На правах рукописи

Фам Суан Нгиа

МОДИФИКАЦИИ АЛГОРИТМА МАК-ЭЛИС ДЛЯ ПОВЫШЕНИЯ ПОКАЗАТЕЛЕЙ КАЧЕСТВА РАДИОСИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ

Специальность: 05.12.04 –
‹‹Радиотехника, в том числе системы и устройства телевидения››

АВТОРЕФЕРАТ
диссертации на соискание учёной степени
кандидата технических наук

Рязань 2007

Работа выполнена в ГОУВПО «Рязанский государственный радиотехнический университет»

Научный руководитель - Заслуженный работник высшей школы РФ, доктор технических наук, профессор **Кириллов Сергей Николаевич**

Официальные оппоненты - Доктор технических наук, профессор **Паршин Юрий Николаевич**

- Кандидат технических наук, доцент **Бурнашев Рустам Умидович**

Ведущая организация - ФГУП ОКБ «Спектр» (г.Рязань)

Защита состоится ‹‹23›› мая 2007 г. в 12 часов на заседании диссертационного совета Д 212.211.04 в Рязанском государственном радиотехническом университете по адресу 390005, г. Рязань, ул. Гагарина, д. 59/1.

С диссертацией можно ознакомиться в библиотеке РГРТУ.

Автореферат разослан « » апреля 2007г.

Ученый секретарь
диссертационного совета
кандидат технических наук  А.Г. Борисов

ОБЩАЯ ХАРАКТЕРИСТИКА ДИССЕРТАЦИОННОЙ РАБОТЫ

Актуальность темы. Одной из важнейших задач при построении современных систем передачи информации является проблема повышения надежности, помехоустойчивости, скрытности и скорости передаваемой информации.

Кроме того, эти системы должны выполнять поставленные задачи в условиях действия различного вида помех.

Одним из решений данной задачи является использование помехоустойчивого кодирования в системах передачи информации. Целесообразность кодирования информации впервые была показана в работе Шеннона К., где было доказано, что если скорость создания сообщений источником не превосходит некоторой величины, называемой пропускной способностью канала, то при правильно выбранных методах кодирования и декодирования можно вести передачу по каналу с шумом со сколь угодно малой вероятностью ошибки. Основные задачи помехоустойчивого кодирования связаны с построением кодов с высокой корректирующей способностью и разработке высокоэффективных, практически реализуемых алгоритмов их декодирования.

Значительный вклад в области повышения помехоустойчивости передаваемой информации внесли такие учёные как Котельников В. А., Злотник Б. М., Кларк Д. Ж., Кейн Д. Ж., Питерсон У., Уэлдон Э., Месси Б. Дж., Кассами Т., Токура Н., Морелос-Сарагоса Р., Золотарёв В. В., Самсонов Б., Плохов Е. М., и.др.

Другим важным требованием к системам передачи информации является обеспечение скрытности, которая характеризуется способностью системы противостоять мерам, направленным на раскрытие содержания информации. Обеспечение скрытности передаваемой информации включает комплекс мер затрудняющих: обнаружение сигнала, определение структуры обнаруженного сигнала (на основе определения ряда его параметров) и раскрытие смысла содержащегося в передаваемой информации. Одним из методов, часто использующимся для повышения скрытности информации, является применение кодирования. Повышением скрытности передаваемой информации занимались Шеннон К., Тузов Г. И., Сивов В. А., Брюс Щнайер, Саломаа А., Алферов А. П., Зубов А. Ю., Нечаев В.И, Молдовян Н. А, Молдовян А. А, Венбо Мао и.др.

В настоящее время широко используются такие системы кодирования, как RSA, Эль-Гамаля, “проблемы рюкзака ”, и. др. Однако, для реализации данных алгоритмов требуются значительные вычисленные затраты, большое количество операций, что приводит к увеличению времени шифрования и дешифрования. Высокая сложность устройств кодирования и декодирования в этих системах затрудняет реализацию алгоритмов в реальном масштабе

времени и существенно ограничивает скорость передачи информации. Кроме того, эти алгоритмы имеют низкую помехоустойчивость.

В отличие от этих систем алгоритм Мак-Элис, основанный на использовании линейных кодов, позволяет одновременно обеспечивать заданную помехоустойчивость и скрытность передаваемой информации. Однако, данный алгоритм обладает такими недостатками, как низкая кодовая скорость, большая длина кодового слова, значительный размер закрытого и открытого ключа. Для широкого использования данного алгоритма, необходимо устранить вышеперечисленные недостатки.

Таким образом, актуальной задачей является исследование и разработка модификаций алгоритма Мак-Элис, позволяющих повысить помехозащищенность высокоскоростных систем передачи информации.

Цель работы. Основной целью работы является разработка и обоснование модификаций алгоритма Мак-Элис в интересах повышения эффективности по скорости, скрытности и помехоустойчивости передачи информации.

Поставленная в работе цель включает решение следующих задач:

– анализ устойчивости алгоритма Мак-Элис в случае действия комплекса помех, при использовании различных линейных кодов (например, коды Хэмминга, Боуза – Чоудхури – Хоквингема, Рида–Соломона, Гоппы, самоортогональных кодов (СОК), произведение кодов, турбо кодов);
– модификации алгоритма Мак-Элис в интересах повышения скрытности, скорости и помехоустойчивости передачи информации;
– исследования применения комбинированных кодов в качестве линейных кодов алгоритма Мак-Элис, позволяющих значительно увеличить помехоустойчивость и скрытность передаваемой информации данного алгоритма;
– исследования применения модификаций алгоритма Мак-Элис для электронной цифровой подписи (ЭЦП) в радиосистемах передачи информации;
– анализ реализации модификаций алгоритма Мак-Элис при использовании программированных логических интегральных систем (ПЛИС) в высокоскоростных системах передачи информации.

