Lecture Notes in Computer Science 8540

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

Carlos Cid · Christian Rechberger (Eds.)

Fast Software Encryption

21st International Workshop, FSE 2014
London, UK, March 3–5, 2014
Revised Selected Papers

Springer

Editors
Carlos Cid
Royal Holloway, University of London
Egham
UK

Christian Rechberger
Technical University of Denmark
Lyngby
Denmark

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-662-46705-3 ISBN 978-3-662-46706-0 (eBook)
DOI 10.1007/978-3-662-46706-0

Library of Congress Control Number: 2015937349

LNCS Sublibrary: SL4 – Security and Cryptology

Springer Heidelberg New York Dordrecht London

Printed on acid-free paper

Springer-Verlag GmbH Berlin Heidelberg is part of Springer Science+Business Media (www.springer.com)

Preface

The 21st International Workshop on Fast Software Encryption (FSE 2014) was held in London March 3–5, 2014. The workshop was organized in cooperation with the International Association for Cryptologic Research, and took place at London's Natural History Museum. The workshop had 156 registered participants, of which 31 were students.

The FSE 2014 Program Committee comprised 26 members, and counted on the support of 75 external reviewers. We received 99 valid submissions, and each submission was reviewed by at least three PC members. After more than two months of deliberation and discussions, a total of 31 papers were accepted. This has been the highest number of accepted papers for an FSE so far, driven by the rather high quality of submissions. We are very grateful to all PC members and reviewers for their effort and contribution to the selection of an outstanding program of original articles in symmetric cryptography.

Besides the 31 selected talks, the workshop program also included two invited talks: Thomas Johansson from Lund University spoke on the application of low weight polynomials in cryptography; Thomas Ristenpart from the University of Wisconsin-Madison closed the workshop with the talk "New Encryption Primitives for Uncertain Times." The workshop also featured a rump session, chaired by Dan Bernstein and Tanja Lange, with several short informal presentations.

As it is tradition, the FSE 2014 Program Committee was asked to select the best submissions to the workshop, based on their scientific quality and contribution. Two submissions received the award for best papers: "Direct Construction of Recursive MDS Diffusion Layers using Shortened BCH Codes" by Daniel Augot and Matthieu Finiasz, and "Differential-Linear Cryptanalysis Revisited" by Céline Blondeau, Gregor Leander, and Kaisa Nyberg. The two papers also received a special solicitation for submission to the *Journal of Cryptology*.

In addition to the authors, PC members, and external reviewers, several other people contributed to the success of FSE 2014: colleagues, students, and supporting staff at DTU and Royal Holloway (in particular Claire Hudson); Shai Halevi, Greg Rose and abhi shelat at the IACR; the members of the FSE Steering Committee; Anne Kramer at Springer; and staff at the Natural History Museum. We were also fortunate to count on the financial support of four sponsors (CESG, KPMG, NXP, and Visa Europe), which made it possible to hold the event in such an impressive venue. We are very grateful to you all for your support.

It was a great honor to have been in charge of the organization of FSE 2014 and to coordinate the selection of its scientific program. It gave us the opportunity to work with a number of outstanding researchers and professionals in the cryptographic community; we were very pleased with its success and greatly enjoyed it. We hope the reader also enjoys the papers in these proceedings.

January 2015

Carlos Cid
Christian Rechberger

FSE 2014

21st International Workshop on Fast Software Encryption
Natural History Museum, London, UK
March 3–5, 2014

General Chairs

Carlos Cid	Royal Holloway, University of London, UK
Christian Rechberger	Technical University of Denmark, Denmark

Program Chairs

Carlos Cid	Royal Holloway, University of London, UK
Christian Rechberger	Technical University of Denmark, Denmark

Program Committee

Martin R. Albrecht	Technical University of Denmark, Denmark
Elena Andreeva	Katholieke Universiteit Leuven, Belgium
Kazumaro Aoki	NTT, Japan
Frederik Armknecht	University of Mannheim, Germany
Daniel J. Bernstein	University of Illinois at Chicago, USA, and Technische Universiteit, Eindhoven, The Netherlands
John Black	University of Colorado at Boulder, USA
Anne Canteaut	Inria Paris-Rocquencourt, France
Joan Daemen	STMicroelectronics, Belgium
Christophe De Cannière	Google, Switzerland
Orr Dunkelman	University of Haifa, Israel
Martin Hell	Lund University, Sweden
Dmitry Khovratovich	University of Luxembourg, Luxembourg
Gregor Leander	Ruhr Universität Bochum, Germany
Subhamoy Maitra	Indian Statistical Institute, Kolkata, India
Mitsuru Matsui	Mitsubishi Electric, Japan
Florian Mendel	Technische Universtität Graz, Austria
Svetla Nikova	Katholieke Universiteit Leuven, Belgium
Elisabeth Oswald	University of Bristol, UK
Thomas Peyrin	Nanyang Technological University, Singapore
Josef Pieprzyk	Macquarie University, Australia
Martijn Stam	University of Bristol, UK
François-Xavier Standaert	Université catholique de Louvain, Belgium
Serge Vaudenay	EPFL, Switzerland
Hongbo Yu	Tsinghua University, China

External Reviewers

Hoda A. Alkhzaimi
Gilles Van Assche
Jean-Philippe Aumasson
Subhadeep Banik
Harry Bartlett
Aslı Bay
Guido Bertoni
Begul Bilgin
Andrey Bogdanov
Sonia Bogos
Christina Boura
Daniel Cabarcas
Claude Carlet
Anupam Chattopadhyay
Alexandre Duc
François Durvaux
Maria Eichlseder
Sebastian Faust
Vincent Grosso
Sourav Sen Gupta
Jialin Huang
Andreas Hülsing
Takanori Isobe
Tetsu Iwata
Guo Jian
Philipp Jovanovic
Angela Jäschke
Pierre Karpman
Elif Kavun
Nathan Keller
Stéphanie Kerckhof
Lars R. Knudsen
Matthias Krause
Stefan Kölbl
Martin M. Lauridsen
Gaëtan Leurent
Zhiqiang Liu
Atul Luykx
Daniel Martin
Bart Mennink
Vasily Mikhalev
Pawel Morawiecki
Nicky Mouha
Tomislav Nad
Mridul Nandi
Ivica Nikolic
Kaisa Nyberg
Kenny Paterson
Michaël Peeters
Ludovic Perret
Christiane Peters
Romain Poussier
Santos Merino Del Pozo
Francesco Regazzoni
Reza Reyhanitabar
Vincent Rijmen
Phillip Rogaway
Santanu Sarkar
Martin Schläffer
Peter Schwabe
Takeshi Shimoyama
Paul Stankovski
Ron Steinfeld
Petr Susil
Seth Terashima
Tyge Tiessen
Kerem Varici
Vesselin Velichkov
Huaxiong Wang
Lei Wang
Meiqin Wang
Quingju Wang
Gaven Watson
Tolga Yalcin
Yusi (James) Zhang

Contents