Неассоциативные алгебраические структуры в криптографии и кодировании*

В. Т. МАРКОВ, А. В. МИХАЛЁВ, А. А. НЕЧАЕВ
Московский государственный университет им. М. В. Ломоносова
e-mail: vtmarkov@yandex.ru

УДК 512.552.7+512.554+512.548.2+512.548.77+519.72

Ключевые слова: неассоциативные алгебраические структуры, групповая алгебра, квазигрупповое кольцо, лупа Муфанг, криптосхема, линейно оптимальный код.

Аннотация

В обзоре рассматриваются приложения неассоциативных алгебраических структур для построения линейно оптимальных кодов и криптосхем.

Abstract

V. T. Markov, A. V. Mikhalev, A. A. Nechaev, Nonassociative algebraic structures in cryptography and coding, Fundamentalnaya i prikladnaya matematika, vol. 21 (2016), no. 4, pp. 99—123.

In this review, we consider applications of nonassociative algebraic structures for the construction of linearly optimal codes and cryptosystems.

В данном обзоре рассмотрены приложения неассоциативных алгебраических структур для построения линейно оптимальных кодов и криптосхем.

Во введении приведены основные понятия и утверждения, необходимые для дальнейшего изложения.

Во разделе 2 описано построение двух семейств линейно оптимальных $[n, n-3, 3]_q$-кодов для $n = 2q$ и $n = 2q-2$ с помощью квазигрупповых колец. Для построения $[2q, 2q-3, 3]_q$-кодов используется представление кодов Рида—Соломона как идеалов группового кольца $\mathbb{F}_{p^n}G$, где G — это p-элементарная абелева группа порядка p^n. Определяются коммутаторные квазигруппы и приводятся линейно оптимальные коды, построенные с помощью коммутаторных квазигрупп для группы диэдра D_n.

В разделе 3 построена криптосхема над градуированным кольцом с мультипликативным базисом как обобщение криптосхемы над групповым кольцом.

*Обзор написан по материалам доклада на конференции CTCrypt 2014, прошедшей 5–6 июня 2014 г. в Москве. Окончательный вариант статьи был сдан в печать в сентябре 2017 года. Работа А. В. Михалёва и В. Т. Маркова была поддержана грантом РФФИ 17-01-00895.

При этом неоднозначность выбора градуировки и мультипликативного базиса расширяет множество подходящих алгебраических структур для шифрования.

В разделе 4 построен протокол выработки общего секретного ключа и сконструирована криптосхема, где все вычисления проводятся в лупе Муфанг.

В разделе 5 вводится понятие группоида с перестановочными степенями (ПС-группоида), описывается протокол выработки общего секретного ключа, аналогичный алгоритму Диффи—Хеллмана, основанный на ПС-группоидах, а также указаны некоторые конструкции ПС-группоидов.

1. Введение

Определение 1.1. *Группоид* — непустое множество с заданной бинарной операцией.

Пусть $(G,\cdot)$ — группоид и a — некоторый элемент из G. Рассмотрим отображения $L(a)\colon G\to G$, $R(a)\colon G\to G$ для любого $a\in G$, определённые следующим образом: $xL(a)=x\cdot a$, $xR(a)=a\cdot x$ для любого $x\in G$.

Определение 1.2. *Квазигруппа* — такой группоид $(G,\cdot)$, что отображения $L(a)$, $R(a)$ являются биекциями для любого $a\in G$.

Определение 1.3. Группоид $(G,\cdot)$ называется *лупой*, если $(G,\cdot)$ — квазигруппа с единицей.

Определение 1.4. Лупа $(L,\cdot)$ с единичным элементом 1 называется *лупой Муфанг*, если выполняется тождество

$$(xy)(zx)=[x(yz)]x$$

для любых $x,y,z\in L$.

Хорошо известна следующая теорема.

Теорема 1.1 [14]. *Пусть $(L,\cdot)$ — лупа Муфанг. Если для $x,y,z\in L$ выполняется $x(yz)=(xy)z$, то x, y, z порождают подгруппу в L.*

Следствие 1.1. *Любая лупа Муфанг $(M,\cdot)$ является диассоциативной, т. е. любые два элемента порождают подгруппу в M.*

Следствие 1.2. *Любая лупа Муфанг $(M,\cdot)$ является лупой с ассоциативными степенями.*

Определение 1.5. Пусть K — ассоциативное кольцо с единицей, L — лупа или квазигруппа. Рассмотрим множество KL, состоящее из всех формальных сумм вида

$$\sum_{l\in L}\alpha_l\cdot l\quad(\alpha_l\in K),$$

в которых конечное число элементов α_l отлично от нуля. Два элемента $a,b\in KL$ считаются равными тогда и только тогда, когда $\alpha_l=\beta_l$ для всех $l\in L$.

На множестве KL определены операции сложения и умножения: если

$$a = \sum_{l \in L} \alpha_l \cdot l, \quad b = \sum_{l \in L} \beta_l \cdot l -$$

элементы KL, то

$$a + b = \sum_{l \in L} (\alpha_l + \beta_l) \cdot l, \quad ab = \sum_{l \in L} \Bigg(\sum_{m,h \in L \colon mh = l} \alpha_m \beta_h \Bigg) l.$$

Относительно этих операций множество KL является неассоциативным кольцом с единицей. Удобно отождествить $l \in L$ с элементом $1 \cdot l \in KL$, а $\alpha \in K$ с элементом $\alpha \cdot e$, где e — единица лупы. Тогда K и L являются подмножествами в KL.

Пусть теперь R — ассоциативное кольцо с единицей $1 \in R$. Рассмотрим группу G в мультипликативной записи с нейтральным элементом $e \in G$.

Определение 1.6. Кольцо R называется *G-градуированным*, если существует такое семейство $\{R_\sigma,\ \sigma \in G\}$ аддитивных подгрупп R_σ аддитивной группы R, что

$$R = \bigoplus_{\sigma \in G} R_\sigma, \quad R_\sigma R_\tau \subseteq R_{\sigma\tau} \ \text{ для всех } \ \sigma, \tau \in G.$$

Строго градуированным называется G-градуированное кольцо R, для которого выполнено равенство $R_\sigma R_\tau = R_{\sigma\tau}$ для всех $\sigma, \tau \in G$. Элемент $x \in R_\sigma$ называется *однородным степени* σ.

Будем обозначать множество обратимых по умножению элементов в кольце R через $U(R)$.

Пусть R — конечномерная некоммутативная алгебра над полем $\mathbb{F}$.

Определение 1.7. *Мультипликативным базисом* конечномерной алгебры R называется такой её базис B, что $B \cup \{0\}$ замкнуто относительно умножения.

Пример. Для алгебры $(n \times n)$-матриц $M_n(\mathbb{F})$ подмножество над полем F естественным мультипликативным базисом является стандартный базис, состоящий из матричных единиц E_{ij}, у которых на позиции ij стоит 1, а остальные элементы — нули.

Пример. Для любой конечномерной (полу)групповой алгебры $\mathbb{F}G$ моноида G в качестве мультипликативного базиса можно выбрать моноид G.

2. Линейно оптимальные коды в квазигрупповых кольцах

Определение 2.1. Линейный $[n, k, d]_q$-код называется *линейно оптимальным*, если k — максимально возможная размерность линейного над полем $\Omega = \mathbb{F}_q$ кода длины n с расстоянием d.

Очевидно, что любой МДР-код оптимален. Более того, можно указать следующий признак линейной оптимальности.

Обозначим через $n(k,q)$ ($m(k,q)$) максимальную длину МДР-кода комбинаторной размерности k над алфавитом из q элементов (соответственно линейного МДР-кода над полем $\mathbb{F}_q$ для примарного числа q). Ясно, что

$$m(k,q) \leqslant n(k,q).$$

Предложение 2.1. *Пусть n, k — натуральные числа, q — такое примарное число, что $n > m(k+1,q)$. Тогда любой линейный $[n, n-k, k]_q$-код линейно оптимален.*

Одним из способов получения линейных над полем $\mathbb{F}_q$ кодов с экстремальными свойствами является следующая конструкция. Для конечной лупы $L = \{l_1, \ldots, l_n\}$ сформируем луповую алгебру $A = \mathbb{F}_q L$ и для каждого левого идеала $I \leqslant {}_A A$ определим код $\mathcal{C} = \mathcal{C}(I)$ как набор всех слов $(\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_q^n$, таких что $\sum \alpha_i l_i \in I$. Такие коды называются луповыми [1]. Каждая луповая алгебра (и даже квазигрупповая алгебра) содержит два *тривиальных МДР-кода*: $[n,1,n]$-код $\mathcal{C}(I_0)$, соответствующий левому идеалу

$$\mathbb{F}_q\Big(\sum_{l\in L} l\Big),$$

и $[n, n-1, 2]$-код $\mathcal{C}(\Delta)$, соответствующий фундаментальному идеалу

$$\Delta(A) = \Big\{ \sum_{l\in L} \alpha(l) l \colon \sum_{l\in L} \alpha(l) = 0 \Big\},$$

который является левым и правым аннулятором идеала I_0.

В [7] строятся цепочки линейных $[n, n-3, 3]_q$-кодов над $\mathbb{F}_q$ для $n = 2q$ и $n = 2q-2$. Эти коды являются линейно оптимальными, что следует из предложения 2.1, а также из того, что $n(k,q) = k+1$ при $q \leqslant k$ (см. [6, 11]).

Заметим, что линейный $[n, n-3, 3]_q$-код над $\mathbb{F}_q$ может быть легко построен с помощью укорочения $[N, N-3, 3]_q$-кода Хемминга [9, 10], где $N = q^2 + q + 1$. Основной результат заключается в построении таких кодов как луповых кодов.

2.1. $[2q, 2q-3, 3]_q$-линейно оптимальные коды

Как и выше, p — простое число, $q = p^n > 2$ и $P = \mathbb{F}_q$.

Сформулируем основной результат этого раздела.

