УДК 004.056.55 **DOI:10.30837/rt.2024.2.217.07**

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

ОЦІНКА ВПЛИВУ АЛГЕБРАЇЧНОЇ СТРУКТУРИ Q-АРНИХ РЕШІТОК НА СКЛАДНІСТЬ КРИПТОАНАЛІЗУ ПРОБЛЕМ НА РЕШІТКАХ

Вступ

Криптографія на решітках стала однією з найбільш перспективних областей досліджень у сучасній криптографії [1]. Основною перевагою криптографії на решітках є її стійкість до квантових атак, що робить її особливо актуальною в контексті розвитку квантових технологій. Такі теоретико-числові проблеми як LWE (англ. Learning With Errors) [2], NTRU (англ. N-th Degree Truncated Polynomial Ring) [3] та SIS (англ. Shortest Integer Solution) [4], демонструють високий рівень безпеки і є основою для побудови таких криптографічних примітивів, як механізми інкапсуляції ключів та електронні підписи.

Для оцінки безпеки криптографічних схем на решітках часто використовується модель GSA (англ. Geometric Series Assumption) [5]. Ця модель базується на припущенні, що під час редукції решіток довжини векторів базису в процесі ортогоналізації утворюють геометричну прогресію. Модель GSA дозволяє спрощено оцінити складність розв'язання важливих задач на решітках, таких як LWE та NTRU.

Однак модель GSA є лише грубим наближенням і має свої обмеження [6]. Вона не завжди точно відображає поведінку реальних алгоритмів редукції решіток. Зокрема, GSA не враховує вплив структури q-арних решіток на довжини векторів базису. Тому результати, отримані за допомогою GSA, слід розглядати як орієнтовні оцінки, а не точні значення.

Для підвищення точності оцінки безпеки криптографічних схем на решітках необхідно розробляти більш комплексні моделі. Такі моделі повинні враховувати широкий спектр факторів, включаючи різні підходи до ортогоналізації, вплив випадкових флуктуацій, а також адаптивні стратегії атаки.

Одним з можливих варіантів є використання симуляторів редукції решіток [7 – 9]. Деякими авторами симулятори вже використовувалися для оцінки безпеки [10]. Проте, по-перше, більшість авторів використовували симулятор Чена–Нгуєна [7], який не враховує багато факторів. По-друге, у більшості випадків симулятор використовувався обмежено тільки для оцінки атак вкладення (англ. Primal USVP Attack) [11]. Іноді, наприклад для оцінки ДСТУ 8961:2019 [12], симулятор використовувався для оцінки гібридних атак. Проте, комплексної методики, що враховує вплив алгебраїчної структури q-арних решіток на процеси редукції решіток, досі не було запропоновано.

Ця робота присвячена комплексній оцінці впливу алгебраїчної структури q-арних решіток на складність криптоаналізу проблем LWE, SIS та NTRU для широкого спектру атак на криптографічні схеми на решітках.

1. Попередні відомості

Введемо необхідні позначення з теорії решіток, згідно з [13]. Решітка L з базисом B є множиною цілочисельних комбінацій лінійно незалежних векторів $b_1, \dots, b_n \in \mathbb{R}^n$:

$$L(b_1, \dots, b_n) = \{\sum_{i=1}^{n} x_i b_i | x_i \in \mathbb{Z}\}. \quad (1)$$

Довжиною вектора v є стандартна евклідова норма $\|v\| = \sqrt{v \cdot v}$, де операція $\cdot$ є скалярним добутком і для двох векторів $v = (v_1, \dots, v_n)$ і $w = (w_1, \dots, w_n)$ визначена як $v \cdot w = \sum_{i=1}^{n} v_i w_i$.

Для заданого базису $B = (b_1, \dots, b_n)$ ортогоналізований за Граммом–Шмідтом базис є $B^* = (b_1^*, \dots, b_n^*)$, де $b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{ij} b_j^*$ для $1 \le j < i \le n$, де $\mu_{ij} = (b_i \cdot b_j^*)/\|b_j^*\|^2$ –

коефіцієнти Грамма–Шмідта, $\|b_j^*\|$ – довжини векторів Грамма–Шмідта (ГШ-довжини). Сукупність ГШ-довжин будемо називати профілем базису.

Для решітки $L = L(B) \subseteq \mathbb{Z}^n$ з базисом $B \in \mathbb{Z}^{n\times k}$ фундаментальний паралелепіпед визначений як $P(B) = \{B \cdot x | x \in [0,1)^k\}$. Детермінант базису решітки є інваріантом і може бути обчислений як $\det(L) = \sqrt{\det(B^T B)} = \prod_{i=1}^{n} \|b_i^*\|$. При цьому, детермінант решітки чисельно дорівнює об'єму фундаментального паралелепіпеда $vol(L)$.

Ортогональна проєкція є відображення $\pi_i: \mathbb{R}^n \mapsto span(b_i, \dots, b_{i-1})^{\perp}$ для $i \in \{1, \dots, n\}$. Проективна решітка $L_{[i:j]}$ – решітка, яка задається наступним чином:

$$L_{[i:j]} = B_i = L(\pi_i(b_i), \pi_i(b_{i+1}), \dots, \pi(b_j)), \tag{2}$$

для $j \in \{i, i+1, \dots, n\}$.

У кожній решітці L існує найменший ненульовий вектор. $\lambda_1(L)$ – норма найменшого вектора. Проблема пошуку найменшого вектора (SVP) полягає у пошуку вектора довжини $\lambda_1(L)$.

Проблема LWE. Нехай $n, q > 0$ – цілі числа, χ – деякий розподіл ймовірностей над множиною цілих чисел $\mathbb{Z}$ та s – секретний вектор з рівномірного розподілу над $\mathbb{Z}_q^n$. $L_{s,\chi}$ є розподілом ймовірностей над $\mathbb{Z}_q^n \times \mathbb{Z}_q$, який отримується наступним чином. Обирається вектор $a \in \mathbb{Z}_q^n$ з рівномірного розподілу, значення помилки $e \in \mathbb{Z}_q$ з розподілу χ та повертається пара $(a, c) = (a, (a, a \cdot s + e) \in \mathbb{Z}_q^n \times \mathbb{Z}_q^n$. Проблема LWE (обчислювальна версія) полягає у тому, щоб для поліноміальної кількості пар (a, c) з розподілу $L_{s,\chi}$ знайти вектор s.

Проблема SIS. Нехай задано ціле число $q > 0$, матриця $A \in \mathbb{Z}_q^{n\times m}$, дійсне число B. Необхідно знайти ненульовий вектор $e \in \mathbb{Z}^m$, для якого виконується $A\mathrm{e} = 0\mathrm{mod}\mathrm{q}$ та $\|e\|_2 \leq B$.

Проблема NTRU. Нехай $n, q > 0$ – цілі числа і задано кільце R_q (на практиці – поле, проте у загальному випадку NTRU визначається для довільних кілець) поліномів степеня n над кільцем лишків за модулем q. Нехай $f, g \in R_q$ – поліноми з деякого розподілу χ і $h = g/f$. Проблема NTRU (обчислювальна версія) полягає у пошуку малих поліномів f, g для заданого полінома h.

2. Моделі базису решіток

Надалі вважаємо, що задана деяка (не обов'язково q-арна) d-вимірна решітка Λ з базисом $B = (b_1, \dots, b_d)$ та ГШ-профілем $B^* = (b_1^*, \dots, b_d^*)$.

В основі аналізу сучасних моделей редукції решіток лежить евристика Гауса [13], сутність якої полягає у тому, що кількість $|\Lambda \cap \Omega|$ точок решітки у довільному вимірюваному тілі $\Omega \subset \mathbb{R}^n$ складає $vol(\Omega)/vol(\Lambda)$. Використовуючи d-вимірний шар у якості вимірюваного тіла, для випадкової решітки $\Lambda \subset \mathbb{R}^d$, очікуваний найменший вектор, згідно з евристикою Гауса, можливо оцінити як

$$GH(\Lambda) = \left(\frac{vol(\Lambda)}{vol(\Omega)}\right)^{1/d} = \frac{\Gamma\left(1+\frac{d}{2}\right)}{\sqrt{\pi}} \cdot vol(\Lambda)^{\frac{1}{d}} \approx \sqrt{\frac{d}{2\pi e}} \cdot vol(\Lambda)^{1/d}. \tag{3}$$

Для зручності аналізу також введемо позначення $gh(d) = \sqrt{d/(2\pi e)}$ та $lgh(\Lambda) = \log_2 gh(\Lambda)$.

Практичні експерименти з алгоритмами LLL та BKZ показують [7 – 9], що $\|b_i^*\|/\|b_{i+1}^*\| \approx const$, якщо $d \gg \beta$. Модель GSA використовує це практичне спостереження та

евристику Гауса. Згідно з моделлю GSA, для довільної BKZ-β редукованої решітки з базисом B та об'ємом V має наступну форму:

$$log\|b_i^*\| = \frac{d-1-2i}{2} \cdot \log(\alpha_\beta) + \frac{1}{d} logV, \tag{4}$$

де $\alpha_\beta = gh(\beta)^{2/(\beta-1)}$.

У якості ілюстрації цього твердження на рис. 1 наведено профілі для 230-мірної випадкової q-арної решітки для $\beta = 2{,}10{,}20{,}30{,}40{,}50$.

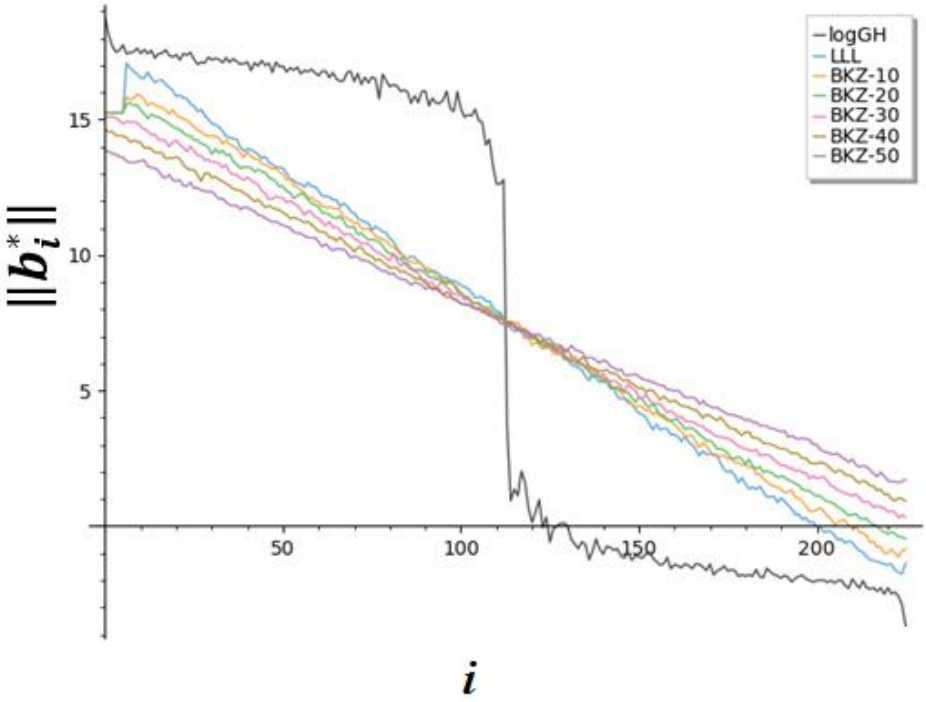

Рис. 1. Профілі 230-мірної q-арної решітки для $\beta = 2{,}10{,}20{,}30{,}40{,}50$.

