

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, Lancaster, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Zurich, Switzerland

John C. Mitchell

Stanford University, Stanford, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Dortmund, Germany

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbrücken, Germany

More information about this series at <http://www.springer.com/series/7410>

Jung Hee Cheon · Tsuyoshi Takagi (Eds.)

Advances in Cryptology – ASIACRYPT 2016

22nd International Conference on the Theory
and Application of Cryptology and Information Security
Hanoi, Vietnam, December 4–8, 2016
Proceedings, Part I

Editors

Jung Hee Cheon
Seoul National University
Seoul
Korea (Republic of)

Tsuyoshi Takagi
Kyushu University
Fukuoka
Japan

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-662-53886-9 ISBN 978-3-662-53887-6 (eBook)
DOI 10.1007/978-3-662-53887-6

Library of Congress Control Number: 2016956613

LNCS Sublibrary: SL4 – Security and Cryptology

© International Association for Cryptologic Research 2016

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, 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.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer-Verlag GmbH Germany
The registered company address is: Heidelberger Platz 3, 14197 Berlin, Germany

Preface

ASIACRYPT 2016, the 22nd Annual International Conference on Theory and Application of Cryptology and Information Security, was held at InterContinental Hanoi Westlake Hotel in Hanoi, Vietnam, during December 4–8, 2016. The conference focused on all technical aspects of cryptology, and was sponsored by the International Association for Cryptologic Research (IACR).

Asiacrypt 2016 received a total of 240 submissions from all over the world. The Program Committee selected 67 papers from these submissions for publication in the proceedings of this conference. The review process was made via the usual double-blind peer review by the Program Committee comprising 43 leading experts in the field. Each submission was reviewed by at least three reviewers and five reviewers were assigned to submissions co-authored by Program Committee members. This year, the conference operated a two-round review system with a rebuttal phase. In the first-round review the Program Committee selected the 140 submissions that were considered of value for proceeding to the second round. In the second-round review the Program Committee further reviewed the submissions by taking into account their rebuttal letter from the authors. The selection process was assisted by a total of 309 external reviewers. These two-volume proceedings contain the revised versions of the papers that were selected. The revised versions were not reviewed again and the authors are responsible for their contents.

The program of Asiacrypt 2016 featured three excellent invited talks. Nadia Heninger gave a talk on “The Reality of Cryptographic Deployments on the Internet,” Hoeteck Wee spoke on “Advances in Functional Encryption,” and Neal Koblitz gave a non-technical lecture on “Cryptography in Vietnam in the French and American Wars.” The conference also featured a traditional rump session that contained short presentations on the latest research results of the field. The Program Committee selected the work “Faster Fully Homomorphic Encryption: Bootstrapping in Less Than 0.1 Seconds” by Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène for the Best Paper Award of Asiacrypt 2016. Two more papers, “Nonlinear Invariant Attack—Practical Attack on Full SCREAM, iSCREAM, and Midori64” by Yosuke Todo, Gregor Leander, Yu Sasaki and “Ciphertext Clipping: Clipping the Power of Kleptographic Attacks” by Alexander Russell, Qiang Tang, Moti Yung, Hong-Sheng Zhou were solicited to submit full versions to the *Journal of Cryptology*.

Many people contributed to the success of Asiacrypt 2016. We would like to thank the authors for submitting their research results to the conference. We are very grateful to all of the Program Committee members as well as the external reviewers for their fruitful comments and discussions on their areas of expertise. We are greatly indebted to Ngo Bao Chau and Phan Duong Hieu, the general co-chairs for their efforts and overall organization. We would also like to thank Nguyen Huu Du, Nguyen Quoc Khanh, Nguyen Duy Lan, Duong Ngoc Thai, Nguyen Ta Toan Khoa, Nguyen Ngoc Tuan,

Le Thi Lan Anh, and the local Organizing Committee for their continuous supports. We thank Steven Galbraith for expertly organizing and chairing the rump session.

Finally we thank Shai Halevi for letting us use his nice software for supporting the paper submission and review process. We also thank Alfred Hofmann, Anna Kramer, and their colleagues at Springer for handling the editorial process of the proceedings. We would like to express our gratitude to our partners and sponsors: XLIM, Microsoft Research, CISCO, Intel, Google.

