УДК 004.056.55

І.Д. ГОРБЕНКО, д-р техн. наук, О.Г. КАЧКО, канд. техн. наук, М.В. ЄСІНА, канд. техн. наук

АНАЛІЗ АЛГОРИТМУ НАПРАВЛЕНОГО ШИФРУВАННЯ NTRU PRIME IIT UKRAINE З УРАХУВАННЯМ ВІДОМИХ АТАК

Вступ

У 2016 – 2017 роках відбувся ряд значущих подій, які уже суттєво вплинули на інтенсивний розвиток постквантової криптографії. До них слід віднести статтю Alfred J. Menezes та Neal Koblitz [2], організацію та проведення NSA та NIST США VII міжнародної конференції з постквантової криптографії [5, 6]. Надзвичайно важливою подією стало опублікування в США звіту «Report on Post – Quatum Cryptography. NISTIR 8105 (DRAFT)» [3], в якому було підтверджено можливості успішного квантового криптоаналізу асиметричних криптосистем електронного підпису (ЕП), а також визначені основні проблеми та можливості і етапи їх вирішення.

NIST США, розуміючи необхідність пошуку нових асиметричних криптографічних примітивів ЕП та асиметричного направленого шифрування (НШ), які будуть актуальними та можуть застосовуватись у постквантовий період, оголосив конкурс на розробку стандартів постквантових асиметричних криптографічних примітивів [5]. Вказане обумовлено двома факторами. По-перше, спостерігається помітний прогрес у розвитку квантових комп'ютерів, у тому числі проводяться експериментальні демонстрації реалізації фізичних кубітів, які можуть бути масштабовані до більших систем. Підтвердженням цьому є послідовний анонс IBM 20, 50 та 53 – кубітних квантових комп'ютерів [26, 27].

По-друге, скоріше всього перехід до постквантової криптографії не буде простим, оскільки навряд чи буде простою заміна поточних стандартів асиметричних криптографічних примітивів. Значні зусилля будуть потрібні для того, щоб розробити, стандартизувати та впровадити нові постквантові криптосистеми. Тому повинен бути значний перехідний етап, коли будуть застосовуватись як нинішні, так і постквантові криптографічні примітиви.

Заявки отримувались NIST до 30 листопада 2017 року. Вони стосуються: асиметричних алгоритмів НШ та ЕП. В подальшому очікується їх детальний аналіз та порівняння, причому на це відводиться період до трьох років. Вказане свідчить про суттєву складність проблеми, що має бути вирішена.

Європейський союз також розпочав активну роботу з підготовки нових постквантових стандартів. Європейською організацією зі стандартизації ETSI сформований новий напрямок «Квантово-захищена криптографія» [1, 4, 7]. За результатами даних досліджень прогнозується прийняття групи стандартів для постквантового періоду. ETSI опублікувала груповий звіт «Квантово-захищена криптографія. Квантово-безпечна інфраструктура» [1], в якому закріплено основи перспективної інфраструктури, представлено алгоритми, описано типи примітивів, що будуть використовуватися. Окремо висунуто вимоги та сформовано критерії оцінки майбутніх кандидатів.

За участі авторів цієї статі на конкурс, що проводиться NIST США, подано криптографічний алгоритм НШ «NTRU Prime IIT Ukraine» [10], який розроблено з використанням NTRU [8] та NTRU Prime [9]. Метою цієї статі є загальний огляд та опис запропонованого криптоперетворення, особливості реалізації, оцінка та порівняння основних характеристик та показників з [8 – 10] за критеріями криптографічної стійкості від існуючих та потенційно можливих атак.

1. Постановка проблеми

На основі аналізу джерел [8, 9] стосовно існуючих на сьогоднішній день алгоритмів НШ, їх особливостей, переваг та недоліків, а також стійкості до атак було визначено, що на їх основі можливо створити новий алгоритм НШ, який буде поєднувати головні переваги існуючих та не буде мати певних недоліків. В результаті широких досліджень обґрунтовано

сутність кандидату, розроблено його реалізації, що мають переваги відносно відомих, зроблено випробовування та оцінки основних характеристик. У листопаді 2017 року повний комплект опису проекту та програмні реалізації були надіслані та отримані NIST США [5]. Вважається за необхідне статтю розглядати як перший етап попереднього дослідження нашої пропозиції та ознайомлення широкого загалу з проблемою створення постквантового стандарту асиметричного НШ. Таким чином, метою цієї статі є обґрунтування та викладення основних ідей побудови постквантового стандарту асиметричного НШ, аналізу стану робіт в указаному напряму, викладення сутності відмін пропозиції «NTRU Prime IIT Ukraine» від відомих, а також обговорення результатів оцінки та випробовування стосовно вимог, що висунуті NIST США.

Аналіз вимог до постквантових криптоперетворень асиметричного шифрування дозволяє зробити висновок, що основною, причому безумовною вимогою щодо «NTRU Prime IIT Ukraine», є вимога криптографічної стійкості щодо відомих та потенційно можливих атак. Вказані атаки можуть бути реалізовані з використанням як класичних атак на основі використання класичних комп'ютерних систем та класичних математичних методів, а також на основі квантових комп'ютерів та відповідних математичних і програмних методів. Очевидно, що криптографічні асиметричні перетворення, повинні забезпечувати захист як від класичних, так і квантових методів криптоаналізу. Вказане повинне враховуватись, по можливості, при побудуванні та аналізі постквантових криптоперетворень, прийнятті на їх основі постквантових стандартів асиметричних криптоперетворень.

2. Опис та аналіз загальних параметрів сучасних NTRU-подібних алгоритмів НШ

Розглянемо далі існуючі сьогодні алгоритми направленого шифрування та створений на їх основі новий алгоритм направленого шифрування «NTRU Prime IIT Ukraine» [8 – 10].

Аналіз алгоритму шифрування NTRU. NTRU – перша криптографічна система відкритого ключа, яка не ґрунтується на факторизації чи проблемі дискретного логарифмування. NTRU ґрунтується на проблемі найкоротшого вектору в решітці. Операції ґрунтуються на об'єктах в зрізаному кільці поліномів $R = \mathbf{Z}[x]/(x^n - 1)$, степінь полінома не більше $n-1$.