Методы проведения исследований. В работе использовались методы статистической радиотехники, математической статистки, численные методы вычислительной математики. Данные теоретические методы сочетались с экспериментальными исследованиями на основе имитационного моделирования.

Научная новизна. В рамках данной работы были получены следующие новые научные результаты:

1. Оценена устойчивость алгоритма Мак-Элис при действии комплекса широкополосной, узкополосной, структурной и импульсной помех в

случае использования кодов Хэмминга, Боуза – Чоудхури – Хоквингема, Рида–Соломона, Гоппы, произведение кодов, СОК, турбо кодов с различными кодовыми скоростями и определена самая опасная помеха.

2. Обоснована модификация алгоритма Мак-Элис на основе изменения исходной последовательности и добавления информации в вектор ошибки, позволяющая повысить скрытность передачи информации и кодовую скорость.
3. Предложены модификации блок-схемы алгоритма Мак-Элис при использовании комбинированных кодов (параллельных и произведения кодов), позволяющие повысить помехоустойчивость и скрытности передачи информации.
4. Предложена модификация алгоритма Мак-Элис с преобразованием исходной информации путем сжатия и использования вектора ошибок, позволяющая получить выигрыш в информационной скрытности, а также значительно повысить кодовую скорость.
5. Показана возможность применения алгоритма Мак-Элис для ЭЦП, а также в радиосистемах передачи информации.

Практическая ценность.

Представленные в работе модифицированные алгоритмы Мак-Элис, имеют высокую помехоустойчивость, скрытность передачи информации и кодовую скорость, что позволяет их использовать для ЭЦП и в различных радиосистемах передачи информации. Модифицированные алгоритмы Мак-Элис, использующие комбинированные коды и обладающие высокой способностью исправлять ошибки, могут применяться в системах передачи данных, требующих высокую помехоустойчивость. Результаты диссертационной работы нашли применения в сетях передачи данных в ОАО «Телекоммуникационной компании Ринфотелс», а также в ГОУ ВПО «Рязанский государственный радиотехнический университет».

Основные положения, выносимые на защиту:

1. Модифицированный алгоритм Мак-Элис, основанный на добавлении информации в вектор ошибки и изменении исходной информации путем использования матрицы хеширования, обеспечивающей информационную скрытность до $1{,}37.10^{16}$ при использовании кода Гоппы (1024, 524).
2. Модифицированный алгоритм Мак-Элис основанный на добавлении информации в вектор ошибок, позволяющий повысить кодовую скорость на ~60%.
3. Модифицированный алгоритм Мак-Элис основанный на использовании параллельных кодов, позволяющий повысить информационную скрытность в 10^{14} раз (при длине кодового слова n=7) по сравнению с исходным алгоритмом.

4. Модифицированный алгоритм Мак-Элис, основанный на применении произведения кодов, обеспечивающий информационную скрытность более $1{,}37.10^{16}$ и число исправляемых ошибок до 91 бит при использовании произведения кода Х(15,11)БЧХ(1024,728).
5. Модифицированный алгоритм Мак-Элис с преобразованием исходной информации путем сжатия и использования вектора ошибок, позволяющий получить информационную скрытность $K \approx 1{,}37.10^{16}$ в случае использования кода Гоппы (1024,524), а также повысить кодовую скорость до 0,95.

Апробация работы. Результаты работы докладывались на следующих научно-технических конференциях:

1. 52-я Студенческая Научно–Техническая Конференция. 2005, Рязань.
2. Всероссийская научно-практическая конференция студентов, молодых учёных и специалистов "Новые информационные технологии в научных исследования и в образовании". 2005, Рязань.
3. Всероссийская научно-практическая конференция "Сети и системы связи", 2005. Рязань.
4. Международная научно-техническая конференция «Проблемы передачи и обработки информации в сетях и системах телекоммуникации». 2005, Рязань.
5. Международная молодежная научная конференция, посвященная 1000 летию города Казани "Туполевские чтения". 2005, Казань.
6. Всероссийская научно-практическая конференция студентов, молодых учёных и специалистов "Новые информационные технологии в научных исследования и в образовании". 2006, Рязань.
7. Всероссийская научно-практическая конференция "Сети и системы связи", 2006. Рязань.
8. Всероссийская научно-практическая конференция студентов, молодых учёных и специалистов "Новые информационные технологии в научных исследования и в образовании". 2007, Рязань.
9. Всероссийская научно-практическая конференция "Сети и системы связи", 2007. Рязань.

Публикации. По теме диссертации опубликовано 13 работ. Из них 3 статьи в журналах, рекомендованных ВАК РФ для кандидатских диссертаций, 1 статья в межвузовских сборниках, 9 тезисов докладов.

Структура и объём работы. Диссертационная работа состоит из введения, трех глав, заключение, списка литературы из 119 наименований и 3 Приложений. Диссертация содержит 168 стр., в том числе 132 стр. основного текста, 12 таблиц и 92 рисунка.

СОДЕРЖАНИЕ ДИССЕРТАЦИОННОЙ РАБОТЫ

Во введении обоснована актуальность выбранной темы; дан обзор состояния вопроса; определены цель и решаемые в работе задачи; изложены новые научные результаты, полученные в работе; показаны её практическая ценность и апробация; сформулированы основные положения, выносимые на защиту.

В первой главе описан алгоритм Мак-Элис и приведены результаты анализа его помехоустойчивости при использовании различных помехоустойчивых кодов в случае действия комплекса помех, включающих широкополосные, узкополосные, структурные и импульсные помехи.

Особенностью алгоритма Мак-Элис является использование линейного кода (с порождающей матрицей G и количеством исправляемых ошибок t), позволяющего не только повысить помехоустойчивость, но и увеличить скрытность передаваемой информации.

