УДК 004.056.5 **DOI:10.30837/rt.2022.2.209.03**

С.О. КАНДІЙ, І.Д. ГОРБЕНКО, д-р техн. наук, Є.В. ОСТРЯНСЬКА

ПОРІВНЯННЯ ЯКОСТІ АЛГОРИТМІВ СЕМПЛУВАННЯ З ДИСКРЕТНОГО НОРМАЛЬНОГО РОЗПОДІЛУ НА NTRU РЕШІТКАХ

Вступ

Постквантова криптографія є напрямом досліджень, що вивчає криптографічні перетворення, які захищені від атак з використанням квантових комп'ютерів. У 2016 році NIST США оголосив про початок конкурсу NIST PQC, метою якого є створення нових постквантових криптографічних стандартів. Наразі триває третій фінальний етап цього конкурсу. Згідно з аналізом спеціалістів NIST [5], одним з перспективних напрямів у постквантовій криптографії є криптографія на алгебраїчних решітках. У звіті [4] зазначається, що NIST планує стандартизувати хоча б один електронний підпис (ЕП) на решітках. Серед електронних підписів фіналістами, які є представниками криптографії на решітках, є CRYSTALS-Dilithium [2] та Falcon[3].

Falcon є підписом типу Hash-and-Sign [6] на основі решіток. У схемах такого роду ключ підпису є «гарним» уявленням решітки, одностороння функція з підказкою, що дає можливість, враховуючи довільну точку в «навколишньому просторі», знайти точки решітки, які є відносно близькими до неї (тобто розв'язати задачу апроксимації найближчого вектора, ApproxCVP); ключ перевірки, з іншого боку, є «поганим» уявленням: він дозволяє будь-кому перевірити, чи є точка в решітці, але не вирішити ApproxCVP. Для того щоб підписати повідомлення, спочатку обчислюється геш, що відображає повідомлення на випадкову точку в навколишньому просторі, а підпис є точкою решітки, близькою до неї, отриманою за допомогою односторонньої функції з підказкою. Щоб перевірити підпис, перевіряється, що підпис є точкою решітки і достатньо близько до геш значення повідомлення.

Для ранніх конструкцій за цим напрямком, такі як схема підпису GGH та NTRUSign [6, 7] виявилося, що вони є небезпечними через поширену критичну вразливість: точки решітки, отримані як підписи, призводять до витоку інформації про односторонню функцію з лазівкою, що використовувалася для їх обчислення, і ця функція може бути відновлена з використанням статистичних методів [7]. Один із кандидатів у першому раунді NIST був фактично зламаний з використанням такої ж ідеї [5].

Таким чином, для безпеки дуже важливо довести, що вибірка підписів здійснюється відповідно до розподілу, що статистично не залежить від односторонньої функції з лазівкою. Першим підходом до цього залишається фреймворк GPV [6]: генерується вирішення задачі ApproxCVP відповідно до дискретного гаусового розподілу з центром у цільовій точці з коваріацією, незалежною від односторонньої функції з лазівкою (зазвичай сферичної).

Загальна структура підписів GPV може сильно відрізнятися залежно від решіток, над якими вони створюються, конструкцій односторонніх функцій з лазівкою і алгоритмів гаусової вибірки, на які вони спираються. Досягнутий рівень безпеки за такою схемою по суті визначається якістю односторонньої функції з лазівкою і алгоритмом вибірки. Якість визначена як мінімальне стандартне відхилення, досяжне в гаусовій вибірці, при збереженні статистичної незалежності виходу.

Метою цієї статті є порівняння якості алгоритмів семплування на решітках. Зокрема, в роботі розглянуто алгоритми Клейна (його модифікацю – алгоритм Преста та Дукаса [3]), алгоритм Пейкерта [7] та алгоритм семплування без використання арифметики з плаваючою крапкою [8].

