Hans Dobbertin
Vincent Rijmen
Aleksandra Sowa (Eds.)

LNCS 3373

Advanced Encryption Standard – AES

4th International Conference, AES 2004
Bonn, Germany, May 2004
Revised Selected and Invited Papers

Springer

Hans Dobbertin Vincent Rijmen
Aleksandra Sowa (Eds.)

Advanced Encryption Standard – AES

4th International Conference, AES 2004
Bonn, Germany, May 10-12, 2004
Revised Selected and Invited Papers

Springer

Volume Editors

Hans Dobbertin
Ruhr-University of Bochum
Cryptology and IT Security Research Group
Universitätsstrasse 150, 44780 Bochum, Germany
E-mail: Hans.Dobbertin@ruhr-uni-bochum.de

Vincent Rijmen
Graz University of Technology
Institute for Applied Information Processing and Communications (IAIK)
Inffeldgasse 16a, 8010 Graz, Austria
E-mail: vincent.rijmen@iaik.tugraz.at

Aleksandra Sowa
Ruhr-University of Bochum
Horst Görtz Institut für Sicherheit in der Informationstechnik
Universitätsstrasse 150, 44780 Bochum, Germany
E-mail: Aleksandra.Sowa@hgi.ruhr-uni-bochum.de

Library of Congress Control Number: 2005928447

CR Subject Classification (1998): E.3, F.2.1-2, I.1.4, G.2.1

ISSN 0302-9743
ISBN-10 3-540-26557-0 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-26557-3 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springeronline.com

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11506447 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 3373

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Lecture Notes in Computer Science

For information about Vols. 1–3476

please contact your bookseller or Springer

Vol. 3580: L. Caires, G.F. Italiano, L. Monteiro, C. Palamidessi, M. Yung (Eds.), Automata, Languages and Programming. XXV, 1477 pages. 2005.

Vol. 3578: M. Gallagher, J. Hogan, F. Maire (Eds.), Intelligent Data Engineering and Automated Learning - IDEAL 2005. XVI, 599 pages. 2005.

Vol. 3576: K. Etessami, S.K. Rajamani (Eds.), Computer Aided Verification. XV, 564 pages. 2005.

Vol. 3574: C. Boyd, J.M. González Nieto (Eds.), Information Security and Privacy. XIII, 586 pages. 2005.

Vol. 3573: S. Etalle (Ed.), Logic Based Program Synthesis and Transformation. VIII, 279 pages. 2005.

Vol. 3572: C. De Felice, A. Restivo (Eds.), Developments in Language Theory. XI, 409 pages. 2005.

Vol. 3570: A. S. Patrick, M. Yung (Eds.), Financial Cryptography and Data Security. XII, 376 pages. 2005.

Vol. 3569: F. Bacchus, T. Walsh (Eds.), Theory and Applications of Satisfiability Testing. XII, 492 pages. 2005.

Vol. 3567: M. Jackson, D. Nelson, S. Stirk (Eds.), Database: Enterprise, Skills and Innovation. XII, 185 pages. 2005.

Vol. 3565: G.E. Christensen, M. Sonka (Eds.), Information Processing in Medical Imaging. XXI, 777 pages. 2005.

Vol. 3562: J. Mira, J.R. Álvarez (Eds.), Artificial Intelligence and Knowledge Engineering Applications: A Bioinspired Approach, Part II. XXIV, 636 pages. 2005.

Vol. 3561: J. Mira, J.R. Álvarez (Eds.), Mechanisms, Symbols, and Models Underlying Cognition, Part I. XXIV, 532 pages. 2005.

Vol. 3560: V.K. Prasanna, S. Iyengar, P.G. Spirakis, M. Welsh (Eds.), Distributed Computing in Sensor Systems. XV, 423 pages. 2005.

Vol. 3559: P. Auer, R. Meir (Eds.), Learning Theory. XI, 692 pages. 2005. (Subseries LNAI).

Vol. 3557: H. Gilbert, H. Handschuh (Eds.), Fast Software Encryption. XI, 443 pages. 2005.

Vol. 3556: H. Baumeister, M. Marchesi, M. Holcombe (Eds.), Extreme Programming and Agile Processes in Software Engineering. XIV, 332 pages. 2005.

Vol. 3555: T. Vardanega, A. Wellings (Eds.), Reliable Software Technology – Ada-Europe 2005. XV, 273 pages. 2005.

