DOI: https://doi.org/10.17721/ISTS.2020.1.23-30
УДК 004.056.55

НОВИЙ ПІДХІД ДО ПОБУДОВИ ПОСТ-КВАНТОВОЇ СХЕМИ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ

Олександр Кузнецов [1]
0000-0003-2331-6326

Анастасія Кіян [1]
0000-0003-2110-010X

Андрій Пушкарьов [2]
0000-0002-2429-0394

Тетяна Кузнецова [1]
0000-0001-6154-7139

[1] Харківський національний університет імені В.Н.Каразіна, майдан Свободи 4, 61022, Харків, Україна, kuznetsov@karain.ua, nastyak931@gmail.com, kuznetsova.tatiana17@gmail.com, https://www.univer.kharkov.ua
[2] Адміністрація Державної служби спеціального зв'язку та захисту інформації України, вул. Солом'янська, 13, 03110, м. Київ, Україна, http://www.dsszzi.gov.ua

Історія статті:
Надійшла до редакції 14.01.2020
Прийнято 28.01.2020

Ключові слова: кодові криптосистеми, електронний цифровий підпис, пост-квантова криптографія, квантова стійкість

Анотація. Методи криптографічного захисту інформації мають важливе значення в розбудові сучасної інфраструктури кібербезпеки. Останнім часом з'явилися нові виклики та загрози криптографічним перетворенням. Зокрема, поява та стрімкий розвиток новітніх технологій квантових обчислень зумовлює негайну потребу в розробці та дослідженні нових методів пост-квантових криптографічних перетворень, тобто таких, які будуть стійкими навіть за умови можливого застосування квантового криптоаналізу. Стаття присвячена аналізу можливостей реалізації схем електронного цифрового підпису з використанням кодів, що виправляють помилки. Подібний підхід дозволяє побудувати схеми, стійкі як до класичного криптоаналізу, так і в умовах криптоаналізу з використанням квантових обчислень. У рамках статті описано принципи функціонування класичної кодової схеми електронного цифрового підпису CFS, що побудована з використанням перетворення Нідеррайтера, а також запропоновано новий підхід, що дозволяє реалізувати підпис згідно перетворень схеми Мак-Еліса. Такий підхід зберігає переваги свого попередника і надає додатковий захист від спеціального виду атак. Також у статті здійснено порівняльний аналіз та характеристику розглянутих схем згідно критеріїв стійкості до класичного та квантового криптоаналізу, складності виконання необхідних перетворень та довжині формованих підписів. Отримані результати дозволяють стверджувати про можливість побудови надійних та безпечних криптографічних перетворень, зокрема, алгоритмів електронного цифрового підпису, які базуються на застосуванні кодів та є безпечними навіть в умовах можливого застосування квантового криптоаналізу. Втім, варто зазначити, що недоліком схем підписів на основі коду є великий обсяг ключових даних, необхідних алгоритму, а також складність у створенні підпису через необхідність багаторазового розшифрування синдрому, що залишається актуальною темою і потребує подальших досліджень.

Key words: Code-based cryptosystems, electronic digital signature, post-quantum cryptography, quantum resistance

Abstract. Cryptographic information security techniques are essential in building a modern cybersecurity infrastructure. Recently, there have been new challenges and threats to cryptographic transformation. In particular, the emergence and rapid development of the latest quantum computing technologies necessitates the urgent need for the development and research of new methods of post-quantum cryptographic transformations, that is, those that will be sustainable even if quantum cryptanalysis is possible. This article is devoted to the analysis of possibilities of implementation of digital signature schemes based on using error-correcting codes. This approach allows cryptographers to build schemes that are resistant to both classic cryptanalysis and cryptanalysis which uses quantum computing. The article describes the principles of the classic digital signature scheme which is named CFS and built using a Niederreiter-like transform, and also we propose a new approach that enables an implementation of signature according to the McEliece transformations. This approach preserves the advantages of its predecessor and provides additional protection against special attacks. Also, a comparative analysis and characterization of the considered schemes according to the criteria of resistance to classic and quantum cryptanalysis, complexity of necessary transformations and length of generated signatures are made. The results show that reliable and secure cryptographic transformations can be built, in particular, electronic

digital signature algorithms that are code-based and secure even in the case of quantum cryptanalysis. However, it should be noted that the drawback of code-based signature schemes is the large amount of key data required by the algorithm, as well as the difficulty in creating a signature due to the need for multiple decryption of the syndrome, which remains a topical topic and needs further research.

1. ВСТУП

Використовуючи закони квантової механіки, можна створити принципово новий тип обчислювальних машин, які дозволять вирішувати деякі завдання, недоступні навіть самим потужним сучасним суперкомп'ютерам. Різко зросте швидкість багатьох складних обчислень; повідомлення, надіслані по лініях квантового зв'язку, неможливо буде ні перехопити, ні скопіювати. Сьогодні вже створені прототипи цих квантових комп'ютерів майбутнього. Активні розробки у сфері квантового комп'ютера у 2016 році логічно призвели до реакції криптографічної спільноти у вигляді анонсування конкурсу пост-квантової стандартизації Національним інститутом стандартів та технологій. Розробники представили свої проекти у трьох напрямках: схеми електронного цифрового підпису, направлене шифрування та інкапсуляції ключів [1-3].

