УДК 003.026:004.056 **DOI:10.30837/rt.2022.2.209.05**

Д.В. ГАРМАШ

АЛГОРИТМ RAINBOW ТА ЙОГО ЗДАТНІСТЬ ПРОТИДІЯТИ АТАКАМ RBS ТА СТОРОННІМИ КАНАЛАМИ

Вступ

Багатовимірні квадратичні схеми є перспективним рішенням для потреби квантових систем, стійких до атак від квантового комп'ютера. Однак оскільки цей клас відносно молодий і багато схем цього класу були порушені в минулому, існує дуже мало їх реалізацій, особливо на вбудованих мікроконтролерах. Щоб оцінити, чи можуть ці схеми колись замінити чинні стандарти, необхідно знати, наскільки ефективно їх можна впровадити на різних платформах. У процесі цієї роботи дано теоретичне введення до багатовимірних квадратичних схем. Потім впроваджуються схеми, які певний час витримували атаки: Unbalanced Oil and Vinegar (UOV), Rainbow та enTTS. Особлива увага приділяється атакам на алгоритм та його здатність їм протидіяти.

Атака RAINBOW-BAND-SEPARATION (RBS)

Атака Rainbow-Band-Separation відновлює секретний ключ Rainbow, розв'язуючи певні системи квадратичних рівнянь, а його складність оцінюється за відомим показником, який називається ступенем регулярності. Однак, як правило, ступінь регулярності більша, ніж ступінь розв'язання в експериментах, і точної оцінки отримати неможливо. Попередні методи оцінки [1, 4] для складності атаки RBS використовують ступінь регулярності як її показник за припущенням, що система квадратичних рівнянь, розв'язана в атаці, є напіврегулярною. Для напіврегулярної системи ступінь регулярності задається як ступінь D_{reg} першого члена, коефіцієнт якого непозитивний у ряді потужностей

$$\frac{(1-t^2)^m}{(1-t)^n}, \tag{1}$$

де m і n – числа рівнянь і змінних відповідно. Оскільки загальноприйнята квадратична система, що вирішується в прямій атаці, часто є напіврегулярною, то при оцінці складності прямої атаки використовується ступінь регулярності [1].

У роботі [5] запропоновано новий показник складності атаки Rainbow-Band-Separation за допомогою алгоритму F_4, який дає більш точну оцінку порівняно з показником, що використовує ступінь регулярності. Цей показник виводиться двома змінними рядами потужності

$$\frac{\prod_{i=1}^{m}(1-t_1^{d_{i1}}t_2^{d_{i2}})}{(1-t_1)^{n_1}(1-t_2)^{n_2}}, \tag{2}$$

що збігається з однозмінним рядом потужностей при $t_1=t_2$, виводячи ступінь регулярності. Крім того, показано залежність між атакою Rainbow-Band-Separation за допомогою гібридного підходу та атакою HighRank. Розглядаючи це відношення та показник, ми отримали нову оцінку складності для атаки Rainbow-Band-Separation. Отже, завдяки цьому, мож на зрозуміти точну безпеку Rainbow від атаки Rainbow-Band-Separation за допомогою алго ритму F_4.

Опис атаки RBS на схему підпису RAINBOW

Нехай m і n – натуральні числа. Позначимо через F кінцеве поле порядку q. Елемент $(f_1, ..., f_m)$ F $[x_1, ..., x_n]^m$ називається поліноміальною системою і дає відображення $F^n \to F^m$ на $a \to (f_1(a),...,f_m(a))$, яке називають поліноміальним відображенням (картою).

Багатовимірна схема підпису відкритого ключа складається з наступних трьох алгоритмів.

Генерація ключів: будуються дві обернені лінійні карти $S:F^n \to F^n$ і $T:F^m \to F^m$ випадковим чином і легко обернена квадратична карта $F: F^n \to F^m$, яку називають центральною картою, а потім обчислюється $P:=T \circ F \circ S$. Відкритий ключ подається у вигляді P. Кортеж (T, F, S) – секретний ключ.

