УДК 004.056.5 **DOI:10.30837/rt.2022.3.210.02**

Ю.І. ГОРБЕНКО, канд. техн. наук, С.О. КАНДІЙ

ПОРІВНЯННЯ АРГУМЕНТІВ БЕЗПЕКИ ПЕРСПЕКТИВНИХ МЕХАНІЗМІВ ІНКАПСУЛЯЦІЇ КЛЮЧІВ

Вступ

Постквантова криптографія є напрямом досліджень, що направлені на розробку та стандартизацію асиметричних криптографічних перетворень, які суттєво будуть захищені від квантових та класичних атак [1 – 3]. У 2016 році NIST США оголосили про початок конкурсу NIST PQC [1], метою якого є створення нових постквантових стандартів криптографічних перетворень. Наразі завершився третій етап цього конкурсу. Спеціалісти NIST обрали механізм інкапсуляції ключів CRYSTALS-Kyber [2] для стандартизації і ряд інших механізмів для подальшого вивчення у четвертому етапі. У той же час в Україні вже стандартизовано механізм інкапсуляції ключів ДСТУ 8961:2019 “Скеля” [3], а в європейській спільноті доволі популярним механізмом є FrodoKEM [4]. Таке різноманіття KEM робить актуальною проблему порівняння та аналізу безпеки цих механізмів.

Метою статті є порівняння теоретичних та практичних аргументів безпеки постквантових механізмів інкапсуляції ключів CRYSTALS-Kyber, FrodoKEM та ДСТУ 8961:2019 “Скеля”, а також розробка рекомендацій з їх використання у світовій на національній практиці.

1. Формальні визначення безпеки

Особливістю сучасної криптографії є те, що безпека кожної криптографічної схеми або протоколу підкріплюється формальними математичними доказами, які, звісно ж, не гарантують, що не існує атак взагалі, проте дозволяють гарантувати, що не існує атак певного виду, які формально визначені через модель атак [5]. Для практичних задач корисними є наступні моделі:

- *Модель атак на основі обраних відкритих текстів (CPA)* [6]. Супротивник обирає відкритий текст, а потім отримує відповідний зашифрований текст. Супротивник використовує отриману інформацію, щоб відновити відповідний відкритий текст для шифротексту, який раніше не бачив. Схеми шифрування з відкритим ключем є прикладом, коли супротивник може зашифрувати будь-яке повідомлення за своїм вибором під відкритим ключем жертви. Модель атак з адаптивно обраним відкритим текстом (CPA2) – це атака CPA, у якій вибір відкритого тексту супротивником може залежати від зашифрованого тексту, створеного під час попередніх шифрувань.
- *Модель атак на основі обраного шифротексту (CCA)* [7]. Під час атаки за допомогою обраного шифротексту супротивник може розшифрувати довільні зашифровані тексти, наприклад, за допомогою доступу до обладнання для дешифрування з надійно вбудованим ключем дешифрування. Мета полягає в тому, щоб вивести відкритий текст із раніше не баченого шифротексту. CCA має два спеціальні варіанти: у неадаптивній атаці на основі шифротексту (CCA1), яку також називають «атакою в обідній час» або «опівночі», зловмисник може мати доступ до системи лише протягом обмеженого часу або обмеженої кількості пар відкритий текст-зашифрований текст. Атаку називають неадаптивною, оскільки зловмисник не може адаптувати свої запити до оракула дешифрування відповідно до зашифрованого тексту виклику. У CCA1 зашифрований текст виклику надається після закінчення терміну дії можливості супротивника здійснювати вибрані запити зашифрованого тексту. Однак зловмисник може зробити адаптивні запити обраного зашифрованого тексту до того, як буде надано зашифрований текст виклику. В адаптивній атаці обраного зашифрованого тексту (CCA2), яка є сильнішою, ніж CCA1, зловмисник має доступ до оракула дешифрування

навіть після отримання зашифрованого тексту. У CCA2 запити супротивника до оракула дешифрування можуть залежати від зашифрованого тексту, але супротивник може не запитувати розшифрування самого зашифрованого тексту виклику.

Щоб застосовувати моделі атак для реальних схем та протоколів, необхідно ввести додаткові поняття, які дозволяють формалізувати визначення моделей CPA, CCA. Ідея поняття нерозрізнювальності (indistinguishability) [8] шифротекстів полягає у тому, що аналітик не може на практиці дізнатися будь-яку значну інформацію про відкритий текст, що лежить в основі зашифрованого тексту. Вважається, що схема має властивість нерозрізнювальності шифротекстів, якщо ймовірність того, що аналітик зможе дізнатися інформацію про відкритий текст, є незначною. Під «незначною» мається на увазі, що ймовірність зменшується зі збільшенням певного параметра безпеки λ швидше (починаючи від деякого λ_0), ніж будь-яка функція вигляду $|1/f(\lambda)|$, де $f(\lambda)$ – будь-який поліном.

На основі цього можливо визначити IND-CPA, IND-CCA1, IND-CCA2 безпеку для схем шифрування з відкритим ключем наступним чином [5]:

Нехай $П = (Gen, Enc, Dec)$ позначає схему шифрування з відкритим ключем, а $A = (A_1, A_2)$ позначає супротивника з двома підалгоритмами. Для атаки $atk \in \{cpa, cca1, cca2\}$ і параметра безпеки λ ймовірність успіху супротивника визначається як $Adv_{A,П}^{ind-atk}(n) = |\Pr[Exp_{A,П}^{ind-atk-1}(n) = 1] - \Pr[Exp_{A,П}^{ind-atk-0}(n) = 1]|$, для $b \in \{0,1\}$, експеримент $Exp_{A,П}^{ind-atk-b}(n) = b'$ визначається як

$$
\begin{array}{ccc}
(pk, sk) & \leftarrow & Gen(1^n) \\
(m_0, m_1, s) & \rightarrow & Gen(1^n) \\
b & \in_R & \{0,1\} \\
c & \leftarrow & Enc_{pk}(m_b) \\
b' & \leftarrow & A_2^{O_2}(m_0, m_1, s, c) \\
Повернути & b' &
\end{array}
$$

де для

$$
\begin{aligned}
&atk = cpa \Rightarrow O_1(\cdot) = \varepsilon, O_2(\cdot) = \varepsilon \\
&atk = cca1 \Rightarrow O_1(\cdot) = O_{Dec}(\cdot), O_2(\cdot) = \varepsilon \\
&atk = cca2 \Rightarrow O_1(\cdot) = O_{Dec}(\cdot), O_2(\cdot) = O_{Dec}(\cdot)
\end{aligned}
$$

Схема шифрування безпечна в сенсі IND-ATK, якщо $Adv_{A,П}^{ind-atk}(\cdot)$ є незначним у λ [9].

2. Ідеалізовані моделі безпеки

Довести безпеку криптографічних схем або протоколів доволі важко у IND-CPA/IND-CCA моделях через використання криптографічних геш-функцій. У тому, як геш-функція взаємодіє з повідомленням бо іншими змінними, можуть бути вразливості, навіть якщо сама геш-функція є криптографічно безпечною [10]. На практиці лише до невеликої кількості геш-функцій можливо застосувати необхідний аналіз. Для інших випадків застосовуються ідеалізовані моделі безпеки [5].

