Lecture Notes in Computer Science 6147

Seokhie Hong Tetsu Iwata (Eds.)

Fast Software Encryption

17th International Workshop, FSE 2010
Seoul, Korea, February 7-10, 2010
Revised Selected Papers

Springer

Volume Editors

Seokhie Hong
Korea University, CIST, Seoul, Korea
E-mail: hsh@cist.korea.ac.kr

Tetsu Iwata
Nagoya University, Dept. of Computational Science and Engineering, Japan
E-mail: iwata@cse.nagoya-u.ac.jp

Library of Congress Control Number: 2010929207

CR Subject Classification (1998): E.3, K.6.5, D.4.6, C.2, J.1, G.2.1

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-642-13857-8 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-13857-7 Springer Berlin Heidelberg New York

springer.com

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 06/3180

Preface

Fast Software Encryption (FSE) 2010, the 17th in a series of workshops on symmetric cryptography, was held in Seoul, Korea, during February 7–10, 2010. Since 2002, the FSE workshop has been sponsored by the International Association for Cryptologic Research (IACR). The first FSE workshop was held in Cambridge, UK (1993), followed by workshops in Leuven, Belgium (1994), Cambridge, UK (1996), Haifa, Israel (1997), Paris, France (1998), Rome, Italy (1999), New York, USA (2000), Yokohama, Japan (2001), Leuven, Belgium (2002), Lund, Sweden (2003), New Delhi, India (2004), Paris, France (2005), Graz, Austria (2006), Luxembourg, Luxembourg (2007), Lausanne, Switzerland (2008), and Leuven, Belgium (2009). The FSE workshop concentrates 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 67 papers were submitted. Each paper was reviewed by at least three reviewers, and papers (co-)authored by Program Committee members were reviewed by at least five reviewers. From the 67 papers, 21 were accepted for presentation at the workshop, and these proceedings contain the revised versions of the papers. At the end of the review phase, the Program Committee selected the paper “Attacking the Knudsen-Preneel Compression Functions” by Onur Özen, Thomas Shrimpton, and Martijn Stam to receive the best paper award. The workshop also featured two invited talks, “The Survey of Cryptanalysis on Hash Functions” by Xiaoyun Wang and “A Provable-Security Perspective on Hash Function Design” by Thomas Shrimpton. Along with the presentation of the papers and the invited talks, the rump session was organized and chaired by Orr Dunkelman.

We would like to thank all the authors for submitting their papers to the workshop. The selection of the papers was a challenging task, and we are deeply grateful to the Program Committee and to all the external reviewers for their hard work to ensure that each paper received a thorough and fair review. We would like to thank Shai Halevi for letting us use his Web Submission and Review Software, which was used for the entire review process from paper submission to preparing these proceedings.

We would also like to thank the General Co-chairs, Jongin Lim and Jongsung Kim, for their hard work, and we also would like to express our gratitude to CIST, Korea University and Korea Institute of Information Security and Cryptology (KIISC) for their support in organizing the workshop. The financial support given to the FSE 2010 workshop by Electronics and Telecommunications Research Institute (ETRI), Ellipsis, Korea University, LG CNS, and National Institute for Mathematical Science (NIMS) is also gratefully acknowledged.

April 2010

Seokhie Hong
Tetsu Iwata

FSE 2010

Seoul, Korea, February 7–10, 2010

Sponsored by the
International Association for Cryptologic Research (IACR)

General Co-chairs

Jongin Lim	Korea University, Korea
Jongsung Kim	Kyungnam University, Korea

Program Co-chairs

Seokhie Hong	Korea University, Korea
Tetsu Iwata	Nagoya University, Japan

Program Committee

Daniel J. Bernstein	University of Illinois at Chicago, USA
Alex Biryukov	University of Luxembourg, Luxembourg
Joan Daemen	STMicroelectronics, Belgium
Orr Dunkelman	École normale supérieure, France and Weizmann Institute, Israel
Helena Handschuh	Katholieke Universiteit Leuven, Belgium and Intrinsic-ID, USA
Seokhie Hong (Co-chair)	Korea University, Korea
Tetsu Iwata (Co-chair)	Nagoya University, Japan
Thomas Johansson	Lund University, Sweden
Antoine Joux	DGA and Université de Versailles, France
Charanjit S. Jutla	IBM T.J. Watson Research Center, USA
Stefan Lucks	Bauhaus-Universität Weimar, Germany
Mitsuru Matsui	Mitsubishi Electric, Japan
Willi Meier	FHNW, Switzerland
Kaisa Nyberg	Aalto University and NOKIA, Finland
Elisabeth Oswald	University of Bristol, UK
Josef Pieprzyk	Macquarie University, Australia
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Christian Rechberger	Katholieke Universiteit Leuven, Belgium
Thomas Ristenpart	UC San Diego, USA
Matt Robshaw	Orange Labs, France
Palash Sarkar	Indian Statistical Institute, India
Serge Vaudenay	EPFL, Switzerland
Kan Yasuda	NTT, Japan

External Reviewers

Elena Andreeva
Gilles Van Assche
Jean-Philippe Aumasson
Steve Babbage
Guido Bertoni
Andrey Bogdanov
Christophe De Cannière
Ji Young Cheon
Joo Yeon Cho
Martin Cochran
Ewan Fleischmann
Christian Forler
Praveen Gauravaram
Benedikt Gierlichs
Michael Gorski
Johann Groszschädl
Jian Guo
Risto Hakala
Philip Hawkes
Miia Hermelin
Shoichi Hirose
Sebastiaan Indesteege
Shahram Khazaei
Dmitry Khovratovich
Ilya Kizhvatov
Simon Knellwolf
Atefeh Mashatan
Krystian Matusiewicz
Cameron McDonald
Sarah Meiklejohn
Florian Mendel
Kazuhiko Minematsu
Petros Mol
Nicky Mouha
Tomislav Nad
Ivica Nikolić
Khaled Ouafi
Andrea Röck
Yu Sasaki
Martin Schläffer
Pouyan Sepehrdad
Yannick Seurin
Thomas Shrimpton
Przemysław Sokołowski
Daisuke Suzuki
Kerem Varıcı
Martin Vuagnoux

Organizing Support

CIST, Korea University
Korea Institute of Information Security and Cryptology (KIISC)

Financial Support

Electronics and Telecommunications Research Institute (ETRI)
Ellipsis
Korea University
LG CNS
National Institute for Mathematical Science (NIMS)

Table of Contents

Stream Ciphers and Block Ciphers

RFID and Implementations

Hash Functions I

Theory

Message Authentication Codes

Hash Functions II

Hash Functions III (Short Presentation)

Cryptanalysis