Чобаль Олександр Ілліч, кандидат фізико-математичних наук, доцент кафедри твердотільної електроніки та інформаційної безпеки фізичного факультету УжНУ.
E-mail: oleksandr.chobal@uzhnu.edu.ua.
Orcid ID:0000-0002-8042-8052.
Чобаль Александр Ильич, кандидат физико-математических наук, доцент кафедры твердотельной электроники и информационной безопасности физического факультета УжНУ.
Chobal Oleksandr, Candidate of Physical and Mathematical Sciences, Associate Professor of the Department of Solid State Electronics and Information Security of the Physical Faculty, UzhNU.

Різак Василь Михайлович, доктор фізико-математичних наук, професор, завідувач кафедри твердотільної електроніки та інформаційної безпеки фізичного факультету УжНУ.
E-mail:vrizak@uzhnu.edu.ua.
Orcid ID: 0000-0002-9177-0662.
Ризак Василий Михайлович, доктор физико-математических наук, профессор, заведующий кафедрой твердотельной электроники и информационной безопасности физического факультета УжНУ.
Rizak Vasyl, Doctor of Physical and Mathematical Sciences, Professor, Head of the Department of Solid State Electronics and Information Security of the Physical Faculty, UzhNU.

DOI: 10.18372/2410-7840.22.14981
УДК 621.391:519.2

ШВИДКА РОЗРІЗНЮВАЛЬНА АТАКА НА ШИФРОСИСТЕМУ NTRUCipher+

Александра Матійко, Антон Олексійчук

Шифросистему NTRUCipher запропоновано в 2017 р. як симетричну версію алгоритму шифрування NTRUEncrypt, який є на сьогодні одним з найшвидших постквантових криптографічних алгоритмів, що базуються на решітках у евклідовому просторі. Метою побудови NTRUCipher є створення симетричної шифросистеми для практичних застосувань, стійкість якої, аналогічно асиметричним, базується на складності розв'язанні лише однієї обчислювальної задачі. Проведені попередні дослідження зазначеної шифросистеми, проте за їх рамками залишається питання про стійкість NTRUCipher відносно розрізнювальних атак, спрямованих на побудову статистичних критеріїв для розрізнення послідовностей шифрованих повідомлень шифросистеми та суто випадкових послідовностей. У даній статті показано, що шифросистема NTRUCipher та навіть її природне удосконалення – NTRUCipher+, запропоноване по аналогії з відомою обґрунтовано стійкою версією асиметричної криптосистеми NTRU, є вразливими відносно розрізнювальних атак. Запропоновано швидку розрізнювальну атаку на шифросистему NTRUCipher+ та (для окремого випадку) ще більш швидку модифікацію цієї атаки. Отримано аналітичні оцінки трудомісткості обох атак, з яких випливає, що вони мають поліноміальну часову складність та можуть бути реалізовані в режимі реального часу (для стандартного набору параметрів шифросистеми). Отримані результати свідчать про те, що для побудови симетричних NRTU-подібних криптосистем слід використовувати інші загальні конструкції.

Ключові слова: *постквантова криптографія, криптосистеми на решітках, розрізнювальна атака, дискретне перетворення Фур'є, NTRUEncrypt, NTRUCipher.*

ВСТУП

На сьогодні асиметричні шифросистеми, побудовані за схемою алгоритму шифрування NTRUEncrypt [8], відносяться до найшвидших постквантових криптосистем і протоколів. Вони будуються на основі арифметичних операцій (додавання, множення та обернення) у кільцях зрізаних поліномів та за умови належного вибору параметрів забезпечують потрібну стійкість відносно відомих атак поряд із високою швидкістю шифрування та прийнятними для багатьох застосувань довжинами відкритих ключів і шифрованих текстів.

До NTRU-подібних (або близьких до них, типу LWE) криптосистем відноситься майже третина усіх постквантових криптографічних алгоритмів, представлених на конкурс NIST зі стандартизації постквантових криптопримітивів (див. роботи [3, 5] та наведені у них посилання).

