О Т З Ы В

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.

Криптографические методы, в том числе основанные на использовании симметричных блочных алгоритмов шифрования, применяются во многих автоматизированных системах для обеспечения защиты информации от несанкционированного доступа. Вопросы анализа надежности применяемых криптографических преобразований являются основополагающими в области информационной безопасности. Появление новых методов криптоанализа зачастую обусловлено нахождением и последующим использованием у алгоритмов блочного шифрования новых структур. Поэтому следует отметить актуальность исследований в области структур итерационных криптографических функций.

В диссертационной работе Пудовкиной М.А. исследуются структуры, обусловленные алгебраическими, комбинаторными и криптографическими свойствами преобразований XSL-алгоритмов, а также их характеристики. Автором введено понятие p_G-структуры, относительно которого рассмотрены современные комбинаторно-алгебраические и теоретико-вероятностные методы анализа. Разработан общий способ поиска и построения p_G-структур для преобразований, составляющих итерационную криптографическую функцию современных семейств алгоритмов блочного шифрования. Исследовано влияние преобразований, составляющих итерационную функцию зашифрования, на наличие потенциально опасных p_G-структур. Описаны групповые свойства 2-мерных p_G-структур Исследовано влияние приводимости линейного преобразования XSL-алгоритма блочного шифрования на свойства p_G-структур. Описаны свойства марковских XSL-алгоритмов блочного шифрования с приводимым линейным преобразованием. Особое внимание уделяется поиску инвариантов частичных функций зашифрования блочных шифров, что имеет большую ценность при анализе адаптивных атак на шифры с подобранными шифртекстами и криптоанализе с подобранными открытыми текстами, дифференциальном криптоанализе.

Основные теоретические и практические результаты диссертации Пудовкиной М.А. получены лично и являются новыми. Автором опубликована 51 научная работа по теме диссертационного исследования, из них 10 статей опубликованы в журналах, рекомендованных ВАК; 4 - в журналах, индексируемых в Web of Science; 2 –в материалах конференций, индексируемых в Scopus. Результаты исследований широко представлены на международных и всероссийских математических конференциях и семинарах, соответствующих тематике проводимого диссертационного исследования.

Практическое использование результатов диссертационного исследования подтверждено Актами о внедрении.

Автореферат написан технически квалифицированно и аккуратно оформлен. Основные этапы проделанной работы и результаты представлены в автореферате в достаточном объеме.

Имеются замечания к представлению результатов исследований в автореферате.

1.Было бы полезно получить информацию по области граничной применимости разработанных способов построения структур для современных итерационных криптографических функций.

2.Хотелось бы увидеть развернутое представление практического использования разработанных способов поиска и построения p_G-структур для задач анализа надежности семейств XLS-алгоритмов шифрования.

Указанные замечания носят рекомендательный характер, не снижают общей ценности диссертационной работы и не влияют на главные теоретические и практические результаты диссертации.

Считаю, что диссертация «Комбинаторно-алгебраические структуры итерационных функций в системах защиты информации» отвечает всем требованиям Положения ВАК РФ о порядке присуждения ученых степеней, предъявляемым к докторским диссертациям, а ее автор Пудовкина Марина Александровна заслуживает присуждения ей ученой степени доктора физико-математических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Профессор кафедры
Безопасность информационных технологий
Южного федерального университета,
доктор технических наук, профессор
(специальность 05.13.19– Методы и
системы защиты информации,
информационная безопасность)

Бабенко
Людмила Климентьевна

Адрес: 347900, г.Таганрог, Ростовской обл.,
ул.Чехова,2
Федеральное государственное автономное
образовательное учреждение высшего образования
Южный федеральный университет
Телефон: 8-(8634)-36-15-18
E-mail: blk@tsure.ru
Инженерно-технологическая академия ЮФУ

ЮФУ: 344006, г. Ростов-на-Дону,
ул. Большая Садовая, 105/42;
Телефон: 8(863)263-31-5
E-mail: info@sfedu.ru; Сайт: www.sfedu.ru

Подпись Л.К. Бабенко

ДИРЕКТОР ИНСТИТУТА КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИТА ЮФУ

Г.Е. ВЕСЕЛОВ

«14» 04 2022 г.