МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ
УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

РАДІОТЕХНІКА

Всеукраїнський
міжвідомчий науково-технічний збірник

ТЕМАТИЧНИЙ ВИПУСК
«ІНФОРМАЦІЙНА БЕЗПЕКА»

Засновано в 1965 р.

В И П У С К 2 0 0

Харків
Харківський національний
університет радіоелектроніки
2020

УДК 621.3

Збірник включено до списку спеціальних видань ВАК України з фізико-математичних та технічних дисциплін.
Реєстраційне свідоцтво КВ № 12098-969 ПР від 14. 12. 2006.
За зміст статті відповідальні автори.

Відповідальний випусковий: *І.Д. Горбенко, д-р техн. наук, проф.*
технічний секретар *О.С. Полякова*.

Рекомендовано Вченою радою Харківського національного університету радіоелектроніки, протокол №3 від 30.04.2020.

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

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

ЗМІСТ

ПЕРСПЕКТИВНІ МЕТОДИ ТА СИСТЕМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

А.М. Олексійчук, В.А. Кулібаба, М.В. Єсіна, С.О. Кандій, Є.В. Острянська, І.Д. Горбенко Обґрунтування перспективного постквантового національного стандарту електронного підпису на основі решіток 5

О.Г. Качко, Ю.І. Горбенко, В.А. Пономар, М.В. Єсіна, С.О. Кандій Оптимізація алгоритму множення поліномів для NTRU-подібних алгоритмів 15

О.С. Шевчук Рандомізована симетрична криптосистема Мак-Еліса на основі узагальнених кодів Ріда – Соломона 25

А.В. Бессалов Алгоритми і оцінки складності обчислень 3- і 5-ізогеній суперсингулярних кривих Едвардса (*рос. мовою*) 37

М.Ю. Родінко, Р.В. Олійников Дослідження продуктивності малоресурсного блокового шифру «Кипарис» на різних платформах 51

О.О. Кузнецов, А.С. Кіян, А.І. Пушкарьов, Т.Ю. Кузнецова Тестування кодових генераторів псевдовипадкових чисел для постквантового застосування 58

К.Є. Лисицький, О.О. Кузнецов Обчислювальні алгоритми розрахунку алгебраїчного імунітету нелінійних вузлів заміни симетричних шифрів (*рос. мовою*) 68

МЕТОДИ ТА МЕХАНІЗМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМІ БЛОКЧЕЙН

І.Д. Горбенко, В.В. Онопрієнко, Ю.І. Горбенко, О.О. Кузнецов, К.В. Ісірова, М.Ю. Родінко Проблеми, принципи побудови та перспективи розвитку національної системи електронного голосування в Україні 85

І.Д. Горбенко, О.Г. Качко, Ю.І. Горбенко, М.В. Єсіна, С.О. Кандій, Є.В. Острянська, А.С. Д'яченко Можливості застосування механізмів повністю гомоморфного шифрування в системах електронного голосування 98

П.І. Стеценко, Г.З. Халімов, Є.В. Котух Аналіз площин атак на Blockchain системи (*англ. мовою*) 114

І.Д. Горбенко, О.О. Кузнецов, М.О. Полуяненко, А.С. Кіян, К.Є. Лисицький, С.О. Кандій Прототипування децентралізованої системи електронного блокчейн-голосування 122

М.О. Полуяненко, О.О. Кузнецов Аналітичне моделювання атаки подвійної витрати на блокчейн-системи із ймовірнісним протоколом консенсусу 140

Н.А. Полуяненко, О.О. Кузнецов Ймовірність успішної атаки подвійної витрати на блокчейн-системи із ймовірнісним протоколом консенсусу 153

МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ В КОМУНІКАЦІЙНИХ СИСТЕМАХ

І.Д. Горбенко, О.А. Замула Теоретичні основи синтезу квазіортогональних систем складних сигналів (*англ. мовою*) 162

І.Д. Горбенко, О.А. Замула, Хо Чі Лик Методи пошуку оптимальних за мінімаксним критерієм систем складних нелінійних дискретних сигналів 175

І.Є. Антіпов, Б.В. Бочаров, Д.Р. Найдьонова Оцінка безпеки користувачів інтернет-банкінгу 188

Р.С. Гриньов, О.В. Сєвєрінов, А.В. Власов Метод виявлення та протидії вірусам у зображеннях формату BMP 195

О.В. Циганкова Аналіз можливостей використання алгоритму Ель-Гамаля з детермінованим внесенням для інкапсуляції ключей (*англ. мовою*) 201

РЕФЕРАТИ 206

CONTENT

PERSPECTIVE METHODS AND SYSTEMS OF CRYPTOGRAPHIC INFORMATION PROTECTION

A.M. Oleksiychuk, V.A. Kulibaba, M.V. Yesina, S.O. Kandy, E.V. Ostryanska, I.D. Gorbenko Substantiation of promising post-quantum national lattice-based electronic signature standard 5

O.G. Kachko, Yu.I. Gorbenko, V.A. Ponomar, M.V. Yesina, S.O. Kandiy Optimization of polynomial multiplication algorithm for NTRU-like algorithms 15

O.S. Shevchuk Randomized symmetric McEliece cryptosystem based on generalized Reed-Solomon codes 25

A.V. Bessalov Algorithms and complexity evaluation of 3- and 5-isogeny calculation of super singular Edwards curves 37

M.Yu. Rodinko, R.V. Oliynykov The research of performance of the “Cypress” lightweight block cipher on different platforms 51

A.A. Kuznetsov, A.S. Kiian, A.I. Pushkar’ov, T.Yu. Kuznetsova Testing of code-based pseudorandom number generators for post-quantum application 58

K. Lisitsky, O. Kuznetsov Computational algorithms for calculating the algebraic immunity of nonlinear nodes of replacing symmetric ciphers 68

METHODS AND MECHANISMS OF CRYPTOGRAPHIC INFORMATION PROTECTION IN THE BLOCKCHAIN SYSTEM

I.D. Gorbenko, V.V. Onoprienko, Yu.I. Gorbenko, A.A. Kuznetsov, K.V. Isirova, M.Yu. Rodinko Problems, construction principles and development prospects of the national electronic voting system in Ukraine 85

I.D. Gorbenko, O.G. Kachko, Yu.I. Gorbenko, M.V. Yesina, S.O. Kandy, E.V. Ostryanska, A.S. Dyachenko Possibilities of using full homomorphic encryption mechanisms in electronic voting systems 98

P.I. Stetsenko, G.Z. Khalimov, E.V. Kotukh Analysis of planes of attacks on the Blockchain system 114

I.D. Gorbenko, A.A. Kuznetsov,N.A. Poluyanenko, A.S Kiyan, K.E. Lisitsky, S.A. Kandy Prototyping decentralized electronic blockchain voting system 122

N.A. Poluyanenko, A.A. Kuznetsov Analytical modeling of the attack of double costs on a blockchain system with a probabilistic consensus protocol 140

N.A. Poluyanenko, A.A. Kuznetsov Probability of a successful attack of double costs on a blockchain system with a probabilistic consensus protocol 153

METHODS AND MEANS OF PROTECTION IN COMMUNICATION SYSTEMS

I.D. Gorbenko, A.A. Zamula Theoretical bases of synthesis of quasi-orthogonal systems of complex signals 162

I.D. Gorbenko, A.A. Zamula, Ho Tri Luc Methods of searching for systems of complex nonlinear discrete signals optimal by the minimax criterion 175

I.E. Antipov, B.V. Bocharov, D.R. Naydenova Estimate of the Internet banking user security 188

R.S. Grynov, A.V. Sievierinov, A.V. Vlasov Method for detecting and counteracting Virus Detection in BMP images 195

O.V. Tsygankova Analysis of possibility to use El Gamal algorithm with deterministic embedding for key encapsulation 201

ABSTRACTS 206

ПЕРСПЕКТИВНІ МЕТОДИ ТА СИСТЕМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

УДК 004.056.55 **DOI:10.30837/rt.2020.1.200.01**

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

ОБҐРУНТУВАННЯ ПЕРСПЕКТИВНОГО ПОСТКВАНТОВОГО НАЦІОНАЛЬНОГО СТАНДАРТУ ЕЛЕКТРОННОГО ПІДПИСУ НА ОСНОВІ РЕШІТОК

Вступ

Важливою особливістю постквантового періоду у криптографії є суттєва невизначеність щодо вихідних даних для криптоаналізу та протидії в частині можливостей квантових комп'ютерів, їх математичного та програмного забезпечень, а також застосування квантового криптоаналізу до існуючих криптоперетворень та криптопротоколів. В якості основних методів обрано математичні методи електронного підпису (ЕП), що пройшли суттєвий аналіз та обґрунтування в процесі широких досліджень криптологами та математиками на найвищому рівні [3 – 18]. Вони детально описані та пройшли дослідження на першому етапі міжнародного конкурсу NIST США [23]. В процесі другого етапу прийнято ряд рішень стосовно об'єднання деяких кандидатів на постквантовий стандарт ЦП. Для подальших досліджень на 2-му етапі залишили 9 кандидатів [24]: CRYSTALS-DILITHIUM, FALCON, GeMSS, LUOV, MQDSS, Picnic, qTESLA, Rainbow та SPHINCS+. Три з них (Dilithium, FALCON, qTeSLA) засновані на стійкості алгебраїчних решіток (Lattice-based), чотири (GeMSS, LUOV, MQDSS, Rainbow) – на основі багатовимірних перетворень (multi-variate), один (SPHINCS+) – на стійкості геш-функції, один (Picnic) – на стійкості геш-функції та блокових потокових шифрів.

На наш погляд, національний стандарт Україні постквантового періоду повинен включати в себе мінімум три алгоритми, що базуються на різних видах математичних перетворень, що визнані світовим криптографічним співтовариством як такі, що можуть забезпечувати необхідний рівень стійкості в умовах квантового криптоаналізу.

Одним із видів криптографічних перетворень типу ЕП, що може бути включений в національний стандарт ЕП постквантового періоду, на наш погляд, може стати ЕП на основі застосування алгебраїчних решіток (Lattice-based) [24].

1. Огляд основних операцій в алгоритмі підпису Dilithium 2-го етапу конкурсу NIST

На рис.1 зображено узагальнену схему ЕП CRYSTALS-DILITHIUM, що подається у [2].

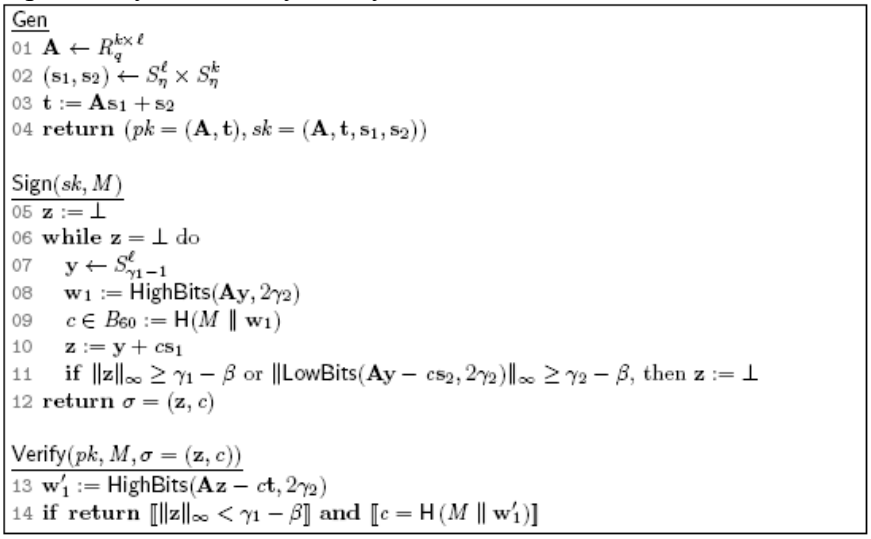


Рис. 1. Узагальнена схема ЕП CRYSTALS-DILITHIUM

Алгоритм належить до так званого класу "Fiat-Shamir з перериваннями"[3]. На рис. 1 подаються у спрощеному вигляді алгоритми генерації відкритого та секретного ключів, а також підпису і перевірки підпису.

Генерація основних складових ключа. Спочатку (рядок 01, рис.1) генерується матриця поліномів **A** розміру $k \times \ell$, кожен з елементів якої є поліномом у кільці $R_q = \mathbb{Z}_q[X]/(X^n+1)$. В процесі попереднього розгляду будемо вважати, що модуль $q=2^{23}-2^{13}+1$, а степінь полінома $n=256$. Потім генеруються (обчислюються) випадкові вектори, тобто множини поліномів секретного ключа $\mathbf{s}_1$ і $\mathbf{s}_2$ (рядок 02) відповідно з числом поліномів k та l. Коефіцієнти цих векторів (поліномів) є елементами поля R_η, тобто з (малими) коефіцієнтами з розміром не більше η (від $-\eta$ до η). Далі з використанням матриці **A** та секретного ключа $\mathbf{s}_1$ і $\mathbf{s}_2$ обчислюється друга частина відкритого ключа $t=As_1+s_2$ (рядок 03), а перша частина відкритого ключа задається значенням ρ. Всі алгебраїчні операції з поліномами в механізмі виконуються над кільцем полінома $R_q = \mathbb{Z}_q[X]/(X^n+1)$. Четвертий рядок показує вихідні значення відкритого P_k та секретного S_k ключів.

Алгоритм підпису у загальному виді. Спочатку в алгоритм перевірки ЕП вводяться значення секретного ключа S_k та повідомлення M, що підписується. Далі обчислюється вектор поліномів маскування **y** з коефіцієнтами, що є меншими, ніж γ_1 (рядок 07), а також обчислюється значення вектора поліномів **Ay.** На основі отриманого значення **Ay** обчислюються старші біти $\mathbf{w}_1$ ("біти високого порядку") коефіцієнтів у цьому векторі поліномів (рядок 08). $\mathbf{w}_1$ є вектором, що містить всі поліноми w1. Потім обчислюється поліном (рядок 09) c, що є поліномом у полі R_q з точно 60 символами ±1, а решта 0. Безпосередньо ЕП обчислюється у вигляді вектора поліномів $\mathbf{z}=\mathbf{y}+c\mathbf{s}_1$.

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

Алгоритм перевірки підпису у загальному виді. Спочатку перевірник обчислює $\mathbf{w}'_1$ як біти високого порядку вектора $\mathbf{Az}-c\mathbf{t}$. Далі ЕП приймається, якщо всі коефіцієнти **z** менше, ніж $\gamma_1 - \beta$ і, якщо c є геш-значенням повідомлення M, що перевіряється, та значення $\mathbf{w}'_1$ (рядок 13). Перевірка виконується за умови, якщо

$$\text{HighBits}(\mathbf{Az}-c\mathbf{t}, 2\gamma_2) = \text{HighBits}(\mathbf{Ay}, 2\gamma_2) \quad (1)$$

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

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

А так як коефіцієнти $c\mathbf{s}_2$ менше ніж β, то додавання $c\mathbf{s}_2$ недостатньо для того, щоб викликати перенесення у старші коефіцієнті, збільшивши будь-який коефіцієнт низького порядку до величини щонайменше γ_2. Таким чином, рівняння (1) є коректним, і підпис перевіряється успішно.

2. Аналіз стійкості алгоритму Dilithium проти основних атак

Наразі в постквантовій криптології актуальними є завдання забезпечення криптографічної стійкості щодо квантових атак. Вона пов'язана з проблемою навчання з помилками.

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

$$(a, c) = (a, \langle a, s \rangle + e) \in \mathbf{Z}_q^n \times \mathbf{Z}_q, \tag{3}$$

де $a \in \mathbf{Z}_q^n$ отримується з рівномірного розподілу та $e \in \mathbf{Z}$ з розподілу χ. В даному випадку атака Decision-LWE полягає у тому, щоб визначити, чи отримана пара $(a, c) \in \mathbf{Z}_q^n \times \mathbf{Z}_q$ з розподілу $L_{s,\chi}$, або рівномірного розподілу. Її Search-LWE складова полягає у знаходженні s з пари $(a, c) \in \mathbf{Z}_q^n \times \mathbf{Z}_q$ [3]. Вважається, що як проблема Decision-LWE, так і Search-LWE [2 – 7] з точки зору складності є еквівалентними та можуть бути зведені одна до одної за поліноміальний час і фактично є різними поглядами на одну і ту ж задачу. Розподіл χ для цих задач зазвичай є дискретним нормальним розподілом над кінцевим полем з математичним очікуванням рівним 0 та дисперсією, що характеризується параметром α. При цьому більшість атак на LWE полягають у знаходженні деякого вектору v з певною нормою на решітці L з фіксованим об'ємом $vol(L)$, але з різною розмірністю m, яка фактично характеризує оптимальну кількість пар $(a_i, c_i) \in \mathbf{Z}_q^n \times \mathbf{Z}_q$ необхідних для атаки.

Аналіз показав, що складність проблеми LWE точно знайдена лише асимптотично. Так, доведено [4, 6], що за певних умов складність вирішення LWE в просторі розмірності n становить щонайменше $2^{O(n)}$. Цей результат зручно використовувати для оцінки загальносистемних параметрів, проте конкретні оцінки складності крипостійкості досі не відомі. Таке пов'язано з тим, що атаки на LWE зводяться в кінцевому випадку до редукції решіток.

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

Аналіз показує, що поліном $f(x) = x^{2^n} + 1$ обраний не випадково. Його властивості дозволяють здійснити доказ щодо стану захищеності асиметричного криптоперетворення щодо квантових атак. Також його властивості дозволяють використати для операцій множення поліномів швидке NTT перетворення, і як наслідок створювати швидкодіючі реалізації криптоперетворень. Однак, з теорії Галуа відомо [3, 4, 6], що поле $R_q = \mathbf{Z}_q[X]/(x^{2^n} + 1)$ має складну структуру підполів, що може бути використано для здійснення криптоаналізу. Проте, на нинішній час, на практиці такі атаки носять більше обмежений теоретичний характер, ніж практичний. Фактично сучасними криптологами ігноруються додаткові можливості, а R-LWE та M-LWE розглядаються як LWE. Це пояснюється тим, що для полінома $f(x) = x^{2^n} + 1$ доведено, що R-LWE та M-LWE є складнішими за LW атаки.

На основі аналізу визначено [7 – 15], що стосовно LWE можливо застосування таких атак:

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

Деталі щодо кожного з видів, а також їх теоретичне обґрунтування наведено у [26].

3. Захищеність алгоритму ЕП від атак сторонніми каналами

В процесі проведення конкурсу на постквантовий стандарт ЕП особлива вимога висунута до захищеності кандидату на ЕП від атак сторонніми каналами. Тому така проблемна задача є актуальною, в першу чергу стосовно ЕП Crystals-Dilithium.

Дослідження стосовно алгоритм ЕП Crystals-Dilithium проведено за такими параметрами [2]:

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

Для проведення експерименту було згенеровано 10000 ключів та виконано 10000 підписів. Результат залежності часу підпису від номеру ключа наведено на рис. 2. Для 10000 ключів максимальне відхилення від нормалізованого середнього (дисперсія) усіх вимірів часу підпису повинно знаходитися в інтервалі $-5.19676 <= d <= 6.62797(\%)$, щоб вважати, що час підпису не залежить від ключа. Номери ключів, для яких було отримано мінімальне та максимальне значення при повтореннях вимірів не повинні співпадати.

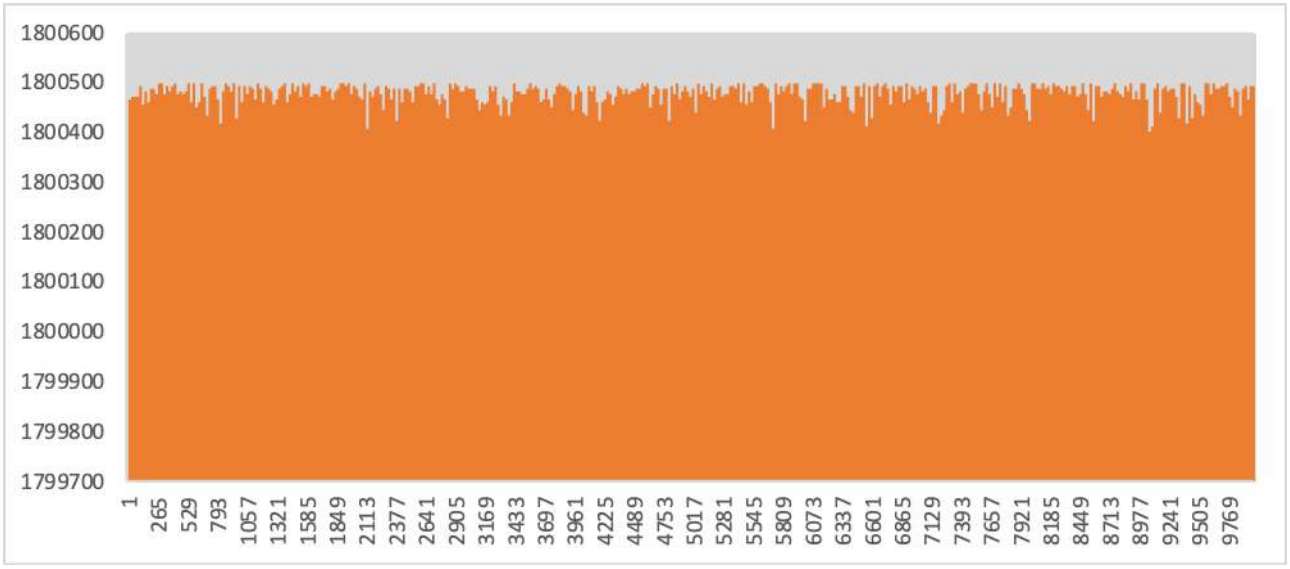


Рис. 2. Залежність часу підпису (у тактах процесору) від номеру ключа

Значення дисперсії $d \approx 2\%$, що свідчить про практично статистичну незалежність часу підпису від ключа, що є важливим з точки зору захищеності від атак сторонніми каналами.

4. Вибір параметрів 5-7 рівнів стійкості

Попередній аналіз показав, що значення параметрів, наведені в [20], табл. 3.1, не забезпечують при застосуванні в механізмі Dilithium стійкість ЕП від класичних атак на рівні 256 бітів. Фактично нижні оцінки стійкості наведено в рядках табл. 3.1 [20] з назвами Best Known Classical bit-cost і Best Known Quantum bit-cost окремо для кожної з двох задач – класичної та

квантової, на складності яких базується стійкість. Це задачі SIS та LWE. Для кожної з них зазначені параметри обчислюються за формулами

$$\text{Best Known Classical bit-cost (класична атака)} = 0,292b \tag{4}$$

$$\text{Best Known Quantum bit-cost (квантова атака)} = 0,265b, \tag{5}$$

де b є довжиною блоку (BKZ bock-size b to break SIS або LWE [2]). В ролі кінцевої оцінки стійкості використовується найменше з двох значень, обчислених для b, що є довжиною блоку для задачі SIS та задачі LWE відповідно.

Наприклад, для останнього стовпця табл. 3.1 в [2] (третя категорія стійкості за вимогами NIST) маємо: BKZ bock-size b to break SIS $= 605$. Отже, значення (4) та (5) дорівнюють відповідно $0,292b = 176$, $0,265b = 160$; BKZ bock-size b to break LWE $= 595$, і значення (4) і (5) дорівнюють відповідно $0,292b = 174$ та $0,265b = 158$ (в табл. 3.1 наведені значення з округленням до цілих, причому не завжди у той самий бік). Таким чином, кінцева нижня оцінка стійкості ЦП для випадку, що розглядається, є 174, тобто схема забезпечує стійкість проти класичної атаки на рівні не менше, ніж 2^{174} та відповідно квантової атаки на рівні не менше, ніж 2^{158}.

Довжина блоку b обчислюється за параметрами k, l, η з табл. 3.1 за допомогою окремих алгоритмів для кожної задачі SIS та LWE. Яких саме, потребує додаткового вивчення, але автори [2] використовують для цього методику, наведену в [2, 3]. Вони зазначають [2, с. 22], що ця методика дозволяє отримувати "консервативні" нижні оцінки стійкості, які "скоріш за все, не зміняться найближчим часом" з появою більш ефективних алгоритмів розв'язання задач SIS та LWE, зокрема, на квантових комп'ютерах. Автори [2] пишуть також про те, що отримані ними оцінки формально є менше в порівнянні з вимогами NIST, але вони вважають, що для параметрів з табл. 3.1 схема Dilithium задовольняє цим вимогам [20].

Таким чином, найвищий рівень класичної стійкості, що забезпечує Dilithium з параметрами, зазначеними в [2, табл. 3.1], є (принаймні) 2^{174}.

Загальні обмеження [2 – 4, 8], які необхідно врахувати при виборі параметрів для забезпечення стійкості на рівні $\lambda \in \{256, 384, 512\}$ бітів.

1. Геш-функція CRH, що використовується у схемі (наприклад, в рядках 07, 10 на рис. 4 [2]), повинна бути стійкою до колізій. Отже, довжина її вектору значень повинна бути, як мінімум, 2λ бітів. (Зокрема, при $\lambda = 256$ функція CRH повинна приймати значення довжини 512, а ні 384, як в оригінальній схемі на рис. 4 [2]).

2. Криптографічна функція H, яка використовується в рядку 16 на рис. 4, повинна бути стійкою відносно знаходження другого прообразу [3] і, отже, приймати, принаймні, 2^{λ} різних значень, що є поліномами з кільця R_q, які мають коефіцієнти $0, 1, -1$ та містять точно h ненульових коефіцієнтів (зауважимо, що кількість таких поліномів дорівнює $2^h \binom{n}{h}$).

При $\lambda = 256$ в [2] рекомендується використовувати параметри $n = 256$, $h = 60$, і умова

$$2^h \binom{n}{h} \geq 2^{\lambda} \tag{6}$$

виконується.

При $\lambda \in \{384, 512\}$ та $n = 256$ забезпечити виконання умови (6) неможливо, якщо $h \leq n/2 = 128$. Отже, треба збільшити n до 512; при цьому числа q, γ_1, γ_2 можна залишити такими самими як в [2]:

$$q = 2^{23} - 2^{13} + 1,$$

$$\gamma_1 = (q-1)/16,\ \gamma_2 = \gamma_1/2. \quad (7)$$

3. Довжини векторів ρ та K, що використовуються відповідно в рядках 01 та 02 на рис. 4 в [2], повинні бути не менше ніж λ.

Таким чином, для забезпечення стійкості схеми цифрового підпису на рівні $\lambda \in \{256, 384, 512\}$ необхідно [25]:

1) використовувати геш-функцію CRH, значеннями якої є двійкові вектори довжини 2λ;

2) використовувати двійкові вектори ρ та K, що мають довжину λ;

3) покласти $n = 256$, якщо $\lambda = 256$; $n = 512$, якщо $\lambda \in \{384, 512\}$;

4) вибрати просте число $q \equiv 1 \bmod 2n$ та обчислити γ_1, γ_2 за формулою (7);

5) обчислити вагу c як найменше натуральне h, що задовольняє умові (3).

Зауважимо, що при $n = 512$, $q = 2^{23} - 2^{13} + 1$ час формування підпису може виявитися занадто великим; в цьому випадку треба збільшити q (приблизно в два рази).

В [1 – 3] немає чіткого викладення зазначених алгоритмів, є тільки певні вказівки. Тому на сьогодні вдалося "відновити" лише один з них, проте його застосування до параметрів з табл. 1 в [2] призводить до значень b, які є приблизно на 10 % більше наведених в цій таблиці.

5. Алгоритм оцінювання довжини блоку b для задачі LWE, пряма атака

Вхідні дані: натуральні числа k, l, η, n, q.

Алгоритм обчислень: для кожного $m = 0, 1, ..., nk$ виконати такі дії:

1) покласти $d = nl + m + 1$;

2) знайти найбільше натуральне $\tilde{b} = \tilde{b}(m) \le d$ таке, що

$$\eta\sqrt{\tilde{b}} \le \delta^{2\tilde{b}-d-1} q^{\frac{m}{d}}, \quad (8)$$

де

$$\delta = \left(\left(\pi\tilde{b}\right)^{\frac{1}{\tilde{b}}} \frac{\tilde{b}}{2\pi e} \right)^{\frac{1}{2(\tilde{b}-1)}}.$$

Результатом алгоритму є число

$$b = \min_{0 \le m \le nk} \{\tilde{b}(m)\}. \quad (9)$$

В табл. 1 наведені значення довжини блоку, отримані за допомогою наведеного вище алгоритму 1, та відповідні значення цього параметра з табл.1 в [2].

Таблиця 1

Значення щодо довжини блоку

(k, l)	(3, 2)	(4, 3)	(5, 4)	(6, 5)
η	7	6	5	3
BKZ bock-size b to break LWE [1]	200	340	485	595
Формула (9)	220	373	525	639

Як видно з табл. 1, формула (9) приводить до більших значень в порівнянні з [1]. Поряд з тим, значення довжини блоку, отримані за цій формулою, базуються тільки на розгляді однієї з двох атак на задачу LWE. Отже, з [2, п. 5.4], збільшення k та l на 1 приводить до збільшення стійкості приблизно на 30 бітів. Отже, виходячи з [1, табл. 1], де для $(k, l) = (6, 5)$,

$\eta = 3$ зазначено оцінку стійкості 2^{174}, можна припустити, що для стійкості 2^{256} достатньо покласти $(k, l) = (9, 8)$, $\eta = 3$.

6. Особливості гешування в алгоритмі ЦП Dilithium

Нехай B_h позначає сукупність елементів R, які мають коефіцієнти h, які є або −1, або 1, а інші є 0. Маємо $|B_h| = 2^h \cdot \binom{n}{h}$. Для нашого механізму ЕП необхідна криптографічна геш-функція, яка використовується для гешування полінома *c*. Алгоритм, який будемо використовувати для створення випадкового елементу у B_{60}, іноді називають «виворотною» версією Fisher-Yates перемішування [1] і його опис високого рівня наведено на рис. 3 (як правило, алгоритм повинен починатися з *i*=0, але оскільки існує 196 0, перші 195 ітерацій будуть просто встановлювати компоненти **c** у 0).

SampleInBall
01 Initialize $\mathbf{c} = c_0 c_1 \dots c_{255} = 00 \dots 0$
02 **for** $i := 196$ to 255
03 $j \leftarrow \{0, 1, \dots, i\}$
04 $s \leftarrow \{0, 1\}$
05 $c_i := c_j$
06 $c_j := (-1)^s$
07 **return c**

Рис. 3. Створення випадкового 256-елементного масиву з 60 ±1 та 196 0

Визначаємо роботу функції $\mathrm{H} : \mu \| \mathbf{w}_1 \mapsto c \in B_{60}$, описану на рис. 3, так як вона використовується в механізмі ЕП. Спочатку H гешує 48 байт μ, а потім відразу ж йдуть 128*k* байт для упаковки бітів представлення $\mathbf{w}_1$ в SHAKE-256. Протягом цих операцій функція стискає SHAKE-256, щоб отримати потік випадкових байтів змінної довжини. Перші 60 бітів у перших 8 байтах цього випадкового потоку інтерпретуються як 60 випадкових знакових бітів $s_i \in \{0, 1\}$, *i*=0,...,59. Інші 4 біта відкидаються. Далі H використовується для обчислення *c*. У кожній ітерації циклу для циклу використовується відхилення вибірки на елементи з {0,...,255}, доки він не отримується $j \in \{0, \dots, i\}$. Елемент у {0,...,255} отримується шляхом інтерпретації наступного байта випадкового потоку з SHAKE-256 як число в цьому наборі. Для підпису *s* використовується відповідний s_{i-196}.

Проведені дослідження показали, що сучасні та перспективні функції гешування для їх застосування в алгоритмах ЕП мають неодмінно відповідати таким вимогам стійкості:

- складність знаходження колізії $C_{col} \geq 2^{hlen/2}$;
- складність відновлення прообразу *M* $C_{preim} \geq 2^{hlen}$;
- складність знаходження іншого прообразу $C_{\mathrm{sec}\_preim} \geq 2^{hlen}$;
- складність знаходження колізії, усіченої на *ht* символів $C_{tr\_col} \geq 2^{(hlen-ht)/2}$.

Наведені вимоги дозволяють ввести безумовні критерії оцінки функцій гешування для криптографічних додатків.

7. Обґрунтування можливості застосування національного стандарту України в якості геш-функції для алгоритму Dilithium

Дві основні операції, що складають практично всю процедуру підпису та перевірки в алгоритмі Dilithium, – це розширення XOF (використовується SHAKE-128 і SHAKE-256) та множення у кільці полінома $R_q = Z_q[X]/(X^n + 1)$. Тому реалізації алгоритму на національному рівні повинні оптимізувати ці операції та працювати за постійний час.

Згідно [18] стандарт ДСТУ 7564:2014 визначає національний стандарт на функцію гешування. Функція гешування ДСТУ 7564:2014 забезпечує обчислення геш-значення з довжинами від 8 до 512 біт з кроком у 8 біт. Режим роботи для формування геш-значення довжиною n біт позначається як «Купина-n». Основними режимами роботи функції гешування, що рекомендуються до застосування, є «Купина-256», «Купина-384» і «Купина-512». Вона забезпечує обчислення геш-значення для повідомлення, що складається з бітової послідовності довжини від 0 біт (порожній рядок) до $2^{96}-1$ біт. При формуванні геш-значення повідомлення доповнюється, далі поділяється на l-бітні блоки $m_0,\ldots,m_t$, після чого виконується обробка кожного блоку шляхом ітеративного виконання функції стиснення ϕ. При обчисленнях формуються значення $h_i=\phi\left(h_{i-1},m_i\right)$, де $i=1,\ldots,t$, а також початкове значення $h_0=IV$. Після обробки останнього блоку повідомлення обчислюється результуюче геш-значення, тобто

$$H\left(M\right)=\Omega(h_t), \tag{10}$$

де Ω – завершальне перетворення, що повертає n – бітне значення, кратне 8 ($n\le\frac{l}{2}$).

Так як геш-функція, що описана в стандарті ДСТУ 7564:2014, забезпечує необхідні для алгоритму довжини геш-значення та є колізійно-стійкою[24], а також *відповідає усім безумовним критеріям* [26], нами пропонується її використання в якості основної функції гешування у новому постквантовому національному стандарті ЕП України.

Висновки

1. За результатами першого етапу конкурсу авторами проекту Crystals-Dilithium було запропоновано пропозиції щодо його удосконалення у плані побудови системних параметрів, що забезпечать більш високі рівні стійкості [3].

2. Актуальною є проблема обґрунтування необхідності та розробки удосконаленої версії ЕП Dilithium, що може забезпечувати в постквантовий період 5, 6 та 7 рівні захищеності від найбільш загрозливих атак [15, 16].

3. Різниця між версіями на першому і другому етапах конкурсу NIST полягає у тому, що початкова ентропія удосконаленого ЕП, тобто у рандомізованій версії, може встановлюватись випадковим чином, тоді як у 1-й, детермінованій версії, вона визначалась тільки у вигляді геш-значення ключа та безпосередньо повідомлення *M*, що підписується.

4. В механізмі Dilithium при генеруванні ключів та загальних параметрів використовуються засоби з рівноймовірним розподілом. Також такі операції як множення поліномів та їх округлення легко реалізуються з однаковою часовою складністю. Вказане забезпечує захист від атак сторонніми каналами на основі різної складності множення поліномів тощо.

5. Використання секретних послідовностей на основі дискретного нормального гаусового розподілу є надзвичайно нетривіальним і може легко призвести до незахищених реалізацій [22]. Це пояснюється тим, що хоча дуже «обережна» реалізація може запобігти подібним атакам, але неможливо припускати, що загальнодоступний механізм типу Crystals-Dilithium, що містить багато тонкощів, завжди буде досконало реалізований.

6. В механізмі Crystals-Dilithium зроблена спроба мінімізувати суму довжин відкритого ключа та ЕП. Внаслідок цього механізм Dilithium має, у порівнянні з іншими механізмами на алгебраїчних решітках, найменше поєднання розміру підпису та розмірів відкритих ключів, з однаковими рівнями безпеки.

7. В механізмі Crystals-Dilithium є можливість оперативної зміни рівня безпеки. Модульність реалізації та можливість оперативної зміни рівня безпеки пов’язані з тим, що по суті в механізмі Crystals-Dilithium виконуються всього дві операції. При генеруванні ключів та па-

раметрів виконується операція розгортання ключів та параметрів, а також множення у кільці полінома $\mathbb{Z}_q[X]/(X^n+1)$.

8. Безпеку механізму ЕП, що наведено на рис. 1, можна довести в моделі випадкового оракула (ROM), ґрунтуючись на складності двох проблем. Перша – це стандартна задача LWE над кільцями багаточленів, в якій пропонується відрізняти (A, $t:=As_1+s_2$) від (A, u), де u – рівномірно випадкове.

9. Механізм Crystals-Dilithium може бути взятий за основу, одним із кандидатів для розробки національного стандарту ЕП з використанням стандартизованих в Україні криптографічних алгоритмів, таких як функція гешування, наведена у ДСТУ 7564:2014 [27].

Список літератури:

1. Donald Knuth The Art of Computer Programming, volume 2. Addison-Wesley, 3 edition, 1997. P. 145.

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

3. Bos J.W., Costello C., Ducas L. [et all] Frodo: take of the ring! Practical, quantum-secure key exchange from LWE // Proc. of ACM CCS 16, ACM Press, Okt. 2006. P. 1006-1018.

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

5. Rueckert M., Schneider M. Estimating the security of lattice-based cryptosystems // Cryptology ePrint Archive, Report 2010/137, http://eprint.iacr.org/2010/0137.

6. Albrecht M.R., Player R., Scott S. On the concrete hardness of learning with errors // Cryptology ePrint Archive, Report 2015/046, http://eprint.iacr.org/2015/046.

7. Rachel Player. Parameter selectionin lattice-based cryptography.

8. Gottfried Herold, Elena Kirshanova, and Alexander May. On the asymptoticcomplexity of solving LWE.Designs, Codes and Cryptography, Jan 2017.

9. Shi Bai and Steven D. Galbraith. Lattice decoding attacks on binary LWE.In Willy Susilo and Yi Mu, editors, ACISP 14, vol. 8544 of LNCS, p. 322–337. Springer, Heidelberg, July 2016.

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

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

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

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

14. Richard Lindner and Chris Peikert. Better key sizes (and attacks) for LWE-based encryption. In Aggelos Kiayias, editor,CT-RSA 2011, vol. 6558 ofLNCS, p. 319–339. Springer, Heidelberg, February 2011.

15. Avrim Blum, Adam Kalai and Hal Wasserman. Noise-tolerant learning, the parity problem, and the statistical query model // Journal of the ACM,50(4):506–519, July 2003.

16. НДР «Визначення напрямків розвитку математичних методів та дослідження перспектив їх застосування для створення сучасних та перспективних криптографічних алгоритмів та протоколів» (Шифр «Скіл»). Т. 9. «Проект стандарту електронного підпису на алгребраїчній решітці для постквантового періоду». Харків, 2018. 127 с.

17. Daniel J. Bernstein, Daira Hopwood, Andreas Hülsing, Tanja Lange, Ruben Niederhagen, Louiza Papachristodoulou, Michael Schneider, Peter Schwabe and Zooko Wilcox-O'Hearn. SPHINCS: Practical stateless hash-based signatures. In Elisabeth Oswald and Marc Fischlin, editors, EUROCRYPT 2015, Part I, vol. 9056 of LNCS, p. 368–397, Sofia, Bulgaria, April 26–30, 2015. Springer, Heidelberg, Germany.

18. ДСТУ 8961:2019 Інформаційні технології. Криптографічний захист інформації. Алгоритми асиметричного шифрування та інкапсуляції ключів.

19. Ducas L., Lepoint T., Lyubachevsky V. [et all] CRYSTALS – Dilithium: digital sygnatures from module lattices / https://cryptojedi.org/papers/dilithium-20170617.pdf.

20. Alkim E., Ducas L., Poeppelmann T., Schwabe P. Post-quantum key exchange – a new hope / http://cryptojedi.org/papers/#newhope, 2016.

21. Bos J.W., Costello C., Ducas L. [et all]. Frodo: take of the ring! Practical, quantum-secure key exchange from LWE // Proc. of ACM CCS 16, ACM Press, Okt. 2006, P. 1006-1018.

22. Albrecht M.R., Player R., Scott S. On the concrete hardness of learning with errors // Cryptology ePrint Archive, Report 2015/046, http://eprint.iacr.org/2015/046.

23. Post-Quantum Cryptography [Electronic resource]. Access mode: https://csrc.nist.gov/projects/post-quantum-cryptography.

24. Горбенко Ю. І. Аналіз шляхів розвитку криптографії після появи квантових комп'ютерів / Ю. І. Горбенко. Р. С. Ганзя // Комп'ютерні системи та мережі : Вісник нац. ун-ту «Львівська політехніка». 2014. № 806. С. 40–49.

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

26. Горбенко І. Д. Постквантова криптографія та механізми її реалізації / І. Д. Горбенко, О. О. Кузнєцов, О. В. Потій, Ю. І. Горбенко, Р. С. Ганзя, В. А. Пономар // Радіотехніка. 2016. Вип. 186. С. 32-52.

27. ДСТУ 7564:2014 Інформаційні технології. Криптографічний захист інформації. Функція гешування.

Харківський національний
університет імені В. Н. Каразіна;
АТ «Інститут інформаційних технологій»

Надійшла до редколегії 07.01.2020

УДК 004.056.55 **DOI:10.30837/rt.2020.1.200.02**

О.Г. КАЧКО, канд. техн. наук, Ю.І. ГОРБЕНКО, канд. техн. наук, В.А. ПОНОМАР, канд. техн. наук, М.В. ЄСІНА, канд. техн. наук, С.О. КАНДІЙ

ОПТИМІЗАЦІЯ АЛГОРИТМУ МНОЖЕННЯ ПОЛІНОМІВ ДЛЯ NTRU-ПОДІБНИХ АЛГОРИТМІВ

Вступ

Наразі актуальною стала проблема криптографічного захисту від класичних та потенційних криптоаналітичних атак з використанням квантового комп'ютера та квантової математики. Розуміючи цю проблему, технологічно розвинені держави направляють суттєві зусилля на аналіз криптографічної стійкості існуючих стандартів криптографічного захисту інформації у постквантовий період та ведуть пошук щодо створення постквантових стандартів асиметричної криптографії. Практичне вирішення цієї проблеми здійснюється на світовому рівні в процесі проведення NIST США міжнародного конкурсу [1]. Причому особливу увагу звернуто на створення Асиметричного шифру (АСШ) та протоколу інкапсуляції ключів (ПІК). Завершено перший раунд (етап) та йде другий етап. У ході другого етапу проведено проміжний семінар, за рішенням якого NIST США рекомендував до подальших досліджень 17 криптопримітивів сумісної реалізації АСШ та ПІК [1 – 3].

Як показали попередні дослідження, надійною математичною основою, на якій можуть бути створені постквантові АСШ та ПІК, нині вважаються алгебраїчні решітки. Спираючись на вказане та виконані національні дослідження, в Україні вже у 2019 р. прийнято національний стандарт ДСТУ 8961:2019 «Алгоритми асиметричного шифрування та інкапсуляція ключів». В основу його побудови якраз і покладено алгебраїчні решітки. Асиметричне шифрування та інкапсуляцію ключів в стандарті виконують на основі математичних перетворень в кільці поліномів над скінченим полем. Також у стандарті враховані вимоги щодо забезпечення криптографічної стійкості проти спеціальних атак на основі витоку по технічних каналах, а також потенційних класичних та квантових атак. Стандарт розроблено з урахуванням досвіду створення та застосування ДСТУ ISO/IEC 18033-2:2015 тощо [3].

Стандарт, залежно від рівня криптографічної стійкості проти класичних та квантових атак, яку необхідно забезпечити, можна застосовувати в трьох режимах роботи АСШ та ПІК:

- режим СКЕЛЯ–КЕМ 256/128 – 256 біт захисту від класичних атак та 128 біт захисту від квантових атак, а також захисту від спеціальних атак;
- режим СКЕЛЯ–КЕМ 384/192 – 384 біт захисту від класичних атак та 192 біт захисту від квантових атак, а також захисту від спеціальних атак;
- режим СКЕЛЯ–КЕМ 512/256 – 512 біт захисту від класичних атак та 256 біт захисту від квантових атак, а також захисту від спеціальних атак.

Також в кожному із режимів роботи можна застосовувати окремо такі криптографічні перетворення:

- незалежний алгоритм (функція) асиметричного шифрування;
- протокол інкапсуляції ключів (функція), що ґрунтується на застосуванні функції асиметричного шифру;
- механізм (функція) симетричного шифрування та автентифікації, що ґрунтується на функціях асиметричного шифрування та інкапсуляції ключів.

У кожному із режимів роботи внаслідок застосування криптографічних перетворень в кільцях поліномів та скінчених полях забезпечують надання послуг конфіденційності, цілісності, справжності, доступності та криптографічної живучості ключа сеансу зв'язку та його узгодження між відправником та отримувачем.

Попередній аналіз показав, що для забезпечення 5 – 7 рівнів криптографічної стійкості необхідно суттєво збільшувати розміри (довжини) параметрів та ключів вказаних алгоритмів криптографічних перетворень АСШ та ПІК на решітках. Але при збільшенні розмірів пара-

метрів та ключів виникла проблема зменшення часової складності алгоритмів генерування параметрів та ключів, а також прямих та зворотних криптографічних перетворень АСШ та ПІК.

Метою статі є оптимізація алгоритму множення поліномів за критерієм часової складності, який використовується для генерування ключів та виконання прямих та зворотних криптографічних перетворень АСШ та ПІК на алгебраїчних решітках.

1. Постановка та аналіз задач досліджень

В NTRU-подібних алгоритмах асиметричних криптоперетворень [4, 5, 7] основними складовими є алгоритми генерування ключів та виконання прямих та зворотних криптографічних перетворень. Так, наприклад, в NTRU-подібних алгоритмах відкритий ключ h, це поліном розміром n (n – просте число), який обчислюється за особистим (F, G) згідно (1), або подібної формули [4]

$$h = G * F^{-1}, \tag{1}$$

де G, F – поліноми розміром n з коефіцієнтами за малим модулем p (зазвичай, p=3). Обчислення виконуються за великим модулем q, який залежить від алгоритму і може бути ступенем 2 або простим числом. В якості прикладів можна назвати модулі з довжиною q=2048, 4591 біт тощо.

Розглянемо, які алгоритми потрібно оптимізувати. Для визначення найбільш обчислювально складної операції реалізації NTRU-подібних алгоритмів розглянемо алгоритми генерації ключів, зашифрування та розшифрування для [4].

Генерація ключів:

Дано: F (1, -1, 0), G (1, -1, 0). Кількість ненульових елементів в поліномах фіксована і залежить від алгоритму.

Обчислити:

$$f = pF + 1; \quad h = pGf^{-1} (\mathrm{mod}\, q) \tag{2}$$

Зашифрування.

Дано: Повідомлення m, відкритий ключ h, випадковий компонент *seed*.

Обчислити:

$$M = m \,||\, seed; \quad r = \lambda(M); \tag{3}$$

$$m' = M \wedge H(r * h (\mathrm{mod}\, q)); \tag{4}$$

$$E = (r * h + m') \bmod q. \tag{5}$$

Розшифрування.

$$m' = ((f * E) \bmod q) \bmod p; \tag{6}$$

$$r * h \bmod q = E - m'; \tag{7}$$

$$M = m' \wedge H(r * h \bmod q); \qquad r = \lambda(M); \tag{8}$$

Якщо E=(r*h+m')mod q, то розшифрування вірне, інакше – помилка.

Усі операції виконуються в кільці поліномів чи в кільці поліномів над скінченим полем, що визначається алгоритмом.

Аналіз алгоритмів генерації ключів, зашифрування та розшифрування показує, що найбільш складною є операція множення поліномів в скінчених полях [6]. Причому, для запобігання атак сторонніми каналами необхідно забезпечити незалежність часу виконання операцій множення поліномів від розміщення ненульових елементів ключа. У [5, 6, 8] для множення поліномів пропонується використовувати метод Тоома разом з методом Карацуби [9],

в [7, 10] – метод Number TheoreticTransform (NTT), але їх використання зменшує продуктивність та накладає свої обмеження.

Мета та методи оптимізації

Оскільки основу алгоритмів генерації ключів, зашифрування та розшифрування складає операція множення поліномів, то в подальшому розглядаються методи та результати оптимізації алгоритму множення поліномів в кільцях поліномів над скінченими полями. Мета оптимізації – досягнення найменшої обчислювальної складності в порівнянні з уже досягнутими результатами [7, 8, 12, 17] за умови неможливості використання часу виконання функції множення для отримання додаткової інформації про особистий ключ. При оптимізації будемо враховувати не тільки алгоритмічні можливості, які дозволяють зменшити кількість операцій, а і засоби оптимізації, які враховують структуру сучасних процесорів, а саме – мінімізацію помилок в прогнозуванні переходів, кількості «промахів» значень кешу, звертання до не «вирівняної» пам'яті [13] тощо.

2. Сутність та властивості алгоритмів оптимізації

Існуючі алгоритми множення поліномів поділимо на 2 класи. До першого класу віднесемо алгоритми, які використовують властивості структури особистого ключа. До другого – алгоритми, аналогічні швидкому перетворенню Фур'є тощо. В першому випадку вдається врахувати, що більшість коефіцієнтів поліному, що визначає особистий ключ NTRU, дорівнюють 0, а ненульові коефіцієнти дорівнюють 1 або -1. Тому операцію множення можна замінити операціями додавання та віднімання, що дає хороші шанси на зменшення часу обчислення. В другому випадку використовуються можливості оптимізації засобом використання методу Тоома – Кука, теоретико-числових перетворень, швидких перетворень Фур'є [9, 11, 14], тощо.

Що стосується алгоритмів другого класу, то використання методу Тоома – Кука разом з методом Карацуби розглянуто в [5, 12]. Цей метод найбільш ефективний, якщо залишок від ділення N на 2^k близький до 2^k. Саме такий параметр обрано розробниками NTRU Prime [2] (N=761, 761 mod 128 = 121). Використання теоретико-числових перетворень (Number TheoreticTransform – NTT) [7, 10] має суттєве обмеження щодо використання, а саме вимоги $q \equiv 1 (\mathrm{mod} 2*N)$ і q – просте число. Саме такі параметри обрані розробниками CRYSTALS-DILITHIUM [2, 7]. Там же досліджено ефективність цього методу. Наші дослідження показали, що використання швидкого перетворення Фур'є [14] значно поступається продуктивності іншим методам, тому в статті результати не наводяться.

Методи, що пропонуються, відносяться до першого класу алгоритмів, їх можна використовувати для довільних значень q, N без обмежень. Основною метою їх використання є оптимізація операцій множення поліномів за умови виключення або мінімізації можливості отримання інформації про структуру ключа.

Опис запропонованих алгоритмів

Нехай поліном a складається з N елементів, кожний елемент за модулем q, значення елементів в інтервалі $[0..q–1]$ (великий поліном).

Другий поліном складається з N елементів, кожний елемент за модулем 3 і приймає значення 0, 1, -1 (малий поліном). Кількість ненульових елементів фіксована, є параметром алгоритму. Позначимо її T. В деяких алгоритмах кількість 1 та -1 співпадає, для деяких вона може бути різною. У даній роботі розглядається більш загальний випадок, коли фіксується тільки загальна кількість 1 та -1.

Алгоритм 1

Вхід: $a(x)=a_0+a_1x+a_2x^2+\ldots+a_{n-1}x^{N-1}$

Вхід: $b(x)=b_0+b_1x+b_2x^2+\ldots+b_{n-1}x^{N-1}$($b_i \in \{0, 1, -1\}$, кількість ненульових елементів T

Вихід: $c(x)=a(x)*b(x)$

1 $c_0=c_1=c_2=\ldots=c_{2n-1}=0$;

2 Для i:=0 до N–1 виконати:

2.1 Якщо b_i==1, то

2.1.1 Для j:=0 до *N*–1 виконати:

2.1.1.1 $C_{i+j}=C_{i+j}+a_j$.

2.2 Якщо b_i==-1, то

2.2.1 Для j:=0 до *N*–1 виконати:

2.2.1.1 $C_{i+j}=C_{i+j}-a_j$.

Недолік алгоритму. Наявність команд умовного переходу. По кількості непередбачених переходів, які впливають на час виконання операції, можна визначити додаткову інформацію про поліном b.

Для виключення операцій переходу будемо задавати поліном b як структуру, в якій визначимо:

індекси одиничних та мінус одиничних елементів;

кількість одиничних елементів.

Алгоритм 2

Вхід: $a(x)=a_0+a_1x+a_2x^2+\ldots+a_{n-1}x^{N-1}$

Вхід: структура з елементами: *ones* – індекси ненульових елементів, спочатку ідуть індекси одиничних, а потім індекси мінус одиничних елементів, розмір цього масиву фіксований (T). *onescount* – кількість одиничних елементів, тоді кількість елементів, які дорівнюють -1 *minusonescount=T–onescount*, далі Структура

Вихід: c(x)=a(x)*b(x)

1 $c_0=c_1=c_2=\ldots=c_{2N-1}=0$;

2 Для i:=0 до onescount–1 виконати:

2.1 k:=$ones_i$;

2.2 Для j:=0 до *N*–1 виконати:

2.2.1 $c_{k+j}=(c_{k+j}+a_j) \bmod q$

3 Для i:=onescount до *T*–1 виконати:

3.1 k:=$ones_i$;

3.2 Для j:=0 до *N*–1 виконати:

3.2.1 $c_{k+j}=(c_{k+j}-a_j) \bmod q$

Операції додавання та віднімання можна розглядати як однакові операції з погляду обчислювальної складності.

Алгоритм потребує *T* операцій додавання поліномів, а з урахуванням степені поліному *T*N* елементарних операцій зсув на *k* елементів не потребує додаткового часу.

Елементарні операції можуть бути замінені блочними операціями.

Для усіх сучасних NTRU алгоритмів значення $q<2^{14}$, тобто коефіцієнти поліному *a* менше, ніж 2^{14}, тому для коефіцієнту можна виділяти 16 бітів. У разі використання AVX операцій один блок складається з 16 коефіцієнтів.

Позначимо кількість блоків для завдання поліному $m=\left\lceil \frac{N}{16} \right\rceil$.

Позначимо поліном *A*, який відповідає поліному *a* і складається з блоків:

$$A(X)=A_0+A_1x^{16}+\ldots+A_{m-1}x^{16(m-1)}. \quad (9)$$

Поліном *b*(*x*) задаємо у вигляді структури як для Алгоритму 2

Результат – поліном

$$C(X)=C_0+Cx^{16}+\ldots+C_{2m-2}x^{16*(2m-2)} \quad (10)$$

Алгоритм 3

Вхід: $A(X)=A_0+A_1x^{16}+\ldots+A_{m-1}x^{16(m-1)}$

Вхід: Структура

Вихід: C(x)=A(x)*b(x)

1 $C_0=C_1=\ldots=C_{2m-2}=0$;
2 Для i:=0 до onescount–1 виконати:
2.1 k:=$ones_i$;
2.2 Обчислити адресу блоку результату *PC*, це адреса *k* елементу в поліномі C
2.3 Для j:=0 до *m*–1 виконати:
2.3.1 $PC_j=PC_j+A_j \bmod q$
3 Для i:=onescount до *T* виконати:
3.1 k:= $ones_i$;
3.2 Обчислити адресу блоку результату *PC*, це адреса *k* елементу в поліномі C
3.3 Для j:=0 до m–1 виконати:
3.3.1 $PC_j=PC_j–A_j \bmod q$

Недолік алгоритму 3.

Операції додавання та віднімання блоків фактично складаються з операцій: завантаження в регістр, виконання потрібної операції з записом результату в регістр, операція запису блоку з регістру в пам'ять. Адреса PC_j визначається номером ненульового елементу, вона може бути вирівняна на границю блоку, тобто ділитися на 16, або не вирівняною. Для сучасних процесорів звертання до не вирівняної та до вирівняної пам'яті відрізняється несуттєво при читанні даних, але запис по не вирівняній адресі може бути використано для отримання інформації про поліном *b*.

Для виключення звертання до не вирівняної пам'яті в режимі запису модифікуємо алгоритм 3 у вигляді алгоритму 4.

Алгоритм 4

Вхід: $A(X)=A_0+A_1x^{16}+\ldots+A_{m-1}x^{16(m-1)}$

Вхід: Структура

Вихід: C(x)= A(x)*b(x)

1. $C_0=C_1=\ldots=C_{2m-2}=0$;
2. Передобчислення: $P_0=A_0$; $P_1=P_0<<1$; $P_2=P_1<<1$;…$P_{15}=P_{14}<<1$; (Операція << означає операцію зсуву вліво на 1 елемент блоку в сторону старших елементів)
3. Для i:=0 до onescount–1 виконати:
3.1 k:=$ones_i$;
3.2 l=k mod 16
3.3 nb=k/16
3.4 $C_{nb}=C_{nb}+P_k$
3.5 Обчислити початкову адресу для поліному B, з урахуванням передобчислень PB=b–l
3.6 Для j:=1 до *m* виконати
3.6.1 $C_{nb+j}=(C_{nb+j}+PB_j) \bmod q$
4. Для i:=onescount до *T* виконати:
4.1 k:=$ones_i$;
4.2 l=k mod 16
4.3 nb=k/16
4.4 $C_{nb}=C_{nb}–P_k$
4.5 Обчислити початкову адресу для поліному B, з урахуванням передобчислень PB=b–l
4.6 Для j:=1 до *m* виконати
4.6.1 $C_{nb+j}=(C_{nb+j}–PB_j) \bmod q$

В алгоритмі 4 не вирівняна пам'ять використовується тільки для звертання до другого поліному в режимі читання. Звертання до поліному результату і в режимі читання, і в режимі запису виконується для вирівняної пам'яті.

Розглянемо операцію обчислення за модулем *q*.

Для усіх сучасних версій NTRU $q<2^{14}$, тобто при додаванні таких елементів, отримаємо значення, яке не перевищує $2^{15}–1$, тобто цілих довжиною 2 байти. Для приведення за модулем достатньо виконати для кожного коефіцієнту:

При додаванні:

$c = a + b;$ якщо $c>q-1$, то $c=c–q$

і при відніманні:

$c=a–b$; якщо $c<0$, то $c=c+q$.

Визначимо кількість блочних операцій для алгоритму 4.

Для операції передобчислень для значення P0 використовується операція копіювання, яка складається з 2 блочних операцій, для зсуву на 1 елемент використовуються дві операції _mm256_alignr_epi8, _mm256_permute2x128_si256 та операція запису в пам'ять, загальна кількість операцій 2+15*3=47. Усі операції виконуються для вирівняних даних. Кількість операцій не залежить від степені поліному.

Для обчислення значення модуля необхідна операція порівняння, виділення, додавання (віднімання) та запису в пам'ять, тобто 4 блочних операції.

Для обчислення C для одного ненульового значення необхідно завантаження поточного блоку для поліному C (вирівняний блок), завантаження поточного блоку для поліному A (не вирівняний блок), додавання (віднімання) та обчислення модуля для кожного результату. Загальна кількість блокових операцій для коефіцієнтів поліному C – $7mT$

Загальна кількість блокових операцій для множення поліномів дорівнює $7mT+47$.

Для $n=761$, $m=48$, $T=286$ загальна кількість блокових операцій дорівнює 96143 операції.

Паралелізація алгоритму

Для паралельного виконання алгоритму 4 необхідно забезпечити достатнє навантаження ядер (грануляція), рівномірний розподіл навантаження між ядрами (балансування).

Максимальна кількість паралельних потоків визначена експериментально.

В сучасних алгоритмах NTRU не фіксується кількість позитивних та негативних елементів, фіксованою є їх загальна кількість. Для балансування кожний потік виконує операції над позитивними і негативними елементами. Якщо кількість потоків дорівнює ThreadsCount, то кожний потік виконує обробку наступних $\left\lceil \frac{onescount}{TheadsCount} \right\rceil$ та $\left\lceil \frac{minuscount}{TheadsCount} \right\rceil$ ненульових елементів. Останній потік оброблює решту елементів.

В якості вхідних даних для потоку задаються 2 структури.

Структура 1 – загальна для усіх потоків, яка містить поліном A, та передобчислені значення P.

Структура 2 – для кожного з потоків містить адреси початку індексів одиничних та мінус одиничних елементів, та їх кількість.

Кожний потік виконує фактично алгоритм 4 за умови, що йому в якості вхідних даних передаються передобчислені значення (структура 1).

Використання паралельних обчислень без врахування накладних витрат дозволяє отримати обчислювальну складність в разі використання 4 потоків в 24024 блокових операцій.

Для збільшення ефективності критичний код написано на асемблері. Застосування асемблеру дозволило мінімізувати вплив звернення до не вирівняної пам'яті навіть при читанні. При зверненні до не вирівняної пам'яті застосовується додаткова команда звернення до вирівняної і навпаки. Таким чином, кількість звернень і до вирівняної і до не вирівняної пам'яті залишається постійною.

3. Експериментальне дослідження алгоритмів

Мета експериментальної перевірки – визначити експериментально обчислювальну складність запропонованого алгоритму та порівняти її з обчислювальною складністю інших авторів за однакових або близьких параметрів.

Перевірити стійкість до атаки, пов'язаної зі сторонніми каналами запропонованого алгоритму за умови збереження константної кількості ненульових елементів в малому поліномі.

Вихідні дані щодо експериментального дослідження складності множення поліномів для стандарту NTRU та алгоритмів, які запропоновані в якості претендентів на постквантові стандарти, наведено в табл. 1.

Таблиця 1

Вихідні дані щодо дослідження складності множення поліномів

Назва алгоритму	Поле	Параметри
ANSI X9.98 – 2010	$Z/qZ[X](X^N-1)$	N=401..1499, q=2048, t=38..157
NTRU Prime	$Z/qZ[X](X^N-X-1)$	N=439..1021, q – просте, t=18..204

В якості параметрів обрано параметри, для яких автори NTRU Prime навели свою реалізацію (функція rq_mult) і має сенс виконати порівняння двох реалізацій, а саме N=761, q=4591 та t=143 [2] за допомогою одного процесору і середовища. Крім того, вперше наведено результати для параметрів, визначених для криптостійкості K=512, а саме N=1471, t=255, q=12269.

Методика експерименту. При обранні методики експерименту використано рекомендації [15]. Для виміру часу використовуються такти процесору. Для зменшення впливу випадкових факторів, а саме переключення на виконання модулів ОС, завантаження коду для додатку та даних в кеш, і т.д., кожний тест виконується PROBS=100 разів, з цих вимірів обирається мінімальне, тому що збільшення часу можливо тільки в разі додаткового впливу випадкових факторів.

Експериментальне дослідження виконувалось для 10000 ключів [6] з використанням процесору Intel(R) Core (TM) i5-4440 CPU @3.10 GHz.

Створено 3 набори ключів, кожний складається з 10000 ключів. Для визначення впливу не вирівняних даних на час виконання штучно формуються малі поліноми, в яких в якості індексів ненульових елементів обирається максимальна кількість індексів, які кратні 16, що забезпечує мінімізацію звернень до не вирівняної пам'яті в AVX-2 командах. Такий набір ключів позначається GOOD. Другий набір ключових даних формується таким чином, щоб усі індекси ненульових елементів були не кратні 16, тобто кількість звернень до не вирівняної пам'яті була максимальною. Такий набір ключів позначається BAD. В третьому наборі даних індекси ненульових елементів обирались випадково, як це необхідно при генерації ключів. Такий набір ключів позначається RAND.

Для визначення точності вимірів і обчислювальної складності створюється додатковий набір ключів, який позначено EQUAL. Він складається з однакових ключів (перший ключ з набору RAND), саме для цього ключа визначається обчислювальна складність та діапазон, в якому змінюються ці значення для функцій, які аналізуються.

Для кожного набору ключових даних проводяться 10 іспитів.

Спочатку наведемо дані про часову складність методів, а потім – результати дослідження можливості використання часу як додаткової атаки на особистий ключ. Для порівняння з нашими результатами використовується функція rq_mult, яка представлена в алгоритмі NTRU Prime [2]. Будемо називати цю функцію базовою. Саме ця функція використовується в якості базової тому, що вона має найкращі результати щодо обчислювальної складності з відомих в літературі, коли не використовуються спеціальні форми завдання малого поліному (добуток), а також вона доступна в вихідних кодах.

Часові характеристики функцій наведені в табл. 2 (Linux). Для виміру використовується набір ключів EQUAL. Похибка виміру для базової функції менше похибки виміру для нашої функції. Це ускладнює задачу криптоаналітиків використати різницю у вимірі часу як побічного каналу.

Таблиця 2

Часові характеристики функцій множення поліномів (тактів)

K	rq_mult	Точність виміру	Mul	Точність виміру
256	27160- 27860	2.6%	13120-13677	4.24%
512	-	-	30376-31200	2.7%

Таким чином, запропонована функція в середньому забезпечує прискорення в порівнянні з базовою практично в два рази. На жаль, ми не змогли порівняти продуктивність функцій для криптостійкості K=512, тому що реалізація функції rq_mult в режимі оптимізації не передбачає використання інших параметрів. Отримані результати показали, що точність вимірів дещо знижується при використанні нашої функції з 2,5 для базової функції до 4,24 % для нашої.

Результати для 10 серій тестів з наборами GOOD, BAD, RAND представлено в табл. 3. Для кожної серії вимірів задані: мінімальне значення часу (колонка min), номер ключа, для якого це мінімальне значення отримано (nmin), максимальний вимір часу (max).

Таблиця 3

Порівняльний аналіз різних груп ключових даних

Номер серії	Набір ключів	K=256, такти			K=512, такти		
		min	nmin	max	min	nmin	max
1	GOOD	13136	7443	13661	29484	4443	31556
	BAD	13180	412	13727	30280	6174	32138
	RAND	13120	3270	13677	30376	31	31200
2	GOOD	13036	3950	13661	29516	8290	31515
	BAD	13196	3846	13734	30332	8552	32119
	RAND	13160	713	13681	29896	6738	31961
3	GOOD	13148	2740	13659	29472	4443	31503
	BAD	13168	2066	13731	30280	7868	32147
	RAND	13128	2886	13681	29936	1158	32024
4	GOOD	13144	3210	13657	29504	8387	31548
	BAD	13148	8603	13726	30076	7786	32151
	RAND	13084	3283	13681	30188	7740	32005
5	GOOD	13124	4243	1366	29352	5956	31537
	BAD	13216	8174	13731	30316	6407	32127
	RAND	13192	4124	13686	30144	827	31981
6	GOOD	13124	5074	13657	29380	3998	31529
	BAD	13204	5303	13730	30304	3773	32127
	RAND	13148	6107	13683	29972	7061	31986
7	GOOD	13088	6254	13664	29516	4443	31549
	BAD	13132	0	13730	30528	277	32141
	RAND	13128	2322	13676	29872	1158	32022
8	GOOD	13100	4691	13663	29424	550	31526
	BAD	13188	7845	13728	30104	6212	32141
	RAND	13180	3337	13678	30108	2544	31982
9	GOOD	13144	5212	13662	29428	5956	31539
	BAD	13120	208	13725	30400	3803	32132
	RAND	13152	2813	13678	30164	6738	32008
10	GOOD	13104	0	13660	29676	2620	31550
	BAD	13184	1204	13726	30300	3539	32149
	RAND	13128	7531	13679	30216	6753	32009

Як показують результати табл. 3, номери ключів, при яких кількість тактів мінімальна, не співпадають для різних серій (значення 0 відповідають різним групам ключів). Таким чином, використання цього фактору для аналізу ключів неможливе. Мінімальне значення часу може бути як для набору ключів GOOD, так і для інших наборів; таким чином, мінімізація кількості звернень до не вирівняної пам’яті не завжди приводить до зменшення часу. Крім того, для отримання таких ключів необхідно, щоб елементи з індексами 0, 16, 32,…, *N* були

ненульовими. Різниця між значеннями часу для наборів GOOD та BAD не перевищує 2.5% – це мінімальна похибка вимірів. Таким чином, використання цих результатів для атаки сторонніми каналами не ефективне. В той же час алгоритм, запропонований в роботі, дозволяє отримати суттєве підвищення продуктивності функції множення. Результати були підтверджені за допомогою статистичної обробки методом Welch's *t*-test [16].

Реалізацію функцій множення для звичайної форми завдання поліномів та форми f1*f2+f3 (PRODUCT) наведено в [18].

Висновки

1. В асиметричних постквантових криптографічних перетвореннях необхідне суттєве збільшення довжин загальних параметрів, асиметричних пар ключів та електронних підписів тощо. Збільшення довжини параметрів та ключів приводить до збільшення часу виконання операцій; у випадку, що розглядається в статті, – до збільшення складності множення поліномів. При переході з 256 бітної до 512 бітної криптостійкості час виконання функції множення збільшується більше, ніж в два рази (див. табл. 2). Так як операція множення поліномів є складовою частиною генерації ключів, прямого та зворотного перетворень, то вона впливає на складність в цілому. Тому збільшення продуктивності цієї операції є дуже важливим.

2. Запропоновані методи оптимізації дозволили отримати функцію множення поліномів, яка дозволяє збільшити продуктивність практично в два рази по відношенню до найбільш продуктивної функції множення, яка є складовою частиною алгоритму NTRU Prime – учасника конкурсу NIST.

3. Виконано аналіз ефективності атаки, пов'язаної зі сторонніми каналами, а саме часу виконання. За допомогою експериментальних досліджень та їх статистичної обробки показано, що для запропонованого алгоритму ця атака не ефективна.

4. Результати проведених експериментів показали, що для запропонованого алгоритму множення поліномів різниця в складності (часі) для найкращих та найгірших ключів (табл. 3) складає не більше 1 %. В той же час похибка виміру складності множення поліномів для конкретного ключа складає не менше 2 %. Тому використання різниці між складністю множення поліномів для різних ключів для успішної атаки сторонніми каналами є практично не можливим.

5. Отримані результати дозволяють реалізувати захищеність зі значеннями 512 біт класичної та 256 біт квантової криптостійкості.

Список літератури:

1. Lily Chen Stephen Jordan Yi-Kai Liu Dustin Moody Rene Peralta Ray Perlner Daniel Smith-Tone. Report on Post-Quantum Cryptography. [Electronic resource]. Access mode: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf.

2. Проекти, які прийняті на конкурс. [Electronic resource]. Access mode: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

3. Daniel J. Bernstein Johannes Buchmann Erik Dahmen. Post-Quantum Cryptography. [Electronic resource]. Access mode: https://www.researchgate.net/profile/Nicolas_Sendrier/publication/226115302_Code-Based_ Cryptography/links/540d62d50cf2df04e7549388/Code-Based-Cryptography.pdf.

4. American National Standard for Financial Services ANSI X9.98 – 2010. Lattice-Based Polynomial Public Key Establishment Algorithm for the Financial Services Industry. Date Approved: 10/15/2010.

5. Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, and Christine van Vredendaal. NTRU Prime. [Electronic resource]. Access mode: https://ntruprime.cr.yp.to/ntruprime-20160511.pdf.

6. Wei Dai, William Whyte, and Zhenfei Zhang. Optimizing polynomial convolution for NTRUEncrypt. [Electronic resource]. Access mode: https://eprint.iacr.org/2018/229.pdf.

7. Léo Ducas, Tancrède Lepoint, Vadim Lyubashevsky and others. CRYSTALS – Dilithium: Digital Signatures from Module Lattices. [Electronic resource]. Access mode: https://eprint.iacr.org/2017/633.pdf.

8. Andreas Hülsing, Joost Rijneveld, John Schanck , and Peter Schwabe. High-speed key encapsulation from NTRU. [Electronic resource]. Access mode: https://cryptojedi.org/papers/ntrukem-20170627.pdf.

9. Toom 3-Way Multiplication. [Electronic resource]. Access mode: https://gmplib.org/manual/Toom-3_002dWay-Multiplication.html.

10. Erdem Alkim, Leo Ducas, Thomas Poppelmann, Peter Schwabe. Postquantum key exchange. A new hope, 2016. [Electronic resource]. Access mode: https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_alkim.pdf.

11. Number-theoretic transform (integer DFT). [Electronic resource]. Access mode: https://www.nayuki.io/page/number-theoretic-transform-integer-dft.

12. Daniel J. Bernstein1, Chitchanok Chuengsatiansup, Tanja Lange, and Christine van Vredendaal. NTRU Prime: reducing attack surface at low cost. [Electronic resource]. Access mode: https://eprint.iacr.org/2016/461.pdf.

13. Intel 64 and IA-32 Architectures Optimization Reference Manual. [Electronic resource]. Access mode: https://software.intel.com/sites/default/files/managed/9e/bc/64-ia-32-architectures-optimization-manual.pdf.

14. Discrete Fourier transform (DFT). https://en.wikipedia.org/wiki/Discrete_Fourier_transform_(general).

15. Oscar Reparaz, Josep Balasch and Ingrid Verbauwhede. Dude, is my code constant time? https://eprint.iacr.org/2016/1123.pdf.

16. Welch's t-test. https://academic.oup.com/biomet/article-abstract/34/1-2/28/210174?redirected From=fulltext.

17. Kachko O., Gorbenko Yu., Yesina M., Akolsina O. Asymmetric Encryption Algorithm Optimization Based on Using NTRU Prime Mathematics // Radiotechnika. 2017. №191. P. 5–10.

18. Kachko O., Gorbenko I., Yesina M., Kandiy S. Polynomials multiplication functions for ordinary and product form of one of the polynomials representation. [Electronic resource]. Access mode: https://github.com/kandiyiit/NTRU-POLYNOMIALS-MULTIPLICATION.

Харківський національний
університет радіоелектроніки;
АТ «Інститут інформаційних технологій»;
Харківський національний
університет імені В. Н. Каразіна

Надійшла до редколегії 09.01.2020

УДК 621.391:519.2 **DOI:10.30837/rt.2020.1.200.03**

О.С. ШЕВЧУК

РАНДОМІЗОВАНА СИМЕТРИЧНА КРИПТОСИСТЕМА МАК-ЕЛІСА НА ОСНОВІ УЗАГАЛЬНЕНИХ КОДІВ РІДА - СОЛОМОНА

Вступ

Однією з актуальних проблем сучасної криптографії є створення практичних постквантових криптосистем, стійкість яких базується на складності розв'язання єдиної обчислювально складної задачі, аналогічно тому як стійкість криптосистеми RSA базується на складності факторизації цілих чисел. Перспективний клас таких криптосистем утворюють кодові криптосистеми, найпершою асиметричною з яких є криптосистема Мак-Еліса [1].

На сьогодні відомо декілька конструкцій симетричних кодових криптосистем, аналогічних криптосистемі Мак-Еліса, наприклад схеми шифрування Жордана [2], Рао [3], Рао - Нама [4] та низка вдосконалень останньої криптосистеми [5, 6], однак жодна з них не задовольняє цілком сучасним вимогам щодо стійкості та практичності одночасно.

В [7] запропоновано рандомізовану криптосистему Мак-Еліса, яка відрізняється від оригіналу використанням випадкових секретних даних при зашифруванні. Показано, що, на відміну від оригінальної, рандомізована криптосистема Мак-Еліса за певних умов є обґрунтовано стійкою відносно атак з підібраним відкритим тестом (CPA-стійкою). Іншим прикладом симетричної кодової криптосистеми, для якої відомо обґрунтування стійкості (security proof), є LPN-C [8], проте задача зменшення довжини ключа або підвищення швидкості передачі інформації при збереженні рівня стійкості цієї криптосистеми залишається актуальною.

Дану роботу присвячено створенню та дослідженню симетричної версії криптосистеми з [7], що будується на основі узагальнених кодів Ріда - Соломона (УРС). Вибір цих кодів зумовлено, перш за все, тим, що вони існують для всіх природних значень параметрів (довжини та вимірності коду) і є максимально дистанційно роздільними (МДР), що дозволяє в широких межах змінювати характеристики відповідних криптосистем. Крім того, для зазначених кодів відомі дуже швидкі алгоритми декодування (до половини кодової відстані та, навіть, за її межами) [9]. Нарешті, асиметричні криптосистеми, побудовані на основі кодів УРС [10, 11], є нестійкими, оскільки для них існують ефективні алгоритми відновлення секретних ключів за відкритими [12, 13]. Це викликає додатковий інтерес до стійкості відповідних симетричних криптосистем.

В роботі отримано оцінки стійкості зазначених криптосистем відносно природної атаки з підібраним відкритим текстом та запропоновано алгоритм вибору параметрів для побудови цих криптосистем. Проведено порівняння досліджених криптосистем з відповідними криптосистемами типу LPN-C і показано, що перші мають помітно меншу довжину ключа при заданій стійкості в порівнянні з останніми.

1. Означення основних понять та уточнення постановки задачі

Нехай F – поле з 2^s елементів, $s \geq 2$. Для матриці M над полем F позначимо $< M >$ лінійний код над цим полем, породжений рядками матриці M. Нехай k, n – натуральні числа, $k \leq n \leq 2^s$, $\alpha = (\alpha_1, \ldots, \alpha_n) \in F^n$, $\beta = (\beta_1, \ldots, \beta_n) \in (F \setminus \{0\})^n$, де α_i є попарно різними, $i \in \overline{1,n}$.

Узагальнений код Ріда - Соломона $GRS_{n,k}(\alpha, \beta)$ визначається як лінійний код над полем F з твірною матрицею

$$G_{\alpha,\beta} = \begin{pmatrix} \beta_1 & \beta_2 & \dots & \beta_n \\ \alpha_1\beta_1 & \alpha_2\beta_2 & \dots & \alpha_n\beta_n \\ \dots & \dots & \dots & \dots \\ \alpha_1^{k-1}\beta_1 & \alpha_2^{k-1}\beta_2 & \dots & \alpha_n^{k-1}\beta_n \end{pmatrix}, \quad (1)$$

тобто $GRS_{n,k}(\alpha,\beta) = < G_{\alpha,\beta} >$. Відомо [14], що цей код є *максимально дистанційно розділь-ним*, тобто має найбільшу для заданих n і k мінімальну відстань $d = n-k+1$, а також найбільшу дуальну відстань $d^{\perp} = k+1$. Код УРС дозволяє виправляти будь-яку кількість $t \le \lfloor 1/2 \cdot (d-1) \rfloor$ (адитивних) помилок, використовуючи $O(2^s s^2)$ арифметичних операцій в полі F [9].

Рандомізована симетрична криптосистема Мак-Еліса з параметрами $l, k, n \in \mathbf{N}$, $\varepsilon \in (0,1)$, де $l \le k \le n \le 2^s$, що будується на основі кодів УРС, визначається таким чином.

Секретними ключами у криптосистемі є пари (α,β), де $\alpha, \beta \in F^n$, координати вектора α є попарно різними, а координати вектора β – ненульовими елементами поля F, $i \in \overline{1,n}$.

Для зашифрування відкритого тексту $m \in F^l$ на ключі (α,β) відправник генерує незалежні випадкові вектори r та $\xi = (\xi_1, \dots, \xi_n)$, де вектор r має рівномірний розподіл ймовірностей на множині F^{k-l}, а координати вектора ξ є незалежними випадковими величинами, що розподілені за законом

$$\mathbf{P}(\xi_i = 0) = 2^{-s}(1+(2^s-1)\varepsilon), \ \mathbf{P}(\xi_i = a) = 2^{-s}(1-\varepsilon), \ a \in F \setminus \{0\}, \ i \in \overline{1,n}. \quad (2)$$

Далі відправник обчислює шифротекст за формулою

$$E(m) = (r, m)G_{\alpha,\beta} \oplus \xi. \quad (3)$$

де матриця $G_{\alpha,\beta}$ визначається за формулою (1).

Для розшифрування повідомлення (3) на ключі (α,β) отримувач обчислює вектор $(r, m)G_{\alpha,\beta}$, використовуючи алгоритм декодування коду $GRS_{n,k}(\alpha,\beta)$ зі складністю $O(2^s s^2)$ операцій [9]. Нарешті, на підставі лінійної незалежності рядків матриці (1) отримувач може відновити вектор (r, m), наприклад, за допомогою алгоритму Гаусса.

Зауважимо, що у випадку, коли число ненульових координат вектора ξ є більше ніж $\lfloor 1/2 \cdot (d-1) \rfloor$, можлива помилка розшифрування, ймовірність якої, як показано далі, можна зробити достатньо малою шляхом вибору параметра ε.

Зауважимо також, що означена вище криптосистема є симетричним аналогом окремого випадку рандомізованої (асиметричної) криптосистеми Мак-Еліса, описаної в [7]. В цій криптосистемі замість коду УРС використовується довільний двійковий лінійний код із швидким алгоритмом декодування (на рівні половини мінімальної відстані). У криптосистемах з відкритим ключем, зокрема рандомізованих, побудованих на основі кодів УРС, матриця (1) відіграє роль частини секретного ключа. При цьому відкритим ключем є деяка інша твірна матриця того ж самого коду [10] або його випадково обраного підкоду [11]. Вразливість таких криптосистем є наслідком того, що, знаючи код УРС $GRS_{n,k}(\alpha,\beta)$ (або навіть його підкод відносно невеликої вимірності), можна відновити вектори α, β за поліноміальний від n час [12, 13]. Для симетричної криптосистеми з рівнянням шифрування (3) код $GRS_{n,k}(\alpha,\beta)$ є невідомим, тому що на цю криптосистему є незастосовними атаки, описані в [12, 13].

2. Умова, що забезпечує малість ймовірності помилки розшифрування

Твердження 1. Нехай для зазначених вище $k, n,\ s$ та $\delta \in (0,1)$ виконується умова

$$1-\frac{1}{1-2^{-s}}\left(\frac{1}{2}-\frac{k}{2n}-\sqrt{\frac{\ln(\delta^{-1})}{2n}}\right)\le \varepsilon<1. \tag{4}$$

Тоді ймовірність того, що законний отримувач відновить відкритий текст m за шифротекстом (2), є не менше ніж $1-\delta$.

Доведення. Згідно з означенням криптосистеми, якщо відбувається помилка розшифрування, то число ненульових координат вектора ξ є більше ніж $\lfloor 1/2\cdot(d-1)\rfloor$.

Введемо випадкові величини $\eta_1,\dots,\eta_n$, де $\eta_i=1$, якщо $\xi_i\neq 0$; $\eta_i=0$ – у протилежному випадку. Тоді $\eta_1,\dots,\eta_n$ є незалежними в сукупності та розподілені за законом $\mathbf{P}(\eta_i=1)=1-\mathbf{P}(\eta_i=0)=(1-2^{-s})(1-\varepsilon)$, $i\in\overline{1,n}$. При цьому ймовірність помилки розшифрування не перевищує ймовірності події $\{\eta_1+\dots+\eta_n\ge 1/2\cdot(n-k)\}$, яку можна оцінити за допомогою нерівності Гефдінга [15].

Дійсно, справедливі такі співвідношення:

$$\mathbf{P}(\eta_1+\dots+\eta_n\ge 1/2\cdot(n-k))=\mathbf{P}\left(\sum_{i=1}^{n}\xi_i-\sum_{i=1}^{n}\mathbf{E}\xi_i\ge 1/2\cdot(n-k)-\sum_{i=1}^{n}\mathbf{E}\xi_i\right)=$$

$$=\mathbf{P}\left(\sum_{i=1}^{n}\xi_i-n(1-2^{-s})(1-\varepsilon)\ge 1/2\cdot(n-k)-n(1-2^{-s})(1-\varepsilon)\right)\le$$

$$\le\exp\left\{-2n\left(\frac{1}{2}-\frac{k}{2n}-(1-2^{-s})(1-\varepsilon)\right)^2\right\}\le\delta,$$

де передостання нерівність випливає з нерівності Гефдінга, а остання – з формули (4).

Твердження доведено.

Надалі вважатимемо, що параметри k, n, ε криптосистеми задовольняють умові (4).

3. Атака на криптосистему на основі підібраного відкритого тексту

Припустимо, що супротивник має доступ до оракула зашифрування E вигляду (3) та подає на його вхід t разів відкритий текст $m=0$. В результаті супротивник отримує систему рівнянь

$$r_jG^{(1)}_{\alpha,\beta}\oplus\xi_j=c_j,\ \ j\in\overline{1,t}, \tag{5}$$

де $G^{(1)}_{\alpha,\beta}$ – підматриця, що складається з перших $k-l$ рядків матриці (1), $c_1,\dots,c_t$ – відомі шифротексти, а $r_1,\dots,r_t$ та $\xi_1,\dots,\xi_t$ – незалежні випадкові вектори, де $r_1,\dots,r_t$ мають рівномірний розподіл на множині F^{k-l}, а координати векторів $\xi_1,\dots,\xi_t$ є незалежними випадковими величинами, розподіленими за законом (2).

З формул (1) і (5) випливає, що $c_1,\dots,c_t$ є словами невідомого коду УРС $GRS_{n,k-l}(\alpha,\beta)$, спотвореними у 2^s-му симетричному каналі зв'язку. Отже, відновивши цей код за набором його спотворених слів, можна знайти вектори α,β за поліноміальний від n час за допомогою алгоритму з [12]. Оскільки $GRS_{n,k-l}(\alpha,\beta)$ є кодом МДР, він є систематичним і для його відновлення можна скористатися методом, викладеним в [16].

Позначимо $G=(I_{k-l},\,X)$ невідому канонічну твірну матрицю коду $GRS_{n,k-l}(\alpha,\beta)$, де I_{k-l} – одинична матриця порядку $k-l$, X – матриця розміру $(k-l)\times(n-k)$. Існує оборотна матриця U над полем F така, що $G^{(1)}_{\alpha,\beta}=UG$. Підставляючи зазначену рівність у формулу (5) та позначаючи $v_j=r_jU$, отримаємо систему рівнянь вигляду

$$v_j(I_{k-l},\,X)\oplus\xi_j=c_j,\ j\in\overline{1,t}, \tag{6}$$

де $v_1,\dots,v_t$ є незалежними випадковими векторами з рівномірним розподілом на множині F^{k-l}.

Слідуючи методу [16], перетворимо систему рівнянь (6) наступним чином. Позначимо $c_j^{(1)}$ та $c_j^{(2)}$ підвектори вектора c_j, що складаються з його перших $k-l$ та останніх $n-(k-l)$ координат відповідно. Аналогічні позначення введемо для випадкового вектора ξ_j, $j\in\overline{1,t}$. Покладемо $A_j=v_j\oplus\xi_j^{(1)}$, $\zeta_j=\xi_j^{(1)}X\oplus\xi_j^{(2)}$, $j\in\overline{1,t}$. Рівність (6) рівносильна співвідношенням $(c_j^{(1)},\,c_j^{(2)})=(v_j\oplus\xi_j^{(1)},\ v_jX\oplus\xi_j^{(2)})$, $j\in\overline{1,t}$, які можуть бути записані у вигляді:

$$A_j=c_j^{(1)},\ A_jX\oplus\zeta_j=c_j^{(2)},\ j\in\overline{1,t}. \tag{7}$$

При цьому на підставі зазначених вище припущень щодо розподілів випадкових векторів $r_1,\dots,r_t$ та $\xi_1,\dots,\xi_t$ вектори $A_1,\dots,A_t$ є незалежними в сукупності та мають рівномірний розподіл на множині F^{k-l}, а вектори $\zeta_1,\dots,\zeta_t$ є незалежними в сукупності та не залежать від $A_1,\dots,A_t$.

Нарешті, як і в [16] позначимо A матрицю, що складається з рядків $A_1,\dots,A_t$, x_i – i-й стовпець матриці X; покладемо $b^{(i)}=(c_{1,i}^{(2)},\dots,c_{t,i}^{(2)})^{\mathrm{T}}$, $\zeta^{(i)}=(\zeta_{1,i},\dots,\zeta_{t,i})^{\mathrm{T}}$, де $c_{j,i}^{(2)}$ та $\zeta_{j,i}$ – i-ті координати векторів $c_j^{(2)}$ та ζ_j відповідно, $j\in\overline{1,t}$, $i\in\overline{1,n-(k-l)}$. На підставі рівностей (7) вектор x_i співпадає з істинним розв'язком $x_i^{(0)}$ системи лінійних рівнянь зі спотвореними правими частинами

$$Ax=b^{(i)}=Ax_i^{(0)}\oplus\zeta^{(i)}, \tag{8}$$

над полем F, де матриця A і вектор $b^{(i)}$ визначаються безпосередньо за набором слів $c_1,\dots,c_t$:

$$A_j=c_j^{(1)},\ b^{(i)}=(c_{1,i}^{(2)},\dots,c_{t,i}^{(2)})^{\mathrm{T}},\ j\in\overline{1,t},\ i\in\overline{1,n-(k-l)}.$$

Отже, атака на криптосистему, що розглядається, полягає у побудові для кожного $i\in\overline{1,n-(k-l)}$ системи лінійних рівнянь зі спотвореними правими частинами вигляду (8) та її розв'язанні за допомогою відомих методів. Відновивши істинні розв'язки зазначених систем рівнянь, знайдемо канонічну твірну матрицю $G=(I_{k-l},\,X)$ коду $GRS_{n,k-l}(\alpha,\beta)$, за якою відновимо вектори α,β, використовуючи алгоритм, описаний в [12].

4. Оцінка ефективності наведеної атаки

Для того, щоб оцінити трудомісткість атаки та обсяг матеріалу t, потрібного для її надійного виконання, треба спочатку знайти розподіл ймовірностей спотворень у правих частинах рівнянь системи (8).

Для будь-якого $\varepsilon \in (0,1)$ назвемо ε-*нерівномірним розподілом* на полі F розподіл ймовірностей вигляду (2).

Наступна лема випливає безпосередньо з наведеного означення та формули повної ймовірності.

Лема 1. Нехай ξ та η є незалежними випадковими величинами на полі F, що мають ε_1-нерівномірний та ε_2-нерівномірний розподіли ймовірностей відповідно. Тоді для будь-якого $c \in F \setminus \{0\}$ випадкова величина $c\xi$ має ε_1-нерівномірний, а випадкова величина $\xi + \eta$ має $\varepsilon_1\varepsilon_2$-нерівномірний розподіл ймовірностей на полі F.

Твердження 2. Для будь-якого $i \in \overline{1, n-(k-l)}$ координати випадкового вектора $\zeta^{(i)}$ у правій частині системи рівнянь (8) мають ε^{k-l+1}-нерівномірний розподіл ймовірностей, де ε визначається згідно з умовою (2).

Доведення. За означенням j-та координата випадкового вектора $\zeta^{(i)}$ має вигляд $\zeta_{j,i} = \xi_j^{(1)} x_i \oplus \xi_j^{(2)}$. При цьому всі координати вектора x_i є ненульовими елементами поля F. Дійсно, оскільки (I_{k-l}, X) – твірна матриця коду МДР $GRS_{n,k-l}(\alpha, \beta)$, то припущення про те, що деяка координата вектора x_i дорівнює нулю, тягне за собою існування слова над полем F, яке анулює зазначений код та має вагу, меншу ніж $k-l+1$, що протирічить тому, що $k-l+1$ є дуальною відстанню цього коду.

Таким чином, $\zeta_{j,i}$ є сумою точно $k-l+1$ незалежних випадкових величин, кожна з яких, згідно з умовою (2), має ε-нерівномірний розподіл ймовірностей на полі F. Отже, на підставі леми 1 $\zeta_{j,i}$ має ε^{k-l+1}-нерівномірний розподіл на цьому полі. Твердження доведено.

Отримаємо оцінку трудомісткості розв'язання системи рівнянь вигляду (8), вважаючи, що для цього використовується один з найефективніших на сьогодні алгоритмів [17].

Зазначений алгоритм залежить від параметрів $k' \geq 2$, що є степенем двійки, та $l' \in \overline{1, k-l}$, які задовольняють умові

$$\log(2\Delta(k')^{-1} l' s \ln 2) \leq s(k-l-l')(\log k')^{-1}, \tag{9}$$

і складається з двох етапів.

На першому етапі за допомогою алгоритму Вагнера (k'-tree algorithm) [18] здійснюється виключення з вхідної системи рівнянь (8) останніх $k-l-l'$ невідомих. В результаті отримується нова система лінійних рівнянь зі спотвореними правими частинами від l' невідомих над полем F, кожне рівняння якої є сумою певних k' рівнянь вхідної системи. На другому етапі отримана система рівнянь розв'язується методом максимальної правдоподібності із застосуванням швидкого перетворення Адамара.

Таким чином, зазначений алгоритм дозволяє відновити перші l' невідомих системи рівнянь (8). Застосовуючи його $\lceil l/l' \rceil$ разів до різних наборів невідомих, що не перетинаються, можна знайти шуканий вектор $x_i^{(0)}$.

В [17] показано, що середня (відносно незалежного випадкового рівноймовірного вибору рядків матриці A) трудомісткість алгоритму розв'язання системи рівнянь (8) визначається за формулою

$$T(k', l') = (m(k', l'))^{\frac{1}{\theta}} k' 2^{\frac{s(k-l-l')}{\theta}} + s(m(k', l') + sl' 2^{sl'}) + 2^{s(l'+1)}, \tag{10}$$

а обсяг матеріалу, потрібного для успішного розв'язання цієї системи, – за формулою

$$t = t(k', l') = k' 2^{\frac{s(k-l-l')}{\theta}} (2l' s \ln 2)^{\frac{1}{\theta}} \Delta(k')^{-\frac{1}{\theta}}, \tag{11}$$

де

$$\theta = 1 + \log k',\ m(k',l') = 2\Delta(k')^{-1} l' s \ln 2, \tag{12}$$

$$\Delta(k') = 2^{-s} \sum_{z \in F} (2^s \mathbf{P}\{\mu_1 + \cdots + \mu_{k'} = z\} - 1)^2,$$

причому $\mu_1, \ldots, \mu_{k'}$ є незалежними випадковими величинами, розподіленими за тим самим законом, що і спотворення у правій частині системи рівнянь (8).

Твердження 3. Справедлива рівність

$$\Delta(k') = (2^s - 1)\varepsilon^{2k'(k-l+1)}. \tag{13}$$

Доведення. На підставі твердження 2 випадкові величини $\mu_1, \ldots, \mu_{k'}$ мають ε^{k-l+1}-нерівномірний розподіл ймовірностей на полі F. Отже, згідно з лемою 1, випадкова величина $\mu_1 + \cdots + \mu_{k'}$ має $\varepsilon^{k'(k-l+1)}$-нерівномірний розподіл ймовірностей. Звідси безпосередньо випливає нерівність (13).

Таким чином, для оцінювання ефективності наведеної атаки можна використовувати наступний алгоритм.

Алгоритм 1.

Вхідні дані:

– верхня межа δ ймовірності помилкового розшифрування відкритого тексту законним отримувачем, $\delta \in (0, 1)$;

– довжина n та вимірність k коду УРС над полем з 2^s елементів, де $s \geq 2$, $k < n - \sqrt{2n \ln(\delta^{-1})}$, $n \leq 2^s$;

– довжина l відкритих текстів у криптосистемі, що розглядається, $l \leq k$.

1. Покласти $\varepsilon = 1 - \dfrac{1}{1 - 2^{-s}} \left(\dfrac{1}{2} - \dfrac{k}{2n} - \sqrt{\dfrac{\ln(\delta^{-1})}{2n}} \right)$.

2. Для будь-яких $l' \in \overline{1, k-l}$ та $k' = 2, 4, 8, 16, \ldots$, що задовольняють умові (9), обчислити значення $T(k', l')$, використовуючи формули (10), (12), (13).

3. Обрати k^* та $l^* \in \overline{1, k-l}$ такі, що $T(k^*, l^*) = \min\{T(k', l')\}$, де мінімум береться за всіма зазначеними вище парами (k', l').

Результат:

– значення k^* та l^* (останнє з яких дорівнює кількості координат довільного фіксованого стовпця канонічної твірної матриці коду УРС, які відновлюються за допомогою атаки);

– середня часова складність атаки $T(k^*, l^*)$;

– обсяг матеріалу $t(k^*, l^*) = k^* 2^{\frac{s(k-l-l^*)}{\theta}} (2l^* s \ln 2)^{\frac{1}{\theta}} \Delta(k^*)^{-\frac{1}{\theta}}$, потрібного для успішної реалізації атаки.

Зауважимо, що нерівності $s \geq 2$ та $k < n - \sqrt{2n \ln(\delta^{-1})}$ тягнуть умову $\varepsilon \in (0, 1)$, яка є необхідною для коректного вибору параметра ε. При цьому значення $T(k^*, l^*)$ визначає нижню межу стійкості криптосистеми відносно розглянутої атаки.

В табл. 1, 2 наведено чисельні значення параметрів та оцінки стійкості деяких криптосистем, що будуються на основі кодів УРС.

Таблиця 1

Результати виконання алгоритму 1 при $\delta = 10^{-8}$, $s = 9$, $n = 512$, $k = 374$ ($\varepsilon = 0{,}9994$)

l	l^*	k^*	$\log T(k^*, l^*)$	$\log t(k^*, l^*)$
1	38	256	362,77	362,76
2	38	256	361,72	361,71
10	37	256	354,28	354,18
50	33	256	316,16	316,15
60	32	256	306,63	306,62
70	31	256	297,10	297,08
100	28	256	268,52	268,48
110	27	256	259,00	258,94
120	26	256	249,49	249,41
200	18	256	174,04	173,12
210	16	256	164,58	164,57
220	15	256	155,04	155,03
245	13	256	130,85	130,69
246	7	512	129,94	129,92
247	7	512	128,94	128,93
365	1	128	18,43	15,63
366	1	64	18,31	14,39
367	1	64	18,25	13,09

Як видно з табл. 1, при $s = 9$, $l = 110$ часова складність розглянутої атаки на криптосистему становить не менше ніж 2^{259}, а обсяг потрібного для реалізації атаки матеріалу складає не менше ніж $2^{258{,}94}$. При цьому швидкість передачі інформації в системі є $l/n = 110/512 = 0{,}2148...$, а довжина ключа складає $2ns = 9216$ біт. В той же час, згідно з табл. 2, майже таку ж саму стійкість відносно розглянутої атаки можна отримати, вважаючи $s = 10$, $l = 600$; при цьому швидкість передачі складає $l/n = 600/1024 = 0{,}5859...$, а довжина ключа збільшується до $2ns = 20480$ біт.

Таблиця 2

Результати виконання алгоритму 1 при $\delta = 10^{-8}$, $s = 10$, $n = 1024$, $k = 827$ ($\varepsilon = 0{,}9986$)

l	l^*	k^*	$\log T(k^*, l^*)$	$\log t(k^*, l^*)$
1	90	256	917,81	917,74
2	90	256	916,67	916,52
10	89	256	907,91	907,85
50	85	256	864,31	863,40
70	82	256	842,28	842,28
100	79	256	808,96	808,94
160	72	256	743,37	743,36
200	68	256	698,93	698,91
260	61	256	633,33	633,33
300	57	256	588,90	588,88
370	49	256	512,18	512,18
420	44	256	456,68	456,61
500	35	256	368,80	368,79
560	29	256	303,01	302,09
600	24	256	258,73	258,72
640	20	256	214,45	214,25
700	13	256	148,63	148,62
720	11	256	126,40	126,37
780	4	256	60,65	60,65
790	3	256	49,49	49,49
800	2	256	38,32	38,31
810	1	256	27,10	27,09
812	1	256	24,71	24,64
813	1	128	23,55	23,41
820	1	64	20,15	13,97

Зауважимо, що в обох випадках ймовірність правильного прийому повідомлень законним отримувачем криптосистеми є не менше ніж $1-10^{-8}$. При цьому застосування швидких алгоритмів кодування та декодування кодів УРС зі складністю $O(2^s s^2)$ операцій в полі F [9]) дозволяє отримувати швидкі програмні реалізації розглянутих криптосистем.

5. Порівняння з криптосистемою LPN-C

Розглянемо окрему версію криптосистеми LPN-C [8], яка будується на основі коду УРС над тим самим полем F, що й досліджена вище (рандомізована симетрична) криптосистема Мак-Еліса.

Зазначена криптосистема LPN-C залежить від параметрів $l_1, l_2, n_1 \in \mathbf{N}$, $\varepsilon \in (0,1)$, де $l_1 \le n_1 \le 2^s$, і визначається за допомогою рівняння шифрування

$$\tilde{E}(m) = (mG_1 \oplus rG_2 \oplus \xi, r), \tag{14}$$

де $m \in F^{l_1}$ – відкритий текст, $\tilde{E}(m)$ – шифрований текст, G_1 – твірна матриця коду УРС довжини n_1 та вимірності l_1 над полем F (яка є загальнодоступною), G_2 – $l_2 \times n_1$-матриця над цим полем, що є секретним ключем, а r та $\xi = (\xi_1, \ldots, \xi_n)$ – незалежні випадкові вектори, де вектор r має рівномірний розподіл ймовірностей на множині F^{l_2}, а координати вектора ξ є незалежними випадковими величинами, розподіленими за законом (2).

Для зашифрування кожного відкритого тексту m вектори r та ξ генеруються незалежно від решти даних так, як це робиться у рандомізованій криптосистемі Мак-Еліса. Для розшифрування повідомлення (14) на ключі G_2 отримувач, знаючи r, обчислює вектор $mG_1 \oplus \xi$, за яким відновлює відкритий текст m, використовуючи швидкий алгоритм декодування коду УРС з відомою твірною матрицею G_1 [11]. Таким чином, на відміну від розглянутої вище криптосистеми Мак-Еліса, де матриця $\begin{pmatrix} G_1 \\ G_2 \end{pmatrix}$ є невідомою твірною матрицею коду УРС, в LPN-C матриця G_1 є загальнодоступною, а матриця G_2 генерується випадково рівноймовірно та відіграє роль секретного ключа. При цьому, на відміну від криптосистеми Мак-Еліса, для забезпечення можливості розшифрування повідомлень в LPN-C у складі шифротексту передається випадковий вектор r.

Зауважимо також, що параметр ε вибирається, виходячи з вимоги до ймовірності правильного відновлення відкритого тексту законним отримувачем. Зокрема, на підставі твердження 1 за умови $l_1 < n_1 - \sqrt{2n_1 \ln(\delta^{-1})}$ значення $\varepsilon = 1 - \frac{1}{1-2^{-s}}\left(\frac{1}{2} - \frac{l_1}{2n_1} - \sqrt{\frac{\ln(\delta^{-1})}{2n_1}}\right)$ забезпечує відновлення відкритого тексту за шифрованим із ймовірністю не менше $1-\delta$.

На криптосистему LPN-C можна здійснити атаку, аналогічну розглянутій вище атаці на криптосистему Мак-Еліса, зашифровуючи t_1 разів повідомлення $m = 0$ та формуючи n_1 систем лінійних рівнянь зі спотвореними правими частинами над полем F відносно стовпців матриці G_2. Кількість невідомих у кожній системі рівнянь дорівнює l_2, а спотворення у їх правих частинах розподілені за тим самим законом, що й координати випадкового вектора ξ (див. формулу (2)). Отже, для оцінювання ефективності такої атаки можна використовувати наступний алгоритм, аналогічний алгоритму 1.

Алгоритм 2.

Вхідні дані:

– верхня межа δ ймовірності помилкового розшифрування відкритого тексту законним отримувачем, $\delta \in (0,1)$;

– довжина n_1 та вимірність l_1 коду УРС над полем з 2^s елементів, де $s \geq 2$, $l_1 < n_1 - \sqrt{2n_1 \ln(\delta^{-1})}$, $n_1 \leq 2^s$;

– число l_2 рядків матриці G_2.

1. Покласти $\varepsilon = 1 - \dfrac{1}{1-2^{-s}}\left(\dfrac{1}{2} - \dfrac{l_1}{2n_1} - \sqrt{\dfrac{\ln(\delta^{-1})}{2n_1}}\right)$.

2. Для будь-яких $l' \in \overline{1, l_2}$ та $k' = 2, 4, 8, 16, \ldots$, що задовольняють умові

$$\log(2\Delta_1(k')^{-1} l' s \ln 2) \leq s(l_2 - l')(\log k')^{-1},$$

де $\Delta_1(k') = (2^s - 1)\varepsilon^{2k'}$, обчислити

$$T_1(k', l') = (m_1(k', l'))^{\frac{1}{\theta}} k' 2^{\frac{s(l_2 - l')}{\theta}} + s(m_1(k', l') + sl'2^{sl'}) + 2^{s(l'+1)},$$

де $\theta = 1 + \log k'$, $m_1(k', l') = 2\Delta_1(k')^{-1} l' s \ln 2$,

3. Обрати k^* та $l^* \in \overline{1, l_2}$ такі, що $T_1(k^*, l^*) = \min\{T_1(k', l')\}$, де мінімум береться за всіма зазначеними вище парами (k', l').

Результат:

– значення k^* та l^* (останнє з яких дорівнює кількості елементів довільного фіксованого стовпця матриці G_2, які відновлюються за допомогою атаки);

– середня часова складність атаки $T_1(k^*, l^*)$;

– обсяг матеріалу $t_1(k^*, l^*) = k^* 2^{\frac{s(l_2 - l^*)}{\theta}} (2l^* s \ln 2)^{\frac{1}{\theta}} \Delta_1(k^*)^{-\frac{1}{\theta}}$, потрібного для успішної реалізації атаки.

Зауважимо, що середню часову складність відновлення всієї матриці G_2 за допомогою наведеної атаки можна оцінити за формулою $T_1^{(\text{tot})}(k^*, l^*) = n_1 \lceil l_2 / l^* \rceil T_1(k^*, l^*)$; при цьому обсяг матеріалу, потрібний для відновлення цієї матриці, співпадає з $t_1(k^*, l^*)$.

