На правах рукописи

Кшевецкий Александр Сергеевич

Разработка новых кодов в ранговой метрике и криптосистем с открытым ключом

Специальность 05.13.17 - Теоретические основы информатики

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата физико-математических наук

Москва – 2007

Работа выполнена в Московском физико-техническом институте (государственном университете)

Научный руководитель:	доктор технических наук, проф. Габидулин Эрнст Мухамедович
Официальные оппоненты:	доктор физико-математических наук, Зиновьев Виктор Александрович,
	кандидат физико-математических наук Соловьева Фаина Ивановна
Ведущая организация:	Санкт-Петербургский государственный университет аэрокосмического приборостроения

Защита состоится «_____» _____ 2007 г. в _____ часов на заседании диссертационного совета Д.002.077.01 при Институте проблем передачи информации РАН по адресу: 127994, Москва, ГСП-4, Большой Каретный переулок, дом 19.

С диссертацией можно ознакомиться в библиотеке Института проблем передачи информации РАН.

Автореферат разослан «_____» _____ 2007 г.

Ученый секретарь диссертационного совета Д.002.077.01
доктор физико-математических наук

И. И. Цитович

Общая характеристика работы

Актуальность темы исследования

При передаче информации по каналам связи можно выделить две фундаментальные проблемы – защиту передаваемой информации от шумов и защиту информации от несанкционированного доступа. Исторически сложилось, что данные проблемы решаются независимо. Вначале информация защищается от несанкционированного доступа, затем используется защита от шумов.

Защита от шумов обеспечивается помехоустойчивым избыточным кодированием. Наиболее распространены помехоустойчивые алгебраические коды, построенные в метрике Хэмминга, например, коды Рида-Соломона. Одни и те же шумы в кодах с разными метриками могут иметь разный вес. Особый интерес представляют метрики, в которых часть физических шумов имеет низкий вес.

Матричные коды в ранговой метрике при передаче сигнала одновременно по нескольким частотам хорошо подходят для исправления ошибок, вызванными импульсными широкополосными или постоянными узкополосными шумами. Ошибки, обусловленные такими шумами, имеют более низкий вес в ранговой метрике, чем в метрике Хэмминга. Ранговые коды[1] были предложены в 1985 г. Расширение классов кодов и создание новых кодов является важной задачей теорией кодирования. Новые коды могут обладать лучшей корректирующей способностью и быть более эффективными в частных применениях. Важной задачей теории ранговых кодов является расширение класса ранговых кодов, исследование их свойств и построение новых алгоритмов декодирования. При наличии в канале сильных шумов становятся актуальными методы декодирования за пределами корректирующей способности кода.

Теоретическими аспектами защиты информации от несанкционированного доступа занимается криптография.

Особый интерес представляют криптосистемы с открытым ключом, построенные на линейных кодах и основанные на трудности решения задачи декодирования сообщения с добавленны-

[1]Габидулин Э. М. Теория кодов с максимальным ранговым расстоянием // Проблемы передачи информации. 1985, т. 21, N 1, с. 3-14

ми искусственными ошибками и при неизвестных порождающей/проверочной матриц кода. Вместе с искусственно добавленными ошибками они могут исправлять и обычные ошибки, возникающие при передаче информации. Открытый ключ может быть построен либо на порождающей матрице (криптосистема типа МакЭлиса), либо на проверочной матрице (криптосистема типа Нидеррайтера). В 1991 году была опубликована криптосистема с открытым ключом, основанная на ранговых кодах[2]. Она получила название ГПТ по фамилиям авторов в русскоязычной литературе и GPT в англоязычной. По сравнению с другими криптосистемами, основанными на линейных кодах, ее преимуществом является маленькая длина открытого ключа и, как следствие, высокая скорость шифрования/расшифрования из-за быстрого алгоритма декодирования. Важной задачей является построение единых методов совместных помехоустойчивого кодирования и защиты от несанкционированного доступа. Проблема является особенно актуальной для мобильных устройств связи, в которых уменьшение числа вычислительных модулей означает большее энергосбережение.

В практических приложениях число выполняемых шифрований данных существенно меньше числа выполняемых расшифрований. Интерес представляют криптосистемы, имеющие быстрое расшифрование. Криптосистема NICE-X[3] в отличие от стандартных криптосистем типа RSA, Эль-Гамаля с кубическим временем расшифрования по битовой длине параметров характеризуется квадратичным временем расшифрования. Криптосистема построена в мнимом квадратичном поле. Актуальной задачей является построение и анализ криптосистем с открытым ключом, обладающих высокой скоростью шифрования/расшифрования с тем, чтобы использовать криптосистемы с открытым ключом для шифрования большого объема данных.

Целью настоящего исследования является: 1) построение новых ранговых кодов и новых алгоритмов декодирования, 2) построение и анализ нетрадиционных криптосистем с открытым ключом: а) на

[2]E. M. Gabidulin, A. V. Paramonov, O. V. Tretjakov. Ideals over a non-commutative ring and their application in cryptology // Advances in Cryptology – EuroCrypt'91, LNCS 547, D. W. Davies, Ed., Springer-Verlag, 1991, pp. 482–489.

[3]Paulus S., Takagi T. A new public-key cryptosystem over a quadratic order with quadratic decryption time // Journal of Cryptography. 2000, vol. 13, no2, pp. 263-272.

основе кодов в ранговой метрике из-за возможности обеспечивать одновременную защиту от помех и несанкционированного доступа при передаче данных, б) в мнимом квадратичном поле из-за быстрой операции расшифрования.

В соответствии с поставленной целью в диссертации были определены следующие задачи.
1) Расширение класса кодов в ранговой метрике и построение новых алгоритмов декодирования.
2) Проведение криптоанализа криптосистем с открытым ключом, основанных на ранговых кодах, и построение криптосистем с улучшенными характеристиками.
3) Криптоанализ и анализ эффективности криптосистем с открытым ключом, построенных в мнимом квадратичном поле, имеющих быстрое расшифрование.

Методы исследования. Для решения поставленных задач в работе использованы методы дискретной математики, алгебры, теории информации, теории вероятностей, линейной алгебры, комбинаторики.

Научная новизна результатов, полученных в диссертации, заключается в том, что в ней впервые:

1. Для построения ранговых кодов в качестве порождающей матрицы выбрана $(k \times n)$ матрица Фробениуса над конечным полем $GF(q^N)$ вида $\|g_j^{q^{im}}\|_{i=0..k-1}^{j=1..n}$, $g_j \in GF(q^N)$ с константой $m, \gcd(m, N) = 1$. Обычная матрица Фробениуса определяется как $\|g_j^{q^i}\|_{i=0..k-1}^{j=1..n}$. Использование матрицы нового вида как порождающей матрицы линейного рангового (n, k, d)-кода позволило обобщить и расширить единственную известную конструкцию ранговых кодов 1985 г. с максимальным ранговым расстоянием.

