УДК 004.056.55 **DOI:10.30837/rt.2020.3.202.05**

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

ГЕНЕРАЦІЯ ЗАГАЛЬНОСИСТЕМНИХ ПАРАМЕТРІВ ДЛЯ КРИПТОСИСТЕМИ FALCON ДЛЯ 256, 384, 512 БІТ БЕЗПЕКИ

Вступ

В останнє десятиріччя спостерігається практично завершальне створення математичних основ та програмного забезпечення квантового комп'ютера [1]. Також спостерігається стійкий прогрес у створенні безпосередньо квантових комп'ютерів різного призначення та різних можливостей [2]. При цьому особлива увага приділяється реалізації великомасштабних квантових комп'ютерів, що призначаються для криптоаналізу існуючих криптосистем з відкритим ключем – електронних підписів, асиметричних шифрів та криптографічних протоколів різного призначення [1 – 3]. Певні сумніви є і щодо симетричних криптоперетворень блокового та потокового шифрування, але збільшення при їх використанні розмірів параметрів та ключів за нинішніх поглядів дозволяє забезпечити криптографічний захист на далеку перспективу. Зважаючи на вказане, Національний інститут стандартів і технологій (NIST) США знаходиться в процесі вибору криптографічних алгоритмів з відкритим ключем через проведення відкритого конкурсу. Прийняті в майбутньому нові стандарти криптографії з відкритим ключем визначатимуть один або кілька додаткових алгоритмів для цифрових підписів, асиметричного шифрування та встановлення ключів. Вважається, що ці стандартизовані алгоритми будуть здатні захистити конфіденційну інформацію уряду США в доступному для огляду майбутньому, в тому числі після появи квантових комп'ютерів. Таким чином, однією з основних проблем сучасної криптографії є створення стандартизованих криптографічних схем, які були б безпечними у постквантовий період.

На світовому рівні зусилля значного числа теоретичних криптологів, математиків та криптологів-практиків зосереджені на відкритому конкурсі NIST PQC [2]. Одним із основних завдань конкурсу є розробка та прийняття постквантового чи постквантових стандартів електронного (цифрового) підпису (ЕП). Фіналістами другого етапу конкурсу NIST стали три механізми ЕП – CRYSTALS-DILITHIUM, FALCON та Rainbow. Окрім цього, були визначені три альтернативних кандидати, які потребують більш детальних досліджень. У цілому всебічний аналіз фіналістів є важливою задачею для криптологів світової криптоспільноти. Причому, безпека, тобто доведення криптографічної стійкості двох кандидатів-фіналістів, на стандарт ЕП – CRYSTALS-DILITHIUM та FALCON, ґрунтується на проблемах з теорії та практики алгебраїчних решіток [1, 3].

Дослідження показали, що серед схем ЕП на решітках дещо відрізняється від інших кандидатів та має перспективи щодо прийняття в якості стандарту FALCON [1, 4]. Основним та домінуючим підходом до проєктування механізму ЕП FALCON є використання перетворення Фіата – Шаміра з перериваннями [5, 6]. Його перевагою є доказова стійкість в межах моделі квантового випадкового оракула. Але його аналізу присвячено значно менше робіт, ніж, наприклад, щодо CRYSTALS-DILITHIUM. Крім того, при проєктуванні ЕП FALCON були прийняті обмеження щодо рівнів безпеки, максимально 256 біт проти класичного та 128 біт проти квантового криптоаналізу. Ці обмеження, на наш погляд, пов'язані зі складністю обчислення загальносистемних параметрів, а також з суттєвим впливом їх збільшення параметрів на швидкодію ЕП. Тобто, для безпечного використання ЕП FALCON повинні бути знайдені набори загальносистемних параметрів, за яких забезпечується стійкість до всіх відомих та потенційних атак. В процесі формування вимог до ЕП NIST у рамках конкурсу був зацікавлений тільки в наборах загальносистемних параметрів до 256 біт класичної безпеки включно. Проте, на нашу думку, на перспективу доцільним є забезпечення не менше 384 і 512 біт безпеки проти класичного криптоаналізу та не менше 192 та 256 біт безпеки проти квантово-

го криптоаналізу. Але, як показали дослідження, як з точки зору теорії так і практики, генерація загальносистемних параметрів для використання 384 і 512 біт безпеки проти класичного криптоаналізу та 192 та 256 біт безпеки проти квантового криптоаналізу.