Vol. 3554: A. Dey, B. Kokinov, D. Leake, R. Turner (Eds.), Modeling and Using Context. XIV, 572 pages. 2005. (Subseries LNAI).

Vol. 3553: T.D. Hämäläinen, A.D. Pimentel, J. Takala, S. Vassiliadis (Eds.), Embedded Computer Systems: Architectures, Modeling, and Simulation. XV, 476 pages. 2005.

Vol. 3552: H. de Meer, N. Bhatti (Eds.), Quality of Service – IWQoS 2005. XV, 400 pages. 2005.

Vol. 3551: T. Härder, W. Lehner (Eds.), Data Management in a Connected World. XIX, 371 pages. 2005.

Vol. 3548: K. Julisch, C. Kruegel (Eds.), Intrusion and Malware Detection and Vulnerability Assessment. X, 241 pages. 2005.

Vol. 3547: F. Bomarius, S. Komi-Sirviö (Eds.), Product Focused Software Process Improvement. XIII, 588 pages. 2005.

Vol. 3543: L. Kutvonen, N. Alonistioti (Eds.), Distributed Applications and Interoperable Systems. XI, 235 pages. 2005.

Vol. 3541: N.C. Oza, R. Polikar, J. Kittler, F. Roli (Eds.), Multiple Classifier Systems. XII, 430 pages. 2005.

Vol. 3540: H. Kalviainen, J. Parkkinen, A. Kaarna (Eds.), Image Analysis. XXII, 1270 pages. 2005.

Vol. 3537: A. Apostolico, M. Crochemore, K. Park (Eds.), Combinatorial Pattern Matching. XI, 444 pages. 2005.

Vol. 3536: G. Ciardo, P. Darondeau (Eds.), Applications and Theory of Petri Nets 2005. XI, 470 pages. 2005.

Vol. 3535: M. Steffen, G. Zavattaro (Eds.), Formal Methods for Open Object-Based Distributed Systems. X, 323 pages. 2005.

Vol. 3533: M. Ali, F. Esposito (Eds.), Innovations in Applied Artificial Intelligence. XX, 858 pages. 2005. (Subseries LNAI).

Vol. 3532: A. Gómez-Pérez, J. Euzenat (Eds.), The Semantic Web: Research and Applications. XV, 728 pages. 2005.

Vol. 3531: J. Ioannidis, A. Keromytis, M. Yung (Eds.), Applied Cryptography and Network Security. XI, 530 pages. 2005.

Vol. 3530: A. Prinz, R. Reed, J. Reed (Eds.), SDL 2005: Model Driven. XI, 361 pages. 2005.

Vol. 3528: P.S. Szczepaniak, J. Kacprzyk, A. Niewiadomski (Eds.), Advances in Web Intelligence. XVII, 513 pages. 2005. (Subseries LNAI).

Vol. 3527: R. Morrison, F. Oquendo (Eds.), Software Architecture. XII, 263 pages. 2005.

Vol. 3526: S.B. Cooper, B. Löwe, L. Torenvliet (Eds.), New Computational Paradigms. XVII, 574 pages. 2005.

Vol. 3525: A.E. Abdallah, C.B. Jones, J.W. Sanders (Eds.), Communicating Sequential Processes. XIV, 321 pages. 2005.

Vol. 3524: R. Barták, M. Milano (Eds.), Integration of AI and OR Techniques in Constraint Programming for Combinatorial Optimization Problems. XI, 320 pages. 2005.

Vol. 3523: J.S. Marques, N. Pérez de la Blanca, P. Pina (Eds.), Pattern Recognition and Image Analysis, Part II. XXVI, 733 pages. 2005.

Vol. 3522: J.S. Marques, N. Pérez de la Blanca, P. Pina (Eds.), Pattern Recognition and Image Analysis, Part I. XXVI, 703 pages. 2005.

Vol. 3521: N. Megiddo, Y. Xu, B. Zhu (Eds.), Algorithmic Applications in Management. XIII, 484 pages. 2005.

Vol. 3520: O. Pastor, J. Falcão e Cunha (Eds.), Advanced Information Systems Engineering. XVI, 584 pages. 2005.

Vol. 3519: H. Li, P. J. Olver, G. Sommer (Eds.), Computer Algebra and Geometric Algebra with Applications. IX, 449 pages. 2005.

