УДК 621.391:519.2 **DOI:10.30837/rt.2023.4.215.05**

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 УЗАГАЛЬНЕНОЇ 2-ГРУПИ СУЗУКІ ТА ГОМОМОРФНОГО ШИФРУВАННЯ

Вступ

Останні розвідки в сфері квантових обчислень суттєво впливають на розробку безпечних криптосистем з відкритим ключем. Одним з основних напрямів у цій області є рішення задачі знаходження спряженого елемента в теорії некомутативних груп і розв'язання проблем введення в групах та напівгрупах.

Проблема складності слова, запропонована Вагнером і Маджаріком [1], була реалізована у декількох криптосистемах. Однією з найбільш вивчених є система, що базується на факторизації в кінцевих групах перестановок і відома як логарифмічна сигнатура [2 – 5].

Magliveras та співавтори [6] у 2008 р. провели всебічний аналіз криптосистеми MST3, визначивши обмеження для логарифмічного підпису і заявивши, що транзитивний логарифмічний підпис не підходить для MST3. У 2009 р. Lempken та інші описали криптосистему з відкритим ключем MST3, засновану на логарифмічному підписі та 2-групі Сузукі [7]. Криптосистеми на неабелевих групах та їх властивості активно вивчались в [8, 9].

У 2010 р. Сваба та інші [10] проаналізували всі відомі атаки на криптографію MST і створили більш безпечну криптосистему eMST3, включивши секретне гомоморфне накриття. Т. ван Трунг у 2018 р. [11] запропонував загальний метод побудови сильних аперіодичних логарифмічних сигнатур для абелевих *p*-груп, що є важливим внеском у розвиток і практичне застосування криптосистем MST.

Криптоаналіз схем шифрування на основі проблеми слова з використанням логаріфмічних підписів відкрив подальші можливості для вдосконалення [12 – 16]. Як приклад, для криптосистем MST було виявлено їх вразливість до атак на основі виділеного тексту. Це пов'язано з конструктивною особливістю відомих реалізацій MST, яка полягає у наявності відомих текстів і, відповідно, можливості криптоаналізу.

У відповідь на ці виклики було запропоновано безпечну схему шифрування на основі загальної 2-групи Сузукі, яка включає гомоморфне шифрування. Гомоморфне шифрування дозволяє виконувати певні обчислення над зашифрованими даними без необхідності їх розшифровувати, тим самим забезпечуючи додатковий рівень безпеки. Впровадження такої технології у криптосистему MST може значно підвищити її стійкість до різноманітних атак, зокрема атак з виділеним текстом.

Розробка криптосистем MST на основі багатопараметричних некомутативних груп, як зазначено в [17 – 28], відкриває нові можливості для оптимізації параметрів і підвищення секретності криптосистем. Ці системи дозволяють більш гнучко управляти параметрами, необхідними для забезпечення безпеки, що підвищує ефективність і надійність. Узагальнені 2-групи Сузукі, які є багатоваріантними і мають високий груповий порядок порівняно з іншими багатоваріантними групами, є особливо перспективними в цьому контексті. Однак перша реалізація криптосистеми на основі узагальненої 2-групи Suzuki не забезпечувала захист від атак методом грубого перебору з послідовним відновленням ключа. Значний науковий та практичний інтерес має розробка саме підходу на узагальнених Сузукі 2-групах та вдосконалення її криптографічних властивостей.

Узагальнені Сузукі 2-групи

Узагальнення 2-груп Сузукі визначено над скінченним полем F_q, $q = 2^n$, $n > 0$ для натурального числа l та $a_1, a_2, ..., a_l \in F$ для деякого автоморфізму θ як F [10]:

$$A_l(n, \theta) = \left\{ S(a_1, a_2, ..., a_l) \mid a_i \in F_q \right\}$$

Кожен елемент $A_l(n,\theta)$ можна виразити однозначно, і з цього випливає, що $|A_l(n,\theta)| = 2^{nl}$ і $A_l(n,\theta)$ визначають групу порядку 2^{nl}. Якщо $l = 2$, ця група ізоморфна 2-групі Сузукі $A(n,\theta)$.

Групова операція визначається як продукт:

$$S(a_1,a_2,...,a_l)S(b_1,b_2,...,b_l) = S(a_1+b_1, a_2+(a_1\theta)b_1+b_2, a_3+(a_2\theta)b_1+(a_1\theta^2)b_2+b_3,$$
$$..., a_l+(a_{l-1}\theta)b_1+...+(a_1\theta^{l-1})b_{l-1}+b_l).$$

з елементом тотожності $S(0_1,0,...,0)$.

Обернений елемент визначається як

$$S(a_1,a_2,a_3,...,a_l)^{-1} = S(a_1, a_2+a_1\theta a_1, a_3+a_2\theta a_1+a_1\theta^2(a_2+a_1\theta a_1),..., a_l+a_{l-1}\theta a_1+...).$$

Група є неабелевою і має нетривіальний центр

$$Z(G) = \left\{S(0,0,...,c)\middle| c \in F_q\right\}.$$

Припустимо, що θ – це автоморфізм $F, \theta : x \to x^2$ Фробеніуса. Для фіксованого кінцевого поля $A_l(n,\theta)$ порядок групи більший, ніж у класичній Сузукі 2-групи.

У новій реалізації криптосистеми ми змінили алгоритм шифрування та пропонуємо використовувати гомоморфне шифрування для випадкових накриттів. У цьому випадку складність атаки відновлення ключа буде визначатися шляхом вичерпного пошуку по всій групі.

Метод, що пропонується

Наша пропозиція полягає у створенні логарифмічної сигнатури для всієї узагальненої 2-групи Сузукі та гомоморфного шифрування випадкових накриттів у логарифмічній сигнатурі.

Давайте розглянемо основні етапи шифрування – генерація ключів, шифрування та дешифрування. Для початку етапу генерації ключів фіксуємо велику групу $A_l(n,\theta) = \left\{S(a_1,a_2,...,a_l) \mid a_i \in F_q\right\}$, $q = 2^n$.

Побудуємо ручні логарифмічні підписи $\beta_k = \left[B_{1(k)},...,B_{s(k)}\right] = \left(b_{ij}\right)_k = S\left(0,..,0,b_{ij(k)},0,...,0\right)$ типу

$$\left(r_{1(k)},...,r_{s(k)}\right),\ i = \overline{0,s(\mathrm{k})},\ j = \overline{1,r_{i(k)}},\ b_{ij(k)} \in F_q,\ k = \overline{1,l}.$$

Встановимо випадкову обкладинку:

$$\alpha_k = \left[A_{1(k)},...,A_{s(k)}\right] = \left(a_{ij}\right)_k = S\left(a^{(1)}_{ij(k)\cdot}, a^{(2)}_{ij(k)\cdot},...,a^{(l)}_{ij(k)}\right)$$

того самого типу β_k, де $a_{ij} \in A_l(n,\theta)$, $a^{(v)}_{ij(k)} \in F_q \setminus \{0\}$, $i = \overline{1,s}$, $j = \overline{1,r_{i(k)}}$, $k = \overline{1,l}$.

Виберемо випадкові обкладинки:

$$w_{(k)} = \left[W_{1(k)},...,W_{s(k)}\right] = \left(w_{ij}\right)_{(k)} = S\left(w^{(1)}_{ij(k)\cdot}, w^{(2)}_{ij(k)\cdot},..., w^{(l)}_{ij(k)}\right)$$

тих самих типів $\beta_{(k)}$, де $w_{ij} \in A_l(n,\theta)$, $w_{ij(k)} \in F_q \setminus \{0\}$, $i = \overline{0,s(\mathrm{k})}$, $j = \overline{1,r_{i(k)}}$, $k = \overline{1,l}$.

Згенеруємо випадкові $t_{0(k)},...,t_{s(k)} \in A_l(n,\theta) \setminus Z$, $t_{i(k)} = S(t_{i1(k)},...,t_{il(\mathrm{k})})$, $t_{ij(\mathrm{k})} \in F^{\times}$, $i = \overline{0,s(\mathrm{k})}$, $k = \overline{1,l}$.

Виберемо

$$\tau_{0(k)},...,\tau_{s(k)} \in A_l(n,\theta) \setminus Z,\ \tau_{i(k)} = S(\tau_{i1(k)},...,\tau_{il(\mathrm{k})}),\ \tau_{ij(\mathrm{k})} \in F^{\times},\ i = \overline{0,s(\mathrm{k})},\ k = \overline{1,l}.$$

Візьмемо $t_{s(k-1)} = t_{0(k)}$, $\tau_{s(k-1)} = \tau_{0(k)}$, $k = \overline{1,l}$.

Визначимо додаткову групову операцію:

$$S(a_1,a_2,...,a_l) \circ^{(k)} S(b_1,b_2,...,b_l) =$$
$$S(a_1+b_1, a_2+b_2,..., a_k+b_k, a_{k+1}+{a_k}^2 b_1+...+{a_1}^{2^k} b_k + b_{k+1},..., a_l+{a_{l-1}}^2 b_1+...+{a_1}^{2^{l-1}} b_{l-1}+b_l).$$

Зворотним елементом $S^{-(k)}$ для групової операції $\circ^{(k)}$ є

$$S^{-(k)}(a_1,a_2,...,a_l) = S(a_1,a_2,...,a_k,\alpha_{k+1},...,\alpha_l)$$

де

$$\alpha_{k+1} = a_{k+1} + a_k{}^2 a_1 + ... + a_2{}^{2^{k-1}} a_{k-1} + a_1{}^{2^k} a_k,$$
$$\alpha_{k+2} = a_{k+2} + a_{k+1}{}^2 a_1 + ... + a_3{}^{2^{k-1}} a_{k-1} + a_2{}^{2^k} a_k + a_1{}^{2^{k+1}} \alpha_{k+1},$$
$$...$$
$$\alpha_l = a_l + a_{l-1}{}^2 a_1 + ... + a_{l-k}^{2^k} a_k + a_{l-k-1}{}^{2^{k+1}} \alpha_{k+1} +, ..., + a_l{}^{2^{l-1}} \alpha_{l-1}$$

Застосування додаткової групової операції $\circ^{(k)}$ призводить до гомоморфного представлення елементів групи $S(a_1, a_2, ..., a_l) \overset{\circ^{(k)}}{\to} S(a_1, a_2, ..., a_k, \alpha_{k+1}, ..., \alpha_l) = S^{(k)}$.