2. Сделано предположение, что степени $(n \times n)$-матриц над полем $GF(2)$, порождающих поле $GF(2^n)$, имеют равномерное распределение элементов над полем $GF(2)$. На основе гипотезы построен метод исправления ошибок стирания веса n для линейных ранговых $(n, 1, n)$-кодов алгоритмом декодирования по информационным совокупностям. Проведенное моделирование подтвердило гипотезу и показало эффективность алгоритма де-

кодирования.

3. Показана эквивалентность разных вариантов криптосистемы ГПТ на основе ранговых кодов одной общей форме открытого ключа. Проведенный криптоанализ общей формы криптосистемы, а не исходных вариантов, позволил найти условия существования и зависимость полиномиальных и экспоненциальных атак относительно параметров криптосистемы.

4. Предложен метод выбора столбцевого скремблера специального вида для криптосистемы на приводимых ранговых кодах. Что позволило создать криптосистему на линейных кодах с искусственной ошибкой веса большего, чем корректирующая способность кода. Одновременно криптосистема может исправлять ошибки, возникающие при передаче по каналу с шумами.

5. Разработан метод быстрого генерирования псевдослучайного целого примитивного идеала мнимого квадратичного поля. Использование метода в алгоритме шифрования криптосистемы NICE-X позволило снизить асимптотическую битовую сложность шифрования с четвертой степени до кубической по битовой длине параметров.

Теоретическая и практическая ценность.

Для коррекции ошибок в каналах с многолучевым распространением используются матричные коды. Матричные коды, построенные в ранговой метрике, успешно исправляют ошибки, вызванные импульсными шумами и эффектом замирания. С 1985 г. была известна только одна конструкция ранговых кодов с максимальным ранговым расстоянием и быстрым алгоритмом декодирования. Предложенные новые ранговые MPP коды расширяют класс известных MPP кодов с быстрым алгоритмом декодирования. Использование новых MPP кодов немного повышает стойкость криптосистем на ранговых кодах с открытым ключом. Декодирование по информационным совокупностям для ранговых кодов представляет интерес для исправления ошибок за пределами корректирующей способности кода.

Криптосистемы с открытым ключом составляют основу защищенных транзакций в сети посредством электронной цифровой подписи (ЭЦП), алгоритмов аутентификации и распределения ключей.

В работе исследованы нетрадиционные криптосистемы с открытым ключом, так как они имеют важные в практическом применении специальные свойства. Одновременное шифрование и исправление ошибок криптосистемами на ранговых кодах уменьшает вычислительные ресурсы, число требуемых вычислительных модулей и экономит потребляемую энергию при беспроводной передаче данных. Быстрое расшифрование криптосистемы в мнимом квадратичном поле имеет значение, так как обычно расшифрование данных выполняется большее число раз, чем шифрование. Быстрое расшифрование экономит вычислительные ресурсы.

Научные положения, выносимые на защиту.

1. Линейные ранговые $(n, k, d = n-k+1)$ коды новой конструкции с максимальным ранговым расстоянием.

2. Декодирование ранговых кодов для плохого канала с мощными узкополосными и импульсными широкополосными шумами по методу информационных совокупностей.

3. Условия существования и оценка сложности полиномиальных и экспоненциальных атак на разные варианты криптосистемы ГПТ на основе ранговых кодов в зависимости от параметров криптосистемы.

4. Криптосистема на основе ранговых кодов с искусственной ошибкой высокого веса и наименьшей длиной открытого ключа.

5. Ускорение шифрования криптосистемы с открытым ключом NICE-X, построенной в мнимом квадратичном поле, и выбор более безопасных параметров схемы.

Апробация работы

Результаты диссертационной работы докладывались на российских и международных конференциях: 1) International Symposium on Information Theory, ISIT, Adelaide, Australia, 2005, 2) International Symposium on Coding Theory and Applications, ISCTA, Ambleside, UK, 2005, 3) Algebraic and Combinatorial Coding Theory, ACCT, Kranevo, Bulguria, 2004, 4) International Symposium on Coding Theory and Applications, ISCTA, Ambleside, UK, 2003, 5) Algebraic and Combinatorial Coding Theory, ACCT, Tsarskoe Selo, Russia, 2002,

6) XLIX, XLVIII, XLVII, XLVI, XLIV ежегодных научных конференциях Московского физико-технического института, Москва-Долгопрудный, 2001-2006.

Основные результаты диссертации неоднократно обсуждались и были одобрены на научных семинарах: 1) School of Information Science and Technology, Southwest Jiatong University, Китай, 2006 г., 2) по теории кодирования Института Проблем Передачи Информации РАН, 2005 г., 3) кафедры радиотехники Московского физико-технического института (ГУ) 2002-2007 гг., 4) Department of Information Technology, Lund University, Швеция, 2002 г.

Публикации. По теме диссертации опубликовано 12 работ, из них 1 статья в журнале из списка ВАК, 1 статья в рецензируемом сборнике научных статей МФТИ, 5 статей в сборниках трудов рецензируемых международных научных конференций, 5 докладов в Трудах научных конференций МФТИ.

Структура и объем диссертации. Диссертация состоит из введения, 3 глав, заключения и списка литературы из 65 наименований. Объем диссертации составляет 128 стр.

Содержание работы

Во введении обоснована актуальность темы, сформулирована цель и определены задачи исследования, дано краткое изложение полученных результатов и содержание диссертации.

Первая глава содержит описание известных и построенных в диссертации конструкций ранговых кодов и алгоритмов кодирования и декодирования.

В первом разделе главы описаны известные конструкции ранговых кодов.

Пусть $GF(q)$ обозначает базовое конечное поле Галуа, $GF(q^N)$ – расширение поля степени N.

Ранговой нормой вектора $(a_1, \ldots, a_n), a_i \in GF(q^N)$, называется максимальное число линейно независимых координат a_i над основным полем $GF(q)$. Ранговое расстояние между двумя векторами определяется как ранговая норма разности двух векторов. Ранговое расстояние линейного кода над полем $GF(q^N)$ определяется как

минимальное ранговое расстояние между кодовыми словами.

