DOI: 10.18372/2410-7840.18.11092
УДК 004.056.55

ДОСЛІДЖЕННЯ КРИПТОГРАФІЧНИХ АТАК НА СХЕМИ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ В ФАКТОР-КІЛЬЦЯХ ЗРІЗАНИХ ПОЛІНОМІВ

Олександр Кузнецов, Юрій Горбенко, Олексій Шевцов, Тетяна Кузнецова

Одним із важливих засобів отримання послуг аутентифікації є електронний підпис. Дослідження постквантових електронних підписів нині набувають актуальності через можливість виникнення квантового комп'ютера. Криптосистеми на решітках мають ряд переваг, серед яких основною є стійкість від квантового криптоаналізу. Тому питання безпеки підписів на решітках потребує детального вивчення. Запропоновано модель атаки підробки електронного цифрового підпису на решітках NTRUSign за допомогою анулюючих поліномів на схему із пертурбаціями з посиленими параметрами. Досліджено ефективність підробки підпису на NTRUSign та наведено практичні приклади успішної атаки. Отримано експериментальні дані, які показують, що алгоритм підпису при використанні техніки пертурбацій не покращує захисту від досліджуваного виду підробки. Обґрунтовуються оцінки захищеності електронного цифрового підпису NTRUSign із застосуванням техніки пертурбації з посиленими параметрами від дослідженого типу загрози. Практична цінність отриманих результатів полягає в експериментальному доведенні того, що ефективність атаки не суттєво зменшується від збільшення параметрів підпису.

Ключові слова: *фактор-кільця зрізаних поліномів, електронний цифровий підпис, алгебраїчні решітки.*

Вступ. Застосування електронних цифрових підписів (ЕЦП) в фактор-кільцях зрізаних поліномів (ФКЗП) дозволить будувати криптопримітиви, які є стійкими до квантового криптоаналізу [1-5]. Однак всі попередні версії ЕЦП в ФКЗП виявилися вразливими до атак, коли атакуючий може нав'язати підроблене повідомлення [1-3]. Тому дослідження умов та можливостей застосування атак підробки підписів є актуальним науковим завданням.

Підпис в фактор-кільцях поліномів NTRUSign є доказово стійким від повного розкриття за умови, що криптоаналітик перехопив тільки одну пару підпис-повідомлення [5]. Проте, у відомій літературі не проаналізовано можливості атаки типу maleability [1] на підпис із пертурбаціями та на схеми із посиленими параметрами, в тому числі, із гаусовським зашумленням [4]. Підписи в ФКЗП потребують більшого обґрунтування захищеності від підробки даного типу.

Метою статті є розробка моделі атаки підробки підпису NTRUSign, аналіз стійкості NTRUSign та визначення можливості підробки підпису типу malleability (гнучкість) у випадку ЕЦП із посиленими параметрами з використанням техніки пертурбації. В першому пункті розглянуто математичну модель підпису в фактор-кільцях зрізаних поліномів NTRUSign. В другому пункті обґрунтовується модель атаки підробки підпису NTRUSign за допомогою анулюючих поліномів на підпис із багатьма раундами пертурбації, представлено експериментальні результати оцінки ефективності підробки.

1. Математична модель підпису в фактор-кільцях зрізаних поліномів NTRUSign. В алгоритмі NTRUSign [2] 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:

$$a = \sum_{i=0}^{N-1} a_i x^i = (a_0, a_1, ..., a_{N-1}).$$

Визначення 1. Алгебраїчна решітка - дискретна адитивна підгрупа, задана на множині R^N. Решітку L можна представити як множину цілочисельних лінійних комбінацій

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

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

Ненульовий вектор решітки мінімальної довжини називається її *найкоротшим вектором.*

Визначення 2. 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 вектори.

Безпека підпису NTRU заснована на важкості вирішення задачі знаходження найкоротших чи найближчих векторів (відповідно, SVP, CVP) в

спеціальних NTRU решітках. Іншими словами, нехай U – це базис решітки L. Задача знаходження найкоротшого вектору (задача SVP) полягає в тому, щоб знайти такий вектор $u \in L$, $u \neq 0$, що $\forall v \in L$, $\| u \| \leq \| v \|$.

Зауваження 1. 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 вектору) полягає в знаходженні вектору $v \in L$, який є *найближчим до вектору* w, де $w \in R^N$ та w не знаходиться в L. Треба знайти такий вектор $v \in L$, який мінімізував би Евклідову норму $\| w - v \|$. Вираз $\| w - v \|$ визначає найменшу відстань між векторами w та v, яка обчислюється як Евклідова норма вектору $\| \cdot \|$. Зокрема, Евклідова норма вектору $a = (a_0, a_1, ..., a_{N-1})$ визначає його довжину та обчислюється за формулою:

$$\| a \| = \sqrt{(a_0)^2 + (a_1)^2 + ... + (a_{N-1})^2}.$$

Далі будемо застосовувати поняття *базису мінімальної довжини*.

Визначення 3. *Базис мінімальної довжини* - це базис U решітки L який складається із найкоротших векторів $u_i \in L$, тобто $U = (u_0, u_1, ..., u_{N-1})$ і $\forall v \in L, \forall u_i \in U : \| u_i \| \leq \| v \|$.

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 вектору решітки $\forall u_i \in U : \| u_i \| \ll \| a \|$.