Застосуємо обернене гомоморфне перетворення для обернених і прямих елементів $S_1^{-(k)}$ групи $S_2^{(k)}$ для обчислення в групі з лівим оберненим елементом $S_1^{-(n)\circ}$: $S_3 = S_1^{-(k)\circ} \cdot S_2^{(k)\circ}$; для $S_1^{-(k)}$ маємо:

$$S^{-(k)\circ} = S^{\circ}(a_1, a_2, ..., a_k, \alpha_{k+1}, ..., \alpha_l) = S(\alpha_1, ..., \alpha_k, \alpha_{k+1}, ..., \alpha_l),$$

де $\alpha_1 = a_1, \alpha_2 = a_2 + a_1{}^2 a_1, ... \alpha_k = a_k + a_{k-1}{}^2 a_1 + ..., a_l{}^{2^{k-1}} a_{k-1}$. і $S_2^{(k)}$ відповідно до $S_3 = S_1^{-(k)\circ} \cdot S_2^{(k)\circ}$; отримуємо

$$S^{(k)\circ} = S^{\circ}(b_1, b_2, ..., b_k, \beta_{k+1}, ..., \beta_l) = S(\beta_1, ..., \beta_k, \beta_{k+1}, ..., \beta_l)$$
$$\beta_1 = b_1, \beta_2 = b_2 + a_1{}^2 (b_1 + a_1), ...$$
$$\beta_k = b_k + a_{k-1}{}^2 (b_1 + a_1) + ..., a_l{}^{2^{k-1}} (b_{k-1} + a_{k-1}).$$

Гомоморфні перетворення для $S^{-(k)\circ}$, $S^{(k)\circ}$ необхідні для того, щоб не порушувати групову операцію при обчисленні елементів групи $A_l(n, \theta)$.

Нехай $f(e)$ – гомоморфне криптографічне перетворення відносно додавання $f(a+b) = f(a) + f(b)$ і $e, a, b \in F_q$ – відповідне обернене перетворення $\hat{f}(e) = e$. Обчислюємо накриття логарифмічних сигнатур:

$$h_{(k)} = \left[h_{1(k)}, ..., h_{s(k)} \right] = t_{(i-1)(k)}^{-(k)} \circ^{(k)} \left(w_{ij} \right)_{(k)} \circ^{(k)} \left(b_{ij} \right)_{(k)} \circ^{(k)} t_{i(k)}$$

та накриття гомоморфного криптографічного перетворення:

$$g_{(k)} = \left[g_{1(k)}, ..., g_{s(k)} \right] = \tau_{(i-1)(k)}^{-(k)} \circ^{(k)} f\left(w_{ij} \right)_{(k)} \circ^{(k)} \tau_{i(k)},$$

де

$$f(w_{(k)}) = f\left(w_{ij} \right)_{(k)} = S\left(f(w_{ij(k)_1}), f(w_{ij(k)_2}), ..., f(w_{ij(k)_l}) \right), \quad i = \overline{1, s(k)}, \quad j = \overline{1, r_{i(k)}}, \quad k = \overline{1, l}.$$

Вихідним відкритим ключем є (a_k, h_k, g_k), а закритим ключем $\left[f, \beta_{(k)}, \left(t_{0(k)}, ..., t_{s(k)} \right), \left(\tau_{0(k)}, ..., \tau_{s(k)} \right) \right]$, $k = \overline{1, l}$ відповідно.

На етапі шифрування виконуємо наступне. Нехай повідомлення буде $x = S\left(x_1, ..., x_l \right)$ і відкритим ключем (a_k, h_k, g_k), $k = \overline{1, l}$ відповідно. Вибираємо випадковий $R = (R_1, ..., R_l)$, $R_1, ..., R_l \in \square_{|F_q|}$.

Обчисліть зашифрований текст y_1, y_2, y_3 як

$$y_1 = \alpha(R) \cdot x = \alpha_1(R_1) \cdot \alpha_2(R_2) \cdots \alpha_l(R_l) \cdot x$$
$$= S\left(\sum_{k=1}^{l} \sum_{i=1, j=R_{i(k)}}^{s(k)} a_{ij(k)}^{(1)} + x_1, \sum_{k=1}^{l} \sum_{i=1, j=R_{i(k)}}^{s(k)} a_{ij(k)}^{(2)} + x_2 + *, ..., \sum_{k=1}^{l} \sum_{i=1, j=R_{i(k)}}^{s(k)} a_{ij(k)}^{(l)} + x_l + *, \right),$$

$$y_2 = h(R) = h_1(R_1) \circ^{(1)} \left(h_2(R_2) \circ^{(2)} \cdots \left(h_{l-1}(R_{l-1}) \circ^{(l-2)} \left(h_{l-1}(R_{l-1}) \circ^{(l-1)} h_l(R_l) \right) \right) \right) =$$

$$S\left(\sum_{k=1}^{l} \sum_{i=1, j=R_{i(k)}}^{s(k)} w_{ij(k)}^{(1)} + \sum_{i=1, j=R_{i(1)}}^{s(1)} \beta_{ij(1)}, \sum_{k=1}^{l} \sum_{i=1, j=R_{i(k)}}^{s(k)} w_{ij(k)}^{(2)} + \right.$$

$$\left. \sum_{i=1, j=R_{i(2)}}^{s(2)} \beta_{ij(2)} + *, ..., \sum_{k=1}^{l} \sum_{i=1, j=R_{i(k)}}^{s(k)} w_{ij(k)}^{(l)} + \sum_{i=1, j=R_{i(l)}}^{s(l)} \beta_{ij(l)} + * \right)$$

Тут $(*)$ компоненти визначаються перехресними обчисленнями в груповій операції добутку $t_{0(k)},...,t_{s(k)}$ та добутку $w_{(k)}(R_k)+\beta_{(k)}(R_k)$:

$$y_3 = g(R) = g_1(R_1) \circ^{(1)} \left(g_2(R_2) \circ^{(2)} \cdots \left(g_{l-1}(R_{l-1}) \circ^{(l-2)} \left(g_{l-1}(R_{l-1}) \circ^{(l-1)} g_l(R_l)\right)\right)\right) =$$

$$S\left(\sum_{k=1}^{l} \sum_{i=1,\, j=R_{i(k)}}^{s(k)} f\left(w_{ij(k)}^{(1)}\right) +, \sum_{k=1}^{l} \sum_{i=1,\, j=R_{i(k)}}^{s(k)} f\left(w_{ij(k)}^{(2)}\right) + *, ...,\right.$$

$$\left.\sum_{k=1}^{l} \sum_{i=1,\, j=R_{i(k)}}^{s(k)} f\left(w_{ij(k)}^{(l)}\right) + *\right)$$

Тут $(*)$ компоненти визначаються перехресними обчисленнями в груповій операції добутку $\tau_{0(k)},...,\tau_{s(k)}$ та добутку $f\left(w_{(k)}(R_k)\right)$.

В и х і д : зашифрований текст (y_1, y_2, y_3) повідомлення x.

Для дешифрування візьмемо зашифрований текст (y_1, y_2, y_3) і особистий ключ $\left[f, \beta_{(k)}, t_{i(k)}, \tau_{i(k)}\right]$, $i = \overline{0, s(k)}$, $k = \overline{1, l}$.

Щоб розшифрувати повідомлення x, потрібно відновити випадкові числа $R = (R_1, R_2, ..., R_l)$.

Обчислимо

$$D^{(1)}(R) = D^{(1)}(R_1, R_2, ..., R_l) = t_{0(1)} \circ^{(1)} y_2 \circ^{(l)} t_{s(l)}^{-(l)} = S\Big(\sum_{i=1,\, j=R_{i(1)}}^{s(1)} w_{ij(1)}^{(1)} + \beta_1(R_1), *, ..., *\Big),$$

$$G^{(1)}(R) = G^{(1)}(R_1, R_2, ..., R_l) = \tau_{0(1)} \circ^{(1)} y_3 \circ^{(l)} \tau_{s(l)}^{-(l)} = S\Big(\sum_{i=1,\, j=R_{i(1)}}^{s(1)} f\left(w_{ij(1)}^{(1)}\right), *, ..., *\Big),$$

$$D^{(1)}(R)' = D^{(1)}(R) \circ^{(1)} \hat{f}(G^{(1)}(R))^{-(1)} = S\Big(\sum_{i=1,\, j=R_{i(1)}}^{s(1)} \beta_{ij(1)}, *, *\Big)$$

Відновлюємо R_1 з $\beta_{(1)}(R_1) = \sum_{i=1,\, j=R_{i(1)}}^{s(1)} \beta_{ij(1)}$, використовуючи $\beta_{(1)}(R_1)^{-1}$, оскільки β_1 є простим.