December 2016

Jung Hee Cheon
Tsuyoshi Takagi

ASIACRYPT 2016

The 22nd Annual International Conference on Theory and Application of Cryptology and Information Security

Sponsored by the International Association for Cryptologic Research (IACR)

December 4–8, 2016, Hanoi, Vietnam

General Co-chairs

Ngo Bao Chau VIASM, Vietnam and University of Chicago, USA
Phan Duong Hieu XLIM, University of Limoges, France

Program Co-chairs

Jung Hee Cheon Seoul National University, Korea
Tsyuyoshi Takagi Kyushu University, Japan

Program Committee

Elena Andreeva KU Leuven, Belgium
Xavier Boyen Queensland University of Technology, Australia
Anne Canteaut Inria, France
Chen-Mou Cheng National Taiwan University, Taiwan
Sherman S.M. Chow Chinese University of Hong Kong, Hong Kong,
SAR China
Nico Döttling University of California, Berkeley, USA
Thomas Eisenbarth Worcester Polytechnic Institute, USA
Georg Fuchsbauer École Normale Supérieure, France
Steven Galbraith Auckland University, New Zealand
Sanjam Garg University of California, Berkeley, USA
Vipul Goyal Microsoft Research, India
Jens Groth University College London, UK
Sylvain Guilley Secure-IC S.A.S., France
Alejandro Hevia Universidad de Chile, Chile
Antoine Joux Foundation UPMC and LIP6, France
Xuejia Lai Shanghai Jiaotong University, China
Hyung Tae Lee Nanyang Technological University, Singapore
Kwangsu Lee Sejong University, Korea
Dongdai Lin Chinese Academy of Sciences, China
Feng-Hao Liu Florida Atlantic University, USA
Takahiro Matsuda AIST, Japan
Alexander May Ruhr University Bochum, Germany

Florian Mendel	Graz University of Technology, Austria
Amir Moradi	Ruhr University Bochum, Germany
Svetla Nikova	KU Leuven, Belgium
Tatsuaki Okamoto	NTT, Japan
Elisabeth Oswald	University of Bristol, UK
Thomas Peyrin	Nanyang Technological University, Singapore
Rei Safavi-Naini	University of Calgary, Canada
Peter Schwabe	Radboud University, The Netherlands
Jae Hong Seo	Myongji University, Korea
Damien Stehlé	ENS de Lyon, France
Ron Steinfeld	Monash University, Australia
Rainer Steinwandt	Florida Atlantic University, USA
Daisuke Suzuki	Mitsubishi Electric, Japan
Mehdi Tibouchi	NTT, Japan
Yosuke Todo	NTT, Japan
Hoang Viet Tung	University of California Santa Barbara, USA
Dominique Unruh	University of Tartu, Estonia
Ivan Visconti	University of Salerno, Italy
Huaxiong Wang	Nanyang Technological University, Singapore
Meiqin Wang	Shandong University, China
Aaram Yun	UNIST, Korea

External Reviewers

Michel Abdalla	Christof Beierle	Ming-Shing Chen
Aysajan Abidin	Fabrice Benhamouda	Yu Chen
Shashank Agrawal	Begül Bilgin	Céline Chevalier
Shweta Agrawal	Céline Blondeau	Chongwon Cho
Ahmad Ahmadi	Tobias Boelter	Kyu Young Choi
Mamun Akand	Carl Bootland	HeeWon Chung
Saed Alsayigh	Jonathan Bootle	Kai-Min Chung
Joël Alwen	Yuri Borissov	Eloi de Chérisey
Abdelrahaman Aly	Christina Boura	Michele Ciampi
Daniel Apon	Colin Boyd	Craig Costello
Muhammad Rizwan	Wouter Castryck	Joan Daemen
Asghar	Dario Catalano	Ricardo Dahab
Tomer Ashur	Andrea Cerulli	Wei Dai
Nuttapong Attrapadung	Gizem Cetin	Bernardo David
Benedikt Auerbach	Pyrros Chaidos	Thomas de Cnudde
Saikrishna	Nishanth Chandran	David Derler
Badrinarayanan	Yu-Chen Chang	Apoorva Deshpande
Shi Bai	Lin Changlu	Christoph Dobraunig
Razvan Barbulescu	Binyi Chen	Yarkin Doroz
Lejla Batina	Cong Chen	Ming Duan
Georg T. Becker	Jie Chen	Léo Ducas