Параметрами NTRU є наступні: n – поліноми у кільці R мають ступінь $n-1$ (не таємний); q – великий модуль, за яким зводиться кожний коефіцієнт (не таємний); p – малий модуль, за яким зводиться кожний коефіцієнт (не таємний); f – поліном, що є секретним ключем; g – поліном, який використовується для генерації відкритого ключа h з f (секретний, але відкидається після початкового використання); h – відкритий ключ, також поліном; r – випадковий "засліплюючий" поліном (секретний, але відкидається після початкового використання); d – коефіцієнт.

Зашифрування відкритого повідомлення m здійснюється за формулою $c = rh + m$.

Розшифрування виконується наступним чином: з використанням особистого полінома f обчислюється поліном $a = f \cdot e (\mathrm{mod}\, q)$. Далі обчислюється поліном $b = a \bmod p$. Використовується ще один особистий поліном f_p для обчислення $c = f_p \cdot b (\mathrm{mod}\, p)$, де c і є вихідним повідомленням m.

Більш детально про алгоритм NTRU описано у [8].

3. Аналіз алгоритму шифрування NTRU Prime

Криптосистема NTRU Prime запропонована як один з альтернативних варіантів асиметричного методу NTRU з метою позбутися слабких місць, притаманних NTRU, які пов'язані з небажаними структурними властивостями кільця $\mathbf{Z}_q[x]/(x^n - 1)$: у багатьох випадках кільце такого виду має підкільця та фактор кільця великого порядку. На відміну від NTRU, в NTRU Prime використовується кільце $\mathbf{Z}_q[x]/(x^n - x - 1)$, яке за умови належного вибору чисел q і

n, є полем, що не містить власних підполів. Крім того, група Галуа полінома $x^n - x - 1$ над полем Q є симетричною групою S_n, що виключає можливість проведення на криптосистему атак певного виду.

У NTRU Prime відкритий ключ обчислюється за формулою $h = g / 3f$, що має значення для створення ефективного протоколу передачі секретних ключів. Однак для побудови асиметричної шифрувальної системи бажано використовувати традиційну формулу $h = 3g / f$.

Розшифрування повідомлень у криптосистемі NTRU Prime відбувається коректно за умови $q > 48t$.

Детальніше про алгоритм NTRU Prime описано у [9].

4. Аналіз алгоритму шифрування NTRU Prime IIT Ukraine

Дане асиметричне криптоперетворення являє собою модифікацію криптоперетворення NTRU та відрізняється від останнього лише двома аспектами:

1. Замість кільця $\mathbf{Z}_q[x]/(x^n - 1)$, що використовується в NTRU, застосовується поле $\mathbf{Z}_q[x]/(x^n - x - 1)$, як у криптосистемі NTRU Prime [9]. Згідно з [9] це унеможливлює проведення на криптосистему атак деякого виду та виключає можливість скористатися (принаймні, потенційними) слабкостями стандартної криптосистеми NTRU, які пов'язані з існуванням нетривіальних підкілець чи факторкілець кільця $\mathbf{Z}_q[x]/(x^n - 1)$.

2. У запропонованому криптоперетворенні поліноми F та r є довільними t-малими, тобто мають $2t$ ненульових коефіцієнтів, які дорівнюють ± 1, в той час як в [8] кожен з зазначених поліномів має точно t ненульових коефіцієнтів, які дорівнюють 1 та -1 відповідно. Аналогічне зауваження справедливе і для полінома g, який є довільним малим поліномом у модифікованій криптосистемі та має однакову кількість ненульових коефіцієнтів, які дорівнюють 1 та -1 відповідно в NTRU. Ця відмінність не є суттєвою, проте надає можливість розширити обсяг ключового простору в порівнянні з NTRU без втрати ефективності реалізації алгоритмів формування ключів та зашифрування-розшифрування повідомлень.

У даному алгоритмі секретним ключем є будь-яка пара поліномів (f, g), де $f = (1 + 3F) \bmod q$, $F, g \in R/3$, $\| F \|_1 = 2t$, а відповідним відкритим ключем – поліном $h = 3g / f \in R/q$.

Зашифрування відкритого повідомлення m здійснюється за формулою $c = m + rh$, де r – випадковий рівноймовірний t-малий поліном, h – відкритий ключ, а додавання та множення здійснюються в полі R/q.

Для відновлення повідомлення m за повідомленням c за допомогою секретного ключа (f, g), слід обчислити $m' = (cf \pmod q) \bmod 3$ та покласти $m'' = (m' f^*) \bmod 3$. Тобто, для розшифрування повідомлень використовуються тільки поліноми f та f^*, де f^* є оберненим до елемента $f \bmod 3$ в кільці $R/3$.

У «NTRU Prime IIT Ukraine» за допомогою відповідних оцінок, що вказані в описі алгоритму, можна (дозволяється) помітно послабити умову щодо розшифрування повідомлень порівняно з NTRU Prime, а саме, замінити її умовою $q > 32t$. А це, в свою чергу, надає можливість зменшити значення q порівняно з NTRUPrime, зберігаючи при цьому коректність розшифрування.

Більш детально алгоритм «NTRU Prime IIT Ukraine» описано у [10].

5. Аналіз алгоритму з урахуванням відомих атак щодо «NTRU Prime IIT Ukraine»

Проведемо аналіз стійкості алгоритму направленого шифрування «NTRU Prime IIT Ukraine» [10] щодо відомих атак.

Атака «зустріч посередині»

Зазначимо, що дана атака на сьогодні реалізується на звичайних комп'ютерах, але безумовно, можлива її реалізація і на квантових комп'ютерах.

Задача відновлення секретного ключа $(f = (1+3F) \bmod q, g)$ за відкритим ключем h криптосистеми зводиться до розв'язання рівняння $(h' + Fh') \bmod q = g$ відносно невідомих $F, g \in R/3$, де $\| f \|_1 = 2t$ і $h' = (3^{-1}h) \bmod q$. Цю задачу можна сформулювати таким чином.