Для подальшого розрахунку необхідно видалити компонент $h_1(R_1)$ від y_2 і $g_1(R_1)$ від y_3. Обчислимо

$$y_2^{(1)} = h_1(R_1)^{-(1)\circ} \cdot y_2^{\circ}, \; y_3^{(1)} = g_1(R_1)^{-(1)\circ} \cdot y_3^{\circ}, \; D(R)^{(2)} = t_{0(2)} \circ^{(2)} y_2^{(1)} \circ^{(l)} t_{s(l)}^{-(l)},$$

$$G(R)^{(2)} = \tau_{0(2)} \circ^{(2)} y_3^{(1)} \circ^{(l)} \tau_{s(l)}^{-(l)},$$

$$D^{(2)}(R)' = D^{(2)}(R) \circ^{(2)} \hat{f}(G^{(2)}(R))^{-(2)} = S(0, \sum_{i=1,\, j=R_{i(2)}}^{s(2)} \beta_{ij(2)_c}, *)$$

і відновлюємо R_2 з $\beta_{(2)}(R_2) = \sum_{i=1,\, j=R_{i(2)}}^{s(2)} \beta_{ij(2)}$, використовуючи $\beta_{(2)}(R_2)^{-1}$, оскільки β_2 є простим. Продовжуємо обчислення ітераційно до останнього значення R_l. Маємо такі рекурентні співвідношення для $n = \overline{1, l-1}$:

$$y_2^{(n)} = h_n(R_n)^{-(n)\circ} \cdot y_2^{(n-1)\circ}, \; y_3^{(n)} = g_n(R_n)^{-(n)\circ} \cdot y_3^{(n-1)\circ},$$

$$D^{(n+1)}(R) = t_{0(n+1)} \circ^{(n+1)} y_2^{(n)} \circ^{(l)} t_{s(l)}^{-(l)}, \; G^{(n+1)}(R) = \tau_{0(n+1)} \circ^{(n+1)} y_3^{(n)} \circ^{(l)} \tau_{s(l)}^{-(l)},$$

$$D^{(n+1)}(R)' = D^{(n+1)}(R) \circ^{(n+1)} \hat{f}(G^{(n+1)}(R))^{-(n+1)} = S(0, 0, ..., 0, \sum_{i=1,\, j=R_{i(n+1)}}^{s(n+1)} \beta_{ij(n+1)}, *)$$

Відновлюємо _ R_{n+1} з $\beta_{(n+1)}(R_{n+1}) = \sum_{i=1,\, j=R_{i(n+1)}}^{s(n+1)} \beta_{ij(n+1)}$, використовуючи $\beta_{(n+1)}(R_{n+1})^{-1}$.

Відновлюємо повідомлення $x = a(R_1, R_2, ..., R_l)^{-1} \cdot y_1$.

Практичні обчислення

Правильність отриманих виразів покажемо на простому прикладі.

Зафіксуємо чотирипараметричну узагальнену групу Сузукі $G = A_4(n,\theta)$ над скінченним полем F_q, $q = 2^5$, $g(\mathrm{x}) = x^5 + x^3 + 1$. Припустимо, що θ – це автоморфізм $F_q, \theta : \alpha \to \alpha^2$ Фробеніуса. Групова операція визначається як

$$S(a_1,a_2,a_3,a_4)S(b_1,b_2,b_3,b_4) = S(a_1+b_1, a_2+a_1^{\,2}b_1+b_2,$$
$$a_3+a_2^{\,2}b_1+a_1^{\,4}b_2+b_3, a_4+a_3^{\,2}b_1+a_2^{\,4}b_2+a_1^{\,8}b_3+b_4).$$

Обернений елемент визначається як

$$S(a_1,a_2,a_3,a_4)^{-1} = S(a_1, a_2+a_1^{\,3}, a_3+a_2^{\,2}a_1+a_1^{\,4}a'_2, a_4+a_3^{\,2}a_1+a_2^{\,4}a'_2+a_1^{\,8}a'_3),$$

де $a'_2 = a_2 + a_1^{\,3}$, $a'_3 = a_3 + a_2^{\,2}a_1 + a_1^{\,4}a'_2$.

Розглянемо основні етапи розрахунків. Перший етап – це генерація ключів.

Перший етап полягає в генерації ручної логарифмічної сигнатури з розмірністю відповідного вибраного типу $\left(r_{1(k)},...,r_{s(k)}\right)$ та кінцевим полем F_q. Побудова масивів логарифмічних сигнатур представлена в [11]. Для нашого прикладу використовуємо побудову простих логарифмічних підписів, не аналізуючи деталі їх секретності. Для $\beta_{(k)}$ матимемо $k = \overline{1,3}$ типи $\left(2^2,2^3\right)$, $\left(2,2^2,2^2\right)$, $\left(2^2,2,2^2\right)$, $\left(2^2,2^2,2\right)$. Вони представлені у вигляді рядків і елементів групи над полем F_q у табл. 1

Таблиця 1

Генерація логарифмічного підпису

$\beta_k = \left[B_{1(k)}, B_{2(k)}, B_{3(k)}, B_{4(k)}\right] = \left(b_{ij}\right)_{(k)}, \left(b_{ij}\right)_{(k)} \in A_{l=4}(n,\theta)$							
Б **1(1)**		***B*** **1(2)**		***B*** **1(3)**		***B*** **1(4)**	
00000	0,0,0,0	00000	0,0,0,0	00000	0,0,0,0	00000	0,0,0,0
10000	α^0,0,0,0	10000	0,α^0,0,0	10000	0,0,α^0,0	10000	0,0,0,α^0
01000	α^1,0,0,0	01000	0,α^1,0,0	***B*** **2(3)**		01000	0,0,0,α^1
11000	α^{14},0,0,0	11000	0,α^{14},0,0	00000	0,0,0,0	11000	0,0,0,α^{14}
B **2(1)**		***B*** **2(2)**		11000	0,0,α^{14},0	***B*** **2(4)**	
01000	α^1,0,0,0	11000	0,α^{14},0,0	10100	0,0,α^{28},0	00000	0,0,0,0
10100	α^{28},0,0,0	11100	0,α^{22},0,0	01100	0,0,α^{15},0	00100	0,0,0,α^2
11010	α^{26},0,0,0	10010	0,α^5,0,0	***Б*** **3 (3)**		***Б*** **3 (4)**	
00110	α^{16},0,0,0	00110	0,α^{16},0,0	01000	0,0,α^1,0	01000	0,0,0,α^1
10001	α^{25},0,0,0	***B*** **3(2)**		10010	0,0,α^5,0	00110	0,0,0,α^{16}
11101	α^{21},0,0,0	10000	0,α^0,0,0	01101	0,0,α^{27},0	00001	0,0,0,α^4
10011	α^{18},0,0,0	10011	0,α^{18},0,0	10111	0,0,α^9,0	11011	0,0,0,α^{19}
11111	α^{20},0,0,0						

Побудуємо випадкові накриття α_k для того самого типу, що й $\beta_{(k)}$:

$$\alpha_k = \left[A_{1(k)},...,A_{s(k)}\right] = \left(a_{ij}\right)_k = S\left(a_{ij(k).}^{(1)}, a_{ij(k)}^{(2)}, a_{ij(k)}^{(3)}, a_{ij(k)}^{(4)}\right),$$

де $a_{ij} \in A_{l=4}(n,\theta)$, $a_{ij(k)}^{(v)} \in F_q \setminus \{0\}$, $i = \overline{1,s}$, $j = \overline{1,r_{i(k)}}$, $k = \overline{1,4}$.

У полі подання α_k має наступний вигляд (табл. 2).

Таблиця 2

Побудова випадкового накриття

$\alpha_k = \left[A_{1(k)},...,A_{s(k)}\right] = \left(a_{ij}\right)_k = S\left(a_{ij(k).}^{(1)}, a_{ij(k)}^{(2)}, a_{ij(k)}^{(3)}, a_{ij(k)}^{(4)}\right)$			
$k = 1$	$k = 2$	$k = 3$	$k = 4$
A **1(1)**	***A*** **1(2)**	***A*** **1(3)**	***A*** **1(4)**
α^6, α^{11}, α^{17}, α^{27}	α^{17}, α^5, α^{26}, α^{28}	α^0, α^2, α^{14}, α^{20}	α^{20}, α^{14}, α^{30}, α^{13}
α^{11}, α^5, α^7, α^5	α^{20}, α^{14}, α^{19}, α^{24}	α^{17}, α^{27}, α^{16}, α^{10}	α^4, α^2, α^{13}, α^{17}
α^{21},α^{18},0,α^{16}	α^{30}, α^{21}, α^6, α^3	***A*** **2(3)**	α^{19}, α^{13}, α^{26}, α^{22}
α^5, α^{29}, α^{12}, α^{16}	α^6, α^9, α^{13}, α^{22}	α^{28},α^{29},0,α^{25}	α^6, α^{28}, α^{12}, α^4
A **2(1)**	***A*** **2(2)**	α^{10}, α^{12}, α^{22}, α^{30}	***A*** **2(4)**

