

Lecture Notes in Computer Science

14438


Founding Editors


Gerhard Goos
Juris Hartmanis

Editorial Board Members

Elisa Bertino, *Purdue University, West Lafayette, IN, USA*

Wen Gao, *Peking University, Beijing, China*

Bernhard Steffen , *TU Dortmund University, Dortmund, Germany*

Moti Yung , *Columbia University, New York, NY, USA*

The series Lecture Notes in Computer Science (LNCS), including its subseries Lecture Notes in Artificial Intelligence (LNAI) and Lecture Notes in Bioinformatics (LNBI), has established itself as a medium for the publication of new developments in computer science and information technology research, teaching, and education.


LNCS enjoys close cooperation with the computer science R & D community, the series counts many renowned academics among its volume editors and paper authors, and collaborates with prestigious societies. Its mission is to serve this international community by providing an invaluable service, mainly focused on the publication of conference and workshop proceedings and postproceedings. LNCS commenced publication in 1973.

Jian Guo · Ron Steinfeld
Editors

Advances in Cryptology – ASIACRYPT 2023

29th International Conference on the Theory
and Application of Cryptology and Information Security
Guangzhou, China, December 4–8, 2023
Proceedings, Part I

Editors

Jian Guo 
Nanyang Technological University
Singapore, Singapore

Ron Steinfeld 
Monash University
Melbourne, VIC, Australia

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-981-99-8720-7

ISBN 978-981-99-8721-4 (eBook)

<https://doi.org/10.1007/978-981-99-8721-4>

© International Association for Cryptologic Research 2023

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, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Paper in this product is recyclable.

Preface

The 29th Annual International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt 2023) was held in Guangzhou, China, on December 4–8, 2023. The conference covered all technical aspects of cryptology, and was sponsored by the International Association for Cryptologic Research (IACR).

We received an Asiacrypt record of 376 paper submissions from all over the world, and the Program Committee (PC) selected 106 papers for publication in the proceedings of the conference. Due to this large number of papers, the Asiacrypt 2023 program had 3 tracks.

The two program chairs were supported by the great help and excellent advice of six area chairs, selected to cover the main topic areas of the conference. The area chairs were Kai-Min Chung for Information-Theoretic and Complexity-Theoretic Cryptography, Tanja Lange for Efficient and Secure Implementations, Shengli Liu for Public-Key Cryptography Algorithms and Protocols, Khoa Nguyen for Multi-Party Computation and Zero-Knowledge, Duong Hieu Phan for Public-Key Primitives with Advanced Functionalities, and Yu Sasaki for Symmetric-Key Cryptology. Each of the area chairs helped to lead discussions together with the PC members assigned as paper discussion lead. Area chairs also helped to decide on the submissions that should be accepted from their respective areas. We are very grateful for the invaluable contribution provided by the area chairs.

To review and evaluate the submissions, while keeping the load per PC member manageable, we selected a record size PC consisting of 105 leading experts from all over the world, in all six topic areas of cryptology. The two program chairs were not allowed to submit a paper, and PC members were limited to submit one single-author paper, or at most two co-authored papers, or at most three co-authored papers all with students. Each non-PC submission was reviewed by at least three reviewers consisting of either PC members or their external sub-reviewers, while each PC member submission received at least four reviews. The strong conflict of interest rules imposed by IACR ensure that papers are not handled by PC members with a close working relationship with the authors. There were approximately 420 external reviewers, whose input was critical to the selection of papers. Submissions were anonymous and their length was limited to 30 pages excluding the bibliography and supplementary materials.

The review process was conducted using double-blind peer review. The conference operated a two-round review system with a rebuttal phase. After the reviews and first round discussions the PC selected 244 submissions to proceed to the second round and the authors were then invited to participate in an interactive rebuttal phase with the reviewers to clarify questions and concerns. The remaining 131 papers were rejected, including one desk reject. The second round involved extensive discussions by the PC members. After several weeks of additional discussions, the committee selected the final 106 papers to appear in these proceedings.

