Отзыв научного консультанта
на диссертационную работу Пудовкиной Марины Александровны
«Комбинаторно-алгебраические структуры итерационных функций
в системах защиты информации» по специальности 05.13.19 –
Методы и системы защиты информации, информационная безопасность
на соискание учёной степени доктора физико-математических наук

Исходя из теоретико-сложностной модели стойкости шифрсистем, множество G всех частичных функций зашифрования (подстановок на алфавите X блоков текста) алгоритма блочного шифрования не должно быть различимо алгоритмами рассматриваемой модели от множества всех подстановок симметрической группы $S(X)$ при равномерном распределении на множестве и всей симметрической группе. В частности, множество G «в среднем» не должно сохранять никакие комбинаторно-алгебраические структуры, заданные на множестве X^t (эффективно вычислимые в той же модели), группа автоморфизмов такой структуры не должна «коррелировать» с множеством G. Отмечу, что в 1878 году Ф. Клейн в своей программе, позже названной Эрлагенской, продолжая идеи Э. Галуа, указал на необходимость изучать геометрии вместе с их группами автоморфизмов. Такой подход позволил Ф. Клейну объединить различные разделы геометрии через группы преобразований. В 80-е годы прошлого века в теории групп появились два результата (классификация конечных простых групп и теорема О'Нэна-Скотта о классификации примитивных групп), говорящие о том, что возможностей для классов групп автоморфизмов различных структур в некотором смысле меньше, чем можно было предположить ранее. Одновременно появилась возможность выделить и сопоставить группы и структуры. С точки зрения этих классификационных результатов основным классам групп подстановок можно сопоставить, прежде всего, следующие комбинаторно-групповые структуры: орбиты, системы импримитивности, метрики графов орбиталов, тройки векторов ранга два и некоторые другие, соответствующие простым группам. Собственно в теории групп подстановок применяется метод инвариантных отношений, основанный на описании свойств орбит на t-граммах множества X и опирающейся на идеи Г. Виланда. Данный метод впоследствии развивался научной школой Л.А. Калужнина в 80-е и 90-е годы прошлого века в Киеве.

В криптографии возникают следующие структуры: системы импримитивности, разности, усеченные разности, гиперплоскости в линейном методе, метрики в регистровых алгоритмах блочного шифрования и т.д.

В настоящее время все в большем числе работ неявно, а иногда и явно, используются структуры криптографических функций, определяемые их групповыми свойствами. В связи с криптоанализом блочных XSL-шифрсистем

немало работ посвящено структурам группы G_{XS}, порожденной группой наложения ключа и нелинейным перемешивающим преобразованием, с точки зрения рассеивания их линейным раундовым преобразованием. С позиций линейного и разностного методов даже сформировалось направление максимально рассеивающих матриц. Однако это касалось действия преобразований лишь в исходном базисе, а структурами, прежде всего, были множества пар элементов (блоков текста) из X с одинаковыми разностями.

Вместе с тем, систематично и с общих позиций структуры в криптографии не рассматривались. Например, группа G_{XL}, порожденная группой наложения ключа и линейным преобразованием, может обладать своими структурами, связанными с приводимостью рассеивающего линейного преобразования. Эти структуры должны рассеиваться уже нелинейным перемешивающим преобразованием. Подобная симметричная ситуация не рассматривалась и соответствующие требования к нелинейным перемешивающим преобразования не предъявлялись. В связи с этим важным является разработка общего направления, связанного со способами построения и исследования комбинаторно-алгебраических структур, возникающих в раундовых преобразованиях блочных шифрсистем и их последующим рассеиванием.

В диссертационной работе М. А. Пудовкиной решена актуальная научная проблема, связанная с разработкой общего комбинаторно-алгебраического направления по описанию структур раундовых преобразованием и рассеиванием их итерационными криптографическими функциями. В рамках решения этой проблемы введено понятие p_G-структуры для множества G криптографических функций (подстановок), унифицирующее и обобщающее целый ряд подходов к описанию свойств основных классов алгоритмов блочного шифрования. p_G-структура задается разбиениями множества X^t с ограничениями на вероятности перехода подмножеств и связана с групповыми свойствами раундовых преобразований.