1. Попередні визначення

Для будь-якого $a \in \mathbb{R}$ задамо $[a]_q = \lfloor aq \rceil / q \in (1/q)\mathbb{Z}$. Через A^t позначимо транспонування будь-якої матриці A. Нехай $s_1(A) = \max_{x \neq 0} \frac{\|Ax\|}{\|x\|}$ – найбільше сингулярне значення A. Нехай $\Sigma \in \mathbb{R}^{n \times n}$ – симетрична матриця. Матриця є позитивно визначеною якщо для будь-якого $x \in \mathbb{R}^n$ виконується $x^t \Sigma x > 0$. Позитивна матриця позначається як $\Sigma \succ 0$. Якщо $\Sigma_1 - \Sigma_2 \succ 0$, то це позначається як $\Sigma_1 \succ \Sigma_2$. $\Sigma \succ 0$ тоді і тільки тоді, коли $\Sigma^{-1} \succ 0$ та $\Sigma_1 \succ \Sigma_2 \succ 0$ тоді і тільки тоді, коли $\Sigma_2^{-1} \succ \Sigma_1^{-1} \succ 0$. Решітка $\mathbf{\Lambda}$ є дискретною адитивною підгрупою евклідового простору. Коли простір $\mathbb{R}^m$, то решітка може бути задана базисом $\Lambda(B) = \{Bx | x \in \mathbb{Z}^d\}$. Якщо B є повноранговою, то d є рангом решітки. Об'єм решітки $\mathbf{\Lambda}$ – $Vol(\Lambda) = \det(B^t B)^{\frac{1}{2}}$ для будь-якого базиса B.

Нехай $d = 2^l$ для деякого $l \geq 1$ та ζ_d буде $2d$-й примітивний корінь з 1. Тоді для фіксованого d буде $\mathcal{K} := \mathbb{Q}(\zeta_d)$ – d-е циклотомічне кільце та кільце його алгебраїчних цілих $\mathcal{R} := \mathbb{Z}[\zeta_d]$. Автоморфізм поля $\zeta_d \mapsto \zeta_d^{-1} = \overline{\zeta_d}$ відповідає комплексному спряженню та f^* є зображенням f у цьому автоморфізмі. Ми маємо $\mathcal{K} \simeq \mathbb{Q}[x]/(x^d + 1)$, $\mathcal{R} \simeq \mathbb{Z}[x]/(x^d + 1)$, $\mathcal{K}_\mathbb{R} := \mathcal{K} \otimes \mathbb{R} \simeq \mathbb{R}[x]/(x^d + 1)$. Кожне $f = \sum_{i=0}^{d-1} f_i \zeta_d^i \in \mathcal{K}_\mathbb{R}$ може бути ідентифіковане вектором коефіцієнтів $(f_0, \dots, f_{d-1}) \in \mathbb{R}^d$. Операція доповнення може бути розширена на $\mathcal{K}_\mathbb{R}$ та $\mathcal{K}_\mathbb{R}^+$ – підпростір елементів, для яких виконується $f^* = f$.

Циклотомічне поле $\mathcal{K}$ асоційоване з d комплексними вкладеннями $\varphi_i : \mathcal{K} \to \mathbb{C}$, які відображають поліном f до його значення в точках ζ_d з непарними індексами. Це відображення визначає канонічне вкладення $\varphi(f) := (\varphi_1(f), \dots, \varphi_d(f))$. Воно легко узагальнюється на $\mathcal{K}_\mathbb{R}$ та визначає простір $\mathcal{H} = \{v \in \mathbb{C}^d : v_i = \overline{v_{\frac{d}{2}+i}}, 1 \leq i \leq \frac{d}{2}\}$. Зауважимо, що $\varphi(fg) = \left(\varphi_i(f)\varphi_i(g)\right)_{i \leq d}$. За потреби це вкладення поширюється на вектори або матриці над $\mathcal{K}_\mathbb{R}$. Через $\mathcal{K}_\mathbb{R}^{++}$ позначимо підмножину $\mathcal{K}_\mathbb{R}^+$, яка має усі додатні коефіцієнти в канонічному вкладенні.

