Криптосистемы на основе логарифмических сигнатур и покрытий конечных групп

Э. А. Применко, А. С. Рыбкин

Аннотация **– В работе приводится обзор криптографического направления, относящегося к постквантовой криптографии и основанного на использовании логарифмических сигнатур и покрытий конечных групп. Данные математические структуры позволяют синтезировать криптографические схемы, стойкость которых основывается на сложности решения задачи факторизации элемента некоторой конечной группы. Эта задача предположительно будет являться достаточно вычислительно сложной даже в случае появления квантового компьютера.**

Приводится список основных определений и функций, связанных с логарифмическими сигнатурами и покрытиями конечных групп. Описывается связь между этими функциями и задачей факторизации элемента конечной группы. Рассматриваются базовые способы генерации логарифмических сигнатур конечных групп и сложность задачи факторизации для каждого из этих способов.

В хронологическом порядке приводится описание существующих криптографических систем, основанных на логарифмических сигнатурах и покрытиях конечных групп. Рассмотренные криптографические системы имеют достаточно широкий функционал, в частности среди них имеются схемы, предназначенные для шифрования данных, формирования и проверки электронной подписи или генерации псевдослучайных чисел. Особое внимание в обзоре уделяется криптографической системе MST3, которая представляется наиболее перспективной схемой шифрования в рассматриваемом направлении. Приводится описание 2-группы Судзуки, традиционно используемой в качестве конечной группы при реализации криптографической системы MST3. Демонстрируется небольшой пример работы криптосистемы MST3, основанной на 2-группе Судзуки. Помимо вопросов синтеза также рассматриваются основные результаты анализа существующих криптографических систем на основе логарифмических сигнатур и покрытий конечных групп.

Ключевые слова **– постквантовая криптография, логарифмические сигнатуры, покрытия, конечные группы, 2-группа Судзуки, MST.**

I. Введение

Асимметричная криптография является неотъемлемой частью многих информационных систем. Стойкость большинства существующих асимметричных криптосистем основывается на предположениях о вычислительной сложности задачи факторизации целых чисел или задачи дискретного логарифмирования. Наличие квантового алгоритма Шора, позволяющего решать эти задачи с полиномиальной сложностью в случае появления квантового компьютера, делает актуальным поиск новых математических задач, остающихся вычислительно сложными и в постквантовую эру.

Одной из таких задач является задача факторизации в конечной группе, заключающаяся в нахождении разложения произвольного элемента конечной группы по некоторым фиксированным последовательностям элементов этой группы: логарифмическим сигнатурам или покрытиям. Первые попытки построения криптосистем на основе логарифмических сигнатур и покрытий были предприняты в конце 1970-х годов, однако наиболее активное развитие в области криптографии с открытым ключом это направление получило уже в XXI веке. За это время было предложено несколько видов криптосистем на основе логарифмических сигнатур и покрытий, в том числе схем шифрования, схем электронной подписи и механизмов генерации случайных чисел.

Э. А. Применко, МГУ имени М. В. Ломоносова (e-mail: primenko@inbox.ru).
А. С. Рыбкин, ОАО «ИнфоТеКС» (e-mail: Andrey.Rybkin@infotecs.ru).

II. Логарифмические сигнатуры и покрытия конечных групп

В данной главе рассматриваются основные обозначения, определения и отображения, связанные с логарифмическими сигнатурами и покрытиями конечных групп.

Пусть G – мультипликативная конечная группа. Обозначим через $G^{[Z]}$ множество всех конечных последовательностей, состоящих из элементов группы G, и будем записывать каждую такую последовательность в виде строки.

Рассмотрим произвольную последовательность $X = [x_1, x_2, \ldots, x_m] \in G^{[Z]}$. Обозначим число элементов в последовательности X через $|X| = m$. Пусть $Z[G]$ – групповое кольцо, построенное по группе G. Рассматривая элементы последовательности X как элементы группового кольца $Z[G]$, обозначим их сумму, принадлежащую $Z[G]$, через $\overline{X} = \sum_{i=1}^{m} x_i$.

Определение 1. Пусть G – мультипликативная конечная группа, J – подмножество элементов этой группы, а $Z[G]$ – групповое кольцо, построенное по группе G. Рассмотрим такой набор $\alpha = [A_1, A_2, \ldots, A_s]$, состоящий из последовательностей $A_i \in G^{[Z]}$, $i = 1, 2, \ldots, s$, таких 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 соотношение

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

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

$$g = g_1 \cdot g_2 \cdot \ldots \cdot g_s, \text{ где } g_i \in A_i, i = 1,2,\ldots,s. \quad (1)$$

Если α является логарифмической сигнатурой для G, то для всех элементов $g \in G$ разложение (1) существует и является единственным, поскольку в этом случае

$$|A_1| \cdot |A_2| \cdot \ldots \cdot |A_s| = |G|.$$

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 справедливость существования соответствующих аналогов и для логарифмических сигнатур.

Пусть $\alpha = [A_1, A_2, \ldots, A_s]$ – покрытие конечной группы G. Последовательности $A_i \in G^{[Z]}, i = 1,2,\ldots,s$, называются *блоками* покрытия α, вектор $r = (r_1, r_2, \ldots, r_s)$, где $r_i = |A_i|, i = 1,2,\ldots,s$, – *типом* покрытия α, а значение $\sum_{i=1}^{s} r_i$ – *длиной* покрытия. В дальнейшем будем рассматривать только такие покрытия и логарифмические сигнатуры α, для типа $r = (r_1, r_2, \ldots, r_s)$ которых выполняется $s \geq 2$ и $r_i \geq 2$, $i = 1,2,\ldots,s$.

Перейдем к рассмотрению основных отображений, связанных с покрытиями и логарифмическими сигнатурами. Пусть $\alpha = [A_1, A_2, \ldots, A_s]$ – покрытие конечной группы G, имеющее тип $r = (r_1, r_2, \ldots, r_s)$. Пусть также каждый блок покрытия α имеет вид $A_i = [a_{i1}, a_{i2}, \ldots, a_{ir_i}], i = 1,2,\ldots,s$. В дальнейшем для сокращения описания такой структуры блоков покрытия будем использовать обозначение $\alpha = (a_{ij})$. Положим

$$m_1 = 1, \quad m_i = \prod_{j=1}^{i-1} r_j, i = 2,3,\ldots,s, \quad m = \prod_{j=1}^{s} r_j.$$

Рассмотрим два отображения:

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

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

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

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

С их помощью можно определить еще одно отображение:

$$\breve{\alpha} : \mathbb{Z}_m \to G,$$
$$\breve{\alpha}(j) = \theta_\alpha(\lambda_\alpha^{-1}(j)). \quad (2)$$

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

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

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

Отметим, что в случае логарифмической сигнатуры типа $r = (r_1, r_2, \ldots, r_s)$ справедливо равенство

$$|G| = \prod_{i=1}^{s} r_i = m.$$

Это позволяет использовать логарифмические сигнатуры конечной группы G для получения подстановок на множестве $\mathbb{Z}_{|G|}$. Так, зафиксировав некоторую логарифмическую сигнатуру η группы G, можно определить следующее отображение:

$$\hat{\alpha} : \mathbb{Z}_{|G|} \to \mathbb{Z}_{|G|},$$
$$\hat{\alpha} = \breve{\eta}^{-1} \breve{\alpha} \in S_{|G|},$$

для произвольной логарифмической сигнатуры α группы G.

Введение таких структур, как покрытия и логарифмические сигнатуры, позволяет сформулировать задачу факторизации в конечной группе G. Задача факторизации заключается в нахождении элементов $g_i \in A_i, i = 1,2,\ldots,s$, соответствующих разложению (1), по известному элементу $g \in G$ и известному покрытию $\alpha = [A_1, A_2, \ldots, A_s]$ группы G. Сложность решения этой задачи зависит от выбранного покрытия. Если разложение (1) для 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 $\breve{\alpha}$ эффективно вычислимо (то есть вычислимо за полиномиальное от $\log|G|$ время) для любого значения из области определения и любого покрытия α. В то же время, обратное отображение $\breve{\alpha}^{-1}$ 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 влечет за собой 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 для достаточно большой группы G нахождение разложения

(1) случайно выбранного элемента $g \in G$ по случайно выбранному покрытию α группы G является вычислительно сложной задачей [4], [8].

