Міністерство освіти і науки України
Харківський національний університет радіоелектроніки
Факультет Комп'ютерної інженерії та управління
(повна назва)
Кафедра Безпеки інформаційних технологій
(повна назва)

АТЕСТАЦІЙНА РОБОТА

Пояснювальна записка

рівень вищої освіти другий (магістерський)

Метод побудови логарифмічних підписів для реалізації квантовостійких криптосистем
(тема)

Виконав: Колесніков М.Є.
(прізвище, ініціали)
студент 2 курсу, групи БДІРм-20-1
Спеціальність 125 Кібербезпека
(код і повна назва спеціальності)
Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма «Безпека державних інформаційних ресурсів»
(повна назва освітньої програми)

Керівник Зав. каф. Халімов Г.З.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Халімов Г.З.
(підпис) (прізвище, ініціали)

2021 р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління
(повна назва)
Кафедра Безпеки інформаційних технологій
(повна назва)
Рівень вищої освіти другий (магістерський)
Спеціальність 125 Кібербезпека
(код і повна назва)
Тип програми освітньо-професійна
(освітньо-професійна, або освітньо-наукова)
Освітня програма «Безпека державних інформаційних ресурсів»
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«____»_____ 20 ___ р.

ЗАВДАННЯ
НА АТЕСТАЦІЙНУ РОБОТУ

студентові *Колеснікову Михайлу Євгеновичу*
(прізвище, ім'я, по батькові)

1. Тема роботи *Метод побудови логарифмічних підписів для реалізації квантовостійких криптосистем*
затверджена наказом по університету від "08" листопада 2021 р. № 1684Ст
2. Термін подання студентом роботи до екзаменаційної комісії
3. Вихідні дані до роботи
1) *Криптографічна система MST3, повністю аперіодичні логарифмічні підписи..*
2) Сваба П. Криптосистема відкритого ключа MST3: криптоаналіз та реалізація / П. Сваба, Т. Ван Трунг // Журнал математики та криптології / П. Сваба, Т. Ван Трунг., 2010. – С. 271–315.
4. Перелік питань, що потрібно опрацювати в роботі
1) Криптографічні системи MST
2) Алгоритм криптографічної системи MST_3
3) Атаки на криптографічну систему MST_3
4) Побудова аперіодичних логарифмічних підписів
5) Типи повністю аперіодичних логарифмічних підписів
6) Опис програмної реалізації модифікованої версії криптосистеми MST_3
5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій
5.1. Кількість основних операцій для одного шифрування/дешифрування FT-MST3.
5.2. Ефективність роботи з логарифмічними підписами різних розмірів
5.3. Фрагмент згенерованого аперіодичного логарифмічного підпису

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	*Отримання завдання*	08.11.2021	
2	*Пошук літератури*	08-10.11.2021	
3	*Аналіз зібраних даних*	11-18.11.2021	
4	*Аналіз криптографічної системи* MST_3	15-18.11.2021	
5	*Аналіз аперіодичних логарифмічних підписів*	13-18.11.2021	
6	*Програмна реалізація криптосистеми* MST_3	18-23.11.2021	
7	*Оформлення пояснювальної записки*	08-29.11.2021	

Дата видачі завдання _08__ ___листопада____2021 р.

Студент _____
(підпис)

Керівник роботи (проекту)_____ Зав. каф._Халімов Г.З._
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка містить: 65 сторінок, 2 рисунки, 2 таблиці, 1 додаток, 17 джерел.

Об'єктом дослідження цієї роботи є модифікована криптографічна система MST3, що використовує аперіодичні логарифмічні підписи.

Предметом досліджень є алгоритм побудови аперіодичних логарифмічних підписів та його інтеграція з криптографічною системою MST3.

Метою дипломної роботи є розгляд алгоритму генерації аперіодичних логарифмічних підписів з метою посилення криптографічної стійкості криптосистеми MST3. Додатковою метою є розробка і програмна реалізація модифікованої версії цієї криптосистеми.

Методи дослідження: аналіз алгоритму побудування аперіодичних логарифмічних підписів, програмна реалізація модифікованої криптосистеми MST3.

Проведено аналіз логарифмічних підписів та їхніх різновидів. Було наведено алгоритм генерації аперіодичних логарифмічних підписів, що мають підвисити криптостійкість криптографічної системи MST3. Було досліджено власне криптосистеми серії MST.

Відповідно до поставленої мети у дипломній роботі вирішуються такі задачі:

1. Вивчення різновидів логарифмічних підписів, необхідних для розуміння переваг аперіодичних підписів, та операцій для їхнього обчислення;
2. Аналіз безпосередньо аперіодичних логарифмічних підписів;
3. Дослідження алгоритмів криптографічних систем MST3;
4. Реалізація модифікованої криптосистеми MST3 на основі аперіодичних логарифмічних підписів.

Ключові слова: КРИПТОСИСТЕМА З ВІДКРИТИМ КЛЮЧЕМ MST3, АПЕРІОДИЧНИЙ ЛОГАРИФМІЧНИЙ ПІДПИС, ПОВНІСТЮ АПЕРІОДИЧНИЙ ЛОГАРИФМІЧНИЙ ПІДПИС, МЕТОД БАУМЕЙСТЕРА-ДЕ ВІЛЬЄСА.

ABSTRACT

The explanatory note contains: 65 pages, 2 figures, 2 tables, 1 appendix, 17 sources.

The object of research of this work is the modified version of the cryptographic system MST3 that uses aperiodic logarithmic signatures.

The subject of research is the algorithm for constructing aperiodic logarithmic signatures and its integration with the cryptographic system MST3.

The purpose of the work is to analyze the algorithm of generating aperiodic logarithmic signatures in order to enhance the cryptographic stability of the cryptosystem MST3. An additional goal is the development and software implementation of its modified version.

Research methods: analysis of the algorithm of constructing aperiodic logarithmic signatures, software implementation of the modified cryptosystem MST3.

The analysis of logarithmic signatures and their variants is carried out. An algorithm of generating aperiodic logarithmic signatures was presented to increase the cryptographic stability of the MST3 cryptographic system. The MST series cryptosystems themselves were investigated.

In accordance with the goal in the diploma work, it provides solutions for the following tasks:

1) Studying the types of logarithmic signatures necessary for understanding the advantages of aperiodic signatures and operations for their calculation;

2) Analysis of aperiodic logarithmic signatures themselves;

3) Research of MST3 the cryptographic system's algorithms;

4) Implementation of a modified cryptosystem MST3 based on aperiodic logarithmic signatures.

Key words: MST3 OPEN KEY CRYPTOGRAPHIC SYSTEM, APERIODIC LOGARITHMIC SIGNATURE, FULLY APERIODIC LOGARITHMIC SIGNATURE, BAUMEISTER-DE WILJES METHOD.

ЗМІСТ

ВСТУП

Останнім часом асиметрична криптографія стала важливою для багатьох інформаційних систем. Було запропоновано багато криптосистем з відкритим ключем, але лише деякі з таких систем залишаються непорушними. Більшість із них ґрунтується на сприйнятті нерозв'язності певних математичних проблем у дуже великих, скінченних циклічних групах у певних конкретних уявленнях. Найважливішими складними проблемами є:

1) проблема розкладання великих цілих чисел на множники;
2) проблема дискретного логарифма, зокрема, представлення великих циклічних груп;
3) пошук короткого базису для заданої інтегральної решітки L великої розмірності.

На жаль, з огляду на квантові алгоритми Шора для цілочисельної факторизації та вирішення проблеми дискретного логарифма [14], відомі системи з відкритим ключем будуть небезпечними, коли квантові комп'ютери стануть практичними. Недавня доповідь під редакцією П. Нгуєна [15] визначає ці та інші проблеми, які стоять перед сферою інформаційної безпеки в майбутньому.

Логарифмічні підписи для кінцевих груп є невід'ємною складовою криптосистем з відкритим ключем MST1 та MST3. Зокрема, вони є основним компонентом закритого ключа MST3. Важливим питанням щодо використання MST3 стало створення нових класів логарифмічних підписів із властивостями, яких не мають трансверсальні та злиті трансверсальні логарифмічні підписи. Для цього Баумейстер та де Вільєс представили новий метод побудови аперіодичних логарифмічних підписів для абелевих груп. У поданій роботі буде введено поняття повністю аперіодичних логарифмічних підписів, показано їхню побудову для абелевих p-груп на основі методу Баумейстера-де Вільєса, а також представлено модифіковану реалізацію MST3, що використовує їх.

Наприкінці 1970-х років Спіросом Магліверасом розпочато дослідження придатності особливої факторизації для кінцевих неабелевих груп – логарифмічного підпису – для використання у криптографії. Пізніше було опубліковано роботи Магліверасом, Траном ван Трунгом та Стінсоном, де описуються розроблені Магліверасом криптографічні системи – MST1 на основі логарифмічних підписів та MST2 на основі альтернативного типу покриттів – так званих [s, r]-осередках. Перешкодою є відсутність будь-якої відомої практичної реалізації MST1 або MST2. Пізніше ним було розроблено іншу криптосистему на основі відкритих ключів – MST3, що поєднує попередні та використовує логарифмічні підписи та випадкові накриття кінцевих

неабелевих груп. 2-групи Судзукі пропонуються як потенційний базовий елемент для реалізації цієї криптосистеми.

Отже, криптосистеми з відкритим ключем MST1 [8] та MST3 [5, 12] було розроблено на основі логарифмічних підписів – своєрідної факторизації кінцевих груп. Основна ідея побудови MST3 полягає у побудові однобічних функцій з потайним входом (люком), використовуючи випадкові покриття для кінцевих неабелевих груп з великим центром. Інтегрована інформація про люк, що є основною частиною закритого ключа схеми, використовує логарифмічні підписи центру. 2-групи Судзукі було запропоновано як основні групи для створення MST3. Проста структура 2-груп Судзукі дозволяє більш уважне дослідження безпечності системи та більш ефективну її реалізацію. У першій реалізації спеціальний клас канонічних логарифмічних підписів разом з елементарними абелевими групами виміру «2» використовується як основа для генерації ключів. Вони прості в побудові та дозволяють дуже ефективно розбивати фактори. Перший аналіз спрощеної версії MST3 [5], що проведено Магліверасом, Свабою, ван Трунгом та Заяцем [9], показує, що трансверсальні логарифмічні підписи непридатні для використання у схемі. Подальші дослідження Блекбьорна, Сіда та М'юллана [2] доводить, що використання злитих трансверсальних логарифмічних підписів також робить спрощену версію MST3 небезпечною. Однак для посиленої версії MST3 [12] показано, що злиті трансверсальні логарифмічні підписи все ще витримують потужну атаку перестановкою матриць [12].

Тому є доцільним вивчити додаткові класи логарифмічних підписів з особливостями, що роблять їх більш придатними для використання у криптосистемах з відкритим ключем на кшталт MST3. У нещодавньому документі [1] Баумейстер та де Вільєс пропонують цікавий метод для створення аперіодичних логарифмічних підписів для абелевих груп, зокрема, для абелевих 2-груп, які перешкоджають атаці Блекбьорна та інших. Варто зазначити, що трансверсальні або злиті трансверсальні логарифмічні підписи мають властивість бути періодичними. У поданій роботі буде введено поняття повністю аперіодичних логарифмічних підписів та представлено їхню побудову для абелевих p-груп на основі методу Баумейстера-де Вільєса. Аперіодичні і повністю аперіодичні логарифмічні підписи забезпечують такі класи логарифмічних підписів, що відповідають використанню MST3. Більше того, повністю аперіодичні логарифмічні підписи для абелевих груп самі по собі представляють теоретичний інтерес.

1 ПЕРЕДУМОВИ

1.1 Математичний опис елементів, необхідних для квантово стійкої криптосистеми

Нехай G – скінченна абстрактна група, її ширина G визначається як ціле додатне число $w = \lceil log|G| \rceil$. Слід позначити сукупність усіх скінченних послідовностей елементів у G як $G^{[Z]}$ і потрібно розглянути елементи $G^{[Z]}$ як однорядні матриці з записами в G. Нехай $X = [x_1, x_2, \dots, x_r]$ та $Y = [y_1, y_2, \dots, y_s]$ – два елементи в $G^{[Z]}$. Тоді

$$X \cdot Y = [x_1y_1, x_1y_2, \dots, x_1y_s, x_2y_1, x_2y_2, \dots, x_2y_s, \dots, x_ry_1, x_ry_2, \dots, x_ry_s].$$

Замість $X \cdot Y$ можливо записати $X \otimes Y$ як звичайний тензорний добуток матриць, або скорочено – XY. Якщо $X = [x_1, \dots, x_r]$, можливо позначити через $\bar{X}$ елемент $\sum_{i=1}^{r} x_i$ в груповому кільці ZG.

Нехай $\alpha = [A_1, A_2, \dots, A_s]$ – це послідовність $A_i \in G^{[Z]}$, така, що $\sum_{i=1}^{r} |A_i|$ обмежена поліномом від $log|G|$. Нехай

$$\overline{A_1} \cdot \overline{A_2} \cdot \dots \cdot \overline{A_s} = \sum_{g \in G} a_g g, a_g \in Z. \quad (1.1)$$

Нехай S є підмножиною G, тоді можливо сказати, що α – це:

1) покриття для G (або S), якщо $a_g > 0$ для всіх $g \in G$ $(g \in S)$.
2) логарифмічний підпис для G (або S) при $a_g = 1$ для всіх $g \in G$ $(g \in S)$.

Таким чином, покриття $\alpha = [A_1, A_2, \dots, A_s]$ для підмножини S кінцевої групи G можливо розглядати як упорядковану колекцію підмножин A_i групи G з $|A_i| = r_i$ так, що кожен елемент $h \in S$ може бути виражений принаймні одним способом як добуток виду

$$h = g_1 \cdot g_2 \dots g_{s-1} \cdot g_s \quad (1.2)$$

для $g_i \in A_i$.

Якщо кожен $h \in S$ можливо виразити рівно одним способом за допомогою рівняння 1.2, то α називається логарифмічним підписом для S. Таким чином, логарифмічні підписи є особливим класом покриттів.

A_i називають блоками, а вектор $(g_1, \dots, g_s)$ з $r_i = |A_i|$ – покриттям типу α. Покриття α є нетривіальним, якщо $s \geq 2$ і $r_i \geq 2$ для $1 \leq i \leq s$; інакше α

називається тривіальним. Покриття називається ручним (або таким, що факторизується), якщо розкладання в рівнянні 1.2 може бути досягнуто за поліноміальний час в ширині w від G, відповідно воно називається диким, якщо воно не ручне. Нехай $\gamma := 1_G = G_0 < G_1 < \cdots < G_s = G$ – ланцюг підгруп G, а A_i – впорядкована повна множина правих (або лівих) представників класу G_{i-1} в G_i. У свою чергу $[A_1, \dots, A_s]$ утворює логарифмічний підпис для G, який називають трансверсальним логарифмічним підписом. Трансверсальні логарифмічні підписи є важливим прикладом ручних логарифмічних підписів [8].

Загалом, задача знаходження факторизації в рівнянні 1.2 відносно випадково згенерованого покриття є, як вважається, нерозв'язною. Є вагомі докази, що підтверджують серйозність проблеми. Наприклад, нехай G – циклічна група, а g – генератор G. Нехай $\alpha = [A_1, A_2, \dots, A_s]$ – будь-яке покриття для G, для якого елементи A_i записуються як степені g. Тоді розкладання на множники відносно α зводиться до розв’язування задачі дискретного логарифма в G.

Примітка 1.1. Варто зазначити, що проблема генерування випадкових покриттів для скінченних груп великого порядку розглядається в [11]. Імовірнісний метод показує, що генерування випадкових покриттів для груп великого порядку можливо здійснити з високою ефективністю та з мінімальними витратами.

Вирішальним моментом, який робить покриття корисними для групової криптографії, є те, що якщо вищезгадана проблема факторизації нерозв’язна, то покриття, по суті, індукують односторонні функції. Це можливо описати наступним чином. Нехай $\alpha = [A_1, A_2, \dots, A_s]$ – покриття типу $(r_1, r_2, \dots, r_s)$ для G з $A_i = [a_{i,1}, a_{i,2}, \dots, a_{i,r_i}]$ і нехай $m = \prod_{i=1}^{s} r_i$. Нехай $m_1 = \prod_{j=1}^{i-1} r_j$ для $i = 2, \dots, s$. Можливо позначити канонічну біекцію від $Z_{r_1} \oplus Z_{r_2} \oplus \dots \oplus Z_{r_s}$ на Z_m; тобто

$$\tau: Z_{r_1} \oplus Z_{r_2} \oplus \dots \oplus Z_{r_s} \to Z_m$$
$$\tau(j_1, j_2, \dots, j_s) := \textstyle\sum_{i=1}^{s} j_i m_i.$$

Використовуючи τ, тепер визначається сюр`єктивне відображення $\breve{\alpha}$, індуковане α.

$$\breve{\alpha}(x) := a_{i,j_1} \cdot a_{i,j_2} \dots a_{s,j_s},$$

де $(j_1, j_2, \dots, j_s) = \tau^{-1}(x)$. Оскільки τ та τ^{-1} ефективно обчислювані,

відображення $\check{\alpha}(x)$ є ефективно обчислюваним.

І навпаки, за наявності покриття α та елемента $y \in G$, щоб визначити будь-який елемент $x \in \check{\alpha}^{-1}(y)$, необхідно отримати будь-яку з можливих факторизацій типу 1.2 для y та визначити індекси $j_1, j_2, \dots, j_s$ такі, що $y = a_{i,j_1} \cdot a_{i,j_2} \dots a_{s,j_s}$. Це можливо тоді і тільки тоді, коли α ручний. Коли вектор $j_1, j_2, \dots, j_s$ визначено, значення $\check{\alpha}^{-1}(y) = \tau(j_1, j_2, \dots, j_s)$ можливо ефективно обчислити.

Існують різні типи трансформацій, які можливо застосувати до покриттів. Тут розглянуто лише один тип, який буде використано в наступних розділах.

Нехай $\alpha = [A_1, A_2, \dots, A_s]$ – покриття для G. Нехай $g_0, g_1, \dots, g_s \in G$ і слід розглянути $\beta = [B_1, B_2, \dots, B_s]$ з $B_i = g_{i-1}^{-1} A_i g_i$. Говориться, що β є двостороннім перетворенням α на $g_0, g_1, \dots, g_s$; в окремому випадку, де $g_0 = 1$, β називається сендвічем з α можливо зауважити, що β є покриттям для G.

Два покриття (логарифмічних підписи) α, β називаються еквівалентними, якщо $\check{\alpha}$=$\check{\beta}$. Наприклад, якщо α є сендвічом з β, то α і β, очевидно, еквівалентні.

Використано наступну криптографічну гіпотезу, що якщо $\alpha = [A_1, A_2, \dots, A_s]$ є випадковим покриттям для “великої” підмножини S групи G, то пошук факторизації в 1.2 є нерозв’язною проблемою. Іншими словами, відображення

$$\check{\alpha}: Z_m \to S$$

Індуковане α при $m = \prod_{i=1}^{s} |A_i|$ – одностороння функція.

У [5] загальну версію криптосистеми з відкритим ключем MST_3 описано для довільно абстрактної неабелевої групи G. Група G повинна задовольняти лише такій властивості: G має нетривіальний центр Z, такий, що G не розщеплюється над Z, тобто не існує підгрупи $H < G$ з $H \cap Z = 1$ такої, що $G = H \cdot Z$. Крім того, припускається, що порядок Z є достатньо великим, щоб задачі вичерпного пошуку були обчислювально нездійсненними в Z. Детальніше про MST_3 буде наведено в наступному підрозділі.

2-групи Судзукі були запропоновані для використання в можливій реалізації загальної версії MST_3. З одного боку, завдяки своїй структурі, 2-групи Судзукі дозволяють вивчати безпеку системи, а з іншого боку, вони мають просту презентацію, що дозволяє ефективно реалізувати схему. Перш ніж представити нову версію MST_3 з використанням 2-груп Судзукі у наступному розділі, буде описано для повноти цей спеціальний клас 2-груп.

Для початку нагадуються деякі основні факти про скінченні p-групи, де p позначає просте число. Скінченна група G порядку a степеня числа p називається p-групою, тобто $|G| = p^n$ для певного натурального числа n. Найменше спільне кратне порядків елементів G називається показником G. Абелева (комутативна) p-група G з показником p називається елементарною абелевою p-групою. Множина $Z(G) = \{z \in G : zg = gz, \forall g \in G\}$ називається центром G. Добре відомо, що $Z(G)$ є підгрупою порядку не менше p для будь-якої p-групи G. Підгрупа G', породжена всіма елементами виду $x^{-1}y^{-1}xy$ називається комутативною підгрупою G. Так звана підгрупа Фраттіні в G, позначена $\Phi(G)$, за визначенням є перетином усіх максимальних підгруп G. Якщо G є p-групою, фактор-група $G/\Phi(G)$ елементарно абелева. Зокрема, якщо G є 2-групою, $\Phi(G) = \langle g^2 | g \in G \rangle$ і. Нарешті, елемент 2-го порядку в групі називається інволюцією.

Формально 2-група Судзукі визначається як неабелева 2-група з більш ніж однією інволюцією, що має циклічну групу автоморфізмів, яка транзитивно переставляє свої інволюції. Цей клас 2-груп досліджував і охарактеризував Г. Хігман [16]. Зокрема, у будь-якій 2-групі Судзукі G є $G' = \Omega_1(G)$, де $\Omega_1(G) = \langle g \in G : g^2 = 1 \rangle$ та $Z(G) = q = 2^m, m > 1$. У [16] показано, що порядок G є q^2. Таким чином, усі інволюції G знаходяться в центрі G, тому $Z(G)$ і фактор-група $G/\Phi(G)$ елементарно абелеві. Отже, всі елементи, що не в $Z(G)$, мають порядок 4, тобто G має показник 4. Відомо, що G має автоморфізм ξ порядку $q - 1$, що циклічно переставляє інволюції G [3, 16].

У даній реалізації MST_3 розглянуто лише клас 2-груп Сузукі, що мають порядок q^2. Використовуючи позначення Хігмана, 2-групу Сузукі порядку q^2 буде позначатись $A(m, \theta)$. Нехай $q = 2^m$ з $3 \leq m \in N$ таке, що поле F_q має нетривіальний автоморфізм непарного порядку. Звідси випливає, що m не є степенем числа 2. Групи $A(m, \theta)$ можливо визначити як матричні групи.

Насправді, якщо визначити

$$G = \{S(a, b) | a.b \in F_q\},$$

де

$$S(a, b) = \begin{pmatrix} 1 & a & b \\ 0 & 1 & a^\theta \\ 0 & 0 & 0 \end{pmatrix}$$

є 3x3-матрицею над F_q, то показано, що група G ізоморфна $A(m,\theta)$. Таким чином, G має порядок q^2, і має

$$Z := Z(G) = \Phi(G) = G' = \Omega_1(G) = \{S(0,b) | b \in F_q\}.$$

Оскільки центр $Z(G)$ є елементарним абелевим та порядку q, його можливо ототожнити з адитивною групою поля F_q. Також фактор-група $G/\Phi(G)$ є елементарною абелевою групою порядку q. Тоді легко перевірити, що множення двох елементів у G визначається за правилом:

$$S(a_1,b_1)S(a_2,b_2) = S(a_1 + a_2, b_1 + b_2 + a_1 a_2^{\theta}) \quad (1.3)$$

У цій матричній формі представлення 2-групи Судзукі $A(m,\theta)$ можливо розглядати як підгрупи загальної лінійної групи $GL(3,q)$ над F_q.

У [16] показано, що групи $A(m,\theta)$ і $A(m,\phi)$ ізоморфні тоді і тільки тоді, коли $\phi = \theta^{\pm 1}$. Для будь-яких $0 \neq \lambda \in F_q$ матриця

$$\Lambda = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda^{\theta+1} \end{pmatrix}$$

індукує автоморфізм $A(m,\theta)$. І Λ діє на $A(m,\theta)$ за правилом

$$\Lambda^{-1} S(a,b) \Lambda = S(a\lambda, b\lambda^{\theta+1}).$$

Якщо $\lambda = \phi$ є примітивним елементом у F_q, то Λ має порядок $q-1$ і циклічно переставляє $q-1$ інволюції в центрі A_m; / $A(m,\theta)$.

1.2 Криптосистема MST3

Тепер є доцільним розглянути алгоритми криптографічної системи MST_3, а також атак на неї з метою зрозуміти важливість аперіодичних логарифмічних підписів в контексті підвищення безпеки.

Нехай $G := A(m,\theta)$ – 2-група Судзукі, визначена на F_q з $q = 2^m$. Оскільки $Z = Z(G)$ є елементарною абелевою 2-групою порядку q, можливо розглядати Z як векторний простір розмірності m над F_2. Отже, група автоморфізмів Z є

загальною лінійною групою $GL(m,2)$, (тобто групу утворюють усі $m \times m$ оборотні матриці над F_2). Слід позначити $Aut(Z) \coloneqq GL(m,2)$. Якщо $z = S(0,b)$ і $\varphi \in Aut(Z)$, то дія φ на z визначається як $z^{\varphi} \coloneqq S(0,b^{\varphi})$.

Нехай $g = S(x,y) \in G$. Тоді слід позначити $g_{.a} \coloneqq x$ та $g_{.b} \coloneqq y$.

Примітка 1.2**.** Нехай f – будь-який гомоморфізм від G до Z. Нехай $N = Ker(f)$. Тоді N нормальна підгрупа групи G і $G/N \cong f(G)$. Отже, фактор-група G/N абелева. Як група комутативів, $G' = Z$ при $N \geq Z$. Звідси випливає, що $f(z) = 1$ для кожного $z \in Z$.

Алгоритм генерації ключів виглядає наступним чином:

1) Обрати велику групу G, як описано вище;
2) Згенерувати логарифмічний підпис, що розкладається на множники $\beta = [B_1, B_2, \dots, B_s] \coloneqq (b_{ij})$ типу $(r_1, \dots, r_s)$ для Z;
3) Згенерувати випадкове покриття $\alpha = [A_1, A_2, \dots, A_s] \coloneqq (a_{ij})$ того самого типу, що й β для певної підмножини J групи G, такої, що $A_1, A_2, \dots, A_s \subseteq G \backslash Z$. Елементи в кожному блоці $A_i = [a_{i,1}, a_{i,2}, \dots, a_{i,r_i}]$ задовольняють наступним умовам:
    а) $a_{(ij_1)_{.a}} \neq a_{(ij_2)_{.a}}$, для $j_1 \neq j_2$. Це еквівалентно тому, що $a_{(ij_1)}$ і $a_{(ij_2)}$ не знаходяться в одному класі Z.
    б) $\sum_{j=1,..,r} a_{(ij)_{.a}} = 0$. Сенс цієї умови стане очевидним, коли буде обговорено безпеку системи в наступному розділі.
4) Обрати $t_0, t_1, \dots, t_s \in G \backslash Z$;
5) Обрати гомоморфізм $f : G \to Z$;
6) Обчислити $\gamma = (h_{ij})$, $h_{ij} = t_{i-1}^{-1} \cdot a_{ij} \cdot f(a_{ij}) \cdot b_{ij} \cdot t_i$.

Тоді $\alpha = (a_{ij})$ і $\gamma = (h_{ij})$ є відкритим ключем. В свою чергу $\beta = (b_{ij})$, $t_1, t_2, \dots, t_s$ та f складають закритий ключ.

Алгоритм шифрування виглядає наступним чином**:**

Вхідні дані: повідомлення $x \in Z$ і відкритий ключ α і γ.

Вихідні дані**:** зашифрований текст (y_1, y_2) повідомлення x. Алгоритм:

1) Обрати випадковий $R \in Z_{|Z|}$;
2) Знайти $y_1 = \breve{\alpha}(R) \cdot x, y_2 = \breve{\gamma}(R) \cdot x = t_0^{-1} \breve{\alpha}(R) \cdot f(\breve{\alpha}(R)) \cdot \breve{\beta}(R) \cdot t_s \cdot x$.

Алгоритм розшифрування виглядає наступним чином:

Вхідні дані: зашифрований текст (y_1, y_2) та приватний ключ $\beta = (b_{ij})$, $t_1, t_2, \dots, t_s$і f.