Параметрами алгоритма Мак – Элис являются целые числа k, n и t, где k – длина информационного сообщения, n – длина кодового слова, t – количество искусственно вводимых ошибок. Каждому абоненту системы для получения открытого и соответствующего закрытого ключа следует выполнить следующие действия:

- определить порождающую матрицу G_{kxn} двоичного (n, k) - линейного кода, исправляющего t ошибок, для которого известен эффективный алгоритм декодирования;
- случайно выбрать двоичную невырожденную матрицу S_{kxk};
- случайно выбрать подстановочную матрицу P_{nxn};
- вычислить произведение матриц $G_p = S \cdot G \cdot P$.

Открытым ключом является пара (G_p, t), закрытым - тройка **(**S,G,P**).** Алгоритм Мак – Эллис показан на рисунке 1, где блок формирования k, n, t, e, S, P, G - формирует все необходимые параметры алгоритма, блоки $\boldsymbol{S^{-1}}$, $\boldsymbol{P^{-1}}$, $\boldsymbol{G^{-1}}$ – вычисляет обратные матрицы, необходимые для декодирования, блок **ИИ** – источник информации, представляет собой генератор случайных чисел. Данный блок генерирует псевдослучайную последовательность импульсов с амплитудой [0,1] заданной длины k, блок ***Кодер*** осуществляет кодирование по алгоритму Мак – Элис, блок **М** – манипулирует по фазе кодовую последовательность, блок ***Канал*** представляет собой модель канала связи с аддитивным белым гауссовым шумом (АБГШ), блок комплекса помех **КП** в зависимости от выбранных типов исследуемых помех формирует модели этих помех, блок ***Декодер*** – осуществляет декодирование по алгоритму Мак – Эллис, блок >< - подсчитывает BER среднюю вероятность ошибки на бит – вероятность превышения числом ошибочно принятых символов заданного значения.

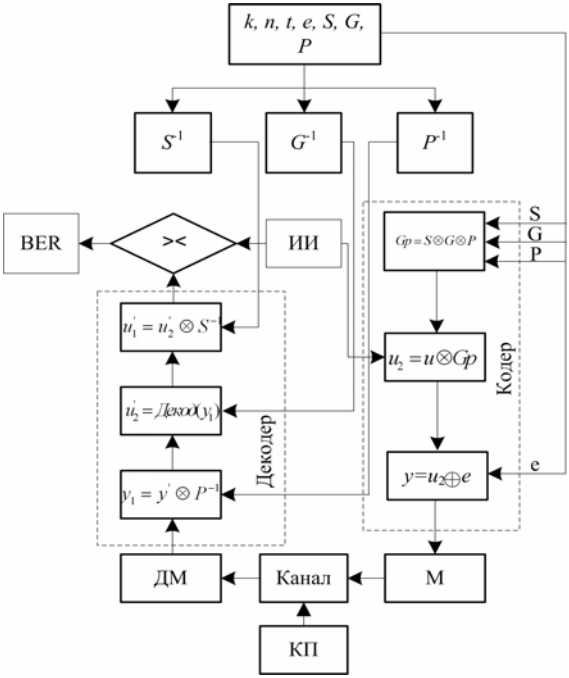

Рисунок 1

Для кодирования сообщения M, предназначенного для абонента В, абоненту А необходимо выполнить следующие действия:

- представить M в виде двоичного вектора u длины k;
- выбрать случайный бинарный вектор ошибок e длины n, содержащий не более t ошибок;
- вычислить бинарный вектор $y = uGp + e$ и передать его абоненту В.

Здесь, расчеты выполнены по модулю 2.

Получив сообщение y, абонент В вычисляет вектор $y_1 = y\,P^{-1}$, с помощью которого, используя алгоритм декодирования кода с порождающей матрицей G, получает векторы u_1 и $u = u_1\,S^{-1}$.

Корректность приведенного алгоритма подтверждает следующее выражение:

$$y_1 = yP^{-1} = (uG_p + e)P^{-1} = \qquad (1)$$

$$(uSGP + e)P^{-1} = (uS)G + eP^{-1},$$

где eP^{-1} – вектор, содержащий не более t единиц. Поэтому алгоритм декодирования кода с порождающей матрицей G декодирует y в вектор

$$u_1 = uS. \qquad (2)$$

Полученные в первой главе результаты показали, что наиболее высокая помехоустойчивость наблюдается при использовании турбо кодов в алгоритме кодирования информации Мак-Элис. Например, при действии широкополосной помехи, для достижения средней вероятности ошибки P_e=10^{-4}, в случае использование турбо кода, имеющего скорость кодирования r=1/2 необходимо отношение сигнал – шум $q_ш$=2,8 дБ, а при применении произведения кода с внешним кодом Х(15,11) и внутренним БЧХ(127, 92) со скоростью кодирования r = 0,53 − $q_ш$= 5,6 дБ. В случае использования самоортогонального кода СОК (162, 81) (r = 0,5) с многопороговым декодером − $q_ш$=6,7 дБ, а при применении кода БЧХ и Хэмминга со скоростью r≈1/2 отношение сигнал-шум $q_ш$ больше, чем 6 дБ.

СОК при использовании порогового или многопорогового декодирования (МПД) обладает выигрышем во времени кодирования и декодирования по сравнению с других представленными кодами, в частности на два – три порядка по сравнению с турбо кодами, которые требуют самое большое время декодирования.

Использование произведения кодов позволяет не только повысить помехоустойчивость информации по сравнению с простыми кодами в 15 раз, но и уменьшить время кодирования и декодирования по сравнению с турбо кодом в два раза.

