ISSN 2519-2310 (Online)

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА, 2024, № 1 (25)

COMPUTER SCIENCE AND CYBERSECURITY, 2024, Iss. 1 (25)

DOI: https://doi.org/10.26565/2519-2310-2024-1-02
УДК 004.056.5

АНАЛІЗ ФАКТОРА ЕРМІТА АЛГОРИТМУ BKZ НА РЕШІТКАХ МАЛОЇ РОЗМІРНОСТІ

Іван Горбенко[1], доктор технічних наук, професор, e-mail: i.d.gorbenko@karazin.ua, ORCID: https://orcid.org/0000-0003-4616-3449
Сергій Кандій[1], аспірант кафедри захисту інформаційних систем та технологій, e-mail: sergeykandy@gmail.com, ORCID: https://orcid.org/0000-0003-4616-3449
[1]*Харківський національний університет імені В.Н. Каразіна, майдан Свободи, 4, Харків, 61022, Україна*

Рукопис надійшов 1 квітня 2024 р. Отримано після рецензування 2 травня 2024 р. Прийнято 3 червня 2024 р.

Анотація: Криптографія на решітках є одним з перспективних напрямів досліджень у сучасній криптографії. Електронні підписи та механізми інкапсуляції ключів на решітках вже використовуються на практиці. У перспективі такі квантово-стійкі перетворення на решітках замінять усі стандарти, що не мають стійкості до атак на квантових комп'ютерах. Це робить аналіз їх безпеки надзвичайно актуальним. Аналіз безпеки криптографічних перетворень на решітках часто зводиться до оцінки мінімального розміру блоку у алгоритмах редукції решіток. Щоб визначити наскільки малі вектори може отримати алгоритм редукції для заданого розміру блоку часто використовується модель GSA, яка використовує так званий фактор Ерміта для передбачення розміру векторів, які може отримати алгоритм редукції решіток при заданих параметрах. Для його оцінки на практиці використовуються асимптотичні формули, проте питання їх точності на криптографічних решітках не до кінця досліджено. В роботі було отримано оцінки точності існуючих асимптотичних оцінок фактору Ерміта для решіток розмірностей 120, 145, 170 для класичного алгоритму BKZ. Дослідження проводились з використанням бібліотеки fpylll. Було показано, що існуючі оцінки з практичної точки зору є еквівалентними та мають достатньо мале середньоквадратичне відхилення від істинних значень. Було отримано формулу, що прив'язує середньоквадратичну похибку апроксимації фактору Ерміта до криптографічних параметрів решіток. Отримані результати є корисними для уточнення оцінок безпеки існуючих криптографічних перетворень.

Ключові слова: *квантово-стійка криптографія, криптографія на решітках, фактор Ерміта, BKZ, GSA*

Як цитувати: Горбенко І., Кандій С.. Аналіз фактора Ерміта алгоритму BKZ на решітках малої розмірності. *Комп'ютерні науки та кібербезпека.* 2024; № 1(25): С. 22–34. https://doi.org/10.26565/2519-2310-2024-1-02

In cites: Gorbenko I., Kandii S. (2024). The analysis of Hermite factor of BKZ algorithm on small lattices. *Computer Science and Cybersecurity.* 1(25): 22–34. https://doi.org/10.26565/2519-2310-2024-1-02 (in Ukrainian)

1. Вступ

Криптографія на решітках є перспективним напрямком досліджень, який активно розвивається в останні роки. Зокрема, фіналістами конкурсу NIST PQC стали криптографічні схеми на решітках [1]. У той же час, в Україні вже навіть є квантово-стійкі стандарти на решітках: стандарт квантово-стійкого асиметричного шифрування ДСТУ 8961:2019 [2] та стандарт квантово-стійкого електронного підпису ДСТУ 9212:2023 [3]. Іншим напрямком застосування криптографії на решітках є схеми гомоморфного шифрування [4], які вже активно використовуються в системах, що потребують роботи з конфіденційною інформацією без її розголошення. Це робить актуальними дослідження безпеки криптографічних перетворень на решітках.

Криптоаналіз сучасних криптографічних перетворень на решітках переважно зводиться до аналізу процесів редукції базису решіток. Алгебраїчні та комбінаторні техніки при цьому грають допоміжну роль [5, 6]. Для оцінки складності редукції решіток використовуються різні моделі, які дозволяють оцінити характеристики базису решітки після редукції. Фактор Ерміта є важливим показником якості редукції базису, який показує наскільки малі вектори здатен отримати заданий алгоритм редукції решіток [5]. Проте, сучасні оцінки фактору Ерміта є асимптотичними і на практиці можуть дещо відрізнятися від реальних значень фактору Ерміта. Оцінка, що була представлена в роботі [7], вважається стандартною оцінкою фактору Ерміта при криптоаналізі криптографічних перетворень на решітках. Проте, у роботі [8] була отримана більш точна асимптотична оцінка фактору Ерміта, хоча і не набула популярності серед дослідників.

Метою цієї роботи є експериментальне порівняння поведінки існуючих асимптотичних оцінок фактору Ерміта на решітках малої розмірності для алгоритму BKZ. У результаті проведеного аналізу були отримані оцінки середньоквадратичної похибки для відомих асимптотичних оцінок фактору Ерміта та було показано, що для криптографічних значень вплив помилки апроксимації фактору Ерміта є незначним.

