CRYPTOLOGY

DOI 10.20535/2411-1031.2020.8.2.222599
УДК 004.056.55

АЛЕКСАНДРА МАТІЙКО

BKW-АТАКА НА ШИФРОСИСТЕМИ NTRUCIPHER ТА NTRUCIPHER+

У зв'язку з появою квантових комп'ютерів, що суттєво зменшить час вирішення певних задач, безпека багатьох стандартизованих криптосистем знаходиться під загрозою. Це стимулювало NIST у 2016 році запустити відкритий конкурс на створення нових постквантових стандартів. Улітку 2020 року алгоритм NTRU – один із найшвидших постквантових алгоритмів, побудований на основі решіток в евклідовому просторі (1996 р.) – увійшов у сімку фіналістів цього конкурсу. Проте лише в 2017 році запропоновано аналог цієї шифросистеми – симетрична шифросистема NTRUCipher. Проведені попередні дослідження цієї шифросистеми, проте не проаналізовано її стійкість відносно природної атаки з підібраним відкритим текстом, яка полягає у складанні системи лінійних рівнянь зі спотвореними правими частинами (над певним скінченним полем простого порядку) та її розв'язанні за допомогою узагальненого алгоритму BKW. В даній статті вперше запропонована шифросистема NTRUCipher+. Її головною відмінністю є використання додаткового випадкового полінома при зашифруванні. Досліджено стійкість шифросистем NTRUCipher та її модифікації NTRUCipher+ відносно BKW-атаки. Подібна атака є можливою саме для симетричних NTRU-подібних шифросистем, проте вона не була розглянута раніше. Отримано аналітичні (верхні та нижні) оцінки складності BKW-атаки на NTRUCipher і NTRUCipher+. Проведено порівняння цих шифросистем за довжиною шифрованих повідомлень відносно BKW-атаки при певних однакових фіксованих параметрах. Показано, що підвищення стійкості шифросистеми NTRUCipher відносно BKW-атаки завдяки використанню додаткового доданку при зашифруванні, майже повністю нівелюється збільшенням верхньої межі ймовірності помилки розшифрування. Проведені дослідження дозволили порівняти ці шифросистеми за стійкістю та практичністю, а також зробити висновок про недоцільність використовувати NTRUCipher+ для підвищення стійкості шифросистеми NTRUCipher відносно BKW-атаки. Надалі планується розробити методи побудови симетричних аналогів криптосистеми NTRU на основі інших загальних конструкцій, що базуються на решітках.

Ключові слова: постквантова криптографія, криптографія на решітках, NTRUCipher, NTRUCipher+, BKW-атака, перетворення Фур'є.

Постановка проблеми. Асиметрична система шифрування NTRUEncrypt запропонована в 1996 р. [1] та є однією з найшвидших постквантових шифросистем. Вона включена до стандарту ANSI X9.98-2010 [2] та є прототипом широкого класу криптосистем з однойменною назвою, стійкість яких базується на складності знаходження коротких векторів в деяких решітках (див., наприклад, [3] - [6]).

Актуальною задачею криптології є створення симетричних шифросистем, стійкість яких, аналогічно асиметричним, базується на складності розв'язання лише однієї конкретної задачі (наприклад, для RSA – це задача факторизації чисел). У зв'язку з цим в 2017 р. на базі NTRUEncrypt створено симетричну шифросистему NTRUCipher [7]. Для неї проведено попередній аналіз стійкості та запропоновано алгоритм вибору параметрів. Обидві шифросистеми мають схожу будову, при цьому в NTRUCipher використовується тільки секретний ключ, що є у два рази коротше секретного ключа шифросистеми NTRUEncrypt. Крім цього, пропонується розглянути шифросистему NTRUCipher+, головною відмінністю

якої є використання додаткового випадкового полінома при зашифруванні, а також дослідити стійкість обох шифросистем відносно специфічної атаки, так званої BKW-атаки, що базується на багатократному зашифруванні однакових повідомлень. Атака полягає у побудові системи лінійних рівнянь зі спотвореними правими частинами відносно невідомого ключа шифросистеми та в розв'язанні цієї системи рівнянь алгоритмом BKW [8], [9]. Отримані результати дозволяють оцінювати стійкість зазначених шифросистем відносно атаки на основі багатократного зашифрування однакових повідомлень та обирати параметри шифросистем, що забезпечують їх належну стійкість.

Аналіз останніх досліджень і публікацій. За останні роки проведено дослідження у галузі квантових комп'ютерів, які використовують квантово-механічні явища для вирішення математичних задач, складних або практично нерозв'язних для звичайних комп'ютерів. Оскільки побудова квантових комп'ютерів є лише питанням часу, це загрожує конфіденційності та цілісності цифрових комунікацій. Це стало поштовхом для оголошення відкритого конкурсу зі стандартизації постквантових криптопримітивів в 2016 році. Майже третина усіх постквантових криптографічних алгоритмів, представлених на цьому конкурсі, належить до NTRU-подібних (або близьких до них, типу LWE) криптосистем (див. [10], [11]).

NTRU є криптосистемою з відкритим ключем, що будується на базі решіток та утворює провідну альтернативу RSA та криптосистемам на еліптичних кривих завдяки своїй більш високій продуктивності та стійкості до квантових атак. Асиметрична система шифрування NTRU запропонована в 1996 р. [1] і є першим представником широкого класу криптосистем з однойменною назвою, стійкість яких заснована на складності знаходження коротких векторів в деяких решітках [3] - [6].

