ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 27 МАТЕМАТИКИ Выпуск 1
2020

В. А. Едемский (Великий Новгород, НовГУ)**. Оценка симметричной 2-адической сложности последовательностей Динга–Хеллесета.**

УДК 519.7

Резюме: Оценена симметричная 2-адическая сложность обобщенных циклотомических последовательностей Динга-Хеллесета второго порядка с периодом p^n. Показано, что эти последовательности имеют высокую симметричную 2-адическую сложность.

Ключевые слова: 2-адическая сложность, бинарные последовательности, циклотомия.

В работе предлагается метод оценки симметричной 2-адической сложности обобщенных циклотомических последовательностей Динга–Хеллесета второго порядка с периодом p^n.

Пусть $\mathbf{s} = (s_0, s_1, \ldots, s_{N-1})$ — бинарная последовательность периода N. 2-адическая сложность $\Phi(\mathbf{s})$ бинарной последовательности является её важной характеристикой. Она определяется как число ячеек регистра сдвига с обратной связью по переносу (feedback with carry shift register), порождающего последовательность [2]. Согласно [1], для оценки секретности бинарных периодических последовательностей лучше применять симметричную 2-адическую сложность, определяемую как $\overline{\Phi}(\mathbf{s}) = \min\left(\Phi(\mathbf{s}), \Phi(\widetilde{\mathbf{s}})\right)$, где $\widetilde{s} = (s_{N-1}, s_{N-2}, \ldots, s_0)$.

Пусть p — нечетное простое число, n — натуральное. Обозначим через g примитивный корень по модулю p^n. Определим

$$D_j^{(p^k)} = \left\{ g^{j+2t} \pmod{p^k} \,|\, 0 \leqslant t < p^{k-1}(p-1)/2 \right\}$$

для $k = 1, 2, \ldots, n$ и $j = 0, 1$. $D_j^{(p^k)}$, $j = 0, 1$ называются обобщенными циклотомическими классами Динга–Хеллесета порядка 2 по модулю p^k. Пусть $C_0 = \bigcup_{k=1}^{n} p^{n-k} D_0^{(p^k)}$ и $C_1 = \bigcup_{k=1}^{n} p^{n-k} D_1^{(p^k)} \cup \{0\}$. Тогда последовательность Динга–Хеллесета второго порядка с периодом p^n определяется как

$$s_i = \begin{cases} 0, & \text{if } i \pmod{p^n} \in C_0, \\ 1, & \text{if } i \pmod{p^n} \in C_1. \end{cases} \tag{1}$$

2-адическая сложность обобщенных циклотомических последовательностей Динга–Хеллесета с периодом p^2 для $p \not\equiv \pm 5 \pmod{24}$ изучена в [3].

Теорема. *Пусть последовательность* $\boldsymbol{s}$ *определена по* (1). *Тогда* $\overline{\Phi}(\boldsymbol{s}) \geq p^n - p^{n-1}$.

Согласно теореме симметричная 2-адическая сложность обобщенной циклотомической последовательности Динга–Хеллесета больше половины периода, более того, для $n > 2$ эта оценка может быть улучшена.

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

СПИСОК ЛИТЕРАТУРЫ

1. *Hu H.*, *Feng D.* On the 2-adic complexity and the k-error 2-adic complexity of periodic binary sequences. — IEEE Trans. Inf. Theory, 2008, v. 54, p. 874–883.
2. *Klapper A.*, *Goresky M.* Feedback shift registers, 2-adic span, and combiners with memory. — Journal of Cryptology, 1997, v. 10, p. 111–147.
3. *Xiao Z.*, *Zeng X.*, *Sun Z.* 2-Adic complexity of two classes of generalized cyclotomic binary sequences. — Internationl Journal of Foundations of Comput. Sci., 2016, v. 27, p. 879–893.

УДК 519.7

Edemskiy V. A. (Veliky Novgorod, Yaroslav-the-Wise Novgorod State University).
Estimate of the symmetric 2-adic complexity of Ding-Helleseth sequences.

Abstract: The symmetric 2-adic complexity of generalized cyclotomic Ding-Helleseth sequences of order two with period p^n is evaluated. It is shown that these sequences have a high symmetric 2-adic complexity.

Keywords: 2-adic complexity, binary sequences, cyclotomy.