Популярним вибором є модель випадкового оракула (ROM) [10]. У цій моделі геш-функції замінюються на їх ідеалізований варіант – випадкових оракулів. Випадковий

оракул це функція, яка на кожен запит повертає істинно випадкове значення з рівномірного розподілу. Значення для кожного аргументу не повторюються. Звичайно, у моделі ROM, можливо довести захист не від всіх атак, проте доказ у моделі ROM є гарним аргументом безпеки.

Модель квантового випадкового оракула (QROM) [11] є аналогом ROM для квантових комп'ютерів. Квантовий супротивник, знаючи як реалізувати деяку функцію f у вигляді послідовності геймів, може реалізувати унітарний оператор, що асоційований до f і дозволяє робити запити до суперпозиції станів $f:\sum_x \alpha_x |x\rangle \mapsto \sum_x \alpha_x |x\rangle |f(x)\rangle$. У моделі QROM супротивник може реалізувати деякий невідомий оператор U_H, який визначений як

$$U_H : |x\rangle |y\rangle \mapsto |x\rangle |y \oplus H(x)\rangle, \quad (1)$$

де $H(x)$ – випадковий оракул. Ця модель є корисною, оскільки існують квантові атаки, що не використовують властивостей геш функцій [12]. Наприклад, багато класичних атак можливо прискорити за допомогою алгоритма Гровера. Проте, варто зауважити, що модель квантового оракула передбачає, що обчислення ведуться на стандартній квантовій машині Тьюринга і не враховує випадки адіабатичних обчислень та інших нестандартних моделей. За необхідності, звичайно ж, можна адаптувати для них QROM, проте цей напрям досліджень наразі майже не розвивається.

3. Складні проблеми у криптографії на решітках

Більшість схем шифрування з асиметричним ключем побудовані на нерозв'язності деяких складних проблем [13]. Під складністю проблеми у теоретико-числовому сенсі зазвичай розуміється складність вирішення найгіршого випадку. Для того щоб проблему можна було використовувати в криптографії, необхідна не тільки складність у найгіршому випадку, але й складність у середньому. Необхідно, щоб ймовірність того, що випадковий екземпляр проблеми можна швидко вирішити, була незначною [14]. У криптографії на решітках використовуються здебільшого проблеми, які мають редукції "від найгіршого до середнього" з проблемами теорії решіток, що є унікальною властивістю, яка з теоретичної точки зору, значно збільшує безпеку схем. Вперше така проблема, що має редукції "від найгіршого до середнього" з проблемами теорії решіток, була запропонована у 2005 році – проблема навчання з помилками (LWE) [15]. Для її формального визначення введемо поняття LWE-розподілу.

Нехай $s \in \mathbf{Z}_q^n$, χ-розподіл ймовірностей для помилок. LWE-розподіл $A_{s,\chi}$ над $\mathbf{Z}_q^n \times \mathbf{Z}_q$ формується через вибір $a \in \mathbf{Z}_q^n$ з рівномірного розподілу, $e \leftarrow \chi$ над $\mathbf{Z}$ та вихідною є пара $(a,b), b = \langle s, a \rangle + e \bmod q$.

Проблема $Search - LWE_{n,m,q,B,\chi}$ формулюється наступним чином. Нехай $s \in \mathbf{Z}_q^n$ обрано з деякого розподілу ймовірностей B. Дано m незалежно отриманих екземплярів $(a_1,b_1),...,(a_m,b_m) \in \mathbf{Z}_q^n \times \mathbf{Z}_q$ з LWE-розподілу $A_{s,\chi}$. Потрібно знайти s.

Проблема $Decision - LWE_{n,m,q,B,\chi}$ формулюється наступним чином. Нехай $s \in \mathbf{Z}_q^n$ обрано з деякого розподілу ймовірностей B. Дано m незалежно отриманих екземплярів $(a_1,b_1),...,(a_m,b_m) \in \mathbf{Z}_q^n \times \mathbf{Z}_q$ з LWE-розподілу $A_{s,\chi}$ або з рівномірного розподілу. Потрібно визначити, з якого саме розподілу були отримані екземпляри $(a_1,b_1),...,(a_m,b_m) \in \mathbf{Z}_q^n \times \mathbf{Z}_q$.

У $Search - LWE_{n,m,q,B,\chi}$ без втрати загальності можна вважати, що розподіли B, χ є нормальньним розподілом з параметром α (розподіл можливо звести до нормального за

допомогою саморедукції [16]). Надалі позначатимемо таку версію $Search-LWE$ як $Search-LWE_{n,m,q,\alpha}$

Існує як квантова, так і класична редукція від проблеми $GapSVP_\gamma$ до $Search-LWE_{n,m,q,\alpha}$. Проблема $GapSVP_\gamma$ визначається наступним чином. Нехай задано решітку Λ розмірності n та деякий вектор v. Необхідно визначити чи знаходиться найближчий до v вектор на решітці на відстані $(1,\gamma]$. Теоретико-числова складність $GapSVP_\gamma$ залежить від значення параметра γ. У табл. 1 зведені відомі результати про складність $GapSVP_\gamma$ в залежності від γ.

Таблиця 1

Складність $GapSVP_\gamma$

Значення параметра γ	Клас складності
$2^{(\log n)^{1-\varepsilon}}$	NP-складна
$\sqrt{n}$	$NP \cap coNP$
$poly(n)$	Невідомо. Найкращі алгоритми (BKZ і т.д.) дають експоненційний час роботи.
$2^{\sim n}$	P

Для $Search-LWE_{n,m,q,\alpha}$ відома наступна редукція. Нехай $n,q \geq 1$ – цілі числа, $\alpha \in (0,1)$, для якого виконується $\alpha q \geq 2\sqrt{n}$. Тоді існує квантова редукція від найгірших випадків n-мірного $GapSVP_{O(n/\alpha)}$ до $Search-LWE_{n,q,\alpha}$. Якщо $q \geq 2^{n/2}$, то існує також квантова редукція.

Ця редукція актуальна саме для тих випадків, що використовуються в криптографії. До LWE існує дуальна проблема – SIS, яка визначається наступним чином.

Нехай $n,m,q>0$ є цілими числами, $\beta>0$ – дійсне число. Дана матриця $A \in \mathbf{Z}_q^{n\times m}$ з рівномірного розподілу, необхідно знайти ненульовий вектор $z \in \mathbf{Z}^m$ з евклідовою нормою $\|z\| \leq \beta$, для якого виконується $Az = 0 \in \mathbf{Z}_q^n$.

Для $SIS_{n,m,q,\beta}$ також існує редукція від найгіршого до середнього з $GapSVP$, проте більш важлива редукція $SIS_{n,m,q,\beta}$ до іншої складної проблеми з теорії решіток – $SIVP_\gamma$, яка полягає у знаходженні n лінійно незалежних векторів на решітці, для яких виконується $\|b_i\| \leq \gamma\lambda_i(\Lambda)$. Для будь-яких поліноміально обмежених m,β та простого $q \geq \beta\omega(\sqrt{n\log n})$ проблема $SIS_{m,m,q,\beta}$ така ж складна, як і $SIVP_\gamma$ з фактором $\gamma = \beta O(\sqrt{n})$.

