КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (22), 2023
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2023.22.1930
УДК 621.391:519.2

Котух Євген Володимирович
кандидат технічних наук, доцент, професор кафедри кібербезпеки
Національний Технічний Університет «Дніпровська політехніка», Дніпро, Україна
ORCID 0000-0003-4997-620X
yevgenkotukh@gmail.com

Халімов Геннадій Зайдулович
доктор технічних наук, професор, завідувач кафедри безпеки інформаційних технологій
Харківський національний університет радіоелектроніки; Харків, Україна
ORCID 0000-0002-2054-9186
hennadii.khalimov@nure.ua

Коробчинський Максим Володимирович
доктор технічних наук, професор, начальник 2-ї кафедри 2-го навчального факультету
Воєнна академія імені Євгенія Березняка Міністерства оборони України, Київ, Україна
ORCID ID: 0000-0001-8049-4730
mars_kor@ukr.net

ПОБУДОВА ПОКРАЩЕНОЇ СХЕМИ ШИФРУВАННЯ НА УЗАГАЛЬНЕНИХ СУЗУКІ 2-ГРУПАХ В КРИПТОСИСТЕМІ MST3

Анотація. У статті запропоновано метод побудови покращеної схеми шифрування на узагальнених Сузукі 2-групах криптосистемі MST3, що покращує параметри безпеки оригінального підходу. Проблема вдосконалення існуючих підходів до побудови криптосистем зумовлена успіхами у створенні квантового комп'ютера з достатньою обчислювальною потужністю, щоб зробити багато криптосистем із відкритим ключем незахищеними. Зокрема, мова йде про криптосистеми, засновані на складності факторизації або проблеми дискретного логарифмування, такі як RSA, ECC тощо. Існує кілька пропозицій, які стали класичними за останні майже 20 років щодо використання некомутативних груп для створювати квантово стійкі криптосистеми. Нерозв'язна проблема слова є цікавою сферою дослідження для побудови криптосистем. Вона була сформульована Вагнером і Магьяриком і лежить у площині застосування груп перестановок. Логарифмічні підписи були запропоновані Магліверасом. У цьому контексті логарифмічний підпис є особливим типом факторизації, вона застосовується до скінченних груп. Остання версія цієї реалізації відома як MST3 і базується на групі Сузукі.
У 2008 році Magliveras продемонстрував транзитивний ліміт LS для криптосистеми MST3. Пізніше Сваба запропонував криптосистему eMST3 із покращеними параметрами захисту. Для цього вдосконалення було додано секретне гомоморфне покриття. Потім, у 2018 році, Т. ван Трунг запропонував підхід MST3 з використанням сильних аперіодичних логарифмічних підписів для абелевих р-груп. Конг і його колеги провели широкий аналіз MST3 і відзначили, що оскільки наразі немає публікацій про квантову вразливість алгоритму, його можна вважати кандидатом для використання в постквантову еру.
Перша реалізація криптосистеми на узагальненій 2-групі Сузукі не забезпечує шифрування всієї 2-групи Сузукі та захисту від атак з послідовним відновленням ключа методом грубої сили. Подальші роботи розвивали ідею публічної криптографії з використанням неабелевих вдосконалення параметрів. У статті пропонується метод побудови схеми шифрування на Сузукі 2-групах, що вдосконалює параметри безпеки існуючої криптосистеми MST3, вирішуючи проблеми з безпекою.

Ключові слова: логарифмічний підпис; покриття; криптосистема MST3, узагальнені Сузукі-2 групи; схема шифрування.

ISSN 2663 - 4023

ВСТУП

Завдання вдосконалення існуючих підходів до побудови криптосистем зумовлено практичними досягненнями у створенні квантових комп'ютерів і, як наслідок, реальна загроза використання квантових алгоритмів для злому сучасних криптосистем, що в свою чергу стимулює дослідження в області розробки криптосистем з відкритим ключем, заснованих на складних для вирішення проблемах, відмінних від класичних, що використовують факторизацію цілих або проблему дискретних логарифмів. У 2000-х роках було розглянуто та запропоновано десятки криптосистем з різних складних проблем теорії груп [1] – [4].

Постановка проблеми. Одним з перспективних напрямів досліджень асиметричних криптосистем є нерозв'язна проблема слова, що була запропонована та досліджена Магліверасом у [5] та стала основою для криптосистеми MST3, що запропонована Вагнером та Магьяриком у [6]. В [7] автори вперше запропонували використання трьохпараметричної групи автоморфізму. Вона застосована для вдосконалення параметрів безпеки криптосистеми MST3. Основна ідея таких криптосистем лежить у площині оптимізації накладних витрат. Цього можна досягти шляхом зменшення довжини ключів і прискорення алгоритмів шифрування та дешифрування. Показано, що криптосистеми з логарифмічними підписами по всій групі можуть бути побудовані на групах великих порядків над малими кінцевими полями. Узагальнена 2-група Сузукі є багатопараметричною групою. Вона має більший груповий порядок порівняно з фіксованим скінченним полем визначення, і це дає перевагу порівняно з класичною групою Сузукі. Перша реалізація криптосистеми на узагальненій 2-групі Сузукі представлена в [8] і не забезпечує шифрування всієї 2-групи Сузукі та захисту від атак з послідовним відновленням ключа методом грубої сили. Подальші роботи розвивали ідею публічної криптографії з використанням неабелевих вдосконалення параметрів [9], [10].

У статті пропонується метод побудови схеми шифрування на Сузукі 2-групах, що вдосконалює параметри безпеки існуючої криптосистеми MST3, вирішуючи проблеми з безпекою.

Аналіз останніх досліджень і публікацій. Оригінальний підхід до побудови криптосистеми MST3 базується на групі Сузукі. Цією проблемою в різні роки займались Н. Вагнер, М. Маг'ярик, С. Магліверас, В. Шпильрейн, Д. Кахробай. Останні серйозні здобутки належать А. Нусс, П. Свабі, Т. Ван Трунгу, В. Лемпкену, В. Вею. Проблеми квантового криптоаналізу криптографії з використанням неабелевих груп цікавлять Й. Конга, Х. Хонга, Ж. Шао, С. Хана, Ж. Лина, С. Жао. В рамках доповідей авторів на конференції було розглянуто результати дослідницької роботи, що демонструє подальше вдосконалення MST3 [7] – [16]. 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.

