ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 20 МАТЕМАТИКИ Выпуск 4
2013

О. В. Антонова (Великий Новгород, НовГУ)**. Метод анализа линейной сложности обобщенных циклотомических последовательностей с периодом p^n .**

Применение классических циклотомических классов и обобщенных циклотомических классов для формирования последовательностей, которые называют, соответственно, классическими циклотомическими последовательностями и обобщенными циклотомическими последовательностями, является важным методом построения последовательностей [1]. Для криптографических приложений важной характеристикой последовательности является линейная сложность L , которая определяется как длина самого короткого линейного регистра сдвига с обратной связью, с помощью которого можно воссоздать последовательность.

Метод вычисления линейной сложности бинарных обобщенных циклотомических последовательностей с периодом p^n , предложенный в [2], обобщается для последовательностей с элементами из конечного поля Галуа и периодом p^n .

Пусть p — нечетное простое число и d — натуральный делитель $p-1$, $d \geqslant 2$. Обозначим $H_0 = \{\theta^{td} \bmod p^n;\ t = 0, \ldots, p^{n-1}(p-1)/d - 1\}$ класс вычетов степени d по модулю p^n .

Пусть $H_k = \theta^k H_0$ для $k = 0, 1, \ldots, d-1$. Классы вычетов H_k образуют разбиение множества обратимых элементов кольца $\mathbf{Z}_{p^n}$ и являются обобщенными циклотомическими классами. В частности, справедливо разбиение

$$\mathbf{Z}_{p^n} = \bigcup_{m=0}^{n-1} \bigcup_{k=0}^{d-1} p^m H_k \cup \{0\}.$$

Пусть $\mathbf{GF}(r)$ — конечное поле из r элементов. Для всех элементов $a \in \mathbf{GF}(r)$ зададим подмножества индексов $I_l^{(a)}$, $l = 0, 1, \ldots, n-1$, элементы которых принимают значения от 0 до $d-1$. При этом, для каждого значения $l = 0, 1, \ldots, n-1$ множества $I_l^{(a)}$ должны образовывать разбиение множества $\{0, 1, \ldots, d-1\}$, т. е.

$$\bigcup_{a \in GF(r)} I_l^{(a)} = \{0, 1, \ldots, d-1\} \text{ и } I_l^{(a)} \cap I_l^{(b)} = \varnothing, \text{ если } a \neq b.$$

Определим последовательность X с периодом p^n и элементами из поля $\mathbf{GF}(r)$ следующим образом: $x_0 = b$, где b — произвольный элемент поля $\mathbf{GF}(r)$, и

$$x_i = a, \text{ если } i \bmod p^n \in \bigcup_{l=0}^{n-1} \bigcup_{k \in I_l^{(a)}} p^l H_k. \tag{1}$$

Вычисление линейной сложности последовательности, определяемой формулой (1) сводится к исследованию многочлена классических циклотомических последовательностей

с периодом p. Свойства многочлена классических циклотомических последовательностей и метод вычисления его значений для конечных полей второго и третьего порядков были изучены в [3]. Обобщая результаты, представленные в [2, 3], получаем метод вычисления линейной сложности обобщенных циклотомических последовательностей, сформированных по (1).

Для иллюстрации предлагаемого метода вычислена линейная сложность над полем третьего порядка троичных последовательностей с периодом p^n, сформированных на основе классов кубических, биквадратичных и шестеричных вычетов, и линейная сложность четвертичных последовательностей над полем четвертого порядка.

СПИСОК ЛИТЕРАТУРЫ

1. *Cusick T.*, *Ding C.*, *Renvall A.* Stream ciphers and number theory. N.-Holl. Math. Libr, 1998.
2. *Edemskiy V.* About computation of the linear complexity of generalized cyclotomic sequences with period p^{n+1}. — Des. Codes Cryptogr., 2011, v. 61, p. 251–260.
3. *Едемский В. А.*, *Гантмахер В. Е.* Синтез двоичных и троичных последовательностей с заданными ограничениями на их характеристики. Великий Новгород: НовГУ, 2009, 189 с.