Аналогічно будемо використовувати поняття *коротких векторів* $a = (a_0, a_1, ..., a_{N-1})$, коли їх норма приблизно дорівнює $\| a \| \approx \sqrt{(N-1)/12}$ [5].

Надалі під *довжиною полінома* $a = \sum_{i=0}^{N-1} a_i x_i$ будемо розуміти довжину відповідного вектору $a = (a_0, a_1, ..., a_{N-1})$, тобто під коротким (великим) поліномом будемо розуміти відповідний короткий (великий) вектор у введених вище позначеннях.

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

Визначення 4 [5]. Секретний ключ NTRUSign визначається кортежом поліномів (f, g, F, G), де g, f – це поліноми з коефіцієнтами, вибраними з діапазону {-1,0,1}, f має інверсію в $(Z/qZ)[X]/(X^N - 1)$, q - ціле число та степінь двійки, F, G - короткі поліноми з нормою приблизно $\| F \| = \sqrt{(N-1)/12}$ та $fG - Fg = q$.

Матричне подання називають секретним базисом решітки, який є базисом мінімальної довжини.

Визначення 5 [5]. Відкритий ключ NTRUSign визначається поліномом $h = f^{-1} \cdot g$ з коефіцієнтами з діапазону $[-q/2, q/2]$.

Зауваження 2. Поліном h, що формує *відкритий базис решітки*:

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

де e – одинична матриця.

Підпис можна представити двома визначеннями.

Визначення 6 [5]. Нехай $m = (m_1, m_2)$ – хеш-значення повідомлення (далі просто повідомлення) та $m = m_1 \| m_2$ – дві рівні половини полінома m. Підпис визначається вектором $(s, t) \in L$, котрий знаходиться близько до повідомлення. Підпис обчислюється за правилом:

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

де B та b обчислюють із співвідношень

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

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

Наведені формули (1), (2) вирішують задачу знаходження найближчого вектору за допомогою секретного ключа. Можна обчислити t іншим способом $t = s \cdot h \ mod(q)$, в такому випадку не треба застосовувати при підписанні g [1].

Для зручності рівняння (1), (2) можна подати в матричному вигляді.

Визначення 7 [5]. Підпис – це вектор $(s, t) \in L$, який задовольняє рівнянню:

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

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

Зауваження 2.

1. Дійсний підпис демонструє, що підписувач знає точку решітки (s,t) в межах так званої *нормальної границі* $(NormBound)$ від вектору повідомлення m [6]. При перевірці підпису – обчислюється відстань від (s,t) до $(m_1 m_2)$, як норма різниці між цими векторами. Відстань має бути не більшою від заздалегідь обрахованої перевірочної відстані $NormBound$:

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

2. Відстань має бути малою, оскільки при реалізації підпису використовуються короткі поліноми. Якщо відстань від (s,t) до (m_1, m_2) більше, ніж $NormBound$, то підпис є недійсним, тобто при його виробленні використовувалися поліноми з коефіцієнтами, більшими, ніж у секретного ключа.

3. Дійсний підпис демонструє вирішення задачі знаходження найближчого вектору $(s,t) \in L$ до заданого вектору $(m_1, m_2) \in R$. 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 [6]

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

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

4. NTRUSign не є підписом із нульовими знаннями. Рівень витоку інформації можна значно зменшити, використовуючи пертурбацію. Пертурбація – це алгоритм, що посилює захист підпису і полягає в тому, що одне повідомлення підписують кількома секретними ключами.

5. Для пертурбації генерується певна визначена кількість різних секретних ключів та відповідних відкритих ключів. 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 одна від одної та від 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 раундів пертурбацій.

6. Нехай повідомлення – це (0, m), тоді підписання із пертурбацією відбувається за допомогою нижченаведеного алгоритму:

Алгоритм 1.

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: $m_i = t_i - (s_i \cdot h_{i-1}) mod\ q$.

встановити: $s = s + s_i$.

$i = i - 1$

if $i = 0$ then

зупинка алгоритму, та вивести підпис s;

end if

end while

2. Модель атаки підробки підпису ntrusign за допомогою анулюючих поліномів з посиленими параметрами. NTRUSign не завжди може знайти застосування на практиці, наприклад, в системах електронних платежів, адже цьому підписові властива наступна слабкість – наявність кількох підписів для одного повідомлення [1]. Автори роботи називають цю особливість malleability (англ. *гнучкість*). Ця особливість пов'язана з явищем анулюючих поліномів.

Визначення 8. Поліном α називається анулюючим, якщо в нього одинакові коефіцієнти та, відповідно, центрована норма анулюючого полінома $\| \widehat{\alpha(x)} \| = 0$.

Властивості 1[1]. В кільці $R = Zq[X]/(X^N - 1)$ існує q анулюючих поліномів. Для випадкового $r \in R$ анулюючого $\alpha \in Z$:

1) різниця $\| \widehat{r + \alpha} \| - \| \widehat{r} \|$ близька до 0;

2) добуток $\| \widehat{r \cdot \alpha} \| = 0.$

Визначення 9 [1]. Центрована норма полінома $s(x) = x^0 c_0 + \ldots x^m c_m$ знаходиться за формулою

$$\widehat{\| s(x)\|^2} = \sum_{i=0}^{N-1}(c_i - \mu_c)^2 \approx$$
$$\approx \sum_{i=0}^{N-1} c^2 - \frac{1}{N}\left(\sum_{i=0}^{N-1} c\right)^2,$$

де μ_c є середнє арифметичне $\frac{1}{N}\sum_{i=0}^{N-1} c_i$ від коефіцієнтів полінома $s(x) = x^0 c_0 + ...x^{N-1} c_{N-1}$.