Генерація підписів: для повідомлення $b \in F^m$ обчислюємо $b'=T^{-1}(b)$. Далі ми можемо обчислити елемент a' з $F^{-1}(\{b'\})$, оскільки F легко обернений. Отже, ми отримуємо підпис

$$a=S^{-1}(a') \in F^n.$$

Перевірка: перевіряється, чи $P(a)=b$ має місце. Для натуральних чисел v, o_1 і o_2, нехай $x=\{x_1, ..., x_v\}$, $y=\{y_1, ..., y_{o1}\}$ і $z=\{z_1, ..., z_{o2}\}$ будуть трьома змінними множинами і $n=v+o_1+o_2$, і $m=o_1+o_2$. Центральна карта $F=(f_1, ..., f_m) \in F[x, y, z]^m$ Rainbow

$$\begin{cases} f_1 = g^{(1)}(\mathbf{x}) + \sum_{i=1}^{o_1} l_i^{(1)}(\mathbf{x}) y_i, \\ \quad \vdots \\ f_{o_1} = g^{(o_1)}(\mathbf{x}) + \sum_{i=1}^{o_1} l_i^{(o_1)}(\mathbf{x}) y_i, \\ f_{o_1+1} = g^{(o_1+1)}(\mathbf{x}, \mathbf{y}) + \sum_{i=1}^{o_2} l_i^{(o_1+1)}(\mathbf{x}, \mathbf{y}) z_i, \\ \quad \vdots \\ f_{o_1+o_2} = g^{(o_1+o_2)}(\mathbf{x}, \mathbf{y}) + \sum_{i=1}^{o_2} l_i^{(o_1+o_2)}(\mathbf{x}, \mathbf{y}) z_i, \end{cases} \tag{3}$$

де $g^{(j)}$ та $l^{(j)}_i$ – випадковим чином обрані квадратичні многочлени та лінійні многочлени відповідно. Тоді за алгоритмом генерації підписів, наведеним вище, ми можемо легко обчислити елемент a' у попередньому зображенні будь-якого елемента $b'=(b'_1, ..., b'_{o1+o2})$ у F^m під F наступним чином.

1. Випадково обрати $a_v{}' = (a_1', ..., a_v')$ як x.
2. Вирішити систему лінійних рівнянь

$$f_1(\mathbf{a}'_v, \mathbf{y}) = b'_1, \ldots, f_{o_1}(\mathbf{a}'_v, \mathbf{y}) = b'_{o_1}.$$

Нехай $\mathbf{a}'_{o_1} = (a'_{v+1}, \ldots, a'_{v+o_1})$ є одним із її рішень, якщо воно існує. В іншому випадку повернутись до кроку 1.

3. Вирішити систему лінійних рівнянь

$$f_{o_1+1}(\mathbf{a}'_v, \mathbf{a}'_{o_1}, \mathbf{z}) = b'_{o_1+1}, \ldots, f_{o_1+o_2}(\mathbf{a}'_v, \mathbf{a}'_{o_1}, \mathbf{z}) = b'_{o_1+o_2}.$$

Нехай $\mathbf{a}'_{o_2} = (a'_{v+o_1+1}, \ldots, a'_{v+o_1+o_2})$ є одним із її рішень, якщо воно існує. В іншому випадку повернутись до кроку 1.

4. Отримати елемент $\mathbf{a}' = (a'_1, \ldots, a'_{v+o_1+o_2})$ у попередньому зображенні b'.