Статистика першого та другого туру конкурсу, що завершився у 2019 році, продемонструвала, що популярними напрямки розробки є криптографія, що базується на решітках, кодова криптографія, мультиваріативна криптографія та криптографія, заснована на геш-функціях. При цьому перші два напрямки охоплюють ¾ з усіх представлених проектів, що підтверджує актуальність всебічного розгляду цих напрямків у контексті реалізації криптографічних перетворень.

Сьогодні ведуться дебати щодо доцільності використання у реальних системах схеми електронних цифрових підписів, побудованих з використанням кодів. Сумніви виникають через великі об'єми ключових даних, що потребуються подібного роду схемам, проблеми швидкої підробки та інше. Слід зауважити, що, на жаль, ні одна кодова схема цифрового підпису не пройшла до другого туру конкурсу стандартизації NIST, а, отже, залишається актуальним питання розробки нових схем, що усували б недоліки своїх попередників [4].

У випадку розгляду кодових схем електронного підпису класичною є схема CFS, що названа згідно ініціалів її розробників Courtois, Finiasz та Sendrier, які вперше застосували підхід, заснований на алгебраїчних блокових кодах по відношенню до цифрового підпису. Вона побудована на використанні перетворень згідно криптосистеми Нідеррайтера. У статті розглянуто принципи функціонування CFS, а також запропоновано нову схему електронного цифрового підпису, що базується на використанні криптосистеми Мак-Еліса. Запропонований підхід дозволяє не тільки реалізувати пост-квантово стійку схему, але і надає додаткові переваги у вигляді захищеності від особливого типу атак. Аналіз такого роду атак по відношенню до схеми, а також порівняльне дослідження запропонованої схеми та схеми CFS розглянуто надалі.

2. CFS ЯК КЛАСИЧНА КОДОВА СХЕМА ЕЦП

CFS передбачає використання алгебраїчного (n, k, d) коду з класу незвідних кодів Гоппи. Формування ключових даних для функціонування схеми проходить аналогічно алгоритму, описаному для формування ключів схеми Нідеррайтера [5]. У якості вхідних даних схеми CFS використовуються:

- функція гешування h;
- швидкий алгоритм декодування алгебраїчного коду;
- безпосередньо повідомлення (відкритий текст).

Швидкий алгоритм декодування алгебраїчного коду, тобто той, що має поліноміальну складність, застосовується для декодування синдромної послідовності $s = (s_0, s_1, ..., s_{n-k-1})$ (криптограми у схемі Нідеррайтера) [6]. У випадку застосування алгоритму можливо виконання однієї з ситуації:

- Якщо декодування успішне, буде виведено знайдений вектор помилок $e = (e_0, e_1, ..., e_{n-1})$, що відповідає синдрому.
- Якщо декодування невдале, буде виведено повідомлення про помилку знаходження вектору помилок.

Алгоритм формування підпису полягає у поступовому виконанні декількох кроків (рис.1) [7].

1. Гешування відкритого тексту M;
2. Присвоєння лічильнику i значення i=1.
3. Геш-значення повідомлення $h(M)$ та лічильника i представляють як бітові послідовності, від конкатенації яких, обчислюють нове геш - значення $h(h(M)\|i)$.
4. $h(h(M)\|i)$ інтерпретується як синдромна послідовність $s_X = (s_0, s_1, ..., s_{n-k-1})$, що обчислена для деякого довільного кодового слова та вектору помилок $e = (e_0, e_1, ..., e_{n-1})$.
5. Формування вектору:

$$s_X^{*T} = X^{-1} \cdot s_X{}^T = X^{-1} \cdot H_X \cdot e^T = \\ = H \cdot P \cdot e^T = H \cdot \bar{e}^T \quad (1)$$

6. Застосування алгоритму швидкого декодування для знаходження вектору $\bar{e}^T = P \cdot e^T$.

7. Якщо декодування невдале, то необхідно інкременувати значення лічильника i, і повернутися на крок 3. Алгоритм застосовується до тих пір, пока не буде виведено знайдений вектор $\bar{e}^T = P \cdot e^T$, що відповідає вектору s_X^*.

