На правах рукописи

Пудовкина Марина Александровна

КОМБИНАТОРНО-АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ ИТЕРАЦИОННЫХ ФУНКЦИЙ В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ

05.13.19 − Методы и системы защиты информации,
информационная безопасность

Автореферат
диссертации на соискание учёной степени
доктора физико-математических наук

Томск – 2017

Работа выполнена в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)» на кафедре «Информационная безопасность».

Научный консультант: действительный член Академии криптографии РФ, Заслуженный деятель науки РФ, доктор физико-математических наук, профессор **Погорелов Борис Александрович**

Официальные оппоненты:

Черёмушкин Александр Васильевич, член-корреспондент Академии криптографии Российской Федерации, доктор физико-математических наук, профессор, федеральное государственное унитарное предприятие «Научно-исследовательский институт «Квант», научный консультант

Бабаш Александр Владимирович, доктор физико-математических наук, профессор, федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет «Высшая школа экономики», кафедра информационной безопасности, профессор

Титов Сергей Сергеевич, доктор физико-математических наук, профессор, федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный университет путей сообщений», кафедра «Информационные технологии и защита информации», главный научный сотрудник

Ведущая организация: Федеральное государственное бюджетное образовательное учреждение высшего образования «Саратовский национальный исследовательский государственный университет имени Н.Г. Чернышевского»

Защита состоится 17 мая 2017 года в 10 час. 30 мин. на заседании диссертационного совета Д 212.267.22, созданного на базе федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский Томский государственный университет», по адресу: 634050, г. Томск, пр. Ленина 36 (учебный корпус №2 ТГУ, аудитория 212Б).

С диссертацией можно ознакомиться в Научной библиотеке и на официальном сайте федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский Томский государственный университет» www.tsu.ru.

Материалы по защите диссертации размещены на официальном сайте ТГУ: http://www.ams.tsu.ru/TSU/QualificationDep/co-searchers.nsf/newpublicationn/PudovkinaMA17052017.html

Автореферат разослан «____» февраля 2017 года.

Ученый секретарь
диссертационного совета
кандидат технических наук, доцент — Тренькаев Вадим Николаевич

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. В связи с активным использованием информационно-телекоммуникационных систем и технологий, в частности, Интернет, возросло число угроз сетевых атак с целью несанкционированного доступа в автоматизированные информационные системы государственных и коммерческих организаций для получения конфиденциальной информации, обеспечения сбоев в работе систем, перехватывания управления критически важными объектами. Поэтому актуальным является совершенствование средств защиты информационных и телекоммуникационных систем, в том числе с помощью все более широко используемых криптографических методов.

В основе криптографических методов защиты информации лежит использование стойких криптосистем, многие из которых основываются на блочных шифрсистемах. Блочная шифрсистема включает в себя алгоритмы шифрования (зашифрования, расшифрования), развёртывания ключа и режимы шифрования. Алгоритм зашифрования реализует криптографическую функцию, зависящую от ключа и называемую *функцией зашифрования*. Далее рассматривается блочная шифрсистема в режиме простой замены [16].

Пусть $\mathbb{N}$ – множество всех натуральных чисел, $\mathbb{N}_0 = \mathbb{N} \bigcup \{0\}$, X – произвольное конечное множество (или алфавит открытого и шифрованного текста); X^t – t-я декартова степень множества X для $t \in \mathbb{N}$, $(X, \otimes)$ – аддитивная абелева группа на множестве X с бинарной операцией $\otimes$; $S(X)$ – симметрическая группа на X, $S_n = S(X)$ при $n = |X|$; $\tilde{K}$ – ключевое множество, K – множество раундовых ключей. Функции зашифрования $f : X \times \tilde{K} \to X$ соответствует множество *частичных функций зашифрования* $\left\{ f_k : X \to X \mid k \in \tilde{K} \right\}$, где функция f_k на каждом фиксированном ключе шифрования $k \in \tilde{K}$ задана условием $f_k : \alpha \mapsto f(\alpha, k)$ для всех $\alpha \in X$. Отметим, что все рассматриваемые далее множества конечны.

При разработке современных алгоритмов шифрования исходят из принципов, сформулированных К. Шенноном [56]. Функция зашифрования строится на основе *итерационного способа*. Согласно данному способу, каждая функция зашифрования $f^{(l)} : X \times \tilde{K} \to X$ однозначно определяется $l \in \mathbb{N}$ *раундовыми функциями* $g^{(i)} : X \times K \to X$, $i = 1, ..., l$, и отображением $\psi^{(l)} : \tilde{K} \to K^l$, реализующим алгоритм развёртывания ключа таким образом, что $\psi^{(l)} : k \mapsto \left(k^{(1)}, ..., k^{(l)} \right)$ и $f_k^{(l)} = g_{k^{(1)}}^{(1)} ... g_{k^{(l)}}^{(l)}$ для каждого $k \in \tilde{K}$, где $\left\{ g_{k^{(i)}}^{(i)} : X \to X \mid k^{(i)} \in K \right\}$ – множество *частичных раундовых функций,* соответствующих $g^{(i)}$ и заданных условием $g_{k^{(i)}}^{(i)} : \alpha \mapsto g^{(i)} \left(\alpha, k^{(i)} \right)$ для всех $\left(\alpha, k^{(i)} \right) \in X \times K$, $i = 1, ..., l$. В этом случае $f^{(l)}$ называется *l-раундовой функцией зашифрования*, а l – *числом раундов*. Раундовые функции состоят из «несложно» реализуемых преобразований, обеспечивающих выполнение не формализуемых

строго свойств функции зашифрования: усложнения, перемешивания и рассеивания [16]. В криптографии итерационным способом реализуются не только функция зашифрования, но также раундовые функции и их компоненты. Все такие функции будем называть *итерационными криптографическими функциями*.

В последние годы части схемы алгоритма шифрования, реализующие свойства усложнения, перемешивания, рассеивания, называются соответственно X*-слоем* (или *слоем наложения ключа*), S*-слоем* (или *слоем* s*-боксов, нелинейным слоем*), L*-слоем* (или *линейным слоем*). Далее под *преобразованием* X-, S- или L*-слоя* понимается преобразование, реализуемое X-, S- или L-слоем соответственно. Алгоритмы блочного шифрования с раундовой функцией, представимой в виде композиции преобразований слоёв X, S и L, называются XSL-*алгоритмами блочного шифрования*. Примерами XSL-алгоритмов блочного шифрования являются: отечественный стандарт шифрования ГОСТ Р. 34.12 –2015 «Кузнечик», американский стандарт шифрования AES, алгоритмы Present [22], Square [33], 3D [52]. У ряда алгоритмов блочного шифрования Фейстеля функция усложнения раундовой функции также является композицией преобразований X, S- и L-слоёв, но действует на половине блока.

Многие методы криптоанализа основаны на наличии нетривиальных «информативных» соотношений между раундовыми ключами, блоками открытого и промежуточного шифрованного текстов, которые позволяют различить частичную функцию зашифрования $f_k^{(j)}: X \to X$, $j \le l$, на случайном неизвестном ключе $k \in \tilde{K}$ от случайной равномерно распределённой на $S(X)$ подстановки. Такие соотношения будем называть *структурами*. Зачастую появление нового метода криптоанализа вызвано нахождением у алгоритма блочного шифрования новой структуры. Многие структуры могут задаваться посредством разбиений множества X^t, в том числе двумя множествами R, R', $R, R' \subseteq X^t$, где множество R характеризует соотношения между блоками открытого текста, а R' – между блоками шифртекста. Эти соотношения по-разному ведут себя относительно преобразований функции зашифрования и случайной идеальной функции. Такие структуры появляются в некоторых основных методах криптоанализа блочных шифрсистем – линейном, разностном и их обобщениях. С линейным методом связаны структуры, заданные линейными соотношениями между раундовыми ключами, блоками открытого и шифрованного текстов, а с разностным – разностные соотношения.

Существование подобных структур может быть вызвано различными комбинаторными и алгебраическими свойствами преобразований, составляющих раундовую функцию, например, приводимостью преобразования L-слоя XSL-алгоритма блочного шифрования. Структура может задаваться или характеризоваться: метрикой Хемминга, классами смежности по некоторой подгруппе, системами импримитивности, парами элементов и т.д. В общем случае построение структур представляет трудную задачу. В частности, в алгоритмах блочного шифрования она характеризуется недостаточными перемешивающими

или рассеивающими свойствами преобразований слоёв X, S или L раундовой функции, а также функцией в целом.

В дискретной математике для классификации объектов часто используется их комбинаторно групповая классификация. Заметим, что подобный подход позволил Ф. Клейну объединить в своей «эрлангенской программе» [6] «различные отрасли геометрии относительно *групп преобразований*, поскольку к этому моменту геометрия, единая по своему существу, раздробилась на ряд почти раздельных дисциплин, которые развивались в значительной степени независимо друг от друга». В этом случае объектами изучения выступали инварианты этих преобразований, а основу составляли утверждения о соотношениях между инвариантными свойствами и группами, их сохраняющими. Наоборот, с конечными группами сопоставляются различные алгебраические и комбинаторные структуры, например, латинские квадраты, системы Штейнера, блок-схемы, конечные геометрии, графы, квадратичные формы, метрики (см., например, [12], [20], [21], [27], [28], [38], [53]). Различные способы задания простых групп, в том числе и как групп, сохраняющих некоторые структуры, содержатся в атласе конечных групп [31].

Встречающиеся структуры криптографических функций обычно связаны с группами, сохраняющими данные структуры. Ранее это были аффинные группы и некоторые их подгруппы. В настоящее время этот список расширяется. Такой группой может быть:

- группа изометрий конечной натурально-значной метрики, например, метрики Хемминга χ и её обобщений, определяющей данную структуру;
- группа инерции криптографической функции (или множества криптографических функций, обладающих общим криптографическим свойством, например, корреляционной иммунностью одного порядка);
- группа, порождённая преобразованиями, которые являются компонентами раундовых функций, или множеством $\{g_k \mid k \in K\}$ частичных раундовых функций.

Основные группы подстановок, сохраняющие структуры на X, естественно разбить на классы: интранзитивных, импримитивных, унипримитивных (т.е. примитивных, но не 2-транзитивных) и 2-транзитивных групп (см. [12]). Кроме того, группе $G \le S(X)$ также могут соответствовать структуры при её действии на множестве X^t при $t \ge 2$ (особенно для кратно транзитивных групп). Для интранзитивных групп подстановок естественными структурами являются орбиты и их объединения. С импримитивными группами в криптографии связан метод гомоморфизмов, а структурой является разбиение на блоки импримитивности. Среди примитивных групп подстановок, классифицированных в теореме О'Нэна-Скотта [46], с точки зрения криптографических приложений интерес представляют: примитивные подгруппы аффинных групп и подгруппы группы экспоненцирования. Аффинные группы определяют структуры, характеризующие, насколько заданное преобразование отлично от аффинного. Эти структуры встречаются в разнообразных методах линеаризации. *Группа*

экспоненцирования $S_q \uparrow S_n$ является группой изометрий метрики Хемминга. При $q = 2$ группа $S_2 \uparrow S_n$ также называется *группой Джевонса* [11]. В криптографии группа $S_q \uparrow S_n$ впервые возникла при геометрической интерпретации теоремы А.А. Маркова о шифрах, не распространяющих искажения [13]. Каждая унипримитивная группа подстановок естественным образом задаёт структуру через 2-арные инвариантные отношения [64], являясь группой изометрий некоторой натурально-значной метрики.

Групповыми свойствами криптографических функций занимались М.М. Глухов, В.Н. Сачков, Б.А. Погорелов, А.В. Черемушкин, Ю.Н. Горчинский, С.П. Горшков, В.С. Анашин, Ф.М. Малышев, М.В. Федюкин, Г.Н. Поваров, И.Г. Шапошников, А.В. Тарасов, Д. Копперсмит, К. Патерсон, Р. Венсдорф, Б. Калиски, Р. Ривест и др. Большая часть работ посвящена описанию группы $\langle g_k \mid k \in K \rangle$, а также групповых свойств преобразований раундовых функций. Например, в работах [43], [50], [57], [61] рассмотрена цикловая структура таких преобразований, а в работах [8], [29], [30], [32], [40], [58], [62], [63] доказано равенство $\langle g_k \mid k \in K \rangle = A(X)$ для алгоритмов блочного шифрования DES, RIJNDAEL, а также для некоторых классов XSL-алгоритмов блочного шифрования и алгоритмов Фейстеля, где $A(X)$ – знакопеременная группа на X. Так, в работах [4], [11], [17], [19], [26], [39], [49] описываются группы, сохраняющие множества криптографических функций. Кроме того, в ряде работ [3], [7], [10], [37] предпринималась попытка переноса соответствий Галуа, рассматривая вместо уравнений над полями $GF(2^n)$ различные отношения на множестве X.

Неявно вопросы, посвящённые связям свойств группы $\langle g_k \mid k \in K \rangle$ с существованием структур у алгоритма блочного шифрования, описаны в [47], [63]. Так, в [63] отмечено, что для отсутствия некоторых структур у алгоритма блочного шифрования требуется примитивность, простота и большой порядок группы $\langle g_k \mid k \in K \rangle$. В работе [47], посвящённой описанию групповых свойств алгоритмов блочного шифрования, утверждается, что условие $\left\langle f_k^{(l)} \mid k \in \tilde{K} \right\rangle = S(X)$ достаточно для гарантирования её стойкости. Однако в [51] приведён пример l-раундового алгоритма блочного шифрования, у которого существует структура, но при этом выполняются равенства: $\langle g_k \mid k \in K \rangle = S(X)$, $\left\langle f_k^{(l)} \mid k \in \tilde{K} \right\rangle = S(X)$ для чётного числа раундов l и $\left\langle f_k^{(l)} \mid k \in \tilde{K} \right\rangle = A(X)$ для нечётного числа раундов l. Таким образом, включение $A(X) \subseteq \left\langle f_k^{(l)} \mid k \in \tilde{K} \right\rangle$, а также «естественные» требования примитивности и 2-транзитивности недостаточны для отсутствия структур у алгоритма блочного шифрования.

