

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, Lancaster, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Zürich, Switzerland

John C. Mitchell

Stanford University, Stanford, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Dortmund, Germany

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbrücken, Germany

More information about this series at <http://www.springer.com/series/7410>

Thomas Peyrin (Ed.)

Fast Software Encryption

23rd International Conference, FSE 2016
Bochum, Germany, March 20–23, 2016
Revised Selected Papers

Editor
Thomas Peyrin
Nanyang Technological University
Singapore
Singapore

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-662-52992-8 ISBN 978-3-662-52993-5 (eBook)
DOI 10.1007/978-3-662-52993-5

Library of Congress Control Number: 2016944480

LNCS Sublibrary: SL4 – Security and Cryptology

© International Association for Cryptologic Research 2016

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, 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.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer-Verlag GmbH Berlin Heidelberg

Preface

The 23rd International Conference on Fast Software Encryption (FSE 2016) was held at Bochum, Germany, during March 20–23, 2016. The conference was organized by Ruhr University Bochum with Gregor Leander serving as the general chair in collaboration with the International Association for Cryptologic Research (IACR). The conference had about 150 registered participants from 28 different countries. FSE 2016 received 91 submissions. The 25 members of the Program Committee were assisted by more than 80 external reviewers. In total, they delivered 304 reviews, with each submission being reviewed by at least three Program Committee members, five in the case of a submission co-authored by members of the Program Committee. The review process was double-blind, and conflicts of interest were handled carefully. It was managed through an online review system that supported discussions among Program Committee members. Eventually, the Program Committee selected 29 papers from 16 countries (a 31.9 % acceptance rate) for publication in the proceedings.

Besides the 29 selected talks, the program included one invited talk by Henri Gilbert from ANSSI, France, on white-box cryptography. The workshop also featured a rump session, chaired by Dan Bernstein and Tanja Lange, with several short informal presentations.

As in previous FSE events, the Program Committee identified the best submissions of the conference for their scientific quality, their originality, and their clarity. The FSE 2016 Best Paper Award went to José Bacelar Almeida, Manuel Barbosa, Gilles Barthe, and François Dupressoir, for their paper “Verifiable Side-Channel Security of Cryptographic Implementations: Constant-Time MEE-CBC.” This paper, along with the article “Stream Ciphers: A Practical Solution for Efficient Homomorphic-Ciphertext Compression” by Anne Canteaut, Sergiu Carpov, Caroline Fontaine, Tancrède Lepoint, María Naya-Plasencia, Pascal Paillier, and Renaud Sirdey received a special invitation for submission to the *Journal of Cryptology*.

Many people contributed to FSE 2016. I would like to thank the authors for contributing their excellent research, but also the Program Committee members and their external reviewers, who spent a lot time and effort reading and analyzing the numerous submissions. I really enjoyed the discussions during the selection phase and I am particularly grateful to Alex Biryukov, Christina Boura, Svetla Nikova, Yu Sasaki, François-Xavier Standaert, and Marc Stevens for accepting to shepherd papers. Finally, I sincerely thank Gregor Leander, the general chair, and his organization team, who worked so hard for the conference to be pleasant for all attendees. Their smooth organization made the event a big success.

I was extremely honored to serve as Program Chair of FSE 2016. The program contained a wide spectrum of the latest research in symmetric cryptography, ranging from cryptanalysis to security proofs, practical implementation aspects to foundations, and considering various primitives such as block ciphers, stream ciphers, hash functions, authenticated encryption, MAC, etc. I hope the selected papers will consolidate

our knowledge in symmetric cryptography, but also open new directions to continue making symmetric cryptography a vibrant research community.