Мета статті. Метою статті є висвітлення результатів дослідження з удосконалення параметрів безпеки існуючої криптосистеми MST3 за рахунок використання узагальненої Сузукі 2-групи..

ISSN 2663 - 4023

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Спеціальний тип факторизації, який називається логарифмічним підписом, застосовується до кінцевих груп. У 2008 році дослідники [11] показали обмеження використання періодичного логарифмічного підпису для криптосистеми MST3. Пізніше вчені [12] представили покращену безпеку в криптосистемі eMST3. Секретне гомоморфне покриття було представлено як покращення безпеки. Потім, у 2018 році, автори [13] запропонували використовувати сильну аперіодичний логарифмічний підпис для абелевих p-груп для конструкції MST3. Криптографи [14] провели комплексний аналіз криптосистеми MST3 і відзначили, що вона може бути використана як кандидат на постквантовий період. Група Сузукі використовується як основна ідея для побудови криптосистеми MST3.

Схема побудови криптосистема MST реалізується наступним чином. Розглянемо G як кінцеву неабелеву групу. Група має нетривіальний центр $\mathbf{z}$, тому G не розкладається над $\mathbf{z}$. Припустимо, що $\mathbf{z}$ настільки великий, що пошук $\mathbf{z}$ є обчислювально непрактичним. Якщо $\alpha=[A_1,...,A_s]$ є логарифмічним підписом, а кожен елемент $g\in G$ може бути однозначно виражений як добуток виду $g=a_1\cdot a_2\cdots a_s$, для $a_i\in A_i$. $\alpha=[A_1,...,A_s]$ то такий підпис називається простим (таким, що розкладається на множники), якщо його можна розкласти на багаточлен w шириною G.

Криптографічна гіпотеза, яка є основою для криптосистеми, полягає в тому, що якщо $\alpha=[A_1,A_2,...,A_s]:=(a_{i,j})$ — випадкова накладка на «великий» матрац S на G, то шукати макет $g=a_{1j_1}a_{2j_2}\cdots a_{sj_s}$ є обчислювально неможливим для будь-якого елемента $g\in G$ відносно α.

Узагальнені Сузукі 2-груп визначені над скінченним полем F_q, $q=2^n$, $n>0$ для натурального числа l і $a_1,a_2,...,a_l\in F$ для деякого автоморфізму θ з F як [16].

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

Для кожного елемента $A_l(n,\theta)$ може бути виражена однозначно, і звідси випливає, що $|A_l(n,\theta)|=2^{nl}$ і $A_l(n,\theta)$ визначає групу порядку 2^{nl}. Якщо $l=2$, ця група ізоморфна 2-групі Сузукі $A(n,\theta)$.

Групова операція визначається добуток

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

Елементом ідентичності є $S(0_1,0,...,0)$. Оберненим елементом є

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

Група є неабелевою і має нетривіальний центр G

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

Припустимо, що θ це автоморфізм Фробеніуса $F,\theta:x\to x^2$. Для фіксованого скінченного поля порядок групи $A_l(n,\theta)$ вище, ніж звичайна Сузукі 2-група. У [13] автори представили базову схему шифрування на основі узагальненої групи Сузукі.

Нехай $A_l(n,\theta)=\left\{S(a_1,a_2,...,a_l)\,|\,a_i\in F_q\right\}$ буде велика група, $q=2^n$ з центром Z.

Обираємо логарифмічні підписи $\beta_k=\left[B_{1(k)},...,B_{s(k)}\right]=\left(b_{ij}\right)_k=S\left(0,..,b_{ij(l/2+k)},0,...\right)$ типу $\left(r_{1(k)},...,r_{s(k)}\right)$, $i=\overline{1,s}$, $j=\overline{1,r_{i(k)}}$, $b_{ij(l/2+k)}\in F_q$, $k=\overline{1,l/2}$.

Простий логарифмічний підпис визначається як біективне та факторизоване відображення $\beta_k(R)$.

Обираємо випадкове накриття $\alpha_k = \left[A_{1(k)},...,A_{s(k)}\right] = S\left(0,...,a^{(1)}_{ij(k)\cdot},0,..,a^{(2)}_{ij(l/2+k)},0,...\right)$ того ж самого типу β, де $a_{ij} \in A_l(n,\theta)$, $a^{(1)}_{ij(k)}, a^{(2)}_{ij(k)} \in F_q \setminus \{0\}$, $i = \overline{1,s}$, $j = \overline{1,r_{i(k)}}$, $k = \overline{1,l/2}$.

Обираємо $t_{0(k)},...,t_{s(k)} \in A_l(n,\theta) \setminus Z$, $t_{i(k)} = S(t_{i1(k)},...,t_{il(k)})$, $t_{ij(k)} \in F^{\times}$, $i = \overline{0,s}$, $j = \overline{1,l}$, $k = \overline{1,l/2}$. Беремо $t_{s(v)} = t_{0(v+1)}$, $v = \overline{1,l/2-1}$.

Будуємо гомоморфізм f, визначений $f\left(S(a_1,...,a_l)\right) = S(0,...,0,a'_{l/2+1} = a_1,...,a'_l = a_{l/2})$.

Обчислимо $\gamma_k = \left[h_{1(k)},...,h_{s(k)}\right] = t^{-1}_{(i-1)(k)} f\left(\left(a_{ij}\right)_k\right)\left(b_{ij}\right)_k t_{i(k)}$, $i = \overline{1,s}$, $j = \overline{1,r_i}$, $k = \overline{1,l/2}$,

де $f\left(\left(a_{ij}\right)_k\right)\left(b_{ij}\right)_k = S\left(0,...,\left(a^{(1)}_{ij}\right)_{l/2+k} + \left(b_{ij}\right)_{l/2+k},0,...\right)$.

Як результат отримаємо відкритий ключ $\left[f,(\alpha_k,\gamma_k)\right]$ і закритий ключ $\left[\beta_k,\left(t_{0(k)},...,t_{s(k)}\right)\right]$, $k = \overline{1,l/2}$.