Нехай $\Phi = \{F \in R : \| F \|_\infty = 1, \| F \|_1 = 2t\}$. Треба знайти поліном $F \in \Phi$ такий, що

$$\| (h' + h'F) \bmod q \|_\infty = 1. \tag{1}$$

Трудомісткість розв'язання поставленої задачі шляхом повного перебору всіх поліномів $F \in \Phi$ потребує $|\Phi| = 4^t \binom{n}{2t}$ операцій. Для зменшення трудомісткості можна застосувати атаки під загальною назвою «зустріч посередині».

Опишемо загальну схему побудови таких атак, базуючись на ідеях робіт [11, 13, 14].

Задамо множини $\Phi_1, \Phi_2 \subseteq \mathbf{Z}^n$ такі, що кожен вектор $F \in \Phi$ має єдине представлення у вигляді $F = F_1 + F_2$, де $F_1 \in \Phi_1$, $F_2 \in \Phi_2$, та певне відображення $D : Z_q{}^n \to \{0,1\}^r$, де $r \le n$.

Алгоритм розв'язання рівняння (1) відносно невідомого $F \in \Phi$ складається з двох етапів, на першому з яких будується таблиця, яка складається з усіх пар $(h'F_1 (\bmod q), D(h'F_1 (\bmod q)))$, розташованих за незростанням цілих чисел, що відповідають двійковим векторам $D(h'F_1 (\bmod q))$, де $F_1 \in \Phi_1$. Потім, на другому етапі для кожного $F_2 \in \Phi_2$ відбувається пошук вектора $D(-h' - h'F_2 (\bmod q))$ серед других компонент пар, які знаходяться в побудованій таблиці. Алгоритм завершується успішно в разі знаходження векторів $F_1 \in \Phi_1$, $F_2 \in \Phi_2$ таких, що $D(h'F_1 (\bmod q)) = D(-h' - h'F_2 (\bmod q))$ та $\| (h' + h'(F_1 + F_2)) \bmod q \|_\infty = 1$.

Зауважимо, що в [9, 11, 13, 14] для різних варіантів криптосистеми NTRU наводяться евристичні оцінки трудомісткості атак зустріч посередині, які базуються на явних чи неявних припущеннях відносно відображення D та розподілу векторів у таблиці, яка будується на першому етапі. Поряд з тим, незалежно від вибору відображення D максимальна трудомісткість описаного алгоритму обмежена знизу значенням $|\Phi_1| + |\Phi_2| \ge 2\sqrt{|\Phi_1||\Phi_2|}$, яке, у свою чергу, є не менше ніж $2\sqrt{|\Phi|} = 2^{t+1} \binom{n}{2t}^{1/2}$.

Таким чином, для забезпечення стійкості криптосистеми «NTRU Prime IIT Ukraine», відносно атак «зустріч посередині» значення n і t вибираються для заданого параметра безпеки k, виходячи з умови

$$2^k \le 2^{t+1} \binom{n}{2t}^{1/2}. \tag{2}$$

Розглянемо надалі атаки в плані їх стійкості при застосуванні квантових алгоритмів [8, 20 – 24], причому спочатку розглянемо атаку «зустріч посередині».

Нехай B – множина булевих багаточленів ступеня N. Також нехай $B(d)$ – підмножина B, багаточлен якого має d коефіцієнтів 1, і $N-d$ коефіцієнтів 0. $T(d+,d-)$ – множина багаточленів, де число коефіцієнтів 1 дорівнює $d+$, а число коефіцієнтів –1 дорівнює $d-$, а інші є 0.

Атака «зустріч посередині» дозволяє при певних умовах криптоаналітику обчислити особистий ключ користувача обраного з простору 2^N елементів за час $O\left(2^{N/2}\right)$. Запропонована атака реалізується наступним чином [9]. Простір особистих ключів ($f=(1+pF) mod\ q$) f розділяється на дві великі частини $f_1 \| f_2$, де f_1 та f_2 мають довжину $N/2$ з $d/2$ одиниць кожен, причому однакове число одиниць досягається циклічним зсувом f при діленні на дві частини. За даної умови на основі ($h = p(f_q^{-1} * g)\ mod\ q$), при $p = 2$, виконується умова, що:

$$f \cdot h = g (\mathrm{mod}\, q) \tag{3}$$

Підставивши замість f його подання у вигляді $f_1 \| f_2$ маємо, що

$$(f_1 \| f_2) \cdot h = g (\mathrm{mod}\, q) \tag{4}$$

Порівняння (4) можна подати у вигляді

$$f_1 \cdot h = g - f_2 \cdot h (\mathrm{mod}\, q) \tag{5}$$

На останок (5) можна подати у вигляді

$$(f_1 \cdot h)_i = \{1,0\} - (f_2 \cdot h)_i (\mathrm{mod}\, q) \forall i \tag{6}$$

Фактично для f може і не виконуватися умова, що половина одиниць попадає в перші $N/2$ записів. Як показано в роботі [23], існує хоча б одне крутіння f, яке буде задовольняти цій властивості, а в якості особистого ключа буде будь-яке крутіння f.

За вказаних умов атака складається з наступних кроків.

1. Визначається число k, яке задовольняє умові:

$$2^k \geq \binom{N/2}{d/2} \tag{7}$$

Далі виділяється пам'ять під 2^k корзин для зберігання багаточленів. Чим більшим буде обрано k, тим швидше буде виконуватися алгоритм, але потрібно буде більше пам'яті.

2. До багаточлену f_1 додається $N/2$ нулів та здійснюється їх перебирання. Перебір займе $\binom{N/2}{d/2}$ кроків. Кожне значення f_1 записується до корзини таким чином, щоб номер корзини, в яку буде поміщатися багаточлен, дорівнював найбільш значимим бітам перших k коефіцієнтів $f \cdot h = g (\mathrm{mod}\, q)$. Позначимо кожну корзину, як $label\_f_1$. При цьому, в деяких корзинах буде по декілька значень багаточленів.