Vol. 3518: T.B. Ho, D. Cheung, H. Liu (Eds.), Advances in Knowledge Discovery and Data Mining. XXI, 864 pages. 2005. (Subseries LNAI).

Vol. 3517: H.S. Baird, D.P. Lopresti (Eds.), Human Interactive Proofs. IX, 143 pages. 2005.

Vol. 3516: V.S. Sunderam, G.D.v. Albada, P.M.A. Sloot, J.J. Dongarra (Eds.), Computational Science – ICCS 2005, Part III. LXIII, 1143 pages. 2005.

Vol. 3515: V.S. Sunderam, G.D.v. Albada, P.M.A. Sloot, J.J. Dongarra (Eds.), Computational Science – ICCS 2005, Part II. LXIII, 1101 pages. 2005.

Vol. 3514: V.S. Sunderam, G.D.v. Albada, P.M.A. Sloot, J.J. Dongarra (Eds.), Computational Science – ICCS 2005, Part I. LXIII, 1089 pages. 2005.

Vol. 3513: A. Montoyo, R. Muñoz, E. Métais (Eds.), Natural Language Processing and Information Systems. XII, 408 pages. 2005.

Vol. 3512: J. Cabestany, A. Prieto, F. Sandoval (Eds.), Computational Intelligence and Bioinspired Systems. XXV, 1260 pages. 2005.

Vol. 3510: T. Braun, G. Carle, Y. Koucheryavy, V. Tsaoussidis (Eds.), Wired/Wireless Internet Communications. XIV, 366 pages. 2005.

Vol. 3509: M. Jünger, V. Kaibel (Eds.), Integer Programming and Combinatorial Optimization. XI, 484 pages. 2005.

Vol. 3508: P. Bresciani, P. Giorgini, B. Henderson-Sellers, G. Low, M. Winikoff (Eds.), Agent-Oriented Information Systems II. X, 227 pages. 2005. (Subseries LNAI).

Vol. 3507: F. Crestani, I. Ruthven (Eds.), Information Context: Nature, Impact, and Role. XIII, 253 pages. 2005.

Vol. 3506: C. Park, S. Chee (Eds.), Information Security and Cryptology – ICISC 2004. XIV, 490 pages. 2005.

Vol. 3505: V. Gorodetsky, J. Liu, V. A. Skormin (Eds.), Autonomous Intelligent Systems: Agents and Data Mining. XIII, 303 pages. 2005. (Subseries LNAI).

Vol. 3504: A.F. Frangi, P.I. Radeva, A. Santos, M. Hernandez (Eds.), Functional Imaging and Modeling of the Heart. XV, 489 pages. 2005.

Vol. 3503: S.E. Nikoletseas (Ed.), Experimental and Efficient Algorithms. XV, 624 pages. 2005.

Vol. 3502: F. Khendek, R. Dssouli (Eds.), Testing of Communicating Systems. X, 381 pages. 2005.

Vol. 3501: B. Kégl, G. Lapalme (Eds.), Advances in Artificial Intelligence. XV, 458 pages. 2005. (Subseries LNAI).

Vol. 3500: S. Miyano, J. Mesirov, S. Kasif, S. Istrail, P. Pevzner, M. Waterman (Eds.), Research in Computational Molecular Biology. XVII, 632 pages. 2005. (Subseries LNBI).

Vol. 3499: A. Pelc, M. Raynal (Eds.), Structural Information and Communication Complexity. X, 323 pages. 2005.

Vol. 3498: J. Wang, X. Liao, Z. Yi (Eds.), Advances in Neural Networks – ISNN 2005, Part III. XLIX, 1077 pages. 2005.

Vol. 3497: J. Wang, X. Liao, Z. Yi (Eds.), Advances in Neural Networks – ISNN 2005, Part II. XLIX, 947 pages. 2005.

Vol. 3496: J. Wang, X. Liao, Z. Yi (Eds.), Advances in Neural Networks – ISNN 2005, Part II. L, 1055 pages. 2005.

Vol. 3495: P. Kantor, G. Muresan, F. Roberts, D.D. Zeng, F.-Y. Wang, H. Chen, R.C. Merkle (Eds.), Intelligence and Security Informatics. XVIII, 674 pages. 2005.

Vol. 3494: R. Cramer (Ed.), Advances in Cryptology – EUROCRYPT 2005. XIV, 576 pages. 2005.