Пусть $\mathbf{H}$ – проверочная $((n-k)\times n)$-матрица, а $\mathbf{G}$ – порождающая $(k\times n)$-матрица с элементами из $GF(q^N)$ линейного (n,k)-кода $\mathcal{C}$ над полем $GF(q^N)$, $\quad n\le N$. Для любого линейного (n,k,d)-кода расстояние d удовлетворяет $d\le n-k+1$. Ранговые коды, для которых достигается граница Синглтона $d=n-k+1$, называются кодами с максимальным ранговым расстоянием, MPP кодами.

Для поля $GF(q^N)$ введем символ $[i]=q^{i \mod N}$, $\quad \alpha^{[i]}=\alpha^{q^{i \mod N}}$.

Пусть $h_i\in GF(q^N),\ i=1,\dots,n$ – линейно независимы над $GF(q)$. Тогда

$$\mathbf{H}=\left\|\begin{array}{cccc} h_1 & h_2 & \dots & h_n \\ h_1^{[1]} & h_2^{[1]} & \dots & h_n^{[1]} \\ \dots & \dots & \dots & \dots \\ h_1^{[d-2]} & h_2^{[d-2]} & \dots & h_n^{[d-2]} \end{array}\right\| = \left\|h_j^{[i]}\right\|_{j=1..n}^{i=0..d-2} \tag{1}$$

проверочная матрица рангового MPP кода $\mathcal{C}$ с расстоянием $d\le n$.

Порождающей матрицей $\mathbf{G}$ для рангового MPP кода $\mathcal{C}$ с расстоянием $d\le n$ является матрица

$$\mathbf{G}=\left\|g_j^{[i]}\right\|_{j=1..n}^{i=0..k-1},\ \mathbf{G}\mathbf{H}^T=0, \tag{2}$$

$g_i\in GF(q^N),\ i=1,\dots,n$, линейно независимы над $GF(q)$.

Пусть $\mathbf{m}$ – информационные символы. Кодовое слово – $\mathbf{g}=\mathbf{m}\mathbf{G}$. Быстрое декодирование принятого слова $\mathbf{y}=\mathbf{g}+\mathbf{e}$, искаженного ошибкой $\mathbf{e}$, выполняется алгоритмом деления Евклида для линеаризованных многочленов.

Криптосистемы с открытым ключом на ранговых кодах, которые имеют наименьшую длину открытого ключа, основаны на приводимых ранговых кодах.

Пусть $\mathbf{G}_{11},\mathbf{G}_{22},\dots,\mathbf{G}_{pp}$ – порождающие матрицы (n_i,k_i)-кодов в ранговой метрике над полем $GF(q^N),\ i=1,\dots,p$. Матрицы $\mathbf{G}_{ii}$ – порождающие матрицы ранговых кодов. Порождающая матрица для приводимого рангового кода $\mathcal{C}_p$:

$$\mathbf{G}_p=\left\|\begin{array}{ccccc} \mathbf{G}_{11} & \mathbf{0} & \dots & \mathbf{0} & \mathbf{0} \\ \mathbf{G}_{21} & \mathbf{G}_{22} & \dots & \mathbf{0} & \mathbf{0} \\ \dots & \dots & \dots & \dots & \dots \\ \mathbf{G}_{p-1,1} & \mathbf{G}_{p-1,2} & \dots & \mathbf{G}_{p-1,p-1} & \mathbf{0} \\ \mathbf{G}_{p,1} & \mathbf{G}_{p,2} & \dots & \mathbf{G}_{p,p-1} & \mathbf{G}_{pp} \end{array}\right\| \tag{3}$$

для некоторых $(k_i \times n_i)$-матриц $\mathbf{G}_{ij},\ i = 2, \ldots, p,\ j = 1, \ldots, p-1$ над $GF(q^N)$.

Длина кода $\mathcal{C}_p$ – $n = \sum_{i=1}^{p} n_i$, размерность – $k = \sum_{i=1}^{p} k_i$, расстояние – $D = \min(d_1, \ldots, d_p)$, где d_i – расстояния кодов, определенных матрицами $\mathbf{G}_{ii}$.

Пусть $\mathbf{m} = (\mathbf{m}_1, \ldots, \mathbf{m}_p)$ является информационной последовательностью. Кодовое слово – $\mathbf{g} = \mathbf{mG}$. Быстрое декодирование принятого слова $\mathbf{y} = \mathbf{g} + \mathbf{e}$, искаженного ошибкой $\mathbf{e}$, осуществляется блоками. Вначале декодируется последний блок сообщения $\mathbf{m}_p$ из $\mathbf{y}_p$ быстрым алгоритмом декодирования кода, заданного $\mathbf{G}_{pp}$, затем $\mathbf{m}_{p-1}$ из $\mathbf{y}_{p-1}$ с учетом найденного $\mathbf{m}_p$ и т.д.

Матричные ранговые $(n, 1, n)$-коды могут использоваться в условиях мощных импульсных широкополосных и постоянных узкополосных шумов. Матричный код можно построить следующим образом.

Пусть порождающая матрица для кода – вектор $\mathbf{g} = (g_1, g_2, \cdots, g_n) = (\alpha^{u_1}, \alpha^{u_2}, \ldots, \alpha^{u_n})$, где α – примитивный элемент поля $GF(2^n)$. Матрица $\mathbf{A}$ на полем $GF(2)$, представляющая поле $GF(2^n)$, находится из условия $\alpha\mathbf{g} = \mathbf{gA}$. Тогда кодовое слово в матричном виде выражается как $V = \sum_{i=1}^{n} x_i \mathbf{A}^{u_i}$.

Если матрица $\mathbf{A}$ – симметричная матрица, то кодовая матрица также симметричная. Такие ранговые коды называются симметричными.

Во втором разделе главы описана конструкция нового класса ранговых кодов, быстрые алгоритмы кодирования и декодирования.

Рассмотрим матрицу

$$\mathbf{H}_m = \left\| h_j^{[im]} \right\|_{j=1..n}^{i=0..d-2} \tag{4}$$

для некоторого целого m с элементами $h_i \in GF(q^N), n \leq N$, линейно независимыми над $GF(q)$. Доказаны следующие теоремы.

Т е о р е м а 1. *Если* $\gcd(m, N) = 1$, *то матрица* $\mathbf{H}_m$ *определяет проверочную матрицу MPP кода.*

Т е о р е м а 2. *Для кода над* $GF(q^N)$ *с проверочной матрицей*

$\mathbf{H}_m$ *порождающая матрица имеет вид*

$$\mathbf{G}_m = \left\| \tilde{g}_j^{[im]} \right\|_{j=1..n}^{i=0..k-1}, \tag{5}$$

где $k = n - d + 1$ *и элементы* $\tilde{g}_i$ *линейно независимы над* $GF(q^N)$.

