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

Диссертация М.А. Пудовкиной посвящена теоретико-групповым свойствам блочно-итерационных криптосистем. Криптосистема (шифрсистема) рассматривается как семейство f ключезависимых подстановок f_k с ключом k, выбранных из $S(X)$ – симметрической группы подстановок, действующей на множестве блоков открытого и шифртекстов X. Основные объекты анализа в диссертации: тактовые подстановки (в диссертации используется термин раундовые функции), композиции которых дают f_k, и S-блоки (в диссертации – S-боксы), которые участвуют в построении тактовых подстановок.

В автореферате представлены несколько тематических линий диссертации. Мы остановимся на основной, той, план которой заявлен во введении. Согласно этому плану, потенциальные слабости криптосистемы – это свойства, которые отличают подстановку, выбранную наудачу из f, от подстановки, выбранной наудачу из $S(X)$. Искомые свойства предлагается выявлять с помощью p_G-структур, т.е. разбиений X^t, на которых действие подстановок f отличается от действия общих подстановок $S(X)$. Понятно, что любая практическая криптосистема имеет p_G-структуру, вопрос только в степени ее выраженности и времени на проверку действия подстановок на ней. К сожалению, эти важные вопросы, которые определяют вероятность успеха атак по распознаванию f и их сложность, в автореферате не освещены. Акцент делается на классификацию p_G-структур и их характеризацию, описание p_G-структур некоторых важных тактовых подстановок (например, Фейстеля) и их композиционных элементов (например, линейных преобразований в схемах XSL). Таким образом, акценты смещаются от вопросов оценки и обоснования стойкости блочных криптосистем к вопросам создания теоретических основ обоснования/оценки. Полученные при этом результаты, безусловно, являются значимыми, они развивают теорию блочно-итерационных криптосистем с точки зрения теории групп подстановок.

Следует отметить большой размах диссертации. В ней, кроме указанной выше темы p_G-структур, имеется еще несколько крупных тем. И в каждой из них используется теоретико-групповой подход.

Отметим еще два значимых результата диссертации:

- достаточно общий способ поиска и построения p_G-структур, обусловленных комбинаторно-алгебраическими свойствами криптографических преобразований, позволяющий строить алгоритмы криптоанализа;
- описание свойств $\otimes_w$-марковских алгоритмов блочного шифрования.

Из автореферата, к сожалению, не ясно какие из результатов диссертации внедрены в Академии Криптографии РФ, ООО «СТЦ» и АО «МакроСистемы».

Считаем, что диссертационная работа отвечает требованиям, предъявляемым ВАК РФ к докторским диссертациям по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность, – а ее автор Марина Александровна Пудовкина безусловно заслуживает присуждения ей ученой степени доктора физико–математических наук.

Директор
Учреждения Белорусского государственного
университета «НИИ прикладных проблем
математики и информатики»,
доктор физико-математических наук
(01.01.09 – Дискретная математика и математическая кибернетика),
профессор, член-корреспондент НАН Беларуси

Юрий Семенович Харин

16 марта 2017 года

Учреждение Белорусского государственного университета
«НИИ прикладных проблем математики и информатики»,
пр. Независимости, 4, к. 802, 220030, г. Минск, Беларусь,
+375 17 209 51 04
E-mail: apmi@bsu.by
Веб-сайт: http://apmi.bsu.by