УДК 621.391:519.2 **DOI:10.30837/rt.2023.2.213.05**

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

ПОБУДОВА ТРЬОХПАРАМЕТРИЧНОЇ СХЕМИ ШИФРУВАННЯ НА ГРУПАХ ЕРМІТА В КРИПТОСИСТЕМІ MST3

Вступ

У статті пропонується метод побудови трьохпараметричної схеми шифрування на групах Ерміта, що вдосконалює параметри безпеки існуючої криптосистеми MST3. Завдання вдосконалення існуючих підходів до побудови криптосистем зумовлено успіхами в побудові квантового комп'ютера з достатньою обчислювальною потужністю, що зробить багато криптосистем із відкритим ключем незахищеними. Зокрема мова йде про ті криптосистеми, що базуються на складності факторизації або проблемі дискретного логарифмування, такі як RSA, ECC тощо. Існує кілька пропозицій, які стали класичними за останні майже 20 років, щодо використання некомутативних груп для побудови квантовостійких криптосистем [1 – 4]. Нерозв'язна проблема слова є цікавою областю дослідження для побудови криптосистеми. Вона була сформульована Вагнером і Магьяриком, досліджена у [5, 6] і лежить у площині застосування груп перестановок. Вперше логарифмічні сигнатури (LS) були запропоновані Магліверасом. У цьому контексті логарифмічна сигнатура є особливим типом факторизації, вона застосовується до кінцевих груп. Покращення оригінальної версії криптосистеми запропоновано в [7, 8]. Остання версія цієї реалізації відома як MST3 [9] і базується на групі Сузукі.

У 2008 р. Магліверас продемонстрував обмеження транзитивного використання LS для криптосистеми MST3. Пізніше Сваба запропонував криптосистему eMST3 з покращеними параметрами безпеки. Для цього вдосконалення було додано секретне гомоморфне покриття. Потім, у 2018 р., Т. ван Трунг запропонував підхід MST3 з використанням сильних аперіодичних LS для абелевих *p*-груп. Конг з колегами провели широкий аналіз MST3 і відзначили, що, оскільки на даний момент немає публікацій про квантову вразливість алгоритму, його можна вважати кандидатом на постквантовий період.

Оригінальний підхід до побудови криптосистеми MST3 базується на групі Сузукі. В рамках доповідей на конференції було розглянуто результати дослідницької роботи, що демонструє подальше вдосконалення MST3 [10 – 19]. Однією з цінних ідей є підвищення ефективності шифрування шляхом оптимізації накладних витрат на обчислення. Це зроблено зі зменшенням великого розміру ключового простору. Цей підхід можна застосовувати для обчислень LS за межами центру групи. І це було зроблено над кінцевими полями малої розмірності з використанням груп з великим порядком.

Групи Сузукі ізоморфні проєктивній лінійній групі $PGL\left(3,F_q\right)$, $q_0=2^n$, де $q=2q_0^2$ і має порядок q^2. Безпека криптосистеми на групах визначається саме груповим порядком. У [13] автори вперше запропонували використання трьохпараметричної групи автоморфізму для вдосконалення параметрів безпеки криптосистеми MST3.

Особливістю пропозиції є те, що $H\left(P_\infty\right)$ має ще $Herm\left|F_{q^2}\right.$ більший порядок $ordH\left(P_\infty\right)=q^3\left(q^2-1\right)$ ніж порядок відповідної групи Сузукі, яка розглядається в оригінальних статтях. Наукова новизна пропозиції полягає в тому, що стаття представляє практичну реалізацію цього нового підходу.

Використання трьохпараметричної групи автоморфізмів функціонального поля Ерміта

Розглянемо $Herm\left|F_{q^2}\right.$ [14]. Використовуємо $Aut\left(Herm\right)$ у $Herm\left|F_{q^2}\right.$, і це можна представити як $H:=Aut\left(Herm\right)=\left\{\psi:Herm\mapsto Herm\left|\psi\ \text{з}\ Herm\right|F_{q^2}\right\}$. Властивості автоморфізмів обговорювалися

в [14]. Порядок цієї групи $ordA = q^3\left(q^2-1\right)\left(q^3+1\right)$. Група розкладання $H\left(P_\infty\right)$ має всі автоморфізми $Aut\left(Herm\right)$ з $Herm\left|F_{q^2}\right.$ та такі властивості:

$$\begin{cases} \psi(y) = \alpha y + \beta \\ \psi(z) = \alpha^{q+1} z + \alpha\beta^q y + \gamma, \end{cases}$$

де $\alpha \in F_{q^2}^* := F_{q^2} \setminus \{0\}$, $\beta \in F_{q^2}$ і $\gamma^q + \gamma = \beta^{q+1}$.

