УДК 004.056.55

ЗАГАЛЬНА АТАКА НА NTRUENCRYPT НА ОСНОВІ ПОМИЛОК РОЗШИФРУВАННЯ

К.А. ПОГРЕБНЯК, Д.С. ДЕНИСОВ

NTRUEncrypt – це криптографічна система з відкритим ключем, яка була створена як альтернатива RSA та криптосистем на еліптичних кривих (ECC). Виключними особливостями NTRU є оригінальний і специфічний математичний апарат та висока швидкість перетворень. Застосування NTRU можливо за умови, що на неї не існує криптоаналітичних атак, які здатні суттєво понизити її криптографічну стійкість. Метою цієї статті є аналіз захищеності криптосистеми від загальної атаки на основі помилок розшифрування.

Ключові слова: NTRU, помилки при розшифруванні, загальна атака на основі помилок розшифрування.

1. СУТНІСТЬ ОСНОВНИХ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

Усі операції відбуваються у кільці $R = Z[X]/(X^N - 1)$, яке має назву кільця зрізаних поліномів. N вважається розміром кільця R. Детально опис криптоперетворень наведено у [1,3].

Позначимо *шириною (Width) полінома* різницю між його найбільшим та найменшим коефіцієнтами.

Для генерації ключової пари використовуються поліноми f та g. Особливістю цих поліномів є те, що вони мають маленьку *ширину*. Зазвичай це бінарні або тернарні поліноми. Бінарні повинні мати d_f та d_g одиниць відповідно, а тернарні d_f та d_g коефіцієнтів 1 і $d_f - 1$ та d_g коефіцієнтів -1 відповідно. Поліном f є особистим ключем і повинен мати мультиплікативні інверсії за двома модулями.

Особистий ключ h обчислюється так:

$$h = p(f_q^{-1} * g) \bmod q . \quad (1)$$

Для шифрування використовуються поліноми r та M. Ці поліноми мають невелику ширину. Спочатку повідомлення M конвертується у відображення повідомлення поліном m. Потім обчислюється криптограма як:

$$e = h * r + m \bmod q . \quad (2)$$

Розшифрування здійснюється способом згортки поліномів у кільці як:

$$a = f * e \bmod q . \quad (3)$$

Після цього відбувається центрування коефіцієнтів поліному a. Для стандарту [1] коефіцієнти зводяться в інтервал [-1024,1024).

Вихідне відображення повідомлення (m) обчислюється як:

$$m = f_p^{-1} * a \bmod p . \quad (4)$$

2. СУТНІСТЬ ПОМИЛОК В ХОДІ РОЗШИФРУВАННЯ

Перепишемо формулу (3) у вигляді:

$$a = f * e = f * (r * h + m) = \\ = p * r * g + f * m \bmod q. \quad (5)$$

Поліноми p, r, g, m, f обираються такими, що мають невелику ширину. В цьому випадку із дуже високою ймовірністю поліном $p * r * g + f * m$ матиме ширину меншу за q, що робить можливою редукцію в діапазоні $[A, A + q - 1]$, тобто порівняння за модулем q. Нагадаємо, що для [1] $A = -1024$. Якщо неправильно обрано загальносистемний параметр A, що відповідає за центрування коефіцієнтів (тоді деякі з коефіцієнтів $p * r * g + f * m$ лежатимуть за межами центрувального діапазону) або коли поліном $p * r * g + f * m$ матиме ширину більшу за q. У цьому випадку відновлене m' відрізнятиметься від вихідного повідомлення m на деякий множник числа q за модулем p. Це викличе помилки при розшифруванні, які можуть розкрити деяку інформацію про особистий ключ.

Існує два типи помилок розшифрування: wrapfailure («помилка обгортання») та gapfailure («помилка великого розриву»). Gapfailure виникає, коли $Width(p * r * g + f * m) \geq q$. Якщо ж $Width(p * r * g + f * m) < q$, але в процесі розшифрування через неправильний вибір A ми отримали помилку (неправильно обрано діапазон дозволених значень коефіцієнтів), то має місце помилка типу «wrap failure».

3. МОДЕЛЬ АТАКИ НА ОСНОВІ ПОМИЛОК РОЗШИФРУВАННЯ

3.1. Модель порушника

В даній атаці порушнику необхідно зібрати велику кількість триплетів (m, r, e), де e – дійсна криптограма, отримана з відображення повідомлення m з використанням ключа сеансу r.

