Lecture Notes in Computer Science 4593

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

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

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 cryptology. 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 Faugére 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 Khovratovich 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 Eyjolfsdottir, 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.

March 2007 Alex Biryukov

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

Table of Contents

Fast Talks: Block Cipher Design

Block Cipher Cryptanalysis

Stream Cipher Cryptanalysis (II)

Cryptanalysis of Hash Functions (II)

Theory of Stream Ciphers

Side Channel Attacks

MACs and Small Block Ciphers