CRYPTOLOGY

DOI 10.20535/2411-1031.2022.10.2.270406
УДК 004.056.55:003.26.09

АЛЕКСАНДРА МАТІЙКО,
АНТОН ОЛЕКСІЙЧУК

МЕТОД ПОБУДОВИ ОБҐРУНТОВАНО СТІЙКИХ СИМЕТРИЧНИХ NTRU-ПОДІБНИХ ШИФРОСИСТЕМ

Асиметричні NTRU-подібні шифросистеми відносяться до найшвидших сучасних постквантових криптосистем. Вони будуються на основі простих (з погляду складності реалізації) перетворень у кільцях зрізаних поліномів та за умови належного вибору їхніх параметрів забезпечують потрібну стійкість відносно відомих атак. Стійкість таких шифросистем базується на складності знаходження коротких векторів у певних решітках в евклідовому просторі. До NTRU-подібних (або близьких до них типу Learning With Errors) криптосистем відноситься майже третина усіх постквантових криптографічних алгоритмів, представлених на конкурс NIST зі стандартизації постквантових криптопримітивів. Поряд з тим, є актуальною задача створення симетричних криптосистем, стійкість яких (аналогічно асиметричним) базується на складності розв'язання єдиної обчислювально складної задачі. На сьогодні відомо тільки одну симетричну NTRU-подібну шифросистему – NTRUCipher, яка виявляється не стійкою відносно певних атак на основі підібраних відкритих текстів. Метою цієї статті є розробка методу побудови симетричних NTRU-подібних шифросистем, які є обґрунтовано стійкими відносно зазначених атак (CPA-стійкими). Доведено, що стійкість запропонованих шифросистем базується на складності розв'язання задачі, відомої як Decision-Ring-LWE, що є однією з еталонних обчислювально складних задач у решітковій криптографії. Показано, що на відміну від раніше відомої шифросистеми NTRUCipher, запропоновані шифросистеми мають обґрунтовану стійкість відносно атак на основі підібраних відкритих повідомлень. При цьому запропоновані шифросистеми мають ту ж саму довжину секретного ключа, що і шифросистема NTRUCipher. Наведено алгоритм вибору параметрів запропонованих шифросистем, які забезпечують їхню стійкість на заздалегідь визначеному рівні. Зазначено, що час зашифрування чи розшифрування повідомлень у запропонованих шифросистемах є порівняним з відповідним часом у криптосистемі NTRU Prime, яка є одним з фіналістів конкурсу NIST зі створення нових постквантових криптографічних стандартів.

Ключові слова: постквантова криптографія, симетрична шифросистема, NTRUCipher, NTRU Prime, обґрунтування стійкості.

Постановка проблеми. Асиметричні NTRU-подібні шифросистеми відносяться до найшвидших сучасних постквантових криптосистем. Вони будуються на основі простих (з погляду складності реалізації) перетворень у кільцях зрізаних поліномів та за умови належного вибору їхніх параметрів забезпечують потрібну стійкість відносно відомих атак. До NTRU-подібних (або близьких до них типу Learning With Errors (LWE)) криптосистем відноситься майже третина усіх постквантових криптографічних алгоритмів, представлених на конкурс NIST зі стандартизації постквантових криптопримітивів (див. роботи [1] - [3] та наведені в них посилання). Поряд з тим, на сьогодні відомо тільки одну симетричну NTRU-подібну шифросистему – NTRUCipher [4], яка (поряд з її вдосконаленням – NTRUCipher+) виявляється не стійкою відносно новітніх атак [5] - [7]. Таким чином, постає задача розробки методу побудови симетричних NTRU-подібних шифросистем, що мають обґрунтовану стійкість відносно атак на основі підібраних відкритих повідомлень.

Аналіз останніх досліджень і публікацій. Асиметричну шифросистему NTRU запропоновано в середині 90-х років [8]. Практично одразу з'ясувалось, що її стійкість базується на складності знаходження коротких векторів у певних решітках в евклідовому просторі [9], що стимулювало численні дослідження, спрямовані на вдосконалення цієї шифросистеми та обґрунтування її стійкості відносно різноманітних атак [1] - [3], [10]. На сьогодні відомо декілька варіантів шифросистеми NRTU, окремі з яких є фіналістами конкурсу NIST зі створення постквантових криптопримітивів [1], [10], [11].

Однією з актуальних задач сучасної криптографії є створення симетричних криптосистем, стійкість яких (аналогічно асиметричним) базується на складності розв'язання тільки однієї обчислювально складної задачі. Серед NTRU-подібних єдиною шифросистемою, яка могла б претендувати на цей статус, є NTRUCipher [4]. Проте в оригінальній роботі не наведено обґрунтування CPA-стійкості цієї шифросистеми, а згідно з результатами [5] - [7] вона (та навіть її природне вдосконалення – NTRUCipher+) є вразливими відносно низки атак.

Метою статті є розробка методу побудови симетричних NTRU-подібних шифросистем, які є обґрунтовано стійкими відносно атак на основі підібраних відкритих текстів (CPA-стійкими [12]).

Виклад основного матеріалу дослідження.

Означення шифросистеми. Нехай n і q – цілі числа такі, що $n,q \ge 2$ і q не ділиться на 3. Позначимо $\mathbf{Z}_q$ кільце класів лишків за модулем q, елементи якого ототожнимо з цілими числами, що належать інтервалу $[-(q-1)/2,(q-1)/2]$ для непарного q та інтервалу $[-q/2, q/2-1]$ для парного q. Зафіксуємо поліном $f(x) = x^n - c_{n-1}x^{n-1} - \cdots - c_0$ над кільцем $\mathbf{Z}_q$ та позначимо $R_{f,q} = \mathbf{Z}_q[x]/(f(x))$ кільце зрізаних поліномів степеня не вище $n-1$, що складається з q^n поліномів вигляду $u = u_0 + u_1x + \cdots + u_{n-1}x^{n-1}$, де $u_i \in \mathbf{Z}_q$, $i \in \overline{0,n-1}$, які додаються та перемножуються за модулем полінома $f(x)$.