The eight volumes of the conference proceedings contain the revised versions of the 106 papers that were selected. The final revised versions of papers were not reviewed again and the authors are responsible for their contents.

The PC nominated and voted for two papers to receive the Best Paper Awards, and one paper to receive the Best Early Career Paper Award. The Best Paper Awards went to Thomas Espitau, Alexandre Wallet and Yang Yu for their paper “On Gaussian Sampling, Smoothing Parameter and Application to Signatures”, and to Kaijie Jiang, Anyu Wang, Hengyi Luo, Guoxiao Liu, Yang Yu, and Xiaoyun Wang for their paper “Exploiting the Symmetry of Z^n : Randomization and the Automorphism Problem”. The Best Early Career Paper Award went to Maxime Plancon for the paper “Exploiting Algebraic Structure in Probing Security”. The authors of those three papers were invited to submit extended versions of their papers to the Journal of Cryptology. In addition, the program of Asiacrypt 2023 also included two invited plenary talks, also nominated and voted by the PC: one talk was given by Mehdi Tibouchi and the other by Xiaoyun Wang. The conference also featured a rump session chaired by Kang Yang and Yu Yu which contained short presentations on the latest research results of the field.

Numerous people contributed to the success of Asiacrypt 2023. We would like to thank all the authors, including those whose submissions were not accepted, for submitting their research results to the conference. We are very grateful to the area chairs, PC members and external reviewers for contributing their knowledge and expertise, and for the tremendous amount of work that was done with reading papers and contributing to the discussions. We are greatly indebted to Jian Weng and Fangguo Zhang, the General Chairs, for their efforts in organizing the event and to Kevin McCurley and Kay McKelly for their help with the website and review system. We thank the Asiacrypt 2023 advisory committee members Bart Preneel, Huaxiong Wang, Kai-Min Chung, Yu Sasaki, Dongdai Lin, Shweta Agrawal and Michel Abdalla for their valuable suggestions. We are also grateful for the helpful advice and organization material provided to us by the Eurocrypt 2023 PC co-chairs Carmit Hazay and Martijn Stam and Crypto 2023 PC co-chairs Helena Handschuh and Anna Lysyanskaya. We also thank the team at Springer for handling the publication of these conference proceedings.

December 2023

Jian Guo
Ron Steinfeld

Organization

General Chairs

Jian Weng
Fanguo Zhang

Jinan University, China
Sun Yat-sen University, China

Program Committee Chairs

Jian Guo
Ron Steinfeld

Nanyang Technological University, Singapore
Monash University, Australia

Program Committee

Behzad Abdolmaleki
Masayuki Abe
Miguel Ambrona
Daniel Apon
Shi Bai
Gustavo Banegas
Zhenzhen Bao
Andrea Basso
Ward Beullens
Katharina Boudgoust
Matteo Campanelli
Ignacio Cascudo
Wouter Castryck
Jie Chen
Yilei Chen
Jung Hee Cheon

University of Sheffield, UK
NTT Social Informatics Laboratories, Japan
Input Output Global (IOHK), Spain
MITRE Labs, USA
Florida Atlantic University, USA
Qualcomm, France
Tsinghua University, China
University of Bristol, UK
IBM Research Europe, Switzerland
Aarhus University, Denmark
Protocol Labs, Denmark
IMDEA Software Institute, Spain
imec-COSIC, KU Leuven, Belgium
East China Normal University, China
Tsinghua University, China
Seoul National University and Cryptolab Inc,
South Korea
Chinese University of Hong Kong, China
Academia Sinica, Taiwan
University of Edinburgh, UK
IT University of Copenhagen, Denmark
Institute of Information Engineering, Chinese
Academy of Sciences, China

