Отзыв

официального оппонента на диссертационную работу Логачева Олега Алексеевича «Построение и анализ эффективности алгоритмов обращения дискретных функций в математических моделях информационной безопасности», представленную на соискание ученой степени доктора физико-математических наук по специальности 05.13.19 - «Методы и системы защиты информации, информационная безопасность»

Дискретные функции являются одним из основных примитивов для синтеза средств обеспечения информационной безопасности (ИБ). Используемые функции должны обладать достаточно широким набором специфических свойств. Некоторые из этих свойств удается обеспечивать за счет определенного выбора их параметров. Другие свойства выявляются в ходе углубленного анализа дискретных функций, ассоциированных со средствами обеспечения ИБ. Методы анализа средств (систем) обеспечения ИБ используют математический аппарат в рамках математических моделей, описывающих функционирование собственно средств обеспечения ИБ, действия противника и возможные угрозы ИБ.

Важнейшим свойством дискретных функций для обеспечения ИБ является свойство односторонности. Говоря неформально, для таких функций значение при известном аргументе вычисляется эффективно, а вычисление любого прообраза функции (т.е. обращение) для известного значения является сложной вычислительной проблемой. Указанное выше свойство позволяет реализовать необходимые для средств обеспечения ИБ функциональности (например, конфиденциальность, имитозащищенность, электронную подпись и т.п.). Строгое математическое понятие односторонней функции определено в рамках теории сложности вычислений. Однако, теоретическая модель односторонней функции представляет собой бесконечное параметризованное семейство дискретных функций и до сих пор является гипотетическим объектом. Поэтому сложность проблемы

обращения (инвертирования) конкретной дискретной функции оценивается в ходе анализа средств обеспечения ИБ. Обращение дискретных функций является фундаментальной научной проблемой, от результатов исследования которой существенно зависит обоснованность оценок уровня защиты информации. Постоянное развитие и совершенствование математического аппарата, математических моделей и методов обращения дискретных функций являются необходимым условием успешного функционирования существующих и создаваемых средств обеспечения информационной безопасности.

Диссертационная работа О.А.Логачева посвящена совершенствованию математических моделей и повышению на основе полученных результатов эффективности алгоритмов и методов решения проблемы обращения дискретных функций, используемых при построении современных средств защиты информации.

Тема диссертации соответствует паспорту специальности 05.13.19 - «Методы и системы защиты информации, информационная безопасность» по следующим направлениям исследований:

1. Теория и методология обеспечения информационной безопасности и защиты информации.

9. Модели и методы оценки защищенности информации и информационной безопасности объекта.

13. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.

В диссертации приводятся новые теоретические результаты, существенно расширяющие возможности математических методов обращения дискретных функций. Приводятся также результаты исследований параметров дискретных функций, позволившие рассмотреть и изучить новые методы частичного и локального обращения дискретных функций.

Учитывая сказанное выше, тема диссертации О.А.Логачева, безусловно, актуальна и имеет много важных как теоретических, так и практических применений в области обеспечения информационной безопасности. В ходе диссертационных исследований использовались математические методы алгебры, дискретной математики, теории вероятностей, математического анализа, теории кодирования, теории автоматов и теории алгоритмов.

Работа состоит из введения, трех глав, заключения, списка литературы и пяти приложений. Суммарный объем диссертации составляет 297 страниц. Список литературы содержит 182 наименования. В приложениях представлены поясняющие примеры для вопросов, рассматриваемых в основном тексте диссертации.

Во введении дан обзор публикаций по теме исследования, обоснована актуальность, сформулированы цели исследования, кратко перечислены основные результаты.

В первой главе приводятся теоретические результаты, развивающие математический аппарат анализа и синтеза дискретных функций, определенных на конечных абелевых группах. На основе понятия производной для широкого класса комплекснозначных функций на конечных абелевых группах строятся и исследуются математические модели в алгебраическом смысле обобщающие известное семейство полиномиальных кодов Рида-Маллера (теоремы 3.1, 3.2, 3.3, леммы 3.7, 3.8, 3.10). В частности, получены необходимые и достаточные условия, накладываемые на абелеву группу, чтобы произвольная дискретная функция из рассматриваемого класса являлась аналогом полинома (следствие 3.9). Предлагаемая система параметров, обобщающая понятие «алгебраическая степень», адекватно описывает свойства исследуемого класса функций. Это обстоятельство дало возможность автору выделить в указанном выше классе функций специальный подкласс бент-функций на конечной абелевой группе, являющийся аналогом для экстремального класса классических бент-

функций, определяемых на элементарных абелевых 2-группах (теоремы 5.3, 5.6, 5.8, 5.10, лемма 5.12, следствия 5.4, 5.9, 5.11). Последовательно используя данный подход, удалось также содержательно определить для данного случая аналог понятия дуальной бент-функции (теорема 5.13).