В целом спектр возникающих структур и их приложений весьма широк и разнообразен. Построение нестандартной структуры функции зашифрования в ряде случаев может требовать развитие специальной математической теории. Нередко новая структура связана с появлением атаки на конкретный алгоритм

блочного шифрования. Тем самым возникает необходимость в построении общих способов поиска и описании структур функций зашифрования, а в общем случае и итерационных криптографических функций.

Объектом исследования являются структуры итерационных криптографических функций, используемые для оценки уязвимостей систем защиты информации.

Предметом исследования являются алгебраические и комбинаторные свойства структур преобразований, составляющих итерационную криптографическую функцию.

Целью диссертационной работы является исследование структур, обусловленных алгебраическими, комбинаторными и криптографическими свойствами преобразований, составляющих итерационную криптографическую функцию.

Для достижения поставленной цели **решены следующие задачи**:

1. Через разбиения t-грамм множества X^t определены p_G-структуры, и в этих терминах дана комбинаторно-алгебраическая интерпретация ряда известных методов криптоанализа (например, в разностном, усечённых разностей, линейном, гомоморфизмов).
2. Для множества G преобразований итерационной криптографической функции выделены следующие направления исследования p_G-структур:
   - описание способов задания p_G-структур;
   - нахождение степени сохранения p_G-структуры множеством G;
   - нахождение расстояний между преобразованиями из множества $H \subseteq S(X)$ и элементами группы автоморфизмов p_G-структуры относительно некоторой метрики на X.

   Эти направления реализованы для p_G-структур с импримитивной группой автоморфизмов.
3. Исследовано влияние подстановочных и комбинаторных свойств преобразований, составляющих итерационную криптографическую функцию, на существование p_G-структур. В частности, для XSL-алгоритмов блочного шифрования рассмотрена зависимость свойств раундовой функции и функции зашифрования от приводимости линейного преобразования. При этом подтверждена актуальность рассмотрения новых структур, возникающих в связи с приводимостью линейного слоя (отличных от ранее применявших в разностном методе и его обобщениях).
4. Выделены два класса p_G-структуры, задаваемые следующими разбиениями: 1) разбиения множества X, в том числе на смежные классы по подгруппе транзитивной абелевой группы $(X,\otimes)$; 2) разбиения, соответствующие натурально-значным метрикам на множестве X, в частности, метрикам типа Хемминга. Исследованы алгебраические и комбинаторные свойства таких p_G-структур, в том числе:
   - описаны группы автоморфизмов p_G-структур;

- описаны свойства графов, соответствующих p_G-структурам, задающихся метриками типа Хемминга.

5. В терминах укрупнений состояний цепи Маркова исследована возможность наследования различными p_G-структурами свойства марковости алгоритмов блочного шифрования.

Данные задачи соответствуют п. 54 Перечня научно-технических проблем обеспечения информационной безопасности РФ («Разработка фундаментальных проблем теоретической криптографии и смежных с ней областей математики»).

Единство решаемых в диссертационной работе задач заключается в разработке общего алгебраического и комбинаторного способа по описанию структурных свойств итерационных криптографических функций, связанного как с введенным понятием p_G-структуры, так и со свойствами преобразований, составляющих итерационные криптографические функции, а также функции зашифрования.

Методы исследования: теоретическая криптография, алгебра, теория групп подстановок, теория графов, комбинаторный анализ, алгебраическая комбинаторика и другие разделы дискретной математики.

Научная новизна. Все результаты диссертационной работы являются новыми. Основные результаты состоят в следующем:

1. Выявлена общая связь комбинаторно-алгебраических свойств отдельных преобразований, составляющих итерационную криптографическую функцию, с существованием различных структур, представляющих интерес в связи с обобщением известных и построением новых методов криптоанализа.
2. Показано, что один из естественных способов описания структур алгоритмов блочного шифрования состоит в сопоставлении им некоторых разбиений множества X^t (p_G-структуры). Описаны классы разбиений множества X^t для $t \in \{1,2\}$, задающие p_G-структуры, а также их алгебраические, комбинаторные и криптографические свойства.
3. Описаны подстановочные и комбинаторные свойства групп, порождённых разными множествами преобразований, составляющих итерационную криптографическую функцию. Так, приведены натурально-значные метрики, задающие p_G-структуры и инвариантные относительно таких групп. Для XSL-алгоритмов блочного шифрования описаны свойства графов орбиталов группы $C_n(g)$, порождённой преобразованиями X - и L-слоёв. В том числе получены условия, при которых графы орбиталов группы $C_n(g)$ принадлежат к таким важным для алгебраической комбинаторики классам графов как дистанционно транзитивные и дистанционно регулярные. Также описаны все линейные преобразования, у которых одна из метрик графов орбиталов изоморфна метрике Хемминга.
4. Выявлена связь натурально-значных метрик, p_G-структур и метрик, инвариантных относительно преобразования линейного слоя, в том числе

метрик типа Хемминга. В связи с этим полностью классифицированы метрики типа Хемминга на V_n, группа изометрий которых является надгруппой группы Джевонса $S_2 \uparrow S_n$. Среди графов орбиталов надгрупп группы Джевонса описаны такие классы графов как дистанционно транзитивные и антиподальные, в том числе проведено сопоставление с ранее известными графами.

5. Предложено понятие L-факторструктуры преобразования, обобщающее известную линейную структуру преобразования, и описана группа автоморфизмов L-факторструктуры.
6. Для каждого $m \in \{1,...,n\}$ описана группа инерции множества всех корреляционно-иммунных функций порядка m, отображающих V_n в $GF(2)$.
7. Показано, что группой автоморфизмов ряда p_G-структур являются сплетения групп подстановок. В связи с этим в качестве меры, характеризующей, насколько подстановки, составляющие функцию зашифрования, не сохраняют такие структуры, введено расстояние между подстановкой и сплетением групп подстановок. Описаны подстановки, максимально далекие от сплетения групп подстановок при заданной системе импримитивности, которые можно считать аналогом функций, максимально далёких от аффинных функций (т.е. аналог бент-функций).
8. Предложены способы описания p_G-структур и комбинаторно-алгебраические свойств у семейства обобщений алгоритма Фейстеля 2-го типа и марковских XSL-алгоритмов блочного шифрования с приводимым преобразованием линейного слоя. Приведена p_G-структура, позволяющая различить семейство обобщений алгоритма Фейстеля 2-го типа от множества случайных равномерно распределённых подстановок. Для XSL-алгоритмов блочного шифрования с приводимым преобразованием предложен способ построения обобщённой разностной характеристики, основанной на смежных классах инвариантного подпространства линейного преобразования.
9. Дана интерпретация широко известных результатов [44] о марковости алгоритмов блочного шифрования в терминах укрупнения состояний вероятностных автоматов. Она распространена на $\otimes_{\mathbf{W}}$-марковские алгоритмы блочного шифрования. Для разбиения $\mathbf{W} = \{W_0,...,W_{r-1}\}$ алфавита текстов X, блоки которого являются смежными классами по некоторой подгруппе W_0 группы $(X,\otimes)$, доказана эквивалентность между $\otimes_{\mathbf{W}}$-марковостью и существованием нетривиального подстановочного гомоморфизма алгоритма шифрования.

Соответствие диссертации паспорту специальности. Тема и содержание диссертационной работы соответствуют требованиям паспорта специальности 05.13.19 − Методы и системы защиты информации, информационная безопасность и соответствует следующим областям исследований паспорта специальности: 9. Модели и методы оценки защищённости информации и

информационной безопасности объекта; 13. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечению информационной безопасности.

Результаты, выносимые на защиту.

1. Описание подстановочных и комбинаторных свойств групп, порождённых преобразованиями, составляющими итерационную криптографическую функцию, в том числе преобразованиями X- и L- слоёв функции зашифрования, а также характеризация свойств соответствующих графов орбиталов и их метрик.
2. Описание натурально-значных метрик, инвариантных относительно группы сдвига V_n.
3. Классификация подметрик метрики Хемминга на V_n и их групп изометрий, и полное описание возникающих при этом дистанционно транзитивных графов орбиталов надгрупп группы Джевонса.
4. Описание группы автоморфизмов L-факторструктуры и группы инерции множества всех двоичных корреляционно-иммунных функций.
5. Общие оценки величины $\chi_{\mathbf{W}}(g)$, характеризующей удаленность произвольного преобразования от сплетения групп подстановок, сохраняющего p_G-структуру. Полное описание подстановок, максимально далеких от сплетения групп подстановок при заданной системе импримитивности.
6. Обобщения $\otimes$-марковости алгоритмов блочного шифрования до $\otimes_{\mathbf{W}}$-марковости. Описание свойств $\otimes_{\mathbf{W}}$-марковских алгоритмов блочного шифрования и $\otimes_{\mathbf{W}}$-марковских преобразований, в том числе условий на разбиение $\mathbf{W}$ множества X, при которых имеет место $\otimes_{\mathbf{W}}$-марковость.

Научная и практическая значимость работы определяется следующим.

1. Разработкой общего способа поиска и построения p_G-структур, обусловленных комбинаторно-алгебраическими свойствами преобразований, составляющих итерационную криптографическую функцию, позволяющего предлагать новые методы криптоанализа, и обобщать известные.
2. Описанием влияния свойств отдельных преобразований, составляющих функцию зашифрования, на существование различных потенциально опасных p_G-структур. В том числе определение влияния приводимости преобразования линейного слоя на стойкость XSL-алгоритмов блочного шифрования.
3. Классификацией подметрик метрики Хемминга на V_n и их групп изометрий, являющихся надгруппами группы Джевонса $S_2 \uparrow S_n$; классификацией дистанционно транзитивных графов, естественным образом соответствующих подметрикам метрики Хемминга.

4. Описанием для каждого $m \in \{1,...,n\}$ группы инерции множества всех двоичных корреляционно-иммунных функций порядка m, отображающих V_n в $GF(2)$.
5. Введением понятий $\otimes_{\mathbf{W}}$-марковских алгоритмов блочного шифрования и $\otimes_{\mathbf{W}}$-марковских преобразований и описанием их свойств.
6. Описанием p_G-структуры семейства обобщённых алгоритмов Фейстеля 2-го типа, позволяющей отличить данное семейство от множества равномерно распределённых случайных подстановок.
7. Разработкой способа анализа XSL-алгоритмов блочного шифрования, использующего инвариантные подпространства линейного преобразования и обобщающего разностный метод.

Внедрение результатов исследований. Основная часть диссертационных исследований выполнялась в 2005 − 2016 гг. в рамках темы 4 (и других тем) Академии криптографии РФ.

Результаты исследований внедрены в Обществе с ограниченной ответственностью «Специальный Технологический Центр» (ООО «СТЦ») (г. Санкт-Петербург) и в Акционерном обществе «МакроСистемы» (г. Москва), а также на кафедре «Информационная безопасность» Московского государственного технического университета имени Н.Э. Баумана (национального исследовательского университета). Они также использованы в тематиках дипломных проектов и аспирантских исследований.

Личный вклад соискателя. Основные результаты диссертации являются новыми и получены автором самостоятельно.

Апробация результатов диссертации. Основные результаты диссертации докладывались на следующих научных конференциях и семинарах: семинар кафедры алгебры МГУ им. М.В. Ломоносова; семинар «Математические методы криптоанализа» МГУ им. М.В. Ломоносова; семинар отдела алгебры и топологи ИММ УрО РАН (г. Екатеринбург); семинар НИИ прикладных проблем математики и информатики БГУ (г. Минск); совместный семинар City College of New York, Stevens Institute of Technology (г. New York); семинар кафедры информационной безопасности МГТУ им. Н.Э. Баумана; семинары и конференции ИКСИ Академии ФСБ РФ; семинар 16 центра ФСБ РФ; международный семинар «Дискретная математика и её приложения» (г. Москва, 2007, 2009, 2012); Общероссийская научно-практическая конференция «Методы и технические средства обеспечения безопасности информации» (г. Санкт-Петербург, 2006, 2007); Сибирская научная школа-семинар с международным участием «Компьютерная безопасность и криптография» (2007 – 2012, 2014 – 2016); международная конференция «Рускрипто» (Московская область, 2008−2013, 2016); международный семинар «Workshop on mathematical cryptology» (Spain, 2008); международный семинар «Asymptotic group theory and applications» (USA, 2009); Белорусская математическая конференция (г. Минск, 2010); международная конференция «Central European conference on cryptology» (Poland, 2010); международный семинар «West European workshop on research in cryptography» (Germany, 2011, 2013); международная конференция «Discrete mathematics, algebra, and their

applications» (г. Минск, 2009); Общероссийская научная конференция «Математика и безопасность информационных технологий» (г. Москва, 2005 – 2011); международный семинар «Foundations and practice of security» (France, 2011); международная конференция «International conference on Bulgarian and Balkans cryptography» (Bulgaria, 2012); международная конференция «Вероятностные методы в дискретной математике» (г. Петрозаводск, 2012); международная конференция «Современные тенденции в криптографии» (г. Нижний Новгород, 2012).