Sherman S. M. Chow
Kai-Min Chung
Michele Ciampi
Bernardo David
Yi Deng

Patrick Derbez	University of Rennes, France
Xiaoyang Dong	Tsinghua University, China
Rafael Dowsley	Monash University, Australia
Nico Döttling	Helmholtz Center for Information Security, Germany
Maria Eichlseder	Graz University of Technology, Austria
Muhammed F. Esgin	Monash University, Australia
Thomas Espitau	PQShield, France
Jun Furukawa	NEC Corporation, Japan
Aron Gohr	Independent Researcher, New Zealand
Junqing Gong	ECNU, China
Lorenzo Grassi	Ruhr University Bochum, Germany
Tim Güneysu	Ruhr University Bochum, Germany
Chun Guo	Shandong University, China
Siyao Guo	NYU Shanghai, China
Fuchun Guo	University of Wollongong, Australia
Mohammad Hajiabadi	University of Waterloo, Canada
Lucjan Hanzlik	CISPA Helmholtz Center for Information Security, Germany
Xiaolu Hou	Slovak University of Technology, Slovakia
Yuncong Hu	Shanghai Jiao Tong University, China
Xinyi Huang	Hong Kong University of Science and Technology (Guangzhou), China
Tibor Jager	University of Wuppertal, Germany
Elena Kirshanova	Technology Innovation Institute, UAE and I. Kant Baltic Federal University, Russia
Eyal Kushilevitz	Technion, Israel
Russell W. F. Lai	Aalto University, Finland
Tanja Lange	Eindhoven University of Technology, Netherlands
Hyung Tae Lee	Chung-Ang University, South Korea
Eik List	Nanyang Technological University, Singapore
Meicheng Liu	Institute of Information Engineering, Chinese Academy of Sciences, China
Guozhen Liu	Nanyang Technological University, Singapore
Fukang Liu	Tokyo Institute of Technology, Japan
Shengli Liu	Shanghai Jiao Tong University, China
Feng-Hao Liu	Florida Atlantic University, USA
Hemanta K. Maji	Purdue University, USA
Takahiro Matsuda	AIST, Japan
Christian Matt	Concordium, Switzerland
Tomoyuki Morimae	Kyoto University, Japan
Pierrick Méaux	University of Luxembourg, Luxembourg

Mridul Nandi	Indian Statistical Institute, Kolkata, India
María Naya-Plasencia	Inria, France
Khoa Nguyen	University of Wollongong, Australia
Ryo Nishimaki	NTT Social Informatics Laboratories, Japan
Anca Nitulescu	Protocol Labs, France
Ariel Nof	Bar Ilan University, Israel
Emmanuela Orsini	Bocconi University, Italy
Adam O'Neill	UMass Amherst, USA
Morten Øy garden	Simula UiB, Norway
Sikhar Patranabis	IBM Research, India
Alice Pellet-Mary	CNRS and University of Bordeaux, France
Edoardo Persichetti	Florida Atlantic University, USA and Sapienza University, Italy
Duong Hieu Phan	Telecom Paris, Institut Polytechnique de Paris, France
Josef Pieprzyk	Data61, CSIRO, Australia and ICS, PAS, Poland
Axel Y. Poschmann	PQShield, UAE
Thomas Prest	PQShield, France
Adeline Roux-Langlois	CNRS, GREYC, France
Amin Sakzad	Monash University, Australia
Yu Sasaki	NTT Social Informatics Laboratories, Japan
Jae Hong Seo	Hanyang University, South Korea
Yaobin Shen	UCLouvain, Belgium
Danping Shi	Institute of Information Engineering, Chinese Academy of Sciences, China
Damien Stehlé	CryptoLab, France
Bing Sun	National University of Defense Technology, China
Shi-Feng Sun	Shanghai Jiao Tong University, China
Keisuke Tanaka	Tokyo Institute of Technology, Japan
Qiang Tang	University of Sydney, Australia
Vanessa Teague	Thinking Cybersecurity Pty Ltd and the Australian National University, Australia
Jean-Pierre Tillich	Inria, Paris, France
Yosuke Todo	NTT Social Informatics Laboratories, Japan
Alexandre Wallet	University of Rennes, Inria, CNRS, IRISA, France
Meiqin Wang	Shandong University, China
Yongge Wang	UNC Charlotte, USA
Yuyu Wang	University of Electronic Science and Technology of China, China
Qingju Wang	Telecom Paris, Institut Polytechnique de Paris, France

