УДК 004 056 55

О.В. ШЕВЦОВ

СУТНІСТЬ ТА ОЦІНКА СТІЙКОСТІ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ В NTRUSIGN

Вступ

Для забезпечення цілісності неспростовності та справжності широко застосовуються електронні цифрові підписи (далі ЕЦП). Створені та знайшли застосування цифрові підписи, що грунтуються на перетвореннях в кільцях (RSA системи), скінченних полях (DSA системи), еліптичних кривих, практично розроблені та випробовуються цифрові підписи на основі гіпереліптичних кривих та спарювання точок еліптичних кривих. Основними недоліками вказаних цифрових підписів є або недостатня стійкість (в першу чергу проти атак повного розкриття), а також для всіх них недостатня швидкодія (складність). В той же час існує необхідність реалізації електронних цифрових підписів в реальному часі (зі швидкістю 10-ки і 100-ні мб/с). Отримані в останні роки теоретичні та практичні результати суттєво підвищують складність підписів, та швидкодія може досягатися на основі використання перетворень в кільцях зрізаних поліномів. Як практично, так і теоретично вказані завдання реалізовані тільки щодо направленого шифрування. Так, результатом останніх досліджень стало обґрунтування та стандартизація алгоритму направленого шифрування (НШ) NTRU у вигляді стандарту США ANSI X9.98, в основу якого покладено криптографічне перетворення в фактор-кільці. Покращені швидкісні характеристики NTRU зробили його більш ефективним поряд із іншими криптосистемами. Тому проявляється великий інтерес і до обґрунтування ЕЦП NTRU – роботи, яка на сьогодні ще триває.

Багато наукових праць [1, 2, 3, 4] присвячено підпису в фактор-кільцях зрізаних поліномів – NTRUSign. Власне NTRUSign доказово стійкий від повного розкриття за умови, що криптоаналітик перехопив тільки одну пару підпис-повідомлення [4]. Проте NTRUSign в поточній версії не має аналогічної стійкості від підробки. Відповідно до цього є доцільним пошук способів забезпечення стійкості підписів в кільцях зрізаних поліномів (далі КЗП).

Всі попередні версії підписів NTRU виявилися вразливими до атак, коли атакуючий може нав’язати підроблене повідомлення [2, 5]. Відтак проблемним, на наш погляд, є доведення та оцінка криптографічної стійкості перетворень в кільцях зрізаних поліномів. Мета статі – визначення сутності криптографічних перетворень в кільцях зрізаних поліномів, математичної моделі ЕЦП NTRUSign, визначення та класифікація потенційно можливих криптоаналітичних атак, а також оцінка їх вразливості.

1. Криптоптосистема NTRU, сучасний стан, діючі стандарти та їх застосування

В 1990-х роках математики Джефрі Хофстейн, Джил Пайфер, Джозеф Сильверман розробили метод асиметричного криптографічного перетворення в фактор кільцях поліномів (далі ФКП) під назвою NTRU, що повністю звучить як N-Th Degree Truncated Polynomial Ring, кільце зрізаних поліномів N-ї степені. По суті, цей метод і на його основі алгоритм були призначені для реалізації криптосистеми з відкритим ключем з меншою складністю і відповідно більш високою швидкодією.

З часу винаходу NTRUEncrypt в 1996 році було запропоновано декілька схем підпису. Першу версію NTRU підпису – NSS (NTRU signature scheme) було представлено на сесії Crypto 2000 року. Проте, згодом вона була зламана [2]. У своїй презентації на Eurocrypt автори NSS переглянули цю схему підпису, і нова схема дістала назву R-NSS (Revised NTRU signature scheme) [2]. Всі попередні версії підпису NTRU мають таку саму захищеність при тих самих параметрах щодо: атак грубої сили, простих зведень в решітках та комбінаторної атаки.

NTRUSign був винайдений між 2001 і 2003 роками винахідниками NTRUEncrypt разом з N. Howgrave-Graham та W. Whyte. Дослідження криптосистеми NTRU є досить актуальним для криптографії через те, що вона, як свідчать її автори [2], залишається стійким до атак із квантовими комп'ютерами. Підпис був стандартизовано EESS1 version 2, аспекти захищеності NTRUSign розглядаються більш детально в IEEE P1363.1 [3] "Проекті Стандарта Специфікацій для криптографії з відкритим ключем, технік, що базуються на важкості задач алгебри решіток". Остання версія підпису NTRUSign мала властивості, що дозволяли сподіватися на її стійкість. Проте вже відомі ефективні атаки на підпис NTRUSign із пертурбаціями [1]. Пертурбація – це алгоритм, що посилює захист підпису і полягає в тому, що одне повідомлення підписують декількома секретними ключами. Так, вважається, що NTRUSign має доказову стійкість тільки у випадку, якщо секретним ключем підписано одне повідомлення [1]. І, навпаки, – при підписанні одним ключем багатьох повідомлень сукупність таких підписів дає витік інформації про секретний ключ.

