УДК 519.719.1 DOI 10.17223/20710410/69/6

ОБЩАЯ СХЕМА ДЛЯ СЕМЕЙСТВА ПРОТОКОЛОВ ВЫРАБОТКИ ОБЩЕГО КЛЮЧА ТИПА ДИФФИ — ХЕЛЛМАНА

А. В. Черемушкин

Академия криптографии РФ, г. Москва, Россия

E-mail: avc238@mail.ru

Изучается общая схема для семейства протоколов выработки ключа по типу протокола Диффи — Хеллмана, предложенная В. А. Артамоновым и В. В. Ященко и основанная на решении функционального тождества $f(x, g(y, a)) = g(y, f(x, a))$. Рассмотрен случай с различными отображениями f, g, а также несколько примеров протоколов на основе некоммутативных и неассоциативных бинарных операций, описываемых данной общей схемой.

Ключевые слова: *протокол Диффи — Хеллмана, сильно зависимые операции, обобщённое тождество медиальности.*

GENERAL SCHEME FOR A CLASS OF DIFFIE — HELLMAN TYPE PROTOCOLS

A. V. Cheremushkin

Academy of Cryptography of the Russian Federation, Moscow, Russia

We consider a general scheme for the class of Diffie — Hellman type protocols proposed by V. Artamonov and V. Yaschenko in 1994. It is based on functional equality $f(x, g(y, a)) = g(y, f(x, a))$ with some functions f, g. We investigate the case with different functions f, g. Some examples of such protocols with nonassociative and noncommutative binary operations are considered.

Keywords: *Diffie — Hellman type protocol, strong dependent operation, general medial identity.*

1. Общая схема протокола типа Диффи — Хеллмана

В работе [1] предложена общая схема протокола Диффи — Хеллмана. Пусть S — множество формируемых общих секретных ключей, K_i — множества личных ключей абонентов, U_i, $i = 1, 2$, — множества открытых ключей абонентов. Общая схема строится на основе четырёх сюръективных отображений $f_1 : K_1 \times U_2 \to S$, $f_2 : K_2 \times U_1 \to S$, $\varphi_1 : K_1 \to U_1$ и $\varphi_2 : K_2 \to U_2$, удовлетворяющих тождеству

$$f_1(k_1, \varphi_2(k_2)) = f_2(k_2, \varphi_1(k_1))$$

при всех $k_i \in K_i$. Для практики удобным является случай, когда $U_1 = U_2 = S$ и отображения φ_i, $i = 1, 2$, задаются на основе функций f_i равенствами $\varphi_i(k_i) = f_i(k_i, a)$, $a \in S$.

1.1. Случай одинаковых функций

Для частного случая $K_1 = K_2$, $U_1 = U_2 = S$, $f_1 = f_2 = f$ и $\varphi_i(k) = f(k, a)$ при некотором фиксированном элементе $a \in S$, $i = 1, 2$, в работе [1] доказана следующая

Теорема 1 [1]. Пусть задано отображение $f : K \times S \to S$ и $a \in S$ — фиксированный элемент, для которого отображение $f_a : K \to S$, заданное равенством $f_a(k) = f(k, a)$, взаимно однозначно. Отображение f является решением функционального уравнения

$$f(k_1, f(k_2, a)) = f(k_2, f(k_1, a))$$

тогда и только тогда, когда K может быть наделено структурой коммутативного группоида с единицей, операция $*$ которого связана с отображением f тождеством $f(k_1, f(k_2, a)) = f(k_1 * k_2, a)$, а единицей является элемент $f_a^{-1}(a)$.

Приведём уточнённую формулировку этого результата. Пусть K и S — конечные множества, $|K| = |S|$ и отображение $f : K \times S \to S$ удовлетворяет условию

$$f(x, f(y, a)) = f(y, f(x, a)) \tag{1}$$

при всех $x, y \in K$ и $a \in S$. Предположим, что хотя бы для одного элемента $a_0 \in S$ отображение $f_{a_0} : K \to S$ является взаимно однозначным.

Напомним, что функция $g : K^m \to K$ называется *сильно зависимой*, если для каждой координаты существует фиксация остальных переменных, при которой получившаяся подфункция (унарная операция) является подстановкой.

Теорема 2. Пусть отображение $f : K \times S \to S$, $|K| = |S|$, удовлетворяет условию (1) и при некотором $a_0 \in K$ отображение $\varphi = f_{a_0} : K \to S$ является взаимно однозначным. Тогда:

1) бинарная операция $\tilde{f} : K \times K \to K$, определяемая равенством

$$\tilde{f}(x, z) = \varphi^{-1}(f(x, \varphi(z))), \quad x, z \in K,$$

является сильно зависимой и удовлетворяет тождеству

$$\tilde{f}(x, \tilde{f}(y, z)) = \tilde{f}(y, \tilde{f}(x, z)) \tag{2}$$

при всех $x, y, z \in K$;

2) найдутся коммутативный моноид $(K, \circ)$ и подстановка $\sigma \in S(K)$, такие, что для сильно зависимой операции $\tilde{f}$ выполнены тождества

$$\tilde{f}(x, z) = \sigma(x \circ \sigma^{-1}(z)),$$
$$\tilde{f}(x, \tilde{f}(y, z)) = \sigma(x \circ y \circ \sigma^{-1}(z))$$

при всех $x, y, z \in K$;

3) при этом для функции f выполнены тождества

$$f(x, a) = (\sigma\varphi)(x \circ (\sigma\varphi)^{-1}(a)),$$
$$f(x, f(y, a)) = (\sigma\varphi)(x \circ y \circ (\sigma\varphi)^{-1}(a))$$

при всех $x, y \in K, a \in S$. Единицей моноида $(K, \circ)$ является элемент $y_0 = \varphi^{-1}(a_0) = f_{a_0}^{-1}(a_0)$.

Доказательство.

1) Для сюръективного отображения $f_{a_0} : K \to S$ найдётся элемент $y_0 \in K$, удовлетворяющий условию $\varphi(y_0) = f(y_0, a_0) = a_0$. Тогда в силу условия (1) выполняется равенство

$$f(x, a_0) = f(x, f(y_0, a_0)) = f(y_0, f(x, a_0)),$$

или

$$\varphi(x) = f(x, \varphi(y_0)) = f(y_0, \varphi(x)),$$

а значит, $f(y_0, a)$ является тождественным отображением по второй переменной. Поэтому операция $\tilde{f}$ является сильно зависимой. Производя замену $a = \varphi(z)$, $z \in K$, в тождестве (1) и учитывая взаимную однозначность отображения φ, получаем тождество (2):

$$\begin{gathered}\tilde{f}(x, \tilde{f}(y, z)) = \varphi^{-1}(f(x, \varphi(\tilde{f}(y, z)))) = \varphi^{-1}(f(x, f(y, \varphi(z)))) = \\ = \varphi^{-1}(f(y, f(x, \varphi(z)))) = \varphi^{-1}(f(y, \varphi(\tilde{f}(x, z)))) = \tilde{f}(y, \tilde{f}(x, z)).\end{gathered}$$

2) Пусть $\tilde{g}(x, y) = \tilde{f}(y, x)$, $x, y \in K$. Тождество (2) можно переписать в виде

$$\tilde{f}(x, \tilde{g}(z, y)) = \tilde{g}(\tilde{f}(x, z), y),$$

где $x, y, z \in K$. Обозначим функцию, стоящую в левой и правой частях этого тождества, через Ф. Согласно теореме о решении уравнения общей ассоциативности из [2], должны существовать подстановки $\pi, \alpha, F_1, F_2, F_3 \in S(K)$ и моноид $(K, *)$, для которых выполняются тождества

$$\begin{gathered}\Phi(x, z, y) = \pi(F_1(x) * F_2(z) * F_3(y)), \\ \tilde{g}(x, y) = \pi(\alpha(x) * F_3(y)), \\ \tilde{f}(x, z) = \alpha^{-1}(F_1(x) * F_2(z)), \\ \tilde{f}(x, z) = F_1(x) * z, \\ \tilde{g}(z, y) = \pi(F_2(z) * F_3(y)),\end{gathered}$$