Benjamin Wesolowski	CNRS and ENS Lyon, France
Shuang Wu	Huawei International, Singapore, Singapore
Keita Xagawa	Technology Innovation Institute, UAE
Chaoping Xing	Shanghai Jiao Tong University, China
Jun Xu	Institute of Information Engineering, Chinese Academy of Sciences, China
Takashi Yamakawa	NTT Social Informatics Laboratories, Japan
Kang Yang	State Key Laboratory of Cryptology, China
Yu Yu	Shanghai Jiao Tong University, China
Yang Yu	Tsinghua University, Beijing, China
Yupeng Zhang	University of Illinois Urbana-Champaign and Texas A&M University, USA
Liangfeng Zhang	ShanghaiTech University, China
Raymond K. Zhao	CSIRO's Data61, Australia
Hong-Sheng Zhou	Virginia Commonwealth University, USA

Additional Reviewers

Amit Agarwal	Pedro Branco
Jooyoung Lee	Lauren Brandt
Léo Ackermann	Alessandro Budroni
Akshima	Kevin Carrier
Bar Alon	André Chailloux
Ravi Anand	Suvradip Chakraborty
Sarah Arpin	Debasmita Chakraborty
Thomas Attema	Haokai Chang
Nuttapong Attrapadung	Bhuvnesh Chaturvedi
Manuel Barbosa	Caicai Chen
Razvan Barbulescu	Rongmao Chen
James Bartusek	Mingjie Chen
Carsten Baum	Yi Chen
Olivier Bernard	Megan Chen
Tyler Besselman	Yu Long Chen
Ritam Bhaumik	Xin Chen
Jingguo Bi	Shiyao Chen
Loic Bidoux	Long Chen
Maxime Bombar	Wonhee Cho
Xavier Bonnetain	Qiaohan Chu
Joppe Bos	Valerio Cini
Mariana Botelho da Gama	James Clements
Christina Boura	Ran Cohen
Clémence Bouvier	Alexandru Cojocaru
Ross Bowden	Sandro Coretti-Drayton

Anamaria Costache
Alain Couvreur
Daniele Cozzo
Hongrui Cui
Giuseppe D'Alconzo
Zhaopeng Dai
Quang Dao
Nilanjan Datta
Koen de Boer
Luca De Feo
Paola de Perthuis
Thomas Decru
Rafael del Pino
Julien Devevey
Henri Devillez
Siemen Dhooghe
Yaoling Ding
Jack Doerner
Jelle Don
Mark Douglas Schultz
Benjamin Dowling
Minxin Du
Xiaoqi Duan
Jesko Dujmovic
Moumita Dutta
Avijit Dutta
Ehsan Ebrahimi
Felix Engelmann
Reo Eriguchi
Jonathan Komada Eriksen
Andre Esser
Pouria Fallahpour
Zhiyong Fang
Antonio Faonio
Pooya Farshim
Joël Felderhoff
Jakob Feldtkeller
Weiqi Feng
Xiutao Feng
Shuai Feng
Qi Feng
Hanwen Feng
Antonio Flórez-Gutiérrez
Apostolos Fournaris
Paul Frixons
Ximing Fu
Georg Fuchsbauer
Philippe Gaborit
Rachit Garg
Robin Geelen
Riddhi Ghosal
Koustabh Ghosh
Barbara Gigerl
Niv Gilboa
Valerie Gilchrist
Emanuele Giunta
Xinxin Gong
Huijing Gong
Zheng Gong
Robert Granger
Zichen Gui
Anna Guinet
Qian Guo
Xiaojie Guo
Hosein Hadipour
Mathias Hall-Andersen
Mike Hamburg
Shuai Han
Yonglin Hao
Keisuke Hara
Keitaro Hashimoto
Le He
Brett Hemenway Falk
Minki Hhan
Taiga Hiroka
Akinori Hosoyamada
Chengan Hou
Martha Norberg Hovd
Kai Hu
Tao Huang
Zhenyu Huang
Michael Hutter
Jihun Hwang
Akiko Inoue
Tetsu Iwata
Robin Jadoul
Hansraj Jangir
Dirmanto Jap
Stanislaw Jarecki
Santos Jha