Метою статті є класифікація та первинний аналіз відомих атак на криптосистему ЕП FALCON, встановлення обмежень та розробка практичних алгоритмів обчислення (генерації) загальносистемних параметрів для забезпечення не менше 256, 384 і 512 біт безпеки проти класичного та не менше 128, 192 та 256 біт проти квантового криптоаналізу.

1. Сутність механізму ЕП FALCON

Проєкт ЕП FALCON [1, 4] у цілому є механізмом (схемою) ЕП на алгебраїчних решітках. Вважається, що безпека ЕП FALCON ґрунтується на складності проблеми SIS (коротке ціле рішення) над решітками NTRU, а докази безпеки наведені як у випадковій моделі оракула (ROM), так і в моделі QROM [5]. Як показують дослідження, механізм ЕП FALCON є складнішим для впровадження, наприклад ніж DILITHIUM[1]. Він вимагає використання деревних структур даних, операцій з плаваючою крапкою та випадкової вибірки з декількох дискретних гауссових розподілів.

Однією з основних переваг FALCON є те, що він забезпечує у порівнянні з ЕП CRYSTALS-DILITHIUM та Rainbow найменші розміри відкритого ключа та ЕП. Безпосередньо ЕП FALCON також ефективний, хоча генерація ключів відбувається повільніше [1]. Також ЕП FALCON можуть легко вводитись існуючі стандартизовані криптографічні протоколи та програми, що в середньому забезпечує хороші загальні показники.

В основу механізму ЕП FALCON покладено перетворення фреймворк GPV [7], в якому відкритим ключем є базис $A \in \mathbb{Z}_q^{n \times m}$ решітки Λ. У якості особистого (закритого) ключа використовується редукований базис $B \in \mathbb{Z}_q^{m \times m}$ дуальної решітки $\Lambda^{\perp}$. В механізмі ЕП FALCON використовуються NTRU решітки виду [4]:

$$A = \begin{bmatrix} 1 & h \\ 0 & q \end{bmatrix}, B = \begin{bmatrix} f & g \\ F & G \end{bmatrix}, \quad (1)$$

де ключові дані f, g, h, F, G є поліномами у кільці поліномів $\mathbb{Z}_q[X]/(\phi(X))$. Щодо них виконується порівняння

$$fG - gF = q \bmod \phi. \quad (2)$$

Якщо f, g є малими поліномами, то задача вирішення рівняння (2) стає складною. Використання структурованих решіток дає змогу зменшити розмір ключів та передавати не всю матрицю базису, а лише поліноми, що її формують.

При виробленні ЕП для повідомлення m застосовується пара поліномів (s_1, s_2), для якої виконується рівність

$$s_1 + s_2 h = H(r \| m) \quad (3)$$

де r – сіль(початкова ентропія) ключа, H – деяка криптографічна геш-функція, що відображає бінарні данні на вектори. Таких (s_1, s_2) існує багато і знайти їх неважко, проте якщо ввести обмеження $\|s\| < \beta$, де β має достатньо мале значення, то задача стає важкою і зводиться до проблеми *SIS*. Таким чином, основною проблемою, на якій ґрунтується безпека механізму ЕП FALCON, є SIS на NTRU-решітках, тобто знаходження короткого цілого рішення (Short Integer Solution).

2. Аналіз атак на ЕП FALCON

Перетворення GPV [7], яке застосовується в ЕП FALCON**,** вимагає щоб геш-функція H була захищена від колізій. Це означає, що розмір солі в бітах повинен бути не меншим за 2λ, де λ – рівень безпеки, що вимагається. Проте, за умовами конкурсу NIST [8] кількість запитів на вироблення ЕП (signature queries) є не більшою за $q_s = 2^{64}$, що дає розмір $\lambda + \log_2(q_s)$. Тобто, для 5-7 рівнів безпеки це дає значення, що наведені в табл. 1.

Таблиця 1

Розмір в бітах солі r

Безпека	Розмір r	Розмір r з врахуванням вимог NIST
256	512	320
384	768	448
512	1024	576

Аналіз показав, що основними атаками ЕП FALCON є атаки на відновлення особистого (секретного) ключ з відкритого ключа та атаки на підробку ЕП. Розглянемо ці атаки.

