На правах рукописи

Самохина Марина Андреевна

ПОСТРОЕНИЕ И ИССЛЕДОВАНИЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ КОДОВ В ПРОЕКТИВНЫХ МЕТРИКАХ

Специальность 05.13.17 – «Теоретические основы информатики»

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата физико-математических наук

Москва 2009

Работа выполнена на кафедре радиотехники Московского Физико-Технического Института (ГУ).

Научный руководитель	доктор технических наук, профессор Габидулин Эрнст Мухамедович
Официальные оппоненты	доктор технических наук, профессор Крук Евгений Аврамович, Санкт-Петербургский государственный университет аэрокосмического приборостроения
	кандидат физико-математических наук Кабатянский Григорий Анатольевич, Институт проблем передачи информации им. ак. А.А.Харкевича
Ведущая организация	Институт математики им. С.Л.Соболева Сибирского отделения Российской академии наук

Защита состоится «24» марта 2009г. в 17:00 на заседании диссертационного совета Д 212.156.04 Московского Физико-Технического Института (ГУ) по адресу: 141700, г. Долгопрудный, Московская обл., Институтский переулок, д. 9, Новый корпус, ауд.204

С диссертацией можно ознакомиться в библиотеке МФТИ (ГУ)

Автореферат разослан « __ » февраля 2009г.

Ученый секретарь
Диссертационного совета Д 212.156.04
Кандидат технических наук, доцент Л.П. Куклев

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Использование линейных кодов для создания систем защиты информации с открытым ключом ведется исследователями в течение многих лет, начиная с первых работ МакЭлиса (1978) и Нидеррайтера (1986).

Классическая система, предложенная Нидеррайтером, отличается высокой скоростью шифрования. Шесть лет спустя после опубликования описания классической системы шифрования, в 1992 году криптографами В.М. Сидельниковым и С.О. Шестаковым была предложена успешная атака на систему Нидеррайтера. Затем было предложено несколько различных модификаций классической криптосистемы Нидеррайтера с целью увеличения ее криптостойкости.

В работе предлагается новая криптосистема, построенная по принципу Нидеррайтера. Одной из особенностей новой криптосистемы является введение дополнительной ошибки в новой метрике. Это позволяет усложнить структуру открытого ключа так, что атаки, аналогичные атаке Сидельникова-Шестакова, оказываются неэффективными.

Системы, обеспечивающие защиту от несанкционированного доступа, часто применяются в каналах с помехами. Предлагаемая новая криптосистема может использоваться в каналах с множественными шумами и осуществлять не только защиту от несанкционированного доступа, но и исправлять ошибки канала. При применении двух различных систем для

защиты от помех и несанкционированного доступа возникает ряд трудоемких задач по согласованию их работы.

Рассматриваемая новая интегрированная система помехо- и криптозащиты может успешно применяться при передаче движущихся изображений. Такое приложение актуально для видеоконференций, систем видеонаблюдения и видеомониторинга.

Целью диссертационной работы является построение и исследование криптосистем, построенных по принципу системы Нидеррайтера с использованием новых метрик и новых кодов для применения в составе интегрированных систем защиты от помех и несанкционированного доступа.

Задачами диссертационного исследования являются:

1. Исследование и криптоанализ существующих модификаций системы Нидеррайтера.
2. Моделирование и исследование новой криптосистемы, построенной по принципу криптосистемы Нидеррайтера.
3. Разработка, реализация и оценка эффективности криптографических атак на предлагаемую новую криптосистему.
4. Моделирование новой криптосистемы в составе экспериментальной интегрированной системы защиты от помех и несанкционированного доступа.
5. Моделирование и исследование новой криптосистемы в составе системы передачи и защиты меняющихся изображений от помех и несанкционированного доступа.

Методы исследования. Для достижения поставленной цели в диссертационной работе используются методы теории информации, дискретной математики, а также имитационного моделирования, линейной алгебры и теории алгебраического кодирования.

Основные положения, выносимые на защиту:

1. Описание и исследование новой метрики и построение кодов в этой метрике.
2. Алгоритмы шифрования и расшифрования новой криптосистемы, построенной по принципу Нидеррайтера.
3. Криптоанализ новой криптосистемы. Выбор параметров криптосистемы.
4. Интегрированная система защиты от множественных помех и несанкционированного доступа.

Научная новизна:

1. Введен класс проективных метрик, позволяющих модернизировать криптосистемы, основанные на линейных кодах.
2. Выбрана новая метрика, используемая при построении криптосистемы с открытым ключом, усиливающая криптостойкость этой системы.
3. Предложена криптосистема с открытым ключом, использующая новую метрику, ассоциированную с матрицей Фробениуса, и ранговые коды.
4. Разработан алгоритм, позволяющий использовать особенности новой криптосистемы для исправления ошибок канала.

