Lecture Notes in Computer Science 5665

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

Orr Dunkelman (Ed.)

Fast Software Encryption

16th International Workshop, FSE 2009
Leuven, Belgium, February 22-25, 2009
Revised Selected Papers

Springer

Volume Editor

Orr Dunkelman
École Normale Supérieure
Département d'Informatique
45 rue d'Ulm, 75230 Paris CEDEX 05, France
E-mail: orr.dunkelman@ens.fr

Library of Congress Control Number: 2009931058

CR Subject Classification (1998): E.3, I.1, E.2, D.4.6, K.6.5

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-642-03316-4 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-03316-2 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12731466 06/3180 5 4 3 2 1 0

Preface

Fast Software Encryption 2009 was the 16th in a series of workshops on symmetric key cryptography. Starting from 2002, it is sponsored by the International Association for Cryptologic Research (IACR). FSE 2009 was held in Leuven, Belgium, after previous venues held in Cambridge, UK (1993, 1996), Leuven, Belgium (1994, 2002), Haifa, Israel (1997), Paris, France (1998, 2005), Rome, Italy (1999), New York, USA (2000), Yokohama, Japan (2001), Lund, Sweden (2003), New Delhi, India (2004), Graz, Austria (2006), Luxembourg, Luxembourg (2007), and Lausanne, Switzerland (2008).

The workshop's main topic is symmetric key cryptography, including the design of fast and secure symmetric key primitives, such as block ciphers, stream ciphers, hash functions, message authentication codes, modes of operation and iteration, as well as the theoretical foundations of these primitives.

This year, 76 papers were submitted to FSE including a large portion of papers on hash functions, following the NIST SHA-3 competition, whose workshop was held just after FSE in the same location. From the 76 papers, 24 were accepted for presentation. It is my pleasure to thank all the authors of all submissions for the high-quality research, which is the base for the scientific value of the workshop. The review process was thorough (each submission received the attention of at least three reviewers), and at the end, besides the accepted papers, the Committee decided that the merits of the paper "Blockcipher-Based Hashing Revisited" entitled the authors to receive the best paper award. I wish to thank all Committee members and the referees for their hard and dedicated work.

The workshop also featured two invited talks. The first was given by Shay Gueron about "Intel's New AES Instructions for Enhanced Performance and Security" and the second was given by Matt Robshaw about "Looking Back at the eSTREAM Project." Along the presentation of the papers and the invited talks, the traditional rump session was organized and chaired by Dan J. Bernstein.

I would like to thank Thomas Baignères for the iChair review management software, which facilitated a smooth and easy review process, and Shai Halevi for the Web Submission and Review Software for dealing with the proceedings.

A special thanks is due to the organizing team. The COSIC team from Katholieke Universiteit Leuven, headed by Program Chair Bart Preneel, did a wonderful job in hosting the workshop. The warm welcome that awaited more than 200 delegates from all over the world was unblemished. The support given to the FSE 2009 workshop by the sponsors Katholieke Universiteit Leuven, PriceWaterhouseCoppers, and Oberthur technologies is also gratefully acknowledged.

May 2009 Orr Dunkelman

Fast Software Encryption 2009

Leuven, Belgium, February 22–25, 2009

Sponsored by the
International Association for Cryptologic Research (IACR)

Program and General Chairs

Program Chair	Orr Dunkelman École Normale Supérieure, France
General Chair	Bart Preneel Katholieke Universiteit Leuven, Belgium

Program Committee

Steve Babbage	Vodafone Group R&D, UK
Alex Biryukov	University of Luxembourg, Luxembourg
Dan J. Bernstein	University of Illinois at Chicago, USA
Joan Daemen	STMicroelectronics, Belgium
Christophe De Cannière	École Normale Supérieure, France and Katholieke Universiteit Leuven, Belgium
Orr Dunkelman (Chair)	École Normale Supérieure, France
Henri Gilbert	Orange Labs, France
Louis Granboulan	EADS Innovation Works, France
Helena Handschuh	Spansion, France
Tetsu Iwata	Nagoya University, Japan
Nathan Keller	Hebrew University, Israel
Stefan Lucks	Bauhaus-University Weimar, Germany
Mitsuru Matsui	Mitsubishi Electric, Japan
Willi Meier	FHNW, Switzerland
Kaisa Nyberg	Helsinki University of Technology and NOKIA, Finland
Raphael Phan	Loughborough University, UK
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Håvard Raddum	University of Bergen, Norway
Christian Rechberger	Graz University of Technology, Austria
Thomas Ristenpart	UC San Diego, USA
Greg Rose	Qualcomm, Australia
Serge Vaudenay	EPFL, Switzerland
Yiqun Lisa Yin	Independent Consultant, USA

