Отзыв официального оппонента на диссертацию
Пудовкиной Марины Александровны
«Комбинаторно-алгебраические структуры итерационных функций в системах защиты информации», представленной на соискание ученой степени доктора физико-математических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность

Актуальность выбранной темы

Диссертационная работа посвящена исследованию структур, определяемых алгебраическими и комбинаторными свойствами итерационных преобразований, которые являются основной составляющей многих средств защиты информации, в том числе функций хэширования, алгоритмов аутентификации и алгоритмов блочного шифрования.

В данной диссертационной работе в основном автор уделяет внимание структурам, которые могут быть представлены в виде пары разбиений, где блоки первого разбиения характеризуют связи между словами открытого текста, а блоки второго разбиения – между соответствующими словами шифртекста. Особое внимание уделяется биграммам, изучаются p_G-структуры на основе соответствующих матриц вероятностей.

Исследование ведётся по трём направления: построение структуры и нахождение степени её сохранения данным множеством преобразований, а также вычисление расстояний между преобразованиями из этого множества и элементами группы автоморфизмов относительно некоторой метрики. Эти направления исследования современных средств защиты информации, составляющие которых моделируются итерационными функциями, в том числе и основывающихся на XSL-алгоритмах блочного шифрования, определяют актуальность и структуру диссертации, которая состоит из введения, пяти глав и заключения. В приложении помещены акты о внедрении работы.

В **главе 1** рассматриваются p_G-структуры, задающиеся разбиениями с равномощными блоками алфавита текстов, и описывается их связь со сплетением групп подстановок, что обобщает понятие линейной структуры и бент-функций. Показано, что в разностном методе и его обобщениях, а также в методе гомоморфизмов, возникает задача оценки расстояния от множества подстановок до некоторых импримитивных групп. Подробно рассмотрены конкретные важные примеры оценки и вычисления этого расстояния, в том числе для алгоритма блочного шифрования SMS4.

Глава 2 посвящена двумерным p_G-структурам, которые задаются метриками, значения расстояний которых – натуральные числа (и нуль). Изучаются канонические и натуральные метрики, обобщающие метрики связного графа, задающиеся кратчайшим расстоянием между его вершинами. Введены важные понятия подметрик и надметрик натуральных метрик, описаны их свойства. Изучены два класса натуральных метрик, близких по своим свойствам к метрике Хэмминга на множестве битовых строк – инвариантные относительно подстановочного представления группы сдвигов и инвариантные относительно группы Джевонса. Для второго класса получено полное описание всех его представителей на основе описания всех орбиталов надгрупп группы Джевонса.

В **главе 3** рассматриваются метрики из этого второго класса и описываются их группы изометрий. Рассматриваются свойства графов, соответствующих орбиталам надгрупп группы Джевонса. При этом возникают интересные классы графов, в том числе дистанционно транзитивные, антиподальные и двудольные. Полученные результаты актуальны в связи с наблюдающимся в настоящее время взаимным проникновением методов алгебры, теории групп подстановок и теории графов. Автор квалифицированно показывает это проникновение с точки зрения приложений к защите информации.

Глава 4 посвящена описанию того, как влияет приводимость матрицы линейного слоя алгоритма блочного шифрования на свойства одномерных и двумерных p_G -структур, что считается важной актуальной проблемой, так как может влиять на криптографические свойства всего алгоритма и быть причиной существования атак на алгоритмы блочного шифрования. Рассматриваются свойства графов орбиталов группы, порождённой действием приводимой матрицей и преобразованиями-сдвигами векторного пространства, и описываются натуральные метрики этих орбиталов, а также условия дистанционной транзитивности графов орбиталов этой группы (в двух важных случаях). Изучены свойства марковских XSL-алгоритмов блочного шифрования с приводимым линейным преобразованием.

В **главе 5** рассматриваются криптографические приложения одномерных и двумерных p_G -структур: к модифицированному алгоритму Фейстеля и к марковским итерационным алгоритмам. Приведён интересный пример того, как «улучшение» конструкции «хорошим» криптографическим преобразованием, а именно – матрицей с наибольшим среди всех матриц из GL_4 коэффициентом рассеивания, приводит к слабому семейству алгоритмов

шифрования. Для марковских алгоритмов предложено применить теорию таких цепей Маркова, укрупнению состояний которых опять соответствует цепь Маркова. При этом марковость соответствующей последовательности случайных величин может сводиться к свойствам s-боксов и преобразования линейного слоя. Приведены примеры. Поскольку APN-подстановки считаются оптимальными для использования в качестве s-боксов, они также подвергнуты изучению с этой точки зрения. Рассмотрены также связи между марковостью алгоритмов блочного шифрования, методом гомоморфизмов и существованием двумерной p_G-структуры.

В **заключении** перечислены результаты диссертационной работы, выносимые на защиту, показана их научная и практическая значимость.

Новизна полученных результатов, выводов и рекомендаций

В диссертации получены следующие новые научные результаты:

- показана связь комбинаторно-алгебраических свойств итерационных криптографических преобразований с наличием структур, позволяющим проведение известных и новых атак.

- предложен и обоснован оригинальный метод описания и изучения свойств структур как некоторых разбиений t-грамм в алфавите открытого и шифрованного текста.

