УДК 003.026:004.056 **DOI:10.30837/rt.2021.4.207.07**

Д.В. ГАРМАШ

СИЛЬНІ ТА СЛАБКІ СТОРОНИ АЛГОРИТМУ НА ОСНОВІ БАГАТОВИМІРНИХ ПЕРЕТВОРЕНЬ RAINOW ТА ЙОГО ЗДАТНІСТЬ БЛОКУВАТИ АТАКИ 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. Впроваджуються схеми, які певний час витримували атаки: Unbalanced Oil and Vinegar (UOV), Rainbow та enTTS. Особлива увага приділяється виявленню усіх загальних моментів схеми Rainbow.

Основна інформація про Rainbow, як він влаштований

Наразі криптосистеми, що засновані на квадратичних поліномах, пройшли за останні 10 років суттєвий розвиток та визнання. Теоретичною основою конструкцій Oil-Vinegar є доведена теорема, згідно з якою вирішення (визначення) набору багатоваріантних поліноміальних рівнянь над кінцевим полем є експоненційно складною проблемою, хоча це є у загальному випадку як необхідною, так і достатньою умовами [2].

Цей напрямок досліджень пов'язаний з появою конструкції Мацумото та Імаї, в тому числі з використанням рівняння лінеаризації [1]. Далі Патарін та його співробітники доклали великих зусиль для розробки безпечних багатоваріантних криптосистем. Один з конкретних напрямків, яким займались Патарін та його співробітники, пов'язаний з рівняннями лінеаризації Dragon, Oil and Vinegar, Unbalanced Oil-Vinegar [1]. Побудова механізму ЕП Rainbow на основі Oil and Vinegar, Unbalanced Oil-Vinegar грунтується на тому, що певні квадратичні рівняння можна легко розв'язати, якщо є можливість вгадувати декілька варіантів [1].

Нехай k буде кінцевим полем. Ключовою конструкцією є відображення (карта) F від k^{o+v} до k^{o}:

$$F(x_1,...,x_0,x_1^{'},...,x_v^{'}) = F(x_1,...,x_0,x_1^{'},...,x_v^{'}),...,F_0(x_1,...,x_0,x_1^{'},...,x_v^{'}) \tag{1}$$

і кожна F_l у формі

$$F(x_1,...,x_0,x_1^{'},...,x_v^{'}) = \sum a_{l,i,j}x_i x_j + \sum b_{l,i,j}x_i^{'}x_j^{'} + \sum c_{l,i}x_i + \sum d_{l,i}x_j^{'} + c_l, \tag{2}$$

де x_i, $i = 1,...,o$ - це Oil значення та $x_j^{'}$, $j = 1,...,v$ значення Vinegar у кінцевому полі k.

Потрібно звернути увагу на схожість наведеної вище формули з рівняннями лінеаризації. Такий тип поліномів називається "поліномом Oil-Vinegar". Причина, по якій вона називається схема "Oil-Vinegar", пов'язана з тим, що в квадратичному вимірі змінні Oil та Vinegar не змішуються повністю. Це дозволяє легко знайти одне рішення для будь-якого рівняння виду

$$F(x_1,...,x_0,x_1^{'},...,x_v^{'}) = (y_1,...,y_o), \tag{3}$$

коли $(y_1,...,y_o)$ дано. Щоб знайти одне рішення, потрібно лише випадковим чином вибрати значення для Vinegar змінних та підключити їх до рівнянь вище, що дасть набір o лінійних рівнянь з o змінними. Це має, з імовірністю, близькою до 1, дати рішення. Якщо цього не сталося, можна спробувати ще раз, вибравши різні значення для Vinegar змінних, поки не вдасться знайти рішення [4].

Це сімейство криптосистем розроблено спеціально для схем підписів, де потрібно лише знайти одне рішення для даного набору рівнянь, а не унікальне рішення. Застосовуючи відображення (карту F), ми «приховуємо» її, складаючи її з лівої та правої сторін за двома оборотними афінними лінійними відображеннями L_1 та L_2. Оскільки L_1 знаходиться на k^o, а L_2 на k^{o+v}, це генерує квадратичне відображення (карту)

$$F^{-} = L_1 \circ F \circ L_2 \tag{4}$$

від k^{o+v} до k^o.

Збалансована схема Oil-Vinegar характеризується тим, що $o = v$, але її удосконалили Кіпніс та Шамір, використовуючи матриці, що відносяться до білінійних форм, визначених квадратичними поліномами [3].

Для незбалансованої схеми Oil-Vinegar, $v > o$, показано, що конкретна атака має складність приблизно $q^{v-o-1}o^4$, коли $v \approx o$. Це означає, що якщо o не надто велике (менше ніж 100) і дане фіксоване поле розміром q, тоді $v - o$ має бути досить великим, але також не надто великим, щоб забезпечити безпеку схеми.

Однак слід зауважити, що в цій схемі документ, що підписується, є вектором у k^o, а підпис – вектором у k^{o+v}. Це означає, що підпис має принаймні вдвічі більший розмір документа, і при великому $v + o$ система стає менш ефективною.

В рамках статті пропонується конструкція, яка використовує конструкцію Oil-Vinegar кілька разів, так що в підсумку підпис буде лише трохи довшим за документ. Отже, ця схема набагато ефективніша. Її називають схемою Rainbow.

Сильні та слабкі сторони алгоритму

1) Короткі підписи. Підписи, отримані схемою підписів Rainbow, мають розмір, що приблизно вдвічі перевищує відповідний рівень безпеки. Тому Rainbow виробляє одні з найкоротших підписів всіх існуючих схем цифрового підпису (як класичного, так і постквантового).

2) Скромні обчислювальні вимоги. Оскільки Rainbow вимагає простої операції лінійної алгебри над невеликим кінцевим полем, її можна ефективно реалізувати на пристроях з низькою вартістю, без необхідності криптографічного співпроцесору.

3) Простота. Дизайн схем Rainbow надзвичайно простий. Тому схема вимагає лише мінімальних знань з алгебри, щоб зрозуміти і реалізувати її. Ця простота також означає, що існує не так багато структурних схем, які можуть бути використані для атаки на Rainbow. Тому малоймовірно, що існують додаткові структури, які можуть бути використані для атаки схеми, які не були виявлені протягом більше ніж 12 років строгого криптоаналізу.

4) Суттєве випробовування часом. Як вже було зазначено, Rainbow базується на добре відомій UOV схемі, яка була винайдена ще у 1999 році. Саму схему Rainbow було створено у 2005 році, а останній напад, який потребував зміни параметрів, стався у 2008 році. За цей час було створено безліч спроб зламати цю схему, але досі Rainbow залишається однією з найбільш захищених схем підпису.

5) З іншого боку головним недоліком Rainbow є великий розмір публічних та приватних ключів, виправлення якого є важливим в наших дослідженнях [3, 4].

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:

- атака диференціального аналізу потужності на SFLASH;
- атака на секретні ключі від модуля SHA-1 схем SFLASH.
- атака 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 на апаратному забезпеченні [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 квантових атак. Ці задачі розглянуто 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 ; заг. 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] / D. McGrew, M. Curcio. 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 07.11.2021

Відомості про авторів:

Гармаш Дмитро Васильович – Харківський національний університет імені В. Н. Каразіна, аспірант кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; Україна; e-mail: dmytro.harmash96@icloud.com