НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. Ігоря СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Звіт з виконання лабораторної роботи

ДОСЛІДЖЕННЯ СУЧАСНИХ АЛГЕБРАЇЧНИХ КРИПТОСИСТЕМ

Виконала студентка
групи ФІ-52мн
Балацька Вікторія

Перевірив:
Фесенко А.В

Київ — 2025

ВСТУП

Мета роботи: Дослідження особливостей реалізації сучасних алгебраїчних криптосистем на прикладі учасників першого раунду національного конкурсу з постквантової криптографії в Кореї (KpqC).

Постановка завдання:

1. Реалізація алгоритму: розробити програмну реалізацію обраного криптографічного алгоритму та всі можливі варіанти цього алгоритму.

2. Перевірка коректності: підтвердити правильність реалізації за допомогою тестів, використовуючи офіційні тестові вектори або офіційну реалізацію.

3. Аналіз продуктивності та порівняння: знайти схожі алгоритми та провести порівняльний аналіз швидкодії за різних умов, дослідити вплив модифікацій окремих складових частин на ефективність.

4. Теоретичне дослідження: надати повний теоретичних опис алгоритму з усіма деталями та відомими результатами досліджень; провести аналіз наявних атак на обраний алгоритм та описати власні дослідження атак; виконати порівняльний аналіз обраного алгоритму зі схожими та дослідити можливість перенесення відомих атак на нього.

Хід роботи: У своїй роботи я досліджуватиму алгоритм підпису SOLMAE. SOLMAE - це схема підпису на основі решіток, що відповідає парадигмі "хеш-і-підпис"і представляється над NTRU решітками.

1 ТЕОРЕТИЧНЕ ДОСЛІДЖЕННЯ

У цій частині звіту я проведу теоретичне дослідження алгоритму підпису SOLMAE: формальне визначення та опис алгоритму; аналіз безпеки та відомі результати; порівняльний аналіз з іншими підписами; можливі атаки та їх перенесення; аналіз продуктивності.

1.1 Формальне визначення та опис алгоритму

SOLMAE - це схема підпису на основі решітки, та розшифровується як quantum-**S**ecure alg**O**rithm for **L**ong-term **M**essage **A**uthentication and **E**ncryption (квантово-безпечний алгоритм для довгострокової автентифікації та шифрування повідомлень). Для ефективної реалізації, структура потребувала класу решіток, що мають ефективно обчислювальні бази з трапдорами (trapdoors) для процедури підпису, дослідивши існуючі класи решіток, автори зупинились на NTRU-решітках. У такому випадку підписання зводиться до вибірки коротких гаусових векторів у відкритій NTRU решітці. Сам алгоритм SOLMAE натхненний дизайном Falcon. Проте, порівнюючи з Falcon, тут є певні нові теоретичні основи: на високому рівні усувається властива процедура вибірки технічності і більша частина її індукованої складності з точки зору реалізації, без втрати ефективності. Простота конструкції перетворюється на швидшу роботу, але при цьому зберігаючи розміри підписів і ключів верифікації, а також надаючи додаткові функції такі як дешевше маскування та можливість паралелізації.

1.1.1 Принципи проектування

Алгоритм підпису SOLMAE побудований за парадигмою hash-then-sign на решітках та покликаний покращити ефективність і безпеку порівняно з попередніми схемами, зокрема Falcon. Його проектування ґрунтується на трьох ключових ідеях (зображені на рисунку 1.1):

- Гібридний семплер (Hybrid Sampler) — швидший, простіший і паралелізований спосіб генерувати гаусові вектори, що спрощує підписування та зменшує обчислювальні витрати.

- Оптимізований алгоритм генерації ключів — спеціально налаштований для покращення якості трапдорів у NTRU-решітках і підвищення рівня безпеки при збереженні продуктивності.

- Техніки стиснення даних — зменшують розмір підписів і ключів без впливу на безпеку, оптимізуючи використання пропускної здатності.