Існує багато поліноміальних редукцій для різноманітних проблем на решітках. Вони утворюють складний ландшафт. Базові проблеми та деякі відомі редукції [17] зображено на рис. 1.

Популярною модифікацією є LWE та SIS на структурованих решітках [18]. Структурованість додається завдяки використанню елементів певного поля $R_q = \mathbf{Z}[X]/(f(x))$. За визначенням решітка є дискретною абелевою групою [19]. То ж, будь-яка підструктура у полі R_q, що є дискретною абелевою групою, може бути розглянута як решітка. Наприклад, розглянемо ідеал $\langle a \rangle$ для елемента $a \in R_q$. Кожен елемент в цьому ідеалі має вигляд $a \cdot s, s \in R_q$. Цей ідеал може бути вкладений у Евклідовий простір за допомогою звичайного коефіцієнтного вкладення:

$$Vec(a_0 + a_1 x + ... + a_{n-1}x^{n-1}) \mapsto (a_0, a_1, ..., a_{n-1}). \quad (2)$$

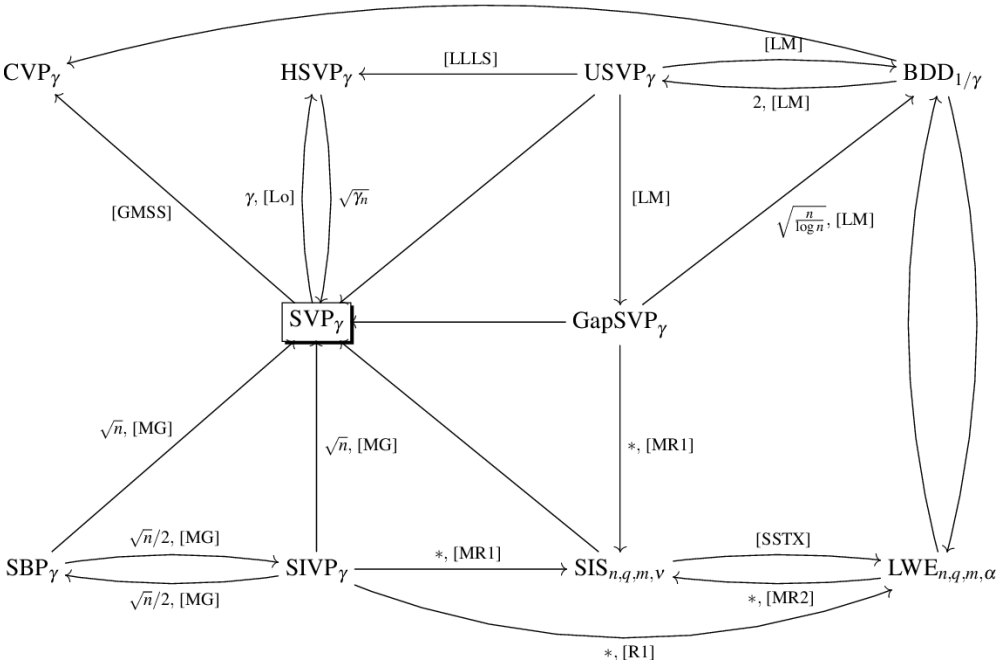

Рис. 1. Поліноміальні редукції між складними проблемами в теорії решіток

Тобто кожному поліному відповідає вектор його коефіцієнтів. Якщо правильно ввести операції додавання та множення на множині усіх векторів $(a_0, a_1, ..., a_{n-1})$, то зберігатиметься структура кільця. Операцію додавання можливо ввести покоординатно:

$$(b_0, b_1, ..., b_{n-1}) + (b_0, b_1, ..., b_{n-1}) = (a_0 + b_0 \bmod q, a_1 + b_1 \bmod q, ..., a_{n-1} + b_{n-1} \bmod q)$$

Множення можливо ввести наступним чином:

$$rot(a) \cdot (b_0, b_1, ..., b_{n-1}) = (c_0 \bmod q, c_1 \bmod q, ..., c_{n-1} \bmod q), \tag{3}$$

де $rot(a)$ є матрицею $n \times n$, яка задається як

$$rot(a) = \begin{pmatrix} Vec(a \bmod f(x)) \\ Vec(a \cdot x \bmod f(x)) \\ \cdots \\ Vec(a \cdot x^{n-1} \bmod f(x)) \end{pmatrix} \tag{4}$$

Фактично $rot(a)$ задає систему з n лінійно незалежних векторів [19]. Оскільки усі елементи вектора $(b_0, b_1, ..., b_{n-1})$ є цілими числами, то маємо звичайну решітку у евклідовому просторі, яка є структурованою у тому сенсі, що базис $rot(a)$ має додаткову структуру ідеалу. Решітки з базисом вигляду

$$\begin{pmatrix} rot(a_1) \\ rot(a_2) \\ \cdots \\ rot(a_m) \end{pmatrix}, a_1, a_2 ..., a_m \in R_q \tag{5}$$

мають назву “ідеальні решітки”. Відповідні складні проблеми з теорії решіток позначаються з префіксом “Ideal-“: $Ideal - SIVP, Ideal - GapSVP, Ideal - SVP$, тощо. Відповідні версії LWE

та SIS мають назву Ring-LWE та Ring-SIS, які також мають відповідні редукції від $Ideal-SIVP, Ideal-GapSVP$. На жаль, виявилося, що $Ideal-SVP$ на квантовому комп'ютері може бути вирішений за поліноміальний час [20].

Наразі популярним узагальненням є Module-LWE (Module-SIS) [22], яке використовує структуру R_q-модуля. Така решітка має вигляд

$$\begin{pmatrix} rot(a_{1,1}) & rot(a_{1,2}) & \dots & rot(a_{1,m}) \\ rot(a_{2,1}) & rot(a_{2,2}) & \dots & rot(a_{2,m}) \\ \vdots & \vdots & \ddots & \vdots \\ rot(a_{m,1}) & rot(a_{m,2}) & \dots & rot(a_{m,m}) \end{pmatrix}, a_{i,j} \in R_q \quad (6)$$

Формальне визначення $Module-SIS_{R,m,k,q,\beta}$ наступне:

Нехай дано m векторів поліномів $a_1,...,a_m \in R_q^k$, що обрані з рівномірного розподілу. Розглянемо їх як стовпці матриці $A \in R_q^{m\times k}$. Необхідно знайти ненульовий вектор поліномів $z \in R_q^k$ з нормою $Az = 0$.

Відповідно визначення $Module-LWE_{R,m,k,q,B,\chi}$ наступне:

Нехай $s \in R_q^k$ – вектор поліномів, що обрано з деякого розподілу B. Дано m екземплярів $(a_1,b_1),...,(a_m,b_m) \in R_q^{m\times k}$. Необхідно визначити чи взяті вони з рівномірного розподілу, або з розподілу LWE $A_{R_q,s,\chi}$ над полем R_q.

