

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

Alfred Kobsa

University of California, Irvine, CA, 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

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Kaisa Nyberg (Ed.)

Fast Software Encryption

15th International Workshop, FSE 2008
Lausanne, Switzerland, February 10-13, 2008
Revised Selected Papers



Springer

Volume Editor

Kaisa Nyberg
Helsinki University of Technology
Department of Information and Computer Science
Konemiehentie 2, 02150 Espoo, Finland
E-mail: kaisa.nyberg@tkk.fi

Library of Congress Control Number: 2008930931

CR Subject Classification (1998): E.3, I.1

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN	0302-9743
ISBN-10	3-540-71038-8 Springer Berlin Heidelberg New York
ISBN-13	978-3-540-71038-7 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 2008
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12435869 06/3180 5 4 3 2 1 0

Preface

Fast Software Encryption (FSE) is the 15th in a series of workshops on symmetric cryptography. It is sponsored 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
2006 Graz, Austria	2007 Luxembourg, Luxembourg	

The FSE workshop is devoted to the foreground 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 72 papers were submitted to FSE including a large number of high-quality and focused submissions, from which 26 papers for regular presentation and 4 papers for short presentation were selected. I wish to thank the authors of all submissions for their scientific contribution to the workshop. The workshop also featured an invited talk by Lars R. Knudsen with the title “Hash functions and SHA-3.” The traditional rump session with short informal presentations on current topics was organized and chaired by Daniel J. Bernstein.

Each submission was reviewed by at least three Program Committee members. Each submission originating from the Program Committee received at least five reviews. The final selection was made after a thorough discussion. I wish to thank all Program Committee members and referees for their generous work. I am also grateful to Thomas Baignères for maintaining and customizing the iChair review management software, which offered an excellent support for the demanding reviewing task. I would also like to thank him for setting up a beautiful and informative website and for compiling the pre-proceedings.

The efforts of the team members of the local Organizing Committee at Lausanne led by Serge Vaudenay and Thomas Baignères were particularly appreciated by the over 200 cryptographers who came from all over the world to attend the workshop. The support given to the FSE 2008 workshop by the sponsors École Polytechnique Fédérale de Lausanne, Nagravision and Nokia is also gratefully acknowledged.

March 2008

Kaisa Nyberg

FSE 2008

February 10–13, 2008, Lausanne, Switzerland

Sponsored by the
International Association for Cryptologic Research (IACR)

Program and General Chairs

Program Chair	Kaisa Nyberg Helsinki University of Technology and NOKIA, Finland
General Co-chairs	Serge Vaudenay and Thomas Baignères École Polytechnique Fédérale de Lausanne, Switzerland

Program Committee

Frederik Armknecht	Ruhr-University Bochum, Germany
Steve Babbage	Vodafone, UK
Alex Biryukov	University of Luxembourg, Luxembourg
John Black	University of Colorado, USA
Anne Canteaut	INRIA, France
Claude Carlet	University of Paris 8, France
Joan Daemen	STMicroelectronics, Belgium
Orr Dunkelman	Katholieke Universiteit Leuven, Belgium
Henri Gilbert	France Telecom, France
Louis Granboulan	EADS, France
Helena Handschuh	Spansion, France
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
Mitsuru Matsui	Mitsubishi Electric, Japan
Willi Meier	Fachhochschule Nordwestschweiz, Switzerland
Kaisa Nyberg (Chair)	Helsinki University of Technology and NOKIA, Finland
Elisabeth Oswald	University of Bristol, UK
Josef Pieprzyk	Macquarie University, Australia
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Vincent Rijmen	Katholieke Universiteit Leuven, Belgium and Graz University of Technology, Austria
Greg Rose	Qualcomm, USA

Referees

Jean-Philippe Aumasson
Côme Berbain
Daniel J. Bernstein
Olivier Billet
Nick Bone
Chris Charnes
Joo Yeon Cho
Scott Contini
Jean-Charles Faugère
Martin Feldhofer
Simon Fischer
Ewan Fleischmann
Raphael Fourquet
Thomas Fuhr
Samuel Galice
Sylvain Guilley
Phillip Hawkes
Alexandre Karlov
Shahram Khazaei
Dmitry Khovratovich
Ulrich Kühn
Yann Laigle-Chapuy
Mario Lamberger
Gregor Leander
Marco Macchetti
Stefan Mangard

Stéphane Manuel
Krystian Matusiewicz
Cameron McDonald
Florian Mendel
Marine Minier
Paul Morrissey
Ivica Nikolic
Ludovic Perret
Thomas Peyrin
Duong Hieu Phan
Norbert Pramstaller
Deike Priemuth-Schmid
Emmanuel Prouff
Christian Rechberger
Matthew Robshaw
Markku-Juhani Saarinen
Martin Schläffer
Joern-Marc Schmidt
Yannick Seurin
François-Xavier Standaert
Dirk Stegemann
Jean-Pierre Tillich
Stefan Tillich
Gilles Van Assche
Huaxiong Wang
Ralf-Philipp Weinmann

Sponsors

École Polytechnique Fédérale de Lausanne, Switzerland
Nagravision, Kudelski Group, Switzerland
Nokia, Finland

