

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, 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, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, 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

Palash Sarkar Tetsu Iwata (Eds.)

Advances in Cryptology – ASIACRYPT 2014

20th International Conference on the Theory
and Application of Cryptology and Information Security
Kaoshiung, Taiwan, December 7-11, 2014
Proceedings, Part I



Springer

Volume Editors

Palash Sarkar
Indian Statistical Institute
Applied Statistics Unit
203, B.T. Road, Kolkata 700108, India
E-mail: palash@isical.ac.in

Tetsu Iwata
Nagoya University
Department of Computer Science and Engineering
Furo-cho, Chikusa-ku, Nagoya 464-8603, Japan
E-mail: iwata@cse.nagoya-u.ac.jp

ISSN 0302-9743

e-ISSN 1611-3349

ISBN 978-3-662-45610-1

e-ISBN 978-3-662-45611-8

DOI 10.1007/978-3-662-45611-8

Springer Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014954246

LNCS Sublibrary: SL 4 – Security and Cryptology

© International Association for Cryptologic Research 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.

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

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

Preface

It is with great pleasure that we present the proceedings of Asiacrypt 2014 in two volumes of *Lecture Notes in Computer Science* published by Springer. The year 2014 marked the 20th edition of the International Conference on Theory and Application of Cryptology and Information Security held annually in Asia by the International Association for Cryptologic Research (IACR). The conference was sponsored by the IACR and was jointly organized by the following consortium of universities and government departments of the Republic of China (Taiwan): National Sun Yat-sen University; Academia Sinica; Ministry of Science and Technology; Ministry of Education; and Ministry of Economic Affairs. The conference was held in Kaohsiung, Republic of China (Taiwan), during December 7-11, 2014.

An international Program Committee (PC) consisting of 48 scientists was formed approximately one year earlier with the objective of determining the scientific content of the conference. As for previous editions, Asiacrypt 2014 also stimulated great interest among the scientific community of cryptologists. A total of 255 technical papers were submitted for possible presentations approximately six months prior to the conference. Authors of the submitted papers are spread all over the world. Each PC member could submit at most two co-authored papers or at most one single-authored paper, and the PC co-chairs did not submit any paper. All the submissions were screened by the PC members and 55 papers were finally selected for presentation at the conference. These proceedings contain the revised versions of the papers that were selected. The revisions were not checked and the responsibility of the papers rest with the authors and not the PC members.

The selection of papers for presentations was made through a double-blind review process. Each paper was assigned four reviewers and submissions by PC members were assigned five reviewers. Apart from the PC members, the selection process was assisted by a total of 397 external reviewers. The total number of reviews for all the papers was more than 1,000. In addition to the reviews, the selection process involved an extensive discussion phase. This phase allowed PC members to express opinion on all the submissions. The final selection of 55 papers was the result of this extensive and rigorous selection procedure.

The decision of the best paper award was based on a vote among the PC members, and it was conferred upon the paper “Solving LPN Using Covering Codes” authored by Qian Guo, Thomas Johansson, and Carl Löndahl. In addition to the best paper, three other papers were recommended for solicitations by the Editor-in-Chief of the *Journal of Cryptology* to submit expanded versions to the journal. These papers are “Secret-Sharing for NP” authored by Ilan Komargodski, Moni Naor, and Eylon Yogev; “Mersenne Factorization Factory” authored by Thorsten Kleinjung, Joppe W. Bos, and Arjen K. Lenstra; and

“Jacobian Coordinates on Genus 2 Curves” authored by Huseyin Hisil and Craig Costello.

In addition to the regular presentations, the conference featured two invited talks. The invited speakers were decided through an extensive multi-round discussion among the PC members. This resulted in very interesting talks on two different aspects of the subject. Kenneth G. Paterson spoke on “Big Bias Hunting in Amazonia: Large-Scale Computation and Exploitation of RC4 Biases,” a topic of importance to practical cryptography, while Helaine Leggat spoke on “The Legal Infrastructure Around Information Security in Asia,” which had an appeal to a wide audience.

Along with the regular presentations and the invited talks, a rump session was organized. This session contained short presentations on latest research results, announcements of future events, and other topics of interest to the audience.

