

Секция «Прикладная дискретная математика»

ДАМЕН Й., РЭМЕН В.

РАЗРАБОТКА RIJNDAEL:
AES — ПЕРСПЕКТИВНЫЙ СТАНДАРТ
ШИФРОВАНИЯ ¹⁾

Содержание

Глава 10. Результаты криптоанализа	5
§ 10.1. Сокращенные дифференциалы	5
§ 10.2. Атаки насыщением	6
10.2.1. Предварительные замечания.	6
10.2.2. Базовый вариант атаки	7
10.2.3. Роль финального раунда	8
10.2.4. Распространение на последующий раунд.	9
10.2.5. Распространение на предшествующий раунд.	10
10.2.6. Атаки на шесть раундов шифра	10
10.2.7. Атака по совокупности	11
§ 10.3. Атака Гилберта -Миниера	12
10.3.1. Критерий для 4 раундов.	12
10.3.2. Атака на семь раундов	12
§ 10.4. Интерполяционные атаки	13
§ 10.5. Симметрия и слабые ключи (применительно к DES).	14
§ 10.6. Слабые ключи (применительно к IDEA).	14
§ 10.7. Атаки с использованием связанных ключей	15
§ 10.8. Атаки, использующие особенности реализации шифра	15
10.8.1. Атаки по времени реализации	16
10.8.2. Анализ энергопотребления	16
§ 10.8. Заключение	19
Глава 11. Родственные блочные шифры.	20
§ 11.1. Обзор	20
11.1.1. Эволюция.	20
11.1.2. Раундовое преобразование.	21
§ 11.2. Шифр SHARK	23
§ 11.3. Шифр Square.	25

© Редакция журнала «ОПИИМ» и Научное издательство «ТВИ», перевод на русский язык с разрешения Springer-Verlag владельца прав на издание оригинала. 2017 г.

¹⁾ От Редакции. Завершаем 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. 4.)

§ 11.4. Шифр BKSQ	28
§ 11.5. Потомки шифра Rijndael	30
11.5.1. Шифр Crypton	31
11.5.2. Шифр Twofish	31
11.5.3. Шифр ANUBIS	32
11.5.4. Шифр GRAND CRU	32
11.5.5. Семейство шифров Hierocrypt	33
§ 11.6. Заключение	33
Список литературы к гл. 10 и 11	34