УДК 004.056.55 **DOI:10.30837/rt.2022.2.209.08**

О.Г. КАЧКО, канд. техн. наук, М.В. ЄСІНА, канд. техн. наук, К.О. КУЗНЕЦОВА

АНАЛІЗ МЕТОДІВ ТА АЛГОРИТМІВ ГЕНЕРАЦІЇ КЛЮЧОВИХ ДАНИХ ДЛЯ FALCON ПОДІБНИХ АЛГОРИТМІВ ЕЛЕКТРОННОГО ПІДПИСУ

Вступ

Алгоритм Falcon [2] є фіналістом конкурсу постквантових алгоритмів електронного підпису [1] завдяки задовільному значенню суми довжин відкритого ключа |pk| та |sig|, але алгоритм генерації ключових даних застосовує багато методів та важкий для реалізації. Автори [2] застосовують цей алгоритм для поліномів розміром n=512, 1024. Для збільшення шостого рівня криптостійкості цей алгоритм може бути розширено для n=2048. Саме дослідженню алгоритму Falcon з урахуванням його розширення для n=512, 1024, 2048 в частині генерації ключових даних присвячена ця робота.

У роботі застосовуються позначення, що прийняті в [2].

1. Алгоритм генерації ключових даних

Параметрами алгоритму є значення n, q.

Значення n визначає степінь поліномів (n=512, 1024, 2048) та відповідне поле $\phi = x^n + 1$. Значення q визначає модуль, за яким обчислюється відкритий ключ і виконуються перетворення при обчисленні електронного підпису, q=12289 для усіх n.

Результатом роботи алгоритму генерації ключових даних є:

– Поліноми f, g – випадкові поліноми.

– Поліноми F, G, що обираються згідно рівнянню:

$$f \cdot G - g \cdot F = q \bmod \phi . \tag{1}$$

Алгоритм генерації ключових даних включає наступні кроки:

Крок 1. Генерація випадкових поліномів f, g в полі $x^p + 1$, $(p = n)$.

Крок 2. Перетворення поліномів f, g в полі $x^p + 1$, $(p = n)$ в поліноми f', g' для поля $x^p + 1$, $(p = 1)$.

Крок 3. Рішення діафантового рівняння $f' \cdot G' - g' \cdot F' = 1$ відносно F', G' для поля $x^p + 1$, $(p = 1)$.

Крок 4. Якщо рішення є, то обчислення $G' = q \cdot G$, $F' = q \cdot F$; інакше повернутися на Крок 1.

Крок 5. Перетворення F', G' для поля $x^p + 1$, $(p = 1)$ в поліноми F, G для поля $x^p + 1$, $(p = 1)$.

2. Генерація випадкових поліномів f, g, які задовільняють розподілу Гауса

Для отримання коротких поліномів обираються параметри розподілу Гауса $\sigma = 1.17 \cdot \sqrt{\frac{q}{2n}}$, $\mu = 0$.

Квадратична норма поліномів обчислюється за формулою

$$norma(f, g) = \sum_{i=0}^{n-1} \left(f_i^2 + g_i^2 \right). \tag{2}$$

Для поліномів $f' = \frac{qf^*}{ff^* + gg^*}$, $g' = \frac{qg^*}{ff^* + gg^*}$ (f^*, g^* – комплексно спряжені поліноми) квадратична норма обчислюється за формулою

$$norma(f', g') = \sum_{i=0}^{n-1} \left(f_i'^2 + g_i'^2 \right). \quad (3)$$

$norma(f, g)$ та $norma(f', g')$ не повинні перевищувати значення *max_norma*=1.172*q*:

Для поліному *f* повинна існувати інверсія f^{-1}, тобто

$$f \cdot f^{-1} = 1 \bmod (\bmod \phi,\ q). \quad (4)$$

Автори Falcon [2] для генерації поліномів з розподілом Гауса застосовують генератори випадкових чисел і накопичувальну таблицю розподілу, яку передобчислюють заздалегідь. Для згенерованих поліномів порівнюють норми, обчислені за формулами (1), (2), з максимальною нормою (3). Поліном *g* приймається, якщо норми не перевищують максимальну норму. Для поліному *f* виконується додаткова перевірка на наявність інверсії. У разі, якщо хоч одна перевірка для жодного поліному не проходить, поліноми генеруються знову. У табл. 1 наведено результати аналізу поліномів з урахуванням обох критеріїв за нормою та наявності інверсії для поліному *f*. Задано кількість відбракованих поліномів за різними критеріями, а також загальний процент відбракованих поліномів.

Таблиця 1

Результати аналізу поліномів з урахуванням обох критеріїв за нормою та наявності інверсії для поліному

Розмір поліному	*N*=512	*N*=1024	*N*=2048
int	4942	4950	4987
double	4079	4364	4671
f^1	49	51	49
Common *g* (%)	90.21	93.14	96.58
Common *f* (%)	90.7	93.64	97.07

У рядку int наведена кількість поліномів, які не пройшли перевірку, пов'язану з квадратичною нормою згідно (1).

У рядку doudle наведена кількість поліномів, які не пройшли перевірку, пов'язану з квадратичною нормою згідно (2).

