Math-Net.Ru

Общероссийский математический портал

А. С. Рыбкин, Исследование криптосистемы MST_3 на основе 2-группы Судзуки, *Дискрет. матем.*, 2014, том 26, выпуск 4, 66–90

DOI: <https://doi.org/10.4213/dm1306>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением <http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.237.206.68

26 апреля 2023 г., 13:23:30

Исследование криптосистемы MST_3 на основе 2-группы Судзуки

© 2014 г. А. С. Рыбкин*

Исследуется предложенная ранее атака на криптосистему с открытым ключом MST_3 на основе 2-группы Судзуки. Приводится теоретическое обоснование практических результатов, полученных авторами рассматриваемой атаки, показывается, что в общем случае данная атака может иметь довольно большую сложность. Кроме того, исследуется множество логарифмических сигнатур для центра 2-группы Судзуки и проводится оценка их количества.

Ключевые слова: MST_3 , 2-группа Судзуки, логарифмические сигнатуры.

1. Введение

В последние годы асимметричная криптография становится неотъемлемой частью многих информационных систем. Стойкость большинства существующих криптосистем с открытым ключом основывается на предположениях о вычислительной сложности математических задач, например, задачи факторизации целых чисел или задачи дискретного логарифмирования. Однако если применение квантового компьютера на практике станет реальностью, то ряд известных криптосистем с открытым ключом перестанет удовлетворять требованиям стойкости ввиду существования квантовых алгоритмов Шора для решения задачи факторизации целых чисел и задачи дискретного логарифмирования. В этой связи становится актуальным поиск новых трудноразрешимых математических задач.

Одним из таких направлений поиска являются исследования, инициированные Магливерасом, который рассмотрел задачу факторизации элементов в конечной группе по некоторым фиксированным последовательностям элементов этой группы [1]. На основе этой задачи Магливерас предложил симметричную криптосистему PGM, в которой впервые использовались такие структуры, как логарифмические сигнатуры для конечной группы. Дальнейшие исследования PGM выявили ряд алгебраических свойств данной криптосистемы, положительно отражающихся на ее стойкости.

Идеи, лежащие в основе PGM, впоследствии были использованы при создании двух криптосистем с открытым ключом на основе задачи факторизации элементов в конечной группе: MST_1 и MST_2 [2]. В процессе криптоанализа данных криптосистем были обнаружены разного рода уязвимости и недостатки, в частности, было показано, что для получения стойких реализаций MST_1 и MST_2 необходимо

*Место работы: МГУ имени М. В. Ломоносова, e-mail: randserg@mail.ru

использовать ключи с довольно большой длиной, что приводит к непрактичности этих криптосистем [3].

В [4] был предложен третий вариант криптосистемы с открытым ключом на основе задачи факторизации элементов в конечной группе. Данная криптосистема, получившая название MST_3 , вызвала как теоретический, так и практический интерес, что повлекло за собой появление ряда работ ([5], [6], [7] [8]), посвященных исследованию ее стойкости и рассмотрению основных аспектов ее реализации. Первоначальные комментарии относительно стойкости MST_3 и простейшая атака на нее были представлены самими авторами криптосистемы в [5]. Более перспективная атака на MST_3 была предложена в [6]. Для демонстрации и проверки работоспособности данной атаки на практике авторы описали в [6] три вида экспериментов с различными реализациями MST_3 .

В первой части работы приводится основная идея представленной в [6] атаки на криптосистему MST_3 , отдельно исследуется каждый из трех экспериментов, осуществленных авторами атаки, приводятся теоретические оценки, связанные с результатами данных экспериментов, а также демонстрируется, что в общем случае рассматриваемая атака может иметь довольно большую сложность. Вторая часть работы посвящена исследованию множества секретных ключей криптосистемы MST_3 .

2. Основные понятия

2.1. Логарифмические сигнатуры и покрытия конечных групп. В этом разделе рассматриваются основные обозначения, определения и отображения, связанные с логарифмическими сигнатурами и покрытиями конечных групп, используемые в работах [4], [5], [8].

Пусть G — некоторая конечная группа. Обозначим через $G^{[\mathbb{Z}]}$ множество всех конечных последовательностей, состоящих из элементов группы G , при этом каждую такую последовательность будем записывать в виде строки.

Рассмотрим произвольную последовательность $X = [x_1, \dots, x_m] \in G^{[\mathbb{Z}]}$. Обозначим число элементов в последовательности X через $|X| = m$. Пусть $\mathbb{Z}[G]$ — групповое кольцо, построенное по группе G . Рассматривая элементы последовательности X как элементы группового кольца $\mathbb{Z}[G]$, обозначим их сумму, принадлежащую $\mathbb{Z}[G]$, через $\bar{X} = \sum_{i=1}^m x_i$.

Определение 1. Пусть G — некоторая конечная группа, J — некоторое подмножество элементов этой группы, а $\mathbb{Z}[G]$ — групповое кольцо, построенное по группе G . Рассмотрим такой набор $\alpha = [A_1, A_2, \dots, A_s]$, состоящий из последовательностей $A_i \in G^{[\mathbb{Z}]}$, $i = 1, 2, \dots, s$, что величина $\sum_{i=1}^s |A_i|$ ограничена сверху полиномом от $\log |G|$. Тогда для некоторого набора коэффициентов $a_g \in \mathbb{Z}$, $g \in G$, справедливо равенство

$$\bar{A}_1 \cdot \bar{A}_2 \cdot \dots \cdot \bar{A}_s = \sum_{g \in G} a_g g \in \mathbb{Z}[G].$$

Будем говорить, что α является:

- *покрытием* группы G (или множества J), если $a_g > 0$ для всех $g \in G$ ($g \in J$);
- *логарифмической сигнатурой* для группы G (или множества J), если $a_g = 1$ для всех $g \in G$ ($g \in J$).

Заметим, что если α — покрытие конечной группы G , то любой элемент $g \in G$ может быть представлен хотя бы одним способом в виде

$$g = g_1 \cdot g_2 \cdot \dots \cdot g_s, \text{ где } g_i \in A_i, i = 1, \dots, s. \quad (1)$$

Если α является логарифмической сигнатурой для G , то для всех элементов $g \in G$ разложение (1) существует и является единственным. Таким образом, множество всех логарифмических сигнатур представляет собой некоторое подмножество множества всех покрытий. В связи с этим при описании основных понятий и преобразований, связанных с покрытиями и логарифмическими сигнатурами, будем ограничиваться рассмотрением покрытий, подразумевая существование соответствующих аналогов и для логарифмических сигнатур.

Пусть $\alpha = [A_1, A_2, \dots, A_s]$ — некоторое покрытие конечной группы G . Последовательности $A_i \in G^{[\mathbb{Z}]}$, $i = 1, \dots, s$, называются *блоками* покрытия α , а вектор $r = (r_1, \dots, r_s)$, где $r_i = |A_i|$, $i = 1, \dots, s$, — *типом* α . В дальнейшем будем рассматривать только такие покрытия и логарифмические сигнатуры α , для типа $r = (r_1, \dots, r_s)$ которых выполняются условия $s \geq 2$ и $r_i \geq 2$, $i = 1, \dots, s$.

Перейдем к рассмотрению основных отображений, связанных с покрытиями и логарифмическими сигнатурами. Пусть $\alpha = [A_1, \dots, A_s]$ — покрытие конечной группы G , имеющее тип $r = (r_1, \dots, r_s)$. Пусть также каждый блок покрытия α имеет вид $A_i = [a_{i1}, \dots, a_{ir_i}]$, $i = 1, \dots, s$. В дальнейшем для сокращения описания такой структуры блоков покрытия будем использовать обозначение $\alpha = (a_{ij})$. Положим

$$m_1 = 1, \quad m_i = \prod_{j=1}^{i-1} r_j, \quad i = 2, \dots, s, \quad m = \prod_{i=1}^s r_i.$$

Рассмотрим два отображения:

$$\lambda_\alpha : \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \times \dots \times \mathbb{Z}_{r_s} \rightarrow \mathbb{Z}_m,$$

$$\lambda_\alpha(j_1, j_2, \dots, j_s) = \sum_{i=1}^s j_i m_i;$$

$$\theta_\alpha : \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \times \dots \times \mathbb{Z}_{r_s} \rightarrow G,$$

$$\theta_\alpha(j_1, j_2, \dots, j_s) = a_{1(j_1+1)} \cdot a_{2(j_2+1)} \cdot \dots \cdot a_{s(j_s+1)}.$$

С их помощью можно определить еще одно отображение:

$$\begin{aligned} \check{\alpha} : \mathbb{Z}_m &\rightarrow G, \\ \check{\alpha}(j) &= \theta_\alpha(\lambda_\alpha^{-1}(j)). \end{aligned} \quad (2)$$

Отображение (2) позволяет для каждой конечной группы разбить все ее покрытия на классы эквивалентности.

Определение 2. Два покрытия α и β конечной группы G называются *эквивалентными*, если отображения $\check{\alpha}$ и $\check{\beta}$ имеют одинаковую область определения и

$$\check{\alpha} \equiv \check{\beta}.$$

Введение таких структур, как покрытия и логарифмические сигнатуры, позволяет сформулировать задачу факторизации в конечной группе G . Задача факторизации заключается в нахождении элементов $g_i \in A_i$, $i = 1, \dots, s$, соответствующих разложению (1), по известному элементу $g \in G$ и фиксированному покрытию

$\alpha = [A_1, A_2, \dots, A_s]$ группы G . Сложность решения этой задачи зависит от выбранного покрытия. Если разложение (1) любого из элементов группы G может быть получено за полиномиальное от $\log |G|$ время, соответствующее покрытие α называется *простым*. В ином случае покрытие α называется *сложным*.

Возвращаясь к рассмотренным выше отображениям, заметим, что отображение $\check{\alpha}$ эффективно (то есть за полиномиальное от $\log |G|$ время) вычислимо для любого значения из области определения и любого покрытия α . В то же время обратное отображение $\check{\alpha}^{-1}$ требует нахождения разложения (1), поэтому эффективность его вычисления зависит от того, простое покрытие при этом используется или сложное.

Следует отметить, что решение задачи факторизации в конечной группе в общем случае подразумевает и решение задачи дискретного логарифмирования в мультипликативной циклической группе. Для этого достаточно сформировать из элементов мультипликативной циклической группы покрытие определенной структуры, позволяющее по известному разложению элемента легко находить его дискретный логарифм. Существует предположение, что в общем случае проблема нахождения разложения (1) для произвольного элемента $g \in G$ и случайно выбранного покрытия α группы G является вычислительно сложной задачей.

2.2. Криптосистема MST_3 . Криптосистема MST_3 , предложенная в [4], является криптосистемой с открытым ключом, основанной на логарифмических сигнатурах и покрытиях конечных групп. Ниже приводится описание основных этапов работы криптосистемы MST_3 .

Подготовительные процедуры. Выбирается некоторая конечная неабелева группа G с достаточно большим нетривиальным центром $Z = Z(G)$. При этом группа G не должна раскладываться в прямое произведение $G = Z \times H$, где H — некоторая подгруппа группы G .