Порядок групи дорівнює $ordH\left(P_\infty\right) = q^3\left(q^2-1\right)$. Структуру групи представимо виразом

$$[\alpha_1,\beta_1,\gamma_1]\cdot[\alpha_2,\beta_2,\gamma_2] = \left[\alpha_1\alpha_2, \alpha_2\beta_1+\beta_2, \alpha_2^{q+1}\gamma_1 + \alpha_2\beta_2^q\beta_1 + \gamma_2\right].$$

Таким чином, маємо тотожність $[1,0,0]$ та інверсію $[\alpha,\beta,\gamma]$:

$$[\alpha,\beta,\gamma]^{-1} = \left[\alpha^{-1}, -\alpha^{-1}\beta, \alpha^{-(q+1)}\gamma^q\right],$$

$H\left(P_\infty\right)$ можна представити простіше:

$$H\left(P_\infty\right)\left\{\left[\alpha,\beta,\frac{\beta^{q+1}}{2}+\gamma\right]\middle|\alpha\in F_{q^2}^*, \beta\in F_{q^2},\ \gamma^q+\gamma=0\right\}.$$

Унікальна *p*-Sylow підгрупа $H\left(P_\infty\right)$ може бути позначена в $H_1\left(P_\infty\right)$ межах представлення $H_1\left(P_\infty\right) = \left\{\psi \in H\left(P_\infty\right)\middle|\psi(y) = y+\beta \text{ для деяких } b\in F_{q^2}\right\}$.

У такому випадку маємо порядок, що дорівнює q^3 для унікальної *p*-Sylow підгрупи:

$$\begin{cases} \psi(y) = y + \beta \\ \psi(z) = z + \beta^q y + \gamma, \end{cases}$$

де $\beta \in F_{q^2}$ і $\gamma^q + \gamma = \beta^{q+1}$, а порядок дорівнює q^3, як ми згадували вище. Структура для групи може бути досягнута шляхом представлення підгрупи PGL(3, *k*)*:*

$$H_1 := \left\{\begin{pmatrix} 1 & \beta & \gamma \\ 0 & 1 & \beta^q \\ 0 & 0 & 1 \end{pmatrix},\ \gamma\in F_{q^2}, \gamma^q+\gamma=\beta^{q+1}\right\}.$$

Групова операція визначається як $[1,\beta_1,\gamma_1]\cdot[1,\beta_2,\gamma_2] = \left[1,\beta_1+\beta_2,\gamma_1+\beta_2^q\beta_1+\gamma_2\right]$ та $[\beta_1,\gamma_1]\cdot[\beta_2,\gamma_2] = \left[\beta_1+\beta_2,\gamma_1+\beta_2^q\beta_1+\gamma_2\right]$. Група факторизації $H\left(P_\infty\right)/H_1\left(P_\infty\right)$ є циклічною за порядком q^2-1. Крім того, вона була створена за $\varsigma\in H\left(P_\infty\right)$ допомогою $\varsigma(y)=\alpha z,\ \varsigma(z)=\alpha^{q+1}z$. Інший автоморфізм $\zeta\in H$ задано $\zeta(y)=y/z,\ \zeta(z)=1/z$. Група автоморфізмів $H\left(P_\infty\right)$ ермітового функціонального поля $Herm\left|F_{q^2}\right.$, що визначає його $\psi(y),\psi(z)$, має порядок $ordH\left(P_\infty\right) = q^3\left(q^2-1\right)$ більший, ніж порядок групи Сузукі.

Метод, що пропонується

Отже, у рамках цієї пропозиції маємо наступні етапи генерації ключів, шифрування та дешифрування.

Маємо велику групу $H\left(P_\infty\right)$. Ця група заснована на автоморфізмі $\psi(y),\psi(z)$. Побудова елементів групи $H\left(P_\infty\right)$ визначається розв'язуванням рівняння $\gamma^q+\gamma=\beta^{q+1}$ відносно γ. Складність знаходження *c* пропорційна q. $H\left(P_\infty\right)$ з $Herm\left|F_{q^2}\right.$ можуть бути представлені так:

$$H\left(P_\infty\right) = \left\{\left[\alpha,\beta,\frac{\beta^{q+1}}{2}+\gamma\right]\middle|\alpha\in F_{q^2}^*, \beta\in F_{q^2},\ \gamma^q+\gamma=0\right\}.$$

І це вірно для непарної характеристики. Якщо λ – твірний елемент поля, то рівняння $\gamma^q+\gamma=0$ має розв'язання $\gamma_i = \lambda^{(q+1)/2+k(q+1)}$, $k=\overline{0,q-1}$. Обчислювальні вектори з використанням матриць LS і випадкових покриттів (RC) транскодуються в координати β,γ підгрупи $H\left(P_\infty\right)$.

