DOI: 10.18372/2410-7840.20.12276
УДК 621.391:519.2

ОЦІНКИ ЙМОВІРНОСТІ ПОМИЛКОВОГО РОЗШИФРУВАННЯ ПОВІДОМЛЕНЬ У ШИФРОСИСТЕМІ NTRUEncrypt ПРИ ФІКСОВАНОМУ КЛЮЧІ

Александра Матійко, Антон Олексійчук

Асиметрична система шифрування NTRUEncrypt є однією з найшвидших постквантових шифросистем. На сьогодні відомо декілька версій цієї шифросистеми, проте усі вони володіють небажаною властивістю припускатися помилок розшифрування, що, поряд з незручностями для законних користувачів, приводить до специфічних атак на шифросистему і, як наслідок, зменшує її стійкість. При традиційному підході до оцінювання ймовірності помилкового розшифрування вважається, що ця ймовірність визначається відносно випадкового вибору всіх елементів, які використовуються для формування шифротексту: відкритого тексту, ключа та так званого рандомізуючого полінома. Поряд з тим, з практичного погляду більш адекватним показником частоти виникнення помилок є набір ймовірностей, обчислених для кожного фіксованого значення секретного ключа. У даній статті отримано верхні оцінки ймовірності помилкового розшифрування повідомлень при фіксованому ключі для однієї з найпоширеніших версій шифросистеми NTRUEncrypt. Перша з двох отриманих оцінок є наближеною в тому сенсі, що при її доведенні здійснюється заміна розподілу ймовірностей суми певних незалежних випадкових величин граничним (нормальним) розподілом. Друга отримана оцінка доводиться за допомогою нерівності Гефдінга та не базується на жодних евристичних припущеннях. В цілому, отримані результати надають більш адекватну інформацію про частоту виникнення помилок при розшифруванні для розглянутої версії NTRUEncrypt та можуть бути використані в подальшому при виборі параметрів цієї шифросистеми для її оптимізації за стійкістю або практичністю.

Ключові слова: *постквантова криптографія, NTRUEncrypt, ймовірність помилкового розшифрування, центральна гранична теорема, нерівність Гефдінга.*

Вступ

Асиметрична система шифрування NTRUEncrypt запропонована в 1996 р. [6] та є однією з найшвидших постквантових шифросистем. На сьогодні відомо декілька версій цієї шифросистеми, які відрізняються способами вибору параметрів та генерації ключів [1, 3, 4, 7, 8], проте усі вони володіють небажаною властивістю припускатися помилок розшифрування: при стандартному виборі параметрів шифротекст, отриманий на відкритому ключі, не завжди може бути коректно розшифрований за допомогою відповідного секретного ключа отримувача.

Поряд з незручностями для законних користувачів, помилки розшифрування приводять до специфічних атак на шифросистему [12] і, як наслідок, зменшують її стійкість, що потребує створення спеціальної схеми доповнення (padding scheme) для протидії можливим атакам та алгоритмів вибору параметрів, для яких ймовірність помилкового розшифрування не перевищує потрібну (малу) величину [4, 8 – 11].

При традиційному підході до оцінювання ймовірності помилкового розшифрування [3, 4, 8] вважається, що ця ймовірність визначається відносно випадкового вибору всіх елементів, які використовуються для формування шифротексту: відкритого тексту, ключа та рандомізуючого (осліплюючого, blinding) полінома. Поряд з тим, з практичного погляду більш адекватним показником частоти виникнення помилок є набір ймовірностей, обчислених для кожного фіксованого значення секретного ключа. Дійсно, звичайно секретний ключ (поряд із відповідним відкритим ключем) використовується певний тривалий час, і треба бути впевненим, що помилки розшифрування є малоймовірними саме при цьому значенні ключа.