Нехай (v, o_1, o_2) – набір параметрів Rainbow, покладемо $n=v+o_1+o_2$ і $m=o_1+o_2$. Для відкритого ключа Rainbow $P=(p_1, ..., p_m)$ атака RBS відновлює свій секретний ключ (T, F, S) наступним чином. За визначенням (3) центральної карти $F=(f_1, ..., f_m)$ кожна матриця, відповідна f і має такий вигляд:

$$M_{f_i} = \begin{cases} \begin{pmatrix} *_{v\times v} & *_{v\times o_1} & 0_{v\times o_2} \\ *_{o_1\times v} & 0_{o_1\times o_1} & 0_{o_1\times o_2} \\ 0_{o_2\times v} & 0_{o_2\times o_1} & 0_{o_2\times o_2} \end{pmatrix} \text{ if } 1 \le i \le o_1, \\ \begin{pmatrix} *_{v\times v} & *_{v\times o_1} & *_{v\times o_2} \\ *_{o_1\times v} & *_{o_1\times o_1} & *_{o_1\times o_2} \\ *_{o_2\times v} & *_{o_2\times o_1} & 0_{o_2\times o_2} \end{pmatrix} \text{ if } o_1+1 \le i \le o_1+o_2. \end{cases} \tag{4}$$

Тут $*_{k\times l}$ означають k на l матриці над F. Аналогічно, матриці, відповідні S і T, можна записати наступним чином.

Матриці $M_{p1}, ..., M_{pm}$, що відповідають відкритим поліномам $p_1, ..., p_m$, задаються як

$$(M_{p_1}, \ldots, M_{p_m}) = (M_S M_{f_1}{}^t M_S, \ldots, M_S M_{f_m}{}^t M_S) M_T. \tag{5}$$

Існує вектор m на 1 t=(1,0 ...,0, λ_{v+o1+1}, ..., $\lambda_{v+o1+o2}$) такий, що $M_T \cdot {}^t t = {}^t(1,0, ..., 0)$. Потім, помноживши рівняння (5) на ${}^t t$, отримаємо

$$M_{p_1} + \sum_{i=1}^{o_2} \lambda_{v+o_1+i} M_{p_{o_1+i}} = M_S M_{f_1}{}^t M_S, \quad (6)$$

де e_k – це n на 1 вектор (0;...;0;1;0;...;0). Тут вилучаємо випадок $k=n$, оскільки рівняння (6) для $k=n$ випливає з рівняння (5).

Оскільки s = (λ_1, ..., λ_{v+o1}, 0, ..., 0,1), зрозуміло, що рівняння (5) і (7) є $n+m-1$ квадратичними рівняннями в n змінних λ_1,...,λ_n і будуються з відкритого ключа p_1,...,p_m. Вирішивши ці квадратичні системи, зловмисник може відновити частину секретного ключа S і T,а саме – s і t. Атака RBS може відновити S і T, повторюючи подібні обговорення, як описано вище (детальніше див. [2]).

Оскільки складність розв'язання квадратичної системи домінує в одній з атак RBS, достатньо оновити лише систему. Квадратична система, що складається з рівнянь (6) та (7), називається домінуючою системою RBS.

З досліджень [5] можна зробити висновок, що домінуюча система RBS є нерегулярною та дворівневою.

Здатність алгоритму RAINBOW протидіяти атаці сторонніми каналами

Криптографічні системи повинні бути захищені від широкого кола атак, включаючи атаки сторонніми каналами. Атака сторонніми каналами належить до фізичної атаки, яка являє собою будь-яку атаку, засновану на інформації, отриманій в результаті фізичної реалізації криптографічних систем, а не на грубій силі чи теоретичних недоліках криптографічних алгоритмів. Основним принципом атаки бічного каналу є те, що інформація бічного каналу, така як споживання енергії, електромагнітні витоки, інформація про синхронізацію або навіть звук, може забезпечити додаткові джерела інформації про секрети в криптографічних системах, наприклад криптографічні ключі, часткова інформація про стан, повна або часткові звичайні тексти, які можна використовувати для розбиття криптографічних систем. Загальні класи атаки бічних каналів включають аналіз синхронізації, аналіз потужності, електромагнітний аналіз, аналіз несправностей, акустичний криптоаналіз, аналіз залишків даних та атаки аналізу молоткових рядів [7].