$\alpha^4, \alpha^7, \alpha^4, \alpha^2$	$\alpha^{30}, \alpha^{14}, \alpha^{27}, \alpha^{30}$	$\alpha^{13}, \alpha^{23}, \alpha^{19}, \alpha^{19}$	$\alpha^{18},\alpha^1,\alpha^1,\alpha^{24}$
$\alpha^{12},\alpha^{11},\alpha^3,\alpha^1$	$\alpha^1,\alpha^{18},0,\alpha^{13}$	$\alpha^0, \alpha^{10}, \alpha^1, \alpha^{20}$	$\alpha^{26},\alpha^{28},\alpha^{15},\alpha^0$
$\alpha^{18}, \alpha^{15}, \alpha^{14}, \alpha^{30}$	$\alpha^1, \alpha^{18}, \alpha^{28}, \alpha^{30}$	$\boldsymbol{A}_{3(3)}$	$\boldsymbol{A}_{3(4)}$
$\alpha^3, \alpha^{19}, \alpha^{26}, \alpha^2$	$\alpha^{25},\alpha^5,\alpha^0,\alpha^{13}$	$\alpha^{11}, \alpha^{27}, \alpha^{29}, \alpha^{18}$	$\alpha^{16}, \alpha^{17}, \alpha^{29}, \alpha^{17}$
$\alpha^{11}, \alpha^{18}, \alpha^{21}, \alpha^{28}$	$\boldsymbol{A}_{3(2)}$	$\alpha^5, \alpha^1, \alpha^{12}, \alpha^{22}$	$\alpha^{18},\alpha^0,\alpha^1,\alpha^{15}$
$\alpha^{16}, \alpha^{18}, \alpha^{10,} \alpha^{24}$	$\alpha^3,\alpha^{29},\alpha^{25},0$	$\alpha^{30}, \alpha^{18}, \alpha^6, \alpha^{11}$	$\alpha^4, \alpha^9, \alpha^{23}, \alpha^{19}$
$\alpha^{17},\alpha^{16},0,\alpha^{27}$	$\alpha^{25}, \alpha^{19}, \alpha^{23}, \alpha^2$	$0,0,\alpha^{17},\alpha^{23}$	$\alpha^{19}, \alpha^{20}, \alpha^{30}, \alpha^{10}$
$\alpha^{25}, \alpha^{17}, \alpha^8, \alpha^{12}$			

Вибираємо випадково $A_i(n,\theta)$ $t_{0(k)}, t_{1(k)}, ..., t_{s(k)} \in A_i(n,\theta)$, $s_{(k)}$, $k = \overline{1,4}$ і $t_{2(1)} = t_{0(2)}$, $t_{3(2)} = t_{0(3)}$, $t_{3(3)} = t_{0(4)}$ (табл. 3).

Таблиця 3

Випадкові t вектори

$t_{0(k)}, t_{1(k)}, ..., t_{s(k)} \in A_{i=4}(n,\theta)$, $s_{(k)}, k = \overline{1,4}$			
$k = 1$	$k = 2$	$k = 3$	$k = 4$
$\alpha^1, \alpha^5, \alpha^{17}, \alpha^{16}$ $\alpha^{25}, \alpha^{17}, \alpha^{23}, \alpha^{27}$ $\alpha^{13}, \alpha^0, \alpha^{28}, \alpha^{10}$	$\alpha^{13}, \alpha^0, \alpha^{28}, \alpha^{10}$ $\alpha^{30},\alpha^2,\alpha^{17},\alpha^2$ $\alpha^6, \alpha^7, \alpha^{30}, \alpha^{18}$ $\alpha^9,\alpha^4,\alpha^9,\alpha^{20}$	$\alpha^9,\alpha^4,\alpha^9,\alpha^{20}$ $\alpha^{14}, \alpha^{28}, \alpha^{17}, \alpha^{22}$ $\alpha^{26}, \alpha^5, \alpha^{16}, \alpha^{30}$ $\alpha^{12}, \alpha^{15}, \alpha^{17}, \alpha^6$	$\alpha^{12}, \alpha^{15}, \alpha^{17}, \alpha^6$ $\alpha^{22}, \alpha^{30}, \alpha^{22}, \alpha^{16}$ $\alpha^{24}, \alpha^{29}, \alpha^{15}, \alpha^{30}$ $\alpha^3,0,\alpha^{14},\alpha^9$

Зворотні елементи $t_{0(k)}^{-(k)}, t_{1(k)}^{-(k)}, ..., t_{s(k)}^{-(k)}$ групи $A_4(n,\theta)$ обчислені, як показано в табл. 4.

Таблиця 4

Обчислення обернених елементів $t_{0(k)}^{-(k)}, t_{1(k)}^{-(k)}, ..., t_{s(k)}^{-(k)}$

$t_{0(k)}^{-(k)}, t_{1(k)}^{-(k)}, ..., t_{s(k)}^{-(k)}$			
$k = 1$	$k = 2$	$k = 3$	$k = 4$
$\alpha^1,\alpha^0,\alpha^{22},\alpha^{21}$ $\alpha^{25}, \alpha^7, \alpha^3, \alpha^{15}$ $\alpha^{13}, \alpha^{19}, \alpha^7, \alpha^{24}$	$\alpha^{13},\alpha^0,\alpha^7,\alpha^{24}$ $\alpha^{30}, \alpha^2, \alpha^{15}, \alpha^{21}$ $\alpha^6, \alpha^7, \alpha^{28}, \alpha^{24}$ $\alpha^9, \alpha^4, \alpha^8, \alpha^{25}$	$\alpha^9,\alpha^4,\alpha^9,\alpha^{25}$ $\alpha^{14}, \alpha^{28}, \alpha^{17}, \alpha^{21}$ $\alpha^{26}, \alpha^5, \alpha^{16}, \alpha^{13}$ $\alpha^{12}, \alpha^{15}, \alpha^{17}, \alpha^{30}$	$\alpha^{12}, \alpha^{15}, \alpha^{17}, \alpha^6$ $\alpha^{22}, \alpha^{30}, \alpha^{22}, \alpha^{16}$ $\alpha^{24}, \alpha^{29}, \alpha^{15}, \alpha^{30}$ $\alpha^3,0,\alpha^{14},\alpha^9$

Аналогічно вибираємо випадкові $\tau_{0(k)}, \tau_{1(k)}, ..., \tau_{s(k)} \in A_i(n,\theta)$, $s_{(k)}$, $k = \overline{1,4}$ і $t_{2(1)} = t_{0(2)}$, $t_{3(2)} = t_{0(3)}$, $t_{3(3)} = t_{0(4)}$ (табл. 5):

Таблиця 5

Обчислення випадкових τ векторів $\tau_{0(k)}, \tau_{1(k)}, ..., \tau_{s(k)} \in A(P_\infty) \setminus Z$

$\tau_{0(k)}, \tau_{1(k)}, ..., \tau_{s(k)} \in A(P_\infty) \setminus Z$, $s_{(k)}, k = \overline{1,4}$			
$k = 1$	$k = 2$	$k = 3$	$k = 4$
$\alpha^4, \alpha^{22}, \alpha^7, \alpha^{12}$ $\alpha^8,0,\alpha^{13},\alpha^{16}$ $\alpha^{29}, \alpha^{21}, \alpha^{30}, \alpha^{13}$	$\alpha^{29}, \alpha^{21}, \alpha^{30}, \alpha^{13}$ $\alpha^{24}, \alpha^{20}, \alpha^{17}, \alpha^{25}$ $\alpha^4, \alpha^7, \alpha^{16}, \alpha^{30}$ $\alpha^2,\alpha^{17},\alpha^{22},\alpha^2$	$\alpha^2,\alpha^{17},\alpha^{22},\alpha^2$ $0,\alpha^{22},\alpha^{16},\alpha^{24}$ $\alpha^6, \alpha^{21}, \alpha^{25}, \alpha^{18}$ $\alpha^{20},0,\alpha^3,\alpha^0$	$\alpha^{20},0,\alpha^3,\alpha^0$ $\alpha^{21}, \alpha^{16}, \alpha^{12}, \alpha^{16}$ $\alpha^{16}, \alpha^{28}, \alpha^{19}, \alpha^{16}$ $\alpha^{28}, \alpha^{17}, \alpha^{26}, \alpha^4$

і обернені елементи $\tau_{0(k)}^{-(k)}, \tau_{1(k)}^{-(k)}, ..., \tau_{s(k)}^{-(k)}$ (табл. 6):

Таблиця 6

Обчислення обернених елементів $\tau_{0(k)}^{-(k)}, \tau_{1(k)}^{-(k)}, ..., \tau_{s(k)}^{-(k)}$

$\tau_{0(k)}^{-(k)}, \tau_{1(k)}^{-(k)}, ..., \tau_{s(k)}^{-(k)}$			
$k = 1$	$k = 2$	$k = 3$	$k = 4$
$\alpha^4, \alpha^{18}, \alpha^9, \alpha^0$ $\alpha^8, \alpha^{24}, \alpha^2, \alpha^{30}$ $\alpha^{29}, \alpha^{15}, \alpha^2, \alpha^5$	$\alpha^{29}, \alpha^{21}, \alpha^2, \alpha^5$ $\alpha^{24}, \alpha^{20}, \alpha^{22}, \alpha^{29}$ $\alpha^4, \alpha^7, \alpha^{12}, \alpha^{28}$ $\alpha^2, \alpha^{17}, \alpha^{24}, \alpha^{11}$	$\alpha^2, \alpha^{17}, \alpha^{22}, \alpha^{11}$ $0,\alpha^{22},\alpha^{16},\alpha^2$ $\alpha^6, \alpha^{21}, \alpha^{25}, \alpha^3$ $\alpha^{20},0,\alpha^3,\alpha^{22}$	$\alpha^{20},0,\alpha^3,\alpha^0$ $\alpha^{21}, \alpha^{16}, \alpha^{12}, \alpha^{16}$ $\alpha^{16}, \alpha^{28}, \alpha^{19}, \alpha^{16}$ $\alpha^{28}, \alpha^{17}, \alpha^{26}, \alpha^4$

Побудуємо випадкові накриття w_k для того самого типу, що й $\beta_{(k)}$:

$w_{(k)} = \left[W_{1(k)},...,W_{s(k)}\right] = \left(w_{ij}\right)_{(k)} = S\left(w^{(1)}_{ij(k)\cdot}, w^{(2)}_{ij(k)\cdot},..., w^{(l)}_{ij(k)}\right)$, де $w_{ij} \in A_{t=4}(n,\theta)$, $w^{(v)}_{ij(k)} \in F_q$, $i = \overline{0, s(\mathrm{k})}$, $j = \overline{1, r_{i(k)}}$, $k = \overline{1,4}$ (табл. 7).

