МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА

На правах рукописи

Карелина Екатерина Константиновна

Методы синтеза корреляционно-иммунных функций на основе минимальных функций

Специальность 2.3.6 — «Методы и системы защиты информации, информационная безопасность»

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата физико-математических наук

Москва — 2024

Работа выполнена на кафедре информационной безопасности факультета вычислительной математики и кибернетики ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова».

Научный руководитель — *Логачев Олег Алексеевич*,
доктор физико-математических наук, доцент

Официальные оппоненты — *Алиев Физули Камилович*,
доктор физико-математических наук, доцент, Министерство обороны Российской Федерации, Департамент информационных систем, консультант отдела

Селезнева Светлана Николаевна,
доктор физико-математических наук, доцент, кафедра математической кибернетики факультета вычислительной математики и кибернетики ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова», профессор

Таранников Юрий Валерьевич,
доктор физико-математических наук, механико-математический факультет ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова», кафедра дискретной математики, доцент

Защита диссертации состоится «18» декабря 2024 г. в 16 часов 45 минут на заседании диссертационного совета МГУ012.3 ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова» по адресу: 119234, Москва, ГСП-1, Ленинские горы, д.1, ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова», механико-математический факультет, аудитория 14-08.

С диссертацией можно ознакомиться в отделе диссертаций научной библиотеки МГУ имени М.В. Ломоносова (Ломоносовский просп., д. 27), а также на портале: `https://dissovet.msu.ru/dissertation/3124`.

Автореферат разослан « » 2024г.

Ученый секретарь
диссертационного совета МГУ012.3,
к.ф.-м.н. Галатенко
Алексей Владимирович

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Жизнь современного общества трудно представить без использования информационных и телекоммуникационных систем. Стремительное развитие информационных технологий с их быстро растущим потенциалом привело к возможности объединения таких разнородных систем в единые информационно-телекоммуникационные системы — IT-системы, которые стали использоваться повсеместно и которые оказывают все большее влияние на все сферы человеческой деятельности. Информация стала одним из главных и мощных ресурсов государств.

Быстрые темпы научно-технического прогресса в информационной сфере, как следствие, привели к возникновению целого ряда угроз безопасности IT-систем со стороны злоумышленников: различные виды мошенничества, компьютерных преступлений, шпионаж, диверсии, несанкционированный доступ и т.п. Противоправные действия с информацией не только затрагивают интересы государства, общества и личности, но и оказывают негативные, а порой трагические и катастрофические воздействия на здания, помещения, личную безопасность обслуживающего персонала и пользователей информации. Таким образом, становится актуальной задача построения защищенных систем, анализ возможных угроз и разработка средств и методов защиты таких систем.

В ходе разработки средств защиты информации большое значение имеют их математические модели. В частности, аппарат булевых функций играет важную роль при построении адекватных математических моделей генераторов псевдослучайных последовательностей и усложняющих преобразований[1] (S-боксов). Для построения качественных средств защиты информации при синтезе их математических моделей необходимо использовать булевы функции, обладающие различными наборами свойств (таких как высокая нелинейность, корреляционная иммунность, алгебраическая иммунность и многие другие). Данная работа посвящена синтезу корреляционно-иммунных функций.

В работах Т. Зигенталера[2–5] были получены основные необходимые и достаточные условия корреляционной иммуности фиксированного порядка (теоретико-информационные, вероятностные, комбинаторные, спектральные). Другие работы посвящены установлению связи понятия CI-функции фиксированного порядка с некоторыми комбинаторными объектами. Например, с орто-

[1]Menezes A., van Oorschot P., Vanstone S. «Handbook of Applied Cryptography», CRC Press, 1996, pp. 816

[2]Siegenthaler T. «Correlation-immunity of nonlinear combining functions for cryptographic applications», IEEE Trans. On Information Theory, vol. IT-30, №5, 1984, pp. 776-780

[3]Siegenthaler T. «Decrypting a Class of Stream Cipher Using Ciphertext Only», IEEE Trans. On Computers, vol. c-34, 1985

[4]Siegenthaler T. «Design of Combiners to Prevent Divide and Concuer Attacks», In Proceedings of CRYPTO'85, LNCS №218, Springer-Verlag, 1986, pp. 273-279

[5]Siegenthaler T. «Cryptanalysis of Nonlinear Filtered ML-Sequences», In Proceedings of EUROCRYPT'86, LNCS №219, Springer-Verlag, pp. 103-110

гональными таблицами[6–7] (массивами).

