УДК 519.2

А.М. ОЛЕКСІЙЧУК
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна, e-mail: *alex-dtn@ukr.net*.

А.А. МАТІЙКО
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна, e-mail: *alexm1710@ukr.net*.

РОЗРІЗНЮВАЛЬНА АТАКА НА ШИФРОСИСТЕМУ NTRUCipher

Анотація. Запропоновано розрізнювальну атаку на симетричну шифросистему NTRUCipher, визначену над кільцем лишків за модулем циклотомічного полінома над скінченним полем простого порядку. Атака базується на існуванні гомоморфізму цього кільця у зазначене поле та може бути досить ефективною за достатньо загальних умов.

Ключові слова: решіткова криптографія, симетрична шифросистема, розрізнювальна атака, циклотомічний поліном, NTRUCipher.

Шифросистему NTRUCipher запропоновано в роботі [1] як симетричний аналог відомої асиметричної схеми шифрування NTRUEncrypt [2]. У працях [3, 4] досліджено різні версії цієї шифросистеми та описано низку атак на них.

У цій статті запропонована розрізнювальна атака (distinguishing attack) на оригінальну версію шифросистеми NTRUCipher [1], яка визначається над кільцем $R(n, q) = \mathbf{Z}_q[x] / (x^n + 1)$, де $n \geq 2$ — степінь двійки, а q – просте число таке, що $q \equiv 1 \bmod 2n$. Ця атака базується на існуванні гомоморфізму кільця $R(n, q)$ у поле $\mathbf{Z}_q$ та, як показано далі, може бути ефективною за достатньо загальних обмежень.

Зауважимо, що за умови $q \equiv 1 \bmod 2n$ мультиплікативна група поля $\mathbf{Z}_q$ містить циклічну підгрупу порядку $2n$, і якщо β є твірним елементом цієї підгрупи, то поліном $x^n + 1$ розкладається над полем $\mathbf{Z}_q$ на лінійні співмножники: $x^n + 1 = (x - \beta)(x - \beta^3) \cdots (x - \beta^{2n-1})$, а отже, збігається з $2n$-циклотомічним поліномом над цим полем (див., наприклад, [5, означення 2.44]).

Зауважимо також, що кільце $R(n, q)$ часто використовується для побудови асиметричних NTRU-подібних (та близьких до них) шифросистем (див., наприклад, [6, 7]). Це пояснюється можливістю застосування швидкого перетворювання Фур'є над полем $\mathbf{Z}_q$ для множення елементів кільця $R(n, q)$, а також відомим результатом [8] стосовно складнісної еквівалентності двох версій задачі Ring-LWE над цим кільцем, що важливо для доведення стійкості (security proof) відповідних криптосистем.

Шифросистема NTRUCipher над кільцем $R(n, q)$ визначається таким чином. Для зашифрування відкритого тексту $m \in R(n, q)$, який є поліномом з коефіцієнтами $0, 1, -1$, на секретному ключі f, що вибирається у визначений спосіб з групи $R(n, q)^*$ оборотних елементів кільця $R(n, q)$, генерується випадковий поліном $r \in R(n, q)$ та обчислюється шифрований текст $c = (m + 3rf^{-1}) \bmod q$. Розшиф-

© А.М. Олексійчук, А.А. Матійко, 2022

рування виконується за формулою $m' = (cf \bmod q) \bmod 3$ і є коректним за відомих умов стосовно вибору поліномів f і r [1–3].

Надалі ми не накладатимемо жодних обмежень на спосіб формування секретного ключа f. Стосовно розподілу випадкового полінома r вважаємо, що цей розподіл задовольняє такій умові β-інваріантності:

$$\forall z \in \mathbf{Z}_q\colon\ p(z) \stackrel{\text{def}}{=} \mathbf{P}(r(\beta) = z) = \mathbf{P}(\beta r(\beta) = z), \tag{1}$$

де β — зазначений вище корінь полінома $x^n + 1$. Вважаємо також, що розподіл ймовірностей (1) відрізняється від рівномірного розподілу на $\mathbf{Z}_q$.

Приклади β-інваріантних законів розподілу містить таке твердження.