Теорема 2.1 [7]. *Пусть L — лупа порядка $2q$, содержащая p-элементарную абелеву группу H порядка q. Пусть также существует элемент $b \in L \setminus H$, обладающий следующими свойствами*:

1) *найдётся $\dot{k} \in \{1, \ldots, p-1\}$, такое что для любого элемента $l \in L \setminus H$ найдётся элемент $\dot{h}_l \in H$, такой что для любого элемента $h \in H$ выполнено $lh = b(\dot{h}_l h^{\dot{k}})$;*

2) *найдётся* $\ddot{k} \in \{1, \ldots, p-1\}$, *такое что для любого элемента* $l \in L \setminus H$ *найдётся элемент* $\ddot{h_l} \in H$, *такой что для любого элемента* $h \in H$ *выполнено* $l(bh) = \ddot{h_l} h^{\ddot{k}}$;
3) *для любого элемента* $\alpha \in H$ *найдётся элемент* $h_\alpha \in H$, *такой что для любого элемента* $h \in H$ *выполнено* $\alpha(bh) = b(h_\alpha h)$.

Тогда если степень расширения n *чётная или если* $P = \mathbb{F}_p$ *и*

$$\text{найдётся} \quad k \in P, \quad \textit{такое что} \quad k^2 = \dot{k}^{-1}\ddot{k}, \tag{2.1}$$

то в решётке левых идеалов PL *содержится структура, изображённая на рис.* 1. *Выделенные на рис.* 1 *идеалы соответствуют* $[2q, 2q-3, 3]_q$*-линейно оптимальным кодам.*

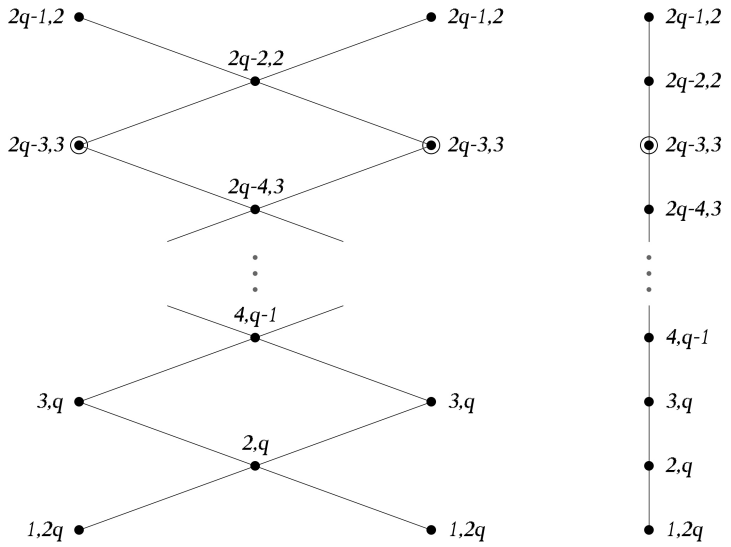

Рис. 1. Решётка идеалов PL при $\operatorname{char} P \neq 2$ (слева) и при $\operatorname{char} P = 2$ (справа). Каждый круг обозначает левый идеал PL, а k, d — сопровождающие числа, где k обозначает размерность, d — расстояние соответствующего кода. Любые два идеала соединены линией тогда и только тогда, когда нижний содержится в верхнем.

Замечание. Если существует элемент $b \in L \setminus H$, удовлетворяющий условию теоремы 2.1, то и любой другой элемент из $L \setminus H$ тоже удовлетворяет этому условию.

2.2. $[2q-2, 2q-5, 3]_q$-линейно оптимальные коды

Сохраним обозначения $P = \mathbb{F}_q$, $q = p^n$.

Теорема 2.2 [7]. *Пусть L — лупа порядка $2q-2$, содержащая циклическую абелеву группу H порядка $q-1$. Пусть также существует элемент $b \in L \setminus H$, обладающий следующими тремя свойствами*:

1) *для любого элемента $l \in L \setminus H$ найдётся элемент $\dot{h}_l \in H$, такой что для любого элемента $h \in H$ выполнено $lh = b(\dot{h}_l h)$;*
2) *для любого элемента $l \in L \setminus H$ найдётся элемент $\ddot{h}_l \in H$, такой что для любого элемента $h \in H$ выполнено $l(bh) = \ddot{h}_l h$;*
3) *для любого элемента $\alpha \in H$ найдётся элемент $h_\alpha \in H$, такой что для любого элемента $h \in H$ выполнено $\alpha(bh) = h_\alpha h$.*

Тогда если $\operatorname{char} P \neq 2$, *то в решётке левых идеалов PL содержится $\varphi(q-1)$ (φ — функция Эйлера) структур следующего вида* (*все идеалы, участвующие в структурах, попарно различны*):

$$\mathcal{L}_i \subseteq \mathcal{M}_i^-, \mathcal{M}_i^+ \subseteq \mathcal{N}_i, \quad i \in \overline{1, q-1}, \tag{2.2}$$

причём $\mathcal{C}(\mathcal{M}_i^\pm)$ являются $[2q-5, 2q-3, 3]_q$-линейно оптимальными кодами.

Если $\operatorname{char} P = 2$, *то в решётке левых идеалов PL содержится $\varphi(q-1)$ цепочек следующего вида* (*все идеалы, участвующие в цепочках, попарно различны*):

$$\mathcal{L}_i \subseteq \mathcal{M}_i \subseteq \mathcal{N}_i, \quad i \in \overline{1, q-1}, \tag{2.3}$$

причём $\mathcal{C}(\mathcal{M}_i)$ являются $[2q-5, 2q-3, 3]_q$-линейно оптимальными кодами.

2.3. Коммутаторные квазигруппы

Определение 2.2. Пусть G — конечная группа. Зафиксируем целые числа c, d и определим новое умножение на элементах G по следующему правилу:

$$x *_{c,d} y = x^{1-d} y^c x^d y^{1-c} = x[x^{-d}, y^c]y, \quad x, y \in G.$$

Получившийся группоид обозначается $(G)_{c,d}$ и называется коммутаторным группоидом (или коммутаторной квазигруппой, если он удовлетворяет определению 1.2) для группы G с параметрами c, d.

Предложение 2.2 [7]. *Обозначим через e единичный элемент G, через $Z(G)$ — центр группы, $m = \exp\big(G/Z(G)\big)$.*

1. *Если группа G удовлетворяет тождеству $[x^c, y^{d-1}] = e$ ($[x^{c-1}, y^d] = e$), то операции в $(G)_{c,d}$ и $(G)_{c,1}$ (соответственно в $(G)_{c,d}$ и $(G)_{1,d}$) совпадают.*
2. *$(G)_{0,d} = (G)_{c,0} = G$ для всех $c, d \in \mathbb{Z}$.*
3. *$(G)_{1,1} = G^{\mathrm{op}}$, где G^{op} — инверсная группа.*
4. *$(G)_{c,d} \cong (G)_{c,d}^{\mathrm{op}}$ для всех $c, d \in \mathbb{Z}$.*
5. *Если $[x, y] = e$ в G, то $x * y = xy$.*
6. *Если $u \equiv c \pmod m$, $v \equiv d \pmod m$, то $(G)_{u,v} = (G)_{c,d}$.*
7. *Пусть $m_1, \ldots, m_k$ — список всех различных порядков элементов группы G. Если $c \equiv i_k \pmod{m_k}$, $d \equiv j_k \pmod{m_k}$, где $i_k, j_k \in \{0, 1\}$, то группоид $G_{c,d}$ — лупа.*

Пункт 6 показывает, что количество неизоморфных группоидов в множестве $(G)_{c,d}$, $c, d \in \mathbb{Z}$, есть мера некоммутативности группы G.

Группоид $(G)_{c,d}$ всегда содержит единичный элемент, но не всегда является лупой. В общем случае мы не знаем условий на G, c, d, которые гарантируют, что $(G)_{c,d}$ является лупой, но для групп $G = D_n$, где D_n — группа диэдра, ответ даёт следующее предложение.

Предложение 2.3 [7]. *Следующая таблица показывает, при каких c и d группоид $(D_n)_{c,d}$ является лупой* («+» — *лупа*, «−» — *не лупа*):

$c \diagdown d$	ч, $2d-1 \in \mathbb{Z}_n^*$	ч, $2d-1 \notin \mathbb{Z}_n^*$	н, $2d-1 \in \mathbb{Z}_n^*$	н, $2d-1 \notin \mathbb{Z}_n^*$
ч, $2c-1 \in \mathbb{Z}_n^*$	+	+	+	+
ч, $2c-1 \notin \mathbb{Z}_n^*$	+	+	−	−
н, $2c-1 \in \mathbb{Z}_n^*$	+	−	+	−
н, $2c-1 \notin \mathbb{Z}_n^*$	+	−	−	−

Предложение 2.4 [7]. *Если $c, d \in \{1, \ldots, \exp(D_n/Z(D_n)) - 1\}$, то $(D_n)_{c,d}$ — полугруппа тогда и только тогда, когда $c = d = 1$ (в этом случае $(D_n)_{c,d} = (D_n)^{\mathrm{op}} \cong D_n$) или когда c и d чётные (в этом случае $(D_n)_{c,d} = D_n$).*

Предложение 2.5. *При различных парах $c, d \in \{1, \ldots, \exp(D_n/Z(D_n)) - 1\}$, таких что c и d нечётные и $2c-1, 2d-1 \in \mathbb{Z}_n^*$, соответствующие им лупы $(D_n)_{c,d}$ неизоморфны.*

Следующая лемма показывает, при каких значениях c и d группоид $(D_n)_{c,d}$ удовлетворяет условиям теорем 2.1 и 2.2.

Лемма 2.1. *Пусть группоид $(D_n)_{c,d}$ является неассоциативной лупой и n — простое число. Тогда эта лупа удовлетворяет условиям* 1)—3) *из теоремы* 2.1.