Существуют различные подходы к синтезу CI-функций. Самым простым с идейной точки зрения является переборный метод, в процессе которого проверяются необходимые и достаточные условия корреляционной иммуности для функций, выбираемых из некоторого подходящего множества. Преимуществами данного метода синтеза является его простота и надежность. Кроме того, в ходе реализации перебора как вспомогательный материал могут быть использованы результаты групповых классификаций (относительно группы Джевонса и полной аффинной группы) булевых функций от небольшого числа переменных.

Комбинаторные методы синтеза[8–10] в основе своей содержат операцию конкатенации таблиц значений пары булевых функций от n переменных. При этом различные варианты выбора этих функций позволяют построить булеву функцию от (n+1) переменной как с сохранением порядка корреляционной иммуности, которым обладали исходные функции от n переменных, так и с увеличением порядка корреляционной иммуности на единицу.

Некоторые методы синтеза CI-функций основаны на использовании булевых функций из фиксированных функциональных классов. При этом для обеспечения необходимого уровня корреляционной иммунности используются определенные конструктивные особенности булевых функций из данного фиксированного класса. Приведем два наиболее характерных примера.

Рассмотрим так называемый класс Майорана-Мак-Фарланда булевых функций. Первоначально он стал известен как один из базовых классов для синтеза бент-функций.[11–12] Неформально конструкцию булевой функции из этого класса можно описать следующим образом. Множество переменных конструируемой булевой функции разбивается на два непересекающихся подмножества мощностей k и m соответственно, $k + m = n$. Конкретную функцию из класса Майорана-Мак-Фарланда определяет семейство из $k + 1$-ой булевых функций от m переменных. Первые k из них образуют функцию, отображающую строки длины m битов в строки длиной k битов. Задав верхнюю границу t для минимума весов строк-значений этой функции, мы можем с помощью конструкции Майорана-Мак-Фарланда построить $(t - 1)$-устойчивую булеву функцию (т.е. уравновешенную корреляционно-иммунную порядка $t - 1$ булеву функцию).

---

[6]Camion P., Carlet C., Charpin P., Sendrier N. «On correlation-immune fucntions», In Proceedings of CRYPTO'91, LNCS №576, Springer, Berlin, Heidelberg, 1992, pp. 91-148

[7]Hedayat A. S., Sloane N. J. A., Stufken J. «Orthogonal arrays. Theory and Applications. Springer series in statistics», Berlin, Heidelberg, Springer-Verlag, 1999, pp. 416

[8]Camion P., Carlet C., Charpin P., Sendrier N. «On correlation-immune fucntions», In Proceedings of CRYPTO'91, LNCS №576, Springer, Berlin, Heidelberg, 1992, pp. 91-148

[9]Siegenthaler T. «Correlation-immunity of nonlinear combining functions for cryptographic applications», IEEE Trans. On Information Theory, vol. IT-30, №5, 1984, pp. 776-780

[10]Wu C.-K., Feng D. «Boolean Functions and Their Applications in Cryptography», Springer-Verlag, Berlin, Heidelberg, 2016, pp. 256

[11]Логачев О.А., Сальников А.А., Смышляев С.В., Ященко В.В. «Булевы функции в теории кодирования и криптологии», Москва: Ленанд, 2021, С. 576

[12]Carlet C. «Boolean Functions for Cryptography and Coding Theory», Cambridge University Press, New York, 2020, pp. 562

