МЕТОДИ ТА АЛГОРИТМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

УДК 004.056.55 **DOI:10.30837/rt.2021.2.205.01**

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

ОСНОВНІ ПОЛОЖЕННЯ ТА РЕЗУЛЬТАТИ ПОРІВНЯННЯ ВЛАСТИВОСТЕЙ ЕЛЕКТРОННИХ ПІДПИСІВ ПОСТКВАНТОВОГО ПЕРІОДУ НА АЛГЕБРАЇЧНИХ РЕШІТКАХ

Вступ

Постквантові проєкти стандартів електронних підписів (ЕП) Falcon [1] та Dilithium [2] є фіналістами, тобто двома із трьох переможців другого раунду конкурсу NIST США [3]. Наразі вони досліджуються на третьому раунді і при позитивних результатах дослідження можуть бути прийняті в якості міжнародних постквантових стандартів ЕП. При їх побудуванні використано математичний апарат алгебраїчних решіток та відповідні методи. При подальшому дослідженні та порівнянні вказаних постквантових проєктів стандартів ЕП, як з теоретичних, так і практичних позицій, основоположним є обґрунтування вимог до параметрів та ключів та у цілому обчислення основних показників згідно прийнятих умовних та безумовних критеріїв [4, 5]. Важливим при таких дослідженнях є визначення достатності забезпечення гарантованості їх захищеності від класичних, квантових, спеціальних та атак на основі помилок [1 – 5]. Вказане може бути забезпеченим, у тому числі, засобом обґрунтованого вибору розмірів загальних параметрів та ключів [6, 7] та практичного їх побудування згідно з прийнятою моделлю безпеки [4, 8, 9]. Але при виборі розмірів загальних параметрів та ключів виникає суттєве протиріччя між властивостями проєктів стандартів ЕП Falcon та Dilithium щодо стійкості та складності перетворень. Так, збільшення розмірів загальних параметрів та ключів приводить до збільшення складності перетворень, і навпаки [6, 7]. Що стосується теоретичних методів щодо побудування загальних параметрів та ключів для ЕП Falcon та Dilithium, то вони у цілому зрозумілі, а якщо використовувати [1, 2, 6, 7], то існує можливість їх побудувати і для більш високих рівнів безпеки, наприклад запропонованих та реалізованих у [6, 7] 6 та 7 рівнів безпеки, коли може бути забезпечено 384 та 512 біт захисту від класичних атак і 192 та 256 біт захисту від квантових атак, а також захищеність від спеціальних атак та атак на основі помилок [1 – 3, 10 – 17]. У цілому, в певному плані існує необхідність уточнення теоретичних питань та безумовна необхідність практичного побудування загальних параметрів та ключів для забезпечення 6 та 7 рівнів безпеки та оцінки і порівняння вказаних проєктів ЕП згідно з запропонованими безумовними, умовними та прагматичними критеріями [6, 7]. Причому, вирішення цих проблемних питань зводиться до реалізації відповідних моделей безпеки, побудованих на основі реальних моделей порушника та загроз.

Мета статі:

1) Аналіз проблемних питань вибору розмірів параметрів та ключів для постквантових проєктів ЕП, побудованих на основі математичних методів Falcon [1] та Dilithium [2], та особливості їх реалізації, в тому числі і реалізації відповідно до прийнятої моделі безпеки.

2) Порівняльний аналіз стійкості та складності проєктів стандартів ЕП Falcon та Dilithium у залежності від розмірів параметрів та ключів, в тому числі для 6 та 7 рівнів безпеки.

3) Розробка пропозицій стосовно рішень щодо прийняття в якості національних постквантових стандартів ЕП на основі математичних методів Falcon та Dilithium.

4) Визначення впливу безумовних, умовних та прагматичних критеріїв на переваги при прийнятті рішення щодо стандартизації ЕП на основі математичних методів Falcon та

Dilithium, в тому числі з урахуванням наявності патентів та необхідності отримання ліцензій тощо.

1. Основні параметри та ключі ЕП Falcon та Dilithium

1.1. Основні параметри та ключі алгоритму Falcon та дані щодо їх розмірів

Нехай розмір відкритого ключа є (PK_SIZE), розмір ЕП (DS_SIZE), а час (складність) перевірки підпису є (CHECK_TIME). В якості загального параметру виберемо степінь поліному n. Основний розгляд проведемо для п'ятого рівня безпеки щодо захищеності від квантових атак з використанням квантових комп'ютерів [1, 2, 18 – 20]. Вище прийняті позначення вибрані з урахуванням узгодженості з програмним забезпеченням.

При дослідженнях використано наступні формули для алгоритму Falcon [1].

Довжина відкритого ключа:

PK_SIZE=$1+n*\log_2 q$, де:

n – степінь полінома, модуль, що визначає основне поле x^n+1, n=1024 (5 рівень безпеки);

q – просте число, модуль для коефіцієнтів,

q=12289, $\log_2 q$=14; DS_SIZE – довжина ЕП.

ЕП обчислюється з використанням довжини випадкового компонента nonce (40 октетів), упакованого формату поліному, коефіцієнти якого задовольняють розподілу Гауса. Довжина коефіцієнту в упакованому форматі залежить від його значення і може займати від 8 до 23 бітів. Тому щодо довжини ЕП автори використовують середнє значення.

1.2. Основні параметри та ключі алгоритмів Dilithium та Falcon, та дані щодо їх розмірів

При дослідженнях використаємо такі основні формули для алгоритму Dilithium [2].

Довжина відкритого ключа:

PK_SIZE=SEED_SIZE+$n*k*(\log_2 q–d)$, де:

SEED_SIZE – розмір випадкового компоненту для відновлення матриці A (32 октету);

n – степінь полінома, модуль, визначає основне поле x^n+1, n=256;

q – просте число, модуль для коефіцієнтів, q=8380417;

d – кількість бітів в молодшій частині коефіцієнтів поліному (d=13);

k – довжина вектору, який складається з поліномів. Кожний поліном містить n коефіцієнтів розміром $w=\log_2 q–d$ бітів; k=8, w=10.

Довжина ЕП Dilithium:

DS_SIZE=SEED_SIZE+$l*n*\log_2 2\gamma_1+(\omega+k)$, де:

SEED_SIZE – розмір компоненту для відновлення поліному по модулю 3, який складається з заданої кількості ненульових елементів;

γ_1 – задає розмір коефіцієнту поліномів $\gamma_1=2^{19}$;

l – довжина вектору, який складається з поліномів (l=7). Кожний поліном містить n коефіцієнтів розміром $w=\log_2 2\gamma_1$ (w=20);

ω – кількість ненульових елементів в бітовій матриці переносів h (ω=75);

k – кількість рядків в матриці переносів (k=8).

Результати розрахунків розмірів відкритих ключів є (PK_SIZE), ЕП (DS_SIZE) та складностей (часових) перевірки підписів (CHECK_TIME) для алгоритмів Falcon та Dilithium для 5-го рівня безпеки наведені і в табл. 1.

Таблиця 1

Порівняння основних показників для алгоритмів Falcon та Dilithium

Алгоритм	PK_SIZE (октетів)	DS_SIZE (октетів)	CHECK_TIME (тактів)
Dilithium, n=256	2592	4595	279936
Falcon, n=1024	1793	1233.29[1]	168498

Як видно з табл. 1, алгоритм Dilithium згідно з наведеними параметрами програє алгоритму Falcon.

[1] Розмір ЕП змінюється в зв'язку з особливістю кодування поліному, коефіцієнти якого задовольняють розподілу Гауса. Кількість бітів для кодування одного коефіцієнту може змінюватись в інтервалі 8 – 24 біта, 8 бітів – найбільш імовірна довжина, 24 біта – найменш імовірна.