Вихідні дані: повідомлення $x \in Z$, що відповідає зашифрованому тексту

(y_1, y_2). Алгоритм:

1) Користуючись тим, що $f(y_1) = f(\check{\alpha}(R))$ із зауваження одного з дослідників [9], обчислити $\check{\beta}(R) = f(\check{\alpha}(R))^{-1} \cdot y_1^{-1} \cdot t_0 \cdot y_2 \cdot t_s^{-1} = f(y_1)^{-1} \cdot y_1^{-1} \cdot t_0 \cdot y_2 \cdot t_s^{-1}$;
2) Відновити R з $\check{\beta}(R)$, який ефективно обчислюється, оскільки β факторизується. Обчислюючи $\check{\alpha}(R)$, відновити x з y_1.

Уточнення гомоморфізму f. Для реалізації криптосистеми MST_3 використовується наступний клас гомоморфізмів. Нехай $g = S(g_{.a}, g_{.b}) \in G$, і нехай $\sigma \in Aut(Z) := GL(m, 2)$. Якщо визначити $f : G \to Z$ та $f(g) := S(0, g_{.a}^{\sigma})$, тоді f є гомоморфізмом від G до Z.

Потрібно зауважити, що якщо f – тривіальний гомоморфізм, тобто $f(g) = S(0,0) = 1_G$ для всіх $g \in G$, то отримано реалізацію "оригінальної" схеми MST_3 [5]. Введення нетривіального гомоморфізму f при розробці нової схеми мотивується атакою, представленою в [9]. Основна ідея полягає в перетворенні логарифмічного підпису $\beta = (b_{ij})$ в оригінальному MST_3 у випадкове покриття $\delta = (b_{ij} \cdot f(a_{ij}))$ у цій новій схемі. В результаті атака в [9] більше не може застосовуватися.

MST_3, щойно описаний для 2-груп Сузукі, може бути узагальнений, звичайно, для багатьох інших класів скінченних груп, наприклад, класу спеціальних p-груп. Цікавий клас p-груп, також званий p-групами Судзукі для непарних простих чисел p [17], може розглядатися як природний кандидат на базові групи MST_3.

Метод шифрування MST_3, описаний вище, є рандомізованим шифруванням. Однак, якщо розглядати $Z_{|Z|}$ як простір повідомлень і зашифроване повідомлення $z \in Z_{|Z|}$ за допомогою обчислень

$$(y_1, y_2) = (\check{\alpha}(z), \check{\gamma}(z))$$

як зашифрований текст, шифрування стає нерандомізованим. Варто зазначити, що нерандомізоване шифрування можливо налаштувати в рамках методу рандомізованого, якщо замінити R на z та використати $x = 1_Z$. Щоб спростити обговорення криптоаналізу схеми в наступних розділах, буде розглянуто лише нерандомізоване шифрування.

Далі будуть досліджуватися різні типи можливих прямих атак на закритий ключ MST_3. Необхідно знайти нижні межі робочого навантаження щодо цих атак. Виявляється, що ці межі мають дуже великий розмір з точки зору порядку використовуваних груп.

Спочатку слід зауважити, що якщо криптоаналітик намагається витягти інформацію про $\beta = (b_{ij})$, головну частину приватного ключа, йому достатньо отримати логарифмічний підпис β', еквівалентний β, тобто будь-який β', який є сендвіч-перетворенням β. Інший результат у [9] показує, що противнику достатньо навіть зламати систему, якщо він може визначити логарифмічний підпис β^* для Z такий, що

$$\check{\beta}^*(x) = \check{\beta}(x) \cdot c \qquad (1.4)$$

для всіх $x \in Z_{|Z|}$, де $c \in Z$ – нерухомий елемент. Наприклад, якщо $\beta^* = [B_1^*, B_2^*, \dots, B_s^*]$ з $B_i^* = z_{i-1}^{-1} B_i z_i$ – двостороннє перетворення β з $z_1, z_2, \dots, z_s \in Z$, тоді $\check{\beta}^*(x) = \check{\beta}(x) \cdot c$, де $c = z_0 z_s$.

Результат показує факт, що має відношення до способу підрахунку кількості елементів t_i, використовуваних при генерації γ. Насправді, якщо замінити t_i на $t_i^* = t_i \cdot z_i$, для $z_i \in Z$, і $i = 0, \dots, s$ буде отримано β^* таке, що $\check{\beta}^*(x) = \check{\beta}(x) \cdot \prod_{i=0}^{s} z_i$. Отже, криптоаналітику достатньо знати підкласи класу Z в G з представниками класу t_i. Тоді він може використовувати будь-який представник класу $t_i^* = t_i \cdot z_i$ замість t_i. Отже, під час аналізу безпеки системи достатньо визначити класи t_i відносно Z, а не сам елемент t_i.

Логарифмічний підпис β^* для Z, що задовольняє рівнянню 1.4, називається перекладом β.

Нехай $K = [\beta, f, t_0, \dots, t_s]$ буде приватним ключем для MST_3. Ключ $K' = [\beta', f, t_0', \dots, t_s']$ є еквівалентом K, якщо β є перекладом $t_i' = t_i \cdot z_i$ для деякого $z_i \in Z$ і всіх $i \in \{0, \dots, s\}$.

Основна мета – довести нижні межі робочих зусиль, необхідних для відновлення еквівалентного приватного ключа. Робоче навантаження вимірюється з точки зору розміру залучених груп, і будуть застосовуватись евристичні та алгебраїчні методи для цього аналізу.

Криптоаналітик може намагатися витягти інформацію про закритий ключ із загальнодоступних відомостей $\alpha = (a_{ij})$ і $\gamma = (h_{ij})$. При використанні цієї атаки потрібно побудувати ключ $K' = [\beta', f, t_0', \dots, t_s']$ еквівалентний закритому ключу $K = [\beta, f, t_0, \dots, t_s]$. Спочатку будується рівняння з невідомими, що включає інформацію про закритий ключ, а потім досліджується складність розв'язування цього рівняння. Для цієї мети використовується операція множення в основних 2-групах Судзукі.

Слід нагадати наступні формули для зручності:

$$S(a_1,b_1)S(a_2,b_2)=S\left(a_1+a_2,b_1+b_2+a_1a_2^{\theta}\right).$$
$$t_i\in G,t_i=S\left(t_{(i)_{.a}},t_{(i)_{.b}}\right),\alpha:=\left(a_{ij}\right),a_{ij}=S\left(a_{(i,j)_{.a}},a_{(i,j)_{.b}}\right).$$
$$g=S(g_{.a},g_{.b})\in G,f(g):=S(0,g_{.a}^{\sigma}),\text{де } Aut(Z)=GL(m,2).$$

Далі $gZ=hZ$ в G з $g=S(x_1,x_2)$ і $g=S(y_1,y_2)$, тоді і тільки тоді, коли $x_1=y_1$. Слід почати з

$$\gamma=\left(h_{ij}\right)=\left(a_{i-1}^{-1}a_{ij}b_{ij}f\left(a_{ij}\right)t_i\right)=\left(S\left(h_{(i,j)_{.a}},h_{(i,j)_{.b}}\right)\right)$$

і зосередитися на одному блоці. Можливо почати з першого блоку. Елементами в цьому блоці є $h_{11},h_{12},\dots,h_{1r_1}$. Нехай $J\subseteq\{1,\dots,r_1\}$ – така підмножина, що $|J|$ парне. Тоді, підсумовуючи елементи першого блоку, що мають індекси в J, буде отримано два наступні вирази, що відповідають «.a частині» та «.b частині» суми.

$$\sum_{j\in J,|J|\text{ парне}}h_{(i,j)_{.a}}=\sum_{j\in J}a_{(1,j)_{.a}} \tag{1.5}$$

$$\sum_{j\in J,|J|\text{ парне}}h_{(i,j)_{.b}}=$$
$$=\sum_{j\in J}a_{(1,j)_{.b}}+\sum_{j\in J}b_{(1,j)_{.b}}+\sum_{j\in J}a_{(1,j)_{.a}}^{\sigma}+t_{(0)_{.a}}\cdot\cdot\sum_{j\in J}a_{(1,j)_{.a}}^{\theta}++t_{(1)_{.a}}^{\theta}\cdot\sum_{j\in J}a_{(1,j)_{.a}} \tag{1.6}$$

Додавання $\sum_{j\in J}a_{(1,j)_{.b}}$ до обох частин 1.6 призводить до рівняння

$$\sum_{j\in J}a_{(1,j)_{.b}}+\sum_{j\in J}h_{(i,j)_{.b}}=$$
$$=\sum_{j\in J}b_{(1,j)_{.b}}+\sum_{j\in J}a_{(1,j)_{.a}}^{\sigma}+t_{(0)_{.a}}\cdot\sum_{j\in J}a_{(1,j)_{.a}}^{\theta}+t_{(1)_{.a}}^{\theta}\cdot\cdot\sum_{j\in J}a_{(1,j)_{.a}} \tag{1.7}$$

Слід зауважити, що ліва частина рівняння 1.7 відома.

При $h_{(1,1)_{.a}}=t_{(0)_{.a}}+a_{(1,1)_{.a}}+t_{(1)_{.a}}$ буде отримано

$$t_{(0)_{.a}} = h_{(1,1)_{.a}} + t_{(1)_{.a}} + a_{(1,1)_{.a}}.$$

Замінивши $t_{(0)_{.a}}$ в 1.7 виходить

$$\sum_{j\in J,|J| \text{ парне}} \left(a_{(1,j)_{.b}} + h_{(i,j)_{.b}}\right) = \sum_{j\in J} b_{(1,j)_{.b}} + \sum_{j\in J} a^{\sigma}_{(1,j)_{.a}} + \left(h_{(1,1)_{.a}} + t_{(1)_{.a}} + a_{(1,1)_{.a}}\right) \cdot \sum_{j\in J} a^{\theta}_{(1,j)_{.a}} + t^{\theta}_{(1)_{.a}} \cdot \sum_{j\in J} a_{(1,j)_{.a}}$$

Отже, вважаючи $t_{(1)_{.a}}$ невідомим, результатом стане тричлен вигляду

$$\mathrm{A}t^{\theta}_{(1)_{.a}} + Bt_{(1)_{.a}} + X = 0, \qquad (1.8)$$

де

$$A = \sum_{j\in J} a_{(1,j)_{.a}},\ B = \sum_{j\in J} a^{\sigma}_{(1,j)_{.a}},$$

$$X = \sum_{j\in J} a_{(1,j)_{.b}} + \sum_{j\in J} h_{(i,j)_{.b}} + \sum_{j\in J} b_{(1,j)_{.b}} + \sum_{j\in J} a^{\sigma}_{(1,j)_{.a}} + \left(a_{(1,1)_{.a}} + +h_{(1,1)_{.a}}\right) \cdot \sum_{j\in J} a^{\theta}_{(1,j)_{.a}}$$

Зауваження: $\left(t_{(1)_{.a}}\right)^{\theta}$ у тричлені виражає дію θ на елемент $t_{(1)_{.a}} \in F_q$.

Оскільки $\mathrm{F_q}$ є автоморфізмом з $q = 2^m$, його можливо записати як степень автоморфізму Фробеніуса $\phi : a^{\phi} \to a^2$ з $\mathrm{F_q}$. Звідси й змінна, наведена вище, якщо $\theta = \phi^n$ для деякого $1 \le n < m$. A і B відомі, але змінна X містить дві невідомі суми $\sum_{j\in J} b_{(1,j)_{.b}}$ та $\sum_{j\in J} a^{\sigma}_{(1,j)_{.a}}$.

Метою противника є вилучення інформації про β. Оскільки в рівнянні 1.8 значення X невідоме, криптоаналітик повинен обчислити значення для змінної $t_{(1)_{.a}}$. Є $q-1$ можливих варіантів для $t_{(1)_{.a}}$.

Відгадавши значення для змінної, він може обчислити відповідне значення для X з рівняння 1.8. Зокрема, він може згодом обчислити

$$C_J := \sum_{j\in J} b_{(1,j)_{.b}} + \sum_{j\in J} a^{\sigma}_{(1,j)_{.a}} \qquad (1.9)$$

Важливо зазначити, що в рівнянні 1.9 залишаються невідомими обидві суми $\sum_{j\in J} b_{(1,j)_{.b}}$, $\sum_{j\in J} a^{\sigma}_{(1,j)_{.a}}$. Для простоти слід визначити

$$b_J := \sum_{j \in J} b_{(1,j)_{.b}} \qquad (1.10)$$

$$a_J^{\sigma} := \sum_{j \in J} a_{(1,j)_{.a}}^{\sigma}$$

Таким чином

$$C_J = b_J + a_J^{\sigma}, \qquad (1.11)$$

де значення у правій частині рівняння не визначені. Потрібно визначити σ, щоб відновити значення b_J і таким чином отримати часткову інформацію про β. З іншого боку, знання β призвело б до реконструкції σ.

Що стосується атаки на b_J, за її допомогою супротивник прагне визначити значення для b_J, щоб отримати рівняння виду $a_J^{\sigma} = C_J - b_J$ для σ, причому, a_J відомий. Він спробує побудувати систему цих лінійно незалежних рівнянь, а потім спробує розв'язати систему, щоб визначити σ. Тепер, оскільки елементи в першому блоці $B_1 = [b_{11}, \dots, b_{1r_1}]$ з β не відомі, йому потрібно вгадати значення b_J для даної парної підмножини J. Оскільки кожен b_J може приймати будь-яке значення з F_q де $q = 2^m$, і оскільки противнику потрібно щонайменше m рівнянь для відновлення, такий підхід призводить до складності розміру $O(q^m)$. Очевидно, такий тип атаки грубою силою неможливий, оскільки q є великим.

Існує більш тонка та складна атака на a_J, що використовує рівняння 1.11 для першого блоку γ. Атака описується наступним алгоритмом:

1) Визначити підмножини $J \subseteq \{1, \dots, r_1\}$ парного розміру, такий що $a_J = 0$ і зібрано рівняння $b_J = C_J$;
2) Спробувати розв'язати систему рівнянь з кроку 1 для множини невідомих $D_1 \subseteq B_1$;
3) Задати $D_1 = \{b_{1j_1}, \dots, b_{1j_r}\}$, використати $b_{1j_i} \in D_1$ з кроку 2, щоб побудувати нетривіальні рівняння виду $a_{J*}^{\sigma} = d_{J*}$, де $d_{J*} := C_{J*} - b_{J*}$ відомий та $J * \subseteq \{1, \dots, r_1\}$ є підмножиною парного розміру. Потім розв'язати систему цих рівнянь, щоб визначити σ.

Помітно, що для застосування цієї атаки розмір блоку B_1 повинен задовольняти умові $r_1 > m$. Якщо це не так, потрібно з'єднати блоки B_1 і $B_2, \dots, B_l$ (тобто $B_1 \otimes B_2 \otimes \dots \otimes B_l$), щоб утворити більший блок, що задовольняє

умові. Отже, для решти аналізу алгоритму атаки на неявно припущено, що $r_1 >> m$.

Перш ніж перейти до детального аналізу алгоритму, варто згадати, що якщо $a_J = 0$, то $a_J^\sigma = 0$. Рівняння $a_J = 0$ не дає жодної інформації про σ, однак воно дає рівняння для b_J, а саме $b_J = C_J$.

Зараз буде розглянуто складність трьох кроків алгоритму атаки на a_J:

1) Оскільки $a_{(1,j)_{,a}}$ відомі, найбільш ефективний спосіб визначення $a_J = 0$ для певної підмножини J – це використовувати атаку дня народження. Точніше –
   а) обрати дві непересічні випадкові підмножини J_1 і J_2 з $\{1, \dots, r_1\}$ такими, що $|J_1 \cup J_2|$ парні, та
   б) перевірити, чи $a_{J_1} = a_{J_2}$.
   в) Якщо це так, то знайдено $a_j = 0$, де $J = J_1 \cup J_2$. Така підмножина J породжує рівняння $b_J = C_J$. Знаходження підмножини J з $a_j = 0$ шляхом атаки дня народження має складність розміру приблизно $O(q^{1/2})$. На цьому кроці кожна парна підмножина J має розмір принаймні чотири, це тому, що всі елементи в кожному блоці α належать до різних класів класу за модулем Z, тобто $a_{(1,j)_{,a}} \neq a_{(1,h)_{,a}}$ для $h \neq j$. Звичайно, враховується припущення $\sum_{j\in\{1,\dots r_1\}} a_{(1,j)_{,a}=0}$. Цю умову буде обговорено в коментарі нижче.
2) Нехай $P = \{J_0 = \emptyset, J_1, \dots, J_w\}$ де $J_i \subseteq \{1, \dots, r_1\}$ – підмножина парного розміру з $|J_i| \geq 4$, така що $a_{J_i} = 0$ для $i \geq 1$. Нехай $\cup_{i=0}^{w} J_i = \{j_1, \dots, j_t\}$. Кожна підсума $a_j = 0$ з кроку (i) відповідає рівнянню $b_J = C_J$. Невідомими цих рівнянь є елементи $b_{1J_1}, \dots, b_{1J_t}$ з B_1. Нехай

$$E_P = \{b_J = C_J : J \in P\}.$$

Оскільки існує t невідомих, можливо розглядати коефіцієнти кожного рівняння в E_P як вектор у $F_2{}^t$, розглядати як векторний простір розмірності t над F_2. Кожен такий вектор 0-1 має парну вагу Хеммінга розміром щонайменше 4. Будь-яка лінійна комбінація двох таких векторів породжує вектор, що відповідає підсумі $a_j = 0$ з $J \in P$, а отже, і рівнянню в E_P. Іншими словами, вектори коефіцієнтів рівнянь у E_P охоплюють лінійний підпростір V у $F_2{}^t$, де кожен ненульовий вектор V має вагу щонайменше 4. І, отже, розмірність V не перевищує $t - 3$. Це еквівалентно тому, що за допомогою елементарних операцій з рядком матриця коефіцієнтів M будь-якої системи рівнянь з E_P буде перетворена в матрицю ешелонної форми рядка, для якої кожен рядок

обов'язково має вагу не менше 4. Отже, такий система рівнянь дає принаймні 3 параметри, які можливо вільно вибирати, тобто ранг M, позначений $rank(M)$, не перевищує $t-3$. Оскільки кожен параметр може приймати будь-яке значення з F_q, розв'язування рівнянь для $b_{1J} \in D_1$ на цьому кроці вимагає складності розміром щонайменше $O(q^3)$. Наявність точної оцінки $rank(M)$ видається важкою проблемою. Це пояснюється тим, що ранг M залежить від множини P, яка, у свою чергу, залежить від випадкових значень $a_{(1,i_1),a}, \dots, a_{(1,i_t),a}$.

Слід зауважити, що $t \geq 4$. Якщо $t = 4$, є $rank(M) = t - 3 = 1$. Цей факт легко побачити, оскільки $J *= \{j_1, j_2, j_3, j_4\}$ – єдина непорожня підмножина при $a_j = 0$. Отже, $b_{1J_1} + b_{1J_2} + b_{1J_3} + b_{1J_4} = C_J$ є єдиним можливим рівнянням з 4 невідомими, які можливо отримати.

Якщо $t > 4$, можливо довести ще сильнішу оцінку цього $rank(M) = t - 4$. Як і вище, слід позначити через V лінійний підпростір F_{2^t}, натягнутий векторами коефіцієнтів рівнянь у E_P. Якщо будь-який вектор з V має вагу щонайменше 6, розмірність V не перевищує $t-5$. І тому $rank(M) \leq t - 5 < t - 4$. Отже, можливо припустити, що V містить вектор v з вагою 4. Без втрати загальності можливо вважати, що v має вигляд $v = 111100 \dots 0$ (просто перейменувавши невідомі). Слід розглянути $w_4 = 111110 \dots 0 \in F_{2^t}$. Нехай $w_1 = 1000 \dots 0$, $w_2 = 0100 \dots 0$, $w_3 = 0010 \dots 0$. Тоді $w_1, w_2, w_3, w_4 \in V$. Нехай W – підпростір F_{2^t}, натягнутий на w_1, w_2, w_3, w_4. Тоді W має розмірність 4. Можливо перевірити, що $x + v$ має вагу не більше 3 для 14 ненульових векторів $x \in W$, тобто $x \neq W$, за винятком $x = y = 000110 \dots 0 \in W$. Але $y \neq V$, оскільки його вага дорівнює 2. Отже, є $W \cap V = \{0\}$. Отже, розмірність V не перевищує $t-4$. Отже, $rank(M) \leq t - 41$. Щоб продовжити атаку, потрібно вгадати значення принаймні для 4 невідомих $b_{1j} \in F_{2^t}$. Тому складність кроку 2 у цьому випадку становить принаймні $O(q^4)$. Наступний крок:

3) Нехай $D_1 = \{b_{1j_1}, \dots, b_{1j_r}\}$ – підмножина, визначена після кроку 2. Для того, щоб можливо було відновити $\sigma \in GL(m, 2)$ необхідно виконання умови $t \geq m$. Використовуючи елементи в D_1, супротивник може побудувати ненульову підсуму $a_J^\sigma = C_J - b_J \neq 0$ з рівняння 1.10 і спробувати розв'язати таку систему рівнянь для відновлення σ. Це можливо зробити за поліноміальний час. Причому, $t \geq m > 4$. Результат цієї атаки фіксується в наступній пропозиції.

Складність, необхідна для відновлення ключа, еквівалентного закритому ключу $[\beta, \mathrm{f}, \mathrm{t}_0, \dots, \mathrm{t}_\mathrm{s}]$ за допомогою алгоритму вище досягає розміру щонайменше $\mathrm{O}(\mathrm{q}^5 \cdot \mathrm{q}^{1/2})$.

Ця складність складається зі:

- складності $O(q^{1/2})$ вибору правильного значення для $t_{(0)_{.a}}$ в тричлені 1.8,
- складності $O(q^{1/2})$ атаки дня народження на кроці 1 та складності розміру щонайменше $O(q^4)$ розв'язування рівнянь для $b_{1,j}$ на кроці 2.

Визначити кращу нижню межу робочого навантаження для відновлення приватного ключа системи є складною відкритою проблемою. Завдання видається складним.

Помітно, що верхня межа для рангу матриці M, отримана на кроці 2 вище, далека від свого фактичного значення, оскільки, щоб спростити обговорення, не було накладено жодних обмежень на $a_{1,j}$, тобто в аргументації вільно використовується всі можливі значення для $a_{1,j}$, коли оцінюється розмірність V. Очевидно, розмірність V залежить від вибору $a_{1,j}$. Можливо очікувати, що розмірність V набагато менша, як і $rank(M)$. Тому складність атаки на a_j набагато вище, ніж $O(q^5 \cdot q^{1/2})$. Можливо припустити, що значення $t - rank(M)$ збільшуються пропорційно зростанню t (тобто $rank(M)$ стає пропорційно меншим, коли t стає більше).

На кроці 2 алгоритму атаки вище враховується припущення $\sum_{j\in\{1,\dots,r_1\}} a_{(1,j)_{.a}} = 0$. Якщо цю умову вилучити, то $\sum_{j\in\{1,\dots,r_1\}} a_{(1,j)_{.a}} \neq 0$. Припущено, що вгадано значення для $u = \sum_{j\in\{1,\dots,r_1\}} b_{(1,j)_{.b}}$. Це можливо зробити зі складністю $O(q)$. Отже, кожна підсума $a_j = 0$, отримана в результаті атаки дня народження, ймовірно, дає $C_K - (u - b_j) = a_K = \sum_{j\in K} a_{(1,j)_{.a}} \neq 0$, де $K = \{1, \dots, r_1\}$. Кожному $a_K \neq 0$ відповідає нетривіальне лінійне рівняння для σ. Отже, якщо супротивник збирає m лінійно незалежних рівнянь, він може відновити σ, як у кроці 3. У цьому випадку складність відновлення ключа еквівалентна закритому ключу $[\beta, f, t_0, \dots, t_s]$ зменшиться до $O(q^5 \cdot q^{1/2})$.

Можливо передбачити подальший метод відновлення σ з рівняння $b_J + a_J^{\sigma} = C_J$. Два основних кроки наступного алгоритму описують цю атаку:

1) Побудувати $2m$ лінійно незалежних векторів розміром $2m$ над F_2, щоб сформувати $2m \times 2m$ регулярну двійкову матрицю A. Кожен рядок A має вигляд $a_J || b_J$, де a_J і b_J розглядаються як вектори довжини m над F_2.
2) Нехай M позначає матрицю $2m \times m$, рядки якої є C_J. M відомий після вибору $t_{(1)_{.a}}$. Обчислити двійкову матрицю X розміром $2m \times m$ таку, що $A \cdot X = M$, тобто $X = A^{-1} \cdot M$.

Далі докладніше про алгоритм атаки на a_j та b_j. Слід задати:

$$X \coloneqq \begin{pmatrix} \sigma^* \\ Y \end{pmatrix}$$

σ^* – двійкова матриця $m \times m$. Будь-яка матриця A, побудована на кроці 1, дає матрицю $X = A^{-1} \cdot M$, оскільки відомо M. Кожен рядок A приймає значення $a_J || b_J$, що відповідає підмножині індексу J парного розміру. Першу частину a_J можливо обчислити, оскільки $a_{(1,j)_a}$ відомі, але потрібно вгадати значення для b_J (вектор бітів m) з невідомих $b_{(iJ)}$, оскільки вони є частиною приватного ключ. Отже, існує q можливих варіантів для кожного рядка A, що відповідає q можливих значень для b_J. Якщо всі $2m$ рядків A вибрано правильно (тобто кожне значення b_J вгадане правильно), матриця X матиме вигляд

$$X \coloneqq \begin{pmatrix} \sigma \\ I \end{pmatrix},$$

де I – тотожна матриця $m \times m$. Це означає, що складність успішної реконструкції σ (тобто $\sigma^* = \sigma$), після того як визначено всі $2m$ рядків A, дорівнює $O(q^{2m})$. У цьому випадку $Y = I$.

Відповідним наслідком комбінованої атаки є наступний факт. Якщо логарифмічний підпис $\beta = (b_{ij})$ має вигляд $\beta = (b_{ij}) = (e_{ij})^{\sigma_1}$, де (e_{ij}) відомі, σ_1 – невідома регулярна матриця $m \times m$ над F_2, то ця атака дозволить відновити σ та σ_1 також. Причину можливо побачити в наступному. Рівняння 1.11 тепер можливо записати як $a_J^{\sigma} + b_j = a_J^{\sigma} + e_J^{\sigma_1} = C_J$. Якщо на кроці 1 можливо побудувати регулярну матрицю $2m \times 2m$ A з рядками виду $a_J || e_J$, то матриця $X = A^{-1} \cdot M$, отримана на етапі (b), матиме вигляд

$$X \coloneqq \begin{pmatrix} \sigma \\ \sigma_1 \end{pmatrix},$$

тобто можливо відновити σ та σ_1. Видно, що це можливо лише тому, що обидва $a_{(1,j)_a}$, $e_{(1j)}$ повністю відомі. Висновками з обговорення аналізу безпеки прямих атак є наступні результати.

Порівнюючи три атаки, представлені в цьому розділі, стає помітним, що найсильніша з них, атака на a_j, дає фактичну оцінку робочого навантаження, необхідного для відновлення ключа, еквівалентного закритому ключу. Робоче навантаження обмежено нижче $O(q^5 \cdot q^{1/2})$, де $q = \sqrt{|G|}$.

Нехай $\alpha \coloneqq S(a_{(1,j)_a}, a_{(1,j)_b})$ буде покриттям, що використовується в

налаштуванні MST_3, таким, що $a_{(1,j)_{.a}} \in H < Z$, де H – підгрупа Z порядку $q_0 = 2^l$. Тоді нижня оцінка, задана твердженням про робоче навантаження вище, стає $O(q^4 \cdot q^{1/2})$. Межа зумовлена тим, що в попередньому аналізі кількість можливих варіантів для $\mathrm{t}(1/\mathrm{a})$ та робоче навантаження, необхідне для атаки дня народження на кроці 1 алгоритму атаки, буде зменшено залежно від порядку H.

Далі розглядається детально вибрана атака відкритого тексту на MST_3, коли використовуються трансверсальні логарифмічні підписи. Це той випадок, коли β генерується без застосування кроку злиття. Насправді, ці логарифмічні підписи можливо по суті розглядати як підписи з ланцюжка підгруп Z. Однак структура β буде змінена, якщо буде застосований крок злиття.

Атака перестановкою матриць, розроблена в цьому розділі, видається потужною, оскільки вона надає доказ того факту, що клас незлитих трансверсальних логарифмічних підписів не може бути використаний у реалізації MST_3. Однак клас об'єднаних трансверсальних логарифмічних підписів витримує атаку перестановкою матриць, як показано нижче.

