УДК 004.056.55 **DOI:10.30837/rt.2020.3.202.06**

В.А. КУЛІБАБА

ПРОЦЕСИ ТА МЕТОДИ ВИБОРУ ЗАГАЛЬНОСИСТЕМНИХ ПАРАМЕТРІВ ПЕРСПЕКТИВНОГО АЛГОРИТМУ ЕЛЕКТРОННОГО ПІДПИСУ НА ОСНОВІ АЛГЕБРАЇЧНИХ РЕШІТОК

Вступ

У липні 2020 р. NIST США оголосив фіналістів другого раунду конкурсу постквантових криптографічних примітивів [1], а також оголосив про старт третього раунду. Серед 26 кандидатів другого раунду для проходження у третій раунд у якості основних кандидатів на стандартизацію будо обрано сім механізмів, чотири – асиметричного шифрування та інкапсуляції ключів, а також три електронних підписи.

Аналіз показав, що складність проблеми навчання з помилками точно знайдена лише асимптотично [2], тому важливим моментом є розгляд конкретних значень загальносистемних параметрів алгоритму ЕП Dilithium в контексті відомих атак на алгоритми, що базуються на проблемі LWE.

Серед обраних кандидатів на стандарт ЕП два із трьох алгоритмів засновані на алгебраїчних решітках, це CRYSTALS-DILITHIUM (далі Dilithium) та FALCON.

У звіті NIST зазначено, що Dilithium використовує один і той же модуль і кільце для всіх наборів параметрів і вибірок за допомогою рівномірного розподілу, що призводить до більш простої реалізації, ніж у його основного конкурента, FALCON. Проте, зважаючи, що обидва алгоритми базуються на решітках, скоріше за все, за заявою NIST, стандартизовано буде лише один із них.

У [3, 4, 14] наведено сутність та результати досліджень щодо властивостей та умов застосування кандидата на постквантовий стандарт ЕП Dilithium, що були сформовані та подані на конкурс постквантових криптографічних стандартів NIST. На першому етапі конкурсу [5] були виявлені певні проблемні питання, а на другому етапі уточнені вимоги щодо деяких властивостей алгоритмів, зокрема стійкості до атак сторонніми каналами, щодо яких авторами проєкту стандарту були обґрунтовані та запропоновані удосконалення алгоритму ЕП Dilithium та оптимізована реалізація AVX2.

В звіті [1] NIST явно рекомендував команді Dilithium додати набір параметрів категорії 5, тобто рівня стійкості 512 бітів класичної безпеки та 256 бітів квантової безпеки.

Метою даної статті є:

- попередній аналіз криптографічної стійкості алгоритму ЕП Dilithium від класичних та квантових атак типу «груба сила» та атак на решітках у перехідний та постквантовий періоди;
- обґрунтування та розробка пропозицій щодо генерування та застосування загальносистемних параметрів алгоритму ЕП Dilithium рівня стійкості 512 бітів класичної безпеки та 256 бітів квантової безпеки;
- експериментальний аналіз захищеності ЕП Dilithium від атак сторонніми каналами, зокрема від атаки на основі різної складності множення поліномів.

1. Основні атаки на алгоритми ЕП, що базуються на алгебраїчних решітках

На основі аналізу визначено [6 – 10], що стосовно атак на LWE можна виділити наступні:

1. Атака грубої сили, тобто повного перебору.
2. Атака зустріч посередині.
3. Атака на основі алгоритму Arora-Ge.
4. Атака типу BKW, коли LWE зводиться до SIS атаки.
5. Атака зведення Search-LWE до BDD.

6. Дуальна атака (Decision-LWE зводиться до SIS).

7. Primal attack. Зведення до uSVP атаки пошуку короткого вектору.

8. Диференційна атака.

У роботі [8] доведено, що для вирішення задачі Search-LWE з параметрами n, q, α та з ймовірністю ε потрібно

$$\Theta(2^{n*\log(2*t*\alpha*q+1)+\log(n)+1+\log(m)})$$

операцій у Z_q, де

$$m = \frac{\log(1-\varepsilon) - n\log(2t\alpha q+1)}{\log(2t\alpha)}, t = \omega(\sqrt{\log(n)}) \tag{1}$$

Для вдалої атаки потрібно не менше, ніж $n+m$ пар $(a,c) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$.