Використовуючи алгоритми 1 і 2, порівняємо розглянуті криптосистеми за довжиною ключа при заданій нижній межі стійкості відносно наведеної атаки, вважаючи, що в обох випадках (як криптосистеми Мак-Еліса, так і криптосистеми LPN-C) зашифровуються відкриті тексти однакової довжини $l = l_1$.

Розглянемо, наприклад, рандомізовану симетричну криптосистему Мак-Еліса з параметрами $l = 110$, $k = 374$, $n = 512$, $\varepsilon = 0{,}9986$ (де $s = 9$, $\delta = 10^{-8}$), яка забезпечує стійкість на рівні $T(k^*, l^*) = 2^{259}$ (див. табл. 1). Вважаючи $l_1 = l$, переберемо всі значення n_1, що задовольняють умові $l_1 < n_1 - \sqrt{2n_1 \ln(\delta^{-1})}$, $n_1 \leq 2^s$, для кожного з яких переберемо усі значення $l_2 = 2, 3, \ldots$, поки не знайдемо найменше $l_2 = l_2(n_1)$, для якого повна середня часова складність $T_1^{(\text{tot})}(k^*, l^*)$ атаки на криптосистему LPN-C з параметрами l_1, n_1 та l_2 (при тих самих s та δ) є не менше ніж 2^{259}. Для кожної пари (n_1, l_2) позначимо $d(n_1, l_2) = sn_1 l_2$ та $\rho(n_1, l_2) = l_1/(n_1 + l_2)$ довжину ключа (у бітах) та швидкість передачі інформації за допомогою криптосистеми LPN-C. Нарешті, визначимо $n_1^{(\text{opt})}$, виходячи з умови $d(n_1^{(\text{opt})}, l_2(n_1^{(\text{opt})})) = \min\limits_{n_1}\{d(n_1, l_2(n_1))\}$. Тоді криптосистема LPN-C з параметрами l_1, $n_1^{(\text{opt})}$, $l_2(n_1^{(\text{opt})})$ має найменшу довжину ключа серед усіх подібних криптосистем з такою ж довжи-

ною відкритого тексту, які забезпечують стійкість відносно розглянутої атаки на рівні $T_1^{(\mathrm{tot})}(k^*,l^*) \geq 2^{259}$.

Результати розрахунків показують (табл. 3, 4), що при $s=9$, $l_1=110$ значення $n_1^{(\mathrm{opt})}$ та $l_2(n_1^{(\mathrm{opt})})$ дорівнюють 219 та 300 відповідно. Отже, при довжині відкритого тексту $l_1=110$ найменша довжина ключа криптосистеми LPN-C, що забезпечує стійкість на рівні 2^{259}, складає 591300 біт (табл. 3). При цьому для забезпечення такої ж самої стійкості за допомогою криптосистеми Мак-Еліса (табл. 1) достатньо використовувати помітно коротший ключ довжини $2ns=9216$ біт. Крім того, обидві криптосистеми мають близькі швидкості передачі, що дорівнюють приблизно $0{,}21$.

Аналогічні результати отримаємо при $s=10$, $l_1=600$: тут значення $n_1^{(\mathrm{opt})}$ та $l_2(n_1^{(\mathrm{opt})})$ дорівнюють 844 та 257 відповідно. При цьому найменша довжина ключа криптосистеми LPN-C, потрібна для забезпечення її стійкості на рівні $2^{258{,}73}$, складає 2253480 біт (табл. 4), в той час як довжина ключа відповідної криптосистеми Мак-Еліса дорівнює 20480 бітам (табл. 2).

Таблиця 3

Значення параметрів, що характеризують стійкість та практичність криптосистем LPN-C

при $s=9$, $l_1=110$, $n_1=219$ ($\delta=10^{-8}$)

l_2	l^*	k^*	$\log t_1(k^*,l^*)$	$\log T_1(k^*,l^*)$	$\log T_1^{(\mathrm{tot})}(k^*,l^*)$	$\rho(n_1,l_2)$	$d(n_1,l_2)$
2	1	2	2,95	18,21	36,17	0,49	3942
5	1	16	10,54	18,21	37,49	0,49	9855
20	2	128	28,77	29,24	47,66	0,46	39420
50	5	256	56,34	56,78	75,06	0,40	98550
80	7	512	81,07	81,07	93,86	0,36	157680
110	10	512	105,42	105,46	120,73	0,33	216810
150	14	512	137,87	138,39	156,99	0,29	295650
190	16	1024	164,28	164,29	176,05	0,26	374490
200	17	1024	171,66	171,66	184,60	0,26	394200
240	21	1024	201,14	201,71	220,52	0,23	473040
290	25	1024	238,80	239,03	256,72	0,21	571590
299	25	1024	246,16	246,16	257,71	0,21	589329
300	26	1024	246,17	246,81	265,76	0,21	591300

Таблиця 4

Значення параметрів, що характеризують стійкість та практичність криптосистем LPN-C

при $s=10$, $l_1=600$, $n_1=844$ ($\delta=10^{-8}$)

l_2	l^*	k^*	$\log t_1(k^*,l^*)$	$\log T_1(k^*,l^*)$	$\log T_1^{(\mathrm{tot})}(k^*,l^*)$	$\rho(n_1,l_2)$	$d(n_1,l_2)$
2	1	4	3,42	20,13	40,97	0,70	16880
5	1	16	11,13	20,13	42,30	0,70	42200
20	2	128	30,73	31,51	53,41	0,69	168800
80	7	512	87,71	87,72	104,22	0,64	675200
110	10	512	114,76	114,86	134,24	0,62	928400
130	11	1024	128,93	128,94	142,25	0,61	1097200
170	15	1024	161,70	162,51	184,66	0,59	1434800
200	17	1024	187,17	187,19	204,80	0,57	1688000
220	19	1024	203,54	203,86	224,87	0,56	1856800
240	20	1024	220,82	220,83	235,30	0,55	2025600
260	22	1024	237,20	237,23	255,03	0,54	2194400
266	22	1024	242,65	242,66	256,14	0,54	2245040
267	23	1024	242,66	243,26	265,04	0,54	2253480

Висновки

1. Досліджена рандомізована кодова криптосистема є симетричним аналогом окремого випадку рандомізованої (асиметричної) криптосистеми Мак-Еліса [7] та являє собою удосконалену версію симетричної кодової криптосистеми LPN-C [8], що будується на основі кодів УРС. На відміну від LPN-C (див. формулу (14)), де матриця G_1 вигляду (1) є загальнодоступною, а матриця G_2 генерується випадково рівноймовірно та відіграє роль секретного ключа, у рандомізованій симетричній криптосистемі Мак-Еліса матриця $\begin{pmatrix} G_1 \\ G_2 \end{pmatrix}$ є невідомою твірною матрицею коду УРС, що утворює секретний ключ. При цьому, на відміну від криптосистеми Мак-Еліса, для забезпечення можливості розшифрування повідомлень в LPN-C у складі шифротексту передається випадковий вектор r.

2. Стійкість рандомізованої симетричної криптосистеми Мак-Еліса відносно розглянутої атаки з підібраним відкритим текстом базується на складності відновлення невідомого коду УРС за набором його спотворених кодових слів. На сьогодні ця задача є обчислювально складною, а відомий метод її розв'язання полягає у складанні та розв'язанні систем лінійних рівнянь зі спотвореними правими частинами вигляду (8) над полем визначення коду УРС. Зауважимо, що оскільки секретний ключ (тобто код УРС) є невідомим, на рандомізовану симетричну криптосистему є незастосовними атаки [12, 13], відомі для асиметричних криптосистем, що будуються на основі кодів УРС.

3. В порівнянні з LPN-C, рандомізована симетрична криптосистема Мак-Еліса характеризується помітно меншою довжиною ключа при заданій стійкості (та однаковій довжині вхідних повідомлень). Зокрема, при $s = 9$, $l_1 = 110$ (див. табл. 1, 3) для забезпечення стійкості на рівні 2^{259} відносно розглянутої атаки за допомогою криптосистеми Мак-Еліса потрібен ключ, довжина якого є понад у 64 рази менше довжини секретного ключа криптосистеми LPN-C, а при $s = 10$, $l_1 = 600$ (див. табл. 2, 4) скорочення довжини ключа криптосистеми Мак-Еліса становить понад 110 разів.

4. На сьогодні залишається відкритим запитання про те, чи є досліджена криптосистема CPA-стійкою (відомо [8], що для LPN-C відповідь на це запитання є позитивною). Зокрема, важливо з'ясувати, чи дозволяють структурні особливості кодів УРС зменшити складність алгоритмів їх відновлення за наборами спотворених кодових слів у порівнянні з алгоритмами відновлення довільних лінійних блокових кодів.

Список літератури:

1. McEliece R.J. A public-key cryptosystem based on algebraic coding theory // Prog. Rep., Jet Prop. Lab., California Inst. Technol, 1978. P. 114 – 116.
2. Jordan J.P. A variant of public-key cryptosystem based on Goppa codes // Sigact news, 1983. P. 61 – 66.
3. Rao T.R.N. Cryptosystems using algebraic codes // Int. Conf on Computer Systems & Signal Processing, 1984.
4. Rao T.R.N. Private-key algebraic code encryption / T.R.N. Rao, K.H. Nam // IEEE Trans. on Inform Theory, 1987. P. 829 – 833.
5. Sobhi Afshar A.A. Efficient secure channel coding based on quasy-ciclic low-density parity-check codes / A.A. Sobhi Afshar, T. Eghlidos, M.R. Aref // Journal of IET-Communications, 2009. P. 279 – 292.
6. Hooshmand R. Improving the Rao-Nam secret key cryptosystem using regular EDF-QC-LDPC codes / R. Hooshmand, T. Eghlidos, M.R. Aref // ISC Journal of Information sequrity, 2012. P. 3 – 14.
7. Nojima R. Semantic security for the McElice cryptosystem without random oracles / R. Nojima, H. Imai, K. Kobara, K. Morozov // Des. Codes Cryptography, 2008. P. 289 – 305.
8. Gilbert H. How to Encrypt with the LPN Problem / H. Gilbert, J.B. Mattew, M.J.B. Robshaw, Y. Seurin // ICALP (2), Proceedings, Springer Verlag, 2008. P. 679- 690.
9. Федоренко С.В. Методы быстрого декодирования линейных блоковых кодов. С.-Петербург : ГУАПб, 2008. 199 с.
10. Niederreiter N. Knapsack-type cryptosystems and algebraic coding theory // Problems of Control and Information Theory, 1986. P. 159 – 166.

11. Berger T. How to mask the structure of codes for a cryptographic use / T. Berger, P. Loidreau // Designs, Codes and Cryptography, 2005. P. 63.

12. Сидельников В.М. О системе шифрования, построенной на основе обобщенных кодов Рида-Соломона / В.М. Сидельников, С.О. Шестаков // Дискретная математика, 1992. Т. 4. Вып. 3. С. 57 – 63.

13. Wieschebrink Ch. Cryptanalysis of the Niederreiters public key scheme based on GRS sub-codes // Post-Quantum Cryptography, 2010 Proceedings. Springer Verlag, 2010. P. 61 – 72.

14. Мак-Вильямс Ф.Дж. Теория кодов, исправляющих ошибки ; пер. с англ. / Ф.Дж. Мак-Вильямс, Н. Дж. А. Слоэн. Москва : Связь, 1979. 743 с.

15. Hoeffding W. Probability inequalities for sums of bounded random variables // J. Amer. Statist. Assoc, 1963. Vol. 58. № 301. P. 13 – 30.

16. Алексейчук А. Н. Метод восстановления систематических линейных кодов по наборам искаженных кодовых слов / А.Н. Алексейчук, А.Ю. Грязнухин // Прикладная радиоэлектроника. 2013. Т. 12. № 2. С. 313 – 318.

17. Zhang B. Fast correlation attacks over extension fields, large-unit linear approximation and cryptanalysis of SNOW 2.0 / B. Zhang, C. Xu, W. // Meier–Cryptology ePrint Archive, 2016/311. http://eprint.iacr.org/2016/311.

18. Wagner D. A generalized birthday problem // Advances in Cryptology – CRYPTO'02, Proceedings. Springer Verlag, 2002. P. 288 – 303.

Інститут спеціального зв'язку та захисту інформації
Національного технічного університету України "КПІ"
імені Ігоря Сікорського

Надійшла до редколегії 11.01.2020

УДК 621.391.15:519.7 **DOI:10.30837/rt.2020.1.200.04**

А.В. БЕССАЛОВ

АЛГОРИТМЫ И ОЦЕНКИ СЛОЖНОСТИ ВЫЧИСЛЕНИЙ 3- И 5-ИЗОГЕНИЙ СУПЕРСИНГУЛЯРНЫХ КРИВЫХ ЭДВАРДСА

Введение

Одной из известных перспектив постквантовой криптографии (PQC) являются алгоритмы, построенные на изогениях суперсингулярных эллиптических кривых (*supersingular isogenies Diffi-Hellman* – SIDH[1]). Сегодня интерес к изогениям связывается с наименьшей длиной ключа в предлагаемых алгоритмах в сравнении с другими известными кандидатами PQC.

Кривые Эдвардса с одним параметром, определенные в работе [2], имеют привлекательные для криптографии преимущества: максимальная скорость экспоненцирования точки, универсальность закона сложения точек, аффинные координаты нейтрального элемента группы точек, повышенная безопасность в отношении атак побочного канала. Введение второго параметра кривой в работе [3] расширило класс *s* кривых Эдвардса и породило кривые с новыми интересными для криптографии свойствами.

Наряду с отмеченными свойствами кривые в форме Эдвардса оказались наиболее быстрой технологией при вычислении изогений. В работе [4] приводятся экспериментальные оценки скорости вычисления изогений на кривых Эдвардса, более чем втрое превышающие показатели для кривых в форме Вейерштрасса. Так как процедура нахождения изогенной точки обычно включает скалярное произведение точки, общий выигрыш в быстродействии алгоритмов на кривых Эдвардса может стать значительным.

Известные реализации алгоритма SIDH используют в основном кривые в форме Вейерштрасса и Монтгомери. Попытка программной реализации алгоритма SIDH с помощью 2- и 3-изогений кривых в форме Эдвардса столкнулась с проблемой наличия четырех особых точек на бесконечности 2-го и 4-го порядков в классе квадратичных кривых Эдвардса. Эти точки имеются во всех подгруппах четных порядков, число которых близко половине всех подгрупп кривой. Чтобы обойти эту проблему, предлагается использовать изогении минимальных нечетных степеней 3 и 5 для точек нечетного порядка кривой. Хотя переход от 2- к 5-изогении усложняет алгоритм вычислений, подобная гладкая реализация алгоритма представляется перспективной.

Среди многочисленных работ по этой проблематике выделим статьи [4 – 6], в которых впервые получены формулы изогений для кривых в форме Эдвардса. Наш анализ опирается на их результаты с использованием свойств суперсингулярных кривых [7, 8]. С целью адаптации определений для арифметики изогений кривых Эдвардса и кривых в форме Вейерштрасса мы используем модифицированный закон сложения точек [9, 10].

В данной статье построены алгоритмы и получены оценки сложности вычислений 3- и 5-изогений двух классов кривых Эдвардса. В разд. 1 дается краткий обзор свойств трех классов кривых Эдвардса согласно новой классификации. В разд. 2 даны определения и доказывается формула для изогений нечетных степеней, выраженная рациональными функциями одной переменной. В разд. 3, 4 построены алгоритмы и получены оценки сложности вычисления 3- и 5-изогений в проективных координатах. В разд. 5 приводятся алгоритмы вычисления 3- и 5-изогений. Наконец, в разд. 6 определены условия существования 3- и 5-изогений и требования к параметрам кривой для алгоритма SIDH [1].

1. Классы кривых в обобщенной форме Эдвардса

Эллиптическая кривая *в обобщенной форме Эдвардса* [9] определяется уравнением

$$E_{a,d}: \quad x^2 + ay^2 = 1 + dx^2y^2,\ a,d \in F_p^*,\ d \neq 1,\ a \neq d,\ p \neq 2 \tag{1}$$

В отличие от уравнения этой кривой в [3] здесь параметр a умножаем на y^2 вместо x^2. Если квадратичный характер $\chi(ad) = -1$, кривая (1) изоморфна *полной кривой* Эдвардса [1] с одним параметром d

$$E_d: \quad x^2 + y^2 = 1 + dx^2y^2,\ \chi(d) = -1,\ d \neq 0,1, \tag{2}$$

В случае $\chi(ad) = 1$, и $\chi(a) = \chi(d) = 1$ имеет место изоморфизм кривой (1) с *квадратичной кривой Эдвардса* [9]:

$$E_d: \quad x^2 + y^2 = 1 + dx^2y^2,\ \chi(d) = 1,\ d \neq 0,1, \tag{3}$$

имеющей, в отличие от (2), параметр d, определенный как квадрат. Это отличие ведет к кардинально различным свойствам кривых (2) и (3) [9], которые резюмируются ниже. Несмотря на это, в статье [3] эти классы кривых объединены общим термином *кривые Эдвардса.*

Кривые с различными значениями a, d изоморфны, если они имеют одинаковый j-инвариант, равный для кривой (1)

$$j(a,d) = \frac{16(a^2 + d^2 + 14ad)}{ad(a-d)^4}.$$

Этот параметр является базовым в структуре графа изогенных кривых, вершины которого задают классы изоморфных кривых.

В работе [9] мы предложили поменять местами x и y координаты в форме кривой Эдвардса. Тогда модифицированный универсальный закон сложения точек кривой (1) имеет вид

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1x_2 - ay_1y_2}{(1 - dx_1x_2y_1y_2)}, \frac{x_1y_2 + x_2y_1}{(1 + dx_1x_2y_1y_2)} \right). \tag{4}$$

При совпадении двух точек получим из (4) закон удвоения точек

$$2(x_1, y_1) = \left(\frac{x_1^2 - ay_1^2}{(1 - dx_1^2y_1^2)}, \frac{2x_1y_1}{(1 + dx_1^2y_1^2)} \right). \tag{5}$$

Использование модифицированных законов (4), (5) позволяет сохранить общепринятую горизонтальную симметрию (относительно оси X) обратных точек. Определяя обратную точку как $-P = (x_1, -y_1)$, получим согласно (4) координаты нейтрального элемента группы точек $O = (x_1, y_1) + (x_1, -y_1) = (1, 0)$. Кроме нейтрального элемента О на оси X всегда лежит точка $D_0 = (-1, 0)$ второго порядка, для которой в соответствии с (5) $2D_0 = (1, 0) = O$. В зависимости от свойств параметров a и d можно получить еще две особые точки 2-го порядка и две или более точек 4-го порядка. Как следует из (1), на оси y могут лежать точки $\pm F_0 = \left(0, \pm 1/\sqrt{a}\right)$ 4-го порядка, для которых $\pm 2F_0 = D_0 = (-1, 0)$. Эти точки существуют над простым полем F_p, если параметр a является квадратом (квадратичным вычетом).

Из уравнения (1) определим квадраты

$$x^2 = \frac{1-ay^2}{1-dy^2}\ , \qquad y^2 = \frac{1-x^2}{a-dx^2}\ ,$$

порождающие особые точки на бесконечности (знак "∞"мы ставим при делении на 0):

$$D_{1,2} = \left(\pm\sqrt{\frac{a}{d}}, \infty\right), \pm F_{11} = \left(\infty, \pm\frac{1}{\sqrt{d}}\right). \tag{6}$$

Они возникают в случаях $\chi(ad) = 1$ и $\chi(d) = 1$ соответственно. Это, например, всегда выполняется в расширении поля.

В зависимости от свойств параметров a и d кривые в обобщенной форме (1) разбиваются на три непересекающиеся (неизоморфных) класса [9, 10]:

- *полные кривые Эдвардса* с условием С1: $\chi(ad) = -1$;
- *скрученные кривые Эдвардса* с условиями С2.1: $\chi(a) = \chi(d) = -1$;
- *квадратичные кривые Эдвардса* с условиями С2.2: $\chi(a) = \chi(d) = 1$.

Основные свойства этих классов кривых [9]:

1. В отношении точек 2-го порядка первый класс полных кривых Эдвардса над простым полем является классом *циклических* кривых (с одной точкой 2-го порядка), скрученные же и квадратичные кривые Эдвардса образуют классы *нециклических* кривых (по три точки 2-го порядка). Максимальный порядок точек кривых последних классов не превышает $N_E / 2$.

2. Класс полных кривых Эдвардса не содержит особых точек.

3. Скрученные кривые Эдвардса содержат лишь две особых точки 2-го порядка $D_{1,2} = \left(\pm\sqrt{\frac{a}{d}}, \infty\right)$, а квадратичные кривые Эдвардса, кроме них – еще две особые точки 4-го порядка $\pm F_{11} = \left(\infty, \pm\frac{1}{\sqrt{d}}\right)$.

4. Скрученные и квадратичные кривые Эдвардса образуют пары квадратичного кручения на основе преобразования параметров: $a = ca,\ d = cd,\ \chi(c) = -1$.

5. В классах скрученных и квадратичных кривых Эдвардса замена $a \leftrightarrow d$ дает изоморфизм $E_{a,d} \sim E_{d,a}$.

6. Полные и квадратичные кривые Эдвардса изоморфны кривым с параметром $a = 1$: $E_{a,d} \sim E_{1.,d/a}$ Введение нового параметра a в уравнение кривой (1) оправдано лишь для класса скрученных кривых Эдвардса.

7. Скрученные кривые Эдвардса при $p \equiv 1 \bmod 4$ не имеют точек 4-го порядка.

Подчеркнем, что в расширении F_{p^2} простого поля F_p все три класса кривых Эдвардса, заданные над простым полем, приобретают свойства квадратичных кривых (3). Поэтому далее мы рассматриваем в основном кривые E_d вида (2) и (3) с одним параметром.

2. Изогении нечетных степеней кривых Эдвардса

Изогения эллиптической кривой $E(K)$ над полем K в кривую $E'(K)$ есть гомоморфизм $\phi : E(\bar{K}) \to E'(\bar{K})$, задаваемый рациональными функциями. Это значит, что для всех $P, Q \in E(K)$ $\phi(P+Q) = \phi(P) + \phi(Q)$ и существует рациональная функция [11]

$$\phi(x, y) = \left(\frac{p(x)}{q(x)}, y\frac{f(x)}{g(x)}\right) = (x', y'), \tag{7}$$

отображающая точки кривой E в точки кривой E'. Степенью изогении называется максимальная из степеней $l = \deg\phi(x,y) = \max\{\deg p(x), \deg q(x)\}$, а ее ядром $\ker\phi = G$ – подгруппа $G \subseteq E$, точки которой отображаются функцией $\phi(x,y)$ в нейтральный элемент O группы E'. Степень сепарабельной изогении равна порядку l ее ядра. Изогения сжимает точки кривой E в l раз (l точек кривой E отображаются в одну точку кривой E'). При $G = O$ изогения становится изоморфизмом со степенью 1.

В основе построения изогений нечетных простых степеней для кривых Эдвардса лежит теорема 2 [4]. Сформулируем ее с учетом модификации (4) закона сложения точек кривой (1) при $a = 1$.

Теорема 2 [4]. Пусть $G = \{(1,0), \pm Q_1, \pm Q_2, ..., \pm Q_s\}$ подгруппа нечетного порядка $l = 2s+1$ точек $\pm Q_i = (\alpha_i, \pm\beta_i)$ кривой E_d.

Определим

$$\phi(P) = \left(\prod_{Q \in G} \frac{x_{P+Q}}{x_Q}, \prod_{Q \in G} \frac{y_{P+Q}}{x_Q} \right)$$

Тогда $\phi(x,y)$ есть l-изогения с ядром G из кривой E_d в кривую $E_{d'}$ с параметром $d' = A^8 d^l$, $A = \prod_{i=1}^{s} \alpha_i$, и отображающей функцией

$$\phi(x,y) = \left(\frac{x}{A^2} \prod_{i=1}^{s} \frac{(\alpha_i x)^2 - (\beta_i y)^2}{1 - (d\alpha_i\beta_i xy)^2}, \frac{y}{A^2} \prod_{i=1}^{s} \frac{(\alpha_i y)^2 - (\beta_i x)^2}{1 - (d\alpha_i\beta_i xy)^2} \right). \quad (8)$$

Доказательство ее дано в [4]. Важным ее следствием является то, что изогенные кривые лежат в тех же классах, что и кривые E_d (т.е. полные кривые Эдвардса отображаются в полные, а квадратичные кривые – в квадратичные). Это существенно отличает изогении нечетных степеней от 2-изогений (для них полные кривые Эдвардса отображаются в квадратичные).

Формула (8) для функции $\phi(x,y)$ прямо следует из определения $\phi(P)$ в формулировке теоремы, закона (4) сложения точек $(x_P, y_P) = (x,y)$ с точками $\pm Q_i = (\alpha_i, \pm\beta_i)$, при этом для пар координат имеем:

$$\frac{x_{P+Q_i}}{x_{Q_i}} \frac{x_{P-Q_i}}{x_{-Q_i}} = \frac{1}{\alpha_i^2} \frac{(\alpha_i x)^2 - (\beta_i y)^2}{1 - (d\alpha_i\beta_i xy)^2}, \qquad \frac{y_{P+Q_i}}{x_{Q_i}} \frac{y_{P-Q_i}}{x_{-Q_i}} = \frac{1}{\alpha_i^2} \frac{(\beta_i x)^2 - (\alpha_i y)^2}{1 - (d\alpha_i\beta_i xy)^2}.$$

Сомножители x и y перед произведениями в координатах функции $\phi(x,y)$ учитывают нейтральный элемент $O = (1_i, 0)$ ядра изогении. Из (8) очевидно выполнение свойства $\phi(1,0) = (1,0)$, т.е. нейтральный элемент отображается в себя. Для всех точек ядра также справедливо $\phi(\pm Q_i = (\alpha_i, \pm\beta_i)) = (1,0)$.

Отображение (8) можно привести к виду (7), тогда определение степени изогении становится очевидным. Из (2) и (3) выразим $y^2 = (1-x^2)/(1-dx^2)$ и подставим это значение в (8). Тогда в числителе первой координаты (8)

$$\alpha_i^2 x^2 - \beta_i^2 y^2 = \alpha_i^2 x^2 - \beta_i^2 \frac{1-x^2}{1-dx^2} = \frac{(\alpha_i^2 + \beta_i^2)x^2 - \beta_i^2 - d\alpha_i^2 x^4}{1-dx^2} = \frac{(1 + d\alpha_i^2\beta_i^2)x^2 - \beta_i^2 - d\alpha_i^2 x^4}{1-dx^2} =$$

$$= \frac{x^2 - \beta_i^2 - d(\alpha_i^2 x^4 - \alpha_i^2\beta_i^2 x^2)}{1-dx^2} = \frac{(x^2 - \beta_i^2)(1 - d\alpha_i^2 x^2)}{1-dx^2}.$$

Аналогично преобразуем знаменатель первой координаты (8)

$$1-(d\alpha_i\beta_i xy)^2 = 1-d^2\alpha_i^{\,2}\beta_i^{\,2}x^2\,\frac{1-x^2}{1-dx^2} = \frac{1-dx^2-d^2\alpha_i^{\,2}\beta_i^{\,2}x^2+d^2\alpha_i^{\,2}\beta_i^{\,2}x^4}{1-dx^2} = \frac{1-d(\alpha_i^{\,2}+\beta_i^{\,2})x^2+d^2\alpha_i^{\,2}\beta_i^{\,2}x^4}{1-dx^2} =$$

$$= \frac{(1-d\alpha_i^{\,2}x^2)(1-d\beta_i^{\,2}x^2)}{1-dx^2}.$$

После сокращения общих сомножителей получаем

$$\frac{(\alpha_i x)^2-(\beta_i y)^2}{1-(d\alpha_i\beta_i xy)^2} = \frac{x^2-\beta_i^{\,2}}{1-d\beta_i^{\,2}x^2}.$$

Аналогичные выкладки можно провести со второй координатой (8). В итоге функцию (8) можно записать в эквивалентной форме

$$\phi(x,y) = \left(\frac{x}{A^2}\prod_{i=1}^{s}\frac{x^2-\beta_i^{\,2}}{1-d\beta_i^{\,2}x^2}, \frac{-y}{A^2}\prod_{i=1}^{s}\frac{x^2-\alpha_i^{\,2}}{1-d\alpha_i^{\,2}x^2}\right), \tag{9}$$

отвечающей классическому виду (7). Эта форма приведена в работе [4] без доказательства. Очевидным ее преимуществом перед (8) является простота и минимальная вычислительная сложность. Кроме этого, степень изогении как максимальная степень полинома $p(x)$ в (7) сразу определяется как $l = 2s+1.$

Рассмотрим пример 3-изогении полной суперсингулярной кривой Эдвардса.

Пример 1. Пусть E_d – полная суперсингулярная кривая Эдвардса (2) при $p = 23, d = -1.$ с j-инвариантом $j = 12^3$ [6]. Она имеет порядок $N_E = 24$ и содержит точки $(\pm1,0), (0,\pm1), (\pm2,\pm2), (\pm3,\pm6), (\pm6,\pm3), (\pm9,\pm10), (\pm10,\pm9)$. Обозначим $P_1 = (3,6)$, $P_2 = (6,3)$ – точки 24-го порядка кривой. $P_3 = (2,2)$ – точка 8-го порядка, $P_4 = (9,10)$ – точка 12-го порядка, $P_3 = (10,9)$ – точка 6-го порядка и $Q = (-10,9)$ – точка 3-го порядка, и для любой точки $P = (x_1, y_1)$ $P^* = P + D_0 = (-x_1, -y_1)$. Заметим, что сумма точек 2-го и 3-го порядка дает точку 6-го порядка, поэтому x-координаты точек 3-го и 6-го порядков имеют обратные знаки. Итак, ядро 3-изогении содержит точки $(1,0)$, $(-10,\pm9)$, т.е. $\alpha = -10$, $\beta = 9$, $A^2 = 8,$ и согласно теореме 2 [4] параметр изогенной кривой $E_{d'}$ равен, $d' = -8^4 = -2$. Эта суперсингулярная кривая с j-инвариантом $j = 3$, кроме точек $O = (1,0)$ $D_0 = (-1,0)$, $\pm F_0 = (0, \pm1)$, имеет точки первого квадранта: $R_1 = (3,5)$ $R_2 = (5,3)$ – точки 24-го порядка кривой. $R_3 = (7,7)$ – точка 8-го порядка, $R_4 = (9,11)$ – точка 6-го порядка и $R_5 = (11,9)$ – точка 12-го порядка и $Q' = (-9,11)$ – точка 3-го порядка. С помощью функции (9)

$$\phi(x,y) = \left(\frac{x}{8}\cdot\frac{x^2-9^2}{1+9^2x^2}, \frac{-y}{8}\frac{x^2-10^2}{1+10^2x^2}\right)$$

получим:

$$\phi(\pm P_1 = (3,\pm6)) = \left(\frac{3}{8}\cdot\frac{3^2-9^2}{1+9^2\cdot3^2}, \frac{\mp6}{8}\frac{3^2-10^2}{1+10^2\cdot3^2}\right) = (-7,\pm7) = \mp R_3^*, \qquad \phi(P_2 = (6,3)) = (7,-7) = -R_3,$$

$$\phi(P_3 = (2,2)) = (7,7) = R_3,$$

$$\phi(P_4 = (9,\pm10)) = (0,\mp1) = \mp F_0,$$

$\phi(P_5 = (10,9)) = (-1,0) = D_0,$

$\phi(\pm Q = (-10,\pm 9)) = (1,0) = O, \phi(O = (1,0)) = (1,0) = O.$

Для преобразования других точек можно использовать свойство функции (9) $\phi(\pm x, \pm y) = (\pm x', \pm y')$ Здесь имеет место отображение «3 в 1» со сжатием E_d в три раза (24 точки кривой E_d отображаются в восемь точек изогенной кривой $E_{d'}{}'$). В частности, восемь точек 24-го порядка вместе с четырьмя точками 8-го порядка отображаются в четыре точки 8-го порядка, четыре точки 12-го порядка вместе с двумя точками 6-го порядка отображаются в две точки 4-го порядка, точки 4-го порядка и 2-го порядков отображаются в точку 2-го порядка, и, наконец, точки ядра отображаются в О. Все преобразования отвечают умножению точек на 3, подобно эндоморфизму $E \to 3E$.

Рассмотрим пример 5-изогении на полной суперсингулярной кривой Эдвардса.

Пример 2. При $p = 19$ и $d = -1$ полная суперсингулярная кривая Эдвардса E_{18} (2) имеет порядок $N_E = 20$ и содержит точки 1-го квадранта: $P_1 = (2,8)$, $P_2 = (4,6)$ – точки 20-го порядка кривой, $P_3 = (8,2)$ – точка 10-го порядка, и $Q_1 = (6,4)$ – точка 5-го порядка. Тогда $Q_2 = 2Q_1 = (-8,-2)$ и ядро 5-изогении содержит точки $\{(1,0),(6,\pm 4),(-8,\pm 2)\}$. Итак, $\alpha_1 = 6, \beta_1 = 4, \alpha_2 = -8, \beta_2 = -2, A = \alpha_1\alpha_2 = 9, A^2 = 5,$ и параметр изогенной суперсингулярной кривой $d' = -5^4 = -2$. Она содержит точки 1-го квадранта: $R_1 = (4,5)$, $R_2 = (7,9)$ – точки 20-го порядка кривой $E_{d'}{}'$,. $R_3 = (5,4)$, $R_4 = (9,7)$ – точки 10-го порядка. 5-изогения (9) здесь имеет вид

$$\phi(x,y) = \left(\frac{x}{5} \cdot \frac{x^2 - 4^2}{1 + 4^2 x^2} \frac{x^2 - 2^2}{1 + 2^2 x^2}, \frac{-y}{5} \cdot \frac{x^2 - 6^2}{1 + 6^2 x^2} \cdot \frac{x^2 - 8^2}{1 + 8^2 x^2} \right).$$

Тогда

$$\phi(P_1 = (2,8)) = \left(\frac{2}{5} \cdot \frac{2^2 - 4^2}{1 + 4^2 2^2} \frac{2^2 - 2^2}{1 + 2^2 2^2}, \frac{-8}{5} \cdot \frac{2^2 - 6^2}{1 + 6^2 2^2} \cdot \frac{2^2 - 8^2}{1 + 8^2 2^2} \right) = (0,1) = F_0$$

$\phi(P_2 = (4,6)) = (0,-1) = -F_0,$

$\phi(P_3 = (8,2)) = (-1,0) = D_0,$

$\phi(\pm Q_1 = (6,\pm 4)) = (1,0) = O, \quad \phi(O = (1,1)) = (1,0) = O.$

Это отображение «5 в 1» преобразует подмножества из пяти точек кривой E_d в одну из четырех точек изогенной кривой 4-го, 2-го порядка или точку O. Здесь функция (9) действует подобно эндоморфизму $E_d \to 5E_d$, снижающему порядки точек порядков, кратных 5, в пять раз.

Важно отметить, что строить изогении составного порядка (к примеру, 15-го) практически бессмысленно. Достаточно построить более простые 3-изогению и 5-изогению и пользоваться свойством их композиции, основанном на гомоморфизме отображения ϕ. Так как подгруппа точек 15-го порядка есть прямая сумма подгрупп простых 3-го и 5-го порядков, т.е. $G_{15} = G_3 \oplus G_5$, то и для соответствующих изогений справедливо $\phi_{15} = \phi_3 \oplus \phi_5$. Это свойство кардинально снижает сложность вычисления изогений составных степеней.

Для построения изогений степеней l^k, $l = 3,5,..,k = 2,3,..,m$ используется очевидное свойство группы: любая циклическая группа точек $< G_k >$ порядка l^k содержит подгруппу

точек $< G_{k-1} >$ порядка l^{k-1} и подгруппу $< G_1 >$ порядка l. Точка порядка l из $< G_k >$ находится скалярным произведением $l^{k-1}G_k$. Тогда, начиная со старшей степени m, можно построить последовательность l-изогений $\{\phi_{m-i}\}$, композиция которых $\phi_{m-t} = \phi_{m-1} \oplus \phi_{m-2} \oplus .. \oplus \phi_{m-t+1}$ дает l^k-изогению при $t = m-k$. Такой алгоритм, выполняемый максимум за m шагов, имеет полиномиальную сложность.

Безопасность алгоритма SIDH [1] требует, чтобы число подгрупп кривой E_d порядка $p+1 = 4 \cdot 3^m \cdot 5^n$ для защиты от квантового компьютера составляло величину более 760 бит. Для эффективного решения этой задачи кривые E_d и $E_{d'}$ рассматриваются над расширением F_{p^2} поля F_p (причем кривая E_d задается над простым полем). Порядок суперсингулярной кривой над расширением F_{p^2} равен $(p+1)^2$, в соответствующей пропорции возрастает число подгрупп кривой (порядка 1,5 КБит). Каждая циклическая подгруппа порядка n суперсингулярной кривой над F_p трансформируется над расширением F_{p^2} в нециклическую подгруппу порядка n^2, содержащую $(n+1)$ циклических подгрупп порядка n. Соответственно, число ядер для 3-изогений равно 4, а для 5-изогений – 6. Нахождение генератора одной из таких подгрупп (или ядра изогении) является одной из сложных задач PQC.

3. Вычисление 3-изогений в проективных координатах

Перспективным решением задачи повышения эффективности вычислений изогений является переход к однокоординатной изогении $(X' : Z')$ [1, 11], тогда как вторая координата точки с точностью до знака при необходимости определяется уравнением изогенной кривой. В этом случае лучшие результаты можно получить с использованием изогении формы (9). Для первой координаты 3-изогении после замены $\beta^2 = (1-\alpha^2)/(1-d\alpha^2)$ имеем:

$$\frac{X'}{Z'} = \frac{x}{\alpha^2} \cdot \frac{x^2 - \beta^2}{1 - d\beta^2 x^2} = \frac{x}{\alpha^2} \cdot \frac{x^2 - \frac{1-\alpha^2}{1-d\alpha^2}}{1 - dx^2 \cdot \frac{1-\alpha^2}{1-d\alpha^2}} = \frac{-x}{\alpha^2} \cdot \frac{x^2 + \alpha^2 - d\alpha^2 x^2 - 1}{d(x^2+\alpha^2) - d\alpha^2 x^2 - 1}$$

Для точек ядра $\pm Q = (\alpha, \pm\beta)$ 3-го порядка из равенства $2Q = -Q$ и формулы (5) легко получить уравнение для полинома деления $2\alpha + 1 - d\alpha^3(2+\alpha) = 0$, откуда $d = (2\alpha+1)/\alpha^3(2+\alpha)$ [11]. Подставляя это значение в последнее равенство, приходим к рациональной функции

$$\frac{X'}{Z'} = x \cdot \frac{x^2 + \alpha^2 + 2\alpha}{x^2 + \alpha^2 + 2\alpha x^2}$$

Важно, что здесь 3-изогения определена лишь *x*-координатами точек P и Q и не зависит от параметра d. В проективных координатах после замены $x \to \frac{X}{Z}$, $\alpha = \frac{X_1}{Z_1}$ получим

$$(X' : Z') = (X(X^2 Z_1^2 + X_1^2 Z^2 + 2X_1 Z_1 Z^2) : Z(X^2 Z_1^2 + X_1^2 Z^2 + 2X_1 Z_1 X^2)). \quad (10)$$

Подобное выражение найдено в работе [11], в которой вместо изогении, определяемой теоремой 2, за основу взята теорема 3 [4]. Эти теоремы дают разные определения для параметра d' изогенной кривой $E_{d'}$. Согласно теореме 2 [4]

$$d' = A^8 d^3, A = \alpha. \tag{11}$$

Определяя здесь параметр $d = (2\alpha + 1)/\alpha^3(2+\alpha)$, в проективных координатах, равенство (11) принимает вид

$$d' = \frac{Z_1}{X_1} \cdot \frac{(2X_1 + Z_1)^3}{(2Z_1 + X_1)^3}. \tag{12}$$

Чтобы избежать инверсии при вычислении параметра d', в работе [11] предложено использовать проективные координаты изоморфной (2) кривой

$$E_{C',D'}: \quad C'(x^2 + y^2) = C' + D'x^2y^2, \quad D' = d'C'.$$

Тогда, согласно (12),

$$D' = Z_1(2X_1 + Z_1)^3 = (2X_1Z_1 + Z_1^2)(4X_1^2 + Z_1^2 + 4X_1Z_1), \tag{13}$$

$$C' = X_1(2Z_1 + X_1)^3 = (2X_1Z_1 + X_1^2)(4Z_1^2 + X_1^2 + 4X_1Z_1). \tag{14}$$

Так как $2X_1Z_1 = (X_1 + Z_1)^2 - X_1^2 - Z_1^2$, вычисления по формулам (13), (14) имеют стоимость $2M + 3S$

Вычисление координаты (10) точки изогенной кривой $E_{d'}'$ можно выполнить с помощью формул [11]:

$$F = (X' + Z') = (X_1Z + Z_1X)^2(X + Z), \tag{15}$$

$$G = (X' - Z') = (X_1Z - Z_1X)^2(X - Z). \tag{16}$$

Тогда $2X' = F + G$, $2Z' = F - G$. Вычисления по формулам (15), (16) имеют стоимость $4M + 2S$. Суммарная стоимость вычисления 3-изогении в проективных координатах равна $6M + 5S$.

4. Вычисление 5-изогений в проективных координатах

Для первой координаты 5-изогении (9) после замены $\beta_{1,2}^2 = (1 - \alpha_{1,2}^2)/(1 - d\alpha_{1,2}^2)$ получим:

$$\frac{X'}{Z'} = \frac{x}{(\alpha_1\alpha_2)^2} \cdot \frac{x^2 + \alpha_1^2 - d\alpha_1^2x^2 - 1}{d(x^2 + \alpha_1^2) - d\alpha_1^2x^2 - 1} \cdot \frac{x^2 + \alpha_2^2 - d\alpha_2^2x^2 - 1}{d(x^2 + \alpha_2^2) - d\alpha_2^2x^2 - 1}. \tag{17}$$

Оценим вычислительную сложность выражения (17) в проективных координатах (алгоритм 1), тогда после замены $x \to \frac{X}{Z}$, $\alpha_{1,2} \to \frac{X_{1,2}}{Z_{1,2}}$ получим

$$\frac{X'}{Z'} = \frac{X(\mathrm{Z}_1\mathrm{Z}_2)^2}{Z(X_1X_2)^2} \cdot \frac{(XZ_1)^2 + (X_1\,\mathrm{Z})^2 - d(X_1X)^2 - (\mathrm{Z}_1\mathrm{Z})^2}{d((XZ_1)^2 + (X_1\,\mathrm{Z})^2) - d(X_1X)^2 - (\mathrm{Z}_1\mathrm{Z})^2} \cdot \frac{(XZ_2)^2 + (X_2\,\mathrm{Z})^2 - d(X_2X)^2 - (\mathrm{Z}_2\mathrm{Z})^2}{d((XZ_2)^2 + (X_2\,\mathrm{Z})^2) - d(X_2X)^2 - (\mathrm{Z}_2\mathrm{Z})^2}$$

Соответственно,

$$X' = XZ_1^2Z_2^2[X^2(Z_1^2 - dX_1^2) + \mathrm{Z}^2(X_1^2 - \mathrm{Z}_1^2)][X^2(Z_2^2 - dX_2^2) + \mathrm{Z}^2(X_2^2 - \mathrm{Z}_2^2)], \tag{18}$$

$$Z' = ZX_1^2X_2^2[dX^2(Z_1^2 - X_1^2) + \mathrm{Z}^2(dX_1^2 - \mathrm{Z}_1^2)][dX^2(Z_2^2 - X_2^2) + \mathrm{Z}^2(dX_2^2 - \mathrm{Z}_2^2)]. \tag{19}$$

Алгоритм 1: вычисления по формулам (18), (19). Вычисления X' согласно алгоритму 1 требуют $6S$ возведений в квадрат всех координат, $3M$ умножений X -координат на параметр

d, и $8M$ остальных умножений. Вместе с $8M$ умножений при вычислении Z' получим оценку стоимости расчета координат $(X':Z')$ 5-изогении, равную $19M+6S$.

Параметр d' изогенной кривой определяется как $d'=A^8d^5, A=\alpha_1\alpha_2$. Параметры изоморфной кривой $E_{C',D'}$ при этом

$$D'=(X_1^2X_2^2\cdot d)^4\cdot d, \tag{20}$$

$$C'=(Z_1^2Z_2^2)^4 \tag{21}$$

Вычисления по формулам (20), (21), с учетом уже известных $X_1^2X_2^2$ и $Z_1^2Z_2^2$, имеют стоимость $2M+4S$. Общая стоимость вычисления 5-изогении согласно алгоритму 1 составляет $21M+10S$.

Обратимся далее к методам, подобным методам предыдущего раздела. Использование полинома деления 24-й степени для точек 5-го порядка здесь не дает такого эффекта, как для 3-изогений. Вместе с тем, нам удалось выразить параметр d как функцию $d(\alpha_1,\alpha_2)$. Для точек Q ядра 5-го порядка справедливо $2Q=(\alpha_2,\beta_2), 4Q=-Q=(\alpha_1,-\beta_1)$. Другими словами, координата α_2 вычисляется по формуле удвоения точки Q, а координата α_1- по формуле удвоения точки $2Q$. Тогда, согласно (5) и (2),

$$\alpha_2=\frac{\alpha_1^2-\beta_1^2}{1-d\alpha_1^2\beta_1^2}=\frac{\alpha_1^2-\dfrac{\alpha_1^2-1}{d\alpha_1^2-1}}{1-d\alpha_1^2\dfrac{\alpha_1^2-1}{d\alpha_1^2-1}}=\frac{d\alpha_1^4-2\alpha_1^2+1}{-d\alpha_1^4+2d\alpha_1^2-1},\quad \alpha_1=\frac{d\alpha_2^4-2\alpha_2^2+1}{-d\alpha_2^4+2d\alpha_2^2-1}.$$

Отсюда

$$d=\frac{2\alpha_1^2-(\alpha_2+1)}{\alpha_1^2[(\alpha_2+1)\alpha_1^2-2\alpha_2]}=\frac{2\alpha_2^2-(\alpha_1+1)}{\alpha_2^2[(\alpha_1+1)\alpha_2^2-2\alpha_1]}$$

Подстановка этих выражений в (17) после ряда сокращений дает не зависящую от параметра d формулу

$$\frac{X'}{Z'}=x\cdot\frac{\{x^2(\alpha_2-1)+\alpha_1^2(\alpha_2+1)-2\alpha_2\}}{\{x^2(\alpha_2+1-2\alpha_1^2)+\alpha_1^2(1-\alpha_2)\}}\cdot\frac{\{x^2(\alpha_1-1)+\alpha_2^2(\alpha_1+1)-2\alpha_1\}}{\{x^2(\alpha_1+1-2\alpha_2^2)+\alpha_2^2(1-\alpha_1)\}} \tag{22}$$

Для числителей $F_{1,2}$ и знаменателей $G_{1,2}$ этой рациональной функции запишем:

$$F_{1,2}=x^2\alpha_{2,1}-x^2+\alpha_{1,2}^2\alpha_{2,1}+\alpha_{1,2}^2-2\alpha_{2,1}, \tag{23}$$

$$G_{1,2}=x^2\alpha_{2,1}+x^2-\alpha_{1,2}^2\alpha_{2,1}+\alpha_{1,2}^2-2x^2\alpha_{1,2}^2. \tag{24}$$

Тогда

$$U_{1,2}=F_{1,2}+G_{1,2}=2\{x^2\alpha_{2,1}+\alpha_{1,2}^2-(\alpha_{2,1}+x^2\alpha_{1,2}^2)\}=2(x^2-1)(\alpha_{2,1}-\alpha_{1,2}^2), \tag{25}$$

$$V_{1,2}=F_{1,2}-G_{1,2}=2\{\alpha_{1,2}^2\alpha_{2,1}+x^2-(\alpha_{2,1}-x^2\alpha_{1,2}^2)\}=2(\alpha_{1,2}^2-1)(\alpha_{2,1}+x^2). \tag{26}$$

В проективных координатах имеем

$$U_{1,2}=2\left(\left(\frac{X}{Z}\right)^2-1\right)\left(\left(\frac{X_{1,2}}{Z_{1,2}}\right)^2-\left(\frac{X_{2,1}}{Z_{2,1}}\right)\right)=2\left(Z_{2,1}Z_{1,2}^2Z^2\right)^{-1}\left(X^2-Z^2\right)\left(X_{1,2}^2Z_{2,1}-X_{2,1}Z_{1,2}^2\right) \tag{27}$$

$$V_{1,2}=2\left(\left(\frac{X_{1,2}}{Z_{1,2}}\right)^2-1\right)\left(\left(\frac{X}{Z}\right)^2+\left(\frac{X_{2,1}}{Z_{2,1}}\right)\right)=2\left(Z_{2,1}{Z_{1,2}}^2Z^2\right)^{-1}\left({X_{1,2}}^2-{Z_{1,2}}^2\right)\left(X^2Z_{2,1}+X_{2,1}Z^2\right). \quad (28)$$

Альтернативные формулы без учета общих сомножителей имеют вид

$$U'_{1,2}=\left(X^2-Z^2\right)\left[-\left(X_{2,1}+Z_{2,1}\right)\left({X_{1,2}}^2-{Z_{1,2}}^2\right)+\left(X_{2,1}-Z_{2,1}\right)\left({Z_{1,2}}^2+{X_{1,2}}^2\right)\right], \quad (29)$$

$$V'_{1,2}=\left({X_{1,2}}^2-{Z_{1,2}}^2\right)\left[\left(X_{2,1}+Z_{2,1}\right)\left(X^2+Z^2\right)-\left(X_{2,1}-Z_{2,1}\right)\left(X^2-Z^2\right)\right]. \quad (30)$$

С учетом $2F_{1,2}=U_{1,2}+V_{1,2}$ и $2G_{1,2}=U_{1,2}-V_{1,2}$ (формулы (27),(28)) можно получить

$$2F_{1,2}=\left[Z^2\left(X_{2,1}+Z_{2,1}\right)\left({X_{1,2}}^2-{Z_{1,2}}^2\right)+Z_{1,2}^2\left(X_{2,1}-Z_{2,1}\right)\left(X^2-Z^2\right)\right] \quad (31)$$

$$2G_{1,2}=\left[-X^2\left(X_{2,1}+Z_{2,1}\right)\left({X_{1,2}}^2-{Z_{1,2}}^2\right)+X_{1,2}^2\left(X_{2,1}-Z_{2,1}\right)\left(X^2-Z^2\right)\right] \quad (32)$$

Итак, функцию (22) на основе (25), (26) можно записать как

$$\frac{X'}{Z'}=\frac{X}{Z}\cdot\frac{F_1}{G_1}\cdot\frac{F_2}{G_2}=\frac{X}{Z}\cdot\frac{U_1+V_1}{U_1-V_1}\cdot\frac{U_2+V_2}{U_2-V_2}. \quad (33)$$

Алгоритм 2: вычисления по формулам (27), (28). После сокращения общих сомножителей функция (22) имеет вид

$$\frac{X'}{Z'}=\frac{X}{Z}\cdot\frac{\left(X^2-Z^2\right)\left(X_1^2Z_2-X_2Z_1^2\right)+\left({X_1}^2-Z_1^2\right)\left(X^2Z_2+X_2Z^2\right)}{\left(X^2-Z^2\right)\left(X_1^2Z_2-X_2Z_1^2\right)-\left({X_1}^2-Z_1^2\right)\left(X^2Z_2+X_2Z^2\right)}\cdot\frac{\left(X^2-Z^2\right)\left(X_2^2Z_1-X_1Z_2^2\right)+\left({X_2}^2-Z_2^2\right)\left(X^2Z_1+X_1Z^2\right)}{\left(X^2-Z^2\right)\left(X_2^2Z_1-X_1Z_2^2\right)-\left({X_2}^2-Z_2^2\right)\left(X^2Z_1+X_1Z^2\right)}$$

Вычислительная стоимость числителя X' здесь составляет, $14M+6S$, а знаменателя Z' – $2M$, в итоге затраты вычисления координат изогенной точки равны $16M+6S.$

Алгоритм 3: вычисления по формулам (29), (30). В числителе (33) выполняется 10 умножений M, а в знаменателе – $6M$, в итоге вновь вычислительные затраты оцениваются величиной $16M+6S.$

Алгоритм 4: вычисления по формулам (31), (32). На основе формул (31) и (32) для пар $2F_{1,2}, 2G_{1,2}$ и (33) рассчитываются по два общих сомножителя ($4M$), к этому добавляется по $6M$ умножений в числителе и знаменателе (33). Общая стоимость вычислений остается неизменной и равна $16M+6S.$ Этот алгоритм приводится в следующем разделе.

Иначе говоря, все три возможных алгоритма вычисления координат $(X':Z')$ изогенной точки согласно (22) имеют равноценную сложность.

Параметр d' изогенной кривой определяется как $d'=A^8d^5, A=\alpha_1\alpha_2.$ Параметры изоморфной кривой $E_{C',D'}$ при этом:

$$D'=(X_1^2\cdot X_2^2\cdot d)^4\cdot d, \quad (34)$$

$$C'=(Z_1^2\cdot Z_2^2)^4 \quad (35)$$

Вычисления по формулам (34), (35) имеют стоимость $4M+4S$. В сравнении с алгоритмом 1 здесь добавляются два умножения $X_1^2\cdot X_2^2$ и $Z_1^2\cdot Z_2^2$. Общая стоимость вычисления 5-изогении согласно алгоритмам 2 – 4 составляет $20M+10S$.

Известная средняя оценка соотношения стоимостей M и S определяется как $M \cong \frac{2}{3}S$ [2]. При этом оценка стоимости вычисления 3-изогении составляет $6M + 5S \cong 9,3M$, а 5-изогении $20M + 10S \cong 26,7M$. Эти оценки отличаются практически втрое.

Следует заметить, что найденные в работе оценки сложности вычисления 3- и 5-изогений справедливы не только для суперсингулярных кривых Эдвардса, но и для всех кривых классов полных и квадратичных кривых Эдвардса.

5. Алгоритмы вычисления 3- и 5-изогений кривых Эдвардса

Вычисление 3- и 5-изогений кривых Эдвардса (2) согласно формулам (13) – (18) и расчету параметра $d' = A^8 d^l$ изогенной кривой осуществляется с помощью приведенных ниже алгоритмов со стоимостью $6M + 5S$ и $20M + 10S$ соответственно.

Вход: точка $P = (X : Z)$ и точка 3-го порядка $Q_1 = (X_1 : Z_1)$, ядра кривой. E_d с параметром d

1. $s_1 \leftarrow X_1^2$
2. $s_2 \leftarrow Z_1^2$
3. $t_1 \leftarrow (X + Z_1)^2 - s_0 - s_2$
4. $t_2 \leftarrow t_1 + s_1$
5. $t_3 \leftarrow t_1 + s_2$
6. $t_4 \leftarrow 2t_1$
7. $t_5 \leftarrow 4s_1 + s_2 + t_4$
8. $t_6 \leftarrow 4s_2 + s_1 + t_4$
9. $D' \leftarrow t_3 \cdot t_5$
10. $C' \leftarrow t_2 \cdot t_6$
11. $u_1 \leftarrow X_1 \cdot Z$
12. $u_2 \leftarrow X \cdot Z_1$
13. $u_3 \leftarrow (u_1 + u_2)^2$
14. $u_4 \leftarrow (u_1 - u_2)^2$
15. $F \leftarrow (X + Z) \cdot u_3$
16. $G \leftarrow (X - Z) \cdot u_4$
17. $2X' \leftarrow F + G$
18. $2Z' \leftarrow F - G$

Выход: точка кривой $E'_{d'}$ $P' = (X' : Z')$ и параметры $(D' : C')$ изогенной кривой $C'E_{d'}{}'$

Алгоритм вычисления 3-изогении кривой Эдвардса

Вход: точка $P = (X : Z)$ и точки 5-го порядка $Q_1 = (X_1 : Z_1)$, , $Q_2 = (X_2 : Z_2)$ ядра кривой E_d с параметром d

1. $s_0 \leftarrow X^2$
2. $s_1 \leftarrow X_1^2$
3. $s_2 \leftarrow X_2^2$
4. $r_0 \leftarrow Z^2$
5. $r_1 \leftarrow Z_1^2$

6. $r_2 \leftarrow Z_2^{\,2}$
7. $t_0 \leftarrow s_0 - r_0$
8. $t_1 \leftarrow s_1 - r_1$
9. $t_2 \leftarrow s_2 - r_2$
10. $u_1 \leftarrow X_1 + Z_1$
11. $u_2 \leftarrow X_2 + Z_2$
12. $v_1 \leftarrow X_1 - Z_1$
13. $v_2 \leftarrow X_2 - Z_2$
14. $f_1 \leftarrow u_2 \cdot t_1$
15. $e_1 \leftarrow v_2 \cdot t_0$
16. $F_1 \leftarrow r_o \cdot f_1 + r_1 \cdot e_1$
17. $G_1 \leftarrow -s_o \cdot f_{11} + r_1 \cdot e_1$
18. $f_2 \leftarrow u_1 \cdot t_2$
19. $e_2 \leftarrow v_1 \cdot t_0$
20. $F_2 \leftarrow r_o \cdot f_2 + r_2 \cdot e_2$
21. $G_1 \leftarrow -s_o \cdot f_2 + r_2 \cdot e_2$
22. $X' \leftarrow X \cdot F_1 \cdot F_2$
23. $Z' \leftarrow Z \cdot G_1 \cdot G_2$
24. $L_1 \leftarrow s_1 \cdot s_2$
25. $L_2 \leftarrow r_1 \cdot r_2$
26. $D \leftarrow L_1 \cdot d$
27. $D \leftarrow D^2$
28. $D \leftarrow D^2$
29. $D' \leftarrow D \cdot d$
30. $C \leftarrow L_2^{\,2}$
31. $C' \leftarrow C^2$

Выход: точка кривой $E'_{d'}$ $P' = (X' : Z')$ и параметры $(D' : C')$ изогенной кривой $C'E_{d'}{}'$

Алгоритм вычисления 5-изогении кривой Эдвардса (алгоритм 4)

Эти алгоритмы отличаются наибольшей простотой и сравнительно малой стоимостью вычислений. В отличие от приведенного в работе [6] алгоритма вычисления 3-изогении мы используем вместо (8) более простое выражение (9) для функции $\phi(x, y)$ вместе с более простой формулой для параметра $d' = A^8 d^l$. Фактически при вычислении 3-изогении мы используем алгоритм, близкий к предложенному в работе [6], с той же эффективностью $6M + 5S$ стоимости вычислений. Оригинальные алгоритмы вычисления 5-изогений, как показал наш анализ, требуют втрое больших вычислительных затрат, чем для 3-изогений. Возрастание в $\frac{3}{2}$ раза числа переменных ($4 \rightarrow 6$) в 2,5 раза увеличивает число смежных произведений $\left(\frac{C_6^2}{C_4^2} = \frac{5}{2}\right)$, что дает грубую завышенную оценку (3.75 раза) выявленной пропорции.

6. Требования к параметрам криптосистемы

Поиск подходящего значения характеристики поля p в задаче SIDH с использованием 3- и 5-изогений кривых Эдвардса должен отвечать ряду необходимых условий.

Утверждение 1. 3- и 5-изогении существуют для суперсингулярных полных и квадратичных кривых Эдвардса E_d соответственно при $p \equiv -1 \bmod 60$ $p \equiv -1 \bmod 120$.

Доказательство. Точки 3-го и 5-го порядков существуют на полной суперсингулярной кривой Эдвардса порядка $p+1 = 4 \cdot 3^m \cdot 5^n$ при выполнении условий $p \equiv -1 \bmod 4$, $p \equiv -1 \bmod 3$ и $p \equiv -1 \bmod 5$, которые сводятся к одному условию $p \equiv -1 \bmod 60$. Минимальным четным кофактором порядка N_E квадратичной кривой Эдвардса является число 8 [7], при этом $p+1 = 8 \cdot 3^m \cdot 5^n$ и справедливо условие $p \equiv -1 \bmod 120$.

Утверждение 2. При нечетном $l = 2s+1$ l-изогении точек P нечетного порядка кривой есть точки нечетного порядка.

Доказательство. Кривая Эдвардса E_d порядка $N_E = 2^c \cdot n, c \geq 2$, содержит точки P нечетного порядка $n = l \cdot m$. Тогда существует l-изогения и изогенная кривая E' того же порядка N_E. l-изогения есть гомоморфизм, сжимающий в l раз точки $< P >$ в подгруппу точек нечетного порядка m кривой E'. Эта подгруппа не содержит точек четного порядка. При $m = 1$ l-изогения отображает все точки $< P >$ в нейтральный элемент O порядка 1.

Утверждение 3. При $p \equiv 1 \bmod 4$ суперсингулярных кривых Эдвардса не существует.

Доказательство. При $p \equiv 1 \bmod 4$ порядок суперсингулярной кривой $p+1 \equiv 2 \bmod 4$, тогда как для любой кривой Эдвардса число 4 делит порядок кривой [7].

Значение модуля p поля определяется требованиями безопасности. В произведении $3^m \cdot 5^n$ оба сомножителя имеют одинаковый порядок при $3^m \approx 5^n$, тогда $m \approx 1.465n$. Это уравновешивает число соответствующих циклических подгрупп. Квантовый уровень безопасности 128 бит с оценкой сложности $\sqrt[6]{p}$ (вместо $\sqrt[4]{p}$ для обычного компьютера) обеспечивается при длине модуля $\log_2 p = 6 \cdot 128 = 768$ бит. В поле F_{p^2} каждая координата точки имеет длину $2\log_2 p = 1536$ бит. Оценка длины ключа в системе SIDH составляет $6 \cdot \log_2 p = 6 \cdot 768 = 4608$ бит. Квантовый уровень безопасности 256 бит удваивает все эти оценки.

Заключение

Итак, использование 3- и 5-изогений кривых Эдвардса для точек нечетного порядка при фиксированной стойкости к атакам квантового компьютера позволит обойти проблемы особых точек, свойственных 2-изогениям этих кривых. Оценки сложности вычисления 3- и 5-изогений кривых Эдвардса, соизмеримые со сложностью групповых операций, позволяют реализовать наиболее быстрые алгоритмы постквантовой криптографии.

Список литературы:

1. Jao D., L. de Feo, Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies // Post-Quantum Cryptography. 2011. P. 19-34.

2. Bernstein D.J., Lange T. Faster Addition and Doubling on Elliptic Curves // Advances in Cryptology – ASIACRYPT'2007 (Proc. 13th Int. Conf. on the Theory and Application of Cryptology and Information Security. Kuching, Malaysia. December 2–6, 2007). Lect. Notes Comp. Sci. V. 4833. Berlin : Springer, 2007. P. 29–50.

3. Bernstein Daniel J., Birkner Peter , Joye Marc , Lange Tanja, Peters Christiane. Twisted Edwards Curves // IST Programme under Contract IST–2002–507932 ECRYPT,and in part by the National Science Foundation under grant ITR–0716498, 2008. P. 1-17.

4. Moody D., Shumow D. Analogues of Velus formulas for isogenies on alternate models of elliptic curves. Mathematics of Computation. 2016. Vol. 85. No. 300. P. 1929–1951.

5. Ahmadi O., Granger R. On isogeny classes of Edwards curves over finite fields // J. Number Theory. 2012. 132 (6). P. 1337-1358.

6. Suhri Kim, Kisoon Yoon, Jihoon Kwon, Seokhie Hong , and Young-Ho Park Efficient Isogeny Computations on Twisted Edwards Curves Hindawi Security and Communication NetworksVolume 2018, Article ID 5747642, 11 pages https://doi.org/10.1155/2018/5747642.

7. Бессалов А.В., Ковальчук Л.В. Суперсингулярные скрученные кривые Эдвардса над простым полем. I. Суперсингулярные скрученные кривые Эдвардса с *j*-инвариантами, равными нулю и 12^3. // Кибернетика и системный анализ. 2019. Т. 55. №3. С.3 – 10.

8. Бессалов А.В., Ковальчук Л.В. Суперсингулярные скрученные кривые Эдвардса над простым полем. II. Суперсингулярные скрученные кривые Эдвардса с *j*-инвариантом, равным 66^3. // Кибернетика и системный анализ. 2019. Т. 55. №5. С. 35–46.

9. Бессалов А.В. Эллиптические кривые в форме Эдвардса и криптография. Киев : Политехника, 2017. 272с.

10. Бессалов А.В., Цыганкова О.В. Число кривых в обобщенной форме Эдвардса с минимальным четным кофактором порядка кривой // Проблемы передачи информации. 2017. Т. 53 (1). С.101-111. doi:10.1134/S0032946017010082.

11. Washington L.C. Elliptic Curvres. Number Theory and Cryptography. Second Edition. CRC Press, 2008.

Киевский Университет имени Бориса Гринченко *Поступила в редколлегию 12.01.2020*

УДК 621.3.06 **DOI:10.30837/rt.2020.1.200.05**

М.Ю. РОДІНКО, Р.В. ОЛІЙНИКОВ, д-р техн. наук

ДОСЛІДЖЕННЯ ПРОДУКТИВНОСТІ МАЛОРЕСУРСНОГО БЛОКОВОГО ШИФРУ «КИПАРИС» НА РІЗНИХ ПЛАТФОРМАХ

Вступ

Особливе місце у сучасній криптографії займають малоресурсні шифри, призначені для використання у пристроях з обмеженою кількістю споживання енергії. Інтерес до малоресурсних примітивів проявив й Національний Інститут Стандартів та Технологій США, який організував конкурс на розробку малоресурсного алгоритму AEAD [1, 2].

Так само як і в традиційних, у малоресурсних блокових шифрах найбільш поширеними типами високорівневої конструкції є SPN-структура та мережа Фейстеля. В деяких шифрах застосовуються специфічні різновиди цих конструкцій такі, наприклад, як ARX-подібна SPN-структура у блоковому шифрі SPARX [3] або один з варіантів узагальненої мережі Фейстеля (англ. Generalized Feistel Network, GFN) у шифрах CLEFIA [4] та TWINE [5].

Серед блокових шифрів, заснованих на SPN-структурі, окремо можна виділити AES-подібні алгоритми, до яких можна віднести блокові шифри KLEIN [6] та Midori [7]. Причиною, з якої автори спираються на AES при розробці нових алгоритмів, є високий рівень вивченості шифру та його стійкість, що доведена математично та перевірена часом. До малоресурсних SPN-шифрів також відносяться PRESENT [8], PRINCE [9] та ін.

Багато малоресурсних блокових шифрів засновано і на мережі Фейстеля. В якості циклової функції мережі Фейстеля у малоресурсних алгоритмах все частіше застосовується не чергування S-блоків та лінійного перетворення, а так зване ARX-перетворення (англ. Addition, Rotation, XOR), що складається з операцій модульного додавання, циклічного зсуву та додавання за модулем 2. Операції, як правило, виконуються не над байтами, а над цілим напівблоком, розмір якого найчастіше складає 32 або 64 біти, що суттєво підвищує швидкодію перетворень при використанні шифру на процесорах з архітектурою аналогічної розрядності. До таких шифрів відносяться SPECK [10], TEA [11], XTEA [12], а також нещодавно розроблений блоковий шифр «Кипарис» [13]. На відміну від інших алгоритмів, «Кипарис» підтримує довжину блока та ключа 256 та 512 біт, завдяки чому залишиться стійким у постквантовий період.

Блоковий шифр «Кипарис» оперує блоками даних розміром l біт, із використанням ключа шифрування довжиною k біт, $l, k \in \{256, 512\}$, $l = k$. Операції циклової функції виконуються над s-бітними словами, $s \in \{32, 64\}$. Як вже було зазначено, «Кипарис» представляє собою мережу Фейстеля з ARX-перетворенням у якості циклової функції, що містить вісім додавань за модулем 2^s, вісім додавань за модулем 2 та вісім циклічних зсувів.

Метою роботи є дослідження продуктивності (а саме, такого показника як швидкість зашифрування в режимі простої заміни, у Мбіт/с) блокового шифру «Кипарис» та порівняння з продуктивністю інших відомих блокових шифрів на платформах Windows, Linux та Android.

1. Методика вимірювання швидкодії блокових шифрів

Для вимірювання швидкодії блокових шифрів використовувалась методика та програмний код, написаний мовою програмування C++, що застосовувались для дослідження продуктивності блокового шифру «Калина» [14]. З метою отримання точних та достовірних результатів методика передбачає багатократне (наприклад, восьмикратне) зашифрування блоку пам’яті фіксованого розміру (наприклад, 1 ГБ) у режимі простої заміни. Блок пам’яті складається з N блоків даних, де N залежить від розміру вхідного блока алгоритму шифру-

вання. Кожен з *N* блоків представляється у вигляді масиву 64-бітових беззнакових цілих чисел (розмірність масиву залежить від розміру блока, яким оперує шифр).

Для кожного з алгоритмів *N* задається константою, наприклад *number_of_blocks_in_memory_128* для шифру з 128-бітовим розміром блока. Для ініціалізації блоку пам'яті певного розміру використовується відповідна функція, наприклад *InitMemoryEncryptionBlock128()*.

Для отримання поточного значення числа тактів процесору призначена функція *DetermineTime()*. Для отримання числа тактів в операційній системі Linux використовувалася функція *gettimeofday()* з бібліотеки <sys/time.h>. Для операційної системи Windows була написана власна функція *Mygettimeofday()*.

На основі значень системного часу до початку та після закінчення виконання програмного блоку, що реалізує зашифрування, було обчислено швидкість зашифрування у Мбіт/с.

Вимірювання швидкодії блокових шифрів здійснювалося на наступних платформах:

– Процесор Intel Core i7-7500U з тактовою частотою 2,7-2,9 GHz, операційна система Windows 10 x32;

– Процесор Intel Core i7-7500U з тактовою частотою 2,7-2,9 GHz, операційна система Windows 10 x64;

– Процесор Intel Core i5-4670U з тактовою частотою 3,4 GHz, операційна система Linux (64-bits);

– Процесор Mediatek MT6582 з тактовою частотою 1,3 GHz, 4 ядра ARM Cortex-A7, операційна система Android 4.2.2 Jelly Bean (32-bits);

– Процесор Exynos 7880 з тактовою частотою 1,9 GHz, 8 ядер ARM Cortex-A53, операційна система Android 8.0.0 (64-bits).

У зв'язку із тим, що процесори, використовувані у мобільних пристроях, мають набагато нижчу продуктивність, для вимірювання швидкодії алгоритмів на ОС Android замість 8 ГБ пам'яті шифрувалося 8 МБ.

Окрім блокових шифрів «Кипарис-256» та «Кипарис-512» для отримання оцінок щодо швидкості зашифрування було обрано наступні блокові шифри:

- AES-256 [15];
- SPECK-64/128 [10];
- SPECK-128/128 [10];
- SPARX-128/128 [3];
- ДСТУ ГОСТ 28147: 2009 [16].

AES та ГОСТ-28147-89 було обрано як найбільш відомі та перевірені часом алгоритми, а SPECK – з міркувань того, що цей шифр, подібно до шифру «Кипарис», заснований на мережі Фейстеля з ARX-перетворенням у якості циклової функції. SPARX був обраний для порівняння як перший (разом із LAX) доказово стійкий малоресурсний блоковий шифр.

Обчислення швидкодії блокового шифру AES-256 здійснювалось для оптимізованої реалізації з використанням таблиць передобчислень, представленої в [14]. Реалізацію шифру ДСТУ ГОСТ 28147:2009 було обрано з того ж джерела [14].

Також були використані реалізації блокових шифрів SPECK-64/128 та SPARX-128/128 з бібліотеки FELICS [17], що містить оптимізовані реалізації найбільш відомих малоресурсних алгоритмів. Зазначимо, що не всі реалізації з цієї бібліотеки видаються достатньо оптимізованими з точки зору швидкодії (принаймні ті, що орієнтовані на застосування на процесорах загального призначення). Так, наприклад, внесення незначних змін у програмний код, що реалізує блоковий шифр SPECK-64/128 (заміна викликів функцій у процедурі зашифрування простою підстановкою коду, який вони містять), дозволило підвищити швидкодію у декілька

разів. Для SPECK-128/128 було обрано реалізацію, запропоновану авторами [18], перевагою якої є дуже компактний програмний код (функція зашифрування містить менше десяти рядків коду).

2. Результати вимірювання швидкодії блокових шифрів

Результати вимірювання швидкодії шифрів на різних платформах наведені в табл. 1 – 3.

Таблиця 1

Порівняння продуктивності малоресурсних блокових шифрів на платформі Windows 10 x32, процесор Intel Core i7-7500U

Блоковий шифр	Розмір блока, біт	Довжина ключа, біт	Швидкість зашифрування, Мбіт/с	Реалізація
«Кипарис-256»	256	256	3472,04	Власна
«Кипарис-512»	512	512	1555,54	Власна
AES-256	128	256	1441,85	[14]
SPECK	64	128	3059,16	[17]
SPECK	128	128	748,96	[18]
SPARX	128	128	661,83	[17]
ДСТУ ГОСТ 28147:2009	64	128	603,4	[14]

Шифри SPECK-128/128, SPARX-128/128 та ДСТУ ГОСТ 28147:2009 показали близький результат у межах 600-750 Мбіт/с. Далі йдуть блокові шифри AES-256 та «Кипарис-512» зі швидкістю порядку 1,5 Гбіт/с. Реалізація блокового шифру SPECK-64/128 [119] забезпечує швидкість шифрування порядку 3 Гбіт/с.

Значна різниця у швидкості зашифрування між реалізаціями шифрів SPECK-64/128 та SPECK-128/128 пояснюється тим, що SPECK-64/128 оперує 32-бітовим блоком, а SPECK-128/128 – 64-бітовим блоком, тому на 32-бітовій платформі SPECK-64/128 значно виграє у швидкодії. Теж саме стосується і шифрів «Кипарис-256» та «Кипарис-512».

Найкращий результат на 32-бітовій платформі Windows 10 показав блоковий шифр «Кипарис-512», його швидкодія склала майже 3,5 Гбіт/с.

Таблиця 2

Порівняння продуктивності малоресурсних блокових шифрів на платформі Windows 10 x64, процесор Intel Core i7-7500U

Блоковий шифр	Розмір блока, біт	Довжина ключа, біт	Швидкість зашифрування, Мбіт/с	Реалізація
«Кипарис-256»	256	256	3502,46	Власна
«Кипарис-512»	512	512	4942,77	Власна
AES-256	128	256	1653,79	[14]
SPECK	64	128	3038,03	[17]
SPECK	128	128	4786,81	[18]
SPARX	128	128	936,373	[17]
ДСТУ ГОСТ 28147:2009	64	128	526,583	[14]

На 64-бітовій платформі Windows 10 найкращий результат очікувано показали блокові шифри «Кипарис-512» (порядку 5 Гбіт/с) та SPECK-128/128 (порядку 4,8 Гбіт/с), які обробляють 64-бітові блоки даних. Крім того, перевагою блоковий шифру «Кипарис-512» є надвисокий рівень стійкості шифру, що дозволить йому застосовуватися у постквантовий період.

Результати для інших алгоритмів значно не змінилися у порівнянні з результатами, отриманими на 32-бітовій платформі, лише швидкість зашифрування алгоритму SPARX-128/128 помітно зросла з 749 до 937 Мбіт/с.

Таблиця 3

Порівняння продуктивності малоресурсних блокових шифрів на платформі Linux (64 bit), процесор Intel Core i5-4670U

Блоковий шифр	Розмір блока, біт	Довжина ключа, біт	Швидкість зашифрування, Мбіт/с	Реалізація
«Кипарис-256»	256	256	8418,3	Власна
«Кипарис-512»	512	512	5356,9	Власна
AES-256	128	256	1920,75	[14]
SPECK	64	128	3179,49	[17]
SPECK	128	128	5276,39	[18]
SPARX	128	128	1049,53	[17]
ДСТУ ГОСТ 28147:2009	64	128	640,469	[14]

Згідно з результатами, представленими у табл. 3, співвідношення між швидкостями досліджуваних алгоритмів на 64-бітовій платформі Linux приблизно таке саме, як і на Windows 10 x64. Головною відмінністю є значне покращення результату для шифру «Кипарис-256», швидкість якого перевершила 8 Гбіт/с, що може бути пов'язано з використанням нової версії компілятора gcc version 5.4.0, який виконує певну оптимізацію. Далі йдуть шифри «Кипарис-512» та SPECK-128/128 з приблизно однаковим результатом у більш ніж 5 Гбіт/с.

У табл. 4, 5 представлено результати вимірювання швидкодії обраних алгоритмів на мобільній платформі Android.

Таблиця 4

Порівняння продуктивності малоресурсних блокових шифрів на платформі Android 4.2.2 (32-bits), процесор Mediatek MT6582

Блоковий шифр	Розмір блока, біт	Довжина ключа, біт	Швидкість зашифрування, Мбіт/с	Реалізація
«Кипарис-256»	256	256	592	Власна
«Кипарис-512»	512	512	467	Власна
AES-256	128	256	109	[14]
SPECK	64	128	599	[17]
SPECK	128	128	205	[18]
SPARX	128	128	71	[17]

Таблиця 5

Порівняння продуктивності малоресурсних блокових шифрів на платформі Android 8.0.0 (64-bits), процесор Exynos 7880

Блоковий шифр	Розмір блока, біт	Довжина ключа, біт	Швидкість зашифрування, Мбіт/с	Реалізація
«Кипарис-256»	256	256	1263	Власна
«Кипарис-512»	512	512	999	Власна
AES-256	128	256	183	[14]
SPECK	64	128	639	[17]
SPECK	128	128	422	[18]
SPARX	128	128	145	[17]

На мобільних платформах «Кипарис» також продемонстрував високі результати. Так, наприклад, на процесорі Exynos 7880 «Кипарис-256» та «Кипарис-512» мають майже 1,3 Гбіт/с та 1 Гбіт/с відповідно, в той час, коли найближчий конкурент SPECK-64/128 має лише 640 Мбіт/с.

На рис. 1, 2 у графічному вигляді подано результати, представлені в табл. 1 – 5.

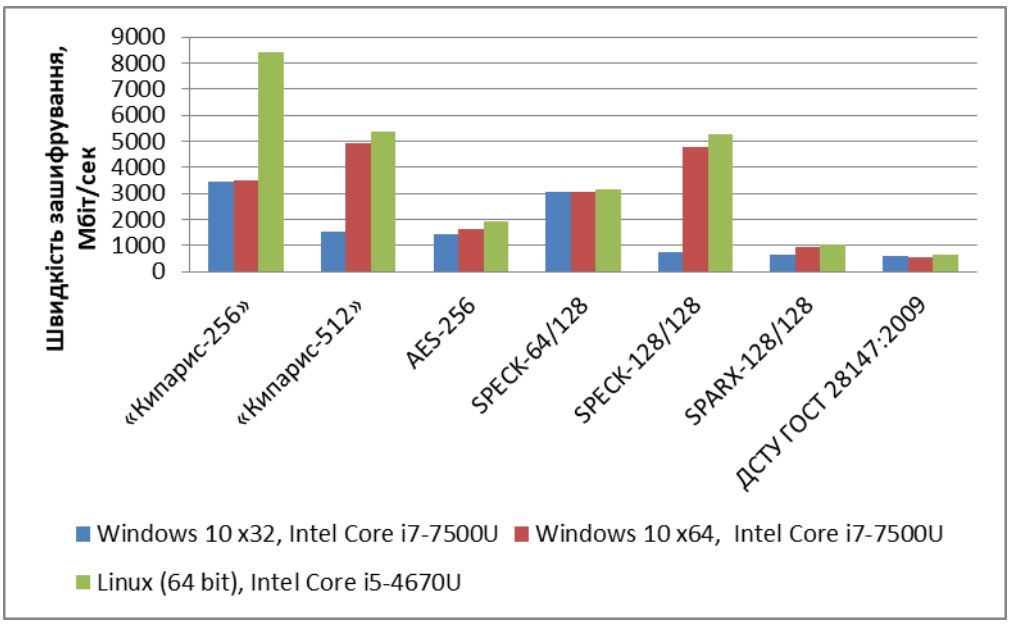


Рис. 1. Порівняння швидкодії шифру «Кипарис» з відомими блоковими шифрами на платформах загального призначення

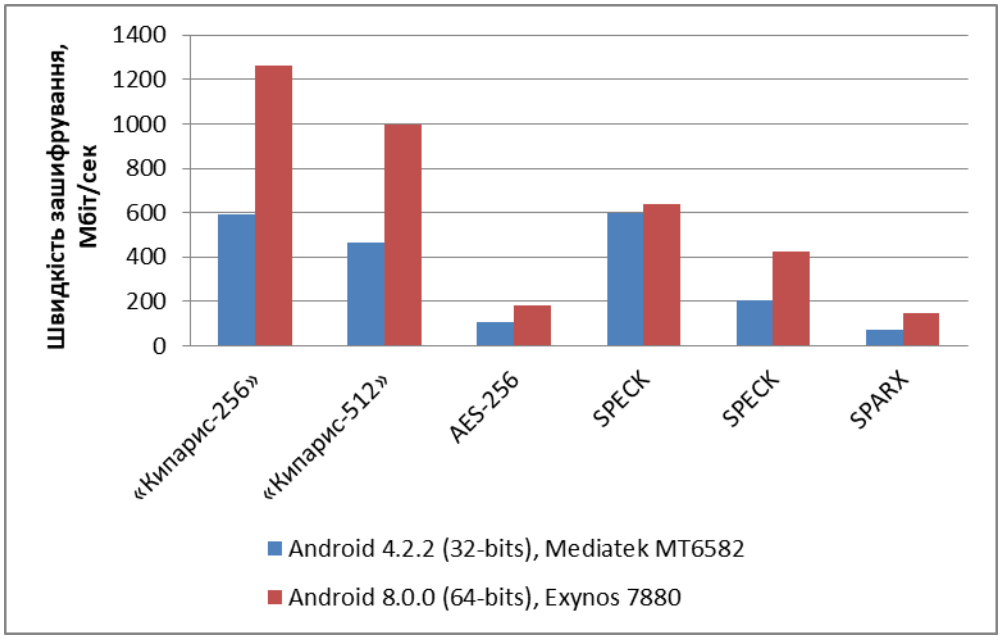


Рис. 2. Порівняння швидкодії шифру «Кипарис» з відомими блоковими шифрами на платформі Android

Висновки

1. Порівняння швидкодії блокового шифру «Кипарис» зі швидкодією відомих малоресурсних алгоритмів здійснювалося із використанням програмної реалізації, розробленої мовою програмування С++, що дозволяє отримати високу продуктивність (на базі нативного коду) за рахунок використання машинно-незалежної мови програмування.

2. Блоковий шифр «Кипарис» продемонстрував високу продуктивність на всіх досліджуваних програмно-апаратних платформах:

а) на платформі Windows 10 з 32-бітовою архітектурою найкращий результат показав шифр «Кипарис-256» (трохи менше 3,5 Гбіт/с), за ним слідує SPECK-128/128 (3 Гбіт/с), а шифр AES-256 відстає майже у 2,5 рази (1,5 Гбіт/с);

б) на платформі Windows 10 з 64-бітовою архітектурою блоковий найкращий результат показав шифр «Кипарис-512» (майже 5 Гбіт/с), якому незначно поступився за швидкістю шифр SPECK-128/128 (4,8 Гбіт/с); при цьому блоковий шифр «Кипарис-512» забезпечує надвисокий рівень стійкості;

в) на платформі Linux з 64-бітовою архітектурою блоковий шифр «Кипарис-256» показав надвисокий результат зі швидкодії (понад 8 Гбіт/с), далі з приблизно однаковим результатом слідують шифри «Кипарис-512» та SPECK-128/128 (понад 5 Гбіт/с);

г) на платформі Android 8.0.0 найкращими також були блокові шифри «Кипарис-256» та «Кипарис-512» (1,3 Гбіт/с та 1 Гбіт/с відповідно), за якими слідує SPECK-64/128 з результатом у 0,6 Гбіт/с.

3. Загалом, з точки зору продуктивності та зручності реалізації на різних програмно-апаратних платформах алгоритм «Кипарис» має наступні переваги:

а) два варіанти шифру («Кипарис-256» та «Кипарис-512») орієнтовані на 32-бітову та 64-бітову архітектури відповідно;

б) висока швидкодія перетворень незалежно від платформи, що використовується;

в) компактна реалізація незалежно від платформи, що використовується (сервер, робоча станція або мобільний пристрій);

г) мінімальний необхідний об’єм пам’яті для швидкодіючої реалізації, відсутність необхідності у таблицях передобчислень;

д) можливість організації ефективних захищених високошвидкісних каналів зв’язку між мобільними системами та серверами, у тому числі тими, що використовують апаратні прискорювачі.

Список літератури:

1. Lightweight cryptography. Project overview. NIST: веб-сайт. URL: https://csrc.nist.gov/projects/lightweight-cryptography.

2. Submission Requirements and Evaluation Criteria for the Lightweight Cryptography Standardization Process. NIST: веб-сайт. URL: https://csrc.nist.gov/CSRC/media /Projects/Lightweight-Cryptography/documents/final-lwc-submission-requirements-august2018.pdf.

3. Daniel Dinu, et al. Design strategies for ARX with provable bounds: Sparx and LAX // International Conference on the Theory and Application of Cryptology and Information Security, Springer, Berlin, Heidelberg, 2016. P. 484-513.

4. Taizo Shirai, et al. The 128-bit blockcipher CLEFIA // International workshop on fast software encryption. Springer, Berlin, Heidelberg, 2007. P. 181-195.

5. Suzaki T., Minematsu K., Morioka S., et al. Twine: A lightweight, versatile block cipher // ECRYPT Workshop on Lightweight Cryptography, LC11, 2011, P. 146–169.

6. Gong Z., Nikova S., Law Y. W. KLEIN: a new family of lightweight block ciphers // International Workshop on Radio Frequency Identification: Security and Privacy Issues. Springer, Berlin, Heidelberg, 2011. P. 1-18.

7. Banik S., et al. Midori: A block cipher for low energy // Advances in Cryptology – ASIACRYPT 2015: Proceedings of 21st International Conference on the Theory and Application of Cryptology and Information Security, 2015, Auckland, New Zealand. Part II. Vol. 9453 of LNCS, Springer, Berlin, Heidelberg, 2015. P. 411-436.

8. A. Bogdanov, et al. PRESENT: An Ultra-Lightweight Block Cipher. Springer, Berlin, Heidelberg, 2007. P. 450-466.

9. Borghoff J., et al. PRINCE – A Low-Latency Block Cipher for Pervasive Computing Applications – Extended Abstract // Advances in Cryptology – ASIACRYPT 2012: Proceedings of 18th International Conference on the Theory and Application of Cryptology and Information Security, 2-6 Dec., 2012, Beijing, China, Vol. 7658 of LNCS. Springer, Berlin, Heidelberg, 2012. P. 208-225.

10. Beaulieu R., et al. The SIMON and SPECK lightweight block ciphers // Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE. IEEE, 2015. P. 1-6.

11. Wheeler D. J. and Needham R. M. TEA, a Tiny Encryption Algorithm // International Workshop on Fast Software Encryption. Springer, Heidelberg, 1995. P. 363–366.

12. Needham R. M., Wheeler D. J. TEA extensions // Technical report, the Computer Laboratory, University of Cambridge, 1997.

13. Родінко М.Ю., Олійников Р.В. Постквантовий малоресурсний симетричний блоковий шифр «Кипарис» // Радіотехніка. 2017. Вип. 189. С. 100-107.

14. Roman-Oliynykov/ciphers-speed: веб-сайт. URL: https://github.com/Roman-Oliynykov/ciphers-speed.

15. Pub, NIST FIPS. 197: Advanced encryption standard (AES), Federal information processing standards publication 197.441: 0311, 2001.

16. ДСТУ ГОСТ 28147: 2009. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования (ГОСТ 28147-89).

17. FELICS. Cryptolux. URL: https://www.cryptolux.org/index.php/FELICS. 18. Ray Beaulieu et al. The SIMON and SPECK Families of Lightweight Block Ciphers, IACR, 19 June, 2013, URL: https://eprint.iacr.org/2013/404.

Харківський національний
університет імені В.Н. Каразіна

Надійшла до редколегії 09.01.2020

УДК 004.056.5 **DOI:10.30837/rt.2020.1.200.06**

О.О. КУЗНЕЦОВ, д-р техн. наук, А.С. КІЯН, А.І. ПУШКАРЬОВ, Т.Ю. КУЗНЕЦОВА

ТЕСТУВАННЯ КОДОВИХ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ ДЛЯ ПОСТКВАНТОВОГО ЗАСТОСУВАННЯ

Вступ

Використання випадкових послідовностей є невід'ємною частиною у сфері інформаційної безпеки та, зокрема, у криптографії [1, 2]: формуванні ключів та паролів користувачів, генерації гамуючих послідовностей при потоковому шифруванні, формуванні векторів ініціалізації для блокових шифрів та інше. З метою отримання подібних послідовностей використовують різноманітні способи генерації, серед яких особливе місце посідають криптографічно стійкі генератори псевдовипадкових послідовностей, що поділяються на блокові, потокові та ті, що базуються на використанні односторонніх функцій. Останні є перспективним напрямком досліджень, з тієї причини, що є доказово стійкими, базуючись на добре вивченій теоретико-складністній задачі [2]. Однак суттєвою проблемою більшості з генераторів псевдовипадкових послідовностей, які використовують односторонню функцію, є поява повномасштабних квантових комп'ютерів, який працює на основі явищ квантової заплутаності та квантової суперпозиції. Подібні пристрої здатні пришвидшити виконання обчислювальних операцій в тисячі разів, порівняно з класичним комп'ютером.

Активні дослідження в області розробки квантових комп'ютерів призвели до реакції зі сторони криптографічної спільноти, що проявляється у вигляді конкурсу постквантової стандартизації, оголошеного Національним інститутом стандартів і технологій у 2017 р., та результатом якого стане стандартизація проектів у сфері шифрування, електронного цифрового підпису та механізмів інкапсуляції ключів [3]. Останній факт впливає на безпечність існуючих криптопримітивів, фактично роблячи їх нестійкими. Звідси набуває актуальності дослідження нових методів побудови генераторів псевдовипадкових послідовностей, які будуть здатні зберігати стійкість в умовах класичного та квантового криптоаналізу, тобто постквантових методів генерації. Перспективним напрямком у цьому контексті є генератори, що базуються на використанні кодів, з декількох причин. По-перше, такі генератори відносяться до доказово стійких, оскільки засновані на відомій проблемі синдромного декодування, що вважається NP-складною. По-друге, є доведеним той факт, що кодові генератори є постквантовими, оскільки, на даний момент, невідомо ефективний алгоритм для вирішення проблеми синдромного декодування ні з застосуванням класичних, ні з застосуванням квантових обчислень [4].

У статті висвітлено принципи побудови класичного кодового генератора псевдовипадкових послідовностей та запропоновано новий підхід до реалізації кодового генератора, що дозволяє подолати недолік у класичній схемі такий, як зменшена практична довжина періоду формуємої послідовності. Надалі проведено евристичне тестування таких генераторів: швидкості генерації послідовності, довжини періоду послідовності та стійкості до класичного та квантового криптоаналізу. Дослідження стійкості здійснено у порівнянні зі стійкістю генераторів, що базуються на складності вирішення поширених теоретико-складнісних задач [5].

Доказово стійкий генератор Фішера – Штерна

Серед доказово стійких генераторів, стійкість яких заснована на проблемі синдромного декодування класичним вважається генератор, запропонований Фішером та Штерном. Саме його структуру покладено в основу розвитку подальших схем. Розглянемо принципи побудови подібного генератора. У його основі лежить використання блокового (n,k,d) коду, який задано перевірочною матрицею H, розміром $n\times k$. Функціонування генератора можна представити за допомогою наступної схеми (рис.1)[6].

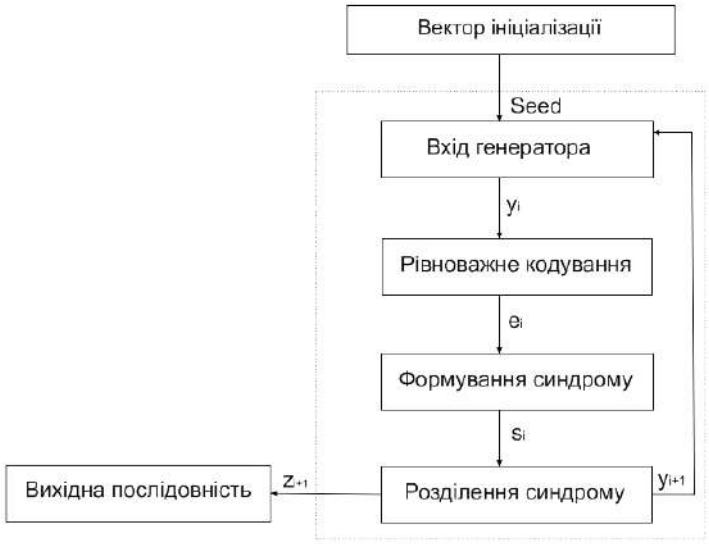


Рис. 1. Структурна схема генератора Фішера – Штерна

Етап 1. Обрати лінійний блоковий (n,k,d) код та необхідну довжину формуємої послідовності-l. На вхід генератора подається вектор ініціалізації($Seed$) довжини $m=\left\lfloor \log_2\binom{n}{t} \right\rfloor$. У цьому випадку $\lfloor x \rfloor$ позначає найбільше ціле число, що не перевищує x .

Етап 2. Вектор ініціалізації $Seed$ перетворюється за допомогою методу рівноважного кодування на вектор e_0, вага Хеммінга якого дорівнює виправляючій здатності коду($w(e_0)=t$). Величина t обчислюється згідно з параметрами обраного коду за правилом $t=\left\lceil \frac{d-1}{2} \right\rceil$.

Етап 3. До зміненого завдяки рівноважному кодуванню вектору e_0 застосовується рекурентне правило:

$$s_i = e_i \cdot H^T$$

де e_i _ двійковий вектор довжини n та $w(e_i)=t$; s_i _ двійковий вектор довжини $n-k$; H _ двійкова перевірочна матриця (n,k,d) коду .

Етап 4. Сформований на попередньому етапі вектор s_i розділяється на дві частини:

$$s_i = y_{i+1} \| z_{i+1}$$

де довжина вектору y_{i+1} дорівнює m біт, а довжина вектору z_{i+1} є $n-k-m$ біт.

Етап 5. Вектор z_{i+1} направляється на вихід генератора у якості частини сформованої послідовності.

Етап 6. Вектор y_{i+1} подається на вхід генератора як вектор ініціалізації для здійснення наступного циклу формування послідовності. Етапи 2-5 повторюються, поки не буде сформована послідовність необхідної довжини. Кількість циклів, що необхідно здійснити для формування послідовності дорівнює:

$$r=\left\lceil \frac{l}{n-k-m} \right\rceil,$$

де $\lceil x \rceil$ є найменшим цілим числом, що перевищує x .

В роботі [11] показано, що розглянутий генератор Фішера – Штерна володіє певними недоліками. Зокрема, проведені дослідження періодичних властивостей формованих послідовностей показали, що можливе раннє зациклювання генератора. В цьому випадку генератор формує послідовності, період яких значно (на декілька порядків) менший за максимальний. Отже, генератор Фішера – Штерна слід застосовувати з обережністю в додатках, які висувають вимоги до періодичних властивостей формованих послідовностей. В цій статті ми

пропонуємо новий генератор, який дозволяє формувати послідовності з максимально можливим періодом [7, 8].

Принципи побудови запропонованого генератора

Пропонований метод направлено на подолання недоліку генератора Фішера – Штерна, а саме зменшеної довжини періоду, порівняно з теоретично очікуваною. Головною особливістю структури нового генератора є додавання додаткових структурних елементів таких, як регістри зсуву з лінійним зворотнім зв'язком та суматору, що позначені на рисунку жирним шрифтом (рис.2) [9].

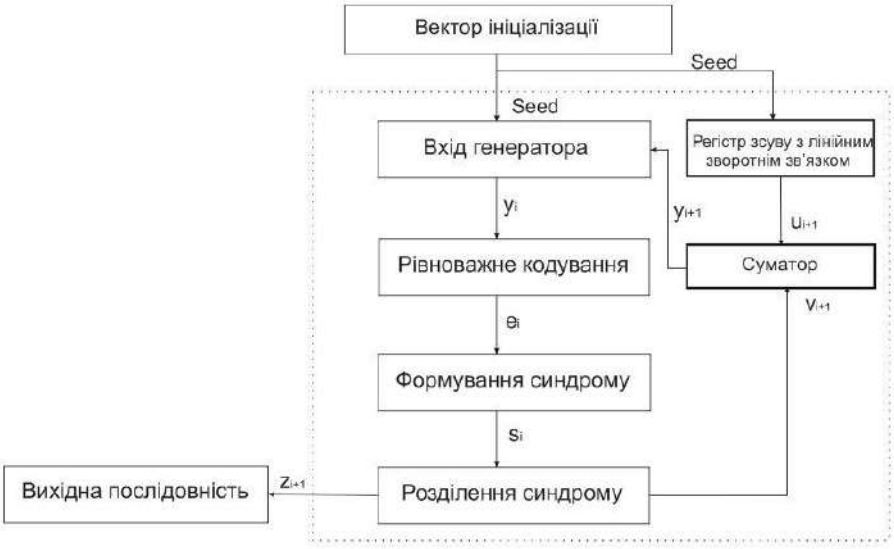


Рис. 2. Структурна схема альтернативного генератора

Аналогічно методу-прототипу в основу безпечності функціонування запропонованого генератора покладено складність вирішення проблеми синдромного декодування. Однак, як можна побачити на схемі, правило формування псевдовипадкових послідовностей змінено. Формалізуємо алгоритм формування псевдовипадкових послідовностей згідно із альтернативною схемою побудови генератора.

Етап 1. Як параметри генератора, необхідно обрати лінійний блоковий (n,k,d) код, потрібну довжину формуємої послідовності l та вектор ініціалізації(*Seed*) довжини $m = \left\lfloor \log_2 \binom{n}{t} \right\rfloor$, що подається на вхід першого циклу алгоритму.

Етап 2. Трансформування вектору ініціалізації *Seed* на вектор e_0, вага Хеммінга якого дорівнює виправляючій здатності коду ($w(e_0) = t$) за допомогою одного з методів рівноважного кодування. Величина t отримана згідно з параметром d обраного коду за правилом $t = \left\lfloor \frac{d-1}{2} \right\rfloor$.

Етап 3. Трансформований засобами рівноважного кодування вектор e_0 помножується на транспоновану перевірочну матрицю обраного коду:

$$s_i = e_i \cdot H^T$$

де e_i _ бітовий вектор, що має довжину n та вагу t; s_i _ отриманий двійковий вектор довжини $n-k$; H _ перевірочна матриця (n,k,d) коду. Отже, перші три етапи формування послідовності збігаються з етапами методу прототипу.

Етап 4. Вектор s_i, що представляє собою синдромну послідовність, розділяється на дві частини:

$$s_i = v_{i+1} \| z_{i+1}$$

де довжина вектору v_{i+1} дорівнює m біт, а довжина вектору z_{i+1} становить $n-k-m$ біт, що залишилися.

Етап 5. Вектор z_{i+1} стає частиною вихідної формуємої псевдовипадкової послідовності.

Етап 6. Вектор v_{i+1} поступає до суматору.

Етап 7. Початковий вектор ініціалізації $Seed$ поступає до регістру зсуву з лінійним зворотнім зв'язком, тобто задає початковий стан u_0 рекурентного перетворення. Кожний наступний стан регістру u_{i+1} обчислюється згідно з правилом [10]:

$$u_{i+1} = \varphi(u_i)$$

Поточний стан регістру далі поступає на суматор.

Етап 8. Обчислюється сума за модулем стану регістру зсуву з лінійним зворотнім зв'язком та вектору v_{i+1}, що отримано після розділення синдрому: $y_{i+1} = u_{i+1} + v_{i+1}$

Етап 9. Отриманий вектор y_{i+1} поступає на вхід генератора як вектор ініціалізації на наступному циклі перетворення. Кількість циклів, що необхідно здійснити для генерації послідовності необхідної довжини визначається за правилом:

$$r = \left\lceil \frac{l}{n-k-m} \right\rceil$$

де l – задана довжина послідовності, $n-k-m$ – довжина вектору, що поступає на вихід в кінці кожного циклу роботи.

Евристичне тестування кодових генераторів

Тестування псевдовипадкових послідовностей прийнято умовно поділяти на три групи: статистичне, евристичне та графічне. Статистичні тести використовують для встановлення чисельної оцінки якості послідовності. До евристичного тестування належать тести на криптостійкість, швидкість формування послідовностей, дослідження періоду, тест на точність визначення деяких констант методом Монте-Карло [11]. Статистичне тестування представлених генераторів було проведено у роботах [12]. У межах цієї статті проведемо дослідження генераторів з точки зору їх швидкодії, періоду послідовностей та стійкості до криптоаналізу.

Дослідження стійкості до класичного та квантового криптоаналізу

Як згадувалося вище, стійкість кодових генераторів псевдовипадкових чисел базується на складності вирішення задачі декодування синдрому. Декодування (n,k,d) коду заключається у знаходженні згідно з матрицями G та H і кодового слову з помилками $c*$ іншого кодового слова c. Отже, формулювання задачі синдромного декодування виглядає наступним чином: знайти вектор помилок з використанням синдромної послідовності.

Для загального випадку використання випадкового лінійного коду, тобто коду, у якому рядки перевірочної матриці обрано випадково та рівноймовірно, складність обчислення кореляційним способом, тобто за допомогою зіставлення кодового слова з помилками всім кодовим словам c (n,k,d) коду буде зростати експоненційно в залежності від параметрів використовуваного коду. Вирішення такої задачі для невповноваженого користувача, тобто того, кому невідомо матрицю, є NP-складною задачею. Подібні задачі вважаються стійкими навіть в умовах використання квантових обчислень.

Відповідно до досліджень, зокрема згідно з описаним у розділі 2 алгоритмом Шора, складність вирішення задач факторизації та дискретного логарифмування в умовах використання квантового комп'ютера зводиться до поліноміальної складності. З генераторами, заснованими на синдромному декодуванні, ситуація протилежна, оскільки таку задачу ототожнюють з NP-складною, звідки можемо зробити висновок, що генератори, які базуються на ній, здатні зберігати свою безпечність в постквантовому середовищі.

Складність класичного криптоаналізу щодо генераторів Фішера – Штерна та альтернативного генератора була обчислена відповідно до оцінки стійкості до перестановочного кодування, а саме оцінки мінімальної кількості покриваючих множин, що обчислюється за допомогою формули [13]:

$$N \geq \frac{C_n^t}{C_{n-k}^t} = \frac{\frac{n!}{t!(n-t)!}}{\frac{(n-k)!}{t!(n-k-t)!}} = \frac{n!(n-k-t)!}{(n-t)!(n-k)!}. \quad (1)$$

Причому $C_n^t = \frac{n!}{t!(n-t)!}$ є загальною кількістю комбінацій помилок, а $C_{n-k}^t = \frac{(n-k)!}{t!(n-k-t)!}$ – максимальною кількістю комбінацій помилок, які можуть бути покриті даною множиною.

Складність квантового криптоаналізу оцінена як кількість ітерацій, яких потребує алгоритм Гровера для вирішення задачі [14]:

$$C^{\frac{n}{2\log n}}, \; C = \frac{1}{(1-R)^{1-R}} \; . \quad (2)$$

У такому випадку R є відносною швидкістю, яку забезпечує використовуваний код. Практичні результати стійкості до класичного та квантового криптоаналізу за формулами (1) та (2) наведені на рис. 3,4 (тут і далі у логарифмічному масштабі за основою 2). Оцінки були проведені щодо різних наборів параметрів (n,k,t) коду. Параметр n обрано у діапазоні від 1024 до 8192.

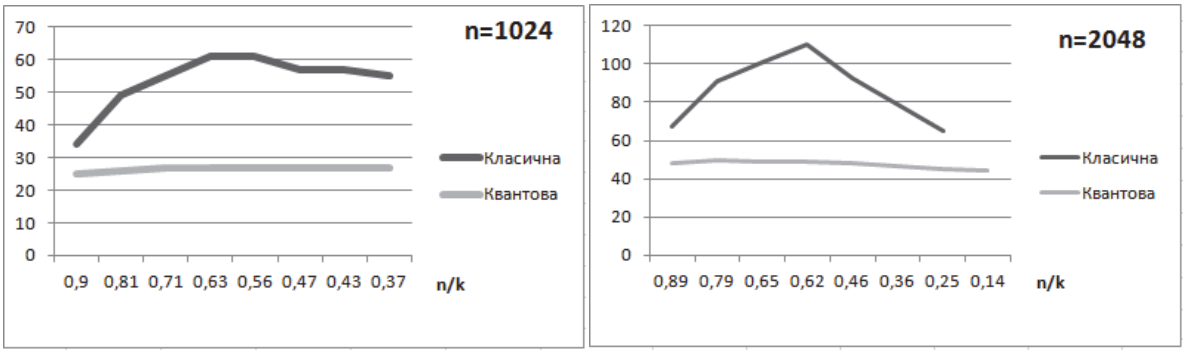


Рис. 3. Стійкість генераторів при n=1024 та при n=2048 відповідно

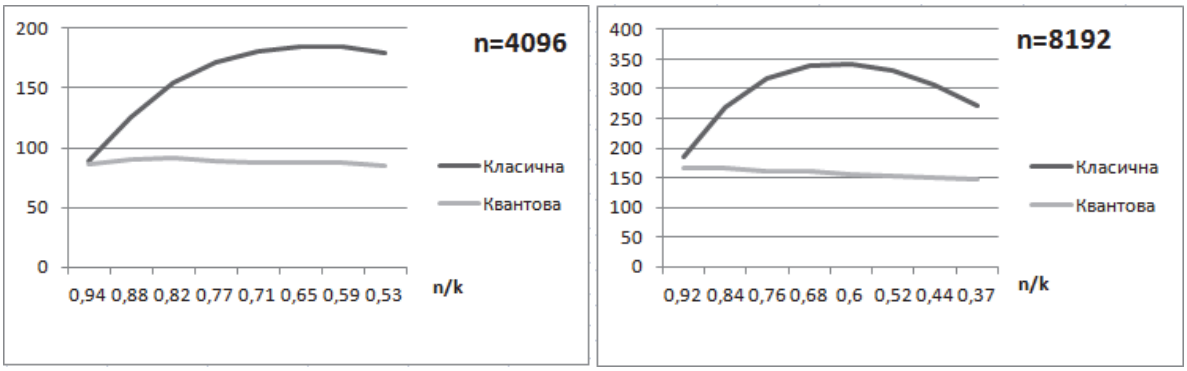


Рис. 4. Стійкість генераторів при n=4096 та n=8192 відповідно

Інформація щодо стійкості задач факторизації та дискретного логарифмування доведена у ряді англомовних видань, а також освітлена у [45].

