Information Security and Cryptography

Series Editors

David Basin
Kenny Paterson

Advisory Board

Michael Backes
Gilles Barthe
Ronald Cramer
Ivan Damgård
Andrew D. Gordon
Joshua D. Guttman
Christopher Kruegel
Ueli Maurer
Tatsuaki Okamoto
Adrian Perrig
Bart Preneel

More information about this series at http://www.springer.com/series/4752

Joan Daemen • Vincent Rijmen

The Design of Rijndael

The Advanced Encryption Standard (AES)

Second Edition

Springer

Joan Daemen
Digital Security Group
Radboud University Nijmegen
Nijmegen, The Netherlands

Vincent Rijmen
COSIC Group
KU Leuven
Heverlee, Belgium

ISSN 1619-7100 ISSN 2197-845X (electronic)
Information Security and Cryptography
ISBN 978-3-662-60768-8 ISBN 978-3-662-60769-5 (eBook)
https://doi.org/10.1007/978-3-662-60769-5

© Springer-Verlag GmbH Germany, part of Springer Nature 2002, 2020
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer-Verlag GmbH, DE part of Springer Nature.
The registered company address is: Heidelberger Platz 3, 14197 Berlin, Germany

Foreword

Rijndael was the surprise winner of the contest for the new Advanced Encryption Standard (AES) for the United States. This contest was organized and run by the National Institute of Standards and Technology (NIST) beginning in January 1997; Rijndael was announced as the winner in October 2000. It was the "surprise winner" because many observers (and even some participants) expressed scepticism that the US government would adopt as an encryption standard any algorithm that was not designed by US citizens.

Yet NIST ran an open, international, selection process that should serve as a model for other standards organizations. For example, NIST held their 1999 AES meeting in Rome, Italy. The five finalist algorithms were designed by teams from all over the world.

In the end, the elegance, efficiency, security, and principled design of Rijndael won the day for its two Belgian designers, Joan Daemen and Vincent Rijmen, over the competing finalist designs from RSA, IBM, Counterpane Systems, and an English/Israeli/Danish team.

This book is the story of the design of Rijndael, as told by the designers themselves. It outlines the foundations of Rijndael in relation to the previous ciphers the authors have designed. It explains the mathematics needed to understand the operation of Rijndael, and it provides reference C code and test vectors for the cipher.

Most importantly, this book provides justification for the belief that Rijndael is secure against all known attacks. The world has changed greatly since the DES was adopted as the national standard in 1976. Then, arguments about security focused primarily on the length of the key (56 bits). Differential and linear cryptanalysis (our most powerful tools for breaking ciphers) were then unknown to the public. Today, there is a large public literature on block ciphers, and a new algorithm is unlikely to be considered seriously unless it is accompanied by a detailed analysis of the strength of the cipher against at least differential and linear cryptanalysis.

This book introduces the "wide trail" strategy for cipher design, and explains how Rijndael derives strength by applying this strategy. Excellent resistance to differential and linear cryptanalysis follows as a result. High efficiency is also a result, as relatively few rounds are needed to achieve strong security.

The adoption of Rijndael as the AES is a major milestone in the history of cryptography. It is likely that Rijndael will soon become the most widely used cryptosystem in the world. This wonderfully written book by the designers themselves is a “must read” for anyone interested in understanding this development in depth.

Ronald L. Rivest
Viterbi Professor of Computer Science
MIT

Preface

This book is about the design of Rijndael, the block cipher that became the Advanced Encryption Standard (AES). According to the 'Handbook of Applied Cryptography' [110], a block cipher can be described as follows:

> A block cipher is a function which maps n-bit plaintext blocks to n-bit ciphertext blocks; n is called the block length. [...] The function is parameterized by a key.

Although block ciphers are used in many interesting applications, such as e-commerce and e-security, this book is *not* about applications. Instead, this book gives a detailed description of Rijndael and explains the design strategy that was used to develop it.