Генерация ключей. Для осуществления генерации секретного и открытого ключей необходимо:

- сгенерировать некоторую простую логарифмическую сигнатуру $\beta = (b_{ij})$ для центра группы — Z , имеющую тип $(r_1, \dots, r_s)$;
- сгенерировать случайное покрытие $\alpha = (a_{ij})$ некоторого заранее не известного подмножества J группы G , имеющее такой же тип, что и β , и удовлетворяющее условию: $a_{ij} \in G \setminus Z$, $j = 1, \dots, r_i$, $i = 1, \dots, s$;
- выбрать элементы $t_0, t_1, \dots, t_s \in G \setminus Z$;
- поэлементно вычислить новое покрытие $\tilde{\alpha} = (\tilde{a}_{ij})$ некоторого подмножества группы G , полученное из α при помощи элементов $t_0, t_1, \dots, t_s$ следующим образом:

$$\tilde{a}_{ij} = t_{i-1}^{-1} a_{ij} t_i, \quad j = 1, \dots, r_i, \quad i = 1, \dots, s; \quad (3)$$

- поэлементно вычислить новое покрытие $\gamma = (h_{ij})$ некоторого подмножества группы G , полученное из β и $\tilde{\alpha}$ следующим образом:

$$h_{ij} = b_{ij} \tilde{a}_{ij}, \quad j = 1, \dots, r_i, \quad i = 1, \dots, s; \quad (4)$$

- выбрать в качестве открытого ключа пару (α, γ) , а в качестве секретного ключа — набор $(\beta, (t_0, t_1, \dots, t_s))$.

Процедура зашифрования. Для зашифрования сообщения $x \in \mathbb{Z}_{|Z|}$ необходимо вычислить два элемента: $y_1 = \check{\alpha}(x) \in G$ и $y_2 = \check{\gamma}(x) \in G$, и назвать шифртекстом пару $y = (y_1, y_2)$.

Процедура расшифрования. Для расшифрования шифртекста $y = (y_1, y_2)$, $y_1, y_2 \in G$, необходимо воспользоваться тем, что для любого $x \in \mathbb{Z}_{|Z|}$ справедлива цепочка равенств

$$\begin{aligned}\check{\gamma}(x) &= b_{1j_1} \tilde{a}_{1j_1} b_{2j_2} \tilde{a}_{2j_2} \dots b_{sj_s} \tilde{a}_{sj_s} = b_{1j_1} b_{2j_2} \dots b_{sj_s} \tilde{a}_{1j_1} \tilde{a}_{2j_2} \dots \tilde{a}_{sj_s} = \\ &= b_{1j_1} b_{2j_2} \dots b_{sj_s} t_0^{-1} a_{1j_1} t_1 t_1^{-1} a_{2j_2} t_2 \dots t_{s-1}^{-1} a_{sj_s} t_s = \\ &= b_{1j_1} b_{2j_2} \dots b_{sj_s} t_0^{-1} a_{1j_1} a_{2j_2} \dots a_{sj_s} t_s = \check{\beta}(x) t_0^{-1} \check{\alpha}(x) t_s,\end{aligned}$$

то есть $\check{\beta}(x) = \check{\gamma}(x) t_s^{-1} (\check{\alpha}(x))^{-1} t_0 = y_2 t_s^{-1} y_1^{-1} t_0$, что следует из соотношений (3) и (4). Так как логарифмическая сигнатура β является простой, то знание значения $\check{\beta}(x)$ позволяет за приемлемое время вычислить исходное сообщение x . Таким образом, окончательно получаем

$$x = \check{\beta}^{-1}(y_2 t_s^{-1} y_1^{-1} t_0).$$

Вариативность криптосистемы MST_3 заключается в возможности выбора неабелевой конечной группы G и способа генерации простой логарифмической сигнатуры β , составляющей основную часть секретного ключа. Авторы криптосистемы MST_3 предложили использовать в качестве конечной группы 2-группу Судзуки. Данный выбор был мотивирован простотой практической реализации и возможностью тщательного анализа стойкости полученной криптосистемы. Это привело к тому, что рассмотрение 2-группы Судзуки зачастую стало практиковаться и в последующих работах, посвященных изучению криптографических свойств MST_3 .

2.3. 2-группа Судзуки.

Определение 3. 2-группа Судзуки — это неабелева 2-группа с более чем одной инволюцией (элементом второго порядка), имеющая циклическую группу автоморфизмов, которая транзитивно переставляет эти инволюции.

Подробное исследование и классификация 2-групп Судзуки были проведены в [9]. В частности, в [9] было показано, что для любой 2-группы Судзуки G выполнено соотношение

$$Z(G) = \Omega_1(G), \quad (5)$$

где

$$\begin{aligned}Z(G) &= \{z \in G \mid zg = gz, \forall g \in G\} \text{ — центр группы,} \\ \Omega_1(G) &= \{g \in G \mid g^2 = 1\} \text{ — множество элементов второго порядка.}\end{aligned}$$

Кроме того, было установлено, что если G — 2-группа Судзуки, то $|Z(G)| = q = 2^m$, $m > 1$, а $|G| = q^2$ или $|G| = q^3$.

Авторы криптосистемы MST_3 предлагают использовать в качестве конечной группы 2-группу Судзуки порядка q^2 . В [9] показано, что если $q = 2^m$, $3 \leq m \in \mathbb{N}$, и при этом поле $\mathbb{F}_q$ имеет нетривиальный автоморфизм θ нечетного порядка, то 2-группа Судзуки порядка q^2 , обозначаемая как $A(m, \theta)$, существует. Кроме того, группа $A(m, \theta)$ является изоморфной группе матриц $G = \{S(a, b) \mid a, b \in \mathbb{F}_q\}$ вида

$$S(a, b) = \begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & a^\theta & 1 \end{pmatrix}, \text{ где } a, b \in \mathbb{F}_q.$$

Непосредственным вычислением легко проверить, что групповая операция в G определяется следующим образом:

$$S(a_1, b_1)S(a_2, b_2) = S(a_1 + a_2, b_1 + b_2 + a_1^\theta a_2). \quad (6)$$

Отсюда следует способ вычисления обратного элемента:

$$S(a, b)^{-1} = S(a, b + aa^\theta). \quad (7)$$

Так как группа матриц G изоморфна 2-группе Судзуки порядка q^2 , то для нее также справедливо равенство (5), поэтому из соотношения (7) следует, что ее центр имеет вид

$$Z(G) = \{S(0, b) \mid b \in \mathbb{F}_q\}. \quad (8)$$

Тогда из соотношений (6) и (8), получаем, что для двух произвольных элементов центра $S(0, b_1)$ и $S(0, b_2)$, где $b_1, b_2 \in \mathbb{F}_q$, выполняется равенство

$$S(0, b_1)S(0, b_2) = S(0, b_1 + b_2). \quad (9)$$

Равенство (9) в совокупности с тем, что $|Z(G)| = q = 2^m$, позволяет рассматривать центр группы матриц G , а следовательно, и центр 2-группы Судзуки $A(m, \theta)$, как аддитивную группу элементов поля $\mathbb{F}_q$, то есть как векторное пространство размерности m над полем $\mathbb{F}_2$ с операцией сложения векторов.

Таким образом, упрощение структуры 2-группы Судзуки порядка q^2 достигается за счет перехода к изоморфной группе матриц G и возможности рассмотрения ее центра как аддитивной группы элементов поля $\mathbb{F}_q$. Совокупность данных упрощений позволяет облегчить исследование криптосистемы MST_3 и ее реализацию, что, возможно, и послужило основанием для авторов MST_3 рекомендовать 2-группу Судзуки в качестве основы этой криптосистемы.

2.4. Основные методы генерации простых логарифмических сигнатур.

В описании криптосистемы MST_3 не фиксируется метод генерации простой логарифмической сигнатуры β , являющейся основной частью секретного ключа. Это послужило причиной появления различных подходов к реализации MST_3 , отличающихся друг от друга алгоритмами генерации простых логарифмических сигнатур. Ниже приводится описание нескольких таких алгоритмов.

Определение 4. Пусть V — векторное пространство размерности m над полем $\mathbb{F}_2$. Рассмотрим произвольное разбиение множества $\{1, \dots, m\}$:

$$\{1, \dots, m\} = K_1 \cup \dots \cup K_v, \quad K_i \cap K_j = \emptyset \text{ при } i, j \in \{1, \dots, v\}, \quad i \neq j.$$

Пусть $|K_i| = k_i$, $i = 1, \dots, v$, $\sum_{i=1}^v k_i = m$. Тогда набор последовательностей $\delta = [D_1, \dots, D_v]$, где D_i содержит все различные 2^{k_i} векторов с нулевыми значениями координат на позициях, соответствующих подмножеству $\{1, \dots, m\} \setminus K_i$, $i = 1, \dots, v$, называется *канонической логарифмической сигнатурой* для аддитивной группы V .

Несложно видеть, что полученный набор последовательностей является простой логарифмической сигнатурой для V .

Определение 5. Пусть G — конечная группа, в которой существует цепочка подгрупп:

$$\langle e \rangle = G_0 < G_1 < \dots < G_v = G.$$

Тогда набор последовательностей $\delta = [D_1, \dots, D_v]$, где $D_i \in G^{[\mathbb{Z}]}$ содержит по одному представителю из каждого смежного класса подгруппы G_i по подгруппе G_{i-1} , $i = 1, \dots, v$, называется *трансверсальной логарифмической сигнатурой* для группы G .

В [10] было показано, что любая трансверсальная логарифмическая сигнатура для конечной абелевой группы является простой.

Рассмотрим следующие преобразования логарифмической сигнатуры $\delta = [D_1, \dots, D_s]$ для конечной абелевой группы G :

- перестановка элементов в блоке D_i ;
- перестановка блоков логарифмической сигнатуры δ ;
- замена блока D_i на блок $D_i \cdot g = \{ag \mid a \in D_i\}$ для некоторого $g \in G$;
- замена двух блоков D_i и D_j на один блок $D_i \cdot D_j = \{ab \mid a \in D_i, b \in D_j\}$.

Определение 6. Пусть G — конечная абелева группа. Набор последовательностей $\delta = [D_1, \dots, D_v]$, где $D_i \in G^{[\mathbb{Z}]}$, $i = 1, \dots, v$, полученный из трансверсальной логарифмической сигнатуры для G с помощью конечного числа введенных выше преобразований, называется *объединенной трансверсальной логарифмической сигнатурой* для группы G .

В [10] было показано, что любая объединенная трансверсальная логарифмическая сигнатура для конечной абелевой группы является простой, если все применяющиеся при ее получении из трансверсальной логарифмической сигнатуры преобразования известны.

3. Исследование атаки на криптосистему MST_3

3.1. Описание атаки. Перейдем к рассмотрению предложенной в [6] атаки на криптосистему MST_3 . Атака применяется в случае использования 2-группы Судзуки в качестве конечной группы и объединенной трансверсальной логарифмической сигнатуры в качестве простой логарифмической сигнатуры β , являющейся основной частью секретного ключа для MST_3 .

В первую очередь, в [6] отмечается возможность упрощения анализа криптосистемы MST_3 на основе 2-группы Судзуки. Авторы атаки предлагают рассматривать для анализа только криптосистему MST_3 , у которых:

- открытый ключ представляет собой два покрытия α и γ , каждый блок которых содержит единичный элемент группы, стоящий на первом месте в блоке;
- секретный ключ представляет собой логарифмическую сигнатуру β , каждый блок которой содержит единичный элемент группы, стоящий на первом месте в блоке, и набор элементов $t_0, \dots, t_s$, для которых выполняется соотношение $t_0 = \dots = t_s = t$.

Демонстрируется, что задача нахождения открытого текста по шифртексту и открытому ключу для произвольной криптосистемы MST_3 может быть сведена к аналогичной задаче для криптосистемы MST_3 с рассмотренными выше ограничениями на открытый и секретный ключи. Таким образом, для решения указанной задачи

в общем случае достаточно научиться решать ее для криптосистем с ограничением на ключи.

Предложенная в [6] атака направлена на нахождение секретного ключа по открытому ключу в случае использования криптосистемы MST_3 с ограничениями на ключи. При этом найденным в результате атаки секретным ключом может являться не исходный секретный ключ, а эквивалентный ему, то есть ключ, позволяющий эффективно и корректно расшифровывать любой шифртекст, полученный на открытом ключе.

