Quadratic Equations Revisited. PKC 2012, LNCS vol. 7293, pp. 156-171. Springer, 2012.

18. W. Beullens, B. Preneel, A. Szepieniec, F. Vercauteren LUOV signature scheme proposal for NIST PQC project (Round 2 version), 2019.

Надійшла до редколегії 05.02.2021

Відомості про авторів:

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 Олегович – АТ «Інститут інформаційних технологій», технік-конструктор, Україна; e-mail: sergeykandy@gmail.com

Острянська Єлизавета Вадимівна – АТ «Інститут інформаційних технологій», аналітик з систем захисту інформації, Україна; e-mail: antelizza@gmail.com

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, АТ «Інститут інформаційних технологій», головний конструктор; Україна; e-mail: GorbenkoI@iit.kharkov.ua; ORCID: https://orcid.org/0000-0003-4616-3449

УДК 621.391 **DOI:10.30837/rt.2021.1.204.03**

І.Д. ГОРБЕНКО, д-р техн. наук, О.В. ПОТІЙ, д-р техн. наук, О.А. ЗАМУЛА, д-р техн. наук

КОНЦЕПЦІЯ СИНТЕЗУ ОДНОГО КЛАСУ САМОСИНХРОНІЗУЮЧИХ ДИСКРЕТНИХ СИГНАЛІВ

Вступ

Відомо, що для мінімізації помилки при прийомі сигналів в широкосмугових комунікаційних системах (ШКС) відстань між векторами (сигналами) слід робити максимально великою [1]. У разі досить великої кількості сигналів завдання одночасної максимізації відстаней між усіма сигналами може виявитися складним, оскільки сигнали конфліктують між собою, «відсуваючи» один вектор від іншого, наближаючи його до деякого третього. Завдання побудови безлічі максимально віддалених сигналів входить в клас так званих завдань «упаковки». Очевидно, що для максимізації відстані між двома векторами їх слід вибирати протилежними. Саме ця умова забезпечує максимально досяжну ймовірність помилки при передачі двійкових даних сигналами з фіксованою енергією.

До теперішнього часу немає єдиної теорії синтезу систем дискретних сигналів (ДС) з заданими авто-, взаємно-, стиковими кореляційними властивостями. По суті, до сьогоднішнього дня в основному розвинена теорія аналізу і синтезу двійкових лінійних рекурентних послідовностей максимального періоду (ЛРПМ) і лінійних рекурентних послідовностей з трирівневою функцією взаємної кореляції (ЛРПТ) [1]. Однак, як показали дослідження [1, 2], введення жорстких обмежень на вид періодичної функції автокореляції (ПФАК) ДС суттєво обмежує можливість джерел сигналів з точки зору ансамблевих і структурних властивостей, а також, в більшості випадків, визначає лінійність законів їх формування. Авторами вперше отримано методи синтезу нового класу нелінійних складних дискретних сигналів – криптографічних сигналів [3 – 7]. Використання такого класу сигналів в якості фізичних переносників даних в комунікаційних системах, завдяки їх особливим ансамблевим, кореляційним, структурним і іншим властивостям, дозволяє поліпшити показники ефективності функціонування таких систем, зокрема інформаційної безпеки та завадозахищеності [8 – 10]. При цьому, кращим є вибір так званих, самосинхронізуючих систем сигналів (ССС) як переносників даних в комунікаційних системах. Використання таких систем сигналів передбачає реалізацію циклової синхронізації в режимі розрізнення сигналів безпосередньо за інформаційними сигналами. При проектуванні і використанні багатокористувачевих комунікаційних систем важливо застосовувати сигнали з максимальним індексом самосинхронізації, який визначається як максимальна відстань між всілякими стиковими словами і всіма інформаційними сигналами.

Основні результати досліджень

Сформулюємо в загальному вигляді, на основі комплексного використання апарату теорії поля Галуа, різницевих множин, комбінаторики, а також теорії чисел та наведемо рішення задачі синтезу ССС.

Нехай джерело ДС Q_W, що володіє з максимальною ентропією $H(Q_W) = \log P^L$, видає L – значні над полем $GF(P)$ дискретні послідовності (ДП) символів, закон формування яких задається t-мірними функціями N_p і f, що входять у вираз (1).

Простір станів каналу ШКС може бути описано функціоналом:

$$\psi = \varphi(L, N, \rho, R_a, R_b, R_H, R_C, D, x, y, S, I, N_p, f) \ , \qquad (1)$$

де L – безліч функцій, що описують закони розподілу тривалості сигналів L_i в словниках $\{W_j\}, i = \overline{1, N}$, ρ – безліч функцій, що описують закони розподілу величин бічних піків апері-

одичних і періодичних функцій взаємної кореляції (АФВК та ПФВК, відповідно); D – функції взаємної невизначеності (ФВН); x, y – безліч функцій, що описують різницю значень максимальних піків функції кореляцій щодо числа символів L_i дискретної послідовності; S – безліч функцій, що описують структурну скритність сигналів; I – безліч функцій, що описують імітостійкість системи, N_p і f – функції, що визначають алгоритм побудови ДП; R_a, R_b, R_H – значення бічних піків авто-, взаємної і стикової функції кореляції відповідно.

Рішення задачі синтезу сигналів з максимальним індексом самосинхронізації може бути засноване на використанні ітераційного рішення систем нелінійних параметричних нерівностей.

Введемо поняття абсолютної «розмитості» систем і сигналів $\{k^j\}$ при $j=\overline{1,N}$.

Система сигналів $\{x^j\}$ є абсолютно «розмитою» за автозгорткою, якщо відносні значення функцій кореляцій векторів (сигналів) $R'_{a_1}(k)$, $R'_{a_2}(k)$, $R'_{b_1}(k)$, $R'_{b_2}(k)$ не погіршуються при зміні x в інтервалі

$$L-x_2 \le k \le L+x_1. \tag{2}$$

Розмитість сигналів будемо представляти сукупністю систем нелінійних нерівностей (СНН):

$$\begin{aligned}
&R_{a_1}(k) \le \sum_{i=\delta}^{L-K} W_i^{\vartheta}(W_{i+k}^{\vartheta})^* + \sum_{i=L-k+1}^{L} W_i^{\vartheta}(W_{i-L+K}^{\vartheta})^* + \sum_{i=1}^{L-K} W_i^{\vartheta}(W_{i+K}^{\vartheta}) + \\
&+ \sum_{i=L-K+1}^{L} W_i^{\vartheta}(W_{i-L+K}^{\vartheta})^* + \sum_{i=1}^{x_1-L+\vartheta} W_i^{\vartheta}(W_{i+K}^{\vartheta})^* \le R'_{a_2}(k);\ k=\overline{0,L+x_2}, \qquad \text{а)} \\
&R_{a_1}(k) \le \sum_{i=\delta}^{L-K} W_i^{\vartheta}(W_{i+k}^{\vartheta})^* + \sum_{i=L-k+1}^{L} W_i^{\vartheta}(W_{i-L+K}^{\vartheta})^* + \sum_{i=1}^{L-K} W_i^{\vartheta}(W_{i+K}^{\vartheta}) + \\
&+ \sum_{i=L-K+1}^{L} W_i^{\vartheta}(W_{i-L+K}^{\vartheta})^* \le R'_{a_2}(k);k=\overline{0,L+x_1}, \qquad \text{б)} \\
&R_{a_2}(k) \le \sum_{i=1}^{L-x_1} W_i^{\vartheta}(W_{i-k}^{\vartheta})^* \le R'_{a_2}(k),\ k=\overline{0,L-x_2}, \qquad \text{в)} \\
&R_{a_1}(k) \le \sum_{i=L-\delta}^{L-K} W_i^{\vartheta}(W_{i+k}^{\vartheta})^* + \sum_{i=L-k+1}^{L} W_i^{\vartheta}(W_{i-L+K}^{\vartheta})^* + \\
&+ \sum_{i=1}^{L-x_2-\vartheta} W_i^{\vartheta}(W_{i+K}^{\vartheta})^* \le R'_{a_2}(k), k=\overline{0,L-x_2}, \qquad \text{г)}
\end{aligned} \tag{3}$$

де $R'_{a_1}(k)$ та $R'_{a_2}(k)$ – різні реалізації ПФАК, які задають при синтезі сигналів.

У разі розмитості за ПФВК та стикової функції взаємної кореляції (СФВК) у інтервалі k, який визначається як: $L-x_2 \le k \le L+x_1$, різниця може бути задана як сукупність СНН виду:

$$\begin{aligned}
&R'_{b_1}(k) \le \sum_{i=\delta}^{L-K} W_i^{q}(W_{i+k}^{\vartheta_1})^* + \sum_{i=L-k+1}^{L} W_i^{q}(W_{i-L+K}^{\delta_2})^* + \sum_{L=1}^{L-K} W_i^{p} \times (W_{L+K}^{\vartheta_2})^* + \\
&+ \sum_{i=L-K+1}^{L} W_i^{p}(W_{i-L+K}^{\vartheta_3})^* + \sum_{i=1}^{L-K} W_i^{r} \times (W_{i+K}^{\vartheta_3})^* \le R'_{b_2}(k);k=\overline{0,L+x},
\end{aligned} \qquad \text{а)}$$

$$R'_{b_1}(k) \le \sum_{i=\delta}^{L-K} W_i^q (W_{i+k}^{\vartheta_1})^* + \sum_{i=L-k+1}^{L} W_i^q (W_{i-L+K}^{\delta_2})^* + \sum_{L=1}^{L-K} W_i^p \times (W_{L+K}^{\vartheta_2})^* +$$

$$+ \sum_{i=L-K+1}^{L} W_i^p (W_{i-L+K}^{\vartheta_3})^* \le R'_{b_2}(k); k = \overline{0, L+x}, \quad \text{б)} \qquad (4)$$

$$R'_{b_2}(k) \le \sum_{i=L-\delta}^{L-K} W_i^q * (W_i^{\vartheta_1} + k)^* \le R_{b_2}(k),\ k = \overline{0, L-x_2}, \quad \text{в)}$$

$$R'_{b_1}(k) \le \sum_{i=L-\delta}^{L-K} W_i^q (W_{i+k}^{\vartheta_2})^* + \sum_{i=L-k+1}^{L} W_i^q (W_{i-L+K}^{\delta_2})^* + \sum_{i=1}^{L-x_2-\delta} W_i^p (W_{i+K}^{\vartheta_2})^* \le R'_{b_2}(k), k = \overline{0, L-x_2}, \quad \text{г)}$$

Розглянемо спочатку теоретичні основи синтезу двох самосинхронізуючих сигналів (СС) x^q і x^p без внесення обмежень розмитості виду (3), (4), а потім зробимо ряд узагальнень на випадок синтезу N дискретних сигналів, що володіють, в тому числі, і розмитими властивостями. При цьому будемо вимагати, щоб ССС володіли ідеальними структурними властивостями, тобто такою структурної скритністю, що під час перехоплення і поелементній обробці будь-якого числа l символів сигналів не можна однозначно передбачити $L-1$ символів, що залишилися. Це може бути виконано, якщо символи ССС незалежні і з'являються з однаковою ймовірністю [11].

Запишемо умови, що визначають деякі граничні умови, яким повинні задовольняти авто- і взаємно кореляційні властивості сигналів x^q і x^p:

$$\xi^1_{a_1}(l) \le \sum_{i=1}^{L} x_i^q \times (x_{i+1}^q)^* \le \xi_{a_2}(l), l = \overline{0, L'}, \quad \text{а)}$$

$$\xi^2_{a_1}(l) \le \sum_{i=1}^{L} x_i^p \times (x_{i+1}^p)^* \le \xi_{a_2}(l), l = \overline{0, L'}, \quad \text{б)}$$

$$\xi^1_{a_1}(l) \le \sum_{i=1}^{L-K} x_i^q \times (x_{i+1}^q) + \sum_{i=L-K+1}^{L-1} x_i^q \times (x_{i-L+K}^p)^* \le \xi^1_{b_2}(l), l = \overline{1, L-1}, \quad \text{в)}$$

$$\xi^2_{b_1}(l) \le \sum_{i=1}^{L-1} x_i^q \times (x_{i+l}^q) + \sum_{i=L-K+1}^{L-1} x_i^q \times (x_{i-L+K}^p)^* \le \xi^2_{b_2}(l), l = \overline{1, L-1}, \text{г)} \qquad (5)$$

$$\xi^3_{b_1}(l) \le \sum_{i=1}^{L-1} x_i^q \times (x_{i+l}^p) + \sum_{i=L-K+1}^{L-1} x_i^q \times (x_{i-L+K}^q)^* \le \xi^3_{b_2}(l), l = \overline{1, L-1}, \text{д)}$$

$$\xi^4_{b_1}(l) \le \sum_{i=1}^{L-1} x_i^p \times (x_{i+l}^p) + \sum_{i=L-K+1}^{L-1} x_i^p \times (x_{i-L+K}^q)^* \le \xi^4_{b_2}(l), l = \overline{1, L-1}, \quad \text{е)}$$

$$\xi^5_{b_1}(l) \le \sum_{i=1}^{L-1} x_i^p \times (x_{i+l}^q) + \sum_{i=L-K+1}^{L-1} x_i^p \times (x_{i-L+K}^p)^* \le \xi^5_{b_2}(l), l = \overline{1, L-1}, \quad \text{ж)}$$

Аналіз виразу (5) показує, що число різних білінійних форм визначає вирази:

$$C_r = 6L - 4, \text{ якщо } L \text{ – парне}, \qquad (6)$$

і

$$C_r = 6L - 5, \text{ якщо } L \text{ – непарне}. \qquad (7)$$

Підкреслимо, що вираз (5) визначає мінімальну сукупність систем нелінійних нерівностей, виконання яких дасть достатні умови побудови двох ДС x^q і x^p з заданими реалізаціями за ПФАК, ПФВК, СФВК.

Твердження 1 однозначно встановлює алгебраїчну структуру сукупності систем нелінійних нерівностей для випадку синтезу v сигналів.

Твердження 1. Нехай x^{υ}, $\upsilon=\overline{1,N}$ – є дійсні або комплексні послідовності символів, а $\xi^{j}_{a_1}(l),\xi^{j}_{a_2}(l),\xi^{i}_{b_1}(l),\xi^{i}_{b_2}(l)$, $j=\overline{1,N}, i=\overline{1,b^2_N}$ – реалізації авто- і взаємних згорток, тоді усі білінійні форми, що утворюють сукупність *N* систем нелінійних нерівностей, що визначені системами (5, а) і сукупність C^2_N систем нелінійних нерівностей (5, в) – (5, ж) не збігаються, а число різних білінійних форм визначається виразом:

якщо L –парне, то

$$C_r = N\left(\frac{N(5L-4)-4L+3}{2}\right), \tag{8}$$

якщо L – непарне, то

$$C_r = N\left(\frac{N(5L-4)-4L+4}{2}\right). \tag{9}$$

Сукупність систем (5) може бути представлена з використанням аперіодичних авто- і взаємних згорток $C^{qp}(l)$, якщо аперіодична згортка є

$$C^{qp}(l)=\sum_{j=0}^{L-1+l} x^q_j (x^p_{j+l})^*, \text{ якщо } \ 0\le l\le L-1, \tag{10}$$

$$C^{qp}(l)=\sum_{j=0}^{L-1+l} x^q_{j-e} (x^p_{j+l})^*, \text{ якщо } 1-N\le l\le 0, \text{ та} \tag{11}$$

$$\text{якщо } |l|\ge N.$$

Тоді, застосовуючи (11), система (10) прийме вид:

$$\begin{cases} \xi^1_{a_1}(l)\le c^{q,q}(l)+c^{q,q}(L-l)\le \xi^1_{a_2}(l), l=\overline{1,L}; \\ \xi^2_{a_1}(l)\le c^{p,p}(l)+c^{p,p}(L-l)\le \xi^2_{a_2}(l), l=\overline{1,L}; \\ \xi^1_{b_1}(l)\le c^{q,p}(l)+c^{q,p}(L-l)\le \xi^1_{b_2}(l), l=\overline{0,L-1}; \\ \xi^2_{b_1}(l)\le c^{q,p}(l)+c^{q,p}(L-l)\le \xi^2_{b_2}(l), l=\overline{0,L-1}; \\ \xi^3_{b_1}(l)\le c^{q,p}(l)+c^{q,q}(L-l)\le \xi^3_{b_2}(l), l=\overline{0,L-1}; \\ \xi^4_{b_1}(l)\le c^{p,p}(l)+c^{p,q}(L-l)\le \xi^4_{b_2}(l), l=\overline{0,L-1}; \\ \xi^5_{b_1}(l)\le c^{q,p}(l)+c^{p,p}(L-l)\le \xi^5_{b_2}(l), l=\overline{0,L-1}. \end{cases} \tag{12}$$

У (12) l приймає ті ж значення, що і в системі (11). Система (12) є аналогом систем (10) і, в разі відсутності вимог розмитості векторів x^q і x^p, являє собою сукупність систем нелінійних нерівностей, кожне з яких є сумою аперіодичних згорток або в часовій області, або в області узагальнених теоретичних перетворень. Останнє дозволить підвищити обчислювальну ефективність як у випадку синтезу, так і при розкритті закону формування сукупності використовуваних кодових форм.

Зокрема розглянемо можливості подання систем (5) з використанням аперіодичної згортки. Введемо поняття усіченої аперіодичної згортки, визначивши її як

$$C^{q,p}_{\delta}=\begin{cases} \sum_{j=\delta}^{L-1-l} x^q_j (x^p_j+e)^*, \text{ при } \upsilon<l<L-\delta-1; \\ 0, \text{ при } l\ge L-\delta. \end{cases} \tag{13}$$

Тоді (4) як найбільш загальна сукупність систем, що включає, зокрема і (3), з урахуванням (13), має вид

$$\begin{cases} R_{b_1}(k) \le C_{\delta}^{q,v_1}(l-k-1) + C_{\delta}^{q,v_2}(L-l) + C_{\delta}^{p,v_2}(l) + \\ C_{\delta}^{p,v_3}(L-l) + C_{\delta}^{r,v_3}(L-l) \le R_{b_2}(k), k = \overline{0, L+X_1}; \ \text{а)} \\ R_{b_1}(k) \le C_{\delta}^{q,v_1}(l-k-1) + C_{\delta}^{q,v_2}(L-l) + C_{\delta}^{p,v_2}(l) + \\ C_{\delta}^{p,v_3}(L-l) \le R_{b_2}(k), k = \overline{0, L+X_1}; \ \text{б)} \\ R_{b_1}(k) \le C_{L-\delta}^{q,v_1}(l-\delta-1) \le R_{b_2}(k), k = \overline{0, L-X_2}; \ \text{в)} \\ R_{b_1}(k) \le C_{L-\delta}^{q,v_1}(l-\delta-1) + C_{\delta}^{q,v_2}(L-l) + \\ C_{\delta}^{p,v_2}(l), k = \overline{0, L-X_2}. \ \text{г)} \end{cases} \quad (14)$$

В (14) відсутні обмежень на область уявлення аперіодичних згорток в часовій області або в області узагальнених теоретичних перетворень.

З порівняння сукупності систем (14) випливає, що білінійні форми (14, а) відрізняються від білінійних форм (14, б) складовою $C_{\delta}^{r,v_s}(l)$, а (14, г) від (14, в) складовими $C_{\delta}^{q,v_2}(L-l) + C_{\delta}^{p,v_2}(l)$.

Зазначену властивість може бути використано при оптимізації процедур визначення закону побудови форм застосовуваних сигналів (векторів) ω^{ϑ}.

Висновки

Аналіз показав, що до теперішнього часу не існує математичного апарату рішення систем нелінійних нерівностей (СНН) другого порядку виду (5). Ще більш жорсткі обмеження на можливість вирішення сукупності такого роду систем накладаються функціоналом (1). На наш погляд, з урахуванням відсутності регулярних (однозначних) обмежень, що вводяться для забезпечення відповідних значень скритності S джерела сигналів Q_W і імітостійкості І передачі даних в (1), єдиним математичним апаратом, що застосовується до вирішення даної задачі, є апарат теорії дослідження операцій і, зокрема, методи нелінійного, динамічного і схоластичного цілочисельного програмування. Дійсно, функціонал (1) можна розглядати як цільову функцію, яка залежить від керованих і некерованих функцій, значення (реалізації) яких можуть визначатися фізичною реалізуємістю ССС із заданими властивостями. Аналіз можливих методів рішень задачі синтезу досліджуваних в даній роботі сигналів показує, що вони повинні відноситися до методів типу «укладання ранця», процедура рішень для яких вимагає значних і, за деяких умов, нескінченних ресурсів.

Сформульовано і у загальному виді вирішено задачу синтезу класу сигналів із заданими кореляційними, ансамблевими і структурними властивостями, а також властивостями «розмитості» за кореляційними характеристиками. Зазначена властивість («розмитість») означає, що збільшення або зменшення довжини дискретного сигналу не змінює кореляційні властивості дискретної послідовності, на основі якої синтезовано сигнал. Застосування безлічі зазначених систем сигналів в сучасних інформаційно-комунікаційних системах дозволить поліпшити показники ефективності функціонування таких систем, насамперед, завадозахищеності, скритності функціонування, інформаційної безпеки, завадостійкості прийому сигналів.

Список літератури:

1. Варакин Л. Е. Системы связи с шумоподобными сигналами.1985. 384 с.

2. Sarvate D.V. Crosleration Properties of Pseudorandom and Related Sequences / D.V. Sarvate, M.V. Parsley // IEEE Trans. Commun. 1980. Vol. Com 68. P. 59–90.

3. Горбенко І.Д., Замула О.А. Моделі та методи синтезу криптографічних сигналів та їх оптимізація за критерієм часової складності // Математичне та комп'ютерне моделювання. Сер.: Фізико-математичні науки: зб. Наук. праць / Інститут кібернетики імені В.М. Глушкова Національної академії наук України, 2017. Вип. 15. 272 с.

4. Gorbenko I.D., Zamula A.A. Cryptographic signals: requirements, methods of synthesis, properties, application in telecommunication systems // Telecommunications and Radio Engineering. 2017. Vol. 76. Issue 12, pages 1079-1100. DOI: 10.1615/TelecomRadEng.v76.i12.50.

5. Gorbenko I.D., Zamula A.A. Theoretical bases of synthesis of quasi-orthogonal systems of complex signals // Радіотехніка. 2020. Вип. 200. С. 162 – 175.

6. Gorbenko I., Zamula A., Ho L., Rodionov S. Derived signals systems for information communication systems applications: synthesis, formation, processing and properties // Problems of Info communications Science and Technology (PIC S and T). Proceedings of 2020 International Scientific-Practical Conference, 6–9 Oct. 2020. Kharkiv : KNURE, 2020. P. 13-20.

7. ISCI'2020: Information Security in Critical Infrastructures. Collective monograph / Edited by Ivan D. Gorbenko, Victor A. Krasnobayev and Alexandr A. Kuznetsov. ASC Academic Publishing, USA, 2020, 308 p. – ISBN: 978-1-7362833-0-1 (Hardback). ISBN: 978-1-7362833-1-8 (Ebook).

8. Gorbenko I., Zamula A., Morozov V. Information and communication systems based on signal systems with improved properties building concept // Workshop Proceedings 2019 CEUR, 2353, с. 974-991.

9. Gorbenko I.D., Zamula A.A., Ho Tri Luk. Synthesis of derivatives of complex signals based on nonlinear discrete sequences with improved correlation properties // Радіотехніка. 2019. Вип. 199. С. 110-120.

10.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. 2017. Vol. 76, Issue 19, pages 1705-1717 DOI: 10.1615/TelecomRadEng.v76.i19.30.

11.Горбенко І.Д. Прикладна криптологія : монографія / І.Д. Горбенко, Ю.І. Горбенко. Харків : Форт. 2012. 868 с.

Надійшла до редколегії 03.02.2021

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, АТ «Інститут інформаційних технологій», головний конструктор; Україна; e-mail: GorbenkoI@iit.kharkov.ua; ORCID: https://orcid.org/0000-0003-4616-3449

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

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

УДК 004.056 **DOI:10.30837/rt.2021.1.204.04**

В.И. ЕСИН, д-р техн. наук, С.Г. РАССОМАХИН, д-р техн. наук, В.В. ВИЛИГУРА

АНАЛИЗ ФОРМАЛЬНЫХ МОДЕЛЕЙ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ ДАННЫХ И ИХ ПРИМЕНИМОСТЬ ДЛЯ БАЗ ДАННЫХ

Введение

Концепции и принципы управления безопасностью, определяющие основные параметры, необходимые для безопасной среды, цели и задачи, которых должны достичь как разработчики политик, так и разработчики систем, чтобы создать безопасное решение, являются неотъемлемыми элементами политики безопасности, формальное представление (в виде математических выражений, схем, диаграмм, алгоритмов и т. д.) которой называют моделью безопасности. Модели безопасности играют важную роль в процессах разработки и исследования защищенных компьютерных систем, так как обеспечивают системотехнический подход. Рассмотрение моделей безопасности целесообразно по нескольким причинам. Во-первых, они могут быть непосредственно использованы для анализа безопасности как существующих, так и перспективных информационных систем (ИС) и их основного функционального компонента – базы данных (БД), особенно в случаях, когда требуется получение гарантий защищенности ИС. Классические модели безопасности ИС позволяют формально анализировать свойства различных механизмов защиты ИС. Во-вторых, существующие модели безопасности могут быть использованы в качестве основы для разработки более совершенных моделей, позволяющих более точно описывать и исследовать особенности функционирования механизмов защиты современных ИС. В-третьих, владение знаниями о моделях безопасности ИС предоставляет специалисту в области компьютерной безопасности возможности для строгого научного и теоретически обоснованного изложения результатов прикладных исследований [1].

Среди формальных моделей безопасности в данной работе рассмотрим модели обеспечения целостности данных и особенности их применения для баз данных.

Модели обеспечения целостности данных

Обеспечение информационной безопасности невозможно без рассмотрения концепции защиты надежности/достоверности (англ. reliability) и правильности/корректности (англ. correctness) данных, представляющей суть обеспечения их целостности. Для многих, особенно невоенных организаций, целостность важнее конфиденциальности. Трудно представить систему, для которой были бы не важны свойства целостности. Например, если вы публикуете информацию в Интернете на Web-сервере и вашей целью является сделать ее доступной для самого широкого круга людей, то конфиденциальность в данном случае не требуется. Однако требования целостности остаются актуальными. Многочисленные атаки направлены на нарушение целостности. К ним можно отнести вредоносные модификации, выполняемые вирусами или другими зловредными программами, ошибки в приложениях. При этом нарушения целостности не ограничиваются преднамеренными атаками. Ошибка пользователя, недосмотр или неумелость являются причиной многих случаев несанкционированного изменения информации. События, которые приводят к нарушениям целостности, включают изменение или удаление файлов, данных в БД, ввод неверных данных, изменение конфигурации, ошибки в командах, внедрение вируса и выполнение вредоносного кода. Нарушение целостности может произойти из-за действий любого пользователя, включая администраторов. Они также могут возникать из-за недосмотра в политике безопасности или из-за неправильно настроенного контроля безопасности.

Целостность целесообразно рассматривать с трех сторон [2]:

– предотвращения (препятствия) внесения изменений неавторизованными субъектами;

– предотвращения внесения авторизованными субъектами несанкционированных изменений, например, ошибок;

– поддержания внутренней и внешней согласованности объектов, чтобы их данные были правильным и истинным отражением реального мира, а любые отношения (связи) с любым дочерним, равным или родительским объектом были действительными (англ. valid), согласованными (англ. consistent) и проверяемыми (англ. verifiable).

Правильно реализованная защита целостности предоставляет средства для авторизованных изменений, одновременно защищая от злонамеренных несанкционированных действий (таких как вирусы и вторжения), а также от ошибок, допущенных авторизованными пользователями (таких как ошибки или недосмотры/оплошности). Это гарантирует, что данные остаются *правильными* (отсутствуют логические ошибки в структуре и в значениях данных), *неизменными* (тождественность данных определенному эталону), *неискаженными* (отсутствие подделки данных) и *сохраненными*. Если механизм безопасности обеспечивает целостность, он обеспечивает высокий уровень гарантии того, что данные, объекты и ресурсы не будут изменены по сравнению с их первоначальным защищенным состоянием.

В зависимости от того, насколько тот или иной аспект области использования данных является наиболее важным, выделяют методы и средства, обеспечивающие их целостность, в смысле [3]:

– правильности, неискаженности и неизменности данных, основывающиеся на так называемых моделях целостности данных;

– неискаженности данных при передаче в линиях связи и хранении в информационных системах, основывающиеся на криптографии (например, использовании таких криптографических примитивов как: цифровая подпись, криптографические хеш-функции, коды проверки подлинности);

– параллельного выполнения транзакций в клиент-серверных системах (транзакции играют важную роль в механизме обеспечения целостности базы данных).

Существуют многочисленные контрмеры, которые могут гарантировать целостность данных при различных возможных угрозах [2]. В том числе обеспечить безопасность легче, если есть четкая модель того, что нужно защищать и кому и что разрешено делать [4]. Поэтому неотъемлемой частью любого проекта по созданию или оценке безопасности ИС и баз данных в том числе, как отмечается в [5], является наличие модели безопасности. Ниже, в первую очередь, остановимся на анализе некоторых наиболее известных моделях безопасности, связанных с аспектами, рассматриваемыми в работе, – формальных моделях целостности данных.

Модель Кларка – Вилсона

Исходя из важности обеспечения целостности данных было разработано несколько моделей безопасности, к числу которых можно отнести модели, предложенные Кларком с Вилсоном и Бибом.

Модель Кларка – Вилсона [6] является описательной. В ней не содержится каких бы то ни было строгих математических выражений. Модель Кларка – Вилсона – это основа и руководство для формализации политик безопасности, а не модель конкретной политики безопасности. В ней подчеркивается важность утверждения руководством процессов и политик безопасности, которым должна следовать организация [7]. Ее, скорее всего, целесообразно рассматривать как совокупность практических рекомендаций по построению системы обеспечения целостности в ИС.

Для лучшего понимания данной модели проведем некоторую формализацию, введя определенные обозначения:

– S – множество субъектов;

– D – множество данных в ИС (множество объектов), причем $D = CDI \bigcup UDI$, $CDI \bigcap UDI = \varnothing$ где CDI (*constrained data items* – «*ограниченный элемент данных*») – данные

(любой элемент данных), целостность которых контролируется (защищена моделью безопасности); *UDI* (*unconstrained data items* – «*неограниченный элемент данных*») – данные, целостность которых не контролируется моделью безопасности;

– *IVP* (*integrity verification procedure*) – процедура проверки целостности *CDI* (процедура, которая сканирует элементы данных и подтверждает их целостность, например путем расчета контрольной суммы или используя возможности современной блокчейновой модели, как это показано в работе [8]);

– *TP* (*transformation procedure*) – процедура преобразования – компонент, который может инициировать транзакцию (последовательность операций), переводящую систему из одного состояния в другое. Процедуры преобразования единственные процедуры, которым разрешено изменять *CDI*. Ограниченный доступ к *CDI* через *TP* составляет основу модели целостности Кларка – Вилсона.

Модель Кларка – Вилсона основывается, как и дискреционные модели разграничения доступа, на тройках: «*субъект – операция (транзакция), не нарушающая целостность – объект*». Субъекты не имеют прямого доступа к объектам. Доступ к объектам можно получить только через *TP*.

В модели выделяются два основных механизма, обеспечивающих базовый контроль доступа и целостность. А именно – правильно сформированная транзакция сохраняет целостность данных и предотвращает произвольное манипулирование данными субъектами. Следует заметить, что концепция правильно сформированной транзакции отлично вписывается в стандартную концепцию транзакций в традиционных СУБД [9]. Разделение обязанностей требует, чтобы каждая критическая операция состояла из двух или более частей, каждая из которых должна выполняться другим субъектом или субъектом с другой ролью.

Модель состоит из двух наборов правил: сертификации (С), которая проводится сотрудником по вопросам безопасности (администратором безопасности), владельцем системы, хранителем системы (англ. system custodian), и правил исполнения (Е), которое осуществляется системой. Правила исполнения соответствуют функциям безопасности, независимым от приложений, а правила сертификации позволяют включать в модель определения целостности для конкретных приложений. Желательно минимизировать правила сертификации, поскольку процесс сертификации сложен, подвержен ошибкам и должен повторяться после каждого изменения процедура преобразования (программы).

Несколько перефразированные относительно оригинала правила модели Кларка – Вилсона приведены ниже:

1. Правило С1. В системе должны иметься *IVP*, способные подтвердить целостность любого *CDI* (в оригинальной работе [6] оно формулируется таким образом: «Все *IVP* должны надлежащим образом гарантировать, что все *CDI* находятся в валидном состоянии на момент работы *IVP*»; под понятием «валидное (valid) состояние» авторы понимают такое состояние системы, при котором в любой момент времени *CDI* удовлетворяют требованиям целостности).

2. (С2) Все процедуры преобразования *TP* должны быть реализованы корректно, в том смысле, что не должны нарушать целостности данных (то есть они должны перевести *CDI* в допустимое конечное состояние, учитывая, что он находится в допустимом состоянии с самого начала), и применяться только по отношению к списку элементов *CDI*, устанавливаемых администратором безопасности (отношение $(TP_i,(CDI_a,CDI_b,CDI_c,...))$).

3. (Е1) Система должна контролировать допустимость применения *TP* к элементам *CDI* в соответствии со списками, указанными в правиле С2.

4. (Е2) Система должна поддерживать список разрешенных конкретным пользователям процедур преобразования *TP* с указанием допустимого для каждой $TP_i \in TP$ и данного субъекта ($s_j \in S$) набора обрабатываемых элементов *CDI* (то есть тройки: $(s_j,TP_i,(CDI_a,CDI_b,CDI_c,...))$.

5. (C3) Список, определенный правилом E2, должен отвечать требованию разграничения функциональных обязанностей (в том числе совместного выполнения).

6. (E3) Система должна аутентифицировать всех пользователей (каждый субъект), пытающихся выполнить какую-либо процедуру преобразования TP.

7. (C4) Каждое применение TP должно регистрироваться в специальном элементе CDI – журнале регистрации, содержащем информацию, достаточную для восстановления полной картины каждого применения этой процедуры преобразования, и доступном только для добавления в него информации.

8. (C5) Любая TP, которая принимает UDI в качестве входных данных, может выполнять только допустимые преобразования для любого возможного значения UDI. TP либо принимает (конвертирует в CDI), либо отклоняет UDI. То есть специальные TP могут корректно обрабатывать UDI, превращая их в CDI.

9. (E4) Только специально уполномоченный субъект (пользователь, агент, которому разрешено сертифицировать объекты) может изменять списки, определенные в правилах C3 и E2. Этот субъект не имеет права выполнять какие-либо действия, если он уполномочен изменять регламентирующие эти действия списки.

Роль каждого из девяти правил модели Кларка – Вилсона в обеспечении целостности данных в работе [10] соотносится с так называемыми теоретическими принципами политики контроля целостности:

1) корректность транзакций;
2) аутентификация пользователей;
3) минимизация привилегий;
4) разграничение функциональных обязанностей;
5) аудит произошедших событий;
6) объективный контроль;
7) управление передачей привилегий;
8) обеспечение непрерывной работоспособности;
9) простота использования защитных механизмов.

Соответствие правил модели Кларка-Вилсона первым шести перечисленным выше принципам показано в табл. 1.

Таблица 1

Правило модели Кларка – Вилсона	Принципы политики контроля целостности
C1	1,6
C2	1
C3	4
C4	5
C5	1
E1	3,4
E2	1,2,3,4
E3	2
E4	4

Как видно из табл. 1, принципы политики контроля целостности 1 (корректность транзакций) и 4 (разграничение функциональных обязанностей) реализуются большинством правил модели Кларка – Вилсона, что соответствует ее основной идее.

На рис. 1 представлена схема применения данных правил для управления работой системы и данными. UDI представляют данные, существующие вне защищенной системы. Правила сертификации обеспечивают правильную проверку таких данных при входе в систему. Например, правило C5 требует, чтобы правильно сформированные TP, которые преобразуют UDI в CDI, выполняли только проверенные преобразования. Правила C1 и C2 требуют, чтобы CDI удовлетворяли требованиям целостности в начальном состоянии и после последующих преобразований. Правило C4 требует регистрации всех транзакций, как это обычно это бывает с базами данных. Ведение журнала базы данных в большей мере предназначено

для восстановления данных после сбоя, отказа (для отката – возврата к предыдущему состоянию), а ведение журнала в модели Кларка – Вилсона – для аудита. Хотя в базах данных может вестись и журнал аудита. Правило С3 требует соответствующего разделения обязанностей. Поскольку данные могут быть введены только в соответствии с правилами сертификации, для систем, которые нас интересуют, следует, что все данные в базе данных должны быть *CDI*.

Правила исполнения предотвращают изменение *CDI* способами, противоречащими *IVP*. Правила Е2 – Е4 относятся к авторизации доступа *TP*. В то время как Е1 гарантируют, что только правильно сформированные сертифицированные (проверенные) *TP* могут использоваться для изменения *CDI*.

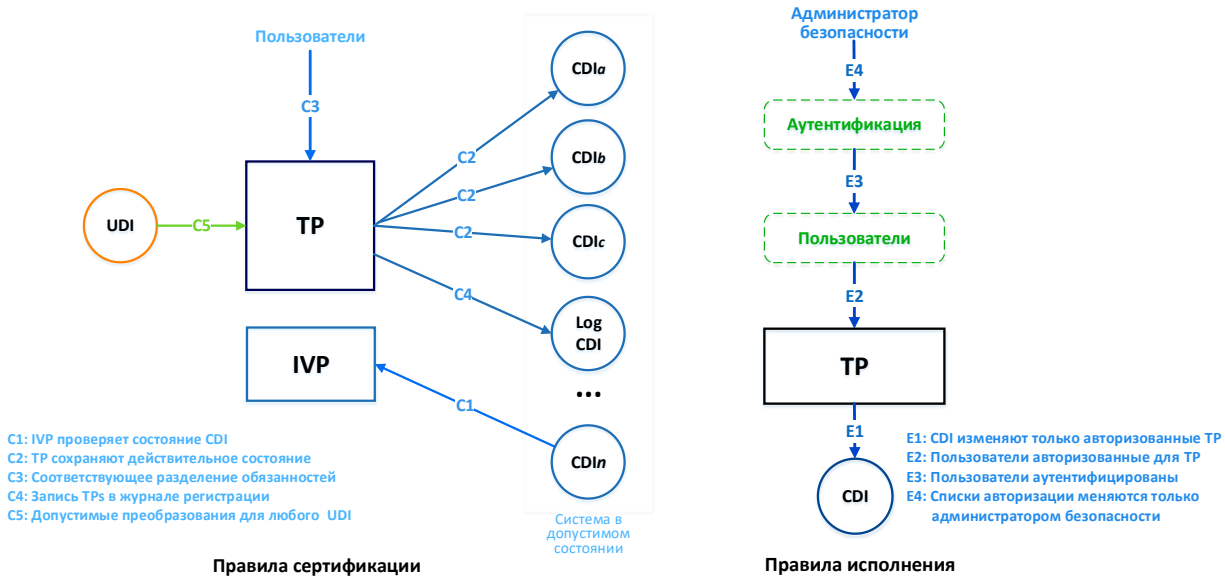


Рис. 1. Схема применения правил модели Кларка – Вилсона

Основной недостаток, обычно упоминаемый для модели Кларка – Вилсона, заключается в том, что *IVP* и связанные с ними методы непросто реализовать в реальных компьютерных системах [11]. Например, основной проблемой реализации механизмов контроля целостности файловых объектов является их достаточно сильное влияние на загрузку вычислительного ресурса системы, что обусловливается следующими причинами [12]: во-первых, может потребоваться контроль больших объемов информации, что связано со значительной продолжительностью выполнения процедуры *IVP*; во-вторых, может потребоваться непрерывное поддержание файлового объекта в эталонном состоянии. В связи с этим возникает вопрос: какой должна быть периодичность запуска процедуры *IVP*? Если выполнять ее часто, то это приведет к существенному снижению производительности системы, если редко, то эффективность такого контроля может оказаться низкой. Поэтому одной из основных задач при реализации механизмов контроля целостности файловых объектов является выбор принципов и механизмов запуска процедуры проверки целостности *CDI*. Другая проблема реализации механизма контроля целостности – это контроль целостности самой контролирующей программы, если контроль целостности реализуется программно. Все это требует определенной дополнительной проработки и принятия соответствующих решений, зависящих, как правило, от особенностей конкретных ИС.

Однако в контексте СУБД отмеченный выше общий недостаток модели Кларка – Вилсона, обусловленный сложностью реализации *IVP* и связанных с ними методов в значительной степени можно преодолеть. Так, например, для реляционных СУБД некоторые ограничения целостности заложены в теории: целостность сущностей, ссылочная целостность. Другие могут быть указаны как статические ограничения с помощью SQL (так называемая декларативная поддержка ограничений целостности). Третьи – как динамические ограничения целостности (так называемая процедурная поддержка ограничений целостности), которые

могут быть реализованы с помощью триггеров и хранимых программ. Все они обеспечивают целостность CDI, к которым осуществляется доступ и их модификация с помощью процедур преобразования TP.

Таким образом, традиционные СУБД поддерживают многие механизмы модели Кларка – Вилсона. Однако реализации, основанные на стандартном SQL, требуют некоторых компромиссов. Например, популярный принцип распространения (предоставления) прав доступа WITH GRANT OPTION (получателю передаваемых привилегий дается привилегия на дальнейшую передачу полученных привилегий, включая привилегию на передачу привилегий) противоречит модели Кларка – Вилсона (правилу E4). Актуальными для СУБД также остаются вопросы, связанные с механизмами контроля целостности хранимых процедур, функций (как файловых объектов). Это обусловливает необходимость дополнительных исследований в соответствующих направлениях.

В целом же, безусловными достоинствами этой модели являются ее относительная простота и легкость совместного использования с другими моделями безопасности.

Модель Биба

Модель Биба [13] была разработана после модели Белла – ЛаПадулы [14]. С точки зрения содержания и формального (математического) представления, эта модель является инверсией мандатной модели Белла – ЛаПадулы, проблема которой заключается в том, что она разработана для сохранения конфиденциальности, не гарантируя при этом целостность данных.

Основные элементы модели Биба:

- S – множество субъектов;
- O – множество объектов, причем $S \bigcap O = \varnothing$;
- $\Lambda_{LI} = (LI, \leq, \square, \otimes)$ – решетка уровней целостности, например: $LI = \{important, very\ important, crucial\}$, где *important*<*very important*<*crucial*;
- $RI = \{modify, invoke, observe, execute\}$ – множество видов доступа, где *modify* – доступ субъекта на модификацию объекта (аналог доступа *write* в модели Белла – ЛаПадулы), *invoke* – доступ на обращение субъекта к субъекту (например, программное средство для доступа к объекту); *observe* – доступ субъекта к объекту на чтение (аналог доступа *read* в модели
Белла – ЛаПадулы), *execute* – доступ на выполнение;
- $B = \{b \subseteq S \times O \times RI\}$ – множество возможных множеств текущих доступов в системе;
- $(i_S, i_O, i_C) \in I = LI^S \times LI^O \times LI^S$ – тройка функций (i_S, i_O, i_C), задающих: $i_S : S \to LI$ – уровень целостности субъектов; $i_O : O \to LI$ – уровень целостности объектов; $i_C : S \to LI$ – текущий уровень целостности субъектов, при этом для каждого $s \in S$ выполняется условие $i_C(s) \leq i_S(s)$;
- $V = B \times I$ – множество состояний системы.

Основные свойства или аксиомы модели Биба (в соответствии с политикой строгой целостности) можно сформулировать следующим образом:

1. *Простое свойство целостности* (*The simple integrity property*). Субъект с уровнем целостности $i_S(s)$ может читать (наблюдать – *observe*) информацию, содержащуюся в объекте с уровнем целостности $i_O(o)$ тогда и только тогда, когда уровень целостности объекта $i_O(o)$ преобладает над уровнем целостности субъекта $i_S(s)$ $(i_S(s) \leq i_O(o))$; другими словами, субъект не может прочитать объект на более низком уровне целостности (так называемое правило *no read-down* (NRD)).

2. *Свойство целостности* * (*The * integrity property*). Субъект с уровнем целостности $i_S(s)$ может изменять (*modify*) информацию, содержащуюся в объекте с уровнем целостности

$i_o(o)$, тогда и только тогда, когда уровень целостности субъекта $i_s(s)$ преобладает над уровнем целостности объекта $i_o(o)$ ($i_o(o) \le i_s(s)$); другими словами, субъект не может изменять объект на более высоком уровне целостности (так называемое правило *no write-up* (NWU)).

3. *Свойство вызова* (*invoke*) указывает на то, что субъектам разрешено вызывать субъекты только равного или более низкого уровня, то есть для $\forall\, s[1], s[2] \in S$, $s[1]$ может вызвать $s[2]$ только тогда, когда $i_s(s[2]) \le i_s(s[1])$.

Два первых свойства этой модели есть инверсия двух соответствующих свойств модели Белла – ЛаПадулы. А именно – правило NRD является полной противоположностью правила NRU модели Белла – ЛаПадулы, за исключением того, что в модели Биба используются уровни целостности, а не уровни безопасности (конфиденциальности), как в модели Белла – ЛаПадулы. Правило NWU мандатной модели целостности Биба является полной противоположностью правилу NWD модели Белла – ЛаПадулы для случая уровней целостности, а не безопасности.

Диаграмму информационных потоков, соответствующую модели Биба в системе с двумя уровнями целостности, можно представить следующим образом (рис. 2).

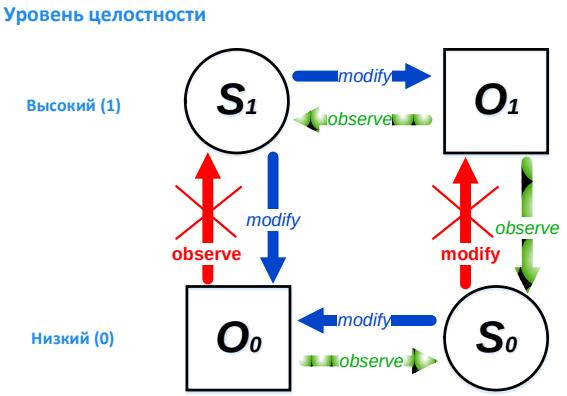


Рис. 2. Диаграмма информационных потоков в системе с двумя уровнями целостности

Многие критикуют модель Биба за то, что она использует целостность как некую меру, ставя под сомнение правомочность отображения свойства данных «целостность» дискретно-упорядоченным множеством. Действительно, в большинстве приложений целостность данных рассматривается как некое свойство (двоичный атрибут), которое либо сохраняется, либо не сохраняется. Тогда введение иерархических уровней целостности может представляться излишним. Однако если уровни целостности в модели Биба рассматривать как уровни достоверности/правильности (различные синтаксические, семантические ошибки могут по-разному влиять на правильность программного кода, вызывая, например, ошибки (errors) или предупреждения (warnings) при трансляции), а соответствующие информационные потоки – как передачу информации из более достоверной совокупности данных в менее достоверную и наоборот, то модель Биба является совершенно адекватной алгебраической структурой.

Поскольку формальное описание модели Биба очень близко с описанием модели Белла – ЛаПадулы, то она, естественно, обладает большинством достоинств и недостатков присущих этой модели.

В реальных ИС редко встречаются системы защиты, ориентированные исключительно на обеспечение конфиденциальности или исключительно на обеспечение целостности информации. Строя защищенные системы, многие хотели бы сочетать оба механизма, используя для этого различные формальные модели безопасности, в том числе такие, как модели Белла – ЛаПадулы и Биба. Это непростая задача. Возможные варианты совместного использования моделей Белла – ЛаПадулы и Биба и возникающие при этом осложнения приведены ниже [3, 15, 16]:

1. Две модели могут быть реализованы в системе независимо друг от друга. В этом случае субъектам S и объектам O независимо присваиваются уровни конфиденциальности и

уровни целостности на основе двух различных решеток. Решение о безопасности доступа принимается одновременно по правилам обеих моделей.

Нетрудно видеть, что при таком подходе к организации доступа возможны неразрешимые ситуации, например, когда по правилам модели Белла – ЛаПадулы доступ может быть разрешен, а по правилам модели Биба – нет, или наоборот.

2. Логическое объединение моделей на основе одной общей решетки уровней безопасности (конфиденциальности/целостности).

В таких системах разрешенными являются только доступы субъектов к объектам в пределах одного уровня безопасности (рис. 3).

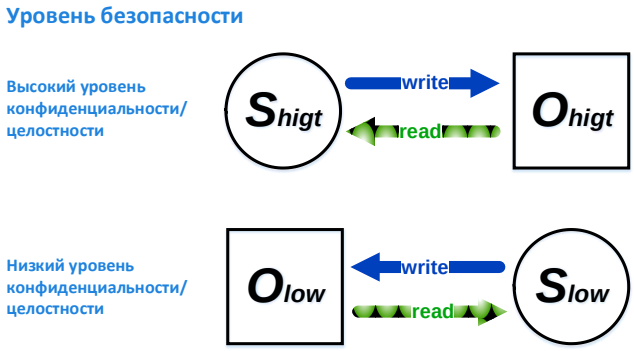


Рис. 3. Совместное использование моделей Белла – ЛаПадулы и Биба
(доступ в пределах одного уровня безопасности)

3. Логическое объединение моделей на основе одной общей решетки, но с двумя метками безопасности: по конфиденциальности и по целостности с противоположным характером их определения. Субъекты и объекты с высокими требованиями конфиденциальности (например, секретные данные и доверенные по секретам пользователи) располагаются на высоких уровнях иерархии решетки. Субъекты и объекты с высокими требованиями целостности (например, системное программное обеспечение и программисты) располагаются на нижних уровнях иерархии решетки (рис. 4).

Рис. 4. Совместное использование моделей Белла – ЛаПадулы и Биба
(на основе единой решетки с двумя метками безопасности)

Несмотря на сложность классификации субъектов и объектов доступа, именно третий вариант находит применение в современных ИС, в частности в СУБД, где реализуется мандатная политика безопасности [3].

Поскольку субъекты и объекты с высокой целостностью находятся внизу иерархии, а компоненты с низкой целостностью – наверху иерархии, то правила *no read up* и *no write down* имитируют мандатную модель целостности Биба в структуре модели Белла – ЛаПадулы. То есть чтение сверху в иерархии модели Белла – ЛаПадулы является чтением снизу в иерархии модели Биба. Аналогично, запись наверх в модели Белла – ЛаПадулы является

записью вниз в модели Биба. На практике это позволяет за счет размещения системных файлов (объектов O), в том числе относящихся к СУБД, и субъектов-администраторов (их процессов) в нижней части иерархии модели Белла – ЛаПадулы, обеспечить защиту целостности таких объектов от обычных субъектов-пользователей (и их процессов), поскольку правило *no write down* не позволяет им осуществлять запись в системные файлы. Кроме этого, если рассматривать исполнение как чтение, то субъекты-администраторы (и их процессы) не смогут исполнять программы вне высшего уровня целостности (или нижнего уровня иерархии модели Белла – ЛаПадулы).

Данная схема обеспечивает защиту системных файлов от вредоносных программ типа «троянский конь» ввиду того, что, если подобная зловредная программа находится на одном из верхних уровней, она никогда не сможет исказить системные файлы из-за необходимости выполнения правила *no write down*. Таким образом, такое объединение моделей осуществляет защиту секретности для верхних уровней определенной иерархии и защиту целостности для нижних уровней [16].

В заключение целесообразно отметить, что существующие теоретические разработки и практические реализации обеспечения безопасности ИС основываются не только на парадигме формального моделирования политики безопасности, но и на другой не менее важной парадигме – криптографии, нацеленной на решение определенных задач. Причем эти различные по происхождению и решаемым задачам подходы дополняют друг друга: криптография предлагает актуальные методы и примитивы для защиты информации, обеспечивая идентификацию, аутентификацию, шифрование, контроль целостности данных, а формальные модели безопасности предоставляют разработчикам защищенных ИС основополагающие принципы, которые лежат в основе архитектуры защищенной системы и определяют концепцию ее построения [17].

Целесообразным представляется проведение дальнейших исследований, результатом которых являлась бы некоторая методология комплексного использования различных моделей безопасности при проектировании и эксплуатации соответствующих ИС и их основного функционального компонента – БД, ведущая к повышению эффективности их защиты.

Выводы

1. Анализ формальных моделей обеспечения целостности данных выявил, что каждая из них, имея определенные преимущества и недостатки, имеет право на использование. Главным решающим фактором является оценка конкретной ситуации, которая позволит сделать правильный выбор, в том числе и комплексного их применения.

2. Модель Кларка – Вилсона является описательной, не содержащей строгих математических выражений. Данная модель – это основа и руководство для формализации политик безопасности, а не модель конкретной политики безопасности. Ее целесообразно рассматривать как совокупность практических рекомендаций по построению системы обеспечения целостности в ИС.

Безусловными достоинствами этой модели являются ее относительная простота и легкость совместного использования с другими моделями безопасности. Основным недостатком модели Кларка – Вилсона считается сложность реализации в реальных ИС методов и процедур проверки целостности данных. При этом в контексте традиционных баз данных от этого недостатка можно в значительной степени избавиться благодаря тому, что в реляционных БД некоторые ограничения целостности заложены в теории (целостность сущностей, ссылочная целостность), другие могут быть указаны как статические ограничения с помощью SQL (декларативная поддержка ограничений целостности), третьи – как динамические ограничения целостности (процедурная поддержка ограничений целостности). Однако для БД актуальными остаются вопросы, связанные с механизмами контроля целостности хранимых процедур, функций (как файловых объектов). Это обусловливает необходимость проведения дополнительных исследований в соответствующих направлениях.

3. Модель Биба, с точки зрения содержания и формального представления, является инверсией мандатной модели Белла – ЛаПадулы, проблема которой заключается в том, что она разработана для хранения секретов, не гарантируя при этом целостность данных. Поскольку формальное описание модели Биба очень близко с описанием модели Белла – ЛаПадулы, то она, естественно, обладает большинством достоинств и недостатков присущих модели безопасности на основе мандатной политики доступа.

На практике для создания защищенных ИС как систем, обеспечивающих конфиденциальность и целостность данных, важным является объединение моделей Белла – ЛаПадулы и Биба, причем объединение на основе одной общей решетки, но с двумя метками безопасности: по конфиденциальности и по целостности, с противоположным характером их определения.

Список литературы:

1. Девянин П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. 2-е изд. Москва : Горячая линия–Телеком, 2013. 338 с.
2. Chapple M., Stewart J. M., Gibson D. CISSP Certified Information Systems Security Professional Official Study Guide, 8th ed. Sybex, John Wiley & Sons, Inc.: Indianapolis, Indiana, 2018. 1050 p.
3. Гайдамакин Н. А. Теоретические основы компьютерной безопасности. Екатеринбург : Изд-во Уральского ун-та, 2008. 212 с.
4. Tanenbaum A. S., Herbert Bos H. Modern Operating Systems. Fourth edition. Pearson, 2015. 1136 p.
5. Смирнов С. Н. Безопасность систем баз данных. Москва : Гелиос АРВ, 2007. 352 с.
6. Clark D. D., Wilson D. R. A Comparison of Commercial and Military Computer Security Policies // Proceedings of the 1987 IEEE Symposium on Research in Security and Privacy (SP'87), May 1987, Oakland, CA : IEEE Press, 1987. P. 184–193.
7. Gollmann D. Computer Security. 3rd ed. Wiley, 2011. 436 p.
8. Yesin V.I., Yesina M.V., Vilihura V.V. Monitoring the integrity and authenticity of stored database objects // Telecommunications and Radio Engineering. 2020. Vol. 79, Issue 12. P. 1029-1054.
9. Sandhu R. S., Jajodia S. Data and database security and controls // Handbook of information security management, Auerbach Publishers. 1993. P. 481-499.
10. Девянин П. Н., Михальский О. О., Правиков Д. И. и др. Теоретические основы компьютерной безопасности. Москва : Радио и связь, 2000. 192 с.
11. Ge X., Polack F., Laleau R. Secure databases: an analysis of Clark-Wilson model in a database environment // International Conference on Advanced Information Systems Engineering. Springer, Berlin, Heidelberg, 2004. P. 234-247.
12. Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа. СПб. : Наука и Техника, 2004. 384 с.
13. Biba K. J. Integrity considerations for secure computer systems. MTR-3153-REV-1. Mitre Corp Bedford MA, 1977. 64 p.
14. Bell D. E., LaPadula L. J. Secure Computer Systems: Unified Exposition and Multics Interpretation (MTR-2997 Rev. 1). Bedford, Mass.: MITRE Corp., 1976. 129 p.
15. Цирлов В. Л. Основы информационной безопасности автоматизированных систем. Ростов-на-Дону : Феникс, 2008. 173 с.
16. Зегжда Д. П. Информационная безопасность. Москва : МГТУ им. Н.Э. Баумана, 2010. 236 с.
17. Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем. Москва : Горячая линия–Телеком, 2000. 452с.

Поступила в редколлегию 08.01.2021

Сведения об авторах:

Есин Виталий Иванович – д-р техн. наук, профессор, Харьковский национальный университет имени В.Н. Каразина, профессор кафедры безопасности информационных систем и технологий, факультета компьютерных наук; Украина; e-mail: v.i.yesin@karazin.ua; ORCID: https://orcid.org/0000-0003-1977-7269

Рассомахин Сергей Геннадьевич – д-р техн. наук, профессор, Харьковский национальный университет имени В.Н. Каразина, заведующий кафедрой безопасности информационных систем и технологий, факультета компьютерных наук; Украина; e-mail: rassomakhin@karazin.ua; ORCID: https://orcid.org/0000-0003-1394-3588

Вилигура Владислав Викторович – Харьковский национальный университет имени В.Н. Каразина, аспирант кафедры безопасности информационных систем и технологий, факультета компьютерных наук; Украина; e-mail: viligura93@gmail.com; ORCID: https://orcid.org/0000-0002-1137-2382

УДК 004.056.55 **DOI:10.30837/rt.2021.1.204.05**

М.В. ЄСІНА, канд. техн. наук, Б.С. ШАХОВ

ДОСЛІДЖЕННЯ ТА АНАЛІЗ РЕАЛІЗАЦІЙ КАНДИДАТІВ ДРУГОГО РАУНДУ КОНКУРСУ NIST PQC, ЩО ОРІЄНТОВАНІ НА СІМЕЙСТВА FPGA XILINX

Вступ

На сьогодні достатньо гостро постає проблема стійкості існуючих криптографічних механізмів захисту до квантових алгоритмів криптоаналізу та квантових комп'ютерів взагалі. Ця проблема є обговорюваною на міжнародному рівні. І задля її вирішення NIST США вирішив організувати та провести конкурс на постквантові криптографічні алгоритми NIST PQC. Результатом конкурсу повинне стати прийняття до стандартизації алгоритмів типу асиметричне шифрування, інкапсуляція ключів та електронний підпис (як мінімум, по одному алгоритму з кожного типу).

На момент початку конкурсу на процес стандартизації було представлено 82 алгоритми. На основі критеріїв мінімальної прийнятності, визначених NIST, для першого раунду було розглянуто 69 алгоритмів. Враховуючи декілька параметрів – безпеку, вартість, продуктивність, характеристики реалізації тощо, 43 і 11 алгоритмів були виключені при завершенні першого і другого раундів відповідно, а інші 15 алгоритмів були збережені для третього раунду [4].

