ОТЗЫВ официального оппонента
на диссертацию 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».

Актуальность темы диссертации.

Методы разработки и анализа систем (средств) обеспечения информационной безопасности имеют математическую природу и используются в рамках математических моделей, описывающих функционирование таких систем, действия противника и возможные угрозы информационной безопасности. Фундаментальной проблемой в области разработки и анализа систем обеспечения информационной безопасности является обеспечение стойкости систем защиты информации против криптографических атак, среди которых выделяются различные виды корреляционных атак.

Признанным и распространенным средством противостояния указанным криптографическим атакам является использование в качестве криптографического примитива булевых функций, обладающих хорошими специфическими характеристиками, включающими степень корреляционной иммунности, нелинейность, глобальную автокорреляционную характеристику и другими.

В связи с этим являются актуальными задачи изучения возможности построения, разработки конструкций и исследования свойств булевых функций, в том числе корреляционно-иммунных, противостоящих в качестве

криптографического примитива различным видам корреляционных атак на системы защиты информации. Методы решения этих задач имеют математическую природу и используют математический аппарат и подходы различных разделов математики, в том числе методы арифметики, алгебры, теории функций, комбинаторики.

Значительное количество работ посвящено изучению свойств корреляционно-иммунных функций (CI-функций). В них рассматривается достаточно широкий спектр направлений, одним из которых является построение функций с высоким порядком корреляционной иммунности от большого числа переменных. На текущий момент одним из основных методов построения таких функций является рекурсивный метод – CI-функция от заданного числа переменных получается путем пошаговой модификации функций от меньшего числа переменных.

Понятие минимальной CI-функции предлагает альтернативный подход к решению указанной задачи: CI-функция от заданного числа переменных с требуемыми параметрами ищется в виде суммы минимальных CI-функций с непересекающимися носителями.

Вопросы, рассматриваемые в научно-квалификационной работе Карелиной Е. К. связаны с реализацией данного подхода.

Таким образом, тема диссертации, посвященной обеспечению стойкости систем защиты информации против корреляционных криптографических атак в математических моделях информационной безопасности актуальна как в теоретическом, так и в прикладном смысле.

Основное содержание работы.

Первая глава работы Карелиной Е. К. содержит основные понятия и существующие результаты, которые будут использоваться автором в дальнейшем.

Вторая глава посвящена описанию метода построения минимальных CI-функций и CI-функций. Автором замечено, что простая операция над CI-функцией (в терминах работы – введенное отображение AC^{ω}) увеличивает число переменных, а также сохраняет свойство минимальности CI-функции. Данная операция лежит в основе предлагаемого и обоснованного метода построения CI-функции. Изучены некоторые свойства данной операции, а также рассмотрена обратная операция к ней. В разделе 2.5 доказана достижимая верхняя оценка числа минимальных CI-функций, получаемых из данной CI-функции за один шаг применения операции AC^{ω}, а в разделе 2.6 – соответствующая нижняя оценка.

В разделе 2.7 обсуждается применение разработанной техники для построения CI-функций из минимальных CI-функций с приведением примеров построенных функций. Надо отметить, что такой подход, как видно, потребовал трудолюбия и определенных затрат вычислительных ресурсов, однако так на практике в большинстве случаев и строятся булевы функции для использования в криптографических примитивах.

В разделе 2.8 приведена классификация CI-функций (минимальных CI-функций) от 4, 5 и 6 переменных относительно группы Джевонса. Классификация для 6 переменных приведена в предположении гипотезы 1: если не существует минимальных CI-функций четного веса w от n переменных, то не существует минимальных CI-функций веса большего от этого же числа переменных. Данная гипотеза позволяет сократить вычислительные затраты, и в предположении данной гипотезы классификацию от 6 переменных для минимальных CI-функций можно считать полной. Построенные классификации позволяют использовать приведенные в них функции в качестве «стартовых точек» для предложенного во второй главе метода построения CI-функций.