NTRU належить до новітнього класу альтернативних схем відкритого ключа – криптографії на основі решіток, яка сама по собі представляє собою активну область для досліджень. Є кілька складних математичних задач, які можуть бути використані для побудови криптосистеми на базі решіток, найпопулярнішою з них є проблема знаходження найкоротшого вектору. Цей напрямок включає в себе такі криптографічні системи, як GGH та NTRU. Згідно з роботами Micciancio і Регева [5], криптографію на основі решіток можна розділити на дві категорії: практичні криптосистеми, такі як NTRU, для яких поки не має доказової стійкості, і теоретичні, такі як матриці на основі навчання з помилками (Learning with Errors, LWE), які мають достатньо сильні докази безпеки, але використовують ключі, які є занадто великими для загального використання. В останні роки ведуться дослідження з об'єднання цих двох категорій і створення нового класу криптографічних систем на основі решіток, які б діяли ефективно як NTRU і були б доказово стійкими як LWE.

Отже, криптографічні конструкції на основі решіток мають великі перспективи для свого використання в інформаційній сфері, так криптосистема NTRU шифрування вже стандартизована (стандарти ANSI X9.98, IEEE 1363.1) і може використовуватися для надання послуги конфіденційності. Стоїть аналогічна задача – створити підпис, який відповідав би сучасним вимогам стійкості та ефективності. Для України є важливим розвиток цього напрямку, враховуючи те, що ця криптосистема є стійкою до квантового криптоаналізу.

2. Математична модель підпису в фактор-кільцях зрізаних поліномів NTRUSign

NTRUSign був винайдений між 2001 і 2003 роками спеціалістами NTRUEncrypt разом з N. Howgrave-Graham та W. Whyte [2]. В алгоритмі NTRUSign базові операції відбуваються в фактор-кільці зрізаних поліномів $K = Z[X]/(X^N - 1)$, де поліном $a(x) \subset K$, може бути представлений вектором його коефіцієнтів наступним чином:

$$a = \sum_{i=1}^{N-1} a_i x_i = (a_0, a_1, ..., a_{N-1}).$$

Безпека підпису NTRU заснована на важкості вирішення задачі знаходження найкоротших чи найближчих векторів (відповідно SVP, CVP) в спеціальних NTRU решітках. Алгебраїчна решітка – дискретна адитивна підгрупа, задана на множині R^N, тобто решітку L можна представити як множину цілочисельних лінійних комбінацій

$$L(b_1, ...b_N) = \sum_{i=1}^{N} x_i b_i : x_1, ..., x_N \in Z$$

N – лінійно незалежних базисних векторів $(\bar{b}_1, ..., \bar{b}_N) \subset R^N$ в N – вимірному просторі, де відповідно N – розмірність решітки, а R – множина дійсних чисел.

Ненульовий вектор решітки мінімальної довжини називається її *найкоротшим вектором*. Під найкоротшим вектором решітки L будемо розуміти вектор, довжина якого

для решітки розмірністю N буде i-й послідовний мінімум $\lambda_i(L)$ – найменший радіус кулі, яка містить i лінійно незалежних векторів:

$$\lambda_i(L) = r, r \in R : \exists v_i \in L, \max_i \|v_i\| \le r,$$

де v_i – це лінійно незалежні вектора.

Іншими словами, нехай U – це базис решітки L. Задача знаходження найкоротшого вектора (задача SVP) полягає в тому, щоб знайти такий вектор $u \in L$, $u \neq 0$, що $\forall v \in L$, $\| u \| \le \| v \|$. Наскільки короткою може бути довжина ненульового вектору в довільній решітці залежить від таких властивостей, як розмірність решітки та її детермінант. Так N-розмірна решітка L має експоненційно багато векторів з нормою $d = \sqrt{N} \det(L)^{1/N}$.

Задача CVP (знаходження найближчого вектора) полягає в знаходженні вектора $v \in L$, який є *найближчим до вектора* w, де $w \in R^N$ та w не знаходиться в L. Тобто треба знайти такий вектор $v \in L$, який мінімізував би Евклідову норму $\| w - v \|$. Тут вираз $\| w - v \|$ означає найменшу відстань між векторами w та v, яка обчислюється як Евклідова норма вектора $\| \cdot \|$. Зокрема, Евклідова норма вектора $a = (a_0, a_1, ..., a_{N-1})$ визначає його довжину та обчислюється за формулою

$$\| a \| = \sqrt{(a_0)^2 + (a_1)^2 + ... + (a_0)^2}.$$

Далі будемо застосовувати поняття *базису мінімальної довжини*, розуміючи такий базис U решітки L який складається із найкоротших векторів $u_i \in L$, тобто $U = (u_0, u_1, ..., u_{N-1})$ і $\forall v \in L, \forall u_i \in U : \| u_i \| \le \| v \|$.

Для зручності оцінки довжини векторів будемо розрізняти *великі вектори* $a = (a_0, a_1, ..., a_{N-1})$, коли їх довжина набагато більша за довжину найкоротшого вектора решітки: $\forall u_i \in U : \| u_i \| = \| a \|$.

Аналогічно будемо використовувати поняття *коротких векторів* $a = (a_0, a_1, ..., a_{N-1})$, коли їх норма приблизно дорівнює [4]: $\| a \| \approx \sqrt{(N-1)/12}$.