Алгоритми, які залишилися у другому раунді, можна розділити на 5 різних категорій залежно від математичного базису, на якому вони засновуються: на основі ізогеній еліптичних кривих (1 алгоритм), на основі алгебраїчних решіток (12 алгоритмів), на основі математичного коду (7 алгоритмів), на основі багатовимірних перетворень (4 алгоритми) і на основі геш-функцій (2 алгоритми) [4, 5].

Безпека є основним критерієм оцінки, що визначає конкуренцію в конкурсі NIST, і, зрозуміло, що реалізації програмного забезпечення кандидатів в основному зосереджені на ній. Однак, вкрай важливо аби алгоритм мав й ефективну апаратну реалізацію. А своєчасне виявлення апаратної неефективності допоможе сконцентрувати зусилля криптографічної спільноти на більш перспективних кандидатах, потенційно заощадивши велику кількість часу, що може бути витрачена на криптоаналіз [3].

Апаратне і програмне забезпечення

Криптографічні алгоритми зазвичай реалізуються з використанням як програмного, так і апаратного забезпечення. Під програмним розуміються реалізації, які можуть бути виконані з використанням апаратних процесорів. Ці процесори можуть варіюватися від недорогих малопотужних вбудованих процесорів, таких як ARM Cortex-M4, до високопродуктивних мікропроцесорів загального призначення, таких як Intel Core i7, з мікроархітектурою Haswell, що підтримують Advanced Vector Extensions 2 (AVX2) і AES New Instructions (AES-NI). Загальною характеристикою є те, що всі ці процесори зазвичай програмуються з використанням мов програмування високого рівня, таких як C. Код, написаний цими мовами, легко переноситься між різними типами процесорів. Програмне забезпечення може бути додатково оптимізовано за допомогою програмування мовою асемблера, що включає інструкції, специфічні для даного процесора (або, точніше, для його архітектури набору інструкцій (ISA)). Програми мовою асемблера не так легко переносяться між процесорами, що працюють на базі різних ISA [1].

Під апаратним забезпеченням розуміються реалізації, які можуть бути виконані з використанням програмованої користувачем вентильної матриці (FPGA), інтегральних схем спеціального призначення (ASIC), програмованої логіки (PL) системи на чіпі FPGA (SoC FPGA), спеціалізованих стандартних продуктів (ASSP) тощо. Основною особливістю є те, що більшість цих реалізацій розробляється з використанням мов опису апаратури (HDL), таких як

VHDL і Verilog. Ці мови суттєво відрізняються від мов програмування високого рівня тим, що в них вводяться поняття сутності, зв'язку, збігу і синхронізації. Вихідний код HDL перетворюється інструментом синтезу в мережевий список, що складається з основних логічних компонентів і з'єднань між цими компонентами. В силу своєї універсальної природи, HDL код може бути легко перенесений між різними технологіями, такими як FPGA і ASIC. Реалізації ASIC швидше, використовують менше енергії і вимагають менше місця на робочому просторі. Реалізації FPGA мають ряд переваг: менш дорогі засоби розробки, набагато менший цикл проектування, а також реконфігурованість, що розуміється як здатність змінювати функції усіх внутрішніх структурних елементів і з'єднань між ними, навіть після того, як задана інтегральна схема була встановлена у реальних пристроях [1].

Сімейство FPGA

Хоча програмні реалізації, швидше за все, будуть домінувати на першому етапі впровадження стандартів PQC в реальних додатках, апаратні реалізації неминуче будуть наступними. Вони, швидше за все, почнуться з апаратних прискорювачів для обмежених середовищ, таких як смарт-картки та пристрої Інтернету речей. Низьковитратні малопотужні процесори, використовувані в таких додатках, можуть не встигати за підвищеними вимогами до обчислювальної потужності і енергоспоживання. Таким чином, ці процесори, можливо, доведеться розширити за рахунок апаратних прискорювачів. У найближчій перспективі з'являться високопродуктивні процесори безпеки, вдосконалені новими стандартами PQC. Ці процесори будуть оптимізовані для обробки на апаратному рівні всіх алгоритмів, пов'язаних з безпечною комунікацією (наприклад, що використовуються в постквантових версіях протоколів TLS, IPSec, IKE і WTLS/WAP) і безпечним зберіганням. Нарешті, в більш довгостроковій перспективі підтримка нових інструкцій, що забезпечують ефективну і стійку до збоїв реалізацію стандартів PQC, швидше за все, буде додана в найбільш популярні процесорні ISA. Співпроцесори для таких інструкцій є, по суті, апаратною реалізацією PQC. Враховуючи, що нові PQC-стандарти, швидше за все, будуть використовуватися протягом довгого часу, всім вказаним випадкам застосування слід приділити особливу увагу. Зокрема, продуктивність алгоритму на апаратному рівні може вплинути на його довгострокову продуктивність в програмному забезпеченні, на процесорах, обладнаних новими спеціалізованими інструкціями. Навіть, якщо апаратні реалізації 2-го раунду не є остаточними з точки зору продуктивності алгоритму, вони дають перше уявлення про придатність кожного кандидата для апаратного прискорення. Вони також створюють відкриту базу вихідних кодів, на якій в 3-му раунді і далі можуть бути вбудовані більш оптимізовані реалізації і реалізації, захищені від атак бічними каналами і збоїв [1].

При використанні однієї і тієї ж технології апаратні реалізації перевершують програмні, використовуючи як мінімум один і, як правило, декілька показників, таких як швидкість, споживана потужність, енергоспоживання і захист від фізичних атак. Вони також дозволяють значно підвищити гнучкість при використанні одного набору цих показників по відношенню до іншого. З точки зору еталонного тестування і ранжування кандидатів, така гнучкість може стати великою проблемою, особливо з урахуванням того, що жодні два показники, швидше за все, не матимуть простої лінійної залежності один від одного. Практичне розв'язання цієї проблеми полягає в тому, щоб в процесі оцінки зосередитися на двох основних типах реалізації: високій швидкості і малоресурсності [1].

У високошвидкісних реалізаціях основною метою є швидкість. Для схем PQC ця мета зводиться до мінімізації часу виконання основних операцій з використанням відкритого та особистого ключа відповідно. Для механізмів інкапсуляції ключів (KEM) ці операції являють собою інкапсуляцію і декапсуляцію; для схем електронного підпису – перевірку і генерацію підписів; для шифрування з відкритим ключем (PKE) – шифрування і розшифрування. Час генерації ключів може також відігравати значну роль у тому випадку, коли з міркувань безпеки пара відкритий/особистий ключ не може бути повторно використана. Використання

ресурсів є другорядним. Проте, розробники апаратного забезпечення, як правило, прагнуть досягнення оптимальності закону Парето, в якому будь-яке подальше покращення швидкості досягається за рахунок непропорційно великих витрат з точки зору використання ресурсів. Головною перевагою високошвидкісних реалізацій є те, що вони розкривають закладений в них потенціал даного алгоритму розпаралелювання. Поки межа використання ресурсів досить висока, вона не впливає на ранжування алгоритмів. У результаті, ранжування сильно співвідноситься з особливостями самих алгоритмів і не схильне до істотного впливу будь-яких додаткових припущень і вибору технології. Крім того, тільки високошвидкісні апаратні реалізації можуть ефективно конкурувати з оптимізованими програмними реалізаціями, націленими на високопродуктивні процесори з векторними інструкціями (наприклад, AVX2) [1].

У малоресурсних реалізаціях основними цілями, як правило, є мінімальне використання ресурсів і мінімальне енергоспоживання, за умови, що час виконання не перевищує визначеного максимуму. Інший метод формулювання мети – досягнення мінімального часу виконання, припускаючи заданий максимальний бюджет з точки зору використання ресурсів, енергоспоживання або енерговитрат. Максимальний бюджет з використання ресурсів пов'язаний з вартістю реалізації; при цьому бюджет з потужності забезпечує правильну роботу без перегріву або виділення додаткових ресурсів на охолодження. Максимальне використання енергії впливає на те, як довго пристрій, що працює від акумулятора, може функціонувати до наступної зарядки акумулятора. У контексті процесу стандартизації криптографічних алгоритмів вказані максимальні бюджети вибрати дуже складно. Будь-яка зміна цих порогових значень може сприятливо позначитися на іншому наборі кандидатів. У зв'язку з тим, що нові стандарти залишаються в експлуатації протягом десятиліть, вимоги до термінів, вартості та потужності нових, і додатків, які ще з’являться, дуже важко передбачити [1].

Крім того, зміни в технології істотно впливають на те, які апаратні архітектури задовольняють конкретним вимогам. Наприклад, архітектура, здатна досягти часу виконання 0.1 секунди (або нижче) при певному бюджеті на електроенергію або енергоспоживання, може істотно змінитися з покращенням технології. В результаті, більшість поточних лімітів обираються різними розробниками довільно або залишаються невизначеними в своїх звітах. Отже, ранжування кандидатів PQC на основі їх полегшених впроваджень, особливо розроблених різними групами, є надзвичайно складним і залежним від припущень. Таке ранжирування має мало спільного з розпаралелюванням, допустимим кожним алгоритмом, так як більшість операцій повинно виконуватися послідовно через малий об'єм ресурсів. Основною особливістю алгоритмів, які виявляються в цих реалізаціях, є кількість і складність окремих елементарних операцій. Кожна головна операція містить в собі додатковий функціональний модуль, збільшуючи використання ресурсів і енергоспоживання. Крім того, малоресурсні апаратні реалізації можуть перевершити тільки програмні реалізації, націлені на конкретні недорогі вбудовані процесори з низьким енергоспоживанням, такі як Cortex-M4 [1].

У разі реалізації FPGA використання ресурсів є вектором, таким як (#LUT, #flip-flops, #DSP модулів, #BRAM). Жоден елемент цього вектора не може бути виражений в термінах інших елементів. У результаті, введення ліміту ресурсів передбачає вказівку значень всіх компонентів цього вектора ресурсів. Одним з можливих підходів може бути вибір ресурсів найменшої FPGA із заданого недорогого сімейства FPGA. Однак сімейства FPGA і їх ресурси з часом змінюються, тому цей обмежувач має тільки фізичне значення протягом обмеженого періоду часу, що охоплює період оцінки, і може втратити свою значимість лише через кілька років після публікації і застосування стандарту. Нарешті, один і той же пристрій FPGA може також знадобитися для розміщення будь-яких накладних витрат, пов'язаних з протидією атакам побічними каналами. У той же час ці надлишкові або навіть ефективні заходи протидії, можуть залишитися невідомими під час оцінки кандидатів [1].

Сімейство FPGA Xilinx

Однією з основних проблем є рекомендація NIST сфокусуватися на порівняльному аналізі апаратного забезпечення з використанням сімейства FPGA Xilinx Artix-7. Ця рекомендація була представлена у декількох презентаціях NIST, пов'язаних з 2-м раундом процесу стандартизації NIST, наприклад, під час PQCrypto 2019 у травні 2019 р. і другій конференції з стандартизації PQC в серпні 2019 р. У своїй нинішній формі ця рекомендація недоцільна і швидше перешкоджає, ніж підтримує справедливе і всеосяжне апаратне і програмно-апаратне еталонне тестування [1].

Сімейство FPGA представляє собою набір пристроїв FPGA, що мають однакову внутрішню структуру і одну й ту ж технологію (також відому як технічний вузол або вузол процесу), що описується числом, пов'язаним з розмірами і щільністю транзисторів, які можуть бути виготовлені з використанням певного промислового процесу. Завдяки неухильному вдосконаленню технології виробництва, описаного в законі Мура, максимальна ємність і швидкість роботи FPGA-пристроїв неухильно ростуть, в той час як їх ціни залишаються приблизно на тому ж рівні. Кожне нове покоління FPGA-пристроїв певного виробника отримує унікальне ім'я, так зване сімейство. Кожне сімейство складається з декількох пристроїв різного розміру для задоволення потреб різних додатків. Всі пристрої певного сімейства мають однакову внутрішню архітектуру і технологію обробки, але відрізняються кількістю ресурсів певного типу, таких як таблиця пошуку (LUT), flip-flops (FF), блок пам'яті та цифрові блоки обробки сигналів (DSP) або мультиплікатори. Більшість виробників випускають як недорогі сімейства (наприклад, Xilinx Artix-7), так і високопродуктивні (наприклад, Xilinx Virtex-7). Більшість з них також випускають сімейства середнього класу, такі як Xilinx Kintex-7. Максимальна кількість ресурсів, доступних в найбільшому пристрої дешевого сімейства, звичайно, значно менша, ніж аналогічна кількість в найбільшому пристрої сімейства високопродуктивних пристроїв (наприклад, більш ніж в п’ять разів менше для Artix-7 у порівнянні з Virtex-7) [1].

Крім того, останнім часом виробники FPGA почали випускати нові типи програмованих пристроїв, які покращують програмувальну логіку традиційних FPGA за допомогою системи обробки, заснованої на вбудованому процесорі з жорсткою проводкою, наприклад ARM. Так як цей процесор спроектований на замовлення, він повною мірою використовує переваги даного технологічного процесу і працює на тактовій частоті значно вище, ніж програмувальна логіка. Завдяки швидкому процесору і ефективному інтерфейсу між цим процесором і програмувальною логікою ці пристрої ідеально підходять для спільного проектування програмних/апаратних засобів, націлених на високу швидкість. Хоча ці типи пристроїв з'являються під декількома комерційними назвами, їх часто колективно називають SoC FPGA. Першим сімейством такого типу був Xilinx Zynq-7000, випущений в 2011 р., заснований на вбудованих процесорах ARM Cortex-A9 [1].

Конструкція обладнання описується мовами апаратного опису. Код HDL, як правило, ідентичний для всіх родин FPGA. На відміну від програмного забезпечення, де для кожного процесора може знадобитися свій оптимізований код на асемблері, для апаратного забезпечення таких концепцій не існує. У результаті, легко синтезувати один і той же код HDL, призначений для різних сімейств FPGA від різних виробників, за умови, що максимальна ємність найбільшого пристрою даного сімейства не буде перевищена.

Загальні характеристики сімейства FPGA Xilinx

Сьогодні найсучаснішою є серія 7 FPGA Xilinx – Artix-7, Kintex-7, Virtex-7. У цій серії анонсовано сімейство FPGA з процесорним ядром ARM Cortex-A9 – Zynq-7000. У новій серії тільки Virtex-7 продовжує існуючу лінійку високопродуктивних FPGA, а два інших сімейства – Artix і Kintex – замінили лінійку Spartan. FPGA Artix призначені для масової продукції, і відрізняються малим енергоспоживанням і невисокою вартістю, а Kintex являє собою, деякою мірою, Spartan, спеціалізований для цифрової обробки сигналів. Досі серія Virtex

традиційно використовувалася і в додатках, побудованих навколо високошвидкісних послідовних приймачів, і в проектах, заснованих на цифровій обробці сигналів. Сімейство Kintex-7 вдало вписується в нішу, де потрібна велика кількість паралельно працюючих блоків ЦОС за помірною ціною, а для систем з великою кількістю апаратних приймачів призначені більш дорогі Virtex-7 (табл. 1) [6].

Таблиця 1

Зведені характеристики сімейств FPGA Xilinx серії 7

Максимальні параметри	Artix-7	Kintex-7	Virtex-7
Логічні комірки, тис.	352	407	1955
Блочна пам'ять	12	29	65
Секції DSP	700	1540	3960
Пікова продуктивність цифрової обробки сигналів для фільтрів з симетричними коефіцієнтами, GMAC/с	504	1965	5053
Приймачі	4	16	88
Максимальна швидкість передачі, Гб/с	3,75	10.325	28,05
Пікова пропускна здатність приймачів, Гб/с	30	330	2784
Інтерфейси PCI Express	Gen1x4	Gen2x8	Gen3x8
Швидкість обміну інтерфейсами пам'яті, МБ/с	800	2133	2133
Зовнішні виводи	450	500	1200

Мікросхеми Zynq-7010 і Zynq-7020 виконані на базі програмованих ресурсів сімейства Artix, а Zynq-7030 і Zynq-7040 – на базі Kintex. Це відображається на піковій продуктивності підсистеми цифрової обробки сигналів – тактова частота молодших FPGA Zynq нижче, в них немає блоків PCI Express і високошвидкісних приймачів (табл. 2) [6].

Таблиця 2

Характеристики FPGA сімейства Zynq-7000

Параметри	Z-7010	Z-7020	Z-7030	Z-7040
Програмовані логічні комірки (вентилі ASIC)	28 K (430 K)	85 K (1,3 M)	125 K (1,9 M)	235 K (3,5 M)
Блоки пам'яті (36 кб)	60	140	265	760
Секції DSP (18x25 MACC)	80	220	400	760
Пікова продуктивність DSP для KIX з симетричними коефіцієнтами, GMAC/с	58	158	480	912
Блоки PCI Express	-	-	Gen2 x4	Gen2 x8
АЦП	2x12 біт, 1 M вибірок/с, 17 диф. каналів			
Шифрування	AES і SHA 256-біт			
Блоки вводу-виводу, 3.3 В	100	195	100	200
Блоки вводу-виводу, 1.8 В	-	-	150	150
Високошвидкісні приймальники	-	-	4	12

Ключова властивість нового покоління FPGA – уніфікація програмованих ресурсів. Передбачається, що для нового покоління FPGA стане можливою швидка міграція між сімействами Virtex/Kintex/Artix без коригування проекту.

Детальні характеристики сімейства FPGA Xilinx

Далі наведені характеристики FPGA сімейства Xilinx, а саме: Spartan-7, Artix-7, Virtex-7, Kintex-7 [2].

Таблиця 3

Характеристика FPGA Spartan-7

				Оптимізація вводу-виводу при найменших витратах і максимальній продуктивності на ват (1.0V, 0.95V)					
Номер деталі				XC7S6	XC7S15	XC7S25	XC7S50	XC7S75	XC7S100
Логічні ресурси	Логічні комірки			6,000	12,800	23,360	52,160	76,800	102,400
	Частини			938	2,000	3,650	8,150	12,000	16,000
	Тригери CLB			7,500	16,000	29,200	65,200	96,000	128,000
Ресурси пам'яті	Максимум розподіленої оперативної пам'яті (Кб)			70	150	313	600	832	1,100
	Блок RAM/FIFO з ECC (по 36 Кб)			5	10	45	75	90	120
	Всього блоків ОЗП (Кб)			180	360	1,620	2,700	3,240	4,320
Часові ресурси	Елементи керування часом (1 MMCM + 1 PLL)			2	2	3	5	8	8
Ресурси вводу-виводу	Максимум контактів вводу/виводу з одним кінцем			100	100	150	250	400	400
	Максимум диференційних пар вводу/виводу			48	48	72	120	192	192
Вбудовані ресурси жорсткої IP-адреси	Фрагменти DSP			10	20	80	120	140	160
	Аналоговий змішаний сигнал (AMS)/XADC			0	0	1	1	1	1
	Налаштування блоків AES/HMAC			0	0	1	1	1	1
Марки швидкості	Комерційна температура (C)			-1 -2	-1 -2	-1 -2	-1 -2	-1 -2	-1 -2
	Промислова температура (I)			-1 -2 -1L	-1 -2 -1L	-1 -2 -1L	-1 -2 -1L	-1 -2 -1L	-1 -2 -1L
	Розширена температура (Q)			-1	-1	-1	-1	-1	-1
	Упаковка	Площа (мм)	Крок (мм)	Доступний ввід-вивід користувача: 3.3V SelectIO™ Ввід-вивід HR					
	CPGA196	8x8	0.5	100	100				
	CSGA225	13x13	0.8	100	100	150			
	CSGA324	15x15	0.8			150	210		
	FTGB196	15x15	1.0	100	100	100	100		
	FGGA484	23x23	1.0				250	338	338
	FGGA676	27x27	1.0					400	400

Таблиця 4

Характеристика FPGA Artix-7

		Оптимізація приймача при найменших витратах і максимальній пропускній здатності DSP (1.0V, 0.95V, 0.9V)							
Номер деталі		XC7A12T	XC7A15T	XC7A25T	XC7A35T	XC7A50T	XC7A75T	XC7A100T	XC7A200T
Логічні ресурси	Логічні комірки	12800	16,640	23,360	33,280	52,160	75,520	101,440	215,360
	Частини	2,000	2,600	3,650	5,200	8,150	11,800	15,850	33,650
	Тригери CLB	16,000	2,800	29,200	41,600	65,200	94,400	126,800	269,200
Ресурси пам'яті	Максимум розподіленої оперативної пам'яті (КБ)	171	200	313	400	600	892	1,188	2,888
	Блок RAM/FIFO з ECC (по 36 Кб)	20	25	45	50	75	105	135	365
	Всього блоків ОЗП (Кб)	720	900	1,620	1,800	2,700	3,780	4,860	13,140
Часові ресурси	Елементи керування годинами (1 MMCM + 1 PLL)	3	5	3	5	5	6	6	10
Ресурси вводу-виводу	Максимум контактів вводу/виводу з одним кінцем	150	250	150	250	250	300	300	500
	Максимум диференційних пар вводу/виводу	72	120	12	120	120	144	144	240

продовження табл. 4

Вбудовані ресурси жорсткої IP-адреси	Фрагменти DSP			40	45	80	90	120	180	240	740
	PCIe® Gen2			1	1	1	1	1	1	1	1
	Аналоговий змішаний сигнал (AMS)/XADC			1	1	1	1	1	1	1	1
	Налаштування блоків AES/HMAC			1	1	1	1	1	1	1	1
	Приймачі GTP (не більше 6,6 Гбіт/с)			2	4	4	4	4	8	8	16
Марки швидкості	Комерційна температура (C)			-1 -2	-1 -2	-1 -2	-1 -2	-1 -2	-1 -2	-1 -2	-1 -2
	Розширена температура (E)			-2L -3	-2L -3	-2L -3	-2L -3	-2L -3	-2L -3	-2L -3	-2L -3
	Промислова температура (I)			-1 -2 -1L	-1 -2 -1L	-1 -2 -1L	-1 -2 -1L	-1 -2 -1L	-1 -2 -1L	-1 -2 -1L	-1 -2 -1L
	Упаковка	Площа (мм)	Крок (мм)	Доступний ввід-вивід користувача: 3.3V SelectIO™ Ввід-вивід HR (Приймачі GTP)							
	CPG236	10x10	0.5		106(2)		106(2)	106(2)			
	CPG238	10x10	0.5	112(2)		112(2)					
	CSG324	15x15	0.8		210(0)		210(0)	210(0)	210(0)	210(0)	
	CSG325	15x15	0.8	150(2)	150(4)	150(4)	150(4)	150(4)			
	FTG256	17x17	1.0		170(0)		170(0)	170(0)	170(0)	170(0)	
	SBG484	19x19	0.8								285(4)
Сумісне місце	FGG484	23x23	1.0		250(4)		250(4)	250(4)	285(4)	285(4)	
	FBG484	23x23	1.0								285(4)
Сумісне місце	FGG676	27x27	1.0						300(8)	300(8)	
	FBG676	27x27	1.0								400(8)
	FFG1156	35x35	1.0								500(16)

Таблиця 5

Характеристика FPGA Kintex-7

		Оптимізовано для кращої ціни і продуктивності (1.0 В, 0.95 В, 0.9 В)						
Номер деталі		XC7K70T	XC7K160T	XC7K325T	XC7K355T	XC7K410T	XC7K420T	XC7K480T
Логічні ресурси	Логічні комірки	10,250	25,350	50,950	55,650	63,550	63,150	74,650
	Частини	65,600	162,240	326,080	356,160	406,720	416,960	477,760
	Тригери CLB	82,000	202,800	407,600	445,200	508,400	521,200	597,200
Ресурси пам'яті	Максимум розподіленої оперативної пам'яті (КБ)	838	2,188	4,000	5,088	5,663	5,938	6,778
	Блок RAM/FIFO з ECC (по 36 Кб)	135	325	445	715	795	835	955
	Всього блоків ОЗП (Кб)	4,860	11,700	16,020	25,740	28,620	30,060	34,380
Часові ресурси	Елементи керування годинами (1 MMCM + 1 PLL)	6	8	10	6	10	8	8
Ресурси вводу-виводу	Максимум контактів вводу/виводу з одним кінцем	300	400	500	300	500	400	400
	Максимум диференційних пар вводу/виводу	144	192	240	144	240	192	192
Вбудовані ресурси жорсткої IP-адреси	Фрагменти DSP	240	600	840	1,440	1,540	1,680	1,920
	PCIe® Gen2	1	1	1	1	1	1	1
	Аналоговий змішаний сигнал (AMS)/XADC	1	1	1	1	1	1	1
	Налаштування блоків AES/HMAC	1	1	1	1	1	1	1
	Приймачі GTP (не більше 12,5 Гбіт/с)	8	8	16	24	16	32	32

продовження табл. 5

Марки швид-кості	Комерційна температура (C)			-1 -2	-1 -2	-1 -2	-1 -2	-1 -2	-1 -2	-1 -2
	Розширена температура (E)			-2L -3	-2L -3	-2L -3	-2L -3	-2L -3	-2L -3	-2L -3
	Промислова температура (I)			-1 -2 -2L	-1 -2 -2L	-1 -2 -2L	-1 -2 -2L	-1 -2 -2L	-1 -2 -2L	-1 -2 -2L
	Упаков-ка	Площа (мм)	Крок (мм)	Доступний власний ввід-вивід: 3.3V ввід-вивід HR, 1.8V ввід-вивід HP (GTX)						
	FBG484	23x23	1.0	185, 100 (4)	185, 100 (4)					
Сумісне місце	FBG676	27x27	1.0	200, 100 (8)	250, 150 (8)	250, 150 (8)		250, 150 (8)		
	FFG676	27x27	1.0		250, 150 (8)	250, 150 (8)		250, 150 (8)		
Сумісне місце	FBG900	31x31	1.0			350, 150 (16)		350, 150 (16)		
	FFG900	31x31	1.0			350, 150 (16)		350, 150 (16)		
	FFG901	31x31	1.0				300, 0 (24)		380, 0 (28)	380, 0 (28)
	FFG1156	35x35	1.0						400, 0 (32)	400, 0 (32)

Таблиця 6

Характеристика FPGA Virtex-7

		Оптимізовано для максимальної продуктивності та ємності системи (1.0 В)										
Номер деталі		XC7V 585T	XC7V2 000T	XC7VX 330T	XC7VX 415T	XC7VX 485T	XC7VX 550T	XC7VX 690T	XC7VX 980T	XC7VX 1140T	XC7VH 580T	XC7VH 870T
Логічні ресурси	Частини	91,050	305,400	51,000	64,400	75,900	86,600	108,300	153,000	178,000	90,700	136,900
	Логічні комірки	582,720	1,954,560	326,400	412,160	485,760	554,240	693,120	979,200	1,139,200	580,480	876,160
	Тригери CLB	728,400	2,443,200	408,000	515,200	607,200	692,800	866,400	1,224,000	1,424,000	725,600	1,095,200
Ресурси пам'яті	Максимум розподіленої оперативної пам'яті (КБ)	6,938	21,550	4,388	6,525	8,175	8,725	10,888	13,838	17,700	8,850	13,275
	Блок RAM/FIFO з ECC (по 36 Кб)	795	1,292	750	880	1,030	1,180	1,470	1,500	1,880	940	1,410
	Всього блоків ОЗП (Кб)	28,620	46,512	27,000	31,680	37,080	42,480	52,920	54,000	67,680	33,840	50,760
Часові ресурси	Елементи керування годинами (1 MMCM + 1 PLL)	18	24	14	12	14	20	20	18	24	12	18
Ресурси вводу-виводу	Максимум контактів вводу/виводу з одним кінцем	850	1,200	700	600	700	600	1,000	900	1,100	600	300
	Максимум диференційних пар вводу/виводу	408	576	336	288	336	288	480	432	528	288	144
Вбудовані ресурси жорсткої IP-адреси	Фрагменти DSP	1,260	2,160	1,120	2,160	2,800	2,880	3,600	3,600	3,360	1,680	2,520
	PCIe® Gen2	3	4	-	-	4	-	-	-	-	-	-
	PCIe Gen3	-	-	2	2	-	2	3	3	4	2	3
	Аналоговий змішаний сигнал (AMS)/XADC	1	1	1	1	1	1	1	1	1	1	1
	Налаштування блоків AES/HMAC	1	1	1	1	1	1	1	1	1	1	1

продовження таблиці 6

	Приймачі GTP (не більше 12,5 Гбіт/с)			36	36	-	-	56	-	-	-	-	-	-	
	Приймачі GTP (не більше 13,1 Гбіт/с)			-	-	28	48	-	80	80	72	96	48	72	
	Приймачі GTP (не більше 28,05 Гбіт/с)			-	-	-	-	-	-	-	-	-	8	16	
Марки швидкості	Комерційна температура (C)			-1 -2	-1 -2	-1 -2	-1 -2	-1 -2	-1 -2	-1 -2	-1 -2	-1 -2	-1 -2	-1 -2	
	Розширена температура (E)			-2L -3	-2L -2G	-2L -3	-2L -3	-2L -3	-2L -3	-2L -3	-2L	-2L -2G	-2L -2G	-2L -2G	
	Промислова температура (I)			-1 -2	-1	-1 -2	-1 -2	-1 -2	-1 -2	-1 -2	-1	-1	-	-	
	Упаковка	Площа (мм)	Крок (мм)	Доступний власний ввід-вивід: 3.3V ввід-вивід HR, 1.8V ввід-вивід HP (GTX, GTH)									1.8V Ввід/вивід HP (GTH, GTZ)		
	FFG1157	35x35	1.0	0, 600 (20, 0)		0, 600 (20, 0)	0, 600 (20, 0)	0, 600 (20, 0)		0, 600 (20, 0)					
Сумісне місце	FFG1761	42.5x42.5	1.0	100, 750 (36, 0)		50, 650 (0, 28)		0, 700 (28, 0)		0, 850 (0, 36)					
	FHG1761	45x45	1.0		0, 850 (36, 0)										
	FLG1925	35x35	1.0		0, 1200 (16, 0)										
	FFG1158	45x45	1.0				0, 350 (0, 48)	0, 350 (0, 48)	0, 350 (0, 48)	0, 350 (0, 48)					
Сумісне місце	FFG1926	45x45	1.0							0, 720 (0, 64)	0, 720 (0, 64)				
	FLG1926	45x45	1.0									0, 720 (0, 64)			
	FFG1927	45x45	1.0				0, 600 (0, 48)	0, 600 (56, 0)	0, 600 (0, 80)	0, 600 (0, 80)					
Сумісне місце	FFG1928	45x45	1.0								0, 480 (0, 72)				
	FLG1928	45x45	1.0									0, 480 (0, 96)			
Сумісне місце	FFG1930	45x45	1.0					0, 700 (24, 0)		0, 1000 (0, 24)	0, 900 (0, 24)				
	FLG1930	45x45	1.0									0, 1100 (0, 24)			
	FLG1155	35x35	1.0										400 (24, 8)		
	FLG1931	45x45	1.0										600 (48, 8)		
	FLG1932	45x45	1.0											300 (72, 16)	

Перевага, що віддається сімейству Xilinx Artix-7, має кілька небажаних наслідків, про які коротко говориться нижче:

1. Artix-7 – бюджетне сімейство FPGA. Як таке, воно не дуже підходить для високошвидкісних реалізацій. Апаратних ресурсів, навіть найбільшого пристрою цього сімейства, часто виявляється недостатньо для демонстрації повного потенціалу розпаралелювання операцій даного алгоритму PQC. Таким чином, використання Artix-7 має сенс для порівняльного аналізу легких реалізацій, але може привести до отримання недостатньо оптимальних результатів для високошвидкісних реалізацій.

2. Artix-7 – це традиційна FPGA, а не SoC FPGA. В результаті, єдиний спосіб розробки однокристальної програмно-апаратної реалізації за допомогою Artix-7 – це використання так званих "м'яких" процесорних ядер, тобто процесорів, реалізованих з використанням

програмувальної логіки. До "м'яких" процесорів, сумісних з Artix-7, належать MicroBlaze і полегшені версії RISC-V. Всі вони працюють на значно низькій тактовій частоті, ніж вбудовані твердотільні процесори SoC FPGA.

3. Artix-7 не підходить для проектів HLS. Такі проекти, як правило, вимагають значно більше ресурсів, ніж проекти, засновані на написанні коду вручну в HDL.

4. Artix-7 – досить старе покоління FPGA, випущене Xilinx в 2010 р. На момент прийняття стандарту PQC цьому сімейству буде вже як мінімум 12 років. Незважаючи на те, що це сімейство як і раніше відносно популярно для недорогих додатків, воно не являє собою сучасну технологію FPGA.

5. Не прийнято засновувати ранжування кандидатів в криптографічних конкурсах на результатах, отриманих для одного сімейства одного постачальника. Хоча Xilinx є найбільшим розробником FPGA і SoC FPGA, Intel посідає друге місце, а інші постачальники, такі як Microchip і Lattice Semiconductor, також розробляють FPGA, які підходять для реалізації криптографічних алгоритмів. Під час конкурсу SHA-3 були оголошені результати за семи родинами FPGA від двох основних постачальників, Xilinx і Altera. Під час конкурсу CAESAR були прийняті в роботу чотири сімейства Xilinx і чотири сімейства Altera. Для всіх цих сімейств результати були сформовані на основі одного і того ж HDL коду. Не було необхідності купувати кілька пристроїв або плат. Досить було безкоштовних або пробних версій інструментів. Конструкції закінчувалися генерацією звітів після розміщення та маршрутизації, в яких правильно описувалися найгірші показники продуктивності конкретного екземпляра даного FPGA-пристрою.

6. Ґрунтуючись на досвіді авторів, численні експерти при рецензуванні робіт, присвячених реалізації кандидатур 2-го раунду PQC, розглядали вибір NIST Artix-7 як абсолютну вимогу. Заявки, що не відповідають цій вимозі, підлягали відхиленню або запитам на внесення великих змін. В результаті благородна мета зробити результати більш зіставними між собою була перетворена в привід для заборони або затримки публікації необхідних результатів [1].

Беручи до уваги ці побоювання, рекомендація для 3-го раунду полягає в тому, щоб заохочувати подання звітів про результати, принаймні, для наступних сімей FPGA:

1. Для малоресурсних апаратних і програмно-апаратних реалізацій на базі програмних процесорних ядер: Xilinx Artix-7 (для сумісності з результатами 2-го раунду) і Intel Cyclone 10 LP.

2. Для малоресурсних програмних та апаратних реалізацій на основі використання жорстких процесорних ядер: серії Xilinx Zynq 7000 та FPGA Intel Cyclone V SoC.

3. Для високошвидкісних апаратних засобів та швидкісних програмно-технічних реалізацій: Zynq Xilinx UltraScale+ та Intel Stratix 10 SoC.

Однією з причин вибору Zynq Xilinx UltraScale+, навіть для чистих апаратних реалізацій, які не потребують використання можливостей SoC, є підтримка цих пристроїв безкоштовною версією інструментарію Xilinx, так званого Vivado HL WebPACK, якого достатньо для отримання всіх необхідних результатів еталонного тестування. FPGA Xilinx Virtex-7 UltraScale+, які можна було б вважати природним претендентом, не підтримуються тією ж безкоштовною версією утиліт. Сімейство Zynq Xilinx UltraScale+ також рекомендується для високошвидкісних програмно-апаратних реалізацій, заснованих на використанні жорстких процесорних ядер, завдяки помірній ціні відповідних прототипних плат і наявності безкоштовного еталонного набору для програмно-апаратних реалізацій схем PQC, розробленого в Університеті Джорджа Мейсона [7].

Реалізації орієнтовані на FPGA

У табл. 7 та 8 підсумовано реалізації, орієнтовані на FPGA Xilinx Artix-7 та пов'язані з ними FPGA Xilinx Zynq-7000 SoC. Для 1-го рівня стійкості шість кандидатів – Classic McEliece, Crystals-Kyber, FrodoKEM, NewHope, SIKE та Saber – повідомили про реалізацію всіх трьох операцій. Попередні реалізації BIKE були зосереджені лише на генерації ключів. Для NewHope не має 3-го рівня стійкості. Щодо рівня 5, то для Classic McEliece результати відсутні.

Для більшості KEM час декапсуляції перевищує час інкапсуляції. Записи в таблиці впорядковуються відповідно до часу декапсуляції в мкс (і, якщо потрібно, відповідно до часу декапсуляції в тактах).

Рейтинг кандидатів, перелічених у табл. 2 та 3, дуже складно визначити на основі наявних результатів. По-перше, може бути несправедливим порівнювати чисто апаратні реалізації з програмно-апаратними. По-друге, важко порівнювати малоресурсні реалізації з швидкісними реалізаціями, оскільки вони оптимізовані з урахуванням різних первинних показників. По-третє, програмно-апаратні реалізації на основі різних процесорів дуже складно порівняти один з одним. Нарешті, навіть для реалізацій, що використовують однаковий тип реалізації (програмну/апаратну) та аналогічний тип процесора (RISC-V) порівняння може бути ненавмисно необ'єктивним. У конкретному випадку [8] було запропоновано суттєво іншу апаратну підтримку алгоритмів, які можуть скористатися теоретико-числовим перетворенням – Kyber та NewHope – проти алгоритму, який не може ним скористатися – Saber. Додатковим, відносно незначним фактором є те, що кілька результатів для класичного McEliece та NewHope стосуються їх IND-CPA-стійкого АСШ, а не IND-CCA-стійкого KEM.

Враховуючи всі ці фактори, майже єдиним способом ранжування, який цілком зрозумілий з табл. 2 та 3, є ранжування кандидатів, які мають результати для чисто апаратної реалізації, орієнтованої на швидкісну. У цій конкретній категорії ранжування для рівня стійкості 1 становить: 1) NewHope, 2) Classic McEliece, 3) FrodoKEM. Якщо припустити, що програмно-апаратна реалізація SIKE з процесором користувача майже настільки ж ефективна як і чисто апаратна реалізація, то також можна додати SIKE на позиції 4). На рівні 3 у NewHope немає варіанту, а на рівні 5 Classic McEliece та FrodoKEM не повідомляють про високошвидкісні чисто апаратні реалізації [1].

У табл. 9 та 10 підсумовано реалізації, орієнтовані на FPGA Xilinx Virtex-7. На жаль, єдиний висновок, який можна зробити з цих таблиць, – це перевага Classic McEliece перед SIKE з точки зору всіх показників продуктивності, окрім кількості LUT та тригерів.

У табл. 11 порівнюються результати, про які було повідомлено наприкінці 2019 р., та результати, про які повідомляли інші групи відповідно до Saber та NewHope. Усі результати були отримані з використанням тієї ж SoC FPGA, Zynq UltraScale+. Програмна/апаратна реалізація Round5 була дуже схожа на чисто апаратну реалізацію. Те ж саме не стосувалось програмного забезпечення та апаратного забезпечення Saber, значний відсоток часу виконання був присвячений функціям, що залишаються в програмному забезпеченні, та передачі даних і контролю між програмним та апаратним забезпеченням. Як результат, найбільш точне порівняння між Round5 та Saber можливе на 3-му рівні стійкості, який має чисто апаратну реалізацію Saber. За рахунок цієї реалізації Saber перевершує Round5 з невеликим відривом у плані часу виконання інкапсуляції та декапсуляції. У той же час, навіть найшвидша реалізація Saber використовує в 1,6 разів менше LUT, ніж Round5, з однаковою кількістю одиниць BRAM та DSP. Показано, що FrodoKEM набагато повільніше, ніж Saber і Round5 для всіх рівнів стійкості.

Дещо інакше, для 5-го рівня стійкості чисто апаратна реалізація NewHope, про яку повідомляється в роботі [9], недостатньо швидка для того, щоб перевершити програмно-технічну реалізацію Round5 з [10]. Однак порівняння дещо ускладнюється тим, що в [9] результати свідчать не про IND-CPA-стійке асиметричне шифрування (а не про IND-CCA-стійкий KEM), а лише про суму генерації та розшифрування ключів (а не про саме розшифрування).

У табл. 12 підсумовано результати, які доступні для реалізації цифрових підписів. Реалізації, орієнтовані на FPGA, розглядаються першими в табл. 12. На жаль, кілька результатів для qTESLA стосуються наборів евристичних параметрів, які були відкликані представниками 20 серпня 2019 р. Серед решти конструкцій, для Artix-7, рейтинг кандидатів на 1-му рівні стійкості: 1) Picnic, 2) Dilithium і 3) qTESLA. Різниці між цими кандидатами щодо часу виконання для створення підписів (більш критично) та перевірки підписів дуже істотні. У той же час, лише реалізація Picnic – це швидкісна та чиста апаратна реалізація. Решта реалізації – це реалізація програмного забезпечення та обладнання на основі RISC-V. Крім того, кількість LUT для Picnic приблизно в шість разів більша, ніж для Dilithium, а кількість BRAM у 3,75 рази більше. У той же час, порівняно з Picnic, час створення підписів у Dilithium-I в 12 разів і у Dilithium-II в 16 разів довший.

Для 3-го рівня реалізація для Picnic відсутня. Реалізації Dilithium-III та qTESLA-p-III схожі за типом, цільовим призначенням та використанням ресурсів. У той же час реалізація Dilithium на порядок ефективніша. Реалізації схем електронного підпису, орієнтованих на Kintex-7 та Virtex-7, узагальнені в одній таблиці. Що стосується реалізації Kintex-7, Rainbow істотно перевершує Picnic для рівня стійкості 1. Для решти родин та рівнів безпеки повідомляється лише про одного кандидата із оновленим набором параметрів [1].

Таблиця 7

1-й рівень KEM та PKE на Artix-7 (за замовчуванням) та Zynq-7000 (позначається верхнім індексом Z)

Algorithm	**Type**	**Target**	**Max. Freq.**	**LUT**	**FF**	**Slice**	**DSP**	**BR AM**	**Key Generation**		**Encaps./Enc.**^{cpa}		**Decaps./(Dec.+Enc.)**^{cpa}	
									cycles	*µs*	**cycles**	*µs*	**cycles**	*µs*
						Security Level 1								
NewHope-512^{cpa}	HW	HS	200	6,780	4,026	–	2	7.0	4,200	21.0	6,600	33.0	9,100	45.5
mceliece348864^{cpa}	HW	HS	106	81,339	132,190	–	0	236.0	202,787	1,920.3	2,720	25.8	12,743	120.7
mceliece348864^{cpa}	HW	HS	108	25,327	49,383	–	0	168.0	1,599,882	14,800.0	2,720	25.2	18,358	169.8
Kyber-512	SW/HW^{RV}	LW	–	23,925	10,844	–	21	32.0	150,106	–	193,076	–	204,843	–
FrodoKEM-640			172	2,587	2,994	855	16	0						
	HW	HS							204,766	1,190.5	207,269	1,212.1	209,867	1,408.5
16x			149	6,881	5,081	1,947	16	12.5						
Kyber-512	SW/HW^{RV}	LW	25*	14,975	2,539	4,173	11	14.0	74,519	2,980.8	131,698	5,267.9	142,309	5,692.4
NewHope-512	SW/HW^{RV}	LW	–	23,925	10,844	–	21	32.0	123,860	–	207,299	–	226,742	–
NewHope-512	SW/HW^{RV}	LW	25*	14,975	2,539	4,173	11	14.0	97,969	3,918.8	236,812	9,472.5	258,872	10,354.9
LightSaber	SW/HW^{RV}	LW	–	23,925	10,844	–	21	32.0	366, 837	–	526, 496	–	657,583	–
Kyber-512	SW/HW^{RV}	LW	59	1,842	1,634	–	5	34.0	710,000	11,993.2	971,000	16,402.0	870,000	14,695.9
NewHope-512	SW/HW^{RV}	LW	59	1,842	1,634	–	5	34.0	904,000	15,270.3	1,424,000	24,054.1	1,302,000	21,993.2
SIKEp434	SW/HW^{c}	HS	162	22,595	11,558	7,491	162	37.0	1,474,200	9100	2,494,800	15,400.0	2,656,800	16,400.0
SIKEp503	SW/HW^{c}	HS	162	22,595	11,558	7,491	162	37.0	1,733,400	10,700.0	2,932,200	18,100.0	3,126,600	19,300.0
FrodoKEM-640			191	971	433	290	1	0						
	HW	LW							3,237,288	16,949.2	3,275,862	17,241.4	3,306,122	20,408.2
1x														
			162	4,446	2,152	1,254	1	12.5						
	SW/HW^{c}													
SIKEp434		LW	143	10,976	7,115	3,512	57	21.0	2,187,902	15,300.0	3,718,004	26,000.0	3,946,804	27,600.0
SIKEp503	SW/HW^{c}	LW	143	10,976	7,115	3,512	57	21.0	2,602,603	18,200.0	4,390,104	30,700.0	4,676,105	32,700.0
FrodoKEM-640	SW/HW^{RV}	LW	25*	14,975	2,539	4,173	11	14.0	11,453,942	458,157.7	11,609,668	464,386.7	12,035,513	481,420.5
BIKE-1 Level 1^{cs}	HW	HS	165	1,907	1,049	608	0	7.0	95,500	578.0	–	–	–	–
BIKE-3 Level 1^{cs}	HW	HS	170	1,397	925	453	0	4.0	98,500	579.0	–	–	–	–
BIKE-2 Level 1^{cs}	HW	HS	160	3,874	2,141	1,312	0	10.0	2,150,000	13,437.0	–	–	–	–
BIKE Level 1	HW	HS	135	1,865	589	590	0	4.0	7,370,429	54,540.0	–	–	–	–

Таблиця 8

3-й та 5-й рівні KEM та PKE на Artix-7 (за замовчуванням) та Zynq-7000 (позначається верхнім індексом Z)

Algorithm	**Type**	**Target**	**Max.**	**LUT**	**FF**	**Slice**	**DSP**	**BR**	**Key Generation**		**Encaps./Enc.**^{cpa}		**Decaps./(Dec.+Enc.)**^{cpa}	
			Freq.					**AM**	**cycles**	*µs*	**cycles**	*µs*	**cycles**	*µs*
						Security Level 3								
mceliece460896^{cpa}	HW	HS	107	38,669	74,858	–	0	303.0	5,002,044	46,704.4	3,360	31.4	31,005	289.5
FrodoKEM-976			169	2,869	3,000	908	16	0						
16x	HW	HS	168	6,188	4,678	1782	16	0	476,056	2,816.9	479,993	2,857.1	483,073	3,076.9
			157	7,213	5,087	2042	16	19.0						
	SW/HW^{A9}													
Saber^{Z}		HS	125	7,400	7,331	–	28	2.0	–	3,273.0	–	4,147.0	–	3,844.0
Kyber-768	SW/HW^{RV}	LW	25*	14,975	2,539	4,173	11	14.0	111,525	4,461.0	177,540	7,101.6	190,579	7,623.2
SIKEp610	SW/HW^{c}	HS	162	22,595	11,558	7,491	162	37.0	2,916,000	18,000.0	5,443,200	33,600.0	5,508,000	34,000.0
FrodoKEM-976			189	1,243	441	362	1	0						
1x	HW	LW	187	4,650	2,118	1,272	1	0	7,560,000	40,000.0	7,480,000	40,000.0	7,714,286	47,619.0
			162	4,888	2,153	1,390	1	19.0						
	SW/HW^{c}													
SIKEp610		LW	143	10,976	7,115	3,512	57	21.0	4,347,204	30,400.0	8,108,108	56,700.0	8,208,208	57,400.0
FrodoKEM-976	SW/HW^{RV}	LW	25*	14,975	2,539	4,173	11	14.0	26,005,326	1,040,213.0	29,749,417	1,189,976.7	30,421,175	1,216,847.0
BIKE Level 3	HW	HS	135	1,884	557	593	0	5	30,447,947	231,400.0	–	–	–	–
						Security Level 5								
NewHope-1024^{cpa}	HW	HS	200	6,781	4,127	–	2	8.0	8,000	40.0	12,500	62.5	17,300	86.5
NewHope-1024^{cpa}	HW	HS	190	13,244	8,272	–	24	18.0	–	–	34,000	178.0	30,600^{KD}	160.0^{KD}
Kyber-1024	SW/HW^{RV}	LW	25*	14,975	2,539	4,173	11	14.0	148,547	5,941.9	223,469	8,938.8	240,977	9,639.1
NewHope-1024	SW/HW^{RV}	LW	25*	14,975	2,539	4,173	11	14.0	97,969	3,918.8	236,812	9,472.5	258,872	10,354.9
Kyber-1024	SW/HW	LW	–	23,925	10,844	–	21	32.0	349,673	–	405,477	–	424,682	–
NewHope-1024	SW/HW	LW	–	23,925	10,844	–	21	32.0	235,420	–	392,734	–	450,541	–
NewHope-1024^{cpa}	SW/HW	HS	25	26,606	26,303	–	32	1.0	357,052	14,282.1	589,285	23,571.4	756,932	30,277.3
FireSaber	SW/HW	LW	–	23,925	10,844	–	21	32.0	1,300,272	–	1,622,818	–	1,898,051	–
Kyber-1024	SW/HW^{RV}	LW	59	1,842	1,634		5	34.0	2,203,000	37,212.8	2,619,000	44,239.9	2,429,000	41,030.4
SIKEp751	SW/HW^{c}	HS	162	22,595	11,558	7,491	162	37.0	3,742,200	23,100.0	6,188,400	38,200.0	6,658,200	41,100.0
NewHope-1024	SW/HW^{RV}	LW	59	1,842	1,634		5	34.0	1,776,000	30,000.0	2,742,000	46,317.6	2,528,000	42,702.7
SIKEp751	SW/HW^{c}	LW	143	10,976	7,115	3,512	57	21.0	7,965,108	55,700.0	13,156,013	92,000.0	14,185,614	99,200.0
FrodoKEM-1344	SW/HW^{RV}	LW	25*	14,975	2,539	4,173	11	14.0	67,994,170	2,719,766.8	71,501,358	2,860,054.3	72,526,695	2,901,067.8

Таблиця 9

КЕМ 1-го рівня на Virtex-7 (за замовчуванням) та Virtex-6 (позначено верхнім індексом ^{V6})

Algorithm	Type	Target	Max. Freq.	LUT	FF	Slice	DSP	BR AM	Key Generation		Encap./Enc.^{cpa}		Decaps./Dec.^{cpa}	
									cycles	μs	cycles	μs	cycles	μs
					Security Level 1									
SIKEp503	HW	HS	171	25,094	26,971	9,514	264	34.0	640,000	3,738.3	1,120,000	6,542.1	1,210,000	7,067.8
SIKEp434	SW/HW	HS	142	21,210	13,657	7,408	162	38.0	981,180	6,900.0	1,677,960	11,800.0	1,777,500	12,500.0
SIKEp503	SW/HW	HS	142	21,210	13,657	7,408	162	38.0	1,166,040	8,200.0	1,976,580	13,900.0	2,104,560	14,800.0
LEDAkem-128^{o,cpa,V6}	HW	LW	235	104	53	33	0	1.0	–	–	712,000	3,029.8	2,620,000	18,714.3
			140	2,222	658	870	0	13.0						
SIKEp434	SW/HW	LW	152	10,937	7,132	3,415	57	21.0	2,191,781	14,400.0	3,713,851	24,400.0	3,957,382	26,000.0
SIKEp503	SW/HW	LW	152	10,937	7,132	3,415	57	21.0	2,602,740	17,100.0	4,383,562	28,800.0	4,672,755	30,700.0

Розробка варіанту КЕМ, стійкого до атаки з обраним відкритим текстом (CPA)

^{V6} Проект реалізовано на Virtex-6

^{o} Проект старого набору параметрів змінено поданими 19 березня 2020 р.

Таблиця 10

КЕМ та АСШ 3-го та 5-го рівнів стійкості на Virtex-7

Algorithm	Type	Target	Max. Freq.	LUT	FF	Slice	DSP	BR AM	Key Generation		Encaps./Enc.^{cpa}		Decaps./(Dec.+Enc.)^{cpa}	
									cycles	μs	cycles	μs	cycles	μs
						Security Level 3								
mceliece460896^{cpa}	HW	HS	131	109,484	168,939	–	0	446.0	515,806	3,943.5	3,360	25.7	17,931	137.1
SIKEp610	SW/HW	HS	142	21,210	13,657	7,408	162	38.0	1,962,360	13,800.0	3,654,540	25,700.0	3,711,420	26,100.0
SIKEp610	SW/HW	LW	152	10,937	7,132	3,415	57	21.0	4,353,120	28,600.0	8,097,412	53,200.0	8,219,178	54,000.0
						Security Level 5								
mceliece6960119^{cpa}	HW	HS	130	116,928	188,324	–	0	607.0	974,306	7,500.4	5,413	41.7	25,135	193.5
mceliece6688128^{cpa}	HW	HS	137	122,624	186,194	–	0	589.0	1,046,139	7,658.4	5,024	36.8	29,754	217.8
mceliece8192128^{cpa}	HW	HS	130	123,361	190,707	–	0	589.0	1,286,179	9,901.3	6,528	50.3	32,765	252.2
mceliece6960119^{cpa}	HW	HS	141	44,154	88,963	–	0	563.0	11,179,636	79,570.4	5,413	38.5	46,141	328.4
mceliece6688128^{cpa}	HW	HS	136	44,345	83,637	–	0	446.0	12,389,742	91,034.1	5,024	36.9	52,333	384.5
mceliece8192128^{cpa}	HW	HS	134	45,150	88,154	–	0	525.0	15,185,314	113,154.4	6,528	48.6	55,330	412.3
SIKEp751	HW	HS	167	45,893	50,390	17,530	512	43.5	1,240,000	7,407.4	2,170,000	12,963.0	2,330,000	13,918.8
SIKEp751	SW/HW	HS	142	21,210	13,657	7,408	162	38.0	2,516,940	17,700.0	4,166,460	29,300.0	4,479,300	31,500.0
SIKEp751	SW/HW	LW	152	10,937	7,132	3,415	57	21.0	7,960,426	52,300.0	13,150,685	86,400.0	14,185,693	93,200.0

Таблиця 11

Усі КЕМ та АСШ на Zynq Ultrascale+

Algorithm	Type	Target	Max. Freq.	LUT	FF	Slice	DSP	BRAM	Key Gen.		Encapsulation		Decapsulation	
									cycles	us	cycles	us	cycles	us
					Security Level 1									
R5ND_1KEM_0d	SW/HW	HS	260	55,442	82,341	10,627	0	2	–	–	–	19.0	–	24.0
LightSaber	SW/HW	HS	322	12,343	11,288	1,989	256	3.5	–	–	–	53.0	–	56.0
FrodoKEM-640	SW/HW	HS	402	7,213	6,647	1,186	32	13.5	–	–	–	1,223.0	–	1,319.0
					Security Level 3									
Saber	HW	HS	250	45,895	18,705	–	0	2	4,320	17.3	5,231	20.9	6,461	25.8
Saber	HW	HS	250	25,079	10,750	–	0	2	5,435	21.8	6,618	26.5	8,034	32.1
R5ND_3KEM_0d	SW/HW	HS	249	73,881	109,211	14,307	0	2	–	–	–	24.0	–	33.0
Saber	SW/HW	HS	322	12,566	11,619	1,993	256	3.5	–	–	–	60.0	–	65.0
FrodoKEM-976	SW/HW	HS	402	7087	6693	1190	32	17	–	–	–	1,642.0	–	1,866.0
					Security Level 5									
R5ND_5KEM_0d	SW/HW	HS	212	91,166	151,019	18,733	0	2	–	–	–	32.0	–	42.0
NewHope-1024^{cpa}	HW	HS	406	13,961	8,149	–	25	18	–	–	34,000	83.0	30,600^{KD}	75.0^{KD}
FireSaber	SW/HW	HS	322	12,555	11,881	2,341	256	3.5	–	–	–	74.0	–	80.0
FrodoKEM-1344	SW/HW	HS	417	7,015	6,610	1,215	32	17.5	–	–	–	2,186.0	–	3,120.0

Таблиця 12

Схеми ЕП на Artix-7, Kintex-7 та Virtex-7

Algorithm	Type	Target	Max.	LUT	FF	Slice	DSP	BR	Key Gen.		Signature Verification		Signature Generation		Family
			Freq.					AM	cycles	us	cycles	us	cycles	us	
						Security Level 1 & 2									
Picnic-L1-FS	HW	HS	91	90,535	23,516	25,160	0	52.5	–	–	29,600	325.6	31,300	344.3	
qTESLA-I [o2]	SW/HW	LW	25*	14,975	2,539	4,173	11	14.0	4,846,949	193,878.0	38,922	1,556.9	168,273	6,730.9	
Dilithium-I	SW/HW	LW	25*	14,975	2,539	4,173	11	14.0	95,202	3,808.1	142,576	5,703.0	376,392	15,055.7	Artix-7
Dilithium-II	SW/HW	LW	25*	14,975	2,539	4,173	11	14.0	130,022	5,200.9	184,933	7,397.3	514,246	20,569.8	
qTESLA-p-I	SW/HW	LW	121	7,212	4,378	2,438	15	139.0	925,431	7,648.2	946,520	7,822.5	4,165,160	34,422.8	
Rainbow-Ic [o1]	HW	HS	90	52,895	32,476	15,112	0	67.0	–	–	–	–	979	10.9	
Rainbow-Ia	HW	HS	111	27,712	27,679	8,939	0	59.0	–	–	–	–	1,980	17.8	Kintex-7
Picnic-L1-FS	HW	HS	125	90,037	23,105	–	0	52.5	–	–	29,600	237.0	31,300	250.0	
Rainbow-Ic [o1]	HW	HS	167	52,721	32,475	15,976	0	67.0	–	–	–	–	979	5.9	
Rainbow-Ia	HW	HS	181	27,556	27,675	7,065	0	59.0	–	–	–	–	1,980	10.9	Virtex-7
							Security Level 3								
qTesla-III-speed [o2]	SW/HW	LW	25*	14,975	2,539	4,173	11	14.0	11,898,241	475,929.6	67,712	2,708.5	317,083	12,683.3	
qTesla-III-size [o2]	SW/HW	LW	25*	14,975	2,539	4,173	11	14.0	11,479,190	459,167.6	69,154	2,766.2	348,429	13,937.2	
Dilithium-III	SW/HW	LW	25*	14,975	2,539	4,173	11	14.0	167,433	6,697.3	229,481	9,179.2	634,763	25,390.5	Artix-7
qTESLA-p-III	SW/HW	LW	121	7,475	4,518	2,473	15	147.0	2,305,220	19,051.4	2,315,950	19,140.1	7,745,088	64,009.0	
						Security Level 4 & 5									
Picnic-L5-FS	HW	HS	125	167,530	33,164	–	0	98.5	–	–	146,600	1,173.0	154,500	1,236.0	Kintex-7
Dilithium-IV	SW/HW	LW	25*	14,975	2,539	4,173	11	14.0	223,272	8,930.9	276,221	11,048.8	815,636	32,625.4	Artix-7

Висновки

У роботі розглянуто попередні дослідження щодо апаратної та програмно-апаратної імплементації PQC-схем в рамках 2-го раунду конкурсу NIST PQC. З 26 кандидатів шість – NewHope, Crystals-Kyber, FrodoKEM, Saber, Round5 та SIKE – отримали найбільше покриття за кількістю реалізацій та пов'язаних публікацій. Усі вони мають як швидкісні, так і малоресурсні реалізації. Було застосовано спільне проектування програмно-технічного забезпечення для швидкісних, а не малоресурсних реалізацій, що призвело до вибору Xilinx Zynq UltraScale+, найсучаснішої групи SoC FPGA, у якості основної платформи. Відмінним фактором є те, що ця платформа включає в себе провідний процесор ARM Cortex-A53, який працює на частоті 1,2 ГГц, і значна кількість програмованої логіки підтримує апаратні прискорювачі, які працюють на тактових частотах до 500 МГц.

