Отзыв на автореферат диссертации
Карелиной Екатерины Константиновны
«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»

Неотъемлемым структурным элементом при построении современных криптографических примитивов являются булевы функции и отображения. В процессе развития средств и методов криптоанализа сформировался ряд математических свойств, наличие которых у функций позволяет обеспечить устойчивость построенных с их помощью криптопримитивов против тех или иных методов криптоанализа.

Корреляционно-иммунные функции были предложены Т. Зигенталером для использования в качестве функции усложнения в комбинирующем и фильтрующем генераторах. Выход такой функции статистически не зависит от значений её аргументов или от значений некоторых функций от её аргументов. Данное свойство позволяет рассматриваемым функциям противостоять корреляционной атаке.

Большое число работ посвящено изучению корреляционно-иммунных функций. Существенный интерес представляет вопрос построения корреляционно-иммунных функций от большого числа переменных. На сегодняшний день существует несколько способов их построения, один из которых является итерационным: к функции от малого числа переменных применяются рекурсивные процедуры, позволяющие наращивать число переменных до нужного значения. Другой способ предлагает использовать альтернативный подход: корреляционно-иммунная функция строится как сумма минимальных корреляционно-иммунных функций. Минимальная корреляционно-иммунная функция – это корреляционно-иммунная функция, из носителя которой нельзя удалить ни одного набора так, чтобы оставшиеся наборы также являлись носителем корреляционно-иммунной функции.

В диссертационной работе Карелиной Е.К. предложен метод построения корреляционно-иммунных функций, объединяющий описанные выше два подхода. Метод прост в реализации и позволяет быстро наращивать нужное число переменных, получая таким образом новые корреляционно-иммунные функции, не имеющих явных структурных характеристик, которые можно было бы использовать для их отличия от случайных функций. На первом этапе метода строятся минимальные корреляционно-иммунные функции от малого числа переменных. Значения таких функций от 4, 5, 6 переменных также приведены в работе, построена их классификация относительно группы Джевонса. С помощью введенного в работе отображения происходит рекурсивное наращивание числа переменных. Данное отображение сохраняет свойства корреляционной иммунности и минимальности. Таким образом, получается множество минимальных корреляционно-иммунных функций от большого числа переменных. На следующем этапе строится множество корреляционно-иммунных функций как суммы минимальных корреляционно-иммунных функций. Среди полученных функций от большого числа переменных ищется функция, удовлетворяющая исходным требованиям задачи.

Сказанное выше объясняет необходимость исследования свойств минимальных корреляционно-иммунных функций. В работе доказаны некоторые из них, а именно: понижена существующая оценка на вес, доказано, что минимальная корреляционно-иммунная функция существенно зависит от всех своих параметров, доказано достаточное условие минимальности, доказан критерий минимальности функции, основанный на исследовании спектра Уолша-Адамара функции.

В диссертации уделяется внимание и вопросам оценок мощности множества корреляционно-иммунных функций. Так в работе доказана верхняя оценка множества корреляционно-иммунных функций от фиксированного числа переменных фиксированного веса, также приводится асимптотическая оценка данного множества. Доказана асимптотическая

оценка множества BCI(n, w). Данное множество содержит корреляционно-иммунные функции от n переменных веса w, за исключением тех функций, которые принимают равные значения на противоположных наборах. В одной из работ, посвященных вопросам изучения корреляционно-иммунных функций, было доказано, что подсчет мощности множества корреляционно-иммунных функций от n переменных сводится к подсчету мощности множества BCI(n, w) для каждого допустимого значения w. С этой точки зрения, оценка, полученная в диссертационной работе, представляет интерес.

Тема исследований диссертационной работы соответствует паспорту специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность». Автореферат диссертации позволяет сделать вывод о практической и теоретической значимости диссертации, о научной новизне результатов, а также о достижении цели диссертационной работы. Согласно списку, приведенному в автореферате, автором подготовлено и опубликовано по теме диссертации 5 статей, опубликованы в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

Судя по автореферату и публикациям, диссертация Карелиной Е.К. по уровню выполнения, новизне и актуальности соответствует критериям, установленным в Положении о присуждении ученых степеней в Московском государственном университете имени М.В. Ломоносова для диссертаций на соискание ученой степени кандидата наук, а ее автор, Карелина Екатерина Константиновна, заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

Кандидат физико-математических наук,

Начальник Отдела криптографических
исследований ООО «КРИПТО-ПРО» Алексеев Е.К.

Адрес места работы:
127018, г. Москва, ул. Сущевский Вал, дом 18

Я, Алексеев Евгений Константинович, даю свое согласие на включение моих персональных данных в документы, связанные с работой диссертационного совета и их дальнейшую обработку.

«29» ноября 2024 г.

Подпись Алексеева Е.К. удостоверяю.