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 (физико-математические науки)

В настоящее время неуклонно растет потребность в совершенствовании средств защиты обрабатываемой и передаваемой информации, что обусловлено нахождением в используемых средствах новых уязвимостей, а вследствие этого и появлением новых методов анализа, обеспечивающих доступ к информации, передаваемой в системах связи, обработки и передачи данных. Ответом на эти вызовы стало возрастание использования криптографических средств защиты информации, многие из которых включают в себя также и алгоритмы блочного шифрования. Одним из основных приёмов, используемых в алгоритмах блочного шифрования, является многократная, состоящая из нескольких циклов, обработка одного блока открытого текста, реализуемая в виде итерационных функций шифрования. Практически все формы анализа алгоритмов блочного шифрования используют тот факт, что некоторые характерные особенности структуры открытого текста могут сохраняться при шифровании и проявляются в соответствующих особенностях зашифрованного текста. В этой связи актуальным является разработка методов исследования структурных свойств итерационных функций, использующихся в системах защиты информации.

В диссертационной работе М.А. Пудовкиной рассматривается научная проблема, связанная с описанием структур итерационных функций, определяемых алгебраическими и комбинаторными свойствами составляющих функции преобразований, и выявлением уязвимостей в системах защиты информации. При этом охватывается широкий круг

фундаментальных математических задач – от классификации графов надгрупп группы Джевонса до приложения теории цепей Маркова к описанию свойств алгоритмов блочного шифрования.

В диссертации, в целях построения единых методов поиска уязвимостей в алгоритмах блочного шифрования, автором введено понятие p_G-структуры, в терминах которого изложены некоторые известные комбинаторно-алгебраические и теоретико-вероятностные методы их анализа. При этом выявлена общая связь между структурными характеристиками отдельных преобразований итерационной функции и структурой всей функции. На основании этого разработана концепция построения p_G-структур для алгоритмов блочного шифрования. Применимость разработанной концепции показана на примере описания p_G-структур некоторых современных семейств алгоритмов блочного шифрования. На основе исследования комбинаторно-алгебраических свойств построенной p_G-структуры можно проводить выявление уязвимости соответствующего алгоритма блочного шифрования, что позволит эффективно применять для дальнейшего анализа этого алгоритма переборные методы с использованием многопроцессорных высокопроизводительных вычислительных средств.

Все основные результаты диссертации М.А. Пудовкиной являются новыми, а научные результаты изложены в виде корректно доказанных утверждений и теорем. Практическая значимость подтверждена актами о внедрении. Результаты диссертации докладывались и обсуждались на российских и международных научных конференциях и научных школах, где соискатель выступала с докладами по данной проблематике и получила положительный отзыв научной общественности.

По автореферату имеются следующие замечания.

1. Автором доказано существование, но в автореферате не приведено описание p_G-структур алгоритмов блочного шифрования PRINTcipher, Robin, iSCREAM, Zorro.

2. Из текста автореферата не прослеживается связь между свойствами орбитальных производных (работа [9] публикаций автора по теме диссертации) и p_G-структур.

Представленная диссертация М.А. Пудовкиной полностью соответствует требованиям «Положения о присуждении ученых степеней», предъявляемым к докторским диссертациям, утвержденного Правительством РФ (постановление № 842 от 24.09.2013 г.), а её автор заслуживает присуждения учёной степени доктора физико-математических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность (физико-математические науки).

Директор ООО «НИЦ СЭ и НК»
доктор технических наук, профессор
(специальность 05.13.11 – Математическое
и программное обеспечение вычислительных машин,
комплексов и компьютерных сетей)
«10» 3 2017 г. Илья Израилевич Левин

Адрес: 347900, г. Таганрог, Ростовская область, пер. Итальянский, 106, Общество с ограниченной ответственностью «Научно-исследовательский центр супер-ЭВМ и нейрокомпьютеров» (ООО «НИЦ СЭ и НК»).
телефон: (8634) 319-092
e-mail: levin@superevm.ru
электронный адрес: http://www.superevm.ru

Подпись доктора технических наук, профессора И.И. Левина удостоверяю.
Начальник отдела кадров
ООО «НИЦ СЭ и НК» А.В. Коваленко

Общество с ограниченной ответственностью «НИЦ Супер-ЭВМ и нейрокомпьютеров» Россия Ростовская область г. Таганрог
ОТДЕЛ КАДРОВ