Many people contributed to Asiacrypt 2014. We would like to thank the authors of all papers for submitting their research works to the conference. Thanks are due to the PC members for their enthusiastic and continued participation for over a year in different aspects of selecting the technical program. The selection of the papers was made possible by the timely reviews from external reviewers, and thanks are due to them. A list of external reviewers is provided in these proceedings. We have tried to ensure that the list is complete. Any omission is inadvertent and if there is an omission, we apologize to that person.

Special thanks are due to D. J. Guan, the general chair of the conference, for working closely with us and ensuring that the PC co-chairs were insulated from the organizational work. This work was carried out by the Organizing Committee and they deserve thanks from all the participants for the wonderful experience. We thank Daniel J. Bernstein and Tanja Lange for expertly organizing and chairing the rump session.

We thank Shai Halevi for developing the IACR conference management software, which was used for the whole process of submission, reviewing, discussions, and preparing these proceedings. We thank Josh Benaloh, our IACR liaison, and San Ling, Asiacrypt Steering Committee Representative, for guidance and advice on several issues. Springer published the volumes and made these available before the conference. We thank Alfred Hofmann, Anna Kramer, Christine Reiss and their team for the professional and efficient handling of the production process.

December 2014

Palash Sarkar
Tetsu Iwata

Asiacrypt 2014

The 20th Annual International Conference on Theory and Application of Cryptology and Information Security

Sponsored by the *International Association for Cryptologic
Research (IACR)*

December 7–11, 2014, Kaohsiung, Taiwan (R.O.C.)

General Chair

D. J. Guan	National Sun Yat-sen University, Taiwan, and National Chung Hsing University, Taiwan
------------	---

Program Co-chairs

Palash Sarkar Tetsu Iwata	Indian Statistical Institute, India Nagoya University, Japan
------------------------------	---

Program Committee

Masayuki Abe Elena Andreeva Paulo S. L. M. Barreto Daniel J. Bernstein	NTT Secure Platform Laboratories, Japan K.U. Leuven, Belgium University of Sao Paulo, Brazil University of Illinois at Chicago, USA, and Technische Universiteit Eindhoven, The Netherlands
Guido Bertoni Jean-Luc Beuchat Debrup Chakraborty Chen-Mou Cheng Jung Hee Cheon Ashish Choudhury Sherman S.M. Chow	STMicroelectronics, Italy ELCA, Switzerland CINVESTAV-IPN, Mexico National Taiwan University, Taiwan Seoul National University, Korea IIIT Bangalore, India Chinese University of Hong Kong, Hong Kong SAR
Kai-Min Chung Carlos Cid	Academia Sinica, Taiwan Royal Holloway, University of London, UK
Jean-Sébastien Coron	University of Luxembourg, Luxembourg

Joan Daemen	STMicroelectronics, Belgium
Itai Dinur	École Normale Supérieure, Paris, France
Marc Fischlin	Darmstadt University of Technology, Germany
Steven Galbraith	University of Auckland, New Zealand
Sanjam Garg	University of California, Berkeley, USA
Marc Joye	Technicolor, USA
Koray Karabina	Florida Atlantic University, USA
Xuejia Lai	Shanghai Jiaotong University, China
Gregor Leander	Ruhr University Bochum, Germany
Jooyoung Lee	Sejong University, Korea
Stefan Mangard	Infineon Technologies, Germany
Willi Meier	FHNW, Switzerland
Jesper Buus Nielsen	Aarhus University, Denmark
Thomas Peyrin	Nanyang Technological University, Singapore
Duong Hieu Phan	University of Paris 8, France
Raphael C.-W. Phan	Multimedia University, Malaysia
María Naya-Plasencia	Inria Paris-Rocquencourt, France
Emmanuel Prouff	ANSSI, France
Christian Rechberger	DTU, Denmark
Alon Rosen	IDC Herzliya, Israel
Abhi Shelat	University of Virginia, USA
Berry Schoenmakers	Technische Universiteit Eindhoven, The Netherlands
Ron Steinfeld	Monash University, Australia
Marc Stevens	CWI, The Netherlands
Daisuke Suzuki	Mitsubishi Electric, Japan
Stefano Tessaro	UCSB, USA
Huaxiong Wang	Nanyang Technological University, Singapore
Meiqin Wang	Shandong University, China
Daniel Wichs	Northeastern University, USA
Duncan S. Wong	City University of Hong Kong, Hong Kong SAR
Kan Yasuda	NTT Secure Platform Laboratories, Japan
Hong-Sheng Zhou	Virginia Commonwealth University, USA

