УДК 003.026:004.056 **DOI:10.30837/rt.2022.2.209.09**

Є.Ю. КАПТЬОЛ

АНАЛІЗ СТАНУ ПОСТКВАНТОВОГО АЛГОРИТМУ ЕЛЕКТРОННОГО ПІДПИСУ RAINBOW ТА АТАК НА НЬОГО НА ПЕРІОД ЗАВЕРШЕННЯ ТРЕТЬОГО РАУНДУ NIST PQC

Вступ

Через поступове покращення існуючих та винайдення нових квантових комп'ютерів існує потреба в стандартизації постквантових електронних підписів. В межах конкурсу NIST PQC до третього раунду було відібрано три електронних підписи, що претендують на стійкість до класичного та квантового криптоаналізу та можливість їх застосування в постквантовий період. Згідно з [1, 2] до третього раунду в якості основних фіналістів увійшли такі електронні підписи: CRYSTALS-DILITHIUM, FALCON, Rainbow. Також окрім основних кандидатів було відібрано три альтернативних: Picnic, SPHINCS+, GeMSS. Так як Rainbow є одним з фіналістів, варто розглянути атаки на нього, зокрема ті, що використовують переваги квантового комп'ютера. Разом зі звичайним алгоритмом Rainbow було також представлено CZ-Rainbow та стислий алгоритм Rainbow. Також слід зазначити, що в ході доповіді в рамках NIST PQC щодо особливостей прийняття перших постквантових стандартів, що відбулася 8 – 11 березня 2022 р., було згадано про деяке занепокоєння щодо безпеки обох мультиваріативних підписів (Rainbow як основний кандидат та GeMSS як альтернативний).

1. Сутність алгоритму Rainbow

Згідно з [3], генерація та верифікація підпису за алгоритмом Rainbow мають вигляд, наведений далі.

Генерація підпису. Маємо документ d, що необхідно підписати, використовується хеш-функція $\mathrm{H}:\{0,1\}\to\mathrm{F}^m$ для обчислення хеш-значення $\mathrm{h}=\mathrm{H}(d)\in\mathrm{F}^m$. Далі підпис $\mathrm{z}\in\mathrm{F}^n$ документа d обчислюється наступними послідовними кроками: обчислюється $\mathrm{x}=\mathrm{S}^{-1}(\mathrm{h})\in\mathrm{F}^m$; обчислюється прообраз $\mathrm{y}\in\mathrm{F}^n$ від x над центральною мапою F; обчислюється підпис $\mathrm{z}\in\mathrm{F}^n$ з $\mathrm{z}=\mathrm{T}^{-1}(\mathrm{y})$.

Верифікація підпису. Маємо документ d та підпис $\mathrm{z}\in\mathrm{F}^n$, справжність підпису перевіряється наступними кроками: використовується хеш-функція H для обчислення хеш-значення $\mathrm{h}=\mathrm{H}(d)\in\mathrm{F}^m$; обчислюється $\mathrm{h}'=\mathrm{P}(\mathrm{z})\in\mathrm{F}^m$. Якщо виконується рівність $\mathrm{h}'=\mathrm{h}$, підпис z приймається, в іншому випадку він відхиляється.

2. Набори параметрів Rainbow

Спочатку потрібно розглянути параметри електронного підпису. У зв'язку з тим, що на конкурс NIST PQC було представлено три варіанти схеми електронного підпису та кожен з них має свої набори параметрів для різних категорій безпеки, їх варто розглядати окремо. Згідно з [3] було представлено такі варіанти схеми електронного підпису Rainbow: звичайний алгоритм Rainbow, CZ-Rainbow та стислий алгоритм Rainbow.

Набори параметрів для зазначених варіантів електронного підпису відповідають різним категоріям безпеки NIST. Так, кожен варіант Rainbow має три набори параметрів: I, III та V. Відповідність наборів параметрів категоріям безпеки NIST наступна [3]: набір параметрів I відповідає категоріям безпеки I та II, набір параметрів III відповідає категоріям безпеки III та IV, набір параметрів V відповідає категорії безпеки V.

