Math-Net.Ru

Общероссийский математический портал

А. В. Барышников, С. Ю. Катышев, Использование неассоциативных структур для построения алгоритмов открытого распределения ключей, *Матем. вопр. криптогр.*, 2018, том 9, выпуск 4, 5–30

DOI: <https://doi.org/10.4213/mvk267>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 3.85.5.30

26 апреля 2023 г., 14:13:10

МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ

2018 Т. 9 № 4 С. 5–30

УДК 512.548.2

DOI <https://doi.org/10.4213/mvk267>

Использование неассоциативных структур для построения алгоритмов открытого распределения ключей

А. В. Барышников, С. Ю. Катышев

ООО «Центр сертификационных исследований», Москва

Получено 11.V.2017

Аннотация. Изучается возможность использования неассоциативных группоидов для реализации алгоритмов открытого распределения ключей, обобщающих алгоритм Диффи–Хеллмана. Найден класс неассоциативных группоидов, обладающих свойством перестановочности степеней; для него изучаются трудоемкость возведения элемента в степень и сложность решения задачи дискретного логарифмирования, в том числе с использованием гипотетического квантового вычислителя.

Ключевые слова: алгоритмы открытого распределения ключей, неассоциативные группоиды, линейные квазигруппы, дискретное логарифмирование, метод Хеллмана, квантовый вычислитель

Application of non-associative structures to the construction of public key distribution algorithms

A. V. Baryshnikov, S. Yu. Katyshev

Certification Research Center, LLC, Moscow

Abstract. We explore the possibility of using non-associative groupoids to construct public key distribution algorithms generalizing the Diffie–Hellmann algorithm. A class of non-associative groupoids satisfying the power permutability property is founded. For this class the complexity of computing powers of an element and the complexity of discrete logarithm problem, including the possible usage of hypothetical quantum computer.

Key words: public key distribution algorithm, non-associative groupoids, linear quasigroups, discrete logarithm problem, Hellmann method, quantum computer

Citation: *Mathematical Aspects of Cryptography*, 2018, v. 9, № 4, pp. 5–30 (Russian)

© Академия криптографии Российской Федерации, 2018 г.

Введение

В работах С. Ю. Катышева, В. Т. Маркова, А. А. Нечаева [6, 16] предлагалось обобщение хорошо известного алгоритма открытого распределения ключей Диффи–Хеллмана [12], использующего циклические группы, на неассоциативные группоиды, обладающие свойством перестановочности степеней.

Алгоритм переносится на произвольный группоид $(G, *)$, в котором под правой (левой) степенью понимается

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

а единственным требованием к элементу g является выполнение равенств

$$\forall m, n \in \mathbb{N}: g^{[m][n]} = (g^{[m]})^{[n]} = (g^{[n]})^{[m]} = g^{[n][m]}. \quad (1)$$

Такой элемент g называют *элементом с перестановочными правыми степенями*, или *ППС-элементом*.

Если это тождество выполняется для всех элементов $g \in G$, то группоид $(G, *)$ называют *ППС-группоидом*. Аналогично вводятся определения ПЛС-элемента и ПЛС-группоида.

Алгоритм 1. *Выбрав (несекретный) ППС-элемент g группоида G , абоненты A и B независимо друг от друга выбирают произвольные (секретные) числа $r_A, r_B \in \mathbb{N}$ соответственно и обмениваются (по открытому каналу) элементами $g^{[r_A]}$ и $g^{[r_B]}$. Затем 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* [6], т. е. сложности решения уравнения

$$g^{[x]} = y. \quad (2)$$

Естественным обобщением данного алгоритма является использование не только правых, но и левых степеней, а точнее их комбинирования. Группоид $(G, *)$ называют *группоидом с перестановочными степенями (ПС-группоидом)*, если он является ПЛС- и ППС-группоидом, а также для любого $g \in G$ и любых $l, r \in \mathbb{N}$ выполняется равенство

$${}^{[l]}(g^{[r]}) = ({}^{[l]}g)^{[r]}.$$

Алгоритм 2. Абоненты A и B независимо друг от друга выбирают такие пары натуральных чисел r, m и s, n , что $r \leq m$, $s \leq n$, и наборы чисел соответственно

$$a_1, \dots, a_m \in \mathbb{N} \quad \text{и} \quad b_1, \dots, b_n \in \mathbb{N}.$$

После обмена сообщениями

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

абоненты A и B вырабатывают общий ключ:

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

Замечание 1. Несмотря на то что в алгоритме 2 формально не введены ограничения на параметры m и n , выбирать их слишком большими — больше мощности группоиды $|G|$ — нецелесообразно, так как при этом трудоемкость реализации алгоритма будет превосходить трудоемкость нахождения общего секретного ключа методом тотального опробования.

Согласно [6] нахождение общего секретного ключа в алгоритме 2 не сложнее решения задачи обобщенного дискретного логарифмирования, т. е. нахождения хотя бы одной пары натуральных чисел u, v и набора $(x_1, \dots, x_v)$, $x_i \in \mathbb{N}$, $i \in \overline{1, v}$, удовлетворяющих равенству

$$[x_1] \dots [x_u] g^{[x_{u+1}] \dots [x_v]} = y, \quad (3)$$

если такие существуют.

Сложность решения уравнений (2), (3) определяется выбором группоиды $(G, *)$ и его конкретной реализацией.

В этой работе для использования в алгоритмах распределения ключей предлагается класс неассоциативных группоидов — *линейные группоиды*.

Пусть $(G, \cdot)$ — произвольная конечная полугруппа с единицей e . Зафиксируем два коммутирующих автоморфизма $\sigma, \tau \in \text{Aut}(G)$ ($\sigma\tau = \tau\sigma$) и некоторый элемент $h \in G$. Тогда *линейным группоидом* будем называть множество G с операцией $*_h$:

$$x *_h y = \sigma(x) \cdot \tau(y) \cdot h.$$

Основные результаты первого раздела статьи показывают возможность использования линейных группоидов в алгоритме открытого распределения ключей.

Полученные во втором разделе результаты позволяют говорить об устойчивости данных алгоритмов к методам, предложенным в [5, 6, 11].

Показано, что для правого дискретного логарифмирования на линейных группоидах возможно использование идей методов согласования и сведения к собственным подгруппам (см., например, [6]). Описано применение метода обращения однонаправленной функции Хеллмана [14] для решения задачи обобщенного дискретного логарифмирования.

Третий раздел посвящен анализу стойкости алгоритма относительно атак, использующих гипотетический квантовый вычислитель. В этих целях исследуется возможность использования квантового вычислителя для решения задачи дискретного логарифмирования на линейном группоиде. Отметим, что для решения задачи обобщенного дискретного логарифмирования на квантовом вычислителе требуются квантовые регистры значительно большей длины, чем для логарифмирования в абелевой группе. Данное обстоятельство может иметь решающее значение при практической реализации атак такого типа.

1. Распространение алгоритма Диффи–Хеллмана на линейные группоиды

В [6] в качестве алгебраического носителя было предложено использовать класс неассоциативных группоидов, называемых медиальными.

Пусть $(G, \cdot)$ — произвольная конечная полугруппа с единицей e , $\text{Aut}(G)$ — группа автоморфизмов полугруппы $(G, \cdot)$.

Зафиксируем два коммутирующих автоморфизма

$$\sigma, \tau \in \text{Aut}(G): \sigma\tau = \tau\sigma \quad (4)$$

и зададим на G операцию $*$ условием

$$\forall x, y \in G: x * y = \sigma(x) \cdot \tau(y). \quad (5)$$

Если $(G, \cdot)$ — абелева полугруппа, то группоид $(G, *)$ называют *медиальным*.

Группоид $(G, *)$ является квазигруппой тогда и только тогда, когда $(G, \cdot)$ — группа. Такие квазигруппы относят к классу *медиальных квазигрупп* [1], т.е. квазигрупп с тождеством

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

Применение квазигрупп в криптографии для построения схем аутентификации, шифрования и однонаправленных функций обсуждалось в [2]. В [9] показано, что можно использовать квазигруппы в качестве алгебраического носителя алгоритма Диффи–Хеллмана.

В работах зарубежных криптографов [13, 15] рассматривались варианты построения алгоритмов открытого распределения ключей с помощью неассоциативных структур. В указанных работах предлагалось использовать частный случай медиальных группоидов, когда автоморфизм τ — тождественный. Медиальные группоиды использовались также для построения гомоморфных систем шифрования с открытым ключом [3].

