**УДК 004.056** **DOI:10.30837/rt.2025.4.223.10**

*А.А. ТЕЛЬНОВА, Т.О. ГРІНЕНКО, канд. техн. наук, О.П. НАРЄЖНІЙ, канд. техн. наук*

# АНАЛІЗ СТІЙКОСТІ АЛГОРИТМІВ ПОСТКВАНТОВОГО ЦИФРОВОГО ПІДПИСУ FULEECA, WAVE, BISCUIT ТА RYDE

## Вступ

Алгоритми постквантового цифрового підпису (PQDS, Post-Quantum Digital Signature) розробляються як альтернатива класичним схемам, що здатна забезпечити криптографічну безпеку навіть за умови наявності квантових обчислювальних потужностей. Процес розробки та впровадження криптографічних алгоритмів цифрового підпису в умовах загрози квантових атак є актуальним питанням. У світовій практиці цим питанням займається Національний інститут стандартів і технологій (NIST). У грудні 2016 р. NIST ініціював відкритий конкурс на стандартизацію постквантових алгоритмів з відкритим ключем – Post-Quantum Cryptography Standardization Process (PQC) [1]. Метою цього конкурсу стало визначення алгоритмів, які могли б замінити існуючі стандарти у світі, де квантові комп'ютери становитимуть реальну загрозу. У вересні 2022 р. NIST оголосив четвертий раунд конкурсу на додаткові пропозиції щодо цифрових підписів, які будуть розглянуті в рамках процесу стандартизації PQC. NIST був зацікавлений, в першу чергу, в додаткових схемах підпису загального призначення, які не базуються на структурованих алгебраїчних решітках, однак також був відкритий і для отримання додаткових пропозицій на основі структурованих алгебраїчних решіток, які б значно перевершували CRYSTALS-Dilithium і FALCON у відповідних критеріях і забезпечували суттєві властивості безпеки [1].

Огляд літературних джерел свідчить про зростаючу увагу світової наукової спільноти до проблематики постквантової криптографії, особливо в аспекті цифрових підписів. У роботах Лео Дюкаса, Томаса Преста, Джеффрі Гоффстейна та інших розглядаються фундаментальні принципи побудови постквантових алгоритмів, заснованих на алгебраїчних решітках, кодах, багатосторонніх рівняннях та ґеш-функціях. Значну частину публікацій присвячено аналізу алгоритмів, які вийшли до фінальних етапів конкурсу NIST, таких як CRYSTALS-Dilithium, FALCON, SPHINCS+, тоді як розгляд менш відомих, але потенційно перспективних схем – Wave, RYDE, FuLeeca, Biscuit – часто обмежується суто математичними аспектами або первинними криптоаналітичними результатами.

Водночас систематизованих досліджень, які б поєднували криптостійкість, ефективність, реалізаційну придатність і технічні характеристики зазначених алгоритмів у порівняльному форматі, наразі обмаль. У доступній літературі відчутною є нестача узагальнень щодо практичного впровадження цих рішень у реальні інформаційні системи з урахуванням апаратних та програмних обмежень. Отже, попри наявність ґрунтовної математичної бази, проблема вибору оптимального постквантового алгоритму цифрового підпису для конкретних умов залишається відкритою та актуальною.

Мета статті – аналіз та дослідження теоретичних і прикладних аспектів функціонування алгоритмів цифрового підпису FuLeeca, Biscuit, Wave та RYDE, що є учасниками конкурсу NIST; аналіз структури побудови, стійкості та вразливостей алгоритмів, з урахуванням актуальних криптоаналітичних досліджень, що стосуються кожного з алгоритмів.

## 1. Постквантові алгоритми цифрового підпису

До чинних стандартів і тих, які зараз перебувають у процесі розробки, можна віднести CRYSTALS-DILITHIUM і SPHINCS+, які в серпні 2024 р. увійшли до стандартів FIPS 204 і FIPS 205, а також FALCON, який має увійти до стандарту FIPS 206. Також варто віднести ETSI TR 103 619 – технічний звіт, що містить рекомендації щодо постквантової криптографії й ETSI TS 103 744 – технічні специфікації щодо постквантових алгоритмів для застосування в різних галузях.

Постквантові цифрові підписи базуються на складних математичних задачах, які вважаються стійкими до атак квантових комп'ютерів. Найбільш поширеними класами задач, що лежать в основі PQDS, є:

- криптосистеми на алгебраїчних решітках (Lattice-based Cryptography): криптосистеми використовують складні задачі на алгебраїчних решітках, наприклад, алгоритми NTRU, BLISS, Falcon та Dilithium;

- кодові криптосистеми (Code-based Cryptography): криптосистеми базуються на складності декодування випадкових лінійних кодів, наприклад, алгоритм McEliece та Niederreiter;

- багатосторонні криптосистеми (Multivariate Quadratic Equations): криптосистеми використовують складність розв'язування систем багатосторонніх квадратичних рівнянь, як-то проблема факторизації многочленів або задача ізогеній еліптичних кривих. До таких алгоритмів відносяться Rainbow та UOV (Unbalanced Oil and Vinegar);

- ґеш-стійкі криптосистеми (Hash-based Cryptography): криптосистеми, що використовують криптографічні ґеш-функції для побудови підписів, наприклад, алгоритми XMSS (eXtended Merkle Signature Scheme) та SPHINCS+;

- еліптичні криві: деякі методи залучають еліптичні криві для постквантових схем [2].

Після оголошення у вересні 2022 р. четвертого раунду конкурсу на додаткові пропозиції щодо цифрових підписів, які будуть розглянуті в рамках процесу стандартизації PQC, NIST отримав 50 заявок, 40 з яких були визнані повними та належними відповідно до вимог.

Серед 40 заявок, що були допущені до подальшого конкурсу, можна виділити наступні категорії згідно з проблемами, які лежать в основі алгоритмів:

- алгоритми на основі кодів: CROSS, Enhanced pqsigRM, FuLeeca, LESS, MEDS і Wave;

- алгоритми на основі ізогеній: SQIsign;

- алгоритми на основі алгебраїчних решіток: EagleSign, EHTv3 і EHTv4, HAETAE, HAWK, HuFu, Raccoon та SQUIRRELS;

- алгоритми на основі багатосторонніх обчислень (MPC): Biscuit, MIRA, MiRitH, MQOM, PERK, RYDE й SDitH;

- алгоритми на основі багатомірності: 3WISE, DME-Sign, HPPC, MAYO, PROV, QR-UOV, SNOVA, TUOV, UOV і VOX;

- алгоритми на основі симетричних підписів: AIMer, Ascon-Sign, FAEST, а також SPHINCS-alpha;

- інші алгоритми: ALTEQ, eMLE-Sig 2.0, KAZ-SIGN, Preon і Xifrat1-Sign.I.

Після більш ніж річної оцінки NIST, у жовтні 2024 р., NIST оголосив про відбір 14 кандидатів на цифровий підпис, які пройшли до другого раунду в процесі стандартизації постквантової криптографії.

Серед основних переваг постквантових алгоритмів цифрового підпису можна виділити:

- стійкість до квантових атак: розроблені для витримки атак квантових комп'ютерів;

- різноманіття підходів: вже зараз існує велика кількість різних методів забезпечення безпеки.

Водночас вже зараз помітні і деякі недоліки постквантових криптосистем, а саме:

- великі розміри ключів та підписів: деякі алгоритми, як наприклад кодові криптосистеми, вимагають великих розмірів ключів та підписів, що може бути незручним для зберігання та передачі;

- часові затримки: деякі алгоритми мають більший час обчислення у порівнянні з класичними алгоритмами.

