УДК 003.26.09:004.056.55:512.71(045)

Горбенко Ю.І., Корченко О.Г., Горбенко І.Д., Пушкарьов О.І., Коряков І.В.

СУТНІСТЬ ТА ОЦІНКА СТІЙКОСТІ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ В КІЛЬЦЯХ ЗРІЗАНИХ ПОЛІНОМІВ

Розглядається сутність, дається загальна характеристика асиметричних крипто- перетворень направленого шифрування, що ґрунтуються на перетвореннях в кільцях зрізаних поліномів. Викладаються основні положення та результати оцінки криптографічної стійкості проти відомих атак, даються рекомендації відносно застосування.

Ключові слова**:** кільця зрізаних поліномів, криптографічні перетворення.

Вступ. Особливий інтерес нині мають інфраструктури відкритих ключів (ІВК), що ґрунтуються на криптографічних перетвореннях в кільці зрізаних поліномів [1-3]. Основною перевагою цього алгоритму є те, що він працює набагато швидше звичайних алгоритмів направленого шифрування з відкритим ключем, наприклад, таких як RSA, в групі точок еліптичних кривих тощо. Перевага у швидкості є особливо великою в генерації ключів, яке найчастіше є найбільш важливою частиною у криптографії з відкритим ключем. Для електроного цифрового підпису (ЕЦП) пряме перетворення виконується на особистому ключі, а зворотне на відкритому. Зважаючи на вказані переваги, в США в 2011 році остаточно прийнято стандарт направленого шифрування в кільці зрізаних поліномів X9.98 – 2010 [1]. Вхідними даними в цьому стандарті є загальні параметри, ключі та повідомлення, які мають бути введені при кожному звертанні до процедури зашифрування. Вихідними даними є шифротекст, що є результатом перетворень над вхідними. Операції задають перетворення над вхідними даними для отримання вихідних даних. У стандарті операції визначені як послідовність кроків, які виконуються.

Особливістю стандарту є те, що в ньому реалізовано сім рівнів безпеки. Безпека (стійкість) шифрування у стандарті залежить від розмірів і властивостей загальних параметрів, розмірів і властивостей ключів, механізмів генерування ключів та вибраних базових методів криптоперетворень. Для порівняння використовуються чотири класи рівнів безпеки, які класифікуються та порівнюються з довжинами ключів блокових симетричних шифрів: «112 бітів», «128 бітів», «192 бітів», і «256 бітів». Наведені рівні безпеки вказують мінімальну складність атаки «грубої сили», наприклад, від 2^{112} до 2^{256} певних групових операцій. Відповідно мінімальні розміри ключа і параметра для даного алгоритму пов’язані з кожним із цих рівнів безпеки. Рівень даних «112 бітів» дозволяється (рекомендується) для шифрування даних, захист яких потрібний не пізніше, ніж до 2030 року. Рівень «128-бітів» – для шифрування даних, які мають бути захищені до 2031 року і пізніше. Рівні «192-бітів» та «256-бітів» призначені для забезпечення підвищених рівнів безпеки. Кожен рівень безпеки відповідає конкретному на основі застосування відповідних параметрів, що задані в цьому стандарті і наведені в табл. 1. Усі параметри та криптоперетворення потрібно вибирати таким чином, щоб забезпечувався мінімальний указаний рівень безпеки. Під множиною параметрів розуміються спеціально генеровані кортежі загальних параметрів, що рекомендуються.

На фоні зменшеної складності направленого шифрування проблемним, на наш погляд, є доведення та оцінка криптографічної стійкості перетворень в кільцях зрізаних поліномів.

Метою цієї статі є визначення сутності криптографічних перетворень в кільцях зрізаних поліномів, математичної моделі направленого шифрування з орієнтацією на стандарт X9.98, визначення сутності та класифікація потенційно можливих крипто аналітичних атак, а також оцінка їх вразливості.

Загальні параметри й алгоритми, що можуть застосовуватись Таблиця 1

Рік	Рівень безпеки	Блоковий шифр	Алгоритм гешування	Множина параметрів
2030	112-бітів	Triple-DES (тільки 3 ключі), AES-128, AES-192, AES-256	SHA-224, SHA-256, SHA-384, SHA-512	ees401ep1, ees541ep1, ees659ep1
2031 та пізніше	128-бітів	AES-128, AES-192, AES-256	SHA-256, SHA-384, SHA-512	ees449ep1, ees613ep1, ees761ep1
	192-бітів	AES-192, AES-256	SHA-384, SHA-512	ees677ep1, ees887ep1, ees1087ep1
	256-бітів	AES-256	SHA-512	ees1087ep2, ees1171ep1, ees1499ep1

1. Математична модель направленого шифрування в кільці зрізаних поліномів

Проведемо аналіз криптосистеми X9.98 використовуючи такі джерела [1-8].