Атаки типу зустріч посередині були реально застосовані та позитивно себе показали при криптоаналізі NTRU-подібних систем. В роботі [5] запропоновано ідею застосування цього підходу стосовно криптосистем на основі LWE та доведено, що атака для деякого параметра $t = \omega(\sqrt{\log(n)})$ буде з ненульовою ймовірністю вирішувати задачу Search-LWE за час

$$\Theta((2t\alpha q+1)^{n/2} * (m*n + \log(n/2) + \\ + \log(\log(t\alpha q)) + n/2 * \log(2t\alpha q+1))) \tag{2}$$

Алгоритм Arora-Ge [7] фактично є оптимізацією алгоритму повного перебору та вирішує Search-LWE. Головна ідея алгоритму полягає у побудові системи нелінійних рівнянь, рішенням якої є секретний поліном s. Система вирішується шляхом лінеаризації рівнянь. Було доведено, що, якщо $D_{GA} \in o(n)$ де $D_{GA} = 8(\alpha q)^2 \log(n) + 1$, то рішення системи буде знайдено зі складністю

$$\Theta(2^{w*D_{GA}\log(n/D_{GA})*(\alpha q)*q*\log(q)}). \tag{3}$$

Визначено також, що якщо $\alpha q \approx \sqrt{n}$, то атака буде успішною з ймовірністю

$$\varepsilon = \frac{3}{\log(\log(n))}.$$

У роботі [8] запропоновано вдосконалення алгоритму Arora-Ge, яке потребує $\Theta(2^{2.35wn+1.13n)})$ часу та пам'яті.

Атака на основі алгоритму BKW [9, 10].

Ідея алгоритму BKW полягає у зведенні задачі LWE до задачі SIS у підрешітках меншої розмірності. В алгоритмі розділення на підрешітки здійснюється шляхом розбиття матриці

$$A = \begin{pmatrix} a_1 \\ (\dots) \\ a_m \end{pmatrix} \in \mathbf{Z}_q^{n \times m}$$

на b матриць виду $a_1^{'}, \dots, a_b^{'}$, кожна з яких належить простору $\mathbf{Z}_q^{\eta \times m}$. Далі кожна з матриць $a_1^{'}, \dots, a_b^{'}$ використовується для вирішення SIS у відповідному підпросторі. Основною перевагою такого алгоритму є можливість суттєво розпаралелити обчислення. Для вирішення задачі Decision-LWE алгоритм потребує часу, що можна оцінити таким виразом

$$\Theta((\frac{q^b-1}{2}) * (\frac{\eta(\eta-1)}{2} * (n+1) - \frac{b\eta(\eta-1)}{4}) - \\ - \frac{b}{6}(\frac{q^b-1}{2})((\eta-1)^3 + \frac{3}{2}(\eta-1)^2 + \frac{1}{2}(\eta-1))) \tag{4}$$

Атака зі застосуванням зведення LWE до BDD. Припускається, що дано m пар.

$$(a_i, c_i) = (a_i, \langle a_i, s_i \rangle + e_i) \in \mathbf{Z}_q^n \times \mathbf{Z}_q.$$

Або у іншому вигляді:

$$(A, c) = (A, A^* s + e) \in \mathbf{Z}_q^{m \times n} \times \mathbf{Z}_q^{m \times 1}.$$

Можливо побудувати решітку

$$L = \{Ax \bmod q : x \in \mathbf{Z}_q^m\}.$$

Очевидно, що s є вектором на решітці та є найближчим до вектору $As + e$. Задача знаходження найближчого вектору на решітці до деякого довільного вектору має назву BDD та вирішується за допомогою алгоритму Бабаї [5 – 7]. Алгоритм працює за поліноміальний час, проте знаходить рішення з деякою ймовірністю. Для LWE цю ймовірність можливо оцінити як