Vol. 3493: N. Fuhr, M. Lalmas, S. Malik, Z. Szlávik (Eds.), Advances in XML Information Retrieval. XI, 438 pages. 2005.

Vol. 3492: P. Blache, E. Stabler, J. Busquets, R. Moot (Eds.), Logical Aspects of Computational Linguistics. X, 363 pages. 2005. (Subseries LNAI).

Vol. 3489: G.T. Heineman, I. Crnkovic, H.W. Schmidt, J.A. Stafford, C. Szyperski, K. Wallnau (Eds.), Component-Based Software Engineering. XI, 358 pages. 2005.

Vol. 3488: M.-S. Hacid, N.V. Murray, Z.W. Raś, S. Tsumoto (Eds.), Foundations of Intelligent Systems. XIII, 700 pages. 2005. (Subseries LNAI).

Vol. 3486: T. Helleseth, D. Sarwate, H.-Y. Song, K. Yang (Eds.), Sequences and Their Applications - SETA 2004. XII, 451 pages. 2005.

Vol. 3483: O. Gervasi, M.L. Gavrilova, V. Kumar, A. Laganà, H.P. Lee, Y. Mun, D. Taniar, C.J.K. Tan (Eds.), Computational Science and Its Applications – ICCSA 2005, Part IV. LXV, 1362 pages. 2005.

Vol. 3482: O. Gervasi, M.L. Gavrilova, V. Kumar, A. Laganà, H.P. Lee, Y. Mun, D. Taniar, C.J.K. Tan (Eds.), Computational Science and Its Applications – ICCSA 2005, Part III. LXV, 1340 pages. 2005.

Vol. 3481: O. Gervasi, M.L. Gavrilova, V. Kumar, A. Laganà, H.P. Lee, Y. Mun, D. Taniar, C.J.K. Tan (Eds.), Computational Science and Its Applications – ICCSA 2005, Part II. LXV, 1316 pages. 2005.

Vol. 3480: O. Gervasi, M.L. Gavrilova, V. Kumar, A. Laganà, H.P. Lee, Y. Mun, D. Taniar, C.J.K. Tan (Eds.), Computational Science and Its Applications – ICCSA 2005, Part I. LXV, 1234 pages. 2005.

Vol. 3479: T. Strang, C. Linnhoff-Popien (Eds.), Location- and Context-Awareness. XII, 378 pages. 2005.

Vol. 3478: C. Jermann, A. Neumaier, D. Sam (Eds.), Global Optimization and Constraint Satisfaction. XIII, 193 pages. 2005.

Vol. 3477: P. Herrmann, V. Issarny, S. Shiu (Eds.), Trust Management. XII, 426 pages. 2005.

¥396.48元

Preface

This volume comprises the proceedings of the 4th Conference on Advanced Encryption Standard, 'AES — State of the Crypto Analysis,' which was held in Bonn, Germany, during 10–12 May 2004.

The conference followed a series of events organized by the US National Institute of Standards and Technology (NIST) in order to hold an international competition to decide on an algorithm to serve as the Advanced Encryption Standard (AES). In 1998, at the first AES conference (AES 1), 15 different algorithms were presented, discussed, reviewed and verified. A second conference was organized in April 1999, and by August 1999 only five candidates were still in the running: MARS, RC6, Rijndael, Serpent and Twofish. After a further conference devoted to verification, testing and examination of the candidate algorithms in order to prove their performance and security, one winning algorithm remained. The encryption scheme Rijndael, designed by the Belgian cryptographers Joan Daemen and Vincent Rijmen, was selected in 2000 to become the successor to the famous DES (Data Encryption Standard) and it is now the Advanced Encryption Standard.

Like DES before it, AES is going to become a de facto world standard for the encryption of data. The security of Internet applications, for instance, is already depending today and, in view of the increasing implementation, will depend in future even more on AES. Analysis of the cryptographic strength of AES belongs therefore certainly to the most important topics in cryptology. A recent key recovery approach, by solving a complicated system of quadratic equations, which is due to Courtois and others, has caused a big debate. Previously, approaches of this kind were considered as purely theoretical, and hopeless in practice. The big unanswered question is whether the addition of newly proposed techniques has changed or can change this situation.

