Section 1. Information control systems

UDC 004.056: 004.9

ПОКРАЩЕНЕ ШИФРУВАННЯ НА ОСНОВІ НЕАБЕЛЕВИХ МАЛИХ ГРУП РІ

Dr.Sci. Є. Котух ORCID: 0000-0003-4997-620X
НТУ «Дніпровська політехника», Україна
E-mail:yevgenkotukh@gmail.com
Dr.Sci. Г. Халімов ORCID: 0000-0002-2054-9186
Харківський національний університет радіоелектроніки, Україна,
E-mail:hennadii.khalimov@nure.ua

Анотація. *У статті описано нову реалізацію схеми шифрування на основі малих груп Ree. Наша пропозиція полягає в тому, щоб використовувати невеликі групи Рі для шифрування повної групи з пов'язаними ключами та складністю атаки грубою силою. Ми поширили логарифмічний підпис на всю групу Ree і змінили алгоритм шифрування, щоб зв'язати ключі логарифмічного підпису та захистити від атаки послідовного відновлення.*

Ключові слова: *криптосистема MST, логарифмічний підпис, випадкове покриття , малі групи Рі.*

1. Постановка проблеми

Поява квантових комп'ютерів, здатних вирішувати будь-які складні проблеми, ставить під сумнів існування криптографії в тому вигляді, в якому вона є сьогодні. Класичні криптографічні протоколи з відкритим ключем, які використовують ідею складності вирішення проблеми факторизації великих чисел, стануть небезпечними. Актуальним стає впровадження криптосистем на некомутативних алгебрах груп, які на даний момент належать до класу важкорозв'язних задач для квантових обчислень.

2. Аналіз досліджень та публікацій

Некомутативна криптографія, заснована на складних для вирішення математичних задачах, була запропонована в 1980-х роках. Вагнер і Маджарик [1] запропонували концепцію криптосистеми, засновану на нерозв'язній проблемі слів у групах і напівгрупах. Біргет та ін. [2] спроектував цю ідею на криптосистему з відкритим ключем у кінцевих згенерованих групах. Швидко розвивався тип криптосистем, заснований на груповій факторизації [3-7].

У 1986 році Магліверас [5] запропонував симетричну криптосистему, засновану на факторизації в кінцевих групах перестановок, яка називається логарифмічною сигнатурою (LS). У 2009 році Lempken та ін. [4] розробили нову криптографічну систему з відкритим ключем - MST3, засновану на

випадкових покриттях і 2-групі Suzuki. У 2008 році Magliveras et al. [8] представили комплексний аналіз криптосистеми MST3 і заявили, що транзитивний логарифмічний підпис не підходить для криптосистеми MST3. У 2010 році Сваба та ін. [6] проаналізували всі опубліковані посилання на атаки на криптографію MST і створили більш безпечну криптосистему eMST3, додавши секретне гомоморфне покриття. У 2018 році ван Трунг [9] запропонував загальний метод побудови сильних аперіодичних логарифмічних сигнатур для абелевих p-груп і зробив внесок у практичне застосування криптосистем MST. Подальший розвиток криптосистем MST3 запропоновано в [10–13]. Тут вперше розглядаються реалізації на багатопараметричних групах. Основна ідея лежить у площині вирішення проблеми оптимізації накладних витрат - зменшення великого розміру ключів і підвищення ефективності алгоритму шифрування (дешифрування). Показано, що на групах великого порядку можна побудувати криптосистеми з обчисленнями логарифмічної сигнатури поза центром групи над скінченними полями малої розмірності.

Цілями статті є: реалізація алгоритму шифрування з логарифмічними підписами на основі малої групи Pi, що дозволить збільшити розмір зашифрованого тексту та зменшити вимоги до розміру логарифмічних підписів; розглянути напрями покращення характеристик безпеки запропонованої конструкції та запропонувати новий алгоритм шифрування з пов'язаними ключами; проаналізувати атаки грубої сили на відновлення ключа для криптосистеми з групами Pi.

3. Виклад основного матеріалу дослідження

Концепція побудови MST криптосистема міститься в застосуванні некоммутативної групової алгебри для покриття логарифмічного підписи. Логарифмічний підпис, як відображення задається наступним визначенням [14].

Визначення (відображення покриття (логарифмічний підпис). Нехай G буде кінцевою абстрактною групою і $\alpha = [A_1, ..., A_s]$ буде покриттям типу $(r_1, r_2, ..., r_s)$ для G з $A_i = \left[a_{i,1}, a_{i,2}, ..., a_{i,r_i} \right]$, де $m = \prod_{i=1}^{s} r_i$. Нехай $m_1 = 1$ і $m_i = \prod_{j=1}^{i-1} r_j$ для $i = 2, ..., s$. Послідовності A_i називаються блоками; вектор $(r_1, r_2, ..., r_s)$ із $r_i = |A_i|$ типом , а довжина визначена як $l(\alpha) = \sum_{i=1}^{s} r_i$. Позначимо τ канонічну біекцію

$$\tau : \square_{r_1} \times \square_{r_2} \times ... \times \square_{r_s} \to \square_m, \quad \tau(j_1, j_2, ..., j_s) = \sum_{i=1}^{s} j_i \cdot m_i .$$

Тоді сюр'єктивне (бієкційне) відображення $\alpha' : \square_m \to G$ є індукованим

$$\alpha'(x) = a_{1j_1} \cdot a_{2j_2} \cdots a_{sj_s}$$

де $(j_1, j_2, ..., j_s) = \tau^{-1}(x)$.

Нехай G кінцева неабелева група з нетривіальним центром $\mathbf{Z}$, така що G не розкладається над $\mathbf{Z}$. Припустимо, він $\mathbf{Z}$ досить великий, так що пошук закінчено $\mathbf{Z}$ є обчислювально непрактичним. У більш загальному випадку, якщо $\alpha = [A_1, ..., A_s]$ є логарифмічним підписом, то кожен елемент $g \in G \in$ може бути виражений однозначно (принаймні одним способом) як добуток форми $g = a_1 \cdot a_2 \cdots a_s$, для $a_i \in A_i$. $\alpha = [A_1, ..., A_s]$ називається простим (таким, що розкладається на множники), якщо наведену вище розкладку можна досягти в поліномі шириною w [G 1 0].

Криптографічна гіпотеза, яка є основою для криптосистеми, полягає в тому, що якщо $\alpha = [A_1, A_2, ..., A_s] := (a_{i,j})$ – випадкове покриття на «велике» відображення S на G, то знайти прообраз $g = a_{1j_1} a_{2j_2} \cdots a_{sj_s}$ для будь-якого елемента $g \in G$ відносно α є нерозв'язною проблемою.

Одна з концепцій секретності лежить у площині застосування аперіодичних логарифмічних підписів. Конструкції аперіодичних логарифмічних підписів широко представлені [9]. Дослідження та оцінки виконані в [9] є досить оптимістичними. Існують також питання до криптоаналізу MST пов'язані з груповою алгеброю. Ми тут опускаємо тонкі питання аналізу основних атак, хоча деталі часто є суттєвими.

Реалізація криптосистеми MST на малій групі Рі експлуатують ідею, що на багатопараметричній групі великого порядку можна отримати хороші характеристики реалізації та секретності. Мала група Рі визначена над кінцевим полем F_q, $q = 3^{2m+1}$ для деяких $m > 0$ і $t = 3^m$ як [15]

$$\mathrm{Re}\,\mathrm{e}(q) = \left\langle \alpha(x), \beta(x), \gamma(x), h(\lambda), I^{-} \middle| x \in F_q, \lambda \in F_q^{\times} \right\rangle.$$

Підгрупа $U(q)$ для групи $\mathrm{Re}\,\mathrm{e}(q)$ верхніх трикутних матриць має представлення

$$U(q) = \left\langle \alpha(x), \beta(x), \gamma(x) \middle| x \in F_q \right\rangle.$$

Кожен елемент $U(q)$ може бути виражений унікальним чином

$$S(a,b,c) = \alpha(a)\beta(b)\gamma(c)$$

отже $U(q) = \left\{ S(a,b,c) \middle| a,b,c \in F_q \right\}$, і з цього випливає, що $|U(q)| = q^3$. Крім того, $U(q)$ є силовською 3-підгрупою $\mathrm{Re}\,\mathrm{e}(q)$, і це показують прямі обчислення

$$S(a_1,b_1,c_1)S(a_2,b_2,c_2) = S(a_1 + a_2, b_1 + b_2 - a_1 a_2^{3t}, c_1 + c_2 - a_2 b_1 + a_1 a_2^{3t+1} - a_1^2 a_2^{3t}),$$

$$S(a,b,c)^{-1} = S(-a, -b - a^{3t+1}, -c - ab + a^{3t+2}).$$

Центр $Z(U(q))=\{S(0,0,c)|c\in F_q\}$.

Підгрупа $U(q)$ для малої групи $\mathrm{Ree}(q)$ має більший порядок $ordU(q)=q^3$ ніж порядок групи Сузукі. Групи Сузукі, які також використовуються в криптосистемах MST3, ізоморфні проективній лінійній групі $PGL(3,F_q)$, де $q=2q_0^2$, $q_0=2^n$ і має порядок q^2.

Пропозиція для схеми шифрування на основі малої групи Рі $\mathrm{Ree}(q)$ має наступне відображення [13]. Далі продемонструємо основні кроки алгоритму шифрування.

Крок 1. Генерація ключів

Вхід : велика група $U(q)=\{S(a,b,c)|a,b,c\in F_q\}$, $q=3^{2m+1}$, $m>0$, $t=3^m$.