Module-LWE також має редукції з $Module-SIVP, Module-GapSVP$ [23]. Наразі невідомо про безпосередні атаки на Module-LWE чи відповідні складні проблеми [2], проте існує поліноміальна редукція від Module-LWE до Ring-LWE, що фактично означає існування квантового поліноміального алгоритму для Module-LWE за певних параметрів [24]. Проте, за тих значень, за яких працює редукція, для криптографічних застосувань ця атака не є актуальною. Хоча сама наявність такої редукції є поганим знаком, проте для Module-LWE невідомо ефективних атак, що враховували модульну структуру решітки.

Існують також інші модифікації, які вносять додаткову структурованість: MP-LWE, Order-LWE, Poly-LWE, Cyclic-LWE, тощо. Гарний огляд існуючих варіантів LWE на структурованих решітках наведено в роботі [18]. Основною проблемою структурованих варіантів є те, що є невідомою складність проблем на таких структурованих решітках. У деякому сенсі, серед зазначених проблем на структурованих решітках найкращі докази має MP-LWE. Є багато редукцій різних проблем до MP-LWE, що є доволі сильним аргументом безпеки. Проте, на практиці, вона працює значно повільніше, то ж не набула популярності.

Варто окремо зазначити проблему Continuous-LWE [25], яка є нещодавньою розробкою та притягла до себе увагу багатьох дослідників. Вона має доволі сильні докази складності. Детальний огляд цієї проблеми виходить за межі цієї роботи, аналіз можливо знайти в роботі [25]. Окремою її особливістю є доказова захищеність від атак з використанням машинного навчання.

Дещо окремо від інших криптографічних проблем на решітках стоїть проблема NTRU [26]. Фактично, NTRU була першою проблемою на решітках, що дозволила створювати дійсно практичні криптографічні схеми та протоколи і має наступне формальне визначення:

Нехай q є цілим додатнім числом. Дано елемент $h \in R_q$ з деякого розподілу D, для якого виконується $h \cdot f = g \bmod q, (f, g) \in R^2, \|f\|, \|g\| \le \sqrt{q} / \gamma$.

У проблемі $Search - NTRU_{R,q,D,\gamma}$ необхідно знайти пару $(f, g) \in R^2$.

Щоб зрозуміти відношення проблеми NTRU до криптографії на решітках, розглянемо матриці

$$\begin{bmatrix} rot(1) & rot(h) \\ rot(0) & rot(q) \end{bmatrix}, \begin{bmatrix} rot(f) & rot(g) \\ rot(F) & rot(G) \end{bmatrix}, \tag{7}$$

де $F, G \in R_q$ задовольняють рівнянню $fG - gF = q$ у полі R_q. Ці матриці задають базис тієї ж самої решітки. Перший базис має великі значення елементів векторів, другий базис має малі значення, тому його можливо використовувати для вирішення складних задач на решітці за поліноміальний час, на відміну від першого.

Одним з недоліків проблеми NTRU є те, що вона, на відміну від LWE та SIS, не має редукцій від найгіршого до середнього від складних проблем з теорії решіток [1]. Нещодавно була знайдена редукція від найгіршого до найгіршого від Module-uSVP до NTRU [35]. Це є слабкішим результатом, проте той факт, що за більш ніж двадцять років NTRU не змогли вирішити за поліноміальний час у загальному випадку є практичним свідченням складності проблеми NTRU.

Криптографічні проблеми в теорії решіток на цьому не обмежуються. Це окремий напрямок досліджень у теоретичній криптографії, який має складний ландшафт. Це є величезною перевагою криптографії на решітках, оскільки інші напрямки досліджень не мають такого різноманіття та динамічності розвитку.

З теоретичної точки зору, захист проблем Module-LWE та NTRU обумовлений тим, що невідомий шлях до узагальнення технік, що використовувалися для вирішення Ideal-SVP через модульну структуру останніх. Більш того, ці техніки ґрунтуються на циклотомічних полях, що означає, що вибір нециклотомічного для цих проблем зробить цей клас квантових атак нерелевантним.

4. Механізми інкапсуляції ключів

Існують різні підходи до побудови механізмів інкапсуляції ключей. Найбільш поширеним є наступний алгоритм [1]:

- Обирається деяка складна проблема.
- Будується CPA-безпечна схема асиметричного шифрування на основі обраної проблеми.
- Застосовується перетворення, що доказово робить з CPA-безпечної схеми CCA-безпечний механізм інкапсуляції ключів.

CRYSTALS-Kyber, FrodoKEM та ДСТУ 8961:2019 “Скеля” побудовані саме за цим принципом. В табл. 2 наведені складні проблеми, на яких ґрунтуються ці схеми.

Таблиця 2

Порівняння складних проблем у перспективних КЕМ

	CRYSTALS-Kyber	FrodoKEM	ДСТУ 8961:2019 “Скеля”
Проблема	Module-LWE	LWE	NTRU
Поле	$\mathbf{Z}_q[X]/(X^n+1)$	-	$\mathbf{Z}_q[X]/(X^n - X - 1)$

ДСТУ 8961:2019 “Скеля” має доволі незвичайний вибір поля. Річ у тому, що на проблему NTRU в полі $\mathbf{Z}_q[X]/(X^n+1)$ існує серія атак, яка дозволяє вирішити проблему NTRU за поліноміальний час, використовуючи структуру підкілець [28]. Зауважимо, що зазначені атаки можливі тільки у випадку $q > O(n^3)$, який не є релевантним для ДСТУ 8961:2019 “Скеля”. Такі ситуації зустрічаються здебільшого тільки у схемах гомоморфного шифрування та більш екзотичних конструкціях. Поле $\mathbf{Z}_q[X]/(X^n - X - 1)$, яке використовується у ДСТУ 8961:2019, не має нетривіальних підкілець, що робить подібні атаки неможливими, навіть у випадку, якщо будуть знайдені розширення цих атак на випадок тих параметрів, що використовуються у ДСТУ 8961:2019. Додатково, вибір цього поля захищає від потенційного узагальнення технік, що використовувалися для вирішення Ideal-SVP за поліноміальний час. Можна сказати, що вибір поля $\mathbf{Z}_q[X]/(X^n - X - 1)$ є додатковим аргументом безпеки для випадку алгебраїчних та квантових атак.

FrodoKEM ґрунтується на проблемі LWE, що дає гарні докази безпеки, оскільки існують редукції до складних проблем в теорії решіток. Проте, з іншої сторони, це також означає наявність множення великих матриць у реалізації, що робить FrodoKEM повільним.

CRYSTALS-Kyber грунтується на проблемі Module-LWE. При цьому використовується поле $\mathbf{Z}_q[X]/(X^n+1)$. Такий вибір поля є стандартним для криптографії на решітках, оскільки воно дозволяє використовувати теоретико-числове перетворення для множення/ділення поліномів [2] і має гарні теоретичні властивості [22] у тому сенсі, що докази безпеки значно спрощуються. Багато доказів безпеки (здебільшого редукцій до складних проблем на модульних решітках) використовують властивості цього поля [16, 19, 22, 24]. CRYSTALS-Kyber має не такі сильні докази, як FrodoKEM, оскільки складність Module-* проблем, від яких Module-LWE має редукції, невідома. Проте, CRYSTALS-Kyber працює швидше, ніж FrodoKEM, що робить його гарним вибором для багатьох практичних застосувань, для яких FrodoKEM є відносно повільним.

