Lecture Notes in Computer Science 13940

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

Springer

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

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 Yeo	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

Attacks

Signatures

Isogenies

Crypto for Crypto

Pairings

Key Exchange and Messaging

Contents – Part II

Homomorphic Cryptography and Other Topics

MPC

Encryption

ZK I

IO and ZK II