Structure of this book

When we wrote this book, we had basically two kinds of readers in mind. Perhaps the largest group of readers will consist of people who want to read a full and unambiguous description of Rijndael. For those readers, the most important chapter of this book is Chap. 3, which gives its comprehensive description. In order to follow our description, it might be helpful to read the preliminaries given in Chap. 2. Advanced implementation aspects are discussed in Chap. 4. A short overview of the AES selection process is given in Chap. 1.

A large part of this book is aimed at readers who want to know *why* we designed Rijndael in the way we did. For them, we explain the ideas and principles underlying the design of Rijndael, culminating in our wide trail design strategy. In Chap. 5 we explain our approach to block cipher design and the criteria that played an important role in the design of Rijndael. Our design strategy has grown out of our experiences with linear and differential cryptanalysis, two cryptanalytical attacks that have been applied with some success to the previous standard, the Data Encryption Standard (DES). In Chap. 6 we give a short overview of the DES and of the differential and the linear attacks that are applied to it. Our framework to describe linear cryptanalysis is explained in Chap. 7; differential cryptanalysis is described in Chap. 8. Finally, in Chap. 9, we explain how the wide trail design strategy follows from these considerations.

Chap. 10 gives an overview of the published attacks on reduced-round variants of Rijndael. Chap. 11 gives an overview of ciphers related to Rijndael. We describe its predecessors and discuss their similarities and differences. This is followed by a short description of a number of block ciphers that have been strongly influenced by Rijndael and its predecessors.

In Chap. 12 we show how linear and differential analysis can be applied to ciphers that are defined in terms of finite field operations rather than Boolean functions. In Chap. 13 we discuss extensions of differential and linear cryptanalysis. In Chap. 14 we study the probability of differentials and trails over two rounds of Rijndael, and in Chap. 15 we define plateau trails. To assist programmers, Appendix A lists some tables that are used in various descriptions of Rijndael, Appendix B gives a set of test vectors, and Appendix C consists of an example implementation of Rijndael in the C programming language.

Acknowledgments

This book would not have been written without the support and help of many people. It is impossible for us to list all people who contributed along the way. Although we probably will make oversights, we would like to name some of our supporters here.

First of all, we would like to thank the many cryptographers who contributed to developing the theory on the design of symmetric ciphers, and from who we learned much of what we know today. We would like to mention explicitly the people who gave us feedback in the early stages of the design process: Johan Borst, Antoon Bosselaers, Paulo Barreto, Craig Clapp, Erik De Win, Lars R. Knudsen and Bart Preneel.

Elaine Barker, James Foti and Miles Smid, and all the other people at NIST who worked very hard to make the AES process possible and visible.

The moral support of our family and friends, without whom we would never have persevered.

Brian Gladman, who provided test vectors.

Othmar Staffelbach, Elisabeth Oswald, Lee McCulloch and other proofreaders, who provided very valuable feedback and corrected numerous errors and oversights.

The financial support of KU Leuven, the Fund for Scientific Research – Flanders (Belgium), Banksys, Proton World and Cryptomathic is also greatly appreciated.

November 2001 *Joan Daemen and Vincent Rijmen*

Preface to the second edition

This edition contains updates of several chapters as well as four new chapters (Chaps. 12 to 15). We adapted our text to new terminology that has come into use since the first edition and removed some material that is now obsolete, including the original Appendix A (Propagation Analysis in Galois Fields) and the original Appendix B (Trail Clustering).

We thank Ronan Nugent of Springer for his persistent encouragements to finalize this second edition. We thank Dave, Eric Bach, Nicolas T. Courtois, Praveen Gauravaram, Jorge Nakahara Jr., Ralph Wernsdorf, Shengbo Xu and Uyama Yasumasa for pointing out errors in the first edition of this book. We thank Bart Mennink for proofreading some of the updates. All remaining errors and those newly introduced are of course our own.