Дослідження постквантової криптографії призводить не лише до подолання деяких викликів, але й до появи нових. Можна виділити такі основними питання для пошуку розв’язання:

- оптимізація продуктивності: криптографічні операції повинні бути достатньо швидкими для практичного використання, особливо на обмежених пристроях;

- розмір підпису: багато постквантових алгоритмів мають великі ключі та підписи, що може бути проблематичним для деяких застосувань;

- стійкість до фізичних атак: алгоритми повинні бути стійкими не лише до теоретичних атак квантових комп'ютерів, але й до практичних фізичних атак.

## 2. Аналіз структури побудови, стійкості та вразливостей FuLeeca, Biscuit, Wave та RYDE

У роботі досліджено чотири постквантові криптографічні алгоритми, що належать до двох принципово різних напрямів – кодових та багатосторонніх схем. Такий вибір зумовлений прагненням порівняти підходи з різною математичною природою, які демонструють високий потенціал у контексті постквантової криптографії та перебувають на різних етапах аналізу і впровадження.

### 2.1. Постквантовий алгоритм цифрового підпису Fuleeca

Алгоритм FuLeeca (Fujisaki-Lee Code-based Encryption with Error Correcting Codes and Approximation) є одним із представників постквантових криптографічних схем, що базуються на так званій лі-метриці – альтернативі більш поширеній гамінговій метриці. Використання цієї метрики дозволяє створювати компактніші ключі та зменшувати обчислювальні витрати, що робить FuLeeca привабливим кандидатом для застосувань у ресурсно обмежених середовищах. Як варіант шифрування на основі кодів, FuLeeca поєднує ідеї з використанням лінійних кодів, випадкових помилок та схем подовження, аби забезпечити як коректність, так і стійкість до відомих атак.

#### 2.1.1. Математична задача, на якій базується стійкість алгоритму Fuleeca

FuLeeca базується на квазіциклічних метричних кодах Лі. Вага Лі секретних генераторів встановлюється на межі Лі-метрики Гілберта–Варшамова (GV). Це дозволяє розглядати секретний код як випадковий лінійний квазіциклічний код Лі-метрики, який досягає цієї межі з високою ймовірністю.

Квазіциклічні коди є спеціальним типом лінійних блокових кодів, що характеризуються тим, що кожен циклічний зсув коду є також кодовим словом. Вони мають високу структуру і регулярність, що дозволяє ефективно їх реалізовувати та декодувати.

Існує два основні методи побудови схем підпису на основі коду: перший застосовує перетворення Фіата–Шаміра до схеми ідентифікації з нульовим знанням на основі коду, а другий називається підходом Hash and Sign. Перший підхід зазвичай страждає від завеликих розмірів підпису через велику ймовірність шахрайства в схемі ідентифікації, а другий має невеликі розміри підпису за рахунок більшого розміру відкритого ключа. Постквантовий алгоритм цифрового підпису FuLeeca базується на підході Hash and Sign.

Першу схему на основі коду, що дотримується цього підходу, представили в 2001 р. Куртуа, Фініаш і Сендріє [3], яка отримала назву CFS. Ця класична схема підпису Hash and Sign є прямою адаптацією схеми шифрування з відкритим ключем McEliece. Схеми підпису на основі коду, засновані на квазіциклічних структурах з кодами низької щільності Геммінга, вразливі до атак зі статистичними ключами. Зловмисник може відновити розріджений секретний ключ, спостерігаючи за розподілом багатьох підписів і порівнюючи його з випадковим розподілом.

Використання метрики Лі перешкоджає вищевказаним атакам, оскільки навіть незважаючи на те, що вага Лі секретного базису низька, кількість ненульових записів може бути дуже високою для досить великих розмірів поля.

Здебільшого атаки на алгоритм Fulleca вимагають розв'язання задачі знаходження кодового слова з заданою вагою Лі. Формально вона визначається наступним чином. Необхідно знайти $c \in \mathbb{F}_p^n$, таке, що

$$\begin{cases} cH^{\intercal} = 0 \\ wt_L(c) = \omega' \end{cases} \quad (1)$$

де $H \in \mathbb{F}_p^{(n-k)\times n}$ і $\omega \in \mathbb{N}$ [4].

Знаходження кодових слів заданої ваги еквівалентно задачі декодування [5]. Версія рішення цієї проблеми була доведена як NP-повна [6].

**2.1.2. Стійкість алгоритму FuLeeca до атак**

Схема підпису FuLeeca полягає в тому, що секретний ключ є квазіциклічною генераторною матрицею, де генератори мають вагу Лі відповідно до обмеження GV метрики Лі, а відкритий ключ є її систематичною формою. Відновлення початкової основи має таку ж складність, як і проблема пошуку кодових слів заданої ваги Лі, яка, як доведено, є NP-складною [6].

Відповідно до вимог NIST було зроблене припущення, що зловмисник має доступ до 264 підписів для вибраних повідомлень. Такі сценарії багаторазового використання вимагають доказу екзистенціальної неможливості підробки під час атаки на вибране повідомлення.

Розробниками було розглянуто атаки, що використовують витік через опубліковані пари ґеш-функції й підпису. Згадані атаки не можуть бути застосовані до FuLeeca, оскільки в метриці Лі вектори з низькою вагою Лі не обов'язково мають малу підтримку Геммінга. Поклавши вагу секретних генераторів на границю GV, можливо трактувати отриманий код як випадковий. Це перешкоджає Геммінг-метричним атакам, оскільки секретні генератори й підписи мають близьку до повної вагу Геммінга.

Встановлення достатньо високого порогу для кількості необхідних збігів підписів запобігає тому, що раніше опублікований підпис може бути безпосередньо використаний для підписання іншого повідомлення. Очевидним узагальненням цієї атаки повторного використання є створення лінійних комбінацій існуючих підписів для підробки нових підписів.

З переважною ймовірністю вага Лі результуючого вектору буде занадто великою, щоб бути прийнятою верифікатором. Отже, така атака, яка подібна до виконання алгоритму просіювання, відомого з решітчастої криптографії, вимагає складності, яка є експоненціальною по відношенню до параметрів коду. Зокрема, в роботах [7, 8] доведено, що знайти кодове слово з меншою вагою Лі в квазіциклічному коді значно простіше, якщо розмірність коду $n = 2$ є складеним числом. Фактично задача захисту зводиться до задачі знаходження кодового слова у квазіциклічному коді.

Щоб уникнути витоку інформації через опубліковані пари ґеш/підпис розробниками було інтегровано спеціальну процедуру в алгоритм підписання, яка отримала назву процедури концентрації. Доцільність цієї процедури була доведена розробниками наступним чином. Для двох різних закритих ключів вони порівняли ваги Лі та збіги значень відповідних підписів після застосування простого підпису (рис. 1).

На рис. 1 показано зв'язок між кодовим словом та цільовим вектором, який є ґешем повідомлення. Оскільки алгоритм підпису ефективно співвідносить секретний ключ і ґеші, то виявляється можливим дізнатися принаймні деяку інформацію про секретний ключ на основі розподілу отриманих кодових слів.

Незважаючи на те, що конкретної атаки, що використовує цю поведінку, не наведено, результати показують, що деяка інформація про приватний ключ витікає й потенційно може бути використана для допомоги в процесі відновлення секретного ключа.

