© Kotukh Y., Khalimov G. Method of encryption based on the functional field of the Hermitian group enhanced by homomorphic transformation// Ukrainian Scientific Journal of Information Security, 2023, vol. 29, issue 3, pp. 124-129. ©

DOI: 10.18372/2225-5036.29.18071

МЕТОД НАПРАВЛЕНОГО ШИФРУВАННЯ НА ОСНОВІ ФУНКЦІОНАЛЬНОГО ПОЛЯ ГРУПИ ЕРМІТА ПОСИЛЕНИЙ ГОМОМОРФНИМ ПЕРЕТВОРЕННЯМ

Євген Котух, Геннадій Халімов

Харківський Національний Університет Радіоелектроніки

КОТУХ Євген Володимирович, к.т.н.
Рік та місце народження: 1980 рік, м. Харків, Харківська Область, Україна.
Освіта: Харківський Національний Університет Радіоелектроніки, 2002 рік.
Посада: докторант кафедри Безпеки Інформаційних Технологій Харківського Національного Університету Радіоелектроніки.
Наукові інтереси: постквантова криптографія, теорія груп, квантовий криптоаналіз.
Публікації: понад 100 наукових публікацій, серед яких наукові статті, монографії, навчальні посібники, тези та матеріали доповідей на конференціях.
E-mail: yevgenkotukh@gmail.com.
Orcid ID: 0000-0003-4997-620X.

ХАЛІМОВ Геннадій Зайдулович, д.т.н., проф.
Рік та місце народження: 1956 рік, м. Горлівка, Україна.
Освіта: ХВВКУ Крилова, 1978 рік.
Посада: завідувач кафедри безпеки інформаційних технологій з 2014 року.
Наукові інтереси: теорія захисту інформації, прикладна криптографія, постквантові криптографічні системи.
Публікації: понад 150 наукових публікацій, серед яких наукові статті, монографії, навчальні посібники, тези та матеріали доповідей на конференціях.
E-mail: hennadii.khalimov@nure.ua.
Orcid ID: 0000-0002-2054-9186.

Анотація. *Проблема реалізації комерційного зразка потужного квантового комп'ютера призведе до компрометації існуючих криптографічних примітивів з асиметричної криптографії. 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. У світі тривають конкурси національного та міжнародного рівня на розробку нових постквантових стандартів для асиметричної системи шифрування, схем цифрового підпису та схем розподілу ключів. Одним з перспективних напрямів в розробці стійких до квантових атак криптосистем є використання задач, що мають високу складність вирішення в певних групах. В статті розглядається метод направленого шифрування посилений гомоморфним перетворенням для криптографічній системи на основі нерозв'язаної проблеми слова, що використовує спеціальним тип факторизації (логарифмічні підписи) в групі Ерміта. побудова криптосистеми. Обґрунтовано, що така реалізація має перевагу в секретності. Доведено, що можливо створити захищену криптосистему з груповими обчисленнями в невеликому кінцевому полі. Застосування гомоморфного шифрування до випадкових покриттів у логарифмічному підписі захищає від відомих атак на реалізації логарифмічного підпису.*

Ключові слова*: криптосистема MST3, групи Ерміта, логарифмічні підписи, гомоморфне перетворення.*

Постановка проблеми

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 [1-6].

Аналіз останніх досліджень і публікацій

Використовуючи групи перестановок, Вагнер і Магьярик [5] запропонували нерозв'язну схему, засновану на проблемі слова, для створення квантовостійких 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]. Остання версія цієї реалізації відома як MST3 [8] і базується на групі Сузукі.

У 2008 р. Магліверас [7] демонстрував істотні обмеження в застосуванні періодичного логарифмічного підпису у криптосистемі MST3. Це відкрило шлях до подальших досліджень та інновацій. Пізніше Сваба розробив вдосконалену версію цієї системи, відому як eMST3, яка включала додатковий рівень захисту через секретне гомоморфне покриття.

Цей підхід значно підвищив безпеку системи проти потенційних квантових атак. Далі, у 2018 р., Т. ван Трунг пропонував інноваційний метод в MST3, використовуючи сильний аперіодичний логарифмічний підпис для абелевих р-груп.