Для того щоб з CPA безпечних схем асиметричного шифрування отримати CCA безпечні KEM, використовуються різновиди перетворення Фуджісакі – Окамото. У табл. 3 зібрана інформація щодо перетворень, що застосовуються у CRYSTALS-Kyber, FrodoKEM та ДСТУ 8961:2019 “Скеля”.

Таблиця 3

Порівняння CCA перетворень у перспективних KEM

	CRYSTALS-Kyber	FrodoKEM	ДСТУ 8961:2019 “Скеля”
Перетворення	Власна модифікація перетворення Фуджісакі – Окамото	Фуджісакі – Окамото з прямим відхиленням	Фуджісакі – Окамото з відхиленням
Докази у ROM	+ (сильний доказ)	+ (сильний доказ)	+/-
Докази у QROM	+	+	+/-

Усі KEM, що розглядаються, мають певні докази у QROM та ROM [2, 3, 4, 27], які можна віднести до них прямо чи непрямо, проте для ДСТУ 8961:2019 ситуація є дещо невизначеною у цьому сенсі. Публікацій, що аналізують саме ДСТУ 8961:2019 у моделях ROM чи QROM, не існує. З іншої сторони, ДСТУ 8961:2019 є модифікацією стандарта ANSI X9.98 [29] і відрізняється тільки іншим полем та алгоритмом формування малих поліномів [30]. У цілому, усі докази у QROM або ROM для ANSI X9.98, що не використовують структуру поля, є релевантними і для ДСТУ 8961:2019. Проте, комплексного аналізу стандарту x9.98 також є доволі мало. Особливо це стосується випадку QROM. Хоча окремі результати відомі, проте для ДСТУ 8961:2019 не вистачає комплексного вивчення у моделях ROM та QROM.

5. Атаки на перспективні КЕМ

Оскільки ДСТУ 8961:2019 ґрунтується на проблемі NTRU, то питання криптоаналізу так чи інакше пов'язане з редукцією відкритого базису:

$$\begin{bmatrix} rot(1) & rot(h) \\ rot(0) & rot(q) \end{bmatrix}. \tag{8}$$

Найкращою відомою атакою для ДСТУ 8961:2019 є гібридна атака [31], яка використовує той факт, що малі поліноми у ДСТУ 8961:2019 мають коефіцієнти з множини {0,1,-1}. Ідея полягає у тому, щоб проводити редукцію не усієї решітки, а лише певної підрешітки з r векторів, потім інші вектори знаходити комбінаторним перебором. Час атаки буде мінімізуватися, якщо час роботи редукції решітки та комбінаторного пошуку буде приблизно однаковим, що можливо зробити, якщо підібрати значення параметра r.

В [32] з використанням евристичних міркувань отримано формулу для трудомісткості комбінаторного етапу описаної атаки:

$$T_2(\delta, r) = \frac{2^{15} r!}{c_{-1}! c_1! (r - c_{-1} - c_1)!} \left(\binom{2c_{-1}}{c_{-1}} \binom{2c_1}{c_1} p^{|S|} \right)^{-1/2} \frac{1}{\tilde{p}}, \tag{9}$$

де

$$p = \prod_{i=1}^{2n-r+1} \left(1 - \frac{1}{r_i B\left(\frac{2n-r}{2}, \frac{1}{2}\right)} \int_{-r_i}^{-r_i} \int_{\max\{-1, z-r_i\}}^{z+r_i} (1-t^2)^{\frac{2n-r-2}{2}} \, dt \, dz \right), \tag{10}$$

$$|S| = 2 + 2(n-t-1) p_S, \tag{11}$$

$$p_S = \frac{p_{\text{NP}} \, 2^{-4c_1} r!}{(2c_{-1})! (2c_1)! (r - 2c_{-1} - 2c_1)!} \binom{n-r}{4t-4c_1} \binom{n}{2t}^{-1}, \tag{12}$$

$$p_{\text{NP}} = \prod_{i=1}^{2n-r+1} \left(1 - \frac{2}{r_i B\left(\frac{2n-r}{2}, \frac{1}{2}\right)} \int_{-1}^{\max\{-r_i, -1\}} (1-t^2)^{\frac{2n-r-2}{2}} \, dt \right), \tag{13}$$

$$\tilde{p} = 1 - (1 - p_S)^{n-t}. \tag{14}$$

У формулах (10), (13) $B(\cdot, \cdot)$ позначає бета-функцію Ойлера, а числа r_i визначаються за формулами

$$r_i = \frac{R_i(\delta)}{2l}, \; i \in \overline{1, 2n-r+1}, \tag{15}$$

де

$$R_i(\delta) = q, \text{ якщо } 1 \le i \le 2n - r + 1 - \mu;$$

$$R_i(\delta) = q^{-2(i-(2n-r+1-\mu)-1)+\mu} q^{\frac{\mu-(n-r)}{\mu}}, \text{ якщо } 2n - r + 1 - \mu < i \le 2n - r + 1,$$

$$\mu = \min\left\{2n - r + 1, \left\lfloor \sqrt{\frac{n-r}{\log_q \delta}} \right\rfloor\right\},\ \delta > 1.$$

Оцінка часу етапу редукції решітки буде розглянута в наступних розділах.

Для FrodoKEM найкращою відомою атакою є безпосередня редукція LWE решітки. LWE задається кортежом $(A,c) = (A, A*s+e) \in \mathbf{Z}_q^{m\times n} \times \mathbf{Z}_q^{m\times 1}$, з яким можна асоціювати решітку $L = \{Ax \bmod q : x \in \mathbf{Z}_q^m\}$. З означення решітки випливає, що вектор s належить решітці та є найближчим до вектора $As+e$ за умови, якщо вектор помилки має достатньо малі значення. Поширеним методом пошуку рішення задачі є алгоритм Бабаї [19]. Для вирішення проблеми алгоритм потребує поліноміальну кількість кроків, проте від того, наскільки якісно редукований базис решітки, залежить ймовірність знаходження правильного рішення. У випадку проблеми LWE відома наступна оцінка ймовірності [33]:

$$\prod_{i=0}^{m-1} erf\left(\frac{\|b_i^*\|\sqrt{\pi}}{2\alpha q}\right), \tag{16}$$

де $\|b_i^*\|$ є $l2$ нормою i-го базисного вектора решітки після процедури ортогоналізації за Граммом – Шмідтом; α, q є параметрами LWE, $erf(\cdot)$ – функція помилок.

Для максимізації ймовірності коректної роботи алгоритму необхідно мінімізувати значення $\|b_i^*\|$, що фактично означає редукцію базису решітки.