Второй пример связан с классом так называемых алгебраически вырожденных булевых функций.[13] Несмотря на имеющуюся в названии данного класса некоторую «негативную» коннотацию, алгебраически вырожденные булевы функции регулярно используются при синтезе криптографических механизмов. Неформально алгебраически вырожденная функция от n переменных может быть представлена в виде суперпозиции некоторой булевой функции от k переменных, $k < n$, и k линейных булевых функций, множество-объединение существенных переменных которых имеет мощность n. Алгебраически такая функция может быть также представлена в виде композиции линейного отображения, описываемого булевой матрицей размера $k \times n$, и булевой функции от k переменных. Фиксируя те или иные свойства функции от k переменных и $(k \times n)$-матрицы, мы можем добиваться выполнения определенных свойств у результирующей алгебраически вырожденной булевой функции от n переменных. В частности, если указанная матрица является порождающей матрицей линейного двоичного $[n, k, d]$-кода, то для любой булевой функции от k переменных порядок корреляционной иммунности результирующей алгебраически вырожденной булевой функции от n переменных не менее $d - 1$. Кроме того, использование семейств линейных кодов, исправляющих ошибки и обладающих некоторыми специальными свойствам, позволяет с использованием данной техники строить семейства CI-функций.

Активно разрабатывался класс методов синтеза CI-булевых функций, обладающих рядом дополнительных свойств, называемых рекурсивными методами (в качестве дополнительных свойств фигурировали - нелинейность, алгебраическая иммунность, уравновешенность и т.п.). Достаточно подробно такие рекурсивные методы синтеза рассмотрены в работах Ботева А. А.[14–19] и Та-

[13] Wu C.-K., Dawson E. «Construction of Correlation Immune Boolean Fucntions», Australasian J. of Combinatorics, 21, 2000, pp. 141-166

[14] Ботев А. А. «Новые соотношения между корреляционной иммунностью, нелинейностью и весом для неуравновешенных булевых функций», Материалы V научной школы по дискретной математике и ее приложениям, Москва, 12-17 ноября 2001 г. М.: издательство центра прикладных исследований при механико-математическом факультете МГУ, 2002 г., С. 20-26

[15] Ботев А. А. «О взаимосвязи корреляционной иммунности и нелинейности для неуравновешенных булевых функций», Материалы XII международной школы-семинара «Синтез и сложность управляющих систем»

[16] Ботев А. А. «О соотношении между корреляционной иммунностью, нелинейностью и весом для неуравновешенных булевых функций», Математические вопросы кибернетики, вып. 11, М., Физматлит, 2002, С. 149-162

[17] Ботев А. А. «Об алгебраической иммунности одной рекурсивно заданной последовательности корреляионно-иммунных функций», Материалы XV международной школы-семинара «Синтез и сложность управляющих систем», Новосибирск, 18-23 октября 2004 г., Новосибирск: издательство института математики СО РАН, 2004 г., С. 8-12

[18] Ботев А. А. «Об алгебраической иммунности рекурсивных конструкций нелинейных фильтров», Материалы III общероссийской конференции «Математика и безопасность информационных технологий», (Мабит-04), М.: МЦНМО, 2005, С. 131-135

[19] Ботев А. А. «Об алгебраической иммунности новых конструкций функций с высокой нелинейностью», Дискретные модели в теории управляющих систем: VI Международная конференция: Москва, 7-11 декабря, 2004 г., Труды, М.: Издательский отдел Факультета ВМК МГУ имени М.В. Ломоносова, 2004, С. 227-231

ранникова Ю. В.[20–21] Суть рекурсивного метода состоит в следующем. Первоначально выбирается CI-функция от небольшого числа переменных (либо из известного класса, либо полученная методом перебора). Далее с помощью рекурсивных процедур к исходной функции добавляются новые переменные (например, пара переменных), что приводит к появлению булевой функции от большего числа переменных, обладающую необходимыми свойствами. Это рекурсивное преобразование может быть реализовано бесконечное число раз, что порождает бесконечную серию CI-функций, для которых параметры, задающие дополнительные свойства, удовлетворяют соответствующим асимптотическим соотношениям.

В дополнение к информации о методах синтеза CI-функций необходимо упомянуть асимптотическую формулу для числа корреляционно-иммунных порядка k булевых функций, доказанную Денисовым О. В.[22] и имеющую важное методологическое значение для всех направлений исследований по тематике CI-функций. К сожалению, в этой работе автором была допущена неточность, которую он исправил в своей следующей работе.[23]

В части, касающейся использования понятийного аппарата (терминологической базы), необходимо отметить, что наряду с термином «k-устойчивая функция» (т.е. уравновешенная CI-функция от n переменных порядка k) используются также и иные термины. В частности, например, в работах, исследующих схемную сложность булевых функций методами гармонического анализа, используют термин «k-сбалансированная n-местная булева функция»[24] (k-balanced Boolean function), что в нашей терминологии означает CI-функция от n переменных порядка $n-k$.

