ОТЗЫВ

на автореферат диссертации 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.

В современном мире без применения математических методов практически невозможно разработать на должном уровне решения многих проблем, возникающих при защите информации. Так, на основе математических методов проводится оценка защищенности информации, в том числе и оценка стойкости используемых в средствах защиты информации криптографических преобразований. На развитие математических методов защиты информации большое влияние оказала работа К.Э. Шеннон 1949 г., в которой он опубликовал основные положения современной теоретической криптографии, а также посредством формальной вероятностной модели дал определение совершенно стойкого шифра и привел пример (в настоящее время его естественное обобщение известно как шифр Вернама по модулю m). Однако практическое применение совершенно стойких шифров для защиты больших объемов информации требует значительных затрат, вызванных изготовлением, распределением, хранением и уничтожением ключевых материалов. Поэтому повсеместно используются практически стойкие шифры, которые обеспечивают надежную защиту, удобны с точки зрения технической реализации и эксплуатации. В настоящее время многие такие шифры, типичным представителем которых являются блочные шифры (фактически задаваемые множеством зависящих от ключа специальных подстановок), стараются разработать таким образом, чтобы их характеристики были близки к характеристикам множества случайных подстановок. Однако осуществить это разработчикам не всегда удаётся. Поэтому многие методы анализа основаны на наличие у подстановок шифра особого свойства (называемого в диссертации структурой), которое может позволить отличить их от случайных подстановок. Соответственно, возникает проблема глубокого анализа математических свойств специального класса подстановок. Как итог мы имеем задачи комбинаторно-алгебраического характера, заключающиеся в классификации свойств подстановок с выделением особенностей, представляющих ценность для математических методов защиты информации, в том числе криптографии. Решению этих проблем посвящена диссертационная работа М.А. Пудовкиной. Конкретно, в данной работе проводится классификация и исследование криптографических свойств подстановок за счет анализа их теоретико-групповых свойств.

Основная новизна представленных в диссертационной работе М.А. Пудовкиной результатов, насколько можно судить из автореферата, состоит в определении и изучении понятия p_G-структуры. В работе показано, как данное понятие может быть использовано для характеризации криптографических свойств рассматриваемого множества подстановок. Фактически наличие p_G-структуры для множества подстановок G означает, что на G может быть естественным образом определено вероятностное распределение, отличное от равномерного. Таким образом, множество G с «сильно выраженной» (в некоторой естественной мере) p_G-структурой нежелательно в качестве источника подстановок, используемых для криптографических целей (например, S-блоков). Характеризация p_G-структур осуществляется через характеризацию их групп автоморфизмов.

В первой главе диссертации изучается связь p_G-структур со сплетениями групп подстановок. Здесь же проведена классификация подстановок, близкая по смыслу к классификации булевых функций по их расстоянию Хемминга до аффинных функций. В частности, описаны подстановки, находящиеся на максимальном расстоянии от импримитивной группы. В некотором роде такие подстановки можно считать аналогами бент-функций. В главе 2 исследуются двумерные p_G-структуры, задаваемые специальным классом метрик (т.н. конечные натурально-значные метрики). Центральный результат второй главы – полная классификация одного типа натурально-значных метрик (метрики, инвариантные относительно группы Джевонса). Этот результат используется в третьей главе, где изучаются групповые свойства двумерных p_G-структур. В четвертой главе исследуется связь между свойствами одно- и двумерных p_G-структур и возможностями построения атак на блочные XSL шифры. В пятой главе рассмотрены приложения p_G- структур и техники, развитой при их изучении, к некоторым активно исследуемым в настоящее время криптографическим проблемам. В частности, с использованием p_G- структур показано, как конкретная последовательность раундовых функций (описанная в литературе), состоящих из преобразований, имеющих хорошие криптографические свойства, дает в композиции криптографически слабое преобразование. Здесь же описаны некоторые свойства APN-подстановок через характеристики групп автоморфизмов, сопоставляемых этим подстановкам специальных графов.

По тексту автореферата можно сделать следующие замечания.

1. Фактически (такой вывод напрашивается из доступной в автореферате информации) результаты диссертации, нашедшие практическое применение, касаются двумерных p_G- структур. Но ведь такие структуры, по сути своей, возникают в анализе биграмм – концепции, которая довольно хорошо разработана в криптографии. Возможно, автору следовало бы более четко выделить сильные стороны предлагаемых в диссертации методов в сравнении с известными подходами к анализу биграмм.

2. На стр. 24 автореферата, перед определением 9 имеется фраза «Примерами $+_W$ –марковских преобразований…». По всей видимости, допущена опечатка и должно быть: «Примерами $\otimes_W$ – марковских преобразований…».

Приведенные замечания несущественны и не оказывают влияния на общую положительную оценку работы. Следует отметить широкий спектр исследованных в диссертации задач, а также многообразие использованных при этом алгебраических методов. Основные результаты диссертации опубликованы в рейтинговых научных изданиях, соответствующих профилю исследования, и доложены на авторитетных российских и международных конференциях. Поскольку методы, развитые в диссертационной работе, могут быть использованы для анализа и разработки примитивов, используемых в системах защиты информации, соответствие работы паспорту специальности 05.13.19 не вызывает сомнений.

Резюмируя сказанное, считаю, что диссертационная работа «Комбинаторно-алгебраические структуры итерационных функций в системах защиты информации» выполнена на высоком уровне, является законченной научно-исследовательской работой, а ее автор Пудовкина Марина Александровна заслуживает присвоения ученой степени доктора физико-математических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность (физико-математические науки).

Ведущий научный сотрудник
Института динамики систем
и теории управления им. В.М. Матросова
Сибирского отделения РАН
доктор физико-математических наук
(специальность 05.13.01 – Системный анализ,
управление и обработка информации)

Анатолий Валентинович Лакеев

10.04.2017

Подпись заверяю
Нач. отдела делопроизводства
и организационного обеспечения
ИДСТУ СО РАН
Т.Б. Кононенко
10.04.2017

Лакеев Анатолий Валентинович
664033, Иркутск, ул. Лермонтова, 134
Институт динамики систем и теории
управления им. В.М. Матросова СО РАН,
тел. +7 (3952) 45-30-54
e-mail: lakeyev@icc.ru