Lecture Notes in Computer Science 7658

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

Alfred Kobsa
University of California, Irvine, CA, USA

Friedemann Mattern
ETH Zurich, Switzerland

John C. Mitchell
Stanford University, CA, USA

Moni Naor
Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz
University of Bern, Switzerland

C. Pandu Rangan
Indian Institute of Technology, Madras, India

Bernhard Steffen
TU Dortmund University, Germany

Madhu Sudan
Microsoft Research, Cambridge, MA, USA

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

Xiaoyun Wang Kazue Sako (Eds.)

Advances in Cryptology – ASIACRYPT 2012

18th International Conference on the Theory
and Application of Cryptology and Information Security
Beijing, China, December 2-6, 2012. Proceedings

Volume Editors

Xiaoyun Wang
Tsinghua University
30 Shuangqing Road, 100084 Beijing, China
E-mail: xiaoyunwang@tsinghua.edu.cn

Kazue Sako
NEC Corporation, Central Research Laboratories
1753 Shimonumabe Nakahara, Kawasaki 211-8666, Japan
E-mail: k-sako@ab.jp.nec.com

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-34960-7 e-ISBN 978-3-642-34961-4
DOI 10.1007/978-3-642-34961-4
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012951486

CR Subject Classification (1998): E.3, D.4.6, F.2, K.6.5, G.2, I.1, J.1

LNCS Sublibrary: SL 4 – Security and Cryptology

© International Association for Cryptologic Research 2012
This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.
The use of general descriptive names, registered names, trademarks, 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.

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

ASIACRYPT 2012, the 18th International Conference on Theory and Application of Cryptology and Information Security, was held during December 2–6 in Beijing International Convention Center, Beijing, China. The conference was sponsored by the International Association for Cryptologic Research (IACR) in cooperation with the Chinese Association for Cryptologic Research (CACR). It was also co-sponsored by the National Natural Science Foundation of China, Huawei Technologies Co. Ltd., and Intel Corporation.

From 241 valid submissions, 43 were accepted for publication after a very tough evaluation process. The Program Committee (PC) with the help of 256 external reviewers provided at least three independent reviews for each paper, and five or more for those with PC contributions.

There were also two invited talks. On Monday, Dan Boneh delivered "Pairing-based Cryptography: Past, Present, and Future" as the IACR Distinguished Lecture. On Wednesday, Chuanming Zong spoke on"Some Mathematical Mysteries in Lattices." In addition to the invited talks, the conference also held a Rump Session, full of academic opinions and enjoyment.

We selected a particularly large and broad PC and encouraged members to focus on the positive aspects of submissions. During the one-and-a-half-month-long independent review phase, each PC member had about 28 submissions to review, our PC members and the external reviewers worked very hard and efficiently. In the following one-month daily discussion phase, PC members communicated each other's opinion on the board. We processed the anonymized questions from the PC members to authors, which resulted in a better quality of review.

We would like to thank the authors of all 241 submissions. Their contributions made this conference possible. We are extremely grateful to the PC members for their enormous investment of time and effort in the difficult and delicate process of review and selection, especially given the last decision days were in the midst of summer vacation time. A list of PC members and external reviewers can be found on the succeeding pages of this volume. We would like to thank Xuejia Lai, Zhijun Qiang, Hao Chen, Juan Liu, Dongdai Lin, Bao Li, Meiqin Wang and Jialin Huang for the conference organization. Special thanks go to Shai Halevi for providing and setting up the splendid review software. We are most grateful to Yue Sun, who provided technical support for the entire ASIACRYPT 2012 review process. We are also grateful to Dong Hoon Lee, the ASIACRYPT 2011 Program Chair, for his timely information and replies to the host of questions we posed during the process.