Це додатково зміцнило систему, зробило її ще більш стійкою до квантових загроз. Конг провів глибокий аналіз криптосистеми MST3 і зазначив, що вона може бути потенційним кандидатом для застосування в постквантовому періоді. Цей аналіз відкрив нові горизонти для дослідження та розвитку в області квантової криптографії.

Основний принцип побудови криптосистеми MST3 базується на групі Сузукі, що давала їй унікальні переваги. 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 [13, 16] першими запропонували трьохпараметричну групу автоморфізмів над функціональним полем Ерміта для створення квантово-стійкої криптосистеми. 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.

Мета та постановка завдання

У статті представлена новітня безпечна схема шифрування, заснована на групі автоморфізму функціонального поля Ерміта та гомоморфному шифруванні.

Виклад основного матеріалу дослідження

Визначення функціонального поля Ерміта, визначення групи, її розмір, порядок, структура та властивості, доступні операції в групі та автоморфізм детально описано в роботі [17].

Базова схема шифрування, заснована на групі автоморфізмів функціонального поля Ерміта, представлена в [16]. Розглянемо наступну схему шифрування.

Нехай $H(P_\infty)$ велика група $Herm\left|F_{q^2}\right.$ з непарною характеристикою:

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

Вибираємо прості логарифмічні підписи: $\beta_{(1)}=\left[B_{1(1)},...,B_{s(1)}\right]=\left(b_{ij}\right)_{(1)}=S\left(1,b_{ij(1)},b_{ij(1)}^{q+1}/2\right)$ та $\beta_{(2)}=\left[B_{1(2)},...,B_{s(2)}\right]=\left(b_{ij}\right)_{(2)}=S\left(1,0,b_{ij(2)}\right)$ тип $\left(r_{1(k)},...,r_{s(k)}\right)$, $i=\overline{1,s(k)}$, $j=\overline{1,r_{i(k)}}$, $k=1,2$ $b_{ij(1)}\in F_{q^2}$, $b_{ij(2)}\in F_q\subset F_{q^2}$.

Вибираємо випадкові покриття:

$$a_{(1)}=\left[A_{1(1)},...,A_{s(1)}\right]=\left(\alpha_{ij}\right)_{(1)}=S\left(a_{ij(1)_1},a_{ij(1)_2},\left(a_{ij(1)_2}\right)^{q+1}/2\right);$$

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

того ж типу, що й $b_{(1)}$, $b_{(2)}$ де $a_{ij}\in H(P_\infty)$.

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

Побудуємо гомоморфізм f_1, що визначається $f_1\left(S\left(a_1,a_2,a_2^{q+1}/2\right)\right)=S\left(1,a_2,a_2^{q+1}/2\right)$. Обчислимо $g_{(1)}=\left[g_{1(1)},...,g_{s(1)}\right]=\tau_{(i-1)(1)}^{-1}f_1\left(\left(w_{ij}\right)_{(1)}\right)\left(v_{ij}\right)_{(1)}\tau_{i(1)}$, $i=\overline{1,s(1)}$, $j=\overline{1,r_{i(1)}}$.

Побудуємо гомоморфізм $f_2\left(S\left(a_1,a_2,a_2^{q+1}/2\right)\right)=S\left(1,0,a_2\right)$.

Обчислимо $g_{(2)}=\left[g_{1(2)},...,g_{s(2)}\right]=\tau_{(i-1)(2)}^{-1}f_2\left(\left(a_{ij}\right)_{(2)}\right)\left(b_{ij}\right)_{(2)}\tau_{i(2)}$, $i=\overline{1,s(2)}$, $j=\overline{1,r_{i(2)}}$.

Отримали відкритий $\left[f_1,f_2,(a_l,g_l)\right]$ та закритий $\left[b_{(l)},\left(\tau_{0(l)},...,\tau_{s(l)}\right)\right]$, $l=\overline{1,2}$ ключі.