2. Теоретичні відомості з теорії решіток

Для аналізу введемо основні теоретичні положення теорії решіток. Теоретичні відомості викладаються згідно [9]. Решітка Λ з базисом $B=(b_1,...,b_n)$ є множиною цілочисельних комбінацій лінійно незалежних векторів $b_1,...,b_n \in \mathbb{R}^n$:

$$\Lambda(b_1,...,b_n)=\left\{\sum_{i=1}^{n} x_i b_i, x_i \in \mathbb{Z}\right\} \quad (1)$$

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

Для заданого базису $B=(b_1,...,b_n)$ для решітки, що задається формулою (1), ортогоналізований за Граммом-Шмідтом базис є $B^*=(b_1^*,...,b_n^*)$, 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. Профілем базису будемо називати вектор $(\|b_1^*\|,\|b_2^*\|,...,\|b_n^*\|)$.

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

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

$$\Lambda_{[i:j]} = \Lambda(\pi_i(b_i), \pi_i(b+1), ..., \pi_i(b_j)) \tag{2}$$

Для $j \in \{i, i+1, ..., n\}$.

У кожній решітці Λ існує найменший ненульовий вектор. $\lambda_1(\Lambda)$ – норма найменшого ненульового вектору. Проблема пошуку найменшого вектору (SVP) полягає у пошуку вектору довжини $\lambda_1(\Lambda)$.

Важливим послабленням проблеми SVP є проблема апроксимації найменшого вектору – α-SVP, яка полягає у пошуку вектору, що має норму, меншу за $\alpha \cdot vol(\Lambda)^{1/n}$, де α – деяка константа, що залежить від розмірності решітки.

Константа Ерміта γ_n визначає обмеження на найменший вектор серед усіх решіток розмірності n і визначена як

$$\gamma_n = \sup_{\Lambda} \{\lambda_1^2(\Lambda) / vol(\Lambda)^{2/n}\} \tag{3}$$

Для константи Ерміта (3) відомі наступні оцінки [9]:

$$\frac{n}{2\pi e} + \frac{\log(\pi n)}{2\pi e} \le \gamma_n \le \frac{1.744n}{2\pi e} + o(n) \tag{4}$$

3. Алгоритми редукції решіток та фактор Ерміта

Алгоритм редукції LLL виконує над базисом дві операції: редукція за розміром $b_i \leftarrow b_i - round(\mu_{ij}) b_j$ для $j \in [i-1]$ та обмін місцями векторів b_i і b_{i+1}, якщо $(\eta - \mu_{i+1,i}^2) \left\| b_{i+1}^* \right\|^2 \le \left\| b_i^* \right\|^2$ для загальносистемного параметра $\eta \in (0.25, 1)$ поки відбуваються зміни у базисі.

Алгоритм BKZ є узагальненням LLL. У алгоритмі BKZ (та його варіаціях) фіксується розмір блоку β і відбувається пошук найменшого вектору на решітках $\Lambda_{[i,i+\beta'-1]}$ (формула (2)) для i від 1 до n–1, де $\beta' = \min(\beta, n-i+1)$. Пошук найменшого вектору відбувається окремою процедурою.

Для індексу i стандартна реалізація алгоритму BKZ викликає алгоритм пошуку найменшого вектору для решітки $\Lambda_{[i,i+\beta'-1]}$ і знаходить найкоротший вектор v на цій решітці. Далі BKZ вставляє v у старий базис між b_{i-1} та b_i. Для базису $(b_1, ..., b_{i-1}, v, b_i, ..., b_{min(i+\beta-1,n)})$ застосовується LLL для отримання нового базису з меншими векторами. Ці процедури складають один раунд алгоритму. У оригінальній версії BKZ алгоритм зупинявся, коли оновлень не відбувалось протягом n–1 раундів.

Для аналізу алгоритму BKZ зазвичай використовується евристика Гауса [5, 6, 9], 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 до евристики Гауса, можливо оцінити як:

$$GH(\Lambda) = \left(\frac{vol(\Lambda)}{vol(\Omega)}\right)^{1/d} = \frac{\Gamma\left(1+\frac{d}{2}\right)}{\sqrt{\pi}} \cdot vol(\Lambda)^{1/d} \approx \sqrt{\frac{d}{2\pi e}} \cdot vol(\Lambda)^{1/d} \quad (5)$$

Практичні експерименти з алгоритмами LLL та BKZ показують [10], що $\left\|b_i^*\right\| / \left\|b_{i+1}^*\right\| \approx const$, якщо $d >> \beta$. У якості ілюстрації цього твердження на рис. 1 наведено профілі для 230-мірної випадкової q-арної решітки для β = 2,10,30,40,50.

