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»

Актуальность и значимость темы. Проблема получения и обоснования оценок уровня защиты информации является центральной в области обеспечения информационной безопасности (ИБ). Методы анализа средств (систем) обеспечения ИБ основаны на ряде разделов математики и используют математические модели, учитывающие возможности противника и угрозы ИБ.

Фундаментальной математической проблемой анализа средств обеспечения ИБ является построение алгоритмов обращения (инвертирования) определенного класса дискретных функций, ассоциированных с этими средствами и определяющих их свойства. Под задачей обращения дискретной функции понимается вычисление значения аргумента, принадлежащего полному прообразу заданного значения функции. Решение этой задачи моделирует действия противника, направленные на вскрытие системы защиты. Характеристики алгоритмов обращения дискретных функций (трудоемкость, надежность, объем используемой память и др.) определяют оценку уровня защиты информации с помощью системы, построенной на основе данных дискретных функций.

Качество предлагаемых решений по проблемам построения и анализа алгоритмов обращения дискретных функций определяется уровнем используемого математического аппарата. В связи с этим актуальными как с теоретической, так и с практической точек зрения являются направления исследований, представленные в диссертации. Заявленная диссертантом цель определена как совершенствование математических моделей и повышение на их основе полученных результатов эффективности алгоритмов (методов) решения задач обращения дискретных функций, используемых при синтезе средств обеспечения информационной безопасности.

Тема, объект и предмет исследований диссертации соответствуют паспорту специальности 05.13.19 - «Методы и системы защиты информации, информационная безопасность» по следующим областям исследований.

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

9. Модели и методы получения 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.

Результаты исследования базируются на фундаментальных положениях алгебры, дискретной математики, теории вероятностей, математического анализа, теории алгоритмов и теории кодирования.

Краткая характеристика основного содержания диссертации. Работа состоит из введения, трех глав, заключения, списка литературы и пяти приложений. Суммарный объем диссертации составляет 297 страниц. Список цитируемой литературы содержит 182 наименования.

В первой главе развивается математический аппарат анализа алгебраических, комбинаторных, криптографических свойств и параметров функций, заданных на конечных абелевых группах. На основе дифференциально-разностного подхода для широкого класса комплекснозначных функций на конечных абелевых группах построены 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). Приведены необходимые и достаточные условия на абелеву группу, при которых любая функция из данного класса является аналогом полинома (следствие 3.9). Введенная автором система параметров (координатизация) адекватно описывает свойства исследуемых функций, что позволяет успешно выделить в данном классе функций экстремальный подкласс, соответствующий экстремальному классу классических бент-функций, заданных на элементарных абелевых 2-группах (теоремы 5.3, 5.6, 5.8, 5.10, лемма 5.12, следствия 5.4, 5.9, 5.11).

Для групповых функций, определенных на произвольных конечных абелевых группах, выделено семейство параметров ($\deg(f)$, $ih(g)$, $\mu l(g)$ и др.), характеризующих «нелинейность» функции и эффективность соответствующих методов обращения, доказан ряд соотношений, связывающих эти параметры (теоремы 7.6, 7.7, лемма 7.5, следствие 7.8).

В рамках дифференциально-разностного подхода для булевых функций исследованы понятия невырожденности и структуры вырождения функции (теорема 8.6, лемма 8.4, предложения 8.2, 8.3, 8.5).

В порядке обобщения понятия дуальности для линейных блочных кодов получены результаты, направленные на поиск аналогий между

конечными модулями и векторными пространствами. На языке теории решеток получены соотношения (теорема 4.5, следствие 4.6), обобщающие известное тождество Мак-Вильямс для дуальных линейных блочных кодов.

На основе использования так называемого циклотомически приведенного полинома уточнена оценка Вейля для сумм аддитивных характеров конечных полей (теоремы 6.5, 6.6).

Вторая глава посвящена характеризации булевых функций с помощью семейств подфункций. Введено понятие (H,u)-стабильности булевой функции (H-аффинное подпространство пространства Хэмминга). Доказан критерий (H,u)-стабильности функции (теорема 12.8), позволяющий построить семейства подпространств, на которых данная функция стабильна. На основе свойства (H,u)-стабильности получена (теорема 12.15) новая характеризация (критерий) свойства корреляционной иммунности.

Исследованы сужения булевых функций на области, называемые локальными аффинностями (в них функция совпадает с аффинной функцией), что важно для сведения исходной нелинейной задачи к некоторой линейной задаче.

Доказано, что асимптотически при стремлении числа переменных к бесконечности уровень аффинности и обобщенный уровень аффинности (обе величины определяются фиксациями константами некоторых переменных) принимают не более двух возможных значений (теоремы 14.8, 14.10, следствие 14.9, замечание 14.11).

Для булевых функций предложена нормальная форма (АффНФ), определяемая разбиениями пространства Хэмминга на локальные аффинности функции. Структура и особенности АффНФ могут быть использованы для вычисления некоторых параметров булевых функций и для описания некоторых классов бент-функций.

Для платовидных функций (этот класс содержит бент-функции) получена верхняя оценка размерности локальной аффинности, определяемая числом переменных и порядком платовидности функции.

