

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



Springer

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

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

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

Sponsoring Institutions

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

Table of Contents

Invited Talks

Pairing-Based Cryptography: Past, Present, and Future	1
<i>Dan Boneh</i>	

Some Mathematical Mysteries in Lattices	2
<i>Chuanming Zong</i>	

Public-Key Cryptography I

Constant-Size Structure-Preserving Signatures: Generic Constructions and Simple Assumptions	4
<i>Masayuki Abe, Melissa Chase, Bernardo David, Markulf Kohlweiss, Ryo Nishimaki, and Miyako Ohkubo</i>	

Dual Form Signatures: An Approach for Proving Security from Static Assumptions	25
<i>Michael Gerbush, Allison Lewko, Adam O'Neill, and Brent Waters</i>	

Breaking Pairing-Based Cryptosystems Using η_T Pairing over $GF(3^{97})$	43
<i>Takuya Hayashi, Takeshi Shimoyama, Naoyuki Shinohara, and Tsuyoshi Takagi</i>	

On the (Im)possibility of Projecting Property in Prime-Order Setting . . .	61
<i>Jae Hong Seo</i>	

Foundation

Optimal Reductions of Some Decisional Problems to the Rank Problem	80
<i>Jorge Luis Villar</i>	

Signature Schemes Secure against Hard-to-Invert Leakage	98
<i>Sebastian Faust, Carmit Hazay, Jesper Buus Nielsen, Peter Sebastian Nordholt, and Angela Zottarel</i>	

Completeness for Symmetric Two-Party Functionalities - Revisited	116
<i>Yehuda Lindell, Eran Omri, and Hila Zarosim</i>	

Adaptively Secure Garbling with Applications to One-Time Programs and Secure Outsourcing	134
<i>Mihir Bellare, Viet Tung Hoang, and Phillip Rogaway</i>	

The Generalized Randomized Iterate and Its Application to New Efficient Constructions of UOWHFs from Regular One-Way Functions 154
Scott Ames, Rosario Gennaro, and Muthuramakrishnan Venkitasubramaniam

Symmetric Cipher

Perfect Algebraic Immune Functions 172
Meicheng Liu, Yin Zhang, and Dongdai Lin

Differential Analysis of the LED Block Cipher 190
Florian Mendel, Vincent Rijmen, Deniz Toz, and Kerem Varici

PRINCE – A Low-Latency Block Cipher for Pervasive Computing Applications: Extended Abstract 208
Julia Borghoff, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knezevic, Lars R. Knudsen, Gregor Leander, Ventzislav Nikov, Christof Paar, Christian Rechberger, Peter Rombouts, Søren S. Thomsen, and Tolga Yalçın

Analysis of Differential Attacks in ARX Constructions 226
Gaëtan Leurent

Integral and Multidimensional Linear Distinguishers with Correlation Zero 244
Andrey Bogdanov, Gregor Leander, Kaisa Nyberg, and Meiqin Wang

Differential Attacks against Stream Cipher ZUC 262
Hongjun Wu, Tao Huang, Phuong Ha Nguyen, Huaxiong Wang, and San Ling

Security Proof

An Asymptotically Tight Security Analysis of the Iterated Even-Mansour Cipher 278
Rodolphe Lampe, Jacques Patarin, and Yannick Seurin

3kf9: Enhancing 3GPP-MAC beyond the Birthday Bound 296
Liting Zhang, Wenling Wu, Han Sui, and Peng Wang

Understanding Adaptivity: Random Systems Revisited 313
Dimitar Jetchev, Onur Özen, and Martijn Stam

RKA Security beyond the Linear Barrier: IBE, Encryption and Signatures 331
Mihir Bellare, Kenneth G. Paterson, and Susan Thomson