III. Основные методы генерации простых логарифмических сигнатур

Рассмотрим основные виды простых логарифмических сигнатур и способы их генерации. Для этого приведем несколько конструктивных определений.

Определение 3. Пусть V_m – векторное пространство размерности m над полем F_2. Рассмотрим произвольное разбиение множества $\{1,2,\ldots,m\}$:

$$\{1,2,\ldots,m\} = K_1 \cup K_2 \cup \ldots \cup K_v,\ K_i \cap K_j = \varnothing,$$

$$\text{при } i, j \in \{1,2,\ldots,v\},\ i \neq j.$$

Пусть $|K_i| = k_i,\ i = 1,2,\ldots,v,\ \sum_{i=1}^{v} k_i = m$. Тогда набор последовательностей $\delta = [D_1, D_2, \ldots, D_v]$, где D_i содержит все различные 2^{k_i} векторов с нулевыми значениями координат на позициях, соответствующих подмножеству $\{1,2,\ldots,m\} \setminus K_i$, $i = 1,2,\ldots,v$, называется *канонической логарифмической сигнатурой* для аддитивной группы V_m.

Несложно видеть, что любая каноническая логарифмическая сигнатура является простой.

Определение 4. Пусть G – конечная группа, в которой существует цепочка подгрупп:

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

Тогда набор последовательностей $\delta = [D_1, D_2, \ldots, D_v]$, где $D_i \in G^{[\mathsf{Z}]}$ содержит по одному представителю из каждого смежного класса подгруппы G_i по подгруппе G_{i-1}, $i = 1,2,\ldots,v$, называется *трансверсальной логарифмической сигнатурой* для группы G.

Заметим, что любая каноническая логарифмическая сигнатура является трансверсальной логарифмической сигнатурой. В [1] было показано, что любая трансверсальная логарифмическая сигнатура для конечной абелевой группы является простой.

Рассмотрим следующие преобразования логарифмической сигнатуры $\delta = [D_1, D_2, \ldots, D_s]$ для конечной абелевой группы G:

- перестановка элементов в блоке D_i, $i \in \{1,2,\ldots,s\}$;
- перестановка блоков логарифмической сигнатуры δ;
- замена блока D_i на блок $D_i \cdot g = \{ag \mid a \in D_i\}$ для произвольного фиксированного $g \in G$;
- замена двух блоков D_i и D_j на один блок $D_i \cdot D_j = \{ab \mid a \in D_i, b \in D_j\}$.

Каждое из этих преобразований, примененное к логарифмической сигнатуре, снова продуцирует логарифмическую сигнатуру.

Определение 5. Пусть G – конечная абелева группа. Набор последовательностей $\tau = [T_1, T_2, \ldots, T_v]$, где $T_i \in G^{[\mathsf{Z}]}$, $i = 1,2,\ldots,v$, полученный из трансверсальной логарифмической сигнатуры для G с помощью конечного числа введенных выше преобразований логарифмической сигнатуры, называется *объединенной трансверсальной логарифмической сигнатурой* для группы G.

В [1] 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.

IV. Криптосистемы на основе логарифмических сигнатур

A. Криптосистема PGM

Криптосистема PGM (Permutation Group Mappings) была предложена Magliveras в [2]. Криптосистема представляет собой симметричную криптографическую схему шифрования. Ниже приводится описание основных этапов работы схемы PGM.

Подготовительные процедуры. Выбирается некоторая конечная группа подстановок G и ее простая фиксированная логарифмическая сигнатура η.

Генерация ключей. В качестве общего секретного ключа используется пара логарифмических сигнатур α и β группы G. Для возможности осуществления операций зашифрования и расшифрования требуется, чтобы обе эти логарифмические сигнатуры были простыми.

Процедура зашифрования. Для зашифрования сообщения $m \in \mathsf{Z}_{|G|}$ используется следующее отображение:

$$E_{\alpha,\beta} : \mathsf{Z}_{|G|} \to \mathsf{Z}_{|G\|},$$

$$E_{\alpha,\beta}(m) = \hat{\alpha}\hat{\beta}^{-1}(m) = c \in \mathsf{Z}_{|G|}.$$

Процедура расшифрования. Для расшифрования сообщения $c \in \mathsf{Z}_{|G|}$ используется обратное отображение:

$$D_{\alpha,\beta} : \mathsf{Z}_{|G|} \to \mathsf{Z}_{|G|},$$

$$D_{\alpha,\beta}(c) = E^{-1}_{\alpha,\beta}(c) = E_{\beta,\alpha}(c) = \hat{\beta}\hat{\alpha}^{-1}(c) = m \in \mathsf{Z}_{|G|}.$$

Таким образом, осуществление зашифрования и расшифрования возможно только в случае знания секретного ключа. Эффективное вычисление отображений α^{-1} и β^{-1} возможно в силу простоты логарифмических сигнатур α, β и η.

B. Криптосистема MST_1

Следующим шагом в построении криптосистем на основе логарифмических сигнатур стало появление криптосистемы MST_1 (Magliveras, Stinson, van Trung), предложенной в [3]. Криптосистема MST_1 является асимметричной криптографической схемой шифрования.

Подготовительные процедуры. Выбирается некоторая конечная группа подстановок G и ее простая фиксированная логарифмическая сигнатура η.

Генерация ключей. Генерацию ключей осуществляет участник взаимодействия, исполняющий роль принимающей стороны. В качестве открытого ключа

выступает пара логарифмических сигнатур α и β группы G. Логарифмическая сигнатура α должна быть сложной, а логарифмическая сигнатура β – простой. В качестве закрытого ключа выступает состоящая из простых логарифмических сигнатур группы G последовательность $[\theta_1, \theta_2, \ldots, \theta_k]$, такая что:

$$\hat{\alpha}\hat{\beta}^{-1} \equiv \hat{\theta}_1\hat{\theta}_2 \ldots \hat{\theta}_k .$$

Процедура зашифрования. Для зашифрования сообщения $m \in \mathsf{Z}_{|G|}$ отправляющая сторона должна использовать отображение, аналогичное рассматриваемому в криптосистеме PGM:

$$E_{\alpha,\beta}(m) = \hat{\alpha}\hat{\beta}^{-1}(m) = c \in \mathsf{Z}_{|G|} .$$

Процедура расшифрования. Для расшифрования сообщения $c \in \mathsf{Z}_{|G|}$ принимающая сторона должна использовать обратное отображение:

$$D_{\alpha,\beta}(c) = E^{-1}_{\alpha,\beta}(c) = E_{\beta,\alpha}(c) = \hat{\beta}\hat{\alpha}^{-1}(c) =$$
$$= \hat{\theta}_k^{-1}\hat{\theta}_{k-1}^{-1} \ldots \hat{\theta}_1^{-1}(c) = m \in \mathsf{Z}_{|G|} .$$

Таким образом, для осуществления зашифрования достаточно знать открытый ключ (α, β) и уметь эффективно обращать отображение $\hat{\beta}(\cdot)$, что возможно в силу простоты логарифмической сигнатуры β. В свою очередь, для осуществления расшифрования требуется знание закрытого ключа $[\theta_1, \theta_2, \ldots, \theta_k]$, позволяющее заменить трудное для вычисления отображение $\hat{\beta}\hat{\alpha}^{-1}$ (из-за сложности логарифмической сигнатуры α) на эквивалентное ему отображение $\hat{\theta}_k^{-1}\hat{\theta}_{k-1}^{-1} \ldots \hat{\theta}_1^{-1}$, являющееся эффективно вычислимым в силу простоты логарифмических сигнатур $\theta_1, \theta_2, \ldots, \theta_k$.