$$\prod_{i=0}^{m-1} erf\left(\frac{\|b_i^*\|\sqrt{\pi}}{2\alpha q}\right),$$

де $\|b_i^*\|$ – норми ортогоналізованих за Граммом – Шмідтом векторів базису решітки (тобто стовбців матриці A). Для того щоб ймовірність вирішення BDD була близька до одиниці, потрібно зменшити $\|b_i^*\|$, тобто редукувати базис. Фактор Ерміта δ_0 для редукції отримаємо з співвідношення

$$\|b_0\|_2 = \delta_0^n q^{\frac{1}{n}}$$

$$\|b_i^*\|_2 \approx \delta_0^{-2i+n} * q^{\frac{1}{n}}$$

Алгоритм BKZ 2.0 залежить від натуральних параметрів β і m, що позначають довжину блоку та кількість ітерацій відповідно, і дозволяє будувати редукований за Коркіним – Золотарьовим [8] базис повної решітки вимірності n за $2^{E(\beta, m, n)}$ операцій, де

$$E(\beta, m, n) = 0,000784314\,\beta^2 + \\ +0,366078\,\beta + \log((n)m) + 0,875. \qquad (5)$$

Атаки на дуальній решітці засобом зведення LWE до SIS. Будується спочатку решітка $L = \{x \in \mathbf{Z}_q^m \mid A^* x = 0 \bmod q\}$. Задача SIS полягає у знаходженні такого найменшого $x \in \mathbf{Z}^n$, щоб $A^* x = 0$. Припустимо, що такий вектор знайдений, тоді можна вирішити задачу Decision-LWE. Нехай дано m пар

$$(A, c) = (A, A^* s + e) \in \mathbf{Z}_q^{m \times n} \times \mathbf{Z}_q^{m \times 1}$$

Обчислюється скалярний добуток $\langle x, c \rangle$:

$$\langle x, c \rangle = x^* a^* s + x^* e = 0^* s + x^* e = x^* e = \langle x, e \rangle$$

Оскільки вектор $x \in \mathbf{Z}^n$ відомий, то з цієї рівності можна знайти значення вектору помилок e, проте простір помилок залишається досить великим. В роботі [9] доведено, що якщо вектор x має норму

$$\|x\|_2 = \frac{1}{\alpha} * \sqrt{\frac{\ln(\frac{1}{\varepsilon})}{\pi}},$$

то з ймовірністю близькою до 1 можливо вирішити задачу, при цьому знадобиться $\frac{1}{\varepsilon^2}$ запусків вирішувача SIS. Вирішувач знаходить достатньо малий вектор на решітці, тобто вирішує задачу SVP. У роботі [6] було показано, що при цьому фактор Ерміта δ_0 має бути не більше

$$\log \delta_0 = \frac{\log^2(\frac{1}{\alpha}\sqrt{\frac{\ln(\frac{1}{\varepsilon})}{\pi}})}{4*n\log q}.. \tag{6}$$

Подальша оцінка атаки потребує вибрати певний вирішувач, наприклад алгоритм BKZ, та проведення експериментальних досліджень з різними параметрами.

У Primal Attack припускають, що решітка містить вектор s. Сутність атаки полягає у тому, щоб побудувати таку решітку, на якій буде лежати вектор $(s,e,1)$ і він буде найменшим унікальним вектором, тобто, вона зводиться до задачі uSVP [4]. Такою решіткою буде

$$\Lambda = \{x \in \mathbf{Z}^{m+n+1} : (A \mid I_m \mid -c) * x = 0 \bmod q\}.$$

Для пошуку вектору можливо скористатися вирішувачем BKZ 2.0 і редукувати решітку, як наслідок b_0 буде рішенням, що необхідно знайти. Далі, для вдалої редукції оцінити фактор Ерміта можливо виразом [6]

$$\log \delta_0 = \frac{1}{4n^2 \ln^2 q}\left(W\left((-2n\ln q) * (\sqrt{n\log q}) * \frac{(\tau\alpha)^2}{2\pi}\right)\right)^2. \tag{7}$$

Атаки на LWE можливо розділити на два великі класи – атаки типу груба сила та атаки, що базуються на редукції решіток. До першого класу належать атаки зустріч посередині, повного перебору та Arora-Ge. Атаки на решітках полягають у зведенні проблеми LWE до достатньо відомих проблем (задач) на решітках: зведення LWE до BDD, зведення LWE до SIS, зведення LWE до uSVP. Кожен з цих підкласів задач зводиться до задачі пошуку достатньо малого вектору на решітці, для чого використовується алгоритм BKZ та його варіації. Проте, точні оцінки для BKZ та його варіацій невідомі, або ще не опубліковані. Це є проблемним питанням при оцінці криптографічної стійкості систем, що базуються на проблемі LWE та темою для подальших досліджень.