Вихід : відкритий ключ $[\alpha,\gamma,f]$ із відповідним закритим ключем $[\beta,(t_0,...,t_s)]$.

Побудуємо два простих логарифмічних підпис:
$\beta_{(1)}=[B_{1(1)},...,B_{s(1)}]=(b_{ij})_{(1)}=S(0,b_{ij(1)},0)$, $\beta_{(2)}=[B_{1(2)},...,B_{s(2)}]=(b_{ij})_{(2)}=S(0,0,b_{ij(2)})$
типів $(r_{1(k)},...,r_{s(k)})$, $i=\overline{1,s(k)}$, $j=\overline{1,r_{i(k)}}$, $b_{ij(k)}\in F_q$, $k=1,2$ для координат b і c.
Побудуємо два випадкові накриття
$\alpha_{(1)}=[A_{1(1)},...,A_{s(1)}]=(a_{ij})_{(1)}=S(a_{ij(1)_a},a_{ij(1)_b},a_{ij(1)_c})$, $\alpha_{(2)}=[A_{1(2)},...,A_{s(2)}]=(a_{ij})_{(2)}=S(0,a_{ij(2)_b},a_{ij(2)_c})$
того самого типу, що й $\beta_{(k)}$, $k=1,2$ соответственно, $a_{ij}\in U(q)$, $a_{ij(k)_a},a_{ij(k)_b},a_{ij(k)_c}\in F_q\setminus\{0\}$.

Беремо $t_{0(k)},t_{1(k)},...,t_{s(k)}\in U\setminus Z$, $t_{i(k)}=S(t_{i(k)_a},t_{i(k)_b},t_{i(k)_c})$, $t_{i(k)_j}\in F_q/\{0\}$, $i=\overline{0,s(k)}$, $j=\overline{1,3}$, $k=\overline{1,2}$ і $t_{s(1)}=t_{0(2)}$ та обчислимо
$\gamma_{(k)}=[h_{1(k)},...,h_{s(k)}]=(h_{ij})_{(k)}=t_{(i-1)(k)}^{-1}f((a_{ij})_{(k)})(b_{ij})_{(k)}t_{i(k)}$, $i=\overline{1,s(k)}$, $j=\overline{1,r_{i(k)}}$,
де f є гомоморфізм $f(S(a,b,c))=S(0,a,b)$, $k=\overline{1,2}$.
Вихідний відкритий ключ $[f,(\alpha_k,\gamma_k)]$ і закритий ключ $[\beta_{(k)},(t_{0(k)},...,t_{s(k)})]$, $k=\overline{1,2}$.

Крок 2. Шифрування

Вхідні дані : повідомлення $m=S(0,m_2,m_3)$ та відкритий ключ $[f,(\alpha_k,\gamma_k)]$, $k=\overline{1,2}$.

Вихід : зашифрований текст (y_1,y_2,y_3) повідомлення m.

Беремо випадковий $R=(R_1,R_2)$, $R_1,R_2\in Z_{|Z|}$.
Обчислимо

$y_1 = \alpha'(R) \cdot m = \alpha_1'(R_1) \cdot \alpha_2'(R_2) \cdot m$, $y_2 = \gamma'(R) = \gamma_1'(R_1) \cdot \gamma_2'(R_2)$, $y_3 = f(\alpha_2'(R_2))$.

Вихід (y_1, y_2, y_3).

Крок 3. Дешифрування

Вхідні дані : зашифрований текст (y_1, y_2, y_3) і особистий ключ $\left[\beta_{(k)}, (t_{0(k)}, ..., t_{s(k)})\right]$, $k = \overline{1,2}$.

Вихід : повідомлення, $m \in A(P_\infty)$ що відповідає зашифрованому тексту (y_1, y_2, y_3).

Щоб розшифрувати повідомлення m, нам потрібно відновити випадкові числа $R = (R_1, R_2)$. Параметр $a_{(1)_1}(R_1)$ відомо з y_1 і він входить до складу другого компонента з y_2.

Обчислимо

$$D^{(1)}(R_1, R_2) = t_{0(1)} \cdot y_2 t_{s(2)}^{-1}, \quad D^*(R) = f(y_1)^{-1} D^{(1)}(R_1, R_2).$$

Відновимо R_1 з $\beta_{(1)}(R_1)$ використовуючи $\beta_{(1)}(R_1)^{-1}$. Заберемо $\gamma_1'(R_1)$ із y_2 $y_2^{(1)} = \gamma_1'(R_1)^{-1} y_2 = \gamma_2'(R_2)$.

Обчислимо

$$D^{(2)}(R_2) = t_{0(2)} \cdot y_2 t_{s(2)}^{-1}, \quad D^*(R) = D^{(2)}(R_2) y_3^{-1} = D^{(2)}(R_2)$$

і відновимо R_2 з $\beta_{(2)}(R_2)$ використовуючи $\beta_{(2)}(R_2)^{-1}$.

Відновимо $R = (R_1, R_2)$ та отримаємо повідомлення m від y_1 $m = \alpha'(R_1, R_2)^{-1} \cdot y_1$.

Коректність такої реалізації показано в [13]. Розглянуте шифрування має кілька суттєвих недоліків.

По-перше, в алгоритмі шифрування ключі R_1 та R_2 є слабо пов'язаними і допускають атаку послідовного відновлення ключів. Відновлення ключа R_1 через атаку грубої сили на основі перебору R_1' можна виконати на основі обчислення $\alpha_1'(R_1')$ з наступним порівнянням значення y_1 у координаті a тому що:

$$y_1 = \alpha'(R') \cdot m = S\left(a_{(1)_a}(R_1'), a_{(1)_b}(R_1') + a_{(2)_b}(R_2') + m_b, *\right).$$

Перебір та знаходження R_1' не залежить від значення R_2. Відновлення ключа R_2 можливо через обчислення $\alpha_2'(R_2')$ та порівняння з y_3 у координаті c $y_3 = f\left(\alpha_2'(R_2')\right) = S\left(0,0,a_{(2)_b}(R_2')\right)$.

У цьому випадку складність атаки на ключі $R=(R_1,R_2)$ складає $2q$. По-друге , алгоритм шифрування не використовує всю область визначення групи Рі, а тільки похідну групу $U_1(q)=\left\{S(0,b,c)\middle|b,c\in F_q\right\}$, яка має $|U_1(q)|=q^2$, що визначає розмір повідомлення під час шифрування $|m|=q^2$.

4. Новий покращений алгоритм

У новій реалізації криптосистеми ми усуваємо ці недоліки . Ми розширили логарифмічний підпис на всю групу Рі $U(q)=\left\{S(a,b,c)\middle|a,b,c\in F_q\right\}$ з $|U(q)|=q^3$ та змінили алгоритм шифрування таким чином щоб зв'язати ключі логарифмічних підписів та захистити від атаки послідовного відновлення . Наша пропозиція полягає в використанні малої групи Рі для шифрування на повній групі $U(q)=\left\{S(a,b,c)\middle|a,b,c\in F_q\right\}$ зі пов'язаними ключами $R=(R_1,R_2,R_3)$ та складністю атаки грубої сили q^3. Пропонуємо опис схеми з послідовним кровами відтворення.

Крок 1. Генерація ключів

Вхід : велика група $U(q)=\left\{S(a,b,c)\middle|a,b,c\in F_q\right\}$, $q=3^{2m+1}$, $m>0$, $t=3^m$.

Вихід : відкритий ключ $[\alpha,\gamma,f]$ із відповідним закритим ключем $[\beta,(t_0,...,t_s)]$.

Вибираємо прості логарифмічні підписи $\beta_{(k)}=\left[B_{1(k)},...,B_{s(k)}\right]=\left(b_{ij}\right)_{(k)}$, де $\left(b_{ij}\right)_{(k)}\in U(q)$ типу $\left(r_{1(k)},...,r_{s(k)}\right)$, $i=\overline{1,s(k)}$, $j=\overline{1,r_{i(k)}}$, $b_{ij(k)}\in F_q$, $k=\overline{1,3}$. Груповий елемент $\left(b_{ij}\right)_{(k)}$ має значення лише в одній координаті a, b, або c відповідно. Наприклад $\left(b_{ij}\right)_{(1)}=S\left(b_{ij(k)_a},0,0\right)$.

Вибираємо випадкові накриття $\alpha_{(k)} = \left[A_{1(k)}, ..., A_{s(k)} \right] = \left(a_{ij} \right)_{(k)} = S\left(a_{ij(k)_a}, a_{ij(k)_b}, a_{ij(k)_c} \right)$ тих самих типів, що й $\beta_{(k)}$, де $a_{ij} \in U(q)$, $a_{ij(k)_a}, a_{ij(k)_b}, a_{ij(k)_c} \in F_q \setminus \{0\}$, $i = \overline{0, s(k)}$, $j = \overline{1, r_{i(k)}}$, $k = \overline{1,3}$.

Вибираємо $t_{0(k)}, t_{1(k)}, ..., t_{s(k)} \in U \setminus Z$, $t_{i(k)} = S\left(t_{i(k)_a}, t_{i(k)_b}, t_{i(k)_c} \right)$, $t_{i(k)_a}, t_{i(k)_b}, t_{i(k)_c} \in F_q / \{0\}$, $i = \overline{0, s(k)}$, $k = \overline{1,3}$. Такі, що $t_{s(k-1)} = t_{0(k)}$, $k = \overline{1,3}$.