Dung Hoang Duong	Vincenzo Iovino	Benoit Libert
Maria Eichlseder	Gorka Irazoqui	Fuchun Lin
Martianus Frederic Ezerman	Ai Ishida	Tingting Lin
Xiong Fan	Takanori Isobe	Meicheng Liu
Pooya Farshim	Tetsu Iwata	Yunwen Liu
Serge Fehr	Aayush Jain	Zhen Liu
Max Fillinger	Sune Jakobsen	Zidong Lu
Dario Fiore	Yin Jia	Yiyuan Luo
Victor Fischer	Shaoquan Jiang	Atul Luykx
Marc Fischlin	Chethan Kamath	Vadim Lyubashevsky
Thomas Fuhr	Sabyasachi Karati	Bernardo Magri
Jake Longo Galea	Sayasachi Karati	Mary Maller
David Galindo	Yutaka Kawai	Alex Malozemoff
Peter Gazi	Carmen Kempka	Antonio Marcedone
Essam Ghadafi	HeeSeok Kim	Benjamin Martin
Mohona Ghosh	Hyoseung Kim	Daniel Martin
Zheng Gong	Jinsu Kim	Marco Martinoli
Rishab Goyal	Myungsun Kim	Daniel Masny
Hannes Gross	Taechan Kim	Maike Massierer
Vincent Grosso	Paul Kirchner	Mitsuru Matsui
Berk Gulmezoglu	Elena Kirshanova	Willi Meier
Chun Guo	Fuyuki Kitagawa	Bart Mennink
Jian Guo	Susumu Kiyoshima	Peihan Miao
Qian Guo	Jessica Koch	Kazuhiko Minematsu
Divya Gupta	Markulf Kohlweiss	Nicky Mouha
Iftach Haitner	Vladimir Kolesnikov	Pratyay Mukherjee
Dong-Guk Han	Thomas Korak	Sean Murphy
Kyoohyung Han	Yoshihiro Koseki	Jörn Müller-Quade
Shuai Han	Ashutosh Kumar	Valérie Nacheff
Goichiro Hanaoka	Ranjit Kumaresan	Michael Naehrig
Christian Hanser	Po-Chun Kuo	Matthias Nagel
Mitsuhiro Hattori	Robert Kübler	Yusuke Naito
Gottfried Herold	Thijs Laarhoven	Mridul Nandi
Felix Heuer	Ching-Yi Lai	María Naya-Plasencia
Takato Hirano	Russell W.F. Lai	Kartik Nayak
Shoichi Hirose	Virginie Lallemand	Khoa Nguyen
Wei-Chih Hong	Adeline Langlois	Ivica Nikolic
Yuan-Che Hsu	Sebastian Lauer	Ventzislav Nikov
Geshi Huang	Su Le	Ryo Nishimaki
Guifang Huang	Gregor Leander	Anca Nitulescu
Jialin Huang	Kwangsu Lee	Koji Nuida
Xinyi Huang	Gaëtan Leurent	Maciej Obremski
Pavel Hubacek	Anthony Leverrier	Toshihiro Ohigashi
Iliia Iliashenko	Jingwei Li	Miyako Ohkubo
Mehmet Sinan Inci	Ming Li	Sumit Kumar Pandey
	Wen-Ding Li	Jong Hwan Park