Для задания атакуемой криптосистемы MST_3 с ограничением на ключи выбираются конечная группа G с центром Z , секретный ключ $(\beta = (b_{ij}), (t, \dots, t))$ и открытый ключ $(\alpha = (a_{ij}), \gamma = (h_{ij}))$. Для осуществления атаки авторы выбирают некоторый элемент $t' \in G \setminus Z$, отмечая, что значение при этом имеет только смежный класс $t'Z$, и поэлементно вычисляют $\beta' = (b'_{ij})$ из α , γ и t' по следующей формуле:

$$b'_{ij} = h_{ij}(t')^{-1}a_{ij}^{-1}t'. \quad (10)$$

Итоговая теорема в [6] утверждает, что если G/Z — абелева группа, то полученный в процессе атаки набор $(\beta', (t', \dots, t'))$ является ключом, эквивалентным секретному ключу $(\beta = (b_{ij}), (t, \dots, t))$, тогда и только тогда, когда β' является биекцией, обратимой за эффективное время.

Таким образом, рассматриваемая атака сводится к выбору подходящего значения элемента t' либо путем его быстрого угадывания, либо путем ограничения множества возможных значений t' из условия, что получаемый в результате набор последовательностей β' должен являться биекцией, обратимой за эффективное время.

Для демонстрации возможности применения своей атаки на практике авторы рассматривают реализацию криптосистемы MST_3 с ограничениями на ключи, основанную на 2-группе Судзуки порядка $q^2 = (2^m)^2 = (2^{81})^2$, и приводят три варианта этой криптосистемы, отличающиеся друг от друга типом использующихся логарифмических сигнатур и покрытий:

- α , β и γ имеют тип $(2, 2, \dots, 2)$;
- α , β и γ имеют тип $(8, 64, 64, \dots, 64)$;
- α , β и γ имеют тип $(2, 2, \dots, 2, 16, 16, \dots, 16)$.

Разберем более подробно каждый из приведенных вариантов.

3.2. α , β и γ имеют тип $(2, 2, \dots, 2)$. Атакуемая криптосистема MST_3 с ограничениями на ключи, основанная на 2-группе Судзуки порядка $(2^{81})^2$, задается логарифмической сигнатурой $\beta = (b_{ij})$, покрытиями $\alpha = (a_{ij})$, $\gamma = (h_{ij})$, где $j = 1, 2$, $i = 1, \dots, 81$, и параметром t , для которых вводятся следующие обозначения:

$$b_{i2} = S(0, d_{i2}), \quad a_{i2} = S(e_{i2}, f_{i2}), \quad d_{i2}, e_{i2}, f_{i2} \in \mathbb{F}_{2^{81}}, \quad i = 1, \dots, 81, \\ t = t_0 = \dots = t_s = S(x, 0), \quad x \in \mathbb{F}_{2^{81}}.$$

Тогда из соотношений (3) и (4) следует, что

$$h_{i2} = S(e_{i2}, d_{i2} + f_{i2} + e_{i2}x^\theta + e_{i2}^\theta x) = S(e_{i2}, g_{i2}), \quad g_{i2} \in \mathbb{F}_{2^{81}}, \quad i = 1, \dots, 81. \quad (11)$$

Авторы атаки случайным образом выбирают элемент $t' = S(y, 0)$ и порождают с его помощью набор $\beta' = (b'_{ij})$ согласно соотношению (10):

$$b'_{i2} = h_{i2}(t')^{-1}a_{i2}^{-1}t' = S(0, g_{i2} + f_{i2} + e_{i2}y^\theta + e_{i2}^\theta y) = S(0, d'_{i2}). \quad (12)$$

Если элементы набора $\{d'_{i2}, i = 1, \dots, 81\}$ являются линейно независимыми, то β' является эффективно обратимой биекцией и, следовательно, согласно теореме в [6], набор $(\beta', (t', \dots, t'))$ представляет собой ключ, эквивалентный секретному ключу $(\beta, (t, \dots, t))$ для рассматриваемой реализации криптосистемы MST_3 .

На основе этого наблюдения авторами атаки был проведен ряд экспериментов с произвольно генерируемыми значениями логарифмической сигнатуры β типа $(2, 2, \dots, 2)$, покрытия α типа $(2, 2, \dots, 2)$ и параметра t . Эти эксперименты показали, что ключ, эквивалентный секретному, получается в среднем приблизительно за 3.47 «угадываний» значения параметра t' и вычислений соответствующего ему набора множеств β' .

Перейдем к теоретическому обоснованию полученной в [6] эмпирической оценки среднего количества «угадываний». Из соотношений (11) и (12) следует, что

$$d'_{i2} = g_{i2} + f_{i2} + e_{i2}y^\theta + e_{i2}^\theta y = d_{i2} + e_{i2}(x + y)^\theta + e_{i2}^\theta(x + y).$$

Предположим, что элементы набора $\{d'_{i2}, i = 1, \dots, 81\}$ независимы и приблизительно равномерно распределены на $\mathbb{F}_{2^{81}}$. Тогда для получения приближительной оценки среднего количества «угадываний» достаточно оценить вероятность p того, что случайный набор из произвольных элементов поля $\mathbb{F}_{2^{81}}$ будет являться набором из линейно независимых элементов поля $\mathbb{F}_{2^{81}}$.

Пусть m — некоторое натуральное число. Количество различных наборов из m линейно независимых элементов поля $\mathbb{F}_{2^m}$ равно

$$\prod_{i=0}^{m-1} (2^m - 2^i).$$

Поэтому отношение числа различных наборов, состоящих из m линейно независимых элементов поля $\mathbb{F}_{2^m}$, к числу различных наборов, состоящих из m произвольных элементов поля $\mathbb{F}_{2^m}$, равно

$$\frac{\prod_{i=0}^{m-1} (2^m - 2^i)}{(2^m)^m} = \prod_{i=0}^{m-1} \frac{2^m - 2^i}{2^m}.$$

Рассмотрим предел данного выражения при m , стремящемся к бесконечности:

$$\begin{aligned} \lim_{m \rightarrow \infty} \prod_{i=0}^{m-1} \frac{2^m - 2^i}{2^m} &= \lim_{m \rightarrow \infty} \prod_{i=0}^{m-1} (1 - 2^{i-m}) = \\ &= \lim_{m \rightarrow \infty} \prod_{n=1}^m \left(1 - \left(\frac{1}{2}\right)^n\right) = \prod_{n=1}^{\infty} \left(1 - \left(\frac{1}{2}\right)^n\right). \end{aligned}$$

Выражение

$$\prod_{n=1}^{\infty} \left(1 - \left(\frac{1}{2}\right)^n\right)$$

является значением функции Эйлера

$$\varphi(q) = \prod_{n=1}^{\infty} (1 - q^n)$$

при $q = \frac{1}{2}$. Для функции Эйлера в [11] предложена оценка вида

$$\varphi(q) = \sqrt{\frac{2\pi}{t}} \exp\left(-\frac{\pi^2}{6t} + \frac{t}{24}\right) + o(1), \quad (13)$$

где $q = e^{-t}$. Подставляя в формулу (13) значение $t = -\log\left(\frac{1}{2}\right)$, получаем

$$\varphi\left(\frac{1}{2}\right) \approx 0.288788.$$

Тогда искомая вероятность p при $m = 81$ может быть оценена так:

$$p \approx 0.288788.$$

Приведенные соотношения позволяют утверждать, что в среднем приблизительно через $\frac{1}{p} \approx 3.462748$ «угадываний» значения элемента t' и вычислений соответствующей последовательности множеств β' будет найден набор $\{d'_{i2}, i = 1, \dots, 81\}$ с линейно независимыми элементами, что, в свою очередь, будет означать получение эквивалентного секретного ключа.

3.3. α , β и γ имеют тип $(8, 64, 64, \dots, 64)$. Атакуемая криптосистема MST_3 с ограничениями на ключи, основанная на 2-группе Судзуки порядка $(2^{81})^2$, задается логарифмической сигнатурой $\beta = (b_{ij})$, покрытиями $\alpha = (a_{ij})$, $\gamma = (h_{ij})$ типа $(8, 64, 64, \dots, 64)$ и параметром t , для которых вводятся следующие обозначения:

$$b_{ij} = S(0, d_{ij}), \quad a_{ij} = S(e_{ij}, f_{ij}), \quad h_{ij} = S(e_{ij}, g_{ij}), \quad d_{ij}, e_{ij}, f_{ij}, g_{ij} \in \mathbb{F}_{2^{81}}, \\ t = t_0 = \dots = t_s = S(x, 0), \quad x \in \mathbb{F}_{2^{81}}.$$

Используя соотношения (3) и (4), авторы атаки получают, что

$$g_{ij} = d_{ij} + f_{ij} + e_{ij}^\theta x + e_{ij} x^\theta$$

и, следовательно,

$$d_{ij} = g_{ij} + f_{ij} + e_{ij}^\theta x + e_{ij} x^\theta. \quad (14)$$

В рассматриваемом случае атака направлена на ограничение количества возможных значений, которые может принимать элемент $t' = S(y, 0)$, $y \in \mathbb{F}_{2^{81}}$, с целью дальнейшего осуществления полного перебора этих значений. Для каждого допустимого значения t' при этом будет необходимо проводить построение оставшейся части секретного ключа — логарифмической сигнатуры β' согласно соотношению (10).

Для возможности проведения ограничений такого рода в [6] устанавливается, что для любой объединенной трансверсальной логарифмической сигнатуры $\beta = [B_1, \dots, B_s] = (b_{ij})$ типа $(r_1, \dots, r_s)$ с единичным элементом в каждом из блоков существуют такой блок B_i и такой нетривиальный элемент этого блока b_{ij} , что

$$B_i \cdot b_{ij} = B_i.$$

Так как в рассматриваемой объединенной трансверсальной логарифмической сигнатуре $\beta = (b_{ij})$ типа $(8, 64, 64, \dots, 64)$ первый элемент каждого блока является единичным, то найдутся такие индексы i и j , что равенство

$$d_{ij} + d_{ik} = d_{il}$$

будет справедливо по крайней мере для $r_i - 2$ пар различных индексов k, l , где $2 \leq k, l \leq r_i$ и r_i — количество элементов в i -м блоке логарифмической сигнатуры β .

Выписывая три соотношения вида (14) для d_{ij} , d_{ik} , d_{il} , складывая их и вводя обозначение $u_{ijkl} = u_{ij} + u_{ik} + u_{il}$, где $u \in \{e, f, g\}$, авторы атаки получают уравнение вида

$$e_{ijkl}^\theta x + e_{ijkl} x^\theta = f_{ijkl} + g_{ijkl} \quad (15)$$

относительно неизвестного элемента $x \in \mathbb{F}_{2^{s_1}}$.

Далее, в [6] утверждается, что если $e_{ijkl} \neq 0$, то при фиксированном автоморфизме $\theta : x \rightarrow x^2$ каждое уравнение вида (15) либо не имеет решений, либо имеет 2 решения, так как отображение

$$\psi_e : \mathbb{F}_q \rightarrow \mathbb{F}_q, \quad \psi_e(x) = e^\theta x + ex^\theta, \quad (16)$$

при $e \in \mathbb{F}_q$, $e \neq 0$ и $q = 2^{s_1}$ имеет ядро мощности 2.

Таким образом, перебор всех значений индексов i, j, k, l , построение соответствующих уравнений вида (15) и нахождение всех их решений (при $\theta : x \rightarrow x^2$ не более двух решений на уравнение) позволяют ограничить множество возможных значений $y \in \mathbb{F}_{2^{s_1}}$ для $t' = S(y, 0)$ множеством данных решений. Помимо этого, авторы атаки замечают, что применяемая ими техника не зависит от выбранного автоморфизма θ .

