

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

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Zürich, Switzerland

John C. Mitchell

Stanford University, Stanford, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Bern, Switzerland

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, Saarbruecken, Germany

For further volumes:

<http://www.springer.com/series/7410>

Shiho Moriai (Ed.)

Fast Software Encryption

20th International Workshop, FSE 2013
Singapore, March 11–13, 2013
Revised Selected Papers

Editor
Shiho Moriai
Network Security Research Institute
National Institute of Information and
Communications Technology (NICT)
Tokyo
Japan

ISSN 0302-9743 ISSN 1611-3349 (electronic)
ISBN 978-3-662-43932-6 ISBN 978-3-662-43933-3 (eBook)
DOI 10.1007/978-3-662-43933-3
Springer Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014942655

© Springer-Verlag Berlin Heidelberg 2014

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. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

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.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

The 20th International Workshop on Fast Software Encryption (FSE 2013) was held at Novotel Singapore Clarke Quay, Singapore, during March 11–13, 2013. The workshop was sponsored by the International Association for Cryptologic Research. FSE 2013 received 97 submissions from 24 countries. The 21 members of the Program Committee were assisted by more than 90 external reviewers. In total, they delivered 337 reviews. Each submission was reviewed by at least three Program Committee members. Submissions by Program Committee members received at least five reviews. The review process was double-blind, and conflicts of interest were carefully handled. The review process was handled through an online review system that supported discussions among Program Committee members. Over the entire review period, more than 200 messages were exchanged between Program Committee members. Eventually, the Program Committee selected 30 papers (a 31 % acceptance rate) for publication in the proceedings.

The program also included two invited talks, by Serge Vaudenay from Ecole Polytechnique Federale de Lausanne, Switzerland, and by Daniel Bernstein from University of Illinois at Chicago, USA, and Technische Universiteit Eindhoven, The Netherlands.

The Program Committee also identified the best submissions from FSE for their scientific quality, their originality, and their clarity. The FSE 2013 Best Paper Award went to Gordon Procter and Carlos Cid from Royal Holloway, University of London, United Kingdom. Their paper, “On Weak Keys and Forgery Attacks against Polynomial-based MAC Schemes”, identifies some properties of hash functions based on polynomial evaluation that arise from the underlying algebraic structure.

Many people contributed to FSE 2013. We thank the authors for contributing their excellent research. We thank the Program Committee members, and their external reviewers, for making a significant effort to select for the program. We particularly thank Dmitry Khovratovich, Subhamoy Maitra, Florian Mendel, and Christian Rechberger for shepherding papers. Finally, we thank Jian Guo and Thomas Peyrin, the general co-chairs, and the FSE Steering Committee members, who worked so hard for the event and helped me a lot.

FSE 2013 collected a diversity of recent results in symmetric cryptography, from theory to practical aspects, from design to cryptanalysis. We feel privileged for the opportunity to develop the FSE 2013 program. We hope that the papers in these proceedings will continue to inspire, guide, and clarify your academic and professional endeavors.

FSE 2013

Workshop on Fast Software Encryption
Singapore, 11–13 March, 2013

Sponsored by the International Association
for Cryptologic Research

General Co-chairs

Jian Guo
Thomas Peyrin

Institute for Infocomm Research, Singapore
Nanyang Technological University, Singapore

Program Chairs

Shiho Moriai

NICT, Japan

Program Committee

Kazumaro Aoki	NTT Corporation, Japan
Jean-Philippe Aumasson	Kudelski Security, Switzerland
Alex Biryukov	University of Luxembourg, Luxembourg
Anne Canteaut	Inria Paris-Rocquencourt, France
Orr Dunkelman	University of Haifa and Weizmann Institute, Israel
Martin Hell	Lund University, Sweden
Tetsu Iwata	Nagoya University, Japan
John Kelsey	NIST, USA
Dmitry Khovratovich	University of Luxembourg, Luxembourg
Gregor Leander	Technical University of Denmark, Denmark
Subhamoy Maitra	ISI Kolkata, India
Florian Mendel	K.U. Leuven, Belgium
Maria Naya-Plasencia	Inria, France
Elisabeth Oswald	University of Bristol, UK
Christian Rechberger	Technical University of Denmark, Denmark
Vincent Rijmen	K.U. Leuven, Belgium and TU Graz, Austria
Matt Robshaw	Impinj, USA
Kyoji Shibutani	Sony Corporation, Japan
François-Xavier Standaert	Universite catholique de Louvain, Belgium
Gilles Van Assche	STMicroelectronics, Belgium