Метою даної статті є отримання верхніх оцінок ймовірності помилкового розшифрування повідомлень при фіксованому ключі для версії NTRUEncrypt, описаної в [1, 4]. Перша з двох отриманих оцінок доводиться аналогічно оцінці з [4] та є *наближеною* в тому сенсі, що при її доведенні (саме так, як і в [4]) здійснюється заміна дограничного розподілу ймовірностей суми певних незалежних випадкових величин граничним (нормальним) розподілом. Друга отримана оцінка доводиться за допомогою нерівності Гефдінга [5] та не базується на жодних припущеннях евристичного характеру.

В цілому, отримані результати надають більш адекватну інформацію про частоту виникнення помилок при розшифруванні для розглянутої версії NTRUEncrypt та можуть бути використані в подальшому при виборі параметрів цієї шифросистеми для її оптимізації за стійкістю або практичністю.

Означення основних понять

Нехай n і q – взаємно прості натуральні числа, $n, q > 3$, q не ділиться на 3. Позначимо $\mathbf{Z}_q$ кільце класів лишків за модулем q, елементи якого ототожнимо з цілими числами, що належать інтервалу $[-(q-1)/2, (q-1)/2]$ для непарного q та інтервалу $[-q/2, q/2-1]$ для парного q. Позначимо $R_{n,q} = \mathbf{Z}_q[x]/(x^n - 1)$ кільце зрізаних поліномів степеня не вище n 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 $x^n - 1$.

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 $\| u \|_\infty = 1$, $i \in \overline{0, n-1}$.

Для будь-яких натуральних чисел d_1, d_2 позначимо S_{d_1,d_2} множину всіх малих поліномів степеня не вище n, серед коефіцієнтів яких є точно d_1, що дорівнюють 1, та точно d_2, що дорівнюють -1.

Для зазначених вище чисел n, q та натурального числа d *шифросистема NTRUEncrypt* [1, 4] визначається таким чином.

Секретним ключем цієї шифросистеми є будь-яка пара поліномів (F, g), де $F \in S_{d,d}$, $g \in S_{d'+1,d'}$, $d' = \lfloor n/3 \rfloor$ і поліном $f = 1 + 3F$ є оборотним елементом кільця $R_{n,q}$. Відповідним відкритим ключем є поліном $h = 3g / f$, який обчислюється в кільці $R_{n,q}$ шляхом множення полінома $3g$ на поліном, обернений до f.

Множина відкритих текстів шифросистеми NTRUEncrypt складається з усіх малих поліномів степеня не вище n. Для зашифрування такого поліному m на відкритому ключі h генерується випадковий поліном $r \in S_{d,d}$ та обчислюється шифротекст $E_h(m, r) = (m + rh) \bmod q$. Розшифрування довільного тексту $c \in R_{n,q}$ на секретному ключі (F, g) здійснюється за формулою $D_f(c) = cf \pmod q \bmod 3$. Якщо при цьому $D_f(E_h(m,r)) \ne m$, то говорять, що відбувається *помилка розшифрування*.

Як випливає з наведених означень, за умови помилки розшифрування принаймні один з коефіцієнтів полінома $mf + 3rg \in \mathbf{Z}[x]$ є за модулем не менше ніж $q/2$. Отже, справедлива імплікація

$$D_f(E_h(m,r)) \ne m \Rightarrow \| mf + 3rg \|_\infty \ge q/2 . \quad (1)$$

Зауважимо, що на підставі рівностей $f = 1 + 3F$, $\| F \|_1 = \| r \|_1 = 2d$ мають місце такі співвідношення:

$$\| mf + 3rg \|_\infty = \| m + 3(mF + rg) \|_\infty \le$$
$$1 + 3(\| m \|_\infty \| F \|_1 + \| r \|_1 \| g \|_\infty) = 1 + 12d .$$

Таким чином, за умови

$$d < (q-2)/24 \quad (2)$$

помилки розшифрування є неможливими. Якщо ж нерівність (2) не виконується, то помилки можливі, і постає задача оцінювання ймовірності помилкового розшифрування повідомлень при тих чи інших припущеннях відносно елементів F, g, m та r.