Побудуємо гомоморфізм, визначений наступним чином

$$f_1\left(S(a,b,c) \right) = S(0,b,c), \quad f_2\left(S(a,b,c) \right) = S(0,0,c).$$

Проведемо наступні розрахунки

$$\gamma_{(1)} = \left[h_{1(1)}, ..., h_{s(1)} \right] = \left(h_{ij} \right)_{(1)} = t^{-1}_{(i-1)(1)} \left(a_{ij} \right)_{(1)} \left(b_{ij} \right)_{(1)} t_{i(1)}, \quad i = \overline{1, s(1)}, \quad j = \overline{1, r_{i(1)}},$$

$$\gamma_{(2)} = \left[h_{1(2)}, ..., h_{s(2)} \right] = \left(h_{ij} \right)_{(2)} = t^{-1}_{(i-1)(2)} f_1\left(\left(a_{ij} \right)_{(2)} \right) \left(b_{ij} \right)_{(2)} t_{i(2)}, \quad i = \overline{1, s(2)}, \quad j = \overline{1, r_{i(2)}},$$

$$\gamma_{(3)} = \left[h_{1(3)}, ..., h_{s(3)} \right] = \left(h_{ij} \right)_{(3)} = t^{-1}_{(i-1)(3)} f_2\left(\left(a_{ij} \right)_{(3)} \right) \left(b_{ij} \right)_{(3)} t_{i(3)}, \quad i = \overline{1, s(3)}, \quad j = \overline{1, r_{i(3)}},$$

де $a_{ij(1)} b_{ij(1)} = S\left(a_{ij(1)_a}, a_{ij(1)_b}, a_{ij(1)_c} \right) S\left(b_{ij(1)_a}, 0, 0 \right) = S\left(a_{ij(1)_a} + b_{ij(1)_a}, *, * \right)$

$$f_1\left(a_{ij(2)} \right) b_{ij(2)} = S\left(0, a_{ij(2)_b}, a_{ij(2)_c} \right) S\left(0, b_{ij(2)_b}, 0 \right) = S\left(0, a_{ij(2)_b} + b_{ij(2)_b}, a_{ij(2)_c} \right),$$

$$f_2\left(a_{ij(3)} \right) b_{ij(3)} = S\left(0, 0, a_{ij(3)_c} \right) S\left(0, 0, b_{ij(3)_c} \right) = S\left(0, 0, a_{ij(3)_c} + b_{ij(3)_c} \right).$$

Вихідний відкритий ключ $\left[f_1, f_2, (\alpha_k, \gamma_k) \right]$ і закритий ключ $\left[\beta_{(k)}, \left(t_{0(k)}, ..., t_{s(k)} \right) \right]$, $k = \overline{1,3}$.

Крок 2. Шифрування

Вхідні дані : повідомлення $m \in U(q)$ та $m = S\left(m_a, m_b, m_c \right)$ відкритий ключ $\left[f_1, f_1, f_2, (\alpha_k, \gamma_k) \right]$, $k = \overline{1,3}$.

Вихід : зашифрований текст $\left(y_1, y_2, y_3 \right)$ повідомлення m.

Вибираємо випадковий $R = (R_1, R_2, R_3)$, $R_k \in Z_{|Z|}$, $k = \overline{1,3}$. Обчислимо ключ шифрування через відображення

$$R' = \pi(R_1, R_2, R_3) = (R_1', R_2', R_3')$$

Обчислимо

$$y_1 = \alpha'(R') \cdot m = \alpha_1'(R_1') \cdot \alpha_2'(R_2') \cdot \alpha_3'(R_3') \cdot m.$$

Обчислювальний компонент y_2.

$$\gamma(R) = \gamma_1'(R_1) \cdot \gamma_2'(R_2) \cdot \gamma_3'(R_3),$$

$$\gamma(R)=S\left(t_{0(1)}{}^{-1}+\sum_{i=1,\,j=R_{i(1)}}^{s(1)}\left(a_{ij(1)_a}+\beta_{ij(1)_a}\right)+t_{s(3)},\sum_{i=1,\,j=R_{i(2)}}^{s(2)}\left(a_{ij(2)_b}+\beta_{ij(2)_b}\right)+*,\sum_{i=1,\,j=R_{i(3)}}^{s(3)}\left(a_{ij(3)_c}+\beta_{ij(3)_c}\right)+*\right)$$

$$y_2=\gamma(R)\cdot f_2\left(\alpha_3'(R_3)\right)\cdot f_1\left(\alpha_3'(R_3)\right)\cdot f_1\left(\alpha_2'(R_2)\right),$$

де

$$f_1\left(\alpha_k'(R_k)\right)=\prod_{i=1,\,j=R_{i(k)}}^{s(k)}S\left(a_{ij(k)_a},0,0\right)=S\left(\sum_{i=1,\,j=R_{i(k)}}^{s(k)}a_{ij(k)_a},*,*\right),\ k=2,3$$

$$f_2\left(\alpha_k'(R_k)\right)=\prod_{i=1,\,j=R_{i(k)}}^{s(k)}S\left(0,a_{ij(k)_b},0\right)=S\left(0,\sum_{i=1,\,j=R_{i(k)}}^{s(k)}a_{ij(k)_b},0\right),\ k=3$$

$$y_2=S\left(t_{0(1)}{}^{-1}+\sum_{k=1}^{3}\sum_{i=1,\,j=R_{i(1)}}^{s(1)}a_{ij(k)_a}+\sum_{i=1,\,j=R_{i(1)}}^{s(1)}\beta_{ij(1)_a}+t_{s(3)},\sum_{i=1,\,j=R_{i(2)}}^{s(2)}\left(a_{ij(2)_b}+\beta_{ij(2)_b}\right)+\sum_{i=1,\,j=R_{i(3)}}^{s(3)}a_{ij(3)_b}+*,\right.$$

$$\left.\sum_{i=1,\,j=R_{i(3)}}^{s(3)}\left(a_{ij(3)_c}+\beta_{ij(3)_c}\right)+*\right)$$

Обчислювальний компонент y_3.

$$\lambda(R)=\alpha_1'(R_1)\cdot f_1\left(\alpha_2'(R_2)\right)\cdot f_1\left(\alpha_3'(R_3)\right),\ y_3=\lambda(R)\,f_1\left(\alpha_3'(R_3)\right)\cdot f_1\left(\alpha_2'(R_2)\right),$$

де

$$f_1\left(\alpha_k'(R_k)\right)=\prod_{i=1,\,j=R_{i(k)}}^{s(k)}S\left(0,a_{ij(k)_b},a_{ij(k)_c}\right)=S\left(0,\sum_{i=1,\,j=R_{i(k)}}^{s(k)}a_{ij(k)_b},\sum_{i=1,\,j=R_{i(k)}}^{s(k)}a_{ij(k)_c}\right)$$

для $k=2,3$ і

$$y_3=S\left(\sum_{k=1}^{3}\sum_{i=1,\,j=R_{i(k)}}^{s(k)}a_{ij(k)_a},\sum_{k=2}^{3}\sum_{i=1,\,j=R_{i(k)}}^{s(k)}a_{ij(k)_b}+*,\sum_{k=2}^{3}\sum_{i=1,\,j=R_{i(k)}}^{s(k)}a_{ij(k)_c}+*\right).$$

Вихід (y_1,y_2,y_3).

Крок 3. Дешифрування

Вхідні дані : зашифрований текст (y_1,y_2,y_3) і особистий ключ $\left[\beta_{(k)},\left(t_{0(k)},\ldots,t_{s(k)}\right)\right]$, $k=\overline{1,3}$.

Вихід : повідомлення, $m\in A(P_\infty)$ що відповідає зашифрованому тексту (y_1,y_2,y_3).

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

Обчислимо

$$D(R_1,R_2,R_3)=t_{0(1)}y_2y_3^{-1}t_{s(3)}^{-1}$$

$$D(R_1,R_2,R_3)=t_{0(1)}S\left(t_{0(1)}{}^{-1}+\sum_{k=1}^{3}\sum_{i=1,\,j=R_{i(1)}}^{s(1)}a_{ij(k)_a}+\sum_{i=1,\,j=R_{i(1)}}^{s(1)}\beta_{ij(1)_a}+t_{s(3)},*,*\right)$$

$$S\left(\sum_{k=1}^{3}\sum_{i=1,\,j=R_{i(k)}}^{s(k)}a_{ij(k)_a},\sum_{k=2}^{3}\sum_{i=1,\,j=R_{i(k)}}^{s(k)}a_{ij(k)_b}+*,\sum_{k=2}^{3}\sum_{i=1,\,j=R_{i(k)}}^{s(k)}a_{ij(k)_c}+*\right)^{-1}t_{s(3)}^{-1}=S\left(\sum_{i=1,\,j=R_{i(1)}}^{s(1)}\beta_{ij(1)_a}+t_{s(3)},*,*\right)$$

Відновимо R_1 з $\beta_{(1)}(R_1)=\sum_{i=1,\,j=R_{i(1)}}^{s(1)}\beta_{ij(1)_a}$ використовуючи $\beta_{(1)}(R_1)^{-1}$, тому що β_1 є простим . Для подальшого розрахунку необхідно видалити компонент $\gamma_1'(R_1)$ від y_2 і $\alpha_1'(R_1)$ від y_3.