Беремо $x = S\left(0,...,0,x_{l/2+1},...,x_l\right)$ як повідомлення $x \in G_{l/2+1}$ та відкритий ключ $\left[f,(\alpha_k,\gamma_k)\right]$, $k = \overline{1,l/2}$.

Для шифрування беремо випадковий $R = (R_1,R_2,...,R_{l/2})$ і $R_1,R_2,...,R_{l/2l} \in \square_{|F_q|}$ обчислимо

$$y_1 = \alpha'(R)\cdot x = \alpha_1'(R_1)\cdot\alpha_2'(R_2)\cdots\alpha_{l/2}'(R_{l/2})\cdot x = S\left(a^{(1)}_1(R_1), a^{(1)}_2(R_2)+*,...,a^{(1)}_{l/2}(R_{l/2})+*,\right.$$
$$\left. a^{(2)}_{l/2+1}(R_1)+x_{l/2+1}+*,...,a^{(2)}_l(R_{l/2})+x_l+*\right),$$
$$y_2 = \gamma'(R) = \gamma_1'(R_1)\cdot\gamma_2'(R_2)\cdots\gamma_{l/2}'(R_{l/2}) = S\left(*,...,a^{(1)}_{l/2+1}(R_1)+\beta_{l/2+1}(R_1)+*,...,a^{(1)}_l(R_{l/2})+\beta_l(R_{l/2})+*\right).$$

Змінні $(*)$ у формулі визначаються груповою операцією продукту.

Як результат отримаємо два вектори (y_1,y_2).

Відновимо випадкові числа $R = (R_1,R_2,...,R_{l/2})$, щоб розшифрувати повідомлення x. Параметр $a^{(1)}_1(R_1)$ відомий з y_1 як перший параметр і включений до $l/2+1$ компонента y_2, оскільки $a^{(1)}_{l/2+1}(R_1) = a^{(1)}_1(R_1)$. Обчислимо

$$D^{(1)}(R_1,R_2,...,R_{l/2}) = t_{0(1)}\cdot y_2 t^{-1}_{s(l/2)} = S\left(0,...,a^{(1)}_{l/2+1}(R_1)+\beta_{l/2+1}(R_1),...,a^{(1)}_l(R_{l/2})+\beta_l(R_{l/2})\right),$$
$$D^*(R) = D^{(1)}(R_1,R_2,...,R_{l/2})\,f(y_1) = S\left(0,...,0,\beta_{l/2+1}(R_1),a^{(1)}_{l/2+2}(R_2)+\beta_{l/2+2}(R_2)+*,...\right).$$

Давайте відновимо R_1 з $\beta_{l/2+1}(R_1)$ за допомогою $\beta_{l/2+1}(R_1)^{-1}$, тому що β - простий. Для подальших обчислень необхідно вилучити $\alpha_1'(R_1)$ з шифротексту компоненти масивів (y_1,y_2) і $\gamma_1'(R_1)$. Обчислимо

$$y^{(1)}_1 = \alpha_1'(R_1)^{-1}\cdot y_1 = \alpha_2'(R_2)\cdot\alpha_3'(R_3)\cdots\alpha_{l/2}'(R_{l/2})\cdot x = S\left(0,a^{(1)}_2(R_2),a^{(1)}_3(R_3)+*,...,a^{(1)}_{l/2}(R_{l/2})+*,...\right),$$
$$y^{(1)}_2 = \gamma_1'(R_1)^{-1}\,y_2 = \gamma_2'(R_2)\cdots\gamma_{l/2}'(R_{l/2}) = S\left(*,..,a^{(1)}_{l/2+2}(R_2)+\beta_{l/2+2}(R_2)+*,...,a^{(1)}_l(R_{l/2})+\beta_l(R_{l/2})+*\right).$$

Повторимо обчислення

$$D^{(2)}(R_2,...,R_{l/2}) = t_{0(2)}\cdot y^{(1)}_2 t^{-1}_{s(l/2)} = S\left(0,...,a^{(1)}_{l/2+2}(R_2)+\beta_{l/2+2}(R_2),...,a^{(1)}_l(R_{l/2})+\beta_l(R_{l/2})\right),$$
$$D^*(R) = D^{(2)}(R_2,...,R_{l/2})\,f\left(y^{(1)}_1\right) = S\left(0,...,0,\beta_{l/2+2}(R_2),a^{(1)}_{l/2+3}(R_3)+\beta_{l/2+3}(R_3)+*,...\right).$$

Давайте відновимо R_2 за $\beta_{l/2+2}(R_2)$ допомогою $\beta_{l/2+2}(R_2)^{-1}$.

Повторюючи ітераційні обчислення після $l/2$ кроків, отримуємо відновлення $R = (R_1,R_2,...,R_{l/2})$ та вихідне повідомлення. Коректність такої реалізації показано в [13]. Розглянуте шифрування має кілька істотних недоліків.

По-перше, в алгоритмі шифрування ключі $R = (R_1,R_2,...,R_{l/2})$ слабко пов'язані між собою і дозволяють атакувати послідовне відновлення ключа. Відновлення ключа R_1

через атаку грубої сили на основі грубої сили може бути виконано на основі обчислення $\alpha_1'(R_1')$ з подальшим порівнянням y_1 значення в координаті, $a_1^{(1)}(R_1)$ оскільки

$$y_1 = \alpha'(R')\cdot m = S\left(a_1^{(1)}(R_1), a_2^{(1)}(R_2)+*,..., a_{l/2}^{(1)}(R_{l/2})+*, a_{l/2+1}^{(2)}(R_1)+x_{l/2+1}+*,..., a_l^{(2)}(R_{l/2})+x_l+*\right)..$$

Пошук і знаходження R_1' не залежать від значення R_2. Відновлення ключа R_2 можливе шляхом обчислення $\alpha_2'(R_2')$ та порівняння в межах координати $a_2^{(1)}(R_2)$

$$y_1^{(1)} = \alpha_1'(R_1)^{-1}\cdot y_1 = \alpha_2'(R_2)\cdot\alpha_3'(R_3)\cdots\alpha_{l/2}'(R_{l/2})\cdot x = S\left(0, a_2^{(1)}(R_2), a_3^{(1)}(R_3)+*,..., a_{l/2}^{(1)}(R_{l/2})+*,\right.$$
$$\left. x_{l/2+1}+*, a_{l/2+2}^{(2)}(R_2)+x_{l/2+2}+*,..., a_l^{(2)}(R_{l/2})+x_l+*\right)$$

Продовжуючи ітераційно кроки $l/2$, усі ключі відновлюються. Складність атаки дорівнює $lq/2$. По-друге, алгоритм шифрування використовує не весь обсяг узагальнень 2-групи Сузукі, а лише центр $Z(G)$, який має $|Z| = q^{l/2}$ і визначає розмір $|x| = q^{l/2}$ повідомлення при шифруванні.