NTRU решітки є вільними $\mathcal{R}$-модулями ранга 2 в $\mathcal{K}^2$, або іншими словами групи форми $\mathcal{R}x + \mathcal{R}y$, де $x = (x_1, x_2), y = (y_1, y_2)$ натягнуто на $\mathcal{K}^2$. Існує природна білінійна форма над $\mathcal{K}^2$, що визначена як $\langle x, y \rangle_\mathcal{K} := x_1^* y_1 + x_2^* y_2 \in \mathcal{K}$. Може бути показано, що для всіх $x \in \mathcal{K}^2, \langle x, y \rangle_\mathcal{K} \in \mathcal{K}_\mathbb{R}^{++}$. Ця форма супроводжується відповідним поняттям ортогональності. Зокрема, процедура ортогоналізації Грама – Шмідта для пари лінійно незалежних векторів $b_1, b_2 \in \mathcal{K}^2$ визначена наступним чином:

$$\tilde{b_1} := b_1, \tilde{b_2} := b_2 - \frac{(b_1, b_2)_\mathrm{K}}{(b_1, b_1)_\mathrm{K}} \tilde{b_1} \tag{1}$$

Легко перевірити, що $\langle \widetilde{b_1}, \widetilde{b_2} \rangle_\mathcal{K} = 0$. Матриця Грама – Шмідта з стовбцями $\widetilde{b_1}, \widetilde{b_2}$ позначена як $\tilde{B}$ та ми маємо $det\tilde{B} = detB$. Для $\Sigma \in \mathcal{K}_\mathbb{R}^{2 \times 2}$ через Σ^* позначимо комплексно спряжену та транспоновану матрицю у $\mathcal{K}_\mathbb{R}$.

Функція Гауса над $\mathbb{R}^d$ з центром c та матрицею коваріації $\Sigma \succ 0$ визначена як $\rho_{c,\Sigma}(x) = \exp\left(-\frac{1}{2}(x - c)^t \Sigma (x - c)\right)$. Якщо $\Sigma = s^2 I_d$, то $\rho_{c,s} = \exp\left(-\frac{\|x-c\|^2}{2s^2}\right)$ та називається сферичною гаусовською функцією. Нормальний розподіл $\mathcal{N}_\Sigma$ з матрицею коваріації $\mathbf{\Sigma}$ має функцію розподілу $((2\pi)^d det\Sigma)^{-1/2} \rho_{0,\Sigma}$. Під $\mathcal{N}_{\mathcal{K}_\mathbb{R},s}$ мається на увазі розподіл $(z_1, \dots, z_d) \leftarrow \left(\mathcal{N}_{\frac{s}{\sqrt{d}}}\right)^d$. Дискретний розподіл Гауса над решіткою $\mathbf{\Lambda}$ з центром c та матрицею коваріації $\mathbf{\Sigma}$ визначений як

$$\forall x \in \Lambda, \mathrm{D}_{\Lambda,c,\Sigma(x)} = \frac{\rho_{c,\Sigma}(x)}{\rho_{c,\Sigma}(\Lambda)} \tag{2}$$

Параметр згладжування η_ε решітки Λ для деякого ε визначений як

$$\eta_\varepsilon(\Lambda) = \min\left\{ s > 0 : \rho_{\frac{1}{s}}\left(\Lambda^\vee\right) \le 1+\varepsilon \right\}, \tag{3}$$

де $\Lambda^\vee$ – дуальна решітка. Обмеження на параметр зглажування надає наступна лемма:

Лемма 1 ([3,7]) Нехай $B\mathcal{R}^2$ є вільним $\mathcal{R}$-модулем та нехай $\Lambda = M(B)\mathbb{Z}^{2d}$ буде асоційованою решіткою в $\mathbb{R}^{2d}$. Тоді для всіх $\varepsilon > 0$ маємо

$$\eta_\varepsilon(\Lambda) \le |B|_{\mathrm{K}} \sqrt{\frac{\log\left(2d\left(1+\frac{1}{\varepsilon}\right)\right)}{2\pi^2}}. \tag{4}$$

2. Алгоритм семплування Пейкерта

У [6] Пейкертом запропоновано алгоритм для семплування з дискретного гаусовського розподілу для заданої решітки з використанням невеликого гаусовського шуму. Фактично цей алгоритм можливо описати як рандомізовану версію алгоритму округлення Бабаї з використанням випадкового шуму, що розподілений за розподілом Гауса для того, щоб приховати структуру решітки. Алгоритм може бути визначений у термінах алгебри $\mathcal{K}_{\mathbb{R}}$, що показано на рис. 1.