Зашифруємо. Беремо $x=S\left(x_1,x_2,x_3\right)$ як відкрите повідомлення, $x\in H(P_\infty)$. Вибираємо $Q=(Q_1,Q_2)$, $Q_1\in Z_{\left|F_{q^2}\right|}$, $Q_2\in Z_{|\mathbb{Z}|}$.

Обчислимо: $y_1=a'(Q)\cdot x=a_1'(Q_1)\cdot a_2'(Q_2)\cdot x,$

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

Перехресні розрахунки $\tau_{0(l)}, ..., \tau_{s(l)}$ використовуються для визначених $(*)$ компонентів. Вона використовується для додавання третьої координати до добутку $a_{(1)_1}(Q_1) + b_{(1)}(Q_1)$. Обчислимо: $y_3 = f_1(a_1'(Q_1)) = S(1, a_{(1)_2}(Q_1), *)$, $y_4 = f_2(a_2'(Q_2)) = S(1, 0, a_{(2)_2}(Q_2))$.

Ми отримали вектори (y_1, y_2, y_3, y_4) повідомлення x. Щоб розшифрувати повідомлення x, нам потрібно відновити випадкові числа $Q = (Q_1, Q_2)$.

Обчислимо $D^{(1)}(Q_1, Q_2) = \tau_{0(1)} y_2 \tau_{s(2)}^{-1} = S(1, a_{(1)_1}(Q_1) + b_{(1)}(Q_1), a_{(2)_2}(Q_2) + b_{(2)}(Q_2) + *)$, $D^*(Q) = y_3^{-1}$ $D^{(1)}(Q_1, Q_2) = S(1, b_{(1)}(Q_1), a_{(2)_2}(Q_2) + b_{(2)}(Q_2))$.

Відновимо Q_1 з $b_{(1)}(Q_1)$ за допомогою $b_{(1)}(Q_1)^{-1}$, оскільки β – просте. Для подальших обчислень необхідно видалити компоненти масивів $\gamma_1'(Q_1)$ із зашифрованого тексту y_2. Обчислимо: $y_2^{(1)} = \gamma_1'(Q_1)^{-1}$ $y_2 = S(*, *, a_{(2)_2}(Q_2) + b_{(2)}(Q_2) + *)$, $D^{(2)}(Q_2) = \tau_{0(2)} y_2^{(1)}$ $\tau_{s(2)}^{-1} = S(1, 0, a_{(2)_2}(Q_2) + b_{(2)}(Q_2))$, $D^*(Q) = D^{(2)}(Q_2) y_4^{-1} = S(1, 0, b_{(2)}(Q_2))$.

Відновимо Q_2 з $b_{(2)}(Q_2)$ за допомогою $b_{(2)}(Q_2)^{-1}$. Отримуємо відновлення $Q = (Q_1, Q_2)$ та повідомлення x від y_1. Коректність такої реалізації показано в [16]. Розглянуте шифрування має кілька істотних недоліків.

В алгоритмі шифрування ключі $Q = (Q_1, Q_2)$ слабко пов'язані та дозволяють атакувати, реалізуючи атаку послідовного відновлення ключа. Відновлення ключа Q_1 через атаку грубої сили може бути виконано на основі обчислення $\alpha_1'(Q_1')$ з подальшим порівнянням y_3 значення в координаті, $a_{(1)_2}(Q_1)$ оскільки $y_3 = f_1(a_1'(Q_1)) = S(1, a_{(1)_2}(Q_1), *)$. Пошук і знаходження Q_1' не залежать від значення Q_2. Відновлення ключа Q_2 можливе шляхом обчислення $\alpha_2'(Q_2')$ та порівняння в межах координати $a_{(2)_2}(Q_2)$, $y_4 = f_2(a_2'(Q_2)) = S(1, 0, a_{(2)_2}(Q_2))$. У цьому випадку складність атаки на ключі дорівнює $q^2 + q$.