Криптосистему NTRUCipher запропоновано як симетричний аналог семантично стійкої асиметричної шифросистеми NTRUEncrypt [6], [7]. Для NTRUCipher проведено попередній аналіз стійкості та запропоновано алгоритм вибору параметрів [7]. Варто зауважити, що в оригінальній роботі містяться суттєві помилки у доведенні CPA-стійкості криптосистеми; крім того, відсутнє порівняння шифросистем NTRUEncrypt та NTRUCipher за стійкістю та практичністю. Порівняльний аналіз цих шифросистем, а також виправлення помилок у доведенні CPA-стійкості NTRUCipher зроблено в [12]. Встановлено, що верхня межа ймовірності помилкового розшифрування повідомлень у шифросистемі NTRUCipher на декілька порядків нижче, ніж у шифросистемі NTRUEncrypt. Показано, що NTRUCipher є CPA-стійкою за більш слабких умов порівняно з її асиметричним аналогом NTRUEncrypt.

Нині за проведених досліджень залишається питання про стійкість шифросистеми NTRUCipher до певних специфічних атак. Варто зауважити, що симетричний характер NTRUCipher надає можливість проводити атаки з підібраним відкритим текстом, які не можуть бути реалізовані на асиметричні шифросистеми. При проведенні цих атак відбувається багатократне зашифрування однакових повідомлень на фіксованому невідомому секретному ключі, в результаті чого будується система лінійних рівнянь зі спотвореними правими частинами, яку необхідно розв'язати. Водночас, розв'язання таких систем рівнянь є відомою задачею LPN. Найефективнішими на цей час алгоритмами розв'язання класичної задачі LPN (над полем з двох елементів) є алгоритм BKW [8], який має субекспоненційну часову складність. У [9] наведено природне узагальнення цього алгоритму на випадок довільного скінченного поля та отримано оцінки часової складності узагальненого алгоритму BKW.

Метою статті є порівняння шифросистем NTRUCipher і NTRUCipher+ за стійкістю та практичністю на основі аналітичних оцінок складності реалізації BKW-атаки.

Виклад основного матеріалу дослідження. 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 Z_q кільце класів лишків за модулем q, елементи якого ототожнимо з цілими числами, що належать інтервалу

$[-(q-1)/2,(q-1)/2]$. Позначимо $R_{n,q}=\mathrm{Z}_q[x]/(x^n-1)$ кільце зрізаних поліномів степеня не вище $n-1$ над кільцем Z_q. Зазначене кільце складається з q^n поліномів вигляду $u=u_0+u_1x+\cdots+u_{n-1}x^{n-1}$, де $u_i\in\mathrm{Z}_q$, $i\in\overline{0,n-1}$, які додаються та перемножуються за модулем полінома x^n-1. Позначимо $R^*_{n,q}$ групу оборотних елементів кільця $R_{n,q}$.

Для будь-якого $u=u_0+u_1x+\cdots+u_{n-1}x^{n-1}\in\mathrm{Z}[x]$ 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 $\|u\|_\infty=1$, $i\in\overline{0,n-1}$.

Позначимо символом S множину всіх малих поліномів степеня не вище $n-1$, а символом S_d множину всіх поліномів $u\in S$, серед коефіцієнтів 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. [13]).

Для зашифрування повідомлення $m\in S$ на ключі F генеруються незалежні випадкові поліноми r та $e=e_0+e_1x+\cdots+e_{n-1}x^{n-1}$, 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

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

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

$$D_f(c)=cf \pmod q \bmod 3, \tag{2}$$

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

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

Отже, за умови

$$d<(q-14)/48 \tag{3}$$

розшифрування отриманих повідомлень відбувається коректно.

Зауважимо, що головною відмінністю шифросистеми NTRUCipher+ від NTRUCipher є використання додаткового випадкового полінома e при зашифруванні (для NTRUCipher доданок e у (1) дорівнює нулю) [7]. Використовувати такий доданок в одній з асиметричних версій криптосистеми NTRU запропоновано в [6] для забезпечення семантичної стійкості криптосистеми.

BKW-атака на шифросистеми NTRUCipher+ та NTRUCipher. Отримаємо оцінку стійкості шифросистеми NTRUCipher+ відносно атаки, при проведенні якої супротивник зашифровує N разів на тому ж самому (невідомому) ключі F відкрите повідомлення $m=0$.

У результаті супротивник отримає систему рівнянь (СР) над кільцем $R_{n,q}$: $3(r^{(i)}f^{-1}+e^{(i)})=c^{(i)}$, $i\in\overline{1,N}$, де $c^{(1)},\dots,c^{(N)}$ – шифровані повідомлення, $r^{(1)},\dots,r^{(N)}$, $e^{(1)},\dots,e^{(N)}$ – незалежні випадкові поліноми, що використовуються при зашифруванні (див. (1)). Цю систему рівнянь можна записати у вигляді

$$3^{-1}c^{(i)}=-c^{(i)}F+(r^{(i)}+e^{(i)}f),\ i\in\overline{1,N},$$

де 3^{-1} є оберненим до 3 елементом поля Z_q. Позначаючи $c^{(i)}=\sum_{j=0}^{n-1}c_{i,j}x^j$, $e^{(i)}=\sum_{j=0}^{n-1}e_{i,j}x^j$, $r^{(i)}=\sum_{j=0}^{n-1}r_{i,j}x^j$ та прирівнюючи вільні члени поліномів у обох частинах наведеної СР, отримаємо таку систему рівнянь зі спотвореними правими частинами відносно коефіцієнтів $F_0,F_1,\dots,F_{n-1}$ невідомого полінома F:

$$3^{-1}c_{i,0}=-\sum_{j=0}^{n-1}c_{i,n-j}F_j+(r_{i,0}+e_{i,0}(1+3F_0)+3\sum_{j=1}^{n-1}e_{i,n-j}F_j),\ i\in\overline{1,N}. \quad (4)$$

Для отримання оцінки складності розв'язання (4) за допомогою одного з найбільш ефективних нині алгоритмів (а саме, узагальненого алгоритму BKW [8], [9]) скористаємося таким твердженням.