2. Постановка задачі та основні результати

В [4] отримано наближену верхню оцінку ймовірності $p_{er} = \mathbf{P}_{F,g,m,r}\{D_f(E_h(m,r)) \ne m\}$ за умови, що коефіцієнти поліномів F, g, m і r є незалежними випадковими величинами, розподіленими за законами

$$\begin{gathered} \mathbf{P}(F_i = 1) = \mathbf{P}(F_i = -1) = dn^{-1}, \\ \mathbf{P}(F_i = 0) = 1 - 2dn^{-1}, \\ \mathbf{P}(g_i = 1) = \mathbf{P}(g_i = -1) = d'n^{-1}, \\ \mathbf{P}(g_i = 0) = 1 - 2d'n^{-1}, \\ \mathbf{P}(m_i = 1) = \mathbf{P}(m_i = -1) = \mathbf{P}(m_i = 0) = 1/3; \end{gathered} \quad (3)$$

$$\begin{gathered} \mathbf{P}(r_i = 1) = \mathbf{P}(r_i = -1) = dn^{-1}, \\ \mathbf{P}(r_i = 0) = 1 - 2dn^{-1}; \end{gathered} \quad (4)$$

$$p_{er} \le 2n\, \Phi\left(-\frac{q-2}{6} \Big/ \sqrt{\frac{4d}{3}\left(1 + \frac{d'}{n}\right)} \right), \quad (5)$$

де $\Phi(x) = \frac{1}{\sqrt{2\pi}} \int\limits_{-\infty}^{x} e^{-\frac{t^2}{2}} dt$ є функція розподілу стандартного нормального закону. Зауважимо, що наближений характер оцінки (5) обумовлений

заміною догранічного розподілу суми певних незалежних випадкових величин її граничним (нормальним) розподілом ймовірностей.

В даній статті розв'язується задача отримання оцінок ймовірності $p_{er}(F,g)=\mathbf{P}_{m,r}\{D_f(E_h(m,r))\neq m\}$ за умови, що поліноми F і g є фіксованими, а коефіцієнти поліномів m і r є незалежними випадковими величинами, розподіленими за законами (3) і (4) відповідно.

Підкреслимо, що набір ймовірностей $(p_{er}(F,g): F\in S_{d,d}, g\in S_{d'+1,d'})$ є суттєво більш точним показником частоти виникнення помилок розшифрування у шифросистемі NTRUEncrypt в порівнянні з єдиним параметром $p_{er}(F,g)$ (який є усередненим значенням ймовірностей $p_{er}(F,g)$ за всіма $F\in S_{d,d}$, $g\in S_{d'+1,d'}$).

Основним результатом статті є таке твердження.

Твердження. Нехай $F\in S_{d,d}$, $g\in S_{d'+1,d'}$, а коефіцієнти поліномів m і r є незалежними випадковими величинами, розподіленими за законами (3) і (4) відповідно. Для будь-якого $i\in\overline{0,n-1}$ позначимо $p(i,F,g)$ ймовірність того, що модуль i-го коефіцієнту випадкового полінома $mf+3rg$ є не менше ніж $q/2$. Тоді справедливі (наближені) нерівності

$$2\,\Phi\left(-\frac{q+2}{6}\Big/\sqrt{\frac{4d}{3}\left(1+\frac{3(2d'+1)}{2n}\right)}\right)\le p(i,F,g)\le 2\,\Phi\left(-\frac{q-2}{6}\Big/\sqrt{\frac{4d}{3}\left(1+\frac{3(2d'+1)}{2n}\right)}\right). \tag{6}$$

Крім того, справедлива (наближена) нерівність

$$p_{er}(F,g)\le 2n\,\Phi\left(-\frac{q-2}{6}\Big/\sqrt{\frac{4d}{3}\left(1+\frac{3(2d'+1)}{2n}\right)}\right), \tag{7}$$