Обратим внимание на отображение (16) и исследуем его свойства подробнее в зависимости от выбора автоморфизма θ . Пусть, согласно условию существования 2-группы Судзуки $A(m, \theta)$, $3 \leq m \in \mathbb{N}$, $q = 2^m$ и поле $\mathbb{F}_q$ имеет нетривиальный автоморфизм θ нечетного порядка. Рассмотрим следующее уравнение относительно переменной $x \in \mathbb{F}_q$:

$$e^\theta x + ex^\theta = 0, \quad e \in \mathbb{F}_q, \quad e \neq 0. \quad (17)$$

Домножим правую и левую части уравнения (17) на e^{-1} :

$$e^{\theta-1} x + x^\theta = 0.$$

Вынося x за скобки, получим эквивалентное уравнение:

$$x(e^{\theta-1} + x^{\theta-1}) = 0.$$

Так как в поле не существует делителей нуля, данное уравнение сводится к системе вида

$$\begin{cases} x = 0, \\ x^{\theta-1} = e^{\theta-1}. \end{cases} \quad (18)$$

Для второго уравнения системы (18) справедливо

$$x^{\theta-1} = e^{\theta-1} \Leftrightarrow (xe^{-1})^{\theta-1} = 1 \Leftrightarrow y^{\theta-1} = 1,$$

где $y = xe^{-1} \in \mathbb{F}_q$.

Так как число различных корней n -й степени из единицы в поле $\mathbb{F}_q$ равно

$$\gcd(n, q-1),$$

а автоморфизм θ поля $\mathbb{F}_{2^m}$ имеет вид $\theta : x \rightarrow x^{2^w}$ для некоторого $w \in \{0, \dots, m-1\}$, то при $q = 2^m$ получаем, что число решений уравнения $y^{\theta-1} = 1$ равно

$$\gcd(2^w - 1, 2^m - 1).$$

Отметим, что для каждого из таких решений y^* можно однозначным образом найти значение $x^* = y^*e$, при этом различным решениям y_1^* и y_2^* соответствуют различные значения $x_1^* = y_1^*e$ и $x_2^* = y_2^*e$.

Рассмотрим формулу, справедливую для любых натуральных v и u :

$$\gcd(2^v - 1, 2^u - 1) = 2^{\gcd(v, u)} - 1. \quad (19)$$

Подставляя значения $v = w$ и $u = m$ в формулу (19), получаем, что количество решений второго уравнения системы (18) при $\theta : x \rightarrow x^{2^w}$ равно $2^{\gcd(w, m)} - 1$. Прибавляя нулевое решение, окончательно имеем, что система (18), как и эквивалентное ей уравнение (17), при $\theta : x \rightarrow x^{2^w}$ имеет $2^{\gcd(w, m)}$ решений.

Таким образом, замечание в [6] о том, что выбор автоморфизма не играет существенной роли, в общем случае неверно. Мощность ядра отображения (16) при $q = 2^m$ равна 2 лишь для таких автоморфизмов $\theta : x \rightarrow x^{2^w}$, что $\gcd(w, m) = 1$. В случае же, когда $\gcd(w, m) > 1$, размер ядра, соответственно, будет равен $2^{\gcd(w, m)} > 2^1 = 2$.

Например, если при $m = 81$ используется автоморфизм $\theta : x \rightarrow x^{2^{27}}$, то число решений любого уравнения вида (15), имеющего хотя бы одно решение, будет равно $2^{\gcd(27, 81)} = 2^{27}$, поэтому их перебор может оказаться существенно сложнее перебора в рассмотренном авторами атаки случае.

3.4. α , β и γ имеют тип $(2, 2, \dots, 2, 16, 16, \dots, 16)$. Атакуемая криптосистема MST_3 с ограничениями на ключи, основанная на 2-группе Судзуки порядка $(2^{81})^2$, задается логарифмической сигнатурой β , покрытиями α , γ типа $(2, 2, \dots, 2, 16, 16, \dots, 16)$ и параметром t . Действуя аналогично случаю с α , β и γ , имеющими тип $(8, 64, 64, \dots, 64)$, и используя идентичные обозначения, авторы атаки получают следующую систему уравнений относительно $x \in \mathbb{F}_{2^{81}}$:

$$\{e_{ijkl}^\theta x + e_{ijkl} x^\theta = f_{ijkl} + g_{ijkl} + v \mid v \in V\}, \quad (20)$$

где V — некоторая группа порядка 2^{41} , состоящая из элементов поля $\mathbb{F}_{2^{81}}$. При этом элемент $x \in \mathbb{F}_{2^{81}}$ является решением всей системы (20), если он является решением хотя бы одного из уравнений этой системы.

В [6] утверждается, что если автоморфизм θ имеет вид $\theta : x \rightarrow x^2$, то любое уравнение из системы (20) либо не имеет решений, либо имеет 2 решения. В этом случае общее число решений системы ограничено сверху величиной 2^{42} . При этом авторы атаки замечают, что применяемая ими техника не зависит от выбранного автоморфизма θ .

Однако, рассуждая схожим предыдущему случаю образом, можно показать, что зависимость сложности атаки от выбранного автоморфизма θ существует. Так, если $\theta : x \rightarrow x^{2^w}$, $w \in \{0, \dots, m-1\}$, то любое уравнение из системы (20), рассматриваемое над полем $x \in \mathbb{F}_{2^m}$, либо не имеет решений, либо имеет $2^{\gcd(w, m)}$ решений. Поэтому общее число решений системы ограничено сверху величиной $2^{\gcd(w, m) + \dim(V)}$, в связи с чем их перебор может оказаться существенно сложнее перебора в рассмотренном авторами атаки случае.

4. Исследование множества логарифмических сигнатур для центра 2-группы Судзуки

4.1. Логарифмические сигнатуры в криптосистеме MST_3 . Одним из параметров стойкости любой криптосистемы является объем ключевого пространства. Применительно к криптосистеме MST_3 на основе 2-группы Судзуки это означает необходимость исследования количества простых логарифмических сигнатур для центра данной группы. Существование алгоритмов генерации канонических и трансверсальных логарифмических сигнатур облегчает задачу оценки их количества. В общем же случае понятие простой логарифмической сигнатуры не имеет конструктивного определения. Одним из вариантов решения данной проблемы является оценка количества всех логарифмических сигнатур.

Следует напомнить, что различные логарифмические сигнатуры могут порождать одинаковые отображения вида (2), тогда они называются эквивалентными. Это приводит к появлению непересекающихся множеств эквивалентных логарифмических сигнатур, что уменьшает количество неэквивалентных ключей криптосистемы MST_3 . Поэтому наряду с исследованием множества всех логарифмических сигнатур будем проводить и исследование множества неэквивалентных логарифмических сигнатур.

Пусть G — 2-группа Судзуки порядка q^2 , где $q = 2^m$, $3 \leq m \in \mathbb{N}$ и поле $\mathbb{F}_q$ имеет нетривиальный автоморфизм θ нечетного порядка. В последующих разделах приводятся результаты исследований количества логарифмических сигнатур для центра группы G , обозначенного через $Z(G) = Z$. Полученные оценки зависят от параметра m и типа логарифмической сигнатуры $(r_1, \dots, r_v)$, где $r_i \geq 2$, $i = 1, \dots, v$, $v \geq 2$ и $\prod_{i=1}^v r_i = 2^m$.

4.2. Исследование количества канонических логарифмических сигнатур.

Утверждение 1. *Количество различных канонических логарифмических сигнатур типа $(r_1, \dots, r_v)$ равно*

$$m! \cdot \prod_{i=1}^v \frac{r_i!}{(\log_2 r_i)!}.$$

Доказательство. Количество канонических логарифмических сигнатур тесно связано с количеством упорядоченных разбиений множества $\{1, \dots, m\}$. Известно, что число упорядоченных разбиений множества мощностью m на v подмножеств мощностей $k_1, \dots, k_v$ равно

$$m! \cdot \frac{1}{\prod_{i=1}^v (k_i)!}. \quad (21)$$

Пусть $[K_1, \dots, K_v]$ — упорядоченное разбиение множества $\{1, \dots, m\}$ и $|K_i| = k_i$, $i = 1, \dots, v$. Построим по разбиению $[K_1, \dots, K_v]$ все такие канонические логарифмические сигнатуры $\delta = [D_1, \dots, D_v] = (d_{ij})$, что для каждого $i = 1, \dots, v$ блоки D_i содержат все различные 2^{k_i} векторов с нулевыми значениями координат на позициях, соответствующих подмножеству $\{1, \dots, m\} \setminus K_i$. Построенные данным образом из одного разбиения $[K_1, \dots, K_v]$ канонические логарифмические сигнатуры будут отличаться друг от друга только порядком расположения элементов в

блоках, поэтому их число для фиксированного разбиения равно

$$\prod_{i=1}^v 2^{k_i!} \quad (22)$$

Из (21) и (22) следует, что общее число различных канонических логарифмических сигнатур типа $(2^{k_1}, \dots, 2^{k_v})$ равно

$$m! \cdot \prod_{i=1}^v \frac{2^{k_i!}}{(k_i)!}. \quad (23)$$

Подставляя $2^{k_i} = r_i$ и $k_i = \log_2 r_i$, $i = 1, \dots, v$, в (23), получаем, что количество различных канонических логарифмических сигнатур типа $(r_1, \dots, r_v)$ равно

$$m! \cdot \prod_{i=1}^v \frac{r_i!}{(\log_2 r_i)!}.$$

Лемма 1. *Две логарифмические сигнатуры δ и δ' одного типа $(r_1, \dots, r_v)$ эквивалентны тогда и только тогда, когда*

$$\theta_\delta \equiv \theta_{\delta'}. \quad (24)$$

Доказательство. Так как логарифмические сигнатуры δ и δ' имеют один тип $(r_1, \dots, r_v)$, то

$$\lambda_\delta \equiv \lambda_{\delta'}, \quad \lambda_\delta^{-1} \equiv \lambda_{\delta'}^{-1}. \quad (25)$$

Пусть логарифмические сигнатуры δ и δ' одного типа $(r_1, \dots, r_v)$ эквивалентны. Из (25) получаем, что для любого набора $(j_1, \dots, j_v) \in \mathbb{Z}_{r_1} \times \dots \times \mathbb{Z}_{r_v}$

$$\theta_\delta(j_1, \dots, j_v) = \theta_\delta(\lambda_\delta^{-1}(x)) = \check{\delta}(x) = \check{\delta}'(x) = \theta_{\delta'}(\lambda_{\delta'}^{-1}(x)) = \theta_{\delta'}(j_1, \dots, j_v),$$

где $x = \lambda_\delta(j_1, \dots, j_v) = \lambda_{\delta'}(j_1, \dots, j_v)$. Следовательно, выполняется соотношение (24).

Пусть логарифмические сигнатуры δ и δ' имеют один тип $(r_1, \dots, r_v)$ и при этом выполняется соотношение (24). Пользуясь (25), получаем, что для любого $x \in \mathbb{Z}_{2^m}$

$$\check{\delta}(x) = \theta_\delta(\lambda_\delta^{-1}(x)) = \theta_{\delta'}(\lambda_{\delta'}^{-1}(x)) = \theta_{\delta'}(\lambda_{\delta'}^{-1}(x)) = \check{\delta}'(x).$$

Следовательно, логарифмические сигнатуры δ и δ' эквивалентны.