Ототожнимо довільний поліном $u = u_0 + u_1x + \cdots + u_{n-1}x^{n-1} \in \mathbf{R}[x]$ з вектором його коефіцієнтів та позначимо $\| u \|_\infty = \max\limits_{0 \le i \le n-1} |u_i|$, $\| u \|_1 = \sum\limits_{i=0}^{n-1} |u_i|$. Для будь-якого $u = u_0 + u_1x + \cdots + u_{n-1}x^{n-1} \in \mathbf{Z}[x]$ позначимо $u \bmod q$ поліном $(u_0 \bmod q) + (u_1 \bmod q)x + \ldots$ $\cdots + (u_{n-1} \bmod q)x^{n-1} \in R_{f,q}$. Аналогічний сенс має позначення $u \bmod 3$.

Зафіксуємо натуральне число d таке, що $2d < n$. Для заданих чисел n, q, d і полінома $f(x)$ симетрична NTRU-подібна шифросистема, що пропонується, визначається таким чином.

Секретними ключами шифросистеми є довільні поліноми $h \in R_{f,q}$ такі, що $\| h \|_\infty = 1$, $\| h \|_1 = 2d$, а відкритими текстами – поліноми $m \in R_{f,q}$ такі, що $\| m \|_\infty = 1$.

Для зашифрування тексту m на ключі h генеруються незалежні випадкові поліноми r, $e_1 = e_{1,0} + e_{1,1}x + \cdots + e_{1,n-1}x^{n-1}$ та $e_2 = e_{2,0} + e_{2,1}x + \cdots + e_{2,n-1}x^{n-1}$, де r має рівномірний розподіл ймовірностей на кільці $R_{f,q}$, а $e_{1,0}, e_{1,1}, \ldots, e_{1,n-1}, e_{2,0}, e_{2,1}, \ldots, e_{2,n-1}$ є незалежними випадковими величинами, які приймають кожне значення $0, 1, -1$ з імовірністю $1/3$. Далі обчислюється шифрований текст

$$E_h(m, r, e_1, e_2) = (c_1, c_2) = ((r - e_1) \bmod q, (m + 3(rh + e_2)) \bmod q). \quad (1)$$

Розшифрування довільного тексту $c = (c_1, c_2) \in R_{f,q} \times R_{f,q}$ на ключі h здійснюється за формулою

$$D_h(c) = ((c_2 - 3hc_1) \bmod q) \bmod 3. \quad (2)$$

Зауважимо, що у формулах (1), (2) і далі додавання та множення поліномів здійснюється за модулем полінома $f(x)$.

Отримаємо умову, за якою розшифрування повідомлення (1) за формулою (2) є коректним.

Позначимо $\theta(f)$ найменше додатне число таке, що $\| ab \|_\infty \le \theta(f) \| a \|_1 \| b \|_\infty$ для будь-яких поліномів $a, b \in \mathbf{R}[x]$ степеня не вище $n-1$, де (згідно з прийнятою вище домовленістю) ab позначає добуток поліномів a і b за модулем полінома $f(x)$ [13].

Помітимо, що на підставі формули (1) $(c_2 - 3hc_1) \bmod q = (m + 3he_1 + 3e_2) \bmod q$. Звідси випливає, що $D_h(E_h(m, r, e_1, e_2)) = m$, якщо $\| m + 3he_1 + 3e_2 \|_\infty < q/2$. При цьому, оскільки $\| h \|_1 = 2d$, $\| m \|_\infty = \| e_1 \|_\infty = \| e_2 \|_\infty = 1$, то

$\| m + 3he_1 + 3e_2 \|_\infty \le \| m \|_\infty + 3\theta(f) \| h \|_1 \| e_1 \|_\infty + 3 \| e_2 \|_\infty = 4 + 6d \cdot \theta(f)$.

Таким чином, за умови

$$d < \frac{q-8}{6 \cdot \theta(f)}. \tag{3}$$

розшифрування отриманих повідомлень відбувається коректно.

Обґрунтування CPA-стійкості запропонованої шифросистеми. Нагадаємо означення CPA-стійкості симетричної шифросистеми (див., наприклад, [12]). Розглядається така "гра" між супротивником і дослідником:

1) дослідник генерує секретний ключ k;

2) супротивник може подавати на вхід оракула E_k, що здійснює зашифрування, будь-які відкриті та отримувати відповідні шифровані тексти;

3) супротивник подає досліднику пару різних текстів m_0 та m_1 однакової довжини;

4) дослідник вибирає випадкове рівноймовірне число $b \in \{0, 1\}$ та повертає супротивнику шифрований текст $c = E_k(m_b)$;

5) супротивник може звертатися до оракула E_k (як в п. 2)) і повинен відновити значення b.

Шифросистема називається (T, ε)-*CPA-стійкою*, якщо будь-який алгоритм відновлення значення b з імовірністю $\varepsilon > 1/2$ у наведеній "грі" виконує не менше ніж T операцій.

Сформулюємо допоміжне твердження, яке використовується далі для обґрунтування CPA-стійкості запропонованої NTRU-подібної шифросистеми.

Розглянемо довільну симетричну шифросистему з множиною відкритих текстів M, множиною шифрованих текстів C, множиною ключів K, множиною секретних параметрів S та оракулом зашифрування вигляду

$$E_k(m) = G(m) + F_k(s), \; m \in M, \; k \in K, \tag{4}$$

де $G : M \to C$ – загальновідома функція;

$F_k : S \to C$ – функція, що залежить від секретного ключа k;

$+$ позначає комутативну групову операцію на множині C;

(невідомий) елемент s вибирається з множини S випадково згідно з певним законом розподілу Γ.

