Отзыв научного руководителя

на диссертацию Карелиной Е. К. «Методы синтеза корреляционно-иммунных функций на основе минимальных функций», представленной на соискание ученой степени кандидата физико-математических наук по специальности 2.3.6 – методы и системы защиты информации, информационная безопасность

Диссертация Е.К. Карелиной «Методы синтеза корреляционно-иммунных функций на основе минимальных функций» посвящена построению криптографических функций и обоснованию их свойств. Раздел синтеза в криптографии занимает особое место в силу ряда причин. Во-первых, наличие достаточно жестких требований по эксплуатации (габариты, масса, электропитание, скорость работы, физическая защита и т.п.). Во-вторых, отсутствие математического обоснования процесса синтеза криптографических примитивов (например, отсутствие нетривиальных нижних оценок сложности алгоритмов решения задач обращения криптографических функций, теоретическая противоречивость целевых криптографических параметров синтезируемых функций, ограниченность методов реализации криптографических функций). В-третьих, необходимость постоянного учета в процессе синтеза развитие методов криптографического анализа и средств вычислительной техники. Указанные выше причины характеризуют процесс синтеза как решение сложной неформализованной оптимизационной задачи. Внешне синтез средств защиты информации (как показывает опыт многочисленных международных конкурсов по разработке криптографических примитивов) представляет собой многоэтапный процесс с чередующимися этапами оптимизации параметров и криптоанализа текущей версии криптографического примитива.

Булевы математические модели лежат в основе большинства криптосистем с секретным ключом. Для многих приложений в области защиты информации необходимым требованием к синтезируемым

криптографическим функциям является их эффективная вычислимость. Из этого требования непосредственно вытекает невысокая схемная сложность синтезируемых функций и специфика методов их синтеза (например, линейное разветвление аффинных функций, матричное расширение области определения функции, дизъюнктная суперпозиция функций и др.).

В течение всего периода использования булевых математических моделей в синтезе и анализе конкретных криптосистем были сформулированы специальные требования, предъявляемые к криптографическим булевым функциям и системам булевых функций. Данные требования определяют семейство свойств булевых функций, которые специалисты обычно называют криптографическими свойствами, а описывающие их параметры – криптографическими характеристиками. Поскольку многие криптографические свойства являются противоречивыми относительно друг друга, то непосредственный выбор конкретной криптографической булевой функции или системы криптографических булевых функций представляет собой сложную оптимизационную задачу, не имеющую в настоящее время строгого математического описания и эффективных алгоритмов решения.

Порядок корреляционной-иммунности является одним из наиболее важных ее криптографических параметров. Корреляционно-иммунные функции не могут быть аппроксимированы аффинными функциями, зависящими существенно от малого числа переменных. Будучи использованными в качестве функции (или системы функций) усложнения криптографического примитива, корреляционно-иммунные функции делают этот криптографический примитив устойчивым (в определенной мере) к ряду методов криптоанализа. Например, к корреляционному методу и быстрому корреляционному методу. Множество корреляционно-иммунных булевых функций от n переменных как правило обозначается CI(n).

Изучению свойств корреляционно-иммунных функций посвящено множество работ, в которых рассматривается широкий спектр вопросов. Среди исследуемых вопросов серьезное место занимает исследование возможности построения функций с высоким порядком корреляционной иммунности. Основным методом построения функций из CI(n) в настоящее время является рекурсивный метод – функция от заданного числа переменных получается путем изменения функции от малого числа переменных. Понятие минимальной функции в CI(n) является первой попыткой исследования возможности построения функций с высоким порядком корреляционной иммунности без выхода за пределы заданного числа переменных.

С этой позиции актуальность работы Карелиной Е. К. не вызывает сомнений.

В первой главе диссертационной работы Карелиной Е. К. приводятся основные термины, определения и необходимые для последующего понимания текста работы существующие результаты.

Во второй главе описывается метод построения минимальных корреляционной-иммунных функций и корреляционно-иммунных функций. С помощью введенных отображений специального вида наращивается число переменных корреляционно-иммунных функций (минимальных корреляционно-иммунных функций) от малого числа переменных. Далее в этой главе исследуются свойства отображений, используемых в методе построения корреляционно-иммунных функций. Эти свойства позволяют получать необходимые характеристики строящихся функций. В заключение данной главы приведена классификации корреляционно-иммунных функций (минимальных корреляционно-иммунных функций) от 4, 5 и 6 переменных относительно группы Джевонса. Функции из данных классификаций могут использоваться в качестве начальных функций, к которым будет применяться предложенный метод.

В третьей главе исследованы некоторые свойства минимальных корреляционно-иммунных функций. Среди полученных результатов для минимальных корреляционно-иммунных функций в диссертационной работе содержатся следующие:

-достаточное условие существования минимальных корреляционно-иммунных функций,

-спектральный критерий минимальности корреляционной-иммунной булевой функции,

-доказано, что все минимальные корреляционно-иммунные булевы функции существенно зависят от всех своих переменных,

-доказаны некоторые весовые свойства минимальных корреляционно-иммунных булевых функций.

В четвертой главе доказаны асимптотическая оценка мощности множества корреляционно-иммунных функций от n переменных фиксированного веса, а также доказана асимптотическая оценка мощности множества корреляционно-иммунных функций фиксированного веса с нулевым ядром четности. Необходимо отметить, что данные результаты вносят определенный новый вклад в исследования особенностей строения множества корреляционно-иммунных булевых функций.

Научные результаты диссертации, выносимые на защиту, получены автором самостоятельно, являются новыми и обоснованными. Результаты других авторов, упомянутые в тексте диссертации, отмечены соответствующими ссылками. Результаты диссертации докладывались и обсуждались на математических семинарах факультета вычислительной математики и кибернетики МГУ, механико-математического факультета МГУ, Института проблем информационной безопасности МГУ, а также на международной конференции CTCrypt в 2017 году.

Материалы диссертации изложены в 5 печатных работах. Из них четыре работы опубликованы в изданиях Web of Science, Scopus, RSCI, рекомендованных для защиты в диссертационном совете МГУ имени М.В.Ломоносова Автореферат соответствует требованиям и правильно отражает содержание диссертации.

Считаю, что диссертационная работа Карелиной Екатерины Константиновны удовлетворяет всем требованиям Положения о присуждении ученых степеней в МГУ имени М.В. Ломоносова и рекомендую ее к защите в диссертационном совете на соискание ученой степени кандидата физико-математических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

Научный руководитель,

доцент кафедры информационной безопасности
факультета вычислительной математики и
кибернетики ФГБОУ ВО
«МГУ имени М.В. Ломоносова»,
д.ф.- м.н., с.н.с. Логачев Олег Алексеевич

« » _____ 2024 г.

Почтовый адрес: 119991, Москва, ГСП-1, Ленинские горы, МГУ имени М.В. Ломоносова, 2-й учебный корпус
Телефон: +7 (495) 930-43-86
Адрес электронной почты: ollog@inbox.ru

Подпись О.А. Логачева удостоверяю.

Декан факультета вычислительной математики и
кибернетики ФГБОУ ВО
«МГУ имени М.В. Ломоносова»,
академик РАН Соколов Игорь Анатольевич