Исследование p_G-структур множества G ведётся в трёх направлениях: 1) построение p_G-структур; 2) нахождение степени сохранения p_G-структуры множеством G; 3) нахождение расстояний относительно некоторой метрики между преобразованиями из множества G и элементами группы автоморфизмов p_G-структуры. Следование данным направлениям при задании и описании свойств p_G-структур приводит к постановке и решению различных задач, актуальных как для дискретной математики в целом так и для криптографии.

Исходя из классификации максимальных подгрупп симметрической группы, основные структуры связаны с системами импримитивности (импримитивные группы), с аффинностью (подгруппы аффинной группы), с метриками и графами орбиталов (унипримитивные группы). Подобные структуры

и рассматриваются в диссертации.

Вводится понятие L-факторструктуры множества подстановок, обобщающее понятие «линейной структуры». Показано, что группой автоморфизмов ряда p_G-структур, в частности, L-факторструктур, являются сплетения групп подстановок. В частности, в связи с этим в диссертационной работе рассматривается расстояние между подстановками и сплетением групп подстановок. В рамках этого подхода описаны подстановки, максимально далекие от сплетения групп подстановок при заданной системе импримитивности, которые можно считать аналогом бент-функций, т.е. функций, максимально далёких от аффинных функций.

Значительная часть диссертационной работы посвящена исследованию свойств p_G-структур, заданных натурально-значными метриками. Выбор натурально-значной метрики как способа задания p_G-структур является естественным для современной математики. В рамках этого в диссертационной работе описываются общие свойства натурально-значных метрик, а также выделяется класс натурально-значных метрик типа метрики Хемминга, представляющих интерес для криптографических приложений, теории кодирования, дискретных функций и др. Первоначально метрики, обобщающие метрику Хемминга, возникли при классификации аффинных надгрупп группы Джевонса $A\tilde{S}_n$, порождённой группой сдвигов n-мерного векторного пространства V_n над полем $GF(2)$ и группой подстановочных $(n\times n)$-матриц $\tilde{S}_n$ над полем $GF(2)$. В свою очередь, каждая надгруппа G задаёт графы орбиталов, «естественными» метриками которых являются подметрики метрики Хемминга. В связи с этим в диссертационной работе изучаются графы орбиталов надгрупп группы Джевонса и описываются их «естественные» метрики. В рамках этого получена полная классификация их групп изометрий, использование которой позволило выявить графы орбиталов, принадлежащие к таким известным классам как дистанционно транзитивные, антиподальные и двудольные. М.А. Пудовкиной проведена классификация дистанционно транзитивных графов орбиталов надгрупп группы Джевонса и рассмотрена связь с известными классами дистанционно транзитивных графов, полученных иными методами.

М.А. Пудовкиной исследуется влияния приводимости матрицы линейного преобразования XSL-алгоритма блочного шифрования на свойства одномерных и двумерных p_G-структур. Для этого рассматриваются свойства группы G_{XL}. В терминах характеристического или минимального многочленов линейного преобразования L-слоя приведены условия связности графов орбиталов, их изоморфизма, примитивности и 2-транзитививности группы G_{XL}, а также условия дистанционной транзитивности её графов орбиталов. Исследуются свойства марковских XSL-алгоритмов блочного шифрования с приводимым линейным

преобразованием. В рамках этого предложен подход, основанный применение последовательности смежных классов инвариантного подпространства линейного преобразования L-слоя, для нахождения вероятности r-раундовой разностной характеристики. Приведённый подход в ряде случаев эффективнее по сравнению со способом нахождения вероятностей «классических» разностных характеристик, что проиллюстрировано на примере инволютивного алгоритма блочного шифрования ISEBERG.