5. Получены характеристики интегрированной системы помехо- и криптозащиты применительно к передаче видеоизображений.

Практическая ценность и реализация результатов

Результаты диссертации получены в рамках следующих научно-исследовательских работ:

- проект № 3969 аналитической ведомственной целевой программы «Развитие научного потенциала высшей школы, 2006-2008 годы»,
- контракт №32/07 от 18.05.2007, заключенный с Институтом проблем управления имени ак. А.А. Харкевича во исполнение государственного контракта №02.514.11.4025 от 1 мая 2007 г. на выполнение научно-исследовательских работ между Федеральным агентством по науке и инновациям и Институтом проблем управления имени ак. А.А. Харкевича.

Результаты диссертационной работы используются в учебном процессе на Кафедре радиотехники МФТИ (ГУ) в рамках курса «Защиты Информации».

Апробация результатов работы

Основные результаты диссертации были доложены и обсуждены на следующих конференциях и семинарах.

1. Международная конференция «International Symposium on Communication Theory and Applications» (ISTA)2005, Ambleside, Lake District, UK, July, 2005.

2. Конференция «Математика и безопасность информационных технологий» (МаБИТ-05). МГУ им. М.В.Ломоносова (2005г., Москва).
3. Конференция Российской криптографической ассоциации «РусКрипто'2008» (2008 г., Москва).
4. Научные конференции МФТИ «Современные проблемы фундаментальных и прикладных наук» (в 2004-2008 гг., Долгопрудный).
5. Научные семинары кафедры радиотехники МФТИ (2004-2008 гг., Долгопрудный).

Публикации

По теме диссертации опубликовано 11 работ, две из них в рецензируемых журналах, утвержденных в перечне ВАК. Список публикаций приведен в конце автореферата на страницах 24-26.

Структура и объем диссертационной работы

Диссертация состоит из введения, шести глав, заключения, списка литературы, включающего 45 наименований, и приложения. Работа изложена на 146 страницах и содержит 15 рисунков и 5 таблиц.

СОДЕРЖАНИЕ РАБОТЫ

Во введении поставлена задача, обоснована актуальность работы, научная новизна и практическая ценность результатов, приведено краткое описание структуры диссертации.

В первой главе описаны основные понятия криптографии и необходимые сведения из теории кодирования.

Рассмотрены симметричные и асимметричные криптосистемы, рассмотрены основные подходы к криптоанализу систем и дано определение стойкости криптосистемы. Рассмотрены коды Рида-Соломона и ранговые коды. Основное внимание уделяется алгебраическим методам кодирования и декодирования ранговых кодов.

Подробно рассмотрены способы кодирования и декодирования кодов Рида-Соломона, дано определение рангового кода. Внимание обращено на тип кодов с максимальным ранговым расстоянием. Описаны алгоритмы кодирования и декодирования ранговых кодов. В качестве примеров рассмотрены различные варианты ошибок и их исправление ранговыми кодами.

Во второй главе описаны классические криптосистемы, основанные на линейных кодах. Рассматриваются основные принципы построения такого рода криптосистем. Дано описание криптосистем МакЭлиса и Нидеррайтера.

В системе с открытым ключом МакЭлиса основная идея построения криптосистемы состоит в том, чтобы создать код и замаскировать его под обычный линейный код. Алгоритм МакЭлиса довольно быстр и работает на порядок быстрее стандартной системы RSA, но имеет существенный недостаток – большой размер открытого ключа. Из-за большого размера открытого ключа шифртекст получается вдвое длиннее открытого ключа, это вызывает увеличение размера передаваемого сообщения и затрудняет практическое использование системы.

Криптосистема Нидеррайтера лишена описанных выше недостатков системы МакЭлиса и также основана на обобщенных кодах Рида–Соломона. Секретными ключами в алгоритме Нидеррайтера являются:

- проверочная матрица $H = [z_j x_j^i]$, где $j = 1,\ldots n$, $i = 0,\ldots r-1$ обобщенного кода Рида–Соломона над полем $GF(q)$;
- случайно выбранная невырожденная скремблирующая матрица S порядка r над полем $GF(q)$. Эта матрица вводится для того, чтобы скрыть от криптоаналитика видимые закономерности, разрушая структуру проверочной матрицы.

Открытым ключом является скремблированная проверочная матрица $H_{cr} = SH$.

Сообщениями являются все векторы с координатами из поля $GF(q)$ с весом, не превосходящим $r/2$. Сообщения не являются кодовыми словами выбранного кода Рида–Соломона, а представляют собой всевозможные ошибки, которые этот код в состоянии исправлять.

