

Joan Daemen • Vincent Rijmen

The Design of Rijndael

AES – The Advanced Encryption Standard

With 48 Figures and 17 Tables



Springer

Contents

1. The Advanced Encryption Standard Process	1
1.1 In the Beginning	1
1.2 AES: Scope and Significance	1
1.3 Start of the AES Process	2
1.4 The First Round	3
1.5 Evaluation Criteria	4
1.5.1 Security	4
1.5.2 Costs	4
1.5.3 Algorithm and Implementation Characteristics	4
1.6 Selection of Five Finalists	5
1.6.1 The Second AES Conference	5
1.6.2 The Five Finalists	6
1.7 The Second Round	7
1.8 The Selection	7
2. Preliminaries	9
2.1 Finite Fields	10
2.1.1 Groups, Rings, and Fields	10
2.1.2 Vector Spaces	11
2.1.3 Fields with a Finite Number of Elements	13
2.1.4 Polynomials over a Field	13
2.1.5 Operations on Polynomials	14
2.1.6 Polynomials and Bytes	15
2.1.7 Polynomials and Columns	16
2.2 Linear Codes	17
2.2.1 Definitions	17
2.2.2 MDS codes	19
2.3 Boolean Functions	19
2.3.1 Bundle Partitions	20
2.3.2 Transpositions	21
2.3.3 Bricklayer Functions	22
2.3.4 Iterative Boolean Transformations	22
2.4 Block Ciphers	23
2.4.1 Iterative Block Ciphers	24

2.4.2	Key-Alternating Block Ciphers	25
2.5	Block Cipher Modes of Operation	27
2.5.1	Block Encryption Modes	27
2.5.2	Key-Stream Generation Modes	27
2.5.3	Message Authentication Modes	28
2.5.4	Cryptographic Hashing	29
2.6	Conclusions	29
3.	Specification of Rijndael	31
3.1	Differences between Rijndael and the AES	31
3.2	Input and Output for Encryption and Decryption	31
3.3	Structure of Rijndael	33
3.4	The Round Transformation	33
3.4.1	The SubBytes Step	34
3.4.2	The ShiftRows Step	37
3.4.3	The MixColumns Step	38
3.4.4	The Key Addition	40
3.5	The Number of Rounds	41
3.6	Key Schedule	43
3.6.1	Design Criteria	43
3.6.2	Selection	43
3.7	Decryption	45
3.7.1	Decryption for a Two-Round Rijndael Variant	45
3.7.2	Algebraic Properties	46
3.7.3	The Equivalent Decryption Algorithm	48
3.8	Conclusions	50
4.	Implementation Aspects	53
4.1	8-Bit Platforms	53
4.1.1	Finite Field Multiplication	53
4.1.2	Encryption	54
4.1.3	Decryption	55
4.2	32-Bit Platforms	56
4.3	Dedicated Hardware	59
4.3.1	Decomposition of S_{RD}	60
4.3.2	Efficient Inversion in $GF(2^8)$	61
4.4	Multiprocessor Platforms	61
4.5	Performance Figures	62
4.6	Conclusions	62
5.	Design Philosophy	63
5.1	Generic Criteria in Cipher Design	63
5.1.1	Security	63
5.1.2	Efficiency	64
5.1.3	Key Agility	64