1.3. Порівняння основних параметрів та ключів ЕП Falcon та ЕП Dilithium для алгоритмів 7 рівня безпеки

На основі математичних методів Falcon [1] та Dilithium [2] розроблено проєкти стандартів ЕП «Вершина 1» та «Вершина 2» 7 рівня криптостійкості 512 біт захисту від класичних атак та 256 біт захисту від квантових атак [6, 7]. В табл. 2 наведені основні показники для цих алгоритмів в разі збільшення степені n та застосування решти необхідних параметрів.

Таблиця 2

Порівняння основних показників для алгоритмів 7 рівня безпеки, побудованих на базі методів ЕП Falcon та Dilithium

Алгоритм	PK_SIZE (октетів)	DS_SIZE (октетів)
Прототип Dilithium, n=512	5824	10708
Прототип Falcon, n=2048	3585	4884

Також, аналогічно як із табл. 1, із табл. 2 випливає, що алгоритм Dilithium відповідно до розглянутих параметрів програє алгоритму Falcon, але генерація ключів та формування ЕП для алгоритму Falcon та його прототипів потребує від розробника застосування багатьох різних алгоритмів та форматів, що може привести к значному звуженню практичного застосування алгоритму ЕП Falcon.

2. Рекомендації щодо практичної реалізації алгоритму ЕП Falcon

Нижче розглянуто практичні рекомендації із генерації ключів для алгоритму Falcon [1]. На наш погляд, цей опис може значно полегшити реалізацію алгоритму для розробників. Ці рекомендації особливо актуальні в умовах збільшення значення степені полінома n до 2048 для забезпечення підвищення криптостійкості включно до 7 рівня [4, 5]. Для цього в якості решітки в алгоритмі застосовується NTRU решітка.

В якості секретних ключів для забезпечення 5 рівня безпеки [1, 3] застосовуються:

- короткі вектори f, g, коефіцієнти яких задовольняють розподілу Гауса та за модулем не перевищують 32;
- короткі вектори F, G, коефіцієнти яких за модулем не перевищують 128 та задовольняють NTRU рівнянню:

$$f^*G - Fg = q. \tag{1}$$

В якості відкритого ключа застосовується поліном, обчислений за формулою

$$h = f^{-1} * g \text{ в полі } Z[x]/(\phi, q), \tag{2}$$

де ϕ – поліном $x^{1024}+1$.

Для обчислення відкритого ключа h застосовується NTT формат [1], що допустимо завдяки спеціальному вибору q. Але випадковий поліном f може не мати інверсію в полі $Z[x]/(\phi, q)$, тоді необхідно сформувати нову пару поліномів f, g. Обчислення ключів f, g, коефіцієнти яких задовольняють розподілу Гауса, не тривіальна задача, особливо в умовах забезпечення захисту від спеціальних атак на основі константного часу обчислень. Обмеження на значення квадратичної норми для поліномів f, g також може привести до необхідності повтору операцій, що впливає на час генерації ключів. Перевірка квадратичної норми виконується не тільки для самих поліномів f, g, а також для поліномів, обчислених за формулою

$$f' = \frac{qf^*}{ff^*+gg^*},\ g' = \frac{qg^*}{ff^*+gg^*}. \tag{3}$$

Для обчислень (3) використовується комплексне подання чисел. Позначення f^*, g^* означають комплексно поєднані значення. Для поліномів f, g виконання операцій множення та ділення поліномів застосовує FFT формат. Таким чином, обчислення f, g, h потребує застосування двох спеціальних форматів NTT та FFT, а для множення за модулем застосовують арифметику Монтгомері [1, 23].

Для рішення NTRU рівняння в [1] запропонована така методика.

2.1. Поступовий перехід від поліномів для поля x^n+1 до поля $x+1$.

Поліном в полі x^n+1 містить n коефіцієнтів. При поступовому переході з поля x^r+1 до поля $x^{r/2}+1$ кількість коефіцієнтів зменшується в 2 рази, а значення цих коефіцієнтів збільшується. Для перетворення поліному p, заданого в полі x^r+1 в поліном $p\_$, заданого в полі $x^{r/2}+1$, виконуються наступні операції:

2.1.1. Для полінома p формуються два поліноми $p1$, $p2$ розміром $r/2$. Для цього в поліном $p1$ записуються коефіцієнти полінома p з парними, а в поліном $p2$ – з непарними номерами, тобто $p1[k]=p[2k]$; $p2[k] = p[2k+1]$; ($k = 0, \ldots r/2–1$);

2.1.2. Обчислюються поліноми $e_2=p_1^2$ та $o_2=p_2^2$ за модулем $x^{r/2}+1$;

2.1.3. Обчислюються коефіцієнти поліному – результату $p\_$ за формулами:

- $p\_[i+1]=e_2[i+1]–o_2[i]$ ($i=0\ldots r/2–2$);
- $p\_[0]=e_2[0]+o_2[i])$; ($i=t/2–1$).

Однакові операції виконуються для поліномів f, g. Позначимо відповідні результати $pf\_$ та $pg\_$ для поліномів f, g відповідно.

Для виконання операцій над коефіцієнтами необхідно виконувати опрацювання довгих чисел, ці операції виконуються без врахування модуля q. Так, при переході від поля $x^{1024}+1$ до поля x^1+1 отримаємо поліноми f', g', які містять по одному коефіцієнту значення якого для поля x^1+1 займає більше ніж 6000 бітів, тобто операції необхідно виконувати над даними, довжина яких значно перевищує довжину даних для інших несиметричних алгоритмів, наприклад, RSA.

Також в [1] не зберігають результатів перетворень, а для кожного поточного значення r для виконання зворотного перетворення обчислюють їх повторно, тому рекомендується їх зберігати, що збільшить навантаження на пам'ять, але зменшить час обчислення для кроку 3.

В результаті виконання цієї операції отримаємо два масиви поліномів, один для поліному f, інший для поліному g. Позначимо ці масиви відповідно pf, pg, $pf[0]$, що дає співпадання поліномому f, gp [0] з поліномом g. $pf[1]$ – результат перетворення полінома f в поліном в полі $x^{n/2}+1$, а $pg[1]$ – результат перетворення поліному g з поліному в полі $x^{n/2}+1$, … у поліном $pf[\log_2 n]$ – результат перетворення полінома f в поліном в полі $x+1$, $pg[\log_2 n]$ – результат перетворення полінома g в поліном в полі $x+1$. Поліноми $pf[\log_2 n]$, $pg[\log_2 n]$ містять по одному коефіцієнту. Позначимо їх lf, lg відповідно.

2.2. Для отриманих значень виконується розширений алгоритм Евкліда для вирішення діафантового порівняння і знаходження значень s, t, та найбільшого спільного дільника для lf, lg:

2.2.1. $lf*s+lg*t=gcd\ (lf, lg)$;

2.2.2. Якщо $gcd\ (lf, lg)\neq 1$, то знову переобчислюються значення f, g, h. Якщо $gcd\ (lf, lg)=1$, то після обчислення $lG=q*s$ та $lF=-q*t$ отримаємо тотожність: $lf*lG–lg*lF=q$ для поля $x+1$.

Значення lG, lF розглядаються як поліноми G, F для поля x^1+1, вони записуються замість $pf[\log_2 n]$ та $pg[\log_2 n]$ і далі необхідно для них виконати зворотне перетворення поліномів для обчислення F та G для поля x^n+1.

2.3. Виконується поступовий зворотний перехід від поля $x+1$ до полів x^2+1 … x^n+1. Вхідними даними для цього етапу є масиви поліномів pf, pg, отримані для полів $x+1$, x^2+1 … x^n+1. Результатом є поліноми F, G.

