УДК 621.391:519.2 **DOI:10.30837/rt.2023.3.214.05**

Є.В. КОТУХ, канд. техн. наук, Г.З. ХАЛІМОВ, д-р техн. наук,
М.В. КОРОБЧИНСЬКИЙ, д-р техн. наук

МЕТОД НАПРАВЛЕНОГО ШИФРУВАННЯ В КРИПТОСИСТЕМІ MST3 НА ОСНОВІ ГРУПИ АВТОМОРФІЗМІВ ФУНКЦІОНАЛЬНОГО ПОЛЯ СУЗУКІ

Вступ

Розвиток комерційних квантових комп'ютерів вносить значні виклики у сферу безпеки багатьох криптосистем з відкритим ключем. Квантовий алгоритм, розроблений Шором, призначений для розв'язання задач цілочисельної факторизації та обчислення дискретних логарифмів, ставить під загрозу безпеку криптосистем, таких як RSA та ECC. Один з перспективних напрямків створення криптосистем, стійких до квантових атак, полягає у використанні задач, що мають високу складність вирішення в певних групах [1 – 11]. Побудова криптосистем на основі нерозв’язних задач була сформульована Шпільрайном та Ушаковим на початку 2000-х років у [3]. З початку 2000-х років запропоновано декілька десятків криптосистем у групових структурах [5 – 11].

Використовуючи групи перестановок, Вагнер і Магьярик [5] запропонували нерозв'язну схему, засновану на проблемі слова, для створення квантово-стійких криптосистем. Квантова безпека таких систем залежить від їх конкретної реалізації, і, на попередньому етапі, можливе використання квантового алгоритму Гровера для криптоаналізу. Ідея нерозв'язної проблеми слова вперше була реалізована в криптосистемі з логарифмічними підписами [6]. Логарифмічний підпис є особливим типом факторизації і застосовується до кінцевих груп. Покращення оригінальної версії були внесені в [7, 8].

Побудова криптосистем на основі неабелевих груп з використанням нерозв’язаних задач залишається перспективним напрямом досліджень [12 – 17]. Сімейство криптосистем MST реалізує практичні результати даних досліджень. Остання версія реалізації відома як MST3 [8] і базується на групі Сузукі. Було розглянуто різні стратегії для покращення MST3 [9 – 19], зокрема, за допомогою багатопараметричних груп великого порядку та оптимізації обчислювальних процесів на малому кінцевому полі.

Одним з ключових нововведень було використання автоморфізмів груп над функціональними полями Сузукі, Ерміта, Рі великого порядку. Автори [18 – 28] першими запропонували напрями посилення секретності та покращення параметрів реалізації даної криптосистеми для створення кандидата квантово-стійкої криптосистеми на основі неабелевих груп Сузукі, Ерміта, Рі. Однак первинні реалізації криптосистем на основі групи автоморфізмів над функціональним полем Ерміта мали недоліки, такі як слабке зв'язування ключів логарифмічних підписів, що підвищувало ризик послідовних атак на відновлення ключа.

У статті представлена новітня безпечна схема шифрування, заснована на групі автоморфізму функціонального поля Сузукі.

Група автоморфізмів функціонального поля Сузукі

Визначення та властивості криптосистеми MST3, визначення групи, її розмір, порядок, детально описано в роботі [13 – 18]. Тому, розглянемо та визначимо властивості автоморфізмів функціонального поля Сузукі.

Нехай F_q – скінченне поле, а F/F_q – поле алгебраїчної функції над повним сталим полем F_q роду g. Функціональне поле Сузукі – це оптимальне функціональне поле, визначене над кінцевим полем з парною характеристикою p. Нехай $p=2$, $q=2^n$ з $n=2s+1$, де $s\in N\setminus\{0\}$, і $q_0=2^s$. Нехай K – кінцеве поле F_q. Функціональне поле Сузукі над K визначається як $S=K(x,y)$ де $y^q+y=x^{2q_0}(x^q+x)$.

$S/K(x)$ є розширенням Галуа ступеня q, а полюс x повністю розгалужений у розширенні $S/K(x)$. Позначимо P_∞ єдине раціональне місце, що S лежить над полюсом x. Рід дорівнює S, $g(S)=q_0(q-1)$, а кількість раціональних розрядів S дорівнює q^2+1.

Група автоморфізмів S позначається $A=Aut(S/K)$ ізоморфною групі Сузукі, $Sz(q)$, яка має порядок $ordA=\left(q^2+1\right)q^2\left(q-1\right)$.

Група розкладання P_∞, яку позначають як $A\left(P_\infty\right)$, складається з автоморфізмів $S\left|F_q\right.$, що діють на ній як

$$\begin{cases}\sigma(x)=ax+b\\ \sigma(y)=a^{2q_0+1}y+ab^{2q_0}x+c,\end{cases}$$

де $a\in F_q^*:=F_q\setminus\{0\}$, $b,c\in F_q$[10]. Інволюцію $\psi\in A$ задають

$$\begin{cases}\psi(x)=y/h\\ \psi(y)=y/h\end{cases},$$

де $h=xy+x^{2q_0+2}+y^{2q_0}$.

Група автоморфізмів S породжується $A\left(P_\infty\right)$ і ψ, тобто $Sz(q)\cong\left\langle A\left(P_\infty\right),\psi\right\rangle$.

Знову ж, автоморфізм у групі розкладання $A\left(P_\infty\right)$ можна ототожнити з трійкою [a, b, c]. Точніше, $A\left(P_\infty\right)=\left[a,b,c\right]$, $a,b,c\in K$, і $a=0$.

Структура групи має вигляд $\left[a_1,b_1,c_1\right]\cdot\left[a_2,b_2,c_2\right]=\left[a_1a_2,a_2b_1+b_2,a_2^{2q_0+1}c_1+a_2b_2^{2q_0}b_1+c_2\right]$.

Тотожність є трійкою $\left[1,0,0\right]$ та оберненою $\left[a,b,c\right]$,

$$\left[a,b,c\right]^{-1}=\left[a^{-1},-a^{-1}b,\left(a^{-1}b\right)^{2q_0+1}-a^{-(2q_0+1)}c\right].$$

Порядок групи дорівнює $ordA\left(P_\infty\right)=q^2\left(q-1\right)$.

З а у в а ж е н н я . Порядкова група $A\left(P_\infty\right)$ більша за групу Сузукі. Групи Сузукі ізоморфні проєктивній лінійній групі $PGL\left(3,F_q\right)$, де $q=2q_0^2$, $q_0=2^n$ і мають порядок q^2 і включені в криптосистеми MST3. Більший груповий порядок дає перевагу секретності криптосистеми.

Запропонований метод на основі групи автоморфізмів функціонального поля Сузукі

Наша пропозиція полягає в тому, щоб використовувати логарифмічний підпис для шифрування не тільки в центрі групи $A\left(P_\infty\right)$, як у відомій реалізації MST3 для груп Сузукі, але також для інших координат поза центром групи. Раніше такий підхід ми розглядали для групи Ерміта [23].

Із з а у в а ж е н н я випливає, що для побудови криптосистеми MST3 перевага надається групі $A\left(P_\infty\right)$ на основі автоморфізму $\sigma(x),\sigma(y)$. Кожен елемент $A\left(P_\infty\right)$ може бути виражений унікально: $A\left(P_\infty\right)=\left\{S(a,b,c)\left|a\in F_q\setminus\{0\},b,c\in F_q\right.\right\}$ де $S(a,b,c)=\left[a,b,c\right]$, і групова операція визначається як $\left[a_1,b_1,c_1\right]\cdot\left[a_2,b_2,c_2\right]=\left[a_1a_2,a_2b_1+b_2,a_2^{2q_0+1}c_1+a_2b_2^{2q_0}b_1+c_2\right]$. Обернення до $S\left(a,b,c\right)$ дорівнює $S\left(a,b,c\right)^{-1}=S\left(a^{-1},-a^{-1}b,\left(a^{-1}b\right)^{2q_0+1}-a^{-(2q_0+1)}c\right)$.

Це легко показати прямими розрахунками. Тотожність – це трійка $S\left(1,0,0\right)$.

З цього випливає, що $\left|A\left(P_\infty\right)\right| = q^2\left(q-1\right)$. Центр $Z\left(A\left(P_\infty\right)\right) = \left\{S(1,0,c)\middle| c \in F_q\right\}$ і $\left|Z\left(A\left(P_\infty\right)\right)\right| = q$.