Для кожного кандидата була зроблена спроба вивантажити якомога більше операцій на обладнанням. Для 50 % досліджуваних KEM цей відсоток сягав 100 %. Таким чином, відповідні реалізації можуть сприйматись у якості апаратних реалізацій, припускаючи, що випадкове початкове число (розміром 16, 24 або 32 байти) було передано апаратному модулю під час інкапсуляції. KEM, реалізований за допомогою цього підходу, включав Kyber, LAC (v3a та v3b), NewHope та Round5 (з кодом для виправлення помилок та без нього). Їх код був протестований за допомогою FPGA Artix-7 та Virtex-7.

Що стосується часу виконання та використання ресурсів, Round5 з кодом виправлення помилок (R5ND_5d) перевершував Round5 без коду виправлення помилок (R5ND_0d). Аналогічно, LAC-v3b виявився кращим за LAC-v3a як за швидкістю, так і у відношенні FPGA-ресурсів. При порівнянні найкращих представників чотирьох кандидатів – Kyber, LAC, NewHope та Round5 можна було зробити наступні висновки. Часи виконання цих кандидатів були надзвичайно близькими один до одного. Для інкапсуляції терміни виконання були в межах 10 % один від одного на рівні безпеки 5, у межах 22 % на рівні безпеки 3 та в межах 32 % на рівні безпеки 1. Для декапсуляції найбільші відмінності складали 26 % на рівні 5, 22 % на рівні 3 та 48 % на рівні 1. У декількох випадках лише зміна сімейства FPGA з недорогого Artix-7 на високоефективний Virtex-7 спричинила суттєві зміни в рейтингу, навіть, якщо код HDL залишився точно таким же. Таким чином, можна зробити висновок, що різниця між цими схемами за швидкістю занадто мала, щоб віддати перевагу будь-якому конкретному кандидату. Ці результати суперечать одному з попередніх звітів, який свідчить про відставання LAC від NewHope та Kyber.

Говорячи про використання ресурсів, підкреслимо, що невелика перевага належить NewHope та Kyber. Обидва використовують меншу кількість LUT та тригерів (FF), ніж LAC та Round5, а використання ними DSP-одиниць та BRAM, хоча і є дещо вищим, але дуже помірне. Крім того, і NewHope, і Kyber використовують майже однакову кількість ресурсів незалежно від рівня безпеки. У випадку LAC та Round5 використання ресурсів різко зростає зі збільшенням рівня безпеки. Здається, колишня властивість є перевагою для програм, які потребують підтримки найвищого або всіх рівнів безпеки. Зокрема, конструкції k-в-1, які підтримують усі k рівні безпеки та дозволяють змінювати їх під час виконання, як правило, мають лише дещо більший рівень використання ресурсів, ніж максимальний рівень безпеки. Таким чином, плоска залежність використання ресурсів від рівня безпеки передбачає потенціал для дуже економічних проектів k-в-1. У той же час, цей потенціал все ж повинен бути підтверджений за допомогою повних проектів.

Також була наведена детальна характеристика FPGA сімейства Xilinx. Кожна конкретна FPGA має використовуватися залежно від мети, очікуваної вартості та продуктивності.

Список літератури:

1. Viet Ba Dang. Implementation and Benchmarking of Round 2 Candidates in the NIST Post-Quantum Cryptography Standardization Process Using Hardware and Software/Hardware Co-design Approaches / Viet Ba Dang, Farnoud Farahmand, Michal Andrzejczak, Kamyar Mohajerani, Duc Tri Nguyen, Kris Gaj. Режим доступу: https://eprint.iacr.org/2020/795.pdf.

2. Xilinx. 7 Series Product Selection Guide. [Електронний ресурс]. Режим доступу: https://www.xilinx.com/support/documentation/selection-guides/7-series-product-selection-guide.pdf.
3. Malik Imran. A Systematic Study of Lattice-based NIST PQC Algorithms: from Reference Implementations to Hardware Accelerators / Malik Imran, Zain Ul Abideen, Samuel Pagliarini. Режим доступу: https://arxiv.org/pdf/2009.07091.pdf.
4. 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.
5. Post-quantum cryptography, round 2 submissions. Режим доступу: https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions.
6. Тарасов И. ПЛИС Xilinx и цифровая обработка сигналов. Особенности, преимущества, перспективы. Режим доступу: https://www.electronics.ru/files/article_pdf/2/article_2788_434.pdf.
7. Farnoud Farahmand et al. Software/Hardware Codesign of the Post Quantum Cryptography Algorithm NTRUEncrypt Using High-Level Synthesis and Register-Transfer Level Design Methodologies // 29th International Conference on Field Programmable Logic and Applications, FPL 2019. Barcelona, Spain: IEEE, Sept. 2019, pp. 225–231. ISBN: 978-1-72814-884-7. DOI: 10.1109/FPL.2019.00042.
8. Kris Gaj. Challenges and Rewards of Implementing and Benchmarking Post-Quantum Cryptography in Hardware // 2018 Great Lakes Symposium on VLSI, GLSVLSI 2018. Chicago, IL, USA: ACM Press, 2018, pp. 359–364. ISBN 978-1-4503-5724-1. DOI: 10/ggbscs.
9. Jens-Peter Kaps et al. Lightweight Implementations of SHA-3 Candidates on FPGAs. In: 12th International Conference on Cryptology in India, Indocrypt 2011. Vol. 7107. LNCS. Chennai, India, Dec. 2011, pp. 270–289. ISBN: 978-3-642-25577-9 978-3-642-25578-6. DOI: 10.1007/978-3-642-25578-6_20. – Режим доступу: https://2011.indocrypt.org/slides/gurung.pdf.
10. Viet B Dang et al. Implementing and Benchmarking Three Lattice-Based Post-Quantum Cryptography Algorithms Using Software/Hardware Codesign // 2019 International Conference on Field Programmable Technology, FPT 2019. Tianjin, China: IEEE, Dec. 9-13, 2019, pp. 206–214. DOI: 10.1109/ICFPT47387.2019.00032.

Надійшла до редколегії 06.02.2021

Відомості про авторів:

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

Шахов Богдан Сергійович – Харківський національний університет імені В.Н. Каразіна, студент кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Україна; e-mail: bogdanshahov2000@gmail.com

УДК 003.026:004.056 **DOI:10.30837/rt.2021.1.204.06**

С.О. КАНДІЙ, Г.А. МАЛЄЄВА

АНАЛІЗ СКЛАДНОСТІ АТАК НА МУЛЬТИВАРІАТИВНІ КРИПТОГРАФІЧНІ ПЕРЕТВОРЕННЯ З ВИКОРИСТАННЯМ АЛГЕБРАЇЧНОЇ СТРУКТУРИ ПОЛЯ

Вступ

В останні роки інтерес до криптосистем, що ґрунтуються на багатовимірних квадратичних перетвореннях (MQ-перетвореннях), значно зріс. В першу чергу це пов'язано з конкурсом NIST PQC [1] та необхідністю у практичних схемах електронного підпису, що є стійкими до атак на квантових комп'ютерах. Незважаючи на те, що світовою спільнотою була проведена велика робота з криптоаналізу представлених схем, багато питань потребують подальшого уточнення. Спеціалісти NIST дуже обережно підходять до процесу стандартизації і закликають криптологів [4] у найближчі три роки провести всесторонній аналіз фіналістів конкурсу NIST PQC перед їх стандартизацією.

Одним з фіналістів є схема електронного підпису Rainbow [2]. Вона є узагальненням схеми UOV (Unbalanced Oil and Vinegar) [3]. Нещодавно на інше узагальнення цієї схеми – LUOV (Lifted UOV) [5] була знайдена атака [6], що за поліноміальний час здатна повністю відновити закритий ключ. Особливістю цієї атаки є використання алгебраїчної структури поля, над яким задане MQ-перетворення. Цей напрямок атак з'явився нещодавно і досі не зрозуміло чи можливо використовувати структуру поля у схемі Rainbow.

Метою цієї роботи є систематизація технік, що використовуються у атаках з використанням алгебраїчної структури поля для криптосистем на основі UOV та аналіз перешкод для їх узагальнення на схему Rainbow.

Схема UOV та її узагальнення

Нехай задано поле $GF(q_1)$ та його підполе $GF(q_2) \subseteq GF(q_1)$. В основі системи UOV лежить перетворення $F : GF^n(q_1) \to GF^m(q_1)$, яке задається n багатовимірними поліномами від m змінних:

$$F(X) = \begin{cases} f^{(1)}(X) = \sum\limits_{i=1}^{n}\sum\limits_{j=i}^{n} \alpha_{ij_1} x_i x_j + \sum\limits_{i=1}^{n} \beta_{i_1} x_i + \gamma_1 \\ f^{(2)}(X) = \sum\limits_{i=1}^{n}\sum\limits_{j=i}^{n} \alpha_{ij_2} x_i x_j + \sum\limits_{i=1}^{n} \beta_{i_2} x_i + \gamma_2 \\ \vdots \\ f^{(m)}(X) = \sum\limits_{i=1}^{n}\sum\limits_{j=i}^{n} \alpha_{ij_m} x_i x_j + \sum\limits_{i=1}^{n} \beta_{i_m} x_i + \gamma_m \end{cases},$$

де коефіцієнти $\alpha_{ij_k}, \beta_{i_k}, \gamma_k$ у загальному випадку належать полю $GF(q_2) \subseteq GF(q_1)$. Знаходження прообразу для цього перетворення є складною задачею, оскільки воно містить нелінійну частину $\sum\limits_{i=1}^{n}\sum\limits_{j=1}^{n} \alpha_{ij_k} x_i x_j$. Надалі це перетворення маскується двома афінними перетвореннями $P = S \circ F \circ T$. Підпис є прообразом для повідомлення відносно цього фінально-

го перетворення. Виробити підпис можливо, якщо зафіксувати частину таким чином, щоб система рівнянь стала лінійною. Нелінійна частина у цьому випадку ділиться на дві незалежні частини. В схемі Rainbow цей поділ узагальнюється на більшу кількість незалежних частин. Детальний огляд змін наданий в специфікації Rainbow [2]. Як правило, в криптосистемах, що побудовані на схемі UOV, використовується поле $GF(2^r)$. Цей вибір обумовлений тим, що для цього поля, на відміну від інших відомих полів, можливо реалізувати швидкі та константні за часом алгоритми множення поліномів. Для поля $GF(p)$, де p-просте число, ці показники значно погіршуються.

Диференційні атаки на підполе

Основною проблемою криптосистем на MQ-перетвореннях є великі розміри ключів. У деяких криптосистемах [5] для вирішення цієї проблеми у якості поля $GF(q_2)$ використовують поле $GF(2)$. Це призвело до появи диференційних атак на підполе (subfield differential attack) [7]. Атака є можливою через наявність проміжних підполів між $GF(q_1)$ та $GF(q_2)$: існує поле $GF(2^d)$, таке що

$$GF(2) \subset GF(2^d) \subset GF(2^r). \tag{1}$$

Якщо таке поле існує, то можливо побудувати ізоморфізм

$$GF(2^r) \cong GF(2^d)[X]/(g(t)), \tag{2}$$

де $g(t)$ є незвідним поліномом степеня $s = r/d$. У цьому випадку компоненти рівнянь можливо перегрупувати за степенями t і створити нову систему рівнянь, яка містить меншу кількість нелінійних компонентів.

Ключова ідея атаки полягає у пошуку прообразу для довільного елемента $Y \in GF^n(2^r)$ в формі диференціалу $X = X' + \bar{X}$, де $X' \in GF^n(2^r)$ і $\bar{X} \in GF^n(2^d)$. При цьому X' обирається випадковим чином. Оскільки $\bar{X}$ належить до проміжного поля $GF(2^d)$, то множина рішень суттєво зменшується.

Розглянемо детальніше процес пошуку рішення. Якщо обчислити $P(X' + \bar{X})$, то матимемо:

$$P(X' + \bar{X}) = \begin{cases} p^{(1)}(X' + \bar{X}) = \sum_{i=1}^{n}\sum_{j=i}^{n} \alpha_{ij_1}(x_i' + \bar{x}_i)(x_j' + \bar{x}_j) + \sum_{i=1}^{n} \beta_{i_1}(x_i' + \bar{x}_i) + \gamma_1 \\ p^{(2)}(X' + \bar{X}) = \sum_{i=1}^{n}\sum_{j=i}^{n} \alpha_{ij_2}(x_i' + \bar{x}_i)(x_j' + \bar{x}_j) + \sum_{i=1}^{n} \beta_{i_2}(x_i' + \bar{x}_i) + \gamma_2 \\ \vdots \\ p^{(m)}(X' + \bar{X}) = \sum_{i=1}^{n}\sum_{j=i}^{n} \alpha_{ij_m}(x_i' + \bar{x}_i)(x_j' + \bar{x}_j) + \sum_{i=1}^{n} \beta_{i_m}(x_i' + \bar{x}_i) + \gamma_m \end{cases}$$

Після розкриття дужок та перегрупування невідомих маємо нову систему рівнянь відносно $\bar{X}$:

$$P(X'+\overline{X})=\begin{cases} p^{(1)}(X'+\overline{X})=\sum_{i=1}^{n}\sum_{j=i}^{n}\alpha_{ij_1}(x_j'\overline{x}_i+x_i'\overline{x}_j+x_i'x_j')+\sum_{i=1}^{n}\beta_{i_1}(\overline{x}_i+x_i')+\gamma_k+\sum_{i=1}^{n}\sum_{j=i}^{n}\alpha_{ij_1}\overline{x}_i\overline{x}_j \\ p^{(2)}(X'+\overline{X})=\sum_{i=1}^{n}\sum_{j=i}^{n}\alpha_{ij_2}(x_j'\overline{x}_i+x_i'\overline{x}_j+x_i'x_j')+\sum_{i=1}^{n}\beta_{i_2}(\overline{x}_i+x_i')+\gamma_k+\sum_{i=1}^{n}\sum_{j=i}^{n}\alpha_{ij_2}\overline{x}_i\overline{x}_j \\ \vdots \\ p^{(m)}(X'+\overline{X})=\sum_{i=1}^{n}\sum_{j=i}^{n}\alpha_{ij_m}(x_j'\overline{x}_i+x_i'\overline{x}_j+x_i'x_j')+\sum_{i=1}^{n}\beta_{i_m}(\overline{x}_i+x_i')+\gamma_k+\sum_{i=1}^{n}\sum_{j=i}^{n}\alpha_{ij_m}\overline{x}_i\overline{x}_j \end{cases}$$

У новій системі рівнянь можливо виділити лінійну частину $G_k(\overline{X}), k=1...m$:

$$G_k(\overline{X})=\sum_{i=1}^{n}\sum_{j=i}^{n}\alpha_{ij_2}(x_j'\overline{x}_i+x_i'\overline{x}_j+x_i'x_j')+\sum_{i=1}^{n}\beta_{i_2}(\overline{x}_i+x_i')+\gamma_k \tag{3}$$

Та квадратичну частину $Q_k(\overline{X}), k=1...m$:

$$Q_k(\overline{X})=\sum_{i=1}^{n}\sum_{j=i}^{n}\alpha_{ij_k}\overline{x}_i\overline{x}_j\ . \tag{4}$$

Оскільки існує ізоморфізм (2), то рішення системи можливо розглядати як поліном відносно деякої змінної t:

$$P(X'+\overline{X})=\sum_{i=0}^{s-1}w_{i_k}t^i\ . \tag{5}$$

При цьому частина матиме вигляд

$$G_k(\overline{X})=\sum_{i=1}^{s-1}g_{i_k}(\overline{X})t^i, \tag{6}$$

де $g_{i_k}(\overline{X})$ - нові лінійні поліноми. І квадратична частина, оскільки $\overline{X}\in GF^n(2^d)$, матиме вигляд

$$Q_k(\overline{X})=w_{0_i} \tag{7}$$

Такий простий вигляд зумовлений тим, що $\alpha_{ij_k}\in GF(2)$. Тож, якщо підсумувати (5) - (7), то отримуємо нову систему рівнянь:

$$P(X'+\overline{X})=\begin{cases} p^{(1)}(X'+\overline{X})=\sum_{i=1}^{s-1}g_{i_2}(\overline{X})t^i+Q_2(\overline{X})=\sum_{i=0}^{s-1}w_{i_2}t^i \\ p^{(2)}(X'+\overline{X})=\sum_{i=1}^{s-1}g_{i_2}(\overline{X})t^i+Q_2(\overline{X})=\sum_{i=0}^{s-1}w_{i_2}t^i \\ \vdots \\ p^{(m)}(X'+\overline{X})=\sum_{i=1}^{s-1}g_{i_m}(\overline{X})t^i+Q_m(\overline{X})=\sum_{i=0}^{s-1}w_{i_m}t^i \end{cases}.$$

Нова система є перевизначеною. Використовуючи метод [8], її можна звести до системи з $m-\left\lfloor (n-(s-1)m)/m \right\rfloor$ рівнянь та невідомих. Для більшості загальносистемних параметрів ця нова система буде суттєво меншою за оригінальну. У свою чергу, вирішення цієї системи матиме меншу складність.

Вкладені диференційні атаки на підполе

Ці атаки узагальнюють диференційні атаки. Замість пошуку прообразу у формі диференціалу $x'+\bar{x}=\sum_{i=0}^{s-1} w_i t^i+\bar{x}$ автори пропонують шукати його в формі

$$X = X_0 + X_1 t + X_2 t^2 \ldots , \tag{8}$$

де $X_0, X_1, X_2 \ldots$ шукаються ітеративно на основі попередніх значень. Для опису процедури пошуку необхідно ввести поняття s-відсічення. Процедура s-відсічення для елемента кільця $GF(2^r)$ (у поліноміальному представленні) полягає у відсіченні старших $r-s$ коефіцієнтів:

$$a=\sum_{i=0}^{r-1} a_i t^i \Rightarrow \bar{a}^s=\sum_{i=0}^{s} a_i t^i .$$

Відповідно для багатомірного полінома:

$$f(\bar{X})=\sum_{i=1}^{n}\sum_{j=i}^{n}\alpha_{ij}\bar{x}_i\bar{x}_j+\sum_{i=1}^{n}\beta_i\bar{x}_i+\gamma \Rightarrow$$

$$\Rightarrow \bar{f}^s(\bar{X})=\sum_{i=1}^{n}\sum_{j=i}^{n}\bar{\alpha}_{ij}^s\bar{x}_i\bar{x}_j+\sum_{i=1}^{n}\bar{\beta}_i^s\bar{x}_i+\bar{\gamma}^s .$$

І для системи рівнянь визначається наступним чином:

$$P(\bar{X})=\begin{cases} p_1(\bar{X}) \\ p_2(\bar{X}) \\ \vdots \\ p_m(\bar{X}) \end{cases} \Rightarrow \bar{P}^s(\bar{X})=\begin{cases} \bar{p}_1^s(\bar{X}) \\ \bar{p}_2^s(\bar{X}) \\ \vdots \\ \bar{p}_m^s(\bar{X}) \end{cases} .$$

Відповідно до введеної нотації змінні $X_0, X_1, X_2 \ldots$ знаходяться з наступних рівнянь:

X_0 - рішення рівняння $\bar{P}^0(X_0)=\bar{Y}^0$,

X_1 - рішення рівняння $\bar{P}^1(X_0+X_1 t)=\bar{Y}^1$,

X_{s-1} - рішення рівняння $\bar{P}^{s-1}(X_0+X_1 t+\ldots+X_{s-2}t^{s-2}+X_{s-1}t^{s-1})=\bar{Y}^{s-1}$.

Оскільки рішення знаходиться ітеративно, то серед цих рівнянь тільки $\bar{P}^0(X_0)=\bar{Y}^0$ є нелінійним:

$$\bar{P}^0(X_0)=\begin{cases} Q_1(X_0) \\ Q_2(X_0) \\ \vdots \\ Q_m(X_0) \end{cases},$$

де $Q_k(X_0)$ визначається за формулою (7). Для всіх інших випадків до рівняння буде додаватися лінійний член. Так для $0<s<r$ система рівнянь матиме вигляд:

$$\bar{P}^s(X_s)=\begin{cases} \sum_{i=1}^{s-1} g_{i_1}(X_i)t^i + Q_1(X_0) + g_{s_1}(X_s) \\ \sum_{i=1}^{s-1} g_{i_2}(X_i)t^i + Q_2(X_0) + g_{s_2}(X_s) \\ \vdots \\ \sum_{i=1}^{s-1} g_{i_m}(X_i)t^i + Q_m(X_0) + g_{s_m}(X_s) \end{cases}.$$

Оскільки нелінійна частина знаходиться на першому кроці, то вирішити всі системи, окрім першої, можливо за поліноміальний час. Тож, складність атаки визначається складністю вирішення системи для випадку $s=0$.

Аналіз атак та перспективи розвитку

Розглянуті атаки ґрунтуються на декількох припущеннях:

- поле, над яким визначена система рівнянь, має нетривіальні підполя. Пошук прообразу відбувається в одному з таких підполів;
- можливо знайти представлення елементів поля як поліномів з коефіцієнтами з підполя в аналітичному вигляді;
- ймовірність того, що існує рішення, яке лежить у підполі, є достатньо великою.

Для оцінки ймовірності існування рішення в диференційній атаці на підполе можливо скористуватися наступною лемою [7].

Лемма 1. Нехай A та B є двома множинами, на яких задано відображення $L: A \to B$. Тоді ймовірність того, що для будь-якого елемента $b \in B$ відображення $L^{-1}(b)$ є не пустою множиною складає $1-\exp\left(\frac{|A|}{|B|}\right)$.

У випадку коли $GF(q_1)=GF(2^r)$ і $GF(q_2)=GF(2^d)$ маємо

$$1-\exp\left(\frac{|GF^n(2^d)|}{|GF^m(2^r)|}\right) \approx 2^{-2^{d*n-r*m}}. \quad (9)$$

Це співвідношення встановлює мінімальний розмір підполя, яке може містити рішення системи з достатньо великою ймовірністю. Виходячи з виразу (9), можна сказати, що якщо використовується поле $GF(2^r)$, то мінімальне підполе $GF(2^d)$ повинно задовольняти співвідношенню

$$d > \frac{r*m}{n}.$$

Необхідність у наявності представлення елементів поля як поліномів з коефіцієнтами з підполя в аналітичному вигляді є умовою, яка суттєво обмежує застосування таких атак. Фактично вони працюють тільки коли коефіцієнти належать полю $GF(2)$. У цьому випадку при поліноміальному представленні маємо

$$\alpha * \overline{x} = \alpha * \sum_{i=0}^{s-1} w_i t^i$$

Фактично, у цьому випадку α є індикаторною величною. А коефіцієнти поліному будуть однозначно визначатися з ізоморфізму (2). Якщо використовується інше підполе, то маємо

$$\alpha * \overline{x} = \sum_{i=0}^{s-1} v_i t^i * \sum_{i=0}^{s-1} w_i t^i = \sum_{i=0}^{s-1} z_i t^i$$

де z_i нелінійно залежить як від α, так від $\overline{x}$. Тож, навіть якщо вдасться вирішити нову систему рівнянь, то відновити $\overline{x}$ з рішення буде складною задачею. В цілому, точний аналіз складності відновлення $\overline{x}$ в відкритих публікаціях відсутній. Це є предметом подальших досліджень. Наразі вирішення цієї задачі вважається достатньо складним, щоб можливо було застосовувати такі атаки на криптосистеми як Rainbow. Тож, для захисту від існуючих атак достатньо, щоб хоча б одна з умов зазначених вище не виконувалася.

Висновки

Незважаючи на те, що криптосистеми на MQ-перетвореннях були запропоновані ще у 80-х роках, вплив поля, над яким задані системи рівнянь, на безпеку схем почав досліджуватися нещодавно. Наразі відомі атаки для випадку, коли коефіцієнти багатовимірних поліномів лежать у $GF(2)$.

Для захисту від існуючих атак достатньо обрати у якості поля для рівнянь $GF(p)$, де p є простим числом. Для оптимізації розміру ключів можливо використовувати поле , що є розширенням $GF(p)$ і має групу Галуа S_n, а коефіцієнти багатовимірних поліномів обирати з $GF(p)$. У цьому випадку не існуватиме проміжних полів і значення p значно зменшиться. Такий вибір дасть гарантований захист від будь-яких атак, що використовують структуру поля. Проте ціною такого вибору є значне погіршення швидкодії системи і складності програмної реалізації.

Для випадків, коли коефіцієнти багатовимірних поліномів лежать у довільному підполі, наразі не має оцінок складності атаки через складність аналізу. Вважається, що атаки є неефективними для цього випадку. Наразі залишається ймовірність узагальнення цих атак на інші криптосистеми, такі як Rainbow. Оскільки він претендує на стандартизацію, то виникає потреба у аналізі атак з використанням структури поля для випадку довільних підполів. Такий аналіз є предметом подальших досліджень.

Список літератури:

1. NIST Web site/ Електронне посилання: https://csrc.nist.gov/projects/post-quantum-cryptography
2. Rainbow Web site / Електронне посилання: https://www.pqcrainbow.org/
3. Wolf, Christopher: Multivariate Quadratic Polynomials in Public Key Cryptography, DIAMANT/EIDMA symposium 2005
4. NISTIR 8309
5. Rainbow Web site / Електронне посилання https://www.esat.kuleuven.be/cosic/pqcrypto/luov/
6. 6 Jintai Ding and Joshua Deaton and Vishakha and Bo-Yin Yang The Nested Subset Differential Attack: A Practical Direct Attack Against LUOV which Forges a Signature within 210 Minutes / Електронне посилання: https://eprint.iacr.org/2020/967.pdf

7. Jintai Ding, Zheng Zhang, Joshua Deaton, Kurt Schmidt, FNU Vishakha New Attacks on Lifted Unbalanced Oil Vinegar, Електронне посилання: https://csrc.nist.gov/CSRC/media/Events/Second-PQC-Standardization Conference/documents/accepted-papers/ding-new-attacks-luov.pdf

8. Enrico Thomae and Christopher Wolf. Solving underdetermined systems of multivari-ate quadratic equations revisited. In Public Key Cryptography- PKC2012-15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, May21-23, 2012. Proceedings, pages 156–171. Springer, 2012

Надійшла до редколегії 07.02.2021

Відомості про авторів:

Кандій Сергій Олегович – АТ «Інститут інформаційних технологій», технік-конструктор, Україна; e-mail: sergeykandy@gmail.com

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

УДК 621.391:519.2 **DOI:10.30837/rt.2021.1.204.07**

Е.В. КОТУХ, канд. техн. наук, А.В. СЕВЕРИНОВ, канд. техн. наук,
А.В. ВЛАСОВ, канд. техн. наук, А.А. ТЕНИЦКАЯ, Е.А. ЗАРУДНАЯ

НЕКОТОРЫЕ РЕЗУЛЬТАТЫ РАЗРАБОТКИ СХЕМ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ С ИСПОЛЬЗОВАНИЕМ НЕАБЕЛЕВЫХ ГРУПП

Введение

Развитие криптографии с открытым ключом было революционной концепцией, появившейся в двадцатом веке. Первым опубликованным исследованием криптографии с открытым ключом была схема согласования ключей, описанная Диффи и Хеллманом (DH) в 1976 г. Наиболее распространенная криптография с открытым ключом и повседневно используемые схемы (DH, RSA, ElGamal, ECC) зависят от структуры абелевых групп. Их безопасность зависит от вычислительной сложности и неразрешимости некоторых сложных проблем теории чисел. Например, алгоритм RSA зависит от задачи целочисленной факторизации. Алгоритмы Диффи – Хеллмана, Эль-Гамаля и ECC зависят от решения задачи дискретного логарифмирования (DLP). В 1997 г. Шор указал, что существуют алгоритмы с полиномиальным временем для решения факторизации и дискретных логарифмических задач, основанные на абелевых группах в приложении для квантового компьютера [1]. С появлением практических результатов в реализации алгоритмов Шора и Гровера на квантовых компьютерах реализация успешной атаки на упомянутые криптосистемы с открытым ключом становится вопросом времени. Современные результаты в решении задачи построения квантового компьютера достаточной мощности мотивируют разработчиков криптопримитивов к пересмотру существующих подходов и определению наиболее эффективных с точки зрения решения задач постквантовой криптографии. Одним из таких перспективных исследовательских приоритетов является исследование криптосистем на основе неабелевых групп.

Проблемы поиска сопряженности, поиска членства и другие варианты являются сложно решаемыми в теории неабелевых групп и являются основой для построения доказуемо безопасных криптосистем с открытым ключом. Наиболее часто обсуждаемые криптографические неабелевые применения включают группы матриц, группы кос, полупрямые произведения, логарифмические подписи (LS) [2 – 8] и алгебраические ластики (AE). Построение криптосистем на основе решения сложной проблемы слова в алгебре групп было предложено Вагнером и Мадьяриком в [9]. Многие неабелевы протоколы установления ключей на основе групп связаны с протоколом Диффи – Хеллмана (DH).

Цель статьи – обзор основных алгоритмов и свойств неабелевых групповых криптосистем с открытым ключом. Предложенные криптосистемы с открытым ключом на основе неабелевых групп реализуют либо шифрование-дешифрование, либо протоколы согласования ключей. Мы обсудим различные криптографические примитивы, которые используют некоммутативные группы в качестве основы для постквантовых примитивов. Здесь и далее мы будем использовать термин «платформа» для обозначения используемой математической основы в построении криптосистемы. Стандартная модель криптографической схемы с открытым ключом состоит из двух сторон, называемых Алисой и Бобом. Предположим, что Алиса хочет отправить сообщение M Бобу. Общая модель схемы шифрования следующая. Алиса использует алгоритм шифрования f_{k_1} для шифрования сообщения $C = f_{k_1}(M)$, где f_{k_1} – односторонняя функция и является публичной. После получения шифра C Боб использует соответствующий алгоритм дешифрования g_{k_2} для декодирования $g_{k_2}(f_{k_1}(M)) = M$, где g_{k_2} должен быть известен только Бобу. Противник Ева использует

методы дифференциального криптоанализа для проведения успешной атаки на платформу или реализацию.

2.1. Матричные группы: схема шифрования Ямамуры

В 1998 г. Ямамурой [10] была предложена ассиметричная схема шифрования на платформе модулярной группы $SL(2,\square)$, которая порождается двумя матрицами $S=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$ и $T=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$, где порядки обоих порождающих $o(S)=4$ и $o(T)=\infty$ и матрица $ST=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$ имеет порядок 6. Также группа $SL(2,\square)$, порожденная матрицами S и ST, имеет условия $S^4=(ST)^4=I$ и $(ST)^3=S^2$. Для матрицы $N\in SL(2,\square)$ матрицы $A:=N^{-1}\begin{pmatrix}0 & -1\\ 1 & 1\end{pmatrix}N$ и $B:=N^{-1}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}N$ удовлетворяют условиям $A^6=B^4=I$ и $A^3=B^2$. Таким образом, матрицы A и B порождают $SL(2,\square)$.

Алгоритм генерации ключа имеет следующий вид.

1. Боб выбирает матрицы $V_1:=(BA)^i$ и $V_2:=\left(BA^2\right)^j\in SL(2,\square)$ для некоторых $i,j\in\square$.

2. Боб выбирает матрицы $M\in GL_2(\square)$ и $F_1(X),F_2(X)\in M_{at_2}(\square[X])$ и $a\in\square$ такое, что $F_1(a)=V_1$ и $F_2(a)=V_2$.

3. Боб вычисляет $W_1(X):=M^{-1}F_1(X)M$ и $W_2(X):=M^{-1}F_2(X)M$.

Теперь у Боба есть публичный ключ: $W_1(X),W_2(X)$ и секретный ключ: M,a

Алгоритм шифрования реализуется следующим образом:

Пусть $b_1...b_n\in\{0,1\}^n$ – сообщение, а Алиса шифрует его следующим образом:

$$C(X):=W_2(X)\prod_{i=1}^{n}\left(W_1(X)^{b_i+1}W_2(X)\right)$$

Криптоанализ. Протокол основан на проблеме поиска сопряженности и проблеме корня. Но Р. Стейнвандт [11] указал, что схема шифрования Ямамуры небезопасна. Предположим, что противник Ева перехватила шифр $C(X)$, тогда она может вычислить $D(X):=W_2(X)^{-1}C(X)=\prod_{i=1}^{n}\left(W_1(X)^{b_i+1}W_2(X)\right)$.

Элементы матрицы T $\left(W_1(X)^{b_i+1}W_2(X)\right)^{-1}D(X)$ должны быть полиномами над C. Начиная с первого бита b_1, если хотя бы один из элементов $D_1:=\left(W_1(X)^2W_2(X)\right)^{-1}D(X)$ содержит непостоянный знаменатель, мы можем заключить, что $b_1=0$, а иначе $b_1=1$. Аналогично, если матрица $D_2:=\left(W_1(X)^2W_2(X)\right)^{-1}D(X)$ содержит неполиномиальный элемент, то можно заключить, что $b_2=0$; в противном случае $b_2=1$. Процесс будет продолжаться, пока не будут восстановлены все биты $b_i,i=1,...,n$. Это означает, что открытый текст $b_1...b_n\in\{0,1\}^n$ может быть эффективно восстановлен только из зашифрованного текста $C(X)$ и публичных данных.

2.2. Матричные группы: BMMC/MMMC1/MMMC2.

В 2013 г. С.К. Росошек [12] предложил схему шифрования типа Эль-Гамаля, названную BMMC (базовая матричная модульная криптосистема), с использованием матриц над $\mathbb{Z}_n$. Общая концепция заключается в следующем. Пусть n – большое натуральное число, и пусть $G(\alpha,\beta,\gamma)$ – свободная подгруппа общей линейной группы $GL(2,\mathbb{Z}_n)$, порожденной тремя образующими A,B и C, где $\alpha,\beta,\gamma\in\mathbb{Z}$ с $|\alpha|,|b|,|\gamma|\geq 3$, $A=\begin{pmatrix}1 & 0\\ \alpha & 0\end{pmatrix}$, $B=\begin{pmatrix}1 & \beta\\ 0 & 1\end{pmatrix}$ и $C=\begin{pmatrix}1-\gamma & r\\ -\gamma & \gamma+1\end{pmatrix}$. Все предложенные переменные – публичные. Пусть q порядок группы $GL(2,\mathbb{Z}_n)$.

Алгоритм генерации ключа имеет следующий вид.

Боб выбирает две случайные матрицы P_1 и U в $G(\alpha,\beta,\gamma)$ с условием, что $P_1U\neq UP_1$ и три целых числа k,s,l с условием, что $-q\leq k,s\leq q$ и $2\leq q$

Боб вычисляет $P_2:=U^{-s}P_1^kU^s$ и $P_3:=U^l$.

Таким образом, у Боба есть общий ключ n,P_1,P_2,P_3 и секретный ключ U,k,s.

Алгоритм шифрования.

Пусть сообщение $m\in Mat(2,\mathbb{Z}_n)$ будет матрицей. Алиса выбирает целые числа $r,t\in\mathbb{Z}_n$ и вычисляет шифротекст выражением $(C_1,C_2):=\left(P_3^{-r}P_1^tP_3^r, mP_3^rP_2^{-t}P_3^{-r}\right)$.

Алгоритм дешифрования. Боб вычисляет m, используя секретные ключи k,s, с помощью выражения: $C_2U^{-s}C_1^kU^s=m$

Криптоанализ. Если Ева хочет сломать систему, Ева должна решить задачи преобразования и гибридную задачу, которые сложнее, чем проблема дискретного логарифма в группе той же мощности. BMMC требует трех матричных модульных возведений в степень для генерации ключа. Есть три возведения в степень при шифровании и два возведения в степень при дешифровании. Для ускорения работы алгоритма С.К. Росошек дал две модифицированные схемы, названные MMMC1 и MMMC2 [13]. Обе модифицированные схемы аналогичны, и по этой причине в работе рассмотрена лишь первая.

Алгоритм генерации ключа.

1. Боб вычисляет целое число n, где n может быть либо степенью простого p^r, либо произведением $n=pq$ двух различных простых чисел.

2. Боб определяет две обратимые матрицы $V,W\in GL(2,\mathbb{Z}_n)$, чтобы определить два коммутирующих внутренних автоморфизма α,β кольца $Mat(2,\mathbb{Z}_n):\alpha(D):=V^{-1}DV$ и $\beta(D):=W^{-1}DW$ для всех $D\in Mat(2,\mathbb{Z}_n)$.

3. Боб вычисляет два автоморфизма $\phi:=\alpha^2\beta$ и $\psi:=\alpha\beta^2$.

4. Боб выбирает матрицу $L\in GL(2,\mathbb{Z}_n)$, такую, чтобы $L\notin G$.

5. Боб получает общий ключ $n,\phi(L),\psi(L^{-1})$ и секретный ключ V,W,α,β.

Алгоритм шифрования.

Для реализации шифрования пусть сообщение $m\in Mat(2,\mathbb{Z}_n)$ будет матрицей, тогда:

1. Алиса выбирает $Y\in G$ и определяет внутренний автоморфизм ζ кольца $Mat(2,\mathbb{Z}_n)$ вычисляя $\zeta(D):=Y^{-1}DY$.

2. Алиса вычисляет матрицы $\zeta(\phi(L)),\zeta\left(\psi\left(L^{-1}\right)\right)$ и $m\zeta(\phi(L))$.

3. Алиса вычисляет блок $\gamma \in \square_n$.

4. Алиса вычисляет шифротекст $(C_1, C_2) := \left(\gamma^{-1} \cdot \zeta\left(\psi\left(L^{-1}\right), \gamma \cdot m \cdot \zeta\left(\phi(L)\right)\right)\right)$.

Алгоритм дешифрования.

1. Боб дешифрует сообщение, используя секретный ключ $C_2 \cdot \alpha^{-1}\beta(C_1) = m$.

Криптоанализ. Безопасность схемы основана на проблеме поиска сопряженности "случайной соли". Для заданных матриц A, B в $Mat(2, \square_n)$ необходимо найти обратимую матрицу $X \in GL(2, \square_n)$ и целое число $0 < \gamma < n$, такое что $X^{-1}AX = \gamma B$. Если целое число γ в алгоритме шифрования удаляется, то система небезопасна. Это связано с тем, что обычная задача поиска сопряженности на общей линейной группе $GL(2, \square_n)$ не является сложной. Уравнение $C_1 = Y^{-1}\psi(L^{-1})Y$ может быть преобразовано в систему четырех линейных уравнений с четырьмя неизвестными. С другой стороны, автор [13] утверждал, что “соль” γ может быть найдена только при атаке грубой силы, и для больших n эта проблема становится неразрешимой.

2.3. Схемы на основе группы кос

Впервые группы кос были явно введены Э. Артиным [14]. Существует несколько способов представления кос, но наиболее распространенным является использование генераторов Артина и основной косы [14]. Группы кос (Артина), обозначаемые как B_n , представляют собой группы кос на n нитях, определяемые следующим представлением

$$B_n := < \sigma_1, ...\sigma_{n-1} \mid \sigma_i\sigma_{i+1} = \sigma_{i+1}\sigma_i, \sigma_{i+1}\sigma_i\sigma_{i+1} = \sigma_i\sigma_{i+1}\sigma_i, 1 \le i \le n-1 > .$$

Это неабелевы апериодические группы. Группы кос Артина казались хорошим кандидатом в качестве группы платформ для криптографических приложений благодаря эффективным прикладным вычислениям. В начале XXI века были предложены некоторые криптосистемы с открытым ключом на основе групп кос. Пионерские работы по криптографии на основе групп кос включают схему Аншеля – Аншеля – Голдфельда (AAG) [15] в 1999 г. и Ко–Ли (название для этой схемы составлено из фамилии первого и последнего авторов) [17] в 2000 г. Безопасность наиболее предлагаемых криптографических схем группы кос основывается на задаче поиска сопряженности или ее различных версиях, например на проблеме поиска членства. К сожалению, проблема поиска сопряженности на линейных группах несложна, и группы кос являются линейными группами [16]. Хотя наиболее предлагаемые криптографические схемы на основе групп кос уязвимы для нескольких анонсированных методов атаки [18], исследования групп кос для криптографии не уменьшились. Помимо проблемы поиска сопряженности существуют и другие сложные проблемы в группах кос, которые не были изучены экстенсивно. Поэтому мы рассматриваем работы Ко–Ли, AAG и соответствующие атаки, основанные на линейных представлениях групп кос. Алгоритмы применимы не только к группам кос, но и к любым неабелевым группам.

Схема Ко–Ли.

Пусть LB_k и RB_{n-k} будут коммутирующими подгруппами группы кос B_n , где $0 < k < n$ состоит из кос, сделанных путем заплетения k левых прядей и заплетения $n-k$ правых прядей из n прядей соответственно. Для любых $a \in LB_k$ и $b \in RB_{n-k}$ выполняется правило коммутативности: $ab = ba$.

Схема согласования ключей представлена в [17]: Алгоритм построен по подобию DH.

Общий ключ: группы кос B_n, LB_k, RB_{n-k} и коса $x \in B_n$.

1. Алиса выбирает случайную секретную косу $a \in LB_k$ и посылает Бобу $y_1 := axa^{-1}$.

2. Боб выбирает случайную секретную косу $b \in RB_{n-k}$ и посылает Алисе $y_2 := bxb^{-1}$.

3. Алиса получает y_2 и вычисляет общий ключ $K = ay_2a^{-1}$.

4. Боб получает y_1 и вычисляет общий ключ $K = by_1b^{-1}$.

Схема шифрования представлена в работе [18]:

Публичный ключ Боба x, y , где $x \in B_n, y := axa^{-1}$ и функция хеширования $H : B_n \to \{0,1\}^l$. Секретный ключ Боба: $a \in LB_k$

Шифрование реализуется следующим образом. Пусть $m \in \{0,1\}^l$ исходный текст сообщения.

1. Алиса выбирает случайную косу $b \in RB_{n-k}$.

2. Алиса вычисляет шифротекст (c, d) , где $c = bxb^{-1}$, $d = H\left(byb^{-1}\right) \oplus m$.

Алгоритм дешифрования. Дешифрование реализуется следующим образом. Боб использует простой ключ α для восстановления сообщения $m = H\left(aca^{-1}\right) \oplus d$.

Криптоанализ. Безопасность обеих этих схем основана на проблеме поиска сопряженности на группах кос. Чтобы сломать обе схемы, Еве достаточно решить проблему сопряженности кос Диффи – Хеллмана. Предлагаемый алгоритм решения задачи DH с косой примерно описывается следующим образом. Предположим, что Ева может найти такую матрицу A, что $\mathrm{K}(y_1)A = A\mathrm{K}(y_1)$ и $\mathrm{K}(\sigma_i)A = A\mathrm{K}(\sigma_i)$ для всех порождающих $\sigma_i \in LB_k$. Тогда $A\mathrm{K}(y_2)A^{-1} = A\mathrm{K}(b)\mathrm{K}(x)\mathrm{K}(b)^{-1}A^{-1} = \mathrm{K}(b)\mathrm{K}(y_1)\mathrm{K}(b)^{-1} = \mathrm{K}(K)$. Обратите внимание, что представление Лоуренса – Краммера является точным и можно эффективно найти образ $\mathrm{K}(g)$ для любого $g \in B_n$. Более того, можно эффективно восстановить $\mathrm{K} \in B_n$ из его образа $\mathrm{K}(K)$, используя алгоритм инверсии Чеона – Джуна [19].

Схема AAG

В отличие от Ко-Ли схемы схема согласования ключей AAG не требует коммутирующих подгрупп [15]. Пусть G – публичная неабелева группа и $a_1,...,a_k,b_1,...b_m \in G$ – публичные векторы. Тогда схема шифрования AAG имеет вид:

1. Алиса выбирает случайный секрет $x = x(a_1,...,a_k) \in G$ как слово в $a_1,...,a_k$.

2. Алиса посылает $b_1^x,...,b_m^x$ Бобу.

3. Боб выбирает случайный секрет $y = y(b_1,...,b_m) \in G$ как слово в $b_1,...b_m$.

4. Боб посылает $a_1^x,...,a_m^x$ Алисе.

5. Алиса вычисляет $x\left(a_1^y,...,a_k^y\right) = x^y = y^{-1}xy$ и $x^{-1}(y^{-1}xy) = K$.

6. Боб вычисляет $y\left(b_1^x,...,b_m^x\right) = y^x = x^{-1}yx$ и $\left(y^{-1}(x^{-1}yx)\right)^{-1} = K$.

Криптоанализ. В работе [16] группы кос выбраны в качестве платформы для схемы. Безопасность схемы AAG основана на проблеме множественного поиска сопряженности, которую иначе называют проблемой поиска членства. Однако для того чтобы Ева извлекла общий ключ K из общедоступной информации, достаточно решить задачу коммутатора обмена ключей, которая иначе называется проблемой AAG, за полиномиальное время. Использование метода Чеона и Джуна [19], для уменьшения проблемы коммутатора обмена ключами в матричных группах над полями.

Схема Штикеля.

В 2003 г. Э. Штикель представил алгоритмы подобные решению Диффи – Хелманна [20, 21], основанные на неабелевых группах. Алгоритмы реализуют согласование ключей,

аутентификацию и цифровую подпись. Пусть G – конечная неабелева группа и пусть $a,b \in G$ с условием $ab \neq ba$ и $o(a) = N, o(b) = M > 1$

Схема согласования ключей Штикеля.

1. Алиса выбирает два случайных натуральных числа $n < N, m < M$ и посылает Бобу $u := a^n b^m$.

2. Боб выбирает два случайных натуральных числа $r < N, s < M$ и посылает Алисе $v := a^r b^s$.

3. Алиса вычисляет общий ключ $K = a^n v b^m$.

4. Боб вычисляет общий ключ $K = a^r u b^s$.

Криптоанализ. Предположим, что Ева хочет взломать систему и перехватила значения u и v. Чтобы получить секретный общий ключ K, Еве не нужно находить пару целых чисел (n,m) или (r,s), а необходимо решить задачу поиска декомпозиции, которую можно описать следующим образом. Для рекурсивно представленной группы G две рекурсивно порожденные подгруппы $A, B \in G$ и два элемента $u, w \in G$. Необходимо найти два элемента $x \in A$ и $y \in B$ такие, чтобы $x \cdot w \cdot y = u$, если существует хотя бы одна такая пара элементов. Предположим, что Ева может найти пару $x, y \in G$, которая удовлетворяет системе уравнений

$$\begin{cases} xa = ax \\ yb = by \\ u = xwy \end{cases}$$

Тогда Ева может воспользоваться перехваченным у Боба значением v , чтобы вычислить

$$xvy = xa^r wb^s y = a^r xwyb^s = a^r ub^s = K$$

Предлагаемые платформы: в статье [21] было предложено использовать общую линейную группу $GL_k(\mathrm{F}_{2^t})$ как базовую группу G. Тогда указанная выше система из трех уравнений, включая нелинейное уравнение, может быть приведена к системе из трех уравнений:

$$\begin{cases} x^{-1}a = ax^{-1} \\ yb = by \\ xu = wy \end{cases}$$

Это делает протокол уязвимым для атак с использованием линейной алгебры. Автор статьи [22] предложил полугруппы с большим количеством необратимых элементов. В этом случае атака, использующая линейную алгебру, неэффективна. В то же время, анализ уязвимости к другим атакам не проводился. В связи с этим пока не доказано, делает ли протокол уязвимым использование полугруппы с большим количеством необратимых элементов в качестве основы.

Заключение

Существуют новаторские идеи по предложению криптографии с открытым ключом на основе неабелевых групп, хотя большинство криптографических систем кажутся уязвимыми с точки зрения безопасности. Например, задача поиска сопряженности на линейных группах, используемых в упомянутых протоколах (матричных группах и группах кос), кажется несложной. Тем не менее, они по-прежнему имеют подтвержденную безопасность. Некоторые из этих систем имеют модификации со все еще достаточным уровнем безопасности. С другой стороны, эффективность и безопасность криптографической системы зависят не только от конструкции алгоритма, но и от выбора платформы. Продолжение исследования

неабелевых групп в качестве платформы для постквантовой криптосистемы рассматривается как перспективное.

Список литературы:

1. Shor P. Polynomial-time algorithms for prime factorization and discrete logarithm problems // SIAM Journal on Computing, vol. 26, pp. 1484-1509, 1997.
2. Magliveras S. S. A cryptosystem from logarithmic signatures of finite groups // Proceedings of the 29th Midwest Symposium on Circuits and Systems, pp. 972–975. Elsevier Publishing, Amsterdam, The Netherlands, 1986.
3. Svaba P. and T. van Trung. Public key cryptosystem MST3 cryptanalysis and realizationт // Journal of Mathematical Cryptology, vol.4, no.3, pp.271–315, 2010.
4. Magliveras S. S., Svaba P, van Trung T, et al. On the security of a realization of cryptosystem MST3 // Tatra Mt Math Publ, 2008, 41: 1–13
5 T. van Trung. Construction of strongly aperiodic logarithmic signatures // J. Math. Cryptol., vol. 12, no. 1, pp. 23-35, 2018.
6. Khalimov G., Kotukh Y., Khalimova S. MST3 cryptosystem based on the automorphism group of the hermitian function field' // IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019 – Proceedings, 2019, pp. 865 – 868.
7. Khalimov G., Kotukh Y., Khalimova S. MST3 cryptosystem based on a generalized Suzuki 2 – Groups // CEUR Workshop Proceedings, 2020, 2711, pp. 1–15.
8. Khalimov G., Kotukh Y., Khalimova S. Encryption scheme based on the automorphism group of the Ree function field // 2020 7th International Conference on Internet of Things: Systems, Management and Security, IOTSMS 2020, 2020, 9340192.
9. Wagner N. R., Magyarik M. R. A public key cryptosystem based on the word problem // Advances in Cryptology (CRYPTO'84). Lecture Notes in Computer Science, vol. 196, pp. 19-36, 1985.
10. Yamamura A. Public-key cryptosystems using the modular group // 1st Internationa Workshop on Practice and Theory in Public Key Cryptography (PKC'98), Lecture Notes in Computer Science, vol. 1431, pp. 203-216, 1998.
11. Steinwandt R. Loopholes in two public key cryptosystems using the modular group // Lecture Notes in Computer Science, vol. 1992, pp. 180-189, 2002.
12. Rososhek S. K. New practical algebraic public-key cryptosystem and Some related algebraic and computational aspects // Applied Mathematics, vol. 4, no, 7, pp. 1043-1049, 2013.
13. Rososhek S. K. Modified matrix modular cryptosystems // Britsh Journal of Mathematics & Computer Science, vol. 5, no. 5, pp. 613-636, 2015.
14. Artin E. Theory of braids // Annal of Mathematics, vol. 48, pp. 101-126, 1947. International Journal of Network Security, Vol.20, No.2, PP.278-290, Mar. 2018 (DOI: 10.6633/IJNS.201803.20(2).09) 289.
15. Anshel I., Anshel M., Goldfeld D., Lemieux S. Key agreement, the algebraic eraserTM, and lightweight cryptography // Contemporary Mathematics, vol. 418, pp. 1-34, 2006.
16. Anshel I., Anshel M., Goldfeld D. An algebraic method for public-key cryptography // Mathematics Research Letter, vol. 6, pp. 287-291, 1999.
17. Ko K. H., Choi D. H., Cho M. S., Lee S. J. New Signature Scheme using Conjugacy Problem, 2002. (http://eprint.iacr.org/2002/168)
18. Ko K. H., Lee S. J., Cheon J. H., Han J. W., Kang J. S., Park C. New public key cryptosystem using braid groups // Advances in Cryptology (CRYPTO'00), pp. 166-184, 2000.
19. Cheon J., Jun B. A polynomial time algorithm for the braid Diffie-Hellman conjugacy problem // Advances in Cryptography (CRYPTO'03), Lecture Notes in Computer Science, vol. 2729, pp. 212-224, 2003.
20. Stickel E. A New Public-Key. Cryptosystem in Non-Abelian Groups, 2003. (https: //www.semanticscholar.org)
21. Stickel E. A new method for exchanging secret keys // Proceedings of the Third International Conference on Information Technology and Applications (ICITA'05), pp. 426-430, 2005.
22. Shpilrain V. Cryptanalysis of stickel's key exchange scheme // Lecture Notes in Computer Science, vol. 5010, pp. 283-288, 2008.

Поступила в редколлегию 03.02.2021

Відомості про авторів:

Котух Євген Володимирович – канд. техн. наук, доцент, кафедра комп'ютерних наук, Сумський державний університет, Україна; ORCID: https://orcid.org/0000-0003-4997-620X; e-mail: yevgenkotukh@gmail.com

Сєвєрінов Олександр Васильович – канд. техн. наук, доцент, кафедра Безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, Україна; ORCID: https://orcid.org/0000-0002-6327-6405; e-mail: oleksandr.sievierinov@nure.ua

Власов Андрій Володимирович – канд. техн. наук, ст. дослідник, ст. викладач, кафедра Безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, Україна; ORCID: https://orcid.org/0000-0003-2599-8834; e-mail: andrii.vlasov@nure.ua

Теницька Альона Олексіївна – студентка, факультет електроніки та інформаційних технологій, Сумський державний університет, Україна; ORCID: https://orcid.org/0000-0002-2526-8842; e-mail: tenickajaalena@gmail.com

Зарудна Катерина Олександрівна – студентка, факультет електроніки та інформаційних технологій, Сумський державний університет, Україна; ORCID: https://orcid.org/0000-0002-0653-3030; e-mail: zarudnayakatyaa@gmail.com

РАДІОТЕХНІЧНІ ТА ТЕЛЕКОМУНІКАЦІЙНІ МЕРЕЖІ ТА СИСТЕМИ

УДК 621.3.006.357 **DOI:10.30837/rt.2021.1.204.08**

Ю.Ю. КОЛЯДЕНКО, д-р техн. наук, О.В. КОЛЯДЕНКО, канд. техн. наук, Б.П. МУЛЯР

МЕТОД ОПТИМІЗАЦІЇ РОЗПОДІЛУ ЧАСТОТНОГО РЕСУРСУ З ПОВТОРНИМ ВИКОРИСТАННЯМ ЧАСТОТ ДЛЯ СИСТЕМ КОГНІТИВНОГО РАДІО

Постановка задачі

Провівши аналіз використання радіочастотного спектру, регуляторні органи в ряді країн, зокрема в США і Великобританії, прийшли до висновку, що більша частина спектра використовується неефективно. Використання спектра залежить від місця і часу, і, крім цього, ліцензійні смуги частот не можуть використовуватися неліцензованими користувачами [1 – 6]. Тому використання спектра, наприклад, безпроводовими технологіями, пристроями малого радіусу дії, було дозволено за умови, що вони не створюють завад і не вимагають захисту від пристроїв, що працюють на первинній основі. У пошуках способу підвищення ефективності використання спектра, а також для забезпечення зв'язку, який змінюється в залежності від мережі і потреб користувачів, вирішено було звернутися до систем когнітивного зв'язку, які, як передбачається, будуть працювати, не створюючи завад і не вимагаючи захисту від інших РЕЗ.

Концепція когнітивного радіо може бути охарактеризована як радіо з вивченням можливостей, тобто як радіо, яке в змозі отримати знання про радіосередовище і коригувати свої експлуатаційні параметри і протоколи відповідно. Властивість когнітивності має на увазі здатність радіосистеми вирішувати такі завдання: перехід від одного стандарту до іншого; використання декількох стандартів; перебудову частоти; можливість участі в динамічному розподілі спектру; можливість до вторинного використання спектра; динамічну оптимізацію ємності; регулювання антен; реконфігурацію транспортної мережі [5, 6].

Відмінною особливістю таких систем, зважаючи на мобільність абонентських станцій (АС), є те, що електромагнітна обстановка (ЕМО) – принципово випадкова. Це вимагає статистичного підходу у вирішенні проблеми ЕМС в угрупуванні радіоелектронних засобів.

Будучи системами з многостаціонарним доступом, мережі когнітивного радіо (МКР) використовують всі основні різновиди та методи цього доступу: FDMA – Frequency Division Multiple Access – багатостанційний доступ з частотним розподілом, TDMA – Time Division Multiple Access – багатостанційний доступ з часовим розподілом, CDMA – Coole Division Multiple Access – багатостанційний доступ з кодовим розподілом.

При FDMA використовуються методи частотного розподілу ресурсу в залежності від сигнально-завадової обстановки (СЗО) в каналі зв'язку. Але при такому рішенні завдання ЕМС може виявитися, що частотний ресурс розподілений не оптимальним чином. На етапі функціонування МКР при розподілі частотного ресурсу між АС актуальною є задача мінімізації смуги частот. В умовах постійно зростаючого попиту на смуги частот постановка такого завдання обумовлена необхідністю підвищення ефективного використання радіочастотного спектру із застосуванням методів повторного використання частот (ПВЧ).

В роботі запропонований метод забезпечення ПВЧ, заснований на отриманні оцінок взаємних відстаней між АС в реальному масштабі часу.

Оцінка взаємних відстаней між АС

Для оцінки взаємних відстаней між АС необхідно визначити кути приходу сигналу до базавої станції (БС) від АС, оцінити відстані між БС і АС і визначити координати місця розташування АС.

В роботі [7] запропоновано рекурсивну процедуру оцінки просторового спектра. Переходячи від одного просторового вікна до іншого, ми на кожному переході формуємо нулі

діаграми спрямованості, орієнтовані на інші напрямки приходу сигналів.

Процедура складається з трьох основних рекурсивних складових:

- виділення просторового вікна;
- подавлення сигналів, що приходять з усіх невиділених напрямків;
- рекурсивне визначення позначки відповідності амплітуди і просторової фази в виділеному вікні $P(k,\theta)$, де k – час, θ – кут приходу сигналу.

Оцінка відстаней між АС і БС може бути здійснена декількома способами [8].

У разі розташування АС поблизу БС оцінка відстаней визначається з рівняння передачі:

$$r_i = \frac{\lambda\sqrt{\dfrac{P_{пер\,i}G_{пер\,i}\,G_{пр}}{P_{пр}\eta_{пер\,i}\,\eta_{пр}}}}{4\pi}, \qquad (1)$$

де $P_{пер\,i}$ – потужність передавача i-ї АС; $P_{пр}$ – потужність сигналу, що приймається; $G_{пер\,i}, G_{пр}$ – відповідно: коефіцієнти підсилення передавальної i-ї АС і приймальної БС антен; λ – довжина хвилі; $\eta_{пр}, \eta_{пер\,t}$ - коефіцієнти корисної дії приймального БС і передавального i-ї АС фідерів.