Для кожного $r = 1, 2, 4, \ldots n/2$ виконуються кроки 2.3.1–2.3.3.

2.3.1. Для зворотного переходу від поліному, заданому в полі x^r+1 до поліному p, заданому в полі $x^{2r}+1$ застосовуються поліноми pfr та pfr_2 з масиву pf для полів x^r+1, $x^{2r}+1$, поліноми pgr та pgr_2 з масиву $\underline{pg}$ для полів x^r+1, $x^{2r}+1$ відповідно. Далі, в процесі перетворення, виконуються такі операції:

- створюється 2 поліноми p_1, p_2 для поля $x^{2r}+1$. Поліном $p1$ формується з поліному *pfr* за рахунок виконання операцій:

$p_1[2k]=pfr\,[k]$; $p_1[2k]=0$; (k=0, 1, …r).

Поліном p_2 формується з поліному pg_2r за рахунок виконання таких операцій:

$p_2[2k]=pg_2r[2k]$; $p_2[2k+1]=-pg_2r[2k+1]$; (k=0, 1, …r);

- обчислюється поліном *pF* для поля $x^{2r}+1$: $pF_2r=p_1*p_2$ для поля $x^{2r}+1$;

- створюється 2 поліноми p_1, p_2 для поля $x^{2r}+1$. Поліном p_1 формується з поліному *pgr* за рахунок виконання операцій:

$p_1[2k]=pgr[k]$; $p_1[2k]=0$; (k=0, 1, …r);

Поліном p_2 формується з поліному pf_2r за рахунок виконання операцій:

$p_2[2k]=pf_2r\,[2k]$; $p_2[2k+1]=-pf_2r[2k+1]$; (k=0, 1,…r);

- обчислюється компонент масиву *pG* для поля $x^{2r}+1$: $pG_2r=p_1*p_2$ для поля $x^{2r}+1$.

2.3.2. Після переходу від поля $x^{r}+1$ до поля $x^{2r}+1$ виконується операція зменшення коефіцієнтів поліномів (reduce).

Вхідні дані для цієї операції:

значення *r*;

поліноми для поля $x^{2r}+1$: pf_2r, pg_2r;

поліноми *pF*, *pG*.

Результатом виконання таких операцій є поліноми *pF*, *pG*.

В результаті виконання цієї операції довжини коефіцієнтів поліномів зменшуються таким чином, щоб вони могли записатися в число з плаваючою точкою без втрати значущих цифр (для поточної реалізації передбачається 53 біта). Зменшення довжини виконується за рахунок виділення старших цифр поліномів.

Операція спочатку виконується для пари поліномів (pf_2r, pg_2r). Для пари визначається максимальна довжина коефіцієнту поліному (max, бітів), обчислюється параметр зсуву (scale=max–53) і виконується зсув усіх коефіцієнтів поліномів пари на задане значення в сторону молодших бітів (операція ділення коефіцієнтів на 2^{scale}). В результаті отримаємо поліноми, в яких довжина кожного коефіцієнту не перевищує 53 біта.

Обчислюється загальна квадратична норма для поліномів pf_2r, pg_2r. Позначимо її *pfg* (операція виконується для FFT формату).

2.3.3. Далі виконується цикл поступового зменшення довжини коефіцієнтів для пари (*pF*, *pG*):

- для пари визначається максимальна довжина коефіцієнту поліному (Max, бітів);

- якщо Max<max, то подальше зменшення неможливо, виконується вихід з циклу;

- обчислюється параметр зсуву (scale=Max–53) і виконується обчислення $lF_1=lF/2^{\text{scale}}$, $lG_1=lG/2^{\text{scaleт}}$;

- обчислюється загальна квадратична норма для поліномів lF_1, lG_1. Позначимо її *pFG* (формат FFT);

- обчислюється значення *d=pFG*/*pfg* (формат FFT);

- перехід від FFT формату до звичайного формату і округлення коефіцієнтів поліному *d* до цілих коефіцієнтів, якщо усі коефіцієнти дорівнюють 0, то вихід з циклу;

- обчислення $lF_1=d*lf \bmod x^{2r}+1$; $lG_1=d*lg \bmod x^{2r}+1$ (*lf*, *lg* – поліноми в полі $x^{2r}+1$);

- обчислення $lF=lF–lF_1*2^{\text{Max}-\text{max}}$; $lG=lG–lG_1*2^{\text{Max}–\text{max}}$.

Таким чином, генерація ключів передбачає застосування наступних методів і форматів:

- формування поліномів з коефіцієнтами, розміри яких обмежені і задовольняють розподілу Гауса;
- застосування NTT формату для фіксованого простого *q* для формування відкритого ключа і множення поліномів в разі застосування CRT формату представлення великих чисел;
- застосування FFT формату для виконання операції ділення для поліномів.

Перехід на початок формування ключів виконується, якщо:

- поліном *f* не має зворотного значення (1);

- квадратична норма коефіцієнтів поліномів f і g перевищує задане значення;
- квадратична норма коефіцієнтів поліномів f' і g' (2) перевищує задане значення;
- найбільший загальний дільник поліномів lf, lg не дорівнює 1.

Як показує аналіз алгоритмів формування ключів, найбільш ресурсно важкими є операції множення поліномів за модулем з коефіцієнтами – довгими числами. Зазвичай ці операції виконуються для декількох поліномів, що спрощує задачу їх паралельного виконання. Зберігання проміжних даних в загальній пам'яті, що практикують автори [1], напроти, ускладнюють задачу паралельного виконання. Тому рекомендується для тимчасового зберігання даних в функціях застосовувати локальну пам'ять.

3. Методи та алгоритми побудови загальних параметрів для ЕП типу Falcon у залежності від їх розмірів

3.1. Постановка проблеми побудування загальносистемних параметрів для Falcon N для 256 та 512 біт безпеки

Одним із основних завдань конкурсу є розробка та прийняття постквантового чи постквантових стандартів ЕП. Фіналістами другого етапу конкурсу NIST стали три механізми ЕП – Dilithium, Falcon та Rainbow [10].

Попередні дослідження показали, що серед схем ЕП на решітках дещо відрізняється від інших кандидатів Falcon [1, 21], він також має перспективи щодо прийняття в якості міжнародного стандарту ЕП. Домінуючим основним концептуальним підходом до проєктування механізму ЕП Falcon є використання перетворення типу «геш-і-підпис» [1, 21]. Перевагою такого підходу є доведена стійкість в межах моделі квантового випадкового оракула. В процесі досліджень виявлено, що навіть його аналізу присвячено значно менше робіт, ніж, щодо інших, наприклад проєкту ЕП Dilithium [2]. Крім того, як і щодо інших, при проєктуванні ЕП Falcon були прийняті обмеження щодо максимальних рівнів безпеки у вигляді максимально 256 біт проти класичного та 128 біт проти квантового криптоаналізу. Тому, як з точки зору теорії, так і практики, генерація загальносистемних параметрів для використання 384 і 512 біт безпеки проти класичного криптоаналізу та 192 і 256 біт безпеки проти квантового криптоаналізу є важливою проблемною задачею.

В якості основних властивостей розглянемо результати первинного аналізу щодо відомих атак на ЕП Falcon. При цьому врахуємо обмеження та практичні алгоритми обчислення загальносистемних параметрів та їх оптимізації для 256 та 512 біт безпеки проти класичного та не менше 128 та 256 біт проти квантового криптоаналізу. Важливим є проведення додаткових досліджень та прийняття рішення щодо реалізації рівнів 384 біт безпеки проти класичного та не менше 192 біт проти квантового криптоаналізу щодо ЕП Falcon. Сутність механізму Falcon наведено в [1, 21] і нижче не розглядається.