September 2012

Xiaoyun Wang
Kazue Sako

ASIACRYPT 2012

The 18th Annual International Conference on the Theory and Application of Cryptology and Information Security

December 2–6, 2012, Beijing, China

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

Organized in cooperation with the *Chinese Association for Cryptologic Research (CACR)*

General Chair

Xuejia Lai	Shanghai Jiao Tong University, China

Program Co-chairs

Xiaoyun Wang	Tsinghua University, China
Kazue Sako	NEC, Japan

Program Committee

Feng Bao	I2R, Singapore
Alex Biryukov	University of Luxembourg, Luxembourg
Xavier Boyen	Prime Cryptography, USA
David Cash	IBM T.J. Watson Research Center, USA
Jung Hee Cheon	Seoul National University, Korea
Sherman S.M. Chow	University of Waterloo, Canada
Joan Daemen	STMicroelectronics, Belgium
Jintai Ding	University of Cincinnati, USA
Orr Dunkelman	University of Haifa and Weizmann Institute, Israel
Marc Fischlin	Darmstadt University of Technology, Germany
Vipul Goyal	Microsoft Research, India
Tetsu Iwata	Nagoya University, Japan
Antoine Joux	DGA and Université de Versailles, PRISM, France
Jonathan Katz	University of Maryland, USA
Eike Kiltz	Ruhr University Bochum, Germany
Lars Ramkilde Knudsen	Technical University of Denmark, Denmark
Dong Hoon Lee	Korea University, Korea
Arjen K. Lenstra	EPFL, Switzerland
Dongdai Lin	CAS, China

Mitsuru Matsui	Mitsubishi Electric, Japan
Willi Meier	FHNW, Switzerland
Florian Mendel	KU Leuven, Belgium
Phong Q. Nguyen	INRIA, France and Tsinghua University, China
Tatsuaki Okamoto	NTT, Japan
Bart Preneel	KU Leuven, Belgium
Christian Rechberger	Technical University of Denmark, Denmark
Rei Safavi-Naini	University of Calgary, Canada
Nigel P. Smart	University of Bristol, UK
Ron Steinfeld	Macquarie University, Australia
Hongjun Wu	Nanyang Technological University, Singapore

External Reviewers

Michel Abdalla
M. Ahmed Abdelraheem
Masayuki Abe
Shashank Agrawal
Ahmad Ahmadi
Hadi Ahmadi
Mohsen Alimomeni
Prabhanjan Ananth
Elena Andreeva
Kazumaro Aoki
Benny Applebaum
Gilles Van Assche
Nuttapong Attrapadung
Jean-Philippe Aumasson
Paul Baecher
Chung Hun Baek
Aurelie Bauer
Josh Benaloh
David Bernhard
Guido Bertoni
Raghav Bhaskar
Andrey Bogdanov
Julia Borghoff
Joppe Bos
Charles Bouillaguet
Christina Brzuska
D. Galindo ChacÓn
Anne Canteaut
Angelo De Caro
Dario Catalano
Melissa Chase
Jiazhe Chen
Jie Chen
Yuanmi Chen
Nathan Chenette
Chen-mou Cheng
Céline Chevalier
Seung Geol Choi
Ashish Choudhary
Sherman Chow
Cheng-Kang Chu
Ji Young Chun
Kai-Min Chung
Carlos Cid
Dana Dachman-Soled
Özgür Dagdelen
Ivan Damgaard
Itai Dinur
Leo Ducas
Aline Dudeanu
Pooya Farshim
Xiutao Feng
Dario Fiore
Pierre-Alain Fouque
Georg Fuchsbauer
Eiichiro Fujisaki
Jun Furukawa
Tommaso Gagliardoni
Steven Galbraith
Nicolas Gama
Praveen Gauravaram
Rosario Gennaro
Benedikt Gierlichs
Serge Gorbunov
Jens Groth
Johann Groschädl
David Gruenewald
Divya Gupta
Iftach Haitner
Shai Halevi
Nadia Heninger
Jens Hermans
Gottfried Herold
Shoichi Hirose
Dennis Hofheinz
Fumitaka Hoshino
Lei Hu
Zhu Huafei
Tao Huang
Jung Yeon Hwang
Toshiyuki Isshiki
Mitsugu Iwamoto
Tibor Jager
Dimitar Jetchev
Mahavir Jhawar
Shaoquan Jiang
Saqib Kakvi
Bhavana Kanukurthi
Alexandre Karlov
Tomasz Kazana
Qiong Tang
Aggelos Kiayias
Dongmin Kim

