Lecture Notes in Computer Science 8282

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

Editorial Board

For further volumes:
http://www.springer.com/series/7410

Tanja Lange · Kristin Lauter
Petr Lisoněk (Eds.)

Selected Areas in Cryptography – SAC 2013

20th International Conference
Burnaby, BC, Canada, August 14–16, 2013
Revised Selected Papers

Springer

Editors
Tanja Lange
Technische Universiteit Eindhoven
Eindhoven
The Netherlands

Petr Lisoněk
Simon Fraser University
Burnaby, BC
Canada

Kristin Lauter
Microsoft Research
Redmond, WA
USA

ISSN 0302-9743 ISSN 1611-3349 (electronic)
ISBN 978-3-662-43413-0 ISBN 978-3-662-43414-7 (eBook)
DOI 10.1007/978-3-662-43414-7
Springer Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014939415

LNCS Sublibrary: SL4 – Security and Cryptology

Printed on acid-free paper

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

Preface

Previously called the Workshop on Selected Areas in Cryptography, the Conference on Selected Areas in Cryptography (SAC) series was initiated in 1994, when the first workshop was held at Queen's University in Kingston. The SAC conference has been held annually since 1994 in various Canadian locations, including Calgary, Kingston, Montreal, Ottawa, Sackville, St. John's, Toronto, Waterloo, and Windsor. More information on SAC conferences can be found at the main SAC conferences website at http://sacconference.org/.

SAC 2013 was the 20th conference in this series, and for this special occasion it was extended to a two-and-half day conference, which was attended by 65 participants.

This volume contains revised versions of papers presented at SAC 2013, held during August 14–16, 2013, at Simon Fraser University in Burnaby, Canada. The objective of the conference is to present cutting-edge research in the designated areas of cryptography and to facilitate future research through an informal and friendly conference setting.

The themes for the SAC 2013 conference were:

- Design and analysis of symmetric key primitives and cryptosystems, including block and stream ciphers, hash functions and MAC algorithms
- Efficient implementations of symmetric and public key algorithms
- Mathematical and algorithmic aspects of applied cryptology
- Elliptic and hyperelliptic curve cryptography, including theory and applications of pairings

There were 105 paper submissions, of which seven were withdrawn prior to the submission deadline, and 98 submissions were refereed. Each submission was reviewed by at least three Program Committee members. Submissions (co-)authored by a Program Committee member were reviewed by at least five Program Committee members. Upon recommendations of the Program Committee, 26 papers were accepted making the acceptance rate 26/98 = 26.5 %. The program also included four invited lectures, which were given by Paulo Barreto, Anne Canteaut, Antoine Joux, and Douglas Stinson. The speakers were invited to submit papers to the proceedings; these invited papers underwent a thorough reviewing process.

We greatly appreciate the hard work of the SAC 2013 Program Committee. We are also very grateful to the many others who participated in the review process. The reviewing process was run using the iChair software, written by Thomas Baignères from CryptoExperts, France, and Matthieu Finiasz from EPFL, LASEC, Switzerland. We are grateful to them for letting us use their software.

SAC 2013 was generously supported by its sponsors and partners: Microsoft Research, Tutte Institute for Mathematics and Computing, Simon Fraser University, Pacific Institute for the Mathematical Sciences, and Interdisciplinary Research in the

Mathematical and Computational Sciences Centre (IRMACS) at Simon Fraser University. The conference was held in co-operation with the International Association for Cryptologic Research (IACR). Hugh Williams from the Tutte Institute delivered the invited lecture "The Tutte Institute for Mathematics and Computing."

Special thanks go to Carlisle Adams, Huapeng Wu, and Ali Miri for generously sharing their experience in organizing SAC conferences with us. We would also like to thank Springer for publishing the SAC proceedings series since 1998 in the *Lecture Notes in Computer Science* series.

We would like to thank Pam Borghardt, Zena Bruneau, and Kelly Gardiner for their hard and tireless work in taking care of the local arrangements.

November 2013

Tanja Lange
Kristin Lauter
Petr Lisoněk

SAC 2013
Conference on Selected Areas in Cryptography

Burnaby, Canada
August 14–16, 2013

Program Chairs

Tanja Lange	Technische Universiteit Eindhoven, The Netherlands
Kristin Lauter	Microsoft Research, USA
Petr Lisoněk	Simon Fraser University, Canada

Program Committee

Carlisle Adams	University of Ottawa, Canada
Jean-Philippe Aumasson	Kudelski Security, Switzerland
Paulo S.L.M. Barreto	University of São Paulo, Brazil
Lejla Batina	Radboud University Nijmegen, The Netherlands and KU Leuven, Belgium
Daniel J. Bernstein	University of Illinois at Chicago, USA and Technische Universiteit Eindhoven, The Netherlands
Andrey Bogdanov	Technical University of Denmark, Denmark
Joppe Bos	Microsoft Research, USA
Christophe De Cannière	Google Switzerland, Switzerland
Anne Canteaut	Inria Paris-Rocquencourt, France
Sanjit Chatterjee	Indian Institute of Science, India
Carlos Cid	Royal Holloway, University of London, UK
Craig Costello	Microsoft Research, USA
Joan Daemen	ST Microelectronics, Belgium
Vassil Dimitrov	University of Calgary, Canada
Orr Dunkelman	University of Haifa, Israel
Andreas Enge	Inria Bordeaux-Sud-Ouest and University of Bordeaux, France
Matthieu Finiasz	CryptoExperts, France
Guang Gong	University of Waterloo, Canada
Tim Güneysu	Ruhr University Bochum, Germany
Huseyin Hisil	Yasar University, Turkey
Sorina Ionica	ENS Paris, France
Mike Jacobson	University of Calgary, Canada
Dmitry Khovratovich	University of Luxembourg, Luxembourg