Задача про розрізнення полягає в наступному. Розглядається оракул, який з імовірністю $1/2$ виробляє незалежні випадкові рівноймовірні елементи множини C (гіпотеза H_0) та з такою ж ймовірністю – випадкові елементи вигляду $F_k(s_1), F_k(s_2), \ldots$ для заздалегідь вибраного з множини K (невідомого) випадкового рівноймовірного елемента k та незалежних

випадкових елементів $s_1, s_2, \ldots$, розподілених на множині S за законом Г (гіпотеза H_1). Маючи доступ до зазначеного оракула, треба з'ясувати, яка з двох гіпотез має місце.

Наступна лема доводиться аналогічно теоремі 3.18 в [12].

Лема. Нехай існує CP-атака, яка використовує t звернень до оракула (4), має часову складність T і ймовірність успіху $1/2+\varepsilon$, де $\varepsilon > 0$. Тоді існує алгоритм, який розв'язує задачу про розрізнення зі складністю не вище ніж $T + \nu t$ та ймовірністю успіху $1/2 \cdot (1+\varepsilon)$, де ν – максимальна часова складність обчислення одного значення вигляду $G(m)+c$ для будь-яких $m \in M$, $c \in C$.

Важливим окремим випадком задачі про розрізнення є відома *задача Decision-Ring-LWE*, на складності якої базується стійкість багатьох сучасних решіткових криптосистем [14]. В цьому випадку $C = R_{f,q} \times R_{f,q}$, $K = R_{f,q}$, а значення $F_k(s_1), F_k(s_2), \ldots$ формуються за правилом

$$F_k(s_i) = (s_{1,i},\ s_{1,i}k + s_{2,i}), \tag{5}$$

де обчислення виконуються в кільці $R_{f,q}$, $s_i = (s_{1,i}, s_{2,i})$ і $s_{1,i}, s_{2,i}$ є незалежними випадковими елементами, перший з яких має рівномірний розподіл ймовірностей на кільці $R_{f,q}$, а другий – певний (відмінний від рівномірного) розподіл на цьому кільці, $i = 1, 2, \ldots$.

Таким чином, задача Decision-Ring-LWE над кільцем $R_{f,q}$ полягає в тому, щоб відрізнити послідовність незалежних випадкових елементів вигляду (5) із зазначеним законом розподілу від суто випадкової послідовності елементів множини $C = R_{f,q} \times R_{f,q}$. Зрозуміло, що складність розв'язання цієї задачі залежить від самого кільця, закону розподілу випадкових поліномів $s_{2,i}$, $i = 1, 2, \ldots$, а також від того, який обсяг даних є доступним для аналізу (у випадку, що розглядається, зазначений обсяг вважається потенційно не обмеженим).

Наступне твердження показує, що означена вище симетрична NTRU-подібна шифросистема є CPA-стійкою, якщо є обчислювально складною задача Decision-Ring-LWE для наступних вхідних даних: у формулі (5) $k = 3h$, де h є секретним ключем криптосистеми; $s_{2,i} = 3(he_{1,i} + e_{2,i})$ в кільці $R_{f,q}$, де $e_{1,i}, e_{2,i}$ – випадкові поліноми степеня не вище $n-1$ з незалежними в сукупності коефіцієнтами, які приймають кожне значення $0, 1, -1$ з імовірністю $1/3$.

Твердження. Нехай існує CP-атака, яка використовує t звернень до оракула (1), має часову складність T і ймовірність успіху $1/2+\varepsilon$, де $\varepsilon > 0$. Тоді існує алгоритм, який розв'язує зазначену вище задачу Decision-Ring-LWE зі складністю не вище ніж $T + O(nt\log q)$ та ймовірністю успіху $1/2 \cdot (1+\varepsilon)$.

Доведення. Помітимо, що шифросистема, що описується рівнянням (1), є окремим випадком шифросистеми, яка описується рівнянням (4): треба покласти $G(m) = (0, m)$, $k = 3h$, $s = (r, e_1, e_2)$, $F_k(s) = (r - e_1, 3rh + 3e_2)$, де обчислення виконуються в кільці $R_{f,q}$.

Отже, на підставі леми з існування CP-атаки, зазначеної у формулюванні твердження, випливає існування алгоритму, який розв'язує відповідну задачу про розрізнення зі складністю не вище ніж $T + \nu t$ та ймовірністю успіху $1/2 \cdot (1+\varepsilon)$, де ν – максимальна часова складність обчислення одного значення вигляду $m + r$ для будь-яких $m, r \in R_{f,q}$. Звідси випливає, що $\nu = O(n\log q)$.

Далі, значення $F_k(s_i) = F_k(r_i, e_{1,i}, e_{2,i})$ має вигляд (5), якщо покласти $s_{1,i} = r_i - e_{1,i}$, $s_{2,i} = 3(he_{1,i} + e_{2,i})$, де обчислення виконуються в кільці $R_{f,q}$. Оскільки за означенням

шифросистеми r_i є випадковим елементом з рівномірним розподілом ймовірностей на кільці $R_{f,q}$, а $e_{1,i}$ не залежить від r_i, то випадковий елемент $s_{1,i}$ має рівномірний закон розподілу на кільці $R_{f,q}$, і для завершення доведення залишається переконатися в тому, що випадкові елементи $s_{1,i}$, $s_{2,i}$ є незалежними.