Варто зауважити, що у більшості робіт замість α_β використовується інша метрика. Доволі зручною метрикою є так званий кореневий фактор Ерміта [6,7], який для базису B визначається як

$$\delta_\beta = (\|b_0\|/vol(\Lambda)^{1/d})^{1/d} \tag{5}$$

З міркувань вище випливає $\delta_\beta = \sqrt{\alpha_\beta}^{1-1/d}$. У роботі [7] запропоновано асимптотичну оцінку

$$\lim_{\beta\to\infty} \delta_\beta = \left(\frac{\beta}{2\pi e} \cdot (\pi\beta)^{\frac{1}{\beta}}\right)^{\frac{1}{2(\beta-1)}} \tag{6}$$

Модель GSA є корисним, проте доволі грубим наближенням форми базису редукованої решітки. По-перше, GSA не враховує того факту, що останній блок буде фактично HKZ редукованим. Оцінити форму HKZ базису можливо аналогічно:

$$h_i = lgh(d-i) - \frac{1}{d-i}\sum_{j<i} h_j \tag{7}$$

Узагальнюючи для довільного базису:

$$\begin{aligned} l_i &= \frac{d-1-2i}{2} \cdot log\alpha_\beta + s, \text{ якщо } 0 \le i \le d-\beta \\ l_i &= h_{i-(d-\beta)} + l_{d-\beta} - h_0, \text{ якщо } d-\beta \le i \le d, \end{aligned} \tag{8}$$

де s є нормуючим фактором, таким, що виконується $\sum l_i = logV$.

Окремо варто розглянути ефекти, що виникають під час редукції q-арних решіток. Такі решітки містять вектор (q, 0, …, 0) та усі його перестановки. Типовою формою базису таких решіток є так звана «Z-форма»:

Приклад Z-форми наведено на рис. 2.

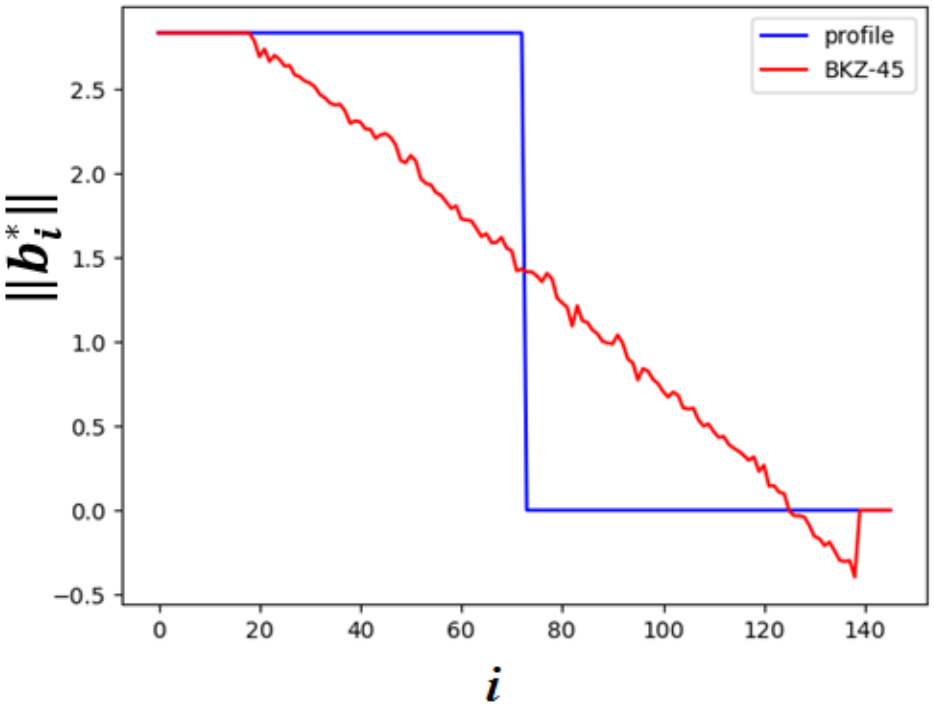

Рис. 2. Z-форма базису решітки

Одним з підходів для моделювання такого базису є модифікація евристики GSA. Такий підхід, зокрема, був популяризований авторами ЕП Crystals-Dilithium. Модифікована евристика GSA (модель ZGSA [6]) визначена наступним чином:

$$\|b_i^*\| = \begin{cases} q, \text{якщо } i \le n-m \\ \sqrt{q} \cdot \alpha_\beta^{\frac{(2d-1-2i)}{2}}, \text{якщо } n-m < i < n+m-1, \\ 1, \text{ якщо } i \ge n+m-1 \end{cases} \quad (9)$$

де $\alpha_\beta = gh(\beta)^{2/(\beta-1)}$ і $m = \frac{1}{2} + \frac{lnq}{2ln\alpha_\beta}$.

Інший підхід базується на основі симуляції. Ідея симуляції ГШ-профілю була запропонована у роботі [7] (Симулятор Чена–Нгуєна). Симулятор замість запуску SVP-оракула визначає очікувану довжину нового вектора за допомогою евристики Гауса. Особливістю симулятора Чена–Нгуєна було використання предобчислених даних для моделювання останнього блоку. У роботі [8] був зала запропонована нова рандомізована версія симулятора Чена–Нгуєна, у якій враховувалася ймовірнісна природа евристики Гауса. Замість точного значення евристики Гауса використовувалися випадкові зміні. Це дало більшу точність симуляції для перших векторів в ГШ-профілі. Втім, для q-арних решіток моделювати «Z-форму» не вдавалося. В роботі [9] запропонований варіант симулятора (симулятор Альбрехта–Лі), що враховує «Z-форму» q-арних решіток.

Для того щоб порівняти якість роботи симуляторів, було проведено ряд експериментів. Для решіток 120, 146, 170 і $q = 17{,}257$ було проведено симуляцію для розмірів блоків 45,50, 55, 60. Для кожного випадку за адаптованою для базисів було обчислено середньоквадратичну похибку. Усереднені значення помилок наведено на рис. 3, 4.

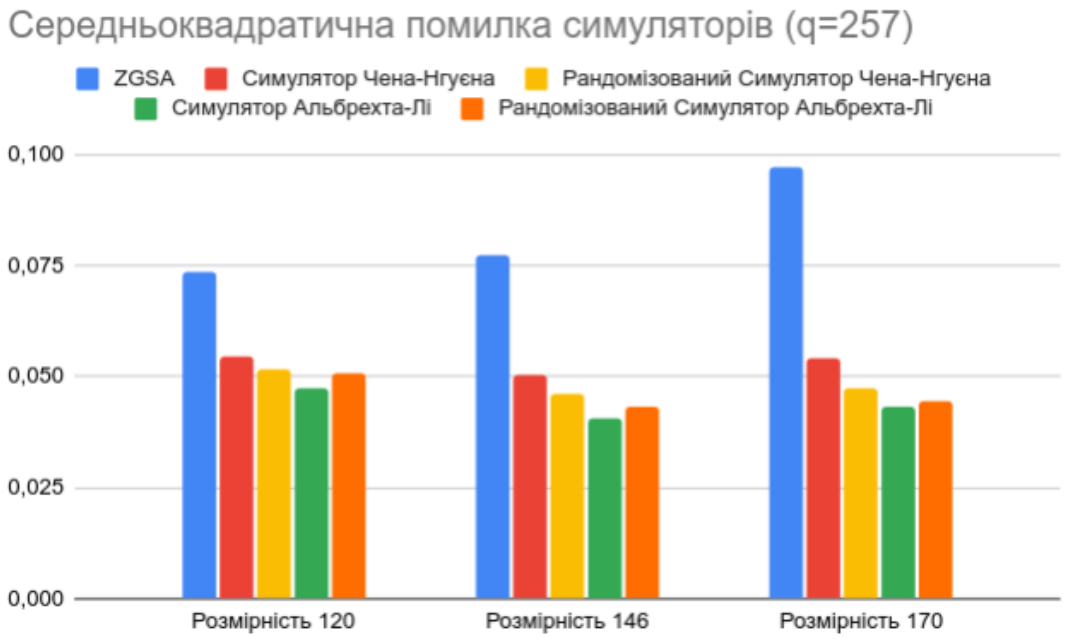

Рис. 3. Середньоквадратичні помилки симуляторів для $q = 256$

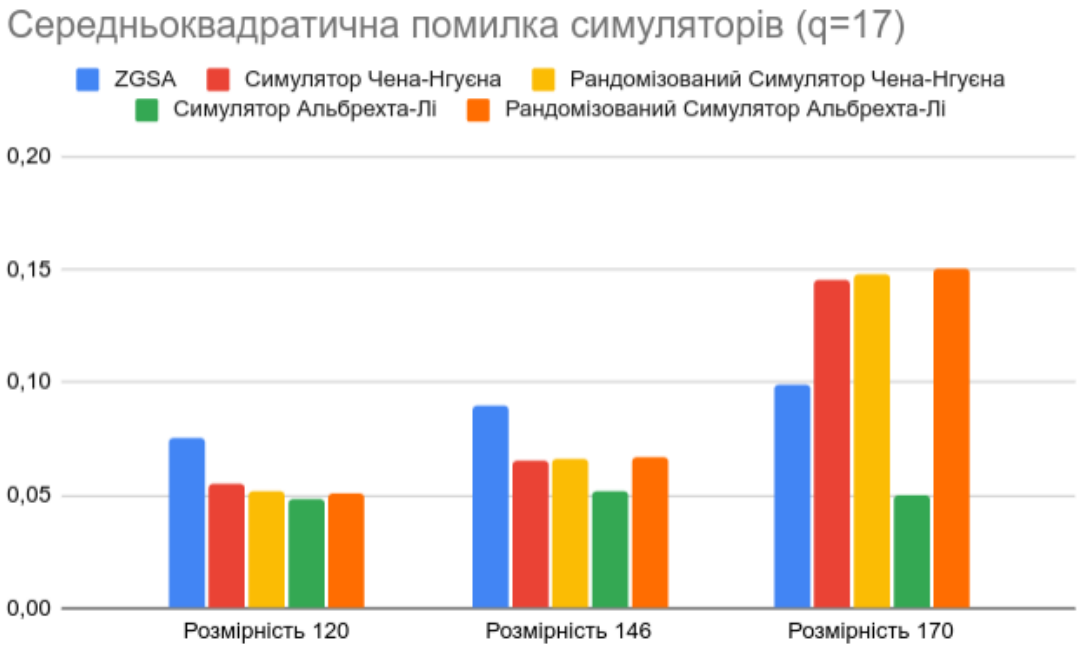

Рис. 4. Середньоквадратичні помилки симуляторів для $q = 17$

З рис. 3, 4 видно, що модель ZGSA доволі непогано себе показує для q=17, проте для q=257 значно програє симуляторам. Симулятор Альбрехта–Лі в обох випадках показує найменшу середньоквадратичну помилку, тож має сенс використовувати його для моделювання редукції решіток. Цікаво, що рандомізована версія симулятора Альбрехта–Лі показує відносно погані результати для q=17 для розмірності 170. Це пов'язано з тим, що через рандомізацію для цієї розмірності якість передбачення Z-форми значно погіршується. На рис. 5 вказано конкретний приклад такої ситуації.