C. Криптосистема MST_2

Криптосистема MST_2 была предложена в [3] наряду с MST_1. Криптосистема MST_2 также является асимметричной криптографической схемой шифрования. Перед описанием этапов работы схемы рассмотрим еще одно определение, связанное с покрытиями конечных групп.

Определение 6. Покрытие $\alpha = [A_1, A_2, \ldots, A_s]$ группы G типа $(r, r, \ldots, r)$ называется $[s, r]$-*решеткой* группы G.

Подготовительные процедуры. Выбирается пара конечных групп G и H, такая что для них существует эпиморфизм $f : G \to H$.

Генерация ключей. Генерацию ключей осуществляет участник взаимодействия, исполняющий роль принимающей стороны. В качестве закрытого ключа выступает эпиморфизм f. В качестве открытого ключа выступает набор вида (G, H, α, β), где α – случайно заданная $[s, r]$-решетка группы G, $\beta = f(\alpha)$ – $[s, r]$-решетка для группы H (преобразование из α в β с помощью f производится поэлементно).

Процедура зашифрования. Для зашифрования сообщения $h \in H$ отправляющая сторона должна выбрать случайное число $R \in_R \mathsf{Z}_{r^s}$ и вычислить три элемента: $y_1 = \breve{\alpha}(R) \in G$, $y_2 = \breve{\beta}(R) \in H$ и $y_3 = hy_2 \in H$. Шифртекстом полагается пара $y = (y_1, y_3)$.

Процедура расшифрования. Для расшифрования сообщения принимающая сторона с помощью закрытого ключа должна вычислить элемент $y_2 = f(y_1)$ и получить окончательный результат путем вычисления элемента $h = y_3 y_2^{-1}$.

Стойкость криптосистемы MST_2 основывается на предположении о сложности инвертирования отображений, порожденных случайными $[s, r]$-решетками для больших конечных групп. Другими словами, считается, что отображение $\breve{\alpha}^{-1}$ не является эффективно вычислимым. При таком предположении злоумышленник, не обладающий закрытым ключом, не может восстановить значение R из величины $y_1 = \breve{\alpha}(R)$ и не может вычислить элемент $y_2 = \breve{\beta}(R)$, необходимый для восстановления сообщения h.

D. Криптосистема MST_3

1) Описание криптосистемы:

Криптосистема MST_3, предложенная в [4], также является асимметричной криптографической схемой шифрования.

Подготовительные процедуры. Выбирается конечная неабелева группа G с достаточно большим нетривиальным центром $Z = Z(G)$ и дополнительным ограничением на то, что группа G не должна раскладываться в прямое произведение $G = Z \times H$, где H – некоторая подгруппа группы G.

Генерация ключей. Генерацию ключей осуществляет участник взаимодействия, исполняющий роль принимающей стороны. Для этого ему необходимо:

- сгенерировать некоторую простую логарифмическую сигнатуру $\beta = (b_{ij})$ для центра Z группы G, имеющую тип $(r_1, r_2, \ldots, r_s)$;
- сгенерировать случайное покрытие $\alpha = (a_{ij})$ некоторого наперед неизвестного подмножества J группы G, имеющее такой же тип, что и β, и удовлетворяющее условию: $a_{ij} \in G \setminus Z$, $j = 1, 2, \ldots, r_i$, $i = 1, 2, \ldots, s$;
- выбрать элементы $t_0, t_1, \ldots, t_s \in G \setminus Z$;
- поэлементно вычислить новое покрытие $\tilde{\alpha} = (\tilde{a}_{ij})$ некоторого подмножества группы G, полученное из α при помощи элементов $t_0, t_1, \ldots, t_s$ следующим образом:
$$\tilde{a}_{ij} = t_{i-1}^{-1} a_{ij} t_i, \quad j = 1, 2, \ldots, r_i, \quad i = 1, 2, \ldots, s ; \quad (3)$$
- поэлементно вычислить новое покрытие $\gamma = (h_{ij})$ некоторого подмножества группы G, полученное из β и $\tilde{\alpha}$ следующим образом:
$$h_{ij} = b_{ij}\tilde{a}_{ij}, \quad j = 1, 2, \ldots, r_i, \quad i = 1, 2, \ldots, s ; \quad (4)$$
- установить в качестве открытого ключа пару (α, γ), а в качестве закрытого ключа – набор $(\beta, (t_0, t_1, \ldots, t_s))$.

Процедура зашифрования. Для зашифрования сообщения $x \in \mathsf{Z}_{|Z|}$ отправляющая сторона должна вычислить два элемента: $y_1 = \breve{\alpha}(x) \in G$ и $y_2 = \breve{\gamma}(x) \in G$. Шифртекстом полагается пара $y = (y_1, y_2)$.

Процедура расшифрования. Для расшифрования сообщения принимающая сторона должна воспользоваться тем, что в силу соотношений (3) и (4) для любого $x \in \mathsf{Z}_{|Z|}$ справедливо

$$\breve{\gamma}(x) = b_{1j_1}\tilde{a}_{1j_1}b_{2j_2}\tilde{a}_{2j_2}\dots b_{sj_s}\tilde{a}_{sj_s} =$$

$$= b_{1j_1}b_{2j_2}\dots b_{sj_s}\tilde{a}_{1j_1}\tilde{a}_{2j_2}\dots\tilde{a}_{sj_s} =$$

$$= b_{1j_1}b_{2j_2}\dots b_{sj_s}t_0^{-1}a_{1j_1}t_1t_1^{-1}a_{2j_2}t_2\dots t_{s-1}^{-1}a_{sj_s}t_s =$$

$$= b_{1j_1}b_{2j_2}\dots b_{sj_s}t_0^{-1}a_{1j_1}a_{2j_2}\dots a_{sj_s}t_s = \breve{\beta}(x)t_0^{-1}\breve{\alpha}(x)t_s,$$

то есть $\breve{\beta}(x) = \breve{\gamma}(x)t_s^{-1}(\breve{\alpha}(x))^{-1}t_0 = y_2t_s^{-1}y_1^{-1}t_0$. Так как логарифмическая сигнатура β является простой, то отображение $\breve{\beta}^{-1}$ является эффективно вычислимым. В результате, исходное сообщение восстанавливается как

$$x = \breve{\beta}^{-1}(y_2t_s^{-1}y_1^{-1}t_0).$$

Криптосистема MST_3 допускает вариативность при своем задании, которая заключается в возможности выбора неабелевой конечной группы G и способа генерации простой логарифмической сигнатуры β, составляющей основную часть закрытого 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 стало практиковаться и в последующих работах, посвященных изучению криптографических свойств MST_3.

2) 2-группа Судзуки:

Определение 7. *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 [5]. В частности, в [5] было показано, что для любой 2-группы Судзуки G выполнено соотношение

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

где

$Z(G) = \{z \in G \mid zg = gz, \forall g \in G\}$ – центр группы,

$\Omega_1(G) = \{g \in G \mid g^2 = 1\}$ – множество элементов второго порядка.

Кроме того, было установлено, что для любой 2-группы Судзуки G:

$$|Z(G)| = q = 2^m, m > 1,$$

при этом $|G| = q^2$ или $|G| = q^3$.

Авторы криптосистемы MST_3 предлагают использовать в качестве конечной группы 2-группу Судзуки порядка q^2. В [5] демонстрируется, что если $q = 2^m, 3 \le m \in \mathsf{N}$, и при этом поле F_q имеет нетривиальный автоморфизм θ нечетного порядка, то 2-группа Судзуки порядка q^2, обозначаемая как $A(m,\theta)$, существует. Более того, группа $A(m,\theta)$ является изоморфной мультипликативной группе матриц $G = \{S(a,b) \mid a,b \in \mathsf{F}_q\}$ вида

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

Непосредственным вычислением можно установить, 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:

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

и вид единичного элемента группы: $S(0,0)$.

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

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

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

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

и для любого элемента центра $S(0,b)$ справедливо, что

$$(S(0,b))^{-1} = S(0,b).$$

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 F_q, то есть как векторное пространство размерности m над полем 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 F_q. Совокупность данных упрощений позволяет облегчить исследование криптосистемы MST_3 и ее реализацию.