а також нерівність

$$p_{er}(F,g)\le 2n\exp\left\{-\frac{(q-2)^2}{72(2d+2d'+1)}\right\}, \tag{8}$$

Доведення. На підставі наведених означень

$$\begin{aligned}p(i,F,g)=\\ \mathbf{P}\{|\,m_i+3(mF)_i+3(rg)_i\,|\ge q/2\}\le\\ \mathbf{P}\{|\,(mF)_i+(rg)_i\,|\ge (q-2)/6\}=\\ =\mathbf{P}\left\{\left|\sum_{j=0}^{n-1}F_j m_{i-j}+\sum_{j=0}^{n-1}g_j r_{i-j}\right|\ge (q-2)/6\right\}.\end{aligned} \tag{9}$$

Позначимо

$$I'=\{j\in\overline{0,n-1}: F_j=1\},$$
$$I''=\{j\in\overline{0,n-1}: F_j=-1\},$$
$$J'=\{j\in\overline{0,n-1}: g_j=1\},$$
$$J''=\{j\in\overline{0,n-1}: g_j=-1\}.$$

Тоді, враховуючи формули (3),(4), можна записати нерівність (9) у вигляді

$$\begin{aligned}p(i,F,g)\\ \le\mathbf{P}\left\{\left|\sum_{j\in I'}m_{i-j}-\sum_{j\in I''}m_{i-j}+\sum_{j\in J'}r_{i-j}-\sum_{j\in J''}r_{i-j}\right|\ge (q-2)/6\right\}=\\ =\mathbf{P}\left\{\left|\sum_{k=1}^{2d}\xi_k+\sum_{l=1}^{2d'+1}\eta_l\right|\ge (q-2)/6\right\},\end{aligned} \tag{10}$$

де ξ_k, η_l є незалежними випадковими величинами, розподіленими за законами

$$\mathbf{P}(\xi_k=1)=\mathbf{P}(\xi_k=-1)=\mathbf{P}(\xi_k=0)=1/3,$$
$$k\in\overline{1,2d},$$
$$\mathbf{P}(\eta_l=1)=\mathbf{P}(\eta_l=-1)=dn^{-1},$$
$$\mathbf{P}(\eta_l=0)=1-2dn^{-1},\ l\in\overline{1,2d'+1}.$$

Позначимо $\varsigma=\sum_{k=1}^{2d}\xi_j+\sum_{l=1}^{2d'+1}\eta_l$. Тоді $\mathbf{E}\varsigma=0$,

$$\mathbf{D}\varsigma=\sum_{k=1}^{2d}\mathbf{D}\xi_j+\sum_{l=1}^{2d'+1}\mathbf{D}\eta_l=2d\cdot\frac{2}{3}+(2d'+1)\cdot\frac{2d}{n}.$$

Отже, підставі центральної граничної теореми справедлива (наближена) рівність

$$\mathbf{P}\{|\,\varsigma\,|\ge (q-2)/6\}=\mathbf{P}\left\{\left|\frac{\varsigma-E\varsigma}{\sqrt{\mathbf{D}\varsigma}}\right|\ge\frac{q-2}{6\sqrt{\mathbf{D}\varsigma}}\right\}=2\Phi\left(-\frac{q-2}{6\sqrt{\mathbf{D}\varsigma}}\right). \tag{11}$$

Безпосередньо з формул (10), (11) випливає верхня оцінка (6).

Нижня оцінка (6) доводиться аналогічно, виходячи з нерівностей

$$\begin{aligned}p(i,F,g)=\mathbf{P}\{|\,m_i+3(mF)_i+3(rg)_i\,|\ge q/2\}\ge\\ \mathbf{P}\{3\,|\,(mF)_i+(rg)_i\,|-1\ge q/2\}=\\ \mathbf{P}\{|\,(mF)_i+(rg)_i\,|\ge (q+2)/6\}=\\ \mathbf{P}\left\{\left|\sum_{j=0}^{n-1}F_j m_{i-j}+\sum_{j=0}^{n-1}g_j r_{i-j}\right|\ge (q+2)/6\right\}.\end{aligned}$$

Далі, формула (7) випливає з верхньої оцінки (6) та нерівності

$$p_{er}(F,g)\le n\cdot\max_{0\le i\le n-1}p(i,F,g), \tag{12}$$

яка є наслідком співвідношення (1).