Таблиця 7

Випадкові накриття w_k

$w_{(k)} = \left[W_{1(k)},...,W_{s(k)}\right] = \left(w_{ij}\right)_{(k)} = S\left(w^{(1)}_{ij(k)\cdot},..., w^{(4)}_{ij(k)}\right)$			
$k=1$	$k=2$	$k=3$	$k=4$
$\boldsymbol{W}_{1(1)}$	$\boldsymbol{W}_{1(2)}$	$\boldsymbol{W}_{1(3)}$	$\boldsymbol{W}_{1(4)}$
$\alpha^{20},\alpha^{20},\alpha^{12},\alpha^{4}$	$\alpha^{9}, \alpha^{28}, \alpha^{27}, \alpha^{2}$	$\alpha^{3},\alpha^{2},\alpha^{10},0$	$\alpha^{30}, \alpha^{14}, \alpha^{1}, \alpha^{28}$
$\alpha^{7}, \alpha^{9}, \alpha^{17}, \alpha^{20}$	$\alpha^{16}, \alpha^{13}, \alpha^{6}, \alpha^{21}$	$\alpha^{5}, \alpha^{10}, \alpha^{19}, \alpha^{16}$	$\alpha^{6}, \alpha^{28}, \alpha^{30}, \alpha^{20}$
$\alpha^{25}, \alpha^{6}, \alpha^{23}, \alpha^{27}$	$\alpha^{25},0,\alpha^{4},\alpha^{27}$	$\boldsymbol{W}_{2(3)}$	$\alpha^{13}, \alpha^{19}, \alpha^{26}, \alpha^{11}$
$\alpha^{3}, \alpha^{0}, \alpha^{23}, \alpha^{29}$	$\alpha^{1},\alpha^{0},\alpha^{17},\alpha^{17}$	$\alpha^{12}, \alpha^{20}, \alpha^{14}, \alpha^{3}$	$\alpha^{16}, \alpha^{27}, \alpha^{9}, \alpha^{21}$
$\boldsymbol{W}_{2(1)}$	$\boldsymbol{W}_{2(2)}$	$\alpha^{23}, \alpha^{12}, \alpha^{5}, \alpha^{27}$	$\boldsymbol{W}_{2(4)}$
$\alpha^{7}, \alpha^{21}, \alpha^{6}, \alpha^{21}$	$\alpha^{21},\alpha^{14},\alpha^{14},\alpha^{0}$	$\alpha^{2}, \alpha^{3}, \alpha^{24}, \alpha^{16}$	$\alpha^{2}, \alpha^{21}, \alpha^{8}, \alpha^{29}$
$\alpha^{18}, \alpha^{21}, \alpha^{22}, \alpha^{6}$	$\alpha^{19}, \alpha^{29}, \alpha^{19}, \alpha^{13}$	$\alpha^{12}, \alpha^{5}, \alpha^{21}, \alpha^{14}$	$\alpha^{4}, \alpha^{2}, \alpha^{1}, \alpha^{23}$
$\alpha^{18}, \alpha^{19}, \alpha^{12}, \alpha^{15}$	$\alpha^{25}, \alpha^{26}, \alpha^{12}, \alpha^{17}$	$\boldsymbol{W}_{3(3)}$	$\boldsymbol{W}_{3(4)}$
$\alpha^{16}, \alpha^{12}, \alpha^{14}, \alpha^{6}$	$\alpha^{10}, \alpha^{19}, \alpha^{23}, \alpha^{4}$	$\alpha^{14},\alpha^{6},\alpha^{0},\alpha^{17}$	$0,\alpha^{0},\alpha^{25},\alpha^{3}$
$\alpha^{23}, \alpha^{4}, \alpha^{1}, \alpha^{30}$	$\boldsymbol{W}_{3(2)}$	$\alpha^{17}, \alpha^{13}, \alpha^{7}, \alpha^{4}$	$\alpha^{3}, \alpha^{19}, \alpha^{17}, \alpha^{24}$
$\alpha^{5}, \alpha^{26}, \alpha^{6}, \alpha^{19}$	$\alpha^{28},\alpha^{0},\alpha^{13},\alpha^{17}$	$\alpha^{25}, \alpha^{24}, \alpha^{27}, \alpha^{8}$	$\alpha^{28}, \alpha^{28}, \alpha^{14}, \alpha^{26}$
$\alpha^{22}, \alpha^{17}, \alpha^{13}, \alpha^{21}$	$\alpha^{14},\alpha^{0},\alpha^{3},\alpha^{3}$	$\alpha^{13},0,\alpha^{21},\alpha^{7}$	$\alpha^{24}, \alpha^{18}, \alpha^{27}, \alpha^{13}$
$\alpha^{28}, \alpha^{27}, \alpha^{9}, \alpha^{24}$			

Наступним кроком є обчислення масивів h_k (табл. 8). В рамках умови прикладу отримуємо: $h_{(\mathrm{k})} = \left[h_{1(\mathrm{k})},...,h_{s(\mathrm{k})}\right] = t^{-(k)}_{(i-1)(\mathrm{k})} \circ^{(k)} \left(w_{ij}\right)_{(\mathrm{k})} \circ^{(k)} \left(b_{ij}\right)_{(\mathrm{k})} \circ^{(k)} t_{i(\mathrm{k})}$; $i = \overline{1, s(\mathrm{k})}$, $j = \overline{1, r_{i(\mathrm{k})}}$, $k = \overline{1,4}$.

Виконаємо гомоморфне криптографічне перетворення для елемента поля $e \Rightarrow \rho_i e$, де ρ_i є секретним параметром. Перетворення вибрано найпростіше. Також можна використовувати більш складні гомоморфні перетворення щодо операції додавання. Визначимо гомоморфне криптографічне перетворення для елемента групи S як

$$f\left(S(e_1,e_2,e_3,e_4)\right) = S\left(\rho_1 e_1, \rho_2 e_2, \rho_3 e_3, \rho_4 e_4\right) \text{ і } \rho = \left(\rho_1,\rho_2,\rho_3,\rho_4\right) = \left(\alpha^4,\alpha^5,\alpha^6,\alpha^7\right).$$

Таблиця 8

Масиви h_k

$h_k = S(h^{(1)}_{ij(k)\cdot}, h^{(2)}_{ij(k)}, h^{(3)}_{ij(k)}, h^{(4)}_{ij(k)})$			
$k=1$	$k=2$	$k=3$	$k=4$
$\boldsymbol{h}_{1(1)}$	$\boldsymbol{h}_{1(2)}$	$\boldsymbol{h}_{1(3)}$	$\boldsymbol{h}_{1(4)}$
$\alpha^{16}, \alpha^{20}, \alpha^{22}, \alpha^{30}$	$\alpha^{24},0,\alpha^{16},0$	$\alpha^{27}, \alpha^{25}, \alpha^{27}, \alpha^{30}$	$\alpha^{7}, \alpha^{25}, \alpha^{9}, \alpha^{19}$
$\alpha^{20},\alpha^{7},\alpha^{21},\alpha^{15}$	$\alpha^{7}, \alpha^{25}, \alpha^{21}, \alpha^{3}$	$\alpha^{21}, \alpha^{15}, \alpha^{20}, \alpha^{14}$	$\alpha^{26},\alpha^{21},\alpha^{26},0$
$0,\alpha^{27},\alpha^{26},\alpha^{13}$	$\alpha^{4},\alpha^{22},0,\alpha^{21}$	$\boldsymbol{h}_{2(3)}$	$\alpha^{16}, \alpha^{5}, \alpha^{30}, \alpha^{10}$
$\alpha^{17}, \alpha^{16}, \alpha^{28}, \alpha^{26}$	$\alpha^{14}, \alpha^{22}, \alpha^{3}, \alpha^{5}$	$\alpha^{27}, \alpha^{10}, \alpha^{21}, \alpha^{23}$	$\alpha^{13},\alpha^{2},\alpha^{1},\alpha^{29}$
$\boldsymbol{h}_{2(1)}$	$\boldsymbol{h}_{2(2)}$	$\alpha^{15}, \alpha^{6}, \alpha^{12}, \alpha^{9}$	$\boldsymbol{h}_{2(4)}$
$\alpha^{26},0,\alpha^{29},\alpha^{11}$	$\alpha^{25}, \alpha^{5}, \alpha^{3}, \alpha^{26}$	$\alpha^{16},\alpha^{2},\alpha^{7},\alpha^{17}$	$\alpha^{20}, \alpha^{5}, \alpha^{19}, \alpha^{6}$
$\alpha^{17}, \alpha^{7}, \alpha^{26}, \alpha^{29}$	$\alpha^{9}, \alpha^{2}, \alpha^{12}, \alpha^{14}$	$\alpha^{27}, \alpha^{28}, \alpha^{28}, \alpha^{11}$	$\alpha^{26}, \alpha^{8}, \alpha^{14}, \alpha^{6}$
$\alpha^{27}, \alpha^{11}, \alpha^{28}, \alpha^{16}$	$\alpha^{21}, \alpha^{26}, \alpha^{25}, \alpha^{21}$	$\boldsymbol{h}_{3(3)}$	$\boldsymbol{h}_{3(4)}$
$\alpha^{2}, \alpha^{3}, \alpha^{11}, \alpha^{4}$	$\alpha^{13}, \alpha^{12}, \alpha^{22}, \alpha^{7}$	$\alpha^{27}, \alpha^{9}, \alpha^{21}, \alpha^{15}$	$\alpha^{30}, \alpha^{26}, \alpha^{30}, \alpha^{14}$
$\alpha^{19}, \alpha^{16}, \alpha^{25}, \alpha^{5}$	$\boldsymbol{h}_{3(2)}$	$\alpha^{7}, \alpha^{8}, \alpha^{4}, \alpha^{4}$	$\alpha^{24}, \alpha^{25}, \alpha^{9}, \alpha^{18}$
$\alpha^{8}, \alpha^{8}, \alpha^{19}, \alpha^{19}$	$\alpha^{29}, \alpha^{9}, \alpha^{1}, \alpha^{12}$	$\alpha^{2}, \alpha^{10}, \alpha^{30}, \alpha^{24}$	$\alpha^{25}, \alpha^{11}, \alpha^{15}, \alpha^{6}$
$\alpha^{8}, \alpha^{10}, \alpha^{1}, \alpha^{30}$	$\alpha^{16}, \alpha^{28}, \alpha^{1}, \alpha^{3}$	$0,\alpha^{11},\alpha^{12},\alpha^{21}$	$\alpha^{3}, \alpha^{10}, \alpha^{10}, \alpha^{22}$
$\alpha^{12},\alpha^{27},\alpha^{0},\alpha^{21}$			