Твердження 1 [9]. Нехай n_1 – натуральне число, $1\le n_1\le n-3$, $\delta\in(0,1)$,

$$u=\left\lceil\frac{\log(n-n_1)}{2}\right\rceil,\ v=\left\lceil\frac{2(n-n_1)}{\log(n-n_1)}\right\rceil,$$

$$k=2^{u-1},\ l=(u+\left\lceil\ln(2t\delta^{-1})\right\rceil-1)q^v,$$

$$N(n_1)=lt, \quad (5)$$

де

$$t=\frac{(1-\delta/2)n_1\log 3+\delta/2\log\delta/2+(1-\delta/2)\log(1-\delta/2)}{\Delta(p^{(k)})},$$

$$\Delta(p^{(k)})=q^{-1}\sum_{z\in\mathrm{Z}_q}(qp^{(k)}(z)-1)^2, \quad (6)$$

$p^{(k)}=(p^{(k)}(z):z\in\mathrm{Z}_q)$ – розподіл імовірностей випадкової величини $\eta_k=\xi_1+\dots+\xi_{k/2}-(\xi_{k/2+1}+\dots+\xi_k)$, де $\xi_1,\dots,\xi_{k/2},\xi_{k/2+1},\dots,\xi_k$ – незалежні випадкові величини, розподілені за тим самим законом, що й спотворення $r_{i,0}+e_{i,0}(1+3F_0)+3\sum_{j=1}^{n-1}e_{i,n-j}F_j$ у правій частині (4). Тоді, для відновлення з цієї СР за допомогою узагальненого алгоритму BKW довільних n_1 коефіцієнтів шуканого полінома F з імовірністю не менше ніж $1-\delta$ необхідно виконати принаймні

$$T(n_1)=2n_1t3^{n_1}+ult \quad (7)$$

операцій над n-вимірними векторами над полем Z_q.

Для того, щоб скористатися твердженням 1, доведемо наступне твердження, яке встановлює аналітичний вираз параметра (6).

Твердження 2. Справедлива рівність

$$\Delta(p^{(k)})=\sum_{\alpha\in\mathrm{Z}_q\setminus\{0\}}|\pi(\alpha)|^{2k}, \quad (8)$$

де

$$\pi(\alpha)=\begin{cases}\theta(dn^{-1},\alpha)\theta(1/3,\alpha)\theta(1/3,3\alpha)^{2d}, \text{ якщо } F_0=0;\\ \theta(dn^{-1},\alpha)\theta(1/3,2\alpha)\theta(1/3,3\alpha)^{2d-1}, \text{ якщо } F_0=1;\\ \theta(dn^{-1},\alpha)\theta(1/3,4\alpha)\theta(1/3,3\alpha)^{2d-1}, \text{ якщо } F_0=-1,\end{cases} \quad (9)$$

і для будь-яких $p\in[0,1]$, $x\in \mathrm{Z}_q$

$$\theta(p,x)=1-2p\left(1-\cos\left(\frac{2\pi x}{q}\right)\right).$$

Доведення. Позначимо $\omega=\exp\{2\pi i q^{-1}\}$, де $i^2=-1$ та розглянемо перетворення Фур'є $\hat{p}^{(k)}(\alpha)=\sum\limits_{z\in \mathrm{Z}_q} p^{(k)}(z)\omega^{-\alpha z}$ розподілу ймовірностей випадкової величини $\eta_k=\xi_1+\cdots+\xi_{k/2}-(\xi_{k/2+1}+\cdots+\xi_k)$. З формули (6) та рівності Парсеваля (див., наприклад, [14]) випливає, що

$$\Delta(p^{(k)})=\sum_{\alpha\in \mathrm{Z}_q\setminus\{0\}}|\hat{p}^{(k)}(\alpha)|^2.$$

При цьому за теоремою про згортку [14]

$$\hat{p}^{(k)}(\alpha)=\pi(\alpha)^{k/2}\,\overline{\pi(\alpha)}^{\,k/2}=|\pi(\alpha)|^k,$$

де $\pi(\alpha)=\sum\limits_{z\in \mathrm{Z}_q} p_{\xi_1}(z)\omega^{-\alpha z}$ є перетворенням Фур'є розподілу випадкової величини ξ_1;

$\overline{\pi(\alpha)}$ позначає комплексно спряжене число до $\pi(\alpha)$, $\alpha\in \mathrm{Z}_q$.

Отже, для завершення доведення залишається переконатися в тому, що перетворення Фур'є випадкової величини ξ_1 має вигляд (9).

З формули $\xi_1=r_{i,0}+e_{i,0}(1+3F_0)+3\sum\limits_{j=1}^{n-1}e_{i,n-j}F_j$ та умови $F\in S_d$ випливає, що випадкова величина ξ_1 має той самий закон розподілу, що і сума

$$\zeta_0=r_0+e_0+3\sum_{j=1}^{2d}e_j, \text{ якщо } F_0=0; \quad (10)$$

$$\zeta_1=r_0+4e_0+3\sum_{j=1}^{2d-1}e_j, \text{ якщо } F_0=1; \quad (11)$$

$$\zeta_{-1}=r_0-2e_0+3\sum_{j=1}^{2d-1}e_j, \text{ якщо } F_0=-1, \quad (12)$$

де r_0, e_j – незалежні випадкові величини, розподілені за законами

$$\mathrm{P}(r_0=1)=\mathrm{P}(r_0=-1)=dn^{-1},\ \mathrm{P}(r_0=0)=1-2dn^{-1}, \quad (13)$$
$$\mathrm{P}(e_j=1)=\mathrm{P}(e_j=-1)=\mathrm{P}(e_j=0)=1/3,\ j\in\overline{0,2d}.$$

Далі, перетворення Фур'є випадкової величини r_0 дорівнює

$$\hat{r}_0(\alpha)=\sum_{z\in \mathrm{Z}_q}\mathrm{P}(r_0=z)\omega^{-\alpha z}=\mathrm{P}(r_0=0)+\mathrm{P}(r_0=1)\omega^{-\alpha}+\mathrm{P}(r_0=-1)\omega^{\alpha}=$$

$$=1-2dn^{-1}+dn^{-1}(\omega^{-\alpha}+\omega^{\alpha})=1-2dn^{-1}\left(1-\cos\left(\frac{2\pi\alpha}{q}\right)\right)=\theta(dn^{-1},\alpha),\ \alpha\in \mathrm{Z}_q, \quad (14)$$

і для будь-якого $c\in \mathrm{Z}_q\setminus\{0\}$ перетворення Фур'є випадкової величини ce_j дорівнює

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

Звідси на основі теореми про згортку та формулах (10) - (12) безпосередньо випливає, що перетворення Фур'є випадкової величини ξ_1 визначається за (9). Твердження доведено.