5.1.4	Versatility	64
5.1.5	Discussion	64
5.2	Simplicity	65
5.3	Symmetry	65
5.3.1	Symmetry Across the Rounds	66
5.3.2	Symmetry Within the Round Transformation	66
5.3.3	Symmetry in the D-box	67
5.3.4	Symmetry and Simplicity in the S-box	68
5.3.5	Symmetry between Encryption and Decryption	68
5.3.6	Additional Benefits of Symmetry	68
5.4	Choice of Operations	69
5.4.1	Arithmetic Operations	70
5.4.2	Data-Dependent Shifts	70
5.5	Approach to Security	71
5.5.1	Security Goals	71
5.5.2	Unknown Attacks Versus Known Attacks	72
5.5.3	Provable Security Versus Provable Bounds	73
5.6	Approaches to Design	73
5.6.1	Non-Linearity and Diffusion Criteria	73
5.6.2	Resistance against Differential and Linear Cryptanalysis	73
5.6.3	Local Versus Global Optimization	74
5.7	Key-Alternating Cipher Structure	76
5.8	The Key Schedule	76
5.8.1	The Function of a Key Schedule	76
5.8.2	Key Expansion and Key Selection	77
5.8.3	The Cost of the Key Expansion	77
5.8.4	A Recursive Key Expansion	78
5.9	Conclusions	79
6.	The Data Encryption Standard	81
6.1	The DES	81
6.2	Differential Cryptanalysis	83
6.3	Linear Cryptanalysis	85
6.4	Conclusions	87
7.	Correlation Matrices	89
7.1	The Walsh-Hadamard Transform	89
7.1.1	Parities and Selection Patterns	89
7.1.2	Correlation	89
7.1.3	Real-valued Counterpart of a Binary Boolean Function	90
7.1.4	Orthogonality and Correlation	90
7.1.5	Spectrum of a Binary Boolean Function	91
7.2	Composing Binary Boolean Functions	93
7.2.1	XOR	93
7.2.2	AND	93

7.2.3	Disjunct Boolean Functions	94
7.3	Correlation Matrices	94
7.3.1	Equivalence of a Boolean Function and its Correlation Matrix	95
7.3.2	Iterative Boolean Functions	96
7.3.3	Boolean Permutations	96
7.4	Special Boolean Functions	98
7.4.1	XOR with a Constant	98
7.4.2	Linear Functions	98
7.4.3	Bricklayer Functions	98
7.5	Derived Properties	99
7.6	Truncating Functions	100
7.7	Cross-correlation and Autocorrelation	101
7.8	Linear Trails	102
7.9	Ciphers	103
7.9.1	General Case	103
7.9.2	Key-Alternating Cipher	104
7.9.3	Averaging over all Round Keys	105
7.9.4	The Effect of the Key Schedule	106
7.10	Correlation Matrices and Linear Cryptanalysis Literature	108
7.10.1	Linear Cryptanalysis of the DES	108
7.10.2	Linear Hulls	109
7.11	Conclusions	111
8.	Difference Propagation	113
8.1	Difference Propagation	113
8.2	Special Functions	114
8.2.1	Affine Functions	114
8.2.2	Bricklayer Functions	114
8.2.3	Truncating Functions	115
8.3	Difference Propagation Probabilities and Correlation	115
8.4	Differential Trails	117
8.4.1	General Case	117
8.4.2	Independence of Restrictions	117
8.5	Key-Alternating Cipher	118
8.6	The Effect of the Key Schedule	119
8.7	Differential Trails and Differential Cryptanalysis Literature	119
8.7.1	Differential Cryptanalysis of the DES Revisited	119
8.7.2	Markov Ciphers	120
8.8	Conclusions	122