3.2. Аналіз атак на ЕП Falcon

Перетворення GPV [1], що використане в ЕП Falcon, вимагає, щоб геш-функція H була захищена від колізій. Це означає, що розмір солі в бітах повинен бути не меншим за 2λ, де λ – рівень безпеки, що вимагається. Проте, за умовами конкурсу NIST [4, 3] кількість запитів на вироблення ЕП (signature queries) є не більшою за $qs=2^{64}$, що вимагає цього розміру у вигляді $\lambda+\log_2(qs)$. В табл. 3 наведено вимоги щодо розмірів до для 5 – 7 рівнів безпеки ЕП Falcon.

Таблиця 3

Розмір (ентропія) початкового значення r (солі) в бітах

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

Попередній аналіз показав, що основними атаками щодо ЕП Falcon є атаки на відновлення особистого ключа з відкритого ключа ЕП та атаки на підробку ЕП. Розглянемо ці атаки.

3.3. Атаки на відновлення особистого ключа ЕП Falcon

Атаки на відновлення особистого ключа з відкритого ключа щодо Falcon можуть зводиться до вирішення проблеми NTRU [1]. У ряді криптосистем, стійкість яких ґрунтується на проблемі NTRU, коли поліноми f та g мають коефіцієнти з множини значень $\{0, 1, -1\}$, виникає проблема забезпечення стійкості проти комбінованих атак. Це робить можливим реалізувати різні комбінаторні атаки. Наприклад, для [24] найефективнішою атакою є гібридна атака, яка знаходить частину вектора комбінаторними шляхами, якщо не збільшувати розмір модуля n. Тому [24] для захисту від цієї атаки потрібно збільшити рівень безпеки до 2^{512}. Щодо Falcon такі атаки неможливі, оскільки поліноми f, g змінюються, точніше, вибираються згідно з нормальним розподілом з заданими параметрами. В даному випадку простір можливих значень поліномів збільшується настільки, що застосування комбінаторних методів стає неефективним. Тому залишається прямий шлях відновлення особистого ключа з відкритого засобом редукції базису решітки [1, 15 – 17]. При цьому, чим менші значення має норма найменшого вектора (f, g), тим більша криптостійкість системи. В криптосистемі Falcon поліноми генеруються над полем

$$Z_q[X]/(\phi(x)), \deg(\phi) = n$$

з математичним очікуванням рівним 0. Перетворення спираються на [1, 21], у яких детально досліджувалися можливості застосування алгоритмів вибірки нормально розподілених величин.

А основною умовою захисту ЕП Falcon від атак на відновлення особистого ключа ЕП з відкритого шляхом редукції є така

$$\left(\frac{B}{2\pi e}\right)^{\frac{2B-2n+1}{2B-2}} < \sqrt{\frac{3eB}{8n}}. \tag{4}$$

3.4. Атаки на підробку ЕП

Атаки на безпосередньо підробку ЕП можуть бути найбільш загрозливими. Тому іншим методом є атака підробки ЕП. При реалізації такої атаки потрібно знайти достатньо короткий вектор s. Відповідно, це можливо зробити, редукувавши базис так, щоб виконувалася умова [6]

$$\| b_1^* \| < \beta. \tag{5}$$

Причому оцінити $\| b_1^* \|$ можливо таким же чином, що і у попередньому випадку, тобто у такій послідовності:

$$\| b_1^* \| \approx GH(B)^{\frac{2n+1-2}{2(B-1)}} \det(\Lambda)^{\frac{1}{2n}} = GH(B)^{\frac{2n-1}{2B-2}} \sqrt{q} = \left(\frac{B}{2\pi e}\right)^{\frac{2n-1}{2B-2}} \sqrt{q}. \tag{6}$$

Отримуємо, що умовою захисту від атак на підробку підпису є

$$\left(\frac{B}{2\pi e}\right)^{\frac{2n-1}{2B-2}} \sqrt{q} < \beta. \tag{7}$$

Для практичного прийняття рішення необхідно визначитись щодо того, як обирати параметр β. Розробники ЕП Falcon N пропонують використовувати значення $\sigma = 1.55\sqrt{q}$ для

полінома $\phi = x^n + 1$ і $\sigma = 1.32 * 2^{1/4} * \sqrt{q}$ для полінома $\phi = x^n - x^{n/2} - 1$. Такий вибір σ базується на результатах роботи [1, 21], і параметр β для полінома $\phi = x^n + 1$ обчислюється як:

$$\beta = 1.2 * \sigma \sqrt{2nq}. \tag{8}$$

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

$$\beta^2 = \frac{(1.2 * \sigma * 2n\sqrt{q})^2}{n}. \tag{9}$$

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

Параметр q обирається згідно наступних міркувань [1, 9, 21, 14]:

- для захисту від алгебраїчних атак q має бути простим числом;
- якщо q буде занадто малим (порядку $q \approx n$), то будуть можливі BKW атаки;
- якщо q буде занадто великим ($q \approx n^{2.83}$), то будуть можливі атаки на підполе;
- якщо використовується поле $x^n + 1$, то для реалізації ефективного множення повинне виконуватися рівняння $q \equiv 1 \bmod 2n$;
- якщо використовується поле $x^n - x^{n/2} - 1$, то для реалізації ефективного множення повинне виконуватися рівняння $q \equiv 1 \bmod 3n$.

Необхідно відмітити, що стійкість найкращого алгоритму пошуку найменшого вектору оцінюється як $2^{0.292B}$, де B – розмір блоку при редукції. Якщо при криптоаналізі застосовувати алгоритм Гровера, то нижня оцінка класичної стійкості в 256 біт складає $2^{0.265B}$ квантової стійкості (при класичній стійкості в 256 біт). Тому, для ЕП на решітках квантова стійкість при класичній стійкості 256 біт набагато більше, ніж 128 біт [21, 22].

3.5. Точність арифметики з плаваючою крапкою

Останнім невизначеним параметром, який необхідно вибрати для забезпечення рівнів стійкості 384 та 512 біт, є необхідна точність виконання операцій у арифметиці з плаваючою крапкою. Розробники Falcon для теоретичної оцінки використовували роботу [1], проте точність обиралася з практичних експериментів. З [1] видно, що рівень безпеки λ слабо впливає на потрібну точність. Основний вплив має кількість запитів на підпис $qs = 2^{64}$, тому є надія, що 53 бітів буде достатньо. Проте, це питання є предметом подальшого дослідження.

Також до недоліку ЕП Falcon необхідно віднести використання арифметики з плаваючою крапкою. Разом з використанням деревоподібних структур це ускладнює аналіз схеми до атак сторонніми каналами. Іншою проблемою є складність реалізації на малоресурсних пристроях.

3.6. Генерація параметрів для 256, 384, 512 біт стійкості ЕП Falcon

У цілому, якщо підсумувати наведене вище, знайти параметри n, q, β можна з системи нерівностей (10) [7]:

$$\begin{cases} \left(\frac{B}{2\pi e}\right)^{\frac{2n-1}{2B-2}} \sqrt{q} < \beta \\ \left(\frac{B}{2\pi e}\right)^{\frac{2B-2n+1}{2B-2}} < \sqrt{\frac{3eB}{8n}} \end{cases}, \tag{10}$$

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

На основі (10) розроблено програмне забезпечення, з використанням якого були обчислені параметри n, q та β_2 для ЕП Falcon для відповідних поліномів для 256, 384, 512 біт безпеки, що наведені в табл. 4.

Отриману криптостійкість наведено в табл. 5. Криптостійкість наведено у форматі «стійкість» λ / розмір блоку.