May 2016

Thomas Peyrin

FSE 2016

23rd International Conference on Fast Software Encryption

Ruhr University Bochum, Germany
March 20–23, 2016

General Chair

Gregor Leander

Ruhr Universität Bochum, Germany

Program Chair

Thomas Peyrin

Nanyang Technological University, Singapore

Program Committee

Alex Biryukov

University of Luxembourg, Luxembourg

Christina Boura

University of Versailles, France

Itai Dinur

École Normale Supérieure, Paris, France

Orr Dunkelman

University of Haifa, Israel

Takanori Isobe

Sony Corporation, Japan

Tetsu Iwata

Nagoya University, Japan

Pascal Junod

HEIG-VD, Switzerland

Gaëtan Leurent

Inria, France

Florian Mendel

Graz University of Technology, Austria

Bart Mennink

KU Leuven, Belgium

Amir Moradi

Ruhr University Bochum, Germany

Mridul Nandi

Indian Statistical Institute, India

Ivica Nikolić

Nanyang Technological University, Singapore

Svetla Nikova

KU Leuven, Belgium

Kenny Paterson

Royal Holloway, University of London, UK

Thomas Peyrin (Chair)

Nanyang Technological University, Singapore

Christian Rechberger

DTU, Denmark

Yu Sasaki

NTT, Japan

Yannick Seurin

ANSSI, France

Thomas Shrimpton

University of Florida, USA

François-Xavier Standaert

Université Catholique de Louvain, Belgium

Marc Stevens

CWI Amsterdam, The Netherlands

Serge Vaudenay

Ecole Polytechnique Fédérale de Lausanne,
Switzerland

Lei Wang

Shanghai Jiao Tong University, China

Meiqin Wang

Shandong University, China

Additional Reviewers

Divesh Aggarwal	Lorenzo Grassi	Oscar Reparaz
Martin Albrecht	Vincent Grosso	Reza Reyhanitabar
Elena Andreeva	Jian Guo	Bastian Richter
Ralph Ankele	Harunaga Hiwatari	Vincent Rijmen
Tomer Ashur	Ashwin Jha	Arnab Roy
Jean-Philippe Aumasson	Anthony Journault	Pascal Sasdrich
Thomas Baignères	Pierre Karpman	Falk Schellenberg
Subhadeep Banik	Elif Bilge Kavun	Tobias Schneider
Achiya Bar-On	Dmitry Khovratovich	Jacob Schuldt
Georg T. Becker	Handan Kılınç	Sourav Sengupta
Christof Beierle	Miroslav Knezevic	Kyoji Shibutani
Rishiraj Bhattacharaya	Stefan Koelbl	Siang Meng Sim
Ritam Bhaumik	Virginie Lallemand	Valentin Suder
Begül Bilgin	Martin M. Lauridsen	Tyge Tiessen
Sonia Bogos	Meicheng Liu	Elmar Tischhauser
Anne Canteaut	Yunwen Liu	Yosuke Todo
Carlos Cid	Zhiqiang Liu	Aleksei Udovenko
Joan Daemen	Atul Luykx	Thomas Unterluggauer
Nilanjan Datta	Marco Macchetti	Thyla van der Merwe
Jean Paul Degabriele	Subhamoy Maitra	Kerem Varici
Daniel Dinu	Santos Merino Del Pozo	Vesselin Velichkov
Christoph Dobraunig	Sean Murphy	Damian Vizár
Alexandre Duc	Léo Paul Perrin	Wei Wang
Avijit Dutta	Peter Pessl	Alexander Wild
Maria Eichlseder	Jérôme Plût	Hongjun Wu
Sebastian Faust	Romain Poussier	Brecht Wyseur
Matthieu Finiasz	Shahram Rasoolzadeh	Guoyan Zhang
Thomas Fuhr	Francesco Regazzoni	Liting Zhang
Peter Gazi	Jean-René Reinhard	

Contents

Operating Modes

New Bounds for Keyed Sponges with Extendable Output: Independence Between Capacity and Message Length	3
<i>Yusuke Naito and Kan Yasuda</i>	
RIV for Robust Authenticated Encryption	23
<i>Farzaneh Abed, Christian Forler, Eik List, Stefan Lucks, and Jakob Wenzel</i>	
A MAC Mode for Lightweight Block Ciphers	43
<i>Atul Luykx, Bart Preneel, Elmar Tischhauser, and Kan Yasuda</i>	

Stream-Cipher Cryptanalysis

Cryptanalysis of the Full Spritz Stream Cipher	63
<i>Subhadeep Banik and Takanori Isobe</i>	
Attacks Against Filter Generators Exploiting Monomial Mappings	78
<i>Anne Canteaut and Yann Rotella</i>	