Атаки аналізу несправностей мають на меті маніпулювати екологічними умовами криптографічних систем, таких як напруга, годинник, температура, випромінювання, світло і вихровий струм, щоб генерувати несправності під час секретних обчислень, наприклад множення та інверсії в кінцевому полі, і спостерігати за пов'язаною поведінкою, яка може допомогти криптоаналітику зламати криптографічні системи. Атаки аналізу несправностей можна спроєктувати, просто підсвітивши транзистор лазерним променем, що змушує деякі біти приймати неправильні значення. Ідея використання несправності, індукованої під час секретного обчислення, для вгадування секретного ключа практично спостерігалася в реалізаціях RSA, що використовують китайську теорему про залишки [7].

Атака аналізу потужності може надати детальну інформацію, спостерігаючи за енергоспоживанням криптографічних систем, що приблизно поділяється на простий аналіз потужності (SPA) та аналіз диференціальної потужності (DPA). У сімействі атак аналізу потужності DPA представляє особливий інтерес і є статистичним тестом, який вивчає велику кількість сигналів енергоспоживання для отримання секретних ключів.

Можна виділити наступні атаки:

- диференціального аналізу потужності на SFLASH;
- на секретні ключі від модуля SHA-1 схем SFLASH;.
- стороннього каналу на enTTS, яка використовує диференціальний аналіз потужності та аналіз несправностей для атаки двох афінних перетворень та центральної трансформації карти. Цей метод показує, що можна отримати всі секретні ключі enTTS.

Оскільки конструкція Rainbow включає два афінні перетворення та перетворення центральної карти, такі методи мають потенціал для отримання її секретних ключів. Таким чином, обговорюється захист від можливої атаки бічного каналу для Rainbow, а контрзаходи описані нижче:

- Нехай це повідомлення і кожен елемент у полягає в $GF((2^4)^2)$;
- Береться випадковий вектор $y'(y_0', y_1', ..., y_{25}')$, кожен елемент якого полягає в $GF((2^4)^2)$;
- Обчислюється $y'' = y' + y$;
- Обчислюється $\bar{y}' = Ay' + b$ та $\bar{y}'' = Ay''$, де A – матриця 26x26, b – вектор розміру 26;
- Обчислюється $\bar{y} = \bar{y}' + \bar{y}''$, що еквівалентно $\bar{y} = Ay + b$;
- Розраховано перше афінне перетворення; тоді ми беремо випадкові байти для Vinegar-змінних;
- Двічі перевіряються випадкові байти для захисту від атак аналізу несправностей;
- Обчислюються багатовимірні поліноміальні оцінки та розв'язування систем лінійних рівнянь до завершення перетворення центральної карти;
- $\bar{x}(\bar{x_0}, \bar{x_1}, ..., \bar{x_{42}})$ – це результат трансформації центральної карти; після цього береться два випадкових вектори $\bar{x}'$ та $\bar{x}''$, де $\bar{x} = \bar{x}' + \bar{x}''$, та елементи полягають в $GF((2^4)^2)$;
- Обчислюється $\bar{x}' = C\bar{x}'$ та $\bar{x}'' = C\bar{x}'' + d$, де C – матриця 43x43, b – вектор розміру 43;
- Обчислюється $\bar{x} = \bar{x}' + \bar{x}''$, що еквівалентно $x = Cx + d$;
- $x(x_0, x_1, ..., x_{42})$ це схема підпису Rainbow для $y(y_0, y_1, ..., y_{25})$.

Використовується аналіз несправностей для атаки випадкових байтів у центральних перетвореннях карти; таким чином, ми двічі перевіряємо випадкові байти для захисту від атак аналізу несправностей. Також використовується аналіз диференціальної потужності для атаки модуля SHA-1; таким чином, ми беремо метод захисту афінних перетворень. Однак зазначений вище контрзахід є теоретичним; потрібна можливість впровадити та перевірити це за допомогою апаратного забезпечення [8].

Висновки

1. Постквантова криптографія – частина криптографії, яка залишається актуальною і при появі квантових комп'ютерів і квантових атак. Так як за швидкістю обчислення традиційних криптографічних алгоритмів квантові комп'ютери значно перевершують класичні комп'ютерні архітектури, сучасні криптографічні системи стають потенційно вразливими до криптографічних атак. Більшість традиційних криптосистем спирається на проблеми факторизації цілих чисел або завдання дискретного логарифмування, які будуть легко розв’язані на досить великих квантових комп’ютерах, що використовують алгоритм Шора.