МЕТОДИКА ДОСЛІДЖЕННЯ

Пропозиція дослідження полягає в тому, щоб побудувати логарифмічний підпис для всієї узагальненої Сузукі 2-групи та реалізувати шифрування для повідомлень із областю видимості для всієї групи. Давайте розглянемо основні етапи шифрування.

На першому етапі згенеруємо ключі. Беремо велику групу $A_l(n,\theta) = \left\{S(a_1,a_2,...,a_l) \mid a_i \in F_q\right\}$, $q = 2^n$.

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

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

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

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

Обчислимо $\gamma_k = \left[h_{1(k)},...,h_{s(k)}\right] = t_{(i-1)(k)}^{-1}\left(a_{ij}\right)_k\left(b_{ij}\right)_k t_{i(k)}$, $j = \overline{1,r_{i(k)}}$, $j = \overline{1,r_{i(k)}}$, $k = \overline{1,l}$.

Як результат отримаємо відкритий (α_k,γ_k) та закритий $\left[\beta_k,\left(t_{0(k)},...,t_{s(k)}\right)\right]$, $k = \overline{1,l}$ ключі.

На другому етапі шифруємо. Згенеруємо повідомлення $x = S(x_1,...,x_l)$ та відкритий ключ (α_k,γ_k), $k = \overline{1,l}$. Обираємо випадковий $R = (R_1,...,R_l)$, $R_1,...,R_l \in \square_{|F_q|}$.

Давайте встановимо ключ шифрування через відображення $R' = \pi(R_1,...,R_l) = (R_1',...,R_l')$.

Обчислимо

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

$$y_2 = \gamma'(R) = \gamma_1'(R_1)\cdot\gamma_2'(R_2)\cdots\gamma_l'(R_l) = S\Bigg(\sum_{k=1}^{l}\sum_{i=1,\,j=R_{i(k)}}^{s(k)} a_{ij(k)}^{(1)} + \sum_{i=1,\,j=R_{i(1)}}^{s(1)} \beta_{ij(1)}, \sum_{k=1}^{l}\sum_{i=1,\,j=R_{i(k)}}^{s(k)} a_{ij(k)}^{(2)} +$$

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

$y_3 = a'(R) = a_1'(R_1)\cdot a_2'(R_2)\cdots a_l'(R_l)$.

Змінні $(*)$ у формулі визначаються груповою операцією продукту.

Як результат маємо (y_1, y_2, y_3).

На третьому етапі дешифруємо. Відновимо випадкові числа $R = (R_1, R_2, ..., R_l)$, щоб розшифрувати повідомлення x. Обчислимо

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

$$D^*(R) = D^{(1)}(R_1, ..., R_l) y_3^{-1} = S\big(\beta_1(R_1), a_2^{(2)}(R_2) + \beta_2(R_2) + *, ...\big).$$

Відновимо R_1 за $\beta_1(R_1)$ допомогою $\beta_1(R_1)^{-1}$, тому що β - простий. Далі необхідно видалити $\gamma_1'(R_1)$ з шифротексту компоненти масиву y_2.

Обчислимо $y_2^{(1)} = \gamma_1'(R_1)^{-1} y_2 = \gamma_2'(R_2)\cdots\gamma_l'(R_l) = S\big(*, a_2^{(2)}(R_2) + \beta_2(R_2) + *, ...\big)$,

$y_3^{(1)} = a_1'(R_1)^{-1} y_3 = a_2'(R_2)\cdots a_l'(R_l)$.

Повторіть обчислення $D^{(2)}(R_2, ..., R_l) = t_{0(2)}\cdot y_2^{(1)} t_{s(l)}^{-1} = S\big(0, a_2^{(2)}(R_2) + \beta_2(R_2), *...\big)$,

$D^*(R) = D^{(2)}(R_2, ..., R_{l/2})\big(y_3^{(1)}\big)^{-1} = S\big(0, \beta_2(R_2), *, ...\big)$.

Відновимо R_2 за $\beta_2(R_2)$ допомогою $\beta_2(R_2)^{-1}$.

Повторюючи ітераційні обчислення після l кроків, отримуємо $R' = \pi(R_1, R_2, ..., R_l) = (R_1', R_2', ..., R_l')$. Таким чином, отримуємо відновлення повідомлення $m = \alpha'(R_1', R_2', ..., R_l')^{-1}\cdot y_1$.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Зафіксуємо узагальнену групу Сузукі $G = A_4(n, \theta)$ над скінченним полем F_q, $q = 2^{10}$. Припустимо, що θ це автоморфізм Фробеніуса $F_q, \theta: \alpha \to \alpha^2$. 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 $a'_2 = a_2 + a_1^3$, $a'_3 = a_3 + a_2^2 a_1 + a_1^4 a'_2$.

Побудуємо прості LS $\beta_k = \big[B_{1(k)}, ..., B_{s(k)}\big] = \big(b_{ij}\big)_k = S\big(0, .., 0, b_{ij(k)}, 0, ..., 0\big)$ типу $(r_{1(k)}, ..., r_{s(k)})$, $i = \overline{1, s_{(k)}}$, $j = \overline{1, r_{i(k)}}$, $b_{ij(k)} \in F_q$, $k = \overline{1, l}$.

