Содержание

Предисловие автора 3

Основные обозначения 4

1. Корреляционная иммунность булевых функций 6
   1.1. Вес функции 6
   1.2. Алгебраическая нормальная форма булевой функции 7
   1.3. Линейные и квазилинейные переменные 12
   1.4. Понятие корреляционной иммунности 13
   1.5. Неравенство Зигенталера 18
   1.6. Преобразование Уолша — Адамара 20
   1.7. Тесты статистической независимости и корреляционной иммунности 26
   Вопросы и задачи 32

2. Нелинейность булевых функций 34
   2.1. Определение и свойства нелинейности 34
   2.2. Бент-функции 36
   2.3. Совершенная нелинейность 41
   2.4. Нелинейность корреляционно-иммунных функций . 46
   Вопросы и задачи 49

3. Лавинные характеристики булевых функций 51
   3.1. Автокорреляция и взаимная корреляция 51
   3.2. Строгий лавинный критерий 53
   3.3. Критерий распространения 56
   3.4. Глобальные лавинные характеристики 57
   3.5. Частично бент-функции 59
   Вопросы и задачи 61

4. Алгебраическая иммунность 62
   4.1. Алгебраическая атака 62
   4.2. Понятие алгебраической иммунности 63
   Вопросы и задачи 66

5. Запреты булевых функций 67

6. Алгоритмические аспекты 70
6.1. Вычисление веса функции 70
6.2. Преобразование Мёбиуса 74
6.3. Преобразование Уолша — Адамара 76

7. Решения некоторых задач 79
Глава 1 79
Глава 2 80
Глава 3 83
Глава 4 84

Литература 86