Шифртекст, соответствующий сообщению $\underline{m}$, представляет собой вектор синдрома и вычисляется следующим образом:

$$\underline{c} = \underline{m} H_{cr}^T = \underline{m} H^T S^T.$$

Авторизованный пользователь после приема шифртекста $\underline{c}$ умножает его справа на матрицу $(S^T)^{-1}$, а затем применяет

известный лишь ему алгоритм быстрого декодирования и получает переданное сообщение.

Подробно рассмотрены алгоритмы криптоанализа криптосистем, основанных на линейных кодах. Криптосистема Нидеррайтера оказалась нестойкой и была взломана Сидельниковым и Шестаковым. Криптоаналитикам удалось подобрать такие матрицы $\tilde{S}$ и $\tilde{H}$, что $H_{cr} = \tilde{S}\tilde{H}$, где $\tilde{H}$ имеет ту же структуру, что и H но, возможно, с другими параметрами.

Далее система будет модифицирована, чтобы противостоять атаке Сидельникова–Шестакова. На основании сравнения криптосистем МакЭлиса и Нидеррайтера делается вывод о том, в каких случаях целесообразнее применять каждый из алгоритмов. Формулируются основные проблемы, возникающие при практическом использовании криптосистем.

Третья глава посвящена проективным метрикам и примерам построения кодов в различных проективных метриках.

В первом параграфе дается определение нормы и расстояния в проективной метрике. Рассмотрены примеры проективных метрик, особое внимание уделено метрике, ассоциированной с матрицей Фробениусовского типа.

Дано определение кода, оптимального в проективной метрике, а также родительского кода. На основании примеров проективных метрик рассмотрены примеры кодов в метриках на основе матрицы Вандермонда и Фробениуса. Приведено

подробное описание алгоритма быстрого декодирования кода в метрике, ассоциированной с матрицей Фробениуса.

Четвертая глава подробно описывает основные подходы к модификации криптосистемы Нидеррайтера.

Основная идея модификаций последних лет заключается в том, чтобы как можно лучше скрыть структуру синдрома. Это делается для того, чтобы избежать структурных атак, подобных атакам Сидельникова–Шестакова. Структура закрытого ключа усложняется так, чтобы синдром родительского кода выступал в роли искусственно созданной ошибки нового кода в новой метрике. В таблице 1 приведены возможные модификации системы Нидеррайтера.

Таблица 1

Возможные варианты модификации криптосистемы Нидеррайтера

№	Код	Метрика	Вид шифртекста	Криптосистема
1	Коды с максимальным ранговым расстоянием	Ранговая метрика	$\underline{m}H_{pub}^{T} = \underline{m}(SH)^{T}$	Рассмотрена авторами Berger T. и Loidreau P. в 2004г.
2	Обобщенные коды Рида–Соломона	На основе матрицы Вандермонда	$H_{pub}\underline{m} = S(F + G^{T}U)P\underline{m}$	Предложена Габидулиным Э.М. и Обернихиным В.А. в 2002г.
3	Модифицированный ранговый код	На основе матрицы Фробениуса	$H_{pub}\underline{m} = S(F + G^{T}U)P\underline{m}$	Предложена Габидулиным Э.М. и Самохиной М.А. в 2005г.

В первой строке таблицы 1 приведена модификация Бергера–Луадро, в которой используются коды с максимальным

ранговым расстоянием. По-видимому, для этой криптосистемы возможна атака типа Сидельникова–Шестакова, хотя в литературе подобные результаты не найдены.

В примерах, приведенных во второй и третьей строке таблицы 1, использована новая идея: шифртекст можно представить в виде суммы векторов $(\underline{g} + \underline{e})$, умноженной на случайно выбранную матрицу S.

Для расшифрования легальному пользователю необходимо сначала найти вектор ошибки, применив алгоритм быстрого декодирования нового кода, который является синдромом родительского кода. Вторым этапом расшифрования является применение алгоритма быстрого декодирования в родительском коде. После применения алгоритма быстрого декодирования в родительском коде легальный пользователь получает открытый текст.

Построение криптосистемы, соответствующей второй строке таблицы 1, с метрикой, основанной на матрице Вандермонда, начинается с выбора матрицы F с элементами из расширенного поля. Матрица F является проверочной для родительского кода, который должен быть построен так, чтобы иметь алгоритм быстрого декодирования в родительской метрике. Следующим шагом является выбор порождающей матрицы G некоторого линейного кода, который должен иметь быстрый алгоритм декодирования в новой метрике.