Атаку можна модифікувати. Замість пошуку вектора s на оригінальній решітці можна побудувати таку решітку, яка буде містити вектор $(s,e,1)$, і він буде найменшим унікальним вектором (задача uSVP) згідно з [2, 33]. Можливим варіантом такої решітки є

$$\Lambda = \{x \in \mathbf{Z}^{m+n+1} : (A \mid I_m \mid -b) * x = 0 \bmod q\}. \tag{17}$$

Аналогічно до попередньої атаки можна застосувати алгоритм редукції решітки. Для оцінки фактора Ерміта можливо скористатися співвідношенням

$$\log \delta_0 = \frac{1}{4n^2 \ln^2 q}\left(W\left((-2n\ln q) * (\sqrt{n \log q}) * \frac{(\tau\alpha)^2}{2\pi}\right)\right)^2, \tag{18}$$

де τ – допустима ймовірність, з якою алгоритм повинен завершити роботу успішно; α, n, q – параметри розподілу LWE; $W(\bullet)$ є W-функція Ламберта, яка визначається як розв'язок функціонального рівняння

$$z = W(z)e^{W(z)}\ . \tag{19}$$

Варто зауважити, що ця функція не може бути представлена через елементарні функції.

Іншим вектором атаки є використання дуальної решітки. Побудуємо дуальну решітку як $\hat{L} = \{x \in \mathbf{Z}_q^m \mid A*x = 0 \bmod q\}$. Редукція такої решітки фактично є вирішенням проблеми SIS. Якщо відомий вектор, що задовольняє умовам проблеми SIS, то задачу Decision-LWE можливо легко вирішити. Розглянемо детальніше редукцію Decision-LWE до SIS. Нехай задано m кортежів векторів вигляду $(A,c) = (A, A*s+e) \in \mathbf{Z}_q^{m\times n} \times \mathbf{Z}_q^{m\times 1}$. Знайдемо скалярний добуток $\langle x, c\rangle$:

$$\langle x, c\rangle = x*a*s + x*e = 0*s + x*e = x*e = \langle x, e\rangle. \tag{20}$$

Так як значення вектора $x \in \mathbf{Z}^n$ є заданим, то значення вектора помилок знаходиться перебором всіх можливих варіантів, оскільки простір пошуку значно зменшується. В роботі [33] показано, що норма вектора x є не більшою за

$$\|x\|_2 = \frac{1}{\alpha} * \sqrt{\frac{\ln(\frac{1}{\varepsilon})}{\pi}}, \tag{21}$$

де ε – допустима ймовірність, з якою алгоритм повинен завершити роботу успішно; α – параметр розподілу SIS.

Можливо з як завгодно близькою ймовірністю до 1 знайти значення вектору помилок, що фактично означає вирішення проблеми навчання з помилками. При цьому знадобиться $\frac{1}{\varepsilon^2}$ запусків вирішувача проблеми SIS. Так як для вирішення задачі потрібно знайти достатньо малий вектор на решітці, то рішення зводиться до задачі SVP. У роботі [33] була надана оцінка необхідного значення фактора Ерміта δ_0 при редукції решітки:

$$\log \delta_0 = \frac{\log^2(\frac{1}{\alpha}\sqrt{\frac{\ln(\frac{1}{\varepsilon})}{\pi}})}{4 * n \log q}, \tag{22}$$

де ε – допустима ймовірність, з якою алгоритм повинен завершити роботу успішно; α, n, q – параметри розподілу SIS.

Сімейство атак з використанням дуальних решіток має назву Dual Attack. При знаходженні кількісних оцінок атаки потрібно враховувати, що існують різні методи вирішення проблеми SIS. Класичним підходом є використання редукції решіток.

Щодо проблеми MLWE – наразі невідомо атак, що використовували би її алгебраїчну структуру, то ж можливо розглядати MLWE як частковий випадок LWE. Багато останніх робіт пропонують нові квантові алгоритми на Ideal-SVP [20, 21], тобто вирішення проблеми знаходження найменшого вектора на ідеальних решітках. Робота [21] присвячена квантовій атаці на Ring-LWE з використанням нової техніки, але використання її до Module-LWE створює численні труднощі. У роботі [24] показана редукція від MLWE до RLWE, тобто на основі поліноміального алгоритму, що може вирішити RLWE з правильними параметрами, можливо побудувати поліноміальний алгоритм, що може вирішити MLWE. Проте, на практиці ця атака веде себе значно гірше, ніж відомі атаки, оскільки зростає розмірність решітки. Це означає, що зростанням розмірності модуля можливо довести безпеку до значень, на які важко реалізувати атаку. Якщо через цю редукцію атакувати CRYSTALS-Kyber, то це призведе до вирішення RLWE з дуже великим модулем та помилками $(q' = q^3, \zeta' > q^2\zeta)$, тому вимагатиме від криптоаналітика більше, ніж 1 семпл.

6. Оцінка часу редукції решіток

У попередньому розділі було показано, що найкращі атаки на механізми KEM зводяться до редукції базису решіток без використання їх алгебраїчної структури. Найкращими відомими алгоритмами редукції решіток є BKZ та його численні модифікації [34]. BKZ є рандомізованим варіантом LLL. На кожному кроці знаходиться найменший вектор на проєктивній решітці розмірності β (розмір блоку редукції), додається до базису і проводиться LLL редукція. У роботі [34] було показано, що BKZ робить

$$O\left(\frac{n^2}{\beta^2}\log n\right) \tag{23}$$

викликів до процедури пошуку малого вектора на решітці розміру β. Від значення параметра β залежить якість редукції базису. Вектор з необхідною нормою можливо знайти за умови [2, 4]:

$$\sigma\sqrt{\beta} \le \delta_0^{2\beta-d-1} q^{\frac{n}{d}}, \tag{24}$$

де σ – середньоквадратичне відхилення для розподілу, з якого отримано коефіцієнти секретного вектора; d – розмірність усієї решітки; δ_0 – максимальне значення фактора Ерміта, за якого решітка стає достатньо редукованою.

Значення δ_0 також залежить від β і виражається [2, 19] як

$$\delta_0 \approx ((\pi B)^{\frac{1}{B}} * \beta / 2\pi e)^{1/2(\beta-1)}. \tag{25}$$

Ці міркування працюють як для LWE, та і для NTRU. Час роботи процедури пошуку малого вектора на решітці розміру β залежить від алгоритму, що використовується. Існує два класичних підходи – комбінаторні методи та методи на основі решета [19]. Комбінаторні методи роблять повний перебір, зменшуючи простір пошуку за допомогою різних евристик та використання інформації про базис решітки. Вони мають час роботи $O(2^\beta \log 2^\beta)$. Методи на основі решета генерують експоненційно велику множину векторів на решітці і на кожній ітерації "просіюють" її, доки не буде отримано достатньо малого вектора. Кількість таких ітерацій є поліноміальною. Такі алгоритми працюють за $O(2^\beta)$. Найкращий відомий класичний алгоритм працює за $2^{0.292\beta}$, а найкращий квантовий алгоритм – за $2^{0.265\beta}$.

На практиці для оцінки безпеки криптографічних систем на решітках, як правило, використовується модель core-SVP, яка полягає у тому, що вартість редукції визначається часом роботи алгоритма пошуку малого вектора. Поліноміальна кількість викликів ігнорується. Модель є доволі старою, проте вона є загальноприйнятим стандартом в криптографії на решітках. Сьогодні у науковій спільноті тривають дискусії про створення інших моделей, що прив'язані до певних технічних чи фізичних характеристик, проте, ці моделі доволі сирі. У табл. 4 зведені дані про конкретні оцінки безпеки КЕМ. На рис. 2 наведено порівняння конкретних оцінок безпеки КЕМ у вигляді діаграми.