В [11] запропоновано симетричну версію алгоритму NTRUEncrypt – шифросистему NTRUCipher, перші дослідження якої проведено в [11, 2]. Зауважимо, що за рамками цих досліджень

залишається питання про стійкість NTRU-послідовностей шифрованих повідомлень шифросистеми та суто випадкових послідовностей (див. Cipher відносно розрізнювальних атак, спрямованих на побудову статистичних критеріїв для розрізнення наприклад, [9], розділ 3).

Мета цієї статті – показати, що шифросистема NTRUCipher та навіть її природне удосконалення – NTRUCipher+, запропоноване по аналогії з обґрунтовано стійкою версією асиметричної криптосистеми NTRU [10], є вразливими відносно розрізнювальних атак. Запропоновано швидку розрізнювальну атаку на шифросистему NTRUCipher+ та (для окремого випадку) ще більш швидку модифікацію цієї атаки.

Отримано аналітичні оцінки трудомісткості обох атак, з яких випливає, що вони мають поліноміальну часову складність та можуть бути реалізовані в режимі реального часу (для стандартного набору параметрів шифросистеми [6]).

Отримані результати свідчать про те, що для побудови симетричних NRTU-подібних криптосистем слід використовувати інші загальні конструкції, які відрізняються за сутністю від запропонованої в [11].

Означення основних понять

Нехай n і q – різні прості числа, $n, q > 3$, причому q є примітивним елементом за модулем n (тобто найменше натуральне l таке, що $q^l \equiv 1 \bmod n$, дорівнює $n-1$). Позначимо $\mathbf{Z}_q$ кільце класів лишків за модулем q, елементи якого ототожнимо з цілими числами, що належать інтервалу $[-(q-1)/2, (q-1)/2]$.

Позначимо $R_{n,q} = \mathbf{Z}_q[x]/(x^n - 1)$ кільце зрізаних поліномів степеня не вище $n-1$ над кільцем $\mathbf{Z}_q$. Зазначене кільце складається з q^n поліномів вигляду $u = u_0 + u_1 x + \cdots + u_{n-1}x^{n-1}$, де $u_i \in \mathbf{Z}_q$, $i \in \overline{0, n-1}$, які додаються та перемножуються за модулем полінома $x^n - 1$.

Позначимо $R_{n,q}^*$ групу оборотних елементів кільця $R_{n,q}$.

Для будь-якого $u = u_0 + u_1 x + \cdots + u_{n-1}x^{n-1} \in \mathbf{Z}[x]$ позначимо $u \bmod q$ поліном:

$(u_0 \bmod q) + (u_1 \bmod q)x + \cdots + (u_{n-1} \bmod q)x^{n-1} \in R_{n,q}$.

Аналогічний сенс має позначення $u \bmod 3$.

Позначимо також $\| u \|_\infty = \max\limits_{0 \le i \le n-1} |u_i|, \| u \|_1 = \sum\limits_{i=0}^{n-1} |u_i|$. Поліном u називається *малим*, якщо $\| u \|_\infty = 1$.

Позначимо символом S множину всіх малих поліномів степеня не вище $n-1$, а символом S_d множину всіх поліномів $u \in S$, серед кофіцієнтів яких є точно d, що дорівнюють 1, та точно d, що дорівнюють -1, $1 \le d \le n-2$.

Для зазначених вище чисел n, q і d *шифросистема NTRUCipher+* визначається таким чином.

Секретними ключами цієї шифросистеми є довільні поліноми $F \in S_d$, а відкритими повідомленнями – довільні малі поліноми.

Зауважимо, що на підставі зроблених припущень стосовно чисел n, q і d виконується умова $f \overset{\text{def}}{=} 1 + 3F \in R_{n,q}^*$ (див. [1]).

