МЕТОДЫ, МЕХАНИЗМЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

УДК 004 056 55

І.Д. ГОРБЕНКО, д-р техн. наук, О.Г. КАЧКО, канд. техн. наук,
К.А. ПОГРЕБНЯК, канд. техн. наук, Л.В. МАКУТОНІНА, канд. техн. наук,

АНАЛІЗ, ОЦІНКИ ТА ПРОПОЗИЦІЇ ВІДНОСНО МЕТОДУ ГЕНЕРАЦІЇ СИСТЕМНИХ ПАРАМЕТРІВ У NTRU-ПОДІБНИХ АСИМЕТРИЧНИХ СИСТЕМАХ

Вступ

Натепер впровадження електронних довірчих послуг в європейському союзі та інших технологічно розвинутих державах є однією з найважливіших задач. Починаючи з 70-х років минулого століття для вирішення цієї задачі використовувалися різні криптографічні методи – перетворення в кільцях, скінченому полі, RSA-перетворення, в групі точок еліптичних кривих. Деякі з них є морально застарілими, деякі вже не використовуються, з потужним розвитком криптоаналітичних систем, в тому числі реалізованих на основі використання квантового комп'ютера та/або квантових обчислень, гостро постає питання підвищення рівня безпеки класичних асиметричних криптографічних методів без погіршення показників складності обчислення та швидкодії таких методів. Це проблемне питання розв'язується шляхом використання криптографічних перетворень в фактор-кільці (алгебраїчних решітках, NTRU-перетворень).

Найважливішим питанням для таких систем є врівноважений підбір системних параметрів, які б задовольняли вимогам стійкості і швидкодії. Робота є продовженням циклу робіт, присвячених аналізу, генерації та оцінки параметрів для класичного [1] та сучасних методів NTRU, наприклад [2]. Перша робота цього циклу [3] присвячена перевірці параметрів класичного NTRU, а саме обчислення імовірності помилки розшифрування, визначення імовірностей формування ключа з потрібною структурою, а також імовірності узгодження результатів MITM атаки та атаки на решітку.

Мета даної роботи - визначення параметрів з урахуванням комбінованої атаки з використанням результатів, які представлені в [3]. Робота [4] є найбільш детальною роботою, яка присвячена генерації параметрів для класичного NTRU.

1. Опис класичного NTRU-методу і системних параметрів

Для нашого випадку дамо наступний опис NTRU-методу. Нехай R позначатиме кільце $Z[X]/(X^N-1,q)$, для деяких цілих N,q. Та нехай T_{d_1,d_2} позначає множину тринарних елементів R зі d_1 кількістю одиниць, d_2 кількістю негативних одиниць і залишковою кількістю $N-d_1-d_2$ нулів. Нехай $a \in_R A$ позначає рівномірний і випадковий процес вибору елементу a із множини A.

Під системними параметрами будемо мати на увазі цілі (q, p, N, d_f, d_g, d_r), де секретний ключ $F \in_R T_{d_f,d_f}$, і $h = g/f$ – відкритий ключ у кільці R, де $g \in_R T_{d_g+1,d_g}$ і $f = 1 + pF$ є оборотним для більшості вибраних значень із F.

Визначимо *примітив зашифрування NTRUEncrypt* наступним чином.

Для деяких m' і $r \in_R T_{d_r,d_r}$, вироблених з відкритого тексту повідомлення за допомогою функції (randomized padding [1]) зведення вхідного повідомлення до заданого вигляду, відповідно до використовуваного поліному, нехай:

$$e := r * h + m' \text{ в } R \in (Z / qZ)[X]/(X^N - 1). \quad (1)$$

Метод NTRUEncrypt можна розглядати як алгебраїчну решітку розміру $(2N)\times(2N)$ і представити матрицею виду

$$L_{NTRU} = \begin{pmatrix} qI_N & 0_N \\ H & I_N \end{pmatrix}, \quad (2)$$

де H позначає $(N)\times(N)$ циркулянтну матрицю генеровану зі h, тобто $H_{i,j} = h_{i-j \bmod N}$. У деяких випадках останнє представлення методу NTRU є корисним при криптографічному аналізі.

Примітив розшифрування NTRUDecrypt представимо наступним чином:

Для деякого секретного тексту a і секретного ключа f є вірним рівняння

$$a := f * e \text{ в } R \in (Z / qZ)[X]/(X^N - 1). \quad (3)$$

Коефіцієнти полінома a для отримання повідомлення m приводяться по модулю в інтервалі [A, $A+q-1$], а також по модулю p для отримання кандидата в розшифроване повідомлення m.