HongTae Kim
Hyoseung Kim
Jihye Kim
Jinsu Kim
Kee Sung Kim
Kitak Kim
Myungsun Kim
Sungwook Kim
Taechan Kim
Mario Kirschbaum
Susumu Kiyoshima
Thorsten Kleinjung
Simon Knellwolf
Yuichi Komano
Woo Kwon Koo
Kaoru Kurosawa
Eyal Kushilevitz
S. Thomas Kutzner
Hidenori Kuwakado
Özgül Küçük
Fabien Laguillaumie
Mario Lamberger
Tanja Lange
Gregor Leander
Hyung Tae Lee
Jooyoung Lee
Kwangsu Lee
Moon Sung Lee
Young-Ran Lee
Younho Lee
Gaëtan Leurent
Allison Bishop Lewko
Pierre-Yvan Liardet
Benoit Libert
Hoon Wei Lim
Yehuda Lindell
Jake Loftus
Jiqiang Lu
Karina M. Magalhães
Hemanta Maji
Avradip Mandal
Mark Manulis
Giorgia Azzurra Marson
Ben Martin
Takahiro Matsuda
Filippo Melzani
Bart Mennink
Alexander Meurer
Andrea Miele
Kazuhiko Minematsu
Marine Minier
Arno Mittelbach
Payman Mohassel
Ravi Montenegro
Amir Moradi
Nicky Mouha
Tomislav Nad
Michael Naehrig
Jesper Buus Nielsen
Ivica Nikolic
Svetla Nikova
Ryo Nishimaki
Geontae Noh
Ryo Nojima
Adam O'Neill
Cristina Onete
Onur Ozen
Ilya Ozerov
Carles Padro
Dan Page
Omkant Pandey
Jong Hwan Park
Jung Youl Park
Seunghwan Park
Kenny Paterson
Roel Peeters
Chris Peikert
Edoardo Persichetti
Christiane Peters
Duong Hieu Phan
Le Trieu Phong
Josef Pieprzyk
Krzysztof Pietrzak
Thomas Plos
David Pointcheval
Joop van de Pol
Arnab Roy
Hyun Sook Rhee
Alfredo Rial
Vincent Rijmen
Thomas Ristenpart
Alon Rosen
Yannis Rouselakis
Carla Ràfols
Minoru Saeki
Amit Sahai
Bagus Santoso
Santanu Sarkar
Sumanta Sarkar
Yu Sasaki
John Schanck
Martin Schläffer
Jörn-Marc Schmidt
Patrick Schmidt
Michael Schneider
Dominique Schröder
Nicolas Sendrier
Jae Woo Seo
Minjae Seo
Siamak Shahandashti
Kyung-Ah Shim
Ji Sun Shin
Taizo Shirai
Igor Shparlinski
Hervé Sibert
Benjamin Smith
Damien Stehlé
Chunhua Su
Takeshi Sugawara
Ruggero Susella
Daisuke Suzuki
Katsuyuki Takashima
Chengdong Tao
Yannick Teglia
Isamu Teranishi
Stefano Tessaro
Enrico Thomae
Mehdi Tibouchi
Elmar Tischhauser
Deniz Toz
Toyohiro Tsurumaru
Vesselin Velichkov
Vinod Vaikuntanathan
Kerem Varici
Daniele Venturi

Frederik Vercauteren
Vanessa Vitse
Huaxiong Wang
Meiqin Wang
Pengwei Wang
Bogdan Warinschi
Brent Waters
Hoeteck Wee
Lei Wei
Ralf-Philipp Weinmann
Daniel Wichs
Michael Wiener
Chuankun Wu
Keita Xagawa
Xiang Xie
Jing Xu
Bo-yin Yang
Yanjiang Yang
Kazuki Yoneyama
Reo Yoshida
Tsz-Hon Yuen
Aaram Yun
Haibin Zhang
Liangfeng Zhang
Rui Zhang
Yunlei Zhao
Hong-Sheng Zhou
Huafei Zhu
Vassilis Zikas

Sponsoring Institutions

National Natural Science Foundation of China
Huawei Technologies Co. Ltd.
Intel Corporation

Table of Contents

Invited Talks

Public-Key Cryptography I

Foundation

Symmetric Cipher

Security Proof

Public-Key Cryptography II

Lattice-Based Cryptography and Number Theory

Public-Key Cryptography III

Hash Function

Cryptographic Protocol I

Cryptographic Protocol II

Implementation Issues

Erratum