Основні етапи нашої схеми шифрування наступні. Згенеруємо ключі.

Згенеруємо перший простий логарифмічний підпис
$\beta_{(1)} = \left[B_{1(1)},...,B_{s(1)}\right] = \left(b_{ij}\right)_{(1)} = S\left(1, b_{ij(1)}, 0\right)$ типу $\left(r_{1(1)},...,r_{s(1)}\right)$, $i = \overline{1,s(1)}$, $j = \overline{1,r_{i(1)}}$, $b_{ij(1)} \in F_q$.

Згенеруємо другий простий логарифмічний підпис
$\beta_{(2)} = \left[B_{1(2)},...,B_{s(2)}\right] = \left(b_{ij}\right)_{(2)} = S\left(1,0,b_{ij(2)}\right)$ типу $\left(r_{1(2)},...,r_{s(2)}\right)$, $i = \overline{1,s(2)}$, $j = \overline{1,r_{i(2)}}$, $b_{ij(2)} \in F_q$.

Згенеруємо перше випадкове накриття $\alpha_{(1)} = \left[A_{1(1)},...,A_{s(1)}\right] = \left(a_{ij}\right)_{(1)} = S\left(a_{ij(1)_1}, a_{ij(1)_2}, a_{ij(1)_3}\right)$ того самого типу, що й $\beta_{(1)}$, де $a_{ij} \in A\left(P_\infty\right)$, $a_{ij(1)_1}, a_{ij(1)_2}, a_{ij(1)_3} \in F_q \setminus \{0\}$.

Згенеруємо друге випадкове накриття $\alpha_{(2)} = \left[A_{1(2)},...,A_{s(2)}\right] = \left(a_{ij}\right)_{(2)} = S\left(a_{ij(2)_1}, a_{ij(2)_2}, a_{ij(2)_3}\right)$ того самого типу, що й $\beta_{(2)}$, де $a_{ij(2)_1}, a_{ij(2)_2}, a_{ij(2)_3} \in F_q \setminus \{0\}$.

Згенеруємо $t_{0(k)}, t_{1(k)},..., t_{s(k)} \in A(P_\infty) \setminus Z$, де $t_{i(k)} = S\left(t_{i(k)_1}, t_{i(k)_2}, t_{i(k)_3}\right)$, $t_{i(\mathrm{k})_j} \in F^\times$, $i = \overline{0,s(\mathrm{k})}$, $j = \overline{1,2}$, $k = \overline{1,2}$. Домовимося, що $t_{s(1)} = t_{0(2)}$.

Побудуємо гомоморфізм f_1, визначений за $f_1\left(S\left(a_1,a_2,a_3\right)\right) = S\left(1,a_1,a_2\right)$.

Проведемо обчислення: $\gamma_{(1)} = \left[h_{1(1)},...,h_{s(1)}\right] = \left(h_{ij}\right)_{(1)} = t_{(i-1)(1)}^{-1} f_1\left(\left(a_{ij}\right)_{(1)}\right)\left(b_{ij}\right)_{(1)} t_{i(1)}$,

де $i = \overline{1,s(1)}$, $j = \overline{1,r_{i(1)}}$, $f_1\left(\left(a_{ij}\right)_{(1)}\right)\left(b_{ij}\right)_{(1)} = S\left(1, a_{ij(1)_1} + b_{ij(1)}, a_{ij(1)_2} + a_{ij(1)_1} b_{ij(1)}^{q_0}\right)$ та визначимо гомоморфізм $f_2\left(S\left(1,a_2,a_3\right)\right) = S\left(1,0,a_2\right)$.

Обчислимо $\gamma_{(2)} = \left[h_{1(2)},...,h_{s(2)}\right] = \left(h_{ij}\right)_{(2)} = t_{(i-1)(2)}^{-1} f_2\left(\left(a_{ij}\right)_{(2)}\right)\left(b_{ij}\right)_{(2)} t_{i(2)}$,

де $i = \overline{1,s(2)}$, $j = \overline{1,r_{i(2)}}$ та $f_2\left(\left(a_{ij}\right)_{(2)}\right)\left(b_{ij}\right)_{(2)} = S\left(1,0,a_{ij(2)_2} + b_{ij(2)}\right)$.

Отримали відкритий $\left[f_1, f_2, (\alpha_k, \gamma_k)\right]$ та закритий $\left[\beta_{(k)}, \left(t_{0(k)},...,t_{s(k)}\right)\right]$, $k = \overline{1,2}$ ключі.

Для шифрування використаємо повідомлення $m \in A\left(P_\infty\right)$, $m = S\left(m_1,m_2,m_3\right)$, $m_1 \in F_q \setminus \{0\}$, $m_2, m_3 \in F_q$ та відкритий ключ $\left[f_1, f_2, (\alpha_k, \gamma_k)\right]$, $k = \overline{1,2}$, в результаті отримаємо зашифрований текст $\left(y_1, y_2, y_3, y_4\right)$ повідомлення m.

Згенеруємо випадковий $R = (R_1, R_2)$, $R_1, R_2 \in Z_{|F_q|}$. Обчислимо:

$$y_1 = \alpha'(R) \cdot m = \alpha_1'(R_1) \cdot \alpha_2'(R_2) \cdot m = S\left(a_{(1)_1}(R_1) a_{(2)_1}(R_2), a_{(2)_1}(R_2) a_{(1)_2}(R_1) + a_{(2)_2}(R_2),\right.$$
$$a_{(2)_1}(R_2)^{2q_0+1} a_{(1)_3}(R_1) + a_{(2)_1}(R_2) a_{(2)_2}(R_2)^{2q_0} a_{(1)_2}(R_1) + a_{(2)_3}(R_2)\ \left.\right) \cdot m =$$
$$S\left(\ a_{(1)_1}(R_1) a_{(2)_1}(R_2) m_1, a_{(2)_1}(R_2) a_{(1)_2}(R_1) m_1 + a_{(2)_2}(R_2) m_1 + m_2, m_3 + *\ \right).$$

Тут $(*)$ компоненти визначаються перехресними обчисленнями в груповій операції добутку $a_{(i)_j}(R_i)$. Обчислимо:

$$y_2 = \gamma'(R) = \gamma_1'(R_1) \cdot \gamma_2'(R_2) = S\left(*, a_{(1)_1}(R_1) + \beta_{(1)}(R_1) + *, a_{(2)_2}(R_2) + \beta_{(2)}(R_2) + *\right).$$

Тут $(*)$ компоненти визначаються перехресними обчисленнями в груповій операції добутку $t_{0(k)},...,t_{s(k)}$, а для третьої координати додається добуток $a_{(1)_1}(R_1) + \beta_{(1)}(R_1)$.

Обчислимо

$y_3 = f_1\left(\alpha_1'(R_1)\right) = S\left(1, a_{(1)_1}(R_1), a_{(1)_1}(R_1) + a_{(1)_2}(R_1) + *\right)$; $y_4 = f_2\left(\alpha_2'(R_2)\right) = S\left(1, 0, a_{(2)_2}(R_2)\right)$.

Тут $(*)$ компоненти визначаються перехресними обчисленнями в груповій операції добутку $a_{(1)_1}(R_1)$. Маємо зашифроване повідомлення (y_1, y_2, y_3, y_4).

Для дешифрування беремо зашифрований текст (y_1, y_2, y_3, y_4) та закритий ключ $\left[\beta_{(k)}, \left(t_{0(k)}, ..., t_{s(k)}\right)\right]$, $k = \overline{1,2}$. В результаті маємо отримати повідомлення $m \in A(P_\infty)$, що відповідає зашифрованому тексту (y_1, y_2, y_3, y_4).

Щоб розшифрувати повідомлення m, нам потрібно відновити випадкові числа $R = (R_1, R_2)$. Параметр $a_{(1)_1}(R_1)$ відомий з y_3 і він включений у другий компонент y_2.

Обчислимо $D^{(1)}(R_1, R_2) = t_{0(1)} \cdot y_2 t_{s(2)}^{-1} = S\left(1, a_{(1)_1}(R_1) + \beta_{(1)}(R_1), a_{(2)_2}(R_2) + \beta_{(2)}(R_2) + *\right)$

та $D^*(R) = y_3^{-1} D^{(1)}(R_1, R_2) = S\left(1, \beta_{(1)}(R_1), a_{(2)_2}(R_2) + \beta_{(2)}(R_2) + *\right)$.