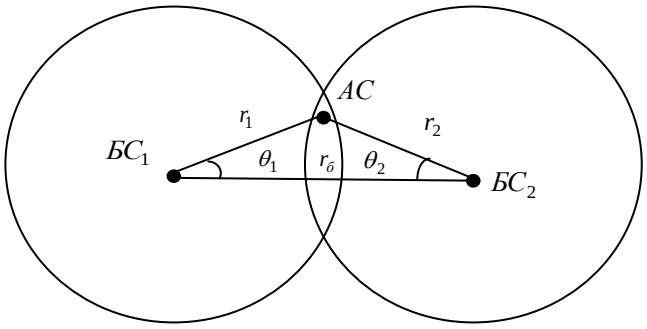


Рис. 1. До задачі визначення відстаней між АС і БС

У разі розташування АС на межі обслуговування базових станцій оцінка відстаней визначається з рівнянь (рис.1):

$$\begin{aligned} r_1 &= r_б \frac{\sin\theta_2}{\sin(180-\theta_1-\theta_2)}, \\ r_2 &= r_б \frac{\sin\theta_1}{\sin(180-\theta_1-\theta_2)}, \end{aligned} \qquad (2)$$

де $r_б$ – відстань між БС; θ_1 и θ_2 – кути приходу сигналу від АС до $БС_1$ і $БС_2$ відповідно.

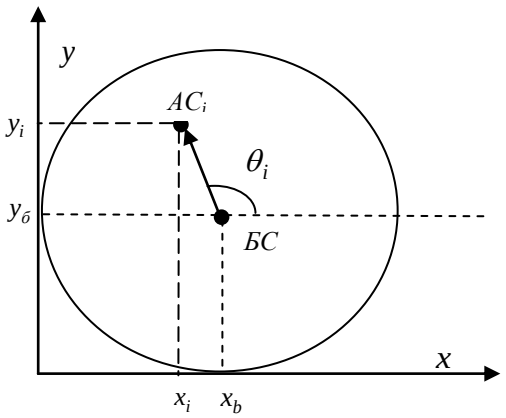


Рис. 2. До задачі визначення координат $АС_i$

Оцінка координат рухомого джерела сигналу $АС_i$ (рис. 2) проводиться згідно з виразами:

$$\begin{aligned} x_i &= x_б + r_i\cos\theta_i, \\ y_i &= y_б + r_i\cos\theta_i, \end{aligned} \qquad (3)$$

де $x_б$, $y_б$ координати БС; r_i – відстань між $АС_i$ і БС; θ_i – кут приходу сигналу від $АС_i$.

Оцінка взаємних відстаней $\|R_{ij}\|$ між АС проводиться згідно з

$$R_{ij} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}, \quad i \neq j. \qquad (4)$$

Метод оптимізації розподілу частотного ресурсу

Задача оптимізації смуги частот формулюється таким чином [8, 9]. Відомо на даний момент розташування в просторі АС в зоні обслуговування БС у вигляді матриці взаємних відстаней $\|R_{ij}\|$, $i, j = 1,2,...,M$. Умови спільного використання АС в зоні обслуговування БС визначаються функцією частотно-територіального розносу (ЧТР), яка при розгляді тільки основних і позасмугових характеристик випромінювання і прийому являє собою монотонно

спадну функцію допустимої розстройки робочих частот АС Δf від їх взаємного видалення R:

$$\Delta f = g(R). \tag{5}$$

Кожній i-й АС потрібно присвоїти робочу частоту $f_i, i = 1,2,..,M$ так, щоб при виконанні умов ЕМС займана ними смуга частот

$$\Delta F = \max_{1 \le i \le M} f_i - \min_{1 \le i \le M} f_i \tag{6}$$

була мінімальною, а її мінімальне значення відповідало б заданій частоті:

$$f_{\min} = 2 f_{cep} - \max_{1 \le i \le M} f_i, \tag{7}$$

де f_{cep} – середнє значення частоти.

За відомою матрицею взаємних відстаней $\|R_{ij}\|$ і заданою функцією частотно-територіального розносу (5) умови ЕМС АС в зоні обслуговування БС можна записати у вигляді матриці допустимих частотних розстроювань між АС $\|\Delta f_{ij}\|$, елементи якої обмежують вибір робочих частот за допомогою співвідношень:

$$\left| f_i - f_j \right| \ge \Delta f_{ij}, \left(\Delta f_{ij} = g(R_{ij}), i, j = 1,2,...,M, i \ne j\right). \tag{8}$$

Тоді математичне формулювання даної задачі можна надати таким чином. В області, яка визначається обмеженнями (7) і (8), необхідно знайти такі значення змінних f_i, при яких цільова функція (6) приймає найменше значення.

В даному випадку умовою локальної оптимальності є те, що робоча частота, яка присвоюється черговій АС, повинна бути найближчою до присвоєної на попередньому кроці частоти за умови співвідношень (8).

Суть цього алгоритму полягає в наступному [9]. Нехай в результаті виконання k кроків алгоритму $\left(1 \le k \le M-1\right)$ маємо такий розподіл частот $0 = f_{v_1} \le f_{v_2} \le ... \le f_{v_k}$, де v_i – номера АС, яким присвоєно частоти f_{v_i} $\left(i = 1,...,k\right)$. Тоді відповідно до умови локальної оптимізації номер v_{k+1} чергової АС на $k+1$ кроці алгоритму визначається зі співвідношення:

$$v_{k+1} = \arg \min_{\substack{1 \le i \le M \\ i \ne v_1,...,v_k}} \max_{1 \le l \le k} \left(\Delta f_{iv_l} - f_{v_k} + f_{v_l}\right), \tag{9}$$

де Δf_{iv_l} – розстройка частот між i-ю АС (станція, якій не присвоєна частота) і v_l АС (станція, якій присвоєна частота); f_{v_k} – частота, яка присвоєна на k-му кроці; f_{v_l} – частота, яка присвоєна v_l-й станції.

Таким чином, визначаються максимальні елементи в кожному стовпці матриці частотних розстроювань $\left(\Delta f_{iv_l} - f_{v_k} + f_{v_l}\right)$ між АС з уже присвоєною частотою і не присвоєною і потім знаходиться мінімальний елемент. Він і визначає номер v_{k+1} чергової АС.

Положення на частотній осі

$$f_{v_{k+1}} = f_{v_k} + \min_{\substack{1 \le i \le M \\ i \ne v_1,...,v_k}} \max_{1 \le l \le k} \left(\Delta f_{iv_l} - f_{v_k} + f_{v_l}\right). \tag{10}$$

В якості початкової точки вибирається довільний номер АС. Для виконання умови задачі оптимізації смуги частот необхідно всі отримані частоти збільшити на $f_{\min}$, що не порушить виконання співвідношень (8).

Структурна схема алгоритму розподілу частотного ресурсу надана на рис.3.

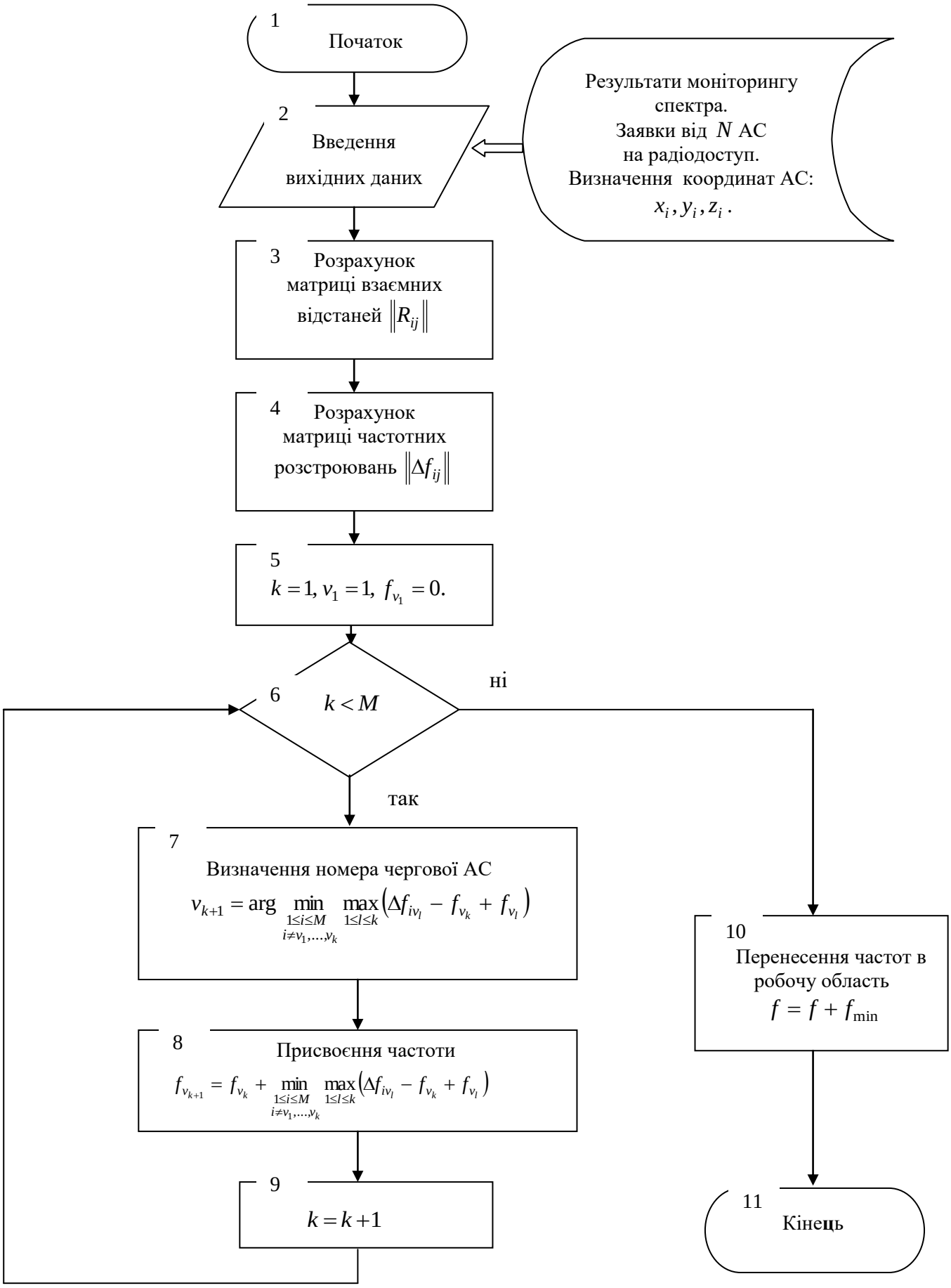


Рис. 3. Структурна схема алгоритму розподілу частотного ресурсу з повторним використанням частот

Аналіз ефективності методу оптимізації розподілу частотного ресурсу

Для аналізу ефективності методу оптимізації розподілу частотного ресурсу використано мережу LTE. Мережі LTE використовують технологію OFDM. Вилучення заборонених частот із загальної смуги частот мережі відбувається наступним чином. Символ OFDM – це група піднесійних частот, яка в даний момент переносить біти паралельних цифрових потоків. Комплексна огинаюча одного OFDM-символу тривалістю T, який починається в момент часу $k\Delta t$, має вигляд [14]:

$$\dot{U}_{ck} = \dot{U}_c(k\Delta t) = \frac{1}{N}\sum_{i=0}^{N-1}\dot{U}_i e^{jik\frac{2\pi}{N}}, \qquad (11)$$

де $\dot{U}_i$ – комплексний символ, який визначає амплітуду і початкову фазу i-ї піднесійної OFDM-сигналу; N – число піднесійих в OFDM-символі.

У разі, коли відомо, на яких частотах не можна вести передачу даних в мережі, треба вилучити випромінювання на цих частотах, попередньо перерахувавши, які піднесійні збігаються з забороненими частотами. Якщо потрібно вилучити випромінювання на i-й частоті мережі, то при формуванні OFDM-символу потрібно $\dot{U}_i$ прирівняти до нуля. Рознос між піднесійними частотами становить 15 кГц.

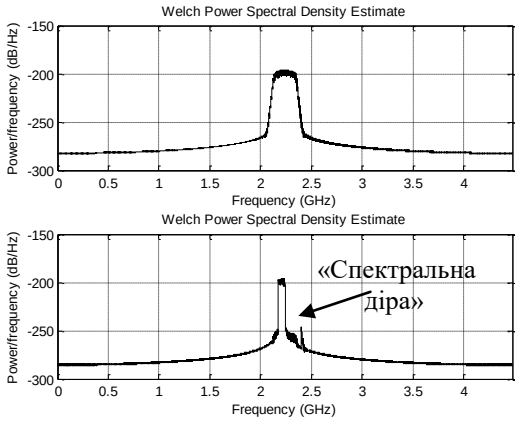


Рис. 4. Результат моніторингу спектра мережі LTE

Для оцінки ефективності алгоритму (10) проведено обчислювальний експеримент на ЕОМ. Нехай в результаті моніторингу спектра не зайнятою смугою частот виявилася смуга від 2,25 ГГц до 2,5 ГГц виділена для передачі АС в напрямку БС. Смуга в межах від 2,1 ГГц до 2,2 ГГц виявилася зайнятою. Таким чином, в діапазоні від 2,25 ГГц до 2,5 ГГц з'явилася так звана «спектральна діра». Результати моніторингу надано на рис. 4. Вгорі на рис. 4 відображена повністю зайнята смуга.

Для математичного моделювання координати розташування АС вибиралися випадковим чином за гаусівським законом розподілу. Приклад розташування АС показано на рис.5.

Розрахунок матриці взаємних відстаней $\|R_{ij}\|$ між АС проводився згідно виразу:

$$R_{ij} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2 + (z_i - z_j)^2},$$

де x_i, y_i, z_i – координати розташування i-ї АС.

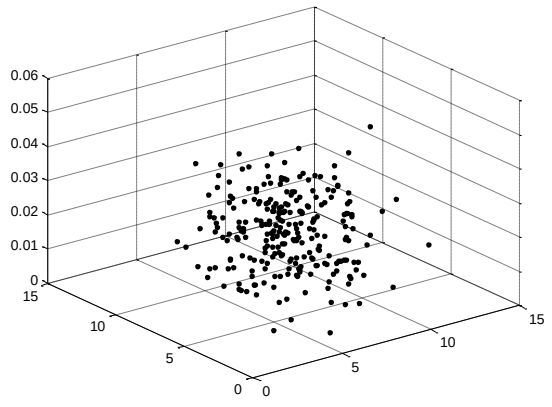


Рис. 5. Розташування АС в зоні обслуговування БС мережі LTE

Матриця допустимих частотних разстроювань формувалася за допомогою матриці взаємних відстаней $\|R_{ij}\|$ і функції частотно-територіального рознесення:

$$\Delta f_{ij}(d) = \begin{cases} 15\ кГц, & 0 < R_{ij} < 0.2\ км; \\ 6\sqrt{\dfrac{0{,}25}{d_{ij}^{\,2}} - 1}\ кГц, & 0{,}2 \le R_{ij} < 0{,}5\ км; \\ 0, & R_{ij} > 0{,}5\ км. \end{cases} \quad (12)$$

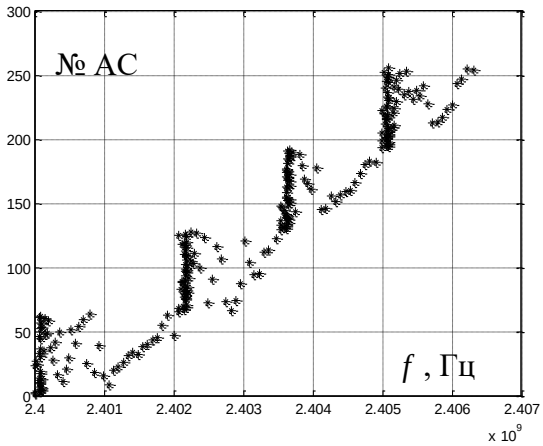


Рис. 6. Результат присвоєння частот АС мережі LTE

Відповідно з розглянутим алгоритмом і функцією частотно-територіального рознесення, розташованих випадковим чином АС в просторі (рис. 5), проведено розподіл частотного ресурсу між АС в діапазоні від 2,5 до 2,5072 ГГц з відповідним присвоєнням їм частот.

Приклад такого присвоєння частот показано на рис. 6. При цьому, як видно з рис. 6, в межах вільного частотного діапазону виділено 256 додаткових каналів, що дозволяє значно збільшити кількість АС, що обслуговуються.

На рис. 7. надана залежність ширини смуги частот від кількості обслуговуваних абонентських станцій мережі LTE. Верхня крива на даному рисунку відповідає випадку розподілу частотного ресурсу без використання запропонованого методу, а нижня крива – з використанням методу повторного використання частот. При цьому як видно з рис. 7, при розподілі частот між 64 АС смуга частот зменшується на 2,6623 МГц. При розподілі частот між 128 АС смуга частот зменшується на 5,2996 МГц. При розподілі частот між 192 АС смуга частот зменшується 9,0163 МГц. А при розподілі частот між 256 АС смуга частот зменшується на 11,92 МГц. Таким чином, можна зробити висновок про те, що з ростом числа одночасно обслуговуваних АС ефективність методу підвищується.

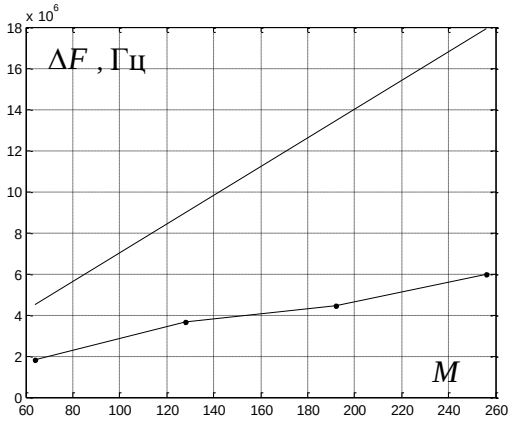


Рис. 7. Залежність ширини смуги частот ΔF від кількості абонентських станцій M мережі LTE

Висновки

Запропоновано алгоритм розв'язання задачі оптимізації розподілу частотного ресурсу для мережі когнітивного радіо з повторним використанням частот. В основі алгоритму лежить метод локальної оптимізації – один з наближених методів дискретного програмування. В даному випадку умовою локальної оптимальності є те, що робоча частота, яка присвоюється черговій АС, повинна бути найближчою до присвоєної на попередньому кроці частоті.

За допомогою імітаційного моделювання проведено аналіз ефективності алгоритму оптимізації розподілу частотного ресурсу для мережі LTE. Отримано залежності ширини смуги частот від кількості АС, що обслуговуються. Аналіз показав, що використання даного алгоритму дозволяє в два-три рази скоротити смугу частот. Також можна зробити висновок про те, що з ростом числа АС, які одночасно обслуговуються, ефективність алгоритму підвищується.

Список літератури:

1. Tafazolli R. (ed) (2006): Technologies for the Wireless Future, volume DOI:https://doi.org/10.1002/0470030453

2. Wireless World Research Forum, (WWRF), John Wiley & Sons, Chichester, England. 2. Burns P. SDR For 3G. Boston, Artech House, 2003. 279 p.

3. Haykin S. Cognitiveradio: brain-empowereswirelesscommunications // IEEE Journal Selected Areasin Communication, vol. 23, no. 2, February 2005. DOI:https://doi.org/10.1109/JSAC.2004.839380

4. Стандарты ETSI TR 102 682 V1.1.1 (2009-07), ETSI TR 102 683 V1.1.1 (2009-09), ETSI TR 102 745 V1.1.1 (2009-10), ETSI TR 102 838 V1.1.1 (2009-10).

5. Mitola J. III and Maguire G.Q. Cognitive radio: making software radios more personal // IEEE Personal Communications. Vol. 6. No. 4. Aug. 1999. P. 13–18. DOI:https://doi.org/10.1109/98.788210

6. Mitola J. III. Cognitive Radio for Flexible Mobile Multimedia Communications // Mobile Multimedia Communications (MoMuC'99). IEEE International Workshop, San Diego, CA, USA, Nov. 1999. P. 3–10.

7. Коляденко Ю.Ю. Рекурсивная процедура оценки пространственного спектра сигналов в задачах управления базисом наблюдения для сотовых систем связи // Радиотехника. 2004. Вып. 138. С. 20 -24.

8. Коляденко Ю.Ю. Оптимизация распределения частотного ресурса в системах сотовой подвижной связи // Праці УНДІРТ. Теоретичний та наук.-практ. журнал радіозв'язку, радіомовлення і телебачення. 2005. № 3 (43). С.80-85.

9. Поповский В. В. Метод обеспечения электромагнитной совместимости при когнитивном распределении частотного ресурса в мобильных системах связи / В. В. Поповский, А. В. Коляденко // Вісник Нац. ун-ту "Львівська політехніка". Сер. "Радіоелектроніка та телекомунікації". 2017. №874. С. 25–30.

Надійшла до редколегії 05.02.2021

Відомості про авторів:

Коляденко Юлія Юріївна – д-р техн. наук, професор, професор кафедри інфокомунікаційної інженерії імені В.В. Поповського, Харківський національний університет радіоелектроніки, Україна; e-mail: yuliia.koliadenko@nure.ua; ORCID: https://orcid.org/0000-0002-0247-2736

Коляденко Олексій Вадимович – канд. техн. наук, iOS Software Engineer, ФОП Коляденко, Україна; e-mail: kolyadenko.kks@gmail.com; ORCID: https://orcid.org/0000-0001-6374-1664

Муляр Богдан Петрович – аспірант кафедри інфокомунікаційної інженерії імені В.В. Поповського, Харківський національний університет радіоелектроніки, Україна; e-mail: bohdan.muliar@nure.ua; ORCID: https://orcid.org/0000-0002-2204-7091

UDC 355.457.2:358.11.6 (043.3) **DOI:10.30837/rt.2021.1.204.09**

M. YERMOSHYN, A. POBEREZHNYI, O. ONOPRIYENKO, M. SHURYHA

ARCHITECTURE OF NETWORK KNOWLEDGE BASE OF A COMPLEX MILITARY SYSTEM

Introduction

Problem statement. A complex military system in modern conditions should have a synergistic effect of interaction between components and elements in a conflict environment, taking into account the adaptability to the conditions and state of the troops in the following main areas [1, 2, 12]:

– a single methodological approach to build the organizational structure of the military system with a network knowledge base is using of modern special software, mathematical models and problems to support real-time management decisions, creating all levels of a single background;

– ensuring the adequacy of forces to perform the task as assigned, the coordination of actions of the forces with information and technical compatibility of the elements of the system (units), the elimination of tasks duplication and management functions in the group of troops;

– building the organizational structure of the military system with a network knowledge base during the transition to the states, systematization of knowledge, experience and development of leaders' thinking, organization of information and psychological struggle, ensuring timely response to changes and possible stressful circumstances during hostilities, increasing timeliness forces due to the maneuver, ensuring the balance of time to develop a plan of action in terms of their ephemerality, uncertainty and difficulties of a comprehensive assessment of the situation, its' generalization, etc**.**

Analysis of scientific research and publications.

In [1] the synthesis of adaptive structures of systems of anti-aircraft missile and artillery cover of military objects is considered, which is reduced to search of structure of components and elements of system and communications between them through network mathematical models which realization allows to satisfy the established requirements to efficiency of functioning of difficult organizational military systems with known resource constraints, etc.

Theoretical foundations of formation and degradation of complex organizational and technical systems [2] provide a description of this system without components, and in [4, 12] there is a problem of synthesis of the structure of a complex organizational system of military purpose and properties, but the knowledge base is not considered.

In [3] the basic concepts of the theory and practice of the Armed Forces of Ukraine on armed struggle in air and space, the basic definitions of a complex system, but not all terms of properties are used in the sense in which they are laid, new approaches to the analysis of properties and synthesis of the organizational structure of complex systems.

The architecture of the subject-oriented knowledge base of the intelligent system [5] is the knowledge base as the basis of any intelligent system. This is primarily due to the fact that the data model embedded in the knowledge base should be easily integrated with the data model embedded in the system itself. Most often, these models coincide. The knowledge base is considered as a set of software that provides search, storage, conversion and recording in memory of complex structured information units (knowledge). In general, the architecture of an intelligent system can be represented as an interface of user interaction with the knowledge base.

The ontology of design is provided in [6] on the construction of a model of the subject area by probing the service Google Scholar Citations

In [7] the representation of knowledge in the information system and methods of artificial intelligence and knowledge representation are considered, the basic concepts of artificial

intelligence and knowledge representation, various methods, basics of Prolog language, descriptions of OntoStudio and MatLab packages for solving problems and cluster analysis.

In [8, 9] the basic concepts of artificial intelligence and knowledge representation, various methods, basics of Prolog language, descriptions of OntoStudio and MatLab packages for solving problems are described, the textbook description presents a systematic presentation of the basics of knowledge representation theory in artificial intelligence systems. The description of the most significant currently models and technological aspects of designing systems based on knowledge is given. Particular attention is paid to the problems of knowledge engineering, and as the main approach to their solution is the author's method of situational analysis and design of the model of the subject area (knowledge base), but insufficient attention is paid to the network knowledge base.

In [10, 11] provided artificial intelligence systems as models, methods and technologies based on knowledge, artificial intelligence as the basis of future control networks regarding the use of computer technology, she believes, has already led to a huge number of unfinished design decisions digital systems. Opposing techno-chauvinism and social illusions about the saving role of technology. Only by understanding the limits of computer technology will we be able to dispose of them in such a way as to make the world a better place.

The unsolved part of the general problem concerning the knowledge base of a complex system of military purpose is the construction of the architecture of the network knowledge base in the subject area of militar arts, to which this article is devoted.

The research aims and objectives: to provide an interpretation of the basic concepts of the architecture of the network knowledge base and the construction of the organizational structure of a complex military system.

Statement of basic materials

In modern conditions, the greatest influence on the change of forms and methods of hostilities, globalization and implementation of the results of the scientific and technological revolution have tendencies of information and psychological struggle, ensuring timely response to changes in combat and possible stressful circumstances in complex military systems.

The military system consists of components and elements.

Components of the military system are its subsystems: fire, intelligence, control, engineering, technical support, etc.

Elements of the military system are military formations, with their capabilities for specific conditions.

The assessment of the effectiveness of the functioning of a complex organizational system for military purposes is carried out taking into account three axioms: at first, weapons and military equipment have certain tactical and technical characteristics; secondly, military formations have appropriate combat capabilities; thirdly, the military system has its own properties (synergy effect, hierarchy, emergence, efficiency and stability, adaptability, operational readiness, communicativeness, secrecy, reflectivity, validity, continuity, rationality, controllability, etc.) [2, 4, 12].

Tactical and technical characteristics of armaments, combat capabilities of military formations, properties of the military system are characterized by indicators, criteria and standards.

A complex system of military purpose is a set of interacting, simultaneously functioning components and elements built according to a single conception and plan, each of which performs one or more functions when military formations perform assigned tasks.

For the description and formalization, the complex military system is presented as [4, 14]

$$S = S\left(C, I, E, A^{i}, A^{ie}, A^{ei}\right),$$

where $C = \{C_1, ..., C_k\}$ – the set of components S;

$I = \{I_1, ..., I_p\}$ – the set of internal elements S;

$E = \{E_1, ..., E_q\}$ – the set of external elements S;

A^{i} – relations of elements (internal structure S);

A^{ie}, A^{ei} – relations between the elements (the structure of the links between the internal and external elements of S and vice versa).

At the present stage, the purpose of creating a military system is to ensure the effective use of groups of troops (forces) within a single system, regardless of their departmental affiliation and the rational use of existing resources.

The structure of the military system is the mutual location of its elements and the set of connections and relations between them, ensuring the integrity of this system and the ability of formations to perform tasks taking into account the basic properties of interacting subsystems and elements according to conditions and forces (Fig. 1) [1, 2, 8].

The input data of the system include data on external influence and management (A^{ei}, A^{i}). Management data correspond to commands to change the values of structural parameters to change the combat task of a group of troops, for example, commands to change the positions of units, teams to change the objects of cover, etc. Data on external influence on the military system include, for example, the values of the parameters of the preliminary reconnaissance of the composition and condition of the enemy, the values of the parameters of the enemy's strike, and others.

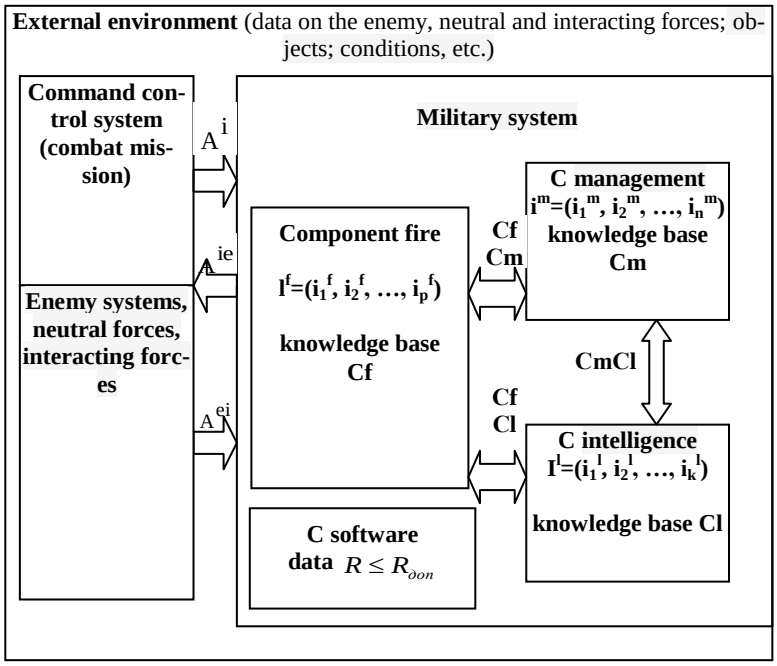


Fig. 1. Block diagram of a complex military system

To the initial data of the military system (A^{ie}) include, for example, the values of parameters for the effectiveness of hostilities, the structure of the system, etc.

The fire system as the main element of the structure is characterized by a set of values of indicators (spatial, temporal, probabilistic) $i^f = (i^f_1, i^f_2, \ldots, i^f_p)$, which determine both its structure and state parameters. Construction of the fire system is achieved by deploying elements of a group of troops in combat order.

The components of the fire system are the realized fire zones of the units located on the battle positions. Therefore, the structural parameters include the characteristics of the weapons in service (i^f_1), the coordinates of the main and reserve positions of the units (i^f_2), the area of fire (i^f_3), and others. A fair assumption about the inclusion of environmental parameters in the internal parameters of the fire system. For example, the terrain can be taken into account in the characteristics of the

weapon (i^f_1) in the form of a realized zone of fire for the entire spectrum of altitudes, and weather conditions in the form of the attenuation coefficient of radio waves and others.

Virtually all parameters of fire, intelligence and control systems should be determined by indicators that can be deterministic or stochastic.

Evaluation of the effectiveness of a complex military system and its components based on the results of modeling the actions of the parties creates a number of problems in terms of non-stochastic uncertainty of the parameters of the situation and actions of different parties, consisting of two classes: analysis tasks; problems of synthesis of the structure of a complex system (component).

When creating the structure of the system should be guided by the principles, among which it is possible to distinguish general and specific [3].

Thus, even in one subject area there are a large number of tasks on the elements of the military system that require the development and application of mathematical models. However, solving these problems encounters a number of serious difficulties. First, these tasks are solved at different times by different organizations and institutions. Second, often even in one organization, different tasks in the same subject area are solved using different models. Third, a single methodological approach to building the organizational structure of a military system with a network knowledge base is often impossible even in a group of troops.

To eliminate these contradictions, it is necessary to solve interdependent problematic issues: to develop tools for a military system with a network knowledge base, focused on a particular class of methods; to develop sufficiently universal models, with the help of which it is possible to solve all or at least most of the problems in one or another subject area and to achieve their approval as industry standards; develop specialized models to solve individual problems that provide an estimation of all or part of the input parameters of the universal model.

This technology of construction and evaluation of the effectiveness of a complex military system with a network knowledge base avoids existing shortcomings, and most importantly, can significantly increase the adequacy of models and tasks, consistency and effectiveness of decisions.

Knowledge base is a special kind of database designed to manage knowledge (metadata), ie the collection, storage, retrieval and dissemination of knowledge. Knowledge-based systems are implemented on the basis of the following intelligent algorithms: expert systems; neural networks; fuzzy logic; genetic algorithms [5, 11, 12].

Expert systems are considered together with knowledge bases as models of behavior of experts in a certain area of knowledge using the procedures of logical inference and decision making, and knowledge bases – as a set of facts and rules of logical inference in the chosen subject area of heuristics activity.

The main task of heuristic activity is to build models for the process of finding a new problem for a given object (phenomenon, process). There are different types of such models, among them are some options: the model of blind search, which is based on the method of trial and error; the labyrinth model in which it is possible to solve a problem is considered as a labyrinth, and process of search of the decision – as wandering on a labyrinth; structural-semantic model, which is based on the fact that the basis of heuristic activities for solving the problem is the principle of building a system of models that reflects the semantic relationships between the objects included in the problem [5, 7, 8].

The most well-known class of such programs are expert systems designed to find ways to solve problems in a particular subject area, based on knowledge base records and a user-defined description of the situation. Simple knowledge bases can be used to create expert storage systems in the organization: documentation, manuals, technical support articles.

The main purpose of creating a knowledge base of the military system – to help the commander to find an existing description of the method of action of units (strategy) to determine the design of hostilities in any difficult situation.

Regarding such a model, the knowledge base should solve the problem: search for the necessary information to the commander (both embedded in the database and indirect information derived from

existing); transformation of the received information into a model of knowledge used within the intellectual system of military purpose and interacts with the knowledge base as an interface of interaction of the commander with the knowledge base; timely updating of knowledge inside; maintaining the integrity and adequacy of information on the implementation of combat missions by assigned units.

Such a subject area of the knowledge base of the military system can be provided in the form of a subject-oriented model, which is based on the fact that the algorithm of logical-analytical activities of the commander and the principle of building network models to support decisions on combat or other decisions that significantly affect to perform a combat mission.

Research and modeling of the management process show [1, 3, 4, 12] that the decision support process should be considered consistently in the form of image of the process: plan-schedule; algorithm; network schedule; network model.

When developing the algorithm of logical-analytical activity of the commander and the staff, the following features are taken into account: this algorithm must correspond to the general system approach to the preparation and conduct of hostilities; the algorithm is divided into separate logical-analytical, informational and computational problems, the solution of which determines the order of application of automation tools, models, methods; the algorithm should be implemented programmatically.

The construction of network schedules for decision support is a continuation and detailing of the algorithm of the commander and staff by determining the required and available time of their work and units that have random values. The network schedule corresponds to the sequence of tasks and functions of management of officials.

To graphically describe the network model, we will use the following notation "goals" and "relationships" (Fig. 2) [1].

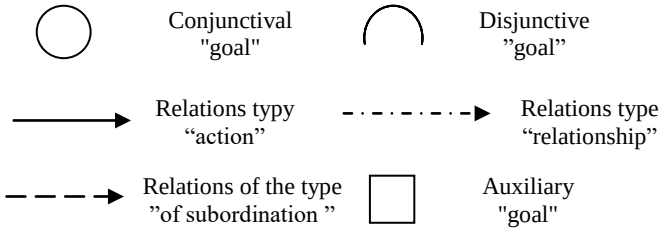


Fig. 2. Graphical notation of "goals" and "relationships" of the network model

An example of a mathematical network model to support combat decisions is given in [1].

The network model in the form of defined "goals" and "relationships" most fully reflects the order of the governing bodies when deciding on hostilities and other activities. It can be informationally detailed according to the stages of this activity of officials on the tasks, the solution of which is assessed by partial indicators of importance, reliability, completeness, accessibility, detailing of information.

In general, the architecture knowledge base of the intelligent military system can be represented as the interface of interaction of the C-commander (E-expert, O-operator) with the network (Fig. 3).

The internal imagination of knowledge in the knowledge base (formal program-logical content) should be implemented in the form of a matrix of contiguity, reflecting the relationship and interconnection between the target institutions, as well as a set of such directories [1]:

– catalog of target installations (CTI);

– catalog of initial conditions (CIC);

– catalog of resources (CR) of groups of troops (time, material, combat and quantitative composition) used, their costs and replenishment;

– catalog of rules of resource consumption (CRC) and the choice of criteria for their allocation in the process of use.

When replenishing the knowledge base, it is advisable to control the correctness of the changes, their compliance with the concept laid down in meta-knowledge, control the contradictions with the existing structure of target settings. Extraction of knowledge from the knowledge base is carried out by the algorithm of logical inference in the process of synthesis of the system structure during decision making and the algorithm of comments (explanations) when disclosing logical and factual premises, on the basis of which these recommendations are formed.

The composition and relationship of all formal and logical means of knowledge base to support decisions on the preparation and conduct of hostilities are shown in Fig. 3 [1, 3].

The structure of the knowledge base is a three-dimensional array of matrices, each plane of which corresponds to one of the above directories. It is advisable to define the following arrays corresponding to the directories:

– matrix of relations between target installations with initial conditions;

– matrix of resources used;

– matrix of compliance with the rules of resource consumption and the choice of criteria for their allocation.

Separating the relationship between initial conditions and target settings in different matrices may initially seem illogical, as they are inextricably linked and form a single integral network, but in the process of logical inference with time constraints, this can significantly reduce the dimension of the problem and time.

The size of the adjacency matrix is determined by the number of vertices (target installations) of the mathematical network model of making decisions on the preparation and conduct of hostilities and the initial conditions that determine the achievement of target installations.

Matrix elements are sets that consist of indices of the corresponding elements, which reflect the relationship and relationship between "goals" according to their numbering in the catalogs. If it is necessary to extract knowledge from the knowledge base, sampling is performed from the appropriate directories according to the indices contained in the elements of the sets.

Replenishment of knowledge (or their correction) is carried out by adding formalized knowledge to the appropriate catalog, changing (if necessary) the dimensionality of the adjacency matrix and establishing the relationship between new "goals" by filling (changing) in the specified matrix of relevant elements.

The initial synthesis of a mathematical network model of knowledge is carried out using synthesis procedures. The theoretical basis for constructing such procedures is the search for a guaranteed strategy.

Directly related to the knowledge base is a group of algorithms for its management [1]: examination, synthesis of a mathematical network model for making decisions on the preparation and conduct of hostilities, control of the correctness of the knowledge base, preparation of source information.

This set of algorithms is used only at the stage of replenishment (correction) of the knowledge base by the officer-programmer, and in the process of combat operation does not participate.

The expertise is designed to organize a dialogue with experts on the preparation and conduct of hostilities and the transformation of information in the process of replenishing the knowledge base.

Tasks to be solved: organization of dialogue with experts in the process of replenishing the knowledge base; transformation of information from the language of communication with experts into the internal language of formalization of the knowledge base; transformation of the received regularities into target installations, initial conditions, relations, rules of use of resources.

The basis of the examination algorithm is a natural language interface that transforms from a limited natural language of communication into the internal language of the expert system. The natural language interface consists of a linguistic processor and a knowledge base about the language of communication [1].

The linguistic processor is provided by modules of the corresponding analysis of the entered information. These is word processing module, morphological analysis module, parsing module,

semantic analysis module, internal image synthesis module. Modules have both semantic and grammatical information about individual semantic component situations for decision making.

Ultimately, the expertise algorithm provides the formation of binary relations between the vertices that characterize a certain state of the system for publication by their expert. The expert approves or rejects the presented relations or forms a new state of the system, which are not included in the catalog. Interaction is carried out by means of the corresponding menus. The given order of functioning actually provides realization of functions which structure can be given by special modules of separate word forms for experts concerning situations of decision-making.

Synthesis of a mathematical network model of decision making will provide a change (correction) of the structure of target settings while replenishing the knowledge base.

Tasks to be solved: selection of vertices and relations from the set of generalization information with experts while replenishing the knowledge base; replenishment of knowledge base catalogs; making changes to the adjacency matrix in accordance with the newly discovered or changed relationships between the target settings.

The formation and transformation of the structures of the target settings allows you to reasonably determine or significantly supplement the structure of the target settings of the system using which the decision is made. A necessary element of the synthesis of a mathematical network model for making decisions on the preparation and conduct of hostilities is to build a structure of target systems of the system for a specific situation.

The following principles are the basis for building mathematical network models for making decisions on the preparation and conduct of hostilities (establishment of binary relations between target installations), which characterizes the actions of management bodies, etc.: purposefulness; massaging resources; maneuverability; unity of management; security; secretiveness; simplicity of design.

Based on an expert survey, a catalog of target settings is compiled and the essence of the relationship between them is clarified. The synthesis of a mathematical network model for making decisions on the preparation and conduct of hostilities begins with a state, the achievement of which ensures the achievement of the ultimate "goal", ie with the "goals" of the highest level of the hierarchy. The synthesis of structures of target installations is carried out until the required level of specificity is reached, ie until the target installations are reached, the conditions for achieving which are only the initial conditions. The truth of the initial conditions can be determined by solving a finite set of calculation problems or on the basis of information from a combat service person.

The theoretical basis of the means of formalizing the synthesis problem is a mathematical apparatus that allows to establish the truth of the relationship between the target settings and to describe the structure of the network model itself. The target settings are divided into conjunctive, disjunctive, conjunctive and disjunctive achievable. As a result of these actions, we obtain the structure of target installations for making decisions on the preparation and conduct of hostilities for the initial conditions.

Building the structure of target installations, making decisions on the preparation and conduct of hostilities is carried out with the help of formal rules by transforming the structure of target installations. The transformation of the structure of the "goals" of the management process begins with the "goals" of the highest level of the hierarchy and is carried out sequentially until the target settings are reached, which are determined only by the initial conditions. At the same time there can be a situation when as a result of the specified transformations the necessary level of concreteness is not reached. In this case, further construction of the structure of target installations to make decisions on the preparation and conduct of hostilities is carried out on the basis of searching for fragments of the structure of target installations in the catalog, describing the dynamic qualities of the process.

The described technique is valid for the initial formation of structures of target installations at the stage of system creation. In the process of functioning of the expert system at change of structure of knowledge base only correction of earlier created structure of target installations is carried out.

Control of correctness of knowledge base is carried out at replenishment of knowledge base: detection of contradictions in structure of target installations at modification of this structure; search and detection of contradictions of the semantic network graph according to the available resources and time; checking the completeness of the graph of the mathematical network model; issuance of identified contradictions to the expert and their elimination. The peculiarities of the control of the correctness of knowledge, provided in the form of target settings, is the need for a joint analysis of the whole set of target settings and the initial conditions in their relationship. To do this, you combine the target relationship matrix and the initial condition relationship matrix.

Detection of contradictions in the structure of target installations in the construction of a mathematical network model, its structure determines the nature of the relationship between target installations and the presence of contours on the graph of the network model, which is evidence of incorrect model and leads to a clear contradiction. The search for the contours of the mathematical network model is carried out by summarizing a generalized matrix of adjacency of target settings and initial conditions.

Checking the completeness of the graph of the mathematical network model consists of detecting "hanging" vertices and their correction. The definition of "hanging" vertices is reduced to checking the presence in the generalized matrix of adjacency of the network model of zero columns. Possible variants of the "hanging" vertex x_i are disjunctive, conjunctive or initial condition.

Checking the correctness of a mathematical network model according to resources and time in the process of achieving a "goal" can reveal a situation where resources are not enough to simultaneously perform certain actions. Control of the correctness of the network model according to resources and time is reduced to identifying options for achieving "goals", which meet the following conditions: the intensity of consumption of each type of resource does not exceed the set value without contradiction of the states of contractors; the total cost of each type of resources in the process of achieving "goals" does not exceed the established value; the available time to achieve the "goal" should not exceed the required time.

The definition of the initial conditions is to determine their truth, which determines the possibility of achieving the appropriate target settings.The connection of the algorithm for determining the initial conditions is carried out periodically by the algorithm-dispatcher according to predetermined parameters, which in the process of combat operation of the system can be quickly changed.In order to reduce the amount of computing resources used for the definition, all procedures for determining the initial conditions are divided into three groups:

– models of representation of knowledge in the form of calculation of predicates and statements, calculation and information problems, the results of which are used repeatedly for specific operational and tactical situations. Tasks of this class use the initial data which arrive both in the form of results of the decision of problems of management process, and those which arrive by communication channels from external sources of information;

– or are connected once as necessary, the results of which are used once. In this case, the information for the definition comes as a result of solving the problems of the management process, or from automation, if such procedures of the management process are not available;procedures for determining the initial conditions, the source information which is the operational information of combatants, are not present in the communication channels of automation, which is introduced immediately after receiving it. After entering such information, the connection and initialization of decisions (tactical tasks), for which it is the source.

The definition procedures are reduced to a catalog that is formed at the development stage. Adjustment of this catalog is carried out at the stage of exploitation.

The formal and logical content of the procedure for determining the initial conditions is reduced to a separate software module, which is performed on a modular basis. The connection of the corresponding definition procedures is carried out by the algorithm-dispatcher from the set of features of the source information in accordance with the above classification and the form of these procedures from the catalog. The form defines the list of features that at the same time are the implementation of the rule of choosing the procedure of the definition to be solved.

Definition procedures are multi-purpose and are used both independently in solving partial problems and to ensure the proper functioning of the intelligent system.

The database is an integral part of the system database using elements of intelligence designed to store, replenish and retrieve data that are the source for solving partial management problems and used in the process of logical inference and comment when receiving requests to the intelligent system.

A database is a set of data arrays and software modules that allow you to manipulate data (perform their replenishment, storage and production) in accordance with the concept, such as a relational database, which provides the following tasks: receiving information interactively from combat service personnel and from sources of information in automatic mode; recording and storing the received information in the form of recording on hard media; recording and storing information, which is repeatedly used in the process of solving computational problems, in database arrays stored in RAM; search and retrieval of information by key; issuing information grouped in accordance with the received request (key) in the form of arrays, or sequentially with the discreteness specified in the key; review of the content of data sets according to the granting of relevant rights (authorized access); organization of priority access when receiving requests for data issuance.

Input and output information to replenish the database can come in two ways: through an interactive dialogue of combatants using the procedures provided by the database management algorithm; from automation tools and external sources and other consumers.

In the process of accessing the database, a number of conflicts may occur, which are determined by the impossibility of simultaneous answering of questions by several consumers and the impossibility of simultaneous writing and reading: conflict between data consumers in the process of simultaneous access to the database; conflict between sources of information in the process of recording data while accessing the database; conflict between sources and consumers of information while accessing the database.

The concept of building a database is based on the image of its logical structure in the form of sets of two-dimensional tables with the following properties: each element of the table represents one data element, repeating groups are absent; the elements of each column are instances of one concept; columns have names; there are no two identical terms in the tables; rows and columns of tables can be viewed in any order and in any sequence, regardless of their information content.

The peculiarity of the database is its functioning in the following time modes: real-time mode - replenishment of the database from communication channels of information sources and automation tools, data issuance to programs operating in this mode; time allocation mode - when replenishing the database from workplaces or viewing reference tables.

Certain data sets, which are repeatedly used in solving computational problems, have high requirements for the speed of sampling (issuance) of information stored in them. Such arrays are placed in RAM when the system is initialized.

The group of tables of structures and connections includes the following: tables of structures; entry connection tables; extension link tables [4, 5].

Structure tables contain information about the classes of structures in the system: objects, connections, processes, conditions and properties. These structures were selected based on the analysis of configuration modeling methods and model data representations.

These structures will allow you to fully describe all the main components of the existing model representations of knowledge. Tables of occurrence relationships allow you to establish occurrence relationships between structures. This is necessary to describe complex structures containing sub-structures.

Inheritance relationship tables allow you to establish inheritance relationships between structures. This is necessary in order to avoid an excess of information in the system, the structure data using these tables can be represented as data on the selected structure and data taken from the base structure.

The tables of these models contain information that relates exclusively to a specific model of knowledge representation. For an ontological model, these can be tables of structure names and their ontological descriptions. For the frame model, these are tables of connections of slots and structures. This organization of data will logically divide the representation of data between models and organize their search methods for each model, while leaving the opportunity to use common search methods for all models [5].

The ontology clarifies the fundamental problems of existence, the development of the essential, the most important, which is the formal specification of the conceptual (abstract) model of the military system, taking into account the functional groups of combat service [6].

Ontology consists of classes of entities of the subject area, the properties of these classes, the relationships between these classes and statements constructed from these classes, their properties and relationships between them.

Frame – a structure that contains a description of the object in the form of attributes and their values, the representation of a conceptual object. Information related to the frame is contained in its constituent slots. To ensure the integrity of the knowledge base, which contains several models of knowledge representation, it is necessary to create tables that reflect both the essences of different types and the relationship between them [5].

The user interface will provide control of the logical output of knowledge for the implementation of intelligent control functions.

Tasks to be solved: determination of possible ways to achieve the set target settings on the basis of the received request, in accordance with the defined set of the specified initial conditions; choosing the best, in a sense, way to achieve the set targets; determining the order of consumption of resources in the sequence that ensures their rational use in the process of achieving a given target setting; formation of the structure of achievement of target settings for the algorithm of formation and issuance of comments; synthesis and issuance of recommendations for achieving the set targets.

The input information of the logic control algorithm is the results of determining the initial conditions; data on the parameters of resource consumption; data on the actual state of resources; information about the available time reserve to achieve the target installation; query information that determines the direction and "purpose" of the inference.

The output information of the logic control algorithm is: information about the possibility of achieving the target setting in accordance with the request for a given set of initial conditions; information on the order of expenditure of resources to ensure the achievement of a given "goal"; structure that characterizes the order of achieving a given "goal" (for the algorithm for forming comments).

The logical inference procedure is implemented on the structures of target settings, stored in the knowledge base and selected in accordance with the mode of operation of the system and the nature of the request. The logical conclusion is made in the following sequence: selection of the target installation in the state of the general structure in accordance with the received request; selection of all possible structures to achieve this target setting for the specified set of initial conditions; fixing the selected structure for transmitting the algorithm for forming comments; formation and issuance of a response to a request (issuance of recommendations).

At formation of possible structures of achievement of the set target installation the operative redistribution of the resources used in the course of achievement of target installations - according to the rules stored in knowledge base is carried out. The rules of redistribution of resources are divided into constant, due to meta-knowledge and laid down at the stage of system development, and variables, for which it is possible to adjust them when replenishing the knowledge base. The selection of the best structure for achieving a given target setting is carried out according to several criteria, the most important of which are: the minimum time to achieve a given target setting; minimum consumption of system resources to achieve it; the minimum number of intermediate goals that are part of it.

The preparation and issuance of comments is carried out in order to increase the level of detail of the results of solving both computational and informational, and logical and analytical tasks issued to combat personnel.

Synthesis and issuance of comments is carried out in the modes of automatic preparation and issuance of comments and explanations, which, in turn, is carried out as part of the conclusion of the results of settlement and information problems (automatic synthesis), and at the request of military personnel.

Automatic preparation and issuance of comments on the results of solving settlement and information problems is carried out on the basis of a form and a catalog of comments, which reflect the affiliation and possible level of detail of the information provided. The form and catalogs put in accordance with specific models and calculation and information tasks a set of procedures for forming comments, the order and conditions of their connection. This approach allows you to change the order and composition of the comments issued, without changing the main software modules of calculation and information tasks in the case of new requirements.

Issuance of comments in the appropriate mode is based on the results of logical inference. The source information in this case is the structure of achieving a given target installation in the form of its adjacency matrix and the corresponding directories. Comments are formed by passing the arcs of the appropriate structure and a sample from the catalog of initial conditions and target settings of the content of the relevant "goals". The issued comments allow to trace all logic of the conclusion, its objective preconditions, structure and the order of use at various stages of resources, etc.

The display and pre-processing of information must comply with the principles of information display, which affect the characteristics of the promotion of information to persons involved in decision-making in a critical situation during the preparation and conduct of hostilities. These are: the availability of perception and the completeness of the information displayed; natural imagination; ergonomics of information display; flexibility of information display.

The output information for the algorithm of display and pre-processing of information comes in the form of solving computational and information problems, intellectual problems, in the process of replenishing databases and knowledge, as well as comes from the workplaces of combat personnel.

The controller is designed to organize the computational process in accordance with the purpose of the mathematical network model for making decisions on the preparation and conduct of hostilities. The manager provides the following tasks: software initialization; organization of information exchange with information sources; organization of priority allocation of resources for computational-informational and logical-analytical tasks; distribution of resources of automation means in accordance with the set tasks; organization of display and documentation of results of solving problems; organization of interaction of software modules on input and output information.

The manager implements the absolute and relative scale of program priorities. Absolute priority is given to real-time software modules in relation to modules operating in time distribution mode. Relative priority is given to modules within one class in accordance with the importance given to each degree. Manager is the core of the software, created as a separate module and is one of the most complex components.

The results of research on the architecture of the network knowledge base of a complex military system (Fig. 3) presented in the article when compared with the results of research in [5, 7, 8] are given as follows:

– mathematical network models for decision supporton the preparation and conduct of hostilities.

– catalog of target installations (CTI);

– catalog of initial conditions (CIC);

– catalog of resources (CR) of groups of troops (time, material, combat and quantitative composition) used, their costs and replenishment;

– catalog of rules of resource consumption (CRC) and the choice of criteria for their allocation in the process of use.

– matrix of relations between target installations with initial conditions;

– matrix of resources used;

– matrix of compliance with the rules of resource consumption and the choice of criteria for their allocation.

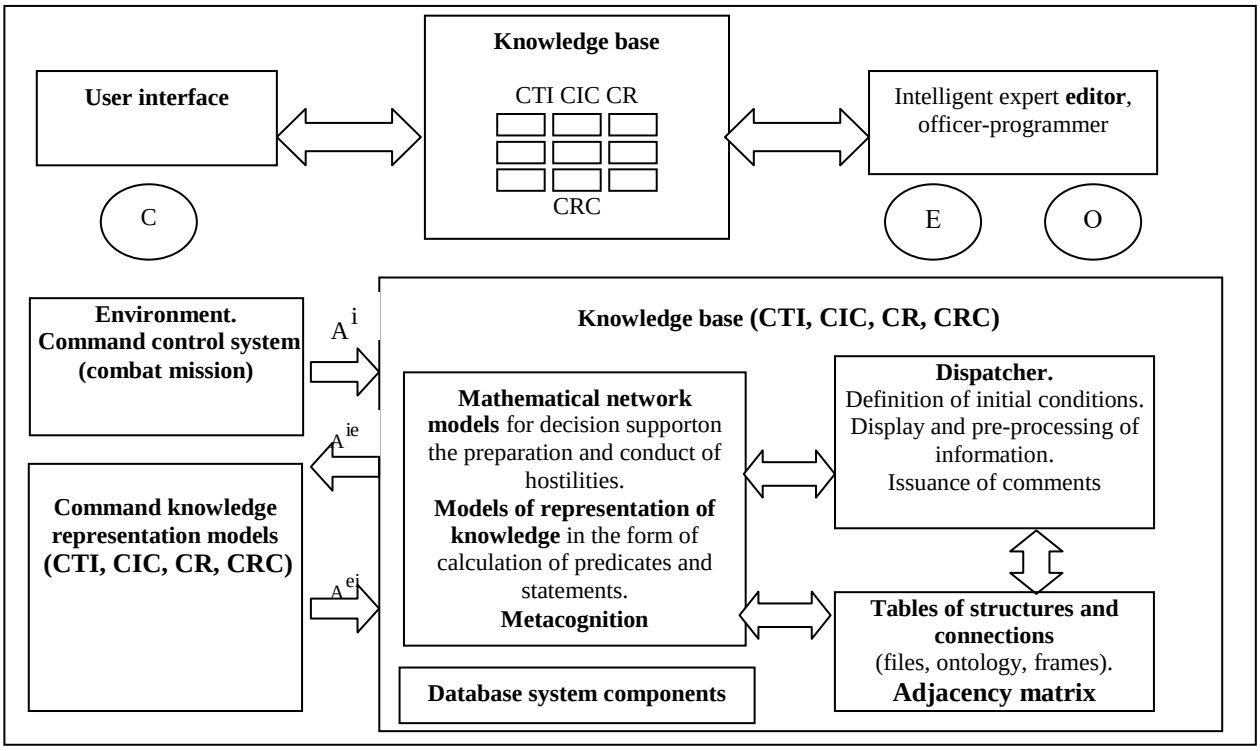


Fig. 3. The architecture of the network knowledge base of a complex military system

Conclusions

In this manner, a complex system of military purpose with a network knowledge base, which is built when creating a group of troops (forces) and will support it in a state when it is able to solve the tasks assigned to it. This requires in-depth elaboration of issues not only of modern armaments and sustainable and continuous management, but also of even more complex issues of scientific substantiation of network knowledge base architecture and structure of complex military system, organization of joint use of automation and weapons.

A practical approach to building the architecture of the network knowledge base and organizational structure of a complex military system can be implemented by substantiating the components and elements of the system when creating a group of troops (forces) and maintaining it in a state where it can solve its tasks.

References:

1. Toropchin A. (2006). Synthesis of adaptive structures of anti-aircraft missile and artillery cover systems for objects and troops and evaluation of their effectiveness (theory, practice, development trends). KhUAF. Kharkiv. 348 p.

2. Smirnov E. (2018). Theoretical foundations of the formation and degradation of complex organizational and technical systems. KhNURE. Kharkiv. 162 p.

3. Yermoshyn M. (2019). Armed struggle in the air and space. KhUAF, Kharkiv. 495 p.

4. Yermoshyn M., Oleshenko A. and Drobakha Hr. (2019). Formulation of the problem synthesis of the structure of a complex organizational system for military purposes. Honor and Law, No. 2, pp. 10-19.

5. Nechaev V., Koshkaryov M. (2015). Educational resources and technology. No 5, pp. 176–162.

6. Lande D. (2015). Building a domain model by probing a service. Design Ontology, No 3(17), pp. 328-335.

7. Sosinskaya S. (2011. Representation of knowledge in the information system. Artificial intelligence methods and knowledge representation. Stary Oskol, TNT, 215 p.

8. Bolotova L. (2012). Artificial intelligence systems: knowledge-based models and technologies. Informatics, M. Finance and statistics. 324 p.

9. Gavrilova T., Kudryavtsev D., Muromtsev D. (2016. Knowledge Engineering. Models and Methods. SPb, Doe. 324p.

10. Meredith Brussard. (2020). Artificial intelligence. The limits of the possible. M. : Alpina non-fiction. ISBN 978-5-00139-080-0.

11. Slyusar V. (October 8–10, 2019). Artificial intelligence as the basis of future control networks.. Coordination problems of military technical and devensive industrial policy in Ukraine. Weapons and military equipment development perspectives // VII International Scientific and Practical Conference. Abstracts of reports. Kyiv, pp. 76-77, DOI: 10.13140/RG.2.2.30247.50087 .

12. Yermoshyn M., Drobaha G., Shuriga M. (2019). The basic properties of a complex military system // Science and Technology of the Air Forces of the Armed Forces of Ukraine. Kharkiv. v. 4 (37), p. 20-26.