Загальні параметри та ключі. Нехай вибрані загальні параметри NTRU направленого шифрування – N, p, і q, де N – розмір кільця R (максимальний степінь поліномів кільця), а p і q – два взаємно прості числа. Число q дещо більше числа p. Вони є модулями, згідно з якими зводяться коефіцієнти багаточленів кілець. Окрім того, параметр *p* визначає інтервал, якому мають належати всі коефіцієнти багаточленів, що використовуються в криптосистемі NTRU. Так, простір повідомлень LM визначається як

$$LM = \{M(x) \in R\}, \quad (1)$$

причому коефіцієнти поліномів-повідомлень належать відрізку

$$[-(p-1)/2, (p-1)/2]. \quad (2)$$

Ключову систему складають:

- асиметрична пара ключів (f, fp, h), де (f, fp) – особистий (конфіденційний) ключ отримувача направлено зашифрованого повідомлення, а h – відкритий ключ зашифрування;
- одноразові ключі – багаточлени g та r, де g – поліном, за допомогою якого обчислюється відкритий ключ h, а r – ключ сеансу зашифрування.

Як додаткові в ключовій системі використовуються параметри df, dg та dr. Ці параметри визначають через коефіцієнти множини багаточленів відповідно:

$$\begin{aligned} Lf &= L(df, df-1); \\ Lg &= L(dg, dg); \\ Lr &= L(dr, dr). \end{aligned} \quad (3)$$

У (3), наприклад, запис у вигляді L (df, df – 1) означає, що множина Lf є сукупністю можливих багаточленів кільця R, кожен із яких в якості коефіцієнтів має df одиниць (1), (df –

1) від'ємних одиниць (–1), а ті коефіцієнти, що залишилися, приймають нульові значення. Аналогічно і для Lg та Lr.

Генерування ключів. При генеруванні ключів вважаються відомими загальні параметри та параметри ключів. За таких умов генерування ключів здійснюється у певній послідовності.

1) Із повної множини Lf вибирається (обчислюється) особистий (конфіденційний) багаточлен ключ f(x).

2) Із повної множини Lg вибирається (обчислюється) особистий (конфіденційний) багаточлен ключ g(x).

3) За відомим f(x) обчислюються мультиплікативно зворотні в кільці R для нього багаточлени fq(x) та fp(x), які задовольняють умовам:

$$f(x) * fq(x)=1(\text{mod } q);$$

$$f(x) * fp(x)=1(\text{mod } p). \quad (4)$$

4) Обчислюється відкритий ключ

$$h(x) = fq(x)* g(x) \ (\text{mod } q). \quad (5)$$

5) Як особистий (конфіденційний) ключ вибирається пара (f(x), fp(x)).

6) Відкритий ключ h(x) необхідно зробити доступним усім користувачам (абонентам) із забезпеченням його цілісності, справжності, доступності й неспростовності.

Направлене зашифрування повідомлень. Зашифрування повідомлення M здійснюється в такій послідовності:

1) Абонент-відправник, який має зашифрувати повідомлення, перетворює повідомлення M на багаточлени M(x), коефіцієнти яких належать відрізку (2).

2) Абонент-відправник генерує (обчислює) разовий (сеансовий) ключ – параметр r(x).

3) Абонент-відправник зашифровує послідовність повідомлень поліномів, використовуючи відкритий ключ отримувача h(x):

$$C(x) = (p* r(x)*h(x) + M(x)) \ (\text{mod } q), \quad (6)$$

і, таким чином, отримує багаточлен – криптограму (шифр текст) C(x).

Направлене розшифрування криптограми (шифротексту) отримувачем. Сутність направленого розшифрування полягає в тому, що абонент, який намагається розшифрувати багаточлени – криптограми, має знати цілісні й справжні загальні параметри та особисту пару ключів (f(x), fp(x)). За таких умов розшифрування може здійснюватись у такій послідовності.