Групова операція визначається як

$$S(\alpha_1,\beta_1,\gamma_1)\cdot S(\alpha_2,\beta_2,\gamma_2)=S\left(\alpha_1\alpha_2,\alpha_2\beta_1+\beta_2,\alpha_2^{q+1}\gamma_1+\alpha_2\beta_2^q\beta_1+\gamma_2\right).$$

Інверсія до $S(\alpha,\beta,\gamma)^{-1}=S\left(\alpha^{-1},-\alpha^{-1}\beta,-\alpha^{-(g+1)}\gamma+\alpha^{-(g+1)}\beta^{q+1}\right)$.

Обчислення оберненого елемента $S(\alpha,\beta,\gamma)^{-1}$ в цьому представленні розширює область для $\gamma_1=\frac{\beta_1^{q+1}}{2}+\gamma'_1$ і $\gamma_2=\frac{\beta_2^{q+1}}{2}+\gamma'_2$. Це ключова ідея в побудові LS на групі $H(P_\infty)$ на основі $Herm\left|F_{q^2}\right.$.

В іншому випадку, якщо γ'_1 і γ'_2 є розв'язанням рівняння $\gamma^q+\gamma=0$, обернений елемент строго визначається через вираз $S(\alpha,\beta,\gamma)^{-1}=S\left(\alpha^{-1},-\alpha^{-1}\beta,\alpha^{-(q+1)}\gamma^q\right)$.

Як вихід ми маємо $[w,\gamma,f]$ як відкритий ключ із відповідним секретним ключем $\left[v,(\tau_0,...,\tau_s)\right]$. Для генерації ключів застосовуємо наступні кроки:

1. Обираємо першу просту LS: $v_{(1)}=\left[V_{1(1)},...,V_{s(1)}\right]=(v_{kn})_{(1)}=S\left(1,v_{kn(1)},v_{kn(1)}^{q+1}/2\right)$ типу $\left(r_{1(1)},...,r_{s(1)}\right)$, $k=\overline{1,s(1)}$, $n=\overline{1,r_{i(1)}}$, $v_{kn(1)}\in F_{q^2}$.

2. Обираємо другу просту LS: $v_{(2)}=\left[V_{1(1)},...,V_{s(2)}\right]=(v_{kn})_{(2)}=S\left(1,0,v_{kn(2)}\right)$ типу $\left(r_{1(2)},...,r_{s(2)}\right)$, $k=\overline{1,s(2)}$, $n=\overline{1,r_{i(2)}}$, $v_{kn(2)}\in F_q\subset F_{q^2}$.

3. Обираємо перше RC: $w_{(1)}=\left[W_{1(1)},...,W_{s(1)}\right]=(w_{kn})_{(1)}=S\left(w_{kn(1)_1},w_{kn(1)_2},\left(w_{kn(1)_2}\right)^{q+1}/2\right)$ того ж типу, що й $v_{(1)}$, де $w_{kn}\in H(P_\infty)$, $w_{kn(1)_1},w_{kn(1)_2}\in F_{q^2}\setminus\{0\}$.

4. Обираємо друге RC: $w_{(2)}=\left[W_{1(2)},...,W_{s(2)}\right]=(w_{kn})_{(2)}=S\left(w_{kn(2)_1},w_{kn(2)_2},\left(w_{kn(2)_2}\right)^{q+1}/2+w_{kn(2)_3}\right)$ того ж типу, що $v_{(2)}$, де $w_{kn(2)_2},w_{kn(2)_3}\in F_q\setminus\{0\}\subset F_{q^2}$.

5. Обираємо: $\tau_{0(l)},\tau_{1(l)},...,\tau_{s(l)}\in H(P_\infty)\setminus Z$, $\tau_{i(l)}=S\left(\tau_{i(l)_1},\tau_{i(l)_2},(\tau_{i(l)_2})^{q+1}/2\right)$, $t_{i(l)_k}\in F^\times$, $i=\overline{0,s(l)}$, $l=\overline{1,2}$. Домовимося, що $\tau_{s(1)}=\tau_{0(2)}$.

6. Будуємо гомоморфізм f_1, що визначається $f_1\left(S\left(w_1,w_2,w_2^{q+1}/2\right)\right)=S\left(1,w_2,w_2^{q+1}/2\right)$.