Tanja Lange (co-chair)	Technische Universiteit Eindhoven, The Netherlands
Kristin Lauter (co-chair)	Microsoft Research, USA
Gregor Leander	Ruhr University Bochum, Germany
Hyang-Sook Lee	Ewha Womans University, Republic of Korea
Jooyoung Lee	Sejong University, Seoul, Republic of Korea
Gaëtan Leurent	UCL Crypto Group, Belgium
Petr Lisoněk (co-chair)	Simon Fraser University, Canada
Stefan Lucks	University Weimar, Germany
Alfred Menezes	University of Waterloo, Canada
Michael Naehrig	Microsoft Research, USA
María Naya-Plasencia	Inria Paris-Rocquencourt, France
Kaisa Nyberg	Aalto University, Finland
Roger Oyono	Université de la Polynésie Française, French Polynesia
Daniel Page	University of Bristol, UK
Christiane Peters	Technical University of Denmark, Denmark
Bart Preneel	KU Leuven, Belgium
Christian Rechberger	Technical University of Denmark, Denmark
Christophe Ritzenthaler	Institut de Mathématiques de Luminy, France
Damien Robert	Inria Bordeaux Sud-Ouest, France
Francisco Rodríguez-Henríquez	CINVESTAV-IPN, Mexico
Yu Sasaki	NTT Secure Platform Laboratories, Japan
Renate Scheidler	University of Calgary, Canada
Martin Schläffer	Graz University of Technology, Austria
Peter Schwabe	Radboud University Nijmegen, The Netherlands
Douglas R. Stinson	University of Waterloo, Canada
Andrew Sutherland	MIT, USA
Vanessa Vitse	Université Joseph Fourier, France
Michael J. Wiener	Irdeto, Canada

External Reviewers

Hoda A. Alkhzaimi	Céline Blondeau	Sebastian Faust
Farzaneh Abed	Andrey Bogdanov	Robert Fitzpatrick
Jithra Adikari	Charles Bouillaguet	Christian Forler
Gora Adj	Christina Boura	Steven Galbraith
Elena Andreeva	Donghoon Chang	Nadia Heninger
Kazumaro Aoki	Jung Hee Cheon	Andreas Hülsing
Thomas Baignères	Itai Dinur	Fei Huo
Guido Bertoni	Christophe Doche	Kimmo Järvinen
Rishiraj Bhattacharyya	Baris Ege	Koray Karabina
Begul Bilgin	Maria Eichlseder	Elif Bilge Kavun
Gaetan Bisson	Xinxin Fan	Nathan Keller

Taechan Kim
Thomas Korak
Soonhak Kwon
Pascal Lafourcade
Martin Gagné
Cédric Lauradoux
Martin M. Lauridsen
Tancréde Lepoint
Yang Li
Seongan Lim
Eik List
Jake Loftus
Adriana Lopez-Alt
Cuauhtemoc Mancillas
Ingo von Maurich
Florian Mendel
Oliver Mischke
Amir Moradi
Sayantan Mukherjee
Sean Murphy
Samuel Neves
Thomaz Oliveira
Cheol-Min Park
Souradyuti Paul
Thomas Pöppelmann
Gordon Procter
Francesco Regazzoni
Matthieu Rivain
Joern-Marc Schmidt
Michael Schneider
Kyoji Shibutani
Boris Skoric
Hadi Soleimany
Raphael Spreitzer
Damien Stehle
Valentin Suder
Yin Tan
Enrico Thomae
Nicolas Thériault
Mehdi Tibouchi
Elmar Tischhauser
Deniz Toz
Michael Tunstall
Gilles Van Assche
Kerem Varici
Damien Vergnaud
Vincent Verneuil
Vanessa Vitse
Jakob Wenzel
Carolyn Whitnall
Brecht Wyseur
Tolga Yalcin
Bo-Yin Yang
Masaya Yasuda
Yongjin Yeom
Bo Zhu
Ralf Zimmermann

Abstract of Invited Talk

Similarities Between Encryption and Decryption: How Far Can We Go?

Anne Canteaut

INRIA Paris-Rocquencourt, France
anne.canteaut@inria.fr

Abstract. In this talk, I will investigate some approaches for reducing the hardware footprint of a block cipher for different constraints of the targeted applications. In this context, I will focus on the strategies which can be used for minimizing the overhead for decryption on top of encryption. These strategies include involutive ciphers and the construction used in PRINCE. In particular, I will discuss the potential weaknesses which might be introduced by this type of constructions.

