УДК 004.056.55

Опис та генерація ключової пари у алгоритмі ЕП Rainbow

Андрій Д'яченко[1], Ганна Малєєва[2]

[1] студент Харківського національного університету імені В. Н. Каразіна, майдан Свободи, 6, 61000, Харків, e-mail: andrey.090220@gmail.com
[2] менеджер офісу АТ "Інститут інформаційних технологій", вул. Бакуліна, 12, 61000, Харків, hanna.malieieva@nure.ua

У роботі наводиться опис представлення та генерації ключової пари для одного з перспективних кандидатів на рівні NIST США у конкурсі NIST PQC за напрямком електронних підписів алгоритму Rainbow. Даний алгоритм є кандидатом третього раунду відбору та можливим варіантом для побудування в Україні власних стандартів ЕП на базі математики багатовимірних квадратичних схем (MQ перетворень), яка використовується у даному алгоритмі. У рамках конкурсу розробники наводять декілька наборів параметрів для різних рівнів безпеки та декілька можливих реалізацій алгоритму (класична, CZ, стисла), проте, наведені опис та заміри продуктивності для описаного алгоритму стосуються тільки класичної схеми Rainbow (хоча заявлене підвищення продуктивності є справедливим й по відношенню до інших версій).

Ключові слова: електронний підпис; MQ-перетворення; постквантова криптографія; асиметричні криптоперетворення

Вступ. Проблема автентифікації та цілісності даних завжди була актуальною для людства у багатьох сферах розвитку. Упродовж останніх років гостро встала проблема збільшення рівня захищеності існуючих криптоалгоритмів на фоні розробки квантових комп'ютерів, потужність роботи яких значно більше навіть за існуючі суперкомп'ютери. Ураховуючи даний контекст, NIST США було об'явлено конкурс для визначення найперспективнішого криптоалгоритму за декількома основними для криптології напрямками, одним з яких є й електронний підпис. Багатообіцяючим напрямком у математиці для постквантового періоду вважаються багатовимірні квадратичні перетворення, на базі яких було розроблено алгоритм одного з кандидатів 3-го раунду конкурсу NIST PQC – Rainbow.

1. Математичні основи та основні параметри

Алгоритм ЕП Rainbow належить до багатовимірних схем з відкритим ключем, у яких відкритий ключ задається набором нелінійних багатовимірних поліномів над скінченим полем, тобто відкритий ключ такої системи – це система

багатовимірних квадратичних поліномів, схожа на приклад (1), показаний нижче, усі коефіцієнти та змінні якого походять з F_q – скінченого поля з q елементами.

$$\begin{aligned} p^{(1)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij}^{(1)} \cdot x_i x_j + \sum_{i=1}^{n} p_i^{(1)} \cdot x_i + p_0^{(1)} \\ p^{(2)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij}^{(2)} \cdot x_i x_j + \sum_{i=1}^{n} p_i^{(2)} \cdot x_i + p_0^{(2)} \\ &\vdots \\ p^{(m)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij}^{(m)} \cdot x_i x_j + \sum_{i=1}^{n} p_i^{(m)} \cdot x_i + p_0^{(m)} \end{aligned} . \quad (1)$$

Тобто сукупність загальновідомих поліномів

$$\mathrm{P}(x_1,\ldots,x_n) = \left(p^{(1)}(x_1,\ldots,x_n),\ldots,p^{(m)}(x_1,\ldots,x_n)\right), \quad (2)$$

математично являє собою відображення F_q^n до F_q^m. Операція верифікації підпису полягає в оцінюванні $\mathrm{P}(x_1,\ldots,x_n)$, тоді як процес генерації підпису відповідає інверсії зазначеного відображення, що є еквівалентним вирішенню проблеми MQ.

Для стандартної конструкції багатовимірної криптосистеми з відкритим ключем вибирається система F з m квадратичних поліномів з n змінними, які можна легко інвертувати (центральне відображення). Після цього вибирається два афінні інвертивні відображення S і T, щоб приховати структуру центрального відображення F у відкритому ключі. Відкритим ключем криптосистеми є складене квадратичне відображення $\mathrm{P} = \mathrm{S} \circ \mathrm{F} \circ \mathrm{T}$, яке, як передбачається, важко інвертувати. Секретний ключ складається з S, F та T, і, отже, дозволяє інвертувати P. Відображення S і T використовуються для захисту відображення F, яке, як зазначалося вище, складається з $m = n - \upsilon_1$ багатовимірних квадратичних поліномів $f^{(\upsilon_1+1)},\ldots,f^{(n)}$ виду

$$f^{(k)}(\mathbf{x}) = \sum_{i,j\in V_\ell} \alpha_{ij}^{(k)} x_i x_j + \sum_{i\in V_\ell, j\in O_\ell} \beta_{ij}^{(k)} x_i x_j + \sum_{i\in V_\ell \cup O_\ell} \gamma_i^{(k)} x_i + \eta^{(k)}, \quad (3)$$

де $\ell \in \{1,\ldots,u\}$ – єдине ціле число, таке що $k \in O_\ell$.