2. Загальносистемні параметри алгоритму ЕП Dilithium, що впливають на стійкість

Як і в більшості алгоритмів електронного підпису, алгоритм Dilithium має набір загальносистемних параметрів, частина з яких є постійною. В табл. 1 наведено постійні параметри та їх значення, що пропонуються до застосування авторами проєкту стандарту.

Таблиця 1

Постійні параметри алгоритму Dilithium, запропоновані авторами

Позначення	Сутність
N=256	Степінь поліному
q=8380417	Усі обчислення виконуються модулем q
SEEDBYTES=32	Довжина seed (байт)
d=14	Параметр, який використовується при виділенні старшої і молодшої частини
BITS_IN_BYTE=8	Кількість бітів в байті
HASHBYTES=64	Довжина початкового значення розгортання ключа

Параметри, які можуть змінюватися, задано в табл. 2 для всіх чотирьох режимів роботи, що наводяться авторами стандарту.

Таблиця 2

Параметри, що можуть змінюватись в ЦП Dilithium

Рівень стійкості	k	l	H	η	β	ω
1	3	2	7	4	375	64
2	4	3	6	4	325	80
3	5	4	5	4	275	96
4	6	5	3	3	175	120

Довжина блоку залежить тільки від значень *k, l,* η, *n, q* і розраховується окремо для кожної з двох задач (SIS та LWE) та двох атак (прямої та дуальної) на кожну з них згідно з методикою, наведеною в [2,3] Для кожної з них зазначені параметри обчислюються за формулами

$$\text{Best Known Classical bit-cost} = 0{,}292b \qquad (8)$$
$$\text{Best Known Quantum bit-cost} = 0{,}265b$$

де b є довжиною блоку (BKZ bock-size b для зламу SIS або LWE [1]). В ролі кінцевої оцінки стійкості використовується найменше з двох значень, обчислених для b, що є довжиною блоку для задачі SIS та задачі LWE відповідно.

У [8 – 13] наводиться детальний аналіз алгоритмів оцінювання довжини блоку b для задачі LWE для прямої і дуальної атаки. Як доведено, достатньою умовою стійкості на рівні λ бітів відносно прямої атаки є нерівність $0{,}292b_*^{(1)} \geq \lambda$, яка при $\lambda = 256$ рівносильно нерівності $b_*^{(1)} \geq 877$, а для дуальної атаки умовою стійкості на рівні λ бітів є нерівність

$$0{,}292b_*^{(2)} + 2c \geq \lambda. \qquad (9)$$

В загальному випадку, пряма атака потребує менше часу в порівнянні з дуальною.

Пояснення кожного параметру наведено в табл. 3.

Таблиця 3

Параметри, що можуть змінюватися та впливають на стійкість алгоритму Dilithium

Параметр	Визначення
q	Більший модуль перетворення коефіцієнтів поліномів
k	Кількість поліномів, визначають кількість рядків матриці A
l	Кількість поліномів, визначають кількість стовбців матриці A
η	Значення коефіцієнтів секретного полінома s, які знаходяться в інтервалі $[-\eta, \eta]$, основа алфавіту ключових даних
(γ_1, γ_2)	Обмеження на максимальні значення коефіцієнтів під час вироблення підпису.
h	Елемент матриці h [i][j] встановлюється в 1, якщо tmp [i][j]$_{high}$ не співпадає з (ct$_{low}$+tmp) [i][j]$_{high}$ і 0, якщо вони співпадають
ω	Цей параметр визначається як верхній поріг для числа одиниць у векторі *h*, який обчислюється на кроці 21 алгоритму формування підпису. Впливає на ймовірність повтору циклу(швидкодію алгоритму підпису) та на розмір підпису. Знаходиться з практичних міркувань.
β	Параметр β вибирається, виходячи з такої умови: ймовірність $p = \mathbf{P}\{\| cs_2 \|_\infty \geq \beta\}$ де s_2 є випадковим вектором з рівномірним розподілом на множині S_η^k, а $c \in B_h$, є достатньо малим числом. Також впливає на максимальне значення коефіцієнтів, проте впливає не стільки на стійкість, скільки на розмір підпису.
d	Цей параметр визначається як найбільше натуральне *d*, що задовольняє умові $2^{d-1}h + 1 \leq 2\gamma_2$.