3. Далі аналогічно перебираються багаточлени f_2 та формуються корзини $label\_f_2$, але нульові біти додаються до початку. Сформований багаточлен розміщується до корзин, номер яких формується наступним чином – найбільш значимі біти для перших k коефіцієнтів багаточлену $-f_2 * h (\mathrm{mod}\, q)$, а також найбільш значимі біти для перших k коефіцієнтів багаточлену $-f_2 * h (\mathrm{mod}\, q)$ до кожного коефіцієнту якого додається 1.

4. У випадку, якщо при записі f_2, в корзині є багаточлен f_1, то він вважається добрим кандидатом для відновлення f. Криптоаналітик обчислює $(f_1 \| f_2)\cdot h = g(\mathrm{mod}\, q)$. Якщо він складається з $\{0,1\}$, то особистий ключ знайдено.

Таким чином, при здійсненні атаки з застосуванням методу типу «зустріч посередині» встановлено, що цей алгоритм завжди може повернути результат, який, швидше за все, є особистим ключем f, або циклічним зсувом f.

Згідно [25] часова та просторова складності атаки «зустріч посередині» можуть бути оцінені як

$$O(\frac{C_{N/2}^{d/2}}{\sqrt{N}}), \tag{8}$$

У цілому (8) дозволяє оцінити складності часової та просторової атаки на алгоритм NTRU. Отримані вище співвідношення можна використати для порівняння складності атаки «повне розкриття» з атаками на основі квантових алгоритмів.

Атака на решітках

Відмітимо, що даний тип атак реалізується на звичайних комп'ютерах, але також у майбутньому можлива його реалізація і на квантових комп'ютерах.

Для будь-якого $h \in R/q$ позначимо $L(h)$ решітку у векторному просторі R^{2n+1}, породжену рядками матриці

$$\begin{pmatrix} 1 & 0_{1\times n} & h' \\ 0_{n\times 1} & I_n & H \\ 0_{n\times 1} & 0_{n\times 1} & qI_n \end{pmatrix}, \tag{9}$$

де I_n – одинична матриця порядку n, H – $n\times n$-матриця, i-й рядок якої дорівнює вектору коефіцієнтів полінома $(x^i h) \bmod (x^n - x - 1)$, $i \in \overline{0, n-1}$, $h' = (3^{-1} h) \bmod q$, 3^{-1} – елемент кільця R/q, обернений до 3:

$$3^{-1} = (5+q)/6, \text{ якщо } q \equiv 1 \bmod 3;\ \ 3^{-1} = (5-q)/6, \text{ якщо } q \equiv -1 \bmod 3.$$

Наступне твердження уточнює (для випадку криптосистеми, що розглядається) основний результат роботи [15].

Твердження 1. Якщо вектор $(f = (1+3F) \bmod q, g)$ є секретним ключем криптосистеми, якому відповідає відкритий ключ h, то

$$(1, F, g) \in L(h) \tag{10}$$

та

$$\| (F,g) \|_2 = \left(\sum_{i=0}^{n-1} |F_i|^2 + \sum_{i=0}^{n-1} |g_i|^2 \right)^{1/2} \le \sqrt{n+2t}\,. \tag{11}$$

З іншого боку, якщо вектор (F, g) задовольняє умові (10) та має довжину

$$\| (F,g) \|_2 < \frac{q-2}{12(\sqrt{n}+\sqrt{2t})}, \tag{12}$$

то за допомогою вектора $f = (1+3F) \bmod q$ можна відновити будь-яке вхідне повідомлення m за повідомленням $c = E_h(m,r)$, вважаючи $m = (cf \,(\bmod q)) \bmod 3$.

Доведення. Перша частина твердження випливає безпосередньо з наведених означень.

Для доведення другої частини розглянемо криптограму $c = (m+rh) \bmod q$, отриману в результаті перетворення вхідного повідомлення $m \in R/3$ за допомогою відкритого ключа h і t-малого полінома r.

На підставі умови (10) справедлива рівність $(3g) \bmod q = (fh) \bmod q$. Зауважимо, що $f \neq 0$, оскільки в протилежному випадку $F = 3^{-1}$, $g = 0$ $\| (F,g) \|_2 \geq \frac{q-5}{6} > \frac{q-2}{12(\sqrt{n}+\sqrt{2t})}$, оскільки $q > 48$, що протирічить умові (12).

Використовуючи оцінку ($\| uv \|_\infty \leq 2 \| u \|_\infty \| v \|_1$) та формулу (12), отримаємо, що

$$\| mf + 3rg \|_\infty \leq \| m \|_\infty + 3(\| mF \|_\infty + \| rg \|_\infty) \leq 1 + 6(\| m \|_2 \| F \|_2 + \| g \|_2 \| r \|_2) \leq$$

$$\leq 1 + 6(\| m \|_2 + \| r \|_2) \| (F,g) \|_2 \leq 1 + 6(\sqrt{n}+\sqrt{2t}) \| (F,g) \|_2 < q/2 .$$

Звідси випливає, що $(cf) \bmod q = (mf + 3rg) \bmod q = mf + 3rg$ і, отже,

$$(cf \,(\bmod q)) \bmod 3 = (mf + 3rg) \bmod 3 = (m(1+3F)) \bmod 3 = m .$$

Твердження доведено.

Таким чином, задача відновлення секретного ключа криптосистеми за її відкритим ключем h зводиться до пошуку достатньо короткого вектора (з першою координатою, що дорівнює одиниці) в решітці $L(h)$. Приймаючи звичайне евристичне припущення, що шуканий вектор є найкоротшим ненульовим вектором решітки $L(h)$, приходимо до висновку, що відновлення секретного ключа рівносильно розв'язанню задачі про найкоротший вектор (shortest vector problem (SVP)) для цієї решітки. Зауважимо, що остання задача рівносильна знаходженню вектора, найближчого до вектора $(0_{1\times n}, h')$, у решітці, породженої рядками матриці $\begin{pmatrix} I_n & H \\ 0_{n\times 1} & qI_n \end{pmatrix}$ (closest vector problem (CVP)).