2.1. Атаки на відновлення особистого (секретного) ключа з відкритого ключа

Атаки на відновлення особистого (секретного) ключа з відкритого ключа можуть зводиться до вирішення проблеми NTRU [4]. У ряді схем, стійкість яких ґрунтуються на проблемі NTRU, поліноми f, g мають коефіцієнти з множини значень $\{0,1,-1\}$. Це робить можливим реалізувати різні комбінаторні атаки. Наприклад, для ДСТУ 8961:2019 «Скеля» найефективнішою атакою є гібридна атака, яка знаходить частину вектора комбінаторними шляхами. Для Falcon такі атаки неможливі, оскільки поліноми f, g змінюються (точніше, семплуються) згідно з нормальним розподілом з заданими параметрами. За даного перетворення простір можливих значень поліномів збільшується настільки, що застосування комбінаторних методів стає неефективним. Залишається прямий шлях відновлення особистого ключа з відкритого засобом редукції базису решітки. При цьому, чим менші значення має норма найменшого вектора (f, g), тим більша криптостійкість системи. В криптосистемі Falcon поліноми генеруються над полем

$$\mathbb{Z}_q[X]/(\phi(x)), \deg(\phi) = n$$

з математичним очікуванням рівним 0. Перетворення спираються на результати роботи [12] , у якій детально досліджувалися можливості застосування алгоритмів семплування нормально розподілених величин. В [12] було показано, що алгоритм семплування Клейна може давати вектори розміру $\approx \sqrt{\frac{qe}{2}}$, що є дуже близьким до теоретичного мінімуму $\sqrt{q}$. Відповідно, щоб отримати такий розмір, кожний коефіцієнт отримується з розподілу з середньоквадратичним відхиленням

$$\sigma' = \sqrt{\frac{qe}{2}} * \frac{1}{\sqrt{2n}}.$$

Згідно з [9] найменший вектор може бути знайдений, якщо його проекція на простір, що натягнутий на перші B векторів $b_1^*, b_2^*, ..., b_B^*$ буде менша за b_{2n-B}^*. Згідно з [9, 12] ця проекція може бути оцінена як

$$\sqrt{\gamma_B} * \det(\Lambda_{[b_1^*,...,b_B^*]}) \approx \sqrt{\frac{3}{4}} * \sigma' \sqrt{B} = \sqrt{\frac{3}{4}} * \sqrt{\frac{qe}{2}} * \frac{1}{\sqrt{2n}} * \sqrt{B} \quad (4)$$

Водночас, згідно з [9, 12] b_{2n-B}^* може бути оцінений як

$$\left\|b^*_{2n-B}\right\| \approx GH(B)^{\frac{2n+1-2(2n-B)}{2(B-1)}} \det(\Lambda)^{\frac{1}{2n}} = GH(B)^{\frac{2B-2n+1}{2B-2}} \sqrt{q} = \left(\frac{B}{2\pi e}\right)^{\frac{2B-2n+1}{2B-2}} \sqrt{q} \quad (5)$$

Таким чином, маємо умову щоб:

$$\left(\frac{B}{2\pi e}\right)^{\frac{2B-2n+1}{2B-2}} \sqrt{q} < \sqrt{\frac{3eB}{8n}} * \sqrt{q}\,. \quad (6)$$

Далі, завдяки вибору $\sigma' = \sqrt{\frac{qe}{2}} * \frac{1}{\sqrt{2n}}$ з обох сторін рівняння маємо множник $\sqrt{q}$, який можна скоротити. Тому умова захисту від атак на відновлення особистого ключа з відкритого шляхом редукції виглядає наступним чином:

$$\left(\frac{B}{2\pi e}\right)^{\frac{2B-2n+1}{2B-2}} < \sqrt{\frac{3eB}{8n}} \quad (7)$$