Описана BKW-атака є застосовною і до криптосистеми NTRUCipher: достатньо побудувати та розв'язати (4), вважаючи $e_{i,0}=...=e_{i,n-1}=0$, $i\in\overline{1,N}$. Складність розв'язання цієї СР у зазначеному випадку можна оцінити за допомогою твердження, яке доводиться аналогічно двом попереднім.

Твердження 3. Нехай у (4) $e_{i,0}=...=e_{i,n-1}=0$, $i\in\overline{1,N}$, причому кількість рівнянь у системі дорівнює

$$N_0=lt_0, \tag{15}$$

де параметри l, u,v,k, δ, n_1 визначаються за аналогією з формулюванням твердження 3,

$$t_0=\frac{2n_1\ln(6\delta^{-1})(\log p_{\max}^{(k)}-\log p_{\min}^{(k)})^2}{(D(p^{(k)}\,\|\,\omega)+D(\omega\|\,p^{(k)}))^2},$$

$$p_{\max}^{(k)}=\max_{z\in Z_q}p^{(k)}(z),\ p_{\min}^{(k)}=\min_{z\in\{Z_q:p^{(k)}(z)\neq 0\}}p^{(k)}(z),$$

$$D(p^{(k)}\,\|\,\omega)=\sum_{z\in\{Z_q:p^{(k)}(z)\neq 0\}}p^{(k)}(z)\log qp^{(k)}(z),\ D(\omega\|\,p)=-q^{-1}\sum_{z\in\{Z_q:p^{(k)}(z)\neq 0\}}\log qp^{(k)}(z),$$

а $p^{(k)}=(p^{(k)}(z):z\in Z_q)$ – розподіл імовірностей випадкової величини $\eta_k=\xi_1+\cdots+\xi_{k/2}-$ $-(\xi_{k/2+1}+\cdots+\xi_k)$, де $\xi_1,...,\xi_{k/2},\xi_{k/2+1},...,\xi_k$ – незалежні випадкові величини, розподілені за (13). Тоді для відновлення з (4) за допомогою узагальненого алгоритму BKW довільних n_1 коефіцієнтів шуканого полінома F з імовірністю не менше ніж $1-\delta$ достатньо виконати

$$T_0=2n_1t_0 3^{n_1}+ult_0 \tag{16}$$

операцій над n-вимірними векторами над полем Z_q.

При проведенні чисельних розрахунків за (15), (16) можна скористатися такою формулою, що випливає з теореми про згортку, рівності (14) та формули для оберненого перетворення Фур'є:

$$p^{(k)}(z)=q^{-1}\sum_{\alpha\in Z_q}\cos\left(\frac{2\pi\alpha z}{q}\right)|\theta(dn^{-1},\alpha)|^k\quad z\in Z_q.$$

Зауважимо, що твердження 1, 2 надають нижню оцінку трудомісткості BKW-атаки на шифросистему NTRUCipher+, в той час як твердження 3 – верхню оцінку трудомісткості цієї атаки на шифросистему NTRUCipher. Для отримання нижньої оцінки трудомісткості BKW-атаки на NTRUCipher можна використовувати твердження 1, 2, вважаючи у формулі (9) $\pi(\alpha)=\theta(dn^{-1},\alpha)$.

Для низки значень n,d,q в табл. 1 наведені чисельні оцінки трудомісткості BKW-атаки на шифросистему NTRUCipher+. Символом $n_{1,\min}$ позначено значення параметра n_1, для якого досягається мінімум значень (7). В табл. 2 наведені чисельні (верхня та нижня) оцінки трудомісткості BKW-атаки на шифросистему NTRUCipher, а також верхня оцінка трудомісткості тривіальної атаки, яка полягає у розв'язанні (4) (при $e_{i,0}=...=e_{i,n-1}=0$, $i\in\overline{1,N}$) методом максимуму правдоподібності.

Для обчислення останньої використано формулу, що випливає з результатів [9]:

$$\log T_{\text{ММР}} = \log\left(\binom{n}{d}\binom{n-d}{d}\right) + \log(t_{\text{ММР}} n) + 1,$$

де $t_{\text{ММР}}$ обчислюється за такою ж формулою, що й t_0 (див. твердження 3), в якій треба покласти $k = 1, n_1 = n$ та замінити 6 на 3:

$$t_{\text{ММР}} = \frac{2n\ln(3\delta^{-1})(\log p_{\max}^{(1)} - \log p_{\min}^{(1)})^2}{(D(p^{(1)} \| \omega) + D(\omega \| p^{(1)}))^2}.$$

Символом $n_{1,\min}$ в табл. 2 позначено значення параметра n_1, для якого досягається мінімум значень (16). Нарешті, для обчислення значень $\log T(n_{1,\min})$ та $\log N(n_{1,\min})$ у табл. 2 використано (7) та (5) відповідно, при застосуванні яких параметр $\pi(\alpha)$ у формулі (8) вважається рівним $\theta(dn^{-1}, \alpha)$ (див. твердження 3).