8. Коли вектор s_X^* знайдено, обчислюємо

$$e^T = P^{-1} \cdot \bar{e}^T = P^{-1} \cdot P \cdot e^T \quad (2)$$

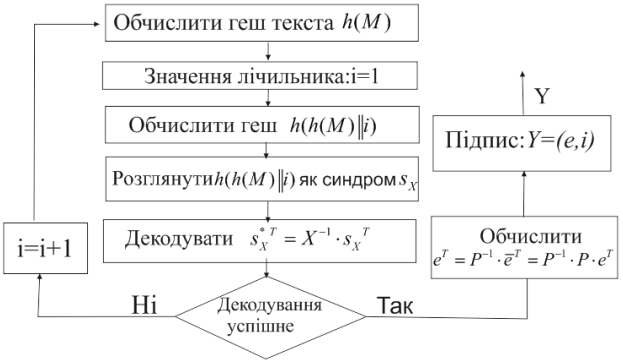

Рис.1 - Процес формування підпису згідно схеми CFS

Результатом виконання послідовності кроків є формування кінцевого підпису повідомлення M, що складається з двох частин: значення лічильника та вектору e, $Y = (e,i)$. Формально можна записати сформований підпис як

$$Y = (e,i) : H_X \cdot e^T = \left(h(h(M)\|i)\right)^T \quad (3)$$

Для того, щоб перевірити справжність підпису у якості вхідних даних необхідно мати відкритий ключ, що складається з матриці H_X, функцію хешування h, сам підпис $Y = (e,i)$ та повідомлення M. Для того, щоб верифікувати підпис потрібно обчислити значення двох векторів:

$$(s'_X)^T = H_X \cdot e^T,\ (s''_X)^T = h(h(M)\|i).$$

Цифровий підпис визнається правильним тільки за умови, що ці два вектори будуть однаковими.

Таким чином сутність функціонування схеми CFS можна визначити як багаторазове гешування повідомлення, конкатенованого з випадковим значенням лічильна для виділення коректної синдромної послідовності.

3. ОСОБЛИВОСТІ ЗАПРОПОНОВАНОЇ СХЕМИ ПІДПИСУ

Ми пропонуємо побудови схему електронного цифрового підпису, що базується на використанні односторонньої функції Мак-Еліса [8]. Формування ключових даних проходить аналогічно схемі CFS. Отже секретними ключами схеми є матриці X та P (у випадку недвійкових кодів додається ще матриця D), які є невиродженою матрицею $k \times k$ та матрицею перестановки $n \times n$ відповідно, а також швидкий алгоритм декодування алгебраїчного коду. Відкритим ключем у свою чергу виступає матриця G_X, що формується згідно правила $G_X = X \cdot H \cdot P \cdot D$, де G - це породжувальна матриця алгебраїчного коду [9].

При формуванні підпису аналогічно схемі CFS використовується функція гешування h, що була докладно описана раніше, тому на ній не буде зосереджуватися увага. Алгоритм декодування полягає у можливості знаходження вектору помилок $e = (e_0, e_1, ..., e_{n-1})$ та вектору $I = (I_0, I_1, ..., I_{k-1})$ згідно початковому кодовому слову з помилками $c_X^* = (c*_0, c*_1, ..., c*_{n-1})$, враховуючи співвідношення $c_X^* = I \cdot G_X + e$.

Алгоритм формування підпису запропонованої схеми проходить згідно таких кроків (рис.5).

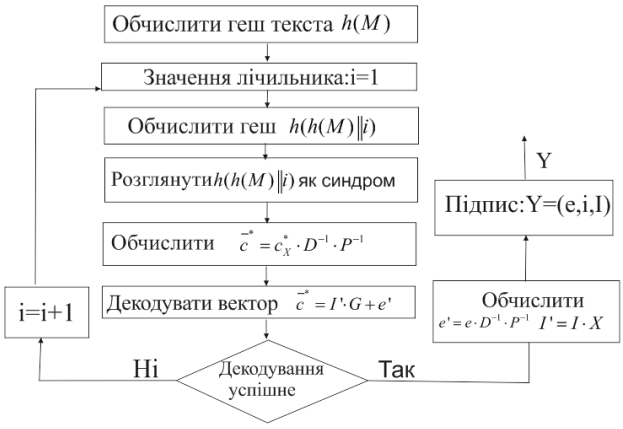

Рис.2 - Процес формування підпису згідно запропонованої схеми

1. Знаходження геш-коду від повідомлення, яке необхідно підписати
2. Присвоюємо значення лічильна i рівним 1.
3. Конкатенуємо геш-значення повідомлення та лічильника з подальшим хешуванням утвореної послідовності: $h(h(M)\|i)$
4. Інтерпретуємо $h(h(M)\|i)$ як кодове слово з помилками $c_X^* = (c*_0, c*_1, ..., c*_{n-1})$, що обчислене для певних векторів $e = (e_0, e_1, ..., e_{n-1})$ та $I = (I_0, I_1, ..., I_{k-1})$.

5. Знаходимо значення вектора $\bar{c}^{*} = c_X^{*} \cdot D^{-1} \cdot P^{-1}$. Цей вектор представляє викревлене не більше, ніж в t позиціях кодове слово, а отже, його можна декодувати з використанням алгоритму поліноміальної складності.

