Вестник ДГТУ, 2005.Т.5.№1(23) *ISBN 5-7890-0319-2*

МАТЕМАТИКА

УДК 681.324

В.М. ДЕУНДЯК, Д.В. ХАРЧЕНКО

О РЕАЛИЗАЦИИ ПОМЕХОУСТОЙЧИВЫХ КОДЕКОВ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ С ИСПОЛЬЗОВАНИЕМ АЛГОРИТМОВ ДЕКОДИРОВАНИЯ СЕРЕБРЯКОВА

Разработаны структурные схемы новых кодеков для алгебро-геометрических кодов на эллиптических кривых с использованием принципиальных алгоритмов декодирования Серебрякова. Полученная программная реализация кодеков позволяет использовать их в компьютерных системах помехоустойчивой связи.
Ключевые слова: *алгебро-геометрические коды, эллиптические кривые, помехоустойчивые кодеки.*

1. Введение и постановка задачи. Для организации надежной передачи информации по каналам связи широко используются различные классы помехоустойчивых кодов. Наряду с детерминированными алгоритмами декодирования [1] в последние годы активно разрабатываются вероятностные алгоритмы, позволяющие увеличить исправляющую способность кода [2]. Большой теоретический интерес представляют интенсивно исследуемые алгебро-геометрические коды (АГ-коды), обладающие замечательными асимптотическими свойствами [3], хотя в настоящее время для этих кодов затруднительна аппаратная реализация декодеров. Однако специалисты считают, что техническая проблема эффективной реализации декодеров для АГ-кодов в ближайшем будущем будет решена [4]. В связи с этим представляется актуальным с помощью компьютерных моделей предварительное экспериментальное исследование как кодеков для АГ-кодов, так и построенных на их основе каскадов. В работе [5] получены два принципиальных алгоритма декодирования АГ-кодов на эллиптических кривых: детерминированный алгоритм для классического случая, когда число ошибок не превосходит половину конструктивного кодового расстояния, и более медленный вероятностный алгоритм для случая, когда число ошибок может превосходить половину конструктивного расстояния. Настоящая работа посвящена разработке структурных схем кодеков, основанных на этих алгоритмах, и проблемам их программной реализации.

2. АГ-коды на эллиптических кривых. Приведем необходимые сведения о семействе АГ-кодов, используемых в работе [5]. Пусть F_q – поле Галуа мощностью q, где q – простое число, большее 3. Невырожденная эллиптическая кривая X над F_q задается уравнением

$$y^2=x^3+ax+b \qquad (4a^3+27b^2\neq 0). \tag{1}$$

Пусть O – бесконечно удаленная точка кривой X, s – натуральное число, $L(sO)$ – линейное пространство рациональных функций на X, у которых порядок полюса в точке O не превосходит s, а других полюсов нет. По теореме Римана-Роха (см. [3]) dim $L(sO) = s$. Пусть $f_1,\dots,f_s$ – базис $L(sO)$, $\Omega = \{P_1,\dots,P_N\}$ – некоторое множество точек кривой X, $O \notin \Omega$ и $N > s$. Рассмотренный в работе [5] АГ-код C, связанный с тройкой (X,Ω,sO), задается проверочной матрицей