Дійсно, позначаючи 3^{-1} обернений до 3 елемент кільця $\mathbf{Z}_q$ (який існує, оскільки q не ділиться на 3) та використовуючи означення випадкових елементів $r_i, e_{1,i}, e_{2,i}$, отримаємо, що для будь-яких $u, v \in R_{f,q}$ справедливі такі рівності:

$$\mathbf{P}(s_{1,i} = u,\ s_{2,i} = v) = \mathbf{P}(r_i - e_{i,1} = u, 3he_{i,1} + 3e_{2,i} = v) =$$
$$= \sum_{w \in R_{f,q}} \mathbf{P}(e_{i,1} = w)\mathbf{P}(r_i = u + w)\mathbf{P}(e_{i,2} = 3^{-1}(v - 3hw)) =$$
$$= \frac{1}{|R_{f,q}|} \sum_{w \in R_{f,q}} \mathbf{P}(e_{i,1} = w)\mathbf{P}(e_{i,2} = 3^{-1}(v - 3hw)),$$
$$\mathbf{P}(s_{1,i} = u)\mathbf{P}(s_{2,i} = v) = \mathbf{P}(r_i - e_{i,1} = u)\mathbf{P}(3he_{i,1} + 3e_{2,i} = v) =$$
$$= \frac{1}{|R_{f,q}|} \sum_{w \in R_{f,q}} \mathbf{P}(e_{i,1} = w)\mathbf{P}(e_{i,2} = 3^{-1}(v - 3hw)).$$

Таким чином, $\mathbf{P}(s_{1,i} = u,\ s_{2,i} = v) = \mathbf{P}(s_{1,i} = u)\mathbf{P}(s_{2,i} = v)$, що і треба було довести.

Твердження доведено.

Вибір параметрів запропонованої шифросистеми для забезпечення її стійкості відносно відомих атак. На підставі доведеного твердження CPA-стійкість запропонованої шифросистеми визначається складністю розв'язання зазначеної вище задачі Decision-Ring-LWE над кільцем $R_{f,q}$, яку (враховуючи оберненість числа 3 за модулем q) можна сформулювати таким чином.

Спостерігається послідовність незалежних випадкових елементів, кожен з яких або є рівномірно розподіленим на множині $R_{f,q} \times R_{f,q}$ (гіпотеза H_0), або має вигляд $(3^{-1}a_i, a_i h + (he_{1,i} + e_{2,i}))$, $i = 1, 2, \ldots$, де обчислення виконуються в кільці $R_{f,q}$, h є невідомим фіксованим елементом цього кільця, $\|h\|_\infty = 1$, $\|h\|_1 = 2d$, $a_i, e_{1,i}, e_{2,i}$ є незалежними випадковими елементами, причому a_i має рівномірний розподіл ймовірностей на кільці $R_{f,q}$, $e_{1,i}, e_{2,i}$ є випадковими поліномами степеня не вище $n-1$ з незалежними в сукупності коефіцієнтами, які приймають кожне значення $0, 1, -1$ з імовірністю $1/3$ (гіпотеза H_1). Треба з'ясувати, яка з двох гіпотез має місце.

Визначимо, як вибирати параметри шифросистеми (числа n, q, d та поліном $f(x)$) для забезпечення належної складності відомих алгоритмів розв'язання наведеної задачі.

Перш за все, зауважимо, що у випадку коли число q має власний дільник $q' > 1$, для розв'язання цієї задачі можна скористатися гомоморфізмом кільця $R_{f,q}$ в кільце $R_{f,q'}$. Останнє має менший порядок, що, в принципі, надає можливість спростити будь-який алгоритм розв'язання поставленої задачі шляхом зведення її до аналогічної задачі меншого розміру над гомоморфним образом вхідного кільця. Аналогічно, якщо у полінома $f(x)$ є нетривіальний дільник $f'(x)$, можна скористатися гомоморфізмом кільця $R_{f,q}$ в кільце $R_{f',q}$ для зведення вхідної задачі до аналогічної задачі меншого розміру. Зауважимо, що при такому зведенні "рівень" спотворення (тобто випадкового елемента $he_{1,i} + e_{2,i}$) збільшиться,

але зменшиться розмір вхідної задачі, що може в цілому зменшити складність її розв'язання (див. роботу [15], де наведено приклад суттєвого зменшення складності розв'язання подібної задачі). Для того, щоб в принципі запобігти можливості застосування методу гомоморфізмів, вважатимемо, що q є простим числом, а поліном $f(x)$ є незвідним над полем $\mathbf{Z}_q$. Крім того, якщо число n не є простим, то поле $R_{f,q}$ (для простого q та незвідного $f(x)$) має власне підполе, відмінне від поля $\mathbf{Z}_q$, що також надає можливість застосувати метод гомоморфізмів до розв'язання поставленої задачі (на кшталт того, як це робиться в [16] із застосування функції сліду).

Таким чином, для протидії методу гомоморфізмів, вважатимемо далі, що n і q є різними простими числами, а $f(x)$ – незвідним над полем $\mathbf{Z}_q$ поліномом. Більш того, виходячи з вимоги практичності шифросистеми (можливості швидкого множення елементів поля $R_{f,q}$), вважатимемо, що $f(x)$ має такий саме вигляд, як і в криптосистемі NTRU Prime: $f(x) = x^n - x - 1$ [10].

На сьогодні єдиним відомим методом розв'язання зазначеної вище задачі Decision-Ring-LWE є її зведення до задачі LWE (див., наприклад, [17], п. 5.3). Сутність цього методу полягає в наступному.

По-перше, розглянемо довільні поліноми $u(x) = \sum_{i\geq 0} u_i x^i$, $v(x) = \sum_{i\geq 0} v_i x^i \in R_{f,q}$ та позначимо $w(x) = \sum_{i=0}^{2n-2} w_i x^i$ їх добуток в кільці $\mathbf{Z}[x]$, $w_i = \sum_{j=0}^{i} u_j v_{i-j}$, $i \in \overline{0,2n-2}$. Тоді, як показує безпосередня перевірка, добуток цих поліномів за модулем полінома $f(x) = x^n - x - 1$ дорівнює $u(x)v(x) = (w_0 + w_n)x^0 + \sum_{i=1}^{n-2}(w_i + w_{i+n} + w_{i+n-1})x^i + (w_{n-1} + w_{2n-2})x^{n-1}$. Отже, вільний член добутку поліномів $u(x)$ та $v(x)$ в полі $R_{f,q}$ дорівнює $(w_0 + w_n) \bmod q = (u_0 v_0 + u_1 v_{n-1} + \cdots + u_{n-1} v_1) \bmod q$.