Цель диссертационной работы заключается в разработке математического аппарата и новых методов синтеза CI-функций и минимальных CI-функций от большого числа переменных, обладающих положительными криптографическими свойствами, а также в изучении свойств минимальных CI-функций и получении оценок мощности множеств CI-функций и минимальных CI-функций. Для достижения цели были поставлены следующие задачи:

1. разработать математический аппарат и метод построения CI-функций и минимальных CI-функций, позволяющий строить CI-функции от неограниченного числа переменных, используя CI-функций от малого числа переменных;

2. построить классификацию минимальных CI-функций от $4, 5, 6$ переменных

[20]Таранников Ю. В. «О корреляционно-иммунных и устойчивых булевых функциях», Математические вопросы кибернетики, 2002. Т. 11. С. 91 – 148

[21]Таранников Ю. В. «Комбинаторные свойства дискретных структур и приложения к криптологии», М.: МЦНМО, 2011, С. 152

[22]Денисов О. В. «Асимптотическая формула для числа корреляционно-иммунных порядка k булевых функций», Дискретная математика, том 3, вып. 2, 1991, С. 25-46

[23]Денисов О. В. «Локальная предельная теорема для распределения части спектра случайной двоичной функции», Дискретн. математика, том 12, вып. 1, 2000, С. 82-95

[24]Bernasconi A. «Harmonic Analysis and Boolean Function Complexity», CALCOLO 35, 1998, pp. 149-186

для их использования в качестве «стартовых» функций в предложенном методе;

3. построить с помощью предложенного метода и вычислительной техники устойчивые функции от $7, 8, 9, 10$ и 11 переменных;

4. разработать математический аппарат для оценки мощностей множеств CI-функций и минимальных CI-функций, получаемых с помощью предложенного метода; провести сравнение теоретических значений мощностей множеств полученных CI-функций с реальными значениями для CI-функций от $4, 5$ и 6 переменных;

5. изучить свойства множества минимальных CI-функций, такие как вес минимальных CI-функций и существенные переменные минимальных CI-функций; сформулировать и доказать критерий минимальности и достаточное условие минимальности;

6. получить асимптотическую оценку мощности множества CI-функций от n переменных.

На защиту выносятся: обоснование актуальности, научная новизна, практическая значимость работы, а также следующие основные положения, которые подтверждаются результатами исследования, представленными в заключении диссертации:

1. Метод построения CI-функций и минимальных CI-функций. Критерий равенства CI-функций, получаемых с помощью данного метода.

2. Классификация относительно группы Джевонса CI-функций и минимальных CI-функций от $4, 5, 6$ переменных.

3. Результаты применения предложенного метода и примеры использования минимальных CI-функций для построения устойчивых CI-функций от $7, 8, 9, 10$ и 11 переменных.

4. Оценки мощностей множеств CI-функций и минимальных CI-функций, получаемых с помощью данного метода.

5. Свойства минимальных CI-функций: вес функций и их существенные переменные, спектральный критерий минимальности, достаточное условие существования минимальных CI-функций.

6. Асимптотические оценки мощностей множеств $CI(n, w)$ и $BCI(n, w)$, верхняя оценка для мощности множества $CI(n, w)$.

Научная новизна. В диссертации получены следующие новые результаты.

1. Предложено отображение AC^w и на его основе сформулирован метод построения CI-функций и минимальных CI-функций, основанный на комбинации рекурсивного и переборного методов. В работе доказано, что результатом применения отображение AC^w к CI-функции и минимальной CI-функции является CI-функция и минимальная CI-функция соответственно. Данный метод использует известные CI-функции и минимальные CI-функции от малого числа переменных и позволяет строить CI-функции и минимальные CI-функции соответственно уже от большего числа переменных.

2. Получена классификация относительно группы Джевонса минимальных CI-функций от $4, 5, 6$ переменных.