Зауваження 3. Центрована норма близька за змістом до стандартного відхилення σ та може бути представлена у вигляді $\widehat{\| s(x)\|} = \sqrt{N}\sigma(s)$. Для полінома з однаковими коефіцієнтами центрована норма дорівнює $\widehat{\| a(x)\|^2} = 0$.

Розглянуті властивості дозволяють побудувати наступну атаку підробки. Основні кроки:

1) криптоаналітик перехоплює дійсний підпис (*s*,*t*) та на основі нього виробляє підробку s':

$s + \alpha = s' \, mod(q)$, де α – це анулюючий поліном;

2) друга половина підпису буде $t' = s' \cdot h \, (mod \; q) = s \cdot h + \alpha \cdot h \, (mod \; q)$;

3) підроблений підпис пройде перевірку у випадку, якщо:

$$\widehat{||t'||} = \widehat{||s \cdot h + \alpha \cdot h||} = \widehat{||s \cdot h||} = \widehat{|t|}.$$

Норма підробленого підпису дорівнює нормі дійсного підпису:

$$\widehat{|| s' - m_1 ||^2} + \widehat{|| t' - m_2 ||^2} =$$
$$\widehat{|| s - m_1 ||^2} + \widehat{|| t - m_2 ||^2} \le NormBound^2.$$

Зауваження 4. Не всі анулюючі поліноми задовольняють рівності $\widehat{\| r + \alpha\|} - \widehat{\| r\|} = 0$. Поліномами, у яких велика ступінь розкиду (відхилення) значень коефіцієнтів від середнього значення коефіцієнтів, мають більшу центровану норму ніж поліноми, що мають невеликий розкид.

Розкид коефіцієнтів - це величина різниці між найменшим та найбільшим коефіцієнтом полінома. Коли значення коефіцієнтів α стають близькими до *q/2,* тоді справедлива нерівність

$$\widehat{\| r + \alpha\|} - \widehat{\| r\|} > 0.$$

Поліном виду $(r + \alpha) \, mod \, (q)$ буде мати більший розкид коефіцієнтів, ніж просто *r*.

Далі наведемо декілька прикладів, щоб показати при якому анулюючому поліномі підробка виконується, а при якому анулюючому поліномі підробка не виконується.

Приклад 1. В даному прикладі моделюється атака методом анулюючих поліномів. Під операцією множення будемо розуміти множення поліномів.

Нехай q = 32, N = 2, h =(0,-20), анулюючий поліном α = (10, 10), поліном s = (0,-1), середнє арифметичне полінома s дорівнює 0, $t = (0,20)$, $s + \alpha = (10,9)$, середнє арифметичне полінома $(s + \alpha)$ дорівнює 9. Обчислимо наступні норми:

$$\widehat{\| s\|^2} = (0-0)^2 + (-1-0)^2 = 1;$$
$$\widehat{\| s + \alpha\|^2} = (10-9)^2 + (9-9)^2 = 1;$$
$$t' = s' \cdot h = (10,9) \cdot (0,-20) =$$
$$= (-8,12) \; mod \; 32.$$

Перевіримо, чи пройде перевірку підроблений підпис (s', t'), тобто, чи виконується нерівність:

$$\widehat{\| m_1 - s'\|^2} + \widehat{\| m_2 - t'\|^2} < Normbound^2.$$
$$(m_1 - s') = (0-10, 0-9); \widehat{\| m_1 - s'\|^2} =$$
$$= (-10+9)^2 + (-9+9)^2 = 1,$$
$$(m_2 - t') = (0+8, 17-12); \widehat{\| m_2 - t'\|^2} =$$
$$(8-6)^2 + (5-6)^2 = 5, \; \widehat{\| m_1 - s'\|} + \widehat{\| m_2 - t'\|} =$$
$$= \sqrt{6} < Normbound = 8,12.$$

Результат – вдалося підробити підпис.

Приклад 2. Нехай q = 32, N = 2, h =(0,-20).

Змінимо анулюючий поліном $\alpha = (12,12)$. Задамо поліном s = (0,-1). Середнє арифметичне полінома s дорівнює 0. Нехай t = (0, 20), $s + \alpha$ = (12, 11). Середнє арифметичне полінома $s + \alpha$ дорівнює 11. Обчислимо норми:

$$\widehat{\| s\|^2} = (0-0)^2 + (-1-0)^2 = 1;$$
$$\widehat{\| s + \alpha\|^2} = (12-11)^2 + (11-11)^2 = 1;$$
$$t' = s' \cdot h = (12,11) \cdot (0,-20) =$$
$$= (16,4) \; mod \; 32.$$

Перевіримо чи пройде перевірку підроблений підпис (s',t'), тобто, чи виконується нерівність:

$$\widehat{\| m_1 - s'\|^2} + \widehat{\| m_2 - t'\|^2} < Normbound^2.$$

$$\left(m_1 - s^{'}\right) = (0-12, 0-11); \| \widehat{m_1 - s'} \|^2 =$$
$$= (-12+11)^2 + (-11+11)^2 = 1,$$

$$\left(m_2 - t^{'}\right) = (0-16, 17-4); \| \widehat{m_2 - t^{'}} \|^2 =$$
$$= (-16+1)^2 + (13+1)^2 = 15^2 + 14^2,$$

$$\| \widehat{m_1 - s'} \| + \| \widehat{m_2 - t'} \| =$$
$$= \sqrt{15^2 + 14^2} > Normbound = 8{,}12.$$

Таким чином, підпис не вдалося підробити.