2. Багато криптографів ведуть розробку алгоритмів, незалежних від квантових обчислень, тобто стійких до квантовим атакам. Ці задачі розглянуті на другому етапі конкурсу NIST США.

3. Схема підпису Rainbow виглядає надійною проти великої кількості методів криптоаналізу та проти атак сторонніми каналами.

4. У зв’язку з можливістю появи потужного квантового комп’ютера актуальними є завдання створення постквантових алгоритмів ЕП. В цьому напрямі уже розпочато дослідження, в певній мірі визначено математичні основи, на яких можуть бути побудовані постквантові алгоритми ЕП. Для цього можна застосувати схему Rainbow.

5. Реалізація квантово-захищених алгоритмів вимагає великих матеріально-технічних ресурсів. Вказане пов’язане з великими довжинами ключів та загальних параметрів. Сучасний рівень розвитку техніки дозволяє оптимістично ставитися до можливості ефективної реалізації квантово-захищених алгоритмів.

6. Мультиваріативні квадратичні перетворення можуть бути застосованими для розроблення постквантового стандарту ЕП. Вони вже були використані для побудови схем підпису, але всі спроби побудувати надійну схему поки не були успішними. Попередній аналіз показав, що мультиваріативні квадратичні перетворення можуть вирішити проблему захищеності від атак на основі квантових комп'ютерів, але для цього ще потрібно провести величезний обсяг досліджень та робіт, а також вкласти значні ресурси.

7. Попередній аналіз показує, що розміри загальних параметрів та ключів не викликають сумнівів відносно криптографічної стійкості стандарту, розробленого на основі мультиваріативного квадратичного перетворення. Але залишається проблема просторової складності, яка пов'язана зі значними довжинами загальних параметрів та відкритих ключів.

Список літератури:

1. Lili Chen, Stephen Jordan, Yi-Kai-Liu, Dustin Moody, Rene Peralta, Ray Perlner, Daniel Smith-Tone. Report on Post – Quatum Cryptography. Nistir 8105 (draft).

2. Інтернет-ресурс. Режим доступу http://www.nkj.ru/archive/articles/5309/

3. Горбенко Ю.І. Методи побудування та аналізу, стандартизація та застосування криптографічних систем : монографія ; зааг. ред. І.Д. Горбенко. Харків : Форт, 2015. 959 с

4. Потій О.В, Горбенко Ю.І., Ганзя Р.С., Пономар В.І. // Матеріали V-ї міжнар. наук.-техн. конф. «Захист інформації і безпеки інформаційних систем». Львів, 2016, 02.06 – 03.06. С. 52.

5. Reinier Broker. Constructing supersingular elliptic curves // J. Comb. Number Theory, (3): pp. 269–273, 2009.

6. McGrew D., Curcio M. Hash-Based Signatures draft-mcgrew-hash-sigs00[Електронний ресурс]. Режим доступу: https://tools.ietf.org/html/draftmcgrew-hash-sigs-00.

7. Lili Chen, Stephen Jordan, Yi-Kai-Liu, Dustin Moody, Rene Peralta, Ray Perlner, Daniel Smith-Tone. Report on Post – Quantum Cryptography. NISTIR 8105 (DRAFT). https://www.google.com.ua/search?

8. Bernstein D. J. Grover vs. McEliece // N. Sendrier, editor, Post-Quantum Cryptography, Third International Workshop, PQCrypto 2010, Darmstadt, Germany, May 25-28, 2010 // Proceedings, volume 6061 of Lecture Notes in Computer Science, pages 73–80. Springer, 2010.

Надійшла до редколегії 07.05.2022

Відомості про автора:

Гармаш Дмитро Васильович – аспірант кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; Харківський національний університет імені В. Н. Каразіна; Україна; e-mail: donni.dima@gmail.com