July 2019 *Joan Daemen and Vincent Rijmen*

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
2.1.8 Functions over Fields 17
2.1.9 Representations of GF(p^n) 18
2.2 Linear Codes 20
2.2.1 Definitions 20
2.2.2 MDS Codes 22
2.3 Boolean Functions 22
2.3.1 Tuple Partitions 23
2.3.2 Transpositions 24
2.3.3 Bricklayer Functions 25
2.3.4 Iterative Boolean Transformations 26

2.4 Block Ciphers 26
2.4.1 Iterative Block Ciphers 27
2.4.2 Key-Alternating Block Ciphers 28

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 39
3.4.4 The Key Addition 41
3.4.5 The Rijndael Super Box 41
3.5 The Number of Rounds 42
3.6 Key Schedule 43
3.6.1 Design Criteria 44
3.6.2 Selection 44
3.7 Decryption 46
3.7.1 Decryption for a Two-Round Rijndael Variant 46
3.7.2 Algebraic Properties 48
3.7.3 The Equivalent Decryption Algorithm 48
3.8 Conclusions 50

4. Implementation Aspects 53
4.1 Eight-Bit Platforms 53
4.1.1 Finite-Field Multiplication 53
4.1.2 Encryption 54
4.1.3 Decryption 55
4.2 Thirty-Two-Bit Platforms 56
4.2.1 T-Table Implementation 56
4.2.2 Bitsliced Software 59
4.3 Dedicated Hardware 60
4.3.1 Decomposition of S_{RD} 61
4.3.2 Efficient Inversion in $\mathrm{GF}(2^8)$ 61
4.3.3 AES-NI 62
4.4 Multiprocessor Platforms 62
4.5 Conclusions 63

5. Design Philosophy 65
5.1 Generic Criteria in Cipher Design 65
5.1.1 Security 65
5.1.2 Efficiency 65
5.1.3 Key Agility 66
5.1.4 Versatility 66

5.1.5 Discussion 66
5.2 Simplicity 66
5.3 Symmetry 67
5.3.1 Symmetry Across the Rounds 67
5.3.2 Symmetry Within the Round Transformation 68
5.3.3 Symmetry in the D-Box 69
5.3.4 Symmetry and Simplicity in the S-Box 69
5.3.5 Symmetry Between Encryption and Decryption 69
5.3.6 Additional Benefits of Symmetry 70
5.4 Choice of Operations 71
5.4.1 Arithmetic Operations 71
5.4.2 Data-Dependent Shifts 72
5.5 Approach to Security 73
5.5.1 Security Goals 73
5.5.2 Translation of Security Goals into Modern Security Notions 74
5.5.3 Unknown Attacks Versus Known Attacks 75
5.5.4 Provable Security Versus Provable Bounds 76
5.6 Approaches to Design 76
5.6.1 Nonlinearity and Diffusion Criteria 76
5.6.2 Resistance Against Differential and Linear Cryptanalysis 76
5.6.3 Local Versus Global Optimization 77
5.7 Key-Alternating Cipher Structure 79
5.8 The Key Schedule 80
5.8.1 The Function of a Key Schedule 80
5.8.2 Key Expansion and Key Selection 80
5.8.3 The Cost of the Key Expansion 81
5.8.4 A Recursive Key Expansion 81
5.9 Conclusions 82

6. The Data Encryption Standard 83
6.1 The DES 83
6.2 Differential Cryptanalysis 85
6.3 Linear Cryptanalysis 87
6.4 Conclusions 89

7. Correlation Matrices 91
7.1 The Walsh-Hadamard Transform 91
7.1.1 Parities and Masks 91
7.1.2 Correlation 91
7.1.3 Real-Valued Counterpart of a Binary Boolean Function 92
7.1.4 Orthogonality and Correlation 92
7.1.5 Spectrum of a Binary Boolean Function 93
7.2 Composing Binary Boolean Functions 95
7.2.1 Addition 95