До осуществления самого шифрования, необходимо выбрать секретный ключ, состоящий из набора матриц

$\{F, G^T, S, P\}$ и матрицы U. Затем вычисляется открытый ключ: $H_{pub} = S(F + G^T U)P$.

При шифровании открытый текст $\underline{m}$ умножается на матрицу-открытый ключ: $\underline{c} = \underline{m}H_{pub}^T$. После получения шифртекста легальный пользователь выполняет умножение $\underline{c}$ на матрицу $(S^T)^{-1}$, получая в результате вектор, который можно представить в виде суммы: $(\underline{g} + \underline{e})$. Далее применяется алгоритм быстрого декодирования в метрике Вандермонда, который выдает в результате **сразу же** вектор $\underline{\tilde{m}}$. Чтобы получить открытый текст, нужно вычислить $\underline{\tilde{m}}(P^T)^{-1}$.

Модификация в третьей строке таблицы 1 является основным результатом диссертации и описана в пятой главе. Кроме того в диссертационной работе проанализированы другие ранее предложенные криптосистемы, построенные на линейных кодах, а также рассмотрены возможные криптоатаки на эти системы. Результатом проведенного анализа является вывод о том, что в ранее предложенных модификациях криптосистемы Нидеррайтера для зашумления используются матрицы ранга 1, что делает такие системы потенциально уязвимыми.

В пятой главе построена новая криптосистема на основе метрики, ассоциированной с матрицей Фробениуса.

В качестве матрицы F размера $N_1 \times n$ с элементами из поля $GF(q^N)$, $N > n$ выбирается матрица Фробениуса:

$$F = \begin{pmatrix} h_1 & h_1^q & \dots & h_1^{q^{n-1}} \\ h_2 & h_2^q & \dots & h_2^{q^{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ h_{N_1} & h_{N_1}^q & \dots & h_{N_1}^{q^{n-1}} \end{pmatrix},$$

где каждый элемент матрицы выбирается из поля $GF(q^N)$. Элементы $h_1, h_2, \dots, h_{N_1}$ выбираются линейно независимыми над базовым полем. Далее для построения кода используется матрица G_k, имеющая такой же вид, как и матрица F:

$$G_k = \begin{pmatrix} g_1 & g_1^q & \dots & g_1^{q^{n-1}} \\ g_2 & g_2^q & \dots & g_2^{q^{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ g_K & g_K^q & \dots & g_K^{q^{n-1}} \end{pmatrix}.$$

Далее используется конкатенация матриц F и G_k:

$$Q = \left(\frac{F}{G_k} \right),$$

где $N = N_1 + K$, h_i, g_j – элементы поля $GF(q^N)$, линейно независимые в совокупности над базовым полем. Верхняя часть матрицы Q с элементами $h_j^{q^i}$ используется для определения метрики, а нижняя часть с элементами $g_j^{q^i}$ используется как порождающая матрица кода.

Открытый ключ имеет вид: $H_{pub} = S(F + G^T U)P$. При шифровании открытый текст $\underline{m}$ умножается на матрицу-открытый ключ: $\underline{c} = \underline{m} H_{pub}^T$.

При расшифровании легальный пользователь умножает полученный шифртекст $(\underline{g}+\underline{e})S^T$ на $(S^T)^{-1}$. Затем применяется алгоритм быстрого декодирования в новой метрике. В результате пользователь получит векторы $\underline{g}$ и $\underline{e}$. После применения алгоритма быстрого декодирования родительского кода легальный пользователь получит вектор $\underline{\tilde{m}}$. При последующем умножении вектора $\underline{\tilde{m}}$ на матрицу $(P^T)^{-1}$ легальный пользователь получает открытый текст $\underline{m}$.

Далее в работе проводится описание атаки на предлагаемую новую криптосистему. К рассмотренной криптосистеме применимы два основных вида атак: прямые и структурные атаки. Структурные атаки – это различные модификации атаки Гибсона, адаптированные к модификациям криптосистемы, и варианты атаки Сидельникова–Шестакова. При оценке трудоемкости каждой из атак, необходимо учитывать размер открытого ключа.

Проведенный криптоанализ показал, что для самого успешного структурного алгоритма атаки вычислительная сложность имеет порядок 2^{140} при размере открытого ключа 1024 байт. На сегодняшний день такая вычислительная сложность атаки является более чем достаточной, чтобы считать, что криптосистема является стойкой. Таким образом, можно заключить, что построена новая криптостойкая система.

Шестая глава посвящена применению криптосистемы на основе метрики, ассоциированной с матрицей Фробениуса в системах передачи и защиты от несанкционированного доступа. Приводится описание системы одновременной помехозащиты и защиты от несанкционированного доступа. Рассматривается работа новой криптосистемы в системе защиты информации при передаче видеоизображений.

