

Lecture Notes in Computer Science

13940

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.


Alexandra Boldyreva · Vladimir Kolesnikov
Editors

Public-Key Cryptography – PKC 2023

26th IACR International Conference
on Practice and Theory of Public-Key Cryptography
Atlanta, GA, USA, May 7–10, 2023
Proceedings, Part I

Editors

Alexandra Boldyreva
Georgia Institute of Technology
Atlanta, GA, USA

Vladimir Kolesnikov 
Georgia Institute of Technology
Atlanta, GA, USA

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-031-31367-7

ISBN 978-3-031-31368-4 (eBook)

<https://doi.org/10.1007/978-3-031-31368-4>

© 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 Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The 26th International Conference on Practice and Theory of Public-Key Cryptography (PKC 2023) was held in Atlanta, Georgia, USA on May 7–10, 2023. It was sponsored by the International Association for Cryptologic Research (IACR).

The conference received 183 submissions, reviewed by the Program Committee of 49 cryptography experts working with 142 external reviewers. The reviewing process took 2.5 months and resulted in selecting 50 papers to appear in PKC 2023.

Papers were reviewed in the usual double-blind fashion. Program committee members were limited to two submissions, and their submissions were scrutinized more closely. The two program chairs were not allowed to submit papers.

The Program Committee recognized two papers and their authors. “The Hidden Number Problem with Small Unknown Multipliers: Cryptanalyzing MEGA in Six Queries and Other Applications,” by Nadia Heninger and Keegan Ryan, and “Post-Quantum Anonymity of Kyber”, by Varun Maram and Keita Xagawa, were selected Best Papers of the conference.

PKC 2023 welcomed Chris Peikert (University of Michigan) as the invited speaker.

The PKC Test-of-Time Award (ToT) recognizes outstanding and influential papers published in PKC about 15 years prior. The inaugural PKC Test of Time Award was given in PKC 2019 for papers published in the conference’s initial years of the early 2000s and late 1990s. In 2023, the ToT committee, consisting of Alexandra Boldyreva, Goichiro Hanaoka, Vlad Kolesnikov, Moti Yung, and Yuliang Zheng, considered papers published in PKC 2006–2008 for the award. The committee selected the PKC 2008 paper “Unidirectional Chosen-Ciphertext Secure Proxy Re-encryption” by Benoît Libert and Damien Vergnaud for the Test-of-Time award.

PKC is the main IACR-sponsored conference with an explicit focus on public-key cryptography. It is a remarkable undertaking, only possible due to the hard work and significant contributions of many people. We would like to express our sincere gratitude to the authors of all submitted works, as well as to the PC and external reviewers, session chairs and presenters. Additionally, we would like to thank the following people and organizations for helping make PKC 2023 a success:

- Joseph Jaeger and Daniel Genkin – PKC 2023 General Chairs,
- Chris Peikert – invited speaker,
- Kay McKelly and Kevin McCurley – all things technical behind the scenes,
- Ellen Kolesnikova – design of the PKC 2023 logo,
- the team at Springer,
- Georgia Tech Hotel and Conference Center,
- Georgia Aquarium,
- School of Cybersecurity and Privacy at Georgia Tech - the academic home of the PKC 2023 Program and General Chairs.

We would also like to thank our sponsors: Google (platinum), Starkware (silver), Amazon AWS (silver), and Algorand (bronze). 2022 and 2023 were difficult years in the

tech industry, making sponsors' contributions ever more valued. Their generous support covered several student travel stipends and helped minimize registration fees, including half-priced registration for all students.

Lastly, a big thanks to everyone who attended PKC 2023 in Atlanta. We hope you enjoyed the conference and the warm welcome of our city and university.