Надалі під *довжиною полінома* $a = \sum_{i=1}^{N-1} a_i x_i$ будемо розуміти довжину відповідного вектора $a = (a_0, a_1, ..., a_{N-1})$, тобто під коротким (великим) поліномом будемо розуміти відповідний короткий (великий) вектор у введених вище позначеннях.

Базис, складений із великих векторів, будемо називати великим базисом.

Секретний ключ NTRUSign містить чотири полінома (f, g, F, G), його матричне подання називають *секретним базисом решітки*, який є базисом мінімальної довжини.

Зокрема g, f – це поліноми з коефіцієнтами, вибраними з діапазону {-1,0,1}, і f має інверсію в $(Z/qZ)[X]/(X^N - 1)$, де q – це ціле число і степінь двійки. Поліноми F, G обирають таким чином, щоб виконувалася рівність $fG - Fg = q$, також F, G – це короткі поліноми, тобто норма їх векторного представлення приблизно дорівнює $\| F \| = \sqrt{(N-1)/12}$ [4].

Для перевірки підпису є відкритий ключ: поліном h, що формує так званий *відкритий базис решітки*:

$$\begin{pmatrix} e & h \\ 0 & q \end{pmatrix}$$

Відкритий базис є великим базисом, де e – одинична матриця. Поліном h знаходиться як $h = f^{-1} \cdot g$ та має коефіцієнти з діапазону $[-q/2, q/2]$.

Підпис – це вектор $(s,t) \in L$, котрий знаходиться дуже близько до повідомлення $m = (m_1, m_2)$, де m_1 та m_2 це дві рівні половини полінома m, які при конкатенації утворюють ціле повідомлення $m = m_1 \| m_2$. Повідомлення спочатку гешують, так що m – це, власне, геш функція від повідомлення. Підпис обчислюється таким чином:

$$\begin{aligned} s &\equiv f \cdot B + F \cdot b (mod\ q), \\ t &\equiv g \cdot B + G \cdot b (mod\ q), \end{aligned} \tag{1}$$

де B та b обчилюють із співвідношень

$$\begin{aligned} G \cdot m_1 - F \cdot m_2 &= A + q \cdot B \\ g \cdot m_1 - f \cdot m_2 &= a + q \cdot b \end{aligned} \tag{2}$$

Поліноми *a, A* мають коефіцієнти із діапазона [-1/2, 1/2] та b, $B \in Z[X]/(X^N - 1)$.

Наведені обчислення (1), (2) вирішують задачу CVP за допомогою секретного ключа. Можна обрахувати t інакше: $t = s \cdot h \, mod(q)$, в такому випадку не треба застосовувати при підписанні g [1].

Для зручності рівності (1), (2) можна подати і в матричному вигляді:

$$(s,t) = (B,b)\begin{pmatrix} f & g \\ F & G \end{pmatrix} = \left[(m_1, m_2)\begin{pmatrix} G/q & -g/q \\ -F/q & f/q \end{pmatrix} \right]\begin{pmatrix} f & g \\ F & G \end{pmatrix} = \left[(m_1, m_2)\begin{pmatrix} f & g \\ F & G \end{pmatrix}^{-1} \right]\begin{pmatrix} f & g \\ F & G \end{pmatrix}, \tag{3}$$

де квадратні скобки [ ] є операцією округлення коефіцієнтів полінома до найближчого цілого. По суті, вектор (s,t) у формулі (3) – це вираження вектору (m_1, m_2), в секретному базисі решітки із округленням, причому власне значення (m_1, m_2) подано в ортонормованому базисі.

Правильний підпис демонструє, що підписувач знає точку решітки (s,t) в межах так званої *нормальної границі* $(NormBound)$ від вектора повідомлення m [3]. При перевірці підпису обчислюється відстань від (s,t) до $(m_1 m_2)$, як норма різниці між цими векторами, ця відстань повинна бути не більше ніж заздалегідь обрахована перевірочна відстань $NormBound$:

$$\| s - m_1 \|^2 + \| t - m_2 \|^2 \le NormBound^2.$$

Ця відстань повинна бути малою, так як при реалізації підпису використовуються короткі поліноми, якщо ж відстань від (s,t) до (m_1, m_2) більше ніж $NormBound$, то підпис недійсний, тобто при його виробленні використовувалися поліноми з коефіцієнтами більшими ніж у секретного ключа. Таким чином, дійсний підпис демонструє вирішення задачі знаходження найближчого вектора $(s,t) \in L$ до заданого вектора $(m_1, m_2) \in R$. Величина нормальної границі *NormBound* обраховується заздалегідь за допомогою знаходження математичного сподівання норм векторів, що беруть участь в рівнянні (1). Так, згідно з підрахунками в роботі [3]:

$$NormBound = \frac{c^2 N^2}{6} + \frac{c^2 N^3}{72},$$

де $c = \sqrt{(2\pi e / q\lambda)(\lambda^2 \| f \|^2 + \| 2g \|^2)}$, при $\lambda = 1$.