Additional Reviewers

Mohammed	Hoda A. Alkhzaimi	Gilles Van Assche
Abdelraheem	Prabhanjan Ananth	Jean-Philippe Aumasson
Arash Afshar	Kazumaro Aoki	Paul Baecher
Shashank Agrawal	Daniel Apon	Chung Hun Baek
Shweta Agrawal	Diego F. Aranha	Shi Bai
Adi Akavia	Hassan Jameel Asghar	Abhishek Banerjee
Martin Albrecht	Gilad Asharov	Kfir Barhum

Aurélie Bauer	Bernardo David	Nicolas Guillermín
Carsten Baum	Patrick Derbez	Sylvain Guilley
Anja Becker	David Derler	Siyao Guo
Amos Beimel	Srinivas Devadas	Divya Gupta
Rishiraj Bhattacharya	Sandra Diaz-Santiago	Patrick Haddad
Begül Bilgin	Vassil Dimitrov	Nguyen Manh Ha
Olivier Billet	Ning Ding	Iftach Haitner
Elia Bisi	Yi Ding	Shai Halevi
Nir Bitansky	Christoph Dobraunig	Fabrice Ben Hamouda
Olivier Blazy	Matthew Dodd	Shuai Han
Céline Blondeau	Nico Döttling	Christian Hanser
Andrej Bogdanov	Rafael Dowsley	Mitsuhiro Hattori
Alexandra Boldyreva	Frédéric Dupuis	Carmit Hazay
Joppe W. Bos	Stefan Dziembowski	Qiongyi He
Elette Boyle	Maria Eichlseder	Brett Hemenway
Zvika Brakerski	Martianus Frederic Ezerman	Jens Hermans
Nicolas Bruneau	Liming Fang	Takato Hirano
Christina Brzuska	Xiwen Fang	Jeffrey Hoffstein
Sébastien Canard	Pooya Farshim	Dennis Hofheinz
Anne Canteaut	Sebastian Faust	Deukjo Hong
Claude Carlet	Omar Fawzi	Hyunsook Hong
Angelo De Caro	Serge Fehr	Wei-Chih Hong
David Cash	Victoria Fehr	Sebastiaan de Hoogh
Dario Catalano	Matthieu Finiasz	Jialin Huang
André Chailloux	Dario Fiore	Kyle Huang
Donghoon Chang	Rob Fitzpatrick	Qiong Huang
Pascale Charpin	Pierre-Alain Fouque	Yan Huang
Sanjit Chatterjee	Tore Kasper Frederiksen	Yun Huang
Jie Chen	Georg Fuchsbauer	Zhengan Huang
Wei-Han Chen	Eiichiro Fujisaki	Andreas Hülsing
Yu-Chi Chen	Philippe Gaborit	Michael Hutter
Ray Cheung	Tommaso Gagliardoni	Jung Yeon Hwang
Céline Chevalier	David Galindo	Malika Izabachene
Dong Pyo Chi	Wei Gao	Abhishek Jain
Ji-Jian Chin	Pierrick Gaudry	Dirmanto Jap
Alessandro Chisea	Peter Gazi	Stanislaw Jarecki
Chongwon Cho	Laurie Genelle	Eliane Jaulmes
Kim-Kwang Raymond Choo	Irene Giacomelli	Jérémy Jean
HeeWon Chung	Sergey Gorbunov	Mahabir Jhanwar
Craig Costello	Dov Gordon	Guo Jian
Giovanni Di Crescenzo	Samuel Dov Gordon	Shaoquan Jiang
Dana Dachman-Soled	Robert Granger	Pascal Junod
Ivan Damgård	Jens Groth	Chethan Kamath
Jean-Luc Danger	Felix Guenther	Pierre Karpman
		Aniket Kate

