С. Ю. К а т ы ш е в (Москва, ТВП). **Алгоритм дискретного логарифмирования на квазигруппах, линейных над абелевой группой.**

Квазигруппа $(G, *)$ называется *линейной над абелевой группой* $(G, \cdot)$ (*T-квазигруппой*), если операция $*$ задана следующим образом:

$$x * y = \sigma(x)\,\tau(y)\,h, \tag{1}$$

где $\sigma, \tau \in \mathrm{Aut}\,(G)$, h — фиксированный элемент из G. Линейные квазигруппы изучались, например, в [2].

Под *правыми степенями* элемента g линейной квазигруппы G будем понимать $g^{[m]} = (\ldots((g * g) * g)\ldots\ m$ раз $\ldots)$.

В операциях группы G правые степени будут выглядеть следующим образом:

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

Определим *правый порядок* произвольного элемента $g \in \Omega$ как такое наибольшее $t \in \mathbf{N}$, что все элементы $g, g^{[2]}, \ldots, g^{[t]}$ различны. Обозначим эту величину $\mathrm{ord}_r g$. Аналогично вводится понятие левого порядка $\mathrm{ord}_l g$.

Возникает вопрос: не будет ли эта квазигруппа изоморфна некоторой квазигруппе $(G, \otimes)$ с операцией

$$\forall x, y \in G\colon\ x \otimes y = \varphi(x)y, \quad \varphi \in \mathrm{Aut}\,(G)? \tag{3}$$

Очевидно следующее утверждение.

Предложение. *Если $(G, *) \cong (G, \otimes)$, то τ — тождественный автоморфизм, а h — нейтральный элемент.*

Покажем, как задачи о вычислении степеней и логарифмировании в квазигруппе $(G, *)$ можно свести к решению аналогичных задач в квазигруппе указанного типа (3). Пусть $(G, \otimes)$ — квазигруппа с операцией

$$\forall x, y \in G\colon\ x \otimes y = \sigma(x)\,y, \tag{4}$$

где σ — автоморфизм из равенства (1).

Для произвольного $h \in G$ обозначим $h^{[*n]}$ и $h^{[\otimes n]}$ правые n-е степени элемента h, соответственно, в $(G, *)$ и в $(G, \otimes)$.

Теорема 1. *При условии* (4) *для любого $g \in G$ справедливо равенство $g^{[*n]} = g\,\alpha^{[\otimes n-1]}$, где $\alpha = \sigma(g)\tau(g)hg^{-1}$. В частности,* $\mathrm{ord}_{r*} g = \mathrm{ord}_{r\otimes} \alpha$.

Для произвольных элементов g и h T-квазигруппы $(G, *)$ задача дискретного логарифмирования формулируется как решение уравнения $g^{[x]} = h$. Модернизировав алгоритм согласования дискретного логарифмирования в абелевой группе [1], получим следующий результат.

Теорема 2. *Задача дискретного логарифмирования в квазигруппе $(G, \otimes)$ с операцией* (4) *имеет сложность $O\left(\sqrt{\mathrm{ord}_r g}\right)$.*

Следствие. *Задача дискретного логарифмирования в квазигруппе $(G, *)$, линейной над абелевой группой, имеет сложность $O\left(\sqrt{\mathrm{ord}_r g}\right)$.*

Все результаты можно перенести на левые степени квазигруппы, линейной на некоторой абелевой группе.

Работа выполнена при финансовой поддержке Совета поддержки научных школ при Президенте РФ(проект НШ-8.2010.10).

СПИСОК ЛИТЕРАТУРЫ

1. *Василенко О. Н.* Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО, 2003.
2. *Белявская Г. Б.*, *Табаров А. Х.* Характеристика линейных и алинейных квазигрупп. — Дискретн. матем., 1992, т. 4, в. 2, с. 142–147.