Four years after the National Institute of Standards and Technology chose Rijndael to be the Advanced Encryption Standard, leading experts and scientists from all over the world were invited to discuss — critically but constructively — the strengths and weaknesses of Rijndael, and to look for solutions that will make it a strong information encryption formula for the next two, five, ten, or maybe dozens of years. The intentions of the AES4 conference organizers were to present the most recent ideas and results on the cryptanalysis of the AES, and to stimulate future research on the important open questions about the perspectives and limits of new cryptanalytic approaches.

The response to the conference was excellent. Ten submission were selected for presentation. The programme included six keynote addresses (invited talks), given by Yvo Desmedt from Florida State University, Vincent Rijmen from the IAIK, Graz University of Technology and Cryptomathic, Carlos Cid from Royal Holloway, University of London, Nicolas T. Courtois from Axalto Smart Cards, Jean-Charles Faugère from the University of Paris VI/INRIA, France, and John Kelsey from the National Institute for Standards and Technology. As a novum, AES4 introduced for the first time a closing panel discussion on the future of Rijndael and cryptography, moderated by Peter Welchering from the German Scientific Press Conference. Researchers took the opportunity to present their opinions and suggestions on the cipher weaknesses, known and unknown attacks, and the future of their work. John Kelsey remarked that most of the practical problems are usually other than the weaknesses of a cipher. Nevertheless, as Nicolas T. Courtois argued, there is still 'plenty of work' to do. Carlos Cid and Vincent Rijmen emphasized the necessity to make the current research transparent, to make it popular and understandable and to let other people know 'what we are talking about' (Vincent Rijmen).

We would like to thank Aleksandra Sowa, the Managing Director of the Horst Görtz Institute (HGI) for IT security at the Ruhr University of Bochum. She did an excellent job as General Chair by organizing the AES4 conference with the help of our young colleagues from the Chair for IT Security and Cryptology (CITS).

We are also grateful to NIST and Cryptomathic for supporting this event, and, last but not least, we would like to thank all the committee members for their work.

April 2005 Hans Dobbertin and Vincent Rijmen

Organization

AES4 was organized by the Ruhr University of Bochum, in cooperation with the Graz University of Technology and NIST.

General Chair

Aleksandra Sowa	Horst Görtz Institute, Ruhr University Bochum

Program Co-chairs

Hans Dobbertin	Horst Görtz Institute, Ruhr University Bochum
Vincent Rijmen	Graz University of Technology

Program Committee

Don Coppersmith	IBM
Nicolas T. Courtois	Axalto Smart Cards
Lars R. Knudsen	Technical University of Denmark
Matt Robshaw	Royal Holloway, University of London

Sponsoring Institutions

Cryptomathic A/S, Århus
NIST

Table of Contents

Cryptanalytic Attacks and Related Results

Algebraic Attacks and Related Results

Hardware Implementations

Other Topics

The Cryptanalysis of the AES - A Brief Survey

Hans Dobbertin[1], Lars Knudsen[2], and Matt Robshaw[3]

[1] Cryptology and IT Security Research Group,
Ruhr-University of Bochum, Germany
Hans.Dobbertin@ruhr-uni-bochum.de
[2] Department of Mathematics,
Technical University of Denmark,
DK-2800 Lyngby, Denmark
Lars.R.Knudsen@mat.dtu.dk
[3] France Télécom Research and Development,
38–40 rue de Général-Leclerc, 92794 Issy Moulineaux, France
Matt.Robshaw@francetelecom.com

Abstract. The Advanced Encryption Standard is more than five years old. Since standardisation there have been few cryptanalytic advances despite the efforts of many researchers. The most promising new approach to AES cryptanalysis remains speculative, while the most effective attack against reduced-round versions is older than the AES itself. Here we summarise this state of affairs.

1 Introduction

In January 1997 the National Institute of Standards and Technology (NIST) initiated the search for a replacement for the *Data Encryption Standard* (DES) [28]. The requirements for the new standard, to be called the *Advanced Encryption Standard* (AES), were that it should be:

- a 128-bit block cipher with the choice of three key sizes of 128, 192, respectively 256 bits,
- a public and flexible design,
- at least as secure as two-key triple-DES, and
- available royalty-free worldwide.

At the conclusion of this standardisation effort, with many man-years of cryptanalytic and implementation expertise provided from around the world, *Rijndael*, developed by Joan Daemen and Vincent Rijmen [11], was a popular choice to become the AES. In November 2001 the AES effort came to its conclusion with the publication of FIPS 197 [29], and today the AES is fast becoming a vital component of the digital infrastructure.