На рис. 2 показано розподіл значень логарифмічної ймовірності збігу та відносних ваг Лі для тих самих ґешів, що й на рис. 1, але вже після завершення концентруючої частини алгоритму. Результати показують, що процедура концентрації значно зменшує витік, який можна спостерігати за відносною вагою Лі та логарифмічною ймовірністю збігу.

У 2023–2024 рр. FuLeeca став об'єктом кількох глибоких криптоаналітичних досліджень. 21 липня 2023 р. Феліцітас Хьорманн і Вессел ван Вурден опублікували можливу атаку на алгоритм FuLeeca, що не зламує всі системи на базі Лі-метрики, але є специфічною для схеми FuLeeca [9]. Вона засвідчила, що алгоритм вразливий до побічних атак, що базуються на витоку інформації (leakage-based learning). Зокрема, при атаці використовується вибір інформаційного вектору $x$, який використовується для отримання підпису $v=xG$. Оскільки цей вектор вибрано з малими записами, зловмисник може розглянути цілочисельну алгебраїчну

решітку *L(G)*. Крім того, вибір *G = (A | B)* як квазіциклічного коду дозволяє зловмиснику працювати в циркулянтній алгебраїчній решітці *L(A)*.

Після публікація атаки, командою розробників було розглянуто методи захисту, але жоден із них не продемонстрував позитивного результату, адже вони призводять до вразливості щодо атак підробки та до непрактичних розмірів відкритих ключів. Наразі розробники алгоритмів працюють над вдосконаленням схеми.

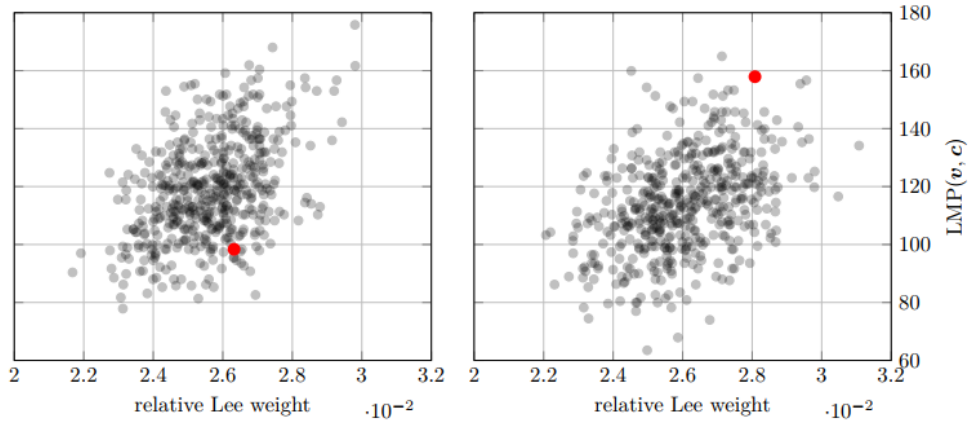


Рис. 1. Оцінка 500 підписів для імітованих ґешів із використанням двох різних ключів після застосування «простого підпису»

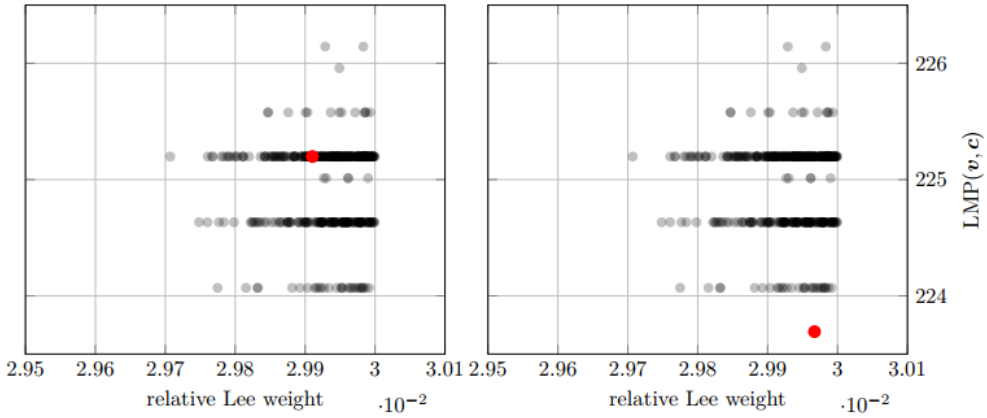


Рис. 2. Оцінка 500 підписів для імітованих ґешів для двох різних ключів після застосування підпису й процедури концентрування

### 2.2. Постквантовий алгоритм цифрового підпису WAVE

Wave – постквантовий алгоритм цифрового підпису, який поєднує ідеї з теорії помилок виправних кодів і концепцію пасток (trapdoor) на основі спеціальних лінійних кодів. Він реалізує підхід Hash-and-Sign для поля $\mathbb{F}_3$ з використанням складної схеми кодування. Його безпека ґрунтується на NP-складній задачі декодування в геммінговій метриці та задачі розрізнення спеціальних кодів від випадкових. Завдяки коротким підписам і швидкій перевірці, Wave є потенційно придатним для використання у високопродуктивних системах з допустимим компромісом – великим розміром відкритого ключа [10].

#### 2.2.1. Математична задача, на якій базується стійкість алгоритму Wave

Цифровий підпис Wave базується на NP-складній задачі декодування лінійних кодів у геммінговій метриці, зокрема її варіації – Decoding One Out of Many (DOOM). Суть цієї задачі полягає у знаходженні кодового слова фіксованої ваги, яке відповідає одному з багатьох синдромів, утворених шляхом ґешування повідомлень [11]. Саме така постановка задачі виникає в схемах типу Hash-and-Sign, до яких належить алгоритм Wave.

Базовою задачею, що лежить в основі Wave, є Decoding Problem (DP). Вона формулюється наступним чином: нехай $H \in \mathbb{F}_3^{(n-k)\times n}$ – матриця перевірки на парність для деякого лінійного коду, а $s \in \mathbb{F}_3^{(n-k)}$ – синдром. Необхідно знайти вектор $e \in \mathbb{F}_3^n$ з геммінговою вагою $|e| = w$, такий що

$$eH^\intercal = s. \tag{2}$$

Ця задача є NP-повною, навіть у випадку фіксованого алфавіту та випадкових матриць H. Саме на ній базується безпека більшості схем, що використовують лінійні коди, зокрема класичних схем McEliece і Niederreiter.

У схемі Wave зловмисник стикається не з однією, а з великою кількістю потенційних синдромів, оскільки підпис формується шляхом підбору випадкового параметра salt, а далі ґешування повідомлення разом із salt:

$$s = H(m||salt). \tag{3}$$

Таким чином, для атаки на підпис зловмисник повинен знайти такий вектор $e$, що для деякого $i$

$$He^\intercal = H(m_i||salt). \tag{4}$$

Це призводить до постановки задачі DOOM, яка формально формулюється так: для заданої матриці $H$ та великої множини синдромів $\{s_1, s_2 \dots s_q\}$ знайти такий вектор $e$ фіксованої ваги $w$ [11], що для деякого $i$

$$He^\intercal = s_i. \tag{5}$$

Задача DOOM вважається складнішою за звичайну задачу DP, оскільки вона передбачає вибір з множини випадкових цілей. Це унеможливлює застосування специфічних декодерів, що працюють лише для обмежених класів синдромів, і забезпечує додаткову стійкість схеми навіть у моделі з доступом до вибраних повідомлень (chosen-message attack).

