Lecture Notes in Computer Science 5086

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

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

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 Morrisey
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

New Hash Function Designs

Block Cipher Cryptanalysis (I)

Implementation Aspects

Hash Function Cryptanalysis (I)

Stream Cipher Cryptanalysis (I)

Security Bounds

Entropy

Block Cipher Cryptanalysis (II)

Hash Function Cryptanalysis (II)

Stream Cipher Cryptanalysis (II)