Таблиця 1 – Оцінки ефективності BKW-атаки на шифросистему NTRUCipher+ ($\delta = 0{,}01$)

(n, d)	q	$n_{1,\min}$	$\log T(n_{1,\min})$ (формула (7))	$\log N(n_{1,\min})$ (формула (5))
(401, 113)	4871	276	455,83	452,23
	5237	277	457,26	453,17
	5701	278	458,84	454,69
	6763	280	461,98	457,61
	7499	281	463,71	459,88
	8161	282	465,23	461,15
	8681	282	466,56	464,22
	9439	283	467,86	465,37
(449,134)	4877	306	504,64	502,15
	5701	308	507,98	505,57
	6577	310	510,73	508,05
	7681	312	513,79	511,01
	8167	313	514,92	511,51
	8837	314	516,46	512,93
	9463	315	517,85	513,73
(677, 157)	4831	448	730,95	728,39
	5867	452	737,04	734,33
	6703	455	741,05	737,43
	7417	457	744,15	740,38
	8059	458	746,93	744,43
	8677	460	748,87	744,95
	9461	461	751,67	749,16
(1091,120)	4831	700	1130,31	1125,49
	5867	706	1140,15	1136,42
	6659	710	1146,56	1142,95
	7537	714	1152,77	1148,83
	8237	717	1157,30	1152,53
	8779	719	1160,45	1155,48
	9439	721	1163,76	1159,46
	4871	748	1206,63	1202,07
	5927	755	1217,67	1212,72
	6733	759	1224,34	1220,55

Продовження таблиці 1

	7561	763	1230,58	1226,53
	8243	766	1235,22	1230,75
	8807	768	1238,57	1234,63
	9241	769	1241,26	1238,56
(443, 143)	4861	303	498,59	493,74
	5981	305	502,64	499,86
	6781	307	505,15	501,19
	7681	308	507,72	505,18
	8387	309	509,51	507,09
	8821	310	510,19	506,90
	9377	311	511,46	507,25
(743, 247)	4817	489	795,17	791,51
	5903	493	802,48	799,86
	6959	497	807,88	804,25
	7681	499	811,17	807,75
	8387	501	814,11	810,18
	8831	502	815,77	812,02
	9371	503	817,69	814,51

Таблиця 2 – Оцінки ефективності атак на шифросистему NTRUCipher $(\delta = 0{,}01)$

(n, d)	q	$n_{1,\min}$	$\log T_0(n_{1,\min})$ (формула (16))	$\log N_0(n_{1,\min})$ (формула (15))	$\log T(n_{1,\min})$ (формула (7))	$\log N(n_{1,\min})$ (формула (5))	$\log T_{\text{ММР}}$
(401, 113)	1543	261	437,46	434,11	431,94	428,46	637,29
	1663	262	439,98	436,79	433,62	430,21	637,41
	1811	263	442,57	439,81	435,55	432,69	637,46
	2141	266	446,51	441,76	439,47	437,11	637,18
	2383	267	447,09	443,72	441,50	438,01	637,33
	2591	268	450,27	447,17	443,25	440,03	637,22
	2753	269	450,41	446,74	444,57	440,76	637,17
	2999	270	452,46	449,09	446,28	442,78	637,38
(449,134)	1553	290	483,98	479,82	477,95	473,63	719,89
	1811	292	487,74	484,74	481,64	478,52	719,95
	2087	294	491,06	488,43	485,20	482,49	719,87
	2437	297	495,65	491,32	489,07	484,58	719,79
	2591	298	496,36	491,70	490,61	485,79	719,96
	2803	299	498,53	494,38	492,29	487,99	719,81
	3001	300	500,24	496,04	493,88	489,52	719,94
(677, 157)	1531	423	693,84	690,06	689,99	686,07	1004,45
	1861	427	702,01	699,53	697,59	695,06	1004,22
	2129	431	706,95	702,66	702,58	698,16	1004,30
	2375	433	710,52	707,54	706,38	703,31	1004,39
	2557	435	713,41	709,65	709,09	705,19	1004,32
	2753	436	716,29	713,82	711,89	709,35	1004,28
	2999	438	718,80	716,19	714,79	712,11	1004,30
(1091,120)	1543	658	1065,75	1062,75	1064,34	1061,26	1086,78
	1861	665	1078,10	1075,51	1076,13	1073,48	1086,56
	2113	670	1085,59	1082,79	1083,67	1080,00	1086,54
	2393	675	1092,93	1089,48	1090,97	1087,40	1086,73
	2617	678	1098,17	1095,25	1096,21	1093,22	1086,74
	2789	681	1102,07	1097,48	1100,09	1095,35	1086,80
	2999	683	1105,28	1102,21	1103,98	1100,82	1086,66

Продовження таблиці 2

(1171, 106)	1549	703	1137,13	1133,89	1135,63	1132,29	1028,61
	1879	711	1148,97	1145,87	1148,46	1145,27	1028,93
	2137	716	1158,48	1155,74	1156,91	1154,11	1028,67
	2399	721	1165,19	1161,83	1164,14	1160,67	1028,92
	2617	724	1171,38	1168,71	1169,75	1167,02	1028,76
	2801	727	1175,42	1172,19	1173,77	1170,46	1028,70
	2939	729	1177,43	1173,89	1176,74	1173,08	1028,71
(443, 143)	1543	286	477,34	474,10	471,91	468,55	716,62
	1901	289	483,97	481,26	477,12	474,32	716,66
	2153	291	486,13	483,19	480,09	477,05	716,72
	2437	293	489,29	485,98	483,02	479,58	716,51
	2663	294	491,04	488,37	485,13	482,38	716,58
	2801	295	492,35	489,08	486,24	482,85	716,64
	2971	296	493,86	490,15	487,64	483,78	716,59
(743, 247)	1531	461	757,05	753,26	750,47	746,53	1193,69
	1877	466	765,42	762,47	758,95	755,91	1193,53
	2207	470	772,58	769,88	765,63	762,86	1193,61
	2437	473	776,79	773,01	769,57	765,66	1193,55
	2663	475	779,72	776,43	772,99	769,59	1193,43
	2801	476	782,23	779,41	775,00	772,10	1193,46
	2969	478	784,05	779,79	777,38	772,97	1193,49