Jonathan Katz	Kaitai Liang	Ventzislav Nikov
Elif Bilge Kavun	Benoît Libert	Svetla Nikova
Akinori Kawachi	Changlu Lin	Ryo Nishimaki
Yutaka Kawai	Huijia (Rachel) Lin	Adam O'Neill
Sriram Keelveedhi	Tingting Lin	Miyako Ohkubo
Dakshita Khurana	Yannis Linge	Tatsuaki Okamoto
Franziskus Kiefer	Helger Lipmaa	Cristina Onete
Eike Kiltz	Feng-Hao Liu	Claudio Orlandi
Jihye Kim	Joseph Liu	David Oswald
Jinsu Kim	Zhen Liu	Elisabeth Oswald
Minkyu Kim	Daniel Loebenberger	Khaled Ouafi
Miran Kim	Victor Lomné	Carles Padro
Myungsun Kim	Yu Long	Jiaxin Pan
Sungwook Kim	Patrick Longa	Omer Paneth
Taechan Kim	Cuauhtemoc	Anat Paskin
Mehmet Sabir Kiraz	Mancillas-López	Rafael Pass
Susumu Kiyoshima	Atul Luykx	Kenneth G. Paterson
Ilya Kizhvatov	Vadim Lyubashevsky	Arpita Patra
Markulf Kohlweiss	Housseem Maghrebi	Roel Peeters
Ilan Komargodski	Mohammad Mahmoody	Chris Peikert
Takeshi Koshihara	Alex Malozemoff	Geovandro
Simon Kramer	Mark Manulis	C. C. F. Pereira
Ranjit Kumaresan	Xianping Mao	Olivier Pereira
Po-Chun Kuo	Joana Treger Marim	Ludovic Perret
Thijs Laarhoven	Giorgia Azzurra Marson	Edoardo Persichetti
Fabien Laguillaumie	Ben Martin	Krzysztof Pietrzak
Russell W.F. Lai	Daniel Martin	Bertram Poettering
Tanja Lange	Takahiro Matsuda	Geong-Sen Poh
Adeline Langlois	Mitsuru Matsui	David Pointcheval
Martin M. Lauridsen	Ingo von Maurich	Antigoni Polychroniadou
Rasmus Winther	Filippo Melzani	Raluca Ada Popa
Lauritsen	Florian Mendel	Manoj Prabhakaran
Changmin Lee	Bart Mennink	Baodong Qin
Hyung Tae Lee	Sihem Mesnager	Somindu C. Ramanna
Kwangsue Lee	Arno Mittelbach	Samuel Ranellucci
Moon Sung Lee	Payman Mohassel	C. Pandu Rangan
Younho Lee	Amir Moradi	Vanishree Rao
Wang Lei	Tomoyuki Morimae	Jean-René Reinhard
Tancrede Lepoint	Kirill Morozov	Ling Ren
Gaëtan Leurent	Nicky Mouha	Oscar Reparaz
Kevin Lewi	Pratyay Mukherjee	Alfredo Rial
Allison Lewko	Gregory Neven	Jefferson E. Ricardini
Liangze Li	Khoa Nguyen	Silas Richelson
Wen-Ding Li	Phon Nguyen	Ben Riva
Guanfeng Liang	Ivica Nikolić	Matthieu Rivain