Зауважимо, що в кожному поліномі $f^{(k)}$ при $k \in O_\ell$ немає квадратного члена $x_i x_j$, де i і j знаходяться в O_ℓ. Цей факт використаний авторами [1] для генерації підпису, через що такі поліноми отримали назву поліномів Oil-Vinegar [2].

Для реалізації схеми підпису важливою умовою є $m \le n$. Генерація підпису для документа d починається з використання геш-функції $\mathrm{H}:\{0,1\}^* \to \mathrm{F}^m$ для обчислення значення $\mathbf{w} = \mathrm{H}(d) \in \mathrm{F}^m$. Тоді обчислюємо $\mathbf{x} = \mathrm{S}^{-1}(\mathbf{h})$, $\mathbf{y} = \mathrm{F}^{-1}(\mathbf{x})$ і

$\mathbf{z} = \mathrm{T}^{-1}(\mathbf{y})$. Підпис документа d – це $\mathbf{z} \in \mathrm{F}^n$. Тут $\mathrm{F}^{-1}(\mathbf{x})$ означає пошук одного (з можливо багатьох) попередніх зображень $\mathbf{x}$ під центральним відображенням F. Оскільки $m \le n$, ми можемо бути впевнені, що таке попереднє зображення існує. Тому кожне повідомлення має підпис. Для верифікації підпису в свою чергу просто обчислюється $\mathbf{w}' = \mathrm{P}(\mathbf{z})$ і геш-значення $\mathbf{w} = \mathrm{H}(d) \in \mathrm{F}^m$ документа. Якщо виконується $\mathbf{w}' = \mathbf{w}$, підпис приймається, в іншому випадку – відхиляється. Схематично цей процес зображено на рис. 1.

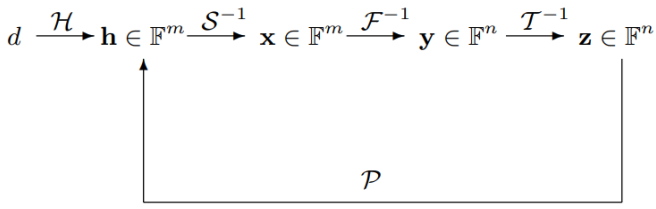


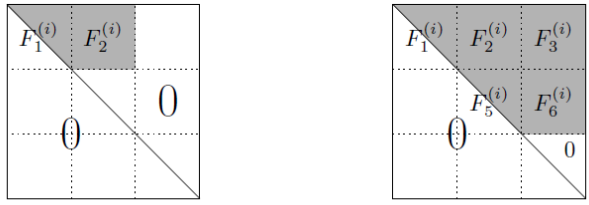
Рис.1. Процес генерації та верифікації підпису Rainbow

Згаданий вище параметр v_1 є одним з основних параметрів, разом з яким також є наступні змінні: кінцеве поле $\mathrm{F} = \mathrm{F}_q$ з елементами q; цілі числа $0 < v_1 < \ldots < v_u < v_{u+1} = n$; множина індексів $V_i = \{1, \ldots, v_i\}$, $O_i = \{v_i + 1, \ldots, v_{i+1}\}(i = 1, \ldots, u)$, де кожне $k \in \{v_1 + 1, \ldots, n\}$ міститься рівно в одному з наборів O_i $(v > u)$; маємо $|V_i| = v_i$ та множину $o_i := |O_i|(i = 1, \ldots, u)$; згадану раніше кількість рівнянь $m = n - v_1$; кількість змінних n [3].

У наведеному прикладі змінними v та u є незбалансовані поліноми Oil-Vinegar або їх відповідні коефіцієнти, кількість яких залежить від інших параметрів (n та m, відповідно).

2. Внесені пропозиції щодо покращення продуктивності

Для прискорення генерації ключової пари та відповідного підвищення швидкості роботи алгоритму, було прийнято рішення щодо введення проміжного відображення $\mathrm{Q} = \mathrm{F} \circ \mathrm{T}$. Відображення F?, Q і P можна представити матрицями, як показано на рис. 2.