7. Обчислюємо $g_{(1)}=\left[g_{1(1)},...,g_{s(1)}\right]=(g_{kn})_{(1)}=\tau_{(k-1)(1)}^{-1}f_1\left((w_{kn})_{(1)}\right)(v_{kn})_{(1)}\tau_{k(1)}$, $k=\overline{1,s(1)}$, $n=\overline{1,r_{i(1)}}$, де $f_1\left((w_{kn})_{(1)}\right)(v_{kn})_{(1)}=S\left(1,w_{kn(1)_2}+v_{kn(1)},w_{kn(1)_2}^{q+1}/2+w_{kn(1)_2}v_{kn(1)}^q+v_{kn(1)}^{q+1}/2\right)$.

8. Визначимо гомоморфізм $f_2\left(S\left(w_1,w_2,w_2^{q+1}/2\right)\right)=S\left(1,0,w_2\right)$ та обчислимо

$$g_{(2)}=\left[g_{1(2)},...,g_{s(2)}\right]=(g_{kn})_{(2)}=\tau_{(k-1)(2)}^{-1}f_2\left((w_{kn})_{(2)}\right)(v_{kn})_{(2)}\tau_{k(2)},\ k=\overline{1,s(2)},\ n=\overline{1,r_{i(2)}},$$

де $f_2\left((w_{kn})_{(2)}\right)v(b_{kn})_{(2)}=S\left(1,0,w_{kn(2)_2}+v_{kn(2)}\right)$.

В результаті виконання кроків 1 – 8 маємо відкритий ключ, що дорівнює $[f_1,f_2,(w_l,g_l)]$, та секретний ключ, що дорівнює $\left[v_{(l)},\left(\tau_{0(l)},...,\tau_{s(l)}\right)\right]$, $l=\overline{1,2}$. Генерацію ключів завершено. Розглянемо наступний етап реалізації нашого методу – шифрування.

Отже, як вхідні дані для шифрування маємо текст $x\in H(P_\infty)$ і $x=S(x_1,x_2,x_3)$, відкритий ключ $[f_1,f_2,(w_l,g_l)]$, $l=\overline{1,2}$. Для етапу шифрування необхідно виконати кроки:

1. Оберемо випадково $Q=(Q_1,Q_2)$, $Q_1\in Z_{\left|F_{q^2}\right|}$, $Q_2\in Z_{|\square|}$.

2. Обчислимо $y_1=w'(Q)\cdot x=w_1'(Q_1)\cdot w_2'(Q_2)\cdot x,$

$$y_2=g'(Q)=g_1'(Q_1)\cdot g_2'(Q_2)=S\left(*,w_{(1)_1}(Q_1)+v_{(1)}(Q_1)+*,w_{(2)_2}(Q_2)+v_{(2)}(Q_2)+*\right).$$

Перехресні розрахунки $\tau_{0(l)},...,\tau_{s(l)}$ використовуються для визначених $(*)$ компонентів та для додавання третьої координати в добуток $w_{(1)_1}(Q_1)+v_{(1)}(Q_1)$.

3. Обчислимо $y_3 = f_1\left(w_1'(Q_1)\right) = S\left(1, w_{(1)_2}(Q_1), *\right)$, $y_4 = f_2\left(w_2'(Q_2)\right) = S\left(1, 0, w_{(2)_2}(Q_2)\right)$.

Як результат обчислень маємо зашифрований вектор (y_1, y_2, y_3, y_4) повідомлення x.

Перевіримо правильність запропонованого підходу на практиці.

Візьмемо кінцеве поле F_{q^2}, $q^2 = 3^6$, $g(z) = z^6 + 2z + 2$ та групу

$$H(P_\infty) = \left\{ \left[\alpha, \beta, \frac{\beta^{q+1}}{2} + \gamma \right] \middle| \alpha \in F_{q^2}^*, \beta \in F_{q^2}, \ \gamma^q + \gamma = 0 \right\}.$$

Для групової операції використовуємо добуток двох матриць:

$$S(\alpha_1, \beta_1, \gamma_1) \cdot S(\alpha_2, \beta_2, \gamma_2) = S\left(\alpha_1\alpha_2, \alpha_2\beta_1 + \beta_2, \alpha_2^{q+1}\gamma_1 + \alpha_2\beta_2^q\beta_1 + \gamma_2\right).$$

$$S(a_1, b_1, c_1) \cdot S(a_2, b_2, c_2) = S\left(a_1a_2, a_2b_1 + b_2, a_2^{q+1}c_1 + a_2b_2^qb_1 + c_2\right),$$

де $\gamma_1 = \frac{\beta_1^{q+1}}{2} + \gamma'_1$, $\gamma_2 = \frac{\beta_2^{q+1}}{2} + \gamma'_2$.

Обернений елемент визначаємо як $S(\alpha,\beta,\gamma)^{-1} = S\left(\alpha^{-1}, -\alpha^{-1}\beta, \alpha^{-(q+1)}\gamma^q\right)$; $S(1,0,0)$ є трійкою і є тотожністю.