Утверждение 2. *Количество различных неэквивалентных канонических логарифмических сигнатур типа $(r_1, \dots, r_v)$ равно*

$$m! \cdot \prod_{i=1}^v \frac{r_i!}{(\log_2 r_i)!}.$$

Доказательство. С учетом утверждения 1 для доказательства достаточно показать, что все различные канонические сигнатуры одного типа неэквивалентны. Пусть $\delta = (d_{ij})$ и $\delta' = (d'_{ij})$ — две эквивалентные канонические логарифмические сигнатуры типа $(r_1, \dots, r_v)$. Из леммы 1 следует, что

$$\theta_\delta \equiv \theta_{\delta'}$$

и так как δ и δ' — логарифмические сигнатуры, а не покрытия, то

$$\theta_\delta^{-1} \equiv \theta_{\delta'}^{-1}.$$

Обозначим нулевой вектор пространства размерности m над полем $\mathbb{F}_2$ символом $\bar{0}$. Из определения канонической логарифмической сигнатуры следует, что каждый ее блок содержит $\bar{0}$, следовательно, разложение элемента $\bar{0}$ по канонической логарифмической сигнатуре всегда единственно и имеет следующий вид:

$$\bar{0} \oplus \bar{0} \oplus \dots \oplus \bar{0} = \bar{0}.$$

Так как $\theta_\delta^{-1}(\bar{0}) = \theta_{\delta'}^{-1}(\bar{0})$, то и соответствующие позиции нулевых векторов в блоках логарифмических сигнатур δ и δ' совпадают. Положим $\theta_\delta^{-1}(\bar{0}) = \theta_{\delta'}^{-1}(\bar{0}) = (j_1^* - 1, \dots, j_v^* - 1)$, тогда элементы $d_{ij_i^*}$ и $d'_{ij_i^*}$ равны $\bar{0}$.

Рассмотрим произвольный элемент d_{ij_i} логарифмической сигнатуры δ и соответствующий элемент d'_{ij_i} логарифмической сигнатуры δ' . Справедлива цепочка равенств:

$$\begin{aligned} d_{ij_i} &= d_{1j_1^*} \oplus \dots \oplus d_{(i-1)j_{i-1}^*} \oplus d_{ij_i} \oplus d_{(i+1)j_{i+1}^*} \oplus \dots \oplus d_{vj_v^*} = \\ &= \theta_\delta(j_1^* - 1, \dots, j_{i-1}^* - 1, j_i - 1, j_{i+1}^* - 1, \dots, j_v^* - 1) = \\ &= \theta_{\delta'}(j_1^* - 1, \dots, j_{i-1}^* - 1, j_i - 1, j_{i+1}^* - 1, \dots, j_v^* - 1) = \\ &= d'_{1j_1^*} \oplus \dots \oplus d'_{(i-1)j_{i-1}^*} \oplus d'_{ij_i} \oplus d'_{(i+1)j_{i+1}^*} \oplus \dots \oplus d'_{vj_v^*} = d'_{ij_i}. \end{aligned}$$

В силу произвольности $j_i = 1, \dots, r_i$ и $i = 1, \dots, v$ имеет место полное совпадение логарифмических сигнатур δ и δ' .

Таким образом, все различные канонические логарифмические сигнатуры одного типа неэквивалентны, что и требовалось показать.

4.3. Исследование количества трансверсальных логарифмических сигнатур.

Утверждение 3. *Количество различных трансверсальных логарифмических сигнатур типа $(r_1, \dots, r_v)$ равно*

$$\prod_{i=0}^{m-1} (2^m - 2^i) \cdot \prod_{i=1}^v \left(\frac{r_i!}{\prod_{j=0}^{\log_2 r_i - 1} (r_i - 2^j)} \left(\prod_{j=1}^{i-1} r_j \right)^{r_i - \log_2 r_i} \right). \quad (26)$$

Доказательство. Зафиксируем некоторую подгруппу $H_1 < Z$, где $|H_1| = n_1$. Будем рассматривать подгруппы H_2 , для которых $|H_2| = n_2$ и $H_1 < H_2 < Z$, и найдем их количество. Для этого воспользуемся возможностью перехода от центра 2-группы Судзуки к векторному пространству размерности m над полем $\mathbb{F}_2$.

Выберем $\log_2 n_2 - \log_2 n_1$ упорядоченных базисных векторов пространства Z , не принадлежащих подпространству H_1 . Это можно сделать

$$\prod_{j=\log_2 n_1}^{\log_2 n_2 - 1} (2^m - 2^j)$$

способами.

Заметим, что факторгруппа любой группы H_2 по H_1 состоит из n_2/n_1 элементов и, таким образом, имеет $\log_2(n_2/n_1)$ базисных векторов. При этом каждый из этих базисных векторов может быть сложен с любым из векторов подпространства H_1 без потери своих базисных свойств. Получаем, что количество упорядоченных базисов факторгруппы группы H_2 по H_1 равно

$$n_1^{\log_2(n_2/n_1)} \cdot \prod_{j=0}^{\log_2(n_2/n_1)-1} (n_2/n_1 - 2^j).$$

Разделив количество всевозможных упорядоченных базисов на количество упорядоченных базисов одной факторгруппы, получим количество всех различных подгрупп H_2 , для которых $|H_2| = n_2$ и $H_1 < H_2 < Z$:

$$\frac{\prod_{j=\log_2 n_1}^{\log_2 n_2-1} (2^m - 2^j)}{n_1^{\log_2(n_2/n_1)} \cdot \prod_{j=0}^{\log_2(n_2/n_1)-1} (n_2/n_1 - 2^j)}. \quad (27)$$

Зафиксируем любую такую подгруппу H_2 , что $|H_2| = n_2$ и $H_1 < H_2 < Z$. Рассмотрим все множества, содержащие по одному представителю из каждого смежного класса подгруппы H_2 по подгруппе H_1 , и найдем их количество. Так как число всех смежных классов равно n_2/n_1 и при этом каждый из них может быть представлен любым из n_1 элементов, то количество таких множеств для любой фиксированной подгруппы H_2 равно

$$n_1^{n_2/n_1}. \quad (28)$$

Из (27) и (28) следует, что количество различных множеств, содержащих по одному представителю из каждого смежного класса произвольной группы H_2 по фиксированной подгруппе H_1 при условии, что $|H_1| = n_1$, $|H_2| = n_2$ и $H_1 < H_2 < Z$, равно

$$\begin{aligned} & \frac{\prod_{j=\log_2 n_1}^{\log_2 n_2-1} (2^m - 2^j)}{n_1^{\log_2(n_2/n_1)} \cdot \prod_{j=0}^{\log_2(n_2/n_1)-1} (n_2/n_1 - 2^j)} \cdot n_1^{n_2/n_1} = \\ & = \frac{\prod_{j=\log_2 n_1}^{\log_2 n_2-1} (2^m - 2^j)}{\prod_{j=0}^{\log_2(n_2/n_1)-1} (n_2/n_1 - 2^j)} \cdot n_1^{n_2/n_1 - \log_2(n_2/n_1)}. \end{aligned}$$

Рассмотрим трансверсальную логарифмическую сигнатуру $\delta = [D_1, \dots, D_v]$ типа $(r_1, \dots, r_v)$. Пусть $\prod_{j=1}^0 r_j = 1$, $\sum_{j=1}^0 \log_2 r_j = 0$ и блоки D_j , $j = 1, \dots, i-1$, при некотором $i = 1, \dots, v$ зафиксированы. Тогда блок D_i содержит по одному представителю из каждого смежного класса некоторой подгруппы Z_i , где $|Z_i| = \prod_{j=1}^i r_j$, по фиксированной подгруппе Z_{i-1} , где $|Z_{i-1}| = \prod_{j=1}^{i-1} r_j$, причем эти представители расположены в произвольном порядке. Из приведенных выше рассуждений, а также из возможности перестановки представителей в блоке следует, что число различных блоков D_i составляет

$$\frac{\prod_{j=\sum_{j=1}^{i-1} \log_2 r_j}^{\sum_{j=1}^i \log_2 r_j-1} (2^m - 2^j)}{\prod_{j=0}^{\log_2 r_i-1} (r_i - 2^j)} \cdot \left(\prod_{j=1}^{i-1} r_j \right)^{r_i - \log_2 r_i} \cdot r_i! \quad (29)$$

Последовательно фиксируя и заполняя блоки с D_1 по D_v , получим все различные трансверсальные логарифмические сигнатуры заданного типа, причем их количество будет равно произведению соответствующих значений выражения (29) при $i = 1, \dots, v$:

$$\prod_{i=0}^{m-1} (2^m - 2^i) \cdot \prod_{i=1}^v \left(\frac{r_i!}{\prod_{j=0}^{\log_2 r_i - 1} (r_i - 2^j)} \left(\prod_{j=1}^{i-1} r_j \right)^{r_i - \log_2 r_i} \right).$$

Лемма 2. Если две логарифмические сигнатуры одного типа $(r_1, \dots, r_v)$ имеют вид

$$[[\bar{0}, d_{12}, \dots, d_{1r_1}], \dots, [\bar{0}, d_{(v-1)2}, \dots, d_{(v-1)r_{v-1}}], [d_{v1}, d_{v2}, \dots, d_{vr_v}]] \quad (30)$$

и являются эквивалентными, то они полностью совпадают.

Доказательство. Пусть логарифмические сигнатуры $\delta = (d_{ij})$ и $\delta' = (d'_{ij})$ одного типа $(r_1, \dots, r_v)$ являются эквивалентными и имеют вид (30). Тогда из леммы 1 следуют соотношения

$$\lambda_\delta \equiv \lambda_{\delta'}, \quad \lambda_\delta^{-1} \equiv \lambda_{\delta'}^{-1}, \quad \theta_\delta \equiv \theta_{\delta'}, \quad \theta_\delta^{-1} \equiv \theta_{\delta'}^{-1}.$$

Рассмотрим элементы d_{vj_v} и d'_{vj_v} , где $j_v \in \{1, \dots, r_v\}$. Тогда справедлива следующая цепочка равенств:

$$\begin{aligned} d_{vj_v} &= d_{11} \oplus \dots \oplus d_{(v-1)1} \oplus d_{vj_v} = \theta_\delta(0, \dots, 0, j_v - 1) = \\ &= \theta_{\delta'}(0, \dots, 0, j_v - 1) = d'_{11} \oplus \dots \oplus d'_{(v-1)1} \oplus d'_{vj_v} = d'_{vj_v}. \end{aligned}$$

Поэтому все элементы блоков D_v и D'_v совпадают, в том числе, $d_{v1} = d'_{v1}$.

Пусть d_{ij_i} — произвольный элемент логарифмической сигнатуры δ , не принадлежащий последнему блоку, а d'_{ij_i} — соответствующий элемент логарифмической сигнатуры δ' . Тогда

$$\begin{aligned} d_{ij_i} &= d_{11} \oplus \dots \oplus d_{(i-1)1} \oplus d_{ij_i} \oplus d_{(i+1)1} \oplus \dots \oplus d_{(v-1)1} \oplus (d_{v1} \oplus d_{v1}) = \\ &= \theta_\delta(0, \dots, 0, j_i - 1, 0, \dots, 0) \oplus d_{v1} = \theta_{\delta'}(0, \dots, 0, j_i - 1, 0, \dots, 0) \oplus d'_{v1} = \\ &= d'_{11} \oplus \dots \oplus d'_{(i-1)1} \oplus d'_{ij_i} \oplus d'_{(i+1)1} \oplus \dots \oplus d'_{(v-1)1} \oplus (d'_{v1} \oplus d'_{v1}) = d'_{ij_i}. \end{aligned}$$

В силу произвольности выбора $j = 1, \dots, r_i$ и $i = 1, \dots, v - 1$ эквивалентные логарифмические сигнатуры δ и δ' одного типа $(r_1, \dots, r_v)$, имеющие вид (30), полностью совпадают.