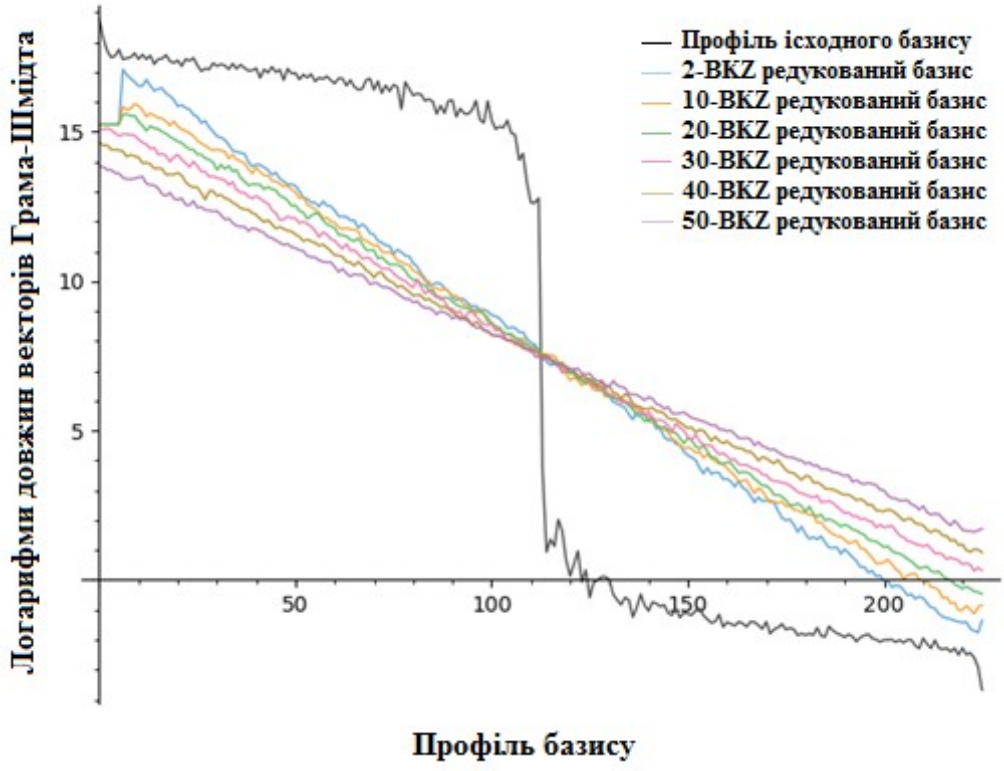

Рис. 1. – Профілі 230-мірної q-арної решітки для β = 2,10,30,40,50
Fig. 1 – Profiles of a 230-dimensional q-ary lattice for β = 2,10,30,40,50

Застосовуючи евристику Гауса (5) до BKZ-β редукованого базису $B = (b_1, ..., b_n)$ та враховуючи припущення $\left\|b_i^*\right\| / \left\|b_{i+1}^*\right\| \approx const$, маємо:

$$\log\left\|b_i^*\right\| = \frac{d-1-2i}{2} \cdot \log(\alpha_\beta) + \frac{1}{d}\log\left(vol(\Lambda)\right) \quad (6)$$

Для деякого α_β, що залежить від властивостей BKZ-β.

Рівняння (6) є моделлю редукції решіток GSA (англ. Geometric Series Assumption) [10]. Експериментальні дослідження у роботах [10, 11] показують доволі гарну точність моделі GSA для $50 < \beta << n$. На рис. 2 наведено приклад застосування моделі GSA.

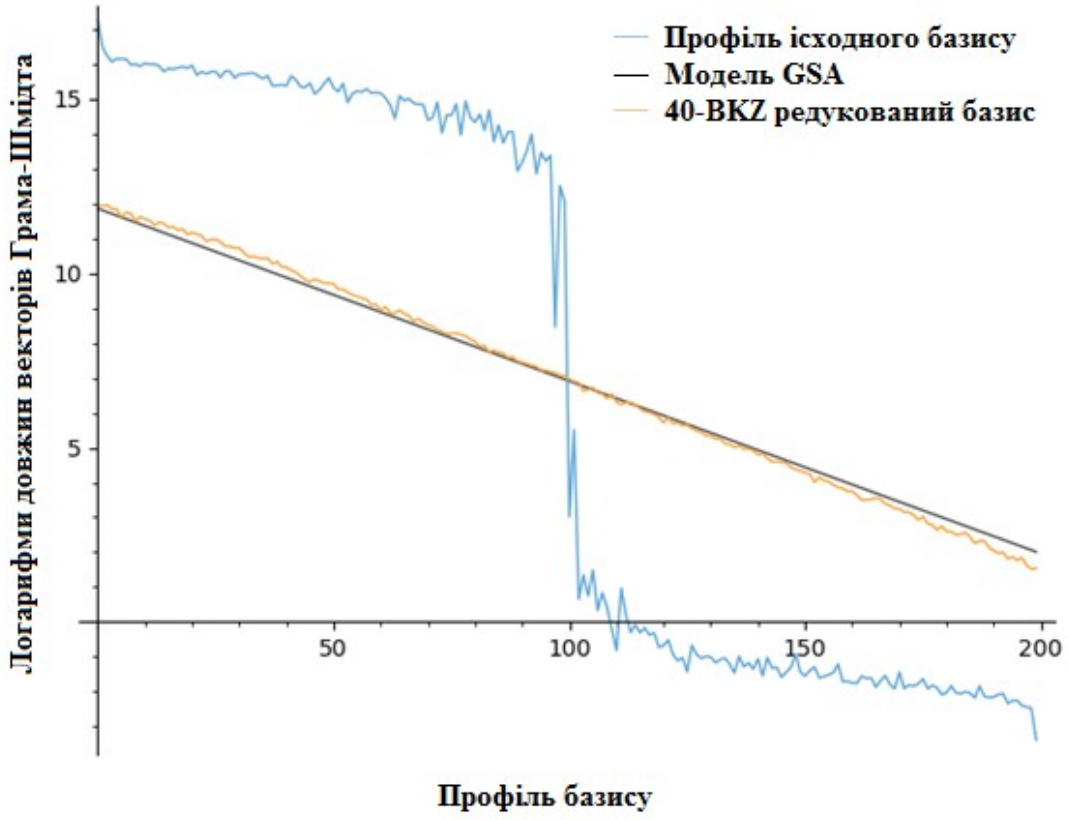

Рис. 2 – Приклад застосування моделі GSA для 200-мірної решітки
Fig. 2 – An example of applying the GSA model to a 230-dimensional lattice