Алгоритм семплування Пейкерта

Вхідні данні: матриця $B \in \mathcal{K}_{\mathbb{R}}^{2\times 2}$ та центральний вектор $c \in \mathcal{K}_{\mathbb{R}}^{2}$
Вихідні данні: $z \in \Lambda$ з розподілом близьким до гаусовсткого
Параметри алгоритма: параметр $r \ge \eta_\varepsilon(\mathcal{R}^2)$ та $\Sigma_0 \in \mathcal{K}_{\mathbb{R}}^{2\times 2}$ для якої $\Sigma_0\Sigma_0^* = \Sigma - r^2 BB^*$
$x \leftarrow \Sigma_0\left(\mathcal{N}_{\mathcal{K}_{\mathbb{R}},1}\right)^2$ $z \leftarrow \lceil B^{-1}(c-x) \rfloor_r$ Повернути Bz

Рис. 1. Алгоритм семплування Пейкерта

Коли $\Sigma \succ r^2 BB^*$, то існування Σ_0 гарантоване. Якість семплування можливо оцінити наступним чином:

Теорема 1 [8]. Позначимо розподіл ймовірностей на виході алгоритму семплування Пейкерта як $\mathcal{D}$. Якщо $\varepsilon \le \frac{1}{2}$ та $\sqrt{\Sigma} \ge s_1(B)\eta_\varepsilon(\mathcal{R}^2)$, то статистична відстань між $\mathcal{D}$ та $\mathcal{D}_{\Lambda,c,\Sigma}$ обмежена 2ε. Більш того,

$$\sup_{x\in B\mathrm{R}^2} \left| \frac{\mathrm{D}(x)}{\mathrm{D}_{\Lambda(B),c,\Sigma}(x)} - 1 \right| \le 4\varepsilon \tag{5}$$

На практиці параметр коваріації є скалярним кратним тотожної матриці або позитивною дійсною константою.

3. Алгоритми семплування Кляйна та Дукаса і Преста.

У роботі [3] запропоновано гібридний алгоритм для семплування з дискретного гаусовського розподілу для заданої решітки. На високому рівні цей гібридний семплер дотримується підходу Кляйна, який є рандомізованою версією алгоритму найближчої площини Бабаї. У контексті кільця виконується підпрограма рандомізації «на рівні кільця», а не «на рівні цілих чисел». Щоб приховати структуру решітки, також використовується шум, але його розподіл тепер залежить від цільового центру. Алгоритм може бути описаний як зображено на рис. 2.

Алгоритм семплування Дукаса і Преста

Вхідні данні: матриця $B \in \mathcal{K}_{\mathbb{R}}^{2\times 2}$, її ортогоралізація Грама-Шмідта $\tilde{B} \in \mathcal{K}_{\mathbb{R}}^{2\times 2}$,центральний вектор $c \in \mathcal{K}_{\mathbb{R}}^{2}$, параметр σ

Вихідні данні: $z \in \Lambda$ з розподілом близьким до гаусовсткого

Параметри алгоритма: $\sigma_i := \sqrt{\frac{\sigma^2}{\langle b_i, b_i \rangle} - r^2}$

$c_2 \leftarrow c, v_2 \leftarrow 0$
$d_2 \leftarrow \frac{\langle \widetilde{b_2}, c_2 \rangle_{\mathcal{K}}}{\langle \widetilde{b_2}, \widetilde{b_2} \rangle_{\mathcal{K}}}$
$u_2 \leftarrow \mathcal{N}_{\mathcal{K}_{\mathbb{R}},1}$
$y_2 \leftarrow \sigma_2 u_2$
$x_2 \leftarrow \lfloor d_2 - y_2 \rceil_r$
$c_1 \leftarrow c_2 - x_2 b_2, v_1 \leftarrow x_2 b_2$
$d_1 \leftarrow \frac{\langle \widetilde{b_1}, c_1 \rangle_{\mathcal{K}}}{\langle \widetilde{b_1}, \widetilde{b_1} \rangle_{\mathcal{K}}}$
$u_1 \leftarrow \mathcal{N}_{\mathcal{N}_{\mathcal{K}_{\mathbb{R}},1}}$
$y_1 \leftarrow \sigma_1 u_1$
$x_1 \leftarrow \lfloor d_1 - y_1 \rceil_r$
$v_0 \leftarrow v_1 + x_1 b_1$
$return\ v_0$