Для доведення формули (8) скористаємося нерівністю Гефдінга [5]: якщо $\zeta_1, \ldots, \zeta_m$ є незалежними випадковими величинами такими, що $\alpha_i \le \zeta_i \le \beta_i$, де $\alpha_i, \beta_i \in \mathbf{R}$, $i \in \overline{1,m}$, то для будь-якого $u > 0$ має місце нерівність

$$\mathbf{P}\left\{\left|\sum_{i=1}^{m}(\xi_i - \mathbf{E}\xi_i)\right| \ge mu\right\} \le 2\exp\left\{-\frac{2m^2u^2}{\sum\limits_{i=1}^{m}(\beta_i-\alpha_i)^2}\right\}. \qquad (13)$$

Застосовуючи оцінку (13) до $m = 2d + 2d' + 1$ випадкових величин у правій частині нерівності (10), на підставі формули (12) отримаємо, що

$$p_{er}(F,g) \le n \cdot \max_{0\le i\le n-1} p(i,F,g) \le 2n\exp\left\{-\frac{(q-2)^2}{72(2d+2d'+1)}\right\}.$$

Таким чином, твердження повністю доведено.

В табл. 1 для низки пар (n, d), перші п'ять з яких рекомендовано в [4], а дві останні – в [3], наведені значення $-\log_2 p$, де p визначається за однією з формул (5) – (9); при цьому $q = 2048$, $d' = \lfloor n/3 \rfloor$.

Таблиця 1

Результати оцінювання параметрів, що характеризують частоту виникнення помилок розшифрування у шифросистемі NTRUEncrypt

(n, d)	Нижня оцінка (6)	Верхня оцінка (6)	Оцінка (7)	Оцінка (8)	Оцінка (5)
(401, 113)	284,26	283,15	274,51	160,49	414,33
(449, 134)	240,31	239,36	230,55	138,12	348,49
(677, 157)	205,59	204,82	195,42	99,24	296,03
(1087, 120)	267,69	266,64	256,55	75,84	388,05
(1171, 106)	302,52	301,35	291,15	73,28	439,97
(443, 143)	225,40	224,54	215,75	134,58	326,28
(743, 247)	131,96	131,45	121,92	74,28	185,96

Як видно з табл. 1, значення верхньої та нижньої оцінок (6) практично співпадають за порядком величини. При цьому значення верхньої оцінки (8) є суттєво більше в порівнянні зі значеннями (наближеної) верхньої оцінки (7). Наприклад, при $(n, d) = (401, 113)$ ймовірність події, яка полягає в тому, що (для фіксованого $i \in \overline{0, n-1}$) модуль i-го коефіцієнту випадкового полінома $mf + 3rg$ є не менше ніж $q/2$, знаходиться в межах від $2^{-284,26}$ до $2^{-283,15}$, а ймовірність помилкового розшифрування повідомлення при будь-якому фіксованому ключі (F, g) не перевищує $2^{-160,49}$. Проте за умови справедливості рівності (11) можна стверджувати, що ця ймовірність не перевищує $2^{-274,51}$.

В табл. 2, 3 показано, як змінюються значення отриманих оцінок з ростом параметра d при фіксованих q і n.

Таблиця 2

Значення верхніх меж ймовірності помилкового розшифрування у шифросистемі NTRUEncrypt при $q = 2048,\ n = 443$

d	86	90	100	105	110	120	130	140	147
Оцінка (7)	361,99	345,69	310,65	295,62	281,97	258,06	237,83	220,48	209,74
Оцінка (8)	169,82	166,80	159,66	156,31	153,08	146,99	141,34	136,09	132,62

Таблиця 3

Значення верхніх меж ймовірності помилкового розшифрування у шифросистемі NTRUEncrypt при $q = 2048,\ n = 743$

d	86	100	120	145	165	190	210	230	247
Оцінка (7)	361,16	309,83	257,26	211,91	185,52	160,32	144,48	131,38	121,92
Оцінка (8)	115,22	110,15	103,58	96,315	91,13	85,32	81,13	77,29	74,27