Оцінки криптостійкості отримувалися з розміру блоку як $0{,}265B$ та $0{,}292B$. Такий підхід вважається класичним і використовувався як авторами Dilithium, так і авторами Falcon [1, 2]. Проте, оцінки є досить грубими. В табл. 5 для деяких квантових атак для 256 і 512 sn отримані значення є трохи меншими за необхідні, проте через грубість оцінки можна вважати, що вони досягають потрібного порога. Для 256 біт згенеровані параметри співпадають із параметрами, що згенеровані авторами Falcon.

Таблиця 4

Основні загальносистемні параметри Falcon *N* для 256, 384, 512 біт безпеки

Безпека	$\phi(x)$	n	q	β_2
256	x^n+1	1024	12289	87070769
384	$x^n - x^{n/2} - 1$	1536	18433	174141539
512	x^n+1	2048	12289	200928983

Обґрунтування та сутність оптимізації за параметром β наведено в [6].

У табл. 6 наведено значення для параметрів τ, n, які можливо використовувати на практиці та відповідні значення β, причому параметр q має значення 12289.

Таблиця 5

Криптостійкість Falcon *N* до атак на основі редукції решіток

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

Таблиця 6

Альтернативні значення параметра β

n	τ	Ймовірність повтору	$\lfloor \beta \rfloor$
1024	1.1	10^{-9}	8382
	1.08	10^{-6}	8230
	1.07	0.0007	8153
	1.05	0.064	8001
2048	1.07	10^{-9}	11710
	1.055	10^{-6}	11545
	1.045	0.0002	11436
	1.03	0.025	11272

Оптимізовані альтернативні набори загальносистемних параметрів для 256 біт класичної стійкості зведені у табл. 7.

Таблиця 7

Оптимізовані альтернативні набори загальносистемних параметрів для 256 біт класичної стійкості

n	q	$\lfloor \beta^2 \rfloor$	Підробка ЕП клас. (біт)	Підробка ЕП квант. (біт)	Відновлення ключа клас. (біт)	Відновлення ключа квант. (біт)
1024	12289	70265242 (τ=1.1)	277	252	273	248
1024	12289	67733370 (τ=1.08)	279	253	273	248
1024	12289	66484856 (τ=1.07)	280	254	273	248
1024	12289	64022669 (τ=1.05)	282	255	273	248

Оптимізовані альтернативні набори загальносистемних параметрів для 512 біт класичної стійкості зведені у табл. 8.

Таблиця 8

Оптимізовані альтернативні набори загальносистемних параметрів для 512 біт класичної стійкості

n	q	$\lfloor \beta^2 \rfloor$	Підробка ЕП клас. (біт)	Підробка ЕП квант. (біт)	Відновлення ключа клас. (біт)	Відновлення ключа квант. (біт)
2048	12289	137125015 (τ=1.07)	618	561	554	503
2048	12289	133307337 (τ=1.055)	621	563	554	503
2048	12289	130792161 (τ=1.045)	622	565	554	503
2048	12289	127064310 (τ=1.03)	625	567	554	503

4. Метод та алгоритми побудови загальних параметрів ЕП типу Dilithium у залежності від їх розмірів

В цьому підрозділі наводяться окремі результати теоретичних та практичних досліджень щодо створення постквантового ЕП Dilithium на алгебраїчній решітці [2, 21, 22]:

- обґрунтування перспективного постквантового національного стандарту ЕП Dilithium на основі алгебраїчних решіток з відхиленням;
- методи обчислення системних параметрів для ЕП Dilithium 128, 256, 384 та 512 біт рівнів безпеки;
- генерація системних параметрів ЕП Dilithium та «Вершина 1» для 128, 256, 384, та 512 біт стійкості.

4.1. Обґрунтування перспективного постквантового національного стандарту електронного підпису на основі алгебраїчних решіток з відхиленням

Одним із видів криптографічних перетворень типу ЕП, що може бути включений в національний стандарт ЕП постквантового періоду, на наш погляд, може стати ЕП на алгебраїчних решітках типу Dilithium [1, 21].

4.2. Аналіз стійкості алгоритму Dilithium проти основних атак

Наразі в постквантовій криптології актуальними є завдання забезпечення криптографічної стійкості щодо квантових атак. Вона ґрунтується не вирішенні проблеми навчання з помилками.

На основі аналізу визначено [9 – 17, 24], що стосовно LWE можливо застосування таких атак:

1. BKW, коли LWE зводиться до SIS атаки.
2. Primal attack (Search-LWE зводиться до BDD атаки).
3. Dual attack (Decision-LWE зводиться до SIS).
4. Зведення до uSVP атаки пошуку короткого вектора.

Деталі щодо кожної з атак, а також їх теоретичне обґрунтування наведено у [2, 7].

4.3. 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 типу Dilithium та рішення для України «Вершина 1»[7].

Дослідження стосовно алгоритму ЕП Dilithium проведено за такими параметрами [5 – 7]:

- BKZ bock-size to break SIS=475;
- BKZ bock-size to break LWE=485;
- k=5; l=4; η=5; ς=4; β=275; ω=96.

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

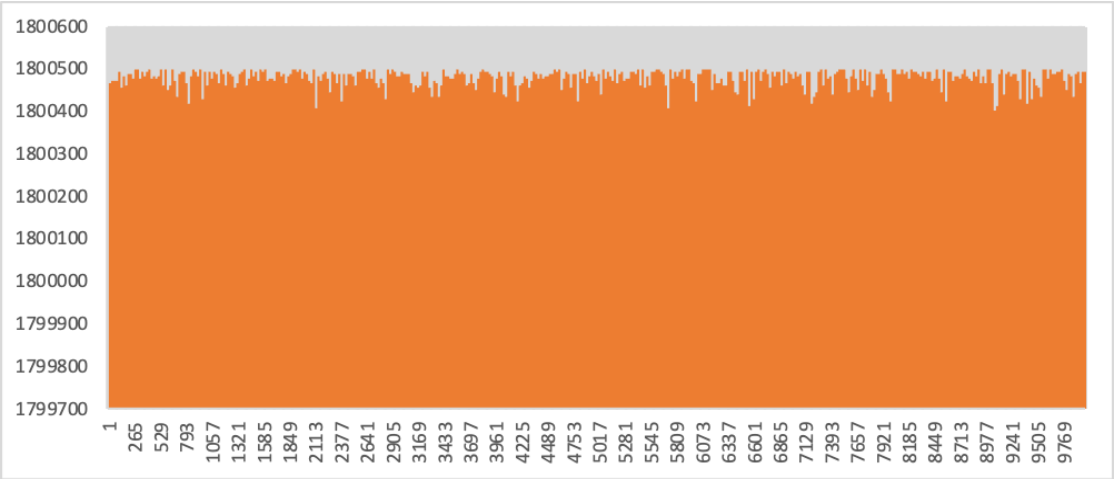

Рис. 1. Залежність часу підпису (у тактах процесору) від номеру ключа

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

4.4. Вибір параметрів 5-7 рівнів стійкості

Попередній аналіз показав, що значення параметрів, наведені в [7], не забезпечують при застосуванні в механізмі Dilithium стійкість ЕП від класичних атак на рівні 256 бітів. Фактично нижні оцінки стійкості наведено в рядках табл. 9 [21] 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

$$\text{Best Known Classical bit-cost (класична атака)} = 0{,}292b, \quad (11)$$

$$\text{Best Known Quantum bit-cost (квантова атака)} = 0{,}265b, \quad (12)$$

де b є довжиною блоку (BKZ bock-size b to break SIS або LWE [7]). В ролі кінцевої оцінки стійкості використовується найменше з двох значень, обчислених для b, що є довжиною блоку для задачі SIS та задачі LWE відповідно.

Загальні обмеження [5 – 7], які необхідно врахувати при виборі параметрів для забезпечення стійкості на рівні $\lambda \in \{256, 384, 512\}$ бітів.