Утверждение 4. Количество различных неэквивалентных трансверсальных логарифмических сигнатур типа $(r_1, \dots, r_v)$ равно

$$\begin{aligned} &\prod_{i=0}^{m-1} (2^m - 2^i) \cdot \left(\frac{r_v!}{\prod_{j=0}^{\log_2 r_v - 1} (r_v - 2^j)} \left(\prod_{j=1}^{v-1} r_j \right)^{r_v - \log_2 r_v} \right) \cdot \\ &\cdot \prod_{i=1}^{v-1} \left(\frac{(r_i - 1)!}{\prod_{j=0}^{\log_2 r_i - 1} (r_i - 2^j)} \left(\prod_{j=1}^{i-1} r_j \right)^{r_i - \log_2 r_i - 1} \right). \end{aligned} \quad (31)$$

Доказательство. Снова воспользуемся возможностью перехода от центра Z к векторному пространству размерности m над полем $\mathbb{F}_2$. Рассмотрим произвольную трансверсальную логарифмическую сигнатуру $\delta = [D_1, \dots, D_v] = (d_{ij})$ типа $(r_1, \dots, r_v)$. Заметим, что прибавление элемента d_{ij} к каждому элементу блока D_i , для любых $j = 1, \dots, r_i$, $i = 1, \dots, v-1$, приведет к получению новой трансверсальной логарифмической сигнатуры δ' , построенной по той же цепочке подгрупп, но, возможно, из других представителей соответствующих смежных классов.

Воспользовавшись этим свойством, добавим к каждому элементу блока D_i элемент d_{i1} для всех $i = 1, \dots, v-1$. Получим некоторую трансверсальную логарифмическую сигнатуру $\delta' = [D'_1, \dots, D'_v]$. Далее к каждому элементу блока D'_v добавим элемент

$$d = d_{11} \oplus d_{21} \oplus \dots \oplus d_{(v-1)1}.$$

Так как $d \in Z_{v-1}$, то его добавление к элементам блока D'_v , состоящего из представителей всех смежных классов подгруппы Z_v по подгруппе Z_{v-1} , также приведет к получению трансверсальной логарифмической сигнатуры δ^* , на основе той же самой цепочки подгрупп. Заметим, что δ^* имеет вид (30).

Покажем, что δ^* эквивалентна δ . Действительно, так как из однотипности этих логарифмических сигнатур следует, что $\lambda_\delta^{-1} \equiv \lambda_{\delta^*}^{-1}$, то для любого такого $x \in \mathbb{Z}_m$, что $\lambda_\delta^{-1}(x) = \lambda_{\delta^*}^{-1}(x) = (j_1 - 1, \dots, j_v - 1)$, справедливы равенства

$$\begin{aligned} \check{\delta}(x) &= \theta_\delta(\lambda_\delta^{-1}(x)) = \theta_\delta(j_1 - 1, \dots, j_v - 1) = d_{1j_1} \oplus \dots \oplus d_{(v-1)j_{v-1}} \oplus d_{vj_v} = \\ &= d_{1j_1} \oplus \dots \oplus d_{(v-1)j_{v-1}} \oplus d_{vj_v} \oplus (d_{11} \oplus \dots \oplus d_{(v-1)1}) \oplus (d_{11} \oplus \dots \oplus d_{(v-1)1}) = \\ &= (d_{1j_1} \oplus d_{11}) \oplus \dots \oplus (d_{(v-1)j_{v-1}} \oplus d_{(v-1)1}) \oplus (d_{vj_v} \oplus d_{11} \oplus \dots \oplus d_{(v-1)1}) = \\ &= d_{1j_1}^* \oplus \dots \oplus d_{(v-1)j_{v-1}}^* \oplus d_{vj_v}^* = \theta_{\delta^*}(j_1 - 1, \dots, j_v - 1) = \theta_{\delta^*}(\lambda_{\delta^*}^{-1}(x)) = \check{\delta}^*(x). \end{aligned}$$

Таким образом, для произвольной трансверсальной логарифмической сигнатуры существует эквивалентная ей трансверсальная логарифмическая сигнатура такого же типа, имеющая вид (30). Это позволяет оценить сверху количество различных неэквивалентных трансверсальных логарифмических сигнатур количеством различных трансверсальных логарифмических сигнатур вида (30).

Лемма 2 позволяет оценить снизу количество различных неэквивалентных трансверсальных логарифмических сигнатур количеством различных трансверсальных логарифмических сигнатур вида (30). Таким образом число различных неэквивалентных трансверсальных логарифмических сигнатур равно числу различных трансверсальных логарифмических сигнатур вида (30).

Аналогично доказательству утверждения 3 получаем формулу (31) количества различных трансверсальных логарифмических сигнатур вида (30), имеющую два отличия от (26): степень $r_i - \log_2 r_i - 1$ вместо $r_i - \log_2 r_i$ и множитель $(r_i - 1)!$ вместо $r_i!$ при $i = 1, \dots, v-1$ (так как во всех блоках, кроме последнего, первый элемент — нулевой вектор).

4.4. Исследование количества всех логарифмических сигнатур. Введем обозначения для следующих наборов из $\mathbb{Z}_{r_1} \times \dots \times \mathbb{Z}_{r_v}$:

$$\begin{aligned} \sigma_0 &= (0, \dots, 0), \\ \sigma_i^j &= (0, \dots, 0, j, 0, \dots, 0), \end{aligned}$$

где элемент $j \in \mathbb{Z}_{r_i}$ расположен на i -й позиции набора, $i = 1, \dots, v$.

Лемма 3. Пусть δ — произвольная логарифмическая сигнатура типа $(r_1, \dots, r_v)$. Тогда для любого набора $(j_1, \dots, j_v) \in \mathbb{Z}_{r_1} \times \dots \times \mathbb{Z}_{r_v}$

$$\theta_\delta(j_1, \dots, j_v) = \begin{cases} \theta_\delta(\sigma_1^{j_1}) \oplus \dots \oplus \theta_\delta(\sigma_v^{j_v}), & \text{если } v \text{ — нечетное,} \\ \theta_\delta(\sigma_1^{j_1}) \oplus \dots \oplus \theta_\delta(\sigma_v^{j_v}) \oplus \theta_\delta(\sigma_0), & \text{если } v \text{ — четное.} \end{cases}$$

Доказательство. Пусть $\delta = (d_{ij})$ — произвольная логарифмическая сигнатура типа $(r_1, \dots, r_v)$, v — нечетное. Тогда для любого набора $(j_1, \dots, j_v) \in \mathbb{Z}_{r_1} \times \dots \times \mathbb{Z}_{r_v}$

$$\begin{aligned} \theta_\delta(j_1, \dots, j_v) &= d_{1(j_1+1)} \oplus \dots \oplus d_{v(j_v+1)} = \\ &= (d_{1(j_1+1)} \oplus d_{21} \oplus d_{31} \oplus \dots \oplus d_{(v-1)1} \oplus d_{v1}) \oplus \\ &\oplus (d_{11} \oplus d_{2(j_2+1)} \oplus d_{31} \oplus \dots \oplus d_{(v-1)1} \oplus d_{v1}) \oplus \\ &\oplus \dots \oplus \\ &\oplus (d_{11} \oplus d_{21} \oplus d_{31} \oplus \dots \oplus d_{(v-1)1} \oplus d_{v(j_v+1)}) = \\ &= \theta_\delta(\sigma_1^{j_1}) \oplus \dots \oplus \theta_\delta(\sigma_v^{j_v}). \end{aligned}$$

Если v — четное, то для любого набора $(j_1, \dots, j_v) \in \mathbb{Z}_{r_1} \times \dots \times \mathbb{Z}_{r_v}$

$$\begin{aligned} \theta_\delta(j_1, \dots, j_v) &= d_{1(j_1+1)} \oplus \dots \oplus d_{v(j_v+1)} = \\ &= (d_{1(j_1+1)} \oplus d_{21} \oplus d_{31} \oplus \dots \oplus d_{(v-1)1} \oplus d_{v1}) \oplus \\ &\oplus (d_{11} \oplus d_{2(j_2+1)} \oplus d_{31} \oplus \dots \oplus d_{(v-1)1} \oplus d_{v1}) \oplus \\ &\oplus \dots \oplus \\ &\oplus (d_{11} \oplus d_{21} \oplus d_{31} \oplus \dots \oplus d_{(v-1)1} \oplus d_{v(j_v+1)}) \oplus \\ &\oplus (d_{11} \oplus d_{21} \oplus d_{31} \oplus \dots \oplus d_{(v-1)1} \oplus d_{v1}) = \\ &= \theta_\delta(\sigma_1^{j_1}) \oplus \dots \oplus \theta_\delta(\sigma_v^{j_v}) \oplus \theta_\delta(\sigma_0). \end{aligned}$$

Сопоставим каждому набору $(s_1, \dots, s_v) \in \mathbb{Z}_{r_1} \times \dots \times \mathbb{Z}_{r_v}$ следующие множества:

$$\Theta(s_1, \dots, s_v) = \{(j_1, \dots, j_v) \mid 0 \leq j_i \leq s_i, i = 1, \dots, v\},$$

$$\Theta_k(s_1, \dots, s_v) = \{(j_1, \dots, j_{k-1}, s_k, j_{k+1}, \dots, j_v) \mid 0 \leq j_i \leq s_i, i = 1, \dots, v, i \neq k\},$$

где $k = 1, \dots, v$.

Лемма 4. Для любого $k = 1, \dots, v$, для произвольного набора $(s_1, \dots, s_{k-1}, s_k, s_{k+1}, \dots, s_v) \in \mathbb{Z}_{r_1} \times \dots \times \mathbb{Z}_{r_{k-1}} \times \mathbb{Z}_{r_k-1} \times \mathbb{Z}_{r_{k+1}} \times \dots \times \mathbb{Z}_{r_v}$

$$\begin{aligned} \Theta(s_1, \dots, s_{k-1}, s_k, s_{k+1}, \dots, s_v) \cap \Theta_k(s_1, \dots, s_{k-1}, s_k + 1, s_{k+1}, \dots, s_v) &= \emptyset, \\ \Theta(s_1, \dots, s_{k-1}, s_k, s_{k+1}, \dots, s_v) \cup \Theta_k(s_1, \dots, s_{k-1}, s_k + 1, s_{k+1}, \dots, s_v) &= \\ = \Theta(s_1, \dots, s_{k-1}, s_k + 1, s_{k+1}, \dots, s_v). \end{aligned}$$

Доказательство. Для доказательства леммы достаточно заметить, что

$$\begin{aligned} \Theta(s_1, \dots, s_{k-1}, s_k + 1, s_{k+1}, \dots, s_v) &= \\ = \{(j_1, \dots, j_v) \mid 0 \leq j_k \leq s_k + 1, 0 \leq j_i \leq s_i, i = 1, \dots, v, i \neq k\} &= \\ = \{(j_1, \dots, j_v) \mid 0 \leq j_k \leq s_k, 0 \leq j_i \leq s_i, i = 1, \dots, v, i \neq k\} \cup & \\ \cup \{(j_1, \dots, j_v) \mid j_k = s_k + 1, 0 \leq j_i \leq s_i, i = 1, \dots, v, i \neq k\} &= \\ = \Theta(s_1, \dots, s_{k-1}, s_k, s_{k+1}, \dots, s_v) \cup \Theta_k(s_1, \dots, s_{k-1}, s_k + 1, s_{k+1}, \dots, s_v). \end{aligned}$$

Лемма 5. Пусть δ — произвольная логарифмическая сигнатура типа $(r_1, \dots, r_v)$. Тогда для любого $k = 1, \dots, v$, для любого набора $(s_1, \dots, s_{k-1}, s_k, s_{k+1}, \dots, s_v) \in \mathbb{Z}_{r_1} \times \dots \times \mathbb{Z}_{r_{k-1}} \times \mathbb{Z}_{r_{k-1}} \times \mathbb{Z}_{r_{k+1}} \times \dots \times \mathbb{Z}_{r_v}$ значение отображения θ_δ на каждом наборе из множества $\Theta_k(s_1, \dots, s_{k-1}, s_k + 1, s_{k+1}, \dots, s_v)$ однозначно определяется значениями отображения θ_δ на наборах из множества $\Theta(s_1, \dots, s_{k-1}, s_k, s_{k+1}, \dots, s_v) \cup \sigma_k^{s_k+1}$.