The proceedings of the Fourth AES Conference that follow in this volume reflect ongoing research efforts into the security and performance of the AES. In this short article, we briefly review some promising – but unsuccessful – attempts to compromise this elegant cipher.

H. Dobbertin, V. Rijmen, and A. Sowa (Eds.): AES 2004, LNCS 3373, pp. 1–10, 2005.

2 AES Design

The AES has been described so often and is, by now, so familiar that a brief overview of the AES design will suffice for our purposes.

The AES is a classic *substitution/permutation* or SP-network that requires 10, 12, or 14 rounds of encryption; the exact number depending on the length of the key. The AES is byte-oriented and heavily reliant on operations in the field GF(2^8). Conceptually, the AES is best described with the sixteen bytes of the 128-bit input block $a_0a_1 \ldots a_{14}a_{15}$ being arranged in a (4×4) matrix of bytes:

a_0	a_4	a_8	a_{12}
a_1	a_5	a_9	a_{13}
a_2	a_6	a_{10}	a_{14}
a_3	a_7	a_{11}	a_{15}

Using the nomenclature of FIPS 197, a typical round of the cipher uses the following operations, "`SubBytes`", "`ShiftRows`", "`MixColumns`" and "`AddRoundKey`". The final round has a slightly different form and omits the `MixColumns` operation.

Encryption begins with an `AddRoundKey` operation, then computation continues for a given number of rounds, with each round using the four operations taken in the order above. In `SubBytes` each byte is replaced by a byte from an invertible S-box. In `ShiftRows` the rows (of bytes) are shifted a number of byte positions to the left. The top row is not shifted, the second row is shifted by one position, the third by two, and the fourth row by three. In `MixColumns` the four bytes in each column are mixed by pre-multiplying the four-byte vector by a fixed, invertible, (4×4)-matrix over GF(2^8), that is derived from an MDS code. `MixColumns` has the property that if two input vectors differ in s bytes, then the output vectors differ in at least $5 - s$ bytes, where $1 \leq s \leq 4$. Each round closes with `AddRoundKey` where 16 round-key bytes are exclusive-or'ed to the 16 data bytes. Each round uses all four operations except the last round when the operation `MixColumns` is omitted. We refer to [29] for more details on this and other aspects of the algorithm.

The key schedule for the AES is relatively simple. It takes the user-supplied key of 16, 24, respectively 32 bytes and returns what is called an `ExpandedKey` of 16×11, 16×13, and 16×15 bytes respectively. The details can be found in [13, 29].

3 The Components

By design, Rijndael, and therefore by extension the AES, is a very structured cipher. This very clean structure has at least two attractive consequences:

1. It is possible to provide a simple explanation for the intended effect of each cipher component. The most striking consequence is that we can derive solid reassurance for the resistance of the AES to basic differential [4] and linear [23] cryptanalytic attacks.
2. The implementor is provided with a wide range of implementation options. This is evidenced by the attractive performance profile of the AES across a wide range of environments.

We will explore the first consequence in this article.

3.1 The S-Box

The cryptographic strength or weakness of the AES depends strongly on the choice of S-box. While it is likely that we would view the S-box as a single entity, it has three distinct components; inversion over GF(2^8) which is naturally augmented to handle the zero input, transformation by a GF(2)-linear map L, and addition of a constant $c =$ `0x63`. Thus, up to a GF(2)-affine modification, the S-box $S(x)$ of the AES is the inversion in the multiplicative group of GF(2^8):

$$S(x) = A(1/x) \quad \text{(with the convention } 1/0 = 0\text{)}, \tag{1}$$

where $A(x) = L(x) + c$ is a GF(2)-affine permutation of GF(2^8).

The cryptographic advantages of $1/x$ on GF(2^n) have been known for some time. It realizes the best known properties of bijective S-box constructions with respect to the following properties:

Degree. *All S-box component functions (i.e. non-zero linear combinations of Boolean coordinate functions of the S-box) have degree* $n-1$.
The degree of all non-zero component functions of a non-constant *power function* x^d is the Hamming weight of the binary representation of the remainder of d modulo $2^n - 1$. Thus the maximal degree $n - 1$ is achieved if, and only if, up to cyclotomic equivalence, $d = -1 = 2^n - 2 = 2(1 + 2 + 2^2 + \ldots + 2^{n-2}) \bmod (2^n - 1)$. On the other hand it is well known that each component function of a *one-to-one* S-box has at most degree $n - 1$.