Для зашифрування повідомлення $m \in S$ на ключі F генеруються незалежні випадкові поліноми r та $e = e_0 + e_1 x + \cdots + e_{n-1}x^{n-1}$, де r має рівномірний розподіл ймовірностей на множині S_d, а $e_0, e_1, \ldots, e_{n-1}$ є незалежними випадковими величинами, які приймають значення $0, 1, -1$ з імовірністю $1/3$.

Далі обчислюється шифроване повідомлення:

$$E_f(m, r, e) = (m + 3(rf^{-1} + e)) \bmod q, \qquad (1)$$

де f^{-1} – обернений до f елемент кільця $R_{n,q}$. Розшифрування довільного повідомлення $c \in R_{n,q}$ на ключі F здійснюється за формулою:

$$D_f(c) = cf \,(\bmod q) \bmod 3, \qquad (2)$$

де $f = 1 + 3F$.

З наведених означень випливає, що $D_f(E_f(m,r,e))=m$, якщо $\|mf+3(r+ef)\|_\infty < q/2$. При цьому, оскільки $\|F\|_1=2d$, $\|e\|_\infty=\|r\|_\infty=1$, то:

$$\|mf+3(r+ef)\|_\infty=\|m+3(mF+r+e+3eF)\|_\infty \le$$
$$\le 1+3(\|m\|_\infty\|F\|_1+\|r\|_\infty+\|e\|_\infty+3\|e\|_\infty\|F\|_1)=$$
$$7+24d.$$

Таким чином, за умови:

$$d<(q-14)/48 \qquad (3)$$

розшифрування отриманих повідомлень відбувається коректно.

Зауважимо, що головною відмінністю шифросистеми NTRUCipher+ від NTRUCipher [11] є використання додаткового випадкового полінома e при зашифруванні (для NTRUCipher доданок e у формулі (1) дорівнює нулю).

Використовувати такий доданок в одній з асиметричних версій криптосистеми NTRU запропоновано в [10] для забезпечення семантичної стійкості криптосистеми.

Проте для визначеної симетричної цей доданок не гарантує стійкості відносно розрізнювальної атаки, яку описано нижче.

ПОСТАНОВКА ЗАДАЧІ ТА ОТРИМАНІ РЕЗУЛЬТАТИ

Розглянемо атаку, мета якої полягає в тому, щоб відрізнити послідовність шифрованих повідомлень шифросистеми NTRUCipher+ від суто випадкової послідовності елементів кільця $R_{n,q}$.

Точна постановка задачі має такий вигляд. Спостерігається послідовність незалежних випадкових величин $c^{(1)},\dots,c^{(t)}$, які з ймовірністю $1/2$ мають рівномірний розподіл на множині $R_{n,q}$ (гіпотеза H_0) та з імовірністю $1/2$ отримуються за формулою:

$$c^{(i)}=(m^{(i)}+3(r^{(i)}(1+3F)^{-1}+e^{(i)}))\bmod q,\ i\in\overline{1,t},$$

(4) де $m^{(i)}$, $r^{(i)}$ та $e^{(i)}$ є незалежними випадковими поліномами, що мають рівномірні розподіли ймовірностей на множинах S, S_d та S відповідно, $i\in\overline{1,t}$, а $F\in S_d$ є невідомим ключем шифросистеми NTRUCipher+ (гіпотеза H_1).

Треба побудувати критерій для розрізнення зазначених гіпотез. Іншими словами, мета розрізнювальної атаки – відрізнити послідовність шифрованих повідомлень (4) шифросистеми NTRUCipher+ від суто випадкової послідовності елементів кільця $R_{n,q}$.

Для побудови критерію перевірки гіпотез H_0 та H_1 розглянемо значення поліномів $c^{(1)},\dots,c^{(t)}$ в точці, що дорівнює одиниці поля $\mathbf{Z}_q$. Зрозуміло, що за умови справедливості гіпотези H_0 елементи $c^{(1)}(1),\dots,c^{(t)}(1)$ є незалежними в сукупності та мають рівномірний розподіл на цьому полі.