May 2023

Alexandra Boldyreva
Vlad Kolesnikov

Organization

General Chairs

Daniel Genkin

Georgia Tech, USA

Joseph Jaeger

Georgia Tech, USA

Program Committee Chairs

Alexandra Boldyreva

Georgia Tech, USA

Vladimir Kolesnikov

Georgia Tech, USA

Steering Committee

Masayuki Abe

NTT, Japan

Jung Hee Cheon

Seoul National University, Korea

Yvo Desmedt

University of Texas at Dallas, USA

Goichiro Hanaoka

AIST, Japan

Aggelos Kiayias

University of Edinburgh, UK

Tanja Lange

Eindhoven University of Technology, Netherlands

David Pointcheval

École Normale Supérieure, France

Moti Yung (Secretary)

Google Inc. & Columbia University, USA

Yuliang Zheng (Chair)

University of Alabama at Birmingham, USA

Program Committee

Ghada Almashaqbeh

University of Connecticut, USA

Nuttapong Attrapadung

AIST, Japan

Carlo Blundo

Università degli Studi di Salerno, Italy

Katharina Boudgoust

Aarhus University, Denmark

Dario Catalano

Università di Catania, Italy

Suvradip Chakraborty

ETH Zurich, Switzerland

Shan Chen

Southern University of Science & Technology,
China

Jean Paul Degabriele

Technology Innovation Institute, UAE

Chaya Ganesh

Indian Institute of Science, India

Sean Hallgren	Penn State University, USA
David Heath	University of Illinois Urbana-Champaign, USA
Kristina Hostakova	ETH Zürich, Switzerland
Sorina Ionica	Université de Picardie Jules Verne, France
Stanislaw Jarecki	University of California, Irvine, USA
Shuichi Katsumata	AIST and PQShield Ltd., Japan
Kaoru Kurosawa	AIST, Japan
Tancrède Lepoint	Amazon, USA
Christian Majenz	Technical University of Denmark, Denmark
Daniel Masny	Meta, USA
Ryo Nishimaki	NTT Social Informatics Laboratories, Japan
Adam O'Neill	UMass Amherst, USA
Charalampos Papamanthou	Yale University, USA
Alain Passelègue	Inria and ENS Lyon, France
Sikhar Patranabis	IBM Research India, India
Alice Pellet-Mary	CNRS and Université de Bordeaux, France
Edoardo Persichetti	Florida Atlantic University, USA
Rachel Player	Royal Holloway, University of London, UK
David Pointcheval	ENS, Paris, France
Antigoni Polychroniadou	JPMorgan AI Research, USA
Willy Quach	Northeastern University, USA
Elizabeth Quaglia	Royal Holloway, University of London, UK
Adeline Roux-Langlois	Normandie Univ, GREYC, France
John Schanck	Mozilla, USA
Peter Scholl	Aarhus University, Denmark
Dominique Schröder	FAU Erlangen-Nürnberg, Germany
Peter Schwabe	MPI-SP & Radboud University, Netherlands
Jae Hong Seo	Hanyang University, Korea
Abhi Shelat	Northeastern University, USA
Akira Takahashi	University of Edinburgh, UK
Keisuke Tanaka	Tokyo Institute of Technology, Japan
Jean-Pierre Tillich	Inria, France
Frederik Vercauteren	KU Leuven, Belgium
Damien Vergnaud	Sorbonne Université, France
Ivan Visconti	University of Salerno, Italy
Benjamin Wesolowski	CNRS and University of Bordeaux, France
David Wu	UT Austin, USA
Kevin Ye	Google and Columbia University, USA
Mark Zhandry	NTT Research & Princeton University, USA
Vassilis Zikas	Purdue University, USA

Additional Reviewers

Behzad Abdolmaleki
 Calvin Abou Haidar
 Ojaswi Acharya
 Gorjan Alagic
 Gennaro Avitabile
 Arnab Bag
 Shi Bai
 Magali Bardet
 Hugo Beguinet
 Fabrice Benhamouda
 Loris Bergerat
 Ward Beullens
 Olivier Blazy
 Maxime Bombar
 Cecilia Boschini
 Vincenzo Botta
 Samuel Bouaziz-Ermann
 Charles Bouillaguet
 Nicholas Brandt
 Lennart Braun
 Matteo Campanelli
 André Chailloux
 Rohit Chatterjee
 Jesus-Javier Chi-Dominguez
 Hien Chu
 Heewon Chung
 Michele Ciampi
 Jean-Sébastien Coron
 Anamaria Costache
 Baptiste Cottier
 Jan-Pieter D’Anvers
 Pratish Datta
 Gareth T. Davies
 Paola De Perthuis
 Jean-Christophe Deneuville
 Julien Devevey
 Mario Di Raimondo
 Javad Doliskani
 Keita Emura
 Andreas Erwig
 Daniel Escudero
 Andre Esser
 Pouria Fallahpour