4. Побудуємо прості LS: $v_{(1)} = \left[V_{1(1)}, ..., V_{s(1)}\right] = (v_{kn})_{(1)} = S\left(1, v_{i_{kn}(1)}, v_{kn(1)}^{q+1}/2\right)$ типу $\left(r_{1(1)}, ..., r_{s(1)}\right)$, $k = \overline{1, s(1)}$, $n = \overline{1, r_{i(1)}}$, $v_{kn(1)} \in F_{q^2}$ для координати β та $v_{(2)} = (v_{kn})_{(2)} = S\left(1, 0, v_{i_{kn}(2)}\right)$ типу $\left(r_{1(2)}, ..., r_{s(2)}\right)$, $k = \overline{1, s(2)}$, $n = \overline{1, r_{i(2)}}$, $v_{kn(2)} \in F_q \subset F_{q^2}$ для координати γ. LS v_1 і v_2 в групових представленнях визначають $v_{kn(1)}$ і $v_{kn(2)}$ координати. Типи $\left(r_{1(l)}, ..., r_{s(l)}\right)$ і LS v_1 і v_2 обираються самостійно. Нехай LS v_1 і v_2 мають типи $\left(r_{1(1)}, r_{2(1)}, r_{3(1)}\right) = \left(3^3, 3^2, 3\right)$, $\left(r_{1(2)}, r_{2(2)}\right) = \left(3^2, 3\right)$; масиви $v_{kn(1)}$ складаються з трьох підмасивів і $v_{kn(2)}$ мають два підмасиви з r_i кількістю рядків. Будь-яку фрагментацію масивів можна обрати за умови $\prod_{i=1}^{s(1)} r_i = 3^6$ для $v_{kn(1)}$ і $\prod_{i=1}^{s} r_i = 3^3$ відповідно. Кожен рядок v_{kn} – це F_{q^2} елемент поля. Побудуємо масиви LS методом, який розглянуто у [2]. Для виконання та підвищення вимог безпеки масивів v_l можемо використовувати різні криптографічні перетворення. Можемо просто додати вектори шуму, переставити рядки в підмасивах V_i, об'єднати масиви V_i або використати матричні перетворення. Це допомагає створити дві різні LS: $v_1 = \left[V_{1(1)}, V_{2(1)}, V_{3(1)}\right]$ і $v_2 = \left[V_{1(2)}, V_{2(2)}\right]$. Масиви LS $v_1 = S\left(1, v_{kn(1)}, v_{kn(1)}^{q+1}/2\right)$ та $v_2 = S\left(1, 0, v_{kn(2)}\right)$ у груповому представленні визначають координати $v_{kn(1)}$ та $v_{kn(2)}$ відповідно.

5. Побудуємо RC w_l для того самого типу, що і v_1 і v_2:

$$w_{(1)} = \left[W_{1(1)}, ..., W_{s(1)}\right] = (w_{kn})_{(1)} = S\left(w_{kn(1)_1}, w_{kn(1)_2}, \left(w_{kn(1)_2}\right)^{q+1}/2\right),$$

$$w_{(2)} = \left[W_{1(2)}, ..., W_{s(2)}\right] = (w_{kn})_{(2)} = S\left(w_{kn(2)_1}, w_{kn(2)_2}, \left(w_{kn(2)_2}\right)^{q+1}/2 + w_{kn(2)_3}\right),$$

де $w_{kn(1)_1}, w_{kn(1)_2} \in F_{q^2} \setminus \{0\}$, $w_{kn(2)_3} \in F_q \setminus \{0\} \subset F_{q^2}$, $k = \overline{1, s_{(l)}}$, $n = \overline{1, r_{k(l)}}$, $l = \overline{1, 2}$.

Ці покриття w_l мають бути визначені трьома масивами $\left(w_{kn(l)_1}, w_{kn(l)_2}, w_{kn(l)_3}\right)$ з ненульовими записами.

6. Згенеруємо RC $w_1 = \left[W_{1(1)}, W_{2(1)}, W_{3(1)}\right]$, $w_2 = \left[W_{1(2)}, W_{2(2)}\right]$. У полі представлення $w_1 = S\left(w_{kn(1)_1}, w_{kn(1)_2}, w_{kn(1)_3}\right)$ і $w_2 = S\left(w_{kn(2)_1}, w_{kn(2)_2}, w_{kn(2)_3}\right)$ має вигляд: $\tau_{0(l)}, \tau_{1(l)}, ..., \tau_{s(l)} \in H(P_\infty) \setminus Z$, $\tau_{i(l)} = S\left(\tau_{i(l)_1}, \tau_{i(l)_2}, (\tau_{i(l)_2})^{q+1}/2\right)$, $\tau_{i(l)_k} \in F^\times$, $i = \overline{0, s(l)}$, $l = \overline{1, 2}$ буде обрано випадковим чином.