Аналізуючи отримані результати, можна зробити висновок, що найбільш ефективним з точки зору безпеки є параметри коду, при якому відношення параметру k до параметру n

приблизно дорівнює 0,66. З іншого боку, при збільшенні параметру n стійкість як до класичного, так і до квантового криптоаналізу стрімко зростає (рис. 5).

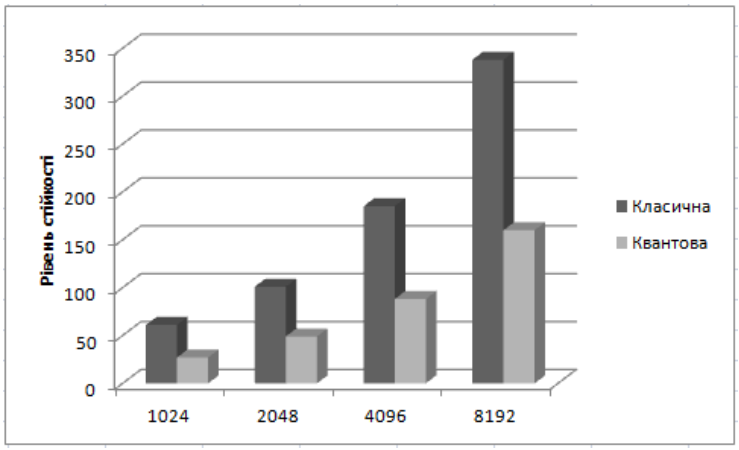


Рис. 5. Стійкість генераторів при співвідношенні $k/n \approx 0,66$ та різних n

Очевидно, що у постквантовому середовищі використовувані параметри повинні зростати і рекомендованими параметрами у цьому випадку є n від 4096.

Як згадувалося раніше, в основі доказово стійких генераторів лежить використання теоретико-складнісних задач. На сьогодні стійкість більшості криптографічних схем базується на складності вирішення задач факторизації (генератор Blum-Blum-Shub) та дискретного логарифмування (Dual_EC_DRBG). Оцінка цих задач описані у ряді джерел, зокрема у [15]. Порівняння стійкості до квантового криптоаналізу задач факторизації, дискретного логарифмування та синдромного декодування продемонстрована на рис. 6 відносно класичного рівня стійкості у 112, 192 та 256 біт.

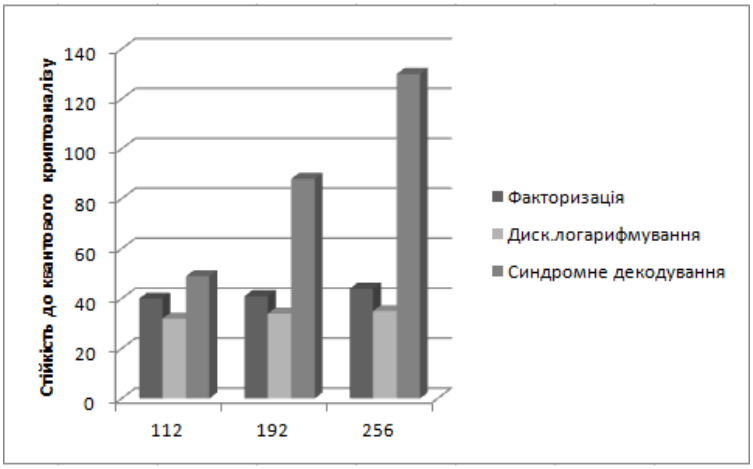


Рис. 6. Стійкість до квантового криптоаналізу теоретико-складністних задач

Аналізуючи дані, варто зазначити, що збільшення параметрів перетворення для генераторів, заснованих на задачі факторизації та на задачі дискретного логарифмування не призводить до суттєвого збільшення стійкості до квантового криптоаналізу, а також, порівняно із класичним криптоаналізом застосування квантових комп'ютерів значно зменшує їх стійкість. У той же час квантовий криптоаналіз синдромного декодування зменшує стійкість генератора відносно класичного криптоаналізу приблизно вдвічі (у логарифмічному масштабі за основою 2), що надає значну перевагу для постквантового періоду[16].

Дослідження довжини періоду послідовностей

Дослідження однієї з важливих характеристик генераторів псевдовипадкових чисел, які можуть застосуватися у криптографії, є довжина періоду послідовності, що гарантує відсутність зациклювання в межах задачі, що вирішується.

Довжина максимального періоду, що забезпечує використання генератора дорівнює $L = 2^m - 1$. Ці розрахунки випливають з того, що вектор ініціалізації, що подається на кожну ітерацію роботи генератора, $m = \left\lfloor \log_2 \binom{n}{t} \right\rfloor$, тому максимальна кількість різних ненульових векторів на кожній ітерації алгоритму генератора дорівнює $2^m - 1$ [17].

Розроблені програмні реалізації були протестовані з точки зору довжини періоду послідовності, що формується згідно з ними. На вхід кожного з генераторів було подано усі можливі конфігурації вектору ініціалізації, тобто було здійснено $2^m - 1$ формувань послідовностей. Параметри коду, для якого було здійснено тестування для кожного з генераторів, дорівнюють $(31,16,7)$. Таким чином, довжина вектору ініціалізації $m = 12$ біт, а довжина періоду відповідно до теоретичних розрахунків повинна бути $L = 2^{12} - 1 = 4095$. Другим випадком, що було розглянуто, є формування послідовності, з параметрами коду $(31,11,5)$. Довжина вектору ініціалізації при вказаних параметрах $m = 17$, а відповідна теоретична довжина періоду $L = 2^{17} - 1 = 131071$. Результати, отримані для генератора Фішера – Штерна, наведено на графіках (рис. 7, 8) [18]. На графіках продемонстровано відношення довжини періоду до кількості векторів ініціалізації, при яких вона отримана. З метою кращого візуального сприйняття графік побудовано у логарифмічному масштабі за основою 10 щодо осі ординат (формула $x = \log_{10} X$, де X є параметром, який слід перетворити; x представляє результат обчислення десяткового логарифма над масштабованим значенням).

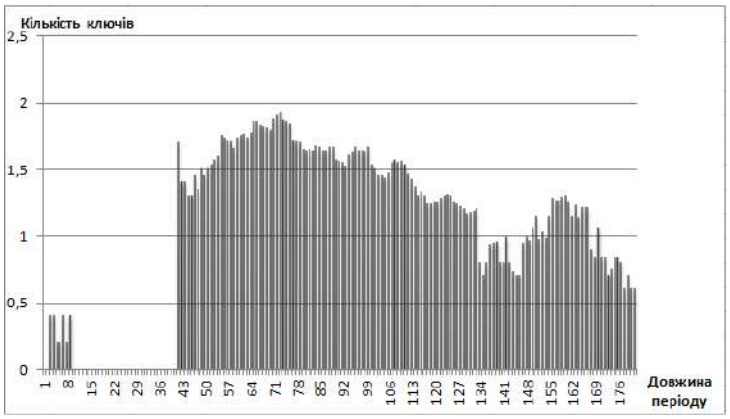


Рис. 7. Розподілення кількості ключів за довжинами періодів послідовності згідно з генератором Фішера – Штерна для коду $(31,16,7)$

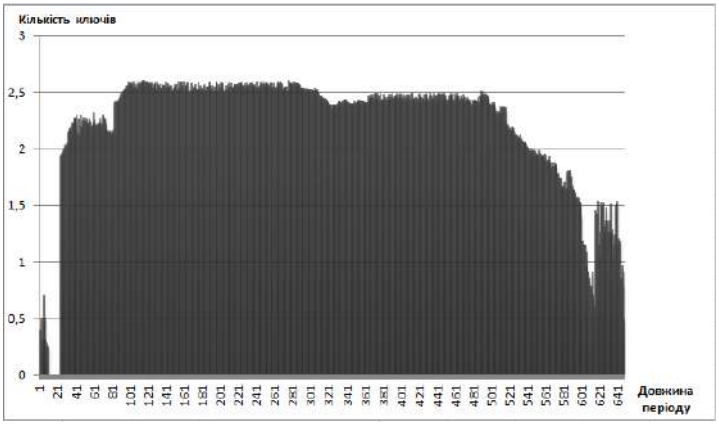


Рис. 8. Розподілення ключів за довжинами періодів послідовності згідно з генератором Фішера – Штерна для $(31,11,5)$ коду

Аналізуючи дані, представлені на графіках, можна зробити висновок, що, незважаючи на те, який вектор ініціалізації буде подано на вхід генератора, досягти максимальної довжина періоду не є можливим на практиці. Більш того, практично отримувані довжини набагато менші з теоретично очікуваною. У кращому випадку при застосуванні коду $(31,16,7)$ практична довжина періоду приблизно в 22 рази менша, ніж теоретично заявлена. У свою чергу кращий випадок для коду $(31,11,5)$ демонструє різницю між довжинами приблизно у 200 разів. Таким чином, зі зростанням довжини вектору ініціалізації, що подається на вхід, а відповідно і вектору кожної ітерації, різниця між теоретичним та практичним результатами буде збільшуватися.

Слід зазначити, що аналогічне тестування запропонованого генератора підтверджує формування ним послідовностей максимального періоду. Дійсно, для усіх можливих значень векторів ініціалізації було сформовано псевдовипадкову послідовність з періодами $L = 2^{12} - 1 = 4095$ (для випадку коду $(31,16,7)$) і $L = 2^{17} - 1 = 131071$ (при застосуванні коду $(31,11,5)$).

Дослідження швидкодії представлених генераторів

Швидкодія кодових генераторів перевірена за допомогою їх програмних реалізацій на мові програмування Java. Реалізаціє не є еталонною, але дозволяє перевірити відносну швидкість двох генераторів. Встановлена довжина формуємої послідовності дорівнює 10^6 біт. Результати швидкодії для кожного генератору отримані для різних комбінацій параметрів коду, що забезпечують різний рівень стійкості, для 10 випадків та освітлені усереднені показники.

Таблиця 1

Показники швидкодії представлених генераторів

Генератор Фішера – Штерна			
Параметри (n,k,t)	Стійкість квантова, біт	Швидкість формування ключових даних, мс	Швидкість генерації послідовності, мс
(127,85,6)	5	4	1,352
(255,177,11)	8	9	6, 317
(511,340,20)	15	23	8,903
(1023,678,37)	27	45	19,111
(2047,1328,60)	50	117	36,261
(4095,3376,67)	91	180	82,663
(8192,6892,100)	167	555	218,238
Запропонований генератор			
Параметри (n,k,t)	Стійкість квантова, біт	Швидкість формування ключових даних, мс	Швидкість генерації послідовності, мс
(127,85,6)	5	4	1,364
(255,177,11)	8	9	6,448
(511,340,20)	15	23	9,213
(1023,678,37)	27	45	19,632
(2047,1328,60)	50	117	38,569
(4095,3376,67)	91	180	86,557
(8192,6892,100)	167	555	228,119

Представимо наведені дані у вигляді залежності часу формування послідовності від параметра *n* використовуваного коду.

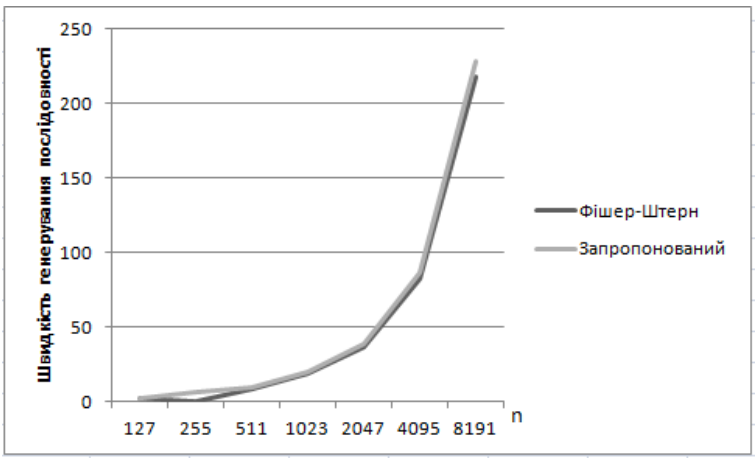


Рис. 9. Залежність швидкості формування послідовності від параметрів коду

Таким чином, можна зробити висновок, що збільшення часу формування псевдовипадкової послідовності згідно з запропонованим генератором за рахунок додання до схеми регістру зсуву з лінійним зворотнім зв'язком є незначним, при цьому він дозволяє зберігати стійкість і забезпечує максимальний період послідовності, на відміну від свого попередника.

Висновки

Перспективним напрямком у сфері постквантової криптографії вважається криптографія, що базується на кодах. Відповідно до статистики конкурсу NIST вона посідає друге місце не тільки у кількості поданих на розгляд проектів, але і у кількості схем, що пройшли до другого туру шляхом досліджень криптографів з усього світу. При цьому застосування принципів побудови кодових криптосистем до реалізації генераторів є можливим варіантом вирішення задачі реалізації постквантового генератора псевдовипадкових послідовностей. Використання даного підходу дозволяє забезпечити ряд переваг: стійкість до класичного та квантового крипто аналізу, високу швидкість криптоперетворень, а також доказову безпеку.

Дослідження кодових генераторів виявили, що класичним у цьому контексті є генератор, розроблений Фішером та Штерном, на його основі базуються подальші варіації кодових генераторів. Однак, алгоритм Фішера – Штерна має вагомий недолік: теоретично обчислювана та реальна довжина періоду послідовності, яка є важливою з криптографічної точки зору, суттєво відрізняються. Для його подолання було запропоновано альтернативний варіант генератору, особливістю реалізації якого є додаткове використання суматору та регістру зсуву з лінійним зворотнім зв'язком. Тестування підтвердило, що подібна побудова генератору, зберігає стійкість до класичного та квантового криптоаналізу, при цьому збільшення часу, що необхідний для формування послідовностей, є незначний у порівнянні з попередником. Також швидкодія може бути збільшена за рахунок застосування швидкого перетворення послідовності у послідовність з постійною вагою, що є актуальною темою для подальших досліджень.

Список літератури:

1. Johnston D. Random Number Generators-Principles and Practices // Sep. 2018. doi:10.1515/9781501506062.
2. Menezes A., Oorschot P. van, Vanstone S. Handbook of Applied Cryptography. CRC-Press, 1996. 816 p.
3. Perlner R. A., Cooper D.A. Quantum Resistant Public Key Cryptography: A Survey IDtrust '09, April 14- 16, 2009, Gaithersburg, MD, pp. 85-93. URL: https://ws680.nist.gov/publication/get_pdf.cfm?pub_id= 901595
4. Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner and Daniel Smith-Tone. NISTIR 8105. Report on Post-Quantum Cryptography. National Institute of Standards and Technology, Internal Report 8105, April 2016. 10 p.
5. Elaine Barker and John Kelsey. Recommendation for random number generation using deterministic random bit generators. National Institute of Standards and Technology, January 2012. 124 p. URL: https://doi.org/10.6028/NIST.SP.800–90A
6. Jean-Dernard Fisher, Jacques Stern. An efficient PseudoRandom Generator Provably as Secure as Syndrome Decodingr // EUROCRYPT'96 Proceeding, LNCS 1070. P. 245–255.

7. Andrea Rock. Pseudorandom Number Generators for Cryptographic Applications // Diplomarbeit zur Erlangung des Magistergrades an der Naturwissenschaftlichen Fakultat der Paris-Lodron-Universitat Salzburg. Salzburg. 2005.

8. Hastad J. Pseudorandom number generators from any one-way function / J. Hastad, R. Impagliazzo, L.A. Levin, M. Luby // SIAM Journal on Computing. 1999.Vol. 28. P.1364-1396.

9. Kuznetsov A., Kavun S., Panchenko V., Prokopovych-Tkachenko D., Kurinniy F. and Shoiko V. Periodic Properties of Cryptographically Strong Pseudorandom Sequences // 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkiv, Ukraine, 2018. P. 129-134. doi: 10.1109/INFOCOMMST.2018.8632021

10. Dubrova E. (2009). How to speed-up your NLFSR-based stream cipher. 878 – 881. 10.1109/DATE.2009.5090786.

11. Kuznetsov A.A., Kiian A.S., Prokopovich-Tkachenko D.I., Zverev V.P., Kotuh E.V., Kuznetsova T.Y. Periodical properties of cryptographic resistance pseudorandom sequences // Applied redioelectronics: sci.-tech. magazine. 2018. Vol.17, №. 3, 4. P. 96–103.

12. Grover L. A fast quantum mechanical algorithm for database search // Proceedings of the 28th annual ACM symposium on the theory of computing (STOC, 96). ACM Press, New York. 1996. P. 212–219.

13. Stipcevic M., Koc C.K. True random number generators // Open Problems in Mathematics and Computational Science. Springer, 2014. P. 275–315.

14. Grover L. A fast quantum mechanics algorithm for database search», Proceeding of the 28th ACM Symposium on Theory of Computation. New York: ACM Press, 1996. P. 212-219.

15. S. P. W: Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // S IAM J. Comput, 1997.

16. Andrew Rukhin. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf

17. Vlad Gheorghiu, Michele Mosca. Benchmarking the quantum cryptanalysis of symmetric, public-key and hash-based cryptographic schemes,URL: https://arxiv.org/pdf/1902.02332.pdf

18. Blum M.. How to generate cryptographycally strong sequences of pseudorandom bits / M. Blum, S. Micali // SIAM Journal on Computing. 1986. Vol. 1. P.850-864.

Харківський національний
університет імені В. Н. Каразіна;
АТ «Інститут інформаційних технологій»

Надійшла до редколегії 14.01.2020

УДК 004.056.5 **DOI:10.30837/rt.2020.1.200.07**

К.Е. ЛИСИЦКИЙ, А.А. КУЗНЕЦОВ, д-р техн. наук

ВЫЧИСЛИТЕЛЬНЫЕ АЛГОРИТМЫ РАСЧЕТА АЛГЕБРАИЧЕСКОГО ИММУНИТЕТА НЕЛИНЕЙНЫХ УЗЛОВ ЗАМЕНЫ СИММЕТРИЧНЫХ ШИФРОВ

1. Введение

Современный мир информационных технологий, в котором постоянно обмениваются информацией, в том числе конфиденциальной, информацией с ограниченным доступом, секретной и т.д., трудно представить без использования криптографических преобразований, таких как алгоритмы шифрования, криптографические протоколы, алгоритмы хеширования, алгоритмы электронной цифровой подписи и пр. Важное место среди алгоритмов шифрования занимают симметричные шифры. Благодаря своей простоте, скорости, они нашли широкий спектр применения во многих областях человеческой деятельности. Поэтому изучение и анализ симметричных криптосистем, а также их отдельных компонентов, таких как линейные и нелинейные преобразования и структуры смешивания блоков данных, безусловно, является актуальной научно-технической задачей. Наряду с совершенствованием методов проектирования и разработки симметричных блочных шифров рассматриваются проблемы совершенствования методов их криптоанализа и, в частности, вопросы дальнейшего повышения показателей их стойкости.

Исследования последних лет в этом направлении характеризуются повышенным интересом к алгебраическим методам криптоанализа.

Основная идея построения алгебраических атак основана на поиске возможности описания шифрования с использованием системы уравнений, позволяющей связать биты открытого текста, ключа и шифртекста. Стойкость к алгебраическим атакам во многих работах связывается с показателем алгебраической иммунности входящих в большинство шифров S-блоков (нелинейных узлов замены). Показатель алгебраической иммунности (алгебраического иммунитета) связан со степенью одночлена аннигилирующего полинома к булевой функции (векторной булевой функции), который определяет возможность понижения начального порядка системы уравнений (их числа) с помощью специально разработанного для этого математического аппарата.

Как показывает анализ, вычисление алгебраического иммунитета является нетривиальной задачей. Это связано с решением системы уравнений большой размерности, требующим значительных вычислительных ресурсов и объема памяти, которые уже для байтовых S-блоков выходят за рамки практически приемлемых затрат.

2. Цели и задачи работы

Задача состоит в том, чтобы разработать ускоренный алгоритм расчета АИ, на основе метода Арса – Фожера. Алгоритм должен вычислять АИ байтовых S-box за приемлемые временные сроки, в отличие от неоптимизированного алгоритма, при этом используя минимум ресурсов ОЗУ на ПК. Это будет универсальный алгоритм, позволяющий вычислять АИ для S-блока как можно большей степени, используя минимум временных затрат и ресурсов ОЗУ на ПК.

3. Обзор литературы

Интерес, возникший в свое время к алгебраическим методам криптоанализа блочных и потоковых шифров в 2003 году благодаря работам Н. Куртуа и В. Майера [1], не ослабевает даже сегодня. Результатом повышенного внимания к этим методам стало появление нового криптографического показателя пригодности S-блоков, показателя в виде алгебраического

иммунитета. В [2] следует напомнить, что понятие алгебраического иммунитета для булевых функций было введено в 2004 году В. Мейером, Э. Пасаликом и К. Карле в [3].

Алгебраическим иммунитетом *AI*(*f*) (АИ) булевой функции *f* называется минимальное число *d* такое, что существует булева функция *g* степени *d*, не тождественно равная нулю, для которой $fg = 0$ или $(f \oplus 1)\ g = 0$. Для любой булевой функции выполняется условие $d \le \lfloor n/2 \rfloor$, и существуют функции, имеющие $d \le \lfloor n/2 \rfloor$. Далее приведем еще одну выдержку из [2].

Понятие алгебраического иммунитета различными способами было обобщено на случай векторной булевой функции. Так, в [5] Ф. Армкнехт и М. Краузе, а также Г. Арс и Ж.-Ш. Фожер в [6] рассмотрели алгебраический иммунитет S-блоков и ввели понятия базового *AI*(*F*) и графического *AIgr*(*F*) алгебраического иммунитета векторных булевых функций. Базовый алгебраический иммунитет используется в потоковых шифрах. Графический алгебраический иммунитет используется для изучения устойчивости к алгебраическим атакам блочных шифров. Следующим обобщением, которое принято многими исследователями как одно из наиболее естественных с криптографической точки зрения, является компонентная алгебраическая иммунность $AI_{\text{comp}}(F)$. Компонентный алгебраический иммунитет AIcomp (F) векторной булевой функции F: $Z_2^n \to Z_2^m$ называется минимальным алгебраическим иммунитетом компонентных функций $b\ F$ ($b \in Z_2^m$, $b \neq 0$) i.e., $AI_{\text{comp}}(F) = \min\{AI(b\ F) : b \in Z_2^m, b \neq 0\}$,, where $b\ F = b_1 f_1 \oplus \ldots \oplus b_m f_m$ [7]. В случае компонентного алгебраического иммунитета было также получено в [6], что $AI_{\text{comp}}(F) \le \lfloor n/2 \rfloor$.

Другой метод определения алгебраической иммунности нелинейных узлов замены по Арсу – Фожеру построен с использованием базисов Грёбнера. Он разработан в [9] и основан на утверждении, приведенном ниже.

Утверждение. Пусть $s : V_n \to V_n$ будет булево отображение (S-блок) с координатной функцией $s_1, \ldots, s_n$. Рассмотрим булеву функцию $s : V_n \to V_n$ $f_s : V_{2n} \to \{0,1\}$, которая определяется с помощью следующего отношения:

$$f_s(x, y) = 1, \text{ если } s(x) = y;\ f_s(x, y) = 0 - \text{в противном случае } x, y \in V_n.$$

Тогда алгебраический иммунитет отображения s (по Арсу – Фожеру) совпадает с минимальной степенью ненулевых многочленов, принадлежащих аннулятору функции $f_s : AI(s) = \min \deg A_{nn}(f_s)$.

Следует отметить, что результаты расчета алгебраического иммунитета S-блоков в методе Арса – Фожера [7] и в расчетах компонентного алгебраического иммунитета [8] не совпадают. Далее мы рассмотрим наиболее правильный метод, при котором можно однозначно построить аннигилирующий полином меньшей степени. Это метод Арса – Фожера, основанный на построении базисов Грёбнера.

В [9] эта проблема решается с помощью стороннего программного обеспечения, а именно, программного пакета приложений Magma [10], который реализует широкий спектр функций, связанных с алгеброй, теорией групп, кольцами и полями, теорией чисел и многими другими разделами математики. Используется стороннее программное обеспечение, так как вычисления таких больших систем уравнений требуют значительных временных затрат. В нашей работе будет представлена оптимизированная реализация метода вычисления АИ, которая позволит нам получить результат в приемлемые сроки.

4. Материалы и методы. Вычисление алгебраической иммунности булевого отображения

Прежде чем привести алгоритм вычисления алгебраической иммунности, введем некоторые обозначения. Следуя работе [4]:

Пусть $GF(2)$ – двоичное поле и $GF(2)^n$ – n-мерное векторное пространство над $GF(2)$.

Булева функция $f(x)$ от n переменных – это отображение $f(x): GF(2)^n \to GF(2)$, где $x = (x_1, ..., x_n)$.

Таблица истинности булевой функции $f(x)$ от n переменных – это двоичный выходной вектор значений функции, который содержит 2^n элементов, каждый элемент принадлежит множеству {0, 1}.

Алгебраическая нормальная форма (*полином Жегалкина*) булевой функции $f(x)$ от n переменных записывается в виде

$$f(x) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus ... \oplus a_n x_n \oplus a_{12} x_1 x_2 \oplus a_{13} x_1 x_3 \oplus ... \oplus a_{(n-1)n} x_{n-1} x_n \oplus ... \oplus a_{123...n} x_1 x_2 x_3 ... x_n,$$

где коэффициенты $a_i \in \{0,1\}$ и каждая булева функция реализуются полиномом Жегалкина единственным образом, т.е. каждое представление $f(x)$ соответствует уникальной таблице истинности.

Алгебраическая степень $Deg(f)$ булевой функции $f(x)$ – число переменных в самом длинном слагаемом алгебраической нормальной формы функции, имеющем ненулевой коэффициент a_i. При этом считаем $Deg(0) = 0$.

Обозначим через V_n множество всех отображений $GF(2)^n \to GF(2)$, т.е. это множество всех возможных булевых функций $f(x)$ от *n* переменных.

Множество V_n будем рассматривать и как кольцо булевых функций и как векторное (линейное) пространство над двоичным полем, т.е. $V_n = GF(2)^{2^n}$.

Булева функция $g \in V_n$ называется *аннигилятором* функции $f \in V_n$, если

$$f \cdot g = 0$$

или

$$(f + 1) \cdot g = 0.$$

Множество различных аннигиляторов булевой функции $g(x)$ образует линейное пространство, которое обозначим

$$Ann(f) = \{g \in V_n \mid f \cdot g = 0\}.$$

Линейное пространство аннигиляторов степени $\le d$ обозначим

$$A_d^n(f) = \{g \in V_n \mid f \cdot g = 0, Deg(g) \le d\} \subset Ann(f).$$

Понятие аннигиляторов булевых функций тесно связано с оценкой эффективности алгебраического криптоанализа поточных шифров [1]. В частности, при использовании фильтрующего генератора (см. рис. 1) псевдослучайных последовательностей (ПСП) поиск начального состояния регистра сдвига с линейной обратной связью (РСЛОС) сопряжен с понижением степени совместной системы полиномиальных булевых уравнений.

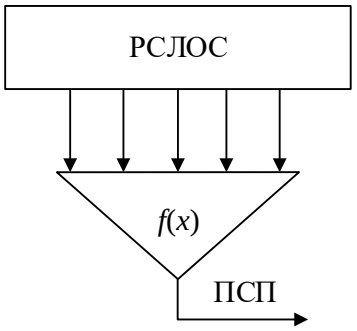


Рис. 1. Структурная схема фильтр-генератора ПСП

Алгоритм алгебраического криптоанализа, предложенный в [1], позволяет, при определенных условиях, по части перехваченной выходной последовательности (ПСП) находить начальное состояние РСЛОС с временно*й* сложностью $O\left((S_n^d)^3\right)$, где

$$S_n^d = \sum_{i=0}^{d} \frac{n!}{i!(n-i)!}$$

и d – наименьшая степень ненулевого аннигилятора фильтрующей булевой функции $f(x)$ или ее инверсии $f(x)+1$.

Таким образом, задачей алгебраического криптоанализа является поиск ненулевых аннигиляторов или, по крайней мере, оценка их минимальной степени. С этой целью в работе [3] введено определение *алгебраической иммунности* $AI(f)$ булевой функции $f \in V_n$ в виде

$$AI(f) = \min\{Deg(g) \mid g \in Ann(f) \text{ или } g \in Ann(f+1)\}.$$

Величина $AI(f)$ численно равна минимальной степени такой булевой функции $g \in V_n$, что $f \cdot g = 0$ или $(f+1) \cdot g = 0$.

Используя введенное выше понятие линейного пространства аннигиляторов степени $\le d$, запишем:

$$AI(f) = \min\{d \mid A_d^n(f) \neq 0 \text{ или } A_d^n(f+1) \neq 0\}, \quad (1)$$

т.е. для оценки алгебраической иммунности булевой функции $f \in V_n$ достаточно найти ненулевой базис пространства аннигиляторов наименьшей степени d.

Величина d позволяет количественно оценить сложность алгебраического криптоанализа и, при достаточно большом d, гарантировать устойчивость поточного криптоалгоритма к алгебраической атаке.

Алгоритм вычисления алгебраической иммунности булевых функций. Один из алгоритмов расчета алгебраической иммунности булевых функций представлен в диссертационной работе [11]. Он основан на построении базиса линейного пространства аннигиляторов $A_d^n(f)$ заданной степени d. Итеративно увеличивая d и повторяя построение базиса пространства $A_d^n(f)$, оценку $AI(f)$ получим по формуле (1), т.е. через ненулевой базис аннигиляторов наименьшей степени.

Для изложения сути алгоритма необходимо ввести следующие дополнительные обозначения.

Моном (одночлен) относительно переменных $x_1,...,x_n$ будем записывать в виде

$$x^u = \prod_{i=1}^{n} x_i^{u_i} = \begin{cases} x_i, u_i = 1, \\ 1, u_i = 0, \end{cases}$$

где $x, u \in V_2^n, x = (x_1,...,x_n), u = (u_1,...,u_n)$ – векторы переменных

Степень одночлена x^u определяется весом Хемминга (числом ненулевых координат) $w_h(u)$ вектора $u = (u_1,...,u_n)$, т.е.

$$Deg(x^u) = w_h(u).$$

С учетом этих обозначений булеву функцию $f(x)$ в алгебраической нормальной форме (в форме полинома Жегалкина) запишем в виде

$$f(x) = \sum_{u \in GF(2)^n} a_u x^u, \; a_u \in GF(2). \quad (2)$$

Функцию (аннигилятор) $g \in A_d^n(f)$ также представим в виде полинома Жегалкина

$$g(x) = \sum_{v \in GF(2)^n : w_h(v) \le d} b x \ , \tag{3}$$

где $b_v \in GF(2)$ – неизвестные коэффициенты аннигилятора, $w_h(v)$ – вес Хемминга вектора $v = (v_1, ..., v_n)$.

Функция g принадлежит пространству аннигиляторов $A_d^n(f)$ только в том случае, если для любого $x \in GF(2)^n$ выполняется равенство $f(x) \cdot g(x) = 0$.

Подставив (2) и (3) получим:

$$f(x) \cdot g(x) = \left(\sum_{u \in GF(2)^n} a_u x^u \right) \left(\sum_{v \in GF(2)^n : w_h(v) \le d} b_v x^v \right) = \sum_{u \in GF(2)^n} \left(\sum_{v \in GF(2)^n : w_h(v) \le d} a_u b_v x^{u \vee v} \right) = 0,$$

где $u \vee v = (u_1 \vee v_1, ..., u_n \vee v_n)$, $\vee$ – дизъюнкция (логическая операция ИЛИ).

После группировки слагаемых по общему множителю, получим равенство

$$\sum_{w \in GF(2)^n} \left(\sum_{a_u, b_v : a_u \vee b_v = w} a_u b_v \right) x^w = 0, \tag{4}$$

которое выполняется для любого $w \in GF(2)^n$. Следовательно, имеем систему линейных однородных уравнений

$$\begin{cases} \sum\limits_{a_u, b_v : a_u \vee b_v = w} a_u b_v = 0, \ \forall w \in GF(2)^n \end{cases} \tag{5}$$

относительно неизвестных коэффициентов b_v аннигилятора $g(x)$.

Поиск пространства аннигиляторов осуществляется путем решения системы линейных уравнений (5), полученных на основе группирования неизвестных коэффициентов по всем различным мономам.

Приведем пример из работы [9] построения базиса пространства $A_d^n(f)$.

В этом примере $f(x)$ – исходный многочлен в виде полинома Жегалкина; $g(x)$ – искомый аннулирующий многочлен.

Пример 1. Для $n = 2$ и $d = 1$ имеем:

$$f(x) = a_{00} + a_{10} x_1 + a_{01} x_2 + a_{11} x_1 x_2 ,$$
$$g(x) = b_{00} + b_{10} x_1 + b_{01} x_2 .$$

После подстановки в $f(x) \cdot g(x) = 0$ получим

$$\begin{aligned} f(x) \cdot g(x) = {} & a_{00} b_{00} + (a_{00} b_{10} + a_{10} b_{10} + a_{10} b_{00}) x_1 + \\ & + (a_{00} b_{01} + a_{01} b_{01} + a_{01} b_{00}) x_2 + \\ & + (a_{10} b_{01} + a_{01} b_{10} + a_{11} b_{00} + a_{11} b_{10} + a_{11} b_{01}) x_1 x_2 = 0, \end{aligned}$$

откуда имеем систему линейных однородных уравнений

$$\begin{cases} a b = 0, \\ a b + a b + a b = 0, \\ a b + a b + a b = 0, \\ a b + a b + a b + a b + a b = 0 \end{cases} \tag{6}$$

относительно неизвестных $b_{00}, b_{10}, b_{01}, \ldots$ – коэффициентов функции $g(x)$.

Тогда, например, для функции $f(x)=x_1+x_2$ (т.е. при $a_{00}=a_{11}=0$ и $a_{10}=a_{01}=1$) получим систему

$$\begin{cases} b_{10}+b_{00}=0, \\ b_{01}+b_{00}=0, \\ b_{01}+b_{10}=0, \end{cases}$$

которой удовлетворяют только два решения:

$$b_{00}=b_{10}=b_{01}=0\text{, т.е. } g(x)=0,$$

$$b_{00}=b_{10}=b_{01}=1\text{, т.е. } g(x)=1+x_1+x_2.$$

Непосредственная проверка показывает, что $g(x)=1+x_1+x_2$ действительно является аннигилятором функции $f(x)=x_1+x_2$:

$$f(x)\cdot g(x)=(x_1+x_2)(1+x_1+x_2)=x_1+x_2+x_1+x_1x_2+x_1x_2+x_2=0.$$

В общем случае для решения системы уравнений (5), например методом Гаусса, строится таблица размером $2^{2n}\times 2^{2n}$, где n – степень S-блока. Ячейки таблицы – сгруппированный результат умножения всех мономов полинома $f(x)$ на полином $g(x)$. Группировка происходит таким образом, что в итоге строчки представляются как все возможные варианты мономов (их 2^{2n}), а столбцы – это неизвестные коэффициенты (их тоже 2^{2n}). Таким образом, значение ячейки таблички может быть = 1, если коэффициент b_i присутствует в конкретном мономе и 0, если такой коэффициент отсутствует. Табл. 1 иллюстрирует этот процесс для примера $f(x)=x_1+x_2$.

Таблица 1

Результирующая таблица сгруппированных коэффициентов

b_{ij} / x	b_{00}	b_{01}	b_{02}	b_{03}
1	0	0	0	0
x_1	1	1	0	0
x_2	1	0	1	0
$x_1 x_2$	0	1	1	0

Подробное описание построения базиса Грёбнера, понятие которого было использовано Жаном Шарлем Фожером для определения алгебраической иммунности S-блоков, приводится в работе [9].

Приведем алгоритм вычисления алгебраической иммунности булевой функции, предлагаемый в работе [9] и оценим его возможную стандартную реализацию по объему вычислений.

4.1. Алгоритм вычисления алгебраической иммунности булевой функции

Вход: $n\in N$, функция $f(x)$ (заданная списком одночленов x^u с ненулевыми коэффициентами a_u в (3)).

Выход: Значение алгебраической иммунности $AI(f)$.

Шаг 1. Присваиваем $d=1$.

Шаг 2. Вычисляем пространство аннигиляторов $A_d^n(f)$ и $A_d^n(f+1)$.

Шаг 3. Если $A_d^n(f)=0$ и $A_d^n(f+1)=0$ присваиваем $d=d+1$ и переходим к шагу 2.

Шаг 4. Если $A_d^n(f)\neq 0$ и/или $A_d^n(f+1)\neq 0$ присваиваем $AI(f)=d$ и подаем на выход алгоритма.

Представленный алгоритм вычисляет алгебраическую иммунность для булевой функции $f(x)$. Для вычисления алгебраической иммунности S-блока по Арсу – Фожеру необходимо перевести (отобразить) нелинейный узел замены в булеву функцию $f(x)$ (таблицу истинности) в соответствии с (1). Чтобы подать на вход алгоритма булеву функцию $f(x)$, ее необходимо представить в виде полинома Жегалкина (3).

Далее обсуждаются возможности оптимизации алгоритма построения полинома Жегалкина.

4.2. Алгоритм приведения булевой функции, заданной в виде таблицы истинности, к алгебраической нормальной форме и оптимизация вычислений

Поиск значения коэффициентов мономов полинома Жегалкина происходит последовательно по всем мономам $a_u x^u$ из (2). В дальнейших рассуждениях вектор будем также представлять в виде целых чисел $U \in \left[0,..,2^n-1\right]: u=(u_1,...,u_n),\ u \in V_2^n$

$$U=\sum_{i=0}^{n-1} u_{i+1} 2^i, \tag{7}$$

а коэффициент $a_{(u_1,...,u_n)}$ одночлена $a_u x^u$ записывать в виде a_U.

Например, одночлену $x^u = x_1 x_2 x_4$ в (2) соответствует вектор $u=(1,1,0,1)$, который запишем как целое число $U=11$, коэффициент $a_{(1,1,0,1)}$ будем обозначать также как a_{11}.

Для заданного одночлена x^u введем определение *компонентных мономов*, под которыми будем понимать все такие ненулевые одночлены x^v, соответствующие вектора $v=(v_1,...,v_n)$ которых могут быть получены по правилу

$$v = u \wedge h = (u_1 \wedge h_1,...,u_n \wedge h_n), \tag{8}$$

где $\wedge$ – конъюнкция (логическая операция И), $h=(h_1,...,h_n)$ – произвольный вектор из V_2^n.

Очевидно, что целочисленное представление H векторов $h=(h_1,...,h_n)$ удовлетворяет условию $0<H<U$ и для поиска всех компонентных мономов необходимо по формуле (7) проверить $U-1$ одночленов. Например, для $x^u = x_1 x_2 x_4$ необходимо выполнить 10 проверок (для всех $0<H<U=11$), компонентными являются одночлены x^v: x_1, x_2, $x_1 x_2$, x_4, $x_1 x_4$, $x_2 x_4$ – им соответствуют целые числа $H=1,2,3,4,5,6$. Очевидно также, что целочисленные представления компонентных мономов также удовлетворяют условию $0<V<U$.

Пусть последовательность булевой функции $f(x)=\sum_{U=0}^{2^n-1} a_U x^U$ над V_2^n представлена в виде вектора двоичных значений $c=(c_0,...,c_{2^n-1})$. Тогда задача нахождения полинома Жегалкина состоит в решении системы линейных уравнений:

$$\begin{pmatrix} a_0 & 0 & 0 & 0 & ... & 0 \\ a_0 & a_1 & 0 & 0 & ... & 0 \\ a_0 & 0 & a_2 & 0 & ... & 0 \\ ... & ... & ... & ... & ... & ... \\ a_0 & a_1 & a_2 & a_3 & ... & a_{2^n-1} \end{pmatrix} = \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ ... \\ c_{2^n-1} \end{pmatrix}. \tag{9}$$

Например, для $n=2$ имеем систему

$$\begin{pmatrix} a_0 & 0 & 0 & 0 \\ a_0 & a_1 & 0 & 0 \\ a_0 & 0 & a_2 & 0 \\ a_0 & a_1 & a_2 & a_3 \end{pmatrix} = \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{pmatrix},$$

решение которой имеет вид

$$a_0 = a_{(0,0)} = c_0;\ a_1 = a_{(1,0)} = c_0 + c_1;\ a_2 = a_{(0,1)} = c_0 + c_2;\ a_3 = a_{(1,1)} = c_0 + c_1 + c_2 + c_3.$$

В общем случае для решения системы линейных уравнений методом Гаусса необходимо порядка $(2^n)^3$ операций сложений и умножений или, формально, $O\left((2^n)^3\right)$. Однако в данном случае алгоритм восстановления АНФ можно существенно упростить. Действительно, из предыдущего примера видно, что задачу нахождения коэффициентов $a_0, a_1 ..., a_{2^n-1}$ можно реализовать последовательно. Коэффициент $a_0 = c_0$ задан однозначно, а для нахождения каждого следующего коэффициента a_U необходимо решить линейное уравнение от одной неизвестной:

$$a_0 + a_1 + ... + a_U = c_U, \tag{10}$$

где в уравнение входят найденные на предыдущих шагах коэффициенты a_V компонентных мономов.

Например, для нахождения значения коэффициента a_9 монома второй степени x_1x_4 в соответствии с (10) имеем уравнение

$$a_0 + a_1 + a_8 + a_9 = c_9$$

где коэффициенты a_0, a_1, a_8 определены на предыдущих шагах алгоритма; c_9 – значение таблицы истинности булевой функции для монома x_1x_4.

С учетом (10) алгоритм приведения булевой функции к алгебраической нормальной форме запишем в следующем виде.

Алгоритм формирования полинома Жегалкина:

Вход: последовательность $c = (c_0, ..., c_{2^n-1})$ булевой функции $f(x)$;

Выход: строка коэффициентов $a_0, a_1 ..., a_{2^n-1}$ полинома Жегалкина булевой функции $f(x)$

Шаг 1. Принять $a_0 = c_0$;

Шаг 2. Принять $U = 1$, где U – десятичное представление одночлена в виде (3);

Шаг 3. Для одночлена U найти все компонентные мономы V, т.е. такие вектора $v = (v_1, ..., v_n)$, для которых выполняется равенство (4);

Шаг 4. Решить уравнение (6), т.е. найти a_U.

Шаг 5. Если $U \le 2^n - 1$ принять $U = U + 1$ и перейти к шагу 2. Иначе вывести строку коэффициентов $a_0, a_1 ..., a_{2^n-1}$.

Оценим сложность приведенного алгоритма.

Всего выполняется $2^n - 1$ проходов по внешнему циклу (для всех $U = 1, 2, ..., 2^n - 1$). На каждом проходе выполняется $U - 1$ операций логического И (для формирования компонентных мономов) и U операций двоичного сложения (для нахождения коэффициента a_U).

Число выполняемых операций двоичного сложения определяется как сумма членов арифметической прогрессии, для которой:

- первый член прогрессии равен 1 (число операций для вычисления коэффициента a_1);

- последний член прогрессии равен $2^n - 1$ (число операций для вычисления коэффициента a_U).

Сумма $2^n - 1$ членов прогрессии

$$\frac{1+2^n-1}{2}(2^n-1) = 2^{2n-1} - 2^{n-1}$$

операций двоичного сложения или, формально, сложность алгоритма – $O\left(2^{2n-1}\right)$.

Для подсчета числа операций логического И имеем арифметическую прогрессию:

- первый член которой равен 0 (для вычисления коэффициента a_1);

- последний член равен $2^n - 2$ (для вычисления коэффициента a_U), т.е. сумма $2^n - 1$ членов прогрессии

$$\frac{0+2^n-2}{2}(2^n-1) = 2^{2n-1} + 2^n - 2^{n-1} - 1$$

или, формально, сложность алгоритма равна $O\left(2^{2n-1}\right)$.

Очевидно, что рассмотренный алгоритм приведения булевой функции к алгебраической нормальной форме значительно проще общего случая вычисления коэффициентов $a_0, a_1 ..., a_{2^n-1}$ через решение системы линейных уравнений (5).

Возвращаясь к общему алгоритму вычисления алгебраической иммунности, зная, как привести булеву функцию к алгебраической нормальной форме, запишем алгоритм вычисления алгебраической иммунности S-блока:

Алгоритм вычисления алгебраической иммунности S-блока:

Вход: Нелинейный узел замены (S-блок) степени $n \in N$.

Выход: Значение алгебраической иммунности нелинейного узла замены.

Шаг 1. Преобразуем нелинейный узел замены (S-блок) степени n в булеву функцию $f(x)$ от $2n$ переменных.

Шаг 2. Приведем булеву функцию $f(x)$ к виду полинома Жегалкина.

Шаг 3. Присваиваем $d = 1$.

Шаг 4. Вычисляем пространство аннигиляторов $A_d^n(f)$ и $A_d^n(f+1)$.

Шаг 5. Если $A_d^n(f) = 0$ и $A_d^n(f+1) = 0$ – присваиваем $d = d + 1$ и переходим к шагу 2.

Шаг 6. Если $A_d^n(f) \neq 0$ и/или $A_d^n(f+1) \neq 0$ – присваиваем $AI(f) = d$ и подаем на выход алгоритма.

Для реализации такого алгоритма подсчета АИ байтового S-блока, то есть булевой функции 16-ти переменных (n = 16), необходимо иметь таблицу размерами $2^{16} \times 2^{16}$. Для хранения одной такой таблицы, которая содержит результат умножения всех возможных мономов полинома $f(x)$ на мономы аннигилирующего полинома $g(x)$, необходимо приблизительно 8.5 Гб ОЗУ на ПК, с учетом того что каждое число в таблице может занимать 2 байта, это без учета вспомогательных таблиц, которые могут также понадобится в ходе вычислений. Ресурсы ОЗУ, которые занимает таблица, нетрудно вычислить, так как это произведение трех сомножителей. Количество строк таблицы, количество столбов таблицы и размер одной ячейки таблицы.

Если говорить о количестве операций, нам понадобятся неоднократные проходы по всей таблице (2^{32} операций на один проход) для решения систем линейных уравнений.

Оптимизированный алгоритм подсчета АИ

Известно, что значение алгебраической иммунности S-блока не может быть больше чем, $n/2$ [2], следовательно, для байтового S-блока значение алгебраической иммунности не мо-

жет быть больше 4. Если вспомнить, что алгебраическая иммунность определяется минимальной степенью ненулевых полиномов $AI(s) = \min \deg Ann(f_s)$, то можно сказать что в результирующей группировке неизвестных коэффициентов b_v, не может оказаться мономов степени выше 4, где b_v – неизвестные коэффициенты аннигилятора. Следовательно, при построении таблицы перемножения всех мономов полинома $f(x)$ на мономы полинома $g(x)$ мы можем брать только те мономы полинома $g(x)$, у которых степень будет меньше, либо равна $n/2$ (для байтового S-блока это четверка).

Количество подходящих нам мономов полинома $g(x)$ в худшем случае, нетрудно посчитать по формуле

$$k = \sum_{i=1}^{n/2} C_{2n}^{i}.$$

Зная, что максимальная АИ не может быть больше $n/2$ и не получив решения системы уравнений для максимальной степени монома $n/2-1$, можно сделать вывод, что АИ будет равным $n/2$. То есть формула подсчета количество подходящих нам мономов полинома $g(x)$ на самом деле будет выглядеть так:

$$k = \sum_{i=1}^{n/2-1} C_{2n}^{i}. \qquad (11)$$

Для байтового S-блока по Арсу – Фожеру получим:

$$k = C_{16}^{1} + C_{16}^{2} + C_{16}^{3}.$$
$$k = 696.$$

Итого, 696 мономов вместо 65536 для байтового S-блока.

Далее все вычисления при расчете максимально возможного значения алгебраической иммунности будут происходить уже с таблицей размерами (65536×696), а это уже $< 2^{26}$ операций для прохода по всей таблице, вместо 2^{32}. И около 0.1 Гб ОЗУ на ПК, вместо 8.5 Гб для хранения одной такой таблицы.

Если рассматривать расчет АИ для блоков нелинейной замены различных степеней, то размер ячейки таблицы должен быть равен 1 байт при подсчете АИ S-box степени меньше либо равной 2^4, 2 байта для S-box степени меньше, либо равной 2^8 и 4 байта для подсчета АИ S-box степени от 2^8 до 2^{16}. Для универсальности расчетов и наглядности примем размер ячейки таблицы равным 4 байта, для любых степеней блока нелинейной замены, до 2^{16}.

Ниже приведена табл. 2, показывающая эффективность оптимизированного алгоритма подсчета АИ S-box по сравнению со стандартным, размер ячейки таблицы принят равным 4 байта для любых степеней блока нелинейной замены.

Таблица 2

Затраты ОЗУ для построения таблицы перемножения мономов, используемой в алгоритмах подсчета АИ для S-box

Алгоритм / Степень S-box	Стандартный	Оптимизированный
2^4	0,26 Мб ОЗУ	0,008 Мб ОЗУ
2^6	67,1 Мб ОЗУ	1,3 Мб ОЗУ
2^8	17,2 Гб ОЗУ	182 Мб ОЗУ
2^9	275 Гб ОЗУ	1,03 Гб ОЗУ
2^{10}	4398 Гб ОЗУ	26 Гб ОЗУ
2^{11}	70369 Гб ОЗУ	153 Гб ОЗУ
2^{12}	1126 Тб ОЗУ	3721 Гб ОЗУ

Получившиеся результаты показывают очень весомую разницу затрат ресурсов ОЗУ на ПК между оптимизированным алгоритмом и обычным.

Возвращаясь к способу оптимизации, отметим, что возникает только одна проблема – мономы полинома никак не упорядочены по степеням и хранятся в произвольном порядке относительно степеней, а точнее в порядке, который задает арифметика цифр (0...65536). Например, моном первой степени можно встретить в позициях (1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768), где позиции большие, чем 696 никак не вписываются в нашу оптимизацию. Для решения этой проблемы, необходимо сгруппировать полином $g(x)$ таким образом, чтобы мономы были упорядочены по степеням. Например, можно хранить позиции интересующих нас мономов отдельно и обращаться только к нужным позициям. Это позволит работать с таблицей (65536×696), вместо (65536×65536)

Пример 2.

Дан S-блок 2-й степени и соответствующая ему булева функция от 4-х переменных, в виде полинома Жегалкина. $f(x) = x_1 + x_1x_2 + x_3 + x_2x_3 + x_1x_4 + x_3x_4$.

Запишем аннигилирующий полином с искомыми коэффициентами b в общем виде

$$g(x) = b_0 + b_1x_1 + b_2x_2 + b_3x_1x_2 + b_4x_3 +$$
$$+b_5x_1x_3 + b_6x_2x_3 + b_7x_1x_2x_3 + b_8x_4 +$$
$$+b_9x_1x_4 + b_{10}x_2x_4 + b_{11}x_1x_2x_4 + b_{12}x_3x_4 +$$
$$+b_{13}x_1x_3x_4 + b_{14}x_2x_3x_4 + b_{15}x_1x_2x_3x_4.$$

Для подсчета АИ исходного S-блока необходимо построить таблицу перемножения всех мономов полинома $f(x)$ на мономы полинома $g(x)$. Для нашего примера она имеет вид, представленный в табл. 3 (число столбцов ограничено из-за недостаточности места в таблице, они не влияют на результаты, так как имеют нулевые значения ячеек). На входы по столбцам таблицы подаются мономы полинома $f(x)$, на входы по строкам подаются мономы полинома $g(x)$. Ячейки таблицы – результат умножения монома строки на моном столбца.

Таблица 3

Результаты умножения мономов полиномов $f(x)$ и $g(x)$

$g(x)$ \ $f(x)$	0	x_1	0	x_1x_2	x_3	0	x_2x_3	0	0	x_1x_4	0	0	x_3x_4
b_0	0	x_1	0	x_1x_2	x_3	0	x_2x_3	0	0	x_1x_4	0	0	x_3x_4
$b_1\ x_1$	0	x_1	0	x_1x_2	x_1x_3	0	$x_1x_2x_3$	0	0	x_1x_4	0	0	$x_1x_3x_4$
$b_2\ x_2$	0	x_1x_2	0	x_1x_2	x_2x_3	0	x_2x_3	0	0	$x_1x_2x_4$	0	0	$x_2x_3x_4$
$b_3\ x_1x_2$	0	x_1x_2	0	x_1x_2	$x_1x_2x_3$	0	$x_1\ x_2x_3$	0	0	$x_1x_2x_4$	0	0	$x_1x_2x_3x_4$
$b_4\ x_3$	0	x_1x_3	0	$x_1x_2x_3$	x_3	0	x_2x_3	0	0	$x_1x_3x_4$	0	0	x_3x_4
$b_5\ x_1x_3$	0	x_1x_3	0	$x_1x_2x_3$	x_1x_3	0	$x_1x_2x_3$	0	0	$x_1x_3x_4$	0	0	$x_1x_3x_4$
$b_6\ x_2x_3$	0	$x_1\ x_2x_3$	0	$x_1x_2x_3$	x_2x_3	0	x_2x_3	0	0	$x_1x_2x_3x_4$	0	0	$x_2x_3x_4$
$b_7\ x_1x_2x_3$	0	$x_1x_2x_3$	0	$x_1x_2x_3$	$x_1x_2x_3$	0	$x_1x_2x_3$	0	0	$x_1x_2x_3x_4$	0	0	$x_1\ x_2x_3x_4$
$b_8\ x_4$	0	x_1x_4	0	$x_1x_2x_4$	x_3x_4	0	$x_2x_3x_4$	0	0	x_1x_4	0	0	x_3x_4
$b_9\ x_1x_4$	0	x_1x_4	0	$x_1x_2x_4$	$x_1x_3x_4$	0	$x_1x_2x_3x_4$	0	0	x_1x_4	0	0	$x_1x_3x_4$
$b_{10}\ x_2x_4$	0	$x_1x_2x_4$	0	$x_1x_2x_4$	$x_2x_3x_4$	0	$x_2x_3x_4$	0	0	$x_1x_2x_4$	0	0	$x_2x_3x_4$
$b_{11}\ x_1x_2x_4$	0	$x_1x_2x_4$	0	$x_1x_2x_4$	$x_1x_2x_3x_4$	0	$x_1x_2x_3x_4$	0	0	$x_1x_2x_4$	0	0	$x_1x_2x_3x_4$
$b_{12}\ x_3x_4$	0	$x_1x_3x_4$	0	$x_1x_2x_3x_4$	x_3x_4	0	$x_2x_3x_4$	0	0	$x_1x_3x_4$	0	0	x_3x_4
$b_{13}\ x_1x_3x_4$	0	$x_1x_3x_4$	0	$x_1x_2x_3x_4$	$x_1x_3x_4$	0	$x_1x_2x_3x_4$	0	0	$x_1x_3x_4$	0	0	$x_1x_3x_4$
$b_{14}\ x_2x_3x_4$	0	$x_1x_2x_3x_4$	0	$x_1x_2x_3x_4$	$x_2x_3x_4$	0	$x_2x_3x_4$	0	0	$x_1x_2x_3x_4$	0	0	$x_2x_3x_4$
$b_{15}\ x_1x_2x_3x_4$	0	$x_1x_2x_3x_4$	0	$x_1x_2x_3x_4$	$x_1x_2x_3x_4$	0	$x_1x_2x_3x_4$	0	0	$x_1x_2x_3x_4$	0	0	$x_1x_2x_3x_4$

Далее происходит группировка неизвестных коэффициентов по всем возможным мономам от 0 до 2^n. Строится таблица сгруппированных неизвестных коэффициентов b_v (см. табл. 4) На входы по строкам подаются все возможные варианты мономов, входы по столб-

цам соответствуют неизвестным коэффициентам b_v (единица обозначает присутствие коэффициента соответствующего монома, а ноль – его отсутствие). Значение ячейки может быть равно нулю, если в табл. 3 нет мономов таких, как моном текущей строки, или если таких мономов четное количество в конкретной строке табл. 3. Значение ячейки таблицы может быть равно единице для некоторой строки *x* и некоторого столбца *y*, если в строке *y* табл. 3 есть нечетное количество мономов *x*.

Практически, заполнение каждой строки табл. 4. соответствует множеству неизвестных коэффициентов (их позиции обозначены единицами) и соответствует одному из уравнений (его левой части) системы линейных уравнений, задаваемых таблицей. Для вычисления АИ далее необходимо решить полученную систему уравнений, например, методом Гаусса. Полученные решения – это пространство аннигиляторов. Воспользовавшись алгоритмом вычисления алгебраической иммунности S-блока начиная с шага 3, находим АИ.

Для оптимизированного варианта вычисления АИ при построении аннигилирующего полинома $g(x)$ необходимо найти количество мономов, которые будут входить в оптимизированный вариант полинома $g(x)$ по формуле (11). Далее найти все мономы, степень которых будет не больше *n*/2 и построить оптимизированный полином $g(x)$, который будет состоять из найденных подходящих мономов. Напомним, что в общем виде мономы никак не упорядочены по степеням, поэтому взять нужные мономы на позициях от 0 до $2^{2n}-1$ не получится. Необходимо найти на каких именно позициях находятся мономы степени не выше *n*/2. Далее аналогично стандартному варианту вычислений строятся табл. 3 и 4, только размер этих таблиц будет значительно меньше. В оптимизированном варианте будут использоваться только строки и столбцы, выделенные в табл. 3 и 4 цветом. Видно, что объем обрабатываемых данных, участвующих в вычислениях, существенно уменьшается. Для вычисления АИ также решается система линейных уравнений, например, методом Гаусса и ищется АИ алгоритмом вычисления алгебраической иммунности S-блока.

Таблица 4

Группировка мономов по неизвестным коэффициентам
(формирование левых частей уравнений)

x \ b_i	b_0	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	b_9	b_{10}	b_{11}	b_{12}	b_{13}	b_{14}	b_{15}
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
x_1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
x_2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
x_1x_2	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
x_3	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
x_1x_3	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0
x_2x_3	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
$x_1x_2x_3$	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0
x_4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
x_1x_4	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
x_2x_4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$x_1x_2x_4$	0	0	1	1	0	0	0	0	1	1	1	1	0	0	0	0
x_3x_4	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
$x_1x_3x_4$	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0
$x_2x_3x_4$	0	0	1	0	0	0	1	0	1	0	1	0	1	0	1	0
$x_1x_2x_3x_4$	0	0	0	1	0	0	1	0	0	1	0	1	1	0	1	0

Для еще большей оптимизации мы можем строить аннигилирующий полином $g(x)$ не из всех степеней мономов, не превышающих *n*/2, а из степеней мономов, не превышающих $i \in 1\ldots n/2$. То есть на первой итерации будет строиться полином $g(x)$, состоящий из мономов,

не превышающих 1-й степени, количество таких мономов будет C_{2n}^1. Если результат решения системы получившихся уравнений не даст ни одного ненулевого решения, то d принимается равным $d\_+ 1$, и строится аннигилирующий полином размером уже $C_{2n}^1 + C_{2n}^2$, степень мономов которого не превышает 2. Так происходит до тех пор, пока в результате решения системы линейных уравнений не будет найдено хотя бы одно ненулевое решение. Выход из алгоритма $AI(f) = d$.

Дополнительная оптимизация затрат ОЗУ на ПК при реализации поиска алгебраической иммунности блока нелинейной замены по Арсу – Фожеру.

Отметим, что основные затраты ОЗУ на ПК занимала табл. 3 перемножения полиномов $f(x)$ и $g(x)$, и именно о сжатии этой таблицы шла речь как об основном результате оптимизации. Этот результат впоследствии позволил посчитать АИ для S-box степени 2^9, требуя всего около 1 Гб ОЗУ, в то время как неоптимизированный алгоритм для подсчета S-box той же степени требовал бы около 275 Гб ОЗУ для хранения одной только такой таблицы. Но вычислить АИ для S-box степени 2^{10} и выше уже не представлялось возможным, по крайней мере, на обычном ПК. Напомним, что для хранения табл. 3 для S-box степени 2^{10} оптимизированный алгоритм требовал уже 26 Гб ОЗУ. Весомость затрат таблицы обусловлена необходимостью содержать в каждой ячейке 4 байта для возможности хранения монома максимальной степени 2^{2n}.

Первым делом можно попытаться сократить количество столбцов этой таблицы. Как говорилось выше, мы должны брать все возможные мономы $f(x)$ и не можем уменьшить количество столбцов. На самом деле это не совсем так, мы можем уменьшить количество столбцов, исключив нулевые столбцы, заведомо зная, что они всегда будут получаться в результате умножения на нулевой моном полинома $f(x)$. Но, сколько таких мономов будут иметь различные полиномы $f(x)$ мы знать, конечно же, не можем. В худшем случае $f(x)$ может иметь 2^{2n} ненулевых мономов, поэтому существенной оптимизации это нам не даст.

Более весомая оптимизация будет строиться на возможности не хранить в ОЗУ сразу не всю табл. 3 перемножения полиномов $f(x)$ и $g(x)$, а хранить только одну строку этой таблицы. Одна строка табл. 3 позволяет полностью построить один столбец табл. 4, таблицы группировки мономов по неизвестным коэффициентам (формирование левых частей уравнений). Таким образом, храня в ОЗУ одну строку табл. 3, затем удаляя ее из ОЗУ и заменяя ее на следующую строку табл. 3, мы можем полностью построить табл. 4. Отсюда следует, что затраты ОЗУ на хранения табл. 3 практически отсутствуют и основные затраты ресурсов ОЗУ на ПК для подсчета АИ блока нелинейной замены будет теперь занимать табл. 4.

Таблица 5

Затраты ОЗУ для построения таблицы, используемой в алгоритмах подсчета АИ для S-box при различных методах оптимизации

Алгоритм / Степень S-box	Стандартный	Оптимизированный	Дополнительная оптимизация
2^4	0,26 Мб ОЗУ	0,008 Мб ОЗУ	0,002 Мб ОЗУ
2^6	67,1 Мб ОЗУ	1,3 Мб ОЗУ	0,3 Мб ОЗУ
2^8	17,2 Гб ОЗУ	182 Мб ОЗУ	45 Мб ОЗУ
2^9	275 Гб ОЗУ	1,03 Гб ОЗУ	250 Мб ОЗУ
2^{10}	4398 Гб ОЗУ	26 Гб ОЗУ	6,5 Гб ОЗУ
2^{11}	70369 Гб ОЗУ	153 Гб ОЗУ	38 Гб ОЗУ
2^{12}	1126 Тб ОЗУ……	3721 Гб ОЗУ	930 Гб ОЗУ

5. Эксперименты

Для проведения тестов использовался ПК с Windows 10, Intel Core i7-3630QM 2.4 Ггц, 8Гб ОЗУ

Первая часть экспериментов была посвящена изучению быстродействия различных алгоритмов вычисления АИ на примере блоков нелинейной замены степени 2^8, использовались узлы нелинейной замены шифров AES и Калина (см. рис. 2, 3).

Алгебраическая иммунность S-блока шифра AES (см. рис. 2) получается равной 2. Воспользовавшись выражением (16), имеем: $k = C_{16}^1 + C_{16}^2$, k = 136.

Алгебраическая иммунность S-блока шифра Калина (см. рис. 3) получается равной 3. Воспользовавшись выражением (16), имеем: $k = C_{16}^1 + C_{16}^2 + C_{16}^3$, k = 696.

Именно такие значения АИ получены с помощью комплекса Magma в работе [9].

Время выполнения вычислений для стандартного алгоритма выходит за приемлемые сроки. Оптимизированный алгоритм вычислений выполнил поставленную задачу за 4 с для S-блока AES и за 20 с для S-блока Калина-2 соответственно. Алгоритм на основе базисов Грёбнера с помощью комплекса Magma [9] справился с поставленной задачей за 5 с.

```
0x63 0x7c 0x77 0x7b 0xf2 0x6b 0x6f 0xc5 0x30 0x01 0x67 0x2b 0xfe 0xd7 0xab 0x76
0xca 0x82 0xc9 0x7d 0xfa 0x59 0x47 0xf0 0xad 0xd4 0xa2 0xaf 0x9c 0xa4 0x72 0xc0
0xb7 0xfd 0x93 0x26 0x36 0x3f 0xf7 0xcc 0x34 0xa5 0xe5 0xf1 0x71 0xd8 0x31 0x15
0x04 0xc7 0x23 0xc3 0x18 0x96 0x05 0x9a 0x07 0x12 0x80 0xe2 0xeb 0x27 0xb2 0x75
0x09 0x83 0x2c 0x1a 0x1b 0x6e 0x5a 0xa0 0x52 0x3b 0xd6 0xb3 0x29 0xe3 0x2f 0x84
0x53 0xd1 0x00 0xed 0x20 0xfc 0xb1 0x5b 0x6a 0xcb 0xbe 0x39 0x4a 0x4c 0x58 0xcf
0xd0 0xef 0xaa 0xfb 0x43 0x4d 0x33 0x85 0x45 0xf9 0x02 0x7f 0x50 0x3c 0x9f 0xa8
0x51 0xa3 0x40 0x8f 0x92 0x9d 0x38 0xf5 0xbc 0xb6 0xda 0x21 0x10 0xff 0xf3 0xd2
0xcd 0x0c 0x13 0xec 0x5f 0x97 0x44 0x17 0xc4 0xa7 0x7e 0x3d 0x64 0x5d 0x19 0x73
0x60 0x81 0x4f 0xdc 0x22 0x2a 0x90 0x88 0x46 0xee 0xb8 0x14 0xde 0x5e 0x0b 0xdb
0xe0 0x32 0x3a 0x0a 0x49 0x06 0x24 0x5c 0xc2 0xd3 0xac 0x62 0x91 0x95 0xe4 0x79
0xe7 0xc8 0x37 0x6d 0x8d 0xd5 0x4e 0xa9 0x6c 0x56 0xf4 0xea 0x65 0x7a 0xae 0x08
0xba 0x78 0x25 0x2e 0x1c 0xa6 0xb4 0xc6 0xe8 0xdd 0x74 0x1f 0x4b 0xbd 0x8b 0x8a
0x70 0x3e 0xb5 0x66 0x48 0x03 0xf6 0x0e 0x61 0x35 0x57 0xb9 0x86 0xc1 0x1d 0x9e
0xe1 0xf8 0x98 0x11 0x69 0xd9 0x8e 0x94 0x9b 0x1e 0x87 0xe9 0xce 0x55 0x28 0xdf
0x8c 0xa1 0x89 0x0d 0xbf 0xe6 0x42 0x68 0x41 0x99 0x2d 0x0f 0xb0 0x54 0xbb 0x16
```

Рис. 2. S-блок шифра AES

```
0xA8 0x43 0x5F 0x06 0x6B 0x75 0x6C 0x59 0x71 0xDF 0x87 0x95 0x17 0xF0 0xD8 0x09
0x6D 0xF3 0x1D 0xCB 0xC9 0x4D 0x2C 0xAF 0x79 0xE0 0x97 0xFD 0x6F 0x4B 0x45 0x39
0x3E 0xDD 0xA3 0x4F 0xB4 0xB6 0x9A 0x0E 0x1F 0xBF 0x15 0xE1 0x49 0xD2 0x93 0xC6
0x92 0x72 0x9E 0x61 0xD1 0x63 0xFA 0xEE 0xF4 0x19 0xD5 0xAD 0x58 0xA4 0xBB 0xA1
0xDC 0xF2 0x83 0x37 0x42 0xE4 0x7A 0x32 0x9C 0xCC 0xAB 0x4A 0x8F 0x6E 0x04 0x27
0x2E 0xE7 0xE2 0x5A 0x96 0x16 0x23 0x2B 0xC2 0x65 0x66 0x0F 0xBC 0xA9 0x47 0x41
0x34 0x48 0xFC 0xB7 0x6A 0x88 0xA5 0x53 0x86 0xF9 0x5B 0xDB 0x38 0x7B 0xC3 0x1E
0x22 0x33 0x24 0x28 0x36 0xC7 0xB2 0x3B 0x8E 0x77 0xBA 0xF5 0x14 0x9F 0x08 0x55
0x9B 0x4C 0xFE 0x60 0x5C 0xDA 0x18 0x46 0xCD 0x7D 0x21 0xB0 0x3F 0x1B 0x89 0xFF
0xEB 0x84 0x69 0x3A 0x9D 0xD7 0xD3 0x70 0x67 0x40 0xB5 0xDE 0x5D 0x30 0x91 0xB1
0x78 0x11 0x01 0xE5 0x00 0x68 0x98 0xA0 0xC5 0x02 0xA6 0x74 0x2D 0x0B 0xA2 0x76
0xB3 0xBE 0xCE 0xBD 0xAE 0xE9 0x8A 0x31 0x1C 0xEC 0xF1 0x99 0x94 0xAA 0xF6 0x26
0x2F 0xEF 0xE8 0x8C 0x35 0x03 0xD4 0x7F 0xFB 0x05 0xC1 0x5E 0x90 0x20 0x3D 0x82
0xF7 0xEA 0x0A 0x0D 0x7E 0xF8 0x50 0x1A 0xC4 0x07 0x57 0xB8 0x3C 0x62 0xE3 0xC8
0xAC 0x52 0x64 0x10 0xD0 0xD9 0x13 0x0C 0x12 0x29 0x51 0xB9 0xCF 0xD6 0x73 0x8D
0x81 0x54 0xC0 0xED 0x4E 0x44 0xA7 0x2A 0x85 0x25 0xE6 0xCA 0x7C 0x8B 0x56 0x80
```

Рис. 3. S-блок шифра Калина

Вторая часть экспериментов была посвящена изучению возможностей различных алгоритмов поиска АИ относительно ресурсов ОЗУ на ПК, а именно – максимально возможной степени нелинейного узла замены, алгебраическую иммунность которого позволяют вычислить рассмотренные алгоритмы. Именно здесь сыграет свою роль алгоритм по методу Арсу – Фожера с дополнительной оптимизацией относительно ресурсов ОЗУ на ПК.

Результаты экспериментов показали, что неоптимизированный алгоритм по методу Арсу – Фожера не смог справиться с поставленной задачей из-за нехватки ресурсов ОЗУ на ПК уже при блоке нелинейной замены степени 2^9. Оптимизированный алгоритм по методу Арсу – Фожера преодолел эту сложность, но не смог справиться с блоком нелинейной замены степени 2^{10}. Алгоритм с дополнительной оптимизацией ОЗУ и алгоритм, реализованный с помощью комплекса Magma [9], справились с S-блоком степени 2^{10}. Таким образом, S-блок степени 2^{10} стал максимально возможным для вычисления АИ этими алгоритмами. Далее были проведен ряд тестов с использованием случайно сгенерированных S-блоков степени 2^{10}, а также детерминированного S-блока степени 2^{10}, состоящего из мультипликативно-обратных элементов поля.

Алгебраическая иммунность ряда случайно сгенерированных S-блоков степени 2^{10} получилась равной 3, что подтвердили оба алгоритма. При этом алгоритм по методу Арсу – Фожера с дополнительной оптимизацией выполнил задачу за 15 мин. Алгоритм, реализованный с помощью комплекса Magma [9], справился с задачей за 30 мин.

Алгебраическая иммунность S-блока, состоящего из мультипликативно-обратных элементов поля, получилась равной 2, что подтвердили оба алгоритма. При этом алгоритм по методу Арсу – Фожера с дополнительной оптимизацией выполнил задачу за 1 мин и 40 с. Алгоритм, реализованный с помощью комплекса Magma [9], справился с задачей за 30 мин.

6. Обсуждение

Рассмотрены детали реализации алгоритма расчета алгебраической иммунности по методу Арсу – Фожера. Проведены тесты, показавшие невозможность расчета АИ для байтовых S-блоков в связи с нехваткой вычислительных ресурсов. Время выполнения известного алгоритма вычисления АИ для байтовых S-блоков превышает приемлемые сроки.

Предложен ускоренный алгоритм расчета алгебраической иммунности, байтовых S-блоков по методу Арсу – Фожера, в котором используются реально существующие практические и теоретические ограничения, характерные для оцениваемого показателя. Он позволяет существенно сократить объемы обрабатываемой информации. В качестве таких ограничений использовано то, что в соответствии с теоретическими расчетами алгебраическая иммунность для байтовых S-блоков не может превышать значения 4, т.е. степень аннулирующего многочлена не может быть выше четвертой.

Последующая операция приведения сокращенной по числу столбцов матрицы коэффициентов к диагональному виду позволяет сократить размеры матрицы коэффициентов и по числу строк (появляются строки из одних нулей). В результате действительно удается существенно ускорить процедуру выполнения вычислений.

Предложен также ускоренный алгоритм расчета алгебраической иммунности по методу Арсу – Фожера с дополнительной оптимизацией ресурсов ОЗУ на ПК, что позволяет вычислять блоки нелинейной замены степени до 2^{10} включительно.

Результаты вычислений были проверены алгоритмом, реализованным с помощью комплекса Magma [9], также проведены сравнительные тесты быстродействия.

Предложена усовершенствованная процедура формирования полиномов Жегалкина по заданному значению таблицы истинности булевой функции S-блока.

7. Выводы

Основным результатом статьи является разработка ускоренного метода расчета алгебраической иммунности байтовых S-блоков, а также ускоренного метода расчета алгебраической иммунности с дополнительной оптимизацией относительно ресурсов ОЗУ на ПК.

Исключение при формировании программы множеств данных, не участвующих на каждом из этапов ее работы, а также учет априорно известных данных относительно конечного результата позволили существенно сократить объемы промежуточных вычислений и добиться повышения производительности программы в сотни раз. Усовершенствована также про-

цедура формирования полиномов Жегалкина по заданному значению таблицы истинности булевой функции S-блока.

Время работы программы при расчете алгебраической иммунности байтового S-блока сосоставляет от 4 до 20 с в зависимости от S-блока. Удалось вычислить АИ для S-блока степени 2^{10}, время работы программы при этом со значением АИ равной 3 составляет около 15 мин и со значением АИ равной 2 – около 2 мин. Таким образом, самым перспективным алгоритмом расчета АИ можно считать предложенный ускоренный алгоритм с дополнительной оптимизацией ресурсов ОЗУ, что в сотни раз быстрее, чем неоптимизированный алгоритм по методу Арсу – Фожера и в несколько раз быстрее алгоритма, реализованного в комплексе Magma [9] для максимальной степени S-блока 2^{10}.

Список литературы:

1. Courtois N. and Meier W. Algebraic attacks on stream ciphers with linear feedback // Eurocrypt'2003. LNCS. 2003. V. 2656. P. 345-359.

2. Покрасенко Д.П. Об алгебраической иммунности векторных булевых функций // Прикладная дискретная математика. Приложение. 2014. № 7. С. 43-48.

3. Meier W., Pasalic E., and Carlet C. Algebraic attacks and decomposition of Boolean functions // Eurocrypt'2004. LNCS. 2004. V. 3027. P. 474-491.

4. Armknecht F. and Krause M. Constructing single- and multi-output Boolean functions with maximal immunity // ICALP'2006. LNCS. 2006. V. 4052. P. 180-191.

5. Armknecht F. and Krause H. Constructing single- and multi-output Boolean functions with maximal immunity // ICALP'2006. V.4052. P. 180-191.

6. Ars G. and Faug`ere J.-C. Algebraic immunities of functions over finite fields // Proc. Conf. BFCA. 2005. P. 21-38.

7. Carlet C. On the algebraic immunities and higher order nonlinearities of vectorial Boolean functions // Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes. Amsterdam: IOS Press, 2009. P. 104-116.

8. Faugère J.-C. (June 1999). A new efficient algorithm for computing Gröbner bases (F4) // Journal of Pure and Applied Algebra. Elsevier Science. 139 (1): 61-88.

9. Покрасенко Д.П. Компонентная алгебраическая иммунность S-блоков, использующихся в некоторых блочных шифрах // Прикладная дискретная математика. Приложение. 2017. № 10. С. 49-51.

10. Кузнецов О.О. Алгебраїчний імунітет нелінійних вузлів симетричних шифрів / О.О. Кузнецов, Ю.І. Горбенко, І.М. Білозерцев та інші // Радиотехника. 2017. Вып. 189. С. 47-58.

11. Magma Computational Algebra System. Available at: http://magma.maths.usyd.edu.au/magma.

12. Баев В. В. Эффективные алгоритмы получения оценок алгебраической иммунности булевых функций : дис. … канд. физ.-мат. наук : 01.01.09 / Баев Владимир Валерьевич; Место защиты: Моск. гос. ун-т им. М.В. Ломоносова. Фак. вычислит. математики и кибернетики. Москва, 2008. 101 с.

13. Gw´enol´e Ars, Jean-Charles Faug`ere. Algebraic Immunities of functions over finite fields // Research Report. RR-5532, INRIA. 2005. P.17.

14. Аржанцев И.В. Базисы Грёбнера и системы алгебраических уравнений. Летняя школа. Современная математика. Дубна, июль 2002. Москва : МЦНМО, 2003. 68 с

15. Злобин А.И., Соколова О.В. Компьютерная алгебра в системе Sage : учеб. пособие. Москва : МГТУ им. Баумана, 2011. 55 с.

16. Faugère, J.-C. (June 1999). A new efficient algorithm for computing Gröbner bases (F4). Journal of Pure and Applied Algebra. Elsevier Science. 139 (1): 61-88.

17. Faugère, J.-C. (July 2002). A new efficient algorithm for computing Gröbner bases without reduction to zero (F5) // Proceedings of the 2002 international symposium on Symbolic and algebraic computation (ISSAC). ACM Press. P.75-83.

18. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. Handbook of Applied Cryptography CRC Press, 1997. 794 p.

19. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Теорія. Практика. Застосування : підручник для вищих навч. закладів. Харків : Форт, 2013. 880 с.

20. Bart Preneel. Analysis and Design of Cryptographic Hash Functions. Электронный ресурс. Режим доступа: homes.esat.kuleuven.be/~preneel/phd_preneel_feb1993.pdf

21. Carlet C. Vectorial Boolean functions for // Cambridge Univ. Press, Cambridge. 95 p. Электронный ресурс. Режим доступа: www.math.univ-paris13.fr/~carlet/chap-vectorial-fcts-corr.pdf

22. Carlet C. Boolean functions for cryptography and error correcting codes // Cambridge Univ. Press, Cambridge. 2007. 148 p. Электронный ресурс. Режим доступа: www1.spms.ntu.edu.sg/~kkhoongm/chap-fcts-Bool.pdf.

23. Zhuo Zepeng, Zhang Weiguo On correlation properties of Boolean functions // Chinese Journal of Electronics. 2011. Vol.20. №1. P. 143-146.

24. O'Connor L. An analysis of a class of algorithms for S-box construction // J. Cryptology. 1994. P. 133-151.

25. Clark J.A., Jacob J.L., Stepney S. The Design of S-Boxes by Simulated Annealing // New Generation Computing. 2005. 23(3). P.219-231.

26. Кузнецов А.А., Белозерцев И.Н., Андрушкевич А.В. Анализ и сравнительные исследования нелинейных узлов замены современных блочных симметричных шифров // Прикладная радиоэлектроника. Харьков : ХНУРЭ. 2015. Т. 14. №4. С.343-350.

27. Massimiliano Sala, Teo Mora, Ludovic Perret, Shojiro Sakata, Carlo Traverso Gröbner Bases, Coding, and Cryptography. Springer-Verlag Berlin Heidelberg. 426 p.

Харьковский национальный
университет имени В.Н. Каразина

Поступила в редколлегию 18.01.2020

МЕТОДИ ТА МЕХАНІЗМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМІ БЛОКЧЕЙН

УДК 004.056.5 **DOI:10.30837/rt.2020.1.200.08**

І.Д. ГОРБЕНКО, д-р техн. наук, В.В. ОНОПРІЄНКО, канд. техн. наук,
Ю.І. ГОРБЕНКО, канд. техн. наук, О.О. КУЗНЕЦОВ, д-р техн. наук,
К.В. ІСІРОВА, М.Ю. РОДІНКО

ПРОБЛЕМИ, ПРИНЦИПИ ПОБУДОВИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ НАЦІОНАЛЬНОЇ СИСТЕМИ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ В УКРАЇНІ

Вступ

Голосування у демократичних країнах є головним способом прийняття важливих рішень, що стосуються нації, держави, уряду, суспільних чи політичних подій, тощо. Волевиявлення проводиться при призначенні виборних осіб, президентів та парламенту, інколи суддів та шерифів, та є обов'язковою складовою представницької демократії. Зокрема, голосування реалізується і через основну форму прямого народовладдя – референдуми, народні збори, національні опитування, тощо.

Перебіг голосування, як і ступінь довіри до отриманих результатів волевиявлення, безпосередньо залежить від чесності організаторів та прозорості їх дій. Зокрема, в історії людства існує багато прикладів, коли свавілля та беззаконня можновладців спотворювало не тільки результати голосування, але і базові принципи демократії, роблячи народ безмовним покірним стадом, прикриваючись при цьому гаслами боротьби за «світле майбутнє» і добробут народу. Відомий вислів Наполеона III, що перефразовано Йосипом Сталіним: «Неважливо, як проголосують, а важливо те, як порахують», точно передає жахливу перспективу спотворення волевиявлення та узурпації влади. Саме тому забезпечення всіх умов для проведення прозорого та чесного голосування є головним завданням національного уряду, запорукою демократії, народної підтримки, гідності та єдності нації. Важливим кроком у цьому напрямку є впровадження електронних засобів та систем, які зменшують можливості адміністративного втручання та зловживання владою, правового тиску та маніпуляцій.

Під електронним голосуванням розуміється спосіб здійснення волевиявлення, при якому процес голосування, підрахунку та оприлюднення результатів здійснюється за допомогою електронних засобів та систем. Це найбільш широке тлумачення, яке включає різні технології: від електронної обробки фізичних носіїв з результатами волевиявлення (наприклад, паперових бюлетенів) до телеопитувань та сучасних технологій Інтернет-голосування. Кожну з відомих технологій можна характеризувати за як рівнем автоматизації певних процесів, так і за ступенем довіри та забезпечуваної безпеки як від зовнішнього втручання так і можливого зловживання організаторами та/або власниками інформаційних систем. Звісно, що практичне застосування на національному рівні можливе лише за умови вивчення та врахування історичного досвіду та відомих проблем, пошуку раціонального компромісу між наданням зручних у користуванні надійних автоматизованих послуг та певних припущень щодо можливих втрат або зловживань. І цей компроміс повинен влаштовувати переважну більшість як тих, хто голосує, так і тих, хто рахує, бо застосовувані технології повинні користуватися довірою і повагою, отримані результати однозначно сприйматися населенням і міжнародною спільнотою, а відомий вислів стосовно «правильного підрахунку» був повністю виключений навіть як гіпотетичний наслідок впровадження такої системи в Україні.

Останніми роками в світі з'явилося багато нових електронних технологій, які підвищують якість нашого життя, надають нові сервіси та послуги, зменшують ризики негативних подій та пом'якшують можливі наслідки. Одна із таких технологій – блокчейн – здійснила справжню революцію в цифровому світі, зробила блакитні мрії безнадійних романтиків реа-

льністю сьогодення. Насправді, вже зараз існують електроні гроші, непідконтрольні жодному центробанку, уряду чи монарху. Справжня децентралізація в електронному світі породжує нову, досі незнайому інфраструктуру, коли будь-хто і будь-де повністю анонімно та безпечно може створювати надійні активи, інвестувати та передавати власність, позичати та давати в борг, навіть невідомій особі. І все це функціонує повністю прозоро, без зайвої метушні можновладців та казнокрадів, без приводу до правоохоронців та податкового тиску. Це справжня демократія фінансового світу, грошове народовладдя, без контролюючих та підконтрольних, без посередників та узурпаторів, це фінансова воля.

Децентралізація в блокчейні реалізується через складні та пов'язані між собою криптографічні механізми, які гарантують, що події, які вже відбулися та задокументовані, не можуть бути змінені чи скомпрометовані. В таких системах неможливо заднім числом ввести додаткове мито чи змінити звітність, неможливо скасувати борг або обвалити курс національної валюти. Блокчейн-системи – це захищені сховища, в яких забезпечується історично стійке зберігання записів (реєстрів), і ці реєстри можуть містити будь-яку важливу інформацію. У криптовалютах таким чином зберігається інформація про наявні цифрові активи, у блокчейн-кадастрах – відомості щодо власників, в електронних аукціонах – історія торгів, тощо. І вся ця інформація не може бути змінена за примхою можновладця чи депутата, бандита чи олігарха, ця інформація історично захищена, незмінна, неспростовна і це надає можливість для якісно нового стану – незалежності та свободи. Свободи фінансів та власності, купляти та продавати, діяти та інвестувати, свободи вибору – і це найголовніше. Дійсно, історично стійке збереження кожного результату волевиявлення особистості забезпечує свободу та незалежність голосування спільноти. І ця технологія вже існує, і наше завдання – впровадити її в Україні.

Метою статті є аналіз можливих шляхів із розбудови національної децентралізованої системи електронного блокчейн-голосування в Україні, обґрунтування її структури та основних складових, надання конкретних пропозицій стосовно архітектури системи, базової моделі та протоколів взаємодії.

Історичний досвід та проблеми побудови національних систем електронного голосування

Забезпечення чесного та прозорого процесу волевиявлення громадян є одним із основних принципів демократичного суспільства та без перебільшення – питанням національної безпеки держави. Традиційний спосіб голосування з використанням друкованих бюлетенів, підрахунок яких здійснюється членами виборчих комісій, є вразливим до маніпуляцій та ресурсоємним, як з точки зору фінансових, так і часових витрат. На друк десятків мільйонів бюлетенів витрачаються величезні кошти, а підрахунок голосів, зазвичай, розтягується на декілька тижнів.

Перші спроби автоматизації процесу підрахунку голосів були зроблені у 60-х роках минулого століття у США. Виборець, як і раніше, власноруч робив відмітку на паперовому бюлетені, проте підрахунок голосів здійснювався вже не вручну, а за допомогою спеціальної машини, яка зчитувала відмітки з бюлетенів. Трохи пізніше з'явилися машини для голосування з електронними дисплеями та кнопками (або сенсорними дисплеями), що замінили паперові бюлетені. Результати голосування зберігалися у пам'яті такої машини. Подібні системи застосовувалися на виборчих дільницях у США, Індії, Бразилії.

Із розвитком комп'ютерних мереж та Інтернету почали розроблятися системи дистанційного голосування, що застосовуються у таких країнах як США, Великобританія, Швейцарія, Естонія. Так, наприклад, у Швейцарії віддалене голосування застосовується при проведенні місцевих референдумів, а пароль для доступу до електронного бюлетеня отримується виборцями через поштову службу.

Однією з найбільш прогресивних країн з точку зору впровадження систем дистанційного волевиявлення є Естонія, де на місцевих та парламентських виборах громадяни мають змогу віддати свої голоси онлайн через систему електронного голосування. Ідентифікація користу-

вачів здійснюється за допомогою ID карток, тому для голосування окрім комп'ютера необхідно мати пристрій для читання електронних карток. Голосування є таємним і здійснюється із застосуванням асиметричної криптографії. Однією зі сторін протоколу голосування є агентство електронного голосування, що розміщує списки виборців, підраховує голоси та публікує результати голосування.

За ступенем автоматизації системи електронного голосування можна поділити на такі, що:

- застосовують для підрахунку голосів електронні пристрої, що зчитують відмітки з паперових бюлетенів;
- застосовують машини для голосування з електронними дисплеями та кнопками (або сенсорними дисплеями) замість паперових бюлетенів; результати голосування зберігаються у пам'яті машини для голосування;
- реалізують дистанційне (віддалене) голосування через мережу Інтернет із використанням криптографічних протоколів.

Перший та другий типи систем електронного голосування хоч і підвищують ефективність процесу голосування, проте не відкидають необхідності приходу виборців на виборчі дільниці. У свою чергу, віддалене голосування дозволяє виборцю віддати свій голос, не виходячи з дому, що підвищує явку виборців.

Очевидно, що віддалене голосування є складнішим у реалізації, оскільки у цьому випадку необхідно забезпечити конфіденційність та цілісність даних, що передаються через мережу Інтернет. Це здійснюється за рахунок застосування асиметричної криптографії, зокрема алгоритмів цифрового підпису та направленого шифрування. Задля забезпечення повної анонімності використовуються алгоритми сліпого підпису та гомоморфне шифрування. Останнє, зокрема, не потребує розшифрування окремих голосів у процесі підрахунку.

За принципом побудови віддалені системи електронного голосування поділяються на централізовані та децентралізовані. Централізована система голосування має ієрархічну структуру, де вся інформація щодо голосування акумулюється у центральному довіреному вузлі, який здійснює підрахунок голосів та публікацію результатів голосування. Недоліками централізованого підходу є наступні:

- збій у роботі центрального вузла призведе до зупинки всієї системи голосування;
- збій у роботі центрального вузла може призвести до втрати всіх даних;
- виборці повинні довіряти центральному вузлу.

У децентралізованій системі немає єдиного довіреного центру, натомість всі вузли є рівноправними учасниками, що можуть працювати без довіри один до одного. Крім того, збій одного з вузлів не вплине на функціонування всієї системи, а інформація щодо голосування зберігається розподілено на різних вузлах. Однак, очевидно, що цей підхід є набагато складнішим у реалізації, ніж централізована система віддаленого електронного голосування.

Майже всі відомі системи електронного голосування в різних країнах є централізованими. Однак, з огляду на очевидні переваги, саме децентралізована система електронного голосування видається найбільш перспективним варіантом у контексті розробки національної системи голосування.

Проблема побудови такої системи може бути вирішена шляхом застосування технології блокчейн, яка в останні роки набула розвитку як у світі в цілому, так і в Україні зокрема. Багато компаній в Україні задіяно у проектах, пов'язаних з блокчейном, реалізований електронний аукціон на блокчейні тощо.

Блокчейн представляє собою ланцюжок з блоків даних (що містять транзакції), який одночасно зберігається різними вузлами мережі. Нові блоки даних можуть бути додані до ланцюжка лише за згодою більшості вузлів в результаті досягнення консенсусу, а блоки, щодо яких вузли вже дійшли згоди, не можуть бути модифіковані у майбутньому. Технологія блокчейн базується на використанні надійної криптографії та дозволяє забезпечити:

- розподілене зберігання інформації на різних вузлах;
- функціонування системи у разі збою одного або декількох вузлів;
- надійність та безпеку операцій в режимі повної недовіри між вузлами.

Побудова системи електронного голосування на основі блокчейну дозволить забезпечити виконання таких властивостей як:

- прозорість: достовірність транзакції, що містить голос виборця, може бути перевірена учасниками протоколу голосування у будь-який момент;
- цілісність: транзакція, що містить голос виборця, не може бути модифікована або вилучена з блокчейну після того, як блок, в якому міститься ця транзакція, було прийнято у результаті консенсусу;
- анонімність голосування, що не дозволяє зв'язати транзакцію, що містить голос виборця, з його особою (ідентифікаційними даними);
- автоматичний підрахунок голосів та публікація результатів голосування.

Впровадження технології блокчейн підвищує довіру до інформаційних ресурсів, надійність збереження інформації та якість наданих послуг. Відмітимо, що в Україні технологія блокчейн вже знайшла застосування при розробці електронних реєстрів.

На сьогодні голосування на блокчейні не набуло широкого впровадження державними інституціями, проте є приклади таких протоколів та їх застосування на приватному рівні.

З огляду на сказане та в контексті реалізації плану "Держава у смартфоні", вважаємо розробку системи електронного голосування, що базуватиметься на використанні технології блокчейн, найбільш перспективним варіантом розбудови національної системи електронного голосування.

Обгрунтування вимог та умов застосування національної системи електронного голосування в Україні

Система електронного голосування – це сукупність взаємопов'язаних правил, методів, процесів, засобів і технологій, а також правових норм, що в сукупності забезпечують і регулюють дистанційне легітимне волевиявлення авторизованих користувачів(виборців). Можна виділити такі обов'язкові вимоги до систем електронного голосування [1]:

- ніхто, крім виборця, не повинен знати його вибору;
- лише легітимні виборці можуть голосувати, крім того, вони повинні мати можливість голосувати лише один раз;
- рішення виборця не може бути таємно або явно змінено будь-ким (крім, можливо, самого виборця).

Додатково висуваються бажані вимоги [1]:

- кожен легітимний виборець може перевірити, чи правильно враховано його голос;
- кожен легітимний виборець може змінити свою думку і змінити свій вибір протягом певного періоду часу;
- система повинна бути захищена від продажу голосів виборцями;
- у разі неправильного підрахунку голосів кожен законний виборець може повідомити про це систему, не виявляючи його особистості;
- неможливість відстежити, звідки віддалено проголосував виборець;
- автентифікація оператора;
- підтримка системи не повинна вимагати великих ресурсів;
- система повинна бути відмовостійкою у разі технічних несправностей (втрата електроживлення), ненавмисних (втрата виборцем ключа) і зловмисних (навмисного маскування себе як іншого виборця, DoS / DDoS атак).

Коректна реалізація всіх зазначених вище вимог неможлива лише технічними засобами або лише нормативним регулюванням. Система електронного голосування не залежно від її архітектури повинна складатися із взаємопов'язаних частин.

Можна виділити такі складові частини (підсистеми/рівні) системи електронного голосування (рис. 1):

- нормативно-правовий рівень;
- організаційний рівень;
- рівень процесів;
- технологічний рівень.

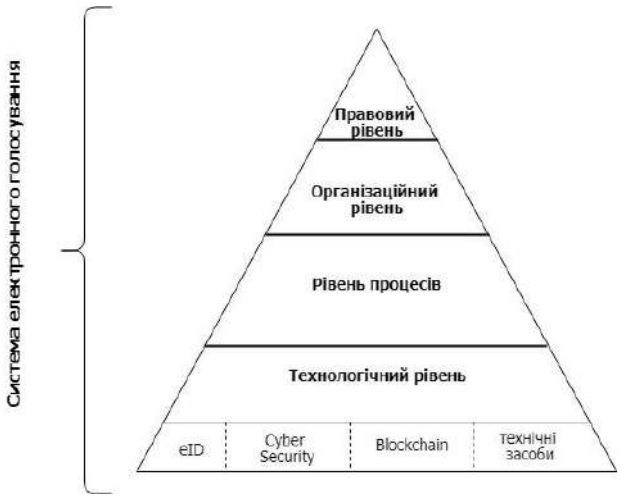


Рис. 1. Рівні системи електронного голосування

Нормативно-правовий рівень включає в себе українські та гармонізовані міжнародні стандарти щодо проведення процедури волевиявлення. Зокрема, на національному рівні мають бути враховані наступні вимоги виборчих процедур, передбачених Конституцією України, Законом України "Про вибори депутатів Верховної Ради Автономної Республіки Крим, місцевих рад та сільських, селищних, міських голів" [2], Законом України "Про вибори президента України" [3], а також прийнятими відповідно до них іншими актами законодавства.

Виборчий процес має здійснюватися на засадах [2, 3]:

- законності та заборони незаконного втручання будь-кого у цей процес;
- політичного плюралізму;
- публічності і відкритості;
- рівності суб'єктів виборчого процесу перед законом;
- рівності прав усіх кандидатів;
- свободи передвиборної агітації, рівних можливостей доступу до засобів масової інформації незалежно від форми власності;
- неупередженості органів державної влади, органів місцевого самоврядування, їх посадових і службових осіб, керівників підприємств, установ і організацій до місцевих організацій партій та кандидатів.

Організаційний рівень включає в себе вимоги щодо архітектури системи електронного голосування.

Традиційна процедура голосування базується, по-перше, на надійній ідентифікації особистості виборця, по-друге – на вимозі збереження його анонімності. Тобто, відповідальні за підрахунок голосів точно впевнені, що голос надійшов від легітимного виборця, проте, вони не мають уявлення від кого саме. Для електронного голосування обидві ці вимоги мають бути збережені. Крім того можна виділити такі основні загрози для систем електронного голосування:

- легітимний виборець не може проголосувати;
- втрата анонімності виборців;
- реєстрація неіснуючих виборців;
- використання пустих бюлетенів виборців, які зареєструвалися, але не взяли участі у виборах.

Рівень процесів описує порядок та процедури взаємодії всіх сторін. Можна виділити такі основні процеси:

- формування списку легітимних виборців;
- формування списку кандидатів;

- волевиявлення;
- підрахунку голосів.

Технологічний рівень включає низку методів, технологій, протоколів та конкретних засобів, направлених на технічну реалізацію процедури електронного волевиявлення.

Обґрунтування структури та основних складових національної системи електронного голосування в Україні

Проведений аналіз [6, 7 – 9] показав, що будь-яка класична (централізована) система має своє максимально допустиме навантаження, при перевищені якого її функціонування стає неефективним. Більше того, необхідно брати до уваги зростаючі ризики з боку кібернетичних атак, які змушують шукати нові стратегії забезпечення безпеки систем [10 – 17]. Особливо це стосується систем, які обробляють критичну інформацію, таку як персональні дані виборців. Традиційним "слабким місцем" будь-якої централізованої структури є її вершина (тобто центральний орган управління), вихід із ладу його внаслідок спрямованої атаки або незапланованого збою фактично означає зупинку функціонування всієї системи. Виходом вбачається перехід на децентралізовані системи.

На рис. 2 схематично зображено структуру традиційної, ієрархічної централізованої структури (ліворуч), та децентралізованої (праворуч). У табл. 1 наведено коротку порівняльну характеристику таких систем з приводу наявних переваг та недоліків.

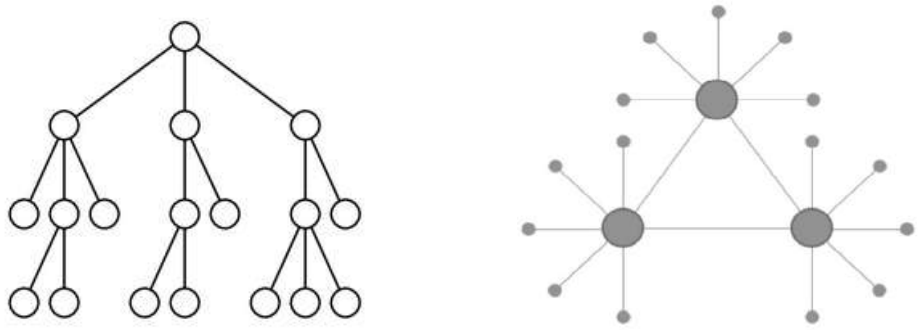


Рис. 2. Централізована ієрархічна (ліворуч) та децентралізована (праворуч) структури

Таблиця 1

Наявні переваги та недоліки централізованих ієрархічних систем

Централізована ієрархічна структура	**Децентралізована структура**
Єдина точка збою • Якщо центр несправний або скомпрометований, то вся система компрометується	Стійкість до збоїв • Центр відсутній, компрометація окремих складових не критична
Користувачі повинні довіряти центру • Необхідність застосування третьої довіреної сторони	Режим повної недовіри • Сторони можуть працювати без довіри один до одного • Довірена сторона не потрібна
Єдиний центр зберігання інформації • Втрата даних у разі збою або порушення центрального серверу	Розподілене зберігання • Однакові дані одночасно зберігаються на різних вузлах • Втрата фактично виключена

Особливо важливим питанням при цьому є формулювання політики та вимог, по яким функціонує децентралізована система. Необхідно забезпечити всім користувачам єдине бачення стану системи в кожний конкретний момент часу. Це можливо із використанням технології blockchain.

В децентралізованому підході забезпечення надійної електронної ідентифікації за допомогою класичного електронного підпису, проте без використання додаткових маскуючих механізмів (наприклад, сліпих підписів), неможливо досягти анонімності виборців. Для того щоб зберегти анонімність та в той же час не перевантажувати протоколи взаємодії, пропонується організувати дворівневу архітектуру системи електронного голосування (рис. 3).

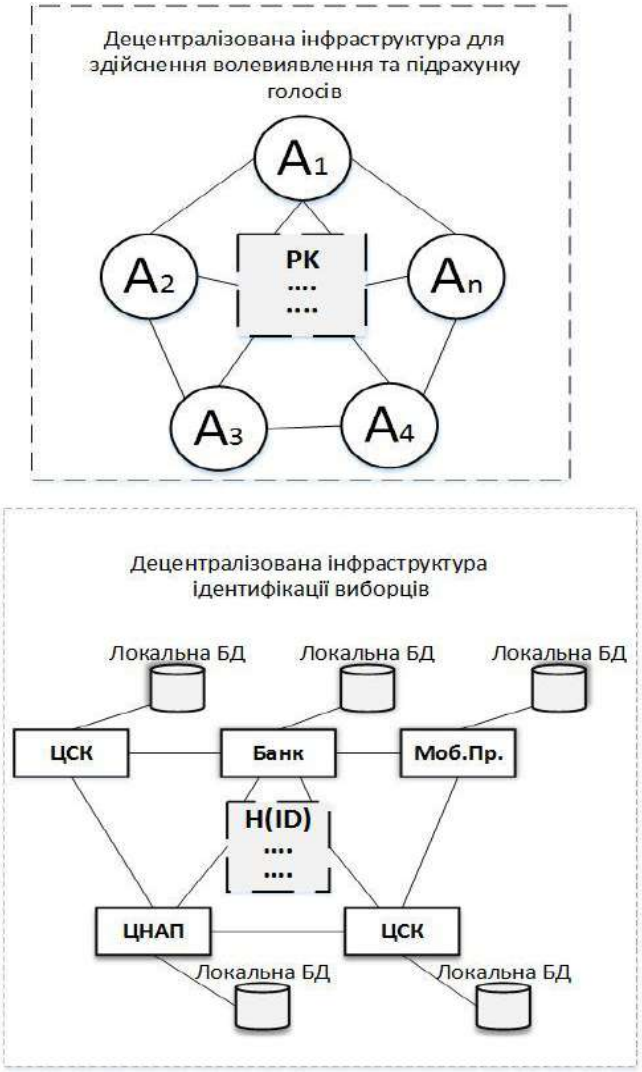


Рис. 3. Рівні системи електронного голосування

Децентралізована інфраструктура ідентифікації виборців (ДІ eID)

Дана інфраструктура має забезпечувати процедуру надійної ідентифікації користувачів та формування списків легітимних виборців. Вона складається із провайдерів послуг ідентифікації громадян (далі – IdP, провайдери). Необхідно забезпечити реалізацію процедури ідентифікації за допомогою:

- засобів BankID;
- засобів MobileID;
- електронного паспорта громадянина;
- цифрового (електронного) підпису:
- програмний носій цифрового підпису;
- апаратний носій цифрового підпису.

Відповідно до висунутих вимог, в ролі *IdP* можуть виступати:

- банківські установи;
- мобільні оператори;

- центри міграційної служби (центри надання адміністративних послуг – ЦНАП);
- центри сертифікації ключів національної системи ЕЦП.

Регламенти функціонування провайдерів встановлюються Законом України "Про електронні довірчі послуги" [4], імплементованим Регламентом ЄС [5] та іншими міжнародними та національними нормативними документами.

Вимоги та процедури ідентифікації залежать від конкретного провайдера.

Мережа провайдерів ідентифікації сформована поза межами децентралізованої системи електронного голосування. Кожен IdP має попередньо сформовану локальну базу даних своїх користувачів, яка містить їхні ідентифікаційні дані та, можливо, локальні ідентифікатори. Відповідальність за надійне збереження та коректне використання локальних баз даних покладається на IdP.

Для організації інфраструктури ідентифікації в рамках децентралізованої системи електронного голосування, IdP об'єднуються в окрему приватну мережу блокчейн (private permissioned Blockchain). В даній мережі кожен із IdP виступає вузлом-валідатором. Необхідно зазначити, що для такої мережі немає необхідності застосовувати складні та енергоємні протоколи консенсусу, оскільки мережа поєднує довірені («чесні») вузли.

Децентралізована інфраструктура для здійснення дистанційного волевиявлення та підрахунку голосів

Інфраструктура має забезпечувати процес дистанційного волевиявлення зареєстрованих (авторизованих) легітимних виборців та процес підрахунку голосів. Додатково в даній інфраструктурі повинні бути організовані процеси реєстрації кандидатів. Довіреними вузлами в даному випадку будуть виступати аналоги територіальних виборчих громад, проте завдяки децентралізованому підходу та технології blockchain наявність головного органу (центральної виборчої комісії) не потрібне. Така організація значно зменшує ризики, пов'язані із людським фактором, включаючи можливості підкупу членів центральної виборчої комісії.