Antonio Faonio
 Joël Felderhoff
 Weiqi Feng
 Rune Fiedler
 Georgios Fotiadis
 Tako Boris Fouotsa
 Georg Fuchsbauer
 Clemente Galdi
 Romain Gay
 Robin Geelen
 Paul Gerhart
 Lenaïck Gouriou
 Mohammad Hajiabadi
 Erin Hales
 Mickaël Hamdad
 Patrick Harasser
 Keitaro Hashimoto
 Sorina Ionica
 Vincenzo Iovino
 Aayush Jain
 Christian Janson
 Corentin Jeudy
 Saqib Kakvi
 Daniel Kales
 Harish Karthikeyan
 Julia Kastner
 Mojtaba Khalili
 Hamidreza Khoshakhlagh
 Ryo Kikuchi
 Dongwoo Kim
 Elena Kirshanova
 Fuyuki Kitagawa
 David Kohel
 Sebastian Kolby
 Walter Krawec
 Mikhail Kudinov
 Péter Kutas
 Roman Langrehr
 Mario Larangeira
 Changmin Lee
 Antonin Leroux
 Andrea Lesavourey
 Varun Madathil

Lorenzo Magliocco
 Jules Maire
 Monosij Maitra
 Takahiro Matsuda
 Liam Medley
 Kelsey Melissaris
 Hart Montgomery
 Ngoc Khanh Nguyen
 Ky Nguyen
 Thi Thu Quyen Nguyen
 Phong Nguyen
 Ruben Niederhagen
 Koji Nuida
 Tapas Pal
 Kunjal Panchal
 Mahak Pancholi
 Lorenz Panny
 Robi Pedersen
 Lucas Prabel
 Thomas Prest
 Sihang Pu
 Krijn Reijnders
 Mahshid Riahinia
 Doreen Riepel
 Felix Rohrbach
 Mélissa Rossi
 Olga Sanina
 Paolo Santini

André Schrottenloher
 Robert Schädlich
 Yixin Shen
 Mark Simkin
 Animesh Singh
 Sayani Sinha
 Luisa Siniscalchi
 Christoph Striecks
 Atsushi Takayasu
 Debadrita Talapatra
 Aravind Thyagarajan
 Junichi Tomida
 Toi Tomita
 Monika Trimoska
 Damien Vidal
 Chenkai Wang
 Yohei Watanabe
 Christian Weinert
 Weiqiang Wen
 Keita Xagawa
 Shota Yamada
 Takashi Yamakawa
 Yibin Yang
 Kazuki Yoneyama
 Yusuke Yoshida
 Bor de Kock
 Rafael del Pino
 Wessel van Woerden

Contents – Part I

Post-quantum Cryptography

Post-quantum Anonymity of Kyber	3
<i>Varun Maram and Keita Xagawa</i>	
QCCA-Secure Generic Transformations in the Quantum Random Oracle Model	36
<i>Tianshu Shan, Jiangxia Ge, and Rui Xue</i>	
A Thorough Treatment of Highly-Efficient NTRU Instantiations	65
<i>Julien Duman, Kathrin Hövelmanns, Eike Kiltz, Vadim Lyubashevsky, Gregor Seiler, and Dominique Unruh</i>	
A Lightweight Identification Protocol Based on Lattices	95
<i>Samed Düzlü, Juliane Krämer, Thomas Pöppelmann, and Patrick Struck</i>	
POLKA: Towards Leakage-Resistant Post-quantum CCA-Secure Public Key Encryption	114
<i>Clément Hoffmann, Benoît Libert, Charles Momin, Thomas Peters, and François-Xavier Standaert</i>	