Thomas Roche	Mario Strefler	Andrea Visconti
Francisco	Takeshi Sugawara	Ivan Visconti
Rodríguez-Henríquez	Ruggero Susella	Niels de Vreede
Lil María	Koutarou Suzuki	Mingqiang Wang
Rodríguez-Henríquez	Alan Szepieniec	Wei Wang
Mike Rosulek	Björn Tackmann	Yanfeng Wang
Arnab Roy	Katsuyuki Takashima	Yuntao Wang
Hansol Ryu	Syh-Yuan Tan	Hoeteck Wee
Minoru Saeki	Xiao Tan	Puwen Wei
Amit Sahai	Qiang Tang	Qiaoyan Wen
Yusuke Sakai	Christophe Tartary	Erich Wenger
Olivier Sanders	Yannick Teglia	Qianhong Wu
Fabrizio De Santis	Sidharth Telang	Keita Xagawa
Yu Sasaki	Isamu Teranishi	Hong Xu
Alessandra Scafuro	Adrian Thillard	Weijia Xue
Christian Schaffner	Aishwarya	Takashi Yamakawa
John Schanck	Thiruvengadam	Bo-Yin Yang
Tobias Schneider	Enrico Thomae	Guomin Yang
Peter Schwabe	Susan Thomson	Wun-She Yap
Gil Segev	Mehdi Tibouchi	Scott Yilek
Nicolas Sendrier	Tyge Tiessen	Eylon Yogev
Jae Hong Seo	Elmar Tischhauser	Kazuki Yoneyama
Karn Seth	Arnaud Tisserand	Ching-Hua Yu
Yannick Seurin	Yosuke Todo	Yu Yu
Ronen Shaltiel	Jacques Traoré	Tsz Hon Yuen
Elaine Shi	Roberto Trifiletti	Aaram Yun
Koichi Shimizu	Viet Cuong Trinh	Mark Zhandry
Ji Sun Shin	Raylin Tso	Cong Zhang
Naoyuki Shinohara	Toyohiro Tsurumaru	Guoyan Zhang
Joseph Silverman	Hoang Viet Tung	Liang Feng Zhang
Marcos A. Simplicio Jr	Yu-Hsiu Tung	Tao Zhang
Boris Skoric	Dominique Unruh	Wei Zhang
Daniel Slamanig	Berkant Ustaoglu	Ye Zhang
Nigel Smart	Meilof Veeningen	Yun Zhang
Fang Song	Muthuramakrishnan	Zongyang Zhang
Douglas Stebila	Venkitasubramaniam	Yongjun Zhao
Damien Stehlé	Daniele Venturi	Yunlei Zhao
Rainer Steinwandt	Frederik Vercauteren	Vassilis Zikas
Marc Stottinger	Damien Vergnaud	

Organizing Committee

Advisors

Lynn Batten	Deakin University, Australia
Eiji Okamoto	Tsukuba University, Japan
San Ling	Nanyang Technological University, Singapore
Kwangjo Kim	Korea Advanced Institute of Science and Technology, Korea
Xuejia Lai	Shanghai Jiaotong University, China
Der-Tsai Lee	National Chung Hsing University, Taiwan, and Academia Sinica, Taiwan
Tzong-ChenWu	National Taiwan University of Science and Technology, Taiwan

Secretary

Chun-I Fan	National Sun Yat-sen University, Taiwan
------------	---

Treasurer

Chia-Mei Chen	National Sun Yat-sen University, Taiwan
---------------	---

Local Committee Members

Shiuhpyng Shieh	National Chiao Tung University, Taiwan
Ching-Long Lei	National Taiwan University, Taiwan
Wen-Guey Tzeng	National Chiao Tung University, Taiwan
Hung-Min Sun	National Tsing Hua University, Taiwan
Chen-Mou Cheng	National Taiwan University, Taiwan
Bo-Yin Yang	Institute of Information Science, Academia Sinica, Taiwan

Sponsors

National Sun Yat-sen University
Academia Sinica
Ministry of Science and Technology
Ministry of Education
Ministry of Economic Affairs

Table of Contents – Part I

Cryptology and Coding Theory

Solving LPN Using Covering Codes	1
<i>Qian Guo, Thomas Johansson, and Carl Löndahl</i>	
Algebraic Attack against Variants of McEliece with Goppa Polynomial of a Special Form	21
<i>Jean-Charles Faugère, Ludovic Perret, and Frédéric de Portzamparc</i>	

New Proposals

Bivariate Polynomials Modulo Composites and Their Applications	42
<i>Dan Boneh and Henry Corrigan-Gibbs</i>	
Cryptographic Schemes Based on the ASASA Structure: Black-box, White-box, and Public-key (Extended Abstract)	63
<i>Alex Biryukov, Charles Bouillaguet, and Dmitry Khovratovich</i>	

Authenticated Encryption

Beyond $2^{c/2}$ Security in Sponge-Based Authenticated Encryption Modes	85
<i>Philipp Jovanovic, Atul Luykx, and Bart Mennink</i>	
How to Securely Release Unverified Plaintext in Authenticated Encryption	105
<i>Elena Andreeva, Andrey Bogdanov, Atul Luykx, Bart Mennink, Nicky Mouha, and Kan Yasuda</i>	
Forging Attacks on Two Authenticated Encryption Schemes COBRA and POET	126
<i>Mridul Nandi</i>	

Symmetric Key Cryptanalysis

Low Probability Differentials and the Cryptanalysis of Full-Round CLEFIA-128	141
<i>Sareh Emami, San Ling, Ivica Nikolić, Josef Pieprzyk, and Huaxiong Wang</i>	