Пусть группоид $(D_n)_{c,d} = (D_{p^l-1})_{c,d}$ является неассоциативной лупой и $n = p^l - 1$. Эта лупа удовлетворяет условиям 1)—3) *из теоремы* 2.2 *тогда и только тогда, когда*

- *c нечётное, d нечётное, $2c \equiv 2 \pmod{n}$;*
- *c чётное, d нечётное $2c \equiv 0 \pmod{n}$;*
- *c нечётное, d чётное.*

Пусть $p > 2$ — простое число, $P = \mathbb{F}_p$.

Теорема 2.3 [7]. *Пусть $(D_p)_{c,d}$ — неассоциативная лупа и выполнено одно из следующих условий*:

- *c нечётное, d нечётное, найдётся $x \in \mathbb{Z}$, такое что $x^2 \equiv 2c - 1 \pmod{p}$;*
- *c чётное, d нечётное, найдётся $x \in \mathbb{Z}$, такое что $x^2 \equiv 1 - 2c \pmod{p}$;*
- *c нечётное, d чётное.*

Тогда луповая алгебра $P(D_p)_{c,d}$ содержит по крайней мере два идеала, отвечающих линейно оптимальным $[2p, 2p-3, 3]_p$-кодам.

В заключение заметим, что существуют лупы с неассоциативными степенями (а значит, не являющиеся коммутаторными квазигруппами), удовлетворяющие условиям теоремы 2.1 или теоремы 2.2. Такие лупы можно построить с помощью следующей конструкции [7] (мы рассматриваем теорему 2.1, для теоремы 2.2 рассуждения аналогичны). Пусть

$$H = \{e, h_1, \ldots, h_{q-1}\} = Z_p^l, \quad q = p^l,$$

и

$$L = \{e, h_1, \ldots, h_{q-1}, b, \ldots, bh_{q-1}\} -$$

расширение H, умножение $*$ в котором определено следующим образом:

$$\begin{gathered} h_i * h_j = h_i h_j, \\ b * h_i = bh_j, \quad be = e, \\ bh_i * h_j = b * (h_i h_j), \\ bh_i * bh_j = \sigma(h_i) h_j, \\ h_i * bh_j = b * (\tau(h_i) h_j), \end{gathered}$$

где σ, τ — произвольные перестановки на множестве H. При таком определении группоид $(L, *)$ будет квазигруппой, а если добавить условие $\tau(e) = e$, то он будет лупой, которая очевидно удовлетворяет теореме 2.1. Рассмотрим $(b * b) * b$ и $b * (b * b)$:

$$\begin{gathered} (b * b) * b = \sigma(e) * b = b * \Big(\tau\big(\sigma(e)\big)\Big), \\ b * (b * b) = b * \sigma(e). \end{gathered}$$

Если $\sigma(e) \neq e$ и $\tau\big(\sigma(e)\big) \neq \sigma(e)$, то $(b * b) * b \neq b * (b * b)$, и лупа L будет лупой с неассоциативными степенями. Кроме того, поскольку $\dot{k} = \ddot{k} = 1$, в $\mathbb{F}_q L$ содержится идеал, отвечающий линейно оптимальному $[2q, 2q-3, 3]_q$-коду.

Интересно, что при $q = 3$ существуют четыре неассоциативные неизоморфные лупы, удовлетворяющие теореме 2.1. Они удовлетворяют и теореме 2.2, а следовательно, доставляют линейно оптимальные $[6, 3, 3]_3$- и $[6, 3, 3]_4$-коды. Согласно [1] этими четырьмя лупами исчерпываются все неассоциативные лупы порядка 6, доставляющие линейно оптимальные коды. Лишь одна из этих луп, а именно $(D_3)_{1,3}$, является коммутаторной квазигруппой.

3. Криптосхемы над градуированными кольцами с мультипликативным базисом

3.1. Конструирование автоморфизмов градуированного кольца

В [3] рассматривались автоморфизмы лупового кольца KL. Из автоморфизмов $\varphi \in \mathrm{Aut}(K)$ и $\psi \in \mathrm{Aut}(L)$ конструировался $\chi \in \mathrm{Aut}(KL)$ по следующему

правилу: для любого

$$h = a_{l_1} l_1 + \ldots + a_{l_n} l_n, \quad h \in KL,$$

по определению полагалось, что

$$\chi(h) = \varphi(a_{l_1})\psi(l_1) + \ldots + \varphi(a_{l_n})\psi(l_n).$$

Таким образом, если нам известна структура групп автоморфизмов $\mathrm{Aut}(K)$ и $\mathrm{Aut}(L)$ по отдельности, то мы получаем возможность строить достаточно много автоморфизмов из $\mathrm{Aut}(KL)$. Заметим, что даже для произвольного группового кольца полного описания его группы автоморфизмов ещё не получено.

Пусть теперь R — кольцо, градуированное конечной группой G. Предположим, что у кольца R существует мультипликативный базис B над R_e. Фиксируя $\varphi \in \mathrm{Aut}(R_e)$ и $\psi \in \mathrm{Aut}(B)$, получаем естественное продолжение автоморфизма φ до автоморфизма χ всего кольца R. Этот автоморфизм будет перемешивать сам мультипликативный базис.

Даже для (полу)группового кольца, меняя градуировку или выбирая другой мультипликативный базис, мы получаем, вообще говоря, уже новые структуры для шифрования со своими автоморфизмами. Это расширяет множество подходящих для криптосхемы структур.

3.2. Построение криптосхемы (см. [3])

Участник А.

1. Участник А выбирает градуированное кольцо R с мультипликативным базисом, такое что группы автоморфизмов $\mathrm{Aut}(B)$ и $\mathrm{Aut}(R_e)$ некоммутативны. Предполагается, что группы $\mathrm{Aut}(B)$ и $\mathrm{Aut}(R_e)$ достаточно богаты некоммутирующими элементами большого порядка с нетривиальными централизаторами большого порядка. Положим $|\mathrm{Aut}(B)| \geqslant t_1$, $|\mathrm{Aut}(R_e)| \geqslant t_2$. Здесь и далее t_i — параметры безопасности, которые по предположению экспоненциально зависят от порядка градуированного кольца R. Участник А фиксирует градуировку и этот базис (если кольцо допускает несколько различных базисов) с учётом вышеперечисленных условий. Эта информация объявляется по открытому каналу. Обозначим базис через B, а группу, по которой градуировано кольцо, — через G, тогда общеизвестны (R, B, G).
2. Участник А задаёт автоморфизм $\sigma \in \mathrm{Aut}(R_e)$ так, чтобы $|\sigma| \geqslant t_3$, причём σ должен иметь нетривиальный централизатор и $|C(\sigma) \setminus \langle\sigma\rangle| \geqslant t_4$. Участник А конструирует автоморфизм $\eta \in \mathrm{Aut}(B)$ так, чтобы $|\eta| \geqslant t_5$, причём η должен иметь нетривиальный централизатор и $|C(\eta) \setminus \langle\eta\rangle| \geqslant t_6$.
3. Участник А случайно выбирает автоморфизм $\tau \in C(\sigma) \setminus \langle\sigma\rangle$.
4. Участник А случайно выбирает $\omega \in C(\eta) \setminus \langle\eta\rangle$.
5. По τ и ω участник А строит секретный автоморфизм $\varphi \in \mathrm{Aut}(R)$: для любого $h \in R$ вида

$$h = a_{b_1} b_1 + \ldots + a_{b_n} b_n,$$

где $B = \{b_1, \ldots, b_n\}$, $a_{b_1}, \ldots, a_{b_n} \in R_e$, полагает

$$\varphi(h) = \tau(a_{b_1})\omega(b_1) + \ldots + \tau(a_{b_n})\omega(b_n).$$

6. Участник A выбирает элементы $a \in R$, $x \in R$ с нулевыми левыми аннуляторами. Это условие будет необходимо для последующей расшифровки.
7. Участник A вычисляет $\varphi(x)$ и $\varphi(a)$.

Таким образом, открытым ключом участника A является

$$\big(\sigma, \eta, x, \varphi(x), a, \varphi(a)\big).$$

Отметим, что при должных параметрах безопасности t_3, t_4, t_5, t_6 автоморфизмов, подходящих для открытого ключа, достаточно много. Сформированный открытый ключ участник A передаёт участнику B по открытому каналу.

Участник B.

1. Участник B выбирает натуральные числа (i, j, k, l).
2. Используя открытый ключ участника A, участник B получает пары автоморфизмов (σ^i, η^j), (σ^k, η^l) и по ним строит автоморфизмы $\psi, \chi \in \mathrm{Aut}(KL)$ таким же способом, как и участник A, т. е. для любого $h \in KL$ вида

$$h = a_{l_1} l_1 + \ldots + a_{l_n} l_n$$

полагает

$$\psi(h) = \sigma^i(a_{l_1})\eta^j(l_1) + \ldots + \sigma^i(a_{l_n})\eta^j(l_n),$$
$$\chi(h) = \sigma^k(a_{l_1})\eta^l(l_1) + \ldots + \sigma^k(a_{l_n})\eta^l(l_n).$$

Автоморфизмы ψ, χ будем называть сеансовыми.

3. Участник B вычисляет $\chi(a) \cdot \psi(x)$.
4. Участник B вычисляет $\chi\big(\varphi(a)\big) \cdot \psi\big(\varphi(x)\big)$. Так как элементы a и x были выбраны с нулевым левым аннулятором, то и у этого произведения будет нулевой левый аннулятор.
5. Участник B записывает исходный текст, который надо передать, в виде $m \in R$ и вычисляет $m \cdot \big[\chi\big(\varphi(a)\big) \cdot \psi\big(\varphi(x)\big)\big]$. При необходимости исходный текст разбивается на блоки и каждый блок шифруется отдельно с разными секретными ключами.
6. Участник B отправляет для A криптограмму

$$\big(\chi(a) \cdot \psi(x),\, m \cdot \big[\chi\big(\varphi(a)\big) \cdot \psi\big(\varphi(x)\big)\big]\big).$$

Получив криптограмму, участник A расшифровывает её.