Далі обчислюємо масиви g_k за допомогою гомоморфного перетворення

$$g_{(\mathrm{k})}=\left[g_{1(\mathrm{k})},...,g_{s(\mathrm{k})}\right]=\tau_{(i-1)(\mathrm{k})}^{-(k)}\circ^{(k)} f\left(w_{ij}\right)_{(\mathrm{k})}\circ^{(k)}\tau_{i(\mathrm{k})}$$

$i=\overline{1,s(\mathrm{k})}$, $j=\overline{1,r_{i(\mathrm{k})}}$, $k=\overline{1,4}$. Результати надано в табл. 9.

Таблиця 9

Масиви g_k

$g_k=S(g_{ij(k)}^{(1)},g_{ij(k)}^{(2)},g_{ij(k)}^{(3)},g_{ij(k)}^{(4)})$			
$k=1$	$k=2$	$k=3$	$k=4$
$\boldsymbol{g}_{1(1)}$	$\boldsymbol{g}_{1(2)}$	$\boldsymbol{g}_{1(3)}$	$\boldsymbol{g}_{1(4)}$
α^{27}, α^{21}, α^{17}, α^{13}	α^{14}, α^{16}, α^{7}, α^{18}	α^{5}, α^{6}, α^{22}, α^{30}	$0,\alpha^{21},\alpha^{19},\alpha^{9}$
α^{28}, α^{18}, α^{2}, α^{1}	$\alpha^{5},\alpha^{25},\alpha^{18},0$	$\alpha^{18},\alpha^{18},\alpha^{8},\alpha^{7}$	$\alpha^{19},\alpha^{3},\alpha^{20},\alpha^{19}$
$0,\alpha^{17},\alpha^{1},\alpha^{13}$	α^{24}, α^{3}, α^{1}, α^{13}	$\boldsymbol{g}_{2(3)}$	α^{4}, α^{4}, α^{30}, α^{30}
α^{22}, α^{9}, α^{29}, α^{26}	$\alpha^{20},\alpha^{0},0,\alpha^{23}$	$\alpha^{12},\alpha^{0},\alpha^{1},\alpha^{0}$	α^{21}, α^{23}, α^{4}, α^{3}
$\boldsymbol{g}_{2(1)}$	$\boldsymbol{g}_{2(2)}$	$\alpha^{2},\alpha^{3},\alpha^{6},0$	$\boldsymbol{g}_{2(4)}$
α^{20}, α^{29}, α^{17}, α^{13}	α^{9}, α^{5}, α^{25}, α^{30}	$0,\alpha^{29},\alpha^{5},\alpha^{11}$	$\alpha^{5},\alpha^{1},\alpha^{15},\alpha^{5}$
$\alpha^{21},\alpha^{0},\alpha^{25},\alpha^{28}$	α^{1}, α^{8}, α^{7}, α^{17}	α^{12}, α^{14}, α^{26}, α^{23}	α^{0}, α^{2}, α^{3}, α^{30}
$\alpha^{21},\alpha^{27},\alpha^{21},\alpha^{21}$	α^{15}, α^{10}, α^{13}, α^{9}	$\boldsymbol{g}_{3(3)}$	$\boldsymbol{g}_{3(4)}$
α^{11}, α^{30}, α^{22}, α^{5}	α^{11}, α^{23}, α^{29}, α^{18}	α^{30}, α^{17}, α^{26}, α^{2}	$\alpha^{5},\alpha^{30},\alpha^{25},\alpha^{11}$
α^{15}, α^{24}, α^{17}, α^{24}	$\boldsymbol{g}_{3(2)}$	α^{8}, α^{23}, α^{16}, α^{9}	$\alpha^{2},\alpha^{0},\alpha^{12},\alpha^{9}$
α^{7}, α^{30}, α^{20}, α^{24}	α^{27}, α^{24}, α^{6}, α^{9}	α^{22}, α^{9}, α^{9}, α^{10}	α^{26}, α^{18}, α^{11}, α^{17}
$\alpha^{19},\alpha^{19},\alpha^{3},\alpha^{2}$	α^{7}, α^{24}, α^{25}, α^{26}	α^{13}, α^{21}, α^{11}, α^{26}	α^{16}, α^{10}, α^{30}, α^{14}
α^{6}, α^{10}, α^{17}, α^{17}			

Вихідний відкритий ключ (a_k,h_k,g_k) і закритий ключ $\left[f,\beta_{(k)},\left(t_{0(k)},...,t_{s(k)}\right),\left(\tau_{0(k)},...,\tau_{s(k)}\right)\right]$, $k=\overline{1,4}$.

На етапі шифрування маємо повідомлення $m\in A_l(n,\theta)$, $m=S\left(m_1,m_2,m_3,m_4\right)$ та $m_i\in F_q$ відкритий ключ $\left[f_k,(a_k,h_k,g_k)\right],.\ k=\overline{1,4}$

Дозволяємо $m=\left(\alpha^1,\alpha^2,\alpha^3,\alpha^4\right)=S\left(\alpha^1,\alpha^2,\alpha^3,\alpha^4\right)$.

Вибираємо випадковий $R=(R_1,R_2,R_3,R_4)=(10,20,30,14)$.

Отримуємо наступні R_i розкладання для заданих типів $\left(r_{1(k)},...,r_{s(k)}\right)$, $k=\overline{1,4}$:

$R_1=\left(R_{1(1)},R_{2(1)}\right)=(2,2)=10$,

$R_2=\left(R_{1(2)},R_{2(2)},R_{3(2)}\right)=(0,1,1)=20$,

$R_3=\left(R_{1(3)},R_{2(3)},R_{3(3)}\right)=(0,3,3)=30$.

$R_4=\left(R_{1(4)},R_{2(4)},R_{3(4)}\right)=(2,1,1)=14$

Обчислюємо зашифрований текст:

$$y_1=a'(R)\cdot m=a_1'(R_1)\cdot a_2'(R_2)\cdot a_3'(R_3)\cdot a_4'(R_4)\cdot m=$$
$$S\left(\alpha^7,\alpha^6,\alpha^{22},\alpha^{11}\right)$$

де

$$a_1'(R_1)=a_1(10)=a_{1(1)}(2)a_{2(1)}(2)=S\left(\alpha^{23},\alpha^{13},\alpha^{20},\alpha^{20}\right),$$
$$a_2'(R_2)=a_2(20)=a_{1(2)}(0)a_{2(2)}(1)a_{3(2)}(1)=S\left(\alpha^{26},\alpha^{3},\alpha^{5},\alpha^{29}\right),$$
$$a_3'(R_3)=a_3(30)=a_{1(3)}(0)a_{2(3)}(3)a_{3(3)}(3)=S\left(0,\alpha^{27},\alpha^{8},\alpha^{4}\right),$$
$$a_4'(R_4)=a_4(14)=a_{1(4)}(2)a_{2(4)}(1)a_{3(4)}(1)=S\left(\alpha^{5},\alpha^{12},\alpha^{21},\alpha^{16}\right).$$

Обчислюємо

$$y_2=h_1(R_1)\circ^{(1)}\left(h_2(R_2)\circ^{(2)}\left(h_3(R_3)\circ^{(3)}h_4(R_4)\right)\right)=S\left(0,\alpha^{8},\alpha^{16},\alpha^{17}\right).$$

Компоненти $h_k'(R_k)$ обчислюються аналогічно $a_k'(R_k)$ компонентам, але з використанням відповідної операції множення. Обчислімо компонент y_3:

$$y_3 = g_1(R_1) \circ^{(1)} \left(g_2(R_2) \circ^{(2)} \left(g_3(R_3) \circ^{(3)} g_4(R_4) \right) \right) = S\left(\alpha^{16}, \alpha^{14}, \alpha^1, \alpha^4\right).$$

Отримаємо вихід $y_1 = \left(\alpha^7, \alpha^6, \alpha^{22}, \alpha^{11}\right)$, $y_2 = \left(0, \alpha^8, \alpha^{16}, \alpha^{17}\right)$, $y_3 = \left(\alpha^{16}, \alpha^{14}, \alpha^1, \alpha^4\right)$.

На етапі дешифрування маємо зашифрований текст (y_1, y_2, y_3) і особистий ключ $\left[f, \beta_{(k)}, t_{i(k)}, \tau_{i(k)} \right]$, $i = \overline{0, s(k)}$, $k = \overline{1,4}$.