Исследования по теме диссертации поддержаны в 2006 – 2016 гг. Академией криптографии РФ.

Структура и объём работы. Диссертация состоит из введения, пяти глав, заключения и приложения. Список литературы включает 154 наименования. Работа изложена на 300 страницах с примерами и таблицами.

Благодарности. Автор выражает глубокую благодарность научному консультанту д.ф.-м.н., профессору Погорелову Б.А. за постоянное внимание к работе и её обсуждение, а также благодарности за поддержку коллективам кафедр «Информационная безопасность» МГТУ им. Н.Э. Баумана и «Криптология и кибербезопасность» НИЯУ МИФИ.

СОДЕРЖАНИЕ РАБОТЫ

Во **введении** показана актуальность темы диссертации, определены цели и задачи проведённых исследований, дано краткое изложение диссертации по главам. Итерационным криптографическим функциям сопоставляются структуры, многие из которых могут быть представлены в виде пары разбиений $(\mathbf{R},\mathbf{R}')$ множества X^t, где блоки первого разбиения $\mathbf{R}$ характеризуют связи между t-граммами открытого текста, а блоки второго разбиения $\mathbf{R}'$ – между t-граммами шифртекста. Среди всех таких разбиений выделяются разбиения, названные p_G-*структурами*. В диссертационной работе существенным отличием p_G-структур от структур, связанных с группами подстановок, является их рассмотрение с точки зрения криптографических приложений, в частности, возможности их локального сохранения.

Пусть χ_n – метрика Хемминга на множестве X^n; $V_n = V_n(2) = \left(GF(2)\right)^n$; $\oplus(+)$ – операция покоординатного сложения векторов в пространстве V_n; GL_n – полная линейная группа; $\alpha^b = \alpha b = b(\alpha)$ – образ элемента $\alpha \in X$ при действии на него подстановкой $b \in S(X)$, $t \in \mathbb{N}$, $\alpha^h = \left(\alpha^h_{t-1},...,\alpha^h_0\right)$ для $\alpha = \left(\alpha_{t-1},...,\alpha_0\right) \in X^t$, $h \in S(X)$; $J^H = \left\{\alpha^h \mid (h,\alpha) \in H \times J\right\}$ для $J \subseteq X^t$ и $H \subseteq S(X)$. Все рассматриваемые далее множества конечны.

Множеству $G \subseteq S(X)$ и разбиениям $\mathbf{R} = (R_1,...,R_c)$, $\mathbf{R}' = (R'_1,...,R'_{c'})$ множества X^t поставим в соответствие $(c \times c')$-матрицу $p(G,\mathbf{R},\mathbf{R}') = \left(p_{R_i,R'_j}(G,\mathbf{R},\mathbf{R}')\right)$, где

$$p_{R_i,R'_j}(G,\mathbf{R},\mathbf{R}') = |G|^{-1} \cdot |R_i|^{-1} \left|\left\{(b,\alpha) \in G \times R_i \mid \alpha^b \in R'_j\right\}\right| = |G|^{-1} \cdot |R_i|^{-1} \left(\sum_{b \in G} \left|R_i^b \cap R'_j\right|\right).$$

Среди элементов матрицы $p(G,\mathbf{R},\mathbf{R}')$ интерес для криптографии часто представляют её наибольшие и наименьшие элементы.

Определение 1. *Будем говорить, что множество* $G \subseteq S(X)$ *имеет* p_G*-структуру* $(\mathbf{R},\mathbf{R}')_t$, *если* $p_{R,R'}(G,\mathbf{R},\mathbf{R}') \neq p_{R,R'}(S(X),\mathbf{R},\mathbf{R}')$ *для некоторых* $(R,R') \in \mathbf{R} \times \mathbf{R}'$. *Число* t *назовём размерностью структуры.*

Неравенство $p_{R,R'}(G,\mathbf{R},\mathbf{R}') \neq p_{R,R'}(S(X),\mathbf{R},\mathbf{R}')$ при $(R,R') \in \mathbf{R} \times \mathbf{R}'$ означает, что вероятность $p_{R,R'}(G,\mathbf{R},\mathbf{R}')$ для преобразований множества G отлична от аналогичной вероятности $p_{R,R'}(S(X),\mathbf{R},\mathbf{R}')$ для случайной равномерно распределённой подстановки из $S(X)$. Более того, считаем, что при выборе подходящей вычислительной модели (теоретико-сложностной, теоретико-информационной, вероятностно-статистической и т.д.) существование такой отличимости может привести к применению «фундаментальной» атаки различением (см. [36]). Оценка трудоёмкости данной атаки и оценка объёма необходимого материала зависят от выбранной вычислительной модели и в данной работе эти вопросы не рассматриваются.

Определение 2. *Пусть* $G \subseteq S(X)$ *и* $\mathbf{R}$, $\mathbf{R}'$ *– разбиения множества* X^t.

1. p_G*-структура* $(\mathbf{R},\mathbf{R}')_t$ *называется* (R,R')*-инвариантной, если* $p_{R,R'}(G,\mathbf{R},\mathbf{R}') = 1$ *для пары* $(R,R') \in \mathbf{R} \times \mathbf{R}'$.
2. p_G*-структура* $(\mathbf{R},\mathbf{R}')_t$ *называется инвариантной, если* $\mathbf{R}^G = \mathbf{R}'$.
3. p_G*-структура* $(\mathbf{R},\mathbf{R}')_t$ *называется* (R,R')*-невозможной, если* $p_{R,R'}(G,\mathbf{R},\mathbf{R}') = 0$ *для некоторой пары* $(R,R') \in \mathbf{R} \times \mathbf{R}'$.

В диссертационной работе рассматриваются p_G-структуры $(\mathbf{R},\mathbf{R}')_t$ размерности $t \in \{1,2\}$, представляющие практический интерес. Каждой p_G-структуре $(\mathbf{R},\mathbf{R}')_t$ поставим в соответствие множества

$$\mathrm{U}(\mathbf{R},\mathbf{R}')_t = \left\{h \in S(X) \mid \mathbf{R}^h = \mathbf{R}'\right\},\ \mathrm{U}_{R,R'}(\mathbf{R},\mathbf{R}')_t = \left\{h \in S(X) \mid R^h = R'\right\},$$

возможно, пустые, где $|R| = |R'|$ для некоторых $(R,R') \in \mathbf{R} \times \mathbf{R}'$. Заметим, что если $\mathbf{R} = \mathbf{R}'$ $(R = R')$, то множество $\mathrm{U}(\mathbf{R},\mathbf{R})_t$ $\left(\mathrm{U}_{R,R}(\mathbf{R},\mathbf{R}')_t\right)$ непусто и является группой. Каждой p_G-структуре $(\mathbf{R},\mathbf{R})_t$ соответствует группа $\mathrm{U}(\mathbf{R},\mathbf{R})_t$, являющаяся *группой автоморфизмов* p_G-структуры. Согласно «эрлангенской программе» Ф. Клейна, классификация и изучение p_G-структур в работе связаны со свойствами их групп автоморфизмов.

Приведены примеры p_G-структур, встречающихся в криптографии, в частности, показана связь p_G-структур с понятием признака в полугруппе, введённого В.М. Фомичёвым [18].

В **главе 1** рассматриваются p_G-структуры, задающиеся разбиениями множества X с равномощными блоками, и описывается их связь со сплетением групп подстановок. §1.1 является вводным. В §1.2 вводится понятие L-факторструктуры множества подстановок, обобщающее понятие «линейной структуры».

Определение 3. *Будем говорить, что множество подстановок* $G \subseteq S(X)$ *обладает* L*-факторструктурой, задаваемой собственными подмножествами* $W, U \subset X$, $|W| = |U|$, *если* $(\beta + W)^s = \beta^s + U$ *для всех* $(\beta, s) \in X \times G$.

Пусть $\mathbf{R} = \{R_\delta \mid \delta \in X\}$ − разбиение декартова произведения X^2 с блоками $R_\delta = \{(\alpha, \alpha+\delta) \mid \alpha \in X\}$ для $\delta \in X$. Для произвольного разбиения $\mathbf{W}$ множества X положим $R_W = \bigcup_{\varepsilon \in W} R_\varepsilon$ для каждого блока $W \in \mathbf{W}$. Тогда $\mathbf{R}_\mathbf{W} = \{R_W \mid W \in \mathbf{W}\}$ − разбиение декартова произведения X^2, определяемое разбиением $\mathbf{W}$.

L-факторструктуре множества подстановок $G \subseteq S(X)$, задаваемой подмножествами $W, U \subset X$, соответствует 2-мерная (R_W, R_U)-инвариантная p_G-структура $(\mathbf{R}_\mathbf{W}, \mathbf{R}_\mathbf{U})_2$, $\mathbf{W}$, $\mathbf{U}$ − такие разбиения множества X, что $(W, U) \in \mathbf{W} \times \mathbf{U}$. Кроме того, L-факторструктура также является $(R_W, R_{U'})$-невозможной p_G-структурой $(\mathbf{R}_\mathbf{W}, \mathbf{R}_\mathbf{U})_2$ для каждого $U' \in \mathbf{U} \setminus \{U\}$.

Пусть $\mathbf{W}_{w,r}$ − множество всех разбиений множества X с r блоками мощности w каждый, $w > 1$, $r > 1$, $|X| = wr$; $G_1 \wr G_2$ − сплетение групп подстановок G_1, G_2; $\mathrm{IG}_\mathbf{W} = (S_w \wr S_r, \mathbf{W})$ − максимальная группа подстановок, сохраняющая разбиение $\mathbf{W} \in \mathbf{W}_{w,r}(X)$.

В утверждении 1.2.1 доказывается, что для разбиения $\mathbf{W} = \{W_0, ..., W_{r-1}\}$, блоки которого являются смежными классами по подгруппе $(W_0, +)$ аддитивной группы $(X, +)$, L-факторструктуре соответствует одномерная инвариантная p_G-структура $(\mathbf{W}, \mathbf{W})_1$, причём $\mathrm{U}(\mathbf{W}, \mathbf{W})_1 = \mathrm{IG}_\mathbf{W}$. Заметим, что наличие группы $\mathrm{IG}_\mathbf{W}$, как группы автоморфизмов p_G-структуры, может означать возможность применения метода гомоморфизмов (см. [1]).

В связи с возможными обобщениями метода гомоморфизмов в §1.3 оценивается расстояние между подстановкой $g \in S(X)$ и подстановками из группы $\mathrm{IG}_\mathbf{W}$. В частности, находится величина $\chi_\mathbf{W}(g) = \min\{\chi(g,h) \mid h \in \mathrm{IG}_\mathbf{W}\}$, названная *расстоянием до импримитивной группы* $\mathrm{IG}_\mathbf{W}$, где $\chi(g, g') = \left|\{\alpha \in X \mid \alpha^g \neq \alpha^{g'}\}\right|$ при $g, g' \in S(X)$. Для этого каждому разбиению $\mathbf{W} = \{W_0, ..., W_{r-1}\}$ множества X с равномощными блоками и преобразованию $g \in S(X)$ ставится в соответствие $(r \times r)$-матрица $c_\mathbf{W}(g) = (c_{i,j}(g))$, где $c_{i,j}(g) = |W_j \cap W_i^g|$. Данная матрица характеризует, насколько блоки разбиения $\mathbf{W}$ перемешаны относительно друг друга преобразованием g. Элементы матрицы

$c_{\mathbf{W}}(g)$ позволяют найти $\chi_{\mathbf{W}}(g)$ и оценить сверху и снизу расстояние Хемминга от подстановки g до произвольной подстановки $s \in \mathrm{IG}_{\mathbf{W}}$.

Напомним, что *остовом* $(r \times r)$-матрицы $c = \left(c_{i,j}\right)$ называется такой набор $\left[t_0,...,t_{r-1}\right]$, $\{t_0,...,t_{r-1}\} \subseteq \{0,...,r-1\}$, что c_{i,t_i} – максимальный элемент в i-й строке матрицы c для каждого $i \in \{0,...,r-1\}$. Если $\{t_0,...,t_{r-1}\} = \{0,...,r-1\}$, то остов $\left[t_0,...,t_{r-1}\right]$ называется *подстановочным*. Величина $v(c) = v\left(c,\left[t_0,...,t_{r-1}\right]\right) = \sum_{i=0}^{r-1} c_{i,t_i}$ – *вес остова* $\left[t_0,...,t_{r-1}\right]$ матрицы c (вес всех остовов одинаков).

Теорема 1.3.4. *Пусть* $w > 1$, $r > 1$, $\mathbf{W} \in \mathbf{W}_{w,r}$, $s \in \mathrm{IG}_{\mathbf{W}}$, $g \in S(X)$. *Тогда:*

1) $\chi(g,s) \geq |X| - v\left(c_{\mathbf{W}}(g)\right)$;

2) $\chi_{\mathbf{W}}(g) = |X| - \max\left\{\sum_{i=0}^{r-1} c_{i,i^h}(g) \middle| h \in S\left(\{0,...,r-1\}\right)\right\}$;

3) *если у матрицы* $c_{\mathbf{W}}(g)$ *существует подстановочный остов, то*

$$\chi_{\mathbf{W}}(g) = |X| - v\left(c_{\mathbf{W}}(g)\right).$$

Описаны подстановки, максимально далекие от группы $\mathrm{IG}_{\mathbf{W}}$, которые можно считать аналогом бент-функций. В этом случае расстояние до аффинного преобразования заменяется расстоянием до импримитивной группы и вместо линейного метода рассматривается применимость метода гомоморфизмов. Оценено максимальное расстояние между произвольной фиксированной подстановкой и группой $\mathrm{IG}_{\mathbf{W}}$.