Ashwin Jha
Dingding Jia
Yanxue Jia
Lin Jiao
Daniel Jost
Antoine Joux
Jiayi Kang
Gabriel Kaptchuk
Alexander Karenin
Shuichi Katsumata
Pengzhen Ke
Mustafa Khairallah
Shahram Khazaei
Hamidreza Amini Khorasgani
Hamidreza Khoshakhlagh
Ryo Kikuchi
Jiseung Kim
Minkyu Kim
Suhri Kim
Ravi Kishore
Fuyuki Kitagawa
Susumu Kiyoshima
Michael Kloob
Alexander Koch
Sreehari Kollath
Dimitris Kolonelos
Yashvanth Kondi
Anders Konring
Woong Kook
Dimitri Koshelev
Markus Krausz
Toomas Krips
Daniel Kuijsters
Anunay Kulshrestha
Qiqi Lai
Yi-Fu Lai
Georg Land
Nathalie Lang
Mario Larangeira
Joon-Woo Lee
Keewoo Lee
Hyeonbum Lee
Changmin Lee
Charlotte Lefevre
Julia Len
Antonin Leroux
Andrea Lesavourey
Jannis Leuther
Jie Li
Shuaishuai Li
Huina Li
Yu Li
Yanan Li
Jiangtao Li
Song Song Li
Wenjie Li
Shun Li
Zengpeng Li
Xiao Liang
Wei-Kai Lin
Chengjun Lin
Chao Lin
Cong Ling
Yunhao Ling
Hongqing Liu
Jing Liu
Jiahui Liu
Qipeng Liu
Yamin Liu
Weiran Liu
Tianyi Liu
Siqi Liu
Chen-Da Liu-Zhang
Jinyu Lu
Zhenghao Lu
Stefan Lucks
Yiyuan Luo
Lixia Luo
Jack P. K. Ma
Fermi Ma
Gilles Macario-Rat
Luciano Maino
Christian Majenz
Laurane Marco
Lorenzo Martinico
Loïc Masure
John McVey
Willi Meier
Kelsey Melissaris
Bart Mennink

Charles Meyer-Hilfiger
Victor Miller
Chohong Min
Marine Minier
Arash Mirzaei
Pratyush Mishra
Tarik Moataz
Johannes Mono
Fabrice Mouhartem
Alice Murphy
Erik Mårtensson
Anne Müller
Marcel Nageler
Yusuke Naito
Barak Nehoran
Patrick Neumann
Tran Ngo
Phuong Hoa Nguyen
Ngoc Khanh Nguyen
Thi Thu Quyen Nguyen
Hai H. Nguyen
Semyon Novoselov
Julian Nowakowski
Arne Tobias Malkenes Ødegaard
Kazuma Ohara
Miyako Ohkubo
Charles Olivier-Anclin
Eran Omri
Yi Ouyang
Tapas Pal
Ying-yu Pan
Jiaxin Pan
Eugenio Paracucchi
Roberto Parisella
Jeongeun Park
Guillermo Pascual-Perez
Alain Passelègue
Octavio Perez-Kempner
Thomas Peters
Phuong Pham
Cécile Pierrot
Erik Pohle
David Pointcheval
Giacomo Pope
Christopher Portmann
Romain Poussier
Lucas Prabel
Sihang Pu
Chen Qian
Luowen Qian
Tian Qiu
Anaïs Querol
Håvard Raddum
Shahram Rasoolzadeh
Divya Ravi
Prasanna Ravi
Marc Renard
Jan Richter-Brockmann
Lawrence Roy
Paul Rösler
Sayandeep Saha
Yusuke Sakai
Niels Samwel
Paolo Santini
Maria Corte-Real Santos
Sara Sarfaraz
Santanu Sarkar
Or Sattath
Markus Schofnegger
Peter Scholl
Dominique Schröder
André Schrottenloher
Jacob Schuldt
Binanda Sengupta
Srinath Setty
Yantian Shen
Yixin Shen
Ferdinand Sibleyras
Janno Siim
Mark Simkin
Scott Simon
Animesh Singh
Nitin Singh
Sayani Sinha
Daniel Slamanig
Fang Song
Ling Song
Yongsoo Song
Jana Sotakova
Gabriele Spini