Для наглядності розглянемо приклад підпису, та визначемо відкритий чи секретний базис більше підходить для підписування. Нехай, для прикладу,

$$q = 32,\ N = 2,\ h = (0, -20).$$

Спочатку побудуємо решітку за допомогою базису мінімальної довжини:

$$(0,3) = f,\ (0,4) = g,\ (0,-5) = F,\ (0,4) = G,$$

та знайдемо точку (s,t), близьку до повідомлення $m = (0,0,0,17)$, тобто $m_1 = (0,0)$, $m_2 = (0,17)$. Також відкритий базис буде сформований як циклічний зсув q та поліномів e,h в матриці з розмірністю $2N$:

$$\begin{pmatrix} 0 & 1 & 0 & -20 \\ 1 & 0 & -20 & 0 \\ 0 & 0 & 0 & 32 \\ 0 & 0 & 32 & 0 \end{pmatrix}$$

Для даного секретного ключа *нормальну границю* *NormBound* можна розрахувати за наступним співвідношенням [6] :

$$\| s - m_1, t - m_2 \|^2 =$$
$$\| (\varsigma_1 f + \varsigma_2 F, \varsigma_1 g + \varsigma_2 G \|^2 .$$

Це більш точна границя для маленьких чисел приклада, в данному випадку:

$$\| (\varsigma_1 f + \varsigma_2 F, \varsigma_1 g + \varsigma_2 G \| =$$
$$\sqrt{(3\cdot 3 + (4\cdot 4) + ((-5) + (-5)) + 2\cdot 2} = 8{,}12$$

Тут $\varsigma_{1,2}$ – поліноми, які мають коефіцієнти в діапазоні (-1/2, 1/2) [6], а значить ними можна знехтувати для приклада з маленькими числами, тобто $\varsigma_{1,2} = 1$.

Підпишемо повідомлення на секретному ключі за формулою (3). Матриця секретного ключа формується циклічним зсувом поліномів даного ключа. Зокрема :

$$\begin{pmatrix} f & g \\ F & G \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 3 & 0 & 4 \\ 3 & 0 & 4 & 0 \\ 0 & -5 & 0 & 4 \\ -5 & 0 & 4 & 0 \end{pmatrix}^{-1} =$$
$$\begin{pmatrix} 0 & 4/32 & 0 & -4/32 \\ 4/32 & 0 & -4/32 & 0 \\ 0 & 5/32 & 0 & 3/32 \\ 5/32 & 0 & 3/32 & 0 \end{pmatrix},$$

звідки

$$(m_1, m_2)\begin{pmatrix} f & g \\ F & G \end{pmatrix}^{-1} =$$

$$(0,0,0,17)\begin{pmatrix} 0 & 4/32 & 0 & -4/32 \\ 4/32 & 0 & -4/32 & 0 \\ 0 & 5/32 & 0 & 3/32 \\ 5/32 & 0 & 3/32 & 0 \end{pmatrix} =$$
$$\left(\frac{85}{32}, 0, \frac{51}{32}, 0\right) \approx (3,0,2,0).$$

Нарешті, маємо підпис

$$(s,t) = (3,0,2,0)\begin{pmatrix} 0 & 3 & 0 & 4 \\ 3 & 0 & 4 & 0 \\ 0 & -5 & 0 & 4 \\ -5 & 0 & 4 & 0 \end{pmatrix} = (0,-1,0,20).$$

Переконаємося, що (s,t) належить решітці: $s \cdot h = (0,-1)\cdot(0,-20) \equiv (0,20)\ mod\ 32 = t.$ Тут і далі операції множення векторів означають множення поліномів.

Тепер, для перевірки підпису, знайдемо відстань між підписом і повідомленням: $\|(0-0)+(0-(-1))+(0-0)+(17-20)\| = \sqrt{10} \approx 3.$ Таким чином, $3 < NormBound = 8{,}12$.

Великий базис не підходить для знаходження найближчого вектора. Спробуємо показати це, для цього підпишемо повідомлення та зробимо перевірку за допомогою відкритого базису.

Маємо

$$\begin{pmatrix} e & h \\ 0 & q \end{pmatrix}^{-1} = \begin{pmatrix} q/q & -h/q \\ 0 & e/q \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 20/32 \\ 1 & 0 & 20/32 & 0 \\ 0 & 0 & 0 & 1/32 \\ 0 & 0 & 1/32 & 0 \end{pmatrix},$$

звідки:

$$(m_1, m_2)\begin{pmatrix} e & h \\ 0 & q \end{pmatrix}^{-1} =$$

$$= (0,0,0,17)\begin{pmatrix} 0 & 1 & 0 & 20/32 \\ 1 & 0 & 20/32 & 0 \\ 0 & 0 & 0 & 1/32 \\ 0 & 0 & 1/32 & 0 \end{pmatrix} =$$

$$(0,0,17/32,0) \approx (0,0,1,0),$$

у результаті отримаємо:

$$(s',t') = (0,0,1,0)\begin{pmatrix} 0 & 1 & 0 & -20 \\ 1 & 0 & -20 & 0 \\ 0 & 0 & 0 & 32 \\ 0 & 0 & 32 & 0 \end{pmatrix} = (0,0,0,32).$$

Отриманий підпис має вигляд $(s',t') = (0,0,0,32)$ і відстань між підписом і повідомленням більше, ніж в попередньому випадку:

$$\| m - s', m - t' \| =$$

$$\sqrt{(0-0)^2 + (0-0)^2 + (0-0)^2 + (17-32)^2} = 15,$$

тому тепер підпис не пройшов перевірку: $15 > NormBound = 8{,}12.$ В першому прикладі відстань між підписом і повідомленням буде найменшою, це означає що підпис в першому прикладі підписаний на секретному ключі, і перший підпис пройшов перевірку.

