КРИПТОГРАФИЧЕСКИЕ СВОЙСТВА АЛГЕБРО-ГЕОМЕТРИЧЕСКИХ КОДОВ ЭРМИТА

С.Б. САЛОМАТИН, В.В. ПАНЬКОВА, Д.М. БИЛЬДЮК

Алгебро-геометрические коды как системы, построенные по точкам алгебраических кривых, характеризуются высокой кардинальностью, лежат выше границы Варшамова-Гильберта и представляют интерес для теории кодирования и защиты информации. При этом криптографически значимый код должен удовлетворять таким требованиям как высокая нелинейность и линейная сложность, обладать корреляционными свойствами, характерными для псевдослучайных последовательностей.

Целью данной работы является исследование криптографических свойств алгебро-геометрических кодов Эрмита (А-ГКЭ).

Алгебраическая кривая задается уравнением кривой Эрмита вида $f = y^4 + y - x^5$, которая на аффинной плоскости в заданном поле имеет рациональные точки $P(x, y)$.

Анализ зависимостей линейной сложности, построенных с помощью алгоритма Берлекэмпа-Месси, показывает, что А-ГКЭ обладают высоким уровнем линейной сложности, близкой к уровням кодам AES и BBS.

Уровень нелинейности оценивался по спектру Уолша-Адамара. Исследования показали близость характеристик А-ГКЭ и криптокода AES.

Процедуры вычисления корреляционных значений, поиска и отбора позволили определить множества кодовых слов алгебро-геометрических кодов Эрмита с низким уровнем боковых лепестков корреляционных функций.

Полученные результаты позволяют рекомендовать использование алгебро-геометрических кодов Эрмита в криптографических преобразованиях и процедурах аутентификации.