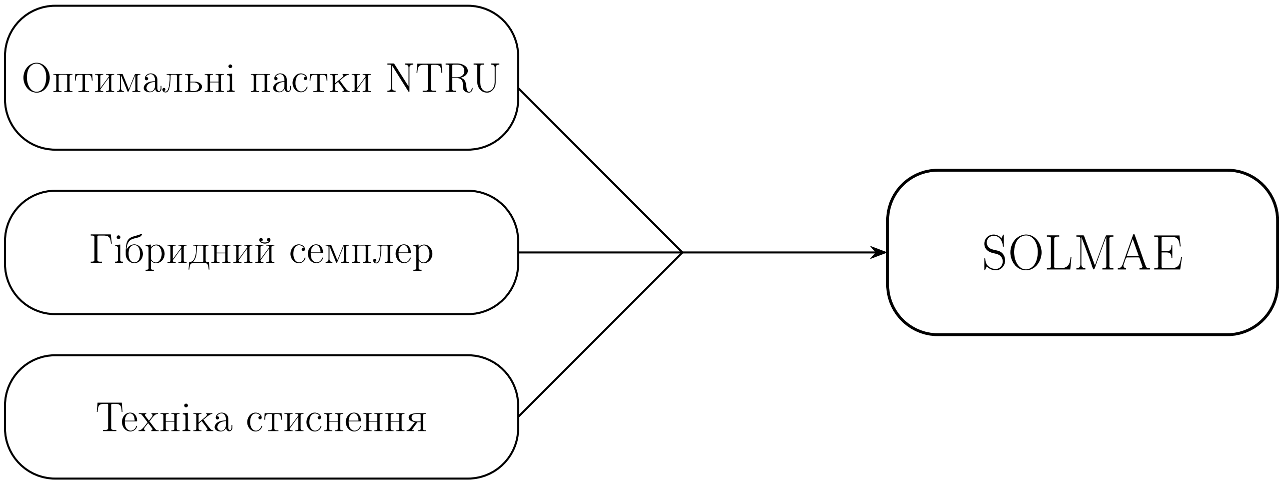

Рисунок 1.1 – Схематичне представлення основних компонентів алгоритму SOLMAE

SOLMAE використовує переваги алгебраїчної структури NTRU-решіток та поєднує сучасні підходи до побудови трапдорів і вибору гаусових вибірок. Завдяки цьому схема досягає високої швидкодії, меншого розміру підписів та ключів, а також зберігає стійкість до відомих атак на базові задачі решіток.

1.1.2 Базові поняття та позначення

Вектори позначаються жирними малими літерами та розглядаються як стовпчикові. Матриці позначаються жирними великими літерами. Коли ми говоримо, що матриця є базисом простору, маємо на увазі, що стовпчики цієї матриці утворюють базис. ℓ_2-норма вектора $\mathbf{x} = (x_1, \ldots, x_d)$ визначається як $\|\mathbf{x}\| = \left(\sum_i |x_i|^2\right)^{1/2}$, а його ℓ_∞-норма — як $\|\mathbf{x}\|_\infty = \max_i |x_i|$.

Решітки. Решітками називають дискретну підгрупу $\mathbb{R}^n$. Іншими словами, решітка - це множина цілочисельних лінійних комбінацій, отриманих з базису $\mathbf{B}$ $\mathbb{R}^n$. Об'єм решітки дорівнює $det(\mathbf{B})$ для будь-якого її базису.

Циклотомічні кільця степенів двійки. Для побудови схеми підпису SOLMAE використовується циклотомічне кільце $K = \mathbb{Q}[X]/(X^d + 1)$, де $d = 2^n$ — степінь двійки. Його цілочисельним підкільцем є $R = \mathbb{Z}[X]/(X^d + 1)$, а дійсне розширення позначається як $K_\mathbb{R} = \mathbb{R}[X]/(X^d + 1)$.

Поліном $f \in K_\mathbb{R}$ може бути представлений кількома способами:

1) Коефіцієнтне подання:

$$f = \sum_{i=0}^{d-1} f_i X^i \quad \longleftrightarrow \quad \mathbf{f} = (f_0, \ldots, f_{d-1}).$$

2) Канонічне вкладення (також відоме як дискретне перетворення Фур'є — DFT):

$$\varphi(f) = (\varphi_1(f), \ldots, \varphi_d(f)), \quad \varphi_j(f) = f(\zeta_j),$$

де $\zeta_j = e^{i(2j-1)\pi/d}$ — d-ті примітивні корені одиниці. У цьому поданні множення поліномів у кільці переходить у покомпонентне множення в $\mathbb{C}^d$.

3) Матриця множення:

$$[f] := \begin{pmatrix} f_0 & -f_{d-1} & \dots & -f_1 \\ f_1 & f_0 & \dots & -f_2 \\ \vdots & \vdots & \ddots & \vdots \\ f_{d-1} & f_{d-2} & \dots & f_0 \end{pmatrix}.$$

Для векторів $\mathbf{x} = (x_1, \dots, x_d)$ використовуються стандартні норми:

$$\|\mathbf{x}\|_2 = \left(\sum_i |x_i|^2 \right)^{1/2}, \qquad \|\mathbf{x}\|_\infty = \max_i |x_i|.$$

Алгебраїчний метод Грама-Шмідта. Для пар (f,g) та $(F,G) \in K_{\mathbb{R}}^{2\times 2}$ визначимо скалярний добуток: $\langle (f,g), (F,G) \rangle_K = f^* F + g^* G$, де f^* та g^* — спряжені елементи у $K_{\mathbb{R}}$.

Ортогоналізація Грама — Шмідта для пари (F,G) відносно (f,g) має вигляд:

$$(\widetilde{F}, \widetilde{G}) = (F, G) - \frac{\langle (f,g), (F,G) \rangle_K}{\langle (f,g), (f,g) \rangle_K} \cdot (f,g).$$

Легко перевірити, що $\langle (f,g), (\widetilde{F}, \widetilde{G}) \rangle_K = 0$, тобто вектори (f,g) та $(\widetilde{F}, \widetilde{G})$ є ортогональними.