При действии широкополосной помехи устойчивость произведения кодов ПК Х(31,26)БЧХ(63,51) ухудшается на 0,7 дБ по сравнению с кодом СОК (567, 378) с МПД, имеющим кодовую скорость r≈0,67, при вероятности ошибки на бит P_e=10^{-6}. В случае сравнения с СОК(162, 81) (r =0,5) при действии узкополосной, структурной, так и импульсной помехи преимущество в помехоустойчивости достигает 13 раз.

Наиболее опасной является импульсная помеха для всех кодов, использованных в качестве линейных или комбинированных кодов алгоритма Мак–Эллис. Например, при действии узкополосной, структурной и импульсной помех с отношением сигнал-помеха q_y=q_c=q_u=15 дБ и при наличии широкополосного шума из канала с $q_ш$=2,5 дБ, в случае использования турбо кода, получаются вероятности ошибки P_{ey}= 7.10^{-4}, P_{ec}= 10^{-3} и P_{eu}= 3,2×10^{-3} соответственно.

Во второй главе показаны предложенные в работе варианты повышения эффективности алгоритма Мак-Элис.

На рисунке 2 приведена блок-схема кодирования алгоритма на основе изменения длины исходной последовательности при использовании матрицы $h_{(n\times k)}$, имеющей размер n×k, в вектор ошибок e. В этом алгоритме, входная информация m состоит из исходной информации m_1 и модифицированной информации вектора ошибки $m_2 = eh$.

Кодовое слово c вычисляется по формуле

$$c = mG_p + e. \qquad (3)$$

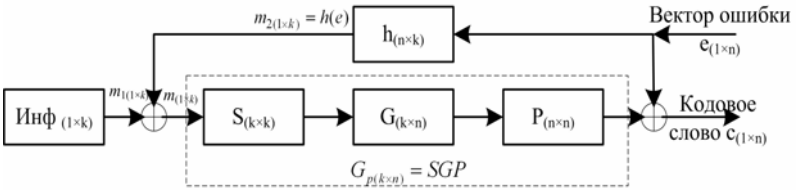

Рисунок 2

Тогда информационная скрытность K вычисляется по формуле

$$K = C_n^k / C_{n-t}^k. \qquad (4)$$

Использование данного алгоритма позволит противостоять атакам, основанным на определении позиций единиц в векторе ошибок e, что значительно повышает информационную скрытность. Например, при применении кода Гоппы (1024, 524) в качестве линейного кода с использованием этого алгоритма, информационная скрытность достигает ~$1{,}37 \cdot 10^{16}$. Кроме того, данный алгоритм позволит расширить пространство закрытых ключей на $2^{n\times k}$ раз по сравнению с исходной схемой. Например, применение кода БЧХ (15, 7) в качестве линейного кода в матрице $h(15,7)$ изменяет вектор $e_{(1\times 15)}$ в последовательность длиной k=7, что повышает пространство закрытых ключей на 2^{105} раз.

Однако, исследование вышепредложенного алгоритма показало, что его помехоустойчивость и скорость передачи информации аналогичны исходному алгоритму Мак-Элис.

На рисунке 3 показана модификация алгоритма Мак-Элис на основе повышения кодовой скорости.

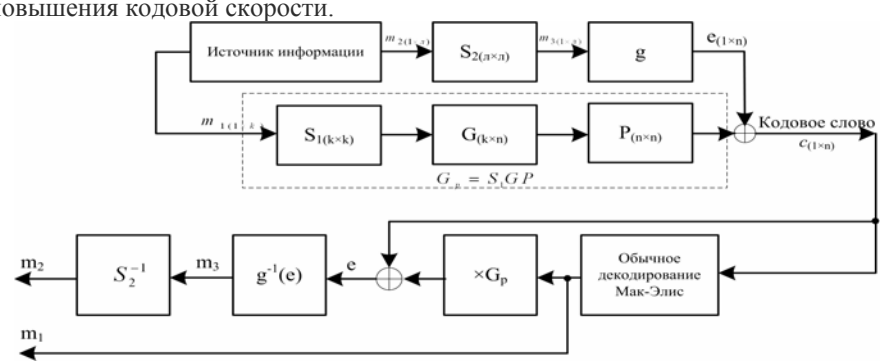

Рисунок 3

Работа данного алгоритма изложена ниже:

Предположим, что входная информация m состоящая из двух частей $m_{1(1\times k)}$ и $m_{2(1\times л)}$, а также квадратная матрица $S_{л\times л}$, используется в интересах изменения позиций бит информационной последовательности m_2.

Тогда кодовое слово можно записать в виде

$$e = c + m_1 G_p, \quad (5)$$

где $e = g(m_2 S_2)$. Причём длина *л* информационной части m_2 должна удовлетворять формуле (4).

Функция *g* выполняет преобразование m_3 в вектор ошибок *e*, который имеет длину *n* и вес *t*.

При декодировании кодового слова *c*, блок информации m_1 получен использованием известного декодирования, а блок информации вычисляет по формуле

$$m_2 = S_2^{-1}(g^{-1}(e)), \quad (6)$$

где $e = c + m_1 G_p$, S_2^{-1} – обратная матрица S_2, g^{-1} – обратная функция *g*.