Рис. 2. Алгоритм семплування Дукаса і Преста

Якість семплування можливо оцінити наступним чином:

Т е о р е м а 2 [8]. Позначимо розподіл ймовірностей на виході алгоритму семплування Дукаса і Преста як $\mathcal{D}$. Якщо $\varepsilon \leq 2^{-5}$ та$\sqrt{\Sigma} \geq s_1(B)\eta_\varepsilon(\mathcal{R}^2)$, то статистична відстань між $\mathcal{D}$ та $\mathcal{D}_{\Lambda,c,\Sigma}$ обмежена 7ε. Більш того,

$$\sup_{x\in BR^2} \left| \frac{\mathrm{D}(x)}{\mathrm{D}_{\Lambda(B),c,\Sigma}(x)} - 1 \right| \leq 14\varepsilon \qquad (6)$$

4. Алгоритм семплування без використання обчислень з плаваючою крапкою

Великим недоліком алгоритма семплування Дукаса і Преста є використання обчислень з плаваючою крапкою, що значно ускладнює криптоаналіз та реалізацію. В роботі [8] запропонований алгоритм семплування, що поєднує алгоритми Пайкерта, Дукаса і Преста та дозволяє семплувати значення з гаусовського розподілу без використання обчислень з пла-

ваючою крапкою за допомогою техніки з роботи [9], в якій було показано як генерувати малий шум за допомогою розкладу Холецького виключно за допомогою цілочисельних обчислень. Розклад Холецького полягає у тому, що можливо представити матрицю у вигляді добутку верхньотрикутної матриці з додатніми елементами на діагоналі на її транспоновану версію. Якщо базис деякої решітки заданий у вигляді верхньотрикутної матриці, то можливо спростити процес семплування. На рис. 3 зображено алгоритм для такого випадку на основі алгоритма Пайкерта, що був описаний вище.

USampler (Алгоритм семплування для верхньотрикутних матриць)

Вхідні данні: верхньотрикутна матриця $U = [(1,0),(u,1)], u \in \mathcal{K}$, параметр $r > 0$

Вихідні данні: $z \in \Lambda$ з розподілом близьким до гаусовського $\mathcal{D}_{\Lambda(U),c,r}$

$z_2 \leftarrow PeikertSampler_{\mathbb{Z}}(c_2, r)$
$c_1' \leftarrow c_1 - z_2 u$
$z_1 \leftarrow PeikertSampler_{\mathbb{Z}}(c_1', r)$
$return\ z = U(z_1, z_2)$

Рис. 3. Алгоритм семплування для випадку, коли базис є верхньотрикутною матрицею

Якщо помножити вихідний вектор алгоритму USampler для відповідної матриції U на ортогоналізацію Грама – Шмідта цільового базиса, то отримаємо вектор на цільовій решітці:

$$\tilde{B}z = \tilde{B}U\left(z_1, z_2\right) = BU^{-1}U\left(z_1, z_2\right) = B\left(z_1, z_2\right) \in \Lambda. \tag{7}$$

Оскільки значення векторів після ортогоналізації Грама – Шмідта можуть мати великі знаменники, то, щоб запобігти цьому, можна використовувати апроксимацію $\hat{B} \in (1/(pq)\,\mathcal{R}^{2\times 2}$ б отриману як округлення за модулем p для B. Вплив на розподіл ймовірностей при цьому буде вимірюватися через найбільше сингулярне значення відповідної матриці Грама – Шмідта $s_1(\tilde{B})$. Алгоритм семплування, що реалізує цю ідею наведено на рис. 4.

В алгоритмі на рис. 4 матрицю A, для якої виконується

$$AA^t = p^2\left(\Sigma_p - I\right) \tag{8}$$

можливо отримати за допомогою алгоритма з роботи [9]. Використання цього алгоритма впливає на вибір параметрів алгоритму семплування, зокрема на вибір параметра s.

Алгоритм на рис. 4 використовує процедуру $OfflinePhase$. Ця процедура також пов'язана з алгоритмом генерації матриці A і адаптована для алгоритму семплування. Вона семплує вектор з розподілу $\mathcal{D}_{\mathcal{R}^2,r^2,\Sigma_p}$. Алгоритм $OfflinePhase$ зображено на рис. 5.

