Lecture Notes in Computer Science 7073

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

Dong Hoon Lee  Xiaoyun Wang (Eds.)

# Advances in Cryptology – ASIACRYPT 2011

17th International Conference on the Theory
and Application of Cryptology and Information Security
Seoul, South Korea, December 4-8, 2011
Proceedings

Springer

Volume Editors

Dong Hoon Lee
Korea University
Center for Information Security Technologies
Anam Dong 5-ga, Seungbuk-gu, Seoul, South Korea
E-mail: donghlee@korea.ac.kr

Xiaoyun Wang
Tsinghua University
Institute for Advanced Study
Beijing 100084, China
E-mail: xiaoyunwang@tsinghua.edu.cn

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-25384-3 e-ISBN 978-3-642-25385-0
DOI 10.1007/978-3-642-25385-0
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011940813

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



*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 2011, the 17th International Conference on Theory and Application of Cryptology and Information Security, was held during December 4–8 in the Silla Hotel, Seoul, Republic of Korea. The conference was sponsored by the International Association for Cryptologic Research (IACR) in cooperation with Korea Institute of Information Security and Cryptology (KIISC), Digital Contents Society (DCS), Korea Internet Security Agency (KISA), and National Security Research Institute (NSRI). It was also co-sponsored by the Center for Information Security Technologies of Korea University (CIST), the Korean Federation of Science and Technology Societies (KOFST), Seoul National University, Electronics and Telecommunications Research Institute (ETRI), and Seoul Metropolitan Government.

We received 266 valid submissions, of which 42 were accepted for publication. With two pairs of papers merged, these proceedings contain the revised versions of 40 papers. The Program Committee (PC) was aided by 243 external reviewers. Every paper received at least three independent reviews, and papers with PC contributions got five or more. Several questions from PC members to authors were relayed in order to increase the quality of submissions. ASIACRYPT 2011 used a rolling Co-chair model and we made all decisions by consensus by sharing a great deal of e-mails.

For the Best Paper Award, the PC selected "A Framework for Practical Universally Composable Zero-Knowledge Protocols" by Jan Camenisch, Stephan Krenn, and Victor Shoup and "Counting Points on Genus 2 Curves with Real Multiplication" by Pierrick Gaudry, David Kohel, and Benjamin Smith. There were two invited talks; Joan Daemen delivered "15 Years of Rijndael" on December 6 and Úlfar Erlingsson spoke on "Securing Cloud Computing Services" on December 7.

We would like to thank the authors of all submissions regardless of whether their papers were accepted or not. Their work 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. A list of PC members and external reviewers can be found on succeeding pages of this volume. We would like to thank Hyoung Joong Kim, who was the General Chair in charge of the local organization and finances. Special thanks go to Shai Halevi for providing and setting up the splendid review software. We are most grateful to Kwangsu Lee and Jong Hwan Park, who provided support for the entire ASIACRYPT 2011 process. We are also grateful to Masayuki Abe, the ASIACRYPT 2010 Program Chair, for his timely information and replies to the host of questions we posed during the process.

September 2011

Dong Hoon Lee
Xiaoyun Wang

# ASIACRYPT 2011

## The 17th Annual International Conference on the Theory and Application of Cryptology and Information Security

December 4–8, 2011, Seoul, Korea

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

*in cooperation with*
Korea Institute of Information Security and Cryptology (KIISC),
Digital Contents Society (DCS),
Korea Internet Security Agency (KISA),
and
National Security Research Institute (NSRI)

### General Chair

| | |
|---|---|
| Hyoung Joong Kim | Korea University, Korea |

### Program Chairs

| | |
|---|---|
| Dong Hoon Lee | Korea University, Korea |
| Xiaoyun Wang | Tsinghua University, China |