Для методов обращения дискретных функций, использующих свойства дифференциального оператора и ранее рассматриваемых для булевых функций, предложен общий подход для представления групповых функций, определенных на произвольных конечных абелевых группах. Это представление обобщает так называемое аффинное расщепление булевой функции. Для групповых функций определяется семейство параметров, характеризующих «нелинейность» функции и эффективность соответствующих методов обращения. Доказывается ряд соотношений, связывающих эти параметры (теоремы 7.6, 7.7, лемма 7.5, следствие 7.8).

Для множества булевых функций вводятся понятия невырожденной булевой функции и структуры вырождения функции и исследуются их свойства (теорема 8.6, лемма 8.4, предложения 8.2, 8.3, 8.5). Невырожденность функции свидетельствует о максимальных возможных алгебраических степенях ее производных. Например, свойство невырожденности квадратичной булевой функции совпадает с ее максимальной нелинейностью. Показано (следствие 8.8), что любая булева функция RM-эквивалентна некоторой невырожденной форме.

Приводятся результаты, обобщающие понятие дуальности линейных блочных кодов для конечных модулей. Основная идея обобщения состоит в определении параметров, позволяющих добиться того, чтобы конечные модули обладали аналогами свойства дуальности для векторных пространств. На языке теории решеток получены соотношения (теорема 4.5, следствие 4.6), связывающие дуальные ρ-структуры для дуальных кодов на конечных модулях, обобщающие известное тождество Мак-Вильямс для дуальных линейных блочных кодов.

Суммы аддитивных характеров конечных полей используются для вычисления спектральных, комбинаторных и других параметров дискретных функций. Автору удалось получить результаты, уточняющие оценку Вейля для модуля сумм аддитивных характеров конечных полей (теоремы 6.5, 6.6). Данное уточнение получено на основе использования так называемого циклотомически приведенного полинома и позволяет в ряде случаев существенно уточнить оценку значения исследуемого параметра функции.

В заключение первой главы приводятся результаты, связанные со свойствами сферической кластеризации булевых функций (теорема 9.1, лемма 9.2) и Δ-эквивалентности булевых функций (теоремы 10.6, 10.7).

Во второй главе рассмотрены вопросы анализа свойств булевых функций с помощью семейств их подфункций. Для изучения наследования комбинаторных и спектральных свойств булевых функций их подфункциями вводится понятие (H,u) - стабильности булевой функции (H-линейное подпространство). Доказан критерий (H,u) - стабильности функции (теорема 12.8). На основе этого критерия предложен алгоритм построения для функции семейства подпространств, для которых данная функция является стабильной. С помощью свойства (H,u) - стабильности удалось доказать (теорема 12.15) новый критерий свойства корреляционной иммунности.

Во второй главе представлены также результаты изучения свойств и параметров аппроксимаций булевых функций на областях, называемых локальными аффинностями. Сужение булевой функции на область, являющуюся ее локальной аффинностью, совпадает с аффинной функцией. Значимость локальных аффинностей определяется возможностью с их помощью сведения исходной нелинейной задачи к некоторой линейной задаче.

Простейшие семейства локальных аффинностей булевой функции могут быть получены с помощью фиксации константами некоторых переменных. Для булевых функций исследованы следующие параметры, характеризующие семейства их локальных аффинностей: уровень

аффинности функции - минимальное число переменных, фиксация которых переводит исходную функцию в аффинную функцию от меньшего числа переменных, и обобщенный уровень аффинности функции - минимальная возможная коразмерность локальных аффинностей функции, являющихся аффинными подпространствами. Автору удалось доказать (теорема 14.8, следствие14.9) верхнюю асимптотическую оценку для значений уровня аффинности (обобщенного уровня аффинности) почти всех булевых функций.