3. Построены устойчивые функции от $7, 8, 9, 10, 11$ переменных с помощью предложенного метода.

4. В работе получена оценка мощности получаемых множеств CI-функций и минимальных CI-функций с помощью данного метода.

5. Понижена верхняя оценка веса минимальных CI-функций. Доказано, что любая минимальная CI-функция существенно зависит от всех своих переменных. Доказан критерий минимальности и сформулировано достаточное условие существования минимальных CI-функций.

6. Получены асимптотические оценки множеств $CI(n, w)$ и $BCI(n, w)$. Данные оценки используются для доказательства верхней оценки мощности множества $CI(n, w)$.

Методология и методы исследования. В рамках исследований применялся математический аппарат алгебры, булевых функций и комбинаторики, а также вычислительная техника для построения CI-функций, их классификаций и для подсчета различных параметров рассматриваемых функций.

Степень достоверности. Достоверность представленных в диссертации результатов гарантируется следующими факторами: все 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 диссертации являются достоверными и прошли апробацию на научных семинарах и конференциях; основные результаты диссертации опубликованы в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 2.3.6 - «Методы и системы защиты информации, информационная безопасность» (физико-математические науки).

Соответствие диссертации паспорту научной специальности. Тема, объект и предмет исследований диссертации соответствуют паспорту специальности 2.3.6 - «Методы и системы защиты информации, информационная

безопасность» (физико-математические науки) 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.

Апробация работы. Результаты, представленные в диссертации, докладывались на следующих международных и отечественных научных конференциях и семинарах:

- на семинаре «Математические методы криптографического анализа» кафедры информационной безопасности факультета Вычислительной математики и кибернетики Московского государственного университета имени М. В. Ломоносова, неоднократно в 2014-2015 годах;

- на семинаре отдела математических проблем информационной безопасности ИПИБ МГУ имени М. В. Ломоносова, неоднократно в 2015-2017 годах;

- на семинаре «Булевы функции в криптологии» кафедры дискретной математики Механико-математического факультета Московского государственного университета имени М. В. Ломоносова, неоднократно в 2013-2015 годах;

- на VI международной научной конференции «Современные тенденции в криптографии», г. Санкт-Петербург, 5-7 июня в 2017 году.

Публикации по теме исследования. Результаты работы изложены в 5 публикациях по теме диссертации, 4 из которых опубликованы в рецензируемых научных изданиях, определенных п. 2.3 Положения о присуждении ученых степеней в Московском государственном университете имени М.В.Ломоносова.

Практическая значимость. Большая часть результатов диссертации имеет теоретический характер. Полученные результаты могут быть полезны в теории булевых функции, при построении, разработке и анализе потоковых шифров.

Структура и объем диссертации. Диссертационная работа состоит из введения, одного вспомогательного раздела, трех глав, заключения, списка ли-

тературы из 45 наименований и приложения. Работа изложена на 125 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во Введении обоснована актуальность темы диссертации, сформулированы цели и задачи исследований, отражены научная новизна, 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 следующих глав.

Во второй главе описывается метод построения минимальных CI-функций, основанный на комбинации переборного и рекурсивного методов. В части, касающейся перебора, строятся минимальные CI-функции от малого числа переменных.[24–25] Такие функции можно получить с помощью вычислительной техники. Далее рекурсивно, используя известные минимальные CI-функции от малого числа переменных, строятся минимальные CI-функции от большего числа переменных. Метод прост в реализации и позволяет быстро наращивать число переменных. Предложенный метод позволяет реализовать указанный выше альтернативный подход: сначала рекурсивно строятся подходящие минимальные CI-функции от нужного числа переменных («опорные точки»), которые затем используются для поиска функций с нужными параметрами без изменения количества переменных.

В основе предложенного рекурсивного метода для наращивания числа переменных лежит использование отображения AC^w. Данное отображение вводится в разделе 2.1. Также в этом разделе вводится отображение DC_i. Действие этого отображения является обратным к действию отображения AC^w: отображение DC_i позволяет уменьшать число переменных. Доказывается, что применение данных отображений к уже известной CI-функции (минимальной CI-функции) с определенными значениями параметров отображений позволяет строить CI-функции (минимальные CI-функции соответственно) от большего или меньшего числа переменных. В этом же разделе описывается сам процесс построения CI-функций.