Відновимо R_1 з $\beta_{(1)}(R_1)$ за допомогою $\beta_{(1)}(R_1)^{-1}$, оскільки β – просте.

Для подальшого розрахунку необхідно видалити компонент масиву $\gamma_1'(R_1)$ з y_2.

Обчислимо $y_2^{(1)} = \gamma_1'(R_1)^{-1} y_2 = \gamma_2'(R_2) = S\left(*, *, a_{(2)_2}(R_2) + \beta_{(2)}(R_2) + *\right)$.

Повторимо обчислення для R_1 відновлення $y_2^{(1)}$:

$D^{(2)}(R_2) = t_{0(2)} \cdot y_2^{(1)} t_{s(2)}^{-1} = S\left(1, 0, a_{(2)_2}(R_2) + \beta_{(2)}(R_2)\right)$ та $D^*(R) = y_4^{-1} D^{(2)}(R_2) = S\left(1, 0, \beta_{(2)}(R_2)\right)$.

Відновимо R_2 з $\beta_{(2)}(R_2)$ за допомогою $\beta_{(2)}(R_2)^{-1}$. Таким чином, відновлюємо $R = (R_1, R_2)$ та повідомлення m від y_1: $m = \alpha'(R_1, R_2)^{-1} \cdot y_1$.

Практична реалізація

Перевіримо правильність отриманих результатів практичними розрахунками. Зафіксуємо групу $A(P_\infty) = \left\{S(a,b,c) \middle| a \in F_q \setminus \{0\}, b, c \in F_q\right\}$ на основі автоморфізму $\sigma(x), \sigma(y)$ над F_q, $q = 2q_0^2$, $q_0 = 2^3$, $g(\mathrm{x}) = x^7 + x^3 + 1$. Групова операція визначається як добуток двох матриць:

$$S(a_1, b_1, c_1) S(a_2, b_2, c_2) = S(a_1 a_2, a_2 b_1 + b_2, a_2^{2q_0+1} c_1 + a_2 b_2^{2q_0} b_1 + c_2)$$

Обернений елемент визначається як $S(a,b,c)^{-1} = S\left(a^{-1}, -a^{-1}b, \left(a^{-1}b\right)^{2q_0+1} - a^{-(2q_0+1)}c\right)$.

Побудуємо прості логарифмічні підписи $\beta_{(1)} = \left[B_{1(1)}, ..., B_{s(1)}\right] = \left(b_{ij}\right)_{(1)} = S\left(1, b_{ij(1)}, 0\right)$ типу $\left(r_{1(1)}, ..., r_{s(1)}\right)$, $i = \overline{1, s(1)}$, $j = \overline{1, r_{i(1)}}$, $b_{ij(1)} \in F_q$ для координати b та $\beta_{(2)} = \left[B_{1(2)}, ..., B_{s(2)}\right] = \left(b_{ij}\right)_{(2)} = S\left(1, 0, b_{ij(2)}\right)$ типу $\left(r_{1(2)}, ..., r_{s(2)}\right)$, $i = \overline{1, s(2)}$, $j = \overline{1, r_{i(2)}}$, $b_{ij(2)} \in F_q$ для координати c.

Логарифмічні підписи β_1 та β_2 в групі визначають координати $b_{ij(1)}$ та $b_{ij(2)}$. Типи $\left(r_{1(k)}, ..., r_{s(k)}\right)$ і логарифмічні підписи β_1 і β_2 вибираються самостійно. Для практичних розрахунків беремо логарифмічні підписи β_1 та β_2 з типами $\left(r_{1(1)}, r_{2(1)}, r_{3(1)}\right) = \left(2^2, 2^3, 2^2\right)$, $\left(r_{1(2)}, r_{2(2)}, r_{3(2)}\right) = \left(2^2, 2^2, 2^3\right)$, а масиви $b_{ij(1)}$ та $b_{ij(2)}$ складаються з трьох підмасивів з кількістю рядків, що дорівнює r_i. Можемо вибрати будь-яку фрагментацію масивів за умови $\prod_{i=1}^{s} r_i = q$. У нашому випадку маємо $\prod_{i=1}^{s} r_i = 2^7$. Кожен рядок b_{ij} є елементом поля F_q.

Побудова масивів логарифмічних підписів представлена в [12].

Перший етап полягає в генерації простого логарифмічного підпису з розмірністю відповідного вибраного типу $\left(r_{1(k)},...,r_{s(k)}\right)$ та кінцевим полем F_q. Для підвищення безпеки масивів β_k можна використовувати різні криптографічні перетворення. Наприклад, такі прості, як додавання векторів шуму, перестановки рядків у підмасивах B_i, злиття масивів B_i, їх перестановка, перетворення матриці. У цьому прикладі використовуємо шум масиву. Це дозволяє побудувати два різні логарифмічні підписи β_1 та β_2.

У рядку та представленні поля β_1, β_2 мають наступний вигляд:

β_1=	$b_{ij(1)}$			$S\left(0,b_{ij(1)},0\right)$	β_2=	$b_{ij(2)}$			$S\left(0,0,b_{ij(2)}\right)$
$B_{1(1)}$	00	000	00	0,0,0	$B_{1(2)}$	00	00	000	0,0,0
	10	000	00	0,α^{0},0		10	00	000	0,0,α^{0}
	01	000	00	0,α^{1},0		01	00	000	0,0,α^{1}
	11	000	00	0,α^{31},0		11	00	000	0,0,α^{31}
$B_{2(1)}$	00	000	00	0,0,0	$B_{2(2)}$	01	00	000	0,0,α^{1}
	01	100	00	0,α^{32},0		00	10	000	0,0,α^{2}
	10	010	00	0,α^{7},0		11	01	000	0,0,α^{15}
	11	110	00	0,α^{93},0		11	11	000	0,0,α^{93}
	11	001	00	0,α^{121},0	$B_{3(2)}$	10	11	000	0,0,α^{84}
	01	101	00	0,α^{16},0		10	11	100	0,0,α^{46}
	10	011	00	0,α^{11},0		00	10	010	0,0,α^{9}
	11	111	00	0,α^{51},0		00	00	110	0,0,α^{35}
$B_{3(1)}$	00	101	00	0,α^{64},0		10	11	001	0,0,α^{120}
	11	011	10	0,α^{89},0		11	10	101	0,0,α^{76}
	00	11	01	0,α^{117},0		01	10	011	0,0,α^{29}
	11	000	11	0,α^{113},0		00	10	111	0,0,α^{48}

Масиви логарифмічних підписів β_1 та β_2 в груповому представленні визначають координати $b_{ij(1)}$ і $b_{ij(2)}$ відповідно:

$$\beta_{(1)}=\left[B_{1(1)},...,B_{s(1)}\right]=\left(b_{ij}\right)_{(1)}=S\left(0,b_{ij(1)},0\right),\ \beta_{(2)}=\left[B_{1(2)},...,B_{s(2)}\right]=\left(b_{ij}\right)_{(2)}=S\left(0,0,b_{ij(2)}\right).$$

Побудуємо випадкові накриття α_k для одного типу, як β_1 і β_2:

$$\alpha_{(\mathrm{k})}=\left[A_{1(\mathrm{k})},...,A_{\mathrm{s}(\mathrm{k})}\right]=\left(a_{ij}\right)_{(\mathrm{k})}=S\left(a_{ij(\mathrm{k})_1},a_{ij(\mathrm{k})_2},a_{ij(\mathrm{k})_3}\right),$$

де $a_{ij(k)_1},a_{ij(k)_2},a_{ij(k)_3}\in F_q\setminus\{0\}$, $i=\overline{1,s}$, $j=\overline{1,r_{i(k)}}$, $k=\overline{1,2}$. Кожне накриття α_k визначається трьома масивами $\left(a_{ij(k)_1},a_{ij(k)_2},a_{ij(k)_3}\right)$ з ненульовими записами. У полі представлення $\alpha_k=S\left(a_{ij(k)_1},a_{ij(k)_2},a_{ij(k)_3}\right)$ має вигляд:

$\alpha_1=\left[A_{1(1)},A_{2(1)},A_{3(1)}\right]$			$\alpha_2=\left[A_{1(2)},A_{2(2)},A_{3(2)}\right]$		
$A_{1(1)}$	$A_{2(1)}$	$A_{3(1)}$	$A_{1(2)}$	$A_{2(2)}$	$A_{3(2)}$
α^{97}, α^{107}, α^{71}	α^{110}, α^{100}, α^{44}	α^{35}, α^{28}, α^{15}	α^{106}, α^{78}, α^{81}	α^{43}, α^{16}, α^{90}	α^{99}, α^{93}, α^{87}
α^{107}, α^{82}, α^{55}	α^{67},α^{2},α^{87}	α^{105}, α^{19}, α^{68}	α^{92}, α^{33}, α^{41}	α^{114}, α^{85}, α^{82}	α^{65}, α^{88}, α^{23}
α^{118}, α^{86}, α^{6}	α^{43}, α^{86}, α^{87}	α^{45}, α^{8}, α^{29}	α^{124}, α^{80}, α^{125}	α^{21}, α^{77}, α^{114}	α^{17}, α^{68}, α^{73}
α^{69}, α^{17}, α^{54}	α^{70}, α^{95}, α^{125}	α^{23}, α^{42}, α^{82}	α^{48}, α^{63}, α^{47}	α^{92}, α^{71}, α^{119}	α^{116}, α^{98}, α^{116}
	α^{101}, α^{45}, α^{115}				α^{0},α^{53},α^{4}
	α^{40}, α^{82}, α^{25}				α^{108}, α^{79}, α^{81}
	α^{19}, α^{60}, α^{84}				α^{85}, α^{62}, α^{23}
	α^{29}, α^{55}, α^{112}				α^{81}, α^{29}, α^{49}

Згенеруємо випадкові $t_{0(k)}, t_{1(k)}, ..., t_{s(k)} \in A(P_\infty) \setminus Z$, $s = 3$, $k = \overline{1,2}$ та $t_{3(1)} = t_{0(2)}$.

Для логарифмічних підписів β_1, β_2 отримаємо представлення:

$t_{0(1)}, t_{1(1)}, ..., t_{s(1)}$	$t_{0(2)}, t_{1(2)}, ..., t_{s(2)}$
$t_{0(1)=(}\ \alpha^{122}, \alpha^{115}, \alpha^{0})$ $t_{1(1)}=(\ \alpha^{23}, \alpha^{93}, \alpha^{107})$ $t_{2(1)}=(\ \alpha^{30}, \alpha^{105}, \alpha^{23})$ $t_{3(1)}=(\ \alpha^{122}, \alpha^{117}, \alpha^{49})$	$t_{0(2)}=(\ \alpha^{122}, \alpha^{117}, \alpha^{49})$ $t_{1(2)}=(\ \alpha^{98}, \alpha^{9}, \alpha^{109})$ $t_{2(2)}=(\ \alpha^{58}, \alpha^{44}, \alpha^{110})$ $t_{3(2)}=(\ \alpha^{32}, \alpha^{120}, \alpha^{53})$
$t_{-10(1)}=(\ \alpha^{122}, \alpha^{95}, \alpha^{100})$ $t_{-11(1)}=(\ \alpha^{23}, \alpha^{102}, \alpha^{68})$ $t_{-12(1)}=(\ \alpha^{30}, \alpha^{34}, \alpha^{89})$ $t_{-10(1)}=(\ \alpha^{122}, \alpha^{100}, \alpha^{27})$	$t_{-10(2)}=(\ \alpha^{122}, \alpha^{100}, \alpha^{27})$ $t_{-11(2)}=(\ \alpha^{98}, \alpha^{23}, \alpha^{10})$ $t_{-12(2)}=(\ \alpha^{58}, \alpha^{117}, \alpha^{50})$ $t_{-13(2)}=(\ \alpha^{32}, \alpha^{69}, \alpha^{38})$

Наступним кроком є обчислення масивів γ_1 і γ_2.

За початковими умовами прикладу отримуємо:

$$\gamma_1 = \left[h_{1(1)}, ..., h_{3(1)} \right] = \left(h_{ij} \right)_1 = t_{(i-1)(1)}^{-1} f_1 \left(\left(a_{ij} \right)_1 \right) \left(b_{ij} \right)_1 t_{i(1)};$$

$$\gamma_2 = \left[h_{1(2)}, ..., h_{3(2)} \right] = \left(h_{ij} \right)_2 = t_{(i-1)(2)}^{-1} f_2 \left(\left(a_{ij} \right)_2 \right) \left(b_{ij} \right)_2 t_{i(2)}.$$

Побудуємо гомоморфізм f_1, визначений за $f_1\left(S\left(a_1, a_2, a_3\right)\right) = S\left(1, a_1, a_2\right)$, та визначимо гомоморфізм f_2: $f_2\left(S\left(1, a_2, a_3\right)\right) = S\left(1, 0, a_2\right)$.

У полі представлення $\gamma_k = S(h_{ij(k)_1}, h_{ij(k)_2}, h_{ij(k)_3})$, $k = \overline{1,2}$ має вигляд:

$\gamma_1 = S(h_{ij(1)_1}, h_{ij(1)_2}, h_{ij(1)_3})$			$\gamma_2 = S(h_{ij(2)_1}, h_{ij(2)_2}, h_{ij(2)_3})$		
$h_{1(1)}$	$h_{2(1)}$	$h_{3(1)}$	$h_{1(2)}$	$h_{2(2)}$	$h_{3(2)}$
$\alpha^{28}, \alpha^{81}, \alpha^{39}$	$\alpha^{7}, \alpha^{93}, \alpha^{65}$	$\alpha^{92}, \alpha^{16}, \alpha^{80}$	$\alpha^{103}, \alpha^{42}, \alpha^{93}$	$\alpha^{87}, \alpha^{27}, \alpha^{14}$	$\alpha^{101}, \alpha^{79}, \alpha^{29}$
$\alpha^{28}, \alpha^{52}, \alpha^{39}$	$\alpha^{7}, \alpha^{115}, \alpha^{17}$	$\alpha^{92}, \alpha^{53}, \alpha^{102}$	$\alpha^{103}, \alpha^{42}, \alpha^{99}$	$\alpha^{87}, \alpha^{27}, \alpha^{120}$	$\alpha^{101}, \alpha^{79}, \alpha^{51}$
$\alpha^{28}, \alpha^{32}, \alpha^{49}$	$\alpha^{7}, \alpha^{56}, \alpha^{42}$	$\alpha^{92}, \alpha^{51}, \alpha^{117}$	$\alpha^{103}, \alpha^{42}, \alpha^{80}$	$\alpha^{87}, \alpha^{27}, \alpha^{16}$	$\alpha^{101}, \alpha^{79}, \alpha^{55}$
$\alpha^{28}, \alpha^{42}, \alpha^{92}$	$\alpha^{7}, \alpha^{66}, \alpha^{105}$	$\alpha^{92}, \alpha^{57}, \alpha^{114}$	$\alpha^{103}, \alpha^{42}, \alpha^{22}$	$\alpha^{87}, \alpha^{27}, \alpha^{1}$	$\alpha^{101}, \alpha^{79}, \alpha^{38}$
	$\alpha^{7}, \alpha^{44}, \alpha^{106}$				$\alpha^{101}, \alpha^{79}, \alpha^{20}$
	$\alpha^{7}, \alpha^{17}, \alpha^{88}$				$\alpha^{101}, \alpha^{79}, \alpha^{120}$
	$\alpha^{7}, \alpha^{109}, \alpha^{50}$				$\alpha^{101}, \alpha^{79}, \alpha^{53}$
	$\alpha^{7}, \alpha^{26}, \alpha^{7}$				$\alpha^{101}, \alpha^{79}, \alpha^{63}$

Для прикладу беремо $R_1 = 77$. Отримаємо наступну базову факторизацію для заданого типу $\left(r_{1(1)}, r_{2(1)}, r_{3(1)}\right) = \left(2^2, 2^3, 2^2\right)$ у формі $R_1 = \left(R_{1(1)}, R_{2(1)}, R_{3(1)}\right) = (1, 3, 2)$, де $R_1 + R_2 2^2 + R_3 2^5 = 77$ та обчислюємо γ_1:

$$\gamma_1(77) = h_{1(1)}(1) h_{2(1)}(3) h_{3(1)}(2) = S(\alpha^{28}, \alpha^{52}, \alpha^{39}) S(\alpha^{7}, \alpha^{66}, \alpha^{105}) S(\alpha^{92}, \alpha^{51}, \alpha^{117}) = S\left(\alpha^{0}, \alpha^{83}, \alpha^{56}\right).$$

Для прикладу беремо $R_2 = 53$. Отримуємо $R_2 = \left(R_{1(2)}, R_{2(2)}, R_{3(2)}\right) = (1, 1, 3) = 53$ для заданого типу $\left(r_{1(2)}, r_{2(2)}, r_{3(2)}\right) = \left(2^2, 2^2, 2^3\right)$ та отримуємо γ_2:

$$\gamma_2(53) = h_{1(2)}(1) h_{2(2)}(1) h_{3(2)}(3) = S\left(\alpha^{103}, \alpha^{42}, \alpha^{99}\right) S\left(\alpha^{87}, \alpha^{27}, \alpha^{120}\right) S\left(\alpha^{101}, \alpha^{79}, \alpha^{38}\right) = S\left(\alpha^{37}, \alpha^{4}, \alpha^{52}\right).$$

Практичні розрахунки кроку шифрування виконуємо наступним чином.

