

Секция 2

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 512.6

НЕЛИНЕЙНЫЕ ПОДСТАНОВКИ НА ВЕКТОРНОМ ПРОСТРАНСТВЕ,
РЕКУРСИВНО-ПОРОЖДЁННЫЕ НАД КОЛЬЦОМ ГАЛУА
ХАРАКТЕРИСТИКИ 4

А. В. Аборнев

Пусть $R = \text{GR}(2^{2r}, 4)$ — кольцо Галуа характеристики 4 из 2^{2r} элементов с разрядным множеством $P = \{\beta \in R : \beta^{2^r} = \beta\}$. В частности, если $r = 1$, то $R = \mathbb{Z}_4$ и $P = \{0, e\}$. Строится класс нелинейных подстановок π_F на векторном пространстве $\text{GF}(2^r)^m$ произвольной размерности $m \geq 3$, каждая из которых представляется композицией линейного рекуррентного преобразования с характеристическим многочленом $F(x)$ и поэлементного выделения первого разряда элементов кольца R . Такие подстановки называются рекурсивно-порождёнными над кольцом Галуа $\text{GR}(2^{2r}, 4)$. Интерес представляет изучение многочленов $F(x)$ с указанным свойством, которые называются разрядно-подстановочными (или РП-многочленами). Нелинейность координатных функций рекурсивно-порождённых подстановок обеспечивается применением разрядной функции кольца Галуа. В силу простоты представления подстановок из рассматриваемого класса, они допускают очень эффективную реализацию. Ранее автором были построены два класса РП-многочленов над кольцом $R = \mathbb{Z}_4$. В качестве криптографического приложения рассматривается применение рекурсивно-порождённых подстановок при построении итеративных криптографических примитивов.

Ключевые слова: разрядно-подстановочный многочлен, РП-многочлен, кольцо Галуа.

Пусть $R = \text{GR}(4^r, 4)$ — кольцо Галуа характеристики 4 и мощности 4^r . Множество $P = \Gamma(R) = \{\beta \in R : \beta^{2^r} = \beta\}$ называется разрядным множеством. Каждый элемент $a \in R$ имеет разложение

$$a = a_0 + 2a_1, \quad a_s = \gamma_s(a) \in P, \quad s \in \{0, 1\},$$

где $\gamma_s : R \rightarrow P$, $s \in \{0, 1\}$, — разрядные функции в разрядном множестве P . Алгебра $(P, \oplus, \cdot)$ с умножением кольца R и операцией сложения $a \oplus b = \gamma_0(a + b)$, $a, b \in P$, является полем из 2^r элементов.

Продолжаются исследования, начатые в работе [1]. Рассматривается задача построения нелинейных подстановок на векторном пространстве P^m большой размерности m с использованием только линейного рекуррентного закона с характеристическим многочленом

$$F(x) = x^m - f_{m-1}x^{m-1} - \dots - f_1x - f_0 \in R[x]$$

и операции выделения старшего разряда элементов кольца R . В [1] впервые доказано существование таких подстановок и описаны два нетривиальных класса для случая кольца $\mathbb{Z}_4$. В данной работе получен новый класс нетривиальных РП-многочле-

нов $F(x)$, индуцирующих нелинейные подстановки на алфавите P^m сколь угодно большой мощности 2^{rm} .

Пусть $u \in L_R(F)$ — линейная рекуррентная последовательность (ЛРП) с характеристическим многочленом $F(x) \in R[x]$. Её знаки удовлетворяют равенству

$$u(i+m) = \sum_{k=0}^{m-1} f_k u(i+k).$$

Каждый знак ЛРП u имеет разложение

$$u(i) = u_0(i) + 2u_1(i), \quad u_0(i), u_1(i) \in P, \quad i = 0, 1, \dots$$

Обозначим через $u[\overline{i, j}]$ отрезок $(u(i), u(i+1), \dots, u(j))$ последовательности $u \in L_R(F)$ и через $L'_R(F)$ — множество всех линейных рекуррентных последовательностей $u \in L_R(F)$, таких, что $u_1[\overline{0, m-1}] = \overline{0}$.

Рассмотрим отображение $\pi_F : P^m \rightarrow P^m$, заданное равенством

$$\pi_F(x) = u_1[\overline{m, 2m-1}],$$

где $u \in L'_R(F)$; $u_0[\overline{0, m-1}] = x$.

Многочлен $F(x) \in R[x]$ степени m , для которого отображение π_F является биекцией, будем называть *разрядно-подстановочным* (или *РП-многочленом*). Будем говорить, что подстановка π_F является *рекурсивно-порождённой* над кольцом R с законом рекурсии $F(x)$. РП-многочлен назовём *нетривиальным*, если подстановка π_F нелинейна. Таким образом, каждый РП-многочлен естественным образом задаёт семейство, вообще говоря, нелинейных подстановок на пространстве P^m .

Будем использовать следующие обозначения:

$$F_0(x) = x^m \oplus \bigoplus_{i=0}^{m-1} \gamma_0(f_i)x^i, \quad F_1(x) = \bigoplus_{i=0}^{m-1} \gamma_1(f_i)x^i.$$

Теорема 1. Пусть $R = \text{GR}(4^r, 4)$, $F(x) \in R[x]$ — многочлен степени $m \geq 3$. Если $F_0(x) = x^m \oplus x^{m-1} \oplus x \oplus e$, то $F(x)$ является РП-многочленом тогда и только тогда, когда для каждого $\delta \in P$ верно равенство

$$\text{НОД}(\delta(x \oplus e) \oplus e \oplus F_1(x), F_0(x)) = e.$$

Данная теорема обобщает результат работы [1] на случай произвольного кольца Галуа характеристики 4.

ЛИТЕРАТУРА

1. *Nechaev A. A. and Abornev A. V.* Nonlinear permutations on a space over a finite field induced by linear transformations of a module over a Galois ring // Математические вопросы криптографии. 2013. Т. 4. № 2. С. 81–100.