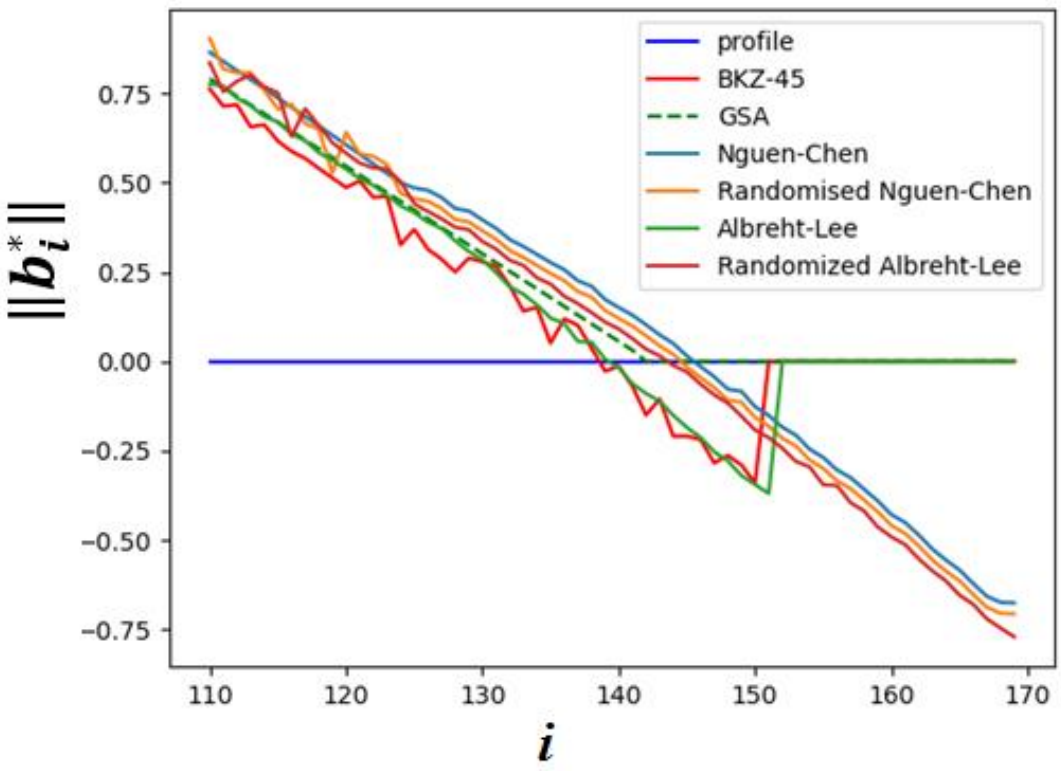

Рис. 5. Приклад поганого передбачення для рандомізованого симулятора Альбрехта–Лі

Тож, найкращу якість передбачення має детермінований симулятор Альбрехта–Лі. Надалі він буде використовуватися для моделювання редукції базису решітки.

3. Вплив розріджених решіток

NTRU решітки окрім q-арної структури мають додаткові алгебраїчні особливості. Особливістю NTRU решіток є велика кількість малих векторів. Зафіксуємо деяке поле $\mathbb{Z}_q[X]/(\phi(X))$ для деякого незвідного полінома $\phi, \deg(\phi) = n$. Якщо $h = g \cdot f^{-1}(mod q)(mod \phi(X))$ для деяких f, g, то решітка розмірності $2n$ з базисом

$$B_{NTRU} = \begin{pmatrix} qI_n & rot(h) \\ 0 & I_n \end{pmatrix} \tag{10}$$

міститиме вектори $(g, f), (x \cdot g, x \cdot f), \dots, (x^{n-1} \cdot g, x^{n-1} \cdot f)$. Ці вектори формують підрешітку розмірності n з базисом

$$B_{NTRU}^{dense} = \begin{pmatrix} rot(g) \\ rot(f) \end{pmatrix} \tag{11}$$

У криптографічному випадку поліноми f, g є малими, тому підрешітка з базисом (11) міститиме велику кількість векторів, що значно менші за евристику Гауса. Знаходження векторів на підрешітці (11) під час редукції решітки дуже швидко призводить до знаходження інших векторів підрешітки, що розбиває редукцію базису (10) на дві незалежні частини і для багатьох параметрів призводить до швидкого знаходження f, g. Приклад такої ситуації наведено на рис. 6.

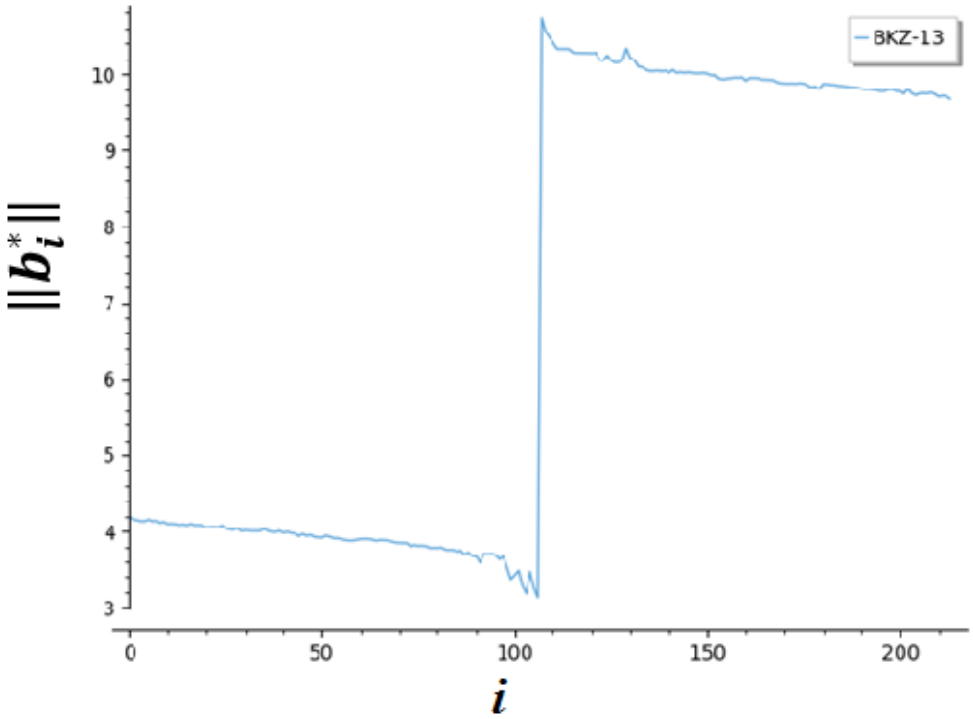

Рис. 6. Перехід на розріджену решітку. Кожна з підрешіток під час редукції не залежить від іншої, що зменшує складність редукції

Вперше ця особливість NTRU решіток була помічена у контексті алгебраїчних атак. Зокрема, так звані атаки на підполе [14]. Проте, у роботі [15] було показано, що розріджені підрешітки призводять до пришвидшення редукції решіток без алгебраїчних технік, що використовувалися в попередніх атаках.

Фактично, при криптоаналізі NTRU решіток є цікавими дві події:

Відновлення таємного ключа – вектор (g, f) буде міститися у базисі решітки.

Потрапляння на розріджену підрешітку – деякий вектор (значно довший за (g, f)) з розрідженої підрешітки буде міститися у базисі

У роботі [15] був отриманий наступний результат. Нехай Λ_{NTRU} – NTRU-решітка розмірності $2n$ з розрідженою решіткою $\Lambda_{NTRU}^{dense} \subset \Lambda_{NTRU}$. Якщо Λ_{NTRU} має базис, що має Z-форму, то під час BKZ-β редукції буде знайдено вектор з розрідженої решітки (що значно більший за таємний ключ), якщо

$$\pi_{n+k-\beta}(v) < \left\| b_{n+k-\beta}^* \right\| \tag{12}$$

де v – найменший вектор на решітці $\Lambda_{proj}^{dense} = \Lambda(\pi_0(b_0), \dots, \pi_0(b_{n+k-1})) \cap \Lambda_{NTRU}^{dense}$.

4. Класифікація та аналіз відомих атак

Відомі атаки на проблему LWE можливо поділити на наступні класи:

- Комбінаторні атаки [16, 17];
- Алгебраїчні атаки [14, 18, 19];
- Атаки декодування [20];
- Атаки розпізнавання [21];
- Атаки вкладення [5];
- Гібридні атаки [22].

До комбінаторних атак належать атака повного перебору та атака MITM (англ. Meet In The Middle) [16]. Зазвичай MITM використовується не самостійно, а як складова більш комплексних гібридних атак. Також до комбінаторних атак можливо віднести атаку BKW [17].

До алгебраїчних атак на LWE відносять атаку Arora-Ge [18], сутність якої полягає у зведенні проблеми LWE до вирішення системи нелінійних рівнянь. Також, якщо розглядати проблему LWE на ідеальних решітках, то існує ряд квантових атак [19], що використовують структуру ідеалів для значного пришвидшення. Проте, такі атаки як правило працюють лише для не криптографічних випадків. Для NTRU алгебраїчною атакою є атака на підрешітку, що була розглянута у розд. 3.

Сутність атак декодування полягає у зведенні проблеми LWE або NTRU до проблеми CVP. Атаки такого роду вимагають побудови та редукції базису решітки таким чином, щоб було можливо вирішити проблему CVP для шуканого таємного вектора.

Атаки вкладення є одними з найбільш ефективних атак на LWE та NTRU. Сутність таких атак полягає у побудові решіток спеціального вигляду, найменший вектор яких містить шуканий секрет. Такі атаки ще називають атаками вкладення, або первинними (англ. Primal) атаками.

Атаки розпізнавання часто називають дуальними атаками через те, що вони зводяться до редукції дуальних (відносно атак вкладення) решіток. У таких атаках використовуються статистичні методи аналізу. Перед криптоаналітиком стоїть задача відрізнення двох розподілів. У поєднанні з комбінаторними методами дуальні атаки можуть давати гарні результати для проблеми LWE. Також їх можливо використовувати для вирішення проблеми SIS.

Гібридні атаки поєднують комбінаторні методи криптоаналізу з атаками вкладення або атаками розпізнавання (гібридні дуальні атаки). Такі атаки при використанні розріджених секретів часто є найкращими для багатьох криптографічних систем.

Розглянемо детально кожен клас атак для оцінки впливу моделей редукції решіток на безпеку криптографічних перетворень.

5. Атаки вкладення

Атака ґрунтується на тому факті, що решітка

$$\Lambda_\omega = \left(x \in \mathbb{Z}^{m+n+1} : \left(I_m \left|\frac{1}{\omega}A\right| - \frac{1}{\omega}b\right)x = 0 mod q\right) \tag{13}$$

містить найменший вектор $v = \lambda_1(\Lambda_\omega) = (e|\omega \cdot s|\omega)$, де ω – параметр масштабування. Значення цього вектора задовільнять LWE рівнянню. Параметр масштабування може бути корисним у випадку, якщо розподіли e та s відрізняються. Типовим значенням є $\omega = \sigma_e/\sigma_s$, де σ_e, σ_s є середньоквадратичними відхиленнями розподілів ймовірностей векторів e, s.

Для оцінки складності пошуку вектора $\lambda_1(\Lambda_\omega)$ не можна застосовувати стандартні припущення на основі Евристики Гауса, оскільки вектор $\lambda_1(\Lambda_\omega)$ набагато менший за $GH(\dim(\Lambda_\omega))$ для типових криптографічних параметрів. На практиці себе добре зарекомендував [5, 6] критерій

$$\left\|\pi_{d-\beta+1}(v)\right\| \le \left\|b^*_{d-\beta+1}\right\|. \tag{14}$$

Ідея, що лежить за критерієм (14), полягає у наступному. Малі вектори у алгоритмі BKZ знаходяться за допомогою SVP-оракула і далі за допомогою алгоритму LLL (більш конкретно – за допомогою кроку редукції за розміром) ці малі вектори вставляються в новий базис. Якщо задано найменше β, для якого виконується (14), то, скоріш за все, потрібний вектор буде знайдено під час останнього виклику SVP-оракула. Знайдений вектор буде вставлений у базис тільки у тому випадку, якщо (14) виконується, за визначенням алгоритму BKZ.