Обчислимо

$$y_2^{(1)}=\gamma_1'(R_1)^{-1}y_2=\gamma_2'(R_2)\gamma_3'(R_3)\cdot f_2(\alpha_3'(R_3))\cdot f_1(\alpha_3'(R_3))\cdot f_1(\alpha_2'(R_2))=$$

$$S\left(t_{0(2)}{}^{-1}+\sum_{k=2}^{3}\sum_{i=1,\,j=R_{i(1)}}^{s(1)}a_{ij(k)_a}+t_{s(3)},\sum_{i=1,\,j=R_{i(2)}}^{s(2)}\left(a_{ij(2)_b}+\beta_{ij(2)_b}\right)+\sum_{i=1,\,j=R_{i(3)}}^{s(3)}a_{ij(3)_b}+*,\sum_{i=1,\,j=R_{i(3)}}^{s(3)}\left(a_{ij(3)_c}+\beta_{ij(3)_c}\right)+*\right).$$

і

$$y_3^{(1)}=\alpha_1'(R_1)^{-1}y_3=f_1(\alpha_2'(R_2))\cdot f_1(\alpha_3'(R_3))\,f_1(\alpha_3'(R_3))\cdot f_1(\alpha_2'(R_2))=$$

$$S\left(\sum_{k=2}^{3}\sum_{i=1,\,j=R_{i(k)}}^{s(k)}a_{ij(k)_a},\sum_{k=2}^{3}\sum_{i=1,\,j=R_{i(k)}}^{s(k)}a_{ij(k)_b}+*,\sum_{k=2}^{3}\sum_{i=1,\,j=R_{i(k)}}^{s(k)}a_{ij(k)_c}+*\right)$$

Повторимо обчислення для $D(R_2,R_3)$

$$D(R_2,R_3)=t_{0(2)}y_2^{(1)}\left(y_3^{(1)}\right)^{-1}t_{s(3)}^{-1}=t_{0(2)}\gamma_2'(R_2)\gamma_3'(R_3)\cdot f_2(\alpha_3'(R_3))\cdot f_1(\alpha_3'(R_3))\cdot f_1(\alpha_2'(R_2))$$

$$\left(f_1(\alpha_2'(R_2))\cdot f_1(\alpha_3'(R_3))\,f_1(\alpha_3'(R_3))\cdot f_1(\alpha_2'(R_2))\right)^{-1}t_{s(3)}^{-1}=$$

$$t_{0(2)}\gamma_2'(R_2)\gamma_3'(R_3)\cdot f_2(\alpha_3'(R_3))\,f_1(\alpha_3'(R_3))^{-1}\,f_1(\alpha_2'(R_2))^{-1}t_{s(3)}^{-1}=S\left(0,\sum_{i=1,\,j=R_{i(2)}}^{s(2)}\beta_{ij(2)_b},\sum_{i=1,\,j=R_{i(3)}}^{s(3)}\left(a_{ij(3)_c}+\beta_{ij(3)_c}\right)+*\right).$$

Відновимо R_2 з $\beta_{(2)}(R_2)=\sum_{i=1,\,j=R_{i(1)}}^{s(2)}\beta_{ij(1)_a}$ використовуючи $\beta_{(2)}(R_2)^{-1}$, тому що β_2 є простим .

Видалимо компонент $\gamma_2'(R_2)$ від $y_2^{(1)}$ і $f_1(\alpha_2'(R_2))$ від $y_3^{(1)}$.

$$y_2^{(2)} = \gamma_2'(R_2)^{-1} y_2^{(1)} = \gamma_3'(R_3)\cdot f_2(\alpha_3'(R_3))\cdot f_1(\alpha_3'(R_3))\cdot f_1(\alpha_2'(R_2)) =$$

$$S\left(t_{0(3)}^{-1} + \sum_{k=2}^{3}\sum_{i=1,\, j=R_{i(1)}}^{s(1)} a_{ij(k)_a} + t_{s(3)}, \sum_{i=1,\, j=R_{i(3)}}^{s(3)} a_{ij(3)_b} + *, \sum_{i=1,\, j=R_{i(3)}}^{s(3)} \left(a_{ij(3)_c} + \beta_{ij(3)_c}\right) + *\right)$$

і

$$y_3^{(2)} = f_1(\alpha_2'(R_2))^{-1} y_3^{(1)} = f_1(\alpha_3'(R_3))\, f_1(\alpha_3'(R_3))\cdot f_1(\alpha_2'(R_2)) =$$

$$S\left(\sum_{k=2}^{3}\sum_{i=1,\, j=R_{i(1)}}^{s(1)} a_{ij(k)_a}, \sum_{i=1,\, j=R_{i(3)}}^{s(3)} a_{ij(3)_b} + *, \sum_{i=1,\, j=R_{i(3)}}^{s(3)} \left(a_{ij(3)_c} + \beta_{ij(3)_c}\right) + *\right)$$

Обчислимо $D(R_3) = t_{0(3)} y_2^{(2)} \left(y_3^{(2)}\right)^{-1} t_{s(3)}^{-1}$,

$$D(R_3) = t_{0(3)} y_2^{(2)} \left(y_3^{(2)}\right)^{-1} t_{s(3)}^{-1} = t_{0(3)}\gamma_3'(R_3)\, f_2(\alpha_3'(R_3))\cdot f_1(\alpha_3'(R_3))\cdot f_1(\alpha_2'(R_2))$$

$$\left(f_1(\alpha_3'(R_3))\, f_1(\alpha_3'(R_3))\cdot f_1(\alpha_2'(R_2))\right)^{-1} t_{s(3)}^{-1} = \gamma_3'(R_3)\, f_2(\alpha_3'(R_3))\cdot f_1(\alpha_3'(R_3))^{-1} = S\left(0, 0, \sum_{i=1,\, j=R_{i(3)}}^{s(3)} \beta_{ij(3)_c}\right)$$

Відновимо R_3 з $\beta_{(3)}(R_3)$ використовуючи $\beta_{(3)}(R_3)^{-1}$.

Ми отримуємо $R' = \pi(R_1, R_2, R_3) = (R_1', R_2', R_3')$ і відновимо повідомлення m від y_1 $m = \alpha'(R_1', R_2', R_3')^{-1}\cdot y_1$.

5. Обґрунтування коректності отриманих результатів

Наступний приклад демонструє коректність отриманих виразів.

Візьмемо підгрупу $U(q) = \left\{S(a,b,c) \middle| a,b,c \in F_q\right\}$ для групи $\mathrm{Ree}(q)$ над F_q, $q = 3^5$, $g(x) = x^5 + 2x + 1$, $t = 3^2$.

Логарифмічні підписи β_k, $k = \overline{1,3}$ в групі відображень визначають $b_{ij(k)}$ координати a,b,c. Типи $\left(r_{1(k)}, \ldots, r_{s(k)}\right)$ та логарифмічні підписи β_k вибираються самостійно. Визначимо логарифмічні підписи β_k, $k = \overline{1,3}$ м, що мають типи $\left(r_{1(1)}, r_{2(1)}, r_{3(1)}, r_{4(1)}\right) = \left(3, 3, 3^2, 3\right)$, $\left(r_{1(2)}, r_{2(2)}, r_{3(2)}\right) = \left(3, 3^2, 3^2\right)$ і $\left(r_{1(3)}, r_{2(3)}, r_{3(3)}, r_{4(3)}\right) = \left(3^2, 3, 3, 3\right)$. Масив $b_{ij(k)}$ складається з підмасивів з кількістю рядків, що дорівнює $r_{i(k)}$. Ви можете

вибрати будь-яку фрагментацію масивів з умовою $\prod_{i=1}^{s} r_i = q$. У нашому випадку ми маємо $\prod_{i=1}^{s} r_i = 3^5$. Кожен рядок b_{ij} є елементом поля F_q.

Вимоги до побудови масивів логарифмічних підписів описані в [16]. Для нашого прикладу ми використовуємо конструкцію з простими логарифмічними підписами. Ми побудуємо $\beta_k = \left[B_{1(k)}, B_{2(k)}, B_{3(k)}\right]$, $k = \overline{1,3}$, які мають наступні відображення у вигляді рядків та елементів групи

Таблиця 1

$\beta_k = \left[B_{1(k)}, B_{2(k)}, B_{3(k)}\right] = \left(b_{ij}\right)_{(k)}$, $\left(b_{ij}\right)_{(k)} \in U(q)$, $k = \overline{1,3}$					
$\boldsymbol{B_{1(1)}}$	$\left(b_{ij}\right)_{(1)}$	$\boldsymbol{B_{1(2)}}$	$\left(b_{ij}\right)_{(2)}$	$\boldsymbol{B_{1(3)}}$	$\left(b_{ij}\right)_{(3)}$
00000	0,0,0	**0**0000	0,0,0	**00**000	0,0,0
10000	α^0,0,0	**1**0000	0,α^0,0	**10**000	0,0,α^0
20000	α^{121},0,0	**2**0000	0,α^{121},0	**20**000	0,0,α^{121}
$\boldsymbol{B_{2(1)}}$		$\boldsymbol{B_{2(2)}}$		**01**000	0,0,α^1
1**0**000	$\alpha^0$0,0	2**00**00	0,α^{121},0	**11**000	0,0,α^{69}
0**1**000	α^1,0,0	0**10**00	0,α^1,0	**21**000	0,0,α^5
1**2**000	α^{126},0,0	1**20**00	0,α^{126},0	**02**000	0,0,α^{122}
$\boldsymbol{B_{3(1)}}$		0**01**00	0,α^2,0	**12**000	0,0,α^{126}
10**00**0	α^0,0,0	0**11**00	0,α^{70},0	**22**000	0,0,α^{190}
10**10**0	α^{46},0,0	0**21**00	0,α^6,0	$\boldsymbol{B_{2(3)}}$	
22**20**0	α^{131}0,0	0**02**00	0,α^{123},0	10**00**0	0,0, α^0
00**01**0	α^3,0,0	2**12**00	0,α^{17},0	01**10**0	0,0,α^{70}
01**11**0	α^{11},0,0	1**22**00	0,α^{88},0	00**20**0	0,0,α^{123}
11**21**0	α^{61},0,0	$\boldsymbol{B_{3(2)}}$		$\boldsymbol{B_{3(3)}}$	
22**02**0	α^{93},0,0	022**00**	0,α^{191},0	21**20**0	0,0,α^{17}
01**12**0	α^{102},0,0	022**10**	0,α^{223},0	20**01**0	0,0,α^{15}
22**22**0	α^{236},0,0	010**20**	0,α^{196},0	11**02**0	0,0,α^{28}
$\boldsymbol{B_{4(1)}}$		020**01**	0,α^{16},0	$\boldsymbol{B_{4(3)}}$	
2012**0**	α^{233},0,0	021**11**	0,α^{217},0	0200**0**	0,0,α^{122}
2022**1**	α^{43},0,0	222**21**	0,α^{203},0	2100**1**	0,0,α^{73}
2112**2**	α^{81},0,0	200**02**	0,α^{68},0	0002**2**	0,0,α^{125}
		121**12**	0,α^{24},0		
		211**22**	0,α^{81},0		