1) Обчислюється згортка особистого ключа та криптограми у вигляді

$$f(x)* C(x) \ (\text{mod } q), \quad (7)$$

У результаті отримуємо:

$f(x)* C(x) \ (\text{mod } q) = (f(x)* p* r(x)*h(x) + f(x)* M(x)) \ \text{mod } q) = (f(x)* p* r(x)* fq(x)* g(x) + f(x)* M(x)) \ \text{mod } q) = a(x).$

З урахуванням (4), тобто що $f(x) * fq(x)=1(\text{mod } q)$, маємо:

$$a(x) = (p* r(x)* g(x) + f(x)* M(x)) \ \text{mod } q). \quad (8)$$

1) Обчислюється значення (8) за модулем меншого параметра p, у результаті маємо:

$$a(x)(\mathrm{mod}\ p) = (p^* r(x)^* g(x) + f(x)^* M(x)))(\mathrm{mod}\ p). \quad (9)$$

У (9) $p^* r(x)^* g(x)(\mathrm{mod}\ p) = 0$, тому

$$b(x) = fp(x)^* a(x)(\mathrm{mod}\ p) = fp(x)^* f(x)^* M(x)(\mathrm{mod}\ p) = M(x), \quad (10)$$

оскільки $f(x) * fp(x) = 1(\mathrm{mod}\ p)$.

Таким чином, доведено, що направлене шифрування в кільці зрізаних багаточленів R є оборотним.

Необхідно відмітити, що правильність розшифрування забезпечується за умови, що коефіцієнти багаточлена a(x) приймають значення в інтервалі

$$(-q/2, q/2). \quad (11)$$

2. Атаки на криптографічні перетворення типу НШ

При розгляді атак, як правило, використовується математичний апарат алгебраїчних решіток. Алгебраїчною решіткою називається множина цілочисленних лінійних комбінацій такого вигляду [1, 9, 10]:

$$L(b1, b2,\ldots, bn) = [\textstyle\sum_{i=1}^{n} xi\ \ bi : x1, x2, \ldots, xn \in Z] \quad . \quad (12)$$

На цей час відомі атаки можна поділити на два основних типи – грубої сили та аналітичні, останні у свою чергу ґрунтуються на методах зведення в решітках. Аналіз показує, що обидва методи можуть бути використані при криптоаналізі. Тільки при знанні цієї пари можна здійснити направлене розшифрування згідно з (7) – (10). В цьому випадку основною задачею криптоаналізу є знаходження особистого ключа.

Пряма матрична атака. Пряма матрична атака на NTRU ґрунтується на решітках та пошуку найкоротшого вектора в конкретній решітці. Для розкриття особистого (конфіденційного ключа) ключа (f(x), fp(x)) криптоаналітик може побудувати матрицю такого вигляду [11, 12].

$$\left(\begin{array}{cccc|cccc} \alpha & 0 & \cdots & 0 & h_0 & h_1 & \cdots & h_{n-1} \\ 0 & \alpha & \cdots & 0 & h_{N-1} & h_0 & \cdots & h_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \alpha & h_1 & h_2 & \cdots & h_0 \\ \hline 0 & 0 & \cdots & 0 & q & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & q & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & q \end{array}\right), \quad (13)$$

де h0, h1, … hN-1 – коефіцієнти відкритого ключа, q – більший із модулів; α – коефіцієнт. Далі із рядків матриці (13) може бути побудована решітка L, причому оскільки матриця містить відкритий ключ h(x) вигляду (5), то дана решітка буде містити й вектор

$$t = (\alpha * f(x), g(x)). \quad (14)$$

Причому вважається, що цей вектор буде найкоротшим у заданій решітці. Тому знаходження такого вектора є умовою знаходження особистого ключа f(x). Але задача визначення найкоротшого вектора в решітці вважається експоненційно складною.

Тимчасову оцінку складності злому NTRU за методом лобової атаки на решітку можна обчислити за формулою [11, 12]:

$$T = 2^{(0,4N - 3,5)}. \quad (15)$$

Використовуючи дані з табл. 2 можна зробити відповідні оцінки.

Загальні параметри NTRU, що рекомендуються до застосування Таблиця 2.

Параметри	N	P	q	df
NTRU 167:3	167	3	128	61
NTRU 251:3	251	3	128	50
NTRU 503:3	503	2	256	216

Так, для N = 503 це складає приблизно 10^{60}, а при N = 251 – приблизно 10^{30}.