Твердження 1. Нехай виконується одна з умов:

1) коефіцієнти $r_0, r_1, \ldots, r_{n-1}$ полінома r є незалежними випадковими величинами, розподіленими за законом $\mathbf{P}(r_i = 1) = \mathbf{P}(r_i = -1) = dn^{-1}$, $\mathbf{P}(r_i = 0) = 1 - 2dn^{-1}$, де $1 \le d \le n - 2$;

2) поліном r формується за правилом $r = r_1 r_2 + r_3$, де r_1, r_2, r_3 — незалежні випадкові поліноми, розподілені за законом, зазначеним в п. 1), а обчислення виконуються в кільці $R(n, q)$.

У цьому разі розподіл ймовірностей випадкового полінома r є β-інваріантним.

Доведення. Нехай $r(x) = r_0 + r_1 x + \cdots + r_{n-1} x^{n-1}$. Оскільки $\beta^n = -1$, то

$$r(\beta) = r_0 + r_1\beta + \cdots + r_{n-1}\beta^{n-1},\ \beta r(\beta) = -r_{n-1} + r_0\beta + \cdots + r_{n-2}\beta^{n-1}.$$

Звідси, використовуючи заміну змінних $b_0 = -a_{n-1}$, $b_1 = a_0, \ldots, b_{n-1} = a_{n-2}$, отримаємо, що за умови 1) для будь-якого $z \in \mathbf{Z}_q$ виконуються рівності

$$\mathbf{P}(\beta r(\beta) = z) = \sum_{b_0 + b_1\beta + \cdots + b_{n-1}\beta^{n-1} = z} \mathbf{P}(r_{n-1} = -b_0)\mathbf{P}(r_0 = b_1)\cdots\mathbf{P}(r_{n-2} = b_{n-1}) =$$

$$= \sum_{-a_{n-1} + a_0\beta + \cdots + a_{n-2}\beta^{n-1} = z} \mathbf{P}(r_{n-1} = a_{n-1})\mathbf{P}(r_0 = a_0)\cdots\mathbf{P}(r_{n-2} = a_{n-2}) =$$

$$= \sum_{-a_{n-1} + a_0\beta + \cdots + a_{n-2}\beta^{n-1} = z} \mathbf{P}(r_0 = -a_{n-1})\mathbf{P}(r_1 = a_0)\cdots\mathbf{P}(r_{n-1} = a_{n-2}) = \mathbf{P}(r(\beta) = z).$$

Далі, за умови 2) з рівності $r(x) = r_1(x)r_2(x) + r_3(x)$ в кільці $R(n, q)$ випливає рівність $r(\beta) = r_1(\beta)r_2(\beta) + r_3(\beta)$ в полі $\mathbf{Z}_q$, яка, в свою чергу, зумовлює рівність $\beta r(\beta) = (\beta r_1(\beta))r_2(\beta) + \beta r_3(\beta)$, де випадкові елементи $\beta r_1(\beta), r_2(\beta), \beta r_3(\beta)$ є незалежними в сукупності та (за доведеним) мають такий самий закон розподілу, що і випадкові елементи $r_1(\beta), r_2(\beta), r_3(\beta)$. Звідси випливає, що розподіли ймовірностей випадкових елементів $r(\beta)$ і $\beta r(\beta)$ співпадають.

Твердження доведено.

Зауважимо, що спосіб, визначений умовою 2) твердження 1, використано в роботі [1] для формування випадкових поліномів r у шифросистемі NTRUCipher.

Запропонована розрізнювальна атака на цю шифросистему має за мету розв'язання такої задачі, відомої під назвою Decision NTRUCipher Ciphertext Cracking Problem [1].

Спостерігається послідовність $\gamma^{(1)}, \dots, \gamma^{(t)}$ незалежних випадкових елементів кільця $R(n, q)$, які з ймовірністю $1/2$ мають рівномірний розподіл на цьому кільці (гіпотеза H_0) і з ймовірністю $1/2$ розподілені за законом

$$\gamma^{(i)} = 3r^{(i)} f^{-1}, \ i \in \overline{1, t}, \tag{2}$$

де $r^{(1)}, \dots, r^{(t)}$ – незалежні випадкові однаково розподілені елементи кільця $R(n, q)$ (гіпотеза H_1). Потрібно побудувати критерій для розрізнення зазначених гіпотез. Інакше кажучи, мета розрізнювальної атаки – відрізнити послідовність (2), яка формується за допомогою шифросистеми NTRUCipher, від випадкової рівноймовірної послідовності елементів кільця $R(n, q)$.