У роботі [23] було доведено, що ймовірність відновлення таємного вектора, якщо виконується вимога (14), складає

$$p = \sum_{i=1}^{d-\beta} \Pr\left[\|\pi_i(v)\| < \min\{\|\pi_i(v) + b_i^*\|, \|\pi_i(v) - b_i^*\|\}\right]. \tag{15}$$

При $\beta > 50$ ймовірність (15) швидко наближається до 1, тож для криптографічних параметрів можливо вважати, що ймовірність відновлення таємного вектора є 1, якщо виконується умова (14). На малих розмірностях іноді таємний вектор може відновлюватися за менших значень β. Це явище пояснюється геометрією решіток [23] і на великих розмірностях не спостерігається, тому при подальшому аналізі ігнорується.

Якщо припустити, що таємний вектор є однорідним (для криптографічних параметрів це є природнім припущенням), то $\left\|\pi_{d-\beta+1}(v)\right\| \approx \sqrt{\beta/d}\|v\|$. У свою чергу, незалежно від розподілу вектору v, з центральної граничної теореми маємо: $\|v\| \approx \sigma\sqrt{d}$. Тож, $\left\|\pi_{d-\beta+1}(v)\right\| \approx \sqrt{\beta}\sigma$, де σ – математичне очікування для компонентів вектора v. Цей факт може бути використаним для перевірки формули (14) на реальних параметрах.

Обчислення правої частини нерівності залежить від моделі редукції решіток. Якщо використовується модель GSA, то

$$\left\|b^*_{d-\beta+1}\right\| \approx \delta_\beta^{2\beta-d} \cdot vol(\Lambda_\omega)^{\frac{1}{d}} = \delta_\beta^{2\beta-d} \cdot q^{\frac{m}{d}}\omega^{(n+1)/d} \tag{16}$$

У випадку використання симуляторів $\left\|b^*_{d-\beta+1}\right\|$ має бути обчислено експериментально.

Варто зауважити, що складність атаки залежить не монотонно від значення m. У роботі [21] доведено, що оптимальним значенням є

$$m_{opt} = \left\lceil \sqrt{\frac{(n+1)(logq-log\omega)}{log\delta_\beta}} - (n+1) \right\rceil \tag{17}$$

Таким чином, оцінка атаки вкладення зводяться до знаходження найменшого β, для якого виконується (14). При цьому мають бути задані:

- Параметри решітки (n, q, σ)
- Модель редукції решіток, що визначає $\left\|b^*_{d-\beta+1}\right\|$
- Модель часу роботи редукції

Модель часу роботи редукції решіток слугує для перетворення оптимальних параметрів редукції у конкретну оцінку безпеки, тому при дослідженні впливу моделей редукції решіток на безпеку, її можливо не задавати, а досліджувати безпосередньо оптимальні параметри атаки.

На рис. 7 наведено результати моделювання атаки вкладення з використанням моделі GSA та симулятора Альбрехта–Лі для $n = 256$ при $\sigma = \{1.1, 1.3, 1.5, 1.8, 2.1\}$. З рис. 7 видно, що при збільшенні параметра q зменшується оптимальне для атаки значення β, що є логічним, враховуючи формулу (16): при збільшенні q права частина рівняння (14) збільшуватиметься, у той час як ліва частина залишатиметься такою ж. Втім, графік для симуляторів має дві ключові відмінності. Відрізняється сила впливу параметра σ на оптимальне значення β. При використанні моделі GSA спостерігається трохи більший розмах між випадками $\sigma = 1.1$ та $\sigma = 2.1$ на більшій частині досліджуваного простору параметрів. При малих значеннях q це може суттєво впливати на значення β.

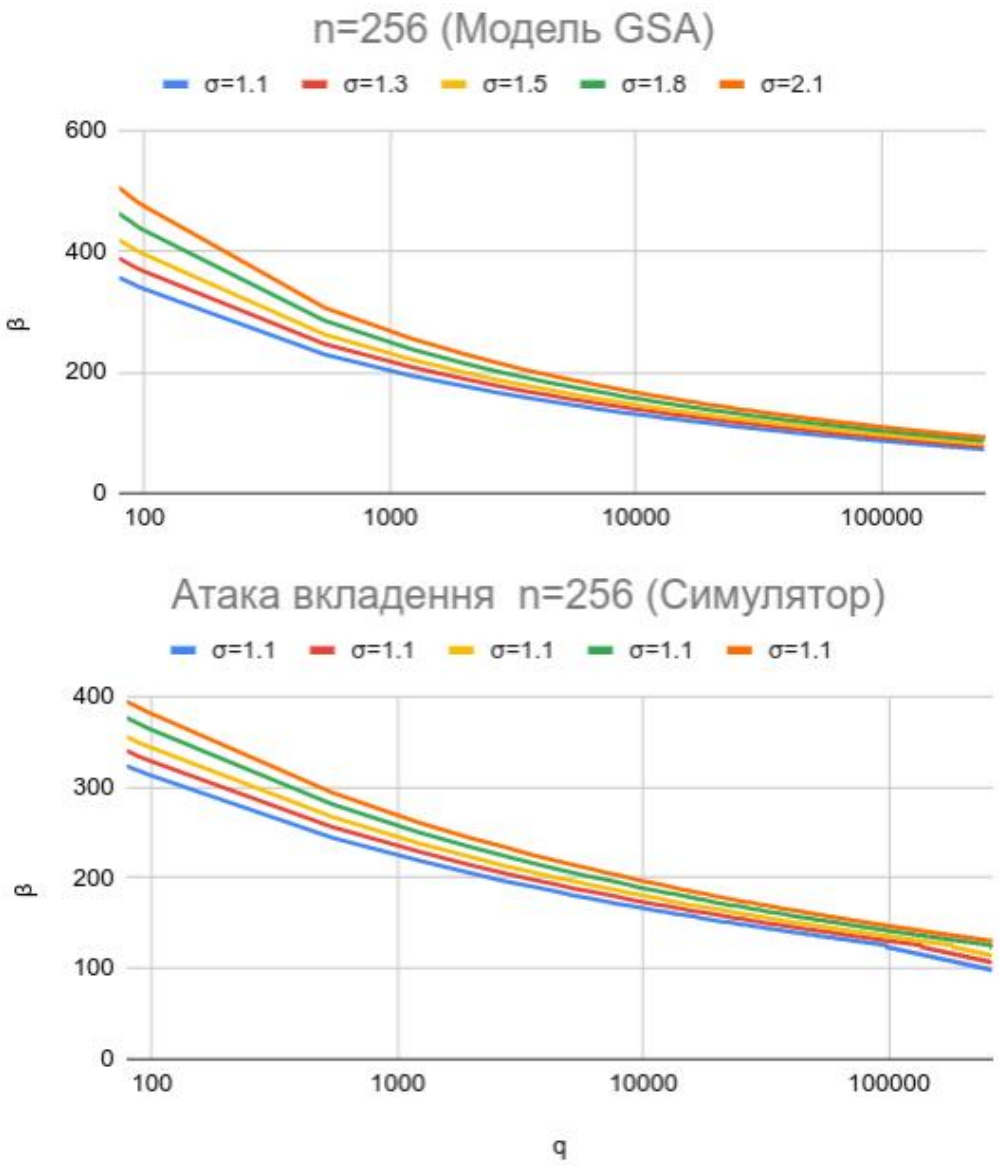

Рис. 7. Результати моделювання атаки вкладення

Для більш наглядної демонстрації різниці між симулятором та моделлю GSA на рис. 8 наведено накладені один на одного графіки з рис. 7. З рис. 8 видно, що на малих значеннях q симулятор дає менші значення параметра β, у порівнянні з моделлю GSA. У той же час, для великих значень q симулятор дає більші значення β, що свідчить про те, що модель GSA дещо занижує рівень безпеки. Отримані свідчення можливо пояснити тим, що останній блок у профілі решітки буде HKZ редукованим, а отже $\left\|b^*_{d-\beta+1}\right\|$ буде мати трохи більше значення, ніж передбачене GSA значення. Оскільки симулятор враховує це явище, то данні на рис. 8 виглядають цілком природніми.

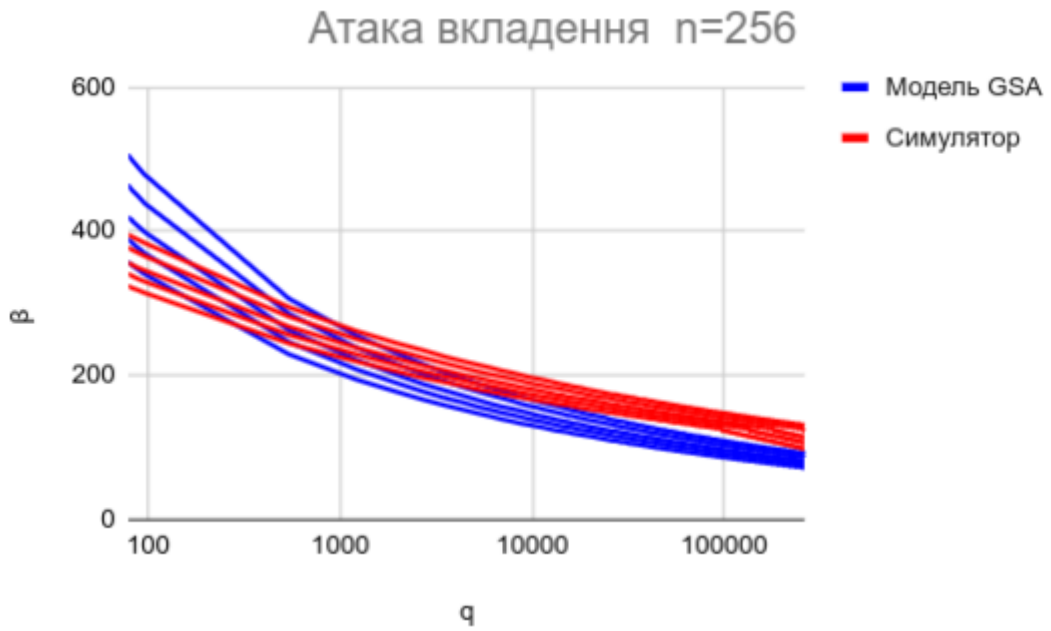

Рис. 8. Порівняння моделі GSA та симулятора Альбрехта–Лі

При збільшенні параметра n результати моделювання виглядають схожим чином і для них зберігаються усі описані явища. На рис. 9 наведено результати моделювання для $n = 256,512,1024,2048$ при фіксованому $\sigma = 1.1$.

