ОТЗЫВ

на автореферат диссертационной работы М. А. Пудовкиной
«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

Работа посвящена одной из наиболее сложных и актуальных тем в симметричной криптографии – исследованию комбинаторных и алгебраических структур дискретных криптографических отображений, построенных итеративным путем. Результаты автора имеют непосредственное отношение к разработке фундаментальных основ современных методов криптографии и криптоанализа.

Неформально, под структурой понимается наличие такой особенности итерационного криптографического отображения, которая позволяет отличить это отображение от случайной перестановки, а следовательно обнаруживает потенциальную возможность применения того или иного метода статистического криптоанализа к шифру, в состав которого входит такое криптографическое отображение.

В теоретико-вероятностных терминах автор вводит строгое математическое определение структуры дискретного отображения, исследует способы описания структур, их групп автоморфизмов. Получена целая серия нетривиальных математических результатов, направленных на классификацию и описание свойств математических структур (среди них – натурально-значные метрики, графы орбиталов, L-факторструктуры, корреляционно-иммунные функции и другие объекты) и связанных с ними групп инерций, а также на интерпретацию полученных результатов для криптографических задач.

Все результаты работы, представленные в автореферате, являются новыми, строго доказанными, прошедшими широкую апробацию на международных и российских конференциях. Без сомнения, они вызывают глубокий интерес у специалистов в области дискретной математики, алгебры, теоретической криптографии и вносят существенный вклад в развитие фундаментальных основ криптографии и криптоанализа. Считаем, что содержание работы соответствует требованиям, предъявляемым к диссертациям на соискание ученой степени доктора физико-математических наук по специальности 05.13.19, а её автор, Марина Александровна Пудовкина, заслуживает присуждения искомой степени.

Сергей Артемьевич Малюгин,
доктор физико-математических наук,
ведущий научный сотрудник лаборатории дискретного анализа
Федерального государственного бюджетного учреждения науки
Институт математики им. С. Л. Соболева Сибирского отделения
Российской академии наук, 630090, Новосибирск, пр. Коптюга, 4.
Тел.: (8-383) 333-28-92, Факс: (8-383) 333-25-98,
Mail: im@math.nsc.ru, Web: www.math.nsc.ru

подпись С. А. Малюгина
удостоверяю Н. Н. Токарева
Зав. орготделом
ИМ СО РАН Н.З. Киндалева
«05» 05 2017 г.

Наталья Николаевна Токарева,
кандидат физико-математических наук,
старший научный сотрудник лаборатории дискретного анализа
Федерального государственного бюджетного учреждения науки
Институт математики им. С. Л. Соболева Сибирского отделения
Российской академии наук, 630090, Новосибирск, пр. Коптюга, 4.
Тел.: (8-383) 333-28-92, Факс: (8-383) 333-25-98,
Mail: im@math.nsc.ru, Web: www.math.nsc.ru

05.05.2017