NTRUSign не є підписом із нульовими знаннями, проте рівень витоку інформації можна значно зменшити, використовуючи пертурбацію.

Для пертурбації генерується певна визначена кількість різних секретних ключів та відповідних ним відкритих ключів. Таким чином, це означає, що підписуюча сторона генерує

решітки $L_1,...,L_b$. У випадку підпису без пертурбації генерується лише одна решітка L_0. Ці решітки генеруються з такими ж параметрами N та q, як і решітка особистого та відкритого ключа L_0, але вони незалежні між собою та L_0. Кожній L_i належать унікальні F_i, G_i, f_i, g_i, h_i. Також кількість наборів секретних ключів, які використовувалися при підписанні із пертурбацією, називається кількістю пертурбацій. Нехай повідомлення – це (0, m), тоді підписання із пертурбацією відбувається за допомогою алгоритму:

Input: на вхід подається $(0, m)$, та набори ключів кількістю $b+1$:
$\{F_0,...,F_b\},\{G_0,...,G_b\},\{f_0,...,f_b\},\{g_0,...,g_b\},\{h_0,...,h_b\}$.
Result: результат роботи алгоритму – підпис s.
Встановити $i = b$;
while: $i > 0$ **do**
Встановити: $(x, y) = (\frac{-m_i \cdot g_i}{q}, \frac{m_i \cdot f_i}{q})$.
Встановити: $s_i = x \cdot f_i + y \cdot g_i$
Обчислити: $m_i = t_i - (s_i \cdot h_{i-1}) \bmod q$.
Встановити: $s = s + s_i$.
$i = i - 1$
if $i = 0$ **then**
зупинка алгоритму, та вивести підпис s;
end if
end while

3. Аналіз стійкості криптоперетворень в фактор-кільцях зрізаних поліномів

Як свідчать дослідження [3, 5], досить важко знайти однопрохідну функцію, побудовану на задачі CVP в решітці, для забезпечення потреб електронного цифрового підпису, яка була одночасно швидкою та криптостійкою. Атаки [5] тільки підтвердили впевненість, що NTRUSign має стійкість лише у разі одноразового використання [9]. Причина витоку ключа із сукупності підписів в тому, що в формулі (3) використовується детермінований алгоритм округлення [ ] коефіцієнтів полінома до найближчого цілого. Для подолання цієї вразливості в останні роки Крисом Пейкертом пропонується змінити цю операцію на випадкове округлення [13].

Стійкість підписів в ФКЗП базується на складності вирішення математичної задачі знаходження найкоротшого вектору в решітці (далі CVP). Нижче наведено складність різних атак на NTRUSign. В табл. 1 в строках 1 – 4 записані складності для атак у випадку, якщо у атакуючого є одна пара підпису та повідомлення, в строках 5,6 – складності атак для підпису із багаторазовим використанням (в атаках використовуються багато перехоплених підписів).

Складності атак для багаторазового використання підпису мають небезпечні значення, тому стоїть проблема як побудувати багаторазовий підпис. Вищевикладене призводить до питання: чи чинний підпис NTRUSign залежить тільки від складності задачі знаходження найкоротшого вектору, чи нема побічних вразливостей. І чи можливо відновлення стійкості даної схеми шляхом заміни техніки пертурбації на більш захищену. Таким чином, залишається відкритим пошук ефективних схем підпису в ФКП із захистом від витоку інформації про секретний ключ із перехоплених підписів та повідомлень [3].

У даному розділі визначається обчислювальна складність функцій вироблення і перевірки ЦП, а також залежність параметрів алгоритмів від необхідного рівня безпеки. Отримані результати порівнюються з аналогічними результатами для формування та перевірки ЦП для RSA та ECDSA алгоритмів [1, 2].

Таблиця 1

Метод	Складність методу
1. Знаходження найкоротшого вектора за допомогою алгоритму LLL [8].	$O(N^3\beta^{\beta/3})$ або $O(N^3(k/6)^{k/4})$
2. Атака груба сила [8].	$O\left(\frac{N!}{df!(N-df)!}\cdot\frac{(N-df)!}{(df-1)!\cdot(N-2df+1)!}\right)$
3. Комбінаторна Атака на ЕЦП [8]. Кількість кроків алгоритма (підбір поліномів f).	$O\left(\frac{C_{N/2}^{df/2}}{\sqrt{N}}\right)$
4. Атака підробки підпису ймовірність успішного здійснення [8] [12].	P (combinatorial forgery) = $\sqrt{\frac{\pi^{\frac{N-1}{2}}}{q^{N-1}\left(\frac{N-1}{2}\right)!}\left(\frac{N}{\beta}\right)^{N-1}} < 2^{-k}$
5. Метод підробки malleability [2].	$O(N)$
6. Атака повного розкриття NTRUSign за допомогою спеціально підібраних повідомлень [3].	$O(N^2)$

При виборі параметрів автори виходили з криптостійкості, яка забезпечується при застосуванні відповідних алгоритмів. В [7, 8] визначено залежність рівня безпеки (еквівалентної довжини ключа k, який треба знайти шляхом повного перебору) від параметрів цифрового підпису для алгоритмів RSA, ECC з простим і двійковими полями і NTRU з кількістю пертурбацій 0, у випадку одноразового підписання (данні про залежність параметрів алгоритмів від необхідного рівня безпеки представлені в табл. 2).