Свойства минимальных CI-функций были мало изучены до исследований в рамках представленной диссертационной работы. Содержание третьей главы позволяет расширить понимание свойств минимальных CI-функций. Так, среди новых результатов для рассматриваемых функций можно выделить результаты о существенных переменных и результат о новой верхней оценке веса минимальных CI-функций. Также в работе приводится достаточное условие существования минимальных CI-функций и доказывается спектральный критерий минимальности.

С использованием полученных во второй главе результатов в четвертой главе получена асимптотика числа CI-функций заданного фиксированного веса от заданного растущего числа переменных, а также асимптотика числа таких функций без противоположных наборов в носителе. Установлено также, что эта асимптотика является точной верхней оценкой.

Приложение к работе иллюстрирует достоверность полученных результатов и эффективность предложенного метода построения CI-функций: содержатся примеры полученных CI-функций, которые раскладываются в сумму минимальных CI-функций веса 2, 4, 6.

Новизна научных результатов.

В диссертационной работе предпринято систематическое развитие подходов как к построению минимальных CI-функций, так и к построению CI-функций, использующему минимальные CI-функции в качестве «стартовых точек». Диссертационное исследование опирается на предшествующие статьи Е. К. Алексеева, однако при этом предъявляет как новые строго доказанные математические результаты, так и алгоритмы работы с минимальными CI-функциями, позволившими получить как большой корпус минимальных CI-функций, включая полную классификацию минимальных CI-функций от не более чем шести переменных, так и

значительное количество примеров построения CI-функций с дополнительными полезными криптографическими характеристиками на основе минимальных CI-функций.

Обоснованность и достоверность научных положений, выводов и рекомендаций, сформулированных в диссертации.

Математические утверждения, содержащиеся в работе, снабжены полными доказательствами, классификационные результаты приведены в полном виде, построенные функции представлены в виде их вектор-строк в шестнадцатеричном формате и потому проверяемы. Используемые в работе понятия и полученные утверждения снабжены большим количеством примеров высокого иллюстративного качества.

Основные положения работы опубликованы автором в рецензируемых изданиях, рекомендованных ВАК РФ.

Результаты работы в дальнейшем могут использоваться как для практического применения, так и в качестве основы для дальнейших теоретических исследований.

Замечания к диссертации.

В работе приведено большое количество результатов практических вычислений. По отдельным фразам на страницах 68 и 71 можно понять, что использовался персональный компьютер, однако не приведено сведений о характеристиках этого компьютера и о затраченных ресурсах (памяти и времени), что могло бы послужить ориентиром для последователей.

От изложения практических вычислительных результатов в разделе 2.7 (а также в разделе 3.5) остается ощущение некоторой недосказанности: приведены примеры функций с числом переменных от 7 до 11 с хорошими дополнительными характеристиками, но некоторые детали их построения кажутся неуточненными. Ранее в диссертации было сказано, что полный перебор при таких параметрах невозможен, – значит, использовался

неполный поиск, а деталей не приведено; непонятно, как удалось обеспечить то, что носители не пересекаются, и как удалось добиться 6- и 7-устойчивости построенных функций. Можно предположить, что были удачные и неудачные попытки, и информация о доле удачных попыток была бы очень интересна и полезна для последователей. Возможно, использовались какие-то элементы алгоритмов эвристического поиска, об этом тоже интересно было бы знать.

Во введении на странице 12 (а также на странице 6 автореферата) в рамках исторической справки сообщается, что О. В. Денисов в статье 1991 года получил асимптотику для числа корреляционно-иммунных функций малого порядка, но в этой работе оказалась неточность, которую Денисов исправил в статье 2000 года. Однако данная информация отражает состояние дел на момент, предшествующий 2010 году. В 2010 году E. R. Canfield, Z. Gao, C. Greenhill, B. D. McKay и R. W. Robinson в статье «Asymptotic enumeration of correlation-immune Boolean functions», опубликованной в журнале «Cryptography and Communications», показали, что результат первой статьи Денисова был верным, а второй – нет. Специально подчеркну, что результаты Денисова упомянуты в диссертации только для исторической справки и для получения результатов никак не используются.