В следующем разделе 2.2 доказываются некоторые свойства введенных отображений.

В разделе 2.3 приводятся примеры действий отображений к заданным функциям.

Применение отображения $AC^w_{v,i}$ к одной и той же функции со всеми возможными параметрами позволяет получить в том числе и равные между собой

[24] Алексеев Е.К., Карелина Е.К. «Классификация корреляционно-иммунных и минимальных корреляционно-иммунных булевых функций от 4 и 5 переменных», Дискретная математика, 2015, Т. 27

[25] Карелина Е.К. «Об одном методе синтеза корреляционно-иммунных булевых функций», Дискретная математика, 2018, Т. 30

функции. В разделе 2.4 приводится критерий равенства двух функций, которые получаются при применении отображения $AC^w_{v,i}$ к некоторой заданной начальной функции. Данный критерий используется при доказательстве нижней и верхней оценок мощности множества CI-функций, которое получается при применении данного отображения к исходной CI-функции. Значение верхней оценки приведено в разделе 2.5, значение нижней оценки — в разделе 2.6.

Рекурсия в процессе построения минимальных функций от большого числа переменных приводит к необходимости исследования
«опорных точек» — минимальных CI-функций от малого числа переменных, в том числе создания их классификации относительно групп, которые сохраняют определенный набор их свойств. Построение классификаций является эффективным и широко применяемым методом исследования свойств и компактного перечисления булевых функций.[24–29]

В разделе 2.7 приводятся результаты применения предложенного метода построения функций.

Раздел 2.8 посвящен построению классификации минимальных CI-функций и CI-функций от малого числа переменных относительно группы Джевонса. В разделе 2.8.1 приведена классификация минимальных CI-функций и CI-функций от 4 переменных, в разделе 2.8.2 приведена классификация минимальных CI-функций и CI-функций от 5 переменных, в разделе 2.8.3 приведена классификация минимальных CI-функций от 6 переменных.

Третья глава посвящена изучению некоторых свойств минимальных CI-функций.

В разделе 3.1 доказывается достаточное условие существования минимальных CI-функций. При доказательстве используется свойство отображения $AC^w_{v,i}$. Доказывается, что для любого $n \geqslant 5$ существуют минимальные CI-функции веса 6 и веса 8, а для любого $n \geqslant 6$ существуют минимальные CI-функции веса 10.

В разделе 3.2 приводится критерий минимальности CI-функции, основанный на исследовании спектра исходной CI-функции (коэффициентов Уолша).

В разделе 3.3 доказывается теорема о существенных переменных минимальных CI-функций. Доказанная теорема показывает, что минимальную CI-функцию от n переменных нельзя описать с помощью минимальной CI-функции от $n-1$ переменной, так как минимальная CI-функция существенно зависит от всех своих переменных.

В разделе 3.4 уточнена верхняя оценка веса минимальных CI-функций.

---

[26]Braeken A., Borissov Y., Nikova S., Preneel B. «Classification of Boolean Functions of 6 Variables or Less with Respect to Cryptographic Properties», Cryptology ePrint Archive, Report 2004/248

[27]Brier E., Langevin P. «Classification of Boolean Cubic Forms of Nine Variables», 2003, IEEE Information Theory Workshop (ITW 2003), IEEE Press, pp. 179-182, 2002

[28]Maiorana J. «A Classification of the Cosets of the Reed-Muller Code R(1,6)», Mathematics of Computation, vol.57, No.195, July 1991, pp.403-414

[29]Harrison M.A. «On the Classification of Boolean Functions by the General Linear and Affine Group», Journal of the Society for industrial and applied mathematics, Vol.12, pp.284-299, 1964

Алексеевым Е. К.[30] было доказано, что вес минимальных CI-функций меньше 2^{n-1} для $n \geqslant 4$. В данной работе оценка понижена до $2^{n-1} - 2$ для $n \geqslant 4$.

