УДК 681.3.06

А.А. КУЗНЕЦОВ, канд. техн. наук, А.В. ПОТИЙ, канд. техн. наук

ОБНАРУЖИВАЮЩАЯ СПОСОБНОСТЬ ПОМЕХОУСТОЙЧИВЫХ КОДОВ И СХЕМ АУТЕНТИФИКАЦИИ

Введение

Техническая задача теории помехоустойчивого кодирования состоит в защите цифровых данных от появляющихся в процессе передачи по каналам связи ошибок. С этой целью в передаваемые данные по некоторому правилу (не секретному) вносится избыточная информация. На основе внутренней структуры передаваемых данных на приемной стороне обнаруживаются (возможно, исправляются) возникшие ошибки. Обнаружение, а соответственно и исправление возникших ошибок носит вероятностный характер и зависит от качества канала связи. Техническая задача теории аутентификации состоит в установлении подлинности информации после возможного на нее воздействия злоумышленником. На основе внутренней структуры передаваемой информации в нее вносят избыточность, сформированную по некоторому (секретному) правилу. На приемной стороне проверяют соответствие переданных данных внесенной избыточности. Установление подлинности также носит вероятностный характер и зависит от выбранной стратегии злоумышленника по навязыванию ложной информации.

Очевидно, что, несмотря на различные технические задачи в теории кодирования и теории аутентификации, используется один способ вероятностного достижения цели – внесение в передаваемые данные сформированной избыточности. При заданной вероятности достижения цели вносимая избыточность минимизируется. Задачей данной работы является исследование обнаруживающей способности помехоустойчивых кодов и схем аутентификации блоков данных, изучение их вероятностных характеристик.

1. Обнаруживающая и исправляющая способность алгебраических кодов, вероятность необнаружения ошибки и вероятность ошибочного декодирования

Рассмотрим алгебраический блоковый код (n,k,d), где n-длина кода (блока), k-число информационных кодовых символов, d-минимальное кодовое расстояние.

Предположим, что ошибки в последовательно передаваемых кодовых символах происходят независимо с вероятностью P_o. Тогда вероятность ошибки кратности i на длине блока n будет

$$P_i = C_n^i P_o^i (1-P_o)^{n-i}.$$

Если код обнаруживает $d-1$ ошибок, то вероятность необнаружения ошибки в блоке

$$P_{но} \geq \sum_{i=d}^{n} P_i = \sum_{i=d}^{n} C_n^i P_o^i (1-P_o)^{n-i}. \qquad (1)$$

Равенство выполняется, если используется эквидистантный код (значения минимального и максимального кодового расстояния совпадают).

Если код правит t ошибок, то вероятность ошибочного декодирования блока

$$P_{од} \geq \sum_{i=t+1}^{n} P_i = \sum_{i=t+1}^{n} C_n^i P_o^i (1-P_o)^{n-i}. \qquad (2)$$

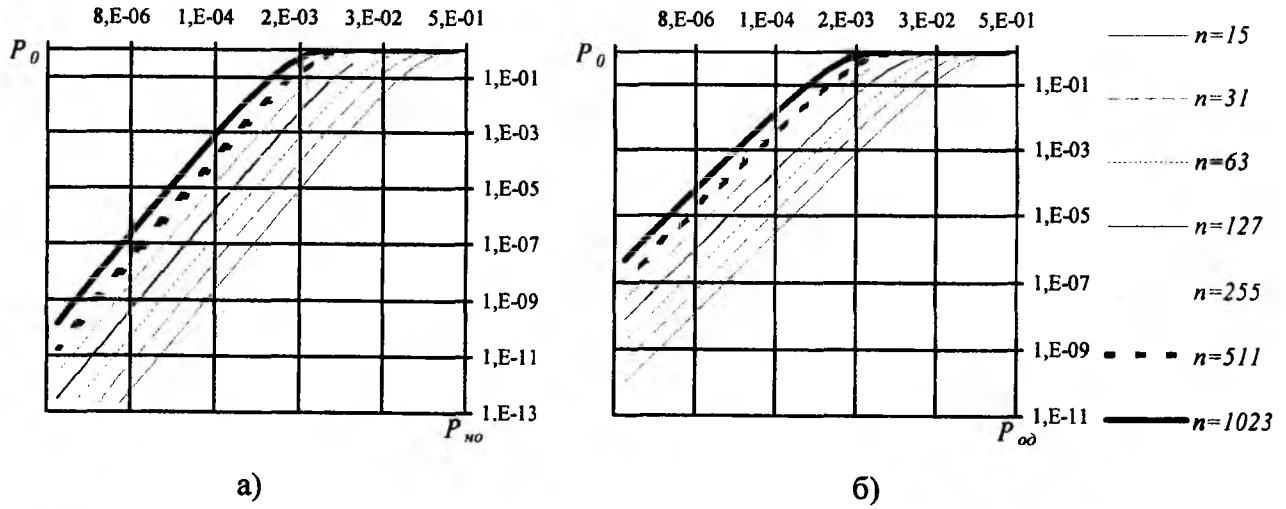
Равенство выполняется, если используется совершенный код. Для совершенного кода сферы одинакового радиуса вокруг кодовых слов, не пересекаясь, покрывают все пространство (радиус сферической упаковки кода совпадает с радиусом покрытия кода). Очевидно, что любой совершенный код является эквидистантным, однако не всякий эквидистантный код совершенен. Важным семейством совершенных кодов, которые легко кодировать и декодировать, являются коды Хемминга, исправляющие одну ошибку [1]. Для двоичного случая коды Хемминга удовлетворяют соотношению