Для організації інфраструктури дистанційного волевиявлення в рамках децентралізованої системи електронного голосування представництва відповідальних за проведення виборчого процесу, наприклад територіальні виборчі громади (A1, A2,...,An), подібно до провайдерів ідентифікації, об'єднуються в окрему приватну мережу блокчейн (private permissioned Blockchain), в якій кожен із Ai виступає вузлом-валідатором – в сукупності вони являють собою децентралізоване Агентство (A). Аналогічно до верхньої мережі Blockchain у нижній також немає необхідності застосовувати складні та енергоємні протоколи консенсусу, оскільки мережа поєднує довірені («чесні») вузли. Вузли-валідатори формують гаманці для легітимних виборців та проводять процедуру автентифікації виборців. Також вони відповідають за процес формування гаманців для альтернатив (кандидатів).

Процес формування списків легітимних виборців у децентралізованій інфраструктурі ідентифікації виборців

Формування списків легітимних виборців відбувається у нижній мережі Blockchain (у децентралізованій інфраструктурі ідентифікації виборців, ДІ eID).

Перед початком формування списків виборців кожен потенційний виборець самостійно генерує собі ключову пару (SK; PK). Після цього він надсилає запит на включення його до списку виборців до одного із доступних йому IdP, в якому у відкритому вигляді надає йому свої ідентифікаційні дані та свій відкритий ключ.

Формат запиту залежить від наявних каналів зв'язку між виборцем та IdP. Він може бути зроблений дистанційно через мережу Інтернет за умови існування надійного каналу зв'язку (рис. 4) або такий ідентифікаційний запит може бути зроблений особисто потенційним виборцем в межах контрольованої зони IdP. Якщо запит здійснюється дистанційно, то відповідальність за дотриманням правил генерації ключової пари покладається на користувача. У випадку, коли запит робиться особисто в межах контрольованої зони, на IdP покладається відповідальність за дотримання умов генерації ключової пари користувача.

Якщо у потенційного виборця вже є згенерована ключова пара відповідно до вимог одного із провайдерів ідентифікації, він може використовувати її. В такому випадку у запит до провайдера має бути включений сертифікат відкритого ключа (рис. 5).

Якщо у потенційного виборця немає локального ідентифікатора у жодного із IdP, то він повинен пройти процедуру первинної ідентифікації у одного із IdP та тільки після цього бути включеним до списку легітимних виборців (рис. 6). Процедура первинної ідентифікації має проводитися відповідно до правил конкретного IdP.

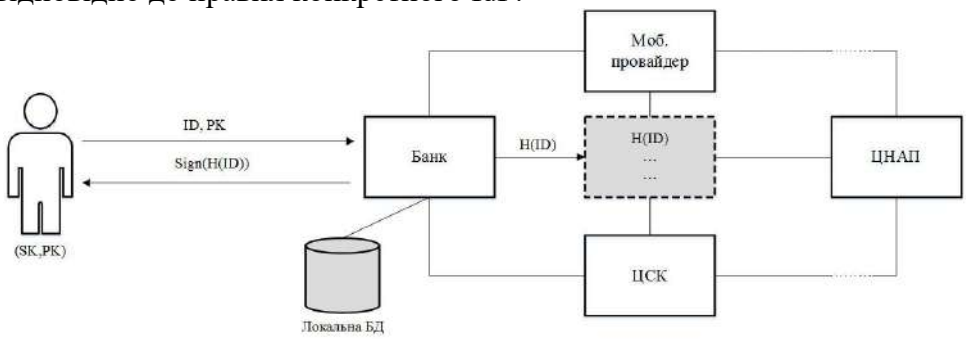


Рис. 4. Процедура ідентифікації на основі відкритого ключа (локального ідентифікатора)

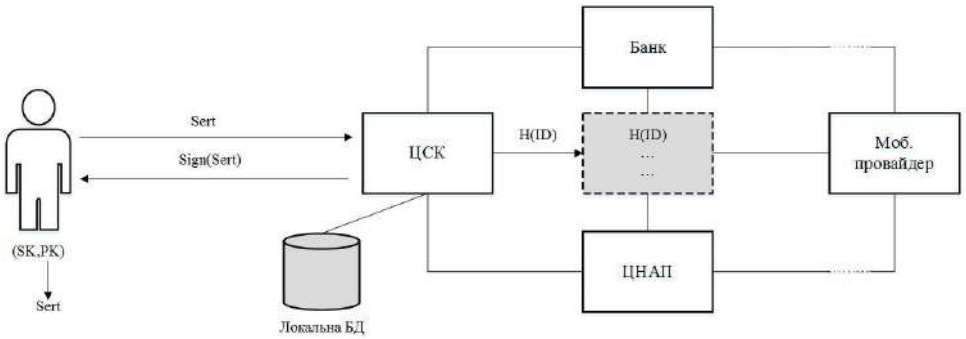


Рис. 5. Процедура ідентифікації на основі сертифікату

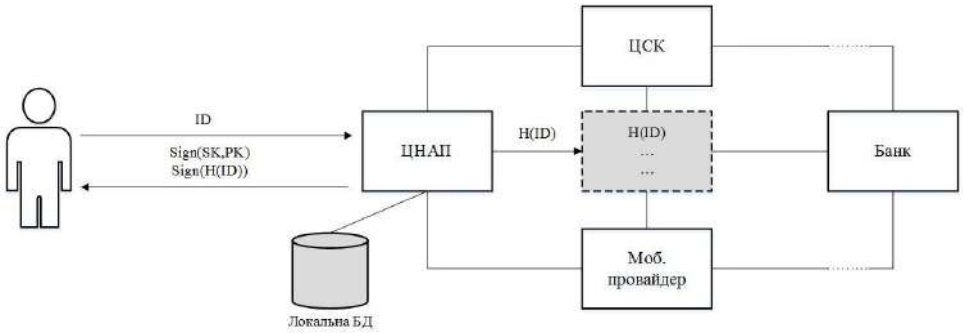


Рис. 6. Процедура ідентифікації на основі персональних даних

Таким чином, коли вичерпався час, виділений на формування легітимних списків виборців, у нижньому блокчейні створено анонімний (деперсоналізований) список потенційних легітимних виборців, а Агентство отримує список всіх зареєстрованих легітимних виборців, але виборці зберігають свою анонімність.

Процес формування списку кандидатів у децентралізованій інфраструктурі для здійснення дистанційного волевиявлення та підрахунку голосів

Реєстрація кандидатів відбувається у верхній мережі Blockchain (децентралізованій інфраструктурі для здійснення дистанційного волевиявлення та підрахунку голосів, ДІ voting). Тут і далі під Агентством будемо розуміти сукупність територіальних виборчих дільниць, об'єднаних в окремий приватний Blockchain.

Відповідальність за процедуру реєстрації (рис. 7) кандидатів покладено на валідаторів верхньої мережі Blockchain.

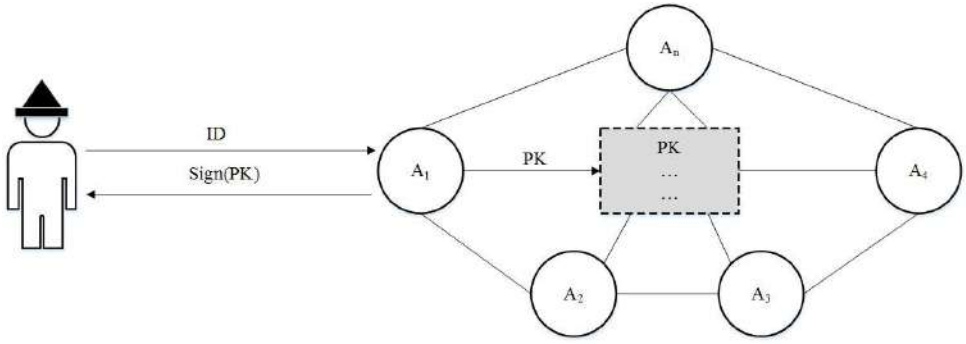


Рис. 7. Процедура реєстрації кандидатів

Представники відповідальних за проведення процедури волевиявлення, які виступають в ролі вузлів-валідаторів у верхній мережі Blockchain, проводять первинну ідентифікацію кандидатів та ініціюють транзакцію на включення даного кандидата до списку. При цьому представництва Агентства несуть відповідальність за дотримання всіх правил та політик ідентифікації кандидатів та перевірку на відповідність вимогам, які встановлені національним законодавством.

Процес голосування у децентралізованій інфраструктурі для здійснення дистанційного волевиявлення та підрахунку голосів

Виборці, які пройшли процедуру автентифікації, здійснюють волевиявлення шляхом пересилки токена на одну із адрес гаманців, які відповідають зареєстрованим кандидатам, формуючи відповідну транзакцію, яку вони підписують власним особистим ключем.

Необхідно зазначити, що запропонований підхід може бути використаний навіть у перехідний період, коли частина виборців вже буде використовувати електронні засоби, а частина все ще буде віддавати перевагу класичним паперовим бюлетеням. Хоча при цьому виборцю, який бажає проголосувати за допомогою паперового бюлетеню, необхідно буде пройти процедуру ідентифікації у нижній мережі blockchain (нагадуємо, що це можливо зробити, навіть не маючи жодних технічних засобів), безпосередньо процес волевиявлення може бути здійснений класичним способом на виборчій дільниці (в даному випадку в межах контрольованої зони одного із представництв децентралізованого Агентства). Для цього передбачається процедура анулювання токена для голосування такого виборця перед наданням йому паперового бюлетеня.

Процес підрахунку голосів у децентралізованій інфраструктурі для здійснення дистанційного волевиявлення та підрахунку голосів

Підрахунок голосів здійснюється автоматично. Результати стають доступними для всіх після завершення часу, відведеного для голосування. Концепція та архітектура системи також передбачає можливість організації моніторингу явки виборців, а також з невеликими додатковими модернізаціями можливість проведення аналізу результатів волевиявлення, наприклад розподіл суспільної думки по регіонах без втрати анонімності виборців.

Висновки та рекомендації

Дослідження довели, що класичні (централізовані ієрархічні) системи голосування не завжди відповідають сучасним вимогам інформаційного демократичного суспільства. Особливо це стосується державних систем із перехідною моделлю управління, коли демократичні цінності не мають сталого історичного підґрунтя або обтяжені авторитарними періодами із свавіллям та беззаконням можновладців. Зокрема, більшість пострадянських держав перебувають під наслідком тривалого тоталітарного правління, коли безальтернативне голосування та «правильний» підрахунок голосів були звичайною практикою ієрархічних суспільних від-

носин. І навіть сьогодні нерідкі прецеденти застосування адміністративного ресурсу, які, хоча і скасовуються інколи через революційні події, але можуть повністю спаплюжити народовладдя через підробку або викривлення результатів волевиявлення. Ієрархічні централізовані системи голосування зазвичай використовуються як вдалий механізм приховування можновладцями своїх корисних намірів, коли різними шляхами за стіною потужних адміністративних парканів та силами державних установ реалізується узурпація влади – від друку додаткових бюлетенів, примусового голосування ув'язнених і т.д. до втручання в електронні системи центральної виборчої комісії. Звісно, що всі переваги централізованих систем (керованість, надійність, автономність і т.д.) нівелюються через можливість викривлення результатів голосування, тобто у разі, коли система не спроможна виконати завдання за призначенням. Отже дослідження, розробка та впровадження нових інформаційних систем і технологій електронного голосування, які б унеможливлювали втручання та викривлення волевиявлення через децентралізацію (звісно із збереженням всіх системних якостей з безпеки та надійності), є безумовно важливим та актуальним науково-прикладним завданням загальнонаціонального значення.

Аналіз показав, що на сьогодні вже створено основне науково-технологічне підґрунтя для розбудови інформаційних систем якісно нового рівня. Це децентралізовані електронні системи, які побудовані за технологією блокчейн та які здатні краще забезпечити функціонування в умовах збільшення спектру інформаційних послуг та при зростанні кількості користувачів. Децентралізоване збереження даних та, що найголовніше, децентралізоване, неупереджене та незалежне прийняття рішення в блокчейн-системах є запорукою розбудови якісно нової загальнонаціональної системи електронного голосування, здатної докорінно змінити соціальні відносини від ієрархічного «начальник-підлеглий» до децентралізованого «партнер-партнер». Впровадження такої системи має за мету унеможливити втручання в виборчий процес, зробити його прозорим та безпечним, підвищуючи тим самим довіру до національної влади, державних інформаційних ресурсів, зменшити час та накладні витрати, підвищити безпеку, тощо. Отже, враховуючи основні засади національного інформаційного суверенітету та з погляду на розбудову демократичного інформаційного суспільства в Україні доцільним є впровадження децентралізованих систем та мереж, які спроможні надавати якісно нові послуги та сервіси, в тому числі, забезпечуючи незалежність, неспростовність, прозорість та безпеку інформаційних ресурсів на всіх етапах їх життєвого циклу.

Сучасна система електронного голосування являє собою взаємопов'язану сукупність правил, методів, процесів, засобів і технологій, а також правових норм, що забезпечують і регулюють дистанційне легітимне волевиявлення авторизованих користувачів (виборців). Електроне голосування охоплює процеси на чотирьох базових рівнях: нормативному, організаційному, рівні процесів та технологічному рівні. Кожен з рівнів забезпечує виконання певних процесів, які забезпечуються окремими технічними, технологічними та нормативно-правовими механізмами. Зокрема, нормативно-правовий рівень забезпечує виконання як гармонізованих міжнародних, так і національних українських стандартів та інших нормативно-правових актів щодо проведення процедури волевиявлення із врахуванням засад законності та заборони незаконного втручання у виборчий процес, політичного плюралізму, публічності і відкритості, рівності суб'єктів виборчого процесу перед законом та прав усіх кандидатів, свободи агітації, рівних можливостей доступу до засобів інформації, неупередженості органів державної влади, місцевого самоврядування, посадових і службових осіб, керівників підприємств, установ і організацій, тощо. Організаційний рівень забезпечує виконання вимог архітектури системи електронного голосування, надійної ідентифікації особистості виборця, вимог збереження анонімності підрахунку голосів, відповідальності організаторів, тощо. Рівень процесів забезпечує встановлений порядок та процедури взаємодії всіх сторін, зокрема, процесів формування списку легітимних виборців та списків кандидатів (альтернатив голосування), процесів волевиявлення та підрахунку голосів, тощо. Технологічний рівень за-

безпечує виконання методів, технологій, протоколів та конкретних засобів технічної та технологічної реалізації процедури електронного волевиявлення.

Для практичної розбудови національної системи електронного голосування в Україні із врахуванням міжнародного досвіду з розгортання, експлуатації та результатів аналізу безпеки інформаційних технологій запропоновано конкретні пропозиції з обґрунтування архітектури, базової моделі та протоколів взаємодії системи електронного блокчейн-голосування. Запропонована, досліджена та випробувана шляхом фізичного прототипування дворівнева архітектура системи електронного блокчейн-голосування. Нижній (перший) рівень цієї системи дозволяє, враховуючи досвід розбудови національних інформаційних комплексів та систем, забезпечити виконання всіх складових процесу електронної ідентифікації за допомогою вже існуючих технічних засобів та організаційно-правових заходів, таких, наприклад, як BankID, MobileID, електронний підпис, тощо. Це забезпечить інтероперабельність системи електронного голосування, успадковуваність вже впроваджених національних інформаційних систем і технологій (зокрема, національної системи електронних довірчих послуг) та відтворюваність результатів фізичного прототипування блокчейн-голосування. Верхній (другий) рівень призначено для реалізації волевиявлення та підрахунку голосів із забезпеченням керівних принципів демократичного волевиявлення (схвалених Венеціанською комісією), зокрема, незалежного контролю за правильністю складання списків виборців; можливості анонімного голосування тільки тими особами, які мають на це право; незмінність та неспростовність результатів волевиявлення; легкість та прозорість перевірки правильності підрахунку голосів, тощо. Отримані результати фізичного прототипування дозволяють стверджувати про ґрунтовність та виваженість розробленої архітектури, її спроможність забезпечити виконання базових вимог децентралізованого електронного голосування, вимог інформаційної та функціональної безпеки та надійності інформаційних технологій. Практичне впровадження розробленої архітектури блокчейн-голосування підвищить довіру до інформаційних ресурсів та сервісів (що є особливо актуальним для державних установ); зменшить час та накладні витрати; унеможливить втручання централізованих установ та можливі корупційні дії; підвищить надійність збереження інформації та якість наданих послуг.

Список літератури:

1. Hannu Nurmi, Arto Salomaa. Conducting secret ballot elections in computer networks: Problems and solutions // Annals of Operations Research / University of Turku. 1994. №51. P.185-194.
2. Закон України “Про вибори депутатів Верховної Ради Автономної Республіки Крим, місцевих рад та сільських, селищних, міських голів”.
3. Закон України “Про вибори президента України”.
4. Закон України “Про електронні довірчі послуги”.
5. Регламент (ЄС) № 910/2014 Європейського Парламенту та Ради від 23 липня 2014 року «Про електронну ідентифікацію та довірчі послуги для електронних транзакцій у межах внутрішнього ринку та про скасування Директиви 1999/93/ЄС» (1) (COM (2012) 0238-C7-0133/2012 – 2012/0146 (COD)).
6. Горбенко І.Д., Кузнецов О.О., Потій О.В., Горбенко Ю.І., Полуяненко М.О. Технологія блокчейн: огляд, сучасні проблеми та перспективи впровадження в Україні // ІІ міжнар. наук.-практ. конф. “Проблеми кібербезпеки інформаційно-телекомунікаційних систем” (PCSITS), 11-12 квітня 2019 р., м. Київ, 2019. С. 217-220.
7. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. Handbook of Applied Cryptography, CRC Press, 1997, 794 p.
8. Yu. I. Gorbenko, K. V. Isirova. Improved mechanism of one-time keys for post-quantum period based on the hashing functions // Telecommunications and Radio Engineering. 2018. Vol. 77, Issue 14. P. 1277-1296.
9. Andrushkevych A., Gorbenko Y., Kuznetsov O., Oliynykov R., Rodinko M. A. A Prospective Lightweight Block Cipher for Green IT Engineering // Kharchenko V., Kondratenko Y., Kacprzyk J. (eds) Green IT Engineering: Social, Business and Industrial Applications. Studies in Systems. Decision and Control. 2019. Vol. 171. Springer, Cham, pp. 95-112. DOI: 10.1007/978-3-030-00253-4_5
10. Потій О. В., Ісірова К. В. Аналіз вимог та моделей безпеки для постквантової криптографії // Математичне та комп’ютерне моделювання. Серія: Технічні науки : зб. наук. праць / Інститут імені В. М. Глушкова Національної академії наук України, Кам’янець-Подільський нац. ун-т імені Івана Огієнка. Кам’янець-Подільський : Кам’янець-Подільський нац. ун-т ім. Івана Огієнка, 2017. Вип. 15- с. 192-197

11. Kateryna Isirova. Blockchain Technology as the Prospective Instrument for Ensuring Electronic Trust Services in Conditions of Cyberthreats // European Cybersecurity Journal. 2018. Issue 5 (1). P 34-43

12. Gorbenko I., Kuznetsov A., Gorbenko Y., Vdovenko S., Tymchenko V., Lutsenko M. (). Studies on Statistical Analysis and Performance Evaluation For Some Stream Ciphers // International Journal of Computing. 2019. 18(1). P. 82-88.

13. Bernstein D., Buchmann J., Dahmen E. Post-Quantum Cryptography. Springer-Verlag, Berlin-Heidleberg, 2009. 245 p.

14. Pass R., Seeman L., Shelat A. Analysis of the blockchain protocol in asynchronous networks // Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2017. P. 643-673.

15. Isirova K., Potii O. Decentralized public key infrastructure development princi-ples // IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). Kiev, 2018. P. 305-310.

16. Kovalchuk L., Kaidalov D., Nastenko A., Rodinko, Shevtsov O., Oliynykov R. Decreasing Security Threshold Against Double Spend Attack in Networks with Slow Synchronization // IEEE INFOCOM 2019, Paris, France, 2019. P. 216-221. doi: 10.1109/INFCOMW.2019.8845301

17. Nurmi H., Salomaa A. Conducting secret ballot elections in computer networks : Problems and solutions // Annals of Operations Research, 1994. Vol. 51, no. 4. P. 185–194.

Харківський національний
університет імені В. Н. Каразіна;
АТ «Інститут інформаційних технологій»

Надійшла до редколегії 15.01.2020

УДК 004.056.55 **DOI:10.30837/rt.2020.1.200.09**

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

МОЖЛИВОСТІ ЗАСТОСУВАННЯ МЕХАНІЗМІВ ПОВНІСТЮ ГОМОМОРФНОГО ШИФРУВАННЯ В СИСТЕМАХ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ

Вступ

Наразі багато аспектів повсякденного життя все більше пов'язані з інформаційно-комунікаційними системами та сервісами, побудованими на їх основі. Важливою є ідея проводити такі важливі соціальні заходи, як голосування, в електронному форматі. Вона з'явилася досить давно, проте досі не існує надійних систем електронного голосування, які б задовольняли усім вимогам. Основними причинами цього є обмеженість існуючих інструментів та можливостей їх застосування [23].

Однією із проблемних вимог, що висунута до систем електронного голосування, є забезпечення анонімності виборців. З однієї сторони, кожен виборець повинен бути ідентифікований, а з іншої – зміст його голосу має бути невідомим. Запропоновані нині методи та механізми, що використовуються у реальних системах голосування, не забезпечують реальної анонімності. Тому як в теоретичному, так і практичному сенсі актуальною та необхідною є проблема розроблення механізмів анонімного підрахунку голосів виборців з забезпеченням захищеності від їх викривлення [23].

Одним із складових механізмів вирішенням вказаної проблеми є використання механізму гомоморфного шифрування. Сутність гомоморфного шифрування полягає у тому, що існує деякий набір операцій, результат виконання яких над шифротекстами (з подальшим розшифруванням) співпадає з аналогічними діями над відкритими текстами [24]. Математично це можливо записати як

$$Dec(Enc(m_1) + Enc(m_2)) = m_1 + m_2 . \quad (1)$$

Тобто, гомоморфне шифрування дозволяє виконувати деякі обчислення над інформацією, при цьому не маючи доступу до самої інформації. Проте при спробі застосувати такі обчислення на практиці виникає ряд проблем. Основними з них є вибір методу асиметричного шифрування, що забезпечує необхідну криптографічну стійкість як від класичних, так і квантових атак, визначення можливих кандидатів асиметричних криптоперетворень при гомоморфному шифруванні, їх оцінка порівняння між собою, та, зрозуміло, вибір найбільш раціональних при заданій множині загроз та обмежень.

Метою цієї статі є обґрунтування можливостей, умов і обмежень щодо застосування стандартизованих асиметричних криптоперетворень при створенні сучасних гомоморфних перетворень типу шифрування, коли безумовно повинна бути забезпечена анонімність електронного голосування та практична реалізація анонімного голосування на основі доведення нульових знань.

1. Сутність та узагальнений попередній розгляд механізмів гомоморфного шифрування

Практично вперше на можливість гомоморфного шифрування у вигляді (1) увага була звернена після розробки алгоритму асиметричного RSA перетворення [24]. RSA є гомоморфним перетворенням відносно операції множення та задовольняє умові

$$\begin{aligned} &Dec(Enc(m_1) * Enc(m_2)) = Dec(m_1^e * m_2^e \bmod n) = \\ &= Dec((m_1 * m_2)^e \bmod n) = ((m_1 * m_2)^e)^d \bmod n = m_1 * m_2 \end{aligned} . \quad (2)$$

Згодом виявилося, що існує безліч інших перетворень, що задовольняють умовам (1) та (2). Якщо механізм має одне гомоморфне перетворення, то його називають частковим. Відносно нього виявилося, що вже за незначної кількості операцій, розрядна сітка переповнюється і механізм втрачає властивість гомоморфності. Така максимальна можлива кількість операцій називається максимальною глибиною гомоморфного перетворення.

Основними характеристиками гомоморфного перетворення є множина гомоморфних операцій та максимальна глибина обчислень. З теорії функціонального аналізу відомо, що у просторі обчислювальних функцій можливо виділити базис. Якщо криптосистема може обчислювати базисні функції, то може обчислювати будь-яку функцію, глибина обчислень якої не перевищує максимальну глибину, характерну для заданої системи. Традиційно, у якості базису обираються операції додавання та множення [24].

Перетворення, гомоморфні операції яких складають повний базис, а глибина обчислень яких може бути при правильному виборі параметрів скільки завгодно великою, отримали назву levelled homomorphic encryption (LHE). Якщо для механізму криптоперетворення існує такий набір загальносистемних параметрів, при якому можна обчислювати функції будь-якої складності, то вона має назву повністю гомоморфної системи криптоперетворення [3].

Аналіз показує, що в сучасній криптографії є значне число гомоморфних перетворень, які можуть бути реалізовані на базі різних алгебраїчних структур. Проте, досягти достатньої глибини для гомоморфних обчислень за адекватних вимог до обчислювальних ресурсів вдалося лише для систем на базі алгебраїчних решіток [3 – 7, 9 – 12]. Цьому сприяє багато факторів, одним з яких є те, що задачі теорії решіток можуть формулюватись мовою поліноміальних кілець, де точки, що належать решітці, представляються деякими поліномами. Таке поліноміальне представлення є достатньо зручним. Зазвичай повідомлення, що шифрується, входить до шифртексту лінійно, що створює природній гомоморфізм щодо операції складання. Схожа ситуація спостерігається і з гомоморфним множенням. Таким чином, природня підтримка базових гомоморфних операцій – додавання та множення, дозволяє реалізовувати оригінальні механізми гомоморфного шифрування.

Перша модель повністю гомоморфної криптографічної системи була запропонована Крейгом Джентрі в 2009 році. Після цього були запропоновані інші механізми гомоморфного перетворення, і на їх основі криптосистеми [9 – 12].

Механізм (схема) Джентрі має GGH-подібну конструкцію. У ньому в якості відкритого ключа виступає деякий "поганий" базис B_{pk} решітки J, разом з базисом B_I деякого ідеалу *I*. Зазвичай $I = (2)$. Безпосередньо шифротекст обчислюється як

$$c = 2r + m \bmod B_{pk}, \tag{3}$$

де m – повідомлення, закодоване у вигляді шуму, а $2r$ – деякий вектор, що належить решітці. При застосуванні (3) повідомлення кодується у вигляді шуму. Для декодування використовується редукований базис B_{sk}. Причому гомоморфність операцій досягається завдяки тому, що при складанні та множенні повідомлень внаслідок замкнутості сума та добуток векторів решітки переходитимуть у інший вектор на решітці, при цьому зберігаючи шум.

Розвитком ідей Джентрі є схема BGV [1]. Стійкість цієї схеми базується на складності вирішення проблеми навчання з помилками. Усі операції виконуються в кільці поліномів $\mathbf{Z}_q[X]/(X^n+1)$. При цьому секретний (особистий) ключ представляється як поліном, усі коефіцієнти якого належать до множини за деяким модулем, наприклад 2 ($\{0,1\}$). Відкритий ключ, обчислюється як пара поліномів

$$(p_0, p_1) = (-(a*s + t*e), a), \tag{4}$$

де a – деякий випадковий поліном, e – "поліном помилки", коефіцієнти якого розподілені за нормальним розподілом.

Безпосередньо шифротекст обчислюється як пара поліномів

$$(c_0, c_1) = (m + p_0 u + te_1 \bmod q,\ p_1 u + te_2 \bmod q). \quad (5)$$

У (5) перший поліном фактично представляє з себе суму повідомлення, маски та вектора шуму. Другий поліном потрібен для розшифрування шифротекста. Якщо обчислимо $c_0 + s * c_1$, то отримаємо поліном, що є сумою повідомлення та деякого невеликого адитивного шуму. Після приведення за модулями t, q шум зникне за умови, що він не перевищував максимальної величини. Шум в схемі BGV представляється величиною виду $t * e$, де t – ціле число, а e – поліном, коефіцієнти якого розподілені за нормальним законом.

Наразі популярною модифікацією схеми BGV є схема BFV [21], у якій запропоновано ряд покращень, що дозволяють краще керувати рівнем шуму та швидкодією. Зокрема, шифротекст обчислюється у вигляді

$$(c_0, c_1) = (\lfloor q / t \rfloor m + p_0 u + e_1 \bmod q,\ p_1 u + e_2 \bmod q). \quad (6)$$

Схеми BFV та BGV і досі залишаються одними з найкращих схем і знаходять своє застосування на практиці.

Також важливим розвитком попередніх ідей є схема CKKS [6]. Справа в тому, що для багатьох перетворень, під час гомоморфних обчислень, виникає потреба апроксимувати певні величини і працювати вже з ними. Ідея такої схеми полягає у тому, щоб представити шум, отриманий під час апроксимації, як частину шуму, отриманого під час шифрування. Цим кодування повідомлень в CKKS дещо відрізняється від попередніх схем. В CKKS схемі повідомлення, як і в попередніх схемах, є поліномом в $\mathbf{Z}_q[X]/(X^n + 1)$, проте для відображення вихідного повідомлення на поліном застосовується канонічне вкладення (canonical embedding map), сутність якого полягає у тому, що між деякою адитивною підгрупою векторів в просторі $\mathbb{C}^{\phi(M)}$ та $\mathbf{Z}_q[X]/(X^M + 1)$ існує гомоморфізм. В цьому випадку повідомлення є вектором комплексних чисел $z = (z_i)_{i \in 0..\phi(M)}$, який відображається в циклотомічне кільце.

Загальна схема такого перетворення наведена на рис 1.

$$\begin{array}{ccccccc} \mathbb{C}^{\phi(M)/2} & \xrightarrow{\pi^{-1}} & \mathbb{H} & \xrightarrow{\lfloor\cdot\rceil_{\sigma(\mathcal{R})}} & \sigma(\mathcal{R}) & \xrightarrow{\sigma^{-1}} & \mathcal{R} \\ z = (z_i)_{i \in T} & \longmapsto & \pi^{-1}(z) & \longmapsto & \lfloor \pi^{-1}(z) \rceil_{\sigma(\mathcal{R})} & \longmapsto & \sigma^{-1}\left(\lfloor \pi^{-1}(z) \rceil_{\sigma(\mathcal{R})}\right) \end{array}$$

Рис. 1. Схема кодування повідомлень в CKKS

Аналіз показує, що в цілому структура шифротексту в CKKS схемі схожа на BGV. Детальний огляд схеми наведено в [6].

Іншим типом повністю гомоморфних систем є схеми на базі проблеми NTRU [5]. Секретним ключем в таких схемах є деякий поліном f, що має зворотній елемент в відповідному полі. Відкритим ключем є поліном $h = 2gf^{-1} \bmod q$. Для шифрування повідомлення m, шифротекст обчислюється як

$$c = h * s + 2e + m \bmod q, \quad (7)$$

де s, e – деякі малі поліноми.

Для розшифрування достатньо обчислити $m = fc \bmod q$, причому гомоморфність операції визначаються наступним чином:

$$\begin{cases} add(c_1, c_2) = c_1 + c_2 \bmod q \\ mult(c_1, c_2) = c_1 * c_2 \bmod q \end{cases}. \quad (8)$$

Важливою властивістю наведених схем є те, що вони дозволяють легко будувати мультиключові протоколи. Для попередніх схем вважалося, що обчислення відбуваються на одному й тому ж ключі, проте для схем на базі NTRU природнім чином зберігається можливість мультиключових обчислень. Для розшифрування достатньо обчислити $m = f_1 ... f_n c \bmod q$. Проте, як буде показано далі, існують деякі алгебраїчні аспекти, що потребують детальної уваги при їх реалізації.

2. Узагальнений аналіз рівня безпеки перспективних схем гомоморфного шифрування

Проведений аналіз дозволив визначити, що безпека найбільш перспективних схем зводиться до наступних проблем:

- NTRU проблема;
- LWE (Learning With Errors) проблема;
- R-LWE (Ring Learning With Errors) проблема.

Проблема NTRU у загальному вигляді полягає в знаходженні пари поліномів $f, g \in \mathbf{Z}_q[X]/(\tilde{f}(n))$, для яких виконується умова

$$h = f^{-1} * g \bmod q \in \mathbf{Z}_q[X]/(\tilde{f}(n)). \quad (9)$$

Причому, для заздалегідь заданого поліному h всі коефіцієнти поліномів f, g є меншими за певну величину, що визначається з вимог безпеки. Альтернативним визначенням, в термінах теорії решіток, є знаходження досить малого вектору (задача SVP_γ) на решітці:

$$\Lambda_h^q = \{(f, g) \in \mathbf{Z}_q^2[X]/(\tilde{f}(n)) \mid h * f - g = 0 \bmod q\}. \quad (10)$$

Аналіз показує, що для вирішення цієї задачі можливо використовувати як методи перебору, так і методи, що базуються на редукції решіток. Одним з найкращих відомих методів криптоаналізу проблеми NTRU є гібридна атака, яка поєднує методи редукції решіток з переборними методами [25].

Основна ідея методу гібридної атаки полягає у тому, щоб розділити шуканий вектор v на дві частини v_1, v_2. Друга частина знаходиться перебором усіх можливих варіантів, наприклад за допомогою метода “зустріч посередині” (meet-in-the-middle, MITM), який дозволяє значно покращити звичайний перебір. Після того, як друга частина v_2 знайдена, вектор $v' = (0, v_2)$ можливо розглядати як зашумлений вектор v. Маючи зашумлений вектор, за умови, що шум достатньо низький, за поліноміальний час можливо знайти вектор v за допомогою алгоритму Бабаї [25], якщо частина решітки, що відповідає вектору v_1, буде достатньо редукована.

У цілому гібридна атака для проблеми NTRU складається з наступних кроків:

1. Необхідно обрати межу, за якою шуканий вектор v буде розділений на дві частини v_1, v_2.
2. Редукувати частину решітки, що відповідає v_1.
3. За допомогою метода “Зустріч посередині” знайти v_2.
4. За допомогою алгоритму Бабаї знайти вектор.

Слід відмітити, що кроки 2 і 3 можливо виконувати паралельно, що дозволяє значно зменшити складність (час) здійснення атаки. Причому, мінімальний результат, очевидно, досягається тоді, коли час виконання кроків 2 і 3 буде рівним. Час виконання кроку 3 можливо оцінити порівняно легко. Але для кроку 2 ця задача складніша.

Найкращими відомими методами редукції решіток є методи, що базуються на алгоритмі блочної редукції Коркіна – Золотарьова (BKZ) [26]. Суть метода полягає у тому, щоб реду-

кувати не всю решітку одночасно, а лише її частини в відповідних підпросторах. Причому, для редукції в підпросторі використовується деякий «Вирішувач», який є загальносистемним параметром. Зазвичай використовуються модифікації метода LLL, оскільки вони себе гарно показали на решітках малої розмірності [26]. Проблема оцінки часу редукції за допомогою методу BKZ є досить складною. Це тому, що BKZ виконує поліноміальну кількість викликів до Вирішувача, проте точної оцінки кількості викликів та точної оцінки часу роботи досі не знайдено. Більш того, за останні роки були знайдені нові більш ефективні вирішувачі. У тому числі був запропонований симулятор BKZ [26], який дозволяє робити більш-менш точні оцінки, проте з ростом розмірності решітки падає і точність її оцінки. Такий симулятор на основі розмірності решітки n, довжини блока β, кількості ітерацій m та фактору Ерміта δ дозволяє визначити час редукції решітки.

Наразі оцінки часу роботи BKZ є емпіричною та базуються на результатах обчислювальних експериментів. Останні оцінки зведені в табл. 1.

Таблиця 1

Емпіричні оцінки часу роботи алгоритму BKZ

Модель	Значення
Sieve [27]	$d^3 * B^2 + 2^{0.292*\beta+16.4+\log_2(8d)}$
Qsieve [28, 29]	$d^3 B^2 + 2^{0.265*\beta+16.4+\log_2(8d)}$
Lp [30]	$d^3 B^2 + 2^{1.8/\log_2 \delta_0 - 110 + \log_2 2.3^9}$
enum [26]	$d^3 B^2 + 8d * 2^{0.270188776350190*\beta*\log(\beta) - 1.0192050451318417\beta + 16.10253135200765 + \log_2 100}$

Позначення: d – розмірність підрешітки, на якій виконувалася редукція. $B = \log_2 q$ кількість бітів, δ_0 – фактор Ерміта, β – оптимальний розмір блока

У більшості NTRU-подібних використовуються циклотомічні поля виду $\mathbf{Z}_q[X]/(X^n - 1)$ та $\mathbf{Z}_q[X]/(X^{2^n} + 1)$ [25]. Такий вибір дозволяє створювати ефективні реалізації, оскільки для циклотомічних полів існують гомоморфізми, що дозволяють максимально ефективно реалізувати NTT та FFT. Проте, нажаль, складна структура поля робить систему вразливою при досить великих q відносно n.

Ідея атак такого типу базується на теорії Галуа, яка стверджує, що підполя нормального сепарабельного розширення деякого поля мають взаємно однозначне відношення з нормальними підгрупами групи автоморфізмів, що залишають незмінними елементи базового поля. Для аналізу таких конструкцій на полі визначається та використовується норма.

Позначимо циклотомічне поле як $K = \mathbf{Z}_q[X]/(X^n + 1)$. Припустимо, що існує деяке підполе $L \supset K$. Тоді група Галуа $G = Gal(K/L)$ складається з множини перестановок елементів, приєднанням яких до L отримується K. Для циклотомічних полів це відображення виду $\sigma_i(\zeta) = \zeta^i$. Нормою елемента $a \in K$ відносно під поля L є

$$N_{K/L}(a) = \prod_{\sigma \in G} \sigma(a). \tag{11}$$

Вказана норма має декілька цікавих властивостей, які застосовуються для побудови атаки. По-перше, вона є мультиплікативною $N_{K/L}(a*b) = N_{K/L}(a) * N_{K/L}(b)$. По-друге, норма, відносно підполя, завжди лежить у цьому підполі. Ідея полягає у тому, що замість пошуку вектору (g, f) на решітці Λ_h^q можна шукати вектор $(N_{K/L}(g), N_{K/L}(f))$ на решітці $\Lambda_{N_{K/L}(h)}^q$. Оскільки поліном f є дільником $N_{K/L}(f)$ (нормальна підгрупа завжди містить одиницю), то маючи норму, можна швидко знайти поліном, що відповідає цій нормі, якщо його коефіцієнти є достатньо малими. Решітка $\Lambda_{N_{K/L}(h)}^q$ має значно меншу розмірність, ніж Λ_h^q. Це відбува-

ється тому, що норма є розрядженим поліномом (більшість коефіцієнтів тотожно рівні 0). Завдяки цьому, деяка частина базисних векторів решітки обнуляється.

Для вдалої атаки потрібно, щоб модуль q значно перевищував n. Для більшості не гомоморфних схем це виконується, але гомоморфні обчислення часто потребують досить великих модулів, які експоненційно залежать від n, що дозволяє в окремих випадках виконати атаку навіть за поліноміальний час. Це значно обмежує застосування NTRU-подібних систем з циклотомічними полями для вирішення реальних задач. Можливим рішенням може стати використання поля $\mathbf{Z}_q[X]/(X^n - X - 1)$, як в стандарті ДСТУ 8961:2019. Проте, при використанні цього поля, неможливо ефективно використовувати NTT і виникає потреба в створенні ефективних алгоритмів множення.

2.1. Аналіз та порівняння безпеки LWE-подібних асиметричних криптосистем

Проблема навчання з помилками (LWE) визначається наступним чином [17]. Нехай n, q є деякими натуральними числами, χ – деякий ймовірнісний розподіл над $\mathbf{Z}$ та s – секретний вектор у $\mathbf{Z}_q^n$. Ймовірнісний розподіл $L_{s,\chi}$ над $\mathbf{Z}_q^n \times \mathbf{Z}_q$ отримується обчисленням

$$(a, c) = (a, \langle a, s \rangle + e) \in \mathbf{Z}_q^n \times \mathbf{Z}_q, \tag{12}$$

де $a \in \mathbf{Z}_q^n$ отримується з рівномірного розподілу та $e \in \mathbf{Z}$ з розподілу χ. Decision-LWE полягає у тому, щоб визначити, чи отримана пара $(a, c) \in \mathbf{Z}_q^n \times \mathbf{Z}_q$ з розподілу $L_{s,\chi}$ або рівномірного розподілу. Search-LWE полягає у знаходженні s з пари $(a, c) \in \mathbf{Z}_q^n \times \mathbf{Z}_q$. Проблеми Decision-LWE та Search-LWE є еквівалентними з точки зору теорії складності та можуть бути зведені одне до одного за поліноміальний час і фактично є різними поглядами на одну і ту ж задачу. Розподіл χ зазвичай є дискретним нормальним розподілом над кінцевим полем з математичним очікуванням рівним 0 та дисперсією, що характеризується параметром α. Більшість атак на LWE полягають у знаходженні деякого вектору v з певною нормою на решітці L з фіксованим об'ємом $vol(L)$, але з різною розмірністю m, яка фактично характеризує оптимальну кількість пар $(a_i, c_i) \in \mathbf{Z}_q^n \times \mathbf{Z}_q$ необхідних для атаки.

Складність проблеми навчання з помилками точно знайдена лише асимптотично. Доведено, що за певних умов складність вирішення LWE в просторі розмірності n становить щонайменше $2^{O(n)}$ [17]. Цей результат зручно використовувати для оцінки загальносистемних параметрів, проте конкретні оцінки складності криптостійкості досі не відомі. Це пов'язано з тим, що атаки на LWE, в кінцевому випадку, зводяться до редукції решіток. В останні 10 років є суттєвий прогрес у цьому напрямку, що призводить до постійної зміни оцінок. В більшості сучасних криптосистем використовуються варіанти LWE над поліноміальними кільцями (PRLWE), тобто, розподіл не над $\mathbf{Z}_q$, а над $\mathbf{Z}_q[X]/(f(x))$. Часто використовується поліном $f(x) = x^n + 1$ і відповідне поле $R_q = \mathbf{Z}_q[X]/(x^n + 1)$. Коли $(a_i, c_i) \in R_q \times R_q$, то задача має назву RLWE. Коли $(a_i, c_i) \in R_q^d \times R_q$ – MLWE відповідно.

Поліном $f(x) = x^n + 1$ має цікаві властивості, які використовуються для доказу криптобезпеки. Також, його властивості дозволяють використати NTT для створення ефективних реалізацій. Однак, з теорії Галуа відомо, що $R_q = \mathbf{Z}_q[X]/(x^n + 1)$ має складну структуру підполів, що може бути використано для криптоаналізу. Для гомоморфних систем шифрування це питання є особливо важливим. Фактично, сучасними криптологами проблеми R-LWE та M-LWE розглядаються як LWE, оскільки для полінома $f(x) = x^n + 1$ доведено, що R-LWE та M-LWE є складнішими за LWE.

При криптоаналізі більшість дослідників розглядають тільки атаки на решітках. Фактично, атаки такого роду полягають у знаходженні деякого вектору v, що лежить на решітці L та має норму $\|v\|$ не більшу за певну величину. Для атаки на LWE відбувається зведення до інших задач у теорії решіток, які у свою чергу вирішуються вже відомими алгоритмами.

2.1.1. Аналіз захищеності від атаки LWE->BDD

Припустимо, що дано m пар $(a_i, c_i) = (a_i, \langle a_i, s_i \rangle + e_i) \in \mathbf{Z}_q^n \times \mathbf{Z}_q$ [17, 31]. Це можливо записати у більш зручному вигляді:

$$(A, c) = (A, A*s + e) \in \mathbf{Z}_q^{m \times n} \times \mathbf{Z}_q^{m \times 1}. \tag{13}$$

Тоді, можливо побудувати решітку $L = \{Ax \bmod q : x \in \mathbf{Z}_q^m\}$. Очевидно, що s вектор на решітці є найближчим до вектору $As + e$. Задача знаходження найближчого вектору на решітці до деякого довільного вектору має назву BDD та вирішується за допомогою алгоритму Бабаї [25]. Алгоритм працює за поліноміальний час, проте знаходить рішення тільки з деякою ймовірністю. Для LWE цю ймовірність можливо оцінити як:

$$\prod_{i=0}^{m-1} erf\left(\frac{\|b_i^*\|\sqrt{\pi}}{2\alpha q}\right), \tag{14}$$

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

2.1.2. Аналіз захищеності від атаки Dual Attack (LWE->SIS)

Існують атаки на дуальній до Λ_h^q решітки [31]. Побудуємо наступну решітку $L = \{x \in \mathbf{Z}_q^m \mid A*x = 0 \bmod q\}$. Задача SIS полягає у знаходженні такого найменшого $x \in \mathbf{Z}^n$, щоб $A*x = 0$. Припустимо, що такий вектор знайдений. Тоді можна вирішити задачу Decision-LWE. Нехай дано m пар $(A, c) = (A, A*s + e) \in \mathbf{Z}_q^{m \times n} \times \mathbf{Z}_q^{m \times 1}$. Обчислимо скалярний добуток $\langle x, c \rangle$: $\langle x, c \rangle = x*a*s + x*e = 0*s + x*e = x*e = \langle x, e \rangle$.

Оскільки вектор $x \in \mathbf{Z}^n$ відомий, то з цієї рівності можна знайти значення вектору помилок e, хоча простір помилок і залишається досить великим. Доведено [31], що, якщо вектор x має норму

$$\|x\|_2 = \frac{1}{\alpha} * \sqrt{\frac{\ln(\frac{1}{\varepsilon})}{\pi}}, \tag{15}$$

то з ймовірністю близькою до 1 можливо вирішити задачу і при цьому знадобиться $\frac{1}{\varepsilon^2}$ запусків Вирішувача SIS. Вирішувач фактично знаходить достатньо малий вектор на решітці, тобто вирішує задачу SVP. Фактор Ерміта δ_0 при цьому повинен бути [31] не більше

$$\log \delta_0 = \frac{\log^2(\frac{1}{\alpha}\sqrt{\frac{\ln(\frac{1}{\varepsilon})}{\pi}})}{4*n\log q}. \tag{16}$$

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

2.1.3. Аналіз захищеності від Primal Attack (LWE->uSVP)

У атаці, що описана в п. 2.1.1, решітка містить вектор s. Ідея Primal Attack полягає у тому, щоб побудувати таку решітку, на якій буде лежати вектор $(s,e,1)$ і він буде найменшим унікальним вектором (задача uSVP) [31]. Такою решіткою буде

$$\Lambda = \{x \in \mathbf{Z}^{m+n+1} : (A \mid I_m \mid -c) * x = 0 \bmod q\}. \quad (17)$$

Відповідно, для пошуку вектору можливо скористатися BKZ 2.0 і редукувати решітку. Тоді b_0 буде шуканим рішенням. Оцінити фактор Ерміта для вдалої редукції можливо як

$$\log \delta_0 = \frac{1}{4n^2 \ln^2 q}\left(W\left((-2n\ln q) * (\sqrt{n \log q}) * \frac{(\tau\alpha)^2}{2\pi}\right)\right)^2. \quad (18)$$

3. Порівняння асиметричних схем гомоморфного шифрування

Попередній аналіз показав, що розробка необхідного програмного забезпечення є дуже складним процесом. По суті воно розробляється вже десятки років та доступне в вигляді відкритих бібліотек. Розглянуті вище асиметричні схеми, стосовно яких наведені оцінки стійкості, реалізовані в декількох існуючих основних бібліотеках [32 – 34].

Для тестування та порівняння було обрано такі бібліотеки як SEAL, HeLib, cuHe. У якості параметрів було обрано $n = 4096$ та $\log(q) = 109$. Для порівняння використовувався метод аналізу ієрархій [35]. Характеристики обраних схем наведено в табл. 2, а також відображені на діаграмах (рис. 2 – 6). Шум та стійкість було оцінено за 10-бальною шкалою у порівнянні один з одним.

Таблиця 2

Характеристики схем гомоморфного шифрування

	Показник	Схема			
		BGV	BFV	CKKS	LTV
1	Час розгортання ключів (ms)	319658	305937	5754892	4258114
2	Швидкість зашифрування (ms)	4538	8465	126751	3089
3	Швидкість розшифрування (ms)	916	1256	1573	341
4	Шум	6	5	5	7
5	Стійкість	6	7	7	5

Рис. 2. Діаграма часу розгортання ключів

Рис. 3. Діаграма часу зашифрування

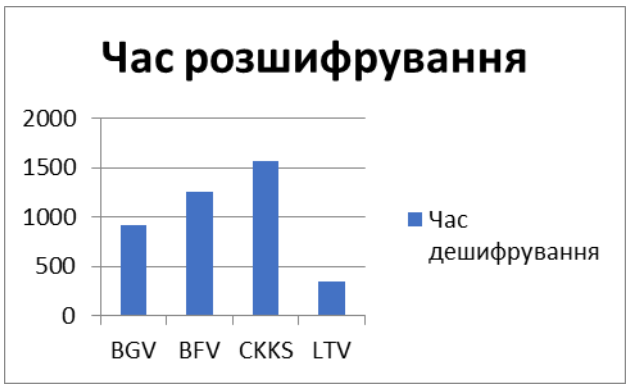


Рис. 4. Діаграма часу розшифрування

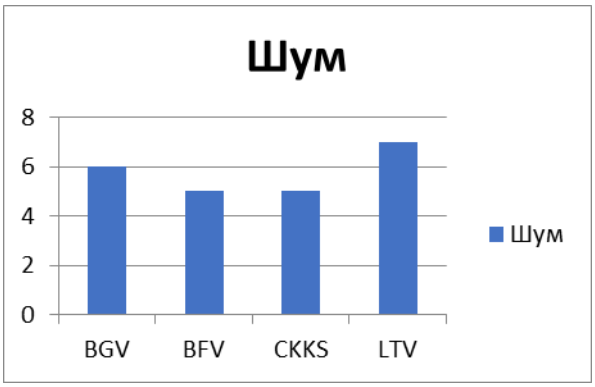


Рис. 5. Діаграма показників шуму

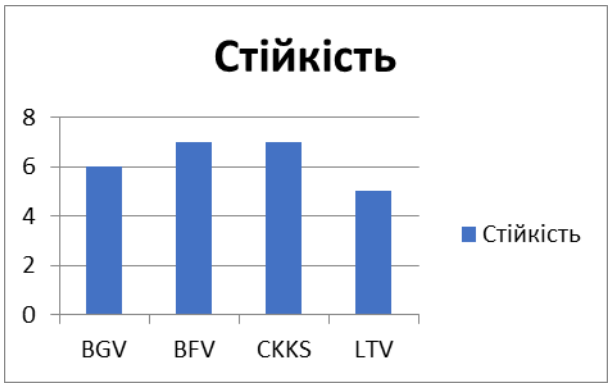


Рис. 6. Діаграма показників стійкості

В подальшому будемо розглядати задачу вибору перспективного шифру у вигляді певної цілі X_0. На даному етапі поки що незрозуміло, яким чином можна досягнути головної мети. Тому здійснимо для головної цілі процедуру декомпозиції та побудуємо дерево цілей [35].

Оскільки змістовна модель визначена у якості об'єкта (схема), то необхідно для першого кроку декомпозиції вибрати модель як основу, що дозволить отримати необхідну сукупність ознак розбиття головної цілі на її складові – підцілі. У якості такої моделі обираємо модель-діяльність [35].

З цією метою у якості підцілей першого рівня, можна використати різні показники якості функціонування шифру:

- технічні показники X_1^1;
- показники цільового призначення X_2^1;

Таким чином, маємо піддерево цілей №1 (рис. 7).

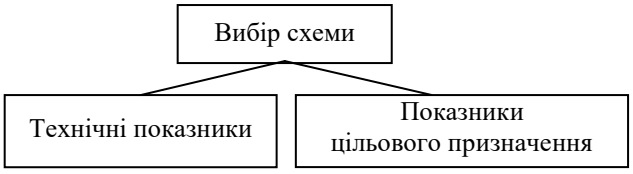


Рис. 7. Піддерево №1

З метою спрощення складності рішення задачі виберемо лише декілька показників для кожної із зазначених вище груп та визначимо піддерева цілей для кожної з них (рис. 8, 9).

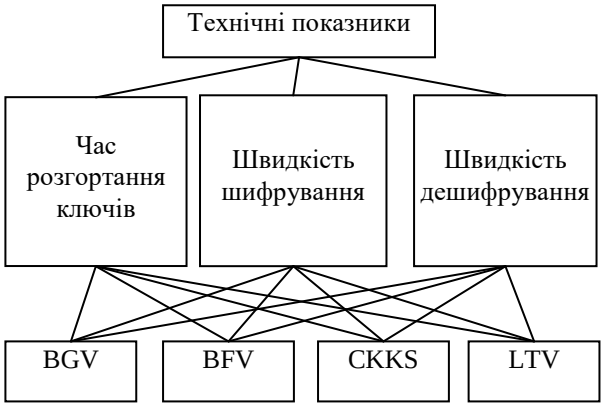


Рис. 8. Піддерево №2

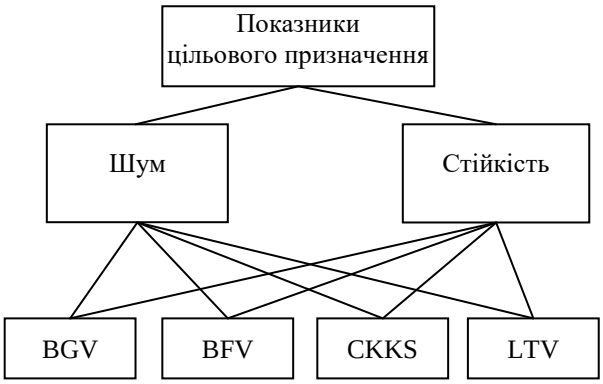


Рис. 9. Піддерево №3

У подальшому будемо використовувати наступні позначення: X_1^2 – час розгортання ключів, X_2^2 – швидкість зашифрування, X_3^2 – швидкість розшифрування, X_4^2 – шум, X_5^2 – стійкість.

Таким чином, дерево цілей буде мати наступний вигляд (рис. 10).

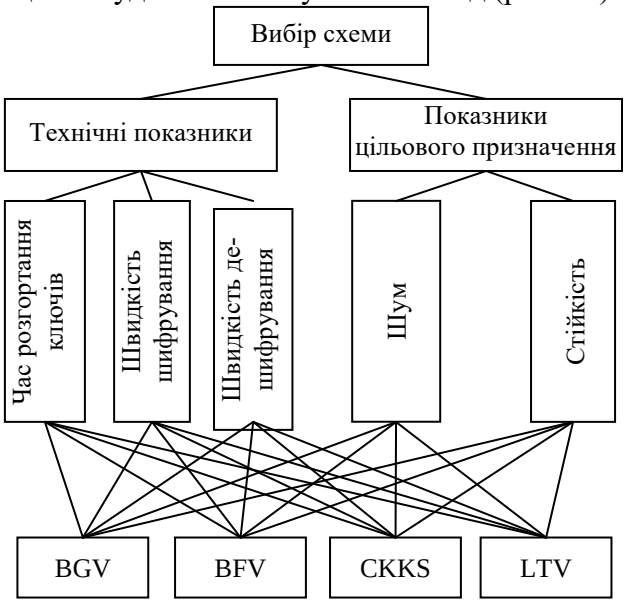


Рис. 10. Дерево цілей

Оцінки значущості вкладу підцілей у досягнення цілі вищого рівня, згідно методу аналізу ієрархій, здійснюються зверху вниз парним порівнянням. Сутність парного порівняння,

наприклад X_i^1 та X_j^1 відносно X^0 до цілі полягає у оцінці (суджень) того, у якій мірі X_i^1 більш важлива (більш вагома) для досягнення цілі X^0, ніж підціль X_j^1. Позначимо цю оцінку через $a_{ij}^{(1)}$. Подібні оцінки надаються експертами та носять суб'єктивний характер. При нашому порівнянні було вживано наступну шкалу оцінок (табл. 3).

Таблиця 3

Шкала оцінок

Перевага X_i^1 над X_j^1	Відсутня	Помірна	Значна	Велика	Дуже велика	Проміжні оцінки
$a_{ij}^{(1)}$	1	3	5	7	9	2, 4, 6, 8

Результати оцінок заносяться у таблиці (матриці) для підцілей r-го рівня.

У лівому стовпці та першому (верхньому) рядку записуються цілі, що порівнюються. У верхній лівій клітинці записується ціль, по відношенню до якої оцінюються підцілі нижчого рівня.

Отримані експертні оцінки підлягають обробці наступним чином:

- обчислюється середнє геометричне для кожного рядка:

$$q_j^{(r-1)} = \sqrt[t_r]{a_{j1}^{(r)} \ldots \times a_{jj}^{(r)} \times a_{jt_r}^{(r)}}; \tag{19}$$

- обчислюються нормовані значення:

$$\gamma_j^{(r-1)} = \frac{q_j^{(r-1)}}{\sum_{i=1}^{t_r} q_i^{(r-1)}}, \tag{20}$$

де $\gamma_j^{(r-1)}$ характеризує значущість цілі $X_j^{(r)}$ для цілі $X^{(r-1)}$. А сукупність усіх $\gamma_j^{(r-1)}$ складає вектор-стовпчик.

Оскільки ми розбили дерево на ряд піддерев, використаємо приведений вище алгоритм послідовно для всіх дерев починаючи з дерева №1 (рис. 1).

Оцінимо важливість показників, що розглядаються (табл. 4).

Таблиця 4

Шкала оцінок X^0

X^0	X_1^1	X_2^1	$q_j^{(0)}$	$\gamma_j^{(0)}$
X_1^1	1	1/2	0.7	0.33
X_2^1	2	1	1.4	0.66

$$\left\| Y_1^{10} \right\| = \begin{pmatrix} 0.33 \\ 0.66 \end{pmatrix}$$

Бачимо, що показники цільового призначення є більш вагомими при порівнянні.

Далі проведемо порівняння важливості технічних показників та показників цільового рівня окремо (табл. 5, 6).

Таблиця 5

Шкала оцінок X_1^1

X_1^1	X_1^2	X_2^2	X_3^2	$q_j^{(1)}$	$\gamma_j^{(1)}$
X_1^2	1	3	1/7	0.754199	0.247
X_2^2	1/3	1	5	1.185615	0.388
X_3^2	7	1/5	1	1.118689	0.366

$$\left\| Y_1^{21} \right\| = \begin{pmatrix} 0.247 \\ 0.388 \\ 0.366 \end{pmatrix}$$

Таблиця 6

Шкала оцінок X_2^1

X_2^1	X_4^2	X_5^2	$q_j^{(1)}$	$\gamma_j^{(1)}$
X_4^2	1	1/6	0.408248	0.143
X_5^2	6	1	2.449489	0.857

$$\left\| Y_2^{21} \right\| = \begin{pmatrix} 0.143 \\ 0.857 \end{pmatrix}$$

Тобто, серед технічних показників найбільш вагомою є швидкість шифрування, а серед показників цільового призначення – стійкість.

Далі, аналогічно попереднім порівнянням, проведемо порівняння технічних показників для кожної схеми окремо та зазначимо отримані результати:

$$\left\| Y_{1-3}^{32} \right\| = \begin{pmatrix} 0.273 & 0.152 & 0.298 \\ 0.053 & 0.633 & 0.087 \\ 0.063 & 0.072 & 0.061 \\ 0.611 & 0.143 & 0.553 \end{pmatrix}$$

Аналогічно зазначимо результати порівняння показників цільового призначення для кожної схеми окремо:

$$\left\| Y_{4-5}^{32} \right\| = \begin{pmatrix} 0.193 & 0.182 \\ 0.368 & 0.364 \\ 0.368 & 0.364 \\ 0.070 & 0.091 \end{pmatrix}$$

Розраховуємо вклад цілей третього рівня для кожного з піддерев:

$$\left\| Y_1^{31} \right\| = \left\| Y_{1-3}^{32} \right\| \times \left\| Y_1^{21} \right\| = \begin{pmatrix} 0.273 & 0.152 & 0.298 \\ 0.053 & 0.633 & 0.087 \\ 0.063 & 0.072 & 0.061 \\ 0.611 & 0.143 & 0.553 \end{pmatrix} \times \begin{pmatrix} 0.247 \\ 0.388 \\ 0.366 \end{pmatrix} = \begin{pmatrix} 0.235475 \\ 0.290537 \\ 0.065823 \\ 0.408799 \end{pmatrix}$$

$$\left\| Y_2^{31} \right\| = \left\| Y_{4-5}^{32} \right\| \times \left\| Y_2^{21} \right\| = \begin{pmatrix} 0.193 & 0.182 \\ 0.368 & 0.364 \\ 0.368 & 0.364 \\ 0.070 & 0.091 \end{pmatrix} \times \begin{pmatrix} 0.143 \\ 0.857 \end{pmatrix} = \begin{pmatrix} 0.053625 \\ 0.104676 \\ 0.104676 \\ 0.023023 \end{pmatrix}.$$

Таким чином, для піддерева, що відображає оцінки технічних показників, найкращою є схема LTV, а для піддерева, що відображає оцінки показників цільового призначення, найкращими є дві схеми BFV та CKKS.

Розрахуємо вклад цілей третього рівня в досягнення головної цілі та представимо отримані результати у вигляді діаграми (рис. 11):

$$\left\|Y_1^{30}\right\| = \left\|Y_{1-2}^{11}\right\| \times \left\|Y_1^{10}\right\| = \begin{pmatrix} 0.235475 & 0.053625 \\ 0.290537 & 0.104676 \\ 0.065823 & 0.104676 \\ 0.408799 & 0.023023 \end{pmatrix} \times \begin{pmatrix} 0.33 \\ 0.66 \end{pmatrix} = \begin{pmatrix} 0.11309925 \\ 0.16496337 \\ 0.09080775 \\ 0.15009885 \end{pmatrix}.$$

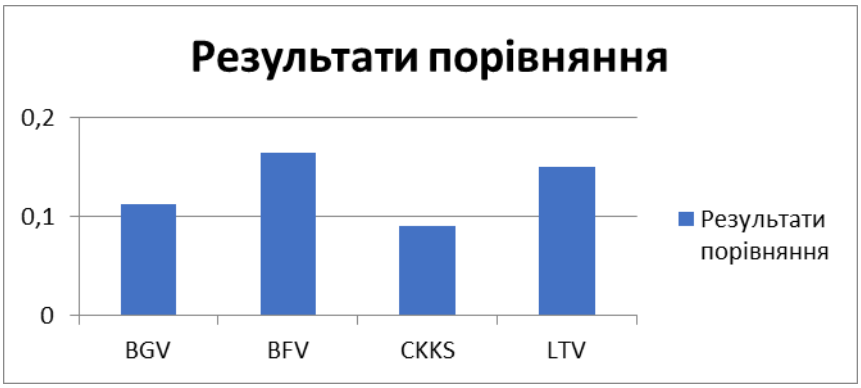


Рис. 11. Результати порівняння

Таким чином, для досягнення головної цілі, тобто вибору кращої схеми, перевагу має BFV (0.165), LTV (0.15), BGV (0.113), CKKS (0.091). Але слід зазначити, що схему необхідно обирати згідно потреб і цілей, для яких вона буде застосована.

4. Обґрунтування методу асиметричного шифрування з нульовими знаннями

Для створення механізму шифрування з верифікацією, зручно скористатися схемою, представленою в роботі [36]. Автори запропонували використовувати фреймворк Фіата – Шаміра для доказів з нульовим розголошенням. Фактично вони додають до криптограми доказ з нульовим розголошенням, який дозволяє перевірити, що деяке повідомлення, закодоване в поліномі m, задовольняє умові

$$B \cdot m \equiv u \bmod t, \tag{21}$$

де (B, r) є заздалегідь відомими параметрами, що однозначно задають множину валідних повідомлень.

Нехай в якості такого валідного значення задається як вектор у $R_q^{N_k}$, де N_k – кількість кандидатів. Разом з цим, у кожного полінома всі коефіцієнти дорівнюють 0, окрім одного молодшого коефіцієнта в одному поліномі. Припустимо, що для валідного значення (голосу) справедливою буде формула

$$f(a) = \sum_{i=1}^{N_k} \left(a_i^2 - a_i\right)^2 + \left(\sum_{i=1}^{N_k} a_i\right)^2 - 1 = 0, \tag{22}$$

де $a_i \in R_q$ – відповідні поліноми.

Для такого значення голосу $a = (a_1, \ldots, a_{N_k}) \in R_q^{N_k}$ обчислимо вектор

$$a' = \left(f(a) + g_1, f(a) + g_2, \ldots, f(a) + g_{N_k}\right), \tag{23}$$

де g_i – наперед задані поліноми (загальносистемні параметри).

За даних умов параметрами B, u та m з формули (8) є: динамічним чином згенерована для кожного голосуючого випадкова матриця $B \in R_q^{N_k \times N_k}$, вектор $u = B \cdot \left(g_1, g_2, \ldots, g_{N_k}\right)$ та вектор-голос m, які потім передаються голосуючому для формування доказу.

Доказ є парою поліномів (c, z). Поліном c формується таким чином, щоб його могла сформувати перевіряюча сторона, використовуючи поліном z, та порівняти з переданим у доказі. Поліном c належить до множини малих поліномів з умовою, що кількість ненульових елементів у ньому не більше, ніж деяке γ, тобто $c \in R_2$, $\|c\|_\infty = \gamma$.

Далі, нехай задана деяка криптографічна геш-функція $H : \{0,1\}^* \to \{u \mid u \in R_2, \|u\|_\infty = \gamma\}$, тоді шифрування з верифікацією для схеми BFV на відкритому ключі $pk = (p_0, p_1)$ для деякого повідомлення $m \in \square_t [X] / (x^n + 1)$, що належить до множини, яку можливо верифікувати за допомогою пари (B, r), буде виглядати наступним чином:

1. Сформувати поліноми u, e_1, e_2 для гомоморфного шифрування.

2. Отримати шифротекст (c_{0m}, c_{1m}) з використанням сформованих на кроці 1 поліномів.

3. Сформувати поліноми u_y, e_{1y}, e_{2y}, m_y.

4. Зашифрувати повідомлення m_y з використанням поліномів u_y, e_{1y}, e_{2y} та отримати шифротекст (c_{0y}, c_{1y}).

5. Обчислити поліном

$$c = H\left(p_0, p_1, B, r, c_0, c_1, c_{0y}, c_{1y}, B \cdot m_y \pmod t\right)$$

6. Обчислити $z = \left(u \cdot c + u_y, e_1 \cdot c + e_{1y}, e_2 \cdot c + e_{2y}, m \cdot c + m_y\right)$.

7. Перевірити, що z задовольняє умовам схеми Фіата-Шаміра.

8. Повернути шифротекст (c_0, c_1) та доказ (c, z).

Для того щоб верифікувати повідомлення, потрібно повторно обчислити поліном c за допомогою z та порівняти його з оригінальним поліномом. Повна процедура верифікації шифротексту (c_0, c_1) за доказом (c, z) виглядатиме наступним чином:

1. Перевірити, що z задовольняє умовам схеми Фіата-Шаміра.

2. Обчислити шифротекст від z : (c_{0z}, c_{1z}).

3. Обчислити поліном:

$$c' = H\left(p_0, p_1, B, r, c_0, c_1, c_{0z} - c \cdot c_0 \pmod q, c_{1z} - c \cdot c_1 \pmod q, B \cdot z_4 - c \cdot r \pmod t\right)$$

4. Якщо $c = c'$ то повернути true, інакше повернути false.

Очевидно, що верифікація пройде успішно, тільки, якщо буде виконуватись наступна система умов:

$$\begin{aligned} & c_{0z} - c \cdot c_0 \equiv c_{0y} \pmod q \\ & c_{1z} - c \cdot c_0 \equiv c_{1y} \pmod q \\ & B \cdot z_4 - c \cdot r \equiv B \cdot m_y \pmod t \end{aligned} \quad . \tag{24}$$

Перші дві умови будуть виконуватися тільки тоді, коли при формуванні z дійсно використовувалося повідомлення m. Третя умова виконується тільки тоді, коли виконується порівняння (21).

Таким чином, наведена вище схема верифікації шифротекстів BFV на основі лінійної залежності $B \cdot m \equiv u \bmod t$ дозволяє здійснити захищену верифікацію шифртексту. Розроблена схема може використовуватися зокрема для систем електронного голосування. В поєднанні з технікою батчінга для повністю гомоморфних схем, запропонована система може сильно

зменшити як складність обчислення, так і об'єм інформації в відповідних криптографічних протоколах.

Висновки

1. Концепція гомоморфного шифрування з'явилася майже одразу після винайдення асиметричних криптосистем, проте тривалий час вона залишалася цікавою можливістю. Побудувати повністю гомоморфні системи для застосування на практиці вдалося відносно нещодавно за допомогою перетворень поліноміальних кілець.

2. Побудова сучасних повністю гомоморфних систем базується на проблемах навчання з помилками (LWE) та NTRU. В цілому LWE-подібні системи вважаються стійкішими до атак, проте під час їх криптоаналізу використовується чимало евристик. Стійкість NTRU зводиться до проблеми знаходження найменшого вектору і є більш зрозумілою.

3. NTRU-подібні повністю гомоморфні системи швидші за LWE-подібні, проте вразливі до алгебраїчних атак на циклотомічні кільця. Захиститися від атак можливо правильним вибором поля. При використанні поля $\mathbf{Z}_q[X]/(X^n - X - 1)$, наприклад, як у стандарті ДСТУ 8961:2019, забезпечується надійний захист від атак такого роду, оскільки група Галуа полінома $X^n - X - 1$ є симетричною групою S_n.

4. На основі порівняння визначено, що для застосування в системах електронного голосування кращі показники показала схема BFV, проте схема LTV поступається лише завдяки потенційній можливості існування алгебраїчних атак. Синтез схеми повністю гомоморфного шифрування на основі ДСТУ 8961:2019 дає змогу побудувати надійну систему гомоморфного шифрування, на основі якої можливо побудувати протоколи електронного голосування з високим рівнем анонімності.

5. Для виборців електронної верифікації голосів можливо використовувати схему доказу Фіата – Шаміра з перериваннями. В цьому випадку перевірку валідності голосу можливо звести до перевірки лінійного відношення, для якого генерується доказ валідності з нульовим розголошенням.

Список літератури:

1. Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (Leveled) fully homomorphic encryption without bootstrapping. In Shafi Goldwasser, editor, ITCS 2012. P. 309–325. ACM, January 2012.

2. Homomorphic Encryption based on Hidden Subspace Membership / Uddipana Dowerah and Srinivasan Krishnaswamy // Indian Institute of Technology Guwahati.

3. Craig Gentry. A fully homomorphic encryption scheme. PhD thesis / Stanford University, 2009.

4. Craig Gentry Amit Sahai Brent Waters Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based.

5. Adriana L´opez-Alt On-the-Fly Multiparty Computation on the Cloud via Multikey Fully Homomorphic Encryption.

6. Jung Hee Cheon1, Andrey Kim1, Miran Kim2, and Yongsoo Song1 Homomorphic Encryption for Arithmetic of Approximate Numbers.

7. Homomorphic Encryption Standardization. [Electronic resource]. Access mode: https://homomorphicencryption.org/.

8. Junfeng Fan and Frederik Vercauteren. Somewhat practical fully homomorphic encryption. Cryptology ePrint Archive, Report 2012/144, 2012. Access mode: http://eprint. iacr.org/2012/144.

9. Marten Van Dijk, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan. Fully homomorphic encryption over the integers // Advances in cryptology–EUROCRYPT 2010. P. 24–43. Springer, 2010.

10. Nigel P Smart and Frederik Vercauteren. Fully homomorphic encryption with relatively small key and ciphertext sizes // International Workshop on Public Key Cryptography. P. 420-443. Springer, 2010.

11. Zvika Brakerski and Vinod Vaikuntanathan. Fully homomorphic encryption from ring-LWE and security for key dependent messages // Advances in Cryptology–CRYPTO 2011. P. 505-524. Springer, 2011.

12. Craig Gentry and Shai Halevi. Implementing gentry's fully-homomorphic encryption scheme // Advances in Cryptology–EUROCRYPT 2011. P. 129–148. Springer, 2011.

13. Zvika Brakerski. Fully homomorphic encryption without modulus switching from classical gapsvp // Annual Cryptology Conference. P. 868-886. Springer, 2012.

14. Craig Gentry, Amit Sahai, and Brent Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based // Advances in Cryptology–CRYPTO 2013. P. 75-92. Springer, 2013.

15. Zvika Brakerski and Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE // SIAM Journal on Computing, 43(2):831-871, 2014.

16. Oded Regev. On lattices, learning with errors, random linear codes, and cryptography // Proceedings of the thirty-seventh annual ACM symposium on Theory of computing. P. 84-93. ACM, 2005.

17. Oded Regev. On lattices, learning with errors, random linear codes, and cryptography // Journal of the ACM (JACM), 56(6):34, 2009.

18. Fully Homomorphic Encryption over the Integers Marten van Dijk, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan.

19. Danger of using fully homomorphic encryption: A look at Microsoft SEAL Zhiniang Peng Qihoo 360 June 18, 2019.

20. Gentry C. Fully homomorphic encryption using ideal lattices[C] // Stoc. 2009, 9(2009): 169-178.

21. Fan J, Vercauteren F. Somewhat Practical Fully Homomorphic Encryption[J]. IACR Cryptology ePrint Archive, 2012, 2012: 144.

22. Chen H, Huang Z, Laine K, et al. Labeled PSI from Fully Homomorphic Encryption with Malicious Security[C]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2018: P.1223-1237.

23. Mursi, Mona & Assassa, Ghazy Moh Rateb & Abdelhafez, Ahmed & Samra, Kareem. (2013). On the Development of Electronic Voting: A Survey // International Journal of Computer Applications. 61. 1-11. 10.5120/10009-4872.

24. Варновский, Н. П. Гомоморфное шифрование / Н. П. Варновский, А. В. Шокуров // Труды ин-та системного программирования РАН. 2006.

25. Hoffstein, Jeff & Pipher, Jill & Schanck, John & Silverman, Joseph & Whyte, William & Zhang, Zhenfei. (2017). Choosing parameters for NTRUEncrypt. 3-18. 10.1007/978-3-319-52153-4_1.

26. Yuanmi Chen Phong BKZ 2.0: Better Lattice Security Estimates / Yuanmi Chen Phong, Q. Nguyen // International Conference on the Theory and Application of Cryptology and Information Security ASIACRYPT 2011: Advances in Cryptology – ASIACRYPT 2011. P. 1-20.

27. Becker A., Ducas L., Gama N., Laarhoven T. (2016). New directions in nearest neighbor searching with applications to lattice sieving // SODA, 2016. P.10-24.

28. Thijs Laarhoven, Michele Mosca, & Joop van de Pol. Finding shortest lattice vectors faster using quantum search. Cryptology ePrint Archive, Report 2014/907, 2014. Access mode: https://eprint.iacr.org/2014/907.

29. Laarhoven T. (2015). Search problems in cryptography: from fingerprinting to lattice sieving (Doctoral dissertation). Eindhoven University ofTechnology. Access mode: http://repository.tue.nl/837539.

30. Lindner R., Peikert C. (2011). Better key sizes (and attacks) for LWE-based encryption // A. Kiayias, CT-RSA~2011. P. 319-339. Springer, Heidelberg.

31. Rachel Player.Parameter selection in lattice-based cryptography. PhD thesis, Royal Holloway, University of London, 2018.

32. Microsoft SEAL. [Electronic resource]. Access mode: https://www.microsoft.com/en-us/research/project/microsoft-seal/.

33. CuHe. [Electronic resource]. Access mode: https://github.com/vernamlab/cuHE.

34. HeLib [Electronic resource]. Access mode: https://github.com/shaih/HElib.

35. Саати Т. Принятие решений. Метод анализа иерархий // Радио и связь, 1993. 278 с.

36. Vadim Lyubashevsky. One-Shot Verifiable Encryption from Lattices / Vadim Lyubashevsky, Gregory Neven // Annual International Conference on the Theory and Applications of Cryptographic Techniques EUROCRYPT 2017: Advances in Cryptology – EUROCRYPT 2017. P. 293-323.

Харківський національний
університет імені В. Н. Каразіна;
АТ «Інститут інформаційних технологій»;
Харківський національний
університет радіоелектроніки

Надійшла до редколегії 09.02.2020

UDC 004.75 **DOI:10.30837/rt.2020.1.200.10**

P. STETSENKO, G. KHALIMOV, Prof., Dr. of Science, Y. KOTUKH, Phd.

ANALYSIS OF ATTACK SURFACES ON BLOCKCHAIN SYSTEMS

This paper presents a study of attack surfaces and possible ways of conducting various attacks on decentralized systems based on Blockchain technology. To accomplish the task, the effectiveness of the attack is studied relative to the plane of its application, namely, relatively:

- cryptographic designs of Blockchain technology;
- distributed architecture of systems based on Blockchain technology;
- Blockchain application context.

Several attacks have been identified for each of these planes, including malicious mining strategies, coordinated peer behavior, 51 % attacks, domain name attacks (DNS), distributed denial of service attacks, delayed consensus achieving, Blockchain branching, orphaned and obsolete blocks, digital wallet thefts and privacy attacks. It then investigates the causal relationship between these attacks and analyzes how one fraudulent action can lead to the possibility of other attacks. A minor contribution of this work is to highlight effective countermeasures adopted by Blockchain technology or proposed by researchers to mitigate the effects of these attacks and fix vulnerabilities in Blockchain-based decentralized systems.

Despite the functionality that Blockchain technology brings to applications, recent reports highlight the security risks associated with the given technology. For example, in June 2016, an unknown attacker managed to withdraw US $ 50 million from the DAO, a decentralized autonomous organization that operates according to the rules of smart contracts based on Blockchain technology [1]. In August 2016, adversaries have stolen Bitcoin cryptocurrency worth $ 72 million from the Bitfinex exchange in Hong Kong [2]. In June 2017, Bitfinex also experienced a distributed denial of service (DDoS) attack, which led to a temporary suspension of its work. Several Bitcoin and Ethereum exchanges (a decentralized Blockchain platform) have also suffered from DDoS attacks, which often impede service availability for users. These attacks have application-specific consequences. For example, for Blockchain cryptocurrencies, the process of constant investment in their work is important, therefore DDoS attacks can cause cryptocurrency devaluation.

Blockchain security is paramount for potential users to participate. For example, investors primarily take into account the security of cryptocurrencies when studying the risks associated with investing in them. Understanding the threats associated with Blockchain systems in general is the first step towards building a secure architecture for decentralized Blockchain-applications. The aim of this work is an in-depth study of attack surfaces for Blockchain technology.

Blockchain technology will be used in many applications in a wide variety of digital fields, so analyzing attacks that could jeopardize existing applications is an urgent task. The paper presents a classification of attacks in three classes:

- attacks related to cryptographic constructions and algorithms used by Blockchain technology (for example, branching of a Blockchain ledger, obsolete and orphaned blocks);
- attacks related to the architecture of a peer-to-peer network, on which Blockchain systems are mainly built (for example, malicious mining, 51 % attack, delay in achieving consensus, DDoS attack and DNS attack)
- attacks related to the context of applications that use Blockchain technology (for example, Blockchain absorption, double-spend attacks and wallet application theft).

The aim of this work is to single out the nature of attacks aimed at decentralized Blockchain-based systems, peer-to-peer architecture and applications. The paper analyzes the causal relationship between conducting an attack and the emergence of opportunities for other attacks because of this and presents the sequence of possible attacks. The work considers the consequences of attacks for Blockchain systems using the example of Bitcoin cryptocurrency. The result of the work can be

applied to development of an integrated approach to building secure Blockchain-based decentralized systems.

1. Attacks on Blockchain technology

1.1. Branching attacks

Branching is a state in which the nodes in the network have a different view of the state of the Blockchain ledger, persisting for long periods of time or indefinitely. Such branches can be created unintentionally due to failures in the mechanism for achieving consensus or incompatibility when updating client software. Branching can also be caused by malicious actions that use conflicting validation rules, or by "malicious mining" (section 2.1). In addition, malicious branching can be either soft or hard, the latter occurring when new blocks accepted by the network are invalid for nodes that have a knowledge of the Blockchain ledger before the branching begins. On the other hand, soft branching occurs when some blocks are invalid for nodes that have a case idea after the branching occurs. Thus, the branching of the Blockchain transaction ledger is a contradictory state that can be used by attackers to cause confusion, conduct fraudulent transactions and spread mistrust in the network [3]. An example of hard branching, which results from peers following conflicting Blockchain ledger status rules is shown on fig. 1.

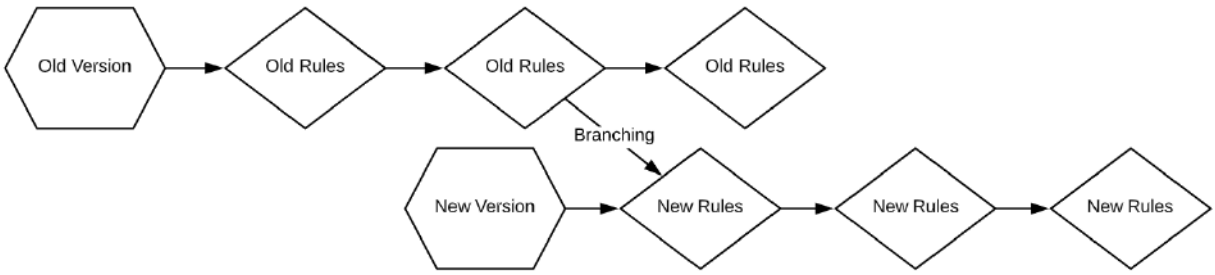


Fig. 1. An example of a hard branching of the Blockchain ledger

An example of the use of Blockchain ledger hard branching is the rollback of transactions on the Ethereum platform to return digital assets after a successful attack on a decentralized autonomous organization (DAO) and theft of a third of the cryptocurrency [1]. However, this required the agreement of most network nodes. In such a scenario, if the delay in achieving consensus is due to a majority attack (or 51 %-attack) or DDoS-attacks, fraudulent actions become difficult and long delays can ultimately lead to the depreciation of the cryptocurrency.

1.2. Obsolete and orphaned blocks

In the process of achieving consensus between participants in the system, two forms of inconsistencies may arise that may leave valid blocks not added to the Blockchain transaction ledger.

1. An "obsolete block" is a block that has been successfully calculated but not accepted in the current main version of the ledger (that is, the version that is most difficult to recreate). Section 2.1 presents that the Blockchain attack vector, known as "malicious mining," can lead to the creation of obsolete blocks in the network, which deprives an honest miner of his reward.
2. An "orphaned block" is a block whose previous (parent) hash field indicates an unauthentic block that is not included in the Blockchain transaction ledger, and therefore cannot be checked and validated.

These discrepancies can be introduced by an attacker or caused by competition conditions in the mining process. Obsolete blocks can initially be accepted by most networks, but they can be rejected later when confirmation is received for a longer chain of blocks (i.e., the new current major version of the transaction ledger state) that does not include this particular block. Fig. 2 shows an example of a Blockchain ledger with obsolete and orphaned blocks.

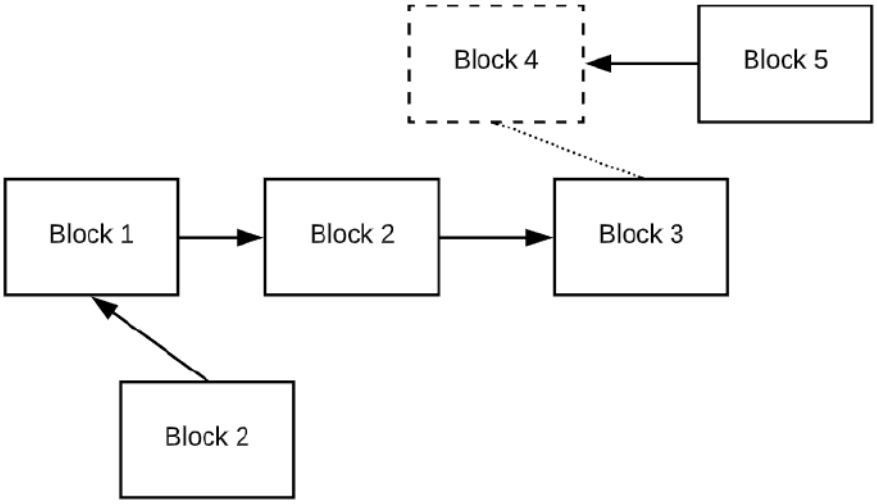


Fig. 2. Example of Blockchain ledger with obsolete and orphaned blocks

It should be noted that the obsolete block (lower block 2 and block 4) are valid, but they are not part of the Blockchain ledger. The orphaned block (block 5) does not have a block preceding it belonging to the current main version of the Blockchain ledger.

In Bitcoin cryptocurrency, the first orphaned block was found on March 18, 2015, this was the beginning of the period of the largest number of orphaned blocks, which lasted until June 14, 2017. Since then, not a single discarded block has been calculated [4].

1.3. Blockchain attacks counteraction

Elimination of the consequences of soft branching of the Blockchain transaction ledger is a relatively simple process, for this it is necessary to achieve a unified opinion on the state of the ledger by all nodes of the network and to resume the decentralized system from this point on. Enabling hard ledger branching can be a difficult task because conflicting versions can be time-consuming and with a large number of transactions over the period of branching. Although the rollback to the ledger version preceding hard branching is a fairly global operation within the framework of a Blockchain-based decentralized system, the decision to carry it out can be achieved by the same principle of consensus building that was presented earlier.

The number of orphaned blocks in Bitcoin cryptocurrency has been decreased due to the transition to highly centralized mining-pool networks, which reduced the likelihood of orphaned blocks, which is high enough for a decentralized mining process.

2. Attacks on Blockchain peer-to-peer network architecture

The peer-to-peer network architecture that underlies Blockchain technology serves as the basis for providing certain guarantees, including security. However, at the same time, this architecture actually contributes to several attack surfaces described in this section.

2.1. The malicious mining

An attack called "malicious mining" is a strategy that some miners choose to try to increase their rewards by intentionally keeping their blocks closed. Instead of revealing the calculation of each block to all participants, such miners continue to calculate new blocks covertly to get a longer version of the Blockchain ledger than the current main system version. As soon as the general main version of the ledger begins to approach the length of the hidden version of the ledger of the malicious miner, they publish the calculated blocks for a reward [5]. The scheme for carrying out an attack of malicious mining is presented in fig. 3.

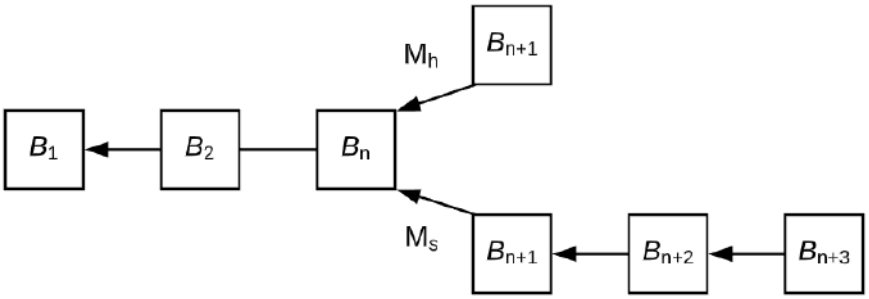


Fig. 3. The scheme for carrying out an attack of malicious mining

Consider the Blockchain ledger with blocks B_1, B_2,…, B_n. Suppose an honest miner M_h has successfully calculated the next block B_{n+1}, and on the same network, the malicious miner M_s has also calculated the next block B_{n+1}. The attacker does not disclose the fact that he successfully calculated a new block and successfully extracts two more blocks – B_{n+2} and B_{n+3}. At the moment, most of the network has a general view on the current main version of the Blockchain transaction ledger, however, despite this, an attack of malicious mining can be carried out.

Let the honest miner M_h has the hash value of block B_{n+1} below both the target threshold set for the current period by the system and the hash value of the attacker block M_s B_{n+1}. If you publish the calculation of only these two blocks, then the new current main version of the ledger with the M_h block would be accepted because of its greater computational complexity compared to the M_s block. Then, after some time, the attacker M_s reveals the calculation of all of his blocks – B_{n+1}, B_{n+2} и B_{n+3}. The mechanism for achieving consensus of Blockchain technology is designed so that the version with a large number of successfully calculated blocks will invariably be selected as the new main version of the ledger. Thus the network switches to the ledger version with M_s blocks, and the B_{n+1} block of the honest miner M_h, for the successful calculation of which computational resources have already been spent, will be considered obsolete. The incentive for an attacker to apply such a mining strategy is to maximize block rewards by covertly calculating and then publishing a longer version of the Blockchain transaction ledger.

The successful conduct of this attack entails the negative consequences of the Blockchain system, since it invalidates the blocks calculated by honest miners who put their computational resources into the operability of a decentralized system. When conducting this attack simultaneously, several attackers open it for other attacks, the relationship between them is shown in fig. 4.

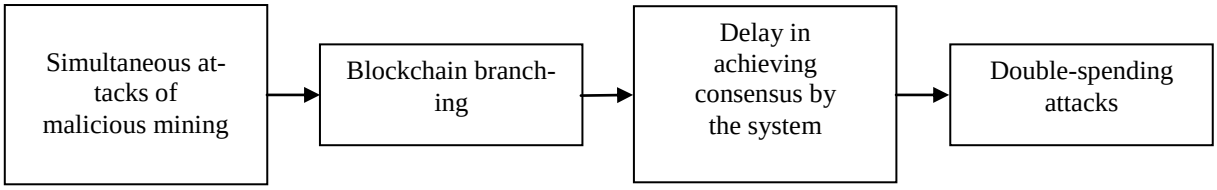


Fig. 4 Consequences of the simultaneous conduct of malicious mining

In the case when two attackers simultaneously carry out this attack, that is, they compete for adding their version of the transaction ledger to the system, the likelihood of branching of the Blockchain ledger increases (section 1). Branching, in turn, can delay in achieving consensus on the network, and this, in turn, can lead to other potential attacks, such as double waste attacks (section 3.2).

2.2. 51 % Attack

A 51 % attack or a majority attack occurs when a single attacker, a group of nodes, or a mining pool (a combination of miners) in a network reaches most of the total computational power of min-

ing in the system and gets the ability to manipulate the functionality of the Blockchain system. Having 51 % of the processing power allows an attacker (s) to:

- prevent verification of transactions or blocks, that is, make them invalid;
- cancel transactions in some time after their confirmation, thereby realizing a double-spending attack;
- not allow other miners in the system to calculate any blocks for a short period of time [6].

In this attack, the attacker's blocks will be added to the Blockchain ledger with a higher probability, since the available computational power allows the attacker to calculate new blocks faster than other participants in the system. An attacker can include fraudulent transactions in their blocks or use them to implement double-spending attacks. Transactions in Blockchain systems are irreversible, and only one transaction of two identical ones can be considered valid.

The 51 % attack is not only theoretical, in July 2014 the association of miners "GHash.IO" owned more than 51 % of the computational power in the Bitcoin network [7]. This has raised concerns about the reliability of cryptocurrency and its vulnerabilities. Later, "GHash.IO" was decreased in size and closed in October 2016. It should be noted that for fraudulent activities it is not always necessary to have more than half of the processing power of the network. A wide range of attacks can be carried out with a sufficient degree of probability in the presence of even 25 % of the computational power of the network.

2.3. DNS-attacks

When you initialize a new node in the network of the Blockchain system, i.e., when you first connect a new member to the network, he will not know about active peer nodes. For example, in the Bitcoin network, to detect them, a bootstrap phase is required, which uses DNS. DNS seeds are requested by the nodes upon joining the network to obtain additional information about other active peers [8]. However, DNS opens up a wide plane for attacks on the Bitcoin network, such as a man in the middle, cache poisoning, etc. As a result, using the plane of DNS attacks, an attacker can potentially isolate the peer nodes of the Blockchain system (by providing them incorrect list of active peers at the boot stage), distribute fake blocks with fraudulent transactions among new nodes, invalidate transactions, etc. [9].

2.4. DDoS-attacks

DDoS-attack is one of the most common attacks on online services. Blockchain technology, despite being a peer-to-peer system, remains susceptible to DDoS-attacks. This is confirmed by successful DDoS-attacks on Blockchain applications such as Bitcoin and Ethereum [10,11]. Manifestations of DDoS-attacks can vary, depending on the nature of the functionality of the Blockchain application, the features of its network architecture and the behavior of peer nodes. For example, on a Bitcoin network, a 51 % attack could lead to a denial of service. In particular, if a group of miners gains significant hash power, they will be able to prevent other participants from adding their calculated blocks to the Blockchain transaction ledger, invalidating current confirmed transactions, thereby causing a malfunction of the system. Intentional branching of the Blockchain ledger can take on the nature of a hard branching, which, in turn, also leads to similar consequences of denial of service.

Another possibility for conducting a denial of service attack is a limited number of transactions in each block of the Blockchain ledger, which can be processed by the network in a separate period of time. For example, on average, Bitcoin cryptocurrency networks require 10 minutes to add a new block, the maximum amount of which is 1 MB. The average transaction volume is approximately 500 bytes, which allows you to place about 2000 transactions in a block, and the maximum number of transactions added to a block in Bitcoin cryptocurrency is 2210 [4]. Based on this, the average transaction processing speed cannot exceed 200 transactions per minute. Taking into account the fact that each transaction requires at least two peers that must participate in the transaction, the total number of active peers served by the network per minute (i.e. when the block containing the transaction is added to the ledger) will be not less than 200.

An attacker can use the operational feature of a decentralized system described above by introducing entities controlled by him into the system, for example, controlling several wallets. In addition, using these entities, an attacker can perform several transactions with a minimum amount of funds between different entities controlled by him. By creating a sufficiently large number of such transactions in a short period of time, the attacker creates a high computational load on the network, necessary to calculate and add his transactions to the ledger. This causes a denial of service for honest users or significantly increases the time for confirming user transactions, which undoubtedly also negatively affects the functionality of the entire system. Moreover, using large delays in confirming transactions of honest users, an attacker can initiate other attacks, for example, a double spending of funds that are not confirmed due to delays.

The Bitcoin cryptocurrency protocol provides that miners do not influence which transactions should be included in the block they compute [8]. Currently, blocks can contain transactions with values up to 0.0001 BTC, which makes it possible to populate the network with low-cost transactions.

2.5. Consensus Delay

Another attack related to the peer-to-peer nature of the Blockchain network is the delay in achieving consensus. This attack was partially presented in the previous section and consists in filling the network with false transactions in order to delay or prevent other participants from reaching consensus on the main version of the transaction ledger. Such delays can be caused either by forcing the network to extract blocks with minimal transactions, or by forcing time to reach consensus on damaged blocks. In particular, since accepting or rejecting false blocks can take a lot of time, this process negatively affects the system's performance and further exacerbates the negative consequences for Blockchain applications, where transactions must be guaranteed to be confirmed with a minimum delay.

2.6. Countermeasures against Peer-to-Peer Architecture Attacks

In a number of researches on malicious mining strategies, countermeasures were proposed that reduce the likelihood of success of this class of attacks and mitigate possible negative consequences [5, 12, 13]. One of the proposed solutions for preventing malicious blocks from being hidden is the "lifetime" of the block, after which the block is automatically rejected by the network and cannot be added to the Blockchain ledger without re-calculation [14]. Another measure to counter malicious mining is a scheme that reduces rewards for an attacker. The essence of this scheme is to add a time stamp to the block, which cannot be falsified, to display the time of calculating the block, then when adding new blocks to the Blockchain ledger, preference is given to more blocks with a newer (fresh) timestamp [13]. This method makes it unprofitable to hide a large number of calculated blocks; thereby conducting such an attack loses all meaning for an attacker, since he will not receive any benefit.

With regard to counteracting the attacks of the majority (51 % attacks), the concept of an improved mechanism for achieving consensus was proposed – a two-phase proof of the work done [7]. The new mechanism for achieving consensus is based on the continuous Markov chain, which includes two computationally complex tasks instead of one. The states of the continuous Markov chain prevent the increase of any particular association of miners above the boundary norm, lowering rewards for miners.

To prevent denial of service attacks aimed at combining miners, a model based on game theory was proposed [15]. Other countermeasures include limiting the minimum amount of funds to create a transaction and increasing the block size to accommodate more transactions, which would increase the system throughput. Another way to increase the system throughput is to reduce the complexity of computing new blocks, which would reduce the time to calculate one block and thereby increase the speed of transaction confirmation in the Blockchain system. It should be noted that each of the proposed methods has its drawbacks. A fairly large number of researches were devoted to the problem of countering DNS attacks, however, the studies were mainly carried out on classical

(on premise) architectures [16]. The attacks discussed in this section are relevant not only for the Bitcoin cryptocurrency, but also for Blockchain-based decentralized systems in general, as they help to identify potential attack planes and the relationships between various attack classes. However, the study of attack surfaces for Blockchain-based systems built in the cloud remains relevant.

3. Attacks on Blockchain Applications

Blockchain technology and its underlying peer-to-peer architecture are separate from application services that use them. Depending on the nature of the applications, they will have their own vulnerabilities. This section presents attacks aimed at Blockchain applications.

3.1. Blockchain Ledger Data Processing

In systems with an open Blockchain ledger, each user has access to transaction data added to the ledger. However, analyzing an open transaction ledger can provide useful information to an attacker. This process is known for processing the data of the Blockchain ledger or Blockchain ingestion, and this process can have negative consequences for the Blockchain system or its users. For example, a credit card company in the open market may use the analysis of data from the open transaction ledger of the Blockchain system to examine and optimize its own transaction processing schemes in order to compete with digital currency. A demonstration of the potential use of publicly available Blockchain ledger data for creating relationships with transaction data and user identification based on graph analysis is presented in [17].

3.2. Double-spending attacks

To demonstrate a double-spending attack, consider the following scenario. In cryptocurrencies, the goal of creating a transaction is to transfer ownership of a digital asset from the sender's address to the recipient's public address, and the value of the transaction is signed using the private key. Once the transaction is signed, it is transmitted to the network in which the recipient verifies the transaction. Verification by the recipient occurs when the recipient looks at the sender’s unspent transaction output, verifies the sender’s signature and waits for the transaction to be calculated by the miners and added to the Blockchain transaction ledger with the new block. This process can take several minutes, and in the Bitcoin cryptocurrency its average time is 10 minutes.

On systems with fast transaction confirmation, or if the recipient trusts the system, he can send the product to the sender of the transaction before it is accepted by the network. This gives the sender the opportunity to sign the same transaction and send it to another recipient. Signing the same transaction with a private key and sending it to two different recipients is called a double-spending attack. During this attack, there are two transactions obtained from the same unspent output of the sender, and only one of them is ultimately added to the Blockchain transaction ledger, and the attacker receives two products by paying only one of them. A delay in consensus on the network (section 2.5) or an attack of 51 % (section 2.2) may increase the attacker's chances of successfully conducting double-spend attacks.

3.3. Digital Wallet Theft

The theft of a digital wallet has negative consequences for the Blockchain system, since the keys associated with peer nodes are stored in the user's digital wallet. For example, in Bitcoin cryptocurrency, by default, the wallet is stored in unencrypted form, which allows an attacker to know the user's credentials and the nature of the transactions conducted by him. There are many services that offer secure storage of digital wallets of users, however, these services can also be compromised, and data can be taken by attackers [1].

3.4. Countermeasures against attacks on Blockchain applications

Many different countermeasures have been proposed with respect to attacks on Blockchain applications. For example, to protect blocks, it is recommended that you keep wallet backups and pro-

tect the keys used to sign transactions. Passwords are easy to crack, so a separate password strength policy is required in the system.

New decentralized cryptocurrency platforms, such as Zcash, hide transactions and maintain the anonymity of users in the Blockchain ledger, thereby preventing the possibility of processing data that is publicly available in the transaction ledger. A double-spend attack is practically unrealizable in systems with fast transaction confirmation, but in systems with a low rate of adding new blocks to the transaction ledger, such an attack has a high chance of success. One of the possible approaches to solving the problem is the use of one-time (or multiple) signatures, such as the extended Merkle signature scheme (XMSS) [18,19].

Conclusion

In this paper, we investigated the attack surfaces for Blockchain technology. Attacks on cryptographic designs of Blockchain technology, peer-to-peer network architecture and applications are considered. The study identified the main threats to Blockchain-based decentralized systems and analyzed the latest security researches of decentralized systems based on Blockchain technology. Some attacks can be carried out with a fairly high probability even despite the existing countermeasures, the work also demonstrated the relationship between the various sequences of attacks.

References:

1. Siegel D. Understanding the DAO attack. [Online]. 2016. Available: https://www.coindesk.com/understanding-dao-hack-journalists .

2. Baldwin C. Bitcoin worth 72 million stolen from Bitfinex exchange in Hong Kong [Online]. Reuters, 2016. Available: http://reut.rs/2gc7iQ9.

3. Kwon Y., Kim D., Son Y., Vasserman E., Kim Y. Be selfish and avoid dilemmas: Fork after withholding (FAW) attacks on Bitcoin, in CCS '17: Proceeding of the 2017 ACM SIGSAC Conference on Computer and Communications Security. 2017. P. 195-209.

4. Eyal I., Sirer E. G. How to disincentivize large Bitcoin mining pools. Bitcoin Block Explorer. 2014. [Online]. Available: https://www.blockchain.com/charts.

5. Eyal I., Sirer E.G. Majority is not enough: Bitcoin mining is vulnerable // Proceedings of the Eighteenth International Conference on Financial Cryptography and Data Security. 2014. P. 436-54.

6. Bitcoin Community. “51 % Attack”. 2017. [Online]. Available: https://learncryptography.com/cryptocurrencyl5l-attack.

7. Bastian M. Preventing the 51 %-attack: A stochastic analysis of two phase proof of work in Bitcoin. [Online]. 2015. Available: https://goo.gl/nJsMzV.

8. Bitcoin developer guide. [Online]. 2017. Available: https://bitcoinorg/en/developer-guide.

9. Kang A.R., Spaulding J., Mohaisen A. Domain name system security and privacy: Old problems and new challenges. [Online]. CoRR. 2016. Available: http://arxiv.org/abs/1606.07080.

10. Muncaster P. World's largest Bitcoin exchange Bitfinex crippled by DDoS. [Online]. 2017. Available: http://bit.ly/2kqo6HU.

11. Cimpanu C. Bitcoin trader hit by 'severe DDoS attack' as Bitcoin price nears all-time high. [Online]. 2017. Available: http://bit.ly/21A5iT6.

12. Sapirshtein A., Sompolinsky Y., Zohar A. Optimal selfish mining strategies in Bitcoin // Financial Cryptography and Data Security. Springer. 2016. P. 515-532.

13. Heilman E. One weird trick to stop selfish miners: fresh Bitcoins, a solution for the honest miner // Financial Cryptography and Data Security. Springer. 2014. P. 161-169.

14. Solat S., Potop-Butucaru M. ZeroBlock: Preventing selfish mining in Bitcoin // arXiv Preprint. ArXiv: v:1605.02435. 2016.

15. Johnson B., Laszka A., Grossklags J., Vasek M., Moore T. Game-theoretic analysis of DDoS attacks against Bitcoin mining pools // Financial Cryptography and Data Security. Springer. 2014. P. 72-86.

16. Silva P. DNSSEC: The antidote to DNS cache poisoning and other DNS attacks // An F5 Networks, Inc Technical Brief. 2009.

17. Fleder M., Kester M.S., Pillai S. Bitcoin transaction graph analysis // arXiv Preprint Xiv:1502.01657. 2015.

18. Huilsing A., Butin D., Gazdag S., Mohaisen A. XMSS: Extended hash-based signatures. [Online]. 2015. Available: https://www.ietf.org/id/draftirtf-cfrg:xmss-hash-based-signatures-10.txt.

19. Saad M., Mohaisen A., Kamhoua C., Kwiat K., Njilla L. Countering double spending in next-generation Blockchains // 2018 IEEE International Conference on Communications. Kansas City. 2018.

Kharkiv National University
of Radio Electronics

Received 25.01.2020

УДК 004.056.5 **DOI:10.30837/rt.2020.1.200.11**

І.Д. ГОРБЕНКО, д-р техн. наук, О.О. КУЗНЕЦОВ, д-р техн. наук,
М.О. ПОЛУЯНЕНКО, канд. техн. наук, А.С. КІЯН, К.Є. ЛИСИЦЬКИЙ, С.О. КАНДІЙ

ПРОТОТИПУВАННЯ ДЕЦЕНТРАЛІЗОВАНОЇ СИСТЕМИ ЕЛЕКТРОННОГО БЛОКЧЕЙН-ГОЛОСУВАННЯ

Вступ

Для забезпечення захищеності інформаційних ресурсів, надійності їх розподіленого зберігання, розгортання децентралізованих систем управляння та різних за функціональним призначенням інформаційних сервісів та послуг застосовуються блокчейн-мережі [1 – 3].

Зазвичай технологія блокчейн застосовується у різних додатках [1]: для створення криптовалют та запрограмованих юридичних зобов'язань (смарт-контрактів); при побудові децентралізованих сховищ (електронні реєстри, кадастри, тощо) та систем електронних довірчих послуг (ідентифікація, голосування, інфраструктура відкритих ключів – ІВК, тощо). На сьогодні в світі вже існує понад 1100 видів цифрових грошей із загальною капіталізацією 133 мільярди доларів (за даними CoinMarketCap – Forbes). В Україні понад 100 приватних компаній та окремих проектів задіяно в індустрії блокчейну (за даними Асоціації Блокчейн України), 37 % з них – від українських інвесторів, 63 % – від іноземних інвесторів. За технологією блокчейн створено державний майданчик для онлайн аукціонів України OpenMarket (СЕТАМ), де Міністерство юстиції України продає арештоване і конфісковане майно [4].

Слід відзначити, що використання нової та неперевіреної часом технології зазвичай несе додаткові ризики та загрози. Зокрема, необхідно проводити експертні випробування з наступних питань:

- безпека технології блокчейн (правильність формування блоків, транзакцій та їх взаємодії);
- безпека транспортного рівня мережі блокчейн (правильність формування повідомлень при комунікації між вузлами мережі);
- безпека вузлів мережі блокчейн (правильність комунікації вузлів та коректність обробки помилок, що можуть виникати);
- безпека консенсусу (правильність роботи протоколів консенсусу та їх захищеність від існуючих та потенційних атак);
- безпека криптографічних модулей (правильність реалізації криптографічних перетворень).