Received 30.01.2021

Відомості про авторів:

Єрмошин Михайло Олександрович – д-р військових наук, професор, Харківський національний університет Повітряних Сил ім. І. Кожедуба, профессор, Україна; ORCID: https://orcid.org/0000-0003-3148-9489

Побережний Андрій Анатолійович – науковий співробітник, Національна академія Національної гвардії України, Україна; email: fix086@ukr.net; ORCID: https://orcid.org/0000-0002-8984-6912

Онопрієнко Олександр Сергійович – ад'юнкт, Національна академія Національної гвардії України, Україна; ORCID: https://orcid.org/0000-0001-7935-4570

Шурига Михайло Павлович – студент, Харківський національний університет радіоелекторики, Україна; email: mykhailo.shuryha@nure.ua; ORCID: https://orcid.org/0000-0001-6437-0527

УДК 621.396 **DOI:10.30837/rt.2021.1.204.10**

О.В. РЯЗАНЦЕВ, канд. физ.-мат. наук, С.В. МАРЧЕНКО, канд. физ.-мат. наук, М.В. КУЛИК

ОБ ЭФФЕКТЕ ДОПЛЕРА В РАДИОЛОКАЦИИ

Введение

Эффект Доплера (ЭД) известен давно [1, 2] и, в частности, используется в радиолокации для определения скорости объектов [3 – 5]. С этим эффектом сталкиваются практически все – классическим примером является изменение тона гудка движущегося локомотива (подвижная система отсчета (ПСО)) для людей, находящихся на платформе (неподвижная система отсчета (НСО)). Т.е. если обозначить частоту тона гудка в СО, связанной с локомотивом f_0, то люди на платформе будут регистрировать частоту $f > f_0$ если локомотив приближается и $f < f_0$, если он удаляется. В общем случае вектор скорости источника может не совпадать с прямой, соединяющей НСО и ПСО, что изображено на рис. 1.

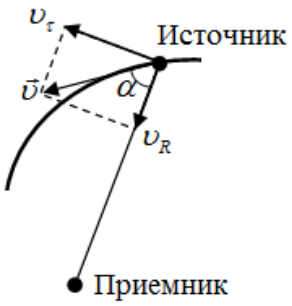


Рис. 1. Разложение вектора скорости источника излучения на радиальную и тангенциальную компоненты

Обычно в такой ситуации вектор $\vec{\upsilon}$ (касательная к траектории в данной точке) разлагают на радиальную υ_R и тангенциальную υ_τ компоненты, причем с υ_R связывают продольный ЭД, а с υ_τ – поперечный. Т.е. υ_R, как видно из рис. 1, связан только с изменением расстояния между источником (И) и приемником (ПР), а υ_τ – с вращением источника относительно приемника при неизменном расстоянии между ними. Тогда идеализированная ситуация с продольным ЭД соответствует движению источника по прямой, соединяющей его с приемником (приближение или удаление), и $\vec{\upsilon}$ имеет только одну компоненту υ_R. Поперечному ЭД соответствует вращение источника по окружности, в центре которой находится приемник, а $\vec{\upsilon}$ характеризуется только компонентой υ_τ. Очевидно, регистрируя лишь один какой-либо из типов ЭД, судить о скорости и траектории объекта затруднительно. Кроме того, даже в простейшем случае продольного ЭД, регистрируя измененную частоту излучателя, невозможно определить его скорость, так как неизвестно сама частота излучения (частота в ПСО).

Постановка задачи

Как правило, в современных радиотехнических системах используется только продольный ЭД, позволяющий определить радиальную составляющую скорости движения объекта. Кроме того, существуют ситуации, для которых вообще невозможно определить скорость объекта без учета поперечного ЭД. Поэтому, целью данной работы является анализ принципиальных возможностей совершенствования функционирования радиолокационных станций

(РЛС), одновременно использующих оба типа ЭД – продольный и поперечный, что позволяет определить полную скорость наблюдаемого объекта в любых ситуациях.

Результаты работы

Рассмотрим продольный ЭД. Если обозначить расстояние между излучателем и приемником *x* то, как известно (см., например, [1, 2]), фазовое отставание колебаний в точке приема $\phi = 2\pi \frac{x}{\lambda_И}$, и если $x = x(t)$, то $\frac{d\phi}{dt} = \frac{2\pi}{\lambda_И} \cdot \frac{dx}{dt}$, или $\omega_Д = \frac{2\pi}{\lambda_И} \cdot \upsilon$, где υ – скорость объекта,

а в данном случае $\upsilon = \upsilon_R$. Величина $\omega_Д$ представляет собой доплеровский сдвиг частоты для наблюдателя. В зависимости от знака *dx* ($dx > 0$ – удаление от объекта, $dx < 0$ – приближение объекта) может быть как положительным, так и отрицательным. Т.е. на векторной диаграмме в фазовой плоскости вектор колебания с частотой $\omega_и$ (СО излучателя) получает для наблюдателя (СО приемника) дополнительное приращение $\pm\omega_Д$, однозначно связанное со скоростью движения объекта, т.е. $\omega_{ПР} = \omega_и \pm \omega_Д$. Учитывая далее, что $\lambda_и = C/f_и$, получаем, что $\omega_Д = \omega_и \cdot \frac{\upsilon_R}{C}$, т.е. $\omega_{ПР} = \omega_и \cdot \left(1 \pm \frac{\upsilon_R}{C}\right)$, где С – фазовая скорость волны, одинаковая в обеих СО.

Заметим, что в системе наблюдателя и излучателя длины волн также будут различны – для излучателя (ПСО) $\lambda_и = C/f_и$, а для наблюдателя (НСО) $\lambda_{ПР} = C/f_{ПР} = C/\left(f_и \pm f_Д\right)$, т.е. $\lambda_{ПР}$ может быть как больше, так и меньше $\lambda_и$. Таким образом:

$$\left(\frac{C}{\lambda_{ПР}} = \frac{C}{\lambda_И} \cdot \left(1 \pm \frac{\upsilon_R}{C}\right)\right) \cdot \left(1 \mp \frac{\upsilon_R}{C}\right) \Rightarrow \lambda_{ПР}\left(1 - \frac{\upsilon_R^2}{C^2}\right) = \lambda_и\left(1 \mp \frac{\upsilon_R}{C}\right),$$

и, полагая $\frac{\upsilon_R}{C} << 1$, пренебрегаем $\left(\frac{\upsilon_R}{C}\right)^2$ в левой части равенства, что дает:

$$\lambda_{ПР} = \lambda_И \cdot \left(1 \mp \frac{\upsilon_R}{C}\right). \qquad (1)$$

Как видно, в случае приближения объекта для наблюдателя в НСО принимаемая частота больше излучаемой, т.е. $\omega_{ПР} > \omega_И$, а длина волны $\lambda_{ПР} < \lambda_И$. При удалении излучателя все наоборот: $\omega_{ПР} < \omega_И$, а $\lambda_{ПР} > \lambda_И$. Для наглядности можно предположить, что λ – пространственный интервал между короткими радиоимпульсами, испускаемыми излучателем. Тогда приближению излучателя к приемнику соответствует сжатие равномерного распределения радиоимпульсов в пространстве (для наблюдателя в НСО), а удалению – растягивание этого распределения.

Стоит отметить, что соотношение $\omega_И = \omega_{ПР} \mp \omega_Д$ приобретает смысл условия сохранения частоты в СО, которые движутся относительно друг друга, причем, изменение частоты приема обусловлено не изменениями внутренних свойств излучателя, а изменениями свойств канала связи, которые вызваны движением излучателя относительно приемника. Для случая РЛС именно эти изменения позволяют определять скорость движения объекта.

Для идеализированной ситуации поперечного ЭД вектор скорости движения объекта $\vec{\upsilon}$ состоит только из тангенциальной компоненты υ_τ (рис.1), т.е., например, излучатель равно-

мерно *вращается вокруг приемника по окружности радиусом R*, а НСО (наблюдатель, РЛС) совмещена с центром окружности (точка О, рис. 2), а излучатель «включается» в точке 1 траектории. Когда же волна достигнет наблюдателя, излучатель будет находиться в точке 2 и для наблюдателя волна пройдет путь $S > R$, т.е. происходит «растягивание» длины волны и можно ожидать понижения частоты колебаний, регистрируемых наблюдателем.

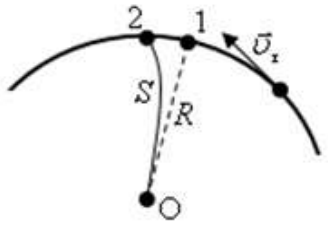


Рис. 2. Иллюстрация к поперечному ЭД

Тогда элемент *ds* можно представить в виде ($c >> v_\tau$):

$$\left(dS\right)^2 = \left(dR\right)^2 + \left(dl\right)^2,$$

где *dl* – элемент длины дуги 1-2; такое соотношение возможно при условии

$$\left(Cdt\right)^2 = \left(C_R dt\right)^2 + \left(\upsilon_\tau dt\right)^2,$$

где C_R – скорость волны в радиальном направлении, т.е. $C^2 = C_R^2 + \upsilon_\tau^2$, откуда

$$\left(C_R = C\sqrt{1-\frac{\upsilon_\tau^2}{C^2}}\right)\frac{2\pi}{\lambda_И} \Rightarrow\ \omega_{ПР} = \frac{2\cdot\pi\cdot C}{CT_И}\cdot\sqrt{1-\frac{\upsilon_\tau^2}{C^2}} = \omega_И\cdot\sqrt{1-\frac{\upsilon_\tau^2}{C^2}} \approx \omega_И\cdot\left(1-\frac{1}{2}\cdot\frac{\upsilon_\tau^2}{C^2}\right) \qquad (2)$$

Как видно, для поперечного ЭД имеет место понижение воспринимаемой частоты, причем это понижение не зависит от направления вращения излучателя. Заметим, что если полученное соотношение переписать в виде $\frac{2\pi C}{T_{ПР}} = \frac{2\pi C}{T_и}\sqrt{1-\frac{\upsilon_\tau^2}{C^2}}$, то получим $T_И = T_{ПР}\sqrt{1-\frac{\upsilon_\tau^2}{C^2}}$, или вообще $t' = t\sqrt{1-\frac{\upsilon_\tau^2}{C^2}}$ – одно из известных соотношений специальной теории относительности, согласно которому время *t'* в ПСО течет медленнее, чем время *t* в НСО. Изложенное показывает, что это «замедление» обусловлено именно свойствами канала связи, т. е. информация, излучаемая подвижным объектом, несколько искаженно воспринимается наблюдателем в НСО, но, как уже указывалось, именно эти искажения позволяют РЛС определять скорость движения объектов.

Из приведенных выражений определить эту скорость по измеряемой величине $\omega_{ПР}$ невозможно, так как неизвестна величина $\omega_И$. Поэтому РЛС активного типа излучает электромагнитную волну известной частоты $\omega_И$, а принимает эхо-сигнал с частотой $\omega_{ПР}$, т.е. упрощенно реализуется схема, показанная на рис. 3.

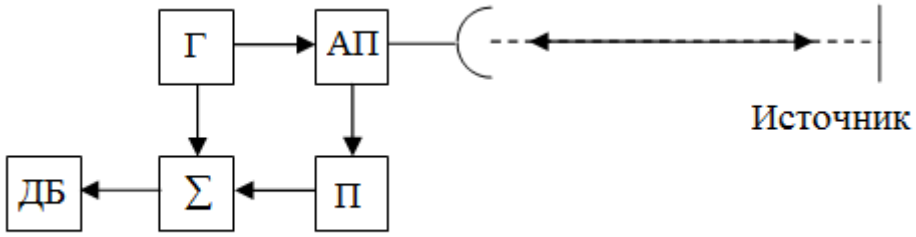


Рис. 3. Упрощенная структура измерителя скорости (Г– генератор ω_u, АП – антенный переключатель, П – приемник эхо-сигнала, ДБ – детектор биений $\omega_И$ и $\omega_{ПР}$)

Такая схема позволяет, например, складывать излучаемый и принимаемый сигналы, а по частоте биений определять скорость объекта.

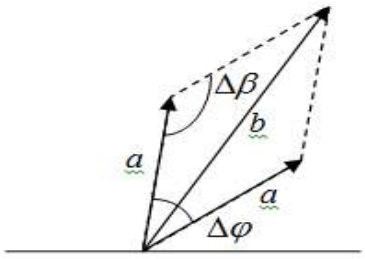


Рис. 4. Векторная диаграмма сигналов на фазовой плоскости

Если, как изображено на рис. 4, на векторной диаграмме изобразить эти разночастотные сигналы в некоторый момент времени, то, учитывая, что $\Delta\beta = \pi - \Delta\varphi$, а также, принимая для простоты амплитуды сигналов одинаковыми, получаем амплитуду биений $b^2 = 2a^2 - 2a^2\cos(\pi - \Delta\varphi)$ и после несложных преобразований:

$$b = 2a\sin\left(\frac{\pi - \Delta\varphi}{2}\right) = 2a\cos\frac{\Delta\varphi}{2}. \tag{3}$$

Рассмотрим вначале продольный ЭД, т.е. ситуацию, когда скорость объекта состоит только из радиальной компоненты υ_R. Используя связь между разностью хода для падающей и отраженной волны относительно РЛС и соответствующей разности фаз, получаем

$$\Delta\varphi = 2\pi\frac{\Delta l}{\lambda_И} = \{\Delta l = 2\upsilon_R\Delta t\} \Rightarrow\ b = 2a\cos\left(\frac{2\pi\upsilon_R}{\lambda_И}\cdot\Delta t\right). \tag{4}$$

Таким образом, величина $\frac{2\pi\upsilon_R}{\lambda_И}$ является частотой изменения амплитуды биений *b*. Заметим, что биения как результат сложения разночастотных колебаний получаются автоматически, без каких либо предположений относительно различия $\omega_И$ и $\omega_{ПР}$, т.е. рассматривалось лишь явление интерференции падающей и отраженной волны с переменной разностью хода. Тогда частота биений:

$$\omega_Б = \frac{\omega_И \pm \omega_{ПР}}{2} = 2\pi\frac{\upsilon_R}{\lambda_И} \Rightarrow\ \omega_{ПР} = \omega_И\left(1 \pm \frac{2\upsilon_R}{C}\right). \tag{5}$$

Как видно, выражение, соответствующее продольному ЭД, получено как результат дополнительного набегания разности фаз между излучаемой и отраженной волной, причиной которого является изменение разности хода, обусловленное движением объекта. Отметим, что такой же результат можно получить сразу, используя соотношение

$$\left(\varphi = 2\pi\frac{l}{\lambda_И}\right)\cdot\frac{d}{dt} \Rightarrow\ \omega_Б = 2\pi\frac{\upsilon_R}{\lambda_u}. \tag{6}$$

Для поперечного ЭД можно повторить приблизительно те же выкладки и, воспользовавшись рис. 2, а также учитывая, что за время «туда-обратно» длина элемента дуги удвоится, получаем $\left(Cdt\right)^2 = \left(C_R dt\right)^2 + \left(2\upsilon_\tau dt\right)^2$, или $C^2 = C_R^2 + 4\upsilon_\tau^2$, а после умножения на $2\pi/\lambda_И$ получаем

$$\omega_{ПР} = \omega_И\sqrt{1-4\frac{\upsilon_\tau^2}{C^2}} \approx \omega_И\left(1-2\frac{\upsilon_\tau^2}{C^2}\right). \tag{7}$$

Получим теперь частоту биений для поперечного ЭД с использованием схемы, изображенной на рис. 3:

$$\omega_Б = \frac{\omega_И - \omega_{ПР}}{2} = \omega_И\frac{\upsilon_\tau^2}{C^2} = 2\pi\frac{\upsilon_\tau^2}{\lambda_И C} \tag{8}$$

Как видно, величины $\omega_Б$ для продольного и поперечного ЭД при одинаковых значениях υ и $\lambda_И$ должны существенно отличаться. Действительно, при $\upsilon = 720$ км/ч = 200 м/с и $\lambda_И = 10^{-2}$ м для продольного ЭД $f_Б \approx 20$ кГц, а для поперечного – всего несколько более 10^{-2} Гц, т.е. частоты ортогональных ЭД находятся в существенно различающихся участках диапазона, что облегчает их раздельное детектирование.

Совместная регистрация обоих видов ЭД и, соответственно, определение компонент υ_R и υ_τ позволяет получить значение модуля реальной скорости объекта $\upsilon = \sqrt{\upsilon_R^2 + \upsilon_\tau^2}$, что иллюстрирует рис. 5.

На рис. 5 изображена траектория плоского прямолинейного приблизительно равномерного движения объекта в плоскости ZOY, при котором переменными являются угол места θ и расстояние до объекта R, а азимутальный угол фиксирован. РЛС помещена в центр координат (точка О). Как видно из рисунка, по мере движения объекта радиальная компонента υ_R монотонно убывает, а тангенциальная υ_τ – возрастает. Соответственно убывает частота биений для продольного ЭД и возрастает – для поперечного. Для некоторого значения угла места θ_0 величина υ_R обращается в 0, а υ_τ достигает максимального значения, т.е. скорость объекта состоит только из тангенциальной компоненты. В этой точке биения для поперечного ЭД имеют максимальную частоту. В дальнейшем радиальная компонента υ_R начинает возрастать от нуля, т.е. для продольного ЭД возникнут биения, фаза которых изменит знак на противоположный (скачок на π в точке, соответствующей θ_0), а частота будет увеличиваться. Тангенциальная компонента υ_τ после прохождения максимального значения и, соответственно, частота биений для поперечного ЭД будут монотонно убывать.

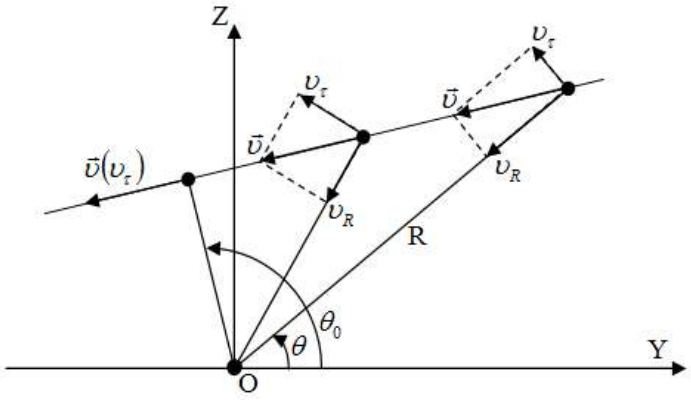


Рис. 5. Динамика изменения υ_R и υ_τ
для случая прямолинейного двухмерного движения объекта

Для частного случая горизонтальной траектории определение скорости объекта упрощается, так как угол места совпадает с углом проецирования $\vec{\upsilon}$ на *R*. Тогда, по измеряемому углу места $\upsilon = \upsilon_R / \cos\theta$ или $\upsilon = \upsilon_\tau / \sin\theta$, а угол места, соответствующий обращению в ноль υ_R и максимальному значению υ_τ, равен $\pi/2$.

Выводы

Проанализированы продольный и поперечный ЭД для случая движущегося излучающего объекта, получены выражения для доплеровского сдвига.

Определены выражения частоты биений в случае активной РЛС для обоих видов эффектов Доплера, позволяющие получить величину скорости объекта в любых ситуациях.

Предложены варианты определения скорости движения объекта при одновременном использовании продольного и поперечного ЭД.

Список литературы:

1. Савельев И.В. Курс общей физики. Т. 2. Москва : Наука, 1978. 480 с.

2. Ландау Л.Д., Лифшиц Е.М Теоретическая физика : учеб. пособие. В 10 т. Т.II Теория поля ; 7-е изд. испр. Москва : Наука, 1988. 512с.

3. Чердынцев В. А. Радиотехнические системы : учеб. пособие для вузов. Минск : Вышэйш. шк., 1988. 369 с.

4. Zhang J., Zhang K., Grenfell R., Deakin R. Short note: on the relativistic Doppler effect for precise velocity determination using GPS // Journal of Geodesy. 2006. Vol. 80, Issue 2, pp.104–110.

5. Ashby N., Spilker J. Introduction to relativistic effects on the global positioning system // Global positioning system: theory and applications / American Institute of Aeronautics and Astronautics, Washington. 1996. Vol. 1. pp. 623–698.

Поступила в редколлегию 11.01.2021

Сведения об авторах:

Рязанцев Олег Вадимович – канд. физ.-мат. наук, доцент, заведующий кафедрой аппаратуры радиосвязи, радиовещания и телевидения; Днепровский государственный технический университет; Украина; e-mail: arrt.dstu@gmail.com; ORCID: https://orcid.org/0000-0002-7253-59663

Марченко Сергей Викторович – канд. физ.-мат. наук, доцент, доцент кафедры аппаратуры радиосвязи, радиовещания и телевидения; Днепровский государственный технический университет; Украина; e-mail: smarsv1979@gmail.com; ORCID: https://orcid.org/0000-0002-6022-5071

Кулик Максим Владимирович – ассистент кафедры аппаратуры радиосвязи, радиовещания и телевидения; Днепровский государственный технический университет; Украина, e-mail: kulik@internic.ua; ORCID: https://orcid.org/0000-0002-5375-7168

УДК 621.391.5: 004.056.53 **DOI:10.30837/rt.2021.1.204.11**

В.Г. КРИЖАНОВСЬКИЙ, д-р техн. наук, С.П. СЕРГІЄНКО, канд. физ.-мат. наук,
Д.В. ЧЕРНОВ, канд. техн. наук, В.В. КРИЖАНОВСЬКИЙ, канд. техн. наук

ПІДСЛУХОВУВАННЯ NFC-ЗВ'ЯЗКУ НА ЧАСТОТАХ ВИЩИХ ГАРМОНІК

Вступ

Широке використання технологій близько польової комунікації (near field communication – NFC) спонукає розглядати різні аспекти удосконалення апаратури та безпеки її використання [1 – 4]. Безпека стосується таких застосувань NFC (та RFID – radio frequency identification device) як безконтактні банківські транзакції, біометричні паспорти та багато іншого. В останній час додалась ще й безпека зарядки електромобілів [5].

У роботі [3] розглянуто різні види атак на NFC-зв'язок, в [4] детально аналізуються можливості збільшення відстані, на якій можливо або підслухати або здійснити звернення до пристроїв з NFC-зв'язком. У роботах [6, 7] розглядається можливість здійснення доступу до NFC картки (RFID пристрою) з використанням прийому сигналу на вищих гармоніках частоти збудження. Аналіз процесу збудження та реєстрації сигналів у цих роботах є доволі детальним, але складність всього комплексу проблем є великою і відпрацювання методики вимірювання та вивчення можливостей впливу на випромінювання та прийом сигналу за цим побічним каналом є актуальною задачею.

Метою даної роботи є аналіз та експериментальне дослідження залежностей відстані, на якій можливо підслуховувати NFC зв'язок з використанням приймача на частотах вищих гармонік частоти 13,56 МГц.

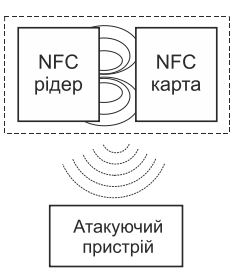
Аналіз стану проблеми та використовуваного обладнання

Зв'язок у близькому полі (NFC) є індуктивним зв'язком близько розташованих котушок індуктивності, пов'язаних спільним магнітним полем [1, 2]. Відповідно напруженість поля зменшується з відстанню за законом $1/r^3$, і на порівняно невеликих відстанях зв'язок стає неможливим, що є передумовою збереження конфіденційності транзакцій. Довжина електромагнітної хвилі на частоті 13,56 МГц складає 22,11 м, і елементи рідера не здатні скласти ефективну антену, але на частоті третьої гармоніки 40,68 МГц довжина хвилі у вільному просторі вже 7,37 м, тому можливе випромінювання цього сигналу пов'язаними провідниками. У роботі [6] такою антеною слугував USB кабель, який з'єднував комп'ютер і рідер. Тому вивчення, в тому числі експериментальне, джерел генерації та випромінювання вищих гармонік несучої частоти обміну інформації у системах NFC та RFID важливе для практики захисту інформації.

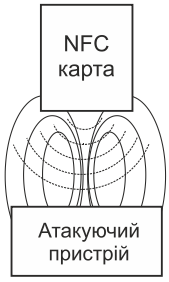
Є два основні варіанти несанкціонованого отримання даних з тегу (карти чи іншого пристрою RFID) – це підслуховування (рис. 1, *а*) чи скіммінг («зняття вершків» у вільному перекладі, рис. 1, *б*). У першому випадку здійснюється отримання інформації зі штатного процесу обміну легального рідеру та безконтактної картки, у другому – зловмисник генерує сигнал, яким запитує від картки інформацію, і потім приймає її без відома власника. Для цього можуть використовуватися збільшенні розміри антенних систем та використовуватися прийом на частотах вищих гармонік [4, 6 – 9]. Відстані, на яких це можливо здійснити, дають можливість розташувати антенні системи у стиснених умовах непомітно для власника картки.

Імітатор NFC-зв'язку. Для виконання експерименту потрібно мати передавач, який зв'язується з тегом на частоті 13,56 МГц. Використання різних реальних систем (смартфон з NFC та картка для сплати за проїзд) має той недолік, що процес встановлення зв'язку неперіодичний, і це ускладнює вимоги до апаратури, яка повинна реєструвати випромінювання

на частоті гармоніки. Тому було використано простішу схему зчитувача (рідера), побудованого на базі процесора Arduino Nano, та пристрою RFID-RC522 (рис. 2).



а



б

Рис. 1

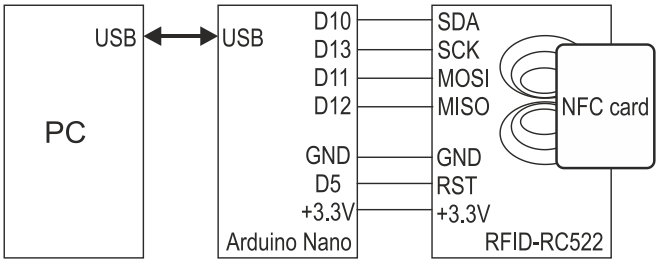


Рис. 2

Програма для Arduino Nano була складена на основі програми [10], вона дозволила проводити періодичне зчитування даних з картки, і тому на спектроаналізаторі можна було дослідити спектр передачі від картки до зчитувача. Спочатку було проведено вимірювання, яке підтвердило, що і в цьому випадку третя гармоніка переважно генерується NFC карткою (табл. 1). На рис. 3 показано спектри без картки (нижня частина) та з карткою (верхня спектрограма). На рис. 4 показана схема експерименту, де 1 – безконтактна картка, 2 – котушка зв'язку, використовувалась NFC антена зі смартфона, FPC1500 – спектроанализатор.

Таблиця 1

Спектр	1 гармоника, dBm	2 гармоника, dBm	3 гармоника, dBm
Без NFC карты	-33,5	-62,56	-73,97
С NFC картой	-31,68	-66,5	-62,7

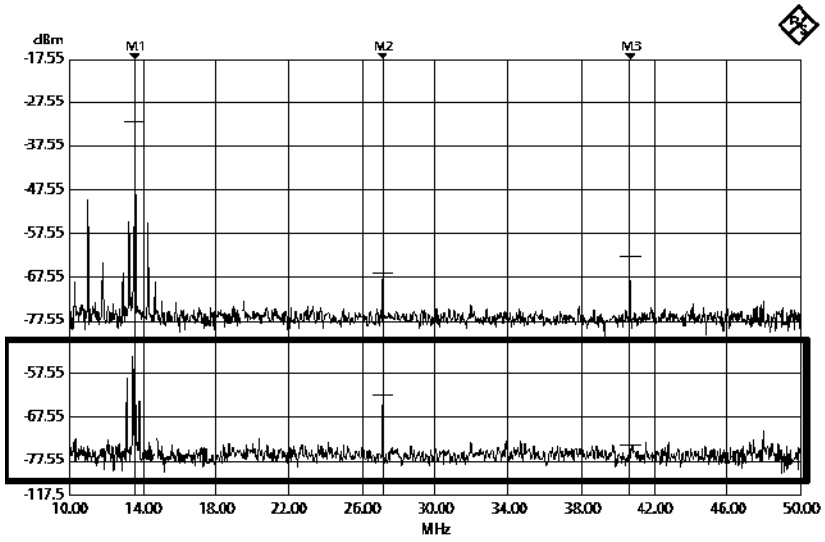


Рис. 3

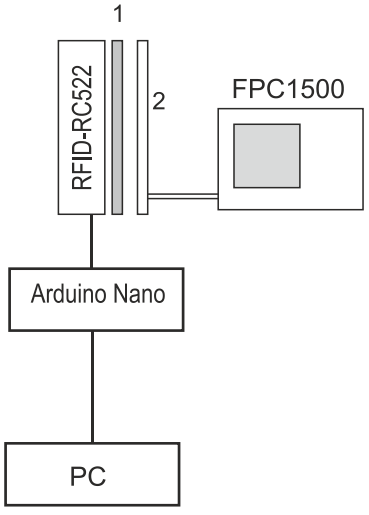


Рис. 4

Видно, що третя гармоніка сигналу значною мірою генерується у NFC картці, і сигнал цієї частоти можна використовувати для отримання інформації про картку.

В роботі використовувалась картка стандарту ISO 14443-3A з криптографічним алгоритмом NXP MIFARE Classic 1k, як це визначено за результатами тестування за допомогою смартфона Sony Xperia Z5 Premium. За стандартом ISO 14443A зчитувач передає кодовані дані з кодом Міллера 106 кбіт/с за допомогою імпульсів 3 мкс. Отже, дані прямого каналу повинні знаходитись у перших 330 кГц спектру. Картка передає закодовані кодом Манчестер 106 кбіт/с дані, які модулюються ASK на піднесучій частоті 847,5 кГц. Зворотний канал повинен бути в діапазоні 424 кГц, зосередженим близько 847,5 кГц. Прямий канал амплітуд-

но модулюється на 13,56 МГц з індексом модуляції 100 %, тоді як зворотний канал має індекс модуляції 8–12 % [2]. На рис. 5 показана спектрограма обміну інформацією між зчитувачем та карткою, видно складові модуляції біля основної частоти $f_0 = 13,56$ МГц та біля піднесучих $f_0 \pm f_M$, де $f_M = f_0/16 = 0,8475$ МГц, використовувався багатофункціональний спектроаналізатор R&S FPC1500. На рис. 6 показано спектр сигналу біля третьої гармоніки основної частоти – 40,68 МГц за вимірюваннями за допомогою рамочної антени. Для показу основних характеристик сигналу виконувалось усереднення сигналу за останні 10 вимірювань. Також було збільшено полосу ВЧ фільтру до 100 кГц та відеофільтру до 1 МГц. Видно, що найбільша бокова складова знаходиться на відстані ±848 кГц. Це свідчить про те, що третя гармоніка основної частоти модулюється безпосередньо частотою піднесучої, а не утворюється за рахунок потроювання складових спектру, що передається карткою. Тому інформацію, яку передає картка до зчитувача, можна відстежувати на частотах 40,68±0,8475 МГц.

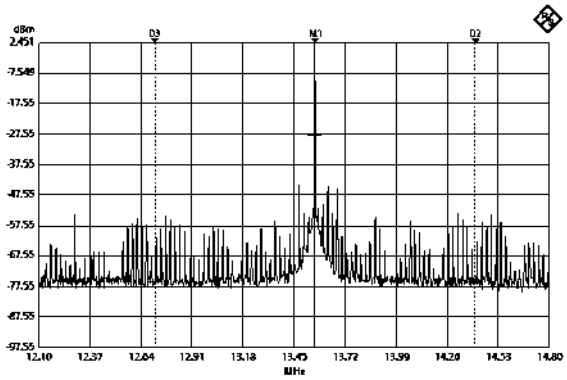


Рис. 5

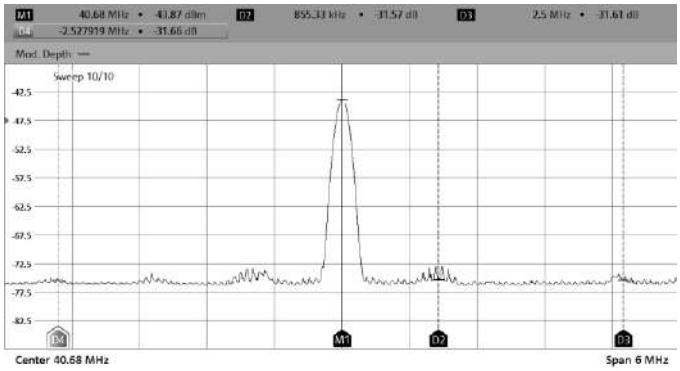


Рис. 6

Для попереднього експерименту було досліджено можливість використання картки без ініціювання її відповіді на запит від рідера. Для цього використовувалася схема рис. 7, де сигнал від картки на частотах 13,56±0,8475 МГц було замінено на подачу АМ сигналу з таким самим спектром; моделювання у часовій області показало, що і в такому режимі картка повинна генерувати частотні складові $3f_0 \pm f_M$ (рис. 8). При цьому мікросхема картки не вмикалась на передачу даних, і сигнал третьої гармоніки генерувався за рахунок нелінійності діодів мостової схеми, як і в штатному режимі роботи. Але при цьому сигнал, що приймався, був стаціонарним і було легше його вимірювати. Передавальна котушка індуктивності L_1 разом з ємністю C_1 утворювали резонансний контур, який пропускав частоти $f_0 \pm f_M$ але послаблював частоти $3f_0 \pm f_M$, це разом з опційним фільтром нижніх частот (ФНЧ) (рис. 7) робило випромінювання схеми живлення картки на частотах третьої гармоніки низьким, і відповідно спостерігалось переважно випромінювання самої картки.

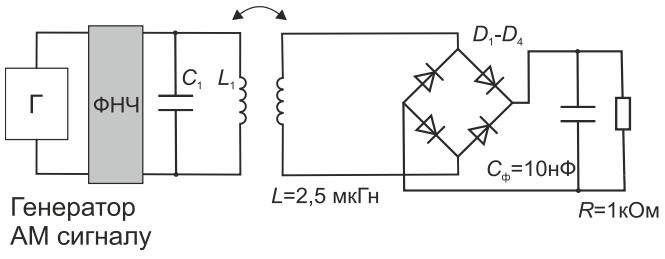


Рис. 7

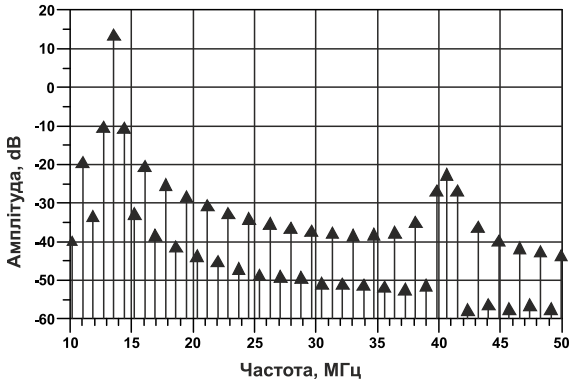


Рис. 8

Перевагою такого рішення є безперервна передача сигналу та більш точне вимірювання спектральних складових прийнятого сигналу. Маючи такі способи генерації тестового сигналу, можна виміряти відстань, на якій можливо зареєструвати сигнал на частоті третьої гармоніки.

Антена на частоту третьої гармоніки та вимірювання відстанні. Аналогічно роботі [7] для прийому сигналу на частоті 40,68 МГц була використана резонансна магнітна антена у вигляді кільцевого вібратора, який навантажений на ємність та узгоджується з лінією 50 Ом за допомогою гамма-узгодження. Антена має діаметр 77 см та виготовлена з алюмінієвого обручу (діаметр трубки 16 мм), рис. 9. КСВН антени показано на рис. 10. Антена має вузьку смугу частот, де вона узгоджена, до того ж узгодження залежить від оточуючих предметів, тому налаштування антени постійно перевірялось при зміні умов експерименту.

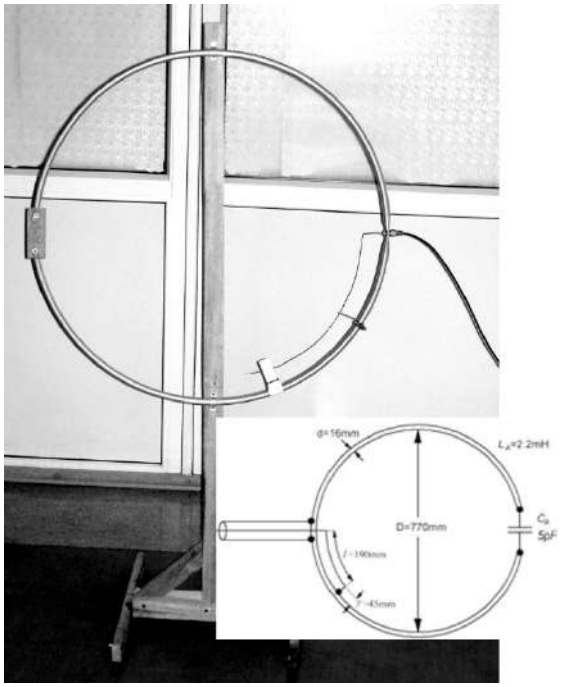


Рис. 9

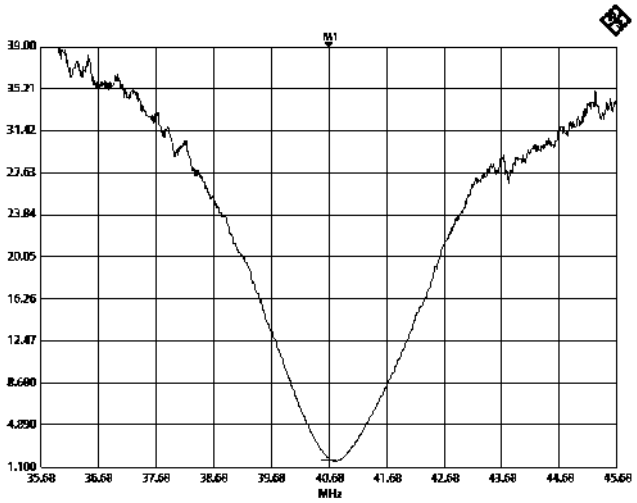


Рис. 10

Використовуючи цю антену, за схемою рис. 7 виміряли залежність сигналу картки в діапазоні частоти третьої гармоніки від відстані між карткою та приймальною антеною. Картка та антена були розташовані на одній горизонтальній осі. Залежність показана на рис. 11, вимірювання проводились при подачі на котушку L_1 змінної напруги 13,56 МГц з 10 %-ю амплітудною модуляцією прямокутним сигналом частотою f_M. Показано залежності для двох значень амплітуди основного сигналу – 6 та 8 В. Картка при цьому не передавала даних, і спостереження проводилось за спектральними складовими на частотах $3f_0$ та $3f_0 \pm f_M$. Результат свідчить про те, що рівень сигналу модуляції знаходиться на рівні шуму спектроаналізатору. В режимі вимірювання аналогової модуляції аналізатор FPC1500 здатен виявити сигнал модуляції на частоті f_M тільки при відстані між карткою и приймальною антеною біля 2 см.

При вимірюванні за схемою рис. 4, коли картка працює в періодичному режимі «запит-відповідь» з живленням від стандартного зчитувача, рівень сигналу на частоті третьої гармоніки при тій же відстані трохи вищий, але так само досягає рівня шумів. Залежність на рис. 12 отримана як результат усереднення 10 вимірювань на кожній відстані, кожне вимірювання є результатом усереднення спектроаналізатором 10 розгорток у часі. Спектрограма

кожного вимірювання має вигляд рис. 6, відповідно можна зробити висновок про наявність сигналу, але складно здійснити детектування сигналу від картки. Для розширення діапазону потрібно розшити полосу частот приймальної антени та удосконалити приймач сигналів. На додаток можна зауважити, що розглянута схема підслуховування може бути використана і у складі більш складних атак на безконтактні картки [4, 11].

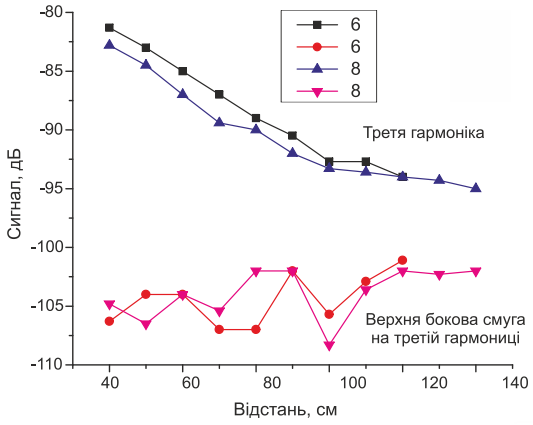


Рис. 11

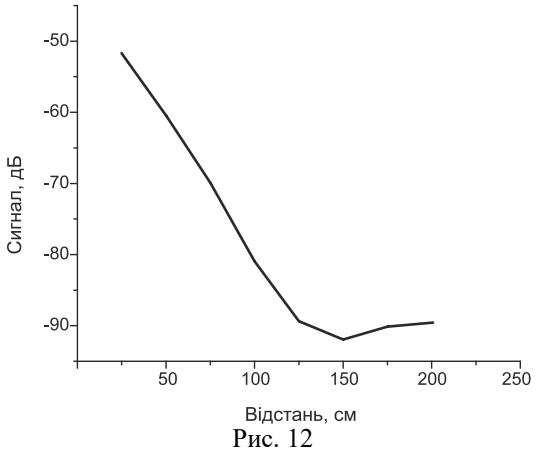


Рис. 12

Висновки

Розроблено обладнання та запропоновано методи вимірювання випромінювання вищих гармонік, які генеруються у безконтактних картках NFC-зв'язку з основною частотою 13,56 МГц. Підтверджено можливість збільшити відстань прийняття сигналу третьої гармоніки від картки, разом з тим при використанні резонансних приймальних антен демодуляція інформативного сигналу викликає складнощі, оскільки рівень бокових складових значно послаблюється і на вході приймача знаходиться на рівні шуму. Для можливості підслуховування сигналу потрібно використовувати відносно широкосмугові антени та підсилювачі з низьким рівнем шуму.

Список літератури:

1. Чернов Д.В., Крыжановський В.Г. Усилитель класса Е в составе трансивера системы ближнеполевой коммуникации // Технічна електродинаміка. Тем. вип. Силова електроніка та енергоефективність. 2011. Ч. 1. С. 293-298.

2. Finkenzeller K. RFID handbook: fundamentals and applications in contactless smart cards and Identification. ; 2nd ed. John Wiley & Sons Ltd, 2003. 427 p.

3. Bolhuis M. Using an NFC-equipped mobile phone as a token in physical access control. Thesis… University of Twente, 2014. 129 p. http://essay.utwente.nl/65419/1/thesis_nfc_martijn_bolhuis_ final.pdf

4. Hancke G. P. Practical eaves dropping and skimming attacks on high-frequency RFID tokens // J. Comput. Security. Mar. 14, 2011. Vol. 19, no. 2, pp. 259–288,

5. Van den Broek F., Poll E., Vieira B. (2015). Securing the Information Infrastructure for EV Charging // Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 61–74.

6. Engelhardt M., Pfeiffer F., Finkenzeller K. and Biebl E. Extending ISO/IEC 14443 Type A Eavesdropping Range using Higher Harmonics // Smart SysTech 2013; European Conference on Smart Objects, Systems and Technologies, Erlangen/Nuremberg, Germany, 2013, pp. 1-8.

7. Habraken R., Dolron P., Poll E & De Ruiter J. 2015 An RFID Skimming Gate Using Higher Harmonics // S Mangard & P Schaumont (eds), Radio Frequency Identification. Security and Privacy Issues. vol. 9440, Lecture Notes in Computer Science, vol. 9440, Springer, pp. 122-137, 11th Workshop on RFID Security, New York, United States, 23/06/15.

8. Ilan Kirschenbaum, Avishai Wool. How to Build a Low-Cost, Extended-Range RFID Skimmer. 15th Security Symposium Security 06. Vancouver, B.C. Canada, 07/2006 https://documen.site/download/how-to-build-a-low-cost-extended_pdf.

9. Brown T. W. C., Diakos T. and Briffa J. A. Evaluating the eavesdropping range of varying magnetic field strengths in NFC standards // 2013 7th European Conference on Antennas and Propagation (EuCAP), Gothenburg, Sweden, 2013, pp. 3525-3528.

10. MFRC522 library https://github.com/miguelbalboa/rfid (ПО для МС)

11. Oren Y., Schirman D., Wool A. Range extension attacks on contactless smart cards // Crampton, J., Jajodia, S., Mayes, K. (eds.) Computer Security – ES-ORICS 2013, LNCS, vol. 8134, pp. 646–663. Springer (2013).

Надійшла до редколегії 28.01.2021

Відомості про авторів:

Крижановський Володимир Григорович – д-р техн. наук, професор, професор кафедри радіофізики та кібербезпеки; Донецький національний університет імені Василя Стуса (м. Вінниця); Україна; email: v.krizhanovski@donnu.edu.ua; ORCID: https://orcid.org/0000-0002-2685-9740

Сергієнко Сергій Петрович – канд. техн. наук, доцент, доцент кафедри радіофізики та кібербезпеки; Донецький національний університет імені Василя Стуса (м. Вінниця); Україна; email: s.serhiienko@donnu.edu.ua; ORCID: https://orcid.org/0000-0001-5515-8946

Чернов Дмитро Вікторович – канд. техн. наук, доцент кафедри радіофізики та кібербезпеки; Донецький національний університет імені Василя Стуса (м. Вінниця); Україна; email: d.chernov@donnu.edu.ua; ORCID: https://orcid.org/0000-0001-7173-0842

Крижановський Володимир Володимирович – канд. техн. наук, Synic Solution Co., Ltd, 37, Hwangsaeul-ro 258 beon-gil, Seongnam-si Republic of Korea; email: vlad@synic.co.kr; ORCID: https://orcid.org/0000-0003-1989-1483

ФІЗИКА ПРИЛАДІВ ТА СИСТЕМ

УДК621.793:678.073 **DOI:10.30837/rt.2021.1.204.12**

В.Н. БОРЩЕВ, д-р техн. наук, А.М. ЛИСТРАТЕНКО, канд. техн. наук,
М.А. ПРОЦЕНКО, канд. техн. наук, И.Т. ТЫМЧУК, канд. техн. наук, А.В. КРАВЧЕНКО,
А.В. СУДЬЯ, Н.И. СЛИПЧЕНКО, д-р физ.-мат. наук, Б.Н. ЧИЧКОВ, д-р техн. наук

ДИСПЕРСИЯ НАНОЧАСТИЦ В ОПТИЧЕСКИ ПРОЗРАЧНЫЕ ПОЛИМЕРНЫЕ МАТРИЦЫ

Введение

В настоящее время широко используются гомогенные оптические среды, такие как оптические стекла, *монокристаллы* и полимерные материалы. Каждая из этих сред имеет конкретный набор свойств, свои преимущества и недостатки.

Например, из полимерных материалов можно производить гибкие и прозрачные пленки, при этом технология производства не является дорогостоящей, возможен серийный выпуск. Тем не менее, показатель преломления полимеров, как правило, не превышает значения 1,6. Полимерные материалы широко применяются в различных отраслях оптики: материалы для фотонной упаковки, регистрирующие среды для голографических применений, оптические волокна, мембраны, элементы интегрально-оптических схем, литографическая печать, матрицы микролинз, френелевская оптика и др.

Монокристаллы и оптические стекла являются классическими оптическими средами с хорошо изученными свойствами. Многие неорганические монокристаллы (например, ZnS или CdS) обладают высоким показателем преломления: 2,35 и 2,53 соответственно. Спектры поглощения этих кристаллов демонстрируют широкие полосы и острые пики поглощения, но технология изготовления устройств из монокристаллов является сложной и дорогостоящей.

Возможность комбинировать разные свойства полимеров и монокристаллов в одном материале перспективна. Решение этой проблемы традиционными способами трудновыполнимо, поскольку свойства этих материалов отражают их различную внутреннюю структуру [1].

Метод наноструктурирования позволяет объединить свойства полимеров и кристаллов. В результате нанокомпозит является смесью неорганических наночастиц, в том числе полупроводниковых, равномерно распределенных в полимерной матрице. При условии равномерного распределения наночастиц и малого размера таких нанокристаллов (2 – 5 нм) они не искажают падающую световую волну и, следовательно, рассеяние света мало. С другой стороны, небольшое расстояние между нанокристаллами предусматривает существенное изменение оптических свойств, например увеличение показателя преломления. Следовательно, при достаточно высокой концентрации нанокристаллов с малым размером нанокомпозит становится фактически однородной средой, в которой при низком значении светорассеяния происходит значительное изменение показателя преломления. Комплекс свойств этой смеси определяется компонентами, а именно – полимерами и нанокристаллами, а также отношением их концентрации [2].

В настоящее время проявляется большой интерес к оптическим наноматериалам. Однако, несмотря на разнообразие исследований, практически отсутствуют данные об оптических материалах, в которых высокая концентрация наночастиц сочетается с хорошими оптическими свойствами.

Действительно, высокая концентрация структурирующих добавок может и обычно сопровождается значительным светорассеянием на них или на флуктуациях их концентрации. Поэтому создание материалов, сочетающих оптические свойства с высокой концентрацией наночастиц, является сложной задачей. Введение наночастиц металлов и их оксидов в полимерные матрицы в последние годы является интенсивно развиваемой областью физикохимии наноразмерного состояния. Структурная организация таких наноразмерных частиц –

серьезнейшая проблема, без решения которой трудно определить и оптимизировать области их практического использования.

Стабилизация наночастиц полимерами рассматривается как экранирование защитным коллоидом. Она создается за счет того, что пространственные размеры низкомолекулярных полимеров соизмеримы с радиусом действия Ван-дер-Ваальсовых сил (дисперсионного взаимодействия) или превышают его. Необходимость повышения устойчивости нанокомпозитов и контроль над обратимыми переходами в таких системах привлекает все более пристальное внимание исследователей к поиску путей управления их морфологией, структурной организацией и архитектурой.

Цель выполненной работы (обзора) – поиск и анализ данных и результатов теоретических и экспериментальных исследований, материалов диссертаций, литературных источников и патентов в области оптического и оптико-электронного приборостроения; обобщение полученных данных и рекомендаций по разработке методов дисперсии наночастиц в полимерные матрицы при создании оптически прозрачных нанокомпозитов для применения не только в оптических устройствах, но и для изделий в сцинтилляционной технике, светотехнике, фотовольтаике и во многих других областях науки и техники.

Свойства нанополимерных материалов

Синтез новых материалов с улучшенными свойствами и эксплуатационными качествами постоянно дополняется новыми методами в химии и материаловедении [3]. В процессе синтеза способность управлять молекулярной структурой на атомном и макроскопическом уровне является одним из ключевых параметров при проектировании материалов для специальных применений.

Значительным шагом вперед в этой области является синтез нанокомпозитов, когда можно контролировать структурный порядок в материале на нанометровых или субмикронных масштабах. Несмотря на то, что материалы, обладающие такой сложной структурой, широко распространены в природе, надежные и универсальные методы подготовки синтетических нанокомпозитов остаются интересной задачей, которая решается исследовательскими группами по всему миру [4].

Наночастицы, синтезируемые разными способами, могут иметь различные внутренние структуры, которые влияют на свойства материалов, сделанных из них. Полной обработки наночастиц довольно сложно добиться на практике, сложно сохранить нанометровый масштаб их размеров, избежать образования агломератов. Из-за своей высокой удельной поверхности наночастицы обладают высокой реакционной способностью, и существует большая вероятность агломерации. Большое количество граничных зерен в нанокристаллических материалах имеет решающее значение для сохранения микроструктуры в нанометровом масштабе в процессе консолидации в таких материалах.

Для достижения низкого уровня светорассеяния в прозрачных нанополимерах необходимы эффекты самоорганизации квазирешетки, имеющей упорядоченное расположение наночастиц. В этом случае можно получить однородность среды и отсутствие искажения света, проходящего через нее. Данная среда будет описываться в приближении гомогенной, а не дисперсной среды. Таким образом, для понижения уровня светорассеяния необходимо создать упорядоченную систему наночастиц в объеме полимерного материала (рис. 1).

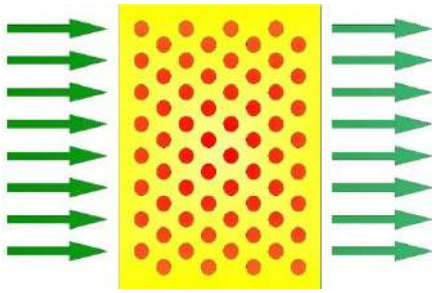


Рис. 1. Светорассеяние в упорядоченной системе наночастиц в объеме полимерного материала

В то же время наночастицы в нанокомпозите стремятся коагулировать или сформировать нерегулярное расположение, при котором концентрация наночастиц будет флуктуировать в соответствии со статистическим распределением. Такой материал будет иметь высокое светорассеяние при высокой концентрации наночастиц (рис. 2).

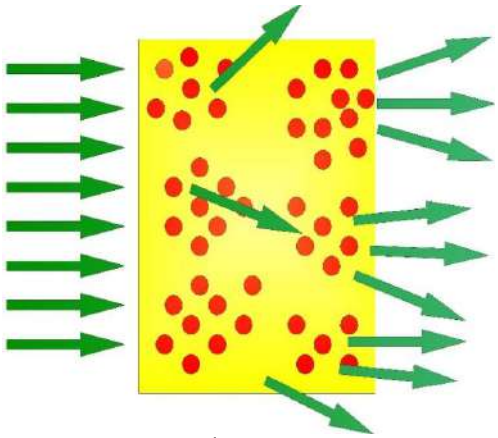


Рис. 2. Светорассеяние на микрофлуктуациях концентрации наночастиц

Таким образом, свойства наночастиц и нанокомпозитов на их основе сильно зависят от размера, концентрации, химического состава используемых наночастиц и многих других факторов. Но, в отличие от традиционных материалов оптического назначения, свойства нанокомпозитов можно улучшать, варьируя указанные выше параметры наночастиц [5].

Методы дисперсии наночастиц в полимерные матрицы

Межфазное взаимодействие является ключевым моментом при создании органо-неорганических композитов, и именно по этому признаку принято условное деление гибридных материалов на два основных класса. К первому классу гибридных материалов относятся нанополимеры со слабым взаимодействием между органической и неорганической частями. Ко второму – материалы, в которых органические и неорганические компоненты связаны посредством химических связей. В этом случае органические компоненты могут играть две различные роли – *сеткообразователей* или *модификаторов* неорганического компонента.

Нанокомпозиты первого класса получают путем прямого смешения наночастиц с матрицей полимера. При этом взаимодействие между полимерной матрицей и неорганическим компонентом относительно слабо и основано на водородных связях, а также на Ван-дер-Ваальсовых взаимодействиях. Низкая степень межфазного взаимодействия гидрофобной полимерной матрицы и гидрофильных частиц наполнителя приводит к агрегированию неорганических частиц, их неравномерному распределению в объеме полимерной матрицы. Таким образом, плохая адгезия на границе фаз является следствием ухудшения заявленных свойств полимерных нанокомпозитов и ограничивает их эффективное применение.

Для решения этой проблемы в процессе синтеза нанокомпозитов второго класса вводят различные стабилизирующие и модифицирующие добавки, позволяющие снизить поверхностную энергию на межфазной границе и повысить совместимость полимера и неорганического компонента. При этом наноструктурирование, как способ получения прозрачных нанокомпозитов, осуществляется путем химической реакции синтеза в разбавленном растворе нанокристаллов фиксированных размеров (порядка 20 – 50 нм) благодаря введению в зону синтеза органического вещества с поверхностно-активными свойствами (ПАВ), которое позволяет получать изолированные друг от друга и стабильные во времени кристаллы нужных размеров. При этом ПАВ (оболочка нанокристаллов) и матрица могут быть из одного или разных органических материалов. Наиболее устойчивые и оптически однородные композиции получаются с использованием в качестве защитной среды поливинилового спирта (ПВС) и поливинилпиридина (ПВП), а также фотографической желатины [6 – 8].

Среди большого числа нанодисперсных наполнителей полимерных матриц при получении композиционных материалов большим вниманием пользуются диоксид титана (TiO_2) и оксид цинка (ZnO). Нанокристаллические TiO_2 и ZnO являются широкозонными полупроводниками и обладают рядом достоинств (хорошая фотокаталитическая активность, высокая химическая и термическая стабильность, нетоксичность и низкая стоимость). Применение композитов, содержащих наночастицы ZnO и TiO_2, определяется, прежде всего, их фотокаталитическими свойствами (создание солнечных ячеек, УФ-фильтров, газовых сенсоров).

Использование гидрофильных полимерных матриц при синтезе нанокомпозитов с TiO_2 существенно облегчает получение гибридных органо-неорганических материалов. Плюсом данного метода является хорошая совместимость двух компонентов и отсутствие необходимости использования модификаторов. Одним из наиболее простых способов получения данных композитов является синтез из общего растворителя. В работе [9] были получены нанокомпозиты с TiO_2 на основе гидрофильных полимеров (поливиниловый спирт, частично гидролизованный поливинилацетат, поливинилпиролидон, поливинилпиридин) путем смешения растворов полимера и высокодисперсного раствора частиц TiO_2. Для получения высокодисперсного раствора TiO_2 в качестве прекурсора использовали $TiCl_4$, который гидролизовали в сильнокислой среде. Размер частиц (Dч) TiO_2 составлял 2,5 нм. Содержание TiO_2 в полимерных композитах варьировали от 2 до 35 мас. %. Полученные нанокомпозиты, содержащие более 24% TiO_2, использовали в качестве UV-фильтров (до 360 нм).

В последнее время большой интерес исследователей привлекают нанокомпозиты на основе биополимеров, поскольку такие материалы являются функциональными аналогами естественных природных материалов. Авторами работы [10] были получены нанокомпозиты на основе привитого сополимера хитозана (15 мас. %) с поливиниловым спиртом (ПВС) и нанодисперсного TiO_2 (Dч 4,5-5 нм). Пленки, содержащие 25 и 8 мас. % TiO_2, были приготовлены методом полива водных растворов сополимера и наночастиц TiO_2. Формирование частиц TiO_2 происходило при гидролизе третбутоксида титана.

Для большинства электронных устройств главной задачей является получение достаточно высокого уровня проводимости, что достигается допированием электропроводящих полимеров и созданием композитов. Известно, что композиты, сочетающие TiO_2 (полупроводник *n*-типа) в наносостоянии и проводящий полимер находят широкое применение в оптоэлектронике. В работе [11] были получены нанокомпозиты с TiO_2 (Dч – 21 нм) на основе матрицы полифениленвинилена (ПФВ) из общего растворителя ($CHCl_3$). Для синтеза нанокомпозитов использовали промышленный TiO_2 (Degussa P25), на 70 % состоящий из кристаллической фазы анатаз. Другим примером [12] является синтез органо-неорганических гибридных систем на основе матрицы полианилина (ПАНИ) и частиц TiO_2 (Dч – 9 нм) с массовым содержанием 17, 18, 30 и 39 мас. %. Синтез композитов проводили из общего растворителя, в качестве прекурсора использовали изопропоксид титана.

Использование гидрофобных матриц для создания нанокомпозитов с TiO_2 является более сложной задачей. Введение наполнителей, термодинамически несовместимых с полимерной матрицей, может сопровождаться образованием больших агрегатов, ухудшающих свойства конечного нанокомпозита. Проблему агрегации можно преодолеть с помощью модификации частиц TiO_2, либо полимерной матрицы, а также добавления в систему различных стабилизаторов. Модифицировать поверхность неорганического компонента можно с помощью поверхностно-активных веществ и связующих агентов путем адсорбции или ковалентного связывания последних на поверхности неорганических частиц (рис. 3). В работе [13] предложены методы получения композитов с различным содержанием TiO_2 (0,25; 0,5; 1; 2; 5; 10 и 13 мас.%) на основе сополимера этилен-винилового спирта и полипропилена (ПП) (0,5; 1; 2; 5 мас.%) путем смешения расплава с частицами TiO_2. Для формирования композитов на основе ПП использовали привитой сополимер ПП с малеиновым ангидридом, последний выступал в качестве связующего агента для стабилизации частиц TiO_2 в полимерной матрице и предотвращения их возможной агрегации. Результатом модификации

полимера являлось получение гибридных композитов, содержащих частицы TiO_2, размер которых составил ~ 10 нм.

