

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

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

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

© International Association for Cryptologic Research 2011

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

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

BKZ 2.0: Better Lattice Security Estimates	1
<i>Yuanmi Chen and Phong Q. Nguyen</i>	
Functional Encryption for Inner Product Predicates from Learning with Errors	21
<i>Shweta Agrawal, David Mandell Freeman, and Vinod Vaikuntanathan</i>	
Random Oracles in a Quantum World	41
<i>Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry</i>	

Public Key Encryption I

Lossy Encryption: Constructions from General Assumptions and Efficient Selective Opening Chosen Ciphertext Security	70
<i>Brett Hemenway, Benoît Libert, Rafail Ostrovsky, and Damien Vergnaud</i>	
Structure Preserving CCA Secure Encryption and Applications	89
<i>Jan Camenisch, Kristiyan Haralambiev, Markulf Kohlweiss, Jorn Lapon, and Vincent Naessens</i>	
Decoding Random Linear Codes in $\tilde{O}(2^{0.054n})$	107
<i>Alexander May, Alexander Meurer, and Enrico Thomae</i>	
Lower and Upper Bounds for Deniable Public-Key Encryption	125
<i>Rikke Bendlin, Jesper Buus Nielsen, Peter Sebastian Nordholt, and Claudio Orlandi</i>	

Public Key Encryption II

Bridging Broadcast Encryption and Group Key Agreement	143
<i>Qianhong Wu, Bo Qin, Lei Zhang, Josep Domingo-Ferrer, and Oriol Farràs</i>	
On the Joint Security of Encryption and Signature, Revisited	161
<i>Kenneth G. Paterson, Jacob C.N. Schuldt, Martijn Stam, and Susan Thomson</i>	
Polly Cracker, Revisited	179
<i>Martin R. Albrecht, Pooya Farshim, Jean-Charles Faugère, and Ludovic Perret</i>	

Database Privacy

Oblivious RAM with $O((\log N)^3)$ Worst-Case Cost	197
<i>Elaine Shi, T.-H. Hubert Chan, Emil Stefanov, and Mingfei Li</i>	
Noiseless Database Privacy	215
<i>Raghav Bhaskar, Abhishek Bhowmick, Vipul Goyal, Srivatsan Larman, and Abhradeep Thakurta</i>	

Hash Function

The Preimage Security of Double-Block-Length Compression Functions	233
<i>Frederik Armknecht, Ewan Fleischmann, Matthias Krause, Jooyoung Lee, Martijn Stam, and John Steinberger</i>	
Rebound Attack on JH42	252
<i>María Naya-Plasencia, Deniz Toz, and Kerem Varici</i>	
Second-Order Differential Collisions for Reduced SHA-256	270
<i>Alex Biryukov, Mario Lamberger, Florian Mendel, and Ivica Nikolić</i>	
Finding SHA-2 Characteristics: Searching through a Minefield of Contradictions	288
<i>Florian Mendel, Tomislav Nad, and Martin Schl��ffer</i>	

Symmetric Key Encryption

Cryptanalysis of ARMADILLO2	308
<i>Mohamed Ahmed Abdelraheem, C��line Blondeau, Mar��a Naya-Plasencia, Marion Videau, and Erik Zenner</i>	
An Experimentally Verified Attack on Full Grain-128 Using Dedicated Reconfigurable Hardware	327
<i>Itai Dinur, Tim G��neysu, Christof Paar, Adi Shamir, and Ralf Zimmermann</i>	
Biclique Cryptanalysis of the Full AES	344
<i>Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger</i>	
Tag Size Does Matter: Attacks and Proofs for the TLS Record Protocol	372
<i>Kenneth G. Paterson, Thomas Ristenpart, and Thomas Shrimpton</i>	

Zero Knowledge Proof

Resetable Cryptography in Constant Rounds – The Case of Zero Knowledge	390
<i>Yi Deng, Dengguo Feng, Vipul Goyal, Dongdai Lin, Amit Sahai, and Moti Yung</i>	
Two Provers in Isolation	407
<i>Claude Crépeau, Louis Salvail, Jean-Raymond Simard, and Alain Tapp</i>	
Efficient Zero-Knowledge Arguments from Two-Tiered Homomorphic Commitments	431
<i>Jens Groth</i>	

Universal Composability

A Framework for Practical Universally Composable Zero-Knowledge Protocols	449
<i>Jan Camenisch, Stephan Krenn, and Victor Shoup</i>	
Non-interactive and Re-usable Universally Composable String Commitments with Adaptive Security	468
<i>Marc Fischlin, Benoît Libert, and Mark Manulis</i>	

Foundation

Cryptography Secure against Related-Key Attacks and Tampering	486
<i>Mihir Bellare, David Cash, and Rachel Miller</i>	
Counting Points on Genus 2 Curves with Real Multiplication	504
<i>Pierrick Gaudry, David Kohel, and Benjamin Smith</i>	
On the Efficiency of Bit Commitment Reductions	520
<i>Samuel Ranellucci, Alain Tapp, Severin Winkler, and Jürg Wullschlegel</i>	
Secure Communication in Multicast Graphs	538
<i>Qiushi Yang and Yvo Desmedt</i>	

Secure Computation and Secret Sharing

Constant-Round Private Function Evaluation with Linear Complexity	556
<i>Jonathan Katz and Lior Malka</i>	

Constant-Rounds, Linear Multi-party Computation for Exponentiation and Modulo Reduction with Perfect Security	572
<i>Chao Ning and Qiuliang Xu</i>	
Computational Verifiable Secret Sharing Revisited	590
<i>Michael Backes, Aniket Kate, and Arpita Patra</i>	
Natural Generalizations of Threshold Secret Sharing	610
<i>Oriol Farràs, Carles Padró, Chaoping Xing, and An Yang</i>	

Public Key Signature

Separating Short Structure-Preserving Signatures from Non-interactive Assumptions	628
<i>Masayuki Abe, Jens Groth, and Miyako Ohkubo</i>	
Short Signatures from Weaker Assumptions	647
<i>Dennis Hofheinz, Tibor Jager, and Eike Kiltz</i>	
Practical Key-Recovery for All Possible Parameters of SFLASH	667
<i>Charles Bouillaguet, Pierre-Alain Fouque, and Gilles Macario-Rat</i>	

Leakage Resilient Cryptography

The Leakage-Resilience Limit of a Computational Problem Is Equal to Its Unpredictability Entropy	686
<i>Divesh Aggarwal and Ueli Maurer</i>	
Leakage-Resilient Cryptography from the Inner-Product Extractor	702
<i>Stefan Dziembowski and Sebastian Faust</i>	
Program Obfuscation with Leaky Hardware	722
<i>Nir Bitansky, Ran Canetti, Shafi Goldwasser, Shai Halevi, Yael Tauman Kalai, and Guy N. Rothblum</i>	
BiTR: Built-in Tamper Resilience	740
<i>Seung Geol Choi, Aggelos Kiayias, and Tal Malkin</i>	

Author Index	759
--------------------	-----