7.2.2 Multiplication 95
7.2.3 Disjunct Boolean Functions 96
7.3 Correlation Matrices 96
7.3.1 Equivalence of a Boolean Function and Its Correlation Matrix 97
7.3.2 Iterative Boolean Functions 98
7.3.3 Boolean Permutations 98
7.4 Special Functions 100
7.4.1 Addition with a Constant 100
7.4.2 Linear Functions 100
7.4.3 Bricklayer Functions 100
7.4.4 Keyed Functions 101
7.5 Derived Properties 101
7.6 Truncating Functions 103
7.7 Cross-correlation and Autocorrelation 104
7.8 Linear Trails 105
7.9 Ciphers 106
7.9.1 General Case 106
7.9.2 Key-Alternating Cipher 106
7.9.3 Averaging over All Round Keys 107
7.9.4 The Effect of the Key Schedule 109
7.10 Correlation Matrices and the Linear Cryptanalysis Literature 111
7.10.1 Linear Cryptanalysis of the DES 111
7.10.2 Linear Hulls 112
7.11 Conclusions 113

8. Difference Propagation 115
8.1 Difference Propagation 115
8.2 Special Functions 116
8.2.1 Affine Functions 116
8.2.2 Bricklayer Functions 117
8.2.3 Truncating Functions 117
8.2.4 Keyed Functions 117
8.3 Relation Between DP Values and Correlations 118
8.4 Differential Trails 119
8.4.1 General Case 119
8.4.2 Independence of Restrictions 120
8.5 Key-Alternating Cipher 121
8.6 The Effect of the Key Schedule 122
8.7 Differential Trails and the Differential Cryptanalysis Literature122
8.7.1 Differential Cryptanalysis of the DES Revisited 122
8.7.2 Markov Ciphers 123
8.8 Conclusions 123

9. The Wide Trail Strategy 125
9.1 Propagation in Key-Alternating Block Ciphers 125
9.1.1 Linear Cryptanalysis 125
9.1.2 Differential Cryptanalysis 126
9.1.3 Differences Between Linear Trails and Differential Trails 128
9.2 The Wide Trail Strategy 128
9.2.1 The $\gamma\lambda$ Round Structure in Block Ciphers 129
9.2.2 Weight of a Trail 131
9.2.3 Diffusion 132
9.3 Branch Numbers and Two-Round Trails 133
9.3.1 Derived Properties 135
9.3.2 A Two-Round Propagation Theorem 135
9.4 An Efficient Key-Alternating Structure 136
9.4.1 The Diffusion Step θ 136
9.4.2 The Linear Step Θ 138
9.4.3 A Lower Bound on the Byte Weight of Four-Round Trails 138
9.4.4 An Efficient Construction for Θ 139
9.5 The Round Structure of Rijndael 140
9.5.1 A Key-Iterated Structure 140
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 151
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 154
10.2.7 The Herds Attack and Other Extensions 154
10.2.8 Division Cryptanalysis 155
10.3 Gilbert-Minier and Demirci-Selçuk Attack 155
10.3.1 The Four-Round Distinguisher 155
10.3.2 The Attack on Seven Rounds 156
10.3.3 The Demirci-Selçuk Attack 157
10.4 Interpolation Attacks 157
10.5 Related-Key Attacks 158
10.5.1 The Key Schedule of Rijndael-256 159

10.5.2 The Biryukov-Khovratovich Attack 159
10.5.3 The KAS of the Biryukov-Khovratovich Attack 160
10.6 Biclique Attacks 162
10.7 Rebound Attacks 162
10.8 Impossible-Differential Attacks 163
10.8.1 Principle of the Attack 163
10.8.2 Application to Rijndael 164
10.9 Implementation Attacks 164
10.9.1 Timing Attacks 164
10.9.2 Power Analysis 165
10.10 Conclusions 166

11. The Road to Rijndael 169
11.1 Overview 169
11.1.1 Evolution 169
11.1.2 The Round Transformation 170
11.2 SHARK 171
11.3 Square 173
11.4 BKSQ 176
11.5 Conclusion 179