Запропонований метод

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

Розглянемо основні етапи шифрування запропонованої схеми. Фіксуємо велику групу $H(P_\infty)$ з $Herm|F_{q^2}$. Групова операція визначається як $S(a_1, b_1, c_1) \cdot S(a_2, b_2, c_2) = S(a_1 a_2, a_2 b_1 + b_2, a_2^{q+1} c_1 + a_2 b_2^q b_1 + c_2)$.

Тотожність дорівнює $[1,0,0]$, а обернена $[\alpha, \beta, \gamma]$ дорівнює $S(a,b,c)^{-1} = S(a^{-1}, -a^{-1}b, a^{-(q+1)}c^q)$.

$H(P_\infty)$ можна представити простіше через характеристику вимкнення:

$$H(P_\infty)\left\{\left[a, b, \frac{b^{q+1}}{2} + c\right] \middle| a \in F_{q^2}^*, b \in F_{q^2} \quad and \quad c^q + c = 0\right\}.$$

Покажемо, якщо породжуючим елементом поля є γ, тоді рівняння $c^q + c = 0$ має рішення $c_i = \gamma^{(q+1)/2 + i(q+1)}$, $i = \overline{0, q-1}$. Згенеруємо ключі. Як і в попередній схемі шифрування, ми створюємо прості логарифмічні підписи $\beta_{(k)}$ та випадкові покриття $a_{(k)} = [A_{1(k)}, ..., A_{s(k)}] = S(a_{ij(k)_1}, a_{ij(k)_2}, (a_{ij(k)_2})^{q+1}/2 + a_{ij(k)_3})$ і $w_{(k)} = [W_{1(k)}, ..., W_{s(k)}] = S(1, w_{ij(k)_2}, (w_{ij(k)_2})^{q+1}/2 + w_{ij(k)_3})$ того ж типу, що й $b_{(k)}$, де $a_{ij} \in H(P_\infty)$, $w_{ij} \in H(P_\infty)$, $i = \overline{0, s(k)}$, $j = \overline{1, r_{i(k)}}$, $k = 1, 2$.

Давайте згенеруємо випадкові $t_{0(k)}, ..., t_{s(k)} \in H(P_\infty) \setminus Z$, $t_{i(k)} = S(t_{i(k)_1}, t_{i(l)_2}, (t_{i(k)_2})^{q+1}/2 + t_{i(k)_3})$, $t_{ij(k)} \in F_{q^2}^{\times}$, $i = \overline{0, s(k)}$, $k = 1, 2$.

Вибираємо $\tau_{0(l)}, \tau_{1(l)}, ..., \tau_{s(l)} \in H(P_\infty) \setminus Z$, $\tau_{i(k)} = S(\tau_{i(k)_1}, \tau_{i(k)_2}, (\tau_{i(k)_2})^{q+1}/2 + \tau_{i(k)_3})$, $\tau_{i(l)_k} \in F_{q^2}^{\times}$, $i = \overline{0, s(k)}$, $k = 1, 2$. Запропонуємо $t_{s(k-1)} = t_{0(k)}$, $\tau_{s(k-1)} = \tau_{0(k)}$, $k = 1, 2$.

Визначимо додаткову групову операцію:

$$S(a_1, b_1, c_1) \cdot S(a_2, b_2, c_2) = S(a_1 a_2, a_2 b_1 + b_2, a_2^{q+1} c_1 + c_2)$$

Інверсією є $\bar{S}(a,b,c)^{-1} = S(a^{-1}, -a^{-1}b, -a^{-(q_0+1)}c)$.

Нехай $f(e)$ – гомоморфне криптографічне перетворення щодо додавання $f(a+b) = f(a) + f(b)$ $e, a, b \in F_q$ і відповідне обернене перетворення $\hat{f}(e) = e$.