Щоб зробити задачу DP розв'язуваною лише для власника секретного ключа, у Wave використовується спеціальна пастка (trapdoor) – структурований код типу $(U||U+V)$, побудований над полем $\mathbb{F}_3$ [11]. Код має наступну конструкцію:

$$C = \{(u, u+v) : u \in U, v \in V\}, \tag{6}$$

де $U, V \subset \mathbb{F}_3^{n/2}$ – лінійні підкоди.

Далі код піддається перестановці координат $\pi$ та додаванню маскуючих векторів $b, c$, що перешкоджає розпізнаванню структури зі сторони.

Секретний ключ – це опис кодів $U$ і $V$, перестановки $\pi$ та векторів маскування. Завдяки цій структурі, власник секретного ключа може ефективно декодувати синдроми шляхом розкладу на $eV$ та $eU$, тоді як для зловмисника задача залишається аналогом випадкового коду.

Розмірність коду та вага $w$ у Wave підібрані так, щоб задача декодування залишалася за межами зони ефективного декодування. Існує відомий інтервал значень $w$, у якому ймовірність існування коду з помилками, що задовольняють умову (4), є низькою, і жоден відомий алгоритм (навіть ISD) не може вирішити задачу швидко. Wave працює за цим порогом, гарантуючи, що навіть оптимальні класичні чи квантові атаки не можуть зламати систему при дотриманні рекомендованих параметрів.

Оскільки схема підпису Wave реалізує парадигму Hash-and-Sign, вона критично залежить від ґеш-функції $H$. Саме вона трансформує повідомлення у синдром, що потрібно декодувати. Щоб уникнути ймовірності відсутності рішення, схема генерує випадкове значення salt і підбирає його доти, поки задача DOOM не має розв'язку для поточного $m||salt$.

Ця особливість підкреслює, що алгоритм фактично шукає серед багатьох DOOM-випадків – саме той, для якого існує придатне $e$, що вдається зробити лише знаючи внутрішню структуру пастки.

### 2.2.2. Стійкість алгоритму Wave до атак

Кодовий криптоалгоритм WAVE дотримується тієї самої схеми, що й FuLeeca, але базується на новій проблемі: декодуванні великих помилок ваги. Цією схемою вдалося запобігти всім вищезазначеним атакам (див. п. 2.1.2), і досі не було встановлено жодного успішного алгоритму криптоаналізу. Однак, стійкість до атак досягається за рахунок непрактично великих розмірів відкритих ключів.

Безпека алгоритму Wave має формальне обґрунтування і базується на складності задач Decoding One Out of Many (DOOM) та розрізнення структури відкритого ключа (DWK). Розробники алгоритму провели повний доказ стійкості в моделі Quantum Random Oracle Model (QROM), враховуючи можливість атак з боку квантових зловмисників. Водночас у схемі враховано потенційні канали витоку інформації з підписів, які мінімізуються завдяки використанню технік rejection sampling та спеціальних розподілів.

Стійкість Wave доведено у моделі existential unforgeability under chosen message attacks (EUF-CMA). Це означає, що навіть за наявності доступу до оракула підпису, зловмисник не зможе згенерувати підпис для нового повідомлення.

У доведенні безпеки Wave використовується зведення атаки на підпис до двох основних задач:

1. DOOM (n, k, w, q) – задача знаходження вектора $e$ фіксованої ваги $w$, яке задовольняє хоча б одне з q рівнянь виду (5).

2. DWK (Distinguishing Wave Keys) – задача визначення, чи є задана матриця відкритого ключа переставленою пасткою (U ||U+V)-коду, чи випадковою.

Формально ймовірність успішної атаки оцінюється як

$$\Pr[forge] \leq 2.(Adv_{DOOM} + Adv_{DWK} + \frac{q_s^2}{2^{\lambda_0}}), \quad (7)$$

де $q_s$ – кількість запитів до оракула підпису, а $\lambda_0$ – довжина salt, яка завжди більше 256.

Відкритий ключ Wave – результат маскування структури коду $(U\|U+V)$ шляхом перестановки $\pi$ і додавання векторів $b$ і $c$. Утворений код має вигляд

$$\pi(U\|(U+V))+b+c. \quad (8)$$

Задача DWK передбачає, що зловмисник намагається розпізнати, чи цей код має приховану структуру, тобто є переставленою версією $(U\|U+V)$-коду. Відомо, що жоден ефективний метод не здатен надійно вирішити цю задачу без знання перестановки $\pi$, особливо коли параметри $n$ і $k$ великі, як у Wave822, Wave1272 та Wave1906.

Щоб запобігти витоку інформації про секретний ключ через спостереження за великою кількістю підписів, у Wave реалізовано механізм відхилення зразків (rejection sampling) [11]. Підпис формується лише в разі, якщо згенерований вектор помилок $e$ належить спеціальному розподілу $D$, який не залежить від ключа.

Зокрема, вектори $e$ формуються з використанням двох внутрішніх розподілів: $DV$ – для частини помилки, яка декодується V-кодом; $DU$ – для помилки в U-коді.

Розподіл усіх підписів наближено до рівномірного на множині векторів фіксованої геммінгової ваги. В [11] показано, що Реньї-дивергенція між реальним і ідеальним розподілом підписів не перевищує $2^{-68}$, тобто навіть за умови доступу до $2^{64}$ підписів, зловмисник не отримає статистично значущої інформації про секретний ключ.

Найефективнішими на практиці є атаки типу ISD (Information Set Decoding) – комбінаторні атаки, які намагаються знайти підмножину координат, де розв'язок має особливу структуру. У Wave ці атаки застосовуються як до задачі DOOM, так і до DWK, але складність залишається експоненційною навіть для найменших параметрів (Wave-822). Наприклад: для класичної моделі: складність $\approx 2^{128}$; для квантової моделі з алгоритмом Гровера: $\approx 2^{64}$, однак необхідна кількість оперативної пам'яті і квантостійкість salt не дозволяють реалізувати такі атаки на практиці.

Навіть за умов обмеження salt-простору, підробити підпис без знання секретного коду залишається складним. Зловмиснику необхідно: вгадати salt, для якого є придатний синдром; знайти вектор $e$ з відповідною геммінговою вагою, що задовольняє $He^{\intercal} = s$; забезпечити, щоб результат підпису пройшов перевірку розподілу. Виконання цих трьох умов одночасно є високоскладним у обчислювальному сенсі, навіть за умов знання великої кількості валідних підписів.

У сукупності наведені властивості забезпечують високий рівень стійкості Wave як у класичній, так і в квантовій моделі атак. Жодна з відомих атак не дозволяє зламати навіть найменший параметр (Wave822) при адекватному рівні обчислювальних ресурсів, що робить цю схему однією з найперспективніших серед постквантових алгоритмів цифрового підпису.

### 2.3. Постквантовий алгоритм цифрового підпису Biscuit

Biscuit – сучасна криптографічна схема цифрового підпису, що базується на складності розв'язування систем багатосторонніх квадратичних рівнянь (MQ), яка вважається стійкою до атак з боку квантових комп'ютерів. Biscuit є однією з небагатьох MQ-схем нового покоління, яка поєднує компактність підпису, порівняно низькі вимоги до обчислювальних ресурсів та оригінальний підхід до обфускації структурних елементів схеми.