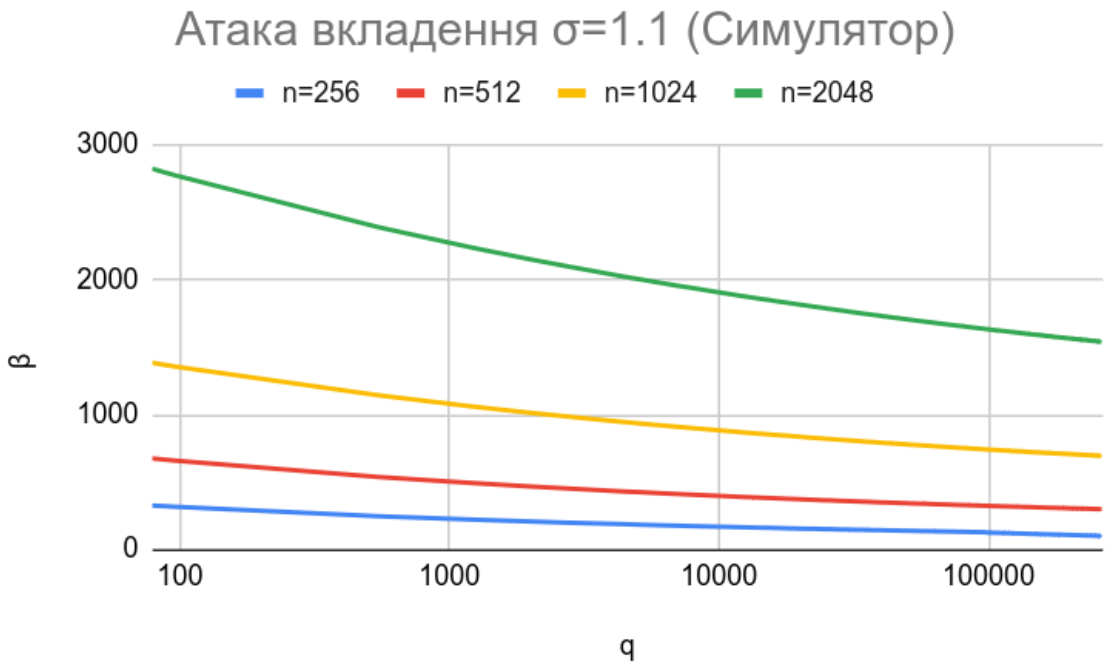

Рис. 9. Результати моделювання атаки вкладення
для $n = 256,512,1024,2048$ при фіксованому $\sigma = 1.1$

З рис. 9 видно, що збільшення n дає лінійний приріст значення β, з чого випливає стратегія пошуку оптимальних загальносистемних параметрів: зафіксувати значення n, що дає близьке до необхідного рівня безпеки значення і підлаштовувати рівень безпеки змінюючи параметри q, σ.

Якщо решітка має розріджену підрешітку, то необхідно додатково використовувати формулу (12) для урахування можливості переходу на розріджену підрешітку. Оскільки формула (12) вже враховує Z-форму базису, то її не має сенсу застосовувати в моделі GSA. Для NTRU решіток починаючи з $q \approx 0.0038 \cdot n^{2.484}$ відбуватиметься перехід на розріджену решітку. При обчисленні безпеки параметрів це необхідно враховувати.

6. Атаки декодування

Атака декодування зводить проблему LWE до задачі знаходження найближчого вектора. Для цього будується решітка

$$\Lambda = \{x \in \mathbb{Z}^m | x = A \cdot s \bmod q\} \tag{18}$$

і для вектора $t = A \cdot s + e$ вирішується задача пошуку найближчого вектора $v = A \cdot s$, знаючи який можливо легко відновити (s, e). Щоб знайти найближчий вектор необхідно провести редукцію базису (18). У загальному випадку складність атаки можливо знайти за формулою

$$(T_{red} + T_{cvp})/p_{succ} \tag{19}$$

де T_{red} – час редукції базису решітки (18), T_{cvp} – час алгоритму пошуку найближчого вектора, p_{succ} – ймовірність вдалого завершення атаки.

У якості алгоритму пошуку найближчого вектора, як правило, використовується алгоритм Бабаї та його узагальнення. Алгоритм Бабаї гарантує [22], що $v - t \in P_{\frac{1}{2}}(B^*)$, тож для цього випадку необхідною умовою вдалого завершення атаки є $e \in P_{\frac{1}{2}}(B^*)$.

У випадку нормального розподілу помилки, у роботі [20] запропонована наступна оцінка:

$$p_{succ} = \Pr\left[e \in P_{\frac{1}{2}}(B^*)\right] = \prod_{i=1}^{m} erf\left(\frac{\|b_i^*\|\sqrt{\pi}}{2s}\right) \tag{20}$$

Для класичного алгоритму Бабаї T_{cvp} є поліноміальним і може не враховуватися. Проте, використання більш складних алгоритмів пошуку найближчого вектора, що працюють за субекспоненційний час, може зменшити (19). Такі алгоритми, як правило, тісно повязані з SVP оракулами. Ідеї, що використовуються для побудови SVP оракулів, також можуть бути адаптованими для побудови алгоритмів вирішення задачі CVP, як як це було показано у роботі [20]. Сутність ідеї полягає у тому, щоб у алгоритмі Бабаї обчислювати не тільки найоптимальніші координати $c_0, \dots, c_{d-1}$, а для кожної координати c_i перебирати d_i найоптимальніших значень. Тоді, складність алгоритму пошуку найближчого вектора при використанні найпростішої стратегії перебору складатиме $O(\prod_i d_i)$, яка вже буде не поліноміальною. Тоді, оцінка (19) буде мінімізуватися, коли $T_{red} \approx T_{cvp}$. Ймовірність p_{succ} відповідно складатиме

$$p_{succ} = \prod_{i=1}^{m} p_{succ}^i = \prod_{i=1}^{m} erf\left(\frac{d_i\|b_i^*\|\sqrt{\pi}}{2s}\right) \tag{21}$$

Питання вибору значень d_i в літературі є малодослідженим. Якщо використовувати модель GSA, то значення $\|b_i^*\|$ будуть розподілені за експоненціальним розподілом. Значення d_i, що мають відмінне від одиниці значення, будуть згруповані у хвості профіля решітки. Проте, оскільки у q-арних решіток останні значення $\|b_i^*\|$ сильно відхиляються від GSA і $\|b_i^*\| \approx 1$, що повинно зменшувати відповідні значення d_i для цих векторів, а отже і зменшувати відповідне значення T_{cvp}.

Для пошуку відповідних значень d_i зафіксуємо мінімальні ймовірність успішного виконання атаки p_0. Стратегія пошуку значень d_i випливає з міркувань, що існує така ймовірність p_{avg}, що

$$p_0 \le \prod_{i=1}^{m} p_{succ}^{i} < \left(p_{avg}\right)^{m} \tag{22}$$

Зрозуміло, що мінімальне таке значення є $p_{avg} = (p_0)^{1/m}$. Тоді, якщо кожне p_{succ}^{i} буде більшим за p_{avg}, то буде виконуватися $p_0 \le p_{succ}$. Звідси, маємо

$$p_{succ}^{i} = erf\left(\frac{d_i \|b_i^*\|\sqrt{\pi}}{2s}\right) \le p_{avg} \Rightarrow$$
$$d_i \le \frac{erfinv(p_{avg})\cdot 2s}{\|b_i^*\|\sqrt{\pi}} \tag{23}$$

На рис. 10 зображена залежність p_{avg} від p_0 для різних значень параметра m.

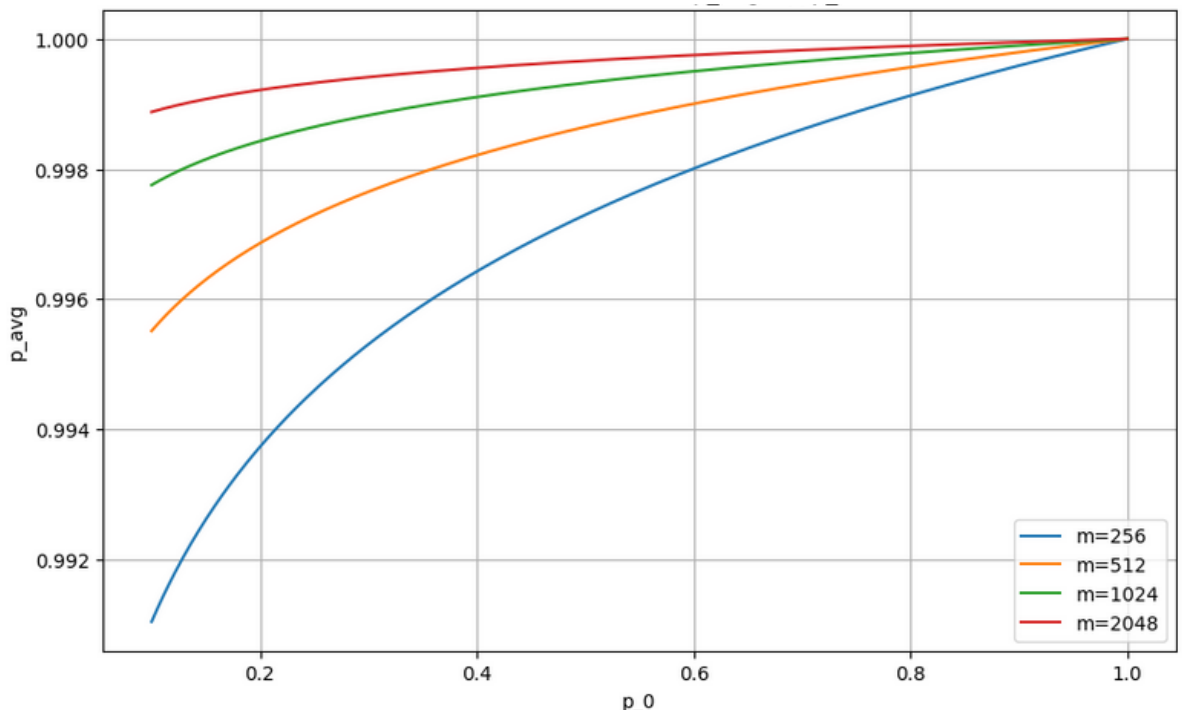

Рис. 10. залежність p_{avg} від p_0 для різних значень параметра m.

З рис. 10 видно, що для типових значень параметра m значення параметра p_{avg}, лежить близько до 1, тобто вплив ймовірності p_0 на значення d_i є не значним.

Тож, для атаки декодування мають бути задані

- Модель редукції решіток, що визначає профіль решітки
- Модель часу роботи редукції
- Модель часу роботи алгоритму CVP

У межах дослідження було проведено моделювання атаки декодування для моделі GSA та симулятора Альбрехта–Лі для розмірностей $N = 256,512,1024,2048$ та значень параметра $\sigma = 1.1,1.3,1.5$. Результати моделювання для розмірності 512 наведені на рис. 11.

З рис. 11 видно, що вартість атаки з використанням симулятора Альбрехта–Лі є вищою, проте такої великої переваги, як в атаках вкладення не має. Це пояснюється тим, що вартість атак вкладення залежить лише від значення $\left\|b_{d-\beta+1}^{*}\right\|$, у той час, як вартість атак декодування залежить цілком від всього профіля редукованої решітки. Також видно, що складність етапу редукції решітки та етапу пошуку найближчого вектора хоч і наближаться один до од-

ного, проте не дорівнюють один одному, тобто мінімум формули (19) не досягається через дискретність параметрів.