Атака «грубої сили» [1, 2]. Як випливає з (4) при зломі із застосуванням атаки «груба сила» порушник (криптоаналітик) може робити спробу підібрати особистий ключ f(x), знаючи, що багаточлен f(x) довжиною N має df коефіцієнтів (1) та (df–1) коефіцієнтів (–1), а ті, що залишились – нулі(0). Безпосереднє підбирання багаточлена f(x) із множини Lf = L (df, df–1) вимагає здійснення деякого числа перевірок. Визначимо цю величину.

Коефіцієнти (1), а їх df, можуть бути розміщені на N позиціях C_N^{df} варіантами. Далі, (df–1) коефіцієнтів (–1) можуть бути розміщені на N–df позиціях, що залишилися не заповненими, C_{N-df}^{df-1} варіантами. Нарешті на позиціях, що залишилися незаповненими числами (1) та (-1), однозначно розміщаються 0. Оскільки розглянуті події є незалежними, то загальне число варіантів перебирання T складає:

$$T = C_N^{df} \; C_{N-df}^{df-1}. \quad (16)$$

Використовуючи дані з табл. 2, ми отримуємо такі оцінки:
при N = 167 і df = 61 – значення $T = 6.5\ 10^{76}$,
при N = 251 і df = 50 – значення $T = 3.3\ 10^{100}$,
при N = 503 і df = 216 – значення $T = 1.4\ 10^{216}$.

На основі порівнянь оцінок для атаки «груба сила» з оцінками для прямої атаки можна зробити висновки про те, що атака груба сила є набагато складнішою і є практично не здійсненною відносно направленого шифру на NTRU.

Атака «зустріч посередині». У [1, 13, 14] відносно NTRU для визначення особистого ключа f(x) розглянута атака типу «зустріч посередині» потребує

$$C_{N/2}^{d/2} / \sqrt{r}, \quad (17)$$

групових операцій (тимчасова складність) та комірок пам’яті на жорсткому диску. Атака «зустріч посередині» дозволяє розмінювати потрібні для обчислень час і пам’ять, що необхідна для зберігання тимчасових даних.

Один із варіантів атаки полягає в такому [1, 13, 14].

Використовуючи (5), визначається багаточлен

$$g(x) = h(x) * f(x) \bmod q. \quad (18)$$

2) Поліном f(x) подається у вигляді двох багаточленів довжиною N/2:

$$f(x) = f1(x) \,||\, f2(x). \quad (19)$$

3) Вираз (18) подається у вигляді

$$g(x) = h(x) * (f1(x) \,||\, f2(x)) = f1(x) * h(x) + f2(x) * h(x) \bmod q. \quad (20)$$

4) Із (3) випливає, що багаточлен g(x) для випадку p = 3 складається з коефіцієнтів {1,0, -1} та {1,0}для p = 2. Тоді для випадку p = 2 маємо, що

$$f1(x) * h(x) = \{1,0\} - f2(x) * h(x). \quad (21)$$

Далі, для p=2 атака може бути здійснена таким чином.

Вибирається число k. Формується 2^k корзин, у яких будуть зберігатися відповідні кандидати f1(x) і f2(x). При цьому необхідно враховувати, що збільшення числа k призводить до зменшення часової складності, але при цьому збільшується обсяг необхідної для злому пам'яті.

Порушник перебирає всі можливі багаточлени f1(x) із довжинами N/2 з df/2 символів (1). Для цього необхідно виконати

$$I = C_{N/2}^{d/2} \quad (22)$$

ітерацій.

Далі порушник поміщає кожен отриманий багаточлен у відповідний кошик таким чином: f1 записуються в кошик з номером, що складається з найбільш значущих бітів перших k коефіцієнтів полінома f1(x) * h(x) mod q.

Наприклад, якщо N = 4 і q = 8, то багаточлен з коефіцієнтами {7,2,3,5} буде поміщатися в кошик з номером {1,0,0,1}, а багаточлен з коефіцієнтами {6,4,3,1} – у кошик {1,1,0,0}. Після цього порушник починає перебирати можливі варіанти багаточлена f2(x), кожен з яких містить df/2 символів (1). Для перебирання цих варіантів необхідно виконати (22) ітерацій.

Під час перебирання багаточленів f2(x) порушник записує кожен отриманий таким чином. По-перше, він записує f2 у той кошик, який відповідає старшим бітам багаточлена (-f2(x)×h(x) mod q), а по-друге, до кожного коефіцієнта з (-f2 * h) додається одиниця. У результаті отримується новий варіант кошиків, у них і записується багаточлен f2(x).