На виході очікуємо отримати повідомлення $m \in A(P_\infty)$, що відповідає зашифрованому тексту (y_1, y_2, y_3).

Щоб розшифрувати повідомлення m, потрібно відновити випадкові числа $R = (R_1, R_2, R_3)$.

Обчислюємо

$$D^{(1)}(R) = t_{0(1)} \circ^{(1)} y_2 \circ^{(4)} t_{s(4)}^{-(4)} = S(\alpha^{29}, \alpha^8, \alpha^{24}, \alpha^{28}),$$
$$G^{(1)}(R) = \tau_{0(1)} \circ^{(1)} y_3 \circ^{(4)} \tau_{s(4)}^{-(4)} = S(\alpha^{18}, \alpha^5, \alpha^7, \alpha^{30}),$$
$$D^{(1)}(R)' = D^{(1)}(R) \circ^{(1)} \hat{f}(G^{(1)}(R))^{-(1)} = S(\alpha^5, \alpha^{22}, \alpha^{21}, \alpha^0).$$

Відновлюємо R_1 з $\beta_{(1)}(R_1) = \sum_{i=1,\, j=R_{i(1)}}^{s(1)} \beta_{ij(1)}$, використовуючи $\beta_{(1)}(R_1)^{-1}$, оскільки β_1 є простим.

Отримуємо $\beta_1(R_1) = \alpha^5 = (10010)$. Виконаємо обернені обчислення $\beta_{(1)}(R_1)^{-1}$.

10| **010** R_1 =(*,2)
11|010 ряд 1 з $B_{4(1)}$
10| **010** −11|010= **01** |000 R_1 = (2,2)

Отримуємо $\beta_1(R_1)^{-1} = (2,2) = 10$

Для подальшого розрахунку необхідно видалити компонент $h_1'(R_1)$ від y_2 і $g_1'(R_1)$ від y_3.

Обчислюємо:

$$y_2^{(1)} = h_1(R_1)^{-(1)\circ} \cdot y_2^{\circ} = S(\alpha^{26}, \alpha^{16}, \alpha^{17}, \alpha^{19}),$$
$$y_3^{(1)} = g_1(R_1)^{-(1)\circ} \cdot y_3^{\circ} = S(\alpha^{19}, \alpha^{18}, \alpha^{12}, \alpha^{19}),$$
$$D^{(2)}(R) = t_{0(2)} \circ^{(2)} y_2^{(1)} \circ^{(4)} t_{s(4)}^{-(4)} = S(\alpha^{26}, \alpha^{18}, \alpha^{16}, \alpha^2),$$
$$G^{(2)}(R) = \tau_{0(2)} \circ^{(2)} y_3^{(1)} \circ^{(4)} \tau_{s(4)}^{-(4)} = S(\alpha^{30}, \alpha^{27}, \alpha^0, \alpha^{11}),$$
$$D^{(2)}(R)' = D^{(2)}(R) \circ^{(2)} \hat{f}(G^{(2)}(R))^{-(2)} = S(0, \alpha^{12}, \alpha^4, \alpha^{30}).$$

Відновлюємо R_2 з $\beta_{(2)}(R_2) = \sum_{i=1,\, j=R_{i(2)}}^{s(2)} \beta_{ij(2)}$, використовуючи $\beta_{(2)}(R_2)^{-1}$, оскільки β_2 є простим. Ми отримуємо $\beta_2(R_2) = \alpha^{12} = (01111)$. Відновити R_2 за допомогою $\beta_2(R_2)$. Використовуємо ті самі обчислення, що й у прикладі для $\beta_2(R_2)^{-1}$, і отримуємо:

01|11| **1** R_2 =(*,*,1)
10|01|1 ряд 1 з $B_{3(2)}$
01|11| **1** −10|01|1=11| **10** |0 R_2 = (*,1,1)
11|10|0 ряд 0 з $B_{3(2)}$
11| **10** |0−11|10|0= **00** |00|0 R_2 = (0,1,1)

Отримуємо $\beta_2(R_2)^{-1} = (0,1,1) = 20$.

Видаляємо компонент $h_2'(R_2)$ від $y_2^{(1)}$ і $g_2'(R_2)$ від $y_3^{(1)}$, отримуємо

$$y_2^{(2)} = h_3(R_3)^{-(2)\circ} \cdot y_2^{(1)\circ} = S(\alpha^{19}, \alpha^{18}, \alpha^{22}, \alpha^{15}),$$
$$y_3^{(2)} = g_3(R_3)^{-(2)\circ} \cdot y_3^{(1)\circ} = S(\alpha^{21}, \alpha^{10}, \alpha^0, \alpha^{19}),$$
$$D^{(3)}(R) = t_{0(3)} \circ^{(3)} y_2^{(2)} \circ^{(4)} t_{s(4)}^{-(4)} = S(\alpha^{23}, \alpha^5, \alpha^{18}, \alpha^{21}),$$
$$G^{(3)}(R) = \tau_{0(3)} \circ^{(3)} y_3^{(2)} \circ^{(4)} \tau_{s(4)}^{-(4)} = S(\alpha^{21}, \alpha^{10}, \alpha^7, \alpha^{13}),$$
$$D^{(3)}(R)' = D^{(3)}(R) \circ^{(3)} \hat{f}(G^{(3)}(R))^{-(3)} = S(0, 0, \alpha^{19}, \alpha^6)$$

Отримуємо $\beta_3(R_3)=\alpha^{19}=(11011)$.

Виконуємо обернені обчислення $\beta_3(R_3)^{-1}$.

1|10| **11** R_3=(*,*,3)
1|01|11 ряд 3 з $B_{3(3)}$
1|10| **11** −1|01|11=0| **11** |00 R_3= *,3,3)
0|11|00 ряд 3 з $B_{2(3)}$
0| **11** |00−0|11|00= **0** |00|00 R_3=(0,3,3)

Отримуємо $\beta_3(R_3)^{-1}=(0,3,3)=30$.

Видаляємо компонент $h_3'(R_3)$ від $y_2^{(2)}$ і $g_3'(R_3)$ від $y_3^{(2)}$, в результаті отримуємо:

$y_2^{(3)}=h_3(R_3)^{-(3)\circ}\cdot y_2^{(2)\circ}=S(\alpha^{19},\alpha^{1},\alpha^{29},\alpha^{17})$,

$y_3^{(3)}=g_3(R_3)^{-(3)\circ}\cdot y_3^{(2)\circ}=S(\alpha^{13},\alpha^{13},\alpha^{0},\alpha^{16})$,

$D^{(4)}(R)=t_{0(4)}\circ^{(4)} y_2^{(3)}\circ^{(4)} t_{s(4)}^{-(4)}=S(\alpha^{7},\alpha^{2},\alpha^{25},\alpha^{21})$,

$G^{(4)}(R)=\tau_{0(4)}\circ^{(3)} y_3^{(3)}\circ^{(4)} \tau_{s(4)}^{-(4)}=S(\alpha^{11},\alpha^{7},\alpha^{0},\alpha^{16})$,

$D^{(3)}(R)'=D^{(4)}(R)\circ^{(4)} \hat{f}(G^{(4)}(R))^{-(4)}=S(0,0,0,\alpha^{29})$

01010

Отримуємо $\beta_4(R_4)=\alpha^{29}=(01010)$. Виконуємо обернені обчислення $\beta_4(R_4)^{-1}$.

01|0| **10** R_3=(*,*,1)
00|1|10 ряд 1 з $B_{3(4)}$
01|0| **10** −00|1|10=01| **1** |00 R_3= (*,1,1)
00|1|00 ряд 1 з $B_{2(4)}$
01| **1** |00−00|1|00= **01** |0|00 R_3=(2,1,1)

Отримуємо $\beta_4(R_4)^{-1}=(2,1,1)=14$.

Далі отримуємо повідомлення $m=a'(R)^{-1}y_1=S(\alpha^1,\alpha^2,\alpha^3,\alpha^4)$.

Аналіз параметрів безпеки та оцінка вартості

Розглянемо атаку грубої сили для відновлення ключа. Можливі три схеми такої атаки.

Атака грубою силою на зашифрований текст. Вибравши $R=(R_1,R_2,...,R_l)$, спробуємо розшифрувати текст $y_1'=\alpha'(R')\cdot m=\alpha_1'(R_1')\cdot\alpha_2'(R_2')\cdots\alpha_l'(R_l')\cdot m$. Обкладинки $\alpha_k=(a_{ij})_k=S(a_{ij(k)\cdot}^{(1)},a_{ij(k)\cdot}^{(2)},....,a_{ij(k)}^{(l)})$ вибираються випадковим чином, а значення визначається множенням у групі без координатних обмежень. Результуючий вектор $\alpha'(R')$ залежить від усіх компонентів $\alpha_i'(R_i')$. Перелік ключових значень $R=(R_1,R_2,...,R_l)$ має оцінку складності. Для практичної атаки повідомлення m також невідоме та має невизначеність на вибір q^l. Це робить атаку грубою силою на ключ неможливою. Якщо взяти модель атаки з відомим текстом, то складність атаки залишається незмінною і дорівнює q^l.

