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»

Для обеспечения стойкости систем защиты информации против различных атак необходимо использовать в качестве криптографического примитива булевы функции, которые обладают определенным набором свойств. К таким свойствам можно отнести высокую степень нелинейности, эффективную схемную реализацию, уравновешенность, алгебраическую и корреляционную иммунность и многие другие. Это обуславливает актуальность решения вопросов построения булевых функций, удовлетворяющих заданным характеристикам.

Согласно представленному тексту автореферата диссертационная работа Карелиной Е.К. посвящена исследованию вопроса синтеза корреляционно-иммунных функций. Данные функции позволяют противостоять корреляционным атакам при их использовании в качестве комбинирующих (фильтрующих) функций в соответствующих генераторах. В работе описан метод построения рассматриваемых функций от большого числа переменных, являющийся комбинацией существующих подходов к решению поставленной проблемы. На первом этапе в описываемом в диссертации методе строится множество минимальных корреляционно-иммунных функций от малого числа переменных. Минимальная корреляционно-иммунная функция – это корреляционно-иммунная функция, из носителя которой нельзя удалить ни одного вектор-набора так, чтобы полученная функция осталась корреляционно-иммунной. В качестве примеров таких функций от малого числа переменных в работе представлена классификация минимальных корреляционно-иммунных функций от 4, 5, 6 переменных. Именно эти функции предлагается использовать для реализации

следующего этапа метода: к ним рекурсивно применяется введенное в работе отображение для наращивания числа переменных, которые сохраняют свойство корреляционной иммунности и минимальности. Далее в описываемом методе корреляционно-иммунная функция строится как сумма минимальных корреляционно-иммунных функций, которые были получены на предыдущем этапе. На завершающем этапе среди полученного множества корреляционно-иммунных функций осуществляется поиск функции, обладающей наилучшими свойствами для ее дальнейшего использования в криптографическом примитиве. В работе приведены примеры успешного применения данного метода: построены устойчивые функции от 7, 8, 9, 10, 11 переменных.

Использование минимальных корреляционно-иммунных функций в предложенном методе обуславливает необходимость исследования их свойств. В диссертации исследованы такие свойства как вес и существенные переменные минимальных корреляционно-иммунных функций; доказано достаточное условие минимальности функции и доказан спектральный критерий минимальности.

Также в работе получены различные оценки мощности множества корреляционно-иммунных функций.

Результаты работы, приведенные в автореферате, позволяют сделать вывод, что все цели диссертационной работы достигнуты, а поставленные задачи выполнены.

Автореферат диссертации четко структурирован, достаточно полно отражает результаты диссертации, опубликованные в 5 статьях, 4 из которых 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,
Заместитель директора Центра разработок
программных продуктов по криптографии,
АО «ИнфоТеКС» Поташников А.В.

Адрес места работы:
127273, Москва, Отрадная ул., 2Б строение 1

Я, Поташников Александр Викторович, даю свое согласие на включение моих персональных данных в документы, связанные с работой диссертационного совета и их дальнейшую обработку.

«18» 11 2024 г.

Подпись Поташникова А.В. удостоверяю.