7. Припустимо, $\tau_{s(1)} = \tau_{0(2)}$. Нехай для 1-*ї* LS β_1 і для 2-ї LS β_2.

8. Масиви g_1 та, g_2, які потрібно обчислити на наступному кроці. Отже, отримуємо

$$g_{(1)} = \left[g_{1(1)}, ..., g_{s(1)}\right] = (g_{kn})_{(1)} = \tau_{(k-1)(1)}^{-1} f_1\left((w_{kn})_{(1)}\right)(v_{kn})_{(1)}\, \tau_{k(1)},$$

$$g_{(2)} = \left[g_{1(2)}, ..., g_{s(2)}\right] = (g_{kn})_{(2)} = \tau_{(k-1)(2)}^{-1} f_2\left((w_{kn})_{(2)}\right)(v_{kn})_{(2)}\, \tau_{k(2)}.$$

за умови наданого прикладу.

9. Побудуємо гомоморфізми f_1, f_2, визначені за

$$f_1\left(S\left(w_1, w_2, w_2^{q+1}/2\right)\right) = S\left(1, w_2, w_2^{q+1}/2\right),\ f_2\left(S\left(w_1, w_2, w_2^{q+1}/2\right)\right) = S\left(1, 0, w_2\right).$$

У полі представлення $g_1 = S(g_{kn(1)_1}, g_{kn(1)_2}, g_{kn(1)_3})$ і $g_2 = S(g_{kn(2)_1}, g_{kn(2)_2}, g_{kn(2)_3})$ мають матричний вигляд. Наприклад, нехай $Q_1 = 379$. Тоді отримуємо наступну базову факторизацію для заданого типу $\left(r_{1(1)}, r_{2(1)}, r_{3(1)}\right) = \left(3^3, 3^2, 3\right)$ у формі $Q_1 = \left(Q_{1(1)}, Q_{2(1)}, Q_{3(1)}\right) = (1,5,1)$, де $Q_1 + Q_2 3^3 + Q_3 3^5 = 379$.

Обчислюємо

$$g_1(379) = g_{1(1)}(1)\, g_{2(1)}(5)\, g_{3(1)}(1) = S\left(\alpha^{14}, \alpha^{150}, \alpha^{232}\right) S\left(\alpha^{499}, \alpha^{561}, \alpha^{678}\right) S\left(\alpha^{608}, \alpha^{24}, \alpha^{632}\right) = S\left(\alpha^{393}, \alpha^{91}, \alpha^{0}\right).$$

Нехай $R_2 = 17$. Отримуємо $Q_2 = \left(Q_{1(2)}, Q_{2(2)}\right) = (8,1) = 17$ для заданого типу $\left(r_{1(2)}, r_{2(2)}\right) = \left(3^2, 3\right)$.

Обчислюємо

$$g_2(17) = g_{1(2)}(8)\, g_{2(2)}(1) = S\left(\alpha^{147}, \alpha^{149}, \alpha^{328}\right) S\left(\alpha^{36}, \alpha^{697}, \alpha^{24}\right) = S\left(\alpha^{183}, \alpha^{192}, \alpha^{433}\right).$$

Розглянемо покроковий алгоритм шифрування. У $x_2, x_3 \in F_{q^2}$ маємо повідомлення $x \in N(P_\infty)$, $x = S(x_1, x_2, x_3)$, $x_1 \in F_{q^2} \setminus \{0\}$ і відкритий ключ $[f_1, f_2, (w_l, g_l)]$, $l = \overline{1,2}$ для введення. Нехай $x = \left(\alpha^1, \alpha^2, \alpha^3\right) = S\left(\alpha^1, \alpha^2, \alpha^3\right)$. $Q = (Q_1, Q_2) = (379,17)$, $Q_1 \in \square_{\left|F_{q^2}\right|}$, $Q_2 \in \square_{|F_q|}$ обираються випадковим чином. Для наступного кроку обчислимо:

$$y_1 = w'(Q) \cdot x = w_1'(Q_1) \cdot w_2'(Q_2) \cdot x = S\left(\alpha^{145}, \alpha^{602}, \alpha^{329}\right),$$

$$y_2 = g'(Q) = g_1'(Q_1) \cdot g_2'(Q_2) = S\left(\alpha^{576}, \alpha^{370}, \alpha^{226}\right),$$

$$y_3 = f_1\left(w_1'(Q_1)\right) = S\left(\alpha^{0}, \alpha^{394}, \alpha^{383}\right),$$

$$y_4 = f_2\left(w_2'(Q_2)\right) = S\left(\alpha^{0}, 0, \alpha^{692}\right).$$

Отримуємо зашифрований текст (y_1, y_2, y_3, y_4) повідомлення x.