где $x, y, z \in K$, причём операция $*$ определена однозначно с точностью до изоморфизма. Достаточно ограничиться случаем, когда π является тождественной подстановкой, в противном случае надо перейти к изоморфной бинарной операции $\tilde{*}$ вида $x \,\tilde{*}\, y = \pi(\pi^{-1}(x) * \pi^{-1}(y))$, $x, y \in K$, а вместо сомножителей $F_i(.)$ рассмотреть $\pi(F_i(.))$, $i = 1, 2, 3$. Из предпоследнего тождества получаем

$$\begin{gathered}\tilde{f}(x, z) = F_1(x) * z, \\ \tilde{f}(x, \tilde{f}(y, z)) = F_1(x) * F_1(y) * z,\end{gathered}$$

где $x, y, z \in K$. Остаётся перейти к изоморфной операции $\circ$, определённой равенством $x * y = F_1(F_1^{-1}(x) \circ F_1^{-1}(y))$:

$$\begin{gathered}\tilde{f}(x, z) = F_1(x \circ F_1^{-1}(z)), \\ \tilde{f}(x, \tilde{f}(y, z)) = F_1(x \circ y \circ F_1^{-1}(z)),\end{gathered}$$

где $x, y, z \in K$, и положить $\sigma = F_1$.

Коммутативность моноида $(K, \circ)$ вытекает из условия (1) и тождества

$$F_1(x \circ y \circ F_1^{-1}(z)) = F_1(y \circ x \circ F_1^{-1}(z)).$$

Действительно, при подстановке в это тождество $z = z_0$, такого, что $F_1^{-1}(z) = e$ (единицы моноида), получаем $F_1(x \circ y) = F_1(y \circ x)$.

3) Имеем $f(x, a) = \varphi(\tilde{f}(x, \varphi^{-1}(a)))$, где $x \in K, a \in S$, откуда

$$f(x, a) = \varphi(\tilde{f}(x, \varphi^{-1}(a))) = \varphi(\sigma(x \circ \sigma^{-1}(\varphi^{-1}(a)))) = (\sigma\varphi)(x \circ (\sigma\varphi)^{-1}(a)),$$
$$f(x, f(y, a)) = (\sigma\varphi)(x \circ y \circ (\sigma\varphi)^{-1}(a))$$

при всех $x, y, z \in K$.

Покажем, что единицей моноида $(K, \circ)$ является элемент $y_0 = f_{a_0}^{-1}(a_0)$. Элемент y_0 выбран из условия выполнения равенства $f(y_0, a_0) = a_0$. С другой стороны, $a_0 = f(y_0, a_0) = (\sigma\varphi)(y_0 \circ (\sigma\varphi)^{-1}(a_0))$, откуда получаем $(\sigma\varphi)^{-1}(a_0) = y_0 \circ (\sigma\varphi)^{-1}(a_0)$. Поскольку элемент a_0 обратим, а моноид обладает единственной единицей, то $y_0 = e$, что и доказывает нужное утверждение.

Теорема 2 доказана. ■

Замечание 1. Данная конструкция является основным примитивом при построении протоколов выработки общего ключа, но поскольку она, как и основной протокол Диффи — Хеллмана, является уязвимой к атакам типа «противник в середине», для защиты от этих и подобных атак её необходимо дополнить вспомогательными конструкциями для обеспечения таких свойств протокола, как аутентификация сторон, аутентификация ключа, подтверждение правильности вычисления ключа и т. п.

Пример 1. Стандартный протокол Диффи — Хеллмана получается при $K = \mathbb{Z}_{p-1} = \{0, 1, \ldots, p-2\}$, $S = \mathbb{Z}_p^* = \{1, \ldots, p-1\}$ и $f(x, a) = a^x \bmod p$, где a — обратимый элемент поля $\mathbb{Z}_p$. Обратимое отображение φ задаётся выражением $\varphi(x) = f(x, a_0) = a_0^x \bmod p$, где a_0 — примитивный элемент поля $\mathbb{Z}_p$, при этом $\varphi^{-1}(a) = \log_{a_0} a \in \mathbb{Z}_{p-1}$. Соответствующая сильно зависимая функция на множестве $K = \mathbb{Z}_{p-1}$ после замены переменной $a = \varphi(z)$ имеет вид

$$\tilde{f}(x, z) = \varphi^{-1}(f(x, \varphi(z))) = \log_{a_0}(\varphi(z)^x \bmod p) = \log_{a_0}((a_0^z)^x \bmod p) = z \cdot x \in \mathbb{Z}_{p-1},$$

причём функция f может быть записана в виде

$$f(x, a) = \varphi(\tilde{f}(x, \varphi^{-1}(a))) = a_0^{x\varphi^{-1}(a)} \bmod p = \varphi(x\varphi^{-1}(a)),$$

где $(\cdot)$ — операция умножения кольца $\mathbb{Z}_{p-1}$. Поскольку число $p-1$ составное, полугруппа $(\mathbb{Z}_{p-1}, \cdot)$ имеет делители нуля. Поэтому при практическом использовании следует выбирать элементы $x, y \in K$ отличными от нуля, а в конце проверять условие $f(x, f(y, a)) \neq 1$.

Пример 2. Другой пример построения протокола Диффи — Хеллмана основан на использовании циклической группы простого порядка. По аналогии с предыдущим примером будем использовать мультипликативную запись, чтобы подчеркнуть имеющиеся отличия. Пусть $\mathbb{Z}_p^* = \{1, \ldots, p-1\}$ и $H = \langle h_0 \rangle = \{h_0^0, h_0^1, \ldots, h_0^{p-1}\}$ — циклическая группа простого порядка p, $h_0^p = e$, где e — нейтральный элемент группы H. Заметим, что $h_0^0 = e$ — неподвижная точка группы $\mathbb{Z}_p^*$. Пусть $K = \mathbb{Z}_p^*$ и $S = \{h_0^1, \ldots, h_0^{p-1}\}$, $|K| = |S| = p-1$, причём действие группы $\mathbb{Z}_p^*$ на S регулярно. Поэтому функция $f(x, a) = a^x$, где $x \in K$, $a \in S$, также удовлетворяет условиям теоремы 2. Здесь

$f(x,a)$ при всех $a \in S$ задаёт взаимно однозначное отображение $K \to S$. Если выбрать $\varphi(x) = f(x,h_0) = h_0^x$, $\varphi^{-1}(a) = \log_{h_0} a \in K$, то

$$f(x,a) = \varphi(\tilde{f}(x,\varphi^{-1}(a))) = \varphi(x \cdot \varphi^{-1}(a)) = h_0^{x\cdot\varphi^{-1}(a)} = a^x,$$

где $(\cdot)$ — операция умножения группы $\mathbb{Z}_p^*$. Соответствующая сильно зависимая функция $\tilde{f}$ на множестве $K = \mathbb{Z}_p^*$ после замены переменной $a = \varphi(z)$ имеет вид

$$\tilde{f}(x,z) = \varphi^{-1}(f(x,\varphi(z))) = \log_{h_0}((h_0^z)^x) = z \cdot x \in K.$$

Пример 3. Пусть $(K,\circ)$ — коммутативный моноид с левым действием на множестве S. Если обозначить действие моноида K на множестве S как $f(x,a) = x(a)$, то при всех $x,y \in K$, $a \in S$ получаем

$$f(x,f(y,a)) = (x \circ y)(a).$$

Свойства протокола определяются свойствами этого действия. В частности, необходимо, чтобы оно было точным и совпадали порядки $|K| = |S|$.

Пример 4. Некоммутативный медиальный моноид $(K,\circ)$ позволяет построить протокол, который обобщает стандартный протокол Диффи — Хеллмана. Как показано в п. 2, для такого моноида выполняется свойство перестановочности степеней

$$(a^n)^m = (a^m)^n,$$

где $a \in K$, а m,n — натуральные числа. Более подробно такой протокол описан ниже.