Marianna Spyrakou
Lukas Stennes
Marc Stoettinger
Chuanjie Su
Xiangyu Su
Ling Sun
Akira Takahashi
Isobe Takanori
Atsushi Takayasu
Suprita Talnikar
Benjamin Hong Meng Tan
Ertem Nusret Tas
Tadanori Teruya
Masayuki Tezuka
Sri AravindaKrishnan Thyagarajan
Song Tian
Wenlong Tian
Raphael Toledo
Junichi Tomida
Daniel Tschudi
Hikaru Tsuchida
Aleksi Udoenko
Rei Ueno
Barry Van Leeuwen
Wessel van Woerden
Frederik Vercauteren
Sulani Vidhanalage
Benedikt Wagner
Roman Walch
Hendrik Waldner
Han Wang
Luping Wang
Peng Wang
Yuntao Wang
Geng Wang
Shichang Wang
Liping Wang
Jiafan Wang
Zhedong Wang
Kunpeng Wang
Jianfeng Wang
Guilin Wang
Weiqiang Wen
Chenkai Weng
Thom Wiggers
Stella Wohnig
Harry W. H. Wong
Ivy K. Y. Woo
Yu Xia
Zejun Xiang
Yuting Xiao
Zhiye Xie
Yanhong Xu
Jiayu Xu
Lei Xu
Shota Yamada
Kazuki Yamamura
Di Yan
Qianqian Yang
Shaojun Yang
Yanjiang Yang
Li Yao
Yizhou Yao
Kenji Yasunaga
Yuping Ye
Xiuyu Ye
Zeyuan Yin
Kazuki Yoneyama
Yusuke Yoshida
Albert Yu
Quan Yuan
Chen Yuan
Tsz Hon Yuen
Aaram Yun
Riccardo Zanotto
Arantxa Zapico
Shang Zehua
Mark Zhandry
Tianyu Zhang
Zhongyi Zhang
Fan Zhang
Liu Zhang
Yijian Zhang
Shaoxuan Zhang
Zhongliang Zhang
Kai Zhang
Cong Zhang
Jiaheng Zhang
Lulu Zhang
Zhiyu Zhang

Chang-An Zhao
Yongjun Zhao
Chunhuan Zhao
Xiaotong Zhou
Zhelei Zhou

Zijian Zhou
Timo Zijlstra
Jian Zou
Ferdinando Zullo
Cong Zuo

Sponsoring Institutions

- Gold Level Sponsor: Ant Research
- Silver Level Sponsors: Sansec Technology Co., Ltd., Topsec Technologies Group
- Bronze Level Sponsors: IBM, Meta, Sangfor Technologies Inc.

Invited Talks

Lattice-Based Cryptography: From Theory to Practice

Xiaoyun Wang

Institute for Advanced Study, Tsinghua University, Beijing, China

Abstract. Nowadays, post-quantum cryptography (PQC) mainly refers to the public-key cryptosystems built on mathematical hard problems in computational complexity theory, resisting the attacks from imaginary quantum computers. In the last 30 years, substantial contributions have been made in PQC research. Among the PQC families, lattice-based cryptography is popularly regarded as a promising candidate; its security relies on the hardness of computational mathematical problems in lattice theory with high-dimension. In this talk, I will recap the mathematical background of lattice-based cryptography. Then I will introduce the recent progress on the practical designs of lattice-based cryptosystems, as well as a quick look at an amazing area called fully homomorphic encryption (FHE) which has interesting applications in privacy computing and federated learning, etc.