1. Геш-функція CRH, що використовується у ЕП, повинна бути стійкою до колізій [2]. Отже, довжина її вектору значень повинна бути, як мінімум, 2λ бітів. (Зокрема, при λ=256 функція CRH повинна приймати значення довжини 512, а ні 384, як в оригінальному методі [7]).

2. Криптографічна функція H, яка використовується, повинна бути стійкою відносно знаходження другого прообразу і, отже, приймати, принаймні, 2λ 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 λ=256 в [2, 7] рекомендується використовувати параметри n=256, h=60, і умова

$$2^h \binom{n}{h} \geq 2^\lambda \tag{13}$$

виконується.

При $\lambda \in \{384, 512\}$ та n=256 забезпечити виконання умови 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, 7]:

$$q=2^{23}-2^{13}+1,$$
$$\gamma_1=(q-1)/16,\ \gamma_2=\gamma_1/2. \tag{14}$$

3. Довжини векторів ρ та K, що використовуються, повинні бути не менше, ніж λ.

Таким чином, для забезпечення стійкості схеми ЕП на рівні $\lambda \in \{256, 384, 512\}$ необхідно:

1) використовувати геш-функцію CRH, значеннями якої є двійкові вектори довжини 2λ [7];

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

3) покласти n=256, якщо λ=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 (14);

5) обчислити вагу c як найменше натуральне h.

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

4.5. Генерація загальносистемних параметрів ЕП Dilithium для 128, 256, 384, 512 біт стійкості

Для генерації системних параметрів удосконаленого ЕП Dilithium використаємо результати аналізу відомих атак на криптосистему, що наведені вище, та встановимо умови, за яких забезпечується захист від них. Основними атаками є [7]:

- відновлення особистого ключа на основі відкритого ключа;
- засобом підробки ЕП.

Враховуючи наведені критерії, алгоритм генерації загальносистемних параметрів виглядає наступним чином [2, 7, 21]:

1. Визначити потрібний рівень безпеки $\lambda \in \{256, 384, 512\}$.
2. Обрати значення N. Якщо λ=256, то N=256, інакше N=512.
3. Обрати значення q: q=8389417.
4. Обчислити γ_1 та γ_2 за формулами $\gamma_1 = (q-1)/16$, $\gamma_2 = \gamma_1/2$.
5. Обчислити значення η. За замовченням встановити η=2. На наступних кроках значення буде уточнене.
6. Встановити значення (k, l)=(2, 1).
7. Обчислити λ_1-стійкість до Primal Attack. Якщо стійкість менша за λ, то оновити параметри (k, l)=(k+1, l+1) та повернутися до кроку 7 або збільшити η та повернутися до кроку 7.
8. Обчислити λ_2-стійкість до Dual Attack. Якщо стійкість менша за λ, то оновити параметри (k, l)=(k+1, l+1) та повернутися до кроку 7 або збільшити η та повернутися до кроку 7.
9. Обчислити λ_3-стійкість до SIS з ζ_1. Якщо стійкість менша за λ, то оновити параметри (k, l)=(k+1, l+1) та повернутися до кроку 7 або збільшити k=k+1 та повернутися до кроку 7.
10. Обчислити λ_4-стійкість до SIS з ζ_2. Якщо стійкість менша за λ, то оновити параметри (k, l)=(k+1, l+1) та повернутися до кроку 7 або збільшити k=k+1 та повернутися до кроку 7.
11. Обчислити h як найбільше ціле, для якого виконується нерівність $2^h \binom{n}{h} \geq 2^\lambda$.
12. Обчислити d як найбільше ціле, для якого виконується нерівність $2^{d-1}h+1 \leq 2\gamma_2$.

13. Встановити $\beta=\eta h$ та зменшувати β, щоб ймовірність повтору циклу була достатньо малою.

14. Обчислити w=0,08nk (цей крок не впливає на криптостійкість та його можливо оптимізувати).

У табл. 9 наведено значення параметрів для удосконаленого ЕП Dilithium.

Таблиця 9

Значення параметрів для 256, 384, 512 біт стійкості

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

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

Результати оцінки криптостійкості для удосконаленого ЕП Dilithium (в бітах) з використанням параметрів з табл. 9 наведено в табл. 10.

Таблиця 10

Оцінки криптостійкості для удосконаленого ЕП Dilithium

Набір	Primal атака (клас.)	Primal атака (квант.)	Dual атака (клас.)	Dual атака (квант.)	SIS (класич.)	SIS (квант.)
256	298	270	296	269	293	266
384	440	399	438	397	503	456
512	582	*527*	579	525	590	535

5. Особливості застосування методики оцінки та результати порівняння постквантових алгоритмів ЕП на алгебраїчних решітках

В даному підрозділі наводяться пропозиції щодо застосування методики з оцінки та порівняння перспективних криптографічних перетворень типу ЕП, в першу чергу щодо криптографічної стійкості.

В табл. 11 наведені характеристики обраних для порівняння алгоритмів (значення швидкості криптоперетворень та генерації ключів наведено в тактах). В порівнянні приймали участь проєкти стандартів «Вершина 1» та «Вершина 2», а також алгоритм Dilithium, який за попередніми дослідженнями мав кращі результати серед постквантових алгоритмів підпису, що засновані на перетвореннях на алгебраїчних решітках. Стійкість алгоритмів «Вершина» 128 біт відповідає 3-му рівню стійкості NIST, 256 – 5-му, тому пропорційно для виконання порівняння згідно шкали оцінок попарного порівняння параметрам 384 був наданий 7-й рівень, а 512 – 9-й.

Таблиця 11

Характеристики алгоритмів ЕП, що засновані на перетвореннях на алгебраїчних решітках

Алгоритми	$I_{ст.}$	$l_{в.к.}$	$l_{о.к.}$	$l_{рез.}$	$T_{пр.}$	$T_{зв.}$	$T_{гк.}$
Dilithium_round3_sec2	2	1 312	3 504	2 420	259 172	118 412	124 031
Dilithium_round3_sec3	3	1 952	3 856	3 293	428 587	179 424	256 403
Dilithium_round3_sec5	5	2 592	5 792	4595	538 986	279 936	298 050
Вершина_1_128	3	1 472	3 488	2 693	133 340	109 818	90 328
Вершина_1_256	5	2 624	5 792	5 345	259 103	233 712	229 669
Вершина_1_384	7	4 528	9 088	6762	411 040	398 029	317 324
Вершина_1_512	9	5 824	11 008	10708	643 744	620 989	485 471
Вершина_2_128	3	897	4097	666	655 672	139 620	33 696 000
Вершина_2_256	5	1 793	8193	1 280	1 338 825	285 714	107 055 000
Вершина_2_512	9	3 585	5121	2 515	2 600 053	265 416	28493603229

В табл. 12 наведені результати досліджень – відносна перевага алгоритмів ЕП, що отримана методом попарних порівнянь за кожною з характеристик.

Таблиця 12

Відносна перевага алгоритмів ЕП за кожною з характеристик

Алгоритми	$I_{ст.}$	$l_{в.к.}$	$l_{о.к.}$	$l_{рез.}$	$T_{пр.}$	$T_{зв.}$	$T_{гк.}$
Dilithium_round3_sec2	0,0198	0,1770	0,1816	0,1131	0,1583	0,1857	0,2090
Dilithium_round3_sec3	0,0299	0,0965	0,1475	0,0606	0,0849	0,0984	0,1082
Dilithium_round3_sec5	0,0697	0,0655	0,0768	0,0507	0,0666	0,0506	0,0915
Вершина_1_128	0,0299	0,1395	0,1816	0,0800	0,3006	0,2195	0,2696
Вершина_1_256	0,0697	0,0655	0,0768	0,0339	0,1583	0,0716	0,1388
Вершина_1_384	0,1453	0,0327	0,0407	0,0261	0,0975	0,0348	0,0797
Вершина_1_512	0,2681	0,0233	0,0296	0,0173	0,0479	0,0218	0,0608
Вершина_2_128	0,0299	0,2487	0,1212	0,3211	0,0479	0,1466	0,0192
Вершина_2_256	0,0697	0,1108	0,0467	0,1989	0,0238	0,1130	0,0146
Вершина_2_512	0,2681	0,0406	0,0973	0,0984	0,0143	0,0581	0,0086

На рис. 2 відображено гістограму загальної відносної переваги алгоритмів ЕП з урахуванням вагових коефіцієнтів характеристик.