Доказательство. Пусть δ — произвольная логарифмическая сигнатура типа $(r_1, \dots, r_v)$, v — нечетное. Тогда из леммы 3 следует, что для произвольного набора $(j_1, \dots, j_{k-1}, s_k + 1, j_{k+1}, \dots, j_v) \in \Theta_k(s_1, \dots, s_{k-1}, s_k + 1, s_{k+1}, \dots, s_v)$

$$\begin{aligned} & \theta_\delta(j_1, \dots, j_{k-1}, s_k + 1, j_{k+1}, \dots, j_v) = \\ & = \theta_\delta(\sigma_1^{j_1}) \oplus \dots \oplus \theta_\delta(\sigma_{k-1}^{j_{k-1}}) \oplus \theta_\delta(\sigma_k^{s_k+1}) \oplus \theta_\delta(\sigma_{k+1}^{j_{k+1}}) \oplus \dots \oplus \theta_\delta(\sigma_v^{j_v}). \end{aligned} \quad (32)$$

Таким образом, значение отображения θ_δ на произвольном наборе из множества $\Theta_k(s_1, \dots, s_{k-1}, s_k + 1, s_{k+1}, \dots, s_v)$ однозначно определяется значениями отображения θ_δ на наборах σ_i^j , $0 \leq j \leq s_i$, $i = 1, \dots, v$, $i \neq k$, и наборе $\sigma_k^{s_k+1}$. Остается заметить, что $\sigma_i^j \in \Theta(s_1, \dots, s_{k-1}, s_k, s_{k+1}, \dots, s_v)$ при $0 \leq j \leq s_i$, $i = 1, \dots, v$, $i \neq k$.

В случае четного v в правой части равенства (32) возникает дополнительное слагаемое $\theta_\delta(\sigma_0)$. Поскольку $\sigma_0 \in \Theta(s_1, \dots, s_{k-1}, s_k, s_{k+1}, \dots, s_v)$, лемма полностью доказана.

Теорема 1. Количество различных неэквивалентных логарифмических сигнатур типа $(r_1, \dots, r_v)$ не превышает

$$\begin{aligned} & 2^m \cdot \prod_{s=2}^{\max_{1 \leq j \leq v} r_j} \prod_{k=1}^{p_s} \left(\left(\sum_{n=k}^{p_s} (s-1)^{p_{s-1}-n} s^{n-1} \cdot \prod_{l=2}^{s-2} l^{p_l-p_{l+1}} \right) + \right. \\ & \left. + \sum_{i=s+1}^{\max_{1 \leq j \leq v} r_j} \left(\sum_{n=1}^{p_i} (i-1)^{p_{i-1}-n} i^{n-1} \cdot \prod_{l=2}^{i-2} l^{p_l-p_{l+1}} \right) \right), \end{aligned} \quad (33)$$

где $p_i = \left| \left\{ r \mid r \in \{r_1, \dots, r_v\}, r \geq i \right\} \right|$, $i = 2, \dots, \max_{1 \leq j \leq v} r_j$.

Доказательство. Лемма 1 позволяет утверждать, что количество неэквивалентных логарифмических сигнатур типа $(r_1, \dots, r_v)$ равно количеству различных отображений $\theta_\delta : \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \times \dots \times \mathbb{Z}_{r_v} \rightarrow \mathbb{F}_{2^m}$ при всевозможных δ типа $(r_1, \dots, r_v)$.

Для получения верхней оценки количества различных отображений θ_δ рассмотрим ряд свойств, характерных для любого отображения θ_δ вне зависимости от выбора логарифмической сигнатуры δ типа $(r_1, \dots, r_v)$. С учетом рассматриваемых свойств будем последовательно определять значения отображения θ_δ на каждом из наборов $(j_1, \dots, j_v) \in \mathbb{Z}_{r_1} \times \dots \times \mathbb{Z}_{r_v}$ и при этом оценивать максимальное число возможных значений $\theta_\delta(j_1, \dots, j_v)$ с учетом уже определенных.

Тривиальная верхняя оценка количества различных отображений θ_δ может быть получена с учетом свойств области определения и области значений любого отображения θ_δ . Так как мощность области определения равна $r_1 \cdot \dots \cdot r_v = 2^m$, мощность область значений равна 2^m , то число различных отображений θ_δ не превышает

$$\prod_{i=1}^{2^m} 2^m = 2^{m2^m}. \quad (34)$$

Заметим, что для любой логарифмической сигнатуры δ типа $(r_1, \dots, r_v)$

$$(j_1, \dots, j_v) = (j'_1, \dots, j'_v) \Leftrightarrow \theta_\delta(j_1, \dots, j_v) = \theta_\delta(j'_1, \dots, j'_v),$$

что говорит о несовпадении элементов $\theta_\delta(j_1, \dots, j_v)$ при различных значениях набора $(j_1, \dots, j_v) \in \mathbb{Z}_{r_1} \times \dots \times \mathbb{Z}_{r_v}$. Отсюда следует новая верхняя оценка числа различных отображений θ_δ :

$$\prod_{i=0}^{2^m-1} (2^m - i) = 2^m! \quad (35)$$

Порядок определения значений отображения θ_δ при получении верхних оценок (34), (35) мог быть произвольным, поскольку связь между значениями отображения θ_δ на конкретных наборах аргументов не учитывалась. Рассмотрим алгоритм последовательного определения значений отображения θ_δ на каждом из наборов $(j_1, \dots, j_v) \in \mathbb{Z}_{r_1} \times \dots \times \mathbb{Z}_{r_v}$ с учетом связи между значениями отображения θ_δ на конкретных наборах аргументов. Обозначим операцию присваивания через $\leftarrow$.

Алгоритм последовательного определения значений отображения θ_δ .

Этап 1.

- Определяем значение $\theta_\delta(\sigma_0)$.
- Полагаем $(j_1, \dots, j_v) \leftarrow \sigma_0$.
- Результат: определены значения отображения θ_δ на всех наборах из множества $\Theta(j_1, \dots, j_v)$.

Этап i ($i = 2, \dots, \max_{1 \leq j \leq v} r_j$).

Шаг 1 (выполняется, если $j_1 \leq r_1 - 2$).

- Определяем значение $\theta_\delta(\sigma_1^{j_1+1})$.
- Однозначно определяем значения отображения θ_δ на всех наборах из множества $\Theta_1(j_1 + 1, j_2, j_3, \dots, j_{v-1}, j_v) \setminus \sigma_1^{j_1+1}$ при помощи леммы 5.
- Результат: определены значения отображения θ_δ на всех наборах из множества $\Theta(j_1 + 1, j_2, j_3, \dots, j_{v-1}, j_v)$, что следует из леммы 4.
- Полагаем $(j_1, j_2, j_3, \dots, j_{v-1}, j_v) \leftarrow (j_1 + 1, j_2, j_3, \dots, j_{v-1}, j_v)$.

Шаг 2 (выполняется, если $j_2 \leq r_2 - 2$).

- Определяем значение $\theta_\delta(\sigma_2^{j_2+1})$.
- Однозначно определяем значения отображения θ_δ на всех наборах из множества $\Theta_2(j_1, j_2 + 1, j_3, \dots, j_{v-1}, j_v) \setminus \sigma_2^{j_2+1}$ при помощи леммы 5.
- Результат: определены значения отображения θ_δ на всех наборах из множества $\Theta(j_1, j_2 + 1, j_3, \dots, j_{v-1}, j_v)$, что следует из леммы 4.
- Полагаем $(j_1, j_2, j_3, \dots, j_{v-1}, j_v) \leftarrow (j_1, j_2 + 1, j_3, \dots, j_{v-1}, j_v)$.

...

Шаг v (выполняется, если $j_v \leq r_v - 2$).

- Определяем значение $\theta_\delta(\sigma_v^{j_v+1})$.
- Однозначно определяем значения отображения θ_δ на всех наборах из множества $\Theta_v(j_1, j_2, j_3, \dots, j_{v-1}, j_v + 1) \setminus \sigma_v^{j_v+1}$ при помощи леммы 5.

- Результат: определены значения отображения θ_δ на всех наборах из множества $\Theta(j_1, j_2, j_3, \dots, j_{v-1}, j_v + 1)$, что следует из леммы 4.
- Полагаем $(j_1, j_2, j_3, \dots, j_{v-1}, j_v) \leftarrow (j_1, j_2, j_3, \dots, j_{v-1}, j_v + 1)$.

Для каждого набора $(j_1, \dots, j_v) \in \mathbb{Z}_{r_1} \times \dots \times \mathbb{Z}_{r_v}$ оценим максимальное число возможных значений $\theta_\delta(j_1, \dots, j_v)$ при условии, что эти значения последовательно определялись согласно приведенному алгоритму. При оценке будем пользоваться тем, что все значения отображения θ_δ должны принадлежать множеству $\mathbb{F}_{2^m}$ и быть различны между собой, поэтому для оценки максимального числа возможных значений отображения θ_δ на некотором наборе необходимо знать количество еще не определенных согласно приведенному алгоритму значений отображения θ_δ .

На первом этапе определяется $\theta_\delta(\sigma_0)$ одним из 2^m значений. Пусть перед выполнением t -го шага, $t = 1, \dots, v$, значения отображения θ_δ определены на всех наборах из множества $\Theta(j_1, \dots, j_v)$. Тогда на t -м шаге будет определено

$$|\Theta_t(j_1, \dots, j_{t-1}, j_t + 1, j_{t+1}, \dots, j_v)| = (j_1 + 1) \cdot \dots \cdot (j_{t-1} + 1) \cdot (j_{t+1} + 1) \cdot \dots \cdot (j_v + 1) \quad (36)$$

новых значений.

Введем величины

$$p_i = \left| \left\{ r \mid r \in \{r_1, \dots, r_v\}, r \geq i \right\} \right|, \quad i = 2, \dots, \max_{1 \leq j \leq v} r_j.$$

Заметим, что на i -м этапе, $i = 2, \dots, \max_{1 \leq j \leq v} r_j$, из v шагов выполняются только p_i шагов. Пусть перед n -м по счету выполняемым шагом i -го этапа, $n = 1, \dots, p_i$, $i = 2, \dots, \max_{1 \leq j \leq v} r_j$, значения отображения θ_δ определены на всех наборах из множества $\Theta(j_1, \dots, j_v)$. Тогда среди элементов набора $(j_1, \dots, j_v)$: ровно $p_{i-1} - n + 1$ элементов равных $i - 2$, ровно $n - 1$ элементов равных $i - 1$ и ровно $p_i - p_{i+1}$ элементов равных i , где $i = 2, \dots, i - 2$. Из (36), где $j_t = i - 2$, следует, что количество значений, определяемых на n -м по счету выполняемом шаге i -го этапа, $n = 1, \dots, p_i$, $i = 2, \dots, \max_{1 \leq j \leq v} r_j$, равно

$$(i - 1)^{p_{i-1} - n} i^{n-1} \cdot \prod_{l=2}^{i-2} l^{p_l - p_{l+1}}. \quad (37)$$

Суммируя выражения вида (37) по всем $n = 1, \dots, p_i$, получаем, что число значений отображения θ_δ , определяемых на i -м этапе, $i = 2, \dots, \max_{1 \leq j \leq v} r_j$, равно

$$\sum_{n=1}^{p_i} (i - 1)^{p_{i-1} - n} i^{n-1} \cdot \prod_{l=2}^{i-2} l^{p_l - p_{l+1}}. \quad (38)$$

Из (37) и (38) получаем, что число еще не определенных значений отображения θ_δ перед k -м по счету выполняемым шагом s -го этапа, $k = 1, \dots, p_s$, $s = 2, \dots, \max_{1 \leq j \leq v} r_j$ равно

$$\begin{aligned} & \left(\sum_{n=k}^{p_s} (s - 1)^{p_{s-1} - n} s^{n-1} \cdot \prod_{l=2}^{s-2} l^{p_l - p_{l+1}} \right) + \\ & + \sum_{i=s+1}^{\max_{1 \leq j \leq v} r_j} \left(\sum_{n=1}^{p_i} (i - 1)^{p_{i-1} - n} i^{n-1} \cdot \prod_{l=2}^{i-2} l^{p_l - p_{l+1}} \right). \end{aligned} \quad (39)$$

Таким образом, на k -м по счету (t -м в алгоритме) шаге s -го этапа значение $\theta_\delta(\sigma_t^{j_t+1})$ может быть определено не более, чем (39) способами. Значения отображения θ_δ на всех наборах из множества $\Theta_t(j_1, \dots, j_{t-1}, j_t + 1, j_{t+1}, \dots, j_v) \setminus \sigma_t^{j_t+1}$, согласно лемме 5, однозначно выражаются из уже определенных значений, поэтому могут быть определены не более, чем одним способом.