### Program Committee

| | |
|---|---|
| Michel Abdalla | ENS and CNRS, France |
| Masayuki Abe | NTT, Japan |
| Kazumaro Aoki | NTT, Japan |
| Jung Hee Cheon | Seoul National University, Korea |
| Carlos Cid | Royal Holloway University of London, UK |
| Craig Gentry | IBM Research, USA |
| Vipul Goyal | Microsoft Research, India |
| Jens Groth | University College London, UK |
| Iftach Haitner | Tel Aviv University, Israel |
| Dennis Hofheinz | Karlsruhe Institute of Technology, Germany |

| | |
|---|---|
| Antoine Joux | DGA and Universite de Versailles, PRISM, France |
| Aggelos Kiayias | University of Connecticut, USA |
| Eike Kiltz | Ruhr University Bochum, Germany |
| Jongsung Kim | Kyungnam University, Korea |
| Lars R. Knudsen | Technical University of Denmark, Denmark |
| Dong Hoon Lee | Korea University, Korea |
| Arjen K. Lenstra | EPFL, Switzerland |
| Stefan Lucks | Bauhaus-University Weimar, Germany |
| Willi Meier | FHNW, Switzerland |
| Alfred Menezes | University of Waterloo, Canada |
| Payman Mohassel | University of Calgary, Canada |
| Phong Q. Nguyen | INRIA and ENS, France |
| Jesper Buus Nielsen | Aarhus University, Denmark |
| Chris Peikert | Georgia Tech, USA |
| Thomas Peyrin | NTU, Singapore |
| Christian Rechberger | ENS, France |
| Palash Sarkar | Indian Statistical Institute, India |
| Nigel P. Smart | University of Bristol, UK |
| Willy Susilo | University of Wollongong, Australia |
| Xiaoyun Wang | Tsinghua University, China |
| Hoeteck Wee | George Washington University, USA |
| Hongbo Yu | Tsinghua University, China |

## External Reviewers

| | | |
|---|---|---|
| Hadi Ahmadi | Simon Blackburn | Ashish Choudhury |
| Martin Albrecht | Bruno Blanchet | Sherman S.M. Chow |
| Mohsen Alimomeni | Andrey Bogdanov | Cheng-Kang Chu |
| Jacob Alperin-Sheriff | Julia Borghoff | Ji Young Chun |
| Tadashi Araragi | Joppe Bos | Kai-Min Chung |
| Frederik Armknecht | Wieb Bosma | Iwen Coisel |
| Man Ho Au | Charles Bouillaguet | Véronique Cortier |
| Jean-Philippe Aumasson | Elette Boyle | Joan Daemen |
| Chung Hun Baek | Christina Brzuska | Ivan Damgård |
| Joonsang Baek | Florian Böhl | M. Prem Laxman Das |
| Endre Bangerter | Jan Camenisch | Yi Deng |
| Masoud Barati | Angelo De Caro | Yvo Desmedt |
| Paulo S.L.M. Barreto | David Cash | Claus Diem |
| Stephanie Bayer | Dario Catalano | Léo Ducas |
| Amos Beimel | Debrup Chakraborty | Nico Döttling |
| Mihir Bellare | Sanjit Chatterjee | Pooya Farshim |
| David Bernhard | Céline Chevalier | Sebastian Faust |
| Rishiraj Bhattacharyya | Kyu Young Choi | Serge Fehr |
| Sanjay Bhattacherjee | Seung Geol Choi | Matthieu Finiasz |

