ОТЗЫВ

официального оппонента на диссертацию
Пудовкиной Марины Александровны
«Комбинаторно-алгебраические структуры итерационных функций в системах защиты информации», представленную к защите на соискание учёной степени доктора физико-математических наук по специальности 05.13.19 - Методы и системы защиты информации, информационная безопасность (физико-математические науки)

Актуальность избранной темы.

Защита информации в различных каналах связи, включая сеть Интернет, типично обеспечивается с применением средств защиты компьютерной информации. Часть таких средств защиты возникла на базе развития и совершенствования простейших шифров (замены и перестановки), путём устранения имеющихся у последних криптографических слабостей. Один из способов заключался в увеличении размера алфавита, который реализован в шифрах многозначной замены, в кодах и в современных блочных шифрах. Современные блочные шифры используются в функциях хеширования и электронно-цифровой подписи. Они математически задаются множеством подстановок на алфавите большой мощности, которое вырабатывается некоторым алгоритмом преобразования, состоящим в реализации многих «раундов» преобразований входной информации (такие преобразования принято называть раундовыми функциями). Каждый такой раунд шифрования моделируется раундовой функцией, а их композиция называется итерационной функцией зашифрования. При этом применение известных методов анализа итерационных функций и разработка новых функций основываются на структурных свойствах раундовых функций. Таким образом, разработка новых методов и усовершенствование известных методов анализа структурных свойств итерационных функций, безусловно, является актуальной и важной научной проблемой. Диссертационная работа Пудовкиной М.А. посвящена решению этой проблемы.

Содержание работы.

Диссертация Пудовкиной Марины Александровны структурно состоит из введения, пяти глав, заключения и приложения, в котором собраны копии актов о внедрении результатов её научной работы. Во введении описана

общая постановка задач исследования, обоснована их актуальность и выполнен достаточно подробный обзор научных результатов, связанных с темой диссертации.

В работе выделен класс структур, названных p_G-структурами итерационных функций, задаваемых через множества t-грамм алфавита текста и представляющих интерес, в том числе и для функций хеширования, Базовые принципы некоторых известных методов анализа изложены соискателем, на введенном языке p_G-структур.

Первая глава посвящена p_G-структурам, заданным разбиением W алфавита текстов на равномощные блоки. Группа автоморфизмов этих p_G-структур суть группа подстановок, совпадающая со сплетением симметрических групп и сохраняющая разбиение W.

Алгоритм блочного шифрования естественно моделируется перестановочным автоматом (частичные функции переходов автомат – взаимно однозначные отображения). Ряд методов анализа основан на наличии нетривиального гомоморфного образа соответствующего перестановочного автомата. Существование такого нетривиального гомоморфизма означает импримитивность группы, порожденной всеми частичными функциями автомата, а потому она является подгруппой некоторого сплетения симметрических групп. Таким перестановочным автоматам естественно сопоставляются p_G-структуры (системы импримитивности). Однако гомоморфный образ у большинства перестановочных автоматов, применяемых при построении функции хеширования, является тривиальным. Поэтому в методах анализа можно рекомендовать использовать вероятностные гомоморфизмы перестановочных автоматов (автоматов, у которых переход блоков определен с некоторыми вероятностями). На этом языке в диссертации дана интерпретация вариаций разностного метода. Для оценки вероятности наилучшего вероятностного подстановочного гомоморфизма соискателем вводится параметр $\chi_W(g)$, отражающий Хэммингову близость подстановки g ко всем подстановкам, сохраняющим разбиение W. Одним из основных результатов практических результатов первой главы является получение нижних и верхних оценок параметра $\chi_W(g)$ для заданного разбиения W алфавита текста. При этом описаны все подстановки с достижимой верхней оценкой. Роль этих подстановок очень схожа с ролью бент-функций относительно множества всех аффинных функций.

Для построения p_G-структур множества подстановок G во второй главе исследуются класс метрик, все значения которых являются элементами множества $\{0,\ldots,d\}$. В работе такие метрики названы натуральными. Они

возникают в дискретной математике, например, метрики связных графов с конечным множеством вершин. Основное внимание уделено характеризации метрик, которые по своим свойствам близки к метрике Хэмминга на пространстве $[GF(2)]^n$. Так, выполнена полная классификация всех подметрик метрики Хэмминга на пространстве $[GF(2)]^n$ при $n \geq 4$. Именно, каждая подметрика является метрикой графа орбитала надгруппы группы Джевонса (группы изометрий метрики Хэмминга на пространстве $[GF(2)]^n$).