Наприклад, багаточлен (-f2(x) * h(x) mod q = {6,2,1,5} записується тільки в кошик {1,0,0,1}, а багаточлен (-f2(x)* h (x)mod q = {7,2,3,5} – у кошики {1,0,0,1}, {1,0,1,1}, {0,0,0,1}, {0,0,1,1}.

Якщо в кошику, у який порушник записує багаточлен f2(x), уже зберігається f1(x), то це означає, що для цих багаточленів виконується умова:

$$f1(x) * h(x) = \{1,0\} - f2(x) * h(x) \bmod q. \quad (23)$$

За цих умов багаточлени вважаються хорошими кандидатами для відновлення f(x).

Далі порушник обчислює (f1(x) || f2(x)) * h(x) mod q, Якщо отримується багато член з коефіцієнтами {0,1}, що відповідає багаточленові g(x), то можна вважати, що особистий (конфіденційний) ключ f (x) знайдено.

Таким чином, якщо простір ключів криптосистеми NTRU має розмір

$$I = C_N^d , \quad (24)$$

то для знаходження ключа за методом «зустріч посередині» необхідно перебрати всього (22), тобто $I = C_{N/2}^{d/2}$ варіантів.

Наприклад, для NTRU з параметрами N = 167, d = 61, простір ключів має розмір ≈ 2.6 10^{46}, а для виконання атаки зустріч посередині необхідно перебрати ≈ 9.4 10^{22} варіантів (виконати таке число групових операцій), але маючи при цьому таке ж число комірок пам'яті. Далі, для NTRU з параметрами N = 503, d = 216, простір ключів має розмір ≈ 6.2 10^{147}, а для виконання атаки зустріч посередині необхідно перебрати ≈ 2.8 10^{73} варіантів, але знову таки маючи при цьому таке ж число комірок пам'яті.

Наведене дозволяє зробити висновок, що для того, щоб гарантувати криптографічну стійкість з рівнем 2^x, необхідно використовувати NTRU з розміром простору ключів 2^{2x}.

Атака з підібраним шифрованим текстом [11, 12]. Сутність атаки з підібраним шифрованим текстом полягає в такому. При розшифруванні необхідно відповідним чином виконати дії, що визначаються (7)–(11). Тобто спочатку обчислити a(x) = (p* r(x)* g(x) + f(x)* M(x)) mod q), але, як видно, за модулем q. Потім знаходимо b(x) = fp(x)* a(x)(mod p) = fp(x)* f(x)* M(x)(mod p) = M(x).

Атака з підібраним шифрованим текстом при застосуванні криптоперетворення NTRU може зводитися до створення такого багаточлена a(x), відносно якого виконується умова що a(x)mod q $\overline{\cdot}$ a(x). У цьому випадку підробка зводиться до такого.

1) Порушник (криптоаналітик), знаючи загальні параметри N, p, q, а також відкритий ключ h(x), наприклад, отримувача A, та деяке значення z, може створити шифрований текст вигляду:

$$C(x) = z * h(x) + z, \quad (25)$$

де z – ціле число. Потім порушник відсилає криптограму C(x) абоненту A, який є отримувачем.

2) При розшифруванні абонент A, використовуючи свою особисту ключову пару (f(x), fp(x)), робить спробу розшифрувати хибну криптограму, тобто виконує такі обчислення:

$$f(x)* C(x) (\text{mod } q) = f(x)* (z * h(x) + z) = z* f(x)*h(x) + z *f(x) \text{ mod } q). \quad (26)$$

Далі, враховуючи (5), знаходимо

$$h(x)/fq(x) = h(x)*f(x)=g(x). \quad (27)$$

Підставивши (27) у (26), отримуємо, що

$$z * g(x) + z *f(x) \text{ mod } q) = a(x). \quad (28)$$

Оскільки в (28) багаточлени g(x) і f(x) мають коефіцієнти {-1,0,1}, то коефіцієнти багаточлена a(x) будуть приймати значення {0, y,-y, 2y,-2y}. Це означає, що якщо порушник вибрав z – таким, що z <q/2 і 2z> q/2, то при зведенні a(x) за модулем q будуть змінюватися тільки ті коефіцієнти багаточлена a(x), у яких рівні коефіцієнти дорівнюють ± 2y.