1. Используя секретный автоморфизм φ, участник A вычисляет $\varphi\big(\chi(a) \cdot \psi(x)\big)$.
2. Участник A расшифровывает посланный текст, пользуясь тем, что χ, ψ и φ коммутируют. Таким образом, участник A знает $m \cdot \big[\chi\big(\varphi(a)\big) \cdot \psi\big(\varphi(x)\big)\big]$ и $\varphi\big(\chi(a) \cdot \psi(x)\big)$. Для расшифровки сообщения m достаточно решить линейную систему с коэффициентами из кольца R_e.

В самом деле, так как $\tau \in C(\sigma) \setminus \langle\sigma\rangle$ и $\omega \in C(\eta) \setminus \langle\eta\rangle$, то коммутируют между собой попарно автоморфизмы τ и σ, а также ω и η. Поэтому коммутируют и сконструированные на их основе автоморфизмы φ и ψ, φ и χ. Вследствие этого

$$\chi\big(\varphi(a)\big) \cdot \psi\big(\varphi(x)\big) = \varphi\big(\chi(a) \cdot \psi(x)\big).$$

Кроме того, элемент $\chi\big(\varphi(a)\big) \cdot \psi\big(\varphi(x)\big)$ был выбран с нулевым левым аннулятором. Поэтому система уравнений $m \cdot \big[\chi\big(\varphi(a)\big) \cdot \psi\big(\varphi(x)\big)\big]$ с коэффициентами из кольца R_e будет иметь единственное решение.

3.3. Анализ атак на криптосистему

Рассмотрим следующую задачу. Пусть R — некоторая алгебраическая структура, A — некоторое подмножество автоморфизмов в $\operatorname{Aut} R$, α — случайно выбранный элемент из A. Предположим, что известно некоторое множество пар $\big(x_i, \alpha(x_i)\big)$, $i = 1, \ldots, n$, где $x_i \in R$. Требуется найти автоморфизм $\alpha' \in A$, такой что $\alpha'(x_i) = \alpha(x_i)$ для всех $i = 1, \ldots, n$. Обозначим эту задачу как $\Omega_n(A, R)$.

Заметим, что при отсутствии существенной информации о множествах A и R задача $\Omega_n(A, R)$ является вычислительно трудной, поскольку она разрешима только полным перебором всех элементов множества A и проверкой условия $\alpha'(x_i) = \alpha(x_i)$, $i = 1, \ldots, n$, для каждого выбранного $\alpha' \in A$.

Рассмотрим некоторые атаки на криптосистему.

Атака только с криптограммой. Пусть криптоаналитик располагает открытым ключом участника A и криптограммой. Перед ним стоит следующая задача: по известным парам $\big(a, \varphi(a)\big)$, $\big(x, \varphi(x)\big)$ найти $\alpha \in \operatorname{Aut}(R)$, индуцированный автоморфизмами σ', η', такой что $\varphi(a) = \alpha(a)$, $\varphi(x) = \alpha(x)$. К тому же необходимо, чтобы $\sigma' \in C(\sigma) \setminus \langle\sigma\rangle$ и $\eta' \in C(\eta) \setminus \langle\eta\rangle$.

Построим α. Положим

$$\alpha(a) := \varphi(a), \quad \alpha(x) := \varphi(x).$$

Тогда определены

$$\alpha(ax) = \alpha(a) \cdot \alpha(x) := \varphi(a) \cdot \varphi(x)$$

и

$$\alpha(xa) = \alpha(x) \cdot \alpha(a) := \varphi(x) \cdot \varphi(a).$$

Но доопределить α на элемент $\chi(a) \cdot \psi(x)$ можно лишь перебором его образа с последующей проверкой того, что $\sigma' \in C(\sigma) \setminus \langle\sigma\rangle$ и $\eta' \in C(\eta) \setminus \langle\eta\rangle$. Это вычислительно не легче перебора всех автоморфизмов, индуцированных парами $(\sigma', \eta') \in (C(\sigma) \setminus \langle\sigma\rangle) \times (C(\eta) \setminus \langle\eta\rangle)$, удовлетворяющих начальным условиям $\alpha(a) = \varphi(a)$ и $\alpha(x) = \varphi(x)$. В итоге получаем задачу $\Omega_2(Y, R)$, где Y — это множество автоморфизмов R, полученных с помощью пар $(\sigma', \eta') \in \in \big[(C(\sigma) \setminus \langle\sigma\rangle) \times (C(\eta) \setminus \langle\eta\rangle)\big]$, что эквивалентно полному перебору секретных ключей.

Для оценки сложности вскрытия криптосистемы злоумышленником рассмотрим мощность множества, элементы которого необходимо перебрать. Тогда

сложность данной атаки будет равна $t_4 \cdot t_6$. Поэтому при надлежащем выборе параметров безопасности данная задача является вычислительно трудной.

Если криптоаналитик располагает несколькими криптограммами, даже при условии фиксированных автоморфизмов σ и η задача взлома всё равно сводится к полному перебору секретных ключей, так как предполагается, что они каждый раз выбираются разными.

Атака на сеансовые автоморфизмы ψ и χ. Другой способ атаки — найти автоморфизмы ψ и χ, а затем решить относительно m уравнение

$$m \cdot \big[\chi\big(\varphi(a)\big) \cdot \psi\big(\varphi(x)\big)\big] = h,$$

где h известен из криптограммы. Пусть ψ был построен с помощью автоморфизмов σ_1, η_1, а автоморфизм χ с помощью σ_2, η_2. Для того чтобы найти ψ и χ, криптоаналитику необходимо осуществить перебор образов $\psi(x)$, $\chi(a)$, таких что $\chi(a)\psi(x) = h_1$, где h_1 известен из криптограммы, и проверить соотношения $(\sigma_1, \eta_1) \in (\langle\sigma\rangle, \langle\eta\rangle)$ и $(\sigma_2, \eta_2) \in (\langle\sigma\rangle, \langle\eta\rangle)$. Это вычислительно не легче перебора пар $(\sigma_1, \eta_1) \in (\langle\sigma\rangle, \langle\eta\rangle)$ и $(\sigma_2, \eta_2) \in (\langle\sigma\rangle, \langle\eta\rangle)$ (а это полный перебор соответствующих автоморфизмов) с последующей проверкой условия $\chi(a)\psi(x) = h_1$. Следовательно, определённая выше сложность атаки будет равна $t_3^2 \cdot t_5^2$. При правильном выборе соответствующих параметров безопасности эта задача является вычислительно трудной.

Атака с выбранным исходным текстом. Эта атака основана на попытке криптоаналитика получить $\chi\big(\varphi(a)\big)\psi\big(\varphi(x)\big) \in R$ и решить уравнение $m \cdot \chi\big(\varphi(a)\big)\psi\big(\varphi(x)\big)$ относительно m посредством нового сеанса связи с участником B в качестве участника A. Даже если участник B повторяет тот же исходный текст m, он должен сконструировать новые сеансовые автоморфизмы $\psi' \neq \psi$ и $\chi' \neq \chi$. Поэтому криптоаналитик получит не $m \cdot \chi\big(\varphi(a)\big)\psi\big(\varphi(x)\big)$, а $m \cdot \chi'\big(\varphi(a)\big)\psi'\big(\varphi(x)\big)$. И даже если он решит новое уравнение относительно $\chi'\big(\varphi(a)\big)\psi'\big(\varphi(x)\big)$, никакой новой информации относительно $\chi\big(\varphi(a)\big)\psi\big(\varphi(x)\big)$ он не получит.

4. Криптосхемы на основе луп (см. [3])

4.1. Протокол выработки общего секретного ключа

Рассмотрим протокол выработки общего ключа, построенный при помощи лупы Муфанг.

Пусть L — общеизвестная лупа Муфанг, $a, b, c \in L$ — общеизвестные элементы. Пусть M, K и N — порядки соответственно элементов a, b и c. Протокол выработки секретного ключа выглядит следующим образом.

1. Абонент A выбирает случайные натуральные числа $m < M$, $k < K$, $n < N$ и посылает абоненту B пару $(u_1, u_2) = (a^m b^k, b^k c^n)$.
2. Абонент B выбирает случайные натуральные числа $r < M$, $l < K$, $s < N$ и посылает сообщение $(v_1, v_2) = (a^r b^l, b^l c^s)$.

3. Абонент A вычисляет $(a^m v_1)b^k$ и $(b^k v_2)c^n$.
4. Абонент B вычисляет $(a^r u_1)b^l$ и $(b^l u_2)c^s$.

Общим ключом абонентов A и B является

$$K_{AB} = (a^{m+r}b^{k+l})(b^{k+l}c^{n+s}).$$

Непосредственно из следствий теоремы Муфанг получаем следующий результат.

Утверждение 4.1. *Если L — лупа Муфанг, $a, b \in L$, то*

$$\big(a^n(a^r b^s)\big)b^m = a^n\big((a^r b^s)b^m\big) = \big(a^s(a^n b^m)\big)b^s = a^r\big((a^n b^m)b^s\big) = a^{r+n}b^{s+m}.$$

Таким образом, ключ абонента A —

$$K_A = \big((a^m v_1)b^k\big)\big((b^k v_2)c^n\big) = (a^{m+r}b^{k+l})(b^{k+l}c^{n+s}) = K_{AB},$$

ключ абонента B —

$$K_B = \big((a^r u_1)b^l\big)\big((b_l u_2)c^s\big) = K_{AB},$$

$K_A = K_B$.

Отметим, что элементы a, b, c лупы L являются общеизвестными, а натуральные числа r, k, s, m, l, n — секретными.

Замечание. Покажем, что знания одного из секретных чисел достаточно для получения секретного ключа. Действительно, пусть злоумышленник каким-либо образом получил число m. Тогда, вычислив $(a^{-m}u_1) = b^k$, $b^{-k}u_2 = c^n$, $\big((a^m v_1)b^k\big)\big(b^k(v_2 c^n)\big) = K$, злоумышленник получает секретный ключ K. Таким образом, стойкость протокола не превышает сложности нахождения одного секретного ключа.