Табл. 1 – 3 містять набори параметрів для звичайного алгоритму Rainbow, CZ-Rainbow та стислого алгоритму Rainbow відповідно [3] (так ми маємо параметри (F, v_1, o_1, o_2), розміри відкритого та закритого ключів, розмір гешу та розмір підпису).

Таблиця 1

Розміри ключів та підписів для звичайного алгоритму Rainbow

Набір параметрів	Параметри (F, v_1, o_1, o_2)	Відкритий ключ (кВ)	Закритий ключ (кВ)	Розмір гешу (біт)	Розмір підпису (біт)
I	(GF(16), 36, 32, 32)	157.8	101.2	256	528
III	(GF(256), 68, 32, 36)	861.4	611.3	576	1,312
V	(GF(256), 96,36, 64)	1,885.4	1,375.7	768	1,696

Таблиця 2

Розміри ключів та підписів для CZ-Rainbow

Набір параметрів	Параметри (F, v_1, o_1, o_2)	Відкритий ключ (кВ)	Закритий ключ (кВ)	Розмір гешу (біт)	Розмір підпису (біт)
I	(GF(16), 36, 32, 32)	58.8	101.2	256	528
III	(GF(256), 68, 32, 48)	258.4	611.3	576	1,312
V	(GF(256), 96,36, 64)	523.6	1,375.7	768	1,696

Таблиця 3

Розміри ключів та підписів для стислого алгоритму Rainbow

Набір параметрів	Параметри (F, v_1, o_1, o_2)	Відкритий ключ (кВ)	Закритий ключ (кВ)	Розмір гешу (біт)	Розмір підпису (біт)
I	(GF(16), 36, 32, 32)	58.8	0.06	256	528
III	(GF(256), 68, 32, 48)	258.4	0.06	576	1,312
V	(GF(256), 92,36, 64)	523.6	0.06	768	1,696

3. Атаки на Rainbow

Як зазначено в [3], всі відомі атаки на Rainbow на даний момент є, в основному, класичними атаками, деякі з котрих можуть бути прискореними за рахунок використання алгоритму Гровера. До атак на Rainbow можна віднести [3]: атаки знаходження колізій на геш-функції, прямі атаки, атаки MinRank, атаки HighRank, атаки "Rainbow-Band-Separation" (RBS), атаки UOV, атаки на диференціальне поле та квантові атаки «грубої сили».

Серед наведених атак передбачається використання квантових методів (а саме, алгоритму Гровера) в наступних атаках: прямі атаки, атаки HighRank, атаки UOV та квантові атаки «грубої сили». Розглянемо атаки, що можуть використовувати квантові методи.

Прямі атаки. Згідно з [3] найбільш прямолінійною атакою на Rainbow як на мультиваріативну схему є пряма алгебраїчна атака, що розглядає рівняння $\mathrm{P}(\mathbf{z}) = \mathbf{h}$ як приклад задачі MQ. Через те, що відкрита система Rainbow є невизначеною системою з $n \approx 1.5 \cdot m$, найефективнішим вважається отримання визначеної системи, що має рівно одне рішення, шляхом фіксації $n - m$ змінних перед застосуванням такого алгоритму, як алгоритм обчислення базисів Гробнера (F_4) [4]. Для досягнення кращих результатів використовують «гібридний підхід» (відгадують додаткові змінні перед вирішенням системи), як в [5]. В [3] складність вирішення такої системи оцінюється як

$$\mathrm{Complexity}_{\mathrm{direct;\ classical}} = \min_k \left(q^k \cdot 3 \cdot \binom{m-k+d_{\mathrm{reg}}}{d_{\mathrm{reg}}} \cdot \binom{m-k}{2} \right)$$

множень у полі, де d_{reg} – це так звана ступінь регулярності системи.

Застосування квантового комп'ютера дозволяє використати алгоритм Гровера для прискорення вгадування додаткових змінних при використанні «гібридного підходу». В [3] складність такої атаки оцінюється як

$$\mathrm{Complexity}_{\mathrm{direct;\ quantum}} = \min_k \left(q^{k/2} \cdot 3 \cdot \binom{m-k+d_{\mathrm{reg}}}{d_{\mathrm{reg}}}^2 \cdot \binom{m-k}{2} \right)$$

множень у полі.