6. Висуваємо припущення:

$$\begin{aligned} \bar{c}^{*} &= c_X^{*} \cdot D^{-1} \cdot P^{-1} = (I \cdot G_X + e) \cdot D^{-1} \cdot P^{-1} = \\ &= (I \cdot X \cdot H \cdot P \cdot D + e) \cdot D^{-1} \cdot P^{-1} = \\ &= I \cdot X \cdot H + e \cdot D^{-1} \cdot P^{-1} \end{aligned} \quad (4)$$

7. Застосовуємо алгоритм поліноміальної складності для декодування кодового слова $\bar{c}^{*} = I' \cdot G + e'$, $e' = e \cdot D^{-1} \cdot P^{-1}$ і отримання вектору $I' = I \cdot X$.

8. Якщо внаслідок декодування не отримано вірний результат, збільшуємо значення лічильника на 1 та повертаємося на крок 3.

9. Якщо декодування успішне, отримуємо значення векторів e' та I'.

10. Обчислюємо значення векторів $e = e' \cdot D \cdot P$ та $I = I' X^{-1}$.

Результатом виконання алгоритму є формування підпису повідомлення, що складається зі значення лічильника, для якого вдало застосовано алгоритм декодування, вектору помилок та інформаційного вектору:

$$Y = (I, e, i) : IG_X + e = \left(h(h(M) \| i)\right) \quad (5)$$

Для запропонованої схеми на вхід декодеру поступає кодове слово з помилками, що має довжину n біт, а звідси загальна кількість n-бітних векторів визначається як 2^n.

При цьому відомо, що складність обчислення векторів I та e по відомому геш-значенню $h(h(M) \| i)$ для криптоаналітика визначається як NP-повна задача.

Для верифікації підпису є необхідним обчислення двох векторів: $c_X^{*}{}' = IG_X + e$ та $c_X^{*}{}'' = h(h(M) \| i)$. Якщо $c_X^{*}{}' = c_X^{*}{}''$ і вага Хеммінга вектора e не перевищує виправляючої здатності коду $w(e) \le t$, то підпис вважається справжнім. У іншому випадку, при невиконанні однієї з умов, робиться висновок, що підпис було змінено.

Таким чином згідно запропонованої схеми електронного цифрового підпису процедура верифікації відрізняється від схеми CFS шляхом додавання ще однієї умови, яка забезпечує альтернативну схему перевагами над CFS, що будуть розглянуті надалі.

Варто зазначити, що оцінка складності перевірки згідно схеми CFS справедлива по відношенню і до альтернативної схеми. При цьому в оцінках обох схем не враховуються обчислювальні затрати на роботу геш-функції та зняття дії маскуючих матриць.

4. ПОРІВНЯННЯ ЕФЕКТИВНОСТІ КОДОВИХ СХЕМ ЕЦП

Порівняльну характеристику схеми CFS та запропонованої схеми доцільно буде провести з використанням декількох критеріїв:

- складність формування та перевірки ЕЦП;
- стійкість ЕЦП;
- довжина підпису;
- обсяги ключових даних.

Проведемо аналіз поступово за всіма пунктами.

Для обох схем найбільш затратним є етап формування підпису, який полягає в успішному декодуванні синдромної послідовності, тому проведемо оцінку кількості спроб декодування для кожної зі схем.

Процес декодування тісно пов'язаний з поняттям синдромної послідовності. У випадку використання CFS ця послідовність має довжину $n-k$. Синдромна послідовність є бітовою послідовністю, тому може складатися лише зі значень 0 та 1. При чому кожне наступне значення не залежить від попереднього. Отже, загальна кількість можливих синдромних послідовностей дорівнює 2^{n-k}.

Відомо, що виправляюча здатність алгебраїчного двійкового блокового (n,k,d) коду визначається як $t = \left\lfloor \frac{d-1}{2} \right\rfloor$, якщо під час передачі відбудеться кількість помилок, що не перевищує значення *t,* усі ці помилки будуть гарантовано виправлені. Отже, кількість синдромних послідовностей, для яких декодування гарантовано пройде успішно можна визначити як:

$$N = \sum_{i=0}^{t} C_n^i . \quad (6)$$

Припустимо, що геш-значення $h(h(M) \| i)$ формуються рівно ймовірно, тоді ймовірність успішного декодування під час виконання алгоритму можна визначити [10-11] :

$$P_{y.\partial.} = \frac{\sum_{i=0}^{t} C_n^i}{2^{n-k}} . \quad (7)$$

У випадку використання двійкових сепарабельних кодів Гоппи, що задовольняють умовам $n = 2^m$, $k = n - mt$, $t = deg\ G(x)$, $d \ge 2t + 1$, можна скористатися апроксимацією:

$$P_{y.\partial.} = \frac{\sum_{i=0}^{t} C_n^i}{2^{n-k}} \approx \frac{\frac{n^t}{t!}}{n^t} = \frac{1}{t!} . \quad (8)$$

Звідси маємо, що здійснивши в середньому $t!$ спроб, декодування буде успішним. Кожна подібна спроба потребує $t^2 \cdot m^3$ двійкових операцій, але цей результат є приблизним, оскільки не береться до