Як видно з табл. 1 і 2, при фіксованих значеннях n, d зі збільшенням q трудомісткість BKW-атаки на кожну шифросистему повільно зростає. Зокрема, при $(n, d) = (1171, 106)$ нижня оцінка трудомісткості BKW-атаки на NTRUCipher змінюється від 2^{1135} до 2^{1176} операцій, в той час як нижня оцінка трудомісткості цієї атаки на NTRUCipher+ змінюється від 2^{1206} до 2^{1241} операцій (в залежності від значення q, яке для криптосистеми NTRUCipher+ є майже у 3 рази більше). Крім того, для n, d і q, зазначених в табл. 1 і 2, трудомісткість BKW-атаки на NTRUCipher+ є від 2^{15} до 2^{69} разів більше, ніж для NTRUCipher (при цьому обидві шифросистеми характеризуються майже однаковими верхніми межами ймовірності помилки розшифрування). Нарешті, як видно з табл. 2, для кожної пари (n, d), за винятком (1091,120) та (1171, 106), складність BKW-атаки на NTRUCipher є на декілька порядків нижче, ніж складність тривіальної атаки. Поряд з тим, BKW-атака потребує набагато більшої кількості рівнянь (див. значення $\log N_0(n_{1,\min})$ в табл. 2) в порівнянні з тривіальною атакою.

У табл. 3 наведено результати порівняння шифросистем NTRUCipher та NTRUCipher+ за довжиною шифрованих повідомлень при заданій множині ключів (параметрах n і d), заданому рівні стійкості L відносно BKW-атаки та заданій верхній межі ймовірністю помилки розшифрування.

Для шифросистеми NTRUCipher+ символом $q_{\min}$ в табл. 3 позначено найменше просте число q (що є примітивним елементом за модулем n), для якого нижня межа $T(q_{\min})$ складності BKW-атаки на шифросистему (згідно з твердженням 2) є не менше ніж 2^L операцій, і верхня межа p_{er} ймовірності помилки розшифрування є не більше ніж 2^{-80}. В табл. 3 наведені також фактичні значення двійкових логарифмів параметрів $T(q_{\min})$ і p_{er} та відповідні значення довжини шифрованих повідомлень $n \log q_{\min}$. Для шифросистеми NTRUCipher параметри в табл. 3 мають той самий сенс.

Як видно з табл. 3, при заданих нижній межі стійкості та верхній межі ймовірності помилкового розшифрування шифровані повідомлення у шифросистемі NTRUCipher+ мають більшу довжину в порівнянні із системою NTRUCipher. Виключення спостерігаються лише для трійок $(n, d, L) = (449, 134, 512)$ та $(n, d, L) = (443, 143, 512)$, коли ці довжини майже

співпадають. Такий ефект пояснюється необхідністю збільшення значення $q_{\min}$ у шифросистемі NTRUCipher+ в порівнянні з NTRUCipher для забезпечення належної малості ймовірності помилки розшифрування. Підвищення стійкості шифросистеми NTRUCipher відносно BKW-атаки завдяки використанню додаткового доданку e в формулі (1), що збільшує рівень спотворень у правих частинах рівнянь системи (4), майже повністю нівелюється збільшенням верхньої межі ймовірності помилки розшифрування. Це призводить до негативного впливу на практичність шифросистеми NTRUCipher+ у порівнянні з NTRUCipher.

Таблиця 3 – Оцінки практичності шифросистем NTRUCipher та NTRUCipher+ $(\delta = 0{,}01)$

(n, d)	L	NTRUCipher				NTRUCipher +			
		$q_{\min}$	$\log T(q_{\min})$	$-\log p_{er}$	$n \log q_{\min}$	$q_{\min}$	$\log T(q_{\min})$	$-\log p_{er}$	$n \log q_{\min}$
(401, 113)	256	1019	422,20	80,58	4007,17	3191	447,70	80,14	4667,56
(449, 134)	256	1109	468,88	80,48	4541,65	3517	497,36	82,22	5289,28
	512	7079	512,14	3714,55	5742,41	7039	512,01	359,66	5738,74
(677, 157)	256, 512	1201	680,39	80,13	6925,72	3793	722,96	80,99	8048,94
(1091, 120)	512, 1024	1087	1041,70	85,71	11003,97	3313	1109,79	80,07	12758,07
(1171, 106)	512, 1024	1039	1108,06	85,91	11710	3119	1180,44	80,24	13591,64
(443, 143)	256	1163	464,70	83,35	4511,35	3613	492,26	81,23	5235,81
	512	9697	512,02	6544,38	5866,79	9697	512,02	647,69	5866,79
(743, 247)	256, 512	1531	750,47	83,36	7861,13	4751	794,88	80,69	9075,01

Висновки. Досліджено стійкість шифросистем NTRUCipher та NTRUCipher+ відносно природної атаки з підібраним відкритим текстом, яка полягає у складанні системи лінійних рівнянь зі спотвореними правими частинами (над певним скінченним полем простого порядку) та її розв'язанні за допомогою узагальненого алгоритму BKW. Подібна атака є можливою саме для симетричних NTRU-подібних шифросистем, проте вона не розглядається в [7], де запропоновано шифросистему NTRUCipher. Отримано аналітичні оцінки складності зазначеної BKW-атаки на NTRUCipher і NTRUCipher+ відповідно, що дозволяє порівняти ці шифросистеми за стійкістю та практичністю.