Automatic Security Evaluation and (Related-key) Differential
Characteristic Search: Application to SIMON, PRESENT, LBlock,
DES(L) and Other Bit-Oriented Block Ciphers 158
*Siwei Sun, Lei Hu, Peng Wang, Kexin Qiao, Xiaoshuang Ma, and
Ling Song*

Scrutinizing and Improving Impossible Differential Attacks:
Applications to CLEFIA, Camellia, LBlock and SIMON 179
Christina Boura, María Naya-Plasencia, and Valentin Suder

A Simplified Representation of AES 200
Henri Gilbert

Side Channel Analysis I

Simulatable Leakage: Analysis, Pitfalls, and New Constructions 223
*Jake Longo, Daniel P. Martin, Elisabeth Oswald,
Daniel Page, Martijin Stam, and Michael J. Tunstall*

Multi-target DPA Attacks: Pushing DPA Beyond the Limits of a
Desktop Computer 243
Luke Mather, Elisabeth Oswald, and Carolyn Whitnall

GLV/GLS Decomposition, Power Analysis, and Attacks on ECDSA
Signatures with Single-Bit Nonce Bias 262
*Diego F. Aranha, Pierre-Alain Fouque, Benoît Gérard,
Jean-Gabriel Kammerer, Mehdi Tibouchi,
and Jean-Christophe Zavalowicz*

Soft Analytical Side-Channel Attacks 282
*Nicolas Veyrat-Charvillon, Benoît Gérard,
and François-Xavier Standaert*

Hyperelliptic Curve Cryptography

On the Enumeration of Double-Base Chains with Applications to
Elliptic Curve Cryptography 297
Christophe Doche

Kummer Strikes Back: New DH Speed Records 317
*Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange,
and Peter Schwabe*

Jacobian Coordinates on Genus 2 Curves 338
Huseyin Hisil and Craig Costello

Factoring and Discrete Log

Mersenne Factorization Factory	358
<i>Thorsten Kleinjung, Joppe W. Bos, and Arjen K. Lenstra</i>	
Improving the Polynomial time Precomputation of Frobenius Representation Discrete Logarithm Algorithms: Simplified Setting for Small Characteristic Finite Fields	378
<i>Antoine Joux and Cécile Pierrot</i>	

Invited Talk I

Big Bias Hunting in Amazonia: Large-Scale Computation and Exploitation of RC4 Biases (Invited Paper)	398
<i>Kenneth G. Paterson, Bertram Poettering, and Jacob C.N. Schuldt</i>	

Cryptanalysis

Multi-user Collisions: Applications to Discrete Logarithm, Even-Mansour and PRINCE	420
<i>Pierre-Alain Fouque, Antoine Joux, and Chrysanthi Mavromati</i>	
Cryptanalysis of Iterated Even-Mansour Schemes with Two Keys	439
<i>Itai Dinur, Orr Dunkelman, Nathan Keller, and Adi Shamir</i>	
Meet-in-the-Middle Attacks on Generic Feistel Constructions	458
<i>Jian Guo, Jérémy Jean, Ivica Nikolić, and Yu Sasaki</i>	
XLS is Not a Strong Pseudorandom Permutation	478
<i>Mridul Nandi</i>	

Signatures

Structure-Preserving Signatures on Equivalence Classes and Their Application to Anonymous Credentials	491
<i>Christian Hanser and Daniel Slamanig</i>	
On Tight Security Proofs for Schnorr Signatures	512
<i>Nils Fleischhacker, Tibor Jager, and Dominique Schröder</i>	

Zero-Knowledge

Square Span Programs with Applications to Succinct NIZK Arguments	532
<i>George Danezis, Cédric Fournet, Jens Groth, and Markulf Kohlweiss</i>	

Better Zero-Knowledge Proofs for Lattice Encryption and Their Application to Group Signatures	551
<i>Fabrice Benhamouda, Jan Camenisch, Stephan Krenn, Vadim Lyubashevsky, and Gregory Neven</i>	
Author Index	573