Исследована «нелинейная» аппроксимация булевых функций на основе биортогональных базисов. Для «нелинейного» базиса, являющегося комбинацией линейных и бент-функций, получено выражение для радиуса покрытия обобщенного кода Адамара (теорема 16.4). Эта важная для «нелинейной» аппрксимации величина совпала с радиусом покрытия классического кода Адамара, относительно линейных функций.

В третьей главе исследована проблема обращения дискретных функций с помощью теоретико-автоматных моделей. В условиях «обращения»,

трактуемого как нахождение по известной выходной последовательности конечного автомата однозначно восстанавливаемых фрагментов неизвестной входной последовательности использован конечный инициальный частично обратный (ЧО) автомат, однозначно определяемый исходным автоматом. Исследованы свойства графа ЧО-автомата, определяющие параметры частичного обращения. С использованием естественной вероятностной модели оценена доля однозначно восстанавливаемых входных символов автомата без потери информации (БПИ-автомата) и его подавтоматов.

Для БПИ-автоматов исследовано частичное обращение, при котором позиция (локализация) однозначно восстанавливаемого фрагмента в прообразе точно определена специальными подсловами-индикаторами в выходном слове. Доказано (теорема 21.10), что приведенный БПИ-автомат Мили локально обратим тогда и только тогда, когда ассоциированный с ним автомат без выхода является синхронизируемым.

Исследован синтез совершенно уравновешенных функций с помощью конструкции сдвиг — композиции совершенно уравновешенных функций от меньшего числа переменных, приводятся примеры построения. Для класса совершенно уравновешенных функций получена теоретико-информационная характеризация (теорема 25.2).

Наиболее интересными в теоретическом и практическом отношении мне представляются следующие результаты:

- по 1-й главе – уточнение оценки Вейля для сумм аддитивных характеров конечных полей;
- по 2-й главе – критерий (H,u)-стабильности булевой функции и свойства нормальной формы АффНФ, определяемой разбиениями пространства Хэмминга на локальные аффинности функции;
- по 3-й главе – результаты по частичному обращению автоматов.

Научная новизна и практическая значимость результатов исследований. Выносимые на защиту результаты диссертации являются новыми, совокупность их составляет крупное научное достижение в области развития математических моделей, используемых для решения проблемы обращения дискретных функций, являющейся определяющей для обеспечения безопасности информационных систем.

Представленные в диссертации теоретические результаты затрагивают весьма широкий спектр специальных свойств дискретных функций, что показывает широкую научную эрудицию диссертанта.

Актуальность результатов диссертации определяется их направленностью на совершенствование методов обращения дискретных

функций и в конечном счете на повышение обоснованности оценок уровня безопасности широкого класса информационных систем. Некоторые результаты диссертации могут быть использованы при подготовке учебных пособий и лекционных курсов по дисциплинам, связанным с информационной безопасностью.

Работа написана на хорошем математическом уровне, все утверждения в диссертации доказаны или снабжены ссылками. Научные положения, выводы и рекомендации диссертационной работы обоснованы. Достоверность выносимых на защиту результатов подтверждена как приведенными в публикациях математическими доказательствами, так и апробацией результатов с помощью докладов автора на соответствующих данной тематике математических конференциях и семинарах.

Представленные в диссертации исследования соответствуют Паспорту специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность». Автореферат соответствует диссертации и с достаточной полнотой отражает ее содержание. Заявленная цель диссертации автором достигнута.

Вместе с тем, по работе имеются замечания:

1. Стоило бы в тексте разъяснить более детально связь некоторых полученных результатов с проблемой обращения дискретных функций (например, результатов по Δ-эквивалентности и глобальным лавинным характеристикам булевых функций).

2. Усилением диссертации были бы результаты по вычислительной сложности распознавания свойств и оценки характеристик дискретных функций, важных для решения задач обращения (например, дать оценки вычислительной сложности построения АффНФ для различных классов булевых функций или оценить возможное снижение сложности задачи обращения при использовании АффНФ).

3. В тексте диссертации имеются повторы (определения БПИ-автомата на стр.197 и 205), небольшое количество опечаток.

Данные замечания не снижают существенно общего положительного впечатления от диссертационной работы.

Заключение по диссертации. Диссертация Логачева Олега Алексеевича на тему «Построение и анализ эффективности алгоритмов обращения дискретных функций в математических моделях информационной безопасности» удовлетворяет требованиям, установленным Московским государственным университетом имени М.В. Ломоносова к докторским диссертациям по физико-математическим наукам, а также критериям,

определенным пп. 2.1-2.5 Положения о присуждении ученых степеней в МГУ им. М.В. Ломоносова, оформлена согласно приложениям № 5, 6 Положения о диссертационном совете МГУ им. М.В. Ломоносова.

Считаю, что 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:
профессор кафедры «Информационная безопасность»
Федерального государственного образовательного бюджетного учреждения высшего образования «Финансовый университет при Правительстве Российской Федерации»,
доктор физико-математических наук по специальности 05.13.19 - «Методы и системы защиты информации, информационная безопасность»,
профессор [redacted] В.М. Фомичев

адрес: 125468, г. Москва, Ленинградский проспект, 49,
[redacted] e-mail: vmfomichev@fa.ru.
26 ноября 2019 года

[redacted]

Подпись Фомичева В
Зам. начальника
УКО [redacted]

Я, Фомичев Владимир Михайлович, даю согласие на включение своих персональных данных в документы, связанные с защитой диссертации Логачева О. А., и на их дальнейшую обработку.