Секция «Математика и механика»

Умножение с параметром и его применение в криптографии.

Годнева Анастасия Валерьевна
Студент
Московский государственный университет имени М.В. Ломоносова,
Механико-математический факультет, Москва, Россия
E-mail: god139@yandex.ru

В некоторых республиках при создании электронной подписи находит широкое применение умножение с параметром. Оно задается парой натуральных чисел (n,R) и определяется следующим образом на элементах $a, b \in Z_n$.

$$a \circledR b = a + b + abR (mod\, n)$$

Основной интерес при исследовании криптографических свойств умножения с параметром представляют общий вид группы обратимых элементов, наличие элементов достаточно большого порядка и сложность дискретного логарифмирования.

В случае взаимной простоты R и n это было сделано в работе [2].

В докладе исследованы эти свойства при остальных значениях (n,R).

Про вид групповую часть алгебры с параметром была доказана теорема о разложении в произведение определенных циклических групп, были найдены образующие этих групп.

Так же автором был представлен и обоснован алгоритм дискретного логарифмирования в задаче умножения с параметром (решения уравнения $a^{\backslash x} = b$) при произвольных значениях n и R, а так же приведена оценка сложности алгоритма.

Полученные результаты могут быть использованы для расширения возможностей использования умножения с параметром в криптографии.

Литература

1. O'z DSt 1092:2009. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. — Узбекское агентство стандартизации, метрологии и сертификации, Ташкент, 2009.

2. Ишматова Ю. А. О некоторых свойствах групп алгебр с параметрами // Интеллектуальные системы, т.15, вып. 1–4, 2011.

3. Василенко О. Н. Теоретико-числовые алгоритмы в криптографии — М.: МЦНМО, 2003.

4. Коблиц Н. Курс теории чисел и криптографии —Москва: Научное изд-во ТВП, 2001.

Слова благодарности

Автор выражает глубокую благодарность Галатенко А.В. за постановку задачи и внимание к работе.