Таблиця 2

Рівень безпеки, k	80	112	128	192	256
Довжина поліномів секретного ключа NTRU	314	394	446	653	743
Двійкова довжина модуля n перетворень RSA	1024	2048	3072	7680	15360
Двійкова довжина простого числа p для базового поля $\mathbf{GF}(p)$ при реалізації ECC	192	224	256	384	521
Ступінь розширення m для базового поля $\mathbf{GF}(2^m)$ при реалізації ECC	163	233	283	409	571

Основним методом криптоаналізу задач, побудованих на знаходженні найменшого вектора, є LLL подібні алгоритми [6]. Час роботи таких алгоритмів прийнято оцінювати в залежності від довжини полінома N. В табл. 3 нижче представленні результати часу виконання атаки LLL, що знаходиться за формулою [7]:

$$\log_{10} T = 0{,}1095 \cdot \mathrm{N} - 12{,}6402,$$

тут N означає максимальну довжину полінома секретного ключа. Таким чином, розмірність решітки буде $2 \cdot N$. В табл. 3 зазначено час T в MIPS-роках, який потребується для зламу підпису для різних параметрів.

Далі наведено результати порівняння процедур формування й перевірки підписів у алгоритмів NTRUSign і RSA за двома критеріям: довжина полінома ключа N і час виконання цих операцій (табл. 4). Данні в таблиці відповідають результатам, отриманим для підпису в Java реалізації [7].

Таблиця 3

Рівень безпеки, k	80	112	128	192	256	360
Довжина поліномів секретного ключа NTRU	314	394	446	653	743	1024
Двійкова довжина модуля n перетворень RSA	1024	2048	3072	7680	15360	-
Час T в MIPS-роках криптоаналізу LLL NTRU	$10^{21.7}$	$10^{30.5}$	$10^{36.1}$	10^{45}	$1,01\cdot10^{68.7}$	$10^{99.48}$
Час T в MIPS-роках криптоаналізу RSA	$1,07\cdot10^{10}$	$1,25\cdot10^{19}$	$4,74\cdot10^{25}$	$1,06\cdot10^{45}$	$1,01\cdot10^{65}$	-

Таблиця 4

Довжина ключа	k	RSA			Довжина ключа	NTRUSign		
		Генерація ключів, мс	Підписання, мс	Перевірка, мс		Генерація ключів, мс	Підписання, мс	Перевірка, мс
512	k <60	200	5	1	-	-	-	-
1024	80	603	10	3	157	491	300	290
2048	112	1753	68	3	394	520	701	503
3072	128	20876	211	6	446	7751	931	1030
7680	192	278876	2981	21	653	19170	5011	2014
15360	256	13170341	42570	753	743	40167	40167	4088

З часом довжини ключів NTRUSign змінювались. Так, згідно із дослідженнями 2005 року в статті [8] залежність рівня захисту від параметрів представлено в табл. 5. Стандарт 2008 року IEEE P1363.1 [9] передбачає наступну залежність рівня захисту від параметрів (в табл.5 представлена залежність параметрів алгоритма NTRUSign від необхідного рівня безпеки):

Таблиця 5

Рівень безпеки, k	80	112	128	192	256
Довжина поліномів секретного ключа NTRU 2005 р.	157	197	223	313	349
Довжина поліномів секретного ключа NTRU 2008 р.	314	394	446	653	743

NTRUSign не має гарантій доказової стійкості. Фактично NTRUSign був зламаний Нгуенгом та Регевом [10], які запропонували поліноміальний алгоритм повного розкриття, використовуючи поліноміальну кількість перехоплених підписів. Так, для розкриття секретного ключа необхідно 400 пар підписів і повідомлень та декілька годин роботи алгоритму криптоаналізу [10]. Повідомлення – це вектори, які оточують точки решітки. Алгоритм підписання знаходить найближчу точку решітки до повідомлення та видає її за підпис. Кожна пара повідомлення та підпис (для повідомлення) належать до вибірки, що рівномірно розподілена в середині N-розмірного паралелепіпеда (задача знаходження схованого паралелепіпеда або HPP), ребра якого будуються за допомогою поліномів секретного ключа. Атака [10] знаходить базис паралелепіпеда за допомогою знаходження мінімуму певної функції багатьох змінних, використовуючи метод градієнтного спуску. Внаслідок успішного криптоаналізу [10] в стандарті [9] було запропоновано посилену схему підпису із пертурбаціями. Проте і вона була зламана для набору параметрів NTRUSign-251 [5], для її успішного завершення необхідно 8000 підписів та декілька годин роботи.