Отриманий поліном a приводиться за модулем, але таким чином, щоб коефіцієнти приймали значення в інтервалі [$-q/2$, $q/2$]. В результаті обчислюється відновлений поліном: $m = a * F_p$, де $F_p = (f_p^{-1})$ є частиною вказаної вище особистого ключа, який є і мультиплікативно зворотним до $fa \bmod p$.

2. Пропозиції та оцінки щодо побудування загальних параметрів для перспективного асиметричного шифру в фактор-кільцях

За результатами аналізу стандарту ANSI X9.98 – 2010 розглядалися три основні задачі та проблемні питання:

1. Можливість помилки розшифрування.
2. Можливість відновлення секретного ключа за відкритим ключем і відомим параметрам.
3. Можливість відновлення поліному маскування по зашифрованим повідомленням.

За обчислювальною складністю друге та третє питання по суті є еквівалентними та зводяться до пошуку коротких векторів в алгебраїчній решітці. Виходячи з цього було прийняте рішення відносно розгляду перших двох питань.

2.1. Умови запобігання помилки розшифрування

Розглянуто в першій статті циклу [3]. Отримані результати наведено в табл. 1.

Таблиця 1

Оцінка максимальних значень d_f

S \ N	401	449	677	1087	541	613
112	133 (113)				180 (49)	
128		149 (134)				204 (55)
192			161 (157)			
256				122 (120)		
S \ N	887	1171	659	761	1087	1499
112			219 (38)			
128				236 (42)		
192	161 (81)				161 (63)	
256		120 (106)				120 (79)

Значення, вказані в таблиці, відповідають обчисленим значенням максимального значення d_f, в дужках наведені значення d_f, які використовує стандарт. Як видно з таблиці, усі значення, які використовуються, не перевищують обчислених значень. Саме ці значення d_f використовуються в якості максимальних значень для інших атак.

2.2. Аналіз криптоаналітичних атак, направлених на відновлення секретного ключа за відкритим ключем і відомим параметрам

2.2.1. *Атака грубої сили.* Для відновлення секретного ключа достатньо перебрати усі варіанти цього ключа. Для кожного наступного варіанту можна обчислити значення $h * f$. Якщо вектор, який отримуємо, є вектором з координатами {-1, 0, 1}, тобто це може бути значення g, такий варіант і є секретним ключем.

Кількість таких варіантів визначається формулою

$$K = \frac{N!}{((d_f)!^2)(N - 2d_f)!}. \tag{4}$$

Результати обчислень наведено в табл. 2

Таблиця 2

Оцінка атаки грубої сили

N	d_f	S	$\log_2 K'$	$\min d_f$
401	113	112	605	10
449	134	128	687	11
677	157	192	970	16
1087	120	256	1048	19
541	49	112	450	9
613	55	128	509	10
N	d_f	S	$\log_2 K'$	$\min d_f$
887	81	192	752	15
1171	106	256	992	19
659	38	112	399	9
761	42	128	448	10
1087	63	192	670	14
1499	79	256	867	18

В таблиці також задані мінімальні значення d_f, при яких досягається задана криптостійкість (S) при здійсненні тільки перебору усіх варіантів для особистого ключа.

Далі розглянуті більш успішні атаки.

2.2.2. *Атака на решітку.* Криптографічну систему NTRU можна представити у вигляді матриці, представленої формулою (5), розміру $(2N) \times (2N)$, де H позначає циркулянт (циклічний визначник) генерованої з h, тобто $H_{i,j} = h_{i-j \bmod N}$ [2]. Цю матрицю зручно використовувати при модулюванні криптоаналітичних атак на алгебраїчну решітку. При цьому нехай $q = 2048$, $d_r = d_f$ і $d_g = \lfloor N / 3 \rfloor$.

$$L_{NTRU} = \begin{pmatrix} qI_N & 0_N \\ H & I_N \end{pmatrix} = \left(\begin{array}{cccccccc} q & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ 0 & q & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & q & 0 & 0 & \dots & 0 \\ \hline h_0 & h_1 & \dots & h_{N-1} & 1 & 0 & \dots & 0 \\ h_{N-1} & h_0 & \dots & h_{N-2} & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ h_1 & h_2 & \dots & h_0 & 0 & 0 & \dots & 1 \end{array}\right) \quad (5)$$

Для знаходження вектору решітки, який складається з ключів f, g, можна використовувати метод редукції BKZ, для якого найоптимістичніша оцінка складності $(n\beta)^n$.