Рассмотрим множество $C_{w,r}$ всех целых неотрицательных $(r \times r)$-матриц $c = \left(c_{i,j}\right)$ со свойством $\sum_{t=0}^{r-1} c_{i,t} = \sum_{t=0}^{r-1} c_{t,j} = w$. Пусть $C_{w,r}^{(\max)}$ – множество всех «максимально равномерных» матриц, т.е. матриц $c = \left(c_{i,j}\right) \in C_{w,r}$, удовлетворяющих одному из следующих трёх условий:

1. c – $(0,1)$-матрица и если $w < r$, то в каждой её строке и в каждом столбце имеется ровно w элементов, равных единице.
2. Если $w \equiv 0 (\mathrm{mod}\, r)$, то в каждой строке все элементы равны wr^{-1}.
3. Если $w > r$, $w \not\equiv 0 (\mathrm{mod}\, r)$, то $c_{i,j} \leq \left\lceil wr^{-1} \right\rceil$ для $i, j = 0,...,r-1$.

Утверждение 1.3.5. *Если* $\mathbf{W} \in \mathbf{W}_{w,r}$ *и* $g \in S(X)$, *то*

$$\chi_{\mathbf{W}}(g) \leq |X| - \left\lceil wr^{-1} \right\rceil r.$$

Равенство имеет место тогда и только тогда, когда $c_{\mathbf{W}}(g) \in C_{w,r}^{(\max)}$.

Найдено расстояние $\chi_{\mathbf{W}}$ для s-боксов $s_0,...,s_{d-1} \in S(X)$ алгоритма блочного шифрования. В утверждении 1.3.7 доказывается, что если $s = (s_{d-1},...,s_0) \in S(X)^d$,

$\mathbf{W}^{(j)} = \left\{W_0^{(j)},...,W_{r^{(j)}-1}^{(j)}\right\}$ – система импримитивности группы $\mathrm{IG}_{\mathbf{W}^{(j)}} \le S(X)$ для $j = 0,...,d-1$, $\mathbf{W} = \mathbf{W}^{(d-1)} \times ... \times \mathbf{W}^{(0)}$, то

$$\chi_{\mathbf{W}}(s) \le |X|^d - \prod_{i=0}^{d-1}\left(|X| - \chi_{\mathbf{W}^{(i)}}(s_i)\right). \qquad (1.1)$$

Кроме того, $c_{\mathbf{W}}(s) = c_{\mathbf{W}^{(d-1)}}(s_{d-1}) \otimes ... \otimes c_{\mathbf{W}^{(0)}}(s_0)$, где $\otimes$ – операция тензорного произведения матриц. Также доказано (утверждение 1.3.8), что неравенство (1.1) становится равенством, если у каждой из матриц $c_{\mathbf{W}^{(0)}}(s_0),\ldots,c_{\mathbf{W}^{(d-1)}}(s_{d-1})$ существует подстановочный остов. С помощью неравенства (1.1) (следствие 1.3.9) получены оценки расстояния $\chi_{\mathbf{W}}$ раундовой функции XSL-алгоритма блочного шифрования от класса разбиений пространства V_n, сохраняемых группой, порождённой преобразованиями X - и L-слоёв.

Пусть X^+ – регулярное подстановочное представление аддитивной группы $(X,+)$; $C_n(g) = \langle g \rangle V_n^+$ – подгруппа аффинной группы AGL_n для линейного преобразования $g \in GL_n$.

В §1.4 для s-боксов и линейного преобразования h алгоритма блочного шифрования SMS4 [65] приведен пример нахождения величины $\chi_{\mathbf{W}}(s)$ с помощью неравенства (1.1) для различных систем импримитивности $\mathbf{W}$ группы $C_{32}(h)$, а также величины $\chi_{\widetilde{\mathbf{W}}}$ – для раундовой функции алгоритма SMS4 и систем импримитивности $\widetilde{\mathbf{W}}$ группы $\left(C_{32}(h)\right)^4$. Заметим, что задача оценивания расстояния между подстановкой g и подстановками из множеств $\bigcup_{\mathbf{W}\in\mathbf{W}_{w,r}} \mathrm{IG}_{\mathbf{W}}$ значительно сложнее, чем для группы $\mathrm{IG}_{\mathbf{W}}$. Она сводится к анализу различия в цикловой структуре подстановок из $\bigcup_{\mathbf{W}\in\mathbf{W}_{w,r}} \mathrm{IG}_{\mathbf{W}}$ и подстановки g. В [15] автором диссертационной работы получены оценки для некоторых классов подстановок множества $\bigcup_{\mathbf{W}\in\mathbf{W}_{w,r}} \mathrm{IG}_{\mathbf{W}}$.

В §1.5 показано, что в разностном методе и его обобщениях, а также в методе гомоморфизмов, возникает задача оценки расстояния от множества подстановок до некоторых импримитивных групп.

Использование натурально-значных метрик является удобным средством для исследований в различных разделах дискретной математики. Кроме того, группа изометрий нетривиальной натурально-значной метрики является либо интранзитивной, либо импримитивной, либо унипримитивной. Поэтому каждой нетривиальной натурально-значной метрике соответствует инвариантная 2-мерная p_G-структура. В связи с этим естественно применить натурально-значные метрики для задания 2-мерных p_G-структур и описания их свойств, а также для нахождения расстояний относительно таких метрик от преобразований из множества G до элементов группы автоморфизмов $\mathrm{U}(\mathbf{R},\mathbf{R})_2$.

Глава 2 посвящена свойствам 2-мерных p_G-структур, задающихся конечными натурально-значными метриками на множестве X. §2.1 является вводным. В §2.2 описаны общие свойства конечных натурально-значных метрик. Так, в теореме 2.2.1 приводятся необходимые и достаточные условия, при которых разбиению **A** множества $X^2 \setminus \{(\alpha,\alpha) \mid \alpha \in X\}$ соответствуют конечные натурально-значные метрики, число которых является бесконечным. Однако при задании на наборе значений этих метрик некоторого отношения линейного (лексикографического) порядка $\preceq$, оказывается, что существует единственный набор значений, наименьший относительно введённого порядка. Метрика, соответствующая разбиению **A** с таким набором значений, названа *канонической*. Дальнейшие исследования в диссертационной работе проводятся только для канонических метрик. Класс канонических метрик включает в себя метрики, принимающие все значения из множества $\{0,...,d\}$, где $d \in \mathbb{N}$, $(d+1)$ *– значность* метрики, названные *натуральными*. Отметим, что метрика любого связного графа, заданная кратчайшим расстоянием между вершинами, является натуральной.

Назовём множество $A \subseteq X^2$ *симметричным*, если $(\alpha_1,\alpha_2) \in A$ тогда и только тогда, когда $(\alpha_2,\alpha_1) \in A$. Далее рассматриваются только 2-мерные p_G-структуры $(\mathbf{R},\mathbf{R})_2$, у которых каждый блок разбиения **R** является симметричным. В §2.3 описан класс 2-мерных p_G-структур $(\mathbf{R}(R),\mathbf{R}(R))_2$, задающихся симметричным множеством $R \subseteq X^2$, которым соответствует натуральная метрика $\rho_R : X^2 \to \mathbb{N}_0$, где $\mathbf{R}(R)$ – разбиение X^2 с симметричными блоками, определяемое блоком $R \subseteq \mathbf{R}(R)$. Множеству R также ставится в соответствие граф $\overline{R} = (X,R)$ с множеством вершин X и множеством рёбер R. В утверждении 2.3.2 доказывается равенство $\mathrm{Isom}(\rho_R) = \mathrm{Aut}(\overline{R})$, где $\mathrm{Isom}(\rho_R)$ – группа изометрий метрики ρ_R на X, $\mathrm{Aut}(\overline{R})$ – группа автоморфизмов графа $\overline{R}$.

§2.4 посвящён описанию свойств подметрик и надметрик натуральных метрик. Среди всех натурально-значных метрик на множестве X можно установить иерархию относительно порядка $\preceq$, как это было описано в §2.2. При сравнении метрик используется также понятие «преобладающей» метрики [34]. Более «тонко» сравнивать метрики можно с помощью понятий «подметрики» и «надметрики» [13], [14].

Определение 4. *Пусть μ – конечная натурально-значная метрика на множестве X, а метрика $\mu' : X^2 \to \mathbb{N}_0$ удовлетворяет для всех $\alpha,\beta,\gamma,\delta \in X$ условиям:*

1) *если* $\mu(\alpha,\beta) = \mu(\gamma,\delta)$, *то* $\mu'(\alpha,\beta) = \mu'(\gamma,\delta)$;
2) $\mu'(\alpha,\beta) \le \mu(\alpha,\beta)$.

Тогда μ' называется подметрикой метрики μ, а μ' – надметрикой метрики μ.

Выделяются два класса натуральных метрик, близкие по своим свойствам к метрике Хемминга на V_n, одной из наиболее часто встречающихся метрик в

различных приложениях в дискретной математике, теории кодирования и криптографии. К первому классу, обозначенному через M_n^+, относятся все натуральные метрики на V_n, инвариантные относительно подстановочного представления группы сдвигов V_n^+, а ко второму классу − натуральные метрики, инвариантные относительно группы Джевонса $S_2 \uparrow S_n$. Первый класс является достаточно представительным. Так, он содержит второй класс, все надметрики и подметрики метрики Хемминга, а также изоморфные ей метрики. В связи с этим провести полную классификацию всех натуральных метрик, входящих в него, не представляется возможным.

В §2.5 показано, что среди метрик множества M_n^+ существуют метрики наибольшей значности, равной 2^n, названные *максимальными*. В теореме 2.5.2 описываются все максимальные метрики множества M_n^+ и доказана их линейная эквивалентность (относительно изоморфизма, задающегося линейным преобразованием из GL_n). В утверждении 2.5.4 доказывается, что все метрики из множества M_n^+ являются подметриками максимальных метрик, разбивающимися на классы линейно эквивалентных метрик. Описаны (следствие 2.5.5) все $(n+1)$-значные подметрики максимальных метрик множества M_n^+, линейно эквивалентные метрике Хемминга, которые можно рассматривать как аналоги метрики Хемминга. В утверждениях 2.5.6, 2.5.7 приводятся примеры двух $(n+1)$-значных метрик μ_1, μ_2 на V_n, линейно эквивалентных метрике Хемминга χ_n и «разбивающих» множество всех бент-функций, где $n = 2^m$. Данные примеры вызваны тем, что относительно метрики Хемминга χ_n каждая бент-функция $f : V_n \to \{0,1\}$ лежит на расстоянии $2^{m-1} - 2^{m/2-1}$ от множества всех аффинных функций. Поэтому представляет интерес описание $(n+1)$-значной метрики, линейно эквивалентной метрике Хемминга χ_n, относительно которой расстояние между некоторыми бент-функциями и множеством всех аффинных функций меньше числа $2^{m-1} - 2^{m/2-1}$.

Напомним (см. [12]), что *орбиталом* группы подстановок $B \le S(X)$ называется орбита группы B при её естественном действии $(\alpha, \alpha')^b = (\alpha^b, \alpha'^b)$ на множестве X^2 для каждого $b \in B$. Группе $B \le S(X)$ ставятся в соответствие графы, называемые *графами орбиталов*, у которых X − множество вершин, а множество рёбер – *орбитал*.

Для второго класса (натуральные метрики, инвариантные относительно группы Джевонса $S_2 \uparrow S_n$) в §2.6 (утверждения 2.6.2 − 2.6.10) получено полное описание всех его представителей. Это связано с тем, что каждая метрика, принадлежащая ему, является натуральной метрикой графа орбитала группы Джевонса или её надгруппы. Поэтому описание всех метрик из второго класса сводится к описанию всех орбиталов надгрупп группы Джевонса, что равносильно классификации подсхем схемы Хемминга [2], которая получена в

[9]. Последнее позволяет выполнить классификацию всех метрик второго класса.

Большая часть **главы 3** посвящена описанию групповых свойств 2-мерных p_G-структур. Рассматриваются метрики из второго класса и описываются их группы изометрий. §3.1 является вводным. В §3.2 (теоремы 3.2.1, 3.2.17) проводится полная классификация групп автоморфизмов графов орбиталов надгрупп группы Джевонса $S_2 \uparrow S_n$. Отсюда следует описание групп изометрий натуральных метрик, задаваемых орбиталами и классифицированных в §2.6.

Пусть $\tilde{S}_n$ – группа всех подстановочных $(n \times n)$-матриц над $GF(2)$. Заметим, что подгруппа $A\tilde{S}_n$ аффинной группы AGL_n подобна группе экспоненцирования $S_2 \uparrow S_n$ при её естественном действии на V_n.