Resistance to linear attack. *Low correlation between S-box component functions and affine Boolean functions.*
The absolute value of the correlation between any non-zero component function of $1/x$ and any affine Boolean function is bounded by $2^{-n/2-1}$ for even n. This can be shown by using the famous Hasse bound for the number of points on elliptic curves. It is an open problem whether this bound can be improved. We mention that for odd n, the bound $2^{-n-1/2}$ is attained by $1/x$ and this is known to be optimal.

Resistance to differential attack. *The designer's dream "for each prescribed input difference one can derive no information about the S-box output difference" is almost achieved.*
For characteristic 2, differences coincide with sums. Thus the number of possible output differences for pre-scribed input difference is at most 2^{n-1}. If this

bound is achieved then the S-box is called *almost perfect nonlinear (APN)*, and in this case each output difference is attained precisely two times. If n is odd then $1/x$ is APN, while $2^{n-1} - 1$ is the number of output differences for even n. The latter is due to the fact that $1/x$ is linear on GF(4). It is not known if there is any APN *one-to-one* S-box for even n.

These properties of inversion are preserved under affine modifications and are therefore valid for the S-box of the AES. The net result is an exceptional resistance to differential and linear cryptanalysis. In [11] it is shown that any four-round differential characteristic has a probability of less than 2^{-150} and that any four-round linear characteristic holds with a correlation less than 2^{-75}. These bounds are sufficient to conclude that the basic attacks based on differential and linear cryptanalysis will not succeed against the AES.

While the resistance of the AES to advanced attacks or those using differentials and/or linear hulls remains open, there have been a series of results that explore these issues [8, 18, 19, 20, 21, 30, 31, 7, 32, 33, 34, 5]. However there seems little chance of a major breakthrough in this direction.

3.2 Rearranging Components

While the structure of Rijndael received cryptanalytic attention during the AES process, (see Section 4) it was only at the tail end of that process that a different kind of observation began to be explored. These observations are based on alternative representations of components, or the entireity, of the AES. Some researchers have considered a continued fraction representation of AES encryption [16] while others have considered the concept and implications of *dual Rijndaels* [3, 35]. Other observations have been concerned with the way AES operations are presented [25, 26].

Clearly, operations such as `SubBytes` and `ShiftRows` trivially commute with one another. Indeed, properties such as these were used by the AES designers to show how AES decryption could be written in a form that more closely resembled encryption. However a more fundamental re-writing is also possible. While it is typical to take the S-box as a single entity, we have already observed that it consists of three separate components; the augmented inversion mapping $1/x$, the linear map L, and addition of the constant `0x63`. Concern about the algebraic simplicity of the inversion operation over GF(2^8) lead the designers to introduce a mixing function (the linear map L) over GF(2), while concern that the input 0 would be mapped to 0 through the two combined operations lead to the final addition of the constant.

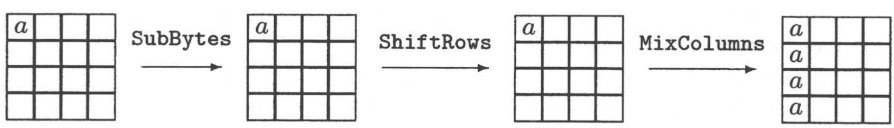
Yet, it is instructive to view this package as the sequence of independent operations it truly is [25, 26]. It is then trivial to see that the parallel addition of sixteen constants `0x63` can be moved (unchanged) through the `ShiftRows` operation. It can also be moved (unchanged) through the `MixColumns` operation. We might therefore remove the addition of the constant from the encryption process entirely and, instead, consider it a minor addition to the key schedule. We can also view the sixteen parallel applications of the linear map L as part of the diffusion layer that follows. While making the diffusion layer slightly more complicated than that given in the standard description, this separation of the components of the AES yields a more unified functional description.

The value of such rewriting has been questioned [12], but it does provide some additional perspectives on the AES structure. But while there is some interaction between this line of work and the aims of algebraic cryptanalysis (see Section 5) these different perspectives on the AES have yet to yield any practical cryptanalytic advance. Instead the most successful attacks on the AES are of an entirely different nature.