Алгоритм розроблено з урахуванням новітніх криптоаналітичних атак на попередні MQ-схеми (наприклад, Rainbow) і має за мету запропонувати підпис, що поєднує в собі гнучкість параметрів безпеки та придатність до використання в практичних сценаріях. У цьому підрозділі детально розглядається математична основа, криптографічна стійкість, продуктивність та вимоги до реалізації алгоритму Biscuit з метою визначення його потенціалу як надійного постквантового рішення.

#### 2.3.1. Математична задача, на якій базується стійкість алгоритму Biscuit

Протокол багатосторонніх обчислень (MPC) – це протокол, який виконується набором з $N$ учасників, які знають відкриту функцію $f$. Мета протоколу – обчислити зображення $z$:

$$z = f(x_1, \dots, x_N), \tag{9}$$

де значення $x_i$ відоме тільки $i$-й стороні.

Протокол MPC вважається безпечним і коректним, якщо в кінці протоколу кожна сторона $i$ знає $z$, і ніяка інформація про її секретне вхідне значення $x_i$ не стає відомою іншим сторонам.

Алгоритм постквантового цифрового підпису Biscuit побудований на проблемі розв'язування багатосторонніх рівнянь, визначених як добуток двох афінних форм. Ця задача параметризується кортежем натуральних чисел *(n, m, q)*, який позначається як *PowAff2*.

Формально ця проблема визначається наступним чином [12]. Необхідно знайти вектор $(s_1, \dots, s_n) \in \mathbb{F}_q^n$, такий, що

$$f_1(s_1, \dots, s_n) = t_1, \dots, f_m(s_1, \dots, s_n) = t_1, \tag{10}$$

де

$$f_1(x_1, \dots, x_n) = A_{k,0}(x_1, \dots, x_n) + \prod_{j=1}^{2} A_{k,j}(x_1, \dots, x_n), \tag{11}$$

для усіх $k \in [m]$, якщо $t = (t_1, \dots, t_m) \in \mathbb{F}_q^m$, афінне перетворення $A_{k,j}(x_1, \dots, x_n) \in \mathbb{F}_q[x_1, \dots, x_n]$, $k \in [m]$ і $0 \le j \le 2$ [12].

Задачу *PowAff2* можна розглядати як структурований варіант задачі розв'язування $m$-квадратних рівнянь у $\mathbb{F}_q[x_1, \dots, x_n]$, тобто багатовимірної квадратної задачі (MQq). Відомо, що ця задача є NP-важкою [13].

При $m=n$ і для достатньо великого поля доведено, що поліноми *PowAff2*, поводяться як звичайні квадратичні поліноми. Очікується, що це також матиме місце у випадку $m>n$ [14], що розглядається у Biscuit.

Варто зазначити, що формальне доведення цього питання еквівалентне розв'язанню гіпотези Фреберга, яка є давньою проблемою у комутативній алгебрі. Таким чином, розв'язати випадкові випадки задачі *PowAff2* було б так само важко, як і випадкові екземпляри задачі $MQ_q$ розв'язування системи нелінійних квадратних рівнянь над скінченним полем $\mathbb{F}_q$ проти загальних алгоритмів.

Захищеність від загальних алгоритмів для задачі $MQ_q$ не виключає можливості існування потенційно нових швидших алгоритмів, які враховують структуру рівнянь або знання афінних карт $A_{k,j}$. Втім, поліноміальні системи зі структурою задачі *PowAff2* були широко вивчені раніше в постквантовій криптографії й наразі відповідних загроз винайдено не було.

**2.3.2. Стійкість алгоритма Biscuit до атак**

На сьогодні існує значна кількість алгоритмів, що розв'язують проблему $MQ_q$ [12]. Найактуальніші алгоритми включають:

1. Алгоритми для недовизначених систем. Система рівнянь називається недовизначеною, якщо вона має більше невідомих, ніж рівнянь, тобто в наших позначеннях $m<n$. Перший підхід полягає у фіксації значень $n-m$ невідомих і подальшому розв'язуванні відповідної квадратної системи рівнянь. Для систем, де $m$ набагато менше, ніж $n$, були запропоновані покращені алгоритми, наприклад алгоритм, запропонований Патаріним, Куртуізом та Губіним [15], алгоритм Thomae-Wolf [16] і його останню модифікацію, запропоновану Хірокі Фуруе, Шухей Накамура та Цуйоші Такагі [17].

2. Швидкий вичерпний пошук. Спосіб виконання полягає у вичерпному пошуку ${\mathbb{F}_2}^n$ шляхом нумерації простору розв'язку кодами Грея. Часова складність знаходження одного розв'язку задачі $MQ_2$ за допомогою цього алгоритму визначається як $4\log(n)2^n$. Цей підхід можна поширити на будь-яке поле $\mathbb{F}_q$ за допомогою лексикографічного впорядкування замість кодів Грея, з часовою складністю задається $O(dq^n)$ [18].

3. Базисні алгоритми Гребнера – це спеціальний набір багаточленів, який має ті ж самі корені, що й початковий набір, але володіє додатковими властивостями. Цей базис дозволяє легко вирішувати багато задач, пов'язаних із системами багаточленів, таких як розв'язання систем нелінійних рівнянь і перетворення між різними представленнями алгебраїчних структур. Існує кілька алгоритмів для побудови базисів Гребнера, серед яких найвідомішими є алгоритм Бухбергера і F4 та F5 алгоритми. Це алгоритм, що дозволяє знайти базис Гребнера шляхом послідовного додавання і спрощення багаточленів, а також його покращені версії, які використовують матричні методи і різні оптимізації для прискорення обчислень [12].

4. Гібридні підходи. У серії робіт автори описують гібридні методи, які поєднують вичерпний пошук і обчислення, подібні до базису Гребнера; що призводить до асимптотично швидких алгоритмів, наприклад алгоритму Hybrid-(F4/F5) і Crossbed. Ефективність таких підходів пов'язана з вибором компромісу між цими двома методами.

5. Імовірнісні алгоритми. Лоскштанов та інші були першими, хто ввів імовірнісні алгоритми, які в гіршому випадку розв'язують $MQ_q$ за час $O(q^{\delta n})$, для деякого $\delta < 1$, що залежить лише від $q$ і ступеня системи, не покладаючись на жодне недоведене припущення.

Щоб полегшити аналіз безпеки на основі $MQ_q$, Р. Макарім, К. Санна та Дж. Вербел [19] запровадили програмний інструмент під назвою MQEstimator, який дозволяє отримати рівень безпеки для вирішення даного екземпляра $MQ_q$ з урахуванням усіх можливих відомих атак.

Приблизну бітову складність можна оцінити як $(log\ q)^\theta$, помножену на $\mathbb{F}_q$-часову складність, з $\theta \in [1,2]$. З іншого боку, складність бітового простору просто дорівнює $log\ q$, помноженому на $\mathbb{F}_q$-просторову складність.

Іншу загрозу складають засоби квантовового криптоаналізу. Зазначимо найдоцільніші з них:

1. Квантовий вичерпний пошук. Перший квантовий алгоритм для $MQ_2$ належать П. Швейбу та Б. Вебштербауну [20]. Автори описали квантовий варіант вичерпного пошуку з

використанням алгоритму Гровера, як результат було отримано точні оцінки ресурсів для їхніх алгоритмів, які демонструють, що квантовий комп'ютер може розв'язувати $m$ двійкових квадратних рівнянь у $n$ двійкових змінних, використовуючи $O(m+n)$ кубітів і вимагаючи оцінки $O(mn^2 2^{n/2})$ квантових воріт. Автори також описують варіант із використанням меншої кількості кубітів, тобто $O(n + log_2(m))$, але з удвічі більшою кількістю квантових воріт, ніж перший підхід.

