

*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>

Carlos Cid · Christian Rechberger (Eds.)

# Fast Software Encryption

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

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  
© International Association for Cryptologic Research 2015

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

Springer-Verlag GmbH Berlin Heidelberg is part of Springer Science+Business Media  
([www.springer.com](http://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.

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

# Contents

## Designs

|   |    |
|---|----|
| Direct Construction of Recursive MDS Diffusion Layers Using Shortened BCH Codes . . . . . | 3  |
| <i>Daniel Augot and Matthieu Finiasz</i>  |    |
| LS-Designs: Bitslice Encryption for Efficient Masked Software Implementations . . . . .   | 18 |
| <i>Vincent Grosso, Gaëtan Leurent, François-Xavier Standaert, and Kerem Varici</i>        |    |
| SPRING: Fast Pseudorandom Functions from Rounded Ring Products. . . . .                   | 38 |
| <i>Abhishek Banerjee, Hai Brenner, Gaëtan Leurent, Chris Peikert, and Alon Rosen</i>      |    |

## Cryptanalysis I

|  |     |
|--|-----|
| Match Box Meet-in-the-Middle Attack Against KATAN . . . . .                              | 61  |
| <i>Thomas Fuhr and Brice Minaud</i>  |     |
| Collision Spectrum, Entropy Loss, T-Sponges, and Cryptanalysis of GLUON-64 . . . . .     | 82  |
| <i>Léo Perrin and Dmitry Khovratovich</i>  |     |
| Improved All-Subkeys Recovery Attacks on FOX, KATAN and SHACAL-2 Block Ciphers . . . . . | 104 |
| <i>Takanori Isobe and Kyoji Shibutani</i>  |     |
| Improved Single-Key Attacks on 9-Round AES-192/256 . . . . .                             | 127 |
| <i>Leibo Li, Keting Jia, and Xiaoyun Wang</i>  |     |

## Authenticated Encryption

|   |     |
|---|-----|
| CLOC: Authenticated Encryption for Short Input . . . . .  | 149 |
| <i>Tetsu Iwata, Kazuhiko Minematsu, Jian Guo, and Sumio Morioka</i>   |     |
| APE: Authenticated Permutation-Based Encryption for Lightweight Cryptography. . . . .                       | 168 |
| <i>Elena Andreeva, Begül Bilgin, Andrey Bogdanov, Atul Luykx, Bart Mennink, Nicky Mouha, and Kan Yasuda</i> |     |



|   |     |
|---|-----|
| COBRA: A Parallelizable Authenticated Online Cipher Without Block Cipher Inverse . . . . .                    | 187 |
| <i>Elena Andreeva, Atul Luykx, Bart Mennink, and Kan Yasuda</i>   |     |
| Pipelineable On-line Encryption . . . . .   | 205 |
| <i>Farzaneh Abed, Scott Fluhrer, Christian Forler, Eik List, Stefan Lucks, David McGrew, and Jakob Wenzel</i> |     |
| Cryptanalysis of FIDES . . . . .  | 224 |
| <i>Itai Dinur and Jérémy Jean</i>   |     |
| <b>Foundations and Theory</b>   |     |
| Security Analysis of Key-Alternating Feistel Ciphers . . . . .  | 243 |
| <i>Rodolphe Lampe and Yannick Seurin</i>  |     |
| The Related-Key Analysis of Feistel Constructions . . . . .   | 265 |
| <i>Manuel Barbosa and Pooya Farshim</i>   |     |
| The Indistinguishability of the XOR of $k$ Permutations . . . . .   | 285 |
| <i>Benoit Cogliati, Rodolphe Lampe, and Jacques Patarin</i>   |     |
| Impact of ANSI X9.24-1:2009 Key Check Value on ISO/IEC 9797-1:2011 MACs . . . . .                             | 303 |
| <i>Tetsu Iwata and Lei Wang</i>   |     |
| <b>Stream Ciphers</b>   |     |
| Plaintext Recovery Attacks Against WPA/TKIP . . . . .   | 325 |
| <i>Kenneth G. Paterson, Bertram Poettering, and Jacob C.N. Schuldt</i>  |     |
| Dependence in IV-Related Bytes of RC4 Key Enhances Vulnerabilities in WPA . . . . .                           | 350 |
| <i>Sourav Sen Gupta, Subhamoy Maitra, Willi Meier, Goutam Paul, and Santanu Sarkar</i>                        |     |
| <b>Cryptanalysis II</b>   |     |
| Probabilistic Slide Cryptanalysis and Its Applications to LED-64 and Zorro . . . . .                          | 373 |
| <i>Hadi Soleimany</i>   |     |
| Improved Linear Sieving Techniques with Applications to Step-Reduced LED-64 . . . . .                         | 390 |
| <i>Itai Dinur, Orr Dunkelman, Nathan Keller, and Adi Shamir</i>   |     |

Differential-Linear Cryptanalysis Revisited . . . . . 411  
*Céline Blondeau, Gregor Leander, and Kaisa Nyberg*

Improved Slender-Set Linear Cryptanalysis . . . . . 431  
*Guo-Qiang Liu, Chen-Hui Jin, and Chuan-Da Qi*

Cryptanalysis of KLEIN . . . . . 451  
*Virginie Lallemand and María Naya-Plasencia*

**Hash Functions**

Branching Heuristics in Differential Collision Search with Applications  
to SHA-512 . . . . . 473  
*María Eichlseder, Florian Mendel, and Martin Schläffer*

On the Minimum Number of Multiplications Necessary for Universal  
Hash Functions . . . . . 489  
*Mridul Nandi*

Collision Attack on 5 Rounds of Grøstl . . . . . 509  
*Florian Mendel, Vincent Rijmen, and Martin Schläffer*

**Cryptanalysis III**

Differential Cryptanalysis of Round-Reduced SIMON and SPECK . . . . . 525  
*Farzaneh Abed, Eik List, Stefan Lucks, and Jakob Wenzel*

Differential Analysis of Block Ciphers SIMON and SPECK . . . . . 546  
*Alex Biryukov, Arnab Roy, and Vesselin Velichkov*

Equivalent Key Recovery Attacks Against HMAC and NMAC  
with Whirlpool Reduced to 7 Rounds . . . . . 571  
*Jian Guo, Yu Sasaki, Lei Wang, Meiqin Wang, and Long Wen*

Multiple Differential Cryptanalysis of Round-Reduced PRINCE . . . . . 591  
*Anne Canteaut, Thomas Fuhr, Henri Gilbert, María Naya-Plasencia,  
and Jean-René Reinhard*

**Advanced Constructions**

Efficient Fuzzy Search on Encrypted Data . . . . . 613  
*Alexandra Boldyreva and Nathan Chenette*

**Author Index** . . . . . 635