Тобто, порушник може проводити пасивну атаку просто прослуховуючи канал зв'язку і збираючи триплети або самостійно відправляти повідомлення і аналізувати криптограми.

3.2. Реверсивне представлення полінома

Позначимо зворотний до c поліном як $\bar{c}(X)$. Якщо $c = [c_0, c_1, c_2, ..., c_{N-1}]$, то зворотний поліном має вигляд $\bar{c} = [c_0, c_{N-1}, c_{N-2}, ..., c_1]$. Відображення $c \to \bar{c}$ є автоморфізмом кільця R, таким чином, застосування відображення двічі дає вихідний поліном c.

Позначимо добуток поліномів $c \cdot \bar{c}$ як $\hat{c}$. Цей добуток має властивість $\hat{c}_i = c \cdot (X^i * c)$, тобто кожний наступний терм полінома $\hat{c}$ отримується шляхом звичайного множення полінома c на свій зсув (ротацію). Відомо, що $\hat{c}_0 = \sum_i c_i^2 = \|c\|^2$, тоді як всі інші терми матимуть довжину приблизно $\|c\|$.

Таким чином, $f * \bar{f}$ має один терм довжини d_f, а всі інші – довжини $\sqrt{d_f}$. Якщо $p*r*g + f*m$ має достатньо велику ширину, це означає, що r значно корелює із $\bar{g}$, а m – із $\bar{f}$.

3.3. Сутність атаки

Загальна атака працює незалежно від використаної схеми доповнення відкритого тексту і використовує лише дійсні криптограми за рахунок повноцінних операцій.

Оскільки, поточна версія алгоритму NTRU вважається стійкою до помилок розшифрування і їх ймовірність складає 2^{-100}, реалізувати повноцінну атаку детектуючи помилки типу «gapfailure» за допомогою оракула O_q фактично неможливо. Тому використовується оракул O_B, який визначає, чи є ширина полінома $p*r*g + f*m$ більша за B, де B можна обирати достатньо близьким до q (в залежності від кількості триплетів, якими володіє порушник).

Алгоритм атаки:

1. Встановити $u, v = 0$.
2. Згенерувати велику кількість дійсних криптограм $e = h*r + m \bmod q$. Для кожного шифротексту:

(a) Викликати $O_B(e)$.

(b) Якщо $O_B(e)$ показує, що ширина більша за B, встановити $u = u + \hat{m}$, $v = v + \hat{r}$.

3. Розділити u та v на кількість використаних криптограм.

При достатньо великій кількості помилок розшифрування u та v мають наблизитися до $\hat{f}$ та $\hat{g}$ відповідно.

4. ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ НА ОСНОВІ ПРОГРАМНОЇ РЕАЛІЗАЦІЇ

Для практичних досліджень для тернарних *поліномів* використовувався набір параметрів ees401ep1: $N = 401$, $q = 2048$, $p = 3$, $d_f = 113$;

Позначимо $Width(u_i, \hat{f}_i)$ як найбільшу різницю між коефіцієнтами поліномів u та $\hat{f}$ на однакових позиціях та $Avr(u_i, \hat{f}_i)$ як середнє арифметичне усіх коефіцієнтів на однакових позиціях.

Звернемо вашу увагу, що у роботі [2] пропонується зворотний до $c = [c_0, c_1, c_2, ..., c_{N-1}]$ поліном подавати у вигляді $\bar{c} = [c_0, c_{N-1}, c_{N-2}, ..., c_1]$. У ході реалізації було встановлено, що краща кореляція буде при поданні зворотного полінома як $\bar{c} = [c_{N-1}, c_{N-2}, ..., c_1, c_0]$, але для цього випадку потрібен буде інший алгоритм встановлення особистого ключа f з $\hat{f} = f * \bar{f}$, ніж зазначений у [4].

Таблиця 1

Дослідження бінарних та тернарних поліномів

Ітерація	Бінарний поліном		Тернарний поліном	
	$Width(u_i, \hat{f}_i)$	$Avr(u_i, \hat{f}_i)$	$Width(u_i, \hat{f}_i)$	$Avr(u_i, \hat{f}_i)$
1	29	9.83	19	7.28
2	24	9.69	18	7.1
5	24	9.66	18	6,82
10	23	9.45	17	6,09
100	22	9.45	16	5,68
1000	22	9.44	15	5,67

Обробка однієї криптограми, тобто один цикл алгоритму, залежить від швидкості шифрування криптосистеми (якщо порушник знаходиться у режимі очікування). Проте, якщо порушник назбирав велику кількість триплетів, то йому не складе зусиль обробити їх за досить невеликий час (один цикл алгоритму виконується приблизно за 1 мс).