Нехай $m = \left(\alpha^0, \alpha^1, \alpha^2\right) = S\left(\alpha^0, \alpha^1, \alpha^2\right)$. Згенеруємо випадковий $R = (R_1, R_2)$, $R_1, R_2, \in \square_{|F_q|}$.

Нехай $R_1 = 77$ і $R_2 = 53$. Обчислимо

$$y_1 = \alpha'(R)\cdot m = \alpha_1'(77)\cdot\alpha_2'(53)\cdot m = \alpha_{1(1)}(1)\cdot\alpha_{2(1)}(3)\cdot\alpha_{3(1)}(2)\cdot\alpha_{1(2)}(1)\cdot\alpha_{2(2)}(1)\cdot\alpha_{3(2)}(3)\cdot m = S(\alpha^{107},\alpha^{82},\alpha^{55})$$

$$S(\alpha^{70},\alpha^{95},\alpha^{125})S(\alpha^{45},\alpha^{8},\alpha^{29})S(\alpha^{92},\alpha^{33},\alpha^{41})S(\alpha^{114},\alpha^{85},\alpha^{82})S(\alpha^{116},\alpha^{98},\alpha^{116})$$

$$S\left(\alpha^0,\alpha^1,\alpha^2\right) = S\left(\alpha^{36},\alpha^{86},\alpha^4\right),$$

$$y_2 = \gamma'(R) = \gamma_1'(77)\cdot\gamma_2'(53) = S\left(\alpha^0,\alpha^{83},\alpha^{56}\right)S\left(\alpha^{37},\alpha^4,\alpha^{52}\right) = S\left(\alpha^{37},\alpha^{27},\alpha^{83}\right),$$

$y_3 = f_1\left(\alpha_1'(R_1)\right) = S\left(\alpha^0,\alpha^{36},\alpha^{16}\right)$ та $y_4 = f_2\left(\alpha_2'(R_2)\right) = S\left(\alpha^0,0,\alpha^{21}\right)$.

Тоді зашифроване повідомлення має вигляд

$y_1 = \left(\alpha^{36},\alpha^{86},\alpha^4\right)$, $y_2 = \left(\alpha^{37},\alpha^{27},\alpha^{83}\right)$, $y_3 = \left(\alpha^0,\alpha^{36},\alpha^{16}\right)$, $y_4 = \left(\alpha^0,0,\alpha^{21}\right)$. Щоб розшифрувати повідомлення m, нам потрібно відновити випадкові числа $R = (R_1, R_2)$. Обчислимо

$$D^{(1)}(R_1,R_2) = t_{0(1)}y_2t_{s(2)}^{-1} = S\left(\alpha^{122},\alpha^{115},\alpha^0\right)S\left(\alpha^{36},\alpha^{86},\alpha^4\right)S\left(\alpha^{32},\alpha^{120},\alpha^{53}\right)^{-1} =$$

$$S\left(\alpha^{122},\alpha^{115},\alpha^0\right)S\left(\alpha^{36},\alpha^{86},\alpha^4\right)S\left(\alpha^{32},\alpha^{69},\alpha^{38}\right) = S\left(\alpha^0,\alpha^{12},\alpha^{114}\right)$$

$$D^*(R) = y_3^{-1}D^{(1)}(R_1,R_2) = S\left(\alpha^0,\alpha^{36},\alpha^{16}\right)^{-1}S\left(\alpha^0,\alpha^{12},\alpha^{114}\right) = S\left(\alpha^0,\alpha^{36},\alpha^{34}\right)S\left(\alpha^0,\alpha^{12},\alpha^{114}\right) = S\left(\alpha^0,\alpha^{68},\alpha^{35}\right).$$

Отримаємо $\beta_1(R_1) = \alpha^{68} = (0100101)$.

Відновлення R_1 від $\beta_1(R_1)$

01|001|01	R_1=(*,*,2)
00|111|01	ряд від β(1)
01|110|00	R_1= (*,3,2)
11|110|00	рядок від β(1)
10|000|00	R_1=(1,3,2)

Для подальших обчислень необхідно вилучити $\alpha_1'(R_1)$ з шифротексту компоненти масивів (y_1, y_2) і $\gamma_1'(R_1)$. Обчислимо:

$$y_2^{(1)} = \gamma_1'(R_1)^{-1}y_2 = S\left(\alpha^0,\alpha^{83},\alpha^{56}\right)^{-1}S\left(\alpha^{37},\alpha^{27},\alpha^{83}\right) = S\left(\alpha^0,\alpha^{83},\alpha^{94}\right)^{-1}S\left(\alpha^{37},\alpha^{27},\alpha^{83}\right) = S\left(\alpha^{37},\alpha^4,\alpha^{52}\right).$$

Повторимо обчислення

$$D^{(2)}(R_2) = t_{0(2)}y_2^{(1)}t_{s(2)}^{-1} = S\left(\alpha^{122},\alpha^{117},\alpha^{49}\right)S\left(\alpha^{37},\alpha^4,\alpha^{52}\right)S\left(\alpha^{32},\alpha^{120},\alpha^{53}\right)^{-1} = S\left(\alpha^0,0,\alpha^{18}\right)$$

та

$$D^*(R) = D^{(2)}(R_2)y_4^{-1} = D^{(2)}(R_2)S\left(0,0,a_{(2)_2}(R_2)\right)^{-1} = S\left(\alpha^0,0,\alpha^{18}\right)S\left(\alpha^0,0,\alpha^{21}\right)^{-1} = S\left(\alpha^0,0,\alpha^{25}\right).$$

Відновимо R_2 з $\beta_2(R_2) = \alpha^{25} = (1010110)$.

Виконаємо обернені обчислення $\beta_2(R_2)^{-1}$. Виберемо групи бітів у векторі $\beta(R)$ відповідно до типу $\left(r_{1(2)},...,r_{s(2)}\right) = \left(3,3^2,3^2\right)$. Використовуємо ті ж обчислення, що й у прикладі для $\beta_1(R_1)^{-1}$, та отримаємо:

10|10|110	R_2=(*,*,3)
00|00|110	рядок від β(2)
10|10|000	R_2= (*,1,3)
00|10|000	рядок від β(2)
10|00|000	R_2=(1,1,3)

$$\beta_2(R')^{-1} = 2|02|01 = \left(R_{1(2)},R_{2(2)},R_{3(2)}\right) = (1,1,3),$$

$$R_2 = \left(R_{1(2)},R_{2(2)},R_{3(2)}\right) = (1,1,3) = 53.$$

Дешифруємо повідомлення:

$$m = \alpha'(R)^{-1} y_1 = \alpha_2'(R_2)^{-1} \cdot \alpha_1'(R_1)^{-1} \cdot y_1 = S\left(\alpha^{36}, \alpha^{39}, \alpha^{99}\right)^{-1} S\left(\alpha^{36}, \alpha^{86}, \alpha^{4}\right) =$$

$$S\left(\alpha^{91}, \alpha^{3}, \alpha^{19}\right) S\left(\alpha^{36}, \alpha^{86}, \alpha^{4}\right) = S\left(\alpha^{0}, \alpha^{1}, \alpha^{2}\right).$$

Отримуємо повідомлення $m = \left(a^0, a^1, a^2\right)$.