Далі нехай і-й коефіцієнт $a_i = 2y$, тоді

$$a(x)(\text{mod } q) = z* g(x) + z*f(x) – q\, x_i. \quad (29)$$

За аналогією з (20), поліном розшифровується абонентом А з використанням частини особистого ключа fp(x), унаслідок чого маємо: fp(x)* a(x)(mod p) = z*fp(x)* g(x) + z* f(x)* fp(x) – q* x_i *fp(x) (mod p), тобто якщо порушник вибирає значення z, що ділиться націло на p, то в результаті отримаємо багаточлен вигляду:

$$-q^* fp(x)^* x_i \bmod p = y(x). \quad (30)$$

5. Нарешті для обчислення особистого ключа абонента А необхідно із (30) обчислити

$$fp(x) = y(x)/(-q^* xi \bmod p). \quad (31)$$

З урахуванням (4), із (31) отримуємо, що f(x) = – q* y(x)-1 * xi mod p.

Вважається, що, застосовуючи таку атаку, криптоаналітик може визначити особистий ключ з імовірністю P = 0.13 або, інакше кажучи, для відновлення секретного ключа атакуючому потрібно відправити лише близько 10 підібраних шифрованих текстів.Захист від атаки з підібраним шифрованим текстом [11, 12]. Для того щоб захистити NTRU від подібної атаки, рекомендується використовувати NTRU спільно зі схемою FORST.

При шифруванні за методом NTRU-FORST абонент В, як і в звичайній схемі NTRU, обчислює багаточлен відкритого тексту m(x) і доповнює багаточлен випадковим набором з k бітів R та обчислює r (x) = H (m (x) | | R), де H(x) – криптографічно сильна функція гешування. Далі абонент В, як і в звичайній схемі NTRU, формує багаточлен, що є блоком шифр тексту вигляду: c (x) = r (x) * h (x) + m (x) mod q.

Отримавши шифртекст, абонент А відновлює повідомлення m(x) і обчислює H(m (x) | | R). Далі абонент А обчислює H(m(x) | | R) * h (x) + m(x)modq і порівнює отримане значення з c(x). Якщо

$$H (m (x) | | R) * h (x) + m (x) \bmod q = c (x), \quad (32)$$

то А приймає повідомлення, інакше – відкидає його.

Атака з адаптивно підібраним шифр текстом [11, 12]. Особливість такої атаки полягає в тому, що для зашифрування двох повідомлень m1 і m2 використовується один і той самий особистий ключ f(x) та поліном r(x) [1]. За даних умов різниця між двома шифр текстами c1 та c2 визначається як c1 – c2 ≡ (m1 – m2) (mod q). З наведеного порівняння можна отримати велику частину повідомлень m1 та m2.

Згідно схеми шифрування, m = M ⊕ MGF(r*h) = (M + MGF(r*h)) mod 2, тому

$$(c1 – c2)(\bmod q)(\bmod 2) = M1 \oplus M2. \quad (33)$$

Для запобігання такого роду атакам потрібно уникати появи двох однакових поліномів для «забілення» r. Параметр r може повторитися лише в таких випадках: коли однакове повідомлення m може бути зашифроване з однаковим b – випадковим доповненням, а також коли для двох різних пар (m, b) існує одинакове значення r.

У той же час імовірність події, коли дві різних пари (m, b) призведуть до однакового r(x), співпадає з імовірністю відбуття колізії з простору всіх імовірних поліномів Lr. Для того щоб існувала така ймовірність виникнення колізії, криптоаналітик має отримати √(dr) повідомлень. У разі якщо криптоаналітику вдається зашифрувати одне й те саме повідомлення m(X), але при використанні різних поліномів r1(x) та r2(x), отримати інформацію про значення r1(X) та r2(X) можна, використовуючи співвідношення: (ph(X))–*1*(e1(X) – e2(X)) ≡ r1(X) – r2(X) (mod q).

Атаки, що пов'язані з некоректним вибором загальносистемних параметрів. При некоректному виборі загальних параметрів також можливими є успішні крипто атаки.

При некоректності параметра q. Якщо у перетворенні r(xh(mod q) q буде використане маленьким або не буде існувати f–1 (Z/qZ) [X]/(XN – 1), криптоаналітик може використати знання h для розв'язання e = rh + m' з використанням лінійної алгебри та отримати значення повідомлення m. Випадок, коли некоректним є параметр N. N – має бути просте число. Якщо обрати непросте N, то з використанням методу Gentry [15] можна отримати значення повідомлення й особистого ключа. У цьому випадку задачі в решітках можна звести до задач у решітках набагато менших ніж N.