При проведенні численних експериментів вдалося показати, наскільки на практиці ефективна така атака на підписи, які згенеровано на різних наборах загальносистемних параметрів NTRUSign. Також експериментально визначено, що техніка пертурбації не суттєво захищає від даної загрози.

Результати вдалих спроб підробки підписів, підписаних на різних за довжиною секретних ключах представлені в табл. 1.

Таблиця 1

Кількості підроблених підписів для різних наборів параметрів підпису

Кількість раундів пертурбацій	Довжина поліному N= 157, q=256	Довжина поліному N= 439, q=2048	Довжина поліному N= 743, q= 2048
0	198	1446	1180
1	187	1200	1170
2	155	990	696
3	121	423	515

Для кожного набору параметрів було сформовано q підроблених підписів, а кількість тих підробок, що пройшли перевірку зазначено у відповідних чарунках табл. 1.

Практична цінність отриманих результатів полягає в експериментальному доведенні того, що ефективність атаки не суттєво зменшується від збільшення раундів пертурбацій. Дійсно, як показують результати таблиці 1 кількість підроблений підписів зменшується від кількості пертурбацій, але це зменшення *не є критичним* (приблизно на 10-30% при збільшенні на один раунд пертурбацій). Навіть після 3-х раундів пертурбацій кількість вдало підроблених підписів зменшилася лише у 2-3 рази, що дозволяє фактично порівняти оцінки стійкості ЕЦП NTRUSign із пертурбацією та без пертурбації. Наприклад, для довжини поліному N= 743 з q= 2048 підроблених підписів 1180 проходять перевірку при застосуванні NTRUSign без посиленої схеми, тобто половина всіх підробок вважається справжніми підписами. Якщо застосувати посилену схему із 3-ма раунди пертурбації із 2048 підроблених підписів 515 вважаються справжніми, тобто кількість підробок, які пройшли перевірку, зменшується удвічі, а це замало, щоб стверджувати про істотне покращення захисту. Практично це означає, що застосовувані досі методи посилення стійкості ЕЦП NTRUSign, які були засновані на техніці пертурбації і які, як вважалося, є ефективними, насправді не дають суттєвого виграшу, їх практичне використання втрачає сенс.

Приклад загальносистемних параметрів та ключові данні підпису s (із 3 раундами пертурбації), що було підроблено, та власне підробки s' представлено нижче.

N = 157.

1. Генеруються ключі.

– для першого раунди пертурбації:

F =[3, 2, 3, 4, 1, -3, 0, -2, 4, -7, -4, 1, -2, 1, -4, 1, 1, -7, -3, 0, -1, -4, 0, -7, 1, -2, 1, 1, -1, -4, -1, 2, -6, -2, -2, -1, -6, -2, 4, -2, 0, -6, -4, 1, -4, 1, 0, -1, 1, -1, -1, 0, 4, -6, 1, -4, -10, 2, -3, 3, -8, 2, 4, 1, -4, 1, -1, 1, -3, 2, 3, -2, -4, -1, 2, -1, 3, -4, -1, -3, 0, 0, -1, -1, -3, -1, 1, 0, 0, 10, 3, -3, 1, 2, -1, -5, 0, -2, -5, 0, -6, -1, 3, -1, -1, 1, 2, -2, -3, -3, 1, -4, 0, -1, -5, 1, -1, -2, -2, -4, -3, 3, -4, -1, -5, 2, 1, -1, 1, 2, 3, -1, 1, -2, -2, -2, 4, 1, 2, -2, 1, 1, 5, 1, 1, 0, -4, -4, -5, -3, 1, -2, 0, 1, 1, -3, 2];

f =[1, 0, 0, 0, 0, -1, -1, 0, 0, -1, 0, 1, 0, -1, -1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, -1, 0, 0, 0, 0, -1, 0, 0, 0, 1, 0, -1, 0, -1, 0, 0, 0, 0, 1, -1, 1, 0, 0, 0, 1, 0, -1, -1, 0, -1, -1, -1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, -1, 0, 0, 1, -1, -1, 0, 0, -1, 0, 0, 0, 0, -1, 0, 0, 1, -1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, -1, 0, 1, 1, 0, 1, 1, 0, 0, -1, 0, 0, 0, -1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, -1, 0, 0, 0, 1, -1, 0, 0, 0, 0, 1, 0, 0, 0, -1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, -1, 0, 0, 0, 1, 0, 0, 0, 0, -1, 0, 0];