Маємо $l = 4$ і визначаємо логарифмічні підписи β_k, $k = \overline{1,4}$. Важливо самостійно вибирати типи $(r_{1(k)}, ..., r_{s(k)})$ і логарифмічні підписи β_k. Отже, нехай LS β_k, $k = \overline{1,4}$, $s_{(k)} = 3$ мають типи $(r_{1(1)}, r_{2(1)}, r_{3(1)}) = (2^2, 2^2, 2^3)$, $(r_{1(2)}, r_{2(2)}, r_{3(2)}) = (2^3, 2^2, 2^2)$, $(r_{1(3)}, r_{2(3)}, r_{3(3)}) = (2^2, 2^3, 2^2)$, $(r_{1(4)}, r_{2(4)}, r_{3(4)}) = (2^2, 2^2, 2^3)$. Щоб детально описати наш приклад продемонструємо детальне представлення логарифмічних підписів нижче.

ISSN 2663 - 4023

Таблиця 1

Представлення логарифмічного підпису

$\beta_k = \left[B_{1(k)},...,B_{s(k)} \right] = \left(b_{ij} \right)_k = S\left(0, b_{ij(k)}, 0, 0\right)$					
Б 1(1)	(b ij) (1)		(b ij) (1)		(b ij) (1)
0000000	0,0,0,0	0110000	0,α^{32},0,0	1011100	0,0,α^{46},0
1000000	α^0,0,0,0	1110000	0,α^{103},0,0	В 3(3)	
0100000	α^1,0,0,0	В 2(2)		0000100	0,0,α^4,0
1100000	α^{31},0,0,0	1100000	0,α^{31},0,0	0011010	0,0,α^{17},0
В 2(1)		0111000	0,α^{104},0,0	0111101	0,0,α^{24},0
0100000	α^1,0,0,0	0100100	0,α^8,0,0	1001111	0,0,α^{97},0
1010000	α^{62},0,0,0	0101100	0,α^{85},0,0	В 1(4)	
1101000	α^{15},0,0,0	В 3(2)		0000000	0,0,0,0
0011000	α^{33},0,0,0	0010100	0,α^{64},0,0	1000000	0,0,0,α^0
В 3(1)		0010010	0,α^9,0,0	0100000	0,0,0,α^1
1011000	α^{84},0,0,0	1001001	0,α^{37},0,0	1100000	0,0,0,α^{31}
1011100	α^{46},0,0,0	0110011	0,α^{29},0,0	В 2(4)	
0011010	α^{17},0,0,0	В 1(3)		0000000	0,0,0,0
1110110	α^{57},0,0,0	0000000	0,0,0,0	0110000	0,0,0,α^{32}
0011001	α^{123},0,0,0	1000000	0,0,α^0,0	1101000	0,0,0,α^{15}
0111101	α^{24},0,0,0	0100000	0,0,α^1,0	0011000	0,0,0,α^{33}
1111011	α^{75},0,0,0	1100000	0,0,α^{31},0	В 3(4)	
0111111	α^{111},0,0,0	В 2(3)		1101000	0,0,0,α^{15}
В 1(2)		1100000	0,0,α^{31},0	1011100	0,0,0,α^{46}
0000000	0,0,0,0	1010000	0,0,α^{62},0	0101010	0,0,0,α^{80}
1000000	0,α^0,0,0	1001000	0,0,α^7,0	0111110	0,0,0,α^{52}
0100000	0,α^1,0,0	0011000	0,0,α^{33},0	0110001	0,0,0,α^{61}
1100000	0,α^{31},0,0	1100100	0,0,α^{121},0	1110101	0,0,0,α^{76}
0010000	0,α^2,0,0	1010100	0,0,α^{79},0	0011011	0,0,0,α^{40}
1010000	0,α^{62},0,0	0101100	0,0,α^{85},0	0001111	0,0,0,α^{96}

Побудуємо випадкові покриття $\alpha_k = \left[A_{1(k)},...,A_{s(k)} \right] = S\left(a^{(1)}_{ij(k)\cdot}, a^{(2)}_{ij(k)\cdot}, a^{(3)}_{ij(k)}, a^{(4)}_{ij(k)} \right)$, де $a_{ij} \in A_4(n,\theta)$ для рівного типу як β_k, $a^{(v)}_{ij(k)} \in F_q \setminus \{0\}$, $i = \overline{1, s_{(k)}}$, $j = \overline{1, r_{i(k)}}$, $k = \overline{1,4}$. Ці покриття також мають представлення полів у формі, яку продемонстровано для логарифмічних підписів вище. Наступним кроком є генерація випадкових векторів $t_{0(k)}, t_{1(k)},..., t_{s(k)} \in U(q) \setminus Z$, $s = 4$ і $k = \overline{1,4}$. $t_{s(j)} = t_{0(j+1)}$. Далі, обчислимо масиви $\gamma_k = \left[h_{1(k)},..., h_{3(k)} \right] = t^{-1}_{(i-1)(k)} \left(a_{ij} \right)_k \left(b_{ij} \right)_k t_{i(k)}$, $i = \overline{1, s_{(k)}}$, $j = \overline{1, r_{i(k)}}$, $k = \overline{1,4}$. Масиви також мають представлення полів у формі, яку продемонстровано як приклад для логарифмічних підписів вище.

Вибираємо $R = (R_1, R_2, R_3, R_4) = (20, 21, 107, 108)$, $R_k \in \square_{|F_q|}$, $k = \overline{1,4}$. Отримуємо наступні розкладання R_k для кожного типу $(r_{1(k)}, r_{2(k)}, r_{3(k)})$ у формі $R_k = \left(R_{1(k)}, R_{2(k)}, R_{3(k)} \right)$, $R_1 = (0,1,1)$, $R_2 = (5,2,0)$, $R_3 = (3,2,3)$, $R_4 = (0,3,6)$. Обчислимо $\gamma_k(R_k) = h_{1(k)}\left(R_{1(k)}\right) h_{2(k)}\left(R_{2(k)}\right) h_{3(k)}\left(R_{3(k)}\right)$

$$\gamma_1(R_1) = h_{1(1)}(0) h_{2(1)}(1) h_{3(1)}(1) = S\left(\alpha^{107}, \alpha^{112}, \alpha^{56}, \alpha^{115}\right)$$
$$\gamma_2(R_2) = h_{1(2)}(5) h_{2(2)}(2) h_{3(2)}(0) = S\left(\alpha^{46}, \alpha^{120}, \alpha^{59}, \alpha^{8}\right)$$
$$\gamma_3(R_3) = h_{1(3)}(3) h_{2(3)}(2) h_{3(3)}(3) = S\left(\alpha^{20}, \alpha^{43}, \alpha^{89}, \alpha^{57}\right)$$
$$\gamma_4(R_4) = h_{1(4)}(0) h_{2(4)}(3) h_{3(4)}(6) = S\left(\alpha^{87}, \alpha^{118}, \alpha^{52}, \alpha^{74}\right)$$