Зазначені проблемні питання ускладняються через переважне застосування інформаційних технологій іноземного виробництва, експертні дослідження щодо яких не проводилися через їх складність та дороговизну.

Окремо слід зазначити можливість застосування найближчим часом квантових методів обчислення для реалізації існуючих та потенційних атак на різні компоненти блокчейн-систем. Зокрема, за прогнозами Національного інституту стандартів і технологій США в найближчі 5 – 10 років стануть доступними універсальні квантові обчислювачі, здатні проводити криптоаналіз практично всіх алгоритмів асиметричного шифрування, інкапсуляції ключів, електронного підпису, тощо [5 – 7].

Отже дослідження технології блокчейн, вивчення її складових, зокрема оцінка інформаційної та функціональної безпеки, прототипування децентралізованих систем, побудованих за цією технологією є безумовно важливим та актуальним завданням.

ПАТ «ІІТ» під керівництвом Департаменту захисту інформації Державної служби спеціального зв'язку та захисту інформації України проведено низку заходів щодо пошукових досліджень технології блокчейн, а також можливостей і напрямків її імплементацій у державній сфері. Досліджено можливість застосування блокчейн-систем при проведенні публічних опитувань, голосувань, референдумів, виборів; створення національної системи електронних

грошей (національної криптовалюти); використання запрограмованих юридичних зобов'язань (смарт-контрактів); відмовостійкого електронного документообігу, електронних реєстрів, кадастрів, тощо. У ході досліджень запропоновано ряд концепцій з використанням переваг блокчейн-технології щодо створення децентралізованих системи електронних довірчих послуг (ідентифікація, інфраструктури відкритих ключів, голосувань). Розроблено апаратно-програмний комплекс для досліджень функціонування реально діючих блокчейн-систем та на його базі розгорнуто прототип системи електронного голосування.

Мета статті – викладення окремих результатів з прототипування децентралізованої системи електронного блокчейн-голосування, дослідження інформаційної та функціональної безпеки, обґрунтування рекомендацій щодо подальшого впровадження в Україні.

Структура децентралізованої системи електронного блокчейн-голосування

Технологія блокчейн призначена для створення захищених цифрових реєстрів, стійких до несанкціонованого доступу. Інформація зберігається розподіленим способом (тобто без центрального сховища) та без центрального органу (наприклад, банку, компанії, або органу влади), при цьому унеможливлюються зміни в уже внесених в реєстр даних [1 – 3].

До безумовних переваги такої технології слід віднести наступні [1]:

– Блокчейн забезпечує історично стійке зберігання інформації. Окремі записи (блоки) зв'язується криптографічними перетвореннями, які унеможливлюють зміну жодного біту в уже внесених в реєстр даних;
– Децентралізація забезпечує надійність збереження інформації. Навіть за умови блокування, виходу із ладу або втрати керування над значною часткою вузлів мережі блокчейн цифрові реєстри не можуть бути змінені або втрачені;
– Криптографічні перетворення забезпечують безпеку інформації (цілісність, неспростовність, доступність та конфіденційність).

Отже, практичне впровадження технології блокчейн підвищує довіру до інформаційних ресурсів та сервісів (що є особливо актуальним для державних установ); зменшує час та накладні витрати; унеможливлює втручання центрального органу та відповідні корупційні дії; підвищує надійність збереження інформації та якість наданих послуг.

Для прототипування основних складових системи електронного голосування запропонована дворівнева архітектура, спрощена схема якої наведена на рис. 1.

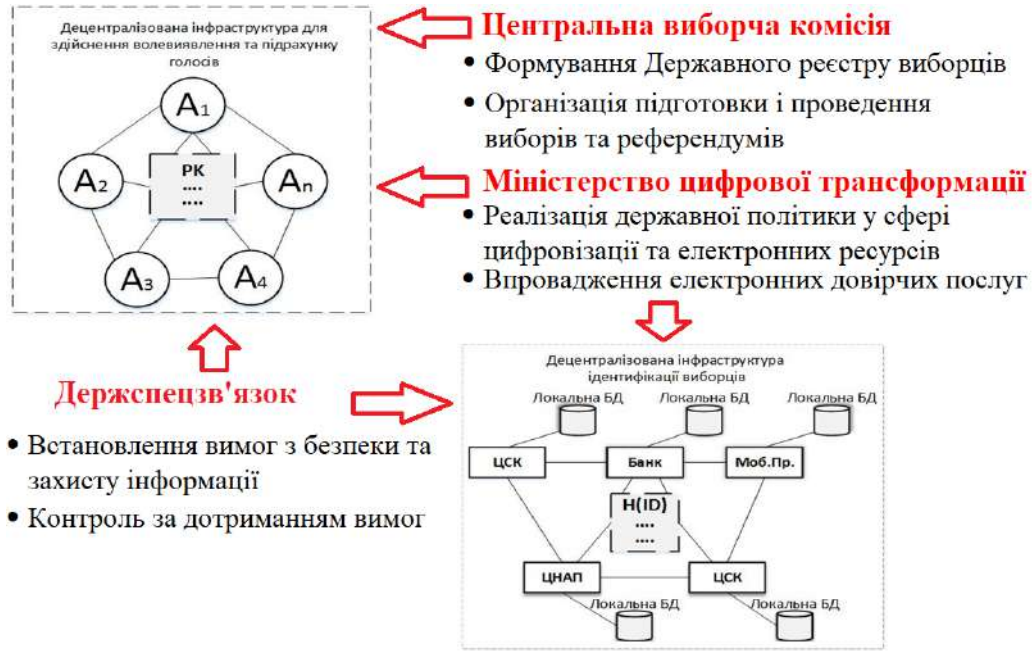


Рис. 1. Спрощена архітектура децентралізованої системи електронного голосування

Децентралізована інфраструктура ідентифікації виборців (ДІ eID) має забезпечувати процедуру надійної ідентифікації користувачів та формування списків легітимних виборців. Вона складається із провайдерів послуг ідентифікації громадян (далі- IdP, провайдери). Необхідно забезпечити реалізацію процедури ідентифікації за допомогою:

- засобів BankID;
- засобів MobileID;
- електронного паспорта громадянина;
- цифрового (електронного) підпису:
- програмний носій цифрового підпису;
- апаратний носій цифрового підпису.

Відповідно до висунутих вимог, в ролі *IdP* можуть виступати:

- банківські установи;
- мобільні оператори;
- центри міграційної служби (центри надання адміністративних послуг – ЦНАП);
- центри сертифікації ключів національної системи ЕЦП.

Регламенти функціонування провайдерів встановлюються Законом України "Про електронні довірчі послуги" [8], імплементованим Регламентом ЄС [9] та іншими міжнародними та національними нормативними документами [10 – 12].

Вимоги та процедури ідентифікації залежать від конкретного провайдера.

Мережа провайдерів ідентифікації сформована поза межами децентралізованої системи електронного голосування. Кожен IdP має попередньо сформовану локальну базу даних своїх користувачів, яка містить їхні ідентифікаційні дані та, можливо, локальні ідентифікатори. Відповідальність за надійне збереження та коректне використання локальних баз даних покладається на IdP.

Для організації інфраструктури ідентифікації в рамках децентралізованої системи електронного голосування, IdP об'єднуються в окрему приватну мережу блокчейн (private permissioned Blockchain). В даній мережі кожен із IdP виступає вузлом-валідатором. Необхідно зазначити, що для такої мережі немає необхідності застосовувати складні та енергоємні протоколи консенсусу, оскільки мережа поєднує довірені («чесні») вузли.

Децентралізована інфраструктура для здійснення дистанційного волевиявлення та підрахунку голосів має забезпечувати процес дистанційного волевиявлення зареєстрованих (авторизованих) легітимних виборців та процес підрахунку голосів. Додатково в даній інфраструктурі повинні бути організовані процеси реєстрації кандидатів. Довіреними вузлами в даному випадку будуть виступати аналоги територіальних виборчих громад, проте завдяки децентралізованому підходу та технології blockchain наявність головного органу (центральної виборчої комісії) не потрібне. Така організація значно зменшує ризики, пов'язані із людським фактором, включаючи можливості підкупу членів центральної виборчої комісії.

Для організації інфраструктури дистанційного волевиявлення в рамках децентралізованої системи електронного голосування представництва відповідальних за проведення виборчого процесу, наприклад територіальні виборчі громади, (A1, A2,...,An), подібно до провайдерів ідентифікації, об'єднуються в окрему приватну мережу блокчейн (private permissioned Blockchain), в якій кожен із Ai виступає вузлом-валідатором – в сукупності вони являють собою децентралізоване Агентство (A). Аналогічно до верхньої мережі Blockchain, у нижній також немає необхідності застосовувати складні та енергоємні протоколи консенсусу, оскільки мережа поєднує довірені («чесні») вузли. Вузли-валідатори формують гаманці для легітимних виборців та проводять процедуру автентифікації виборців. Також вони відповідають за процес формування гаманців для альтернатив (кандидатів).

На рис. 1 наведено також відповідальні міністерства та відомства із зазначенням основних завдань та функцій при розгортанні децентралізованої системи електронного голосування.

Обрис прототипу системи електронного голосування

На сьогодні існує низка програмних рішень, що надають інструменти для розробки, розгортання та підтримки систем, заснованих на використанні технології блокчейн. Серед існуючих альтернатив для реалізації прототипу системи електронного голосування було обрано платформу Exonum [13, 14] з декількох причин.

По-перше, Exonum спроектовано таким чином, що система працює виключно на обчислюваних потужностях вузлів-валідаторів, які зацікавлені у її надійному функціонуванні. Такими вузлами-валідаторами у випадку електронного голосування є представники децентралізованого агентства. Кожний з них зберігає у себе копію стану бази даних, усі атомарні операції щодо якої, оформлені в блоки та формують Blockchain. Окрім того, система, побудована на Exonum, продовжує коректно функціонувати навіть у випадку компрометації чи відключення 2/3 вузлів-валідаторів системи, та унеможливлює підробку даних блокчейна шляхом змови вузлів за рахунок наявності процедури «Біткоінг-анкорінг», що регулярно відправляє зліпки стану системи в публічний блокчейн Біткоіна. Такий підхід дозволяє унеможливити наявність неправомірних дій зі сторони вузлів-валідаторів та попередити атаки на них.

По-друге, платформа Exonum надає високу продуктивність, що в сотні разів перевищує показники швидкодії її альтернатив, а саме забезпечується виконання до 5000 транзакцій в секунду із затримкою в 0,5 с. Така продуктивність є важливою характеристикою під час розробки системи електронного голосування, коли протягом одного дня усі громадяни мають здійснити доступ та волевиявлення у системі. Додатковою перевагою, що забезпечується Exonum, є тонкий клієнт, за рахунок якого кінцеві користувачі(виборці або спостерігачі) можуть перевірити наявність та коректність транзакцій.

По-третє, нині вже функціонують успішні проекти, реалізовані з використанням Exonum, не тільки у комерційному секторі, але і на державному рівні. Одним з таких прикладів є система реєстрації земельних ділянок у Грузії, реалізована сумісно компанією Bitfury та Національним агентством публічного реєстру Грузії. Використання Exonum у цьому випадку дозволило не тільки запобігти неправомірному оскарженню прав власності за рахунок видачі власникам цифрових сертифікатів їх активів, підкріплених криптографічними підтвердженнями (геш-значеннями), що публікуються у Blockchain та не можуть бути у подальшому змінені, але і значно зменшити часові та матеріальні затрати під час процесу реєстрації земельних ділянок.

Децентралізована процедура проведення виборчого процесу та підрахунку голосів є верхньою мережею розробленої дворівневої архітектури електронного голосування. Протокол голосування у подібній системі з функціональної точки зору складається з наступних етапів:

1. Формування списків легітимних виборців, тобто виборців, що мають право здійснювати волевиявлення у межах конкретного виборчого процесу.
2. Генерація гаманців легітимних виборців у системі голосування, що є необхідною умовою для подальшого їх доступу до системи.
3. Реєстрація кандидатів у децентралізованій системі голосування, інформація про яких попередньо пройшла перевірку спеціальними органами.
4. Автентифікація виборців при першому доступі до системи голосування системи, що полягає у зарахуванні на рахунок виборця одного голосу, який він зможе віддати на користь того чи іншого кандидата.
5. Здійснення волевиявлення у системі, після якого виборець вже не може змінити свій вибір.
6. Підрахунок голосів у системі голосування, що значно полегшує сучасний процес з точки зору використовуваного часу, матеріальних та людських ресурсів

Перший етап реалізується нижньою мережею архітектури, інші функціонують у верхній мережі, прототип якої було практично реалізовано. Таким чином у прототипі передбачено, що виборці пройшли попередню ідентифікацію у певного провайдера та володіють ключовою парою, відкритий ключ якої поступив до верхньої мережі і є деперсоналізованим іден-

тифікатором користувача у системі голосування. Загалом схему голосування можна уявити наступним чином (рис. 2).

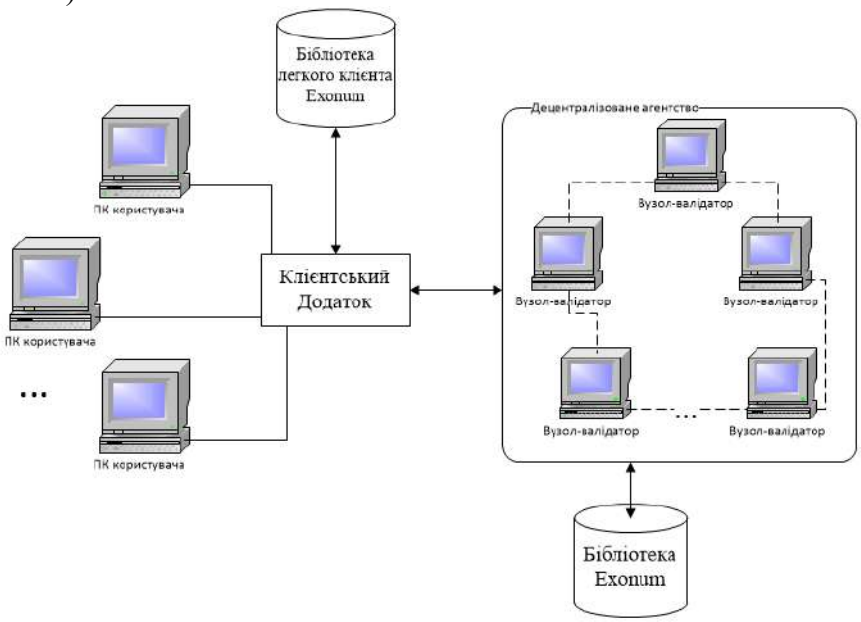


Рис. 2. Структурна схема прототипу електронного голосування

Логіка роботи системи реалізується за рахунок комплексного функціонування її чотирьох складових частин:

- клієнтського додатку;
- децентралізованого агентства;
- бібліотеки Exonum;
- бібліотеки легкого клієнта Exonum.

Бібліотеки Exonum та легкого клієнта Exonum зазначені на структурній схемі системи, оскільки мають принципове значення для реалізації функціонування програмного забезпечення. Бібліотека Exonum у складі системи забезпечує створення приватного Blockchain, вузлами якого є представництва децентралізованого агентства, чіткий регламент обробки транзакцій, який незалежно від кількості вузлів, не може бути змінено, забезпечення прозорості обробки транзакцій, що може бути продемонстрована третім сторонам, підписання транзакцій та інше.

Етап 2 – 6 описаного вище протоколу у прототипі представляє собою конкретний вид транзакції у системі, інформація про яку записується до Blockchain та не може бути у подальшому змінена. Відповідно, всього у системі наявні 4 типи транзакцій: реєстрація кандидата, реєстрація виборців, зарахування голосу на рахунок виборця при його першому вході до системи і перерахування голосу з рахунку виборця на рахунок кандидата під час здійснення волевиявлення. У свою чергу легкий клієнт Exonum надає інструменти формування та відправлення транзакцій до мережі Blockchain Exonum, що представлена децентралізованим агентством, та формування запитів до вузлів та перевірку їх відповідей.

Для коректного функціонування прототипу системи голосування через клієнтський додаток з системою взаємодіють три типи користувачів, яким надано конкретні повноваження:

1. Виборець: здійснює вхід до системи голосування; здійснює передачу голосу обраному кандидату; переглядає особисту інформацію кандидата.
2. Адміністратор: здійснює вхід до системи голосування; додає особисту інформацію кандидата до системи, створюючи йому особистий гаманець; отримує доступ до поточних результатів голосування; переглядає особисту інформацію кандидата; володіє інструментами для перевірки коректності транзакції у Blockchain.

3. Кандидат: не здійснює вхід до системи, оскільки його особистий ключ невідомий; отримує голоси від виборців.

Кожен користувач в системі має зареєстрований гаманець, ідентифікатором якого є його відкритий ключ. На етапі авторизації користувач у клієнтському додатку вводить свою ключову пару, і якщо гаманець з відповідним відкритим ключем наявний у системі, а секретний ключ відповідає відкритому (при цьому секретний ключ відомий лише користувачу, а його коректність перевіряється шляхом підписання контрольної фрази), отримує доступ до системи. При цьому, як було зазначено, ключова пара кандидата невідома ні одній зі сторін виборчого процесу, тому здійснити вхід до системи від його обличчя неможливо.

Після отримання доступу користувачем-виборцем системою здійснюється перевірка, чи брав він участь у виборчому процесі. Якщо виборець вже віддав голос за одного з кандидатів, його дії у системі обмежуються переглядом інформації про зареєстрованих кандидатів, у випадку якщо на його рахунку ще наявний голос, виборець може віддати його за обраного кандидата, ініціювавши при цьому транзакцію голосування, яка буде підписана його ключем і внесена до Blockchain.

У свою чергу користувач-адміністратор після отримання доступу до системи має право зареєструвати кандидата, заповнивши усю інформацію про нього та підписавши транзакцію про створення кандидата своїм ключем, переглянути кількість голосів відданих за кандидата, що відбувається шляхом отримання інформації про стан гаманця кандидата, переглянути реєстр Blockchain, а саме дані транзакцій, що записані до нього, їх статус, та ключ того, ким було ініційовано певну транзакцію.

Отже, клієнтський додаток забезпечує інтерфейс для взаємодії користувача та безпосередньо логіки функціонування системи. Він є проміжним елементом взаємодії децентралізованого агентства, діяльність якого побудована на використанні фреймворку Exonum та легкого клієнта Exonum. З цієї точки зору функціями клієнтського додатку є:

- ініціювання створення транзакції;
- ініціювання запиту на отримання даних.

Функціональна взаємодія клієнтського додатку, вузлів-валідаторів та легкого клієнта з метою створення транзакції продемонстрована на рис. 3.

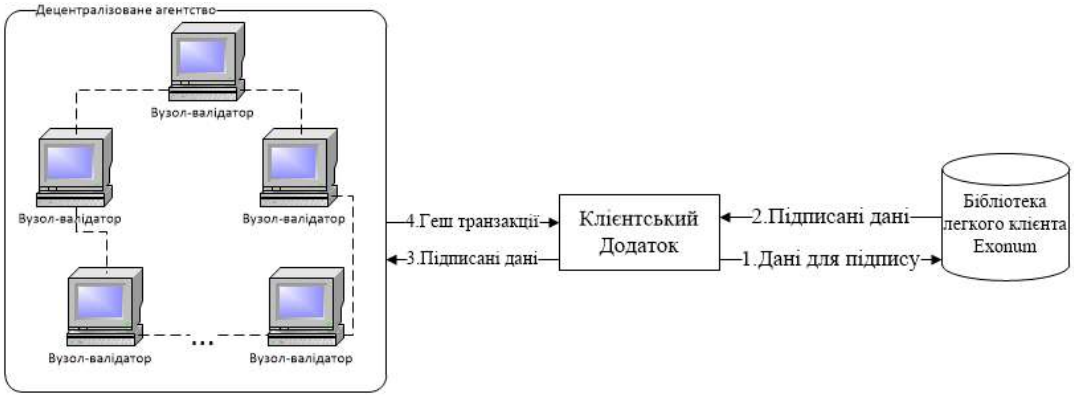


Рис. 3. Схема взаємодії складових системи в межах формування транзакції

Ініціювання створення транзакцій забезпечує виконання загальних функцій системи таких, як реєстрація виборця, голосування та реєстрація кандидатів у децентралізованій системі волевиявлення.

Відповідно ініціювання запиту на отримання даних підтримує авторизацію користувача у системі та підрахунок голосів, відданих на користь конкретного кандидата. Схема взаємодії клієнтського додатку, вузлів-валідаторів та легкого клієнта під час запиту даних продемонстрована на рис. 4.

Рис. 4. Схема взаємодії складових системи в межах запиту даних

Таким чином, прототип уособлює основні процеси, які необхідні для організації виборчого процесу. При цьому кожна дія, що змінює стан Blockchain реєструється і не може бути спростована. Цей факт забезпечує гарантію незмінності вибору, єдиноразовість здійснення волевиявлення одним виборцем, а також зарахування голосів на рахунок кандидатів тільки від легітимних виборців.

Обґрунтування механізмів та протоколів безпеки технології блокчейн

Ключовим аспектом технології блокчейна є визначення того, хто з користувачів публікує наступний блок. Це вирішується шляхом реалізації однієї з багатьох можливих моделей консенсусу. В інклюзивних блокчейн-мережах зазвичай існує безліч вузлів публікації, що конкурують одночасно за публікацію наступного блоку. Вони зазвичай роблять це, щоб отримати винагороду за формування блоку та/або підтвердження транзакцій. Як правило, вони не довіряють користувачам, які можуть знати один одного тільки за їх публічними адресами. Кожен, хто публікує блок, швидше за все, мотивований прагненням до фінансової вигоди, а не добробутом інших вузлів публікацій або навіть самої мережі [1].

У такій ситуації навіщо користувачеві поширювати блок, який інший користувач намагається опублікувати? Крім того, хто вирішує конфлікти, коли кілька вузлів публікують блок приблизно в один і той же час? Щоб вирішувати ці протиріччя, технологія блокчейн використовує консенсусні моделі, щоб дозволити групі користувачів, які не мають взаємної довіри один до одного, працювати разом.

Консенсус є процедурою прийняття рішення. Його мета – забезпечити те, щоб всі учасники мережі погодили свій поточний стан після додавання нової інформації, блоку даних або пакета транзакцій. Іншими словами, консенсус-протокол гарантує те, що ланцюг вірний, і дає стимул учасникам залишатися чесними (тобто дотримуватися процедур визначених у системі). Це є важливим процесом, який запобігає ситуації, коли хтось контролює всю систему, і процедура консенсусу гарантує те, що всі учасники системи дотримуються правил мережі.

Коли користувач приєднується до блокчейн-мережі, він погоджується з початковим станом системи. Це записано в єдиному попередньо сконфігурованому блоці – генезис блоці. Кожна блокчейн-мережа має опублікований генезис блок, і кожен блок повинен бути доданий в блокчейн після нього на основі узгодженої моделі консенсусу.

Концептуально безпека блокчейн-технології ґрунтується на наступних властивостях:

- Узгоджений початковий стан системи. Це є єдиний попередньо сконфігурований блок – генезис блок.
- Користувачі погоджуються з консенсусною моделлю, на основі якої блоки додаються в систему та оновлюється її поточний стан.
- Кожен блок пов’язаний з попереднім блоком шляхом включення криптографічного геш-значення попереднього заголовку блока (за винятком першого генезис-блоку, який не має попереднього блоку).

- Об’єктивність. Для визначення поточного стану системи не потрібна довіра авторитетним джерелам – корінь довіри знаходиться в самому блокчейні та у використанні криптографічно надійних функцій – користувачі можуть перевірити кожен блок самостійно.

Незалежно від моделі консенсусу, кожен блок повинен бути дійсним і, отже, може бути перевірений незалежно кожним користувачем блокчейн-мережі. Використовуючи початковий стан та можливість перевірки кожного блоку, користувачі можуть незалежно та самостійно узгодити поточний стан блокчейн-системи.

У табл. 1 наведено основних виділені ідей [2], які можуть / повинні (в залежності від поставлених завдань та вибраних шляхів реалізації) бути закладені в механізми консенсусу.

Таблиця 1

Основні чинники механізмів консенсусу у блокчейн-системах

Послуги / показники	**Визначення**
Децентралізоване управління	Єдиний центральний орган не може забезпечити завершеність транзакції.
Структурованість взаємовідносин	Вузли обмінюються повідомленнями заздалегідь визначеними способами, які можуть включати етапи або рівні.
Автентифікація	Процес надає засоби для перевірки особи учасників.
Цілісність	Забезпечення перевірки цілісності транзакції (наприклад, математично за допомогою криптографічних геш-функції).
Неспростовність	Надаються засоби для перевірки того, що передбачуваний відправник дійсно відправив повідомлення
Конфіденційність	Конфіденційність гарантує, що тільки визначений одержувач може прочитати повідомлення.
Відмовостійкість	Мережа працює ефективно і швидко, навіть якщо деякі вузли, сервери або інші компоненти мережі виходять з ладу або працюють неналежним чином.
Продуктивність	Враховує пропускну здатність, життєздатність, масштабованість та затримку.

В межах цих ідей існують значні відмінності між різними механізмами консенсусу. Ряд перерахованих вище параметрів реалізується за допомогою основних методів криптографії, які використовують математичні функції для забезпечення безпеки і конфіденційності. Ці методи включають симетричне і не симетричне шифрування і геш-функції.

Ключовою особливістю блокчейн-технології є те, що немає необхідності в тому, щоб довірена третя сторона надавала стан системи – кожен користувач у системі має все необхідне, щоб власноруч, з деякого доступного набора станів визначитися з поточним станом та перевірити цілісність системи.

Щоб додати новий блок в блокчейн-систему, всі вузли з часом повинні прийти до спільної згоди, проте деякі тимчасові розбіжності можливі.

В блокчейн-мережах модель консенсусу повинна працювати навіть у присутності, можливо, недобросовісних користувачів (тобто таких, які навмисно або ненавмисно недотримуються визначених у системі процедур), оскільки ці користувачі можуть спробувати порушити або спотворити ланцюжок блоків.

Звернемо увагу на те, що технологія блокчейн не є механізмом, який безумовно гарантує цілісність та справжність даних у блокчейн-мережі, технологія блокчейн лише надає механізм для виявлення таких маніпуляцій з даними у системі.

У деяких блокчейн-мережах може існувати деякий рівень довіри між вузлами публікації. В залежності від рівня цієї довіри може знадобитися узгоджена модель ресурсномістких процесів (час обчислень, інвестиції тощо) щоб визначити який учасник додає наступний блок до ланцюжка. Як правило, в міру підвищення рівня довіри зменшується потреба у використ-

танні ресурсів в якості міри формування довіри. Для деяких ексклюзивних блокчейн реалізацій уявлення про консенсус виходить за рамки забезпечення достовірності блоків, але охоплює всі системи перевірок від пропозиції транзакції до її остаточного включення в блок.

Варто відзначити, що завдання розподіленого консенсусу не специфічна для блокчейн систем і має добре перевірені рішення для багатьох інших розподілених систем. Навіть завдання консенсусу, в якому вузли можуть бути недобросовісними, – завдання візантійського консенсусу – вперше була сформульовано в 80-х роках минулого століття, а методи його вирішення з'явилися в кінці 90-х.

Як і всі розподілені системи, реалізація блокчейна пов'язана з низкою проблем – затримка в мережі, помилки при передачі, помилки в програмному забезпеченні, лазівки в системі безпеки та хакерські погрози, що впливає на її масштабованість, ефективність і безпеку. Більш того, децентралізований характер технології передбачає, що жодному з учасників системи не можна довіряти. Можуть з'явитися шкідливі вузли, а також різниця в даних через суперечливість інтересів. Для протидії вказаним проблемам існують кілька базових моделей консенсусу. Умовно всі моделі консенсусу можна розділити на декілька основних типів зображених на рис. 5.

Пошук методу досягнення консенсусу, без довіри між учасниками в розподіленому середовищі, який може масштабуватися необмеженим лінійним способом та був би надійним, триває і досі.

Консенсуси, засновані на доказах, працюють з тим припущенням, що учасники мережі будуть витрачати фінансові ресурси, щоб отримати прийняття рішення про вибір наступного блоку. Унікальність цих алгоритмів в тому, що вони економічно стимулюють вузли до певної фінансової участі для отримання можливості отримати винагороду за блоки. Ці моделі консенсусу роблять протоколи стійким за своєю природою до атак Сивіли. При цьому відпадає необхідність в Інфраструктурі Відкритих Ключів або інших схемах автентифікації.

Будь-яка з децентралізованих систем повинна мати стимул для підтримки свого існування учасниками цієї системи. Як правило, в ролі стимулу виступає матеріальна зацікавленість, що характерно для інклюзивних систем і для ексклюзивних систем, спрямованих на фінансову сферу. Як «стимул» участі може бути адміністративний ресурс, який зобов'язує учасників підтримувати функціонування блокчейн-систем. І якщо в другому випадку кількість учасників і їх можливості в підтримці роботи блокчейн-мережі визначаються і обмежуються обсягом фінансування, то в першому визначаються їх вигодою, що тягне за собою ризики пов'язані з монополізації децентралізованої системи.

Крім того, з ростом розміру блокчейна зростають вимоги до сховища, пропускної здатності та обчислювальної потужності, що застосовуються до повноправних вузлів мережі. У певний момент система стає досить громіздкою, у якої повноправно функціонувати можуть лише деякі вузли, які можуть дозволити собі ресурси для обробки блоків – що призводить до ризику централізації.

Розглядаючи більш детально життєві цикли блокчейн-систем, що мають фінансову стимуляцію підтримки свого існування, бачимо, що нарощування вливання в блокчейн систему її учасника призводить до збільшення прибутку цього учасника, що стимулює його до максимального нарощування частки своєї участі в блокчейн-системі. Для блокчейн-систем, побудованих на механізмах консенсусу, в основі яких лежить виконання трудомісткого завдання, це виражається в закупівлі та побудові дорогих ферм на спеціалізованому високопродуктивному обладнанні; якщо розглядати механізми консенсусу, засновані на частці володіння, – виражається в прямому вливанні фінансових ресурсів; при використанні BFT протоколів консенсусу – створення додаткової кількості учасників (які, як правило, вимагають певного фінансування); інші алгоритми консенсусу, також засновані на матеріальному або нематеріальному фінансовому забезпеченні, що при проектуванні блокчейн-мереж повинно обмежувати участь окремого представника і залучати якомога більше незалежних учасників. Однак постійне експоненціальне збільшенням фінансових вливань призводить до експоненціально-

го збільшення складності (вартості) участі в підтримці консенсусу, що призводить до витіснення з системи «слабких» учасників або стимулює їх до об'єднання в великі пули (з втратою можливості самостійного контролю блокчейн-мережі).

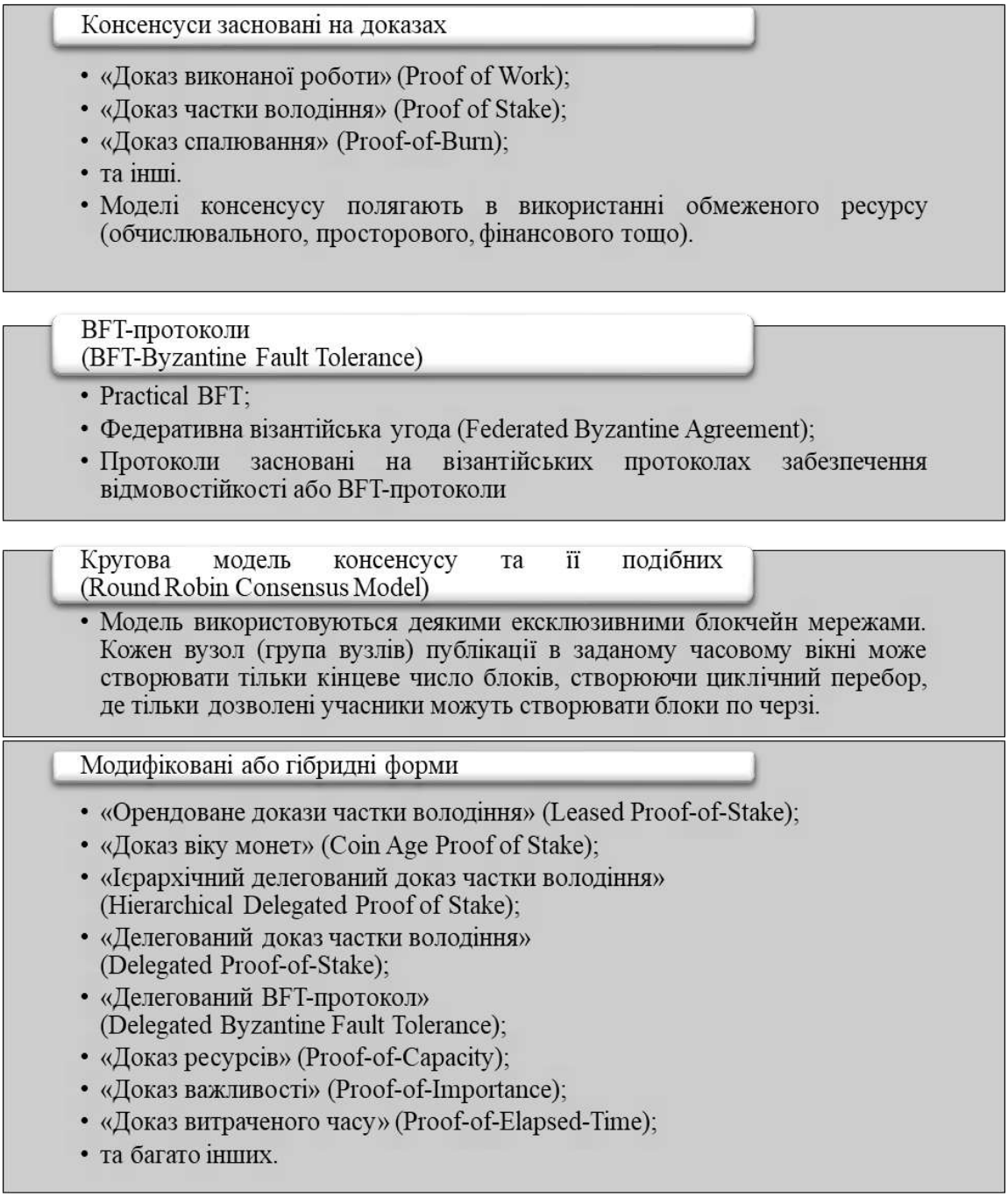


Рис. 5. Найпоширеніші моделі консенсусу

Таким чином, замість децентралізованої блокчейн-мережі з досить великою кількістю незалежних учасників (змова між якими практично виключена) в мережі починають домінувати кілька великих пулів або монополій, кількість яких складають одиниці. У даних умовах об'єднання великих гравців стає простим завданням, а з огляду на їх загальний інтерес в фінансову вигоду – практично неминучі.

Якщо ж об'єднання учасників блокчейн-системи не відбувається, але при цьому складність (вартість) участі в ній стає дедалі більше – система починає втрачати учасників, яким стає не вигідно підтримувати її функціонування. В результаті в системі залишається обмеже-

не вузьке коло, що має інші причини крім фінансових в підтримці роботи алгоритмів консенсусу, або блокчейн-система «гине».

В обох випадках, блокчейн-системи, побудовані за принципом фінансової зацікавленості учасників в підтримки роботи її механізмів консенсусу, схильні до високого ризику централізації її управління, що неминуче призводить до втрати довіри до блокчейн-системи як до незалежного та децентралізованого механізму.

На відміну від інклюзивних мереж ексклюзивні блокчейн-мережі дозволяють адміністративним шляхом впливати на саму можливість брати участь в підтриманні функціонування системи або впливати на фінансову вигоду кожного з учасника і тим самим забезпечувати необхідну кількість учасників гарантуючи малу ймовірність їх взаємної змови. Але при цьому необхідні достатні фінансові витрати адміністратора мережі – на фінансову зацікавленість участі сторонніх учасників у підтримці консенсусу мережі або на забезпечення призначених учасників всім необхідним для виконання своїх функцій.

У таких ексклюзивних блокчейн-мережах адміністратор має всі можливості прямо або побічно впливати на прийняття рішення цієї «децентралізованої» системи. У зв'язку з чим не рекомендується участь в блокчейн-системах сторонніх організацій для ведення та документування своїх будь-яких операцій, без повної довіри до цієї третьої сторони.

З іншого боку, такі ексклюзивні блокчейн-системи ідеально підходять для ведення та контролю операцій всередині певного кола суб'єктів взаємодії, де є недовіра між собою або необхідна можливість повного аудиту проведених операцій. У таких випадках в реєстрі блокчейн-системи заносяться всі операції і дані, необхідні для його аудиту, та по принципам побудови блокчейн-ланцюга заносяться до реєстру за участю всіх зацікавлених суб'єктів взаємодії включаючи сторони, які беруть участь в аудиті.

Резюмуючи наведене, враховуючи необхідність організації публічної колективної демократії, з дотриманням всіх вимог безпеки її проведення, необхідно застосовувати ексклюзивні блокчейн-системи з використанням BFT-протоколів консенсусу. Причому до вузлів публікації повинна бути залучена необхідна, але обмежена, кількість незалежних учасників (спостерігачів, незалежних громадських об'єднань). Їх кількість обмежується принципами неможливості вплинути на процеси формування реєстру блокчейн-мережі, але при цьому залишає факт фіксації їх участі в перевірці та підтвердженні кожного сформованого блоку, що надалі виключить будь-яку можливість маніпулювання з блокчейн-реєстром власником системи.

Доступ до реєстру повинен бути організований з дотриманням публічності та прозорості, що надасть можливість реалізувати основну перевагу блокчейн-технології – кожен користувач зможе особисто провести підрахунок голосів та переконатися у легітимності результатів голосування.

Обґрунтування механізмів та протоколів криптографічного захисту інформації

Криптографія як наука з'явилася, перш за все, для забезпечення конфіденційності інформації. З розвитком технологій стало зрозуміло, що криптографічні методи можуть бути застосовані для надання інших послуг, таких як забезпечення цілісності пакетів, неспростовності отримання інформації, автентифікації користувачів, тощо. Більш того, сучасний світ важко уявити без електронних цифрових підписів, направленого шифрування та кодів автентифікації повідомлень, на базі яких будуються численні криптографічні протоколи, що становлять основу для інформаційно-комунікаційних систем. Задача побудови надійної системи електронного голосування є гарним прикладом проблеми, що стимулює розвиток нових криптопримітивів для синтезу відповідних протоколів. Розглянемо основні вимоги до протоколів електронного голосування:

- Анонімність. Ніхто не має зв'язувати волевиявлення виборця з його особистістю.
- Валідація виборчих бюлетенів. Система повинна відрізняти валідні бюлетені від зіпсованих. Наприклад, коли виборець віддав свій голос за декількох кандидатів.

- Ідентифікація виборців. Система повинна запобігати спробам проголосувати декілька разів або спробам проголосувати за іншого виборця.
- Відкритість. Незалежні аудитори повинні мати змогу перевірити коректність даних.

На перший погляд вимоги суперечать одне одному, але це не так. Для реалізації послуги забезпечення анонімності зручно використати механізми гомоморфного шифрування. Гомоморфне шифрування є криптографічним примітивом, який дозволяє виконувати обчислення над шифротекстами таким чином, щоб після розшифрування результат співпадав з аналогічними обчисленнями над відкритими текстами. Припустимо, що є два відкритих тексти в форматі цілих чисел – m_1 і m_2. Тоді схема вважатиметься гомоморфною по відношенню до операції додавання, якщо сума шифротекстів $Enc(m_1)$ і $Enc(m_2)$ буде дорівнювати сумі відкритих текстів після розшифрування, тобто виконуватиметься рівність

$$Dec(Enc(m_1)+Enc(m_2))=m_1+m_2\ . \tag{1}$$

Тобто, виборець може зашифрувати свій голос та відправити до виборчої дільниці, на якій з застосуванням операції гомоморфного складання відбудеться підрахунок голосів. При цьому, зміст голосу не буде відомий дільниці, оскільки він зашифрований. Як буде показано далі, для забезпечення інших послуг, на схему гомоморфного шифрування накладаються більш складні вимоги, ніж підтримка операції гомоморфного складання. У загальному випадку потрібна можливість обчислювати досить велику кількість різноманітних математичних операцій над шифротекстами.

Криптосистеми, які можуть обчислювати над шифротекстами будь-які операції, називаються повністю гомоморфними. Тривалий час не вдавалося побудувати такі системи, проте у 2009 році американським криптологом G. Gentry була розроблена перша така система. З тих пір напрямок гомоморфного шифрування отримав поштовх для розвитку. Цікавим є те, що математичні перетворення, які застосовуються у найкращих сучасних повністю гомоморфних системах, належать до класу криптографії на гратках (lattice-based cryptography), яка при певному виборі загальносистемних параметрів є стійкою до атак на квантових комп'ютерах. Нещодавно прийнятий стандарт направленого шифрування та інкапсуляції ключів ДСТУ 8961:2019 також базується на стійкості проблем в теорії граток та може бути адаптований для випадку повністю гомоморфного шифрування.

Для валідації бюлетенів можливо застосувати докази з нульовим розголошенням. Доказ з нульовим розголошенням є протоколом, у якому одна сторона доводить іншій певне твердження, при цьому не розголошуючи інформації про це твердження. Наприклад, виборець хоче довести дільниці, що його гомоморфно зашифрований голос є валідним, при цьому не надаючи жодної інформації про вміст шифротекста. Для простоти викладення представимо, що голос є набором з N чисел, що належать множині $\{0,1\}$, де всі числа є нулями, а i-те число є одиницею та відповідно позначає номер кандидата, за якого проголосував виборець. Тобто валідними голосами будуть всі набори вигляду

$$\begin{aligned}&(1,0,0,...,0,0)\\&(0,1,0,...,0,0)\\&(0,0,1,....,0,0)\\&...\\&(0,0,0,...,1,0)\\&(0,0,0,...,0,1)\end{aligned} \tag{2}$$

Шляхом нескладних математичних обчислень можливо довести, що голос, представлений набором цілих чисел $a=(a_1,a_2,...,a_N)$, належить до множини голосів (2), якщо виконується рівність

$$f(a) = \sum_{i=1}^{N} (a_i^2 - a_i)^2 + (\sum_{i=1}^{N} a_i)^2 = 1 \quad (3)$$

Якщо гомоморфно провести всі обчислення, то задача доказу валідності голоса зводиться до доказу того, що у отриманому шифротексті після обчислення $f(a)$ буде одиниця. Для вирішення цієї задачі існують різні протоколи. Для сучасних схем гомоморфного шифрування є перспективним підходи на основі схеми Фіата – Шаміра з перериваннями (Fiat – Shamir With Aborts), але детальний їх розгляд виходить за межі цієї статті.

Однією з послуг, що надається електронним цифровим підписом є ідентифікація користувача, або групи користувачів, яка володіє секретним ключем, на якому було вироблено підпис. Цей принцип можливо використати для забезпечення вимоги ідентифікації виборців. Якщо кожен виборець має свій секретний ключ, то до голосу і доказу валідності можливо додати підпис, який однозначно ідентифікує користувача.

В Україні розгорнута інфраструктура відкритих ключів, активно розвиваються такі технології, як MobileID та SmartID. Для організації виборів доцільно використовувати ресурси цих, вже існуючих систем. Узагальнена модель голосу виборця наведена на рис. 6.

Рис. 6. Узагальнена модель бюлетеня для системи електронного голосування

Оскільки всі голоси є гомоморфно зашифрованими, то незалежні аудитори можуть провести всі обчислення незалежно від ЦВК і після завершення виборів перевірити результати, чим забезпечується відкритість голосування. В залежності від інших вимог у модель бюлетеня можуть вноситися зміни, наприклад, для збору статистики по окремим регіонам.

Окрім цього, в зв'язку зі збільшенням кількості кібератак в світі виникає потреба в побудові надійної інфраструктури, яка буде зберігати та оброблювати данні виборців. Технологія блокчейн дозволяє будувати надійні розподілені інформаційні системи, функціонування яких можливе навіть якщо 49 % інфраструктури пошкоджено зловмисниками. Такі властивості забезпечуються за допомогою великої кількості криптографічних примітивів, які узгодженим чином формують надійні протоколи.

Сам блокчейн є спеціально сформованою базою даних, яка зберігає транзакції. До кожної транзакції, спрощено кажучи, додається електронний цифровий підпис. Наприклад, у випадку електронного голосування це може бути підпис на закритому ключі виборчої дільниці, до якої надійшов голос. Це унеможливлює "вкидування голосів" від третіх сторін. Транзакції групуються у блоки. Кожен блок містить геш-значення від усіх транзакції у ньому, сформований за допомогою дерева Меркла. Це забезпечує цілісність блока. На рис. 7 схематично наведена структура блоків.

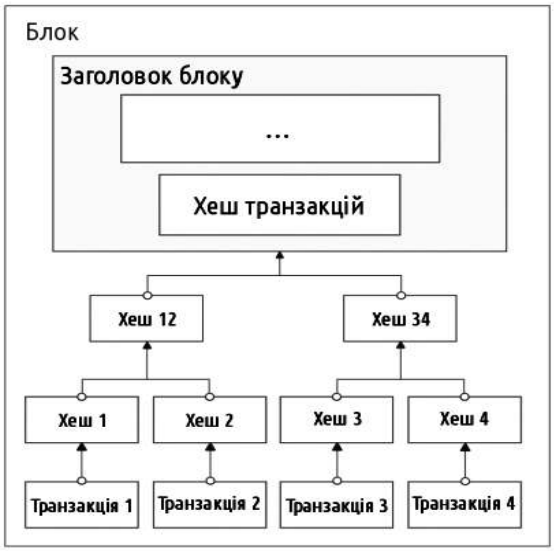


Рис. 7. Узагальнена структура блока в блокчейні

Окрім цього, до блока додається геш-значення від попереднього блока, тим самим створюється ланцюг блоків. Зрозуміло, що змінити данні, що зберігаються в якомусь блоці, дуже важко, оскільки доведеться коригувати усі блоки.

Блокчейн є децентралізованою структурою. Кожен з вузлів містить повні або часткові копії даних, що зберігаються на інших вузлах. Для забезпечення безпечної комунікації між окремими вузлами використовуються складні протоколи, розгляд яких виходить за межі цієї статті. Зазначимо лише, що для реалізації цих протоколів, окрім згаданих вище, в більшості випадків вимагається наявність блочних та/або поточних шифрів. Тож, виникає задача вибору криптопримітивів для функціонування блокчейн-системи.

В Україні запроваджено ряд стандартів у галузі криптографічної діяльності. Розглянимо деякі з них.

ДСТУ 4145-2002 є стандартом електронного цифрового підпису. Він ґрунтується на перетвореннях у групі точок еліптичних кривих над полями Галуа $GF(2^m)$. Схема підпису схожа на ECDSA (міжнародний стандарт підпису), проте не потребує операції взяття зворотного елемента в полі, що дозволяє швидше виробляти та перевіряти підпис. Стандарт дозволяє проводити обчислення як в поліноміальному базисі, так і у оптимальному нормальному базисі. ДСТУ 4145-2002 є основним видом підпису для державної інфраструктури відкритих ключів та навіть застосовується в системах, у яких циркулює інформація з обмеженим доступом, що становить державну таємницю. Надійність та ефективність ДСТУ 4145-2002 підтверджена численними дослідженнями як українських, так і зарубіжних криптологів.

ДСТУ 7624-2014 є стандартом симетричного блочного шифрування. Визначає rijndael-подібний блочний шифр “Калина”. Калина забезпечує нормальний, високий і надвисокий рівні стійкості, із довжинами блока і ключа 128, 256 і 512 бітів. Стійкість rijndael-подібних шифрів підтверджена часом. До того ж, у Калині значно покращені показники безпеки. Лінійний та диференційний криптоаналіз є неефективним вже при п’яти ітераціях. В рамках консервативного і прозорого підходу до проектування блокового шифру, шар нелінійного перетворення циклової функції реалізований на базі S-блоків. Розмір S-блоку був обраний виходячи з можливості ефективної реалізації на процесорах загального призначення. Шифр, на відміну від міжнародного стандарту AES, орієнтований на 64-бітні системи, що дозволяє отримати кращі результати на сучасних платформах. Обчислення гарно розпаралелюються за допомогою AVX2, NEON та інших наборів SIMD інструкцій. Стандарт підтримує 10 режимів роботи, які дозволяють гнучко використовувати шифр для різних призначень, серед яких є унікальні режими, характерні тільки для Калини.

ДСТУ 7564-2014 є стандартом гешування. Визначає ітеративну криптографічну геш-функцію “Купина”. Купина за структурою є SPN-мережею. Результатом роботи геш-функції є бітова послідовність від 8 до 512 біт. Така гнучкість є особливістю стандарту. Основними режимами роботи, рекомендованими до застосування, є «Купина-256», «Купина-384» і «Купина-512». Геш-функція, як і блочний шифр Калина, мають високі показники стійкості до лінійного та диференційного криптоаналізу, оскільки при розробці особлива увага приділяється криптостійкості.

ДСТУ 8845-2019 є новим стандартом потокового шифрування. Шифр має високу пропускну здатність до 17 Гб/с. Дизайн шифру схожий на міжнародний потоковий шифр SNOW-2, але значно покращений. Криптосистема орієнтована на 64-бітні системи. Також збільшені довжини ключа та вектору ініціалізації, що дозволяє захиститися від атак на квантовому комп’ютері, таких як алгоритм Гровера. Окрім того, шифр забезпечує зв’язок між окремими елементами шифропослідовностей, що значно підвищує стійкість до нав’язування помилкових символів та режимів роботи.

Тож, Україна має всі необхідні криптографічні стандарти для побудови надійних блокчейн-систем для електронного голосування.

Обґрунтування механізмів та протоколів безпеки комп’ютерних мереж, вузлів та інфраструктури

Обґрунтування безпеки комп’ютерних мереж, вузлів та інфраструктури системи електронного голосування на основі Blockchain базується на основі оцінки захищеності (вразливостей) стосовно існуючих та потенційних атак, спрямованих на порушення безпеки

Вимоги захищеності зазвичай обґрунтовуються через забезпечення цілісності та неспростовності (авторства) інформації стосовно існуючих та потенційних атак, спрямованих на порушення безпеки. Неповний перелік вимог до механізмів та протоколів безпеки комп’ютерних мереж, вузлів та інфраструктури представлено в табл. 2. При цьому розглядалася модель блокчейн-системи, яка функціонує із застосуванням технології Exonum, що вже є впровадженою в Україні. В таблиці наведено загальний опис вразливостей, мета та спосіб моделювання існуючих та потенційних атак (або перевірки на відповідність реалізації).

Таблиця 2

Перелік вимог, вразливостей та способів їх моделювання

Вимоги	Реалізація вимоги	Перевірка вимогам
BFT-протокол забезпечує надійну роботу навіть в ненадійних мережах за умови, що більше 2/3 вузлів облікової системи є чесними. При зменшенні цієї частки блокчейн-система втрачає працездатність.	Встановлення найменшої кількості (або частки) діючих вузлів валідаторів, за якої система буде забезпечувати надійну роботу. Встановити, як система реагує на «злочинні» дії вузлів-валідаторів, тобто такі дії, за яких вузол повідомляє хибну інформацію.	Шляхом навмисного зменшення кількості діючих вузлів-валідаторів моделюється умова, за якою частка працездатних (чесних) вузлів облікової системи менша за 2/3.
BFT протокол консенсусу є ефективним у системах з низькою затримкою, але дуже чутливий до кількості вузлів і пропускної здатності, так як одне повідомлення генерує безліч інших запитів і перевірок. Якщо використовувати велику кількість вузлів, то відбувається стрімке зростання кількості повідомлень і дуже велике зростання навантаження на мережу. В останньому	Встановлення залежності між пропускною здатністю системи та кількістю вузлів-валідаторів. Встановити поріг сталого функціонування системи Exonum при збільшені вузлів валідаторів.	Шляхом масштабування (зміни кількості) вузлів-валідаторів моделюється робота блокчейн-мережі у різних режимах.
	Встановлення залежності між ненадійністю у роботі каналів зв’язку та працездатністю блокчейн-системи. Необхідно встановити поріг сталого функціонування системи Exonum	Шляхом зміни затримок у каналі зв’язку (через короткотермінову зупинку окремих вузлів) моделюється зменшення загальної пропускної здатності системи.

Вимоги	Реалізація вимоги	Перевірка вимогам
випадку протокол працює неефективно.	при збільшені часу обміну між вузлами валідаторів (загублення пакетів даних, низька пропускна спроможність каналу зв'язку, збільшення часу обміну даними між вузлами).	
В базовому варіанті Practical BFT протоколу передбачається наявність лідера, що може стати точкою DoS-атаки для зупинки роботи облікової системи зловмисником. Оскільки є «лідер», що відправляє всім транзакції для підтвердження. Вимога стійкість системи до DoS-атак.	Встановлення максимальної кількості, повідомлень при яких вузол-валідатор зберігає своє стале функціонування.	Максимальна кількість повідомлень, при яких вузол-валідатор зберігає своє стале функціонування, виходить за межі обчислювальних ресурсів, якими володіє комплекс. Отже моделювання цієї вразливості в комплексі не реалізоване.
Стійкість розподілених систем Exonum до віддалених атак, оскільки їх компоненти використовують відкриті канали передачі даних.	Виконання основних вимог через перевірку неможливості проведення ефективних віддалених атак	Встановлення умов, які потрібні для здійснення атак. Перевірка через аудит початкових кодів (реалізовані протоколи передачі даних забезпечують захист від віддалених атак).
Відсутність помилок в реалізації протоколу BFT блокчейн-мережа які допускають порушення безпеки.	Відповідність реалізації протоколу BFT наданої документації.	Перевірка через виконання тестів внутрішніх програмних компонентів (ВПК) Exonum та аудиту початкових кодів (реалізований протокол BFT повинен відповідати наданій документації).
Зберігання особистих ключів від компрометації та / або модифікації конфігураційних файлів вузлів-валідаторів.	Встановлення наявних механізмів захисту особистих ключів та конфігураційних файлів вузлів-валідаторів від несанкціонованого доступу.	Перевірка через виконання тестів ВПК Exonum та аудиту початкових кодів (реалізовані механізми захисту особистих ключів та конфігураційних файлів вузлів-валідаторів повинні виключати можливість несанкціонованого доступу).

Проведення випробувань щодо рівня захисту від актуальних атак на Blockchain-платформи включає встановлення:

1. надійності роботи у ненадійних мережах;
2. надійності системи при масштабуванні кількості вузлів-валідаторів;
3. надійності системи при ненадійній роботі каналів зв'язку;
4. можливості захисту системи від віддалених атак;
5. відповідності реалізації протоколу BFT;
6. можливості віддаленого несанкціонованого доступу (компрометація особистих ключів) та / або модифікації конфігураційних файлів вузлів-валідаторів.

Розглянемо ці випробування більш докладно.

Встановлення надійності роботи у ненадійних мережах. Дослідження безпеки здійснюється шляхом моделювання блокчейн-мережі із порушеннями в роботі окремих вузлів. Зокрема моделюються випадки, коли доля ненадійних вузлів перевищує частку, достатню для правильної роботи системи.

Встановлення надійності системи при масштабуванні кількості вузлів-валідаторів. В мережі з великим числом вузлів в каналі зв'язку превалюють повідомлення із неприйняттям консенсусом або повторною спробою. Завдяки зростаючим затримкам та переповненості каналу зв'язку більшість вузлів очікують або виводять повідомлення про те, що власна висота блока нижче ніж висота блока більшості вузлів. Робота мережі характеризується нерівномірною швидкістю прийняття блоків. Середня швидкість знижується на 30 – 40 % відсотків. При відключенні вузлів кількістю від 1/3 від загальної значно збільшується кількість повідомлень про відмову з'єднання. Це погіршує швидкодію, загострюються відрив між вузлами по висоті блока, збільшуються перерви на очікування вузлів, що відстали.

Встановлення надійності системи при ненадійній роботі каналів зв'язку. Моделюється система із оцінкою швидкості прийняття блоків у залежності від загальної кількості валідаторів, збільшуючи процент зупинених вузлів. Встановлюються кількісні показники співвідношення між працюючими та зупиненими вузлами.

Встановлення відповідності реалізації протоколу BFT. BFT-протокол забезпечує надійну роботу навіть в ненадійних мережах за умови, що більше 2/3 вузлів системи є чесними, тобто діють за протоколом. Для прийняття консенсусу на одному раунді відбувається попереднє голосування, поріг для прийняття консенсусу – це отримання щонайменше +2/3 попередніх голосів щодо визначеного раунду та геша, щодо яких встановлюється консенсус.

Встановлення можливості віддаленого несанкціонованого доступу (компрометація особистих ключів) та / або модифікації конфігураційних файлів вузлів-валідаторів. У ситуації, коли вузол симулює неправильні адресу або порт при підписанні транзакцій на неправильному ключі, виникає помилка, консенсус не досягнуто, система не приймає підписані транзакції на неправильному ключі. При моделюванні спроб неправильної конфігурації ключів не вдалося запустити мережу, тобто обійти встановлений протоколом захист. При зміні адреси іншого вузла не вийде досягнути з'єднання. Це запобігає довільному приєднанню чужих вузлів. Також команда запуску ноди потребує знання паролю pass, який ніде не зберігається у відкритому вигляді. Таким чином, команда має захист від несанкціонованого запуску вузла, навіть якщо приватним ключем володіє неуповноважений користувач.

Висновки та рекомендації

У ході пошукових досліджень розроблено апаратно-програмний комплекс для перевірки функціонування реально діючих блокчейн-систем та на його базі розгорнуто прототип системи електронного голосування. Головною перевагою розробленого прототипу є імплементація вітчизняних криптографічних стандартів які є стійкими і в умовах постквантового періоду. Проведено дослідження безпеки блокчейн-систем стосовно децентралізованих атак та атак, направлених на вибрані алгоритми консенсусу. Сформовано основні засади щодо розробки моделей загроз та моделей порушника відносно децентралізованих облікових систем, які дозволять проводити обґрунтовані оцінки стану безпеки децентралізованих систем та технологій.

Практичне впровадження технології блокчейн підвищує довіру до інформаційних ресурсів та сервісів (що є особливо актуальним для державних установ), зменшує час та накладні витрати, унеможливлює втручання центральних органів та відповідні корупційні дії, підвищує надійність збереження інформації та якість наданих послуг. З метою реалізації вироблених концепцій, сприяння розвитку та продуктивного використання інформаційних технологій в державі доцільною є розробка «Дорожньої карти з впровадження технології блокчейн в Україні», яка повинна включати:

- перелік додатків, щодо яких є доцільним застосування технології блокчейн в Україні;
- визначення рекомендованих компонентів технології блокчейн для різних практичних застосувань в Україні;
- перелік «базових» блокчейн-систем із рекомендованими компонентами для різних практичних застосувань в Україні;

– низка програм та методик проведення експертних досліджень «базових» блокчейн-систем для практичних застосувань в Україні;
– результати експертних досліджень «базових» блокчейн-систем із наданням рекомендацій щодо практичних застосувань в Україні;
– положення концепції та програми впровадження технології блокчейн в Україні.

Доцільним є також розгортання найближчим часом елементів децентралізованої інфраструктури електронного голосування із застосуванням технології блокчейн. Це надасть змогу у якості експерименту вже восени цього року провести перші в Україні місцеві вибори із застосуванням новітніх блокчейн-технологій, які унеможливлюють адміністративне втручання, підробку або викривлення результатів волевиявлення населення, забезпечують автоматичний підрахунок голосів та захищене документування результатів. До експерименту слід залучити окремі райони із переважно молодим та прогресивно думаючим населенням (студентські містечка, гуртожитки, університетські кампуси, тощо). Вибори необхідно провести із залученням нових комп'ютерних технологій, блокчейн-систем, смарт-контрактів, тощо, і це повністю відповідає загальній стратегії Президента України із розгортання новітніх технологій та систем державного управляння, зокрема є елементом державної стратегії з надання *е*-послуг «Держава у смартфоні».

Заплановані заходи спрямовані на підвищення ефективності державного управляння загалом та, зокрема, надання державних інформаційних послуг, усунення адміністративних бар'єрів та виключення умов виникнення корупції, підвищення довіри громадян України до національної влади, органів самоврядування, держави загалом.

Список літератури:

1. NISTIR 8202 Blockchain Technology Overview https://doi.org/10.6028/NIST.IR.8202
2. Consensus – Immutable agreement for the Internet of value https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/kpmg-blockchain-consensus-mechanism.pdf
3. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System, 2009. 9 p.
4. СЕТАМ. https://setam.net.ua/
5. Vlad Gheorghiu, Michele Mosca. Benchmarking the quantum cryptanalysis of symmetric, public-key and hash-based cryptographic schemes,URL: https://arxiv.org/pdf/1902.02332.pdf
6. Perlner R. A., Cooper D.A. "Quantum Resistant Public Key Cryptography: A Survey", IDtrust '09, April 14- 16, 2009, Gaithersburg, MD. P. 85-93. URL: https://ws680.nist.gov/publication/get_pdf.cfm?pub_id= 901595
7. Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner and Daniel Smith-Tone. "NISTIR 8105. Report on Post-Quantum Cryptography" / National Institute of Standards and Technology. Internal Report 8105, April 2016. 10 p.
8. Закон України "Про вибори президента України".
9. Закон України "Про електронні довірчі послуги".
10. Регламент (ЄС) № 910/2014 Європейського Парламенту та Ради від 23 липня 2014 року «Про електронну ідентифікацію та довірчі послуги для електронних транзакцій у межах внутрішнього ринку та про скасування Директиви 1999/93/ЄС» (1) (COM (2012) 0238-C7-0133/2012 – 2012/0146 (COD)).
11. Горбенко І.Д., Кузнецов О.О., Потій О.В., Горбенко Ю.І., Полуяненко М.О. Технологія блокчейн: огляд, сучасні проблеми та перспективи впровадження в Україні // ІІ міжнар. наук.-практ. конф. "Проблеми кібербезпеки інформаційно-телекомунікаційних систем" (PCSITS), 11-12 квітня 2019 р., м. Київ, 2019. С. 217-220.
12. Isirova K. and Potii O. Decentralized public key infrastructure development principles // 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). Kiev, 2018. P. 305-310.
13. Exonum documentation //URL: https://exonum.com/doc/version/0.12/
14. Bitfury Exonum //URL: https://exonum.com/ru/index

Харківський національний
університет імені В. Н. Каразіна;
АТ «Інститут інформаційних технологій»

Надійшла до редколегії 06.02.2020

УДК 004.056.5 **DOI:10.30837/rt.2020.1.200.12**

М.О. ПОЛУЯНЕНКО, канд. техн. наук, О.О. КУЗНЕЦОВ, д-р техн. наук

АНАЛІТИЧНЕ МОДЕЛЮВАННЯ АТАКИ ПОДВІЙНОЇ ВИТРАТИ НА БЛОКЧЕЙН-СИСТЕМИ ІЗ ЙМОВІРНІСНИМ ПРОТОКОЛОМ КОНСЕНСУСУ

1. Вступ

Чи не найголовнішим аспектом побудови безпечних та надійних розподілених децентралізованих систем за блокчейн-технологією є питання створення пов'язаних між собою безперервних ланцюжків блоків інформації, несанкціонована зміна яких унеможливлюється застосованими криптографічними механізмами. Це досягається використанням односпрямованих, стійких до колізій та пошуку прообразів криптографічних функцій, обчислені геш-значення яких від попередніх блоків включаються у наступні блоки. В результаті, несанкціоновану зміну бодай одного біту даних в попередніх блоках буде відразу виявлено, створення хибних записів, навмисне або випадкове викривлення інформаційних даних унеможливлюється. Але у разі розподіленого зберігання інформації виникає додаткова вимога синхронізації окремих ланцюгів блоків, які зберігаються різними вузлами. Ці та інші питання вирішуються шляхом застосування механізмів встановлення консенсусу, за допомогою яких після виконання певної послідовності дій безперервна послідовність блоків (блокчейн-ланцюг) стає однаковою на всіх вузлах децентралізованої мережі.

Головними завданнями при проектуванні блокчейн-систем є проведення досліджень технології, оцінка вразливостей до проведення атак, спрямованих на порушення безпеки (порушення цілісності, неспростовності, доступності та конфіденційності) інформації, що обробляється та зберігається за блокчейн-технологією. З урахуванням складності та важливості зазначених завдань актуальними є питання аналізу існуючих протоколів встановлення консенсусу в децентралізованих мережах, дослідження особливостей побудови та, безпосередньо, оцінка безпеки блокчейн-систем при застосуванні певних алгоритмів консенсусу. Важливою та актуальною є, на нашу думку, перевірка базових положень та припущень, які використовуються при моделюванні роботи блокчейн-мереж, та які безпосередньо впливають на кінцеві співвідношення стосовно оцінки ймовірності успішної реалізації певних атак на застосовані протоколи встановлення консенсусу.

В роботі досліджується одна з основних вразливості блокчейн-систем, побудованих за допомогою консенсусу з ймовірнісною завершеністю, а саме – атака подвійної витрати [1].

2. Ймовірності формування ланцюжка блоків з однаковими початковими умовами

Припустимо, що будь-який суб'єкт має у своєму розпорядженні потужності, які дають йому можливість сформувати блок за одну спробу (або за певний інтервал часу Δt) з ймовірністю p.

Зауважимо, що в умовах блокчейн-систем ймовірність p для кожного окремого суб'єкта не залежить від номера випробувань і від інших суб'єктів і визначається виключно потужністю, яку він має (справедливо для алгоритмів консенсусу Доказу виконаної роботи та його аналогів). Ймовірність p можна прив'язати до гешрейту (кількості протестованих геш-функцій в секунду), але в загальному випадку покладемо значення p – ймовірність сформувати блок за деяку умовну одиницю часу.

Ймовірність появи події A (в даному випадку – формування блоку) при кожному з нескінченної (або кінцевої, але досить великої) послідовності випробувань дорівнює p. Випадкова величина, при якій відбулася вперше подія A, є дискретною випадковою величиною. В такому випадку завдання знаходження ймовірності події A при t-му випробуванні зводиться до знаходження закону розподілу випадкової величини t.

Механізм атаки подвійної витрати докладно викладено у роботах Сатоші Накамото [2] та Мені Розенфельда [3] та багатьох інших авторів. При викладі матеріалу будемо вважати, що читач вже знайомий з цими роботами. Нагадаємо, що зловмисник може перемогти чесну мережу в момент початку гонки, тобто, коли чесною мережею сформовано N підтверджень транзакцій, стосовно якої зловмисник бажає здійснити зміни. При цьому йому необхідно сформувати N або більше блоків до того моменту коли чесна мережа сформує N блоків. Якщо йому це не вдасться, то у нього все ще є можливість наздогнати чесну мережу на $N+j$ блоці, де j – кількість блоків, сформованих чесною мережею на додаток до необхідних N блоків.

В роботах Сатоші Накамото [2] та Мені Розенфельда [3] отримано вираз з урахуванням ряду припущень, серед яких:

- ймовірність перемоги зловмисника еквівалентна задачі про «розорення гравця», тобто група подій в гонці між чесною мережею і зловмисником складається тільки з двох подій, ймовірності яких однозначно пов'язані між собою співвідношенням $p+q=1$. Ми будемо отримувати вираз ймовірності перемоги, вважаючи, що ймовірності сформувати блок чесною мережею та зловмисником є незалежними подіями, які визначаються безпосередньо потужностями, якими володіють учасники, та зазначені ймовірності ніяк не залежать один від одного, тобто будемо використовувати модель «незалежних гравців» (більш детально дивиться у [4]). Випадок, коли $p+q=1$ у моделі «незалежних гравців», є лише окремим випадком, а не обов'язковою вимогою як в моделі «розорення гравця»;

- зловмисник має можливість (бажання) нескінченно довго проводити атаку на мережу, формуючи альтернативний ланцюг, тобто зловмисник має необмежені для цього ресурси. Ми будемо виходити з більш реалістичної картини, коли зловмисник обмежується (на підставі можливості або раціональності, більш детально це розглянуто у роботах [5] та [6]) деякою максимальною кількістю спроб $t_{\max}$, що складається з N, j та кількості невдалих спроб сформувати блок чесною мережею (k), тобто $t_{\max}=N+j+k$. Якщо протягом цього часу зловмиснику не вдалося перемогти чесну мережу – йому зараховується поразка і гонка завершується. На практиці, якщо загальний гешрейт зловмисника у два рази менше чесної мережі, зловмиснику буде економічно не вигідно підтримувати процес гонки довше ніж декілька десятків блоків, тобто $n_{\max}<20$ є цілком природне (більш детально у [5]);

- вираз ймовірності успішного формування альтернативного ланцюжка зловмисником отримано для випадку, коли зловмисник лише наздожене, а не випередить, чесну мережу або, як наведено в роботах Сатоші Накамото [2] та Мені Розенфельда [3], за припущенням, що один блок був попередньо здобутий атакуючим до початку атаки, тобто не враховувалися ймовірність його формування. В даній роботі ми не будемо робити цього припущення, а отримуємо вираз безпосередньо для умови, що зловмиснику треба випередити чесну мережу, тобто сформувати хоча б на один блок більш за чесну мережу. Отримуємо ймовірність перемоги зловмисника з рівними початковими умовами, тобто коли система стартує з нульовою (з деякого початкового моменту часу) кількістю сформованих блоків як у чесній мережі так і у зловмисника.

2.1. Ймовірність перемоги зловмисника при $N=1, j=0$

Для отримання формули ймовірності успішного проведення атаки подвійної витрати зловмисником розглянемо такі можливі ймовірності і комбінації, в яких зловмисник здобуває перемогу:

1. При першій спробі ($t = N + j + k = 1 + 0 + 0 = 1$) перемога неможлива. Зловмисник може сформувати не більш одного блоку за одну спробу, а для перемоги йому необхідно дочекатися формування чесною мережею блоку і поширити ланцюжок блоків на один більше. Таким чином, зловмиснику необхідно сформувати як мінімум два блоки.

Ймовірність перемоги зловмисника буде визначатися як: $PI_{N=1,\,j=0,k=0} = 0$;

2. При другій спробі ($t = N + 0 + 1 = 2$) зловмисник може перемогти, якщо йому вдасться сформувати за обидві спроби по блоку, а чесна мережа сформує тільки один блок (неважливо за першу або другу спробу).

Загальна ймовірність даної події:

$$PI_{N=1,\,j=0,k=1} = p\cdot(1-p)\cdot[q\cdot q] + (1-p)\cdot p\cdot[q\cdot q] = 2\cdot p\cdot(1-p)\cdot q^2$$

3. При третій спробі ($t = N + 0 + 2 = 3$): якщо чесна мережа сформує блок при першій або другій спробі, то другий блок повинен бути сформований зловмисником тільки на третій спробі, в іншому випадку (якщо другий блок буде сформований на другій спробі) буде попередній випадок (як для $PI_{N=1,\,j=0,k=1}$). Якщо чесна мережа формує другий блок на третій спробі, то на зловмисника не накладаються жодних обмежень з можливості формування блоків.

Сумарна ймовірність настання подій буде обчислюватися аналогічно описаним подіям, підсумкова ймовірність якої буде:

$$\begin{aligned}
PI_{N=1,\,j=0,k=2} = {} & p\cdot(1-p)\cdot(1-p)\cdot\left[q\cdot(1-q)\cdot q + (1-q)\cdot q\cdot q\right] + \\
& + (1-p)\cdot p\cdot(1-p)\cdot\left[q\cdot(1-q)\cdot q + (1-q)\cdot q\cdot q\right] + \\
& + (1-p)\cdot(1-p)\cdot p\cdot\left[q\cdot q\cdot(1-q) + q\cdot(1-q)\cdot q + (1-q)\cdot q\cdot q + \right. \\
& \left. + q\cdot q\cdot q\right] = \\
& = 2\cdot p^1\cdot(1-p)^2\left[2\cdot q^2\cdot(1-q)^1\right] + \\
& + p^1\cdot(1-p)^2\left[3\cdot q^2\cdot(1-q)^1 + q^3\right]
\end{aligned}$$

4. При четвертій спробі ($t = N + 0 + 3 = 4$) – аналогічно ситуації, описаної в попередньому пункті. Сумарна ймовірність перемоги зловмисника буде визначатися:

$$\begin{aligned}
PI_{N=1,\,j=0,k=3} = {} & p\cdot(1-p)\cdot(1-p)\cdot(1-p)\cdot\left[q\cdot(1-q)\cdot(1-q)\cdot q + (1-q)\cdot q\cdot(1-q)\cdot q + (1-q)\cdot(1-q)\cdot q\cdot q\right] + \\
& + (1-p)\cdot p\cdot(1-p)\cdot(1-p)\cdot\left[q\cdot(1-q)\cdot(1-q)\cdot q + (1-q)\cdot q\cdot(1-q)\cdot q + (1-q)\cdot(1-q)\cdot q\cdot q\right] + \\
& + (1-p)\cdot(1-p)\cdot p\cdot(1-p)\cdot\left[q\cdot(1-q)\cdot(1-q)\cdot q + (1-q)\cdot q\cdot(1-q)\cdot q + (1-q)\cdot(1-q)\cdot q\cdot q\right] + \\
& + (1-p)\cdot(1-p)\cdot(1-p)\cdot p\cdot\left[q\cdot(1-q)\cdot(1-q)\cdot q + (1-q)\cdot q\cdot(1-q)\cdot q + (1-q)\cdot(1-q)\cdot q\cdot q + \right. \\
& \quad + q\cdot q\cdot(1-q)\cdot(1-q) + q\cdot(1-q)\cdot q\cdot(1-q) + (1-q)\cdot q\cdot q\cdot(1-q) + \\
& \quad + q\cdot q\cdot q\cdot(1-q) + q\cdot q\cdot(1-q)\cdot q + q\cdot(1-q)\cdot q\cdot q + (1-q)\cdot q\cdot q\cdot q + \\
& \quad \left. + q\cdot q\cdot q\cdot q\right] = \\
& = 3\cdot p^1\cdot(1-p)^3\left[3\cdot q^2\cdot(1-q)^2\right] + \\
& + p^1\cdot(1-p)^3\left[6\cdot q^2\cdot(1-q)^2 + 4\cdot q^3\cdot(1-q)^1 + q^4\right].
\end{aligned}$$

5. При t-й спробі ($t = N + 0 + k$) ймовірність перемоги зловмисника визначається:

$$PI_{N=1,\,j=0,k=k} = k\cdot p^1\cdot(1-p)^k\cdot\left[k\cdot q^2\cdot(1-q)^{k-1}\right]+$$
$$+p^1\cdot(1-p)^k\cdot\left[\binom{k+1}{2}\cdot q^2\cdot(1-q)^{k-1}+\binom{k+1}{3}\cdot q^3\cdot(1-q)^{k-2}+\right.$$
$$\left.+\binom{k+1}{4}\cdot q^4\cdot(1-q)^{k-3}+\ldots+\binom{k+1}{k}\cdot q^k\cdot(1-q)^1+\binom{k+1}{k+1}\cdot q^{(k+1)}\right].$$

Проводячи спрощення, розкладаючи вираз $(a+b)^n$ в степеневий ряд, отримуємо вираз в наступному вигляді:

$$PI_{N=1,\,j=0,k=k} = p^1\cdot(1-p)^k\cdot\left\{k^2\cdot q^2\cdot(1-q)^{k-1}+\left[1-\binom{k+1}{0}\cdot q^0\cdot(1-q)^{k+1}-\binom{k+1}{1}\cdot q^1\cdot(1-q)^k\right]\right\}.$$

Проводячи аналогічні побудови і підсумовуючи всі $k=0,1,2,\ldots$ ми знайдемо ймовірність успішного проведення зловмисником атаки подвійної витрати за умови, що чесною мережею сформовано не більше $N=1$ блоків:

$$PI_{N=1,\,j=0} = \sum_{k=1}^{\infty}\left\{p\cdot(1-p)^k\cdot\left[k\cdot q^2\cdot(1-q)^{k-1}+\right.\right.$$
$$\left.\left.+\left(1-\binom{k+1}{0}\cdot q^0\cdot(1-q)^{k+1}-\binom{k+1}{1}\cdot q^1\cdot(1-q)^k\right)\right]\right\}$$

Зауважимо, що $\binom{k+1}{0}=1$ и $\binom{k+1}{1}=k+1$, однак тут ми залишаємо саме в такому вигляді для можливості подальшого більш наочного узагальнення виразу.

2.2. Ймовірність перемоги зловмисника при довільному N та $j=0$

Розглянемо випадок для $N=2,\ j=0$.

При $k=0$, як і в попередньому випадку, перемога неможлива.

При $k=1$ і, отже, $t=N+0+1=3$, ймовірність перемоги зловмисника буде визначатися:

$$PI_{N=2,\,j=0,k=1} = p\cdot p\cdot(1-p)\cdot[q\cdot q\cdot q]+$$
$$+p\cdot(1-p)\cdot p\cdot[q\cdot q\cdot q]+$$
$$+(1-p)\cdot p\cdot p\cdot[q\cdot q\cdot q]=3\cdot p^2\cdot(1-p)\cdot q^3$$

При $k=2$ ($t=4$), ймовірність перемоги зловмисника визначається:

$$PI_{N=2,\,j=0,k=2} = p\cdot p\cdot(1-p)\cdot(1-p)\cdot\left[q\cdot q\cdot(1-q)\cdot q + q\cdot(1-q)\cdot q\cdot q + (1-q)\cdot q\cdot q\cdot q\right] +$$
$$+ p\cdot(1-p)\cdot p\cdot(1-p)\cdot\left[q\cdot q\cdot(1-q)\cdot q + q\cdot(1-q)\cdot q\cdot q + (1-q)\cdot q\cdot q\cdot q\right] +$$
$$+ (1-p)\cdot p\cdot p\cdot(1-p)\cdot\left[q\cdot q\cdot(1-q)\cdot q + q\cdot(1-q)\cdot q\cdot q + (1-q)\cdot q\cdot q\cdot q\right] +$$
$$+ p\cdot(1-p)\cdot(1-p)\cdot p\cdot\left[q\cdot q\cdot(1-q)\cdot q + q\cdot(1-q)\cdot q\cdot q + (1-q)\cdot q\cdot q\cdot q + q\cdot q\cdot q\cdot(1-q) + q\cdot q\cdot q\cdot q\right] +$$
$$+ (1-p)\cdot p\cdot(1-p)\cdot p\cdot\left[q\cdot q\cdot(1-q)\cdot q + q\cdot(1-q)\cdot q\cdot q + (1-q)\cdot q\cdot q\cdot q + q\cdot q\cdot q\cdot(1-q) + q\cdot q\cdot q\cdot q\right] +$$
$$+ (1-p)\cdot(1-p)\cdot p\cdot p\cdot\left[q\cdot q\cdot(1-q)\cdot q + q\cdot(1-q)\cdot q\cdot q + (1-q)\cdot q\cdot q\cdot q + q\cdot q\cdot q\cdot(1-q) + q\cdot q\cdot q\cdot q\right] =$$
$$= 3\cdot p^2\cdot(1-p)^2\cdot\left[3\cdot q^3\cdot(1-q)\right] +$$
$$+ 3\cdot p^2\cdot(1-p)^2\cdot\left[4\cdot q^3\cdot(1-q) + q^4\right]$$

При $k=3$ ($t=5$) ймовірність перемоги зловмисника визначається:

$$PI_{N=2,\,j=0,k=3} = 6\cdot p^2\cdot(1-p)^3\cdot\left[6\cdot q^3\cdot(1-q)^2\right] +$$
$$+ 4\cdot p^2\cdot(1-p)^3\cdot\left[10\cdot q^3\cdot(1-q)^2 + 5\cdot q^4\cdot(1-q)^1 + 1\cdot q^5\right]$$

Наведені результати дають можливість отримати вирази для довільного значення N і k:

$$PI_{N=N,\,j=0} = \sum_{k=1}^{\infty}\left\{\binom{t-1}{N}\cdot p^N\cdot(1-p)^k\cdot\left[\binom{t-1}{N}\cdot q^{N+1}\cdot(1-q)^{k-1} + \binom{t-1}{N-1}\cdot p^N\cdot(1-p)^k\cdot\left(1-\sum_{i=0}^{N}\binom{t}{i}\cdot q^i\cdot(1-q)^{t-i}\right)\right]\right\}$$

Спрощуючи наведений вираз, отримуємо ймовірність перемоги зловмисника для довільного значення N і k, але за умови, що чесна мережа сформувала не більше N блоків ($j=0$):

$$PI_{N=N,\,j=0} = \sum_{k=1}^{\infty} p^N\cdot(1-p)^k\cdot\left\{\binom{t-1}{N}^2\cdot q^{N+1}\cdot(1-q)^{k-1} + \binom{t-1}{N-1}\cdot\left[1-\sum_{i=0}^{N}\binom{t}{i}\cdot q^i\cdot(1-q)^{t-i}\right]\right\}$$

2.3. Ймовірність перемоги зловмисника при формуванні чесною мережею більш N блоків ($j>0$)

Розглянемо випадок для $N=1,\ j=1$.

При $k=0$ перемога зловмисника неможлива.

При $k=1$ ймовірність перемоги зловмисника визначається:

$$PI_{N=1,\,j=1,k=1} = p\cdot p\cdot(1-p)\cdot\left[q\cdot q\cdot q\right]$$

При $k=2$ ($t=4$) ймовірність перемоги зловмисника визначається:

$$PI_{N=1,\,j=1,k=2} = p\cdot p\cdot(1-p)\cdot(1-p)\cdot\left[q\cdot q\cdot(1-q)\cdot q+q\cdot(1-q)\cdot q\cdot q+(1-q)\cdot q\cdot q\cdot q\right]+$$
$$+\,p\cdot(1-p)\cdot p\cdot(1-p)\cdot\left[q\cdot(1-q)\cdot q\cdot q+(1-q)\cdot q\cdot q\cdot q\right]+$$
$$+\,(1-p)\cdot p\cdot p\cdot(1-p)\cdot\left[q\cdot(1-q)\cdot q\cdot q+(1-q)\cdot q\cdot q\cdot q\right]=$$
$$=p^2\cdot(1-p)^2\cdot\left[q^3\cdot(1-q)\cdot\{3+2+2\}\right]$$

При $k=3$ ($t=5$) ймовірність перемоги зловмисника визначається:

$$PI_{N=1,\,j=1,k=3} = p^2\cdot(1-p)^3\cdot\left[6\cdot q^3\cdot(1-q)^2\right]+$$
$$+\,p^2\cdot(1-p)^3\cdot\left[5\cdot q^3\cdot(1-q)^2\right]+$$
$$+\,p^2\cdot(1-p)^3\cdot\left[5\cdot q^3\cdot(1-q)^2\right]+$$
$$+\,p^2\cdot(1-p)^3\cdot\left[3\cdot q^3\cdot(1-q)^2\right]+$$
$$+\,p^2\cdot(1-p)^3\cdot\left[3\cdot q^3\cdot(1-q)^2\right]+$$
$$+\,p^2\cdot(1-p)^3\cdot\left[3\cdot q^3\cdot(1-q)^2\right]=$$
$$=p^{N+j}\cdot(1-p)^k\cdot q^{N+j+1}\cdot(1-q)^{k-1}\cdot\left\{\binom{k}{1}\cdot\binom{t-1}{2}+\binom{k-1}{1}\cdot\binom{t-2}{2}+\binom{k-2}{1}\cdot\binom{t-3}{2}\right\}$$

Таким чином, узагальнюючи наведені результати для довільних початкових значень, отримуємо ймовірність успішного проведення зловмисником атаки подвійний витрати (PI) на блокчейн-системи, що використовують алгоритм консенсусу Доказ виконаної роботи на основі геш-функції (без фори зловмисника в один попередньо сформований блок):

$$PI = p^N\cdot\sum_{k=1}^{\infty}(1-p)^k\cdot\left\{\binom{t-1}{N}^2\cdot q^{(N+1)}\cdot(1-q)^{(k-1)}+\binom{t-1}{N-1}\cdot\left[1-\sum_{i=0}^{N}\binom{t}{i}\cdot q^i\cdot(1-q)^{(t-i)}\right]\right\}+$$
$$+\sum_{j=1}^{\infty}\left\{p^{(N+j)}\cdot q^{(N+j+1)}\cdot\sum_{k=1}^{\infty}\left[sum_p\cdot(1-p)^k\cdot(1-q)^{(k-1)}\right]\right\},\qquad(1)$$

де $t=N+j+k$;

$$sum_p=\sum_{ip_{(N+j)}=1}^{k}\left(\sum_{ip_{(N+j-1)}=ip_{(N+j)}+1}^{k+1}\left(\dots\sum_{ip_2=ip_3+1}^{t-2}\left(\sum_{ip_1=ip_2+1}^{t-1}\left(sum_q\right)\right)\right)\right);$$

$$sum_q=\sum_{iq_{(N+j)}=1}^{k}\left(\sum_{iq_{(N+j-1)}=iq_{(N+j)}+1}^{k+1}\left(\dots\sum_{iq_{(j+1)}=iq_{(j+2)}+1}^{t-j-1}\left(\sum_{iq_{(j)}=\max\left(iq_{(j+1)}+1,ip_{(j)}\right)}^{t-j}\left(\dots\sum_{iq_2=\max(iq_3+1,ip_2)}^{t-2}\left(\sum_{iq_1=\max(iq_2+1,ip_1)}^{t-1}(1)\right)\right)\right)\right)\right).$$

3. Екстраполяція суми у формулі розрахунку ймовірності перемоги зловмисника

Незважаючи на те, що вираз (1) надає можливість отримати точний кількісний результат щодо ймовірності атак подвійної витрати, він також має і обмеження стосовно можливості його застосування, що пов'язано з поліноміальною складність обчислювальних розрахунків.

Значення сум (sum_p та sum_q) дуже швидко зростає і вже при $j=10$ і $k=15$ розрахунок стає обчислювальна дуже складною задачею. Наприклад, при $j=20$ та $k=7$ сума $sum_p=16\ 570\ 275\ 123$ (це значення комп'ютер розраховував декілька годин). З іншого боку, ці суми для кожного значення N можна підрахувати однократно і використовувати їх для

різних ймовірностей. У табл. 1, 2, в якості прикладу наведено розраховані значення sum_p для $N = 1,5$ та деяких значень j та k.

Таблиця 1

Значення sum_p у виразі (1) для $N = 1$

j	k						
	1	**2**	**3**	**4**	**5**	**6**	**7**
1	1	7	25	65	140	266	462
2	1	11	58	210	602	1470	3192
3	1	16	117	563	2073	6327	16797
4	1	22	213	1314	6041	22528	71775
5	1	29	359	2761	15495	69305	260923
6	1	37	570	5345	35950	189909	833918
7	1	46	863	9690	76927	473768	2399565
8	1	56	1257	16648	154007	1093596	6327475
9	1	67	1773	27349	291592	2364642	15498742
10	1	79	2434	43256	526520	4835606	35639160
11	1	92	3265	66225	912695	9423549	77586723
12	1	106	4293	98570	1526907	17608428	161007165
13	1	121	5547	143133	2476031	31706737	320288355
14	1	137	7058	203359	3905808	55248173	613629478
15	1	154	8859	283376	6011425	93484314	1136709035
16	1	172	10985	388080	9050125	154064036	2042783757
17	1	191	13473	523225	13356092	247916850	3571657702
18	1	211	16362	695518	19357870	390392550	6090688552
19	1	232	19693	912719	27598589	602713571	10151890353
20	1	254	23509	1183746	38759285	913805304	16570275123

Таблиця 2

Значення sum_p у виразі (1) для $N = 5$

j	k						
	1	**2**	**3**	**4**	**5**	**6**	**7**
1	1	43	631	5335	31795	148219	575107
2	1	51	900	9100	64215	350709	1578214
3	1	60	1265	15185	125925	799834	4145505
4	1	70	1745	24600	237279	1736315	10277050
5	1	81	2361	38661	429387	3587388	24053848
6	1	93	3136	59045	748230	7079128	53381664
7	1	106	4095	87850	1259860	13400268	112900788
8	1	120	5265	127660	2056860	24434838	228674250
9	1	135	6675	181615	3266253	43084995	445514295
10	1	151	8356	253486	5059063	73710049	838128214
11	1	168	10341	347755	7661745	122712954	1527675457
12	1	186	12665	469700	11369715	199311469	2705845884
13	1	205	15365	625485	16563225	316537844	4669213780
14	1	225	18480	822255	23725842	492518292	7867415920
15	1	246	22051	1068236	33465804	752091712	12969669012
16	1	268	26121	1372840	46540540	1128836172	
17	1	291	30735	1746775	63884655	1667581587	
18	1	315	35940	2202160	86641695	2427497877	
19	1	340	41785	2752645	116200021	3485859706	
20	1	366	48321	3413536	154233135	4942601727	

Однак, враховуючи обмежену кількість обчислених коефіцієнтів sum_p, вираз (1) дає хороший збіг з експериментальними даними (постановка обчислювального експерименту докладно наведено у [4]), коли ймовірності q та p значно (у два і більше разів) відрізняються один від одного. При цьому відсутня необхідність прораховувати велику кількість значень у сумі по j, що дозволяє обмежитись деякою невеликою попередньо обчисленою множеною значень sum_p. Також, при $q, p > 0,2$ блоки будуть формуватися з відносно високою ймовірністю, що дає можливість значно скоротити суму по k. Крім того, при менших значеннях N сума sum_p зростає повільніше, що дає змогу прорахувати sum_p для більшої кількості значень j та k.

Однак для підвищення точності обчислення (збільшення урахованих коефіцієнтів j та k) є можливість провести екстраполяцію значень sum_p за допомогою поліноміальної апроксимації. Так, для $j=1$ значення sum_p дуже добре апроксимується (в межах відомих значень k) та екстраполюється (за межами вже обчислених значень k) поліномом

$$sum_p(N=1, j=1, k) = 0,125\cdot k^4 + 0,4167\cdot k^3 + 0,375\cdot k^2 + 0,0833\cdot k,$$

для $j=2$:

$$sum_p(N=1, j=2, k) = 0,0097\cdot k^6 + 0,0792\cdot k^5 + 0,2431\cdot k^4 + 0,3542\cdot k^3 + \\ +0,2464\cdot k^2 + 0,0947\cdot k - 0,2158.$$

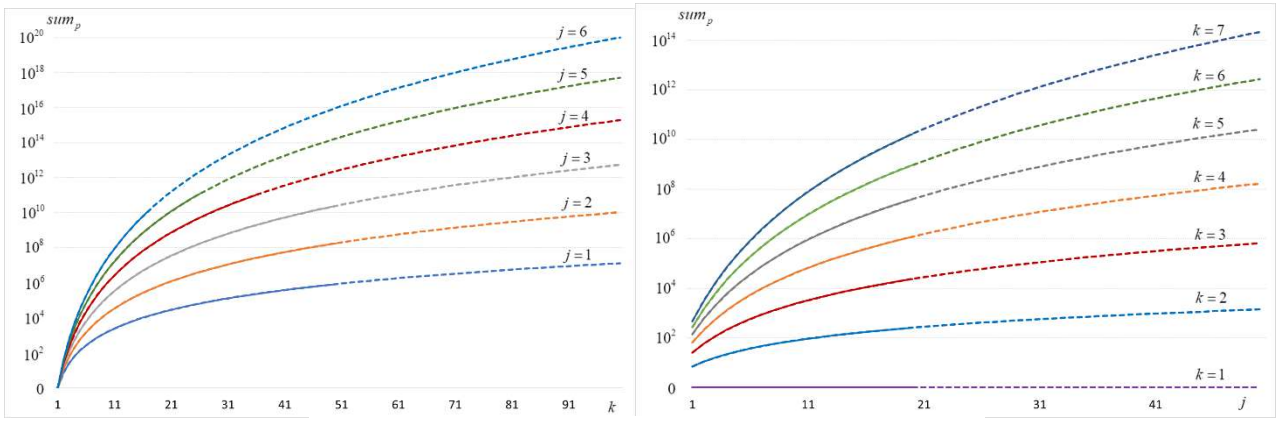
Екстраполяція також добре здійснюється по j, при цьому фіксується значення k.

Як встановлено дослідним шляхом, при обчислювальних методах бажано використовувати інтерполяційний многочлен Лагранжа (дивиться, наприклад, [7] або [8]). Суть якого полягає в наступному. Нам відомі деякі значення sum_p при перших значеннях x_i (x_i вважаємо k_i або j_i), де $i=1,2,\ldots,n$, а n – кількість точок, за допомогою яких будується многочлен Лагранжа (в нашому випадку, для $N=1$, n повинно обиратися як $n=3+2\cdot j$ для екстраполяцій по k та $n=2\cdot k\pm 1$ – для екстраполяцій по j), тоді sum_p можна буде екстраполювати за допомогою інтерполяційного многочлена Лагранжа:

$$sum_p = \sum_{i=0}^{n}\left(sum_p(x_i)\cdot \prod_{\substack{s=0,\\ s\neq i}}^{n} \frac{x-x_s}{x_i-x_s} \right)$$

Результати екстраполяції значення sum_p ілюструє рис. 1, де наведено графік залежності точно обчислених значень sum_p (суцільна лінія) за формулою (1) та її апроксимації та екстраполяції (пунктирна лінія).

Екстраполяція за допомогою полінома дає дуже добру точність, але зі зростанням k (j) зростає кількість перших значень sum_p, які повинні бути відомими та значення яких враховуються у інтерполяційному многочлені Лагранжа. Враховуючи те, що нам відома досить обмежена кількість sum_p (наприклад, у табл. 2 для $k=7$ це sum_p лише для $j\le 15$) поліноміальна екстраполяція також буде мати свої межі застосування.



а *б*

Рис. 1. Залежності значень sum_p (суцільна лінія) обчислених за формулою (1) та її апроксимації та екстраполяції (пунктирна лінія) для $N=1$: *а* – экстраполяция по k, *б* – экстраполяция по j

Наступним методом екстраполяції, який ми застосували, є біноміальна екстраполяція, тобто екстраполяція за допомогою біноміальних коефіцієнтів виду

$$sum_p = d \cdot \binom{N + j + k_i - 1}{N + j}^2$$

де d – деякий коефіцієнт $0 < d < 1$, підбирається дослідним шляхом.

Біноміальна екстраполяція дає значно меншу точність (див. рис. 3, 6, 9), ніж поліноміальна, але кращу ніж неврахування доданків взагалі. Особливо це помітно, коли $q \approx p$ та треба враховувати значну кількість коефіцієнтів j та k.

4. Кількісні розрахунки. Ймовірність вдалого розгалуження блокчейн-ланцюга

Вираз (1) дає можливість наблизити обчислення до реальних умов та не застосовує ряд обмежень та припущень, які притаманні існуючим найбільш популярним аналогічним виразам, що вигідно відрізняє запропоновану модель від існуючих.

При врахуванні фіксованого числа спроб ($t_{\max} = N + n_{\max} + k_{\max}$, де $n_{\max}$ – кількість вдалих, а $k_{\max}$ – невдалих спроб чесної мережі) зловмисником наздогнати блокчейн-ланцюг чесної мережі вираз (1) з напівнескінченного ряду приймає вигляд

$$PI = p^N \cdot \sum_{k=1}^{k_{\max}} (1-p)^k \cdot \left\{ \binom{t-1}{N}^2 \cdot q^{(N+1)} \cdot (1-q)^{(k-1)} + \binom{t-1}{N-1} \cdot \left[1 - \sum_{i=0}^{N} \binom{t}{i} \cdot q^i \cdot (1-q)^{(t-i)} \right] \right\} +$$

$$+ \sum_{j=1}^{n_{\max}} \left\{ p^{(N+j)} \cdot q^{(N+j+1)} \cdot \sum_{k=1}^{k_{\max}} \left[sum_p \cdot (1-p)^k \cdot (1-q)^{(k-1)} \right] \right\},$$

значення sum_p залишається таким же як у (1).

Обчислені за даним виразом графіки ймовірності вдалого формування зловмисником альтернативного блокчейн-ланцюга, для довільного значення p та q наведені на рис. 2, 5, 8. При цьому, для $N=1$ було обрано $n_{\max}=50, k_{\max}=300$; для $N=3$ – $n_{\max}=20, k_{\max}=300$; для $N=5$ – $n_{\max}=20, k_{\max}=300$. На рис. 3, 6, 9 та 4, 7, 10 наведені відносна похибка отриманих розрахунків та кількість реалізацій моделі тестування відповідно. Тестування проводилось як описано у [4]).

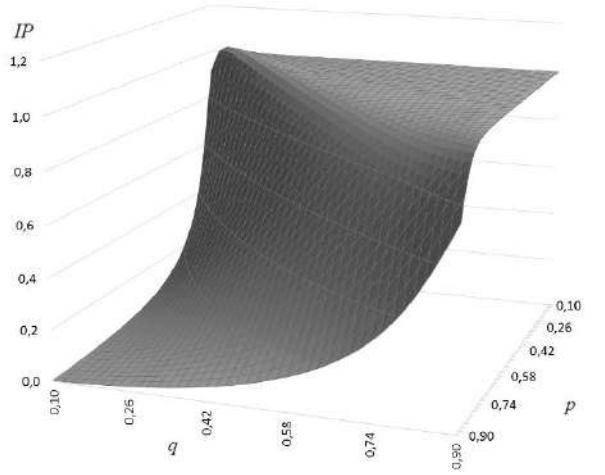


Рис. 2. Функція розподілу ймовірності для різних значень p та q при довжині сформованого ланцюжка з $N=1$ блок

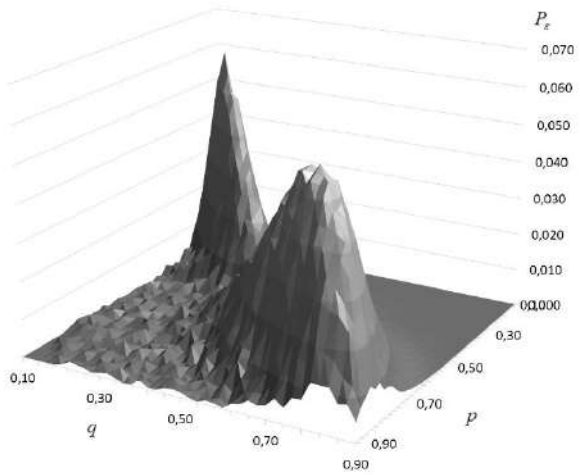


Рис. 3. Відносна похибка розбіжностей між експериментальними і теоретичними значеннями при $N=1$ блок

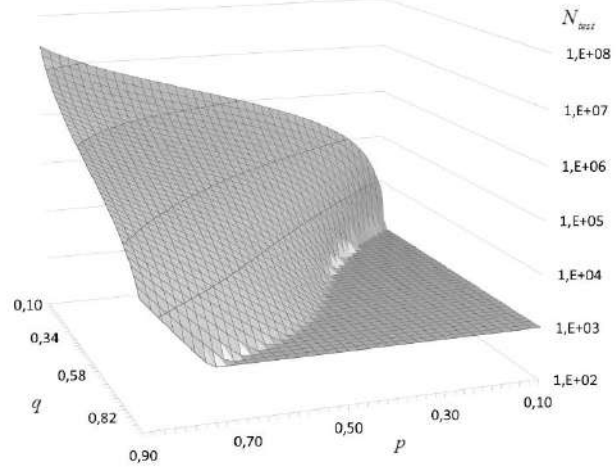


Рис. 4. Число проведених випробувань, що використовувались у експериментальних обчисленнях при довжині сформованого ланцюжка з $N=1$ блок

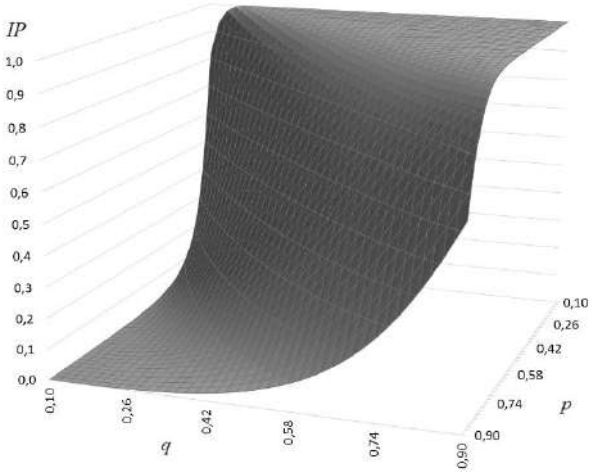


Рис. 5. Функція розподілу ймовірності для різних значень p та q при довжині сформованого ланцюжка з $N=3$ блоки

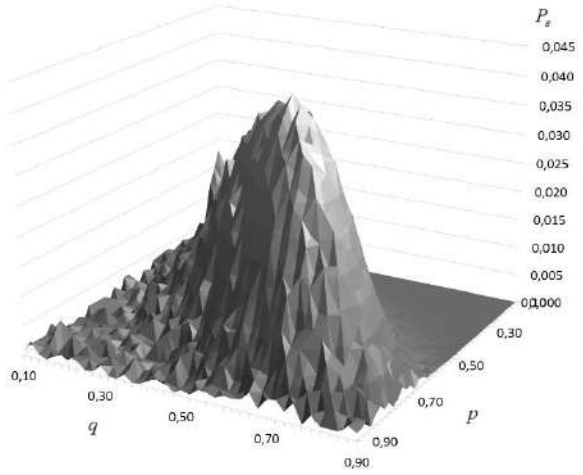


Рис. 6. Відносна похибка розбіжностей між експериментальними і теоретичними значеннями при $N=3$ блоки

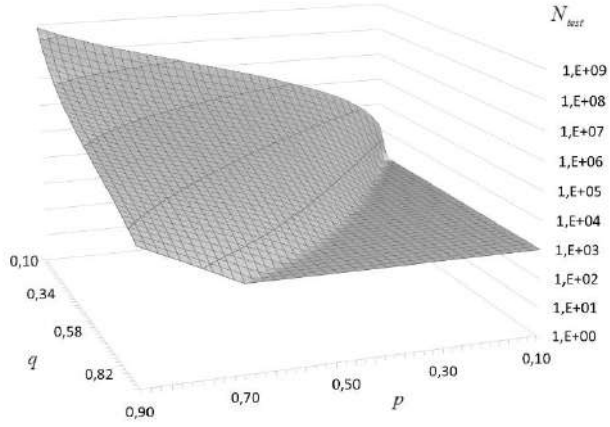


Рис. 7. Число проведених випробувань, що використовувались у експериментальних обчисленнях при довжині сформованого ланцюжка з $N=3$ блоки

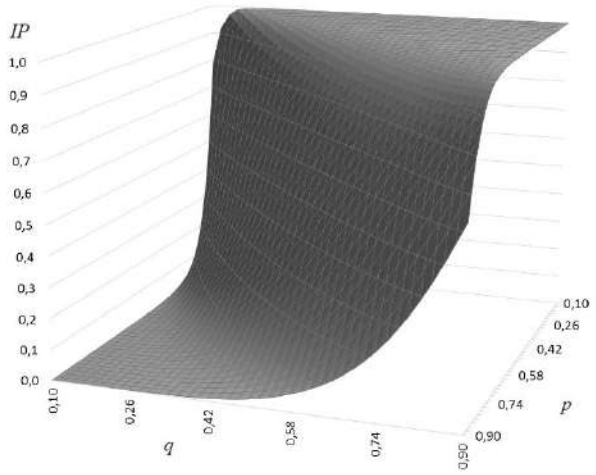


Рис. 8. Функція розподілу ймовірності для різних значень p та q при довжині сформованого ланцюжка з $N=5$ блоків

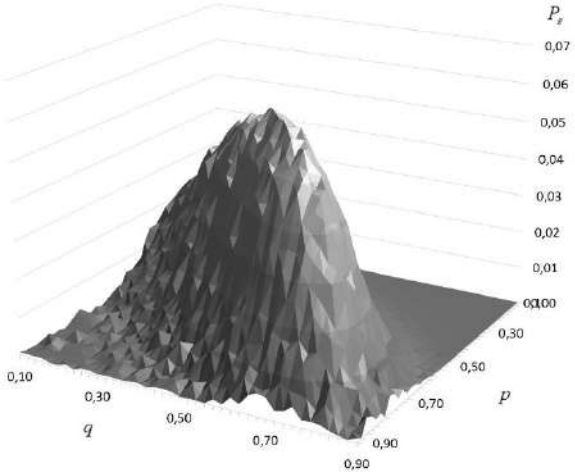


Рис. 9. Відносна похибка розбіжностей між експериментальними і теоретичними значеннями при $N=5$ блоків

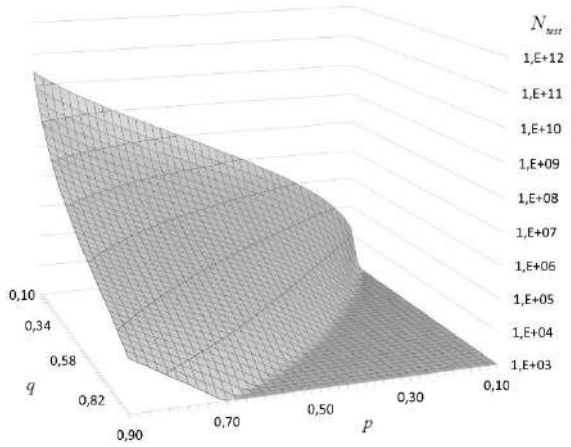


Рис. 10. Число проведених випробувань, що використовувались в експериментальних обчисленнях при довжині сформованого ланцюжка з $N=5$ блоків

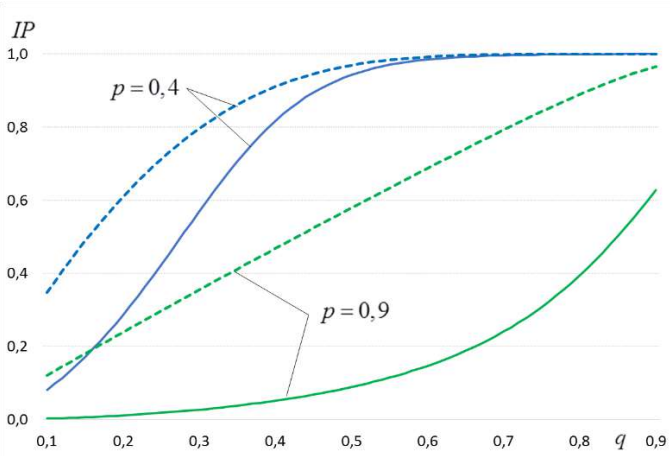


Рис. 11. Функція розподілу ймовірності при $N=1$. Пунктирна лінія – ймовірність з одним попередньо сформованим блоком зловмисником, суцільна – ймовірність з однаковими початковими умовами

Як бачимо, при $q \approx p$ відносна похибка вище обраного значення (обрано відносну помилку не гірше 1 % при довірчій ймовірності не менш 99 %), що обумовлено значно нижчою точністю екстраполяції, яку забезпечує біноміальна екстраполяція.