Для классификации использовано описание надгрупп группы Джевонса $S_2 \uparrow S_n$ в аффинной группе AGL_n, полученное в [13]. В [13] показано, что надгруппами $A\tilde{S}_n$ являются аффинные подгруппы $AS_n^{(1)}$, $AR_n^{(1)}$, $AS_n^{(2)}$, $AO_n^{(1)}$, $AO_n^{(2)}$, ASp_n, где $S_n^{(1)} \cong S_{n+1}$, $R_n^{(1)} \cong S_{n+1}$, $S_n^{(2)} \cong S_{n+2}$, Sp_n – симплектическая подгруппа группы GL_n, $O_n^{(1)}$, $O_n^{(2)}$ – ортогональные подгруппы группы GL_n для чётного n. В §3.2 доказано, что если группа автоморфизмов графа орбитала примитивна, то она совпадает с одной из групп $AS_n^{(1)}$, $AR_n^{(1)}$, $AS_n^{(2)}$, $AO_n^{(1)}$, $AO_n^{(2)}$, ASp_n, $S(V_n)$. Если же группа импримитивна, то системы импримитивности имеют блоки вида $\left\{\alpha, \alpha \oplus \vec{1}_n\right\}$ или $V_n^{(0)}$, $V_n^{(1)}$, где $\vec{1}_n$ – n-мерный единичный вектор, $V_n^{(i)} = \left\{\alpha \in V_n \mid \|\alpha\| \equiv i \pmod 2\right\}$ для $i \in \{0,1\}$, а $\|\alpha\|$ – вес Хемминга вектора $\alpha \in V_n$. Отсюда следует, что группа автоморфизмов графов орбиталов надгрупп группы Джевонса $A\tilde{S}_n$ совпадает со сплетением или прямым произведением групп S_2, $S_{2^{n-1}}$, $AS_{n-1}^{(1)}$, $AR_{n-1}^{(1)}$, $AS_{n-1}^{(2)}$, $AO_{n-1}^{(1)}$, $AO_{n-1}^{(2)}$, ASp_{n-1}.

В §3.3, §3.4 рассматриваются свойства графов, соответствующих орбиталам надгрупп группы Джевонса.

Напомним, что связный граф $\overline{\Gamma} = (X, \Gamma)$ с множеством вершин X и множеством рёбер Γ называется *дистанционно транзитивным*, если для любых вершин $\alpha, \alpha', \beta, \beta' \in X$, для которых $\mu(\alpha, \alpha') = \mu(\beta, \beta')$, существует элемент $g \in \mathrm{Aut}(\overline{\Gamma})$, удовлетворяющий равенствам $\beta = \alpha^g$, $\beta' = \alpha'^g$, где $\mu(\alpha, \alpha')$ – кратчайшее расстояние между вершинами α, α' в графе $\overline{\Gamma}$.

Среди графов, соответствующих орбиталам надгрупп группы Джевонса, возникают такие интересные классы графов как дистанционно транзитивные, антиподальные и двудольные. Подобным графам посвящён целый ряд работ [24], [25], [41], [42], [55] и др. Данные результаты актуальны в связи с взаимным проникновением в настоящее время методов алгебры, теории групп подстановок и теории графов. В связи с этим в §3.3 среди графов орбиталов надгрупп группы Джевонса $A\tilde{S}_n$ выявлены (теорема 3.3.2) все дистанционно транзитивные графы. Среди последних в утверждении 3.3.4 описываются двудольные, антиподальные и примитивные графы. В §3.4 рассматривается связь между дистанционно

транзитивными графами орбиталов надгрупп группы Джевонса и известными классами дистанционно транзитивных графов, полученных иными методами [23], [25]. В теореме 3.4.1 доказывается, что среди дистанционно транзитивных графов орбиталов надгрупп группы Джевонса имеются графы, изоморфные следующим: 1) полному графу K_{2^n}; 2) полному двудольному графу $K_{2^{n-1},2^{n-1}}$; 3) половинному $(n+1)$-кубу; 4) сложенному $(n+1)$-кубу; 5) сложенному половинному $(n+2)$-кубу; 6) графам знакопеременных форм; 7) графу Тейлора (для графов диаметра 3); 8) дополнению $2\times 2^{n-1}$-решётки (для графов диаметра 3); 9) дополнению графа $2^{n-1}K_2$, состоящего из 2^{n-1} двух вершинных компонент связности; 10) графу Адамара (для графов диаметра 4); 11) графам инцидентности $2\text{-}\left(2^{n-1},u_j^{(n)},2u_{j-1}^{(n-2)}\right)$ блок-схем (для графов диаметра 3 при нечётном $n\geq 5$), $j\in\{1,3\}$, где

$$u_i^{(n)}=\sum_{k=0}^{\lfloor (n-i)/4\rfloor}\binom{n}{4k+i},\ i=0,1,2,3.$$

Пусть $P_n=\left\{\lambda\middle|\lambda:V_n\to\{0,1\}\right\}$ – множество всех двоичных функций от n переменных; $I_G(H)=\{g\in G\mid f^g\in H,\forall f\in H\}$, где $G\leq S(V_n)$, $H\subseteq P_n$, $f^g(\alpha)=f(\alpha^g)$ для каждого $\alpha\in V_n$ и $f\in P_n$.

В §3.5 приведён пример применения полученной классификации групп автоморфизмов графов орбиталов надгрупп группы Джевонса для описания группы инерции $I_{S(V_n)}(C_{n,m})$ множества $C_{n,m}$ всех корреляционно-иммунных функций порядка $m\in\{1,...,n\}$ из множества P_n. В теореме 3.5.1 доказывается, что если n, m – произвольные натуральные числа, $n\geq 4$, $m\in\{1,...,n\}$, то

$$I_{S(V_n)}(C_{n,m})=\begin{cases}A\tilde{S}_n, & \text{если } m\leq n-2,\ m\equiv 1\ (\mathrm{mod}\ 2),\\ AR_n^{(1)}, & \text{если } m\leq n-2,\ m\equiv 0\ (\mathrm{mod}\ 2),\\ S_{2^{n-1}}\wr S_2, & \text{если } m=n-1,\\ S(V_n), & \text{если } m=n.\end{cases}$$

Тем самым исправлено описание группы инерции, полученное в [49], где утверждалось, что $I_{S(V_n)}(C_{n,m})=A\tilde{S}_n$ для каждого $m\in\{1,...,n-2\}$.

Глава 4 посвящена описанию влияния приводимости матрицы линейного преобразования XSL-алгоритма блочного шифрования на свойства одномерных и двумерных p_G-структур. Заметим, что исследование влияния приводимости матрицы линейного на свойства XSL-алгоритма считается важной проблемой в международном криптографическом сообществе [35]. §4.1 является вводным. В §4.2 рассматриваются свойства графов орбиталов группы $C_n(h)=\left\langle h,V_n^+\right\rangle$ для приводимой матрицы $h\in GL_n$ и описываются натуральные метрики этих орбиталов (лемма 4.2.1, 4.2.2). В терминах характеристического или минимального многочленов h приведены условия связности графов орбиталов,

их изоморфизма, примитивности и 2-транзитививности группы $C_n(h)$ (утверждения 4.2.4, 4.2.6, 4.2.7).

Исследование группы $C_n(h)$ непосредственно связано с выявлением влияния приводимости линейного преобразования h на свойства XSL-алгоритма блочного шифрования. Так, если линейное преобразование h приводимо и W_0 – соответствующее инвариантное подпространство, то группа $C_n(h)$ имеет инвариантную одномерную $p_{C_n(h)}$-структуру $(\mathbf{W},\mathbf{W})_1$, где $\mathbf{W}=\{W_0,...,W_{r-1}\}$, W_j – j-й класс смежности группы $(V_n,\oplus)$ по подгруппе $(W_0,\oplus)$ для $j=0,...,r-1$. Причём для каждого $i\in\{0,...,r-1\}$ существует такой элемент $j_i\in\{0,...,r-1\}$, что $p_{C_n(h)}$-структура $(\mathbf{W},\mathbf{W})_1$ является (W_i,W_{j_i})-инвариантной. Эта структура является системой импримитивности. Существование $p_{C_n(h)}$-структуры у группы $C_n(h)$, порожденной преобразованиями X,L-слоёв XSL-алгоритма, может влиять на криптографические свойства всего алгоритма. В частности, из существования такой $p_{C_n(h)}$-структуры следует существование атак на алгоритмы блочного шифрования PRINTcipher, Robin, iSCREAM, Zorro [45] и ISEBERG [59].

В §4.3 указаны условия дистанционной транзитивности графов орбиталов группы $C_n(h)$. В §4.4, §4.5 рассмотрены также свойства графов орбиталов группы $C_n(h)$ в двух случаях: когда h лежит в «небольших» надгруппах подстановочных групп и когда h берётся из унитреугольной группы UT_n, $n=2^m$. Так, в утверждении 4.5.5 приводятся условия на орбиталы, при которых соответствующие метрики изоморфны метрике Хемминга (на пространстве V_m, $m\le n$), а также её надметрикам или подметрикам. Описаны натуральные метрики и другие характеристики графов орбиталов группы $C_n(g)$ для циркулянтной матрицы g и матрицы алгоритма блочного шифрования E2.

§4.6 посвящён описанию свойств марковских XSL-алгоритмов блочного шифрования с приводимым линейным преобразованием.

Определение 5. *Алгоритм блочного шифрования с частичной l-раундовой функцией зашифрования $f^{(l)}_{\vec{k}_l}=g_{k^{(1)}}...g_{k^{(l)}}$ на каждом ключе $\vec{k}_l=\left(k^{(1)},....,k^{(l)}\right)\in K^l$ называется l-раундовым итерационным алгоритмом блочного шифрования.*

В диссертационной работе рассматриваются только итерационные алгоритмы шифрования с независимыми и равномерно распределёнными раундовыми ключами. Заметим, что разностный метод и его обобщения часто применяются в марковской модели для таких алгоритмов блочного шифрования.

Пусть $(X,\otimes)$ – произвольная аддитивная абелева группа на множестве X с бинарной операцией $\otimes$; α^{-1} – обратный к α элемент относительно операции $\otimes$, $\alpha\otimes\beta^{-1}=\alpha\,\overline{\otimes}\,\beta$ для любых $\alpha,\beta\in X$; $X^{\times}=X\setminus\{e\}$, если e – нейтральный элемент относительно заданной на X бинарной операции; $\mathrm{P}\{A\}$ – вероятность события A. Для элементов $\theta,\varepsilon\in X$ и раундовой функции $g: X\times K\to X$ положим

$$p_{\theta,\varepsilon}(g)=|K|^{-1}|X|^{-1}\left|\left\{(\alpha,k)\in X\times K\,\middle|\,(\theta\otimes\alpha)^{g_k}=\varepsilon\otimes\alpha^{g_k}\right\}\right|,$$

$$p_{\theta,\varepsilon}(g\,|\,\beta)=|K|^{-1}\left|\left\{k\in K\,\middle|\,(\theta\otimes\beta)^{g_k}=\varepsilon\otimes\beta^{g_k}\right\}\right|,\ \beta\in X\,.$$

Определение 6 [44]. *Итерационный алгоритм блочного шифрования с раундовой функцией g и с независимыми и равномерно распределёнными раундовыми ключами называется $\otimes$-марковским, если для всех элементов $\theta,\varepsilon\in X^{\times}$, $\alpha\in X$ выполняется равенство $p_{\theta,\varepsilon}(g|\alpha)=p_{\theta,\varepsilon}(g)$.*

В [44] доказано, что если $\xi^{(0)}$ – дискретная случайная величина на множестве X, то в l-раундовом итерационном $\otimes$-марковском алгоритме блочного шифрования с независимыми и равномерно распределёнными раундовыми ключами $k^{(1)},\ldots,k^{(l)}$ раундовые разности $\xi^{(t)}=\left(\xi^{(0)}\otimes\alpha\right)^{f_{k_t}^{(t)}}\overline{\otimes}\,\alpha^{f_{k_t}^{(t)}}$ для $t=1,...,l$, являясь случайными величинами, образуют цепь Маркова.

Определение 7. *Для $\otimes$-марковского алгоритма блочного шифрования с раундовой функцией g под «классической» r-раундовой разностной характеристикой будем понимать набор $\left(\lambda^{(r)},...,\lambda^{(1)},\lambda^{(0)}\right)\in\left(V_n^{\times}\right)^{r+1}$ с вероятностью*

$$\mathrm{P}\left\{\left(\lambda^{(r)},...,\lambda^{(1)},\lambda^{(0)}\right)\right\}=\prod_{i=1}^{r}p_{\lambda^{(i-1)},\lambda^{(i)}}(g),$$

а под r-раундовой парой разностей будем понимать пару $\left(\lambda^{(0)},\lambda^{(r)}\right)$.

Для марковского XSL-алгоритма блочного шифрования с приводимым линейным преобразованием вместо «классической» r-раундовой разностной характеристики в разностном методе рассматривается r-раундовая характеристика, заданная последовательностью смежных классов инвариантного подпространства линейного преобразования L-слоя. Полученные при таком подходе вероятности могут увеличить число атакуемых раундов XSL-алгоритма. Приведённый подход в ряде случаев эффективнее по сравнению со способом нахождения вероятностей «классических» разностных характеристик. Предложенный подход проиллюстрирован на примере инволютивного алгоритма блочного шифрования ISEBERG [59]. Проведено сравнение полученных результатов с результатами работы [60].

В **главе** 5 рассматриваются дальнейшие криптографические приложения одномерных и двумерных p_G-структур. §5.1 является вводным.