Добавление информации в вектор ошибки *e* позволяет не только повысить скорость, но и увеличить скрытность передаваемой информации по сравнению с исходной схемой. Например, при использовании кода Гоппы (1024, 524) (добавленное число бит *л* = 264), скорость возрастает с 0,5 до 0,79, а при использовании кода Гоппы (1024, 65) (*л* = 225) в качестве линейного кода скорость возрастает с 0,63 до 0,87. Заметим, что в случае когда злоумышленник декодировал кодовое слово *c* (из канала), он не сможет получить полную информацию, потому что, информационная часть (~60% передаваемой информации) присутствует в векторе *e*. При использовании матрицы S_2 повышается информационную скрытность части m_2, также увеличится пространство закрытых ключей (на $K_ч(m_2) = 0.29 \times 2^{n^2}$). Например, при использовании кода БЧХ (1023,513) в качестве линейного кода алгоритма Мак-Элис, следует, что *л* = 313 и $K_ч(m_2) = 0.29 \times 2^{313^2}$. Анализ данного алгоритма показал, что его помехоустойчивость аналогична исходной схеме, кроме того при этом наблюдается низкая информационная скрытность под действием атаки, основанной на определении позиций единиц в векторе ошибок.

На рисунке 4 показан алгоритм, основанный на совмещении требований повышения кодовой скорости и скрытности передачи информации.

Здесь двоичная матрица *h* имеет размер *n*×*k*. Тогда кодовое слово можно записать как

$$c = (m_1 + h(e_1))G_p + e, \quad (7)$$

где вектор e_1 рассчитывается по формуле

$$e_1 = g(m_2 S_2), \quad (8)$$

а вектор ошибки *e* по формуле

$$e = (g(m_2 S_2))P_2 = e_1 P_2, \quad (9)$$

где P_2 – подстановочная матрица с размером *n*×*n*, S_2 – двоичная невырожденная матрица, имеющая *л*×*л*, функция *g* выполняет преобразование двоичной последовательности $m_4 = m_2 S_2$ с длиной *л* и любым весом в вектор ошибок *e*, который имеет длину *n* и вес *t*.

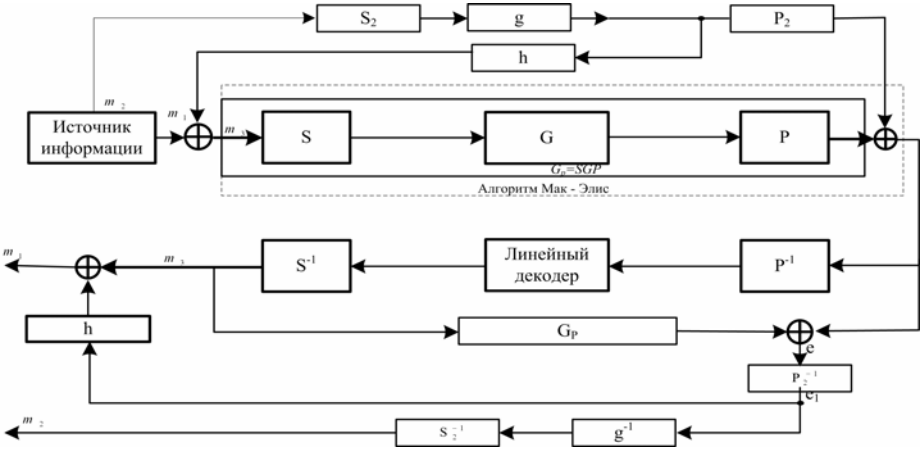

Рисунок 4

Анализ блок-схемы на рисунке 4 показал, что при использовании данного алгоритма затруднено обнаружение информации, передаваемой в векторе *e*. Поэтому можно защитить передаваемую информацию от атак, основанных на повторной передаче информации, при использовании кода Гоппы (1024, 524), при этом информационная скрытность достигает K~1,37.10^{16}. Кроме того, скорость передаваемой информации, благодаря добавлению информации в вектор ошибок, значительно повышается (с 0,5 до 0,79 при использовании кода Гоппы (1024, 524)). В случае применения кода БЧХ (1023, 523) скорость передачи r увеличивается с 0,51 до 0,84 (добавленное количество бит $л$=305), а при использовании кода БЧХ (1023, 618), r увеличивается с 0,6 до 0,85 ($л$=257). Применение двоичной невырожденной матрицы S_2 и подстановочной матрицы P_2, позволит дополнительно повысить пространство закрытого ключа на $\Delta_{Кш}=0.29\times 2^{л^2} n!$. Например, при использовании кода БЧХ (1023, 513), когда $л$ = 313, n=1023, следует $\Delta_{K_{Ш}} = 0,29.2^{313^2}1023!$.

На рисунке 5 приведена блок-схема алгоритма Мак-Элис, использующего параллельные коды. Предлагается блок-схема алгоритма, содержащая две ветви, структура каждой аналогична исходному алгоритму с закрытыми - (S_1,G_1,P_1), (S_2, G_2, P_2) и открытыми ключами (t_1, $G_{p1} = S_1G_1P_1$), (t_2, $G_{p2}= S_2G_2P_2$). Информация на выходе источника состоит из двух частей. Входная информация для каждой ветви представляется строками матриц $m_{1(n_2\times k_1)}$ и $m_{2(n_1\times k_2)}$. Кодирование в каждой ветви выполняет по строкам матриц m_1 и m_2. Блоки M_1 и M_2 объединяют кодовые слова, поступающие из соответствующей ветви, в последовательность длиной n_1n_2, в чем и состоит особенность данного алгоритма.

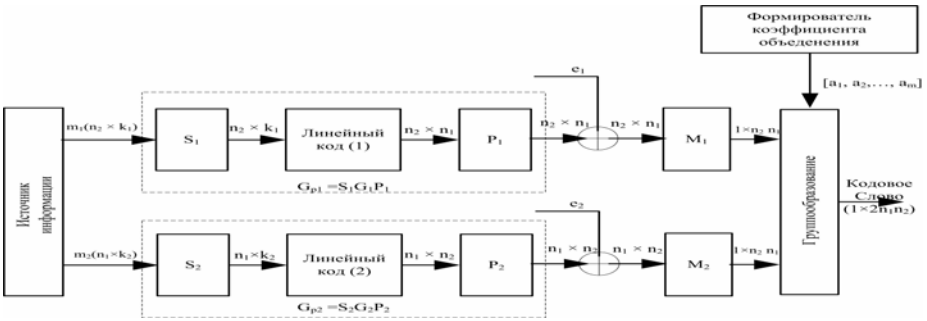

Рисунок 5

Выходная последовательность кодера имеет длину $2n_1n_2$. Декодирование основано на разделении кодовой последовательности на две подпоследовательности длиной n_1n_2, декодирование которых осуществляется на основе исходного алгоритма.