Перш ніж представити атаку з перестановкою матриць, потрібно згадати дві прості атаки, які природно виникають із представлення елементів у Сузукі 2 групи.

Перша атака – атака базису. Виходячи з опису схеми, $.a$ частина γ є просто випадковими покриттями для центру Z. Z є векторним простором розмірності m над F_2 і Z також ототожнюється з F_q. Тому елементи Z також називаються векторами. Нехай через $\alpha_{.a}$ покриття Z, блоки якого утворюють $.a$ частину α, буде визначено $J := \breve{\alpha}_{.a}(Z_{|Z|})$. Таким чином, J є підмножиною Z, і відношення $p := |Z|/|J|$ можливо розглядати як середню кількість представлень для кожного елемента J щодо $\alpha_{.a}$. Точніше, завдяки зв'язку між генерацією випадкових покриттів і проблемою заповнюваності [11] можливо отримати наближення для відношення, задане наступною формулою

$$p \approx \lambda\left(\frac{e^{\lambda}}{e^{\lambda}-1}\right),$$

де $\lambda = (1/|Z_1|)\prod_{i=1}^{s} r_i$ та $(r_i, \dots, r_s)$ – тип $\alpha_{.a}$, а Z_1 – найменша підгрупа Z, що містить J. В рамках лінійної алгебри можливо знайти максимальну підмножину лінійно незалежних векторів, які походять з усіх блоків $\alpha_{.a}$. Використовуючи двостороннє перетворення на $\alpha_{.a}$, можливо припустити, що перші блоки $s-1$ містять нульовий вектор. Лінійно незалежні вектори разом із нульовими

векторами утворюють покриття, що дозволяє ефективно факторизувати певну кількість зашифрованих текстів, створених $\alpha_{.a}$. Ця сума становить приблизно $(1/p)\prod_{i=1}^{s}(k_i+1)$, де $k_i = \lceil log_2 r_i \rceil$. Тому ймовірність того, що даний зашифрований текст може бути правильно розшифрований, визначається як

$$\approx \frac{1}{p}\prod_{i=1}^{s}\frac{(k_i+1)}{r_i}.$$

В результаті, якщо p або/та r_i збільшити, ця ймовірність буде зменшена. Отже, якщо вибрати елементи $\alpha_{.a}$ з підпростору Z_1 у Z так, що $p = |Z|/|Z_1|$ є великим, то ця проста атака стає нездійсненною.

Також існує тривіальна атака грубої сили на будь-яке випадкове покриття δ, яка для даного $y = \check{\delta}(x)$ намагається визначити x за допомогою методу компромісу часу та пам'яті. Цей тип атаки загалом називається атакою «Зустріч посередині».

Для MST$_3$ це описується наступним чином. Частину $.a$ тобто, $a := (a_{ij.a})$, можливо розглядати як випадкове покриття типу $(r_i, \dots, r_s)$ для центру Z. Припущено, що $y_{.a} = \check{\alpha}_{.a}(x)$ дано для деякого $x \leftrightarrow (j_1, \dots, j_s)$.

Отже, можливо написати $y_{.a} = \check{\delta}_1(x_1) \cdot \check{\delta}_2(x_2)$, де:

$$x_1 = (j_1, \dots, j_{\lfloor s/2 \rfloor}),\ x_2 = (j_{\lfloor s/2 \rfloor+1}, \dots, j_s) \text{ та}$$
$$\check{\delta}_1(x_1) = \sum_{i=1}^{\lfloor s/2 \rfloor} a_{ij.a},\ \check{\delta}_2(x_2) = \sum_{j_{\lfloor s/2 \rfloor+1}}^{s} a_{ij.a}.$$

Тут $\delta_1 := (a_{ij.a})$, $i = 1, \dots, \lfloor s/2 \rfloor$; $j = 1, \dots, r_i$, і $\delta_1 := (a_{ij.a})$, $i = \lfloor s/2 \rfloor + 1, \dots, s$; $j = 1, \dots, r_i$. Спочатку слід побудувати таблицю T усіх можливих пар (u, v) з $u = u_1, \dots, u_{\lfloor s/2 \rfloor}$, $u_i \in F_{2^{r_i}}$ і $v \in \check{\delta}_1(u)$. Розмір T приблизно дорівнює $O(\sqrt{q})$.

Атака працює наступним чином: для кожного обраного $w = (u_{\lfloor s/2 \rfloor+1}, \dots, u_s)$, $u_i \in F_{2^{r_i}}$, слід обчислити добуток $g = y_{.a} \cdot \left(\check{\delta}_2(w)\right)\text{^}(-1)$. Якщо є пара (u, v) в T така, що $g = v$, то існує $x \leftrightarrow u||w$, наприклад $x \leftrightarrow (u_1, \dots, u_{\lfloor s/2 \rfloor}, u_{\lfloor s/2 \rfloor+1}, \dots u_s)$. У середньому потрібно побудувати $O(\sqrt{q})$ значень для g, поки не отримано $g = v$.

Таким чином, ця атака вимагає пам'яті $O(\sqrt{q})$ і часу $O(\sqrt{q})$. При цьому, якщо $\alpha_{.a}$ побудовано з підпростору Z_1 простору Z так, що $p = |Z|/|Z_1|$ є великим, атака «Зустріч посередині» не може бути застосована.

Тепер буде представлено атаку матричної перестановки на реалізацію MST_3, що використовує незлитий трансверсальний логарифмічний підпис β (коротко називається NFT-MST_3). Це сильна атака є обраним типом атаки із відкритим текстом, яка намагається змінити функцію шифрування системи. Основна ідея атаки перестановки матриць полягає в тому, щоб побудувати серію матриць і відновити перестановки, що використовуються при генерації β, які в кінцевому підсумку дозволять противнику розшифрувати будь-який заданий шифртекст.

Нехай $\omega := (w_{ij})$ буде покриттям типу $(r_1, \dots, r_i)$ для G і нехай $x \in Z_{|Z|}$ відповідає $(j_1, \dots, j_i) \in Z_{r_1} \otimes \dots \otimes Z_{r_s}$. Нехай $\xi \in S_S$ і $v_l := l^{\xi}$ для $l \in \{1, \dots, s\}$. Тоді:

$$\breve{\omega}_{k,\xi}(x) := \prod_{i=1}^{k} w_{v_i, j_{v_i}}. \qquad (1.12)$$

Що стосується схеми NFT-MST_3, нехай $[\alpha, \gamma]$ будуть відкритим ключем із відповідним закритим ключем $[\beta, f, t_0, \dots, t_s]$. Нагадується, що $\alpha := (a_{i.j_i})$, $\beta := (b_{i,j_i})$ та $\gamma := (h_{i.j_i})$ мають тип $(r_1, \dots, r_s)$ і що ξ є перестановкою, використаною на кроці 5 $\pi_1, \dots, \pi_s$ – перестановки, використані на кроці 4 алгоритму генерації логарифмічного підпису.

Нехай α, β, γ будуть покриттями типу $(r_1, \dots, r_s)$ як описано вище. Нехай $x \in Z_{|Z|}$ відповідає $(j_1, \dots, j_i) \in Z_{r_1} \otimes \dots \otimes Z_{r_s}$ і $v_l := l^{\xi}$ для $l \in \{1, \dots, s\}$. Далі нехай $\breve{\alpha}_{l,\xi}(x)$, $\breve{\beta}_{l,\xi}(x)$, $\breve{\gamma}_{l,\xi}(x)$ – значення, обчислені за рівнянням 1.12. Нехай $k_l := \lceil log_2 r_l \rceil$. Тоді існує двійкова $(2m+1) \times k_{v_l}$ матриця M_{v_l} така, що

$$\left(\breve{\alpha}_{l,\xi}(x)_{.a} \middle|\middle| \breve{\alpha}_{l,\xi}(x)_{.b} + \breve{\gamma}_{l,\xi}(x)_{.b} \middle|\middle| 1\right) M_{v_l} = \pi_{v_l}(j_{v_l}), \qquad (1.13)$$

де «1» – біт, встановлений на одиницю. Щоб довести це, спочатку слід показати, що існує двійкова $(2m+1) \times m$ матриця N_{v_l} така, що

$$\left(\breve{\alpha}_{l,\xi}(x)_{.a} \middle|\middle| \breve{\alpha}_{l,\xi}(x)_{.b} + \breve{\gamma}_{l,\xi}(x)_{.b} \middle|\middle| 1\right) N_{v_l} = \breve{\beta}_{l,\xi}(x)_{.b}. \qquad (1.14)$$

Слід почати з рівняння:

$$\breve{\alpha}_{l,\xi}(x)_{.b} + \breve{\gamma}_{l,\xi}(x)_{.b} = \sum_{i=1}^{l} b_{(v_i, j_{v_i}).b} + t_{(0).a} \sum_{i=1}^{l} a^{\varsigma}_{(v_i, j_{v_i}).a} +$$
$$+ t^{\theta}_{(v_l).a} \sum_{i=1}^{l} a_{(v_i, j_{v_i}).a} + C_l$$

де $C_l = t_{(0).b} + t_{(v_l).b}^{\theta-1} + t_{(v_l).b} + t_{(0).a} t_{(v_l).a}^{\theta}$. Оскільки елементи $t_{(0).a}, t_{(v_l).a} \in F_q$ є константами, добутки $t_{(0).a} \sum_{i=1}^{l} a_{(v_i, j_{v_i}).a}^{\theta}$ та $t_{(v_l).a}^{\theta} \sum_{i=1}^{l} a_{(v_i, j_{v_i}).a}$ є лінійними відображеннями. Тому існують двійкові $m \times m$ матриці T_0 і T_{v_l} такі, що

$$t_{(0).a} \sum_{i=1}^{l} a_{(v_i, j_{v_i}).a}^{\theta} = \sum_{i=1}^{l} a_{(v_i, j_{v_i}).a} T_0$$

$$t_{(v_l).a}^{\theta} \sum_{i=1}^{l} a_{(v_i, j_{v_i}).a} = \sum_{i=1}^{l} a_{(v_i, j_{v_i}).a} T_{v_l}$$

З цього випливає множина

$$N_{v_l} = \begin{pmatrix} T_0 + T_{v_l} + \sigma \\ I_m \\ C_l \end{pmatrix}$$

де I_m – тотожна матриця $m \times m$. Тепер неважко перевірити, що $(2m+1) \times m$ матриця N_{v_l} задовольняє рівнянню 1.14. Якщо задати $\varepsilon' := (e_{ij}{}')$ з $e'_{ij} = b_{i,j}^{\varsigma^{-1}}$, тоді

$$\left(\check{\beta}'_{l,\xi}(x)_{.b}\right)^{\varsigma^{-1}} = \left(\check{\varepsilon}'_{l,\xi}(x)_{.b}\right).$$

Далі розглядається лінійне відображення φ_l, визначене наступним чином:

$$\check{\varepsilon}^{*}_{l,id}(x)_{.b} = \sum_{i=1}^{l} e^{*}_{(i,j_i).b} \longmapsto j_l,$$

де id є перестановкою ідентичності. Це відображення добре визначене для класу трансверсальних логарифмічних підписів, зокрема для ε^{*}, створеного в алгоритмі генерації підпису. j_l є двійковим представленням індексу для e_{l,j_l} та є ідентичним k_l бітовому вектору e_{l,j_l} в позиціях K_l. Нехай $\varepsilon'' := e_{ij}{}''$ отримано з ε^{*} на кроці 4 алгоритму генерації логарифмічного підпису. φ_l діє на $\check{\varepsilon}''_{l,id}(x)_{.b}$ наступним чином:

$$\check{\varepsilon}''_{l,id}(x)_{.b} = \sum_{i=1}^{l} e''_{(i,j_i).b} \longmapsto \pi_l(j_l).$$

Застосовуючи крок 5 алгоритму до ε'', отримано ε'. Тому φ_l діє на

$\check{\varepsilon}'_{l,\xi}(x)_{.b}$ відповідно до трансформації:

$$\check{\varepsilon}'_{l,id}(x)_{.b} = \sum_{i=1}^{l} e'_{\left(v_i, j_{v_i}\right).b} \longmapsto \pi_{v_i}\left(j_{lv_i}\right).$$

Якщо задати матрицю M_{v_l} як

$$M_{v_l} \coloneqq N_{v_l} \cdot \varsigma^{-1} \cdot P_{v_l},$$

тоді M_{v_l} – двійкова матриця, яка задовольняє рівнянню 1.13.

Нехай $M_{l,p}$ позначає p-й стовпець матриці M_l, де $p = 1, \dots, k$. Можливо спостерігати, що $\pi_l(j_l)$ є двійковим вектором довжини k_l. Аналогічно позначається $\pi_{l,p}(j_l)$ p-ий біт $\pi_l(j_l)$.

Використовуючи це позначення та твердження, де визначено ξ, є наступна пропозиція. Нехай $v_l \coloneqq l^{\xi}$ і $M_{v_l,p}$ – p-й стовпець M_{v_l} та $\pi_{v_l}\left(j_{lv_l}\right)$ – p-й біт $\pi_{v_l}\left(j_{lv_l}\right)$. Тоді

$$\left(\check{\alpha}_{l,\xi}(x)_{.a} \middle|\middle| \check{\alpha}_{l,\xi}(x)_{.b} + \check{\gamma}_{l,\xi}(x)_{.b} \middle|\middle| 1\right) M_{v_l,p} = \pi_{v_l}\left(j_{lv_l}\right). \qquad (1.15)$$

Нехай α, β, γ будуть покриттями типу $(r_1, \dots, r_s)$ як описано вище. Нехай $x \in Z_{|Z|}$ відповідає $(j_1, \dots, j_i) \in Z_{r_1} \otimes \dots \otimes Z_{r_s}$ і $v_l \coloneqq l^{\xi}$. Далі нехай $v_l \coloneqq l^{\xi}$ для $l \in \{1, \dots, s\}$ $k_l \coloneqq \lceil log_2 r_l \rceil$. Тоді існує двійкова $(2m+1) \times m$ матриця L_{v_l} така, що

$$\left(\check{\alpha}(x)_{.a} + A_l \middle|\middle| \check{\alpha}(x)_{.b} + \check{\gamma}(x)_{.b} + B_l \middle|\middle| 1\right) L_{v_l} = \pi_{v_l}\left(j_{lv_l}\right), \qquad (1.16)$$

де

$$A_l \coloneqq \sum_{i=l=1}^{s} a_{\left(v_i, j_{v_i}\right).a},$$

$$B_l \coloneqq \sum_{i=l+1}^{s} \left(a_{\left(v_i, j_{v_i}\right).b} + h_{\left(v_i, j_{v_i}\right).b}\right) + \sum_{i=l+1}^{s} a^{\theta}_{\left(v_i, j_{v_i}\right).b} \left(t_{(0).b} + t_{(v_{i-1}).a}\right) +$$

$$+ \sum_{i=l=1}^{s} \left(a_{\left(v_i, j_{v_i}\right).b} \left(t_{(v_i).a} + t_{(s).a}\right)^{\theta}\right)$$

де $l \in \{1, \dots, s\}$, $A_s = B_s = (0, \dots, 0)$ та «1» – біт, встановлений на одиницю.

Для l=s рівняння 1.16 отримано з пропозиції вище. Отже, відтепер буде вважатись, що $l \in \{1, \dots, s-1\}$. Для цього потрібні наступні рівняння:

$$\breve{\alpha}(x)_{.a} + \sum_{i=l+1}^{s} a_{\left(v_i, j_{v_i}\right).a} = \sum_{i=1}^{l} a_{\left(v_i, j_{v_i}\right).a}$$

$$\breve{\beta}(x)_{.b} + \sum_{i=l+1}^{s} b_{\left(v_i, j_{v_i}\right).b} = \sum_{i=1}^{l} b_{\left(v_i, j_{v_i}\right).b}$$

Спочатку буде показано, що існує двійкова матриця $(2m+1) \times m$ N_{v_l} така, що

$$\left(\sum_{i=1}^{l} a_{\left(v_i, j_{v_i}\right).a} \left|\left|\breve{\alpha}(x)_{.a} + \breve{\gamma}(x)_{.b} + B_l\right|\right| 1\right) N_{v_l} = \\ = \sum_{i=1}^{l} b_{\left(v_i, j_{v_i}\right).b}. \tag{1.17}$$

$$\breve{\alpha}(x)_{.a} + \breve{\gamma}(x)_{.b} + B_l = \breve{\alpha}(x)_{.a} + \breve{\gamma}(x)_{.b} + \sum_{i=l+1}^{s} \left(a_{\left(v_i, j_{v_i}\right).b} + h_{\left(v_i, j_{v_i}\right).b}\right) +$$
$$+ \sum_{i=l+1}^{s} a^{\theta}_{\left(v_i, j_{v_i}\right).b} \left(t_{(0).b} + t_{(v_{i-1}).a}\right) + \sum_{i=l=1}^{s} \left(a_{\left(v_i, j_{v_i}\right).b} \left(t_{(v_i).a} + t_{(s).a}\right)^{\theta}\right) =$$

$$= \sum_{i=1}^{l} b_{\left(v_i, j_{v_i}\right).b} + \sum_{i=1}^{l} a^{\varsigma}_{\left(v_i, j_{v_i}\right).a} + t_{(0).b} + t^{\theta+1}_{(0).a} + t_{(s).b} + t_{(0).a} t^{\theta}_{(s).a} +$$
$$+ t_{(0).a} \sum_{i=1}^{l} a^{\theta}_{\left(v_i, j_{v_i}\right).a} + t^{\theta}_{(s).a} \sum_{i=1}^{s} a_{\left(v_i, j_{v_i}\right).a} + \sum_{i=l+1}^{l} b_{\left(v_i, j_{v_i}\right).b} +$$
$$+ \sum_{i=l+1}^{l} a^{\varsigma}_{\left(v_i, j_{v_i}\right).a} + + \sum_{i=l+1}^{l} \left(t_{(v_{i-1}).a} a^{\theta}_{\left(v_i, j_{v_i}\right).a} + a_{\left(v_i, j_{v_i}\right).a} t^{\theta}_{(v_i).a} +\right.$$
$$\left. + t_{(v_{i-1}).a} t^{\theta}_{(v_i).a} + t_{(v_{i-1}).b} + t^{\theta+1}_{(v_{i-1}).a} + + t_{(v_i).b}\right) + t_{(0).a} \sum_{i=l+1}^{l} a^{\theta}_{\left(v_i, j_{v_i}\right).a} +$$
$$+ \sum_{i=l+1}^{s} a^{\theta}_{\left(v_i, j_{v_i}\right).a} t^{\theta}_{(v_{i-1}).a} + + \sum_{i=l+1}^{s} a_{\left(v_i, j_{v_i}\right).a} t^{\theta}_{(v_i).a} + t^{\theta}_{(s).a} \sum_{i=l+1}^{s} a_{\left(v_i, j_{v_i}\right).a} =$$
$$= \sum_{i=1}^{l} b_{\left(v_i, j_{v_i}\right).b} + \sum_{i=l}^{l} a^{\varsigma}_{\left(v_i, j_{v_i}\right).a} + + t_{(0).a} \sum_{i=l+1}^{l} a^{\theta}_{\left(v_i, j_{v_i}\right).a} +$$
$$+ t^{\theta}_{(s).a} \sum_{i=1}^{s} a_{\left(v_i, j_{v_i}\right).a} + C_l,$$

де змінна

$$C_l = \sum_{i=l+1}^{l} \left(t_{(v_{i-1}).a} t^{\theta}_{(v_i).a} + t^{\theta}_{(v_{i-1}).b} + t^{\theta+1}_{(v_{i-1}).a} + t_{(v_i).b}\right) + t_{(0).b} + t^{\theta+1}_{(0).a} + \\ + t_{s.b} + t_{(0).a} t^{\theta}_{s.a}$$

розглядається як константа в F_{2^m}. Отже, рівняння 1.17 стає таким:

$$\left(\sum_{i=1}^{l} a_{\left(v_i, j_{v_i}\right).a} \left|\right| \sum_{i=1}^{l} b_{\left(v_i, j_{v_i}\right).b} + \sum_{i=l}^{l} a^{\varsigma}_{\left(v_i, j_{v_i}\right).a} + + t_{(0).a} \sum_{i=l+1}^{l} a^{\theta}_{\left(v_i, j_{v_i}\right).a} + t^{\theta}_{(s).a} \sum_{i=1}^{s} a_{\left(v_i, j_{v_i}\right).a} + C_l \left|\right| 1\right) N_{v_l} = \quad (1.18)$$

$$= \sum_{i=1}^{l} b_{\left(v_i, j_{v_i}\right).b},$$

де I_m – тотожна матриця $m \times m$. Тоді легко перевірити, що матриця $(m2 + 1) \times m$ N_{v_l} задовольняє рівнянню 1.18. Подібно до доведення пропозиції вище, використовуючи рівняння:

$$\left(\sum_{i=1}^{l} b_{\left(v_i, j_{v_i}\right).b}\right) \varsigma^{-1} = \sum_{i=1}^{l} e'_{\left(v_i, j_{v_i}\right).b} := \check{\varepsilon}_{l,\xi}{}'(x)_{.b},$$

$$\left(\check{\varepsilon}_{l,\xi}{}'(x)_{.b}\right) P_{v_l} = \pi_{v_l}\left(j_{v_l}\right),$$

можливо визначити $L_{v_l} := N_{v_l} \varsigma^{-1} \cdot P_{v_l}$. Тоді L_{v_l} – двійкова матриця, що задовольняє рівнянню 1.16. Тепер можливо описати алгоритм відновлення перестановок $\pi_1, \dots, \pi_s$ для атаки перестановкою матриць. Алгоритм також забезпечує перестановку ξ. Вхідними даними є відкритий ключ $[\alpha, \gamma]$, вихідними – перестановки $[\pi_1, \dots, \pi_s, \xi]$. Алгоритм:

1) Обрати випадковий відкритий текст $x^i \longmapsto \left(j_1^{(i)}, \dots, j_s^{(i)}\right)$, і побудувати вектори $y^{(i)} := \left(\check{\alpha}_{l,id}(x)^{(i)}_{.a} \left| \left| \check{\alpha}_{l,id}(x)^{(i)}_{.b} + \check{\gamma}_{l,id}(x)^{(i)}_{.b} \right| \right| 1\right)$, як у пропозиції вище. Визначити n_l як максимальну кількість лінійно незалежних векторів $y^{(i)}$, де $n_l = n'_l + 1 + \sum_{m=1}^{l} k_m$. Тут n'_l – максимальна кількість лінійно незалежних стовпців матриці, утворених векторами $\left(\check{\alpha}_{l,id}(x)^{(i)}_{.a}\right)$;
2) Задати множину $v \longleftarrow 1$;
3) Починаючи з $p \longleftarrow 1$ та закінчуючи k_v:
   а) Обирати множини J_v із k_v випадково вибраних векторів у $F_{2^{k_v}}$;
   б) Обирати випадкові двійковий вектор $w = \left(w_1, \dots, w_{k_v}\right)$ та множину $\pi_{w,p}(j_i) = w_i$ для кожного $j_i \in J_v$;
   в) Обирати випадковий відкритий текст $x^{(i)} \longmapsto \left(j_1^{(i)}, \dots, j_s^{(i)}\right)$, де $j_v^{(i)} \in J_v$, будувати вектор $y^{(i)} := \left(\check{\alpha}_{l,id}(x)^{(i)}_{.a} \left| \left| \check{\alpha}_{l,id}(x)^{(i)}_{.b} + \check{\gamma}_{l,id}(x)^{(i)}_{.b} \right| \right| 1\right)$. Повторяти цей крок для відповідної кількості варіантів $x^{(i)}$ і сформувати

матрицю Y_v з рядками, які є лінійно незалежними векторами $y^{(i)}$. Якщо $rank(Y_v) < n_l$, то повернутися до кроку 3.a;

г) Нехай $x^{(i)} \mapsto \left(j_1^{(i)}, \dots, j_v^{(i)}, \dots, j_s^{(i)}\right)$ для $(i) = 1, \dots, n_l$ буде відкритим текстом, використаним для побудови рядка (i) двійкової матриці $n_l \times (2m+1)$ Y_v на попередньому кроці. Сформувати $n_l \times 1$ матрицю $Z_{v,p}$ зі значенням $\pi_{v,p}\left(j_v^{(i)}\right)$ як запис у рядку (i);

д) Побудувати $(2m+1) \times n_l$ двійкову матрицю кодування E_v, таку, що $rank(Y_v \cdot E_v) = n_l$;

е) Обчислити матрицю $M_{v,p} = E_v \cdot (Y_v \cdot E_v)^{-1} \cdot Z_{v,p}$;

ж) Для кожного $j_v \in F_{2^{k_v}} \bigvee_v$ обрати випадковий відкритий текст $x^{(i)} \mapsto \left(j_1^{(i)}, \dots, j_v^{(i)}, \dots, j_s^{(i)}\right)$ і обчислити значення для $\pi_{v,p}(j_v)$ для $\pi_{v,p}(j_v) := \left(\breve{\alpha}_{l,id}(x)_{.a} \| \breve{\alpha}_{l,id}(x)_{.b} + \breve{\gamma}_{l,id}(x)_{.b} \| 1\right) M_{v,p}$;

з) Обрати випадковий відкритий текст $x \mapsto (j_1, \dots, j_v, \dots, j_s)$ і обчислити значення $y = \left(\breve{\alpha}_{l,id}(x)_{.a} \| \breve{\alpha}_{l,id}(x)_{.b} + \breve{\gamma}_{l,id}(x)_{.b} \| 1\right) M_{v,p}$;

и) Якщо $y \neq \pi_{v,p}(j_v)$, то повернутися до кроку 3.b і спробувати інший вибір для $w \in F_{2^{k_v}}$ (це можливо зробити щонайбільше 2^{k_v}). Якщо вибір w неможливий, задати $v \leftarrow (v+1)$ і повернутися до кроку 3. Якщо $\pi_{v,p}(j_v)$, повторити крок 3.h відповідну кількість разів;

4) Встановити транспонування $\xi_l := (v, l)$. Переставити блоки α та γ з використанням транспозиції ξ_l, щоб отримати α' і γ'. Задати $\alpha \leftarrow \alpha'$ та $\gamma \leftarrow \gamma'$;

5) Для кожного $j_v \in F_{2^{k_v}}$, використовуючи $\pi_{v,p}(j_v)$ для $p = 1, \dots, k_v$, отримано $\pi_v(j_v)$ і таким чином визначається перестановка π_v;

6) Повернути $[\pi_1, \dots, \pi_s, \xi]$, де $\xi = \xi_s \circ \dots \circ \xi_1$.

Слід зробити декілька уточнень відносно цього алгоритму. По кроках:

1) Щоб визначити максимальне значення для параметра n_l, потрібно виконати цей крок для достатньої кількості випадкових входів $x^{(i)}$.

2) Цей крок ініціалізує параметр v, щоб почати наступні кроки алгоритму для визначення $v = l^{\xi}$.