Table of Contents

SHA Collisions

Collisions for Step-Reduced SHA-256	1
<i>Ivica Nikolić and Alex Biryukov</i>	
Collisions on SHA-0 in One Hour	16
<i>Stéphane Manuel and Thomas Peyrin</i>	

New Hash Function Designs

The Hash Function Family LAKE	36
<i>Jean-Philippe Aumasson, Willi Meier, and Raphael C.-W. Phan</i>	
SWIFFT: A Modest Proposal for FFT Hashing	54
<i>Vadim Lyubashevsky, Daniele Micciancio, Chris Peikert, and Alon Rosen</i>	

Block Cipher Cryptanalysis (I)

A Unified Approach to Related-Key Attacks	73
<i>Eli Biham, Orr Dunkelman, and Nathan Keller</i>	
Algebraic and Slide Attacks on KeeLoq	97
<i>Nicolas T. Courtois, Gregory V. Bard, and David Wagner</i>	
A Meet-in-the-Middle Attack on 8-Round AES	116
<i>Hüseyin Demirci and Ali Aydın Selçuk</i>	

Implementation Aspects

Block Ciphers Implementations Provably Secure Against Second Order Side Channel Analysis	127
<i>Matthieu Rivain, Emmanuelle Dottax, and Emmanuel Prouff</i>	
SQUASH – A New MAC with Provable Security Properties for Highly Constrained Devices Such as RFID Tags	144
<i>Adi Shamir</i>	
Differential Fault Analysis of Trivium (Short Talk)	158
<i>Michal Hojsík and Bohuslav Rudolf</i>	

Accelerating the Whirlpool Hash Function Using Parallel Table Lookup and Fast Cyclical Permutation (Short Talk)	173
<i>Yedidya Hilewitz, Yiqun Lisa Yin, and Ruby B. Lee</i>	

Hash Function Cryptanalysis (I)

Second Preimage Attack on 3-Pass HAVAL and Partial Key-Recovery Attacks on HMAC/NMAC-3-Pass HAVAL	189
<i>Eunjin Lee, Donghoon Chang, Jongsung Kim, Jaechul Sung, and Seokhie Hong</i>	
Cryptanalysis of LASH	207
<i>Ron Steinfeld, Scott Contini, Krystian Matusiewicz, Josef Pieprzyk, Jian Guo, San Ling, and Huaxiong Wang</i>	
A (Second) Preimage Attack on the GOST Hash Function	224
<i>Florian Mendel, Norbert Pramstaller, and Christian Rechberger</i>	

Stream Cipher Cryptanalysis (I)

Guess-and-Determine Algebraic Attack on the Self-Shrinking Generator	235
<i>Blandine Debraize and Louis Goubin</i>	
New Form of Permutation Bias and Secret Key Leakage in Keystream Bytes of RC4	253
<i>Subhamoy Maitra and Goutam Paul</i>	
Efficient Reconstruction of RC4 Keys from Internal States	270
<i>Eli Biham and Yaniv Carmeli</i>	

Security Bounds

An Improved Security Bound for HCTR	289
<i>Debrup Chakraborty and Mridul Nandi</i>	
How to Encrypt with a Malicious Random Number Generator	303
<i>Seny Kamara and Jonathan Katz</i>	
A One-Pass Mode of Operation for Deterministic Message Authentication—Security beyond the Birthday Barrier	316
<i>Kan Yasuda</i>	

Entropy

Post-Processing Functions for a Biased Physical Random Number Generator	334
<i>Patrick Lacharme</i>	

Entropy of the Internal State of an FCSR in Galois Representation (Short Talk)	343
<i>Andrea R��ck</i>	

Block Cipher Cryptanalysis (II)

Bit-Pattern Based Integral Attack	363
<i>Muhammad Reza Z'aba, H��vard Raddum, Matt Henricksen, and Ed Dawson</i>	
Experiments on the Multiple Linear Cryptanalysis of Reduced Round Serpent	382
<i>Baudoin Collard, Fran��ois-Xavier Standaert, and Jean-Jacques Quisquater</i>	
Impossible Differential Cryptanalysis of CLEFIA	398
<i>Yukiyasu Tsunoo, Etsuko Tsujihara, Maki Shigeri, Teruo Saito, Tomoyasu Suzuki, and Hiroyasu Kubo</i>	

Hash Function Cryptanalysis (II)

MD4 Is Not One-Way	412
<i>Ga��tan Leurent</i>	
Improved Indifferentiability Security Analysis of chopMD Hash Function	429
<i>Donghoon Chang and Mridul Nandi</i>	
New Techniques for Cryptanalysis of Hash Functions and Improved Attacks on Snefru	444
<i>Eli Biham</i>	

Stream Cipher Cryptanalysis (II)

On the Salsa20 Core Function (Short Talk)	462
<i>Julio Cesar Hernandez-Castro, Juan M.E. Tapiador, and Jean-Jacques Quisquater</i>	
New Features of Latin Dances: Analysis of Salsa, ChaCha, and Rumba	470
<i>Jean-Philippe Aumasson, Simon Fischer, Shahram Khazaei, Willi Meier, and Christian Rechberger</i>	
Author Index	489