Из анализа блок-схемы алгоритма (рисунок 5) следует, что объединение двух кодовых последовательностей значительно повышает скрытность передаваемой информации. При таком объединении информационная скрытность повышается на $\min(2^{n_1n_2}, C^{n_1n_2}_{2n_1n_2})$ по сравнению с исходной схемой.

Например, при использовании в данном алгоритме двух кодов с длиной кодового слова $n=7$, выигрыш составит порядка $\sim 5\times10^{14}$. Из анализа данного алгоритма следует, что хотя кодовое слово, имеет не большую длину или не большой размер открытого и закрытого ключа, но при этом обеспечивается высокая скрытность.

На рисунке 6 предложен вариант реализации алгоритма Мак-Элис на основе произведения кодов.

Принцип работы данного алгоритма аналогичен исходному алгоритму. Однако, различием между этими алгоритмами является замена простого линейного кода на произведение кодов. Принцип работы и структурная схема алгоритма Мак-Элис при использовании произведения кодов аналогичны исходному алгоритму (рисунок 1).

На рисунке 6, вектор ошибок также содержит часть входной информации. При кодировании необходимо использовать функцию *g* и матрицу *h*. Аналогично первому алгоритму, представленному на рисунке 2, матрица *h* позволяется изменять вектор ошибок с длиной *n* и весом *t* в последовательность m_4 с длиной *k* и любым весом. В данном алгоритме характеристики функции *g*, аналогичны алгоритму, представленному на рисунке 3. Функция *g* осуществляет преобразование информационной части m_2 с длиной *л* и любым весом в вектор ошибок.

Кодирование и декодирование, при использовании данного способа повышения эффективности системы кодирования, осуществляется аналогично исходному алгоритму Мак-Элис.

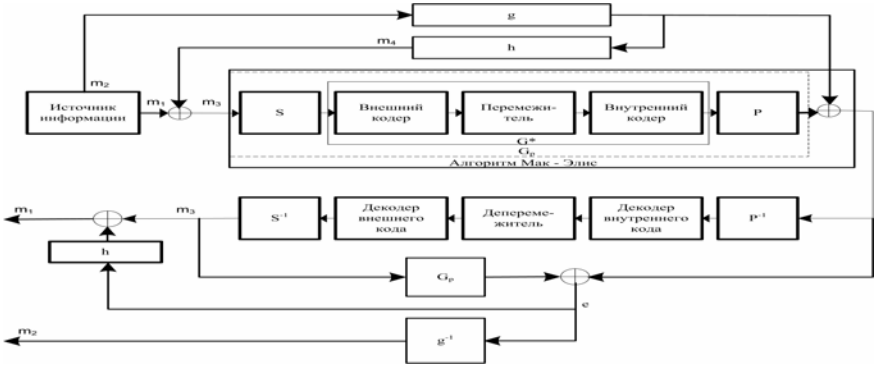

Рисунок 6

При этом открытый ключ вычисляется по следующим формулам:

$$G_p = SG^*P, \tag{10}$$

$$t = (d_1 d_2 - 1)/2, \tag{11}$$

где $G^* = G_1 P_1 G_2$; G_1 – порождающая матрица внешнего кода; G_2 - порождающая матрица внутреннего кода; P_1 – матрица перемежителя; d_1 – минимальное кодовое расстояние внешнего кода; d_2 – минимальное кодовое расстояние внутреннего кода. Закрытым ключом является сочетание пяти матриц (S,G_1,P_1,G_2,P).

информационная скрытность K данной модификации алгоритма Мак-Элис определяется по формуле (4).

Выражение (11) показывает, что исправляющая способность алгоритма представленного на рисунке 6 значительно повышается по сравнению с алгоритмом на основе простых линейных кодов. Использование произведения кодов в алгоритме Мак–Элис обеспечивает выигрыш в информационной скрытности, а так же помехоустойчивости системы передачи информации. Кроме того, при добавлении информации в вектор ошибок можно повысить кодовую скорость на 60% по сравнению с исходной схемой.

Результаты сравнения информационной скрытности и количества исправляемых ошибок в случае использования кода Гоппы (1024, 524), кода БЧХ (1023, 523) и произведения кода с внешним кодом Хэмминга (15, 11) и внутренним БЧХ (1023, 728) в качестве линейного в алгоритме Мак-Элис представлены в таблице 1.

Другой вариант, позволяющий повысить эффективность алгоритма Мак-Элис, реализуется на основе применения метода сжатия информации. Блок-схема данного алгоритма показана на рисунке 7. С использованием этой схемы кроме улучшения помехоустойчивости повышается и скрытность передаваемой информации.

В случае, если противник получил кодовое слово из канала, то он не сможет открыть информацию, т.к. информационная скрытность может достигать $K = 2^{n_2}$.

Таблица 1–***Результаты сравнения кода Гоппы (1024, 524), кода БЧХ (1023, 523) и ПК X(15,11)БЧХ(1023, 728)***

Код / Параметр	Гоппа (1024, 512)	БЧХ (1023, 523)	ПК X(15,11)БЧХ(1023, 728)
Кодовая скорость	0,5	0,51	0,52
Информационная скрытность	$1{,}37\times10^{16}$	$6{,}27\times10^{17}$	$>6{,}27\times10^{17}$
Количество исправляемых ошибок	50	57	91

Например, для кода БЧХ(31,21) требуется k=21, со средним коэффициентом уменьшения длины последовательности на 20%, n_2=26 следует $K\approx10^7$.