В третьей главе получена полная классификация групп изометрий подметрик метрики Хэмминга на $[GF(2)]^n$. Также идентифицированы дистанционно-транзитивные графы, задаваемые подметриками метрики Хэмминга, среди которых выявлены примитивные, двудольные и антиподальные графы.

Классификация подметрик метрики Хэмминга и классификация их групп изометрий в главах 2, 3 диссертационной работы, относятся к многочисленным результатам, инициированных результатом А.А. Маркова, полученным в 1956 г., о биективных преобразованиях множества слов Ω^* в конечном алфавите Ω, сохраняющих длину слов и не увеличивающих метрику Хэмминга между словами одной длины. Результат А.А. Маркова направлен на описание шифров, не размножающих искажения типа замены буквы в словах. Различными вариациями, рассмотренной А.А. Марковым задачи и вытекающими из неё проблемами, занимались в разное время многие представители отечественной криптографической школы, в том числе М.М. Глухов, Г.П. Шанкин, Б.А. Погорелов и оппонентом.

В четвертой главе указывается связь между приводимостью матрицы линейного преобразования AES-подобного алгоритма блочного шифрования и свойствами его p_G-структуры. Описаны свойства графов, группа автоморфизмов которых порождена приводимой обратимой матрицей и подстановочным представлением группы сдвигов пространства $[GF(2)]^n$. В качестве приложения результатов главы четыре конкретизированы для алгоритма блочного шифрования ISEBERG.

В пятой главе даются практические приложения, полученных результатов выше по p_G-структурам для основных класса приложений: \

1) класса алгоритмов, основанных на модификации схемы Фейстеля 2-го типа;

2) алгоритмы блочного шифрования с возможностью их моделирования так называемой цепью Маркова с дальнейшим укрупнением ее состояний.

В первом классе алгоритмов соискателем представлена p_G-структура, сохраняемая каждым используемым раундовым ключом. Это свойство

позволяет строить статистические критерии для определения раундового ключа.

Второй класс алгоритмов используются разности между парами текстов (открытых и шифрованных). Для некоторых алгоритмов этого класса соискателем удалось указать p_G-структуру, соответствующую укрупненной цепи Маркова. Указаны теоретико-автоматные модели так называемых AES-подобных алгоритмов блочного шифрования, для которых данное укрупнение существует тогда и только тогда, когда этот данный автомат имеет гомоморфный образ с меньшим числом состояний.

В заключении рассматриваемой диссертации приведены основные результаты, указана их научная и практическая значимость.

Степень обоснованности и достоверность научных результатов, положений и выводов, сформулированных в диссертации.

Все научные результаты и положения, сформулированные в диссертации, строго обоснованы, а их достоверность подтверждается строгими математическими доказательствами, а также, состоявшимися публикациями в авторитетных реферируемых научных изданиях (Труды по дискретной математики, Математические вопросы криптографии, Дискретная математика, Прикладная математика). Кроме того, ряд результатов обобщает или исправляет известные ранее (см., теорема 3.5.1 и раздел 5.3).

Научная новизна и практическая значимость

Диссертационная работа Пудовкиной М.А. содержит новые научные результаты в области разработки методов исследования и описания структурных свойств итерационных криптографических функций. Полученные результаты могут быть применены при анализе систем защиты информации, в которых используются итерационные алгоритмы блочного шифрования, для поиска возможных уязвимостей, основанных на наличие различных нетривиальных потенциально опасных p_G-структур. Для этого в диссертации:

1) разработан общий способ поиска и построения p_G-структур, обусловленных комбинаторно-алгебраическими свойствами преобразований, составляющих итерационную криптографическую функцию;

2) описано влияния свойств отдельных преобразований, составляющих функцию зашифрования, на существование различных потенциально опасных p_G-структур (главы 1, 4, 5);
3) разработан способ анализа XSL-алгоритмов блочного шифрования, использующего инвариантные подпространства линейного преобразования и обобщающего разностный метод (глава 4).

Результаты диссертационной работы внедрены в ООО «Специальный технологический центр», АО «МакроСистемы», а также на кафедре «Информационная безопасность» МГТУ им. Н.Э. Баумана.

Замечания по диссертационной работе и автореферату.

