Lecture Notes in Computer Science 7549

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

Anne Canteaut (Ed.)

Fast Software Encryption

19th International Workshop, FSE 2012
Washington, DC, USA, March 19-21, 2012
Revised Selected Papers

Springer

Volume Editor

Anne Canteaut
INRIA Paris-Rocquencourt
B.P. 105
78153 Le Chesnay, France
E-mail: anne.canteaut@inria.fr

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-34046-8 e-ISBN 978-3-642-34047-5
DOI 10.1007/978-3-642-34047-5
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012948466

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

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

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

Preface

These are the proceedings of FSE 2012, the 19th International Workshop on Fast Software Encryption. The workshop, organized in cooperation with the International Association for Cryptologic Research, was held March 19–21, 2012, in Washington DC. The General Chair was Bruce Schneier, from British Telecom, USA.

This year, a total of 89 papers were submitted to the workshop. Each submission was reviewed by at least three Program Committee (PC) members, while submissions co-authored by PC members were reviewed by at least five PC members. After the reviews were submitted, the committee deliberated online in depth and we eventually selected 24 submissions for presentation. The authors of the accepted papers were then given more than one month to revise their manuscript and to take into account the comments from the reviewers. This revision process allowed some interactions between the authors and the PC, and I am grateful to the PC members who spent a lot of time on this and contributed to guaranteeing the high standards of these papers. At the workshop, the papers were made available to the audience in electronic form. Then, the authors prepared the final versions which are included in these proceedings. Since these final versions were not checked again before publication, the authors bear the responsibility for the contents of their papers.

The PC selected three papers for invitation to the *Journal of Cryptology*: "Improved Rebound Attack on the Finalist Grøstl" by Jérémy Jean, María Naya-Plasencia, and Thomas Peyrin, "Recursive Diffusion Layers for Block Ciphers and Hash Functions" by Mahdi Sajadieh, Mohammad Dakhilalian, Hamid Mala, and Pouyan Sepehrdad, and "New attacks on Keccak-224 and Keccak-256" by Itai Dinur, Orr Dunkelman, and Adi Shamir.

In addition to the papers included in this volume, we were fortunate to have in the program two invited talks: one by Kaisa Nyberg on "Provable" Security against Differential and Linear Cryptanalysis" and the other by Mitsuru Matsui on "The History of Linear Cryptanalysis." An invited paper corresponding to Kaisa Nyberg's talk is included in the proceedings. The conference also featured a rump session with short informal presentations. Dan Bernstein and Tanja Lange served as the Chairs of the rump session.

I wish to thank all the authors who submitted their work to the conference. I am very grateful to the PC members for their hard and generous work. In addition, I gratefully acknowledge the help of a number of colleagues who provided reviews for the PC. I am also indebted to Andrei Voronkov for his very nice EasyChair conference management system that helped me compile this volume.

Finally, I would like to say that being the Program Chair for FSE 2012 has been a great honor and an exciting task.

May 2012 Anne Canteaut

Conference Organization

General Chair

Bruce Schneier	British Telecom, USA

Program Chair

Anne Canteaut	INRIA Paris-Rocquencourt, France

Program Committee

Alex Biryukov	University of Luxembourg, Luxembourg
Guang Gong	University of Waterloo, Canada
Martin Hell	Lund University, Sweden
Antoine Joux	Université de Versailles Saint-Quentin-en-Yvelines and DGA, France
Pascal Junod	HEIG-VD, Switzerland
John Kelsey	NIST, USA
Dmitry Khovratovich	Microsoft Research, USA
Lars Knudsen	Technical University of Denmark, Denmark
Gregor Leander	Technical University of Denmark, Denmark
Stefan Lucks	Bauhaus-Universität Weimar, Germany
Subhamoy Maitra	ISI Kolkata, India
Willi Meier	FHNW, Switzerland
Shiho Moriai	Sony Corporation, Japan
María Naya-Plasencia	Université de Versailles Saint-Quentin-en-Yvelines, France
Elisabeth Oswald	University of Bristol, UK
Vincent Rijmen	K.U. Leuven, Belgium and TU Graz, Austria
Matt Robshaw	Orange Labs, France
Yu Sasaki	NTT Corporation, Japan
François-Xavier Standaert	Université catholique de Louvain, Belgium
Gilles Van Assche	STMicroelectronics, Belgium
Serge Vaudenay	EPFL, Switzerland

External Reviewers

Mohamed Ahmed Abdelraheem
Toru Akishita
Kazumaro Aoki
Jean-Philippe Aumasson
Subhadeep Banik
Aslı Bay
Guido Bertoni
Rishiraj Bhattacharyya
Céline Blondeau
Andrey Bogdanov
Julia Borghoff
Ioana Boureanu
Qi Chai
Anupam Chattopadhyay
Jiazhe Chen
Baudoin Collard
Joan Daemen
Xinxin Fan
Matthieu Finiasz
Ewan Fleischmann
Christian Forler
Thomas Fuhr
Praveen Gauravaram
Benedikt Gierlichs
Kishan Gupta
Benoît Gérard
Honggang Hu
Takanori Isobe
Tetsu Iwata
Selçuk Kavut
Shahram Khazaei
Simon Knellwolf
Yuichi Komano
Gaëtan Leurent
Marco Macchetti
Atefeh Mashatan
Marcel Medwed
Florian Mendel
Mridul Nandi
Svetla Nikova
Kaisa Nyberg
Khaled Ouafi
Goutam Paul
Emmanuel Prouff
Christian Rechberger
Jean-René Reinhard
Arnab Roy
Santanu Sarkar
Martin Schläffer
Sourav Sen Gupta
Pouyan Sepehrdad
Yannick Seurin
Kyoji Shibutani
Taizo Shirai
Paul Stankovski
Fatih Sulak
Petr Sušil
Soren S. Thomsen
Stefan Tillich
Elmar Tischhauser
Deniz Toz
Michael Tunstall
Kerem Varici
Lei Wang
Ralf-Philipp Weinmann
Jakob Wenzel
Carolyn Whitnall
Teng Wu
Kan Yasuda
Bo Zhu
Martin Ågren

Table of Contents

Modes of Operation

Hash Functions II

New Tools for Cryptanalysis

New Designs

Keccak