Seunghwan Park	Luisa Siniscalchi	Carolyn Whitnall
Alain Passelègue	Daniel Slamanig	Alexander Wild
Christopher Patton	Nigel Smart	Baofeng Wu
Bo-Yuan Peng	Raphael Spreitzer	Keita Xagawa
Rachel Player	Douglas Stebila	Zejun Xiang
Antigoni Polychroniadou	Christoph Striecks	Hong Xu
Bertram Pöttering	Takeshi Sugawara	Weijia Xue
Sebastian Ramacher	Yao Sun	Shota Yamada
Vanishree Rao	Berk Sunar	Takashi Yamakawa
Shuqin Ren	Koutarou Suzuki	Hailun Yan
Reza Reyhanitabar	Alan Szepieniec	Jun Yan
Bastian Richter	Mostafa Taha	Bo-Yin Yang
Thomas Ristenpart	Somayeh Taheri	Bohan Yang
Mike Rosulek	Junko Takahashi	Guomin Yang
Hansol Ryu	Katsuyuki Takashima	Mohan Yang
Akshayaram Srinivasan	Benjamin Tan	Shang-Yi Yang
Yusuke Sakai	Jean-Pierre Tillich	Kan Yasuda
Kochi Sakumoto	Junichi Tomida	Xin Ye
Amin Sakzad	Yiannis Tselekounis	Wentan Yi
Simona Samardjiska	Himanshu Tyagi	Scott Yilek
Yu Sasaki	Thomas Unterluggauer	Kazuki Yoneyama
Pascal Sasdrich	Damien Vergnaud	Rina Zeitoun
Falk Schellenberg	Gilles Villard	Fan Zhang
Benedikt Schmidt	Vanessa Vitse	Guoyan Zhang
Tobias Schneider	Damian Vizar	Liang Feng Zhang
Jacob Schuldt	Michael Walter	Liangfeng Zhang
Okan Seker	Han Wang	Tao Zhang
Nicolas Sendrier	Hao Wang	Wentao Zhang
Jae Hong Seo	Qiungju Wang	Yusi Zhang
Minhye Seo	Wei Wang	Zongyang Zhang
Yannick Seurin	Yuyu Wang	Jingyuan Zhao
Masoumeh Shafienezad	Yohei Watanabe	Yongjun Zhao
Barak Shani	Hoeteck Wee	Yixin Zhong
Danilo Sijacic	Wei Wei	Hong-Sheng Zhou
Alice Silverberg	Mor Weiss	Xiao Zhou
Siang Meng Sim	Mario Werner	Jincheng Zhuang
Dave Singelee	Bas Westerbaan	

Local Organizing Committee

Co-chairs

Ngo Bao Chau
Phan Duong Hieu

VIASM, Vietnam and University of Chicago, USA
XLIM, University of Limoges, France

Members

Nguyen Huu Du	VIASM, Vietnam
Nguyen Quoc Khanh	Vietcombank, Vietnam
Nguyen Duy Lan	Microsoft Research, USA
Duong Ngoc Thai	Google, USA
Nguyen Ta Toan Khoa	NTU, Singapore
Nguyen Ngoc Tuan	VIASM, Vietnam
Le Thi Lan Anh	VIASM, Vietnam

Sponsors

XLIM
Microsoft Research
CISCO
Intel
Google

Invited Talks

Advances in Functional Encryption

Hoeteck Wee

ENS, Paris, France
wee@di.ens.fr

Abstract. Functional encryption is a novel paradigm for public-key encryption that enables both fine-grained access control and selective computation on encrypted data, as is necessary to protect big, complex data in the cloud. In this talk, I will provide a brief introduction to functional encryption and an overview of the state of the art, with a focus on constructions based on lattices.

The Reality of Cryptographic Deployments on the Internet

Nadia Heninger

University of Pennsylvania, Philadelphia, USA

Abstract. Security proofs for cryptographic primitives and protocols rely on a number of (often implicit) assumptions about the world in which these components live. They assume that implementations are correct, that specifications are followed, that systems make sensible choices about error conditions, and that reliable sources of random numbers are present. However, a number of real world studies examining cryptographic deployments have shown that these assumptions are often not true on a large scale, with catastrophic effects for security. In addition to simple programming errors, many real-world cryptographic vulnerabilities can be traced back to more complex underlying causes, such as backwards compatibility, legacy protocols and software, hard-coded resource limits, and political interference in design choices.

Many of these issues appear on the surface to be at an entirely different level of abstraction from the cryptographic primitives used in their construction. However, by taking advantage of the structure of many cryptographic primitives when used at Internet scale, it is possible to uncover fundamental vulnerabilities in implementations. I will discuss the interplay between mathematical cryptanalysis techniques and the thorny implementation issues that lead to vulnerable cryptographic deployments in the real world.