3) Внутрішній цикл використовується для визначення кожного біта $\pi_{v,p}(j_v)$ $\pi_v(j_v)$ для $p = 1, \dots, k_v$, окремо, для яких $\pi_v(j_v) := \left(\pi_{v,1}(j_v) \| \dots \| \pi_{v,k_v}(j_v)\right)$ для всіх $j_v \in F_{2^{k_v}}$;

а) Вибір параметра k_v, тобто розміру множини J_v, впливає на поведінку алгоритму. Якщо $|J_v| < k_v$, крок 3.c неможливо завершити (тобто завжди буде $rank(Y_v) < n_l$). Якщо $|J_v| > k_v$, робоче навантаження, необхідне на кроці 3.b, буде збільшено порівняно з випадком $|J_v| = k_v$;

б) На цьому кроці шукається p-й біт $\pi_{v,p}(j_v)$ $\pi_v(j_v)$ для всіх $j_v \in J_v$;

в) На цьому кроці відкритий текст $x^{(i)} \mapsto \left(j_1^{(i)}, \dots, j_v^{(i)}, \dots, j_s^{(i)}\right)$ вибирається таким чином, що компонент $j_i^{(i)}$ належить J_v (вибрано на кроці 3.a. Інші компоненти j_v з $u \neq v$ вибираються довільно. Повторюється цей крок, поки не буде отримано матрицю Y_v з $rank(Y_v) = n_l$. Якщо елементи J_v, $|J_v| = k_v$, обрані таким чином, що множина $\{\pi_v(j_v) \mid j_v \in J_v\}$ має менше k_v лінійно незалежних векторів (розміру k_v), $rank(Y_v)$ буде менше n_l. У цьому випадку алгоритм повертається до кроку (C.1) і генерує новий набір J_v. Іншою можливістю може бути розширення розміру набору J_v, тобто $|J_v| > k_v$;

г) Потрібно побудувати $n_l \times 1$ матрицю $Z_{v,p}$ зі значеннями $\pi_{v,p}\left(j_v^{(i)}\right)$ за допомогою значень з кроків 3.б і 3.в;

д) На цьому кроці буде побудовано двійкову $(2m+1) \times n_l$ матрицю E_v таку, що $rank(Y_v \cdot E_v) = n_l$. Це робиться таким чином: нехай $Q = \{1, \dots, 2m+1\}$ – індексний набір стовпців Y_v. Потрібно знайти підмножину $Q_v \subseteq Q$ з $|Q_v| = n_l$, таку, що всі стовпці з індексами в Q_v є лінійно незалежними. Існує тотожність $(2m+1) \times (2m+1)$ матриці $I_{(2m+1)}$. Слід видаліти усі стовпці $Q \backslash Q_v$ з індексами в $I_{(2m+1)}$, щоб сформувати матрицю $(2m+1) \times n_l$ E_v;

е) Використовуючи E_v з кроку (C.5), визначається p-й стовпець M_{vp} матриці M_v;

ж) На цьому кроці обчислюється p-ий біт $\pi_{v,p}(j_v)$ $\pi_v(j_v)$ для всіх інших $j_v \in F_{2^{k_v}}$;

з) На цьому етапі перевіряється, чи правильний біт $\pi_{v,p}(j_v)$ знайдено на кроці 3.b або обчислений на кроці 3.g для всіх $j_v \in F_{2^{k_v}}$, і чи задовольняє значення $v = l^{\xi}$. Виконання цього кроку достатню кількість разів дозволяє перевірити ці вимоги;

4) На цьому кроці використовується $v = l^{\xi}$, визначений у попередньому циклі, щоб побудувати транспозицію ξ_l. Оновлюється α шляхом переставлення блоків з використанням ξ_l та продовжується основний цикл з новим значенням $l \leftarrow (l-1)$;

5) З p-го розряду $\pi_{v,p}(j_v)$ для всіх $p = 1, \dots, k_v$ можливо побудувати $\pi_v(j_v)$. Зібравши всі $\pi_v(j_v), j_v \in F_{2^{k_v}}$, можливо відновити перестановку π_v.

Нехай α, γ будуть покриттями типу $(r_1, \dots, r_s)$, що використовуються як відкритий ключ у NFT-MST3. Нехай $l_k := \lceil \log_2 r_l \rceil$. Навантаження, необхідне для відновлення перестановок $[\pi_1, \dots, \pi_s, \xi]$ з використанням алгоритму атаки

перестановкою матриць, обмежено $O\left(\sum_{l=1}^{s} l k_l 2^{k_l-1}\right)$.

На кроці 3.б алгоритму потрібно вгадати вектор w з k_v бітів, щоб встановити p-й біт $\pi_{v,p}(j_v)$ з $\pi_v(j_v)$ для всіх $j_v \in J_v$. Складність алгоритму включає час, необхідний для проходження всіх бітів $p \in \{1, \dots, k_v\}$ із середнім значенням $l/2$ рази, доки крок 8.з успішно не завершиться шляхом знаходження $v := l^{\xi}$, а також кроків у головному циклі для $l \in \{1, \dots, s\}$. Підсумовуючи їх разом, буде отримано робоче навантаження у зазначеній межі.

Слід зауважити, що для будь-якого $j_m \in \{1, \dots, r_m\}$:

$$\left(t_{(0).a} + t_{(l-1).a}\right) = \sum_{m=1}^{l-1} \left(a_{(m,j_m).a} + h_{(m,j_m).a}\right) = \sum_{m=1}^{l-1} \left(a_{(m,1).a} + h_{(m,1).a}\right)$$

$$\left(t_{(0).a} + t_{(l-1).a}\right)^{\theta} = \sum_{m=l+1}^{s} \left(a_{(m,j_m).a} + h_{(m,j_m).a}\right)^{\theta} = \sum_{m=l+1}^{s} \left(a_{(m,1).a} + h_{(m,1).a}\right)^{\theta}$$

Пропозицію про складність відновлення перестановок можливо використати для розробки наступного алгоритму відновлення матриці для атаки. Вхідними даними є відкритий ключ $[\alpha, \gamma]$, вихідними – перестановки $[\pi_1, \dots, \pi_s, \xi]$. Алгоритм:

1) Задати $A_s \leftarrow (0, \dots, 0)$, m-бітовий нульовий вектор. Задати $v = l^{\xi}$;
2) Обрати випадковий відкритий текст $x^{(i)} \mapsto \left(j_1^{(i)}, \dots, j_s^{(i)}\right)$, і побудувати вектори $y^{(i)} := \left(\breve{\alpha}_{l,\xi}(x)_{.a}^{(i)} \middle| \breve{\alpha}(x)_{.b}^{(i)} + \breve{\gamma}(x)_{.b}^{(i)} + A_l^{(i)} \middle| 1\right)$, як у пропозиції вище. Задати n_v, максимальну кількість лінійно незалежних векторів $y^{(i)}$, де $n_v = n'_v + 1 + \sum_{m=1}^{l} k_{m^{\xi}}$. Тут n'_v – максимальна кількість лінійно незалежних стовпців матриці, утворених векторами $\breve{\alpha}_{l,\xi}(x)_{.a}^{(i)}$. Повторити цей крок для відповідної кількості варіантів $x^{(i)}$ і сформувати матрицю Y_v з n_v рядків, які є лінійно незалежними векторами $y^{(i)}$;
3) Нехай $x^{(i)} \mapsto \left(j_1^{(i)}, \dots, j_s^{(i)}\right)$ для $(i) = 1, \dots, n_v$ буде відкритим текстом, використаним для побудови рядка (i) двійкової матриці $n_v \times (2m+1)$ на попередньому кроці. Сформувати матрицю $n_v \times k_v$ Z_v зі значенням $\pi_v(j_v)$ як запис у рядку (i);
4) Побудувати матрицю двійкового кодування $(2m+1) \times n_v$, таку, що $rank(Y_v \cdot E_v) = n_v$;
5) Обчислити матрицю $L_v = E_v \cdot (Y_v \cdot E_v)^{-1} \cdot Z_v$. Якщо $l = 1$, то поверніть $[L_1, \dots, L_s]$;
6) Задати

$$A_{l-1} \leftarrow A_l + a_{(v,j_v).b} + h_{(v,j_v).b} + a^{\theta}_{(v,j_v).a} \sum_{m=1}^{l-1} \left(a_{(m^{\xi},1).a} + h_{(m^{\xi},1).a}\right) + a_{(v,j_v).a} \sum_{m=l+1}^{s} \left(a_{(m^{\xi},1).a} + h_{(m^{\xi},1).a}\right)^{\theta}$$

Використовуючи інформацію, обчислену за алгоритмами підготовки до атаки вище, представлено алгоритм для розшифрування поданого зашифрованого тексту $y = (y_1, y_2)$. Вхідними даними є $[\pi_1, \dots, \pi_s, \xi, L_1, \dots, L_s]$ для відкритого ключа $[\alpha, \gamma]$, зашифрований текст $y = (y_1, y_2)$. Вихідними даними є простий текст $x^{(i)} \mapsto \left(j_1^{(i)}, \dots, j_s^{(i)}\right)$ такий, що $y_1 = \breve{\alpha}(x)$, $y_2 = \breve{\gamma}(x)$. Алгоритм:

1) Задати $A_s \leftarrow (0, \dots, 0)$. Задати $v = l^{\xi}$;
2) Побудувати вектор $w = (y_{1.a} || y_{1.b} \oplus y_{2.b} \oplus A_l || 1)$;
3) Обчислити $\pi_v(j_v) = w \cdot L_v$;
4) Відновити j_v за допомогою $\pi_v(j_v)$ і перестановки π_v. Якщо $l = 1$, то повернути $(j_1, \dots, j_s)$;
5) Встановити $y_{1.a} \leftarrow y_{1.a} \oplus a_{(v,j_v).a}$,

$$A_{l-1} \leftarrow A_l + a_{(v,j_v).b} + h_{(v,j_v).b} + a^{\theta}_{(v,j_v).a} \sum_{m=1}^{l-1} \left(a_{(m^{\xi},1).a} + h_{(m^{\xi},1).a}\right) + + a_{(v,j_v).a} \sum_{m=l+1}^{s} \left(a_{(m^{\xi},1).a} + h_{(m^{\xi},1).a}\right)^{\theta}$$

Як наведено вище, атака перестановкою матриці на NFT-MST$_3$ використовує алгоритм для відновлення перестановок $[\pi_1, \dots, \pi_s, \xi]$, а потім алгоритм для побудови матриць $[L_1, \dots, L_s]$. Знання $[L_1, \dots, L_s]$ та $[\pi_1, \dots, \pi_s, \xi]$ дозволяє криптоаналітику розшифрувати будь-який зашифрований текст за допомогою алгоритму розшифрування. Використання незлитих трансверсальних підписів дозволяє побудувати таку матрицю L_i для будь-якого блоку $i = \{1, \dots, s\}$ і обчислити образ $\pi_i(j_i)$ при перестановці j_i, як показано в пропозиції вище. Цей факт використовується на кроці 3 алгоритму. Оскільки π_i є біекцією, прообраз j_i можливо відновити, якщо $\pi_i(j_i)$ відомий, як показано на кроці 4 того ж алгоритму.

Визначення перестановок $[\pi_1, \dots, \pi_s, \xi]$ і побудова матриць $[L_1, \dots, L_s]$ можливо розробити за єдиним алгоритмом. Однак такий алгоритм буде дуже заплутаним. Тому для наочності щодо опису атаки перестановкою матриць було представлено два окремих алгоритми.

Оскільки робоче навантаження, необхідне для алгоритму атаки, є незначним, складність атаки перестановкою матриць зводиться до складності визначення перестановок $[\pi_1, \dots, \pi_s, \xi]$ за відповідним алгоритмом. Отже, існує

наступна пропозиція.

Використовуючи ту саму нотацію, що й у пропозиції про обчислювальну складність вище, робоче навантаження, необхідне для відновлення відкритого тексту для поданого зашифрованого тексту за допомогою атаки перестановкою матриць на схемі NFT-MST$_3$, приблизно дорівнює такому ж обсягу, як і для відновлення перестановок $[\pi_1, \dots, \pi_s, \xi]$, і обмежена $O(\sum_{l=1}^{s} lk_l 2^{k_l-1})$.

Ця складність показує, зокрема, що для відносно малих значень k_i, які зазвичай використовуються в реальній версії схеми MST$_3$, ($k_l \leq 15$), незліті трансверсальні логарифмічні підписи не можуть бути використані для безпечної реалізації MST$_3$.

Далі буде визначено складність атаки перестановкою матриць на FT-MST$_3$. Як було показано попередньо, атака перестановкою матриць повністю використовує спосіб розкладання на множники щодо незлитого трансверсального логарифмічного підпису β, навіть якщо супротивник не знає β. Таким чином, знання, надані факторизацією щодо β, будуть вирішальною інформацією для оцінки складності відновлення відкритого тексту під час застосування атаки перестановкою матриць.

Щоб спростити опис атаки перестановкою матриць на FT-MST$_3$, його буде обмежено використанням лише кроку 1 та кроку 3 алгоритму створення логарифмічного підпису β.

Нехай $\{K_1, K_2, \dots, K_v\}$ – розбиття на множині $\{1, \dots, m\}$ з $|K_i| = k_i$ і $t_i = 2^{k_i}$, як описано в алгоритмі створення логарифмічного підпису. Нехай $\varepsilon^* := (e^*_{i,j})$ є підписом типу $(t_1, \dots, t_v)$, створеним після кроку 1 цього алгоритму.

Нехай $\beta := (b_{i,j})$ э логарифмічним підписом, створеним шляхом злиття блоків $(l, l+2)$ та $(l+1, l+3)$ в ε^*. (Жодні послідовні блоки не об'єднуються.) Тоді $\beta = [B_1, \dots, B_s]$ має тип $(r_1, \dots, r_s)$, де $r_l = t_l \cdot t_{l+2}$ і $r_{l+1} = t_{l+1} \cdot t_{l+3}$.

Нехай $u^{[n]}_{i,j_i}$ (відповідно $e^{[n]}_{i,j_i}$) – вектор довжини k_n, що складається з бітів b_{i,j_i} на позиціях, що відповідають K_n. Нехай $x \mapsto (j_1, \dots, j_s)$, також нехай $x' \mapsto (j'_1, \dots, j'_s)$, де $j'_l = j_l || j_{l+1}$ та $j'_{l+1} = j_{l+2} || j_{l+3}$. Тоді:

$$e^*_{1,j_1} = (\cdots || \quad \bar{0} \quad \cdots \quad \bar{0} \quad \cdots \quad \bar{0} \quad \cdots \quad \bar{0} \quad || \cdots)$$

$$e^*_{l-1,j_{l-1}} = (\cdots || \quad \bar{0} \quad \cdots \quad \bar{0} \quad \cdots \quad \bar{0} \quad \cdots \quad \bar{0} \quad || \cdots)$$

$$e^*_{l,j_l} = \left(\cdots || \quad e^{[l]}_{l,j_l} \quad \cdots \quad \bar{0} \quad \cdots \quad \bar{0} \quad \cdots \quad \bar{0} \quad || \cdots\right)$$

$$e^*_{l+1,j_{l+2}} = \left(\cdots \| \quad e^{[l]}_{l+1,j_{l+2}} \quad \cdots \quad e^{[l+1]}_{l+1,j_{l+2}} \quad \cdots \quad \bar{0} \quad \cdots \quad \bar{0} \quad \| \cdots\right)$$

$$e^*_{l+2,j_{l1+1}} = \left(\cdots \| \quad e^{[l]}_{l+2,j_{l+1}} \quad \cdots \quad e^{[l+1]}_{l+2,j_{l+1}} \quad \cdots \quad e^{[l+2]}_{l+2,j_{l+1}} \quad \cdots \quad \bar{0} \quad \| \cdots\right)$$

$$e^*_{l+3,j_{l1+3}} = \left(\cdots \| \quad e^{[l]}_{l+3,j_{l+3}} \quad \cdots \quad e^{[l+1]}_{l+3,j_{l+3}} \quad \cdots \quad e^{[l+2]}_{l+3,j_{l+3}} \quad \cdots \quad e^{[l+3]}_{l+3,j_{l+3}} \quad \| \cdots\right)$$

$$\breve{\beta}(x') = b_{1,j'_1} \oplus \ldots \oplus b_{l,j'_l} \oplus b_{l+1,j'_{l+1}} \oplus \ldots \oplus b_{s,j'_s},$$

де

$$b_{l,j'_l} = \left(\cdots \| \quad e^{[l]}_{l,j_l} \oplus \quad \cdots \quad u^{[l+1]}_{l+2,j_{l+1}} \quad \cdots \quad e^{[l+1]}_{l+2,j_{l+1}} \quad \cdots \quad \bar{0} \quad \| \cdots\right)$$

$$b_{l+1,j'_{l+1}} = \left(\cdots \| \quad \begin{matrix} e^{[l]}_{l,j_l} \\ u^{[l]}_{l+2,j_{l+1}} \end{matrix} \oplus \quad \cdots \quad \begin{matrix} u^{[l+1]}_{l+2,j_{l+1}} \\ e^{[l+1]}_{l+3,j_{l+3}} \end{matrix} \quad \cdots \quad e^{[l+2]}_{l+3,j_{l+3}} \quad \cdots \quad e^{[l+3]}_{l+3,j_{l+3}} \quad \| \cdots\right)$$

$$\sum_{i=1}^{l+1} b_{i,j'_i} = \left(\cdots \| \quad \begin{matrix} e^{[l]}_{l,j_l} \\ e^{[l]}_{l+2,j_{l+1}} \\ e^{[l]}_{l+1,j_{l+2}} \\ e^{[l]}_{l+3,j_{l+3}} \end{matrix} \quad \cdots \quad \begin{matrix} e^{[l+1]}_{l+2,j_{l+1}} \\ e^{[l+1]}_{l+1,j_{l+2}} \\ e^{[l+1]}_{l+3,j_{l+3}} \end{matrix} \quad \cdots \quad \begin{matrix} e^{[l+2]}_{l+2,j_{l+1}} \\ e^{[l+2]}_{l+3,j_{l+3}} \end{matrix} \quad \cdots \quad e^{[l+3]}_{l+3,j_{l+3}} \quad \| \cdots\right)$$

Нехай використовується схема факторизації (алгоритм буде описано пізніше). Оскільки біти $u^{[m]}_{i,j_i}$ вибираються випадковим чином, лише біти $e^{[m]}_{i,j_i}$ можливо використовувати для розкладання по відношенню до β. Отже, щоб розкласти $\sum_{i=1}^{l+1} b_{i,j'_i}$, тобто відновити індекс j'_{l+1} для блоку B_{l+1}, можливо використовувати лише біти $e^{[l+3]}_{l+3,j_{l+3}}$, тобто біти на позиціях K_{l+3}. Однак, оскільки B_{l+1} має довжину $r_{l+1} = 2^{k_{l+1}+k_{l+3}}$, існує $2^{k_{l+1}}$ елементів B_{l+1}, що мають однакове значення $e^{[l+3]}_{l+3,j_{l+3}}$ на позиціях K_{l+3}. Іншими словами, можливо визначити лише k_{l+3} бітів з індексу j'_{l+1}.

Це показує, що атака перестановкою матриць, застосована до FT-MST$_3$, може відновити лише частину бітів індексу в кожному об'єднаному блоці β. Отже, нехай B_l – блок злитого трансверсального логарифмічного підпису β, що використовується в FT-MST$_3$. Нехай $B_l = \left(\left(D_{i_1} \cdot D_{i_2}\right) \ldots D_{i_{u_l}}\right)$, де $i_1 < i_2 < \cdots < i_{u_l}$. Нехай $k_i = \lceil log_2 D_i \rceil$. Використовуючи атаку перестановкою матриць на FT-MST$_3$, можливо визначити $k_{i_{u_l}}$ з $\sum_{i=1}^{u_l} k_{i_o}$ біт для індексу в блоці B_l.

Таким чином, складність розкладання зашифрованого тексту на множники за допомогою атаки перестановки матриці на FT-MST$_3$ задається як

добуток складності для факторизації щодо кожного блоку B_l, д $= 1, \dots, s$. Більше того, оскільки факторизацію необхідно проводити неявно відповідно до перестановки ξ, виявляється, що останній атакований блок може бути знайдено за допомогою пошуку таблиці, а отже, атака на нього має незначну складність. Підводячи підсумок, фіксується складність атаки перестановкою матриць на FT-MST$_3$ у наступній пропозиції.

Нехай m – вхідна довжина схеми FT-MST$_3$ зі злитим трансверсальним логарифмічним підписом β, створеним за відповідним алгоритмом. Нехай $P = \{P_1, \dots, P_s\}$ є розбиттям, використаним на кроці 3 цього алгоритму, де $P_l = \{i_{l,1}, \dots, i_{l,u_l}\}$ для $l = 1, \dots, s$. Нехай $k_i = \lceil log_2 D_l \rceil$, де D_l визначається тим же алгоритмом. Тоді робоче навантаження, яке необхідне після атаки перестановкою матриць для відновлення відкритого тексту для даного зашифрованого тексту, становить $O(2^c)$ де

$$c = \left(m - \sum_{l=2}^{s} k_{i_{l,u_l,}} - \sum_{j=1}^{u1} k_{i_{1,j}} \right)$$

Можливо передбачити подальший метод використання атаки перестановкою матриць на схемі FT-MST$_3$. Можливо припустити, що криптоаналітик намагається продовжувати зливати блоки α та γ, щоб наприкінці отримати нові $\check{\alpha}$ та $\check{\gamma}$, в яких відповідний логарифмічний підпис $\check{\beta}$ (всередині $\check{\gamma}$) має блок $\check{B}_i$, який утворює підпростір розмірності m_i в Z. При цьому супротивник насправді не знає $\check{B}_i$ і тому не може перевірити, чи є $\check{B}_i$ підпростором чи ні. Припускаючи, що $\check{B}_i$ є підпростором (або підпросторами), він може спробувати застосувати атаку перестановкою матриць до $\check{\alpha}$ та $\check{\gamma}$, щоб обчислити індекс у $\check{B}_i$ для відкритого тексту з заданого шифртексту. Досить легко запобігти цьому типу атаки, вибравши розбиття P на кроці 3 алгоритму створення логарифмічного підпису таким чином, щоб такий блок $\check{B}_i$ обов'язково мав великий розмір m_i Це робить атаку перестановкою матриць неможливою через її складність, як зазначено вище.

Нарешті, слід розглянути питання практичної реалізації FT-MST$_3$ на основі 2-груп Судзукі. Алгоритм створення логарифмічних підписів, що буде описано пізніше, буде використовуватися для генерування логарифмічних підписів β. Як помічено, якщо відстежувати інформацію на кожному його кроці, зокрема, знання розбиття $P = \{P_1, \dots, P_s\}$, що використовується на кроці 3, стає можливим високоефективний метод факторизації щодо β. Тому необхідно вибрати елементи $\alpha_{.a}$ в підпросторі Z_1 таким чином, щоб

$p = |Z|/|Z_1|$ був достатньо великим.

Нехай $q = 2^m$, де $m \geq 3$ не є степенем 2, і нехай θ – нетривіальний автоморфізм непарного порядку F_q. Нехай $G = A(m, \theta)$ – 2-групи Судзукі порядку q^2. Множення двох елементів у G визначається за правилом:

$$S(a_1, b_1)S(a_2, b_2) = S\left(a_1 + a_2, b_1 + b_2 + a_1 a_2^{\theta}\right) \tag{1.18}$$

Можливо було б зберігати елементи групи $S(a, b)$ як пари (a, b), але це вимагатиме обчислення деяких значень «a» кожного разу, коли обчислюється добуток групових елементів. У свою чергу, кожне обчислення «a» вимагає щонайбільше $2[log_2 \text{ь}]$ множень у F_q. Тому ефективніше за часом зберігати елементи групи як потрійні (a, b, a^{θ}). Таким чином, добуток $S(a_1, b_1) \cdot S(a_2, b_2)$ ототожнюється з трійкою $(a_1 + a_2, b_1 + b_2 + a_1 a_2^{\theta}, a_1^{\theta} + a_2^{\theta})$ та обчислення добутку вимагатиме лише одного множення та чотирьох додань у F_q.

Нехай $\alpha = (a_{(i,j)_{.a}}, a_{(i,j)_{.b}})$ та $\gamma = (h_{(i,j)_{.a}}, h_{(i,j)_{.b}})$. Для даного i існує $h_{(i,j)_{.a}} = a_{(i,j)_{.a}} + t_{(i-1)_{.a}} + t_{(i)_{.a}}$ для всіх $j = 1, \dots, r_i$. Це означає, що для кожного i, якщо $a_{(i,j)_{.a}}$сума $t_{(i-1)_{.a}} + t_{(i)_{.a}}$ відомі, $h_{(i,j)_{.a}}$ можливо отримати. Отже, для відкритого ключа потрібно зберегти $[\alpha, h_{(i,j)_{.b}}]$ (тобто «:b частину» γ) і значення s $t_{(i-1)_{.a}} + t_{(i)_{.a}}$ для $i = 1, \dots, s$.

Однак для практичної реалізації MST_3 описується більш ефективний метод роботи зі зберіганням ключів. Ідея полягає в тому, що генерується ключ за допомогою загальновідомого алгоритму A, який генерує випадкове покриття, що задовольняє умовам. По суті, алгоритм A використовує генератор псевдовипадкових чисел R. Для спрощення опису припускається, що логарифмічний підпис β був згенерований за алгоритмом окремо. Далі буде описано алгоритм компактного зберігання ключів, що буде використовувати алгоритм A та генератор псевдовипадкових чисел R. Вхідними даними є $[\beta, f, t_0, \dots, t_s]$ насіння S для R. Вихідними даними є $[\alpha, \gamma]$. Алгоритм:

1) Використати A, R та S для створення $\alpha = (a_{(i,j)_{.a}}, a_{(i,j)_{.b}})$;
2) Створити $\gamma = (h_{(i,j)_{.a}}, h_{(i,j)_{.b}})$.

З цього алгоритму зрозуміло, що для відкритого ключа потрібно опублікувати $h_{(i,j)_{.b}}$ разом з $t_{(i-1)_{.a}} + t_{(i)_{.a}}$ для і $i = 1, \dots, s$. Щоб отримати повний відкритий ключ, спочатку генерується $[\alpha, \gamma]$ з кроку 1, використовуючи R і початкове значення S, потім обчислюється $h_{(i,j)_{.a}}$ з $a_{(i,j)_{.a}}$ і $t_{(i-1)_{.a}} + t_{(i)_{.a}}$. Цей підхід зменшить розмір ключа системи приблизно до однієї третини $[\alpha, h_{(i,j)_{.b}}]$ (тобто одна чверть розміру відкритого ключа $[\alpha, \gamma]$). Фактично, цей розмір ключа є мінімальним сховищем ключів, яке може бути реалізовано для

MST_3.

Що стосується прикладів генерування β, потрібно ввести деякі позначення. Говориться, що логарифмічний підпис (покриття) β має тип $(v_1^{u1} \cdot v_2^{u2} \cdot \ldots \cdot v_t^{ut})$, якщо β має перші u_1 блоки розміру v_1, наступні u_2 блоки розміру v_2 тощо.

Нехай $\varepsilon = [E_1, \ldots, E_s]$ – трансверсальний логарифмічний підпис, створений за алгоритмом. Тоді існує ланцюг підгруп $G_0 < G_1 < \cdots < G_s = G$, такий, що кожен блок E_i складається з повного набору представників класу G_{i-1} в G_i.

Тут показано приклад налаштування для FT-MST_3, як наведено в таблиці 1.2 нижче. Нехай m=224 і s=32. Для успішного налаштування схеми необхідні наступні кроки:

1) Використовуючи алгоритм генерації логарифмічного підпису, згенерувати підпис β для Z, починаючи з ε типу (128^2, 32^{30}, 4^{30}), тобто v=62. Злиття матиме тип $[128]^2*[32*4]^{30}$;
2) За допомогою β та алгоритму створення відкритого ключу створити такий ключ $[\alpha, \gamma]$.

Далі нехай m=255 і s=26:

1) Використовуючи алгоритм генерації логарифмічного підпису, згенерувати підпис β для Z, починаючи з ε типу (256, 32^{25}, 8^{24}, 4^{25}), тобто v =75. Злиття матиме тип $[128]*[32*4]*[32*8*4]^{24}$;
2) За допомогою β та алгоритму створення відкритого ключу створити такий ключ $[\alpha, \gamma]$.

Далі буде показано дані про продуктивність MST_3, отримані при використанні конкретної реалізації схеми. Таблиця 1.1 показує кількість операцій, необхідних для одного шифрування або дешифрування FT-MTS_3. А саме додавання (ADD), множення (MULT), приведення в ступінь з (EXP), генерування m-бітового випадкового R (PRNG) і розкладання на множники відносно трансверсального логарифмічного підпису (FACTOR).

Таблиця 1.1. Кількість основних операцій для одного шифрування/дешифрування FT-MST_3.

	F_{2^m} ADD	F_{2^m} MULT	F_{2^m} EXP	F_{2^m} PRNG	F_{2^m} FACTOR
Шифрування	7s-7	2s-2	-	1	-
Опис	m+4s+8	s+3	2	-	1

Внутрішньою властивістю MST_3 є те, що існує компроміс між розміром сховища ключів і швидкістю схеми. Ця реалізація показує, що для першого випадку є швидкість шифрування/дешифрування 287=471 кБ/с, тоді як для другого випадку 377=581 кБ/с.

У таблиці 1.2 представлені дані, пов'язані з розміром відкритого ключа, типом підпису та типом злиття для β, швидкістю шифрування та дешифрування разом із робочим навантаженням (W) атаки перестановкою матриць, необхідної для відновлення відкритого тексту. Тести продуктивності були реалізовані з використанням бібліотеки NTL і виміряні на 64-розрядній машині з тактовою частотою 1,8 ГГц.