Для алгоритму BKZ, з формули (6) випливає наступна оцінка:

$$\|b_0\| \le \sqrt{\alpha_\beta}^{d-1} \cdot vol(\Lambda(B))^{1/d} \tag{7}$$

Фактор Ерміта визначає найменше значення α, для якого алгоритм BKZ-β може вирішити задачу α-SVP. Він є аналогом константи Ерміта (3), тільки для конкретного базису і формально визначений як

$$\delta_\beta = \left(\|b_0\| / vol(\Lambda)^{1/d} \right)^{1/d} \tag{8}$$

З рівнянь (7) та (8) випливає, що $\delta_\beta = \sqrt{\alpha_\beta}^{1-1/d}$. Ця рівність поєднує формальне визначення фактору Ерміта з його практичним застосуванням для оцінки якості редукції.

У роботі [7] була запропонована асимптотична оцінка

$$\lim_{\beta \to \infty} \delta_\beta = \left(\frac{\beta}{2\pi e} \cdot (\pi\beta)^{1/\beta} \right)^{\frac{1}{2(\beta-1)}} \tag{9}$$

Ця оцінка використовується у всіх сучасних моделях безпеки. У роботі [8] було показано, що ця оцінка є лише першим наближенням і може бути уточнена наступним чином:

$$\lim_{\beta\to\infty}\delta_\beta=\left(\frac{\beta}{2\pi e}\cdot(\pi\beta)^{1/\beta}\right)^{\frac{1}{2(\beta-1)}+\frac{\beta}{2n^2}} \tag{10}$$

На рис. 3 зображено графік фактору Ерміта. З рисунку видно, що оцінка (9) наближається до нижньої теоретичної межі (константи Ерміта, формула (4)), у той час як оцінка (10) є більш помірною.

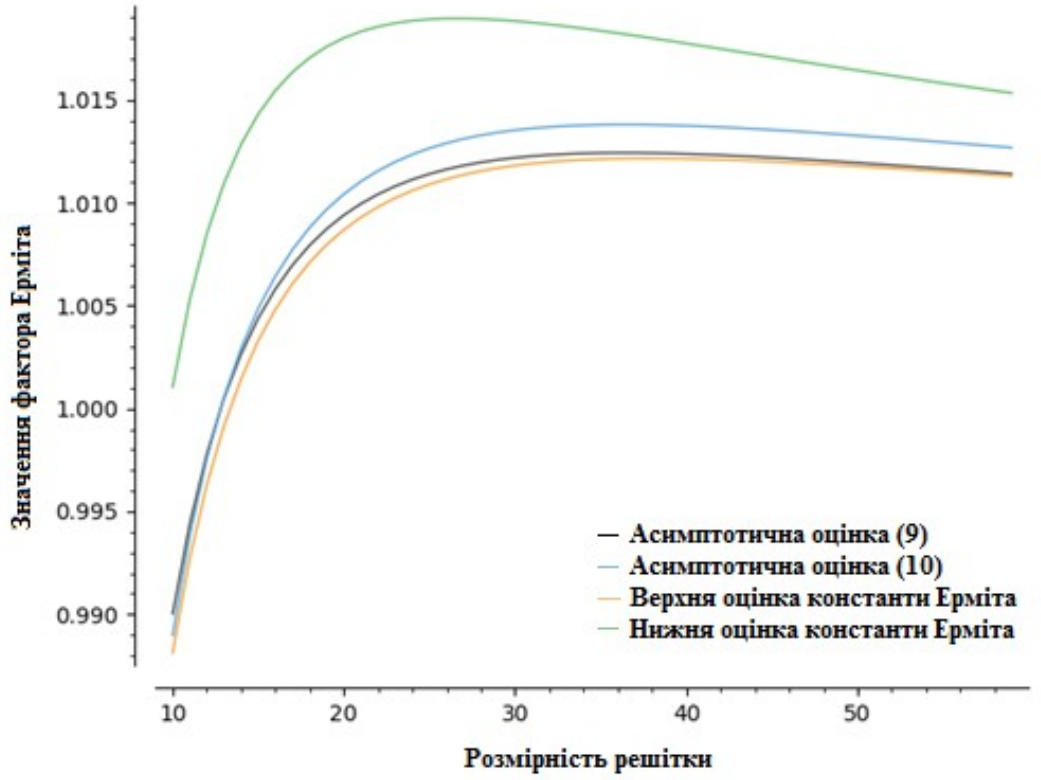

Рис. 3 – Значення фактору Ерміта
Fig. 3 – Asymptotic estimates of the Hermite factor

Фактично, фактор Ерміта у моделі GSA повністю визначає профіль для заданої решітки, тому важливо розуміти які він приймає значення на практиці. Для криптографічно значущих розмірностей, звісно, отримати значення неможливо, проте можливо протестувати на малих розмірностях.

4. Експериментальна оцінка фактору Ерміта

У загальному випадку на значення фактору Ерміта можуть впливати розмір блоку редукції, розмірність решітки та розмір в бітах кожного коефіцієнта векторів в базисі. Для виявлення впливу кожного з цих факторів були проведені експериментальні дослідження поведінки кореневого фактору Ерміта на випадкових решітках.