3. Параметри алгоритму ЕП Dilithium для рівнів 512/256 бітів класичної та квантової стійкості

Питання генерування параметрів більш високого рівня стійкості 512 бітів, є актуальним для алгоритму ЕП Dilithium, так як авторами кандидату не будо запропоновано загальносистемних параметрів для рівнів безпеки вище, ніж 256 бітів, а лише дані загальні рекомендації щодо їх генерування. NIST США для третього раунду конкурсу рекомендував авторам надати набір параметрів 5-го рівня, що, враховуючи ряд проблемних питань в описі відповідних алгоритмів, є актуальною задачею досліджень.

Попередні оцінки стійкості наведено в підрозд. 3 та в [15] для довжини блоку *b* BKZ у вигляді нижніх оцінок. Також для параметра *n* необхідно використовувати $n = 256$, якщо $\lambda = 256$; або $n = 512$, якщо $\lambda \geq 256$

В проєкті стандарту[4] авторами наводяться параметри тільки до 4-го рівня стійкості NIST (принаймні так важко зламати, як AES256 (вичерпний перебір ключів). Проте існує задача генерування параметрів більш високого рівня стійкості 512 бітів класичної та 256 бітів квантової стійкості.

Алгоритм обчислення параметрів рівня стійкості 512/256:

1. Нехай $\lambda \in 512$, $\eta = 2$
2. Обрати значення N. Так як $\lambda \geq 256$, то $N = 512$
3. $\gamma_1 = (q-1)/16 = 523776$, $\gamma_2 = \gamma_1/2 = 261888$
4. Встановити початкові значення за замовчанням $k = 2$ та $l = 1$
5. Обчислити $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ – стійкість до Primal Attack, Dual Attack, стійкість до SIS з $\zeta_1 = \max(\gamma_1 - \beta, 2\gamma_2 + 1 + 2^{d-1}h)$, стійкість до SIS з $\zeta_2 = \max(2(\gamma_2 - \beta), 4\gamma_2 + 2)$ згідно [4 – 6].
6. Якщо

$$\lambda_1 < 512 \square \lambda_2 < 512 \square \lambda_3 < 512 \square \lambda_4 < 512 \tag{10}$$

тобто стійкість до будь-якої з атак менша за необхідне значення $\lambda = 512$, то збільшити *k* та *l,* і повернутися до кроку 5

7. Обчислити h як найбільше ціле, для якого виконується нерівність

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

$$2^h \binom{n}{h} \geq 2^{512} \tag{11}$$

$$h = 118$$

8. Обчислити d як найбільше ціле, для якого виконується нерівність

$$2^{d-1}h + 1 \leq 2\gamma_2$$

$$2^{d-1} \square 118 + 1 \leq 2 \square 261888 \tag{12}$$

$$d = 13$$

9. Обчислити $w = \lfloor 0.08nk \rfloor = 0.08 \square 9 \square 512 = 368.64 = 368$

Зведені значення параметрів для $\lambda = 512$ наведено в табл. 4.

В табл. 5 наведено значення загальносистемних параметрів рівня стійкості 512/256 при $k = 9$ та $l = 8$.

Таблиця 4

Значення загальносистемних параметрів для рівня стійкості 512/256

Стійкість	N	γ_1	γ_2	η	β	d	h	ω
$\lambda = 512$	512	523776	261888	2	76	13	118	368

4. Захищеність алгоритму ЕП від атак сторонніми каналами

В процесі проведення конкурсу на другому етапі була висунута особлива вимога до захищеності кандидату на стандарт ЕП від атак сторонніми каналами.