В 2013 р. запропоновано суттєву оптимізацію цього методу (BKZ 2), яка дозволила виконати пошук короткого вектору для решіток розміру 725-825 [5 - 7]. Для оцінки кількості потрібних операцій для виконання редукції решітки в роботах [1, 4] запропоновано емпіричну формулу

$$w = \frac{2mn}{(1-\alpha)^2} + 3\ln\frac{2n}{1-\alpha} + c \quad (6)$$

де m=0.2, c = -50 – константи; α – характеризує якість знаходження найкоротшого вектору решітки.

В табл. 3 наведено результати розрахунку мінімальної обчислювальної складності редукції решітки, відносно формули (6), для α = [0.09,0.2].

Таблиця 3

Оцінка мінімальної обчислювальної складності редукції решітки

S=112		S=128	
N	W	N	W
401	164.04	449	187.56
541	232.56	613	267.71
659	290.15	761	339.85
S = 192		S=256	
N	W	N	W
677	298.93	1087	498.393
887	401.18	1171	539.19
1087	498.39	1499	698.37

Таким чином, атака на решітку як самостійна атака не має сенсу.

2.2.3. *Атака «зустріч посередині» (MITM атака)*. Для оцінки обчислювальної складності MITM атаки [1] визначається кількість варіантів, які треба обробити для цієї атаки. Для визначення кількості варіантів використовується формула

$$W = \binom{N}{d_f/2 \;\; d_f/2} \Big/ \binom{d_f}{d_f/2 \;\; d_f/2}. \quad (7)$$

Результати використання цієї атаки представлені в табл. 4.

Таблиця 4

Розраховані значення системних параметрів зі урахуванням можливості MITM атаки

S	N	d_f (standart)	W (standart)	mind_f
112	401	113	339	21
	541	49	233	19
	659	38	205	18
128	449	134	390	24
	613	55	262	21
	761	42	230	20
192	677	157	524	35
	887	81	386	32
	1087	63	342	30
256	1087	120	540	43
	1171	106	508	42
	1499	79	441	39

За допомогою цієї атаки визначено мінімальне значення d_f, при якому тільки за допомогою MITM атаки можна обчислити особистий ключ. Саме це значення d_f буде використано в якості нижньої границі для наступної атаки. В якості верхньої границі будемо використовувати значення d_f, яке забезпечує правильне розшифрування (табл. 1).

Значення W (standart) відповідає кількості операцій, які треба виконати для цієї атаки при стандартному значенні d_f, яке визначено в відповідній колонці. Для усіх значень N це значення суттєво перевищує значення S (криптостійкості).

2.2.4. *Комбінована атака* [4, 8]. На теперішній час є самою успішною атакою на NTRU-метод. Коротко цю атаку можна описати так:

Верхня частина матриці містить нульові елементи і відомі значення та не становить інтерес для криптоаналізу. Для другої частини може застосовуватися атаки декількох видів.

Матриця (5) ділиться на три частини по рядкам за наступним правилом:

$$\begin{aligned} &1)\ y_1 < N; \\ &2)\ [y_1, y_2),\ N < y_2 < 2N; \\ &3)\ [y_2, 2N]. \end{aligned} \tag{8}$$

1) Перша частина рядків не оброблюється, так як містить елементи вектора g.

2) Для другої частини матриці застосовується методи редукції (зведення) решітки, з використанням методів редукції, наприклад BKZ 2. Час виконання зазвичай оцінюється емпіричною формулою [4]

$$t_{LLL} = \frac{2m(y_2 - N)}{(1-\alpha)^2} + 3\log\frac{2(y_2 - N)}{1-\alpha} + c. \tag{9}$$

3) До третьої частини застосовується атака зустріч посередині.

Для узгодження останніх двох атак повинні виконуватися наступні умови [4]:

– значення *c* повинні мати коректну кількість -1 і 1 в останній $2N - y_2$ частині множини F (імовірність p_{split});

– в результаті редукції необхідно отримати короткий вектор з відповідною кількістю -1 і 1 (імовірність p_s).

Очікувана кількість операцій для третьої частини зі урахуванням p_s, без урахування парадоксу дня народження та зі урахуванням, оцінюється як [4]:

$$N_{MITM} = \frac{\binom{2N - y_2}{c/2 \;\; c/2}}{p_s * \binom{c}{c/2 \;\; c/2}}; \quad N_{MITM+BP} = \frac{\binom{2N - y_2}{c/2 \;\; c/2}}{\sqrt{p_s * \binom{c}{c/2 \;\; c/2}}}. \tag{10}$$

Загальний час виконання комбінованої атаки оцінюється як $T = tN / p_{split}$, де t – час виконання однієї ітерації [4]. Згідно з результатами, отриманими авторами в [3], обчислено загальний час виконання комбінованої атаки для обох варіантів, пов'язаних з парадоксом дня народження. Визначені мінімальні значення d_f, при яких забезпечується потрібна криптостійкість.