На рис. 11 наведене порівняння ймовірностей вдалого розгалуження блокчейн-ланцюга за умови одного попередньо сформованого блоку зловмисником (розраховано за тими ж умовами, крім попередньо сформованого блоку, що і вираз (1) – пунктирні лінії) та з однаковими початковими умовами (розраховано за формулою (1) – суцільні лінії), при $n_{\max}=50, k_{\max}=300$.

Як бачимо, за умови відсутності фори, ймовірність перемоги зловмисника суттєво знижується, що є природно, у зв'язку з тим, що зловмиснику необхідно випередити чесну мережу, тобто сформувати на один блок більше. При цьому, як бачимо, різниця є досить значна та може досягати кілька разів. Таким чином, при рівних ймовірностях зловмиснику потрібні значно більші потужності (гешрейт), ніж потужності, розраховані за умови заздалегідь сформованого зловмисником блоку.

5. Висновки

Докладно розглянута одна з основних вразливостей блокчейн-систем, побудованих за допомогою консенсусу з вірогідною завершеністю – атака подвійної витрати.

На підставі моделі «незалежних гравців» отримано аналітичний вираз розрахунку ймовірності успішного проведення зловмисником атаки подвійної витрати на блокчейн-системи, що використовують алгоритм консенсусу Доказ виконаної роботи (PoW) на основі геш-функції у залежності від використовуваної кількості підтверджень та кількості спроб, а також гешрейту чесної мережі і зловмисника.

Прийнята модель «незалежних гравців» та отримана на її основі формула (1) дозволяють позбавитись значних недоліків, які притаманні іншим роботам в даній галузі, а саме:

– проведення гонки між двома учасниками мережі не потрібно уявляти нескінченою, достатньо обмежуватись деяким фіксованим числом спроб;

– використовує більш адекватну, на погляд авторів, модель незалежних гравців, яка включає в себе простір з чотирьох елементарних подій, замість двох, що використовується у моделі «розорення гравця»;

– ймовірності сформувати блок чесною мережею і зловмисником є незалежними величинами, які визначаються безпосередньо потужностями, якими володіють учасники, та зазначені ймовірності ніяк не залежать один від одного, тобто вимога $p+q=1$ є не обов'язковою;

– обчислюється ймовірність саме випередження зловмисником чесної мережі, а ні тільки ймовірність її наздогнати, тобто коли зловмисник не має фори в один попередньо сформований блок.

Наведено кількісні значення, отримані за виразом (1), ймовірності вдалої атаки для різних можливостей зловмисника (ймовірності сформувати блок), різної кількості сформованих блоків, після яких угода вважається підтвердженою, різної тривалості гонки (кількості блоків, протягом яких зловмисник продовжує спроби наздогнати чесну мережу). За допомогою комп'ютерного моделювання експериментально перевірено розраховані за формулою (1) значення. Всі емпіричні оцінки отримано для високої точності (відносна помилка не гірше 1 %) і достовірності (довірча ймовірність не менш 99 %). Для підтвердження адекватності отриманих результатів наведено порівняння емпіричних результатів з теоретичними розрахунками.

Дослідження дозволили отримати нові аналітичні оцінки ймовірностей реалізації атак подвійної витрати на блокчейн-системи із протоколом консенсусу Доказу виконаної роботи. Ці аналітичні оцінки є відмінними від отриманих та відомих раніше, оскільки побудовані на іншій системі припущень та базових положень стосовно моделювання дій різних гравців в блокчейн-мережах, що застосовують Доказ виконаної роботи.

На основі отриманих результатів можна зробити висновок, що безпека блокчейн-систем, які використовують алгоритми консенсусу з ймовірнісною завершеністю (доказ виконаної роботи та її модифікації), мають більш високу надійність, ніж вважалось раніше.

Отримані результати можуть бути корисними при обґрунтуванні конкретних показників та параметрів протоколу консенсусу на основі Доказу виконаної роботи, при застосуванні його у якості основного механізму встановлення консенсусу перспективних децентралізованих розподілених систем та мереж, побудованих за технологією блокчейн.

Список літератури:

1. Zaghloul E., Li T., Mutka M.W. & Ren, J. (2019). Bitcoin and Blockchain: Security and Privacy. ArXiv, abs/1904.11435

2. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System / Satoshi Nakamoto, 2009. 9 с.

3. Rosenfeld M. Analysis of hashrate-based double-spending / Meni Rosenfeld, 2014. 13 с.

4. Полуяненко Н.А., Кузнецов А.А. Моделирование атаки двойной траты на протокол консенсуса «proof of work» // Радиотехника. 2019. № 198. С. 146–161. DOI: 10.30837/rt.2019.3.198.11

5. Zaghloul E., Li T., Mutka M.W. & Ren J. (2019). Bitcoin and Blockchain: Security and Privacy. ArXiv, abs/1904.11435

6. A. Pinar Ozisik, Brian Neil Levine. An Explanation of Nakamoto's Analysis of Double-spend Attacks https://arxiv.org/pdf/1701.03977.pdf

7. Турчак Л.И., Плотников П.В. Основы численных методов : учеб. пособие ; 2-е изд., перераб. и доп. Москва : Физматлит, 2003. 304 с.

8. Archer, Branden and Weisstein, Eric W. Lagrange Interpolating Polynomial. From MathWorld-A Wolfram Web Resource. http://mathworld.wolfram.com/LagrangeInterpolatingPolynomial.html.

Харківський національний
університет імені В. Н. Каразіна;
АТ «Інститут інформаційних технологій»

Надійшла до редколегії 05.02.2020

УДК 004.056.5 **DOI:10.30837/rt.2020.1.200.13**

Н.А. ПОЛУЯНЕНКО, канд. техн. наук, О.О. КУЗНЕЦОВ, д-р техн. наук

ЙМОВІРНІСТЬ УСПІШНОЇ АТАКИ ПОДВІЙНОЇ ВИТРАТИ НА БЛОКЧЕЙН-СИСТЕМИ ІЗ ЙМОВІРНІСНИМ ПРОТОКОЛОМ КОНСЕНСУСУ

Вступ

Як правило, всі «класичні» платіжні системи є централізованими, що мають адміністративну ланку, яка забезпечує контроль легітимності будь-якої операції. При цьому, підстава для прийняття рішень про легітимність платежу є інформація, яка надається адміністратором, а не інформація, яка представлена платником. Тому платник в змозі лише сформувати заявку на повторну витрату одних і тих же засобів, а адміністративна ланка підтвердить тільки першу заявку і відкине всі інші, що блокує можливість подвійної витрати одних і тих же цінностей. У блокчейн-системах передбачається відсутність адміністративного ресурсу, і отже, можливість проведення подвійної витрати одних і тих же цінностей стає можливим.

Атака подвійного витрачання буває в багатьох формах. Кожен з можливих методів, що реалізує ту чи іншу форму, повинен перевірятися і оброблятися програмним забезпеченням повного вузла. Наведемо різні методи, які можуть бути застосовані для проведення повторної витрати одних і тих же коштів:

- одна транзакція в mempool, що витрачає один і той же вхідні значення (UTXO – Unspent Transaction (TX) Output) кілька разів;
- кілька транзакцій в mempool, які витрачають кошти, посилаючись на одні і ті ж вхідні значення (UTXO);
- транзакція в одному блоці, яка проводить одні і ті ж вхідні значення (UTXO) кілька разів;
- кілька транзакцій в різних блоках витрачають одні і ті ж вхідні значення (UTXO);
- проведення атаки за допомогою вдалого розгалуження блокчейн-реєстру, при цьому кожна з гілок містить різні транзакції, що змінюють діючий стан блокчейн-системи.

Вразливостям, що засновані на перших чотирьох наведених методах, можна вдало запобігти за допомогою відповідної реалізації програмного забезпечення. Однак все одно залишається можливість її реалізації, наприклад у [1, 2] наведено опис виявлених вразливостей у Bitcoin Core, а також детальний аналіз причини їх появи [3].

Щоб максимально унеможливити маніпулювання блокчейн-системою на свою користь однієї особи, процес майнинга Bitcoin розроблений як дорога і ресурсномістка операція. Для формування нового блоку з транзакціями в блокчейн-систему майнери повинні надати дійсні докази виконаної роботи. Але не зважаючи на це, у зловмисника, який намагається виконати п'ятий спосіб, так само є не менш чотирьох варіантів його проведення (більш детально дивиться у [4]) серед яких є атака 51 %.

Сутність атаки 51 % полягає у наступному: зловмисник генерує платіжну транзакцію і випускає її в мережу; продавець очікує отримання відповідної кількості підтверджень, перш ніж прийняти платіж і здійснити операцію. Одночасно зловмисник таємно починає формувати блок, що містить шахрайську транзакцію, за якою слідують додаткові блоки для її підтвердження. Оскільки обчислювальна потужність атакуючого більше, ніж решта обчислювальної потужності всіх майнерів разом узятих, атакуючий може добувати блоки за менший час. Як тільки продавець приймає транзакцію, зловмисник розповсюджує таємно здобуті блоки, щоб створити розгалуження в блокчейн-реєстрі. Якщо шахрайське розгалуження, створене атакуючим, містить більшу кількість блоків, ніж початковий ланцюг, воно стає домінуючим, і всі майнери приймають дане розгалуження за основне і починають його поширювати, а також включати в ланцюжок блоків при формуванні наступних блоків. Таким чином, первісна платіжна транзакція більше не існує в блокчейн-реєстрі.

Ця атака є найбільшою загрозою для блокчейн-систем з консенсусами, які мають ймовірнісний характер завершеності, оскільки вона безпосередньо пов'язана з ресурсами, які може використовувати зловмисник. Ресурси виміряються з точки зору фінансової та обчислювальної потужності. Важливо відзначити, що навіть при обчислювальній потужності менше 50 % зловмисник все ще може маніпулювати системою.

Для захисту від атаки 51 % продавці можуть приймати різні заходи захисту, найбільш ефективним з них є очікування включення транзакції з оплатою в один з блоків блокчейн-реєстру. При цьому вузол, який формує блок, не допустить включення в блок транзакцій, які намагаються повторно витратити раніш витрачені кошти. І якщо навіть такий блок буде сформовано вузлом зловмисника, його відкинуть вузли чесної мережі і блок не буде додано до блокчейн-реєстру чесних користувачів.

Процес включення транзакції до складу нового блоку називається підтвердженням транзакції. Включення в один блок відповідає одному підтвердженню. Формування і додавання до реєстру блокчейн-ланцюжка ще з $(N-1)$ блоків, які посилаються на блок з транзакцією, відповідає N підтвердженням. Однак, якщо використовується алгоритм консенсусу Доказ виконаної роботи та зловмисник має досить великі ресурси (володіє високопродуктивним обладнанням, здатним забезпечити високий гешрейт (англ. – hashrate) зловмисника) у нього все ще залишається досить висока ймовірність успішно провести подвійну витрату шляхом формування альтернативного ланцюжка блокчейн реєстру.

Успіх атаки подвійних витрат безпосередньо залежить від ресурсів (гешрейта) атакуючого і кількості підтверджень. Ймовірність формування альтернативного ланцюжка експоненціально зменшується зі зростанням кількості підтверджень і зменшенням гешрейта атакуючого. Чим більше підтверджень має транзакція, тим менш імовірне скасування транзакції через заміну діючого ланцюжка альтернативним, що сформовано зловмисником. Однак, з іншого боку, чим більше продавець чекає підтверджень, тим довше затримується проведення самої угоди, що внаслідок веде до значних затримок, дискомфорту використання системи та збиткам взаємодіючих сторін.

Тому угоди з нульовим підтвердженням потенційно мають великий ризик стати жертвою атаки подвійних витрат, а угоди, які очікують велику кількість підтверджень, – зазнати збитків через затримки в їх укладанні. Тому, знаходження оптимальної кількості підтверджень, при яких ризик атаки подвійної витрати буде нижче деякого прийнятного рівня, а час очікування буде мінімально необхідним, є актуальним завданням.

Наприклад, існує думка [5 – 8], якщо використовується механізм консенсусу на основі Доказу виконаної роботи на основі геш-функції і у атакуючого знаходиться 10 % обчислювальної потужності (гешрейт) від загальної мережі і очікується шість підтверджень, – ймовірність успіху такої атаки складе 0,1 %. Наведена оцінка ґрунтується на моделі «розорення гравця» (см. [9]), яка не використовує незалежні події для чесної мережі і зловмисника та багато інших припущень.

Сукупність цих припущень та обмежень дає значну похибку між експериментальними моделюваннями методами Монте-Карло та відповідно ймовірностями проведення успішних атак на блокчейн-системи, які використовують механізм консенсусу на основі Доказу виконаної роботи [10]. Ця стаття є логічним продовженням роботи в цьому напрямку та дає аналітичний вираз ймовірності успішного розгалуження ланцюжка блоків при використанні алгоритму консенсусу Доказ виконаної роботи.

Моделі, що застосовується при оцінки вдалої реалізації атаки 51 %

Оцінку ймовірності вдалої реалізації атаки 51 % дано ще в роботі Сатоши Накамото [11], а також більш точні результати отримано Мені Розенфельдом [5], які на сьогоднішній день є одними з найпопулярніших і цитованих робіт в даній сфері. Існують також інші роботи, які уточнюють і доповнюють результати отримані Сатоши Накамото і Мені Розенфельдом, більш детально про це було описано в [10].

Згадані роботи формують свої виводи на підставі моделі «розорення гравця». На основі даної моделі отримується формула для розрахунку ймовірності успішного проведення атаки. В основу цієї моделі покладено факт, що у кожному випробуванні або виграє зловмисник (формуючи черговий блок), або зловмисник програє і при цьому вважається, що виграє чесна мережа (формуючи черговий блок). Однак в роботах не наводиться будь-якого обґрунтування обраної моделі. Автори припускають, що якщо блок не сформував зловмисник, то в такому випадку блок обов'язково формує чесна мережа, при цьому це припущення ніяк не обґрунтовується.

Ми пропонуємо використовувати модель «незалежних гравців». У даній моделі, на відміну від моделі «розорення гравця», формування чергового блоку у зловмисника і чесної мережі відбувається повністю незалежно один від одного. Нехай ймовірність сформувати блок зловмисником буде q, а чесною мережею – p, відмовившись від обов'язкового для моделі «розорення гравця» виконання умови $p=1-q$, ми отримаємо в результаті кожної спроби (або серії спроб протягом заданого інтервалу часу) простір елементарних подій, що містить наступні події:

- елементарна подія «блок сформований чесною мережею і атакуючий не сформував блок» з ймовірністю $p\cdot(1-q)$;
- елементарна подія «блок не сформований чесною мережею і атакуючий сформував блок» з ймовірністю $(1-p)\cdot q$;
- елементарна подія «блок не сформований чесною мережею і атакує не сформував блок» з ймовірністю $(1-p)\cdot(1-q)$;
- елементарна подія «блок сформований чесною мережею і атакуючий сформував блок» $p\cdot q$.

Безліч всіх елементарних подій становить повну групу подій:

$$p\cdot(1-q)+(1-p)\cdot q+(1-p)\cdot(1-q)+p\cdot q=1.$$

Ця модель з чотирма елементарними подіями описує реальний ймовірнісний процес в блокчейн-системі при встановленні консенсусу на основі алгоритму «Proof of work».

З метою можливості порівняння з результатами, отриманими у роботах Сатоши Накамото і Мені Розенфельда, також будемо використовувати деякі спрощення:

- час поширення блоку у мережі дуже малий, тобто обмін інформацією між вузлами відбувається практично миттєво (час синхронізації дорівнює нулю);
- гешрейт зловмисника, гешрейт чесної мережі і складність майнінгу не змінюється з часом протягом всієї гонки;
- можливості зловмисника з підтримки стану гонки досить великі, але не безмежні;
- крім зловмисника всі інші користувачі мережі діють строго відповідно до правил протоколу блокчейн-мережі;
- перемогою зловмисника будемо вважати формування необхідної кількості блоків підтвердження раніше або одночасно (вважається, що один блок зловмисник сформував заздалегідь) або, в іншому випадку, – подальшого формування ланцюжка блоків рівною з чесною мережею довжини.

Зауважимо, що в умовах блокчейн-систем ймовірність p для кожного окремого суб'єкта не залежить від номера випробувань і від інших суб'єктів і визначається виключно потужністю, яку він має (справедливо для алгоритмів консенсусу Доказу виконаної роботи та його аналогів). Ймовірність p можна прив'язати до гешрейту (кількості протестованих геш-функцій в секунду), але в загальному випадку покладемо значення p – ймовірність сформувати блок за деяку умовну одиницю часу.

Зловмисник може перемогти в момент початку гонки. При цьому йому необхідно сформувати N або більше блоків до того моменту, коли чесна мережа сформує N блоків. Якщо йому це не вдасться, то у нього все ще є можливість наздогнати чесну мережу на

$N + j$ блоці, де j – кількість блоків сформованих чесною мережею на додаток до необхідних N блоків.

Отримаємо вираз, який характеризує ймовірність формування блоків в залежності від N, j і кількості невдалих спроб сформувати блок чесною мережею (k).

Ймовірність перемоги зловмисника

Ґрунтуючись на наведеній групі подій, отримаємо наступні можливі ймовірності і комбінації в яких зловмисник здобуває перемогу (для $N=1, j=0$):

1. При першій спробі (в даному випадку при $t = N + j + k = 1 + 0 + 0 = 1$). Комбінація може бути тільки одна – коли і чесна мережа, і зловмисник одночасно знаходять блоки. У цьому випадку ймовірність перемоги зловмисника буде визначатися як $PI_{N=1,\,j=0,k=0} = p \cdot q$;

2. При другій спробі ($t = N + 1 = 2$). При цьому, може бути дві різні ситуації

- чесна мережа знаходить блок при першому випробуванні, але не знаходить при другому (ймовірність чого дорівнює $p \cdot (1-p)$). У даному випадку, якщо зловмисник знайде блок при першому випробуванні, ми прийдемо до п.1, отже, він може знайти блок тільки за друге випробування (ймовірність $(1-q)\cdot q$);

- чесна мережа не знаходить блок при першому випробуванні, а знаходить тільки при другому (ймовірність чого дорівнює $(1-p)\cdot p$). При цьому зловмисник може знайти блок при першому випробуванні (з ймовірністю $q\cdot(1-q)$) або при другому випробуванні (з ймовірністю $(1-q)\cdot q$), і при обох випробуваннях (з ймовірністю $q \cdot q$).

Загальна ймовірність даної події:

$$PI_{N=1,\,j=0,k=1} = \left[p\cdot(1-p)\cdot(1-q)\cdot q \right] +$$
$$+\left[(1-p)\cdot p\cdot q\cdot(1-q) + (1-p)\cdot p\cdot(1-q)\cdot q + (1-p)\cdot p\cdot q\cdot q \right] =$$
$$= p\cdot(1-p)\cdot\left[(1-q)\cdot q \right] + (1-p)\cdot p\cdot\left[q\cdot(1-q) + (1-q)\cdot q + q\cdot q \right];$$

3. При третій спробі ($t = N + 2 = 3$). Тут також можна розглянути три ситуації: чесна мережа формує блок на першому, на другому або на третьому випробуванні і при цьому існують різні комбінації, коли може бути сформований блок (або блоки) зловмисником. Сумарна ймовірність настання подій буде обчислюватися аналогічно вищеописаним подіям, підсумкова ймовірність яких буде:

$$\begin{aligned} PI_{N=1,\,j=0,k=2} &= p\cdot(1-p)\cdot(1-p)\cdot\left[(1-q)\cdot(1-q)\cdot q \right] + \\ &+ (1-p)\cdot p\cdot(1-p)\cdot\left[(1-q)\cdot(1-q)\cdot q \right] + \\ &+ (1-p)\cdot(1-p)\cdot p\cdot\left[q\cdot(1-q)\cdot(1-q) + (1-q)\cdot q\cdot(1-q) + \right. \\ &+ (1-q)\cdot(1-q)\cdot q + q\cdot q\cdot(1-q) + q\cdot(1-q)\cdot q + (1-q)\cdot q\cdot q + \\ &\left. + q\cdot q\cdot q \right] = \\ &= p^1\cdot(1-p)^2\left[q^1\cdot(1-q)^2 \right] + p^1\cdot(1-p)^2\left[q^1\cdot(1-q)^2 \right] + \\ &+ p^1\cdot(1-p)^2\left[3\cdot q^1\cdot(1-q)^2 + 3\cdot q^2\cdot(1-q)^1 + q^3 \right] \end{aligned}$$

4. При t-й спробі ($t = N + k$). Ймовірність перемоги зловмисника буде визначатися:

$$PI_{N=1,\,j=0,k=k} = k \cdot p^1 \cdot (1-p)^k \cdot \left[q^1 \cdot (1-q)^k \right] + \\ + p^1 \cdot (1-p)^k \cdot \left[(k+1) \cdot q^1 \cdot (1-q)^k + \binom{k+1}{2} \cdot q^2 \cdot (1-q)^{k-1} + \right. \\ \left. + \binom{k+1}{3} \cdot q^3 \cdot (1-q)^{k-2} + \ldots + (k+1) \cdot q^k \cdot (1-q)^1 + q^{(k+1)} \right]$$

При цьому, розкладаючи вираз $(a+b)^n$ в степеневий ряд, отримуємо співвідношення з біноміальними коефіцієнтами:

$$(a+b)^n = a^n + n \cdot a^1 \cdot b^{(n-1)} + \binom{n}{2} \cdot a^2 \cdot b^{n-2} + \binom{n}{3} \cdot a^3 \cdot b^{n-3} + \ldots + n \cdot a^1 \cdot b^{n-1} + 1 \cdot a^n,$$

припускаючи $a = q$, $b = (1-q)$, а $n = k+1$, отримуємо вираз у других квадратних дужках з точністю до першого доданка, тобто:

$$((1-q)+q)^{k+1} = (1-q)^{k+1} + (k+1) \cdot (1-q)^k \cdot q^1 + \binom{k+1}{2} \cdot (1-q)^{k-1} \cdot q^2 + \\ + \binom{k+1}{3} \cdot (1-q)^{k-2} \cdot q^3 + \ldots + (k+1) \cdot (1-q)^1 \cdot q^k + q^{(k+1)}$$

Разом з тим $((1-q)+q)^{k+1} = 1^{k+1} = 1$. Таким чином, можна спростити вираз:

$$PI_{N=1,\,j=0,k=k} = k \cdot p^1 \cdot (1-p)^k \cdot \left[q^1 \cdot (1-q)^k \right] + p^1 \cdot (1-p)^k \cdot \left[1 - (1-q)^{k+1} \right].$$

Підсумовуючи $k = 0, 1, 2, \ldots$, знайдемо ймовірність успішного проведення зловмисником атаки подвійної витрати за умови, що чесною мережею сформоване не більше $N = 1$ блоків:

$$PI_{N=1,\,j=0} = \sum_{k=0}^{\infty} \left\{ k \cdot p \cdot (1-p)^k \cdot \left[q \cdot (1-q)^k \right] + p \cdot (1-p)^k \cdot \left[1 - (1-q)^{k+1} \right] \right\} = \\ = p \cdot q \cdot \sum_{k=0}^{\infty} \left\{ k \cdot (1-p)^k \cdot \left[(1-q)^k \right] \right\} + p \cdot \sum_{k=0}^{\infty} \left\{ (1-p)^k \cdot \left[1 - (1-q)^{k+1} \right] \right\}$$

Проводячи аналогічні міркування і далі отримуємо ймовірність виграшу зловмисника у чесній мережі (PI):

$$PI = p^N \cdot \sum_{k=0}^{\infty} \left((1-p)^k \cdot \binom{t-1}{N-1} \cdot \left[\binom{t-1}{N} \cdot q^N \cdot (1-q)^k + \left\{ 1 - \sum_{i=0}^{N-1} \binom{t}{i} \cdot q^i \cdot (1-q)^{t-i} \right\} \right] \right) + \\ + \sum_{j=1}^{\infty} \left[p^{(N+j)} \cdot q^{(N+j)} \cdot \sum_{k=1}^{\infty} \left(sum_p \cdot (1-p)^k \cdot (1-q)^k \right) \right], \qquad (1)$$

де

$t = N + j + k$;

$$sum_p = \sum_{ip_{(N+j)}=1}^{k} \left(\sum_{ip_{(N+j-1)}=ip_{(N+j)}+1}^{k+1} \left(\ldots \sum_{ip_2=ip_3+1}^{N+j+k-2} \left(\sum_{ip_1=ip_2+1}^{N+j+k-1} \left(sum_q \right) \right) \right) \right);$$

$$sum_q = \sum_{iq_{(N+j)}=1}^{k+1} \left(\sum_{iq_{(N+j-1)}=iq_{(N+j)}+1}^{k+2} \left(\ldots \sum_{iq_{(N+1)}=iq_{(N+2)}+1}^{k+N-1} \left(\sum_{iq_N=\max(iq_{(N+1)}+1,\,ip_{(N-1)})}^{k+N} \left(\ldots \sum_{iq_3=\max(iq_4+1,\,ip_2)}^{N+j+k-2} \left(\sum_{iq_2=\max(iq_3+1,\,ip_1)}^{N+j+k-1} (1) \right) \right) \right) \right) \right).$$

Звертаємо увагу, якщо $N=1$, то зовнішнє підсумовування для sum_q починається с $iq_{(N+j)}=ip_{(N+j-1)}$, а якщо і $j=0$, то в цьому випадку $sum_q=1$.

Порівняння результатів з моделлю розорення гравця. Рекомендації щодо «безпечного» числа підтверджень

На основі отриманих виразів покажемо, яка необхідна кількість підтверджень для збереження ймовірності успіху зловмисника нижче заданого «безпечного» значення, при різних значеннях гешрейта. Під «безпечним» значенням будемо розуміти таке значення P_S, при якому верхня межа ймовірності проведення атаки подвійної витрати може вважатися прийнятним ризиком.

Конкретне «безпечне» значення ймовірності проведення атаки подвійної витрати кожен користувач визначає для себе сам в залежності від прийнятних для нього ризиків (величини угоди, ризиків репутації, необхідної оперативності проведення операції тощо). Нами розглянуто значення $P_S=0{,}1;0{,}01;\ 0{,}001$ і проведено порівняння отриманих результатів з результатами, отриманими на підставі моделі розорення гравця, які детально досліджені в роботі Мені Розенфельда [5].

На рис. 1 – 3 наведено мінімальну кількість підтверджень, необхідну для підтримки ймовірності успішного проведення атаки подвійної витрати, в залежності від гешрейта атакуючого, що дорівнює або нижче значення P_S. Гешрейт чесної мережі як і раніше будемо вважати $p=1-q$.

При порівнянні отриманих результатів з результатами, розрахованими відповідно до моделі розорення гравця, що наведені в роботі Мені Розенфельда [5.], бачимо, що ймовірність успішного проведення атаки подвійної витрати нижче, ніж вважалося до цього. У зв'язку з чим можливо обмежитись меншою кількістю необхідних підтверджень в блокчейн-системі при тому ж рівні безпеки. Це на практиці дозволить значно знизити час очікування для укладання угоди і, як наслідок, значно підвищити швидкість проведення операцій з блокчейн-системами.

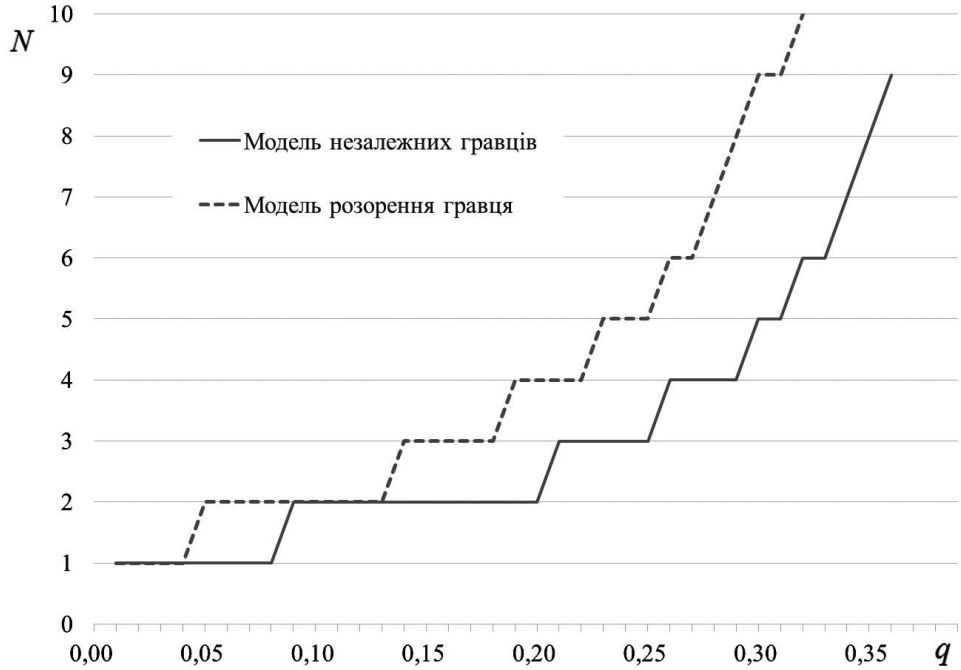


Рис. 1. Кількість підтверджень, необхідних для підтримки ймовірності успіху зловмисника на рівні, який не перевищує $P_S=0{,}1$. Суцільна лінія відповідає моделі незалежних гравців, пунктирна – моделі розорення гравця

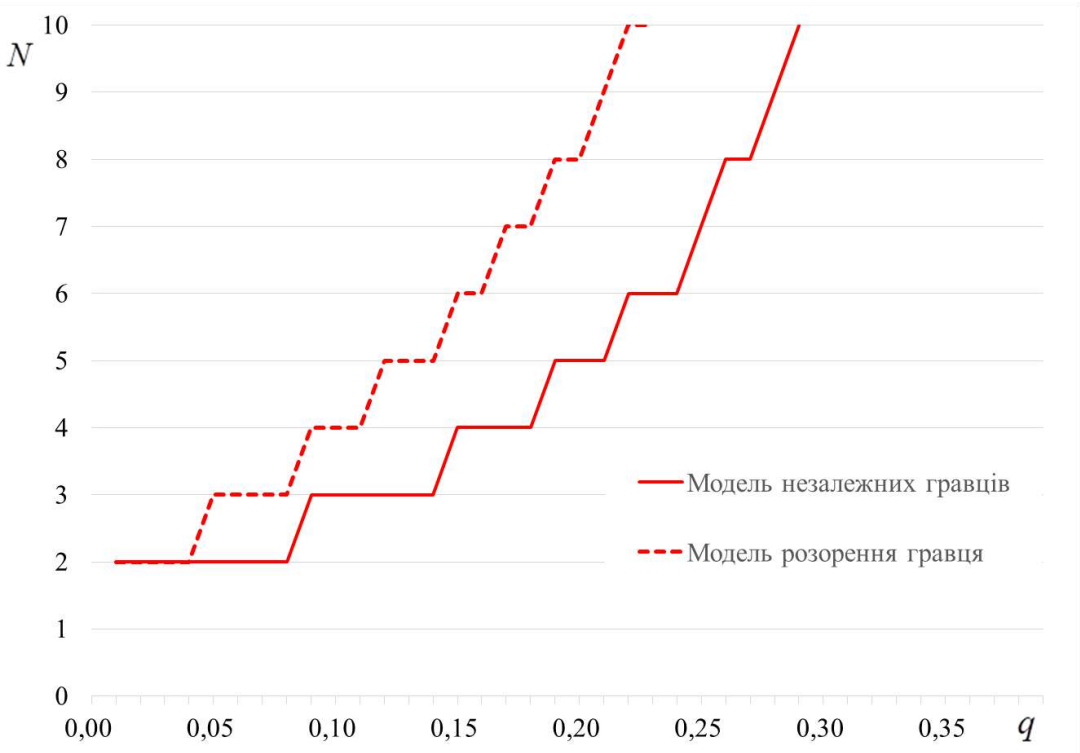


Рис. 2. Кількість підтверджень, необхідних для підтримки ймовірності успіху зловмисника на рівні, який не перевищує $P_S = 0,01$. Суцільна лінія відповідає моделі незалежних гравців, пунктирна – моделі розорення гравця.

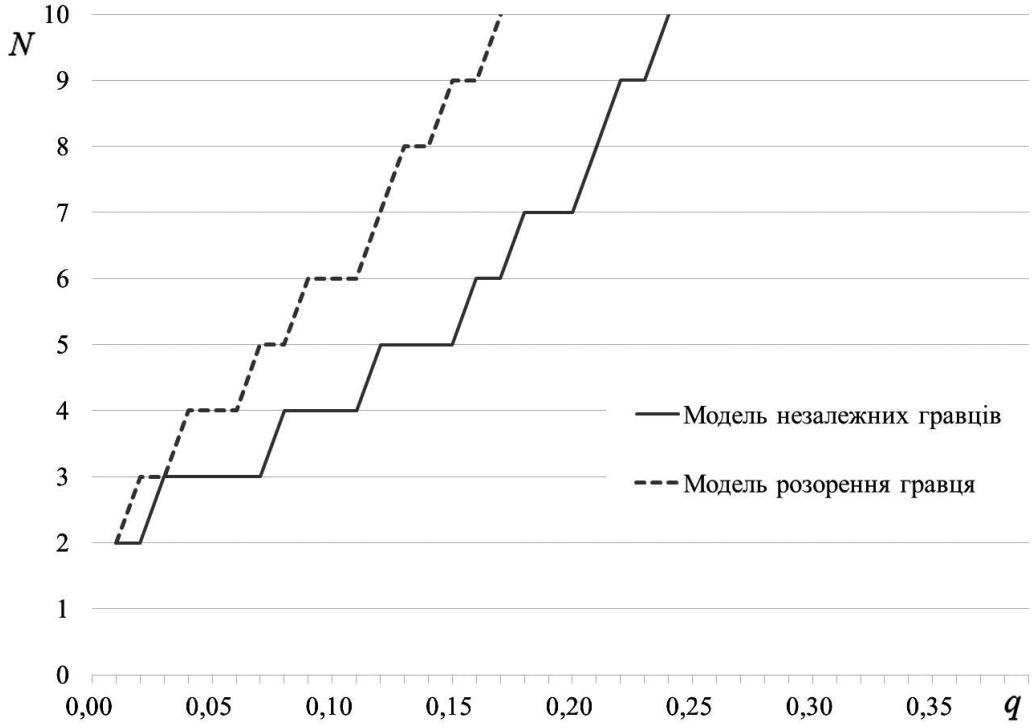


Рис. 3. Кількість підтверджень, необхідних для підтримки ймовірності успіху зловмисника на рівні, який не перевищує $P_S = 0,001$. Суцільна лінія відповідає моделі незалежних гравців, пунктирна – моделі розорення гравця

Так, якщо передбачається, що в розпорядженні зловмисника є 15 % від загальної потужності мережі, то необхідно два підтвердження, щоб зберегти ймовірність успіху зловмисника не вище 10 %, в той час, як для моделі розорення гравця необхідно очікувати три підтвердження. Якщо необхідна ймовірність успіху зловмисника не вище 1 % (при тих же умовах), необхідно очікувати чотири підтвердження, а для моделі розорення гравця – шість підтверджень. Якщо бажаємо забезпечити ймовірність успіху зловмисника не вище 0,1 %, необхідно очікувати п'ять підтверджень, а для моделі розорення гравця – дев'ять.

Таким чином, для вибраного прикладу необхідний середньостатистичний час, який витрачається на очікування підтвердження угод можна скоротити на $1/3$ (33 %) для $P_S = 10\%$; на $2/6$ (33 %) для $P_S = 1\%$ і на $4/9$ (44 %) для $P_S = 0{,}1\%$. В інших випадках з наведених результатів середньостатистичний час очікування може скоротитися і до двох разів (наприклад, при $P_S = 0{,}1$ и $q = 0{,}5 - 0{,}8; 0{,}19 - 2{,}0; 0{,}29$).

Висновки

На підставі моделі незалежних гравців отримано аналітичний вираз розрахунку ймовірності успішного проведення зловмисником атаки подвійної витрати на блокчейн-системи, що використовують алгоритм консенсусу Доказ виконаної роботи на основі геш-функції. Вираз отримано для випадку, коли передбачається, що зловмисник попередньо сформував один блок (для порівняння з раніш незалежно отриманими результатами). Отриманий вираз (1) характеризує ймовірність зловмисником провести успішну атаку подвійної витрати на блокчейн-систему у залежності від використовуваної кількості підтверджень, а також гешрейта чесною мережею і зловмисником. Наведено кількісні значення даної ймовірності.

На основі отриманих результатів наведено рекомендації щодо визначення «безпечної» кількості підтверджень для успішного протистояння атаки подвійної витрати на блокчейн-систему. Проведено порівняння з результатами, отриманими Мені Розенфельдом (які використовують модель розорення гравця). Показано, що можливо обмежитись меншою кількістю необхідних підтверджень в блокчейн-системі при тому ж рівні безпеки. Отримані результати на практиці дозволять значно (до двох разів) знизити час очікування для укладання угоди і, як наслідок, значно підвищити швидкість проведення операцій з блокчейн-системами при збереженні заданого рівня безпеки.

Список літератури:

1. Hackernoon: Two Ways to Double-Spend https://medium.com/hackernoon/bitcoin-core-bug-cve-2018-17144-an-analysis-f80d9d373362.
2. BitcoinCore: CVE-2018-17144 Full Disclosure https://bitcoincore.org/en/2018/09/20/notice/.
3. Hackernoon: Two Ways to Double-Spend https://medium.com/hackernoon/bitcoin-core-bug-cve-2018-17144-an-analysis-f80d9d373362.
4. Zaghloul, E., Li, T., Mutka, M.W., & Ren, J. (2019). Bitcoin and Blockchain: Security and Privacy. ArXiv, abs/1904.11435.
5. Rosenfeld M. Analysis of hashrate-based double-spending / Meni Rosenfeld, 2014. 13 c.
6. Gervais A., Ritzdorf H., Karame G. O., & Čapkun S. (2015). Tampering with the delivery of blocks and transactions in Bitcoin. In CCS 2015 – Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (Vol. 2015-October, pp. 692-705). Association for Computing Machinery. https://doi.org/10.1145/2810103.2813655.
7. Zaghloul E., Li T., Mutka M.W., & Ren J. (2019). Bitcoin and Blockchain: Security and Privacy. ArXiv, abs/1904.11435.

8. BitcoinWiki: Double-spending https://ru.bitcoinwiki.org/wiki/Double-spending
9. Ширяев А. Н. Вероятность : в 2-х кн. ; 4-е изд., перераб. и доп. Москва : МЦНМО, 2007.
10. Полуяненко Н.А., Кузнецов А.А. Моделирование атаки двойной траты на протокол консенсуса «proof of work» // Радиотехника. 2019. № 198. С. 146–161. DOI: 10.30837/rt.2019.3.198.11
11. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System / Satoshi Nakamoto, 2009. 9 с.

Харківський національний
університет імені В. Н. Каразіна;
АТ «Інститут інформаційних технологій»

Надійшла до редколегії 07.02.2020

МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ В КОМУНІКАЦІЙНИХ СИСТЕМАХ

UDC 621.391 **DOI:10.30837/rt.2020.1.200.14**

I.D. GORBENKO, Dr. Sci. (Technology), O.A ZAMULA, Dr. Sci. (Technology)

THEORETICAL BASIS OF SYNTHESIS OF COMPLEX SIGNAL QUASIORTOGONAL SYSTEMS

Introduction

In modern telecommunication systems and networks the task of providing the necessary indicators of noise immunity (noise immunity and secrecy functioning) at the level of the source of signals – physical carriers of information is traditionally solved on the basis of increasing the ratio of signal power to the power of interference at the reception of the receiving device, as well as improving the directivity of the antennas of the transmitter and receiver. Signal intensity or signal-to-noise ratio is a key parameter that determines the characteristics of any receiving task. However, the energy parameters of the system may be limited. Among the main directions for improving the noise immunity and secrecy of the telecommunications network one can identify the directions associated with the use of channels with high redundancy, high spatial, structural, energy and time secrecy. One of the ways to solve this problem is to use radio channels with frequency redundancy [1 – 4]. To provide this type of redundancy, discrete signals are now widely used at the physical level, in which manipulated parameters (amplitude, phase, frequency) are changed at strictly fixed time intervals. Rules for changing the parameter being manipulated are specified by discrete sequences, which completely determine the properties of the discrete signals and are often identified with them. That is why the attention of scientists has been focused on the analysis, synthesis and processing of discrete sequences.

In the systems of radar, sonar, navigation, communication and transmission of information the use of the discrete sequences for the formation of complex wideband and ultrawideband signals as manipulating sequences made it possible to resolve the contradiction between the throughput and range of the systems operation, to increase their noise immunity and electromagnetic compatibility, increase radio bandwidth efficiency use due to code division of channels, to improve the ecology in the radio coverage area by reducing the peak radiation power, create satellite-based radar, radio navigation and communication systems, providing for observation, determination of coordinates and transmission of information to any point on our planet, to implement hidden location and communication using noise-like signals and much more. Today a large number of the discrete sequences classes are known. All of them differ from each other by the rule and the coding power, the priority qualitative characteristic (sequences with perfect periodic autocorrelation function, orthogonal, quasi-orthogonal, trans-orthogonal, maximally trans-orthogonal, optimum in minimum-maximal, or in some other kind, noise-like sequences, periodic, impulse, regular, irregular impulse sequences, etc.); they differ in a number of essential parameters (characteristics): period (length), peak factor, degree of equilibrium, uncertainty function, autocorrelation, reciprocal and butt-correlation functions, etc.

The main results of the research

To date, there is no unified theory for the synthesis of discrete signal (DS) systems with predetermined auto-, mutually-, joint correlation properties. Moreover, it is not possible to answer the question: how signals with a large period close to optimal ones are known. Therefore, it is relevant to search for effective methods of the discrete signals (DS) search with the necessary (for certain applications) correlation, ensemble, statistical and structural properties. One such method is based on the use of iterative algorithms [5]. Relatively good in this sense signals can be obtained with the appropriate choice of the initial approximation and the use of integer optimization by the minimum

or medium degree criteria. However, the disadvantage of the iterative methods is the dependence on the initial approximation, a sharp increase in the search time of the signal as the signal period increases. Other methods include finding the necessary conditions for the existence of discrete sequences with the given parameters. It is known [6] that discrete sequences with a good aperiodic autocorrelation function (APFAC) can be found only among sequences with a good periodic autocorrelation function (PFAC). In the first stage, many sequences of candidates with good PFAC are formed. In the second stage, an exhaustive search is carried out for the criterion of the lowest level of the maximum of the side lobes of the APFAC among all cyclic shifts of one-period segments of the candidate sequences. The search result is a sequence with a minimum value of the APFAC side lobes. The method of the discrete sequences synthesis by homomorphic mapping of multiplicative groups of simple and extended Galois fields with k-valued character. Studies have shown that with the increase in the field characteristics and the number of classes, the amount of computations in the directional search is increasing dramatically [7]. Known methods of the discrete sequences synthesis with the given correlation functions are based usually on the operation of sorting multiple options to select the best result, and with a significant period of the discrete sequence application of such methods becomes problematic.

Let us formulate the problem of synthesis of one class of signals with given correlation, ensemble and structural properties. We will require that such signal systems have a "fuzziness" property in correlation properties. This property means that increase or decrease in the duration of the discrete signal does not change the correlation properties inherent in the output signal.

Under the problem of signal synthesis we will understand the task of constructing dictionaries (subsets) of vectors (signals) $(W_m^q), q=\overline{1,N},\ m=\overline{1,M},$ the whole set of which forms a system of uniform quasi-orthogonal signals (UQOS) of $M_k = N \times M_x$ dimension such that the following conditions are fulfilled in each of the dictionaries.

1. The mathematical model for the periodic autocorrelation function of each W_m^q of discrete signals (DSs) satisfies the system of nonlinear parametric inequalities (SNPI)

$$R_{a_1}^q(l) \le \sum_{i=1}^{L-1} W_i^q (W_{i+c}^q)^* \le R_{a_2}^q(l),\ l=\overline{1,L-1},\ q=\overline{1,N}, \tag{1}$$

where $R_{a_1}^q(l)$ and $R_{a_2}^q(l)$ are specified (such as required) values of the side lobes of the PFAC.

2. The mathematical model for the joint function of mutual correlation (JFMC) (W^q, W^p) of discrete signals (DSs) with joining words W^{qp} and W^{pq} satisfies a set of systems of nonlinear parametric inequalities:

$$\begin{aligned}
R_{b_{1,1}}^{qp}(l) &\le \sum_{i=0}^{L-K} W_i^q \times (W_{i+l}^p)^* + \sum_{i=L-K+1}^{L-1} W_i^q \times (W_{i-l+K}^p)^* \le R_{b_{2,1}}^{qp}(l);\\
R_{b_{1,2}}^{qp}(l) &\le \sum_{i=0}^{L-K} W_i^q \times (W_{i+l}^q)^* + \sum_{i=L-K+1}^{L-1} W_i^q \times (W_{i-l+K}^p)^* \le R_{b_{2,2}}^{qp}(l);\\
R_{b_{1,3}}^{qp}(l) &\le \sum_{i=0}^{L-K} W_i^q \times (W_{i+l}^p)^* + \sum_{i=L-K+1}^{L-1} W_i^q \times (W_{i-l+K}^q)^* \le R_{b_{2,3}}^{qp}(l);\\
R_{b_{1,4}}^{qp}(l) &\le \sum_{i=0}^{L-K} W_i^p \times (W_{i+l}^p)^* + \sum_{i=L-K+1}^{L-1} W_i^p \times (W_{i-l+K}^q)^* \le R_{b_{2,4}}^{qp}(l);\\
R_{b_{1,5}}^{qp}(l) &\le \sum_{i=0}^{L-K} W_i^p \times (W_{i+l}^q)^* + \sum_{i=L-K+1}^{L-1} W_i^p \times (W_{i-l+K}^p)^* \le R_{b_{2,5}}^{qp}(l);
\end{aligned} \tag{2}$$

moreover, $l=\overline{1,L-1},$ for various combinations q and p, $q=\overline{1,N},\ p=\overline{1,N},\ q \ne p,$ where $R_{b_{1,j}}^{qp}(l)$ and $R_{b_{2,j}}^{qp}(l)$ - are specified (required) PFMC (Periodic Function of Mutual Correlation) and JFMC (Joint Function of Mutual Correlation) implementation.

3. Studies show that significant difficulties in overcoming the hidden functioning of radio channels can be created by giving "fuzziness" properties to signals. Let us introduce the concept of fuzziness. Moreover, we first formulate the problem of synthesis of a single signal W^q having the fuzziness in cyclic convolution. Let us define the fuzziness interval Δx by duration

$$L - x_2 \le \Delta x \le L + x_1, \tag{3}$$

Considering that, in the general case $|x_1| \ne |x_2|, |x_1|, |x_2| < L$, the fuzziness interval Δy relative to the true values of the cyclic frequency in the form

$$L - y_2 \le \Delta y \le L + y_1 \ , \tag{4}$$

and $|y_1| \ne |y_2|, |y_1|, |y_2| < L$.

Let us assume that based on the processing of the signal flow either signal

$$W^{\vartheta}_{x_L} = W^{\vartheta}_{L-\delta} W^{\vartheta}_{L} W^{\vartheta}_{x_1 - L - \delta}, \tag{5}$$

or signal

$$W^{\vartheta}_{x_1} = W^{\vartheta}_{L-\delta} W^{\vartheta}_{X_1+\delta} \tag{6}$$

is accepted as true

with $\Delta x \ge L$, either signal

$$W^{\vartheta}_{x_2} = W^{\vartheta}_{L-X_2}, \tag{7}$$

or signal

$$W^{\vartheta}_{x_{21}} = W^{\vartheta}_{\delta} W^{\vartheta}_{L-x_2-\delta} \ , \tag{8}$$

with $\Delta x < L$, where indices x_1 i x_2, $\delta, L, x_1 + \delta - L, L - \delta, x_1 + \delta, \ L - x_2 - \delta$ indicate the number of characters of the truncated W^{ϑ} signal (the first or last, according to the arrangement of its characters $W^{\vartheta}_{X_1}$ or $W^{\vartheta}_{X_2}$). Then the fuzziness of the signals given by (5 – 8) is a set of systems of nonlinear parametric inequalities:

$$R_{a_1}(k) \le \sum_{i=\delta}^{L-K} W_i^{\vartheta} \left(W_{i+k}^{\vartheta}\right)^* + \sum_{i=L-k+1}^{L} W_i^{\vartheta} \left(W_{i-L+K}^{\vartheta}\right)^* + \sum_{i=1}^{L-K} W_i^{\vartheta} \left(W_{i+k}^{\vartheta}\right) + \sum_{i=L-k+1}^{L} W_i^{\vartheta} \left(W_{i-L+K}^{\vartheta}\right)^* +$$
$$+ \sum_{i=1}^{x_1 - L + \vartheta} W_i^{\vartheta} \left(W_{i+k}^{\vartheta}\right)^* \le R'_{a_2}(k); \ k = \overline{0, L + x_2}, \qquad \text{a)}$$

$$R_{a_1}(k) \le \sum_{i=\delta}^{L-K} W_i^{\vartheta} \left(W_{i+k}^{\vartheta}\right)^* + \sum_{i=L-k+1}^{L} W_i^{\vartheta} \left(W_{i-L+K}^{\vartheta}\right)^* + \sum_{i=1}^{L-K} W_i^{\vartheta} \left(W_{i+k}^{\vartheta}\right) + \sum_{i=L-k+1}^{L} W_i^{\vartheta} \left(W_{i-L+K}^{\vartheta}\right)^* \le R'_{a_2}(k); \qquad \text{b)}$$

$$R_{a_2}(k) \le \sum_{i=1}^{L-x_1} W_i^{\vartheta} \left(W_{i-k}^{\vartheta}\right)^* \le R'_{a_2}(k), k = \overline{0, L - x_2}, \qquad \text{c)}$$

$$R_{a_1}(k) \le \sum_{i=L-\delta}^{L-K} W_i^{\vartheta} \left(W_{i+k}^{\vartheta}\right)^* + \sum_{i=L-k+1}^{L} W_i^{\vartheta} \left(W_{i-L+K}^{\vartheta}\right)^* + \sum_{i=1}^{L-x_2+\vartheta} W_i^{\vartheta} \left(W_{i+k}^{\vartheta}\right)^* \le R'_{a_2}(k); \ k = \overline{0, L - x_2}, \text{d)} \tag{9}$$

where $R'_{a_1}(k)$ and $R'_{a_2}(k)$ – are various implementations of the PFAC that are specified in the synthesis of signals. In the case of "fuzziness" in the duration of sequences of characters in the interval Δx, which is defined as:

$$L - x_2 \le \Delta x \le L + x_1,$$

the mathematical model of fuzziness can be specified by a set of nonlinear inequality systems:

$$R_{b_1}^{'}(k) \le \sum_{i=\delta}^{L-K} W_i^q \left(W_{i+k}^{\vartheta_1}\right)^* + \sum_{i=L-k+1}^{L} W_i^q \left(W_{i-L+K}^{\vartheta_2}\right)^* +$$
$$+\sum_{L=1}^{L-K} W_i^p \times \left(W_{L+k}^{\vartheta_2}\right)^* + \sum_{i=L-K+1}^{L} W_i^p \left(W_{i-L+K}^{\vartheta_3}\right)^* + \quad \text{a)}$$
$$+\sum_{i=1}^{L-K} W_i^r \times \left(W_{i+K}^{\vartheta_3}\right)^* \le R_{b_2}^{'}(k);\ k = \overline{0, L+x},$$

$$R_{b_1}^{'}(k) \le \sum_{i=\delta}^{L-K} W_i^q \left(W_{i+k}^{\vartheta_1}\right)^* + \sum_{i=L-k+1}^{L} W_i^q \left(W_{i-L+K}^{\vartheta_2}\right)^* +$$
$$+\sum_{L=1}^{L-K} W_i^p \times \left(W_{L+k}^{\vartheta_2}\right)^* + \sum_{i=L-K+1}^{L} W_i^p \left(W_{i-L+K}^{\vartheta_3}\right)^* \le R_{b_2}^{'}(k); \quad \text{b)}$$
$$k = \overline{0, L+x},$$

$$R_{b_2}^{'}(k) \le \sum_{i=L-\delta}^{L-K} W_i^q * (W_i^{\vartheta_1} + k)^* \le R_{b_2}(k), k = \overline{0, L-x_{2,}} \quad \text{c)}$$

$$R_{b_1}^{'}(k) \le \sum_{i=L-\delta}^{L-K} W_i^q \left(W_{i+k}^{\vartheta_2}\right)^* + \sum_{i=L-k+1}^{L} W_i^q \left(W_{i-L+K}^{\delta_2}\right)^* +$$
$$+ \sum_{i=1}^{L-x_2+\delta} W_i^p \left(W_{i+k}^{\vartheta_2}\right)^* \le R_{b_2}^{'}(k); k = \overline{0, L-x_2}, \quad \text{d) (10)}$$

Thus, the condition that must be fulfilled for the signals W_m^q synthesized system can be formulated as follows: the dictionary $\{W_m^q\}$ satisfies the set of systems of nonlinear parametric inequalities (9) – (10), i.e. the dictionary $\{W_m^q\}$ has in intervals Δx and Δy a blur in duration and cycle frequency.

4. In each of the M dictionaries there are signals $W_{m_1}^{q_1}$ and $W_{m2}^{q_2}$, auto – and mutual convolution of which will satisfy the set of inequalities of the form (1) and (2);

5. The law of signal W_m^q formation has perfect structural secrecy.

6. The mathematical model for the normalized APFAC of signal W_m^q satisfies the system of nonlinear inequalities

$$r_{a_1}^q(l) \le \sum_{i=1}^{L-m} W_i^q \left(W_{i+1}^q\right)^* \le r_{a_2}^q(l); \quad (11)$$
$$l = \overline{1, L},\ \ m = \overline{1, L},$$

where $r_{a_1}^q(l)$ and $r_{a_2}^q(l)$ – are the specified implementations of the APFAC.

7.The mathematical model for the aperiodic function of mutual correlation (APFMC) satisfies two systems of nonlinear parametric inequalities

$$r_{b_{1,1}}^{qp}(l) \le \frac{1}{L-m} \sum_{i=0}^{L-m} W_i^q \left(W_{i+1}^q\right)^* \le r_{b_{1,2}}^{qp}(l);$$
$$l = \overline{1, L}, m = \overline{1, L},$$
$$r_{b_{2,1}}^{qp}(l) \le \frac{1}{L-m} \sum_{i=0}^{L-m} W_i^p \left(W_{i+1}^q\right)^* \le r_{b_{2,2}}^{pq}(l); \quad (12)$$
$$l = \overline{1, L}, m = \overline{1, L},$$

8. The objective function

$$Int(E) = \sum_{j=1}^{n} C_j S_j \tag{13}$$

belongs to the interval (A, B), where S_j – is the value of the implementation of the functions of the information transmission system, describing the laws of distribution of values of aperiodic and periodic correlation functions, which determine the structural secrecy of signals, algorithms for the construction of the discrete signals (DSs), etc and C_j – are the penalties corresponding to them.

Let us formulate the problem of the signal system synthesis, taking into account the main difference from the signal system considered earlier: the durations of some (all) vectors (signals) W^q in each of the dictionaries differ from the average duration L_{cp} by $\pm\Delta L$ value. Let such a system is termed the system of non-uniform quasi-orthogonal signals (NUQOS).

Let the source of the DS Q_m give L_j-valued with maximum entropy $H(Q_m = \log p^{L_{cp}})$ sequence such that for some or all signals the condition: $L_i \neq L_j$, $i, j = \overline{1, N}$, $i \neq j$), is fulfilled, then under the problem of synthesis of the NUQOS systems we will understand the problem of constructing dictionaries (subsets) of vectors $\{W_m^q\}$, $q = \overline{1, H}, m = \overline{1, M}$, the totality of which forms the NUQOS system of signals that meet these conditions.

1. The mathematical model for the periodic autocorrelation function of each W_m^q of the DS satisfies the system of nonlinear parametric inequalities of the form (1).

2. The conditions (11 – 12) are true.

3. The mathematical model for mutual convolution or joint function of mutual correlation (JFMC) of the DS $W^q(W^p)$ with joint dictionaries $W^{pp}(W^{qq}), W^{qp}, W^{pq}$, provided that $L_q < L_p$ satisfies the set of systems of nonlinear parametric inequalities:

$$\begin{cases} R_{b_{1,1}}(0) \le W_1^q W_1^p + W_2^q W_2^p + \ldots + W_\delta^q W_\delta^p + \ldots + & W_{Lq}^q W_{Lq}^p \le R_{b_{2,1}}(0), a) \\ R_{b_{1,1}}(1) \le W_1^q W_2^p + W_2^q W_3^p + \ldots + W_\delta^q W_{\delta+1}^p + \ldots + & W_{Lq}^q W_{Lq+1}^p \le R_{b_{2,1}}(1), б) \\ R_{b_{1,1}}(2) \le W_1^q W_3^p + W_2^q W_4^p + \ldots + W_\delta^q W_{\delta+2}^p + \ldots + & W_{Lq}^q W_{Lq+2}^p \le R_{b_{2,1}}(2), в) \\ R_{b_{1,1}}(\xi) \le W_1^q W_{\xi+1}^p + W_2^q W_{\xi+2}^p + \ldots + W_\delta^q W_{\xi+\delta}^p + \ldots + & W_{Lq}^q W_\xi^p \le R_{b_{2,1}}(\xi), г) \\ R_{b_{1,1}}(Lp) \le W_1^q W_{Lp}^p + W_2^q W_1^p + \ldots + W_\delta^q W_{\xi-1}^p + \ldots + & W_{Lq}^q W_{Lp-1}^p \le R_{b_{2,1}}(Lp), д) \end{cases} \tag{14}$$

$$\begin{cases} R_{b_{2,1}}(1) \le W_1^q W_2^q + W_2^q W_3^q + \ldots + W_\delta^q W_{\delta+1}^p + \ldots + & + W_{Lq}^q W_1^p \le R_{b_{2,2}}(1), a) \\ R_{b_{1,2}}(2) \le W_1^q W_3^q + W_2^q W_4^q + \ldots + W_\delta^q W_{\delta+2}^p + \ldots + & + W_{Lq}^q W_2^p \le R_{b_{2,2}}(2), б) \\ R_{b_{1,2}}(3) \le W_1^q W_4^q + W_2^q W_5^p + \ldots + W_\delta^q W_{\delta+3}^q + \ldots + & + W_{Lq}^q W_3^p \le R_{b_{2,2}}(3), в) \\ R_{b_{1,2}}(\xi) \le W_1^q W_{\xi+1}^p + W_2^q W_{\xi+2}^p + \ldots + W_\delta^q W_{\xi+\delta}^p + \ldots + & + W_{Lq}^q W_\xi^p \le R_{b_{2,2}}(\xi), г) \\ \ldots. & \ldots. \\ R_{b_{1,2}}(Lq-1) \le W_1^q W_{Lp}^p + W_2^q W_1^p + \ldots + W_\delta^q W_{\delta-1}^p + \ldots + & + W_{Lq}^q W_{Lq-1}^p \le R_{b_{2,2}}(Lq-1), д) \end{cases} \tag{15}$$

$$R_{b_{1,3}}(0) \le W_1^q W_1^p + W_2^q W_2^p + \ldots + W_\delta^q W_\delta^p + \ldots + W_{Lq}^q W_{Lq}^p \le R_{b_{2,3}}(0),$$

$$R_{b_{1,3}}(1) \le W_1^q W_2^p + W_2^q W_3^p + \ldots + W_\delta^q W_{\delta+1}^p + \ldots + W_{Lq}^q W_{Lq+1}^p \le R_{b_{2,3}}(1),$$

$$R_{b_{1,3}}(Lp-Lq+1) \le W_1^q W_{Lp-Lq+2}^p + W_2^q W_{Lp-Lq+3}^p + \ldots + W_\delta^q W_{Lp-Lq+\delta-1}^p + \ldots + W_{Lq}^q W_1^q \le R_{b_{2,3}}(Lp-Lq+1),$$

$$R_{b_{1,3}}(Lp) \le W_1^q W_{Lp}^p + W_2^q W_1^p + \ldots + W_p^q W_{\delta-1}^p + \ldots + W_{Lq}^q W_{Lq-1}^q \le R_{b_{2,3}}(Lp),$$

$$R_{b_{1,3}}(Lp) \le W_1^q W_{Lp}^p + W_2^q W_1^p + \ldots + W_p^q W_{\delta-1}^p + \ldots + W_{Lq}^q W_{Lq-1}^q \le R_{b_{2,3}}(Lp),$$

for all kinds of combinations q and p, where $q, p = \overline{1, N}$, $q \neq p$ and where $R_{b_{1,1}}(l), R_{b_{1,2}}(l), R_{b_{1,3}}(l), R_{b_{2,1}}(l), R_{b_{2,2}}(l),$ and $R_{b_{2,3}}(l),$ – are the values of the PFMC and JFMC implementations.

4. Conditions (14) and (15) are satisfied for aperiodic auto – and mutual correlations for all W^q, $q = \overline{1, N}$ and any combination of the DS W^q and W^p, $q, p = \overline{1, N}, q \neq p$, the objective function (14) fits the interval (A, B).

We emphasize that the stated formulation of problems of the NUQOSs synthesis is more general than the formulation of the uniform quasi-orthogonal signals (UQOS) synthesis tasks. Both the formulation of the problem of synthesis of UQOS (UNQOS) signal systems and the proposed approach are new. Therefore, obtaining even partial solutions makes it possible to move further towards solving the problems of synthesis of the discrete signals (DS) with the specified correlation, ensemble and structural properties.

It is shown in [8] that the improvement of the ensemble, structural and correlation properties of the DS in case of insignificant complication of algorithms and devices of their formation, can be achieved based on the use of the so-called compound signals (CS). Thus components will be called signal systems for two reasons. First, the law of formation of complex elements in a composite signal may change, and secondly, complex elements forming the CS have identical (close) auto – and mutually correlating properties, so their mutual combination does not lead to deterioration of correlation properties and, at the same time, makes it possible to improve the ensemble properties, to increase the structural secrecy and to implement the mode of change of correspondence: m bits of the message – 2^m CS, without much complication of mechanisms of formation and processing of such signals.

Let us formulate the problem of synthesis of compound quasi-orthogonal signals (CQOS). Let the DS source form the UQOS or NUQOS systems each with the volume N_j. For such signal systems, conditions (1) – (2), (11) – (12), and (14) – (15) are satisfied. Then, by the task of building the CQOS system, we will understand the procedure of combining compound elements, which are UQOS or NUQOS. In this case, each CQOS contains 2^m CS and the following conditions are fulfilled:

1. The objective function of the form (13) for a given (pre-selected) penalty matrix belongs to the interval (A_C, B_C);

2. Auto – and mutual CQOS convolutions $W_i^{q_c}$ (PFAC, PFMC) in terms of maximum permissible lateral emissions and dispersion σ_R do not depend on the configuration type of the CS formation.

3. The law of all 2^m CS formation changes in each of the constituent elements.

In this formulation, the task of constructing compound quasi-orthogonal signals is reduced to a step-by-step solution of the problems of synthesis of the UQOS or NUQOS signal systems.

The conducted analysis showed that the solution of the problems of synthesis of the UQOSs, NUQOSs and CQOSs signal systems is primarily related to the study of the algebraic structure of systems of nonlinear parametric inequalities (1) – (2), (11) – (12), the development of approaches and theoretical basis for their solution.

Let us first consider the theoretical basis for the synthesis of two UQOSs signals x^p and x^q, without imposing restrictions on the blur of the form (10) and (11), and then make a series of generalizations to the synthesis case of N discrete signals, which also have blurred properties. At the same time, we will require that the UQOS signals have perfect structural properties, that is, such

structural secrecy that during the interception and element-wise processing of any number of l symbols of UQOS signals, one cannot unambiguously predict the type of $L-l$ remaining symbols. This can be done if the symbols in the UQOS signals are independent and appear with equal probability.

Taking into account the systems of the form (1) – (2), for the case of synthesis of two discrete signals, the set of systems of nonlinear inequalities has the form:

$$\xi^1 a_1(l) \le \sum_{i=1}^{L} x_i^q \times (x_{i+l}^q)^* \le \xi^1 a_2(l),\ l = \overline{0, L-1} \qquad \text{a)}$$

$$\xi^2 a_1(l) \le \sum_{i=1}^{L-K} x_i^p \times (x_{i+l}^p)^* \le \xi^2 a_2(l),\ l = \overline{0, L-1} \qquad \text{b)}$$

$$\xi^1 b_1(l) \le \sum_{i=0}^{L-K} x_i^q \times (x_{i+l}^p)^* + \sum_{i=L-K+1}^{L-K} x_i^q \times (x_{i-L+K}^p)^* \le \xi^1 b_2(l),\ l = \overline{0, L-1} \qquad \text{c)}$$

$$\xi^2 b_1(l) \le \sum_{i=0}^{L-K} x_i^p \times (x_{i+l}^p)^* + \sum_{i=L-K+1}^{L-1} x_i^p \times (x_{i-L+K}^p)^* \le \xi^2 b_2(l),\ l = \overline{0, L-1} \qquad \text{d)}$$

$$\xi^3 b_1(l) \le \sum_{i=0}^{L-K} x_i^q \times (x_{i+l}^q)^* + \sum_{i=L-K+1}^{L-1} x_i^q \times (x_{i-L+K}^p)^* \le \xi^3 b_2(l),\ l = \overline{0, L-1} \qquad \text{e)} \qquad (16)$$

$$\xi^4 b_1(l) \le \sum_{i=0}^{L-K} x_i^q \times (x_{i+l}^p)^* + \sum_{i=L-K+1}^{L-1} x_i^p \times (x_{i-L+K}^p)^* \le \xi^4 b_2(l),\ l = \overline{0, L-1} \qquad \text{f)}$$

$$\xi^5 b_1(l) \le \sum_{i=0}^{L-K} x_i^p \times (x_{i+l}^p)^* + \sum_{i=L-K+1}^{L-1} x_i^p \times (x_{i-L+K}^q)^* \le \xi^5 b_2(l),\ l = \overline{0, L-1} \qquad \text{g)}$$

$$\xi^6 b_1(l) \le \sum_{i=0}^{L-K} x_i^p \times (x_{i+p}^q)^* + \sum_{i=L-K+1}^{L-1} x_i^p \times (x_{i-L+K}^p)^* \le \xi^6 b_2(l),\ l = \overline{0, L-1}. \qquad \text{h)}$$

The algebraic structure of systems (16) is established by the statements below.

Statement 1. The real or complex sequence of L – symbols X^δ, whose values of a commutative auto convolution are limited by functions $\xi a_1^i(l)$ and $\xi a_2^i(l), i = \overline{1,2}$, $l = \overline{1, L-1}$, has $L/2-1$ degrees of freedom in the case if L even and $L-1/2$ degrees of freedom in the case if L is odd. By the number of degrees of freedom we will mean the number of nonlinear inequalities that coincide with each other in the commutativity of convolution operations.

Statement 2. In systems of inequalities (16a) and (16b) for even L, $l = 1, L/2$, and for odd L,- $l = \overline{1, \frac{L+1}{2}}$. That is, this statement answers the question: how many inequalities in (16) coincide. From the statement it follows that the presence of the specified number of degrees of freedom determines the multiplicity of the solutions of system (16a) and (16b).

Statement 3. A mutual commutative convolution X^q with a cyclic sequence X^p extension, symbols that are defined by $\bmod L$, up to the number of the mutual convolution element W^p, coincides with a cyclic elongated sequence X^q whose symbols are defined by $\bmod L$.

It follows from Statement 3 that the systems (16c) and (16g) coincide, and the bilinear forms included in them differ only in the order of their location in the systems. Therefore, one of (16c) or (16g) systems is excessive.

Statement 4. Various bilinear forms obtained by calculating the time convolution of a sequence X^q with component sequences $X^qX^p(X^pX^q)$ or sequence X^p with component sequences $X^qX^p(X^pX^q)$ are different.

Statement 4 makes it possible to find out the algebraic structure of systems of nonlinear inequalities (16c), (16f), (16g), (16h). From Statement 4 it follows that in systems (16e) and (16h) all nonlinear inequalities are different and there is no redundancy.

Statement 5. Various bilinear forms that are included in the system of nonlinear inequalities (16e), (16a), for $l=0$, are different.

In the above statement, the task of synthesizing the vocabularies of one class of signals is the most generalized one, since it sets out the task of synthesizing signal systems with given correlation properties, formation laws, structural and ensemble properties. In particular, in our view, it is necessary to study the algebraic structure of systems of non-linear parametric inequalities of the form (16).

It is known that, to date, there is no mathematical apparatus for solving the second-order system of nonlinear parametric inequalities (SNPI). The only mathematical apparatus used to solve this problem is the apparatus of the theory of operations research, in particular, methods of nonlinear, dynamic and scholastic integer programming. Indeed, the set of systems of nonlinear inequalities (16) are functions of the consumption of permissible resources.

Analysis of possible solutions to the problem of synthesis of the UQOS signals shows that they must relate to tasks such as "packing a backpack", the procedure of repetition of the solution for which requires considerable and, in some conditions, endless resources. With this in mind, let us formulate more rigorously the problem of synthesis of the UQOS signal systems with blurred properties using the language of the operations research. To do this, let's go to the objective function E_j with the appropriate values of penalties C_j. Then the problem of synthesis of the UQOS signals in the language of the theory of operations research is the task of ensuring the interval value of the objective function

$$\text{int}(E)=\sum_{j=1}^{n}C_jS_j \tag{17}$$

subject to the limitations (without blurring). Aanalytical expressions for determining constraints of the objective function (17) are as follows:

$$\begin{cases} \xi^1_{a_1}(l)\le\sum\limits_{i=1}^{L}x^1_i\times(x^1_{i+l})^*\le\xi^1_{a_2}(l),\ l=\overline{0,L'} \\ \xi^2_{a_1}(l)\le\sum\limits_{i=1}^{L}x^2_i\times(x^2_{i+l})^*\le\xi^2_{a_2}(l),\ L'=\dfrac{L-1}{2},\ \textit{if L is odd} \\ \qquad\qquad\cdots \\ \xi^j_{a_1}(l)\le\sum\limits_{i=1}^{L}x^j_i\times(x^j_{i+l})^*\le\xi^j_{a_2}(l),\ L'=\dfrac{L}{2},\ \textit{if L is even} \\ \xi^N_{a_1}(l)\le\sum\limits_{i=1}^{L}x^N_i\times(x^N_{i+l})^*\le\xi^N_{a_2}(l). \end{cases} \tag{18}$$

$$\begin{cases} \xi_{b_1}^1(l) \le \sum\limits_{i=1}^{L} x_i^1 \times (x_{i+l}^2)^* + \sum\limits_{i=L-k+1}^{L} x_i^1 \times (x_{i-L+k}^2)^* \le \xi_{b_2}^1(l); \\ \xi_{b_1}^1(l) \le \sum\limits_{i=1}^{L-k} x_i^1 \times (x_{i+l}^3)^* + \sum\limits_{i=L-k+1}^{L} x_i^1 \times (x_{i-L+k}^3)^* \le \xi_{b_2}^2(l); \\ \cdots \\ \xi_{b_1}^1(l) \le \sum\limits_{i=1}^{L-k} x_i^1 \times (x_{i+l}^j)^* + \sum\limits_{i=L-k+1}^{L} x_i^1 \times (x_{i-L+k}^j)^* \le \xi_{b_2}^j(l); \\ \cdots \\ \xi_{b_1}^1(l) \le \sum\limits_{i=1}^{L-k} x_i^1 \times (x_{i+l}^N)^* + \sum\limits_{i=L-k+1}^{L} x_i^1 \times (x_{i-L+k}^N)^* \le \xi_{b_2}^N(l). \end{cases} \quad l = \overline{0, L-1}. \tag{19}$$

$$\begin{cases} \xi_{b_1}^2(l) \le \sum\limits_{i=1}^{L-k} x_i^2 \times (x_{i+l}^3)^* + \sum\limits_{i=L-k+1}^{L} x_i^2 \times (x_{i-L+k}^3)^* \le \xi_{b_2}^2(l); \\ \xi_{b_1}^3(l) \le \sum\limits_{i=1}^{L-k} x_i^2 \times (x_{i+l}^4)^* + \sum\limits_{i=L-k+1}^{L} x_i^2 \times (x_{i-L+k}^4)^* \le \xi_{b_2}^3(l); \\ \cdots \\ \xi_{b_1}^{j+1}(l) \le \sum\limits_{i=1}^{L-k} x_i^2 \times (x_{i+l}^{j+1})^* + \sum\limits_{i=L-k+1}^{L} x_i^2 \times (x_{i-L+k}^{j+1})^* \le \xi_{b_2}^{j+1}(l); \\ \cdots \\ \xi_{b_1}^N(l) \le \sum\limits_{i=1}^{L-k} x_i^2 \times (x_{i+l}^N)^* + \sum\limits_{i=L-k+1}^{L} x_i^2 \times (x_{i-L+k}^N)^* \le \xi_{b_2}^N(l). \end{cases} \quad l = \overline{0, L-1}. \tag{20}$$

$$\begin{cases} \xi_{b_1}^{\upsilon}(l) \le \sum\limits_{i=1}^{L-k} x_i^{\upsilon} \times (x_{i+l}^{\upsilon+1})^* + \sum\limits_{i=L-k+1}^{L} x_i^{\upsilon} \times (x_{i-L+k}^{\upsilon+1})^* \le \xi_{b_2}^{\upsilon}(l); \\ \xi_{b_1}^{\upsilon+1}(l) \le \sum\limits_{i=1}^{L-k} x_i^{\upsilon} \times (x_{i+l}^{\upsilon+2})^* + \sum\limits_{i=L-k+1}^{L} x_i^{\upsilon} \times (x_{i-L+k}^{\upsilon+2})^* \le \xi_{b_2}^{\upsilon+1}(l); \\ \cdots \\ \xi_{b_1}^{m}(l) \le \sum\limits_{i=1}^{L-k} x_i^{\upsilon} \times (x_{i+l}^{\upsilon+m})^* + \sum\limits_{i=L-k+1}^{L} x_i^{\upsilon} \times (x_{i-L+k}^{\upsilon+m})^* \le \xi_{b_2}^{m}(l); \\ \cdots \\ \xi_{b_1}^N(l) \le \sum\limits_{i=1}^{L-k} x_i^{\upsilon} \times (x_{i+l}^N)^* + \sum\limits_{i=L-k+1}^{L} x_i^{\upsilon} \times (x_{i-L+k}^N)^* \le \xi_{b_2}^N(l). \end{cases} \quad l = \overline{0, L-1}. \tag{21}$$

$$\begin{cases} \xi_{b_1}^1(l) \le \sum\limits_{i=1}^{L-k} x_i^{N-2} \times (x_{i+l}^{N-1})^* + \sum\limits_{i=L-k+1}^{L} x_i^{N-2} \times (x_{i-L+k}^{N-1})^* \le \xi_{b_2}^1(l); \\ \xi_{b_1}^2(l) \le \sum\limits_{i=1}^{L-k} x_i^{N-2} \times (x_{i+l}^N)^* + \sum\limits_{i=L-k+1}^{L} x_i^{N-2} \times (x_{i-L+k}^N)^* \le \xi_{b_2}^2(l); \\ \xi_{b_1}^1(l) \le \sum\limits_{i=1}^{L-k} x_i^{N-1} \times (x_{i+l}^N)^* + \sum\limits_{i=L-k+1}^{L} x_i^{N-1} \times (x_{i-L+k}^N)^* \le \xi_{b_2}^1(l). \end{cases} \quad l = \overline{1, L-1}. \tag{22}$$

$$\begin{cases} \xi_{b_1}^1(l) \le \sum\limits_{i=1}^{L} x_i^1 \times (x_{i+l}^1)^* + \sum\limits_{i=L-k+1}^{L} x_i^1 \times (x_{i-L+k}^1)^* \le \xi_{b_2}^1(l); \\ \xi_{b_1}^2(l) \le \sum\limits_{i=1}^{L-k} x_i^1 \times (x_{i+l}^2)^* + \sum\limits_{i=L-k+1}^{L} x_i^1 \times (x_{i-L+k}^2)^* \le \xi_{b_2}^2(l); \\ \cdots \\ \xi_{b_1}^3(l) \le \sum\limits_{i=1}^{L-k} x_i^2 \times (x_{i+l}^2)^* + \sum\limits_{i=L-k+1}^{L} x_i^2 \times (x_{i-L+k}^2)^* \le \xi_{b_2}^3(l); \\ \cdots \\ \xi_{b_1}^4(l) \le \sum\limits_{i=1}^{L-k} x_i^2 \times (x_{i+l}^1)^* + \sum\limits_{i=L-k+1}^{L} x_i^2 \times (x_{i-L+k}^1)^* \le \xi_{b_2}^4(l). \end{cases} \quad (23)$$

$$\begin{cases} \xi_{b_1}^1(l) \le \sum\limits_{i=1}^{L} x_i^1 \times (x_{i+l}^1)^* + \sum\limits_{i=L-k+1}^{L} x_i^1 \times (x_{i-L+k}^j)^* \le \xi_{b_2}^1(l); \\ \xi_{b_1}^2(l) \le \sum\limits_{i=1}^{L-k} x_i^1 \times (x_{i+l}^j)^* + \sum\limits_{i=L-k+1}^{L} x_i^1 \times (x_{i-L+k}^1)^* \le \xi_{b_2}^2(l); \\ \cdots \\ \xi_{b_1}^3(l) \le \sum\limits_{i=1}^{L-k} x_i^j \times (x_{i+l}^j)^* + \sum\limits_{i=L-k+1}^{L} x_i^j \times (x_{i-L+k}^1)^* \le \xi_{b_2}^3(l); \\ \cdots \\ \xi_{b_1}^4(l) \le \sum\limits_{i=1}^{L-k} x_i^j \times (x_{i+l}^1)^* + \sum\limits_{i=L-k+1}^{L} x_i^j \times (x_{i-L+k}^j)^* \le \xi_{b_2}^4(l). \end{cases} \quad (24)$$

$$\begin{cases} \xi_{b_1}^1(l) \le \sum\limits_{i=1}^{L} x_i^1 \times (x_{i+l}^1)^* + \sum\limits_{i=L-k+1}^{L} x_i^1 \times (x_{i-L+k}^N)^* \le \xi_{b_2}^1(l); \\ \xi_{b_1}^2(l) \le \sum\limits_{i=1}^{L-k} x_i^1 \times (x_{i+l}^N)^* + \sum\limits_{i=L-k+1}^{L} x_i^1 \times (x_{i-L+k}^1)^* \le \xi_{b_2}^2(l); \\ \cdots \\ \xi_{b_1}^3(l) \le \sum\limits_{i=1}^{L-k} x_i^N \times (x_{i+l}^N)^* + \sum\limits_{i=L-k+1}^{L} x_i^N \times (x_{i-L+k}^1)^* \le \xi_{b_2}^3(l); \\ \cdots \\ \xi_{b_1}^4(l) \le \sum\limits_{i=1}^{L-k} x_i^N \times (x_{i+l}^1)^* + \sum\limits_{i=L-k+1}^{L} x_i^N \times (x_{i-L+k}^N)^* \le \xi_{b_2}^4(l). \end{cases} \quad (25)$$

$$A_{2,j},\ j = \overline{j, N}; l = \overline{1, L-1}; \quad (26)$$

$$A_{3,j},\ j = \overline{4, N}; l = \overline{1, L-1}; \quad (27)$$

$$A_{\upsilon,j},\ j = \overline{\upsilon+1, N}; l = \overline{1, L-1}; \quad (28)$$

$$\begin{cases} \xi^1_{b_1}(l) \le \sum\limits_{i=1}^{L} x_i^{N-1} \times (x_{i+l}^{N-1})^* + \sum\limits_{i=L-k+1}^{L} x_i^{N-1} \times (x_{i-L+k}^{N})^* \le \xi^1_{b_2}(l); \\ \xi^2_{b_1}(l) \le \sum\limits_{i=1}^{L-k} x_i^{N-1} \times (x_{i+l}^{N})^* + \sum\limits_{i=L-k+1}^{L} x_i^{N-1} \times (x_{i-L+k}^{N-1})^* \le \xi^2_{b_2}(l); \\ \quad \cdots \\ \xi^3_{b_1}(l) \le \sum\limits_{i=1}^{L-k} x_i^{N} \times (x_{i+l}^{N-1})^* + \sum\limits_{i=L-k+1}^{L} x_i^{N} \times (x_{i-L+k}^{N-1})^* \le \xi^3_{b_2}(l); \\ \quad \cdots \\ \xi^4_{b_1}(l) \le \sum\limits_{i=1}^{L-k} x_i^{N} \times (x_{i+l}^{N-1})^* + \sum\limits_{i=L-k+1}^{L} x_i^{N} \times (x_{i-L+k}^{N})^* \le \xi^4_{b_2}(l). \end{cases} \quad (29)$$

Ensuring the interval value of the objective function (17) and the restrictions associated with x_1, x_2, y_1 and y_2 fuzziness:

$$\xi^1_{b_1}(k) \le \sum_{i=\delta}^{L-k} x_i^q \times (x_{i+k}^{\nu_1})^* + \sum_{i=L-k+1}^{L} x_i^q \times (x_{i-L+k}^{\nu_2})^* + \sum_{i=1}^{L-k} x_i^p \times (x_{i+k}^{\nu_2}) + \\ + \sum_{i=L-k+1}^{L} x_i^p \times (x_{i-L+k}^{\nu_3})^* + \sum_{i=L-k+1}^{L-k} x_i^r \times (x_{i-L+k}^{\nu_3})^* \le \xi^1_{b_2}(k), k = \overline{1, L + x_1}; \quad \text{a) (30)}$$

$$\xi^2_{b_1}(k) \le \sum_{i=\delta}^{L-k} x_i^q \times (x_{i+k}^{\nu_1})^* + \sum_{i=L-k+1}^{L} x_i^q \times (x_{i-L+k}^{\nu_2})^* + \sum_{i=1}^{L-k} x_i^p \times (x_{i+k}^{\nu_2}) + \\ + \sum_{i=L-k+1}^{L} x_i^p \times (x_{i-L+k}^{\nu_3})^* \le \xi^2_{b_2}(k), k = \overline{0, L + x_2}; \quad \text{b)}$$

$$\xi^3_{b_1}(k) \le \sum_{i=L-\delta}^{L-k} x_i^q \times (x_{i+k}^{\nu_1}) \le \xi^3_{b_2}(k), k = \overline{0, L - x_2}; \quad \text{c)}$$

$$\xi^4_{b_1}(k) \le \sum_{i=L-\delta}^{L-k} x_i^q \times (x_{i+k}^{\nu_1}) + \sum_{i=L-k+1}^{L} x_i^q \times (x_{i-L+k}^{\nu_2})^* + \sum_{i=1}^{L-x_2-\delta} x_i^p \times (x_{i+k}^{\nu_2}) \le \xi^2_{b_2}(k), k = \overline{0, L + x_2}; \quad \text{d)}$$

Moreover (30) is a collection of systems whose number is determined by all possible combinations of indices in the joint words $x_{x_1}^{qp}$, $x_{x_2}^{qp}$, $x_{x_2}^{q}$, $x_{x_2}^{p}$ and $x_{x_1}^{\upsilon_1\upsilon_2\upsilon_3}$, $x_{x_1}^{\upsilon_1\upsilon_2\upsilon_3}$, $x_{x_2}^{\upsilon_1}$ and $x_{x2}^{\upsilon_1\upsilon_2}$, that is, for

$$q, p, r, \upsilon_1, \upsilon_2, \upsilon_3 = \overline{1, N}. \quad (31)$$

Thus, the solution of the problem of synthesis of the UQOS systems with fuzziness properties can be reduced to solving the set of the SNPI of the form (18) – (31).

The statement formulated below defines sufficient conditions for the existence of P-th UQOSs with fuzziness properties, which provides interval (required) values of the objective function $\mathrm{int}(E)$.

Statement 6. Suppose that $\{x^j\}$, $j = \overline{1, N}$ is a dictionary (set) of P signals in a temporal or generalized theoretical representation, then, in order for the dictionary $\{x^j\}$ to belong to the UQOS system with fuzziness of order x_1, x_2, y_1, y_2, it is sufficient that each of x_i^j signals satisfies (is a solution)

$$C_1 = \frac{N}{2}(5N - 3) \quad (32)$$

the set of the SNPI of the form (18), and the joimt words of the form (19) – (22), respectively

$$C_2 = [(N(N-1)(N-2))]^2 (L - x_1)L, \tag{33}$$

$$C_3 = [(N(N-1))]^2 L(L - x_1), \tag{34}$$

$$C_4 = Nx_2(L - x_2), \tag{35}$$

$$C_5 = [(N(N-1))]^2 x_2(L - x_2). \tag{36}$$

the set of the SNPI of the form (30).

Statement 7. The number of the SNPI of the form (30), which provides sufficient conditions x_1 and x_2 of fuzziness of the dictionary $\{x^j\}$, is determined by the expression

$$C = [(N(N-1))]^2 L(L - x_2)((N-2)^2 + 1) + x_2(L - x_2)N(N-1)^2 + 1. \tag{37}$$

Expression (36) makes it possible to estimate the total number of the SNPI that need to be analyzed both in the synthesis and in the attempts to disclose the signals forms and order x_1 and x_1 of the blur. It should be emphasized that the number of unknowns in (29) is less than the number of nonlinear inequalities.

Let us formulate a number of provisions, the conclusions of which will be used in the development of algorithms for the synthesis of the NUQOSs, UQOSs, and CQOS signal systems.

Statement 8. Let the maximum (minimum) values of the realizations of functions ξ'_{a_1} and ξ'_{a_2} (18) be such that the value Δ is defined as

$$\Delta = \left|\xi'_{a_1}(l) - \xi_{a_1}(l)\right|, \text{ or } \left|\xi'_{a_2}(l) - \xi_{a_2}(l)\right| \ \Delta \neq 0,1,2,3\ldots P-1, P, \tag{38}$$

is more than P, and w^j signal is defined above the field $GF(P)$ or above the ring of numbers modulo P, then many values of the cyclic convolution $\xi_{a_2}(l)$ may belong to the interval

$$(\min \xi_{a_1}(l) - \max \xi_{a_2}(l)). \tag{39}$$

At least when rejecting Q of the latter and adding Q of the first w^j signal characters where $Q = \frac{\Delta}{P}$, if $\frac{\Delta}{P}$ and $Q = \frac{\Delta + t}{P}$, if $\frac{\Delta}{P}$.

Statement 9. If $N_j^{\nu} \in GF(P)$, then $Q = \frac{\Delta}{2}$, if Δ - is even, and $Q = \frac{\Delta + t}{P}$, if Δ - is odd.

Statement 10. Suppose that the subspace $\{x^j\}$ is a set of signals of L duration over $GF(2)$, then the necessary conditions n-equality on cyclic auto-convolution with k levels, each of x^j is a condition of not more than Δ-imbalance (unbalance) in the number of characters $1 - k^1$ and $(-1) - k^{-1}$, in this case

$$\Delta = \left|k^1 - k^{-1}\right| \le \sqrt{L + \sum_{i=1}^{n} n_i R_i}\ . \tag{40}$$

To determine the existence of optimal steps and their values, we formulate the following statement.

Statement 11. Suppose that x^j is a vector whose symbols in the temporal representation take values over $GF(P)$, and the imbalance in the number of symbols defined in terms of the value Q

as $\Delta i = |k_i - Q|$ is corresponding $\Delta_1, \Delta_2, \ldots, \Delta_Q$, then vector x^j satisfying the necessary conditions can be formed only by rejecting and adding, at least,

$$\upsilon = \frac{1}{q} \sum_{i=1}^{Q} \Delta i \tag{41}$$

symbols.

Thus, the solution of the problem of synthesis of the UQOSs signals with fuzziness properties can be reduced to solving the set of the SNPI of (18) – (31) form.

Conclusions

The efforts of the researchers are aimed at finding ensembles of complex signals whose characteristics with increasing duration approach the boundary of "dense packing" [2], that is, an ensemble, whose representatives have zero constant component, an ideal periodic autocorrelation function (PFAC), periodic mutual correlation function (PFMC), and have the largest possible volume. A widespread criterion for such an approximation is the minimum criterion, which focuses on ensemble synthesis by minimizing maximum values for the set of all undesirable correlations. Ensembles that have correlation peak values that reach the boundaries defined by the lower boundaries of Welch and Sidelnikov [6] are optimal and are sometimes called minimal ones. The problems of synthesis of a number of classes of signals with given correlation, ensemble and structural properties, including such systems of signals, which have "blurring" properties on correlation properties, are formulated in the general form. The said property 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 that is synthesized is formed. Theoretical bases of synthesis of quasioptimal uniform, nonuniform, complex signal systems with given auto -, mutually correlation, ensemble and structural properties are given. The use of many of these signal systems in modern information and communication systems will make it possible to improve the performance of such systems, first of all, noise protection, secrecy of operation, information security, noise immunity of receiving signals.

References:

1. 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. P. 1079-1100. DOI: 10.1615/TelecomRadEng.v76.i12.50.

2. Gorbenko I.D., Zamula A.A. Analytical assessment of the maximum lateral emissions of the correlation functions of complex nonlinear discrete signals // Radiotekhnika. 2017. Issue 191. P. 76 – 88.

3. 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. P. 1705-1717 DOI: 10.1615/TelecomRadEng.v76.i19.30.

4. Gorbenko I.D., Zamula A.A., Morozov V. L. Information and communication systems based on signal systems with improved properties building concept. Workshop Proceedings 2019 CEUR.

5. Gantmakher V. E., Bystrov N. E., Chebotarev D. V. Noise-like signals. Analysis, synthesis, processing. SPb. : Science and Technology, 2005. 400 p.

6. 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.

7. Sverdlik M.B. Optimal discrete signals. Moskva : Sov. Radio, 1975. 200 p.

8. Zamula A.A. Prospects for the use of nonlinear discrete signals in modern telecommunication systems and networks / Zamula A.A., Semenko E.A. // Information processing systems. Kharkiv : HUPS, 2015. Issue 5 (130). P. 129–134.

Kharkiv National V.N. Karazin University;
JSC "Institute of Information Technologies"

Received 08.02.2020

УДК 621.391 **DOI:10.30837/rt.2020.1.200.15**

І.Д. ГОРБЕНКО, д-р техн. наук, О.А. ЗАМУЛА, д-р техн. наук, ХО ЧІ ЛИК

МЕТОДИ ПОШУКУ ОПТИМАЛЬНИХ ЗА МІНІМАКСНИМ КРИТЕРІЄМ СИСТЕМ СКЛАДНИХ НЕЛІНІЙНИХ ДИСКРЕТНИХ СИГНАЛІВ

Вступ

На сьогодні для найважливіших додатків інформаційно-комунікаційних систем (ІКС), а саме: супутникових систем зв'язку, високошвидкісних систем стільникового мобільного телефонного зв'язку, систем радіолокації, радіонавігації, цифрового телебачення і радіо, актуальними є дослідження, що пов'язані з використанням сигналів – фізичних переносників даних в ІКС. Значне число сучасних ІКС відносяться до багатокористувачевих систем. У таких системах безліч каналів розміщуються в межах загального частотно-часового ресурсу. Одним із способів підвищення ефективності використання діапазону частот, з урахуванням електромагнітної сумісності, є використання множинного доступу з кодовим розділенням абонентів, що працюють в загальній смузі частот. Зазначений спосіб доступу є найбільш перспективним за багатьма характеристиками: висока завадозахищеність каналів і забезпечення конфіденційності даних; висока швидкість передачі і ефективність використання смуги частот; висока енергетична економічність і абонентська ємність мережі. Оскільки кодове розділення каналів ТКС грунтується на відмінності сигналів, що надаються абонентам системи, то побудова таких систем і їх характеристики визначаються вибором сигналів і їх властивостями. Дослідження показали, що перспективним напрямком забезпечення безпеки інформаційних ресурсів є використання технології розподіленого спектра (широкосмугових шумоподібних сигналів). Такі сигнали утворюють шляхом амплітудно-фазової модуляції дискретних послідовностей (сигнатур) користувача потоком даних. Наприклад, виконується множення бітового інформаційного потоку $B_k(t)$-го абонента на специфічну для кожного користувача (в багатокористувачевих системах, наприклад в CDMA додатках) на сигнатуру $S_k(t)$, а результат добутку $S_k(t)\cdot B_k(t)$ модулює безперервну несучу, тобто

$$S_k(t,b_k)=S_k(t)\cdot B_k(t)\cdot\cos(2\cdot\pi\cdot f_0\cdot t), \qquad (1)$$

де $b_k=(\ldots,b_{k,-1},b_{k,0},b_{k,1}\ldots)$ – бітовий потік k-го користувача, а $B_k(t)=b_{k,i}=\pm1,(i-1)\cdot T_b<t<i\cdot T_b$ (T_b – тривалість імпульсів позитивної і негативної полярності інформаційного сигналу k-го користувача).

В описаному прикладі потік бітів спочатку модулює бінарну сигнатуру, а результат використовується для бінарної фазової маніпуляції несучої.

При цьому маніпулюючі дискретні послідовності (ДП), які не залежать від бітового інформаційного потоку, повністю визначають властивості сигналів і часто ототожнюються з ними [1].

Як показують дослідження [2 – 4], основні показники ефективності ІКС: інформаційна безпека (в тому числі, конфіденційність, захищеність від нав'язування хибних повідомлень, режимів роботи системи – автентичність), завадозахищеність (завадостійкість прийому сигналів і скритність функціонування), значною мірою визначаються властивостями сигналів – фізичних переносників даних в ІКС. Тому увага дослідників сфокусована на аналізі, синтезі і обробці ДП з необхідними кореляційними, ансамблевими, статистичними, структурними та іншими властивостями.

Основні результати досліджень

При проектуванні багатокористувачевих ІКС основною проблемою є вибір способу множинного доступу, тобто можливості одночасного використання багатьма абонентами каналу зв'язку з мінімальним взаємним впливом. Оскільки кодове поділ грунтується на відмінності сигналів, то побудова багатокористувацьких комунікаційних систем і показники ефективності зазначених систем визначаються вибором сигналів і їх властивостями.

Зазвичай число абонентів в сучасних ІКС досить велике, тому вибір сигналів для систем зводиться до визначення систем сигналів із заданими властивостями. Зусилля дослідників направлені на пошуки ансамблів складних сигналів, характеристики яких з ростом довжини наближаються до кордонів щільної упаковки, або характеристик так званого гіпотетичного ансамблю, тобто ансамблю, всі представники якого мають нульову постійну складову, ідеальну періодичну функцію автокореляції (ПФАК) і нульові пелюстки періодичної функції взаємної кореляції (ПФВК) [5]:

$$\tilde{a}_{k,0} = 0;\ \rho_{kk}(m) = 0, m \neq 0 \bmod N;\ \rho_{kl}(m) = 0, k, l = 1, 2, ..., K. \qquad (2)$$

Широко застосовуваним критерієм подібного наближення є мінімаксний критерій, який орієнтує синтез ансамблю на мінімізацію максимального значення на множині всіх небажаних кореляцій. Для ідеального гіпотетичного ансамблю кореляційний пік $\rho_{\max}$ визначають як найбільшу з двох величин: максимуму серед усіх бічних пелюсток автокореляцій $\rho^a_{\max}$ послідовностей і максимуму серед значень взаємних кореляцій $\rho^c_{\max}$ всіх пар послідовностей

$$\rho_{\max} = \max\left\{\rho^a_{\max}, \rho^c_{\max}\right\}, \rho^a_{\max} = \max_{k, m\neq 0}\left|\rho_{p,kk}(m)\right|, \rho^c_{\max} = \max_{k,l,mk\neq l}\left|\rho_{p,kl}(m)\right|. \qquad (3)$$

Природно, що для ідеального гіпотетичного ансамблю $\rho_{\max}$ дорівнює нулю, а для будь-якого реального ансамблю може служити адекватною мірою його близькості до ідеального.

Мінімізація рівня бічних пелюсток автокореляційної функції (АКФ) має найбільше значення при конструюванні сигналу для таких додатків як виявлення сигналу, синхронізація, оцінка часу запізнювання і ін. При побудові багатокористувачевих широкосмугових систем з багатостанційним доступом і кодовим ущільненням каналів найбільш важливими проблемами є синтез, формування і обробка сигналів із заданими взаємно кореляційними властивостями.

В даний час відсутні регулярні методи синтезу дискретних послідовностей (ДП) оптимальних за мінімаксним критерієм. Більш того, не представляється можливим відповісти на питання: наскільки відомі сигнали з великим числом позицій (періодом) близькі до оптимальних.

Відомо, що будь-який сигнал $S(t)$ кінцевої енергії може бути представлений як сума незліченого числа гармонійних коливань, амплітуди і фази яких в межах нескінченно малого діапазону частот $[f, f + df]$ визначаються спектральною щільністю або спектром $\bar{S}(f)$. Математичним відображенням цього факту служить пара зворотного і прямого перетворень Фур'є:

$$S(t) = \int_{-\infty}^{\infty} \bar{S}(f)\cdot\exp(j\cdot 2\cdot\pi\cdot f\cdot t)df, \tilde{S}(f) = \int_{-\infty}^{\infty} S(t)\cdot\exp(-2\cdot\pi\cdot f\cdot t)dt. \qquad (4)$$

У теорії зв'язку найбільш поширеною моделлю служить канал з адитивним білим гаусовським шумом, в якому ймовірність трансформації каналом заданого вхідного сигналу в те чи інше вихідне спостереження $y(t)$ (перехідна ймовірність – $P\left[y(t)\,|\,S(t)\right]$) експоненціально зменшується зі зростанням квадрата Евклідової відстані між переданим сигналом і вихідним коливанням [5]:

$$P\left[y(t)\middle|S(t)\right] = \kappa \cdot \exp\left(-\frac{1}{N_0} d(s,y)\right), \tag{5}$$

де κ – константа, що не залежить від $S(t)$ і $y(t)$, N_0 – спектральна щільність потужності одностороннього білого шуму, а Евклідова відстань між $S(t)$ і $y(t)$ визначається як

$$d(S,y) = \sqrt{\int_0^T \left[y(t) - S(t)\right]^2 dt} \tag{6}$$

Відповідно до співвідношень (5) і (6) схожість сигналу (ймовірність того, що він перетворений каналом в спостереження) $y(t)$ зменшується зі збільшенням Евклідової відстані між $S(t)$ і $y(t)$. У разі рівної ймовірності всіх повідомлень джерела (що досягається при правильному проектуванні системи) оптимальною стратегією спостерігача, що забезпечує мінімальну помилку щодо прийняття рішення відносно сигналу, який передано, є правило (критерій) максимальної правдоподібності (МП). Згідно з цим критерієм, після того, як коливання $y(t)$ прийнято, рішення приймається на користь того сигналу, для якого ймовірність трансформації його каналом в прийняте спостереження $y(t)$ є найбільшою (в порівнянні з ймовірностями для інших сигналів). З урахуванням викладеного МП рішення для гаусова каналу може бути перетворено в правило мінімуму відстані:

$$d(S_j, y) = \min d(S_j, y) \Rightarrow H_j, \tag{7}$$

тобто рішення приймається на користь сигналу $S_j(t)$, оскільки він найбільш близький (в сенсі Евклідової відстані) до спостереження $y(t)$ серед всіх конкуруючих сигналів.

Важливою геометричною характеристикою оптимального правила пошуку систем сигналів у відповідності до правила максимальної правдоподібності (МП) є скалярний добуток двох сигналів:

$$(U,V) = \int_0^T U(t) \cdot V(t) dt, \tag{8}$$

яке може трактуватися як гранична форма скалярного добутку двох n – мірних векторів. Ця ж характеристика може бути обчислена за допомогою довжини векторів і косинуса кута α між ними: $(U,V) = \|U\|\|V\|\cos\alpha$ і, таким чином, скалярний добуток векторів свідчить про близькість або схожість сигналів, оскільки, чим ближче сигнали однакової довжини (енергії) один до одного, тим менше $\cos\alpha$ відрізняється від одиниці , і тим більше скалярний добуток. На підставі цього скалярний добуток (8) називають також кореляцією сигналів.

Розкривши дужки в (6), приходимо до співвідношення

$$d^2(S_i, y) = \int_0^T y^2(t) dt - 2 \cdot \int_0^T y(t) \cdot S(t) dt + \int_0^T S^2(t) dt = \|y\|^2 - 2 \cdot Z_i + \|S_i\|^2, \tag{9}$$

де Z_i – відповідає кореляції між спостереженням $y(t)$ та i -м сигналом $S(t)$

$$Z_i = (y_i, S_i) = \int_0^T y(t) \cdot S(t) dt. \tag{10}$$

Перший доданок в правій частині співвідношення (9) фіксовано для даного спостереження і не впливає на відстані і рішення, що аналізуються, відносно того, який з сигналів був прийнятий. Останній член суми є ні що інше, як енергія i-го сигналу E_i. З огляду на це, правило мінімуму відстані (7) може бути сформульовано як правило максимуму кореляції:

$$Z_j - \frac{E_j}{2} = \max(Z_i - \frac{E_j}{2}) = H_j . \qquad (11)$$

Останній вираз означає, що з M можливих сигналів з однаковою енергією фактично прийнятим вважається той, який має максимум кореляції зі спостереженням $y(t)$.

Наведені міркування вказують на спосіб конструювання безлічі сигналів. На рис. 1 зображено сигнальні вектори.

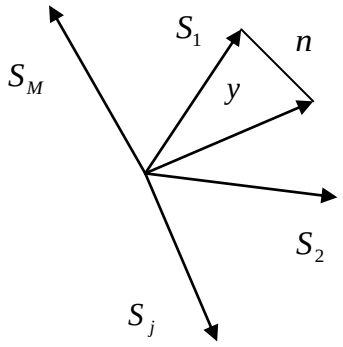


Рис. 1. Геометрична інтерпретація оптимального правила пошуку систем сигналів

Припустимо, що передавався сигнал S_1 і що він піддається спотворенню в каналі з адитивним білим гаусовим шумом, наслідком чого служить додавання до вектору S_1 шуму *n*. Вектор спостереження $y = S_1 + n$ буде випадковим чином (оскільки гаусовський вектор n характеризується симетричним ймовірнісним розподілом, що експоненціально спадає зі збільшенням довжини вектору *n,* що очевидно випливає з (1) після видалення з нього сигналу (тобто при підстановки $S(t) = 0$), переміщатися навколо, як це показано на рисунку, і тоді, згідно з правилом мінімуму відстані (7), як тільки y виявиться ближче до певного іншого, ніж сигнал S_1, то буде прийнято помилкове рішення. Для мінімізації ймовірності виникнення такого роду помилки слід розташовувати інші сигнали на максимально великій відстані від S_1. Оскільки будь-який з M сигналів може передаватися рівноймовірно, тобто займати місце S_1, то, очевидно, що всі відстані між сигналами $d(S_i, S_j), 1 \le i \le j \le M$ слід робити максимально великими.

Завдання побудови безлічі максимально віддалених один від одного сигналів (що входить в клас так званих задач упаковки) виявляється досить складним, і поки що не має спільного рішення. Одним з обмежень при синтезі сигналів є розмірність сигнального простору, всередині якого здійснюється їх упаковка. Фізична сутність цього обмеження обумовлена практичним ресурсом, наприклад шириною частотної смуги ΔF. Якщо частотно-часовий ресурс, в якому можуть розташовуватися M сигналів, обмежений параметрами ΔF і тривалістю сигналу T відповідно, то відповідно до теореми відліків є близько ΔFT незалежних відліків, які можуть бути використані при синтезі *M* сигналів, причому кожен з сигналів трактується як вектор в просторі розмірності $n_S = \Delta FT$.

Задача вибору безлічі сигналів може бути сформульована таким чином: знайти в просторі заданої розмірності n_S сузір'я з *M* векторів, що задовольняє енергетичним обмеженням і володіє максимально можливим мінімумом відстані між векторами $\mathrm{d}\min = \max$. У світлі виразів (2) – (3), а також (8) – (10) перевагу надають сигналами з найменшим значенням максимального бічного пелюстка. Ця вимога завжди супроводжується обмеженням на метод модуляції або на алфавіт, якому належать символи кодової послідовності. Таким чином, вимоги, що пред'являються до найкращого сигналу, можуть бути сформульовані у вигляді такої

оптимізаційної задачі: на безлічі всіх можливих послідовностей довжини N з символами з заздалегідь обраного алфавіту знайти послідовність або послідовності з мінімальною величиною максимального бічного пелюстка кореляційної функції.