Дослідження проводилося на випадкових q-арних решітках, оскільки саме такі решітки використовуються в криптографії на решітках. Для простого $q \geq 2$ q-арна решітка визначається базисом

$$B = \begin{pmatrix} qI_m & A \\ 0 & \zeta I_n \end{pmatrix} \in \mathbb{Z}^{(m+n)\times(m+n)}$$

де ζ – деяка константа. Детермінант такої решітки відповідно має значення $q^m\zeta^n$. У проведених експериментах використовувалося значення $\zeta = 1$.

Варто зауважити, що в q-арних решітках у загальному випадку перші та останні вектори можуть не підпорядковуватися моделі GSA, проте при обраних для дослідження параметрах модель GSA працює достатньо гарно.

У таблицях 1-3 наведено результати виміру фактору Ерміта для випадкових q-арних решіток. Для досліджень використовувалися випадкові решітки розмірностей 120, 145, 170. Для кожної з цих розмірностей розглядалися значення $\log_2 q = 10, 20, 40$ для розмірів блоку від 3 до 60.

Для кожного набору параметрів виконувалася оцінка щонайменше на 200 випадкових решітках, генерація яких відбувалася за допомогою засобів бібліотеки fpylll, що реалізує алгоритми редукції решіток. Редукція решіток відбувалася з використанням алгоритму BKZ з стандартними налаштуваннями.

Таблиця 1 – Експериментальні оцінки фактору Ерміта для $\log_2 q = 10$
Table 1 – Experimental estimation of the Hermite factor for $\log_2 q = 10$

β	**Розмірність 120**	**Розмірність 145**	**Розмірність 170**
3	1.017378	1.017690	1.016867
5	1.017378	1.017690	1.016867
10	1.015669	1.016230	1.015883
15	1.014016	1.014413	1.014484
20	1.013434	1.013680	1.013671
25	1.012825	1.013024	1.013012
30	1.012559	1.012833	1.012833
35	1.012352	1.012610	1.012653
40	1.012187	1.012415	1.012458
45	1.011986	1.012163	1.012241
50	1.011449	1.011726	1.011718
55	1.011132	1.011373	1.011397
60	1.010854	1.011097	1.011049

З таблиці 1 видно, що фактор Ерміта залежить від розмірність решітки має вплив на значення фактору Ерміта.

Таблиця 2 – Експериментальні оцінки фактору Ерміта для $\log_2 q = 20$
Table 2 – Experimental estimation of the Hermite factor for $\log_2 q = 20$

β	**Розмірність 120**	**Розмірність 145**	**Розмірність 170**
3	1.017318	1.017987	1.018275

5	1.017318	1.017987	1.018275
10	1.015702	1.016254	1.016846
15	1.013923	1.014496	1.015003
20	1.013243	1.013654	1.013946
25	1.012820	1.012977	1.013223
30	1.012630	1.012746	1.013053
35	1.012296	1.012596	1.012792
40	1.012116	1.012393	1.012651
45	1.011863	1.012116	1.012360
50	1.011399	1.011695	1.011787
55	1.011200	1.011372	1.011453
60	1.010895	1.011065	1.011194

З таблиці 2 видно, що значення q впливає лише на малих значеннях β.

Таблиця 3 – Експериментальні оцінки фактору Ерміта для $\log_2 q = 40$
Table 3 – Experimental estimation of the Hermite factor for $\log_2 q = 40$

β	**Розмірність 120**	**Розмірність 145**	**Розмірність 170**
3	1.017322	1.017685	1.018242
5	1.017322	1.017685	1.018242
10	1.015547	1.016249	1.016789
15	1.013991	1.014420	1.014897
20	1.013351	1.013708	1.013915
25	1.012738	1.013018	1.013307
30	1.012563	1.012835	1.013085
35	1.012377	1.012607	1.012849
40	1.012162	1.012407	1.012661
45	1.012019	1.012167	1.012385
50	1.011495	1.011734	1.011870
55	1.011121	1.011356	1.011508
60	1.010811	1.011107	1.011172

Введемо функціонал середньоквадратичної похибки:

$$MSE(\delta_{etalon}, \delta_{experiment}) = \frac{1}{d}\sum_{i=0}^{d-1}\left(\delta_{etalon}[i] - \delta_{experiment}[i]\right)^2 \quad (11)$$

У таблицях 4-5 наведено значення середньоквадратичної похибки (11) для оцінок фактору Ерміта, починаючи від $\beta > 30$ для (9) та (10) відповідно.

Таблиця 4 – Значення MSE для оцінок фактору Ерміта (9)
Table 4 – MSE estimate for the Hermite factor estimation (9)

	Розмірність 120	**Розмірність 145**	**Розмірність 170**
$\log_2 q = 10$	0.0003728998	0.0002477775	0.0002575795
$\log_2 q = 20$	0.0003651147	0.0002409057	0.0003197217
$\log_2 q = 40$	0.0003566181	0.0002485526	0.0003261832

Таблиця 5 – Значення MSE для оцінок фактору Ерміта (10)
Table 5 – MSE estimate for the Hermite factor estimation (10)

	Розмірність 120	**Розмірність 145**	**Розмірність 170**
$\log_2 q = 10$	0.0021920808	0.0013799646	0.0010351942
$\log_2 q = 20$	0.0021856184	0.0014050912	0.0009452115
$\log_2 q = 40$	0.0021794041	0.0013804805	0.0009179317

З таблиць 4-5 випливає, що середньоквадратична помилка для оцінки (9) є меншою.

На рис. 4 наведено графіки δ_{etalon} та $\delta_{experiment}$, усереднені за параметром q для розмірності 170.