2. GroverXL. Автори запропонували квантовану версію XL, розглянувши варіант FXL, який поєднує XL з вичерпним пошуком. Принцип GroverXL полягає в поєднанні FXL з алгоритмом Гровера. GroverXL вирішує $MQ_q$ з часовою складністю $2^{(t+o(1)))n}$ комп'ютера з mesh-з'єднанням області $2^{(a+o(1)))n}$. Значення $t$ і $a$ можуть бути явно обчислені для заданих параметрів екземпляра $MQ_q$, що розглядається.

3. QuantumMQSolve. Пропонується й дещо інший підхід для поєднання квантових алгоритмів і базисів Гребнера. На сьогодні це найшвидший відомий квантовий алгоритм для вирішення $MQ_q$. Нехай:

$$m = \lceil \alpha n \rceil, \text{ де } \alpha \geq 1. \tag{12}$$

Для $q = 2$ QuantumMQSolve має середню складність:

$$O(2^{\left(\frac{1}{2} - 0.0375\alpha\right)n}). \tag{13}$$

Зокрема, для $\alpha = 1$ складність визначається як $O(2^{(0.462n)})$.

Коли $n = m \to \infty, q \to \infty$ і $log_2(q) \leq n$, QuantumMQSolve має середню складність:

$$O(2^{n\left(2.76 - \frac{1.26}{log_2(\sqrt{q})}\right)}). \tag{14}$$

Наведені нижче складності є асимптотичними та неточними для заданих параметрів *(q, n, m)*. Але вартість QuantumMQSolve також можна чітко обчислити шляхом мінімізації компромісу та використання більш точної форми складності.

4. Квантові алгоритми Гребнера. Новий підхід для розв'язання $MQ_2$ і більш загальний $MQ_q$ полягає у використанні квантового алгоритму А. Харроу, А. Хасідіма та С. Ллойда (HLL) для вирішення лінійних систем. Квантовий вичерпний пошук майже завжди є швидшим, ніж підхід HLL для $MQ_2$ Чена та Гао. Автори також запропонували вдосконалений варіант алгоритму Чена і Гао для $MQ_2$, складність якого експоненціальна у вазі Геммінга. Зокрема, ця версія перевершує квантовий вичерпний пошук, коли вага Геммінга рішення логарифмічна за кількістю змінних.

### 2.4. Постквантовий алгоритм цифрового підпису RYDE

Алгоритм RYDE (Rank-sYndrome-based Digital signaturE) – RYDE (Rank-sYndrome-based Digital signaturE) побудований на складності задачі декодування синдрому в ранговій метриці, що є NP-важкою і не має відомих квантових алгоритмів, здатних її ефективно розв'язати. На відміну від класичних кодових криптосистем у геммінговій метриці, використання рангової метрики дозволяє суттєво зменшити розміри ключів та підписів [21].

RYDE поєднує у своїй структурі кодові схеми з сучасними криптографічними техніками, такими як zero-knowledge докази та багатосторонні обчислення (MPC-in-the-head), що забезпечують високий рівень конфіденційності та автентичності. Цей підрозділ присвячено аналізу математичної основи, стійкості до криптоаналітичних атак, продуктивності та практичної реалізації алгоритму RYDE в умовах квантової загрози.

#### 2.4.1. Математична задача, на якій базується стійкість алгоритму RYDE

Схема цифрового підпису RYDE побудована на NP-складній задачі декодування синдрому в ранговій метриці – Rank Syndrome Decoding (Rank-SD). Це одна з фундаментальних задач у кодовій криптографії, яка залишається важкою навіть за умови використання кванто-

вих обчислень. Її складність зростає експоненційно з параметрами, і саме це забезпечує криптографічну стійкість алгоритму.

Rank-SD є узагальненням задачі декодування синдрому, що широко використовується в класичних схемах McEliece або Niederreiter, але замість метрики Геммінга тут використовується рангова метрика. У ранговій метриці вага вектора визначається як ранг відповідної матриці, яка утворюється з координат вектора при розкладі над основним полем. Таким чином, вага рангу є мінімальною розмірністю підпростору, що містить усі координати вектора.

Формально задача Rank Syndrome Decoding визначається таким чином: дано випадкову матрицю $H \in \mathbb{F}_{q^m}^{(n-k)\times n}$, а також вектор $y$, що має рангову вагу не більше за деяке $r$:

$$y = Hx, x \in \mathbb{F}_{q^m}^{n}. \tag{15}$$

Необхідно знайти вектор $x$, знаючи $H$ та $y$. Ця задача зберігає свою складність навіть у випадку випадкових кодів, і є доведено складною у сенсі NP-повноти [22].

В основі схеми RYDE лежить перетворення задачі знання рішення Rank-SD у доказ із нульовим розголошенням знань. Для цього використовується так званий підхід MPC-in-the-Head, при якому імітується багатосторонній протокол обчислень (MPC), де кожна «партія» володіє часткою секретного вектора $x$. За допомогою цього підходу будується інтерактивний доказ володіння рішенням до задачі Rank-SD, який згодом перетворюється на підпис завдяки трансформації Фіата-Шаміра.

Відмітною особливістю рангової метрики є значно менша кількість можливих векторів заданої ваги порівняно з метрикою Геммінга. Це дозволяє побудувати компактніші підписи без втрати стійкості. Крім того, проблема Rank-SD демонструє високу стійкість як до комбінаторних атак (перебору підтримки вектора), так і до алгебраїчних атак, таких як методи базисів Гребнера. Складність атак істотно зростає з параметрами та лишається високою навіть при застосуванні квантових алгоритмів (наприклад, Гровера).

Таким чином, безпека схеми підпису RYDE прямо залежить від складності задачі Rank Syndrome Decoding, що робить її перспективним кандидатом у сфері постквантової криптографії.

### 2.4.2. Стійкість алгоритму RYDE до атак

Схема цифрового підпису RYDE базується на задачі декодування синдрому в ранговій метриці (Rank-SD), що є NP-складною. Однак для повноти аналізу безпеки важливо розглянути не лише математичну складність базової задачі, а й стійкість алгоритму до конкретних типів атак, що можуть бути застосовані проти як Rank-SD, так і проти структури підпису як такого. У цьому підрозділі розглянуто основні напрями атак: комбінаторні, алгебраїчні, атаки на схему підпису на основі доказів з нульовим розголошенням знань, а також вплив квантових алгоритмів.

Найбільш класичними атаками на Rank-SD [22] є комбінаторні методи, які зводяться до перебору можливих підтримок (підпросторів) секретного вектора. Основна ідея полягає в тому, щоб вгадати підпростір $E \subset F_{q^m}$, що містить підтримку вектора $x$, і потім перетворити рівняння (15) у систему лінійних рівнянь над полем $F_q$.

Найвідомішим є алгоритм Chabaud-Stern, складність якого оцінюється як

$$O((nr + M)^3 \cdot q^{(m-r)(r-1)}), \tag{16}$$

де $n$ – довжина вектора, $r$ – ранг вектору, $m$ – розмірність поля.

Через експоненційний множник $q^{(m-r)(r-1)}$ атака стає непридатною при достатньо великих параметрах, які використовуються в RYDE.

