УДК 003.026:004.056 **DOI:10.30837/rt.2020.4.203.07**

Д.В. ГАРМАШ, Г.А. МАЛЄЄВА, С.О. КАНДІЙ

ПРОЕКТ СТАНДАРТУ ЕЛЕКТРОННОГО ПІДПИСУ RAINBOW ТА ЙОГО ОСНОВНІ ВЛАСТИВОСТІ І МОЖЛИВОСТІ ЩОДО ЗАСТОСУВАННЯ

Вступ

За результатами другого етапу міжнародного конкурсу щодо проведення досліджень та розробки стандартів асиметричних криптографічних перетворень постквантового періоду позитивну оцінку та визнання фіналістом отримав механізм електронного підпису (ЕП) Rainbow [1]. Його важливими перевагами, у порівнянні з іншими постквантовими ЕП, це менша складність прямого та зворотного перетворень – вироблення та перевірки підпису, а також суттєво зменшена довжина підпису. Разом з тим довжина відкритого ключа у нього достатньо велика. Тому є думка, що Rainbow не підходить, як алгоритм ЕП загального призначення для заміни алгоритмів, які наразі визначені у FIPS 186-4. Зокрема, великі відкриті ключі роблять ланцюги сертифікатів надзвичайно великими. Однак є додатки, яким не потрібно надто часто надсилати ключі, тому цей недолік у цих випадках може бути несуттєвим. За цих умов механізм ЕП Rainbow може знайти застосування, в тому числі збільшуючи різноманітність постквантових ЕП. Також, суттєво проблемним є обмеження рівнів безпеки ЕП Rainbow 256 біт проти класичного та 128 біт проти квантового криптоаналізу.

Предметом статті є аналіз та узагальнення конструкцій механізму Oil-Vinegar систем автентифікації з відкритим ключем на основі застосування ЕП Rainbow. Це важливий напрямок щодо створення безпечних та ефективних систем автентифікації для практичних застосувань з використанням відкритих ключів, наприклад недорогих смарт-карт, коли потрібна швидкодія при виробленні та перевірці ЕП. Особливістю такого механізму автентифікації є реалізація ідеї багаторівневої системи Oil-Vinegar [2]. Вважається, що система автентифікації на основі ЕП повинна бути більш безпечною у змісті криптографічної стійкості та більш ефективною у змісті широкого застосування у малопотужних тощо додатках. Важливість вирішення цієї проблемної задачі полягає у потенційному застосуванні механізму Rainbow, як надійно безпечної та дуже ефективної системи автентифікації з відкритим ключем на основі ЕП.

Загальні положення щодо схеми ЕП RAINBOW

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 [MI88], в тому числі використовуючи 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}:

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

і кожна F_l у формі:

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

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.

Сбалансована схема Oil-Vinegar характеризується тим, що $o = v$, але її удосконалили Кіпніс та Шамір [KS99], 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 (меньше 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.

Сутність та властивості схеми підпису RAINBOW

Загальна конструкція Rainbow.

Нехай S – множина $\{1, 2, 3, ..., n\}$. Нехай $v_1,...,v_u$ – цілі числа, такі що попадають в умову $0 < v_1 < v_2 < \cdots < v_u = n$ і визначимо декілька наборів цілих чисел $S_l = \{1, 2, ..., v_l\}$ для $l = 1,...,u$, так що ми маємо $S1 \subset S2 \subset \cdots \subset Su = S$

Нехай O_i є такою множиною, що $O_i = S_{i+1} - S_i$, $fori = 1,...,u-1$.

Нехай P_l – лінійний простір квадратних многочленів, що задаються поліномами

$$\sum_{i \in O_{l,j} \in S_l} \alpha_{i,j}x_i x_j + \sum_{i \in O_{l,j} \in S_l} \beta_{i,j}x_i x_j + \sum_{i \in O_{l,j} \in S_l} \gamma_i x_i + \eta \tag{5}$$

Видно, що це багаточлени типу Oil-Vinegar, такі що x_i, $i \in O_l$ – змінні Oil наряду з x_i, $i \in S_l$ – змінні Vinegar. x_i, $i \in O_l$ називаються l-м рівнем Oil змінної, а x_i, $i \in S_l$ являються l-м рівнем Vinegar змінної.