Public-Key Cryptography II

Fully Secure Unbounded Inner-Product and Attribute-Based Encryption	349
<i>Tatsuaki Okamoto and Katsuyuki Takashima</i>	
Computing on Authenticated Data: New Privacy Definitions and Constructions	367
<i>Nuttapong Attrapadung, Benoît Libert, and Thomas Peters</i>	
A Coding-Theoretic Approach to Recovering Noisy RSA Keys	386
<i>Kenneth G. Paterson, Antigoni Polychroniadou, and Dale L. Sibborn</i>	
Certifying RSA	404
<i>Saqib A. Kakvi, Eike Kiltz, and Alexander May</i>	

Lattice-Based Cryptography and Number Theory

Faster Gaussian Lattice Sampling Using Lazy Floating-Point Arithmetic	415
<i>Léo Ducas and Phong Q. Nguyen</i>	
Learning a Zonotope and More: Cryptanalysis of NTRUSign Countermeasures	433
<i>Léo Ducas and Phong Q. Nguyen</i>	
On Polynomial Systems Arising from a Weil Descent	451
<i>Christophe Petit and Jean-Jacques Quisquater</i>	

Public-Key Cryptography III

ECM at Work	467
<i>Joppe W. Bos and Thorsten Kleinjung</i>	
IND-CCA Secure Cryptography Based on a Variant of the LPN Problem	485
<i>Nico Döttling, Jörn Müller-Quade, and Anderson C.A. Nascimento</i>	

Hash Function

Provable Security of the Knudsen-Preneel Compression Functions	504
<i>Jooyoung Lee</i>	
Optimal Collision Security in Double Block Length Hashing with Single Length Key	526
<i>Bart Mennink</i>	

Bicliques for Permutations: Collision and Preimage Attacks in Stronger Settings	544
<i>Dmitry Khovratovich</i>	
Investigating Fundamental Security Requirements on Whirlpool: Improved Preimage and Collision Attacks	562
<i>Yu Sasaki, Lei Wang, Shuang Wu, and Wenling Wu</i>	
Generic Related-Key Attacks for HMAC	580
<i>Thomas Peyrin, Yu Sasaki, and Lei Wang</i>	

Cryptographic Protocol I

The Five-Card Trick Can Be Done with Four Cards	598
<i>Takaaki Mizuki, Michihito Kumamoto, and Hideaki Sone</i>	
A Mix-Net from Any CCA2 Secure Cryptosystem	607
<i>Shahram Khazaei, Tal Moran, and Douglas Wikström</i>	
How Not to Prove Yourself: Pitfalls of the Fiat-Shamir Heuristic and Applications to Helios	626
<i>David Bernhard, Olivier Pereira, and Bogdan Warinschi</i>	

Cryptographic Protocol II

Sequential Aggregate Signatures with Lazy Verification from Trapdoor Permutations (Extended Abstract)	644
<i>Kyle Brogle, Sharon Goldberg, and Leonid Reyzin</i>	
Commitments and Efficient Zero-Knowledge Proofs from Learning Parity with Noise	663
<i>Abhishek Jain, Stephan Krenn, Krzysztof Pietrzak, and Aris Tentes</i>	
Calling Out Cheaters: Covert Security with Public Verifiability	681
<i>Gilad Asharov and Claudio Orlandi</i>	
A Unified Framework for UC from Only OT	699
<i>Rafael Pass, Huijia Lin, and Muthuramakrishnan Venkatasubramanian</i>	

Implementation Issues

Four-Dimensional Gallant-Lambert-Vanstone Scalar Multiplication	718
<i>Patrick Longa and Francesco Sica</i>	

Shuffling against Side-Channel Attacks: A Comprehensive Study with Cautionary Note	740
<i>Nicolas Veyrat-Charvillon, Marcel Medwed, Stéphanie Kerckhof, and François-Xavier Standaert</i>	
Theory and Practice of a Leakage Resilient Masking Scheme	758
<i>Josep Balasch, Sebastian Faust, Benedikt Gierlichs, and Ingrid Verbauwhede</i>	

Erratum

Investigating Fundamental Security Requirements on Whirlpool: Improved Preimage and Collision Attacks	E1
<i>Yu Sasaki, Lei Wang, Shuang Wu, and Wenling Wu</i>	
Author Index	777