В даний час відсутні регулярні методи синтезу дискретних послідовностей (ДП), оптимальних за мінімаксним критерієм. Більш того, не представляється можливим відповісти на питання: наскільки відомі сигнали з великим числом позицій N близькі до оптимальних. Тому актуальним залишається пошук ефективних методів розрахунку ДП з хорошими мінімаксними властивостями.

Наявність в N-вимірному лінійному просторі не більше N ортогональних векторів (сигналів) робить гіпотетичним ідеальний, з точки зору мінімаксного критерію, ансамбль дискретних послідовностей з нульовими боковими пелюстками функції авто- і взаємної кореляції, і обмежує потенціал зниження кореляційного викиду R при фіксованих N і числі абонентів K багатокористувачевої мережі.

При вирішенні низки задач теорії оптимального прийому сигналів, зокрема, виявлення сигналу, оцінка параметрів сигналів (затримки, амплітуди, початкової фази) та ін., важливим є автокореляційні властивостей систем сигналів, що використовуються.

Задача оцінювання часової затримки сигналу є типовою для телевізійних систем (канали синхронізації), цифрових систем мобільного радіозв'язку (пілотні канали, схеми стеження за часом), систем локації (вимір дальності до цілі), систем навігації космічного і наземного базування (вимірювання відстані до маяків) і ін. Фактично для адекватної роботи будь-якої сучасної системи обробки інформації необхідно відновити часову шкалу, що міститься в прийнятому коливанні, і це саме те, що відомо як оцінка затримки по часу [5].

Задача оцінки параметрів може бути сформульована таким чином. Нехай спостереження $y(t)$ поряд з шумом містить детермінований сигнал $s(t;\lambda)$, в якому єдиним невідомим є точне значення постійного параметра λ. Спостерігач, ґрунтуючись на аналізі $y(t)$, повинен прийняти рішення про те, яке значення з діапазону можливих прийняв параметр сигналу. Це рішення прийнято називати оцінкою і позначати як $\hat{\lambda}$. Оскільки в прийнятому спостереженні $y(t)$ завжди присутній шум, то при кожному сеансі прийому оцінка $\hat{\lambda}$ відрізняється від невідомого істинного значення параметра λ. У зв'язку з цим виникає питання: як прийняти оптимальне рішення, яке гарантувало б найменшої шкоди, зумовленої цими відмінностями. В принципі, задача оцінювання нічим не відрізняється від задачі розрізнення M сигналів. Тому для оцінки параметрів може бути застосована оптимальна стратегія рішень – правило максимальної правдоподібності. Це означає, що серед всіх конкуруючих значень λ в якості оцінки $\hat{\lambda}$ слід вибирати те, яке максимізує ймовірність трансформації каналом сигналу $s(t;\lambda)$ в спостережуване коливання $y(t)$. Для каналу з адитивним білим гаусовським шумом це правило еквівалентно правилу мінімуму відстані, яке з використанням введених позначень представимо у вигляді

$$d(s_\lambda, y) = \min_{\lambda} d(s_\lambda, y) \Rightarrow \lambda, \tag{12}$$

де s_λ – векторне позначення сигналу.

Застосування даного правила забезпечує отримання максимально правдоподібної (МП) оцінки $\hat{\lambda}$ в результаті знаходження такого значення, при якому сигнал найбільш близький за відстані Евкліда до спостереження $y(t)$. Достовірність (точність) оцінювання можна характеризувати величиною відхилення $\varepsilon = \hat{\lambda} - \lambda$ оцінки параметра $\hat{\lambda}$ від його істинного значення λ. Представляється розумною вимога: математичне очікування помилки ε, усереднене по

всіх можливих спостереженнях $y(t)$ при фіксованому істинному значенні λ, має дорівнювати нулю, тобто оцінка $\hat{\lambda}$ в середньому повинна збігатися з істинним значенням λ:

$$\bar{\varepsilon} = \overline{\hat{\lambda} - \lambda} = 0 \Leftrightarrow \bar{\lambda} = \lambda, \forall\lambda . \quad (13)$$

Суттєве значення для якісної оцінки параметрів сигналу має також величина розкиду оцінки відносно істинного значення. Традиційною і адекватною мірою розкиду служить дисперсія помилки $D\{\varepsilon\} = \overline{(\hat{\lambda} - \lambda)^2}$. Тоді, правило прийняття рішення повинно забезпечувати отримання оцінки з мінімальним значенням дисперсії для всіх дійсних значень λ:

$$D\{\varepsilon\} = \overline{(\hat{\lambda} - \lambda)^2} = \min, \forall\lambda . \quad (14)$$

У теорії оцінювання фундаментальна межа Крамера – Рао [5] встановлює нижню межу величини дисперсії будь оцінки:

$$D\{\lambda\} = D\{\varepsilon\} \approx -\frac{1}{\rho''(0) \cdot q^2}, q >> 1. \quad (15)$$

Присутність у (15) відношення сигнал-шум $q^2 = 2E / N_0$ в знаменнику правої частини співвідношення означає: що для будь-якого правила оцінювання справедливим є твердження: чим вище відношення сигнал-шум, тим менше помилка і тим вище точність вимірювань. Друга похідна говорить про кривизну або гостроту функції в даній точці і для випуклої кривої є негативною. У свою чергу, гострота $\rho(\lambda)$ в нульовій точці показує чутливість сигналу по відношенню до неузгодженості в величині λ: чим гостріше $\rho(\lambda)$, тим швидше копія сигналу з неузгодженістю за величиною втрачає свою подобу з вихідної копією.

Поряд з $\rho_o''(0)$ як індикатор гостроти автокореляційної функції (АКФ) сигналу може використовуватися характеристика, звана протяжністю кореляції, або часом кореляції τ_c. Зазначений параметр характеризує ширину АКФ сигналу. У світлі визначення АКФ будемо вважати, що копії сигналу, які зсунуті в часі на величину $\tau < \tau_C$, мають значну схожість, тоді як при $\tau < \tau_C$ їх схожість зневажливо мала. Зазначене дозволяє зробити висновок: сигнали з вузькою АКФ, тобто малим часом кореляції, є кращими для здійснення точного оцінювання з часової затримки.

Таким чином, якщо визначено закон внутрішньої кутової модуляції, що забезпечує час кореляції сигналу значно менше його тривалості, тобто $\tau_c << T$, тоді автокореляційна функція сигналу має яскраво виражений гострий характер, забезпечуючи високу точність оцінювання часової затримки, незважаючи на велику тривалість самого сигналу T . Але з урахуванням існуючої залежності між часом кореляції τ_C і смугою W частот ($\tau_C \approx 1/W$) нерівність $\tau_C << T$ означає, що сигнал характеризується великим значенням частотно-часового добутку $WT >> 1$, тобто є сигналом з розподіленим (широким) спектром. Тоді стає очевидним, що залучення технології розподіленого спектра дозволяє зняти протиріччя між величиною миттєвої потужності і точністю оцінювання: необхідна енергія вкладається в сигнал за рахунок його тривалості, а не потужності, тоді як висока точність вимірювання досягається завдяки синтезу систем сигналів з відповідним законом модуляції.

В [6] вказані принципово досяжні значення максимальних бічних піків періодичної функції автокореляції (межі «щільної упаковки») для заданого періоду послідовності N :

$$\rho \geq \begin{cases} 0, \text{если } N \equiv 0 (\text{mod } 4); \\ 1, \text{если } N \equiv 1 (\text{mod } 4); \\ 2, \text{если } N \equiv 2 (\text{mod } 4); \\ -1, \text{если } N \equiv 3 (\text{mod } 4), \end{cases} . \quad (16)$$

Наведені в (12) межі «щільної упаковки» встановлюють критерій синтезу безлічі ДП. Ансамблі з відповідним законом модуляції, зі значеннями кореляції, що досягають межі (12), є оптимальними за критерієм кореляційного піку, і називаються мінімаксними.

Аналіз [2, 5 – 6] показав, що на сьогодні відсутні регулярні методи синтезу ДП оптимальних за мінімаксним критерієм. Завдання синтезу ДП виявляється ще складнішим, якщо висуваються вимоги до розмірності (об'єму) системи сигналів, структурним властивостям і числу елементів ДП. Таким чином, досить актуальною проблемою залишається пошук ефективних методів синтезу дискретних сигналів (послідовностей), що відповідають потенційно можливим граничним характеристикам кореляційних функцій (границі «щільної упаковки») і володіють необхідними кореляційними, структурними, ансамблевими властивостями.

Хорошим інструментом для оцінки нижньої границі кореляції ρ KN векторів (K – число користувачів в системі, N – число елементів (період) ДП) є границя Велча [7]. Для числа $K > 2$ маємо

$$\rho \geq [K - 1/\, NK - 1]^{1/2}. \tag{17}$$

Ця нерівність визначає фундаментальну нижню границю, нижче якої кореляція між усіма циклічними копіями всіх K ДП (сигнатур), включаючи власні копії кожної сигнатури, опуститися ніколи не може. При числі користувачів близько десяти або більше ця версія границі Велча має вид

$$\rho \geq 1/\, N, K >> 1 \tag{18}$$

Таким чином, у відповідність з (16) – (18) для відповідних значень періоду сигналів можуть бути встановлені межі значень функцій кореляції і здійснюватися відбір сигналів, значення бічних пелюсток функції кореляції яких, не перевищує ці границі.

Для ідеального гіпотетичного ансамблю максимальні значення кореляційних функцій авто- і взаємної кореляції дорівнюють нулю, а для будь-якого реального ансамблю – може служити адекватною мірою його близькості до ідеального.

До числа ансамблів сигналів, які відповідають умовам (16) – (18), можна віднести нелінійні характеристичні дискретні сигнали, нелінійні криптографічні дискретні сигнали, багатофазні сигнали; троїчні сигнали, бінарні послідовності з непротилежною модуляцією та ін.

Побудова характеристичних сигналів (ХС) [6] базується на використанні характеру ψ мультиплікативної групи поля $GF(p^n)$ для $N = 4x + 2 = p^n - 1$ і $N = 4x = p^n - 1$. Правила кодування ХС приводять до коду з дворівневою періодичною функцією автокореляції з значеннями максимальних бічних функції автокореляції: $\mathrm{R}_\mu = \{-2, 2\}$, та $\mathrm{R}_\mu = \{0, -4\}$.

Об’єм системи характеристичних сигналів визначається зі співвідношення

$$M = \phi(L)/\, n, \tag{19}$$

де n – ступінь розширення поля Галуа.

Під криптографічними дискретними сигналами (КС) пропонується розуміти сукупності послідовностей (векторів) символів певного алфавіту, які обов’язково мають необхідні (задані) структурні, ансамблеві та кореляційні властивості, часову та просторову складності та можливості формування на основі ключів. Правила побудови КС [8] грунтуються на використанні випадкових чи псевдовипадкових процесів (в тому числі, методів криптографічного перетворення). КС повинні володіти: абсолютною структурною скритністю щодо законів їх формування та зміни сигналів в динамічному режимі; поліпшеними ансамблевими властивостями (існувати практично для будь-якого значення періоду, мати значний обсяг системи сигналів); необхідними (для забезпечення заданого значення завадостійкості прийому) кореляційними властивостями. Для захищених радіоканалів використання системи сигналів визначається додатками, в яких вони застосовуються. Зокрема, це можуть бути як окремі

сигнали або пари сигналів, так і великі безлічі дискретних сигналів з необхідними, але об'єктивно обмеженими значеннями «щільної упаковки», авто- і взаємно-кореляційними, ансамблевими властивостями.

Результати досліджень властивостей нелінійних ХС та нелінійних КС наведено в [9] і [10 – 15] відповідно. З точки зору границь «щільної упаковки» (16), ХС та КС можуть бути віднесені (за мінімаксним критерієм) до оптимальних сигналів.

Крім важливості застосовування у ряді додатків ІКС оптимальних сигналів в якості сигналів – фізичних переносників інформації, при вирішенні задач синхронізації (процеси пошуку, супроводження), оцінки параметрів сигналів, доцільним є застосування сигналів, які мають нульові значення піків кореляції поблизу центрального піку (області найбільшої кореляції τ_c).

В табл. 1 – 3 наведено приклади ізоморфізмів ХС та КС з числом елементів $N = 256$ і $N = 1020$ зі значеннями нульових бокових піків кореляції поблизу центрального піку ПФАК для цих сигналів. На рис. 2 – 5 наведено (у відповідності до табл. 1 – 3) вид ПФАК для ХС та КС з числом елементів $N = 256$ і $N = 1020$.

Таблиця 1

№	Характеристичні сигнали	ПФАК
1	[1, 1, 1, 1, -1, 1, 1, -1, -1, -1, -1, -1, -1, 1, -1, 1, 1, -1, 1, 1, -1, 1, 1, 1, -1, 1, -1, 1, 1, 1, -1, 1, -1, -1, 1, -1, -1, 1, 1, 1, 1, 1, 1, -1, 1, 1, -1, -1, 1, -1, -1, -1, -1, 1, 1, 1, 1, -1, -1, -1, -1, -1, 1, 1, -1, 1, 1, -1, 1, -1, 1, 1, 1, 1, -1, 1, -1, 1, 1, 1, -1, -1, -1, -1, -1, -1, -1, 1, -1, -1, -1, -1, -1, -1, -1, -1, 1, -1, -1, 1, 1, -1, -1, 1, 1, -1, -1, -1, 1, 1, 1, -1, -1, 1, 1, -1, -1, -1, 1, 1, 1, -1, 1, 1, 1, -1, -1, -1, 1, 1, 1, 1, 1, 1, -1, 1, -1, 1, 1, 1, -1, -1, 1, 1, -1, 1, 1, -1, 1, 1, 1, -1, -1, 1, -1, -1, 1, -1, -1, -1, 1, -1, 1, -1, 1, -1, -1, -1, 1, -1, -1, 1, 1, -1, 1, -1, -1, -1, -1, -1, 1, -1, 1, 1, 1, 1, 1, 1, -1, -1, 1, -1, 1, -1, 1, -1, 1, 1, -1, -1, 1, 1, 1, 1, 1, 1, -1, -1, 1, 1, 1, -1, -1, -1, 1, -1, 1, -1, 1, -1, -1, -1, -1, -1, 1, -1, 1, 1, -1, -1, -1, 1, 1, 1, 1, 1, -1, 1, 1, 1, 1, -1, 1, 1, -1, -1, -1, 1, 1, -1, -1, -1, 1, 1, 1, -1, 1, 1, -1, 1, -1, 1, 1, 1, 1, -1, -1, 1, -1, -1, -1, -1, 1, 1, 1]	[256, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, 256]
2	[-1, 1, 1, -1, 1, -1, -1, 1, -1, 1, 1, 1, 1, -1, -1, 1, 1, 1, 1, 1, -1, -1, -1, 1, -1, -1, 1, -1, 1, 1, 1, -1, 1, -1, 1, -1, -1, 1, 1, 1, -1, 1, -1, -1, -1, 1, -1, 1, 1, 1, -1, 1, 1, -1, 1, 1, -1, -1, 1, 1, 1, -1, -1, 1, -1, -1, -1, -1, -1, -1, 1, -1, -1, 1, 1, -1, 1, -1, 1, -1, -1, -1, -1, 1, -1, 1, 1, -1, -1, -1, 1, -1, 1, -1, 1, -1, -1, -1, -1, 1, -1, 1, 1, -1, -1, 1, -1, 1, -1, -1, 1, 1, -1, -1, 1, -1, 1, -1, 1, -1, -1, -1, -1, 1, -1, 1, 1, -1, -1, 1, -1, -1, -1, -1, -1, -1, 1, -1, 1, -1, -1, -1, -1, 1, -1, 1, -1, 1, -1, -1, 1, -1, 1, -1, 1, 1, 1, 1, 1, -1, -1, 1, 1, 1, -1, -1, 1, -1, 1, -1, 1, 1, 1, 1, 1, -1, -1, -1, -1, -1, -1, 1, -1, 1, -1, 1, 1, -1, -1, 1, 1, 1, -1, 1, -1, -1, 1, 1, 1, -1, 1, 1, -1, 1, 1, -1, 1, 1, 1, 1, 1, -1, 1, 1, 1, 1, -1, 1, 1, -1, -1, -1, -1, -1, -1, 1, -1, -1, -1, -1, 1, 1, 1, -1, 1, 1, -1, 1, -1, 1, 1, -1, -1, 1, -1, 1, 1, 1, 1, 1, -1, -1, -1, 1, 1, 1]	[256, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, 256]

Таблиця 2

Характеристичні сигнали	ПФАК
[-1, 1, 1, 1, -1, -1, 1, -1, 1, -1, 1, 1, -1, -1, 1, -1, 1, 1, 1, -1, -1, -1, -1, -1, -1, -1, -1, 1, -1, 1, 1, -1, 1, -1, 1, -1, -1, -1, 1, -1, 1, -1, 1, 1, 1, -1, -1, 1, 1, 1, -1, 1, 1, 1, -1, -1, -1, 1, -1, 1, -1, 1, 1, 1, 1, -1, 1, 1, 1, -1, 1, 1, -1, 1, -1, -1, -1, -1, 1, -1, -1, -1, 1, -1, 1, -1, -1, 1, -1, -1, 1, -1, 1, -1, -1, 1, -1, 1, - 1, -1, -1, 1, 1, -1, -1, 1, -1, 1, 1, -1, -1, -1, 1, 1, 1, -1, 1, -1, -1, 1, -1, -1, 1, -1, 1, 1, -1, -1, 1, 1, -1, 1, -1, -1, -1, 1, 1, -1, -1, 1, 1, -1, -1, -1, 1, -1, 1, 1, 1, -1, -1, -1, -1, -1, -1, -1, 1, 1, 1, -1, -1, -1, 1, 1, -1, 1, -1, 1, -1, 1, -1, 1, 1, -1, -1, 1, -1, 1, 1, -1, -1, -1, -1, 1, 1, 1, -1, 1, -1, 1, 1, 1, -1, -1, 1, 1, 1, 1, -1, 1, 1, -1, -1, 1, -1, 1, -1, 1, 1, 1, -1, -1, -1, 1, 1, 1, -1, 1, -1, -1, 1, 1, -1, -1, -1, 1, 1, -1, -1, 1, - 1, 1, 1, -1, 1, 1, 1, -1, -1, -1, -1, 1, -1, -1, -1, 1, - 1, -1, -1, 1, 1, 1, -1, 1, -1, 1, 1, -1, 1, -1, 1, 1, -1, 1, -1, 1, -1, -1, 1, -1, -1, 1, 1, -1, 1, 1, -1, -1, 1, 1, 1, -1, 1, 1, 1, -1, 1, -1, -1, 1, 1, 1, -1, -1, 1, -1, -1, 1, 1, -1, 1, -1, 1, 1, -1, 1, -1, -1, -1, -1, -1, 1, 1, - 1, -1, 1, -1, 1, 1, 1, 1, -1, 1, -1, -1, -1, -1, 1, 1, 1, 1, -1, -1, 1, -1, 1, -1, 1, 1, 1, 1, -1, 1, 1, -1, -1, -1, -1, 1, -1, -1, -1, -1, -1, 1, 1, 1, -1, 1, -1, 1, 1, -1, - 1, 1, -1, -1, -1, 1, 1, 1, 1, -1, -1, -1, -1, -1, 1, -1, 1, -1, -1, 1, -1, 1, -1, -1, -1, -1, -1, 1, 1, -1, 1, -1, -1, -1, 1, -1, -1, -1, -1, -1, 1, -1, 1, -1, 1, -1, 1, 1, -1, 1, 1, 1, 1, 1, 1, -1, -1, -1, 1, 1, -1, -1, 1, -1, 1, -1, 1, 1, 1, 1, 1, -1, 1, -1, -1, 1, -1, -1, -1, 1, -1, - 1, -1, 1, -1, -1, -1, 1, 1, -1, -1, -1, -1, -1, 1, 1, 1, 1, 1, 1, -1, 1, 1, 1, -1, -1, -1, -1, -1, 1, 1, 1, 1, 1, 1, 1, -1, 1, -1, -1, -1, 1, -1, -1, -1, -1, 1, 1, 1, -1, - 1, 1, 1, -1, -1, 1, -1, -1, 1, -1, 1, -1, 1, -1, 1, 1, 1, -1, 1, 1, 1, 1, 1, 1, 1, 1, -1, -1, -1, 1, 1, -1, -1, 1, 1, -1, 1, 1, -1, 1, -1, -1, -1, 1, -1, -1, -1, -1, 1, -1, 1, -1, 1, -1, -1, 1, -1, 1, -1, -1, 1, -1, -1, -1, 1, -1, 1, -1, 1, 1, -1, 1, -1, 1, 1, -1, -1, 1, -1, -1, -1, 1, - 1, -1, -1, 1, -1, -1, -1, 1, 1, 1, 1, -1, 1, -1, 1, 1, 1, 1, 1, 1, -1, -1, 1, 1, -1, 1, 1, -1, 1, -1, 1, -1, -1, -1, 1, 1, 1, 1, 1, 1, 1, 1, -1, 1, -1, 1, 1, 1, -1, 1, 1, 1, 1, -1, -1, 1, -1, 1, -1, -1, -1, -1, -1, 1, 1, 1, 1, 1, - 1, 1, -1, 1, 1, -1, 1, -1, -1, 1, -1, -1, -1, 1, 1, -1, - 1, -1, -1, -1, 1, -1, -1, 1, -1, 1, -1, -1, -1, 1, -1, 1, 1, -1, -1, -1, 1, -1, 1, 1, 1, 1, 1, 1, -1, -1, 1, -1, 1, 1, -1, 1, -1, -1, -1, -1, 1, -1, 1, 1, 1, 1, -1, -1, 1, 1, -1, 1, -1, 1, 1, 1, 1, -1, -1, -1, -1, -1, 1, 1, -1, -1, - 1, 1, 1, -1, 1, 1, -1, -1, -1, -1, 1, -1, -1, -1, 1, -1, - 1, 1, 1, -1, -1, -1, 1, 1, -1, -1, -1, 1, 1, 1, 1, 1, 1, - 1, -1, -1, -1, -1, 1, 1, 1, 1, 1, -1, 1, 1, -1, 1, 1, 1, - 1, 1, 1, 1, -1, 1, -1, -1, 1, -1, -1, -1, 1, 1, 1, 1, -1, -1, 1, 1, -1, 1, 1, -1, -1, 1, 1, 1, 1, -1, 1, 1, -1, 1, 1, -1, 1, 1, 1, 1, 1, 1, -1, -1, 1, 1, 1, -1, 1, -1, -1, 1, 1, -1, 1, 1, 1, 1, 1, -1, 1, 1, -1, 1, -1, -1, 1, 1, 1, 1, -1, -1, 1, 1, 1, 1, 1, 1, 1, 1, 1, -1, -1, 1, -1, -1, 1, -1, -1, 1, -1, 1, -1, 1, -1, -1, 1, -1, -1, -1, -1, 1,	[1020, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, - 4, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, - 4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, - 4, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, - 4, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, - 4, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0,

-1, -1, 1, 1, -1, -1, 1, 1, -1, 1, 1, 1, 1, -1, -1, 1, 1, -1, -1, -1, -1, 1, 1, 1, -1, -1, -1, -1, 1, -1, -1, 1, -1, -1, 1, 1, 1, 1, -1, -1, 1, 1, -1, 1, 1, 1, 1, 1, -1, -1, -1, 1, -1, -1, -1, 1, 1, 1, -1, -1, -1, -1, -1, 1, -1, -1, -1, 1, -1, 1, 1, 1, 1, 1, -1, -1, -1, 1, -1, -1, -1, 1, -1, 1, 1, 1, 1, 1, 1, 1, -1, 1, 1, 1, -1, 1, 1, 1, -1, 1, 1, -1, -1, 1, -1, -1, -1, -1, -1, 1, -1, -1, -1, -1, -1, 1, 1, 1, 1, -1, 1, -1, 1, -1, 1, -1, -1, 1, -1, -1, -1, -1, 1, 1, -1, -1, -1, -1, -1, 1, 1, -1, 1, 1, -1]	0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 1020]

Таблиця 3

Характеристичні сигнали	ПФАК
[-1, -1, 1, 1, 1, -1, -1, 1, 1, 1, 1, -1, 1, 1, -1, 1, 1, 1, -1, -1, 1, 1, 1, 1, -1, 1, 1, 1, 1, 1, -1, -1, 1, 1, -1, 1, 1, 1, -1, 1, -1, 1, 1, -1, 1, 1, -1, 1, 1, 1, -1, -1, -1, 1, -1, -1, 1, 1, 1, -1, -1, -1, 1, -1, 1, 1, 1, -1, 1, 1, -1, 1, -1, -1, -1, 1, 1, 1, 1, -1, -1, -1, -1, -1, -1, 1, 1, 1, -1, 1, -1, 1, 1, -1, 1, -1, -1, 1, -1, -1, -1, 1, -1, -1, -1, -1, -1, 1, -1, -1, -1, 1, 1, 1, 1, 1, 1, 1, -1, 1, -1, 1, -1, -1, -1, 1, 1, -1, 1, 1, -1, -1, 1, 1, 1, 1, 1, 1, -1, 1, -1, -1, 1, -1, -1, -1, 1, 1, 1, -1, -1, 1, -1, -1, 1, 1, -1, 1, 1, -1, 1, -1, -1, -1, -1, -1, 1, -1, -1, 1, 1, -1, 1, 1, -1, 1, -1, -1, 1, -1, 1, 1, -1, 1, -1, -1, -1, 1, -1, 1, 1, 1, -1, -1, 1, -1, 1, 1, -1, 1, 1, -1, 1, 1, -1, 1, 1, -1, -1, -1, -1, -1, 1, -1, -1, 1, 1, -1, 1, 1, 1, -1, -1, -1, 1, 1, -1, -1, -1, -1, -1, 1, -1, 1, 1, 1, -1, 1, -1, -1, -1, -1, -1, 1, -1, -1, 1, 1, -1, -1, -1]	[256, 0, 0, 0, 0, -8, 20, -20, 8, 20, -16, -8, 8, -8, -16, -8, 20, 4, 24, -20, 16, 20, -8, 4, 28, 4, -8, 16, -20, 12, -28, -32, 0, 8, -4, -4, 0, -8, 16, 16, 16, 16, -8, -8, 12, 28, -16, 24, -16, 0, 0, -24, -12, 12, -12, 0, 24, -12, -8, -16, -24, 20, 12, -4, 0, 20, 4, 20, 8, -16, -12, -12, -4, -28, 12, -20, 12, 8, 24, -12, 0, -4, 4, 8, -12, -12, -4, -8, 24, -12, 0, -8, 0, -16, -8, -28, 0, -24, -24, 8, 24, 4, 0, -20, 0, -4, 8, -28, -8, -16, -12, -4, 4, -20, 0, 16, -4, 16, 0, -24, -16, 0, 4, 28, 16, 4, -4, -8, -4, -8, -4, 4, 16, 28, 4, 0, -16, -24, 0, 16, -4, 16, 0, -20, 4, -4, -12, -16, -8, -28, 8, -4, 0, -20, 0, 4, 24, 8, -24, -24, 0, -28, -8, -16, 0, -8, 0, -12, 24, -8, -4, -12, -12, 8, 4, -4, 0, -12, 24, 8, 12, -20, 12, -28, -4, -12, -12, -16, 8, 20, 4, 20, 0, -4, 12, 20, -24, -16, -8, -12, 24, 0, -12, 12, -12, -24, 0, 0, -16, 24, -16, 28, 12, -8, -8, 16, 16, 16, 16, -8, 0, -4, -4, 8, 0, -32, -28, 12, -20, 16, -8, 4, 28, 4, -8, 20, 16, -20, 24, 4, 20, -8, -16, -8, 8, -8, -16, 20, 8, -20, 20, -8, 0, 0, 0, 0, 256]

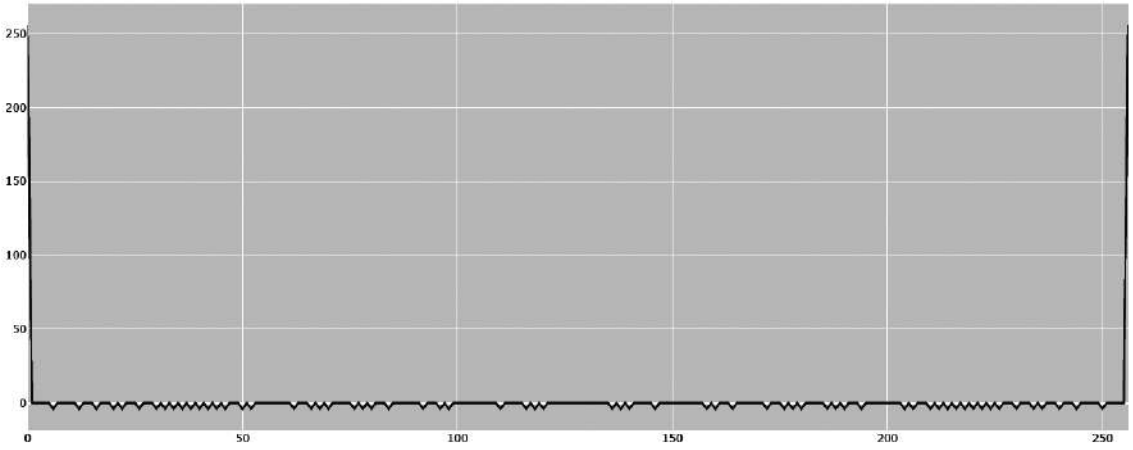


Рис. 2. Вид ПФАК для ХС з $N = 256$ (табл. 1, №1)

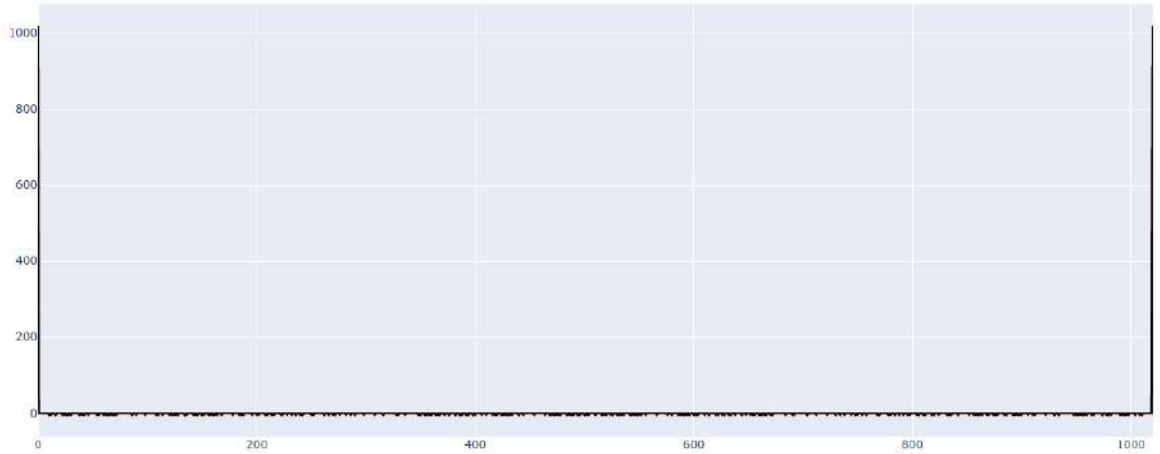


Рис. 3. Вид ПФАК для ХС з N = 1020 (табл. 2)

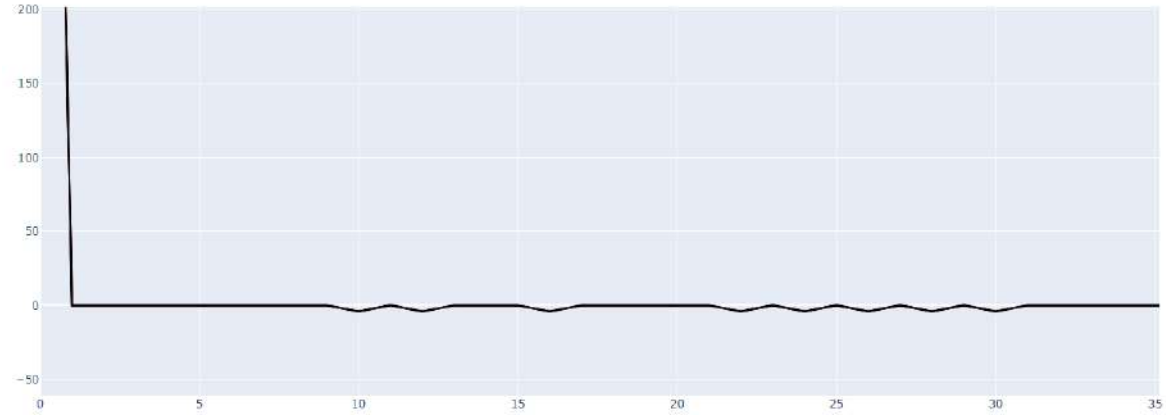


Рис. 4. Збільшений фрагмент ПФАК (щодо рис. 2), який свідчить про наявність нульових піків ПФАК в області найбільшої кореляції τ_c

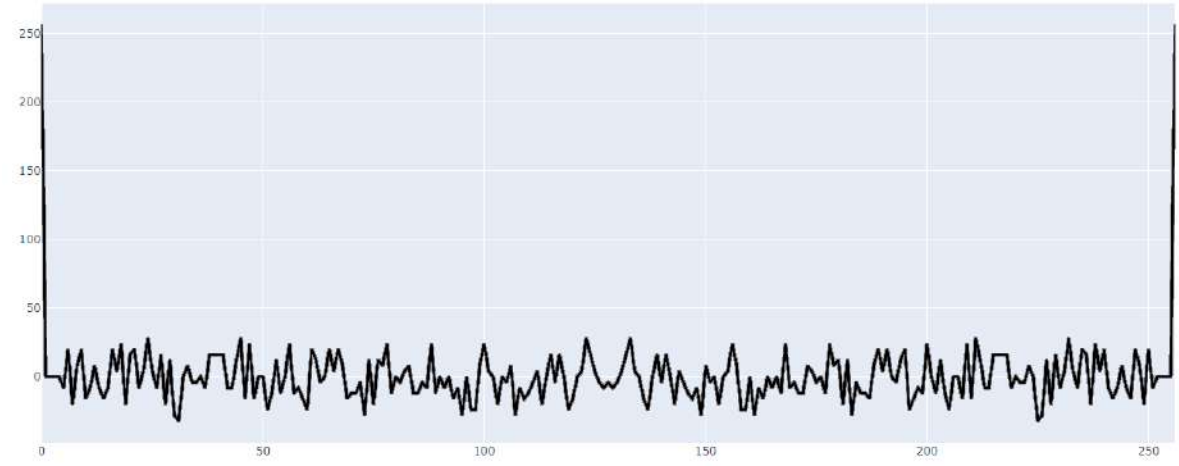


Рис. 5. Вид ПФАК для КС з N = 256 (табл. 3)

При побудові захищених ІКС загального та спеціального призначення, для яких в якості основних вимог висуваються вимоги забезпечення конфіденційності інформаційного обміну, цілісності даних, завадостійкості прийому сигналів, захищеності від нав'язування хибних повідомлень, важливими завданнями, які потребують вирішення, є пошук методів синтезу, формування і обробки ансамблів сигналів, які володіють покращеними не тільки кореляцій-

ними, а й ансамблевими, структурними (в сенсі складності визначення (стороною протидії) закону (правила) побудови таких сигналів, технологічними та іншими властивостями.

В табл. 3 наведено дані відносно ансамблевих і кореляційних властивостей КС, в тому числі, зазначено кількість сигналів, що мають нульові значення бокових піків функцій автокореляції в області максимальної кореляції. Як випливає з даних табл. 3, КС володіють суттєво покращеними у порівнянні з лінійними класами сигналів ансамблевими властивостями. Так, ансамбль КС з числом елементів 256, сигнали якого задовольняють границі «щільної упаковки», більш ніж на порядок перевищує ансамбль, складений з лінійних сигналів, отриманих на основі M -послідовностей. Крім того, КС, як показали результати проведеного тестування [15], за своїми статистичними властивостями, близькі до властивостей випадкових послідовностей, тобто володіють практично ідеальною структурної скритністю, що дає можливість поліпшити показники інформаційної безпеки функціонування ТКС. До ансамблю КС з періодом 256 елементів входить 302 сигналів, для яких бічні піки ПФАК мають один і більше нульових викидів функції кореляції поблизу центрального піку.

Таблиця 4

Число елементів КС (N)	Граничні значення (границя «щільної упаковки»)	ПФАК			
		Число КС, що задовольняють границі «щільної упаковки»	Найменше значення $R6_{max}$, що досягається для КС з числом елементів N	Кількість КС з найменшим значенням $R6_{max}$	Кількість КС, які мають один або більше нульових піків ПФАК в області найбільшої кореляції
64	17	9545	8	14	2041
256	33	680	28	48	81
256	36	2940	28	48	302
1024	80	247	72	3	7
1024	90	2209	72	3	123
2048	129	409	116	12	39

Висновки

На основі застосування мінімаксного критерію запропоновано методи пошуку оптимальних нелінійних дискретних складних сигналів для низки додатків ІКС загального та спеціального призначення при вирішенні задач теорії оптимального прийому, зокрема, виявлення сигналу, розрізнення сигналів, оцінка параметрів сигналів. Показано, що застосування запропонованих систем сигналів дозволить поліпшити показники завадостійкості прийому сигналів, точності оцінки параметрів сигналів, інформаційної безпеки та скритності функціонування ІКС в умовах кібератак, дії природніх та організованих, в тому числі, структурних, ретрансльованих і інших завад.

Список літератури:

1. 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.

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

3. 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. P. 1705-1717 DOI: 10.1615/TelecomRadEng.v76.i19.30.

4. Gorbenko I., Zamula A., Morozov V. Information and communication systems based on signal systems with improved properties building concept // Workshop Proceedings 2019 CEUR.

5. Ipatov V. Spread Spectrum and CDMA. Principles and Applications / University of Turku, Finland and St. Petersburg Electrotechnical University 'LETI', Russia // John Wiley & Sons Ltd. The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England. 2005. 385 p.

6. Свердлик М.Б. Оптимальные дискретные сигналы. Москва : Сов. радио, 1975. 200 с.

7. Welch L. R. Lower bound on the maximum cross-correlation of signals // IEEE Trans. Inform. Theory. 1974. Vol. 20. P. 397-399.

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

9. Горбенко І.Д., Замула О.А., Хо Чі Лик Оптимізація пошуку дискретних складних сигналів з необхідними властивостями для застосування у сучасних інформаційно-комунікаційних системах // Математичне та комп'ютерне моделювання. Серія: Техн. науки : Зб. наук. праць / Ін-т кібернетики імені В.М. Глушкова Національної академії наук України, 2019. Вип. 19. 160 с.

10. Горбенко І.Д., Замула О.А., Хо Чі Лик Оптимізація синтезу нелінійних дискретних складних сигналів з визначеними властивостями // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. Матеріали дев'ятої міжнародної науково-технічної конференції. 11-12 квітня 2019. С. 5-6.

11. Горбенко И.Д., Замула А.А. Аналитическая оценка значений максимальных боковых выбросов функций корреляции сложных нелинейных дискретных сигналов // Радиотехника. 2017. Вып. 191. С. 76 88.

12. Замула А.А. Перспективы применения нелинейных дискретных сигналов в современных телекоммуникационных системах и сетях / Замула А.А., Семенко Е.А // Системи обробки інформації. Харків : ХУПС, 2015.

13. Gorbenko I.D., Zamula A.A., Semenko Ye.A. Ensemble and correlation properties of cryptographic signals for telecommunication system and network applications // Telecommunications and Radio Engineering. 2016. Vol. 75, Issue 2. P. 169-178. DOI: 10.1615/TelecomRadEng.v75.i2.60.

14. Methods for implementing communications in info-communication systems based on signal structures with specified properties / I. Gorbenko, A. Zamula, V. Morozov // 2017 4th International Scientific-Practical Conference Problems of Info communications Science and Technology, PIC S and T 2017 Proceedings. DOI: 10.1109/INFOCOMMST.2017.8246359.

15. Gorbenko I., Zamula A., Morozov V. Information and communication systems based on signal systems with improved properties building concept systems with improved properties building concept 2019 CEUR Workshop Proceedings.

АТ «Інститут інформаційних технологій»;
Харківський національний
університет імені В.Н. Каразіна

Надійшла до редколегії 15.02.2020

УДК 004.056.53 **DOI:10.30837/rt.2020.1.200.16**

И.Е. АНТИПОВ, д-р техн. наук, Б.В. БОЧАРОВ, Д.Р. НАЙДЕНОВА

ОЦЕНКА БЕЗОПАСНОСТИ ПОЛЬЗОВАТЕЛЕЙ ИНТЕРНЕТ-БАНКИНГА

Введение

Дистанционное банковское обслуживание или Интернет-банкинг (ИБ) – технология, позволяющая удаленно осуществлять финансовые операции и контролировать движение средств, прочно вошла в нашу жизнь. Ее удобства и преимущества неоспоримы. К сожалению, уязвимости у этой технологии тоже существуют.

В публикациях часто описываются различные приемы, которыми пользуются мошенники для хищения средств и даются советы о том, как им противостоять. Но они, в основном, носят частный, разрозненный характер. Авторы статьи полагают, что проблема обеспечения безопасности ИБ должна рассматриваться комплексно. Для этого необходимо решить следующие задачи:

- систематизировать уязвимости пользователей ИБ;
- предложить методику их численной оценки;
- предложить меры по противодействию угрозам;
- предложить методику оценки эффективности их применения.

В статье рассмотрены и систематизированы угрозы для пользователей интернет-банкинга, обусловленные уязвимостями мобильных телефонов и мобильной связи, контрмеры, доступные пользователю, а также способы численной оценки уязвимостей и эффективности контрмер.

Анализ и обобщение уязвимостей для пользователей ИБ

При подготовке статьи был рассмотрен ряд публикаций, в которых описаны пути несанкционированного доступа к сервисам ИБ [2 – 14]. Не исключено, что в скором времени будут изобретены новые способы доступа, а ныне известные потеряют свою актуальность. В рамках научной статьи будет уместно рассмотреть, обобщить и систематизировать основные пути, которыми пользуются злоумышленники.

Итак, на основании анализа [2 – 14], мы выделили четыре основные уязвимости:

1. Похищение телефона вместе со всей имеющейся в нем информацией;
2. Методы социальной инженерии (СИ), при которых мошенническим путем извлекаются необходимые данные (телефон при этом – просто средство связи);
3. Перехват данных, передаваемых или хранящихся на мобильном устройстве;
4. Похищение данных sim-карты (физически sim-карта при этом остается у пользователя).

Две последние группы могут быть разделены на подгруппы, что требует дополнительных пояснений.

Перехват данных может осуществляться путем установки вредоносного программного обеспечения (ПО) на устройство пользователя, либо через уязвимость сети связи. Это наиболее распространенный способ похищения данных. Как отмечается в [12], до 43 % ПО для мобильных телефонов, находящегося в открытом доступе, потенциально опасно. Кроме того, встречаются сообщения о случаях «открытого» копирования данных пользователей с использованием административного ресурса[*] (на границах при въезде/выезде в некоторые страны и районы) [5, 6].

Установка вредоносного ПО может происходить при использовании программ из непроверенных источников и при переходе по фишинговым ссылкам [2]. Отмечаются случаи уста-

[*] Предполагается, что административный ресурс, упоминаемый здесь и далее в этой статье, доступен только уполномоченным государственным органам и применяется исключительно в благих целях. Однако, как показывает практика, такое предположение не всегда верно, о чем свидетельствуют [7, 8].

новки вредоносного ПО еще на этапе производства мобильного устройства [4]. Намеренная установка вредоносного ПО может произойти при временной передаче устройства в чужие руки (на ремонт, под предлогом «посмотреть», «позвонить» и т. д.) Также имеют место случаи установки такого ПО с использованием административного ресурса [5].

Перехват данных через сеть (без доступа к устройству пользователя) может быть осуществлен с использованием уязвимостей сетей мобильной связи, а также с использованием административного ресурса. Отдельно следует выделить опасность перехвата данных при подключении через Wi-Fi сети, которые уступают по защищенности сетям мобильной связи.

Для похищения данных sim-карты не обязательно иметь к ней физический доступ. Хакерские технологии позволяют создать «клон» sim-карты, используя уязвимости сетей мобильной связи [3, 9]. Также некоторые операторы мобильной связи позволяют восстановить утерянную (или «якобы утерянную») sim-карту с помощью нового стартового пакета [10]. Это дает возможность мошенникам, используя различные приемы, получить дубликат sim-карты, попутно заблокировав при этом карту законного пользователя [13, 14]. Также есть случаи получения дубликата sim-карты с использованием административного ресурса [11].

Рассмотренные уязвимости схематично показаны на рис. 1.

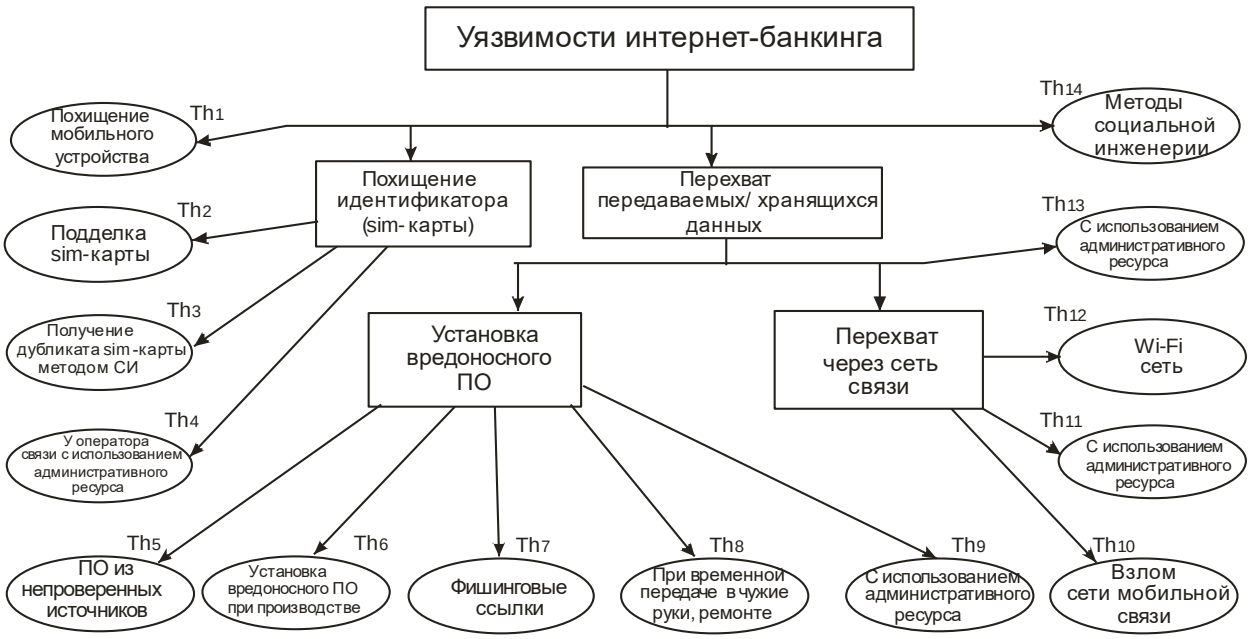


Рис. 1. Схематическое представление уязвимостей для пользователей ИБ

Известная методика численной оценки

Перейдем к рассмотрению указанных уязвимостей с точки зрения одной из базовых угроз информационной безопасности – конфиденциальности данных, которые позволяют злоумышленнику получить доступ к счету пользователя. Для каждой уязвимости должен быть рассчитан уровень угрозы Th_i. Согласно [15], это величина является безразмерной и означает критичность воздействия данной угрозы на ресурс. В ней также учитывается вероятность реализации данной угрозы. Выражение для расчета уровня угрозы:

$$Th_i = ER_i \times P_i, \quad (1)$$

где P_i – вероятность реализации каждой угрозы (отношение количества успешных попыток реализации угрозы для некоторой уязвимости к общему числу попыток, предпринимаемых злоумышленниками), ER_i – критичность реализации угрозы, которая отражает меру нанесенного ущерба по отношению к максимально возможному ущербу, если она будет реализована.

После определения уровня угрозы Th_i, согласно [15], необходимо рассчитать уровень угрозы для всех уязвимостей

$$CTh = 1 - \prod_{i=1}^{n} (1 - Th_i). \quad (2)$$

Далее оценивается стоимость ресурса C и суммарный риск:

$$R = C \times CTh. \quad (3)$$

Таким образом, для расчета уровней угроз согласно методике [15] необходимо составить таблицу вида (табл. 1):

Таблица 1

Номер	Угроза/уязвимость	Вероятность реализации *P, %*	Критичность реализации *ER, %*
1	Угроза 1 / Уязвимость 1	P_{11}	ER_{11}
..	…	…	…
N	Угроза 3 / Уязвимость m	P_{3m}	ER_{3m}

Методика оценки уязвимости пользователей ИБ

Для нашего случая таблица принимает вид табл. 2.

Таблица 2

Уязвимость / пути реализации			Вероятность реализации	Критичность реализации	Уровень угрозы
Похищение телефона			P_1	ER_1	Th_1
Похищение данных sim-карты		- путем подделки sim-карты	P_2	ER_2	Th_2
		- путем получения дубликата средствами СИ	P_3	ER_3	Th_3
		- у оператора связи с использованием админресурса	P_4	ER_4	Th_4
Перехват/ копирование данных телефона	- путем установки вредоносного ПО	- из непроверенных источников	P_5	ER_5	Th_5
		- на этапе производства	P_6	ER_6	Th_6
		- через фишинговые ссылки	P_7	ER_7	Th_7
		- при передаче в чужие руки	P_8	ER_8	Th_8
		- с использованием админресурса	P_9	ER_9	Th_9
	- через сеть	- путем «взлома» сети	P_{10}	ER_{10}	Th_{10}
		- Wi-Fi	P_{11}	ER_{11}	Th_{11}
		- с использованием админресурса	P_{12}	ER_{12}	Th_{12}
	- с использованием админресурса		P_{13}	ER_{13}	Th_{13}
Методы социальной инженерии			P_{14}	ER_{14}	Th_{14}

Для ее заполнения необходимо знать вероятности P_i и критичности реализации ER_i. Они могут быть получены из анализа полицейских сводок, данных о попытках взломов и их результативности, что по силам только службам безопасности банков. Эти данные могут различаться для разных местностей и меняться с течением времени, но именно они могут служить точным исходным материалом для оценки уязвимости согласно [15] и использоваться для совершенствования систем безопасности со стороны банков.

Авторам статьи такие данные недоступны, поэтому для получения хотя бы оценочных значений уязвимостей был применен следующий подход.

У каждого пользователя ИБ имеется свое представление об угрозах, связанных с безопасностью их банковских счетов. Оно формируется на основании личного опыта, опыта

ближайшего окружения, публикаций в СМИ, социальных сетях и т. д. Опрос даже ограниченного количества пользователей может помочь получить требуемые оценки.

Сложность опроса состояла в том, что далеко не все пользователи различают и готовы разбираться в понятиях «вероятность реализации угрозы», «критичность реализации» и др. Поэтому опрашиваемым было предложено ответить на такой вопрос:

- допустим, имеется 1000 пользователей ИБ, ведущих такой же образ жизни, применяющих то же оборудование и практикующих тот же подход к мерам безопасности в ИБ, что и они. Сколько из них могут стать жертвами злоумышленников в результате той или иной уязвимости?

Результаты опроса, нормированные к числу гипотетических одинаковых пользователей, представлены в табл. 3 как уровень угрозы.

Удобство такого подхода состоит в том, что каждый пользователь, если он заинтересован в повышении своей безопасности в ИБ, может изучить элементарные сведения о существующих уязвимостях и путях их реализации (хотя бы, в рамках данной статьи) и самостоятельно оценить уровень угроз для себя.

Таблица 3

Уязвимость / пути реализации			Уровень угрозы	
Похищение телефона			Th_1	0.001
Похищение данных sim-карты	- путем подделки sim-карты		Th_2	0.001
	- путем получения дубликата средствами СИ		Th_3	0.005
	- у оператора связи с использованием админресурса		Th_4	~0
Перехват/ копирование данных телефона	- путем установки вредоносного ПО	- из непроверенных источников	Th_5	0.01
		- на этапе производства	Th_6	~0
		- через фишинговые ссылки	Th_7	0.01
		- при передаче в чужие руки	Th_8	~0
		- с использованием админресурса	Th_9	~0
	- через сеть	- путем «взлома» сети	Th_{10}	~0
		- Wi-Fi	Th_{11}	0.001
		- с использованием админресурса	Th_{12}	~0
	- с использованием админресурса		Th_{13}	~0
Методы социальной инженерии			Th_{14}	0.1

Меры повышения безопасности пользователей ИБ

Рассмотрим теперь, какие контрмеры может принять пользователь ИБ для повышения свой безопасности.

1. Отказ от смартфона в пользу простого телефона без операционной системы.

При применении данной контрмеры исключаются уязвимости, связанные с установкой вредоносного ПО. Вероятность утечки данных через небезопасное Wi-Fi-соединение также окажется равна нулю – в простых телефонах нет функции доступа к Wi-Fi сетям. Кроме того, уменьшается вероятность похищения мобильного устройства, поскольку такие телефоны не представляют особой ценности для злоумышленников. Даже в случае похищения телефона критичность реализации будет невысока, поскольку статический пароль в простом телефоне не хранится.

2. Функция разблокировки по отпечатку пальца.

Эта функция не позволит мошеннику получить доступ к функциям телефона даже в случае его похищения, а также сделает невозможной установку вредоносного ПО на устройство, оставленное без присмотра. Это позволит защитить устройство от целого ряда уязвимостей.

3. Установка антивирусного ПО на смартфон делает его гораздо более устойчивым к атакам с использованием вредоносного ПО. Вероятность реализации угроз уменьшается.

4. Использование именной (не анонимной) sim-карты затруднит для злоумышленника получение ее дубликата методами СИ, что уменьшит вероятность реализации угрозы.

5. Использование отдельного смартфона для финансовых операций уменьшает вероятность взлома, связанную с наличием вредоносного ПО, при условии, что этот смартфон не

используется ни для чего больше, кроме как для финансовых операций. Также снижается вероятность атак с использованием методов СИ, если номер этого телефона не используется для других целей кроме ИБ. Уменьшаются также вероятности применения других способов взлома, если это устройство ни при каких обстоятельствах не передается в чужие руки.

6. Использование простого телефона для финансовых операций объединяет достоинства п. 1 и 5.

7. Использование sim-карты иностранного оператора связи затрудняет злоумышленникам и даже спецслужбам процедуру получения дубликата, следовательно, снижаются вероятности кражи и клонирования sim-карты. Кроме того, мошенники неохотно совершают дорогие международные звонки, что снижает вероятность атак методами СИ. Также сам пользователь, вероятнее всего, не будет использовать дорогой роуминговый интернет для посещения сторонних интернет-ресурсов и открывать фишинговые ссылки, что снижает вероятность установки вредоносного программного обеспечения.

8. Обязательное отключение телефона на ночь позволит избежать звонков от мошенников в то время, когда критичность восприятия получаемой информации снижается, а доверие к собеседнику возрастает [16]. При этом снижается вероятность использования методов СИ. Неактивность телефона в ночное время уменьшит возможность несанкционированного доступа к нему через Wi-Fi соединение в случае взлома роутера.

9. Отключение функции геолокации в смартфоне затруднит определение местоположения для потенциальных мошенников и сделает пользователя менее уязвимым к атакам методами СИ.

10. Отсутствие у пользователя профиля в социальной сети также усложняет для злоумышленников сбор информации о нем и ее использование при атаках методами СИ (при этом вовсе не обязательно, чтобы доступ к аккаунту осуществлялся с того же устройства). Также снизятся вероятности установки вредоносного ПО, поскольку утверждение, что социальные сети являются «рассадниками» вредоносного ПО, не лишено оснований.

Методика оценки эффективности контрмер

Для оценки эффективности перечисленных мер был проведен опрос экспертов, которым было предложено оценить, как повлияет каждая из предлагаемых мер на ту или иную уязвимость. Подчеркнем, что в отличие от предыдущего опроса (опроса пользователей), здесь опрос проводился именно среди специалистов, знакомых с принципами организации и работы мобильной связи и др. Качественные (лингвистические) оценки, данные экспертами, были переведены в численные значения K, названное коэффициентом ослабления угрозы по шкале, приведенной в табл. 4. В табл. 5 представлены осредненные по всем экспертам значения К для каждой из предлагаемых контрмер и по каждой из рассмотренных уязвимостей.

Таблица 4

Ответ эксперта	K
никак не повлияет	1
повлияет незначительно	0,8
повлияет умеренно	0,5
повлияет значительно	0,2
полностью устранит	0

Индексы коэффициентов $K_1 ... K_{14}$ соответствуют номерам уязвимостей из табл. 3.

Для расчета эффективности вводимых контрмер необходимо перемножить все соответствующие коэффициенты K_i. Тогда результирующие коэффициенты ослабления угроз определяются как

$$K_i^* = \prod_j K_i^j \,. \qquad (4)$$

где K_i^j – коэффициенты из табл. 4, причем индекс i соответствует уязвимости, индекс j – контрмере (номер строки из табл. 4). Перемножаются только коэффициенты, соответствующие принятым контрмерам.

Таблица 5

№	Уязвимость / Контрмера	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	K_9	K_{10}	K_{11}	K_{12}	K_{13}	K_{14}
1	Отказ от смартфона в пользу телефона без ОС	0.7	1	1	1	0	0.23	0	0.23	0.3	0.8	0.05	1	0.3	1
2	Функция разблокировки по отпечатку пальца	0.28	0.88	1	0.88	1	1	1	0.38	0.38	1	1	1	0.88	1
3	Антивирусноее ПО на смартфоне	0.88	1	1	1	0.4	0.7	0.23	0.78	0.7	0.88	0.7	0.95	0.95	0.95
4	Использование именной sim-карты	0.95	0.65	0.23	0.78	1	1	1	1	1	1	1	1	1	1
5	Отдельный смартфона для финансовых операций	0.7	0.75	0.75	0.95	0.3	0.95	0.35	0.3	0.68	1	0.95	1	0.75	0.53
6	Отдельный телефон для финансовых операций	0.48	0.68	0.75	0.88	0.35	0.55	0.1	0.05	0.48	0.83	0.2	0.95	0.45	0.5
7	Использование роуминго-вой sim-карты	1	0.3	0.2	0.1	0.6	0.95	0.4	0.83	0.75	0.68	0.58	0.55	0.55	0.58
8	Обязательное отключение телефона на ночь	0.83	0.7	0.88	1	0.95	1	0.95	1	1	0.73	0.58	0.75	0.75	0.63
9	Отключение функции геолокации	0.95	1	1	1	1	1	1	0.95	1	1	1	0.95	0.95	0.85
10	Отсутствие профиля в социальной сети	0.88	0.95	0.83	0.95	1	1	1	1	1	1	0.95	1	1	0.7

Например, если пользователь установил антивирусное ПО на свой смартфон и пользуется sim-картой иностранного оператора (контрмеры 3 и 7), то уязвимость, вызванная потерей данных при переходе по фишинговой ссылке (столбец 7), будет оцениваться как:

$$K_7^* = K_7^3 \times K_7^7 = 0,23 \times 0,4 = 0,092.$$

Тогда уровень угрозы для всех уязвимостей с учетом принятых контрмер можно рассчитать как

$$CTh_{NEW} = 1 - \sum_{i=1}^{n} \left(1 - Th_i K_i^*\right). \quad (5)$$

Далее, применив выражение (3), можно вычислить риск, после чего оценить результирующую эффективность контрмер(ы) как

$$E = \frac{R_{OLD} - R_{NEW}}{R_{OLD}}. \quad (6)$$

Предложенные методики могут быть полезны для оценки эффективности не только мер, которые перечислены в данной статье, но и других, например предложенных в [17].

Выводы

1. Обобщены и проанализированы угрозы для пользователей ИБ, связанные с использованием телекоммуникационных сетей и средств связи. Следовательно, можно отметить, что для общего понимания угроз необходимо было наглядно показать все виды угроз, с которыми сталкивается ежедневно каждый пользователь ИБ.

2. Методом эвристического анализа и экспертных оценок предложена методика оценки уязвимости пользователя ИБ, обусловленная этими угрозами. Показано, что наибольшую угрозу представляют мобильные устройства с операционной системой, а также устройства, имеющие постоянный доступ к мобильной сети или Wi - Fi.

3. Также методом экспертных оценок обобщены способы повышения уровня защиты пользователей ИБ от угроз, связанных с использованием телекоммуникационных сетей и средств связи и предложена методика оценки их эффективности.

Список литературы:

1. Антипов И. Е., Найденова Д. Р. О численной оценки уязвимостей пользователей интернет-банкинга // Радіоелектроніка та молодь у XXI столітті, Харків, Україна, 2019. С. 152-153.

2. Названы основные способы кражи персональных данных россиян [Электронный ресурс]. Режим доступа: https://vz.ru/news/2019/7/13/987219.html

3. Операторы связи и ФСБ выступили против используемой в iPhone технологии [Электронный ресурс]. Режим доступа: https://www.rbc.ru/technology_and_media/08/04/2019/5ca8e3319a79470abf10b8ac?from=from_main

4. В компании Google рассказали об установленных еще до продажи вирусах в смартфонах с операционной системой Android. [Электронный ресурс]. Режим доступа: https://vz.ru/news/2019/6/10/981789.html

5. Шпион на границе: чем китайцы заражают телефоны туристов [Электронный ресурс]. Режим доступа: https://www.gazeta.ru/tech/2019/07/03/12473611/spying_china.shtml

6. Таможня США может проверять содержимое ваших девайсов, изымать их и даже запрашивать пароли [Электронный ресурс]. Режим доступа: http://nashiusa.com/novosti/tamojna-proverka-device/

7. СБУшник продавал данные о телефонных разговорах, в том числе известных людей [Электронный ресурс]. Режим доступа: https://inforesist.org/sbushnik-prodaval-dannye-o-telefonnyh-razgovorah-v-tom-chisle-izvestnyh-lyudej/

8. В Киеве банда торговала информацией из базы данных Нацполиции и МВД [Электронный ресурс]. Режим доступа: https://www.segodnya.ua/kiev/kaccidents/v-kieve-policeyskie-torgovali-informaciey-iz-bazy-dannyh-nacpolicii-i-mvd-1224346.html

9. Клонирование SIM-карт – так ли это просто? [Электронный ресурс]. Режим доступа: https://tech-geek.ru/sim-card-cloning/

10. Операции с SIM/ USIM-картами и номером [Электронный ресурс]. Режим доступа: http:// https://www.vodafone.ua/ru/support/sim-usim-card-operation

11. МТС на службе ФСБ? Как взломали аккаунты оппозиционеров в Telegram [Электронный ресурс]. Режим доступа: https://openrussia.org/notes/614328/

12. Три четверти мобильных приложений оказались небезопасными [Электронный ресурс]. Режим доступа: https://vz.ru/news/2019/6/19/983148.html

13. Как мошенники увели SIM-карту у киевского IT-аналитика и украли 285 000 грн. [Электронный ресурс]. Режим доступа: http://cripo.com.ua/investigations/kak-moshenniki-uveli-sim-kartu-u-kievskoj-it-analitika-i-ukrali-285-000-grn/

14. Мошенники придумали новый способ вламываться в «Приват-24» Электронный ресурс]. Режим доступа: https://minfin.com.ua/2017/09/28/30182177/

15. Методика оценки риска ГРИФ 2005 из состава Digital Security [Электронный ресурс]. Режим доступа: https://bugtraq.ru/library/security/grifarmet.html?k=9

16. Как отличить звонок мошенника от звонка сотрудника банка? [Электронный ресурс]. Режим доступа: https://aif.ru/money/mymoney/kak_otlichit_zvonok_moshennika_ot_zvonka_sotrudnika_banka

17. Антипов И. Е., Найденова Д.Р. Пути повышения защищенности абонента мобильной связи от определения местоположения // Радіотехніка та молодь у XXI столітті. Т. 3. С.113-114.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 07.02.2020

УДК 004.491.4 **DOI:10.30837/rt.2020.1.200.17**

Р.С. ГРИНЬОВ, О.В. СЄВЄРІНОВ, канд. техн. наук, А.В. ВЛАСОВ, канд. техн. наук.

МЕТОД ВИЯВЛЕННЯ ТА ПРОТИДІЇ ВІРУСАМ У ЗОБРАЖЕННЯХ ФОРМАТУ BMP

Вступ

З розвитком технологій нас оточує все більше технічних засобів, яким довіряється конфіденційна інформація. Створюються нові методики приховування і поширення комп'ютерних вірусів [1, 2]. Тому задача їх пошуку та протидії є актуальною не тільки для простих користувачів, а й для великих фірм та компанії. Для приховування комп'ютерних вірусів широко використовуються можливості стеганографії [3].

Саме тому, для забезпечення захисту даних користувачів було розроблено та досі створюються різні засоби захисту інформації. Наприклад, антивірусне програмне забезпечення, системи виявлення вторгнень (IDS), системи запобігання вторгнень (IPS), брандмауери та фаєрволи [4]. Проте навіть цих засобів може бути недостатньо для того, щоб захистити дані.

Метод подолання засобів захисту з використанням вразливостей графічних файлів формату BMP

Зловмисники додають до вірусів різні нові функції та розробляють нові методики приховування шкідливого коду, щоб подолати засоби захисту [5]. Зловмисники можуть впроваджувати вірусне програмне забезпечення в зображення для обходу антивірусних засобів, IDS/IPS і пісочниць. Перш ніж вірус буде запущений на комп'ютері співробітника, його проаналізує багато пристроїв (рис. 1).

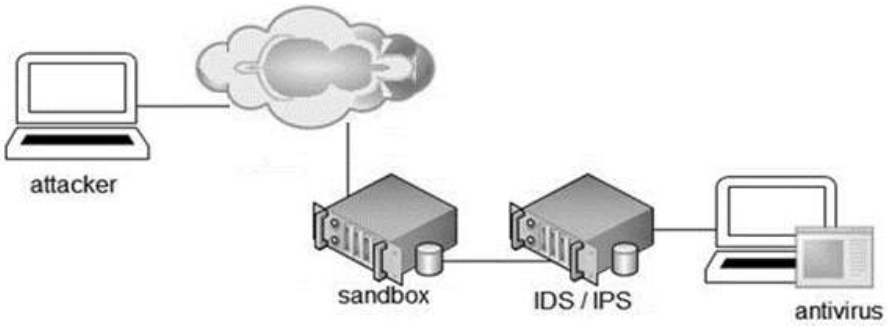


Рис. 1. Візуалізація шляху вірусу до цільового комп'ютера

Більшість методів аналізу файлів включають використання сигнатур вірусів і аналіз поведінки в пісочниці, а саме перевірку:

- поточного домену;
- запущених процесів;
- обсягу пам'яті;
- розміру диска;
- часу безвідмовної роботи.

Більшість пісочниць аналізуватимуть тільки виконувані файли, бібліотеки DLL, документи Word, аплети Java [6]. Більшість із засобів захисту просто не звертають уваги на зображення або інший безпечний тип файлу. Оскільки вважають, що немає причин витрачати процесорний цикл на аналіз зображення [7].

Так, наприклад, можна впровадити вірус у зображення формату BMP, таким чином, що користувач не помітить нічого підозрілого. Він не побачить ніяких дивних пікселів на зображенні. Справа в тому, що штучно зменшивши висоту зображення на декілька пікселів в заголовку можна приховати спотворені пікселі, але людина цього не помітить [8].

Ін'єкція можлива через те, що байти, які вказують на тип файлу, з яких і починається файл, BM в ASCII, в шістнадцятковому вигляді – 42 4D, при конвертації в інструкції асемблера не призводять до помилки виконання, а подальші 8 байт заголовка ніяк не впливають на інтерпретацію зображення [8]. Ці 8 байт можна заповнити будь-якими інструкціями асемблера, наприклад записати в них jmp-інструкцію, яка вкаже на вірус, що зберігається в зображенні. Щоб виконати код, що зберігається в зображенні, можна використати набір команд PowerShell.

Основна небезпека подібних зображень з вірусами полягає в тому, що для виявлення загрози необхідно використовувати нестандартні методи. Можна змінити налаштування засобів захисту, щоб вони перевіряли всі типи файлів, але це суттєво сповільнить або навіть повністю паралізує роботу всієї інформаційно-комунікаційної системи. Крім того, використання подібних інфікованих зображень може сильно ускладнити розбір інциденту інформаційної безпеки в організації. По-перше, системи безпеки можуть не відреагувати на вірус і виявити факт проникнення буде дуже складно. По-друге, якщо факт проникнення буде встановлений, буде майже неможливо з'ясувати як саме воно відбулося. Це обумовлено тим, що в першу чергу працівники відділу безпеки будуть з'ясовувати які виконувані файли, бібліотеки DLL, документи Microsoft Office, файли PDF потрапили в систему та використовувалися останнім часом. А через те, що не відома навіть приблизна дата проникнення, обсяг інформації, яку треба обробити значно зросте. В цьому випадку ніхто з працівників не буде досліджувати файли зображень.

Але аналіз показує, що віруси можуть заражати не тільки виконувані файли і динамічні бібліотеки, а й файли зображень, аудіо та відео.

Оскільки зображення неможна запустити як виконуваний файл, то і засоби захисту і технічні фахівці можуть легковажно ставитися до його вмісту та знехтувати цією загрозою. Однак такий файл може нести серйозну небезпеку. Необхідно уважно ставитися до налаштування систем запобігання вторгнень. І більш ретельно проводити розслідування інцидентів інформаційної безпеки.

Крім того, така вірусна атака може бути поєднана з HID-атаками, що робить її ще небезпечнішою [9]. Так, наприклад, зловмисник може запрограмувати мікроконтролер, щоб він при підключенні відкривав командний рядок, вводив та виконував команду PowerShell, що завантажить зображення та запустить вірус. Такий пристрій може бути замаскований під флеш-накопичувач, клавіатуру або інше периферійне обладнання [10].

HID-атаки

Використання HID-атак є рідкісним явищем для сучасного світу, хоча вони відомі досить давно. Шкідливі HID пристрої можуть бути різної форми та замасковані під різну апаратуру, проте всі вони виконують одні й ті ж завдання. Найчастіше вони виглядають, як звичайні флеш накопичувачі, проте насправді є HID пристроями і прикидаються в системі клавіатурою. Головна їх ідея полягає в тому, що клавіатура, як і решта HID пристроїв, є довіреними для системи та засобів захисту на відміну від виконуваних файлів, що перевіряються засобами захисту на наявність комп'ютерних вірусів. При підключенні подібного пристрою він починає виконувати запрограмовані дії. Наприклад, відкриває PowerShell та виконує команди, що завантажують зображення і виконують вірус, який знаходиться в ньому. З точки зору всіх систем захисту, це звичайний користувацький ввід команд через клавіатуру і він не є шкідливим, а пристрій – лише клавіатура. За допомогою шкідливих HID пристроїв зловмисник може скомпрометувати комп'ютерну систему без необхідності безпосередньо взаємодіяти з нею.

Методи виявлення вірусів у файлах зображень формату BMP

В першу чергу для протидії описаній в роботі атаці необхідно розроблювати нові засоби захисту та методи виявлення вірусів. А саме:

- необхідно, щоб антивірусні засоби захисту перевіряли файли зображень на наявність вірусів, в тому числі і за допомогою "масок";

- перевіряти файли зображень формату BMP на наявність будь-яких даних у зарезервованих полях заголовку відмінних від нулів. Якщо ці поля мають не нульові значення, це може означати, що у файл був впроваджений вірус;

- якщо поле “Size” в заголовку файлу не відповідає розміру файлу в байтах, це теж може свідчити про прихований шкідливий код;

- на основі кількості піксельних даних можна отримати інформацію про дійсний розмір зображення в пікселях, якщо він не відповідає ширині та висоті, які вказані в заголовку, це може свідчити про наявність вбудованого вірусу;

- також для виявлення шкідливого коду можна використовувати програми, що будуть визначати аномалії в зображенні. Так, при наявності великої кількості спотворених пікселів можна стверджувати про наявність в зображенні вірусу.

Суттєвим недоліком такого підходу є необхідність детального аналізу файлів та використання ресурсів обчислювальної системи. При великому навантаженні ІТС це може призвести до серйозних втрат працездатності та відмові в обслуговуванні. Крім того, для попередження подібних атак необхідно:

- чітко визначити перелік доступних інтернет-ресурсів для користувачів. Це унеможливить розміщення інфікованого зображення на web-ресурсах, до яких мають доступ зловмисники;

- фільтрувати та контролювати трафік організації. Якщо можливо, заборонити співробітникам завантажувати виконувані файли, скрипти, бібліотеки динамічних посилань (DLL). Крім того, завантажувати документи з невідомих джерел, що були створені в пакеті Microsoft Office та подібних, а також файли зображень формату BMP.

В ході дослідження було розроблено програму мовою Python, що перевіряє зарезервовані поля зображення BMP, поле SIZE, а також визначає справжню кількість пікселів та перевіряє зі значенням кількості пікселів по горизонталі та вертикалі, що зазначені в заголовку зображення.

При перевірці оригінального зображення не було виявлено жодних аномалій (рис. 2).

```
└── $ python BMP_CHECK.py
Введите путь к изображению: default.bmp
        [*] >>> Тип файла BM
        [+] >>> Файл является изображением формата BMP
        [*] >>> Размер файла в байтах указанный в заголовке 481078
        [+] >>> Настоящий размер файла в байтах 481078
        [+] >>> Поле SIZE в заголовке файла не было модифицированно
        [+] >>> Зарезервированное поле №1 = 0000
        [+] >>> Зарезервированное поле №2 = 0000
        [*] >>> Размер изображения указанный в заголовке: 800 x 600
        [*] >>> Изображение должно состоять из 480000 пикселей
        [*] >>> Положение пиксельных данных относительно начала файла в байтах 1
078
        [+] >>> Реальное количество пикселей 480000
```

Рис. 2. Перевірка оригінального зображення

При перевірці інфікованого зображення були виявлені аномалії за ключовими ознаками (рис. 3).

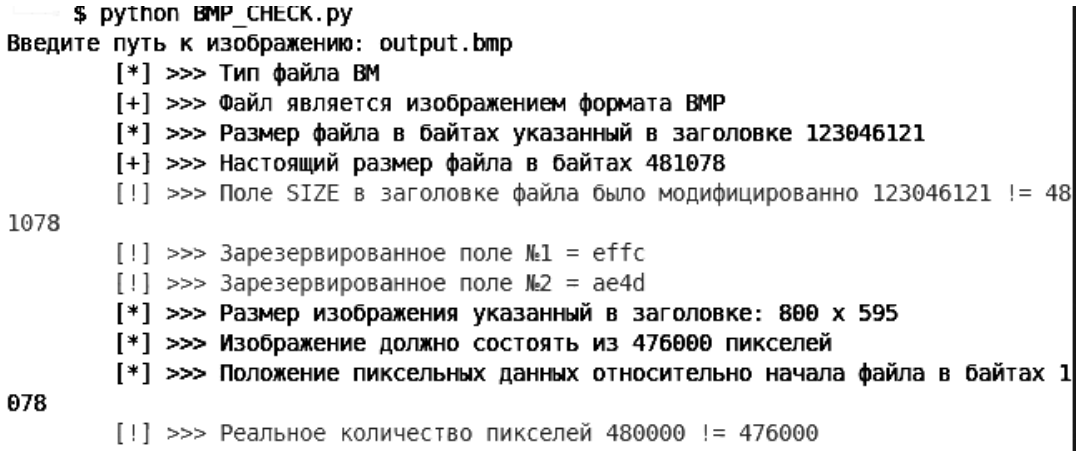


Рис. 3. Перевірка інфікованого зображення

Методи виявлення та протидії HID-атакам

Для виявлення та протидії HID-атакам необхідно:

- перевіряти придбане обладнання та обладнання після ремонту на наявність закладних пристроїв. Проводити періодичну перевірку існуючого обладнання;

- обмежити доступ до обладнання сторонніх осіб та працівників, які з ним не взаємодіють;

- необхідно, щоб при запуску PowerShell та CMD не тільки для адміністратора, але й будь-якого користувача було б необхідна обов'язкова автентифікація з використанням логіну та паролю;

- заборона на установку з'ємних пристроїв – реалізується за допомогою групової політики безпеки як для локальної машини та і для робочих станцій в домені. Однак при цьому не буде доступний "Plug'n'play";

- використання "білого списку" – списку довірених пристроїв. Однак слід враховувати, що пристрої ідентифікуються системою по зв'язці Vendor ID і Product ID, які можуть бути запрограмовані зловмисником і повністю відповідати вже зареєстрованим в системі. Таким чином, навіть блокування за "білим списком" не є абсолютним захистом;

- одним з найбільш ефективних засобів захисту від HID-атак є використання для виявлення та блокування евристичних методів аналізу, наприклад заснованих на аналізі зміни швидкості введення.

В ході дослідження була розроблена програма мовою Python, що виявляє та протидіє HID-атакам, аналізуючи швидкість введення тексту та її зміну. Якщо швидкість введення суттєво збільшилась і вона набагато вища за можливу людську, програма виявить атаку. Програма має чотири режими:

- коли атака буде виявлена, вона просто буде зареєстрована в журналі, без протидії;

- коли атака виявлена, кілька натискань клавіш будуть перервані (цього досить, щоб перервати будь-яку атаку, виглядає так, ніби нападник зробив помилку). Атака також буде зареєстрована в журналі;

- при виявленні атаки введення з клавіатури буде тимчасово відключено. Після того, як атака буде закінчена, введення з клавіатури знову буде дозволено. Атака також буде зареєстрована в журналі;

- при виявленні атаки блокує всі подальші натискання клавіш до тих пір, поки не буде введений правильний пароль. (Встановити пароль можна в файлі .conf). Атака також буде зареєстрована в журналі.

Програма не має графічного інтерфейсу. Після запуску програма функціонує як фоновий процес. Атака на комп'ютер під керуванням операційної системи Windows XP показана на

рис. 4. Варто зазначити, що до цієї атаки вразливі всі версії операційних системи сімейства Windows, Linux. MacOS також вразлива до цих атак.

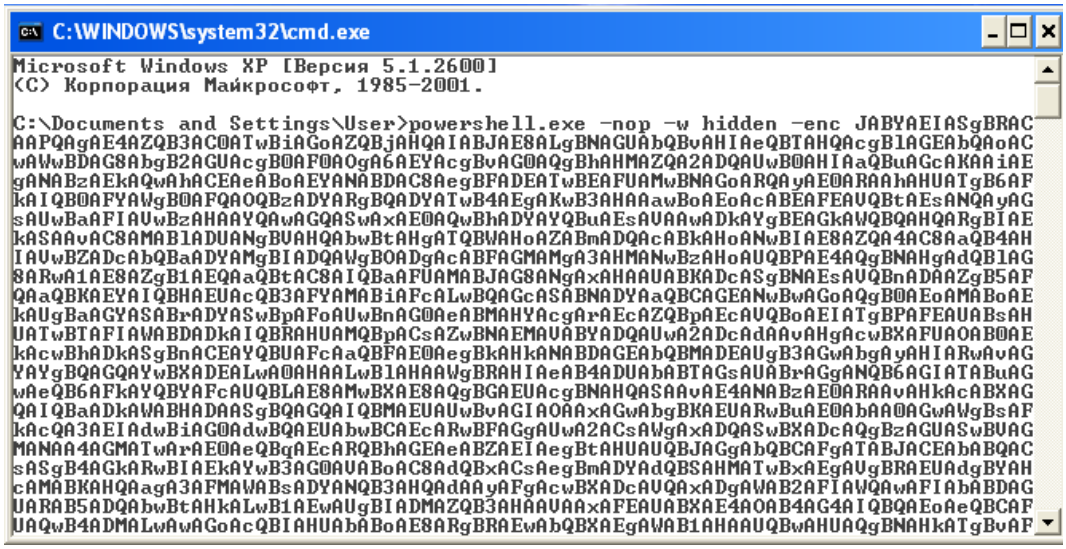


Рис. 4. Успішна атака на незахищену систему

Після запуску програми HID-атака була виявлена та знешкоджена (рис. 5).

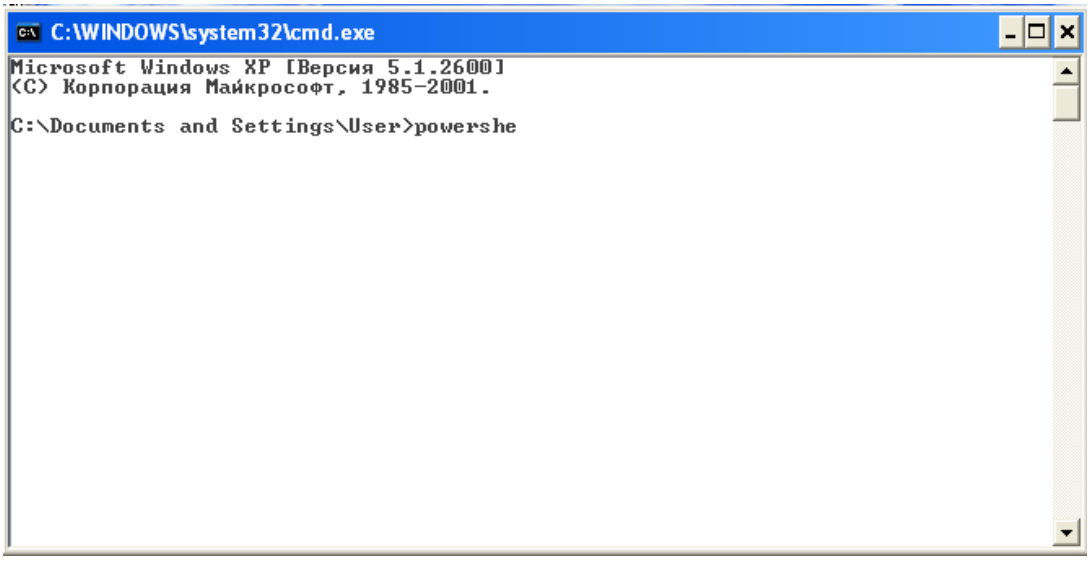


Рис. 5. Виявлена та знешкоджена атака за допомогою розробленої програми

Висновки

У ході досліджень розроблений та продемонстрований метод, що дозволяє виявити прихований вірус у зображеннях BMP. Створена програма для виявлення та протидії HID-атакам.

Проаналізувавши отримані результати, можна стверджувати, що даний метод виявлення прихованого вірусу дозволяє успішно виявити прихований шкідливий код у зображеннях формату BMP. Крім того, програма для захисту від HID-атак успішно виявила та знешкодила атаку.

За результатами випробувань можна стверджувати, що розроблені методи виявлення прихованого вірусного коду в зображенні формату BMP та протидії HID-атакам є більш ефективним для протидії цим атакам, ніж сучасні засоби захисту. Результати даної роботи мож-

на використовувати під час розробки засобів антивірусного захисту та комплексних засобів захисту ІТС та для їх модернізації з метою попередження подібних атак.

При цьому необхідно враховувати, що навіть звичайні файли з простою структурою без підтримки скриптів можуть становити серйозну загрозу. Тому необхідно розроблювати нові, більш ефективні засоби захисту.

Основна небезпека подібних зображень з вірусами полягає в тому, що для виявлення загрози необхідно використовувати нестандартні методи. Можна змінити налаштування засобів захисту, щоб вони перевіряли всі типи файлів, але це суттєво сповільнить або навіть повністю паралізує роботу всієї інформаційно-комунікаційної системи.

Список літератури:

1. Гриньов Р.С., Сєвєрінов О.В. Аналіз тенденцій вірусних загроз в Україні // Сучасні напрямки розвитку інформаційно-комунікаційних технологій та засобів управління : міжнар. конф. Харків, 2019. 100 с.

2. Гриньов Р.С. Аналіз статистики та особливостей розповсюдження вірусів в Україні // Сучасні напрямки розвитку інформаційно-комунікаційних технологій та засобів управління : міжнар. конф. Харків, 2019.

3. Pare. Virus spread over networks: Modeling, analysis, and control : Ph.D. Electrical & Computer Eng / University of Illinois at Urbana-Champaign, 2018.

4. Jingwei LEI. Virus program detection method, terminal, and computer readable storage medium. United States, 2018. 19 c.

5. Wen-Kwang Tsao. Detecting malicious code in sections of computer files / Wen-Kwang Tsao, Pinghuan Wu, Zipan Bai. United States, 2018. 15 c.

6. Lubomir Sikora. Swarm Virus, Evolution, Behavior and Networking / Lubomir Sikora, Ivan Zelinka. Berlin, 2017.

7. Carey Parker. Computer Security. North Carolina USA, 2018.

8. Гриньов Р.С., Севєрінов О.В. Аналіз небезпеки впровадження вірусного програмного забезпечення в зображення // Комп'ютерні та інформаційні системи і технології : міжнар. наук.-техн. конф. Харків, 2019. С. 75.

9. Гриньов Р.С., Сєвєрінов О.В. Шкідливий USB HID-емулятор // Радіоелектроніка та молодь у XXI столітті : міжнар. форум. Харків, 2018. С. 120-121.

10. Гриньов Р.С., Севєрінов О.В. Аналіз небезпеки апаратних закладних пристроїв // Радіоелектроніка та молодь у XXI столітті : міжнар. форум. Харків, 2019. С. 93-94.

11. Гриньов, Р. С., Сєвєрінов О. В. Метод подолання засобів захисту з використанням вразливостей графічних файлів формату BMP // Радіотехніка. 2019. Вип. 198. С. 192-202.

Харківський національний
університет радіоелектроніки

Надійшла до редколегії 11.01.2020

UDC 621.391.15:519.7 **DOI:10.30837/rt.2020.1.200.18**

O.V. TSYGANKOVA

ANALYZING OF POSSIBILITY OF USING ELGAMAL ALGORITHM WITH DETERMINISTIC EMBEDDING FOR KEY ENCAPSULATION

Introduction

Suppose some parties, A and B, use some symmetrical encryption algorithm (for example, AES) to encrypt their messages from A to B and from B to A. They get their secret keys from some Trusted Authority (TA). TA generates keys and then delivers them to correspondent users. The simplest and, may be, the optimal way to deliver the secret key to user A is to encrypt it (using some asymmetrical encryption algorithm) with A's public key and then to send it to A via public channel. Such procedure is called "key encapsulation".

Key encapsulation algorithms are widely used in the modern cryptography and represented in national and ISO/IEC standards of key encapsulations [1, 2].Building the key encapsulation algorithm [3], which may be used as a national standard, is an actual problem nowadays. Ukrainian cryptographers are also working on such standard [4]. Modified Elliptic Curve Integrated Encryption Scheme (ECIES), included in the ANSI X9.63, ISO/IEC 18033-2, IEEE 1363a and SECG SEC1 standards, was used in the project of national standard for key encryption.

In this article we discuss some alternative encryption algorithm on elliptic curve which also may be used for this purpose.

Generally speaking, we can use arbitrary asymmetric encryption algorithm for key encapsulation. One of the simplest and preferable algorithms is ElGamal encryption algorithm [5]. To use this algorithm on elliptic curve, we need algorithms for embedding key into point on elliptic curve and for retrieving it back. Several lines of work in both the number theory and cryptography literature have considered the problem of deterministically mapping field element to point on elliptic curve. However, only probabilistic algorithms of such embedding existed until 2016, when deterministic algorithm for hash embedding was proposed in [6]. But key embedding is much more complicated procedure than hash embedding.

In what follows we describe how this algorithm for key embedding can be built and then discuss the problems that appear if we want to use it in key encapsulation.

To formalize our problem, we need the next designations.

Let $E(F_p)$ be an elliptic curve over F_p given with the equation

$$E: y^2 = g(x), \text{ where } g(x) = x^3 + ax + b, \quad a,b \in F_p, ab \neq 0.$$

We assume that key length is n and for some large prime p we have $p > 2^n$. In this case we can consider vector k as binary representation of some element $k \in F_p$.

Our purpose is to build mapping $F_p \to E(F_p)$, which maps each element $k \in F_p$ into correspondent point $P_k \in E(F_p)$. Moreover, such mapping should be invertible for key retrieving from the point.

1. Classical ElGamal cryptosystem and its elliptic analogue

Classical ElGamal public-key encryption scheme was built in multiplicative group F_p^* for large prime p. Its security is based on the intractability of the discrete logarithm problem [7,8]. To understand the problem of key embedding into the elliptic curve point let us describe the basic ElGamal and Elliptic Curve ElGamal encryption schemes.

Let p be large prime, g be a generator of F_p^*.

Also suppose that party A has his private key a, $2 \le a \le p-2$, and correspondent public key $h = g^a \bmod p$.

Assume TA generates key k (for example, for AES encryption) and should deliver it to parties A and B using only public channels. Suppose TA uses classical ElGamal algorithm (in F_p^*) to encrypt the key k. In this case it does the next steps.

Algorithm 1.

Classical ElGamal algorithm (key encryption)

1. Generates random r, $2 \le r \le p-2$.
2. Evaluates $C_1 = g^r \bmod p$.
3. Evaluates $R = h^r \bmod p$.
4. Evaluates $C_2 = k \cdot R \bmod p$.
5. Forms ciphertext $C = (C_1, C_2)$ and sends it to A.

Then TA does the same procedure for user B, using B's private key.

When A obtains ciphertext $C = (C_1, C_2)$ he decrypts it and finds key k, using secret key a, as $k = C_1^{-a} \cdot C_2 \bmod p$. User B do the same with correspondent cipher text and his secret key.

These scheme can be easily transformed to correspondent elliptic analogue, but there exist some nuances. For example, we may mention Koblitz paper [9] where this analogue was firstly proposed. But the bottleneck of correspondent elliptic algorithm is the step 4 in Algorithm 1: we need k to be some point on elliptic curve. The remaining steps of the algorithm are directly transferred to elliptic case.

Let for large prime p the base point P of elliptic curve (EC) $E(F_p)$ has order n. Party A has his private key a, $2 \le a \le n-2$, and correspondent public key $G = aP$. TA generates key k and should deliver it to parties A and B using only public channels. Suppose TA uses ElGamal algorithm in over $E(F_p)$ to encrypt the key k embedded into point on elliptic curve K. In this case it does the next steps.

Algorithm 2.

EC ElGamal algorithm (key encryption)

1. Generates random r, $2 \le r \le n-2$.
2. Evaluates $C_1 = rP$.
3. Evaluates $C_2 = K + rG$.
4. Forms ciphertext $C = (C_1, C_2)$ and send it to A.

Then TA does the same procedure for user B, using B's private key.

A obtains cipher text $C = (C_1, C_2)$ and decrypts it using secret key a, as $K = C_2 - aC_1$. User B do the same with correspondent cipher text and his secret key.

To solve the problem of embedding key into point on elliptic curve and retrieving it, Koblitz in [9] proposed some probabilistic algorithm of embedding k into elliptic curve point. But usage of such algorithm makes system very complicated and inconvenient. That is why elliptic analogue of ElGamal algorithm is not used in practice till nowadays.

In the next paragraph we will build deterministic algorithm for key embedding into elliptic curve point. We also describe the inverse algorithm, i.e. the algorithm of retrieve key from elliptic curve point and proof the correctness of these algorithms.

2. Embedding algorithm justification

To build key embedding algorithm, we use the algorithm of hash imbedding into elliptic curve point, which was recently proposed by Boneh and others in [6]. We firstly describe the Boneh's algorithm and then explain how we can modify it for our purposes. Note that in our case we should be able not only to embed the key into point on the curve, but also to reveal it univocally after decryption.

Let for some $\xi \in F_p$ we have $\xi \notin Q_p$ (i.e. ξ is quadratic non-residue in F_p, Q_p is the set of all quadratic residues in F_p). Then for key $\xi \in F_p$ set $u_k = k^2 \xi$. Note that u_k is also quadratic non-residue in F_p, or another words $u_k \notin Q_p$. Note that we should exclude case $u_k = -1$, which may happened with negligible probability (only if $-1 \notin Q_p$ and $k^2 \bmod p = -\xi^{-1} \bmod p$).

Now find the value x_k such that the next equation holds:

$$g(u_k x_k) = u_k{}^3 g(x_k). \tag{1}$$

The equation (1) is equivalent to the equation

$$(u_k x_k)^3 + a u_k x_k + b = u_k{}^3 \left(x_k{}^3 + a x_k + b \right),$$

from where we obtain

$$x_k = b\left(u_k^3 - 1\right)\left(a u_k \left(1 - u_k^2\right)\right)^{-1}. \tag{2}$$

The equality (2) can be simplified as

$$x_k = b \cdot \frac{u_k^3 - 1}{a u_k \left(1 - u_k\right)^2} = \frac{b\left(u_k^2 + u_k + 1\right)}{-a u_k \left(u_k + 1\right)}$$

$$x_k = -\frac{b}{a} \cdot \left(\frac{u_k^2 + u_k + 1}{u_k^2 + u_k} \right)$$

$$x_k = -\frac{b}{a} \cdot \left(1 + \frac{1}{u_k{}^2 + u_k} \right) \tag{3}$$

For such x_k we have

$$g(x_k) g(u_k x_k) = g(x_k) u_k^3 g(x_k) =$$
$$= g(x_k)^2 u_k^3 = g(x_k)^2 \left(k^2 \xi\right)^3 = \left(g(x_k) k^3 \xi\right)^2 \xi$$

i.e. $g(x_k) g(u_k x_k)$ is a quadratic non-residue in F_p. It means that exactly one of the next two elements, $g(x_k)$ or $g(u_k x_k)$, is a quadratic residue in F_p, and the other is non-residue.

If $g(x_k) \notin Q_p$ then redefine $x_k \leftarrow u_k x_k$. In this case to retrieve u_k we use the equation

$$\frac{x_k}{u_k} = -\frac{b}{a} \cdot \left(1 + \frac{1}{u_k{}^2 + u_k} \right) \tag{4}$$

instead of (3).

Hence we have $g(x_k) \in Q_p$, so there exist two square roots from $g(x_k)$ in F_p, $y_{1,2} = \pm\sqrt{g(x_k)}$. Note that one of $y_{1,2}$ has least significant bit equal to 0 (i.e. $lsb = 0$), and other has $lsb = 1$. We can chose any of these two roots according to some predefined rule, for example, with $lsb = 0$ and define $y_k = y_1$, if $lsb\left(y_1\right) = 0$, and $y_k = y_2$, else. Therefore the point $P_k(x_k, y_k) \in E\left(F_p\right)$, correspondent to field element $k \in F_p{}^*$, was constructed and actually the mapping $F_p \to E\left(F_p\right)$ wasconstructed which implies that for any key $k \in F_p{}^*$ there exists correspondent point $P_k(x_k, y_k) \in E\left(F_p\right)$.

The common form for this mapping for key $k \in F_p$, some fixed $\xi \notin Q_p$, and $u_k = k^2\xi$ can be described as

$$P_k = \begin{cases} \left(x_k, \sqrt{g(x_k)}\right), if g(x_k) \in Q_p; \\ \left(u_k x_k, \sqrt{u_k^3 g(x_k)}\right), if g(x_k) \notin Q_p. \end{cases}$$

So we obtain the next algorithm for key embedding into elliptic curve point.

Algorithm 3.

Key embedding into elliptic curve point.

Input: $a, b, k, \xi \in F_p$, $\xi \notin Q_p$

1. Evaluate $u_k = k^2\xi$.
2. Evaluate $t_1 = lsb(u_k)$.
3. Evaluate $x_k = -\frac{b}{a}\left(1 + \frac{1}{u_k^2 + u_k}\right)$.
4. Evaluate $g_k = x_k^3 + ax_k + b$; $t_2 \leftarrow 0$.
5. If $g_k \notin Q_p$ then $x_k \leftarrow u_k x_k$, $t_2 \leftarrow 1$, and $g_k \leftarrow u_k^3 g_k$.
6. Evaluate $y_{1,2} = \sqrt{g(x_k)}$.
7. If $lsb(y_k) = 1$ then $y_k \leftarrow p - y_k$.
8. Evaluate $t_3 = lsb(k)$.

Output: $P_k(x_k, y_k)$, t_1, t_2, t_3.

The main problem which appears now is: how to reveal the key k from the point $P_k(x_k, y_k)$? If we solve it, we will have simple algorithm for key encapsulation based on ElGamal encryption algorithm.

Note that values t_1, t_2, t_3 in Algorithm 3 serve just for the solution of the problem. It is described in the next paragraph.

3. Algorithm of retrieving k from point $P_k(x_k, y_k) \in E(F_p)$

In what follows, we are going to build the algorithm for retrieving k. We use the equalities (3) and (4) for this purpose. From these equalities, we can get u_k as the solution of correspondent quadratic equation. In case when $g_k \in Q_p$ we use the equality (3) and obtain

$$(u_k^2 + u_k)\left(ab^{-1}x_k + 1\right) + 1 = 0;$$

$$u_k = \frac{-\left(ab^{-1}x_k + 1\right) \pm \sqrt{\left(ab^{-1}x_k + 1\right)^2 - 4\left(ab^{-1}x_k + 1\right)}}{2\left(ab^{-1}x_k + 1\right)};$$

$$u_k = \frac{-1 \pm \sqrt{\left(ab^{-1}x_k + 1\right) - 4}}{2};$$

$$u_k = \frac{p-1}{2}\left(-1 \pm \sqrt{\left(ab^{-1}x_k - 3\right)}\right).$$

In case when $g_k \notin Q_p$ the transformation $x_k \leftarrow u_k x_k$ was done in step 5 of Algorithm 3, so we get equality (4). Solving correspondent quadratic equation we get the value u_k as:

$$\frac{ab^{-1}x_k}{u_k}+1+\frac{1}{u_k\left(u_k+1\right)}=0;$$

$$u_k{}^2+u_k\left(ab^{-1}x_k+1\right)+\left(ab^{-1}x_k+1\right)=0;$$

$$u_k=\frac{-\left(ab^{-1}x_k+1\right)\pm\sqrt{\left(ab^{-1}x_k+1\right)^2-4\left(ab^{-1}x_k+1\right)}}{2};$$

$$u_k=\frac{p-1}{2}\left(ab^{-1}x_k+1\right)\left(1\pm\sqrt{1-4\left(ab^{-1}x_k+1\right)^{-1}}\right).$$

Now we can recover the value k from u_k.

Note that to get the value u_k uniquely we need the bit values t_1, t_2, t_3. from Algorithm 3. So we get the next Algorithm for key retrieving.

Algorithm 4.

Key retrieving from elliptic curve point.

Input: $x_k \in F_p$, $t_1, t_2, t_3 \in \{0,1\}$.

1. If $t_2=0$ then evaluate $u_k=\frac{p-1}{2}\left(-1\pm\sqrt{\left(ab^{-1}x_k-3\right)}\right)$ and choose u_k such that *lsb* (u_k) = t_1

else evaluate $u_k=\frac{p-1}{2}\left(ab^{-1}x_k+1\right)\left(1\pm\sqrt{1-4\left(ab^{-1}x_k+1\right)^{-1}}\right)$ and choose u_k such that *lsb* (u_k) = t_1.

2. Evaluate $k=\sqrt{-u_k}$

3. If *lsb(k)* $\neq t_3$. than evaluate $k=p-k$.

Output: k.

Conclusion

We described deterministic algorithms for key embedding into elliptic curve point and for key retrieving. These two algorithms give us an opportunity to use elliptic ElGamal algorithm for key encapsulation. Note that such algorithm is much more efficient (in speed) than one used in Belorussian national standard for Key Transport and is at least not less efficient than proposed Ukrainian project of standard for key encapsulation. But to make more definite conclusion about its merits and demerits, this algorithm should be analyzed in more detail. This analysis will be the topic of our further researches.

References:

1. СТБ 34.101.45-2013 Информационные технологии и безопасность. Алгоритм электронной цифровой подписи и транспорта ключа на основе эллиптических кривых. Available via https://apmi.bsu.by/resources/std.html/.
2. ISO/IEC 18033-2:2006 Information technology – Security techniques – Encryption algorithms / Part 2: Asymmetric ciphers.
3. Проект національного стандарту Інформаційні технології. Криптографічний захист інформації. Алгоритм шифрування коротких повідомлень, що ґрунтується на скручених еліптичних кривих Едвардса. Available via http://crypton.ua/images/Проект_стандарту.pdf
4. V.Shoup. A Proposal for an ISO Standard for Public Key Encryption. Preprint, December 2001. Available via https://www.shoup.net/papers/iso-2.pdf
5. Wenbo Mao. Modern Cryptography: Theory and Practice. PrenticeHall, 2003. 707 p.
6. Wahby Riad S. and Dan Boneh. Fast and simple constant-time hashing to the BLS12-381 elliptic curve // IACR Cryptologye Print Archive. 2019. 403 p.
7. P. van Oorschot S. Vanstone, A. Menezes. Handbook of Applied Cryptography. CRC Press, 1996.
8. W. Diffie, M. Hellman. New directions in cryptography // IEEE Trans. Inform. Theory. 1976. Vol. IT-22. P. 472-492,
9. Neal Koblitz. Elliptic Curve Cryptosystems. January 1987. Vol. 48. Number 177. P. 203-209.

National Technical University of Ukraine
"Igor Sikorsky KPI",
Institute of Physics and Technology

Received 09.02.2020

РЕФЕРАТЫ РЕФЕРАТИ ABSTRACTS

ПЕРСПЕКТИВНІ МЕТОДИ ТА СИСТЕМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

ПЕРСПЕКТИВНЫЕ МЕТОДЫ И СИСТЕМЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

PERSPECTIVE METHODS AND SYSTEMS OF CRYPTOGRAPHIC INFORMATION PROTECTION

УДК 004.056.55

Обґрунтування перспективного постквантового національного стандарту електронного підпису на основі решіток / *А.М. Олексійчук, В.А. Кулібаба, М.В. Єсіна, С.О. Кандій, Є.В. Острянська, І.Д. Горбенко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 5 – 14.

Важливою особливістю постквантового періоду у криптографії є суттєва невизначеність щодо вихідних даних для криптоаналізу та протидії в частині можливостей квантових комп'ютерів, їх математичного та програмного забезпечень, а також застосування квантового криптоаналізу до існуючих криптоперетворень та криптопротоколів. В якості основних методів обрано математичні методи електронного підпису (ЕП), що пройшли суттєвий аналіз та обґрунтування в процесі широких досліджень криптологами та математиками на найвищому рівні. Проаналізовано існуючі алгоритми електронного підпису на основі решіток 2-го етапу конкурсу NIST. Розглядається можливість використання постквантового механізму електронного підпису на основі алгебраїчних решіток у якості постквантового національного стандарту електронного підпису. У якості такого алгоритму електронного підпису пропонується використовувати постквантовий алгоритм Crystals-Dilithium. Розглядається даний алгоритм та обґрунтовується можливість його застосування, параметри алгоритму та правила їх побудування. Аналізуються відмінності та особливості безпечної реалізації алгоритму в порівнянні з 1-м етапом. Проводиться аналіз та робиться висновок, що алгоритм Crystals-Dilithium може бути взятий за основу, одним із кандидатів для розробки національного стандарту електронного підпису з використанням стандартизованих в Україні криптографічних алгоритмів, таких як функція гешування, що описується у ДСТУ 7564:2014. На погляд авторів, національний стандарт України постквантового періоду повинен включати в себе мінімум три алгоритми, що базуються на різних видах математичних перетворень, що визнані світовим криптографічним співтовариством як такі, що можуть забезпечувати необхідний рівень стійкості в умовах квантового криптоаналізу.

Ключові слова: електронний підпис; постквантовий стандарт; алгебраїчні решітки.

Табл. 1. Іл. 3. Бібліогр.: 27 назв.

УДК 004.056.55

Обоснование перспективного постквантового национального стандарта электронной подписи на основе решеток / *А.Н. Алексейчук, В.А. Кулибаба, М.В. Есина, С.А. Кандий, Е.В. Острянская, И.Д. Горбенко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 200. С. 5 – 14.

Важной особенностью постквантового периода в криптографии является существенная неопределенность относительно исходных данных для криптоанализа и противодействия в части возможностей квантовых компьютеров, их математического и программного обеспечения, а также применение квантового криптоанализа к существующим криптопреобразованиям и криптопротоколам. В качестве основных методов выбраны математические методы электронной подписи (ЭП), прошедшие существенный анализ и обоснование в процессе широких исследований криптологами и математиками на высшем уровне. Анализируются существующие алгоритмы электронной подписи на основе решеток 2-го этапа конкурса NIST. Рассматривается возможность использовать постквантовый механизм электронной подписи на основе алгебраических решеток в качестве постквантового национального стандарта электронной подписи. В качестве такого алгоритма электронной подписи предлагается использовать постквантовый алгоритм Crystals-Dilithium. Рассматривается данный алгоритм и обосновывается возможность его применения. Рассматриваются параметры алгоритма и правила их построения. Проводится анализ различий и особенностей безопасной реализации алгоритма по сравнению с 1-м этапом. Проводится анализ и делается вывод, что алгоритм Crystals-Dilithium может быть взят за основу, одним из кандидатов для разработки национального стандарта электронной подписи с использованием стандартизированных в Украине криптографических алгоритмов, таких как функция хеширования, что описывается в ДСТУ 7564: 2014. На взгляд авторов, национальный стандарт Украины постквантового периода должен включать в себя минимум три алгоритма, основанные на различных видах математических преобразований, которые признаны мировым криптографическим сообществом как такие, которые могут обеспечивать необходимый уровень устойчивости в условиях квантового криптоанализа.