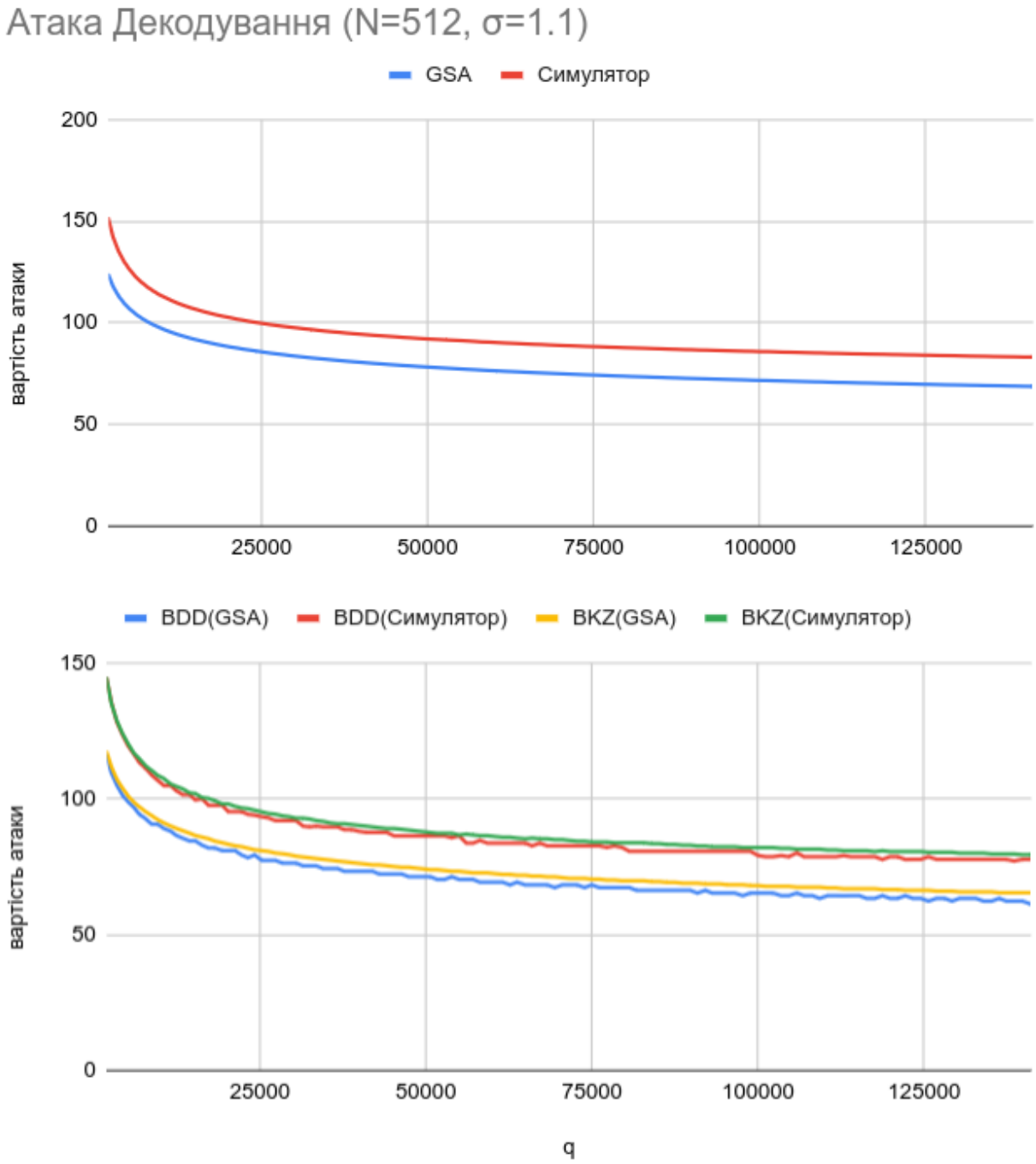

Рис. 11. Результати моделювання атаки декодування для $N = 512, \sigma = 1.1$

На рис. 12 показано вплив збільшення параметра N на складність атак декодування.

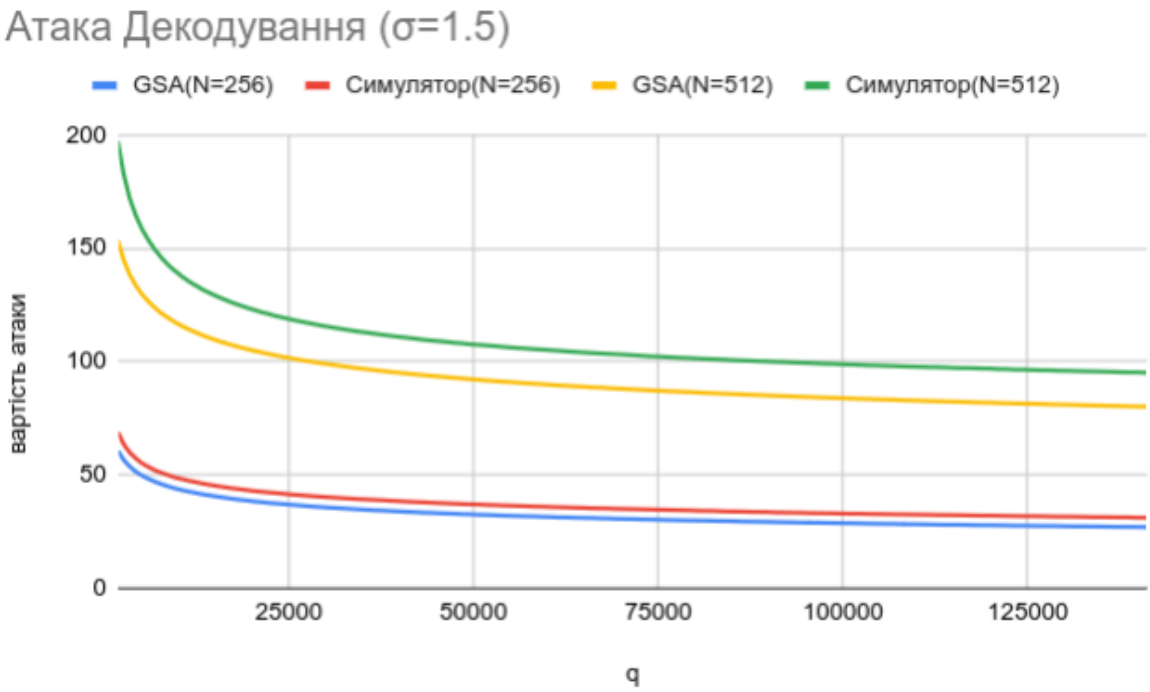

Рис. 12. Вплив параметра N на складність атак декодування

Як видно з рис. 12, збільшення параметра N вдвічі збільшує складність атаки приблизно вдвічі. Цікаво, що при цьому зростає вплив симулятора на складність атаки, чого так явно не спостерігалося для атак вкладення, що , знов ж таки, пояснюється тим, що форма профіля базису в атаках декодування впливає сильніше на складність атаки.

На рис. 13 показано вплив параметра σ на вартість атак декодування.

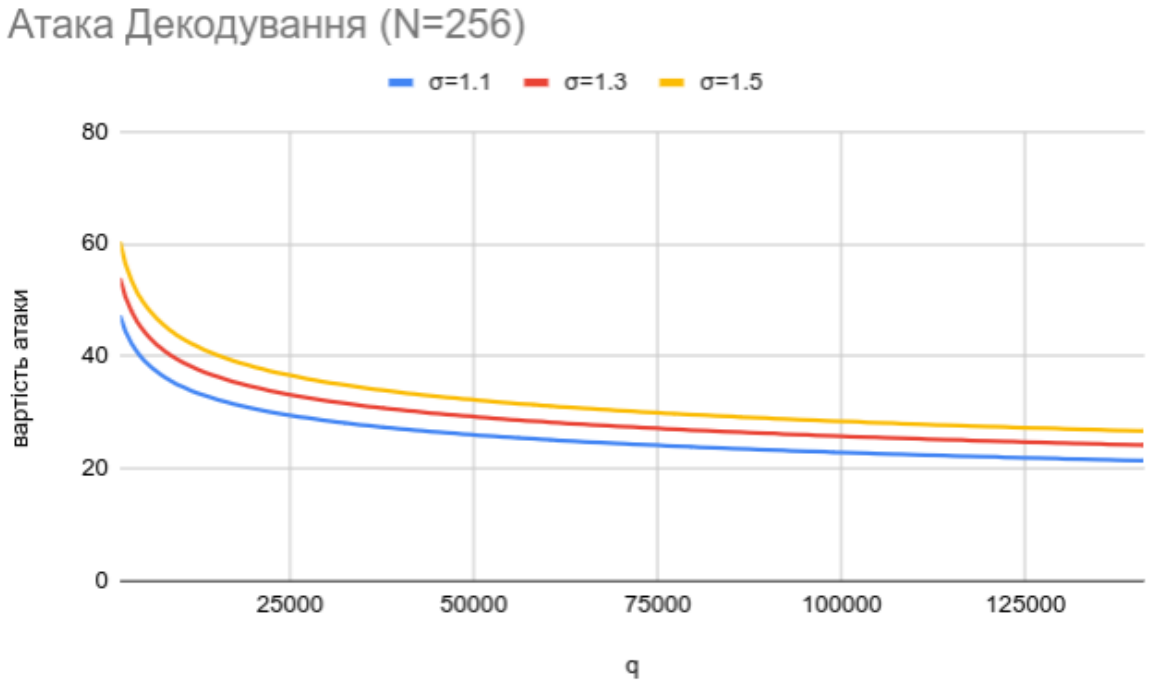

Рис. 13. Вплив параметра σ на вартість атак декодування

Великої різниці у впливі параметра σ при використанні моделі GSA та симулятору не має. Як і в атаках вкладення, параметр σ можливо використовувати для уточнення параметрів безпеки.

На рис. 14 наведено порівняння складності атак вкладення та декодування.

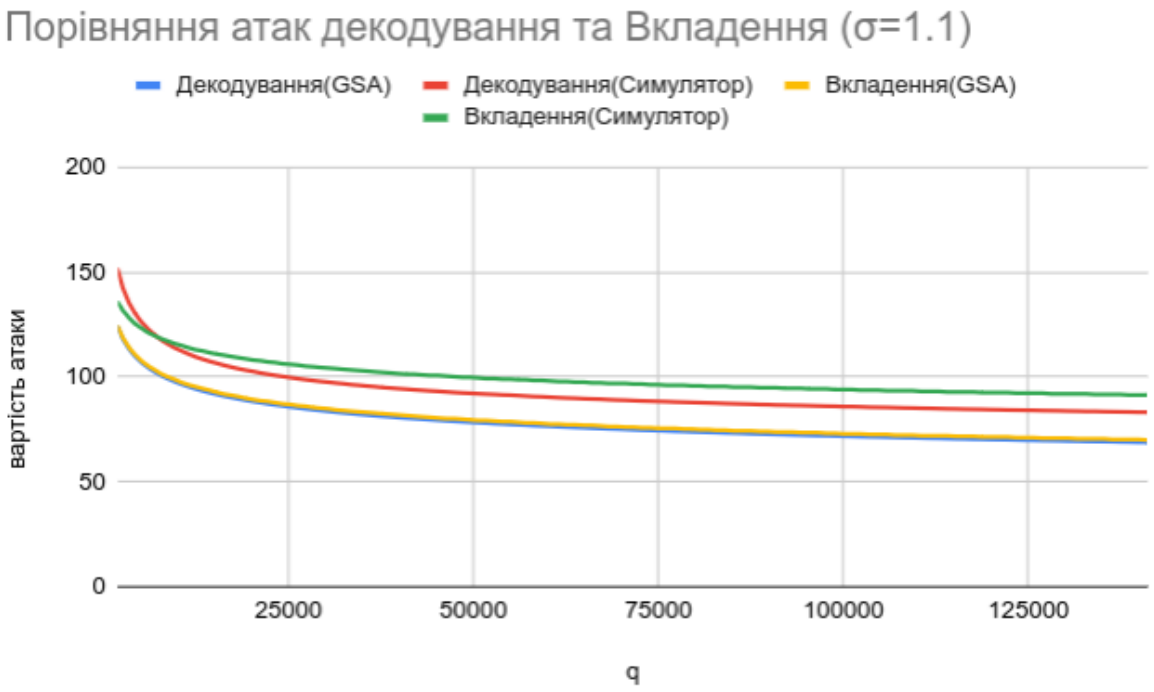

Рис. 14. порівняння атак вкладення та декодування

З рис. 14 можливо зробити декілька висновків. При використанні моделі GSA складність атак декодування та вкладення є майже однаковою. Фактично, різниця настільки не суттєва, що їх вартість можливо вважати однаковою. Проте, при використанні симуляторів різниця між атаками вкладення та декодування стає помітною. Для переважної частини параметрів атака декодування перевершує атаку вкладення, проте на малих значеннях параметра q атака вкладення все ж стає кращою. Різниця є достатньо малою, проте при виборі параметрів, все ж, її варто враховувати. Тож, при оцінці безпеки не можна нехтувати атаками декодування.