В дальнейшем при работе с элементами 2-группы Судзуки применяются следующие обозначения:

$$\forall x, y \in \mathsf{F}_q: \quad S(x,y)_{.a} = x, \quad S(x,y)_{.b} = y. \quad (10)$$

3) Примеры 2-групп Судзуки, логарифмических сигнатур для них и демонстрация основных этапов работы криптосистемы MST_3:

Зафиксируем значение $m = 3$ и рассмотрим 2-группу Судзуки G порядка $q^2 = (2^m)^2 = (2^3)^2$. Выберем конкретное представление поля $\mathsf{F}_{2^3} = \mathsf{F}_2[X]/(X^3 + X + 1)$. Для обозначения элементов

поля F_{2^3} будем использовать их векторное представление:

$$a = (a_0, a_1, a_2), \text{ где } a = a_2 X^2 + a_1 X + a_0 \in \mathsf{F}_{2^3}.$$

Зафиксируем автоморфизм θ поля F_{2^3}, имеющий нечетный порядок:

$$\forall a \in \mathsf{F}_{2^3} : \theta(a) = a^{2^2}.$$

Этот автоморфизм можно представить в виде матрицы из нулей и единиц размера 3×3:

$$\theta = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Действие автоморфизма на элемент поля при таком представлении моделируется умножением вектора-строки на матрицу.

Зафиксированные параметры m и θ однозначно задают 2-группу Судзуки $A(m,\theta)$, которую, в свою очередь, можно представить в виде группы матриц $G = \{S(a,b) \mid a,b \in \mathsf{F}_{2^3}\}$. Для элемента $S(a,b)$ будем использовать следующее обозначение

$$((a_0, a_1, a_2), (b_0, b_1, b_2)).$$

В качестве закрытого ключа рассмотрим трансверсальную логарифмическую сигнатуру β группы $Z = Z(G)$ типа $(2,2,2)$, где блоки $\beta = [B_1, B_2, B_3]$ имеют следующий вид:

$$B_1 = [((0,0,0),(0,0,0)), ((0,0,0),(1,1,0))],$$
$$B_2 = [((0,0,0),(0,0,1)), ((0,0,0),(1,1,0))],$$
$$B_3 = [((0,0,0),(1,1,0)), ((0,0,0),(0,1,1))],$$

и набор $t_0, t_1, t_2, t_3 \in G \setminus Z$:

$$t_0 = ((0,0,1),(1,1,0)), t_1 = ((1,0,0),(0,0,1)),$$
$$t_2 = ((1,1,1),(1,1,0)), t_3 = ((0,1,0),(0,0,0)).$$

Сгенерируем случайное покрытие $\alpha = [A_1, A_2, A_3]$ типа $(2,2,2)$, где

$$A_1 = [((1,0,0),(0,1,0)), ((0,0,1),(1,1,1))],$$
$$A_2 = [((0,1,1),(0,1,1)), ((0,1,1),(1,1,0))],$$
$$A_3 = [((1,0,0),(1,0,1)), ((0,1,0),(1,0,1))],$$

и с помощью β и t_0, t_1, t_2, t_3 построим по нему покрытие $\gamma = [H_1, H_2, H_3]$ типа $(2,2,2)$ согласно (3) и (4):

$$H_1 = [((0,0,1),(1,1,1)), ((1,0,0),(1,1,0))],$$
$$H_2 = [((0,0,0),(0,0,1)), ((0,0,0),(0,1,1))],$$
$$H_3 = [((0,0,1),(1,0,1)), ((1,1,1),(1,0,0))].$$

Рассмотрим процессы зашифрования и расшифрования согласно описанию криптосистемы MST_3. Выберем сообщение $x \in \mathsf{Z}_{|Z|} = \mathsf{Z}_{2^3}$, например, $x = 3$. Вычислим соответствующее значение шифртекста:

$$y_1 = \breve{\alpha}(3) =$$
$$= ((0,0,1),(1,1,1)) \cdot ((0,1,1),(1,1,0)) \cdot ((1,0,0),(1,0,1)) =$$
$$= ((1,1,0),(0,0,0)),$$
$$y_2 = \breve{\gamma}(3) =$$
$$= ((1,0,0),(1,1,0)) \cdot ((0,0,0),(0,1,1)) \cdot ((0,0,1),(1,0,1)) =$$
$$= ((1,0,1),(0,0,1)).$$

При расшифровании получаем:

$$\breve{\beta}(x) = y_2 t_3^{-1} y_1^{-1} t_0 =$$
$$= ((1,0,1),(0,0,1)) \cdot ((0,1,0),(0,0,0))^{-1} \cdot$$
$$\cdot ((1,1,0),(0,0,0))^{-1} \cdot ((0,0,1),(1,1,0)) =$$
$$= ((0,0,0),(1,1,0)).$$

Факторизуя получившийся элемент $((0,0,0),(1,1,0))$ группы Z по логарифмической сигнатуре β, имеем:

$$((0,0,0),(1,1,0)) = ((0,0,0),(1,1,0)) \cdot ((0,0,0),(1,1,0)) \cdot$$
$$\cdot ((0,0,0),(1,1,0)) = b_{12} \cdot b_{22} \cdot b_{31}.$$

В результате, восстанавливаем исходное сообщение $x \in \mathsf{Z}_{2^3}$:

$$x = \breve{\beta}^{-1}(y_2 t_3^{-1} y_1^{-1} t_0) = \lambda_\beta(\theta_\beta^{-1}(y_2 t_3^{-1} y_1^{-1} t_0)) = \lambda_\beta(1,1,0) =$$
$$= 1*1 + 1*2 + 0*4 = 3.$$

E. Криптосистема MST^*_3

Криптосистема MST^*_3, предложенная в [6], представляет собой модификацию криптосистемы MST_3.

Подготовительные процедуры. В качестве конечной неабелевой группы используется 2-группа Судзуки $G = A(m,q)$, $q = 2^m$.

Генерация ключей. Генерацию ключей осуществляет участник взаимодействия, исполняющий роль принимающей стороны. Для этого ему необходимо:

- сгенерировать некоторую простую логарифмическую сигнатуру $\beta = (b_{ij})$ для центра Z группы G, имеющую тип $(r_1, r_2, \ldots, r_s)$;
- сгенерировать случайное покрытие $\alpha = (a_{ij})$ некоторого наперед неизвестного подмножества J группы G, имеющее такой же тип, что и β, и удовлетворяющее условиям:
  - $a_{ij} \in G \setminus Z, \quad j = 1,2,\ldots,r_i, \quad i = 1,2,\ldots,s$;
  - $(a_{ij_1})_{.a} \neq (a_{ij_2})_{.a}$, для $j_1 \neq j_2$, $i = 1,2,\ldots,s$;
  - $\sum_{j=1,2,\ldots,r_i} (a_{ij})_{.a} = 0$, $i = 1,2,\ldots,s$;
- выбрать элементы $t_0, t_1, \ldots, t_s \in G \setminus Z$;
- выбрать гомоморфизм $f : G \to Z$;
- поэлементно вычислить новое покрытие $\tilde{\alpha} = (\tilde{a}_{ij})$ некоторого подмножества группы G, полученное из α при помощи элементов $t_0, t_1, \ldots, t_s$ следующим образом:
$$\tilde{a}_{ij} = t_{i-1}^{-1} a_{ij} t_i, \quad j = 1,2,\ldots,r_i, \quad i = 1,2,\ldots,s; \quad (11)$$
- поэлементно вычислить новое покрытие $\gamma = (h_{ij})$ некоторого подмножества группы G, полученное из α, β, $\tilde{\alpha}$ и f следующим образом:
$$h_{ij} = f(a_{ij}) b_{ij} \tilde{a}_{ij}, \quad j = 1,2,\ldots,r_i, \quad i = 1,2,\ldots,s; \quad (12)$$
- установить в качестве открытого ключа пару (α, γ), а в качестве закрытого ключа – набор $(\beta, (t_0, t_1, \ldots, t_s), f)$.