Будь-який поліном у P_l називається l-м рівнем поліном Oil та Vinegar. З цього маємо, що

$$P_i \subset P_j \text{ для } i < j.$$

Таким чином, кожен $P_l, l = 1,...,u-1$ є набором багаточленів Oil та Vinegar. Кожен поліном у P_l має x_i, $i \in O_l$ як змінні Oil і x_i, $i \in S_l$ як змінні Vinegar. Поліноми Oil та Vinegar у P_i можна визначити як поліноми так, що $x_i \in O_l$ – змінні Oil, а x_i, $i \in S_l$ – Vinegar змінні. Це можна проілюструвати тим, що $S_i + 1 = \{S_i, O_i\}$.

Тепер ми визначимо відображення (карту) F схеми підпису Rainbow. Це карта F від k^n до k^{n-v1} така, що

$$F(x_1,...,x_n) = (\tilde{F}_1(x_1,...,x_n),...,\tilde{F}_{u-1}(x_1,...,x_n)) = (F_1(x_1,...,x_n),...,F_{n-v_1}(x_1,...,x_n)), \quad (6)$$

кожен $\tilde{F}_i$ складається з o_i випадково обраних квадратичних многочленів з P_i. Під випадково обраним поліномом маємо на увазі, що ми вибираємо його коефіцієнти випадковим чином [4].

Таким чином, можна зазначити, що F насправді має $u-1$ рівні Oil-Vinegar конструкцій. Перший рівень складається з поліномів o_1 $F_1,...,F_{o1}$, таких що x_j, $j \in O_1$ – змінні Oil, а x_j, $j \in S_1$ – змінні Vinegar. I-й рівень складається з поліномів o_i, $F_{vi}+1,...,F_{vi+1}$, так що x_j, $j \in O_i$ – змінні Oil, а x_j, $j \in S_i$ – змінні Vinegar. З цього ми можемо побудувати «веселку» з наших змінних:

$$[x_1,...,x_{v1}];\{x_{v1}+1,...,x_{v2}\}\ [x_1,...,x_{v1},x_{v1}+1,...,x_{v2}];\{x_{v2}+1,...,x_{v3}\}$$
$$[x_1,...,x_{v1},x_{v1}+1,...,x_{v2},x_{v2}+1,...,x_{v3}];\{x_{v3}+1,...,x_{v4}\}\ [x_1,...,...,x_{vu-}1];\{x_{vu-}1+1,...,x_n\} \quad (7)$$

Кожен рядок вгорі представляє рівень Rainbow. Для l-го рівня, наведеного вище, є змінні Vinegar, у { } – змінні Oil, а змінні Vinegar кожного рівня складаються з усіх змінних попереднього рівня.

F можна назвати поліноміальною картою Rainbow з рівнями $u-1$.

Нехай L_1 і L_2 є двома випадковими обраними аффінними лінійними картами, L_1 знаходиться на $kn-v1$ і L_2 на kn.

$\bar{F}(x_1,...,x_n) = L_1 \circ F \circ L_2(x_1,...,x_n)$ який складається з $n-v_1$ квадратних многочленів з n змінними.

Тепер можна використати вищезазначене для побудови схеми підпису Rainbow із відкритим ключем.

Публічний ключ – для схеми підпису Rainbow відкритий ключ складається з $n-v_1$ поліноміальних компонентів F та структури поля k. Приватний ключ складається з карт L_1, L_2 та F.

Підписати документ, який є елементом $Y' = (y_1',...,y_{n-v_1}')k^{n-v_1}$ потрібно знайти рішення рівняння

$$L_1 \circ F \circ L_2(x_1,...,x_n) = F(x_1,...,x_n) = Y^l \quad (8)$$

Для цього спочатку можна застосувати обернену до L_1, а потім виявляється

$$F \circ L_2(x_1,...,x_n) = L_1^{-1}Y^l = Y^l \tag{9}$$

Далі потрібно інвертувати F . У цьому випадку потрібно вирішити рівняння

$$F(x_1,...,x_n) = Y^l = (y_1^{-l},...,y_{n-v_1}^{-l}) \tag{10}$$

Спочатку необхідно випадково вибрати значення $x_1,...,x_{v1}$ і підключити їх до першого рівня o_1, заданих