Пример 5. В работе [3] предлагается для построения протокола использовать неассоциативную лупу Муфанг. Это группоид $(X,\cdot)$, удовлетворяющий одному из тождеств

$$\begin{gathered}((x\cdot yz)x = xyzx,\\ x(yz\cdot x) = xy\cdot zx,\\ x(y\cdot xz) = (xy\cdot x)z,\\ (zx\cdot y)x = z(K_1\cdot yx),\end{gathered}$$

где $x,y,z \in X$. Квазигруппа, удовлетворяющая любому из этих тождеств, является лупой. Два последних тождества выделяют класс коммутативных луп. Для лупы Муфанг имеет место ассоциативность степеней, т. е. значение произведения $a\cdot a\cdot\ldots\cdot a$ не зависит от расстановки скобок. Это даёт возможность построить обобщение протокола Диффи — Хеллмана. Один из практических вариантов такого протокола описан в [3].

1.2. Случай разных функций

Рассмотрим теперь более общий вариант предыдущего протокола, когда у сторон имеются различные отображения $f : K_1 \times S \to S$, $g : K_2 \times S \to S$, $|K_1| = |K_2| = |S|$ и при этом выполняется условие

$$f(x,g(y,a)) = g(y,f(x,a)) \tag{3}$$

при всех $x \in K_1$, $y \in K_2$ и $a \in S$. Предположим, что хотя бы для одного элемента $a_0 \in S$ и одного $b_0 \in S$ отображения $f_{a_0} : K_1 \to S$ и $g_{b_0} : K_2 \to S$ являются взаимно однозначными.

Теорема 3. Пусть отображения $f : K_1 \times S \to S$ и $g : K_2 \times S \to S$ удовлетворяют условию (3), при некоторых $a_0 \in K_1$ и $b_0 \in S$ отображения $\varphi = f_{a_0}$ и $\psi = g_{b_0}$ являются взаимно однозначными и $\tau : K_1 \to K_2$ — биекция из условия $\psi\tau = \varphi$. Тогда:

1) бинарные операции $\tilde{f}, \tilde{g} : K_1 \times K_1 \to K_1$, определяемые равенствами

$$\tilde{f}(x,u) = \varphi^{-1}(f(x,\varphi(u))),\ x,u \in K_1,$$
$$\tilde{g}(x,u) = \varphi^{-1}(g(\tau(x),\varphi(u))),\ y,z \in K_1,$$

являются сильно зависимыми на множестве K_1 и удовлетворяют тождеству

$$\tilde{f}(x,\tilde{g}(y,z)) = \tilde{g}(y,\tilde{f}(x,z)) \tag{4}$$

при всех $x,y,z \in K_1$;

2) найдутся коммутативный моноид $(K_1,*)$, подстановки $\sigma,\beta \in S(K_1)$ и элемент $c \in K_1$, такие, что для сильно зависимых операций $\tilde{f}$ и $\tilde{g}$ выполнены тождества

$$\tilde{f}(x_1,z) = \sigma(x_1) * z,$$
$$\tilde{g}(x_2,x_3) = x_3 * c * \beta(x_2),$$
$$\tilde{f}(x_1,\tilde{g}(x_2,x_3)) = \sigma(x_1) * x_3 * c * \beta(x_2)$$

при всех $x_1,x_2,x_3,z \in K_1$;

3) при этом для функций f и g выполнены тождества

$$f(x,a) = \varphi(\sigma(x) * \varphi^{-1}(a)),$$
$$g(y,a) = \varphi(\varphi^{-1}(a) * c * \beta(\tau^{-1}(y))), \tag{5}$$
$$f(x,g(y,a)) = \varphi(\sigma(x) * \varphi^{-1}(a) * c * \beta(\tau^{-1}(y)))$$

при всех $x \in K_1$, $y \in K_2$, $a \in S$.

Единицей моноида $(K_1,*)$ является $\sigma(y_0)$, где элемент y_0 выбирается из условия $\varphi(y_0) = f(y_0,a_0) = a_0$.

Доказательство. Проводится аналогично доказательству теоремы 2 с учётом различия функций f и g:

1) Для сюръективного отображения $g_{b_0} : K_2 \to S$ найдётся элемент $y_0 \in K_2$, удовлетворяющий условию $\psi(y_0) = g(y_0,b_0) = a_0$. Тогда в силу условия (3) выполняется равенство

$$\varphi(x) = f(x,a_0) = f(x,g(y_0,b_0)) = g(y_0,f(x,b_0)),$$

а значит, $g(y_0,s)$ является подстановкой на множестве S.

Пусть $\tau : K_1 \to K_2$ — биекция из условия $\psi\tau = \varphi$. Производя у функции g замену переменных, получаем, что функция $\tilde{g}(x,v) = \varphi^{-1}(g(\tau(x),\varphi(v))$, $x,v \in K_1$, определена на множестве K_1 и является сильно зависимой.

Аналогично, выбирая x_0 так, чтобы $f(x_0,a_0) = b_0$, с помощью равенства

$$\psi(x) = g(y,b_0) = g(y,f(x_0,a_0)) = f(x_0,g(y,a_0))$$

можно показать, что $f(x_0,a)$ является взаимно однозначным отображением на множестве S, поэтому операция $\tilde{f}(x,u) = \varphi^{-1}(f(x,\varphi(u)))$ является сильно зависимой на K_1.

Производя замену переменных $x = x_1$, $y = \tau(x_2)$, $a = \varphi(x_3)$, $x_2,x_2,x_3 \in K_1$, в (3):

$$f(x_1,g(\tau(x_2),\varphi(x_3))) = g(\tau(x_2),f(x_1,\varphi(x_3))),$$

и переходя к функциям $\tilde{f}, \tilde{g}$, получаем тождество (4):

$$\tilde{f}(x_1, \tilde{g}(x_2, x_3)) = \varphi^{-1}(f(x_1, \varphi(\tilde{g}(\tau(x_2), x_3)))) = \varphi^{-1}(f(x_1, g(\tau(x_2), \varphi(x_3)))) =$$
$$= \varphi^{-1}(g(\tau(x_2), f(x_1, \varphi(x_3)))) = \varphi^{-1}(g(\tau(x_2), \varphi(\tilde{f}(x_1, x_3)))) = \tilde{g}(x_2, \tilde{f}(x_1, x_3)).$$

2) Обозначая через $\tilde{h}$ функцию $\tilde{h}(x_1, x_2) = \tilde{g}(x_2, x_1)$, получаем тождество

$$\tilde{f}(x_1, \tilde{h}(x_3, x_2)) = \tilde{h}(\tilde{f}(x_1, x_3), x_2).$$

Пусть Φ — функция, стоящая в левой и правой частях этого тождества. Согласно теореме о решении уравнения общей ассоциативности из [2], должны существовать подстановки $\pi, \alpha, F_1, F_2, F_3 \in S(K_1)$ и моноид $(K_1, *)$, для которых выполняются тождества

$$\begin{gathered}
\Phi(x_1, x_3, x_2) = \pi(F_1(x_1) * F_2(x_3) * F_3(x_2)), \\
\tilde{h}(z, x_2) = \pi(\alpha(z) * F_3(x_2)), \\
\tilde{f}(x_1, x_3) = \alpha^{-1}(F_1(x_1) * F_2(x_3)), \\
\tilde{f}(x_1, z) = F_1(x_1) * z, \\
\tilde{h}(x_3, x_2) = \pi(F_2(x_3) * F_3(x_2)),
\end{gathered} \tag{6}$$

где $x_1, x_2, x_3, z \in K_1$, причём операция $*$ определена однозначно с точностью до изоморфизма. Как и в теореме 2, достаточно рассмотреть случай, когда π является тождественной подстановкой, иначе надо перейти к изоморфной бинарной операции $\tilde{*}$ и вместо сомножителей $F_i(.)$ рассмотреть $\pi(F_i(.))$, $i = 1, 2, 3$.

Из равенств (6) получаем

$$\tilde{f}(x_1, z) = F_1(x_1) * z = \alpha^{-1}(F_1(x_1) * F_2(z)),$$
$$\tilde{g}(x_2, x_3) = F_2(x_3) * F_3(x_2) = \alpha(x_3) * F_3(x_2),$$

где $x_1, x_2, x_3, z \in K_1$. Отсюда $\alpha = F_2$ и $x * z = \alpha^{-1}(x * \alpha(z))$, или иначе $\alpha(x * z) = x * \alpha(z)$. Значит, $\alpha(x) = x * \alpha(e)$, где e — единица моноида $(K_1, *)$.