Для оцінки якості роботи алгоритму семплування без використання обчислень з плаваючою крапкою можливо скористатись наступною теоремою.

Теорема 3 [8]. Нехай для $\varepsilon \in (0,1)$ задано $s > s_1(\tilde{B})(1+\sqrt{2d/p})+1$ та ціле число $r \geq \eta_\varepsilon(\mathbb{Z}^{2d})$, тоді статистична відстань між $\mathcal{D}$ та $\mathcal{D}_{\Lambda(\mathrm{B}),\mathrm{c},\mathrm{sr}}$ обмежена 15ε. Більше того,

$$\sup_{x\in\Lambda(B)}\left|\frac{\mathrm{D}\left(x\right)}{\mathrm{D}_{\Lambda(B),c,\Sigma}\left(x\right)}-1\right| \leq 30\varepsilon \tag{9}$$

Алгоритм семплування без використання обчислень з плаваючою крапкою

Вхідні данні: Матриця $\hat{B} \in \mathcal{R}^{2\times 2}$, для якої виконується $\hat{B}U_{\hat{u}} = B = \hat{B}U_u$, де $\hat{u} = \lceil u \rfloor_p \in \frac{1}{p}\mathcal{R}$, центр $c \in \mathcal{R}^2$ та параметри $r, s > 0$

Вихідні данні: $z \in \Lambda$ з розподілом близьким до гаусовського $\mathcal{D}_{\Lambda(B),c,rs}$

Параметри алгоритма: $\Sigma_v = s^2 I - \hat{B}\hat{B}^t$ та матриця A, для якої виконується $AA^t = p^2(\Sigma_p - I)$

$p \leftarrow OfflinePhase(p, A)$
$\hat{c} \leftarrow \hat{B}^{-1}(c - p)$
$z' = USampler(\hat{u}, \hat{c}, s)$
$return\ z = \hat{B}z'$

Рис. 4. Алгоритм семплування без використання обчислень з плаваючою крапкою

$OfflineSampler$

Вхідні данні: ціле число $p > 0$, матриця $A \in \mathcal{R}^{2\times m}$

Вихідні данні: $p \in \mathcal{R}$ з розподілом близьким до $\mathcal{D}_{\mathcal{R}^2, r^2\Sigma}$, де $\Sigma = \frac{1}{p^2}AA^t + I$

Параметри алгоритма: цілі числа $r > \eta_\varepsilon(\mathcal{R}^2)$ та L, для якого виконується $Lr \geq \eta_\varepsilon(\Lambda(A)^\perp)$

$x \leftarrow (\lceil 0 \rfloor_{Lr})^m$
$p' \leftarrow \frac{1}{pL}Ax$
$p \leftarrow \lceil p' \rfloor_r$
$return\ p$

Рис. 5. Оффлайн фаза семплування у алгоритмі семплування без використання обчислень з плаваючою крапкою

5. Порівняння якості алгоритмів семплування для NTRU решіток

У випадку NTRU решіток, одностороння функція з лазівкою є секретний базис

$$B_{f,g} = \begin{bmatrix} f & F \\ g & G \end{bmatrix} \tag{10}$$

Стандартне відхилення дискретного гаусовського розподілу σ, що використовується з цією односторонньою функцією може бути різним і значно залежить від алгоритму семплування. У загальному випадку для NTRU решіток [3, 6] σ має вигляд

$$\sigma = \alpha\eta_{\varepsilon}\left(\mathrm{R}^{2}\right)\sqrt{q} \tag{11}$$

де фактор $\alpha \geq 1$, який є показником якості і залежить від алгоритму семплування.