Автором предложен новый вид нормальной формы булевой функции - Аффинная нормальная форма (АффНФ), определяемый относительно фиксированного разбиения области определения функции на ее локальные аффинности. Строение и свойства АффНФ могут быть использованы для вычисления некоторых параметров представляемой этой нормальной формой булевой функции. В частности, получен общий вид коэффициента Уолша - Адамара булевой функции, зависящий от параметров ее АффНФ (теорема 15.6). На основе так называемых центрально-дуальных разбиений на локальные аффинности с помощью АффНФ описан подкласс бент-функций, для которых в явном виде получены выражения для АффНФ соответствующих им дуальных бент-функций (теорема 15.9, следствие 15.10).

Размерности локальных аффинностей конкретных булевых функций существенным образом зависят от свойств функциональных классов, к которым они принадлежат. Например, показано, что для платовидной функции (этот класс содержит все бент-функции) имеет место граница сверху для размерности любой ее локальной аффинности, зависящая от числа переменных и порядка платовидности этой функции (теорема 15.12).

В заключение второй главы представлены результаты, характеризующие возможности «нелинейной» аппроксимации булевых функций на основе биортогональных базисов. Для «нелинейного» базиса, задаваемого комбинацией линейных и бент-функций, получено выражение для радиуса покрытия обобщенного кода Адамара (теорема 16.4). Эта

величина (как и в случае «линейного» базиса) определяет возможности аппроксимации функций «нелинейным» базисом. В данном случае она совпала с радиусом покрытия классического кода Адамара, относительно линейных функций. Это свидетельствует о том, что возможности «нелинейной» аппроксимации не меньше, чем у «линейной». Получены также соотношения, связывающие коэффициенты Уолша-Адамара булевой функции и коэффициенты базисного разложения этой же функции относительно указанного выше комбинированного «нелинейного» базиса (лемма 16.5). Они могут быть использованы для вычисления параметров конкретных аппроксимаций.

Третья глава посвящена исследованию теоретико-автоматной модели обращения дискретных функций. Для данной математической модели рассмотрен наиболее общий вариант обращения. Обращение определяется как нахождение по известной выходной последовательности конечного автомата однозначно восстанавливаемых фрагментов соответствующей неизвестной входной последовательности этого автомата. Данный вариант обращения автор называет частичным обращением и для его реализации использует конечный инициальный автомат (так называемый частично обратный автомат - ЧО-автомат), однозначно определяемый исходным автоматом. Исследованы свойства графа ЧО-автомата, влияющие на параметры частичного обращения (теоремы 19.3 и 19.7, леммы 19.2 и 19.6, следствия 19.4 и 19.5). Для описания процесса частичного обращения конечного автомата без потери информации (БПИ-автомата) использована теоретико-вероятностная модель конечных цепей Маркова. Доказано (лемма 20.3), что при случайном и равновероятном выборе для БПИ-автомата пары (начальное состояние - входная последовательность) цепь Маркова, моделирующая функционирование ЧО-автомата является однородной. Приводятся результаты, описывающие ассимптотическое поведение математического ожидания случайной величины, равной доле однозначно восстанавливаемых входных символов БПИ-автомата (леммы 20.1-20.3,

теоремы 20.4 и 20.5). В частности, доказано, что доля однозначно восстанавливаемых входных символов для любого подавтомата не меньше, чем у исходного БПИ-автомата (теорема 20.6).

Для БПИ-автоматов рассмотрен также вариант частичного обращения, для которого позиция однозначно восстанавливаемого фрагмента в прообразе однозначно определяется появлением в соответствующем выходном слове специальных подслов-индикаторов. Данный вариант обращения назван локальным обращением. Получен критерий локальной обратимости. Для БПИ-автомата Мили вводится понятие ассоциированного с ним автомата без выхода. Доказано (теорема 21.10), что приведенный БПИ-автомат Мили обладает свойством локальной обратимости тогда и только тогда, когда ассоциированный с ним автомат без выхода обладает свойством синхронизируемости. Аналогичное утверждение доказано (теорема 22.6) для специального класса БПИ-автоматов - двоичных регистров сдвига с фильтрующими булевыми функциями. Получены достаточные условия локальной обратимости (теоремы 22.11, 22.16, 22.17) для этого вида автоматов.