Випадок, коли некоректним є параметри q та N. Для кожного простого дільники q0 числа q, поліном XN – 1 mod q0 не повинен мати дільників маленького степеню (окрім X – 1). Якщо N просте, то XN – 1 mod q0 розкладається як (X – 1)A1(x)…Ae(x), де Ai(x) та має ступінь рівну до степеня мультиплікативного порядку q0 mod N. Якщо h(x) чи r(x) нульові в полі mod Ai(x), це призводить до витоку значення m (x) в цьому полі. В разі якщо Ai(x) має ступінь t, ймовірність того що h(x) чи r(x) ділиться на Ai(x) можливо 1=qt. Для запобігання атак заснованих на факторизації h(x) та r(x), рекомендується для кожного простого дільника P числа q, порядок P (mod N) має бути N-1 чи (N-1)/2. Це також дозволяє збільшити ймовірність того що випадково обране значення f(x) буде мати зворотнє в кільці Rq.

Випадок, коли некоректним є параметри p, q та N. В разі якщо модуль p є дільником більшого модулі q, то з виразу

$$(p*r*h + m) \bmod q, \qquad (34)$$

можна відновити повідомлення m. В загальному випадку p та q повинні бути взаємно простими в кільці Z [X]/(X^N – 1). Вказане еквівалентно твердженню, що q, p, та X^N – 1 повинні генерувати ідеал кільця Z [X]. Більший модуль q має бути в кільці Z, при цьому менший модуль p може й не бути в кільці Z.

3. Оцінка стійкості криптоперетворень в кільцях зрізаних поліномів

В табл. 3 наведені узагальнені дані відносно складності криптоаналізу в кільцях зрізаних поліномів

Складність криптоаналізу в кільцях зрізаних поліномів Таблиця 3

Назва методу	Складність методу
Задачі SVP та CVP аналізу	$2O(n(\log\log n)^2/\log n)$
Алгоритм BKZ-LLL знаходження ненульового вектора **v**	$O(n^2(\beta^{\beta/2+o(\beta)}+n^2))$.
Знаходження найкоротшого вектора за допомогою алгоритму BKZ-LLL	$O(n^2\beta^{\beta/2})$ або $O(n^3(k/6)^{k/4})$
Задачі SVP та CVP(час роботи)	$2O(n \log n)$
Лобова атака на решітку	$T = 2^{(0.4N-3,5)}$.
Атака «грубої сили»	$T = C_N^{df}\ C_{N-df}^{df-1}$
Атака зустріч посередині	$I = C_{N/2}^{d/2}$
Комбінаторна атака на ЕЦП	$\omega(N,d) = \log_2\left(\frac{\binom{N}{d+1}}{\sqrt{N}}\right)$.
Атака на основі вгадування позицій нулів	$\varpi_{lk}(N, d, A, B, A_{ZF}, B_{ZF}) = \log_2(T_{normal}) - \max_{0\le r\le 2N-2d-1}\{\log_2(\sigma)\}$
Атака, що заснована на підробці підпису (ймовірність успішного здійснення атаки)	$P(\text{combinatorial forgery}) \approx \sqrt{\frac{\pi^{\frac{N-1}{2}}}{q^{N-1}(\frac{N-1}{2})!}\left(\frac{\mathcal{N}}{\beta}\right)^{N-1}}\ ! < 2^{-k}$.

Висновки та рекомендації. Загальними параметрами направленого (NTRU) шифрування є N, p, і q, де N – розмір кільця R, а p і q два взаємно прості числа. Параметри p і q є модулями, згідно яких приводяться коефіцієнти багаточленів кілець. Також, параметр p визначає інтервал, якому повинні належати усі коефіцієнти багаточленів, що

використовуються в криптосистемі NTRU. Для криптоперетворень в кільці зрізаних поліномів ключову систему складають асиметрична пара ключів (f, fp, h), де (f, fp) – особистий (конфіденційний) ключ отримувача направленого зашифрованого повідомлення, а h – відкритий ключ зашифрування, а також одноразові ключі – багаточлени g та r, де g – поліном, за допомогою якого обчислюється відкритий ключ h, а r – ключ сеансу зашифрування. Відомі атаки можна поділити на два основних типи – грубої сили та аналітичні. Останні ґрунтуються на методах зведення в решітках. Аналіз показує, що обидва методи можуть бути використаними при криптоаналізі. При цьому основною задачею криптоаналізу є знаходження особистого ключа, тобто, знаходження пари розшифрування (f(x), fp (x)). Тільки при відомій цій парі можна здійснити направлене розшифрування згідно.