Attacks

The Hidden Number Problem with Small Unknown Multipliers: Cryptanalyzing MEGA in Six Queries and Other Applications	147
<i>Nadia Heninger and Keegan Ryan</i>	
Hull Attacks on the Lattice Isomorphism Problem	177
<i>Léo Ducas and Shane Gibbons</i>	
A Key-Recovery Attack Against Mitaka in the t -Probing Model	205
<i>Thomas Prest</i>	

Signatures

Hardening Signature Schemes via Derive-then-Derandomize: Stronger Security Proofs for EdDSA	223
<i>Mihir Bellare, Hannah Davis, and Zijing Di</i>	

Security Analysis of RSA-BSSA	251
<i>Anna Lysyanskaya</i>	
Extendable Threshold Ring Signatures with Enhanced Anonymity	281
<i>Gennaro Avitabile, Vincenzo Botta, and Dario Fiore</i>	
Tracing a Linear Subspace: Application to Linearly-Homomorphic Group Signatures	312
<i>Chloé Héban, David Pointcheval, and Robert Schädlich</i>	
Isogenies	
SCALLOP: Scaling the CSI-FiSh	345
<i>Luca De Feo, Tako Boris Fouotsa, Péter Kutas, Antonin Leroux, Simon-Philipp Merz, Lorenz Panny, and Benjamin Wesolowski</i>	
Round-Optimal Oblivious Transfer and MPC from Computational CSIDH	376
<i>Saikrishna Badrinarayanan, Daniel Masny, Pratyay Mukherjee, Sikhar Patranabis, Srinivasan Raghuraman, and Pratik Sarkar</i>	
Generic Models for Group Actions	406
<i>Julien Duman, Dominik Hartmann, Eike Kiltz, Sabrina Kunzweiler, Jonas Lehmann, and Doreen Riepel</i>	
Crypto for Crypto	
CRAFT: Composable Randomness Beacons and Output-Independent Abort MPC From Time	439
<i>Carsten Baum, Bernardo David, Rafael Dowsley, Ravi Kishore, Jesper Buus Nielsen, and Sabine Oechsner</i>	
Efficient and Universally Composable Single Secret Leader Election from Pairings	471
<i>Dario Catalano, Dario Fiore, and Emanuele Giunta</i>	
Simple, Fast, Efficient, and Tightly-Secure Non-malleable Non-interactive Timed Commitments	500
<i>Peter Chvojka and Tibor Jager</i>	
Certifying Giant Nonprimes	530
<i>Charlotte Hoffmann, Pavel Hubáček, Chethan Kamath, and Krzysztof Pietrzak</i>	

Transparent Batchable Time-lock Puzzles and Applications to Byzantine Consensus	554
<i>Shravan Srinivasan, Julian Loss, Giulio Malavolta, Kartik Nayak, Charalampos Papamanthou, and Sri Aravinda Krishnan Thyagarajan</i>	
Pairings	
Decentralized Multi-Authority Attribute-Based Inner-Product FE: Large Universe and Unbounded	587
<i>Pratish Datta and Tapas Pal</i>	
Multi-Client Inner Product Encryption: Function-Hiding Instantiations Without Random Oracles	622
<i>Elaine Shi and Nikhil Vanjani</i>	
GLUE: Generalizing Unbounded Attribute-Based Encryption for Flexible Efficiency Trade-Offs	652
<i>Marloes Venema and Greg Alpar</i>	
Key Exchange and Messaging	
EKE Meets Tight Security in the Universally Composable Framework	685
<i>Xiangyu Liu, Shengli Liu, Shuai Han, and Dawu Gu</i>	
A Universally Composable PAKE with Zero Communication Cost: (And Why It Shouldn't Be Considered UC-Secure)	714
<i>Lawrence Roy and Jiayu Xu</i>	
Sender-binding Key Encapsulation	744
<i>Laurin Benz, Wasilij Beskorovajnov, Sarai Eilebrecht, Jörn Müller-Quade, Astrid Ottenhues, and Rebecca Schwerdt</i>	
Pattern Matching in Encrypted Stream from Inner Product Encryption	774
<i>Élie Bouscaté, Guilhem Castagnos, and Olivier Sanders</i>	
Author Index	803

