

А
Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Оренбургский государственный университет»

Т.М. Отрыванкина, А.Н. Благовисная

КРИПТОГРАФИЧЕСКИЕ СВОЙСТВА БУЛЕВЫХ ФУНКЦИЙ

Рекомендовано Редакционно-издательским советом федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Оренбургский государственный университет» в качестве методических указаний для студентов, обучающихся по программам высшего профессионального образования по направлениям подготовки 010400.62 Прикладная математика и информатика, 010500.62 Математическое обеспечение и администрирование информационных систем и специальности 090301.65 Компьютерная безопасность

Оренбург
2014

А

УДК 519.7 (076.5)
ББК 22.18я7
О 86

Рецензент – профессор, доктор физико-математических наук С.А. Пихтильков

Отрыванкина, Т.М.

О 86 Криптографические свойства булевых функций: методические указания / Т.М. Отрыванкина, А.Н. Благовисная; Оренбургский гос. ун-т. – Оренбург: ОГУ, 2014. – 55 с.

Методические указания содержат материал, предназначенный для самостоятельной работы студентов в процессе изучения криптографических булевых функций.

Методические указания предназначены для студентов, обучающихся по направлениям подготовки 010400.62 Прикладная математика и информатика, 010500.62 Математическое обеспечение и администрирование информационных систем и специальности 090301.65 Компьютерная безопасность, и составлены в соответствии с утвержденными рабочими программами дисциплин, связанных с математическими методами защиты информации. Они могут использоваться и на других направлениях математического профиля и направлениях, связанных с защитой информации.

УДК 519.7 (076.5)
ББК 22.18я7

© Отрыванкина Т.М.,
Благовисная А.Н., 2014
© ОГУ, 2014

Содержание

Введение	4
1 Определения, числовые и метрические характеристики булевых функций.....	6
1.1 Определение булевой функции, способы задания	6
1.2 Алгебраическая нормальная форма	9
1.3 Алгебраическая степень булевой функции	12
1.4 Вес булевой функции.....	13
1.5 Расстояние между булевыми функциями.....	14
1.6 Преобразования Фурье и Уолша-Адамара	16
1.7 Понятие эквивалентных булевых функций.....	21
1.8 Понятие булевых отображений	23
2 Криптографические свойства булевых функций	25
2.1 Высокая алгебраическая степень.....	26
2.2 Нелинейность.....	26
2.3 Уравновешенность	30
2.4 Устойчивость	31
2.5 Корреляционная иммунность	32
2.6 Алгебраическая иммунность.....	34
2.7 Критерии распространения	36
3 Примеры булевых функций, применяемых в криптографических конструкциях ..	39
4 Рекомендации для дальнейшего изучения криптографических булевых функций	42
Список использованных источников	44
Приложение А Ответы и указания	48
Приложение Б Вопросы для самопроверки.....	52
Приложение В Примерные направления учебно-исследовательской работы студентов по криптографическим булевым функциям	55