

Секция «Прикладная дискретная математика»

ДАМЕН Й., РЭМЕН В.

**РАЗРАБОТКА RIJNDAEL:
AES — ПЕРСПЕКТИВНЫЙ СТАНДАРТ
ШИФРОВАНИЯ¹⁾**

Содержание

Глава 7.	Корреляционные матрицы	291
§ 7.1.	Преобразование Уолша–Адамара	291
7.1.1.	Линейные комбинации и выборочные шаблоны	291
7.1.2.	Корреляции	292
7.1.3.	Вещественнозначное представление булевой функции	292
7.1.4.	Ортогональность и корреляция	292
7.1.5.	Спектр двоичной булевой функции	293
§ 7.2.	Составные булевы функции	295
7.2.1.	Сумма по модулю два (XOR) двух булевых функций	295
7.2.2.	Логическое произведение (AND) двух булевых функций	295
7.2.3.	Ортогональные булевы функции	296
§ 7.3.	Корреляционные матрицы	296
7.3.1.	Эквивалентность булевого отображения и корреляционной матрицы	297
7.3.2.	Итеративные булевы отображения	298
7.3.3.	Булевы преобразования	298
§ 7.4.	Булевы отображения специального вида	300
7.4.1.	Сложение с константой	300
7.4.2.	Линейные отображения	300
7.4.3.	Отображения с блочной структурой	300
§ 7.5.	Производные свойства	301
§ 7.6.	Усеченные функции	302
§ 7.7.	Взаимная корреляция и автокорреляция	303
§ 7.8.	Линейные цепочки	304

© Редакция журнала «ОПиПМ» и Научное издательство «ТВП», перевод на русский язык с разрешения Springer-Verlag — владельца прав на издание оригинала. 2016 г.

¹⁾ От Редакции. Продолжаем публикацию журнальной редакции перевода И. В. Харламова на русский язык книги «Разработка Rijndael: AES — перспективный стандарт шифрования». Запланировано, что после завершения публикации журнальной редакции будет осуществлено издание полного перевода в форме защищенной от копирования π -книги (Портативной Интерактивной книги), а впоследствии Редакция намерена издать ее как очередной том в серии «Прогресс теоретической и прикладной дискретной математики».

(Продолжение примечания см. на с. 290.)

§ 7.9. Применение к шифрам	305
7.9.1. Общий случай	305
7.9.2. Шифр с чередующимся прибавлением ключа	306
7.9.3. Усреднение по всем раундовым ключам.	307
7.9.4. Роль ключевой развертки	308
§ 7.10. Литература по корреляционным матрицам и линейному криптоанализу	311
7.10.1. Линейный криптоанализ шифра DES	311
7.10.2. Линейные оболочки	313
§ 7.11. Выводы	315
Список литературы к гл. 7	316

Начатая во втором выпуске этого года вводными «Гл. 1. Процесс разработки и принятия перспективного стандарта шифрования (AES)» и «Гл. 2. Начальные сведения» и продолженная в третьем выпуске тома 23 (2016) («Гл. 3. Описание алгоритма Rijndael», «Гл. 4. Вопросы реализации», «Гл. 5. Принципы конструирования», «Гл. 6. Стандарт шифрования данных (DES)»), публикация будет далее продолжена в выпусках 4 и 6 («Гл. 8. Разностные соотношения» и «Гл. 9. Стратегия «широкого хвоста»»), и в первом выпуске тома 24 (2017) («Гл. 10. Результаты криптоанализа» и «Гл. 11. Родственные блочные шифры»).

Издание каждого отрывка книги сопровождается списком упомянутых в ней литературных источников.