Contents – Part II

Homomorphic Cryptography and Other Topics

On Homomorphic Secret Sharing from Polynomial-Modulus LWE	3
<i>Thomas Attema, Pedro Capitão, and Lisa Kohl</i>	
Discretization Error Reduction for High Precision Torus Fully Homomorphic Encryption	33
<i>Kang Hoon Lee and Ji Won Yoon</i>	
Verifiable Capacity-Bound Functions: A New Primitive from Kolmogorov Complexity: (Revisiting Space-Based Security in the Adaptive Setting)	63
<i>Giuseppe Ateniese, Long Chen, Danilo Francati, Dimitrios Papadopoulos, and Qiang Tang</i>	
A Holistic Approach Towards Side-Channel Secure Fixed-Weight Polynomial Sampling	94
<i>Markus Krausz, Georg Land, Jan Richter-Brockmann, and Tim Güneysu</i>	

MPC

Private Polynomial Commitments and Applications to MPC	127
<i>Rishabh Bhadauria, Carmit Hazay, Muthuramakrishnan Venkitasubramaniam, Wenxuan Wu, and Yupeng Zhang</i>	
Credibility in Private Set Membership	159
<i>Sanjam Garg, Mohammad Hajiabadi, Abhishek Jain, Zhengzhong Jin, Omkant Pandey, and Sina Shiehian</i>	
Improved Private Set Intersection for Sets with Small Entries	190
<i>Dung Bui and Geoffroy Couteau</i>	
Pseudorandom Correlation Functions from Variable-Density LPN, Revisited	221
<i>Geoffroy Couteau and Clément Ducros</i>	
Threshold Private Set Intersection with Better Communication Complexity	251
<i>Satrajit Ghosh and Mark Simkin</i>	

Encryption

Almost Tightly-Secure Re-randomizable and Replayable CCA-Secure Public Key Encryption	275
<i>Antonio Faonio, Dennis Hofheinz, and Luigi Russo</i>	
Multi-authority ABE for Non-monotonic Access Structures	306
<i>Miguel Ambrona and Romain Gay</i>	
Multi-instance Secure Public-Key Encryption	336
<i>Carlo Brunetta, Hans Heum, and Martijn Stam</i>	
Unidirectional Updatable Encryption and Proxy Re-encryption from DDH	368
<i>Peihan Miao, Sikhar Patranabis, and Gaven Watson</i>	
Backward-Leak Uni-Directional Updatable Encryption from (Homomorphic) Public Key Encryption	399
<i>Yao Jiang Galteland and Jiaxin Pan</i>	
Functional Encryption Against Probabilistic Queries: Definition, Construction and Applications	429
<i>Geng Wang, Shi-Feng Sun, Zhedong Wang, and Dawu Gu</i>	

ZK I

A Generic Transform from Multi-round Interactive Proof to NIZK	461
<i>Pierre-Alain Fouque, Adela Georgescu, Chen Qian, Adeline Roux-Langlois, and Weiqiang Wen</i>	
Fine-Grained Verifier NIZK and Its Applications	482
<i>Xiangyu Liu, Shengli Liu, Shuai Han, and Dawu Gu</i>	
Zero-Knowledge Arguments for Subverted RSA Groups	512
<i>Dimitris Kolonelos, Mary Maller, and Mikhail Volkhov</i>	
Dew: A Transparent Constant-Sized Polynomial Commitment Scheme	542
<i>Arasu Arun, Chaya Ganesh, Satya Lokam, Tushar Mopuri, and Sriram Sridhar</i>	

IO and ZK II

Non-Interactive Publicly-Verifiable Delegation of Committed Programs	575
<i>Riddhi Ghosal, Amit Sahai, and Brent Waters</i>	

Laconic Function Evaluation for Turing Machines	606
<i>Nico Döttling, Phillip Gajland, and Giulio Malavolta</i>	
A Map of Witness Maps: New Definitions and Connections	635
<i>Suvradip Chakraborty, Manoj Prabhakaran, and Daniel Wichs</i>	
Structure-Preserving Compilers from New Notions of Obfuscations	663
<i>Matteo Campanelli, Danilo Francati, and Claudio Orlandi</i>	
Author Index	695