На наступному кроці генеруємо випадкові обкладинки α_k для того самого типу, що й β_k, $k = \overline{1,3}$

$$\alpha_k = \left[A_{1(k)}, ..., A_{s(k)}\right] = \left(a_{ij}\right)_{(k)} = S\left(a_{ij(k)_a}, a_{ij(k)_b}, a_{ij(k)_c}\right),$$

де $a_{ij} \in U(q)$, $a_{ij(k)_a}, a_{ij(k)_b}, a_{ij(k)_c} \in F_q \setminus \{0\}$, $i = \overline{1, s(k)}$, $j = \overline{1, r_{i(k)}}$, $k = \overline{1,3}$.

У полі відображення $\alpha_k = S\left(a_{ij(k)_a}, a_{ij(k)_b}, a_{ij(k)_c}\right)$ має наступний вигляд

Таблиця 2

$\alpha_k = \left[A_{1(k)}, ..., A_{s(k)} \right] = S\left(a_{ij(k)_a}, a_{ij(k)_b}, a_{ij(k)_c} \right)$		
$k = 1$	$k = 2$	$k = 3$
$\boldsymbol{A}_{1(1)}$	$\boldsymbol{A}_{1(2)}$	$\boldsymbol{A}_{1(3)}$
$\alpha^{92}, \alpha^{114}, \alpha^{205}$	$\alpha^{66}, \alpha^{128}, \alpha^{44}$	$\alpha^{121}, \alpha^{3}, \alpha^{105}$
$\alpha^{172}, \alpha^{116}, \alpha^{227}$	$\alpha^{41}, \alpha^{183}, \alpha^{126}$	$\alpha^{96}, \alpha^{69}, \alpha^{39}$
$\alpha^{210}, \alpha^{111}, \alpha^{193}$	$\alpha^{12}, \alpha^{3}, \alpha^{156}$	$\alpha^{195}, \alpha^{180}, \alpha^{34}$
$\boldsymbol{A}_{2(1)}$	$\boldsymbol{A}_{2(2)}$	$\alpha^{113}, \alpha^{68}, \alpha^{109}$
$\alpha^{20}, \alpha^{91}, \alpha^{168}$	$\alpha^{75}, \alpha^{158}, \alpha^{31}$	$\alpha^{119}, \alpha^{175}, \alpha^{207}$
$\alpha^{228}, \alpha^{106}, \alpha^{39}$	$\alpha^{20}, \alpha^{238}, \alpha^{197}$	$\alpha^{189}, \alpha^{212}, \alpha^{224}$
$\alpha^{100}, \alpha^{45}, \alpha^{156}$	$\alpha^{49}, \alpha^{111}, \alpha^{27}$	$\alpha^{211}, \alpha^{171}, \alpha^{40}$
$\boldsymbol{A}_{3(1)}$	$\alpha^{176}, \alpha^{136}, \alpha^{61}$	$\alpha^{215}, \alpha^{157}, \alpha^{7}$
$\alpha^{164}, \alpha^{52}, \alpha^{207}$	$\alpha^{138}, \alpha^{21}, \alpha^{164}$	$\alpha^{230}, \alpha^{14}, \alpha^{44}$
$\alpha^{17}, \alpha^{226}, \alpha^{65}$	$\alpha^{15}, \alpha^{90}, \alpha^{2}$	$\boldsymbol{A}_{2(3)}$
$\alpha^{38}, \alpha^{65}, \alpha^{38}$	$\alpha^{154}, \alpha^{176}, \alpha^{159}$	$\alpha^{36}, \alpha^{126}, \alpha^{8}$
$\alpha^{106}, \alpha^{26}, \alpha^{12}$	$\alpha^{163}, \alpha^{172}, \alpha^{206}$	$\alpha^{167}, \alpha^{25}, \alpha^{100}$
$\alpha^{96}, \alpha^{160}, \alpha^{42}$	$\alpha^{1}, \alpha^{190}, \alpha^{184}$	$\alpha^{210}, \alpha^{11}, \alpha^{135}$
$\alpha^{241}, \alpha^{190}, \alpha^{100}$	$\boldsymbol{A}_{3(2)}$	$\boldsymbol{A}_{3(3)}$
$\alpha^{11}, \alpha^{163}, \alpha^{110}$	$\alpha^{66}, \alpha^{118}, \alpha^{179}$	$\alpha^{32}, \alpha^{142}, \alpha^{94}$
$\alpha^{110}, \alpha^{128}, \alpha^{152}$	$\alpha^{121}, \alpha^{221}, \alpha^{169}$	$\alpha^{224}, \alpha^{166}, \alpha^{43}$
$\alpha^{199}, \alpha^{134}, \alpha^{81}$	$\alpha^{63}, \alpha^{45}, \alpha^{226}$	$\alpha^{218}, \alpha^{128}, \alpha^{164}$
$\boldsymbol{A}_{4(1)}$	$\alpha^{89}, \alpha^{131}, \alpha^{209}$	$\boldsymbol{A}_{4(3)}$
$\alpha^{157}, \alpha^{39}, \alpha^{169}$	$\alpha^{191}, \alpha^{124}, \alpha^{49}$	$\alpha^{156}, \alpha^{58}, \alpha^{147}$
$\alpha^{156}, \alpha^{79}, \alpha^{102}$	$\alpha^{32}, \alpha^{204}, \alpha^{139}$	$\alpha^{153}, \alpha^{10}, \alpha^{54}$
$\alpha^{126}, \alpha^{110}, \alpha^{238}$	$\alpha^{20}, \alpha^{93}, \alpha^{48}$	$\alpha^{22}, \alpha^{8}, \alpha^{49}$
	$\alpha^{56}, \alpha^{123}, \alpha^{125}$	
	$\alpha^{34}, \alpha^{89}, \alpha^{91}$	

Вибираємо $t_{0(k)}, t_{1(k)}, ..., t_{s(k)} \in U(q) \setminus Z$ випадковим і $k = \overline{1,3}$, нехай $t_{3(j)} = t_{0(j+1)}$

Таблиця 3

$t_{0(k)}, t_{1(k)}, ..., t_{s(k)} \in U(q) \setminus Z$, $s(k)$, $k = \overline{1,3}$		
$k = 1$	$k = 2$	$k = 3$
$(\alpha^{14}, \alpha^{169}, \alpha^{59})$ $(\alpha^{14}, \alpha^{206}, \alpha^{63})$ $(\alpha^{154}, \alpha^{69}, \alpha^{38})$ $(\alpha^{53}, \alpha^{180}, \alpha^{77})$ $(\alpha^{109}, \alpha^{229}, \alpha^{106})$	$(\alpha^{109}, \alpha^{229}, \alpha^{106})$ $(\alpha^{21}, \alpha^{66}, \alpha^{44})$ $(\alpha^{43}, \alpha^{54}, \alpha^{29})$ $(\alpha^{52}, \alpha^{125}, \alpha^{228})$	$(\alpha^{52}, \alpha^{125}, \alpha^{228})$ $(\alpha^{117}, \alpha^{143}, \alpha^{78})$ $(\alpha^{159}, \alpha^{207}, \alpha^{74})$ $(\alpha^{228}, \alpha^{111}, \alpha^{225})$ $(\alpha^{196}, \alpha^{164}, \alpha^{2})$
$t_{0(k)}^{-1}, t_{1(k)}^{-1}, ..., t_{s(k)}^{-1} \in U(q) \setminus Z$, $s = 3$, $k = \overline{1,3}$		
$(\alpha^{135}, \alpha^{127}, \alpha^{19})$ $(\alpha^{135}, \alpha^{5}, \alpha^{37})$ $(\alpha^{33}, \alpha^{136}, \alpha^{61})$ $(\alpha^{174}, \alpha^{167}, \alpha^{174})$ $(\alpha^{230}, \alpha^{50}, \alpha^{150})$	$(\alpha^{230}, \alpha^{50}, \alpha^{150})$ $(\alpha^{142}, \alpha^{116}, \alpha^{34})$ $(\alpha^{164}, \alpha^{193}, \alpha^{222})$ $(\alpha^{173}, 0, \alpha^{117})$	$(\alpha^{173}, 0, \alpha^{117})$ $(\alpha^{238}, \alpha^{237}, \alpha^{118})$ $(\alpha^{38}, \alpha^{35}, \alpha^{80})$ $(\alpha^{107}, \alpha^{69}, \alpha^{37})$ $(\alpha^{75}, \alpha^{164}, \alpha^{123})$

Наступним кроком є обчислення масивів γ_k, $k=\overline{1,3}$. За умовою прикладу отримуємо

$\gamma_{(1)}=\left[h_{1(1)},...,h_{s(1)}\right]=\left(h_{ij}\right)_{(1)}=t^{-1}_{(i-1)(1)}\left(a_{ij}\right)_{(1)}\left(b_{ij}\right)_{(1)}t_{i(1)}$, $i=\overline{1,4}$, $j=\overline{1,r_{i(1)}}$,

$\gamma_{(2)}=\left[h_{1(2)},...,h_{s(2)}\right]=\left(h_{ij}\right)_{(2)}=t^{-1}_{(i-1)(2)}f_1\left(\left(a_{ij}\right)_{(2)}\right)\left(b_{ij}\right)_{(2)}t_{i(2)}$, $i=\overline{1,3}$, $j=\overline{1,r_{i(2)}}$,

$\gamma_{(3)}=\left[h_{1(3)},...,h_{s(3)}\right]=\left(h_{ij}\right)_{(3)}=t^{-1}_{(i-1)(3)}f_2\left(\left(a_{ij}\right)_{(3)}\right)\left(b_{ij}\right)_{(3)}t_{i(3)}$, $i=\overline{1,4}$, $j=\overline{1,r_{i(3)}}$.