Розглянемо покроковий алгоритм дешифрування. Маємо зашифрований текст (y_1, y_2, y_3, y_4) і закритий ключ $\left[v_l, \left(\tau_{0(l)}, ..., \tau_{s(l)}\right)\right]$ як вхідні дані. Випадкові числа $Q = (Q_1, Q_2)$ будуть відновлені наступними кроками для розшифровки повідомлення x:

$$D^{(1)}(Q_1, Q_2) = \tau_{0(1)} y_2 \tau_{s(2)}^{-1} = \tau_{0(1)} S\left(\alpha^{576}, \alpha^{370}, \alpha^{226}\right) \tau_{s(2)}^{-1} = S\left(\alpha^{0}, \alpha^{273}, \alpha^{139}\right),$$

$$D^{*}(Q) = y_3^{-1} D^{(1)}(Q_1, Q_2) = S\left(\alpha^{0}, \alpha^{30}, \alpha^{149}\right) S\left(\alpha^{0}, \alpha^{273}, \alpha^{139}\right) = S\left(\alpha^{0}, \alpha^{32}, \alpha^{408}\right).$$

Отримуємо $v_1(Q_1) = \alpha^{32} = (202211)$.

Відновлення Q_1 зроблено раніше: $Q_1 = \left(Q_{1(1)}, Q_{2(1)}, Q_{3(1)}\right) = (1,5,1)$.

Компоненти масивів $w_1'(Q_1)$ і $w_1'(Q_1)$ будуть видалені із зашифрованого тексту (y_1, y_2) для подальших обчислень: $y_2^{(1)} = \gamma_1'(Q_1)^{-1} y_2 = S\left(\alpha^{393}, \alpha^{91}, \alpha^{0}\right)^{-1} S\left(\alpha^{576}, \alpha^{370}, \alpha^{226}\right) = S\left(\alpha^{183}, \alpha^{192}, \alpha^{433}\right)$.

Повторюємо обчислення

$$D^{(2)}(Q_2) = \tau_{0(2)} y_2^{(1)} \tau_{s(2)}^{-1} = \tau_{0(2)} S\left(\alpha^{183}, \alpha^{192}, \alpha^{433}\right) \tau_{s(l/2)}^{-1} = S\left(\alpha^{0}, 0, \alpha^{589}\right),$$

$$D^{*}(Q) = D^{(2)}(Q_2) y_4^{-1} = S\left(\alpha^{0}, 0, \alpha^{589}\right) S\left(\alpha^{0}, 0, \alpha^{692}\right)^{-1} = S\left(\alpha^{0}, 0, \alpha^{2}\right).$$

Відновимо Q_2 за допомогою $v_2(Q_2) = \alpha^2 = (001000)$.

Виконуємо обернені обчислення $v_2(Q_2)^{-1}$. Ми знайшли групи бітів $v(Q)$ відповідно до типу $\left(r_{1(2)}, ..., r_{s(2)}\right) = \left(3^2, 3\right)$. Те саме обчислення, яке буде використано в прикладі для $v_1(Q_1)^{-1}$. Тоді отримаємо $Q_2 = \left(Q_{1(2)}, Q_{2(2)}\right) = (8,1) = 17$.

Отримуємо відкрите повідомлення:

$$x = w'(Q)^{-1} y_1 = \left[w_1'(Q_1) \cdot w_2'(Q_2)\right]^{-1} \cdot y_1 = \left[S\left(\alpha^{391}, \alpha^{39}, \alpha^{36}\right) S\left(\alpha^{481}, \alpha^{52}, \alpha^{637}\right)\right]^{-1} S\left(\alpha^{145}, \alpha^{602}, \alpha^{329}\right) = S\left(\alpha^{1}, \alpha^{2}, \alpha^{3}\right)$$

Вихід: повідомлення $x = \left(\alpha^1, \alpha^2, \alpha^3\right)$.

Аналіз безпеки запропонованого методу

Розглянемо і опишемо можливі атаки. По-перше, атака, відома як груба сила (BFA), може бути виконана над зашифрованим текстом. Вибравши $Q=(Q_1,Q_2)$, спробуємо розшифрувати текст $y_1=w'(Q)\cdot x=w_1'(Q_1)\cdot w_2'(Q_2)\cdot x$. У цьому випадку складність атаки дорівнює q^3.