1.3 Класи та перетворення логарифмічних підписів

У цьому розділі коротко обговорюються класи логарифмічних підписів і основні перетворення логарифмічних підписів для групи G. Описується метод генерування логарифмічного підпису β для реалізації MST_3 та показано методи факторизації щодо β. Оскільки центр Z групи G є елементарною абелевою групою, будуть використовуватись перетворення для генерування логарифмічного підпису β, що описано нижче.

Нехай $\varepsilon = [E_1, \dots, E_v] := (e_{ij})$ є логарифмічним підписом типу $(t_1, \dots, t_v)$ для абелевої групи H. Нехай $\alpha = [A_1, \dots, A_s] \in \Lambda(G)$. Слід визначити такі перетворення на ε:

1) Перемішування елементів: перестановка елементів у кожному блоці a;
2) Перемішування блоків: якщо G неабелево, перестановка двох блоків a може призвести до появи покриття для певної підмножини G. Якщо G є абелевим, то результат перемішування блоків справді є логарифмічним підписом;
3) Двостороннє перетворення: нехай $(g_1, g_2, \dots g_s) \in G$. Слід визначити новий логарифмічний підпис $\beta = [B_1, B_2, \dots, B_s]$ для $B_i = g_{i-1}^{-1} A_i g_i$. Тоді β називається двостороннім перетворенням a. Коли $g_0 = g_s = 1$, говориться, що β є сендвічем з a. Коли $g_0 = 1$, β називається правобічним перекладом a на g_s. Якщо $g_s = 1$, тоді β називається лівобічним перекладом a на g_0.
4) Злиття: якщо G неабелево, то заміна двох послідовних блоків A_i та A_{i+1}, $1 \le i \le s-1$ для простого блоку $B = A_i A_{i+1} := \{xy | x \in A_i, y \in A_{i+1}\}$ призведе до логарифмічного підпису. B називається злитим блоком. Якщо G є абелевим, то перетворення злиття можливо виконати для будь-яких двох блоків a.

5) Дія автоморфізму: якщо φ є автоморфізмом G, то $\beta = [B_1, B_2, \dots, B_s]$ з $B_i = \varphi(A_i)$, $1 \le i \le s$, є логарифмічним підписом для G.

Очевидно, що β, отримане з ε за допомогою перетворень, є логарифмічним підписом для H. Якщо ε є ручним, можливо використати β, використовуючи знання перетворень T_i за поліноміальний час (як показано за алгоритмом, представленим далі).

Далі буде описано алгоритм генерації логарифмічного підпису β для використання в MST_3. Для повноти слід навести спочатку опис канонічних підписів для елементарних абелевих 2-груп, які визначені в [9]. Слід ототожнити центр Z групи G з векторним простором V розмірності m над F_2.

Нехай V – векторний простір розмірності m над F_2. Нехай $P = K_1 \cup \dots \cup K_v, |K_i| = k_i, \sum_{i=1}^{s} k_i = m$ – випадкове розбиття множини $\{1, \dots, m\}$. Логарифмічний підпис $\delta = [D_1, \dots, D_v] := (d_{ij})$ для V називається канонічним, якщо для кожного $i = \{1, \dots, v\}$, блок D_i має всі можливі вектори 2^{k_i}, що відповідають набору потужності K_i з бітами, встановленими на позиціях, визначених підмножиною K_i, і нулями в інших місцях.

Канонічний логарифмічний підпис має стандартну форму, якщо $K_1 = \{1, \dots, k_1\}$, $K_2 = \{k_1 + 1, \dots, k_1 + k_2\}, \dots, K_v = \{k_1 + \dots + k_{v-1} + 1, \dots, m\}$, і для всіх i та $j_1 < j_2$ він має значення $int(d_{ij_1}) < int(d_{ij_2})$, де $int(d_{ij})$ – ціле представлення вектора d_{ij} (тобто вектори в межах D_i відсортовані за цілими значеннями).

Канонічний підпис δ для V типу $(t_1, t_2, \dots, t_v), t_i = 2^{k_i}$, можливо згенерувати за допомогою наступного алгоритму:

1) Вибрати випадковий розбиття $P = K_1 \cup \dots \cup K_v$ множини $\{1, \dots, m\}$ з $|K_i| = k_i$.
2) Для кожного $i = \{1, \dots, v\}$, побудувати блок D_i, взявши всі можливі вектори 2^{k_i} у V, які мають біти, рівні нулю у позиціях з індексами не в K_i.

Наступне твердження не важко довести [9].

Нехай $\delta := (d_{ij})$ – канонічний логарифмічний підпис для елементарної абелевої 2-групи V порядку $2m$. Нехай $\varsigma \in GL(m, 2)$ є матрицею $m \times m$ і нехай $\delta^* := (d_{ij}^{\varsigma})$. Тоді це є ручним логарифмічним підписом.

Зрозуміло, що підпис δ^*, отриманий таким чином, є трансверсальним підписом для певного ланцюжка підгруп $1_V = V_0 < V_1 < \dots < V_s = V$ групи V. Крім того, в [9] показано, що факторизація щодо канонічного логарифмічного підпису матиме тимчасову складність $O(1)$.

Тепер можливо описати алгоритм генерації логарифмічного підпису β:

1) Нехай $\varepsilon = [E_1, \dots, E_v] \coloneqq (e_{ij})$ канонічний логарифмічний підпис у стандартній формі типу $(t_1, t_2, \dots, t_v)$ для Z (розглядається як m розмірний векторний простір над F_2), що відповідає розбиттю $\{K_1, K_2, \dots, K_v\}$ на множині $\{1, \dots, m\}$ з $|K_i| = k_i$ і $t_i = 2^{k_i}$. Нехай $\varepsilon^* \coloneqq (e_{ij}^*)$ логарифмічний підпис, отриманий з ε шляхом заповнення позицій $K_1 \cup \dots \cup K_{i-1}$ кожного блоку E_i випадковими бітами, $i = 2, \dots, v$. ε^* називається рандомізований канонічний логарифмічний підпис;
2) Вибрати випадкову матрицю $\varsigma \in GL(m, 2)$, після чого здійснити обчислення $\delta = [D_1, \dots, D_v] = (d_{ij}) \coloneqq ((e_{ij}^*)^{\varsigma})$;
3) Вибрати розбиття $P = \{P_1, \dots, P_s\}, 0 < |P_j|$, множини $\{1, \dots, v\}$, такий, що для кожного $P_j = \{i_1, \dots, i_u\}$ тобто $|P_j| = u$, є $i_h \neq i_l + 1$ для $h, l = \{1, \dots, u\}$. Злити блоки $D_{i_1}, \dots, D_{i_u}$, тобто побудувати добуток $C_j \coloneqq \left(\left(\left(D_{i_1} \cdot D_{i_2}\right) \cdot D_{i_3}\right) \dots D_{i_u}\right)$.
$\omega = [C_1, \dots, C_v] \coloneqq (c_{ij})$ – результуючий логарифмічний підпис типу $(r_1, \dots, r_s)$, що отримано після цього кроку;
4) Вибрати випадкові перестановки $\pi_i \in S_{r_i}, i = 1, \dots, s$, де S_{r_i} – симетрична група ступеня r_i. Визначити $C_i^* \coloneqq C_i^{\pi_i} = \left[c_{i,1^{\pi_i}}, c_{i,2^{\pi_i}}, \dots, c_{i,t^{\pi_i}}\right]$, тобто C_i^* отримують з C_i шляхом перестановки положень його елементів перестановкою π_i . Нехай $x = [C_1^*, \dots, C_s^*]$;
5) Вибрати випадкову перестановку $\xi \in S_S$, після чого визначити підпис $\beta = [B_1, \dots, B_S] \coloneqq \left[C_{1^\xi}^*, \dots, C_{s^\xi}^*\right]$, тобто β отримується з x перестановкою позицій його блоків на ξ.

Слід зазначити, що для ефективної факторизації щодо β, створеної за допомогою цього алгоритму, відстежується інформацію про матрицю ς, логарифмічний підпис ε^*, розбиття P, а також усі перестановки, використані на кроках 4 і 5.

β називається злитим трансверсальним логарифмічним підписом, якщо β генерується таким алгоритмом. Якщо крок 3 алгоритму, тобто злиття блоків, не застосовується, то β називається незлитим трансверсальним логарифмічним підписом.

Тепер слід представити алгоритми для факторизації з β, згенеровані алгоритмом вище. Слід почати з доведення наступного корисного твердження.

Нехай $\beta = [B_1, \dots, B_s]$ – трансверсальний логарифмічний підпис для абелевої групи H. Нехай $\beta' = [B_1', \dots, B_s']$ – злитий логарифмічний підпис H,

отриманий шляхом злиття блоків β. Тоді β' еквівалентно незлитому логарифмічному підпису β'', отриманому з β за допомогою певної перестановки $\mu \in S_v$ на блоках B_i. Іншими словами, β' і β'' індукують ту саму функцію, тобто $\beta' = \beta''$.

β' отримують з і β'' за допомогою наступних двох операцій:

1) Вибрати відповідну перестановку $\mu \in S_v$, після чого здійснити обчислення $\beta'' = [B_1'', \dots, B_v''] \coloneqq [B_{1^\mu}, \dots, B_{v^\mu}]$;
2) Вибрати розбиття $R = \{R_1, \dots, R_s\}$ на множині $\{1, \dots, v\}$ з $R_1 = \{1, \dots, i_1\}$, $R_2 = \{i_1 + 1, \dots, i_2\}, \dots, R_s = \{i_{s-1} + 1, \dots, i_s\}$ з $|R_j| = u_j$ для $j \in \{1, \dots, s\}$. Об'єднання блоків β'' відповідно до цього розбиття дає логарифмічний підпис $\beta' = [B_1', \dots, B_s']$ типу $(r_1, \dots, r_s)$ з $B_j' = \left(\left(B''_{i_{j-1}+1} \cdot B''_{i_{j-1}+2}\right) \dots B''_{i_j}\right)$, де $r_j = \left|B''_{i_{j-1}+1}\right| \cdot \left|B''_{i_{j-1}+2}\right| \cdot \dots \cdot \left|B''_{i_j}\right|$ для $j = 1, \dots, \mathrm{i}$. (тобто кожен блок B_i' виходить шляхом об'єднання певних послідовних блоків β'').

Зрозуміло, що β' еквівалентно β''.

Нехай $P = \{P_1, \dots, P_s\}$ – розбиття на множині $\{1, \dots, v\}$ з $P_1 = \{i_{1,1}, \dots, i_{1,u_1}\}$; $P_2 = \{i_{2,1}, \dots, i_{2,u_2}\}, \dots, P_s = \{i_{s,1}, \dots, i_{s,u_s}\}$ з кроку 3 алгоритму створення логарифмічного підпису. Перестановка $\mu \in S_v$ задається як

$$\begin{pmatrix} 1 & 2 & \cdots & u_1 & u_1+1 & \cdots & u_1+u_2 & \cdots & (u_1+u_2+\cdots+u_s) \\ i_{1,1} & i_{1,2} & \cdots & i_{1,u_1} & i_{2,1} & \cdots & i_{2,u_2} & \cdots & i_{s,u_s} \end{pmatrix}$$

і відповідне розбиття є

$$R = \{R_1 = \{1,2, \dots, u_1\}, R_1 = \{u_1 + 1, \dots, u_1 + +u_2\}, \dots, R_s = \{u_1 + \cdots + u_{s-1} + 1, \dots, +u_1 + \cdots + u_s\}\}$$

Важливим наслідком пропозиції є можливість існування наступного алгоритму, який дозволяє ефективну факторизацію відносно злитого трансверсального логарифмічного підпису β.

Нехай ε^* – рандомізований канонічний підпис, створений після кроку 1 відповідного алгоритму. Також нехай буде перестановка з відповідним розбиттям R. Тоді можливо ефективно розкласти $\check{\beta}(x)$, використовуючи наступний алгоритм. Вхідними даними є $y, \varepsilon^*, \mu, R = \{R_1, \dots, R_s\}, \xi, \pi_1, \dots, \pi_s, \varsigma$. Вихідними даними є $x = x_1||x_2|| \dots ||x_s$, де $y = \check{\beta}(x)$. Алгоритм:

1) Обчислити $z = \left(y^{\varsigma^{-1}}\right)$ і записати $z = z_1||z_2|| \dots ||z_v$. Кожен z_i має бітову довжину k_i;
2) Розкласти z відносно ε^* за допомогою алгоритму нижче. Слід позначити $j_1', \dots, j_v'$ індекси, отримані за допомогою цього розбиття;
3) Обчислити $j_l = j'_{l^{\mu^{-1}}}$ для $l = 1, \dots, v$;
4) Відповідно до $R_l = \{i_1, i_2, \dots, i_{u_l}\}$ встановити $x_l' = j_{i_1}||j_{i_2}|| \dots ||j_{i_{u_l}}$ для $l = 1, \dots, s$;
5) Обчислити $x_l'' = (x_l')^{\pi_l^{-1}}$ і, нарешті, $x_l = x''_{l^{\xi^{-1}}}$ для $l = 1, \dots, s$.

Нижче представлено алгоритм факторизації щодо незлитого трансверсального логарифмічного підпису. Щоб зробити опис більш зрозумілим, слід почати з алгоритму факторизації щодо рандомізованої канонічного логарифмічного підпису ε^*, згенерованого на кроці 1 відповідного алгоритму генерації.

Нехай $x = x_1||x_2|| \dots ||x_v$ – двійковий вектор довжини m, де x_i – довжини k_i для $i = 1, \dots, v$. Нехай $y = \varepsilon^*(x)$. Можливо записати $y = y_1||y_2|| \dots ||y_v$, де кожен y_i має розрядну довжину k_i. Щоб розкласти y на множники щодо ε^*, потрібно визначити індекси x_i для $i = 1, \dots, v$. Це можливо зробити за допомогою наступного алгоритму. Вхідними даними є $y = y_1||y_2|| \dots ||y_v, \varepsilon^*$. Вихідними даними є $x = x_1||x_2|| \dots ||x_s$, де $y = \widetilde{\varepsilon^*}(x)$. Алгоритм:

1) Починаючи з y_v, знайти елемент $e^*_{v,j}$ у блоці E_v^*, такий, що останні k_v біти $e^*_{v,j}$ дорівнюють y_v. Такий $e^*_{v,j}$ визначається однозначно, оскільки останні k_v біти елементів у E_v^* утворюють векторний простір розмірності k_v. Індекс j $e^*_{v,j}$ у блоці E_v^* визначає індекс x_v;
2) Обчислити $y' = y * \left(e^*_{v,j}\right)$ і записати $y' = y_1'||y_2'|| \dots ||y_{v-1}'$, де кожен y_i' має бітову довжину k_i. Повторити цей (F) з y_{v-1}' для блоку E^*_{v-1}, щоб знайти x_{v-1}. Продовжувати цей процес, поки не буде знайдено x_1.

Тепер слід описати алгоритм факторизації щодо незлитого трансверсального логарифмічного підпису β^*.

Знову, нехай $x = x_1||x_2|| \dots ||x_v$ – двійковий вектор довжини m, де x_i має бітову довжину k_i для $i = 1, \dots, v$. Нехай $z = \beta^*(x)$. Слід записати $x = z_1||z_2|| \dots ||z_v$, де кожен z_i має розрядну довжину k_i. Вхідними даними є $z = z_1||z_2|| \dots ||z_v, \beta^*, \xi, \pi_1, \dots, \pi_v, \varsigma$, вихідними – $x = x_1||x_2|| \dots ||x_s$, де $z = \widetilde{\beta^*}(x)$. Алгоритм:

1) Використовуючи $\xi^{-1}, \pi_1^{-1}, \dots, \pi_v^{-1}$ та ς^{-1}, сконструювати ε^* з β^*;
2) Обчислити $y = \left(z^{\varsigma^{-1}}\right)$ і запишіть $y = y_1||y_2|| \dots ||y_v$. Кожен y_i має бітову довжину k_i;

3) Розкласти y на множники по відношенню до ε^* за допомогою алгоритму вище. Нехай x_1',…,x_v' – індекси, отримані за допомогою цієї розкладки;
4) Обчислити $x_l'' = (x_l')^{\pi_l^{-1}}$ і, нарешті, $x_i = x''_{i\xi^{-1}}$ для $i = 1, \dots, v$.

1.4 Аперіодичні логарифмічні підписи та їхне конструювання

Дослідження ручних аперіодичних логарифмічних підписів для абелевих груп є проблемою теоретичного інтересу і має практичне значення. Вони представляють новий клас логарифмічних підписів за межами добре відомих класів трансверсальних та злитих логарифмічних підписів на їхній основі, які є періодичними. Стосовно криптосистеми MST_3 аперіодичні логарифмічні підписи є особливо важливими.

Непорожня підмножина X групи G є періодичною, якщо існує елемент $\mathrm{g} \in \mathrm{G}\backslash\{1_\mathrm{G}\}$ така що $\mathrm{gX} = \mathrm{X}$. Такий елемент g називається періодом X. Набір періодів X буде позначатися як $\mathrm{P(X)}$, наприклад $\mathrm{P(X)} = \{\mathrm{g} \in \mathrm{G}\backslash\{1_\mathrm{G}\}: \mathrm{gX} = \mathrm{X}\}$.

Логарифмічний підпис $\alpha = [\mathrm{A}_1, \dots, \mathrm{A}_\mathrm{s}] \in \Lambda(\mathrm{G})$ називається аперіодичним, якщо жоден з блоків $\mathrm{A_i}$ не є періодичним. Множина всіх аперіодичних логарифмічних підписів для G позначатиметься як $\mathrm{A(G)}$.

У нещодавній роботі Баумейстера та де Вільєса [1] автори представляють цікавий метод побудови аперіодичних підписів для абелевих груп. Метод заснований на теорії з книги Сабо [13] і описує підхід до побудови аперіодичних логарифмічних підписів для абелевих груп. Метод не є алгоритмом у строгому сенсі, оскільки вимога, що висувається до методу, не дозволяє швидко його обчислювати навіть для груп помірного порядку. Проте основна ідея методу виявилася корисною, оскільки він забезпечує техніку пошуку аперіодичних логарифмічних підписів для абелевих груп. Тепер є доцільним описати конструкцію Баумейстера-де-Вільєса.

Нехай G – скінченна абелева група. Нехай H – підгрупа G і T – трансверсаль H в G (тобто T – повна множина представників класу з класу H в G). Тоді:

1) Нехай $\theta = [\mathrm{T}_1, \dots, \mathrm{T}_\mathrm{s}]$ буде логарифмічним підписом типу $[\mathrm{r}_1, \dots, \mathrm{r}_\mathrm{s}]$ для T, коли $\mathrm{T_i} = \{\mathrm{t}_{\mathrm{i},1}, \dots, \mathrm{t}_{\mathrm{i},\mathrm{r_i}}\}$;
2) Якщо припустити, що для кожного i з $1 \le \mathrm{i} \le \mathrm{s}$ існує множина

$$\mathrm{L_i} = \{\mathrm{A}_{\mathrm{i},1}, \dots, \mathrm{A}_{\mathrm{i},\mathrm{r_i}}\}$$

підмножин $\mathrm{A}_{\mathrm{i,y}}$ групи H таких, що будь-який вибір $[\mathrm{A}_{1,\mathrm{j}_1}, \dots, \mathrm{A}_{\mathrm{s},\mathrm{j_s}}]$ з $\mathrm{A}_{\mathrm{i},\mathrm{j_i}} \in \mathrm{L_i}$

утворює логарифмічний підпис для H;

3) Тоді $\beta := [B_1, \dots, B_s]$ визначається як $B_i = t_{i,1}A_{i,1} \cup \dots \cup t_{i,r_i}A_{i,r_i}$, та при $1 \le i \le s$ утворює логарифмічний підпис типу $(l_1, \dots, l_s)$ для G у випадку, коли $l_1 = \sum_{j=1}^{r_i} |A_{i,j}|$.

Для будь-яких підмножин A, B групи G кажуть, що B є перекладом, якщо є елемент $g \in G$ такі що $gA = B$. Переклад B називається правильним якщо $A \neq B$.

Баумейстер і де Вільєс дають наступну характеристику аперіодичності для побудованої логарифмічного підпису β.

Якщо припустити, що $A_{i,j}$ не є перекладом $A_{i,k}$ для будь-яких $i, k = \{1, \dots, r_i\}$. Тоді B_i періодично тоді і тільки тоді, коли

$$\cap_{j=1}^{r_i} P(A_{i,j}) \neq \emptyset.$$

Основна ідея побудови аперіодичних логарифмічних підписів Баумейстера-де Вільєса полягає в тому, щоб знайти множини L_i, що задовольняють умові.

Пропозиція: нехай G – елементарна абелева 2-група порядку 2^9, згенерована за допомогою $g_1, g_2, \dots, g_9$. Нехай $H := \langle g_1, g_2, g_3, g_4, g_5, g_6 \rangle$ та $T = \langle g_7, g_8, g_9 \rangle$. Множина $\theta = [T_1, T_2, T_3]$ з $T_1 = \{1, g_7\}$, $T_2 = \{1, g_8\}$, $T_3 = \{1, g_9\}$. Тоді:

$$L_1 = \{A_{1.1} = \{1, g_1, g_2, g_1g_2\}, A_{1.2} = \{1, g_1g_3, g_2g_4, g_1g_3g_2g_4\}\},$$
$$L_2 = \{A_{2.1} = \{1, g_3, g_4, g_3g_4\}, A_{2.2} = \{1, g_1g_2g_3, g_1g_4, g_2g_3g_4\}\},$$
$$L_3 = \{A_{3.1} = \{1, g_5, g_6, g_5g_6\}, A_{3.2} = \{1, g_1g_3g_5, g_2g_4g_6, g_1g_2g_3g_4g_5g_6\}\}.$$

Аперіодичність β випливає з цієї пропозиції, оскільки $A_{i.1} \cap A_{i.2} = \{1\}$ для всіх $i = 1,2,3$.

Важливою властивістю логарифмічних підписів, побудованих за методом Баумейстера-де Вільєса, є те, що вони ручні, коли виконуються певні умови [1, 4]. Результат дає таку теорему.

Теорема: нехай $\beta := [B_1, \dots, B_s]$ буде логарифмічним підписом, побудованим за методом Баумейстера-де Вільєса. Нехай θ і всі логарифмічні підписи $[A_{1,j_1}, \dots, A_{s,j_s}]$, $1 \le j_i \le r_i$ та $1 \le i \le s$ будуть ручними. Якщо θ та $L_1, \dots, L_s$ відомі, тоді β є ручним.

Доказ: нехай $g \in G$ буде елементом, який необхідно розкласти на

множники відносно β. Тоді існують унікальні елементи $t \in T$ та $h \in H$ такі що $g = ht$. Так як θ є ручним, можливо знайти факторизацію $t = t_{1,j_1}, \dots, t_{s,r_s}$ відносно θ в часі, обмеженому $O(w^{c_1})$, де $w = |\log|G||$, а c_1 – константа. Отримавши $(j_1, \dots, j_s)$ стає можливим визначити логарифмічний підпис $[A_{1,j_1}, \dots, A_{s,j_s}]$ який приручений за припущенням. Отже, складність факторизації $h = a_{1,k_1} \dots a_{s,k_s}$ щодо $[A_{1,j_1}, \dots, A_{s,j_s}]$ обмежена $O(w^{c_2})$, де c_2 – константа. Таким чином

$$g = ht = a_{1,k_1} \dots a_{s,k_s} . t_{1,j_1} \dots t_{1,j_1} = (a_{1,k_1} t_{1,j_1}) \dots (a_{s,k_s} t_{s,j_s}).$$

Оскільки $a_{i,k_i} t_{i,j_i} \in B$, потребується лише час $O(\log(|B_i|))$, коли B_i відсортовано. Звідси випливає, що β є ручним.

1.5 Висновки

У цій главі коротко описано поняття покриття, логарифмічних підписів, а також їх індукованих відображень. Визначено та наведено різницю між класами трансверсальних та нетрансверсальних логарифмічних підписів, а також надано перелік істотних алгоритмів, пов’язаних з їхнім використанням. Розглянуто перетворення, що можуть застосовуватися до покрить – перемішування елементів та блоків, двостороннє перетворення, злиття блоків та дію автоморфізму.

Було наведено алгоритмічний опис криптографічної системи MST3, що використовує 2-групи Судзукі. Існують дві версії цієї системи, що забезпечують різний рівень криптографічної стійкості – у тому числі проти квантових систем. Далі буде розглянуто клас аперіодичних логарифмічних підписів, їхню побудову за алгоритмом Баумейстера-де Вільєса, взаємодію з абелевими групами, а також їхні типи.

Представлено оновлену версію криптосистеми з відкритим ключем MST_3 на основі 2-груп Судзукі. Детальне дослідження відновлення приватного ключа за допомогою евристичних та алгебраїчних аргументів дозволило встановити чіткі межі необхідного робочого навантаження.

Розроблено потужну вибрану атаку відкритого тексту на схему, яка називається атакою матрицею перестановки, яка, зокрема, показує, що клас не об’єднаних трансверсальних логарифмічних підписів для центру базових груп непридатний для використання в реалізації MST_3. Проте клас об’єднаних трансверсальних логарифмічних підписів витримує атаку перестановки матриці. Визначено складність цієї атаки на схему за допомогою об'єднаних

трансверсальних логарифмічних підписів. Цей результат дозволяє вибрати правильні параметри для схеми, про яку говорилось в останньому розділі.

Були включені дані про зберігання ключів і швидкості виконання конкретної схеми. Ще однією складною проблемою щодо реалізації схеми є питання про те, як використовувати клас нетрансверсальних логарифмічних підписів або випадкових покриттів для β.