Зауважимо, що на сьогодні вважається прийнятним такий вибір параметрів шифросистеми NTRUEncrypt, для яких ймовірність помилкового розшифрування $p_{er} = \mathbf{P}_{F,g,m,r}\{D_f(E_h(m,r)) \neq m\}$ не перевищує 2^{-80} (див., наприклад, [2], с. 13). Отримані результати показують, що параметри, рекомендовані в [3, 4], задовольняють навіть більш жорсткому критерію, згідно з яким ймовірність $p_{er}(F,g) = \mathbf{P}_{m,r}\{D_f(E_h(m,r)) \neq m\}$ обмежена зверху величиною такого ж порядку для будь-якого фіксованого ключа (F,g).

Висновки

Основними результатами статті є аналітичні верхні оцінки ймовірності помилкового розшифрування повідомлень при фіксованому секретному ключі для шифросистеми NTRUEncrypt, описаної в [1, 4]. Отримані оцінки надають більш адекватну інформацію про частоту виникнення помилок при розшифруванні для цієї версії NTRUEncrypt та можуть бути використані в подальшому при виборі параметрів шифросистеми для її оптимізації за стійкістю або практичністю. Результати чисельних розрахунків показують, що параметри шифросистеми, рекомендовані в [3, 4], задовольняють більш жорсткому критерію малості ймовірності помилкового розшифрування для будь-якого фіксованого секретного ключа (а не тільки критерію малості середнього значення цієї ймовірності за всіма секретними ключами).

ЛІТЕРАТУРА

[1]. American National Standard X9.98-2010. Lattice-based polynomial public key encryption algorithm, Part 1: key establishment, Part 2: data encryption. 2010.

[2]. D. Bernstein, Ch. Chuengsatiansup, T. Lange, Ch. Van Vredendaal, "NTRU Prime: redusing attack surface at low cost", *Cryptology ePrint Archive, Report 2016/461*. [Electronic resource]. Online: http://eprint.iacr.org/2016/461.

[3]. C. Chen, J. Hoffstein, W. Whyte, Z. Zhang, "NIST PQ Submission: NTRUEncrypt. A lattice based algorithm". [Electronic resource]. Online: https://cscr.nist.gov/Projects/Post-Quantum-Cryptorraphy, 2017.

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

[5]. W. Hoeffding, "Probability inequalities for sums of bounded random variables", J. *Amer. Statist. Assoc.*, Vol. 58, no. 301, pp. 13-30, 1963.

[6]. J. Hoffstein, J. Pipher, J.H. Silverman, "NTRU: a new high speed public key cryptosystem", *Preprint, presented at the rump session of Crypto'96*. 1996.

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

[8]. J. Hoffstein, J. Pipher, J.M. Schanck, J.H. Silverman, W. Whyte, Z. Zhang, "Choosing parameters for NTRUEncrypt", *Cryptology ePrint Archive, Report 2015/708*. [Electronic resource]. Online: http://eprint.iacr.org/2015/708.

[9]. N. Howgrave-Graham, P. Nguyen, D. Pointcheval, J. Proos, J.H. Silverman, A. Singer, W. Whyte, "The impact of decryption failures on the security of NTRU encryption", *Advanced in Cryptology, Crypto 2003, LNCS*, Vol. 2729, pp. 226-246, 2003.

[10]. N. Howgrave-Graham, J.H. Silverman, W. Whyte, "Choosing parameter sets for NTRUEncrypt with NAEP and SVES-3", *Topics in Cryptology. CT-RSA 2005, LNCS*, Vol. 3376, pp. 118-135, 2005.

[11]. N. Howgrave-Graham, J.H. Silverman, A. Singer, W. Whyte, "NAEP: provable security in the presence of decryption failures", *Cryptology ePrint Archive, Report 2003/172*. [Electronic resource]. Online: http://eprint.iacr.org/2003/172

[12]. J.A. Proos, Imperfect decryption and an attack on the NTRU encryption scheme, *Cryptology ePrint Archive, Report 2003/002*. [Electronic resource]. Online: http://eprint.iacr.org/2003/002.