Многократно используется выражение «длина столбца». Обычно в таких случаях говорят про высоту «столбца», поскольку столбец – частный случай матрицы, и в этом смысле его длина равна единице.

Представляется неудачным словосочетание «минимальных CI-функций и CI-функций» в названии второй главы и некоторых других местах.

Представляется неверным с точки зрения оформления, что нумерация разделов приложения продолжает нумерацию разделов четвертой главы.

Нет знаков препинания после некоторых выносных формул на протяжении всей диссертации, в частности, в разделах 2.1, 2.4, 2.5, нет точек в конце абзацев в верхней части страницы 37.

В верхней строчке на стр. 41 лишняя частица «не».

В формулировке теоремы 9 на странице 43 слово «справедливо» оказалось сокращено до «справе».

Формулировка теоремы 9 формально записана не вполне корректно, поскольку сначала говорится про разбиение, потом оказывается, что оно не полное, а потом про k и m написано, как про конкретные значения, хотя таких значений k и m много.

Внизу страницы 46 идет ссылка на «критерий равенства функций 9». Это на самом деле теорема 9.

На странице 48 написано: «Таким образом, … существуют функции, для которых … оценка … достижима», однако достижимость оценки поясняется только после этого.

На странице 57 в верхнем абзаце раздела 2.7 слово «построения» повторяется два раза подряд, далее идет ошибка в слове «рассмотренны» (удвоенная «н»), еще чуть ниже говорится об использовании результатов главы 2.8, хотя глава имеет номер 2; видимо, имеется в виду расположенный дальше раздел 2.8.

В формулировке предложения 7 на странице 74 используется термин «подфункция» в значении, не соответствующем общераспространенному значению этого термина, которое определяется в диссертации на странице 25.

Заключение по диссертации.

Вместе с тем, указанные замечания не умаляют значимости диссертационного исследования. Диссертация отвечает требованиям, установленным Московским государственным университетом имени М.В.Ломоносова к работам подобного рода. Содержание диссертации соответствует специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность» (по физико-математическим наукам) по следующим областям исследования: 1) теория и методология обеспечения информационной безопасности и защиты информации; 5) методы и средства (комплексы средств) информационного противодействия угрозам нарушения

информационной безопасности в открытых компьютерных сетях, включая Интернет; 10) модели и методы оценки защищенности информации и информационной безопасности объекта; 15) принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности; 19) исследования в области безопасности криптографических алгоритмов, криптографических примитивов, криптографических протоколов, защита инфраструктуры обеспечения применения криптографических методов, а также критериям, определенным пп. 2.1-2.5 Положения о присуждении ученых степеней в Московском государственном университете имени М.В.Ломоносова, а также оформлена согласно требованиям Положения о совете по защите диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук Московского государственного университета имени М.В.Ломоносова.

Таким образом, соискатель Карелина Екатерина Константиновна заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность».

Официальный оппонент:
Доктор физико-математических наук,
доцент кафедры дискретной математики
механико-математического факультета
МГУ им. М. В. Ломоносова «_____
_____»

ТАРАННИКОВ Юрий Валерьевич *подпись*

Дата подписания
10.12.2024

Контактные данные:

Специальность, по которой официальным оппонентом защищена диссертация:
2.3.6. «Методы и системы защиты информации, информационная безопасность».

Адрес места работы:
119991, Москва, ГСП-1, Ленинские горы, д. 1,
механико-математический факультет
Тел.: 7(495)9391244; e-mail: office@mech.math.msu.su

Подпись сотрудника механико-математического факультета МГУ им. М. В. Ломоносова Ю. В. Таранникова удостоверяю:

Ученый секретарь
Диссертационного совета
МГУ.012.3,
к.ф.-м.н. /А.В. Галатенко/