Як видно, найбільшу перевагу має алгоритм «Вершина 1» з параметрами стійкості 128 біт, для більш стійких параметрів перевага вже у алгоритму «Вершина 2». «Вершина 2» на даному етапі програє через свою низьку швидкодію, якщо її реалізація буде більш оптимізована, то вже «Вершина 2» буде на першому місці.

Таким чином, зроблено порівняння алгоритмів, що пройшли до третього етапу NIST, а також алгоритмів проєктів стандарту «Вершина 1» та «Вершина 2». При порівнянні використовувалися два методи порівняння для отримання більш точної оцінки в залежності від вимог до алгоритмів ЕП.

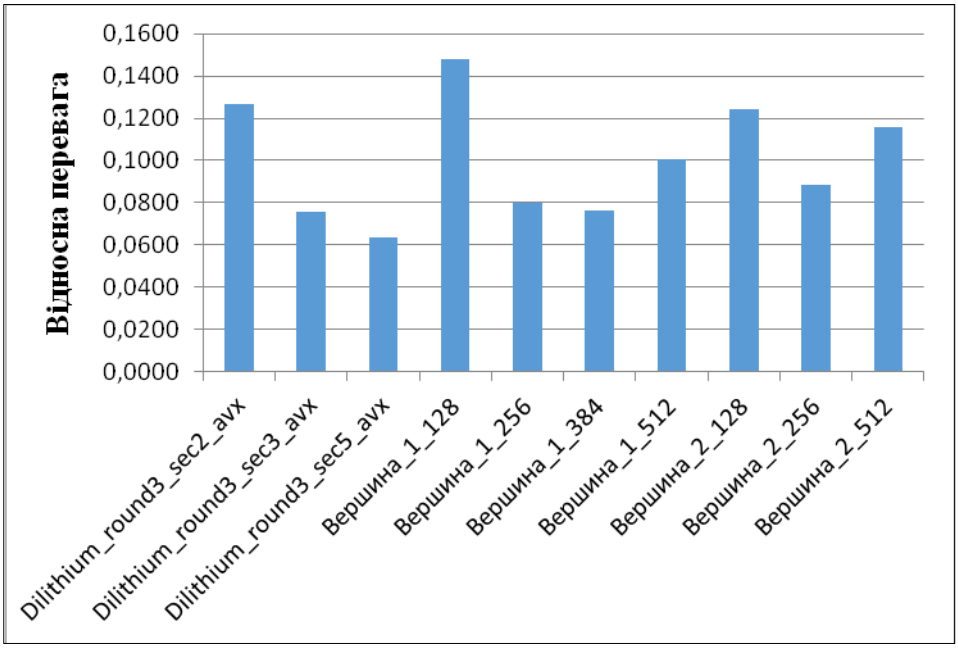

Рис. 2. Переваги алгоритмів ЕП

Висновки

1. Математичні методи Falcon та Dilithium є теоретичними основами для створення постквантових проєктів стандартів ЕП Falcon та Dilithium. Ці ЕП є фіналістами міжнародного конкурсу NIST США. Наразі вони досліджуються на третьому раунді і при позитивних результатах дослідження можуть бути прийняті в якості міжнародних постквантових стандартів ЕП. При їх побудування використано математичний апарат алгебраїчних решіток та відповідні методи.

2. Як з теоретичних, так і практичних позицій, основоположним щодо цих ЕП є обґрунтування вимог до параметрів та ключів та їх побудування за умови достатності забезпечення гарантованості їх захищеності від класичних, квантових, спеціальних та атак на основі помилок

3. При виборі розмірів загальних параметрів та ключів виникає суттєве протиріччя між властивостями проєктів стандартів ЕП Falcon та Dilithium щодо стійкості та складності перетворень. Збільшення розмірів загальних параметрів та ключів приводить до збільшення складності перетворень, і навпаки.

4. Що стосується теоретичних методів побудування загальних параметрів та ключів для ЕП Falcon та Dilithium, то вони у цілому зрозумілі, а якщо використовувати [1, 2, 6, 7], то існує можливість їх побудувати і для більш високих, але обґрунтованих рівнів безпеки – 6-го та 7-го, коли може бути забезпечено 384 і 512 біт захисту від класичних атак та 192 і 256 біт захисту від квантових атак, а також захищеність від спеціальних атак та атак на основі помилок.

5. Результати розрахунків розмірів відкритих ключів (PK_SIZE), електронних підписів (DS_SIZE) та складностей (часових) перевірки підписів (CHECK_TIME) для алгоритмів ЕП Falcon та Dilithium для 5-го рівня безпеки наведені в табл. 1, які свідчать про те, що ЕП Dilithium для 5-го рівня безпеки програє ЕП Falcon.

6. На основі математичних методів Falcon та Dilithium розроблено проєкти стандартів ЕП «Вершина 1» та «Вершина 2» 7-го рівня криптостійкості 512 біт захисту від класичних атак та 256 біт захисту від квантових атак. В табл. 2 наведені основні показники для цих алгоритмів в разі збільшення степені n та застосування решти необхідних параметрів.

7. Генерація ключів та формування електронного підпису для алгоритму Falcon та його прототипів потребує від розробника застосування багатьох різних алгоритмів та форматів, що може привести к значному звуженню практичного застосування алгоритму ЕП Falcon.

8. У [1] не зберігають результатів перетворень, а для кожного поточного значення r для виконання зворотного перетворення обчислюють їх повторно, тому рекомендується їх зберігати, що збільшить навантаження на пам’ять, але зменшить час обчислення. Для тимчасового зберігання даних в функціях рекомендується застосовувати локальну пам'ять.

9. Попередній аналіз дозволяє зробити висновки, що Falcon все таки має перспективи щодо прийняття в якості міжнародного стандарту ЕП. Домінуючим основним концептуальним підходом до проєктування механізму ЕП Falcon є використання перетворення типу «геш-і-підпис». Перевагою такого підходу є доведена стійкість в межах моделі квантового випадкового оракула.

10. Безпосередньо ЕП Falcon та його аналізу присвячено значно менше робіт, ніж щодо інших, наприклад проєкту ЕП Dilithium. Крім того, як і щодо інших, при проєктуванні ЕП Falcon були прийняті обмеження щодо максимальних рівнів безпеки у вигляді максимально 256 біт проти класичного та 128 біт проти квантового криптоаналізу.

11. Попередній аналіз показав, що основними атаками щодо ЕП Falcon є атаки на відновлення особистого ключа з відкритого ключа ЕП та атаки на підробку ЕП.

12. Атаки на відновлення особистого ключа з відкритого ключа щодо Falcon можуть зводиться до вирішення проблеми NTRU. У ряді криптосистем, стійкість яких ґрунтуються на проблемі NTRU, коли поліноми f та g мають коефіцієнти з множини значень {0, 1, –1}, виникає проблема забезпечення стійкості проти комбінованих атак.