Замечание. Злоумышленник для нахождения ключа может решить задачу дискретного логарифмирования в подгруппе $\langle a, b\rangle \subseteq L$ или $\langle b, c\rangle \subseteq L$ или перебором найти элемент лупы, который является общим ключом.

В качестве примера рассмотрим класс луп Пейджа. В качестве a, b, c можно выбрать элементы вида

$$\begin{pmatrix} \eta & e_1 \\ (0,0,0) & \eta^{-1} \end{pmatrix}, \quad \begin{pmatrix} \theta & e_2 \\ (0,0,0) & \theta^{-1} \end{pmatrix}, \quad \begin{pmatrix} \zeta & e_3 \\ (0,0,0) & \zeta^{-1} \end{pmatrix},$$

где η, θ, ζ — примитивные элементы поля F_q. Порядки данных элементов равны $(q-1)/2$.

4.2. Схема шифрования

Пусть L — конечная лупа и задана последовательность $\alpha = [A_1, \ldots, A_s]$, где $A_i \in L^r$ для некоторого натурального числа r, т. е. $A_i = (a_{i,1}, \ldots, a_{i,r}), a_{i,j} \in L$. Для каждого $i = 1, \ldots, s$ обозначим через A'_i элемент лупового кольца $\sum\limits_j a_{i,j} \in ZA$. Тогда $A'_1 \cdot \ldots \cdot A'_s = \sum a_l l$.

Определение 4.1. Последовательность $\alpha = [A_1, \ldots, A_s]$ называется $[s, r]$-покрытием для L, если для элемента лупового кольца $\sum a_l l = A'_1 \cdot \ldots \cdot A'_s$ выполняются следующие условия: $a_l > 0$ для всех $l \in L$ и $|A_i| = r$, $i = 1, \ldots, s$.

Рассмотрим криптосхему, которая основана на $[s, r]$-покрытиях лупы Муфанг. Пусть L — конечная лупа Муфанг и $\alpha = (a_{i,j})$ — $[s, r]$-покрытие лупы L. В [12] было показано, что сложность задачи разложения на множители

$$g = a_{1,j_1} \cdot a_{2,j_2} \cdot a_{3,j_3} \cdot \ldots \cdot a_{s,j_s}$$

в конечной группе G эквивалентна сложности задачи дискретного логарифмирования в группе G. Тогда в общем случае задача разложения элемента лупы $l \in L$ на множители

$$l = (a_{1,j_1} \cdot (a_{2,j_2} \cdot (a_{3,j_3} \cdot \ldots \cdot a_{s,j_s})$$

с неизвестной расстановкой скобок имеет не меньшую сложность, чем аналогичная задача в конечной группе.

Участник A.

1. Участник A выбирает две лупы Муфанг L, M с достаточно большим количеством порождающих. Участник A генерирует случайное $[s, r]$-покрытие $\alpha = (a_{i,j})$ для L.
2. Участник A выбирает эпиморфизм $f\colon L \to M$, который он хранит в секрете, и вычисляет $\beta = (b_{i,j}) = f(\alpha) = f(a_{i,j})$. Заметим, что β является $[s, r]$-покрытием для лупы M.

Открытым ключом является $(\{\alpha\}, \{\beta\})$.

Участник B.

1. Участник B формирует сообщение $x \in M$.
2. Участник B выбирает произвольное y_1 из покрытия α, причём расстановка скобок осуществляется произвольным способом. Таким образом,
$$y_1 = a_{1,j_1} \cdot (a_{2,j_2} \cdot (a_{3,j_3} \cdot \ldots \cdot a_{s,j_s}).$$
3. Участник B образует $y_2 \in \beta$ с аналогичной пункту 2 расстановкой скобок.
4. Участник B формирует $y_3 = xy_2$.
5. Участник B посылает участнику A криптограмму (y_1, y_3).

Участник A, получив пару (y_1, y_3), вычисляет $f(y_1) = y_2$ и $y_3 y_2^{-1}$. Так как M — лупа Муфанг, то $y_3 y_2^{-1} = (xy_2)y_2^{-1} = x$.

Замечание. С практической точки зрения участнику A лучше заранее составить таблицу значений для эпиморфизма f.

Замечание. Конструкция легко может быть обобщена на произвольную квазигруппу, если умножение на y_2^{-1} справа в алгоритме расшифрования заменить на правое деление.

Замечание. Любое $[s, r]$-покрытие можно представить в виде матрицы $\alpha = (a_{i,j})$, где $a_{i,j} \in L$, $1 \leqslant i \leqslant s$, $1 \leqslant j \leqslant r$. Тогда с практической точки зрения $[s, r]$-покрытие удобно задавать случайной $(s \times r)$-матрицей с проверкой необходимых условий.

5. Группоиды с перестановочными степенями

В этом разделе изучается возможность использования неассоциативных группоидов для реализации процедуры открытого распределения ключей на основе алгоритма, обобщающего хорошо известный алгоритм Диффи—Хеллмана. Приведены конструкции группоидов, обладающих необходимым для этого свойством перестановочности степеней и не являющихся группоидами с ассоциативными степенями (см. [4]).

5.1. Алгоритмы выработки общего секретного ключа, использующие свойство перестановочности степеней

Для элемента g конечного группоида $(\Omega, *)$ и заданных $r, l \in \mathbb{N}$ определим *правую r-ю и левую l-ю степени* равенствами

$$g^{[r]} = \underbrace{(\dots((g*g)*g)\dots)}_{r \text{ сомножителей}}, \quad {}^{[l]}g = \underbrace{(\dots(g*(g*g))\dots)}_{l \text{ сомножителей}}.$$

Назовём g *элементом с перестановочными правыми степенями* или *ППС-элементом*, если

$$g^{[m][n]} = g^{[n][m]} \quad \text{для всех} \quad m, n \in \mathbb{N}. \tag{5.1}$$

Если это тождество выполняется для всех элементов $g \in \Omega$, то будем называть $(\Omega, *)$ *ППС-группоидом*. Аналогично с использованием тождества

$${}^{[m][n]}g = {}^{[n][m]}g \quad \text{для всех} \quad m, n \in \mathbb{N}$$

определяются *элементы и группоиды с перестановочными левыми степенями*, *ПЛС-элементы* и *ПЛС-группоиды*.

Алгоритм 1 открытого распределения ключей. Выбрав (несекретный) ППС-элемент g группоида Ω, абоненты A и B независимо друг от друга выбирают произвольные числа $r_A, r_B \in \mathbb{N}$ соответственно и обмениваются элементами $g^{[r_A]}$ и $g^{[r_B]}$. Затем они формируют общий секретный ключ $g^{[r_A][r_B]} = g^{[r_B][r_A]}$.

Сложность восстановления наблюдателем секретного ключа по открытой информации g, $g^{[r_A]}$, $g^{[r_B]}$ не превосходит сложности *задачи правого дискретного логарифмирования в группоиде*, т. е. сложности решения уравнения

$$g^{[x]} = h. \tag{5.2}$$

Естественным обобщением данного подхода к построению процедур открытого распределения ключей является комбинирование правых и левых степеней.

Будем говорить, что группоид $(\Omega, *)$ — *группоид с перестановочными степенями* (*ПС-группоид*), если он является ПЛС- и ППС-группоидом, а также для любого $g \in \Omega$ и любых $l, r \in \mathbb{N}$ выполняется равенство

$${}^{[l]}\left(g^{[r]}\right) = \left({}^{[l]}g\right)^{[r]}$$

Будем говорить, что элемент g произвольного группоида $(\Omega, *)$ — *ПС-элемент*, если он порождает ПС-группоид.

Можно предложить следующий алгоритм с использованием ПС-элемента g.

Алгоритм 2 открытого распределения ключей. Абонент A выбирает пару чисел

$$(l_A, r_A), \quad l_A, r_A \in \mathbb{N},$$

а абонент B — пару чисел

$$(l_B, r_B), \quad l_B, r_B \in \mathbb{N}.$$

Абоненты A и B открыто обмениваются элементами ${}^{[l_A]}g^{[r_A]}$ и ${}^{[l_B]}g^{[r_B]}$. В качестве общего ключа выбирается элемент

$${}^{[l_A]}\big({}^{[l_B]}g^{[r_B]}\big)^{[r_A]} = {}^{[l_B]}\big({}^{[l_A]}g^{[r_A]}\big)^{[r_B]}.$$

При такой процедуре сложность вычисления общего секретного ключа наблюдателем оценивается сверху сложностью решения задачи лево-правого логарифмирования, т. е. сложностью решения уравнения

$${}^{[x]}g^{[y]} = h \tag{5.3}$$

с двумя неизвестными x, y.

Ещё большее число неизвестных включает следующий алгоритм.

Алгоритм 3 открытого формирования ключа. Абоненты A и B независимо друг от друга выбирают наборы чисел $a_1, \ldots, a_m \in \mathbb{N}$ и $b_1, \ldots, b_n \in \mathbb{N}$ соответственно и натуральные числа r, m, s, n, такие что $r \leqslant m$, $s \leqslant n$, и обмениваются сообщениями

$$g_A = {}^{[a_1]\ldots[a_r]}g^{[a_{r+1}]\ldots[a_m]}, \quad g_B = {}^{[b_1]\ldots[b_s]}g^{[b_{s+1}]\ldots[b_n]}.$$

Абоненты A и B вырабатывают общий ключ

$$g_{AB} = {}^{[a_1]\ldots[a_r]}g_B^{[a_{r+1}]\ldots[a_m]} = {}^{[b_1]\ldots[b_s]}g_A^{[b_{s+1}]\ldots[b_n]} = \\ = {}^{[a_1]\ldots[a_r]\,[b_1]\ldots[b_s]}g^{[b_{s+1}]\ldots[b_n][a_{r+1}]\ldots[a_m]}.$$

Нахождение общего секретного ключа в алгоритме 3 не сложнее решения задачи обобщённого дискретного логарифмирования, т. е. нахождения хотя бы одной пары натуральных чисел u, v и набора $(x_1, \ldots, x_v)$, $x_i \in \mathbb{N}$, $i \in \overline{1, v}$, удовлетворяющих равенству

$${}^{[x_1]\ldots[x_u]}g^{[x_{u+1}]\ldots[x_v]} = h, \tag{5.4}$$

если такие существуют.