Решітка NTRU. Нехай q — ціле число, а $f \in R$ таке, що f є оборотним за модулем q (еквівалентно, $\det[f]$ взаємно простий із q). Позначимо $h = g/f \bmod q$ та розглянемо $NTRU$-модуль, пов'язаний з h: $\mathcal{M}_{\mathrm{NTRU}} = \{(u,v) \in R^2 : \ hu - v = 0 \bmod q\}$, а також його ґраткову версію $\mathcal{L}_{\mathrm{NTRU}} = \{(\mathbf{u},\mathbf{v}) \in \mathbb{Z}^{2d} : \ [h]\mathbf{u} - \mathbf{v} = 0 \bmod q\}$.

Ця ґратка має об'єм q^d. Над R вона породжується парою (f,g) та будь-якими (F,G), що задовольняють $fG - gF = q$. У такому випадку $\mathcal{L}_{\mathrm{NTRU}}$ має базис вигляду:

$$\mathbf{B}_{f,g} = \begin{bmatrix} [f] & [F] \\ [g] & [G] \end{bmatrix}.$$

Легко перевірити, що $([h], -\mathrm{Id}_d) \cdot \mathbf{B}_{f,g} = 0 \bmod q$, тому відкритим ключем є h.

Задача NTRU-search формулюється так: маючи $h = g/f \bmod q$, знайти будь-яку пару $(f' = x^i f,\ g' = x^i g)$.

У варіанті decision потрібно розрізнити $h = g/f \bmod q$ від рівномірно випадкового $h \in R_q := \mathbb{Z}[X]/(q, X^d + 1)$. Ці задачі вважаються складними при великому d.

Якість базису NTRU. Секретний базис $\mathbf{B}_{f,g}$ не може бути довільною парою, оскільки він повинен забезпечувати можливість відбору коротких гаусових векторів у ґратці $\mathcal{L}_{\mathrm{NTRU}}$ за допомогою гібридного семплінгу. Якість базису $\mathbf{B}_{f,g}$ визначається наступною величиною:

$$\mathcal{Q}(f,g) = \max_{1 \leqslant i \leqslant d/2} \max \left(\frac{|\varphi_i(f)|^2 + |\varphi_i(g)|^2}{q},\ \frac{q}{|\varphi_i(f)|^2 + |\varphi_i(g)|^2} \right)^{1/2}.$$

Гаусові розподіли. Гаусова функція, центрована в точці $\mathbf{c} \in \mathbb{R}^d$ з додатно визначеною коваріаційною матрицею Σ, визначається як $\rho_{\mathbf{c},\Sigma}(\mathbf{x}) = \exp\big(-\frac{1}{2}(\mathbf{x} - \mathbf{c})^t \Sigma^{-1} (\mathbf{x} - \mathbf{c})\big)$.

Нормальний розподіл $\mathcal{N}_{\mathbf{c},\Sigma}$ із центром у $\mathbf{c}$ та коваріацією Σ має щільність, пропорційну $\rho_{\mathbf{c},\Sigma}$.

Коли ми пишемо $\mathbf{x} \leftarrow \mathcal{N}_\Sigma^{K_\mathbb{R}}$, ми маємо на увазі, що відповідний d-вимірний вектор

$\frac{1}{\sqrt{d}}\big(\Re\varphi_1(\mathbf{x}),\ \Im\varphi_1(\mathbf{x}),\ \ldots,\ \Re\varphi_{d/2}(\mathbf{x}),\ \Im\varphi_{d/2}(\mathbf{x})\big)$ має розподіл $\mathcal{N}_\Sigma$, де $\Re z, \Im z$ — це дійсна та уявна частини комплексного числа z.

Для ґратки $\mathcal{L} \subset \mathbb{R}^d$ дискретний гаусовий розподіл із параметрами $\mathbf{c} \in \mathbb{R}^d$ та Σ визначається для всіх $\mathbf{x} \in \mathcal{L}$ як

$$D_{\mathcal{L},\mathbf{c},\Sigma}(\mathbf{x}) = \frac{\rho_{\mathbf{c},\Sigma}(\mathbf{x})}{\rho_\Sigma(\mathcal{L} - \mathbf{c})}.$$

Якщо центр $\mathbf{c} = 0$, його часто опускають. Коли $\Sigma = s^2 I$ (скалярна матриця), використовують позначення $\mathcal{N}_s$ або $D_{\mathcal{L},s}$.

1.1.3 Загальний огляд схеми підпису SOLMAE

Як і в будь-якій схемі підпису нам потрібно ввести три алгоритми: генерації ключів (KeyGen), підпису (Sign) та верифікації (Verif).