Задача обернення функції E_h або, що рівносильно, відновлення вхідного повідомлення $m \in R/3$ за вихідною криптограмою $c = (m+rh) \bmod q$, де $r \in R/3$, $\| r \|_1 = 2t$, також зводиться до пошуку найкоротшого (або достатньо короткого) вектора решітки $L(h,c)$, породженої рядками матриці

$$\begin{pmatrix} 1 & 0_{1\times n} & c \\ 0_{n\times 1} & I_n & H \\ 0_{n\times 1} & 0_{n\times 1} & qI_n \end{pmatrix}.$$

Обидві решітки $L(h)$, $L(h,c)$ мають однаковий вигляд та відносяться до класу модулярних решіток.

Гібридна атака

Слід вказати, що ця атака реалізується на звичайних комп'ютерах, але також можлива її реалізація у майбутньому і на квантових.

Гібридна атака на класичну криптосистему NTRU запропонована в [13] і в подальшому досліджувалась в багатьох публікаціях. Певним підсумком цих досліджень можна вважати роботу [16], де показано, що оцінки трудомісткості гібридної атаки, отримані раніше для різ-

них криптосистем, є дуже неточними внаслідок помилкових припущень та сумнівних евристичних міркувань, що використовуються для отримання цих оцінок.

Зауважимо, що в [16] також використовуються певні евристичні припущення, тому питання про строго обґрунтовані оцінки трудомісткості гібридної атаки є предметом подальших досліджень.

Стосовно криптосистеми, що розглядається, гібридна атака здійснюється таким чином [16].

Розглянемо решітку $L(h)$, породжену рядками матриці (9), зафіксуємо число $r \in \overline{1, n-1}$ та запишемо матрицю H у вигляді $H = \begin{pmatrix} H_1 \\ H_2 \end{pmatrix}$, де H_1 та H_2 є цілочисельними матрицями розміру $r \times n$ та $(n-r) \times n$ відповідно. Довільний вектор $F \in Z^n$ будемо записувати у вигляді $F = (F_1, F_2)$, де $F_1 \in Z^r$, $F_2 \in Z^{n-r}$.

Помітимо, що вектор $(1, F, g)$ належить решітці $L(h)$ тоді й тільки тоді, коли існує вектор $x \in Z^n$ такий, що

$$F_1(0_{r\times 1}, 0_{r\times(n-r)}, H_1) = -(1, F_2, x)\begin{pmatrix} 1 & 0_{1\times(n-r)} & h' \\ 0_{(n-r)\times 1} & I_{n-r} & H_2 \\ 0_{n\times 1} & 0_{n\times(n-r)} & qI_n \end{pmatrix} + (1, F_2, g). \qquad (13)$$

Остання рівність рівносильна тому, що вектор $F_1(0_{r\times 1}, 0_{r\times(n-r)}, H_1) - (1, F_2, g)$ належить решітці $L_r(h)$, породженої рядками матриці

$$\begin{pmatrix} 1 & 0_{1\times(n-r)} & h' \\ 0_{(n-r)\times 1} & I_{n-r} & H_2 \\ 0_{n\times 1} & 0_{n\times(n-r)} & qI_n \end{pmatrix}.$$

Згідно з [16], гібридна атака залежить від параметрів r, l, c_{-1}, c_1 і спрямована на знаходження вектора $(1, F_1, F_2, g) \in L(h)$, який задовольняє таким умовам:

а) F_1 є малим вектором, що має точно $2c_{-1}$ координат, які дорівнюють -1, та $2c_1$ координат, які дорівнюють 1;

б) (F_2, g) є малим вектором, що має евклідову норму l.

Атака складається з двох етапів, на першому з яких тим чи іншим чином будується редукований базис B решітки $L_r(h)$. Далі, на другому етапі, перебираються вектори F_1, що задовольняють умові (а), за якими обчислюються вектори $(v, F_2, g) = \mathrm{NP}_B(\hat{F}_1)$, де $v \in Z$, а $\mathrm{NP}_B(\hat{F}_1)$ позначає результат застосування до вектора $\hat{F}_1 = F_1(0_{r\times 1}, 0_{r\times(n-r)}, H_1)$ та базису B решітки $L_r(h)$ алгоритму Бабаї. Зазначений алгоритм знаходить «достатньо короткий» вектор $e = \mathrm{NP}_B(\hat{F}_1)$, для якого $\hat{F}_1 - e \in L$, за умови, що базис B є «достатньо добре» редукованим [17].

З рівності (13) та умови (б) випливає, що вектор $\hat{F}_1$ є близьким до решітки $L_r(h)$, тому природно шукати найближчий до нього вектор цієї решітки у вигляді $\hat{F}_1 - \mathrm{NP}_B(\hat{F}_1)$. Крім того, на підставі рівності (13) для будь-якого $F_1 \in Z^r$ вектор $(1, F_1, F_2, g)$ належить решітці

$L(g)$, якщо $\mathrm{NP}_B(\hat{F}_1)=(1,F_2,g)$. Тому все, що залишається перевірити для вектора $\mathrm{NP}_B(\hat{F}_1)$ на другому етапі атаки, є рівність $\nu=1$ та умова (б).

Для того щоб пришвидшити пошук векторів на другому етапі, застосовується метод «зустрічі посередині»: замість векторів F_1, що задовольняють умові (а), перебираються малі вектори f_1 довжини r, кожний з яких має точно c_{-1} координат, що дорівнюють -1, та c_1 координат, що дорівнюють 1. Кожний вектор f_1 зберігається у геш-таблиці за адресами з певної множини $A(f_1)$, яка залежить тільки від вектора $\mathrm{NP}_B(\hat{f}_1)$, де $\hat{f}_1 = f_1(0_{r\times 1}, 0_{r\times(n-r)}, H_1)$, та складається з деяких двійкових векторів довжини $2n-r+1$. Множини адрес збудовані таким чином, що $A(f_1')\cap A(f_1'')\neq\varnothing$, якщо різниця між векторами $\mathrm{NP}_B(\hat{f}_1')$ та $\mathrm{NP}_B(\hat{f}_1'')$ є малим вектором.

