Lecture Notes in Computer Science 8424

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

Editorial Board

For further volumes:
http://www.springer.com/series/7410

Shiho Moriai (Ed.)

Fast Software Encryption

20th International Workshop, FSE 2013
Singapore, March 11–13, 2013
Revised Selected Papers

Springer

Editor
Shiho Moriai
Network Security Research Institute
National Institute of Information and
Communications Technology (NICT)
Tokyo
Japan

ISSN 0302-9743 ISSN 1611-3349 (electronic)
ISBN 978-3-662-43932-6 ISBN 978-3-662-43933-3 (eBook)
DOI 10.1007/978-3-662-43933-3
Springer Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014942655

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

The 20th International Workshop on Fast Software Encryption (FSE 2013) was held at Novotel Singapore Clarke Quay, Singapore, during March 11–13, 2013. The workshop was sponsored by the International Association for Cryptologic Research. FSE 2013 received 97 submissions from 24 countries. The 21 members of the Program Committee were assisted by more than 90 external reviewers. In total, they delivered 337 reviews. Each submission was reviewed by at least three Program Committee members. Submissions by Program Committee members received at least five reviews. The review process was double-blind, and conflicts of interest were carefully handled. The review process was handled through an online review system that supported discussions among Program Committee members. Over the entire review period, more than 200 messages were exchanged between Program Committee members. Eventually, the Program Committee selected 30 papers (a 31 % acceptance rate) for publication in the proceedings.

The program also included two invited talks, by Serge Vaudenay from Ecole Polytechnique Federale de Lausanne, Switzerland, and by Daniel Bernstein from University of Illinois at Chicago, USA, and Technische Universiteit Eindhoven, The Netherlands.

The Program Committee also identified the best submissions from FSE for their scientific quality, their originality, and their clarity. The FSE 2013 Best Paper Award went to Gordon Procter and Carlos Cid from Royal Holloway, University of London, United Kingdom. Their paper, "On Weak Keys and Forgery Attacks against Polynomial-based MAC Schemes", identifies some properties of hash functions based on polynomial evaluation that arise from the underlying algebraic structure.

Many people contributed to FSE 2013. We thank the authors for contributing their excellent research. We thank the Program Committee members, and their external reviewers, for making a significant effort to select for the program. We particularly thank Dmitry Khovratovich, Subhamoy Maitra, Florian Mendel, and Christian Rechberger for shepherding papers. Finally, we thank Jian Guo and Thomas Peyrin, the general co-chairs, and the FSE Steering Committee members, who worked so hard for the event and helped me a lot.

FSE 2013 collected a diversity of recent results in symmetric cryptography, from theory to practical aspects, from design to cryptanalysis. We feel privileged for the opportunity to develop the FSE 2013 program. We hope that the papers in these proceedings will continue to inspire, guide, and clarify your academic and professional endeavors.

May 2014 Shiho Moriai

FSE 2013

Workshop on Fast Software Encryption
Singapore, 11–13 March, 2013
Sponsored by the International Association
for Cryptologic Research

General Co-chairs

Jian Guo	Institute for Infocomm Research, Singapore
Thomas Peyrin	Nanyang Technological University, Singapore

Program Chairs

Shiho Moriai	NICT, Japan

Program Committee

Kazumaro Aoki	NTT Corporation, Japan
Jean-Philippe Aumasson	Kudelski Security, Switzerland
Alex Biryukov	University of Luxembourg, Luxembourg
Anne Canteaut	Inria Paris-Rocquencourt, France
Orr Dunkelman	University of Haifa and Weizmann Institute, Israel
Martin Hell	Lund University, Sweden
Tetsu Iwata	Nagoya University, Japan
John Kelsey	NIST, USA
Dmitry Khovratovich	University of Luxembourg, Luxembourg
Gregor Leander	Technical University of Denmark, Denmark
Subhamoy Maitra	ISI Kolkata, India
Florian Mendel	K.U. Leuven, Belgium
Maria Naya-Plasencia	Inria, France
Elisabeth Oswald	University of Bristol, UK
Christian Rechberger	Technical University of Denmark, Denmark
Vincent Rijmen	K.U. Leuven, Belgium and TU Graz, Austria
Matt Robshaw	Impinj, USA
Kyoji Shibutani	Sony Corporation, Japan
François-Xavier Standaert	Universite catholique de Louvain, Belgium
Gilles Van Assche	STMicroelectronics, Belgium

External Reviewers

Aagren, Martin
Ahmed Abdelraheem, Mohamed
Akishita, Toru
Albrecht, Martin
Arnab, Roy
Banciu, Valentina
Banik, Subhadeep
Bay, Asli
Bertoni, Guido
Bhattacharya, Srimanta
Bilgin, Begul
Blondeau, Céline
Bogdanov, Andrey
Borghoff, Julia
Boura, Christina
Burr, Bill
Carlet, Claude
Chattopadhyay, Anupam
Collard, Baudoin
Daemen, Joan
De Mulder, Yoni
Duc, Alexandre
Durvaux, François
Dworkin, Morris
Fuhr, Thomas
Gangopadhyay, Sugata
Gaëtan, Leurent
Gérard, Benoît
Grosso, Vincent
Gérard, Benoît
Güneysu, Tim
Hiwatari, Harunaga
Isobe, Takanori
Junod, Pascal
Kerckhof, Stéphanie
Kizhvatov, Ilya
Knellwolf, Simon
Kucuk, Ozgul
Lamberger, Mario
Lange, Tanja
Leurent, Gaetan
Lucks, Stefan
Luykx, Atul
Macchetti, Marco
Medwed, Marcel
Mehl Lauridsen, Martin
Meier, Willi
Melzani, Filippo
Mennink, Bart
Minier, Marine
Mironov, Ilya
Misoczki, Rafael
Mitsuda, Atsushi
Moradi, Amir
Nad, Tomislav
Nakahara Jr, Jorge
Nandi, Mridul
Nikolic, Ivica
Paul, Goutam
Peeters, Michaël
Perlner, Ray
Petit, Christophe
Peyrin, Thomas
Pietrzak, Krzysztof
Prouff, Emmanuel
Ralf-Philipp, Weinmann
Regazzoni, Francesco
Reinhard, Jean-René
Reyhanitabar, Reza
Ristenpart, Thomas
Sarkar, Palash
Sasaki, Yu
Schläffer, Martin
Schmidt, Joern-Marc
Sen Gupta, Sourav
Shimoyama, Takeshi
Shirai, Taizo
Sonmez Turan, Meltem
Stankovski, Paul
Susil, Petr

Tillich, Stefan
Tischhauser, Elmar
Todo, Yosuke
Toz, Deniz
Tunstall, Michael
Varici, Kerem
Vesselin, Velichkov
Veyrat-Charvillon, Nicolas
Whitnall, Carolyn
Wyseur, Brecht
Xagawa, Keita

Contents

Hash Functions

Message Authentication Codes

Provable Security

Implementation Aspects