$$\left(n = 2^r - 1, k = 2^r - 1 - r, d = 3\right). \quad (3)$$

При использовании двоичных кодов, лежащих на границе Хемминга, величина t определяется как наименьшее целое, удовлетворяющее неравенству

$$2^{n-k} \geq \sum_{i=0}^{t} C_n^i .$$

На рис.1 представлены зависимости: а) вероятности необнаружения ошибки $P_{но}$; б) вероятности ошибочного декодирования $P_{оо}$ для кодов Хемминга от P_0 для различных n с вносимой избыточностью $r = \overline{4,10}$



а) б)

Рис.1

Приведенные зависимости описывают идеальный случай – эквидистантный совершенный код с характеристиками (3), для которого существуют эффективные алгоритмы декодирования. Совершенные коды (если они существуют) обладают замечательными свойствами, однако они достаточно редки, вследствие чего имеют ограниченное практическое значение. Квазисовершенные коды (для которых все слова лежащие вне радиуса сферической упаковки кода находятся на расстоянии $t+1$ хотя бы от одного кодового слова) встречаются чаще, чем совершенные коды. Однако, они так же достаточно редки и не находят широкого применения. В практических схемах, как правило, используются каскадные конструкции кодов, характеристики которых отличны от (3). Выражения (1) и (2) в этом случае используют для оценки потенциальных обнаруживающих и исправляющих способностей алгебраических кодов – граничных вероятностей необнаружения ошибки и ошибочного декодирования.

2. Обнаруживающая способность кодов аутентификации, вероятность коллизии

Рассмотрим кодовую последовательность длины k. По некоторому правилу (секретному) сформируем и присоединим к ней аутентификатор длины r. Для двоичного случая мощность множества всех полученных таким образом блоков составит 2^k. При передаче блока возможно его искажение (как умышленное, так и в результате воздействия помех). Если аутентификатор для кодовой последовательности в искаженном блоке не соответствует сформированному по фиксированному правилу, то ошибка (или преднамеренное искажение блока) будет обнаружена. Искаженный блок, кроме того, может соответствовать разрешенному блоку, т.е. блоку, аутентификатор которого соответствует сформированному по фиксированному правилу. В этом случае наблюдается коллизия – совпадение аутентификаторов для двух различных кодовых последовательностей. Вероятность такого события соответствует вероятности необнаружения ошибки для помехоустойчивых кодов. Если искажение блока преднамерено, то совпадение аутентификаторов приведет к навязыванию ложной кодовой последовательности. Мощность множества принимаемых блоков 2^{k+r}. Вероятность коллизий

$$P_{кол} = \frac{2^k}{2^{k+r}} = 2^{-r} \qquad (4)$$

и зависит только от длины аутентификатора.

Это выражение дает нижнюю границу и соответствует идеальному правилу формирования кодов аутентификации. Физический смысл такого правила состоит в равновероятном распределении кодовых последовательностей по аутентификаторам. Другими словами, для всех аутентификаторов число соответствующих им кодовых последовательностей одинаково. В практических схемах формирования кодов аутентификации вероятность коллизий определяют, как правило, статистической проверкой гипотезы о предполагаемом значении вероятности. Исключение, в этом смысле, составляют схемы, эквивалентные строго универсальному классу хеширующих функций [2-3]. Значение вероятности коллизий для таких схем определяют не проверкой гипотезы, а постулированием свойств хеширирующего класса. Ортогональные таблицы [1] соответствуют строго универсальному классу, вероятность коллизий которого определяется (4). Практического распространения такие схемы не получили в виду того, что необходимый объем ключевых данных превышает объем передаваемых данных [4]. Композиционная схема ортогональных таблиц и алгебраических кодов [5] лишена подобных недостатков, она также соответствует строго универсальному классу, вероятность коллизий которого определяется выражением