Ключевые слова: электронная подпись; постквантовый стандарт; алгебраические решетки.

Табл. 1. Ил. 3. Библиогр.: 27 назв.

UDC 004.056.55

Substantiation of promising post-quantum national lattice-based electronic signature standard / *A.M. Oleksiychuk, V.A. Kulibaba, M.V. Yesina, S.O. Kandy, E.V. Ostryanska, I.D. Gorbenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №200. P. 5 – 14.

An important feature of the post-quantum period in cryptography is the significant uncertainty about the input data for cryptanalysis and counteracting the capabilities of quantum computers, their mathematical and software, and the application of quantum cryptanalysis to existing cryptoprotocols and cryptotransformations. Mathematical electronic signature (ES) methods have been selected as the main methods in the work, which have undergone significant analysis and substantiation in the process of extensive research by cryptologists and mathematicians at the highest level. The article analyzes the existing electronic signature algorithms based on the lattices of stage 2 of the NIST competition. The possibility of using the post-quantum electronic signature mechanism based on algebraic lattices as the post-quantum national electronic signature standard is considered. It is proposed to use the post-quantum Crystals-Dilithium algorithm as such electronic signature algorithm. The article considers this algorithm and substantiates the possibility of its application. The algorithm parameters and rules for their construction are considered. The differences and features of safe implementation of the algorithm in comparison with stage 1 are analyzed. The analysis is conducted and it is concluded that the Crystals-Dilithium algorithm can be taken as one of the candidates for the development of a national electronic signature standard using cryptographic algorithms, standardized in Ukraine, such as the hashing function described in DSTU 7564:2014. According to the authors of the article, the post-quantum period national standard of Ukraine should include at least 3 algorithms based on different types of mathematical transformations, which are recognized by the world cryptographic community as those that can provide the necessary level of stability in the conditions of quantum cryptanalysis.

Key words: electronic signature; post-quantum standard; algebraic lattices.

1 tab. 3 fig. Ref: 27 items.

УДК 004.056.55

Оптимізація алгоритму множення поліномів для NTRU-подібних алгоритмів / *О.Г. Качко, Ю.І. Горбенко, В.А. Пономар, М.В. Єсіна, С.О. Кандій* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 15 – 24.

Наразі актуальною стала проблема криптографічного захисту від класичних та потенційних криптоаналітичних атак з використанням квантового комп'ютера та квантової математики. Розуміючи цю проблему, технологічно розвинені держави направляють суттєві зусилля на аналіз криптографічної стійкості існуючих стандартів криптографічного захисту інформації у постквантовий період та ведуть пошук щодо створення постквантових стандартів асиметричної криптографії. Практичне вирішення цієї проблеми здійснюється на світовому рівні в процесі проведення NIST США міжнародного конкурсу. Як показують попередні дослідження, надійною математичною основою, на якій можуть бути створені постквантові АСШ та ПІК, нині вважаються алгебраїчні решітки. NTRU-подібні алгоритми – клас алгоритмів криптоперетворень, які в основному задовольняють вимогам постквантової криптографії. В NTRU-подібних алгоритмах асиметричних криптоперетворень основними складовими є алгоритми генерування ключів та виконання прямих та зворотних криптографічних перетворень. Ряд авторів сьогодні зосереджені на оптимізації множення поліномів для цих алгоритмів за критерієм часової складності. Особливою вимогою до них є незалежність часу виконання операції множення від самих поліномів, що робить неможливим здійснювати атаку сторонніми каналами. В роботі пропонується використання алгоритмів NTT та Тоома – Кука. Запропоновано нове рішення цієї проблеми, яке дозволило отримати прискорення практично в два рази при забезпеченні константного часу множення поліномів. Мета статі – оптимізація алгоритму множення поліномів за критерієм часової складності, який використовується для генерування ключів та виконання прямих та зворотних криптографічних перетворень АСШ та ПІК на алгебраїчних решітках.

Ключові слова: NTRU, NTRUPrime; множення поліномів; оптимізація; константний час.

Табл. 3. Бібліогр.: 18 назв.

УДК 004.056.55

Оптимизация алгоритма умножения полиномов для NTRU-подобных алгоритмов / *Е.Г. Качко, Ю.И. Горбенко, В.А. Пономарь, М.В. Есина, С.А. Кандий* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 200. С. 15 – 24.

Сегодня актуальной стала проблема криптографической защиты от классических и потенциальных криптоаналитических атак с использованием квантового компьютера и квантовой математики. Понимая эту проблему, технологически развитые государства направляют существенные усилия на анализ криптографической стойкости существующих стандартов криптографической защиты информации в постквантовый период и ведут исследования по созданию постквантовых стандартов асимметричной криптографии. Практическое решение этой проблемы осуществляется на мировом уровне в процессе проведения NIST США международного конкурса. Как показывают предварительные исследования, надежной математической основой, на которой могут быть созданы постквантовые АСШ и ПИК, сейчас считаются алгебраические решетки. NTRU-подобные алгоритмы – класс алгоритмов криптопреобразования, которые в основном удовлетворяют требованиям постквантовой криптографии. В NTRU-подобных алгоритмах асимметричных криптопреобразований основными составляющими являются алгоритмы генерации ключей и выполнения прямых и обратных криптографических преобра-

зований. Ряд авторов сосредоточены на оптимизации умножения полиномов для этих алгоритмов по критерию временной сложности. Особым требованием к ним является независимость времени выполнения операции умножения от самых полиномов, что делает невозможным осуществлять атаку сторонними каналами. В работе предлагается использовать алгоритмы NTT и Тоома – Кука. Предложено новое решение этой проблемы, которое позволило получить ускорение практически в два раза при обеспечении константного времени умножения полиномов. Цель статьи – оптимизация алгоритма умножения полиномов по критерию временной сложности, который используется для генерирования ключей и выполнения прямых и обратных криптографических преобразований АСШ и ПИК на алгебраических решетках.

Ключевые слова: NTRU, NTRUPrime; умножение полиномов; оптимизация; константное время.

Табл. 3. Библиогр.: 18 назв.

UDC 004.056.55

Optimization of polynomial multiplication algorithm for NTRU-like algorithms / *O.G. Kachko, Yu.I. Gorbenko, V.A. Ponomar, M.V. Yesina, S.O. Kandiy* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №200. P. 15 – 24.

The problem of cryptographic protection against classical and potential crypto-analytic attacks with the use of quantum computer and quantum mathematics has become an urgent issue. Understanding this problem, technologically advanced states are making significant efforts to analyze the cryptographic stability of existing standards for cryptographic information security in the post-quantum period and are seeking to establish post-quantum standards for asymmetric cryptography. A practical solution to this problem is being pursued globally during the NIST USA international competition. As previous studies have shown, algebraic lattices are now considered to be a reliable mathematical basis on which post-quantum asymmetric encryptions and PIK can be created. NTRU-like algorithms are a class of crypto-transformations algorithms that satisfy basically the requirements of post-quantum cryptography. Algorithms for key generation direct and reverse cryptographic transformations are the basic components in NTRU-like algorithms for asymmetric crypto-transformations. A number of authors today focus on optimizing polynomial multiplication for these algorithms by the criterion of time complexity. A special requirement for them is the independence of the time of the multiplication operation from the polynomials themselves, which makes it impossible to attack by side channels. This paper proposes the use of the NTT and Toom-Kuk algorithms. It proposes a new solution to this problematic issue, which made it possible to obtain an acceleration of almost 2 times while providing a constant polynomial multiplication time. The objective of this article is to optimize the polynomial multiplication algorithm by the time complexity criterion, used to generate keys and perform direct and reverse cryptographic transformations of asymmetric encryptions and PIK on algebraic lattices.

Key words: NTRU, NTRUPrime; multiplication of polynomials; optimization; constant time.

3 tab. Ref.: 18 items

УДК 621.391:519.2

Рандомізована симетрична криптосистема Мак-Еліса на основі узагальнених кодів Ріда-Соломона / *О.С. Шевчук* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 25 – 36.

Однією з актуальних проблем сучасної криптографії є створення практичних пост квантових криптосистем, стійкість яких базується на складності розв'язання єдиної обчислювально складної задачі, аналогічно тому як стійкість криптосистеми RSA базується на складності факторизації цілих чисел. Перспективний клас таких криптосистем утворюють кодові криптосистеми, найпершою асиметричною з яких є криптосистема Мак-Еліса. Дану роботу присвячено створенню та дослідженню симетричної версії криптосистеми Мак-Еліса, що будується на основі узагальнених кодів Ріда-Соломона (УРС). Вибір цих кодів зумовлено тим, що вони існують для всіх природних значень параметрів (довжини та вимірності коду) і є максимально дистанційно роздільними, що дозволяє в широких межах змінювати характеристики відповідних криптосистем. Крім того, для зазначених кодів відомі дуже швидкі алгоритми декодування (до половини кодової відстані та, навіть, за її межами). Нарешті, асиметричні криптосистеми, побудовані на основі кодів УРС, є нестійкими, оскільки для них існують ефективні алгоритми відновлення секретних ключів за відкритими.

Запропоновано симетричну кодову криптосистему, що є більш ефективнивною (за довжиною секретного ключа при заданих вимогах до стійкості) в порівнянні з криптосистемою LPN-C. Отримано оцінку стійкості запропонованої криптосистеми відносно атаки з підібраним відкритим текстом та запропоновано алгоритм вибору параметрів для побудови цієї криптосистеми. Проведено порівняння запропонованої криптосистеми з криптосистемою LPN-C за довжиною ключа при заданій нижній межі стійкості відносно розглянутої атаки.

Ключові слова: постквантова криптографія; кодова криптосистема; криптосистема Мак-Еліса; узагальнений код Ріда-Соломона; криптосистема LPN-C; система лінійних рівнянь зі спотвореними правими частинами.

Табл. 4. Бібліогр.: 18 назв.

УДК 621.391:519.2

Рандомизированная симметричная криптосистема Мак-Елиса на основе обобщенных кодов Рида-Соломона / *О.С. Шевчук* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 200. С. 25 – 36.

Одной из актуальных проблем современной криптографии является создание практичных постквантовых криптосистем, стойкость которых базируется на сложности решения одной вычислительно сложной задачи, аналогично тому как стойкость криптосистемы RSA базируется на сложности факторизации целых чисел. Пер-

спективный класс таких криптосистем образуют кодовые криптосистемы, первой асимметричной из которых есть криптосистема Мак-Элиса. Работа посвящена созданию и исследованию симметричной версии криптосистемы Мак-Элиса, которая строится на основе обобщенных кодов Рида-Соломона. Выбор этих кодов обусловлен тем, что они существуют для всех естественных значений параметров (длины и размерности кода) и являются максимально дистанционно разделимыми, что позволяет в широких пределах изменять характеристики соответствующих криптосистем. Кроме того, для указанных кодов известны очень быстрые алгоритмы декодирования. Наконец, асимметричные криптосистемы, построенные на основе обобщенных кодов Рида-Соломона, являются нестойкими, поскольку для них существуют эффективные алгоритмы восстановления секретных ключей по открытым.

Предложена симметричная кодовая криптосистема, более эффективная (с точки зрения длины секретного ключа при заданных требованиях к стойкости) по сравнению с криптосистемой LPN-C. Получена оценка стойкости предложенной криптосистемы относительно атаки с подобранным открытым текстом и предложен алгоритм выбора параметров для построения этой криптосистемы. Проведено сравнение предложенной криптосистемы с криптосистемой LPN-C по длине ключа при заданной нижней границе стойкости относительно рассматриваемой атаки.

Ключевые слова: постквантовая криптография; кодовая криптосистема; криптосистема Мак-Элиса; обобщенный код Рида-Соломона; криптосистема LPN-C; система линейных уравнений с искаженными правыми частями.

Табл. 4. Библиогр.: 18 назв.

UDC 621.391:519.2

Randomized symmetric McEliece cryptosystem based on generalized Reed-Solomon codes / *O.S. Shevchuk* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №200. P. 25 – 36.

One of the actual problems of modern cryptography is the design of practical post-quantum cryptosystems whose security is based on the complexity of solving one computationally challenging problem, in the same way as the security of the RSA cryptosystem is based on the complexity of integer factorization. A promising class of such cryptosystems is formed by code-based cryptosystems the first asymmetric of which is the McEliece cryptosystem. The purpose of this work is to design and research a symmetric version of the McEliece cryptosystem based on generalized Reed-Solomon codes. These codes were chosen because they exist for all natural values of the parameters (the length and dimension of the code) and they are maximal distance separable allowing a wide range to change the characteristics of the relevant cryptosystems. In addition, very fast decoding algorithms are known for these codes. Asymmetric cryptosystems based on the generalized Reed-Solomon codes are not secure because for them there are efficient algorithms for recovering private keys from public keys.

A symmetric code cryptosystem is proposed that is more efficient (in terms of the length of the secret key for given security requirements) compared to the LPN-C cryptosystem. An estimate of the security of the proposed cryptosystem relative to an attack with the chosen plaintext is obtained and an algorithm for selecting parameters for constructing this cryptosystem is proposed. The proposed cryptosystem is compared with the LPN-C cryptosystem along the key length for a given lower limit of security to the attack in question.

Key words: post-quantum cryptography; code-based cryptosystem; McEliece cryptosystem; generalized Reed-Solomon code; LPN-C cryptosystem; system of noised linear equations.

4 tab. Ref.: 18 items.

УДК 621.391.15:519.7

Алгоритми і оцінки складності обчислень 3- і 5-ізогеній суперсингулярних кривих Едвардса / *А.В. Бессалов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 37 – 50.

Дано аналіз властивостей і умов існування 3- і 5-ізогеній повних і квадратичних суперсингулярних кривих Едвардса над полями непарної характеристики $p>3$. Для задачі інкапсуляції ключів на основі алгоритму постквантової криптографії SIDH пропонується використовувати ізогенії мінімального непарного ступеня 3 і 5, що дозволяє обійти проблему особливих точок 2-го і 4-го порядків, які характерні для 2-ізогеній класів нециклічних кривих Едвардса. Дано огляд основних властивостей класів кривих Едвардса. Проаналізовано властивості ізогеній непарних степенів кривих Едвардса з одним параметром d в афінних координатах, приведено приклади їх обчислення. Відомі формули 3- і 5-ізогеній в афінних координатах трансформовані в проективні координати. Для зростання швидкості обчислення ізогеній застосовується лише x-координата афінної точки кривої. Отримано формули для координат і оцінок складності обчислень 3-ізогеній у класах повних і квадратичних кривих Едвардса у проективних координатах. Для ядра 5-го порядку параметр d кривої вдалось виразити через x-координати точок ядра, що дозволило отримати не залежні від d формули для координат 5-ізогеній. Проведено порівняльний аналіз складності чотирьох алгоритмів обчислення координат 5-ізогеній. Побудовані алгоритми обчислення 3- і 5-ізогеній в класах повних і квадратичних суперсінгулярних кривих Едвардса. Розглянуто деякі вимоги до параметрів криптосистеми.

Ключові слова: крива в узагальненої формі Едвардса; повна крива Едвардса; скручена крива Едвардса; квадратична крива Едвардса; порядок кривої; порядок точки; ізоморфізм; ізогенія; степінь ізогенії; ядро ізогенії; квадратичний лишок; квадратичний не лишок.

Бібліогр.: 11 назв.

УДК 621.391.15:519.7

Алгоритмы и оценки сложности вычислений 3- и 5-изогений суперсингулярных кривых Эдвардса / *А.В. Бессалов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 200. С. 37 – 50.

Дан анализ свойств и условий существования 3- и 5-изогений полных и квадратичных суперсингулярных кривых Эдвардса над полями нечетной характеристики $p>3$. Для задачи инкапсуляции ключей на основе алгоритма постквантовой криптографии SIDH предложено использовать изогении минимальных нечетных степеней 3 и 5, что позволяет обойти проблему особых точек 2-го и 4-го порядков, характерную для 2-изогений классов нециклических кривых Эдвардса. Приведен обзор основных свойств классов кривых Эдвардса. Дан анализ свойств изогений нечетных степеней кривых Эдвардса с одним параметром *d* в аффинных координатах, приведены примеры их вычисления. Известные формулы 3- и 5-изогений в аффинных координатах трансформированы в проективные координаты. Для увеличения скорости вычисления изогений используется лишь *x*-координата аффинной точки кривой. Получены формулы для координат и оценок сложности вычислений 3-изогений в классах полных и квадратичных кривых Эдвардса в проективных координатах. Для ядра 5-го порядка параметр *d* кривой удалось выразить через *x*-координаты точек ядра, что позволило получить не зависящие от *d* формулы для координат 5-изогений. Проведен сравнительный анализ сложности четырех алгоритмов вычисления координат 5-изогений. Построены алгоритмы вычисления 3- и 5-изогений в классах полных и квадратичных суперсингулярных кривых Эдвардса. Рассмотрены некоторые требования к параметрам криптосистемы.

Ключевые слова: кривая в обобщенной форме Эдвардса; полная кривая Эдвардса; скрученная кривая Эдвардса; квадратичная кривая Эдвардса; порядок кривой; порядок точки; изоморфизм; изогения; степень изогении; ядро изогении; квадратичный вычет; квадратичный невычет.

Библиогр.: 11 назв.

UDC 621.391.15:519.7

Algorithms and complexity evaluation of 3- and 5-isogeny calculation of super singular Edwards curves / *A.V. Bessalov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №200. P. 37 – 50.

The properties and existence conditions of 3- and 5-isogenies for complete and quadratic super singular Edwards curves over the fields of p>3 odd characteristic are analyzed. It is proposed to use the minimum odd degrees 3- and 5—isogenies for the task of keys encapsulation based on the SIDH algorithm of post quantum cryptography, which allows bypassing the problem of special points of the 2nd and 4th orders. These points always arise on 2-isogenies for the classes of noncyclic Edwards curves. A review of the main properties of the Edwards curve classes is given. An analysis of the properties of isogenies of odd degrees of Edwards curves with one parameter *d* in affine coordinates and examples of their calculation are given The known formulas of 3- and 5-isogeny in affine coordinates are transformed into projective coordinates. To increase the rate of isogeny calculation, only the *x*-coordinate of the affine point of the curve is used. Formulas for the coordinates and complexity evaluation for 3-isogeny calculations in the classes of complete and quadratic Edwards curves in projective coordinates are obtained. The parameter *d* of the curve was expressed in terms of the *x*-coordinates of the points of the nucleus for the 5th order nucleus, which allowed us to obtain formulas independent of *d* for the coordinates of 5-isogenies. A comparative analysis of the complexity of 4 algorithms for calculating the coordinates of 5 isogenies is carried out. Algorithms for computing 3- and 5-isogenies in the classes of complete and quadratic super singular Edwards curves are constructed. Some requirements for the parameters of the cryptosystem are considered.

Key words: Edwards curve in generalized form; complete Edwards curve; twisted Edwards curve; quadratic Edwards curve; curves order; points order; isomorphism; isogeny; isogeny kernel; square; non square.

Ref.: 11 items.

УДК 621.3.06

Дослідження продуктивності малоресурсного блокового шифру «Кипарис» на різних платформах / *М.Ю. Родінко, Р.В. Олійников* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 51 – 57.

Блоковий шифр «Кипарис» є малоресурсним алгоритмом, що представляє собою мережу Фейстеля з ARX-перетворенням у якості циклової функції. Блоковий шифр «Кипарис» підтримує довжину блока та ключа 256 та 512 біт. У статті досліджено продуктивність малоресурсних блокових шифрів «Кипарис-256» і «Кипарис-512» та порівняно з продуктивністю інших відомих блокових шифрів таких, як AES-256, SPECK-64/128, SPECK-128/128, SPARX-128/128, ДСТУ ГОСТ 28147: 2009. Продуктивність оцінювалась на платформах Windows, Linux та Android шляхом вимірювання швидкості зашифрування в режимі простої заміни, у Мбіт/с. Блоковий шифр «Кипарис» продемонстрував високу продуктивність на всіх досліджуваних програмно-апаратних платформах. На платформі Windows 10 з 32-бітовою архітектурою найкращий результат показав шифр «Кипарис-256» (майже 3,5 Гбіт/с). На платформі Windows 10 з 64-бітовою архітектурою найкращий результат показав шифр «Кипарис-512» (майже 5 Гбіт/с). На платформі Linux з 64-бітовою архітектурою блоковий шифр «Кипарис-256» показав надвисокий результат зі швидкодії (понад 8 Гбіт/с). На платформі Android найкращими також були блокові шифри «Кипарис-256» та «Кипарис-512» (1,3 Гбіт/с та 1 Гбіт/с відповідно). З точки зору продуктивності та зручності реалізації на різних програмно-апаратних платформах алгоритм «Кипарис» має ряд переваг: два варіанти шифру («Кипарис-256» та «Кипарис-512») орієнтовані на 32-бітову та 64-бітову архітектури відповідно; висока швидкодія та компактна реалізація перетворень незалежно від платформи, що використовується (сервер, робоча станція або мобільний пристрій); мінімальний необхідний об’єм пам’яті для швидкодію-

чої реалізації, відсутність таблиць передобчислень; можливість організації ефективних захищених високошвидкісних каналів зв'язку між мобільними системами та серверами, у тому числі тими, що використовують апаратні прискорювачі.

Ключові слова: блоковий шифр; малоресурсна криптографія; швидкість зашифрування; ARX-перетворення; мережа Фейстеля.

Табл. 5. Іл. 2. Бібліогр.: 18 назв.

УДК 621.3.06

Исследование производительности малоресурсного блочного шифра «Кипарис» на разных платформах / *М.Ю. Родинко, Р.В. Олейников* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 200. С. 51 – 57.

Блочный шифр «Кипарис» является малоресурсным алгоритмом, который представляет собой сеть Фейстеля с ARX-преобразованием в качестве цикловой функции. Блочный шифр «Кипарис» поддерживает длину блока и ключа 256 и 512 бит. В статье исследуется производительность малоресурсных блочных шифров «Кипарис-256» и «Кипарис-512» и сравнивается с производительностью других известных блочних шифров, таких как AES-256, SPECK-64/128, SPECK-128/128, SPARX-128/128, ДСТУ ГОСТ 28147: 2009. Производительность оценивалась на платформах Windows, Linux и Android путем измерения скорости зашифрования в режиме простой замены, в Мбит/сек. Блочный шифр «Кипарис» продемонстрировал высокую производительность на всех исследуемых программно-аппаратних платформах. На платформе Windows 10 с 32-битовой архитектурой лучший результат показал шифр «Кипарис-256» (почти 3,5 Гбит/с). На платформе Windows 10 с 64-битовой архитектурой лучший результат показал шифр «Кипарис-512» (почти 5 Гбит/с). На платформе Linux с 64-битовой архитектурой блочный шифр «Кипарис-256» показал очень высокий результат по скорости (более 8 Гбит/с). На платформе Android лучшими также были блочные шифры «Кипарис-256» и «Кипарис-512» (1,3 и 1 Гбит/с соответственно). С точки зрения производительности и удобства реализации на различных программно-аппаратных платформах алгоритм «Кипарис» имеет ряд преимуществ: два варианта шифра («Кипарис-256» и «Кипарис-512») ориентированы на 32-битную и 64-битную архитектуры соответственно; высокое быстродействие и компактная реализация преобразований независимо от используемой платформы (сервер, рабочая станция или мобильное устройство); минимальный необходимый объем памяти для быстродействующей реализации, отсутствие таблиц предвычислений; возможность организации эффективных защищенных высокоскоростных каналов связи между мобильными системами и серверами, в том числе теми, которые используют аппаратные ускорители.

Ключевые слова: блочный шифр; малоресурсная криптография; скорость зашифрования; ARX-преобразование; сеть Фейстеля.

Табл. 5. Ил. 2. Библиогр.: 18 назв.

UDC 621.3.06

The research of performance of the "Cypress" lightweight block cipher on different platforms / *M.Yu. Rodinko, R.V. Oliynykov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №200. P. 51 – 57.

The Cypress block cipher is a lightweight algorithm based on the Feistel network with ARX-transformation as a round function. The Cypress block cipher supports 256-bit and 512-bit block and key length. The paper presents results of researches on the performance of lightweight block ciphers Cypress-256 and Cypress-512 and it gives comparison of performance of other well-known block ciphers such as AES-256, SPECK-64/128, SPECK-128/128, SPARX-128/128, DSTU GOST 28147: 2009. Performance was evaluated on Windows, Linux and Android platforms by measuring the encryption speed in the Electronic Code Book mode, in Mbps. The Cypress block cipher has demonstrated high performance on all selected platforms. Cypress-256 showed the best result (almost 3.5 Gbps) on the Windows 10 platform with 32-bit architecture. Cypress-512 also showed the best result (almost 5 Gbps) on the Windows 10 platform with 64-bit architecture. On the Linux platform with a 64-bit architecture, Cypress-256 showed a very high speed result (more than 8 Gbps). Cypress-256 and Cypress-512 block ciphers were also the best (1.3 Gbps and 1 Gbps, respectively) on the Android platform. In terms of performance and simplicity of implementation on different software and hardware platforms, Cypress algorithm has several advantages. Two variants of cipher (Cypress-256 and Cypress-512) are oriented on 32-bit and 64-bit architectures, respectively; high speed and compact implementation of transformations regardless of the platform used (server, workstation or mobile device). Minimum amount of memory is required for high-speed implementation, there is no need in pre-computed tables; there is an ability to organize efficient secure high-speed communication channels between mobile systems and servers, including those using hardware accelerators.

Keywords: block cipher; lightweight cryptography; encryption speed; ARX-transformation; Feistel network.

5 tab. 2 fig. Ref.: 18 items

УДК 004.056.5

Тестування кодових генераторів псевдовипадкових чисел для пост-квантового застосування / *О.О. Кузнецов, А.С. Кіян, А.І. Пушкарьов, Т.Ю. Кузнецова* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 58 – 67.

Останні досягнення в області квантових обчислень, заснованих на нових принципах і явищах квантової механіки, показують, що квантовий криптоаналіз сучасних криптографічних алгоритмів може стати реальним вже в найближчі роки. Наприклад, за прогнозами національного інституту стандартів і технологій (NIST) США

в найближче десятиліття буде доступний квантовий криптоаналіз більшості використовуваних сьогодні несиметричних криптосистем. З цієї причини NIST оголосив про проведення конкурсу постквантових (тобто стійких до квантового криптоаналізу) криптографічних алгоритмів направленого шифрування, електронного підпису та інкапсуляції ключів. У найближчі роки очікується стандартизація обраних алгоритмів і їх якнайшвидше впровадження. Очевидно, що подальшої ревізії будуть піддаватися і інші криптоалгоритми, наприклад генератори псевдовипадкових чисел, засновані на вирішенні теоретико-складних завдань (дискретного логарифмування, факторизації та ін.). Ці генератори також підлягають заміні на надійні та безпечні алгоритми, придатні до використання навіть в умовах можливого застосування квантового криптоаналізу (тобто у постквантовий період). Дана стаття присвячена дослідженню доказово стійких генераторів, безпека яких ґрунтується на складності рішення задачі синдромного декодування. Подібна схема дозволяє генераторам зберігати стійкість як до класичного криптоаналізу, так і до криптоаналізу із застосуванням квантових обчислень. Представлені особливості функціонування класичного представника кодових генераторів, запропонованого Фішером і Штерном, вивчені її переваги і недоліки. Запропоновано схему нового генератору на основі кодів, в якій, за рахунок використання лінійних рекурентних регістрів зсуву, вдається формувати послідовності максимального періоду. Наведено результати евристичного тестування розглянутих генераторів, досліджено можливості їх застосування в постквантовий період.

Ключові слова: постквантова криптографія; доказово стійкий генератор; кодова криптографія; синдромне декодування.

Табл. 1. Іл. 9. Бібліогр.: 18 назв.

УДК 004.056.5

Тестирование кодовых генераторов псевдослучайных чисел для постквантового применения / *А.А. Кузнецов, А.С. Киян, А.И. Пушкарев, Т.Ю. Кузнецова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 200. С. 58 – 67.

Последние достижения в области квантовых вычислений, основанных на новых принципах и явлениях квантовой механики, показывают, что квантовый криптоанализ современных криптографических алгоритмов может стать реальным уже в ближайшие годы. Например, по прогнозам национального института стандартов и технологий (NIST) США в ближайшее десятилетие будет доступен квантовый криптоанализ большинства используемых сегодня несимметричных криптосистем. По этой причине NIST объявил о проведении конкурса постквантовых (т.е. устойчивых к квантовому криптоанализу) криптографических алгоритмов направленного шифрования, электронной подписи и инкапсуляции ключей. В ближайшие годы ожидается стандартизация выбранных алгоритмов и их скорейшее внедрение. Очевидно, что дальнейшей ревизии будут подвергаться и другие криптоалгоритмы, например генераторы псевдослучайных чисел, основанные на решении теоретико-сложностных задач (дискретного логарифмирования, факторизации и пр.). Эти генераторы также подлежат замене на надежные и безопасные алгоритмы, пригодные к использованию даже в условиях возможного применения квантового криптоанализа (т.е. в постквантовый период). Статья посвящена исследованию доказуемо стойких генераторов, безопасность которых основывается на сложности решения задачи синдромного декодирования. Подобная схема позволяет генераторам сохранять стойкость как к классическому криптоанализу, так и к криптоанализу с применением квантовых вычислений. Представлены особенности функционирования классического представителя кодовых генераторов, предложенного Фишером и Штерном, изучены ее достоинства и недостатки. Предложена схема нового генератора на основе кодов, в которой, за счет использования линейных рекуррентных регистров сдвига, удается формировать последовательности максимального периода. Приведены результаты эвристического тестирования рассмотренных генераторов, исследованы возможности их применения в постквантовый период.

Ключевые слова: постквантовая криптография; доказуемо стойкий генератор; кодовая криптография; синдромное декодирование.

Табл. 1. Ил. 9. Библиогр.: 18 назв.

UDC 004.056.5

Testing of code-based pseudorandom number generators for post-quantum application / *A.A. Kuznetsov, A.S. Kiian, A.I. Pushkar'ov, T.Yu. Kuznetsova* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №200. P. 58 – 67.

Recent advances in quantum computing based on new principles and phenomena of quantum mechanics show that quantum cryptanalysis of modern cryptographic algorithms can become real in the coming years. For example, according to the forecasts of the US National Institute of Standards and Technology (NIST) in the next decade, quantum cryptanalysis of most asymmetric cryptosystems used today will be available. For this reason, NIST announced a contest of post-quantum (i.e., resistant to quantum cryptanalysis) cryptographic algorithms for directional encryption, electronic signature, and key encapsulation. In the coming years, standardization of the selected algorithms and their early implementation is expected. Obviously, other cryptographic algorithms, for example, pseudorandom number generators based on solving complex theoretical problems (discrete logarithm, factorization, etc.), will also be subject to further revision. These generators must also be replaced by reliable and safe algorithms suitable for use even in the conditions of the possible application of quantum cryptanalysis (i.e., in the post-quantum period). This paper is devoted to the study of provably secure generators whose resistance is based on the complexity of solving the syndrome decoding problem. This structure allows the generators to keep the resistance to both classical cryptanalysis and cryptanalysis using quantum computing. The design features of classic code-based generator representative proposed by Fisher and

Stern are presented, and a new generator scheme is proposed to overcome the drawback of its predecessor, such as a reduced practical maximum period length, by using a linear feedback shift register. Within this paper Results of heuristic testing of the above-mentioned generators is conducted in terms of the sequence period, the speed of sequence generation, the cryptographic resistance of the generators and the possibility of their use in the post-quantum period.

Keywords: post-quantum cryptography; provable secure generator; code-based cryptography; syndrome decoding.

1 tab. 9 fig. Ref.: 18 items

УДК 004.056.5

Обчислювальні алгоритми розрахунку алгебраїчного імунітету нелінійних вузлів заміни симетричних шифрів / *К.Є. Лисицький, О.О. Кузнецов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 68 – 84.

Важливим елементом більшості сучасних симетричних шифрів є блок нелінійних замін (вузол ускладнення, блок підстановок, S-box). Це елементарний криптографічний примітив, призначений для перемішування вхідних даних і внесення нелінійності. За допомогою заміни блоків невеликого розміру іншими блоками досягається замішування та розсіювання даних, а багаторазове циклічне повторення такої процедури дозволяє добитися необхідних криптографічних властивостей шифру. До блоків підстановок висувається багато різних критеріїв (збалансованість, висока нелінійність, низька автокореляція, кореляційний імунітет, необхідні лавинні властивості та ін). Кожен критерій виражає формалізовану вимогу стійкості до певних видів криптографічного аналізу (диференціального, лінійного і т.д.), тобто при проектуванні шифрів використовують комплексний підхід, обираючи S-блоки по сукупності окремих показників. З розвитком алгебраїчного криптоаналізу з'явився новий показник ефективності вузлів замін – алгебраїчний імунітет, який розраховується як мінімальна ступінь найпростішого (в певному сенсі) алгебраїчного рівняння, що описує S-блок. Для пошуку такого рівняння використовують спеціальні методи, засновані на побудові базисів Гребнера. Якщо задати вузол замін через булеву функцію, тоді для розрахунку алгебраїчної імунності достатньо знайти функцію найменшого ступеня з простору анігіляторів. У статті розглядаються різні способи обчислення алгебраїчного імунітету, аналізується їх обчислювальна ефективність, обговорюються деталі реалізації, обґрунтовуються способи оптимізації обчислень за часовими (по числу операцій) і ємнісними (за витратами пам'яті) показниками складності. Пропонується удосконалений алгоритм розрахунку алгебраїчного імунітету, оптимізований по обчислювальних ресурсах, в тому числі за необхідними розмірами оперативної пам'яті. Наведено результати експериментальних досліджень, зокрема, результати обчислень алгебраїчного імунітету 8x8 S-блоків для деяких відомих сучасних шифрів (AES, Калина, Коник, BelT), а також результати, отримані для випадкових 8x8, 9x9 і 10x10 S-блоків.

Ключові слова: симетричний шифр; алгебраїчний імунітет; анігілюючий поліном; булева функція.

Табл. 5. Іл. 3. Бібліогр.: 26 назв.

УДК 004.056.5

Вычислительные алгоритмы расчета алгебраического иммунитета нелинейных узлов замены симметричных шифров / *К.Е. Лисицкий, А.А. Кузнецов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 200. С. 68 – 84.

Важным элементом большинства современных симметричных шифров является блок нелинейных замен (узел усложнения, блок подстановок, S-box). Это элементарный криптографический примитив, предназначенный для перемешивания входных данных и внесения нелинейности. Посредством замены блоков небольшого размера другими блоками достигается замешивание и рассеивание данных, а многократное циклическое повторение такой процедуры позволяет добиться требуемых криптографических свойств шифра. К блокам подстановок выдвигается много различных критериев (сбалансированность, высокая нелинейность, низкая автокорреляция, корреляционная иммунность, требуемые лавинные свойства и др). Каждый критерий выражает формализованное требование устойчивости к определенным видам криптографического анализа (дифференциального, линейного и т.д.), т.е. при проектировании шифров используют комплексный подход, выбирая S-блоки по совокупности отдельных показателей. С развитием алгебраического криптоанализа появился новый показатель эффективности узлов замен – алгебраическая иммунность, которая рассчитывается как минимальная степень простейшего (в некотором смысле) алгебраического уравнения, описывающего S-блок. Для поиска такого уравнения используют специальные методы, основанные на построении базисов Гребнера. Если задать узел замен через булеву функцию, тогда для расчета алгебраической иммунности достаточно найти функцию наименьшей степени из пространства аннигиляторов. В статье рассматриваются различные способы вычисления алгебраической иммунности, анализируется их вычислительная эффективность, обсуждаются детали реализации, обосновываются способы оптимизации вычислений по временным (по числу операций) и емкостным (по затратам памяти) показателям сложности. Предлагается усовершенствованный алгоритм расчета алгебраической иммунности, оптимизированный по вычислительным ресурсам, в том числе, по необходимым размерам оперативной памяти. Приводятся результаты экспериментальных исследований, в частности результаты вычислений алгебраического иммунитета 8x8 S-блоков для некоторых известных современных шифров (AES, Калина, Кузнечик, BelT), а также результаты, полученные для случайных 8x8, 9x9 и 10x10 S-блоков.

Ключевые слова: симметричный шифр; алгебраическая иммунность; аннигилирующий полином; булева функция.

Табл. 5. Ил. 3. Библиогр.: 26 назв.

UDC. 004.056.5

Computational algorithms for calculating the algebraic immunity of nonlinear nodes of replacing symmetric ciphers / *K. Lisitsky, O. Kuznetsov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №200. P. 68 – 84.

Block of nonlinear replacements (complication node, substitution block, S-box) is an important element of most modern symmetric ciphers. This is an elementary cryptographic primitive designed to mix input data and introduce nonlinearity. By replacing small blocks with other blocks, mixing and scattering of data is achieved, and repeated cyclic repetition of such a procedure makes it possible to achieve the required cryptographic properties of the cipher. Many different criteria are put forward to substitution blocks (balance, high nonlinearity, low autocorrelation, correlation immunity, required avalanche properties, and many others). Each criterion expresses a formalized requirement of resistance to certain types of cryptographic analysis (differential, linear, etc.), i.e. when designing ciphers, they use an integrated approach, choosing S-blocks according to the totality of individual indicators. With the development of algebraic cryptanalysis, a new indicator of the effectiveness of substitution nodes has appeared – algebraic immunity, which is calculated as the minimum degree of the simplest (in a sense) algebraic equation describing the S-block. To search for such an equation, special methods are used, based on the construction of Gröbner bases. If you specify a knot of substitutions through a Boolean function, then to calculate algebraic immunity it is enough to find a function of the least degree from the annihilator space. This article discusses various methods of calculating algebraic immunity, analyzes their computational efficiency, discusses implementation details, substantiates methods for optimizing calculations in terms of time (in terms of number of operations) and capacitive (in terms of memory costs) of complexity. An advanced algorithm for calculating algebraic immunity is proposed, optimized for computing resources, including the necessary RAM sizes. The results of experimental studies are presented, in particular, the results of calculations of the algebraic immunity of 8x8 S-blocks for some well-known modern ciphers (AES, Kalina, Grasshopper, BelT), as well as the results obtained for random 8x8, 9x9 and 10x10 S-blocks.

Keywords: symmetric cipher; algebraic immunity; annihilating polynomial; Boolean function.

5 tab. 3 fig. Ref.: 26 items

МЕТОДИ ТА МЕХАНІЗМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМІ БЛОКЧЕЙН

МЕТОДЫ И МЕХАНИЗМЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМЕ БЛОКЧЕЙН

METHODS AND MECHANISMS OF CRYPTOGRAPHIC INFORMATION PROTECTION IN THE BLOCKCHAIN SYSTEM

УДК 004.056.5

Проблеми, принципи побудови та перспективи розвитку національної системи електронного голосування в Україні / *І.Д. Горбенко, В.В. Онопрієнко, Ю.І. Горбенко, О.О. Кузнецов, К.В. Ісірова, М.Ю. Родінко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 85 – 97.

Розглядаються проблеми, принципи побудови та перспективи розвитку національної системи електронного голосування в Україні. Під електронним голосуванням розуміється спосіб здійснення волевиявлення, при якому процес голосування, підрахунку та оприлюднення результатів здійснюється за допомогою електронних засобів та систем. Більшість існуючих систем голосування побудовано за централізованими принципами і це дозволяє забезпечити певні переваги, наприклад, високу керованість системи, її надійність та автономність. Однак ієрархічним системам притаманні і суттєві недоліки, зокрема, наявність єдиного центру прийняття рішень та централізованого сховища зумовлює вразливість до кібернетичних атак на центр зберігання та прийняття рішень. Слід відзначити, що в централізованих системах можливі спотворення результатів волевиявлення через зловживання адміністративним ресурсом, і це є найбільшою загрозою сучасного демократичного інформаційного суспільства. Отже перспективним є дослідження, розробка та впровадження нових технологій електронного голосування, які б унеможливлювали втручання та викривлення результатів волевиявлення через децентралізацію із збереженням всіх системних якостей з безпеки та надійності. В статті зроблено конкретні пропозиції з обґрунтування архітектури, базової моделі та протоколів взаємодії децентралізованої системи електронного блокчейн-голосування. Запропоновано, досліджено та випробувано шляхом фізичного прототипування дворівневу архітектуру блокчейн-голосування. Її практичне впровадження підвищить довіру до інформаційних ресурсів та сервісів (що є особливо актуальним для державних установ); зменшить час та накладні витрати; унеможливить втручання централізованих установ та можливі корупційні дії; підвищить надійність збереження інформації та якість наданих послуг.

Ключові слова: електронне голосування; децентралізація; інформаційні технології; блокчейн-мережі; інформаційна та кібербезпека.

Табл. 1. Іл. 5. Бібліогр.: 17 назв.

УДК 004.056.5

Проблемы, принципы построения и перспективы развития национальной системы электронного голосования в Украине / *И.Д. Горбенко, В.В. Оноприенко, Ю.И. Горбенко, А.А. Кузнецов, К.В. Исирова, М.Ю. Родинко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 200. С. 85 – 97.

Рассматриваются проблемы, принципы построения и перспективы развития национальной системы электронного голосования в Украине. Под электронным голосованием понимается способ осуществления волеизъявления, при котором процесс голосования, подсчета и обнародования результатов осуществляется с помощью электронных средств и систем. Большинство существующих систем голосования построено по централизованным принципам, и это позволяет обеспечить определенные преимущества, например, высокую управляемость системы, ее надежность и автономность. Однако иерархическим системам присущи и существенные недостатки, в частности, наличие единого центра принятия решения и централизованного хранилища приводит к уязвимости перед кибернетическими атаками на центр хранения и принятия решений. Следует отметить, что в централизованных системах возможны искажения результатов волеизъявления из-за злоупотребления административным ресурсом, и это является самой большой угрозой современного демократического информационного общества. Перспективным является исследование, разработка и внедрение новых технологий электронного голосования, которые бы делали невозможными вмешательство и искажения результатов волеизъявления через децентрализацию с сохранением всех системных качеств по безопасности и надежности. В статье представлены конкретные предложения по обоснованию архитектуры, базовой модели и протоколов взаимодействия децентрализованной системы электронного блокчейн-голосования. Предложена, исследована и проверена посредством физического прототипирования двухуровневая архитектура блокчейн-голосования. Ее практическое внедрение повысит доверие к информационным ресурсам и сервисам (что особенно актуально для государственных учреждений) уменьшит время и накладные расходы; сделает невозможными вмешательство централизованных учреждений и возможные коррупционные действия; повысит надежность хранения информации и качество предоставляемых услуг.

Ключевые слова: электронное голосование; децентрализация; информационные технологии; блокчейн-сети; информационная и кибербезопасность.

Табл. 1. Ил. 5. Библиогр.: 17 назв.

UDC 004.056.5

Problems, construction principles and development prospects of the national electronic voting system in Ukraine / *I.D. Gorbenko, V.V. Onoprienko, Yu.I. Gorbenko, A.A. Kuznetsov, K.V. Isirova, M.Yu. Rodinko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №200. P. 85 – 97.

The present paper considers national electronic voting system problems in Ukraine, principles of construction and development prospects. Electronic voting refers to a way to exercise will, in which the voting, counting, and publication of the results processes are carried out by electronic means and systems. Most existing voting systems are built on centralized principles and this allows providing certain advantages, for example, high controllability of the system, its reliability, and autonomy. However, hierarchical systems also have significant drawbacks, in particular, single decision center and centralized storage leads to vulnerability to cyberattacks on them. Also it should be noted, that in centralized systems due to the abuse of administrative resources distortions of the results of expression of will are possible. This is the biggest threat to the modern democratic information society. Research, development, and implementation of new technologies of electronic voting, which would make it impossible to intervene and distort the results of the will through decentralization while maintaining all the system qualities for safety and reliability are promising. This article proposes particular proposals for architecture substantiating as well as a basic model and interaction protocols of a decentralized electronic blockchain voting system. A two-level blockchain voting architecture is proposed, researched and verified through physical prototyping. Its implementation will increase confidence in information resources and services (which is especially important for government agencies) will reduce time and overhead costs; make it impossible for centralized institutions to intervene and possible corrupt practices; will increase the reliability of information storage and the quality of services provided.

Keywords: electronic voting; decentralization; information technology; blockchain networks; information and cybersecurity.

1 tab. 5 fig. Ref.: 17 items

УДК 004.056.55

Можливості застосування механізмів повністю гомоморфного шифрування в системах електронного голосування / *І.Д. Горбенко, О.Г. Качко, Ю.І. Горбенко, М.В. Єсіна, С.О. Кандій, Є.В. Острянська, А.С. Д'яченко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 98 – 113.

Розглядається поняття гомоморфного шифрування та можливість його застосування у механізмі електронного голосування. Однією із проблемних вимог, що висунута до систем електронного голосування, є забезпечення анонімності виборців. З однієї сторони, кожен виборець повинен бути ідентифікований, а з іншої – зміст його голосу має бути невідомим. Запропоновані нині методи та механізми, що використовуються у реальних системах голосування, не забезпечують реальної анонімності. Тому як в теоретичному, так і практичному змісті актуальною та необхідною є проблема розроблення механізмів анонімного підрахунку голосів виборців з забезпеченням захищеності від їх викривлення. У роботі також проводиться узагальнений аналіз рівня безпеки перс-

пективних схем гомоморфного шифрування. Сутність гомоморфного шифрування полягає у тому, що існує деякий набір операцій, результат виконання яких над шифротекстами (з подальшим розшифруванням) співпадає з аналогічними діями над відкритими текстами. Гомоморфне шифрування дозволяє виконувати деякі обчислення над інформацією, при цьому не маючи доступу до самої інформації. Проте при спробі застосувати такі обчислення на практиці виникає ряд проблем. Основними з них є вибір методу асиметричного шифрування, що забезпечує необхідну криптографічну стійкість як від класичних, так і квантових атак, визначення можливих кандидатів асиметричних криптоперетворень при гомоморфному шифруванні, їх оцінка порівняння між собою та вибір найбільш раціональних при заданій множині загроз та обмежень. Порівнюються асиметричні схеми гомоморфного шифрування за допомогою методу аналізу ієрархій. Обґрунтовується метод асиметричного шифрування з нульовими знаннями. Мета статі – обґрунтування можливостей, умов і обмежень щодо застосування стандартизованих асиметричних криптоперетворень при створенні сучасних гомоморфних перетворень типу шифрування, коли повинна бути забезпечена анонімність електронного голосування та практична реалізація анонімного голосування на основі доведення нульових знань.

Ключові слова: асиметричні криптосистеми; гомоморфне шифрування; електронне голосування; механізм.

Табл. 6. Іл. 11. Бібліогр.: 36 назв.

УДК 004.056.55

Возможности применения механизмов полностью гомоморфного шифрования в системах электронного голосования / *И.Д. Горбенко, Е.Г. Качко, Ю.И. Горбенко, М.В. Есина, С.А. Кандий, Е.В. Острянская, А.С. Дьяченко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 200. С. 98 – 113.

Рассматривается понятие гомоморфного шифрования и возможность его применения в механизме электронного голосования. Одним из проблемных требований, выдвинутых к системам электронного голосования, является обеспечение анонимности избирателей. С одной стороны, каждый избиратель должен быть идентифицирован, а с другой – содержание его голоса должно быть неизвестным. Методы и механизмы, используемые в реальных системах голосования, не обеспечивают реальной анонимности. Потому как в теоретическом, так и практическом смысле актуальной и необходимой является проблема разработки механизмов анонимного подсчета голосов избирателей с обеспечением защищенности от их искажения. В статье проводится обобщенный анализ уровня безопасности перспективных схем гомоморфного шифрования. Сущность гомоморфного шифрования заключается в том, что существует некоторый набор операций, результат выполнения которых над шифротекстами (с последующей расшифровкой) совпадает с аналогичными действиями над открытыми текстами. Гомоморфное шифрование позволяет выполнять некоторые вычисления над информацией, при этом не имея доступа к самой информации. Однако при попытке применить такие вычисления на практике возникает ряд проблем. Основными из них являются выбор метода асимметричного шифрования, что обеспечивает необходимую криптографическую стойкость как от классических, так и квантовых атак, определение возможных кандидатов асимметричных криптопреобразований при гомоморфном шифровании, их оценка сравнения между собой, и выбор наиболее рациональных при заданном множестве угроз и ограничений. Сравниваются асимметричные схемы гомоморфного шифрования с помощью метода анализа иерархий. Обосновывается метод асимметричного шифрования с нулевыми знаниями. Цель статьи – обоснование возможностей, условий и ограничений по применению стандартизированных асимметричных криптопреобразования при создании современных гомоморфных преобразований типа шифрования, когда должна быть обеспечена анонимность электронного голосования и практическая реализация анонимного голосования на основе доказательства нулевых знаний.

Ключевые слова: асимметричные криптосистемы; гомоморфное шифрование; электронное голосование; механизм.

Табл. 6. Ил. 11. Библиогр.: 36 назв.

UDC 004.056.55

Possibilities of using full homomorphic encryption mechanisms in electronic voting systems / *I.D. Gorbenko, O.G. Kachko, Yu.I. Gorbenko, M.V. Yesina, S.O. Kandy, E.V. Ostryanska, A.S. Dyachenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №200. P. 98 – 113.

The paper deals with the concept of homomorphic encryption and the possibility of its use in the mechanism of electronic voting. One of the problematic requirements for electronic voting systems is voter anonymity. On the one hand, each voter must be identified, and on the other, the content of his or her vote must be unknown. Currently, the methods and mechanisms used in real voting systems do not provide real anonymity. Therefore, both theoretical and practical content is an urgent and necessary problem of developing mechanisms for anonymous counting of votes with the protection of their distortion. The paper also provides a general analysis of the security level of prospective homomorphic encryption schemes. The essence of homomorphic encryption is that there is some set of operations whose result of executing over ciphertexts (with subsequent decryption) coincides with similar actions over plaintexts. Homomorphic encryption allows you to perform some calculations on information without having access to the information itself. However, there are a number of problems when trying to apply such calculations. The main ones are the choice of the method of asymmetric encryption, which provides the necessary cryptographic stability from both classical and quantum attacks, the identification of possible candidates for asymmetric cryptotransformations in homomorphic encryption, their evaluation of comparison with each other, and, of course, the choice of the most rational for a given multiple restrictions. The asymmetric schemes of homomorphic encryption are compared using the hierarchy analysis process. The method of asymmetric encryption with zero knowledge is substantiated. The objective of this

article is to substantiate the possibilities, conditions, and constraints on the use of standardized asymmetric cryptotransformations in the creation of modern homomorphic encryption-type transformations, when anonymity of electronic voting and practical implementation of anonymous voting based on proof of zero knowledge must be guaranteed.

Key words: asymmetric cryptosystems; homomorphic encryption; electronic voting; mechanism.

6 tab. 11 fig. Ref: 36 items.

УДК 004.75

Аналіз площин атак на Blockchain системи / *П.І. Стеценко, Г.З. Халімов, Є.В. Котух* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 114 – 121.

Представлено дослідження площин атак і можливі способи проведення різних атак на децентралізовані системи на основі технології Blockchain. Розглянуто ефективність атаки відносно площини її застосування: криптографічних конструкцій технології Blockchain, розподіленої архітектури систем на основі технології Blockchain, контексту додатки Blockchain. Для кожної з цих площин виділено кілька атак, в тому числі стратегії злочинного Майнінг, узгоджена поведінка тимчасових вузлів, атаки 51 %, атаки на доменні імена (DNS), атаки «відмова в обслуговуванні», затримування досягнення консенсусу, розгалуження регістра Blockchain, відкинуті і застарілі блоки, крадіжки цифрового гаманця і атаки на конфіденційність.

Атака злочинного майнінгу дозволяє зловмисникові збільшити винагороду, навмисно зберігаючи свої блоки закритими, щоб отримати довшу версію регістра Blockchain, ніж поточна головна версія регістра. Атака 51 % відбувається, коли один зловмисник, група вузлів або майнінг-пул (об'єднання майнерів) в мережі досягає більшої частини загальної обчислювальної потужності майнінгу в системі і отримує можливість маніпулювати функціональністю Blockchain-системи. У площині DNS-атак зловмисник може потенційно ізолювати одноранговi вузли Blockchain-системи, поширювати серед нових вузлів підроблені блоки з шахрайськими транзакціями, робити недійсними транзакції. Прояви DDoS-атаки можуть різноманітними, залежно від характеру функціональності Blockchain-додатків, особливостей його мережевої архітектури та поведінки тимчасових вузлів. Розглянуто заходи протидії атакам на однорангову піринговy архітектуру.

Ключові слова: технологія Blockchain; зловмисний Майнінг; атака 51 %; DDoS-атаки і DNS-атаки.

Іл. 4. Бібліогр.: 19 назв.

УДК 004.75

Анализ плоскостей атак на Blockchain системы / *П.И. Стеценко, Г.З. Халимов, Е.В. Котух* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 200. С. 114 – 121.

Представлено исследование плоскостей атак и возможные способы проведения различных атак на децентрализованные системы на основе технологии Blockchain. Рассмотрена эффективность атаки относительно плоскости ее применения: криптографических конструкций технологии Blockchain, распределенной архитектуры систем на основе технологии Blockchain, контекста приложения Blockchain. Для каждой из этих плоскостей выделено несколько атак, в том числе стратегии злоумышленного майнинга, согласованное поведение одноранговых узлов, атаки 51 %, атаки на доменные имена (DNS), атаки «отказ в обслуживании», задержка достижения консенсуса, разветвление регистра Blockchain, отброшенные и устаревшие блоки, кражи цифрового кошелька и атаки на конфиденциальность.

Атака злоумышленного майнинга позволяет злоумышленнику увеличить вознаграждение, намеренно сохраняя свои блоки закрытыми, чтобы получить более длинную версию регистра Blockchain, чем текущая главная версия регистра. Атака 51 % происходит, когда один злоумышленник, группа узлов или майнинг-пул (объединение майнеров) в сети достигает большей части общей вычислительной мощности майнинга в системе и получает возможность манипулировать функциональностью Blockchain-системы. В плоскости DNS-атак злоумышленник может потенциально изолировать одноранговые узлы Blockchain-системы, распространять среди новых узлов поддельные блоки с мошенническими транзакциями, делать недействительными транзакции. Проявления DDoS-атаки могут разнообразными, в зависимости от характера функциональности Blockchain-приложения, особенностей его сетевой архитектуры и поведения одноранговых узлов. Рассмотрены меры противодействия атакам на одноранговую пиринговую архитектуру.

Ключевые слова: технология Blockchain; злоумышленный майнинг; атака 51 %; DDoS-атаки и DNS-атаки.

Ил. 4. Библиогр.: 19 назв.

UDC 004.75

Analysis of planes of attacks on the Blockchain system / *P.I. Stetsenko, G.Z. Khalimov, E.V. Kotukh* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №200. P. 114 – 121.

This paper presents a study of attack planessurfaces and possible ways of conducting various attacks on decentralized systems based on Blockchain technology. To accomplish the task, the effectiveness of the attack is studied relative to the plane of its application, namely, relatively: cryptographic designs of Blockchain technology, distributed architecture of systems based on Blockchain technology, Blockchain application context. Several attacks have been identified for each of these planes, including malicious mining strategies, coordinated peer behavior, 51% attacks, domain name attacks (DNS), distributed denial of service attacks, delayed consensus achieving, Blockchain branching, orphaned and obsolete blocks, digital wallet thefts and privacy attacks.

An attack by malicious mining allows an attacker to increase rewards by intentionally keeping his blocks closed in order to obtain a longer version of the Blockchain register than the current main version of the register. A 51% attack occurs when a single attacker, a group of nodes, or a mining pool (a combination of miners) in a network reaches most of the total processing power of mining in the system and gets the ability to manipulate the functionality of the Blockchain system. In the plane of DNS attacks, an attacker can potentially isolate peers of the Blockchain system, distribute fake blocks with fraudulent transactions among new nodes, and invalidate transactions. Manifestations of DDoS attacks can vary, depending on the nature of the functionality of the Blockchain application, the features of its network architecture and the behavior of peer nodes. Measures to counter attacks on peer-to-peer peer-to-peer architecture are considered.

Keywords: Blockchain technology; malicious mining; 51% attack; DDoS attacks and DNS attacks.

4 fig. Ref.: 19 items

УДК 004.056.5

Прототипування децентралізованої системи електронного блокчейн-голосування / *І.Д. Горбенко, О.О. Кузнецов, М.О. Полуяненко, А.С. Кіян, К.Є. Лисицький, С.О. Кандій* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 122 – 139.

Сучасна система електронного голосування являє собою взаємопов'язану сукупність правил, методів, процесів, засобів і технологій, а також правових норм, що забезпечують і регулюють дистанційне легітимне волевиявлення авторизованих користувачів (виборців). В статті запропоновано, досліджено та випробувано шляхом фізичного прототипування дворівневу архітектуру системи електронного блокчейн-голосування. Нижній (перший) рівень дозволяє забезпечити виконання всіх складових процесу електронної ідентифікації за допомогою вже існуючих систем, таких, наприклад, як BankID, MobileID, електронний підпис, тощо. Це забезпечить інтероперабельність електронного голосування, успадковуваність вже впроваджених національних інформаційних систем, зокрема, національної системи електронних довірчих послуг, відтворюваність результатів фізичного прототипування блокчейн-голосування. Верхній (другий) рівень призначено для реалізації волевиявлення та підрахунку голосів із забезпеченням незалежного контролю за правильністю складання списків виборців; можливості анонімного голосування тільки тими особами, які мають на це право; незмінності та неспростовності результатів волевиявлення; легкості та прозорості перевірки правильності підрахунку голосів, тощо. Отримані результати фізичного прототипування дозволяють стверджувати про ґрунтовність та виваженість розробленої архітектури, її спроможність забезпечити виконання базових вимог децентралізованого електронного голосування, вимог інформаційної та функціональної безпеки та надійності інформаційних технологій. Практичне впровадження розробленої архітектури блокчейн-голосування підвищить довіру до інформаційних ресурсів та сервісів (що є особливо актуальним для державних установ); зменшить час та накладні витрати; унеможливить втручання централізованих установ та можливі корупційні дії; підвищить надійність збереження інформації та якість наданих послуг.

Ключові слова: електронне голосування; децентралізація; інформаційні технології; блокчейн-мережі; інформаційна та кібербезпека.

Табл. 2. Іл. 7. Бібліогр.: 14 назв.

УДК 004.056.5

Прототипирование децентрализованной системы электронного блокчейн-голосования / *И.Д. Горбенко, А.А. Кузнецов, Н.А. Полуяненко, А.С. Киян, К.Е. Лисицкий, С.А. Кандий* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 200. С. 122 – 139.

Современная система электронного голосования представляет собой взаимосвязанную совокупность правил, методов, процессов, средств и технологий, а также правовых норм, обеспечивающих и регулирующих дистанционное легитимное волеизъявления авторизованных пользователей (избирателей). В статье предложена, исследована и проверена путем физического прототипирования двухуровневая архитектура системы электронного блокчейн-голосования. Нижний (первый) уровень позволяет обеспечить выполнение всех составляющих процесса электронной идентификации с помощью уже существующих систем, таких, например, как BankID, MobileID, электронная подпись и тому подобное. Это обеспечит интероперабельность электронного голосования, наследуемость уже внедренных национальных информационных систем, в частности, национальной системы электронных доверительных услуг, воспроизводимость результатов физического прототипирования блокчейн-голосования. Верхний (второй) уровень предназначен для реализации волеизъявления и подсчета голосов с обеспечением независимого контроля за правильностью составления списков избирателей; возможности анонимного голосования только теми лицами, которые имеют на это право; неизменности и неотказуемости результатов волеизъявления; легкости и прозрачности проверки правильности подсчета голосов и тому подобное. Полученные результаты физического прототипирования позволяют утверждать об обоснованности и взвешенности разработанной архитектуры, ее способности обеспечить выполнение базовых требований децентрализованного электронного голосования, требований информационной и функциональной безопасности и надежности информационных технологий. Практическое внедрение разработанной архитектуры блокчейн-голосования повысит доверие к информационным ресурсам и сервисам (что особенно актуально для государственных учреждений); уменьшит время и накладные расходы; сделает невозможным вмешательство централи-

зованных учреждений и возможные коррупционные действия; повысит надежность хранения информации и качество предоставляемых услуг.

Ключевые слова: электронное голосование; децентрализация; информационные технологии; блокчейн-сети; информационная и кибербезопасность.

Табл. 2. Ил. 7. Библиогр.: 14 назв.

UDC 004.056.5

Prototyping decentralized electronic blockchain voting system / *I.D. Gorbenko, A.A. Kuznetsov, N.A. Poluyanenko, A.S Kiyan, K.E. Lisitsky, S.A. Kandy* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №200. P. 122 – 139.

The modern electronic voting system is an interconnected set of rules, methods, processes, tools and technologies, as well as legal norms that ensure and regulate the remote legitimate will of authorized users (voters). This article proposes, investigates, and verifies by physical prototyping the two-tier architecture of the electronic blockchain voting system. The lower (first) level enables all components of the electronic identification process to be fulfilled by existing systems such as BankID, MobileID, electronic signature, and the like. This will ensure interoperability of electronic voting, inheritance of already implemented national information systems, in particular, of the national system of electronic confidential services, reproducibility of the results of physical prototyping of blockchain voting. The upper (second) level is intended for the implementation of the expression of votes and the counting of votes, with the provision of independent control over the correctness of the compilation of voter lists; the possibility of anonymous voting only by those who are entitled to it; the invariability and irrevocability of the results of the will; ease and transparency of checking the correctness of the vote count and the like. The obtained results of physical prototyping make it possible to confirm the validity and weight of the developed architecture, its ability to meet the basic requirements of decentralized electronic voting, the requirements of information and functional security and reliability of information technologies. The practical implementation of the developed blockchain voting architecture will increase trust in information resources and services (which is especially relevant for government agencies) and will reduce time and overhead; will make impossible the intervention of centralized institutions and possible corruption; will increase the reliability of information storage and the quality of services provided.

Keywords: electronic voting; decentralization; information technology; blockchain networks; information and cybersecurity.

2 tab. 7 fig. Ref.: 14 items

УДК 004.056.5

Аналітичне моделювання атаки подвійної витрати на блокчейн-системи із ймовірнісним протоколом консенсусу / *М.О. Полуяненко, О.О. Кузнецов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 140 – 152.

Для побудови безпечних та надійних розподілених децентралізованих систем за технологією блокчейн створюється безперервний ланцюжок блоків, несанкціонована зміна яких унеможливлюється застосованими криптографічними механізмами. Це досягається використанням односпрямованих, стійких до колізій та пошуку прообразів криптографічних функцій, геш-значення яких від попередніх блоків включаються у наступні блоки. В результаті несанкціоновану зміну бодай одного біту даних в попередніх блоках буде відразу виявлено. Але у разі розподіленого зберігання інформації виникає додаткова вимога синхронізації окремих ланцюгів блоків, які зберігаються різними вузлами. Ці та інші питання вирішуються шляхом застосування механізмів встановлення консенсусу, за допомогою яких після виконання певної послідовності дій безперервна послідовність блоків (блокчейн-ланцюг) стає однаковою на всіх вузлах децентралізованої мережі. В роботі досліджується одна з основних вразливостей блокчейн систем, побудованих за допомогою консенсусу з ймовірнісною завершеністю, а саме – атака подвійної витрати. На підставі моделі «незалежних гравців» отримано аналітичний вираз розрахунку ймовірності успішного проведення зловмисником атаки подвійної витрати. Наведено кількісні значення ймовірності вдалої атаки для різних можливостей зловмисника, різної кількості сформованих блоків та різною тривалістю гонки. За допомогою комп'ютерного моделювання експериментально перевірено розраховані значення. Всі емпіричні оцінки отримані для високої точності (відносна помилка не гірше 1 %) і достовірності (довірча ймовірність не менш 99 %). Для підтвердження адекватності отриманих результатів наведено порівняння емпіричних результатів з теоретичними розрахунками.

Ключові слова: децентралізована система; технологія блокчейн; протокол консенсусу; модель незалежних гравців; атака подвійної витрати.

Табл. 2. Іл. 11. Бібліогр.: 8 назв.

УДК 004.056.5

Аналитическое моделирование атаки двойной затраты на блокчейн-системы с вероятностным протоколом консенсуса / *Н.А. Полуяненко, А.А. Кузнецов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 200. С. 140 – 152.

Для построения безопасных и надежных распределенных децентрализованных систем по технологии блокчейн создается непрерывная цепочка блоков, несанкционированное изменение которых не допускается применяемыми криптографическими механизмами. Это достигается использованием однонаправленных, устойчивых к коллизиям и поиску прообразов криптографических функций, хеш-значения которых от предыду-

щих блоков включаются в последующие блоки. В результате несанкционированное изменение хотя бы одного бита данных в предыдущих блоках будет сразу обнаружено. Однако в случае распределенного хранения информации возникает дополнительное требование синхронизации отдельных цепочек блоков, которые хранятся различными узлами. Эти и другие вопросы решаются путем применения механизмов установления консенсуса, с помощью которых после выполнения определенной последовательности действий непрерывная последовательность блоков (блокчейн-цепочка) становится одинаковой на всех узлах децентрализованной сети. В работе исследуется одна из основных уязвимостей блокчейн-систем, построенных с помощью консенсуса с вероятностной завершенностью, а именно – атака двойной траты. На основании модели «независимых игроков» получено аналитическое выражение расчета вероятности успешного проведения злоумышленником атаки двойной траты. Приведены количественные значения вероятности удачной атаки для различных возможностей злоумышленника, разного количества сформированных блоков и разной продолжительности гонки. С помощью компьютерного моделирования экспериментально проверены рассчитанные значения. Все эмпирические оценки получены с высокой точностью (относительная ошибка не выше 1 %) и достоверности (доверительная вероятность не менее 99 %). Для подтверждения адекватности полученных результатов приведено сравнение эмпирических результатов с теоретическими расчетами.

Ключевые слова: децентрализованная система; технология блокчейн; протокол консенсуса; модель независимых игроков; атака двойной расходы.

Табл. 2. Ил. 11. Библиогр.: 8 назв.

UDC 004.056.5

Analytical modeling of the attack of double costs on a blockchain system with a probabilistic consensus protocol / *N.A. Poluyanenko, A.A. Kuznetsov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №200. P. 140 – 152.

To build safe and reliable distributed decentralized systems using blockchain technology, a continuous chain of blocks is created, the unauthorized modification of which is not allowed by the applied cryptographic mechanisms. This is achieved by using unidirectional, collision resistant and search prototypes of cryptographic functions whose hash values from previous blocks are included in subsequent blocks. As a result, an unauthorized change in at least one bit of data in the previous blocks will be immediately detected. However, in the case of distributed storage of information, there is an additional requirement of synchronization of individual chains of blocks that are stored by various nodes. These and other issues are resolved by applying consensus building mechanisms, through which, after a certain sequence of actions, a continuous sequence of blocks (blockchain chain) becomes the same on all nodes of a decentralized network. This work examines one of the main vulnerabilities of blockchain systems built by consensus with probabilistic completion, namely, a double-spend attack. Based on the model of “independent players”, an analytical expression is obtained for calculating the probability of an attacker's successful double-spending attack. The quantitative values of the probability of a successful attack are given for various abilities of an attacker, a different number of generated blocks and a different race duration. Using computer simulation, the calculated values are experimentally verified. All empirical estimates were obtained with high accuracy (relative error not higher than 1%) and reliability (confidence level of at least 99%). To confirm the adequacy of the results obtained, a comparison of empirical results with theoretical calculations is given.

Key words: decentralized system; blockchain technology; consensus protocol model of independent players; attack double costs.

2 tab. 11 fig. Ref.: 8 items

УДК 004.056.5

Ймовірність успішної атаки подвійної витрати на блокчейн-системи із ймовірнісним протоколом консенсусу / *Н.А. Полуяненко, О.О. Кузнецов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 153 – 161.

Більшість традиційних інформаційних систем побудовано за централізованим ієрархічним принципом. В таких системах існує єдиний центр прийняття рішень, щодо якого інші вузли є підлеглими, отже повинні безумовно сприймати та виконувати централізовані інструкції. Крім того, наявність центру прийняття рішень зумовлює і додаткові загрози, оскільки для порушення роботи всієї системи достатньо знищити або скомпрометувати головний вузол. Отже більш стійкими та безпечними, особливо в ситуації повної недовіри один до одного, є децентралізовані системи. Вони є більш надійними для збереження важливої інформації, наприклад цифрових активів, реєстрів, кадастрів, тощо. Саме тому технології блокчейн для побудови децентралізованих систем стають все більш популярними та поширеними. Однак при розгортанні децентралізованих систем виникає завдання узгодження стану різних вузлів мережі. Це особливо актуально, коли вузли функціонують в режимі повної недовіри один до одного, тобто якщо можливі ситуації, коли частка вузлів контролюється зловмисниками. Цю задачу вирішують за допомогою протоколів консенсусу, тобто таких правил та алгоритмів, при виконанні яких досягається однаковий стан більшості вузлів децентралізованої системи. В статті розглядаються ймовірнісні протоколи консенсусу, тобто коли виникнення певного стану є випадковою подією. Отже погодження станів системи можливе різними шляхами, в тому числі можливі хибні випадки, які нав’язуються зловмисниками. Наприклад, зловмисники можуть подвоїти свої електронні активи шляхом їх подвійної витрати. Звісно, якщо більшість вузлів контролюється зловмисниками, система буде працювати хибно. Але навіть при меншій частці ресурсів зловмисники також можуть з певною ймовірністю нав’язати хибний стан системи та

реалізувати у такий спосіб атаку подвійної витрати. В статті розглядаються різні ситуації та можливі стани системи, аналітичним шляхом виводяться формули розрахунку ймовірності успішної атаки подвійної витрати на блокчейн-системи із ймовірнісним протоколом консенсусу. При проведенні досліджень застосовувалася модель незалежних гравців, яка, на відміну від відомих робіт, враховує повну множину елементарних подій та станів системи. На основі отриманих результатів наведено рекомендації щодо безпечного функціонування децентралізованої системи.

Ключові слова: децентралізована система; технологія блокчейн; протокол консенсусу; модель незалежних гравців; атака подвійної витрати.

Іл. 3. Бібліогр.: 11 назв.

УДК 004.056.5

Вероятность успешной атаки двойной затраты на блокчейн-системы с вероятностным протоколом консенсуса / *Н.А. Полуяненко, А.А. Кузнецов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 200. С. 153 – 161.

Большинство традиционных информационных систем построено по централизованному иерархическому принципу. В таких системах существует единый центр принятия решений, по отношению к нему другие узлы являются подчиненными, следовательно, должны безусловно воспринимать и выполнять централизованные инструкции. Кроме того, наличие центра принятия решений обуславливает и дополнительные угрозы, поскольку для нарушения работы всей системы достаточно уничтожить или скомпрометировать главный узел. Более устойчивыми и безопасными, особенно в ситуации полного недоверия друг к другу, являются децентрализованные системы. Они более надежны для сохранения важной информации, например цифровых активов, реестров, кадастров и тому подобное. Именно поэтому технологии блокчейн для построения децентрализованных систем становятся все более популярными и распространенными. Однако при развертывании децентрализованных систем возникает задача согласования состояния различных узлов сети. Это особенно актуально, когда узлы функционируют в режиме полного недоверия друг к другу, то есть если возможны ситуации, когда доля узлов контролируется злоумышленниками. Эту задачу решают с помощью протоколов консенсуса, то есть таких правил и алгоритмов, при выполнении которых достигается одинаковое состояние большинства узлов децентрализованной системы. В статье рассматриваются вероятностные протоколы консенсуса, то есть когда возникновение определенного состояния является случайным событием. Согласование состояний системы возможно различными путями, в том числе возможные ложные случаи, которые навязываются злоумышленниками. Например, злоумышленники могут удвоить свои электронные активы путем их двойной траты. Конечно, если большинство узлов контролируется злоумышленниками, система будет работать неправильно. Но даже при меньшей доле ресурсов злоумышленники также могут с определенной вероятностью навязать ложное состояние системы и реализовать атаку двойной траты. В статье рассматриваются различные ситуации и возможные состояния системы, аналитическим путем выводятся формулы расчета вероятности успешной атаки двойной траты на блокчейн системы с вероятностным протоколом консенсуса. При проведении исследований применялась модель независимых игроков, которая, в отличие от известных работ, учитывает полное множество элементарных событий и состояний системы. На основе полученных результатов приведены рекомендации по безопасному функционированию децентрализованной системы.

Ключевые слова: децентрализованная система; технология блокчейн; протокол консенсуса; модель независимых игроков; атака двойной траты.

Ил. 3. Библиогр.: 11 назв.

UDC 004.056.5

Probability of a successful attack of double costs on a blockchain system with a probabilistic consensus protocol / *N.A. Poluyanenko, A.A. Kuznetsov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №200. P. 153 – 161.

Most traditional information systems are built on a centralized hierarchical principle. In such systems, there is a single decision-making center, to which other nodes are subordinate, therefore, they must certainly perceive and follow centralized instructions. In addition, the presence of a decision center causes additional threats, since to disrupt the operation of the entire system it is enough to destroy or compromise the main node. Decentralized systems are more stable and secure, especially in a situation of complete distrust of each other. They are more reliable for storing important information, such as digital assets, registries, inventories and the like. That is why blockchain technologies for building decentralized systems are becoming increasingly popular and widespread. However, when deploying decentralized systems, the task of coordinating the state of various network nodes arises. This is especially true when the nodes operate in a mode of complete distrust of each other, that is, if situations are possible where the proportion of nodes is controlled by intruders. This problem is solved using consensus protocols, that is, such rules and algorithms that, when executed, achieve the same state for most nodes of a decentralized system. This article discusses probabilistic consensus protocols, that is, when the occurrence of a certain state is a random event. Coordination of system states is possible in various ways, including possible false cases that are imposed by attackers. For example, attackers can double their electronic assets by spending them twice. Of course, if most nodes are controlled by intruders, the system will not work properly. But even with a smaller share of resources, attackers can also with a certain probability impose a false state of the system and thus implement a double-spend attack. The article discusses various situations and possible states of the system, analytically deriving formulas for calculating the probability of a successful double spending attack on a

blockchain system with a probabilistic consensus protocol. When conducting research, the model of independent players was used, which, unlike the well-known works, takes into account the complete set of elementary events and system states. Based on the results obtained, recommendations are given on the safe functioning of a decentralized system.

Key words: decentralized system; blockchain technology; consensus protocol; independent player model; double waste attack.

3 fig. Ref.: 11 items.

МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ В КОМУНІКАЦІЙНИХ СИСТЕМАХ
МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ В КОММУНИКАЦИОННЫХ СИСТЕМАХ
METHODS AND MEANS OF PROTECTION IN COMMUNICATION SYSTEMS

УДК 621.391

Теоретичні основи синтезу квазіортогональних систем складних сигналів / *І.Д. Горбенко, О.А. Замула* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 162 – 174.

Функціонування низки сучасних інфокомунікаційних систем (ІКС) здійснюється в умовах зовнішніх і внутрішніх впливів, обумовлених, з одного боку, дією природних перешкод, перешкод від інших радіотехнічних систем, що функціонують на близьких частотах або в спільній ділянці діапазону частот, з іншого боку – навмисних завад, створюваних станціями протидії з метою радіоелектронного подавлення діючих систем. Можливими стратегіями станції протидії є: визначення змісту повідомлень при використанні легальними абонентами алгоритмів криптографічного захисту даних; фальсифікація повідомлень; порушення цілісності даних; постановка різних типів перешкод і інше. Тому, до ІКС, особливо критичного призначення, пред'являються все більш жорсткі вимоги щодо забезпечення ефективності їх функціонування: достовірності і швидкості передачі інформації, живучості, завадозахищеності, інформаційної безпеки. У таких умовах особливого значення набуває наявність і застосування захищених інформаційно-комунікаційних систем. Під захищеністю систем розуміють, перш за все, їх здатність забезпечувати необхідні показники з завадозахищеності, імітостійкості, інформаційної, енергетичної і структурної скритності, швидкості передавання інформації, частотної і енергетичної ефективності. Необхідність застосування захищених радіоканалів змушує дослідників по-новому подивитися як на режими функціонування захищених радіоканалів, так і на аспекти формування і застосування складних сигналів – фізичних переносників даних для таких систем. У роботі на основі дослідження алгебраїчної структури систем нелінійних параметричних нерівностей сформульовані і у загальному виді вирішені задачі синтезу низки класів квазіоптимальних рівномірних, нерівномірних, складних дискретних сигналів із заданими кореляційними, ансамблевими і структурними властивостями, в тому числі таких систем сигналів, які мають властивості «розмитості» за кореляційними властивостями. Зазначена властивість означає, що збільшення або зменшення довжини дискретного сигналу не змінює кореляційні властивості дискретної послідовності, на основі якої синтезовано сигнал. Показано, що застосування безлічі зазначених систем сигналів в сучасних інформаційно-комунікаційних системах дозволить поліпшити показники функціонування таких систем, насамперед, завадозахищеності, скритності функціонування, інформаційної безпеки, завадостійкості прийому сигналів.

Ключові слова: функція кореляції; ортогональні сигнали; дискретні послідовності; складові системи сигналів; синтез систем сигналів; шумоподібний сигнал..

Бібліогр.: 8назв.

УДК 621.391

Теоретические основы синтеза квазиортогональных систем сложных сигналов / *И.Д. Горбенко, А.А. Замула* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 200. С. 162 – 174.

Функционирование ряда современных инфокоммуникационных систем (ИКС) осуществляется в условиях внешних и внутренних воздействий, обусловленных, с одной стороны, действием естественных помех, помех от других радиотехнических систем, функционирующих на близких частотах или в общем участке диапазона частот, с другой стороны – умышленных помех, создаваемых станциями противодействия с целью радиоэлектронного подавления действующих систем. Возможными стратегиями станции противодействия являются: определение содержания сообщений при использовании легальными абонентами алгоритмов криптографической защиты данных; фальсификация сообщений; нарушение целостности данных; постановка различных типов помех и др. Поэтому, к ИКС, особенно критического назначения, предъявляются все более жесткие требования по обеспечению эффективности их функционирования: достоверности и скорости передачи информации, живучести, помехозащищенности, информационной безопасности. В таких условиях особое значение приобретает наличие и применение защищенных ИКС. Под защищенностью систем понимают, прежде всего, их способность обеспечивать необходимые показатели по помехозащищенности, информационной, энергетической и структурной скрытности, скорости передачи информации, частотной и энергетической эффективности. Необходимость применения защищенных систем заставляет исследователей по-новому посмотреть на режимы функционирования защищенных радиоканалов и на аспекты формирования и применения сложных сигналов – физических переносчиков данных для таких систем. В работе на основе исследования алгебраической структуры систем нелинейных параметрических неровностей сформулированы и в общем виде решены задачи синтеза ряда

классов квазиоптимальных равномерных, неравномерных, сложных дискретных сигналов с заданными корреляционными, ансамблевыми и структурными свойствами, в том числе таких систем сигналов, которые обладают свойствами «размытости» по корреляционным свойствам. Указанное свойство означает, что увеличение или уменьшение длительности дискретной последовательности не изменяет корреляционные свойства сигнала, на основе которой синтезирован сигнал. Показано, что применение множества указанных систем сигналов в современных информационно-коммуникационных системах позволит улучшить такие показатели функционирования таких систем, как помехозащищенность, скрытность функционирования, информационная безопасность, помехоустойчивость приема сигналов.

Ключевые слова: функция корреляции; ортогональные сигналы; дискретные последовательности, составные системы сигналов; синтез систем сигналов; шумоподобный сигнал.

Библиогр.: 8 назв.

UDC 621.391

Theoretical bases of synthesis of quasi-orthogonal systems of complex signals / *I.D. Gorbenko, A.A. Zamula* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №200. P. 162 – 174.

Functioning of a number of modern infocommunication systems (ICS) is carried out under external and internal influences, caused, on the one hand, by natural interference, interference from other radio systems operating at close frequencies or in a common part of the frequency range, on the other hand, intentional interference created by counteraction stations with the aim of electronic suppression of existing systems. Possible strategies of the counter station are as follows: determining the content of messages when legal subscribers use cryptographic data protection algorithms; falsification of messages; violation of data integrity; staging of various types of interference, etc. Therefore, more stringent requirements are imposed on the ICS, especially for critical purposes, to ensure the effectiveness of their functioning: reliability and speed of information transfer, survivability, noise immunity, information security. In such conditions, the presence and use of protected ICS is of particular importance. Under the security systems one should understand, first of all, their ability to provide the necessary indicators for noise immunity, information, energy and structural secrecy, information transfer speed, frequency and energy efficiency. The need for the use of secure systems makes researchers take a fresh look at both the modes of operation of secure radio channels and the aspects of formation and use of complex signals – physical data carriers for such systems. In this paper, based on the study of the algebraic structure of systems of non-linear parametric irregularities, the problems of synthesis of a number of classes of quasi-optimal uniform, non-uniform, complex discrete signals with specified correlation, ensemble and structural properties, including such signal systems that have the properties “blur" by correlation properties. This property means that an increase or decrease in the duration of a discrete sequence does not change the correlation properties of the signal, on the basis of which the signal is synthesized. It is shown that the use of many of the indicated signal systems in modern information and communication systems will improve such indicators of the functioning of such systems as noise immunity, operational secrecy, information security, noise immunity of signal reception.

Key words correlation function; orthogonal signals; discrete sequences, composite signal systems; synthesis of signal systems; noise-like signal.

Ref.: 8 items

УДК 621.391

Методи пошуку оптимальних за мінімаксним критерієм систем складних нелінійних дискретних сигналів / *І.Д. Горбенко, О.А. Замула, Хо Чі Лик* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 175 – 187.

Серед основних напрямків поліпшення показників інформаційної безпеки, завадозахищеності і скритності інформаційно-комунікаційних систем (ІКС) можна виділити напрямки, які пов'язані із застосуванням каналів з великою частотною надмірністю, значною просторовою, структурною, енергетичною та часовою скритністю. Для забезпечення частотної надмірності на фізичному рівні широке застосування отримали дискретні сигнали, в яких маніпульовані параметри (амплітуда, фаза, частота) змінюються через строго фіксовані інтервали часу. Закон зміни зазначених параметрів задається дискретними послідовностями, які повністю визначають властивості дискретних сигналів і часто ототожнюються з ними. При синтезі систем сигналів (для застосування у захищених ІКС) прагнуть забезпечити певні властивості сигналів, насамперед: задано структурну скритність щодо визначення законів формування сигналів; поліпшено ансамблеві властивості (існування практично для будь-якого значення періоду, значний об’єм системи сигналів); визначено (для забезпечення необхідного значення завадостійкості прийому) кореляційні властивості. На основі критеріїв максимальної правдоподібності, мінімаксного критерію, фундаментальної границі оцінювання Крамера – Рао сформульовано вимоги до вибору систем сигналів для широкого спектру додатків багатокористувацьких ІКС. Зокрема, запропоновано великі ансамблі нелінійних складних сигналів в якості сигналів – фізичних переносників даних в ІКС. Показано, що такі сигнали мають поліпшені (в порівнянні з широко використовуваними класами лінійних сигналів) ансамблеві, кореляційні, структурні та інші властивості. Зазначене дозволяє поліпшити такі показники функціонування ІКС як завадозахищеність, електромагнітна сумісність, скритність і інформаційна безпека, що є дуже важливим для деяких додатків ІКС загального і критичного призначення. Показана можливість використання запропонованих систем сигналів при вирішенні класичних завдань оптимального прийому: виявлення та розрізнення сигналів, оцінка параметрів сигналів. При цьому (внаслідок хороших кореляційних властивостей запропонованих систем

сигналів) забезпечуються необхідні (для відповідних завдань) показники завадостійкості прийому сигналів і точності оцінки параметрів сигналів.

Ключові слова: функція кореляції; дискретні послідовності; синтез систем сигналів; шумоподібний сигнал, оцінка параметрів сигналу; завадостійкість прийому сигналів; криптографічний сигнал.

Табл. 4. Іл. 5. Бібліогр.: 15 назв.

УДК 621.391

Методы поиска оптимальных по минимаксному критерию систем сложных нелинейных дискретных сигналов / *И.Д. Горбенко, А.А. Замула, Хо Чи Лык* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 200. С. 175 – 187.

Среди основных направлений улучшения показателей информационной безопасности, помехозащищенности и скрытности информационно-коммуникационных систем (ИКС) можно выделить направления, связанные с применением каналов с большой частотной избыточностью, значительной пространственной, структурной, энергетической и временной скрытностью. Для обеспечения частотной избыточности на физическом уровне широкое применение получили дискретные сигналы, в которых манипулируемые параметры (амплитуда, фаза, частота) меняются через строго фиксированные интервалы времени. Закон изменения указанных параметров задается дискретными последовательностями, которые полностью определяют свойства дискретных сигналов и часто отождествляются с ними. При синтезе систем сигналов (для применения в защищенных ИКС) стремятся обеспечить определенные свойства сигналов, прежде всего: заданная структурная скрытность по определению законов формирования сигналов; улучшенные ансамблевые свойства (существование практически для любого значения периода, значительный объем системы сигналов); необходимые (для обеспечения требуемого значения помехоустойчивости приема) корреляционные свойства. На основе критериев максимального правдоподобия, минимаксного критерия, фундаментальной границы оценивания Крамера – Рао сформулированы требования к выбору систем сигналов для широкого спектра приложений многопользовательских ИКС. В частности, предложены большие ансамбли нелинейных сложных сигналов в качестве сигналов – физических переносчиков данных в ИКС. Показано, что такие сигналы обладают улучшенными (по сравнению с широко используемыми классами линейных сигналов) ансамблевыми, корреляционными, структурными и другими свойствами. Указанное позволяет улучшить такие показатели функционирования ИКС как помехоустойчивость, электромагнитная совместимость, скрытность и информационная безопасность, что важно для некоторых приложений ИКС общего и критичного назначения. Показана возможность использования предложенных систем сигналов при решении классических задач оптимального приема: обнаружение и различение сигналов, оценка параметров сигналов. При этом (вследствие хороших корреляционных свойств предложенных систем сигналов) обеспечиваются необходимые (для соответствующих задач) показатели помехоустойчивости приема сигналов и точности оценки параметров сигналов.

Ключевые слова: функция корреляции; дискретные последовательности; синтез систем сигналов; шумоподобный сигнал, оценка параметров сигнала; помехоустойчивость приема сигналов; криптографический сигнал.

Табл. 4. Ил. 5. Библиогр.: 15 назв.

UDC 621.391

Methods of searching for systems of complex nonlinear discrete signals optimal by the minimax criterion / *I.D. Gorbenko, A.A. Zamula, Ho Tri Luc* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №200. P. 175 – 187.

Among the main directions of improving information security indicators, noise immunity and secrecy of information and communication systems (ICS), we can single out areas related to the use of channels with high frequency redundancy, significant spatial, structural, energy and temporal secrecy. To ensure frequency redundancy at the physical level, discrete signals are widely used, in which the manipulated parameters (amplitude, phase, frequency) change at strictly fixed time intervals. The law of variation of these parameters is set by discrete sequences that completely determine the properties of discrete signals and are often identified with them. In the synthesis of signal systems (for use in protected ICS), they strive to provide certain properties of signals, first of all: a given structural secrecy in determining the laws of signal formation; improved ensemble properties (existence for almost any period value, a significant amount of the signal system); necessary (to ensure the desired value of the noise immunity of the reception) correlation properties. Based on the criteria of maximum likelihood, minimax criterion, the fundamental boundary of the Cramer-Rao assessment, the requirements to the choice of signal systems for a wide range of multi-user ICS applications are formulated. In particular, large ensembles of nonlinear complex signals are proposed as signals — physical data carriers in ICS. It is shown that such signals have improved (in comparison with the widely used classes of linear signals) ensemble, correlation, structural and other properties. The aforementioned allows to improve such performance indicators of the ICS as noise immunity, electromagnetic compatibility, secrecy and information security, which is very important for some general and critical ICS applications. The possibility of using the proposed signal systems in solving classical problems of optimal reception is shown: detection and discrimination of signals, estimation of signal parameters. In this case (due to the good correlation properties of the proposed signal systems), the necessary (for the corresponding tasks) indicators of noise immunity of signal reception and the accuracy of the estimation of signal parameters are provided.

Keywords: correlation function; discrete sequences; synthesis of signal systems; noise-like signal, estimation of signal parameters; noise immunity of signal reception; cryptographic signal.

4 tab. 5 fig. Ref.: 15 items.

УДК 004.056.53

Оцінка безпеки користувачів інтернет-банкінгу / *І.Є. Антіпов, Б.В. Бочаров, Д.Р. Найдьонова* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 188 – 194.

Стаття присвячена загрозам безпеки в популярному сервісі – інтернет-банкінгу, який останнім часом стає все більш поширеним. У статті узагальнено і проаналізовано загрози для користувачів інтернет-банкінгу, пов'язані з використанням телекомунікаційних мереж і засобів зв'язку. Виділено чотири основні вразливості: викрадення телефону, методи соціальної інженерії, перехоплення даних переданих або тих, щозберігаються на мобільному пристрої, і викрадення даних sim-карти. Запропоновано методику чисельної оцінки вразливості користувача інтернет-банкінгу, обумовлену цими погрозами, в основі якої лежить метод експертних оцінок. Отримані чисельні оцінки дозволять скористатися існуючими методами розрахунку ризику. Показано, що в даний час найбільшу загрозу становлять методи соціальної інженерії. Запропоновано набір заходів для користувачів інтернет-банкінгу з протидії розглянутим загрозам і методику оцінки їх ефективності, також засновану на методі експертних оцінок. Показано, що найбільш ефективним заходом є використання для інтернет-банкінгу окремого телефону без операційної системи. Запропоновані методики можуть бути використані для оцінки ефективності будь-яких інших заходів щодо підвищення рівня безпеки користувачів інтернет-банкінгу від загроз, пов'язаних з використанням телекомунікаційних мереж і засобів зв'язку. Методики можуть доопрацьовуватися і підлаштовуватися під інші об'єкти інформаційної безпеки або тимчасові зміни в області захисту інформації.

Ключові слова: Інтернет-банкінг; телекомунікації; безпека; користувачі; метод експертних оцінок; загрози та вразливості.

Табл. 5. Іл. 1. Бібліогр.: 17 назв.

УДК 004.056.53

Оценка безопасности пользователей интернет-банкинга / *И.Е. Антипов, Б.В Бочаров, Д.Р. Найденова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 200. С. 188 – 194.

Статья посвящена угрозам безопасности в популярном сервисе – интернет-банкинге, который в последнее время становится все более распространенным. Обобщены и проанализированы угрозы для пользователей интернет-банкинга, связанные с использованием телекоммуникационных сетей и средств связи. Выделены четыре основные уязвимости: похищение телефона, методы социальной инженерии, перехват данных передаваемых или хранящихся на мобильном устройстве и похищение данных sim-карты. Предложена методика численной оценки уязвимости пользователя интернет-банкинга, обусловленная этими угрозами, в основе которой лежит метод экспертных оценок. Полученные численные оценки позволят воспользоваться существующими методами расчета риска. Показано, что в настоящее время наибольшую угрозу представляют методы социальной инженерии. Предложены набор мер для пользователей Интернет-банкинга по противодействию рассмотренным угрозам и методика оценки их эффективности, также основанная на методе экспертных оценок. Показано, что наиболее эффективной мерой является использование для интернет-банкинга отдельного телефона без операционной системы. Предложенные методики могут быть использованы для оценки эффективности любых других мер по повышению уровня безопасности пользователей интернет-банкинга от угроз, связанных с использованием телекоммуникационных сетей и средств связи. Методики могут дорабатываться и подстраиваться под другие объекты информационной безопасности или временные изменения в области защиты информации.

Ключевые слова: Интернет-банкинг; телекоммуникации; безопасность; пользователи; метод экспертных оценок; угрозы и уязвимости.

Табл. 5. Ил. 1. Библиогр.: 17 назв.

UDC 004.056.53

Estimate of the Internet banking user security / *I.E. Antipov, B.V. Bocharov, D.R. Naydenova* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №200. P. 188 – 194.

The paper deals with security threats in the popular Internet banking service, the spread of which is becoming more common. Threats to the Internet banking users related to the use of telecommunication networks and means of communication are summarized and analyzed. Four main vulnerabilities have been identified: phone theft, social engineering methods, interception of data transmitted or stored on a mobile device, theft of SIM card data. Methods for numerically assessing the vulnerability of an Internet banking user due to these threats have been proposed. They are based on expert assessment method. The obtained numerical estimates will make it possible to use the existing methods for calculating risk. It is shown that currently the greatest threat is posed by methods of social engineering. A set of measures is proposed for users to counter the considered threats and a methodology for assessing their effectiveness, based on the expert assessment method too. It is shown that the most effective measure is the use of a separate telephone for Internet banking without an operating system. The proposed methods can be used to assess the effectiveness of any other measures to improve the security level of Internet banking users from threats associated with the use of telecommunication networks and communications. This method can be refined and adjusted to other information security objects or temporary changes in the field of information protection

Key words: Internet-banking; telecommunication; security; users; method of expert evaluations; threat and vulnerability.

5 tab. 1 fig. Ref.: 17 items

УДК 004.491.4

Метод виявлення та протидії вірусам у зображеннях формату BMP / *Р.С. Гриньов, О.В. Сєвєрінов, А.В. Власов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 195 – 200.

Мета статті – розробка методу захисту сучасних систем від атак з використанням графічних файлів формату BMP та HID-атак. Розглядаються особливості зображень формату BMP, спосіб їх використання для впровадження комп'ютерних вірусів та проведення атак з метою подолання засобів захисту. Також розглядаються HID-атаки та можливість поєднання цих атак; особливості функціонування сучасних засобів захисту IDS, IPS, антивірусів, брандмауерів та їх недоліки. Подібні атаки можливі через те, що засоби захисту аналізуватимуть тільки виконувані файли, бібліотеки DLL, документи Word, аплети Java. Більшість із засобів захисту просто не звертають уваги на зображення або інший безпечний тип файлу, оскільки вважають, що немає причин витрачати процесорний цикл на аналіз зображення. HID пристрої сприймаються засобами захисту як простий інтерфейс між комп'ютером та користувачем, тому є цілком довіреними. Запропоновано методи виявлення вірусів у графічних файлів формату BMP, засновані на перевірці зарезервованих полів, що мають бути нульовими; відповідності справжнього розміру файлу зазначеному у заголовку файлу; відповідності розміру зображення у пікселях, що зазначений у заголовку справжньому, Також запропоновано метод протидії HID-атакам, що заснований на аналізі швидкості введення тексту. Розроблено програми, що демонструють ефективність захисту від розглянутих атак.

Ключові слова: файл зображення формату BMP; комп'ютерний вірус; шелл-код; подолання систем захисту; приховування вірусу; антивірус; IDS; IPS; вразливість, експлойт; HID-атака; протидія атакам; методи захисту.

Іл. 5. Бібліогр.: 11 назв.

УДК 004.491.4

Метод выявления и противодействия вирусам в изображениях формата BMP / *Р.С. Гринев, А.В. Северинов, А.В. Власов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 200. С. 195 – 200.

Цель статьи – разработка метода защиты современных систем от атак с использованием графических файлов формата BMP и HID-атак. Рассматриваются особенности изображений формата BMP, способ их использования для внедрения компьютерных вирусов и проведения атак с целью преодоления средств защиты. Рассматриваются HID-атаки и возможность сочетания этих атак; особенности функционирования современных средств защиты IDS, IPS, антивирусов, брандмауэров и их недостатки. Подобные атаки возможны из-за того, что средства защиты будут анализировать только исполняемые файлы, библиотеки DLL, документы Word, апплеты Java. Большинство из средств защиты просто не обращают внимания на изображения или другой безопасный тип файла. Поскольку считают, что нет причин тратить процессорный цикл на анализ изображения. HID устройства воспринимаются средствами защиты как простой интерфейс между компьютером и пользователем, поэтому являются доверенными. Предложены методы выявления вирусов в графических файлах формата BMP, основанные на проверке зарезервированных полей, которые должны быть нулевыми, соответствии настоящего размера файла значению в заголовке файла, соответствии размера изображения в пикселях указанному в заголовке настоящему. Также предложен метод противодействия HID атакам, основанный на анализе скорости ввода текста. Разработаны программы, демонстрирующие эффективность защиты от рассмотренных атак.

Ключевые слова: файл изображения формата BMP; компьютерный вирус; шелл-код; преодоление систем защиты; сокрытия вируса; антивирус; IDS; IPS; уязвимость; эксплойт; HID-атака; противодействие атакам; методы защиты.

Ил. 5. Библиогр.: 11 назв.

UDC 004.491.4

Method for detecting and counteracting Virus Detection in BMP images / *R.S. Grynov, A.V. Sievierinov, A.V. Vlasov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №200. P. 195 – 200.

The aim of the article is to develop a method for protecting modern systems against attacks using BMP image files and HID attacks. This article describes the features of BMP format images. The method of injecting computer viruses in BMP image and attacks to overcome the means of protection. HID attacks and the possibility of combining these attacks are also considered. Features of functioning of modern means of protection IDS, IPS, antiviruses, firewalls and their shortcomings are presented. Such attacks are possible due to the fact that security tools will only analyze executable files, DLLs, Word documents, Java applets. Most of the protection tools simply do not pay attention to images or another secure file type. Because they believe, that there is no reason to spend the processor cycle on image analysis. HID devices are perceived by security tools as a simple interface between a computer and a user, therefore they are trusted. The article suggests methods for detecting viruses in BMP image files based on checking reserved fields that should be zero, matching the real file size with the value in the file header, matching the pixel size specified in the header with real. The article also offers a method to counteract HID attacks based on analysis of text input speed. Developed programs demonstrate the effectiveness of protection against the considered attacks.

Key words: BMP image file; computer virus; shell code; overcoming protection systems; virus hiding; antivirus; IDS; IPS; vulnerability; exploit; HID attack; protection methods.

5 fig. Ref.: 11 items.

УДК 621.391.15:519.7

Аналіз можливостей використання алгоритму Ель-Гамаля з детермінованим внесенням для інкапсуляції ключей / *О.В. Циганкова* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 201 – 205.

Припустимо що дві сторони, А та В, використовують деякий симетричний алгоритм шифрування (наприклад, AES) для шифрування повідомлень, що надсилаються від А до В та від В до А. Вони отримують свої спільні секретні ключі від деякого Довіреного Центру (ДЦ). ДЦ генерує ключі і потім доставляє їх до відповідних користувачів. Найпростіший, та, мабуть, і найоптимальніший спосіб доставляти ключі до користувача А полягає у зашифруванні його (деяким асиметричним алгоритмом шифрування) публічним ключем користувача А і надсилати цьому користувачу відкритим каналом. Така процедура називається "інкапсуляція ключа".

Алгоритми інкапсуляції ключа широко використовуються у сучасній криптології та є представленими у національних стандартах та стандартах ISO/IEC. Побудова алгоритму інкапсуляції ключа, який можна було б використовувати як Національний стандарт, на сьогодні залишається актуальною проблемою. Українські криптологи також зараз працюють над таким стандартом. У проекті Національного стандарту інкапсуляції ключа запропоновано використати модифіковану схему шифрування на еліптичних кривих (ECIES), включену в стандарти ANSI X9.63, ISO/IEC 18033-2, IEEE 1363a та SECG SEC1.

У роботі запропоновано деякий альтернативний алгоритм шифрування на еліптичних кривих, який також можна використовувати для інкапсуляції ключів.

Для інкапсуляції ключа можна використовувати довільний асиметричний алгоритм шифрування. Одним з найпростіших таких алгоритмів є алгоритм Ель-Гамаля. Але для використання цього алгоритму на еліптичних кривих потрібно спочатку вкласти ключ у деяку точку еліптичної кривої, а потім виконати зворотне перетворення. Багато робіт, як з теорії чисел, так і з криптології, розглядали проблему побудови детермінованого відображення елементів поля у точки еліптичної кривої. Проте лише у 2016 р. вдалось побудувати алгоритм вкладення геш-значення у точку кривої, а до того існували лише імовірнісні алгоритми was proposed. Зазначимо, що алгоритм вкладення ключа побудувати складніше, оскільки відповідне відображення має бути бієктивним.

Показано, як можна побудувати такий алгоритм вкладення ключа, а також обговоримо проблеми, які виникають при його використанні як складової алгоритму інкапсуляції ключа.

Ключові слова: ключовий алгоритм інкапсуляції ключа; алгоритм Ель-Гамаля; еліптична крива.

Бібліогр.: 9 назв.

УДК 621.391.15:519.7

Анализ возможности использования алгоритма Эль-Гамаля с детерминированным вложением для инкапсуляции ключей / *О.В. Цыганкова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 200. С. 201 – 205.

Предположим, что две стороны А и В, используют некоторый симметричный алгоритм шифрования (например AES) для шифрования сообщений, посылаемых от А до В и от В к А. Они получают свои общие секретные ключи от некоторого Доверенного Центра (ДЦ). ДЦ генерирует ключи и затем доставляет их к соответствующим пользователям. Самый простой, и, пожалуй, самый оптимальный способ доставлять ключи к пользователю А заключается в зашифровании его (некоторым асимметричным алгоритмом шифрования) публичным ключом пользователя А и направлении этому пользователю открытым каналом. Такая процедура называется "инкапсуляция ключа".

Алгоритмы инкапсуляции ключа широко используются в современной криптологии и представлены в национальных стандартах и стандартах ISO / IEC. Построение алгоритма инкапсуляции ключа, который можно было бы использовать как Национальный стандарт, на сегодня остается актуальной проблемой. Украинские криптологи также сейчас работают над таким стандартом. В проекте Национального стандарта инкапсуляции ключа предложено использовать модифицированную схему шифрования на эллиптических кривых (ECIES), включенную в стандарты ANSI X9.63, ISO / IEC 18033-2, IEEE 1363a и SECG SEC1.

В работе предлагается некоторый альтернативный алгоритм шифрования на эллиптических кривых, который также можно использовать для инкапсуляции ключей.

Для инкапсуляции ключа можно использовать произвольный асимметричный алгоритм шифрования. Одним из самых простых таких алгоритмов является алгоритм Эль-Гамаля. Но, для использования этого алгоритма на эллиптических кривих, нужно сначала вложить ключ в некоторую точку эллиптической кривой, а затем выполнить обратное преобразование. Во многих работах, как по теории чисел, так и по криптологии, рассматривалась проблема построения детерминированного отображения элементов поля в точке эллиптической кривой, однако только в 2016 г. удалось построить алгоритм вложения геш-значения в точку кривой, до этого же существовали только вероятностные алгоритмы was proposed. Отметим, что алгоритм вложения ключа построить сложнее, поскольку соответствующее отражение должно быть биективним.

Показано, как можно построить такой алгоритм вложения ключа, а также обговорены проблемы, которые возникают при его использовании в качестве составляющей алгоритма инкапсуляции ключа.

Ключевые слова: алгоритм инкапсуляции ключа; алгоритм Эль-Гамаля; эллиптическая кривая.

Библиогр.: 9 назв.

UDC 621.391.15:519.7

Analysis of possibility to use El Gamal algorithm with deterministic embedding for key encapsulation / *O.V. Tsygankova* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №200. P. 201 – 205.

Suppose some parties, A and B, use some symmetrical encryption algorithm (for example, AES) to encrypt their messages from A to B and from B to A. They get their secret keys from some Trusted Authority (TA). TA generates keys and then delivers them to correspondent users. The simplest and, may be, the optimal way to deliver the secret key to user A is to encrypt it (using some asymmetrical encryption algorithm) with A's public key and then to send it to A via public channel. Such procedure is called "key encapsulation".

Key encapsulation algorithms are widely used in the modern cryptography and represented in national and ISO/IEC standards of key encapsulations. Building the key encapsulation algorithm, which may be used as a national standard, is an actual problem nowadays. Ukrainian cryptographers are also working on such standard. Modified Elliptic Curve Integrated Encryption Scheme (ECIES), included in the ANSI X9.63, ISO/IEC 18033-2, IEEE 1363a and SECG SEC1 standards, was used in the project of national standard for key encryption.

In this article we propose some alternative encryption algorithm on elliptic curve which also may be used for this purpose.

Generally speaking we can use arbitrary asymmetric encryption algorithm for key encapsulation. One of the simplest and preferable algorithms is El Gamal encryption algorithm. To use this algorithm on elliptic curve, we need algorithms for embedding key into point on elliptic curve and for retrieving it back. Several lines of work in both the number theory and cryptography literature have considered the problem of deterministically mapping field element to point on elliptic curve. However, only probabilistic algorithms of such embedding existed until 2016, when deterministic algorithm for hash embedding was proposed. But key embedding is much more complicated procedure than hash embedding, because the correspondent mapping must be bijection.

In what follows we describe how this algorithm for key embedding can be built and then discuss the problems that appear if we want to use it in key encapsulation.

Key words: key encapsulation algorithm; El Gamal algorithm; elliptic curve.

Ref.: 9 items

ЗБІРНИК НАУКОВИХ ПРАЦЬ
РАДІОТЕХНІКА
Випуск 200
Українською, російською, та англійською мовами

СБОРНИК НАУЧНЫХ ТРУДОВ
РАДИОТЕХНИКА
Выпуск 200
На украинском, русском и английском языках

COLLECTION OF SCIENTIFIC PAPERS
RADIOTEKHNIKA
Issue 200
In Ukrainian, Russian and English

Коректор Л.І. Сащенко

Підп. до друку 30.04.2020. Формат 60x90/8. Папір офсет. Гарнітура Таймс. Друк. ризограф.
Ум. друк. арк**.** 11,2. Обл.-вид. арк. 10,9. Тираж 300 прим. Зам. № 298. 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.