

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Germany

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbruecken, Germany

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

© International Association for Cryptologic Research 2012

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

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 J  r  my Jean, Mar  a 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.

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
Ash 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 Shibusaki
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

Invited Talk

- “Provable” Security against Differential and Linear Cryptanalysis 1
Kaisa Nyberg

Block Ciphers

- Improved Attacks on Full GOST 9
Itai Dinur, Orr Dunkelman, and Adi Shamir
- Zero Correlation Linear Cryptanalysis with Reduced Data
Complexity 29
Andrey Bogdanov and Meiqin Wang

Differential Cryptanalysis

- A Model for Structure Attacks, with Applications to PRESENT
and Serpent 49
Meiqin Wang, Yue Sun, Elmar Tischhauser, and Bart Preneel
- A Methodology for Differential-Linear Cryptanalysis and
Its Applications 69
Jiqiang Lu
- New Observations on Impossible Differential Cryptanalysis
of Reduced-Round Camellia 90
*Ya Liu, Leibo Li, Dawu Gu, Xiaoyun Wang, Zhiqiang Liu,
Jiazhe Chen, and Wei Li*

Hash Functions I

- Improved Rebound Attack on the Finalist Grøstl 110
Jérémy Jean, María Naya-Plasencia, and Thomas Peyrin
- (Pseudo) Preimage Attack on Round-Reduced Grøstl Hash Function
and Others 127
*Shuang Wu, Dengguo Feng, Wenling Wu, Jian Guo, Le Dong, and
Jian Zou*
- Practical Cryptanalysis of ARMADILLO2 146
María Naya-Plasencia and Thomas Peyrin

On the (In)Security of IDEA in Various Hashing Modes 163
*Lei Wei, Thomas Peyrin, Przemysław Sokołowski, San Ling,
 Josef Pieprzyk, and Huaxiong Wang*

Modes of Operation

The Security of Ciphertext Stealing 180
Phillip Rogaway, Mark Wooding, and Haibin Zhang

McOE: A Family of Almost Foolproof On-Line Authenticated
 Encryption Schemes 196
Ewan Fleischmann, Christian Forler, and Stefan Lucks

Cycling Attacks on GCM, GHASH and Other Polynomial MACs
 and Hashes 216
Markku-Juhani O. Saarinen

Hash Functions II

Collision Attacks on the Reduced Dual-Stream Hash Function
 RIPEMD-128 226
Florian Mendel, Tomislav Nad, and Martin Schl affer

Bicliques for Preimages: Attacks on Skein-512 and the SHA-2 Family . . . 244
Dmitry Khovratovich, Christian Rechberger, and Alexandra Savelieva

Converting Meet-In-The-Middle Preimage Attack into Pseudo Collision
 Attack: Application to SHA-2 264
Ji Li, Takanori Isobe, and Kyoji Shibutani

New Tools for Cryptanalysis

UNAF: A Special Set of Additive Differences with Application
 to the Differential Analysis of ARX 287
*Vesselin Velichkov, Nicky Mouha, Christophe De Canni ere, and
 Bart Preneel*

ElimLin Algorithm Revisited 306
*Nicolas T. Courtois, Pouyan Sepehrdad, Petr Su il, and
 Serge Vaudenay*

New Designs

Short-Output Universal Hash Functions and Their Use in Fast
 and Secure Data Authentication 326
Long Hoang Nguyen and A.W. Roscoe

Lapin: An Efficient Authentication Protocol Based on Ring-LPN	346
<i>Stefan Heyse, Eike Kiltz, Vadim Lyubashevsky, Christof Paar, and Krzysztof Pietrzak</i>	
Higher-Order Masking Schemes for S-Boxes	366
<i>Claude Carlet, Louis Goubin, Emmanuel Prouff, Michael Quisquater, and Matthieu Rivain</i>	
Recursive Diffusion Layers for Block Ciphers and Hash Functions	385
<i>Mahdi Sajadieh, Mohammad Dakhilalian, Hamid Mala, and Pouyan Sepehrdad</i>	
Keccak	
Unaligned Rebound Attack: Application to Keccak	402
<i>Alexandre Duc, Jian Guo, Thomas Peyrin, and Lei Wei</i>	
Differential Propagation Analysis of Keccak	422
<i>Joan Daemen and Gilles Van Assche</i>	
New Attacks on Keccak-224 and Keccak-256	442
<i>Itai Dinur, Orr Dunkelman, and Adi Shamir</i>	
Author Index	463