По-друге, розглянемо послідовність випадкових елементів $(3^{-1}a_i, b_i)$, які є вхідними даними для задачі Decision-Ring-LWE, тобто розподілені відповідно до однієї з двох зазначених вище гіпотез H_0, H_1. Обчислимо вільні члени $b_{i,0}$ поліномів b_i, $i = 1, 2, \ldots$. Якщо має місце гіпотеза H_0, тобто b_i є випадковим рівноймовірним елементом поля $R_{f,q}$, що не залежить від a_i, то $b_{i,0}$ є випадковим рівноймовірним елементом поля $\mathbf{Z}_q$, який також не залежить від a_i. Якщо ж справедлива гіпотеза H_1, тобто $b_i = a_i h + (he_{1,i} + e_{2,i})$, то на підставі зазначеної вище формули для вільного члена добутку двох поліномів у полі $R_{f,q}$, а також рівностей $\| h \|_\infty = 1$, $\| h \|_1 = 2d$ має місце таке співвідношення над полем $\mathbf{Z}_q$:

$$b_{i,0} = a_{i,0} h_0 + a_{i,1} h_{n-1} + \cdots + a_{i,n-1} h_1 + \xi_i, \tag{6}$$

де $\sum_{j=0}^{n-1} a_{i,j} x^j = a_i$;

$\sum_{j=0}^{n-1} h_j x^j = h$;

ξ_i є сумою $2d+1$ незалежних випадкових величин, які приймають кожне значення $0, 1, -1$ з імовірністю $1/3$ та не залежать від a_i.

Таким чином, за умови гіпотези H_1 вектор коефіцієнтів полінома h задовольняє системі лінійних рівнянь зі спотвореними правими частинами вигляду (6). Отже, для перевірки гіпотез H_0, H_1 достатньо відновити вектор $(h_0, h_{n-1}, \dots, h_1)$ із зазначеної системи рівнянь за відомими векторами $(a_{i,0}, a_{i,1}, \dots, a_{i,n-1})$ та значеннями $b_{i,0}$, $i = 1, 2, \dots$. В цьому полягає один з варіантів задачі LWE над полем $\mathbf{Z}_q$ [18].

На сьогодні відомі такі методи розв'язання зазначеної задачі: метод максимальної правдоподібності [19], метод зустрічі посередині та його вдосконалення [20], [21], метод BKW [22], а також решіткові методи (так звані первинна та дуальна атаки) [23], [24]. Використовуючи відомі алгоритми оцінювання трудомісткості цих методів, що базуються на результатах відзначених робіт, можна обчислити для заздалегідь вибраного рівня стійкості λ значення параметрів n, q, d запропонованої шифросистеми, для яких трудомісткість найкращого із зазначених методів (яка визначає CPA-стійкість цієї шифросистеми) є не менше ніж λ.

Нижче в табл. 1 представлено результати чисельних розрахунків, проведених для низки значень n, q і d. Підкреслимо, що за означенням шифросистеми n і q є різними простими числами такими, що поліном $f(x) = x^n - x - 1$ є незвідним над полем $\mathbf{Z}_q$; d є натуральним числом таким, що $n > 2d$ і $q > 12d + 8$. При цьому стійкість шифросистеми базується на складності задачі LWE, яка полягає у розв'язанні системи лінійних рівнянь зі спотвореними правими частинами від n невідомих над полем $\mathbf{Z}_q$, де істинний розв'язок системи є $(0, 1, -1)$-вектором, який містить точно $2d$ ненульових координат, а спотворення в правій частині кожного рівняння є сумою $2d + 1$ незалежних випадкових величин, які приймають кожне значення $0, 1, -1$ з імовірністю $1/3$.

Нижні оцінки складності алгоритмів розв'язання задачі LWE визначаються таким чином.

1. Метод максимуму правдоподібності (повний перебір) [19]:

$$T_1 = 2^{2d} \binom{n}{2d}.$$

2. Удосконалений алгоритм зустрічі посередині [20], [21]:

$$T_2 = \sqrt[4]{T_1}\,.$$

3. Решіткові алгоритми.

Первинна атака: виконати наступний алгоритм [23], [24].

Алгоритм 1: для кожного $m = 1, 2, \dots$ виконати такі дії:

1) покласти $t = n + m + 1$;

2) знайти найменше $b = b^{(1)}(m) \in \{200, 201, \dots, t\}$ таке, що

$$(2d + 1)\sqrt{\frac{b}{3}} \le \delta^{2b-t} q^{\frac{m}{t}},$$

де $\delta = \left((\pi b)^{\frac{1}{b}} \frac{b}{2\pi e} \right)^{\frac{1}{2(b-1)}}$,

та завершити обчислення.

Нижня оцінка складності атаки: $T_3 = 2^{0,292b}$.

Дуальна атака: виконати наступний алгоритм [23], [24].

Алгоритм 2: для кожного $m = 1, 2, \dots$ виконати такі дії:

1) покласти $t = n + m$;

2) знайти найменше число $b = b^{(2)}(m) \in \{200, 201, ..., t\}$ таке, що $\delta^t q^{\frac{n}{t}} \le \frac{q}{\pi\sqrt{2d+1}}\sqrt{\frac{(c+2)\ln 2}{2}}$,

де $\delta = \left((\pi b)^{\frac{1}{b}} \frac{b}{2\pi e}\right)^{\frac{1}{2(b-1)}}$, $c = 8$,

та завершити обчислення.

Нижня оцінка складності атаки: $T_4 = 2^{0,292b+2c}$.

4. BKW-атака. Розрахунки проводяться згідно з твердженнями 1, 2 у [5], де у формулі (8) слід покласти $\pi(\alpha) = \theta(1/3, \alpha)^{2d+1}$.