Атака грубою силою на зашифрований текст y_2. Виберіть $R=(R_1,R_2,...,R_l)$ відповідність y_2. Вектор y_2 має таке визначення над компонентами $\alpha_i'(R_i)$:

$$y_2=S\left(\sum_{k=1}^{l}\sum_{i=1,j=R_{i(k)}}^{s(k)} w_{ij(k)}^{(1)}+\sum_{i=1,j=R_{i(1)}}^{s(1)}\beta_{ij(1)},\sum_{k=1}^{l}\sum_{i=1,j=R_{i(k)}}^{s(k)} w_{ij(k)}^{(2)}+\right.$$
$$\left.\sum_{i=1,j=R_{i(2)}}^{s(2)}\beta_{ij(2)}+*,...,\sum_{k=1}^{l}\sum_{i=1,j=R_{i(k)}}^{s(k)} w_{ij(k)}^{(l)}+\sum_{i=1,j=R_{i(l)}}^{s(l)}\beta_{ij(l)}+*\right).$$

Значення координат y_2 визначаються розрахунками над векторами $w_1'(R_1),w_2'(R_2),...,w_l'(R_l)$. Ключі $R=(R_1,R_2,...,R_l)$ пов'язані, і зміни будь-якого з них призводять до змін y_2. Атака грубою силою на ключ R має складність q^l.

Атака грубою силою на зашифрований текст y_3. Виберіть $R=(R_1,R_2,...,R_l)$ відповідність y_3. Вектор y_3 має таке визначення над компонентами $\rho_i w_i'(R_i)$:

$$y_3 = S\left(\sum_{k=1}^{l}\sum_{i=1,\, j=R_{i(k)}}^{s(k)} f\left(w_{ij(k)}^{(1)}\right)+,\sum_{k=1}^{l}\sum_{i=1,\, j=R_{i(k)}}^{s(k)} f\left(w_{ij(k)}^{(2)}\right)+*,...,\sum_{k=1}^{l}\sum_{i=1,\, j=R_{i(k)}}^{s(k)} f\left(w_{ij(k)}^{(l)}\right)+*\right).$$

Значення координат y_3 визначаються розрахунками над векторами $w_1'(R_1), w_2'(R_2),..., w_l'(R_l)$. Ключі $R_1,R_2,...,R_l$ пов'язані, і зміни будь-якого з них призводять до змін y_3. Атака грубою силою на ключ R має складність q^l.

Атака грубою силою на вектори $\left(t_{0(k)},...,t_{s(k)}\right)$ і $\left(\tau_{0(k)},\tau_{1(k)},...,\tau_{s(k)}\right)$. Атака грубою силою $\left(t_{0(k)},...,t_{s(k)}\right)$ є загальною для криптосистем MST і для розрахунку в полі F_q над центром групи $Z(G)$ має оптимістичну оцінку складності, що дорівнює q. Для запропонованого алгоритму всі обчислення виконуються на всій групі $|A_l(n,\theta)|=q^l$, і складність атаки грубою силою на $\left(t_{0(k)},...,t_{s(k)}\right)$ і $\left(\tau_{0(k)},\tau_{1(k)},...,\tau_{s(k)}\right)$ дорівнюватиме q^l.

Атака на алгоритм. Атака на алгоритм реалізації криптосистеми MST на основі узагальненої 2-групи Сузукі є багатогранною. Практичні атаки розглядають особливості логарифмічних підписів і випадкових накриттів, відомих криптоаналітику. Одним із рішень є використання аперіодичних логарифмічних підписів. У новій криптосистемі з гомоморфним шифруванням випадкові накриття є секретом для криптоаналітика. У цьому випадку відомі атаки на основі слабкості логарифмічних сигнатур неможливі.

Оцінимо параметри безпеки та ключів узагальненої групової криптосистеми Suzuki-2. Зафіксуємо узагальнену 2-групу Сузукі $A_l(n,\theta)=\left\{S(a_1,a_2,...,a_l)\,|\,a_i\in F_q\right\}$, яка визначена над полем F_q, $q=2^n$. Тоді для l-параметричної групи досягаємо $K=nl$ бітової криптографії. Логарифмічний масив підписів і випадкові накриття є відомими параметрами, які використовуються в шифруванні таким чином:

$$\alpha_k=\left[A_{1(k)},...,A_{s(k)}\right]=\left(a_{ij}\right)_k=S\left(a_{ij(k)\cdot}^{(1)},a_{ij(k)\cdot}^{(2)},...,a_{ij(k)}^{(l)}\right),$$

$$h_{(k)}=\left[h_{1(k)},...,h_{s(k)}\right]=S\left(h_{ij(k)\cdot}^{(1)},h_{ij(k)\cdot}^{(2)},...,h_{ij(k)}^{(l)}\right).$$

Крім того, ми знаємо випадкове накриття з гомоморфним шифруванням

$$g_{(k)}=\left[g_{1(k)},...,g_{s(k)}\right]=S\left(g_{ij(k)\cdot}^{(1)},g_{ij(k)\cdot}^{(2)},...,g_{ij(k)}^{(l)}\right)$$

для $k=\overline{1,l}$.

Кількість векторів у масивах α_k, $h_{(k)}$, $g_{(k)}$ визначається типом логарифмічної сигнатури $\left(r_{1(k)},...,r_{s(k)}\right)$ і дорівнює $N=\sum_{k=1}^{l}\left(r_{1(k)}+r_{2(k)}+...+r_{s(k)}\right)$.

Оскільки масиви α_k є випадковими і можуть бути побудовані за допомогою детермінованого генератора випадкових бітів з деякого початкового вектора V, $g_{(k)}$, то можемо визначити α_k над $g_{(k)}$ вектором V. Зафіксуємо довжину вектора V рівною nl бітам.

Розмір масиву $g_{(k)}$ дорівнює: $N_g=l\sum_{k=1}^{l}\left(r_{1(k)}+r_{2(k)}+...+r_{s(k)}\right)$ n-бітовим словам.

До секретних параметрів криптосистеми відносяться вектори t, τ, ρ:

$$t_{0(k)},...,t_{s(k)}\in A_l(n,\theta)\setminus Z,\ t_{i(k)}=S(t_{i1(k)},...,t_{il(k)}),$$

$$\tau_{0(k)},...,\tau_{s(k)}\in A_l(n,\theta)\setminus Z,\ \tau_{i(k)}=S(\tau_{i1(k)},...,\tau_{il(k)}),\ \rho=\left(\rho_1,\rho_2,...,\rho_l\right),\ k=\overline{1,l}.$$

Кількість векторів $t_{i(k)}$ дорівнює $\tau_{i(k)}$: $N_t=N_\tau=l\sum_{k=1}^{l}s(k)$ n-бітовим словам.

Довжина вектора ρ дорівнює nl бітам.

Очевидно, що N_g, N_t, N_τ залежать від типу $\left(r_{1(k)},...,r_{s(k)}\right)$.

Нехай секретність криптографічних перетворень визначається K бітами.

Визначимо тип $\left(r_{1(k)},...,r_{s(k)}\right)=\left(2,...,2\right)$, потім $s(\mathrm{k})=n$ над полем $F(2^n)$. Отримуємо наступні значення:

$$N_g = nl\sum_{k=1}^{l}\left(r_{1(k)}+r_{2(k)}+...+r_{s(k)}\right)=2n^2l^2=2K^2 \text{ біт},$$

$$N_t = N_\tau = nl\sum_{k=1}^{l}s(k)=n^2l^2=K^2 \text{ біт}.$$

Довжина векторів V, ρ дорівнює $N_V = N_\rho = nl = K$ бітам. Визначимо тип $\left(r_{1(k)},...,r_{s(k)}\right)=\left(2^8,...,2^8\right)$, $s(\mathrm{k})=n/8$ над полем $F(2^n)$. Досягаємо

$$N_g = nl\sum_{k=1}^{l}\left(r_{1(k)}+r_{2(k)}+...+r_{s(k)}\right)=2^5n^2l^2=2^5K^2 \text{ біт},$$

$$N_t = N_\tau = nl\sum_{k=1}^{l}s(k)=n^2l^2/8=2^{-3}K^2 \text{ біт}.$$

Приблизні витрати на впровадження представлені в табл. 10.

Витрати пам'яті для масивів спільних і секретних параметрів не залежать від поля $F(2^n)$ і кількості параметрів узагальненої групи Сузукі. Вибір поля F_q та параметрів групи Suzuki визначатиме швидкість обчислень по групі та залежить від програмної реалізації.

Таблиця 10

Орієнтовні витрати на впровадження

$K=256$, $\left(r_{1(k)},...,r_{s(k)}\right)=\left(2,...,2\right)$			
$F(2^n)$	N_g Кбайт	N_t (N_τ), Кбайт	N_V (N_ρ), біт
$F(2^8),\ldots,F(2^{256})$	4	2	256
$K=256$, $\left(r_{1(k)},...,r_{s(k)}\right)=\left(2^8,...,2^8\right)$			
$F(2^8),\ldots,F(2^{256})$	64	0,25	256
$K=512$, $\left(r_{1(k)},...,r_{s(k)}\right)=\left(2,...,2\right)$			
$F(2^8),\ldots,F(2^{512})$	64	32	512
$K=512$, $\left(r_{1(k)},...,r_{s(k)}\right)=\left(2^8,...,2^8\right)$			
$F(2^8),\ldots,F(2^{512})$	1024	8	512

Висновки

Узагальнені 2-групи Сузукі є багатопараметричними групами і можуть мати як завгодно великий порядок. Криптосистеми MST на основі узагальненої групи Сузукі 2 мають перевагу над іншими реалізаціями схем у секретності та реалізації. Можемо побудувати високозахищену криптосистему з груповими обчисленнями в невеликому кінцевому полі. Застосування гомоморфного шифрування до випадкових накриттів у логарифмічному підписі забезпечує захист від відомих атак на реалізації логарифмічного підпису. Для побудови криптосистеми можна використовувати захищені логарифмічні підписи простої конструкції, що призводить до низьких витрат на загальні параметри криптосистеми. Запропонована криптосистема з гомоморфним шифруванням є хорошим кандидатом для постквантової криптографії.

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 12.10.2023

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,