Referees

Elena Andreeva
Kazumaro Aoki
Frederik Armknecht
Jean-Philippe Aumasson
Guido Bertoni
Olivier Billet
Billy Brumley
Rafik Chaabouni
Donghoon Chang
Joo Yeon Cho
Shanshan Duan
Baha Dundar
Ewan Fleischmann
Chistian Forler
Pasqualina Fragneto
Benedikt Gierlichs
Michael Gorski
Jian Guo
Risto Hakala
Miia Hermelin
Shoichi Hirose
Michael Hutter
Sebastiaan Indesteege
Kimmo Järvinen
Pascal Junod
Charanjit Jutla
Liam Keliher
Shahram Khazaei
Dmitry Khovratovich
Jongsung Kim
Matthias Krause
Mario Lamberger
Changhoon Lee
David McGrew
Florian Mendel
Nicky Mouha
Jorge Nakahara Jr.
Maria Naya-Plasencia
Ivica Nikolić
Khaled Ouafi
Matthew Parker
Sylvain Pasini
Chris Peikert
Thomas Peyrin
Thomas Roche
Martin Schläffer
Yannick Seurin
Zhijie Shi
Thomas Shrimpton
Hervé Sibert
Dirk Stegemann
Daisuke Suzuki
Stefano Tessaro
Stefan Tillich
Elena Trichina
Gilles Van Assche
Martin Vuagnoux
Ralf-Philipp Weinmann
Bo-Yin Yang
Scott Yilek
Erik Zenner
Fan Zhang

Sponsors

Katholieke Universiteit Leuven, Belgium
PriceWaterhouseCoppers, Belgium
Oberthur technologies, Belgium

Table of Contents

Stream Ciphers

Cube Testers and Key Recovery Attacks on Reduced-Round MD6 and Trivium 1
Jean-Philippe Aumasson, Itai Dinur, Willi Meier, and Adi Shamir

An Efficient State Recovery Attack on X-FCSR-256 23
Paul Stankovski, Martin Hell, and Thomas Johansson

Key Collisions of the RC4 Stream Cipher 38
Mitsuru Matsui

Invited Talk

Intel's New AES Instructions for Enhanced Performance and Security 51
Shay Gueron

Theory of Hash Functions

Blockcipher-Based Hashing Revisited 67
Martijn Stam

On the Security of TANDEM-DM 84
Ewan Fleischmann, Michael Gorski, and Stefan Lucks

Indifferentiability of Permutation-Based Compression Functions and Tree-Based Modes of Operation, with Applications to MD6 104
Yevgeniy Dodis, Leonid Reyzin, Ronald L. Rivest, and Emily Shen

Hash Functions Analysis I

Cryptanalysis of `RadioGatún` 122
Thomas Fuhr and Thomas Peyrin

Preimage Attacks on Reduced Tiger and SHA-2 139
Takanori Isobe and Kyoji Shibutani

Cryptanalysis of the LAKE Hash Family 156
Alex Biryukov, Praveen Gauravaram, Jian Guo, Dmitry Khovratovich, San Ling, Krystian Matusiewicz, Ivica Nikolić, Josef Pieprzyk, and Huaxiong Wang

Block Ciphers Analysis

New Cryptanalysis of Block Ciphers with Low Algebraic Degree 180
Bing Sun, Longjiang Qu, and Chao Li

Algebraic Techniques in Differential Cryptanalysis 193
Martin Albrecht and Carlos Cid

Multidimensional Extension of Matsui's Algorithm 2 209
Miia Hermelin, Joo Yeon Cho, and Kaisa Nyberg

Hash Functions Analysis II

Meet-in-the-Middle Attacks on SHA-3 Candidates 228
Dmitry Khovratovich, Ivica Nikolić, and Ralf-Philipp Weinmann

Practical Collisions for EnRUPT 246
Sebastiaan Indesteege and Bart Preneel

The Rebound Attack: Cryptanalysis of Reduced Whirlpool and `Grøstl` 260
Florian Mendel, Christian Rechberger, Martin Schläffer, and Søren S. Thomsen

Block Ciphers

Revisiting the IDEA Philosophy 277
Pascal Junod and Marco Macchetti

Cryptanalysis of the ISDB Scrambling Algorithm (MULTI2) 296
Jean-Philippe Aumasson, Jorge Nakahara Jr., and Pouyan Sepehrdad

Beyond-Birthday-Bound Security Based on Tweakable Block Cipher ... 308
Kazuhiko Minematsu

Theory of Symmetric Key

Enhanced Target Collision Resistant Hash Functions Revisited 327
Mohammad Reza Reyhanitabar, Willy Susilo, and Yi Mu

Message Authentication Codes

MAC Reforgeability 345
John Black and Martin Cochran

New Distinguishing Attack on MAC Using Secret-Prefix Method 363
Xiaoyun Wang, Wei Wang, Keting Jia, and Meiqin Wang

Fast and Secure CBC-Type MAC Algorithms 375
Mridul Nandi

HBS: A Single-Key Mode of Operation for Deterministic Authenticated Encryption 394
Tetsu Iwata and Kan Yasuda

Author Index 417