Для исправления ошибок канала нужно наложить дополнительные ограничения на выбор матриц в модуле инициализации. Необходимо собрать статистику и, предварительно проанализировав ее, определить характер ошибок и осуществить модификацию криптосистемы с целью исправления ошибок. В базовом поле шифртекст представляет собой матрицу с элементами из поля $GF(q)$:

$$C = \begin{pmatrix} c_{11} & \dots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{N1} & \dots & c_{Nn} \end{pmatrix}.$$

Элементы матрицы C имеют вид:

$$c_{ij} = [s_{ij}(g_1 u_{1i} + \dots + g_k u_{ki} + h_i) + \dots + s_{jj}(g_1^{q^{j-1}} u_{1i} + \dots + h_i^{q^{j-1}})]m_j$$

На этапе расшифрования приемник получает шифртекст, искаженный ошибкой, в виде $(\underline{g} + \underline{e} + \underline{\tilde{e}})$. Для того чтобы гарантировать коррекцию ошибок канала, необходимо наложить дополнительные ограничения на выбор матрицы Q. Код с порождающей матрицей G_k должен исправлять большее

количество ошибок. Дополнительные ограничения увеличивают размер ключей криптосистемы, что незначительно влияет на скорость шифрования и расшифрования. В таблице 2 ε обозначает количество векторов, имеющих ранг равный 1 над базовым полем; η – количество векторов, имеющих ранг равный 2; ξ – количество векторов в матрице, задающей метрику.

Пусть в представлении ошибки $\underline{\tilde{e}} = \sum_i \varsigma \underline{f_i}$ минимальное количество ненулевых коэффициентов ς равно τ. Тогда для того, чтобы гарантировать исправление ошибки при декодировании, необходимо чтобы $t = 1/2(d - 2\tau - 1)$, где t – норма $\underline{e}$.

Таблица 2

Исправление ошибок канала

Ранг $\underline{\tilde{e}}$	**Норма** $\underline{\tilde{e}}$	**Количество матриц**	**Комментарий**
1	1	$\xi \times \varepsilon$	Ранг над базовым полем одного из векторов равен 1
1	2	$\xi \times (\xi - 1) \times q^2 \times \varepsilon$	Ранг линейной комбинации любой из пары векторов равен 1
2	1	$\xi \times \eta$	Ранг полем одного из векторов равен 2
2	2	$\xi \times (\xi - 1) \times q^2 \times \eta$	Ранг линейной комбинации любой из пары векторов равен 2

Новая модификация криптосистемы Нидеррайтера использована в работе над контрактом №32/07 от 18.05.2007

"Разработка и исследование сигнально-кодовых конструкций для передачи и защиты меняющихся изображений". В работе показано, что криптосистема может успешно применяться как часть системы с открытым ключом для передачи и защиты меняющихся изображений. На рисунке 1 приведена зависимость скорости шифрования от размера ключа криптосистемы для модифицированной системы Нидеррайтера, основанной на матрице Фробениуса, и криптосистемы RSA для не шумящего канала. Скорость шифрования новой криптосистемы оказывается больше скорости шифрования криптосистемы RSA.

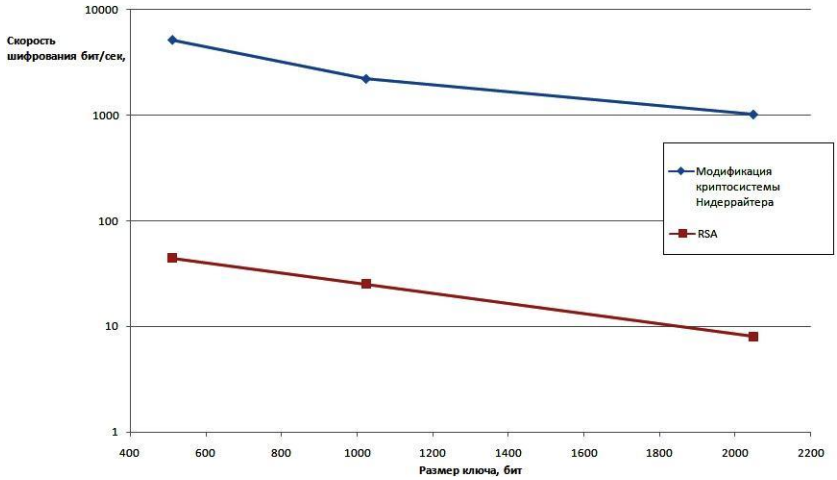

Рис. 1.Зависимость скорости шифрования от размера ключа криптосистемы

На графике рис.1 красная линия соответствует значениям поддерживаемой частоты смены изображений для криптосистемы RSA при размере ключа 512 бит в бесшумном

канале. Значение поддерживаемой частоты для RSA в 2 раза ниже, чем аналогичное значение у разработанной новой криптосистемы. Такое сравнение не совсем корректно для шумящего канала, так как для использования RSA в шумящем канале необходимо производить кодирование с вероятностью ошибки в бите не более 10^{-8}. Кодирование с такой вероятностью ошибки невозможно реализовать практически. В результате, кроме превосходства по скоростям, новая криптосистема не требует дополнительных затрат как со стороны разработки программного комплекса, так и в плане увеличения вычислительных мощностей используемого аппаратного комплекса.