Поряд з тим, на підставі формули (4) та рівностей $R_{n,q}=\mathbf{Z}_q[x]/(x^n-1)$, $F(1)=r^{(i)}(1)=0$ за умови справедливості гіпотези H_1 має місце співвідношення

$$c^{(i)}(1)=(m^{(i)}(1)+3e^{(i)}(1))\bmod q,\ i\in\overline{1,t}. \qquad (5)$$

Для будь-якого $x\in\mathbf{Z}_q$ позначимо $\theta(x)=\frac{1}{3}\left(1+2\cos\left(\frac{2\pi x}{q}\right)\right)$.

Лема. Розподіл ймовірностей випадкової величини (5) визначається за формулою:

$$p(z)\overset{\text{def}}{=}\mathbf{P}(c^{(i)}(1)=z)=$$
$$=q^{-1}\sum_{\alpha\in\mathbf{Z}_q}\cos\left(\frac{2\pi\alpha z}{q}\right)\theta(\alpha)^n\theta(3\alpha)^n,\ z\in\mathbf{Z}_q. \qquad (6)$$

Доведення. Оскільки випадкові поліноми $m^{(i)}, e^{(i)}$ є незалежними та мають рівномірний розподіл ймовірностей на множині S, то їх коефіцієнти є незалежними випадковими величинами, що приймають кожне значення $0,1,-1$ з ймовірністю $1/3$.

Позначимо ω примітивний комплексний корінь степеня q з одиниці та обчислимо перетворення Фур'є:

$$\hat{p}(\alpha)=\sum_{z\in\mathbf{Z}_q}\mathbf{P}(m_j^{(i)}=z)\omega^{-\alpha z}$$ [4] j-го коефіцієнту випадкового полінома $m^{(i)}$:

$$\hat{p}(\alpha)=\mathbf{P}(m_j^{(i)}=0)+\mathbf{P}(m_j^{(i)}=1)\omega^{-\alpha}+\mathbf{P}(m_j^{(i)}=-1)\omega^{\alpha}$$

$$= 1/3\,(1+\omega^{-\alpha}+\omega^{\alpha}) = \frac{1}{3}\left(1+2\cos\left(\frac{2\pi\alpha}{q}\right)\right) = \theta(\alpha),$$

$\alpha \in \mathbf{Z}_q$.

Аналогічно отримаємо, що перетворення Фур'є j-го коефіцієнту випадкового полінома $3e^{(i)}$ дорівнює $\theta(3\alpha)$, $i \in \overline{1,t}$, $j \in \overline{0,n-1}$. Звідси на підставі теореми про згортку [4] випливає, що перетворення Фур'є розподілу випадкової величини (5) дорівнює $\theta(\alpha)^n\theta(3\alpha)^n$, $\alpha \in \mathbf{Z}_q$. Отже, згідно з формулою оберненого перетворення Фур'є [4] має місце рівність (6).

Лему доведено.

Позначимо

$$M = \{z \in \mathbf{Z}_q : p(z) > q^{-1}\}, C = \frac{1}{2}\sum_{z\in M}\left(p(z)+q^{-1}\right),$$

$$\Delta = \sum_{\alpha\in\mathbf{Z}_q\setminus\{0\}} \theta(\alpha)^{2n}\theta(3\alpha)^{2n}$$

та опишемо алгоритм, що дозволяє перевіряти справедливість однієї з гіпотез H_0, H_1 із (середньою) ймовірністю помилки, яка не перевищує заданого порогу.

Алгоритм 1 (розрізнювальна атака на NTRUCipher+). Вхідні дані: вибірка $c^{(1)}, \ldots, c^{(t)}$, члени якої розподілені відповідно до однієї з гіпотез H_0, H_1.

Кроки обчислення. Обчислити послідовність $c^{(1)}(1), \ldots, c^{(t)}(1)$ та підрахувати значення $N = |\{i \in \overline{1,t} : c^{(i)}(1) \in M\}|$.

Результат: якщо $N \le Ct$, прийняти гіпотезу H_0; інакше – прийняти гіпотезу H_1.