Т е о р е м а 3. *Матрица* $\mathbf{H}_m$ *определяет MPP код (множество кодовых слов), которые не могут быть получены из первоначальной конструкции проверочной матрицы вида* $\mathbf{H}$. *При* $m = 1$ *проверочные матрицы совпадают* $\mathbf{H}_{m=1} = \mathbf{H}$ *и задают один код. В общем случае коды различны.*

Для порождающей матрицы $\mathbf{G}_m$ кодовое слово $\mathbf{g}$, соответствующее информационным символам $(u_0, \ldots, u_{k-1})$, выражается через линеаризованные многочлены $F(z)$ специального вида $\mathbf{g} = (F(g_1), F(g_2), \ldots, F(g_n))$, $F(z) = \sum_{i=0}^{k-1} u_i z^{[mi]}$.

Алгоритм декодирования новых ранговых кодов основан на алгоритме декодирования известных ранговых кодов. Алгоритм декодирования использует алгоритм деления Евклида для линеаризованных многочленов. В основе модификации находится использование линеаризованных многочленов специального вида: $F(z) = \sum_{i=0}^{r} f_i z^{[mi]}$, $f_r \neq 0$. Введем норму многочлена $F(z)$ как число $r : |F(z))| = r$.

Т е о р е м а 4. *Линеаризованный многочлен* $F(z) = \sum_{j=0}^{r} f_j z^{[mj]}$ *с* $f_r = 1$ *над полем* $GF(q^N)$ *имеет не более* r *линейно независимых над* $GF(q)$ *корней, если* $\gcd(m, N) = 1$.

Используя теорему и норму многочлена вместо максимальной степени многочлена, остальная модификация алгоритма декодирования для новых кодов достаточно проста.

В третьем разделе главы разработано декодирование ранговых кодов для плохого канала с мощными импульсными широкополосными и постоянными узкополосными шумами. Предполагается, что мощные шумы детектируемы и при приеме кодовой матрицы вычисляется матрица надежностей принятых символов и список стертых строк и столбцов.

Информационная совокупность – это минимальное подмножество символов кодового слова, позволяющее восстановить информационный вектор.

Пусть матричный код над $GF(2^n)$ определен как: $\mathbf{M} = \sum_{i=1}^{k} x_i \mathbf{A}_i$, где $\mathbf{x} = (x_1, \ldots, x_k),\ x_i \in GF(2)$ – информационные символы, и $\mathbf{A}_i$ – линейно независимые над $GF(2)$ $(n \times m)$-матрицы.

Множество S_k из k элементов кодового слова $\mathbf{M}$ называют информационной совокупностью, если можно найти все первоначальные информационные символы $(x_1, \ldots, x_k)$ из S_k.

Т е о р е м а 5. *Пусть P_{S_k} - вероятность того, что случайная выборка S_k из $\mathbf{M}$ является информационной совокупностью. Пусть случайно выбранные матрицы $\mathbf{A}_i$ имеют однородное распределение элементов над $GF(2)$. Тогда, P_{S_k} равняется вероятности P_k того, что случайная $(k \times k)$ матрица с однородным распределением элементов над $GF(2)$ не вырождена: $P_{S_k} = P_k \overset{k\to\infty}{\approx} 0.29$.*

Рассмотрим представление конечного поля $GF(2^n)$ поля матрицами. Пусть $(n \times n)$ матрица $\mathbf{A}$ представляет примитивный элемент поля. Пусть ранговый $(n, 1, n)$-код в матричном виде определяется $\mathbf{V} = \sum_{i=1}^{k} x_i \mathbf{A}^{u_i}$.

Г и п о т е з а 1. *Матрицы $\mathbf{A}^i, i = 1..2^n - 1$, имеют почти однородное распределение элементов над $GF(2)$ для большого n. Часть информационных совокупностей среди всех выборок S_n из $\mathbf{V}$ составляет $P_n \approx 0.29$ для большого n.*

В основе разработанных алгоритмов декодирования матричных ранговых $(n, 1, n)$-кодов находится идея случайной выборки n двоичных элементов из кодового слова (матрицы) и проверке, является ли данная выборка информационной совокупностью. Результаты выполненного численного моделирования подтверждают гипотезу. Показано, что плотность информационных совокупностей среди всех выборок составляет 29%.

Также проведено моделирование на возможность исправления ошибок стирания ранга n, вызванных стертыми линиями, строками и столбцами, для $n = 5$ и $n = 8$. Такой ранг ошибки соответствует

мощным помехам, которые не могут быть скорректированы обычными алгоритмами декодирования ранговых кодов.

Эксперимент показал, что n стертых линий, то есть ошибка ранга n, могут быть исправлены декодированием по информационным совокупностям с шансами близкими к 100%.

В предположении о равномерном случайном распределении информационных символов x_i в кодовой матрице, произведена оценка шансов успешного декодирования для заданного числа случайно стертых линий. Оценено максимальное число стертых линий, которые могут быть исправлены – $\sim 2n - 2\sqrt{n}$. Вычисленные оценки согласуются с данными сделанного моделирования.

Во второй главе производится криптоанализ и построение новых криптосистем с открытым ключом на ранговых кодах.

В первом разделе главы кратко описываются известные результаты о видах и защищенности криптосистем с открытым ключом на ранговых кодах.

Во втором разделе главы производится обобщение разных известных вариантов ГПТ в одну общую форму, строится атака на разложение открытого ключа на основе известных атак на исходную ГПТ и оценивается сложность и осуществимость взлома.

Вводится обозначения для двух рангов матрицы:
• обычный ранг матрицы $\mathbf{A}$ над $GF(q^N)$ – $\mathsf{r}(\mathbf{A}|q^N)$,
• столбцевой ранг матрицы $\mathbf{A}$ над основным полем $GF(q)$ как максимальное число линейно независимых столбцов над $GF(q)$ – $\mathsf{colr}(\mathbf{A}|q)$.

Для матрицы/вектора $\mathbf{A}$ обозначим операцию возведения всех элементов в степень $[i] = q^i$ как $\mathbf{A}^{[i]}$.