В связи с оценкой скорости рассеивания в диссертационной работе на базе вероятностных автоматов дана интерпретация и обобщение на ряд структур широко известных результатов Лея и Месси о марковости алгоритмов блочного шифрования в терминах укрупнений состояний цепи Маркова. Так, М.А. Пудовкиной рассматривается последовательность случайных величин $\xi^{(0)}, \xi^{(1)}, \ldots, \xi^{(l)}$, соответствующую биграммам промежуточных текстов из множества X^2, и её дальнейшие укрупнения $\xi_{\mathbf{W}}^{(0)}$, $\xi_{\mathbf{W}}^{(1)}, \ldots, \xi_{\mathbf{W}}^{(l)}$ посредством разбиения $\mathbf{W}$ множества X. Для этого введены понятия $\otimes_{\mathbf{W}}$-марковского алгоритма блочного шифрования и $\otimes_{\mathbf{W}}$-марковского преобразования. Даны условия $\otimes_{\mathbf{W}}$-марковости некоторых классов преобразований. Описана связь между $\otimes_{\mathbf{W}}$-марковостью алгоритмов блочного шифрования и методом гомоморфизмов для некоторых классов разбиений $\mathbf{W}$. Рассмотрены также связи между $\otimes_{\mathbf{W}}$-марковостью раундовых функций и свойствами линейных преобразований, являющихся их компонентами.

Кроме этого, в диссертационной работе описаны p_G-структуры семейства обобщённых алгоритмов Фейстеля 2-го типа, что позволило отличить данное семейство от множества равномерно распределённых случайных подстановок.

М. А. Пудовкина защитила диссертацию на соискание учёной степени кандидата физико-математических наук по специальности 05.13.19 в 2004 г. в Московском инженерно-физическом институте (государственном университете).

М. А. Пудовкина работает в должности доцента в МГТУ им. Н.Э. Баумана на кафедре «Информационная безопасность» и в НИЯУ МИФИ на кафедре криптологии и дискретной математики, где преподаёт общематематические и криптографические дисциплины, является научным руководителем выпускных работ специалистов и магистров, а также научных исследований аспирантов кафедры криптологии и дискретной математики НИЯУ МИФИ.

Этапы диссертационного исследования регулярно обсуждалась на научных конференциях и семинарах различного уровня, в том числе в Институте криптографии, связи и информатики Академии ФСБ России, МГУ им. М.В. Ломоносова и ИММ УрО РАН (г. Екатеринбург). Значительная часть результатов, представленных в диссертации, получена во время выполнения различных

научных тем Академии криптографии РФ. Все результаты, приведённые в диссертационной работе, получены лично соискателем.

В целом, М. А. Пудовкина проявила себя ученым, способным самостоятельно решать важные научные задачи, а её диссертационная работа, на мой взгляд, является целостной и завершенной научно-квалификационной работой.

Считаю, что диссертационная работа соответствует требованиям, предъявляемым к докторским диссертациям по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность (физико-математические науки), а сама Марина Александровна Пудовкина заслуживает присуждения ученой степени доктора физико-математических наук.

Научный консультант
информация о занимаемой должности закрыта,
действительный член Академии криптографии Российской Федерации,
Заслуженный деятель науки Российской Федерации,
доктор физико-математических наук по специальности 20.03.04
(информация о наименовании специальности закрыта),
профессор _____ Погорелов Борис Александрович

27 . 06 .2016 г.

Подпись заверяется по месту назначения научным консультантом:
Полное наименование организации: Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)».
Почтовый адрес: 105005, Москва, 2-я Бауманская ул., д. 5, стр. 1.
Телефон: (499) 263-6391
Адрес электронной почты: bauman@bmstu.ru.
Адрес официального сайта организации: http://www.bmstu.ru.

Подпись Б.А. Погорелова заверяю:

Руководитель научно-учебного комплекса
«Информатика и системы управления»,
заведующий кафедрой «Информационная безопасность»,
Заслуженный деятель науки Российской Федерации,
доктор технических наук,
профессор _____ В.А. Матвеев