У рядку f^{-1} наведена кількість ключів, які не пройшли перевірку, пов'язану з наявністю інверсії (4). Виконується тільки для поліному *f*. У рядках *Common g* (%) та *Common f* (%) наведено % пар поліномів, які не пройшли усіх перевірок.

Як видно з табл. 1, з поліномів, які генеруються за методикою авторів [2], не менше, ніж 90 % пар поліномів треба відбракувати, кількість відбракованих пар поліномів збільшується зі збільшенням *n* разом з часом генерації для цих поліномів. Подалі цей спосіб будемо називати Спосіб 1.

Пропонується інший спосіб (Спосіб 2) генерації поліномів із застосуванням формули імовірності для розподілу Гауса:

$$P(k) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{k^2}{2\sigma^2}}. \quad (4)$$

Розраховуємо ймовірність $0, \pm1, \pm2, \ldots$ і далі з урахуванням значення *n*. У результаті отримаємо поліном, який задовольняє вимогам розподілу Гауса та досягаємо непарності суми коефіцієнтів за модулем 2. За допомогою алгоритму випадкової перестановки [3] отримаємо поліноми *f*, *g*. В табл. 2 наведено норми для таких поліномів в залежності від *n*.

Таблиця 2

Норми для поліномів *f, g* в залежності від *n*

n	512	1024	2048
$\sum_{i=0}^{n-1}\left(f_i^2+g_i^2\right)$	16270	16642	16750

Значення максимальної норми згідно з (2) дорівнює 16822.4121, тобто усі поліноми, згенеровані таким чином, задовольняють цій нормі.

Результати порівняння кількості коефіцієнтів з різними значеннями для алгоритмів згідно [2] та алгоритму, розглянутому вище, наведено в табл. 3.

У табл. 3 для кожного значення *n* наведено дві колонки. Ліва колонка відповідає середній кількості значень коефіцієнтів поліному (*k*) для прийнятних ключів, розрахованих першим способом, а права – для ключів, розрахованих другим способом.

Таблиця 3

Результати порівняння кількості коефіцієнтів з різними значеннями для алгоритмів згідно [2] та алгоритму, розглянутому вище

K	*n*=512		*n*=1024		*n*=2048	
	Cnt1	Cnt2	Cnt1	Cnt2	Cnt1	Cnt2
0	51.02	52	143.37	144	404.48	404
±1	98.42	98	271.40	268	716.59	714
±2	90.21	90	224.24	224	496.50	496
±3	77.34	76	163.95	164	268.25	270
±4	62.00	62	106.80	108	113.15	114
±5	46.69	48	61.28	62	36.92	38
±6	33.18	34	30.85	32	9.81	10
±7	22.12	22	13.87	14	1.89	1
±8	13.93	14	5.64	6	0.33	1
±9	8.13	8	1.80	1	0.04	
±10	4.61	4	0.58	1		
±11	2.36	2	0.16			
±12	1.14	1	0.04			
±13	0.49	1	0.01			
±14	0.21					
±15	0.09					
±16	0.03					
±17	0.01					
	511.98	512	1023.99	1024	2047.96	2048

Загальна кількість коефіцієнтів для першого варіанту задається не цілими значеннями, тому що отримали середнє для усіх поліномів, які пройшли необхідні перевірки.

Результати порівняння показують, що для більшості значень кількість співпадає; для значень, для яких вона відрізняється, значення різниці незначне.

Визначимо простір ключів для другого способу формування коефіцієнтів поліному:

$$C=\frac{n!}{\prod_{i=0}^{18} Cnt2_i!}\cdot \tag{4}$$

Це практично не відрізняється від простору ключових даних для першого варіанту, про що свідчить практичне співпадіння даних в табл. 3.

Застосування другого варіанту замість першого дозволяє генерувати поліноми *f, g* без відбракування їх. Перший варіант передбачав відбракування не менше, ніж 90 % поліномів, а для n=2048 навіть більше, ніж 97 %.

Результати подальшого аналізу алгоритму генерації ключових даних будуть представлені у майбутніх роботах.

Список літератури:

1. Post-Quantum Cryptography. Round 3 Submissions. [Електронний ресурс]. Режим доступу: https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions.

2. Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU. [Електронний ресурс]. Режим доступу: https://falcon-sign.info/.

3. Donald E. Knuth The Art of Computer Programming. Seminumerical algorithms. Vol. 2 (3rd ed.). Boston: Addison–Wesley, 1998. 774p.

Надійшла до редколегії 05.05.2022

Відомості про авторів:

Качко Олена Григорівна – канд. техн. наук, Харківський національний університет радіоелектроніки, професор кафедри програмної інженерії, факультет комп'ютерних наук, начальник відділу програмування АТ «Інститут інформаційних технологій», Україна, e-mail: iit@iit.kharkov.ua, ORCID: https://orcid.org/0000-0001-9249-0497

Єсіна Марина Віталіївна – канд. техн. наук, Харківський національний університет імені В.Н. Каразіна, доцент кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; науковий співробітник-консультант АТ «ІІТ»; Україна; e-mail: rinayes20@gmail.com; ORCID: https://orcid.org/0000-0002-1252-7606

Кузнецова Катерина Олександрівна – студентка; Харківський національний університет імені В.Н. Каразіна; Україна; e-mail: kate7smith12@gmail.com