Contents

Invited Talk

The Realm of the Pairings 3
Diego F. Aranha, Paulo S.L.M. Barreto, Patrick Longa, and Jefferson E. Ricardini

Lattices Part I

A Three-Level Sieve Algorithm for the Shortest Vector Problem 29
Feng Zhang, Yanbin Pan, and Gengran Hu

Improvement and Efficient Implementation of a Lattice-Based Signature Scheme 48
Rachid El Bansarkhani and Johannes Buchmann

Towards Practical Lattice-Based Public-Key Encryption on Reconfigurable Hardware 68
Thomas Pöppelmann and Tim Güneysu

Invited Talk

Practical Approaches to Varying Network Size in Combinatorial Key Predistribution Schemes 89
Kevin Henry, Maura B. Paterson, and Douglas R. Stinson

Discrete Logarithms

A Group Action on $\mathbb{Z}_p^\times$ and the Generalized DLP with Auxiliary Inputs 121
Jung Hee Cheon, Taechan Kim, and Yong Soo Song

Solving a 6120-bit DLP on a Desktop Computer 136
Faruk Göloğlu, Robert Granger, Gary McGuire, and Jens Zumbrägel

Stream Ciphers and Authenticated Encryption

How to Recover Any Byte of Plaintext on RC4 155
Toshihiro Ohigashi, Takanori Isobe, Yuhei Watanabe, and Masakatu Morii

The LOCAL Attack: Cryptanalysis of the Authenticated Encryption Scheme ALE 174
Dmitry Khovratovich and Christian Rechberger

AEGIS: A Fast Authenticated Encryption Algorithm. 185
Hongjun Wu and Bart Preneel

Post–quantum (Hash-Based and System Solving)

Fast Exhaustive Search for Quadratic Systems in $\mathbb{F}_2$ on FPGAs 205
Charles Bouillaguet, Chen-Mou Cheng, Tung Chou, Ruben Niederhagen, and Bo-Yin Yang

Faster Hash-Based Signatures with Bounded Leakage 223
Thomas Eisenbarth, Ingo von Maurich, and Xin Ye

White Box Crypto

White-Box Security Notions for Symmetric Encryption Schemes 247
Cécile Delerablée, Tancrède Lepoint, Pascal Paillier, and Matthieu Rivain

Two Attacks on a White-Box AES Implementation 265
Tancrède Lepoint, Matthieu Rivain, Yoni De Mulder, Peter Roelse, and Bart Preneel

Block Ciphers

Extended Generalized Feistel Networks Using Matrix Representation 289
Thierry P. Berger, Marine Minier, and Gaël Thomas

Zero-Correlation Linear Cryptanalysis with FFT and Improved Attacks on ISO Standards Camellia and CLEFIA 306
Andrey Bogdanov, Huizheng Geng, Meiqin Wang, Long Wen, and Baudoin Collard

Implementing Lightweight Block Ciphers on `x86` Architectures 324
Ryad Benadjila, Jian Guo, Victor Lomné, and Thomas Peyrin

Invited Talk

A New Index Calculus Algorithm with Complexity $L(1/4 + o(1))$ in Small Characteristic 355
Antoine Joux

Lattices Part II

High Precision Discrete Gaussian Sampling on FPGAs 383
Sujoy Sinha Roy, Frederik Vercauteren, and Ingrid Verbauwhede

Discrete Ziggurat: A Time-Memory Trade-Off for Sampling from a Gaussian Distribution over the Integers 402
Johannes Buchmann, Daniel Cabarcas, Florian Göpfert, Andreas Hülsing, and Patrick Weiden

Elliptic Curves, Pairings and RSA

A High-Speed Elliptic Curve Cryptographic Processor for Generic Curves over GF(p) 421
Yuan Ma, Zongbin Liu, Wuqiong Pan, and Jiwu Jing

Exponentiating in Pairing Groups 438
Joppe W. Bos, Craig Costello, and Michael Naehrig

Faster Repeated Doublings on Binary Elliptic Curves 456
Christophe Doche and Daniel Sutantyo

Montgomery Multiplication Using Vector Instructions 471
Joppe W. Bos, Peter L. Montgomery, Daniel Shumow, and Gregory M. Zaverucha

Hash Functions and MACs

Improved Single-Key Distinguisher on HMAC-MD5 and Key Recovery Attacks on Sandwich-MAC-MD5 493
Yu Sasaki and Lei Wang

Provable Second Preimage Resistance Revisited 513
Charles Bouillaguet and Bastien Vayssière

Multiple Limited-Birthday Distinguishers and Applications 533
Jérémy Jean, María Naya-Plasencia, and Thomas Peyrin

Side-Channel Attacks

Horizontal Collision Correlation Attack on Elliptic Curves 553
Aurélie Bauer, Eliane Jaulmes, Emmanuel Prouff, and Justine Wild

When Reverse-Engineering Meets Side-Channel Analysis – Digital Lockpicking in Practice 571
David Oswald, Daehyun Strobel, Falk Schellenberg, Timo Kasper, and Christof Paar

Author Index 589