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

$$t = \left\lceil \frac{8q\ln(\delta^{-1})}{\Delta} \right\rceil. \qquad (7)$$

Тоді алгоритм 1 дозволяє розрізнити гіпотези H_0 і H_1 із середньою ймовірністю помилки не вище ніж δ, використовуючи $O(nt)$ операцій над елементами поля $\mathbf{Z}_q$.

Доведення. Позначимо ξ_i індикатор події $\{c^{(i)}(1) \in M\}$, $i \in \overline{1,t}$. Має місце рівність $N = \xi_1 + \cdots + \xi_t$.

Якщо справедлива гіпотеза H_0, то ймовірність помилки алгоритму 1 дорівнює $\mathbf{P}(\xi_1 + \cdots + \xi_t > Ct)$, і випадкові величини $\xi_1, \ldots, \xi_t$ є незалежними та рівномірно розподіленими на полі $\mathbf{Z}_q$.

Отже, на підставі нерівності Гефдінга [7] та означення параметра C справедливі рівності

$$\mathbf{P}(\xi_1+\cdots+\xi_t > Ct) = \mathbf{P}\left(\sum_{i=1}^{t}\xi_i - tq^{-1}|M| > t(C-q^{-1}|M|)\right) \le$$

$$\le \exp\left\{-2t(C-q^{-1}|M|)^2\right\} = \exp\left\{-1/2\cdot td^2\right\},$$

де $d = \sum_{z\in M}\left(p(z)-q^{-1}\right)$.

Якщо справедлива гіпотеза H_1, то ймовірність помилки алгоритму 1 дорівнює $\mathbf{P}(\xi_1 + \cdots + \xi_t \le Ct)$, і випадкові величини $\xi_1, \ldots, \xi_t$ є незалежними та мають математичні сподівання, що дорівнюють

$$p(M) \stackrel{\text{def}}{=} \sum_{z\in M} p(z)\cdot$$

Отже, згідно з нерівністю Гефдінга:

$$\mathbf{P}(\xi_1+\cdots+\xi_t \le Ct) = \mathbf{P}\left(\sum_{i=1}^{t}\xi_i - tp(M) \le t(C-p(M))\right) \le$$

$$\le \exp\left\{-2t(C-p(M))^2\right\} = \exp\left\{-1/2\cdot td^2\right\}.$$

Таким чином, середня ймовірність помилки алгоритму 1 не перевищує $\exp\left\{-1/2\cdot td^2\right\}$. Звідси, використовуючи співвідношення

$$d^2 = \left(\sum_{z\in M}\left(p(z)-q^{-1}\right)\right)^2 = \left(\frac{1}{2q}\sum_{z\in\mathbf{Z}_q}|qp(z)-1|\right)^2 \ge$$

$$\frac{1}{4q^2}\sum_{z\in\mathbf{Z}_q}|qp(z)-1|^2 = \frac{1}{4q}\sum_{\alpha\in\mathbf{Z}_q\setminus\{0\}}\hat{p}(\alpha)^2 = \frac{\Delta}{4q},$$

передостаннє з яких є наслідком рівності Парсеваля [4], а останнє випливає з формули (6), отримаємо, що середня ймовірність помилки алгоритму 1 не перевищує $\exp\left\{-\frac{\Delta\cdot t}{8q}\right\}$, що, у

свою чергу, є не вище ніж δ згідно з формулою (7).

Твердження доведено.

В табл. 1 наведено результати розрахунків інформаційної складності (тобто параметра (7)) запропонованої атаки для низки значень n, рекомендованих в [6], та відповідних їм значень q (зауважимо, що складність атаки не залежить від параметра d).