Дослідження стосовно алгоритму ЕП Dilithium було проведено за такими параметрами [15]:

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

Для проведення експерименту було згенеровано 10000 ключів та виконано 10000 підписів. Результат залежності часу підпису від номеру ключа наведено на рис. 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 практично не залежить від ключа. Номери ключів, для яких було отримано мінімальне та максимальне значення при повтореннях вимірів не повинні співпадати.

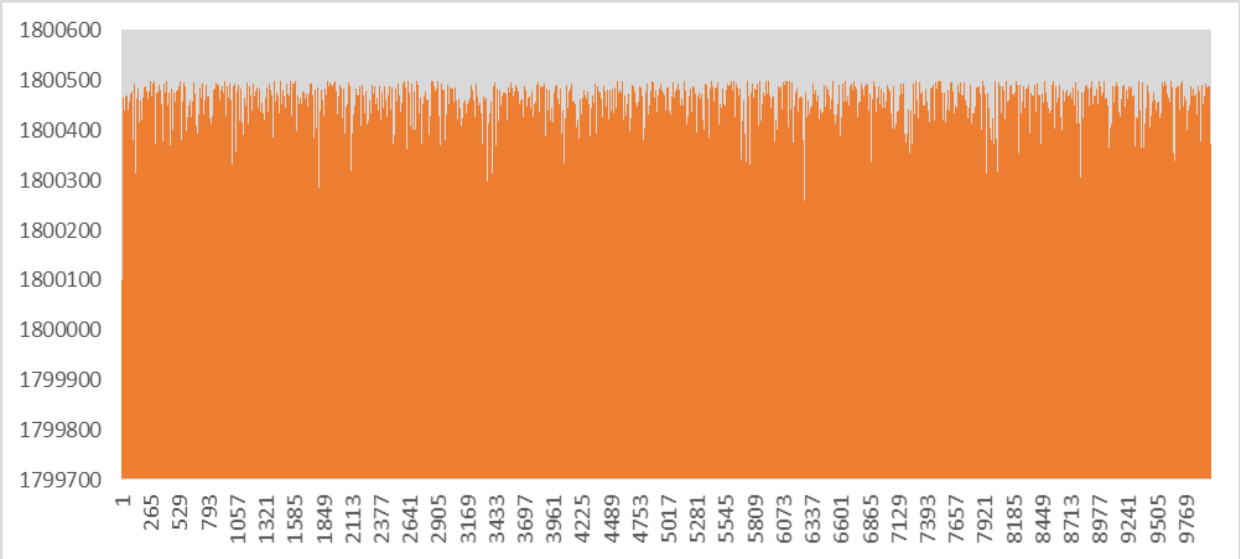

Рис. 1. Залежність часу підпису (у тактах процесору) від номеру ключа

Значення дисперсії $d \approx 2\%$, що свідчить про практично (враховуючи можливі відхилення при роботі операційної системи) статистичну незалежність часу підпису від ключа, що є важливим з точки зору захищеності від атак сторонніми каналами на основі різної складності множення поліномів тощо.

Висновки

1. Другий етап конкурсу NIST PQC завершився прийняттям для подальшого розгляду трьох основних алгоритмів електронного підпису [1]: Rainbow, CRYSTALUS-DILITHIUM та FALCON. Причому, з останніх двох скоріше за все буде обрано один, так як вони обидва ґрунтуються на проблемі LWE.

2. Алгоритм ЕП Dilithium з параметрами, наведеними в [4, 5], забезпечує тільки 1-4 рівні безпеки за класифікацією NIST. NIST ставить питання про генерацію параметрів рівня стійкості 5 та вище, що є перспективним напрямком подальших досліджень в контексті впливу параметрів більш високих рівнів стійкості на техніко-експлуатаційні характеристики, такі як швидкодія.

3. Генерування параметрів для більш високих рівнів безпеки є проблемним питанням через те, що не всі алгоритми детально описані і потребують подальших досліджень.

4. В алгоритмі Dilithium при генеруванні загальних параметрів використовуються засоби з рівноймовірним розподілом, що було доведено в [5, 11 – 13], а також перевірено практично. Також такі операції, як множення поліномів та їх округлення реалізовані з однаковою часо-

вою складністю. Це забезпечує захист від атак сторонніми каналами на основі різної складності множення поліномів тощо.