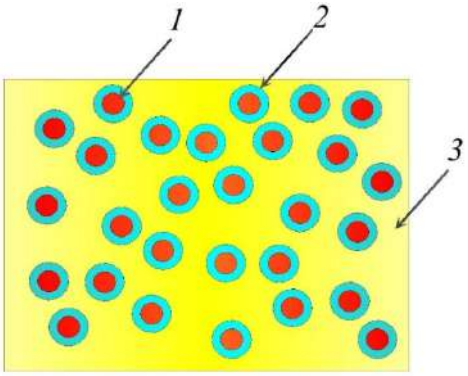


Рис. 3. Структурная модель нанокомпозита: *1* – нанокристалл неорганического полупроводника; *2* – оболочка из органического материала; *3* – органическая (жидкая или твердая) матрица

Для того чтобы улучшить совместимость между неорганическим материалом и полимерной матрицей и предотвратить агрегацию частиц, используют метод химической модификации поверхности неорганического компонента. В качестве модификаторов частиц TiO_2 часто используют различные силановые агенты, которые способны химически связываться с их поверхностью, в то время как наличие в их молекулах гидрофобных радикалов улучшает совместимость неорганических частиц с полимерной матрицей. Один из способов формирования органо-неорганических гибридных систем заключается в полимеризации мономера на поверхности частиц TiO_2 (при наличии или отсутствии модификаторов). В работе [14] описан метод получения нанокомпозитов путем полимеризации стирола, химически связанного с поверхностью модифицированных частиц TiO_2**.** Содержание частиц TiO_2 в композитах на основе полистирола варьировали от 0,5 до 2,0 мас. %. Авторы работы [15] путем проведения полимеризации метилметакрилата получили композиты со структурой, подобной ореху, когда ядро из модифицированных частиц TiO_2 (Dч – 260 нм) заключено в “скорлупу” из полиметилметакрилата.

Итак, с помощью химической модификации поверхности частиц TiO_2 можно решить вопрос, связанный с термодинамической несовместимостью компонент, входящих в состав нанокомпозита. Использование данного метода дает возможность предотвратить процесс агрегации частиц и получить полимерные нанокомпозиты с высоким уровнем дисперсности неорганического компонента.

В одном из вариантов изготовления нанополимеров, введение наночастиц ZnO в полисилоксансодержащие эпоксиуретановые полимеры осуществляли методом интеркаляции: порошкообразные наночастицы ZnO растворяли в смеси растводителей (30 мас.% этилового спирта +70 мас.% ксилола) при массовом соотношении 8:2, чтобы вызвать набухание наноразмерных частиц в растворителе. Затем этот раствор подвергали магнитному перемешиванию со скоростью вращения 800 об/мин в течение 30 мин, затем в течение 15 мин обрабатывали ультразвуком. Растворенные наночастицы добавляли к полимеру и перемешивали в течение 20 мин при 1000 об/мин, затем проводили 15 мин обработку ультразвуком перед добавлением отвердителя.

Исследование разработанных покрытий на основе полисилоксансодержащих эпоксиуретановых олигомеров, модифицированных наночастицами ZnO, показало, что они обладают высокой гидрофобностью, устойчивостью к действию окружающей среды и антикоррозионными свойствами [16].

В работе [17] в одном из примеров из области создания наноматериалов для сцинтилляционной техники, а именно для пластмассовым сцинтилляторов (ПС), описан метод создания трехкомпонентного ПС (полимерная основа, первичный люминофор, вторичный люминофор). ПС состоит из полимерной основы, которая содержит первичный и вторичный люми-

нофоры, соединенные атомами кремния в наноразмерные разветвленные макромолекулы. В качестве полимерной основы может быть использован любой полимер из группы винилароматических полимеров, например полистирол. Первичный люминофор выбирается из группы соединений, у которых максимум длинноволновой полосы спектра поглощения находится в интервале от 270 до 350 нм. При этом квантовый выход флуоресценции составляет не менее 5 %.

Вторичный люминофор выбирается из группы соединений, у которых максимум длинноволновой полосы спектра поглощения находится в интервале от 330 до 400 нм. При этом квантовый выход флуоресценции составляет не менее 30 %. Увеличение светового выхода сцинтиллятора и сокращение длительности сцинтилляции достигается благодаря тому, что в наноразмерной разветвленной макромолекуле с заявляемыми параметрами эффективность безызлучательного переноса энергии электронного возбуждения от звеньев первичного к звеньям вторичного люминофора может достигать 100 %.

Заготовку сцинтиллятора получают, смешивая наноструктурированный наполнитель с полимером, выбранным в качестве основы, в двухшнековом смесителе с возвратным каналом (при температуре 180°С и частоте вращения шнеков 600 об/мин).

В работе [18] описана кремнийорганическая композиция для соединения оптических элементов и метод создания кремнийорганической смазочной композиции, которая обеспечивает максимальное светопропускание в контакте оптических устройств, устойчива в диапазоне температур минус 70°С плюс 200°С. Для соединения и герметизации оптических элементов на основе пластичной основы и загустителя предложена новая композиция, состоящая из основы – смеси полидиметилсилоксановой (ПМС) и полиметилфенилсилоксановой (ПФМС) жидкости с вязкостью от 3000 до 40000 мм^2/с при температуре 20°С и загустителя диоксида кремния. Для создания такой композиции в емкость, снабженную обогревателем, перемешивающим устройством и термометром, загружают 180 – 270 г ПМС жидкости с вязкостью 1000 – 20000 мм^2/с и 270 – г ПФМС жидкости с вязкостью 10000 – 20000 мм^2/с. Содержимое емкости перемешивают и получают 450 г смеси с вязкостью 3000 – 20000 мм^2/с, являющуюся основой композиции, затем добавляют 20 – 50 г порошка диоксида кремния, массу нагревают до температуры 40 – 60°С и перемешивают в течение 3 – 4 часов.

В работе [19] описан процесс эффективного диспергирования порошка наночастиц Al_2O_3 в бисерной мельнице. Получаемые сегодня неорганические порошки обладают размером частиц в субмикронном или наноразмерном диапазоне с достаточно узким распределением на гранулометрической кривой. В процессе хранения и транспортировки частицы слипаются, образуя конгломераты. Применение такого порошка приведет к формированию дефектов в структуре нанополимеров. Поэтому обязательным этапом при производстве нанополимеров является диспергирование мелкодисперсных и наноразмерных порошков.

Однако высокоэффективное механическое измельчение возможно лишь в присутствии диспергаторов и эмульгаторов – поверхностно-активных веществ, снижающих поверхностную энергию диспергируемых твердых тел или жидкостей. Кроме того, они препятствуют агрегации, т. е. слипанию мелких частиц и слиянию капель.

Эффективность процесса измельчения зависит от метода диспергирования. Как правило, процесс диспергирования порошков осуществляется на бисерных и шаровых мельницах. Использование бисерных мельниц по сравнению с шаровыми позволяет значительно сократить время помола от нескольких суток до одного-двух часов.

Для проведения исследований была приготовлена 30 % (по объему) водная суспензия порошка Al_2O_3. Для предотвращения слипания частиц в процессе диспергирования в суспензию был добавлен дифлокулянт Dolapix производства компании Zschimmer & Schwartz в количестве 2 % от веса порошка. При проведении исследований использовался порошок Al_2O_3 SG марки CT-3000 производства компании Almatis (Германия). Диспергирование производили на бисерной мельнице Netzsch MiniCer.

Диспергирование на бисерной мельнице производили при скорости вращения вала 3000 об/мин, давлении 6,2 бар и температуре суспензии 28 ^{o}C. При диспергировании на шаровой мельнице скорость вращения барабана составляла 90 об/мин. Барабан заполняли суспензией и шарами на 45 % в соотношении 5:1. Время помола составляло 48 часов. Исследования показали, что при работе с исходным порошком Al_2O_3 CT3000 SG производства компании Almatis для достижения характеристик порошкового материала, заявленного производителем, диспергирование на бисерной мельнице с мелющими телами из диоксида циркония диаметром 1 мм необходимо производить в течение 50 – 60 мин.

Большой интерес для разработки нанокомпозитов представляют соединения редкоземельных элементов (РЗЭ), в том числе фториды лантаноидов. Они обладают прозрачностью в широкой спектральной области (от 0,2 до 6 мкм), более высокой влагостойкостью по сравнению с другими классами веществ, обладающих широким окном пропускания, высокой теплопроводностью, и т.д.

В работе [20] описан процесс получения полимерных пленочных материалов, содержащих нанокристаллы фторида празеодима PrF_3. При этом в качестве матрицы для их введения применялся желатин как пленкообразующий полимер, который наряду с прозрачностью в видимой области спектра обладает свойствами ПАВ. В работе использовались желатин и нанокристаллы PrF3, полученные по реакции взаимодействия нитрата празеодима с фторидом натрия:

$$Pr(NO_3)_3 + 3\ NaF = PrF_3 + 3\ NaNO_3.$$

Эта реакция протекает в водном растворе при контроле pH (pH = 4-5). Наноразмерный характер (30x50 нм) синтезированных таким образом частиц PrF_3 подтвержден данными атомной электронной микроскопии. В свежеприготовленный 10%-й водный раствор желатина вводилось расчетное количество нанокристаллов PrF_3. Диспергирование нанокристаллов в водно-желатиновых растворах проводилось на установке ИЛ100-6/4, позволяющей осуществлять обработку жидких сред ультразвуком. Полимерные пленки получали путем полива приготовленного полимерного раствора на подложки из кварцевого стекла или фторопласта. Поверхности названных подложек предварительно обрабатывались (обезжиривались) этиловым спиртом. Полученные образцы выдерживались при комнатной температуре до полного улетучивания растворителя в течение ~12 часов. При этом толщина полученных желатиновых пленок варьировалась от 100 до 380 мкм.

Для получения исходных нанокомпозиций были апробированы две методики диспергирования нанопорошка PrF_3 в водно-желатиновом растворе с использованием ультразвука. Первая заключалась в том, что действию ультразвука подвергалась заранее приготовленная дисперсия нанопорошка PrF_3 в водно-желатиновой среде. Вторая методика отличалась тем, что сначала проводилось ультразвуковое диспергирование данных нанокристаллов в водной среде и лишь после этого в данную дисперсную систему при постоянном перемешивании вводился раствор желатина. При этом во втором случае образовывалась гораздо более устойчивая дисперсная система с более равномерным распределением по объему высокодисперсной фазы. Это объясняется тем, что ультрадиспергирование нанопорошка PrF_3 первоначально в воде происходит наиболее эффективно из-за ее меньшей вязкости (в сравнении с водно-желатиновой средой). Поэтому при последующем растворении в этой дисперсии желатин, как полимерного ПАВ, на поверхности наночастиц образуются гидрофильные слои (оболочки), препятствующие объединению (укрупнению) наночастиц.

Одним из наиболее распространенных и эффективных методов защиты полимеров от ультрафиолетового излучения является использование различных дисперсных материалов (наполнителей). Например, порошки оксида цинка с размером частиц от 0.5 до 20 мкм в состав большого числа косметических препаратов и светостабилизаторов, применяемых в полимерной промышленности. Одной из важнейших функций этих порошков является защита полимера от излучения ультрафиолетового диапазона. Замена микрочастиц ZnO на

частицы нанометрового диапазона представляет большой практический интерес, поскольку позволяет существенно уменьшить содержание светостабилизаторов одновременно с сохранением или улучшением необходимых свойств. Таким образом, разработка методов управления физико-химическими параметрами и оптическими свойствами дисперсий на основе наночастиц оксида цинка в процессе их синтеза позволяет не только создать эффективные светостабилизаторы для использования в полимерной и косметической отраслях промышленности, но и снизить экономический ущерб от разрушения полимерных материалов под действием солнечного излучения. В связи с этим разработка таких систем представляет значительный научный и практический интерес.

Существует множество методов синтеза наночастиц ZnO с различными формами и размерами, в том числе метод лазерной абляции, который является удобным и универсальным способом получения наносуспензий твердофазных материалов в жидкости. При этом, варьируя технологические режимы лазерного воздействия, материал мишени и жидкую среду, можно получать различные по составу, размеру и свойствам нанодисперсные продукты в жидкости. В работах [21 – 23] представлены результаты изучения характеристик продуктов, полученных импульсной лазерной абляцией окиси цинка в жидких средах. Взаимодействие импульсного лазерного излучения с цинковой мишенью создает область плазмы над поверхностью мишени, которая состоит из атомов и кластеров цинка. Плазма расширяется адиабатически и создает ударную волну на границе раздела, повышая давление и температуру. При высоких давлениях и температурах цинк окисляется водой и коагулирует. Образовавшиеся кластеры индуцируют дальнейший рост наночастиц. После исчезновения области плазмы, которая поддерживается лазерным излучением, размер частиц увеличивается относительно медленно, из-за того что поверхность наночастиц покрыта молекулами ПАВ. Наночастицы могут быть поликристаллическими или почти аморфными из-за развития процессов коагуляции и коалесценции. Следует отметить, что наночастицы устойчивы к коалесценции до определнного уровня, который близок к 20 нм. Так как наночастицы ZnO в водном растворе заряжены положительно из-за неокончательного окисления, то заряженные поверхности могут стать главным фактором преодоления Ван-дер-Ваальсовых сил между наночастицами.

Основные преимущества лазерной абляции в жидкости – техническая простота и химическая чистота. Однако применение ПАВ для ограничения коалисценции наночастиц часто приводит к большой дисперсии размеров. Введение молекул ПАВ может привести к потере одного из основных преимуществ лазерной абляции в водном растворе, поскольку снижается удельная поверхность наночастиц. В работе [23] наночастицы ZnO были получены методом импульсной лазерной абляции (ИЛА) из цинковой мишени в водном растворе. Таким методом получаются наночастицы ZnO с очень узким распределением по размерам. Авторами обнаружено, что наночастицы ZnO, полученные в растворе NaCl, сильно коалесцируют. Замечено, что величина экситонной эмиссии в области зеленого излучения постепенно увеличивается при снижении среднего размера частиц. Это означает, что на большей площади поверхности у более мелких наночастиц образуется больше кислородных дефектов. Результаты экспериментов, представленные в указанной выше работе, демонстрируют, что после пассивации наночастиц поверхностно-активным веществом (лаурилбетаиндиметиламиновой кислотой) и снижения поверхностного заряда наночастицы ZnO могут излучать в «зеленой» области за счет кислородных дефектов на поверхности. Среда, в которой синтезируются наночастицы ZnO с помощью лазерной абляции, оказывает сильное влияние на спектр поглощения. Поглощение наночастиц ZnO, полученных в HCl и NaOH, намного больше в УФ-диапазоне, чем у наночастиц, полученных в деионизированной воде. Высокий по абсолютной величине поверхностный заряд наночастиц, полученных в HCl или NaOH растворе, ведет к увеличению силы отталкивания между наночастицами и подавлению их роста за счет коагуляции. Спектры демонстрируют сильное поглощение в диапазоне длин волн до 400 нм.

Тем не менее, за последнее время лазерная абляция под слоем жидкости стала перспективной технологией для синтеза наночастиц. Такие преимущества перед другими способами

синтеза наночастиц, как простота метода, экологичность, низкая стоимость, сделали лазерную абляцию в жидкой среде популярной среди исследователей. Что также немаловажно, этот метод позволяет получать более чистые коллоидные растворы без использования поверхностно-активных веществ и других примесей.

Заключение

Анализ рассмотренных работ позволяет сделать вывод, что для создания гибридных органо-неорганических композитов с высоким уровнем дисперсности неорганического компонента приходится решать проблемы, связанные с совместимостью компонент и стабилизацией наночастиц наполнителя в полимерной матрице. В связи с ограниченным кругом гидрофильных полимеров, способных к формированию композитов с наночастицами без стабилизаторов, основными подходами к получению гибридных композитов являются использование модифицирующих добавок поверхностно активных веществ и проведение сложных химических реакций на поверхности наночастиц неорганического наполнителя. Данные способы получения нанокомпозитов с наночастицами трудоемки, связаны с образованием побочных продуктов и дополнительной очисткой. При этом, вследствие отличий в химической природе полимеров, для каждого из них требуется индивидуальный подход в выборе модифицирующей добавки и способа стабилизации.

В то же время использование наночастиц в полимерах не следует рассматривать как однозначное положительное решение всех проблем. К их практическому применению в составе полимерных матриц следует подходить продуманно, с учетом конечных целей исследований. В этой связи приобретают актуальность планирование исследований для выбора приоритетных свойств нанокомпозитов и поиск новых подходов для улучшения качеств гибридных композитов для оптических и оптико-электронных устройств на основе широкого круга полимеров и наночастиц.

Список литературы:

1. Герасин В.А., Антипов Е.М., Карбушев В.В., Куличихин В.Г., Карпачева Г.П., Тальрозе Р.В., Кудрявцев Я.В. Новые подходы к созданию гибридных полимерных нанокомпозитов: от конструкционных материалов к высокотехнологичным применениям // Успехи химии. 2013. Т. 82. № 4. С. 303–332.
2. Denisyuk I.Yu., Williams T.R., Burunkova J.E. Hybrid Optical Material with Nanoparticles at High Concentrations in UV-Curable Polymers – Technology and Properties // Molecular Crystals and Liquid Crystals. 2008. Vol. 497. P. 142–153.
3. Шапорев А.С., Ванецев А.С., Кирюхин Д.П., Соколов М.Н., Бузник В.М. Синтез полимерных композитов на основе золей ZnO, CeO_2 и Gd_2O_3 // Конденсированные среды и межфазные границы. 2011. Т. 13. № 3. С. 374–380.
4. Трофимчук Е.С., Никонорова Н.И., Нестерова Е.А., Музафаров А.М., Мешков И.Б., Волынский А.Л., Бакеев Н.Ф. Получение пленочных композитов на основе крейзованных полимеров и наночастиц силиказоля // Российские нанотехнологии. 2009. Т. 4. № 9. С. 164–166.
5. Позднякова С.А. Струкурирование и самоорганизация нанокомпозитов в поле световой волны : дис. … канд. физ.-мат. наук. 2014. 120 с.
6. Полянская В.В. Органо-неорганические нанокомпозиты на основе оксидов металлов и полиолефинов, деформированных по механизму крейзинга : дис. … канд. хим. наук. 2015. 138 с.
7. Серова В.Н. Оптические и другие материалы на основе прозрачных полимеров : монография / Федер. агентство по образованию. Казан. гос. технол. ун-т. Казань : КГТУ, 2010. 540 с.
8. Бурункова Ю.Э., Денисюк И.Ю., Шекланова Е.Б., Фокина М.И. Оптические полимерные нанокомпозиты. СПб : Ун-т ИТМО, 2017. 80 с.
9. Nussbaumer R. J., Caseri W. R., Smith P., Th Tervoort. Polymer-TiO_2 nanocomposites: a route towards visually transparent broadband UV filters and high refractive index materials // Macromol. Mater. Eng. 2003. V. 288. № 1. P. 44-49.
10. Озерин А. Н., Перов Н. С., Зеленецкий А. Н., Акопова Т. А., Озерина Л. А., Кечекьян А. С., Сурин Н. М., Владимиров Л. В., Юловская В. Д. Гибридные нанокомпозиты на основе привитого сополимера хитозана с поливиниловым спиртом и оксида титана // Российские нанотехнологии. 2009. Т. 4. № 5-6. С. 76-79.
11. Baratony M.-I., Merhariz L., Wangx J., Gonsalves K. E. Investigation of the TiO_2/PPV nanocomposite for gas sensing applications // Nanotechnology. 1998. V. 9. № 4. P. 356-359.
12. Shnitzler D.C., Zabrin J.G. J. Organic/Inorganic hybrid materials formed from TiO_2 nanoparticles and polyaniline // Braz. Chem. Soc. 2004. V. 15. No №3. P. 378-384.

13. Jimenez Rioboo R.J., De Andres A., Kubacka A., Fernandez-Garcia M., Cerrada M.L., Serrano C. Influence of nanoparticles on elastic and optical properties of a polymeric matrix: Hypersonic studies on ethylene–vinyl alcohol copolymer-titania nanocomposites // Europ. Polym. J. 2010. V. 46. P. 397-403.

14. Rong Y., Chen H.-Z., Wu G., Wang M. Preparation and characterization of titanium dioxide nanoparticle/polystyrene composites via radical polymerization // Materials Chemistry and Physics. 2005. V. 91. No 2-3. P. 370-374.

15. Caris C. H. M., Van Elven L. P. M., Van Herk A. M., A. L. German. Polymerization of MMA at the surface of inorganic submicron particles // British Polymer Journal. 1989. V. 21. No 2. P. 133-140.

16. Нгуен Ван Нган. Разработка композиционных материалов на основе эпоксисодержащих олигомеров с повышенной химической и биологической стойкостью : дис. …канд. хим. наук / Нгуен Ван Нган. 2019. 139 с.

17. Патент РФ № 2380726 Пластмассовый сцинтиллятор с наноструктурированными люминофорами. Публикация патента: 27.01.2010 г.

18. Патент РФ № 2505569 Кремнийорганическая композиция. Публикация патента: 27.01.2014 г.

19. Горяйнова О.А., Мельникова Е.В., Кузьмин К. Эффективность диспергирования порошка Al_2O_3 в бисерной мельнице / Новосибир. гос. техн. ун-т // XX Междунар. науч.-практ. конф. «Современные техника и технологии». 2013. Секция 6: Материаловедение.

20. Серова В.Н., Идрисов Р.А., Шевцова С.А., Морозов О.А., Ловчев А.В. Получение полимерных пленочных материалов, содержащих нанокристаллы фторида празеодима // Вестник Казан. гос. технол. ун-та. Казань, 2014. С.152-154.

21. Semaltianos N.G., Logothetidis S., Frangis N., Tsiaoussis I., Perrie W., Dearden G., Watkins K.G., Chem. Phys. Lett. 496 (2010) 113.

22. Kim K.K. et al. Formation of ZnO nanoparticles by laser ablation in neat water / Chemical Physics Letters 511 (2011) 116–120.

23. Ch. He, Sasaki T., Usui H., Shimizu Y., Koshizaki N. Fabrication of ZnO nanoparticles by pulsed laser ablation in aqueous media and pH-dependent particle size: An approach to study the mechanism of enhanced green photoluminescence // Journal of Photochemistry and Photobiology A: Chemistry 191 (2007) 66–73.

Поступила в редколлегию 05.02.2021

Сведения об авторах:

Борщев Вячеслав Николаевич – д-р техн. наук, профессор, ООО «Научно производственное предприятие «ЛТУ», первый заместитель директора – главный конструктор; Украина; e-mail: viatcheslav.borshchov@cern.ch; ORCID: https://orcid.org/0000-0002-5579-8932

Листратенко Александр Михайлович – канд. техн. наук, ООО «Научно производственное предприятие «ЛТУ», ведущий научный сотрудник; Украина; e-mail: sasha.listratenko.12@gmail.com; ORCID: https://orcid.org/0000-0001-7643-5295

Проценко Максим Анатольевич – канд. техн. наук, ООО «Научно производственное предприятие «ЛТУ», начальник отделения – заместитель главного конструктора; Украина; e-mail: max.protsenko.1978@gmail.com; ORCID: https://orcid.org/0000-0001-9313-1701

Тымчук Игорь Трофимович – канд. техн. наук, ООО «Научно производственное предприятие «ЛТУ», главный технолог; Украина; e-mail: ihortymchuk78@gmail.com; ORCID: https://orcid.org/0000-0002-6436-7253

Кравченко Александр Викторович – ООО «Научно производственное предприятие «ЛТУ», научный сотрудник; Украина; e-mail: kravcenkoaleksandr671@gmail.com; ORCID: https://orcid.org/0000-0002-7145-4304

Судья Александр Валерьевич – ООО «Научно производственное предприятие «ЛТУ», научный сотрудник; Украина; e-mail: 4el1195@gmail.com; ORCID: https://orcid.org/0000-0002-2403-979X

Слипченко Николай Иванович – д-р физ.-мат. наук, профессор, Институт сцинтилляционных материалов НАНУ, ведущий научный сотрудник; Украина; e-mail: naukovets.big@gmail.com; ORCID: https://orcid.org/0000-0002-4242-4800

Чичков Борис Николаевич – д-р техн. наук, профессор, Институт квантовой оптики, Ганноверский университет имени Лейбница, заведующий лабораторией нанопроизводства; Германия; e-mail: chichkov@iqo.uni-hannover.de; ORCID: https://orcid.org/0000-0002-8129-7373

УДК 681.128.82 **DOI:10.30837/rt.2021.1.204.13**

Б.В. ЖУКОВ, канд. техн. наук, А.В. ОДНОВОЛ

КОНТРОЛЬ РАЗНОСТИ УРОВНЕЙ ЖИДКОСТИ В СМЕЖНЫХ РЕЗЕРВУАРАХ

Введение

Для систем охлаждения тепловых и атомных электростанций используют воду расположенных в непосредственной близости водохранилищ. Чтобы предотвратить попадание водорослей и других посторонних продуктов в систему охлаждения в водохранилище устанавливают сетку, после которой производят забор охлаждающей жидкости. В процессе эксплуатации такой системы возможно засорение заграждающей сетки, что приводит к снижению ее пропускной способности, а значит и объема охлаждающей жидкости, поступающей в систему охлаждения электростанций. Поэтому возникает необходимость текущего контроля пропускной способности заграждающей сетки. С этой целью производят текущий контроль уровня охлаждающей жидкости до и после заграждающей сетки.

До настоящего времени контроль уровней осуществляют с помощью двух поплавковых уровнемеров, один из которых устанавливается до заграждающей сетки, а второй – после нее. На рис.1 приведена возможная схема установки уровнемеров, где 1 – измерительная труба уровнемера 4, установленного до заграждающей сетки 2, а 3 – измерительная труба уровнемера 5, установленного после заграждающей сетки 2.

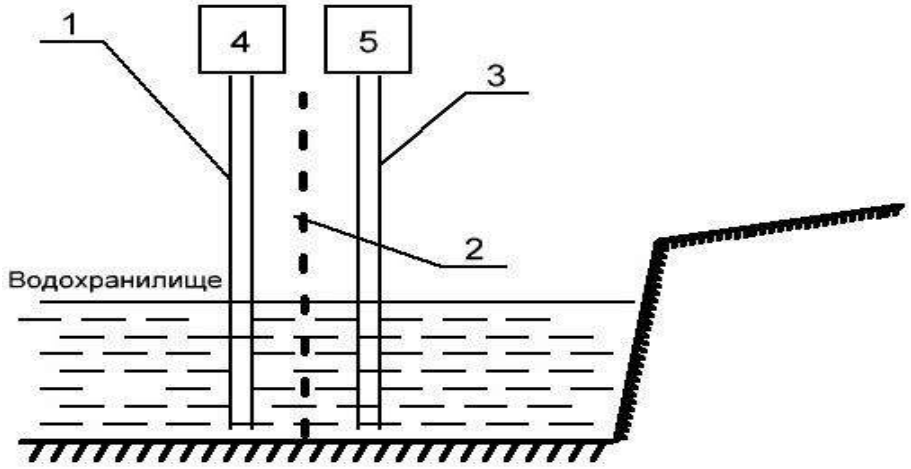


Рис.1. Установка уровнемеров

К недостатку использования двух отдельных устройств измерения уровня следует отнести необходимость дополнительной системы измерения разности уровней, которая несет информацию о пропускающей способности заграждающей сетки. Кроме того, необходим текущий контроль работоспособности каждого уровнемера.

В работе рассмотрена возможность создания специализированного уровнемера, обеспечивающего синхронный текущий контроль уровней и разности уровней жидкости в двух смежных резервуарах.

Основная часть

В [1, 2] предложен вариант использования уровнемера с плоской акустической волной для контроля уровня и скорости потока в безнапорных водоводах. В этом варианте общий волноведущий тракт разветвлялся на два раздельных канала, один из которых использовался для контроля уровня, а второй, заканчивавшийся трубкой Пито, – скорости потока.

Если первый из волноведущих каналов расположить в водохранилище до разделительной сетки, а второй (без трубки Пито) – после нее, то такой вариант уровнемера обеспечит

возможность синхронного контроля уровней жидкости до и после заградительной сетки, а также разности уровней в обеих частях водохранилища.

Структурная схема такого уровнемера, который может быть реализован как в акустическом, так и радиочастотном диапазонах волн, приведена на рис. 2.

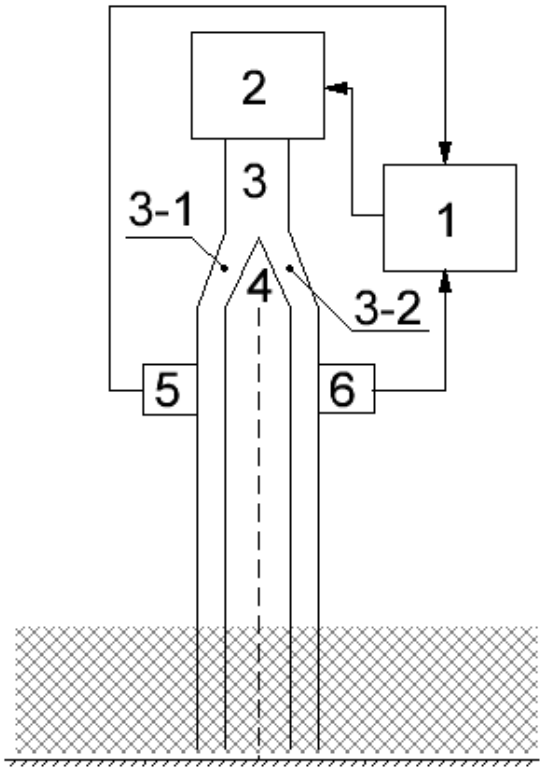


Рис. 2. Уровнемер для контроля разности уровней жидкости

В состав уровнемера для контроля разности уровней жидкости входят:

1 – процессорный блок управления и обработки результатов измерения уровней в обоих каналах;

2 – источник излучения импульсного сигнала;

3 – волновод общий, 3-1 – волновод канала перед заградительной сеткой, 3-2 – волновод канала после заградительной сеткой;

4 – заградительная сетка;

5 – приемник сигнала канала до заградительной сетки;

6 – приемник сигнала канала после заградительной сетки.

Уровнемер (рис. 2), реализованный в акустическом диапазоне волн, работает следующим образом. После подключения питания в блоке обработки 1 вырабатывается импульс запуска (ИЗ) (рис. 3, *а*), который поступает в источник излучения, где преобразуется в акустический импульсный сигнал, который излучается в общий волноведущий тракт 2.

В тройнике общего волноведущего тракта 3 [3] происходит разделение импульсного акустического сигнала на два канала:

3-1 – волновода, установленного до разделительной сетки;

3-2 – волновода, установленного после разделительной сетки.

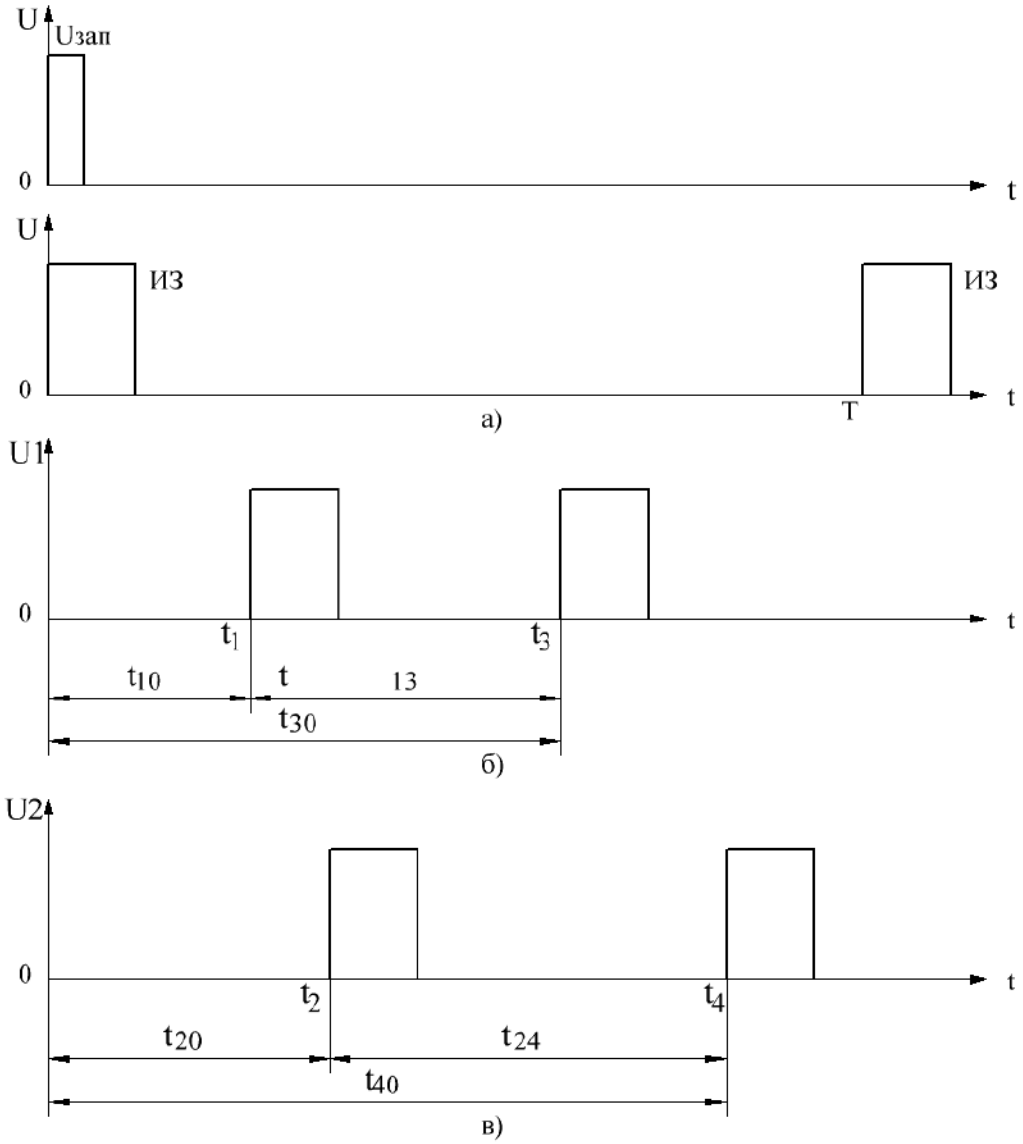


Рис. 3. Временные диаграммы

Излученный (прямой) сигнал (рис. 3, *а*) по волноведущему тракту 3-1 в момент времени t_1 достигает плоскости установки приемника 5 канала до заградительной сетки, поступает на его вход, где усиливается и преобразуется в видеоимпульс (рис. 3, *в*), который поступает в блок обработки 1. Одновременно излученный (прямой) сигнал по волноведущему тракту 3-2 в момент времени t_2 достигает плоскости установки приемника 6 канала после заградительной сетки, поступает на его вход, где усиливается и преобразуется в видеоимпульс, который также поступает в блок обработки 1.

Пройдя плоскости установки приемников 5 и 6, излученные сигналы по волноведущим трактам 3-1 и 3-2 достигают поверхности жидкости. Отраженные сигналы в моменты времени t_3 и t_4 вновь поступают на входы приемников 5 и 6, где они усиливаются и преобразуются в видеоимпульсы (рис. 3, *в*), поступающие также в блок обработки 1.

В блоке обработки вычисляются временные интервалы $t_{31} = t_3 - t_1$ и $t_{42} = t_4 - t_2$, которые используются для расчета расстояний R_1 и R_2 (рис. 4) от плоскостей установки приемников 5 и 6 до поверхности жидкости соответственно до и после заградительной сетки 4.

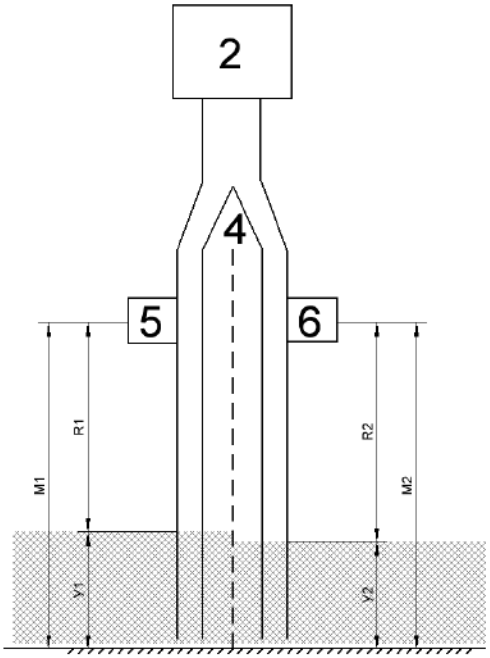


Рис. 4. Контролируемые расстояния и уровни

На рис. 4 M_1 и M_2 – максимальные уровни жидкости от дна резервуара (водохранилища), $R_1 = V(t^0)t_{31}/2$ и $R_2 = V(t^0)t_{42}/2$ – расстояния от плоскостей установки приемников 5 и 6 до поверхности жидкости до и после заградительной сетки, $V(t^0)$ – скорость распространения акустической волны, а $Y_1 = M_1 - R_1$ и $Y_2 = M_2 - R_2$ – измеряемые уровни жидкости от дна резервуара.

Применение единого для обоих каналов источника излучения импульсного сигнала 2 позволяет определить разность уровней между плоскостями установки приемников 5 и 6 (рис. 4) $M_2 - M_1 = V(t^0)\Delta t$, которая позволяет исключить погрешность высот установки приемников над дном резервуара (водохранилища).

Данные вычислений t_{31}, t_{42} и $\Delta t = t_{10} - t_{20}$ позволяют определить уровни жидкости Y_1 и Y_2, а также разность уровней до и после заградительной сетки:

$$Y_1 - Y_2 = (M_1 - M_2) - 0{,}5V(t^0)(t_{31} - t_{42}) = V(t^0)[\Delta t - 0{,}5(t_{31} - t_{42})].$$

Для устранения взаимного влияния условий распространения акустических волн в каналах до и после заградительной сетки 4 (рис. 2) в уровнемере, выполненном в акустическом диапазоне, устройство разделения общего канала 3 на каналы 3-1 и 3-2 должно удовлетворять условию [3]

$$S_3 = S_{3\text{–}1} + S_{3\text{–}2},$$

где S_3, $S_{3\text{–}1}$ и $S_{3\text{–}2}$ – соответственно площади внутренних сечений общего и разделенных волноведущих трактов.

Данное требование позволяет установить соотношение внутренних диаметров цилиндрических труб, используемых в качестве звуководов акустических волн $D_3 = \sqrt{2}D_{3\text{–}1} = \sqrt{2}D_{3\text{–}2}$, где D_3 и $D_{3\text{–}1} = D_{3\text{–}2}$ – соответственно внутренние диаметры труб общего 3 и разделенных 3-1 и 3-2 звуководов.

Использование двухканального приемного тракта при общем источнике акустических колебаний обеспечивает возможность синхронного контроля уровней жидкости в каждом

канале и разности уровней до и после заградительной сетки. При этом обеспечивается автоматический учет различия высот плоскостей приемников над плоскостью дна резервуара.

В расходомере для безнапорных водоводов [1] был использован акустический приемо-передатчик АП-7Т уровнемера ЗОНД-3М [4], в котором время прихода прямого и отраженного сигналов регистрируется в момент превышения заданного порога передним фронтом первого колебания самого импульсного сигнала, что позволяет измерить уровень жидкости с абсолютной погрешностью не хуже ±1мм. Данную величину погрешности уровнемер должен обеспечивать при контроле уровней охлаждающего масла в двух смежных резервуарах при допустимом диапазоне изменения уровней не более нескольких сантиметров.

Диапазон изменения уровней жидкости в водохранилищах систем охлаждения тепло и атомных электростанций может превышать рабочий диапазон приемо-передатчика АП-7Т, который составляет 10 – 12 м. Поэтому для контроля уровней жидкости в системах охлаждения ТЭС и АЭС необходимо использовать приемо-передатчик АП-70Т уровнемера -3М, рабочий диапазон которого превышает 20 м. В отличие от АП-7Т в приемо-передатчике АП-70Т время прихода прямого и отраженного сигналов регистрируется в момент превышения заданного порога передним фронтом огибающей импульсного сигнала. Поэтому абсолютная погрешность контроля уровня уровнемера с датчиком АП-70ВТ составляет около ±1см, что вполне удовлетворяет требованиям к контролю уровней жидкости в системах охлаждения ТЭС и АЭС.

Выводы

Двухканальный уровнемер с единым источником сигнала обеспечивает синхронный контроль уровней и разности уровней жидкости в двух смежных резервуарах и двух частях водохранилища до и после разделительной сетки.

В составе уровнемера ЗОНД-3М имеются приемо-передатчики, обеспечивающие необходимый диапазон контроля уровней и погрешность его измерения как в системах охлаждения ТЭС и АЭС, так и в системах охлаждения специализированных двигателей.

Список литературы:

1. Жуков Б.В., Одновол А.В., Борбульов С.І., Сосновчик Д.М. Патент на корисну модель № 82450. Пристрій для вимірювання об`ємної витрати рідини у відкритих каналах і закритих трубопроводах без напору. 12.08.2013.

2. Жуков Б.В., Одновол А.В., Акустический уровнемер – расходомер для контроля расхода жидкости в безнапорных водоводах // Радиотехника. 2016. Вып. 184.

3. Ржевкин С.Н. Курс лекций по теории звука. Москва : МГУ, 1960. 336с.

4. Жуков Б.В., Солярский Н.Ф. и др. Низкочастотные модификации акустических преобразователей уровнемера “ЗОНД-3М”// Датчики и системы. 2007. №.3. С.42 - 46.

Поступила в редколлегию 03.02.2021

Сведения об авторах:

Жуков Борис Владимирович – канд. техн. наук, старший научный сотрудник отдела физических основ радиолокации; Институт радиофизики и электроники им А.Я. Усикова НАН Украины, Украина; e-mail: zhukov@ire.kharkov.ua

Одновол Андрей Владимирович – младший научный сотрудник; Институт радиофизики и электроники им А. Я. Усикова НАН Украины, Украина.

РАДІОТЕХНІЧНІ ПРИСТРОЇ ТА ЗАСОБИ ТЕЛЕКОМУНІКАЦІЙ

УДК 621.375.4 **DOI:10.30837/rt.2021.1.204.14**

Д.Г. МАКАРОВ, Д.В. ЧЕРНОВ, канд. техн. наук, В.В. КРИЖАНОВСЬКИЙ, канд. техн. наук, Ю.В. РАССОХИНА, канд. физ.-мат. наук, В.Г. КРИЖАНОВСЬКИЙ, д-р техн. наук, А.В. ГРЄБЄННІКОВ, канд. техн. наук

ДОСЛІДЖЕННЯ ПІДСИЛЮВАЧА КЛАСУ E/F3 З ПАРАЛЕЛЬНИМ КОНТУРОМ

Вступ

Продовжується удосконалення схем та вивчення режимів роботи підсилювачів з високим ККД, що відносяться до сімейства класу E з додатковими рисами підсилювачів класу F або інверсного класу F. Такі підсилювачі можуть бути виконані у двотактному варіанті або на одному активному елементі [1 – 4]. Метою використання таких гібридних режимів є прагнення при збережені високого коефіцієнта корисної дії (ККД) поліпшити інші параметри: ширину робочої смуги частот, зменшення максимальної напруги на стоці транзистору, робота на навантаження, що змінюється та інше. Існує кілька варіантів виконання таких підсилювачів, з послідовнім та паралельнім контуром, з різним включенням додаткових контурів на частоти вищих гармонік. І самі ці контури можуть бути виконані у вигляді послідовних або паралельних коливальних контурів [5, 6]. Поєднання цих схемних особливостей дає поєднання рис класу E – ключовий режим з виконанням умов перемикання при нульовій напрузі (ПНН) та класу F – режим с управлінням амплітудного та фазового спектру на гармоніках робочої частоти [2]. Варіанти побудови підсилювачів з використанням послідовних контурів на частоти вищих гармонік досліджені доволі детально, і є приклади аналізу підсилювачів класів EF, EF2 та E/F3 [6 – 10]; також розглядалися підсилювачі з додатковими паралельними контурами [6] і навіть автогенератори, що працюють у цьому режимі [11, 12], але теорія таких пристроїв не розроблена детально.

Метою даної роботи є удосконалення метода розрахунку та експериментальна перевірка підсилювача класу E/F_3 в схемі з паралельним контуром, що шунтує навантаження [6]. Цей режим містить риси підсилювача класу E (виконання умов ПНН) та інверсного класу F на частоті третьої гармоніки – тобто навантажувальний імпеданс на стоці транзистора на частоті третьої гармоніки має дорівнювати нулю. Такий режим вивчається доволі широко, але до цих пір немає строгої теорії проєктування таких підсилювачів.

Розрахунок робочого режиму підсилювача

На рис. 1 показана еквівалентна схема підсилювача, в якому можуть бути реалізовані різні гібридні режими роботи завдяки наявності додаткового контуру L_nC_n, ємність C_{bl} виконує функцію поділу за постійним струмом і у розрахунках не враховується. Будемо використовувати метод розрахунку з роботи [6].

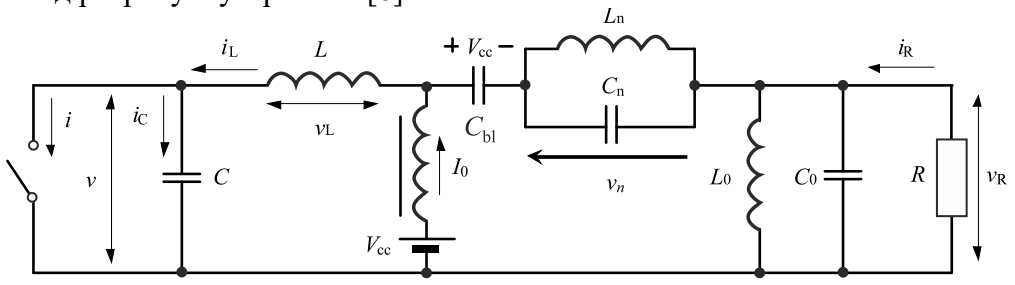


Рис. 1

Для спрощення аналізу роботи підсилювача зробимо припущення: у замкненому стані ключа його опір є нульовий, в розімкненому – нескінчений, перемикання відбувається миттєво, елементи схеми є ідеальними.

Умови ПНН для напруги на ключі v записується як ($\theta = \omega t$):

$$v(\theta)\big|_{\theta=2\pi} = 0\,, \qquad \left.\frac{dv(\theta)}{d\theta}\right|_{\theta=2\pi} = 0\,. \tag{1}$$

В припущенні великої добротності контуру L_0C_0 вважаємо струм через навантаження синусоїдальним:

$$i_R(\theta) = I_R \sin(\theta + \phi)\,, \tag{2}$$

де I_R – амплітуда струму основної частоти та ϕ – початковий фазовий зсув. На інтервалі $0 \le \theta \le \pi$ ключ УВІМК; позначаючи $v_L(\theta) = \omega L\left(di_L(\theta)/d\theta\right)$, $v_R(\theta) = V_R \sin(\theta + \phi)$, $V_R = I_R R$ отримаємо рівняння

$$v(\theta) = V_{cc} - v_L(\theta) - v_n(\theta) - v_R(\theta) = 0\,. \tag{3}$$

Струми через елементи резонансного контуру L_nC_n можна записати через напругу на ньому:

$$i_{Cn}(\theta) = \omega C_n \frac{dv_n(\theta)}{d\theta}\,, \quad i_{Ln}(\theta) = \frac{1}{\omega L_n}\int_0^{\theta} v_n(\theta)\,. \tag{4}$$

Записавши аналогічні рівняння для стану ключа ВИМК, можна записати і розв'язати диференціальні рівняння для струму та напруги, наприклад як у [6]. Але є два принципових моменти: по-перше, фактично ми постулювали нескінченну добротність контуру, який є паралельним навантаженню, і це буде принципово впливати на розрахунок схеми, а по-друге, це те, що кількості рівнянь не вистачає для визначення елементів схеми, в якій можна було б отримати потрібні форми напруги. Тобто, не повністю визначена задача розрахунку схеми. Для подолання цих недоліків було змінено підхід до вирішення задачі – додано розгляд умов для сплощення верхівки форми імпульсу напруги на активному елементі в залежності від параметрів системи. Ці умови вимагають нульову першу похідну і позитивну (чи рівну або більшу нуля) другу похідну напруги у точці біля центру інтервалу, де ключ є розімкненим (стан ВИМК). На доданок, з умовами класу Е (1) та рівняннями, що пов'язують напругу на навантаженні з параметрами кола, та напругу на додатковому контурі (квадратурні співвідношення), отримаємо п'ять рівнянь та вираз для умов пласкої вершини імпульсу:

$$F_1\left(q, \phi, \tilde{V}_R, p, \tilde{V}_p\right) = 0 \tag{5}$$

$$F_2\left(q, \phi, \tilde{V}_R, p, \tilde{V}_p\right) = 0\,, \tag{6}$$

$$F_3\left(q, \phi, \tilde{V}_R, p, \tilde{V}_p\right) = 0\,, \tag{7}$$

$$F_4\left(q, \phi, \tilde{V}_R, p, \tilde{V}_p, n\right) = 0\,, \tag{8}$$

$$F_5\left(q, \phi, \tilde{V}_R, p, \tilde{V}_p.y_0\right) = 0\,, \tag{9}$$

$$F_6\left(q, \phi, \tilde{V}_R, p, \tilde{V}_p, y_0\right) > 0\,. \tag{10}$$

Функції F_i – складні функції, описати які не дозволяє об'єм статті. Параметри n – номер гармоніки, на яку налаштований контур L_nC_n та y_0 – координата, де очікується локальний мінімум імпульсу стокової напруги, – задаються. Невідомі $q, \phi, \tilde{V}_R, p, \tilde{V}_p$ знаходяться

з рішення цієї системи та мають значення: $q = 1/\omega\sqrt{LC}$, $\tilde{V}_R = V_R/V_{cc}$ – нормована напруга на навантаженні, V_{cc} – напруга живлення, $\tilde{V}_p = V_p/V_{cc}$ – нормована напруга на додатковому контурі, $p = 1/\omega\sqrt{C_n L_\Sigma}$, $L_\Sigma = L \cdot L_n/(L + L_n)$.

Після знаходження параметрів режиму q, ϕ, V_R, p, V_p можна побудувати форми нормованих напруги та струму на ключі за виразами:

$$\tilde{v}(\theta) = C_1\left(q, \phi, \tilde{V}_R, p, \tilde{V}_p\right)\cos(q\theta) + C_2\left(q, \phi, \tilde{V}_R, p, \tilde{V}_p\right)\sin(q\theta) + 1 + \frac{q^2}{1-q^2}\tilde{V}_R \sin(\theta + \phi) + \\ + \frac{q^2}{p^2 - q^2}\tilde{V}_p \frac{1}{\sin(p\pi)}\cos\left(p(\theta - \pi)\right), \tag{11}$$

$$\tilde{i}(\theta) = 2\pi\left\{\theta + \tilde{V}_R\left(\cos(\theta + \phi) - \cos(\phi)\right) - \tilde{V}_p \frac{1}{p}\left[\frac{\sin\left[p(\theta - \pi)\right]}{\sin(p\pi)} + 1\right]\right\} \cdot \\ \cdot \left[\frac{\pi^2}{2} - \tilde{V}_R\left(2\sin(\phi) + \pi\cos(\phi)\right) + \tilde{V}_p \frac{\tan\left(\frac{p}{2}\pi\right) - p\pi}{p^2}\right]^{-1} \tag{12}$$

Фаза θ для струму змінюється від 0 до π, а для напруги – від π до 2π. В (11) входять функції

$$C_1\left(q, \phi, \tilde{V}_R, p, \tilde{V}_p\right) = -\cos(q\pi) - q\pi\sin(q\pi) + \frac{q\tilde{V}_R\left[q\cos(q\pi)\sin\phi + \left(1 - 2q^2\right)\sin(q\pi)\cos(\phi)\right]}{1 - q^2} + \\ + q\tilde{V}_p\left[-\frac{\cos(q\pi)}{\sin(p\pi)}\frac{q}{p^2 - q^2} + \frac{1}{p}\sin(q\pi)\right], \tag{13}$$

$$C_2\left(q, \phi, \tilde{V}_R, p, \tilde{V}_p\right) = -\sin(q\pi) + q\pi\cos(q\pi) + \frac{q\tilde{V}_R\left[q\sin(q\pi)\sin(\phi) - \left(1 - 2q^2\right)\cos(q\pi)\cos(\phi)\right]}{1 - q^2} - \\ - q\tilde{V}_p\left[\frac{\sin(q\pi)}{\sin(p\pi)}\frac{q}{p^2 - q^2} + \frac{1}{p}\cos(q\pi)\right]. \tag{14}$$

Тобто, маючи набір даних, наприклад: $q = 2,2566$, $\phi = 0,5711$, $\tilde{V}_R = 1,0359$, $\tilde{V}_p = 0,8882$, $p = 2,6024$, $n = 2$ і змінюючи y_0 в діапазоні від 4,2 до 4,55, можна отримати форми нормованих струму та напруги на ключі, які свідчать про те, що при ідеальних параметрах елементів навантажувальної ланки досягається мета зменшення максимальної напруги на ключі (рис. 2).

Далі з цих параметрів можемо отримати значення елементів вихідної ланки. Вихідний паралельний контур розраховувався виходячи з його навантаженої добротності $Q_0 = 8,8$. Тоді елементи вихідного контуру дорівнюють $L_0 = 0,45$ мкГн та $C_0 = 14070$ пФ.

Елементи L та C обраховуються за формулами:

$$\frac{\omega L}{R} = \frac{1}{\pi\tilde{V}_R^2}\left[\frac{\pi^2}{2} - \tilde{V}_R\left(2\sin(\phi) + \pi\cos(\phi)\right) + \tilde{V}_p \frac{\tan\left(\pi\frac{\pi}{2}\right) - p\pi}{p^2}\right], \tag{15}$$

$$\omega CR = \frac{1}{q^2 \dfrac{\omega L}{R}}. \qquad (16)$$

З формул (15) і (16) для частоти 2 МГц для схеми з активним елементом у вигляді ключа знаходимо значення шунтуючої ємності та першої індуктивності $C = 435$ пФ і $L = 2{,}847$ мкГн. При розрахунку елементів контуру $L_n C_n$ є деякі варіанти: оскільки в результаті розрахунку отримаємо тільки резонансну частоту контуру $L_n C_n$, а для визначення кожного елементу потрібно ще задати, наприклад, добротність цього контуру або співвідношення індуктивності L_n / L, обираючи добротність 100, отримаємо $L_n = 0{,}929$ мкГн та $C_n = 1006$ пФ.

Для реалізації класу E/F$_3$ потрібно мати малий навантажувальний імпеданс на частоті третьої гармоніки. Розрахунок імпедансу за формулою [6]

$$\operatorname{Im} Z(\omega) = \omega L + \frac{\omega L_n}{1 - \omega^2 L_n C_n} \qquad (17)$$

дає для уявної частини імпедансів значення: $\operatorname{Im} Z(\omega_0) = 49{,}5$ Ом, $\operatorname{Im} Z(2\omega_0) = 128{,}6$ Ом, $\operatorname{Im} Z(3\omega_0) = 0{,}7$ Ом.

Для перевірки отриманих результатів було проведено моделювання вихідної ланки підсилювача (рис. 3) та побудовано годограф вхідного імпедансу (у перерізі С) (рис. 4). Було перевірено вплив активних опорів індуктивностей на вхідний імпеданс. Сімейство кривих відповідають зміні активного опору L_n від 0,05 Ом до 0,65 Ом. Видно, що активна складова вхідного імпедансу на частоті третьої гармоніки (6 МГц) складає при цьому вдесятеро більшу величину, при опорі L_n, що дорівнює 0,65 Ом, це буде 6,1 Ом. Таким чином, ускладняються умови отримання режиму класу E/F$_3$ в експерименті, оскільки змінюються як амплітуди, так і фази вищих гармонійних складових.

Моделювання режиму підсилювача на ключі методом гармонійного балансу дає форми сигналів, схожі до розрахованих. Враховувалась обмежена кількість гармонік, чим і пояснюється пульсація струму на рис. 5. Вихідна потужність при напрузі на стоці 24 В складає 7,5 Вт.

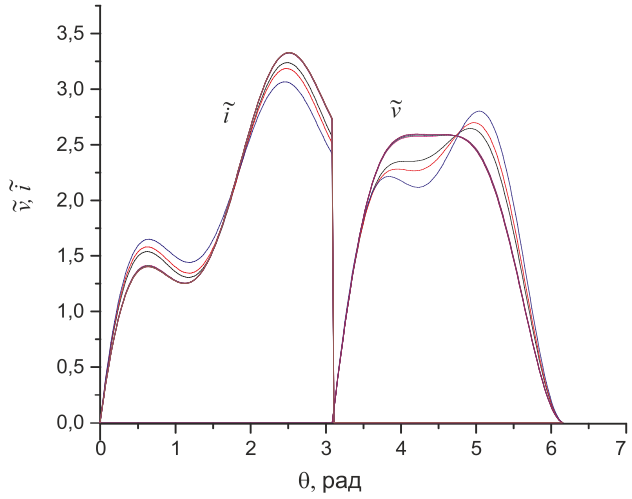


Рис. 2

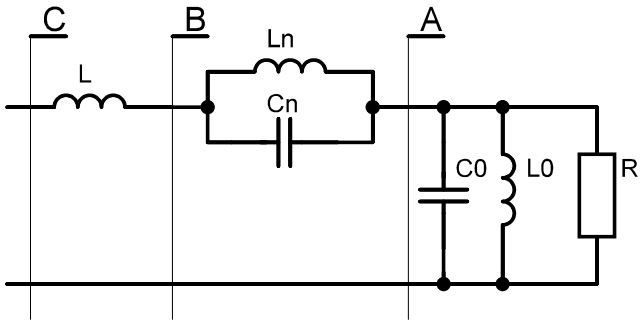


Рис. 3.

Експериментальне дослідження

Експериментальний макет підсилювача створено на транзисторі IRF530 на частоту 2 МГц, навантаженням слугував перетворювач вимірювача потужності NRP з атенюатором 30 дБ та опором 50 Ом. Для відповідності параметрів макету даним, що були розраховані, у кожному перерізі схеми (рис. 3) проводилося вимірювання та налаштування вхідного імпедансу на багатофункціональному спектроаналізаторі FPC 1500, відповідні дані наведені в табл. 1. Експериментальний годограф навантажувального імпедансу наведено на рис. 6. Значення імпедансів на частотах розташування міток: М1 – 2 МГц – 37+j51,6 Ом, М2 – 4 МГц – 0,79+j130,6 Ом, М3 – 6 МГц – 4,36-j101 Ом. Видно, що у розрахунках потрібно враховувати втрати у контурі L_nC_n, разом з тим це ускладнює розрахунки, тому і потрібно моделювання та експериментальне дослідження підсилювача з налаштуванням на вищих гармоніках.