Обозначая $\beta = F_3$, $\sigma = F_1$ и $c = \alpha(e)$, получаем

$$\tilde{f}(x_1, z) = \sigma(x_1) * z,$$
$$\tilde{g}(x_2, x_3) = x_3 * c * \beta(x_2),$$
$$\tilde{f}(x_1, \tilde{g}(x_2, x_3)) = \sigma(x_1) * x_3 * c * \beta(x_2).$$

3) Поскольку

$$f(x, a) = \varphi(\tilde{f}(x, \varphi^{-1}(a))),$$
$$g(y, a) = \varphi(\tilde{g}(\tau^{-1}(y), \varphi^{-1}(a))),$$

где $x \in K_1$, $y \in K_2$, $a \in S$, то

$$f(x, a) = \varphi(\sigma(x) * \varphi^{-1}(a)),$$
$$g(y, a) = \varphi(\varphi^{-1}(a) * c * \beta(\tau^{-1}(y))),$$
$$f(x, g(y, a)) = \varphi(\sigma(x) * \varphi^{-1}(a) * c * \beta(\tau^{-1}(y)))$$

при всех $x \in K_1$, $y \in K_2$,$a \in S$.

Покажем, что единицей моноида $(K_1, *)$ является элемент $\sigma(y_0)$, где y_0 выбирается из условия выполнения равенства $\varphi(y_0) = f(y_0, a_0) = a_0$, т. е. $y_0 = \varphi^{-1}(a_0)$. С другой стороны, $a_0 = f(y_0, a_0) = \varphi(\sigma(y_0) * \varphi^{-1}(a_0))$, откуда получаем $\varphi^{-1}(a_0) = \sigma(y_0) * \varphi^{-1}(a_0)$. Поскольку a_0 обратим, а моноид обладает единственной единицей, то $\sigma(y_0) = e$.

Теорема 3 доказана. ■

Замечание 2. Если в п. 3 теоремы 3 вместо моноида $(K_1, *)$ использовать изоморфный моноид $(S, \circ)$ с операцией $\circ$, задаваемой равенством $x \circ y = \varphi(\varphi^{-1}(x) * \varphi^{-1}(y))$, то функции f и g можно записать в виде

$$f(x, a) = \varphi(\sigma(x)) \circ a,$$
$$g(y, a) = a * \varphi(c) \circ \varphi(\beta(\tau^{-1}(y))),$$
$$f(x, g(y, a)) = \varphi(\sigma(x)) \circ a \circ \varphi(c) \circ \varphi(\beta(\tau^{-1}(y)))$$

при всех $x \in K_1$, $y \in K_2$, $a \in S$, или в более компактной форме

$$f(x, a) = \hat{\alpha}(x) \circ a,$$
$$g(y, a) = a \circ \hat{\beta}(y),$$
$$f(x, g(y, a)) = \hat{\alpha(x)} \circ a \circ \hat{\beta}(y)$$

при $\hat{\alpha} = \sigma\varphi$, $\hat{\beta} = \tau^{-1}\beta\varphi$. Таким образом, в некоммутативном случае функции f и g задаются различными выражениями: с помощью левого и правого умножения относительно операции моноида с единицей. При этом отображения $\hat{\alpha} : K_1 \to S$ и $\hat{\beta} : K_2 \to S$ должны быть взаимно однозначными. Это следует из существования элементов a_0 и b_0 из условия теоремы 3.

Пример 6. Некоммутативный моноид $(K, *)$ с операциями, задаваемыми равенствами вида (5), может быть использован для построения протокола выработки общих ключей парной связи для любой пары (i, j) абонентов сети связи с N абонентами. Пусть i-й абонент обладает парой бинарных операций $f_i, g_i : K \times S \to S$, $|K| = |S|$, при некоторых подстановках $\alpha_i, \beta_i : K \to K$ и взаимно однозначном отображении $\varphi : K \to S$, обладающем свойством однонаправленности:

$$f_i(x, a) = \varphi(\alpha_i(x) * \varphi^{-1}(a)),$$
$$g_i(x, a) = \varphi(\varphi^{-1}(a) * \beta_i(x)), \qquad i = 1, \ldots, N.$$

Общие ключи k_{ij}, k_{ji} для направлений от i к j и от j к i вычисляются по формулам

$$k_{ij} = f_i(x_i, g_j(x_j, a)) = \varphi(\alpha_i(x_i) * \varphi^{-1}(a) * \beta_j(x_j)),$$
$$k_{ji} = f_j(x_i, g_i(x_j, a)) = \varphi(\alpha_j(x_j) * \varphi^{-1}(a) * \beta_i(x_i))$$

для случайных элементов $x_i, x_j \in K$, $a \in S$.

Пример 7. Для некоммутативных медиальных моноидов $(K, \circ)$ и $(K, *)$, операции которых удовлетворяют обобщённому тождеству медиальности, можно построить обобщение стандартного протокола Диффи — Хеллмана для случая, когда каждая из сторон использует операцию возведения в степень относительно своей бинарной операции. Более подробно такой протокол описан далее.

2. Протокол на основе медиальных бинарных операций

Сначала приведём необходимые сведения о свойстве перестановочности степеней.

2.1. Перестановочность степеней для одной бинарной операции

Пусть $Q = (X, *)$ группоид, $*$ — бинарная операция и $x \in X$. *Медиальным* называется группоид, операция которого удовлетворяет тождеству

$$(a * b) * (c * d) = (a * c) * (b * d).$$

Рассмотрим n-ю степень x^n элемента x, которая определяется индуктивно как

$$x^1 = x, \quad x^{n+1} = (x^n) * x, \ n \geqslant 1.$$

В работе [4] D. C. Murdoch заметил, что медиальные группоиды обладают свойством *перестановочности степеней* (*palintropic property*)[1].

Теорема 4 [4, Theorem 10]. Для любых элементов $x, y \in X$ медиального группоида $(X, *)$ и всех $m, n \geqslant 1$ выполнены равенства

$$(x * y)^n = x^n * y^n, \quad (x^n)^m = (x^m)^n.$$

Для некоммутативной и неассоциативной бинарной операции $*$ возможны и другие определения степени. Каждое такое произведение отличается способом расстановки скобок в последовательности $\underbrace{x * x * \ldots * x}_{n}$. Например, при $n = 3$ получаем два возможных произведения:

$$(x * x) * x, \quad x * (x * x),$$

а при $n = 4$ уже пять:

$$((x * x) * x) * x, \quad (x * (x * x)) * x, \quad (x * x) * (x * x), \quad x * ((x * x) * x), \quad x * (x * (x * x)).$$

Такие выражения называются скобочными (shapes). Общее число скобочных выражений длины m называется $(m-1)$-м числом Каталана и равно

$$A_m = \frac{1}{m}\binom{2(m-1)}{m-1}.$$

Перечисленные выше произведения можно записать в индексной форме: при $n = 3$ как $x^2 * x = x^{2+1}$ и $x * x^2 = x^{1+2}$; при $n = 4$ получаем

$$x^{(2+1)+1}, \ x^{(1+2)+1}, \ x^{2+2}, \ x^{1+(2+1)}, \ x^{1+(1+2)}.$$

Обозначим степени $(x^n)^m$ и $(x^m)^n$ как $x^{n \cdot m}$ и $x^{m \cdot n}$ соответственно. Каждое скобочное выражение можно записать как степень $x^{\mathbf{A}}$ элемента x, показатель $\mathbf{A}$ которой — формальное алгебраическое выражение над натуральными числами с использованием символов операций сложения, умножения и возведения в степень (выражается через умножение):

$$x^{\mathbf{A}+\mathbf{B}} = x^{\mathbf{A}} * x^{\mathbf{B}}, \quad x^{\mathbf{A} \cdot \mathbf{B}} = (x^{\mathbf{A}})^{\mathbf{B}}, \quad x^{\mathbf{A}^t} = \underbrace{(((x^{\mathbf{A}})^{\mathbf{A}}) \ldots)^{\mathbf{A}}}_{t},$$

[1] Ранее для медиальных группоидов использовался термин *entropoid*, а свойство медиальности называлось *entropic property* и определялось так: для всех $x, e, z, w \in G$ если $x * y = z * w$, то $x * z = y * w$.