Для етапу шифрування маємо такі вхідні дані : повідомлення $m \in A_4(n,\theta)$ та відкритий ключ $[f,(\alpha_k,\gamma_k)]$. $k=\overline{1,4}$. Отже, матимемо зашифрований текст (y_1,y_2,y_3) повідомлення m в якості результату обчислень.

Нехай $m=(a^{78},a^{10},a^{20},a^{21})=S(a^{78},a^{10},a^{20},a^{21})$. Виберемо випадковий $R=(R_1,R_2,R_3,R_4)=(20,21,107,108)$. Встановимо ключ шифрування через відображення

$R'=\pi(20,21,107,108)=(107,20,21,108)$. Обчислимо $y_1=\alpha'(R')\cdot m=S(\alpha^0,\alpha^{76},\alpha^{112},\alpha^{23})$,

$y_2=\gamma'(R)=\gamma_1'(R_1)\cdot\gamma_2'(R_2)\cdot\gamma_3'(R_3)\cdot\gamma_4'(R_4)=S(\alpha^{100},\alpha^{51},\alpha^{11},\alpha^{52})$,

$y_3=\alpha'(R)=S(\alpha^{52},\alpha^{14},\alpha^{86},\alpha^2)$.

Результат $y_1=(\alpha^0,\alpha^{76},\alpha^{112},\alpha^{23})$ $y_2=(\alpha^{100},\alpha^{51},\alpha^{11},\alpha^{52})$, $y_3=(\alpha^{52},\alpha^{14},\alpha^{86},\alpha^2)$.

Щоб розшифрувати повідомлення m потрібно відновити випадкові числа $R=(R_1,R_2,R_3,R_4)$. Обчислимо

$D^{(1)}(R_1,R_2,R_3,R_4)=t_{0(1)}y_2t_{s(4)}^{-1}=t_{0(1)}S(\alpha^{100},\alpha^{51},\alpha^{11},\alpha^{52})t_{3(4)}^{-1}=S(\alpha^{122},\alpha^{110},\alpha^{26},\alpha^2)$,

$D^*(R)=D^{(1)}(R_1,...,R_4)y_3^{-1}=S(\alpha^{34},\alpha^{101},\alpha^{35},\alpha^{63})$.

Отримуємо $\beta_1(R_1)=\alpha^{34}=(0001100)$. Відновимо R_1.

00|01| 100 R 1 =(*,*,1)
10|11|100 ряд 1 з B 3(1)
00|01| 100 −10|11|100=10| 10 |000 R 1 = (*,1,1)
10|10|000 ряд 1 з B 2(1)
10| 10 |000−10|10|000= 00 |00|000 R 1 =(0,1,1)
$R_1=(R_{1(1)},R_{2(1)},R_{3(1)})=(0,1,1)=20$

Як передумова для наступних кроків, потрібно видалити компоненти масивів $\gamma_1'(R_1)$, $\gamma_1'(R_2)$, $\gamma_1'(R_3)$та $\alpha_1'(R_1)$, $\alpha_2'(R_2)$, $\alpha_3'(R_3)$із зашифрованого тексту (y_2,y_3).

Щоб знайти R_2, обчислимо

$$y_2^{(1)}=\gamma_1'(R_1)^{-1}y_2=S(\alpha^{103},\alpha^{36},\alpha^{97},\alpha^{113}),$$
$$y_3^{(1)}=a_1'(R_1)^{-1}y_3=S(\alpha^{27},\alpha^{92},\alpha^{72},\alpha^{38}),$$
$$D^{(2)}(R_2,R_3,R_4)=t_{0(2)}y_2^{(1)}t_{3(4)}^{-1}=S(\alpha^{27},\alpha^6,\alpha^{47},\alpha^{65}),$$
$$D^*(R)=D^{(2)}(R_2,...,R_4)(y_3^{(1)})^{-1}=S(0,\alpha^{31},\alpha^{20},\alpha^{35}).$$

Отримуємо $\beta_2(R_2)=\alpha^{31}=(1100000)$. Відновимо R_2 так само, як для R_1.

110|00| 00 R 2 =(*,*,0)
001|01|00 ряд 0 з B 3(2)
110|00| 00 −001|01|00=111|01| 00 R 2 = (*,2,0)
010|01|00 ряд 2 з B 2(2)
111| 01 |00−010|01|00=101| 01 |00 R 2 =(5,2,0)
$R_2=(R_{1(2)},R_{2(2)},R_{3(2)})=(5,2,0)=21$.

Продовжимо обчислення

$$y_2^{(2)}=\gamma_2'(R_2)^{-1}y_2^{(1)}=S(\alpha^{85},\alpha^{29},\alpha^{44},\alpha^{77}),$$
$$y_3^{(2)}=a_2'(R_2)^{-1}y_3^{(1)}=S(\alpha^{113},\alpha^{15},\alpha^{35},\alpha^{105}),$$
$$D^{(3)}(R_3,R_4)=t_{0(3)}y_2^{(2)}t_{3(4)}^{-1}=S(\alpha^{113},\alpha^{15},\alpha^{92},\alpha^{122}),$$
$$D^*(R)=D^{(3)}(R_3,R_4)(y_3^{(2)})^{-1}=S(0,0,\alpha^{74},\alpha^0).$$

ISSN 2663 - 4023

Отримуємо $\beta_3(R_3)=\alpha^{74}=(1100111)$. Так само відновлюємо R_3.