Таблиця 1

Оцінки інформаційної складності розрізнювальної атаки на шифросистему NTRUCipher+ $(\delta = 0{,}01)$

n	q	$\log t$	Δ
401	139	19,22	0,01
	1051	13,00	4,73
	2393	12,84	12,05
449	389	13,80	1,01
	2207	12,94	10,38
	3449	12,89	16,78
677	409	14,36	0,72
	2423	13,25	9,17
	5171	13,17	20,71
1091	457	15,00	0,51
	4217	13,55	12,95
	8581	13,49	27,38
1171	443	15,25	0,42
	3851	13,62	11,29
	8009	13,56	24,57

Як видно з табл. 1, із збільшенням параметра q збільшується значення параметра Δ та зменшується інформаційна (а, отже, і часова) складність атаки. При $n = 401$, $q = 139$ спостерігається найбільше значення обсягу матеріалу $t = 2^{19}$, потрібного для реалізації атаки із середньою ймовірністю помилки не вище ніж δ.

Покажемо зараз, що у випадку, коли

$$8n + 1 < q, \qquad (8)$$

для надійного розрізнення гіпотез H_0 і H_1 можна використовувати більш простий (та більш ефективний з погляду трудомісткості) алгоритм.

Алгоритм 2 (удосконалена розрізнювальна атака на NTRUCipher+). Вхідні дані: вибірка $c^{(1)}, \dots, c^{(t)}$, члени якої розподілені відповідно до однієї з гіпотез H_0, H_1.

Кроки обчислення. Обчислити послідовність $c^{(1)}(1), \dots, c^{(t)}(1)$.

Результат: якщо існує $i \in \overline{1,t}$ таке, що $|c^{(i)}(1)| > 4n$, прийняти гіпотезу H_0; інакше – прийняти гіпотезу H_1.

Твердження 2. Нехай виконується умова (8), $\delta \in (0, 1/2)$ і

$$t = \left\lceil \frac{\log\left((2\delta)^{-1}\right)}{\log\left(\frac{q}{8n+1}\right)} \right\rceil. \qquad (9)$$

Тоді алгоритм 2 дозволяє розрізнити гіпотези H_0 і H_1 із середньою ймовірністю помилки не вище ніж δ, використовуючи $O(nt)$ операцій над елементами поля $\mathbf{Z}_q$.

Доведення. Якщо справедлива гіпотеза H_0, то $c^{(1)}(1), \dots, c^{(t)}(1)$ є незалежними випадковими величинами з рівномірним розподілом ймовірностей на полі $\mathbf{Z}_q$, і алгоритм 2 припускається помилки тоді й тільки тоді, коли усі ці величини приймають значення в інтервалі $[-4n, 4n]$.

Отже, ймовірність помилки алгоритму 2 в цьому випадку дорівнює $\left(\frac{8n+1}{q}\right)^t$.

Якщо справедлива гіпотеза H_1, то ймовірність помилки алгоритму дорівнює нулю. Дійсно, внаслідок умови $m^{(i)}, e^{(i)} \in S$ модуль суми коефіцієнтів полінома $m^{(i)} + 3e^{(i)}$ в кільці цілих чисел не перевищує $4n$, що є менше ніж $(q-1)/2$ на підставі нерівності (8).

Отже, зазначений модуль співпадає зі значенням $|(m^{(i)}(1) + 3e^{(i)}(1)) \bmod q|$, яке дорівнює $|c^{(i)}(1)|$ згідно з формулою (5), $i \in \overline{1,t}$.

Таким чином, середня ймовірність помилки алгоритму 2 дорівнює $\frac{1}{2}\left(\frac{8n+1}{q}\right)^t$, що не перевищує δ на підставі рівності (9). Твердження доведено.

ВИСНОВКИ

Отримані результати показують, що запропонована розрізнювальна атака (алгоритм 1) на NTRUCipher+ дозволяє зламати цю шифросистему в режимі реального часу. Зокрема, для

значень параметрів n і q, зазначених у табл. 1, часова складність атаки не перевищує $2^{19}n$ операцій в полі $\mathbf{Z}_q$. За умови (8) є застосовною удосконалена розрізнювальна атака (алгоритм 2), яка дозволяє зламати шифросистему за фіксований час (що не залежить від n і q, а визначається лише верхньою межею ймовірності помилки атаки). Зауважимо, що жодна з наведених вище атак не розглянута в роботі [11], де запропоновано шифросистему NTRUCipher. Проте існування таких атак свідчить про те, що для побудови симетричного аналога криптосистеми NTRU слід використовувати інші загальні конструкції шифросистем, що базуються на решітках.

