

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

Alex Biryukov (Ed.)

Fast Software Encryption

14th International Workshop, FSE 2007
Luxembourg, Luxembourg, March 26-28, 2007
Revised Selected Papers

Volume Editor

Alex Biryukov

FSTC, University of Luxembourg

6, rue Richard Coudenhove-Kalergi, 1359 Luxembourg-Kirchberg, Luxembourg

E-mail: alex.biryukov@uni.lu

Library of Congress Control Number: 2007933305

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 3-540-74617-X Springer Berlin Heidelberg New York

ISBN-13 978-3-540-74617-1 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

© International Association for Cryptologic Research 2007

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper SPIN: 12115600 06/3180 5 4 3 2 1 0

Preface

Fast Software Encryption 2007 was the 14th annual workshop in the series, which was sponsored by the International Association for Cryptologic Research (IACR) for the sixth time. FSE has become a brand which attracts top research papers on symmetric cryptography. This includes papers on fast and secure primitives for symmetric cryptography, such as the design and analysis of block ciphers, stream ciphers, encryption schemes, hash functions, and message authentication codes (MACs), and on tools for analysis and evaluation. Previous editions of FSE took place in Cambridge, Leuven, Haifa, Rome, New York, Yokohama, Lund, Delhi, Paris, and Graz.

The Fast Software Encryption 2007 workshop was held March 26-28, 2007 in Luxembourg. It was organized by the General Chair Jean-Claude Asselborn (University of Luxembourg) in cooperation with the research lab LACS (Laboratory of Algorithms, Cryptography and Security) of the Computer Science and Communications research unit of the University of Luxembourg. The conference was attended by 160 registered participants from 36 different countries.

There were 104 papers submitted to FSE 2007, from which 28 were selected for presentation. The selection of papers was a challenging task, each submission had at least four reviewers, papers from Program Committee members having at least five. About 450 reviews were written by the committee and the external reviewers. The discussion phase was very fruitful, leading to more than 400 discussion comments in total, with several discussions going beyond 20 comments. I would like to thank the Program Committee and the external reviewers, who did an excellent job. It was a real pleasure to work with this team.

The conference program also featured an invited talk by Jean-Charles Faugère on the topic “Groebner Bases. Applications in Cryptology.” The traditional rump session with short informal presentations of recent results was chaired by Joan Daemen.

We would also like to thank the following people: Thomas Baignères and Matthieu Finiasz as the authors of the iChair review software; Dmitry Khovratchov for his help with the conference Web site and compilation of the proceedings; Volker Müller, Michel Carpentier, Christian Hutter, and SIU for videotaping the talks and providing a wireless LAN for the participants. We would like to thank the students of the Lycée Technique “Ecole de Commerce et de Gestion” and our secretaries Elisa Ferreira, Ragga Eyjolfssdottir, and Mireille Kies for their help in the organization of the workshop. We would also like to thank IACR and in particular Helena Handschuh, Shai Halevi, and Bart Preneel for constant support. Thanks to Britta Schlüter for the public relations work. Finally we are grateful to our sponsors FNR — Luxembourg National Research Fund — and the University of Luxembourg as well as the Centre de Culture et de Rencontre Neumünster, Ministry of Culture, Research and Universities.

FSE 2007

March 26–28, 2007, Luxembourg City, Luxembourg

Sponsored by
the International Association for Cryptologic Research (IACR)

General Chair

Jean-Claude Asselborn, University of Luxembourg, Luxembourg

Program Chair

Alex Biryukov, University of Luxembourg, Luxembourg

Program Committee

Frederik Armknecht	NEC, Germany
Steve Babbage	Vodafone, UK
Alex Biryukov (chair)	University of Luxembourg, Luxembourg
Claude Carlet	University of Paris 8 and INRIA, France
Nicolas Courtois	University College London, UK
Joan Daemen	STMicroelectronics, Belgium
Orr Dunkelman	K.U.Leuven, Belgium
Henri Gilbert	France Telecom, France
Louis Granboulan	EADS, France
Helena Handschuh	Spansion, France
Jin Hong	Seoul National University, Korea
Seokhie Hong	CIST, Korea
Tetsu Iwata	Nagoya University, Japan
Thomas Johansson	Lund University, Sweden
Antoine Joux	DGA and University of Versailles, France
Pascal Junod	Nagravision, Switzerland
Charanjit Jutla	IBM T.J. Watson Research Center, USA
John Kelsey	NIST, USA
Lars R. Knudsen	Technical University of Denmark, Denmark
Stefan Lucks	University of Mannheim, Germany
Mitsuru Matsui	Mitsubishi Electric, Japan
Willi Meier	FHNW, Switzerland

Kaisa Nyberg	Nokia and Helsinki University of Technology, Finland
Elisabeth Oswald	University of Bristol, UK
Josef Pieprzyk	Macquarie University, Australia
Bart Preneel	K.U.Leuven, Belgium
Greg Rose	Qualcomm, USA
Palash Sarkar	Indian Statistical Institute, India
Serge Vaudenay	EPFL, Switzerland