Для медиальных группоидов в [5, 6] описан ряд методов, позволяющих снизить стойкость рассматриваемых алгоритмов, в том числе по отношению к квантовым вычислителям. При определенных условиях на автоморфизмы использование методов из [11] также приводит к снижению стойкости.

В данной работе для использования в алгоритмах распределения ключей предлагается новый класс, обобщающий медиальные группоиды — *линейные группоиды*. Линейные группоиды обладают свойствами, которые позволяют говорить о неприменимости описанных в [5, 6, 11] атак.

Введем соответствующие определения. Пусть $(G, \cdot)$ — произвольная конечная полугруппа с единицей e . Зафиксируем два коммутирующих автоморфизма

$$\sigma, \tau \in \text{Aut}(G): \sigma\tau = \tau\sigma,$$

и некоторый элемент $h \in G$. *Линейным* группоидом будем называть множество G с операцией $*_h$:

$$x *_h y = \sigma(x) \cdot \tau(y) \cdot h. \quad (6)$$

Прежде всего доказывается корректность использования линейных группоидов в алгоритмах открытого распределения ключей, а именно: перестановочность степеней и возможность эффективного возведения в степень. При доказательстве перестановочности степеней будет использоваться следующая лемма.

Лемма 1. Для любого элемента g группоиды $(G, *_h)$, для любого натурального n верны следующие равенства:

$$g^{[n]} = \sigma^{n-1}(g) \cdot \prod_{i=0}^{n-2} \sigma^i(\tau(g) \cdot h), \quad (7)$$

$$^{[n]}g = \tau^{n-1}(g) \cdot \prod_{i=0}^{n-2} \tau^i(\sigma(g) \cdot h). \quad (8)$$

Доказательство. Указанные в лемме тождества вытекают непосредственно из определения операции (6). $\square$

Следующая теорема обосновывает перестановочность правых степеней в линейном группоиде $(G, *_h)$.

Теорема 1. Для любого элемента g группоида $(G, *_h)$, для любых натуральных n и k верно следующее равенство:

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

Доказательство. Пользуясь леммой 1, получаем, что для любых $k, n \in \mathbb{N}$

$$(g^{[k]})^{[n]} = \sigma^{n-1}(g^{[k]}) \cdot \prod_{i=0}^{n-2} \sigma^i(\tau(g^{[k]} \cdot h)).$$

Из коммутативности полугруппы $(G, \cdot)$ и того, что σ — гомоморфизм, следует равенство

$$(g^{[k]})^{[n]} = \sigma^{n-1}(g^{[k]}) \cdot \prod_{i=0}^{n-2} \sigma^i(h) \prod_{i=0}^{n-2} \sigma^i(\tau(g^{[k]})).$$

Используя (7), свойство коммутативности полугруппы $(G, \cdot)$ и перестановочность автоморфизмов σ и τ , получаем:

$$\begin{aligned} (g^{[k]})^{[n]} &= \sigma^{n+k-2}(g) \cdot \prod_{j=0}^{k-2} \sigma^{j+n-1}(\tau(g) \cdot h) \cdot \prod_{i=0}^{n-2} \sigma^i(h) \cdot \\ &\cdot \prod_{i=0}^{n-2} \sigma^{i+k-1}(\tau(g)) \cdot \prod_{i=0}^{n-2} \prod_{j=0}^{k-2} \sigma^{i+j}(\tau(\tau(g) \cdot h)). \end{aligned}$$

Выделим в произведении выражение, содержащее элемент h :

$$\begin{aligned} (g^{[k]})^{[n]} &= \sigma^{n+k-2}(g) \cdot \prod_{j=0}^{k-2} \sigma^{j+n-1}(\tau(g)) \cdot \prod_{i=0}^{n-2} \sigma^{i+k-1}(\tau(g)) \cdot \prod_{i=0}^{n-2} \prod_{j=0}^{k-2} \sigma^{i+j}(\tau^2(g)) \cdot \\ &\cdot \prod_{i=0}^{n-2} \sigma^i(h) \cdot \prod_{j=0}^{k-2} \sigma^{j+n-1}(h) \prod_{i=0}^{n-2} \prod_{j=0}^{k-2} \sigma^{i+j}(\tau(h)). \end{aligned}$$

После перегруппировки множителей

$$(g^{[k]})^{[n]} = \sigma^{n+k-2}(g) \cdot \prod_{j=0}^{k-2} \sigma^{j+n-1}(\tau(g)) \cdot \prod_{i=0}^{n-2} \sigma^{i+k-1}(\tau(g)) \cdot \prod_{i=0}^{n-2} \prod_{j=0}^{k-2} \sigma^{i+j}(\tau^2(g)) \cdot \prod_{t=0}^{n+k-3} \sigma^i(h) \prod_{i=0}^{n-2} \prod_{j=0}^{k-2} \sigma^{i+j}(\tau(h)) \quad (9)$$

нетрудно видеть, что правая часть равенства (9) симметрична относительно k и n . Следовательно g — ППС-элемент. $\square$

Левые степени элементов группоида также обладают свойством перестановочности.

Теорема 2. Для любого элемента g группоида $(G, *_h)$, для любых натуральных n и k верно следующее равенство:

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

Доказательство. Теорема доказывается аналогично теореме 1. $\square$

Кроме того, для группоида $(G, *_h)$ имеет место перестановочность степеней.

Теорема 3. Для любого элемента g группоида $(G, *_h)$, для любых натуральных n и k верно следующее равенство:

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

Доказательство. Применяя лемму 1, находим, что для любых $k, n \in \mathbb{N}$

$$^{[k]}(g^{[n]}) = \tau^{k-1}(g^{[n]}) \cdot \prod_{i=0}^{k-2} \tau^i(\sigma(g^{[n]}) \cdot h).$$

Из коммутативности полугруппы $(G, \cdot)$ и свойства гомоморфизма τ следует, что

$$^{[k]}(g^{[n]}) = \tau^{k-1}(g^{[n]}) \cdot \prod_{i=0}^{k-2} \tau^i(h) \cdot \prod_{i=0}^{k-2} \tau^i(\sigma(g^{[n]})).$$

Используя (7) и коммутативность полугруппы $(G, \cdot)$, получаем:

$$\begin{aligned} [k](g^{[n]}) &= \tau^{k-1} \sigma^{n-1}(g) \cdot \prod_{j=0}^{n-2} \tau^{k-1} \sigma^j(\tau(g) \cdot h) \cdot \prod_{i=0}^{k-2} \tau^i(h) \cdot \\ &\quad \cdot \prod_{i=0}^{k-2} \tau^i \sigma^{n-1}(\sigma(g)) \cdot \prod_{i=0}^{k-2} \prod_{j=0}^{n-2} \tau^i \sigma^j(\sigma \tau(g) \cdot h). \end{aligned}$$

Ввиду перестановочности автоморфизмов σ и τ

$$\begin{aligned} [k](g^{[n]}) &= \sigma^{n-1} \left(\tau^{k-1}(g) \cdot \prod_{i=0}^{k-2} \tau^i(\sigma(g) \cdot h) \right) \cdot \\ &\quad \cdot \prod_{j=0}^{n-2} \sigma^j \left(\tau \left(\tau^{k-1}(g) \cdot \prod_{i=0}^{k-2} \tau^i(\sigma(g) \cdot h) \right) \cdot h \right). \end{aligned}$$

Пользуясь леммой 1, находим, что

$$[k](g^{[n]}) = \sigma^{n-1}([k]g) \cdot \prod_{j=0}^{n-2} \sigma^j(\tau([k]g) \cdot h) = ([k]g)^{[n]}. \quad \square$$

Приведенные теоремы являются обоснованием корректности алгоритмов 1 и 2, построенных на линейных группоидах.

Для эффективной реализации этих алгоритмов необходимо, чтобы трудоемкость возведения элемента в степень была существенно ниже сложности дискретного логарифмирования. Заметим, что задачу возведения в степень в группоиде $(G, *_h)$ можно свести к возведению в степень в медиальном группоиде $(G, \star)$, где операция $\star$ задана соотношением

$$\forall x, y \in G: x \star y = \sigma(x) \cdot y, \quad (10)$$

т. е. является частным случаем операции $*$, заданной соотношением (6).