$$F_1 = (y_1,...,y_{o_1}^{-l}) \tag{11}$$

Це дає набір лінійних рівнянь o_1 зі змінними o_1, $x_{o1}+1,...,x_{v2}$, які вирішуються, щоб знайти значення $x_{o1}+1,...,x_{v2}$. Тоді отримуються всі значення x_i, $i \in S_2$ [1]. Потім ми підключаємо ці значення до другого рівня багаточленів, який знову дасть o_2 число лінійних рівнянь, яке потім дасть значення всіх x_i, $i \in S_3$ Процедура повторюється, поки не буде знайдено рішення. Якщо в будь-який час набір лінійних рівнянь не має рішення, все починається з початку, вибравши інший набір значень для $x_1,...,x_{v1}$. Це буде продовжуватись, поки не буде знайдено рішення. З [Pat96] відомо, що з дуже великою ймовірністю можна розраховувати на успіх, якщо кількість рівнів не надто велика.

Потім ми застосовуємо обернену до L_2, яка дає нам підпис Y, який позначається

$$X^l = (x_n^l,...,x_n^l). \tag{12}$$

Щоб перевірити підпис, потрібно лише перевірити, чи справді

$$F(X^l) = Y^l. \tag{13}$$

Для того щоб підписати великий документ, можна пройти ту саму процедуру для Flash, що і в [PCG01], застосувавши спочатку хеш-функцію, а потім підписати хеш-значення документа.[4]

Практична реалізація схеми Rainbow.

Для практичної реалізації ми вибрали k кінцевим полем розміром $q = 2^8$.

Нехай $n = 33$ і S – множина $\{1,2,3, ..., 33\}$.

Нехай $u = 5$ і $v_1 = 6$, $v_2 = 12$, $v_3 = 17$, $v_4 = 22$, $v_5 = 33$.

Маємо $o_1 = 6$, $o_2 = 5$, $o_3 = 5$, $o_4 = 11$

У цьому випадку і F^{-}, і F є картами від k^{33} до k^{27}.

Відкритий ключ складається з 27 квадратних многочленів із 33 змінними. Загальна кількість коефіцієнтів для відкритого ключа становить $27 \times 34 \times 35/2 = 16\,065$, або близько 15 КБ пам'яті.

Приватний ключ складається з 11 багаточленів з 22 змінами Vinegar та 11 змінних Oil, 5 поліномів з 17 змінами Vinegar та 5 Oil, 5 поліномів з 12 змінними Vinegar та 5 Oil, та 6 поліномів з 6 змінними Vinegar та 6 Oil плюс дві афінні лінійні перетворення L_1 і L_2. Загальний розмір – близько 10 КБ.[5]

Ця схема підпису підписує документ розміром $8 \times 27 = 216$ біт із підписом $8 \times 33 = 264$ біт.

Криптоаналіз схеми підпису 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 [D09] [6].

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:

$$V1 \subset V2 \subset \cdots \subset Vt,$$

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].

Метод атаки на Oil-Vinegar схеми.

Аналіз показав, шо, 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 $q^{22-11-1} \times 11^4 > 2^{90}$.

Метод MinRank

Існує два абсолютно різних способи використання методу MinRank. 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 $\tilde{F}_1$. 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 MinRank 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 $\tilde{F}_i$, $i < 4$. У цьому випадку метод MinRank 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 $27 \times 33^3 \times (2^8)^{12} \times 5 > 2^{100}$.

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 попередньому. Тобто, можна сказати, що всі рівні злипаються, і ми ніяк не можемо зробити будь-якого розділення змінних. Це зрозуміло при розгляданні поліномів останнього рівня P_4. Тому атака з використанням властивості паралельних незалежних гілок у [Pat95] 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].

Загальні методи

Іншими методами, які можуть бути використані для атаки на нашу схему підписів, є такі, які безпосередньо вирішують поліноміальні рівняння, наприклад метод XL та різні його узагальнення, або такі, що використовують основи Гробнера. 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 проектування 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].

Загальний аналіз безпеки

На основі цього можна побачити, що для атаки на систему можна підійти до неї або з верхнього рівню, або сформувати нижній рівень. Безпека нижнього рівню 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].