Беручи до уваги міркування, аналогічні представленим у доведенні теореми 3.18 з роботи [9], неважко переконатися, що у разі, коли задача Decision NTRUCipher Ciphertext Cracking Problem є обчислювально складною, шифросистема NTRUCipher є стійкою до атак з підібраним відкритим текстом (CPA secure). Звідси постає природне питання про оцінки складності розв'язання цієї задачі, які можна використовувати для вибору параметрів шифросистеми NTRUCipher.

Для викладення алгоритму розв'язання цієї задачі уведемо додаткові позначення. Зафіксуємо довільну множину A представників усіх суміжних класів групи $R(n, q)^*$ за підгрупою, породженою елементом β. Для заданого розподілу ймовірностей (1) (який відрізняється від рівномірного розподілу на $\mathbf{Z}_q$) позначимо

$$M = \{z \in \mathbf{Z}_q : p(z) > q^{-1}\}, \ p(M) = \sum_{z \in M} p(z),$$

$$C = 1/2 \cdot (p(M) + |M| q^{-1}), \ D = p(M) - |M| q^{-1}.$$

Алгоритм

Вихідні дані: вибірка $\gamma^{(1)}, \dots, \gamma^{(t)}$, члени якої розподілені відповідно до однієї із зазначених вище гіпотез H_0, H_1.

1. Обчислити $\xi^{(i)} = \gamma^{(i)}(\beta)$ для кожного $i \in \overline{1, t}$.

2. Для кожного $a \in A$ обчислити значення $n_a = |\{i \in \overline{1, t} : a\xi^{(i)} \in M\}|$.

Результат: якщо $n_a < Ct$ для усіх $a \in A$, прийняти гіпотезу H_0; інакше – прийняти гіпотезу H_1.

Твердження 2. Нехай $\delta \in (0, 1/2)$,

$$t = \left\lceil 2D^{-2} \ln\left(\frac{\delta^{-1}(q - 1 + 2n)}{2n} \right) \right\rceil. \tag{3}$$

Тоді запропонований алгоритм дає змогу розрізнити гіпотези H_0 і H_1 із середньою ймовірністю помилки не більше $\delta/2$, використовуючи $O\left(\left(\frac{q-1}{n} + n \right) t \right)$ операцій над елементами поля $\mathbf{Z}_q$.

Доведення. Позначимо $\eta_{i,a}$ індикатор події $\{a\xi^{(i)} \in M\}$, $i \in \overline{1, t}$. Справедлива рівність $n_a = \eta_{1,a} + \dots + \eta_{t,a}$, $a \in A$.

Нехай справедлива гіпотеза H_0 і алгоритм припускається помилки. Тоді існує елемент $a \in A$ такий, що $\eta_{1,a} + \cdots + \eta_{t,a} \geq Ct$. При цьому випадкові величини $\eta_{1,a}, \ldots, \eta_{t,a}$ є незалежними в сукупності та мають математичне сподівання, що дорівнює $\mathbf{P}(a\gamma^{(i)}(\beta) \in M) = |M| q^{-1}$, $i \in \overline{1, t}$. Отже, на основі нерівності Гефдінга [10] та визначення параметрів C і D матимемо

$$\mathbf{P}(\eta_{1,a} + \cdots + \eta_{t,a} \geq Ct) = \mathbf{P}\left(\sum_{i=1}^{t} \eta_{i,a} - tq^{-1}|M| \geq t(C - q^{-1}|M|) \right) \leq$$

$$\leq \exp\{-2t(C - q^{-1}|M|)^2\} = \exp\{-1/2 \cdot tD^2\}.$$

Отже, ймовірність помилки алгоритму за умови справедливості гіпотези H_0 не перевищує

$$p_0 = |A| \exp\{-1/2 \cdot tD^2\} = \frac{q-1}{2n} \exp\{-1/2 \cdot tD^2\}. \qquad (4)$$

Нехай зараз справедлива гіпотеза H_1, тобто випадкові величини $\gamma^{(1)}, \ldots, \gamma^{(t)}$ розподілені за законом (2).

Позначимо g обернений елемент до полінома $f \in R(n, q)^*$ та покладемо $a_0 = 3g(\beta)$. З урахуванням формули (2) справедлива рівність $\xi^{(i)} = a_0 r^{(i)}(\beta)$, $i \in \overline{1, t}$, де $a_0 \neq 0$. При цьому згідно з означенням множини A існує число $j \in \overline{0, 2n-1}$ таке, що $a \overset{\text{def}}{=} (a_0)^{-1} \beta^j \in A$.