2.2. Атаки на підробку ЕП

Атаки на безпосередньо підробку ЕП можуть бути найбільш загрозливими. Тому іншим вектором атаки є атака підробки ЕП. При реалізації такої атаки потрібно знайти достатньо короткий вектор s. Відповідно, це можливо зробити, редукувавши базис так, щоб виконувалася умова

$$\left\|b^*_1\right\| < \beta \quad (8)$$

Причому оцінити $\left\|b^*_1\right\|$ можливо таким же чином, що і у попередньому випадку, тобто у такій послідовності:

$$\left\|b^*_1\right\| \approx GH(B)^{\frac{2n+1-2}{2(B-1)}} \det(\Lambda)^{\frac{1}{2n}} = GH(B)^{\frac{2n-1}{2B-2}} \sqrt{q} = \left(\frac{B}{2\pi e}\right)^{\frac{2n-1}{2B-2}} \sqrt{q}\,. \quad (9)$$

Отримуємо, що умовою захисту від атак на підробку підпису є

$$\left(\frac{B}{2\pi e}\right)^{\frac{2n-1}{2B-2}} \sqrt{q} < \beta \quad (10)$$

Для практичного прийняття рішення необхідно визначитись щодо того, як обирати параметр β. Розробники ЕП Falcon пропонують використовувати значення $\sigma = 1.55\sqrt{q}$ для полінома $\phi = x^n + 1$ і $\sigma = 1.32 * 2^{1/4} * \sqrt{q}$ для полінома $\phi = x^n - x^{n/2} - 1$. Такий вибір σ базується на результатах роботи [10] і параметр β для полінома $\phi = x^n + 1$ обчислюється як:

$$\beta = 1.2 * \sigma \sqrt{2nq}\,. \quad (11)$$

Для полінома $x^n - x^{n/2} - 1$ β обчислюється таким чином:

$$\beta^2 = \frac{\left(1.2 * \sigma * 2n\sqrt{q}\right)^2}{n}. \quad (12)$$

Формули відрізняються тому, що для полінома $x^n - x^{n/2} - 1$ замість L2 норми обчислення виконуються за допомогою embedding norm під час генерації ключів та підпису.

Якщо підставити значення β у рівняння для оцінки захищеності від атак на підробку підпису, то також обидві сторони будуть пропорційні значенню $\sqrt{q}$. Таким чином, середньоквадратичні відхилиння при семплуванні поліномів з нормального розподілу підібрані таким чином, щоб від q складність атаки не залежала. Проте на параметр q існує безліч інших обмежень, які впливають на його вибір.

Параметр q обирається згідно наступних міркувань [4]:

- для захисту від алгебраїчних атак q має бути простим числом;

- якщо q буде занадто малим (порядку $q \approx n$), то будуть можливі BKW атаки;

- якщо q буде занадто великим ($q \approx n^{2.83}$), то будуть можливі атаки на підполе;

- якщо використовується поле $x^n + 1$, то для реалізації ефективного множення повинне виконуватися рівняння $q \equiv 1 \bmod 2n$;

- якщо використовується поле $x^n - x^{n/2} - 1$, то для реалізації ефективного множення повинне виконуватися рівняння $q \equiv 1 \bmod 3n$.

Примітка: Стійкість найкращого алгоритму пошуку найменшого вектору оцінюється як 2 ^ 0.292B, де B – розмір блоку при редукції. Якщо при криптоаналізі застосовувати алгоритм Гровера, то нижня оцінка класичної стійкості в 256 біт складає 2 ^ 0.265B квантової стійкості (при класичній стійкості в 256 біт. Тому, для ЕП на решітках квантова стійкість при класичній стійкості 256 біт набагато більше ніж 128 біт.

2.3. Точність арифметики з плаваючою крапкою

Останнім невизначеним параметром, який необхідно вибрати для забезпечення рівнів стійкості 384 та 512 біт, є необхідна точність виконання операцій у арифметиці з плаваючою крапкою. Розробники Falcon для теоретичної оцінки використовували роботу [10], проте точність обиралася з практичних експериментів. З роботи [10] видно, що рівень безпеки λ слабо впливає на потрібну точність. Основний вплив має кількість запитів на підпис $q_s = 2^{64}$, тому є надія, що 64 бітів буде достатньо. Проте, це питання виходить за межі даної статті і є предметом подальшого дослідження.

Також до проблемного питання щодо недоліку ЕП FALCON необхідно віднести використання арифметики з плаваючою крапкою. Разом з використанням деревоподібних структур це ускладнює аналіз схеми до атак по стороннім каналам. Іншою проблемою є складність реалізації на малоресурсних пристроях.