Аналіз безпеки запропонованого методу

Мета криптоаналітика – знайти невідомий закритий ключ $\left[\beta_{(1)}, \beta_{(2)}, \left(t_{0(1)}, ..., t_{s(1)}\right), \left(t_{0(2)}, ..., t_{s(2)}\right)\right]$. Основні вирази, які визначають параметри відкритого та закритого ключів, такі:

$S(a_1, b_1, c_1) S(a_2, b_2, c_2) = S(a_1 a_2, a_2 b_1 + b_2, a_2^{2q_0+1} c_1 + a_2 b_2^{2q_0} b_1 + c_2)$;

$\beta_{(1)} = \left(b_{ij}\right)_{(1)} = S\left(1, b_{ij(1)}, 0\right)$, $\beta_{(2)} = \left(b_{ij}\right)_{(2)} = S\left(1, 0, b_{ij(2)}\right)$ типів $\left(r_{1(\mathrm{k})}, ..., r_{s(\mathrm{k})}\right)$;

$t_{i(k)} = S\left(t_{i(k)_a}, t_{i(k)_b}, t_{i(k)_c}\right)$;

$\left(a_{ij}\right)_{(\mathrm{k})} = S\left(a_{ij(\mathrm{k})_a}, a_{ij(\mathrm{k})_b}, a_{ij(\mathrm{k})_c}\right)$;

$\gamma_{(\mathrm{k})} = \left(h_{ij}\right)_{(\mathrm{k})} = t_{(i-1)(\mathrm{k})}^{-1} f_k\left(\left(a_{ij}\right)_{(\mathrm{k})}\right)\left(b_{ij}\right)_{(\mathrm{k})} t_{i(\mathrm{k})} = S\left(h_{ij(\mathrm{k})_a}, h_{ij(\mathrm{k})_b}, h_{ij(\mathrm{k})_c}\right)$.

Масив $\gamma_{(\mathrm{k})}$ векторів складається з підмасивів $\gamma_{(1)}$ і $\gamma_{(2)}$, які, в свою чергу, складаються з $s(1)$ і $s(2)$ блоків відповідно.

Розглянемо можливості криптоаналітика на основі $\gamma_{(1)}$ аналізу. Вираз $\gamma_{(1)}$ має вигляд

$$\gamma_{(1)} = \left(h_{ij}\right)_{(1)} = t_{(i-1)(1)}^{-1} f_1\left(\left(a_{ij}\right)_{(1)}\right)\left(b_{ij}\right)_{(1)} t_{i(1)} = S\left(h_{ij(1)_a}, h_{ij(1)_b}, h_{ij(1)_c}\right)$$

Беремо $h_{ij(1)_a}, h_{ij(1)_b}, h_{ij(1)_c}$, наприклад, для першого блоку $\gamma_{(1)}$ масиву:

$h_{1j(1)_a} = t_{0(1)_a}^{*} t_{1(1)_a}$

$h_{1j(1)_b} = t_{0(1)_b}^{*} t_{1(1)_a} + a_{1j(1)_a} t_{1(1)_a} + b_{1j(1)} t_{1(1)_a} + t_{1(1)_b}$

$h_{1j(1)_c} = t_{1(1)_a}^{2q_0+1} t_{0(1)_c}^{*} + t_{1(1)_a}^{2q_0+1} t_{0(1)_b}^{*} a_{1j(1)_a}^{2q_0} + t_{1(1)_a}^{2q_0+1} t_{0(1)_b}^{*} b_{1j(1)}^{2q_0} + t_{1(1)_a}^{2q_0+1} a_{1j(1)_b} +$

$t_{1(1)_a}^{2q_0+1} a_{1j(1)_a} b_{1j(1)}^{q_0} + t_{1(1)_a} t_{1(1)_b}^{2q_0} t_{0(1)_b}^{*} + t_{1(1)_a} t_{1(1)_b}^{2q_0} a_{1j(1)_a} + t_{1(1)_a} t_{1(1)_b}^{2q_0} b_{1j(1)} + t_{1(1)_c}$

Значення $h_{1j(1)_a} = t_{0(1)_a}^{*} t_{1(1)_a}$ однакове для будь-якого j. Якщо додамо елементи з першого зразкового блоку для різних j, то отримаємо

$$\sum_{j \in J} h_{1j(1)_b} = |J| t_{0(1)_b}^{*} t_{1(1)_a} + t_{1(1)_a} \sum_{j \in J} a_{1j(1)_a} + t_{1(1)_a} \sum_{j \in J} b_{1j(1)}$$

$|J|$ – кількість елементів у J наборі. Для парного значення $|J|$ отримуємо рівняння $\sum_{j \in J} h_{1j(1)_b} = t_{1(1)_a} \sum_{j \in J} a_{1j(1)_a} + t_{1(1)_a} \sum_{j \in J} b_{1j(1)}$ з двома невідомими $t_{1(1)_a}$ і $\sum_{j \in J} b_{1j(1)}$. Існує кілька $q-1$ можливих $t_{1(1)_a}$ варіантів. Зафіксуємо значення $\hat{t}_{1(1)_a}$ і нехай $|J| = 2$. Складемо всі вибірки з пар значень. У нас є $r_{1(1)}(r_{1(1)} - 1)/2$ рівняння для невідомих $b_{1j(1)}$:

$$\hat{t}_{1(1)_a}^{-1} \sum_{j \in J} h_{1j(1)_b} + \sum_{j \in J} a_{1j(1)_a} + \sum_{j \in J} b_{1j(1)} = 0.$$

Розв'язок цих рівнянь визначає логарифмічний підпис для першого блоку відносно вибраного $\hat{t}_{1(1)_a}$. Оскільки є $q-1$ можливі варіанти $t_{1(1)_a}$, отримуємо $q-1$ можливі варіанти логарифмічних підписів. Оскільки для побудови логарифмічного підпису використовується

рандомізація на основі шуму, злиття та матричні перетворення підблоків, питання про те, як можна встановити, що $\hat{t}_{1(1)_a}$ – істинне, не має відповіді. Припустимо, що рівняння матриці перетворення для логарифмічних сигнатур мають поліноміальну оцінку складності розділь-ної здатності, тоді нижню межу можна взяти для оцінки складності атаки $b_{1j(1)}$ на $\mathrm{O}(q)$. Для $\hat{t}_{1(1)_a}$ можна обчислити , $\hat{t}^*_{0(1)_a} = \hat{t}^{-1}_{1(1)_a} h_{1j(1)_a}$, а щоб визначити $t^*_{0(1)_b}$, $t_{1(1)_b}$ потрібно розв'язати рів-няння $h_{1j(1)_b} = t^*_{0(1)_b} t_{1(1)_a} + a_{1j(1)_a} t_{1(1)_a} + b_{1j(1)} t_{1(1)_a} + t_{1(1)_b}$.

Існують $q-1$ можливі варіанти $t^*_{0(1)_b}$, $t_{1(1)_b}$. Тоді отримуємо оцінку складності атаки за $t_{i(1)_a}, t_{i(1)_b}$ параметрами $t_{i(1)}$ вектора, що дорівнює $\mathrm{O}(q^2)$. Це те саме для визначення $t^*_{0(1)_c}$, $t_{1(1)_c}$, де можна розв'язати рівняння для $h_{1j(1)_c}$ в межах вибору $q-1$ можливих значень $t^*_{0(1)_c}$, $t_{1(1)_c}$. Результуюча атака на $t_{i(1)} = S\left(t_{i(1)_a}, t_{i(1)_b}, t_{i(1)_c}\right)$ за складністю буде меншою ніж $\mathrm{O}(q^3)$.

Для $s(1)$ підблоків логарифмічного підпису $\gamma_{(1)}$ маємо застосувати $s(1)$ час для пошуку $t_{i(1)} = S\left(t_{i(1)_a}, t_{i(1)_b}, t_{i(1)_c}\right)$, і підсумкова складність атаки буде оцінена в $\mathrm{O}(q^{3s(1)})$.

Поширимо цю атаку на всі підблоки логарифмічного підпису. Отримаємо вираз $\sum_{i=1,\, j=j_i}^{s(1)} h_{ij(1)_b} = t^*_{0(1)_b} t_{s(1)_a} + t_{s(1)_a} \sum_{i=1,\, j=j_i}^{s(1)} a_{ij(1)_a} + t_{s(1)_a} \sum_{i=1,\, j=j_i}^{s(1)} b_{ij(1)} + t_{s(1)_b}$, де $(j_1, ..., j_{s(1)})$ – номери обраних записів у відповідних підблоках. Зробимо парну вибірку за записами підблоків, отримаємо рівняння

$$\sum_{i=1,\, j\in J_i}^{s(1)} h_{ij(1)_b} = t_{s(1)_a} \sum_{i=1,\, j\in J_i}^{s(1)} a_{ij(1)_a} + t_{s(1)_a} \sum_{i=1,\, j\in J_i}^{s(1)} b_{ij(1)},$$

що однаково для атаки на один підблок. Аналогічний вираз отримуємо для $h_{ij(1)c}$. Можна з високою впевненістю припустити, що складність атаки в цьому випадку не буде меншою $\mathrm{O}(q^3)$.