По-друге, варіант BFA на $Q=(Q_1,Q_2)$, знов обираємо такий $Q=(Q_1,Q_2)$, щоб знайти $y_2=g'(Q)=g_1'(Q_1)\cdot g_2'(Q_2)$. У цьому випадку складність атаки також дорівнює q^3.

По-третє, якщо вибрати Q_1 відповідним значенню $w_{(1)_2}(Q_1)$ у векторі $y_3=f_1(w_1'(Q_1))=S(1,w_{(1)_2}(Q_1),*)$. У цьому випадку складність атаки дорівнює q^2. Крім того, можемо спробувати вибрати Q_2 з відповідним значенням $w_{(2)_2}(Q_2)$ у векторі y_4. У цьому випадку він менш складний і дорівнює q. Ми розглядаємо можливість використання матричного перетворення як можливого механізму захисту.

Далі можемо застосувати BFA до $(\tau_{0(l)},...,\tau_{s(l)})$ векторів. У цьому випадку складність атаки дорівнює $(q^2)^2$.

Крім того, існує атака на сам алгоритм. Параметри вилучення $w_{(1)_1}(Q_1)$, $w_{(2)_2}(Q_2)$ з y_3, y_4 не дозволяють обчислити $w_1'(Q_1)\cdot w_2'(Q_2)$ в $y_1=w_1'(Q_1)\cdot w_2'(Q_2)\cdot x$. Якщо ми просто спробуємо знайти параметри Q_1,Q_2, потрібні зусилля на рівні BFA зі складністю q^2. q^2. Оскільки $H(P_\infty)$ з $Herm|F_{q^2}$ визначається над полем F_{q^2}, яке є достатньо великим, ця атака просто неможлива.

Висновки

Для криптосистеми $H(P_\infty)$ з використанням β на основі $Herm|F_{q^2}$ маємо наступні висновки. В цьому випадку LS $v=[V_1,...,V_s]=(v_{kn})=S(1,v_{kn(2)}.v_{kn(3)}.)$ є підгрупою $H(P_\infty)=\{S(\alpha,\beta,\gamma)|\alpha,\beta\in F_{q^2},\gamma^q+\gamma=\beta\}$, а RC $w=[W_1,...,W_s]=(w_{kn})=S(w_{kn(1)},w_{kn(2)},w_{kn(3)})$ – однакового типу з v. Фактично, розмір масивів v і w визначається типом $(r_1,...,r_s)_2$ і $(r_1,...,r_s)_3$ для β,γ в $H(P_\infty)$ підгрупах. Таким чином, вони обидва повинні бути перетворені в елементи груп. Розв'язок задачі знайдено для випадку, коли поле має непарну характеристику. Ця вимога залишається також для розширених груп автоморфізмів. Гомоморфізм $H(P_\infty)$ групи $Herm|F_{q^2}$ має просте представлення поля непарної характеристики. Вектори, що використовують матриці LS і RC, тепер легко транскодуються. І це дає нам координати підгрупи $H(P_\infty)$. В свою чергу це дає перевагу розміру повідомлення для запропонованої конструкції криптосистеми MST3. В рамках аналізу безпеки розглянуто різноманітні атаки на компоненти схеми шифрування. Отримані результати дають можливість стверджувати, що реалізація атак має високу складність.

Список літератури:

1. 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.
2. 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
3. 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
4. Халімов Г., Котух Є., Сергійчук Ю., Марухненко О. Аналіз складності реалізацій криптосистеми на групі Сузукі // Радіотехніка. 2018. Вип. 193. С. 75–81.
5. 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
6. 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.

7. Magliveras S. New approaches to designing public key cryptosystems using one-way functions and trap-doors in finite groups / S. Magliveras, D. Stinson, T. van Trung // Journal of Cryptology. 2002. Vol. 15. P. 285–297.

8. Lempken W. A public key cryptosystem based on non-abelian finite groups / W. Lempken, T. Van Trung, S.S. Magliveras, W. Wei // Journal of Cryptology. 2009. Vol. 22 (1). P. 62–74.

9. 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.

10.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

11.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.

12.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

13.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.

14.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.

15.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

16.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.

17.Khalimov G., Kotukh Y., Khalimova S. MST3 cryptosystem based on the automorphism group of the Hermitian function field' // IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T Proceedings, 2019, pp. 865–868.

18.Khalimov G., Kotukh Y. and Khalimova S. Encryption scheme based on the automorphism group of the Ree function field // 2020 7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS). Paris, France, 2020, pp. 1–8. doi: 10.1109/IOTSMS52051.2020.9340192.

19.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 27.05.2023

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 2-го навчального факультету Воєнної академії імені Євгенія Березняка Міністерства оборони України; м. Київ, Україна; e-mail: mars_kor@ukr.net; ORCID: https://orcsd.org/0000-0001-8049-4730