уваги витрати на формування геш-кодів та зняття дій маскуючи матриць. Звідси можна оцінити середню кількість бітових операцій, яких вимагає виконання алгоритму формування підпису згідно схеми CFS:

$$N_{ф.п.} = t^2 \cdot m^3 \cdot t!. \quad (8)$$

У випадку використання альтеративної схеми на вході декодеру опиняється кодове слово з помилками $\overline{c}^{*} = I' \cdot G + e'$, що має довжину n біт. Загальна кількість n-бітних векторів визначається як 2^n. Кодове слово складається з двох компонент: k-бітного вектору I' (він може приймати одне з 2^k значень) та вектору e', вага Хеммінга якого не перевищує виправляючої здатності коду, тому, за аналогією з CFS, цей вектор набуває одного з значень. Значення I' та e' не залежить одне від одного. З вищесказаного можна зробити висновок, що кодове слово може набувати одне з $2^k \cdot N$ значень. Отже, ймовірність успішного декодування одиничного випадку можна визначити як:

$$P_{у.д.} = \frac{2^k \cdot \sum_{i=0}^{t} C_n^i}{2^n} = \frac{\sum_{i=0}^{t} C_n^i}{2^{n-k}}. \quad (9)$$

Очевидно, що дана оцінка збігається з оцінкою успішного декодування у схемі CFS. Звідси можна здійснити апроксимацію з урахуванням кодових відношень кодів Гоппа і отримати оцінку:

$$N_{ф.п.} = t^2 \cdot m^3 \cdot t!. \quad (10)$$

Наступним кроком оцінимо складність перевірки підпису згідно обох схем. При використанні схеми CFS необхідно обчислити геш-значення $h(h(M)\|i)$ і порівняти його з добутком $H_X \cdot e^T$. За умови, що складність хешування не враховується, як і в оцінці формування підпису, складність перевірки ЕЦП залежить тільки від кількості бітових операцій складання та множення при обчисленні добутку, тобто складність визначається як:

$$N_{п.п.} = (n-k) \cdot n = m \cdot t \cdot 2^m. \quad (11)$$

Ця оцінка справедлива по відношенню і до запропонованої схеми.

Отже, оцінки складності формування та перевірки підпису згідно схеми CFS та нової схеми є тотожними. При цьому в оцінках обох схем не враховуються обчислювальні затрати на роботу геш-функції та зняття дій маскуючи матриць [14, 25].

Як зазначалося раніше, схема CFS базується на використанні односторонньої функції з криптосистеми Нідеррайтера. Стійкість цієї функції до атаки, заснованої на переставному декодуванні, визначається як кількість кровельних множин, при яких можливо виправити всі комбінації з t помилок без знання секретного ключа [12]:

$$N \geq \frac{C_n^t}{C_{n-k}^t} = \frac{\frac{n!}{t!(n-t)!}}{\frac{(n-k)!}{t!(n-k-t)!}} = \frac{n!(n-k-t)!}{(n-t)!(n-k)!}. \quad (12)$$

З метою формування підпису $Y' = (e', i')$ для зміненого повідомлення M' зловмиснику потрібно реалізувати декодування випадкового коду в середньому $t!$ разів. Враховуючи цей факт, оцінку стійкості ЕЦП за схемою CFS можна визначити як:

$$N_c \geq t! \frac{C_n^t}{C_{n-k}^t} = t! \frac{n!(n-k-t)!}{(n-t)!(n-k)!} = t! \frac{2^m!(mt-t)!}{(2^m-t)!(mt)!}. \quad (13)$$

В ряді робіт виконано дослідження, що демонструють еквівалентність стійкостей криптосистем Мак-Еліса та Нідеррайтера. Звідси можна застосувати припущення, що стійкості схем CFS та запропонованої схеми, також еквівалентні.

У випадку використання квантового криптоаналізу оцінки стійкості обох схем набувають іншого характеру. Використовуючи один з найпопулярніших квантових алгоритмів, алгоритм Гровера, можна визначити кількість ітерацій для декодування випадкового коду, які потрібно виконати *t!* разів [13]:

$$C^{\frac{n}{2\log n}},\ C = \frac{1}{(1-R)^{1-R}}. \quad (14)$$

Припустимо, що квантовий алгоритм може бути застосовано для пошуку значення лічильника i, шляхом перебору значень (атака груба сила), що потребує в середньому $\frac{\pi}{4}\sqrt{t!}$ спроб. Отже, стійкість схем ЕЦП в умовах застосування квантових комп'ютерів можна визначити [14-15]:

$$N_{с.к.} \geq \frac{\pi}{4}\sqrt{t!}\left(\frac{1}{(1-R)^{1-R}}\right)^{\frac{n}{2\log n}} = \frac{\pi}{4}\sqrt{t!}\left(\left(1-\frac{k}{n}\right)^{\frac{k}{n}-1}\right)^{\frac{n}{2\log n}} = \frac{\pi}{4}\sqrt{t!}\left(1-\frac{k}{n}\right)^{\frac{k-n}{2\log n}} = \frac{\pi}{4}\sqrt{t!}\left(\frac{m \cdot t}{2^m}\right)^{t/2}. \quad (15)$$