Table of Contents – Part II

Encryption Schemes

Concise Multi-challenge CCA-Secure Encryption and Signatures with Almost Tight Security	1
<i>Benoît Libert, Marc Joye, Moti Yung, and Thomas Peters</i>	
Efficient Identity-Based Encryption over NTRU Lattices	22
<i>Léo Ducas, Vadim Lyubashevsky, and Thomas Prest</i>	
Order-Preserving Encryption Secure Beyond One-Wayness	42
<i>Isamu Teranishi, Moti Yung, and Tal Malkin</i>	

Outsourcing and Delegation

Statistically-secure ORAM with $\tilde{O}(\log^2 n)$ Overhead	62
<i>Kai-Min Chung, Zhenming Liu, and Rafael Pass</i>	
Adaptive Security of Constrained PRFs	82
<i>Georg Fuchsbauer, Momchil Konstantinov, Krzysztof Pietrzak, and Vanishree Rao</i>	

Obfuscation

Poly-Many Hardcore Bits for Any One-Way Function and a Framework for Differing-Inputs Obfuscation	102
<i>Mihir Bellare, Igors Stepanovs, and Stefano Tessaro</i>	
Using Indistinguishability Obfuscation via UCEs	122
<i>Christina Brzuska and Arno Mittelbach</i>	
Indistinguishability Obfuscation versus Multi-bit Point Obfuscation with Auxiliary Input	142
<i>Christina Brzuska and Arno Mittelbach</i>	
Bootstrapping Obfuscators via Fast Pseudorandom Functions	162
<i>Benny Applebaum</i>	

Homomorphic Cryptography

Homomorphic Authenticated Encryption Secure against Chosen-Ciphertext Attack	173
<i>Chihong Joo and Aaram Yun</i>	

Authenticating Computation on Groups: New Homomorphic Primitives
and Applications 193
Dario Catalano, Antonio Marcedone, and Orazio Puglisi

Compact VSS and Efficient Homomorphic UC Commitments 213
*Ivan Damgård, Bernardo David, Irene Giacomelli,
and Jesper Buus Nielsen*

Secret Sharing

Round-Optimal Password-Protected Secret Sharing and T-PAKE
in the Password-Only Model 233
Stanislaw Jarecki, Aggelos Kiayias, and Hugo Krawczyk

Secret-Sharing for NP 254
Ilan Komargodski, Moni Naor, and Eylon Yogev

Block Ciphers and Passwords

Tweaks and Keys for Block Ciphers: The TWEAKEY Framework 274
Jérémy Jean, Ivica Nikolić, and Thomas Peyrin

Memory-Demanding Password Scrambling 289
Christian Forler, Stefan Lucks, and Jakob Wenzel

Side Channel Analysis II

Side-Channel Analysis of Multiplications in $GF(2^{128})$:
Application to AES-GCM 306
Sonia Belaid, Pierre-Alain Fouque, and Benoît Gérard

Higher-Order Threshold Implementations 326
*Begül Bilgin, Benedikt Gierlichs, Svetla Nikova, Ventsislav Nikov,
and Vincent Rijmen*

Masks Will Fall Off: Higher-Order Optimal Distinguishers 344
Nicolas Bruneau, Sylvain Guilley, Annelie Heuser, and Olivier Rioul

Black-Box Separation

Black-Box Separations for One-More (Static) CDH
and Its Generalization 366
*Jiang Zhang, Zhenfeng Zhang, Yu Chen, Yanfei Guo,
and Zongyang Zhang*

Black-Box Separations for Differentially Private Protocols 386
Dakshita Khurana, Hemanta K. Maji, and Amit Sahai

Composability

Composable Security of Delegated Quantum Computation	406
<i>Vedran Dunjko, Joseph F. Fitzsimons, Christopher Portmann, and Renato Renner</i>	
All-But-Many Encryption: A New Framework for Fully-Equipped UC Commitments	426
<i>Eiichiro Fujisaki</i>	

Multi-Party Computation

Multi-valued Byzantine Broadcast: The $t < n$ Case	448
<i>Martin Hirt and Pavel Raykov</i>	
Fairness versus Guaranteed Output Delivery in Secure Multiparty Computation	466
<i>Ran Cohen and Yehuda Lindell</i>	
Actively Secure Private Function Evaluation	486
<i>Payman Mohassel, Saeed Sadeghian, and Nigel P. Smart</i>	
Efficient, Oblivious Data Structures for MPC	506
<i>Marcel Keller and Peter Scholl</i>	
Author Index	527