7. Атаки розпізнавання

Атаки розпізнавання є статистичними атаками, у яких супротивник намагається відрізнити пари $(A, t = A^T s + e)$ від пари (A, b) з рівномірного розподілу. Це можливо зробити, якщо відомо деякий малий вектор v, для якого виконується $Av = 0 mod q$ (тобто він лежить на дуальній решітці $\Lambda_q^{\perp}(A^T)$). Для вектора $t = A^T s + e$ скалярний добуток $\langle v, t \rangle mod q$ буде мати нормальний розподіл, оскільки $\langle v, t \rangle = vA^T s + \langle v, e \rangle mod q = \langle v, e \rangle$. Для вектору b відповідний розподіл буде рівномірним.

Атаки розпізнавання у багатьох моделях безпеки, наприклад у Crystals-Dilithium, чи New-Hope, аналізуються чисто як атаки, що дозволяють відрізнити розподіл LWE від рівномірного розподілу. Звичайно, факт відрізнення LWE розподілу від рівномірного руйнує усі докази безпеки у таких моделях безпеки, як IND-CCA для схем асиметричного шифрування, чи IND-CMA для електронних підписів, проте в реальному світі зловмисників цікавить саме відновлення таємного ключа, а не лише відрізнення розподілів. Перетворення атаки розрізнення на атаку відновлення ключів потребує деяких додаткових обчислювальних ресурсів, тому такі оцінки є дещо заниженими. Враховуючи, що навіть такі занижені оцінки є гіршими за атаки вкладення та декодування, то уточнені оцінки будуть ще гіршими. Тож, у моделі безпеки їх можливо не враховувати.

8. Гібридні атаки

Основна ідея гібридної атаки ґрунтується на тому, що якщо q – просте число, то для будь-якої вимірної -арної решітки Λ базис можливо представити у вигляді

$$B = \begin{pmatrix} B_1 & B_2 \\ 0 & I_r \end{pmatrix} \in \mathbb{Z}^{n \times n}, \tag{24}$$

де $0 < r < n$, $B_1 \in \mathbb{Z}^{(n-r)\times(n-r)}$, $B_2 \in \mathbb{Z}^{(n-r)\times r}$.

Використовуючи структурованість базиса, довільний вектор $v \in \Lambda$ можливо представити як конкатенацію векторів меншої розмірності:

$$v = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = B \begin{pmatrix} x \\ v_2 \end{pmatrix} = \begin{pmatrix} B_1 x + B_2 v \\ v_2 \end{pmatrix} \tag{25}$$

$$v_1 \in \mathbb{Z}^{(n-r)}, v_2 \in \mathbb{Z}^r$$

для деякого $x \in \mathbb{Z}^{(n-r)}$.

З формули (25) маємо рівняння $B_2 v_2 = -B_1 x + v_1$. Оскільки v_1 є малим вектором, то вектор $B_2 v_2$ знаходиться близько до решітки $\Lambda(B_1)$ і за умови, що B_1 є достатньо редукованим базисом, може бути відновлений за допомогою алгоритма найближчої площини Бабаї [22]: $v_1 = NearestPlane_{B_1}(B_2 v_2)$.

Гібридна атака складається з трьох етапів:

- Редукувати базис B_1.
- Знайти вектор v_2 за допомогою комбінаторних технік.
- Знайти вектор v_1 за допомогою алгоритма $NearestPlane$

Оскільки розмірності, у яких виконується пошук, є меншими, то загальний час виконання буде значно меншим за умови, що комбінарторна частина атаки має не велику оцінку. Оскільки реалізація комбінаторної частини атаки сильно залежить від конкретної криптографічної схеми, то конкретні оцінки комбінаторної частини атаки будуть сильно відрізнятися для різних схем. Фактично, гібридна атака є модифікацією атаки декодування, тому графік для простору параметрів буде схожим на рис. 11, тільки зміщеним на деякий фактор, який визначається комбінаторною частиною.

Є цікавим той момент, що формула (21), яка визначає ймовірність знаходження вектора v_1, отримана з припущення, що таємний вектор матиме нормальний розподіл, у той час, як гібридна атака застосовується переважно для векторів, що мають розподіл відмінний від нормального. Ця проблема у літературі зазвичай обходиться стороною.

Ми пропонуємо при оцінці гібридної атаки для розподілів, що відмінні від нормального, апроксимувати цей розподіл ймовірностей нормальним розподілом, що мінімізує відстань Колмогорова-Смірнова, яка визначена як максимальна абсолютна різниця між двома емпіричними функціями розподілу.

Для нормального розподілу у межах $[-\epsilon, +\epsilon]$ для $\epsilon = 1, \ldots, 10$ ми обчислили оптимальні значення дисперсії σ у табл. 1. На рис. 15 у якості ілюстрації наведено порівняння функцій розподілу для $\epsilon = 3$.

Таблиця 1

Оптимальні значення σ для мінімізації відстані Колмогорова-Смірнова

ϵ	Оптимальне σ	Відстань Колмогорова–Смірнова	ϵ	Оптимальне σ	Відстань Колмогорова–Смірнова
1	1.03	0.16666	6	4.14	0.07339
2	1.71	0.12074	7	4.73	0.06963
3	2.30	0.09644	8	5.34	0.06701
4	2.93	0.08589	9	5.94	0.064911
5	3.53	0.07807	10	6.54	0.063163

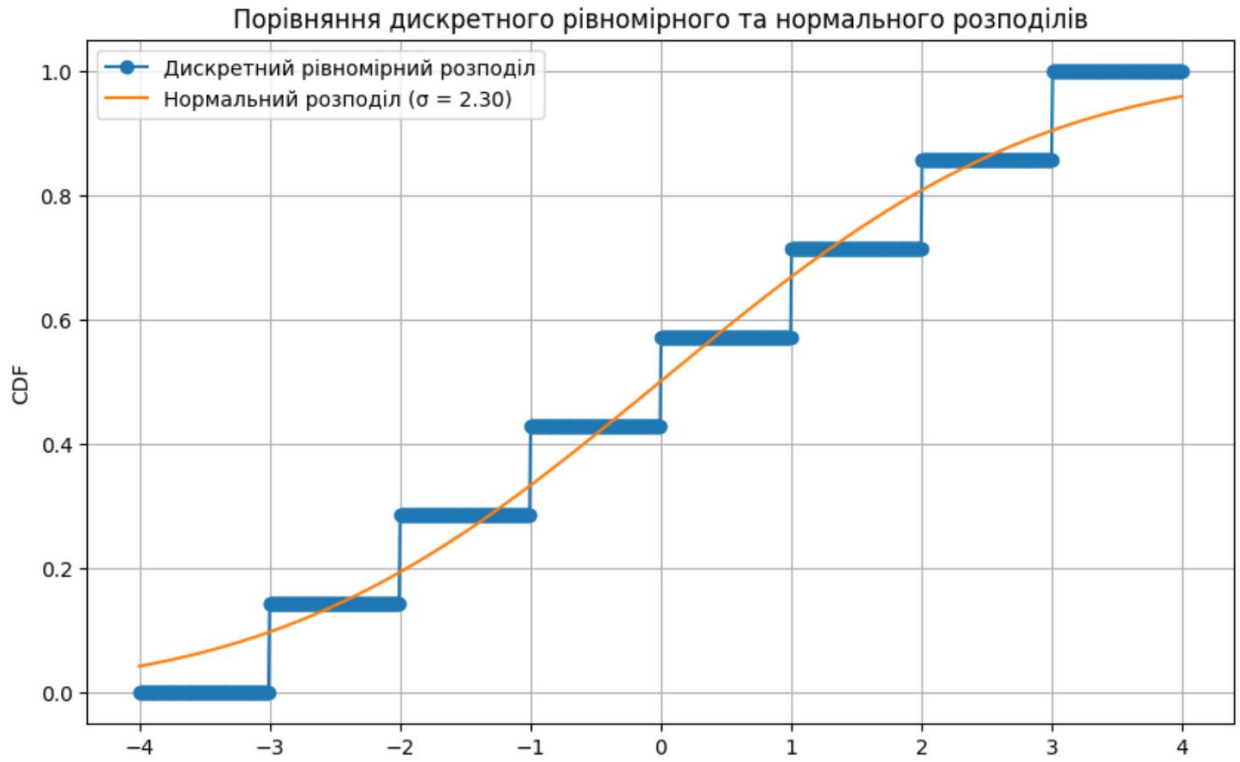

Рис. 15. Порівняння дискретного рівномірного розподілу
та його апроксимації нормальним розподілом

Отримані значення, на нашу думку, дозволяють з достатньою точністю апроксимувати заданий розподіл нормальним розподілом і застосувати описаний вище підхід до атаки декодування та гібридної атаки.

9. Атаки на проблему SIS

Проблема SIS дещо відрізняється від проблем LWE та NTRU тим, що вимагається знаходження вектора, що є малим у l_∞ нормі. Відповідний вектор лежить на решітці

$$\Lambda(A) = \{z \in \mathbb{Z}^d | Az = 0\} \tag{26}$$

Існуючі в літературі підходи до оцінки складності проблеми SIS через редукцію решіток вважають, що нам відомий розмір шуканого вектору у l_2 нормі. Проте, з визначення проблеми не випливає, що нам необхідний вектор саме з конкретною l_2 нормою. Тому ми розробили власний підхід, який враховує те, що для шуканого вектора з l_∞ нормою можуть бути знайдені рішення з різними l_2 нормами.

Щоб оцінити ймовірність події знаходження вектора v, що має l_∞ норму B можливо використати властивість концентрації мери на гіперсфері. Для -вимірної гіперсфери ймовірність того, що довільна компонента вектора v_i буде далеко від середнього значення експоненціально зменшується з збільшенням відстані. Для кожного v_i маємо

$$\Pr[|v_i| \geq B] \leq 2exp\left(-\frac{\left(\frac{B\sqrt{d}}{\|v\|_2}\right)^2}{2}\right) \tag{27}$$

Відповідно, для усього вектора маємо:

$$\Pr\left[\|v\|_\infty \leq B\right] \approx \left(1 - 2exp\left(-\frac{\left(\frac{B\sqrt{d}}{\|v\|_2}\right)^2}{2}\right)\right)^d \tag{28}$$

Запропонований підхід до вирішення SIS полягає у наступному:

- Провести редукцію базису SIS-решітки з параметром β_1
- За допомогою алгоритму просіювання у розмірності β_2 отримати N малих векторів з значенням норми α
- Для заданого значення α знайти ймовірність p_{succ} того, що l_∞ норма не перевищує значення B за формулою (28).
- Оцінити складність атаки як $(T_{red} + T_{sieve})/(\min(1, N \cdot p_{succ}))$

Алгоритм просіювання може повернути н $2^{0.2075\beta}$ векторів з нормою $\alpha = \rho \cdot \|b_0\|_2$, де ρ оцінюється як

$$\sqrt{4/3} \cdot \delta_{\beta_1}^{\beta_1 - 1} \delta_{\beta_2}^{1-\beta_2} \tag{29}$$

Моделювання атаки показало, що застосування симуляторів майже не впливає на оцінки безпеки для атаки на SIS. На рис. 16 показано результати моделювання.