11|001| 11 R 3 =(*,*,3)
10|011|11 ряд 3 з В 3(2)
11|001| 11 −10|011|11=01| 010 |00 R 3 = (*,2,3)
10|010|00 ряд 2 з В 2(2)
01| 010 |00−10|010|00= 11 |000|00 R 3 =(3,2,3)

$R_3=(R_{1(3)},R_{2(3)},R_{3(3)})=(3,2,3)=107$.

Обчислимо R_4

$$y_2^{(3)}=\gamma_3'(R_3)^{-1}y_2^{(2)}=S(\alpha^{87},\alpha^{118},\alpha^{52},\alpha^{74}),$$
$$y_3^{(3)}=a_3'(R_3)^{-1}y_3^{(2)}=S(\alpha^{55},\alpha^{78},\alpha^{110},\alpha^{74}),$$
$$D^{(4)}(R_4)=t_{0(4)}y_2^{(3)}t_{3(4)}^{-1}=S(\alpha^{55},\alpha^{78},\alpha^{110},\alpha^{121}),$$
$$D^*(R)=D^{(4)}(R_4)(y_3^{(3)})^{-1}=S(0,0,0,\alpha^{36}).$$

Отримуємо $\beta_4(R_4)=\alpha^{36}=(0000011)$. Відновимо R_4.

00|00| 011 R 4 =(*,*,6)
00|11|011 ряд 6 з В 3(1)
00|00| 011 −00|11|011=00| 11 |000 R 4 = (*,3,6)
00|11|000 ряд 3 з В 2(1)
00| 11 |000−00|11|000= 00 |00|000 R 4 =(0,3,6)

$R_4=(R_{1(4)},R_{2(4)},R_{3(4)})=(0,3,6)=108$.

Переставимо $R'=\pi(20,21,107,108)=(107,20,21,108)$ і відновимо $m=\alpha'(R')^{-1}\cdot y_1=S(a^{78},a^{10},a^{20},a^{21})$.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Наш підхід полягає у використанні узагальненої Сузукі 2-групи як платформи для криптосистеми MST3. Повне групове шифрування $G=A_l(n,\theta)$ з відповідними ключами $R=(R_1,...,R_l)$ покращує параметри безпеки та ускладнює атаку до q^l. Запропоноване вдосконалення також поширює логарифмічний підпис на всю узагальнену Сузукі 2-групу $A_l(n,\theta)$ $|A_l(n,\theta)|=q^l$. Запропоновано алгоритм зв'язування ключі та змінюємо алгоритм шифрування. Це вдосконалення забезпечує додатковий захист від послідовних атак відновлення. В рамках аналізу безпеки розглянуто різноманітні атаки на компоненти схеми шифрування. Отримані результати дають можливість стверджувати, що реалізація атак має високу складність.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Ko, K., et al. (2000). New public-key cryptosystem using braid groups. *Springer*, 166–183.
2 Eick, B., & Kahrobaei, D. (2004). Polycyclic groups: a new platform for cryptology? *arXiv.org*. http://arxiv.org/abs/math/0411077
3 Shpilrain, V., & Ushakov, A. (2005). Thompsons group and public key cryptography. *Applied Cryptography and Network Security, 3531,* 151–164.
4 Kahrobaei, D., Koupparis, C., & Shpilrain, V. (2013). Public key exchange using matrices over group rings. *Groups, Complexity, and Cryptology, 5(1),* 97–115.

5 Magliveras, S., (1986). A cryptosystem from logarithmic signatures of finite groups. *Proceedings of the 29th Midwest Symposium on Circuits and Systems*, 972–975.
6 Wagner, N., & Magyarik, M., (1985). A public-key cryptosystem based on the word problem. *Proc. Advances in Cryptology*, *Springer-Verlag*, 19–36.
7 Khalimov, G., et al. (2021). Towards three-parameter group encryption scheme for MST3 cryptosystem improvement. *2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4)*, 204–211. https://doi.org/10.1109/WorldS451998.2021.9514009
8 Khalimov, G., et al. (2021). Towards advance encryption based on a Generalized Suzuki 2-groups. *2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, 1–6. https://doi.org/10.1109/ICECCME52200.2021.9590932
9 Van Trung, T., (2001). New approaches to designing public key cryptosystems using one-way functions and trapdoors in finite groups. *J. Cryptol.*, 15(4), 285–297.
10 Lempken, W., et al., (2009). A public key cryptosystem based on non-abelian finite groups. *J. of Cryptology*, *22*, 62–74.
11 Magliveras, S., et al. (2008). On the security of a realization of cryptosystem MST3. *Tatra Mt Math Publ, 41*, 1–13.
12 Svaba, P., & Van Trung, T., (2010). Public key cryptosystem MST3 cryptanalysis and realization. *J. of Math.Cryptol., 4(3)*, 271–315.
13 Van Trung, T., (2018). Construction of strongly aperiodic logarithmic signatures. *J. Math. Cryptol., 12(1)*, 23–35.
14 Cong, Y., et al. (2019). A New Secure Encryption Scheme Based on Group Factorization Problem. *IEEExplore.* https://doi.org/10.1109/ACCESS.2019.2954672
15 Magliveras, S., (2002). New approaches to designing public key cryptosystems using one-way functions and trap-doors in finite groups. *J. of Cryptol., 15*, 285–297.
16 Lempken, W., (2009). A public key cryptosystem based on non-abelian finite groups. *J. of Cryptol., 22(1)*, 62–74.
17 Khalimov, G., Kotukh, Y., Khalimova, S., (2020). MST3 Cryptosystem Based on a Generalized Suzuki 2-Groups. http://ceur-ws.org/Vol-2711/paper1.pdf
18 Khalimov, G., et al. (2020). Encryption Scheme Based on the Automorphism Group of the Suzuki Function Field. *2020 IEEE PIC S&T*, 383–387. https://doi.org/10.1109/PICST51311.2020.9468089
19 Khalimov, G., et al. (2022). Encryption Scheme Based on the Generalized Suzuki 2-groups and Homomorphic Encryption. *Silicon Valley Cybersecurity Conference, 1536*, 59–76. https://doi.org/10.1007/978-3-030-96057-5_5