Інший метод – це GRS-алгоритм, що є адаптацією методу інформаційного множини для рангової метрики. Його ефективність залежить від ймовірності вгадати підпростір, що містить підтримку вектора, і складність також має експоненційну залежність від параметрів виду

$$O((n-k)^3 m^3 \cdot q^{r\cdot\left\lfloor\frac{(k+1)m}{n}\right\rfloor}). \quad (17)$$

У RYDE ці атаки не є ефективними, оскільки схема використовує параметри, близькі до межі Гілберта–Варшамова в ранговій метриці, що забезпечує мінімальну ймовірність вгадування підтримки.

Алгебраїчні атаки формулюють задачу Rank-SD як систему поліноміальних рівнянь і розв'язують її методами алгебраїчної геометрії (наприклад, базисами Гребнера). Найефективнішими на сьогодні є:

MaxMinors Modeling – метод, що формує систему рівнянь на основі мінорів добутку матриць;

Support Minors Modeling – розширення попереднього підходу, яке зменшує кількість змінних за рахунок фіксації частини підтримки.

Для обох моделей існує гібридний метод, який фіксує деякі змінні (припущення) та перебирає всі їх значення, зменшуючи розмір системи, але збільшуючи кількість запусків. У будь-якому разі ці підходи залишаються експоненційно складними при параметрах, рекомендованих для схеми RYDE.

У контексті постквантової безпеки важливо враховувати можливість застосування квантових алгоритмів:

- алгоритм Гровера дозволяє прискорити перебір до $O(2^{\frac{n}{2}})$ замість $2^n$, що впливає на комбінаторні атаки;

- для алгебраїчних методів, зокрема тих, що базуються на базисах Гребнера, переваги квантових обчислень наразі не доведені, тобто ці атаки не покращуються на квантових комп'ютерах.

Розробники RYDE встановили параметри, що вдвічі перебільшують мінімально необхідні для стійкості до квантових атак. Наприклад, для рівня безпеки AES-128, складність атаки Rank-SD повинна бути щонайменше $2^{256}$, що дозволяє квантове зниження до $2^{128}$ [21].

Схеми підпису, що базуються на доказах з нульовим розголошенням знань, також уразливі до так званих атаки Калеса–Заверучі, які використовують факт повторного використання випадковостей у кількох сесіях доказу. Вони дозволяють зменшити складність підробки, якщо кількість раундів кількість раундів MPC-симуляції $\tau$ недостатня. Значення $\tau$ у схемі RYDE обране так, щоб атака Калеса–Заверучі не давала жодної практичної переваги. Крім того, алгоритм використовує гіперкубову структуру для подання MPC-партій, що дозволяє приховати інформацію при відкритті лише частини протоколу.

Як і для будь-якої схеми підпису, важливо враховувати можливість атак за багаторазовим використанням. У RYDE зловмисник потенційно може мати доступ до великої кількості пар повідомлення-підпис. Схема проєктувалась таким чином, щоб:

- кожен підпис був унікальним завдяки випадковим сольовим значенням;

- кількість інформації, яка розкривається в MPC-протоколі, контролюється через вибір параметра $N$ (кількість партій);

- параметри обрані так, щоб статистичний аналіз підписів не давав змоги відновити частини секретного ключа.

Таким чином, схема RYDE демонструє високу стійкість до всіх відомих типів атак:

- NP-складна математична основа (Rank-SD);

- низька ймовірність вгадування підпростору підтримки;

- стійкість до атак на перетворення Фіата–Шаміра через налаштування $\tau$ і MPCitH;

- стійкість до квантових атак завдяки подвоєній оцінці параметрів.

У сукупності це робить RYDE одним із найбільш надійних алгоритмів цифрового підпису в умовах як класичних, так і квантових загроз.

**Висновки**

Постквантові алгоритми цифрового підпису є ключовим напрямом сучасної криптографії, які гарантують безпеку даних у майбутньому світі з квантовими комп'ютерами. Різноманіття підходів дозволяє обрати оптимальний алгоритм для конкретних умов використання, але також ставить перед викликами, пов'язаними з ефективністю та розміром ключів. Подальші дослідження в цій галузі є вкрай необхідними для забезпечення безпеки інформації у квантову еру.

Проведене дослідження алгоритмів цифрового підпису, стійких до квантового криптоаналізу, дозволило системно проаналізувати один із найактуальніших напрямів сучасної криптографії, що виник у відповідь на стрімкий розвиток квантових обчислювальних технологій. У ході роботи досліджено чотири алгоритми цифрового підпису, подані до четвертого раунду конкурсу NIST: FuLeeca, Biscuit, Wave та RYDE. Вибір саме цих алгоритмів пояснюється їхньою різною математичною природою, а також потенціалом для використання в сучасних IT-системах із різним рівнем ресурсних обмежень.

Дослідження алгоритму FuLeeca підтвердило його концептуальну ефективність у контексті постквантової криптографії, однак виявило критичні вразливості при наявності побічних каналів витоку інформації. Попри математичну надійність конструкції на рівні базової моделі, практична безпека значною мірою залежить від фізичного середовища реалізації. Атака FuLeakage демонструє можливість витягнення секретного ключа за допомогою машинного навчання, навіть без повного доступу до внутрішнього стану системи. Це свідчить про необхідність інтеграції контрзаходів на рівні реалізації, зокрема технік маскування або шумозахисту. Хоча FuLeeca не є універсально скомпрометованою схемою, її практичне використання потребує серйозного перегляду підходів до безпечної реалізації. Подальші дослідження повинні зосередитися на розробці захищених реалізацій та перевірці стійкості до широкого спектра побічних атак.

Алгоритм Wave є багатосторонньою схемою цифрового підпису, побудованою на кодах та використанні гаусового приховування. Його відмінною рисою є відсутність структури в матрицях приватного ключа, що потенційно підвищує стійкість до структурних атак. Проведений аналіз підтвердив коректність роботи алгоритму, а також теоретичну стійкість до атак, що використовують класичні та квантові обчислення. Попри публікації, в яких пропонувались потенційні атаки на Wave, жодна з них не продемонструвала практичного компрометування схеми за рекомендованих параметрів. Ключовим елементом забезпечення безпеки залишається правильна реалізація вибірки підписів із використанням rejection sampling. Саме ця процедура унеможливлює витоки інформації, що могли б бути використані для відновлення секретного ключа. Слід зауважити, що Wave не пройшов до фінальних етапів початкового конкурсу NIST через відкликання заявки з боку авторів, однак вартий розгляду як перспективний стійкий до квантового криптоаналізу алгоритм.

Аналіз алгоритму Biscuit показав, що ця MQ-схема є перспективним кандидатом для застосування в постквантових умовах, завдяки високій стійкості до квантового криптоаналізу та порівняно помірним вимогам до апаратного забезпечення. Алгоритм демонструє хорошу продуктивність при генерації ключів, підписанні та перевірці, а також забезпечує гнучке налаштування параметрів для досягнення різних рівнів безпеки. Особливою перевагою Biscuit є його захист від сучасних атак на структуру MQ-схем завдяки ефективним методам приховування внутрішніх параметрів. Водночас деякі обмеження, зокрема пов’язані з розміром відкритого ключа та необхідністю ретельної параметризації, залишають простір для подальших досліджень і оптимізацій. Загалом, Biscuit може розглядатися як реалістична альтернатива для реалізації квантово-стійких електронних підписів, особливо в контексті систем, що потребують високого рівня безпеки та підтримують багатосторонню криптографічну основу.