Якщо алгоритм припускається помилки, то для кожного, а отже, і для зазначеного вище елемента a виконується нерівність $\eta_{1,a} + \cdots + \eta_{t,a} < Ct$. При цьому випадкові величини $\eta_{1,a}, \ldots, \eta_{t,a}$ є незалежними в сукупності та мають математичне сподівання

$$\mathbf{P}(a\xi^{(i)} \in M) = \mathbf{P}((a_0)^{-1} \beta^j a_0 r^{(i)}(\beta) \in M) = \mathbf{P}(r^{(i)}(\beta) \in M) = p(M), \; i \in \overline{1, t},$$

де передостання рівність випливає з формули (1). Звідси на підставі нерівності Гефдінга отримуємо нерівність

$$\mathbf{P}(\eta_{1,a} + \cdots + \eta_{t,a} < Ct) = \mathbf{P}\left(\sum_{i=1}^{t} \eta_{i,a} - tp(M) < t(C - p(M)) \right) \leq$$

$$\leq \exp\{-2t(C - p(M))^2\} = \exp\{-1/2 \cdot tD^2\}.$$

Отже, ймовірність помилки алгоритму за умови справедливості гіпотези H_1 не перевищує

$$p_1 = \exp\{-1/2 \cdot tD^2\}. \qquad (5)$$

З формул (4), (5) випливає, що середня ймовірність помилки алгоритму не перевищує $1/2 \cdot (p_0 + p_1) = \frac{1}{2}\left(\frac{q-1}{2n} + 1 \right) \exp\{-1/2 \cdot tD^2\}$, що на основі формули (3) не перевищує $\delta / 2$.

Крім того, складність обчислення всіх значень $\xi^{(i)}$, $i \in \overline{1, t}$, з використанням схеми Руфіні–Горнера на кроці 1 алгоритму складає $O(nt)$ арифметичних операцій у полі $\mathbf{Z}_q$ (див., наприклад, [11]), а обчислення всіх значень n_a, $a \in A$, на кроці 2 потребує $O(|A|t) = O\left(\frac{q-1}{2n} t \right)$ операцій. Звідси безпосередньо випливає, що часова складність алгоритму дорівнює $O\left(\left(\frac{q-1}{n} + n \right) t \right)$.

Твердження доведено.

Таблиця 1. Оцінки інформаційної складності розрізнювальної атаки на шифросистему NTRUCipher

Вихідні дані для розрахунків			Отримані результати	
n	q	β	$-\log_2 D$	$\log_2 t$
256	7681	17	33.95	71.79
	10753	11	31.82	67.59
	11777	3	33.88	71.71
	12289	11	33.33	70.62
	13313	3	33.02	70.03
512	12289	11	56.09	116.03
	13313	3	56.46	116.77
	15361	7	57.93	119.75
	18433	5	55.35	114.61
	19457	3	59.91	123.75

У табл. 1 наведено оцінки інформаційної складності (date complexity) (3) розрізнювальної атаки на шифросистему NTRUCipher для низки значень n і q у разі, коли розподіл ймовірностей випадкового полінома r визначається відповідно до умови 1) твердження 1 (для $dn^{-1} = 1/3$, $\delta = 0.01$). Для проведення розрахунків використано таке твердження.

Твердження 3. За умови 1) твердження 1 розподіл ймовірностей (1) визначається за формулою

$$p(z) = q^{-1} \sum_{\alpha \in \mathbf{Z}_q} \cos\left(\frac{2\pi\alpha z}{q}\right) \prod_{j=0}^{n-1} \theta(dn^{-1}, \alpha\beta^j), \ z \in \mathbf{Z}_q, \tag{6}$$

де $\theta(p, x) = 1 - 2p\left(1 - \cos\left(\frac{2\pi x}{q}\right)\right)$ для будь-яких $p \in [0,1]$, $x \in \mathbf{Z}_q$.

Доведення. Позначимо $r(x) = r_0 + r_1 x + \cdots + r_{n-1} x^{n-1}$, $\omega = \exp\{2\pi i q^{-1}\}$, де $i^2 = -1$, і знайдемо перетворення Фур'є $\hat{p}(\alpha) = \sum_{z \in \mathbf{Z}_q} \mathbf{P}(r(\beta) = z)\omega^{-\alpha z}$, $\alpha \in \mathbf{Z}_q$, розподілу ймовірностей (1).