Кожного разу, коли в процесі перебору здійснюється повторне звернення до таблиці за тією ж самою адресою, тобто для деяких векторів f_1', f_1'', що перебираються, виконується умова $A(f_1')\cap A(f_1'')\neq\varnothing$, обчислюється вектор (F_1,F_2,g), де $F_1 = f_1' + f_1''$, $(\nu,F_2,g)=\mathrm{NP}_B(\hat{f}_1')+\mathrm{NP}_B(\hat{f}_1'')$, для якого перевіряються умови (а) і (б) та рівність $\nu=1$. Отже, атака завершується успішно, якщо існує пара малих векторів f_1', f_1'', що задовольняють таким умовам:

(а′) кожний з векторів f_1', f_1'' має точно c_{-1} координат, що дорівнюють -1, та c_1 координат, що дорівнюють 1;

(б′) вектор $F_1 = f_1' + f_1''$ задовольняє умові (а);

(в′) вектор $\mathrm{NP}_B(\hat{F}_1)$ дорівнює $\mathrm{NP}_B(\hat{f}_1')+\mathrm{NP}_B(\hat{f}_1'')$, має першу координату $\nu=1$ і задовольняє умові (б).

У [16] з використанням евристичних міркувань отримано формулу для трудомісткості другого етапу описаної атаки:

$$T_2(\delta,r)=\frac{2^{15}r!}{c_{-1}!c_1!(r-c_{-1}-c_1)!}\left(\binom{2c_{-1}}{c_{-1}}\binom{2c_1}{c_1}p\,|S|\right)^{-1/2}\frac{1}{\tilde{p}}, \tag{14}$$

де

$$p=\prod_{i=1}^{2n-r+1}\left(1-\frac{1}{r_i B\left(\frac{2n-r}{2},\frac{1}{2}\right)}\int_{-r_i-1}^{-r_i}\int_{\max\{-1,z-r_i\}}^{z+r_i}(1-t^2)^{\frac{2n-r-2}{2}}dtdz\right), \tag{15}$$

$$|S|=2+2(n-t-1)p_S, \tag{16}$$

$$p_S=\frac{p_{\mathrm{NP}}2^{-4c_1}r!}{(2c_{-1})!(2c_1)!(r-2c_{-1}-2c_1)!}\binom{n-r}{4t-4c_1}\binom{n}{2t}^{-1}, \tag{17}$$

$$p_{\mathrm{NP}}=\prod_{i=1}^{2n-r+1}\left(1-\frac{2}{r_i B\left(\frac{2n-r}{2},\frac{1}{2}\right)}\int_{-1}^{\max\{-r_i,-1\}}(1-t^2)^{\frac{2n-r-2}{2}}dt\right), \tag{18}$$

$$\tilde{p}=1-(1-p_S)^{n-t}. \tag{19}$$

У формулах (15), (18) $B(\cdot,\cdot)$ позначає бета-функцію Ейлера, а числа r_i визначаються за формулами

$$r_i = \frac{R_i(\delta)}{2l},\ i \in \overline{1, 2n-r+1}, \tag{20}$$

де

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

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

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

При цьому рекомендується використовувати такі значення параметрів:

$$|c_{-1}| = |c_1| = \left\lceil \frac{rt}{2n} \right\rceil,\ l = \sqrt{\frac{2n}{3} + \frac{2t(n-r)}{n}}. \tag{21}$$

Для оцінювання першого етапу гібридної атаки (побудови редукованого базису B решітки L) використовується традиційний підхід [18]. Вважається, що базис B будується за допомогою блокового алгоритму Коркіна – Золотарьова: BKZ 2.0 [19] (який вважається на сьогодні одним з найкращих алгоритмів розв'язання подібних задач). Алгоритм BKZ 2.0 залежить від натуральних параметрів β і m, що позначають так звані довжину блоку та кількість ітерацій відповідно, і дозволяє будувати редукований за Коркіним – Золотарьовим базис повної решітки вимірності $2n-r+1$ за $2^{E(\beta,m,2n-r+1)}$ операцій, де

$$E(\beta, m, 2n-r+1) = 0{,}000784314\beta^2 + 0{,}366078\beta + \log((2n-r+1)m) + 0{,}875 \tag{22}$$

(зауважимо, що формула (22) є емпіричною оцінкою, яка базується на результатах обчислювальних експериментів [18]).

Мірою якості редукованого базису, який будується за допомогою алгоритму, є так званий кореневий фактор Ерміта (root Hermite facror): число $\delta > 1$, що визначається за формулою

$$\| b_1 \|_2 = \delta^{2n-r+1} \left(\det L(H_2, h)\right)^{\frac{1}{2n-r+1}} = \delta^{2n-r+1} q^{\frac{n}{2n-r+1}},$$

де b_1 є найкоротшим вектором у побудованому базисі. У [19] описано симулятор алгоритму BKZ 2.0, який дозволяє обчислювати за вхідним параметром $\delta > 1$ такі значення параметрів β і m, що застосування алгоритму BKZ 2.0 з цими параметрами до будь-якого вхідного базису повної решітки вимірності $2n-r+1$ призводить до її редукованого базису з кореневим фактором Ерміта δ.

Розрахунок трудомісткості $T_1(\delta, r)$ першого етапу гібридної атаки здійснюється наступним чином:

1) використовуючи симулятор алгоритму BKZ 2.0 [19], знайти β і m за вхідними даними $2n-r+1$ і δ;

2) покласти

$$T_1(\delta, r) = 2^{E(\beta,m,2n-r+1)}, \tag{23}$$

де $E(\beta, m, 2n-r+1)$ визначається за формулою (22).