ЛІТЕРАТУРА

[1] Алексейчук А.Н., Матийко А.А. Оценки вероятности обратимости случайных многочленов, используемых в модифицированной версии криптосистемы NTRU // *Радиотехника*. – 2017. – Вип. 189. – С. 38 – 46.

[2] Матійко А.А. Порівняльний аналіз алгоритмів шифрування NTRUEncrypt та NTRUCipher // *Математичне та комп'ютерне моделювання*. Серія: Технічні науки, Вип. 19. – 2019. – С. 81 – 87.

[3] 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*. [Електронний ресурс] – Режим доступу до ресурсу: http://eprint.iacr.org /2018/331.

[4] Babai L. *The Fourier transform and equations over finite abelian groups* [Електронний ресурс] – Режим доступу до ресурсу: http:// peple.cs.uchicago.du/~laci/ren/fourier.pdf.

[5] Diop S., Sane′ B.O., Seck M., Diarra N. NTRU-LPR IND-CPA: a new ideal lattice-based scheme // *Cryptology ePrint Archive, Report 2018/109* [Електронний ресурс] – Режим доступу до ресурсу: http://eprint. iacr.org/2018/109.

[6] Hirschhorn P., Hoffstein J., Howgrave-Graham N., Whyte W. Choosing NTRU parameters in light of combined lattice reduction and MITM aproaches // *Applied Cryptography and Network Security, LNCS*. – Vol. 5536. – 2009. – pp. 437 – 455.

[7] Hoeffding W. Probability inequalities for sums of bounded random variables // *J. Amer. Statist. Assoc.* – 1963. – Vol. 58. – № 301.

[8] Hoffstein J., Pipher J., Silverman J.H. NTRU: a new high speed public key cryptosystem // *Algorithmic Number Theory (ANTS III). LNCS*. – Vol. 1423. – 1998. – pp. 267 – 288.

[9] Katz J., Lindell Y. *Introduction to modern cryptography*. – CRC Press, 2015. – 598 p.

[10] Stehle′ D., Steinfeld R. Making NTRU as secure as worst-case problems over ideal lattices // Advances in Cryptology – *EUROCRYPT 2011*. – Proceedings. – Springer-Verlag. – 2011. – pp.27–47.

[11] Valluri M.R. *NTRUCipher-lattice based secret key encryption* // arXiv:1710.01928V2. [Електронний ресурс] – Режим доступу до ресурсу: https://arxiv.org/pdf/ 1710.01928.pdf.

БЫСТРАЯ РАЗЛИЧАЮЩАЯ АТАКА НА ШИФРОСИСТЕМУ NTRUCipher+

Шифрсистему NTRUCipher предложено в 2017 г. как симметричную версию алгоритма шифрования NTRUEncrypt, который является сегодня одним из самых быстрых постквантових криптографических алгоритмов, основанных на решетках в эвклидовом пространстве. Целью построения NTRUCipher является создание симметричной шифрсистемы для практических применений, стойкость которой, аналогично асимметричным, базируется на сложности решения только одной вычислительной задачи. Проведены предварительные исследования указанной шифрсистемы, однако остается вопрос о стойкости NTRUCipher относительно различающих атак, направленных на построение статистических критериев для различия последовательностей шифрованных сообщений шифрсистемы и полностью случайных последовательностей. В данной статье показано, что шифрсистема NTRUCipher и даже её естественное усовершенствование – NTRUCipher+, предложенное по аналогии с известной обоснованно стойкой версией асимметричной криптосистемы NTRU, уязвимы к различающим атакам. Предложено быструю различающую атаку на шифрсистему NTRUCipher+ и (для частного случая) еще более быструю модификацию этой атаки. Получены аналитические оценки трудоёмкости обеих атак, из которых следует, что они имеют полиномиальную временную сложность и могут быть реализованы в режиме реального времени (для стандартного набора параметров шифрсистемы). Полученные результаты свидетельствуют о том, что для построения симметричных NRTU-подобных криптосистем следует использовать другие общие конструкции.