Вначале показывается эквивалентность всех опубликованных вариантов ГПТ одной общей форме для целей криптоанализа:

$$\mathbf{G}_{pub} = \mathbf{S}[\mathbf{X}|\mathbf{G}]\mathbf{P}. \tag{6}$$

• $\mathbf{S}$ – строковый скремблер, обратимая $(k \times k)$-матрица над $GF(q^N)$.
• $\mathbf{G}$ – порождающая $(k \times n)$-матрица МРР (n, k, d)-кода.
• $\mathbf{X}$ – шумовая $(k \times t_X)$-матрица над $GF(q^N)$ с полным столбцевым рангом $\mathsf{colr}(\mathbf{X}|q) = t_X$ и рангом $\mathsf{r}(\mathbf{X}|q^N) = r_X, \quad r_X \leq t_X$. Матрица

$[\mathbf{X}|\mathbf{G}]$ имеет так же полный столбцевой ранг $\mathsf{colr}([\mathbf{X}|\mathbf{G}]|q) = n + t_X$.
• $\mathbf{P}$ – столбцевой скремблер, $((t_X+n)\times(t_X+n))$-матрица над $GF(q)$.
• $t_X + n$ может быть больше N, $\quad n \le N$.

Строится расширенный открытый ключ $\mathbf{G}_{pe}$ как вертикальный вектор, состоящий из матриц $\mathbf{G}_{pub}^{[i]}$, $i = 0..u = n - k - 1$.

$$\mathbf{G}_{pe} = \left\| \begin{array}{c} \mathbf{G}_{pub} \\ \mathbf{G}_{pub}^{[1]} \\ \mathbf{G}_{pub}^{[2]} \\ \dots \\ \mathbf{G}_{pub}^{[u]} \end{array} \right\| = \underbrace{\left\| \begin{array}{ccccc} \mathbf{S} & 0 & 0 & \dots & 0 \\ 0 & \mathbf{S}^{[1]} & 0 & \dots & 0 \\ 0 & 0 & \mathbf{S}^{[2]} & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \mathbf{S}^{[u]} \end{array} \right\|}_{\mathbf{S}_{ext}} \times \underbrace{\left\| \begin{array}{c|c} \mathbf{X} & \mathbf{G} \\ \mathbf{X}^{[1]} & \mathbf{G}^{[1]} \\ \mathbf{X}^{[2]} & \mathbf{G}^{[2]} \\ \dots & \dots \\ \mathbf{X}^{[u]} & \mathbf{G}^{[u]} \end{array} \right\|}_{[\mathbf{X}_{ext}|\mathbf{G}_{ext}]} \times \mathbf{P} \tag{7}$$

Т е о р е м а 6. *Матрица* $[\mathbf{X}_{ext}|\mathbf{G}_{ext}]$ *имеет полный столбцевой ранг* $\mathit{colr}([\mathbf{X}_{ext}|\mathbf{G}_{ext}]|q) = n + t_X$ *и ранг* $r([\mathbf{X}_{ext}|\mathbf{G}_{ext}]|q^N) \le n - 1 + \min(r_X(n-k), t_X, k(n-k))$.

Т е о р е м а 7. *Если ранг* $r(\mathbf{G}_{pe}|q^N) = n + t_X - 1$, *то ключ разлагается на множители за* $O((n+t_X)^3)$ *операций в* $GF(q^N)$.

В основе атаки находится решение уравнения $\mathbf{G}_{pe}\mathbf{h}^T = 0$ для вектора $\mathbf{h}$. Вектор $\mathbf{Ph}$ оказывается вектором первой строки проверочной матрицы для рангового кода с порождающей матрицей $\mathbf{G}$.

Т е о р е м а 8. *Если* $\mathbf{G}_{pe}$ *имеет ранг* $r(\mathbf{G}_{pe}|q^N) = n + t_X - 1 - \alpha$, *тогда сложность разложения открытого ключа составляет* $O(q^{\alpha N}(n+t_X)^3)$ *операций над* $GF(q^N)$.

Для выбора стойких параметров с экспоненциальной атакой следует задавать матрицу $\mathbf{X}$ с условиями $t_X - \alpha \le \min(r_X(n-k), t_X, k(n-k))$.

Т е о р е м а 9. *Если матрица* $\mathbf{X}$ *выбрана над* $GF(q)$, *то открытый ключ* $\mathbf{G}_{pe}$ *имеет ранг* $r(\mathbf{G}_{pe}|q^N) = n + t_X - 1$ *и может быть взломан за* $O((n+t_X)^3)$ *операций в* $GF(q^N)$.

Например, можно создавать матрицу $\mathbf{X}$ над $GF(q^N)$ и требова-

ниями:

$$r_X < \frac{t_X}{n-k},$$
$$1 \le r_X = \left\lfloor \frac{t_X - \alpha}{n-k} \right\rfloor \le \min(t_X, k), \qquad (8)$$
$$t_X > n-k,$$
$$Rate = \frac{k}{n+t_X} \approx \frac{k}{n + r_X(n-k) + \alpha},\ Rate < \frac{k}{2n-k}.$$

В третьем разделе главы приведена конструкция разработанной криптосистемы на приводимых ранговых кодах, в которой искусственная ошибка имеет высокий вес, который больше, чем корректирующая способность кода. Ошибка высокого веса становится возможной за счет выбора столбцевого скремблера специальной формы.

Пусть приводимый ранговый код определен порождающей матрицей $\mathbf{G}_p = \|\mathbf{G}_{ij}\|, \quad i,j = 1,\ldots,p$. Матрицы $\mathbf{G}_{ii}$ – случайные порождающие $(n_i \times k_i)$ матрицы новых построенных в диссертации МРР кодов.

Выберем матрицы $\mathbf{S}, \mathbf{X}, \mathbf{P}$ следующим образом.

Возьмем случайную $(k \times k)$ невырожденную матрицу, строковый скремблер, $\mathbf{S}$ над $GF(q^N)$.

Сгенерируем случайную шумовую верхнетреугольную матрицу $\mathbf{X} = \|\mathbf{X}_{ij}\|_{i=1..p}^{j=1..p}$ из $(k_i \times n_i)$ подматриц $\mathbf{X}_{ij}$ с $\mathbf{X}_{ij} = \mathbf{0}$ для $i > j$. Причем, столбцевые ранги матриц $\|\mathbf{X}_{i,1}\|_{i=1}, \|\mathbf{X}_{i,2}\|_{i=1..2}, \ldots, \|\mathbf{X}_{i,p}\|_{i=1..p}$ должны быть равны $t_1, \quad t_1 < t$ – параметр криптосистемы.

Создадим случайную $(n \times n)$ невырожденную матрицу $\mathbf{P}$, столбцевой скремблер, из основного поля $GF(q)$ так, чтобы $\mathbf{P}^{-1}$ состояла из подматриц $\mathbf{P}_{ij}^{-1}$ размера $(n_i \times k_i)$: $\mathbf{P}^{-1} = \left\|\mathbf{P}_{ij}^{-1}\right\|_{i=1..p}^{j=1..p}$ с некоторыми нулевыми блоками как показано на рисунке 1.