$$P_{кол} = 2^{-r+1}.$$

Отметим, что в выражение для вероятности коллизий не входят вероятностные характеристики качества канала связи. Это объяснимо тем, что искажение блока данных может быть преднамеренным, а любые искажения вследствие воздействия помех можно интерпретировать как действия противника. Искажение кодовых символов определяется стратегией злоумышленника, которая, строго говоря, может заключаться в случайном искажении (или его замене) блока данных. В этом случае технические задачи аутентификации и помехоустойчивого кодирования совпадают, а физический смысл вероятности коллизий соответствует вероятности необнаружения ошибки.

3. Сравнительный анализ вероятностных характеристик помехоустойчивого кодирования и схем формирования аутентификаторов

Основное отличие теории алгебраических кодов от теории аутентификации состоит в распределении множества 2^k кодовых слов по множеству 2^n блоков. В первом случае распределение кодовых слов должно быть таким, чтобы наиболее вероятные изменения любого кодового слова лежали как можно ближе к нему. Наилучшим кодом в таком случае будет тот, который:

- для фиксированного множества 2^n блоков распределит 2^k кодовых слов таким образом, что мера различия между любыми двумя кодовыми словами будет одинакова для всего их множества (эквидистантность кода);
- для фиксированного множества 2^{n-k} блоков распределит их по каждому кодовому слову из множества 2^k так, что наименее отличающиеся от кодового слова блоки расположены ближе к нему и наоборот, блоки с большей мерой отличия расположены дальше (обнаружение наиболее вероятных ошибок).

В теории аутентификации распределение кодовых слов должно быть таким, чтобы минимизировать вероятность перехода из одного кодового слова в другое. Строго говоря, выбор распределения должен исходить из предполагаемой стратегии злоумышленника по навязыванию ложных блоков. Если учесть самую примитивную из стратегий – навязывание путем случайного изменения блока, то очевидно, распределение кодовых слов для целей аутентификации должно удовлетворять первому условию распределения кодовых слов для целей помехоустойчивого кодирования. Выполнение второго условия необязательно. Это означает, что для целей аутентификации сообщений необязательна группировка наиболее вероятных

изменений кодового слова вокруг него. Обязательно равновероятное распределение этих изменений по всему множеству 2^n слов. Такое распределение возможно при выполнении равенства числа кодовых последовательностей, соответствующих каждому аутентификатору.

Положим $r \le k$. Тогда если число кодовых слов, соответствующих фиксированному аутентификатору соответствует

$$\frac{2^k}{2^r} = 2^{2k-n}$$

для всего множества аутентификаторов, то имеем идеальное правило формирования аутентификаторов, вероятность коллизий при котором соответствует (4). Интерес представляет сравнение обнаруживающей способности помехоустойчивых алгебраических кодов и кодов аутентификации. На рис. 2 представлены зависимости вероятности необнаружения ошибки $P_{но}$, вероятности ошибочного декодирования $P_{оо}$ эквидистантных совершенных кодов и вероятности коллизий $P_{кол}$ кодов аутентификации от P_0 для различных n при внесенной избыточности r: а) $r = 10$; б) $r = 20$; в) $r = 30$; г) $r = 40$.