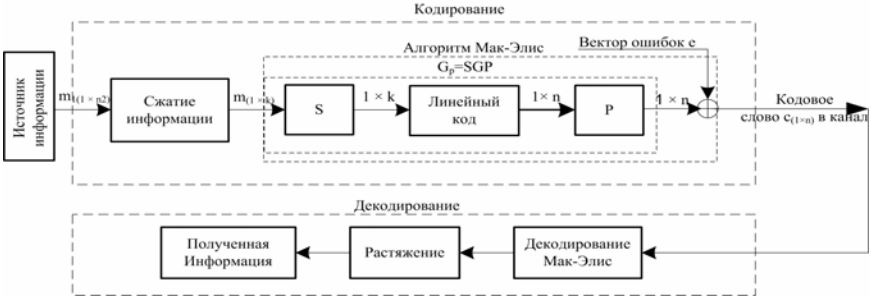

Рисунок 7

Эффективность алгоритма Мак-Элис повысится, если совместить данный алгоритм с алгоритмом на основе добавления информации в вектор ошибок (рисунок 3), в этом случае кодовая скорость вычислят по формуле

$$r = (n_2 + л)/n, \qquad (12)$$

где n_2 – длина исходной последовательности (m_1), $л$ – длина добавленной информации (m_2), n – длина кодового слова. В этом случае кодовая скорость может быть близка к 0,95. Например, при использовании кода БЧХ (31,21,2), как выше определено n_2=26 и $л$=3 (по формуле (12)), следует r=(26+3)/31≈0,93.

В третьей главе рассмотрены вопросы использования модифицированных алгоритмов Мак-Элис для электронной цифровой подписи (ЭЦП), а также вопросы практической реализации алгоритма Мак-Элис на ПЛИС в высокоскоростных системах передачи информации.

Блок-схема радиосистемы передачи информации, применяющая алгоритм Мак-Элис, представлена на рисунке 8 показано, что благодаря замене алгоритмов шифрования и канального кодирования на алгоритм Мак-Элис в 9 раз сократится время обработки сигнала в устройстве. Однако, при применении этого алгоритма для передачи закрытых ключей определенное количество исправляемых ошибок линейного кода используется для создания открытого ключа, поэтому помехоустойчивость системы передачи информации уменьшается.

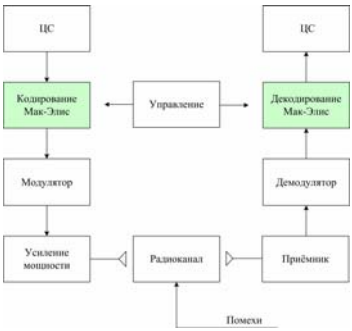

Рисунок 8

Полученные результаты третьей главе показали, что:

–в случае использования исходного алгоритма Мак-Элис не требуется передача секретного алгоритма (или ключа), при этом данный алгоритм обладает преимуществом по скрытности информации ($\sim 10^{50}$). Кроме того, использование модифицированного алгоритма Мак-Элис позволяет повысить в два раза информационную скрытность системы ЭЦП по сравнению с применением исходной схемы.

–достижение заданной помехоустойчивости и скрытности передачи информации в алгоритме Мак-Элис увеличивает сложность устройства и приводит к потерям в отношении сигнал-шум. Эти потери значительно зависят от используемого кода в системе. Например, для достижения средней вероятности на бит $Pe = 10^{-5}$, при использовании кода СОК(567, 378) с МПД в качестве линейного кода потери в отношении сигнал-шум ($\Delta q_ш$) равны 3дБ, что повышает информационную скрытность (K) на $\sim 2\times10^4$, а при применении произведения кода ПК БЧХ(63, 51)Х(31,26) – $\Delta q_ш$=1 дБ и $K=2\times10^4$.

–показано, что количество вычисленных операций в известной схеме системы передачи информации, применяющей RSA и канального кодирования Гоппы (1024,524), в 9 раз выше, чем при использовании алгоритма Мак-Элис. Возможна реализация алгоритма Мак-Элис на ПЛИС XC4VSX55 (семейства Virtex-4), при скорости передачи информации в кодере 250 Мбит/с.

В заключении приведены основные результаты диссертационной работы.

1.Показано, что наиболее высокая помехоустойчивость наблюдается при использовании турбо кодов в алгоритме кодирования информации Мак-Элис. Например, при действии широкополосной помехи, для достижения средней вероятности ошибки $P_e=10^{-4}$, в случае использование турбо кода, имеющего скорость кодирования r=1/2 необходимо $q_ш$=2,8 дБ, а при применении произведения кода с внешним кодом Х(15,11) и внутренним БЧХ(127, 92) со кодовой скоростью r = 0,53 − $q_ш$= 5,6 дБ. В случае использования кода СОК (162, 81) (r = 0,5) с многопороговым декодером − $q_ш$=6,7 дБ, а при применении

кода БЧХ и Хэмминга со скоростью $_r \approx 1/2$ отношение сигнал-шум $q_ш$ больше, чем 6 дБ.

2.Доказано, что использование произведения кодов в алгоритме Мак-Элис позволит не только повысить помехоустойчивость информации по сравнению с простыми кодами до 15 раз, но и уменьшить время кодирования и декодирования по сравнению с турбо кодом в два раза.