Процедура зашифрования. Для зашифрования сообщения $x \in Z$ отправляющая сторона должна

выбрать случайное значение $R \in_R \mathsf{Z}_{|Z|}$ и вычислить два элемента: $y_1 = \breve{\alpha}(R)x \in G$ и $y_2 = \breve{\gamma}(R)x \in G$. Шифртекстом полагается пара $y = (y_1, y_2)$.

Процедура расшифрования. Для расшифрования сообщения принимающая сторона должна воспользоваться тем, что для любого $R \in \mathsf{Z}_{|Z|}$ справедливо

$$\breve{\gamma}(R) = f(a_{1j_1})b_{1j_1}\tilde{a}_{1j_1} f(a_{2j_2})b_{2j_2}\tilde{a}_{2j_2} \dots f(a_{sj_s})b_{sj_s}\tilde{a}_{sj_s} =$$
$$= f(a_{1j_1}) f(a_{2j_2}) \dots f(a_{sj_s})b_{1j_1}b_{2j_2} \dots b_{sj_s}\tilde{a}_{1j_1}\tilde{a}_{2j_2} \dots \tilde{a}_{sj_s} =$$
$$= f(a_{1j_1}a_{2j_2} \dots a_{sj_s})b_{1j_1}b_{2j_2} \dots b_{sj_s}t_0^{-1}a_{1j_1}t_1t_1^{-1}a_{2j_2}t_2 \dots t_{s-1}^{-1}a_{sj_s}t_s =$$
$$= f(a_{1j_1}a_{2j_2} \dots a_{sj_s})b_{1j_1}b_{2j_2} \dots b_{sj_s}t_0^{-1}a_{1j_1}a_{2j_2} \dots a_{sj_s}t_s =$$
$$= f(\breve{\alpha}(R))\breve{\beta}(R)t_0^{-1}\breve{\alpha}(R)t_s,$$

то есть

$$\breve{\beta}(R) = (f(\breve{\alpha}(R)))^{-1}\breve{\gamma}(R)t_s^{-1}(\breve{\alpha}(R))^{-1}t_0 =$$
$$= f(\breve{\alpha}(R))\breve{\gamma}(R)t_s^{-1}(\breve{\alpha}(R))^{-1}t_0xx^{-1} =$$
$$= f(\breve{\alpha}(R))\breve{\gamma}(R)xt_s^{-1}(\breve{\alpha}(R)x)^{-1}t_0 =$$
$$= f(\breve{\alpha}(R)x)\breve{\gamma}(R)xt_s^{-1}(\breve{\alpha}(R)x)^{-1}t_0 = f(y_1)y_2t_s^{-1}y_1^{-1}t_0.$$

Так как логарифмическая сигнатура β является простой, то отображение $\breve{\beta}^{-1}$ является эффективно вычислимым. В результате, исходное сообщение восстанавливается как

$$R = \breve{\beta}^{-1}(f(y_1)y_2t_s^{-1}y_1^{-1}t_0),$$
$$x = (\breve{\alpha}(R))^{-1}y_1.$$

В качестве гомоморфизма $f : G \to Z$ авторы предлагают использовать отображение

$$f(S(a,b)) = S(0, a^{\sigma}),$$

где σ – автоморфизм поля F_q.

F. *Криптосистема MST**3*

Криптосистема MST**3, предложенная в [7], также представляет собой модификацию криптосистемы MST3.

Подготовительные процедуры. В качестве конечной неабелевой группы используется 2-группа Судзуки $G = A(m,q)$, $q = 2^m$.

Генерация ключей. Генерацию ключей осуществляет участник взаимодействия, исполняющий роль принимающей стороны. Для этого ему необходимо:

- сгенерировать некоторую простую логарифмическую сигнатуру $\beta = (b_{ij})$ для центра Z группы G, имеющую тип $(r_1, r_2, \dots, r_s)$;
- сгенерировать случайное покрытие $\alpha = (a_{ij})$ некоторого наперед неизвестного подмножества J группы G, имеющее такой же тип, что и β, и удовлетворяющее условию: $a_{ij} \in G \setminus Z$, $j = 1, 2, \dots, r_i$, $i = 1, 2, \dots, s$;
- выбрать элементы $t_0, t_1, \dots, t_s \in G \setminus Z$;
- выбрать гомоморфизм $f : G \to Z$, такой что $f(S(a,b)) = S(0,a)$;
- поэлементно вычислить новое покрытие $\gamma = (h_{ij})$ некоторого подмножества группы G, полученное из α, β и f следующим образом:

$$h_{ij} = t_{i-1}^{-1} f(a_{ij}) b_{ij} t_i, \quad j = 1, 2, \dots, r_i, \quad i = 1, 2, \dots, s; \quad (13)$$

- установить в качестве открытого ключа тройку (α, γ, f), а в качестве закрытого ключа – набор $(\beta, (t_0, t_1, \dots, t_s))$.

Процедура зашифрования. Для зашифрования сообщения $x \in Z$ отправляющая сторона должна выбрать случайное значение $R \in_R \mathsf{Z}_{|Z|}$ и вычислить два элемента: $y_1 = \breve{\alpha}(R)x \in G$ и $y_2 = \breve{\gamma}(R) \in G$. Шифртекстом полагается пара $y = (y_1, y_2)$.

Процедура расшифрования. Для расшифрования сообщения принимающая сторона должна воспользоваться тем, что для любого $R \in \mathsf{Z}_{|Z|}$ справедливо

$$\breve{\gamma}(R) = t_0^{-1} f(a_{1j_1})b_{1j_1} f(a_{2j_2})b_{2j_2} \dots f(a_{sj_s})b_{sj_s}t_s =$$
$$= t_0^{-1} f(a_{1j_1}) f(a_{2j_2}) \dots f(a_{sj_s})b_{1j_1}b_{2j_2} \dots b_{sj_s}t_s =$$
$$= t_0^{-1} f(a_{1j_1}a_{2j_2} \dots a_{sj_s})b_{1j_1}b_{2j_2} \dots b_{sj_s}t_s = t_0^{-1} f(\breve{\alpha}(R))\breve{\beta}(R)t_s,$$

то есть

$$\breve{\beta}(R) = (f(\breve{\alpha}(R)))^{-1}t_0\breve{\gamma}(R)t_s^{-1} = f(\breve{\alpha}(R))t_0\breve{\gamma}(R)t_s^{-1} =$$
$$= f(\breve{\alpha}(R)x)t_0\breve{\gamma}(R)t_s^{-1} = f(y_1)t_0y_2t_s^{-1}.$$

Так как логарифмическая сигнатура β является простой, то отображение $\breve{\beta}^{-1}$ является эффективно вычислимым. В результате, исходное сообщение восстанавливается как

$$R = \breve{\beta}^{-1}(f(y_1)t_0y_2t_s^{-1}),$$
$$x = (\breve{\alpha}(R))^{-1}y_1.$$

G. *Схема электронной подписи на основе MST**3*

Помимо схемы шифрования MST**3, в [7] была предложена первая схема электронной подписи, основанная на применении логарифмических сигнатур и покрытий конечных групп.

Подготовительные процедуры. В качестве конечной неабелевой группы используется 2-группа Судзуки $G = A(m,q)$, $q = 2^m$.

Генерация ключей. Генерацию ключей осуществляет участник взаимодействия, исполняющий роль подписывающего. Для этого ему необходимо:

- сгенерировать некоторую простую логарифмическую сигнатуру $\beta = (b_{ij})$ для центра Z группы G, имеющую тип $(r_1, r_2, \dots, r_s)$;
- сгенерировать случайное покрытие $\alpha = (a_{ij})$ некоторого наперед неизвестного подмножества J группы G, имеющее такой же тип, что и β, и удовлетворяющее условию: $a_{ij} \in G \setminus Z$, $j = 1, 2, \dots, r_i$, $i = 1, 2, \dots, s$;
- выбрать элементы $t_0, t_1, \dots, t_s \in G \setminus Z$;
- выбрать гомоморфизм $f : G \to Z$, такой что $f(S(a,b)) = S(0,a)$;

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

$$h_{ij} = t_{i-1}^{-1} f(a_{ij}) b_{ij} t_i, \quad j = 1,2,\ldots,r_i, \quad i = 1,2,\ldots,s; \quad (14)$$

- выбрать хэш-функцию $H : G \times G \to G$;
- установить в качестве открытого ключа набор (α, γ, f, H), а в качестве закрытого ключа – набор $(\beta, (t_0, t_1, \ldots, t_s))$.