В одной из работ, посвященных изучению CI-функций, было предложено использовать минимальные CI-функции для исследования «окрестностей» заданных CI-функций.[31] Для этого требуется разложить заданную CI-функцию на минимальные CI-функции. Результат использования предложенного подхода можно найти в разделе 3.5. В разделе 3.6 приведены некоторые характеристики разложений CI-функций, а также характеристики разложения константы $\mathbf{1}$ на минимальные CI-функции от 4 и 5 переменных.

В четвертой главе исследуются вопросы оценок мощности множества CI-функций. В одной из работ, посвященной изучению свойств CI-функций, рассматривалось строение множества CI-функций. Автором было введено множество $BCI(n, w)$[30], и было доказано, что подсчет мощности множества CI-функций от n переменных сводится к подсчету мощности множества $BCI(n, w)$ для каждого $w = 0, \ldots, 2^{n-1}$.

В разделе 4.1 приводится асимптотическая оценка мощности CI-функций фиксированного веса, в разделе 4.2 асимптотическая оценка мощности множества $BCI(n, w)$. Верхняя оценка мощности множества $CI(n, w)$ доказывается в разделе 4.3. В работе проводится сравнение полученных оценок с точными значениями, вычисленными теоретически или с помощью вычислительной техники.

В Заключении перечислены основные результаты диссертации.

В Приложении содержатся таблицы с практическими результатами.

Заключение. Основные результаты диссертационной работы состоят в следующем.

1. Предложен метод построения CI-функций и минимальных CI-функций, основанный на комбинации рекурсивного и переборного методов. На первом этапе с помощью перебора строятся минимальные CI-функции от малого числа переменных. Примеры таких функций от $4, 5, 6$ переменных получены с помощью вычислительной техники и представлены в работе. Далее для построения минимальных CI-функций от большего числа переменных в работе предложено преобразование, которое позволяет быстро наращивать число переменных. Доказано, что применение такого преобразования к минимальной CI-функции или к CI-функции позволяет построить функцию, которая также является минимальной CI-функцией или CI-функцией соответственно, но уже зависит от большего числа аргументов. С помощью построенных таким образом минимальных CI-функций от большого числа переменных реализуется второй этап метода: CI-функции от заданного

[30] Алексеев Е.К. «О некоторых алгебраических и комбинаторных свойствах корреляционно-иммунных булевых функций» Дискретная математика. 2010. Т. 22. С. 110 – 126

[31] Alekseev E.K., Karelina E.K., Logachev O.A. «On construction of correlation-immune functions via minimal functions», Математические вопросы криптографии, 2018, Т. 9, No 2 С. 7 – 21

числа переменных строятся как сумма минимальных CI-функций от этого же числа переменных с непересекающимися носителями.

2. Представлены классификации минимальных CI-функций от $4, 5$, 6 переменных. Посчитаны мощности классов, а для каждого представителя класса посчитаны и приведены в таблицах такие значения параметров функции, как вес, степень, нелинейность, порядок корреляционной-иммунности и невырожденность.

3. Построены устойчивые функции от 7, 8, 9, 10, 11 переменных с помощью предложенного метода.

4. Доказан критерий равенства CI-функций, полученных с помощью введенного преобразования для наращивания числа переменных. Данный критерий используется в ходе доказательства верхней и нижней оценки мощности множеств CI-функций, получаемых подобным образом. Теоретические оценки подтверждены практическими результатами: в работе представлено сравнение теоретических значений мощностей полученных множеств с реальными значениями для CI-функций от $4, 5$ и 6 переменных. Практические оценки получены с помощью вычислительной техники.

5. Понижена верхняя оценка веса минимальных CI-функций. Доказано, что любая минимальная CI-функция существенно зависит от всех своих переменных. Доказан критерий минимальности и сформулировано и доказано достаточное условие существования минимальных CI-функций.

6. Получены асимптотические оценки множеств $CI(n, w)$ и $BCI(n, w)$. Получена верхняя оценка мощности множества $CI(n, w)$.

Полученные результаты могут быть полезны специалистам Московского Государственного Университета им. М. В. Ломоносова, Института прикладной математики и кибернетики им. М. В. Келдыша, Института математики им. С. Л. Соболева СО РАН, Института криптографии, связи и информатики академии ФСБ России, Центра проблем информационной безопасности факультета ВМК МГУ имени М. В. Ломоносова.