Одной из главных характеристик криптосистем является их стойкость. Стойкость криптосистемы характеризуется количеством простых битовых операций, требуемых для реализации самой эффективной криптоатаки на систему.

Новая криптосистема может поддерживать различную частоту смены видеокадров, поддерживаемая частота зависит от выбранных параметров системы. Также в зависимости от выбранных параметров находится и стойкость рассматриваемой криптосистемы. На рисунке 2 приведен график зависимости стойкости новой криптосистемы от поддерживаемой частоты смены кадров в бесшумном канале при размере кадров, соответствующих сотовому телефону SonyEricsson W900. Размер кадра при использовании современных методов сжатия составляет в среднем 12 килобит.

Из графика, приведенного на рисунке 2, видно, что для стандартной частоты 25 кадров в секунду стойкость криптосистемы остается настолько высокой, что потери стойкости для исправления ошибок канала несущественны.

В работе получены результаты для различных размеров кадров и частот смены видеоизображений, соответствующих стандартам. На рисунке 3 приведены зависимости поддерживаемой частоты смены кадров от размера ключа при различных размерах кадров при использовании разработанной новой криптосистемы. По оси ординат отложена максимально возможная поддерживаемая частота смены изображений в fps (количество кадров за секунду), а по оси абсцисс соответствующий размер ключа в битах.

В случае передачи видео изображения повышенного качества HDTV (High-Definition Television) — телевидения высокой чёткости, частота смены изображений поддерживаемой системой сокращается в 20 раз.

Наиболее часто используемый на сегодняшний день формат – это видео стандартной четкости SD с частотой смены изображений, равной 25 кадров в секунду. Из графика на рисунке 3 видно, что такая поддерживаемая частота соответствует ключу размером в 384 бита.

Скорость шифрования в системе можно увеличить, осуществляя шифрование изображения с помощью более производительных симметричных алгоритмов, а шифрование

сеансового ключа осуществлять уже при помощи новой системы. Эта модификация может быть применена только для канала без шума. Например, можно использовать в качестве симметричного алгоритма AES или российского ГОСТ28147-89. При применении одного из симметричных алгоритмов для шифрования передаваемого сообщения и шифровании сеансового ключа новой разработанной криптосистемой с открытым ключом можно гарантировать передачу изображения в формате стандарта телевидения высокой чёткости.