ОЦЕНКИ ВЕРОЯТНОСТИ ОШИБОЧНОГО РАСШИФРОВАНИЯ СООБЩЕНИЙ В ШИФРОСИСТЕМЕ NTRUEncrypt ПРИ ФИКСИРОВАННОМ КЛЮЧЕ

Асимметричная система шифрования NTRUEncrypt является одной из самых быстрых постквантових шифрсистем. В настоящее время известно несколько версий этой шифрсистемы, однако все они обладают не-

желательным свойством допускать ошибки расшифрования, что, наряду с неудобствами для законных пользователей, приводит к специфическим атакам на шифрсистему и, как следствие, уменьшает её стойкость. При традиционном подходе к оценке вероятности ошибочного расшифрования предполагается, что эта вероятность определяется относительно случайного выбора всех элементов, используемых для формирования шифртекста: открытого текста, ключа и так называемого рандомизирующего полинома. Вместе с тем, с практической точки зрения более адекватным показателем частоты появления ошибок является набор вероятностей, вычисленных для каждого фиксированного значения секретного ключа. В данной статье получены верхние оценки вероятности ошибочного расшифрования сообщений при фиксированном ключе для одной из наиболее распространённых версий шифросистемы NTRUEncrypt. Первая из двух полученных оценок является приближенной в том смысле, что при ее обосновании производится замена распределения вероятностей суммы определенных независимых случайных величин предельным (нормальным) распределением. Вторая полученная оценка доказывается с помощью неравенства Гефдинга и не базируется на каких-либо эвристических предположениях. В целом, полученные результаты дают более адекватную информацию о частоте возникновения ошибок при расшифровании для рассмотренной версии NTRUEncrypt и могут быть использованы в дальнейшем при выборе параметров этой шифрсистемы для ее оптимизации по стойкости или практичности.

Ключевые слова: постквантовая криптография, NTRUEncrypt, вероятность ошибочного расшифрования, центральная предельная теорема, неравенство Гефдинга.

BOUNDS OF DECRYPTION FAILURE PROBABILITY IN NTRUEncrypt ENCRYPTION SCHEME FOR A FIXED KEY

The asymmetric encryption scheme NTRUEncrypt is one of the fastest post-quantum encryption schemes. To date, there are several versions of this encryption scheme but all of them have an unwanted feature that assumes decryption failure. Besides the inconvenience for authorized users, this feature leads to specific attacks on the encryption scheme and consequently reduces its security. The traditional approach to estimating the decryption failure probability assumes that this probability is determined by random selection of all elements used to form the encrypted message: the plain text, the key and so-called randomizing polynomial. At the same time, from a practical point of view, a more adequate indicator of the failure frequency is the set of probabilities calculated for each fixed value of the secret key. In this article, we get upper bounds for the decryption failure probability for a fixed key for one of the most extensive versions of the NTRUEncrypt encryption scheme. The first of two obtained bounds is approximate in the sense that, when it is proved, the replacement of the probability distribution of certain independent random variables sum by the limit (normal) distribution is carried out. The second obtained bound is due to Hoeffding's inequality and it is not based on any heuristic assumptions. In general, the obtained results provide more adequate information about the frequency of decryption failure for the considered version of NTRUEncrypt and can be used later in choosing the parameters of this encryption scheme to optimize it for security or practicality.

Keywords: post-quantum cryptography, NTRUEncrypt, decryption failure probability, central limit theorem, Hoeffding's inequality.

Матійко Александра Андріївна, курсант Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».
E-mail: alexm1710@ukr.net.

Матийко Александра Андреевна, курсант Института специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт имени Игоря Сикорского».

Matiyko Aleksandra, cadet of Institute of Special Communication and Information Protection National technical university of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute».

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.

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, 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».