Таблиця 4

Конкретні оцінки безпеки перспективних КЕМ

Рівень безпеки	FrodoKEM	CRYSTALS-Kyber	ДСТУ 8961:2019 "Скеля"
128	145/132	118/107	-
192	210/191	183/166	-
256	275/250	255/232	265/248
384	-	-	424/408
512	-	-	562/534
Найкраща атака	Редукція решітки	Редукція решітки	Гібридна атака

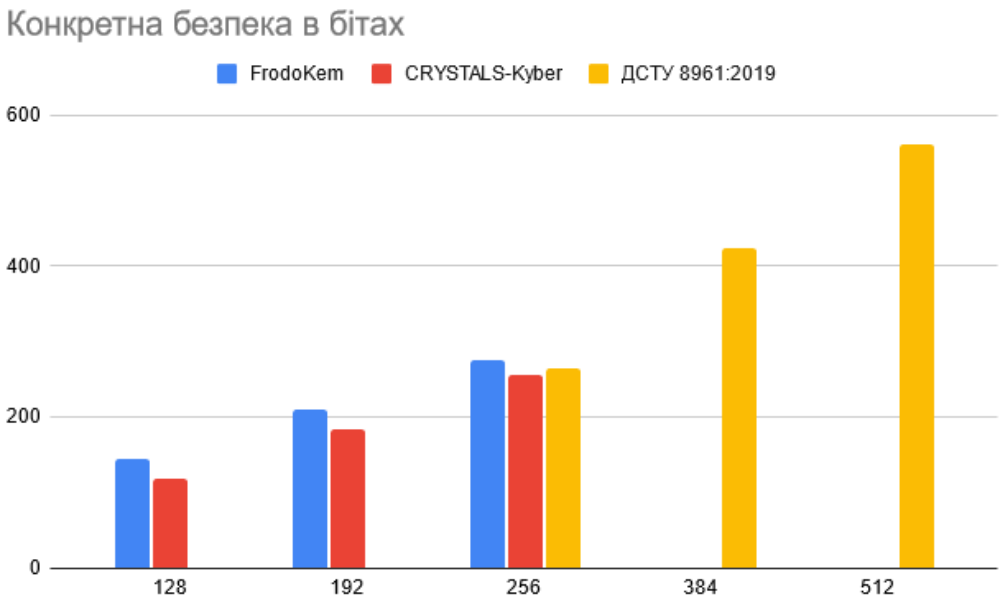

Рис. 2. Порівняння конкретної безпеки в бітах для класичних атак

Висновки

1. ДСТУ 8961:2019 “Скеля” ґрунтується на проблемі NTRU, яка має довгу історію вивчення, що є практичним аргументом безпеки. Структура, яку мають NTRU решітки, добре відома, проте редукцій від найгіршого до середнього від складних проблем теорії решіток (GapSVP, SIVP, тощо) до варіанту NTRU, що використовується у ДСТУ 8961:2019 “Скеля”, невідомо, хоча нещодавно була знайдена редукція від найгіршого до найгіршого для Module-uSVP. То ж, можливо сказати, що у той час, як практичний аспект безпеки NTRU є доволі вивченим, теоретичні питання досі потребують досліджень. Використання поля з твірним поліномом $X^n - X - 1$ у ДСТУ 8961:2019 “Скеля” є нетиповим вибором для криптосистем на решітках. З однієї сторони це дає захист від ряду алгебраїчних та деяких потенційних квантових атак, оскільки не існує нетривіальних підполів, проте, з іншої сторони, властивості цього полінома не так добре вивчені, як $X^n + 1$, який є стандартним вибором у криптографії на решітках. Хоча поява алгебраїчних атак на поле з твірним поліномом $X^n - X - 1$ є малоймовірною подією, проте це питання також потребує додаткових досліджень.

2. FrodoKEM ґрунтується на проблемі LWE. Широкі дослідження цієї проблеми почалися не так давно, як NTRU, проте вона має редукції від найгіршого до середнього від складних проблем теорії решіток, що є сильним теоретичним аргументом, якого не мають більшість розділів криптографії. Серед розглянутих варіантів FrodoKEM має найкращі теоретичні докази безпеки, проте через необхідність виконання операцій з матрицями реалізація FrodoKEM є помітно повільнішою за інші схеми, що фактично стало причиною виключення її з конкурсу NIST PQC після третього етапу.

3. CRYSTALS-Kyber ґрунтується на проблемі Module-LWE, яка є структурованим варіантом LWE. Ця структурованість дозволяє перейти до операцій в полі поліномів, що робить її надзвичайно швидкою. Module-LWE має редукції, аналогічно до LWE, від складних проблем на Module-LWE решітках, проте складність цих проблем є під питанням. Відомо, коли для складних проблем на структурованих решітках знаходили поліноміальні алгоритми вирішення, що використовують цю структурованість. Наразі для Module-LWE невідомо атак, які б ефективно використовували структурованість, проте це питання потребує детальнішого вивчення.

4. Для FrodoKEM та CRYSTALS-Kyber існують докази у моделях ROM та QROM, що є значною перевагою. Для ДСТУ 8961:2019 “Скеля” ситуація є дещо складнішою. Досліджень безпеки ДСТУ 8961:2019 у моделях ROM та QROM, на жаль, немає. Проте, зважаючи, що ДСТУ 8961:2019 є модифікованою версією стандарта ANSI X9.98, який є версією криптосистеми NTRUEncrypt, то відомі для цієї криптосистеми результати можуть бути адаптовані для ДСТУ 8961:2019. Питання доказів безпеки ДСТУ 8961:2019 “Скеля” у моделях ROM та QROM потребує додаткових досліджень.

5. ДСТУ 8961:2019 “Скеля”, на відміну від інших KEM, має параметри безпеки від 256 до 512 біт. З однієї сторони це робить її безпечнішою у деякому сенсі, при появі нових атак, що знижують безпеку на експоненційний фактор, проте, з іншої сторони, це означає, що реалізація буде дещо повільнішою, ніж FrodoKEM та CRYSTALS-Kyber (можливо, окрім набору параметрів для 256 біт безпеки), що робить її застосування доречним переважно для тих випадків, коли стійкість до появи нових малоймовірних атак важливіша за швидкодію.

6. Криптографія на решітках має величезне різноманіття складних проблем. Разом з редукціями це дає дуже різноманітний ландшафт для вивчення. Це є унікальною властивістю криптографії на решітках, що непритаманна іншим напрямкам досліджень, як у доквантовій, так і у постквантовій криптографії. При проєктуванні криптографічних систем це, безсумнівно, має враховуватись. Розглянуті KEM є рішеннями, які можливо впровадити “тут і зараз”. Проте, у майбутньому вірогідна поява інших криптографічних систем на решітках, які зможуть перевершити показники існуючих. Необхідне вивчення ландшафту проблем теорії решіток та застосування структурованості решіток.

