УДК 621.396

В.Я. Чечельницкий

Одесский национальный политехнический университет, Одесса

ЗАЩИТА ИНФОРМАЦИИ С ПОМОЩЬЮ ОРТОГОНАЛЬНЫХ КОРРЕКТИРУЮЩИХ КОДОВ НА ОСНОВЕ СОВЕРШЕННЫХ МНОГОУРОВНЕВЫХ РЕШЕТОК

Современные системы телекоммуникаций, действующие в условиях многолучевого распространения радиоволн, естественных и искусственных помех, должны обладать высокой помехозащищенностью, т.е. помехоустойчивостью и обеспечивать защиту информации от несанкционированного доступа.

В обычных классах систематических корректирующих (n,k)-кодов k информационных символов всегда располагаются в явном виде на одних и тех же позициях каждого кодового слова [1] и поэтому они не могут применяться для защиты информации от несанкционированного доступа. Однако, в данной работе показано, что путем перехода к несистематическому кодированию ортогональных кодов удается обеспечить одновременно и коррекцию ошибок и защиту информации от несанкционированного доступа.

Пусть $G(N)$ – совершенная многоуровневая решетка (СМР), произвольного заданного порядка N. Путем всех циклических сдвигов $G(N)$ по строкам и/или столбцам построим эквивалентный класс СМР [2], или по-другому – двумерный циклический $G_i(N)$-код, $i=\overline{1,J}$, мощности $J=N^2$ двумерных кодовых слов СМР. Путем конкатенации строк СМР получим эквивалентный одномерный $K(n)$-код, длины $n=N^2$, той же мощности $J=N^2$, ортогональный по построению и обладающий свойством двухпетлевого циклического N-сдвига [3]. Полагаем, что источник сообщений после устройства кодирования источника формирует ансамбль равновероятных сообщений $A=\{a_i\}$, $i=\overline{1,J}$. Правило отображения сообщений в кодовые слова (манипуляционный код) принимает вид

$$\Pi=\begin{pmatrix} a_{i_1}, & a_{i_2}, & \cdots, & a_{i_J} \\ G_1(N), & G_2(N), & \cdots, & G_J(N) \end{pmatrix}.$$

Поскольку $K(n)$-код ортогональный, с одинаковой энергией каждого кодового слова, то каждое правило отображения Π одинаково эффективно, число таких правил пропорционально числу уровней защиты информации от несанкционированного доступа, и определяется факториальным соотношением:

$$\gamma_{\text{защиты}}=J!=N^2!.$$

В данной работе проведено также исследование эффективности двух методов декодирования многоуровневых нелинейных корректирующих $K(n)$ $K(n)$-кодов:

– двумерное корреляционное декодирование принятого в условиях помех кодового слова $Y(N)$ с опорным кодовым словом $G_1(N)$, согласно [2], в метрике Евклида;

– декодирование $Y(N)$ по минимуму кодового расстояния в метрике Хэмминга.

В целом проведенные исследования корректирующих свойств многоуровневых $(q>2)$ $K(n)$-кодов показали, что декодирование этих кодов целесообразно проводить по минимуму кодового расстояния в метрике Хэмминга, поскольку *q*-ичные (недвоичные) коды имеют неоптимальное (отличное от единицы) значение пик-фактора. Этот факт имеет ясную физическую трактовку, например при переходе (ошибке) вида $-7 \Rightarrow 8$ данный символ кодового слова изменяется на 15 условных единиц в метрике Евклида, в то время как в метрике Хэмминга это соответствует просто одному несовпадению. Вместе с тем, для всех ортогональных $K(n)$-кодов практически достигается верхняя граница кодового расстояния Плоткина.

Список литературы

1. Скляр Б. Цифровая связь. Теоретические основы и практическое применение: Пер. с англ. – Изд. 2-е испр. – М.: Издательский дом «Вильямс», 2003. – 1104 с.

2. Мазурков М.И., Чечельницкий В.Я. Классы эквивалентных и порождающих совершенных двоичных решеток для CDMA технологий. // Изв. вузов Радиоэлектроника. – 2003. – № 5. – С. 54-63.

3. Трахтман А.М., Трахтман В.А. Основы теории дискретных сигналов на конечных интервалах. – М.: Сов. радио, 1975. – 208 с.