Зауважимо, що на основі умови 1) твердження 1 перетворення Фур'є випадкової величини $r_j \beta^j$ має вигляд

$$\sum_{z \in \mathbf{Z}_q} \mathbf{P}(r_j \beta^j = z)\omega^{-\alpha z} = \mathbf{P}(r_j = 0) + \mathbf{P}(r_j = 1)\omega^{-\alpha\beta^j} + \mathbf{P}(r_j = -1)\omega^{\alpha\beta^j} =$$

$$= 1 - 2dn^{-1} + dn^{-1}(\omega^{-\alpha\beta^j} + \omega^{\alpha\beta^j}) = 1 - 2dn^{-1}\left(1 - \cos\left(\frac{2\pi\alpha\beta^j}{q}\right)\right) = \theta(dn^{-1}, \alpha\beta^j),$$

$$\alpha \in \mathbf{Z}_q, \ j \in \overline{0, n-1}.$$

Звідси унаслідок незалежності випадкових величин $r_0, r_1\beta, \ldots, r_{n-1}\beta^{n-1}$ і теореми про згортку знаходимо, що $\hat{p}(\alpha) = \prod_{j=0}^{n-1} \theta(dn^{-1}, \alpha\beta^j)$, $\alpha \in \mathbf{Z}_q$.

З отриманого співвідношення та формули обернення для перетворення Фур'є випливає рівність (6).

Твердження доведено.

Як видно з табл. 1, для $n = 256$ інформаційна складність атаки змінюється в межах від $2^{67.59}$ до $2^{71.79}$ (часова складність перевищує інформаційну приблизно в $\frac{q-1}{n} + n$ разів). Отриманий результат свідчить про необхідність враховувати розрізнювальну атаку (поряд з іншими) під час вибору параметрів шифросистеми NTRUCipher для забезпечення належної стійкості (security).

СПИСОК ЛІТЕРАТУРИ

1. Valluri M.R. NTRUCipher-lattice based secret key encryption. arXiv:1710.01928V2. 6/10/2017.
2. Hoffstein J., Pipher J., Silverman J.H. NTRU: a new high speed public key cryptosystem. Algorithmic Number Theory (ANTS III). *LNCS.* 1998, Vol. 1423. P. 267–288.
3. Матійко А.А. Порівняльний аналіз алгоритмів шифрування NTRUEncrypt та NTRUCipher. *Математичне та комп'ютерне моделювання. Серія*: *Технічні науки*. 2019, Вип. 19. С. 81–87.
4. Матійко А.А. BKW-атака на шифросистеми NTRUCIPHER та NTRUCIPHER+. *Information Technology and Security*. 2020. Т. 8, № 2. С. 164–176.
5. Albrecht M.R., Curtis B.R., Deo A., Davidson A., Player R., Postlethwaite E.W., Virdia F., Wunderer T. Estimate all the {LWE, NTRU} schemes!. Cryptology ePrint Archive, Report 2018/331. URL: http://eprint.iacr.org/2018/331.
6. Diop S., Sané B.O., Seck M., Diarra N. NTRU-LPR IND-CPA: a new ideal lattice-based scheme. Cryptology ePrint Archive, Report 2018/109. URL: http://eprint.iacr.org/2018/109.
7. Лидл Р., Нидеррайтер Г. Конечные поля: В 2 т. Пер. с англ. Москва: Мир, 1988. 818 с.
8 Lybashevsky V., Peikert C., Regev O. On ideal lattices and learning with errors over rings. Advanced in Cryptology – EUROCRYPT 2010. *LNCS 6110.* Springer-Verlag, 2010. P. 1–23.
9. Katz J., Lindell Y. Introduction to modern cryptography. *CRC Press*, 2015. 598 p.
10. Hoeffding W. Probability inequalities for sums of bounded random variables. *J. Amer. Statist. Assoc*. 1963. Vol. 58, N 301. P. 13–30.
11. Черемушкин А.В. Лекции по арифметическим алгоритмам в криптографии. Москва: МЦНМО, 2002. 104 с.

A.N. Alekseychuk, A.A. Matiyko

DISTINGUISHING ATTACK ON THE NTRUCipher ENCRYPTION SCHEME

Abstract. A distinguishing attack on the NTRUCipher symmetric encryption scheme, defined over the residue ring modulo a cyclotomic polynomial over a finite field of simple order, is proposed. The attack is based on the existence of a homomorphism from this ring into the specified field and can be quite effective under sufficiently general conditions.

Keywords: lattice-based cryptography, symmetric encryption scheme, distinguishing attack, cyclotomic polynomial, NTRUCipher.

Надійшла до редакції 22.09.2021