Contents – Part I

Asiacrypt 2016 Best Paper

Faster Fully Homomorphic Encryption: Bootstrapping in Less Than 0.1 Seconds	3
<i>Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène</i>	

Mathematical Analysis I

A General Polynomial Selection Method and New Asymptotic Complexities for the Tower Number Field Sieve Algorithm	37
<i>Palash Sarkar and Shashank Singh</i>	
On the Security of Supersingular Isogeny Cryptosystems	63
<i>Steven D. Galbraith, Christophe Petit, Barak Shani, and Yan Bo Ti</i>	

AES and White-Box

Simpira v2: A Family of Efficient Permutations Using the AES Round Function	95
<i>Shay Gueron and Nicky Mouha</i>	
Towards Practical Whitebox Cryptography: Optimizing Efficiency and Space Hardness.	126
<i>Andrey Bogdanov, Takanori Isobe, and Elmar Tischhauser</i>	
Efficient and Provable White-Box Primitives	159
<i>Pierre-Alain Fouque, Pierre Karpman, Paul Kirchner, and Brice Minaud</i>	

Hash Function

MiMC: Efficient Encryption and Cryptographic Hashing with Minimal Multiplicative Complexity	191
<i>Martin Albrecht, Lorenzo Grassi, Christian Rechberger, Arnab Roy, and Tyge Tiessen</i>	
Balloon Hashing: A Memory-Hard Function Providing Provable Protection Against Sequential Attacks.	220
<i>Dan Boneh, Henry Corrigan-Gibbs, and Stuart Schechter</i>	

Linear Structures: Applications to Cryptanalysis
of Round-Reduced KECCAK. 249
Jian Guo, Meicheng Liu, and Ling Song

Randomness

When Are Fuzzy Extractors Possible? 277
Benjamin Fuller, Leonid Reyzin, and Adam Smith

More Powerful and Reliable Second-Level Statistical Randomness Tests
for NIST SP 800-22 307
Shuangyi Zhu, Yuan Ma, Jingqiang Lin, Jia Zhuang, and Jiwu Jing

Authenticated Encryption

Trick or Tweak: On the (In)security of OTR’s Tweaks 333
Raphael Bost and Olivier Sanders

Universal Forgery and Key Recovery Attacks on ELMd Authenticated
Encryption Algorithm 354
Asli Bay, Oğuzhan Ersoy, and Ferhat Karakoç

Statistical Fault Attacks on Nonce-Based Authenticated Encryption
Schemes 369
*Christoph Dobraunig, Maria Eichlseder, Thomas Korak, Victor Lomné,
and Florian Mendel*

Authenticated Encryption with Variable Stretch 396
Reza Reyhanitabar, Serge Vaudenay, and Damian Vizár

Block Cipher I

Salvaging Weak Security Bounds for Blockcipher-Based Constructions 429
Thomas Shrimpton and R. Seth Terashima

How to Build Fully Secure Tweakable Blockciphers from Classical
Blockciphers. 455
Lei Wang, Jian Guo, Guoyan Zhang, Jingyuan Zhao, and Dawu Gu

Design Strategies for ARX with Provable Bounds: SPARX and LAX 484
*Daniel Dinu, Léo Perrin, Aleksei Udovenko, Vesselin Velichkov,
Johann Großschädl, and Alex Biryukov*

SCA and Leakage Resilience I

Side-Channel Analysis Protection and Low-Latency in Action:
– Case Study of PRINCE and Midori – 517
Amir Moradi and Tobias Schneider

Characterisation and Estimation of the Key Rank Distribution
in the Context of Side Channel Evaluations 548
Daniel P. Martin, Luke Mather, Elisabeth Oswald, and Martijn Stam

Taylor Expansion of Maximum Likelihood Attacks for Masked
and Shuffled Implementations. 573
*Nicolas Bruneau, Sylvain Guilley, Annelie Heuser, Olivier Rioul,
François-Xavier Standaert, and Yannick Tégli*