1. В разделе 1.3 введён параметр χ_W, характеризующий расстояние от подстановки g до максимальной импримитивной группы IG_W, сохраняющей разбиение W с равномощными блоками. Интересно было бы: а) описать класс подстановок из IG_W, находящихся на минимальном расстоянии Хэмминга от подстановки g, и сравнить данное минимальное расстояние с величиной $\chi_W(g)$; б) для класса XSL-алгоритмов блочного шифрования и разбиения W, описанных в следствие 1.3.9, построить такую приближенную автоматную модель, что группа, порождённая всеми её частичными функциями, являлась подгруппой группы IG_W, а также сравнить на одном произвольном ключе расстояние между частичными функциями приближенно автоматной модели и функцими зашифрования.
2. В диссертационной работе на стр. 91 сказано, что «при $n<9$ в формулировке теоремы 2.6.1 уменьшается число случаев двух списках из-за изоморфизма». Для полноты изложения хорошо было бы указать совпадающие случаи для малых n, $n<9$.
3. В диссертационной работе используется много понятий из различных областей математики, зачастую известные только работающим в этой области специалистам. Хотя необходимые понятия приводятся по тексту диссертационной работы, но наличие предметного указателя значительно бы облегчило чтение диссертации.
4. В диссертационной работе и автореферате имеются опечатки и стилистические неточности (стр. 67, 130, 180, 181 и т.д.). Так, на стр. 19 автореферата сказано, что «группа совпадает со сплетением или прямым произведением», но из формулировки теоремы 3.2.1 диссертационной работы (см. табл. 3.2.1), а также введения 3.1 следует, что должно быть «группа совпадает со сплетением или полупрямым произведением».

6. Диссертационная работа перегружена избыточной информацией, в том числе и обзорного характера, например, в общем введении в работу (стр. 11, 12), а также в введениях к главе 1 (стр. 27, 28), главе 2 (стр. 58-60), главе 5 (стр. 217).
7. По тексту диссертационной работы не всегда присутствуют явные ссылки на публикации соискателя, в которых опубликованы приведённые в диссертационной работе результаты соискателя.
8. Диссертационная работа плохо структурирована. Четко не выделены главные результаты в каждой главе работы.
9. Неформальное использование понятия «случайная подстановка» (стр. 216).
10. Отсутствуют ссылки на описание функционирования упоминаемых в работе некоторых алгоритмов шифрования, например, ARIA, Camellia, MIBS (стр. 179), SAFER (стр. 207), CAST-256, MARS, SMS4, CLEFIA, Piccolo, HIGHT (стр. 216), Grindahl (стр. 222).

Указанные замечания уменьшают общее благоприятное впечатление от работы и её значимость. Тем не менее, полученные научные результаты, их изложение ясным и строгим языком, их актуальность и новизна достаточна для рекомендации присуждения Пудовкиной М.А. учёной степени доктора физико-математических наук.

Трудность оппонирования диссертаций по направлению 05.13.19 всем известна. Она заключается в размежевании неотъемлемой части защиты информации – криптографии от собственно защиты информации. А трудность любого соискателя по данной дисциплине удовлетворить требованиям оппонента и положениям ВАКа. По мнению оппонента Пудовкиной М.А. удалась в оформить текст диссертации в рамках требования ВАКа.

Общее заключение. Диссертационная работа является законченной научно-исследовательской работой, посвященной актуальной научной проблеме разработки и развития методов исследования комбинаторно-алгебраических структур итерационных функций в системах защиты информации. Работа отличается научной новизной и достаточной практической значимостью полученных результатов.

Материалы исследования полно отражены в публикациях автора и неоднократно докладывались на научных конференциях и семинарах различного уровня. Автореферат полно и точно отражает содержание диссертации. Высокий научный уровень диссертации подтверждается

регулярным включением результатов в отчеты по темам Академии криптографии РФ в 2005 – 2016 гг.

На основании вышесказанного считаю, что диссертация Марины Александровны Пудовкиной «Комбинаторно-алгебраические структуры итерационных функций в системах защиты информации» полностью соответствует критериям, установленным «Положением о присуждении ученых степеней», и удовлетворяет всем требованиям ВАК, предъявляемым к диссертациям на соискание учёной степени доктора физико-математических наук по специальности 05.13.19 - Методы и системы защиты информации, информационная безопасность, а сама Пудовкина Марина Александровна заслуживает присуждения ей учёной степени доктора физико-математических наук по данной специальности.

Официальный оппонент:
доктор физико-математических наук, профессор,
специальность 20.03.04
(информация о наименовании специальности закрыта)
профессор кафедры информационной безопасности
ФГАОУВО Национального исследовательского университета
«Высшая школа экономики»

Бабаш Александр Владимирович

18 апреля 2017 г.

Подпись заверяю
специалист по кадрам
1 категории Коневская
18.04.2017

Федеральное государственное автономное образовательное учреждение высшего образования федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет «Высшая школа экономики»

101000, г. Москва, ул. Мясницкая, 20,
Тел: +7 (495) 7713232;
e-mail: hse@hse.ru;
http://www.hse.ru