Процедура подписи. Для подписи сообщения $x \in G$ подписывающая сторона должна выбрать случайное значение $z \in_R Z$ и вычислить элемент $r = t_0^{-1} z t_s \in G$. Затем она должна установить значения $c_1 = H(x, r)$, $c_2 = r$ и вычислить подпись (S_1, S_2), где

$$S_1 = \breve{\beta}^{-1}((f(c_1))^{-1} t_0 c_2 t_s^{-1}) \in \mathsf{Z}_{|Z|},$$

$$S_2 = (\breve{\alpha}(S_1))^{-1} c_1 \in G.$$

Процедура проверки подписи. Для проверки подписи проверяющая сторона должна вычислить $A = \breve{\alpha}(S_1) S_2$, $B = H(x, \breve{\gamma}(S_1) f(S_2))$ и, воспользовавшись тем, что

$$\breve{\gamma}(S_1) = t_0^{-1} f(\breve{\alpha}(S_1)) \breve{\beta}(S_1) t_s =$$
$$= t_0^{-1} f(\breve{\alpha}(S_1)) \breve{\beta}(\breve{\beta}^{-1}((f(c_1))^{-1} t_0 c_2 t_s^{-1})) t_s =$$
$$= t_0^{-1} f(\breve{\alpha}(S_1)) (f(c_1))^{-1} t_0 c_2 t_s^{-1} t_s =$$
$$= t_0^{-1} t_0 f(c_1^{-1}) f(\breve{\alpha}(S_1)) c_2 t_s^{-1} t_s =$$
$$= f(c_1^{-1} \breve{\alpha}(S_1)) c_2 = (f((c_1^{-1} \breve{\alpha}(S_1))^{-1}))^{-1} c_2 =$$
$$= (f((\breve{\alpha}(S_1))^{-1} c_1))^{-1} c_2 = (f(S_2))^{-1} c_2,$$

признать подпись верной в случае $A = B$ и не верной в ином случае.

H. Генератор псевдослучайных чисел MSTg

В [8] была предложена конструкция, позволяющая осуществлять генерацию псевдослучайных чисел с использованием логарифмических сигнатур и покрытий конечных групп.

Подготовительные процедуры. Выбираются две конечные группы G_1 и G_2, такие что $|G_1| = n$, $|G_2| = m$ и $n \geq m$. Выбирается случайное покрытие α группы G_1 типа $(u_1, u_2, \ldots, u_t)$, $l = \prod_{i=1}^{t} u_i$. Выбираются случайные покрытия $\alpha_1, \alpha_2, \ldots, \alpha_k$ некоторого подмножества группы G_1 типа $(r_1, r_2, \ldots, r_s)$, такого что $\prod_{i=1}^{s} r_i = |G_1|$. Выбирается случайное покрытие γ некоторого подмножества группы G_2 типа $(r_1, r_2, \ldots, r_s)$. Предполагается, что существуют эффективно вычислимые биективные отображения $f_1 : G_1 \to \mathsf{Z}_n$ и $f_2 : G_2 \to \mathsf{Z}_m$. Определяется функция $F : \mathsf{Z}_l \to \mathsf{Z}_m$, действующая следующим образом:

$$\mathsf{Z}_l \xrightarrow{\breve{\alpha}} G_1 \xrightarrow{f_1} \mathsf{Z}_n \xrightarrow{\breve{\alpha}_1} G_1 \xrightarrow{f_1} \mathsf{Z}_n \xrightarrow{\breve{\alpha}_2} \ldots$$
$$\ldots \xrightarrow{\breve{\alpha}_k} G_1 \xrightarrow{f_1} \mathsf{Z}_n \xrightarrow{\breve{\gamma}} G_2 \xrightarrow{f_2} \mathsf{Z}_m.$$

Генерация псевдослучайных чисел. Выбираются константа $C \in \mathsf{Z}_l$ и случайное секретное значение соли $s_0 \in_R \mathsf{Z}_l$. Вычисляются j псевдослучайных выходных значений $z_1, z_2, \ldots, z_j \in \mathsf{Z}_m$, такие что

$$z_i = F(s_i), \quad i = 1,2,\ldots,j,$$

где $s_i = (s_{i-1} + C) \bmod l, \quad i = 1,2,\ldots,j$.

V. Краткий обзор работ по исследованию криптосистем на основе логарифмических сигнатур и покрытий конечных групп

В данном разделе приводится обзор основных работ, посвященных исследованию криптосистем на основе логарифмических сигнатур и покрытий конечных групп. Большая часть работ по данной тематике посвящена вопросам синтеза и анализа криптосистем, а также вопросам построения логарифмических сигнатур и покрытий с заданными свойствами.

В [2] предлагается первая криптосистема, основанная на основе логарифмических сигнатур – криптосистема PGM. В [9] исследуются алгебраические свойства криптосистемы PGM. В частности, в [9] демонстрируется, что в случае использования трансверсальных логарифмических сигнатур в качестве ключа, в большинстве случаев (группы, являющиеся исключениями, выписываются явным образом), замыкание операции зашифрования PGM изоморфно симметричной группе подстановок соответствующей размерности. Помимо этого, в [9] рассматривается ряд преобразований трансверсальных логарифмических сигнатур, используемых с целью получения новых типов сигнатур, а также исследуются вопросы эквивалентности логарифмических сигнатур.

В [3] предлагаются первые асимметричные криптосистемы на основе логарифмических сигнатур – MST_1 и MST_2. Доказывается утверждение о том, что трансверсальные логарифмические сигнатуры являются простыми в случае группы подстановок. Доказывается утверждение о возможности проверки за полиномиальное время того факта, что логарифмическая сигнатура является трансверсальной. Рассматривается ряд преобразований трансверсальных логарифмических сигнатур с целью получения новых типов сигнатур и дается определение нетрансверсальных, полностью нетрансверсальных и полностью апериодических логарифмических сигнатур. В заключение рассматриваются две атаки на криптосистему MST_2.

В [10] исследуются свойства криптосистем MST_1 и MST_2. Рассматриваются вопросы построения логарифмических сигнатур минимальной длины и доказывается утверждение о достижимости нижней границы длины для разрешимых групп и симметрической группы. Отмечается, что для построения схем MST_1 и MST_2 с достаточным для практического применения уровнем стойкости необходимо использовать открытые ключи, длина которых слишком велика даже в случае задействования логарифмических сигнатур минимальной длины. Демонстрируется, что использование полностью нетрансверсальной логарифмической сигнатуры в криптосистеме MST_1 не гарантирует стойкости схемы. Также отмечается возможность восстановления секретного эпиморфизма f в криптосистеме MST_2 в случае неудачного выбора используемых конечных групп. Проблема наличия слабых ключей в криптосистеме MST_1 также рассматривается в [11].

В [4] предлагается еще одна асимметричная криптосистема на основе логарифмических сигнатур и

покрытий – MST_3. Отмечается, что в случае когда каждый элемент подмножества J покрывается покрытием α достаточно большое число раз, предположение о сложности факторизации элемента по случайному покрытию не является обязательным. Приводится две атаки на криптосистему MST_3: прямая – для определения закрытого ключа по открытому ключу, и более сложная – для определения закрытого ключа по парам «исходный текст, шифртекст».