Атаки HighRank. Згідно з [6] метою атаки HighRank є виявлення змінних, що з'являються найменшу кількість разів у центральних поліномах (вони відповідають Oil-змінним останнього рівня Rainbow).

Складність цієї атаки в [3] оцінюється як

$$\text{Complexity}_{\text{HighRank; classical}} = q^{O_u} \cdot \frac{n^3}{6}.$$

Застосування квантового комп'ютера дозволяє використати алгоритм Гровера для прискорення пошуку. У такому випадку складність атаки становить

$$\text{Complexity}_{\text{HighRank; quantum}} = q^{O_u/2} \cdot \frac{n^3}{6}$$

множень у полі.

Атаки UOV. Оскільки Rainbow можна розглядати як продовження добре відомої схеми підписів Oil and Vinegar [7], її можна атакувати, використовуючи всі відомі атаки UOV. Наприклад, атака UOV «Oil Subspace» Кіпніса та Шаміра [8].

Можна розглядати Rainbow як екземпляр UOV з $\upsilon = \upsilon_1 + o_1$ та $o = o_2$. Метою цієї атаки є пошук попереднього зображення так званого Oil підпростору O афінного перетворення T, де $\mathrm{O} = \left\{ \mathrm{x} \in \mathrm{F}^n : x_1 = \cdots = x_\upsilon = 0 \right\}$. Знаходження цього простору дозволяє відокремити Oil від змінних Vinegar та відновити закритий ключ.

Складність цієї атаки оцінюється як

$$\text{Complexity}_{\text{UOV-Attack; classical}} = q^{n-2_{o_2}-1} \cdot o_2^4$$

множень у полі.

Застосування квантового комп'ютера та алгоритма Гровера зменшує складність до

$$\text{Complexity}_{\text{UOV-Attack; classical}} = q^{\frac{n-2_{o_2}-1}{2}} \cdot o_2^4$$

множень у полі [3].

Квантові атаки «грубої сили». За наявності квантових комп'ютерів атаку грубої сили проти схеми можна різко прискорити за допомогою алгоритму Гровера.

У роботі [9] було показано, що можливо розв'язати систему $m-1$ двійкових квадратних рівнянь з $n-1$ двійкових змінних, використовуючи $m+n+2$ кубітів та обчислюючи схему з $2^{n/2} \cdot \left(2m\left(n^2+2n\right)+1\right)$ квантових логічних елементів.

Також було наведено інший варіант, який вирішує систему, використовуючи менше кубітів, але з більшою схемою, що має приблизно в два рази більше квантових логічних елементів. Наприклад, коли $n = m$, то може бути вирішена двійкова система з m рівнянь у m змінних, використовуючи $2^{m/2} \cdot 2 \cdot m^3$ бітових операцій. Загалом, завдяки алгоритму Гровера очікується квадратичне прискорення атаки грубої сили.

У табл. 4 – 6 наведено складність різних атак для наборів параметрів I, III та V відповідно [3]. У першому рядку наведено кількість необхідних для здійснення атаки класичних логічних елементів, а у другому – кількість необхідних для здійснення атаки квантових логічних елементів.

Таблиця 4

Складність атак на підпис з набором параметрів I

Набір параметрів	Параметри (F, v_1, o_1, o_2)	$\log_2$ (#гейтів)		
		прямі	HighRank	UOV
I	(GF(16), 36, 32, 32)	164	150	157
		122	86	91

Таблиця 5

Складність атак на підпис з набором параметрів III

Набір параметрів	Параметри (F, v_1, o_1, o_2)	$\log_2$ (#гейтів)		
		прямі	HighRank	UOV
III	(GF(256), 68, 32, 48)	234	410	437
		200	218	233

Таблиця 6

Складність атак на підпис з набором параметрів V

Набір параметрів	Параметри (F, v_1, o_1, o_2)	$\log_2$ (#гейтів)		
		прямі	HighRank	UOV
V	(GF(256), 96, 36, 64)	285	539	567
		243	283	299

4. Сумніви в безпеці мультиваріативних схем

В ході доповіді в рамках NIST PQC щодо особливостей прийняття перших постквантових стандартів було згадано про занепокоєння щодо безпеки обох мультиваріативних підписів (Rainbow як основний кандидат та GeMSS як альтернативний). Зокрема було зроблено посилання на атаку, котра повертає ключ для набору I параметрів Rainbow в середньому за 53 години обчислень «на стандартному ноутбуці». Разом із цим було зазначено, що це слугує нагадуванням того, що не потрібно поспішати додавати схеми-кандидати до застосунків-продуктів до завершення процесу прийняття стандартів.