Для алгоритму семплування Клейна (і відповідно Дукаса і Преста), який використовується в Falcon $\alpha\sqrt{q}$ дорівнює нормі від ортогоналізованого за Грамом – Шмідтом базисом $B_{f,g}$ [3]:

$$\alpha\sqrt{q} = \left\|B_{f,g}\right\|_{GS} = \max_{1\leq i\leq 2d}\left\|b_i^{\square}\right\|_2. \tag{12}$$

Для алгоритму семплування Пейкерта над $\mathcal{K}$ маємо [10]:

$$\alpha\sqrt{q} = \mathrm{s}_1\left(B_{f,g}\right). \tag{13}$$

І для алгоритму семплування без використання арифметики з плаваючою крапкою маємо [8]:

$$\alpha\sqrt{q} = \left|B_{f,g}\right|_{\mathrm{K}}. \tag{14}$$

У докторській роботі [10] Прест за допомогою ряду евристик визначив оптимальні асимптотичні значення для параметра α, які можливо досягти на практиці для алгоритму Клейна та алгоритму Пейкерта. Для алгоритму семплування Пейкерта оптимальне значення становить $\alpha = O(d^{\frac{1}{4}}\sqrt{\log d})$. Для алгоритму семплування Клейна (і відповідно Дукаса і Преста) маємо $\sqrt{e/2}$, тобто $\alpha = O(1)$. Для алгоритму семплування без використання аріфметики з плаваючою крапкою [8] маємо $\alpha = O(d^{1/8}\log^{1/4} d)$. У табл. 1 зведені загальні результати для алгоритмів семплування.

Таблиця 1

Порівняння якості алгоритмів семплування

Алгоритм семплування	Стандартне відхілення, що може бути досягнуто	Асимптотична оцінка параметра α
Алгоритм Пейкерта	$\sigma = s_1(B_{f,g})\eta_{\varepsilon}(\mathcal{R}^2)\sqrt{q}$	$\alpha = O(d^{\frac{1}{4}}\sqrt{\log d})$
Алгоритм Клейна (і модифікація Дукаса – Преста)	$\sigma = \left\|B_{f,g}\right\|_{GS}\eta_{\varepsilon}(\mathcal{R}^2)\sqrt{q}$	$\alpha = O(1)$
Алгоритм без використання арифметики з плаваючою крапкою	$\sigma = \left\|B_{f,g}\right\|_{\mathcal{K}}\eta_{\varepsilon}(\mathcal{R}^2)\sqrt{q}$	$\alpha = O(d^{1/8}\log^{1/4} d)$

Висновки

1. Підписи типу Hash-and-Sign на решітках зазвичай розробляються відповідно до фреймворка GPV [20] за допомогою гешування повідомлення до певного вектору та повернення як підпису точки решітки близько до цього вектору. Це робиться за допомогою «гарного» представлення решітки, яке називається односторонньою функцією з лазівкою, що дає можливість підписувачу вирішити проблему ApproxCVP з відносно невеликим фактором апроксимації. Крім того, щоб запобігти витоку інформації про секретний ключ, близькі точки решітки необхідно відбирати відповідно до статистично незалежного розподілу. Зазвичай використовується сферичний дискретний гаусовий розподіл, що заданий на решітці і має

математичне очікування у точці, що відповідає повідомленню. Для того щоб сформувати такий вектор, використовуються алгоритми семплування з гаусівського розподілу.

2. Безпека схем підпису залежить від стандартного відхилення дискретного гаусівського розподілу, який має алгоритм семплування. Чим менше стандартне відхилення, тим ближче відстань до вектора, що кодує повідомлення, і тим складніше відповідна проблема ApproxCVP, а отже, і вищий рівень безпеки. Однак існує нижня межа (залежно від односторонньої функції з лазівкою) до того, наскільки маленького стандартного відхилення може досягти алгоритм семплування, зберігаючи статистику майже близько до бажаного сферичного гаусівського розподілу, нижче якого розподіл може починати відрізнятися від розподілу Гауса способами, які могли б розкрити інформацію про односторонню функцію з лазівкою, і таким чином ставить під загрозу безпеку електронного підпису.

3. В роботі було розглянуто найбільш розповсюджені варіанти алгоритмів семплування. Якість всіх алгоритмів значно залежить від структури решітки, для якої відбувається семплування.

4. Алгоритм семплування Пейкерта був розроблений історично першим. На NTRU решітках він дає найбільш погані результати, проте його можливо використовувати як підпроцедуру у більш складних алгоритмах семплування.

