Lecture Notes in Computer Science 8873

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

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

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. Kennth 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	Indian Statistical Institute, India
Tetsu Iwata	Nagoya University, Japan

Program Committee

Masayuki Abe	NTT Secure Platform Laboratories, Japan
Elena Andreeva	K.U. Leuven, Belgium
Paulo S. L. M. Barreto	University of Sao Paulo, Brazil
Daniel J. Bernstein	University of Illinois at Chicago, USA, and Technische Universiteit Eindhoven, The Netherlands
Guido Bertoni	STMicroelectronics, Italy
Jean-Luc Beuchat	ELCA, Switzerland
Debrup Chakraborty	CINVESTAV-IPN, Mexico
Chen-Mou Cheng	National Taiwan University, Taiwan
Jung Hee Cheon	Seoul National University, Korea
Ashish Choudhury	IIIT Bangalore, India
Sherman S.M. Chow	Chinese University of Hong Kong, Hong Kong SAR
Kai-Min Chung	Academia Sinica, Taiwan
Carlos Cid	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 Abdelraheem	Hoda A. Alkhzaimi	Gilles Van Assche
Arash Afshar	Prabhanjan Ananth	Jean-Philippe Aumasson
Shashank Agrawal	Kazumaro Aoki	Paul Baecher
Shweta Agrawal	Daniel Apon	Chung Hun Baek
Adi Akavia	Diego F. Aranha	Shi Bai
Martin Albrecht	Hassan Jameel Asghar	Abhishek Banerjee
	Gilad Asharov	Kfir Barhum

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

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

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

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

New Proposals

Authenticated Encryption

Symmetric Key Cryptanalysis

Side Channel Analysis I

Hyperelliptic Curve Cryptography

Factoring and Discrete Log

Invited Talk I

Cryptanalysis

Signatures

Zero-Knowledge

Table of Contents – Part II

Encryption Schemes

Outsourcing and Delegation

Obfuscation

Homomorphic Cryptography

Secret Sharing

Block Ciphers and Passwords

Side Channel Analysis II

Black-Box Separation

Composability

Multi-Party Computation