Сложность решения уравнений (5.2)—(5.4) определяют прежде всего два фактора:

1) выбор алгебраического носителя алгоритма: группоида $(\Omega, *)$ и элемента g, обеспечивающий стойкость алгоритма по отношению к методам, связанным с факторизацией группоида и перебором;

2) выбор способа представления алгебраического носителя, при котором функция возведения в правую (левую) степень однонаправленная.

5.2. Построение классов ПС-группоидов

Определим *правый дефект* $D_{\mathrm{r}}(g)$ и *правый период* $T_{\mathrm{r}}(g)$ элемента g соответственно как дефект и период последовательности $g^{\mathbb{N}} = \{g^{[n]}\}_{n\in\mathbb{N}}$. Аналогично определим левые дефект $D_{\mathrm{l}}(g)$ и период $T_{\mathrm{l}}(g)$ элемента g.

Назовём *правым потенциалом* (*левым потенциалом*) произвольного элемента $g \in \Omega$ наибольшее $t \in \mathbb{N}$, такое что все элементы $g, g^{[2]}, \ldots, g^{[t]}$ $(g, {}^{[2]}g, \ldots, {}^{[t]}g)$ различны, и обозначим эту величину $\mathrm{pot}_{\mathrm{r}}\, g$ (соответственно $\mathrm{pot}_{\mathrm{l}}\, g$).

Пользуясь введёнными числовыми характеристиками, можно показать, что для проверки того, что g — ПС-элемент, достаточно проверить конечное число тождеств.

Пусть *правый дефект* $D_{\mathrm{r}} = D_{\mathrm{r}}(\Omega)$ *группоида* $(\Omega, *)$ и его *правый период* T_{r} определены соотношениями

$$D_{\mathrm{r}} = \max\{D_{\mathrm{r}}(g),\ g \in \Omega\}, \quad T_{\mathrm{r}} = \mathrm{НОК}\{T_{\mathrm{r}}(g),\ g \in \Omega\}.$$

Для каждого элемента g группоида выполнены соотношения

$$g^{[i]} = g^{[i+T_{\mathrm{r}}]} \ \text{ для каждого } \ i > D_{\mathrm{r}}.$$

Теорема 5.1 [4]. *Элемент g группоида $(\Omega, *)$ является ППС—элементом тогда и только тогда, когда*

$$\left(g^{[n]}\right)^{[k]} = \left(g^{[k]}\right)^{[n]} \ \text{ для любых } \ n, k \in \overline{1, D_{\mathrm{r}} + T_{\mathrm{r}}}. \tag{5.5}$$

5.2.1. Медиальные и локально-медиальные группоиды

Пусть $(\Omega, \cdot)$ — произвольная конечная полугруппа единицей e, $\widetilde{\mathrm{Aut}}(\Omega)$ — группа всех автоморфизмов и антиавтоморфизмов полугруппы Ω.

Зафиксируем два коммутирующих (анти)автоморфизма

$$\sigma, \tau \in \widetilde{\mathrm{Aut}}(\Omega), \quad \sigma\tau = \tau\sigma, \tag{5.6}$$

и зададим на Ω новую операцию $*$ условием

$$x * y = \sigma(x) \cdot \tau(y) \ \text{ для всех } \ x, y \in \Omega. \tag{5.7}$$

Будем называть группоид $(\Omega, *)$ *медиальным*.

Теорема 5.2 [4]. *Если $(\Omega, \cdot)$ — абелева полугруппа и σ, τ — её коммутирующие (анти)автоморфизмы, то группоид $(\Omega, *)$ с операцией* (5.7) *является ПС-группоидом.*

Условие коммутативности полугруппы в теореме можно несколько ослабить.

Теорема 5.3. *Пусть* $(\Omega, \cdot)$ *— произвольная полугруппа, выполнено условие* (5.6) *и* $H = \langle \sigma, \tau \rangle$ *— подгруппа группы* $\widetilde{\mathrm{Aut}}(\Omega)$*, порождённая автоморфизмами* σ*,* τ*. Тогда для группоида* $(\Omega, *)$ *с операцией* (5.7) *справедливо следующее. Если для некоторого элемента* $g \in \Omega$ *элементы орбиты* $H(g)$ *попарно перестановочны в* $(\Omega, \cdot)$*, то* g *— ПС-элемент. Если последнее условие перестановочности выполняется для всех* $g \in \Omega$*, то* $(\Omega, *)$ *— ПС-группоид.*

Будем называть группоиды из последней теоремы *локально-медиальным на элементе* g и *локально-медиальным*.

Пример. Пусть $(\Omega, \cdot)$ — произвольная конечная группа, $\sigma = \mathrm{id}_\Omega$ — тождественный автоморфизм и τ — (анти)автоморфизм вида $\tau(g) = g^{-1}$. Тогда группоид $(\Omega, *)$ с операцией (5.7) является локально-медиальным.

Предложение 5.1. *Пусть* $(\Omega, \cdot)$ *— группа. Если* $(\Omega, *)$ *— локально-медиальный группоид с операцией* (5.7)*, то для любого* $g \in \Omega$ *справедливо соотношение*

$$\mathrm{pot}_r\, g \mid \mathrm{ord}\,\sigma \cdot \mathrm{ord}\, g.$$

5.3. Оценка сложности вычисления степени элемента в локально-медиальном группоиде

Можно заметить, что в группоиде с операцией (5.7) при вычислении правых степеней правый автоморфизм τ ведёт себя «весьма пассивно». В связи с этим возникает вопрос: не будет ли этот группоид изоморфен некоторому группоиду $(\Omega, \star)$ с операцией

$$x \star y = \varphi(x) y \quad \text{для всех} \quad x, y \in \Omega, \quad \varphi \in \mathrm{Aut}(\Omega). \tag{5.8}$$

Оказывается, что при нетождественном отображении τ это невозможно.

Предложение 5.2. *Если* $(\Omega, \cdot)$ *— полугруппа с единицей* e *и операции* (5.7)*,* (5.8) *таковы, что* $(\Omega, *) \cong (\Omega, \star)$*, то* τ *— тождественный автоморфизм.*

Однако если $(\Omega, *)$ — локально-медиальный группоид, то даже при условии $\tau \neq \varepsilon$ задачи о вычислении степеней и логарифмировании в этом группоиде можно свести к решению аналогичных задач в группоиде с операцией

$$x \star y = \sigma(x) \cdot y \quad \text{для всех} \quad x, y \in \Omega. \tag{5.9}$$

Сложность возведения в степень (анти)автоморфизма, заданного на полугруппе, зависит от способа его задания. Обозначим через $\mathrm{AUT}(\sigma, t)$ трудоёмкость вычисления значения $\sigma^t(h)$ для произвольного элемента h полугруппы $(\Omega, \cdot)$.

Теорема 5.4 [4]. *Пусть* $(\Omega, \cdot)$ *— полугруппа с единицей,* g *— обратимый элемент. Для локально-медиального группоида* $(\Omega, *)$ *с операцией* (5.7)*, где* σ*,* τ *удовлетворяют* (5.6)*, существует алгоритм, который вычисляет степень* $g^{[m]}$ *со сложностью* $O(\mathrm{AUT}(\sigma, n) \log_2 n)$ *операций в полугруппе* $(\Omega, \cdot)$.

Замечание. Традиционно автоморфизмы задаются действием на образующих элементах. В этом случае трудоёмкость возведения в степень, а значит и алгоритмов 1—3, оценивается величиной $O(\log^2|\Omega|)$. В случае если автоморфизмы σ, τ имеют небольшой по сравнению с мощностью группы порядок, эта величина становится равной оценке сложности реализации протокола Диффи—Хеллмана.

Сложность возведения в левую степень оценивается аналогично.

5.4. Решение задачи дискретного логарифмирования на локально-медиальном группоиде

Методы дискретного логарифмирования, использующие идеи согласования и сведения к собственным подгруппам, обобщаются на локально-медиальные группоиды.

Пример (модификация алгоритма Гельфонда—Шенкса)**.**

Алгоритм 5.1.

Дано. $(\Omega,\cdot)$ — полугруппа с единицей, g, h — обратимые элементы полугруппы $(\Omega,\cdot)$, (анти)автоморфизмы $\sigma,\tau\in\widetilde{\mathrm{Aut}}(\Omega,\cdot)$.

Выход. Решение x уравнения (5.2) $g^{[x]}=h$.

Шаг 1. Возьмём $d:=\lfloor\sqrt{\mathrm{pot_r}\,g}\rfloor+1$.

Шаг 2. Выделим память. Поставим в соответствие элементам группоида ячейки памяти размера, необходимого для хранения индекса $i\in\overline{1,d}$. Заполним память нулями.

1. Положим $g_0=g^{[0]}=e$.
2. Вычислим элемент $c=\rho_d\bigl(g,\tau^{-1}(g),\ldots,\tau^{-1}(g)\bigr)$.
3. Для $i\in\overline{1,d}$ вычислим элементы $g_i=g^{[\mathrm{id}]}$,
$$g_i=\sigma^{d-1}(g_{i-1})*c,$$
и по адресу g_i запишем в память число i.

Шаг 3. Для $j\in\overline{1,d}$ будем вычислять элементы $\beta_j=\rho_{j+1}(h,g,\ldots,g)$ и проверять память по адресу β_j. Если по адресу β_j записано $i>0$, то выведем ответ $n=id-j$.

Шаг 4. Если ни для одного j мы не нашли в памяти ненулевого числа, то выводим ответ «Нет решений».

Теорема 5.5. *Алгоритм* 5.1 *работает корректно, при этом для реализации алгоритма требуется* $O(\sqrt{\mathrm{pot_r}\,g})$ *операций в полугруппе* $(\Omega,\cdot)$ *и память объёмом* $O\bigl(\sqrt{\mathrm{pot_r}\,g}\cdot\log_2(\sqrt{\mathrm{pot_r}\,g})\bigr)$.