Порівняння з іншими схемами багатоваріантних підписів

Порівняння з незбалансованою Oil-Vinegar

По-перше, система, що розглядається, є узагальненням оригінальної конструкції Oil-Vinegar, і оригінальну схему можна трактувати як просто однорівневу схему Rainbow, де $u = 2$. Припустимо, що ми хочемо створити незбалансовану схему Oil-Vinegar, яка має однакову довжину для документа, який може бути підписаний, як наш практичний приклад вище. У цьому випадку ми знову вибираємо k як кінцеве поле розміром $q = 28$, і ми знаємо, що кількість змінних Oil має бути 27. Через атаку на дисбаланс схем Oil-Vinegar [KPG99], ми знаємо, що число змін Vinegar має бути не менше $27 + 11 = 38$, щоб мати однаковий рівень безпеки [1]. Далі, відкритий ключ складається з 27 поліномів із $38 + 27 = 65$ змінними. Отже, розмір відкритого ключа становить $27 \times (67 \times 66/2)$ байт, що становить приблизно 116 КБ, що приблизно в 10 разів перевищує наш практичний приклад. Це означає, що публічне обчислення перевірки підпису триватиме щонайменше в 10 разів довше.

Приватний ключ для незбалансованої схеми Oil-Vinegar складається з одного афінного лінійного перетворення на k^{27} та іншого на k^{65} та набору з 27 поліномів Oil та Vinegar з 27 змінними Oil та 38 змінними Vinegar. Це означає, що закритий ключ становить близько 40 КБ. Також, що приватний розрахунок для підписання документа займе приблизно у чотири рази довше порівняно з нашим прикладом. Довжина підпису становить $65 \times 8 = 520$ біт, що також приблизно вдвічі перевищує розмір підпису нашого прикладу [2]. З цього ми робимо висновок, що наша схема має бути набагато кращим вибором загалом як з точки зору безпеки, так і ефективності.

Порівняння з Sflash

NESSIE, «Нові європейські схеми підписів, цілісності та шифрування» – це проект в рамках Програми Європейської комісії з технологій інформаційного суспільства. Він зробив остаточний вибір крипто алгоритму після більш ніж 2-річного процесу. Sflashv2, швидку багатоваріантну схему підпису було обрано консорціумом Nessie і рекомендовано для недорогих смарт-карт. Однак, з погляду безпеки, дизайнер Sflash одного разу рекомендував не використовувати Slashv2, натомість рекомендується нова версія Sflashv3. Це просте розширення Sflashv2 за рахунок збільшення довжини підпису. Sflashv3 має довжину підпису 469 біт і відкритий ключ 112 Кбайт. Але нещодавно Sflashv2 знову визнали безпечним, і ми порівняли нашу реалізацію із Sflashv2. Sflashv2 має підпис довжиною $37 \times 7 = 259$ для документа $26 \times 7 = 182$ біт. Наш приклад має підпис довжиною $33 \times 8 = 264$ для документа розміром $27 \times 8 = 216$ біт. З точки зору ефективності на біти ці два фактично однакові [3].

Для порівняння часу роботи було застосовано Sflashv2, як описано в [ACDG03]. Генерація підпису приблизно вдвічі швидша для нашого прикладу з Rainbow у порівнянні з Sflash. Час перевірки підпису, звичайно, майже однаковий. З цього можна зробити висновок, що схема має бути хорошим вибором як з точки зору безпеки, так і ефективності.

Також можна порівняти цю систему з новими схемами TTS, але ці схеми атаковані, як це було показано в презентації в IWAP'04 [DY04]. Слід також побачити, що Tractable Rational Map Signature, як представлено в [WHLCY], дуже схожий на TTS і може розглядатися як дуже особливий приклад нашої схеми [5].

Побудова системних параметрів для RAINBOW для 384 біт безпеки

Аналіз показав, що для схеми Rainbow актуальною є задача побудови системних параметрів для рівня безпеки 384 біт. В цьому розділі наводяться результати попередніх досліджень щодо вирішення вказаної задачі.

До загальносистемних параметрів Rainbow належать поле $GF(q)$, над яким задані поліноми, кількість «oil» змінних o_1, o_2 (в Rainbow використовується 2 рівня), кількість «vinegar» змінних v_1.