Список літератури:

1. NIST Post-Quantum Cryptography Standartization Project : веб сайт. URL: https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization
2. CRYSTALS Kyber: a CCA-secure module-lattice-based KEM / Leo Ducas., and other. // URL: https://eprint.iacr.org/2017/634.pdf
3. ДСТУ 8961:2019 Інформаційні технології. Криптографічний захист інформації. Алгоритми асиметричного шифрування та інкапсуляції ключів // URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=88056
4. FrodoKEM. Learning With Errors Key Encapsulation Algorithm Specifications. And Supporting Documentation. / Leo Ducas., and other // URL: https://frodokem.org/files/FrodoKEM-specification-20210604.pdf
5. M. Toorani Security Protocols in a Nutshell // URL: https://arxiv.org/abs/1605.09771
6. Katz, Jonathan; Lindell, Yehuda (2007). Introduction to Modern Cryptography: Principles and Protocols.
7. Chakraborty, Debrup; Rodríguez-Henríquez., Francisco (2008). Çetin Kaya Koç (ed.). Cryptographic Engineering. p. 340. ISBN 9780387718170.
8. Möller, Bodo (2004). A Public-Key Encryption Scheme with Pseudo-random Ciphertexts // Computer Security – ESORICS 2004. Lecture Notes in Computer Science. Vol. 3193. pp. 335–351.
9. M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway. Relations among notions of security for public-key encryption schemes. // Advances in Cryptology – CRYPTO’98, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 1998, vol. 1462, pp. 26–45. [Online]. Available: http://dx.doi.org/10.1007/BFb0055718
10. Canetti R., Goldreich O., Halevi S. The random oracle methodology, revisited // 30th symposium on theory of computing. STOC, 1998. P. 209–218.
11. Boneh D., Dagdelen O., Fischlin M., Lehmann A., Schaffner C., Zhandry M (2011). Random oracles in a quantum world. Advances in Cryptology – ASIACRYPT 2011, eds Lee DH, Wang X (Springer Berlin Heidelberg, Berlin, Heidelberg), pp 41–69.
12. P. W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // URL: https://arxiv.org/abs/quant-ph/9508027
13. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. Теорія. Практика. Застосування : монографія. Харків : Форт, 2012. 880 с.
14. Goldreich O. Foundations of Cryptography : Vol. 1. Cambridge University Press, 2000. 392 p.
15. O. Regev. On lattices, learning with errors, random linear codes, and cryptography// ACM, 56(6):1–40, 2009. Preliminary version in STOC 2005.
16. Classical Hardness of Learning with Errors / Chris Peikert, Oded Regev, and other // URL: http://perso.ens-lyon.fr/damien.stehle/downloads/LWE.pdf
17. Thijs Laarhoven, J. V. D. Pol, B. D. Weger Solving Hard Lattice Problems and the Security of Lattice-Based Cryptosystems // URL: http://deweger.xs4all.nl/papers/%5B51%5DLvdPdW-Kolkata%5B2012%5D.pdf

18. Обзор LWE на структурированых решетках.
19. Vaikuntanathan V. Advanced Topics in Cryptography: Lattices : веб сайт. URL: https://people.csail.mit.edu/vinodv/6876-Fall2015/
20. Kirsten Eisenträger, Sean Hallgren, Alexei Kitaev, and Fang Song. A quantum algorithm for computing the unit group of an arbitrary degree number field. In STOC '14 Proceedings of the forty-sixth annual ACM symposium on Theory of computing, pages 293–302. ACM, 2014. http://www.personal.psu. edu/kxe8/unitgroup.pdf. 31
21. Ronald Cramer, Léo Ducas, and Benjamin Wesolowski. Short Stickelberger class relations and application to Ideal-SVP. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, Advances in Cryptology – EUROCRYPT 2017, volume 10210 of LNCS, pages 324–348. Springer, 2017. https: //eprint.iacr.org/2016/885. 31, 35
22. Yang Wang, Mingqiang Wang Module-LWE versus Ring-LWE, Revisited // URL: https://eprint.iacr.org/2019/930
23. A. Langlois, D. Stehlé. Worst-Case to Average-Case Reductions for Module Lattices // URL: https://perso.ens-lyon.fr/damien.stehle/downloads/MSIS.pdf
24. Martin R. Albrecht, A. Deo. Large Modulus Ring-LWE ≥ Module-LWE // URL: https://eprint.iacr.org/2017/612.pdf
25. Joan Bruna, Oded Regev, Min Jae Song, Yi Tang. Continuous LWE // URL: https://arxiv.org/abs/2005.09595
26. Hoffstein J., Pipher J., Silverman J.H. NTRU: a ring based public key cryptosystem // Algorithmic Nuber Theory, Third International Symposium, Portland, Oregon, USA, June 21 – 25, 1998. Proceedings. Springer, 1998. P. 267 – 288.
27. Proovable NTRU.
28. Micheli G., Heninger N., Shani B. Characterizing overstretched NTRU attacks Journal of Mathematical Cryptology. 2020. Vol 14, Is 1. P. 110-119.
29. American National Standard X9.98-2010. Lattice-based polynomial public key encryption algorithm, Part 1: key establishment, Part 2: data encryption. 2010.
30. I.D. Gorbenko. Calculation of general parameters for NTRU Prime Ukraine of 6-7 levels of stability / I. D. Gorbenko, A. N. Alekseychuk, O. Kachko ,M. Yesina, I. V. Stelnik, S. Kandy,V. A. Bobukh // Telecommunications and Radio Engineering. 78(4):327-340.
31. I.D. Gorbenko. Methods of building general parameters and keys for ntru prime ukraine of 5th-7th levels of stability. product form / I. D. Gorbenko, Yu. I. Gorbenko, O. Kachko ,M. Yesina, I. V. Stelnik, S. Kandy // Telecommunications and Radio Engineering. 78(7):579-594.
32. Wunderer Th. Revising the hibrid attack: improved analysis and refined security estimates // URL: http://eprint.iacr.org/2016/733.
33. Player R. Parameter selectionin lattice-based cryptography. URL: https://pure.royalholloway.ac.uk/portal/files/29983580/2018playerrphd.pdf
34. Jianwei Li, Phong Q. Nguyen. A Complete Analysis of the BKZ Lattice Reduction Algorithm // URL: https://eprint.iacr.org/2020/1237.pdf
35. J.Felderhoff, A. Pellet-Mary, D.Stehl. On Module Unique-SVP and NTRU // URL: https://eprint.iacr.org/2022/1203.pdf.

Надійшла до редколегії 12.09.2022

Відомості про авторів:

Горбенко Юрій Іванович – канд. техн. наук, АТ "Інститут Інформаційних Технологій", перший заступник головного конструктора, Україна; e-mail: gorbenkou@iit.kharkov.ua; ORCID: https://orcid.org/0000-0003-0073-9107

Кандій Сергій Олегович – Харківський національний університет імені В. Н. Каразіна; аспірант кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, АТ "Інститут Інформаційних Технологій", технік-конструктор; Україна; e-mail: sergeykandy@gmail.com , ORCID: https://orcid.org/0000-0003-0552-8341