где $\mathbf{A}, \mathbf{B} \in (\mathbb{N}; +, \cdot)$ Заметим, что в силу теоремы 4 операция умножения в показателе степени коммутативна и ассоциативна, хотя операция сложения в общем случае не является ни коммутативной, ни ассоциативной. При этом закон дистрибутивности сложения относительно умножения сохраняется:

$$x^{2(1+3)} = x^{2\cdot 1+2\cdot 3} = x^{1\cdot 2+3\cdot 2} = x^{(1+3)2}.$$

Показатель $\mathbf{A}$ называют *степенны́м индексом* (power index), или просто *индексом*. Степенны́е индексы $\mathbf{A}$ и $\mathbf{B}$ называются *эквивалентными* ($\mathbf{A} \sim \mathbf{B}$) для группоида Q, если $x^{\mathbf{A}} = x^{\mathbf{B}}$ для всех $x \in X$. Множество классов эквивалентности индексов образует факторалгебру $L_Q = (\mathbb{N}; +, \cdot)/_\sim$ с двумя бинарными операциями, которую I. M. H. Etherington [5] назвал *логарифметической* (logarithmetic). Если $X = \{x_1, x_2, \ldots, x_n\}$, то изоморфным представлением для L_Q является множество различных упорядоченных наборов вида

$$\{(x_1^{\mathbf{A}}, x_2^{\mathbf{A}}, \ldots, x_n^{\mathbf{A}}) : \mathbf{A} \in (\mathbb{N}; +, \cdot)\} \subseteq X^X,$$

которые соответствуют классам эквивалентности $[\mathbf{A}]$ отношения $\sim$ и являются табличными заданиями соответствующих отображений из множества X в множество X.

Используя такие обозначения, I. M. H. Etherington [5] доказал, что если вместо степеней элементов рассматривать произвольные скобочные выражения (степенны́е индексы), то для медиальных группоидов свойство перестановочности степеней оказывается справедливым и в этом случае.

Теорема 5 [5, Theorem 10]. Пусть $\mathbf{A}$ и $\mathbf{B}$ — произвольные степенны́е индексы. Для любых элементов $x, y \in X$ медиального группоида $(X, *)$ выполнены равенства

$$(x * y)^{\mathbf{A}} = x^{\mathbf{A}} * y^{\mathbf{A}}, \quad (x^{\mathbf{A}})^{\mathbf{B}} = (x^{\mathbf{B}})^{\mathbf{A}}.$$

В работе [6] предлагается распространение этого свойства на парамедиальные квазигруппы. В этом случае, как показали авторы, приходится уточнять свойство перестановочности степеней путём подправления индексов в правой части равенства $(x^{\mathbf{A}})^{\mathbf{B}} = (x^{\bar{\mathbf{B}}})^{\bar{\mathbf{A}}}$, где вид индексов $\bar{\mathbf{A}}$ и $\bar{\mathbf{B}}$ определяется чётностью высот деревьев, соответствующих скобочным выражениям с индексами $\mathbf{A}$ и $\mathbf{B}$.

2.2. Перестановочность степеней для двух бинарных операций

Свойство перестановочности степеней для случая, когда степени вычисляются с использованием произвольных скобочных выражений, остаётся справедливым и для двух бинарных операций, удовлетворяющих обобщённому тождеству медиальности.

Говорят, что бинарные операции $f(x, y) = x \circ y$ и $g(u, v) = u * v$ на множестве X удовлетворяют *обобщённому тождеству медиальности*, если

$$f(g(x, y), g(u, v)) = g(f(x, u), f(y, v)),$$

или иначе

$$(x * y) \circ (u * v) = (x \circ u) * (y \circ v).$$

Обозначим степени относительно каждой из операций следующим образом:

$$\begin{aligned} x^{\{n\}} &= (((x \circ x) \circ x) \circ \ldots \circ x)x = x^{\{n-1\}} \circ x, \\ y^{[m]} &= (((y * y) * y) * \ldots * y)y = y^{[m-1]} * y. \end{aligned} \tag{7}$$

Для записи степеней со степенны́ми индексами при различных бинарных операциях будем также использовать разные обозначения: $x^{\{\mathbf{A}\}}$ и $x^{[\mathbf{B}]}$.

Теорема 6 [7]. Пусть $\mathbf{A}$ и $\mathbf{B}$ — произвольные степенны́е индексы. Для любых группоидов $(X, \circ)$ и $(X, *)$, операции которых удовлетворяют обобщённому тождеству медиальности, для любых элементов $x, y \in X$ выполнены равенства

$$(x * y)^{\{\mathbf{A}\}} = x^{\{\mathbf{A}\}} * y^{\{\mathbf{A}\}}, \quad \left(x^{\{\mathbf{A}\}}\right)^{[\mathbf{B}]} = \left(x^{[\mathbf{B}]}\right)^{\{\mathbf{A}\}}.$$

2.3. Протокол для случая одной бинарной операции

В работах [8, 9] рассмотрены способы построения протокола Диффи — Хеллмана на основе использования односторонних левых и правых степеней в квазигруппах. В [10] для построения протокола предложено рассматривать уже произвольные скобочные выражения на медиальных квазигруппах. В общем случае для медиальных группоидов теорема 5 утверждает, что для всех элементов $a \in X$ медиального группоида $Q = (X, *)$ и любых степенны́х индексов $\mathbf{A}$ и $\mathbf{B}$ выполнено тождество

$$(a^{\mathbf{A}})^{\mathbf{B}} = (a^{\mathbf{B}})^{\mathbf{A}}.$$

Поэтому в качестве множества общих ключей S можно взять подгруппоид

$$S = \langle a \rangle = \{x \in X : \exists \mathbf{A}\, (x = a^{\mathbf{A}})\} \subseteq Q$$

группоида Q для некоторого элемента $a \in X$, а в качестве ключевого множества K — соответствующую логарифметическую алгебру L_S, элементами которой являются классы эквивалентности $[\mathbf{A}]$ степенны́х индексов $\mathbf{A}$ на подгруппоиде S. Если $S = \{a_0, a_1, \ldots, a_{n-1}\}$, то изоморфным представлением для $K = L_S$ является множество различных упорядоченных наборов

$$\bar{K} = \{(a_0^{\mathbf{A}}, a_1^{\mathbf{A}}, \ldots, a_{n-1}^{\mathbf{A}}) : \mathbf{A} \in K\} \subseteq S^S.$$

В нашем случае $S = \langle a \rangle$, поэтому можно полагать $(a_0, \ldots, a_{n-1}) = (a, a^{\mathbf{A}_1}, \ldots, a^{\mathbf{A}_{n-1}})$ при некоторых $\mathbf{A}_1, \ldots, \mathbf{A}_{n-1}$. Обозначим $x^{\mathbf{A}_0} = x^1 = x$. Пусть $m = |\bar{K}|$, $m \geqslant n$. Тогда все отображения из $\bar{K}$ можно представить в виде столбцов таблицы:

$\mathbf{A}_0$	$\mathbf{A}_1$	$\ldots$	$\mathbf{A}_i$	$\ldots$	$\mathbf{A}_{m-1}$
$a_1 = a$	$a^{\mathbf{A}_1}$	$\ldots$	$a^{\mathbf{A}_i}$	$\ldots$	$a^{\mathbf{A}_{m-1}}$
$a_2 = a^{\mathbf{A}_1}$	$(a^{\mathbf{A}_1})^{\mathbf{A}_1}$	$\ldots$	$(a^{\mathbf{A}_1})^{\mathbf{A}_i}$	$\ldots$	$(a^{\mathbf{A}_1})^{\mathbf{A}_{m-1}}$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
$a_j = a^{\mathbf{A}_j}$	$(a^{\mathbf{A}_j})^{\mathbf{A}_1}$	$\ldots$	$(a^{\mathbf{A}_j})^{\mathbf{A}_i}$	$\ldots$	$(a^{\mathbf{A}_j})^{\mathbf{A}_{m-1}}$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
$a_{n-1} = a^{\mathbf{A}_{n-1}}$	$(a^{\mathbf{A}_{n-1}})^{\mathbf{A}_1}$	$\ldots$	$(a^{\mathbf{A}_{n-1}})^{\mathbf{A}_i}$	$\ldots$	$(a^{\mathbf{A}_{n-1}})^{\mathbf{A}_{m-1}}$

Элементы первого столбца повторяются в первой строке таблицы. Поскольку в первом столбце выписаны все различные элементы из $S = \langle a \rangle$ и в силу теоремы 5 каждое отображение из $\bar{K}$, соответствующее степенно́му индексу $\mathbf{A}_i$, однозначно определяется первым элементом в соответствующем столбце, получаем $m = n$.