Mathematical Problems Arising from Timing Attacks on Signatures and Their Countermeasures

Mehdi Tibouchi

NTT Social Informatics Laboratories, Japan

Abstract. One of the aspects of cryptology that make it such an exciting field to work in is the great variety of people's backgrounds, and of the reasons that brought them in to begin with. I personally arrived in cryptology looking for interesting mathematical problems to solve. I did find lots of interesting problems, that I mostly could not solve.

Side-channel attacks, and timing attacks in particular, are of course an important challenge to the deployment of real-world cryptographic systems. In this talk, however, I would like to discuss them from the perspective of a mathematical problem solver. Based on several examples from the analysis of signature schemes, I would like to argue that they are, both on the offensive and on the defensive side, a great source of non-trivial yet tractable mathematical problems.

Contents – Part I

Secure Multi-party Computation

Breaking the Size Barrier: Universal Circuits Meet Lookup Tables	3
<i>Yann Disser, Daniel Günther, Thomas Schneider, Maximilian Stillger, Arthur Wigandt, and Hossein Yalame</i>	
Amortized NISC over \mathbb{Z}_{2^k} from RMFE	38
<i>Fuchun Lin, Chaoping Xing, Yizhou Yao, and Chen Yuan</i>	
Two-Round Concurrent 2PC from Sub-exponential LWE	71
<i>Behzad Abdolmaleki, Saikrishna Badrinarayanan, Rex Fernando, Giulio Malavolta, Ahmadreza Rahimi, and Amit Sahai</i>	
Degree- D Reverse Multiplication-Friendly Embeddings: Constructions and Applications	106
<i>Daniel Escudero, Cheng Hong, Hongqing Liu, Chaoping Xing, and Chen Yuan</i>	
Adaptive Distributional Security for Garbling Schemes with $\mathcal{O}(x)$ Online Complexity	139
<i>Estuardo Alpírez Bock, Chris Brzuska, Pihla Karanko, Sabine Oechsner, and Kirthivaasan Puniamurthy</i>	
MPC with Delayed Parties over Star-Like Networks	172
<i>Mariana Gama, Emad Heydari Beni, Emmanuela Orsini, Nigel P. Smart, and Oliver Zajonc</i>	
Ramp Hyper-invertible Matrices and Their Applications to MPC Protocols	204
<i>Hongqing Liu, Chaoping Xing, Yanjiang Yang, and Chen Yuan</i>	
Scalable Multi-party Private Set Union from Multi-query Secret-Shared Private Membership Test	237
<i>Xiang Liu and Ying Gao</i>	
Robust Publicly Verifiable Covert Security: Limited Information Leakage and Guaranteed Correctness with Low Overhead	272
<i>Yi Liu, Junzuo Lai, Qi Wang, Xianrui Qin, Anjia Yang, and Jian Weng</i>	

LERNA: Secure Single-Server Aggregation via Key-Homomorphic Masking	302
<i>Hanjun Li, Huijia Lin, Antigoni Polychroniadou, and Stefano Tessaro</i>	
Unconditionally Secure Multiparty Computation for Symmetric Functions with Low Bottleneck Complexity	335
<i>Reo Eriguchi</i>	
Threshold Cryptography	
Simple Threshold (Fully Homomorphic) Encryption from LWE with Polynomial Modulus	371
<i>Katharina Boudgoust and Peter Scholl</i>	
VSS from Distributed ZK Proofs and Applications	405
<i>Shahla Atapoor, Karim Baghery, Daniele Cozzo, and Robi Pedersen</i>	
Threshold Linear Secret Sharing to the Rescue of MPC-in-the-Head	441
<i>Thibault Feneuil and Matthieu Rivain</i>	
Author Index	475