External Reviewers

Aagren, Martin
Ahmed Abdelraheem, Mohamed
Akishita, Toru
Albrecht, Martin
Arnab, Roy
Banciu, Valentina
Banik, Subhadeep
Bay, Asli
Bertoni, Guido
Bhattacharya, Srimanta
Bilgin, Begül
Blondeau, Céline
Bogdanov, Andrey
Borghoff, Julia
Boura, Christina
Burr, Bill
Carlet, Claude
Chattopadhyay, Anupam
Collard, Baudoin
Daemen, Joan
De Mulder, Yoni
Duc, Alexandre
Durvaux, François
Dworkin, Morris
Fuhr, Thomas
Gangopadhyay, Sugata
Gaëtan, Laurent
Gérard, Benoît
Grosso, Vincent
Gérard, Benoît
Güneysu, Tim
Hiwatari, Harunaga
Isobe, Takanori
Junod, Pascal
Kerckhof, Stéphanie
Kizhvatov, Ilya
Knellwolf, Simon
Kucuk, Ozgul
Lamberger, Mario
Lange, Tanja

Leurent, Gaetan
Lucks, Stefan
Luykx, Atul
Macchetti, Marco
Medwed, Marcel
Mehl Lauridsen, Martin
Meier, Willi
Melzani, Filippo
Mennink, Bart
Minier, Marine
Mironov, Ilya
Misoczki, Rafael
Mitsuda, Atsushi
Moradi, Amir
Nad, Tomislav
Nakahara Jr, Jorge
Nandi, Mridul
Nikolic, Ivica
Paul, Goutam
Peeters, Michaël
Perlner, Ray
Petit, Christophe
Peyrin, Thomas
Pietrzak, Krzysztof
Prouff, Emmanuel
Ralf-Philipp, Weinmann
Regazzoni, Francesco
Reinhard, Jean-René
Reyhanitabar, Reza
Ristenpart, Thomas
Sarkar, Palash
Sasaki, Yu
Schläffer, Martin
Schmidt, Joern-Marc
Sen Gupta, Sourav
Shimoyama, Takeshi
Shirai, Taizo
Sonmez Turan, Meltem
Stankovski, Paul
Susil, Petr

Tillich, Stefan
Tischhauser, Elmar
Todo, Yosuke
Toz, Deniz
Tunstall, Michael
Varici, Kerem

Vesselin, Velichkov
Veyrat-Charvillon, Nicolas
Whitnall, Carolyn
Wyseur, Brecht
Xagawa, Keita

Contents

Block Ciphers

Complementing Feistel Ciphers	3
<i>Alex Biryukov and Ivica Nikolić</i>	
On the Wrong Key Randomisation and Key Equivalence Hypotheses in Matsui's Algorithm 2	19
<i>Andrey Bogdanov and Elmar Tischhauser</i>	
Cryptanalysis of WIDEA	39
<i>Gaëtan Leurent</i>	

Invited Talk

Towards Secure Distance Bounding	55
<i>Ioana Boureanu, Aikaterini Mitrokotsa, and Serge Vaudenay</i>	

Lightweight Block Ciphers

Reflection Cryptanalysis of PRINCE-Like Ciphers	71
<i>Hadi Soleimany, Céline Blondeau, Xiaoli Yu, Wenling Wu, Kaisa Nyberg, Huiling Zhang, Lei Zhang, and Yanfeng Wang</i>	
Security Analysis of PRINCE	92
<i>Jérémy Jean, Ivica Nikolić, Thomas Peyrin, Lei Wang, and Shuang Wu</i>	
Cryptanalysis of Round-Reduced LED.	112
<i>Ivica Nikolić, Lei Wang, and Shuang Wu</i>	

