НЕЛИНЕЙНЫЙ КОД АДАМАРА НАД КВАДРАТИЧНЫМИ ВЫЧЕТАМИ В ПОЛЕ ГАЛУА

Ле Нгуен Лонг, магистрант

Белорусский государственный университет информатики и радиоэлектроники,
Институт информационных технологий,
г. Минск, Республика Беларусь

Митюхин А.И. – доцент

Рассматривается построение нелинейного кода, который предназначен не только для исправления ошибок в канале с шумами, но и для защиты информации от несанкционированного съема информации в широковещательном канале.

Для защиты информации в широковещательном канале необходимо иметь наибольшую возможную мощность M (n, M, d)- кода, где $n-$ длина кодового слова с элементами над простым полем Галуа, $d-$ кодовое расстояние. Для защиты информации следует применять нелинейные конструкции кодов. В общем случае нелинейные коды формируются при условии, когда не выполняются некоторые аксиомы в конечных полях Галуа. Практически это достигается изменением линейные оболочки кода, например, матрицы Сильвестра. Для этого можно выполнять следующие операции над линейным кодом $\mathcal{E}$. 1. Расширение кодовых координат. 2. Выкалывание кодовых координат. 3. Весовое выбрасывание кодовых слов.

В работе исследовались построение нелинейной конструкции на основе двоичных ДПФ подобных функций Адамара [1]. Высказано предположение (но не доказано), что матрицы Адамара существуют для любого n, кратного 4. Последнее значение n, которое практически проверено равно 664. Используя операцию расширения линейного кода Адамара, в работе построен нормализованный нелинейный код $\mathbf{A}_n$ с кодовым расстоянием $d = n/2$. Операция расширения позволяла сформировать длину кода, определяемого выражением $n = p^m + 1$, где $p-$ простое число, $m \in \square^+$. Базисом построения матрицы $\mathbf{A}_n$ являются квадратичные вычеты по над полем $GF(p)$

$$1^2,\ 2^2,...,\ ((p-1)/2)^2 \bmod p)$$

и матрица Джекобстола $\mathbf{Q} = \left(q_{i,j}\right),\ q_{i,j} = \chi(j-i),$ где функция $\chi(i)$ определяется символом Лежандра.

$$\chi(i) = \begin{cases} 0, \text{ если } i \text{ кратно } p \text{ (делится на } p); \\ 1, \text{ если } i \text{ квадратичный вычет по модулю } p; \\ -1, \text{ если } i \text{ квадратичный невычет по модулю } p. \end{cases}$$

Нелинейный нормализованный код $\mathbf{A}_n$ над полем $GF(p)$ порядком $n = p+1$ строится по выражению

$$\mathbf{A}_n = \begin{pmatrix} 1 & \mathbf{1} \\ \mathbf{1}^T & \mathbf{Q}-\mathbf{I} \end{pmatrix},$$

где $\mathbf{I}-$ единичная матрица размером $p \times p$,
$\mathbf{1}-$ единичная строка размером $1 \times p$.

Как и в нормализированной матрице Адамара $\mathbf{H}_n$ строки матрицы $\mathbf{A}_n$ обладают свойством ортогональности. В этом случае рассмотренная нелинейная конструкция кода фактически образует фазоманипулированные видеосигналы, которые можно применять в современных мобильных коммуникационных системах спецификации G.

Список использованных источников:

1. Mitsiukhin, A. Compressing the geospatial data of testing grounds / A. Mitsiukhin / WSEAS Transactionson Environment and Development, ISSN: 1790-5079 E-ISSN: 2224-3496 Volume 19, 2023 (March 2024, A. Mitsiukhin). Art. #125. Pages: 1386-1391 DOI: 10.37394/232015.2023.19.125.