АЛГОРИТМ ПОМЕХОУСТОЙЧИВОГО СИСТЕМАТИЧЕСКОГО КОДИРОВАНИЯ ПО КРИВЫМ ЭРМИТА

к.т.н. Лысенко В.Н., к.т.н. Ляпа Н.Н,
курсант Свинаренко В.Ю.
(Военный институт РВ и А СумГУ)

Зафиксируем конечное поле *GF (q)*. Пусть X – гладкая проективная алгебраическая кривая в проективном пространстве P^n над, $g = g(X)$ - род кривой, X (*GF (q)*) – множество точек над конечным полем, $N = | X (GF (q)) |$ - их число. Пусть C – класс дивизоров на X степени $\alpha > g-1$. Тогда C определяет отображение $\varphi: X \to P^{k-1}$, где $k \geq \alpha - g + 1$ Набор $y_i = \varphi(x_i)$ задает код. Эта конструкция позволяет строить коды с параметрами $k + d \geq n - g + 1$, длина n которых меньше либо равна числу точек на кривой *X*.

Алгеброгеометрический код по кривой X над *GF(q)* – это линейный код , состоящий из всех слов $(c_1, c_2 \ldots c_n)$ длинны n $\leq$ N, для которых выполняется равенство d + g –1 уравнений

$$\sum_{i=0}^{n-1} c_i F_j(P_i) = 0,$$

где $c_i \in GF(q)$, $d \geq \alpha - 2g + 2$, $\alpha = degX \cdot degF$.

Алгоритм систематического кодирования. Пусть I – множество k информационных позиций кодового слова (т.е. множество номеров позиций, входящих в заданный информационный набор кода) и h – множество $r = n-k$ проверочных позиций. объединение множеств $I \cup h$ содержит все целые числа (номера) от 0 до n-1. На информационных позициях

разместим k символов сообщения, а на проверочных нули. Вычислим суммы

$S_j = \sum_{i \in I} c_i F_j(P_i),\ j = \overline{0, r-1}$,или в матричной форме

$$\|S_j\|_r = \|F_j(P_i)\|_{k,r} \|c_i\|_r^T \qquad (1)$$

Для нахождения значений r=n-k проверочных символов можно использовать методы обращения матриц . Запишем в матричной форме:

$$\|c_i\|_r = \|F_j(P_i)\|_{k,r}^{-1} \| - S_j\|_r^T \qquad (2)$$

Сам алгоритм определим как последовательность следующих шагов:

1. На заранее определенные информационные позиции кодового слова поместим k символов сообщения.

2. Вычислим матрицу-строку $\|S_j\|_r$, используя (1).

3. Вычислим матрицу-строку $\|c_i\|_r$, используя (2).

4. Поместим элементы матрицы $\|c_i\|_r$ на проверочные позиции кодового слова .

Разработанный алгоритм алгеброгеометрического кодирования позволяет формировать кодовые слова для произвольных k символов сообщения .

Алгоритм допускает построение кодов по произвольной кривой в P^2 над $GF(q)$.

Если кривая Эрмита построена по однородному многочлену, то однородные одночлены F(x,y,z) на точках такой кривой можно представить в виде некоторых функций F(x,y,1). Подобное представление функций отображения позволяет существенно упростить необходимые для алгеброгеометрического кодирования вычисления.