ОТЗЫВ
официального оппонента о диссертации
на соискание ученой степени кандидата физико-математических наук
Карелиной Екатерины Константиновны
на тему: «Методы синтеза корреляционно-иммунных функций на основе минимальных функций»,
по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность»

Диссертационная работа Карелиной Екатерины Константиновны «Методы синтеза корреляционно-иммунных функций на основе минимальных функций» посвящена разработке метода синтеза криптографических булевых функций, обладающих свойством отсутствия статистической зависимости между значением функции и определенными наборами ее переменных при естественных теоретико-вероятностных предположениях.

Использование корреляционно-иммунных булевых функций (далее CI-функций) в составе средств защиты информации существенно повышает их устойчивость относительно корреляционных методов анализа. Этим объясняется их востребованность для разработки и создания широкого спектра средств защиты информации. Что, в свою очередь, приводит к необходимости обеспечения у этих функций ряда дополнительных свойств, которые довольно часто могут быть «взаимно противоречивыми».

CI-функции составляют хорошо известный математический объект, тесно связанный с комбинаторикой, теорией кодирования и криптографией. В ранее проведенных исследованиях CI-функций предложен и обоснован ряд методов их синтеза. Наиболее значимые из них и их авторы указаны во введении к диссертации. Однако тематика данного направления далеко не исчерпана. Актуальность разработки новых методов синтеза CI-функций непосредственно вытекает из необходимости создания надежных средств защиты информации для использования в государственной, коммерческой и социальной сферах.

Таким образом, тема диссертационного исследования является актуальной как в теоретическом, так и в практическом плане.

Разработанный автором диссертации метод синтеза CI-функций является новым и органично дополняет имеющиеся методы. Особенностью предлагаемого в диссертации метода, отличающей ее от ранее известных, является использование в качестве базовых элементов минимальных CI-функций, под которыми понимаются корреляционно-иммунные функции, из носителей которых нельзя исключить ни одного вектора так, чтобы полученные функции остались корреляционно-иммунными.

Целью диссертации является разработка необходимого математического аппарата и на его основе нового метода синтеза CI-функций и минимальных CI-функций.

Диссертационная работа изложена на 125 страницах, состоит из введения, четырех глав, заключения, списка литературы из 45 наименований и приложения.

Во введении обоснована актуальность темы диссертации, сформулированы цели и задачи исследований, отражены научная новизна и практическая значимость полученных результатов, представлены основные результаты, которые выносятся на защиту.

В первой главе диссертации приводятся основные понятия и ранее известные результаты, которые используются далее в работе или представляются важными для понимания последующих глав.

Вторая глава состоит из восьми разделов и в ней описывается метод построения CI-функций, основанный на комбинации существующих подходов к построению рассматриваемых функций. Метод прост в реализации и позволяет быстро наращивать большое число переменных. Он состоит из двух основных этапов: на первом этапе предлагается строить минимальные CI-функции от заданного числа переменных с помощью определенных рекурсивных процедур, на втором этапе – CI-функция

синтезируется как сумма минимальных CI-функций от нужного числа переменных. В основе метода лежит вводимое в работе отображение AC^w, позволяющее увеличивать число переменных функции. В работе вводится также и обратное к отображению AC^w отображение - DC^w, доказываются некоторые свойства этих отображений. Ключевым свойством данных отображений является то, что они сохраняют свойство корреляционной иммунности функции, что позволяет использовать их для построения рассматриваемых функций. Для реализации метода необходимы начальные минимальные корреляционно-иммунные функции, к которым будут применяться рекурсивные процедуры увеличения числа переменных. В данной главе приводится классификация минимальных корреляционно-иммунных функций от 4, 5, 6 переменных, которые можно использовать как «стартовые» функции в предложенном методе. Также в этой главе приводятся примеры реализации предложенного метода.

Третья глава посвящена изучению некоторых параметров и свойств минимальных CI-функций, таких как вес, существенные переменные. Здесь же доказан спектральный критерий минимальности булевой функции и доказано достаточное условие минимальности.

В четвертой главе исследуются вопросы оценки мощности множества CI-функций от фиксированного числа переменных фиксированного с заданным весом.

В заключении перечислены основные результаты диссертации.

К основным результатам диссертации можно отнести следующие:

- разработан новый метод построения корреляционно-иммунных функций; преимуществом данного метода является быстрое наращивание большого числа переменных;

- получена классификация относительно группы Джевонса минимальных корреляционно-иммунных функций от 4, 5, 6 переменных;

- с помощью предложенного метода построены устойчивые функции от 7, 8, 9, 10, 11 переменных;

- получена оценка мощности синтезируемых с помощью данного метода множеств корреляционно-иммунных и минимальных корреляционно-иммунных функций;

- получены новые результаты относительно минимальных корреляционно-иммунных функций: уточнена верхняя оценка для веса, доказана существенная зависимость от всех переменных, сформулированы и доказаны достаточное условие минимальности, а также спектральный критерий минимальности;

- получена асимптотическая и верхняя оценки мощности множества корреляционно-иммунных функций от фиксированного числа переменных фиксированного веса.

Результаты диссертации имеют законченный характер и снабжены строгими математическими доказательствами; все результаты диссертации являются новыми, а результаты других авторов, упомянутые в диссертации, отмечены соответствующими ссылками; результаты работы изложены в 5 публикациях, из них 4 работы опубликованы в рецензируемых научных изданиях, определенных п. 2.3 Положения о присуждении ученых степеней в Московском государственном университете имени М.В. Ломоносова. Результаты работа апробированы на международной конференции и научных семинарах.

Автореферат диссертации в достаточной степени отражает содержание диссертации.

В целом представленные в диссертации результаты вносят определенный вклад в развитие и совершенствование методики разработки и обоснования криптографических свойств средств защиты информации. Математические результаты являются продвижением в области исследования свойств CI-функций и минимальных CI-функций. Результаты диссертации могут быть использованы в учебном процессе при подготовке специалистов в области математических проблем защиты информации и информационной безопасности.

Имеется следующее замечание: в тексте диссертационной работы встречаются стилистические погрешности (например, на стр. 8, 19, 43, 74, 96).

Указанное замечание не влияет на высокую оценку диссертационного исследования.

На основании вышеизложенного считаю, что диссертация Карелиной Екатерины Константиновны на тему «Методы синтеза корреляционно-иммунных функций на основе минимальных функций» отвечает всем требованиям, установленным Московским государственным университетом имени М.В. Ломоносова к кандидатским диссертациям.

Содержание диссертации соответствует специальности 2.3.6 - «Методы и системы защиты информации, информационная безопасность» (физико-математические науки), а также критериям, определенным пп. 2.1-2.5 Положения о присуждении ученых степеней в Московском государственном университете имени М.В. Ломоносова, оформлена согласно требованиям Положения о диссертационном совете Московского государственного университета имени М.В. Ломоносова.

Карелина Екатерина Константиновна заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 2.3.6 - «Методы и системы защиты информации, информационная безопасность» (физико-математические науки).

Официальный оппонент:
член-корреспондент Академии криптографии
Российской Федерации,
доктор физико-математических наук,
консультант отдела
Департамента информационных систем
Министерства обороны
Российской Федерации Алиев Физули Камилович

«29» ноября 2024 г.

Контактные данные:

адрес места работы: г. Москва, Фрунзенская наб. д.22/2;

Подпись Алиева Физули Камиловича заверяю.

Руководитель Департамента
информационных систем Министерства обороны
Российской Федерации О.В. Масленников