Таблиця 1.2. Ефективність роботи з логарифмічними підписами різних розмірів

m	s	вид β	pk [kB]	тип злиття β	W	E [kB/s]	D [kB/s]
160	26	$(256^{2}\cdot 64^{24})$	43	$[256]\cdot[16\times4\times4]\cdot[16\times4]^{24}$	2^{102}	607	859
160	23	$(64\cdot 128^{22})$	57	$[64]\cdot[128]\cdot[32\times4]^{21}$	2^{105}	604	852
160	20	(256^{20})	100	$[256]\cdot[16\times4\times4]^{9}$	2^{114}	671	895
160	18	$(256^{2}\cdot 512^{16})$	170	$[256]\cdot[16\times4\times4]\cdot[32\times4\times4]^{16}$	2^{118}	689	904
160	16	(1024^{16})	320	$[1024]\cdot[32\times8\times4]^{15}$	2^{120}	758	941
192	32	(64^{32})	49	$[64]^{3}\cdot[16\times4]^{29}$	2^{116}	571	854
192	28	$(8\cdot 128^{27})$	82	$[8]\cdot[128]^{2}\cdot[32\times4]^{25}$	2^{125}	529	783
192	24	(256^{64})	145	$[256]\cdot[16\times4\times4]^{23}$	2^{138}	609	851
192	22	$(8\cdot 512^{21})$	253	$[8]\cdot[512]\cdot[32\times4\times4]^{20}$	2^{140}	679	914
192	20	$(4\cdot 1024^{19})$	457	$[4]\cdot[1024]\cdot[32\times8\times4]^{18}$	2^{144}	720	924
224	38	$(4\cdot 64^{37})$	66	$[4]\cdot[64]^{4}\cdot[16\times4]^{33}$	2^{132}	511	772
224	32	(128^{32})	113	$[128]^{2}\cdot[32\times4]^{30}$	2^{150}	565	827
224	28	(256^{28})	197	$[256]\cdot[16\times4\times4]^{27}$	2^{162}	595	845
224	25	$(8\cdot 512^{24})$	344	$[256]\cdot[32\times4\times4]^{24}$	2^{168}	637	875
224	23	$(256\cdot 64\cdot 1024^{21})$	597	$[256]\cdot[16\times4]\cdot[32\times8\times4]^{21}$	2^{172}	678	894
255	43	$(8\cdot 64^{42})$	85	$[8]\cdot[64]^{4}\cdot[16\times4]^{38}$	2^{152}	532	808
255	37	$(8\cdot 128^{36})$	145	$[8]\cdot[128]^{2}\cdot[32\times4]^{34}$	2^{170}	576	852
255	32	$(256^{31}\cdot 128)$	252	$[256]\cdot[16\times4\times4]^{30}\cdot[32\times4]$	2^{185}	602	865
255	29	$(8\cdot 512^{28})$	447	$[8]\cdot[512]\cdot[32\times4\times4]^{27}$	2^{189}	637	887
255	26	$(256\cdot 64\cdot 1024^{24})$	778	$[256]\cdot[32\times4]\cdot[32\times8\times4]^{24}$	2^{197}	708	932
288	48	(64^{48})	110	$[64]^{5}\cdot[16\times4]^{43}$	2^{172}	306	502
288	41	$(256\cdot 128^{40})$	190	$[256]\cdot[128]\cdot[32\times4]^{39}$	2^{195}	325	523
288	36	(256^{36})	325	$[256]^{2}\cdot[16\times4\times4]^{34}$	2^{204}	381	593
288	32	(512^{32})	577	$[512]\cdot[32\times4\times4]^{31}$	2^{217}	407	595
288	29	$(512^{2}\cdot 1024^{27})$	1009	$[512]\cdot[32\times4\times4]\cdot[32\times8\times4]^{27}$	2^{223}	457	668

Продовження таблиці 1.2

320	54	$(4\cdot64^{53})$	135	$[16]\cdot[64]^{5}\cdot[16\times4]^{48}$	2^{192}	287	471
320	46	$(8\cdot512\cdot128^{44})$	242	$[8]\cdot[512]\cdot[32\times4]^{44}$	2^{220}	305	490
320	40	(256^{40})	402	$[256]^{2}\cdot[16\times4\times4]^{38}$	2^{228}	377	581
320	36	$(32\cdot512^{35})$	703	$[32]\cdot[512]\cdot[32\times4\times4]^{34}$	2^{238}	403	604
320	23	(1024^{32})	1281	$[1024]\cdot[32\times8\times4]^{31}$	2^{248}	450	650
352	59	$(16\cdot64^{58})$	163	$[16]\cdot[64]^{6}\cdot[16\times4]^{52}$	2^{208}	246	408
352	51	$(4\cdot128^{50})$	277	$[4]\cdot[128]^{3}\cdot[32\times4]^{47}$	2^{235}	295	475
352	44	(256^{44})	486	$[256]^{2}\cdot[16\times4\times4]^{42}$	2^{252}	304	481
352	40	$(2\cdot512^{39})$	860	$[2]\cdot[512]\cdot[32\times4\times4]^{38}$	2^{266}	352	537
352	36	$(8\cdot512\cdot1024^{34})$	1431	$[8]\cdot[512]\cdot[32\times8\times4]^{34}$	2^{272}	378	566
384	64	(64^{64})	195	$[64]^{6}\cdot[16\times4]^{58}$	2^{232}	252	421
384	55	$(64\cdot128^{54})$	330	$[64]\cdot[128]^{3}\cdot[32\times4]^{51}$	2^{255}	287	466
384	48	(256^{48})	578	$[256]^{2}\cdot[16\times4\times4]^{46}$	2^{276}	303	485
384	43	$(64\cdot512^{42})$	1013	$[64]\cdot[512]\cdot[32\times4\times4]^{41}$	2^{287}	352	535
384	39	$(16\cdot1024^{38})$	1827	$[16]\cdot[1024]\cdot[32\times8\times4]^{37}$	2^{296}	364	554

2 ПОВНІСТЮ АПЕРІОДИЧНІ ЛОГАРИФМІЧНІ ПІДПИСИ

2.1 Повністю аперіодичні логарифмічні підписи для абелевих груп

У класі $A(G)$ аперіодичних логарифмічних підписів заслуговує на увагу підклас, який називається повністю аперіодичними логарифмічними підписами, який позначатиметься як $SA(G)$.

Просте спостереження показує, що властивість аперіодичності логарифмічного підпису зберігається при описаних вище перетвореннях, за винятком злиття. З'єднання двох або більше блоків аперіодичного логарифмічного підпису може призвести до періодичного логарифмічного підпису.

Є важливим те, що при об'єднанні всіх блоків логарифмічного підпису β буде отримано один блок, а саме власне групу G, яка, у свою чергу, є тривіальним періодичним логарифмічним підписом, що є вартим виключення. Таким чином, злиття можливо здійснити на будь-якому наборі не більше $s - 1$ блоків β. Загалом було очікуваним, що дозволено будь-яке нетривіальне злиття, однак це не завжди так, як буде видно з наступних результатів, як показано в книзі Жабо [13] для абелевих p-груп.

Теорема. Нехай p просте і нехай G – абелева група порядку p^n. Далі нехай $r_1 \geq r_2 \geq \cdots \geq r_s \geq p$ – степені p такі, що

$$\prod_{i=1}^{s} r_i = p^n:$$

1) Нехай $p = 2$ та G – елементарна абелева 2-група. Логарифмічний підпис α типу $(r_1, \dots, r_s)$ з $r_1 \geq \cdots \geq r_s \geq 2$ може бути лише аперіодичним, якщо:
   - $s = 2$ та $r_2 \geq 8$, або
   - $s \geq 3$ та $r_1 \geq 8, r_2 \geq \cdots \geq r_s \geq 4$.

   α завжди є періодичним для кожного з наступних випадків:
   - $r_s = 2$,
   - $s = 2$ та $r_2 | 4$,
   - $s \geq 3$ та $r_1 | 4, \dots r_s | 4$;
2) Нехай $p = 3$ та G не є циклічним або нетиповим $(3^{n-1}, 3)$. Нехай $(r_1, \dots, r_s) \in \{(3, \dots, 3), (3^2, 3, \dots, 3), (3^{n-1}, 3)\}$, Тоді існують аперіодичні логарифмічні підписи типу $(r_1, \dots, r_s)$ для G;
3) Нехай $p = 2$ та G не є циклічним або нетиповим $(r_1, \dots, r_s) \neq (p, \dots, p)$. Тоді існують аперіодичні логарифмічні підписи типу $(r_1, \dots, r_s)$ для G.

Нехай існує аперіодичний логарифмічний підпис $\beta = [B_1, \dots, B_s]$ за умови $s \geq 3$ для елементарної абелевої 2-групи G. З теореми $|B1| \geq 8$ і $|Bi| \geq 4$ за умови $2 \leq i \leq s$. Якщо β має тип $|Bi| \geq 8$ для $1 \leq i \leq s$, тоді β є повністю аперіодичним, коли будь-яке злиття щонайбільше $s - 1$ блоків призводить до аперіодичного логарифмічного підпису.

Проте якщо припустити, наприклад, що $|B_1| = 8$ і $|B_2| = \dots = |B_s| = 4$, тоді β є повністю аперіодичним, якщо будь-яке злиття його блоків призводить до аперіодичного логарифмічного підпису γ, коли тип γ задовольняє умовам аперіодичності наведеної теореми.

Це говорить, зокрема, про те, що якби блок B_1 був об'єднаний з $(s - 2)$ іншими блоками, результатом був би логарифмічний підпис γ типу $(2^{3+2(s-2)}, 4)$, що є періодичним відповідно до теореми. Отже, такий тип злиття для β є «неприпустимим». Іншими словами, блок B_1 можливо об'єднати щонайбільше з $(s - 3)$ іншими блоками. Більше того, об'єднання всіх блоків $B_2, \dots, B_s$ β разом допустимо, оскільки це призведе до логарифмічного підпису типу $(8, 2^{2(s-1)})$, що не порушує умови аперіодичності теореми. Теорема обґрунтовує наведене нижче визначення.

Нехай G – абелева група і $\beta = [B_1, \dots, B_s] \in A(G)$. Злиття певних d-блоків $B_{i1}, \dots, B_{i_d}$ називається допустимим, якщо тип результуючого логарифмічного підпису γ не порушує необхідних умов аперіодичності. Нехай $\{d_1, \dots, d_t\}$ – множина натуральних чисел, d_i вказує найбільшу можливу кількість блоків, дозволених допустимим злиттям певного «типу». Значення $d_1, \dots, d_t$ називаються допустимими ступенями злиття β. Буде вважитися, що β досягає допустимих ступенів злиття, якщо для кожного $d_i \in \{d_1, \dots, d_t\}$ будь-яке «припустиме» злиття $d_i \in \{d_1, \dots, d_t\}$-блоків β призводить до аперіодичного логарифмічного підпису.

Наприклад, нехай $\beta = [B_1, B_2, \dots, B_s]$, $s \geq 3$ – аперіодичний логарифмічний підпис типу $(8,4,4,\dots,4)$ для елементарної абелевої групи G порядку 2^{2s+1}. Тоді з теореми та визначення вище допустимі ступені злиття β дорівнюють $\{s - 2, s - 1\}$.

Визначення: нехай G – абелева група і $\beta = [B_1, \dots, B_s] \in A(G)$. Логарифмічний підпис β називається повністю аперіодичним, якщо він досягає допустимих ступенів злиття. Втім, це не відноситься до неабелевих груп. Це пов'язано з тим, що об'єднання непослідовних блоків майже заборонено, оскільки в цьому випадку результат більше не є логарифмічним підписом.

Як приклад, буде використано налаштування для G, H і T і θ, як у попередньому прикладі. Нехай

$$L_1 = \{A_{1.1} = \{1, g_1, g_2, g_1g_2\}, A_{1.2} = \{1, g_1g_2g_4g_6, g_2g_3g_5, g_1g_3g_4g_5g_6\}\},$$
$$L_2 = \{A_{2.1} = \{1, g_3, g_4, g_3g_4\}, A_{2.2} = \{1, g_1g_3, g_2g_4, g_1g_3g_2g_4\}\},$$
$$L_3 = \{A_{3.1} = \{1, g_5, g_6, g_5g_6\}, A_{3.2} = \{1, g_1g_5, g_2g_6, g_1g_5g_2g_6\}\}.$$

Тоді стає можливим отримати аперіодичний логарифмічний підпис $\beta = [B_1, B_2, B_3]$ типу (8,8,8) для G з

$$B_1 = \{1, g_1, g_2, g_1g_2, g_7, g_1g_2g_4g_6g_7, g_2g_3g_5g_7, g_1g_4g_5g_7g_7\},$$
$$B_2 = \{1, g_3, g_4, g_3g_4, g_8, g_1g_3g_8, g_2g_4g_8, g_1g_3g_2g_4g_8\},$$
$$B_3 = \{1, g_5, g_6, g_5g_6, g_9, g_1g_5g_9, g_2g_6g_9, g_1g_5g_2g_6g_9\}.$$

Тепер можливо перевірити, що злиття будь-яких двох блоків β дає аперіодичний блок. Отже, β є повністю аперіодичним. Слід зауважити, що логарифмічний підпис β у першому прикладі є аперіодичним, але не повністю аперіодичним, бо при з'єднанні B_1 з B_2 результатом стане періодичний блок. Більше того, B_1B_2 є підгрупою порядку 2^6 в G.

Оскільки далі буде використовуватися алгоритм Баумейстера-де Вільєса («BW-конструкція») для дослідження повністю аперіодичних логарифмічних підписів, слід здійснити наступне просте спостереження щодо операції злиття на логарифмічному підпису, отриманому з BW-конструкції.

Лема: використовуються позначення, як описано в BW-конструкції вище. Об'єднання блоків B_i і B_j, $i \neq j$, β призводить до логарифмічного підпису, що знову випливає з BW-конструкції, в якій L_i і L_j замінені на L_iL_j, а T_i і T_j на T_iT_j.

Наступна лема корисна для запиту про сильну аперіодичність логарифмічного підпису.

Лема: нехай G – абелева група. Нехай $\beta = [B_1, B_2, B_3]$ буде логарифмічним підписом для G. Нехай $I \subseteq \{1, \dots, s\}$, а злитий блок $\prod_{i\in I} B_i$ аперіодичний. Тоді стає очевидним, що $\prod_{j\in J} B_J$ є аперіодичним для будь-якої непорожньої підмножини $J \subseteq I$.

Доведення: перемішування елементів не впливає на періодичність. Якщо припустити за методом протиріччя, що $B_J := \prod_{j\in J} B_J$ є періодичним для підмножини $J \subseteq I$, $g \in G\backslash\{1\}$ є періодичним для B_J, множина

$$B_I := \prod_{i\in I} B_i, \text{ а } B_I = B_J \cdot C,$$

де

$$C := \prod_{k \in I \setminus J} B_k$$

(при цьому B_I в лівій частині рівності $B_I = B_J \cdot C$ розглядається як невпорядкована множина, оскільки перестановка елементів B_I не впливає на властивість аперіодичності), випливає, що оскільки g є періодом для B_J, $gB_I = gB_J \cdot C = B_J \cdot C = B_I$. Таким чином ствердження про те, що g є періодом для B_I, є протиріччям.

Остання лема є важливим інструментом. За необхідності перевірити сильну аперіодичність логарифмічного підпису β, що має s блоків та умови, що дозволяється об'єднати до будь-яких $s - 1$ блоків β, без цієї леми було б необхідним перевірити всі

$$(s/1) + (s/2) + \cdots + (s/s - 1) = 2^s - 2$$

можливі злиття блоків β, тоді як за нею достатньо лише перевірити $(s/s - 1) == s$ злиття всіх комбінацій $s - 1$ блоків β.

У решті розділів наводяться конструкції повністю аперіодичних підписів для елементарних абелевих p-груп. Основним інструментом залишається BW-конструкція. Спочатку будуватимуться певні типи аперіодичних логарифмічних підписів, а потім на подальшому більш складному кроці буде доведено, що вони повністю аперіодичні.

Відтепер нехай G – елементарна абелева p-група. Буде використовуватися адитивне позначення для групової операції, а 0 буде позначати тотожність G. Фактично G ототожнюється з адитивною групою області Галуа F_{p^n}. Таким чином, G буде розглядатися як векторний простір розмірності n над F_p, і тому стає можливим вільно використовувати мову лінійної алгебри відносно абелевої p-групи G. Наприклад, мінімальний набір генераторів для G можливо назвати базисом для G.

2.2 Повністю аперіодичні логарифмічні підписи типу $(p^3, \dots, p^3)$

У цьому розділі спочатку будуватиметься повністю аперіодичний логарифмічний підпис типу $(\mathrm{p}^3, \dots, \mathrm{p}^3)$ для елементарної абелевої p-групи G порядку p^{3s}, де $\mathrm{p} = 2$ або p – непарне просте і $s \geq 2$. Нехай

$$v_1, v_2, \ldots, v_{2s}, \ldots, v_{3s} -$$

генератор G. Використовуючи конструювання за алгоритмом Баумейстера-де Вільєса, стає можливим визначити:

$$1)\ T = \langle v_{2s+1}, \ldots, v_{3s} \rangle \text{ та } \theta = |T_1, \ldots, T_s| \text{ при}$$

$$T_i = \{0, v_{2s+1}, 2v_{2s+1}, \ldots, (p-1)v_{2s+i}\} \text{ для } i = 1, \ldots, s;$$

$$2)\ H = \langle v_1, \ldots, v_{2s} \rangle.$$

Нехай $u = \{1, \ldots, p-1\} = F_p \backslash \{0\}$ буде обраним параметром. Для $i = 1, \ldots, s$ множину

$$L_i = \{A_{i,0}, A_{i,1}, \ldots, A_{i,(p-1)}\}$$

буде визначено наступним чином.

$$A_{1,0} = \langle v_1, v_2 \rangle, A_{i,j} = \langle v_1 + v_2 + j \cdot \sum_{l=2}^{n} v_{2l}, u \cdot v_2 + j \cdot \sum_{l=2}^{n} v_{2l-1} \rangle \text{ для всіх } j \in \{1, \ldots, p-1\},$$

$$A_{i,j} = \langle v_{2i-1} + jv_1, v_{2i} + jv_{2,} \rangle \text{ для всіх } i \in \{2, \ldots, s\}, j \in \{0, \ldots, p-1\}.$$

Примітка: слід зауважити, що в формули з пункту 1 можливо замінити T будь-яким трансверсальним TR групи H. Тут TR взагалі не є підгрупою. Насправді, легко створити логарифмічний підпис для трансверсалі H, перейшовши до групи факторів $\bar{T} = G/H$. А саме, нехай $\bar{\theta} = |T_1, \ldots, T_s|$ – Логарифмічний підпис для $\bar{T}$, де

$$T_i = \left|x_{i,0}H, \ldots, x_{i,(p-1)}H\right|, 1 \leq i \leq s.$$

Слід звернути увагу, що є $|H|$ можливостей вибору $x_{i,j}$ як представника класу. Піднявши $\bar{\theta}$ до G, результатом стає логарифмічний підпис

$$\theta = |T_1, \ldots, T_s| \text{ з } T_i = \left|x_{i,0}, \ldots, x_{i,(p-1)}\right|$$

для певної трансверсалі TR H.

Тепер слід довести, що підмножини $A_{i,j}$ множини L_i, $1 \leq i \leq s$ задовольняють другій умові BW-конструкції. Це означає, що для будь-якого $(j_1, j_2, \ldots, j_s) \in \{0, 1, \ldots, p-1\}^s$s множина $[A_{1,j_1}, A_{2,j_2}, \ldots, A_{s,j_s}]$ утворює

логарифмічний підпис для H. Це еквівалентно ствердженню, що основні елементи $A_{1,j_1}, A_{2,j_2}, \dots, A_{s,j_s}$ є лінійно незалежними.

Спочатку буде розглянуто випадок $j_1 = 0$. Тоді:

$$A_{1,j_1} = \langle v_1, v_2 \rangle, A_{2,j_2} = \langle j_2 \cdot v_1 + v_3, j_2 \cdot v_2 + v_4 \rangle,$$
$$A_{3,j_3} = \langle j_3 \cdot v_1 + v_5, j_3 \cdot v_2 + v_6 \rangle, \dots, A_{s,j_s} = \langle j_s \cdot v_1 + v_{2s-1}, j_s \cdot v_2 + v_{2s} \rangle.$$

При формуванні лінійної комбінації базових елементів $A_{1,0}, A_{2,j_2}, \dots, A_{s,j_s}$ для нульового елемента є рівним наступне рівняння:

$$0 = \lambda_{1.1}(v_1) + \lambda_{1.2}(v_2) + \lambda_{2.1}(v_{2i-1} + j_2 v_1) + \lambda_{2.2}(v_{2i} + j_2 v_2) + \cdots$$
$$+ \lambda_{s.1}(v_{2s-1} + j_s v_1) + \lambda_{s.2}(v_{2s} + j_s v_2)$$

при $\lambda_{i.j} \in F_p$. Матрична форма цього рівняння має вигляд:

$$(\lambda_{1.1}, \lambda_{1.2}, \dots, \lambda_{s.1}, \lambda_{s.1})M = (0,0, \dots, 0),$$

де M – наступна $(2s \times 2s)$-матриця над F_p.

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ j_2 & 0 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & j_2 & 0 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ j_3 & 0 & 0 & 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & j_3 & 0 & 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ j_s & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & j_s & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 \end{pmatrix}.$$

Оскільки M є нижньою трикутною матрицею з усіма 1 на головній діагоналі, M є оборотним, і рівняння має $\lambda_{i.j} = 0$ для всіх $1 \le i \le s$ і $1 \le j \le 2$ як єдиний розв'язок. Таким чином, базові елементи $A_{1,j_1}, A_{2,j_2}, \dots, A_{s,j_s}$ є лінійно незалежними. Це говорить, зокрема, про те, що $[A_{1,j_1}, A_{2,j_2}, \dots, A_{s,j_s}]$ утворює логарифмічний підпис для H.

Тепер буде розглянуто випадок $j_1 \neq 0$. Тоді:

$$A_{1,j_1} = \langle v_1 + v_2 + j_1 \sum_{l=2}^{s} v_{2l}, u \cdot v_2 + j_1 \sum_{l=2}^{s} v_{2l-1} \rangle,$$
$$A_{2,j_2} = \langle j_2 \cdot v_1 + v_3, j_2 \cdot v_2 + v_4 \rangle, \; A_{3,j_3} = \langle j_3 \cdot v_1 + v_5, j_2 \cdot v_2 + v_6 \rangle, \dots$$
$$A_{s,j_s} = \langle j_s \cdot v_1 + v_{2s-1}, j_s \cdot v_2 + v_{2s} \rangle,$$

і лінійна комбінація нульового елемента буде виглядати таким чином:

$$0 = \lambda_{1.1}\left(v_1 + v_2 + j_1\sum_{l=2}^{s} v_{2l}\right) + \lambda_{1.2}\left(u \cdot v_2 + j_1\sum_{l=2}^{s} v_{2l-1}\right) + \\ +\lambda_{2.1}(v_{2i-1} + j_2 v_1) + \lambda_{2.2}(v_{2i} + j_2 v_2) + \cdots \\ + \lambda_{s.1}(v_{2s-1} + j_s v_1) + \lambda_{s.2}(v_{2s} + j_s v_2) \quad (2.1)$$

Матриця коефіцієнтів M рівняння 2.1 має вигляд

$$M = \begin{pmatrix} 1 & 1 & 0 & j_1 & 0 & j_1 & \dots & j_1 & 0 & j_1 \\ 0 & u & j_1 & 0 & 0 & 0 & \dots & 0 & j_1 & 0 \\ j_2 & 0 & 1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & j_2 & 0 & 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ j_3 & 0 & 0 & 0 & 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & j_3 & 0 & 0 & 0 & 1 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots \\ j_s & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 \\ 0 & j_s & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 1 \end{pmatrix}$$

Віднімаючи j_1, помножену на рядки $4,6,\dots,2s$ з першого рядка, а також помножуючи j_1 на рядки $3,5,\dots,2s-1$ з другого рядка M, отримано наступну матрицю:

$$\begin{pmatrix} 1 & 1 - j_l * \sum_{l=2}^{s} j_l & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ -j_l * \sum_{l=2}^{s} j_l & u & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ j_2 & 0 & 1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & j_2 & 0 & 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ j_3 & 0 & 0 & 0 & 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & j_3 & 0 & 0 & 0 & 1 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots \\ j_s & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 \\ 0 & j_s & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 1 \end{pmatrix}$$

з визначником $u + (1 - J)J = -(J^2 - J - u)$, де $J = j_1 \sum_{l=2}^{s} j_l$. Оскільки для кожного заданого p можливо вибрати $au \in F_p \setminus \{0\}$ так, що поліном $X^2 - X - - u \in F_p[X]$ не має кореня в F_p, можливо зробити висновок, що

матриця M є оборотною, а отже, рівняння 2.1 має єдине рішення з $\lambda_{i.j} = 0$ для всіх $1 \leq i \leq s$ і $1 \leq j \leq 2$. Отже, базові елементи $A_{1,j_1}, A_{2,j_2}, \ldots, A_{s,j_s}$ є лінійно незалежними. Отже $[A_{1,j_1}, A_{2,j_2}, \ldots, A_{s,j_s}]$ утворює логарифмічний підпис для H.

Таким чином, побудовано логарифмічний підпис β типу $(p^3, \ldots, p^3)$ для G за методом Баумейстера та де Вільєса. Використовуючи той факт, що $A_{i,j} \cap A_{i,k} = \{0\}$ для будь-яких $A_{i,j}, A_{i,k} \in \mathrm{L_i}$ з $j \neq k$ і для всіх $1 \leq i \leq s$, можливо зробити висновок, що β є аперіодичним.

Повна аперіодичність β буде доведена наступною теоремою.

Теорема: побудований вище логарифмічний підпис β типу $(\mathrm{p}^3, \ldots, \mathrm{p}^3)$ є повністю аперіодичним.

Доведення: слід нагадати, що в першій лемі сказано, що об'єднання будь-яких двох блоків β призводить до логарифмічного підпису, який знову отримується з BW-конструкції. Використовуючи другу лему, потрібно лише розглянути злиття будь-яких $(s-1)$ блоків β.

Нарешті, можливо використати одну з пропозицій, щоб показати, що результуючий логарифмічний підпис, отриманий від кожного такого злиття, є аперіодичним. Це робиться, показуючи, що злиття будь-яких $(s-1)$ множин L_i дає набір підгруп групи G, які мають у своєму перетині лише ідентичний елемент 0 для G. Для цього існує три способи.

Спосіб 1 – злиття $L_2, \ldots, L_s$. Нехай $L_2 + \ldots + L_s$ – множина, отримана шляхом злиття $L_2, \ldots, L_s$. Підмножини $L_2 + \ldots + L_s$ мають вигляд $(A_{1,j_1}, A_{2,j_2}, \ldots, A_{s,j_s})$ з $(j_1, j_2, \ldots, j_s) \in \{0, 1, \ldots, p-1\}^{s-1}$. Наступні рівняння доведуть це.

$$\bigcup_{\substack{\forall (j_1, j_2, \ldots, j_s) \\ \in \{0,1,\ldots,p-1\}^{s-1}}} A_{2,j_2} + A_{3,j_3} + \cdots + A_{s,j_s} = \{0\}$$

$$(A_{2,0} + A_{3,0} + \cdots + A_{s,0}) \cap (A_{2,1} + A_{3,0} + \cdots + A_{s,0}) =$$

$$= \langle v_3, v_4, v_5, v_6, \ldots, v_{2s-1}, v_{2s} \rangle \cap \langle v_1 + v_3, v_2 + v_5 + v_4, v_5, v_6, \ldots, v_{2s-1}, v_{2s} \rangle =$$

$$= \langle v_5, v_6, \ldots, v_{2s-1}, v_{2s} \rangle = A_{3,0} + A_{4,0} + A_{s,0}$$

$$(A_{2,0} + A_{3,0} + A_{4,0} + \cdots + A_{s,0}) \cap (A_{2,0} + A_{3,1} + A_{4,0} + \cdots + A_{s,0}) =$$

$$= A_{2,0} + A_{4,0} + \cdots + A_{s,0}, \ldots,$$

$$(A_{2,0} + \cdots + A_{s-1.0} + A_{s,0}) \cap (A_{2,0} + A_{s-2,0} + A_{s-1,1} + A_{s,0}) =$$

$$= A_{2,0} + A_{3,0} + \cdots + A_{s+2,0} + A_{s,0}$$

$$(A_{2,0} + \cdots + A_{s-1.0} + A_{s,0}) \cap (A_{2,0} + A_{3,0} + \cdots + A_{s-1,0} + A_{s,1}) = \\ = A_{2,0} + A_{3,0} + \cdots + A_{s-1,0}$$

Очевидно, що перетин елементів у правій частині наведених вище рівнянь є тривіальним.

Спосіб 2 – злиття $L_1, L_2, \ldots, L_s$. Аналогічно це можливо довести шляхом використання наступних рівнянь.

$$\bigcup_{\substack{\forall(j_1,j_2,\ldots,j_s) \\ \in\{0,1,\ldots,p-1\}^{s-1}}} A_{1,j_1} + A_{2,j_2} + \cdots + A_{s-1,j_{s-1}} = \{0\}$$

$$A_{1,0} = \langle v_1, v_2\rangle, A_{1,j} = \langle v_1 + v_2 + j\sum_{l=2}^{s} v_{2l}, u \cdot v_2 + j\sum_{l=2}^{s} v_{2l-1}\rangle,$$

$$j \in \{1, \ldots, p-1\},$$

$$A_{i,j} = \langle v_{2i-1} + jv_1, v_{2i} + jv_2\rangle, i \in \{2, \ldots, s\}, j \in \{0, \ldots, p-i\}.$$

$$(A_{1,0} + A_{2,0} + \cdots + A_{s-1,0}) \cap (A_{1,1} + A_{2,0} + \cdots + A_{s-1,0}) =$$

$$= \langle v_1, v_2, v_3, v_4, \ldots, v_{2s-3}, v_{2s-2}\rangle \cap \langle v_1 + v_2 + \sum_{l=2}^{s} v_{2l}, u \cdot v_2 + \\ + \sum_{l=2}^{s} v_{2l-1}, v_3, v_4, \ldots, v_{2s-3}, v_{2s-2}\rangle = \langle v_3, v_4, \ldots, v_{2s-3}, v_{2s-2}\rangle = A_{2,0} + A_{3,0} + \\ + \cdots + A_{s-1,0}$$

.

$$(A_{2,0} + A_{3,0} + \cdots + A_{s-1,0}) \cap (A_{1,1} + A_{2,1} + A_{3,0} + \cdots + A_{s-1,0}) \\ = (A_{2,0} + A_{3,0} + \cdots + A_{s-1,0}) \cap (A_{2,1} + A_{3,0} + \cdots + A_{s-1,0}) =$$

$$= \langle v_3, v_4, v_5, \ldots, v_{2s-3}, v_{2s-2}\rangle \cap \langle v_3 + v_1, v_4 + v_2, \ldots, v_{2s-3}, v_{2s-2}\rangle =$$

$$= \langle v_5, v_6, \ldots, v_{2s-3}, v_{2s-2}\rangle = (A_{3,0} + \cdots + A_{s-1,0}).$$

$$(A_{3,0} + \cdots + A_{s-1,0}) \cap (A_{1,1} + A_{2,0} + A_{3,1} + A_{4,0} + \cdots + A_{s-1,0}) = \\ = (A_{3,0} + \cdots + A_{s-1,0}) \cap (A_{2,0} + A_{3,1} + A_{4,0} + \cdots + A_{s-1,0}) =$$

$$= \langle v_5, v_6, \ldots, v_{2s-3}, v_{2s-2}\rangle \cap \langle v_3, v_4, v_5 + v_1, v_6 + v_2, v_7 \ldots, v_{2s-3}, v_{2s-2}\rangle =$$

$$= \langle v_7, v_8, \ldots, v_{2s-3}, v_{2s-2}\rangle = A_{4,0} + \cdots + A_{s-1,0}.$$

Цей процес необхідно повторювати до тих пір, поки не буде отримано $\{0\}$ як перетин.