Поэтому $|S| = |K|$ и отображение $\varphi : K \to S$, которое ставит в соответствие каждому классу эквивалентности $[\mathbf{A}] \in L_S$ (набору $(a_0^{\mathbf{A}}, a_1^{\mathbf{A}}, \ldots, a_{n-1}^{\mathbf{A}})$) элемент $a^{\mathbf{A}}$, является взаимно однозначным на S. Тем самым условия теоремы 2 оказываются выполненными. В этом случае тождество (1), согласно теореме 2, гарантирует, что операция умножения факторалгебры L_S должна быть коммутативной с нейтральным элементом, соответствующим тождественному отображению $\mathbf{A}_0 : x \mapsto x^1$.

Заметим, что для квазигрупп Q, не имеющих нетривиальных гомоморфных образов, в которых каждый элемент является образующим, в [11] доказано, что $|L_Q| = n^{n/r}$, где $n = |X|$ — порядок квазигруппы Q; r — порядок её группы автоморфизмов.

Способ построения протокола на основе медиальных квазигрупп рассматривается в работе [12]. Показано, что для некоторых квазигрупп решение задачи обобщённого дискретного логарифмирования (GDLP) требует больше квантовых вентилей при использовании гипотетического квантового вычислителя, чем для решения задачи дискретного логарифмирования (DLP) в абелевой группе того же порядка.

Автором [10] замечено, что эффективный квантовый алгоритм Шора, позволяющий решать задачу DLP для коммутативных групп, основан на использовании бинарного алгоритма возведения в степень путём последовательного возведения в квадрат. Но этот алгоритм работает только для коммутативных и ассоциативных операций умножения. Поэтому при использовании некоммутативных и неассоциативных операций требуется использовать другие подходы. Однако в работе [13] L. Panny заметил, что для любой медиальной бинарной операции $*$ на X в силу теоремы К. Тойода можно определить на X абелеву групповую операцию $\cdot$, такую, что при некоторых попарно коммутирующих автоморфизмах σ, τ группы $(X, \cdot)$ и некотором $b \in X$ выполняется равенство

$$x_1 * x_2 = x_1^{\sigma} \cdot x_2^{\tau} \cdot b. \tag{8}$$

Используя такое представление, он доказал, что для произвольного степенно́го индекса $\mathbf{A}$ при всех $x \in G$ степень $x^{\mathbf{A}}$ может быть записана в виде $x^{\xi} \cdot b^{\gamma}$, где $\xi, \gamma \in \mathbb{Z}[\sigma, \tau]$.

Теорема 7 [13, Lemma 2]. Для произвольного степенно́го индекса $\mathbf{A}$ при всех $x \in G$ для операции $*$ вида (8) выполнено равенство

$$x^{\mathbf{A}} = x^{1+(\sigma+\tau-1)\gamma}\, b^{\gamma},$$

где $\gamma \in \mathbb{Z}[\sigma, \tau]$. Более того, если это равенство выполнено для одного $x = a \in X$, то оно выполнено для всех $x \in \langle a \rangle$.

Таким образом, задача GDLP решения уравнения $a^{\mathbf{A}} = c$ может быть эффективно сведена к решению уравнения $a(a^{\sigma+\tau-1})^{\gamma}\, b^{\gamma} = c$ относительно неизвестного $\gamma \in \mathbb{Z}[\sigma, \tau]$.

2.4. Протокол для случая двух бинарных операций

Рассмотрим теперь вариант алгоритма типа Диффи — Хеллмана на основе двух бинарных операций $f(x, y) = x \circ y$ и $g(u, v) = u * v$ на множестве X, удовлетворяющих обобщённому тождеству медиальности. В силу теоремы 6 можно построить протокол типа Диффи — Хеллмана, в котором каждый из участников выполняет вычисления с использованием своей бинарной операции. Сначала они договариваются об образующем элементе $a \in X$. Каждый участник вырабатывает своё случайное число и производит вычисления в соответствии с (7), а затем они обмениваются полученными значениями:

$$A \to B : a^{\{n\}},$$
$$A \leftarrow B : a^{[m]}.$$

В заключение они вычисляют общий ключ $k = \left(a^{\{n\}}\right)^{[m]} = \left(a^{[m]}\right)^{\{n\}}$.

Поскольку обобщённое свойство перестановочности степеней остаётся справедливым для случая произвольной расстановки скобок в выражениях для степеней, то в предыдущем протоколе можно использовать скобочные выражения общего вида,

причём каждая сторона вычисляет выражения обобщённой степени на основе своей бинарной операции. Будем, как и выше, использовать разные обозначения $x^{\{\mathbf{A}\}}$ и $x^{[\mathbf{B}]}$ для степеней, вычисленных с помощью этих операций. Тогда такой протокол можно записать в виде

$$A \to B : a^{\{\mathbf{A}\}},$$
$$A \leftarrow B : a^{[\mathbf{B}]},$$

причём стороны вычисляют общий ключ по формулам

$$k = \left(a^{\{\mathbf{A}\}}\right)^{[\mathbf{B}]} = \left(a^{[\mathbf{B}]}\right)^{\{\mathbf{A}\}}.$$

Этот случай также может быть описан общей теоремой 3. Только здесь появляются уже два группоида $(X, \circ)$ и $(X, *)$, удовлетворяющие условию

$$S = \{x \in X : \exists \mathbf{A}\,(x = a^{\{\mathbf{A}\}})\} = \{x \in X : \exists \mathbf{B}\,(x = b^{[\mathbf{B}]})\}$$

при некоторых $a, b \in X$, и две логарифметических алгебры:

— K_1 — логарифметическая алгебра $L_S(\circ)$, элементами которой являются классы эквивалентности $\{\mathbf{A}\}$ степенны́х индексов $\mathbf{A}$ на группоиде $(S, \circ)$,

— K_2 — логарифметическая алгебра $L_S(*)$, элементами которой являются классы эквивалентности $[\mathbf{B}]$ степенны́х индексов $\mathbf{B}$ на группоиде $(S, *)$.

Если $b = a_j = a^{\{\mathbf{A}_j\}}$, то логарифметическая алгебра $L_S(*)$ описывается следующей таблицей:

$\mathbf{B}_0$	$\mathbf{B}_1$	$\dots$	$\mathbf{B}_i$	$\dots$	$\mathbf{B}_{n-1}$
$a_1 = a$	$a^{[\mathbf{B}_1]}$	$\dots$	$a^{[\mathbf{B}_i]}$	$\dots$	$a^{[\mathbf{B}_{n-1}]}$
$a_2 = a^{\{\mathbf{A}_1\}}$	$(a^{\{\mathbf{A}_1\}})^{[\mathbf{B}_1]}$	$\dots$	$(a^{\{\mathbf{A}_1\}})^{[\mathbf{B}_i]}$	$\dots$	$(a^{\mathbf{A}_1})^{[\mathbf{B}_{n-1}]}$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$a_j = a^{\{\mathbf{A}_j\}}$	$(a^{\{\mathbf{A}_j\}})^{[\mathbf{B}_1]}$	$\dots$	$(a^{\{\mathbf{A}_j\}})^{[\mathbf{B}_i]}$	$\dots$	$(a^{\{\mathbf{A}_j\}})^{[\mathbf{B}_{n-1}]}$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$a_{n-1} = a^{\{\mathbf{A}_{n-1}\}}$	$(a^{\{\mathbf{A}_{n-1}\}})^{[\mathbf{B}_1]}$	$\dots$	$(a^{\{\mathbf{A}_{n-1}\}})^{[\mathbf{B}_i]}$	$\dots$	$(a^{\{\mathbf{A}_{n-1}\}})^{[\mathbf{B}_{n-1}]}$

Для случая двух операций теорема 7 может быть переформулирована следующим образом. Согласно [7, теорема 6], сильно зависимые операции, удовлетворяющие обобщённому тождеству медиальности, должны иметь вид

$$\begin{aligned} x_1 \circ x_2 &= x_1^{\alpha} \cdot x_2^{\beta} \cdot c, \\ x_1 * x_2 &= x_1^{\sigma} \cdot x_2^{\tau} \cdot b, \end{aligned} \tag{9}$$

где $(X, \cdot)$ — коммутативный моноид; $\alpha, \beta, \sigma, \tau$ — автоморфизмы моноида $(X, \cdot)$; $c, d \in X$, удовлетворяющие соотношениям $\alpha\tau = \sigma\beta$, $\alpha\sigma = \sigma\alpha$, $\beta\tau = \tau\beta$, $c \circ d = d * c$.