Unknown-Input Attacks in the Parallel Setting: Improving the Security
of the CHES 2012 Leakage-Resilient PRF 602
*Marcel Medwed, François-Xavier Standaert, Venzislav Nikov,
and Martin Feldhofer*

Block Cipher II

A New Algorithm for the Unbalanced Meet-in-the-Middle Problem. 627
Ivica Nikolić and Yu Sasaki

Applying MILP Method to Searching Integral Distinguishers Based
on Division Property for 6 Lightweight Block Ciphers. 648
Zejun Xiang, Wentao Zhang, Zhenzhen Bao, and Dongdai Lin

Reverse Cycle Walking and Its Applications. 679
Sarah Miracle and Scott Yilek

Mathematical Analysis II

Optimization of LPN Solving Algorithms 703
Sonia Bogos and Serge Vaudenay

The Kernel Matrix Diffie-Hellman Assumption. 729
Paz Morillo, Carla Ràfols, and Jorge L. Villar

Cryptographic Applications of Capacity Theory: On the Optimality
of Coppersmith’s Method for Univariate Polynomials 759
Ted Chinburg, Brett Hemenway, Nadia Heninger, and Zachary Scherr

A Key Recovery Attack on MDPC with CCA Security
Using Decoding Errors 789
Qian Guo, Thomas Johansson, and Paul Stankovski

SCA and Leakage Resilience II

A Tale of Two Shares: Why Two-Share Threshold Implementation Seems
Worthwhile—and Why It Is Not. 819
Cong Chen, Mohammad Farmani, and Thomas Eisenbarth

Cryptographic Reverse Firewall via Malleable Smooth Projective Hash Functions. 844
Rongmao Chen, Yi Mu, Guomin Yang, Willy Susilo, Fuchun Guo, and Mingwu Zhang

Efficient Public-Key Cryptography with Bounded Leakage and Tamper Resilience. 877
Antonio Faonio and Daniele Venturi

Public-Key Cryptosystems Resilient to Continuous Tampering and Leakage of Arbitrary Functions 908
Eiichiro Fujisaki and Keita Xagawa

Author Index 939

Contents – Part II

Asiacrypt 2016 Award Papers

Nonlinear Invariant Attack: Practical Attack on Full SCREAM, iSCREAM, and Midori64	3
<i>Yosuke Todo, Gregor Leander, and Yu Sasaki</i>	
Cliptography: Clipping the Power of Kleptographic Attacks	34
<i>Alexander Russell, Qiang Tang, Moti Yung, and Hong-Sheng Zhou</i>	

Zero Knowledge

Zero-Knowledge Accumulators and Set Algebra	67
<i>Esha Ghosh, Olga Ohrimenko, Dimitrios Papadopoulos, Roberto Tamassia, and Nikos Triandopoulos</i>	
Zero-Knowledge Arguments for Matrix-Vector Relations and Lattice-Based Group Encryption	101
<i>Benoît Libert, San Ling, Fabrice Mouhartem, Khoa Nguyen, and Huaxiong Wang</i>	

Post Quantum Cryptography

From 5-Pass \mathcal{MQ} -Based Identification to \mathcal{MQ} -Based Signatures	135
<i>Ming-Shing Chen, Andreas Hülsing, Joost Rijneveld, Simona Samardjiska, and Peter Schwabe</i>	
Collapse-Binding Quantum Commitments Without Random Oracles	166
<i>Dominique Unruh</i>	
Digital Signatures Based on the Hardness of Ideal Lattice Problems in All Rings	196
<i>Vadim Lyubashevsky</i>	

Provable Security

Adaptive Oblivious Transfer and Generalization	217
<i>Olivier Blazy, Céline Chevalier, and Paul Germouty</i>	
Selective Opening Security from Simulatable Data Encapsulation	248
<i>Felix Heuer and Bertram Poettering</i>	

Selective-Opening Security in the Presence of Randomness Failures 278
Viet Tung Hoang, Jonathan Katz, Adam O’Neill, and Mohammad Zaheri

Efficient KDM-CCA Secure Public-Key Encryption
for Polynomial Functions 307
Shuai Han, Shengli Liu, and Lin Lyu

