МОНОМИАЛЬНЫЕ ПОРЯДКИ И РАЗДЕЛЕНИЕ ДОСТУПА

Т.В. Галибус, Г.В. Матвеев, Н.Н. Шенец

Белгосуниверситет, факультет прикладной математики и информатики,
Независимости 4, 220030 Минск, Беларусь
galibus@bsu.by, matveev@bsu.by, shenets_n_1984@tut.by

Основы теории разделения доступа были заложены А. Шамиром [1]. Впоследствии М. Миньоттом был предложен модулярный подход [2]. При этом общим паролем считается натуральное число s, а паролем i-го участникаЁ— натуральный модуль m_i и наименьший неотрицательный вычет s_i пароля s по этому модулю. Эти параметры определяют на множестве всех участников $P = \{1, 2, \ldots, t\}$ некоторую структуру доступа Γ, т.е. семейство подмножеств, обладающих свойством: система сравнений $x \equiv s_i (\mathrm{mod}\, m_i)$, $i \in A$. $A \in \Gamma$, позволяет участникам из подмножества A правильно найти пароль s.

Недавно С. Ифтене [3] была поставлена задача: какие структуры доступа можно реализовать модулярно с попарно взаимно простыми модулями над кольцом целых чисел. Будем далее такие структуры называть *элементарными*. Нами найдено решение этой задачи не только над кольцом целых чисел, но и над кольцом полиномов от одной переменной $\mathbb{F}_{\text{II}}[\curvearrowleft]$ над полем Галуа $\mathbb{F}_{\text{II}}$. При этом мы использовали теорию мономиальных упорядочений [4]. С этой целью введем переменные $x_1, x_2, \ldots, x_t$, а подмножества $A \subset P$ будем естественным образом отождествлять с мономами. Например, подмножеству $A = \{1, 2, 3\}$ отвечает моном $x_1x_2x_3$. *Сечением* множества 2^P всех подмножеств относительно заданного мономиального порядка $\prec$ назовем представление его в виде $2^P = \Gamma \cup \overline{\Gamma}$, где

$$B \in \overline{\Gamma}, A \in \Gamma \Rightarrow B \prec A.$$

Теорема 1. *Структура доступа будет элементарной над кольцом полиномов* $\mathbb{F}_{\text{II}}[\curvearrowleft]$ *тогда и только тогда, когда она получена путем сечения* 2^P *относительно некоторого мономиального порядка.*

Имеется глубокая интерпретация мономиальных порядков с помощью линейных форм [5]. В частности известно, что мономиальный порядок на конечном множестве задается лишь одной линейной формой с положительными коэффициентами. Это позволяет распространить наш результат и на кольцо целых чисел.

Теорема 2. *Элементарные структуры доступа над кольцами* $\mathbb{Z}$ *и* $\mathbb{F}_{\text{II}}[\curvearrowleft]$ *совпадают.*

Попутно получен и критерий элементарности без использования мономиальных порядков. В принципе он сводится к описанию подмножеств элементарной структуры доступа.

Литература

1. *Shamir A.* How to Share a Secret // Communications of the ACM. 1979. V. 22. P. 612—613.

2. *Mignotte M.* How to Share a Secret // Lecture Notes in Computer Science. Springer-Verlag, 1983. Vol. 149. P. 371-375.

3. *Iftene S.* General secret sharing based on the Chinese remainder theorem // Cryptology ePrint Archive. 2006. V. 166. URL: http://eprint.iacr.org/2006/166.pdf.

4. *Becker T., Weispfenning V.* Gröbner Bases. A Computational Approach to Commutative Algebra. Springer-Verlag, 1993.

5. *Хованский А.Г., Чулков С.П.* Геометрия полугруппы $Z^n_{\geqslant 0}$. М.: МЦНМО, 2006.