Теорема 8. Для операций $\circ$ и $*$ вида (9) и для произвольных степенны́х индексов $\{\mathbf{A}\}$ и $[\mathbf{B}]$ при всех $x \in G$ выполнено равенство

$$(x^{\{\mathbf{A}\}})^{[\mathbf{B}]} = x^{1+(\sigma+\tau-1)\gamma_1+(\alpha+\beta-1)\gamma_2} \cdot b^{\gamma_1} \cdot c^{\gamma_2},$$

где $\gamma_1, \gamma_2 \in \mathbb{Z}[\alpha, \beta, \sigma, \tau]$. Более того, если это равенство выполнено для одного $x = a \in X$, то оно выполнено для всех $x \in \langle a \rangle$.

Доказательство. Представим степенно́й индекс $[\mathbf{B}]$ в виде $[\mathbf{B_1}]+[\mathbf{B_2}]$. По предположению индукции

$$\left(x^{\{\mathbf{A}\}}\right)^{[\mathbf{B_1}]} = x^{1+(\sigma+\tau-1)\gamma_1+(\alpha+\beta-1)\gamma_2}\cdot b^{\gamma_1}\cdot c^{\gamma_2},$$
$$\left(x^{\{\mathbf{A}\}}\right)^{[\mathbf{B_2}]} = x^{1+(\sigma+\tau-1)\delta_1+(\alpha+\beta-1)\delta_2}\cdot b^{\delta_1}\cdot c^{\delta_2},$$

где $\gamma_1,\gamma_2,\delta_1,\delta_2\in\mathbb{Z}[\alpha,\beta,\sigma,\tau]$. Поэтому

$$\left(x^{\{\mathbf{A}\}}\right)^{[\mathbf{B}]} = \left(x^{\{\mathbf{A}\}}\right)^{[\mathbf{B_1}]} * \left(x^{\{\mathbf{A}\}}\right)^{[\mathbf{B_2}]} =$$
$$= (x^{1+(\sigma+\tau-1)\gamma_1(\alpha+\beta-1)\gamma_2}\cdot b^{\gamma_1}\cdot c^{\gamma_2})^{\sigma}(x^{1+(\sigma+\tau-1)\delta_1+(\alpha+\beta-1)\delta_2}\cdot b^{\delta_1}\cdot c^{\delta_2})^{\tau}b =$$
$$= x^{\sigma+\tau}\cdot x^{(\sigma+\tau-1)(\gamma_1\sigma+\delta_1\tau)+(\alpha+\beta-1)(\gamma_2\sigma+\delta_2\tau)}\cdot b^{\gamma_1\sigma+\delta_1\tau}c^{\gamma_2\sigma+\delta_2\tau}\cdot b =$$
$$= x^{1+(\sigma+\tau-1)(\gamma_1\sigma+\delta_1\tau+1)+(\alpha+\beta-1)(\gamma_2\sigma+\delta_2\tau)}\cdot b^{\gamma_1\sigma+\delta_1\tau+1}\cdot c^{\gamma_2\sigma+\delta_2\tau} =$$
$$= x^{1+(\sigma+\tau-1)\xi_1+(\alpha+\beta-1)\xi_2}\cdot b^{\xi_1}\cdot c^{\xi_2},$$

где $\xi_1=\gamma_1\sigma+\delta_1\tau+1$, $\xi_2=\gamma_2\sigma+\delta_2\tau\in\mathbb{Z}[\alpha,\beta,\sigma,\tau]$. ■

Доказанные теоремы показывают, что для построения протокола желательно подобрать различные нетривиальные операции $\circ$ и $*$ вида (9). Для этого необходимо выбрать коммутативный моноид $(X,\cdot)$ с группой автоморфизмов $\mathrm{Aut}(\cdot)$, содержащей достаточно большую коммутативную подгруппу; сам моноид должен содержать большую группу обратимых элементов, чтобы при возведении элементов в высокие степени не происходило их быстрое вырождение.

3. Протокол на основе хаотического отображения

Модифицированными многочленами Чебышева (Enhanced Chebyshev polynomial) называются многочлены над кольцом $\mathbb{Z}_N$ из последовательности $T_n(x)$, $n=0,1,2,\ldots$, определяемой линейным рекуррентным соотношением второго порядка следующим образом:

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x) \bmod N,\ n\geqslant 2,$$

где $T_0=1$ и $T_1=x$. Нетрудно видеть, что многочлен $T_n(x)$ имеет степень n и может быть вычислен с использованием матричного равенства

$$\begin{bmatrix} T_n(x) \\ T_{n+1}(x)\end{bmatrix} = A^n\begin{bmatrix} T_0(x)\\ T_1(x)\end{bmatrix},\qquad A=\begin{bmatrix}0 & 1\\ -1 & 2x\end{bmatrix}.$$

Пусть $n=p$ — нечётное простое. Для $n,m\in\mathbb{N}$ многочлены $T_n(x)$ задают отображения $T_n:\mathbb{Z}_p\to\mathbb{Z}_p$, удовлетворяющие свойству

$$T_n(T_m(x)) = T_{n+m}(x) = T_m(T_n(x)) \pmod p.$$

При $x=a\in\mathbb{Z}_p$ последовательность $T_n(a)$ является линейной рекуррентной последовательностью над $\mathbb{Z}_p$ второго порядка с характеристическим многочленом $\lambda^2-2a\lambda+1$. Значения периодов последовательностей $\{u_n = T_n(a) \bmod p\}$, $a\in\mathbb{Z}_p$, $n=0,1,2,\ldots$, описывает следующая

Теорема 9 [14, Theorem 1]. Пусть p — нечётное простое; $a\in\mathbb{Z}_p$, $0\leqslant a<p$; k — период последовательности $T_n(a) \bmod p$, $n=0,1,2,\ldots$; многочлен $\lambda^2-2a\lambda+1$ имеет корни α_1,α_2. Тогда:

(i) если корни лежат в $\mathrm{GF}(p)$, то $k\,|\,(p-1)$;

(ii) если корни лежат в $\mathrm{GF}(p^2)$, то $k\,|\,(p+1)$.

Многочлены $T_n(x)$ можно использовать для построения протокола выработки общего ключа, полагая $f(n,a) = T_n(a)$, $n \in \{0,1,\ldots,p\} = K$. Элемент $a \in \mathbb{Z}_p = S$ выбирается так, что многочлен $\lambda^2 - 2a\lambda + 1$ является неприводимым. В этом случае по теореме 9 минимальный период последовательности $\{T_n(a) \bmod p : n = 1,2,\ldots\}$ является делителем числа $p+1$ и при некоторых значениях элемента a может с ним совпадать. Общий ключ вычисляется по формулам

$$k_{AB} = f(n, f(m,a)) = f(m, f(n,a)) = T_{m+n}(a) \bmod p,$$

где $m, n \in \{0,1,\ldots,p\}$ — случайные числа.