Structure-Preserving Smooth Projective Hashing 339
Olivier Blazy and Céline Chevalier

Digital Signature

Signature Schemes with Efficient Protocols and Dynamic Group Signatures
from Lattice Assumptions 373
*Benoît Libert, San Ling, Fabrice Mouhartem, Khoa Nguyen,
and Huaxiong Wang*

Towards Tightly Secure Lattice Short Signature and Id-Based Encryption . . . 404
Xavier Boyen and Qinyi Li

From Identification to Signatures, Tightly: A Framework and Generic
Transforms 435
Mihir Bellare, Bertram Poettering, and Douglas Stebila

How to Obtain Fully Structure-Preserving (Automorphic) Signatures
from Structure-Preserving Ones. 465
*Yuyu Wang, Zongyang Zhang, Takahiro Matsuda, Goichiro Hanaoka,
and Keisuke Tanaka*

Functional and Homomorphic Cryptography

Multi-key Homomorphic Authenticators. 499
Dario Fiore, Aikaterini Mitrokotsa, Luca Nizzardo, and Elena Pagnin

Multi-input Functional Encryption with Unbounded-Message Security 531
Vipul Goyal, Aayush Jain, and Adam O’Neill

Verifiable Functional Encryption. 557
Saikrishna Badrinarayanan, Vipul Goyal, Aayush Jain, and Amit Sahai

ABE and IBE

Dual System Encryption Framework in Prime-Order Groups
via Computational Pair Encodings. 591
Nuttapong Attrapadung

Efficient IBE with Tight Reduction to Standard Assumption in the Multi-challenge Setting	624
<i>Junqing Gong, Xiaolei Dong, Jie Chen, and Zhenfu Cao</i>	
Déjà Q All Over Again: Tighter and Broader Reductions of q -Type Assumptions	655
<i>Melissa Chase, Mary Maller, and Sarah Meiklejohn</i>	
Partitioning via Non-linear Polynomial Functions: More Compact IBEs from Ideal Lattices and Bilinear Maps	682
<i>Shuichi Katsumata and Shota Yamada</i>	
Foundation	
How to Generate and Use Universal Samplers	715
<i>Dennis Hofheinz, Tibor Jager, Dakshita Khurana, Amit Sahai, Brent Waters, and Mark Zhandry</i>	
Iterated Random Oracle: A Universal Approach for Finding Loss in Security Reduction	745
<i>Fuchun Guo, Willy Susilo, Yi Mu, Rongmao Chen, Jianchang Lai, and Guomin Yang</i>	
NIZKs with an Untrusted CRS: Security in the Face of Parameter Subversion	777
<i>Mihir Bellare, Georg Fuchsbauer, and Alessandra Scafuro</i>	
Cryptographic Protocol	
Universal Composition with Responsive Environments	807
<i>Jan Camenisch, Robert R. Enderlein, Stephan Krenn, Ralf Küsters, and Daniel Rausch</i>	
A Shuffle Argument Secure in the Generic Model.	841
<i>Prastudy Fauzi, Helger Lipmaa, and Michał Zajac</i>	
Efficient Public-Key Distance Bounding Protocol	873
<i>Handan Kılınç and Serge Vaudenay</i>	
Indistinguishable Proofs of Work or Knowledge	902
<i>Foteini Baldimtsi, Aggelos Kiayias, Thomas Zacharias, and Bingsheng Zhang</i>	
Multi-party Computation	
Size-Hiding Computation for Multiple Parties	937
<i>Kazumasa Shinagawa, Koji Nuida, Takashi Nishide, Goichiro Hanaoka, and Eiji Okamoto</i>	

How to Circumvent the Two-Ciphertext Lower Bound for Linear Garbling Schemes	967
<i>Carmen Kempka, Ryo Kikuchi, and Koutarou Suzuki</i>	
Constant-Round Asynchronous Multi-Party Computation Based on One-Way Functions	998
<i>Sandro Coretti, Juan Garay, Martin Hirt, and Vassilis Zikas</i>	
Reactive Garbling: Foundation, Instantiation, Application.	1022
<i>Jesper Buus Nielsen and Samuel Ranellucci</i>	
Author Index	1053