Вычислим матрицу $\mathbf{G}_{pub} = \mathbf{S}(\mathbf{G}_p + \mathbf{X})\mathbf{P}$. Открытый ключ – матрица $\mathbf{G}_{pub}$. Секретный ключ – матрицы $\mathbf{S}, \mathbf{G}_p, \mathbf{X}, \mathbf{P}$.

Шифрование открытого текста вектора $\mathbf{m}$ длины k над полем $GF(q^N)$ выполняется как $\mathbf{c} = \mathbf{m}\mathbf{G}_{pub} + \mathbf{e}$, где искусственная ошибка $\mathbf{e}$ ранга $\mathsf{col r}(\mathbf{e}|q) > t$ выбрана, как показано на рисунке 1. Итого, добавлена искусственная ошибка ранга больше, чем корректирующая способность приводимого кода, заданного $\mathbf{G}_p$.

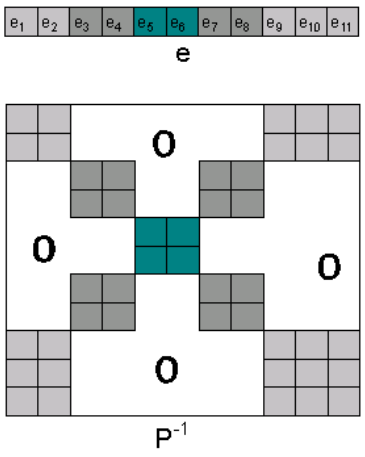

Рис. 1: Пример матрицы $\mathbf{P}^{-1}$ и искусственной ошибки $\mathbf{e}$ с $p = 11$ блоками $\mathsf{colr}(\mathbf{e}_1\mathbf{e}_2 \dots \mathbf{e}_{11}|q) \geq D$ и $p' = 3$ группами блоков $\mathsf{colr}(\mathbf{e}_1\mathbf{e}_2\mathbf{e}_9\mathbf{e}_{10}\mathbf{e}_{11}|q) = t_e$, $\mathsf{colr}(\mathbf{e}_3\mathbf{e}_4\mathbf{e}_7\mathbf{e}_8|q) = t_e$, $\mathsf{colr}(\mathbf{e}_5\mathbf{e}_6|q) = t_e$, $t_e = t - t_1$.

Криптос-ма	Поле	p	n_i	k_i	n	k	Rate	t	t_1	t_e	Ключ	Атака
Исходная	$GF(q^{24})$	2	23	11	46	22	0.48	6	1	5	24 Kbits	2^{87}
Новая	$GF(q^{18})$	4	13	5	65	20	0.38	4	1	9	18.7 Kbits	2^{98}

Таблица 1: Сравнение характеристик криптосистем.

При расшифровании шифротекста $\mathbf{c}$ легальный пользователь выполняет декодирование $\mathbf{cP}^{-1}$ в приводимом ранговом коде, получая $\mathbf{mS}$.

Дополнительно, криптосистема может исправлять ошибки ранга $\mathsf{colr}(\mathbf{e}|q) \leq t - t_1$, возникающие при передаче сообщения по каналу с шумами.

Далее осуществлены криптоанализ и оценена сложность взлома построенной криптосистемы. Использование новых MPP кодов увеличивает сложность взлома в $(\phi(N))^p$ раз, где $\phi(N)$ – функция Эйлера. Ограничивающим фактором на минимальный размер ключа в построенной криптосистеме становятся не атаки на разложение ключа или декодирование как случайного, а атака перебором ошибки. Битовая сложность атаки – $O(q^{p'(Nr_e - N - 2r_e^2) + nr_e})$, где p' – число независимых групп блоков ошибки. На рисунке 1 $p' = 3$.

В таблице 1 приведено сравнение примера новой криптосистемы с ранее известным опубликованным примером криптосистемы на приводимых ранговых кодах.

В третьей главе представлена разработанная в диссертации улучшенная модификация криптосистемы с открытым ключом

NICE-X с быстрым расшифрованием.

В первом разделе главы приведено краткое сравнение наиболее используемых криптосистем с открытым ключом, RSA и Эль-Гамаля, с криптосистемой NICE-X по отношению к скорости алгоритмов и криптостойкости.

Во втором разделе главы изложены математические основы классов эквивалентности идеалов в кольцах целых элементов мнимых квадратичных полей.

Пусть число $\Delta_1 \in \mathbb{Z}, \Delta_1 < 0$ является дискриминантом мнимого квадратичного поля, т.е. $\Delta_1 = 1 \mod 4$ или $\frac{\Delta_1}{4} = 2, 3 \mod 4$. Пусть число $\Delta_q = \Delta_1 q^2, \Delta_q = 0, 1 \mod 4$ с некоторым $q \in \mathbb{Z}, q > 0$.

Множество $\mathcal{O}_{\Delta_1} = \mathbb{Z} + \frac{\Delta_1 + \sqrt{\Delta_1}}{2}\mathbb{Z}$ является кольцом целых алгебраических элементов в мнимом квадратичном поле $\mathbb{Q}(\sqrt{\Delta_1})$. Множество $\mathcal{O}_{\Delta_q} = \mathbb{Z} + \frac{\Delta_q + \sqrt{\Delta_q}}{2}\mathbb{Z}$ является подкольцом $\mathcal{O}_{\Delta_1}$, $\mathcal{O}_{\Delta_q} = \mathbb{Z} + q\mathcal{O}_{\Delta_1}$.

Определим число Δ как Δ_1 для кольца $\mathcal{O}_{\Delta_1}$ или Δ_q для $\mathcal{O}_{\Delta_q}$.

Целый примитивный идеал $\mathfrak{a}$ в $\mathcal{O}_{\Delta_1}$ или $\mathcal{O}_{\Delta_q}$ представляется в виде $\mathfrak{a} = (a, b) = \left(a\mathbb{Z} + \frac{b + \sqrt{\Delta}}{2}\mathbb{Z}\right)$, $b^2 \equiv \Delta \mod 4a$, $a, b \in \mathbb{Z}$, $a > 0$, $b \in (-a, a]$. Норма идеала равна $N(\mathfrak{a}) = a$.

Пусть q – простое число и $\sqrt{|\Delta_1|/3} < q$. Идеалы образуют абелеву группу по умножению. Фактор-группа группы идеалов по подгруппе главных идеалов является группой классов эквивалентности, обозначаемой $Cl(\Delta)$. В каждом классе эквивалентности идеал с минимальной нормой называется редуцированным. Обозначим $Red_\Delta(\mathfrak{a})$ редуцированный идеал, эквивалентный идеалу $\mathfrak{a}$.