Таблиця 1 – Двійкові логарифми нижніх оцінок складності відомих атак на запропоновану шифросистему

Параметри			ММП	Зустріч посередині	Первинна атака	Дуальна атака	BKW-атака
n	q	d					
439	6833	142	690,6	172,7	490,9	329,0	501,3
503	2879	59	508,8	127,2	505,5	419,8	545,6
503	8663	67	549,9	137,5	388,1	309,5	571,9
569	3929	81	647,6	161,9	594,8	476,2	618,5
607	6317	131	855,9	213,9	672,2	495,2	669,4
631	2081	43	444,0	111,0	610,9	573,7	658,3
631	2693	56	533,1	133,3	632,8	560,9	667,2
677	3251	67	615,2	153,8	691,7	599,9	717,5
727	5827	121	904,27	226,1	798,1	623,1	786,1
787	4243	88	774,6	193,6	832,2	705,7	833,1
829	1657	34	402,9	100,7	777,3	821,6	832,5
883	8089	168	1177,1	294,3	1005,4	768,5	952,2
947	3917	81	782,3	195,6	990,8	890,2	982,75
991	9349	194	1339,8	334,9	1145,8	873,9	1064,9
1019	6691	139	1134,4	283,6	1136,2	929,9	1077,1
1021	5393	112	993,9	248,5	1110,8	949,5	1068,7
1021	8819	183	1321,9	330,5	1172,9	910,4	1091,9

Висновки. У статті запропоновано метод побудови обґрунтовано стійких симетричних NTRU-подібних шифросистем, сутність якого полягає у використанні для зашифрування і розшифрування перетворень, що визначаються за формулами (1) і (2) відповідно. На відміну від раніше відомої симетричної NTRU-подібної шифросистеми [4], яка не є стійкою відносно певних атак [5] - [7], запропоновані шифросистеми мають обґрунтовану стійкість відносно атак на основі підібраних відкритих повідомлень.

Для вибору параметрів n, q і d, що забезпечують стійкість запропонованих шифросистем на заздалегідь вибраному рівні λ, можна використовувати відомі методи оцінювання складності розв'язання задачі Decision-Ring-LWE. Результати чисельних розрахунків свідчать про те, що для забезпечення стійкості на рівні $\lambda = 2^{128}$ можна вважати $n = 631$, $q = 2693$, $d = 56$, а для забезпечення стійкості на рівні $\lambda = 2^{256}$ можна вважати $n = 883$, $q = 8089$, $d = 168$. При таких значеннях вхідних параметрів час зашифрування чи розшифрування повідомлень у запропонованих шифросистемах є порівняним з відповідним часом у криптосистемі NTRU Prime [10], яка є одним з фіналістів конкурсу NIST зі створення нових постквантових криптографічних стандартів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] M.R. Albrecht et al., "Estimate all the schemes!", in *Security and Cryptography for Networks*, D. Catalano and R. De Prisco, Eds. Cham, Switzerland: Springer, 2018, vol. 11035, pp. 351-367, doi: https://doi.org/10.1007/978-3-319-98113-0_19.

[2] S. Diop, D.O. Sane, M. Seck, and N. Diarra, "NTRU-LPR IND-CPA: a new ideal lattice-based scheme", *Cryptology ePrint Archive, Report 2018/109*, doi: https://doi.org/10.13140/ RG.2.2. 15424.35840.

[3] V. Lyubashevsky, and G. Seiler, "NTTRU: Truly fast NTRU using NTT", *ACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2019, iss. 3, pp. 180-201, 2019, doi: https://doi.org/10.13154/tches.v2019.i3.180-201.

[4] M.R. Valluri, "NTRUCipher-lattice based secret key encryption", in *Proc. World Congress on Internet Security*, Cambridge, 2017, pp. 1-5, doi: https://doi.org/10.48550/arXiv.1710. 01928.

[5] А.А. Матійко, "BKW-атака на шифросистеми NTRUCIPHER та NTRUCIPHER+", *Information Technology and Security*, vol. 8, iss. 2 (15), pp. 164-176, July – December 2020, doi: https://doi.org/10.20535/2411-1031.2020.8.2.222599.

[6] А.А. Матійко, та А.М. Олексійчук, "Швидка розрізнювальна атака на шифросистему NTRUCipher+", *Захист інформації*, т. 22, № 3, с. 183-189, 2020, https://doi.org/10.18372/ 2410-7840.22.14981

[7] А.М. Олексійчук, та А.А. Матійко, "Розрізнювальна атака на шифросистему NTRUCipher", *Кібернетика та системний аналіз,* т. 58, № 2, с. 186-190, 2022, doi: https://doi.org/10.1007/s10559-022-00449-y.

[8] J. Hoffstein, J. Pipher, and J. Silverman, "NTRU: a new high speed public key cryptosystem". [Online]. Available: https://web.securityinnovation.com/hubfs/files/ntru-orig.pdf. Accessed on: Sept. 07, 2022.

[9] D. Coppersmith, and A. Shamir, "Lattice attack on NTRU", in *Proc. Advances in Cryptology – EUROCRYPT'97,* Konstanz, 1997, pp. 52-61.

[10] D.J. Bernstein, Ch. Chuengsatiansup, T. Lange, and Ch. van Vredendaal, "NTRU Prime: reducing attack surface at low cost", in *Proc. Selected Areas in Cryptography – SAC 2017*, Ottawa, 2018, pp. 235-260, doi: https://doi.org/10.1007/978-3-319-72565-9_12.

[11] C. Chen, J. Hoffstein, W. Whyte, and Z. Zhang, "NIST PQ Submission: NTRUEncrypt. A lattice based algorithm", 2017. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography. Accessed on: Sept. 03, 2022.

[12] J. Katz, and Y. Lindell, *Introduction to modern cryptography*. Boca Raton, Florida, USA: CRC Press, 2015.

[13] V. Lyubashevsky, "Towards practical lattice-based cryptography", Doctor of Philosophy in Computer Science University of California, San Diego, CA, USA, 2008. [Online]. Available: https://escholarship.org/uc/item/0141w93p. Accessed on: Aug. 15, 2022.