Пример (обобщение метода сведения к собственным подгруппам)**.** Пусть $(\Omega,\cdot)=(G,\cdot)$ — абелева группа, $(G,*)$ — медиальная квазигруппа с операцией (5.7). Для решения задачи логарифмирования правых степеней по предложению 5.2 можем полагать, что автоморфизм τ тождественный.

Непосредственной проверкой доказывается следующее утверждение.

Предложение 5.3. *Для произвольного элемента $g \in G$ и для произвольных натуральных n и k выполнено равенство*

$$\left(g^{[n]}\right)^k = (g^k)^{[n]}.$$

Перейдём к описанию метода. Пусть g, h — произвольные элементы квазигруппы $(G, *)$. Решается уравнение вида $g^{[x]} = h$.

1. Рассмотрим первый случай: порядок группы G представим в виде $|G| = pq$, где p и q — взаимно простые числа. Как следствие нашего уравнения получаем систему

$$\begin{cases} \left(g^{[x]}\right)^p = h^p, \\ \left(g^{[x]}\right)^q = h^q. \end{cases}$$

Очевидно, что $\left(g^{[x]}\right)^p \in pG$, где $pG = \{w^p \mid w \in G\}$ — подгруппа мощности $|pG| = q$. Автоморфизм σ оставляет эту подгруппу на месте. По предложению 5.3 степень в медиальной квазигруппе перестановочна с групповой степенью. Таким образом, если x — решение исходного уравнения, то x — решение уравнения $(g^p)^{[x]} = h^p$ в подквазигруппе $(pG, *)$. Потенциал элемента g^p в подквазигруппе $(pG, *)$ по предложению 5.1 будет делить $q \operatorname{ord} \sigma$. Аналогичные рассуждения проводятся для подгруппоида $(qG, *)$. А значит, решая уравнения в группоидах $(pG, *)$ и $(qG, *)$, находим все наборы решений вида

$$\begin{cases} x \equiv x_p \pmod{(q \operatorname{ord} \sigma)}, \\ x \equiv x_q \pmod{(p \operatorname{ord} \sigma)}. \end{cases}$$

Данная система имеет решение по модулю $pq \operatorname{ord} \sigma$ тогда и только тогда, когда разрешимо исходное уравнение дискретного логарифмирования.

Таким образом, если исходное уравнение над группоидом $(G, *)$, мощности $|G| = p_1^{k_1} \cdot \ldots \cdot p_t^{k_t}$ имеет решение, то его нахождение можно свести к решению уравнений над группоидами примарной мощности.

2. Рассмотрим второй случай: порядок группы $|G|$ имеет вид $|G| = p^n$. Пусть $\exp G = p^k$. Возведя обе части уравнения в степень p^{k-1}, получим уравнение (5.2) над группоидом $(p^{k-1}G, *)$. Интересно, что $(p^{k-1}G, \cdot) \cong \mathbb{Z}_p \dot{+} \ldots \dot{+} \mathbb{Z}_p$. Таким образом, порядок любого элемента группоида $(p^{k-1}G, *)$ по предложению 5.1 делит $p \operatorname{ord} \sigma$. Находим все решения x_0 по модулю $p \operatorname{ord} \sigma$.

Решение исходного уравнения представим в виде $x = x_0 + x_1 p \operatorname{ord} \sigma$. Тогда исходное уравнение представляется в виде

$$g^{[x_0 + x_1 p \operatorname{pot} \sigma]} = h.$$

Данное равенство преобразуем к виду

$$\sigma^{x_0}\left(g^{[x_1 p \operatorname{ord} \sigma]}\right) = h\left(g^{[x_0]}\right)^{-1},$$
$$\left(g^{[\operatorname{ord} \sigma]}\right)^{p x_1} = \sigma^{-x_0}\left(h\left(g^{[x_0]}\right)^{-1}\right).$$

Обозначив

$$g_1 = \left(g^{[\operatorname{ord} \sigma]}\right)^p, \quad h_1 = \sigma^{-x_0}\left(h\left(g^{[x_0]}\right)^{-1}\right),$$

получим уравнение

$$g_1^{x_1} = h_1.$$

Для решения этого уравнения относительно x_1 в циклической группе $\langle g_1 \rangle$ порядка p^{k-1} можно использовать идеи метода Гельфонда.

Подведём итог. Принципиальное отличие в сложности правого логарифмирования на медиальном группоиде есть лишь на этапе логарифмирования в медиальном группоиде, построенном над группой, изоморфной $\mathbb{Z}_p \dot{+} \ldots \dot{+} \mathbb{Z}_p$.

Очевидно, что для логарифмирования левых степеней возможно привести алгоритмы и методы, аналогичные вышеприведённым, имеющие точно такую же сложность.

5.5. Верхняя оценка стойкости процедур открытого распределения ключей

Пусть $(\Omega, *)$ — произвольный ПС-группоид. Рассмотрим алгоритм 3 открытого распределения ключей.

Назовём δ — отображение группоида $(\Omega, \star)$ на себя, — *отображением, имитирующим секретный ключ* $(r, n, a_1, \ldots, a_m)$ абонента A, если для любого секретного ключа $(s, n, b_1, \ldots, b_n)$ абонента B выполняется равенство

$$\delta\big({}^{[b_1]\ldots[b_s]}g^{[b_{s+1}]\ldots[b_n]}\big) = {}^{[a_1]\ldots[a_r][b_1]\ldots[b_s]}g^{[b_{s+1}]\ldots[b_n][a_{r+1}]\ldots[a_m]}, \tag{5.10}$$

т. е. если при использовании преобразования δ вместо преобразования, задаваемого ключом абонента A, мы всё равно получим истинное значение общего ключа. Кратко будем называть δ имитирующим отображением.

Предложение 5.4. *Отображение δ, заданное на $(\Omega, *)$, является имитирующим тогда и только тогда, когда отображение δ перестановочно с операциями возведения в правую и левую степень, причём выполняется равенство*

$${}^{[a_1]\ldots[a_r]}g^{[a_{r+1}]\ldots[a_m]} = \delta(g). \tag{5.11}$$

Например, если выполнено соотношение $g^{[r]} = {}^{[a_1]\ldots[a_r]}g^{[a_{r+1}]\ldots[a_m]}$, то операция возведения в правую степень r есть имитирующие отображение.

Основываясь на этом, можно предложить следующую атаку.

Алгоритм 5.2.

Дано. Группоид $(\Omega, *)$, открытый ключ абонента A вида $K_A = {}^{[a_1]\ldots[a_r]}g^{[a_{r+1}]\ldots[a_m]}$.

Выход. Общий секретный ключ K_{AB}.

Шаг 1. Решаем уравнение

$$g^{[x]} = K_A, \tag{5.12}$$

используя алгоритмы, рассмотренные в разделе 5.4.

Шаг 2. Если решение существует, находим общий ключ $({}^{[b_1]\ldots[b_s]}(g)^{[b_{s+1}]\ldots[b_n]})^{[x]}$. Иначе переходим к шагу 3.

Шаг 3. Решаем уравнение

$$^{[x]}g = K_A, \tag{5.13}$$

используя алгоритмы, рассмотренные в разделе 5.4.

Шаг 4. Если решение существует, находим общий ключ $^{[x]}\bigl(^{[b_1]\ldots[b_s]}(g)^{[b_{s+1}]\ldots[b_n]}\bigr)$.

Трудоёмкость Q метода определяется сложностью решения уравнений на первом и третьем шагах и составляет $O\bigl(\mathrm{Lg}(\Omega,*)\bigr)$, где $\mathrm{Lg}(\Omega,*)$ — трудоёмкость одностороннего логарифмирования. Надёжность оценивается снизу величиной

$$\mathcal{P} = \frac{\bigl|^{[\mathbb{N}]}g \cup g^{[\mathbb{N}]}\bigr|}{|\Omega|}.$$

Таким образом, стойкость оценивается сверху величиной

$$\mathrm{Lg}(\Omega,*)\frac{|\Omega|}{\bigl|^{[\mathbb{N}]}g \cup g^{[\mathbb{N}]}\bigr|}.$$

Для локально-медиального группоида удаётся показать достижимость максимума стойкости алгоритма 2 относительно данной атаки.

Теорема 5.6. *Максимум стойкости алгоритма* 2 *относительно алгоритма 5.2 достигается при* $\mathrm{pot_r}\, g \sim \mathrm{pot_l}\, g \sim \sqrt{|\Omega|}$, $\mathrm{pot_{lr}}\, g \sim |\Omega|$ *и равен* $O(|\Omega|^{3/4})$.

Группоиды, в которых оценка достижима, существуют.

Пример. Пусть $\langle a\rangle$ — циклическая группа порядка m и $(\Omega,\cdot) = \langle a\rangle \otimes \langle a\rangle$ — внешнее прямое произведение групп. Тогда группоид $(\Omega,*)$, определяемый равенством (5.7) при $\tau = \mathrm{id}_\Omega$ (тождественный автоморфизм) и $\sigma(x,y) = (y,x)$, — медиальная квазигруппа.

Рассмотрим элемент $g = (a,e) \in \Omega$. Нетрудно показать, что $\mathrm{pot_r}\, g = m$, $\mathrm{pot_l}\, g = 2m$ и $\mathrm{pot_{lr}}\, g > \phi(m)m$, где $\phi(m)$ — функция Эйлера.

Наряду с возведением в степень в локально-медиальном группоиде в качестве имитирующего гомоморфизма может быть использована операция возведения в степень в исходной полугруппе. Такая атака успешна в случае, когда, например, каждый из автоморфизмов (5.6), задающих операцию в группоиде, есть возведение в степень.