12. Correlation Analysis in GF(2^n) 181
12.1 Description of Correlation in Functions over GF(2^n) 182
12.1.1 Functions That Are Linear over GF(2^n) 184
12.1.2 Functions That Are Linear over GF(2) 184
12.2 Description of Correlation in Functions over GF(2^n)$^\ell$ 186
12.2.1 Functions That Are Linear over GF(2^n) 187
12.2.2 Functions That Are Linear over GF(2) 187
12.3 Boolean Functions and Functions in GF(2^n) 188
12.3.1 Relationship Between Trace Masks and Selection Masks188
12.3.2 Relationship Between Linear Functions in GF$(2)^n$ and GF(2^n) 189
12.4 Rijndael-GF 192

13. On the EDP and the ELP of Two and Four Rijndael Rounds195
13.1 Properties of MDS Mappings 195
13.2 Bounds for Two Rounds 198
13.2.1 Difference Propagation 200
13.2.2 Correlation 202
13.3 Bounds for Four Rounds 203
13.4 Conclusions 204

14. Two-Round Differential Trail Clustering 205
14.1 The Multiplicative Inverse in GF(2^n) 205
14.2 Bundles in the Rijndael Super Box 207
14.2.1 Differentials, Trails and Trail Cores 207
14.2.2 Bundles 209
14.2.3 Number of Bundles with a Given Number of Active Bytes 210
14.3 Conditions for a Trail Core to Extend to a Trail 211
14.3.1 The Naive Super Box 211
14.3.2 Sharp Conditions and Blurred Conditions 212
14.4 Number of Trail Cores in a Bundle Extending to a Trail 213
14.4.1 Bundles with One Active S-Box in the First Round ... 213
14.4.2 Any Bundle 214
14.4.3 Experimental Verification 215
14.5 EDP of a Bundle 216
14.5.1 Multiple Solutions 217
14.5.2 Occurrence in Trails 217
14.5.3 How L_i Makes a Difference 218
14.6 EDP of a Differential 218
14.6.1 Differentials with Activity Pattern (1110; 1110) 218
14.6.2 A Bound on the Multiplicity 219
14.7 Differentials with the Maximum EDP Value 220
14.8 Conclusions 221

15. Plateau Trails 223
15.1 Motivation 223
15.2 Two-Round Plateau Trails 224
15.2.1 Planar Differentials and Maps 224
15.2.2 Plateau Trails 226
15.2.3 Plateau Trails in Super Boxes 227
15.3 Plateau Trails over More Than Two Rounds 229
15.4 Further Observations 230
15.4.1 Effect of the Key Schedule 230
15.4.2 Impact on the DP of Differentials 231
15.5 Two-Round Trails in Rijndael 231
15.5.1 Trails in the Rijndael Super Box 231
15.5.2 Observations 232
15.5.3 Influence of L 234
15.6 Trails over Four or More Rounds in Rijndael 234
15.7 DP of Differentials in Rijndael 236
15.8 Related Differentials 236
15.8.1 Definitions 236
15.8.2 Related Differentials and Plateau Trails 237
15.9 Determining the Related Differentials 239
15.9.1 First Example 239

15.9.2 For Any Given Differential 240
15.9.3 For All Differentials with the Same Activity Pattern . . 241
15.9.4 Second Example 241
15.9.5 A Combinatorial Bound 243
15.10 Implications for Rijndael-Like Super Boxes 244
15.10.1 Related Differentials over Circulant Matrices 244
15.10.2 Related Differentials in `MixColumns` 244
15.10.3 Avoiding Related Differentials 245
15.11 Conclusions and Further Work 246

A. Substitution Tables 249
A.1 $\mathrm{S_{RD}}$ 249
A.2 Other Tables 252
A.2.1 `xtime` 252
A.2.2 Round Constants 252

B. Test Vectors 253
B.1 `KeyExpansion` 253
B.2 Rijndael(128,128) 253
B.3 Other Block Lengths and Key Lengths 255

C. Reference Code 259

Bibliography 267

Index 279