Загальна трудомісткість гібридної атаки обчислюється за формулою

$$T(\delta, r) = T_1(\delta, r) + T_2(\delta, r); \tag{24}$$

при цьому оцінкою стійкості криптосистеми відносно цієї атаки є число $T_{\min} = \min\{T(\delta, r) : \delta > 1, r \in \overline{1, n-1}\}$.

Згідно з [16] для обчислення значення $T_{\min}$ слід для кожного $r \in \overline{1, n-1}$ знайти таке $\delta_r > 1$, що $T(\delta_r, r) = \min\{T(\delta, r) : \delta > 1\}$ та покласти $T_{\min} = \min\{T(\delta_r, r) : r \in \overline{1, n-1}\}$. Для знаходження δ_r можна застосувати ітераційний алгоритм (дихотомії), виходячи з того, що $T_1(\delta, r)$ є спадаючою, а $T_2(\delta, r)$ – зростаючою функцією параметра $\delta > 1$: шукане значення δ_r приблизно дорівнює кореню рівняння $T_1(\delta, r) = T_2(\delta, r)$.

Таким чином, використовуючи формули (14), (23), (24), можна оцінити стійкість криптосистеми, що розглядається, відносно гібридної атаки. Для забезпечення стійкості на рівні k достатньо виконання умови

$$2^k \le T_{\min}. \tag{25}$$

Методи решета

Такі атаки сьогодні реалізуються на звичайних комп'ютерах, але у майбутньому можлива їх реалізація і на квантових комп'ютерах.

Протягом останніх років запропоновано низку алгоритмів розв'язання задач SVP та CVP за допомогою методів решета. Найефективніші з відомих сьогодні таких алгоритмів мають евристичну трудомісткість $(3/2)^{N/2+o(1)}$ при $N \to \infty$, де N – вимірність решітки, причому залишковий член $o(1)$ є додатним [20, 21]. Оскільки в нашому випадку $N = 2n+1$, то для забезпечення стійкості криптосистеми відносно атак, що базуються на методах решета, достатньо виконання умови

$$2^k \le (3/2)^n. \tag{26}$$

Висновки

1. Аналіз вимог до постквантових криптоперетворень асиметричного шифрування дозволяє зробити висновок, що основною, причому безумовною вимогою щодо криптоперетворення «NTRU Prime IIT Ukraine», є вимога криптографічної стійкості щодо відомих та потенційно можливих атак. Вказані атаки можуть бути реалізовані з використанням як класичних атак на основі використання класичних комп'ютерних систем та класичних математичних методів, так і на основі квантових комп'ютерів та відповідних математичних і програмних методів.

2. Очевидно, що криптографічні асиметричні перетворення повинні забезпечувати захист як від класичних, так і від квантових методів криптоаналізу. Вказане має враховуватись, по можливості, при побудуванні та аналізі взагалі постквантових криптоперетворень, та прийнятті на їх основі постквантових стандартів асиметричних криптоперетворень.

3. У криптосистемі «NTRU Prime IIT Ukraine» в якості основного криптоперетворення, як в NTRU Prime, на відміну від NTRU, застосовується перетворення в скінченному полі. Вказане унеможливлює проведення щодо криптографічної системи «NTRU Prime IIT Ukraine» ряду потенційних атак та виключає потенційні слабкості, що присутні криптосистемі NTRU. В основному вони пов'язані з існуванням нетривіальних підкілець чи факторкілець фактор кільця (зрізаних) поліномів.

4. У криптосистемі «NTRU Prime IIT Ukraine» поліноми F та r є довільними t-малими, вони мають $2t$ ненульових коефіцієнтів (+1, -1), в той час як в NTRU кожний з зазначених поліномів має точно t ненульових коефіцієнтів, які дорівнюють 1 та -1 відповідно. Аналогічне справедливе і для полінома g, який використовується у криптосистемі «NTRU Prime IIT Ukraine», є довільним малим поліномом з $2t$ ненульових коефіцієнтів (+1, -1). Вказане дозволяє розширити у порівнянні з NTRU розмір ключового простору без втрати ефективності реалізації алгоритмів формування ключів та виконання алгоритмів зашифрування і розшифрування.

4. Для забезпечення стійкості криптосистеми відносно атаки з відомим відкритим повідомленням, яка базується на переборі векторів $b \in \{0,1\}^{l_2}$, значення l_2 (з урахуванням квантових алгоритмів перебору) повинно бути не менше ніж $2k$, де k – параметр безпеки. При цьому довжина початкового стану генератора гами, що використовується для отримання вектора b, повинна бути не менше ніж $2k+64$ біт.

5. Для криптосистеми «NTRU Prime IIT Ukraine» від найбільш ефективних з відомих потенційних атак необхідно обґрунтовано вибирати параметри n, t і q у залежності від параметра безпеки k. При цьому необхідно забезпечити виконання таких умов:

1) вибирати просте число n таким чином, щоби воно задовольняє нерівності (26);

2) для заданого n вибрати, за умови існування, натуральне t, яке задовольняє нерівності (2);

3) для заданих n та t вибрати проте число $q \geq 48t+3$ таке, щоби поліном $x^n - x - 1$ був незвідним над полем $\mathbf{Z}_q$, та виконувалась умова (25).

6. Достатньою умовою криптографічної стійкості криптоперетворення «NTRU Prime IIT Ukraine» з заданою трійкою параметрів (n,t,q) є безумовне виконання умови (25).

