Lecture Notes in Computer Science 3373

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

Editorial Board

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

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

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

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