УТВЕРЖДАЮ

Руководитель ФГУП «18 ЦНИИ» МО РФ

к.т.н О. Швыдя

«13» 04 2017 г.

ОТЗЫВ

на автореферат диссертации Пудовкиной Марины Александровны «Комбинаторно-алгебраические структуры итерационных функций в системах защиты информации»

Актуальность темы. Глубокое проникновение информационных технологий во все сферы деятельности личности, общества и государства определяет важность защиты информации в современном мире, что отражено в Доктрине информационной безопасности РФ. Основой обеспечения безопасности информации является применение криптографических методов защиты информации. Повышенный интерес представляют исследования итерационно криптографических функций XSL-алгоритмов блочного шифрования в связи с их широким распространением. Несмотря на стабильно высокий уровень научной активности в данном направлении до сих пор не была решена проблема взаимосвязи между алгебраическими, комбинаторными и криптографическими свойствами этих функций с соотношениями между раундовыми ключами, блоками открытого и промежуточного шифрованного текста. Решению данной проблемы и посвящено настоящее диссертационное исследование. В этой связи, выбранная диссертантом тема является безусловно актуальной.

Научная новизна. Результаты, полученные в ходе диссертационной работы, обладают несомненной научной новизной. Особенно следует отметить, что:

- выявлена связь натурно-значных метрик, p_G-структур и метрик, инвариантных относительно преобразования линейного слоя;

- предложено понятие L-факторструктуры преобразования, обобщающее известную линейную структуру преобразования;

- показано, что группой автоморфизмов ряда p_G-структур являются сплетения групп подстановок;

- предложены способы описания p_G-структур и комбинаторно-алгебраических свойств у семейства обобщений алгоритма Фейстеля 2-го типа и марковских XSL-алгоритмов блочного преобразования с приводимым преобразованием линейного слоя.

Теоретическая и практическая значимость. Из представленного автореферата следует, что диссертация носит в основном теоретический характер, что согласуется с требованиями выбранного паспорта специальности. В то же время, развитые теоретические положения позволили разработать общий способ поиска и построения p_G-структур, позволяющего предлагать новые методы криптоанализа и обобщать известные. Использование p_G-структур семейства алгоритмов Фейстеля 2-го типа позволяет отличить данное семейство от множества равномерно распределённых случайных подстановок. В частности, из существования $p_{C_n(h)}$-структуры следует существование атак на алгоритмы блочного шифрования PRINTcipher, Robin, Iscream, Zorro и ISEBERG. Разработанный способ анализа XSL-алгоритмов блочного шифрования, обобщающий разностный метод, позволяет увеличить число атакуемых раундов.

Достоверность научных положений и выводов обеспечивается строгим применением математического аппарата теории групп, теории вероятностей и комбинаторики. Полученные в ходе диссертационного исследования результаты опубликованы в 51 печатной работе. Основные результаты диссертации опубликованы в журналах, входящих 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 (32 публикации). В изданиях, входящих в базы цитирования SCOPUS, опубликованы 2 работы; в изданиях, входящих в базы цитирования Web of Science, – 4 работы. Результаты диссертационного исследования представлены на 10 международных семинарах и конференциях. Работы были поддержаны Академией криптографии РФ, что также свидетельствует об их значимости и высоком научном уровне проводимых исследований.

Автореферат диссертации написан грамотным языком, хорошо оформлен и даёт адекватное представление о выполненной работе. Содержание автореферата соответствует паспорту специальности, по которой диссертация представляется к защите.

В целом автореферат диссертационной работы Пудовкиной М.А. оставляет благоприятное впечатление, но следует отметить ряд *замечаний*.

