

В. А. Е д е м с к и й (Великий Новгород, НовГУ). **О линейной сложности бинарных последовательностей, определяемых характеристиками конечных полей.**

В работе предлагается метод построения бинарных последовательностей с высокой линейной сложностью, определяемых посредством квадратичных характеристик конечных полей. Линейная сложность бинарной последовательности (ранг) (s_i) над полем второго порядка определяется как наименьшее натуральное L , для которого выполняется следующее рекуррентное соотношение:

$$s_i = c_1 s_{i-1} + \dots + c_L s_{i-L} \text{ для } i \geq L,$$

где коэффициенты $c_1, c_2, \dots, c_L \in \{0, 1\}$ [1]. Последовательности с высокой линейной сложностью представляют интерес для криптографических приложений.

Пусть p — нечетное простое число и $\mathbb{F}_q$ — конечное поле порядка q , где $q = p^r$, $r \in \mathbb{N}$. Пусть $\{\gamma_1 = 1, \gamma_2, \dots, \gamma_r\}$ — базис $\mathbb{F}_q$, как линейного пространства над конечным полем $\mathbb{F}_p$ [1]. Любое целое число i от 0 до $q-1$ можно представить в виде:

$$i = i_1 + i_2 p + \dots + i_r p^{r-1}, \quad 0 \leq i_m < p, \quad m = 1, \dots, r,$$

и поставить ему в соответствие элемент $\mathbb{F}_q$ по правилу:

$$\xi_i = i_1 \gamma_1 + i_2 \gamma_2 + \dots + i_r \gamma_r.$$

Определим бинарную последовательность $\sigma = (\sigma_0, \sigma_1, \dots, \sigma_{q-1}, \dots)$ с периодом q следующим образом:

$$\sigma_i = (1 - \chi(\xi_i))/2 \text{ для } i : 0 \leq i < q \text{ и } \sigma_{i+q} = \sigma_i \text{ для } i \geq q,$$

где χ — квадратичный характер $\mathbb{F}_q$, $\chi(0) = 1$. Последовательность σ также можно определить посредством дискретного логарифма в $\mathbb{F}_q$.

Последовательность σ при $r = 1$ является последовательностью Лежандра, свойства которой, в том числе и линейная сложность, хорошо известны. Линейная сложность σ для $r = 2$ была вычислена в [2]. Здесь обобщаем результаты из [2] и показываем, что последовательность σ обладает высокой линейной сложностью при нечетных значениях r .

Исследование выполнено при финансовой поддержке РФФИ и ГФЕН Китая в рамках научного проекта № 19-51-53003.

СПИСОК ЛИТЕРАТУРЫ

1. Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988, 820 с.
2. Chen Z., Wang Q. On the k -Error Linear Complexity of Binary Sequences Derived from the Discrete Logarithm in Finite Fields. — Complexity, 2019, <https://doi.org/10.1155/2019/8635209>.