Атаки, що орієнтовані NTRU, можна розділити на такі: атаки на крипто перетворення типу НШ; атаки, що орієнтовані на криптографічне перетворення типу ЦП; атаки на криптографічні протоколи, включаючи протоколи управління ключами; атаки за допомогою квантових комп'ютерів. Атаки на ЦП (NTRUSign) можна поділити на два основних типи – комбінаторні атаки і атаки, що ґрунтуються на методах зведення в решітках. Обидва типи атак можуть бути використаними для отримання особистого ключа відповідного криптографічного перетворення.

Відомо, що алгоритм NTRU запатентований, що знижує до нього інтерес дослідників. Але відсутність публікацій про серйозні вразливості за практично 15-річний період існування, дозволяє з оптимізмом дивитися на його подальше можливе використання та розвиток. Більш того, навіть в самому песимістичному, коли появиться квантовий комп'ютер, сумнівів відносно NTRU ще немає. Тому NTRU є цілком надійним варіантом криптосистеми навіть у «пост квантовий» період.

ЛІТЕРАТУРА

1. ANSI X9. 98 – 2010. Lattice-Based Polynomial Public Key Establishment Algorithm for the Financial Services Industry.

2. NTRU Cryptosystems. Technical reports. Available at http:www. ntru. com, 2003

3. Hoffstein, J. NTRU: A ringbased public key cryptosystem./J. Hoffstein, J. Pipher, J. H. Silverman//In Buhler, pp. 267–288.

4. The NTRU public key cryptosystem//A tutorial. The NTRU Cryptosystems. Inc. URI/: http//securityinnovation. com/cryptolab/tutorials. shtml/

5. J. Hoffstein, J. Pipher, J. H. Silverman, NTRU: A new high speed public key cryptosystem, Algorithmic Number Theory (ANTS III), Portland, OR, June 1998, Lecture Notes in Computer Science 1423, J. P. Buhler (ed.), Springer-Verlag, Berlin, 1998, pp. 267–288

6. J. Hoffstein, N. Howgrave-Graham, J. Pipher, J. H. Silverman, W. Whyte, NTRUSign: Digital Signatures in the NTRU Lattice, CT-RSA 2003.

7. J. Hoffstein, N. Howgrave-Graham, J. Pipher, J. H. Silverman, W. Whyte, Hybrid lattice reduction and meet-in-the-middle resistant parameter selection for NTRU. Preprint, available from [Електронний ресурс]. Режим доступу: http://grouper. ieee. org/groups/1363/lattPK/subm issions. html#2007-02.

8. J. Hoffstein, J. Silverman, W. Whyte, NTRU Technical Report #12, v2, Estimating Breaking Times for NTRU Lattices. Available from http://www. ntru. com/cryptolab/tech_notes. htm#012.

9. *Андерсон, Джеймс А.* Дискретная математика и комбинаторика: Пер. с англ. – М.: Изд-во «Вильямс», 2003. – 960 с.

10. *Фомичев В.М* Методы дискретной математики в криптологии. – М.: Диалог-МИФИ, 2010. – 434с.

11.NTRUEncrypt криптосистема будущего? http://habrahabr.ru/blogs/crypto/127878/

12. Mariano Monteverde NTRU software implementation for constrained devices. 3. Phong Q. Nguyen and David Pointcheval Analysis and Improvements,.. kronus.me/.../ntruencrypt-криптосистема-будущего/

13. N. Howgrave-Graham, A Hybrid lattice reduction and meet-in-the-middle-attack against NTRU. Crypto 2007.

14. N. Howgrave-Graham, J. H. Silverman, W. Whyte, A meet-in-the-middle attack on an NTRU.

15. Phong Q. Nguyen, David Pointcheval: Public Key Cryptography – PKC 2010, 13th, Pointcheval: Analysis and Improvements of NTRU Encryption Paddings, www.informatik.uni-trier.de

Надійшла: 21.12.2011

Рецензент: д.т.н., проф. Конахович Г.Ф.