Загальна кількість рівнянь є $n = o_1 + o_2 + v_1$

Загальна кількість змінних є $m = o_1 + o_2$

Всі ефективні атаки на Rainbow полягають в використанні лінеаризації рівнянь.

До основних атак належать:

1) Прямі алгебраїчні атаки. Полягають у безпосередньому застосуванні алгоритмів вирішення квадратичних рівнянь над полями Галуа. Автори Rainbow зазначають, що алгоритм XL (та його модифікації) дає найкращі результати. Час роботи алгоритму залежить від константи d_{reg} – степені регуляризації системи.

2) MinRank атаки. Атаки цього класу полягають у пошуку лінійної комбінації мінімального рангу поліномів. Аналіз, що приведений в специфікації Rainbow є спрощеним. Повну методику обчислення параметрів автори виклали у [1].

3) HighRank атаки. Полягають у пошуку «oil» змінних в останньому рівні. Оцінити складність атаки можливо за формулою

$$C_{HighRank} = q^{o_2} * \frac{n^3}{6}. \tag{14}$$

При застосуванні алгоритму Гровера можливо пришвидшити пошук:

$$C_{HighRank(quantum)} = q^{o_2/2} * \frac{n^3}{6}. \tag{15}$$

4) UOV атаки. Оскільки Rainbow є узагальненням OUV, то атаки на цю схему можливо також узагальнити. Оцінити складність атаки можливо за формулою

$$C_{HighRank} = q^{n-2o_2-1} * o_2^4. \tag{16}$$

При застосуванні алгоритму Гровера можливо пришвидшити пошук:

$$C_{HighRank} = q^{\frac{n-2o_2-1}{2}} * o_2^4. \tag{17}$$

5) Rainbow-Band-Separation атаки. Полягає у пошуку маскуючих афінних перетворень *S* і *T*.

Загальні зауваження щодо атак:

1) Атаки HighRank і атаки на UOV сильно залежать від поля.

2) Атаки Rainbow-Band-Separation і прямі атаки сильно залежать від кількості невідомих змінних m, кількості рівнянь n і кількості «oil» змінних на останньому рівні o_2.

3) Від кількості «oil» змінних на першому рівні o_1 безпека залежить значено менше, ніж від кількості «oil» змінних на останньому рівні o_2.

Параметри для 384 біт наведені в таблиці:

Рівень	Параметри	прямі	MR	HR	UOV	RBS
384	$(o_1 = 108, o_2 = 96, v_1 = 134, GF(256))$	?	533	406	602	?

Також наведемо проблемні (невирішені) питання.

Прямі атаки та RBS атаки потребують детальнішого вивчення для оцінки.

Автори Rainbow використовують поле $GF(2^x)$. Чи є доцільним використовувати поле іншої форми?

Висновки

1. Постквантова криптографія – частина криптографії, яка залишається актуальною і при появі квантових комп'ютерів і квантових атак. Так як по швидкості обчислення тради-

ційних 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'язуватись 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 2-му етапі конкурсу NIST США.

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

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

5. 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 досі не увінчалися успіхом. 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.

6. 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). https://www.google.com.ua/search?

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 І.Д. Аналіз проблем криптографічного захисту інформації у постквантовий період та можливі шляхи їх вирішення / І.Д. Горбенко, О.О. Кузнєцов, Р.В. Олійников, О.В. Потій, Ю.І. Горбенко, Р.С. Ганзя, В.І. Пономар // 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-sigs-00 [Электронный ресурс]. Режим доступа: https://tools.ietf.org/html/draft-mcgrew-hash-sigs-00

7. Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, and Christine van Vredendaal. NTRU Prime

8. D. J. Bernstein. 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 06.09.2020

Відомості про авторів:

Гармаш Дмитро Васильович – аспірант кафедри кібербезпеки, Харківський національний університет імені В.Н. Каразіна; Україна, e-mail: donni.dima@gmail.com

Малєєва Ганна Андріївна – аспірант кафедри безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, Україна; e-mail: hanna.malieieva@nure.ua

Кандій Сергій Олегович – технік-конструктор, АТ "ІІТ", Україна; e-mail: sergeykandy@gmail.com