УДК 621.391

КОДИРОВАНИЕ АДРЕСНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НЕЛИНЕЙНЫМ КОДОМ

А.И. Митюхин

Институт информационных технологий учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. Рассматривается построение конструкции нелинейного бинарного кода для использования в качестве адресных слов, а также реализации начальной надежной синхронизаии в радиосистемах с расширением спектра. Полученная система сигналов может использоваться для обеспечения помехоустойчивой передачи, процедуры распознавания адреса и защиты кодированной информации от перехвата. Ансамбль кодовых слов строится с использованием квадратичных вычетов по модулю простого числа и обладает криптографическими свойствами.

Ключевые слова: помехоустойчивость; спектр; радиосистема; корреляция; квадратичный вычет; ансамбль кодов; матрица Джекобстола.

ENCODING ADDRESS SEQUENCES WITH NONLINEAR CODE

A. Mitsiukhin

Institute of Information Technologies of the Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. The construction of a nonlinear binary code for use as addressable codes, as well as the implementation of initial reliable synchronization in radio systems with spread spectrum, is considered. The resulting signal system can be used to ensure noise-free transmission, address recognition and protection of coded information from interception. The ensemble of codewords is built using quadratic deductions modulo prime and has cryptographic properties.

Keywords: noise immunity; spectrum; radio system; correlation; quadratic deduction; an ensemble of codes; Jacobsthal matrix.

Введение

Передача информации с использованием методов с расширением спектра позволяет обеспечить защиту от перехвата и воздействия организованных помех (глушение передачи) в плотно расположеных физических каналах тактического уровня. При этом особое внимание уделяется к выбору конструкций (n, M, d)-кодов с хорошими взаимно-корреляционными, спектральными и крипто характеристиками [1]. Основными критериями выбора параметров кода должны быть:

недопустимость предсказания закона формирования символов кодовой последовательности длиной n по правильно принятому сегменту слова длиной $k < n$;

значительная величина мощности M кода с заданным кодовым расстоянием d;

желательно иметь код со свойствами ортогональности при вычисления взаимной корреляционной функции R (ВКФ) между входным процессом и копией сигнала [1].

законы кодирования кода должны эффективно меняться в сеансах связи;

период $T = n\tau$ $(\tau -$ длительности чипа слова$)$ последовательности должен превышать длительность сеанса связи, т. е. отвечать свойству апериодичности.

На выбор кода для реальной радиосистемы влияет и такой системный аспект как синхронизация. Прием или декодирование информации становится возможным только после установления синхронизации по начальной фазе кодовой последовательности.

Теоретические принципы

Предметом статьи является обсуждение вопроса пригодности применения для передачи информации бинарного блокового нелинейного кода, построенного на основе использования квадратичных вычетов в конечном поле Галуа $GF(p^m)$, $m \in \mathrm{Z}^+$ и матриц Джекобстола размером $(p \times p)$. В сравнении с линейными кодами над расширенным полем $GF(2^m)$, $m \in \mathrm{Z}^+$ нелинейные конструкций кодов характеризуются значительно большей мощностью кода M и лучшими

криптографическими свойствами за счет негруппового свойста, т. е. не выполнения аксиомы замкнутости на множестве кода.

В обобщенном виде структура нелинейного квадратично вычетного кода порядком $n = p + 1,$ определяется выражением

$$\mathbf{H} = \begin{pmatrix} 1 & \mathbf{1} \\ \mathbf{1}^T & \mathbf{Q} - \mathbf{I} \end{pmatrix}, \quad (1)$$

где $\mathbf{I}-$ единичная матрица размером $p \times p$;

$\mathbf{1}-$ единичная строка размером $1 \times p$.

$\mathbf{Q} = (q_{ij}) -$ матрица Джекобстола порядком $(p \times p)$.

Элементы матрицы $\mathbf{Q} = (q_{ij})$ определяются как

$$q_{ij} = \chi((j - i) \bmod p)) = \chi\left(\frac{j - i}{p} \right), \quad (2)$$

где $\chi(i) -$ символ Лежандра.

В работе представлено построение кода на квадратичных вычетах в простом поле $GF(139)$ (1). Выбор значения $p = 139$ определялся параметром значности кода $n = p + 1.$ Сравнение важнейших свойств полученного кода, удовлетворяющих требованиям приведенным выше, дано с известным линейным симплексным M -кодом

$$\left[n,\ k,\ d \right] = \left(2^m - 1,\ m,\ 2^{m-1} \right) = \left(127,\ 7,\ 64 \right).$$

Основные теоретические и сравнительные экспериментальные результаты исследования приведены в таблице. Число ансамблейей M -кода вычислено через функцию Эйлера числа n, $M = \varphi(n)/k = 126/7 = 18.$ Число ансамблейей нелинейного кода совпадает с длиной кода, что практически в 8 раз больше чем у линейного кода. Значения других параметров получены экспериментально, используя моделирование в среде MATLAB.

Свойства линейного и нелинейного кода
Properties of linear and nonlinear code

Конструция кода	Блоковая длина кода n	Мощность кода M	Постоянная компонента кода $DC=-1/n$	Амплитудные коэффициены ДПФ $\lvert f_k \rvert$	ВКФ $\max R(\tau),\ \tau=0$
Линейный M -код	127	18	$-0,0078$	$11,269$ для $k=(1,\cdots,126).$	$-1;\ -17;\ 15$
Нелинейый код	140	140	0	$11,8$ для $k=(1,\cdots,139).$	0

В отличие от нулевой криптостойкости M-кода, криптостойкость кода на квадратичных вычетах зависит от знания числа p. Стандартные атаки становятся неэффектимными из-за сложности нахождения формулы формирования (генерации) кода.

Заключение

Задача несанкционированного обнаружения нелинейного кода в сравнении с линейным M-кодом усложняется из-за использования ансамбля мощностью в 8 раз больше, а также отсутствием постоянной составляющей. В синхронном режиме и для кодового разделения каналов исследуемый нелинейный код имеет большую помехоустойчивость за счет идеальной ортогональности и может найти применение в радиосистемах с расширением спектра.

Список использованных источников / References

1. Mitsiukhin A. (2025) Detection and Analysis of Moving Objects. *International Journal on Applied Physics and Engineering*, Volume 4, 2025, 62–71.

Сведения об авторе

Митюхин А.И. Доцент, доцент, Институт информационных технологий учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», mityuhin@bsuir.by.

Information about the author

Mitsiukhin A. Associate Professor**,** Associate Professor, Institute of Information Technologies of the Educational Institution "Belarusian State University of Informatics and Radioelectronics", mityuhin@bsuir.by.