У полі відображення $\gamma_k=S(h_{ij(k)_a},h_{ij(k)_b},h_{ij(k)_c})$, $k=\overline{1,3}$ має наступний вигляд

Таблиця 4

$\gamma_k=S(h_{ij(k)_a},h_{ij(k)_b},h_{ij(k)_c})$, $k=\overline{1,3}$		
h **1(1)**	***h*** **1(2)**	***h*** **1(3)**
α^{92}, α^{18}, α^{72}	α^{91}, α^{155}, α^{100}	α^{93}, α^{176}, α^{223}
α^{182}, α^{22}, α^{90}	α^{91}, α^{116}, α^{38}	α^{93}, α^{176}, α^{29}
α^{143}, α^{35}, α^{128}	α^{91}, α^{153}, α^{91}	α^{93}, α^{176}, α^{28}
h **2(1)**	***h*** **2(2)**	α^{93}, α^{176}, α^{38}
α^{41}, α^{130}, α^{59}	α^{110}, α^{176}, α^{219}	α^{93}, α^{176}, α^{110}
α^{35}, α^{140}, α^{49}	α^{110}, α^{48}, α^{140}	α^{93}, α^{176}, α^{127}
α^{81}, α^{205}, α^{86}	α^{110}, α^{34}, α^{61}	α^{93}, α^{176}, α^{179}
ч **3(1)**	α^{110}, α^{125}, α^{145}	α^{93}, α^{176}, α^{185}
α^{70}, α^{24}, α^{216}	α^{110}, α^{25}, α^{217}	α^{93}, α^{176}, α^{166}
α^{20}, α^{64}, α^{183}	α^{110}, α^{35}, α^{241}	***h*** **2(3)**
α^{200}, α^{162}, α^{124}	α^{110}, α^{1}, α^{11}	α^{77}, α^{86}, α^{149}
α^{80}, α^{164}, α^{140}	α^{110}, α^{27}, α^{5}	α^{77}, α^{86}, α^{52}
α^{136}, α^{118}, α^{149}	α^{110}, α^{63}, α^{137}	α^{77}, α^{86}, α^{57}
α^{191}, α^{77}, α^{5}	***h*** **3(2)**	***ч*** **3(3)**
α^{62}, α^{174}, α^{10}	α^{88}, α^{145}, α^{196}	α^{160}, α^{107}, α^{99}
α^{46}, α^{229}, α^{156}	α^{88}, α^{174}, α^{148}	α^{160}, α^{107}, α^{128}
α^{40}, α^{63}, α^{237}	α^{88}, α^{156}, α^{29}	α^{160}, α^{107}, α^{59}
h **4(1)**	α^{88}, α^{118}, α^{12}	***ч*** **3(3)**
α^{203}, α^{77}, α^{16}	α^{88}, α^{228}, α^{63}	α^{129}, α^{60}, α^{86}
α^{14}, α^{137}, α^{162}	α^{88}, α^{28}, α^{77}	α^{129}, α^{60}, α^{138}
α^{222}, α^{90}, α^{128}	α^{88}, α^{156}, α^{14}	α^{129}, α^{60}, α^{196}
	α^{88}, α^{186}, α^{41}	
	α^{88}, α^{162}, α^{190}	

Наприклад, нехай $R_1=209$. Ми отримуємо наступну базову факторизацію для заданого типу $\left(r_{1(1)},r_{2(1)},r_{3(1)},r_{4(1)}\right)=\left(3,3,3^2,3\right)$ у формі $R_1=\left(R_{1(1)},R_{2(1)},R_{3(1)},R_{4(1)}\right)=(2,0,5,2)$, де $R_{1(1)}+R_{2(1)}3+R_{3(1)}3^2+R_{4(1)}3^4=209$.

Обчислимо γ_1

$\gamma_1(209) = h_{1(1)}(2)h_{2(1)}(0)h_{3(1)}(5)h_{4(1)}(2) = S\left(\alpha^{143},\alpha^{35},\alpha^{128}\right)S\left(\alpha^{41},\alpha^{130},\alpha^{59}\right)S\left(\alpha^{191},\alpha^{77},\alpha^{5}\right)S\left(\alpha^{222},\alpha^{90},\alpha^{128}\right) = S\left(\alpha^{5},\alpha^{123},\alpha^{41}\right)$.

Виберемо $R_2 = 81$. ми отримати для а типу $\left(r_{1(2)}, r_{2(2)}, r_{3(2)}\right) = \left(3, 3^2, 3^2\right)$ наступну факторизацію

$$R_2 = \left(R_{1(2)}, R_{2(2)}, R_{3(2)}\right) = (0,0,3) = 81$$

і значення γ_2

$$\gamma_2(81) = h_{1(2)}(0)h_{2(2)}(0)h_{3(2)}(3) = S\left(\alpha^{105},\alpha^{149},\alpha^{27}\right).$$

Нехай $R_3 = 129$, ми маємо $R_3 = \left(R_{1(3)}, R_{2(3)}, R_{3(3)}, R_{4(3)}\right) = (3,2,1,1) = 129$ для типу $\left(r_{1(3)}, r_{2(3)}, r_{3(3)}, r_{4(3)}\right) = \left(3^2, 3, 3, 3\right)$ та значення γ_3

$$\gamma_3(129) = h_{1(3)}(3)h_{2(3)}(2)h_{3(3)}(1)h_{4(3)}(1) = S\left(\alpha^{94},\alpha^{222},\alpha^{30}\right).$$

Перейдем до кроків шифрування і дешифрування.

Крок 1. Шифрування

Вхідні дані : повідомлення $m \in U(q)$, $m = S\left(m_a, m_b, m_c\right)$ та відкритий ключ $\left[f_1, f_2, (\alpha_k, \gamma_k)\right]$,. $k = \overline{1,3}$

Вихід : зашифрований текст (y_1, y_2, y_3) повідомлення m.

Нехай $m = \left(a^{10}, a^{20}, a^{30}\right) = S\left(\alpha^{10}, \alpha^{20}, \alpha^{30}\right)$.

Виберемо випадковий $R = (R_1, R_2, R_3) = (209, 81, 129)$. Визначимо відображення для шифрування ключів у відео

$$R' = \pi(R_1, R_2, R_3) = (R_3, R_2, R_1) = (129, 81, 209).$$

Обчислимо зашифрований текст

Для $R_3 = 129$ ми 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 $R_1 = \left(R_{1(1)}, R_{2(1)}, R_{3(1)}, R_{4(1)}\right) = (0,1,5,1)$, де $R_1 + R_2 3 + R_3 3^2 + R_4 3^4 = 129$.

Для $R_1 = 209$ ми отримуємо наступну базову факторизацію для заданого типу $\left(r_{1(3)}, r_{2(3)}, r_{3(3)}, r_{4(3)}\right) = \left(3^2, 3, 3, 3\right)$ у формі $R_1 = \left(R_{1(1)}, R_{2(1)}, R_{3(1)}, R_{4(1)}\right) = (2,2,1,2)$, де $R_1 + R_2 3^2 + R_3 3^3 + R_4 3^4 = 209$.