G =[5, -1, -1, -5, 1, 1, -3, 2, 4, -2, 4, 1, -3, 2, 2, -1, 1, 2, 2, 4, -1, 2, 2, 0, 1, 1, 3, 2, 2, 0, 4, -2, -2, 2, 4, 3, 2, -7, 2, 1, 2, 3, 2, -5, 3, 2, 3, 2, 3, 1, 4, 1, -1, 1, -1, -1, 1, 0, 3, 2, 0, 3, 0, 2, 3, 0, 0, -1, 5, 3, 2, 0, 3, -2, 2, 2, 2, -4, 0, -2, -2, -4, 3, -1, -7, -3, 5, 3, -1, -2, 0, 5, -1, 7, 3, 3, 4, 0, -2, 0, 2, 1, -2, 3, 2, -1, -2, 4, 0, -1, 1, 4, -4, 11, 3, -2, 5, 4, 0, 1, -1, 3, 0, 3, 1, -2, -3, 1, -1, 1, 1, 2, 2, 2, -2, 0, 4, 1, -4, -1, 5, 1, 1, -1, -2, 0, 1, 2, 1, -2, 2, -5, -1, 0, -2, 4, 3];

– для другого раунди пертурбації:

F =[-3, -5, -3, 2, -1, 9, 0, 3, 2, -5, 0, 2, 2, -1, 1, -4, -2, -1, 1, -2, -1, -3, 0, 2, -3, 0, 2, -3, 1, 0, 4, -3, -2, 5, 2, 0, 0, 2, -2, -1, 0, -1, 5, 2, -1, -1, 0, 0, 7, 3, -2, -3, 1, -2, -7, -4, -3, -3, 0, -1, 2, -6, 1, -4, -1, 0, 0, -1, 2, -4, 3, 0, -1, 0, 0, -3, -4, 3, -1, -5, -1, -3, 1, 0, -4, -4, 1, -7, -4, 0, -2, -1, -5, -2, -4, 0, 0, 0, -5, 0, 4, 3, -10, 2, 3, -3, 1, -3, 3, -1,

-6, 2, -1, -5, 0, 2, -1, 2, -1, 2, 0, -6, -4, -1, -6, -2, -1, -3, -3, 2, 1, 2, -1, -1, 0, 0, -2, -3, -3, 1, 3, 0, 0, -2, 0, 0, 5, -3, -3, -4, -3, -3, 0, -3, -2, 4, 1];

f =[1, 0, 0, 1, 0, 0, 0, 1, 0, 0, -1, 0, 1, -1, 0, -1, 0, 0, 0, 1, 1, -1, 1, 0, -1, 0, 1, -1, 0, 1, 0, -1, 0, 0, 0, 0, 0, 0, -1, 0, 0, 1, 0, -1, 1, 0, 0, -1, 0, 0, 0, 0, 0, 0, 1, -1, 0, 0, -1, 0, 0, -1, 0, 0, 1, 0, -1, -1, 0, 0, 0, 0, 0, 0, 0, -1, -1, 0, 0, 0, 0, 0, 0, 0, 1, -1, 0, 0, 0, 0, 0, -1, 0, 1, 0, 0, 1, -1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, -1, 0, -1, 0, 0, -1, 0, 0, 1, 1, 0, -1, 0, 1, 0, 0, -1, 0, 1, 0, 0, -1, 1, 0, -1, 0, 0, 1, 0, 1, 1, 0, 0, -1, 0, 0, 0, 1, 0, -1, 1];

G =[1, 2, 4, -4, 3, -2, 2, -5, 0, -5, 2, 3, 0, -1, 2, 1, -5, 0, 3, 2, -4, 1, -2, 4, 5, -3, 4, 1, 2, 1, -1, 4, 0, 3, -1, 0, -2, 4, -4, -4, 2, -8, 1, 1, -3, 0, 1, 0, 3, 1, 2, 3, -1, 1, 10, 7, 3, 0, 2, 2, 4, 2, 4, 4, 0, 2, 5, 3, -2, -5, -1, 0, -1, 4, 1, 3, 1, -1, -4, 2, 1, 3, 1, -1, 1, 4, 0, -1, 0, 2, 2, -3, 5, 4, -5, 0, -4, -3, -4, 0, 3, 0, 1, 3, 0, -2, -2, 1, 2, 2, -1, 3, 2, 4, 1, -2, 2, 1, 3, 1, -2, 1, 3, 3, 3, 4, -3, 0, 6, 0, 1, 0, 0, -2, 0, -3, -1, 8, 0, 2, -2, 0, 1, 2, 0, 6, 0, -3, 3, 0, 6, 2, 5, 3, 5, 0, 4];

– для третього раунди пертурбації:

F =[0, 2, 5, -2, 0, -5, 2, 2, -4, 3, -3, -4, 0, 1, -1, -2, -3, -2, 1, -2, 0, -3, -2, 1, -2, 1, 0, -2, -3, 4, -3, 3, -3, -1, -7, 2, 1, 2, -6, -1, -1, -1, -1, -4, -4, -1, -2, -1, -5, 0, 2, 1, -1, -2, -1, -3, 5, -2, 2, 2, 0, -1, 1, -2, 1, 1, 3, 0, -3, 3, 4, 0, -2, 2, 2, 1, -2, -3, 0, 1, -2, 1, 0, -2, -3, 2, -2, -5, -4, 0, 1, 4, -2, -5, 1, -2, 3, -8, -4, -1, -2, 2, -3, -2, -5, 0, -3, 2, 2, -3, 0, -3, 2, -2, -5, -4, -4, -5, 2, -1, 4, 2, -2, 2, -3, -5, 1, -1, 3, 2, -5, -1, -3, 0, -2, -1, -3, -4, -3, 5, -5, -1, 5, -2, -2, 4, 1, -4, 0, -2, -3, 3, -4, -2, 0, 3, -2];

