Lecture Notes in Computer Science 4047

Matthew Robshaw (Ed.)

Fast
Software Encryption

13th International Workshop, FSE 2006
Graz, Austria, March 15-17, 2006
Revised Selected Papers

Springer

Volume Editor

Matthew Robshaw
Telecom Research and Development
38-40 rue du General Leclerc, 92794 Issy les Moulineaux, Cedex 9, France
E-mail: matt.robshaw@francetelecom.com

Library of Congress Control Number: 2006928940

CR Subject Classification (1998): E.3, F.2.1, E.4, G.2, G.4

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-36597-4 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-36597-6 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springer.com

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11799313 06/3142 5 4 3 2 1 0

Preface

Fast Software Encryption (FSE) 2006 is the 13th in a series of workshops on symmetric cryptography. It has been sponsored for the last five years by the International Association for Cryptologic Research (IACR), and previous FSE workshops have been held around the world:

1993	Cambridge, UK	1994	Leuven, Belgium	1996	Cambridge, UK
1997	Haifa, Israel	1998	Paris, France	1999	Rome, Italy
2000	New York, USA	2001	Yokohama, Japan	2002	Leuven, Belgium
2003	Lund, Sweden	2004	New Delhi, India	2005	Paris, France

The FSE workshop is devoted to research on fast and secure primitives for symmetric cryptography, including the design and analysis of block ciphers, stream ciphers, encryption schemes, analysis and evaluation tools, hash functions, and message authentication codes.

This year more than 100 papers were submitted to FSE for the first time. After an extensive review by the Program Committee, 27 papers were presented at the workshop. Of course, the program would not have been complete without the invited speaker, and the presentation by Eli Biham on the early history of differential cryptanalysis was particularly appreciated by workshop attendees.

We are very grateful to the Program Committee and to all the external reviewers for their hard work. Each paper was refereed by at least three reviewers, with papers from Program Committee members receiving at least five reviews. The local Organizing Committee at Graz worked very hard and we particularly thank Melanie Blauensteiner, Christophe De Cannière, Sharif Ibrahim, Florian Mendel, Norbert Pramstaller, Christian Rechberger, and Michaela Tretter-Dragovic for their generous efforts and strong support. In Paris we are indebted to Henri Gilbert and Helena Handschuh, who shared their valuable experience from FSE 2005, and to Côme Berbain and Olivier Billet for proofreading and preparing the FSE pre-proceedings.

To close, we thank the IACR secretariat, Kevin McCurley, and Shai Halevi for their help with the registration process and we thank the IACR for their support of FSE. We are grateful to K.U. Leuven for their web-based review software and we thank both France Telecom and Siemens, Munich for their financial support of FSE 2006.

Matt Robshaw	France Telecom R&D	FSE 2006 Program Chair
Vincent Rijmen	Graz University of Technology	FSE 2006 General Chair

FSE 2006
March 15-17, 2006, Graz, Austria

Sponsored by the
International Association for Cryptologic Research (IACR)

Program and General Chairs

Matt Robshaw	France Telecom R&D	Program Chair
Vincent Rijmen	Graz University of Technology	General Chair

Program Committee

Kazumaro Aoki	NTT, Japan
Steve Babbage	Vodafone, UK
Anne Canteaut	INRIA, France
Carlos Cid	Royal Holloway, University of London, UK
Joan Daemen	STMicroelectronics, Belgium
Orr Dunkelman	Technion–Israel Institute of Technology, Israel
Helena Handschuh	Spansion, France
Thomas Johansson	Lund University, Sweden
Antoine Joux	DGA and University of Versailles, France
Charanjit Jutla	IBM Watson Research Center, USA
Xuejia Lai	Shanghai Jiaotong University, China
Stefan Lucks	University of Mannheim, Germany
Mitsuru Matsui	Mitsubishi Electric, Japan
Willi Meier	FH Aargau, Switzerland
Kaisa Nyberg	Helsinki University of Technology and Nokia, Finland
Elisabeth Oswald	Graz University of Technology, Austria
Bart Preneel	K.U.Leuven, Belgium
Håvard Raddum	University of Bergen, Norway
Matt Robshaw	France Telecom R&D, France
Phillip Rogaway	U.C.Davis, USA and Mah Fah Luang Univ., Thailand
Moti Yung	RSA Security and Columbia University, USA

Sponsors

France Telecom R&D
Siemens, Munich

External Reviewers

Frederik Armknecht
Daniel Augot
Elad Barkan
Mihir Bellare
Côme Berbain
Dan Bernstein
Eli Biham
Alex Biryukov
John Black
Nick Bone
Christophe de Cannière
Pascale Charpin
Frédéric Didier
Claus Diem
Martin Feldhofer
Henri Gilbert
Louis Granboulan
Johann Groszschaedl
Shai Halevi
Philip Hawkes
Martin Hell
Christoph Herbst
Tetsu Iwata
Nathan Keller
John Kelsey
Alexander Kholosha
Lars Knudsen
Ted Krovetz
Ulrich Kühn
Simon Künzli
Joe Lano
Cédric Lauradoux
Stefan Mangard
Florian Mendel
Marine Minier
Sean Murphy
Anderson Nascimento
Philippe Oechslin
Matthew Parker
Ludovic Perret
Raphael C.-W. Phan
Norbert Pramstaller
Christian Rechberger
Vincent Rijmen
Greg Rose
Markku-Juhani O. Saarinen
Tsuneo Sato
Eric Schost
Tom Shrimpton
Hervé Sibert
Dirk Stegemann
John Steinberger
Michael Steiner
Stefan Tillich
Jean-Pierre Tillich
Hiroki Ueda
Charlotte Vikkelso
Johan Wallén
Dai Watanabe
Ralf-Philipp Weinmann
Doug Whiting
Go Yamamoto
Kan Yasuda

Table of Contents

Stream Ciphers I

Block Ciphers

Hash Functions I

Analysis

Proposals

Hash Functions II

Modes and Models

Implementation and Bounds

Stream Ciphers II