Обчислимо $y_1 = \alpha'(R) \cdot m = \alpha_1'(R_3) \cdot \alpha_2'(R_2) \cdot \alpha_3'(R_1) \cdot m = S\left(\alpha^{118}, \alpha^{102}, \alpha^{224}\right)$

$\gamma(R)=\gamma_1'(R_1)\cdot\gamma_2'(R_2)\cdot\gamma_3'(R_3)=S\left(\alpha^5,\alpha^{123},\alpha^{41}\right)S\left(\alpha^{105},\alpha^{149},\alpha^{27}\right)S\left(\alpha^{94},\alpha^{222},\alpha^{30}\right)=S\left(\alpha^{138},\alpha^{113},\alpha^{45}\right)$ і другий компонент шифрованого тексту

$$y_2=\gamma(R)\cdot f_2\left(\alpha_3'(R_3)\right)\cdot f_1\left(\alpha_3'(R_3)\right)\cdot f_1\left(\alpha_2'(R_2)\right)=S\left(\alpha^{138},\alpha^{113},\alpha^{45}\right)S\left(0,\alpha^{41},0\right)S\left(\alpha^{219},\alpha^{227},\alpha^{162}\right)$$
$$S\left(\alpha^{100},\alpha^{204},\alpha^{27}\right)=S\left(\alpha^{94},\alpha^{222},\alpha^{30}\right).$$

Обчислювальний компонент y_3.

$$\lambda(R)=\alpha_1'(R_1)\cdot f_1\left(\alpha_2'(R_2)\right)\cdot f_1\left(\alpha_3'(R_3)\right)=S\left(\alpha^{210},\alpha^{21},\alpha^{103}\right)S\left(0,\alpha^{68},\alpha^{126}\right)S\left(0,\alpha^{41},\alpha^{217}\right)=$$
$$S\left(\alpha^{210},\alpha^{141},\alpha^{22}\right)$$
$$y_3=\lambda(R)\,f_1\left(\alpha_3'(R_3)\right)\cdot f_1\left(\alpha_2'(R_2)\right)=S\left(\alpha^{210},\alpha^{141},\alpha^{22}\right)S\left(0,\alpha^{41},\alpha^{217}\right)S\left(0,\alpha^{68},\alpha^{126}\right)=$$
$$S\left(\alpha^{91},\alpha^{155},\alpha^{213}\right).$$

Ми отримали вихід $y_1=\left(\alpha^{118},\alpha^{102},\alpha^{224}\right),\ y_2=\left(\alpha^{100},\alpha^{204},\alpha^{27}\right),\ y_3=\left(\alpha^{91},\alpha^{155},\alpha^{213}\right)$.

Крок 2. Дешифрування

Вхідні дані : зашифрований текст (y_1,y_2,y_3) і особистий ключ $\left[\beta_k,\left(t_{0(k)},\ldots,t_{s(k)}\right)\right]$, $k=\overline{1,3}$.

Вихід : повідомлення, $m\in U(q)$ що відповідає зашифрованому тексту (y_1,y_2,y_3).

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

Обчислимо

$$D(R_1,R_2,R_3)=t_{0(1)}y_2y_3^{-1}t_{s(3)}^{-1}=S\left(\alpha^{14},\alpha^{169},\alpha^{59}\right)S\left(\alpha^{100},\alpha^{204},\alpha^{27}\right)S\left(\alpha^{91},\alpha^{155},\alpha^{213}\right)^{-1}S\left(\alpha^{196},\alpha^{164},\alpha^{2}\right)^{-1}$$
$$=S\left(\alpha^{50},\alpha^{83},\alpha^{56}\right)$$

Ми отримуємо $\beta_1(R_1)=\alpha^{50}=(02101)$.

Відновлення R_1 було зроблено раніше $R_1=\left(R_{1(1)},R_{2(1)},R_{3(1)},R_{4(1)}\right)=(0,1,5,1)$.

0|2|10| 1
2|0|22| 1
0|2|10| 1 −2|0|22| 1 =1|2|21| 0 R_1 =(*,*,5,1)
1|1| 21|0
1|2 |21|0 −1|1 |21|0 =0| 1 | 00|0 R_1 =(*,1,5,1)
0| 1 | 00|0
0| 1 | 00|0 −0| 1 | 00|0 = 0 | 0 | 00|0 R_1 =(0,1,5,1)

Для подальших обчислень необхідно видалити компоненти s і $\alpha_1'(R_1)$ із $\gamma_1'(R_1)$ зашифрованого тексту (y_2,y_3).

Обчислимо

$$y_2^{(1)} = \gamma_1'(R_1)^{-1} y_2 = S\left(\alpha^5, \alpha^{123}, \alpha^{41}\right)^{-1} S\left(\alpha^{100}, \alpha^{204}, \alpha^{27}\right) = S\left(\alpha^{137}, \alpha^{187}, \alpha^{160}\right)$$

і

$$y_3^{(1)} = \alpha_1'(R_1)^{-1} y_3 = S\left(\alpha^{210}, \alpha^{21}, \alpha^{103}\right)^{-1} S\left(\alpha^{91}, \alpha^{155}, \alpha^{213}\right) = S\left(0, \alpha^{166}, \alpha^{107}\right)$$

Обчислимо

$$D(R_2, R_3) = t_{0(2)} y_2^{(1)} \left(y_3^{(1)}\right)^{-1} t_{s(3)}^{-1} = S\left(\alpha^{109}, \alpha^{229}, \alpha^{106}\right) S\left(\alpha^{137}, \alpha^{187}, \alpha^{160}\right) S\left(\alpha^{135}, \alpha^{63}, \alpha^{10}\right)^{-1} S\left(\alpha^{196}, \alpha^{164}, \alpha^{2}\right)^{-1}$$
$$= S\left(0, \alpha^{166}, \alpha^{107}\right)$$

Ми отримуємо $\beta_2(R_2) = \alpha^{166} = (22001)$.

Відновимо R_2 за допомогою $\beta_2(R_2) = \alpha^{166} = (22001)$.

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

2|20| 01
0|20|01
2|20| 01 −0|20|01=2|00| 00 R_2 = (*,0,3)
2| 00|00
2| 00 | 00 −2 |00|00 =0| 00|00 R_2 =(0,0,3)

$\beta_2(R')^{-1} = 2|20|01 = \left(R_{1(2)}, R_{2(2)}, R_{3(2)}\right) = (0,0,3)$. $R_2 = \left(R_{1(2)}, R_{2(2)}, R_{3(2)}\right) = (0,0,3) = 81$

Видалимо компонент $\gamma_2'(R_2)$ від $y_2^{(1)}$ і $f_1(\alpha_2'(R_2))$ від $y_3^{(1)}$.

$$y_2^{(2)} = \gamma_2'(R_2)^{-1} y_2^{(1)} = S\left(\alpha^{105}, \alpha^{149}, \alpha^{27}\right)^{-1} S\left(\alpha^{137}, \alpha^{187}, \alpha^{160}\right) = S\left(\alpha^{159}, \alpha^{136}, \alpha^{23}\right)$$

і

$$y_3^{(2)} = f_1\left(\alpha_2'(R_2)\right)^{-1} y_3^{(1)} = S\left(0, \alpha^{68}, \alpha^{126}\right)^{-1} S\left(\alpha^{135}, \alpha^{63}, \alpha^{10}\right) = S\left(\alpha^{135}, \alpha^{11}, \alpha^{212}\right)$$

Обчислимо

$$D(R_3) = t_{0(3)} y_2^{(2)} \left(y_3^{(2)}\right)^{-1} t_{s(3)}^{-1} = S\left(\alpha^{52}, \alpha^{125}, \alpha^{228}\right) S\left(\alpha^{159}, \alpha^{136}, \alpha^{23}\right) S\left(\alpha^{135}, \alpha^{11}, \alpha^{212}\right)^{-1} S\left(\alpha^{196}, \alpha^{164}, \alpha^{2}\right)^{-1}$$
$$= S\left(0, 0, \alpha^{98}\right)$$

,

Ми отримуємо $\beta_3(R_3) = \alpha^{98} = (10212)$.

Відновимо R_3 за допомогою $\beta_3(R_3) = \alpha^{98} = (10212)$.

Виконаємо обернені обчислення $\beta_3(R_3)^{-1}$. Виберемо групи бітів у векторі $\beta(R)$ відповідно до типу $\left(r_{1(3)}, r_{2(3)}, r_{3(3)}, r_{4(3)}\right) = \left(3^2, 3, 3, 3\right)$. Ми отримуємо

10|2|1| 2
00 | 0 | 0| 2

10|2|1| 2 −00 |0 |0| 2 =10|2 |1 |0 R_3 =(*,*,1,2)
20|0| 1 | 0
10|2 |1 |0 −20|0| 1 | 0 =20|2| 0 | 0 R_3 =(*,2,1,2)
00| 2 | 0 | 0
20| 2 | 0 | 0 −00| 2 | 0 | 0 =20| 0 | 0 | 0 R_3 =(2,2,1,2)

$\beta_3(R')^{-1} = 10|2|1|2| = (R_{1(3)}, R_{2(3)}, R_{3(3)}, R_{4(3)}) = (2,2,1,2)$.

$R_3 = (R_{1(3)}, R_{2(3)}, R_{3(3)}, R_{4(3)}) = (2,2,1,2) = 209$

Отримаємо повідомлення

$$m = \alpha'(R)^{-1} y_1 = \alpha_3'(R_3)^{-1} \alpha_2'(R_2)^{-1} \cdot \alpha_1'(R_1)^{-1} \cdot y_1$$
$$= S(\alpha^{49}, \alpha^{184}, \alpha^{211})^{-1} S(\alpha^{200}, \alpha^{50}, \alpha^{124})^{-1}$$
$$S(\alpha^{144}, \alpha^{65}, \alpha^{173})^{-1} S(\alpha^{13}, \alpha^{135}, \alpha^{203})$$
$$= S(\alpha^0, \alpha^1, \alpha^2).$$

Вихід : повідомлення $m = (a^0, a^1, a^2)$.

6. Аналіз безпеки конструкції

Розглянемо атаку грубою сили на відновлення ключа $R = (R_1, R_2, R_3)$.
Можливі три реалізації такої атаки.

Атака на шифротекст. Вибираючи $R = (R_1, R_2, R_3)$ ми спробуємо розшифрувати текст $y_1' = \alpha'(R') \cdot m = \alpha_1'(R_1') \cdot \alpha_2'(R_2') \cdot \alpha_3'(R_3') \cdot m$.