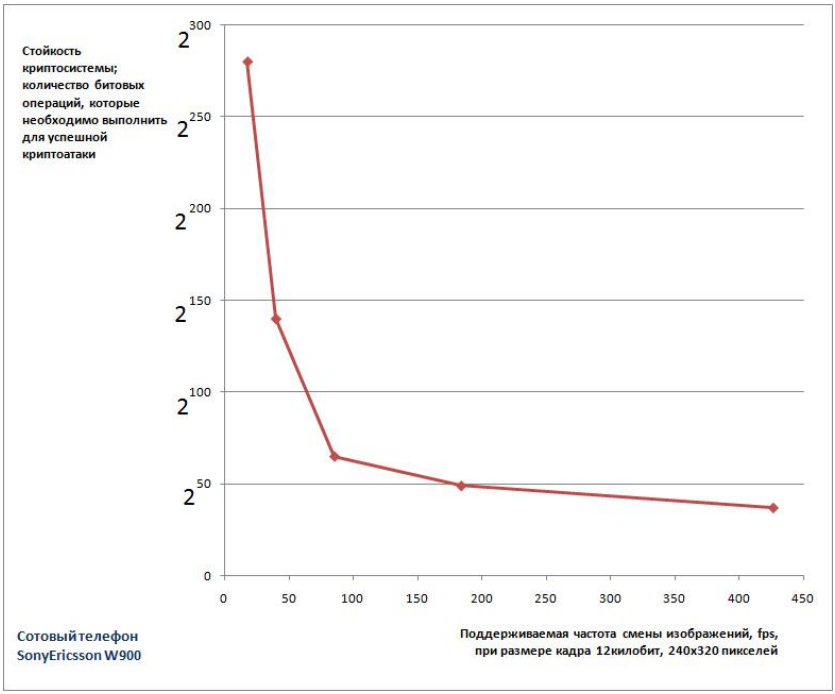

Рис. 2. Зависимость стойкости от поддерживаемой частоты смены кадров

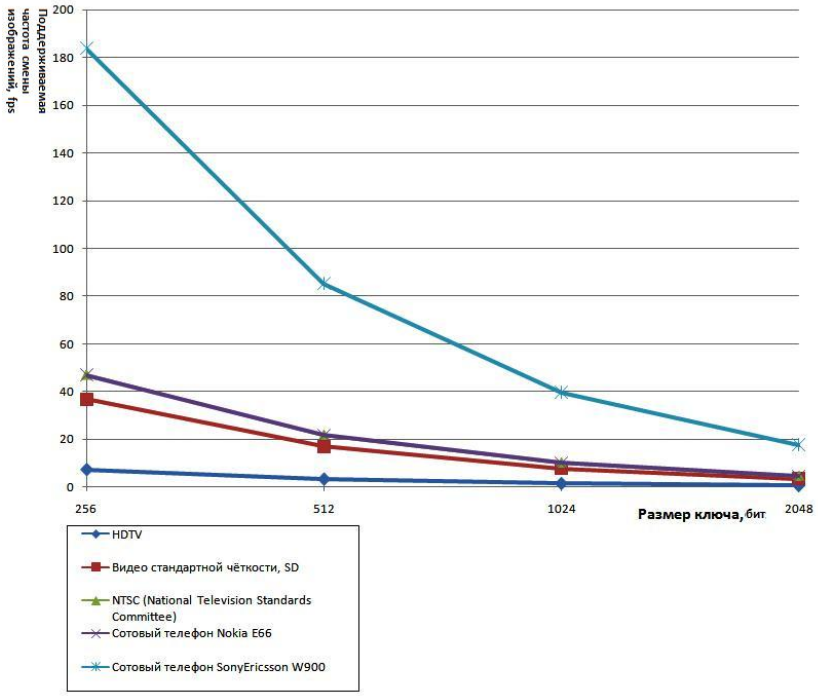

Рис. 3. Зависимость частоты смены кадров от размера ключа

На рисунке 4 приведена зависимость поддерживаемой частоты смены кадров от размера кадров при использовании симметричного алгоритма AES256 и новой модификации криптосистемы Нидеррайтера. Размер сеансового ключа составляет 256 бит, размер открытого ключа системы – 512 бит.

На графике светло-зеленая линия соответствует стандартной реализации AES без ускорений, а темно-зеленая линия соответствует теоретически максимально быстрой реализации AES. Из графика, приведенного на рисунке 4, видно, что при стандартной реализации AES без ускорений поддерживаемая

частота смены изображений возрастает в десять раз по сравнению с реализацией без применения симметричного алгоритма.