В заключение третьей главы рассмотрены вопросы анализа и синтеза совершенно уравновешенных функций, используемых для построения БПИ-автоматов. Приведены результаты (теорема 24.6) исследований возможности синтеза совершенно уравновешенных функций с использованием конструкции сдвиг - композиции совершенно уравновешенных функций от меньшего числа переменных. Приведены примеры построения таких классов. Получена (теорема 25.2) теоретико-информационная характеризация класса совершенно уравновешенных функций.

В заключении сформулированы результаты диссертации.

Все перечисленные результаты являются новыми. Диссертация написана четким и понятным языком, результаты изложены корректно и имеют строгие математические доказательства. Необходимо отметить

значительное количество поясняющих примеров в тексте диссертации, положительно влияющих на восприятие излагаемых результатов

Вместе с тем имеются отдельные замечания:

1. В тексте диссертации используются избыточные понятия. Например (см.§22), определив неавтономный регистр со свойством синхронизируемости, автор использует далее понятие функции обратной связи этого регистра, обладающей свойством синхронизируемости.

2. В тексте диссертации используются одинаковые условные обозначения для разных операций (комплексное сопряжение - стр.89 и теоретико-множественное дополнение - стр.160).

3. В тексте диссертации имеет место небольшое количество опечаток.

Все указанные выше недостатки имеют частный характер и не влияют на общую положительную оценку диссертационной работы О.А.Логачева.

Заключение

В целом результаты диссертации О.А.Логачева можно квалифицировать как новое крупное научное достижение в области развития математических моделей и методов обеспечения информационной безопасности, а также совершенствования алгоритмов и методов решения фундаментальной научной проблемы обращения дискретных функций.

Научная новизна и практическая значимость результатов диссертационного исследования состоят в строго доказанных утверждениях и характеризуются следующими результатами.

Для широкого класса дискретных функций, определенных на произвольной конечной абелевой группе, разработана алгебраическая модель, обобщающая классические полиномиальные коды Рида-Маллера и позволяющая использовать преимущества полиномиального представления дискретных функций. Для этих функций удалось также корректно и содержательно определить и исследовать обобщение известного экстремального класса бент-функции. Для групповых функций предложено представление, обобщающее аффинное расщепление булевых отображений, и

исследованы его параметры. Предложена новая нормальная форма булевой функции — аффинная нормальная форма и получены соотношения, описывающие связи спектральных параметров булевой функции с параметрами представляющей ее аффинной нормальной формы. Указанные результаты вносят существенный вклад в развитие математических методов анализа дискретных функций.

Предложены новые подходы к изучению свойств булевых функций и отображений, исследованы новые семейства параметров булевых функций и их связи. Данные результаты вносят существенный вклад в развитие булевых моделей информационной безопасности, могут способствовать выбору оптимальных параметров дискретных функций, а также способствовать повышению обоснованности оценок уровня защиты информации.

Предложена и обоснована теоретико-автоматная модель обращения дискретных функций, исследованы свойства и параметры новых видов обращения - частичного обращения и локального обращения. Данные результаты могут быть использованы в анализе дискретных функций, представляющих собой последовательные композиции функций, а также способствовать развитию методов обращения дискретных функций, ассоциированных с конкретными средствами обеспечения ИБ.

Результаты диссертации опубликованы в 17 статьях в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 05.13.19 - «Методы и системы защиты информации, информационная безопасность» и индексируемых системами Web of Science и Scopus. Содержание автореферата соответствует диссертации.

На основании вышеизложенного считаю, что диссертация О.А.Логачева на тему «Построение и анализ эффективности алгоритмов обращения дискретных функций в математических моделях информационной безопасности» соответствует всем требованиям, установленным Московским государственным университетом имени М.В.Ломоносова к докторским диссертациям. Содержание диссертации соответствует паспорту

специальности 05.13.19 - «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 приложениям № 5, 6 Положения о диссертационном совете Московского государственного университета имени М.В.Ломоносова, а соискатель Логачев Олег Алексеевич заслуживает присуждения ему ученой степени доктора физико-математических наук по специальности 05.13.19 - «Методы и системы защиты информации, информационная безопасность» (физико-математические науки).

Официальный оппонент:
доктор технических наук, профессор, член-
корреспондент Академии криптографии
Российской Федерации [redacted] В.Г.Никонов

[redacted]

«25» ноября 2019г.

[redacted]

Подпись Никонова Владимира Глебовича
удостоверяю.

[redacted]

Управляющий делами аппарата президиума
Академии криптографии
Российской Федерации [redacted] А.Н.Андреев

«06» 12 2019г.