Спосіб 3 – злиття $L_1, \ldots, L_{k-1}, L_{k+1}, \ldots, L_{s-1}, L_s$ для всіх $k \in \{2,3, \ldots s-2, s-1\}$. Процес доведення при використанні цього сценарію є аналогічним попереднім.

$$\bigcap_{\substack{\forall(j_1,\dots j_{k-1},j_{k+1},\dots,j_s)\\ \in\{0,1,\dots,p-1\}^{s-1}}} \left(A_{1,j_1}+\dots+A_{k-1,j_{k-1}}+A_{k+1,j_{k+1}}\dots+A_{s,j_s}\right)=\{0\}$$

Слід визначити ізоморфізм Φ групи G так:

$$\Phi(v_i)=\begin{cases} v_{2s-1} \text{ якщо } i=2k-1\\ v_{2k-1} \text{ якщо } i=2s-1\\ v_{2s} \text{ якщо } i=2k\\ v_{2k} \text{ якщо } i=2s\\ v_i \text{ інакше}\end{cases}.$$

Таким чином, Φ замінює v_{2k-1} на v_{2s-1}, v_{2k} на v_{2s} та фіксує решту твірних. Тоді є вірним наступне:

$$\Phi\left(A_{1,j_1}\right)=\Phi(\langle v_1+v_2+j_1\textstyle\sum_{l=2}^{s}v_{2l}\,,u\cdot v_2+j_1\sum_{l=2}^{s}v_{2l-1}\rangle)=A_{1,j_1},$$

$$\Phi\left(A_{2,j_2}\right)=\Phi(\langle j_2\cdot v_1+v_3,j_2\cdot v_2+v_4\rangle)=A_{2,j_2},\dots,$$

$$\Phi\left(A_{k-1,j_{k-1}}\right)=\Phi\left(\langle j_{k-1}\cdot v_1+v_{2(k-1)-1},j_2\cdot v_2+v_{2(k-1)}\rangle\right)=A_{k-1,j_{k-1}},\dots,$$

$$\Phi\left(A_{k,j_k}\right)=\Phi(\langle j_k\cdot v_1+v_{2k-1},j_k\cdot v_2+v_{2k}\rangle)=\langle j_k\cdot v_1+v_{2s-1},j_k\cdot v_2+v_{2s}\rangle=A_{s,j_k},$$

$$\Phi\left(A_{k+1,j_{k+1}}\right)=\Phi\left(\langle j_{k+1}\cdot v_1+v_{2(k+1)-1},j_2\cdot v_2+v_{2(k+1)}\rangle\right)=A_{k+1,j_{k+1}},$$

$$\Phi\left(A_{s-1,j_{s-1}}\right)=\Phi\left(\langle j_{s-1}\cdot v_1+v_{2(s-1)-1},j_2\cdot v_2+v_{2(s-1)}\rangle\right)=A_{s-1,j_{s-1}},$$

$$\Phi\left(A_{s,j_s}\right)=\Phi(\langle j_s\cdot v_1+v_{2s-1},j_s\cdot v_2+v_{2s}\rangle)=\langle j_s\cdot v_1+v_{2k-1},j_s\cdot v_2+v_{2k}\rangle=A_{k,j_s}.$$

$$\bigcap_{\substack{\forall(j_1,j_2\dots j_s)\\ \in\{0,1,\dots,p-1\}^{s-1}}} \left(A_{1,j_1}+A_{2,j_2}+\dots+A_{s-1,j_{s-1}}\right)=\{0\}$$

$$\bigcap_{\substack{\forall(j_1,j_2\dots j_s)\\ \in\{0,1,\dots,p-1\}^{s-1}}} \left(\Phi\left(A_{1,j_1}\right)+\Phi\left(A_{2,j_2}\right)+\dots+\Phi\left(A_{s-1,j_{s-1}}\right)\right)=\{0\}$$

$$\bigcap_{\substack{\forall(j_1,j_2\dots j_s)\\ \in\{0,1,\dots,p-1\}^{s-1}}} \left(A_{1,j_1}+\dots+A_{k-1,j_{k-1}}+\Phi\left(A_{k,j_k}\right)+A_{k+1,j_{k+1}}+\dots+A_{s-1,j_{s-1}}\right)=$$

$$=\{0\}$$

$$\bigcap_{\substack{\forall(j_1,j_2\dots j_s)\\ \in\{0,1,\dots,p-1\}^{s-1}}} \left(A_{1,j_1}+\dots+A_{k-1,j_{k-1}}+A_{s,j_k}+A_{k+1,j_{k+1}}+\dots+A_{s-1,j_{s-1}}\right)=\{0\}$$

Кожне рівняння випливає з попереднього. На цьому процес доведення закінчено у необхідний та достатній шлях.

При цьому повністю аперіодичний логарифмічний підпис β типу (8,8,8) у прикладі, наведеному вище, є необхідним будувати методом, наведеним у цьому розділі.

2.3 Повністю аперіодичні логарифмічні підписи типу $(2^3, 2^2, \dots, 2^2)$

У цьому розділі буде побудовано повністю аперіодичні логарифмічні підписи типу $(2^3, 2^2, \dots, 2^2)$ для елементарної абелевої 2-групи G порядку 2^{2s-1} з $s \geq 4$. Нехай $v_1, v_2, \dots, v_s, v_{s+1}$ — генератор G. Використовуючи алгоритм конструювання аперіодичних логарифмічних підписів Баумейстера-де Вільєса, потрібно визначити:

1) $T = \langle v_{s+1}, \dots, v_{2s-1}\rangle$ та $\theta = [T_1, T_3, T_4, \dots, T_s]$ з $T_1 = \{0, v_{s+1}\}$ та $T_i = \{0, v_{s+(i-1)}\}$ для $i = 3,4, \dots, 2s$;

2) $H = \langle v_1, \dots, v_s\rangle$.

Слід зауважити, що з метою спрощування опису алгоритму пропущено сценарій $i = 2$ при індексації множин L_i, а також блоків T_i, так що розглядаються лише $s - 1$ блоків.

Для $i = 1,3,4, \dots, s$ слід визначити множину $L_i = \{A_{i,0}, A_{i,1}\}$ наступним чином:

$$A_{i,0} = \langle v_1, v_2\rangle, A_{i,1} = \langle v_1 + \textstyle\sum_{l=1}^{[i/2]} v_{2l}\rangle, \text{ якщо } i \text{ непарне}$$
$$A_{i,0} = \langle v_1\rangle, A_{i,1} = \langle v_1 + \textstyle\sum_{l=1}^{i/2} v_{2l-1}\rangle, \text{ якщо } i \text{ парне}$$

Аналогічно є можливим вибрати θ як логарифмічний підпис для певної трансверсальної $TR\ H$ в G. Для уможливлення цього сценарію спочатку слід довести, що для будь-якого вибору $(j_1, j_2, \dots, j_s) \in \{0,1\}^{s-1}$ відповідна множина $[A_{1,j_1}, A_{2,j_2}, \dots, A_{s,j_s}]$ утворює логарифмічний підпис для H. Еквівалентно це показує, що лінійна комбінація нульового елемента G відносно базових елементів дорівнює $A_{1,j_1}, A_{3,j_3}, A_{4,j_4}, \dots, A_{s,j_s}$, тобто

$$0 = \lambda_1 \left(v_1 + j_1 \sum_{l=2}^{[s/2]} v_{2l-1}\right) + \lambda_{1.2} \left(v_2 + j_1 \sum_{l=2}^{[s/2]} v_{2l}\right) + + \sum_{i=2}^{[(s-1)/2]} \lambda_{2i+1} (v_{2i+1} + + j_{2i+1} \sum_{l=2}^{i} v_{2l}) \cdot \sum_{i=2}^{[(s-1)/2]} \lambda_{2i} \cdot (v_{2i} + j_{2i} \sum_{l=2}^{i} v_{2l-1})$$

має мати лише тривіальний розв'язок $\lambda_i = 0$ для всіх $i = 1,3,\dots,s$. В свою чергу це означатиме, що матриця коефіцієнтів $(s \times s)$ $M_s(j_1, j_3, j_4, \dots, j_s)$ для λ_i рівняння 2.1 є оборотною.

Якщо s парне, то

$$M_s(j_1, j_3, j_4, \dots, j_s) = \begin{pmatrix} 1 & 0 & j_1 & 0 & j_1 & 0 & \cdots & j_1 & 0 & j_1 & 0 \\ 0 & 1 & 0 & j_1 & 0 & j_1 & \cdots & 0 & j_1 & 0 & j_1 \\ 0 & j_3 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ j_4 & 0 & j_4 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & j_5 & 0 & j_5 & 1 & 0 & \cdots & 0 & 0 & 0 & 0 \\ j_6 & 0 & j_6 & 0 & j_6 & 1 & \cdots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & j_{s-3} & 0 & 0 & j_{s-3} & 0 & \cdots & 1 & 0 & 0 & 0 \\ j_{s-2} & 0 & j_{s-2} & 0 & j_{s-1} & 0 & \cdots & j_{s-2} & 1 & 0 & 0 \\ 0 & j_{s-1} & 0 & j_{s-1} & 0 & j_{s-1} & \cdots & 0 & j_{s-1} & 1 & 0 \\ j_s & 0 & j_s & 0 & j_s & 0 & \cdots & j_s & 0 & j_s & 1 \end{pmatrix}$$

Якщо s непарне, то

$$M_s(j_1, j_3, j_4, \dots, j_s) = \begin{pmatrix} 1 & 0 & j_1 & 0 & j_1 & 0 & \cdots & j_1 & 0 & j_1 & 0 \\ 0 & 1 & 0 & j_1 & 0 & j_1 & \cdots & 0 & j_1 & 0 & j_1 \\ 0 & j_3 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ j_4 & 0 & j_4 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & j_5 & 0 & j_5 & 1 & 0 & \cdots & 0 & 0 & 0 & 0 \\ j_6 & 0 & j_6 & 0 & j_6 & 1 & \cdots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ j_{s-3} & 0 & j_{s-3} & 0 & j_{s-3} & 0 & \cdots & 1 & 0 & 0 & 0 \\ 0 & j_{s-2} & 0 & j_{s-2} & 0 & j_{s-2} & \cdots & j_{s-2} & 1 & 0 & 0 \\ j_{s-1} & 0 & j_{s-1} & 0 & j_{s-1} & 0 & \cdots & 0 & j_{s-1} & 1 & 0 \\ 0 & j_s & 0 & j_s & 0 & j_s & \cdots & j_s & 0 & j_s & 1 \end{pmatrix}$$

В обох випадках матриця є оборотною, якщо $j_1 = 0$. Тому буде вважатися, що $j_1 = 1$. За допомогою індукції за s потрібно показати, що визначник $M_s(j_1, j_3, j_4, \dots, j_s)$ в обох випадках дорівнює 1.

Для початку, якщо $s = 3$, то

$$M_3(j_1, j_3) = \begin{pmatrix} 1 & 0 & j_1 \\ 0 & 1 & 0 \\ 0 & j_3 & 1 \end{pmatrix} = 1$$

Тепер нехай $s > 3$. Якщо s парне, потрібно відняти j_s, помножений на перший рядок з останнього рядка, що призведе до наступного рівняння:

$$det M_s(j_1, j_3, j_4, \dots, j_s) =$$

$$= det \begin{pmatrix} 1 & 0 & j_1 & 0 & j_1 & 0 & \cdots & j_1 & 0 & j_1 & 0 \\ 0 & 1 & 0 & j_1 & 0 & j_1 & \cdots & 0 & j_1 & 0 & j_1 \\ 0 & j_3 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ j_4 & 0 & j_4 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & j_5 & 0 & j_5 & 1 & 0 & \cdots & 0 & 0 & 0 & 0 \\ j_6 & 0 & j_6 & 0 & j_6 & 1 & \cdots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \vdots \\ 0 & j_{s-3} & 0 & j_{s-3} & 0 & j_{s-3} & \cdots & 1 & 0 & 0 & 0 \\ j_{s-2} & 0 & j_{s-2} & 0 & j_{s-2} & 0 & \cdots & j_{s-2} & 1 & 0 & 0 \\ 0 & j_{s-1} & 0 & j_{s-1} & 0 & j_{s-1} & \cdots & 0 & j_{s-1} & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 1 \end{pmatrix} =$$

$$= det \begin{pmatrix} 1 & 0 & j_1 & 0 & j_1 & 0 & \cdots & j_1 & 0 & j_1 \\ 0 & 1 & 0 & j_1 & 0 & j_1 & \cdots & 0 & j_1 & 0 \\ 0 & j_3 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ j_4 & 0 & j_4 & 0 & j_4 & 0 & \cdots & 0 & 0 & 0 \\ 0 & j_5 & 0 & j_5 & 1 & 0 & \cdots & 0 & 0 & 0 \\ j_6 & 0 & j_6 & 0 & j_6 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ 0 & j_{s-3} & 0 & j_{s-3} & 0 & j_{s-3} & \cdots & 1 & 0 & 0 \\ j_{s-2} & 0 & j_{s-2} & 0 & j_{s-2} & 0 & \cdots & j_{s-2} & 1 & 0 \\ 0 & j_{s-1} & 0 & j_{s-1} & 0 & j_{s-1} & \cdots & 0 & j_{s-1} & 1 \end{pmatrix} =$$

$$= det M_{s-1}(j_1, j_3, j_4, \dots, j_{s-1})$$

Якщо s непарне, потрібно відняти j_s, помножений на другий рядок з останнього рядка, що призведе до такого рівняння:

$$det M_s(j_1, j_3, j_4, \dots, j_s) =$$

$$= det \begin{pmatrix} 1 & 0 & j_1 & 0 & j_1 & 0 & \cdots & 0 & j_1 & 0 & j_1 \\ 0 & 1 & 0 & j_1 & 0 & j_1 & \cdots & j_1 & 0 & j_1 & 0 \\ 0 & j_3 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ j_4 & 0 & j_4 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & j_5 & 0 & j_5 & 1 & 0 & \cdots & 0 & 0 & 0 & 0 \\ j_6 & 0 & j_6 & 0 & j_6 & 1 & \cdots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \vdots \\ j_{s-3} & 0 & j_{s-3} & 0 & j_{s-3} & 0 & \cdots & 1 & 0 & 0 & 0 \\ 0 & j_{s-2} & 0 & j_{s-2} & 0 & j_{s-2} & \cdots & j_{s-2} & 1 & 0 & 0 \\ j_{s-1} & 0 & j_{s-1} & 0 & j_{s-1} & 0 & \cdots & 0 & j_{s-1} & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$== det \begin{pmatrix} 1 & 0 & j_1 & 0 & j_1 & 0 & \cdots & j_1 & 0 & j_1 \\ 0 & 1 & 0 & j_1 & 0 & j_1 & \cdots & 0 & j_1 & 0 \\ 0 & j_3 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ j_4 & 0 & j_4 & 0 & j_4 & 0 & \cdots & 0 & 0 & 0 \\ 0 & j_5 & 0 & j_5 & 1 & 0 & \cdots & 0 & 0 & 0 \\ j_6 & 0 & j_6 & 0 & j_6 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ j_{s-3} & 0 & j_{s-3} & 0 & j_{s-3} & 0 & \cdots & 1 & 0 & 0 \\ 0 & j_{s-2} & 0 & j_{s-2} & 0 & j_{s-2} & \cdots & j_{s-2} & 1 & 0 \\ j_{s-1} & 0 & j_{s-1} & 0 & j_{s-1} & 0 & \cdots & 0 & j_{s-1} & 1 \end{pmatrix} =$$

$$= det M_{s-1}(j_1, j_3, j_4, \dots, j_{s-1})$$

В обох випадках індукція показує, що визначник дорівнює 1. Отже, $[A_{1,j_1}, A_{2,j_2}, \dots, A_{s,j_s}]$ утворює логарифмічний підпис для H.

Таким чином, побудовано логарифмічний підпис β типу $(2^3, 2^2, \dots, 2^2)$ для G за методом Баумейстера та де Вільєса. Використовуючи той факт, що $A_{i,1} \cap A_{i,2} = \{0\}$ для будь-якого $i = 1,3,4,\dots,s$, β є аперіодичним.

Далі буде доведено наступну теорему.

Теорема: побудований вище логарифмічний підпис β типу $(2^3, 2^2, \dots, 2^2)$ дуже схожий на періодичний.

Доказ повної аперіодичності для β дає ряд лем. З огляду на попередні теореми, слід розглянути два типи злиття для β:

1) Об'єднання всіх $(s-1)$ блоків розміром 2^2 кожен;
2) З'єднання будь-яких $(s-2)$ блоків, де один блок має розмір 2^3.

Для типу 1 злиття $L_3, L_4, \dots, L_s$ та для типу 2 злиття L_1 з будь-якими $(s-3)$ іншими множинами кожне L_i дає множину підгруп G, які мають лише

одиничний елемент 0 у своєму перетині.

Випадок 1: злиття $L_3, L_4, \ldots, L_s$.

Лема:

$$\bigcap_{\substack{\forall(j_2,j_4\ldots,j_{s-1},j_s)\\ \in\{0,1\}^{s-2}}} \left(A_{3,j_3} + A_{4,j_4} + \cdots + A_{s-1,j_{s-1}} + A_{s,j_s}\right) = \{0\}$$

Доведення. Буде розглянуто наступні дві суми та їхній перетин:

$$[A_{3,0} + A_{4,0} + A_{5,0} + \cdots + A_{s-2.0} + A_{s-1.0} + A_{s.1}] = \langle v_3, v_4, \ldots, v_{s-1}, v_s\rangle,$$
$$= \langle v_3, v_4, \ldots, v_{s-2}, v_{s-1}, v_s + v_{s-1} + v_{s-3} + \cdots\rangle$$

,

$$\langle v_3, v_4, \ldots, v_{s-1}, v_s\rangle.$$

Перетин випливає с того факту, що v_1 або v_2 зустрічається як доданок в останньому доданку другої суми. При подальшому перетині $\langle v_3, v_4, \ldots, v_{s-1}, v_s\rangle$ з сумою

$$A_{3,0} + A_{4,0} + A_{5,0} + \cdots + A_{s-3.0} + A_{s-2.0} + A_{s-1.1} + A_{s.0} =$$
$$= \langle v_3, v_4, \ldots, v_{s-3}, v_{s-2}, v_s(v_{s-1} + v_{s-2} + v_{s-4} + \cdots)\rangle$$

отримано наступну множину:

$$\langle v_3, v_4, \ldots, v_{s-3}, v_{s-2}\rangle,$$

як їх перетин, оскільки v_1 або v_2 зустрічається як доданок в останніх двох доданках суми. Виконуючи подальші ітерації, в кінцевому підсумку отримано $\{0\}$ як перетин, як й очікувалось.

Випадок 2: злиття L_1 зі $(s-3)$ іншими значеннями L_i.

Тепер нехай $I = \{i_1, \ldots, i_{s-3}\} \subseteq \{3,4,\ldots,s\}$ довільне з $|I| = s-3$. Нехай $\{3,4,\ldots,s\}\backslash I = \{k_1, k_2\}$, де вважається, що $k_1 < k_2$. Потрібно довести, що при

$$\bigcap_{\forall\begin{pmatrix} j_1,j_3,j_4\ldots, \\ j_{k_1-1},j_{k_1+1},\ldots \\ j_{k_2-1},j_{k_2+1},\ldots j_s \end{pmatrix} \in\{0,1\}^{s-3}} \left(\sum_{i\in I\cup\{1\}} A_{i,j_i}\right) = \{0\} \qquad (2.2)$$

виконується наступне рівняння:

$$\sum_{i\in I} A_{j,0} = \langle v_1, v_2, v_{i_1}, v_{i_2}, \ldots, v_{k_1-1}, v_{k_2-1}, \ldots, v_{i_s-2}\rangle.$$

Є три підвипадки, які необхідно обробляти окремо:

1) $k_1 \equiv k_2 \equiv 1\ mod\ 2$;
2) $k_1 \equiv k_2 \equiv 0\ mod\ 2$;
3) $k_1 + k_2 \equiv 1\ mod\ 2$.

Лема. Нехай $k_1 \equiv k_2 \equiv 1\ mod\ 2$. Тоді рівняння 2.2 виконується.

Доведення. Спочатку слід розглянути наступне рівняння:

$$A_{1,1} + \sum_{i\in I} A_{i,0} = \langle v_1 + v_3 + v_5 +, \ldots v_2 + v_4 + v_6 + \\ + \cdots v_{i_1}, v_{i_2}, \ldots, v_{k_1-1}, v_{k_2-1}, \ldots, v_{i_s-3}\rangle$$

Оскільки $v_1 \in A_{1,1} + \sum_{i\in I} A_{i,0}$ та $v_2 \in A_{1,1} + \sum_{i\in I} A_{i,0}$, то

$$C := \left(A_{1,1} + \sum_{i\in I} A_{i,0}\right) \cap \left(A_{1,1} + \sum_{i\in I} A_{i,0}\right) = \langle\{v_2\} \cup \{v_1 | i \in I\}\rangle.$$

Щоб обчислити подальші перетини, знадобиться ввести деякі позначення. При $i \in I$ нехай A_i визначається як

$$A_i := A_{i,1} + \sum_{j\in I, j\neq i} A_{j,0}.$$

Тоді

$$A_i = \langle\left\{v_j | j \in I\backslash\{i\}\right\} \cup \{v_i + v_{i-1} + v_{i-3} + \cdots\}\rangle.$$

Для $i, j \in I$ нехай $A_{i,j}$ буде визначено так:

$$A_{i,j} := A_{i,1} + A_{j,1} + \sum_{l\in I, l\neq i,j} A_{l,0}.$$

З цього випливає, що

$$A_{i,j} = \langle \{v_l | l \in I \backslash \{i,j\}\} \cup \{v_i + v_{i-1} + v_{i-3} + \cdots, v_j + v_{j-1} + v_{j-3} + \cdots\} \rangle.$$

Для доведення 2.2 буде виконано ряд кроків для різних сценаріїв.

Крок 1: k парне та $k > k_1$. Доведення:

$$C \cap (A_{1,0} + A_k) = \langle \{v_2\} \cup \{v_j | j \in I \backslash \{k\}\} \rangle.$$

Оскільки

$$A_{1,0} + A_k = A_{1,0} + \langle \{v_j | j \in I \backslash \{k\}\} \cup \{v_k + v_{k-1} + v_{k-3} + \cdots\} \rangle = \langle \{v_j | j \in I \backslash \{k\}\} \cup \{v_1, v_2, v_k + v_{k-1} + v_{k-3} + \cdots\} \rangle$$

$$\langle \{v_2\} \cup \{v_j | i \in I \backslash \{k\}\} \rangle \subseteq C \cap (A_{1,0} + A_k).$$

Крім того, оскільки $\langle \{v_2\} \cup \{v_j | i \in I \backslash \{k\}\} \rangle$ має корозмірність 1 у C, достатньо показати, що $v_k \in A_{1,0} + A_k$. Нехай, заради доведення шляхом протиріччя, $v_k \in A_{1,0} + A_k$. Тоді існують $\lambda_1, \lambda_2, \cdots \in \{0,1\}$ при

$$v_k = \lambda_1 v_1 + \lambda_2 v_2 + \lambda_k (v_k + v_{k-1} + v_{k-3} + \cdots) + \sum_{j \in I \backslash \{k\}} \lambda_j v_j.$$

Це призводить до протиріччя. Отже, для всіх $k > k_1$ з парними k

$$C \cap (A_{1,0} + A_k) = \langle \{v_2\} \cup \{v_j | j \in I \backslash \{k\}\} \rangle.$$

Нехай $I' := \{k \in I \mid k > k_1, k \text{ парне}\}$. Тоді

$$C'' := C \cap \left(\cap_{k \in I'} (A_{1,0} + A_k)\right) = \cap_{k \in I'} \left(C \cap (A_{1,0} + A_k)\right) = \cap_{k \in I'} \left(\langle \{v_2\} \cup \cup \{v_j | j \in I \backslash \{k\}\} \rangle\right) = \left(\langle \{v_2\} \cup \{v_j | j \in I \backslash I'\} \rangle\right)$$

Далі потрібно довести, що $C'' := C' \cap (A_{1,1} + A_{k_1+1}) = \langle \{v_j | j \in I \backslash I'\} \rangle$. Існує

$$A_{1,1} + A_{k_1+1} = A_{1,1} + \langle \{v_j | j \in I \backslash \{k_1 + 1\}\} \cup \{v_{k_1+1}, v_{k_1} + v_{k_1+2} + \cdots\} \rangle =$$
$$= \langle \{v_j | j \in I \backslash \{k_1 + 1\}\} \cup \{v_1 + v_3 + v_5 + \cdots, v_2 + v_4 + v_6 + \cdots, v_{k_1+1}, v_{k_1} + + v_{k_1+2} + \cdots\} \rangle$$

Оскільки $k_1 + 1 \in I'$, очевидно, що $\langle\{v_j | j \in I \backslash I'\}\rangle \subseteq C''$.

Крім того, оскільки $\langle\{v_j | j \in I \backslash I'\}\rangle$ має корозмірність 1 у C', достатньо показати, що $v_2 \notin A_{1,1} + A_{k_1+1}$. Нехай, шляхом протиріччя, $v_2 \in A_{1,1} + A_{k_1+1}$. Тоді існують $\lambda_1, \lambda_2, \cdots \in \{0,1\}$ при

$$v_2 = \lambda_1(v_1 + v_3 + v_5 + \cdots) + \lambda_2(v_2 + v_4 + v_6 + \cdots) + \lambda_{k_1+1}(v_{k_1+1} + v_{k_1} + \\ + v_{k_1-2} + \cdots) + \sum_{j \in I \backslash \{k_1+1\}} \lambda_j v_j$$

Але v_{k_2} зустрічається рівно один раз у правій частині цього рівняння, отже, $\lambda_1 = 0$; також, оскільки v_{k_1} зустрічається лише один раз у правій частині цього рівняння, $v_{k_1+1} = 0$; далі, оскільки v_{k_1+1} зустрічається лише один раз, то $\lambda_2 = 2$. Але це протиріччя.

Крок 2. k парне і $k < k_1$. Доведення:

$$C' \cap (A_{1,1} + A_{k,k_1+1}) = \langle\{v_j | j \in (I \backslash I') \backslash \{k\}\}\rangle.$$

$$A_{1,1} + A_{k,k_1+1} = A_{1,1} + \langle\{v_j | j \in I \backslash \{k, k_1+1\}\} \cup \{v_k, v_{k-1} + v_{k-3} + \\ + \cdots, v_{k_1+1}, v_{k_1} + v_{k_1+2} + \cdots\}\rangle = \langle\{v_j | j \in I \backslash \{k, k_1+1\}\} \cup \{v_1 + v_3 + v_5 + \\ + \cdots, v_2 + v_4 + v_6 + \cdots, v_k, v_{k-1} + v_{k-3} + \cdots, v_{k_1+1}, v_{k_1} + v_{k_1+2} + \cdots\}\rangle$$

$$\langle\{v_j | j \in (I \backslash I') \backslash \{k\}\}\rangle \subseteq C''' \cap (A_{1,1} + A_{k,k_1+1}).$$

Крім того, оскільки $\langle\{v_j | j \in (I \backslash I') \backslash \{k\}\}\rangle$ має корозмірність 1 у C'', достатньо показати, що $v_2 \notin A_{1,1} + A_{k,k_1+1}$. Нехай, шляхом протиріччя, $v_2 \in A_{1,1} + A_{k_1+1}$. Тоді існують $\lambda_1, \lambda_2, \cdots \in \{0,1\}$ при

$$v_k = \lambda_1(v_1 + v_3 + v_5 + \cdots) + \lambda_2(v_2 + v_4 + v_6 + \cdots) + \lambda_k(v_k + v_{k-1} + v_{k-3} + \\ + \cdots) + \lambda_{k_1+1}(v_{k_1+1} + v_{k_1} + v_{k_1-2} + \cdots) + \sum_{j \in I \backslash \{k, k_1+1\}} \lambda_j v_j$$

Це означає, що в правій частині цього рівняння коефіцієнт v_k дорівнює 1, а всі інші коефіцієнти $v_j, j \neq 6$ дорівнюють 0. Нижче наводиться множина відповідних коефіцієнтів $\{v_{k_1+1}, v_{k_1}, v_1, v_2\}$:

$$\{\lambda_2 + \lambda_{k_1+1} = 0, \lambda_1 + \lambda_{k_1+1} = 0, \lambda_1 + \lambda_{k_1+1} = 0, \lambda_2 = 0\}.$$

Звідси випливає, що $\lambda_2 = \lambda_1 = \lambda_k = \lambda_{k_1+1} = 0$. Отже, $\lambda_2 + \lambda_k = 0$, але це протиріччя, оскільки $\lambda_2 + \lambda_k$ є коефіцієнтом v_k і має дорівнювати 1.

