**Логачев Олег Алексеевич Построение и анализ эффективности алгоритмов обращения дискретных функций в математических моделях информационной безопасности**

ОГЛАВЛЕНИЕ ДИССЕРТАЦИИ

доктор наук Логачев Олег Алексеевич

Введение

Глава 1. Алгебраические, комбинаторные и метрические

характеристики дискретных функций, используемые в методах (алгоритмах) обращения

§1 Групповые дискретные функции

§2 Комплекснозначные функции на конечных абелевых группах и

их свойства

§3 Групповые коды Рида-Маллера и их свойства

§4 Понятие дуальности для конечных модулей. Обобщённые

тождества Мак-Вильямс

§5 Бент-функции на конечной абелевой группе

§6 сг-полиномы и приведенная оценка Вейля

§7 Некоторые характеристики "нелинейности" групповых

отображений

§8 Невырожденные булевы функции

§9 Пространства линейных трансляторов и пустые секции

Фурье-кластеризации булевых функций

§10 Д-эквивалентность и глобальные лавинные характеристики

булевых функций

Глава 2. О связях алгебраических, комбинаторных и

криптографических свойств булевых функций со свойствами их сужений

§11 Сужения булевых функций

§12 Наследование комбинаторных и спектральных свойств при

сужении булевых функций. (Н, ^-стабильность

§13 Аффинные сужения булевых функций и отображений. Понятие

локальной аффинности

§14 Локальные аффинности булевых функций, связанные с

фиксацией переменных

§15 Аффинная нормальная форма булевой функции и ее свойства . . 164 §16 Нелинейная аппроксимация булевых функций

Глава 3. Математические модели обращения дискретных

функций

§17 Задача обращения дискретных функций в обеспечении

информационной безопасности

§18 Теоретико-автоматная модель для задачи обращения

§19 Частично обратный автомат

§20 Асимптотическое поведение характеристик частичного

обращения для БПИ-автоматов

§21 Локальное обращение БПИ-автоматов

§22 Локальное обращение неавтономных регистров сдвига с

фильтрующими функциями

§23 Локальные аффинности в задачах обращения дискретных

функций

§24 Синтез совершенно уравновешенных функций на основе

операции "сдвиг-композиция"

§25 Теоретико-информационная характеризация совершенно

уравновешенных функций

Заключение

Список литературы

Приложение А. Некоторые примитивы, используемые при

синтезе средств обеспечения информационной безопасности

Приложение Б. Аффинная нормальная форма фильтрующей

функции генератора псевдослучайных последовательностей шифра ЫЫ-128

Приложение В. Локальные аффинности булевых отображений

Приложение Г. Аффинное обращение

ограниченно-детерминированных функций, реализуемых конечными автоматами вида

БК(пЛ)