6. Медиальная квазигруппа на группе точек эллиптической кривой

Пусть $p > 2$ — простое число, $q = p^k$, F_q — поле Галуа и $A, B \in F_q$. Эллиптическая кривая $E = E(F_q)$ есть множество решений $P = (a,b) \in F_q^2$ уравнения

$$y^2 = x^3 + Ax + B \tag{6.1}$$

в совокупности с Θ — бесконечно удалённой точкой. На $E(F_q)$ определяется структура абелевой группы $(E,\oplus)$ с нейтральным элементом Θ. Сложность реализации операции $\oplus$ оценивается как $O(1)$ операций в поле F_q.

В общем случае трудоёмкость задачи дискретного логарифмирования на группе точек эллиптической кривой имеет корневую оценку, поэтому медиальные квазигруппы, построенные на них, могут оказаться подходящими алгебраическими структурами для построения алгоритма открытого распределения ключа с большей стойкостью.

При условии $A, B \in F_p$ существует автоморфизм σ группы $(E, \oplus)$, определяемый равенством

$$\sigma\big((x, y)\big) = (x^p, y^p). \tag{6.2}$$

Пусть τ — тождественный автоморфизм этой группы. Зададим на E операцию $*$ равенством (5.7). Тогда $(E, *)$ — медиальная квазигруппа.

Замечание. Известно, что автоморфизм Фробениуса на $(E(\bar{F}_q), \oplus)$ не может соответствовать умножению точки на некоторое целое число.

Оценим стойкость алгоритма 2 открытого распределения ключей, реализованного на ПС-группоиде $(E, *)$.

Очевидно, что построение имитирующего отображения в случае, когда $\sigma(P) = kP$, равносильно логарифмированию на группе точек эллиптической кривой, а значит, с точки зрения анализа интерес представляет случай, когда автоморфизм Фробениуса σ на кривой $E(F_q)$ не соответствует умножению точки на некоторое целое число. В дальнейшем будем рассматривать только такие кривые.

Группа эллиптической кривой $E(F_q)$ порядка m изоморфна группе $\mathbb{Z}_{m_1} \dot{+} \mathbb{Z}_{m_2}$, где $m = m_1 m_2$, $m_2 \mid (m_1, q-1)$.

Если $m_2 = 1$, то $(E, \oplus)$ — циклическая группа. В этом случае стойкость общего секретного ключа из алгоритмов 1—3 не превосходит трудоёмкости дискретного логарифмирования на кривой $(E(F_q), \oplus)$.

Рассмотрим интересный частный случай.

Пример. Пусть эллиптическая кривая $E(F_{p^2})$, заданная уравнением (6.1), при $A, B \in F_p$, изоморфна группе $\mathbb{Z}_n \dot{+} \mathbb{Z}_n$, $n \in \{p-1, p+1\}$. Такие кривые относятся к классу суперсингулярных [15]. Тогда автоморфизм σ, задаваемый равенством (6.2), имеет порядок 2 и можно показать, что медиальная квазигруппа $(E, *)$ содержит элемент g, такой что $\mathrm{pot}_{\mathrm{l}}\, g = n$, $\mathrm{pot}_{\mathrm{r}}\, g = 2n$, $\mathrm{pot}_{\mathrm{lr}}\, g \geqslant \varphi(n)n$, где φ — функция Эйлера.

Таким образом стойкость алгоритма 2 относительно алгоритма 5.2 в данном примере будет достигать своего максимума $O(n^{3/2})$.

Замечание. Порядки точек эллиптической кривой из предыдущего примера не превосходят n. Таким образом, стойкость процедуры Диффи—Хеллмана, построенной на $(E, \oplus)$, оценивается сверху величиной $n^{1/2}$.

Однако для медиальных группоидов, построенных на группе точек эллиптической кривой, можно предложить другие атаки, основанные на построении имитирующего отображения.

Атака 1. Любая комбинация правых и левых степеней элемента g такого группоида представляется в виде

$$^{[l]}P^{[r]} = k_1 P \oplus k_2\sigma(P)$$

для некоторых натуральных k_1, k_2.

Гомоморфизм δ, действующий на элементах группы E по правилу

$$\delta(Q) = k_1 Q \oplus k_2\sigma(Q), \tag{6.3}$$

очевидно перестановочен с автоморфизмом σ и тождественным гомоморфизмом τ. А значит, δ будет имитирующим гомоморфизмом.

Для нахождения имитирующего гомоморфизма δ воспользуемся методом согласования. Трудоёмкость метода — $O(\sqrt{|E|})$ операций в поле F_q, объём требуемой памяти — $O(\sqrt{|E|})$.

Для описания следующей атаки введём определения.

Пусть $m = |E(F_q)|$ и $(m, p) = e$. Обозначим через $E(\bar{F}_q)$ кривую, заданную уравнением (6.1), над алгебраическим замыканием поля $\bar{F}_q$. Определим $E[m] = \{P \in E(\bar{F}_q)\colon [m]P = \Theta\}$. В [15] показано, что для некоторого натурального t $E[m]$ является подгруппой группы точек эллиптической кривой $E(F_{q^t})$.

Очевидно, справедливы неравенства $E(F_q) < E[m] < E(F_{q^t})$.

Пусть $M_m = \{\mu \in F_{q^t}\colon \mu^m = 1\}$ — множество корней из 1 порядка m поля F_{q^t}. В [15] вводится билинейное отображение $e_m\colon E[m] \times E[m] \to M_m$, называемое *спариванием Вейля*. Показывается, что существует точка $T \in E(F_q)$, такая что отображение $\psi\colon E[m] \to F_{q^t}$, задаваемое по правилу $\psi(S) = e_m(S, T)$, является изоморфным вложением. Параметр t этого отображения называют MOV-степенью (Menezes, Okamoto, Vanstone) группы $E(F_q)$.

Замечание. Эффективные алгоритмы вычисления значения спаривания Вейля предложены в [13].

Если MOV-степень t рассматриваемой эллиптической кривой невелика, то можно предложить следующую атаку.

Атака 2. Будем искать имитирующий гомоморфизм δ вида (6.3).

Для нахождение k_1, k_2 рассмотрим следующие спаривания:

$$e_m\big(^{[l]}P^{[r]}, \sigma P\big) = e_m\big(k_1 P + k_2\sigma(P), \sigma(P)\big) = e_m(P, \sigma P)^{k_1},$$
$$e_m\big(^{[l]}P^{[r]}, P\big) = e_m(k_1 P + k_2\sigma(P), P) = e_m(\sigma(P), P)^{k_2}.$$

Получаем два логарифмических уравнения над полем $GF(q^{2t})$:

$$e_m\big(P, \sigma(P)\big)^{k_1} = e_m\big(^{[l]}P^{[r]}, \sigma(P)\big);$$
$$e_m(\sigma(P), P)^{k_2} = e_m\big(^{[l]}P^{[r]}, P\big).$$

Таким образом имитирующий гомоморфизм найден. Трудоёмкость атаки равна сложности двух логарифмирований в поле F_{q^t}.

Если исходная кривая суперсингулярная, трудоёмкость построения имитирующего отображения не превосходит сложности двух логарифмирований в поле F_{q^2}.

Остаётся отметить, что трудоёмкость построения суперсингулярных кривых с требуемыми свойствами требует минимальных затрат на предварительном этапе, в то время как построение кривых, использующихся в российских стандартах цифровой подписи (ГОСТ 34.10), — это трудоёмкий процесс, занимающий длительное время.

Литература

[1] Гонсалес С., Коусело Е., Марков В. Т., Нечаев А. А. Групповые коды и их неассоциативные обобщения // Дискрет. матем. — 2004. — Т. 14, № 1. — С. 146—156.

[2] Грибов А. В. Гомоморфность некоторых криптографических систем на основе неассоциативных структур // Фундамент. и прикл. матем. — 2015. — Т. 20, вып. 1. — С. 135—149.

[3] Грибов А. В., Золотых П. А., Михалёв А. В. Построение алгебраической криптосистемы над квазигрупповым кольцом // Матем. вопр. криптографии. — 2010. — Т. 1, № 4. — С. 23—33.

[4] Катышев С. Ю., Марков В. Т., Нечаев А. А. Использование неассоциативных группоидов для реализации процедуры открытого распределения ключей // Дискрет. матем. — 2014. — Т. 26, № 3. — С. 45—64.

[5] Кузьмин А. С., Марков В. Т., Михалёв А. А., Михалёв А. В. Криптографические алгоритмы на группах и алгебрах // Фундамент. и прикл. матем. — 2015. — Т. 20, вып. 1. — С. 205—222.

[6] Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. — М.: Связь, 1979.

[7] Марков В. Т., Михалёв А. В., Грибов А. В., Золотых П. А., Скаженик С. С. Квазигруппы и кольца в кодировании и построении криптосхем // Прикл. дискрет. матем. — 2012. — № 4. — С. 31—52.

[8] Росошек С. К. Криптосистемы групповых колец // Вестн. Томск. гос. ун-та. — 2003. — № 6. — С. 57—62.

[9] Brouwer A. E. Bounds on linear codes // Handbook of Coding Theory / V. S. Pless, W. C. Huffman, eds. — Amsterdam: Elsevier, 1998. — P. 295—461.

[10] Grassl M. Searching for linear codes with large minimum distance // Discovering Mathematics with Magma / W. Bosma, J. Cannon, eds. — Berlin: Springer, 2006.

[11] Heise W., Quattrocci P. Informations- und Codierungstheorie. — Berlin: Springer, 1995.

[12] Magliveras S. S., Stinson D. R., Tran van Trung. New approaches to designing public key cryptosystem using one-way functions and trap-doors in finite groups // J. Cryptology. — 2008. — Vol. 15, no. 4. — P. 285—297.

[13] Menezes A., Okamoto T., Vanstone S. Reducing elliptic curve logarithms to logarithms in a finite field // IEEE Trans. Inform. Theory. — 1993. — Vol. 39, no. 5. — P. 1639—1646.

[14] Pflugfelder H. O. Quasigroups and Loops: Introduction. — Berlin: Heldermann, 1990. — (Sigma Ser. Pure Math.; Vol. 8).

[15] Silverman J. The Arithmetic of the Elliptic Curves. — Berlin: Springer, 1986.