Между идеалами в $\mathcal{O}_{\Delta_q}$ и $\mathcal{O}_{\Delta_1}$ можно определить изоморфизм ϕ: $\phi(\mathfrak{a} \subset \mathcal{O}_{\Delta_q}) = \mathfrak{a}\mathcal{O}_{\Delta_1} = \mathfrak{u} \subset \mathcal{O}_{\Delta_1}$, $\phi^{-1}(\mathfrak{u} \subset \mathcal{O}_{\Delta_1}) = \mathfrak{u} \cap \mathcal{O}_{\Delta_q} = \mathfrak{a} \subset \mathcal{O}_{\Delta_q}$. Изоморфизм сохраняет норму идеала. Отображение ϕ также задает гомоморфизм группы классов $Cl(\Delta_q)$ в $Cl(\Delta_1)$: $q - \epsilon(\Delta_1, q) = q \pm 1$ классов из группы $Cl(\Delta_q)$ отображаются в один класс группы $Cl(\Delta_1)$, где ϵ – символ Якоби. Ядро гомоморфизма представляется группой идеалов в $\mathcal{O}_{\Delta_q}$, которые отображаются в подгруппу главных идеалов в $\mathcal{O}_{\Delta_1}$.

Каждый класс эквивалентности однозначно представляется редуцированным идеалом. Вычисления в группе классов производятся

как вычисления с идеалами, принадлежащими классами и последующим редуцированием. Операции редуцирования, умножения, отображения ϕ и ϕ^{-1} идеалов являются квадратичными по времени относительно битовой длины Δ_1, q. Для выполнения операций ϕ, ϕ^{-1} требуется знание Δ_1, q.

В третьем разделе главы сжато описаны криптосистемы с открытым ключом, построенные в мнимом квадратичном поле, и подробно описана криптосистема NICE-X с быстрым расшифрованием.

Криптосистема NICE-X устроена следующим образом. Определяется гомоморфизм ϕ_q идеалов: $\phi_q \equiv Red_{\Delta_1} \circ \phi$. Пусть идеал $\mathfrak{p}$ принадлежит ядру гомоморфизма $Ker(\phi_q)$, т.е. $\phi_q(\mathfrak{p}) = Red_{\Delta_1}(\mathfrak{p}\mathcal{O}_{\Delta_1})$ – главный идеал. Открытым ключом является $(\Delta_q, \mathfrak{p})$, множители (Δ_1, q) – секретный ключ.

Шифрование выполняется так. Пусть $\mathfrak{r}$ – случайный редуцированный идеал в $\mathcal{O}_{\Delta_q}$ с нормой $N(\mathfrak{r}) < \sqrt{|\Delta_1|/4}$. Редуцированный идеал $\mathfrak{r}$ задает элемент $Cl(\Delta_q)$, причем $\phi_q(\mathfrak{r}) = \phi(\mathfrak{r}),\ \phi^{-1}(\phi_q(\mathfrak{r})) = \mathfrak{r}$. Определим редуцированные идеалы $\mathfrak{t} = Red_{\Delta_q}(\mathfrak{p}^k),\ \mathfrak{c} = Red_{\Delta_q}(\mathfrak{r}\mathfrak{t})$, где k – случайное целое число меньше $q - \epsilon(\Delta_1, q)$. Шифрование переводит элемент $Cl(\Delta_q)$ в один из $q - \epsilon(\Delta_1, q)$ классов из $Cl(\Delta_q)$, которые гомоморфизмом ϕ переводятся в один элемент $Cl(\Delta_1)$. Идеал $\mathfrak{r}$ имеет среди редуцированных идеалов этих классов минимальную норму. Шифротекстом битового сообщения m является $[C = m \oplus hash(\mathfrak{t}), \mathfrak{c}]$.

Зная Δ_1 и q, расшифрование шифротекста выполняется как $\mathfrak{r} = \phi^{-1}(\phi_q(\mathfrak{c})),\ \mathfrak{t} = Red_{\Delta_q}(\frac{\mathfrak{c}}{\mathfrak{r}}),\ m = C \oplus hash(\mathfrak{t})$.

В четвертом разделе главы подробно описаны процедуры по генерированию параметров криптосистемы, шифрованию и расшифрованию NICE-X на основе выполненной в диссертации полной программной реализации.

В пятом разделе главы построено ускоренное шифрование для NICE-X, найден класс слабых ключей и показан способ создания безопасных ключей.

Медленное шифрование NICE-X обусловлено генерированием большого случайного квадратичного идеала $\mathfrak{r}$ и возведением $\mathfrak{p}$ в случайную степень k. Предложенный авторами криптосистемы NICE-X

Открытый ключ, биты	NICE-X		Модификация NICE-X		RSA	
	Шифрование, мс	Расшифрование, мс	Шифрование, мс	Расшифрование, мс	Шифрование, мс	Расшифрование, мс
512	244	0.78	202	0.78	0.24	15
1024	666	1.46	516	1.46	0.71	79
2048	2807	3.30	1492	3.30	2.31	514

Таблица 2: Сравнение скорости криптосистем: исходной NICE-X, сделанной модификации NICE-X и RSA с $e = 2^{16} + 1$ на Athlon 1133 MHz.

метод генерирования идеала включает генерирование псевдопростого числа битовой длины n, которое имеет битовую сложность порядка $O(\frac{n^4}{\log n})$ или немного меньше. Битовая сложность возведения идеала в степень – кубическая. Таким образом, шифрование NICE-X имеет битовую сложность четвертой степени.

Генерирование идеала означает создание пары чисел $(a, b) : b^2 = \Delta_q \mod 4a,\ a > 0,\ -a < b \leq a$. Выбирается простое $a = 3 \mod 4$. С вероятностью $\frac{1}{2}$ решение существует $b = \pm\Delta_q^{\frac{a+1}{4}} \mod a$.

Предлагается вычислить 5 маленьких идеалов с 50-битовыми простыми a_i, а большой идеал представить произведением: $(a, b) = \prod_{i=1}^{5}(a_i, b_i)^{k_i}$ для некоторых k_i. Мощность множества возможных значений a составляет $(\pi(2^{50}))^5 \sim 2^{220}$, где $\pi(n)$ – число простых чисел меньших n. Такой мощности множества значений a вполне достаточно для защищенности схемы.

