УДК 003.026:004.056 **DOI:10.30837/rt.2021.2.205.07**

Д. В. ГАРМАШ

ВЛАСТИВОСТІ БАГАТОВИМІРНОГО АЛГОРИТМУ RAINBOW ТА ЙОГО ЗДАТНІСТЬ ПРОТИСТОЯТИ РІЗНОМАНІТНИМ МЕТОДАМ КРИПТОАНАЛІЗУ І АТАЦІ 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 виявленню усіх загальних моментів схеми Rainbow.

1. Загальні положення щодо схеми ЕП RAINBOW

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.

2. Застосування різноманітних методів крипто аналізу проти алгоритму RAINBOW

Представляється короткий криптоаналіз схеми підпису Rainbow, розглянувши його для наведеного вище прикладу. Є кілька способів атак, з якими будуть мати справу користувачі алгоритму. Для тих методів, де використовуються квадратні форми, слід пам'ятати, що теорія квадратних форм над скінченними полями відрізняється, коли характеристика дорівнює 2, у порівнянні з випадком, коли характеристика є непарною [6].

2.1. Метод зниження рангу

Метод зниження рангу використовується для розбиття схеми підпису біраціональної перестановки Шаміра. Причина, по якій ця атака може спрацювати, полягає в тому, що простір, що охоплюється поліноміальними компонентами шифру схеми Шаміра, складається з прапора пробілів:

$$V1 \subset V2 \subset \cdots \subset Vt, \tag{5}$$

де V_t – простір, охоплений поліноміальними компонентами шифру, кожна V_i є власною підмножиною V_{t+1}, а ранг відповідної білінійної форми, що відповідає елементам у $V_{t+1} - V_i$, занадто більший, ніж у V_i, а різниця розмірів між V_i та V_{t+1} рівно 1. Завдяки цим властивостям, зокрема останньому, це дозволяє легко знайти цей прапор просторів, а саме всі V_i, спочатку знайшовши V_{n-1}, потім V_{n-2} і так далі шляхом зменшення рангу [8]. Але цей метод атаки вже не може працювати проти цієї схеми. Причиною цього є те, що, в нашому випадку, існує також такий прапор просторів, що кількість компонентів – це точно кількість рівнів, розмірність кожного компонента прапора точно відповідає розміру V_{i+1}, $i = 1,...,u-1$, але

різниця в розмірах останніх двох великих просторів – це точно $O_u - 1$, яка була обрана спеціально для досить великого числа 11, на відміну від випадку Шаміра, коли воно дорівнює 1.

Властивість, наведена вище, якраз і є причиною того, що атака більше не може працювати. Тут не можна використовувати метод зниження рангу через те, що $O_u - 1 = 11$ і більше не 1. „Останній товстий рівень Oil" дозволяє схемі протистояти атаці зниження рангу [7].

2.2. Метод атаки на Oil-Vinegar схеми

Аналіз показав, що дія L_1 полягає у змішуванні всіх поліноміальних компонентів F. Отже, кожен компонент шифру F тепер належить до верхнього рівня поліномів Oil-Vinegar, а саме всі вони є елементами P_4. Це багаточлени Oil-Vinegar з 22 змінними Vinegar та 11 змінними Oil [1]. Для цього випадку можна застосувати метод для незбалансованої схеми підпису Oil-Vinegar, щоб спробувати атакувати систему, що дозволить відокремити змінні верхнього шару Oil-Vinegar. Для цього нам потрібно розділити верхній (або кінцевий) рівень з 11 змінних Oil та 22 змінних Vinegar. Відповідно до криптоаналізу складність атаки цього першого кроку становить $q^{22-11-1} \times 11^4 > 2^{90}$.

2.3. Метод Мінранка

Існує два абсолютно різних способи використання методу Мінранка. Перший – пошук полінома, асоційована матриця якого має найнижчий ранг серед усіх можливих варіантів. Цей набір поліномів із 6 змінними Vinegar та 6 Oil належить до першого рівня, тобто $P1$, і позначався $F\tilde{}_1$. Для цього спочатку ми прив'язуємо до кожного полінома білінійну форму, яка має матрицю розміром 33×33. Потім ми можемо використовувати лінійні комбінації матриць, пов'язаних із компонентами F, для виведення полінома, пов'язана з яким матриця має ранг 12 [3]. В цьому випадку, щоб атакувати систему, проблемою стає пошук матриці рангу 12 серед групи з 27 матриць розміром 33×33. З методу Мінранка ми знаємо, що складність пошуку такої матриці становить $q^{12} \times 27^3$, що набагато більше, ніж 2100.