Обчислюємо покриття логарифмічних підписів $h_{(1)} = [h_{1(1)}, ..., h_{s(1)}] = t_{(i-1)(1)}^{-1} \cdot (w_{ij})_{(1)} \cdot (b_{ij})_{(1)} \cdot t_{i(1)}$, $h_{(2)} = [h_{1(2)}, ..., h_{s(2)}] = \bar{t}_{(i-1)(2)}^{-1} \circ (w_{ij})_{(2)} \circ (b_{ij})_{(2)} \circ t_{i(2)}$, покриття гомоморфного криптографічного перетворення:

$g_{(1)} = \left[g_{1(1)}, ..., g_{s(1)} \right] = \tau^{-1}_{(i-1)(1)} \cdot f\left(w_{ij}\right)_{(1)} \cdot \tau_{i(1)}$, $g_{(2)} =$, $\left[g_{1(2)}, ..., g_{s(2)} \right] = \overline{\tau}^{-1}_{(i-1)(2)} \circ f\left(w_{ij}\right)_{(2)} \circ \tau_{i(2)}$, де $f\left(w_{ij}\right) =$, $S\left(1, f(w_{ij(k)_2}), f\left(\left(w_{ij(k)_2}\right)^{q+1}/2\right) + f\left(w_{ij(k)_3}\right)\right)$, $i = \overline{1, s(\mathrm{k})}$, $j = \overline{1, r_{i(\mathrm{k})}}$, $k = 1,2$.

Нехай $\hat{f}\left(w_{ij}\right)$ є оберненим перетворенням відносно $f\left(w_{ij}\right)$.

Отримали відкритий (a_k, h_k, g_k) і закритий $\left[f, \beta_{(k)}, t_{i(k)}, \tau_{i(k)} \right]$, $i = \overline{0, s(\mathrm{k})}$, $k = 1,2$ ключі.

На кроці шифрування використаємо повідомлення $x \in H\left(P_\infty\right)$, $x = S\left(x_1, x_2, x_3\right)$ та відкритий ключ (a_k, h_k, g_k),. $k = 1,2$. Обираємо $Q = (Q_1, Q_2)$, $Q_1 \in Z_{\left|F_{q^2}\right|}$, $Q_2 \in Z_{|\mathbb{Z}|}$.

Обчислюємо зашифрований текст y_1, y_2, y_3: $y_1 = a'(Q) \cdot x = a_1'(Q_1) \cdot a_2'(Q_2) \cdot x$, $y_2 = h'(Q) = h_1'(Q_1) \cdot h_2'(Q_2) = S\left(*, \sum_{i=1, j=Q_{i(1)}}^{s(1)} \left(w_{ij(1)_2} + \beta_{ij(1)}\right) + *, \sum_{i=1, j=Q_{i(2)}}^{s(2)} \left(w_{ij(2)_3} + \beta_{ij(2)}\right) + *\right)$, тут $(*)$ компоненти визначаються перехресними обчисленнями в груповій операції добутку $t_{0(k)}, ..., t_{s(k)}$ та добутку $w_{(k)}\left(Q_k\right), \beta_{(k)}\left(Q_k\right)$; $y_3 = g'(Q) = g_1'(Q_1) \cdot g_2'(Q_2) = S\left(*, \sum_{k=1}^{2} \sum_{i=1, j=Q_{i(k)}}^{s(k)} w_{ij(k)_2} + *, \sum_{k=1}^{2} \sum_{i=1, j=Q_{i(k)}}^{s(k)} w_{ij(k)_3} + *\right)$, тут $(*)$ компоненти визначаються перехресними обчисленнями в груповій операції добутку $\tau_{0(k)}, ..., \tau_{s(k)}$ та добутку $w_{(k)}\left(Q_k\right)$.

Отримали зашифрований текст $\left(y_1, y_2, y_3\right)$ повідомлення x.

Для дешифрування беремо зашифрований текст $\left(y_1, y_2, y_3\right)$ та закритий ключ $\left[f, \beta_{(k)}, t_{i(k)}, \tau_{i(k)} \right]$, $i = \overline{0, s(\mathrm{k})}$, $k = 1,2$. Щоб розшифрувати повідомлення x, нам потрібно відновити випадкові числа $Q = (Q_1, Q_2)$.

Обчислимо $D(Q) = t_{0(1)} y_2 \circ \overline{t}^{-1}_{s(3)}$, $G(Q) = \tau_{0(1)} y_3 \circ \overline{\tau}^{-1}_{s(3)}$, $D(Q)' = D(Q) \cdot \hat{f}\left(G(Q)\right)^{-1} = S(1, \sum_{i=1, j=R_{i(1)}}^{s(1)} \beta_{ij(1)}, *)$.

