ОТЗЫВ

на автореферат диссертации Пудовкиной Марины Александровны

«Комбинаторно-алгебраические структуры итерационных функций в системах защиты информации»,

представленной на соискание учёной степени доктора физико-математических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность

Диссертационная работа соискателя посвящена исследованию уязвимостей систем защиты информации, в которых используются алгоритмы блочного шифрования. Автор решает задачу поиска уязвимостей с учётом атак на алгоритм блочного шифрования, являющейся частью системы защиты информации, основанных на выявлении характерных структур между цикловыми ключами, блоками открытого и промежуточного шифрованного текстов. Для этого М.А. Пудовкиной была выявлена, разработана и описана связь алгебраических и комбинаторных свойств преобразований, составляющих функцию зашифрования и реализующих принципы усложнения, перемешивания и рассеивания, сформулированные К. Шенноном.

В диссертационной работе развито новое направление, посвященное описанию структур алгоритмов блочного шифрования путём сопоставления им разбиений (названных p_G-структурами) множества X^t, удовлетворяющих ряду условий, которое имеет высокую научную и практическую значимость. Так, с помощью него в работе получена p_G-структура семейства обобщённых алгоритмов Фейстеля 2-го типа, позволившая впервые отличить данное семейство от множества равномерно распределённых подстановок.

В работе рассмотрены разные подходы к заданию p_G-структур, одним из которых является метрический. В связи с этим получено описание натурально-значимых метрик, инвариантных относительно группы сдвигов пространства $V_n(2)$. Как следствие из классификации групп изометрий метрик на $V_n(2)$, инвариантных относительно группы сдвигов и группы перестановок координат, для каждого элемента $m \in \{1, \dots, n\}$ найдена группа инерции множества всех двоичных корреляционно-иммунных функций порядка

m, отображающих группу сдвигов пространства $V_n(2)$ в поле Галуа из двух элементов $GF(2)$, что имеет высокую научную новизну.

Представленная диссертационная работа имеет значительную научную и практическую ценность и отвечает всем требованиям Положения о присуждении учёных степеней ВАК РФ, предъявляемым к докторским диссертациям, а автор Пудовкина Марина Александровна заслуживает присуждения ей учёной степени доктора физико-математических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Отзыв рассмотрен и одобрен на заседании секции №8 научно-технического совета ФГУП «ЦНИИХМ».

Отзыв разработали:

главный научный сотрудник ЦБС, доктор технических наук, специальность 20.02.21, информация о наименовании специальности закрыта — В.Н.Товчигречко

старший научный сотрудник 908 научно-исследовательского отдела центра прикладных разработок, кандидат технических наук, специальность 05.13.19 – Методы и системы защиты информации, информационная безопасность — И.Ю.Коркин

начальник центра прикладных разработок – заместитель генерального директора, кандидат технических наук, специальность 20.02.23, информация о наименовании специальности закрыта — К.В.Малёваный

Подписи 3-х сотрудников заверяю
Ведущий специалист управления по работе с персоналом — В.И.Литке

10 марта 2017 года

Государственный научный центр Российской Федерации федеральное государственное унитарное предприятие «Центральный научно-исследовательский институт химии и механики».
Адрес: 115487, г. Москва, ул. Нагатинская, д.16а
Телефон: +7 (499) 611-51-29, факс: +7 (499) 782-23-21
Электронная почта: mail@cniihm.ru, веб-сайт: http://www.cniihm.ru

Владимир Николаевич Товчигречко
Игорь Юрьевич Коркин
Константин Васильевич Малёваный