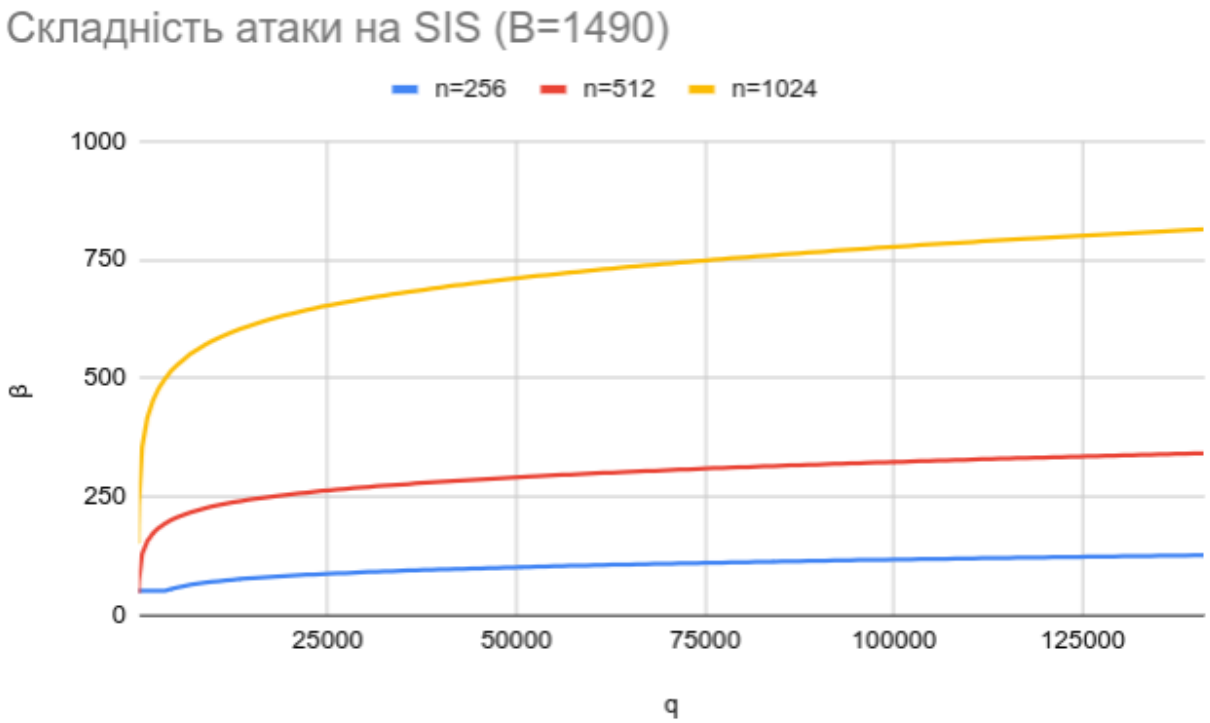

Рис. 16. Результати оцінки атаки на SIS

Додатково для оцінки впливу нової моделі на складність криптоаналізу SIS були розраховані оцінки для Crystals-Dilithium. Відповідні оцінки наведено у табл. 2.

Таблиця 2

Оцінка складності проблеми SIS для Crystals-Dilithium

Рівень безпеки NIST	Оцінка авторів Crystals-Dilithium (біт)	Наша оцінка
2	123	111
3	186	163
5	265	236

З табл. 2 видно, що наша оцінка дає менші значення безпеки, ніж очікувалися авторами Crystals-Dilithium.

Висновки

1. Для виявлення найкращої моделі редукції решіток, що дозволяє найточніше моделювати профіль решітки, було обчислено середньоквадратичну помилку на решітках малої розмірності для моделі GSA (ZGSA) та варіантів симулятору Чена–Нгуєна і симулятору Альбрехта–Лі. Детермінований симулятор Альбрехта–Лі показав найкращі результати для усіх значень параметрів.

2. При врахуванні алгебраїчної структури q-арних решіток в атаках вкладення було виявлено, що модель GSA занижує значення безпеки. Цей ефект пояснюється тим, що GSA не враховує того, що останній блок в базисі є HKZ-редукованим і має іншу форму. На малих значеннях параметра q уточнені оцінки показують менші показники безпеки, проте зі збільшенням праметра ситуація повністю змінюється. Оцінки безпеки стають більшими, ніж для GSA. Більшість існуючих криптографічних параметрів потрапляють у другу зону. Це вказує на те, що існуючи схеми переважно є безпечнішими, ніж вважалося раніше. Для NTRU решіток також необхідно враховувати можливість переходу на розріджену решітку.

3. Для атак декодування було запропоновано стратегію вибору параметрів атаки d_i. З використанням цих параметрів було показано, що атаки декодування можуть бути кращими за атаки вкладення. Вплив алгебраїчної структури q-арних решіток на атаки відновлення є не таким сильним, як при атаках вкладення. Це пояснюється тим, що на атаки декодування впливає вся форма профіля, а не лише конкретне значення в останньому блоці, як у атаках вкладення.

4. Гібридні атаки є, фактично, узагальненням атак декодування, хоча вони історично з'явилися раніше. Оцінки гібридних атак та атак декодування ґрунтуються на тому, що розподіл таємного вектора є нормальним. Проте, це не так для більшості параметрів, для яких гібридні атаки можливо застосувати. Щоб подолати цю ситуацію було запропоновано апроксимувати відповідні розподіли нормальним розподілом, мінімізуючи відстань Колмогорова-Смірнова та обчисленні конкретні оптимальні параметри апроксимуючих нормальних розподілів.

5. Існуючі в літературі підходи до оцінки складності проблеми SIS через редукцію решіток вважають, що нам відомий розмір шуканого вектору у l_2 нормі. Проте, з визначення проблеми не випливає, що нам необхідний вектор саме з конкретною l_2 нормою. У межах дослідження було розроблено метод, що враховує факт того, що при фіксованих вимогах до l_∞ норми, l_2 норма може мати різні значення. Отримані оцінки показують, що складність криптоаналізу Crystals-Dilithium є меншою, ніж вважалося раніше. Для п'ятого рівня безпеки різниця становить 2^{30}, що є суттєвим.

Список літератури:

1. Post-quantum cryptography: CSRC, CSRC. Available at: https://csrc.nist.gov/projects/post-quantum-cryptography (Accessed: 21 July 2024).
2. O. Regev. The Learning with Errors Problem. Available: https://cims.nyu.edu/~regev/papers/lwesurvey.pdf
3. J. Hoffstein, J. Pipher, and J. Silverman. NTRU: A Ring-Based Public Key Cryptosystem. Available: https://www.ntru.org/f/hps98.pdf
4. C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for Hard Lattices and New Cryptographic Constructions. ePrint IACR, 2007. https://eprint.iacr.org/2007/432
5. C. Schnorr. Lattice Reduction by Random Sampling and Birthday Methods, 2003. Accessed: Jul. 21, 2024. [Online]. Available: https://d-nb.info/1153616645/34
6. M. Albrecht and L. Ducas. LATTICE ATTACKS ON NTRU AND LWE: A HISTORY OF REFINEMENTS. Available: https://eprint.iacr.org/2021/799.pdf
7. Y. Chen and P. Nguyen. BKZ 2.0: Better Lattice Security Estimates. Accessed: Jul. 21, 2024. [Online]. Available: https://www.iacr.org/archive/asiacrypt2011/70730001/70730001.pdf
8. S. Bai, D. Stehlé, and W. Wen. Measuring, simulating and exploiting the head concavity phenomenon in BKZ // Cryptology ePrint Archive (eprint.iacr.org), 2018. https://eprint.iacr.org/2018/856 (accessed Jul. 21, 2024).
9. Z. Zhao and G. Xu. On the Measurement and Simulation of the BKZ Behavior for q-ary Lattices // Lecture notes in computer science, pp. 463–482, Jan. 2023, doi: https://doi.org/10.1007/978-3-031-26553-2_25.
10. I. D. Gorbenko, O. G. Kachko, Y. I. Gorbenko, I. V. Stelnik, S. O. Kandy, and M. V. Yesina. METHODS OF

BUILDING GENERAL PARAMETERS AND KEYS FOR NTRU PRIME UKRAINE OF 5TH – 7TH LEVELS OF STABILITY. PRODUCT FORM // Telecommunications and radio engineering, vol. 78, no. 7, pp. 579–594, Jan. 2019, doi: https://doi.org/10.1615/telecomradeng.v78.i7.30.

11. E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe. Post-quantum key exchange – a new hope // Cryptology ePrint Archive (eprint.iacr.org), 2015. https://eprint.iacr.org/2015/1092

12. ДСТУ 8961:2019. Інформаційні технології. Криптографічний захист інформації. Алгоритми асиметричного шифрування та інкапсуляції ключів. Чин. від 21.12.2019. Вид. офіц. Київ: УкрНДНЦ, 2019. 72 с.

13. C. Peikert. A Decade of Lattice Cryptography // Foundations and Trends® in Theoretical Computer Science, vol. 10, no. 4, pp. 283–424, 2016, doi: https://doi.org/10.1561/0400000074.

14. M. Albrecht, S. Bai, and L. Ducas. A subfield lattice attack on overstretched NTRU assumptions: Cryptanalysis of some FHE and Graded Encoding Schemes // Cryptology ePrint Archive (eprint.iacr.org), 2016. https://eprint.iacr.org/2016/127 (accessed Jul. 21, 2024).

15. L. Ducas and W. van Woerden. NTRU Fatigue: How Stretched is Overstretched? // Cryptology ePrint Archive (eprint.iacr.org), 2021. https://eprint.iacr.org/2021/999 (accessed Jul. 21, 2024).

16. C. van Vredendaal. Reduced memory meet-in-the-middle attack against the NTRU private key // LMS Journal of Computation and Mathematics, vol. 19, no. A, pp. 43–57, 2016, doi: https://doi.org/10.1112/s1461157016000206.

17. Q. Guo, T. Johansson, and P. Stankovski. Coded-BKW: Solving LWE Using Lattice Codes // Accessed: Jul. 21, 2024. [Online]. Available: https://www.iacr.org/archive/crypto2015/92160189/92160189.pdf

18. M. Albrecht, C. Cid, J.-C. Faugère, R. Fitzpatrick, and L. Perret. On the complexity of the Arora-Ge Algorithm against LWE On the complexity of the Arora-Ge Algorithm against LWE. 2012 // Accessed: Jul. 21, 2024. [Online]. Available: https://inria.hal.science/hal-00776434/PDF/SCC_AG_2012.pdf

19. D. Bernstein and T. Lange. Non-randomness of S-unit lattices. Accessed: Jul. 21, 2024. [Online]. Available: https://eprint.iacr.org/2021/1428.pdf

20. R. Lindner and C. Peikert, “Better Key Sizes (and Attacks) for LWE-Based Encryption, 2010 // Accessed: Jul. 21, 2024. [Online]. Available: https://eprint.iacr.org/2010/613.pdf

21. N. Alkadri, J. Buchmann, R. Bansarkhani, and J. Krämer. A Framework to Select Parameters for Lattice-Based Cryptography // Accessed: Jul. 21, 2024. [Online]. Available: https://eprint.iacr.org/2017/615.pdf

22. L. Bi, X. Lu, J. Luo, and K. Wang. Hybrid Dual and Meet-LWE Attack // Cryptology ePrint Archive (eprint.iacr.org), 2022. https://eprint.iacr.org/2022/1330 (accessed Jul. 21, 2024).

23. S. Bai, S. Miller, and W. Wen. A refined analysis of the cost for solving LWE via uSVP, 2019 // Accessed: Jul. 21, 2024. [Online]. Available: https://hal.science/hal-02886638/document

Надійшла до редколегії 29.04.2024

Відомості про авторів:

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», науковий консультант; Україна; e-mail: sergeykandy@gmail.com; ORCID: https://orcid.org/0000-0003-0552-8341

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