Ключевые слова: постквантовая криптография, криптосистемы на решётках, различающая атака, дискретное превращение Фурье, NTRUEncrypt, NTRUCipher.

FAST DISTINGUISHING ATTACK ON NTRUCipher + ENCRYPTION SCHEME

The NTRUCipher encryption system was proposed in 2017 as a symmetric version of the encryption scheme NTRUEncrypt, which is currently one of the fastest post-quantum cryptographic algorithms based on lattices in Euclidean space. The purpose of building NTRUCipher is to create a symmetric encryption scheme for practical applications, the security of which, similarly asymmetric, is based on the difficulty of solving only one computational problem. Preliminary exploring of this encryption scheme have been conducted, however the question of NTRUCipher's security against distinguishing attacks aimed at constructing statistical criteria for distinguishing sequences of encrypted messages and purely random sequences.This article shows that the NTRUCipher and even its natural improvement NTRUCipher+ proposed by analogy with the well-known provable secure version of asymmetric NTRU encryption scheme, are vulnerable to distinguishing attacks. Fast distinguishing attack on the NTRUCipher+ and (for a special case) even faster modification of this attack are proposed. Analytical estimates of both attacks' complexity are obtained, from which follows that they have polynomial time complexity and can be implemented in real-time. The obtained results show that other general constructions should be used to build symmetric NRTU-like encryption schemes.

Key words: post-quantum cryptography, lattice-based cryptography, distinguishing attack, discrete Fourier transform, NTRUEncrypt, NTRUCipher.

Олексійчук Антон Миколайович, доктор технічних наук, доцент, професор кафедри Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського».
E-mail: alex-dtn@ukr.net.
Orcid ID: 0000-0003-4385-4631.

Алексейчук Антон Николаевич, доктор технических наук, доцент, профессор кафедры Института специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт имени Игоря Сикорского".

Alekseychuk Anton Nikolaevich, Doctor of Technical Sciences, Assistant professor, Professor of The Institute of Special Communication and Information Protection of National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute".

Матійко Александра Андріївна, викладач кафедри Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».
E-mail: alexm1710@ukr.net.
Orcid ID: 0000-0002-6947-5958.

Матийко Александра Андреевна, преподаватель кафедры Института специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт имени Игоря Сикорского".

Matiyko Aleksandra Andriivna, teacher of Institute of Special Communication and Information Protection National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute".

DOI: 10.18372/2410-7840.22.14982
УДК 004[056.53+413.4]:303.732.46

МЕТОД СИНТЕЗУВАННЯ ПОВЕДІНКИ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Василь Цуркан

Визначено поведінку систем управління інформаційною безпекою через діяльність зі збереження конфіденційності, цілісності та доступності інформації в організаціях. Охарактеризовано її з боку структурних елементів послідовністю дій стосовно поводження з ризиками. Встановлено передумови такої діяльності. Серед них виокремлено визначення зовнішніх і внутрішніх обставин діяльності організацій, потреб і очікувань зацікавлених сторін, сфери та меж застосування систем управління інформаційною безпекою, встановлення критеріїв прийнятності та обирання методу оцінювання ризиків. Зважаючи на це запропоновано синтезування поведінки систем управління інформаційною безпекою за трьома аспектами. Для цього використано діаграми діяльності, послідовності та кінцевого автомату в графічній нотації SysML. Кожною зі зазначених діаграм синтезовано її особливості як окремих структурних елементів, так і систем управління інформаційною безпекою загалом. Діаграмою діяльності специфіковано поведінку через контрольовану послідовність дій. Характерною особливістю такого специфікування є орієнтованість на встановлення умов їх-