В §5.2 p_G-структуры описываются для модификации алгоритма Фейстеля 2-го типа. На основе конструкции, предложенной в [66], вводится семейство l-раундовых алгоритмов шифрования $FG_l^{(4)}$. Для него в утверждениях 5.2.1 и 5.2.2 доказывается существование таких нетривиальных разбиений $\mathbf{W}$, $\mathbf{U}$ пространства V_n, что множеству G всех l-раундовых частичных функций зашифрования алгоритма $FG_l^{(4)}$ соответствует 2-мерная p_G-структура $\left(\mathbf{R}_{\mathbf{W}},\mathbf{R}_{\mathbf{U}}\right)_2$,

являющаяся одновременно (W,U)-инвариантной и (W,U')-невозможной для некоторых $W \in \mathbf{W}$, $U,U' \in \mathbf{U}$, $U \neq U'$. Использование таких 2-мерных p_G-структур позволяет различить каждую частичную l-раундовую функцию зашифрования алгоритма $FG_l^{(4)}$ от случайной подстановки независимо от числа его раундов l. В частности, это означает, что 2-транзитивность группы, порождённой всеми частичными раундовыми функциями алгоритма $FG_l^{(4)}$, не достигается для произвольного числа раундов. Полученный результат является примером того, как желание улучшить конструкцию (в данном случае алгоритм Фейстеля 2-го типа) «хорошим» криптографическим преобразованием, а именно, (4×4)-матрицей из GL_4 с наибольшим среди всех матриц из GL_4 коэффициентом рассеивания, приводит к слабому семейству алгоритмов шифрования.

Оставшаяся часть главы 5 посвящена описанию связи 2-мерных p_G-структур с марковскими l-раундовыми итерационными алгоритмами блочного шифрования с раундовой функцией $g: X \times K \to X$ и с независимыми и равномерно распределёнными раундовыми ключами из множества K.

В теории цепей Маркова изучаются такие укрупнения состояний цепи Маркова, которым опять соответствует цепь Маркова. Состояниями новой цепи являются блоки разбиений множества состояний исходной цепи. В §5.3 первоначально рассматривается последовательность случайных величин $\xi^{(0)}, \xi^{(1)}, \ldots, \xi^{(l)}$, соответствующих биграммам промежуточных текстов. В рамках автоматной модели (вероятностного преобразователя) элементарно получается цепь Маркова с множеством состояний X^2 и матрицей вероятностей переходов, элементы которой заданы условием

$$p_{(\alpha_1,\alpha_0),(\alpha_1',\alpha_0')}(g) = \mathrm{P}\left\{\left(\alpha_1^{g_k}, \alpha_0^{g_k}\right) = (\alpha_1', \alpha_0')\right\},$$

где раундовый ключ k выбирается случайно и равновероятно из множества K и, естественно, независимо от биграмм $(\alpha_1,\alpha_0), (\alpha_1',\alpha_0') \in X^2$. Описываются свойства различных укрупнений состояний марковской последовательности $\xi^{(0)}, \xi^{(1)}, \ldots, \xi^{(l)}$ с применением соответствующей теории цепей Маркова [5]. Показано, что результаты основополагающей работы [44] о марковости последовательности $\xi_{\mathbf{R}}^{(0)}, \xi_{\mathbf{R}}^{(1)}, \ldots, \xi_{\mathbf{R}}^{(l)}$, полученной из последовательности $\xi^{(0)}$, $\xi^{(1)}, \ldots, \xi^{(l)}$ укрупнением её состояний посредством разбиения $\mathbf{R} = \{R_\varepsilon \mid \varepsilon \in V_n\}$, непосредственно следуют из [5], где $R_\varepsilon = \{(\alpha, \alpha \oplus \varepsilon) \mid \alpha \in V_n\}$ для $\varepsilon \in V_n$.

В утверждении 5.3.2 приводятся условия, при которых последовательность $\xi_{\mathbf{R}_\mathbf{W}}^{(0)}, \ldots, \xi_{\mathbf{R}_\mathbf{W}}^{(l)}$, полученная посредством дальнейшего укрупнения состояний марковской последовательности $\xi_{\mathbf{R}}^{(0)}, \ldots, \xi_{\mathbf{R}}^{(l)}$ разбиением $\mathbf{W} = \{W_0, \ldots, W_{r-1}\}$ множества X, также является марковской, где $\mathbf{R}_\mathbf{W} = \{R_W \mid W \in \mathbf{W}\}$, а $R_W = \bigcup_{\varepsilon \in W} R_\varepsilon$ для каждого блока $W \in \mathbf{W}$.

Определение 8. *Итерационные алгоритмы блочного шифрования, у которых последовательность* $\xi^{(0)}_{\mathbf{R_W}},\ldots,\xi^{(l)}_{\mathbf{R_W}}$ *является марковской, названы* $\otimes_{\mathbf{W}}$*-марковскими.*

У каждого $\otimes_{\mathbf{W}}$-марковского алгоритма шифрования может существовать p_G-структура $(\mathbf{R_W},\mathbf{R_W})_2$ для $G=\{g_k \mid k\in K\}$.

В XSL-алгоритмах блочного шифрования и алгоритмах шифрования Фейстеля с XSL-функцией усложнения марковость последовательности случайных величин $\xi^{(0)}_{\mathbf{W}},\ldots,\xi^{(l)}_{\mathbf{W}}$ может редуцироваться к свойствам s-боксов и преобразования линейного слоя. В связи с этим введено понятие $\otimes_{\mathbf{W}}$*-марковского преобразования,* следующее из определения $\otimes_{\mathbf{W}}$-марковости алгоритма блочного шифрования. В §5.4 рассмотрены широко используемые в криптографии преобразования, основанные на операциях экспоненцирования и логарифмирования в кольце вычетов $\mathbb{Z}_{2^d}$ и поле $GF(p)$, p − простое число. Указаны разбиения $\mathbf{W}$ множества X, при которых эти преобразования являются $\otimes_{\mathbf{W}}$-марковскими (утверждения 5.4.2, 5.4.4). Примерами $+_{\mathbf{W}}$-марковских преобразований являются s-боксы алгоритма блочного шифрования SAFER [48].

Определение 9 [54]. *APN-подстановкой называется подстановка* $b\in S(V_n)$*, удовлетворяющая равенству*

$$\max\left\{\hat{p}_{\varepsilon,\delta}(b)\mid(\varepsilon,\delta)\in\left(V_n^{\times}\right)^2\right\}=2^{1-n},$$

где

$$\hat{p}_{\theta,\varepsilon}(b)=2^{-n}\left|\left\{\alpha\in V_n\middle|\left(\alpha\oplus\theta\right)^b=\varepsilon\oplus\alpha^b\right\}\right|,\ (\varepsilon,\delta)\in\left(V_n^{\times}\right)^2.$$

Из определения 9 следует, что у любой APN-подстановки $b\in S(V_n)$ наибольший элемент каждой строки матрицы $\hat{p}(b)=\left(\hat{p}_{\theta,\varepsilon}(b)\right)$ вероятностей переходов разностей равен 2^{1-n}. Данное значение является наименьшим среди всех подстановок из $S(V_n)$. Поэтому APN-подстановки считаются (см. [54]) оптимальными для использования в качестве s-боксов для улучшения стойкости алгоритма блочного шифрования относительно разностного метода.

Каждой APN-подстановке поставим в соответствие орграф $\overline{\Gamma}(b)$ с множеством вершин $V_n^{\times}$ и множеством дуг, определяемым $(2^n-1)\times(2^n-1)$-матрицей смежности $q(b)=\left(q_{i,j}(b)\right)$, где при $i,j\in\{1,\ldots,2^n-1\}$ элемент $q_{i,j}(b)$ задаётся условием

$$q_{i,j}(b)=\begin{cases}1, \text{ если } \hat{p}_{i,j}(b)=2^{1-n},\\ 0, \text{ если } \hat{p}_{i,j}(b)=0.\end{cases}$$

Утверждение 5.4.5. *Пусть* b − *произвольная APN-подстановка на* V_n. *Тогда для каждого элемента* $g=\left(\alpha_1^{(1)},\ldots,\alpha_{d_1}^{(1)}\right)\ldots\left(\alpha_1^{(r)},\ldots,\alpha_{d_r}^{(r)}\right)\in\mathrm{Aut}\left(\overline{\Gamma}(b)\right)$

подстановка b *является* $\oplus_{\mathbf{W}^{(g)}}$*-марковской для разбиения* $\mathbf{W}^{(g)} = \{W_0,...,W_r\}$*, где* $W_0 = \{\vec{0}_n\}$ *и* $W_j = \{\alpha_1^{(j)},...,\alpha_{d_j}^{(j)}\}$ *для* $j = 1,...,r$.

Для ряда APN-подстановок b приведены группы автоморфизмов орграфа $\overline{\Gamma}(b)$ и указаны такие разбиения $\mathbf{W}$ пространства V_n, что: 1) b – $\oplus_{\mathbf{W}}$-марковская подстановка; 2) разбиение $\mathbf{W}$ определяется цикловой структурой элемента группы автоморфизмов $\mathrm{Aut}(\overline{\Gamma}(b))$, где соответствующее задание описано в утверждении 5.4.5.

В §5.5 рассмотрены связи между $\otimes_{\mathbf{W}}$-марковостью алгоритмов блочного шифрования, методом гомоморфизмов и существованием p_G-структуры $(\mathbf{R}_{\mathbf{W}}, \mathbf{R}_{\mathbf{W}})_2$. Для разбиений $\mathbf{W} = \{W_0,...,W_{r-1}\}$ алфавита текстов X, блоки которых являются смежными классами по некоторой подгруппе $(W_0, \otimes)$ группы $(X, \otimes)$, в теореме 5.5.1 доказывается эквивалентность между $\otimes_{\mathbf{W}}$-марковостью и существованием нетривиального подстановочного гомоморфизма алгоритма шифрования. Показано, что в общем случае класс $\otimes_{\mathbf{W}}$-марковских алгоритмов шифрования и преобразований не ограничивается только такими разбиениями. В §5.6 рассмотрены также связи между $\otimes_{\mathbf{W}}$-марковостью раундовых функций и свойствами линейных преобразований, являющихся их компонентами.

В **заключении** перечислены основные результаты диссертационной работы, указана их научная и практическая значимость.

Список литературы

[1] *Бабаш А. В., Шанкин Г. П.* Криптография / А. В. Бабаш, Г. П. Шанкин.– М.: Солон-Пресс, 2007.–512 с.

[2] *Баннаи Э., Ито Т.* Алгебраическая комбинаторика / Э. Баннаи, Т. Ито. – М.: Мир, 1987.– 373 с.

[3] Теория Галуа для классов Поста. I, II / В. Г. Боднарчук [и др.] // Кибернетика. – 1969. – Вып. 3. – С. 1–10. – Вып. 5. – С. 1 – 9.

[4] *Горшков С. П., Тарасов А. В*. О максимальных группах инвариантных преобразований мультиаффинных, биюнктивных, слабо положительных и слабо отрицательных булевых функций / С. П. Горшков, А. В. Тарасов // Дискретная математика. – 2009. – Т. 21. Вып. 2. – С. 94 – 101.

[5] *Кемени Д., Снелл Д.* Конечные цепи Маркова / Д. Кемени, Д. Снелл. – М.: Наука, 1970. – 272 с.

[6] *Клейн Ф.* Сравнительное обозрение новейших геометрических исследований («Эрлангенская программа»). // В книге: Об основаниях геометрии. Сборник классических работ по геометрии Лобачевского и развитию ее идей / Ф. Клейн. – М.: Государственное издательство технико-теоретической литературы, 1956. – С. 399 – 434.

[7] *Литвиненко В. С., Тарасов А. В.* Классы Шефера, классы Поста и соответствия Галуа / В. С. Литвиненко, А. В. Тарасов// Математические вопросы криптографии. – 2015.− Т. 6. Вып. 1. – С. 81–107.

[8] *Маслов А. С.* Об условиях порождения SA-подстановками знакопеременной группы / А. С. Маслов // Труды института математики НАН Беларуси. – 2007. – Т.15. Вып. 2. – С. 58 – 68.

[9] *Музычук М. Е.* Подсхемы схемы Хемминга. Исследования по алгебраической теории комбинаторных объектов. ВНИИ системных исследований/ М. Е. Музычук //Труды семинара.– 1985. – С. 49 − 76.

[10] *Парватов Н. Г.* Соответствие Галуа для замкнутых классов дискретных функций / Н. Г. Парватов // Прикладная дискретная математика. – 2010. – Т. 8. Вып. 2. – С. 10–15.

[11] *Поваров Г. Н.* О групповой инвариантности булевых функций / Г. Н. Поваров // В. сб. «Применение логики в науке и технике». – М.: АН СССР, 1961. – С. 263–340.

[12] *Погорелов Б. А.* Основы теории групп подстановок. Часть 1. Общие вопросы / Б. А. Погорелов.– М.: в/ч 33965, 1986. – 316 с.

[13] *Погорелов Б. А.* Подметрики метрики Хемминга и теорема А.А. Маркова / Б. А. Погорелов // Труды по дискретной математике. – 2006. –Т. 9.– С. 190 − 219.

[14] *Погорелов Б. А., Пудовкина М. А.* Натуральные метрики и их свойства. Ч.1. Подметрики и надметрики/ Б. А. Погорелов, М. А. Пудовкина // Математические вопросы криптографии. – 2011.– Т. 2. Вып. 4. – С. 49–74.

[15] *Погорелов Б. А., Пудовкина М. А.* О расстояниях от подстановок до объединения всех импримитивных групп с равными параметрами систем импримитивности / Б. А. Погорелов, М. А. Пудовкина // Дискретная математика.– 2014. – Т. 26. Вып. 1.– С. 103–117.

[16] Словарь криптографических терминов / ред. Б. А. Погорелов, В. Н. Сачков. – М: МЦНМО, 2006. – 94 с.

[17] *Токарева Н. Н.* Группа автоморфизмов множества бент-функций / Н. Н. Токарева // Дискретная математика. – 2010. – Т. 22. Вып.4. – С. 34–42.

[18] *Фомичев В. М.* Методы дискретной математики и криптологии/ В. М. Фомичев. – М.: ДИАЛОГ-МИФИ, 2010. – 424 с.