5. Аналіз показав, що складність проблеми навчання з помилками знайдена лише асимптотично. Так, доведено [2], що за певних умов складність вирішення LWE в просторі розмірності n становить щонайменше $2^{O(n)}$

6. На основі аналізу визначено [9 – 13], що стосовно атак на LWE можливо виділити та необхідно розглядати такі атаки як: атака грубої сили, тобто повного перебору; традиційна атака зустріч посередині; атака на основі алгоритму Arora-Ge; BKW, коли LWE зводиться до SIS атаки; primal attack (Search-LWE зводиться до BDD атаки); Dual attack (Decision-LWE зводиться до SIS); зведення до uSVP атаки пошуку короткого вектора

7. Як видно з табл. 3, нижня оцінка довжини блоку, потрібної для успішної реалізації дуальної атаки, є помітно вище в порівнянні зі значенням цього параметру для прямої атаки.

Знаходження довжини блоку b за параметрами k, l, η – найбільш нетривіальна частина алгоритму вибору параметрів. Довжина блоку залежить від значень k, l, η, n, q і розраховується для кожної з двох задач (SIS та LWE) та двох можливих атак (прямої та дуальної) на кожну з них згідно з методикою, наведеною в [8, 9] (таким чином, для обчислення b слід застосувати чотири різні алгоритми та взяти найменше з отриманих значень – п. 6 алгоритму вибору параметрів у підрозд. 3).

Список літератури:

1. NISTIR 8309 / Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper,Quynh Dang,John Kelsey,Yi-Kai Liu,Carl Miller,Dustin Moody,Rene Peralta,Ray Perlner,Angela Robinson,Daniel Smith-Tone. Access mode: http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf.

2. *Gottfried Herold, Elena Kirshanova, and Alexander May*. On the asymptotic complexity of solving LWE // Designs, Codes and Cryptography, Jan 2017.

3. *Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler and Damien Stehlé* CRYSTALS-Dilithium: Algorithm Specifications and Supporting Documentation. Access mode: https://pq-crystals.org/dilithium/data/dilithium-specification.pdf.

4. Post-Quantum Cryptography. Round 2 Submissions. Electronic resource. Access mode: https://csrc.nist.gov/Projects/post-quantum-cryptography/round-2-submissions.

5. *Lyubachevsky V., Ducas L., Kiltz E.* et all. CRYSTALS–Dilithium. Techn. rep. NIST (2017). Electronic resource. Access mode: https://crc.nist.gov./projects/post-quantum-cryptogtraphy/ round-1-submissions.

6. *Rachel Player*. Parameter selection in lattice-based cryptography. Access mode: https://pure.royalholloway.ac.uk/portal/files/29983580/2018playerrphd.pdf.

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

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

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

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

11. *Vadim Lyubashevsky*. Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures // ASIACRYPT, pages 598–616, 2009.

12. *Vadim Lyubashevsky*. Lattice signatures without trapdoors. In EUROCRYPT, pages 738–755, 2012.

13. *Tim Güneysu, Vadim Lyubashevsky, and Thomas Pöppelmann*. Practical lattice-based cryptography: A signature scheme for embedded systems. In CHES, pages 530–547, 2012.

14. *Горбенко І. Д.*, Постквантова криптографія та механізми її реалізації / І. Д. Горбенко, О. О. Кузнецов, О. В. Потій, Ю. І. Горбенко, Р. С., Ганзя, В. А. Пономар // Радиотехника. 2017. Вип. 186. С. 32–52.

15. *Кулібаба В.А.*, Перспективні методи та системи критптографічного захисту інформації / О.М. Олексійчук, В.А. Кулібаба, М.В. Єсіна, С. О. Кандій, Є.В. Острянська, І.Д. Горбенко // Радіотехніка. 2020. Вип. 200. С. 5-13.

Надійшла до редколегії 05.09.2020

Відомості про авторів:

Кулібаба Владислав Андрійович – Харківський національний університет імені В.Н. Каразіна, аспірант кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Україна, E-mail: vlad.kulibaba1994@gmail.com.