Subreviewers

Elena Andreeva	Cameron McDonald
Thomas Baignères	Florian Mendel
Gregory V. Bard	Marine Minier
Côme Berbain	Joydip Mitra
Guido Bertoni	Jean Monnerat
Olivier Billet	Alp Öztarhan
Nick Bone	Sylvain Pasini
Christophe De Cannière	Ludovic Perret
Chris Charnes	Thomas Peyrin
Lily Chen	Gilles Piret
Scott Contini	Thomas Popp
Morris Dworkin	Norbert Pramstaller
Martin Feldhofer	Emmanuel Prouff
Matthieu Finiasz	Christian Rechberger
Benedikt Gierlichs	Matt Robshaw
Sylvain Guilley	Allen Roginsky
Philip Hawkes	Martin Schläffer
Christoph Herbst	Yannick Seurin
Katrin Hoeper	Nicolas Sendrier
Deukjo Hong	Igor Shparlinski
Alexandre Karlov	Soren Steffen Thomsen
Nathan Keller	Dirk Stegemann
Alexander Kholosha	Ron Steinfeld
Dmitry Khovratovich	Jaechul Sung
Jongsung Kim	Daisuke Suzuki
Andrew Klapper	Emin Tatli
Özgül Küçük	Charlotte Vikkelsoe
Ulrich Kühn	Martin Vuagnoux
Changhoon Lee	Ralf-Philipp Weinmann
Svetla Nikova	Christopher Wolf
Stefan Mangard	Hongjun Wu
Stéphane Manuel	Jin Yuan
Krystian Matusiewicz	Erik Zenner
Alexander Maximov	

Table of Contents

Hash Function Cryptanalysis and Design (I)

Producing Collisions for PANAMA, Instantaneously	1
<i>Joan Daemen and Gilles Van Assche</i>	
Cryptanalysis of FORK-256	19
<i>Krystian Matusiewicz, Thomas Peyrin, Olivier Billet, Scott Contini, and Josef Pieprzyk</i>	
The Grindahl Hash Functions	39
<i>Lars R. Knudsen, Christian Rechberger, and Søren S. Thomsen</i>	

Stream Ciphers Cryptanalysis (I)

Overtaking VEST	58
<i>Antoine Joux and Jean-René Reinhard</i>	
Cryptanalysis of Achterbahn-128/80	73
<i>María Naya-Plasencia</i>	
Differential-Linear Attacks Against the Stream Cipher Phelix	87
<i>Hongjun Wu and Bart Preneel</i>	

Theory

How to Enrich the Message Space of a Cipher	101
<i>Thomas Ristenpart and Phillip Rogaway</i>	
Security Analysis of Constructions Combining FIL Random Oracles	119
<i>Yannick Seurin and Thomas Peyrin</i>	
Bad and Good Ways of Post-processing Biased Physical Random Numbers	137
<i>Markus Dichtl</i>	

Fast Talks: Block Cipher Cryptanalysis

Improved Slide Attacks	153
<i>Eli Biham, Orr Dunkelman, and Nathan Keller</i>	
A New Class of Weak Keys for Blowfish	167
<i>Orhun Kara and Cevat Manap</i>	

Fast Talks: Block Cipher Design

The 128-Bit Blockcipher CLEFIA (Extended Abstract)	181
<i>Taizo Shirai, Kyoji Shibutani, Toru Akishita, Shiho Moriai, and Tetsu Iwata</i>	
New Lightweight DES Variants	196
<i>Gregor Leander, Christof Paar, Axel Poschmann, and Kai Schramm</i>	

Block Cipher Cryptanalysis

A New Attack on 6-Round IDEA	211
<i>Eli Biham, Orr Dunkelman, and Nathan Keller</i>	
Related-Key Rectangle Attacks on Reduced AES-192 and AES-256	225
<i>Jongsung Kim, Seokhie Hong, and Bart Preneel</i>	
An Analysis of XSL Applied to BES	242
<i>Chu-Wee Lim and Khoongming Khoo</i>	

Stream Cipher Cryptanalysis (II)

On the Security of IV Dependent Stream Ciphers	254
<i>Côme Berbain and Henri Gilbert</i>	
Two General Attacks on Pomaranch-Like Keystream Generators	274
<i>Håkan Englund, Martin Hell, and Thomas Johansson</i>	
Analysis of QUAD	290
<i>Bo-Yin Yang, Owen Chia-Hsin Chen, Daniel J. Bernstein, and Jiun-Ming Chen</i>	

Cryptanalysis of Hash Functions (II)

Message Freedom in MD4 and MD5 Collisions: Application to APOP . . .	309
<i>Gaëtan Leurent</i>	
New Message Difference for MD4	329
<i>Yu Sasaki, Lei Wang, Kazuo Ohta, and Noboru Kunihiro</i>	
Algebraic Cryptanalysis of 58-Round SHA-1	349
<i>Makoto Sugita, Mitsuru Kawazoe, Ludovic Perret, and Hideki Imai</i>	

Theory of Stream Ciphers

Algebraic Immunity of S-Boxes and Augmented Functions	366
<i>Simon Fischer and Willi Meier</i>	

Generalized Correlation Analysis of Vectorial Boolean Functions	382
<i>Claude Carlet, Khoongming Khoo, Chu-Wee Lim, and Chuan-Wen Loe</i>	

Side Channel Attacks

An Analytical Model for Time-Driven Cache Attacks	399
<i>Kris Tiri, Onur Acıgmez, Michael Neve, and Flemming Andersen</i>	

MACs and Small Block Ciphers

Improving the Security of MACs Via Randomized Message Preprocessing.	414
<i>Yevgeniy Dodis and Krzysztof Pietrzak</i>	
New Bounds for PMAC, TMAC, and XCBC	434
<i>Kazuhiko Minematsu and Toshiyasu Matsushima</i>	
Perfect Block Ciphers with Small Blocks	452
<i>Louis Granboulan and Thomas Pornin</i>	

Author Index	467
-------------------------------	-----