5. Алгоритм семплування Клейна, зокрема його модифікація – алгоритм Дукаса – Преста, дає найменші вектори. З теоретичної точки зору він набагато кращий за алгоритм Клейна на NTRU решітках, проте він вимагає використання арифметики з плаваючою крапкою, що значно ускладнює аналіз його безпеки та створення програмної чи апаратної реалізації. Алгоритм без використання обчислень з плаваючою крапкою з теоретичної точки зору є трохи гіршим, проте завдяки своїй простоті він легше піддається аналізу, що значно підвищує його привабливість для розробників електронних підписів.

6. Компенсувати гіршу якість семплування можливо іншими засобами у електронних підписах, в той час як буде залишатися простота реалізації. Це є безсумнівним плюсом для побудови сучасних постквантових схем. Потенційно це дає можливість вирішити недолік схеми Falcon і значно зменшити складність реалізації.

Список літератури:

1. Gorhan Alagic Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. 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
2. 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
3. Thomas Prest et Al. aFlcon: Fast-Fourier Lattice-basedCompact Signatures over NTRU. Access mode: https://falcon-sign.info/falcon.pdf
4. NISTR 8309. Status Report on the Second Round of the NIST Post-Quantum Cryptography Standartization Process. NIST, 2020. 39 p.
5. NIST Post-Quantum Cryptography Standartization Project : веб сайт. URL: https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization (дата звернення: 27.11.2020)
6. Craig Gentry, Chris Peikert, Vinod Vaikuntanathan How to Use a Short Basis: Trapdoors for Hard Lattices and New Cryptographic Constructions. -Access mode: https://eprint.iacr.org/2007/432.pdf
7. Phong Q. Nguyen, Oded Regev Learning a Parallelepiped: Cryptoanalysis of GGH and NTRU Signatures. Access mode: https://iacr.org/archive/eurocrypt2006/40040273/40040273.pdf
8. Thomas Espitau et all. MITAKA: A Simpler, Parallelizable Maskable Variant of Falcon. Access mode: https://eprint.iacr.org/2021/1486.pdf
9. Ducas L., Galbraith S., Prest T., Yu Y.: Integral matrix gram root and lattice gaussian sampling without floats // Canteaut A., Ishai Y. (eds.) EUROCRYPT 2020, Part II. LNCS, vol. 12106, pp. 608–637. Springer, Heidelberg (May 2020).
10. Thoms Prest Gaussian Sampling in Lattice-Based Cryptography. Access mode: https://tprest.github.io/pdf/pub/thesis-thomas-prest.pdf

11. Garillot F., Kondi Y., Mohassel P., Nikolaenko V. Threshold schnorr with stateless deterministic signing from standard assumptions // Malkin, T., Peikert, C.(eds.) Advances in Cryptology – CRYPTO 2021. pp. 127–156. Springer International Publishing, Cham (2021)

12. Fukumitsu M., Hasegawa S. A lattice-based provably secure multisignature scheme in quantum random oracle model // Nguyen, K., Wu, W., Lam, K.Y.,Wang, H. (eds.) Provable and Practical Security. pp. 45–64. Springer International Publishing, Cham (2020)

13. Esgin M.F., Steinfeld R., Sakzad A., Liu J.K., Liu D. Short lattice-based one-out-of-many proofs and applications to ring signatures. Cryptology ePrint Archive, Report 2018/773 (2018), https://ia.cr/2018/773

14. Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William Whyte, Zhenfei Zhang. Falcon: Fast-Fourier Lattice-basedCompact Signatures over NTRU. [Electronic resource]. Access mode: https://falcon-sign.info/falcon.pdf.

15. PQC Standardization Process: Third Round Candidate Announcement. July 22, 2020. [Electronic resource]. Access mode: https://csrc.nist.gov/News/2020/pqc-third-round-candidate-announcement

Надійшла до редколегії 03.03.2022

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, АТ "Інститут Інформаційних Технологій", головний конструктор, Україна; e-mail: gorbenkoi@iit.kharkov.ua; ORCID: https://orcid.org/0000-0003-4616-3449

Кандій Сергій Олегович – Харківський національний університет імені В. Н. Каразіна, аспірант кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, АТ «Інститут Інформаційних технологій», технік-конструктор, Україна; e-mail: sergeykandy@gmail.com

Острянська Єлизавета Вадимівна – аналітик з систем захисту інформації, АТ «Інститут Інформаційних технологій», Україна; e-mail: antelizza@gmail.com