- изучены свойства групп подстановок, порождённых множествами преобразований, составляющих итерационную криптографическую функцию, в том числе описаны линейные преобразования, у которых одна из метрик графов орбиталов изоморфна метрике Хэмминга.

- разработан метод натурально-значных метрик, полностью классифицированы метрики типа Хэмминга, группа изометрий которых является надгруппой группы Джевонса, некоторые ранее известные графы реализованы как графы орбиталов надгрупп группы Джевонса.

- предложено новое математическое понятие L-факторструктуры преобразования и описана группа её автоморфизмов.

- описана группа инерции множества всех корреляционно-иммунных функций данного порядка.

- описаны подстановки, максимально далекие от сплетения групп подстановок при заданной системе импримитивности, которые являются, таким образом, аналогом максимально нелинейных функций.

- для обобщений алгоритма Фейстеля и марковских моделей алгоритмов блочного шифрования найдена p_G-структура, позволяющая провести фундаментальную атаку различением.

- для класса марковских алгоритмов блочного шифрования доказана эквивалентность между $\otimes$w -марковостью и существованием нетривиального подстановочного гомоморфизма.

Достоверность основных положений, выводов и рекомендаций подтверждается строгим использованием математического аппарата, включающего алгебраические и комбинаторные методы теории групп (в том числе групп подстановок), теории графов, метрических пространств, линейной алгебры над конечными полями. Все результаты логически обоснованы на современном уровне математической строгости.

Теоретическое и практическое значение работы

1. Разработанные в диссертации методы позволяют существенно расширить способы поиска и построения структур для новых методов анализа на основе изучения свойств преобразований XSL-слоёв, классификации соответствующих групп, графов и метрик.

2. Предложенный в диссертации подход решает важную научную проблему поиска и построения структур итерационных функций в системах защиты информации и открывает перспективы, в том числе и их криптографического применения.

3. Предложенные в работе математические модели могут быть применены для анализа уязвимостей современных средств защиты информации, основанных на XSL-алгоритмах блочного шифрования.

Использование результатов работы.

Результаты работы могут быть практически использованы в приложениях, в том числе и криптографических, теории защиты информации для построения, исследования и оптимизации математических моделей реальных систем защиты информации.

Замечания по работе. Существенных замечаний по диссертации не имеется. Из замечаний отмечу следующие.

1. В стандарте ГОСТ Р 34.11-2012 «Стрибог» дано написание терминов «функция хэширования» и «хэш- функция» через «э»; в диссертации же используется написание через «е» (см., например, с. 6).

2. Встречаются не вполне согласованные предложения (см., например, с. 11, 14, 17, 18, 22).

3. Имеются некоторые отклонения в обозначениях (см., например, с .9, 13, 50).

4. Очень неудачные примеры на с. 49 и 50 (видимо, допущена арифметическая ошибка): на с. 49 сумма элементов матрицы подстановки равна 45 и не равна сумме максимумов строк 48 (в работе указано значение 44), аналогично – на с. 50. Причина: в строках 5,6 и 7 матрицы на с. 49 максимальное значение достигается в одном и том же столбце номер два, а на с. 50 в строках 2 и 8 максимальные значения достигаются в столбце номер 15, а также в строках 0 и 13 максимальное значение достигается только в столбце номер 7. Поэтому подстановочного остова не существует.

Эти замечания не снижают общего положительного впечатления о диссертационной работе, которая может быть положена в основу монографии с включением примеров и приложений, в том числе к классическим задачам, не рассмотренным в диссертации, например – к максимально нелинейным функциям в случае нечётной размерности.

Общее заключение. Диссертационная работа Пудовкиной Марины Александровны «Комбинаторно-алгебраические структуры итерационных функций в системах защиты информации» является законченной научно-исследовательской работой, посвященной решению научной проблемы анализа уязвимостей современных средств защиты информации, составляющие которых моделируются итерационными функциями, на основе описания структур компонент этих функций и структур функций в целом. Совокупность представленных в ней результатов можно классифицировать как новое решение этой актуальной научной проблемы. Основное содержание диссертации достаточно полно отражено в печатных изданиях высокого уровня, основные результаты апробированы на представительных международных и всероссийских конференциях, доклады М. А. Пудовкиной на которых, как я могу свидетельствовать, всегда вызывали большой интерес. Автореферат правильно и в достаточной мере отражает содержание диссертационной работы, соответствует ей.

На основании вышесказанного считаю, что диссертационная работа Пудовкиной М. А. удовлетворяет требованиям ВАК, предъявляемым к докторским диссертациям по физико-математическим наукам по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность, а ее автор, Пудовкина Марина Александровна, заслуживает присуждения ей ученой степени доктора физико-математических наук по этой специальности.

Официальный оппонент –
доктор физико-математических наук,
профессор,
(специальность 01.01.02 – Дифференциальные уравнения)
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Уральский государственный университет путей сообщения»,
главный научный сотрудник
кафедры «Информационные технологии и
защита информации»
Титов Сергей Сергеевич
620034, г. Екатеринбург, ул. Колмогорова, 66;
rector@usurt.ru; www.usurt.ru
Тел. (343)2212444
e-mail: stitov@usaaa.ru

С.С. Титов
11 апреля 2017 г.

Подпись профессора Титова Сергея Сергеевича заверяю:

Ученый секретарь УрГУПС Т.И. Бушуева