13. Атаки безпосередньої підробки ЕП Falcon можуть бути найбільш загрозливими. Тому іншим впливом є атака підробки ЕП. При реалізації такої атаки потрібно знайти достатньо короткий вектор s. Відповідно, це можливо зробити, редукувавши базис так, щоб виконувалася необхідні умови.

14. До недоліку ЕП Falcon необхідно віднести використання арифметики з плаваючою крапкою. Разом з використанням деревоподібних структур це ускладнює аналіз методу до

атак сторонніми каналами. Іншою проблемою є складність реалізації перетворень на малоресурсних пристроях.

15. Одним із видів криптографічних перетворень типу ЕП, що може бути включений в національний стандарт ЕП постквантового періоду, на наш погляд, може стати ЕП на алгебраїчних решітках типу Dilithium.

16. Наведені у табл. 11 та 12 результати порівняння проєктів стандартів ЕП «Вершина 1» та «Вершина 2», а також алгоритму Dilithium, показали, що кращі результати серед постквантових алгоритмів ЕП, що засновані на перетвореннях на алгебраїчних решітках, мають проєкти ЕП «Вершина 1» та «Вершина 2».

17. Кращі показники у алгоритмів «Вершина 1» та «Вершина 2» («Вершина 2» на даному етапі програє через свою низьку швидкодію, якщо її реалізація буде більш оптимізована, то вже «Вершина 2» буде на першому місці).

Список літератури:

1. Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU. Round 3 Submissions. [Електронний ресурс]. Режим доступу: https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions.
2. Léo Ducas Crystals-Dilithium: Algorithm Specifications and Supporting Documentation. Round 3 Submissions. [Електронний ресурс]. Режим доступу: https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions.
3. Gorjan Alagic NISTIR 8309 Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process / Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone. Режим доступу: https://doi.org/10.6028/NIST.IR.8309.
4. Chen L Report on Post-Quantum Cryptography / Chen L, Jordan S, Liu Y-K, Moody D, Peralta R, Perlner RA, Smith-Tone D // (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8105 (2016). Режим доступу: https://doi.org/10.6028/NIST.IR.8105.
5. Горбенко І. Д. Методи, методика та результати порівняльного аналізу кандидатів на постквантовий стандарт електронного підпису / І. Д. Горбенко, О. Г. Качко, М. В. Єсіна, В. А. Пономар // XX Ювілейна Міжнар. наук.-практ. конференція "Безпека інформації в інформаційно-телекомунікаційних системах", 22-24 травня, 2018, м. Буча. С. 96-97.
6. Горбенко І. Д. Генерація загальносистемних параметрів для криптосистеми Falcon для 256, 384, 512 біт безпеки / І. Д. Горбенко, С.О. Кандій, М.В. Єсіна, Є.В. Острянська // Радіотехніка. 2020. Вип. 202. С. 57-63.
7. Горбенко І. Д. Методи обчислення системних параметрів для електронного підпису «Crystals-Dilithium» 128, 256, 384 та 512 біт рівнів безпеки / І. Д. Горбенко, А. М. Олексійчук, О. Г. Качко, Ю. І. Горбенко, М. В. Єсіна, С. О. Кандій // Радіотехніка. 2020. Вип. 202. С. 5-28.
8. Yesina Maryna Comparative Analysis of Key Encapsulation Mechanisms / Maryna Yesina, Mikolaj Karpinski, Volodymyr Ponomar, Yurij Gorbenko, Tomasz Gancarczyk, Uliana Iatsykovska // Proceedings of the 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). September 18-21, 2019, Metz, France. Volume 1. – P. 7-12.
9. Горбенко Ю. І. Моделі загроз щодо асиметричних криптоперетворень перспективного електронного підпису / Ю.І. Горбенко, М.В. Єсіна, В.В. Онопрієнко, Г.А. Малєєва // Радіотехніка. 2020. Вип. 202. С. 72-78.
10. Горбенко Ю. І. Аналіз стійкості постквантового електронного підпису Dilithium до атак на помилки / Ю.І. Горбенко,О.С. Дроздова // Радіотехника. 2020. Вип. 202. С. 49 – 56.
11. Daniel J. Bernstein, Tanja Lange, Christiane Peters Attacking and defending the McEliece cryptosystem. [Електронний ресурс]. Режим доступу: https://link.springer.com/chapter/10.1007/978-3-540-88403-3_3.
12. Martin Albrecht, Shi Bai, Leo Ducas A Subfield Lattice Attack on Overstretched NTRU Assumptions. In Matthew Robshaw and Jonathan Katz, editors, Advances inCryptology – CRYPTO 2016, pages 153–178, Berlin, Heidelberg, 2016. Springer BerlinHeidelberg.
13. Paul Kirchner, Pierre-Alain Fouque Revisiting Lattice Attacks on Overstretched NTRU Parameters. In Jean-Sebastien Coron and Jesper Buus Nielsen, editors, Advancesin Cryptology – EUROCRYPT 2017, pages 3-26, Cham, 2017. Springer InternationalPublishing.
14. Vadim Lyubashevsky, Daniel Wichs Simple lattice trapdoor sampling from a broad class of distributions. In Jonathan Katz, editor, PKC 2015, volume 9020 of LNCS, pages 716 – 730, Gaithersburg, MD, USA, March 30 – April 1, 2015. Springer, Heidelberg, Germany.
15. Martin R. Albrecht On the complexity of the BKW algorithm on LWE / Martin R. Albrecht, Carlos Cid, Jean-Charles Faugère, Robert Fitzpatrick, Ludovic Perret //. Designs, Codes and Cryptography, 74: 325-354, 2015.
16. Ronald Cramer, Léo Ducas, Benjamin Wesolowski Short stickelberger class relations and application to ideal-SVP. In Coron and Nielsen, pages 324-348.
17. Avrim Blum, Adam Kalai, Hal Wasserman Noise-tolerant learning, the parity problem, and the statistical query model. Journal of the ACM, 50(4): 506-519, July 2003.
18. Квантовый компьютер. [Електронний ресурс]. Режим доступу: http://www.tadviser.ru/index.php/.
19. Каптьол Є. Ю. Аналіз можливостей та особливості програмування задач криптології на квантовому комп'ютері /Є. Ю. Каптьол, І.Д. Горбенко // Радіотехніка. 2020. Вип. 202. С. 37-48.

20. Горбенко Ю. І. Аналіз можливостей квантових комп'ютерів та квантових обчислень для криптоаналізу сучасних криптосистем / Ю. І. Горбенко, Р. С. Ганзя // Східно-європейський журнал передових технологій. 2014. № 1/9 (67). С. 8-15.

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

22. Олексійчук А. М. 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. 2020. Вип. 200. С. 5-14.

23. Качко О. Г. Оптимізація алгоритму множення поліномів для NTRU – побітних алгоритмів / О. Г. Качко, Ю. І Горбенко, В. А. Пономар, М. В. Єсіна, С. О. Кандій // Радіотехніка. 2020. Вип. 200. С. 15-24.

24. Nick Howgrave-Graham A hybrid lattice-reduction and meet-in-the-middle attack against NTRU. In Alfred Menezes, editor, CRYPTO 2007, volume 4622 of LNCS, pages 150–169, Santa Barbara, CA, USA, August 19-23, 2007. Springer, Heidelberg, Germany.

Надійшла до редколегії 05.04.2021

Відомості про авторів:

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

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

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

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

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

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

Стельник Ігор Валерійович – Адміністрація Державної служби спеціального зв'язку та захисту інформації України, заступник директора Департаменту.

Пономар Володимир Андрійович – канд. техн. наук, Харківський національний університет імені В.Н. Каразіна, науковий співробітник кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; Україна; e-mail: Laedaa@gmail.com; ORCID: https://orcid.org/0000-0001-5271-2251