Накриття $\alpha_{(k)} = [A_{1(k)}, ..., A_{s(k)}] = (a_{ij})_{(k)} = S(a_{ij(k)_a}, a_{ij(k)_b}, a_{ij(k)_c})$ вибрано випадково та значення $\alpha'(R')$ обрано множенням у групі без координатних обмежень . Результативний вектор $\alpha'(R')$ залежить від усіх компонентів $\alpha_1'(R_1'), \alpha_2'(R_2'), \alpha_3'(R_3')$. Перебір значень ключа $R = (R_1, R_2, R_3)$ має оцінку складності q^3. Для практичної атаки повідомлення m так само не відомо і маєм невизначеність для вибору q^3. Це робить атаку на ключ неможливою . Якщо взяти модель атаки з відомим текстом тоді складність атаки все одно є рівною q^3.

Атака на шифротекст y_2. Виберемо $R = (R_1, R_2, R_3)$ що співпадає з $y_2 = \gamma(R) \cdot f_2(\alpha_3'(R_3)) \cdot f_1(\alpha_3'(R_3)) \cdot f_1(\alpha_2'(R_2))$. Уявимо y_2 через компоненти $\alpha_i'(R_i)$

$$y_2 = S\left(t_{0(1)}{}^{-1} + \sum_{k=1}^{3} \sum_{i=1,\, j=R_{i(1)}}^{s(1)} a_{ij(k)_a} + \sum_{i=1,\, j=R_{i(1)}}^{s(1)} \beta_{ij(1)_a} + t_{s(3)}, \sum_{i=1,\, j=R_{i(2)}}^{s(2)} \left(a_{ij(2)_b} + \beta_{ij(2)_b} \right) + \sum_{i=1,\, j=R_{i(3)}}^{s(3)} a_{ij(3)_b} + *, \right.$$

$$\left. \sum_{i=1,\, j=R_{i(3)}}^{s(3)} \left(a_{ij(3)_c} + \beta_{ij(3)_c} \right) + * \right).$$

Тут, $(*)$ компоненти визначаються за допомогою перехресних розрахунків в груповій операції добутку $t_{0(k)}, \ldots, t_{s(k)}$ і добутку $a_{(1)_a}(R_1), \beta_{(1)}(R_1)$ для координати b та добутку $a_{(1)_a}(R_1), \beta_{(1)}(R_1), a_{(2)_b}(R_2), \beta_{(2)}(R_2)$ для координати c.

Значення координат y_2 отримаємо обчисленнями над векторами $\alpha_1'(R_1), \alpha_2'(R_2), \alpha_3'(R_3)$. Ключі R_1, R_2, R_3 є пов'язаними зміна будь -якого з них причини до змін y_2. Перебірна атака на ключ $R = (R_1, R_2, R_3)$ має оцінку складності q^3.

Атака на шифротекст y_3. Виберемо $R = (R_1, R_2, R_3)$ що співпадає з $y_3 = \lambda(R) f_1(\alpha_3'(R_3)) \cdot f_1(\alpha_2'(R_2))$. Визначимо y_3 через компоненти $\alpha_i'(R_i)$. Ми отримаємо

$$y_3 = S\left(\sum_{k=1}^{3} \sum_{i=1,\, j=R_{i(k)}}^{s(k)} a_{ij(k)_a}, \sum_{k=2}^{3} \sum_{i=1,\, j=R_{i(k)}}^{s(k)} a_{ij(k)_b} + *, \sum_{k=2}^{3} \sum_{i=1,\, j=R_{i(k)}}^{s(k)} a_{ij(k)_c} + * \right)$$

Значення координат y_3 ознайомитися обчисленнями над векторами $\alpha_1'(R_1), \alpha_2'(R_2), \alpha_3'(R_3)$. Ключі R_1, R_2, R_3 є також пов'язаними зміна будь - якого з них причини до змін y_3. Перебірна атака на ключ $R = (R_1, R_2, R_3)$ також має оцінку складності q^3.

Атака на вектори $(t_{0(k)}, \ldots, t_{s(k)})$. Перебірна атака $(t_{0(k)}, \ldots, t_{s(k)})$ є загальною для MST криптосистем і для обчислення у полі F_q над центром групи $Z(G)$ має оцінку складності q. Для нашого алгоритму шифрування обчислення підтримується на всій групі $|G| = q^3$ та складність атаки грубої сили на $(t_{0(k)}, \ldots, t_{s(k)})$ буде мати складність q^3.

Атака на алгоритм . Оцінка такої атаки буде справедлива для реалізації MST на будь-якій некомутативної групи та вимагає окремого аналізу . Ця атака має багато деталей, які пов'язані з уразливістю логарифмічного підпису та можливо з груповими операціями.

7. Висновки дослідження та подальші напрями

Наша пропозиція полягає у використанні малих груп Рі для шифрування на повній групі $U(q)=\left\{S(a,b,c)\middle|a,b,c\in F_q\right\}$ з пов'язаними ключами $R=(R_1,R_2,R_3)$ та складністю атаки грубої сили q^3. Ми розширили логарифмічний підпис на всю групу Рі $U(q)=\left\{S(a,b,c)\middle|a,b,c\in F_q\right\}$, з $\left|U(q)\right|=q^3$ та змінили алгоритм шифрування таким чином , щоб зв'язати ключі логарифмічних підписів та захистити від атаки послідовного відновлення ключа.

В подальшому пропонується провести більш змістовний аналіз безпеки використання некомутативних груп для побудови криптосистем на основі запропонованого алгоритму, розглянути можливість реалізації атак з використанням алгоритмів, що реалізовано за допомогою квантових обчислень та визначити напрями забезпечення стійкості щодо методів квантового криптоаналізу.

8. Література

[1] N.R. Wagner and M.R. Magyarik, A public-key cryptosystem based on the word problem", Proc. Advances in Cryptology – CRYPTO 1984, LNCS 196, Springer-Verlag (1985), 19–36.

[2] J. Birget, S. S. Magliveras, and M. Sramka, ``On public-key Cryptosystems based on combinatorial group theory," Tatra Mt. Math. Publ., vol. 33, pp. 137-148, Jan. 2006.

[3] A. Caranti and F. D. Volta, ``The round functions of cryptosystem PGM generate the symmetric group," Des. Codes Cryptogr., vol. 38, no. 1,pp. 147_155, 2006.

[4] W. Lempken, S.S. Magliveras, Tran van Trung and W. Wei, "A public key cryptosystem based on non-abelian finite groups", J. of Cryptology, 22 (2009), 62–74.

[5] S. S. Magliveras, "A cryptosystem from logarithmic signatures of finite groups," in Proceedings of the 29th Midwest Symposium on Circuits and Systems , pp. 972–975, Elsevier Publishing, Amsterdam, The Netherlands, 1986.

[6] P. Svaba and T. van Trung, "Public key cryptosystem MST3 cryptanalysis and realization", Journal of Mathematical Cryptology,vol.4,no.3,pp.271–315,2010.

[7] T. van Trung, ``New approaches to designing public key cryptosystems using one-way functions and trapdoors in finite groups," J. Cryptol., vol. 15, no. 4, pp. 285-297, 2002.

[8] Magliveras S S, Svaba P, van Trung T, et al. On the security of a realization of cryptosystem MST3. Tatra Mt Math Publ, 2008, 41: 1–13

[9] T. van Trung, ``Construction of strongly aperiodic logarithmic signatures," J. Math. Cryptol., vol. 12, no. 1, pp. 23-35, 2018.

[10] G. Khalimov, Y. Kotukh, S.Khalimova "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 2019 - Proceedings, 2019, pp. 865–868.
[11] G. Khalimov, Y. Kotukh, S.Khalimova "MST3 cryptosystem based on a generalized Suzuki 2 - Groups" // CEUR Workshop Proceedings, 2020, 2711, pp. 1–15.
[12] G. Khalimov, Y. Kotukh, S.Khalimova "Encryption scheme based on the automorphism group of the Ree function field" The 7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS 2020) Paris, France. December 14-16, 2020 Date Added to IEEE Xplore: 02 February 2021 ISBN Information: DOI: 10.1109/IOTSMS52051.2020.9340192
[13] G. Khalimov, Y. Kotukh, I. Didmanidze, S.Khalimova "Encryption scheme based on small Ree groups" The 7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS 2020) Paris, France. December 14-16, 2020 Date Added to IEEE Xplore: 02 February 2021 ISBN Information: DOI: 10.1109/IOTSMS52051.2020.9340192
[14] W. Lempken and T. van Trung, "On minimal logarithmic signatures of finite groups," Experimental Mathematics,vol.14, no. 3, pp. 257–269, 2005.
[15] Gregor Kemper, Frank L¨ubeck, and Kay Magaard, Matrix generators for the Ree groups 2G2(q), Comm. Algebra 29 (2001), no. 1, 407–413. MR MR1842506 (2002e:20025)
[16] P. Svaba, "Covers and logarithmic signatures of finite groups in cryptography", Dissertation, https://bit.ly/2Ws2D24

IMPROVED ENCRYPTION BASED ON NON-BELEAL SMALL RI GROUPS

Dr.Sci. E. Kotukh ORCID: 0000-0003-4997-620X
NTU "Dniprovska Polytechnic", Ukraine
E-mail: yevgenkotukh@gmail.com
Dr.Sci. G. Khalimov ORCID: 0000-0002-2054-9186
Kharkiv National University of Radio Electronics, Ukraine,
E-mail: hennadii.khalimov@nure.ua

Annotation*. The paper describes a new implementation of an encryption scheme based on Ree small groups. Our proposal is to use small groups of Ri to encrypt the full group with associated keys and brute-force attack complexity. We extended the logarithmic signature to the entire Ree group and modified the encryption algorithm to link the logarithmic signature keys and protect against a sequential recovery attack.*

Keywords: *MST cryptosystem, logarithmic signature, random coverage, small groups of Ri.*