В описанном способе создания идеалов в операции шифрования отсутствует генерирование большого псевдопростого числа. Сложность генерирования маленьких простых чисел можно считать константой. Сложность шифрования становится кубической. Программная реализация показала ускорение шифрования до двух раз, см. таблицу 2.

В исходной криптосистеме NICE-X не заданы ограничения на генерируемые параметры схемы. В диссертации рассмотрена безопасность выбора произвольных параметров.

Порядок ядра является составным числом $h = q - \epsilon(\Delta_1, q) = q \pm 1$, поэтому не любой идеал $\mathfrak{p}$ из ядра гомоморфизма является безопасным. Если $\mathfrak{p}$ принадлежит маленькой подгруппе, то криптосистема легко взламывается. $\mathfrak{p}$ гарантированно должен быть гене-

ратором всего ядра Ker_ϕ или большой подгруппы.

При выборе параметров схемы предлагается генерировать простое число q с известным разложением числа $h = q \pm 1$ на множители. Тогда можно проверить, является ли $\mathfrak{p}$ генератором большой подгруппы.

В заключении сформулированы основные результаты диссертационной работы.

Основные результаты работы

1. Разработаны новые линейные ранговые коды с максимальным ранговым расстоянием вместе с алгоритмом быстрого декодирования. Коды являются $(n, k, d = n - k + 1)$ кодами с максимальным ранговым расстоянием на границе Синглтона. Новые коды являются обобщением единственных ранее известных ранговых кодов 1985 г.

2. Построен алгоритм декодирования ранговых $(n, 1, n)$-кодов для плохого канала с мощными узкополосными и импульсными широкополосными шумами, вызывающими стирания строк и столбцов в передаваемой кодовой матрице. Найдена доля информационных совокупностей – 29%. Проведено моделирование стираний строк и столбцов и показана возможность декодирования ошибок веса n с шансами 80-100%.

3. Рассмотрена защищенность криптосистем на ранговых кодах типа ГПТ. Показана эквивалентность нескольких вариантов ГПТ одной общей форме открытого ключа. Построена атака на открытый ключ общей формы на основе последних атак на исходную версию ГПТ. Показано, что атака является либо полиномиальной, либо экспоненциальной в зависимости от параметров. Предложен способ выбора безопасных параметров.

4. Разработана новая криптосистема с открытым ключом на основе ранговых кодов, в которой введена искусственная ошибка высокого веса. Добавленная ошибка имеет вес больше, чем корректирующая способность кода. Новая криптосистема имеет лучшую криптостойкость и меньшую длину открытого клю-

ча, чем ранее известные криптосистемы с открытым ключом на ранговых кодах.

5. Построена модификация криптосистемы NICE-X с открытым ключом, построенной в мнимом квадратичном поле с ускоренным шифрованием. Исследована стойкость схемы. Предложен способ выбора более безопасных ключей.

Список публикаций по теме диссертации

1. **Кшевецкий А. С.** Уменьшение размера открытого ключа в криптосистемах на линейных ранговых кодах // Безопасность информационных технологий (БИТ). 2006, т. 3, с. 72–76.

2. **Кшевецкий А. С.** Выбор стойких ключей для криптосистем на ранговых кодах // Труды XLIX научной конференции МФТИ: Современные проблемы фундаментальных и прикладных наук. Москва-Долгопрудный. 2006, ч. 1, с. 8–8.

3. **Кшевецкий А. С., Габидулин Э. М.** Декодирование ранговых кодов новой конструкции // В сб. научных трудов «Некоторые проблемы фундаментальной и прикладной математики и их приложениях в задачах физики». М.: МФТИ, 2005, с. 53–61.

4. **A. Kshevetskiy, E. Gabidulin.** The new construction of rank codes // Proc. of IEEE International Symposium on Information Theory (ISIT'2005). 2005, pp. 2105–2108.

5. **A. Kshevetskiy, E. Gabidulin.** High-weight errors in reducible rank codes // Proc. of the 8th International Symposium on Communication Theory & Applications (ISCTA'2005). 2005, pp. 71–76.

6. **Кшевецкий А. С.** Ошибки высокого веса в криптосистемах, основанных на ранговых кодах // Труды XLVIII научной конференции МФТИ: Современные проблемы фундаментальных и прикладных наук. Москва-Долгопрудный. 2005, ч. 1, с. 11–12.

7. **A. Kshevetskiy.** Information set decoding for rank codes // Proc. of the Ninth International Workshop "Algebraic and Combinatorial Coding Theory" (ACCT'2004). 2004, pp. 254–259.

8. **Кшевецкий А. С.** Построение новых ранговых кодов с максимальным ранговым расстоянием // Труды XLVII научной конференции МФТИ: Современные проблемы фундаментальных и прикладных наук. Москва-Долгопрудный. 2004, ч. 1, с. 9–10.

9. **A. Kshevetskiy.** Modification of the public-key cryptosystem NICE-X // Proc. of the Seventh International Symposium on Communications Theory & Applications (ISCTA'03). 2003, pp. 210–214.

10. **Кшевецкий А. С.** Криптосистемы с открытым ключом, построенные в квадратичных порядках // Труды XLVI научной конференции МФТИ: Современные проблемы фундаментальных и прикладных наук. Москва-Долгопрудный. 2003, ч. 1, с. 8–8.

11. **A. Kshevetskiy.** Several properties of public-key cryptosystems based on quadratic orders // Proc. of the Eighth International Workshop "Algebraic and Combinatorial Coding Theory" (ACCT'2002). 2002, pp. 172–175.

12. **Кшевецкий А. С.** Практическая реализация криптосистемы с открытым ключом в мнимом поле квадратичного порядка, имеющей квадратичное время расшифрования // Труды XLIV научной конференции МФТИ: Современные проблемы фундаментальных и прикладных наук. Москва-Долгопрудный. 2001, ч. 1, с. 9–9.

В работе 3 автору принадлежит идея модификации алгоритма декодирования известных ранговых кодов для декодирования новых ранговых кодов. В работе 4 автору принадлежит конструкция новых ранговых кодов, алгоритмы кодирования и декодирования. В работе 5 автору принадлежит модификация столбцевого скремблера для достижения ошибок высокого веса и криптоанализ новой криптосистемы.

.

Кшевецкий Александр Сергеевич

Разработка новых кодов в ранговой метрике и криптосистем с открытым ключом

Автореферат

Подписано в печать __.__.2007. Формат 60x90/16
Усл. печ. л. 1.0. Тираж 70 экз. Заказ № ____
Московский физико-технический институт
(государственный университет)

141700, г. Долгопрудный, Институтский пер., д. 9