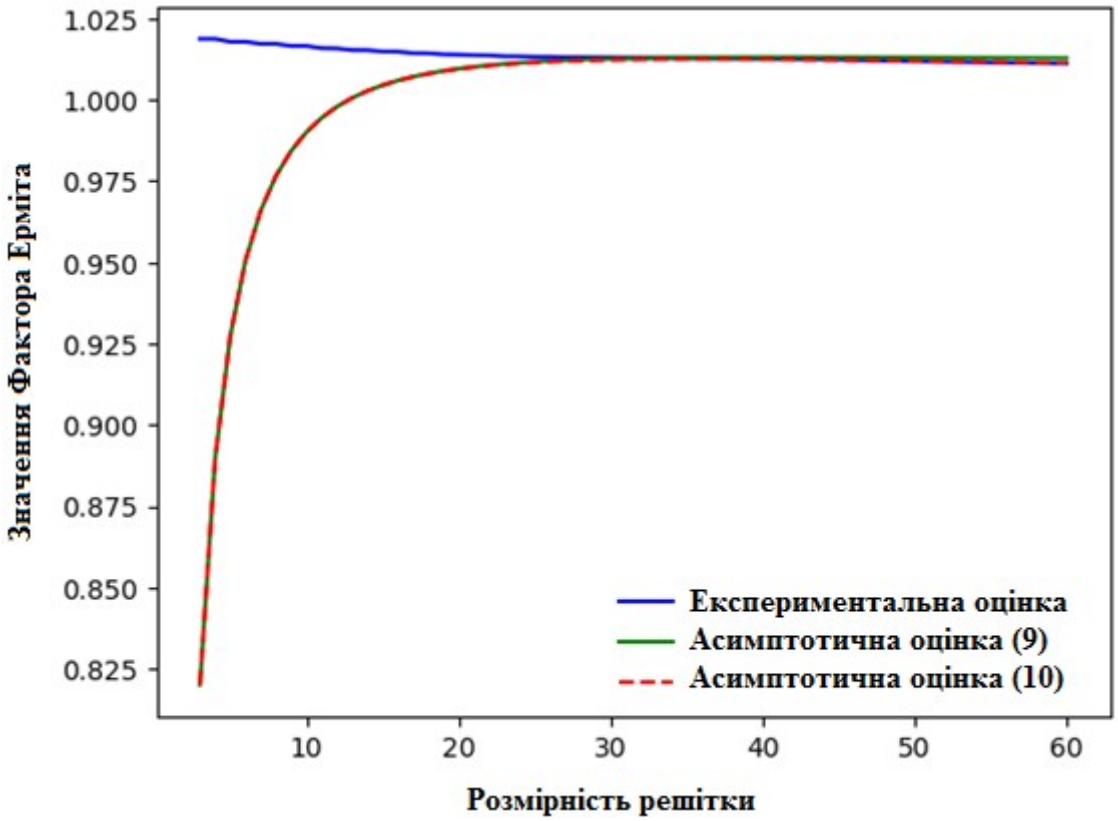

Рис. 4 – Експериментальна оцінка фактору Ерміта для розмірності 170
Fig. 4 – Experimental estimation of the Hermite factor for dimension 170

З рис. 4 видно, що на малих значеннях $\beta < 30$ оцінки (9) та (10) не працюють через свій асимптотичний характер. Далі експериментальна оцінка наближається до (9).

5. Обговорення результатів

На рис. 5 зображено фрагмент рис. 4 для значень $20 \le \beta \le 30$. З рис. 5 видно, що реальне експериментально обчислене значення фактору Ерміта на малих розмірностях навіть менше, ніж дає оцінка (9). При цьому з ростом розмірності реальні значення фактору Ерміта збільшуються, тому для оцінки фактору Ерміта можливо виділити 3 сценарії на решітках у криптографічно значимих розмірностях:

- Песимістичний сценарій. Значення фактору Ерміта не будуть досягати оцінки (9).
- Оптимістичний сценарій. Значення фактору Ерміта будуть близькі до оцінки (10).
- Реалістичний сценарій. Значення фактору Ерміта будуть більшими за (9), проте меншими за (10).