Предложение 1. Если g — обратимый элемент полугруппы $(G, \cdot)$, то при любом $n \in \mathbb{N}$ справедливо равенство

$$g^{[*_h n]} = \alpha^{[\star(n-1)]} \cdot g, \quad \alpha = \sigma(g) \tau(g) h g^{-1}. \quad (11)$$

Доказательство. Проведем доказательство индукцией по n . При $n = 2$ имеем:

$$g^{[*_h 2]} = \sigma(g)\tau(g)h = \sigma(g)\tau(g)hg^{-1}g = (\sigma(g)\tau(g)hg^{-1}) \cdot g = \alpha \cdot g.$$

Пусть утверждение верно для $n = k \geq 2$. Покажем, что оно верно для $n = k + 1$. По определению

$$g^{[*_h k+1]} = g^{[*_h k]} *_h g = \sigma(g^{[*_h k]})\tau(g)h.$$

Отсюда и из предположения индукции следует, что

$$g^{[*_h(k+1)]} = \sigma(\alpha^{[*^{(k-1)}]}g)\tau(g)h = \sigma(\alpha^{[*^{(k-1)}]})\tau(g)h \cdot (g^{-1}g).$$

Воспользовавшись свойством ассоциативности операции в полугруппе, получаем:

$$g^{[*_h(k+1)]} = \sigma(\alpha^{[*^{(k-1)}]})(\sigma(g)\tau(g)hg^{-1}) \cdot g = (\alpha^{[*^{(k-1)}]} \star \alpha) \cdot g = \alpha^{[*^k]} \cdot g. \quad \square$$

Данное предложение позволяет применять описанные в [6] алгоритмы возведения элементов линейного группоида $(G, *_h)$ в степень n со сложностью $O(\text{Aut}(\sigma, n) \cdot \log_2 n)$, где $\text{Aut}(\sigma, n)$ — трудоемкость вычисления $\sigma^n(a)$, a — произвольный элемент группоида. Если автоморфизмы заданы действием на образующих элементах, то оценка приобретает вид $O(\log_2^2 n)$. В случае если автоморфизмы σ , τ имеют небольшой по сравнению с мощностью группы порядок, эта величина становится равной оценке сложности реализации протокола Диффи–Хеллмана.

Дадим определения некоторых числовых характеристик элементов, введенных в [6].

Правым потенциалом (левым потенциалом) элемента g произвольного группоида $(\Omega, *)$ называется наибольшее такое $t \in \mathbb{N}$, что все элементы $g, g^{[2]}, \dots, g^{[t]}$ (соответственно $g, {}^{[2]}g, \dots, {}^{[t]}g$) различны. Будем обозначать эту величину $\text{pot}_r g$ (соответственно $\text{pot}_l g$) или $\text{pot}_{r*} g$, когда необходимо подчеркнуть зависимость от операции $*$.

Также определим *правый дефект* $D_r(g)$ и *правый период* $T_r(g)$ элемента g соответственно как дефект и период последовательности $g^{\mathbb{N}}$:

$$D_r(g) = \min \{l \in \mathbb{N}_0 : \exists t \in \mathbb{N} \forall i \in \mathbb{N} \quad g^{[l+i+t]} = g^{[l+i]}\},$$

$$T_r(g) = \min \{t \in \mathbb{N} : \forall i \in \mathbb{N} \quad g^{[D_r(g)+i+t]} = g^{[D_r(g)+i]}\}.$$

Аналогично определим левые дефект $D_l(g)$ и период $T_l(g)$.

Приведем следствия хорошо известных свойств периодических последовательностей из [6].

Предложение 2 ([6]). Пусть g — элемент произвольного конечного группоида $(\Omega, *)$. Тогда:

- 1) если $t, t' \in \mathbb{N}$ и $t' > t$, то $g^{[t]} = g^{[t']} \Leftrightarrow t \geq D_r(g), T_r(g) | t' - t$,
- 2) $D_r(g) + T_r(g) \leq |\Omega|$ ($D_l(g) + T_l(g) \leq |\Omega|$).

Элемент $g \in \Omega$ будем называть *реверсивным (справа)*, если $D_r(g) = 0$, т. е. $g^{[t+1]} = g$ для некоторого $t \in \mathbb{N}$, или, другими словами, $T_r(g) = \text{pot}_r(g)$.

Из предложения 2 видно, что функция «потенциал» для реверсивных элементов группоида обладает свойством, аналогичным основному свойству функции «порядок» для элементов группы.

Предложение 3 ([6]). Пусть g — реверсивный элемент группоида $(\Omega, *)$. Тогда

$$\forall t, t' \in \mathbb{N} : g^{[t]} = g^{[t']} \Leftrightarrow \text{pot}_r g | t' - t.$$

Таким образом, в нашем случае вместо порядков элементов будут оцениваться их потенциалы.

Замечание 2. Любой обратимый элемент полугруппы $(G, \cdot)$ является реверсивным в медиальном группоиде $(G, \star)$.

Предложение 4 ([6]). Пусть $(G, \star)$ — медиальный над полугруппой $(G, \cdot)$ группоид с операцией $\star$, определенной соотношением (10). Тогда для любого обратимого $g \in G$ справедливо соотношение

$$\text{pot}_r g | \text{ord } \sigma \cdot \text{ord } g,$$

где $\text{ord } \sigma$ и $\text{ord } g$ — порядки элементов σ и g соответственно.

Предложение 5. Пусть $(G, \star_h)$ — линейный над полугруппой $(G, \cdot)$ группоид с операцией $\star_h$, определенной соотношением (6). Тогда если g и h — обратимые элементы, то

$$\text{pot}_r g | \text{ord } \sigma \cdot \text{ord } \alpha, \quad \text{где } \alpha = \sigma(g)\tau(g)hg^{-1}.$$

Доказательство. Из предложения 1 следует, что $g^{[n]} = \alpha^{[\star(n-1)]} \cdot g$. Тогда для любых натуральных m и n , $m \geq n$, верна цепочка

$$g^{[\star m]} = g^{[\star n]} \Leftrightarrow \alpha^{[\star(m-1)]} \cdot g = \alpha^{[\star(n-1)]} \cdot g \Leftrightarrow \alpha^{[\star(m-1)]} = \alpha^{[\star(n-1)]}.$$

Таким образом, $\text{pot}_r g = \text{pot}_r \alpha$.

Так как g — обратимый, то и $\alpha = \sigma(g)\tau(g)hg^{-1}$ — обратимый в полугруппе $(G, \cdot)$. Тогда $\text{pot}_r \alpha | \text{ord } \sigma \cdot \text{ord } \alpha$ по предложению 4. $\square$

Замечание 3. Ввиду симметричности операции $*_h$ относительно автоморфизмов σ и τ для произвольных $g \in G$ и натурального n верно

$$[*_h n]g = g[\tilde{*}_h n],$$

где $\tilde{*}_h$ — операция, заданная соотношением $x\tilde{*}_h y = \tau(x) \cdot \sigma(y) \cdot h$. Поэтому приведенные выше результаты справедливы и для левых степеней (с учетом замены автоморфизма σ на τ и обратно).

2. Дискретное логарифмирование на линейных группоидах

В [6] предложены модификации алгоритма Гельфонда–Шенкса и метода сведения к собственным подгруппам, позволяющие решать задачу дискретного логарифмирования в медиальных квазигруппах. В силу предложения 1 указанные методы распространяются и на линейные квазигруппы.

Для решения задачи обобщенного дискретного логарифмирования в [6] описан метод построения имитирующего отображения. В частности, рассматриваются варианты использования в качестве имитирующего отображения гомоморфизма исходной полугруппы. Такой подход имеет место, поскольку операция возведения в степень в медиальном группоиде есть гомоморфизм.

Далее будет показано принципиальное отличие линейных группоидов от медиальных: операция возведения в степень в линейном группоиде не является гомоморфизмом исходной полугруппы.

Предложение 6. Если операция возведения в произвольную правую (левую) степень $k \in \mathbb{N}$ в линейном группоиде $(G, *_h)$ является гомоморфизмом полугруппы $(G, \cdot)$, то $h^2 = h$.

