

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Matthew Robshaw (Ed.)

Fast Software Encryption

13th International Workshop, FSE 2006

Graz, Austria, March 15-17, 2006

Revised Selected Papers

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

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media

springer.com

© Springer-Verlag Berlin Heidelberg 2006

Printed in Germany

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 proof-reading 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 Groszschädl
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 Vinkelso
Johan Wallén	Dai Watanabe	Ralf-Philipp Weinmann
Doug Whiting	Go Yamamoto	Kan Yasuda

Table of Contents

Stream Ciphers I

Cryptanalysis of Achterbahn <i>Thomas Johansson, Willi Meier, Frédéric Muller</i>	1
Cryptanalysis of Grain <i>Côme Berbain, Henri Gilbert, Alexander Maximov</i>	15
Cryptanalysis of the Stream Cipher DECIM <i>Hongjun Wu, Bart Preneel</i>	30

Block Ciphers

On Feistel Structures Using a Diffusion Switching Mechanism <i>Taizo Shirai, Kyoji Shibutani</i>	41
Pseudorandom Permutation Families over Abelian Groups <i>Louis Granboulan, Éric Leveil, Gilles Piret</i>	57
A Zero-Dimensional Gröbner Basis for AES-128 <i>Johannes Buchmann, Andrei Pyshkin, Ralf-Philipp Weinmann</i>	78

Hash Functions I

Cryptanalysis of the Full HAVAL with 4 and 5 Passes <i>Hongbo Yu, Xiaoyun Wang, Aaram Yun, Sangwoo Park</i>	89
Collisions and Near-Collisions for Reduced-Round Tiger <i>John Kelsey, Stefan Lucks</i>	111
Analysis of Step-Reduced SHA-256 <i>Florian Mendel, Norbert Pramstaller, Christian Rechberger, Vincent Rijmen</i>	126

Analysis

Improved Linear Distinguishers for SNOW 2.0 <i>Kaisa Nyberg, Johan Wallén</i>	144
--	-----

Reducing the Space Complexity of BDD-Based Attacks on Keystream Generators	
<i>Matthias Krause, Dirk Stegemann</i>	163
Breaking the ICE - Finding Multicollisions in Iterated Concatenated and Expanded (ICE) Hash Functions	
<i>Jonathan J. Hoch, Adi Shamir</i>	179

Proposals

A New Dedicated 256-Bit Hash Function: FORK-256	
<i>Deukjo Hong, Donghoon Chang, Jaechul Sung, Sangjin Lee, Seokhie Hong, Jaesang Lee, Dukjae Moon, Sungtaek Chee</i>	195
Some Plausible Constructions of Double-Block-Length Hash Functions	
<i>Shoichi Hirose</i>	210
Provably Secure MACs from Differentially-Uniform Permutations and AES-Based Implementations	
<i>Kazuhiko Minematsu, Yukiyasu Tsunoo</i>	226

Hash Functions II

Searching for Differential Paths in MD4	
<i>Martin Schl��ffer, Elisabeth Oswald</i>	242
A Study of the MD5 Attacks: Insights and Improvements	
<i>John Black, Martin Cochran, Trevor Highland</i>	262
The Impact of Carries on the Complexity of Collision Attacks on SHA-1	
<i>Florian Mendel, Norbert Pramstaller, Christian Rechberger, Vincent Rijmen</i>	278

Modes and Models

A New Mode of Encryption Providing a Tweakable Strong Pseudo-random Permutation	
<i>Debrup Chakraborty, Palash Sarkar</i>	293
New Blockcipher Modes of Operation with Beyond the Birthday Bound Security	
<i>Tetsu Iwata</i>	310

The Ideal-Cipher Model, Revisited: An Uninstantiable Blockcipher-Based Hash Function <i>John Black</i>	328
--	-----

Implementation and Bounds

How Far Can We Go on the x64 Processors? <i>Mitsuru Matsui</i>	341
Computing the Algebraic Immunity Efficiently <i>Frédéric Didier, Jean-Pierre Tillich</i>	359
Upper Bounds on Algebraic Immunity of Boolean Power Functions <i>Yassir Nawaz, Guang Gong, Kishan Chand Gupta</i>	375

Stream Ciphers II

Chosen-Ciphertext Attacks Against MOSQUITO <i>Antoine Joux, Frédéric Muller</i>	390
Distinguishing Attacks on the Stream Cipher Py <i>Souradyuti Paul, Bart Preneel, Gautham Sekar</i>	405
Resynchronization Attacks on WG and LEX <i>Hongjun Wu, Bart Preneel</i>	422
Author Index	433