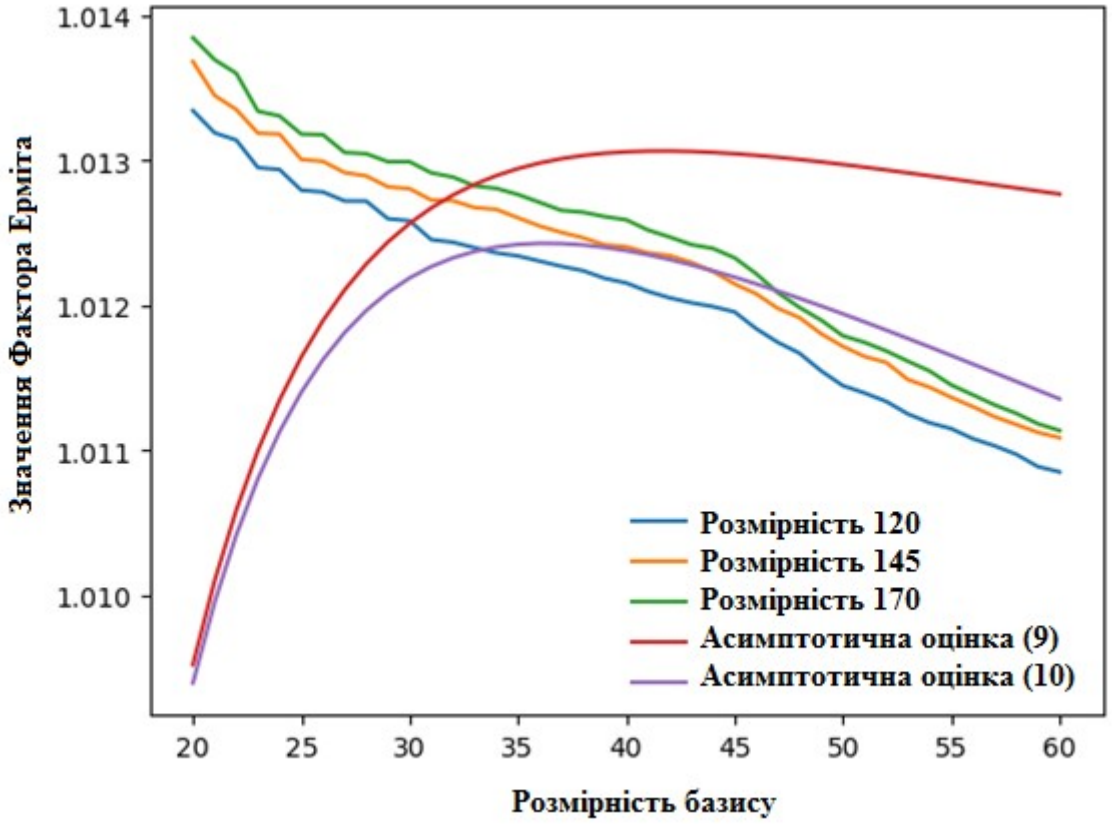

Рис. 5 – Експериментальна оцінка фактору Ерміта для розмірностей 120, 145, 170
Fig. 5 – Experimental estimation of the Hermite factor for dimensions 120,145,170

Для того, щоб знайти вплив похибки вимірювання τ_{mse} фактору Ерміта для великих розмірностей скористаємося біноміальною апроксимацією $(1+x)^{\alpha} \approx 1+\alpha x$ до формули (7):

$$\begin{aligned} \|b_0\| &= \delta^d \cdot vol(\Lambda)^{1/d} \approx (1-(\delta_{real}-1)+\tau_{mse})^d \cdot vol(\Lambda)^{1/d} \\ &\approx (1+d((\delta_{real}-1)+\tau_{mse}))) \cdot vol(\Lambda)^{1/d} = \|b_0\|_{etalon} + d\tau_{mse} \cdot vol(\Lambda)^{1/d} \end{aligned} \quad (12)$$

Оскільки для криптографічних випадків $vol(\Lambda)^{1/d} = q^m$, то з формули (12) маємо оцінку похибки

$$\tau_\delta = d\tau_{mse} \cdot q^{m/d} \approx d\tau_{mse} \cdot \sqrt{q} \quad (13)$$

Тож, для практичних обчислень можливо враховувати похибку апроксимації за формулою (13). Для типових криптографічних параметрів $d\sqrt{q} \approx 10^6$. Оскільки вже для малих розмірностей решіток значення $\tau_{mse} \approx 10^{-3} - 10^{-4}$ і має тенденцію до зменшення, то для криптографічних наборів параметрів похибка буде достатньо малою, щоб не впливати на оцінку безпеки.

6. Висновки

Існуючі асимптотичні оцінки дають гарну апроксимацію фактору Ерміта вже на малих розмірностях решіток. На решітках малої розмірності не було виявлено впливу розміру коефіцієнтів векторів в базисі на значення фактор Ерміта, проте розмірність решітки дійсно має вплив на фактор Ерміта. Хоча оцінка (9) не враховує цього, проте дає кращі результати у порівнянні з оцінкою (10), що враховує вплив розмірності. Проте, оскільки отримана середньоквадратична помилка має порядок 10^{-3}-10^{-4}, то можливо стверджувати, що помилка апроксимації фактору Ерміта не має впливу на оцінку складності редукції решіток для криптографічних параметрів, враховуючи асимптотичних характер формул.

Конфлікт інтересів

Автори повідомляють про відсутність конфлікту інтересів.

Список літератури:

1. Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce. (n.d.). *Post-Quantum Cryptography | CSRC | CSRC*. Retrieved from https://csrc.nist.gov/projects/post-quantum-cryptography
2. Інформаційні технології. Криптографічний захист інформації. Алгоритми асиметричного шифрування та інкапсуляції ключів: ДСТУ 8961:2019. (2019). Київ: Держспоживстандарт України.
3. Інформаційні технології. Криптографічний захист інформації. Алгоритм електронного підпису на алгебраїчних решітках із відхилами: ДСТУ 9212:2023. (2023). Київ: Держспоживстандарт України.
4. Acar, A., Aksu, H., Uluagac, A. S., & Conti, M. (2018). A survey on homomorphic encryption schemes. *ACM Computing Surveys*, 51(4), 1–35. https://doi.org/10.1145/3214303
5. Albrecht, M. R., Göpfert, F., Virdia, F., & Wunderer, T. (2017). Revisiting the expected cost of solving USVP and applications to LWE. *In Lecture notes in computer science* (pp. 297–322). https://doi.org/10.1007/978-3-319-70694-8_11
6. Albrecht, M. R., Bai, S., Li, J., & Rowell, J. (2021). Lattice Reduction with Approximate Enumeration Oracles. *In Lecture notes in computer science* (pp. 732–759). https://doi.org/10.1007/978-3-030-84245-1_25
7. Chen, Y., & Nguyen, P. Q. (2011). BKZ 2.0: Better Lattice Security Estimates. *In Lecture notes in computer science* (pp. 1–20). https://doi.org/10.1007/978-3-642-25385-0_1
8. Li, J., & Nguyen, P. Q. (2022, March 5). A complete analysis of the BKZ Lattice Reduction algorithm. Retrieved from https://eprint.iacr.org/2020/1237
9. Nguyen, P. Q., & Valle, B. (2010). The LLL algorithm. *Information security and cryptography.* https://doi.org/10.1007/978-3-642-02295-1
10. Schnorr, C. P. (2003). Lattice reduction by random sampling and birthday methods. *In Lecture notes in computer science* (pp. 145–156). https://doi.org/10.1007/3-540-36494-3_14