При фіксованих значеннях n, d зі збільшенням q трудомісткість BKW-атаки на кожну із зазначених шифросистем повільно зростає. Зокрема, при $(n, d) = (1171, 106)$ нижня оцінка трудомісткості BKW-атаки на NTRUCipher змінюється від 2^{1135} до 2^{1176} операцій, в той час як нижня оцінка трудомісткості цієї атаки на NTRUCipher+ змінюється від 2^{1206} до 2^{1241} операцій (в залежності від значення q, яке для криптосистеми NTRUCipher+ є майже у 3 рази більше). Крім того, трудомісткість BKW-атаки на NTRUCipher+ є від 2^{15} до 2^{69} разів більше, ніж для NTRUCipher (при цьому обидві шифросистеми характеризуються майже однаковими верхніми межами ймовірності помилки розшифрування).

Підвищення стійкості шифросистеми NTRUCipher відносно BKW-атаки за рахунок використання додаткового доданку e у (1), що збільшує рівень спотворень у правих частинах рівнянь (4), майже повністю нівелюється збільшенням верхньої межі ймовірності помилки розшифрування. Це призводить до негативного впливу на практичність шифросистеми NTRUCipher+ в порівнянні з NTRUCipher (див. табл. 3) та свідчить про недоцільність використовувати NTRUCipher+ для підвищення стійкості шифросистеми NTRUCipher відносно BKW-атаки.

У перспективах подальших досліджень планується розробити методи побудови симетричних аналогів криптосистеми NTRU на основі інших загальних конструкцій, що базуються на решітках.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] J. Hoffstein, J. Pipher, and J. Silverman, "NTRU: a new high speed public key cryptosystem". [Online]. Available: https://web.securityinnovation.com/hubfs/files/ntru-orig.pdf. Accessed on: Sept. 07, 2020.

[2] American national standards institute. (2010, Oct. 15; reafiirmed 2017, Febr. 2). *ANSI X9.98-2010. Lattice-based polynomial public key encryption algorithm for the Financial Services Industry*. [Online]. Available: https://webstore.ansi.org/preview-pages/ASCX9/preview_ANSI+X9.98-2010+(R2017).pdf. Accessed on: Sept. 07, 2020.

[3] R. Steinfeld, "NTRU cryptosystem: recent developments and emerging mathematical problems in finite polynomial rings", *Algebraic Curves and Finite Fields: Cryptography and Other Applications*, pp. 179-211, 2014, doi: 10.1515/9783110317916.179.

[4] D. J. Bernstein, Ch. Chuengsatiansup, T. Lange, and Ch. van Vredendaal, "NTRU Prime: reducing attack surface at low cost", in *Proc. International Conference on Selected Areas in Cryptography*, Ottawa, 2017, pp. 235-260, doi: 10.1007/978-3-319-72565-9_12.

[5] P. Hirschhorn, J. Hoffstein, N. Howgrave-Graham, and W. Whyte, "Choosing NTRU parameters in light of combined lattice reduction and MITM approaches", *Applied Cryptography and Network Security*, vol. 5536, pp. 437-455, 2009, doi: 10.1007/978-3-642-01957-9_27.

[6] D. Stehle', and R. Steinfeld, "Making NTRU as secure as worst-case problems over ideal lattices", in *Proc. International Conference on Advances in Cryptology*, Tallin, 2011, pp. 27-47, doi: 10.1007/978-3-642-20465-4_4.

[7] M. R. Valluri, "NTRUCipher-lattice based secret key encryption", in *World Congress on Internet Security*. [Online]. Available: https://arxiv.org/abs/1710.01928. Accessed on: Sept. 07, 2020.

[8] A. Blum, A. Kalai, and H. Wasserman, "Noise-tolerant learning, the parity problem, and the statistical query model", *Journal of the ACM*, vol. 50, no. 3, pp. 506-519, 2003, doi: 10.1145/792538.792543.

[9] А. М. Олексійчук, С. М. Ігнатенко, та М. В. Поремський, "Системи лінійних рівнянь зі спотвореними правими частинами над скінченними кільцями", *Математичне та комп'ютерне моделювання. Серія: Технічні науки*, вип. 15, с. 150-155, 2017, doi: 10.32626/2308-5916.2017-15.150-155.

[10] M. R. Albrecht at al., "Estimate all the {LWE, NTRU} schemes!", in *Proc. International Conference on Security and Cryptography for Networks*, Amalfi, 2018, pp. 351-367, doi: 10.1007/978-3-319-98113-0_19.

[11] S. Diop, D. O. Sane', M. Seck, and N. Diarra, "NTRU-LPR IND-CPA: a new ideal lattice-based scheme", *Cryptology ePrint Archive, Report 2018/109*. [Online]. Available: http://eprint.iacr.org/2018/109. Accessed on: Sept. 07, 2020, doi: 10.13140/RG.2.2.15424. 35840.

[12] А. А. Матійко "Порівняльний аналіз алгоритмів шифрування NTRUEncrypt та NTRUCipher", *Математичне та комп'ютерне моделювання. Серія: Технічні науки*, вип. 19, с. 81-87, 2019, doi: 10.32626/2308-5916.2019-19.81-87.

[13] А. Н. Алексейчук, А. А. Матийко, "Оценки вероятности обратимости случайных многочленов, используемых в модифицированной версии криптосистемы NTRU", *Радіотехніка*, вип. 189, с. 38-46, 2017.

[14] L Babai, "The Fourier transform and equations over finite abelian groups". [Online]. Available: *http://people.cs.uchicago.edu/~laci /ren/fourier.pdf*. Accessed on: Sept. 07, 2020.

Стаття надійшла до редакції 17.09.2020.

REFERENCES

[1] J. Hoffstein, J. Pipher, and J. Silverman, "NTRU: a new high speed public key cryptosystem". [Online]. Available: https://web.securityinnovation.com/hubfs/files/ntru-orig.pdf. Accessed on: Sept. 07, 2020.