Згідно схеми CFS підпис $Y = (e, i)$ містить дві складові: двійковий вектору *e*, що має довжину *n*, і ціле число i. Останнє може набувати значень в діапазоні $0,1,..,2^{n-k}-1$. Звідси маємо, що бітова довжина підпису визначається згідно виразу:

$$l_{ЕЦП} = 2 \cdot n - k = 2^m + m \cdot t. \quad (16)$$

Як зазначалося під час розгляду складності формування підпису, вектор e здатен набувати обмеженої кількості значень. Обмеження накладається згідно виправляючої здатності використовуваного коду. Кількість можливих векторів e визначається як [13]:

$$N_{w(e)\le t} = \sum_{i=0}^{t} C_n^i. \quad (17)$$

Через те, що вектор e відповідає умові вище, його можливо перетворити у беззбиткову послідовність $e*$ з довжиною $\lceil \log_2(N_{w(e)\le t}) \rceil$ біт. Тоді маємо:

$$l_{ЕЦП}* = \left\lceil \log_2 \left(\sum_{i=0}^{t} C_n^i \right) \right\rceil + n - k = \\ = \left\lceil \log_2 \left(\sum_{i=0}^{t} C_{2^m}^i \right) \right\rceil + m \cdot t. \quad (18)$$

Використовуючи вираз для верхньої границі Хеммінга, вираз можна перетворити:

$$l_{ЭЦП}* \le \left\lceil \log_2 \left(2^{n-k} \right) \right\rceil + n - k = 2 \cdot m \cdot t. \quad (19)$$

У випадку використання запропонованої схеми складових підпису $Y = (I, e, i)$ стає більше: вектор I (довжина k біт), вектор e та цілого числа i, довжина яких визначається так же, як і у схемі CFS. Звідси маємо, що довжина підпису $Y = (I, e, i)$ визначається згідно виразу:

$$l_{ЕЦП} = 2 \cdot n = 2^{m+1}. \quad (20)$$

Якщо здійснити беззбиткове перетворення вектора e, тоді цю оцінку можна переписати як:

$$l_{ЕЦП}* = \left\lceil \log_2 \left(\sum_{i=0}^{t} C_n^i \right) \right\rceil + n = \\ = \left\lceil \log_2 \left(\sum_{i=0}^{t} C_{2^m}^i \right) \right\rceil + 2^m. \quad (21)$$

Аналогічно розгляду CFS, використовуючи верхню границю Хеммінга маємо[16]:

$$l_{ЕЦП}* \le \left\lceil \log_2 \left(2^{n-k} \right) \right\rceil + n = m \cdot t + 2^m. \quad (22)$$

Схема CFS та її альтернатива побудовані на двох різних підходах: перша полягає у використанні функції зі схеми Нідеррайтера, друга-зі схеми Мак-Еліса, від яких прямо залежать обсяги ключових даних схем підпису. Відкритий ключ:

1. Довжина відкритого ключа CFS визначається кількістю комірок матриці $H_X = X \cdot H \cdot P$:

$$l_{в.к.} = (n-k) \cdot n = n^2 - kn = m \cdot t \cdot 2^m. \quad (23)$$

2. Довжина відкритого ключа альтернативної схеми визначається кількістю комірок матриці $G_X = X \cdot G \cdot P$:

$$l_{в.к.} = k \cdot n = (2^m - m \cdot t) \cdot 2^m. \quad (24)$$

Секретний ключ:

1. Довжина секретного ключа CFS визначається сумою кількості двійкових комірок матриці X (має розмір) та довжини n цілих чисел в діапазоні $0,1,..,n-1$ для визначення матриці P:

$$l_{с.к.} = (n-k)^2 + n \cdot \lceil \log_2 n \rceil = \\ = (m \cdot t)^2 + 2^m \cdot m. \quad (25)$$

2. Довжина секретного ключа альтернативної схеми визначається сумою кількості двійкових комірок матриці X (має розмір $k \times k$) та довжини n цілих чисел в діапазоні $0,1,..,n-1$ для визначення матриці P:

$$l_{с.к.} = k^2 + n \cdot \lceil \log_2 n \rceil = (2^m - m \cdot t)^2 + 2^m \cdot m. \quad (26)$$

Одразу слід зауважити, що в попередньому підрозділі було описано, що стійкість схем CFS та альтернативної схеми еквівалентні, що слідує з еквівалентності оцінок криптосистем Мак-Еліса та Нідеррайтера, на яких базуються вказані вище схеми підпису. Незважаючи на це, стійкість CFS та її альтернативи від деяких видів атак різниться. Цей факт докладніше буде розглянуто надалі. На сьогодні, на схему підпису CFS існує два типи атак: відновлення секретного ключа, та атака підробки підпису, яка полягає у намаганні створити дійсний підпис для повідомлення без знання секретного ключа. Атаки відновлення ключа проти схеми Мак-Еліса традиційно вважаються менш ефективними, ніж атаки дешифрування, і в даний момент не знайдено ефективної атаки цього типу у випадку використання кодів Гоппа. Через це в подальшому буде розглянуто атаки в контексті атак на алгоритми формування цифрового підпису-атаку підробки.