Зокрема під «стандартним ноутбуком» в [11] малася на увазі машина з 8-ядровим CPU n Intel i9-10885H з тактовою частотою 2,5 GHz. Також було згадано, що вирішення системи (котре потрібно повторити приблизно 15 разів) потребує 1.1 GB пам'яті.

Також слід зазначити, що такі параметри часу атака досягає з варіантом параметрів з другого раунду NIST PQC, тоді як параметри третього раунду потребують більших ресурсів (згідно до розрахунків авторів атаки на факторіал 2^8).

В [11] було наведено дві атаки на підпис (одна є модифікацією іншої), які вказують на недостатність визначених наборів параметрів: проста атака та, як її більш ефективна версія, комбінована з прямокутною атакою MinRank.

Як наведено в табл. 7, проста атака виграє в інших атак не у всіх випадках, в той час як комбінована показує кращі результати для всіх наборів параметрів. Варто зауважити, що для набору параметрів I проводиться атака відновлення ключа, в той час як для інших – атаки підробки.

Таблиця 7

Порівняння складності запропонованих в [11] атак з аналогічними відомими атаками на Rainbow

Набір параметрів	Проста атака ($\log_2$ (#гейтів))	Комбінована атака ($\log_2$ (#гейтів))	Інші відомі атаки ($\log_2$ (#гейтів))
I	69	99	127
III	160	157	177
V	257	206	226

Згідно з [11] проста атака спрямована на те, щоб зменшити рівень безпеки Rainbow до рівня меншого UOV, з $m' = m - o_2$ та $n' = n - o_2$ змінних. Це стає можливим завдяки усуненню другого шару Rainbow шляхом знаходження вектора в O_2 (при $o_2 \in O_2$ та $O_2 \subset \mathrm{F}_q^n$), що можливо ціною

$$3\binom{n-m-1+D}{D}^2\binom{n-m+1}{2}$$

множень в полі за умови непарного q та ціною

$$3\binom{n-m-2+D}{D}^2\binom{n-m}{2}$$

множень в полі за умови парного q.

Комбінована з прямокутною атакою MinRank атака в свою чергу застосовує просту атаку для того, щоб зменшити кількість матриць для вирішення задачі MinRank від звичайних для оригінальної прямокутної атаки MinRank $n-o_2+1$ до $n-m$ матриць. Хоча також слід зауважити, що це призводить до необхідності повтору атаки в середньому q разів (поки $\ker(D_x)\cap O_2 \neq \{0\}$, де $D_x : \mathrm{F}_q^n \to \mathrm{F}_q^m : y \mapsto \mathrm{P}'(x,y)$).

З варіантів уникнення можливості цих атак можна виділити збільшення параметрів, що призведе до збільшення розмірів ключа та підпису. Якщо брати до уваги [10] та інші джерела щодо NIST PQC, можна помітити, що розміри ключа Rainbow і так вважаються великими (хоча й альтернатива у вигляді GeMSS не сильно відрізняється за цим параметром).

Висновки

Конкурс NIST PQC підходить до моменту демонстрації результатів шляхом формування проектів стандартів для постквантового періоду. З врахуванням цього та трьох раундів цікавим є те, що з мультиваріативних електронних підписів залишилися лише Rainbow в якості основного кандидату та GeMSS – в якості альтернативного. Логічним було б припустити, що в них найменша вразливість до криптоаналізу з усіх поданих мультиваріативних, але це не означає, що в них немає проблем та не може бути виявлено нових можливостей для проведення криптоаналізу.

З попередньо відомих атак можна було зробити висновок, що Rainbow певною мірою готовий до постквантового періоду. Особливо цікавим було те, що атаки були класичними та могли використовувати квантовий комп'ютер для пришвидшення певних кроків (окрім цілком квантової атаки «грубої сили»).