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (22), 2023
ISSN 2663 - 4023

Yevgen Kotukh
PhD, associate professor, professor of the cyber security department
National Technical University "Dniprovsk Polytechnic"; Dnipro, Ukraine
ORCID 0000-0003-4997-620X
yevgenkotukh@gmail.com

Hennadii Khalimov
Doctor of Science, professor, head of the Information Technology Security Department
Kharkiv National University of Radio Electronics; Kharkiv, Ukraine
ORCID 0000-0002-2054-9186
hennadii.khalimov@nure.ua

Maksym Korobchynskyi
Doctor of Science, professor, head of the 2nd department of the 2nd educational Faculty
Yevgeny Bereznyak Military Academy of the Ministry of Defense of Ukraine, Kyiv, Ukraine
ORCID 0000-0001-8049-4730
mars_kor@ukr.net

CONSTRUCTION OF AN IMPROVED ENCRYPTION SCHEME ON GENERALIZED SUZUKI 2-GROUPS IN THE MST3 CRYPTOSYSTEM

Abstract. This paper proposes a method for constructing an improved encryption scheme on generalized Suzuki 2-groups for the MST3 cryptosystem, which improves the security parameters of the original approach.

The challenge of improving existing cryptosystem design approaches is driven by advances in building quantum computers with sufficient computing power to render many public-key cryptosystems insecure. In particular, this includes cryptosystems based on the factorization problem or the discrete logarithm problem, such as RSA and ECC. There have been several proposals in the past two decades for using non-commutative groups to create quantum-resistant cryptosystems. The unsolvable word problem is a promising area of research for building cryptosystems. It was formulated by Wagner and Magyarik and lies in the realm of permutation groups. Magliveras proposed logarithmic signatures, which are a special type of factorization that applies to finite groups. The latest version of this implementation, known as MST3, is based on the Suzuki group. In 2008, Magliveras demonstrated a transitive LS limit for the MST3 cryptosystem. Later, Svaba proposed the eMST3 cryptosystem with improved security parameters, achieved by adding a secret homomorphic cover. In 2018, T. van Trung proposed an MST3 approach using strong aperiodic logarithmic signatures for abelian p-groups. Kong and his colleagues conducted an extensive analysis of MST3 and noted that, since there are currently no publications on the quantum vulnerability of the algorithm, it can be considered a candidate for use in the post-quantum era. The first implementation of the cryptosystem on the generalized Suzuki 2-group does not provide encryption of the entire Suzuki 2-group and does not protect against attacks with sequential key recovery by the brute-force method. Further work has developed the idea of public cryptography using non-Abelian refinements of parameters. This paper proposes a method for constructing an encryption scheme on Suzuki 2-groups that improves the security parameters of the existing MST3 cryptosystem and solves its security problems.

Keywords: logarithmic signature; covers; MST3 cryptosystem; generalized Suzuki-2 groups; encryption scheme.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1 Ko, K., et al. (2000). New public-key cryptosystem using braid groups. *Springer*, 166–183.
2 Eick, B., & Kahrobaei, D. (2004). Polycyclic groups: a new platform for cryptology? *arXiv.org*. http://arxiv.org/abs/math/0411077

3 Shpilrain, V., & Ushakov, A. (2005). Thompsons group and public key cryptography. *Applied Cryptography and Network Security, 3531,* 151–164.
4 Kahrobaei, D., Koupparis, C., & Shpilrain, V. (2013). Public key exchange using matrices over group rings. *Groups, Complexity, and Cryptology, 5(1),* 97–115.
5 Magliveras, S., (1986). A cryptosystem from logarithmic signatures of finite groups. *Proceedings of the 29th Midwest Symposium on Circuits and Systems,* 972–975.
6 Wagner, N., & Magyarik, M., (1985). A public-key cryptosystem based on the word problem. *Proc. Advances in Cryptology, Springer-Verlag,* 19–36.
7 Khalimov, G., et al. (2021). Towards three-parameter group encryption scheme for MST3 cryptosystem improvement. *2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4),* 204–211. https://doi.org/10.1109/WorldS451998.2021.9514009
8 Khalimov, G., et al. (2021). Towards advance encryption based on a Generalized Suzuki 2-groups. *2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME),* 1–6. https://doi.org/10.1109/ICECCME52200.2021.9590932
9 Van Trung, T., (2001). New approaches to designing public key cryptosystems using one-way functions and trapdoors in finite groups. *J. Cryptol.,* 15(4), 285–297.
10 Lempken, W., et al., (2009). A public key cryptosystem based on non-abelian finite groups. *J. of Cryptology, 22,* 62–74.
11 Magliveras, S., et al. (2008). On the security of a realization of cryptosystem MST3. *Tatra Mt Math Publ, 41,* 1–13.
12 Svaba, P., & Van Trung, T., (2010). Public key cryptosystem MST3 cryptanalysis and realization. *J. of Math.Cryptol., 4(3),* 271–315.
13 Van Trung, T., (2018). Construction of strongly aperiodic logarithmic signatures. *J. Math. Cryptol., 12(1),* 23–35.
14 Cong, Y., et al. (2019). A New Secure Encryption Scheme Based on Group Factorization Problem. *IEEExplore.* https://doi.org/10.1109/ACCESS.2019.2954672
15 Magliveras, S., (2002). New approaches to designing public key cryptosystems using one-way functions and trap-doors in finite groups. *J. of Cryptol., 15,* 285–297.
16 Lempken, W., (2009). A public key cryptosystem based on non-abelian finite groups. *J. of Cryptol., 22(1),* 62–74.
17 Khalimov, G., Kotukh, Y., Khalimova, S., (2020). MST3 Cryptosystem Based on a Generalized Suzuki 2-Groups. http://ceur-ws.org/Vol-2711/paper1.pdf
18 Khalimov, G., et al. (2020). Encryption Scheme Based on the Automorphism Group of the Suzuki Function Field. *2020 IEEE PIC S&T,* 383–387. https://doi.org/10.1109/PICST51311.2020.9468089
19 Khalimov, G., et al. (2022). Encryption Scheme Based on the Generalized Suzuki 2-groups and Homomorphic Encryption. *Silicon Valley Cybersecurity Conference, 1536,* 59–76. https://doi.org/10.1007/978-3-030-96057-5_5