3. Генерація параметрів для 256, 384, 512 біт стійкості

У цілому, якщо підсумувати наведене вище, то знайти параметри n, q, β можна з системи нерівностей (13) та умов (1) – (5):

$$\begin{cases} \left(\frac{B}{2\pi e}\right)^{\frac{2n-1}{2B-2}} \sqrt{q} < \beta \\ \left(\frac{B}{2\pi e}\right)^{\frac{2B-2n+1}{2B-2}} < \sqrt{\frac{3eB}{8n}} \end{cases} \tag{13}$$

де параметр β визначається як $\beta = 1.2 * \sigma \sqrt{2nq}$, якщо використовується поліном $x^n + 1$ і $\beta^2 = \frac{\left(1.2 * \sigma * 2n\sqrt{q}\right)^2}{n}$, якщо використовується поліном $x^n - x^{n/2} - 1$.

На основі (13) розроблено програмне забезпечення, з використанням якого були обчислені параметри n, q та β^2 ЕП FALCON для відповідних поліномів для 256, 384, 512 біт безпеки, що наведені в табл. 2.

Таблиця 2

Основні загальносистемні параметри
для 256, 384, 512 біт безпеки

Безпека	$\phi(x)$	n	q	β^2
256	x^n+1	1024	12289	87070769
384	$x^n-x^{n/2}-1$	1536	18433	174141539
512	x^n+1	2048	12289	200928983

4. Отриману криптостійкість наведено в табл. 3. Криптостійкість наведено у форматі «стійкість» λ /розмір блоку.

Таблиця 3

Криптостійкість до атак на основі редукції решіток

Безпека	Стійкість до відновлення ключа (класична)	Стійкість до відновлення ключа (квантова)	Стійкість до підробки підпису (класична)	Стійкість до підробки підпису (квантова)
256	273/936	248/936	269/922	244/922
384	413/1417	375/1417	430/1474	390/1474
512	554/1899	503/1899	599/2053	544/2053

Оцінки криптостійкості отримувалися з розміру блоку як 0,265B та 0,292B. Такий підхід вважається класичним і використовувався авторами Dilithium і авторами Falcon. Проте, оцінки є досить грубими. Якщо використати підхід як в qTesla, то значення криптостійкості при тих же самих параметрах буде суттєво більшим. В табл. 3 для квантових атак для 256 і 512 sn отримані значення є трохи меншими за необхідні, проте через грубість оцінки можна вважати, що вони досягають потрібного порога. Для 256 біт згенеровані параметри співпадають із параметрами, згенерованими авторами Falcon для 256 біт рівня криптостійкості.

Висновки

1. Одним із основних завдань конкурсу NIST США є розробка та прийняття постквантового чи постквантових стандартів ЕП. Фіналістами другого етапу конкурсу NIST стали три механізми ЕП – CRYSTALS-DILITHIUM, FALCON та Rainbow. Причому, подальше вирішення проблеми безпеки, тобто доведення криптографічної стійкості двох кандидатів-фіналістів, на стандарт ЕП FALCON, може ґрунтується на проблемах теорії та практики алгебраїчних решіток.

2. Схеми цифрового підпису на решітках є основними претендентами на перемогу в конкурсі NIST PQC. Тому, їх подальший детальний аналіз та порівняння щодо основних характеристик стійкості є першочерговою задачею. Схема FALCON, як фіналіст другого етапу, потребує особливої уваги, оскільки має нетиповий дизайн, що використовує арифметику з плаваючою крапкою.

3. Криптостійкість ЕП FALCON залежить від двох добре вивчених – NTRU та SIS – проблем. Завдяки використанню семплування особистих ключів застосуванням нормального розподілу, гібридні атаки для зламу недоцільні, а NTRU атаки можуть зводиться до прямої атаки редукцією решітки. Також SIS проблема, в свою чергу, може вирішуватись за допомогою редукції решітки.

4. Завдяки використанню циклотомічних поліномів розробники проєкту FALCON досягли гарної швидкодії вироблення та перевірки ЕП з використанням бінарних та тернарних дерев. Проте недоліком такого підходу є недостатня гнучкість при генерації загальносистемних параметрів. Криптостійкість здебільшого залежить від параметра n, який має або бути ступенем двійки, або невеликим кратним до ступеня двійки. Можливі значення параметра лежать у невеликій множині, що сильно обмежує вибір параметрів.

