Lecture Notes in Computer Science 9783

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

Editorial Board

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

Springer

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

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

Contents