Если h — обратимый элемент полугруппы $(G, \cdot)$, то операция возведения в произвольную правую (левую) степень $k \in \mathbb{N}$ в линейном группоиде $(G, *_h)$ является гомоморфизмом полугруппы $(G, \cdot)$ тогда и только тогда, когда $h = e$.

Доказательство. Если возведение в степень — гомоморфизм полугруппы $(G, \cdot)$, то

$$(ab)^{[2]} = a^{[2]}b^{[2]}.$$

Распишем левую и правую части равенства. Для произвольных элементов $a, b \in (G, *_h)$ верны цепочки равенств

$$(ab)^{[2]} = \sigma(ab)\tau(ab)h,$$

$$a^{[2]}b^{[2]} = (\sigma(a)\tau(a)h)(\sigma(b)\tau(b)h) = \sigma(ab)\tau(ab)h^2.$$

Тогда, положив $a = b = e$, получим $h = h^2$, что равносильно $h = e$, если h — обратимый элемент.

Если $h = e$ — единица полугруппы $(G, \cdot)$, то группоид $(G, *_h)$ является медиальным. В [6] доказано, что операция возведения в степень в медиальном группоиде является гомоморфизмом полугруппы $(G, \cdot)$. Следовательно, операция возведения в произвольную правую (левую) степень $k \in \mathbb{N}$ в линейном группоиде $(G, *_h)$ при $h = e$ является эндоморфизмом полугруппы $(G, \cdot)$. $\square$

Для получения верхних оценок стойкости алгоритмов открытого распределения ключей, построенных на неассоциативных группоидах, возможно использование метода Хеллмана [14]. Метод Хеллмана — вероятностный метод обращения произвольной однонаправленной функции $f(x)$, т. е. нахождения x по известному $y = f(x)$.

Рассмотрим возможность его применения к решению задачи обобщенного логарифмирования в группоидах с перестановочными степенями.

Пусть $(G, *)$ — ПС-группоид и

$$K = \{(u, v, a_1, \dots, a_v) \mid u, v \in \mathbb{N}, a_i \in \mathbb{N}, i \in \overline{1, v}\}$$

— множество наборов степеней (множество секретных ключей абонента в алгоритме 2). На множестве K введем отношение ϵ правилом

$$(u, v, a_1, \dots, a_v) \epsilon \sim (u', v', a'_1, \dots, a'_v) \Leftrightarrow [a_1] \dots [a_u] g^{[a_{u+1}] \dots [a_v]} = [a'_1] \dots [a'_{u'}] g^{[a'_{u'+1}] \dots [a'_v]}.$$

Нетрудно видеть, что отношение ϵ является отношением эквивалентности на множестве K и разбивает его на классы эквивалентных ключей. Отметим, что множество классов эквивалентности конечно и не превосходит мощности группоида G .

Пусть

$$\mathcal{G} = \{[a_1] \dots [a_u] g^{[a_{u+1}] \dots [a_v]} \mid u, v \in \mathbb{N}, a_i \in \mathbb{N}, i \in \overline{1, v}\}$$

— множество всевозможных элементов G , полученных путем возведения элемента g в некоторую степень.

Выберем пару отображений: биективное $\rho_1: \mathcal{G} \rightarrow K/\epsilon$ и инъективное $\rho_2: K/\epsilon \rightarrow K$. Через $\mathcal{K}$ обозначим множество образов для элементов K/ϵ при действии отображения ρ_2 .

Определим отображение $R: \mathcal{G} \rightarrow \mathcal{K}$ соотношением $R(g) = \rho_2(\rho_1(g))$ для любого $g \in \mathcal{G}$. Нетрудно видеть, что R является биекцией.

Определим функцию $f_g: K \rightarrow \mathcal{K}$ следующим образом:

$$f_g(u, v, a_1, \dots, a_v) = R([a_1] \dots [a_u] g^{[a_{u+1}] \dots [a_v]}).$$

Алгоритм 3.

Дано. $(G, *)$ — ПС-группоид, элементы $g, h \in G$.

Выход. Элемент $\vec{x} \in K$ — решение уравнения (3):

$$[x_1] \dots [x_u] g [x_{u+1}] \dots [x_v] = h.$$

Предварительный этап.

Шаг 1. Присвоить $i = 1$.

Шаг 2. Случайно равномерно выбрать t элементов $x_{1,0}, \dots, x_{m,0} \in K$.

Шаг 3. Пока $i \leq m$, повторять:

3.1. Вычислить i -ю цепочку по формулам:

$$x_{i,j} = f_g(x_{i,j-1}), \quad \forall j \in \overline{1, t}.$$

3.2. Записать в память пару $(x_{i,0}, x_{i,t})$.

3.3. Увеличить i : $i = i + 1$.

Оперативный этап.

Шаг 1. Присвоить $j = 0$.

Шаг 2. Вычислить $y = R(h)$.

Шаг 3.

Если значение y совпадает с $x_{i,t}$ для некоторого i , **то** вычислить $x_{i,t-j-1}$, присвоить $x = x_{i,t-j-1}$ и завершить алгоритм.

Иначе присвоить $y = f_g(y)$, $j = j + 1$ и повторить шаг 3.

Теорема 4. При условии, что на шаге 2 элементы $x_{i,0}, i \in \overline{1, m}$, выбираются из множества K случайно и равномерно, алгоритм 3 находит решение уравнения (3) с вероятностью

$$P \geq \frac{1}{|K|} \sum_{i=1}^m \sum_{j=0}^{t-1} \left(\frac{|K| - it}{|K|} \right)^{j+1}.$$

Доказательство. Введем вспомогательные множества. Пусть

$$A = \{x_{i,j}, i \in \overline{1, m}, j \in \overline{0, t-1}\}$$

— множество классов ключей во всех построенных цепочках,

$$A_0 = \emptyset, \quad A_k = \{x_{i,j}, i \in \overline{1, m-1}, j \in \overline{0, t-1}\}, \quad k \in \overline{1, m},$$

— множества классов ключей в цепочках с номерами с 0 по $k-1$,

$$A_{i,0} = \emptyset, \quad A_{i,j} = A_i \cup \{x_{i,0}, \dots, x_{i,j-1}\}$$

— множества классов ключей, построенных «до» класса $x_{i,j}$.

Через S обозначим событие, при котором класс решений уравнения (3) $x \in \mathcal{K}$ содержится в множестве A . Тогда

$$\mathbf{P}(S) = \frac{\mathbf{E}|A|}{|\mathcal{K}|} = \mathbf{E} \sum_{i=1}^m \sum_{j=0}^{t-1} \frac{I\{x_{i,j} \notin A_{i,j}\}}{|\mathcal{K}|} = \sum_{i=1}^m \sum_{j=0}^{t-1} \frac{\mathbf{P}\{x_{i,j} \notin A_{i,j}\}}{|\mathcal{K}|},$$

где $\mathbf{E}$ обозначает математическое ожидание, а $I\{A\}$ — индикатор события A . Рассмотрим каждую из вероятностей

$$\mathbf{P}\{x_{i,j} \notin A_{i,j}\} \geq \mathbf{P}\{x_{i,0} \notin A_{i,0}, x_{i,1} \notin A_{i,1}, \dots, x_{i,j} \notin A_{i,j}\}$$

по отдельности. Из свойств условных вероятностей следует

$$\begin{aligned} \mathbf{P}\{x_{i,0} \notin A_{i,0}, x_{i,1} \notin A_{i,1}, \dots, x_{i,j} \notin A_{i,j}\} &= \\ &= \mathbf{P}\{x_{i,0} \notin A_{i,0}\} \mathbf{P}\{x_{i,1} \notin A_{i,1} | x_{i,0} \notin A_{i,0}\} \dots \\ &\dots \mathbf{P}\{x_{i,j} \notin A_{i,j} | x_{i,0} \notin A_{i,0}, \dots, x_{i,j-1} \notin A_{i,j-1}\}. \end{aligned}$$

Учитывая, что ограничение f_g на множестве $\mathcal{K}$ биективно, а элементы $x_{i,0}, i \in \overline{1, m}$, выбираются из множества $\mathcal{K}$ случайно и равновероятно, получаем

$$\begin{aligned} \mathbf{P}\{x_{i,0} \notin A_{i,0}\} \cdot \dots \cdot \mathbf{P}\{x_{i,j} \notin A_{i,j} | x_{i,0} \notin A_{i,0}, \dots, x_{i,j-1} \notin A_{i,j-1}\} &= \\ = \frac{|\mathcal{K}| - |A_i|}{|\mathcal{K}|} \cdot \frac{|\mathcal{K}| - |A_i| - 1}{|\mathcal{K}|} \cdot \dots \cdot \frac{|\mathcal{K}| - |A_i| - j}{|\mathcal{K}|}. \end{aligned} \quad (12)$$