Відновимо Q_1 з $\beta_{(1)}\left(Q_1\right) = \sum_{i=1, j=Q_{i(1)}}^{s(1)} \beta_{ij(1)}$ використовуючи $\beta_{(1)}\left(Q_1\right)^{-1}$, тому що $\beta_{(1)}$ – просте.

Для подальшого розрахунку необхідно видалити компонент $h_1'\left(Q_1\right)$ з y_2 і $g_1'\left(Q_1\right)$ з y_3.

Обчислимо: $y_2^{(1)} = h_1'\left(Q_1\right)^{-1} \cdot y_2$, $y_3^{(1)} = g_1'\left(Q_1\right)^{-1} \cdot y_3$, $D(Q)^{(1)} = t_{0(2)} \circ y_2^{(1)} \circ \overline{t}^{-1}_{s(3)}$, $G(Q)^{(1)} = \tau_{0(2)} \circ y_3^{(1)} \circ \overline{\tau}^{-1}_{s(3)}$, $D(Q)'' = D(Q)^{(1)} \circ \hat{f}$ $(G(Q)^{(1)})^{-1} = S(1, 0, \sum_{i=1, j=R_{i(2)}}^{s(2)} \beta_{ij(2)})$ і відновимо Q_2 з $\beta_{(2)}\left(Q_2\right) = \sum_{i=1, j=R_{i(2)}}^{s(2)} \beta_{ij(2)}$, використовуючи $\beta_{(2)}\left(Q_2\right)^{-1}$, тому що $\beta_{(2)}$ – просте.

Відновимо повідомлення $x = a'\left(Q_1', Q_2'\right)^{-1} \cdot y_1$.

Аналіз безпеки запропонованого методу

Розглянемо основні аспекти відновлення ключів методом грубої сили та атак на алгоритми.

1. *Атака грубою силою на зашифрований текст* y_1. Вибираємо $Q = (Q_1, Q_2)$, спробуємо розшифрувати текст $y_1 = a'(Q) \cdot x$. Покриття $a_{(k)}$ вибираються випадковим чином, а $a'(Q)$ визначається множенням у групі. Результуючий $a'(Q)$ вектор залежить від усіх $a_k'\left(Q_k\right)$ компонентів. Перебір усіх значень ключа $Q = (Q_1, Q_2)$ має оцінку складності q^3. Для практичної атаки x повідомлення невідоме та має невизначеність вибору q^3. Це унеможливлює атаку грубою силою на ключ через порівняння за значенням y_1. Якщо взяти модель атаки з відомим текстом, то складність атаки залишиться такою ж і дорівнює q^3.

2. *Атака грубою силою на зашифрований текст* y_2. Виберемо такі значення Q_1' і Q_2', для яких розраховане $y_2\left(Q_1', Q_2'\right)$ збігається з істинним значенням $y_2\left(Q_1, Q_2\right)$. Ключі $Q = (Q_1, Q_2)$ пов'язані, і зміна будь-якого з них призводить до зміни y_2. Атака грубою силою на ключ має складність, що дорівнює q^l.

3. *Атака грубою силою на зашифрований* текст y_3. Вибираємо значення ключів $Q = (Q_1, Q_2)$, обчислюємо $y_3\left(Q_1', Q_2'\right)$ і порівнюємо їх з потрібними $y_3\left(Q_1, Q_2\right)$. Значення y_3 для всіх координат залежить від значень $w_{ij(k)_2}$, $w_{ij(k)_3}$ векторів масивів, $W_{1(k)}, ..., W_{s(k)}$ вибраних ключем. Отже, ключі Q_1, Q_2 пов'язані, і зміна будь-якого з них призводить до зміни y_3. Таким чином, атака грубою силою на ключ має складність, що дорівнює q^l.