В [12] приводится две атаки на криптосистему MST_3, основанную на 2-группе Судзуки. Первая атака предназначена для получения закрытого ключа по открытому и является более эффективной по сравнению с аналогичной атакой, предложенной в [4], устанавливая, тем самым, новую верхнюю границу стойкости схемы MST_3. Вторая атака эксплуатирует особенности конкретного используемого ключа и позволяет в случае применения в качестве ключа разновидности канонической логарифмической сигнатуры атаковать схему MST_3 со значительно большей эффективностью, чем в случае применения первой атаки.

В [13] исследуются вопросы стойкости криптосистемы MST_3. Авторы обращают внимание на замечание, данное в [4], согласно которому сложность решения задачи факторизации по случайно сгенерированному покрытию может не являться необходимым условием для получения стойкой схемы MST_3. Осуществляется ряд экспериментов, демонстрирующих, что в среднем каждый элемент подмножества J покрывается покрытием α не более 2 раз, поэтому предположение о сложности задачи факторизации по случайно сгенерированному покрытию все-таки является обязательным для построения стойкой схемы MST_3. Также приводится замечание о необходимости использования в MST_3 ключей, имеющих очень большую длину, так как существует возможность построения из сложного покрытия α простого покрытия для некоторого подмножества $I \subseteq J$ достаточно большого размера. Такое простое покрытие может быть в дальнейшем использовано для корректной факторизации элементов множества I по α.

В [14] также исследуются вопросы стойкости криптосистемы MST_3. Предлагается упрощение криптосистемы MST_3, которое может быть осуществлено без ограничения общности. Приводится первая атака, предназначенная для получения закрытого ключа по открытому и имеющая ту же сложность, что и атака, приведенная в [12], но более простое описание по сравнению с ней. Рассматривается вторая атака, возможная в случае, когда фактор-группа G/Z является абелевой группой. Рассматривается три варианта применения второй атаки в зависимости от конкретного типа логарифмической сигнатуры, используемой в качестве закрытого ключа криптосистемы MST_3 на основе 2-группы Судзуки. В [15] демонстрируется, что в двух вариантах из трех рассмотренная атака, в общем случае, может иметь достаточно большую сложность (в зависимости от используемого автоморфизма поля F_q).

В [6] предлагается модифицированная версия криптосистемы MST_3 и исследуется стойкость этой модифицированной версии. Рассматривается прямая атака на закрытый ключ и более эффективная атака, использующая особенности применяемой в качестве ключа логарифмической сигнатуры. Также исследуются вопросы производительности схемы и приводятся численные значения скорости, полученные в результате практических экспериментов.

В [7] предлагается первая схема электронной подписи, основанная на логарифмических сигнатурах и покрытиях конечных групп. Предварительно приводится еще одна модифицированная версия схемы шифрования MST_3. Обе предложенные схемы исследуются с точки зрения стойкости и эксплуатационных характеристик.

В [16], [17], [8] исследуется возможность построения генераторов псевдослучайных чисел на основе логарифмических сигнатур и покрытий конечных групп.

В качестве отдельного направления можно выделить исследования методов построения логарифмических сигнатур и покрытий с заданными свойствами. Такие исследования, как правило, преследуют следующие две цели: уменьшение длин логарифмических сигнатур известных типов и построение новых видов логарифмических сигнатур и покрытий. Вопросам построения логарифмических сигнатур минимальной длины посвящены работы [18], [19], [20], [21], [22], [23], [25], [24], [26]. Построение новых видов логарифмических сигнатур и покрытий отчасти является составляющей синтеза новых криптосистем, отчасти – самодостаточным процессом. В частности, вопросы построения апериодических логарифмических сигнатур, то есть сигнатур, не имеющих периодических блоков, являются предметом отдельных исследований и рассматриваются в [27], [28], [29].

VI. Заключение

В работе приведен обзор криптосистем на основе логарифмических сигнатур и покрытий конечных групп. Описаны основные способы генерации логарифмических сигнатур, дано определение базовых функций, связанных с этими структурами. Рассмотрены существующие криптосистемы, предназначенные для шифрования, формирования электронной подписи и генерации псевдослучайных чисел, и основанные на применении логарифмических сигнатур и покрытий. Приведено описание результатов криптоанализа этих криптосистем.

Обозреваемое направление представляется достаточно перспективным, поскольку относится к, так называемой, постквантовой криптографии. К актуальным задачам в этой области можно отнести разработку новых способов построения логарифмических сигнатур, получение более эффективных с точки зрения производительности криптосистем и построение доказуемо стойких схем.

Библиография

[1] P. Svaba, T. van Trung, P. Wolf, “Logarithmic signatures for Abelian groups and their factorization”, Tatra Mt. Math. Publ., 57:1 (2013), 21–33.

[2] S.S. Magliveras, “A cryptosystem from logarithmic signatures of finite groups”, Proceedings of the 29th Midwest Symposium on Circuits and Systems, 1986, 972–975.

[3] S.S. Magliveras, D.R. Stinson, T. van Trung, “New approaches to designing public key cryptosystems using one-way functions and trapdoors in finite groups”, Journal of cryptology, 15:4 (2002), 285–297.
[4] W. Lempken, T. van Trung, S.S. Magliveras, W. Wei, “A public key cryptosystem based on non-Abelian finite groups”, J. Cryptology, 22:1 (2009), 62–74.
[5] G. Higman, “Suzuki 2-groups”, Illinois J. Math., 7:1 (1963), 79–96.
[6] P. Svaba, T. van Trung, “Public key cryptosystem MST3: cryptanalysis and realization”, Journal of Mathematical Cryptology, 4:3 (2010), 271–315.
[7] H. Hong, J. Li, L. Wang, Y. Yang, X. Niu, “A Digital Signature Scheme Based on MST3 Cryptosystems”, Mathematical Problems in Engineering, 2014.
[8] P. Svaba, P. Marquardt, T. van Trung, “MSTg: Cryptographically strong pseudorandom number generator and its realization”, 2013.
[9] S.S. Magliveras, N.D. Memon, “Algebraic properties of cryptosystem PGM”, Journal of cryptology, 5:3 (1992), 167–183.
[10] M.I.G. Vasco, R. Steinwandt, “Obstacles in two public key cryptosystems based on group factorizations”, Tatra Mt Math. Publ., 25 (2002), 23–37.
[11] J.-M. Bohli, R. Steinwandt, M.I.G. Vasco, C. Martinez, “Weak keys in MST1”, Designs, Codes and Cryptography, 37:3 (2005), 509–524.
[12] S.S. Magliveras, P. Svaba, T. van Trung, P. Zajac, “On the security of a realization of cryptosystem MST3”, Tatra Mt. Math. Publ., 41 (2008), 65–78.
[13] M.I.G. Vasco, A.L.P. del Pozo, P.T. Duarte, “A note on the security of MST3”, Des. Codes and Cryptography, 55:2-3 (2010), 189–200.
[14] S.R. Blackburn, C. Cid, C. Mullan, “Cryptanalysis of the MST3 public key cryptosystem”, J. Math. Cryptology, 3:4 (2009), 321–338.
[15] A.S. Rybkin, “Investigation of the cryptosystem MST3 based on a Suzuki 2-group”, Discrete Mathematics and Applications, 25:3 (2015), 157–177.
[16] C. Song, M. Xu, C. Tang, “Pseudorandom generators based on subcovers for finite groups”, International Conference on Information Security and Cryptology, 2011, 379–392.
[17] P. Marquardt, P. Svaba, T. van Trung, “Pseudorandom number generators based on random covers for finite groups”, Designs, Codes and Cryptography, 64:1-2 (2012), 209–220.
[18] W. Lempken, T. van Trung, “On minimal logarithmic signatures of finite groups”, Experimental Mathematics, 14:3 (2005), 257–269.
[19] N. Singhi, N. Singhi, S.S. Magliveras, “Minimal logarithmic signatures for finite groups of Lie type”, Designs, Codes and Cryptography, 55:2-3 (2010), 243–260.
[20] N. Singhi, N. Singhi, “Minimal logarithmic signatures for classical groups”, Designs, Codes and Cryptography, 60:2 (2011), 183–195.
[21] N. Singhi, “The existence of minimal logarithmic signatures for classical groups”, 2011, 177–192.
[22] N. Singhi, “On the minimal logarithmic signature conjecture”, 2011.
[23] H. Hong, L. Wang, Y. Yang, H. Ahmad, “All exceptional groups of lie type have minimal logarithmic signatures”, Applicable Algebra in Engineering, Communication and Computing, 25:4 (2014), 287–296.
[24] H. Hong, L. Wang, Y. Yang, “Minimal logarithmic signatures for the unitary group Un(q)”, Designs, Codes and Cryptography, 77:1 (2015), 179–191.
[25] H. Hong, L. Wang, H. Ahmad, J. Li, Y. Yang, “Minimal logarithmic signatures for sporadic groups”, arXiv preprint arXiv:1507.01162, 2015.
[26] H. Hong, L. Wang, H. Ahmad, J. Shao, Y. Yang, “Minimal logarithmic signatures for one type of classical groups”, Applicable Algebra in Engineering, Communication and Computing, 28:2 (2017), 177–192.
[27] B. Baumeister, J.-H. de Wiljes, “Aperiodic logarithmic signatures”, Journal of Mathematical Cryptology, 6:1 (2012), 21–37.
[28] R. Staszewski, T. van Trung, “Strongly aperiodic logarithmic signatures”, Journal of Mathematical Cryptology, 7:2 (2013), 147–179.
[29] T. van Trung, “Construction of strongly aperiodic logarithmic signatures”, Journal of Mathematical Cryptology, 12:1 (2018), 23–35.