Заметим, что $|A_i| \leq (i-1)t$, а значит, каждый сомножитель (12) не меньше

$$\frac{|\mathcal{K}| - it}{|\mathcal{K}|}.$$

Следовательно,

$$\mathbf{P}\{x_{i,j} \notin A_{i,j}\} \geq \left(\frac{|\mathcal{K}| - it}{|\mathcal{K}|} \right)^{j+1}$$

и искомую вероятность можно оценить так:

$$\mathbf{P}(S) \geq \frac{1}{|\mathcal{K}|} \sum_{i=1}^m \sum_{j=0}^{t-1} \left(\frac{|\mathcal{K}| - it}{|\mathcal{K}|} \right)^{j+1}. \quad \square$$

Хеллманом [14] был найден компромисс между значениями m и t — количеством требуемой памяти и объемом проводимых вычислений. Показано, что наиболее эффективно использовать значения

$$m = t = N^{1/3},$$

где N — мощность ключевого множества. В нашем случае в качестве параметров m и t можно взять $|\mathcal{G}|^{1/3}$, это значение обеспечит вероятность $P \geq |\mathcal{G}|^{-1/3}$ нахождения решения. Тогда для реализации алгоритма потребуется $O(|\mathcal{G}|^{2/3})$ операций на предварительном этапе, $O(|\mathcal{G}|^{1/3})$ операций на оперативном этапе и $O(|\mathcal{G}|^{1/3})$ ячеек памяти. При $|\mathcal{G}|^{1/3}$ независимых реализациях алгоритма вероятность успеха станет существенно положительным числом.

Стоит отметить, что помимо вычисления цепочек на предварительном этапе требуется построение отображений ρ_1 и ρ_2 . Вопрос о построении этих отображений пока не решен.

3. Квантовые алгоритмы дискретного логарифмирования на линейных группоидах

Задача одностороннего дискретного логарифмирования в линейном группоиде может быть решена с использованием квантового вычислителя.

Приведем необходимые определения и утверждения о математической модели квантового вычислителя (подробное описание см., например, в [4]). Пусть $\mathbb{C}$ — поле комплексных чисел. Рассмотрим пространство $\mathbb{C}^{2^n}$ вектор-столбцов размерности 2^n над полем $\mathbb{C}$. Для обозначения вектор-столбца пространства $\mathbb{C}^{2^n}$ используется символ Дирака $|\psi\rangle$. Вектор, комплексно сопряженный к вектору $|\psi\rangle$, обозначается $|\psi^*\rangle$. На пространстве $\mathbb{C}^{2^n}$ естественным образом вводится операция скалярного произведения

$$\langle\psi|\varphi\rangle = \sum_{i=1}^{2^n} \psi_i^* \varphi_i = |\psi^*\rangle^T \cdot |\varphi\rangle$$

векторов

$$|\psi\rangle = (\psi_1, \dots, \psi_n)^T \quad \text{и} \quad |\varphi\rangle = (\varphi_1, \dots, \varphi_n)^T.$$

С использованием скалярного произведения стандартным образом вводятся понятия *ортogonalности векторов*, *нормы вектора* ($\| |\psi\rangle \|$), *ортонормированного базиса*, *унитарного* (сохраняющего норму вектора) *оператора* (см., например, [4]).

Для векторов стандартного базиса $(100 \dots 0 \dots 0)^T$, $(010 \dots 00 \dots 0)^T$, $\dots$, $(000 \dots 0 \dots 1)^T$ пространства $\mathbb{C}^{2^n}$ введем систему обозначений:

$$\begin{aligned} |0\rangle &= |\underbrace{0, 0, \dots, 0}_n, 0\rangle = (100 \dots 00 \dots 0)^T, \\ |1\rangle &= |0, 0, \dots, 0, 1\rangle = (010 \dots 00 \dots 0)^T, \\ &\dots \\ |i\rangle &= |i_{n-1}, \dots, i_1, i_0\rangle = (\underbrace{000 \dots 0}_i 1 \dots 0)^T, \\ &\dots \\ |2^n - 1\rangle &= |1, 1, \dots, 1, 1\rangle = (000 \dots 00 \dots 1)^T, \end{aligned} \quad (13)$$

где $(i_{n-1}, \dots, i_1, i_0)$ — двоичная запись числа i , т. е.

$$i = i_{n-1} 2^{n-1} + \dots + i_1 2^{n-2} + i_0 2^0.$$

В дальнейшем все вычисления будут производиться именно в этом базисе.

Заметим, что справедливо следующее разложение вектора $|i\rangle \in \mathbb{C}^{2^n}$ в тензорное произведение:

$$|i\rangle = |i_{n-1}, \dots, i_1, i_0\rangle = |i_{n-1}\rangle \otimes \dots \otimes |i_1\rangle \otimes |i_0\rangle, \quad (14)$$

где $|i_{n-1}\rangle, \dots, |i_0\rangle$ — векторы пространства $\mathbb{C}^2$, определенные соотношением (13).

Основой для дальнейшего изложения материала служит понятие *кубит* (*quantum-bit*). С точки зрения излагаемой математической модели будем понимать под кубитом некоторую физическую систему, состояние которой есть вектор-столбец пространства $\mathbb{C}^2$, имеющий норму 1, т. е. вектор вида

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \text{где } \alpha, \beta \in \mathbb{C}, \quad |\alpha|^2 + |\beta|^2 = 1.$$

Замечание 4. Как и в случае классического бита, когда говорим о кубите, нас интересует не сама физическая система, а только значение, которое она «хранит», т. е. *состояние кубита*.

Система из n кубит называется *квантовым регистром длины n* , его состояние определяется как вектор-столбец $|\psi\rangle$ пространства $\mathbb{C}^{2^n}$, имеющий норму 1, т. е. вектор вида

$$|\psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle, \quad \text{где } \alpha_i \in \mathbb{C}, \quad \sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1. \quad (15)$$

Если квантовый регистр состоит из n кубит, находящихся в состояниях $|\psi_{n-1}\rangle, \dots, |\psi_1\rangle, |\psi_0\rangle \in \mathbb{C}^2$, то состояние квантового регистра $|\psi\rangle$ равно тензорному произведению состояний кубит:

$$|\psi\rangle = |\psi_{n-1}\rangle \otimes \dots \otimes |\psi_1\rangle \otimes |\psi_0\rangle,$$

однако не каждое состояние квантового регистра может быть представлено в таком виде, поскольку не любой вектор из пространства $\mathbb{C}^{2^n}$ представляется в виде тензорного произведения векторов из $\mathbb{C}^2$.

Пусть A — подсистема из k кубит, стоящих на местах $t_1, \dots, t_k$, U — произвольный унитарный оператор пространства $\mathbb{C}^{2^k}$. Определим *элементарное преобразование* $U[A]$ пространства $\mathbb{C}^{2^n}$, состоящее в применении оператора U к подсистеме кубит A . Обозначим через $j_1, \dots, j_{n-k}$ места оставшихся кубит. Определим линейный оператор $T: \mathbb{C}^{2^n} \rightarrow \mathbb{C}^{2^n}$, действие которого на базисных векторах $|i\rangle = |i_{n-1}\rangle \otimes \dots \otimes |i_1\rangle \otimes |i_0\rangle$, $i \in \overline{0, 2^n - 1}$, определяется соотношением

$$T(|i_{n-1}\rangle \otimes \dots \otimes |i_1\rangle \otimes |i_0\rangle) = |i_{j_{n-k}}\rangle \otimes \dots \otimes |i_{j_1}\rangle \otimes |i_{t_k}\rangle \otimes \dots \otimes |i_{t_1}\rangle. \quad (16)$$

Тогда элементарное преобразование будет состоять из «перестановки состояний кубит» при помощи оператора T , применения оператора

$$E_{2^{n-k} \times 2^{n-k}} \otimes U$$

и обратной перестановки, т. е.

$$U[A] = T^{-1}(E_{2^{n-k} \times 2^{n-k}} \otimes U)T, \quad (17)$$

где $E_{2^{n-k} \times 2^{n-k}}$ — единичная матрица.