Components

Lightweight MDS Generalized Circulant Matrices	101
<i>Meicheng Liu and Siang Meng Sim</i>	
On the Construction of Lightweight Circulant Involutory MDS Matrices	121
<i>Yongqiang Li and Mingsheng Wang</i>	
Optimizing S-Box Implementations for Several Criteria Using SAT Solvers . . .	140
<i>Ko Stoffelen</i>	

Side-Channels and Implementations

Verifiable Side-Channel Security of Cryptographic Implementations: Constant-Time MEE-CBC	163
<i>José Bacelar Almeida, Manuel Barbosa, Gilles Barthe, and François Dupressoir</i>	
White-Box Cryptography in the Gray Box: – A Hardware Implementation and its Side Channels –	185
<i>Pascal Sasdrich, Amir Moradi, and Tim Güneysu</i>	

Detecting Flawed Masking Schemes with Leakage Detection Tests	204
<i>Oscar Reparaz</i>	

There Is Wisdom in Harnessing the Strengths of Your Enemy: Customized Encoding to Thwart Side-Channel Attacks	223
<i>Housseem Maghrebi, Victor Servant, and Julien Bringer</i>	

Automated Tools for Cryptanalysis

Automatic Search for Key-Bridging Technique: Applications to LBlock and TWINE	247
<i>Li Lin, Wenling Wu, and Yafei Zheng</i>	

MILP-Based Automatic Search Algorithms for Differential and Linear Trails for Speck	268
<i>Kai Fu, Meiqin Wang, Yinghua Guo, Siwei Sun, and Lei Hu</i>	

Automatic Search for the Best Trails in ARX: Application to Block Cipher SPECK	289
<i>Alex Biryukov, Vesselin Velichkov, and Yann Le Corre</i>	

Designs

Stream Ciphers: A Practical Solution for Efficient Homomorphic-Ciphertext Compression	313
<i>Anne Canteaut, Sergiu Carpov, Caroline Fontaine, Tancrede Lepoint, Maria Naya-Plasencia, Pascal Paillier, and Renaud Sirdey</i>	

Efficient Design Strategies Based on the AES Round Function	334
<i>Jérémy Jean and Ivica Nikolić</i>	

Block-Cipher Cryptanalysis

Bit-Based Division Property and Application to SIMON Family	357
<i>Yosuke Todo and Masakatu Morii</i>	

Algebraic Insights into the Secret Feistel Network.	378
<i>Léo Perrin and Aleksei Udovenko</i>	

Integrals Go Statistical: Cryptanalysis of Full Skipjack Variants	399
<i>Meiqin Wang, Tingting Cui, Huaifeng Chen, Ling Sun, Long Wen, and Andrey Bogdanov</i>	

Note on Impossible Differential Attacks.	416
<i>Patrick Derbez</i>	

Improved Linear Hull Attack on Round-Reduced SIMON with Dynamic Key-Guessing Techniques	428
<i>Huaifeng Chen and Xiaoyun Wang</i>	

Foundations and Theory

Modeling Random Oracles Under Unpredictable Queries	453
<i>Pooya Farshim and Arno Mittelbach</i>	
Practical Order-Revealing Encryption with Limited Leakage.	474
<i>Nathan Chenette, Kevin Lewi, Stephen A. Weis, and David J. Wu</i>	
Strengthening the Known-Key Security Notion for Block Ciphers.	494
<i>Benoît Cogliati and Yannick Seurin</i>	
Related-Key Almost Universal Hash Functions: Definitions, Constructions and Applications.	514
<i>Peng Wang, Yuling Li, Liting Zhang, and Kaiyan Zheng</i>	

Authenticated-Encryption and Hash Function Cryptanalysis

Key Recovery Attack Against 2.5-Round π -Cipher	535
<i>Christina Boura, Avik Chakraborti, Gaëtan Leurent, Goutam Paul, Dhiman Saha, Hadi Soleimany, and Valentin Suder</i>	
Cryptanalysis of Reduced NORX	554
<i>Nasour Bagheri, Tao Huang, Keting Jia, Florian Mendel, and Yu Sasaki</i>	
Analysis of the Kupyna-256 Hash Function	575
<i>Christoph Dobraunig, Maria Eichlseder, and Florian Mendel</i>	
Author Index	591