Итоговая верхняя оценка количества различных отображений θ_δ получается путем перемножения величин (39) по всем $k = 1, \dots, p_s$, $s = 2, \dots, \max_{1 \leq j \leq v} r_j$, и величины 2^m , равной количеству возможных значений $\theta_\delta(\sigma_0)$:

$$2^m \cdot \prod_{s=2}^{\max_{1 \leq j \leq v} r_j} \prod_{k=1}^{p_s} \left(\left(\sum_{n=k}^{p_s} (s-1)^{p_{s-1}-n} s^{n-1} \cdot \prod_{l=2}^{s-2} l^{p_l-p_{l+1}} \right) + \right. \\ \left. + \sum_{i=s+1}^{\max_{1 \leq j \leq v} r_j} \left(\sum_{n=1}^{p_i} (i-1)^{p_{i-1}-n} i^{n-1} \cdot \prod_{l=2}^{i-2} l^{p_l-p_{l+1}} \right) \right).$$

Теорема 2. *Количество различных логарифмических сигнатур типа $(r_1, \dots, r_v)$ не превышает*

$$2^{m(v-1)} \cdot 2^m \cdot \prod_{s=2}^{\max_{1 \leq j \leq v} r_j} \prod_{k=1}^{p_s} \left(\left(\sum_{n=k}^{p_s} (s-1)^{p_{s-1}-n} s^{n-1} \cdot \prod_{l=2}^{s-2} l^{p_l-p_{l+1}} \right) + \right. \\ \left. + \sum_{i=s+1}^{\max_{1 \leq j \leq v} r_j} \left(\sum_{n=1}^{p_i} (i-1)^{p_{i-1}-n} i^{n-1} \cdot \prod_{l=2}^{i-2} l^{p_l-p_{l+1}} \right) \right),$$

где $p_i = \left| \left\{ r \mid r \in \{r_1, \dots, r_v\}, r \geq i \right\} \right|$, $i = 2, \dots, \max_{1 \leq j \leq v} r_j$.

Доказательство. Рассмотрим логарифмическую сигнатуру $\delta = (d_{ij})$ типа $(r_1, \dots, r_v)$. Пусть $a_1, \dots, a_{v-1}$ — произвольные элементы из $\mathbb{F}_{2^m}$. Построим по ним новую логарифмическую сигнатуру $\delta' = (d'_{ij})$ типа $(r_1, \dots, r_v)$:

$$d'_{ij} = d_{ij} \oplus a_i, \quad j = 1, \dots, r_i, \quad i = 1, \dots, v-1, \\ d'_{vj} = d_{vj} \oplus a_1 \oplus a_2 \oplus \dots \oplus a_{v-1}, \quad j = 1, \dots, r_v. \quad (40)$$

Так как δ и δ' имеют одинаковый тип, то $\lambda_\delta \equiv \lambda_{\delta'}$, $\lambda_\delta^{-1} \equiv \lambda_{\delta'}^{-1}$, поэтому для каждого $x \in \mathbb{Z}_{2^m}$

$$\check{\delta}(x) = \theta_\delta(j_1 - 1, \dots, j_v - 1) = d_{1j_1} \oplus \dots \oplus d_{(v-1)j_{v-1}} \oplus d_{vj_v} = \\ = d_{1j_1} \oplus \dots \oplus d_{(v-1)j_{v-1}} \oplus d_{vj_v} \oplus (a_1 \oplus \dots \oplus a_{v-1}) \oplus (a_1 \oplus \dots \oplus a_{v-1}) = \\ = (d_{1j_1} \oplus a_1) \oplus \dots \oplus (d_{(v-1)j_{v-1}} \oplus a_{v-1}) \oplus (d_{vj_v} \oplus a_1 \oplus \dots \oplus a_{v-1}) = \\ = \theta_{\delta'}(j_1 - 1, \dots, j_v - 1) = \check{\delta}'(x),$$

где $(j_1 - 1, \dots, j_v - 1) = \lambda_\delta^{-1}(x) = \lambda_{\delta'}^{-1}(x)$. Отсюда получаем, что δ' эквивалентна δ .

Заметим, что различные наборы элементов $(a_1, \dots, a_{v-1}) \in \mathbb{F}_{2^m} \times \dots \times \mathbb{F}_{2^m}$ порождают различные эквивалентные исходной логарифмические сигнатуры δ' . Количество таких наборов, очевидно, равно

$$\prod_{i=1}^{v-1} 2^m = 2^{m(v-1)}.$$

Следовательно, количество различных логарифмических сигнатур типа $(r_1, \dots, r_v)$ в каждом из классов эквивалентности не меньше, чем $2^{m(v-1)}$.

Рассмотрим две эквивалентные логарифмические сигнатуры $\delta = (d_{ij})$ и $\delta^* = (d_{ij}^*)$ одного типа $(r_1, \dots, r_v)$. Используя в качестве элементов $a_1, \dots, a_{v-1}$ элементы $d_{11}, \dots, d_{(v-1)1}$ (соответственно, $d_{11}^*, \dots, d_{(v-1)1}^*$), аналогично (40) построим по δ (соответственно, по δ^*) эквивалентную ей логарифмическую сигнатуру δ' (соответственно, $\delta^{*'}).$ Так как логарифмические сигнатуры δ' и $\delta^{*'}$ одного типа эквивалентны и имеют вид (30), то по лемме 2 они полностью совпадают. Отсюда следует, что

$$\begin{aligned} d_{ij} \oplus d_{i1} &= d_{ij}^* \oplus d_{i1}^*, \quad j = 1, \dots, r_i, \quad i = 1, \dots, v-1, \\ d_{vj} \oplus d_{11} \oplus d_{21} \oplus \dots \oplus d_{(v-1)1} &= d_{vj}^* \oplus d_{11}^* \oplus d_{21}^* \oplus \dots \oplus d_{(v-1)1}^*, \quad j = 1, \dots, r_v. \end{aligned}$$

Таким образом, для двух произвольных эквивалентных логарифмических сигнатур δ и δ^* одного типа $(r_1, \dots, r_v)$ существуют элементы:

$$a_1 = d_{11} \oplus d_{11}^*, \dots, a_{v-1} = d_{(v-1)1} \oplus d_{(v-1)1}^*,$$

для которых выполняются соотношения

$$\begin{aligned} d_{ij}^* &= d_{ij} \oplus a_i, \quad j = 1, \dots, r_i, \quad i = 1, \dots, v-1, \\ d_{vj}^* &= d_{vj} \oplus a_1 \oplus a_2 \oplus \dots \oplus a_{v-1}, \quad j = 1, \dots, r_v. \end{aligned}$$

Отсюда следует, что количество различных логарифмических сигнатур типа $(r_1, \dots, r_v)$ в каждом из классов эквивалентности не превышает $2^{m(v-1)}$.

Получаем, что нижняя и верхняя оценки количества различных логарифмических сигнатур типа $(r_1, \dots, r_v)$ в каждом из классов эквивалентности совпадают и равны

$$2^{m(v-1)}. \quad (41)$$

Для получения итоговой верхней оценки воспользуемся результатом теоремы 1. Умножая выражения (33) и (41), то есть верхнюю оценку количества неэквивалентных логарифмических сигнатур типа $(r_1, \dots, r_v)$ на число логарифмических сигнатур такого типа в одном классе эквивалентности, получаем, что количество различных логарифмических сигнатур типа $(r_1, \dots, r_v)$ не превышает

$$\begin{aligned} 2^{m(v-1)} \cdot 2^m \cdot \prod_{s=2}^{\max_{1 \leq j \leq v} r_j} \prod_{k=1}^{p_s} \left(\left(\sum_{n=k}^{p_s} (s-1)^{p_{s-1}-n} s^{n-1} \cdot \prod_{l=2}^{s-2} l^{p_l-p_{l+1}} \right) + \right. \\ \left. + \sum_{i=s+1}^{\max_{1 \leq j \leq v} r_j} \left(\sum_{n=1}^{p_i} (i-1)^{p_{i-1}-n} i^{n-1} \cdot \prod_{l=2}^{i-2} l^{p_l-p_{l+1}} \right) \right). \end{aligned}$$

5. Заключение

В работе рассматривается атака на криптосистему с открытым ключом MST_3 на основе 2-группы Судзуки, предложенная в [6]. При естественных предположениях показано, что если логарифмическая сигнатура β , составляющая основную часть секретного ключа криптосистемы MST_3 , имеет тип $(2, 2, \dots, 2)$, то случайно выбранный секретный ключ эквивалентен исходному секретному ключу с вероятностью, приблизительно равной 0.288788. В случае использования логарифмической

сигнатуры β типа $(8, 64, 64, \dots, 64)$ или $(2, 2, \dots, 2, 16, 16, \dots, 16)$ сложность атаки существенно зависит от автоморфизма θ , с помощью которого задается 2-группа Судзуки, и может быть довольно большой, что ограничивает условия применения атаки.

Для центра 2-группы Судзуки получены точные оценки количества различных канонических и трансверсальных логарифмических сигнатур, а также верхние оценки количества различных логарифмических сигнатур произвольного вида.

Список литературы

1. Magliveras S. S., “A cryptosystem from logarithmic signatures of finite groups”, In Proc. 29'th Midwest Symp. Circuits and Systems, 1986, 972–975.
2. Magliveras S. S., Stinson D. R., Trung van T., “New approaches to designing public key cryptosystems using one-way functions and trapdoors in finite groups”, *J. Cryptology*, **15**:4 (2002), 285–297.
3. Vasco M. I. G., Steinwandt R., “Obstacles in two public key cryptosystems based on group factorizations”, *Tatra Mount. Math. Publ.*, **25** (2002), 23–37.
4. Lempken W., Trung van T., Magliveras S. S., Wei W., “A public key cryptosystem based on non-Abelian finite groups”, *J. Cryptology*, **22**:1 (2009), 62–74.
5. Magliveras S. S., Svaba P., Trung van T., Zajac P., “On the security of a realization of cryptosystem MST3”, *Tatra Mount. Math. Publ.*, **41** (2008), 65–78.
6. Blackburn S. R., Cid C., Mullan C., “Cryptanalysis of the MST3 public key cryptosystem”, *J. Math. Cryptology*, **3**:4 (2009), 321–338.
7. Vasco M. I. G., Pozo del A. L. P., Duarte P. T., “A note on the security of MST3”, *Des. Codes and Cryptography*, **55**:2-3 (2010), 189–200.
8. Svaba P., Trung van T., “Public key cryptosystem MST3: cryptanalysis and realization”, *J. Math. Cryptology*, **4**:3 (2010), 271–315.
9. Higman G., “Suzuki 2-groups”, *Illinois J. Math.*, **7**:1 (1963), 79–96.
10. Svaba P., Trung van T., Wolf P., “Logarithmic signatures for Abelian groups and their factorization”, *Tatra Mount. Math. Publ.*, **57**:1 (2013), 21–33.
11. Gordon B., McIntosh R. J., “Some eighth order mock theta functions”, *J. London Math. Soc.*, **62**:2 (2000), 321–335.

Статья поступила 12.09.2014.