9. The Wide Trail Strategy	123
9.1 Propagation in Key-alternating Block Ciphers	123
9.1.1 Linear Cryptanalysis	123
9.1.2 Differential Cryptanalysis	125
9.1.3 Differences between Linear Trails and Differential Trails	126
9.2 The Wide Trail Strategy	126
9.2.1 The $\gamma\lambda$ Round Structure in Block Ciphers	127
9.2.2 Weight of a Trail	129
9.2.3 Diffusion	130
9.3 Branch Numbers and Two-Round Trails	131
9.3.1 Derived Properties	133
9.3.2 A Two-Round Propagation Theorem	133
9.4 An Efficient Key-Alternating Structure	134
9.4.1 The Diffusion Step θ	134
9.4.2 The Linear Step Θ	136
9.4.3 A Lower Bound on the Bundle Weight of Four-Round Trails	136
9.4.4 An Efficient Construction for Θ	137
9.5 The Round Structure of Rijndael	138
9.5.1 A Key-Iterated Structure	138
9.5.2 Applying the Wide Trail Strategy to Rijndael	142
9.6 Constructions for θ	143
9.7 Choices for the Structure of $\mathcal{I}$ and π	145
9.7.1 The Hypercube Structure	145
9.7.2 The Rectangular Structure	147
9.8 Conclusions	147
10. Cryptanalysis	149
10.1 Truncated Differentials	149
10.2 Saturation Attacks	149
10.2.1 Preliminaries	150
10.2.2 The Basic Attack	150
10.2.3 Influence of the Final Round	152
10.2.4 Extension at the End	153
10.2.5 Extension at the Beginning	153
10.2.6 Attacks on Six Rounds	153
10.2.7 The Herds Attack	154
10.3 Gilbert–Minier Attack	154
10.3.1 The Four-Round Distinguisher	154
10.3.2 The Attack on Seven Rounds	155
10.4 Interpolation Attacks	156
10.5 Symmetry Properties and Weak Keys as in the DES	156
10.6 Weak keys as in IDEA	157
10.7 Related-Key Attacks	157
10.8 Implementation Attacks	157

10.8.1	Timing Attacks	157
10.8.2	Power Analysis	158
10.9	Conclusion	160
11.	Related Block Ciphers	161
11.1	Overview	161
11.1.1	Evolution	161
11.1.2	The Round Transformation	162
11.2	SHARK	163
11.3	Square	165
11.4	BKSQ	168
11.5	Children of Rijndael	171
11.5.1	Crypton	171
11.5.2	Twofish	172
11.5.3	ANUBIS	172
11.5.4	GRAND CRU	173
11.5.5	Hierocrypt	173
11.6	Conclusion	173

Appendices

A.	Propagation Analysis in Galois Fields	175
A.1	Functions over $\text{GF}(2^n)$	176
A.1.1	Difference Propagation	177
A.1.2	Correlation	177
A.1.3	Functions that are Linear over $\text{GF}(2^n)$	179
A.1.4	Functions that are Linear over $\text{GF}(2)$	180
A.2	Functions over $(\text{GF}(2^n))^\ell$	181
A.2.1	Difference Propagation	182
A.2.2	Correlation	182
A.2.3	Functions that are Linear over $\text{GF}(2^n)$	182
A.2.4	Functions that are Linear over $\text{GF}(2)$	183
A.3	Representations of $\text{GF}(p^n)$	184
A.3.1	Cyclic Representation of $\text{GF}(p^n)$	184
A.3.2	Vector Space Representation of $\text{GF}(p^n)$	184
A.3.3	Dual Bases	185
A.4	Boolean Functions and Functions in $\text{GF}(2^n)$	186
A.4.1	Differences in $\text{GF}(2)^n$ and $\text{GF}(2^n)$	186
A.4.2	Relationship Between Trace Patterns and Selection Patterns	187
A.4.3	Relationship Between Linear Functions in $\text{GF}(p)^n$ and $\text{GF}(p^n)$	187
A.4.4	Illustration	190
A.5	Rijndael-GF	192

B. Trail Clustering	195
B.1 Transformations with Maximum Branch Number	196
B.2 Bounds for Two Rounds	199
B.2.1 Difference Propagation	200
B.2.2 Correlation	202
B.3 Bounds for Four Rounds	204
B.4 Two Case Studies	205
B.4.1 Differential Trails.....	205
B.4.2 Linear Trails.....	207
C. Substitution Tables	211
C.1 <code>SRD</code>	211
C.2 Other Tables.....	212
C.2.1 <code>xtime</code>	212
C.2.2 Round Constants.....	212
D. Test Vectors	215
D.1 <code>KeyExpansion</code>	215
D.2 <code>Rijndael(128,128)</code>	215
D.3 Other Block Lengths and Key Lengths	217
E. Reference Code	221
Bibliography	229
Index	235