f =[1, 0, 1, -1, 0, -1, -1, 1, 0, 0, 0, 0, 0, -1, -1, 0, 1, 0, 1, -1, 1, 0, -1, 0, 1, 0, 0, 1, 0, 0, -1, 0, 0, 0, 0, 0, 0, 1, -1, -1, 0, 1, 0, 0, -1, 0, -1, 0, 0, 0, 0, 1, -1, 0, -1, 0, -1, -1, 1, 0, -1, 0, -1, 0, 1, 0, 0, -1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, -1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, -1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, -1, 0, 0, 0, 0, 0, -1, 1, 1, 0, 0, 0, 0, 0, 1, -1, 0, -1, 0, 0, -1, 1, 0, 0, 0, 0, 0, 0, -1, 0, 1, 0, 0, 0, -1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, -1, 0, 1, 1];

G =[0, 4, 4, 1, 0, 4, 3, 3, 0, 2, 1, -3, -1, -1, -1, 5, 3, 1, -7, 0, 1, -1, -1, 0, 0, 2, -3, -4, 3, -1, -1, 4, -4, -3, 4, -4, 0, -3, 2, 1, 3, 2, 0, 3, 7, 5, -1, -2, 0, 5, 3, 2, -2, 2, 0, 3, 3, 10, 2, 7, 4, 6, 7, 1, 1, 0, -2, 5, 0, 1, 2, 1, -1, 4, 3, 4, -2, -3, 2, 4, 1, 2, -2, 2, 5, -1, 2, -3, -1, 3, -3, 0, -1, 5, 3, -5, -2, -2, 0, -1, -2, -4, 2, -1, 1, -3, 0, 2, 0, 2, -1, -5, 4, 4, 0, 1, 1, 2, -4, -2, 5, 2, 0, -6, 1, 1, 2, 1, 2, 3, 0, -3, -1, 3, 3, 0, -2, 5, -1, 0, 2, 2, 3, -1, -2, -1, 3, 2, 1, -1, 4, -1, -2, 1, 1, 6, -1].

2. Обчислюється підпис для повідомлення.

Message= [38, 145, 238, 14, 230, 133, 86, 205, 33, 124, 160, 109, 228, 169, 186, 99, 238, 110, 116, 89, 170, 170, 126, 216, 173, 82, 8, 75, 128, 133, 39, 186, 28, 113, 47, 83, 123, 247, 100, 213, 159, 128, 87, 250, 77, 176, 209, 158, 197, 231, 211, 127, 197, 67, 25, 156, 109, 220, 91, 143, 30, 141, 164, 76, 119, 181, 220, 244, 153, 49, 73, 13, 181, 133, 255, 9, 165, 235, 108, 213, 140, 196, 142, 154, 1, 100, 221, 235, 23, 13, 100, 225, 102, 22, 16, 117, 123, 210, 4, 90, 168, 52, 100, 119, 206, 62, 179, 10, 158, 33, 229, 222, 161, 201, 7, 235, 246, 69, 96, 52, 115, 41, 160, 150, 16, 0, 212, 180, 117, 234, 10, 18, 135, 56, 124, 202, 205, 182, 59, 31, 186, 113, 43, 210, 180, 144, 56, 1, 239, 116, 23, 75, 199, 246, 217, 169, 113];

s = [17, 253, 217, 251, 7, 236, 235, 247, 241, 22, 236, 2, 6, 5, 4, 34, 2, 224, 25, 4, 29, 253, 238, 248, 30, 230, 244, 234, 35, 248, 8, 255, 255, 247, 254, 27, 236, 255, 10, 49, 250, 252, 15, 22, 9, 241, 11, 10, 8, 245, 13, 7, 27, 232, 249, 46, 226, 9, 7, 27, 230, 24, 253, 25, 19, 243, 250, 0, 14, 232, 238, 220, 10, 246, 23, 25, 8, 31, 15, 16, 249, 12, 31, 26, 238, 218, 252, 251, 16, 237, 22, 229, 14, 238, 248, 4, 238, 5, 240, 15, 229, 2, 6, 248, 20, 254, 237, 5, 237, 3, 2, 242, 255, 5, 26, 7, 2, 253, 34, 213, 247, 251, 250, 26, 220, 251, 4, 9, 241, 16, 255, 243, 6, 253, 226, 240, 255, 246, 255, 226, 20, 11, 10, 0, 12, 4, 237, 12, 219, 234, 250, 238, 13, 6, 230, 229, 242];

3. Обчислюється підроблений підпис з використанням анулюючого поліному α з коефіцієнтами в діапазоні $1 \div q-1$.

Для $q = 256$ маємо:

a = [21, 21];

$s' = s + a(mod q)$ = [38, 18, 238, 16, 28, 1, 0, 12, 6, 43, 1, 23, 27, 26, 25, 55, 23, 245, 46, 25, 50, 18, 3, 13, 51, 251, 9, 255, 56, 13, 29, 20, 20, 12, 19, 48, 1, 20, 31, 70, 15, 17, 36, 43, 30, 6, 32, 31, 29, 10, 34, 28, 48, 253, 14, 67, 247, 30, 28, 48, 251, 45, 18, 46, 40, 8, 15, 21, 35, 253, 3, 241, 31, 11, 44, 46, 29, 52, 36, 37, 14, 33, 52, 47, 3, 239, 17, 16, 37, 2, 43, 250, 35, 3, 13, 25, 3, 26, 5, 36, 250, 23, 27, 13, 41, 19, 2, 26, 2, 24, 23, 7, 20, 26, 47, 28, 23, 18, 55, 234, 12, 16, 15, 47, 241, 16, 25, 30, 6, 37, 20, 8, 27, 18, 247, 5, 20, 11, 20, 247, 41, 32, 31, 21, 33, 25, 2, 33, 240, 255, 15, 3, 34, 27, 251, 250, 7].