Замечание 5. Оператор T , определяемый соотношением (16), — унитарный, более того, он реализуется как умножение вектора из $\mathbb{C}^{2^n}$ на некоторую подстановочную матрицу.

Зафиксируем некоторое множество унитарных операторов $\mathcal{U}$ (действующих, вообще говоря, на разных пространствах) и, следуя [7], будем называть его базисом.

Рассмотрим квантовый регистр длины n . *Квантовой схемой в базисе $\mathcal{U}$* будем называть последовательность элементарных преобразований $U_1[A_1], U_2[A_2], \dots, U_k[A_k]$, где каждый $U_j \in \mathcal{U}$, $A_j \subset \overline{0, n-1}$ — подмножество множества номеров кубит. Скажем, что оператор $U: \mathbb{C}^{2^n} \rightarrow \mathbb{C}^{2^n}$ реализуется данной квантовой схемой, если

$$U = U_k[A_k] \cdot \dots \cdot U_1[A_1].$$

Естественным образом (см., например, [7]) определяется полный базис.

Выбор базиса для построения квантовых схем представляет собой отдельный вопрос, выходящий за рамки данной работы (подробнее см., например, [7]). Далее будем полагать, что построение схем происходит в *стандартном базисе*, состоящем из элемента Адамара, фазового элемента, управляемого NOT, элемента Тоффли. Такой базис является полным.

Пусть F — последовательность унитарных операторов $\{F_n\}_{n \in \mathbb{N}}$. *Квантовый алгоритм для вычисления F* — это однородная последовательность квантовых схем, реализующих операторы F_n . Термин «однородная» означает, что по n можно построить описание соответствующей квантовой схемы на обычной полиномиально ограниченной машине Тьюринга. Будем говорить, что алгоритм работает с трудоемкостью (за время) $T(n)$, если квантовая схема для вычисления F_n состоит из $T(n)$ элементарных преобразований.

Замечание 6. Нетрудно показать, что выбор полного базиса для построения квантовых схем не влияет на оценку трудоемкости вида « O -большое».

Квантовым преобразованием Фурье будем называть линейный оператор, действующий на базисных векторах пространства $\mathbb{C}^{2^n}$ следующим образом:

$$|j\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i j k / 2^n} |k\rangle.$$

Трудоемкость выполнения квантового преобразования Фурье составляет $O(n^2)$ элементарных преобразований. Аналогично определяется обратное квантовое преобразование Фурье, его выполнение также требует $O(n^2)$ элементарных преобразований.

Для получения информации о состоянии регистра кубит проводится его *измерение*. Измерение — это вероятностный процесс, т. е., измеряя квантовый регистр $|\psi\rangle = \sum_i \alpha_i |i\rangle$, мы можем получить любое значение i с вероятностью $|\alpha_i|^2$.

Отметим, что можно провести измерение состояний части кубит регистра. При этом вероятности исходов измерения могут быть вычислены по формуле полной вероятности (суммирование по всем базисным векторам неизмеряемых кубит), а сама система кубит в результате измерения изменит свое состояние (см., например, [4]).

Перейдем к задаче дискретного логарифмирования. Пусть дан линейный группоид $(G, *_h)$ с операцией, заданной тождеством (6), а также элементы $g \in G$ и $y = g^{[s]} \in G$. Необходимо найти такой $x \in \mathbb{N}$, что

$$g^{[x]} = y.$$

Предложение 1 позволяет перейти от решения задачи в линейном группоиде $(G, *_h)$ к дискретному логарифмированию в медиальном группоиде $(G, \star)$, где операция $\star$ задана соотношением

$$\forall x, y \in G: x \star y = \sigma(x) \cdot y.$$

Далее под возведением в степень в квадратных скобках $g^{[t]}$ будем понимать возведение в степень в группоиде $(G, \star)$. При $k \in 0, (\text{ord } \sigma - 1)$ дополнительно определим правую степень в фигурных скобках с индексом k элемента g равенством

$$g^{\{n\}_k} = \prod_{j=0}^{n-1} \sigma^{kj}(g) = \sigma^{k(n-1)}(g) \sigma^{k(n-2)}(g) \cdot \dots \cdot g.$$

Для $k \in \overline{0, (\text{ord } \sigma - 1)}$ зададим функции $f_k: \mathbb{Z} \times \mathbb{Z} \rightarrow G$ равенством

$$f_k(x_1, x_2) = \sigma^{x_2} \left(h^{\{x_1\}_k} \right) \cdot g^{[x_2]}.$$

Предложение 7. Если $k \equiv s \pmod{\text{ord } \sigma}$, то выполнено тождество

$$f_k(x_1, x_2) = g^{[x_1 s + x_2]}.$$

Доказательство. При тождественном автоморфизме τ верно равенство

$$g^{[n+m]} = \sigma^m(g^{[n]}) \cdot g^{[m]}.$$

Тогда

$$\begin{aligned} g^{[x_1 s + x_2]} &= \sigma^{x_2} (g^{[x_1 s]}) \cdot g^{[x_2]} = \sigma^{x_2} (\sigma^{(x_1-1)s} (g^{[s]}) g^{[(x_1-1)s]}) \cdot g^{[x_2]} = \\ &= \sigma^{x_2} \left((\sigma^s)^{(x_1-1)} (g^{[s]}) (\sigma^s)^{(x_1-2)} (g^{[s]}) \cdot \dots \cdot g^{[s]} \right) \cdot g^{[x_2]}. \end{aligned}$$

Поэтому при $k \equiv s \pmod{\text{ord } \sigma}$ по определению функции f_k получаем:

$$g^{[x_1 s + x_2]} = f_k(x_1, x_2). \quad \square$$

Заметим, что для функции f_k при $k \equiv s \pmod{\text{ord } \sigma}$ и любом целом l выполняется равенство

$$f_k(x_1 + l, x_2 - l s) = f_k(x_1, x_2),$$

поэтому функция f_k , заданная на группе $\mathbb{Z} \times \mathbb{Z}$, инвариантна на смежных классах по циклической подгруппе $\langle (1, -s) \rangle$.

Пусть $|G| = N$. Перенумеруем элементы полугруппы некоторым образом. Везде далее будем считать, что вместо элемента полугруппы в квантовый регистр записывается его номер. Алгоритм работает в предположении, что правый потенциал элемента g и порядок автоморфизма σ известны.

Изложенный ниже алгоритм можно рассматривать как распространение с некоторым усложнением на неассоциативный медиальный группоид квантового алгоритма дискретного логарифмирования на абелевой группе из [17]. Обоснование корректности алгоритма будет приведено ниже.

Алгоритм 4.

Дано. $(G, \cdot)$ — полугруппа, $\sigma \in \text{Aut}(G, \cdot)$, $g, y \in G$ — обратимые элементы, r — правый потенциал элемента g .

Выход. Натуральное s , удовлетворяющее условию

$$g^{[s]} = y. \quad (18)$$

Выберем произвольное ε — вероятность ошибки алгоритма.

Необходимые квантовые элементы:

- 1) два t -кубитовых регистра, где $t = \lceil \log_2 r \rceil + \lceil \log_2(1/\varepsilon) \rceil$, установленные в состояние $|0\rangle$,
- 2) регистр длины $\lceil \log_2 N \rceil$ для записи значений функции, установленный в состояние $|0\rangle$,
- 3) черные ящики U_k для $k \in \overline{0, (\text{ord } \sigma - 1)}$, осуществляющие операцию, которая определяется на векторах вычислительного базиса следующим образом:

$$U_k |x_1\rangle |x_2\rangle |z\rangle = |x_1\rangle |x_2\rangle |z \oplus f_k(x_1, x_2)\rangle.$$

Шаг 1. Присвоить $k = 0$.