Проте також слід зауважити, що пришвидшення атак за допомогою квантового комп'ютера є нерівномірним. Через це для різних наборів параметрів оптимальними є різні атаки. Так, наприклад для набору параметрів I найкращою атакою з використанням квантового комп'ютера була атака HighRank, а для наборів параметрів III та V – пряма атака.

Також важливим моментом є те, що повністю квантовою атакою з наведених є лише квантова атака «грубої сили». Інші атаки використовують квантовий комп'ютер лише для виконання певного кроку атаки.

Ситуація змінилася з появою атаки, що здатна здійснити криптоаналіз електронного підпису Rainbow «за допомогою ноутбука на вихідних» для одного з наборів параметрів. Про це навіть було згадано в ході доповіді в рамках NIST PQC щодо особливостей прийняття перших постквантових стандартів, що відбулася 8 – 11 березня 2022 р.

Але згадано про це було доволі коротко та у поєднанні з нагадуванням про те, що не варто вбудовувати схеми-кандидати до продуктів заздалегідь до завершення розробки стандартів.

Також не було згадано про те, що такі оцінки криптоаналізу Rainbow (53 години обчислень на машині з 8-ядровим CPU n Intel i9-10885H з тактовою частотою 2.5 GHz) дійсні лише для набору параметрів I з тих наборів параметрів, що було надано на другий раунд NIST PQC. Для набору параметрів, поданого для третього раунду, ситуація виглядає дещо кращою (приблизно на 2^8, за словами авторів атаки). Цієї атаки можна уникнути збільшенням параметрів Rainbow. Хоча просто збільшення параметрів призведе до збільшення ключа та підписа, що не є цілком вірним виходом через те, що розмір ключа і так вважаєтьтся великим та подальше його збільшення робить застосування Rainbow менш вигідним.

Список літератури:

1. Post-Quantum Cryptography PQC. Round 3 Submissions. NIST Computer Security Resource Center (CSRC). URL: https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions (last accessed on 16.06.2022).
2. PQC Standardization Process: Third Round Candidate Announcement. NIST Computer Security Resource Center (CSRC). July 22, 2020. URL: https://csrc.nist.gov/News/2020/pqc-third-round-candidate-announcement (last accessed on 15.06.2022).
3. Jintai Ding. Rainbow – Algorithm Specification and Documentation. The 3d round Proposal. Department of Mathematical Sciences, University of Cincinnati.
4. J.-C. Faugere. A new efficient algorithm for computing Grobner Bases (F4). Journal of Pure and Applied Algebra, 139 (1999) 61-88. DOI: https://doi.org/10.1016/S0022-4049(99)00005-5 (last accessed on 13.06.2022).
5. L. Bettale, J.-C. Faugere, L. Perret. Hybrid approach for solving multivariate systems over finite fields. Journal of Mathematical Cryptology, 3, pp. 177-197, 2009.
6. D. Coppersmith, J. Stern, S. Vaudenay. Attacks on the birational signature scheme. CRYPTO 1994, pp. 435-443. Springer, 1994.
7. A. Kipnis, J. Patarin, L. Goubin. Unbalanced Oil and Vinegar schemes. EUROCRYPT 1999, pp. 206-222. Springer, 1999.
8. A. Kipnis, A. Shamir. Cryptanalysis of the Oil and Vinegar signature scheme. CRYPTO 1998, pp. 257-266. Springer,1998.
9. P. Schwable, B. Westerbaan. Solving Binary MQ with Grover's Algorithm. SPACE 2016, pp. 303-322. Springer 2016.
10. Post-Quantum Cryptography PQC. The Beginning of the End: The First NIST PQC Standards. NIST Computer Security Resource Center (CSRC). URL: https://csrc.nist.gov/Presentations/2022/the-beginning-of-the-end-the-first-nist-pqc-standa (last accessed on 13.06.2022).
11. W. Beullens. Breaking Rainbow Takes a weekend on a Laptop. Cryptology ePrint Archive 2022/214. URL: https://eprint.iacr.org/2022/214 (last accessed on 17.06.2022).

Надійшла до редколегії 11.05.2022

Відомості про автора:

Каптьол Євгеній Юрійович – аспірант кафедри безпеки інформаційних систем і технологій; Харківський національний університет імені В. Н. Каразіна, , Україна; email: kaptevg@gmail.com