Дослідження алгоритму RYDE підтверджує його потенціал як криптографічної схеми, здатної забезпечити високий рівень безпеки в умовах епохи квантових обчислень. Алгоритм

демонструє достатні показники ефективності, зокрема – відносно невеликі розміри ключів і підписів, що є перевагою над деякими іншими PQDS-схемами. Застосування складної задачі декодування синдрому в ранговій метриці як основи стійкості робить RYDE несприйнятливим до широкого спектру як класичних, так і квантових атак. Крім того, використання концепції zero-knowledge і багатосторонніх обчислень у проєктуванні алгоритму підвищує довіру до його криптографічних властивостей. Разом з тим, складність реалізації MPC-підходу може створювати додаткові виклики при імплементації в обмежених середовищах. Проте загальний баланс між безпекою, продуктивністю та ефективністю дозволяє вважати RYDE одним із сильних кандидатів для стандартизації та подальшого впровадження в системи, що потребують високого рівня криптографічного захисту.

**Список літератури:**


1. Additional PQC Digital Signature Candidates Announced | Computer Security Resource Center. URL: https://csrc.nist.gov/news/2023/additional-pqc-digital-signature-candidates
2. Post-Quantum Cryptography: Digital Signature Schemes | Computer Security Resource Center. URL: https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures
3. Nicolas T Courtois, Matthieu Finiasz, and Nicolas Sendrier. How to achieve a McEliece-based digital signature scheme. B Advances in Cryptology–ASIACRYPT 2001 // 7th International Conference on the Theory and Application of Cryptology and Information Security Gold Coast, Australia, December 9-13, 2001 Proceedings 7, pages 157-174. Springer, 2001.
4. Stefan Ritterhoff, Sebastian Bitzer, Patrick Karl, Georg Maringer, Thomas Schamberger, Jonas Schupp, Georg Sig,l Antonia Wachter-Zeh, Violetta Weger. FuLeeca Submission to the NIST Post-Quantum Cryptography Standardization Process Algorithm Specifications and Supporting Documentation // Technical University of Munich, Germany. 2023. URL: https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/FuLeeca-spec-web.pdf.
5. Anna-Lena Horlemann-Trautmann and Violetta Weger. Information set decoding in the Lee metric with applications to cryptography // Advances in Mathematics of Communications. 2001. 15(4).
6. Violetta Weger, Karan Khathuria, Anna-Lena Horlemann, Massimo Battaglioni, Paolo Santini, and Edoardo Persichetti. On the hardness of the Lee syndrome decoding problem // Advances in Mathematics of Communications, April 2022. Publisher: Advances in Mathematics of Communications.
7. Craig Gentry. Key recovery and message attacks on ntru-composite. In Advances in Cryptology–EUROCRYPT 2001 // International Conference on the Theory and Application of Cryptographic Techniques Innsbruck, Austria, May 6-10, 2001 Proceedings 20, pages 182-194. Springer, 2001.
8. Carl Löndahl, Thomas Johansson, Masoumeh Koochak Shooshtari, Mahmoud Ahmadian-Attari, and Mohammad Reza Aref. Squaring attacks on McEliece public-key cryptosystems using quasicyclic codes of even dimension // Designs, Codes and Cryptography. 2016. 80:359-377.
9. Round 1 (Additional Signatures) OFFICIAL COMMENT: FuLeeca. URL: https://eprint.iacr.org/2024/353
10. Gustavo Banegas et al. Wave Round 1 Submission . NIST Computer Security Resource Center | CSRC. URL: https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/wave-spec-web.pdf .
11. Bénéteau J., Deneuville J.-C., Gaborit P., & Zémor G. Wave: A new family of trapdoor one-way preimage sampleable functions based on codes. Post-Quantum Cryptography, PQCrypto 2019. URL: https://doi.org/10.1007/978-3-030-25510-7_15.
12. Luk Bettale, Delaram Kahrobaei. Biscuit: Shorter MPC-based Signature from PoSSo. URL: https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/Biscuit-spec-web.pdf.
13. M. R. Garey and David S. Johnson. Computers and Intractability: A Guide to the Theory of NP-Completeness. W. H. Freeman, 1979.
14. Lisa Nicklasson. On the hilbert series of ideals generated by generic forms // Communications in Algebra.2016. No45(8). P.3390–3395.
15. Aviad Kipnis, Jacques Patarin, and Louis Goubin. Unbalanced oil and vinegar signature schemes // Jacques Stern, editor, Advances in Cryptology – EUROCRYPT ’99. P. 206–222. Berlin, Heidelberg, 1999. Springer Berlin Heidelberg.
16. Enrico Thomae and Christopher Wolf. Solving underdetermined systems of multivariate quadratic equations revisited // Marc Fischlin, Johannes Buchmann, and Mark Manulis, editors, Public Key Cryptography – PKC 2012. P. 156 Berlin, Heidelberg, 1999. Springer Berlin Heidelberg.171. Springer Berlin Heidelberg 012.
17. H. Furue, S. Nakamura, and T. Takagi. Improving Thomae-Wolf algorithm for solving underdetermined multivariate quadratic polynomial problem // J. H. Cheon and J.-P. Tillich, editors, PQcrypto 2021. LNCS. P. 65–78, Cham, 2021. Springer International Publishing.
18. Hiroki Furue and Tsuyoshi Takagi. Fast enumeration algorithm for multivariate polynomials over general finite fields // Cryptology ePrint Archive, Paper 2023/619, 2023. https://eprint.iacr.org/2023/619.

19. Emanuele Bellini, Rusydi H. Makarim, Carlo Sanna, and Javier A. Verbel. An estimator for the hardness of the MQ problem. In Lejla Batina and Joan Daemen, editors, Progress in Cryptology – AFRICACRYPT 2022 // 13th International Conference on Cryptology in Africa, AFRICACRYPT 2022, Fes, Morocco, July 18-20, 2022, Proceedings, Lecture Notes in Computer Science. P. 323–347. Springer Nature Switzerland, 2022.

20. Peter Schwabe and Bas Westerbaan. Solving binary MQ with grover's algorithm // Claude Carlet, M. Anwar Hasan, and Vishal Saraswat, editors, Security, Privacy, and Applied Cryptography Engineering – 6th International Conference, SPACE 2016, Hyderabad, India, December 14-18, 2016, Proceedings, volume 10076 of Lecture Notes in Computer Science. P. 303–322. Springer, 2016.

21. Nicolas Aragon et al. RYDE specifications. NIST Computer Security Resource Center | CSRC. URL: https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/ryde-spec-web.pdf

22. Rahul Mishra, Bhupendra Singh, Radhakrishnan Delhibabu. Searching for S-boxes with better Diffusion using Evolutionary Algorithm. IACR Cryptology ePrint Archive. URL: https://eprint.iacr.org/2023/353

*Надійшла до редколегії 20.10.2025*

*Відомості про авторів:*

**Тельнова Аліна Анатоліївна** – Харківський національний університет імені В. Н. Каразіна, магістр кафедри кібербезпеки інформаційних систем, мереж і технологій, Україна; e-mail: telnova.alina@student.karazin.ua; ORCID: https://orcid.org/0009-0001-3574-7425

**Гріненко Тетяна Олексіївна** – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри безпеки інформаційних технологій, Україна; e-mail: tetiana.grinenko@nure.ua; ORCID: https://orcid.org/0000-0002-8251-8991

**Нарєжній Олексій Павлович –** канд. техн. наук, Харківський національний університет імені В.Н. Каразіна, доцент кафедри кібербезпеки інформаційних систем, мереж і технологій, Україна; e-mail: o.nariezhnii@karazin.ua; ORCID: https://orcid.org/0000-0003-4321-0510