Розглянемо атаку відновлення $t_{1(1)_a}$ зі значення $b_{1j(1)}$. У рівнянні для $\sum_{j\in J} h_{1j(1)_b}$ будемо вибирати $b_{1j(1)}$ таким чином, що $\sum_{j\in J} b_{1j(1)} = 0$. Значення $\hat{t}_{1(1)_a}$ можуть бути в межах рівняння $\hat{t}^{-1}_{1(1)_a} \sum_{j\in J} h_{1j(1)_b} + \sum_{j\in J} a_{1j(1)_a} = 0$.

Нам відомі $h_{1j(1)_b}$ та $a_{1j(1)_a}$. Атака на логарифмічний підпис була запропонована в [16]. Залишається відкритим питання, як ідентифікувати один раз $\sum_{j\in J} b_{1j(1)} = 0$ для рандомізованого логарифмічного підпису. Якщо побудувати аперіодичний логарифмічний підпис без наявно-сті таких блоків $\sum_{j\in J} b_{1j(1)} = 0$, то така атака стає неможливою [16].

Тепер розглянемо криптоаналіз для масиву $\gamma_{(2)}$. Основні вирази для першого блоку масиву $\gamma_{(2)}$:

$$\gamma_{(2)} = \left(h_{ij}\right)_{(2)} = t^{-1}_{(0)(2)} f_2\left(\left(a_{ij}\right)_{(2)}\right)\left(b_{1j}\right)_{(2)} t_{1(2)} = S\left(t^*_{0(2)_a}, t^*_{0(2)_b}, t^*_{0(2)_c}\right)$$
$$S\left(1, 0, a_{ij(1)_c} + b_{ij(2)}\right) S\left(t_{s(2)_a}, t_{s(2)_b}, t_{s(2)_c}\right) = S\left(h_{ij(2)_a}, h_{ij(2)_b}, h_{ij(2)_c}\right)$$

Узагальнимо цю атаку на всі підблоки логарифмічного підпису. Отримаємо вирази:

$$\sum_{i=1,\,j=j_i}^{s(2)} h_{ij(2)_a} = t^*_{0(2)_a} t_{s(2)_a}, \qquad \sum_{i=1,\,j=j_i}^{s(2)} h_{ij(2)_b} = t^*_{0(2)_b} t_{1(2)_a} + t_{1(2)_b},$$

$$\sum_{i=1,\,j=j_i}^{s(2)} h_{ij(2)_c} = t^{2q_0+1}_{s(2)_a} t^*_{0(2)_c} + t^{2q_0+1}_{s(2)_a} \sum_{i=1,\,j=j_i}^{s(2)} a_{ij(2)_c} + t^{2q_0+1}_{s(2)_a} \sum_{i=1,\,j=j_i}^{s(2)} b_{1j(2)} + t_{s(2)_a} t^{2q_0}_{s(2)_b} t^*_{0(2)_b} + t_{s(2)_c},$$

де $(j_1,..., j_{s(2)})$ – номери виділених записів у відповідних підблоках. Зробимо парну вибірку за записами підблоків, маємо таке рівняння:

$$\sum_{i=1,\,j\in J_i}^{s(2)} h_{ij(2)_c} = t^{2q_0+1}_{s(2)_a} \sum_{i=1,\,j\in J_i}^{s(2)} a_{ij(2)_c} + t^{2q_0+1}_{s(2)_a} \sum_{i=1,\,j\in J_i}^{s(2)} b_{1j(2)}.$$

Рівняння має два невідомих $t_{s(2)_a}$ і $\sum_{j\in J} b_{ij(2)}$. Існують $q-1$ можливі варіанти $t_{s(2)_a}$. Як і у випадку з масивом $\gamma_{(1)}$, у нас є те саме відкрите питання про те, як з'ясувати, де $t_{s(2)_a}$ – істинне значення рандомізованого логарифмічного підпису. Можна з високою впевненістю припустити, що складність атаки на $t_{s(2)_a}$ буде меншою, ніж $O(q)$ в такому випадку, а складність атаки на всі компоненти $t_{0(2)} = S\left(t_{0(2)_a}, t_{0(2)_b}, t_{0(2)_c}\right)$і $t_{s(2)} = S\left(t_{s(2)_a}, t_{s(2)_b}, t_{s(2)_c}\right)$ буде меншою, ніж $O(q^3)$.

Підводячи підсумки щодо атаки з закритим ключем, можна зробити висновок, що складність буде не меншою $O(q^3)$.

Розглянемо основні атаки на зашифрований текст. Успіх атаки зашифрованого тексту визначається знаходженням ключа $R=(R_1,R_2)$. Мають місце наступні види атак.

Атака грубою силою на зашифрований текст. Обираємо $R=(R_1,R_2)$ та спробуємо розшифрувати текст $y_1 = \alpha'(R)\cdot m = \alpha_1'(R_1)\cdot\alpha_2'(R_2)\cdot m$. Успіх атаки визначається попередньою інформацією про повідомлення. Складність атаки визначається умовою повного пошуку ключів R_1, R_2 і його рівністю $O(q^2)$.

Атака грубою силою на $R=(R_1,R_2)$. Обираємо $R=(R_1,R_2)$ відповідно $y_2 = \gamma'(R) = \gamma_1'(R_1)\cdot\gamma_2'(R_2)$. Складність такої атаки $O(q^2)$. Можлива послідовна атака відновлення R_1, R_2. Обираємо R_1 відповідно до значення $a_{(1)_1}(R_1)$ у векторі y_1 та обираємо R_2 відповідно значенню $a_{(2)_2}(R_2)$ у векторі y_2. Атака має складність $O(q)$. Для захисту від атаки послідовного відновлення слід розглянути механізми зв'язування ключів.

Атака на алгоритм. Параметри вилучення $a_{(1)_1}(R_1)$, $a_{(2)_2}(R_2)$з y_3, y_4 не дозволяють обчислити $\alpha_1'(R_1)\cdot\alpha_2'(R_2)$в $y_1 = \alpha_1'(R_1)\cdot\alpha_2'(R_2)\cdot m$. Простий пошук параметрів R_1, R_2 призводить до атаки грубої сили зі складністю q^2. Оскільки група автоморфізму $A(P_\infty)$ функціонального поля Сузукі визначена над великим полем F_q, атака обчислювально неможлива.

Висновки

У роботі обґрунтовано наступні переваги пропозиції: висока секретність схеми шифрування на основі групи автоморфізмів поля $A(P_\infty)$ функції Сузукі над F_q, що дорівнює q^2; довжина зашифрованого тексту призначена $3\log q$ для обчислення в скінченному полі над F_q; обчислення в кінцевому полі простіші в порівнянні з криптосистемою в групі Сузукі. Крім того, шифрування виконується на кінцевому полі втричі меншого розміру порівняно з

криптосистемою на основі груп Сузукі, а довжина логарифмічного масиву підпису визначається кінцевим полем понад F_q і є значно меншою порівняно з криптосистемою MST3.

Реалізація криптосистеми на групі автоморфізмів $A(P_\infty)$ функціонального поля Сузукі вимагає побудови логарифмічного підпису β на векторах 2^h, де h визначається розміром типу $r_i = 2^h$. Підкреслимо, що всі блоки B_i є підгрупами $U(q) = \left\{ S(1,b,c) \middle| b,c \in F_q \right\}$. Розмір масивів β і α визначається типом $(r_1,...,r_s)_b$ і $(r_1,...,r_s)_c$ координатою b,c для підгруп $U(q)$. Для 128-бітної криптографії, яка еквівалентна обчисленням над полем $q = 2^{64}$, якщо r_i тип $r_i = 2^2$, $s = 32$, для криптографії в групі потрібні лише 256 записів по 64 біти. У порівнянні з MST3 у Сузукі 2-групи матиме 256 записів по 128 біт для $r_i = 2^2$, $s = 64$ і 512 записів – для $r_i = 4^2$, $s = 32$. Однак це все ще є недоліком пропозиції з великим розміром ключових даних і необхідністю обчислення оберненого елемента в кінцевому полі.