Результати наведено в табл. 5. Для обчисленого значення d_f задано два числа. Перше відповідає випадку, коли кількість варіантів N_{MITM} (задається першим рядком), а інше $N_{MITM+BP}$ (задається другим рядком). Як видно з табл. 5, обчислене значення d_f для першого варіанту завжди нижче, ніж визначено стандартом, тобто стандарт гарантовано забезпечує необхідну складність. Відносно другого варіанту, значення d_f, отримані нами, перевищують задані стандартом. Це означає, що якщо атака буде організована з урахуванням парадоксу дня народження, як це було для ключових даних, які задавались 0, 1, то задані значення для d_f недостатні.

Таблиця 5

Розраховані значення системних параметрів з урахуванням можливості комбінованої атаки

S=112				S=128			
N	df (standart)	W	Min df	N	df (standart)	W	Min df
401	113	113	78	449	134	129	89
			132				147
541	49	113	41	613	55	129	46
			53				59
659	38	113	32	761	42		36
			39				43
S= 192				S=256			
N	df (standart)	W	Min df	N	df (standart)	W	Min df
677	157	193	112	1087	120	257	99
			158				120
887	81	193	68	1171	106	257	89
			86				112
1087	63	193	54	1499	79	257	68
			64				80

Поки що незрозуміло, як саме ця атака буде реалізована проти теперішньої версії НШ NTRU.

Висновки

З появою квантових комп'ютерів одним з найперспективніших асиметричних криптографічних методів, який задовольняє вимоги стійкості і швидкодії, стала NTRU криптосистема, документована американським стандартом ANSI X9.98 – 2010.

Основними проблемними питаннями цієї криптосистеми є ймовірність виникнення помилки під час операції розшифрування, унеможливлення успішної реалізації атак на секрет-

ний ключ за відкритим ключем і відомими параметрами, а також на відновлення поліному маскування по зашифрованому тексту. Ці три питання вирішуються шляхом урівноваженого підбору системних параметрів. Можна показати, що третє питання не є складнішим за друге, тому потрібно вирішити перше і друге питання.

Нами проаналізовані параметри, наведені в стандарті ANSI X9.98 – 2010, відносно вирішення саме цих питань, а також розроблена програму для обчислення наведених та нових системних параметрів. Для вирішення другого питання реалізовано модель комбінованої атаки, яка, відповідно сучасним даним, є найперспективнішою атакою для перетворення в фактор-кільці. Отримані результати наведено в табл. 5.

Як видно з таблиці, результати збігаються зі стандартними параметрами у випадку неможливості застосування атаки, пов'язаної з використанням парадоксу дня народження. Нами знайдено значення системних параметрів, які, в разі знаходження можливості використання цього парадоксу, задовольняють усім наведеним вище рівням безпеки.

Отримані результати дозволяють обчислювати нові системні параметри з урахуванням поточних можливостей атак і можуть бути використані в разі появи перспективних атак не тільки для методу NTRU, а і інших алгоритмів, які використовують алгебраїчні решітки.

Список літератури: 1. *American* National Standard X9.98-2010. Lattice-Based Polynomial Public Key Encryption Algorithm Part 1: Key Establishment: Part 2: Data Encryption, 2010. 2. *Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, and Christine van Vredendaal.* NTRU Prime, https://ntruprime.cr.yp.to/ntruprime-20160511.pdf. 3. *Gorbenko, I., Kachko, O., Pogrebnyak, K.* Features of parameters calculation for NTRU algorithm // Прикладная радиоэлектроника. – 2015. – Т. 14, № 3. – С. 272-277. 4. *Jeff Hoffstein, Jill Pipher, John M. Schanck, Joseph H. Silverman, William Whyte, and Zhenfei Zhang* Choosing Parameters for NTRUEncrypt. https://eprint.iacr.org/2015/708.pdf. 5. *Phong Q. Nguyen*. Lattice Reduction Algorithms: Theory and Practice. http://link.springer.com/chapter/10.1007%2F978-3-642-20465-4_2#page-5. 6. *Yuanmi Chen and Phong Q. Nguyen.* BKZ 2.0 Better Lattice Security Estimates, http://link.springer.com/chapter/10.1007%2F978-3-642-25385-0_1#page-1. 7. *TU DARMSTADT* LATTICE CHALLENGE. http://latticechallenge.org. 8. *Nick Howgrave-Graham.* A hybrid lattice-reduction and meet-in-the-middle attack against NTRU. https://www.iacr.org/archive/ crypto2007/46220150/ 46220150.pdf

Харківський національний
університет імені В.Н. Каразіна

Надійшла до редколегії 11.09.2016