Благодарности. Автор диссертации выражает благодарность доктору физико-математических наук, доценту Логачеву Олегу Алексеевичу, кандидату физико-математических наук Алексееву Евгению Константиновичу, кандидату физико-математических наук Ошкину Игорю Борисовичу.

СПИСОК ПУБЛИКАЦИЙ АВТОРА ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 2.3.6 — «Методы и системы защиты информации, информационная безопасность» и входящих в базы цитирования Scopus, Web of Science и RSCI:

- Карелина Е. К. «Классификация корреляционно-иммунных и минимальных корреляционно-иммунных булевых функций от 4 и 5 переменных» / Алексеев Е. К., Карелина Е. К. // Дискретная математика. — 2015. — Т.27, №1. — С.22-33. DOI: https://doi.org/10.4213/dm1312 (1.39 п.л. / авторский вклад - 1.39 п.л. Входит в перечень ВАК РФ, RSCI, двухлетний ИФ РИНЦ 2022: 0,506). / Соавтор верифицировал полученные практические результаты. /

  Перевод:

  Alekseev E. K., Karelina E. K. «Classification of correlation-immune and minimal correlation-immune Boolean functions of 4 and 5 variables» // Discrete Mathematics and Applications. — 2015. — Т.25, №4. — С.193-202. DOI: https://doi.org/10.1515/dma-2015-0019 (1.04 п.л. / авторский вклад - 1.04 п.л. Web of Science, Scopus, SJR — 0.177).

- Karelina E.K., «On construction of correlation-immune functions via minimal functions» / Alekseev E.K., Karelina E.K., Logachev O.A. //Математические вопросы криптографии. — 2018 — Т.9, №2. — С. 7-22 DOI: https://doi.org/10.4213/mvk251 (1.85 п.л. / авторский вклад - 0.45 п.л. Входит в перечень ВАК РФ, RSCI, ИФ РИНЦ 2022: 0,548). / Соавторам принадлежит формулирование метода построения CI-функций, основанного на переборе CI-функций в некотором подпространстве. Базис для этого пространства может быть построен с помощью метода, предложенного автором настоящей диссертации (раздел 4.1 по тексту статьи). Также Карелиной Е. К. получены практические результаты использования предложенного метода (раздел 6 по тексту). /

- Карелина Е. К. «Об одном методе синтеза корреляционно-иммунных булевых функций» // Дискретная математика. — 2018. — Т.30, №4. — С.12-28 DOI: https://doi.org/10.4213/dm1524 (1.96 п.л. Входит в перечень ВАК РФ, RSCI, двухлетний ИФ РИНЦ 2022: 0,506).

  Перевод:

  Karelina E. K. «On a method of synthesis of correlation-immune Boolean functions» // Discrete Mathematics and Applications. — 2020. — Т.30, №2. — С.79-91. DOI: https://doi.org/10.1515/dma-2020-0008 (1.39 п.л. Web of Science, Scopus, SJR — 0.177).

- Карелина Е. К. «Мощностные оценки множества корреляционно-иммунных булевых функций» // Дискретная математика. — 2021. — Т.33, №1. — С.12-19 DOI: https://doi.org/10.4213/dm1628 (0.92 п.л. Входит в перечень ВАК РФ, RSCI, двухлетний ИФ РИНЦ 2022: 0,506).

  Перевод:

  Karelina E. K. «Some cardinality estimates for the set of correlation-immune Boolean functions» // Discrete Mathematics and Applications. — 2022. — Т.32,

№2. — С. 91-96. DOI: https://doi.org/10.1515/dma-2022-0008 (0.58 п.л. Web of Science, Scopus, SJR — 0.177).

Публикации в рецензируемых научных изданиях, входящих в перечень ВАК Минобрнауки России:

- Карелина Е. К. «Мощностные оценки множества корреляционно-иммунных функций, получаемого с помощью отображения AC^w» // International Journal of Open Information Technologies. — 2022. — Т.10, №1. — С. 28-35 (0.92 п.л. Двухлетний ИФ РИНЦ 2023: 0,842).