$v_1 + 1 \le i \le v_2$ $\quad$ $v_2 + 1 \le i \le n$

Рис. 2. Матриці $F^{(i)}(i = v_1 + 1, \ldots, n)$

Після того, як було обрано початкове 256-бітне значення та випадково згенеровано матриці та ненульові коефіцієнти відповідних центральних відображень, починається обчислення матриці $\mathrm{Q}^{(i)} = T^T \square F^{(i)} \square T$. Після обчислення усіх частин матриць $\mathrm{Q}^{(i)}$, обчислюється структура MQ [4], де $\frac{n \cdot (n+1)}{2}$ ненульових елементів матриці $\mathrm{Q}^{(i)}$ вставляються в $(i - \upsilon_1)$-й рядок MQ таким чином:

- Перші $\frac{\upsilon_1 \cdot (\upsilon_1 + 1)}{2} + \upsilon_1 o_1$ позиції $(i - \upsilon_1)$-го рядка заповнені елементами матриці $\mathrm{Q}_1^{(i)} \square \mathrm{Q}_2^{(i)}$ (зліва направо та зверху вниз).
- Наступні $\upsilon_1 \cdot o_2$ позиції заповнені елементами $\mathrm{Q}_3^{(i)}$ (так само зліва направо та зверху вниз).
- Наступні $\frac{o_1 \cdot (o_1 + 1)}{2} + o_1 o_2$ позицій заповнені елементами $\mathrm{Q}_5^{(i)} \square \mathrm{Q}_6^{(i)}$ (зліва направо та зверху вниз).
- Останні $\frac{o_2 \cdot (o_2 + 1)}{2} + o_1 o_2$ позиції рядка заповнені елементами матриці $\mathrm{Q}_9^{(i)}$.

Останньою обчислюється матриця, що містить відкритий ключ – MP. Обидві матриці мають структуру, що складається з декількох шарів, які схематично зображено на рис. 3.

$$MP = \begin{array}{|c|}\hline MP_1 \\ \hline MP_2 \\ \hline \end{array} \qquad MQ = \begin{array}{|c|}\hline MQ_1 \\ \hline MQ_2 \\ \hline \end{array}$$

Рис.3. Матриці MQ та MP для класичної схеми підпису Rainbow

Наскільки таке впровадження є доцільним можна побачити у таблиці 1. Заміри продуктивності алгоритму виконувалися на мобільному комп'ютері, оснащеному процесором Intel(R) Core(TM) i7-9750H CPU.

Таблиця 1

Заміри продуктивності алгоритму після впровадження проміжної матриці Q

	До впровадження Q	Після впровадження Q
Ia	3,7	0,029
IIIc	67,09	0,0938
Vc	286,27	0,22

Висновки. Rainbow та багатовимірна математика загалом є досить перспективними напрямками у постквантовій криптології, що чудово демонструє конкурс NIST PQC. Сам алгоритм усе ще потребує певних досліджень, адже на даний момент точно можна зробити висновок щодо покращення продуктивності,

за рахунок «розвантаження» обчислювальних операцій та введення структур матриць певного типу, але питання щодо збереження показників криптостійкості після введення таких структур відкрите, адже такі структури передбачають заповнення їх полів нулями, що повинно негативно вплинути на показники безпеки. Евристика цього впровадження залишає відкритим для дослідження питання щодо появи нових вразливостей та ін.

Література

[1] *J. Ding, D. Schmidt*: Rainbow, a new multivariable polynomial signature scheme. ACNS 2005, LNCS vol. 3531, pp. 164 - 175. Springer, 2005.
[2] *A. Kipnis, J. Patarin, L. Goubin*: Unbalanced Oil and Vinegar schemes. EUROCRYPT 1999, LNCS vol. 1592, pp. 206-222. Springer, 1999.
[3] *Albrecht Petzoldt, Stanislav Bulygin, Johannes Buchmann*: Selecting Parameters for the Rainbow Signature Scheme – Extended Version. PQCrypto`10, pp. 21. 2010.
[4] *Rainbow Signature / Ding J., and other*. 2020. P. 16-22. [Electronic resource]. – Access mode: https://www.pqcrainbow.org/.

Description and generation of the key pair in the ES Rainbow algorithm

Andriy Diachenko, Hanna Malieieva

This paper describes the representation and generation of a key pair for one of the promising candidates at the NIST USA level in the NIST PQC competition for the direction of digital signatures of the Rainbow algorithm. This algorithm is a candidate for the third round of selection and a possible option for Ukraine to build its own DS standards based on the mathematics of multivariable quadratic schemes (MQ transformations), which is used in this algorithm. Within the competition, the developers give several sets of parameters for different security levels and several possible implementations of the algorithm (classical, CZ, compressed), but the given description and performance measurements, for the described algorithm, concern the classical Rainbow scheme (although the declared performance improvement is also fair in relation to other versions).

Отримано 26.02.21