[14] V. Lybashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings" in *Proc. Advanced in Cryptology – EUROCRYPT 2010*, French Riviera, 2010, pp.1-23.

[15] S.M. Ihnatenko, "Security estimates of a Ring-LWE symmetric cryptosystem against chosen plaintext attack", *Cybernetics and Systems Analysis*, vol. 58, no. 2, pp. 322-325, 2020, doi: https://doi.org/10.1007/s10559-020-00248-3.

[16] А.М. Олексійчук, та М.В. Поремський, "Загальна схема побудови кореляційних атак на SNOW 2.0-подібні потокові шифри", *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, вип. 1 (32), с. 70-79, 2018.

[17] V. Lyubachevsky, L. Ducas, and E. Kiltz, "CRYSTALS–Delithium. Techn. rep. NIST", 2017. [Online]. Available: https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-1-submissions. Accessed on: Sept. 12, 2022.

[18] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography" in *Proc. the 37th Annual ACM Symposium on Theory of Computing*, Baltimore, USA, 2005, pp. 84-93.

[19] А.М. Олексійчук, С.М. Ігнатенко, та М.В. Поремський, "Системи лінійних рівнянь зі спотвореними правими частинами над скінченними кільцями", *Математичне та комп'ютерне моделювання. Серія: Технічні науки*, вип. 15, с. 150-155, 2017, doi: https://doi.org/10.32626/2308-5916.2017-15.150-155

[20] A. May, "How to Meet Ternary LWE Keys", in *Proc. Advances in Cryptology – CRYPTO 2021. Lecture Notes in Computer Science*. Cham, Switzerland: Springer, 2021, vol. 12826, pp. 701-731, doi: https://doi.org/10.1007/978-3-030-84245-1_24.

[21] E. Kirshanova, and A. May, "How to Find Ternary LWE Keys Using Locality Sensitive Hashing", in *Proc. 18th IMA International Conference, IMACC 2021, Virtual Event*, Cham, Switzerland: Springer, 2021, vol. 13129, pp. 247-264, doi: https://doi.org/10.1007/978-3-030-92641-0_12.

[22] A. Blum, A. Kalai, and H. Wasserman, "Noise-tolerant learning, the parity problem, and the statistical query model", *Journal of the ACM*, vol. 50, no. 3, pp. 506-519, 2003, doi: https://doi.org/10.48550/arXiv.cs/0010022.

[23] E. Alkim, L. Ducas, T. Poeppelmann, and P. Schwabe, "Post-quantum key exchange – a new hope", 2016. [Online]. Available: http://cryptojedi.org/papers/#newhope. Accessed on: Sept. 12, 2022.

[24] J.W. Bos, C. Costello, and L. Ducas, "Frodo: take of the ring! Practical, quantum-secure key exchange from LWE*", Proc. of Conference on Computer and Communications Security*, Vienna, 2006, pp. 1006-1018, doi: https://doi.org/10.1145/2976749. 2978425.

Стаття надійшла до редакції 21.09.2022.

REFERENCES

[1] M.R. Albrecht et al., "Estimate all the {LWE, NTRU} schemes!", in *Security and Cryptography for Networks*, D. Catalano and R. De Prisco, Eds. Cham, Switzerland: Springer, 2018, vol. 11035, pp. 351-367, doi: https://doi.org/10.1007/978-3-319-98113-0_19.

[2] S. Diop, D.O. Sane', M. Seck, and N. Diarra, "NTRU-LPR IND-CPA: a new ideal lattice-based scheme", *Cryptology ePrint Archive, Report 2018/109*, doi: https://doi.org/10.13140/ RG.2.2. 15424.35840.

[3] V. Lyubashevsky, and G. Seiler, "NTTRU: Truly fast NTRU using NTT", *ACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2019, iss. 3, pp. 180-201, 2019, doi: https://doi.org/10.13154/tches.v2019.i3.180-201.

[4] M.R. Valluri, "NTRUCipher-lattice based secret key encryption", in *Proc. World Congress on Internet Security*, Cambridge, 2017, pp. 1-5, doi: https://doi.org/10.48550/arXiv.1710. 01928.

[5] A. Matiyko, "BKW-attack on NTRUCIPHER and NTRUCIPHER+ encryption schemes", *Information Technology and Security*, vol. 8, iss. 2 (15), pp. 164-176, July – December 2020, doi: https://doi.org/10.20535/2411-1031.2020.8.2.222599.

[6] A. Matiyko, and A. Alekseychuk, "Fast distinguishing attack on NTRUCipher+ encryption scheme", *Ukrainian Information Security Research Journal*, vol. 22, no. 3, pp. 183-189, 2020, doi: https://doi.org/10.18372/2410-7840.22.14981.

[7] A. Alekseychuk, and A. Matiyko, "Distinguishing Attack on the NTRUCipher Encryption Scheme", *Cybernetics and Systems Analysis*, vol. 58, no. 2, pp. 186-190, 2022, doi: https://doi.org/10.1007/s10559-022-00449-y.

[8] J. Hoffstein, J. Pipher, and J. Silverman, "NTRU: a new high speed public key cryptosystem". [Online]. Available: https://web.securityinnovation.com/hubfs/files/ntru-orig.pdf. Accessed on: Sept. 07, 2022.

[9] D. Coppersmith, and A. Shamir, "Lattice attack on NTRU", in *Proc. Advances in Cryptology – EUROCRYPT'97,* Konstanz, 1997, pp. 52-61.

[10] D.J. Bernstein, Ch. Chuengsatiansup, T. Lange, and Ch. van Vredendaal, "NTRU Prime: reducing attack surface at low cost", in *Selected Areas in Cryptography – SAC 2017,* Ottawa, 2018, pp. 235-260, doi: https://doi.org/10.1007/978-3-319-72565-9_12.