5. Криптостійкість FALCON сильно залежить від того, наскільки малі вектори можливо семплувати з нормального розподілу. Розробники FALCON детально вивчили відомі алгоритми та обрали алгоритм Клейна, оскільки він у порівнянні з іншими алгоритмами дає найменші вектори. У подальшому дослідження та розробка нових алгоритмів семплування можуть дати можливість зменшити розміри ЕП та підвищити швидкодію.

6. До основного проблемного питання щодо недоліку ЕП FALCON необхідно віднести використання арифметики з плаваючою крапкою. Разом з використанням деревоподібних структур це ускладнює аналіз схеми до атак по стороннім каналам. Іншою проблемою є складність реалізації на малоресурсних пристроях.

7. Основним результатом, що отриманий в процесі досліджень та наведений у цій статті, є співвідношення (13), з використанням якого були обчислені та запропоновані набори загальносистемних параметрів для рівнів безпеки 256, 384, 512 біт.

8. Необхідно відмітити, що для безпеки 256 біт результат збігається з запропонованим розробниками проєкту ЕП FALCON.

9. Для отримання оцінок щодо складності задачі SIS та NTRU було використано зведення проблеми до редукції решіток. Причому через недостатню гнучкість схеми для 384 біт класичної стійкості був використаний поліном $x^n - x^{n/2} - 1$.

Список літератури:

1. *Gorjan 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, Angela Robinson, Daniel Smith-Tone // 22 July 2020. Режим доступу: https://doi.org/10.6028/NIST.IR.8309.
2. Cryptography Standardization Process. Electronic resource]. Access mode: http://www.nist.gov/pqcrypto.
3. Post-Quantum Cryptography. Round 2 Submissions. [Electronic resource]. Access mode: https://csrc.nist.gov/Projects/post-quantum-cryptography/round-2-submissions.
4. Falcon. [Electronic resource]. Access mode: https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions.
5. Eike Kiltz, Vadim Lyubashevsky, and Christian Schaffner. A concrete treatment of fiat-shamir signatures in the quantum random-oracle model. Cryptology ePrint Archive, Report 2017/916, 2017. [Electronic resource]. Access mode: http://eprint.iacr.org/2017/916.
6. Dominique Unruh. Post-quantum security of fiat-shamir // IACR Cryptology ePrintArchive, 2017:398, 2017.
7. Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and newcryptographic constructions // Richard E. Ladner and Cynthia Dwork, editors,40th ACM STOC,pages 197–206. ACM Press, May 2008.
8. 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
9. Daniele Micciancio and Michael Walter. Practical, predictable lattice basis reduction // Marc Fischlin and Jean-Sébastien Coron, editors,EUROCRYPT 2016, Part I, volume9665 ofLNCS, pages 820–849, Vienna, Austria, May 8–12, 2016. Springer, Heidelberg,Germany.
10. Thomas Prest. Sharper bounds in lattice-based cryptography using the Rényi divergence // Takagiand Peyrin [TP17], pages 347–374.
11. Martin R. Albrecht, Shi Bai, and Léo Ducas. A subfield lattice attack on overstretchedNTRU assumptions – cryptanalysis of some FHE and graded encoding schemes // Matthew Robshaw and Jonathan Katz, editors,CRYPTO 2016, Part I, volume 9814 ofLNCS, pages 153–178, Santa Barbara, CA, USA, August 14–18, 2016. Springer, Heidelberg, Germany.
12. Thomas Prest.Gaussian Sampling in Lattice-Based Cryptography // Theses, École NormaleSupérieure, December 2015

Надійшла до редколегії 14.08.2020

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, Україна, e-mail: GorbenkoI@iit.kharkov.ua, ORCID: https://orcid.org/0000-0003-4616-3449

Кандій Сергій Олександрович – Харківський національний університет імені В. Н. Каразіна, студент кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Україна, e-mail: kandy.sergey@yandex.ua

Єсіна Марина Віталіївна – канд. техн. наук, Харківський національний університет імені В. Н. Каразіна, старший викладач кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Україна, e-mail: rinayes20@gmail.com, ORCID: https://orcid.org/0000-0002-1252-7606

Острянська Єлизавета Вадимівна – Харківський національний університет імені В. Н. Каразіна, студент кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Україна, e-mail: antelizza@gmail.com