Шаг 2. Применив элемент Адамара к каждому кубиту первых двух квантовых регистров, получить состояние

$$\frac{1}{2^t} \sum_{x_1=0}^{2^t-1} \sum_{x_2=0}^{2^t-1} |x_1\rangle |x_2\rangle |0\rangle.$$

Шаг 3. Применив преобразование U_k , осуществляемое черным ящиком, к системе всех трех регистров, получить состояние

$$\frac{1}{2^t} \sum_{x_1=0}^{2^t-1} \sum_{x_2=0}^{2^t-1} |x_1\rangle |x_2\rangle |f_k(x_1, x_2)\rangle.$$

Шаг 4. Применив обратное квантовое преобразование Фурье к каждому из первых двух регистров, получить состояние

$$\frac{1}{\sqrt{r}} \sum_{l_2=0}^{r-1} |\widetilde{m/r}\rangle |\widetilde{l_2/r}\rangle |\widetilde{f_k(s_k l_2, l_2)}\rangle,$$

где $m \equiv s_k l_2 \pmod{r}$.

Шаг 5. Измерив состояния двух первых регистров, получить пару чисел

$$(\widetilde{m/r}, \widetilde{l/r}),$$

где l некоторое число от 0 до $r-1$, а $m \equiv s_k l \pmod{r}$.

Шаг 6. Применив к числам $(\widetilde{m/r}, \widetilde{l/r})$ о бобщенный метод цепных дробей [8, 10], найти числители подходящих дробей m' и l' .

Шаг 7. Решив сравнение $s_k l' \equiv m' \pmod{r}$, вычислить s_k .

Шаг 8. Непосредственно проверить s_k . Если $g^{[s_k]} \neq y$, то присвоить $k = k+1$ и при $k < \text{ord } \sigma$ перейти на шаг 1. Иначе вывести решение s_k .

Замечание 7. Числа $\widetilde{m/r}$, $\widetilde{l/r}$ на шагах 4–6 суть запись вещественных числе m/r , l/r в конечное число кубит. Для успешного нахождения $m' = m$ и $l' = l$ на шаге 6 требуется, чтобы точность измерения на шаге 5 была не менее $(2r)^{-1}$. Обоснование вероятности измерения с указанной точностью приводится при доказательстве корректности работы алгоритма.

Теорема 5. Алгоритм 4 решает уравнение (18) с вероятностью $1-\varepsilon$. Для этого используется одно обращение к каждому черному ящику U_k , $k \in \overline{1, \text{ord } \sigma}$,

$$O\left(\text{ord } \sigma \cdot \left(\log r + \log \frac{1}{\varepsilon}\right)^2\right)$$

элементарных преобразований на квантовом вычислителе и $O(\log^3 r)$ арифметических операций.

Доказательство. Пусть s — решение уравнения (18). Очевидно, что при некотором $k \in \overline{0, (\text{ord } \sigma - 1)}$ выполнено сравнение $k \equiv s \pmod{\text{ord } \sigma}$. Будем рассматривать действие алгоритма именно при этом значении k .

Состояние на втором шаге создается при воздействии на каждый из t кубит 1-го и 2-го регистров элементом Адамара, действие которого определяется умножением вектора состояния кубита на унитарную матрицу

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Пусть $|\tilde{f}_k(l_1, l_2)\rangle$ — состояние, полученное преобразованием Фурье из $|f_k(x_1, x_2)\rangle$, $x_1, x_2 \in \overline{0, (2^t - 1)}$:

$$|\tilde{f}_k(l_1, l_2)\rangle = \sum_{y_1=0}^{r-1} \sum_{y_2=0}^{r-1} e^{-2\pi i(l_1 y_1 + l_2 y_2)/r} |f_k(y_1, y_2)\rangle. \quad (19)$$

Докажем, что при $k \equiv s \pmod{\text{ord } \sigma}$ для состояния на шаге 3 будет верно равенство

$$\begin{aligned} & \frac{1}{2^t} \sum_{x_1=0}^{2^t-1} \sum_{x_2=0}^{2^t-1} |x_1\rangle |x_2\rangle |f_k(x_1, x_2)\rangle = \\ &= \frac{1}{2^t \sqrt{r}} \sum_{l_2=0}^{r-1} \left[\sum_{x_1=0}^{2^t-1} e^{2\pi i(s_k l_2 x_1)/r} |x_1\rangle \right] \left[\sum_{x_2=0}^{2^t-1} e^{2\pi i(l_2 x_2)/r} |x_2\rangle \right] |\tilde{f}_k(s_k l_2, l_2)\rangle. \end{aligned} \quad (20)$$

Так как набор состояний $|\tilde{f}_k(l_1, l_2)\rangle$, $l_1, l_2 \in \overline{0, (r-1)}$, суть преобразование Фурье от $|f_k(x_1, x_2)\rangle$, $x_1, x_2 \in \overline{0, (2^t - 1)}$, то по определению обратного преобразования Фурье

$$|f_k(x_1, x_2)\rangle = \frac{1}{\sqrt{r}} \sum_{l_1=0}^{r-1} \sum_{l_2=0}^{r-1} e^{2\pi i(l_1 x_1 + l_2 x_2)/r} |\tilde{f}_k(l_1, l_2)\rangle. \quad (21)$$

Покажем, что если $sl_2 \equiv l_1 \pmod{r}$, то вектор $|\tilde{f}_k(l_1, l_2)\rangle$ в представлении $f(x_1, x_2)$ — нулевой. Регруппируем слагаемые в правой части (19) при помощи замены $y_1 = sk_1 + k_2 \pmod{r}$, $y_2 = (k_1 - sk_2) \pmod{r}$. Эта замена является вырожденной лишь при условии $s^2 \equiv -1 \pmod{r}$, такие значения s можно проверить отдельно. Получаем:

$$|\tilde{f}_k(l_1, l_2)\rangle = \sum_{k_1=0}^{r-1} \sum_{k_2=0}^{r-1} e^{-2\pi i((sk_1+k_2)l_1+(k_1-sk_2)l_2)/r} |f(sk_1+k_2, k_1-sk_2)\rangle. \quad (22)$$

Согласно предложению 7 функция $f_k(sk_1 + k_2, k_1 - sk_2) = g^{[s^2 k_1 + k_1]}$ не зависит от k_2 . Вынесем из суммы в правой части (22) общий множитель, не зависящий от k_2 :

$$|\tilde{f}_k(l_1, l_2)\rangle = \sum_{k_1=0}^{r-1} e^{-2\pi i(sk_1 l_1 + (k_1 - s)l_2)/r} |g^{[s^2 k_1 + k_1]}\rangle \sum_{k_2=0}^{r-1} e^{-2\pi i k_2 (l_1 - sl_2)/r}. \quad (23)$$

Известно, что

$$\sum_{k_2=0}^{r-1} e^{-2\pi i k_2/r} = 0. \quad (24)$$

Поэтому из (23) и (24) следует, что если $sl_2 \not\equiv l_1 \pmod{r}$, то

$$|\tilde{f}(l_1, l_2)\rangle = (0, \dots, 0)^T$$

и равенство (21) принимает вид

$$|f_k(x_1, x_2)\rangle = \frac{1}{\sqrt{r}} \sum_{l_2=0}^{r-1} e^{2\pi i (sl_2 x_1 + l_2 x_2)/r} |\tilde{f}_k(sl_2, l_2)\rangle.$$

Отсюда получаем

$$\begin{aligned} \frac{1}{2^t} \sum_{x_1=0}^{2^t-1} \sum_{x_2=0}^{2^t-1} |x_1\rangle |x_2\rangle |f_k(x_1, x_2)\rangle &= \\ &= \frac{1}{2^t} \sum_{x_1=0}^{2^t-1} \sum_{x_2=0}^{2^t-1} \frac{1}{\sqrt{r}} \sum_{l_2=0}^{r-1} e^{2\pi i (sl_2 x_1 + l_2 x_2)/r} |x_1\rangle |x_2\rangle |\tilde{f}_k(sl_2, l_2)\rangle = \\ &= \frac{1}{2^t \sqrt{r}} \sum_{l_2=0}^{r-1} \left[\sum_{x_1=0}^{2^t-1} e^{2\pi i (sl_2 x_1)/r} |x_1\rangle \right] \left[\sum_{x_2=0}^{2^t-1} e^{2\pi i (l_2 x_2)/r} |x_2\rangle \right] |\tilde{f}_k(sl_2, l_2)\rangle, \end{aligned}$$

что и доказывает нужное равенство (20).

Таким образом, в соответствии с определением квантового преобразования Фурье на шаге 4 получим состояние

$$\frac{1}{\sqrt{r}} \sum_{l_2=0}^{r-1} |\widetilde{m/r}\rangle |\widetilde{l_2/r}\rangle |\tilde{f}_k(s_k l_2, l_2)\rangle,$$

где $m \equiv s_k l_2 \pmod{r}$.