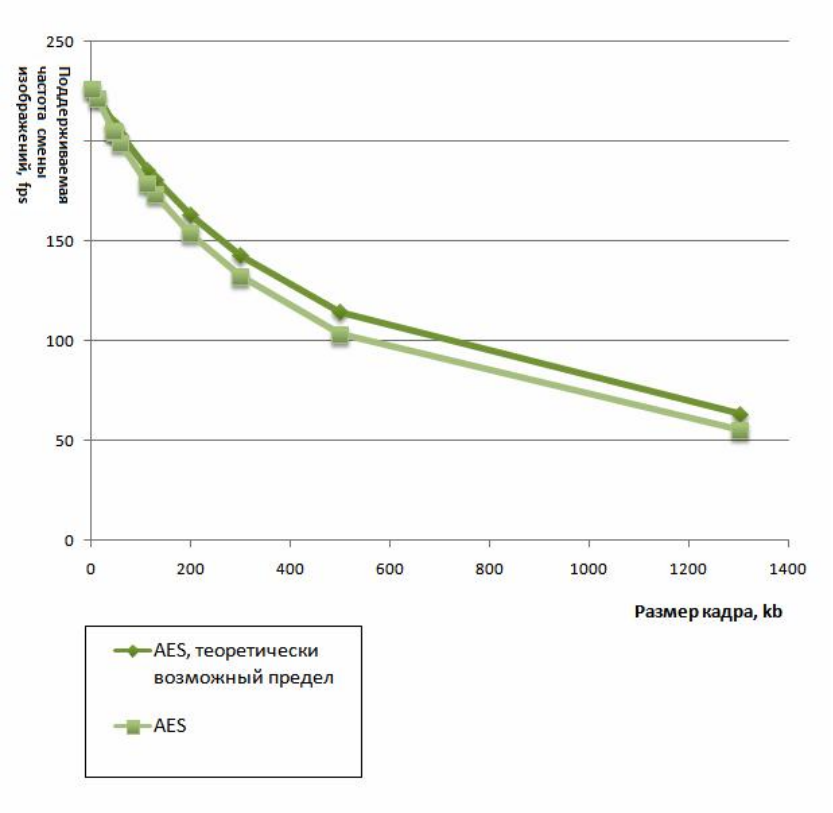

Рис. 4. Зависимость частоты смены кадров от размера кадра

ОСНОВНЫЕ РЕЗУЛЬТАТЫ И ВЫВОДЫ

1. Предложена новая криптосистема, использующая принцип Нидеррайтера и новую метрику, ассоциированную с матрицей Фробениуса. Новая криптосистема обеспечи-

вает высокую скорость шифрования при высокой стойкости системы.

2. Моделирование новой криптосистемы показало, что она может применяться для успешного одновременного помехоустойчивого кодирования и защиты от несанкционированного доступа.
3. На основе предложенных алгоритмов создан комплекс математических методов, позволяющих успешно исправлять ошибки канала при одновременном шифровании и расшифровании передаваемой информации.
4. Предложенные алгоритмы апробированы в системе передачи и защиты видеоизображений. Моделирование показало высокую скорость шифрования и надежность.

СПИСОК РАБОТ, ОПУБЛИКОВАННЫХ ПО ТЕМЕ ДИССЕРТАЦИИ

1. Чурусова (Самохина) М.А., Новая метрика для криптосистем с открытым ключом, основанных на линейных кодах // Современные проблемы фундаментальных и прикладных наук: Труды XLVII научной конференции МФТИ, Часть I, Радиотехника и Кибернетика – Москва – Долгопрудный, 2004. – Стр. 18−19.
2. Чурусова (Самохина) М.А., Габидулин Э.М., Модификация криптосистемы Нидеррайтера, основанная на новой метрике. // Научный вестник Московского государ-

ственного института радиотехники, электроники и автоматики. - Москва, Январь, 2005. - Стр. 27-29.

3. M.A. Churusova., E.M.Gabidulin. The modified Niederreiter cryptosystem based on new metric. Proceedings of ISCTA2005, Ambleside, Lake District, UK, July, 2005.
4. Чурусова (Самохина) М.А., Ассоциированные метрики и их применение для модификации криптосистем // Современные проблемы фундаментальных и прикладных наук: Труды 49-й научной конференции МФТИ, Часть I, Радиотехника и Кибернетика – Москва–Долгопрудный, 2005. – Стр. 13-16.
5. Чурусова (Самохина) М.А., Габидулин Э.М., Ассоциированные метрики и их применение для модификации криптосистемы Нидеррайтера // Материалы конференции "Математика и безопасность информациионных технологий" (МаБИТ-05). МГУ им. М.В.Ломоносова, ноябрь 2005г. – М.: МЦНМО, 2005.
6. Чурусова (Самохина) М.А., Криптоанализ и модификация системы Нидеррайтера // Современные проблемы фундаментальных и прикладных наук: Труды XLIX научной конференции МФТИ, Факультет Радиотехника и Кибернетика, Радиотехника и Кибернетика – Москва – Долгопрудный, 24-25 ноября 2006 года. – Стр. 4-5.
7. Самохина М.А., Анализ модификаций криптосистемы Нидеррайтера.//Современные проблемы фундаменталь-

ных и прикладных наук: Труды 50-й научной конференции МФТИ, Часть I, Радиотехника и Кибернетика – Москва – Долгопрудный, 2007. – Стр. 25-26.

8. Самохина М.А., Применение модификаций криптосистем Нидеррайтера в системах исправления ошибок и защиты от несанкционированного доступа. // Моделирование и обработка информации. Сборник научных трудов - Москва 2008. – Стр.127-136.
9. Самохина М.А., Криптоанализ систем, основанных на линейных кодах. // Проблемы информационной безопасности. Компьютерные системы, №2, 2008 г. - Санкт-Петербург, 2008. – Стр. 94-103.
10. Самохина М.А., Использование модифицированной криптосистемы Нидеррайтера при передаче и для защиты меняющихся изображений. // Современные проблемы фундаментальных и прикладных наук: Труды 51-й научной конференции МФТИ, Часть I, Радиотехника и Кибернетика – Москва - Долгопрудный, 2008.- Стр. 11-14.
11. Самохина М.А., Применение модификации криптосистемы Ниддерайтера для защиты информации при передаче видеоизображений. // Информационно-управляющие системы, №1, 2009 г. - Санкт-Петербург, 2009.