Список літератури: 1. *ETSI GR QSC 001 V.1.1.1 (2016-07).* Quntum-Safe Cryptography (QSC); Quantum-safe algorithmic framework. [Електронний ресурс]. – Режим доступу: https://portal.etsi.org/webapp/workProgram /Report_WorkItem.asp?wki_id=46690. 2. *Koblitz Neal* A riddle wrapped in an enigma / Neal Koblitz, Alfred J. Menezes. – Режим доступу: https://eprint.iacr.org/2015/1018.pdf. 3. *Lily Chen* Report on Post-Quatum Cryptography. NISTIR 8105 (DRAFT) / Lili Chen, Stephen Jordan, Yi-Kai-Liu, Dustin Moody, Rene Peralta, Ray Perlner, Daniel Smith-Tone. – Режим доступу: http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf. 4. *Mosca M.* Setting the Scene for the ETSI Quantum-safe Cryptography Workshop / M. Mosca // E-proceedings of "1st Quantum-Safe-Crypto Workshop", Sophia Antipolis, Sep 26-27, 2013. – Режим доступу: http://docbox.etsi.org/Workshop/2013/201309_CRYPTO/eproceedings_Crypto_2013.pdf. 5. *Post-quantum* crypto project. [Електронний ресурс]. – Режим доступу: http://csrc.nist.gov/groups/ST/post-quantum-crypto/index.html. 6. *Proposed* Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process. [Електронний ресурс]. – Режим доступу: http://csrc.nist.gov/groups/ST/post-quantum-crypto/documents/call-for-proposals-draft-aug-2016.pdf. 7. Quantum Safe Cryptography and Security. An introduction, benefits, enablers and challenges. ETSI White Paper No. 8, 2015. [Електронний ресурс]. – Режим доступу: http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf. 8. *American* National Standard for Financial Services – Lattice-Based Polynomial Public Key Establishment Algorithm for the Financial Services Industry – ANSI X9.98–2010, 2010. – 284 p. 9. *Daniel J.* Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, Christine van Vredendaal: NTRU Prime. – Режим доступу: https://ntruprime.cr.yp.to/ntruprime-20160511.pdf. 10. *Качко О. Г.* Оптимізація NTRU подібного алгоритму для несиметричного шифрування з "незручними параметрами" / О. Г. Качко, Л. В. Макутоніна, О. С. Акользіна // Математичне та комп'ютерне моделювання. Серія: Техн. науки, 2017. – 15 (2017). – С. 79–85. 11. *Hoffstein J.* NTRU: a ring based public key cryptosystem / J. Hoffstein, J. Pipher, J. H. Silverman // Algorithmic Number Theory, Third International Symposium, Portland, Oregon, USA, June 21 – 25, 1998. – Proceedings. – Springer, 1998. – P. 267–288. 12. Campbell P., Groves M., Shepherd D. SOLYLOQUI: a cautionary tale, 2014. – Режим доступу: http:docbox.etsi.org/Workshop/2014/201410_CRYPTO/S07_Systams_and_Ayyacks/S07_Groves_Annex.pdf.
13. *Howgrave-Graham N.* A hibrid lattice-reduction and the meet-in-the-midle attack against NTRU / N. Howgrave-Graham // Advances in Cryptology – CRYPTO 2007. – Proceedings. – Springer-Verlag. – 2007. – P. 150–169. 14. *Howgrave-Graham N.* A meet-in-the-midle attack on an NTRU private key / N. Howgrave-Graham, J. H. Silverman, W. Whyte // Technical report, NTRUCryptosystems, June 2003. Report, 2003. 15. *Coppersmith D.* Lattice attack on NTRU / D. Coppersmith, A. Shamir // Advances in Cryptology – EUROCRYPT'97. – Proceedings. –

Springer-Verlag. – 1997. – P. 52–61. 16. *Wunderer Th.* Revising the hibrid attack: improved analysis and refined security estimates. – Режим доступу: http://eprint.iacr.org/2016/733. 17. *Babai L.* On Lova′sz' lattice reduction and the nearest lattice point problem / L. Babai // Combinatorica. – 1986. – Vol. 5. – № 6(11). – P. 1–13. 18. *Hoffstein J., Pipher J., Schanck J.M., Silverman J.H., Whyte W., Zhang Z.* Choosing parameters for NTRUEncrypt. – Режим доступу: http://eprint.iacr.org/2015/708. 19. Chen Y. BKZ 2.0: better lattice security estimates / Y. Chen, P.Q. Nguyen // Advances in Cryptology – ASIACRYPT 2011. – Proceedings. – Springer-Verlag. – 2011. – P. 1–20. 20. *Горбенко Ю. І.* Спеціальна тема / Ю. І. Горбенко, Р. С. Ганзя // Зб. наук. праць, вип.2(22) Спеціальні телекомунікаційні системи та захист інформації, прим. №59 ДССЗЗІ України. – С. 17–26. 21. *Горбенко Ю. І.* Аналіз стійкості популярних криптосистем проти квантового криптоаналізу на основі алгоритму Гровера / Ю. І. Горбенко, Р. С. Ганзя // Захист інформації. – 2014. – Т. 16, №2. – С. 106–112. 22. *Горбенко Ю. І.* Аналіз шляхів розвитку криптографії після появи квантових комп'ютерів / Ю. І. Горбенко, Р. С. Ганзя // Вісник Нац. ун-ту «Львівська Політехніка». Сер. «Комп'ютерні системи та мережі», 2014. – № 806. – С. 40–49. 23. *J. Silverman and A. Odlyzko*. NTRU Report 004, Version 2, A Meet-The Middle Attack on an NTRU Private Key, Technical Report, NTRU Cryptosysytems, (2003). 24. *A Chosen-Ciphertext* Attack against NTRU. [Електронний ресурс]. – Режим доступу: http://www.iacr.org/archive/crypto2000/18800021/18800021.pdf. 25. *Information* technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms : ISO/IEC 9796-2:2010. – 54 p. 26. *IBM* Raises the Bar with a 50-Qubit Quantum Computer. [Електронний ресурс]. – Режим доступу: https://www.technologyreview.com/s/609451/ibm-raises-the-bar-with-a-50-qubit-quantum-computer/?utm_campaign=add_this&utm_source=twitter&utm_medium=post. 27. *Создан* первый квантовый компьютер на 53 кубитах. [Електронний ресурс]. – Режим доступу: https://hightech.fm/2017/11/30/53-qubit.

Акціонерне товариство
«Інститут інформаційних технологій»,
Харківський національний
університет радіоелектроніки,
Харківський національний
університет імені В.Н.Каразіна

Надійшла до редколегії 06.10.2017