О Б О З Р Е Н И Е
П Р И К Л А Д Н О Й И П Р О М Ы Ш Л Е Н Н О Й
Том 21 М А Т Е М А Т И К И Выпуск 5
2014

С. Ю. К а т ы ш е в (Москва, ТВП). **Алгоритм открытого распределения ключей на неассоциативных структурах.**

Хорошо известна процедура открытого распределения ключей — алгоритм У. Диффи и М. Э. Хеллмана [1], основанный на том, что в качестве общего ключа используется степень g^{mn} некоторого элемента g (обычно циклического образующего) группы G. При этом числа m и n секретны, передаются же только степени g^m и g^n. Установление общего ключа происходит благодаря соотношению: $\forall m, n \in \mathbf{N}$ $(g^m)^n = (g^n)^m$.

Идея о переносе протокола Диффи–Хеллмана на неассоциативный группоид впервые была сформулирована в 2004 году В. Т. Марковым и А. А. Нечаевым. Протокол предлагалось перенести на произвольный неассоциативный группоид $(\Omega, *)$, в котором возведение $g \in \Omega$ в правую степень понимается как умножение справа нужное число раз:

$$g^{[r]} = \underbrace{(\ldots((g * g) * g)\ldots)}_{r \text{ раз}},$$

а единственным требованием к операции умножения на Ω является выполнение тождеств:

$$\forall m, n \in \mathbf{N}: \quad g^{[m][n]} = g^{[n][m]}. \tag{1}$$

Элемент g, удовлетворяющий этой системе тождеств, называется элементом с перестановочными правыми степенями или *ППС-элементом*. Группоид, в котором это тождество выполнено для всех элементов g, называется *ППС-группоидом*.

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

Классы ППС-группоидов найдены среди обобщений квазигрупп, линейных над абелевой группой.

Пусть $(\Omega, \cdot)$ — абелева группа. Зафиксируем два автоморфизма $\sigma, \tau \in \mathrm{Aut}(\Omega)$ и элемент $h \in \Omega$, и зададим на Ω новую операцию $*$ условием:

$$\forall\, x, y \in \Omega \quad x * y = \sigma(x) \cdot \tau(y) \cdot h. \tag{2}$$

Группоид $(\Omega, *)$ называют *квазигруппой, линейной над абелевой группой* $(\Omega, \cdot)$ (см., например, [2]). По аналогии, если $(\Omega, \cdot)$ — абелева полугруппа, группоид $(\Omega, *)$ с операцией (2) будем называть *группоидом, линейным над полугруппой* $(\Omega, \cdot)$ или *линейным группоидом*.

Теорема 1. *Пусть $(\Omega, \cdot)$ — абелева полугруппа, $\sigma, \tau \in \mathrm{Aut}(\Omega)$ — коммутирующие между собой автоморфизмы. Тогда линейный группоид $(\Omega, *)$ с операцией* (2) *есть ППС-группоид.*

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

Для вычисления степени элемента в произвольном локально-медиальном группоиде $(\Omega, *)$, заданном на полугруппе $(\Omega, \cdot)$ с единицей можно предложить алгоритм, трудоемкость которого оценена в следующей теореме.

Теорема 2. *Трудоемкость вычисления степени $g^{[m]}$ обратимого (в полугруппе $(\Omega, \cdot)$) элемента g есть $O(\mathrm{AUT}(\sigma, m)\log_2 m)$ операций в полугруппе $(\Omega, \cdot)$.*

Данная теорема позволяет сделать вывод, о том, что трудоемкость предложенного алгоритма для линейного ППС-группоида не превосходит трудоемкости алгоритма Диффи–Хеллмана.

Оценку стойкости предлагаемого алгоритма открытого распределения ключей естественно начать с исследования проблемы дискретного логарифмирования, т. е. решения уравнения:

$$g^{[x]} = h. \tag{3}$$

Изучаются методы дискретного логарифмирования, основанные на идеях метода согласования (Гельфонда–Шенкса) (см., например, [3]) и метода сведения к собственным подгруппам (В. И. Нечаева [4]).

Теорема 3. *Алгоритм Гельфонда–Шенкса логарифмирования на абелевой группе допускает обобщение на линейный группоид $(\Omega, *)$ с операцией (2), при этом для реализации алгоритма требуется $O(\sqrt{|\Omega|})$ операций в полугруппе $(\Omega, \cdot)$ и память объемом $O(\sqrt{|\Omega|}\cdot\log_2(\sqrt{|\Omega|}))$.*

Опишем реализацию метода дискретного логарифмирования на линейной квазигруппе, обобщающего метод В. И. Нечаева.

Пусть $(\Omega, \cdot) = (G, \cdot)$ — абелева группа, $(G, *)$ — линейная квазигруппа с операцией (2). Для натурального k, введем обозначение $G^{\langle k\rangle} = \{f^k | \forall f \in G\}$.

Пусть $|G| = pq$, где p и q взаимно простые числа. Уравнение (3) сводится к решению системы уравнений

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

где первое уравнение решается в группоиде $(G^{\langle p\rangle}, *)$, второе — в $(G^{\langle q\rangle}, *)$, где $|G^{\langle p\rangle}| = q$ и $|G^{\langle q\rangle}| = p$.

Пусть $|G| = p^n$, где $\exp G = p^k$. Тогда решение уравнения (3) сводится к нахождению решения уравнения $(g^{p^{k-1}})^{[x]} = h^{p^{k-1}}$ в группоиде $(G^{\langle p^{k-1}\rangle}, *)$, где $(G^{\langle p^{k-1}\rangle}, \cdot)$ изоморфна прямой сумме $\mathbf{Z}_p \dot{+} \cdots \dot{+} \mathbf{Z}_p$, и логарифмированию в циклической группе порядка p^{k-1}.

Таким образом принципиальное отличие в сложности правого логарифмирования в линейном группоиде от логарифмирования в ассоциативном случае может возникнуть лишь на этапе логарифмирования в медиальном группоиде, построенном на группе, изоморфной $\mathbf{Z}_p \dot{+} \cdots \dot{+} \mathbf{Z}_p$.

СПИСОК ЛИТЕРАТУРЫ

1. *Diffie W., Hellman M. E.* New directories in cryptography. — IEEE Trans. on Inf. Theory, 1976, v. 22, p. 644–654.
2. *Белявская Г. Б., Табаров А. Х.* Тождества с подстановками, приводящие к линейности квазигрупп. — Дискретн. матем., 2009, т. 21, в. 1, с. 36–51.

3. *Глухов М. М*, *Круглов И. А.*, *Пичкур А. Б.*, *Черемушкин А. В.* Введение в теоретико-числовые методы криптографии. Учебное пособие. СПб.: Лань, 2010, 400 с.
4. *Нечаев В. И.* Элементы криптографии. Основы защиты информации. М.: Высшая школа, 1999, 109 с.