Cryptosystems based on logarithmic signatures and covers of finite groups

Eduard Primenko, Andrey Rybkin

***Abstract* – In this paper, we survey a cryptographic direction of post-quantum cryptography based on logarithmic signatures and covers of finite groups. These mathematical structures allows designing cryptosystems with security based on hardness of the factorization problem in finite group. This problem is assumed computationally hard even in post-quantum era.**

We give basic definitions and functions related to logarithmic signatures and covers of finite groups. Relations between these functions and the factorization problem in finite group are explained. We describe some logarithmic signatures generation methods and consider the hardness of the factorization problem in each case.

We give a description of the existing cryptosystems based on logarithmic signatures and covers of finite groups in chronological order. These cryptographic systems applicable for such purposes as data ciphering, digital signing or pseudo random number generation. We mainly focus on cryptosystem MST3 that is the most perspective ciphering system in the direction. Description of Suzuki 2-groups traditionally used as a finite group in cryptographic system MST3 is given. A toy example of MST3 based on Suzuki 2-group is demonstrated. We also consider the main analysis results of existing cryptosystems based on logarithmic signatures and covers of finite groups.

***Keywords* – post-quantum cryptography, logarithmic signatures, covers, finite groups, Suzuki 2-group, MST.**

REFERENCES

[1] P. Svaba, T. van Trung, P. Wolf, “Logarithmic signatures for Abelian groups and their factorization”, Tatra Mt. Math. Publ., 57:1 (2013), 21–33.

[2] S.S. Magliveras, “A cryptosystem from logarithmic signatures of finite groups”, Proceedings of the 29th Midwest Symposium on Circuits and Systems, 1986, 972–975.

[3] S.S. Magliveras, D.R. Stinson, T. van Trung, “New approaches to designing public key cryptosystems using one-way functions and trapdoors in finite groups”, Journal of cryptology, 15:4 (2002), 285–297.

[4] W. Lempken, T. van Trung, S.S. Magliveras, W. Wei, “A public key cryptosystem based on non-Abelian finite groups”, J. Cryptology, 22:1 (2009), 62–74.

[5] G. Higman, “Suzuki 2-groups”, Illinois J. Math., 7:1 (1963), 79–96.

[6] P. Svaba, T. van Trung, “Public key cryptosystem MST3: cryptanalysis and realization”, Journal of Mathematical Cryptology, 4:3 (2010), 271–315.

[7] H. Hong, J. Li, L. Wang, Y. Yang, X. Niu, “A Digital Signature Scheme Based on MST3 Cryptosystems”, Mathematical Problems in Engineering, 2014.

[8] P. Svaba, P. Marquardt, T. van Trung, “MSTg: Cryptographically strong pseudorandom number generator and its realization”, 2013.

[9] S.S. Magliveras, N.D. Memon, “Algebraic properties of cryptosystem PGM”, Journal of cryptology, 5:3 (1992), 167–183.

[10] M.I.G. Vasco, R. Steinwandt, “Obstacles in two public key cryptosystems based on group factorizations”, Tatra Mt Math. Publ., 25 (2002), 23–37.

[11] J.-M. Bohli, R. Steinwandt, M.I.G. Vasco, C. Martinez, “Weak keys in MST1”, Designs, Codes and Cryptography, 37:3 (2005), 509–524.

[12] S.S. Magliveras, P. Svaba, T. van Trung, P. Zajac, “On the security of a realization of cryptosystem MST3”, Tatra Mt. Math. Publ., 41 (2008), 65–78.

[13] M.I.G. Vasco, A.L.P. del Pozo, P.T. Duarte, “A note on the security of MST3”, Des. Codes and Cryptography, 55:2-3 (2010), 189–200.

[14] S.R. Blackburn, C. Cid, C. Mullan, “Cryptanalysis of the MST3 public key cryptosystem”, J. Math. Cryptology, 3:4 (2009), 321–338.

[15] A.S. Rybkin, “Investigation of the cryptosystem MST3 based on a Suzuki 2-group”, Discrete Mathematics and Applications, 25:3 (2015), 157–177.

[16] C. Song, M. Xu, C. Tang, “Pseudorandom generators based on subcovers for finite groups”, International Conference on Information Security and Cryptology, 2011, 379–392.

[17] P. Marquardt, P. Svaba, T. van Trung, “Pseudorandom number generators based on random covers for finite groups”, Designs, Codes and Cryptography, 64:1-2 (2012), 209–220.

[18] W. Lempken, T. van Trung, “On minimal logarithmic signatures of finite groups”, Experimental Mathematics, 14:3 (2005), 257–269.

[19] N. Singhi, N. Singhi, S.S. Magliveras, “Minimal logarithmic signatures for finite groups of Lie type”, Designs, Codes and Cryptography, 55:2-3 (2010), 243–260.
[20] N. Singhi, N. Singhi, “Minimal logarithmic signatures for classical groups”, Designs, Codes and Cryptography, 60:2 (2011), 183–195.
[21] N. Singhi, “The existence of minimal logarithmic signatures for classical groups”, 2011, 177–192.
[22] N. Singhi, “On the minimal logarithmic signature conjecture”, 2011.
[23] H. Hong, L. Wang, Y. Yang, H. Ahmad, “All exceptional groups of lie type have minimal logarithmic signatures”, Applicable Algebra in Engineering, Communication and Computing, 25:4 (2014), 287–296.
[24] H. Hong, L. Wang, Y. Yang, “Minimal logarithmic signatures for the unitary group Un(q)”, Designs, Codes and Cryptography, 77:1 (2015), 179–191.
[25] H. Hong, L. Wang, H. Ahmad, J. Li, Y. Yang, “Minimal logarithmic signatures for sporadic groups”, arXiv preprint arXiv:1507.01162, 2015.
[26] H. Hong, L. Wang, H. Ahmad, J. Shao, Y. Yang, “Minimal logarithmic signatures for one type of classical groups”, Applicable Algebra in Engineering, Communication and Computing, 28:2 (2017), 177–192.
[27] B. Baumeister, J.-H. de Wiljes, “Aperiodic logarithmic signatures”, Journal of Mathematical Cryptology, 6:1 (2012), 21–37.
[28] R. Staszewski, T. van Trung, “Strongly aperiodic logarithmic signatures”, Journal of Mathematical Cryptology, 7:2 (2013), 147–179.
[29] T. van Trung, “Construction of strongly aperiodic logarithmic signatures”, Journal of Mathematical Cryptology, 12:1 (2018), 23–35.