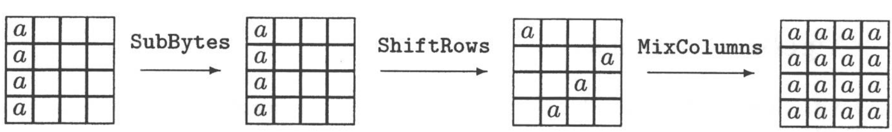
4 Structural Attacks

The most effective attacks on reduced-round variants of the AES are variants of the *Square* attack which is due to Knudsen. Since this attack was used against a predecessor [10] of the AES it was accounted for by the AES designers [11].

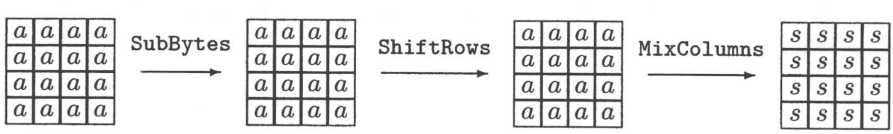
In this attack we take a set of 256 plaintexts where the first byte takes all possible values. The other 15 bytes of the input can take any value but the same value in a given byte position must be used across all 256 texts. We will describe a set of texts that have this property as an *integral*. Imagine one begins an AES-round with such an integral. In the following we shall denote the byte-position containing a variable value with an "*a*" (for "all"). Consider the actions of `SubBytes`, `ShiftRows`, and `MixColumns`.



The `AddRoundKey` operation adds the same round key to each of the 256 texts in the integral, therefore any integral before `AddRoundKey` will yield an integral after. Consider a second round of transformation.



It follows that after two rounds of encryption and for each byte position, every possible value in a given byte position is taken once and only once in the set of 256 texts. Now consider a third round.



Here s indicates that the sum of the texts in a particular byte can be determined (and in this case is equal to zero). The interesting part is what happened during the `MixColumns` operation. Before the operation, in each byte position the 256 values were a permutation of the values $0, \ldots, 255$. `MixColumns` combines four bytes to yield one byte in a linear way. This means that after the application of `MixColumns` every byte position will be balanced, that is, if we exclusive-or all 256 values in any single byte position we will get zero as a result. Note how this property, after three rounds of AES encryption does not depend on the details of the S-box nor on the value of the secret key.

Such three-round structures can be used to attack the AES reduced to six rounds (where the first round consists of `AddRoundKey` and the last round is without `MixColumns`). The structure is used over rounds two to four. Then by guessing four key bytes in the first round, four key bytes in the final application of `AddRoundKey` and one key byte in the second-last application of `AddRoundKey`, in total nine key bytes, one can compute a candidate value for the sum of the texts in one byte position after four rounds of encryption. For a structure of 256 plaintexts of the form above, this sum is known to be zero. In fact, there will be values of the nine key bytes that will return zero as the value of the sum by chance. So to eliminate false alarms, the attack needs to be repeated a few times to uniquely determine the correct key bytes. Once the nine key bytes have been found, we find the remaining twelve key bytes of the final application of `AddRoundKey`, after which the user-selected key can be derived. Taking advantage of some advanced observations, there is a more effective extension of this attack. This can be used to find the secret key with $6 \cdot 2^{32}$ chosen plaintexts in a time equivalent to 2^{44} encryptions and 2^{32} words of memory [15, 22]. There have also been some further extensions to the basic Square attack, but these require an explosive increase in the running time [15, 22].

Another kind of structural attack that has been described against the AES is sometimes referred to as a *collision* or *bottleneck* attack. These attacks require around 2^{32} plaintexts and exploit a three-round structure [17, 24]. These approaches can be used to attack AES reduced to seven rounds but the running time is almost the same as an exhaustive search for the key.

5 Algebraic Attacks

We saw in Section 3.1 that the S-box was carefully constructed around inversion in $GF(2^8)$. As a consequence, if we appeal to our earlier notation (1), then we have the implicit equation $A^{-1}(S(x))x = 1$ for $x \neq 0$. Thus there are eight *quadratic* equations that relate the bits of $S(x)$ and x. Of these eight equations seven holds always, while the eighth holds only when $x \neq 0$, that is, in 255 of 256 cases. In addition, another 32 quadratic equations can be derived since $xy = 1$ implies that

$$x^2y = x,\ xy^2 = y,\ x^4y = x^3,\ \text{and that}\ xy^4 = y^3.$$

Each of these equations leads to eight quadratic equations on the bit level and all of these always hold. The resulting 39 quadratic equations turn out to be a