4. *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 $|A_1(n,\theta)| = q^5$, і в такому випадку складність атаки методом грубої сили на $(t_{0(k)},...,t_{s(k)})$ і $(\tau_{0(k)},\tau_{1(k)},...,\tau_{s(k)})$ дорівнюватиме q^5.

5. Атака на алгоритм. Атака на алгоритм шифрування, заснований на групі автоморфізмів функціонального поля Ерміта, залучає різноманітні стратегії, оскільки криптосистема має свої унікальні властивості. Основні аспекти такої атаки включають:

- особливості логарифмічних підписів та випадкових покриттів: Ці елементи є критичними для безпеки системи. Практичні атаки зазвичай спрямовані на виявлення слабкостей у цих компонентах;

- атаки на основі відомих текстів і випадкових покриттів; криптоаналітик намагається використати відомі тексти та випадкові покриття для виявлення шаблонів або слабкостей, що дозволяють розшифрувати повідомлення;

- секретність випадкових покриттів у гомоморфній криптосистемі; у системах з гомоморфним шифруванням випадкові покриття є ключовим секретом. Їх складність і випадковість захищають від атак, які базуються на слабкостях логарифмічних підписів.

З огляду на ці фактори, запропонована криптосистема з гомоморфним шифруванням є стійкою до методів криптоаналізу, що залежать від слабкостей логарифмічних підписів. Вона вимагає нових підходів для аналізу та потенційного злому, а також може вимагати значних обчислювальних ресурсів для ефективної атаки.

Висновки. Криптосистема MST3, заснована на групі автоморфізму функціонального поля Ерміта, має перевагу над іншими реалізаціями в секретності. Ми можемо створити захищену криптосистему з груповими обчисленнями в невеликому кінцевому полі. Застосування гомоморфного шифрування до випадкових покриттів у логарифмічному підписі захищає 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]. 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.

[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".

[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.

[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. pp. 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). pp. 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.

[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.

[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. pp. 33-37.

[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.

[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. pp. 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.

[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.

[17]. Kotukh Y., Khalimov G., Korobchinskyi M. Construction of a three-parameter encryption scheme on Hermitian groups in the MST3 cryptosystem // Radiotekhnika. 2023. pp. 49-55.

[18]. 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.

[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.

УДК 621.391:519.2

Kotukh Y., Khalimov G. Method of encryption based on the functional field of the Hermitian group enhanced by homomorphic transformation

Abstract. *The challenge of implementing a commercial model for a powerful quantum computer is poised to compromise existing cryptographic primitives within asymmetric cryptography. Shor's quantum algorithm, capable of solving integer factorization and discrete logarithms, threatens the security of cryptosystems like RSA and ECC. Globally, national and international competitions are underway to develop new post-quantum standards for asymmetric encryption systems, digital signature schemes, and key distribution methods. A promising direction in developing cryptosystems resistant to quantum attacks involves utilizing problems that are highly complex to solve in certain groups. This article explores the method of directional encryption, enhanced by homomorphic transformation, within a cryptographic system based on an unsolved word problem. This system employs a special type of factorization known as logarithmic signatures within the Hermitian group. We substantiate that this implementation offers enhanced secrecy and demonstrate the feasibility of creating a secure cryptosystem using group computations in a small finite field. Furthermore, the application of homomorphic encryption to random coverages in a logarithmic signature provides protection against known attacks targeting logarithmic signature implementations.*

Keywords*: MST3 cryptosystem, Hermitian group, logarithmic signatures, homomorphic transformation.*

Котух Євген Володимирович, докторант кафедри безпеки інформаційних технологій Харківського Національного Університету Радіоелектроніки.
Yevgen Kotukh, PhD, post-doc student of the Department of the Security of Information Technologies of the Kharkiv National University of Radioelectronics.

Халімов Генадій Зайдулович, доктор технічних наук, професор, завідувач кафедри безпеки інформаційних технологій Харківського Національного Університету Радіоелектроніки.
Hennadii Khalimov, Dc.S, Professor, Head of the Department of the Security of Information Technologies of the Kharkiv National University of Radioelectronics.

Отримано *27 вересня 2023 року*, затверджено редколегією *30 жовтня 2023 року*