[2] American national standards institute. (2010, Oct. 15; reafiirmed 2017, Febr. 2). *ANSI X9.98-2010. Lattice-based polynomial public key encryption algorithm for the Financial Services Industry*. [Online]. Available: https://webstore.ansi.org/preview-pages/ASCX9/preview_ANSI+ X9.98-2010+(R2017).pdf. Accessed on: Sept. 07, 2020.

[3] R. Steinfeld, "NTRU cryptosystem: recent developments and emerging mathematical problems in finite polynomial rings", *Algebraic Curves and Finite Fields: Cryptography and Other Applications*, pp. 179-211, 2014, doi: 10.1515/9783110317916.179.

[4] D. J. Bernstein, Ch. Chuengsatiansup, T. Lange, and Ch. van Vredendaal, "NTRU Prime: reducing attack surface at low cost", in *Proc. International Conference on Selected Areas in Cryptography*, Ottawa, 2017, pp. 235-260, doi: 10.1007/978-3-319-72565-9_12.

[5] P. Hirschhorn, J. Hoffstein, N. Howgrave-Graham, and W. Whyte, "Choosing NTRU parameters in light of combined lattice reduction and MITM approaches", *Applied Cryptography and Network Security*, vol. 5536, pp. 437-455, 2009, doi: 10.1007/978-3-642-01957-9_27.

[6] D. Stehle', and R. Steinfeld, "Making NTRU as secure as worst-case problems over ideal lattices", in *Proc. International Conference on Advances in Cryptology*, Tallin, 2011, pp. 27-47, doi: 10.1007/978-3-642-20465-4_4.

[7] M. R. Valluri, "NTRUCipher-lattice based secret key encryption", in *World Congress on Internet Security*. [Online]. Available: https://arxiv.org/abs/1710.01928. Accessed on: Sept. 07, 2020.

[8] A. Blum, A. Kalai, and H. Wasserman, "Noise-tolerant learning, the parity problem, and the statistical query model", *Journal of the ACM*, vol. 50, no. 3, pp. 506-519, 2003, doi: 10.1145/792538.792543.

[9] A. N. Alekseychuk, S. M. Ignatenko, and M. V. Poremskyi, "Systems of linear equations corrupted by noise over arbitrary finite rings," *Mathematical and Computer Modelling, Series: Technical science*, iss. 15, pp. 150-155, 2017, doi: 10.32626/ 2308-5916.2017-15.150-155.

[10] M. R. Albrecht at al., "Estimate all the {LWE, NTRU} schemes!", in *Proc. International Conference on Security and Cryptography for Networks*, Amalfi, 2018, pp. 351-367, doi: 10.1007/978-3-319-98113-0_19.

[11] S. Diop, D. O. Sane', M. Seck, and N. Diarra, "NTRU-LPR IND-CPA: a new ideal lattice-based scheme", *Cryptology ePrint Archive, Report 2018/109*. [Online]. Available: http://eprint.iacr.org/2018/109. Accessed on: Sept. 07, 2020, doi: 10.13140/RG.2.2.15424. 35840.

[12] A. A. Matiyko, "The comparative analysis of *NTRUCipher* and *NTRUEncrypt* encryption schemes", *Mathimatical and computer modelling. Series: Technical science*, iss. 19, pp. 81-87, 2019, doi: 10.32626/2308-5916.2019-19.81-87.

[13] A. N. Alekseychuk, A. A. Matiyko, "Estimates of the probability of reversibility of random polynomials used in the modified version of NTRU cryptosystem", *Radiotekhnica*, iss. 189, pp. 38-46.

[14] L. Babai, "The Fourier transform and equations over finite abelian groups". [Online]. Available: *http://people.cs.uchicago.edu/~laci /ren/fourier.pdf*. Accessed on: Sept. 07, 2020.

ALEXANDRA MATIYKO

BKW-ATTACK ON NTRUCIPHER AND NTRUCIPHER+ ENCRYPTION SCHEMES

Due to the appearance of quantum computers, which will significantly reduce the time of solving certain problems, the security of many standardized cryptosystems is under threat. This prompted NIST to launch an open competition to create new post-quantum standards in 2016. In the summer of 2020, the NTRU algorithm, one of the fastest post-quantum algorithms based on lattices in Euclidean space (1996), was entered the seven finalists of this competition. However, only in 2017 was proposed an analog of this encryption scheme – symmetric encryption scheme

NTRUCipher. Preliminary researches of this encryption scheme have been conducted but it's security to chosen-plaintext attack, which consists of compiling a system of linear equations corrupted by noise (over a finite field of simple order) and solving it using a generalized BKW algorithm, have not been analyzed. For the first time, the NTRUCipher + cipher scheme is proposed in this article. Its main difference is the usage of an additional random polynomial when encrypting. The security of NTRUCipher cipher scheme and its modification NTRUCipher+ against BKW-attack is researched. Such an attack is possible for symmetric NTRU-like cipher schemes but it has not been considered before. Analytical (upper and lower) bounds of the BKW attack's complexity on NTRUCipher and NTRUCipher + are obtained. The comparison of these cipher schemes on the encrypted messages' length against BKW-attack at certain identical fixed parameters is carried out. It is shown that the security increase of the NTRUCipher cipher scheme against BKW-attack due to the usage of an additional additive in encryption is almost completely leveled by increasing the upper bound of the decryption failure probability. Research allows to compare these cipher schemes in terms of security and practicality and to conclude that it is inexpedient to use NTRUCipher+ to increase the security of the NTRUCipher cipher scheme to BKW attack. In the future, it is planned to develop methods for constructing symmetric analogs of the NTRU cryptosystem based on other general lattice-based structures.

Keywords: postquantum cryptography, lattice-based cryptography, NTRUCipher, NTRUCipher+, BKW-attack, Fourier transform.

Матійко Александра Андріївна, викладач кафедри безпеки державних інформаційних ресурсів, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

ORCID: 0000-0002-6947-5958.

E-mail: alexm1710@ukr.net.

Matiyko Alexandra, lecturer at the state information resources academic department, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.