4. Виконуємо перевіряння підробленого підпису з використанням відкритого ключа.

h = [47, 23, 22, 69, 15, 44, 123, 63, 29, 218, 122, 229, 106, 230, 196, 40, 192, 86, 161, 36, 19, 102, 41, 225, 84, 13, 215, 201, 79, 30, 51, 223, 101, 224, 32, 103, 200, 41, 231, 97, 27, 180, 225, 172, 160, 194, 17, 82, 141, 69, 70, 26, 216, 58, 82, 180, 118, 111, 81, 3, 216, 154, 44, 153, 121, 119, 76, 233, 188, 125, 57, 19, 229, 114, 211,

188, 243, 153, 3, 70, 255, 111, 0, 250, 39, 196, 1, 86, 203, 228, 49, 60, 112, 182, 66, 149, 245, 64, 157, 13, 172, 166, 234, 126, 77, 189, 137, 241, 15, 97, 252, 143, 78, 206, 234, 100, 136, 122, 101, 196, 27, 221, 26, 116, 184, 153, 205, 158, 183, 26, 155, 43, 213, 226, 81, 16, 149, 178, 188, 244, 1, 113, 121, 93, 172, 135, 164, 196, 167, 110, 143, 60, 208, 236, 118, 169, 192].

$Normbound^2 = 190000.0$.

Дійсний підпис пройшов перевірку $\|\hat{s}\|^2 = 175798 < 190000.0$.

Підроблене підпис пройшов перевірку $\|\hat{s} + \alpha\|^2 = 175798 < 190000.0$.

Результат – вдалося підробити підпис.

Висновки. Вперше запропоновано модель атаки підробки на підпис в ФКЗП із посиленими параметрами та із застосуванням техніки пертурбації, що дозволило отримати меншу складність підробки в порівнянні з повним перебором. Дана модель атаки відрізняється від відомих раніше врахуванням особливостей реалізації ЕЦП NTRUSign із посиленими параметрами та додатковим захистом за допомогою техніки пертурбації. Це дозволило отримати нові оцінки стійкісті ЕЦП NTRUSign, які показують, що використання техніки пертурбацій не покращує захист від досліджуваного виду підробки. Вперше проаналізовано та показано, що ефективність атаки не суттєво зменшується від збільшення раундів пертурбацій. Отримано експериментальні підтвердження у вигляді кількісних показників ефективності атаки (кількість вдалих спроб підробки підпису) для великих розмірів вхідних параметрів підпису. Важливою та актуальною задачею є подальший аналіз можливості поширення запропонованої моделі атаки для інших підписів на решітках.

ЛІТЕРАТУРА

[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]. 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/ DucasNguyen/Learning.pdf, свободный.

[4]. Carlos Aguilar Melchor. Sealing the Leak on Classical NTRU Signatures [Електронний ресурс] / Carlos Aguilar Melchor , Xavier Boyen, Jean-Christophe Deneuville, Philippe Gaborit. Cryptology ePrint Archive, 2014. Режим доступу: url: http://eprint. iacr.org/2014/48

[5]. Gentry Craig. Cryptanalysis of the Revised NTRU Signature Scheme [Електронний ресурс] / Craig Gentry, Mike Szydlo. Режим доступу: http://www. szydlo.com/ ntru-revised-short02.pdf, свободный.

[6]. Meskanen Tommi. On the NTRU Cryptosystem [Електронний ресурс] / Tommi Meskanen. Режим доступу: http:// www/ tucs./ publications/ attachment.php?fname=DISS63.pdf, свободный.

[7]. Jeffrey Hoffstein, Nick Howgrave-Graham, Jill Pipher, Joseph H. Silverman, and William Whyte. 2003. NTRUSign: digital signatures using the NTRU lattice. In Proceedings of the *2003 RSA* conference on The cryptographers' track (CT-RSA'03), Marc Joye (Ed.). Springer-Verlag, Berlin, Heidelberg, C. 122-140.

[8]. sourceforge. Ntru sourceforgenet, The source code repository. 2012. URL: http: //sourceforge.net/ projects/ntru/?source.

REFERENCES

[1]. Sung Jun Min, Go Yamamoto, and Kwangjo Kim (2005), "Weak property of malleability in NTRUSign". Mode of access: http://www.academy.ualiberty. com/ ru/goodsquality/details/174.

[2]. Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman (2001), "NSS: The NTRU Signature SchemeNTRU Cryptosystems". Mode of access: http://www. citeseerx.ist.psu.edu.

[3]. L. Ducas, P. Q. Nguyen (2013). "Learning a Zonotope and More: Cryptanalysis of NTRUSign countermeasures". Mode of access: http://www.di. ens.fr/ducas/NTRUSignCryptanalysis/DucasNguyen /Learning.pdf.