1) В автореферате несколько раз используются утверждения о потенциальной возможности без указания чётких параметров и примеров реализации, что не позволяет критически оценить следующие выводы автора: «существование такой отличимости **может** привести к применению «фундаментальной» атаки различением» (стр. 13); «наличие группы IG_W… **может** означать возможность применения метода гомоморфизмов» (стр. 14); «Существование $p_{C_n(h)}$-структуры у группы $C_n(h)$ … **может** влиять на криптографические свойства всего алгоритма» (стр. 21) и т.д.

2) Автор указывает, что полученные научные результаты позволяют «предлагать новые методы криптоанализа, и обобщать известные» (стр. 10), при этом в автореферате не приведено ни конкретных примеров таких методов, ни сравнение их с существующими методами криптоанализа.

3) Утверждение диссертанта «Приведённый подход в **ряде случаев эффективнее** по сравнению со способом нахождения вероятностей «классических» разностных характеристик.» (стр. 22) не подтверждено

в автореферате. Не раскрыто понятие эффективности: учитываются ли в нём требования к вычислительным, временным и другим ресурсам; качественно ли определена эффективность или количественно. Не определены границы применимости предложенного подхода. Не ясно, какова эффективность данного подхода по сравнению с методами, использующими отличные от «классических» разностные характеристики.

4) Неправильно оформлены отсылки к библиографическим записям в затекстовой ссылке (ГОСТ Р. 7.0.5–2008. Библиографическая ссылка. Общие требования и правила составления. М., 2008. С. 6, пункт 7.5.4). Кроме того, для некоторых источников не указаны сведения о местоположении объекта ссылки в документе: «атаки различением (см. [36])»; «понятие «преобладающей» метрики [34]» и т.д.

5) На странице 24 вместо термина «$\otimes_W$-марковских» используется «$+_W$-марковских».

Указанные замечания не снижают значимости полученных Пудовкиной М.А. в ходе диссертационного исследования результатов и не влияют на общую положительную оценку представленной к защите диссертации.

Заключение. Диссертационное исследование Пудовкиной М.А. обладает научной новизной, имеет несомненную теоретическую значимость, соответствует современному состоянию исследований в выбранной автором области, а его результаты востребованы при решении практических задач криптографии. Диссертация представляет завершённое исследование, содержит успешные решения актуальных исследовательских задач, необходимых для достижения цели представленной научной работы. Результаты диссертационного исследования соответствуют паспорту специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность (пункты 9 и 13). Диссертация «Комбинаторно-алгебраические структуры итерационных функций в системах защиты информации» по уровню решаемых задач и предлагаемых автором решений

отвечает требованиям, предъявляемым к диссертациям на соискание учёной степени доктора физико-математических наук. Её автор, Пудовкина М.А., вносит существенный вклад в развитие научно-методического аппарата оценки уязвимостей систем защиты информации.

Исходя из текста автореферата, учитывая актуальность представляемого диссертационного исследования, теоретическую значимость полученных результатов и их практическую востребованность, следует, что данная научно-квалификационная работа соответствует требованиям, предъявляемым к докторским диссертациям, установленным п. 9 Положения о присуждении учёных степеней, утверждённого постановлением Правительства РФ №842 от 24.09.2013 г. Диссертант, Пудовкина Марина Александровна, заслуживает присуждения ей учёной степени доктора физико-математических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Автореферат диссертации «Комбинаторно-алгебраические структуры итерационных функций в системах защиты информации» рассмотрен 30.03.2017 г. на секции № 7 НТС ФГУП «18 ЦНИИ» МО РФ под председательством начальника управления Игумнова Д.Л.

Секретарь секции № 7
Старший научный сотрудник
к.т.н. Островский А.С.
Островский Александр Сергеевич

Советник руководителя ФГУП «18 ЦНИИ» МО РФ
д.т.н., профессор Голубев Е.А.
Голубев Евгений Александрович

Начальник лаборатории
к.т.н. Кононов Д.С.
Кононов Дмитрий Сергеевич

Почтовый адрес: 111123, г. Москва, Свободный пр-т, 4, тел.: +7 495 302 94 40