Задача схованого паралелепіпеда (далі HPP) формулюється наступним чином. Нехай $\mathrm{GL_n(R)}$ – це група матриць $n\times n$ з речовими елементами і в групі є зворотні матриці. Нехай є секретний базис $V=\{v_i,....v_n\}\in GL_n(R)$ і також нехай $P(V)=\{\sum_{i=1}^{n}x_iv_i : x_i\in[-1,1]\}$ це паралелепіпед, породжений V. Тоді вхідними даними до алгоритму знаходження HPP будуть

послідовність незалежних вибірок із рівномірного розподілу $D_{P(V)}$. Задача вирішена, якщо

знайдено точне наближення векторів $\pm V$. На практиці замість $D_{P(V)}$ використовують $2(s-m)$ для всіх пар підписів та повідомлень (s,m). Для находження секретного базису це наближення округлюють до найближчих цілих значень. На першому етапі атаки форму паралелепіпеда змінюють на *N*-розмірний куб [10]. Тобто зводять задачу знаходження *N*-розмірного паралелепіпеда до більш легкої задачі знаходження *N*-розмірного куба, який знаходиться за допомогою техніки градієнтного спуска [5]. У випадку із пертурбаціями розподіл вибірки пар підписів та повідомлень змінюється наступним чином. Нехай R та R' – це два секретних базиси, які використовуються послідовно для підписання, тоді розподіл $(s-m)$ перетворюється в $P(R)\oplus P(R')$ тобто розподіл суми Мінковського для двох паралелепіпедів [5]. Ця сума отримується в результаті складання двох рівномірних розподілів від обох паралелепіпедів $P(R), P(R')$. Як наслідок, атака [5] для випадку підпису із пертурбаціями ґрунтується на видозміненні атаки [10] для випадку підпису без пертурбації. Обидві атаки використовують майже ті самі математичні прийоми.

Табл. 6 представляє результати атаки Нгуенга – Регева [5] в залежності від параметрів NTRUSign [5]. Кожна успішно проведена атака зайняла часу менше одного дня, і для виконання алгоритму необхідно до 8 Гб пам'яті.

Таблиця 6

Рівень безпеки, *k* / розмір полінома *N*	*k* < 80 / 94	80 біт / 314	112 біт / 394	128 біт / 446
0 пертурбацій	300:(0,1)	400:(0,1)	400:(0,1)	600:(0,1)
1 пертурбація	1000:(1,2)	5000:(0,1)	4000:(0,1)	4000:(0,1)
2 пертурбації	10000:(5,3)	12000:(0,2)		
3 пертурбації	12000:(5,3)			
4 пертурбації	100000:(0,1)			

Як зазначають автори [5], кожна непорожня чарунка таблиці представляє успішну атаку, де колонки поставлені в залежності від рівня безпеки та розміру полінома ключа, а рядки – в залежності від кількості пертурбацій. Чарунки мають вид $s:(e=\| e_F \|_1, w=\| e_G \|_\infty)$, де *s* це кількість підписів використаних алгоритмом атаки, а $(e_F \mid e_G)$ – вектор помилок в найкращому наближенні, яке отримано за допомогою градієнтного спуску [5]. Складність виконання даного алгоритму атаки близько $(N/2)^{[e/2]+1}$ для такого w.

Подібні експерименти підтверджують теоретичний аналіз, що NTRUSign незахищена при використанні постійної кількості пертурбацій. Також можна побачити, що кількість підписів, необхідних для успішної атаки, росте із зростанням кількості пертурбацій.

В табл. 7 показано рівень стійкості параметрів NTRUSign після атаки [5].

Таблиця 7

Рівень безпеки, *k*	80	112	128	192	256
NTRU довжина поліномів секретного ключа	314	394	446	653	743
Рівень безпеки, *k*, для NTRU з урахуванням атаки [5]	8,34	8,62	8,8	-	-

Відповідно до результатів в таблиці вище видно, що рівень безпеки із врахуванням останньої атаки [5] зменшився до неприйнятного рівня. Немає необхідності нарощувати довжини ключів алгоритму NTRUSign, це, безумовно, погіршить швидкодію підпису, і не змінить базових вразливостей схеми підпису. З одного боку, конструкція алгоритму NTRUSign походить із розробок, які проводились ще до досліджень 2005 – 2015 рр., і це стало причиною, чому підпис постраждав від декількох атак. З іншого боку, навіть сучасні дослідження не сумніваються в актуальності решіток типу NTRU, які досі представляють великий

інтерес для побудови ефективних та захищених схем підпису. Поряд із тим атаки на NTRUSign не вплинули на стійкість NTRU шифрування.