Інша можливість – це пошук поліномів, що відповідають поліномам у другому останньому рівні, а саме той, який належить P_3 і походить від лінійних комбінацій $F\tilde{}_i$, $i < 4$. У цьому випадку метод Міранка однозначно не може бути використаний , оскільки вони взагалі мають ранг 22. Одним із шляхів, безсумнівно, є випадковий пошук. Оскільки розмірність P_3 дорівнює 16, це стає проблемою пошуку елемента в підпросторі розмірності 16 в загальному просторі розмірності 27. Отже, такий випадковий пошук потребує щонайменше q^{11} пошуків, щоб знайти його, але нам також потрібно визначити, чи дійсно рейтинг нижче 22 для кожного пошуку. У цьому випадку загальна складність повинна бути не менше $q^{11} \times (22 \times 33^2 / 3) > 2^{100}$. Ця ідея атаки насправді пов'язана з іншим методом атаки, і наведений вище аргумент пояснює, чому цей метод більше не може працювати [8].

З останніх результатів електронного друку в цьому напрямку, де вивчаються дуже загальна система, яка називається STS, ми знаємо, що їх метод може бути застосований і до нашого випадку. Відповідно до їх оцінки, безпека нашої системи становить принаймні $27 \times 33^3 \times (2^8)^{12} \times 5 > 2^{100}$.

2.4. Атака за допомогою структури багатошаровості.

Для випадку криптосистеми Мацумото – Імай Патарін зрозумів, що якщо шифр складається з декількох незалежних паралельних «гілок», можна виконати поділ змінних таким чином, що всі поліноми в шифрі виведені як лінійні комбінації поліномів над кожною групою змінних. Ця властивість насправді може бути використана для атаки на систему. На перший погляд, можна подумати, що рівні виглядають як різні «гілки». Тим не менше, слід усвідомити, що рівні жодним чином не є «незалежними», оскільки кожен з них будується на попере-

ньому. Простіше кажучи, можна сказати, що всі рівні злипаються, і ми ніяк не можемо зробити будь-якого розділення змінних. Це зрозуміло, коли розглядаються поліноми останнього рівню P_4. Тому атака з використанням властивості паралельних незалежних гілок у тут не може працювати. Подібним чином можна стверджувати, що атака з використанням системних систем також не може працювати тут, оскільки немає гілок і все насправді «склеєно» [2].

2.5. Загальні методи

Іншими методами, які можуть бути використані для атаки на нашу схему підписів, є ті, які безпосередньо вирішують поліноміальні рівняння, наприклад метод XL та різні його узагальнення, або такі, що використовують основи Грубонера. Безумовно, дуже складно вирішити набір з 27 рівнянь із 33 змінними, оскільки для цього набору рівнянь існує надто багато рішень. Загалом, набагато краще розв'язувати рівняння лише з однією змінною. Через характер проєктування системи можна здогадатися про значення для будь-якого набору змінних $v_1 = 6$, і ми маємо ймовірність $1 / e < 1 / 2.71828 < 0.37$ отримати унікальне рішення. Тепер задача стає проблемою вирішення набору з 27 квадратних рівнянь із 33 змінними. Ми повинні думати про це так, ніби це сукупність випадково вибраних квадратних рівнянь. Відповідно до того, що прийнято вважати, для вирішення цього набору рівнянь складність становить щонайменше $23 \times 27 > 281$.

З цього ми робимо висновок, що загальна складність атаки на наш приклад становить принаймні 280 [3].

2.6. Загальний аналіз безпеки

На основі цього можна побачити, що для атаки на систему можна підійти до неї або з верхнього рівня, або сформувати нижній рівень. Безпека нижнього рівня залежить від того, наскільки ефективно можна використовувати метод Minrank. Загалом складність атаки дорівнює $q^{(v2-1)}o^3{}_u - 1 if v_1 > o_1$, якщо $v_1 > o_1$, або $q^{2v1}o_u{}^3 - 1$, якщо $v_1 \le o_1$. З цього можна отримати, що не можна дозволити $v_2 = o_1 + v_1$ бути занадто малим. З останніх результатів електронного друку [WBP], безпека системи становить принаймні $(n - v_1) \times n^3 \times (q)^{o1+v1} \times u$, що, безсумнівно, вимагає, щоб $o_1 + v_1$ не був малим.

Що стосується випадку атаки зверху, метод атаки для незбалансованого методу Oil-Vinegar говорить, що $v_u - 1 - o_u - 1$ не може бути занадто малим. Також щоб уникнути випадкових атак пошуку $o_u - 1$ не повинно бути занадто малим [4].

3. 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.

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.

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 дві 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.

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'юте-

рні 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 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. Інтернет-ресурс. Режим доступу http://www.win.tue.nl/diamant/symposium05/abstracts/wolf.pdf

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

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

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

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

8. 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.

9. 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 02.04.2021

Відомості про автора:

Гармаш Дмитро Васильович – Харківський національний університет імені В.Н. Каразіна, аспірант кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Україна, e-mail: dmitriy.garmash96@icloud.com