Tweakable Block Ciphers

Tweakable Blockciphers with Asymptotically Optimal Security	133
<i>Rodolphe Lampe and Yannick Seurin</i>	

Stream Ciphers I

Smashing WEP in a Passive Attack	155
<i>Pouyan Sepehrdad, Petr Sušil, Serge Vaudenay, and Martin Vuagnoux</i>	
Full Plaintext Recovery Attack on Broadcast RC4	179
<i>Takanori Isobe, Toshihiro Ohigashi, Yuhei Watanabe, and Masakatu Morii</i>	

Hash Functions

Time-Memory Trade-Offs for Near-Collisions 205
Gaëtan Leurent

Collision Attacks on Up to 5 Rounds of SHA-3 Using Generalized
 Internal Differentials 219
Itai Dinur, Orr Dunkelman, and Adi Shamir

Rotational Cryptanalysis of Round-Reduced KECCAK 241
Paweł Morawiecki, Josef Pieprzyk, and Marian Srebrny

Partial-Collision Attack on the Round-Reduced Compression Function
 of Skein-256 263
Hongbo Yu, Jiazhe Chen, and Xiaoyun Wang

Message Authentication Codes

On Weak Keys and Forgery Attacks Against Polynomial-Based
 MAC Schemes 287
Gordon Procter and Carlos Cid

Secure Message Authentication Against Related-Key Attack 305
Rishiraj Bhattacharyya and Arnab Roy

Provable Security

Attacks and Security Proofs of EAX-Prime 327
Kazuhiko Minematsu, Stefan Lucks, Hiraku Morita, and Tetsu Iwata

Towards Understanding the Known-Key Security of Block Ciphers 348
Elena Andreeva, Andrey Bogdanov, and Bart Mennink

On Symmetric Encryption with Distinguishable Decryption Failures 367
*Alexandra Boldyreva, Jean Paul Degabriele, Kenneth G. Paterson,
 and Martijn Stam*

Implementation Aspects

Minimalism of Software Implementation 393
Mitsuru Matsui and Yumiko Murakami

Higher-Order Side Channel Security and Mask Refreshing 410
*Jean-Sébastien Coron, Emmanuel Prouff, Matthieu Rivain,
 and Thomas Roche*

Masking Tables—An Underestimated Security Risk 425
Michael Tunstall, Carolyn Whitnall, and Elisabeth Oswald

Lightweight Authenticated Encryption

ALE: AES-Based Lightweight Authenticated Encryption. 447
Andrey Bogdanov, Florian Mendel, Francesco Regazzoni, Vincent Rijmen, and Elmar Tischhauser

Related-Key Attacks Against Full Hummingbird-2 467
Markku-Juhani O. Saarinen

Stream Ciphers II

A Low Data Complexity Attack on the GMR-2 Cipher Used
in the Satellite Phones. 485
Ruilin Li, Heng Li, Chao Li, and Bing Sun

Improving Key Recovery to 784 and 799 Rounds of Trivium
Using Optimized Cube Attacks. 502
Pierre-Alain Fouque and Thomas Vannet

Near Collision Attack on the Grain v1 Stream Cipher. 518
Bin Zhang, Zhenqi Li, Dengguo Feng, and Dongdai Lin

Automated Cryptanalysis

Exhausting Demirci-Selçuk Meet-in-the-Middle Attacks Against
Reduced-Round AES. 541
Patrick Derbez and Pierre-Alain Fouque

A Framework for Automated Independent-Biclique Cryptanalysis 561
Farzaneh Abed, Christian Forler, Eik List, Stefan Lucks, and Jakob Wenzel

Boolean Functions

A New Criterion for Avoiding the Propagation of Linear Relations
Through an Sbox 585
Christina Boura and Anne Canteaut

Author Index 605