Dario Fiore
Ewan Fleischmann
Christian Forler
Pierre-Alain Fouque
Georg Fuchsbauer
Atsushi Fujioka
Eiichiro Fujisaki
Jakob Funder
Steven Galbraith
Nicolas Gama
Praveen Gauravaram
Ran Gelles
Michael Gorski
Rob Granger
Fuchun Guo
Jian Guo
Kishan Chand Gupta
Shai Halevi
Mike Hamburg
Dong-Guk Han
Jinguang Han
Carmit Hazay
Jens Hermans
Shoichi Hirose
Hyunsook Hong
Qiong Huang
Xinyi Huang
Pavel Hubacek
Jung Yeon Hwang
Yuval Ishay
Kouichi Itoh
Tetsu Iwata
Abhishek Jain
David Jao
Jeremy Jean
Ik Rae Jeong
Dimitar Jetchev
Nam-Su Jho
Saqib Kakvi
Seny Kamara
Koray Karabina
Jonathan Katz
Shahram Khazaei
Jihye Kim
Kitak Kim
Minkyu Kim
Myungsun Kim
Sungwook Kim
TaeHyun Kim
Thorsten Kleinjung
Edward Knapp
Simon Knellwolf
Woo Kwon Koo
Daniel Kraschewski
Mathias Krause
Stephan Krenn
Ranjit Kumaresan
Hidenori Kuwakado
Soonhak Kwon
Junzuo Lai
Gregor Leander
Hyung Tae Lee
Kwangsu Lee
Mun-Kyu Lee
Yuseop Lee
Anja Lehmann
Allison Lewko
Jin Li
Benoît Libert
Seongan Lim
Huijia Lin
Yehuda Lindell
Richard Lindner
Jake Loftus
Jiqiang Lu
Vadim Lyubashevsky
Daegun Ma
Subhamoy Maitra
Hemanta Maji
Mark Manulis
Alexander May
James McKee
Sigurd Meldgaard
Florian Mendel
Alexander Meurer
Andrea Miele
Marine Minier
Tal Moran
Ciaran Mullan
Sean Murphy
Mridul Nandi
Kris Narayan
María Naya-Plasencia
Salman Niksefat
Ryo Nishimaki
Peter Sebastian Nordholt
Miyako Ohkubo
Tatsuaki Okamoto
Eran Omri
Claudio Orlandi
Onur Ozen
Dan Page
Periklis Papakonstantinou
Hyun-A Park
Je Hong Park
Jong Hwan Park
Jung Youl Park
Anat Paskin-Cherniavsky
Valerio Pastro
Kenny Paterson
Arpita Patra
Serdar Pehlivanoglu
Ludovic Perret
Christiane Peters
Viet Pham
Duong Hieu Phan
Krzysztof Pietrzak
Benny Pinkas
David Pointcheval
Tal Rabin
Somindu C Ramanna
Vanishree Rao
Mariana Raykova
Mohammad Reza Reyhanitabar
Thomas Ristenpart
Aaron Roth
Ron Rothblum
Carla Ràfols
S. Sharmila Deva Selvi
Subhabrata Samajder
Yu Sasaki
Takakazu Satoh

Christian Schaffner
Martin Schläffer
Dominique Schröder
Jacob Schuldt
Jörg Schwenk
Sven Schäge
Mike Scott
Jae Hong Seo
Hakan Seyalioglu
Abhi Shelat
Shashank Singh
Adam Smith
Martijn Stam
Paul Stankovski
Douglas Stebila
John Steinberger
Rainer Steinwandt
Mario Strefler
Christoph Striecks
Koutarou Suzuki
Tsuyoshi Takagi
Qiang Tang
Tamir Tassa
Aris Tentes
Stefano Tessaro
Abhradeep Guha Thakurta
Nicolas Theriault
Enrico Thomae
Søren S Thomsen
Mehdi Tibouchi
Tomas Toft
Berkant Ustaoglu
Yevgeniy Vahlis
Frederik Vercauteren
Damien Vergnaud
Ivan Visconti
Martin Vuagnoux
Lei Wang
Bogdan Warinschi
Gaven Watson
Lei Wei
Daniel Wichs
Christopher Wolf
Hongjun Wu
Qianhong Wu
Keita Xagawa
Guomin Yang
Kan Yasuda
Kazuki Yoneyama
Tsz Hon Yuen
Greg Zaverucha
Erik Zenner
Hong-Sheng Zhou
Angela Zottarel

## Sponsoring Institutions

Center for Information Security Technologies of Korea University (CIST)
Korean Federation of Science and Technology Societies (KOFST)
Seoul National University
Electronics and Telecommunications Research Institute (ETRI)
Seoul Metropolitan Government

# Table of Contents

## Lattices and Quantum Cryptography



## Public Key Encryption I



## Public Key Encryption II

## Database Privacy



## Hash Function



## Symmetric Key Encryption

## Zero Knowledge Proof



## Universal Composability



## Foundation



## Secure Computation and Secret Sharing

## Public Key Signature



## Leakage Resilient Cryptography