ОПЕРАЦИЯ РАЗЛОЖЕНИЯ ГРУППЫ В КАНАЛЕ С ПОДСЛУШИВАНИЕМ

Конколович А.А.

Институт информационных технологий Белорусского государственного университета информатики и радиоэлектроники
г. Минск, Республика Беларусь

Митюхин А.И. – доцент

Аннотация. Рассматривается применение операции разложения группы на смежные классы кода для обеспечения информационной безопасности в двоичном симметричном канале.

Одним из методов декодирования корректирующего [*n, k, d*]-линейного кода над полем Галуа $GF(2)$ является метод с использованием операция разложение группы G порядка 2^n на множество $C = \{C_i\}, i = 1, \dots, 2^r$ смежных классов. Параметры *n, k, d, r* , соответственно, длина, размерность, кодовое расстояние и число проверочных символов кода. Декодирование сводится к анализу таблицы стандартного расположения для кода размером $2^r \times 2^k$ [1]. Временная сложность декодирования оценивается объемом $V = n2^r$ памяти, необходимым для хранения столбца лидеров смежных классов (каждый элемент столбца – это двоичный вектор-строка размером *n*) и суммарным временем доступа к памяти. Если использовать низкоскоростное кодирование, когда $r \gg k$, даже для сравнительно небольшой длины n эффективное декодирование по таблице стандартного расположения на множестве 2^r векторов практически осуществить невозможно из-за значительных временных затрат. Не зная уравнение кодирования, фактор значительной сложности декодирования предлагается использовать для защиты информации от перехвата нелегальным пользователем.

Декодирование сводится к анализу смеси

$$\mathbf{Y} = \mathbf{X} + \mathbf{E}$$

где $\mathbf{Y} = (y_1, \dots, y_n), y_i \in GF(2)$ – вход декодера, $\mathbf{X} = (x_1, \dots, x_n), x_i \in GF(2)$ – вход канала, $\mathbf{E} = (e_1, \dots, e_n), e_i \in GF(2)$ – шумовой вектор, препятствующий правильному декодированию в канале подслушивания. Неопределенность получения правильной информации на выходе канала можно достичь, если подмножество $\{\mathbf{X}\}$ распределить по всему n-мерному пространству, а не по смежному

классу самого кода G. Это достигается, переходом к коду $G^{\perp}$, ортогональному исходному [1] и разложением $G^{\perp}$ по подгруппе H порядка 2^r. Степень защиты информации за счет процедуры распределения кода $\{\mathbf{X}\}$ в евклидовом подпространстве и зашумления вида (1) оценивается с использования энтропийного подхода теории информации [2]. Надежная защита информации связана с оценкой средней взаимной информация I_u на выходе декодера [2]

$$I_u = \frac{k}{n} H(U) - H(U|Y), \quad (1)$$

где $H(U)$ – энтропия источника, $H(U|Y)$ – условная энтропия (потеря информации) в двоично симметричном канале). С позиции защиты информации, составляющая $H(U|Y)$ определяет энтропию шумовой составляющей на выходе канала. В рассматриваемом случае $H(U|Y)$ определяется энтропийной функцией Шеннона [2]

$$H(U|Y) = -[p \log_2 p + (1-p) \log_2 (1-p)], \quad (2)$$

где p вероятность ошибок в канале.

Выражения (1) и (2) позволяют определить параметры *n, k, d* кода, кратность ошибок *t* в зависимости от заранее определенной степени защиты. При этом основном канале декодер работает с минимально возможной ошибкой декодирования. Представлен расчет необходимых параметров ортогонального кода для рассматриваемой модели передачи информации с кодированием на основе теории алгебраических групп [3], разложения группы на смежные классы

Показано, что использование операции разложения группы на смежные классы широкополосных *m*-кодов, корректирующих ошибки, позволяет осуществить надежную защиту информации.

Список использованных источников:

1. Mac Willams F.J., Sloane N.J.A. The Theory of Error-Correcting Codes / F.J. Mac Willams, N.J.A Sloane. – Oxford, 1977.
2. Митюхин А.И. Прикладная теория информации : учеб. пособие / Митюхин А.И. – Минск, БГУИР, 2018.
3. Митюхин А. И. Элементы алгебры для теории кодирования / Митюхин А.И. – Akademikerverlag GmbH, Saarbrücken, Germany, 2013.