Висновки

Таким чином, деяка дефектність схеми підписів в кільцях зрізаних поліномів випливає із того, що підпис містить інформацію про секретний ключ, так як підпис – це результат арифметичних операцій в фактор-кільці зрізаних поліномів над многочленами секретного ключа. Так, на відміну від NTRUSign, NTRU шифрування при прямому перетворенні використовує відкритий ключ шифрування. Тобто в NTRU шифруванні секретний ключ не застосовується для отримання шифрограм, які потім передаються каналами зв'язку. І перехоплення цих шифрограм призводить до витоку секретного ключа шифрування не в такій мірі, як це відбувається у випадку із підписом. Для NTRUSign постає більш важка задача: при виробленні підписів необхідно запобігати витоку секретного ключа. На сьогоднішній день, із огляду на те, що NTRUSign не може забезпечити багаторазове використання секретного ключа, NTRUSign *не може бути впроваджений* на практиці у чинній редакції. Так як однопрохідні задачі, побудовані на решітках, мають квантову криптостійкість, напрямком подальших досліджень є винайдення та обґрунтування підпису в алгебраїчних решітках із швидкодією, порівняною із нині існуючими системами та криптостійкістю, достатньою для протистояння квантовому криптоаналізу.

NTRUSign на даний момент є зламаним, і причиною тому є вразливість, що міститься в схемі підпису, а не в алгебраїчній решітці, на якій побудована ця схема. Одним із шляхів відновлення стійкості, як пропонують автори Джентри, Пейкерт, Вайкутанатан [13], може бути використання техніки гаусівської вибірки всередині алгоритма NTRUSign. Стаття [13] не присвячена безпосередньо NTRU, проте їх техніка може бути застосована для підпису, побудованого на NTRU решітках або на решітках, дуже подібних до NTRU [11]. Як вважає Лео Дукас [11], вибір решітки для NTRU ще не остаточний і можуть бути інші не гірші варіанти для застосування. З іншого боку, одним із практичних шляхів пошуку стійкого підпису є впровадження нових схем підпису в ФКП, не пов'язаних із алгоритмом NTRU. Новим претендентом міг би стати підпис, запропонований в [11], який використовує техніку вибірки з відхиленням.

Список літератури: 1. *Min Sung Jun*. Weak property of malleability in NTRUSign [Електронний ресурс] / Sung Jun Min, Go Yamamoto, and Kwangjo Kim. Режим доступу: http://www.academy.ualiberty.com/ru/goodsquality/details/174, свободный. 2. *Hoffstein Jeffrey*. NSS: The NTRU Signature SchemeNTRU Cryptosystems [Електронний ресурс] / Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman. Режим доступу: http://www/citeseerx.ist.psu.edu, свободный. 3. *Meskanen Tommi*. On the NTRU Cryptosystem [Електронний ресурс] / Tommi Meskanen. Режим доступу: http://www/tucs./publications/-attachment.php?fname=DISS63.pdf, свободный. 4. *Gentry Craig*. Crypt-analysis of the Revised NTRU Signature Scheme [Електронний ресурс] / Craig Gentry, Mike Szydlo. Режим доступу: http://www.szydlo.com/ntru-revised-short02.pdf, свободный. 5. *Nguyen P. Q*. Learning a Zonotope and More: Cryptanalysis of NTRUSign countermeasures [Електронний ресурс] / L. Ducas, P. Q. Nguyen. Режим доступу: http://www.di.ens.fr/ducas/-NTRUSignCryptanalysis/Ducas-Nguyen/Learning.pdf, свободный. 6. *Hoffstein Jeffrey*. An Introduction to Mathematical Cryptography [Електронний ресурс] / Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman. Режим доступу: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.11182.9999&rep=rep1&type=pdf, свободный. 7. *Sourceforge*. Ntru sourceforgenet, The source code repository. 2012. URL: http: //sourceforge.net/projects/-ntru/?source. 8. *Jeff Hoffstein*. Performance Improvements and a Baseline Parameter Generation Algorithm for NTRUSign (2005) [Електронний ресурс] / Jeff Hoffstein , Nicholas Howgrave-graham , Jill Pipher , Joseph H. Silverman, William Whyte. Режим доступу: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.60.4614 9. *W. Whyte*. IEEE P1363.1 Draft 10: Draft Standard for Public Key Crypto-graphic Techniques Based on Hard Problems over Lattices [Електронний ресурс] / N. Howgrave-Graham, J. Hostein, J. PIpher, J.H. Silverman. Режим доступу: http://grouper.ieee.org/groups/1363/WorkingGroup/contact.html. 10. *Nguyen P. Q*. Learning a Parallelepiped: Cryptanalysis of GGH and NTRU Signatures [Електронний ресурс] / Q. Nguyen, Oded Regev. Режим доступу: http://www.iacr.org/cryptodb/archive/2006/EUROCRYPT/2606/2606.pdf, свободный. 11. *Leo Ducas*. Lattice Signatures and Bimodal Gaussians [Електронний ресурс] / Leo Ducas, Alain Durmus, Tancrede Lepoint, and Vadim Lyubashevsky. Режим доступу: http://homepages.cwi.nl/~ducas/bimodal/bimodal.pdf, свободный. 12. *Прикладна* криптологія. Теорія. Практика. Застосування / Горбенко І. Д., Горбенко Ю. І. – Харків : Форт, 2012. – 868 с. 13. *C. Gentry*. Trapdoors for hard lattices and new cryptographic constructions. [Електронний ресурс] / C. Peikert, and V. Vaikuntanathan. Режим доступу: http://www.cc.gatech.edu/~cpeikert/pubs/trap_lattice.pdf

Харківський національний
університет радіоелектроніки

Надійшла до редколегії 20.04.2015