В [10, 17] показано, что при использовании квантовых регистров длины

$$t = \lceil \log_2 r \rceil + \lceil \log_2(1/\varepsilon) \rceil$$

кубит вероятность измерения результата обратного преобразования Фурье на первых двух регистрах с точностью $(2r)^{-1}$ будет не менее $1 - \varepsilon$.

Трудоемкость метода обобщенных цепных дробей (см., например, [8]) для построения подходящей дроби с точностью $(2r)^{-1}$ есть $O(\log^3 r)$ арифметических операций.

Таким образом, трудоемкость алгоритма складывается из обращения к каждому черному ящику U_k , $k \in \overline{1, \text{ord } \sigma}$, и применения квантового преобразования Фурье $\text{ord } \sigma$ раз, что составляет

$$O(\text{ord } \sigma \cdot (\log r + \log(1/\varepsilon))^2)$$

элементарных преобразований на квантовом вычислителе и $O(\log^3 r)$ арифметических операций. $\square$

Замечание 8. В алгоритме считается, что потенциал элемента g известен. Для нахождения потенциала реверсивного элемента в линейном группоиде применим квантовый алгоритм нахождения порядка элемента в группе мощности N , имеющий трудоемкость $O(\log^2 N)$ [10, стр. 293].

Перейдем к задаче обобщенного дискретного логарифмирования. Пусть дан линейный группоид $(G, *_h)$ с операцией, заданной тождеством (6), а также элементы

$$g \in G \quad \text{и} \quad y = [s_1] \dots [s_l] g [s_{l+1}] \dots [s_n] \in G.$$

Необходимо найти хотя бы одну пару натуральных чисел u , v и набор $(x_1, \dots, x_v)$, $x_i \in \mathbb{N}$, $i \in \overline{1, v}$, удовлетворяющие равенству

$$[x_1] \dots [x_u] g [x_{u+1}] \dots [x_v] = y, \quad (25)$$

если такие существуют.

Для любого элемента g произвольного группоида $(\Omega, *)$ и любого натурального n через $I_n(g)$ обозначим множество

$$I_n(g) = \{[a_1] \dots [a_l] g [a_{l+1}] \dots [a_n] \mid l \in \{0, \dots, n-1\}, (a_1, \dots, a_n) \in \mathbb{N}^n\},$$

т.е. множество всевозможных элементов Ω , полученных при возведении g в произвольные n степеней. Будем называть *степенным индексом* элемента $g \in \Omega$ число

$$\text{pind } g = \min\{n \in \mathbb{N} : I_{n+1}(g) = I_n(g)\}.$$

Предложение 8. Для любого $g \in \Omega$:

1) если $I_{n+1}(g) = I_n(g)$ для некоторого натурального n , то

$$I_{n+t}(g) = I_n(g) \quad \forall t \in \mathbb{N},$$

2) $1 \leq \text{pind } g \leq |\Omega|$.

Доказательство. Заметим, что множество $I_{n+t}(g)$, $t, n \in \mathbb{N}$, получается из множества $I_{n+t-1}(g)$ путем возведения всех элементов $I_{n+t-1}(g)$ в одну степень слева или справа. Отсюда следует первое утверждение предложения.

Доказательство второго утверждения следует из неравенств

$$1 \leq |I_{n+1}(g) \setminus I_n(g)| \leq |\Omega|. \quad \square$$

Согласно [10] задача дискретного логарифмирования является частным случаем задачи о скрытой подгруппе, которую можно сформулировать следующим образом:

Пусть f — функция из конечно порожденной группы H в конечное множество G , постоянная на смежных классах по некоторой подгруппе K и принимающая различные значения на разных смежных классах. Найти множество образующих группы K .

Для нахождения решения уравнения (25) необходимо выбрать группу $H \subset \mathbb{Z}^m$, $m \in \mathbb{N}$, и некоторую функцию $f: H \rightarrow G$.

Предложение 9. $|H| \geq \text{pind } g \cdot \max\{\text{pot}_l g, \text{pot}_r g\}$.

Доказательство. Пусть X — множество решений уравнения (25). Выберем из X элемент $x = (u, v, x_1, \dots, x_v)$ с наименьшим количеством координат (с наименьшим значением v среди всех решений). Пусть $n = \text{pind } g$, тогда если $x \in I_n(g) \setminus I_{n-1}(g)$, то $v = n$. Значит, $m \geq n = \text{pind } g$ и, следовательно, $|H| \geq \text{pind } g \cdot \max\{\text{pot}_l g, \text{pot}_r g\}$. $\square$

При использовании квантовых алгоритмов поиска скрытой подгруппы в группе H необходимо поместить все элементы группы в квантовый регистр. Таким образом, необходим квантовый регистр для хранения элементов группы мощности не менее $\text{pind } g \cdot \max(\text{pot}_l g, \text{pot}_r g)$. Указанная величина не может превышать мощность исходной группы (см. пример 3 из [6]).

Длина необходимых квантовых регистров является одним из параметров алгоритмов на квантовых вычислителях, в том числе алгоритмов поиска скрытой подгруппы. Увеличение указанного параметра может сделать невозможным практическую реализацию алгоритмов такого типа.

Список литературы

- [1] Белявская Г. Б., Табаров А. Х., “Тождества с подстановками, приводящие к линейности квазигрупп”, *Дискретная математика*, **21**:1 (2009), 36–51.
- [2] Глухов М. М., “О применениях квазигрупп в криптографии”, *Прикл. дискр. матем.*, № 2(2) (2008), 28–32.
- [3] Грибов А. В., “Гомоморфность некоторых криптографических систем на основе неассоциативных структур”, *Фундам. и прикл. матем.*, **20**:1 (2015), 135–143.
- [4] Кайе Ф., Лафлам Р., Моска М., *Введение в квантовые вычисления. Пер. с англ.*, М.: Мир, 2009, 337 с.
- [5] Катышев С. Ю., “Алгоритм дискретного логарифмирования на квазигруппах, линейных над абелевой группой”, *Обозр. прикл. и промышл. матем.*, **17**:6 (2011), 894–895.
- [6] Катышев С. Ю., Марков В. Т., Нечаев А. А., “Использование неассоциативных группоидов для открытого распределения ключей”, *Дискретная математика*, **46**:3 (2014), 51–59.
- [7] Вялый М., Китаев А., Шень А., *Классические и квантовые вычисления*, М.: МЦНМО, 1999, 192 с.
- [8] Коблиц Н., *Курс теории чисел в криптографии*, М.: ТВП, 2001, 254 с.
- [9] Кузьмин А. С., Марков В. Т., Михалёв А. А., Михалёв А. В., Нечаев А. А., “Криптографические алгоритмы на группах и алгебрах”, *Фундам. и прикл. матем.*, **20**:1 (2015), 205–222.
- [10] Нильсен М., Чанг И., *Квантовые вычисления и квантовая информация. Пер. с англ.*, М.: Мир, 2006, 824 с.
- [11] Романьков В. А., *Алгебраическая криптография: монография*, Омск: Изд-во ОмГУ, 2013, 136 с.
- [12] Diffie W., Hellman M. E., “New directions in cryptography”, *IEEE Trans. Inf. Theory*, **22**:6 (1976), 644–654.
- [13] Habeeb M., Kahrobaei D., Koupparis C., Shpilrain V., “Public key exchange using semidirect product of (semi)groups”, *Lect. Notes Comput. Sci.*, **7954**, 2013, 475–486.
- [14] Hellman M., “A cryptanalytic time–memory trade-off”, *IEEE Trans. Inf. Theory*, **26**:4 (1980), 401–406.
- [15] Kahrobaei D., Shpilrain V., “Using semidirect product of (semi)groups in public key cryptography”, *Cryptology ePrint Archive, Report 2016/378*.
- [16] Katyshev S. Yu., Markov V. T., Nechaev A. A., “On constructing open key cryptosystems using non associative structures”. In: “*VI Int. Conf. Non Assoc. Algebra and Appl.*”, Spain: Zaragoza, 2011.
- [17] Shor P., “Algorithms for quantum computation: discrete logarithms and factoring.”. In: “*Proc. 35th Ann. IEEE Symp. Found. Comput. Sci.*”, 1994, 124–134.