Список літератури:

1. K.H. Ko, S.J. Lee, J.H .Cheon, J.W. Han, J. Kang, and C. Park. New public-key cryptosystem using braid groups // Advances in cryptology–CRYPTO 2000, vol.1880of Lecture Notes in Computer Science, pp. 166–183, Springer, Berlin, Germany, 2000.
2. B. Eick and D. Kahrobaei. Polycyclic groups: a new platform for cryptology // http://arxiv.org/abs/math/0411077.
3. V. Shpilrain and A. Ushakov. Thompsons group and public key cryptography // Applied Cryptography and Network Security, vol. 3531 of Lecture Notes in Computer Science, pp. 151–164, 2005.
4. D. Kahrobaei, C. Koupparis, and V. Shpilrain. Public key exchange using matrices over group rings // Groups, Complexity, and Cryptology ,vol.5,no.1, pp.97–115, 2013.
5. N.R. Wagner and M.R. Magyarik. A public-key cryptosystem based on the word problem // Proc. Advances in Cryptology–CRYPTO 1984, LNCS 196, Springer-Verlag (1985), pp. 19–36.
6. S.S. Magliveras. A cryptosystem from logarithmic signatures of finite groups // Proceedings of the 29th Midwest Symposium on Circuits and Systems , pp. 972–975, Elsevier Publishing, Amsterdam, The Netherlands, 1986.
7. W. Lempken, S.S. Magliveras, Tran van Trung and W. Wei. A public key cryptosystem based on non-abelian finite groups // Journal of Cryptology, 22 (2009), 62–74.
8. H.Hong, J.Li, L.Wang, Y. Yang, X.Niu. A Digital Signature Scheme Based on MST3 Cryptosystems // Hindawi Publishing Corporation, Mathematical Problems in Engineering, vol 2014, 11 p., http://dx.doi.org/10.1155/2014/630421
9. Y. Cong, H. Hong, J. Shao, S. Han, J. Lin and S. Zhao. A New Secure Encryption Scheme Based on Group Factorization Problem // IEEExplore, November 20, 2019 Digital Object Identifier 10.1109/ACCESS.2019.2954672 https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8907845
10. P. Svaba and T. van Trung. Public key cryptosystem MST3 cryptanalysis and realization // Journal of Mathematical Cryptology,vol.4,no.3,pp.271–315,2010
11. T. van Trung. Construction of strongly aperiodic logarithmic signatures // Journal Math. Cryptol., vol. 12, no. 1, pp. 23–35, 2018.
12. Kotukh Y., Severinov E., Vlasov O., Tenytska A., Zarudna E. Some results of development of cryptographic transformations schemes using non-abelian groups // Радіотехніка. 2021. Вип. 204. С. 66–72.
13. Котух Є., Сєвєрінов О., Власов А. та ін. Методи побудови та властивості логарифмічних підписів // Радіотехніка. 2021. Вип. 205. С. 94–99. https://doi.org/10.30837/rt.2021.2.205.09
14. Kotukh Y., Khalimov G. Hard Problems for Non-abelian Group Cryptography, 2021 // Fifth International Scientific and Technical Conference "Computer and Information systems and technologies". https://doi.org/10.30837/csitic52021232176
15. Халімов Г., Котух Є., Сергійчук Ю., Марухненко О. Аналіз складності реалізацій криптосистеми на групі Сузукі // Радіотехніка. 2018. Вип. 193. С. 75–81.
16. Котух Є., Охріменко Т., Дяченко О., Ротаньова Н., Козіна Л., Зеленський Д. Криптоаналіз систем на основі проблеми слова з використанням логарифмічних підписів // Радіотехніка. 2021. Вип. 206. С. 106–114. https://doi.org/10.30837/rt.2021.3.206.09
17. Kotukh Y., Khalimov G. Towards practical cryptoanalysis of systems based on word problems and logarithmic signatures // Proceedings of II International Conference Information security: problems and prospects, 25 Nov 2022, Baku, Azerbaijan, pp. 55–58.
18. Khalimov G., Kotukh Y. et al. Towards advance encryption based on a Generalized Suzuki 2-groups // 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME). Mauritius, 2021, pp. 1–6. doi: 10.1109/ICECCME52200.2021.9590932.

19.Khalimov G., Kotukh Y., Khalimova S. MST_3 Cryptosystem Based on a Generalized Suzuki 2-Groups [Electronic resource]. Access mode : http://ceur-ws.org/Vol-2711/paper1.pdf

20.Khalimov G., Kotukh Y., Didmanidze I., Sievierinov O., Khalimova S. and Vlasov A. Towards three-parameter group encryption scheme for MST3 cryptosystem improvement // 2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4), London, United Kingdom, 2021, pp. 204–211. doi: 10.1109/WorldS451998.2021.9514009.

21.Khalimov G., Kotukh Y., Didmanidze I., Khalimova S. 2021. Encryption scheme based on small Ree groups // Proceedings of the 2021 7th International Conference on Computer Technology Appli-cations (ICCTA '21). ACM, New York, NY, USA, 33–37. https://doi.org/10.1145/3477911.3477917

22.Khalimov G., Kotukh Y., Shonia O., Didmanidze I., Sievierinov O., Khalimova S. Encryption Scheme Based on the Automorphism Group of the Suzuki Function Field // 2020 IEEE PIC S&T, Kharkiv, Ukraine, 2020, pp. 383–387. doi: 10.1109/PICST51311.2020.9468089.

23.Khalimov G., Kotukh Y., Khalimova S. Encryption scheme based on the extension of automorphism group of the Hermitian function field // Book of Abstract 20th Central European Conference on Cryptology. 2020. P. 30 – 32.

24.Khalimov G., Kotukh Y. et al. (2022). Encryption Scheme Based on the Generalized Suzuki 2-groups and Homomorphic Encryption // Chang SY., Bathen L., Di Troia F., Austin T.H., Nelson A.J. (eds). Silicon Valley Cybersecurity Conference. SVCC 2021. Communications in Computer and Information Science, vol 1536. Springer, Cham. https://doi.org/10.1007/978-3-030-96057-5_5

25.Khalimov G., Sievierinov O., Khalimova S., Kotukh Y., Chang S.-Y. and Balytskyi Y. Encryption Based on the Group of the Hermitian Function Field and Homomorphic Encryption // 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T). Kharkiv, Ukraine, 2021, pp. 465–469. doi: 10.1109/PICST54195.2021.9772219.

26.Kotukh Y., Khalimov G., Korobchinsky M. Construction of a three-parameter encryption scheme on Hermitian groups in the MST3 cryptosystem // Radiotekhnika. 2023. 213. P. 49–55. https://doi.org/10.30837/rt.2023.2.213.05

27.Kotukh Y., Khalimov G., Korobcninskiy M. Method of Security Improvement for MST2 Cryptosystem Based on Automorphism Group of Ree Function Field// 2023 Theoretical and applied cybersecurity, vol.5, no. 2, pp. 31–39. https://doi.org/10.20535/tacs.2664-29132023.2.290414

28.Khalimov G., Kotukh Y., Khalimova S. Improved encryption scheme based on the automorphism group of the Ree function field field // 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), IEEE Xplore. 2021.

Надійшла до редколегії 20.08.2023

Відомості про авторів:

Котух Євген Володимирович – канд. техн. наук, доцент, професор кафедри кібербезпеки; Національний технічний університет «Дніпровська політехніка»; Дніпро, Україна; e-mail: yevgenkotukh@gmail.com; ORCID: https://orcid.org/0000-0003-4997-620X

Халімов Геннадій Зайдулович – д-р техн. наук, професор, завідувач кафедри безпеки інформаційних технологій; Харківський національний університет радіоелектроніки; Харків, Україна; e-mail: hennadii.khalimov@nure.ua; ORCID: https://orcid.org/0000-0002-2054-9186

Коробчинський Максим Володимирович, д-р техн. наук, професор, начальник 2-ї кафедри технічних видів розвідки та інформаційних технологій 2-го навчального інституту Воєнної академії імені Євгенія Березняка Міністерства оборони України, м. Київ, Україна; mars_kor@ukr.net; ORCID:https://orcid.org/0000-0001-8049-4730,