3.Показано, что наиболее опасной является импульсная помеха для всех кодов, использованных в качестве линейных или комбинированных в алгоритма Мак–Эллис. Например, при действии узкополосной, структурной и импульсной помех с отношением сигнал-помеха $q_у=q_с=q_и$ =15 дБ и при наличии широкополосного шума из канала с $q_ш$=2,5 дБ, в случае использования турбо кода, получаются вероятности ошибки $P_{еу}= 7.10^{-4}$, $P_{ес}= 10^{-3}$ и $P_{еи}= 3{,}2\times10^{-3}$ соответственно.

4.Показано, что изменение исходной последовательности с использованием функции хеширования в одну сторону, позволяет повысить информационную скрытность до $\sim 1{,}37.10^{16}$ при применении кода Гоппы (1024, 524) в качестве линейного кода в алгоритме Мак-Элис. Предложено для повышения информационной скрытности использовать матрицу (h) с размером ($n\times k$) вместо функции хеширования $h(e)$, что расширило пространство закрытых ключей на 2^{105} раз по сравнению с исходной схемой при k=7, n=15.

5.Предложена модификация алгоритма Мак-Элис при добавлении информации в вектор ошибок, позволяющая повысить кодовую скорость на ~60% при этом наблюдается низкая информационная скрытность действием атаки, основанной на определении позиции единиц в векторе ошибок.

6.Предложена модификация алгоритма Мак-Элис с преобразованием исходной информации путем сжатия и использования вектора ошибок, позволяющая получить выигрыш в скрытности $K\approx 1{,}37.10^{16}$ в случае использования кода Гоппы (1024, 524), а также повысить кодовую скорость до 0,95.

7. Показана возможность применения алгоритма Мак-Элис для ЭЦП при этом не требуется передача секретного алгоритма (или ключа), а скрытность информации повышается в $\sim 10^{50}$ и в два раза возрастает информационную скрытность системы ЭЦП по сравнению с применением исходной схемы.

8.Доказано, что реализация алгоритма Мак-Элис требует в 9 раз меньше вычисленных операций, чем алгоритма RSA и помехоустойчивого кода Гоппы (1024, 524) в системе передачи информации при тех же параметрах.

9.Показана возможность реализации алгоритма Мак-Элис на ПЛИС XC4VSX55 (семейства Virtex-4), при скорости передачи информации 250 Мбит/с.

Список публикаций

1. Крысяев Д.Е., Фам С.Н. Анализ помехоустойчивости алгоритма кодирования информации Мак-Элис // ВНТК «Новые информационные технологии в научных исследования и в образовании». Тезисы докладов 2005.С. 41.

2. Крысяев Д.Е., Фам С.Н. Исследование влияния комплекса помех на алгоритм кодирования информации Мак-Элис // Всероссийский научно-практический семинар. Сети и системы связи. Тезисы докладов 2005. С. 281.
3. Крысяев Д.Е., Фам С.Н. Исследование влияния комплекса помех на алгоритм кодирования информации Mc-Eliece // СНТК-52. Рязанская государственная радиотехническая академия. Тезисы докладов 2005. С. 4.
4. Крысяев Д.Е., Фам С.Н. Исследование помехоустойчивости системы кодирования Мак-Элис // Вестник РГРТА. 2005 №15. С.112-116.
5. Крысяев Д.Е., Фам С.Н. Исследование помехоустойчивости алгоритма кодирования информации Мак-Элис при воздействии комплекса помех // «Туполевские чтения». Тезисы докладов 2005. С. 84-85.
6. Крысяев Д.Е., Фам С.Н. Исследование помехоустойчивости системы передачи информации на основе алгоритма Мак-Элис при использовании кода Рида-Соломона // «Биомедицинские технологии и радиотехника». Рязань 2005.С.140-145.
7. Кириллов С.Н., Крысяев Д.Е., Фам С.Н. Исследование помехоустойчивости алгоритма Мак-Элис на основе кода Гоппы и порогового декодирования блокового самоортогонального кода // 14-ая МНТК «Проблемы передачи и обработки информации в сетях и системах телекоммуникации».Тезисы доклада. Рязань 2005. С.62-63.
8. Крысяев Д.Е., Фам С.Н. Исследование помехоустойчивости алгоритма Мак-Элис на основе каскадного кодирования // ВНТК «Новые информационные технологии в научных исследования и в образовании». Тезисы докладов 2006 – С. 130-131.
9. Крысяев Д.Е., Фам С.Н. Исследование помехозащищенности алгоритма Мак –Элис на основе произведения кодов // Всероссийская научно-практическая конференция. Сети, системы связи и телекоммуникации. Тезисы докладов 2006 С. 154 - 155.
10. Кириллов С.Н., Крысяев Д.Е., Фам С.Н. Способы повышения эффективности системы кодирования информации Мак-Элис // Вестник РГРТУ. 2006. №19. С. 35–39.
11. Фам Суан Нгиа. Анализ применения алгоритма Мак-Элис для электронной цифровой подписи // Вестник РГРТУ 2007. №20. С. 41-45.
12. Фам С.Н. Повышение эффективности алгоритма Мак-Элис на основе сжатия информации // ВНТК «Новые информационные технологии в научных исследованиях и в образовании». Тезисы докладов 2007. С.17.
13. Фам Суан Нгиа. Исследование помехозащищенности алгоритма Мак–Элис на основе турбо кодов // Всероссийская научно-практическая конференция. Сети, системы связи и телекоммуникации. Тезисы докладов 2007. С. 150 - 151.

Фам Суан Нгиа

Модификации алгоритма Мак-элис для повышения показателей качества радиосистем передачи информации

Автореферат диссертации на соискание учёной степени кандидата технических наук

Отпечатано в ГНУ ВНИМС,
Рязань, Щорса 38/11
Формат бумаги 60×84 1/16.
Печатных листов 1.
Заказ № 25 Тираж 100 экз.

16 апреля 2007г.