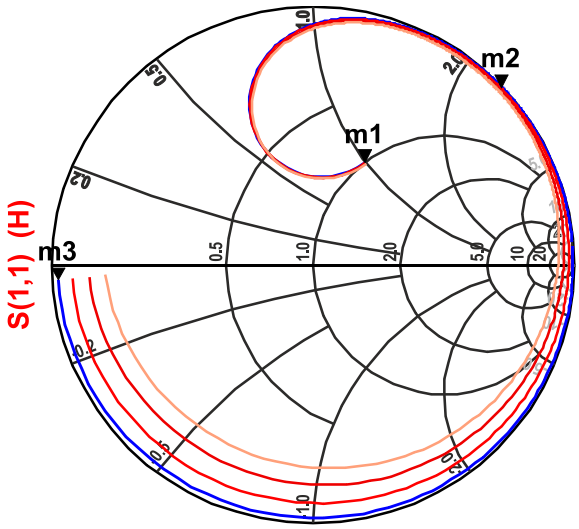


Рис. 4

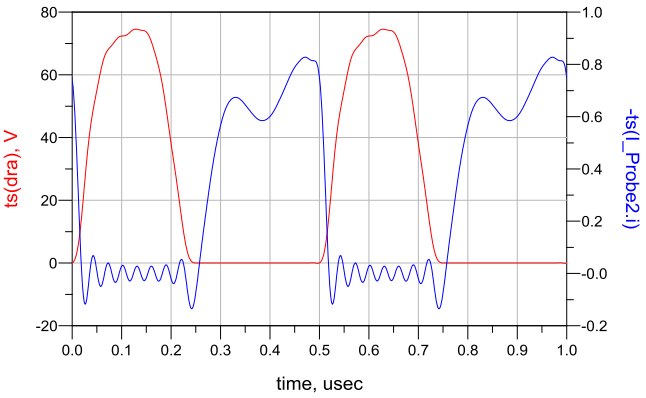


Рис. 5

Видно, що в цілому вдалося досягти відповідності імпедансних характеристик вихідних ланок. Експериментальні форми сигналів на стоці та виході підсилювача показано на рис. 7.

Таблиця 1

Імпеданс вихідного кола по перерізах

Переріз	Моделювання			Експеримент		
	2 МГц	4 МГц	6 МГц	2 МГц	4 МГц	6 МГц
A	$50+j0.1$	$0.3-j4$	$0.1-j2$	$44-j0.4$	$0.7-j1.5$	$0.2+j1.5$
B	$50+j14$	$0.3+j53$	$0.1-j108$	$36+j14$	$1.5+j60$	$1.7-j101$
C	$50+j45$	$0.3+j125$	$0.1-j1.5$	$37+j52$	$0.8+j130$	$4-j1$

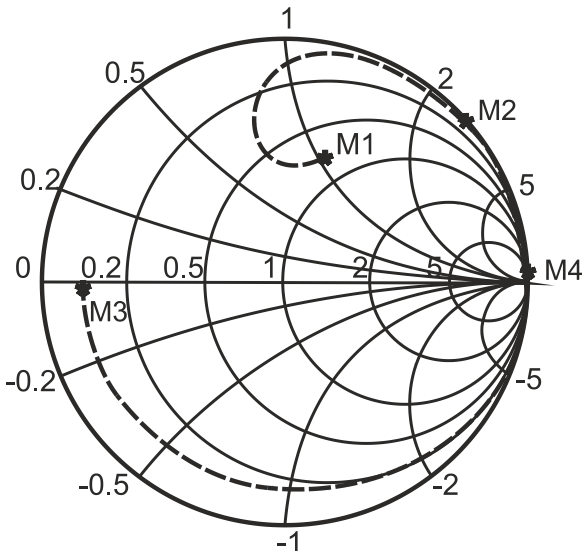


Рис. 6

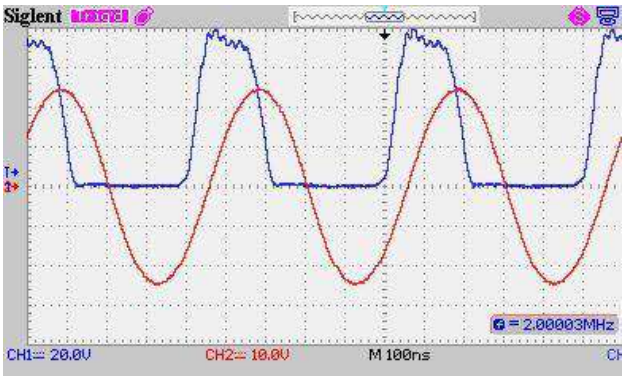


Рис. 7

Пікове значення напруги на стоці транзистору складає 78 В, тобто, відношення цієї напруги до напруги живлення складає 3,25, в той час, як для схеми підсилювача класу Е з паралельним вихідним контуром без додаткового паралельного контуру дане співвідношення складає 3,68 [6]. Відповідно, у даній схемі експериментально отримано зменшення співвідношення пікової напруги до напруги живлення на 12 %.

Спектр вихідного сигналу підсилювача показано на рис. 8. Рівень другої гармоніки склав - 28,98 дБ, а третьої -28,46 дБ, четвертої -43,42 дБ щодо сигналу основної частоти. Спостерігається відносне зменшення рівня другої гармоніки внаслідок впливу додаткового контуру. Експериментальні залежності вихідної потужності та стокового ККД показано на рис. 9. Підсилювач демонструє ключовий режим роботи та може використовуватися у схемах зі зміною потужності шляхом зміни напруги живлення.

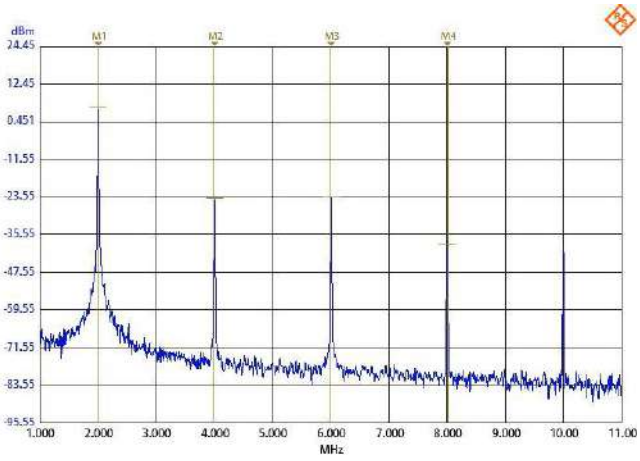


Рис. 8

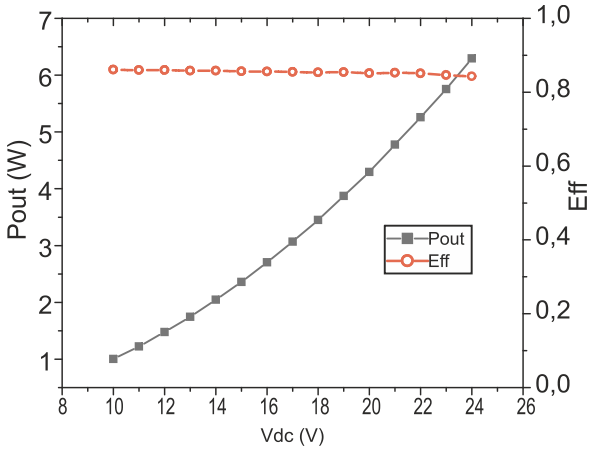


Рис. 9

В табл. 2 наведено параметри елементів вихідної ланки, отримані в результаті розрахунків, моделювання та експериментального налаштування підсилювача. Видно, що отримано досить близькі значення елементів, враховуючи складність отримання потрібних значень індуктивностей та вплив активного опору реактивних компонентів.

Таблиця 2

Номінали елементів вихідної ланки

	C, пФ	L, мкГн	C_n, пФ	L_n, мкГн	C_0, пФ	L_0, мкГн	R, Ом
Теорія	435	2,847	1006	0,929	14072	0,45	50
Моделювання	268	2,847	1006	0,929	14070	0,45	50
Експеримент	144	2.85	961	0.89	17010	0.39	50

Висновки

Розраховано елементи та проаналізовано режими роботи підсилювача класу Е з шунтуючою ємністю та паралельним контуром і з додатковим фільтром у навантажувальному колі. Показано наявність різних режимів, які можуть виникати в такій схемі за умови ідеальних елементів. Розглянуто варіанти реалізації підсилювача у режимі класу E/F3, та проведено його моделювання і експериментальне дослідження. Вказано на значну роль втрат у додатковому контурі на характеристики підсилювача. На частоті 2 МГц отримано вихідну потужність 6,3 Вт на навантаженні 50 Ом при ККД 84,3% та напрузі живлення 24 В. Дана схема підсилювача може бути корисна для роботи на більш високих частотах, де потрібній годограф імпедансу буде легше реалізувати.

Список литературы:

1. Kee S. D., Aoki I., Hajimiri A. and Rutledge D. The class-E/F family of ZVS switching amplifiers // IEEE Trans. Microw. Theory Tech., vol. 51, no. 6, pp. 1677–1690, Jun. 2003.
2. Krizhanovski V.G., *High-efficiency transistor power amplifiers*. Donetsk : Apex, 2004. 448 p. (in Rus.)
3. Grebennikov A., Sokal N. O. and Franco M. J. *Switchmode RF and Microwave Power Amplifiers*. 2nd ed. Orlando, FL, USA : Academic, 2012. 667 p.
4. Kazimierczuk M. K. *RF Power Amplifiers*. 2nd ed. 2015 John Wiley & Sons Ltd. 686 p.
5. Kaczmarczyk Z. High-Efficiency Class E, EF2, and E/F3 Inverters // IEEE Transactions on Industrial Electronics, vol. 53, no. 5, pp. 1584-1593, Oct. 2006, doi: 10.1109/TIE.2006.882011
6. Grebennikov A. High-efficiency Class-E power amplifier with shunt capacitance and shunt filter // *IEEE Trans. Circuits and Systems – I: Regular Papers*. vol. CAS-I-63, pp. 12-22, Jan. 2016.
7. Aldhaher S., Yates D. C. and Mitcheson P. D. Modeling and Analysis of Class EF and Class E/F Inverters With Series-Tuned Resonant Networks // IEEE Transactions on Power Electronics. vol. 31, no. 5, pp. 3415-3430, May 2016, doi: 10.1109/TPEL.2015.2460997.
8. Mustafa Acar, Anne Johan Annema, Bram Nauta, Analytical Design Equations for Class-E Power Amplifiers // IEEE Transactions on Circuits and Systems // Regular Papers, V. 54, N. 12, Dec. 2007, p. 2706-2717.
9. Chen P., Yang K. and Zhang T. Analysis of a Class-E Power Amplifier With Shunt Filter for Any Duty Ratio // IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 64, no. 8, pp. 857-861, Aug. 2017, doi: 10.1109/TCSII.2016.2609393.
10. Zaijun H., Fengchen H., Jianni L. and Zhao C. Analysis of Class E Power Amplifier With Shunt Filter under Different Duty Cycles // 2020 IEEE 3rd International Conference on Information Communication and Signal Processing (ICICSP), Shanghai, China, 2020, pp. 47-51, doi: 10.1109/ICICSP50920.2020.9232044.
11. Inaba T., Koizumi H. Class E/F3 Tuned Power Oscillator // IEEE Transactions on Power Electronics. 2018. Vol. 33, No. 2. pp. 1420-1427.
12. 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, 2018. P. 607 – 611.

Надійшла до редколегії 06.02.2020

Відомості про авторів:

Макаров Денис Григорович – інженер, кафедра комп'ютерних наук та інформаційних технологій, Донецький національний університет імені Василя Стуса (м. Вінниця), Україна; email: d.makarov@donnu.edu.ua, ORCID: https://orcid.org/0000-0002-5415-5978

Чернов Дмитро Вікторович – канд. техн. наук, доцент, кафедра радіофізики та кібербезпеки, доцент, Донецький національний університет імені Василя Стуса (м. Вінниця), Україна; email: d.chernov@donnu.edu.ua, ORCID: https://orcid.org/0000-0001-7173-0842.

Крижановський Володимир Володимирович – канд. техн. наук, Synic Solution Co., Ltd, 37, Hwangsaeul-ro 258 beon-gil, Seongnam-si Republic of Korea; email: vlad@synic.co.kr; ORCID: https://orcid.org/0000-0003-1989-1483

Рассохіна Юлія Валентинівна – канд. фіз.-мат. наук, старший науковий співробітник, кафедра радіофізики та кібербезпеки, Донецький національний університет імені Василя Стуса (м. Вінниця), Україна; email: yu.rassokhina@donnu.edu.ua, ORCID: https://orcid.org/0000-0003-0538-8908

Крижановський Володимир Григорович – д-р техн. наук, професор, кафедра радіофізики та кібербезпеки, професор, Донецький національний університет імені Василя Стуса (м. Вінниця), Україна; email: v.krizhanovski@donnu.edu.ua; ORCID: https://orcid.org/0000-0002-2685-9740

Грєбєнніков Андрій Вікторович – канд. техн. наук, Sumitomo Electric Europe Ltd, 220 Centennial Park, Centennial Avenue, Elstree, Herts, WD6 3SL, UK; email: grandrei@ieee.org, ORCID: https://orcid.org/0000-0003-2636-7049

ПІДГОТОВКА СПЕЦІАЛІСТІВ В ОБЛАСТІ РАДІОТЕХНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ

UDC 004.94 **DOI:10.30837/rt.2021.1.204.15**

I. MOSHCHENKO, PhD, O. NIKITENKO, PhD, Yu. KOZLOV, PhD

POSSIBILITIES OF USING CMS MAPLE TO STUDY RANDOM VARIABLE DISTRIBUTION LAWS

Introduction

One of the fundamental notion of probability theory is the notion of a random variable. If we know all possible values which the random variable was assumed and probability for every their variable then we find it theoretically defined distribution. Thus distribution law of a random variable defined its probability as function defined on event set. Random variables, distribution laws and other performances are used during applied and fundamental experiment in many science and technique areas. For this reason, the study of random variables distribution laws is actual.

Statistical calculations without computer are difficult and require many functional and quintiles tables of standard laws. It does not contribute to feel the element of novelty in the material students are studying, to change problem conditions and so on. It requires much time to solve applied tasks and is inappropriate.

Today in the world market there are more than 1000 widest packages solved statistical data analysis problems at differential computer operational systems. Statistical applied programs divided on universal, semiuniversal, special packages and statistical expert systems. Specialized mathematical packages (SAS, SPSS, STATISTIKA, STATGRAPHICS) are not relevant for study. Their use for studying requires very high education level in mathematical statistics.

Thus to determine and research random variables distribution laws both in practical applications and in studying we must use special mathema

tical packages. The most extended of them are Mathcad, MatLab, Mathematica, Maple.

Most of the existing math packages allow users to operate at random variables, including the Computer Mathematics System (CMS) Maple [1].

Thus this article purpose is a description of the studying possibilities of the random variables distribution laws with CMS Maple and the application of the acquired skills in the independent work of students.

Choice of Computer Mathematics System

Computer Mathematics Systems are effective method to mathematic learning by students from Europe, USA, Japan, China and other countries. Unfortunately in our education system both students and teachers are used modern computer mathematics systems not enough. It very slowed down solving some problems to implement our education system in world education one where computer mathematics systems are in active using.

Publication analysis evident about intensive investigation on the implementation of information and communication technologies in particular computer oriented education systems.

Choice of Computer Mathematics System is depend on the ultimate goal of program using, tasks class, its appointment.

Didactical functions of such systems are:

- visual means data presenting (electron reference book with hypertext help system and intuitive interface, animate examples audio and video accompaniment);
- solving practical problems means, complex models research, thorough analysis of solving tasks' variants, development of practical skills of mathematical reasoning.

CMS can be divided into seven classes: systems for numerical calculations; table processors; matrix systems; systems for statistical calculations; systems for special calculations; systems for analytical calculations (computer algebra); universal systems [2].

CMS comparison was shown in table [3].

CMS comparison

CMS	Advantages	Disadvantages
Mathematika	Compatibility with computer platforms. 3D-graphics. Documents (notebook). Sound synthesis support.	Excessive copy protection. Targeting experienced users.
Matlab	Unique matrix tools, descriptor graphics, high speed calculations, adaptation to user's tasks and number of system packages.	Limited opportunities of symbolic calculations. High cost of the system and their packages.
MathCad	Quality graphics and visualization during calculations. Comfortable interface. Mathematical signs palette availability. Huge choice of electron books and libraries, operators and functions.	Symbolic mathematic limitation. Primitive programming. Cost of electron books and libraries.
Maple	Thoughtful kernel of symbolic calculations. Documents (notebook). High quality graphics. Convenient help system.	No sound synthesis.

Compared to other mathematical software packages, CMS Maple has several advantages that are of particular importance when solving statistical applied problems in the field of metrology, namely: possibility of symbolic calculations, operation of numbers with arbitrary accuracy, representation of graphs in dynamic mode, etc [1].

Statistics with Maple

As well known, random variables are divided into discrete and continuous ones. Accordingly, the random variables distribution laws are divided into distribution laws for discrete random variables and the distribution laws for continuous random variables.

Statistics in CMS Maple has a sophisticated packages suite to handle applications of various types and purposes. Maple commands for statistics work are intended for those categories of users who need an environment that makes it easy to move from one mathematical specialization to another without spending too much time transforming data and mastering a software variety.

The Maple Statistics Library has a large set of commands for analyzing data, computing various numerical characteristics of random variables, graphing their distribution laws, and for statistical data processing [4 – 8].

This library provides the ability to operate with the following laws for the discrete random variables distributions: Bernoulli, binomial, discrete uniform, empirical, geometric, hypergeometric, negative binomial (Pascal), Poisson; and continuous random variables: beta, Cauchy, χ^2, Erlang, error (exponential power), exponential, Fisher, gamma, Gumbel, inverse gaussian (Wald), Laplace, logistic, log normal, Maxwell, Moyal, noncentral beta, noncentral χ^2, noncentral f-distribution, noncentral t-distribution, normal (gaussian), Pareto, power, Rayleigh, Student-t, triangular, uniform (rectangular), von Mises, Weibull. In addition, it is possible to create new distribution laws and to study their properties.

The presence of such large list of random variables distribution laws allows them to be studied and investigated by students both in the course of laboratory or practical work, as well as during independent work, as well as in solving applied and theoretical problems in all fields of science and technology.

Below we showed the algorithm of the random variables distribution laws study. This algorithm consists of such stages:

1. To define the random variables distribution law.

2. To obtain the Cumulative Distribution Function expression.

3. To obtain the Probability Density Function expression.

4. To obtain the descriptive statistics expression.

5. To generate random sample according to the chosen distribution law.

6. To compare theoretical descriptive statistics' values and generated descriptive statistics' values.

7. To plot Probability Density Function graphic.

Let's take an example results which obtained using above mentioned algorithm for three distribution laws: one for discrete random variables, one for continuous random variables and one for created law.

Below are the results obtained using above mentioned algorithm to Poisson distribution law (discrete random variables), Maxwell distribution law (continuous random variables) and created distribution law.

Probability density function of the created distribution law was defined as

$$f(x)=\begin{cases}0 & x<-1\\ (x+1)^2 & -1\le x<0\\ 1-x^2 & 0\le x<1\\ 0 & x\ge 1\end{cases}. \tag{1}$$

This function was shown in fig. 1.

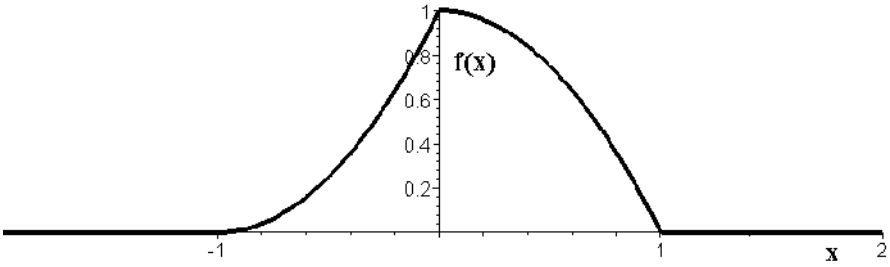


Fig. 1. Probability density function of the created distribution law

Descriptive statistics using classical approach were defined as:

Cumulative Distribution Function

$$F(x)=\int f(x)dx=\begin{cases}0 & x<-1\\ \dfrac{(x+1)^3}{3} & -1\le x<0\\ x-\dfrac{1}{3}x^3+\dfrac{1}{3} & 0\le x<1\\ 1 & x\ge 1\end{cases}. \tag{2}$$

Expected value

$$M=\int_{-\infty}^{\infty} xf(x)dx=\frac{1}{6}. \tag{3}$$

Variance

$$D=\int_{-\infty}^{\infty}(x-M)^2 f(x)dx=\frac{5}{36}. \tag{4}$$

Standard Deviation

$$\sigma=\sqrt{D}=\frac{\sqrt{5}}{6}. \tag{5}$$

Skewness

$$As = \frac{\int_{-\infty}^{\infty} (x - M)^3 f(x) dx}{\sigma^{3/2}} = -\frac{8\sqrt{5}}{125}. \quad (6)$$

Kurtosis

$$Ex = \frac{\int_{-\infty}^{\infty} (x - M)^4 f(x) dx}{D^2} = \frac{309}{125}. \quad (7)$$

To create a new distribution law we must use command **Distribution.**

First, define new distribution law as

f :=simplify(piecewise(x < -1,0, x < 0,(x+1)^2, x < 1, 1-x^2, x>1, 0)):

Second, create this law

MyLaw **:= Distribution(PDF = unapply(f, x)):**

Define random variables distribution laws by commands

> xx := Poisson(lambda); X := RandomVariables(xx):

> xx := Maxwell(alpha); Y := RandomVariables(xx):

> xx := MyLaw; Z := RandomVariables(xx):

For selected distribution laws we obtained cumulative distribution functions using command **CDF**.

> CDF(X,p); CDF(Y,x); CDF(Z,x);

$$-\frac{\Gamma(2 + floor(p))}{(floor(p)+1)!} + 1 + \frac{(floor(p)+1)\Gamma(floor(p)+1, \lambda)}{(floor(p)+1)!}$$

$$\begin{cases} 0 & x < 0 \\ \frac{1}{3}\frac{\sqrt{2}x^3 hypergeom\left(\left[\frac{3}{2}\right], \left[\frac{5}{2}\right], -\frac{x^2}{2\alpha^2}\right)}{\alpha^3} & otherwise \end{cases}$$

$$\begin{cases} 0 & x < -1 \\ \frac{(x+1)^3}{3} & x \le 0 \\ x - \frac{1}{3}x^3 + \frac{1}{3} & x \le 1 \\ 1 & otherwise \end{cases}$$

For selected distribution laws we obtained probability density functions using command **PDF**.

> PDF(X,p); PDF(Y,x); PDF(Z,x);

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{(-\lambda)} Dirac(p - k)}{k!}$$

$$\begin{cases} 0 & x < 0 \\ \frac{\sqrt{2}\sqrt{\frac{1}{\pi}} x^2 e^{\left(-\frac{x^2}{2\alpha^2}\right)}}{\alpha^3} & otherwise \end{cases}$$

$$\begin{cases} 0 & x < -1 \\ (x+1)^2 & -1 \le x < 0 \\ 1 - x^2 & 0 \le x < 1 \\ 0 & otherwise \end{cases}$$

Using command **Mean** from Statistics library we obtained theoretical value of expected value and its empirical value for 250 elements sample to mentioned distribution laws.

> Mean(X); Mean(Y); Mean(Z);

$$\lambda$$

$$\frac{2\sqrt{2}\alpha}{\sqrt{\pi}}$$

$$\frac{1}{6}$$

> A:=Sample(X,250);B:= Sample(Y,250);C:= Sample(Z,250);

> Mean(A); Mean(B); Mean(C);

14.848

3.27

0.1667

Using command **Variance** and **StandardDeviation** from Statistics library we obtained theoretical value of Variance, Standard Deviation and its empirical value for 250 elements sample to mentioned distribution laws.

> Variance(X); Variance(Y); Variance(Z);

$$\lambda$$

$$\frac{\alpha^2(3\pi - 8)}{\pi}$$

$$\frac{5}{36}$$

> StandardDeviation(X); StandardDeviation(Y); StandardDeviation(Z);

$$\sqrt{\lambda}$$

$$\alpha\sqrt{\frac{3\pi - 8}{\pi}}$$

$$\frac{\sqrt{5}}{6}$$

> Variance(A); Variance(B); Variance(C);

13.2298

1.799

0.138889

> StandardDeviation(A); StandardDeviation(B); StandardDeviation(C);

3.637

1.341

0.3727

Using command **Skewness** from Statistics library we obtained theoretical value of Skewness and its empirical value for 250 elements sample to mentioned distribution laws.

> Skewness(X); Skewness(Y); Skewness(Z);

$$\frac{1}{\sqrt{\lambda}}$$

$$-\frac{2\sqrt{2}(5\pi-16)}{\pi^{(3/2)}\left(\frac{3\pi-8}{\pi}\right)^{(3/2)}}$$

$$-\frac{8\sqrt{5}}{125}$$

> Skewness(A); Skewness(B); Skewness(C);

0.25

0.3733

-0.143

Using command **Kurtosis** from Statistics library we obtained theoretical value of Kurtosis and its empirical value for 250 elements sample to mentioned distribution laws.

> Kurtosis(X); Kurtosis(Y); Kurtosis(Z);

$$\frac{3\lambda+1}{\lambda}$$

$$\frac{16\pi-192+15\pi^2}{(3\pi-8)^2}$$

$$\frac{309}{125}$$

> Kurtosis(A); Kurtosis(B); Kurtosis(C);

2.685

2.9374

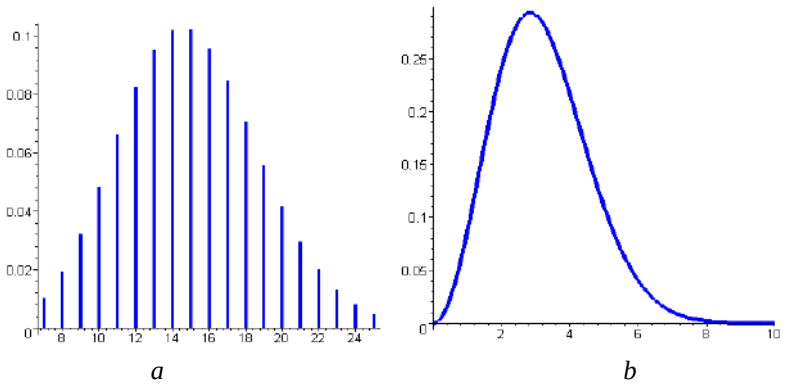
2.472

Using command **DensityPlot** from Statistics library we plotted graphics to mentioned distribution laws shown in fig. 2 (Poisson (a) and Maxwell (b) distribution laws).

> DensityPlot(X, colour=blue, thickness=4);

> DensityPlot(Y, colour=blue, thickness=4, range=0..10);

> DensityPlot(Z, colour=black, thickness=4);



a *b*

Fig. 2. Probability density function of the Poisson (a) and Maxwell (b) distribution laws

Conclusion

Thus, thanks to a powerful set of statistical tools, the ability to symbolically calculate and process expressions and data, the extensive CMS Maple, the extensive capabilities of graphically interpreting the results not only in static but also in dynamic form (two- and three-dimensional animation), it is advisable to use when studying the topic "Distribution Laws of random variables" in students' practical and independent work for further use of their acquired skills in solving applied science and technology problems.

References:

1. Aladjev V. Z. Prohramirovanie v paketakh Maple и Mathematica : Sravnitel'nyj aspekt [Programming in Maple and Mathematica packages : Comparison aspect]. Hrodno, HrSU, 2011. 517 p.
2. Djakonov V.P. Kompjuternaja matematika [Computer mathematics] // Sorosovskij obrazovatel'nyj zhurnal. 2001. vol. 7. (in Rus.)
3. Hrybjuk O.O., Yunchyk V.L. Vykorystannja system kompjuternoji matematyky u konteksti modeli zmishanoho navchannia [Using of computer mathematics systems on context mixing education model]. Matematyka // Informatsijni tekhnolohii. Osvita: [zb. statej] / SNU imeni Lesi Ukrajinky. Luts'k : Svitjaz', 2015. P. 52 – 71.
4. Korchakova A.S., Nikitenko O.M. Osoblyvosti statystychnoji obrobky danykh za dopomohoju kompjutera [Feature of statistical data processing by computer] // Metrolohija ta prylady. 2014. № 1. P. 138-142.
5. Manzon B. M. Maple V Power Edition. Moscow : Informatsionno-izdatel'skij dom "Filin", 1998. 240 p.
6. Matrosov A. V. Maple 6. Reshenije zadach vysshej matematiki i mekhaniki [Maple 6. Problems' solving of higher mathematics and mechanics]. Sankt-Peterburh : BHV, 2000. 528 p.
7. Hovorukhin V. N. Kompjuter v matematicheskom issledovanii: Maple, MATLAB, LaTeX. [Computer at mathematical research: Maple, MATLAB, LaTeX]. Sankt-Peterburh: Piter, 2001. 624 p.
8. Matematicheskij paket Maple V. Rukovodstvo pol'zovatelja [Mathematical package Maple V. User's manual] ; ed. H. B. Prochorov, V. V. Kolbeev, K. I. Zhelnov, M.A. Ledev. Kaluha. Oblizdat, 1998. 200 p.

Надійшла до редколегії 12.02.2021

Відомості про авторів:

Мощенко Інна Олексіївна – канд. техн. наук, старший викладач кафедри метрології та технічної експертизи; Харьковский национальный университет радиоэлектроники, Україна; e-mail: inna.moshchenko@nure.ua; ORCID: https://orcid.org/0000-0002-2738-0037

Нікітенко Олександр Миколайович – канд. техн. наук, доцент, доцент кафедри метрології та технічної експертизи; Харьковский национальный университет радиоэлектроники, Україна; e-mail: nikonxipe@gmail.com; ORCID: https://orcid.org/0000-0002-1082-5247

Козлов Юрій Валентинович – канд. техн. наук, доцент, доцент кафедри метрології та технічної експертизи; Харьковский национальный университет радиоэлектроники, Украина; e-mail: yurii.kozlov@nure.ua; ORCID: https://orcid.org/0000-0002-6165-4978

РЕФЕРАТИ РЕФЕРАТЫ ABSTRACTS

МЕТОДИ ТА МОДЕЛІ КРИПТОГРАФІЧНОГО АНАЛІЗУ ТА КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

МЕТОДЫ И МОДЕЛИ КРИПТОГРАФИЧЕСКОГО АНАЛИЗА И КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

METHODS AND MODELS OF CRYPTOGRAPHIC ANALYSIS AND CRYPTOGRAPHIC TRANSFORMATIONS

УДК 621.391:519.2

Узагальнений диференціально-лінійний криптоаналіз блокових шифрів / *А.М. Олексійчук* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 204. С. 5 – 15.

Диференціально-лінійний метод криптоаналізу блокових шифрів запропоновано в 1994 р. Він виявляється більш ефективним в порівнянні з (окремо) диференціальним та лінійним методами, проте його наукове обґрунтування залишається предметом подальших досліджень. Відомо декілька публікацій, присвячених формалізації диференціально-лінійного методу та з'ясуванню умов, за яких його трудомісткість може бути оцінено математично строго. Однак проблема наукового обґрунтування диференціально-лінійного методу в повному обсязі залишається невирішеною.

В роботі викладено перші результати, отримані автором у напрямі вирішення цієї проблеми. Розширено клас диференціально-лінійних атак на блокові шифри. А саме, розглянуто як розрізнювальні атаки, так і атаки, спрямовані на відновлення одного біту інформації про ключ. При цьому не робиться жодних припущень (як у відомих публікаціях) про можливість представлення шифру у вигляді певних двох компонент. Отримано нижні оцінки інформаційної складності зазначених атак, вирази яких залежать від усереднених (за ключами) значень квадратів елементів узагальненої автокореляційної таблиці шифрувального перетворення. На відміну від відомих, отримані оцінки інформаційної складності диференціально-лінійних атак не базуються на жодних евристичних припущеннях відносно блокових шифрів, що досліджуються, та є справедливими для більш широкого класу атак в порівнянні з традиційною диференціально-лінійною атакою. Наведено співвідношення, які встановлюють взаємозв'язок між, відповідно, диференціальними, лінійними та диференціально-лінійними властивостями бієктивних булевих відображень. На відміну від відомих робіт, використовується матрична форма запису співвідношень, що дозволяє краще з'ясувати їх сутність та спростити доведення. Отримано нове співвідношення для елементів узагальненої автокореляційної таблиці шифрувального перетворення добутку двох блокових шифрів, яке може бути корисним в подальших дослідженнях.

Ключові слова: симетрична криптографія; блоковий шифр; диференціально-лінійний криптоаналіз; узагальнена таблиця автокореляції; обґрунтування стійкості.

Бібліогр.: 16 назв.

УДК 621.391:519.2

Обобщенный дифференциально-линейный криптоанализ блочных шифров / *А.Н. Алексейчук* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 204. С. 5 – 15.

Дифференциально-линейный метод криптоанализа блочных шифров предложен в 1994 г. Он оказывается более эффективным по сравнению с (отдельно) дифференциальным и линейным методами, однако его научное обоснование остается предметом дальнейших исследований. Известно несколько публикаций, посвященных формализации дифференциально-линейного метода и выяснению условий, при которых его трудоемкость может быть оценена математически строго. Однако проблема научного обоснования дифференциально-линейного метода в полном объеме остается не решенной.

В работе изложены первые результаты, полученные автором в направлении решения этой проблемы. Расширен класс дифференциально-линейных атак на блочные шифры. А именно, рассмотрены как различающие атаки, так и атаки, направленные на восстановление одного бита информации о ключе. При этом не делается никаких предположений (как в известных публикациях) о возможности представления шифра в виде некоторых двух компонент. Получены нижние оценки информационной сложности указанных атак, выражения которых зависят от усредненных (по ключам) значений квадратов элементов обобщенной автокорреляционной таблицы шифрующего преобразования. В отличие от известных, полученные оценки информационной сложности дифференциально-линейных атак не базируются на каких-либо эвристических допущениях об исследуемых блочных шифрах и справедливы для более широкого класса атак по сравнению с традиционной дифференциально-линейной атакой. Приведены также соотношения, устанавливающие взаимосвязь между, соответственно, дифференциальными, линейными и дифференциально-линейными свойствами биективных булевых отображений. В отличие от известных работ, используется матричная форма записи соотношений, что позволяет лучше выяснить их сущность и упростить доказательства. Получено новое соотношение для элементов обобщенной автокорреляционной таблицы шифрующего преобразования произведения двух блочных шифров, которое может быть полезным в дальнейших исследованиях.

Ключевые слова: симметричная криптография; блочный шифр; дифференциально-линейный криптоанализ; обобщенная таблица автокорреляции; обоснование стойкости.

Библиогр.: 16 назв.

UDC 621.391:519.2

Generalized differential-linear cryptanalysis of block ciphers / *A.N. Alekseychuk* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №204. P. 5 – 15.

Differential-linear cryptanalysis of block ciphers was proposed in 1994. It turns out to be more efficient in comparison with (separately) differential and linear cryptanalytic methods, but its scientific substantiation remains the subject of further research. There are several publications devoted to formalization of differential-linear cryptanalysis and clarification of the conditions under which its complexity can be mathematically accurately assessed. However, the problem of the differential-linear cryptanalytic method substantiation remains completely unresolved.

This paper presents first results obtained by the author in the direction of solving this problem. The class of differential-linear attacks on block ciphers is expanded. Namely, both distinguishing attacks and attacks aimed at recovering one bit of information about a key are considered. In this case, no assumptions are made (as in well-known publications) about the possibility of representing the cipher in the form of some two components. Lower bounds of information complexity of these attacks are obtained. The expressions of these bounds depend on the averaged (by keys) values of the elements' squares of the generalized autocorrelation table of the encryption transformation. In contrast to the known ones, the obtained bounds are not based on any heuristic assumptions about the investigated block ciphers and are valid for a wider class of attacks as compared to the traditional differential-linear attack. Relations between, respectively, differential, linear and differential-linear properties of bijective Boolean mappings are given. In contrast to the well-known works, the matrix form of the relations is used that makes it possible to clarify better their essence and simplify the proofs. A new relation is derived for the elements of the generalized autocorrelation table of the encryption transformation of the product of two block ciphers, which may be useful in further research.

Key words: symmetric cryptography; block cipher; differential-linear cryptanalysis; generalized autocorrelation table; security proof.

Ref: 16 items.

УДК 004.056.55

Генерація загальносистемних параметрів для схеми електронного підпису Rainbow для 384 та 512 біт безпеки / *М.В. Єсіна, С.О. Кандій, Є.В. Острянська, І.Д. Горбенко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 204. С. 16 – 23.

На сьогодні спостерігається стрімкий прогрес у створенні квантових комп'ютерів щодо вирішення обчислювально складних задач та для різних цілей. При цьому особливі зусилля докладаються до створення такого квантового комп'ютера, що зможе вирішувати задачі криптоаналізу існуючих криптосистем – асиметричних шифрів, протоколів інкапсуляції ключів, електронних підписів тощо. Попередження таких загроз може бути досягнуто засобом розробки таких криптографічних систем, що будуть захищені як від квантових, так і від класичних атак, а також зможуть взаємодіяти з протоколами і мережами зв'язку, що вже існують. Також є суттєва необхідність захисту від атак сторонніми каналами. На даний момент значні зусилля криптологів зосереджені на відкритому конкурсі NIST PQC. Основною ідеєю конкурсу NIST PQC є визначення математичних методів, на основі яких можуть бути розроблені стандарти на асиметричні криптоперетворення, в першу чергу електронного підпису, а також асиметричні шифри та протоколи інкапсуляції ключів. За підсумками другого етапу фіналістами третього етапу конкурсу NIST PQC стали три схеми електронного підпису – Crystals-Dilithium, Falcon та Rainbow. Перші дві з них базуються на математиці алгебраїчних решіток, а Rainbow базується на багатовимірних перетвореннях. Наразі всебічний аналіз фіналістів є важливою задачею для усієї світової криптоспільноти. Переважна більшість схем, що стали фіналістами або альтернативним алгоритмами, ґрунтується на проблемах з теорії алгебраїчних решіток. Також особлива увага була приділена схемі електронного підпису Rainbow, що ґрунтується на основі багатовимірних перетворень. Метою даної роботи є попередній аналіз існуючих атак щодо перспективного електронного підпису Rainbow, визначення вимог до загальносистемних параметрів для забезпечення криптографічної стійкості не менше 512 біт включно проти класичного та 256 біт проти квантового криптоаналізу, а також розроблення та практична реалізація щодо Rainbow алгоритмів генерації загальносистемних параметрів для 512 біт проти класичного та 256 біт проти квантового криптоаналізу.

Ключові слова: атаки; багатовимірні перетворення; електронний підпис; загальносистемні параметри; Rainbow.

Табл. 7. Іл. 1. Бібліогр.: 18 назв.

УДК 004.056.55

Генерация общесистемных параметров для схемы электронной подписи Rainbow для 384 и 512 бит безопасности / *М.В. Есина, С.О. Кандий, Е.В. Острянская, И.Д. Горбенко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 204. С. 16 – 23.

Сегодня наблюдается стремительный прогресс в создании квантовых компьютеров по решению вычислительно сложных задач и для различных целей. При этом особые усилия прилагаются к созданию такого квантового компьютера, который сможет решать задачи криптоанализа существующих криптосистем – асимметрич-

ных шифров, протоколов инкапсуляции ключей, электронных подписей и т.д. Предупреждение таких угроз может быть достигнуто средством разработки криптографических систем, которые будут защищены как от квантовых, так и от классических атак, а также смогут взаимодействовать с протоколами и сетями связи, которые уже существуют. Также есть необходимость в защите от атак сторонними каналами. На данный момент значительные усилия криптологов сосредоточены на открытом конкурсе NIST PQC. Основной идеей конкурса NIST PQC является определение математических методов, на основе которых могут быть разработаны стандарты на асимметричные криптопреобразования, в первую очередь электронной подписи, а также асимметричные шифры и протоколы инкапсуляции ключей. По итогам второго этапа финалистами третьего этапа конкурса NIST PQC стали три схемы электронной подписи – Crystals-Dilithium, Falcon и Rainbow. Первые две из них основаны на математике алгебраических решеток, а Rainbow базируется на многомерных преобразованиях. Сейчас всесторонний анализ финалистов является важной задачей для всего мирового криптосообщества. Подавляющее большинство схем, ставших финалистами или альтернативным алгоритмами, основывается на проблемах теории алгебраических решеток. Также особое внимание было уделено схеме подписи Rainbow, основанной на основе многомерных преобразований. Цель данной работы – предварительный анализ существующих атак на перспективную электронную подпись Rainbow, определение требований к общесистемным параметрам для обеспечения криптографической стойкости не менее 512 бит включительно против классического и 256 бит против квантового криптоанализа, а также разработка и практическая реализация для Rainbow алгоритмов генерации общесистемных параметров для 512 бит против классического и 256 бит против квантового криптоанализа.

Ключевые слова: атаки; многомерные преобразования; электронная подпись; общесистемные параметры; Rainbow.

Табл. 7. Ил. 1. Библиогр.: 18 назв.

UDC 004.056.55

Generation of general system parameters for Rainbow electronic signature scheme for 384 and 512 security bits / *M.V. Yesina, S.O. Kandiy, E.V. Ostryanska, I.D. Gorbenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №204. P. 16 – 23.

Today, there is rapid progress in the creation of quantum computers to solve various computational problems and for different purposes. At the same time, special efforts are made to create such a quantum computer that can solve the problems of cryptanalysis of existing cryptosystems: asymmetric ciphers, key encapsulation protocols, electronic signatures, etc. Prevention of such threats can be achieved by developing cryptographic systems that will be protected against both quantum and classical attacks, and be able to interact with existing protocols and communication networks. There is also a significant need for protection against attacks by side channels. Currently, significant efforts of cryptologists are focused on the NIST PQC open competition. The main idea of the NIST PQC competition is to define mathematical methods based on which standards for asymmetric cryptotransformations, primarily electronic signatures, as well as asymmetric ciphers and key encapsulation protocols can be developed. Three electronic signature schemes – Crystals-Dilithium, Falcon and Rainbow become the finalists of the third stage of the NIST PQC competition according to the results of the second stage. The first two are based on the mathematics of algebraic lattices, and Rainbow is based on multivariate transformations. Currently, a comprehensive analysis of the finalists is an important task for the entire global crypto community. The vast majority of schemes that have become finalists or alternative algorithms are based on problems in the theory of algebraic lattices. Special attention was also paid to the Rainbow electronic signature scheme based on multivariate transformations. The purpose of this work consists in a preliminary analysis of existing attacks on promising electronic signature Rainbow, definition of requirements to the system-wide parameters to ensure cryptographic stability of at least 512 bits against classical and 256 bits against quantum cryptanalysis, as well as development and practical implementation of Rainbow algorithms for generating system-wide parameters for 512 bits against classical and 256 bits against quantum cryptanalysis.

Key words: attacks; multivariate transformations; electronic signature; general system parameters; Rainbow.

7 tab. 1 fig. Ref: 18 items.

УДК 621.391

Концепція синтезу одного класу самосинхронізуючих дискретних сигналів / *І.Д. Горбенко, О.В. Потій, О.А. Замула* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 204. С. 24 – 29.

Застосування широкосмугових сигналів (ШСС) дозволяє підвищити завадостійкість перед завадами, що присутні в інформаційно-комунікаційних системах (ІКС). Реальна завадостійкість буде нижчою за потенційну. Причинами зниження завадостійкості при входженні в синхронізм і при розрізненні сигналів є наявність бічних піків кореляційних функцій (КФ). Виходячи з цього, ШСС, що застосовуються в ІКС, повинні володіти такими кореляційними властивостями, коли бічні піки КФ ШПС є якомога меншими, тобто в ідеальному випадку повинні прагнути до нуля. При цьому необхідно визначити вплив бічних піків на характеристики виявлення сигналів, вимірювання їх параметрів, розрізнення сигналів, знайти умови отримання малих бічних піків. Сформульована і у загальному виді вирішена задача синтезу класу сигналів із заданими кореляційними, ансамблевими і структурними властивостями, а також властивостями «розмитості» за кореляційними характеристиками. Зазначена властивість («розмитість») означає, що збільшення або зменшення довжини дискретного сигналу не змі-

нює кореляційні властивості дискретної послідовності, на основі якої синтезовано сигнал. Застосування безлічі зазначених систем сигналів в сучасних інформаційно-комунікаційних системах дозволить поліпшити показники ефективності функціонування таких систем, насамперед завадозахищеності, скритності, інформаційної безпеки, завадостійкості прийому сигналів.

Ключові слова: самосинхронізуючий сигнал; скритність; інформаційна безпека; дискретні послідовності; система нелінійних нерівностей; функція кореляції.

Бібліогр.: 11 назв.

УДК 621.391

Концепция синтеза одного класса самосинхронизирующихся дискретных сигналов / *И.Д. Горбенко, А.В. Потий, А.А. Замула* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 204. С. 24 – 29.

Применение широкополосных сигналов (ШПС) позволяет повысить помехоустойчивость информационно-коммуникационных систем (ИКС) при воздействии структурных (взаимных) и организованных помех. Реальная помехоустойчивость будет ниже потенциальной. Причинами снижения помехоустойчивости при вхождении в синхронизм и при различении сигналов является наличие боковых пиков корреляционных функций. Исходя из этого применяемые в ИКС ШПС должны обладать такими корреляционными свойствами, когда боковые пики КФ ШПС являются как можно меньшими, т.е. в идеальном случае должны стремиться к нулю. При этом необходимо определить влияние боковых пиков на характеристики обнаружения сигналов, измерения их параметров, различения сигналов, найти условия получения малых боковых пиков. Сформулирована и в общем виде решена задача синтеза класса сигналов с заданными корреляционными, ансамблевыми и структурными свойствами, а также свойствами «размытости» по корреляционным характеристикам. Указанное свойство («размытость») означает, что увеличение или уменьшение длины дискретного сигнала не изменяет корреляционные свойства дискретной последовательности, на основе которой синтезирована сигнал. Применение множества указанных систем сигналов в современных информационно-коммуникационных системах позволит улучшить показатели эффективности функционирования таких систем, прежде всего, помехозащищенности, скрытности, информационной безопасности, помехоустойчивости приема сигналов.

Ключевые слова: самосинхронизирующийся сигнал; скрытность; информационная безопасность; дискретные последовательности; система нелинейных неравенств; функция корреляции.

Библиогр.: 11 назв.

UDC 621.391

The concept of synthesis of one class of self-synchronizing discrete signals / *I.D. Gorbenko, O.V. Potii, A.A. Zamula* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №204. P. 24 – 29.

The use of broadband signals (BSS) makes it possible to increase the noise immunity of information and communication systems (ICS) when exposed to structural (mutual) and organized interference. The real noise immunity will be lower than the potential one. The reason for the decrease in noise immunity, when entering synchronism and when distinguishing signals, is the presence of side peaks of the correlation functions. Proceeding from this, the NLS used in ICS should have such correlation properties when the side peaks of the NLS CF are as small as possible, i.e. ideally should tend to zero. In this case, it is necessary to determine the influence of side peaks on the characteristics of signal detection, measure their parameters, distinguish signals, and find the conditions for obtaining small side peaks. The problem of synthesizing a class of signals with given correlation, ensemble and structural properties, as well as properties of "blurring" in correlation characteristics, is formulated and solved in general form. The specified property ("fuzziness") means that increasing or decreasing the length of the discrete signal does not change the correlation properties of the discrete sequence on the basis of which the signal is synthesized. The use of many of these signal systems in modern information and communication systems will improve the performance indicators of such systems, first of all, noise immunity, secrecy, information security, noise immunity of signal reception.

Key words: self-synchronizing signal; secrecy; information security; discrete sequences; system of nonlinear inequalities; correlation function.

Ref: 11 items.

УДК 004.056

Аналіз формальних моделей забезпечення цілісності даних і їх застосовність для баз даних / *В.І. Єсін, С.Г. Рассомахін, В.В. Вілігура* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 204. С. 30 – 39.

Інформаційні системи в цілому і бази даних, зокрема. уразливі для випадкових або зловмисних атак, спрямованих на порушення цілісності даних. Забезпечити безпеку легше, якщо є чітка модель, що представляє собою формальне вираження політики безпеки. У статті досліджуються відомі моделі безпеки, пов'язані із забезпеченням цілісності даних, їх можливість застосування і значення для баз даних. Аналіз формальних моделей забезпечення цілісності даних виявив, що кожна з них, маючи певні переваги і недоліки, має право на використання. Вирішальним фактором у прийнятті рішення є оцінка конкретної ситуації, яка дозволить зробити правильний вибір, в тому числі і комплексного їх застосування. Так в роботі відзначається, що модель Кларка – Вілсона, безумовними перевагами якої є її простота і легкість спільного використання з іншими моделями безпеки, доцільно застосовувати як сукупність практичних рекомендацій з побудови системи забезпечення цілісності в інформаційних системах. Констатуючи факт, що традиційні СУБД підтримують багато механізмів мо-

делі Кларка – Вілсона, автори вказують, що реалізації, засновані на стандартному SQL, вимагають деяких компромісних рішень. Аналіз моделі Біба дозволив зробити висновок про її відносну простоту і використання добре вивченого математичного апарату. Відзначається, що на практиці для створення захищених інформаційних систем як систем, що забезпечують конфіденційність і цілісність даних, важливим є об'єднання моделей Белла – ЛаПадули і Біба, причому об'єднання на основі однієї загальної решітки, але з двома мітками безпеки: за конфіденційністю і за цілісністю, з протилежним характером їх визначення. Саме такий варіант об'єднання моделей Белла – ЛаПадули і Біба рекомендується застосовувати в сучасних інформаційних системах і СУБД, де реалізується мандатна політика безпеки.

Ключові слова: модель безпеки; цілісність даних; інформаційна система; база даних.

Табл. 1. Іл. 4. Бібліогр.: 17 назв.

УДК 004.056

Анализ формальных моделей обеспечения целостности данных и их применимость для баз данных / *В.И. Есин, С.Г. Рассомахин, В.В. Вилигура* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 204. С. 30 – 39.

Информационные системы в целом и базы данных, в частности, уязвимы для случайных или злонамеренных атак, направленных на нарушение целостности данных. Обеспечить безопасность легче, если имеется четкая модель, представляющая собой формальное выражение политики безопасности. В статье исследуются известные модели безопасности, связанные с обеспечением целостности данных, их возможность применения и значение для баз данных. Анализ формальных моделей обеспечения целостности данных выявил, что каждая из них, имея определенные преимущества и недостатки, имеет право на использование. Решающим фактором в принятии решения является оценка конкретной ситуации, которая позволит сделать правильный выбор, в том числе и комплексного их применения. Так в работе отмечается, что модель Кларка – Вилсона, безусловными достоинствами которой являются ее простота и легкость совместного использования с другими моделями безопасности, целесообразно применять как совокупность практических рекомендаций по построению системы обеспечения целостности в информационных системах. Констатируя факт, что традиционные СУБД поддерживают многие механизмы модели Кларка – Вилсона, авторы указывают, что реализации, основанные на стандартном SQL, требуют некоторых компромиссных решений. Анализ модели Биба позволил сделать вывод о ее относительной простоте и использовании хорошо изученного математического аппарата. Отмечается, что на практике для создания защищенных информационных систем, как систем, обеспечивающих конфиденциальность и целостности данных, важным является объединение моделей Белла – ЛаПадулы и Биба, причем объединение на основе одной общей решетки, но с двумя метками безопасности: по конфиденциальности и по целостности, с противоположным характером их определения. Именно такой вариант объединение моделей Белла – ЛаПадулы и Биба рекомендуется применять в современных информационных системах и СУБД, где реализуется мандатная политика безопасности.

Ключевые слова: модель безопасности; целостность данных; информационная система; база данных.

Табл. 1. Ил. 4. Библиогр.: 17 назв.

UDC 004.056

Analysis of formal models for ensuring data integrity and their applicability to databases / *V.I. Yesin, S.G. Rassomakhin, V.V. Vilihura* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №204. P. 30 – 39.

Information systems in general and databases in particular are vulnerable to accidental or malicious attacks aimed at compromising data integrity. Security is easier if you have a clear model that is the formal expression of security policy. The paper explores known security models related to data integrity, their applicability and significance for databases. The analysis of formal models for ensuring data integrity revealed that each of them, having certain advantages and disadvantages, has the right to use. The decisive factor in making a decision is an assessment of a specific situation, which will make it possible to make the right choice, including their complex application. In this regard, the paper notes that the Clark-Wilson model, the undoubted advantages of which are its simplicity and ease of joint use with other security models, is advisable to use as a set of practical recommendations for building an integrity assurance system in information systems. While stating the fact that traditional DBMSs support many of the mechanisms of the Clark-Wilson model, the article points out that implementations based on standard SQL require some compromise solutions. Analyzing the Biba model, the paper concludes about its relative simplicity and the use of a well-studied mathematical apparatus. It is noted that in practice, for the creation of secure information systems, as systems that ensure the confidentiality and data integrity, it is important to unite the Bell-LaPadula and Biba models. Moreover, this union should be on the basis of one common lattice, but with two security labels (confidentiality and integrity) with the opposite character of their definition. This is exactly the variant of combining the Bell-LaPadula and Biba models that is recommended for use in modern information systems and DBMSs, where a mandatory security policy is implemented.

Key words: security model; data integrity; information system; database.

1 tab. 4 fig. Ref: 17 items.

УДК 004.056.55

Дослідження та аналіз реалізацій кандидатів другого раунду конкурсу NIST PQC, що орієнтовані на сімейства FPGA Xilinx / *М.В. Єсіна, Б.С. Шахов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 204. С. 40 – 58.

Сьогодні досить гостро постає питання щодо стійкості сучасних існуючих криптографічних механізмів до квантових алгоритмів криптоаналізу зокрема та квантових комп'ютерів взагалі. Ця проблема активно обговорюється на міжнародному рівні. Тому, задля її вирішення, NIST США вирішив організувати та проводить на сьогодні конкурс на кандидатів на постквантові криптографічні алгоритми NIST PQC. Результатом конкурсу повинне стати прийняття до стандартизації криптографічних алгоритмів різного типу – асиметричне шифрування, інкапсуляція ключів та електронний підпис (як мінімум по одному алгоритму з кожного типу). На момент початку конкурсу на процес стандартизації було представлено 82 алгоритми. На основі критеріїв мінімальної прийнятності, визначених NIST, для 1-го раунду було розглянуто 69 алгоритмів. З урахуванням декількох параметрів – безпека, вартість, продуктивність, характеристики реалізації тощо, – 43 і 11 алгоритмів були виключені при завершенні 1-го і 2-го раундів відповідно, а інші 15 алгоритмів були збережені для 3-го раунду. Алгоритми, які залишилися у 2-му раунді, можна розділити на 5 різних категорій залежно від математичного базису, на якому вони засновуються: на основі ізогеній еліптичних кривих, на основі алгебраїчних решіток, на основі математичного коду, на основі багатовимірних перетворень і на основі геш-функцій. Безпека є основним критерієм оцінки, що визначає конкуренцію в конкурсі NIST, і, зрозуміло, що реалізації програмного забезпечення кандидатів в основному зосереджені на ній. Однак вкрай важливо аби алгоритм мав й ефективну апаратну реалізацію. А своєчасне виявлення апаратної неефективності допоможе сконцентрувати зусилля криптографічної спільноти на більш перспективних кандидатах, потенційно заощадивши велику кількість часу, що може бути витрачена на криптоаналіз. У даній роботі розглядаються та порівнюються між собою FPGA сімейства Xilinx. Наводяться та порівнюються між собою дані щодо реалізацій кандидатів 2-го раунду в процесі стандартизації постквантової криптографії NIST, що орієнтовані на FPGA сімейства Xilinx.

Ключові слова: апаратне забезпечення; електронний підпис; конкурс NIST PQC; постквантова криптографія; FPGA; Xilinx.

Табл. 12. Бібліогр.: 10 назв.

УДК 004.056.55

Исследования и анализ реализаций кандидатов второго раунда конкурса NIST PQC, ориентированных на семейства FPGA Xilinx / *М.В. Есина, Б.С. Шахов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 204. С. 40 – 58.

Сегодня достаточно остро стоит вопрос о стойкости современных существующих криптографических механизмов к квантовым алгоритмам криптоанализа в частности и квантовым компьютерам вообще. Эта проблема активно обсуждается на международном уровне. Поэтому, для ее решения NIST США решил организовать и проводит конкурс на кандидатов на постквантовые криптографические алгоритмы NIST PQC. Результатом конкурса должно стать принятие к стандартизации криптографических алгоритмов разного типа – асимметричное шифрование, инкапсуляция ключей и электронная подпись (как минимум по одному алгоритму с каждого типа). К началу конкурса на процесс стандартизации было представлено 82 алгоритмы. На основе критериев минимальной приемлемости, определенных NIST, для 1-го раунда было рассмотрено 69 алгоритмов. С учетом нескольких параметров – безопасность, стоимость, производительность, характеристики реализации и т.п., – 43 и 11 алгоритмов были исключены при завершении 1-го и 2-го раундов соответственно, а остальные 15 алгоритмов были сохранены для 3-го раунда. Алгоритмы, которые остались во 2-м раунде, можно разделить на 5 различных категорий в зависимости от математического базиса, на котором они основываются: на основе изогений эллиптических кривых, на основе алгебраических решеток, на основе математического кода, на основе многомерных преобразований и на основе хеш-функций. Безопасность является основным критерием оценки, определяет конкуренцию в конкурсе NIST, и, понятно, что реализации программного обеспечения кандидатов в основном сосредоточены на ней. Однако крайне важно, чтобы алгоритм имел и эффективную аппаратную реализацию. А своевременное выявление аппаратной неэффективности поможет сконцентрировать усилия криптографического сообщества на более перспективных кандидатах, потенциально сэкономив большое количество времени, которое может быть потрачено на криптоанализ. В данной работе рассматриваются и сравниваются между собой FPGA семейства Xilinx. Приводятся и сравниваются между собой данные по реализаций кандидатов 2-го раунда в процессе стандартизации постквантовой криптографии NIST, ориентированные на FPGA семейства Xilinx.

Ключевые слова: аппаратное обеспечение; электронная подпись; конкурс NIST PQC; постквантовая криптография; FPGA; Xilinx.

Табл. 12. Библиогр.: 10 назв.

UDC 004.056.55

Research and analysis of implementations of the NIST PQC competition second round candidates focused on the Xilinx FPGA family / *M.V. Yesina, B.S. Shahov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №204. P. 40 – 58.