[19] *Черемушкин А. В.* Методы аффинной и линейной классификации двоичных функций / А. В. Черемушкин // Труды по дискретной математике. – 2001. – Т.4. – С. 273 – 314.

[20] *Beth T., Jungnickel D., Lenz H.* Design theory /T. Beth, D. Jungnickel, H. Lenz. – Cambridge: Cambridge University Press, 1999.

[21] *Biggs N.L., White A.T.* Permutation groups and combinatorial structures / N.L. Biggs, A.T. White. – London Math. Soc. Lect. Note Series. – V. 33. – Cambridge: Cambridge Univ. Press., 1979.

[22] PRESENT: an ultra-lightweight block cipher / A. Bogdanov [et. al.] // CHES. Lect. Notes Comp. Sci.– 2007. – V. 4727. – P. 450 – 466.

[23] *van Bon J.* Finite primitive distance-transitive graphs / J. van Bon // European Journal of Combinatorics. – 2007.– V. 28. – P. 517–532.

[24] *van Bon J. T. M., Brouwer A. E.* The distance-regular antipodal covers of classical distance-regular graphs / J. T. M. van Bon, A. E. Brouwer // Colloq. Math. Soc. János Bolyai, Proc. Eger 1987. – 1988. – P. 141 – 166.

[25] *Brouwer A. E., Cohen A. M., Neumaier A.* Distance Regular Graphs / A. E. Brouwer, A. M. Cohen, A. Neumaier. – Berlin: Springer-Verlag, 1989.

[26] *Budaghyan L., Carlet C.* On CCZ-equivalence and its use in secondary constructions of bent functions / L. Budaghyan, C. Carlet // Preproceedings of WCC'2009.– 2009.– P. 19–36.

[27] *Buekenhout F.* Diagrams for geometries and groups / F. Buekenhout// J. Combinatorial Theory (A). – V. 27. – P. 121 – 151.

[28] *Buekenhout F.* The geometry of the finite simple groups / F. Buekenhout // In: Buildings and the geometry of diagrams. Lecture Notes in Math.– 1986.– V. 1181.–P. 1–78.

[29] *Caranti A., Dalla Volta F., Sala M.* On some block ciphers and imprimitive groups [Электронный ресурс] / A. Caranti, F. Dalla Volta, M. Sala // URL: http://arxiv.org/abs/math/0806.4135 (дата обращения: 10.02.2011).

[30] *Caranti A., Dalla Volta F., Sala M.* An application of the O'Nan-Scott theorem to the group generated by the round functions of an AES-like cipher/ A. Caranti, F. Dalla Volta, M. Sala // Designs, Codes and Cryptography. – 2009. – V. 52. – P. 293–301.

[31] Atlas of finite groups. Maximal subgroups and ordinary characters for simple groups / J. H. Conway [et. al.].− Oxford: Clarendon Press, 1985.

[32] *Coppersmith D., Grossman E.* Generators for certain alternating groups with applications to cryptography/ D. Coppersmith, E. Grossman // SIAM J. Appl. Math. – 1975. – V. 29. №4. – P. 624–627.

[33] *Daeman J., Knudsen L. R., Rijmen V.* The block cipher Square / J. Daeman, L. R. Knudsen, V. Rijmen // FSE '97. Lect. Notes Comp. Sci. – 1997. – V. 1267. – P. 149 – 165.

[34] *Deza M., Deza E.* Encyclopedia of distances / M. Deza, E. Deza.– Berlin: Springer-Verlag, 2009.

[35] D.STVL.9. Ongoing Research areas in symmetric cryptography// IST-2002-507932. ECRYPT. European Network of Excellence in Cryptology. – 2008.

[36] Encyclopedia of cryptography and security/ ed. by H. C. A. van Tilborg. – New York: Springer, 2005.

[37] Investigations in Algebraic Theory of Combinatorial Objects/ed. by I. A. Faradzev [et. al.]. – Kluwer Academic Publishers, 1994.

[38] *Gorenstein D., Lyons R., Solomon R.* The classification of finite simple groups / D. Gorenstein, R. Lyons, R. Solomon. – Providence: American Mathematical Society, 1994.

[39] *Harrison M. A.* On the classification of Boolean function by the general linear and affine groups / M. A. Harrison // J. Soc. for Indust. and Appl. Math. – 1964. – V. 12. №2.– P. 285–299.

[40] *Hornauer G., Stephan W., Wernsdorf R.* Markov ciphers and alternating groups / G. Hornauer, W. Stephan, R. Wernsdorf // EuroCrypt'93. Lect. Notes Comp. Sci. – 1994. – V. 765. – P. 453–460.

[41] *Ivanov A. A.* Distance-transitive graphs and their classification / A. A. Ivanov// Investigations in algebraic theory of combinatorial objects.– Dordrecht: Kluwer, 1994.– P. 283–378.

[42] Antipodal distance-transitive covers of complete bipartite graphs/ A. A. Ivanov [et. al.] // European J. Combin.– 1997.– V.18.– P. 11–33.

[43] *Kaliski B.S.Jr., Rivest R.L., Sherman A. T.* Is the data encryption standard a group? (Results of cycling experiments on DES) / B. S. Jr. Kaliski, R. L. Rivest, A. T. Sherman // Journal of Cryptology. – 1988. – V. 1. № 1. – P. 3–36.

[44] *Lai X., Massey J. L., Murphy S.* Markov ciphers and differential cryptanalysis / X. Lai, J. L. Massey, S. Murphy // EuroCrypt'91. Lect. Notes Comp. Sci.– 1991.– V. 547. – P. 17–38.

[45] *Leander G., Minaud B., Rønjom S.* A Generic approach to invariant subspace attacks: cryptanalysis of Robin, iSCREAM and Zorro / G. Leander, B. Minaud, S. Rønjom // EuroCrypt'2015. Part I. Lect. Notes Comp. Sci.– 2015. – V. 9056. – P. 254 – 283.

[46] *Liebeck M. W., Praeger C. E., Saxl J.* On the O'Nan-Scott theorem for finite primitive permutation groups / M. W. Liebeck, C. E. Praeger, J. Saxl // J. Austral. Math. Soc. (A). – 1988. – V. 44. – P. 389 – 396.

[47] *Magliveras S. S., Memon N. D.* Algebraic properties of cryptosystem PGM / S. S. Magliveras, N. D. Memon // Journal of Cryptology. – 1992. – V. 5. – P. 167 – 184.

[48] *Massey J. L.* SAFER K-64: One year later / J. L. Massey // FSE'94. Lect. Notes Comp. Sci. –1994. – V. 1008. – P. 212 – 232.

[49] *Meier W., Staffelbach O.* Nonlinearity criteria for cryptographic functions / W. Meier, O. Staffelbach // EuroCrypt'89. Lect. Notes Comp. Sci. – 1989. –V. 434. – P. 549–562.

[50] *Moore J. H., Simmons G. J.* Cycle structure of the DES with weak and semi-weak keys / J. H. Moore, G. J. Simmons // Crypto '86. Lect. Notes Comp. Sci. – 1986 – V. 263. – P. 9 – 34.

[51] *Murphy S., Paterson K., Wild P.* A weak cipher that generates the symmetric group / S. Murphy, K. Paterson, P. Wild // Journal of Cryptology. – 1994. – V. 7. – P. 61 – 65.

[52] *Nakahara Jr. J.* 3D: a three-dimensional block cipher / Jr. J. Nakahara // CANS 2008. Lect. Notes Comp. Sci. – 2008. – V. 5339. – P. 252–267.

[53] *Neumann P. M.* The structure of finitary permutation groups / P.M. Neumann // Arch. Math. –1976. – V. 27. – P. 3 – 17.

[54] *Nyberg K., Knudsen L. R.* Provable security against differential cryptanalysis// Crypto'92. Lect. Notes Comp. Sci. –1993. –V. 740. –P. 566 – 574.

[55] *Praeger C. E.* Finite transitive permutation groups and bipartite vertex-transitive graphs / C. E. Praeger // Illinois J. Math. – 2003. – V. 47. – P. 461 – 475.

[56] *Shannon C. E.* Communication theory of secret system /C. E. Shannon // Bell System Journal.− 1949.− V. 28. − P. 656– 715.

[57] *Song B., Seberry J.* Further observations on the structure of the AES algorithm / B. Song, J. Seberry // FSE 2003. Lect. Notes Comp. Sci.– 2003. − V. 2887.− P. 223–234.

[58] *Sparr R., Wernsdorf R.* Group theoretic properties of RIJNDAEL-like ciphers / R. Sparr, R. Wernsdorf // Discrete Appl. Math. – 2008. – V. 156. №16. – P. 3139–3149.

[59] ICEBERG: An involutional cipher efficient for block encryption in reconfigurable hardware / F.-X. Standaert [et. al.] // FSE'2004. Lect. Notes Comp. Sci.– 2004. –V. 3017. – P. 279–299.

[60] Differential cryptanalysis of reduced-round ICEBERG / Y. Sun [et. al.] // AfricaCrypt'2012. Lect. Notes Comp. Sci. –2012. – V. 7374. – P. 155–171.

[61] Complementation-like and cyclic properties of AES round functions / T. Van Le [et. al.] // AES'2004. Lect. Notes Comp. Sci. – 2005. –V. 3373. – P. 128 – 141.

[62] *Wernsdorf R.* The round functions of RIJNDAEL generate the alternating group / R. Wernsdorf // FSE'2002. Lect. Notes Comp. Sci. – 2002. – V. 2365. – P. 143–148.

[63] *Wernsdorf R.* The one-round functions of the DES generate the alternating group / R. Wernsdorf // EuroCrypt'92. Lect. Notes Comp. Sci. – 1993.– V. 658. – P. 99–112.

[64] *Wielandt H.W.* Permutation groups through invariant relations and invariant functions / H.W. Wielandt. – Ohio:The Ohio State University Columbus, 1969.

[65] *Zhang L., Zhang W., Wu W.* Cryptanalysis of reduced-round SMS4 block cipher / L. Zhang, W. Zhang, W. Wu// ACISP'08. Lect. Notes Comp. Sci. – 2008.– V. 5107.– P. 216 – 229.

[66] *Zhang L., Zhang W., Wu W.* Proposition of two cipher structures/ L. Zhang, W. Zhang, W. Wu // InsCrypt'2009. Lect. Notes Comp. Sci.– 2010. – V.6151. – P. 215–229.

Публикации автора по теме диссертации:

Статьи в журналах, включенных в Перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук:

1. **Пудовкина М. А.** Невозможные разности XSL алгоритмов шифрования Фейстеля / М. А. Пудовкина // Системы высокой доступности. – 2011. – Вып. 2. – С. 28–33. – 0,66 п.л.

2. Погорелов Б. А. Натуральные метрики и их свойства. Ч. 1. Подметрики и надметрики / Б. А. Погорелов, **М. А. Пудовкина** // Математические вопросы криптографии. – 2011. – Т. 2, вып. 4. – С. 49–74. – 2,86 / 1,90 п.л.

3. Погорелов Б. А. Натуральные метрики и их свойства. Ч. 2. Метрики типа Хемминга / Б. А. Погорелов, **М. А. Пудовкина** // Математические вопросы криптографии. – 2012. – Т. 3, вып. 1. – С. 71–95. – 2,75 / 1,83 п.л.

4. Погорелов Б. А. Факторструктуры преобразований / Б. А. Погорелов, **М. А. Пудовкина** // Математические вопросы криптографии. – 2012. – Т. 3, вып. 3. – С. 81–104. – 2,64 / 1,76 п.л.

5. **Пудовкина М. А.** О классах слабых ключей обобщенной шифрсистемы PRINT / М. А. Пудовкина, Г. И. Хоруженко // Математические вопросы криптографии. – 2013. – Т. 4, вып. 2. – С. 113–125. – 1,43 / 0,72 п.л.

6. **Пудовкина М. А.** Атака на шифрсистему ГОСТ 28147-89 с 12 связанными ключами / М. А. Пудовкина, Г. И. Хоруженко // Математические вопросы криптографии. – 2013. – Т. 4, вып. 2. – С. 127–152. – 2,86 / 0,95 п.л.

7. Погорелов Б. А. Комбинаторная характеризация XL-слоев / Б. А. Погорелов, **М. А. Пудовкина** // Математические вопросы криптографии.– 2013. – Т. 4, вып. 3. – С. 99–129. – 3,41 / 2,73 п.л.

8. Погорелов Б. А. Орбитальные производные над кольцом вычетов. Часть I. Общие свойства / Б. А. Погорелов, **М. А. Пудовкина** // Математические вопросы криптографии. – 2014. – Т. 5, вып. 4. – С. 99–127. – 3,19 / 2,12 п.л.

9. Погорелов Б. А. Орбитальные производные над кольцом вычетов. Часть II. Вероятностно-комбинаторные свойства / Б. А. Погорелов, **М. А. Пудовкина** // Математические вопросы криптографии. – 2015. – Т. 6, вып. 1. – С. 117–133. – 1,87 / 1,24 п.л.

10. **Пудовкина М. А.** Об оценке числа раундов с невозможными разностями в обобщённых алгоритмах шифрования Фейстеля / М. А. Пудовкина, А. В. Токтарев// Прикладная дискретная математика. – 2015. – № 1 (27). – С. 37–51. – 1,65 / 0,82 п.л.

в том числе статьи в журнале, переводные версии которого индексируются Web of Science:

11. Погорелов Б. А. О расстояниях от подстановок до импримитивных групп при фиксированной системе импримитивности / Б. А. Погорелов, **М. А. Пудовкина** // Дискретная математика. – 2013. – Т. 25, вып. 3. – С. 78–95. – 1,98 / 1,32 п.л.