Для реалізації атаки підробки потрібно вирішити проблему декодування синдрому: знаходження вектору помилки найменшої ваги відповідно до наданого синдрому. Однак, на противагу стандартній проблемі декодування синдрому, тільки одна може бути вирішена як одна з багатьох [17].

Проблема декодування одного з багатьох: присутні параметри n,k,t та N, двійкова $k \times n$ матриця H і набір з N k-бітних двійкових векторів s_i. Потрібно знайти двійковий вектор помилок e з вагою Хеммінга t або менше таких, що задовольняють умові [24]:

$$\exists i \in [1,N] : e \cdot H^T = s_i . \qquad (27)$$

Існують дві найпопулярніші атаки на кодові криптосистеми: декодування множини даних (ISD) та загальний алгоритм, що базується на парадоксі «днів народжень» (GBA) [18]. ISD атака в умовах застосування принципу «декодування один з багатьох» здатна зменшити реальні затрати на виконання майже в $\sqrt{N}$ разів, де N - кількість доступних варіантів, порівняно з випадком, коли потрібно знайти один конкретний синдром. Атаки типу GBA, на відміну від атак ISD, здатні працювати лише у випадку наявності багатьох рішень. Ідею використання парадоксу «про дні народження» у контексті моделювання атак на схеми цифрового підпису належить Даніелю Блейхенбахеру. Він запропонував створювати список бажаних синдромів і використовувати цей список як один з початкових списків GBA. Порівняно з атакою ISD це дозволяє значно скоротити витрати на підробку підпису. Складність даної атаки відносно CFS з лічильником можна оцінити за наступною формулою:

$$C_{GBA} = L \log(L), \qquad (28)$$

де

$$L = \min\left(\frac{2^k}{C_n^{t-\lfloor t/3 \rfloor}}, \sqrt{\frac{2^k}{C_n^{\lfloor t/3 \rfloor}}}\right),$$

L - це довжина найбільшого списку, що використовується в алгоритмі. У випадку CFS з повним декодуванням, бажаним варіантом є знаходження слова з вагою $t+\delta$ і оскільки $C_n^{t+\delta} > 2^{mt}$, список, сформований із застосуванням операції XOR стовпчиків матриці H, є достатньо великим і розмір L найбільшого списку близький до значення $2^{\frac{mt}{3}}$.

Аналізуючи альтернативну схему, варто зауважити, що вона володіє вагомою перевагою перед CFS, оскільки здатна забезпечити захист від швидкої підробки підпису на основі додавання довільного кодового слова. Атака цього типу по відношенню до CFS може бути організована завдяки виконанню наступних дій:

– Обираємо довільне кодове слово c використовуваного (n,k,d) коду, перевірочна матриця якого позначається як H_x. В такому випадку справедлива рівність $H_x \cdot c^T = 0$. Маємо сформований підпис $Y = (e,i)$.

– Виконуємо додавання кодового слова:

$$\begin{aligned} Y &= (e+c,i) : H_x \cdot (e+c)^T = \\ &= H_x \cdot e^T + H_x \cdot c^T = \\ &= H_x \cdot e^T = (h(h(M) \| \mathrm{i}))^T . \end{aligned} \qquad (29)$$

Змінюючи останній вираз стосовно альтернативної схеми, отримаємо

$$Y = (I, e+\hat{c}, i) : IG_X + e + \hat{c} \neq \left(h(h(M) \| i)\right). \qquad (30)$$

тобто швидка підробка підпису у такому випадку неможлива. Також ця властивість посилена завдяки додатковій перевірці ваги Хеммінга вектору помилок під час процедури верифікації підпису. Це дозволяє захиститися також від інших гіпотетичних атак таких, як одночасна підробка двох елементів підпису і т.п.

5. ВИСНОВКИ

Стаття присвячена дослідженням способів цифрового підпису на основі кодів, що виправляють помилки. Стійкість таких схем ґрунтується на складності розв'язання теоретично складної проблеми розшифровки синдрому, що належить до класу задач NP-складних. З останнього факту випливає стійкість схем як до класичного криптоаналізу, так і до криптоаналізу з використанням квантових обчислень. У статті пропонується новий підхід до формування схеми цифрового підпису, що докорінно відрізняється від відомої схеми CFS. Однією із відмінністю запропонованої схеми є додавання нового елемента до підпису, це рішення дозволяє забезпечити захист від спеціальних видів атак, таких як одночасна підробка. Звичайно, додавання нового елемента збільшує остаточний розмір підпису, але таке збільшення не є критичним. Слід зазначити, що, незважаючи на відмінності в побудові підписів, обидві схеми забезпечують рівноцінний рівень захисту від класичного та квантового криптоаналізу. Однак варто зазначити, що недоліком схем підписів на основі коду є великий обсяг ключових даних, необхідних алгоритму, а також складність у створенні підпису через необхідність багаторазового розшифрування синдрому, що залишається актуальною темою і потребує подальших досліджень.

6. СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] D. Moody, “Post-Quntum Cryptography: NIST’s Plan for the Future,” *The Seventh International Conference on PostQuntum Cryptography*, Japan, 2016.
[2] R. Overbeck, N. Sendrier, *Code-based cryptography*. in: Daniel J. Bernstein, et al. (eds), First International Workshop on Post-quantum Cryptography, PQ Crypto 2006, Leuven, The Netherland, May 23-26, 2006. Selected papers, pp. 95-145.
[3] *Post - quantum cryptography*, [Online]. Available: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography
[4] D. Bernstein, J. Buchmann and E. Dahmen, *Post-Quantum Cryptography*, Springer-Verlag, Berlin-Heidleberg, 2009, 245 p.
[5] H. Niederreiter, “Knapsack-type cryptosystems and algebraic coding theory,” *Problem Control and Inform Theory*, v. 15, pp. 19-34, 1986.
[6] N. Courtois, M. Finiasz and N. Sendrier, “How to achieve a McEliece-based digital signature scheme”, *in Advances in Cryptology - ASIACRYPT 2001*, volume 2248, pp. 157-174.
[7] M. Finiasz, *Parallel-CFS: Strengthening the CFS McEliece-based signature scheme*, in Biryukov, A., Gong, G., Stinson, D., eds.: Selected Areas in Cryptography. Volume 6544 of LNCS., Springer, 2010, pp. 159-170.
[8] R. J. McEliece, *A public-key cryptosystem based on algebraic coding theory*, DSN Progress Report 42-44, Jet Propulsion Lab., Pasadena, CA, January-February, 1978, pp. 114-116.
[9] Yu.V. Stasev, A.A. Kuznetsov, “Asymmetric code-theoretical schemes constructed with the use of algebraic geometric codes,” *Kibernetika i Sistemnyi Analiz*, No. 3, pp. 47-57, May-June 2005.
[10] В. Д. Гоппа, “Новый класс линейных корректирующих кодов,” *Проблемы передачи информации*, т. 6, вып. 3, с. 24-30, 1970.
[11] В. Д. Гоппа, “На неприводимых кодах достигается пропускная способность ДСК,” *Проблемы передачи информации*, т. 10, вып. 1, с. 111-112, 1974.
[12] A. Kuznetsov, R. Serhiienko and D. Prokopovych-Tkachenko, "Construction of cascade codes in the frequency domain," *2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkov, 2017, pp. 131-136.
[13] A. Kuznetsov, I. Svatovskij, N. Kiyan and A. Pushkar'ov, "Code-based public-key cryptosystems for the post-quantum period," *2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkov, 2017, pp. 125-130.
[14] L. Grover, “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, pp. 212-219.
[15] L. Grover, “A framework for fast quantum mechanical algorithms,” *Proceedings of the 13th annual ACM symposium on theory of computing*, ACM Press, New York, 1998, pp. 53-62.
[16] Y. X. Li, R.H. Deng, X.M. Wang, *On the equivalence of McEliece’s and Niederreiter’s public-key cryptosystems*. [Online]. Available: https://ieeexplore.ieee.org/document/272496
[17] J. Stern, *A method for finding codewords of small weight*, in Cohen, G., Wolfmann, J., eds.: Coding theory and applications, Volume 388 of LNCS., Springer, 1989, pp. 106-113.
[18] N. Sendrier, “Decoding one out of many,” *in Yang, B.Y., ed.: PQCrypto 2011*. Volume 7071 of LNCS. Springer, 2011, pp. 51-67.

***Кузнецов Олександр Олександрович**, професор кафедри безпеки інформаційних систем і технологій Харківського національного університету імені В.Н.Каразіна, м. Харків, Україна. Сфера наукових інтересів: криптографія, теорія алгебраїчного кодування, пост-квантові криптоперетворення.*

***Кіян Анастасія Сергіївна**, здобувач кафедри безпеки інформаційних систем і технологій Харківського національного університету імені В.Н.Каразіна, м. Харків, Україна. Сфера наукових інтересів: криптографія, теорія алгебраїчного кодування, пост-квантові криптоперетворення.*

***Пушкарьов Андрій Іванович,** директор департаменту захисту інформації Державної служби спеціального зв’язку та захисту інформації України, м. Київ, Україна. Сфера наукових інтересів: інформаційна та кібербезпека, пост-квантові криптоперетворення.*

***Кузнецова Тетяна Юріївна,** науковий співробітник науково-дослідної частини Харківського національного університету імені В.Н.Каразіна, м. Харків, Україна. Сфера наукових інтересів: криптографія та теорія алгебраїчного кодування.*