[11] C. Chen, J. Hoffstein, W. Whyte, and Z. Zhang, "NIST PQ Submission: NTRUEncrypt. A lattice based algorithm", 2017. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography. Accessed on: Sept. 03, 2022.
[12] J. Katz, and Y. Lindell, *Introduction to modern cryptography*. Boca Raton, Florida, USA: CRC Press, 2015.
[13] V. Lyubashevsky, "Towards practical lattice-based cryptography", Doctor of Philosophy in Computer Science University of California, San Diego, CA, USA, 2008. [Online]. Available: https://escholarship.org/uc/item/0141w93p. Accessed on: Aug. 15, 2022.
[14] V. Lybashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings" in *Proc. Advanced in Cryptology – EUROCRYPT 2010*, French Riviera, 2010, pp.1-23.
[15] S. Ihnatenko, "Security estimates of a Ring-LWE symmetric cryptosystem against chosen plaintext attack", *Cybernetics and Systems Analysis*, vol. 58, no. 2, pp. 322-325, 2020, doi: https://doi.org/10.1007/s10559-020-00248-3.
[16] A. Alekseychuk, and M. Poremskyi, "A general scheme for design of correlation attacks on SNOW 2.0-like stream ciphers", *Legal, regulatory and metrological support of information security system in Ukraine*, iss. 1 (32), pp. 70-79, 2018.
[17] V. Lyubachevsky, L. Ducas, and E. Kiltz, "CRYSTALS–Delithium. Techn. rep. NIST", 2017. [Online]. Available: https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-1-submissions. Accessed on: Sept. 12, 2022.
[18] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography" in *Proc. the 37th Annual ACM Symposium on Theory of Computing*, Baltimore, USA, 2005, pp. 84-93.
[19] A. Alekseychuk, S. Ignatenko, and M. Poremskyi, "Systems of linear equations corrupted by noise over arbitrary finite rings," *Mathematical and Computer Modelling, ser. Technical Sciences*, iss. 15, pp. 150-155, 2017, doi: https://doi.org/10.32626/2308-5916.2017-15.150-155.
[20] A. May, "How to Meet Ternary LWE Keys", in *Proc. Advances in Cryptology – CRYPTO 2021. Lecture Notes in Computer Science*. Cham, Switzerland: Springer, 2021, vol. 12826, pp. 701-731, doi: https://doi.org/10.1007/978-3-030-84245-1_24.
[21] E. Kirshanova, and A. May, "How to Find Ternary LWE Keys Using Locality Sensitive Hashing", in *Proc. 18th IMA International Conference, IMACC 2021, Virtual Event*, Cham, Switzerland: Springer, 2021, vol. 13129, pp. 247-264, doi: https://doi.org/10.1007/978-3-030-92641-0_12.
[22] A. Blum, A. Kalai, and H. Wasserman, "Noise-tolerant learning, the parity problem, and the statistical query model", *Journal of the ACM*, vol. 50, no. 3, pp. 506-519, 2003, doi: https://doi.org/10.48550/arXiv.cs/0010022.
[23] E. Alkim, L. Ducas, T. Poeppelmann, and P. Schwabe, "Post-quantum key exchange – a new hope", 2016. [Online]. Available: http://cryptojedi.org/papers/#newhope. Accessed on: Sept. 12, 2022.
[24] J.W. Bos, C. Costello, and L. Ducas, "Frodo: take of the ring! Practical, quantum-secure key exchange from LWE*", Proc. of Conference on Computer and Communications Security*, Vienna, 2006, pp. 1006-1018, doi: https://doi.org/10.1145/2976749. 2978425.

ALEXANDRA MATIYKO,
ANTON ALEKSEYCHUK

METHOD FOR DESIGN SECURE SYMMETRIC NTRU-LIKE ENCRYPTION SCHEMES

Asymmetric NTRU-like encryption schemes are among the fastest modern post-quantum cryptosystems. They are designed on simple (from the point of view of implementation complexity) transformations in truncated polynomials rings and provide required security against well-known attacks if their parameters are properly chosen. The security of such encryption schemes is based on the difficulty of finding short vectors in certain lattices in Euclidean space. Almost a third of all

post-quantum cryptographic algorithms submitted to the NIST competition for standardization of post-quantum cryptographic primitives belong to NTRU-like (or close to them as Learning With Errors) cryptosystems. Along with that, an actual task is to create symmetric cryptosystems, the security of which (similarly to asymmetric ones) is based on the complexity of solving only one computationally hard problem. As of now, the only one symmetric NTRU-like encryption scheme is known that is not secure against certain chosen plaintexts attacks – NTRUCipher. The purpose of this article is to develop a method for design symmetric NTRU-like cipher systems that are secure against specified attacks (CPA secure). It is shown that the security of proposed encryption schemes is based on the hardness of the Decision-Ring-LWE problem, which is one of the well-known computationally hard problems in lattice-based cryptography. It is shown that, unlike the previously known NTRUCipher encryption scheme, the proposed encryption schemes are secure against chosen-plaintext attacks. Concurrently, the proposed encryption schemes have the same secret key length as the NTRUCipher encryption scheme. An algorithm for choosing the parameters that ensure the security of proposed encryption schemes at a predetermined level, is presented. It is shown that the time of encryption or decryption messages in proposed encryption schemes is comparable to the corresponding time in the NTRU Prime cryptosystem, which is one of the finalists in the NIST competition of design new post-quantum cryptographic standards.

Keywords: post-quantum cryptography, symmetric encryption scheme, NTRUCipher, NTRU Prime, security proof.

Матійко Александра Андріївна, викладач кафедри безпеки державних інформаційних ресурсів, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0002-6947-5958, alexm1710@ukr.net.

Олексійчук Антон Миколайович, доктор технічних наук, доцент, професор кафедри безпеки державних інформаційних ресурсів, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0003-4385-4631, alex-dtn@ukr.net.

Matiyko Alexandra, lecturer at the state information resources security academic department, Institute of Special Communication and Information Protection of the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.

Alekseychuk Anton, doctor of technical science, professor, professor at the state information resources security academic department, Institute of Special Communication and Information Protection of the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.