в переводной версии журнала:

Pogorelov B. On the distance from permutations to the imprimitive groups with fixed parameters of imprimitivity systems/ B. Pogorelov, **M. Pudovkina** // Discrete Mathematics and Applications. – 2014. – Vol. 24, is. 2. – P. 95–108. – DOI: 10.4213/dm1249

12. Погорелов Б. А. О расстояниях от подстановок до объединения всех импримитивных групп с равными параметрами систем импримитивности / Б. А. Погорелов, **М. А. Пудовкина** // Дискретная математика. – 2014. – Т. 26, вып. 1. – С. 103–117. – 1,65 / 1,1 п.л.

в переводной версии журнала:

Pogorelov B. On the distance from permutations to the union of all imprimitive groups with identical parameters of imprimitivity systems / B. Pogorelov, **M. Pudovkina**// Discrete Mathematics and Applications. – 2014. – Vol. 24, is. 3. – P. 163–173. – DOI: 10.4213/dm1271

13. Погорелов Б. А. Надгруппы аддитивных регулярных групп порядка 2^n кольца вычетов и векторного пространства / Б. А. Погорелов, **М. А. Пудовкина** // Дискретная математика. – 2015. – Т. 27, вып. 3. – С. 74–94. – 2,31 / 1,16 п.л. – DOI: 10.4213/dm1336.

14. Погорелов Б. А. Орбитальные производные по подгруппам и их

комбинаторно-групповые свойства / Б. А. Погорелов, **М. А. Пудовкина** // Дискретная математика. – 2015. – Т. 27, вып. 4. – С. 94–119. – 2,86 / 1,43 п.л. – DOI: 10.4213/dm1350.

Статьи в научных журналах и в приложениях к научным журналам:

15. **Пудовкина М. А.** Группы, стабилизирующие некоторые классы функций/ М. А. Пудовкина // Вестник Томского государственного университета. Приложение. – 2007. – Вып. 8. – С. 48–51. – 0,44 п.л.

16. Погорелов Б. А. Подметрики метрики Хемминга и преобразования, распространяющие искажения в заданное число раз / Б. А. Погорелов, **М. А. Пудовкина** // Труды по дискретной математике. – 2007. – Т. 10. – С. 202–238. – 4,07 / 1,35 п.л.

17. **Пудовкина М. А**. Линейные структуры групп подстановок над конечным модулем / М. А. Пудовкина // Прикладная дискретная математика. – 2008. – Т. 1, вып. 1. – С. 25–28. – 0,44 п.л.

18. **Пудовкина М. А.** Свойства некоторых алгоритмов шифрования Фейстеля относительно двух групп сплетения / М. А. Пудовкина // Прикладная дискретная математика. – 2008. – Т. 1, вып. 2. – С. 58–61. – 0,44 п.л.

19. Погорелов Б. А. Подметрики Хемминга и их группы изометрий / Б. А. Погорелов, **М. А. Пудовкина** // Труды по дискретной математике. – 2008. – Т. 11, вып. 2.– С. 147–191. – 4,95 / 3,30 п.л.

20. **Пудовкина М. А**. Оценка показателя 2-транзитивности обобщённых алгоритмов шифрования Фейстеля / М. А. Пудовкина // Прикладная дискретная математика. Приложение. – 2009. – № 1. – С. 24–26. – 0,33 п.л.

21. Погорелов Б. А. Свойства графов орбиталов надгрупп группы Джевонса / Б. А. Погорелов, **М. А. Пудовкина** // Математические вопросы криптографии. – 2010. – Т. 1, вып. 1. – С. 55–83. – 3,19 / 2,12 п.л.

22. **Пудовкина М. А**. О слабом классе алгоритмов развёртывания ключа относительно метода связанных ключей / М. А. Пудовкина // Прикладная дискретная математика. Приложение. – 2010. – № 3. – С. 27–29. – 0,33 п.л.

23. **Пудовкина М. А.** Атаки на алгоритм блочного шифрования ГОСТ 28147-89 с двумя и четырьмя связанными ключами / М. А. Пудовкина, Г. И. Хоруженко // Прикладная дискретная математика. Приложение. – 2010. – № 3. – С. 29–30. – 0,22 / 0,11 п.л.

24. **Пудовкина М. А.** Разностная атака на 6-раундов Whirlpool-подобных алгоритмов блочного шифрования / М. А. Пудовкина // Прикладная дискретная математика. Приложение. – 2010. – № 3. – С. 30–31. – 0,22 п.л.

25. Погорелов Б. А. О приближении подстановок импримитивными группами / Б. А. Погорелов, **М. А. Пудовкина**// Прикладная дискретная математика. Приложение. – 2011. – № 4. – С. 17–18. – 0,22 / 0,11 п.л.

26. **Пудовкина М. А**. О невозможных усечённых разностях XSL-алгоритмов блочного шифрования / М. А. Пудовкина // Прикладная дискретная математика. Приложение. – 2011. – № 4. – С. 38–39. – 0,22 п.л.

27. Погорелов Б. А. О комбинаторных свойствах группы, порождённой XL-слоями / Б. А. Погорелов, **М. А. Пудовкина** // Прикладная дискретная

математика. Приложение. – 2012. – № 5. – С. 22–23. – 0,22 / 0,11 п.л.

28. **Пудовкина М. А**. Структурные свойства X, S-слоёв / М. А. Пудовкина // Прикладная дискретная математика. Приложение. – 2012. – № 5. – С. 26–28. – 0,33 п.л.

29. **Пудовкина М. А.** О вероятностях r-раундовых пар разностей XSL-алгоритма блочного шифрования Маркова с приводимым линейным преобразованием / М. А. Пудовкина // Прикладная дискретная математика. Приложение. – 2014. – № 7. – С. 52–54. – 0,33 п.л.

30. Погорелов Б. А. Свойства группы, порождённой группами сдвигов векторного пространства и кольца вычетов / Б. А. Погорелов, **М. А. Пудовкина** // Прикладная дискретная математика. Приложение. – 2015. – № 8. – С. 15–16. – 0,22 / 0,11 п.л.

31. Погорелов Б. А. $\otimes_{\mathbf{W},\mathrm{ch}}$-марковские преобразования / Б. А. Погорелов, **М. А. Пудовкина** // Прикладная дискретная математика. Приложение. – 2015. – № 8. – С. 17–19. – 0,33 / 0,22 п.л.

32. Погорелов Б. А. $\otimes_{\mathbf{W},\mathrm{ch}}$-марковость и импримитивность в блочных шифрсистемах / Б. А. Погорелов, **М. А. Пудовкина** // Прикладная дискретная математика. Приложение. – 2015. – № 8. – С. 69–71. – 0,33 / 0,22 п.л.

Публикации в сборниках материалов конференций:

33. Погорелов Б. А. Аффинные преобразования, распространяющие искажения, и проблема А.А. Маркова / Б. А. Погорелов, **М. А. Пудовкина** // Проблемы безопасности и противодействия терроризму : материалы 1-й международной конференции. Москва, 02–03 ноября 2005 г. – Москва, 2006. – С. 208–215. – 0,88 / 0,59 п.л.

34. Погорелов Б. А. Метрические свойства некоторых классов функций / Б. А. Погорелов, **М. А. Пудовкина** // Проблемы безопасности и противодействия терроризму: материалы 2-й международной конференции. Москва, 25–26 октября 2006 г. – Москва, 2007. – С. 201–209. – 0,99 / 0,66 п.л.

35. **Пудовкина М. А.** Метрики сплетения симметрических групп / М. А. Пудовкина // Дискретная математика и её приложения : материалы IX международного семинара. Москва, 18–23 июня 2007 г. – Москва, 2007. – С. 454–456. – 0,33 п.л.

36. **Пудовкина М. А.** О групповых свойствах эластичных функций / М. А. Пудовкина // Методы и технические средства обеспечения безопасности информации : материалы XV Общероссийской научно-технической конференции. Санкт-Петербург, 27–29 июня 2007 г. – Санкт-Петербург, 2007. – С. 201–202. – 0,22 п.л.

37. **Пудовкина М. А.** Групповые свойства некоторых алгоритмов шифрования Фейстеля i-го типа / М. А. Пудовкина // Белорусская математическая конференция (БМК-10) : тезисы докладов 10-й международной конференции. Минск, 03–07 ноября 2008 г. – Минск, 2008. – Ч. 5. – С. 69–71. – 0,33 п.л.

38. **Пудовкина М. А**. Копредставления групп в криптографии / М. А. Пудовкина // Белорусская математическая конференция (БМК-10) : тезисы

докладов 10-й международной конференции. Минск, 03–07 ноября 2008 г. – Минск, 2008. – Ч. 5. – С. 71–73. – 0,33 п.л.

39. Погорелов Б. А. О метриках, изометричных относительно группы сдвигов / Б. А. Погорелов, **М. А. Пудовкина** // Проблемы безопасности и противодействия терроризму : материалы 4-й международной конференции. Москва, 30–31 октября 2008 г. – Москва, 2009. – С. 128−136. – 0,99 / 0,66 п.л.

40. Погорелов Б. А. Линейные структуры групп подстановок векторных пространств / Б. А. Погорелов, **М. А. Пудовкина** // Проблемы безопасности и противодействия терроризму : материалы 3-й международной конференции. Москва, 25–27 сентября 2007 г. – Москва, 2008. – С. 142–147. – 0,66 / 0,44 п.л.

41. **Пудовкина М. А.** О группе трансляций универсальной алгебры, связанной с алгоритмом шифрования NLS / М. А. Пудовкина // Discrete mathematics, algebra, and their applications (DIMA-09) : материалы международной конференции. Минск, Беларусь, 19–22 октября 2009 г. – Минск, 2009. – С. 88–90.– 0,33 п.л.

42. **Пудовкина М. А**. О групповых свойствах некоторых классов криптографических преобразований / М. А. Пудовкина // Проблемы безопасности и противодействия терроризму : материалы 5-й международной конференции. Москва, 29–30 октября 2009 г. – Москва, 2010. – Т. 2. – С. 61–67. – 0,77 п.л.

43. **Пудовкина М. А**. Одно обобщение линейных структур / М. А. Пудовкина // Дискретная математика и её приложения: материалы X международного семинара. Москва, 01–06 февраля 2010 г. – Москва, 2010. – С. 120–124. – 0,55 п.л.

44. **Pudovkina M.** Symmetry groups of some classes of cryptographic Boolean functions / M. Pudovkina // Second workshop on mathematical cryptology (WMC-08) : extended abstracts. Santander, Spain, October 23–25, 2008. – Santander, 2008. – P. 178–182. – 0,55 п.л.

45. **Pudovkina M**. Some generalized Feistel ciphers and wreath products of symmetric groups / M. Pudovkina // Second workshop on mathematical cryptology (WMC-08) : extended abstracts. Santander, Spain, October 23–25, 2008. – Santander, 2008. – P. 182–186. – 0,55 п.л.

46. **Pudovkina M**. Related-key attacks on the full GOST block cipher / M. Pudovkina, G. Khoruzhenko // West European workshop on research in cryptography (WEWoRC-2011) : abstracts of international workshop. Weimar, Germany, July 20–22, 2011. – Weimar, 2011. – P. 96–99. – 0,44 / 0,22 п.л.

47. **Pudovkina M**. Differential attack on the family of block ciphers based on the SPN structure / M. Pudovkina // Central European conference on cryptology : abstracts of the 10th international conference. Bedlewo, Poland, June 10–12, 2010. – Bedlewo, 2010. − P. 34−35. – 0,22 п.л.

48. **Pudovkina M.** Related-key attacks on the full GOST block cipher with two or four related keys / M. Pudovkina, G. Khoruzhenko // 1st International conference on Bulgarian and Balkans cryptography (BulCrypt 2012) : proceedings. Sofia, Bulgaria, September 20–21, 2012. – Sofia, 2012. – P. 107–127. – 2,3 / 1,1 п.л.

49. **Pudovkina M.** On full-round differential distinguishers for some type-2i generalized Feistel schemes / M. Pudovkina // 1st International conference on Bulgarian

and Balkans cryptography (BulCrypt 2012) : proceedings. Sofia, Bulgaria, September 20–21, 2012. – Sofia, 2012. – P. 97–106. – 1,1 п.л.

в том числе статьи в сборниках материалов конференций, индексируемых Scopus:

50. **Pudovkina M**. A related-key attack on block ciphers with weak recurrent key schedules / M. Pudovkina // Lecture Notes in Computer Science. – 2011. – Vol. 6888 : Foundations and Practice of Security (FPS'2011) : Revised Selected Papers of the 4th Canada-France MITACS Workshop. Paris, France, May 12–13, 2011. – P. 90–101. – DOI: 10.1007/978-3-642-27901-0_8. – 1,32 п.л.

51. **Pudovkina M.** Numerical semigroups and bounds on impossible differential attacks on generalized Feistel scheme / M. Pudovkina, A. Toktarev // Communications in Computer and Information Science. – 2014. – Vol. 448 : Cryptography and Security Systems (CSS'2014) : Proceedings of the Third International Conference. Lublin, Poland, September 22–24, 2014). – P. 1–11. – DOI: 10.1007/978-3-662-44893-9_1. – 1,21 / 0,60 п.л.

Подписано в печать: 31.01.2017г.
Заказ № 1558 Тираж: 100 экз.
Типография «ОПБ-Принт»
ИНН 7715893757
107078, г. Москва, Мясницкий пр-д, д. 2/1
(495) 777 33 14
www.opb-print.ru