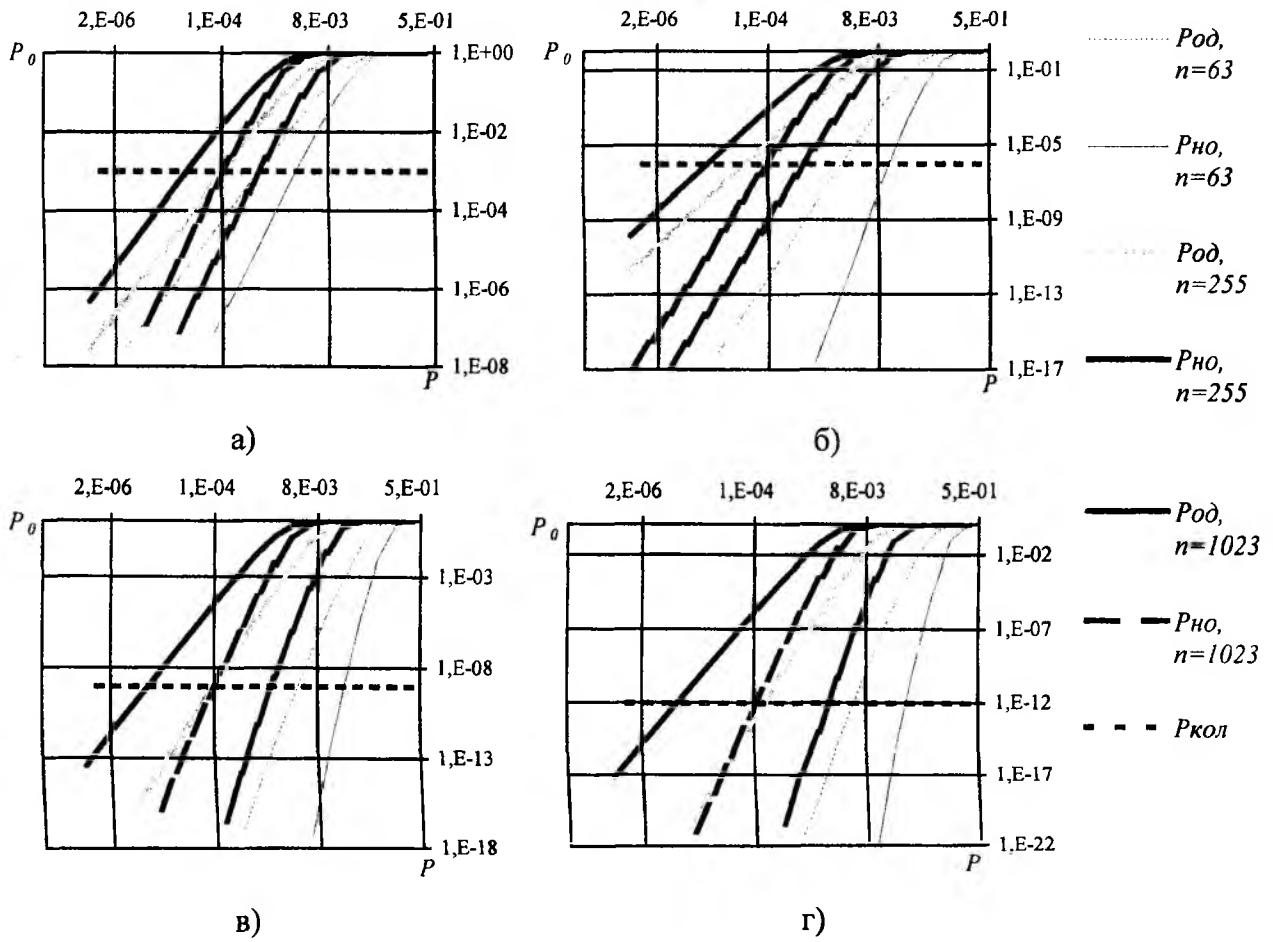


Рис.2

Интерес представляют схемы, решаюшие одновременно две задачи - защиту цифровых данных от ошибок в канале связи и задачу установления подлинности информации. Исправляющую способность такой конструкции предлагается использовать для обнаружения и исправления ошибок в канале связи, а обнаруживающую способность предлагается использовать для проверки подлинности передаваемых блоков. Если такая конструкция соответствует эквидистантному коду, то возможность навязывания ложного блока при исправлении ошибок минимизируется. Это объяснимо тем, что навязывание, соответствующее переходу одного кодового слова в другое, возможно в случае исправления декодером d ошибок, что невозможно по определению. Если код совершенен, то значение вероятности ошибочного декоди-

рования будет лежать на границе (2). Обнаруживающая способность такой конструкции будет соответствовать (1) при обнаружении ошибок в канале связи, а для решения задачи аутентификации блоков – выражению (4). Значение вероятности ошибки декодирования такой конструкции ограничено $P_{од}$ на рис.2., а значение вероятности навязывания ложных блоков данных будет ограничена вероятностью коллизий $P_{кол}$.

Список литературы: **1.** *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки: Пер. с англ. М.: Связь, 1979. 744 с. **2.** *J. L. Carter, M. N. Wegman.* Universal classes of hash functions. //J. Computer and System Sci. 18 (1979), 143-154. **3.** *D. R. Stinson.* Universal Hashing and Authentication Codes. //Designes, Codes and Criptography 4 (1994), 369-380. A preliminary version appeared in the Procecdins of CRYPTO 91, Lecture Notes in Computer Science 576 (1992), 74-85. **4.** *Г.З. Халимов, А.А.Кузнецов.* Аутентификация и универсальное хеширование // Радиотехника: Всеукр. межвед. науч.-техн. сб. 2001. Вып. 119. С 88-94. **5.** *Г.З. Халимов, А.А.Кузнецов.* Аутентификация с применением алгеброгеометрических кодов // Радиотехника: Всеукр. межвед. науч.-техн. сб. 2001. Вып. 119. С 81-87.

Харьковский военный университет

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 19.03.2002