[4]. Carlos Aguilar Melchor , Xavier Boyen, Jean-Christophe Deneuville, Philippe Gaborit (2014) , "Sealing the Leak on Classical NTRU Signatures". Cryptology ePrint Archive. Mode of access: http:// eprint.iacr.org/2014/48

[5]. Craig Gentry, Mike Szydlo (2001), "Cryptanalysis of the Revised NTRU Signature Scheme". Mode of access: http:// www. szydlo. Com / ntru-revised-short02.pdf.

[6]. Meskanen Tommi (2005). "On the NTRU Cryptosystem". Mode of access: http://www.tucs/ publications/attachment.php?fname=DISS63.pdf.

[7]. Jeffrey Hoffstein, Nick Howgrave-Graham, Jill Pipher, Joseph H. Silverman, and William Whyte. (2003). NTRUSign: digital signatures using the NTRU lattice. In Proceedings of the *2003 RSA* conference on The cryptographers' track (CT-RSA'03), Marc Joye (Ed.). Springer-Verlag, Berlin, Heidelberg, pp. 122-140.

[8]. sourceforge. Ntru sourceforgenet, The source code repository. (2012). Mode of access: http: //sourceforge.net/projects/ntru/?source.

ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ АТАК НА СХЕМЫ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ В ФАКТОР-КОЛЬЦЕ УСЕЧЕННЫХ ПОЛИНОМОВ

Одним из важных средств получения услуг аутентификации является электронная подпись. Исследование постквантовых электронных подписей в настоящее время приобретают актуальность из-за возможности возникновения квантового компьютера. Криптосистемы на решетках имеют ряд преимуществ, среди которых основной является устойчивость от квантового криптоанализа. Поэтому вопросы безопасности подписей на решетках требует детального анализа. Предложена модель атаки подделки подписи NTRUSign с помощью аннулирующих полиномов на схему с пертурбациями с усиленными параметрами. Анализируется эффективность подделки NTRUSign на практике. Обосновываются экспериментальные оценки защищенности усиленных параметров подписи NTRUSign от указанного типа угрозы. Практическая ценность полученных результатов заключается в экспериментальном доказательстве того, что эффективность атаки незначительно уменьшается от увеличения параметров подписи.

Ключевые слова: фактор-кольца усеченных полиномов, электронная цифровая подпись (ЭЦП), алгебраические решетки.

STUDY OF CRYPTOGRAPHIC ATTACKS ON THE DIGITAL SIGNATURE SCHEME IN QUOTIENT RING OF TRUNCATED POLYNOMIALS

One of the main techniques obtaining authentication is using digital signatures. Research of posquantum digital signatures now acquired urgency because of the potential appearance of quantum computer. Lattice based cryptosystems have several advantages, among which are resistance to quantum cryptanalysis. Therefore, the question of security of lattice based signatures requires detailed analysis. A model of forgery attack using annihilating polynomials against NTRUSign with strengthened parameters and perturbations is proposed. Also we analyse the effectiveness of NTRUSign counterfeiting in practice. The experimental estimates of NTRUSign enhanced parameter settings to this type of threat are considered. The practical value of the obtained results is the experimental evidence that the effectiveness of attack is not significantly reduced by increasing the signature parameter.

Keywords: the quotient ring of truncated polynomials, the electronic digital signature, algebraic lattices

Кузнецов Олександр Олександрович, доктор технічних наук, професор кафедри безпеки інформаційних систем і технологій Харківського національного університету ім. В.Н. Каразіна, м. Харків, Україна.
E-mail: kuznetsov@karazin.ua

Кузнецов Александр Александрович, доктор технических наук, профессор кафедры безопасности информационных систем и технологий Харьковского национального университета им. В.Н. Каразина, г. Харьков, Украина.
Kuznetsov Olexandr, Doctor of science (habilitation), Professor of Department of Information Systems and Technologies Security, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.

Горбенко Юрій Іванович, кандидат технічних наук, провідний науковий співробітник кафедри безпеки інформаційних систем і технологій Харківського національного університету ім. В.Н. Каразіна, м. Харків, Україна.
E-mail: s1necerra@gmail.com.
Горбенко Юрий Иванович, кандидат технических наук, ведущий научный сотрудник кафедры безопасности информационных систем и технологий Харьковского национального университета им. В.Н. Каразина, г. Харьков, Украина.
Gorbenko Yurii, Phd, Chief Scientist, Department of Information Systems and Technologies Security, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.

Шевцов Олексій Володимирович, молодший науковий співробітник кафедри безпеки інформаційних систем і технологій Харківського національного університету ім. В.Н. Каразіна, м. Харків, Україна.
E-mail: s1necerra@gmail.com.
Шевцов Алексей Владимирович, младший научный сотрудник кафедры безопасности информационных систем и технологий Харьковского национального университета им. В.Н. Каразина, г. Харьков, Украина.
Shevtsov Oleksiy, junior research fellow**,** Department of Information Systems and Technologies Security, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.

Кузнецова Тетяна Юріївна, науковий співробітник кафедри безпеки інформаційних систем і технологій Харківського національного університету ім. В.Н. Каразіна, м. Харків, Україна.
E-mail: s1necerra@gmail.com.
Кузнецова Татьяна Юрьевна, научный сотрудник кафедры безопасности информационных систем и технологий Харьковского национального университета им. В.Н. Каразина, г. Харьков, Украина.
Kuznetsova Tetjna, research fellow**,** Department of Information Systems and Technologies Security, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.