Today, the question of the stability of modern existing cryptographic mechanisms to quantum algorithms of cryptanalysis in particular and quantum computers in general is quite acute. This issue is actively discussed at the interna-

tional level. Therefore, to solve it, NIST USA has decided to organize and is currently holding a competition for candidates for post-quantum cryptographic algorithms NIST PQC. The result of the competition should be the adoption of various types of cryptographic algorithms for standardization, namely, asymmetric encryption, key encapsulation and electronic signature (at least one algorithm of each type). 82 algorithms were submitted by the start of the competition for the standardization process. Based on the minimum eligibility criteria defined by NIST, 69 algorithms were considered for the 1st round. Given several parameters, namely, security, cost, performance, implementation characteristics, etc., 43 and 11 algorithms were excluded at the end of the 1st and 2nd rounds, respectively, and the other 15 algorithms were left for participation in the 3rd round. The algorithms left in the 2nd round can be divided into 5 different categories depending on their mathematical basis: those based on the isogeny of elliptic curves, those based on algebraic lattices, those based on mathematical code, those based on multivariate transformations and those based on hash functions. Security is the main evaluation criterion that determines competition in the NIST competition, and it is clear that candidates' software implementations are focused mainly on it. However, it is extremely important that the algorithm has an effective hardware implementation. Timely identification of hardware inefficiencies will help focus the cryptographic community efforts on more promising candidates, potentially saving a large amount of time that can be spent on cryptanalysis. This paper discusses and compares the FPGAs of Xilinx family. Data on the implementation of the candidates of the 2nd round in the process of standardization of post-quantum cryptography NIST, which are focused on the FPGA of the Xilinx family, are presented and compared.

Key words: hardware; electronic signature; NIST PQC competition; post-quantum cryptography; FPGA; Xilinx.
12 tab. Ref: 10 items.

УДК 003.026:004.056

Аналіз складності атак на мультиваріативні криптографічні перетворення з використанням алгебраїчної структури поля / *С.О. Кандій, Г.А. Малєєва* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 204. С. 59 – 65.

В останні роки інтерес до криптосистем, що ґрунтуються на багатовимірних квадратичних перетвореннях (MQ-перетвореннях), значно зріс. В першу чергу це пов’язано з конкурсом NIST PQC [1] та необхідністю у практичних схемах електронного підпису, що є стійкими до атак на квантових комп’ютерах. Незважаючи на те, що світовою спільнотою була проведена велика робота з криптоаналізу представлених схем, багато питань потребують подальшого уточнення. Спеціалісти NIST дуже обережно підходять до процесу стандартизації і закликають криптологів [4] у найближчі три роки провести всесторонній аналіз фіналістів конкурсу NIST PQC перед їх стандартизацією.

Одним з фіналістів є схема електронного підпису Rainbow [2]. Вона є узагальненням схеми UOV (Unbalanced Oil and Vinegar) [3]. Нещодавно на інше узагальнення цієї схеми – LUOV (Lifted UOV) [5] була знайдена атака [6], що за поліноміальний час здатна повністю відновити закритий ключ. Особливістю цієї атаки є використання алгебраїчної структури поля, над яким задане MQ-перетворення. Цей напрямок атак з’явився нещодавно і досі не зрозуміло чи можливо використовувати структуру поля у схемі Rainbow.

Метою цієї роботи є систематизація технік, що використовуються у атаках з використанням алгебраїчної структури поля для криптосистем на основі UOV та аналіз перешкод для їх узагальнення на схему Rainbow.

Ключові слова: класичний та квантовий криптоаналіз; диференційні атаки на підполе; аналіз атак; постквантовий період.
Бібліогр.: 8 назв.

УДК 003.026:004.056

Анализ сложности атак на мультивариативные криптографические преобразования с использованием алгебраической структуры поля / *С.О. Кандий, А.А. Малеева* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 204. С. 59 – 65.

В последние годы интерес к криптосистемам, основанным на многомерных квадратичных преобразованиях (MQ-преобразованиях), значительно возрос. В первую очередь это связано с конкурсом NIST PQC [1] и необходимостью в практических схемах электронной подписи, которые являются стойкими к атакам на квантовых компьютерах. Несмотря на то, что мировым сообществом была проведена большая работа по криптоанализу представленных схем, многие вопросы требуют дальнейшего уточнения. Специалисты NIST очень осторожно подходят к процессу стандартизации и призывают криптологов [4] в ближайшие 3 года провести всесторонний анализ финалистов конкурса NIST PQC перед их стандартизацией.

Один из финалистов схема электронной подписи Rainbow [2]. Она является обобщением схемы UOV (Unbalanced Oil and Vinegar) [3]. Недавно на другое обобщение этой схемы – LUOV (Lifted UOV) [5] была найдена атака [6], которая за полиномиальное время способна полностью восстановить закрытый ключ. Особенностью этой атаки является использование алгебраической структуры поля, над которым задано MQ-преобразования. Это направление атак появилось недавно и до сих пор не понятно возможно ли использовать структуру поля в схеме Rainbow.

Целью настоящей работы является систематизация техник, используемых в атаках с использованием алгебраической структуры поля для криптосистем на основе UOV, и анализ препятствий для их обобщения на схему Rainbow.

Ключевые слова: классический и квантовый криптоанализ; дифференциальные атаки на подполе; анализ атак; постквантовий период.

Библиогр.: 8 назв.

UDC 003.026:004.056

Analysis of the complexity of attacks on multivariate cryptographic transformations using algebraic field structure / *S. Kandiy, G. Maleeva* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №204. P. 59 – 65.

In recent years, interest in cryptosystems based on multidimensional quadratic transformations (MQ transformations) has grown significantly. This is primarily due to the NIST PQC competition [1] and the need for practical electronic signature schemes that are resistant to attacks on quantum computers. Despite the fact that the world community has done a lot of work on cryptanalysis of the presented schemes, many issues need further clarification. NIST specialists are very cautious about the standardization process and urge cryptologists [4] in the next 3 years to conduct a comprehensive analysis of the finalists of the NIST PQC competition before their standardization.

One of the finalists is the Rainbow electronic signature scheme [2]. It is a generalization of the UOV (Unbalanced Oil and Vinegar) scheme [3]. Recently, another generalization of this scheme – LUOV (Lifted UOV) [5] was found to attack [6], which in polynomial time is able to recover completely the private key. The peculiarity of this attack is the use of the algebraic structure of the field over which the MQ transformation is given. This line of attack has emerged recently and it is still unclear whether it is possible to use the field structure in the Rainbow scheme.

The aim of this work is to systematize the techniques used in attacks using the algebraic field structure for UOV-based cryptosystems and to analyze the obstacles for their generalization to the Rainbow scheme.

Key words: classical and quantum cryptanalysis; differential attacks on the underground; attack analysis; postquantum period.

Ref: 8 items.

УДК 621.391:519.2

Деякі результати розробки схем криптографічних перетворень з використанням неабелевих груп / *Є.В. Котух, О.В. Северинов, А.В. Власов, А.О. Теницька, Е. О. Зарудна* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 204. С. 66 – 72.

З появою практичних результатів в реалізації алгоритмів Шора і Гровера на квантових комп'ютерах реалізація успішної атаки на класичні криптосистеми з відкритим ключем стає дедалі реальною. Сучасні результати у вирішенні завдання побудови квантового комп'ютера достатньої потужності обґрунтовують необхідність до перегляду існуючих підходів і визначення найбільш ефективних, з точки зору вирішення завдань постквантової криптографії. Одним з таких перспективних дослідницьких пріоритетів є дослідження криптосистем на основі неабелевих груп.

Проблеми пошуку пов'язаності, пошуку членства й інші варіанти є складно вирішувані в теорії неабелевих груп і є основою для побудови доказово безпечних криптосистем з відкритим ключем. В роботі надано огляд найбільш часто обговорюваних алгоритмів з використанням неабелевих груп: групи матриць, групи кіс, напівпрямі добутки і алгебраїчні ластики (AE). Наведено аналіз побудови схем шифрування і дешифрування, механізмів обміну ключами. Багато неабелевих протоколів встановлення ключів на основі груп пов'язані з протоколом Діффі – Хеллмана (DH). В роботі проаналізовано властивості неабелевих групових схем шифрування з відкритим ключем. Розглядаються різні криптографічні примітиви, які використовують некомутативні групи в якості основи для постквантових схем.

Ключові слова: постквантова криптографія; напівпрямі добутки; групи матриць; групи кіс; логарифмічні підписи; алгебраїчний ластик.

Бібліогр.: 22 назв.

УДК 621.391:519.2

Некоторые результаты разработки схем криптографических преобразований с использованием неабелевых групп / *Е.В. Котух, А.В. Северинов, А.В. Власов, А.А. Теницкая, Е. А. Зарудная* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 204. С. 66 – 72.

С появлением практических результатов в реализации алгоритмов Шора и Гровера на квантовых компьютерах, реализация успешной атаки на классические криптосистемы с открытым ключом становится все более реальной. Современные результаты в решении задачи построения квантового компьютера достаточной мощности обосновывают необходимость к пересмотру существующих подходов и определению наиболее эффективных с точки зрения решения задач постквантовой криптографии. Одним из таких перспективных исследовательских приоритетов является исследование криптосистем на основе неабелевых групп.

Проблемы поиска сопряженности, поиска членства и другие варианты являются сложно решаемыми в теории неабелевых групп и являются основой для построения доказуемо безопасных криптосистем с открытым ключом. В работе дается обзор наиболее часто обсуждаемых алгоритмов с использованием неабелевых групп: группы матриц, группы кос, полупрямые произведения и алгебраические ластики (AE). Приводится анализ построения схем шифрования и дешифрования, механизмов обмена ключами. Многие неабелевы протоколы установления ключей на основе групп связаны с протоколом Диффи – Хеллмана (DH). В работе анализируются

свойства неабелевых групповых схем шифрования с открытым ключом. Рассматриваются различные криптографические примитивы, использующие некоммутативные группы в качестве основы для постквантовых схем.

Ключевые слова: постквантовая криптография; полупрямые произведения; группы матриц; группы кос; логарифмические подписи; алгебраический ластик.

Библиогр.: 22 назв.

UDC 621.391:519.2

Towards results of cryptographic transformations schemes development with application of nonabelian groups / *E.V. Kotukh, O.V. Severinov, A.V. Vlasov, A.O. Tenytska, E.O. Zarudna* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №204. P. 66 – 72.

The implementation of a successful attack on classical public key cryptosystems becomes real with the advent of practical results in the implementation of Shor's and Grover's algorithms on quantum computers. Modern results in solving the problem of the powerful enough quantum computer construction substantiate the need to revise the existing approaches and determine the most effective from the post-quantum cryptography point of view. One of these promising research priorities is the study of cryptosystems based on non-abelian groups.

The problems of conjugacy search, membership search, and others are difficult to solve in the theory of non-abelian groups and can be considered as a basis for constructing provably secure public key cryptosystems. This paper gives an overview of the most frequently discussed algorithms using non-abelian groups: matrix groups, braid groups, semidirect products, and algebraic erasers (AE). The analysis of the construction of encryption and decryption schemes, key establishment mechanisms is given. Many non-abelian group-based key establishment protocols are associated with the Diffie – Hellman (DH) protocol. The paper analyzes the properties of non-abelian group public key encryption schemes. Various cryptographic primitives are considered that using non-commutative groups as a basis for post-quantum schemes.

Key words: post-quantum cryptography; semidirect products; matrix groups, braid groups; logarithmic signatures; algebraic eraser.

Ref: 22 items.

РАДІОТЕХНІЧНІ ТА ТЕЛЕКОМУНІКАЦІЙНІ МЕРЕЖІ ТА СИСТЕМИ
РАДИОТЕХНИЧЕСКИЕ И ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ И СИСТЕМЫ
RADIO AND TELECOMMUNICATION NETWORKS AND SYSTEMS

УДК 621.3.006.357

Метод оптимізації розподілу частотного ресурсу з повторним використанням частот для систем когнітивного радіо / *Ю.Ю. Коляденко, О.В. Коляденко, Б.П. Муляр* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 204. С. 73 – 79.

Концепція когнітивного радіо може бути охарактеризована як радіо з вивченням можливостей, тобто як радіо, яке в змозі отримати знання про радіосередовище і коригувати свої експлуатаційні параметри і протоколи відповідно.

На етапі функціонування мережі когнітивного радіо при розподілі частотного ресурсу між абонентськими станціями актуальною є задача мінімізації смуги частот. В умовах постійно зростаючого попиту на смуги частот постановка такого завдання обумовлена необхідністю підвищення ефективного використання радіочастотного спектру із застосуванням методів повторного використання частот.

В роботі запропонований метод забезпечення повторного використання частот, заснований на отриманні оцінок взаємних відстаней між абонентськими станціями в реальному масштабі часу. Запропоновано алгоритм розв'язання задачі оптимізації розподілу частотного ресурсу для мережі когнітивного радіо з повторним використанням частот. В основі алгоритму лежить метод локальної оптимізації – один з наближених методів дискретного програмування. В даному випадку умовою локальної оптимальності є те, що робоча частота, яка присвоюється черговій абонентській станції, повинна бути найближчою до присвоєної на попередньому кроці частоті.

За допомогою імітаційного моделювання проведено аналіз ефективності алгоритму оптимізації розподілу частотного ресурсу для мережі LTE. Отримано залежності ширини смуги частот від кількості абонентських станцій, що обслуговуються. Аналіз показав, що використання даного алгоритму дозволяє в 2 – 3 рази скоротити смугу частот. Також аналіз показав, що з ростом числа абонентських станцій, які одночасно обслуговуються, ефективність алгоритму підвищується.

Ключові слова: розподіл частотного ресурсу; мережа когнітивного радіо; повторне використання частот.

Іл. 7. Бібліогр.: 9 назв.

УДК 621.3.006.357

Метод оптимизации распределения частотного ресурса с повторным использованием частот для систем когнитивного радио / *Ю.Ю. Коляденко, А.В. Коляденко, Б.П. Муляр* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 204. С. 73 – 79.

Концепция когнитивного радио может быть охарактеризована как радио с изучением возможностей, то есть как радио, которое в состоянии получить знания о радиосреде и корректировать свои эксплуатационные параметры и протоколы соответственно.

На этапе функционирования сети когнитивного радио при распределении частотного ресурса между абонентскими станциями актуальна задача минимизации полосы частот. В условиях постоянно растущего спроса на полосы частот постановка такой задачи обусловлена необходимостью повышения эффективного использования радиочастотного спектра с применением методов повторного использования частот.

В работе предложен метод обеспечения повторного использования частот, основанный на получении оценок взаимных расстояний между абонентскими станциями в реальном масштабе времени. Предложен алгоритм решения задачи оптимизации распределения частотного ресурса для сети когнитивного радио с повторным использованием частот. В основе алгоритма лежит метод локальной оптимизации – один из приближенных методов дискретного программирования. В данном случае условием локальной оптимальности является то, что рабочая частота, присваиваемая очередной абонентской станции, должна быть ближайшей к присвоенной на предыдущем шаге частоте.

С помощью имитационного моделирования проведен анализ эффективности алгоритма оптимизации распределения частотного ресурса для сети LTE. Получены зависимости ширины полосы частот от количества обслуживаемых абонентских станций. Анализ показал, что использование данного алгоритма позволяет в 2 – 3 раза сократить полосу частот. Также анализ показал, что с ростом числа абонентских станций, которые одновременно обслуживаются, эффективность алгоритма повышается.

Ключевые слова: распределение частотного ресурса; сеть когнитивного радио; повторное использование частот.

Ил. 7. Библиогр.: 9 назв.

UDC 621.3.006.357

Method for optimization of frequency resource allocation with frequency reuse for cognitive radio systems / *Yu.Yu. Kolyadenko, O.B. Kolyadenko, B.P. Mulyar* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №204. P. 73 – 79.

The concept of cognitive radio can be described as a radio with the study of capabilities, i.e. as a radio that is able to gain knowledge about the radio environment and adjust its operating parameters and protocols accordingly.

The task of minimizing the frequency band is relevant at the stage of the cognitive radio network functioning when distributing the frequency resource between subscriber stations. With the ever-growing demand for frequency bands, this challenge is driven by the need to improve the efficient use of the radio frequency spectrum through frequency reuse methods.

This paper proposes a method for ensuring the reuse of frequencies based on obtaining estimates of mutual distances between subscriber stations in real time. An algorithm is proposed for solving the problem of frequency resource allocation optimization for a cognitive radio network with frequency reuse. The algorithm is based on the method of local optimization, one of the approximate methods of discrete programming. In this case, the condition of local optimality is that the operating frequency assigned to the next subscriber station must be the closest to the frequency assigned in the previous step.

The efficiency of the frequency resource optimization algorithm for the LTE network was analyzed using simulation modeling. The dependences of the bandwidth on the number of subscriber stations served are obtained. The analysis showed that the use of this algorithm allows to reduce the frequency band by 2 -3 times. The analysis also showed that the efficiency of the algorithm increases with the growth of the number of subscriber stations served simultaneously.

Key words: frequency resource allocation; cognitive radio network; frequency reuse.

7 fig. Ref: 9 items.

УДК 355.457.2:358.11.6 (043.3)

Архітектура сітьової бази знань складної системи воєнного призначення / *М.О. Єрмошин, А.А Побережний, О.С. Онопрієнко, М.П. Шурига* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 204. С. 80 – 92.

Розглядається архітектура сітьової бази знань та організаційна структура складної системи воєнного призначення, що будується при створенні угруповання військ (сил) та підтриманні його у стані, коли воно здатне вирішувати покладені на нього завдання. Це вимагає глибокого розроблення питань не тільки сучасної тактики щодо підготовки та ведення бойових дій, а й ще більш складних питань наукового обґрунтування архітектури сітьової бази знань та структури складної системи воєнного призначення з сітьовою базою знань. Внутрішню уяву знань у базі знань (формальний програмно-логічний зміст) доцільно реалізовувати у вигляді матриці суміжності, що відображає відношення та взаємозв'язок між цільовими установами; початковими умовами; ресурсами угруповання військ (часовими, матеріальними, бойовими та кількісного складу), їх витратами та поповненням; правил витрати ресурсів і вибору критеріїв їх розподілу. У базі знань здійснюється синтез математичної сітьової моделі вироблення рішень, що забезпечує зміну (корекцію) структури цільових установок при поповненні бази знань. Задачі, що розв'язуються у базі знань, такі: виділення вершин і відношень при поповненні

каталогів; внесення зміни до матриці суміжності у відповідності до виявлених або змінених відношень між цільовими установками. Необхідним елементом синтезу математичної сітьової моделі вироблення рішень щодо підготовки та ведення бойових дій є побудова структури цільових установок системи для конкретної ситуації. Особливістю контролю коректності знань, що надані у вигляді цільових установок, є необхідність сумісного аналізу всієї сукупності цільових установок і початкових умов у їх взаємозв'язку. Для цього здійснюється об'єднання матриці відношень цільових установок і матриці відношень початкових умов. Контроль коректності бази знань здійснюється при поповненні бази знань, він включає: виявлення протиріч в структурі цільових установок при внесенні змін в цю структуру; пошук та виявлення протиріч графу семантичної мережі згідно наявним ресурсам і часу; перевірку повноти графу математичної сітьової моделі; видачу виявлених протиріч експерту та їх усунення. Практичний підхід щодо побудови архітектури сітьової бази знань та організаційної структури складної системи воєнного призначення може бути реалізований під час обґрунтування компонентів та елементів системи при створенні угруповання військ (сил).

Ключові слова: структура системи воєнного призначення; сітьова база знань.

Іл. 3. Бібліогр.: 12 назв.

УДК 355.457.2:358.11.6 (043.3)

Архитектура сетевой базы знаний сложной системы военного назначения / *М.А. Ермошин, А.А Побережный, А.С. Оноприенко, М.П. Шурыга* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 204. С. 80 – 92.

Рассматривается архитектура сетевой базы знаний и организационная структура сложной системы военного назначения, которая строится при создании группировки войск (сил) и поддержании ее в состоянии, когда она способна решать возложенные на нее задачи. Это требует глубокой проработки вопросов не только современной тактики относительно подготовки и ведения боевых действий, но и более сложных вопросов научного обоснования архитектуры сетевой базы знаний и структуры сложной системы военного назначения с сетевой базой знаний. Внутреннее представление знаний в базе знаний (формальное программно-логическое содержание) целесообразно реализовывать в виде матрицы смежности, которая отображает отношения и взаимосвязь между целевыми установками; начальными условиями; ресурсами группировки войск (временными, материальными, боевыми и количественного состава), их затратами и пополнением; правилами расходования ресурсов и выбора критериев их распределения. В базе знаний осуществляется синтез математической сетевой модели выработки решений, которая обеспечивает изменение (коррекцию) структуры целевых установок при пополнении базы знаний. Задачи, решаемые в базе знаний: выделение вершин и отношений при пополнении каталогов; внесение изменений в матрицу смежности в соответствии с выявленными или измененными отношениями между целевыми установками. Необходимым элементом синтеза математической сетевой модели выработки решений по подготовке и ведению боевых действий является построение структуры целевых установок системы для конкретной ситуации. Особенностью контроля корректности знаний, представленных в виде целевых установок, есть необходимость совместного анализа всей совокупности целевых установок и начальных условий в их взаимосвязи. Для этого осуществляется объединение матрицы отношений целевых установок и матрицы отношений начальных условий. Контроль корректности базы знаний осуществляется при пополнении базы знаний, он включает: выявление противоречий в структуре целевых установок при внесении изменений в эту структуру; поиск и обнаружение противоречий в графе семантической сети согласно располагаемым ресурсам и времени; проверку полноты графа математической сетевой модели; выдачу выявленных противоречий эксперту и их устранение. Практический подход относительно построения архитектуры сетевой базы знаний и организационной структуры сложной системы военного назначения может быть реализован во время обоснования компонентов и элементов системы при создании группировки войск (сил).

Ключевые слова: структура системы военного назначения; сетевая база знаний.

Ил. 3. Библиогр.: 12 назв.

UDC 355.457.2:358.11.6 (043.3)

Architecture of network knowledge base of a complex military system / *M. Yermoshyn, A. Poberezhnyi, O. Onopriyenko, M. Shuryha* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №204. P. 80 – 92.

The article examines the architecture of a networked knowledge base and the organizational structure of a complex military-purpose system, which is built when a group of troops (forces) is created and kept in a state where it is capable of solving the tasks assigned to it. This requires a deep study of issues not only of modern tactics regarding the preparation and conduct of hostilities, but also more complex issues of scientific substantiation of the architecture of a networked knowledge base and the structure of a complex military system with a networked knowledge base. The internal representation of knowledge in the knowledge base (formal programmatic and logical content) is advisable to implement in the form of an adjacency matrix, which displays the relationship and relationship between target settings; initial conditions; the resources of the grouping of troops (temporary, material, combat and quantitative composition), their costs and replenishment; rules for the use of resources and the choice of criteria for their distribution. The knowledge base synthesizes a mathematical network model for making decisions, which provides a change (correction) of the structure of target attitudes when replenishing the knowledge base. Tasks solved in the knowledge base: selection of vertices and relations when replenishing catalogs; making changes to the adjacency matrix in accordance with the identified or changed relationships between targets. A necessary element of the synthesis of a mathematical network model for making decisions on the preparation and conduct of hostilities is the construction of the structure of the target

systems of the system for a specific situation. A feature of controlling the correctness of knowledge presented in the form of target attitudes is the need for a joint analysis of the entire set of target attitudes and initial conditions in their relationship. For this, the matrix of the relations of target attitudes and the matrix of the relations of initial conditions are combined. The control of the correctness of the knowledge base is carried out when replenishing the knowledge base, it includes: identification of contradictions in the structure of target attitudes when making changes to this structure; search and detection of contradictions in the graph of the semantic network according to available resources and time; checking the completeness of the graph of the mathematical network model; issuance of revealed contradictions to an expert and their elimination. A practical approach to building the architecture of a networked knowledge base and the organizational structure of a complex military system can be implemented during the substantiation of the components and elements of the system when creating a grouping of troops (forces).

Key words: structure of the military system; network knowledge base.

3 fig. Ref: 12 items.

УДК 621.396

Про ефект Доплера в радіолокації / *О.В. Рязанцев, С.В. Марченко, М.В. Кулик* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 204. С. 93 – 98.

Аналізуються можливості одночасного використання поздовжнього і поперечного ефектів Доплера, а також отримано вирази відповідних частот биття між випромінюваним і прийнятим сигналами.

Як правило, в сучасних радіотехнічних системах використовується тільки поздовжній ефект Доплера, що дозволяє визначити радіальну складову швидкості руху об'єкта. Крім того, існують ситуації, для яких взагалі неможливо визначити швидкість об'єкта без урахування поперечного ефекту Доплера.

В роботі проведено аналіз принципових можливостей вдосконалення функціонування радіолокаційних станцій, одночасно використовуються обидва типи ефектів Доплера – поздовжній і поперечний, що дозволяє визначити повну швидкість об'єкта, що спостерігається в будь-яких ситуаціях.

Проаналізовано поздовжній і поперечний ефекти Доплера для випадку рухомого об'єкта, що випромінює, та отримано вирази для доплерівського зсуву, а також визначено вирази частоти биття в разі активної радіолокаційної станції для обох видів ефектів Доплера, що дозволяють отримати величину швидкості об'єкта в будь-яких ситуаціях.

Запропоновано варіанти визначення повної швидкості рухомого об'єкту з урахуванням визначення її радіальної і тангенціальної компонент. Розглянуто ідеалізовані ситуації, в яких проявляється тільки один з ефектів Доплера.

Ключові слова: поперечний та повздовшній ефекти Доплера; швидкість об’єкта; радіолокаційна станція; система відліку.

Іл. 5. Бібліогр.: 5 назв.

УДК 621.396

Об эффекте Доплера в радиолокации / *О.В. Рязанцев, С.В. Марченко, М.В. Кулик* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 204. С. 93 – 98.

Анализируются возможности одновременного использования продольного и поперечного эффектов Доплера, а также получены выражения соответствующих частот биений между излучаемым и принимаемым сигналами.

Как правило, в современных радиотехнических системах используется только продольный эффект Доплера, позволяющий определить радиальную составляющую скорости движения объекта. Кроме того, существуют ситуации, для которых вообще невозможно определить скорость объекта без учета поперечного эффекта Доплера.

Проведен анализ принципиальных возможностей совершенствования функционирования радиолокационных станций, одновременно использующих оба типа эффектов Доплера – продольный и поперечный, что позволяет определить полную скорость наблюдаемого объекта в любых ситуациях.

Авторами проанализированы продольный и поперечный эффекты Доплера для случая движущегося излучающего объекта, получены выражения для доплеровского сдвига, а также определены выражения частоты биений в случае активной радиолокационной станции для обоих видов эффектов Доплера, позволяющие получить величину скорости объекта в любых ситуациях.

Предложены варианты определения полной скорости движущегося объекта с учетом определения ее радиальной и тангенциальной компонент. Рассмотрены идеализированные ситуации, в которых проявляется только один из эффектов Доплера.

Ключевые слова: поперечный и продольный эффекты Доплера; скорость объекта; радиолокационая станция; система отсчета.

Ил. 5. Библиогр.: 5 назв.

UDC 621.396

On the Doppler effect in radar / *O.V. Ryazantsev, S.V. Marchenko, M.V. Kulik* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №204. P. 93 – 98.

The possibilities of simultaneous use of the longitudinal and transverse Doppler effects have been analyzed, and expressions have been derived for the corresponding beat frequencies between the emitted and received signals.

As a rule, only the longitudinal Doppler effect is used in modern radio engineering systems, which makes it possible to determine the radial component of the object's speed. In addition, there are situations for which it is generally impossible to determine the speed of an object without taking into account the transverse Doppler effect.

The authors analyze the fundamental possibilities of improving the functioning of radar stations that simultaneously use both types of Doppler effects – longitudinal and transverse ones – making it possible to determine the total speed of the observed object in any situations.

The authors have analyzed the longitudinal and transverse Doppler effects for the case of a moving emitting object, derived expressions for the Doppler shift and expressions for the beat frequency in the case of an active radar station for both types of Doppler effects, which make it possible to obtain the value of the object's speed in any situations.

Variants of determining the total speed of a moving object have been proposed, accounting the determination of its radial and tangential components. Idealized situations in which only one of the Doppler effects appeared have been considered.

Key words: the longitudinal and transverse Doppler effects; object speed; radar station; reference system

5 fig. Ref: 5 items.

УДК 621.391.5: 004.056.53

Підслуховування NFC-зв'язку на частотах вищих гармонік / *В.Г. Крижановський, С.П. Сергієнко, Д.В. Чернов, В.В. Крижановський* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 204. С. 99 – 104.

Широке використання технології NFC-комунікації у близькому полі спонукає розглядати різні аспекти безпеки її використання. Відомі приклади обміну інформацією з карткою на відстані, яка значно більше ніж типові максимальні 5 – 10 см. Також привертає увагу можливість отримати сигнал з картки на частотах вищих гармонік, які потенційно можуть випромінюватися у вигляді електромагнітних хвиль, а не тільки існувати як індуктивне поле котушки зв'язку. В роботі досліджено випромінювання третьої гармоніки частоти 13,36 МГц карткою стандарту ISO 14443-3A у різних режимах збудження, – за допомогою пристрою RFID-RC522, смартфона Sony Xperia Z5 Premium та сигналом 13,36 МГц з прямокутною модуляцією 10 % на частоті піднесучої відповіді картки 847,5 кГц. В програмі аналізу електронних схем проведено моделювання відгуку картки в діапазоні третьої гармоніки. І моделювання і експеримент підтвердили, що найбільшим сигналом (крім основного) є сигнал на частоті третьої гармоніки та її бокових частотах 40,68 ± 0,8475 МГц. Для прийому сигналу на частоті третьої гармоніки було виготовлено резонансну антену у вигляді кільцевого вібратора, що навантажений на ємність. Це дозволяє зменшити розміри приймальної системи, хоча проблема складної взаємодії електромагнітних полів та антенних структур у ближній зоні залишається відкритою. За результатами вимірювання характеристик імпедансу цієї антени було визначено її вузьку смугу частот, що ускладнює прийом сигналу відповіді картки. Експерименти з використання трьох методів генерації сигналу відповіді картки показали, що сигнал третьої гармоніки реєструється на відстані більше 1,5 м, що може скласти загрозу для безпеки транзакцій за допомогою платіжних банківських карт. Разом з тим, великий вплив шуму при такій відстані може зробити неможливим детектування короткочасного сигналу від картки, що потребує додаткового вивчення.

Ключові слова: NFC пристрої; RFID пристрої; вищі гармоніки робочої частоти; спектральний склад випромінювання; кібербезпека.

Табл. 1. Іл. 12. Бібліогр.: 11 назв.

УДК 621.391.5: 004.056.53

Прослушивание NFC-связи на частотах высших гармоник / *В.Г. Крыжановский, С.П. Сергиенко, Д.В. Чернов, В.В. Крыжановский* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 204. С. 99 – 104.

Широкое использование технологии NFC-коммуникации в ближнем поле вызывает интерес к различным аспектам безопасности ее использования. Известны примеры обмена информацией с карточкой на расстоянии большем, чем стандартные 5–10 см. Также интересна возможность использовать сигналы высших гармоник, которые потенциально могут излучаться в виде электромагнитных волн, а не только существовать как индуктивное поле рассеяния. В работе исследовано излучение третьей гармоники частоты 13,56 МГц карточкой стандарта ISO 14443-3A в разных режимах возбуждения, – с помощью устройства RFID-RC522, смартфона Sony Xperia Z5 Premium и сигналом 13,56 с прямоугольной модуляцией 10 % на частоте поднесущего ответа карточки 847,5 кГц. В программе анализа электронных схем промоделировано отклик карточки в диапазоне третьей гармоники. И моделирование, и эксперимент подтвердили, что наибольшим сигналом (кроме сигнала на основной частоте) есть сигнал на частоте третьей гармоники и ее боковых частотах 40,68 ± 0,8475 МГц. Для приема сигнала на частоте третьей гармоники была изготовлена резонансная антенна в виде кольцевого вибратора, нагруженного на емкость. Это позволяет уменьшить размеры приемной системы, но остается проблема сложной структуры полей в ближней зоне излучающих структур. При измерении входного импеданса антенны отмечена ее узкая полоса рабочих частот, что затрудняет регистрацию сигнала ответа карточки. Эксперименты с исполь-

зованием трех методов генерации сигнала подтвердили, что сигнал третьей гармоники регистрируется на расстоянии больше 1,5 м, что может представлять угрозу для безопасности транзакций с помощью бесконтактных карт. Вместе с тем, влияние высокого уровня шума на таком расстоянии может сделать невозможным декодирование кратковременного сигнала от карточки, что требует дополнительного изучения.

Ключевые слова: NFC устройства; RFID метки; высшие гармоники рабочей частоты; спектральный состав излучения; кибербезопасность.

Табл. 1. Ил. 12. Библиогр.: 11 назв.

UDC 621.391.5: 004.056.53

Listening to NFC at higher harmonic frequencies / *V.G. Kryzhanovskyi, S.P. Serhiienko, D.V. Chernov, V.V. Kryzhanovskyi* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №204. P. 99 – 104.

The widespread use of the NFC technology (Near Field Communication) arouses interest to various security aspects. There are known examples of information exchange with card at a distance greater than standard 5-10 cm. It is also interesting to use signals of higher harmonics, which potentially may be radiated in the form of electromagnetic waves, rather than exists as a magnetic field of scattering. In this work, the radiation of third harmonic by card of standard ISO 14443-3A with the fundamental frequency 13.56 MHZ for various excitation modes using the RFID-RC522 reader, smartphone Sony Xperia Z5 Premium, and continuous 10% amplitude modulated 13.56 MHz signal from generator with the subcarrier of imitated smart card response 847.5 kHz was investigated. The card response at third harmonic was simulated in circuit analysis software. Both simulation and experiment proved, that the third harmonic with its side frequencies 40,68 ± 0,8475 MHz have the highest level after the fundamental. To receive the third harmonic signal, the resonant loop antenna in the form of ring vibrator loaded on capacitor was used. This allows the sizes of the received system to be reduced, but the problem of complex field structure in the near-field zone remains. Due to narrow bandwidth of the receiver antenna, the registration of card response signal was complicated. The experiments with three methods of signal generation proved, that third-harmonic signal is registered at the distance more than 1.5m, which may pose a threat for contactless smart-cards transactions security. At the same time, the influence of high level of noise at such a distance may cause difficulties to decode the short-duration signals, which requires further study.

Key words: NFC devices; RFID devices; higher operating frequency harmonics; radiation spectrum; cybersecurity.

1 tab. 12 fig. Ref: 11 items.

ФІЗИКА ПРИЛАДІВ ТА СИСТЕМ
ФИЗИКА ПРИБОРОВ И СИСТЕМ
PHYSICS OF INSTRUMENTS AND SYSTEMS

УДК 621.793:678.073

Дисперсія наночасток в оптично прозорі полімерні матриці / *В.М. Борщов, О.М. Лістратенко, М.А. Проценко, І.Т. Тимчук, О.В. Кравченко, О.В. Суддя, М.І. Сліпченко, Б.М. Чічков* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 204. С. 105 – 114.

Проведено пошук і аналіз даних, результатів теоретичних і експериментальних досліджень, матеріалів дисертацій, літературних джерел та патентів в області оптичного і оптико-електронного приладобудування. Узагальнено отримані дані та рекомендації з розробки методів дисперсії наночасток в полімерні матриці при створенні оптично прозорих нанокомпозитів для застосування у багатьох областях науки та техніки. Аналіз розглянутих робіт дозволяє зробити висновок, що для створення гібридних органо-неорганічних композитів з високим рівнем дисперсності неорганічного компоненту доводиться вирішувати проблеми, пов'язані з сумісністю компонент і стабілізацією наночасток наповнювача в полімерній матриці. У зв'язку з обмеженою кількістю гідрофільних полімерів, здатних до формування композитів з наночастками без стабілізаторів, основними підходами до отримання гібридних композитів є використання модифікуючих добавок поверхнево активних речовин, а також проведення складних хімічних реакцій на поверхні наночасток неорганічного наповнювача. Дані способи отримання нанокомпозитів з наночастками трудомісткі пов'язані з утворенням побічних продуктів і додатковим очищенням. Показано, що серед великої кількості нанодисперсних наповнювачів полімерних матриць при отриманні композиційних матеріалів великою увагою користуються діоксид титану (TiO_2) і оксид цинку (ZnO). Існує безліч методів синтезу наночасток ZnO та TiO_2 з різними формами і розмірами, в тому числі метод лазерної абляції, який є зручним і універсальним способом отримання наносуспензій твердофазних матеріалів в рідині. Переваги перед іншими способами синтезу наночасток, як простота методу, екологічність, низька вартість і можливість отримувати більш чисті колоїдні розчини без використання поверхнево-активних речовин та інших домішок, зробили лазерну абляцію в рідкому середовищі популярною серед дослідників.

Ключові слова: дисперсія наночасток; наноматеріали; оптично прозорі полімерні матриці.

Іл. 3. Бібліогр.: 23 назв.

УДК 621.793:678.073

Дисперсия наночастиц в оптически прозрачные полимерные матрицы / *В.Н. Борщев, А.М. Листратенко, М.А. Проценко, И.Т. Тымчук, А.В. Кравченко, А.В. Судья, Н.И. Слипченко, Б.Н. Чичков* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 204. С. 105 – 114.

Проведен поиск и анализ данных, результатов теоретических и экспериментальных исследований, материалов диссертаций, литературных источников и патентов в области оптического и оптико-электронного приборостроения. Обобщены полученные данные и рекомендации по разработке методов дисперсии наночастиц в полимерные матрицы при создании оптически прозрачных нанокомпозитов для применения в многих областях науки и техники. Анализ рассмотренных работ позволяет сделать вывод, что для создания гибридных органо-неорганических композитов с высоким уровнем дисперсности неорганического компонента приходится решать проблемы, связанные с совместимостью компонент и стабилизацией наночастиц наполнителя в полимерной матрице. В связи с ограниченным кругом гидрофильных полимеров, способных к формированию композитов с наночастицами без стабилизаторов, основными подходами к получению гибридных композитов являются использование модифицирующих добавок поверхностно активных веществ, а также проведение сложных химических реакций на поверхности наночастиц неорганического наполнителя. Данные способы получения нанокомпозитов с наночастицами трудоемки, связаны с образованием побочных продуктов и дополнительной очисткой. Показано, что среди большого числа нанодисперсных наполнителей полимерных матриц при получении композиционных материалов большим вниманием пользуются диоксид титана (TiO_2) и оксид цинка (ZnO). Существует множество методов синтеза наночастиц ZnO и TiO_2 с различными формами и размерами, в том числе метод лазерной абляции, который является удобным и универсальным способом получения наносуспензий твердофазных материалов в жидкости. Преимущества перед другими способами синтеза наночастиц, такими как простота метода, экологичность, низкая стоимость и возможность получать более чистые коллоидные растворы без использования поверхностно-активных веществ и других примесей, сделали лазерную абляцию в жидкой среде популярной среди исследователей.

Ключевые слова: дисперсия наночастиц; наноматериалы; оптически прозрачные полимерные матрицы.

Ил. 3. Библиогр.: 23 назв.

UDC 621.793:678.073

Dispersion of nanoparticles in optically transparent polymer matrices / *V.M. Borshchov, O.M. Listratenko, M.A. Protsenko, I.T. Tymchuk, O.V. Kravchenko, O.V. Syddia, M.I. Slipchenko, B.M. Chichkov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №204. P. 105 – 114.

Search and analysis of results of theoretical and experimental studies, materials of dissertations, literature sources and patents in the field of optical and optoelectronic instrumentation were carried out. Obtained data and recommendations on the development of methods for dispersing nanoparticles into polymer matrices for the creation of optically transparent nan composites for use in many fields of science and technology are generalized. Analysis of considered results makes it possible to conclude that for creating hybrid organic-inorganic composites with high level of dispersion of inorganic component, it is necessary to solve problems relating to compatibility of components and stabilization of filler nanoparticles in polymer matrix. Due to the limited range of hydrophilic polymers capable of forming composites with nanoparticles without stabilizers, the main approaches to the preparation of hybrid composites are using modifying additives of surfactants, as well as complex chemical reactions on the surface of inorganic filler nanoparticles. Such methods of obtaining nanocomposites with nanoparticles are laborious and involve formation of by-products and additional purification. It is shown that titanium dioxide (TiO_2) and zinc oxide (ZnO) are of great interest among a large number of nanodispersed fillers of polymer matrices in preparing composite materials. There are many methods for synthesis of ZnO and TiO_2 nanoparticles with various shapes and sizes, including laser ablation method, which is convenient and universal method for preparing nanosuspensions of solid-phase materials in liquid. Advantages over other methods for nanoparticle synthesis, such as the simplicity of method, environmental friendliness, low cost, and the ability to obtain cleaner colloidal solutions without using surfactants and other impurities, have made laser ablation in a liquid medium very popular among researchers.

Key words: dispersion of nanoparticles; nanomaterials; optically transparent polymer matrices

3 fig. Ref: 23 items.

УДК 681.128.82

Контроль різниці рівнів рідини в суміжних резервуарах / *Б.В. Жуков, А.В. Одновол* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 204. С. 115 – 119.

Розглянуто можливість синхронного контролю рівнів охолоджувальної рідини в системах охолоджування атомних і теплових електростанцій до і після загороджувальної сітки за допомогою спеціалізованого рівнеміра.

Представлено структурну схему рівнеміра, що забезпечує поточний синхронний контроль рівнів рідини в двох суміжних каналах (резервуарах), а також різниці рівнів рідини в них. Особливість структурної схеми спеціалізованого акустичного рівнеміра полягає у використанні загального для обох каналів джерела випромінювання і пристрою поділу спільного хвилеведучого тракту по двох каналах.

Розроблено алгоритм функціонування спеціалізованого рівнеміра, в якому на підставі часових діаграм показано як проводиться контроль рівня в кожному каналі і розраховується різниця рівнів рідини до і після загороджувальної сітки. Опис алгоритму супроводжується розрахунковими виразами для визначення рівнів та різниці рівнів рідини.

Для рівнеміра, виконаного в акустичному діапазоні хвиль, наведена умова, яка необхідна для створення пристрою, що забезпечує узгодження при розподілі загального каналу на два незалежні канали поширення

імпульсного сигналу. Дана умова дозволила встановити взаємозв'язок між внутрішніми діаметрами циліндричних труб, що застосовуються в якості хвилеведучих трактів акустичної хвилі.

Запропоновано варіанти реалізації спеціалізованого рівнеміра на базі двох модифікацій рівнеміра ЗОНД-3М, у яких в якості хвилеведучих систем застосовуються циліндричні труби. Наведено, що при використанні приємо-передавача АП-7Т рівнемір матиме робочий діапазон до 10 м при розрішенні рівнів ± 1мм, а при використанні приємо-передавача АП-70Т – робочий діапазон до 20 м при розрішенні рівнів ± 1см.

Ключові слова: рівнемір; різниця рівнів; імпульсний сигнал; хвилеведучий тракт; контроль рівня; розподільник каналів; розрішення рівнів; суміжні резервуари.

Іл. 4. Бібліогр.: 4 назв.

УДК 681.128.82

Контроль разности уровней жидкости в смежных резервуарах / *Б.В. Жуков, А.В. Одновол* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 204. С. 115 – 119.

Рассмотрена возможность синхронного контроля уровней охлаждающей жидкости в системах охлаждения атомных и тепловых электростанций до и после заграждающей сетки с помощью специализированного уровнемера.

Представлена структурная схема уровнемера, обеспечивающего текущий синхронный контроль уровней жидкости в двух смежных каналах (резервуарах), а также разности уровней жидкости в них. Особенность структурной схемы специализированного акустического уровнемера заключается в использовании общего для обоих каналов источника излучения и устройства разделения общего волноведущего тракта по двум каналам.

Разработан алгоритм функционирования специализированного уровнемера, в котором на основании временных диаграмм показано как производится контроль уровня в каждом канале и рассчитывается разность уровней жидкости до и после заграждающей сетки. Описание алгоритма сопровождается расчетными выражениями для определения уровней и разности уровней жидкости.

Для уровнемера, выполненного в акустическом диапазоне волн, приведено условие необходимое для создания устройства, обеспечивающего согласование при разделении общего канала на два независимых канала распространения импульсного сигнала. Данное условие позволило установить взаимосвязь между внутренними диаметрами цилиндрических труб, применяемых в качестве волноводных трактов акустической волны.

Предложены варианты реализации специализированного уровнемера на базе двух модификаций уровнемера ЗОНД-3М, в которых в качестве волноведущих систем применяются цилиндрические трубы. Приведено, что при использовании приемо-передатчика АП-7ВТ уровнемер будет иметь рабочий диапазон до 10м при разрешении уровней ±1мм, а при использовании приемо-передатчика АП-70Т – рабочий диапазон до 20м при разрешении уровней ±1см.

Ключевые слова: **у**ровнемер; разность уровней; импульсный сигнал; волноведущий тракт; контроль уровня; разделитель каналов; разрешение уровней; смежные резервуары.

Ил. 4. Библиогр.: 4 назв.

UDC 681.128.82

Monitoring the difference in liquid levels in adjacent tanks / *B.V. Zhukov, A.V. Odnovol* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №204. P. 115 – 119.

The possibility of synchronous monitoring of coolant levels in the cooling systems of nuclear and thermal power plants before and after the barrier mesh using a specialized level gauge is considered.

The block diagram of a level gauge providing current synchronous control of liquid levels in two adjacent channels (reservoirs), as well as the difference in liquid levels in them, is presented. A feature of the structural diagram of a specialized acoustic level gauge is the use of a radiation source common to both channels and a device for dividing the common waveguide path into two channels.

An algorithm for the functioning of a specialized level gauge has been developed, in which, based on time diagrams, it is shown how the level is controlled in each channel and the difference in liquid levels before and after the barrier grid is calculated. The description of the algorithm is accompanied by calculated expressions for determining the levels and the difference in liquid levels.

For a level gauge made in the acoustic wavelength range, a condition is given that is necessary for the creation of a device that provides matching when dividing a common channel into two independent channels of pulse signal propagation. This condition made it possible to establish the relationship between the inner diameters of cylindrical pipes used as waveguide paths of an acoustic wave.

Variants of the implementation of a specialized level gauge based on two modifications of the ZOND-3M level gauge are proposed, in which cylindrical pipes are used as waveguiding systems. It is shown that when using the AP-7VT transceiver, the level gauge will have an operating range of up to 10m with a level resolution of ± 1mm, and when using the AP-70T transceiver, it will have an operating range of up to 20m with a level resolution of ± 1cm.

Key words: level gauge; level difference; pulse signal; wave-guiding tract; level control; channel separator; level resolution; adjacent tanks.

4 fig. Ref: 4 items.

РАДІОТЕХНІЧНІ ПРИСТРОЇ ТА ЗАСОБИ ТЕЛЕКОМУНІКАЦІЙ
РАДИОТЕХНИЧЕСКИЕ УСТРОЙСТВА И СРЕДСТВА ТЕЛЕКОММУНИКАЦИЙ
RADIO ENGINEERING DEVICES AND TELECOMMUNICATIONS MEANS

УДК 621.375.4

Дослідження підсилювача класу E/F3 з паралельним контуром / *Д.Г. Макаров, Д.В. Чернов, В.В. Крижановський, Ю.В. Рассохіна, В.Г. Крижановський, А. Гребєнніков* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 204. С. 120 – 127.

Аналітично сформульована система рівнянь для процесів у вихідній ланці підсилювача, в якій враховано параметри коливальних контурів на частотах вищих гармонік. Для розрахунку була складена система з п’яти рівнянь для п’яти невідомих, до яких була додана умова на те, що друга похідна в точці екстремуму напруги стокового імпульсу буде більше нуля. Два рівняння відповідають умовам класу Е, два – квадратурні форми для напруги на навантаженні та на додатковому контурі і одне рівняння – умова екстремуму в точці поблизу середини імпульсу напруги. Дану систему розв’язувалось у програмі комп’ютерної алгебри. За знайденими параметрами розраховуються форми сигналів та елементів схеми. Обираючи різні параметри, можна отримати варіанти реалізації підсилювачів, які будуть за принципом роботи мати риси інших варіантів класу F. Отримані параметри кіл перевірялися у програмі гармонійного балансу та проводилось порівняння форм сигналів стокової напруги та струму через транзистор (ключ) з результатами розрахунку у програмі. Варіант, який був ближче до режиму класу E/F_3, було обрано для створення експериментального макету на частоту 2 МГц з використанням транзистору IRF530, макет перевіряли у діапазоні напруги живлення до 24 В. Отримано вихідну потужність більше 6 Вт при ККД більше 80 %. В експерименті було виміряно відношення максимальної напруги на стоці польового транзистору до напруги живлення, воно склало значення 3,3 при коефіцієнті заповнення 50 % на відміну від підсилювача класу Е, де теоретичне значення 3,65, а на практиці, з урахуванням нелінійності ємності стік-витік, може бути і 4. В експерименті значення другої гармоніки на виході на рівні -29 дБ відносно першої, а третьої -28,5 дБ, що обумовлено впливом додаткового фільтру на частоту другої гармоніки. Результати роботи корисні для впровадження таких схем у практику.

Ключові слова: підсилювач класу Е; підсилювач класу E/F_3; коефіцієнт корисної дії; аналіз у часовій області; метод гармонійного балансу.

Табл. 2. Іл. 9. Бібліогр.: 12 назв.

УДК 621.375.4

Исследование усилителя класса E/F3 с параллельным контуром / *Д.Г. Макаров, Д.В. Чернов, В.В. Крыжановский, Ю.В. Рассохина, В.Г. Крыжановский, А. Гребенников* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 204. С. 120 – 127.

Сформулирована аналитическая система уравнений, описывающая процессы в выходной цепи усилителя, учитывающая параметры колебательных контуров на высших гармониках сигнала. Для расчетов составлена система из пяти уравнений для пяти неизвестных, к которым было добавлено условие положительности второй производной в точке экстремума напряжения на стоке. Два уравнения отвечают условиям класса Е, два – квадратурным формам для напряжения на нагрузке и на дополнительном контуре и еще одно уравнение – условие экстремума в точке вблизи середины импульса напряжения. Эту систему решали в программе компьютерной алгебры. По найденным параметрам рассчитывались формы сигналов и элементы схемы. Выбирая разные значения, можно получить варианты реализации усилителя, которые будут иметь черты класса F. Полученные схемы проверялись в программе гармонического баланса и сравнивались формы сигналов на ключе. Для экспериментального исследования был выбран вариант, близкий к E/F_3, частота 2 МГц, транзистор IRF530 при напряжении питания 24 В. Получена выходная мощность более 6 Вт при КПД больше 80%. Экспериментально измерено отношение максимального напряжения на стоке к напряжению питания, оно равно 3,3 при коэффициенте заполнения 50 % в отличие от усилителя класса Е, где теоретическое значение 3,65, а на практике, с учетом нелинейности емкости сток-исток, может быть и 4. Значение второй гармоники в эксперименте -29 дБ относительно первой, а третьей -28,5 дБ, что обусловлено влиянием дополнительного фильтра на частоту второй гармоники. Результаты работы будут полезны для внедрения таких схем на практике.

Ключевые слова: усилители класса Е; усилители класса E/F_3; коэффициент полезного действия; анализ во временной области; метод гармонического баланса.

Табл. 2. Ил. 9. Библиогр.: 12 назв.

UDC 621.375.4

Investigation into Class E/F3 with Parallel Network / *D.G. Makarov, D.V. Chernov, V.V. Kryzhanovskyi, Yu.V. Rassokhina, V.G. Kryzhanovskyi, A. Grebennikov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №204. P. 120 – 127.

The system of equations for processes in the amplifier output network is analytically formulated. This system of equations considers parameters of resonant networks at higher harmonics. To calculate amplifier output network, the system of five equations was built for five unknowns, to which the condition of positive second voltage derivative at extremum of drain voltage was added. Two equations correspond to class E conditions, another two — quadrature waveforms at load and at additional resonant network. The last equation is the condition of extremum at the point near

middle of drain voltage pulse. This system was solved using computer algebra program. The circuit elements and waveforms were calculated using the derived parameters. By choosing different parameters, it is possible to obtain various amplifier realizations, which will demonstrate features of different class F variants. The obtained amplifier parameters drain voltage and current waveforms were verified with calculated ones using the harmonic balance simulating software. The variant, which is closer to class E/F_3 mode, was chosen to build an experimental amplifier prototype on frequency 2MHz using IRF530 MOSFET as a switch. The prototype was tested in the range of supply dc voltage up to 24V with the output power greater than 6W, while the amplifier efficiency was >80%. In the experiment, the ratio of peak drain voltage to dc supply voltage was measured to be 3.3 at the duty ratio 50%, unlike class E amplifier, where this value is around 3.65, and on practice, considering non-linear drain to source capacitance, it may achieve 4. The experimental second harmonic level amounted to be -20 dB relatively to fundamental, and the third one — 28.5 dB, which is due to an additional second harmonic filter. The paper results are useful for introduction of such circuits to practice.

Key words: class E amplifier; class E/F_3; efficiency; transient analysis; harmonic balance.

2 tab. 9 fig. Ref: 12 items.

ПІДГОТОВКА СПЕЦІАЛІСТІВ В ОБЛАСТІ РАДІОТЕХНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ

ПОДГОТОВКА СПЕЦИАЛИСТОВ В ОБЛАСТИ РАДИОТЕХНИКИ И ТЕЛЕКОММУНИКАЦИЙ

TRAINING OF SPECIALISTS IN THE FIELD OF RADIO AND TELECOMMUNICATIONS

УДК 004.94

Можливості застосування СМК Maple для дослідження законів розподілу випадкових величин / *І.О. Мощенко, О.М. Нікітенко, Ю.В. Козлов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 204. С. 128 – 134.

Описано використання СМК Maple для практичної та самостійної роботи студентів при вивченні законів розподілу випадкових величин.

Статистичні розрахунки без допомоги ЕОМ є складними й потребують використання багатьох таблиць функцій та квантилів стандартних розподілів. Це не сприяє тому, щоб відчути елемент новизни в матеріалі, який вивчається, мати можливість змінити задовільно умови задач тощо, потребує багато часу під час вирішення прикладних виробничих завдань, що є недоцільним.

Тому для визначення та дослідження законів розподілу випадкових величин як в практичній діяльності, так і під час навчання, використовують спеціальні математичні програмні пакети прикладних програм, найбільш поширеними серед яких є Mathcad, MatLab, Mathematica, Maple.

Таким чином метою цієї публікації є опис можливостей вивчення законів розподілу випадкових величин за допомогою СМК Maple та застосування отриманих навичок у самостійній роботі студентів.

Бібліотека Statistics має великий набір команд для аналізу даних з обчисленням різноманітних числових характеристик випадкових величин, графічного зображення їх законів розподілу, а також для статистичної обробки даних.

Таким чином, СМК Maple завдяки потужному набору статистичних інструментів, можливості символьних обчислень та обробки виразів та даних, широким можливостям графічної інтерпретації отриманих результатів не тільки в статичному, але і в динамічному виді (дво- та тривимірна анімація) доцільно використовувати під час вивчення теми «Закони розподілу випадкових величин» на практичних заняттях та у самостійній роботі студентів для подальшого використання ними набутих навичок при вирішенні прикладних завдань науки та техніки.

Ключові слова: статистика; закон розподілу; випадкова величина; система комп'ютерної математики; Maple.

Табл. 1. Іл. 2. Бібліогр.: 8 назв.

УДК 004.94

Возможности использования СМК Maple для исследования законов распределения случайных величин / *И.А. Мощенко, А.Н. Никитенко, Ю.В. Козлов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 204. С. 128 – 134.

Описано использование СМК Maple для практической и самостоятельной работы студентов при изучении законов распределения случайных величин.

Статистические расчеты без помощи ЭВМ являются сложными и требуют использования множества таблиц функций и квантилей стандартных распределений. Это не способствует тому, чтобы почувствовать элемент новизны в материале, который изучается, иметь возможность изменить произвольно условия задач и т.п., требует много времени при решении прикладных производственных задач, что является нецелесообразным.

Поэтому для определения и исследования законов распределения случайных величин, как в практической деятельности, так и во время обучения, используют специальные математические программные пакеты прикладных программ, наиболее распространенными из которых являются Mathcad, MatLab, Mathematica, Maple.

Таким образом, целью данной публикации является описание возможностей изучения законов распределения случайных величин с помощью СМК Maple и использование полученных навыков в самостоятельной работе студентов.

Библиотека Statistics имеет большой объем команд для анализа данных с вычислением числовых характеристик случайных величин и графического изображения их законов распределения.

СМК Maple благодаря мощному набору статистических инструментов, возможности символьных вычислений и обработки данных, широким возможностям графической интерпретации полученных результатов не только в статическом, но и в динамическом виде целесообразно использовать при изучении темы «Законы распределения случайных величин» на практических занятиях и в самостоятельной работе студентов для использования ими приобретенных навыков при решении прикладных задач науки и техники.

Ключевые слова: статистика; закон распределения; система компьютерной математики; Maple.

Табл. 1. Ил. 2. Библиогр.: 8 назв.

UDC 004.94

Possibility of using CMS Maple to study laws of distribution of random variables / *I. Moshchenko, O. Nikitenko, Yu.V. Kozlov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №204. P. 128 – 134.

The use of CMS Maple for students' practical and independent work is described. The study of random variable distribution laws is actual.

Statistical calculations without computer are difficult and require many functional and quintiles tables of standard distributions. This does not contribute to feeling the element of novelty in the material being studied, to be able to arbitrarily change the conditions of tasks, etc., it takes a lot of time in solving applied production problems, which is inappropriate

Thus to determine and research random variable distribution laws both in practical applications and in studying we must use special mathematical packages. The most extended of them are Mathcad, MatLab, Mathematica, Maple. Specialized statistical packages (SAS, SPSS, STATISTIKA, STATGRAPHICS) are not relevant to study. Their use for studying requires very high education level in mathematical statistics.

Most of the existing math packages allow users to operate at random variables, including the Computer Mathematics System (CMS) Maple.

Thus, the purpose of this article is a description of the studying possibilities of the random variables distribution laws with CMS Maple and the application of the acquired skills to the independent work of students.

The Maple Statistics Library has a large set of commands for analyzing data, computing various numerical characteristics of random variables, graphing their distribution laws, and for statistical data processing.

Thanks to a powerful set of statistical tools, the possibility of symbolic calculations and data processing of CMS Maple, wide possibilities of graphical interpretation of the results obtained not only in a static but also in a dynamic form, it is advisable to use it when studying the topic "Distribution Laws of Random Variables" in students' practical and independent work to use their acquired skills in solving applied problems of science and technology.

Key words: statistics; distribution law; random variable; computer mathematics system; Maple.

1 tab. 2 fig. Ref: 8 items.

ЗБІРНИК НАУКОВИХ ПРАЦЬ
РАДІОТЕХНІКА
Випуск 204
Українською, російською, та англійською мовами

СБОРНИК НАУЧНЫХ ТРУДОВ
РАДИОТЕХНИКА
Выпуск 204
На украинском, русском и английском языках

COLLECTION OF SCIENTIFIC PAPERS
RADIOTEKHNIKA
Issue 204
In Ukrainian, Russian and English

Коректор Л.І. Сащенко

Підп. до друку 09.04.2021. Формат 60x90/8. Папір офсет. Гарнітура Таймс. Друк. ризограф.
Ум. друк. арк**.** 9,9. Обл.-вид. арк. 8,2. Тираж 300 прим. Зам. № 434. 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.