Однако этот вариант протокола не удовлетворяет условию теоремы 2, так как в данном случае не выполняется условие о существовании элемента a, для которого отображение $f_a : \mathbb{Z}_p \to \mathbb{Z}_p$ взаимно однозначно. В работе [14] отмечается, что порождаемая последовательность является симметричной, поэтому содержит не более половины различных элементов кольца $\mathbb{Z}_N$. Например, при $p = 11$ и $a = 3$ последовательность $\{u_n : n = 0,1,2,\ldots\}$ имеет период 12 [14]:

$$\mathbf{1,\ 3,\ 6,\ 0,\ 5,\ 8,\ 10,\ 8,\ 5,\ 0,\ 6,\ 3,}\ 1,3,6,0,5,8,10,8,5,0,6,3,\ldots$$

Сформулируем этот факт в виде следующей теоремы:

Теорема 10. Пусть в условиях теоремы 9 период последовательности $\{u_n = T_n(a) \bmod p : n = 0,1,2,\ldots\}$ равен k, $1 \leqslant k \leqslant p+1$. Тогда:

(i) $u_i = u_{k+1-i}$, $1 \leqslant i \leqslant k$;

(ii) в последовательности $\{u_n\}$ встречается не более $\lceil k/2 \rceil$ различных элементов.

Доказательство. Если последовательность $\{u_n\}$ выписать в обратном порядке, то можно заметить, что она также образует линейную рекуррентную последовательность

$$u_{n-2}(x) = 2au_{n-1}(x) - u_n(x) \mod p, \qquad n = p+1, p, \ldots, 1, 0,$$

с тем же характеристическим многочленом $\lambda^2 - 2a\lambda + 1$. Рассмотрим отрезок

$$u_0, u_1, \ldots, u_{k-1}, u_k. \tag{10}$$

По определению периода $1 = u_0 = u_k$, $a = u_1 = u_{k+1}$. Учитывая, что $u_{k-1} = 2au_k - u_{k+1} = 2a - a = a$, получаем, что начальные члены линейной рекуррентной последовательности

$$u_k, u_{k-1}, \ldots, u_1, u_0 \tag{11}$$

также равны 1 и a, а значит, отрезки (10) и (11) совпадают. Отсюда, очевидно, следуют утверждения (i) и (ii). ■

Автор выражает искреннюю благодарность К. Д. Лушникову за многочисленные полезные замечания.

ЛИТЕРАТУРА

1. *Артамонов В. А., Ященко В. В.* Многоосновные алгебры в системах открытого шифрования // УМН. 1994. Т. 49. Вып. 4. С. 149–150.
2. *Сохацкий Ф. Н.* Обобщение двух теорем Белоусова для сильно зависимых функций k-значной логики // Математические исследования. 1985. Т. 83. С. 105–115.
3. *Марков В. Т., Михалёв А. В., Грибов А. В. и др.* Квазигруппы и кольца в кодировании и построении криптосхем // Прикладная дискретная математика. 2012. № 4(18). С. 31–52.

4. *Murdoch D. C.* Quasi-groups which satisfy certain generalized associative laws // Amer. J. Math. 1939. V. 61. No. 2. P. 509–522.
5. *Etherington I. M. H.* Groupoids with additive endomorphisms // The Amer. Math. Monthly. 1958. V. 65. No. 8. P. 596–601.
6. *Глухов М. М., Карюк Н. А., Катышев С. Ю.* Исследование принципов применения неассоциативных алгебраических структур при синтезе асимметричных криптографических механизмов. CTCrypt 2024. `https://ctcrypt.ru/files/files/2024/04/pc/Катышев.pdf`.
7. *Черемушкин А. В.* Обобщённые тождества медиальности и парамедиальности для сильно зависимых операций // Прикладная дискретная математика. 2024. № 65. С. 21–40.
8. *Katyshev S. Yu., Markov V. T., and Nechaev A. A.* On constructing open key cryptosystems using non associative structures // VI Int. Conf. Non Assoc. Algebra and Appl. Spain, Zaragoza, 2011.
9. *Катышев С. Ю., Марков В. Т., Нечаев А. А.* Использование неассоциативных группоидов для реализации процедуры открытого распределения ключей // Дискретная математика. 2014. Т. 26. № 3. С. 45–64.
10. *Gligoroski D.* Entropoid Based Cryptography. Cryptology ePrint Archive. 2021. Paper 2021/469. `https://eprint.iacr.org/2021/469`.
11. *Alderson (Popova) H.* The structure of the logarithmetics of finite plain quasigroups // J. Algebra. 1974. V. 31. No. 1. P. 1–9.
12. *Baryshnikov A. V. and Katyshev S. Yu.* Key agreement schemes based on linear groupoids // Матем. вопр. криптогр. 2011. Т. 8. № 1. С. 7–12.
13. *Panny L.* Entropoids: Groups in Disguise. Cryptology ePrint Archive. 2021. Paper 2021/583. `https://eprint.iacr.org/2021/583`.
14. *Fee G. J. and Monagan M. B.* Cryptography using Chebyshev polynomials // Maple Summer Workshop. Burnaby, Canada, 2004. P. 1–15.

REFERENCES

1. *Artamonov V. A. and Yaschenko V. V.* Multibasic algebras in public key distribution systems. Russian Math. Surveys, 1994, vol. 49, no. 4, pp. 145–146.
2. *Sokhatskiy F. N.* Obobshchenie dvukh teorem Belousova dlya sil'no zavisimykh funktsiy k-znachnoy logiki [Generalization of two Belousov theorems for strongly dependent functions of k-valued logic]. Matematiceskie Issledovanija, 1985, vol. 83, pp. 105–115. (in Russian)
3. *Markov V. T., Mikhalev A. V., Gribov A. V., et al.* Kvazigruppy i kol'tsa v kodirovanii i postroenii kriptoskhem [Quasigroups and rings in coding theory and cryptography]. Prikladnaya Diskretnaya Matematika, 2012, no. 4(18), pp. 31–52. (in Russian)
4. *Murdoch D. C.* Quasi-groups which satisfy certain generalized associative laws. Amer. J. Math., 1939, vol. 61, no. 2, pp. 509–522.
5. *Etherington I. M. H.* Groupoids with additive endomorphisms. The Amer. Math. Monthly, 1958, vol. 65, no. 8, pp. 596–601.
6. *Glukhov M. M., Karyuk N. A., and Katyshev S. Yu.* Issledovanie printsipov primeneniya neassotsiativnykh algebraicheskikh struktur pri sinteze asimmetrichnykh kriptograficheskikh mekhanizmov [Study of principles of application of non-associative algebraic structures in synthesis of asymmetric cryptographic mechanisms]. CTCrypt 2024. `https://ctcrypt.ru/files/files/2024/04/pc/Катышев.pdf`. (in Russian)
7. *Cheremushkin A. V.* Obobshchennye tozhdestva medial'nosti i paramedial'nosti dlya cil'no zavisimykh operatsiy [Medial and paramedial general identities for strong dependance operations]. Prikladnaya Diskretnaya Matematika, 2024, no. 65, pp. 21–40. (in Russian)

8. *Katyshev S. Yu., Markov V. T., and Nechaev A. A.* On constructing open key cryptosystems using non associative structures. VI Int. Conf. Non Assoc. Algebra and Appl., Spain, Zaragoza, 2011.
9. *Katyshev S. Yu., Markov V. T., and Nechaev A. A.* Application of non-associative groupoids to the realization of an open key distribution procedure. Discrete Math. Appl., 2015, vol. 25, no. 1, pp. 9–24.
10. *Gligoroski D.* Entropoid Based Cryptography. Cryptology ePrint Archive, 2021, paper 2021/469, `https://eprint.iacr.org/2021/469`.
11. *Alderson* (*Popova*) *H.* The structure of the logarithmetics of finite plain quasigroups. J. Algebra, 1974, vol. 31, pp. 1–9.
12. *Baryshnikov A. V. and Katyshev S. Yu.* Key agreement schemes based on linear groupoids. Matematicheskie Voprosy Kriptografii, 2011, vol. 8, no. 1, pp. 7–12.
13. *Panny L.* Entropoids: Groups in Disguise. Cryptology ePrint Archive, 2021, paper 2021/583, `https://eprint.iacr.org/2021/583`.
14. *Fee G. J. and Monagan M. B.* Cryptography using Chebyshev polynomials. Maple Summer Workshop, Burnaby, Canada, 2004, pp. 1–15.