Отже, для всіх $k < k_1$ з парними k є дійсним

$$C'' \cap \left(A_{1,1} + A_{k,k_1+1}\right) = \langle \{v_2\} \cup \left\{v_j | j \in (I \backslash I') \backslash \{k\}\right\} \rangle.$$

Нехай $I'' \coloneqq \{k \in I \mid k < k_1, k \text{ парне}\}$. З цього випливає:

$$D \coloneqq C'' \cap \left(\cap_{k \in I''} \left(A_{1,1} + A_{k,k_1+1}\right)\right) = \cap_{k \in I'} \left(C'' \cap \left(A_{1,1} + A_{k,k_1+1}\right)\right) =$$
$$= \cap_{k \in I'} \left(\langle v_j | j \in (I \backslash I') \backslash \{k\} \rangle\right) = \left(\langle v_j | j \in \left(I \backslash (I' \cup I'')\right) \rangle\right) = \langle v_j | j \in I, j - \text{непарне} \rangle$$

.

Крок 3: k непарне і $k < k_1$.

Нехай $I = I_o \cup I_e$, де I_o та I_e — підмножини непарних чисел відповідно парних в I. Доведення:

$$D \cap \left(A_{1,1} + A_{k,k_1+1}\right) = \langle \left\{v_j | j \in I_0 \backslash \{k\}\right\} \rangle.$$
$$A_{1,1} + A_{k,k_1+1} = A_{1,1} + \langle \left\{v_j | j \in I \backslash \{k, k_1 + 1\}\right\} \cup \{v_k, v_{k-1} + v_{k-3} +$$
$$+ \cdots, v_{k_1+1}, v_{k_1} + v_{k_1+2} + \cdots\} \rangle = \langle \left\{v_j | j \in I \backslash \{k, k_1 + 1\}\right\} \cup \{v_1 + v_3 + v_5 +$$
$$+ \cdots, v_2 + v_4 + v_6 + \cdots, v_k, v_{k-1} + v_{k-3} + \cdots, v_{k_1+1}, v_{k_1} + v_{k_1-2} + \cdots\} \rangle$$
$$\langle \left\{v_j | j \in I_0 \backslash \{k\}\right\} \rangle \subseteq D \cap \left(A_{1,1} + A_{k,k_1+1}\right).$$

Крім того, оскільки $\langle \left\{v_j | j \in I_0 \backslash \{k\}\right\} \rangle$ має корозмірність 1 у D, достатньо показати, що $v_k \notin A_{1,1} + A_{k,k_1+1}$. Можливо припустити, шляхом протиріччя, що $v_k \in A_{1,1} + A_{k_1+1}$. Тоді існують $\lambda_1, \lambda_2, \cdots \in \{0,1\}$ при

$$v_k = \lambda_1 (v_1 + v_3 + v_5 + \cdots) + \lambda_2 (v_2 + v_4 + v_6 + \cdots) + \lambda_k (v_k + v_{k-1} + v_{k-3} +$$
$$\cdots) + \lambda_{k_1+1} \left(v_{k_1+1} + v_{k_1} + v_{k_1-2} + \cdots\right) + \sum_{j \in I \backslash \{k, k_1+1\}} \lambda_j v_j$$

Це означає, що в правій частині цього рівняння коефіцієнт v_k дорівнює 1, а всі інші коефіцієнти $v_j, j \neq k$ дорівнюють 0. Нижче наводиться множина відповідних коефіцієнтів $\left\{v_{k_1+1}, v_{k_1}, v_1, v_2\right\}$:

$$\{\lambda_2 + \lambda_{k+1} = 0, \lambda_1 + \lambda_{k+1} = 0, \lambda_2 + \lambda_{k+1} = 0, \lambda_1 = 0\}.$$

Звідси випливає, що $\lambda_1 = \lambda_{k+1} = \lambda_{k2} = \lambda_k = 0$. Отже, $\lambda_1 + \lambda_k + \lambda_{k+1} = 0$, але це протиріччя через те, що $\lambda_1 + \lambda_k + \lambda_{k+1}$ є коефіцієнтом v_k і має дорівнювати 1. Отже, для всіх $k < k_1$ з непарними k є дійсним

$$D \cap \left(A_{1,1} + A_{k,k_1+1}\right) = \langle \left\{v_j | j \in I_0 \backslash \{k\}\right\} \rangle.$$

Нехай $J \coloneqq \{k \in I_o \mid k < k_1, k \text{ непарне}\}$. Через це є дійсним рівняння

$D' \coloneqq D \cap \left(\cap_{k\in I''} \left(A_{1,1} + A_{k,k_1+1}\right)\right) = \cap_{k\in I'} \left(D \cap \left(A_{1,1} + A_{k,k_1+1}\right)\right) =$
$\cap_{k\in I'} \left(\langle v_j | j \in I_o \backslash \{k\}\rangle\right) = \left(\langle v_j | j \in I_o \backslash J\rangle\right)$

Крок 4: k непарне і $k > k_1$. Розглядаючи подальші перетини D' з $A_{1,0} + +A_{k_1-1,k}$ для всіх непарних $k > k_1$, видно, що рівняння 2.2 виконується.

$$D' \cap \left(A_{1,0} + A_{k_1-1,k}\right) = \langle\{v_j | j \in I_0 \backslash (J \cup \{k\})\}\rangle.$$

$A_{1,0} + A_{k_1-1,k} = A_{1,0} + \langle\left\{v_j | j \in I \backslash \{k-1, k\}\right\} \cup \{v_{k-1}, v_{k-2} + v_{k-4} +$
$+ \cdots\}, \{v_k, v_{k-1} + v_{k-3} + \cdots\}\rangle = \langle\left\{v_j | j \in I \backslash \{k-1, k\}\right\} \cup \{v_1, v_2, v_{k-1} + v_{k-2} +$
$+ v_{k-4} + \cdots, v_k, v_{k-1} + v_{k-3} + \cdots\}\rangle$

Зрозуміло, що

$$\langle\{v_j | j \in I_0 \backslash (J \cup \{k\})\}\rangle \subseteq D' \cap \left(A_{1,0} + A_{k-1,k}\right).$$

Крім того, оскільки $\langle\{v_j | j \in I_0 \backslash (J \cup \{k\})\}\rangle$ має корозмірність 1 у D', достатньо показати, що $v_k \notin A_{1,0} + A_{k-1,k}$. Нехай, шляхом протиріччя, $v_k \in A_{1,0} + A_{k-1,k}$. Тоді існують $\lambda_1, \lambda_2, \cdots \in \{0,1\}$ при

$v_k = \lambda_1 v_1 + v_2 + \lambda_{k-1}(v_{k-1} + v_{k-2} + v_{k-4} + \cdots) + \lambda_k(v_k + v_{k-1} + v_{k-3} +$
$+ \cdots) + \sum_{j\in I\backslash\{k-1,k\}} \lambda_j v_j$

У правій частині цього рівняння коефіцієнт v_k дорівнює 1, а всі інші коефіцієнти $v_j, j \neq k$ дорівнюють 0. Тепер коефіцієнт v_{k-1} дорівнює $\lambda_{k-1} + \lambda_k == 0$. Примітно, що v_{k_1} з'являється один раз у доданку $v_{k-1} + v_{k-2} + v_{k-4} + \cdots$. Отже, коефіцієнт v_{k_1} дорівнює $\lambda_{k-1} = 0$. Це означає, що $\lambda_k = 0$, що суперечить тому, що $\lambda_k = 1$, оскільки коефіцієнт v_k дорівнює λ_k. Отже, для всіх $k > k_1$ з непарними k є дійсним

$$D \cap \left(A_{1,0} + A_{k-1,k}\right) = \langle\{v_j | j \in I_0 \backslash (J \cup \{k\})\}\rangle.$$

Нехай $J' \coloneqq \{k \in I_o \mid k > k_1, k \text{ непарне}\}$. Через це

$D' \coloneqq D' \cap \left(\cap_{k\in I''} \left(A_{1,0} + A_{k-1,k}\right)\right) = \cap_{k\in I'} \left(D' \cap \left(A_{1,0} + A_{k-1,k}\right)\right) =$
$= \cap_{k\in I'} \left(\langle v_j | j \in I_o \backslash (J \cup \{k\})\rangle\right) = \langle v_j | j \in I_o \backslash (J \cup J')\rangle = \{0\}$

На цьому лему доведено, тому буде розглянуто іншу.

Лема. Нехай $k_1 \equiv k_2 \equiv 0 \; mod \; 2$. Тоді рівняння 2.2 виконується.

Доведення леми подібне до доведення попередньої леми, а тому опущено. Наступна ж лема стосується останнього підвипадку.

Лема. Нехай $k_1 + k_2 \equiv 1 \; mod \; 2$. Тоді рівняння 2.2 виконується.

Доведення. Нехай $k_1 \equiv 1 \; mod \; 2$ і $k_2 \equiv 0 \; mod \; 2$. Далі буде короткий опис кроків, які необхідно виконати для доведення 2.2, не показуючи деталей.

Крок 1: доведення дійсності рівняння нижче.

$$C \coloneqq A_{1,0} + \sum_{i \in I} A_{i,0} = \langle \{ v_j | j \in I \} \rangle.$$

Крок 2: k непарне, $k < k_2$. Доведення:

$$C \cap (A_{1,1} + A_k) = \langle \{ v_j | j \in I \backslash \{k\} \} \rangle$$
$$v_k \notin (A_{1,1} + A_k)$$

Нехай $I'' \coloneqq \{k \in I \mid k < k_2, k \text{ непарне}\}$.

$$C' \coloneqq C \cap \left(\cap_{k \in I'} (A_{1,0} + A_k) \right) = \cap_{k \in I'} \left(C \cap (A_{1,0} + A_k) \right) = \cap_{k \in I'} \left(\langle \{ v_j | j \in I \backslash \{k\} \} \rangle \right) = \left(\langle \{ v_j | j \in I \backslash I' \} \rangle \right)$$

Крок 3: k непарне, $k > k_2$. Доведення:

$$C \cap (A_{1,0} + A_k) = \langle \{ v_j | j \in I \backslash \{k\} \} \rangle$$
$$v_k \notin (A_{1,0} + A_k)$$

Нехай $I'' \coloneqq \{k \in I \mid k > k_2, k \text{ непарне}\}$. Тоді

$$C'' \coloneqq C' \cap \left(\cap_{k \in I''} (A_{1,0} + A_k) \right) = \cap_{k \in I''} \left(C \cap (A_{1,0} + A_k) \right) = \cap_{k \in I'} \left(\langle \{ v_j | j \in I \backslash \{I' \cup k\} \} \rangle \right) = \left(\langle \{ v_j | j \in I \backslash I' \cup I''' \} \rangle \right) = \langle \{ v_j | j \in I_e \} \rangle$$

де I_e — підмножина всіх парних чисел у I.

Крок 4: k парне, $k < k_1$. Доведення:

$$C'' \cap (A_{1,1} + A_k) = \langle \{ v_j | j \in I_e \backslash \{k\} \} \rangle$$

$$v_k \notin (A_{1,1} + A_k)$$

Нехай $J := \{k \in I_e \mid k < k_1, k \text{ парне}\}$. Тоді

$$D := C'' \cap \left(\cap_{k \in I''} (A_{1,1} + A_k) \right) = \cap_{k \in I'} \left(C'' \cap (A_{1,1} + A_k) \right) = \cap_{k \in I'} (\langle v_j | j \in \in I_e \backslash \{k\} \rangle) = (\langle v_j | j \in (I \backslash J) \rangle)$$

Крок 5: k парне, $k > k_1$. Доведення:

$$D \cap (A_{1,0} + A_k) = \langle \{ v_j | j \in I_e \backslash (J \cup k) \} \rangle$$

$$v_k \notin (A_{1,0} + A_k)$$

Нехай $J' := \{k \in I_e \mid k > k_1, k \text{ парне}\}$. Тоді

$$D' := D \cap \left(\cap_{k \in J'} (A_{1,0} + A_{,k}) \right) = \cap_{k \in J'} \left(D \cap (A_{1,0} + A_k) \right) = \cap_{k \in J'} (\langle v_j | j \in \in I_e \backslash (J \cup k) \rangle) = \langle v_j | j \in I \backslash (J \cup J') = \{0\} \rangle$$

що доводить рівняння 2.2.

2.4 Висновки

Було розглянуто сутність аперіодичних логарифмічних підписів, метод їхнього побудування, а також деякі їхні різновиди. Логарифмічний підпис β, побудований за методом Баумейстера-де Вільєса, є ручним, якщо логарифмічні підписи $[A_{1,j_1}, \dots, A_{1,j_s}]$ θ відомі і ручні. Очевидно, якщо θ або/та $[A_{1,j_1}, \dots, A_{s,j_s}]$ не ручні, навіть якщо вони відомі, є невідомим ефективний метод щодо факторизації β. Варто знайти відповідь на наступне питання.

Нехай $[A_{1,j_1}, \dots, A_{1,j_s}]$, $1 \le j_i \le r_i$ і θ ручні, але вони невідомі. Також нехай β буде повністю аперіодичним. Чи можливо (ефективно) розкласти елементи G щодо β?

Результати криптоаналізу розширеної версії MST_3 [12] показали, що схема є безпечною при використанні об'єднаних трансверсальних

логарифмічних підписів. Точніше, об'єднані трансверсальні логарифмічні підписи витримують потужну атаку перестановкою матриць, тип обраної атаки простого тексту і, крім того, можливо визначити межу складності атаки для даного об'єднаного трансверсального логарифмічного підпису. Виявляється, що складність менше вхідної довжини схеми [12]. На основі методу побудови Баумейстера-де Вільєса можливо припустити, що складність атаки перестановкою матриць проти MST_3 залежить від розміру вхідної довжини, коли використовуються повністю аперіодичні логарифмічні підписи, побудовані в цій роботі.

Тому залишається актуальним складне і важливе питання визначення складності атаки перестановки матриць на розширену версію MST_3, коли використовуються повністю аперіодичні логарифмічні підписи, побудовані у поданій роботі.

Злиття блоків повністю аперіодичних логарифмічних підписів, побудованих в цій роботі, залишається логарифмічним підписом типу Баумейстера-де Вільєса. Крім того, логарифмічний підпис $\beta = [\beta_1, \dots, \beta_s]$ використовується в MST_3. Проблема складності атаки перестановки матриць вище передбачає розумний розмір блоку, наприклад $\beta_i \geq 2^6$ для $1 \leq i \leq s$. Отже, β стає результатом об’єднання блоків логарифмічного підпису.

Потрібно нагадати, що з’єднання блоків повністю аперіодичних логарифмічної підписів, побудованої в цій роботі, залишається логарифмічним підписом типу Баумейстера-де Вільєса. Крім того, логарифмічний підпис $\beta = [\beta_1, \dots, \beta_s]$ використовується в MST_3. Має бути розумний розмір блоку, $\beta_i \geq 2^6$ для $1 \leq i \leq s$. Отже, β виходить шляхом об’єднання блоків логарифмічного підпису, побудованого вище.

Таким чином, було додатково введено концепцію повністю аперіодичних логарифмічних підписів, які мають властивості, придатні для використання в криптосистемі MST_3. Розроблено алгебраїчний підхід на основі методу Баумейстера-де Вільєса, який дає можливість побудувати такі логарифмічні підписи для елементарних абелевих p-груп. Існування повністю аперіодичних логарифмічних підписів не тільки розширює простір приватних ключів MST_3, але й значно сприяє його безпеці. Тому варто дослідити подальший метод побудови повністю аперіодичних логарифмічних підписів для абелевих груп.

3 РЕАЛІЗАЦІЯ КРИПТОСИСТЕМИ MST3 З ВИКОРИСТАННЯМ ПОВНІСТЮ АПЕРІОДИЧНИХ ЛОГАРИФМІЧНИХ ПІДПИСІВ

Завдяки дослідженню інформації про криптографічну систему MST_3 та аперіодичні логарифмічні підписи стало можливим розробити прототип оновленої криптосистеми.

Нова версія:

1) Використовує наведений тип логарифмічних підписів;
2) Здійснює перестановки елементів не в межах певного блоку, а між декількома блоками одночасно. Повна перестановка виключає залежність від того чи іншого блоку, зменшуючи кількість потенційних атак на криптосистему;
3) Використовує мультиплікативну групу замість адитивної, що додатково підвищує складність проведення атаки на систему та підвищує її безпеку.

Для реалізації було застосовано мову програмування C++. Розглядалося використання зовнішньої бібліотеки для роботи з лінійною алгеброю Eigen, оскільки криптографічна система, окрім іншого, спирається на перемноження матриць. Але через використання поля Галуа GL(16, 2) її підключення було визнано зайвим – бітові операції у достатній мірі вирішують цю проблему у більш швидкий шлях. Втім, для більших полів її застосування вважається доцільним.

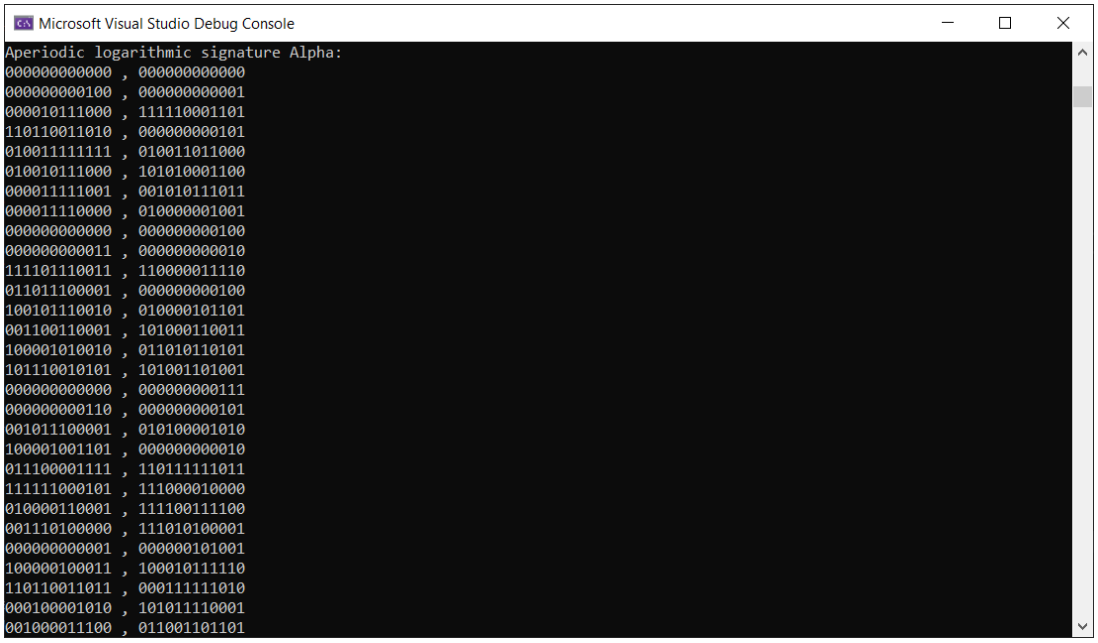

Рисунок 3.1 – Початок згенерованого аперіодичного логарифмічного підпису

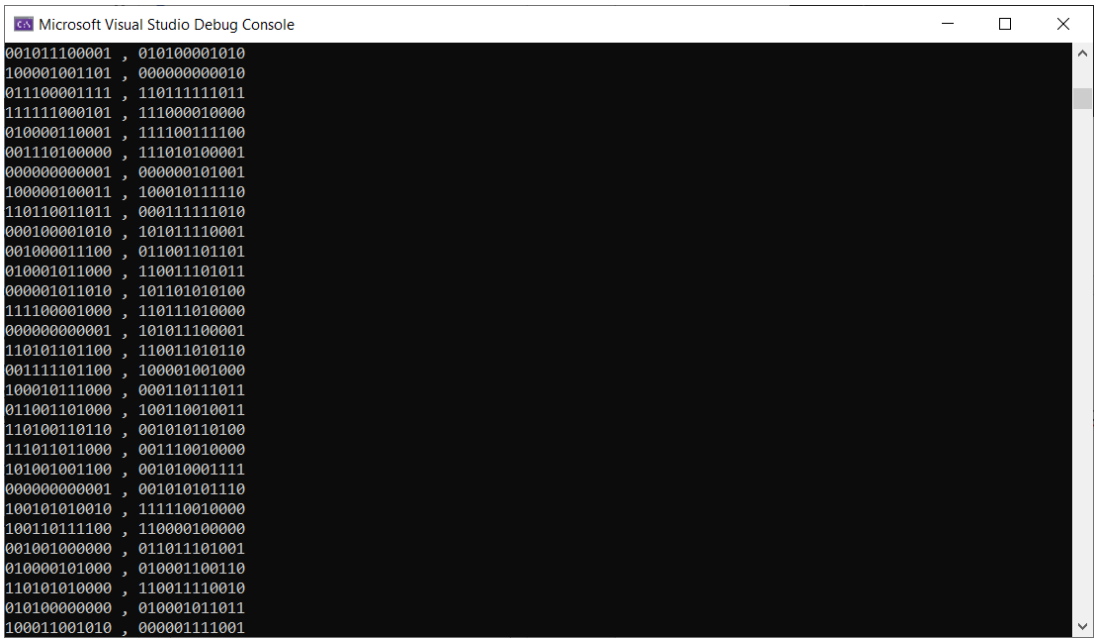

Рисунок 3.2 – Кінець згенерованого аперіодичного логарифмічного підпису

ВИСНОВКИ

У рамках поданої роботи було вивчено логарифмічні підписи та додаткові їхні різновиди, що мають здатність підвисити перспективність їхнього використання у криптосистемах з відкритим ключем на кшталт MST3 – аперіодичні логарифмічні підписи. Керуючись методом побудування, розробленим Баумейстером та де Вільєсом, для створення аперіодичних логарифмічних підписів для абелевих груп, зокрема, для абелевих 2-груп, які перешкоджають атаці Блекбьорна та інших, було виведено та проаналізовано додаткові типи. Варто зазначити, що трансверсальні або злиті трансверсальні логарифмічні підписи мають властивість бути періодичними. У поданій роботі було введено клас повністю аперіодичних логарифмічних підписів, а також представлено їхню побудову для абелевих p-груп на основі наведеного вище методу. Аперіодичні і повністю аперіодичні логарифмічні підписи забезпечують придатні до використання в MST3 класи логарифмічних підписів. Більше того, повністю аперіодичні логарифмічні підписи для абелевих груп самі по собі представляють теоретичний інтерес.

Було введено концепцію повністю аперіодичних логарифмічних підписів, які мають властивості, придатні для використання в криптосистемі MST_3. Було розроблено алгебраїчний підхід на основі методу Баумейстера-де Вільєса, який дає можливість побудувати такі логарифмічні підписи для елементарних абелевих p-груп. Існування повністю аперіодичних логарифмічних підписів не тільки розширює простір приватних ключів MST_3, але й значно сприяє його безпеці. Тому варто дослідити подальший метод побудови повністю аперіодичних логарифмічних підписів для абелевих груп.

Було представлено програмну реалізацію оновленої криптосистеми MST_3. Ця версія використовує вивчені аперіодичні логарифмічні підписи, застосовує мультиплікативну групу замість адитивної, а також здійснює перестановки не в межах одного блоку логарифмічного підпису, а між декількома блоками одразу – кожен з цих заходів зменшує ймовірність успішної атаки на криптографічну систему. Програмний код реалізації наведено у додатку А.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Баумейстер Б. Аперіодичні логарифмічні підписи / Б. Баумейстер, Д. Х. де Вільєс. // JMathCryptol. – 2012. – №6. – С. 21–37.
2. Блекберн С. Р. Криптоаналіз криптосистеми відкритого ключа MST3 / С. Р. Блекберн, К. Сід, К. Муллан // Журнал математики та криптології / С. Р. Блекберн, К. Сід, К. Муллан., 2009. - С. 321-338.
3. Х'юпперт Б. Кінцеві групи / Б. Х'юпперт, Н. Блекберн. - Нью-Йорк: Шпрингер-Ферлаг, 1982.
4. Сташевський Р. Повністю аперіодичні логарифмічні підписи / Р. Сташевський, Т. ван Трунг. – Ессен: Дуйсбург-Ессен, 2018. – 27 с.
5. Криптосистема відкритого ключа на основі неабелевих кінцевих груп / У. Лемпкен, С. С. Магліверас, Т. Ван Трунг, У. Уей // Журнал криптології / У. Лемпкен, С. С. Магліверас, Т. Ван Трунг, У. Уей., 2009. – С. 62–74.
6. Магліверас С. С. Новий генератор випадкових чисел на основі груп перестановок / С. С. Магліверас, Б. Е. Оберг, А. Д. Суркан // Фізико-математичний міланський симпозіум / С. С. Магліверас, Б. Е. Оберг, А. Д. Суркан. – Мілан, 1984. – С. 203–223.
7. Магліверас С. С. Алгебраїчні властивості криптосистеми PGM / С. С. Магліверас, Н. Д. Мемон // Журнал з криптології / С. С. Магліверас, Н. Д. Мемон., 1992. - С. 167-183.
8. Магліверас С. С. Нові підходи до проектування криптосистем відкритого ключа з використанням однобічних функцій та люків у кінцевих групах / С. С. Магліверас, Т. Ван Трунг, Д. Р. Стінсон // Журнал криптології / С. С. Магліверас, Т. Ван Трунг, Д. Р. Стінсон., 2002. – С. 285–297.
9. Про безпеку реалізації криптосистеми MST3 / С. С. Магліверас, П. Сваба, Т. Ван Трунг, П. Заяц // Математичні публікації Татра Маунтейнз / С. С. Магліверас, П. Сваба, Т. Ван Трунг, П. Заджак., 2008. – С. 1–13.
10. Марквард П. Генератори псевдовипадкових чисел на основі випадкових накрить для кінцевих груп [Електронний ресурс] / П. Марквард, П. Сваба, Т. Ван Трунг // Конструкції, коди та криптографія. – 2011. – Режим доступу до ресурсу: https://link.springer.com/article/10.1007/s10623-011-9485-1.
11. Сваба П. Про генерацію випадкових покрить для кінцевих груп / П. Сваба, Т. Ван Трунг // Математичні публікації Татра Маунтейнз / П. Сваба, Т. Ван Трунг., 2007. - С. 105-112.
12. Сваба П. Криптосистема відкритого ключа MST3: криптоаналіз та реалізація / П. Сваба, Т. Ван Трунг // Журнал математики та криптології / П. Сваба, Т. Ван Трунг., 2010. – С. 271–315.

13. Жабо С. Теми з факторизації абелевих груп / С. Жабо., 2004.
14. Шор П. В. Алгоритми поліноміального часу для розкладання на множники та дискретні логарифми на квантовому комп'ютері // Огляд SIAM. – 1999. – Т. 41. – №. 2. – С. 303-332.
15. Нгуєн П. Нові тенденцій у криптології // Резонанс. – 2001. – Т. 414. – С. 883-887.
16. Хігман Г. 2-групи Судзукі // Іллінойський математичний журнал. – 1963. – Т. 7. – №. 1. – С. 79-96.
17. Беркович Ю., Янко З. Групи первинного владного порядку, том 2. – де Грюйтер, 2008.