Далі порушник може викрити особистий ключ f, використовуючи поліноміальний алгоритм, запропонований у [4]. Оскільки, отримане значення f є лише наближенням до дійсного, порушник може перебирати значення коефіцієнтів f зі значно меншого інтервалу та (або) виконати такі кроки:

1. Отримати значення v, яке є наближеним до $\hat{g}$. Згідно з алгоритмом атаки цей крок виконується паралельно з обчисленням u. Так, наприклад, на 1000-й ітерації для бінарних поліномів $Width(u_i, \hat{f}_i) = 27$, $Avr(u_i, \hat{f}_i) \approx 12$. А для тернарних: $Width(u_i, \hat{f}_i) = 18$, $Avr(u_i, \hat{f}_i) \approx 4$.

2. З формули (1) обчислення відкритого ключа маємо:

$$f * h = pg \bmod q. \qquad (6)$$

Маючи відкритий ключ h та малий модуль p, порушник може змінювати коефіцієнти полінома f до отримання бінарного або тернарного полінома g використовуючи отримані наближення. Під час знаходження такого поліному його потрібно розглядати як претендента.

ВИСНОВОК

Хоча помилки під час розшифрування і не становлять суттєвої загрози на переглянуту версію NTRU (ймовірність такої помилки складає 2^{-100}), на їхній основі можна будувати досить успішні атаки. Це можливо за рахунок наявності кореляційних зв'язків поліномів та наближення ширини поліномів до значення великого модуля q, що й було використано у розглянутій моделі атаки.

Література

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

[2] N. Howgrave-Graham, P. Q. Nguyen, D. Pointcheval, J. Proos, J. H. Silverman,A. Singer, and W. White. The impact of decryption failures on the security of NTRU encryption.

[3] *Горбенко І.Д., Горбенко Ю.І. П*рикладна криптологія: Теорія. Практика. Застосування: Монографія. Вид. 2-ге, перероб. і доп. – Харків: Видавництво «Форт», 2012. – 880 с.

[4] *C. Gentry, M. Szydlo***.** Cryptanalysis of the Revised NTRU Signature Scheme in Eurocrypt ‘02, LNCS 2332, pages 299–320 Springer-Verlag, Berlin, 2002.

Надійшла до редколегії 27.06.2014

Погребняк Костянтин Анатолійович, доцент кафедри БІТ ХНУРЕ, начальник відділу КЗІ АТ «ІІТ». Наукові інтереси: застосування методів алгебраїчної геометрії в криптології, асиметричний криптоаналіз.

Денисов Денис Сергійович, студент ІІІ-го курсу ХНУРЕ напряму БІКС. Наукові інтереси: асиметричні криптосистеми.

УДК 004.056.55

Общая атака на NTRUENCRYPT на основе ошибок расшифрования / К.А. Погребняк, Д.С. Денисов // Прикладная радиоэлектроника: науч.-техн. журнал. – 2014. – Том 13. – № 3. – С. 298–300.

NTRUEncrypt – это криптографическая система с открытым ключом, которая была создана в качестве альтернативы RSA и криптосистемам на эллиптических кривых (ECC). Исключительными особенностями NTRU являются оригинальный специфический математический аппарат и высокая скорость преобразований. Использование NTRU возможно при условии, что не существует криптоаналитических атак, которые могли бы существенно понизить ее криптографическую стойкость. Цель этой статьи – анализ защищенности криптосистемы от общей атаки на основе ошибок расшифрования.

Ключевые слова: NTRU, ошибки при расшифровании, общая атака на основе ошибок расшифрования.

Табл.: 01. Библиогр.: 04 назв.

UDK 004.056.55

General attack against NTRUEncrypt based on decryption failures / K.A. Pogrebnyak, D.S. Denisov// Applied Radio Electronics: Sci. Journ. – 2014. – Vol. 13. – № 3. – P. 298–300.

The NTRUEncrypt is a public key cryptosystem that has been developed as an alternative to RSA and ECC. NTRU is characterized by such features as specific background mathematics and high speed of transformations. The application of NTRU is possible if there are no cryptoanalytical attacks which can substantially decrease its security. The aim of this paper is to analyze the cryptosystem security against a general attack based on decryption failures.

Keywords: NTRU, decryption failures, general attack based on decryption failures.

Tab.: 01. Ref.: 04 items.