11. Alkim, E., Ducas, L., Pöppelmann, T., & Schwabe, P. (2019, July 10). Post-quantum key exchange - a new hope. Retrieved from https://eprint.iacr.org/2015/1092

THE ANALYSIS OF HERMITE FACTOR OF BKZ ALGORITHM ON SMALL LATTICES

Ivan Gorbenko[1], Doctor of Sciences (Engineering), Full Prof.; e-mail: i.d.gorbenko@karazin.ua; ORCID: https://orcid.org/0000-0003-4616-3449
Serhii Kandii[1], Ph.D. Student, Department of Security of Information Systems and Technologies; e-mail: sergeykandy@gmail.com; ORCID: https://orcid.org/0000-0003-0552-8341
[1] *V. N. Karazin Kharkiv National University, Ukraine*
Manuscript was received April 1, 2024; Received after review May 2, 2024; Accepted June 3, 2024

Abstract. Lattice cryptography is one of the promising directions in modern cryptography research. Digital signatures and key encapsulation mechanisms on lattices have already been used in practice. In the future, such quantum-resistant transformations on lattices replace all standards that are not resistant to attacks on quantum computers. This makes the analysis of their security extremely relevant. Analysis of the security of cryptographic transformations on lattices is often reduced to the estimation of the minimum block size in the lattice reduction algorithm. For the expansion of small vectors, a reduction algorithm can be obtained for a given block size, the GSA model is often used, which uses the so-called Hermitian factor to predict the size of the vectors that the lattice reduction algorithm can obtain given the parameters. Asymptotic formulas have been developed to evaluate it in practice, but the question of their accuracy on cryptographic lattices has not been fully investigated. The work obtained estimates of the accuracy of the existing asymptotic estimates of the Hermite factor for lattices of sizes 120, 145, 170 for the classical BKZ algorithm. Research was conducted using the fpylll library. It was shown that the existing estimators are equivalent from a practical point of view and have a sufficiently small root mean square deviation from the true values. A formula was obtained that binds the root-mean-square error of approximation of the Hermit factor to the cryptographic parameters of lattices. The obtained results are useful for refining the security assessments of existing cryptographic transformations.

Keywords: *quantum-resistant cryptography; lattice cryptography; the Hermite factor, BKZ, GSA*

Conflicts of Interest: the authors declare no conflict of interest.

References

1. Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce. (n.d.). Post-Quantum Cryptography | CSRC | CSRC. Retrieved from https://csrc.nist.gov/projects/post-quantum-cryptography
2. Information technologies. Cryptographic protection of information. Algorithms for asymmetric encryption and key encapsulation: DSTU 8961:2019. (2019). Kiev: State Committee for Standardization of Ukraine.
3. Information technologies. Cryptographic protection of information. Algorithm for electronic signature on algebraic lattices with wicks: DSTU 9212:2023. (2023). Kiev: State Committee for Standardization of Ukraine.
4. Acar, A., Aksu, H., Uluagac, A. S., & Conti, M. (2018). A survey on homomorphic encryption schemes. *ACM Computing Surveys*, 51(4), 1–35. https://doi.org/10.1145/3214303

5. Albrecht, M. R., Göpfert, F., Virdia, F., & Wunderer, T. (2017). Revisiting the expected cost of solving USVP and applications to LWE. In Lecture notes in computer science (pp. 297–322). https://doi.org/10.1007/978-3-319-70694-8_11
6. Albrecht, M. R., Bai, S., Li, J., & Rowell, J. (2021). Lattice Reduction with Approximate Enumeration Oracles. In Lecture notes in computer science (pp. 732–759). https://doi.org/10.1007/978-3-030- 84245-1_25
7. Chen, Y., & Nguyen, P. Q. (2011). BKZ 2.0: Better Lattice Security Estimates. In Lecture notes in computer science (pp. 1–20). https://doi.org/10.1007/978-3-642-25385-0_1
8. Li, J., & Nguyen, P. Q. (2022, March 5). A complete analysis of the BKZ Lattice Reduction algorithm. Retrieved from https://eprint.iacr.org/2020/1237
9. Nguyen, P. Q., & Valle, B. (2010). The LLL algorithm. Information security and cryptography. https://doi.org/10.1007/978-3-642-02295-1
10. Schnorr, C. P. (2003). Lattice reduction by random sampling and birthday methods. In Lecture notes in computer science (pp. 145–156). https://doi.org/10.1007/3-540-36494-3_14
11. Alkim, E., Ducas, L., Pöppelmann, T., & Schwabe, P. (2019, July 10). Post-quantum key exchange - a new hope. Retrieved from https://eprint.iacr.org/2015/1092