Lecture Notes in Computer Science 12107

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

Anne Canteaut · Yuval Ishai (Eds.)

Advances in Cryptology – EUROCRYPT 2020

39th Annual International Conference on the Theory and Applications of Cryptographic Techniques
Zagreb, Croatia, May 10–14, 2020
Proceedings, Part III

Springer

Editors
Anne Canteaut
Équipe-projet COSMIQ
Inria
Paris, France

Yuval Ishai
Computer Science Department
Technion
Haifa, Israel

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-45726-6 ISBN 978-3-030-45727-3 (eBook)
https://doi.org/10.1007/978-3-030-45727-3

LNCS Sublibrary: SL4 – Security and Cryptology

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

Eurocrypt 2020, the 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, was held in Zagreb, Croatia, during May 10–14, 2020.[1] The conference was sponsored by the International Association for Cryptologic Research (IACR). Lejla Batina (Radboud University, The Netherlands) and Stjepan Picek (Delft University of Technology, The Netherlands) were responsible for the local organization. They were supported by a local organizing team consisting of Marin Golub and Domagoj Jakobovic (University of Zagreb, Croatia). Peter Schwabe acted as the affiliated events chair and Simona Samardjiska helped with the promotion and local organization. We are deeply indebted to all of them for their support and smooth collaboration.

The conference program followed the now established parallel-track system where the works of the authors were presented in two concurrently running tracks. The invited talks and the talks presenting the best paper/best young researcher spanned over both tracks.

We received a total of 375 submissions. Each submission was anonymized for the reviewing process and was assigned to at least three of the 57 Program Committee (PC) members. PC members were allowed to submit at most two papers. The reviewing process included a rebuttal round for all submissions. After extensive deliberations the PC accepted 81 papers. The revised versions of these papers are included in these three volume proceedings, organized topically within their respective track.

The PC decided to give the Best Paper Award to the paper "Optimal Broadcast Encryption from Pairings and LWE" by Shweta Agrawal and Shota Yamada and the Best Young Researcher Award to the paper "Private Information Retrieval with Sublinear Online Time" by Henry Corrigan-Gibbs and Dmitry Kogan. Both papers, together with "Candidate iO from Homomorphic Encryption Schemes" by Zvika Brakerski, Nico Döttling, Sanjam Garg, and Giulio Malavolta, received invitations for the *Journal of Cryptology*.

The program also included invited talks by Alon Rosen, titled "Fine-Grained Cryptography: A New Frontier?", and by Alice Silverberg, titled "Mathematics and Cryptography: A Marriage of Convenience?".

We would like to thank all the authors who submitted papers. We know that the PC's decisions can be very disappointing, especially rejections of very good papers which did not find a slot in the sparse number of accepted papers. We sincerely hope that these works eventually get the attention they deserve.

We are also indebted to the members of the PC and all external reviewers for their voluntary work. The PC work is quite a workload. It has been an honor to work with

[1] This preface was written before the conference took place, under the assumption that it will take place as planned in spite of travel restrictions related to the coronavirus.

everyone. The PC's work was simplified by Shai Halevi's submission software and his support, including running the service on IACR servers.

Finally, we thank everyone else – speakers, session chairs, and rump-session chairs – for their contribution to the program of Eurocrypt 2020. We would also like to thank the many sponsors for their generous support, including the Cryptography Research Fund that supported student speakers.

May 2020

Anne Canteaut
Yuval Ishai

Eurocrypt 2020

The 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques

Sponsored by *the International Association for Cryptologic Research (IACR)*

May 10–14, 2020
Zagreb, Croatia

General Co-chairs

Lejla Batina	Radboud University, The Netherlands
Stjepan Picek	Delft University of Technology, The Netherlands

Program Co-chairs

Anne Canteaut	Inria, France
Yuval Ishai	Technion, Israel

Program Committee

Divesh Aggarwal	National University of Singapore, Singapore
Benny Applebaum	Tel Aviv University, Israel
Fabrice Benhamouda	Algorand Foundation, USA
Elette Boyle	IDC Herzliya, Israel
Zvika Brakerski	Weizmann Institute of Science, Israel
Anne Broadbent	University of Ottawa, Canada
Nishanth Chandran	MSR India, India
Yilei Chen	Visa Research, USA
Aloni Cohen	Boston University, USA
Ran Cohen	Boston University and Northeastern University, USA
Geoffroy Couteau	CNRS, IRIF, Université de Paris, France
Joan Daemen	Radboud University, The Netherlands
Luca De Feo	IBM Research Zurich, Switzerland
Léo Ducas	CWI Amsterdam, The Netherlands
Maria Eichlseder	Graz University of Technology, Austria
Thomas Eisenbarth	University of Lübeck and WPI, Germany
Thomas Fuhr	ANSSI, France
Romain Gay	Cornell Tech, USA
Benedikt Gierlichs	KU Leuven, Belgium
Rishab Goyal	UT Austin, USA

Vipul Goyal	Carnegie Mellon University, USA
Tim Güneysu	Ruhr-Universität Bochum and DFKI, Germany
Jian Guo	Nanyang Technological University, Singapore
Mohammad Hajiabadi	UC Berkeley, USA
Carmit Hazay	Bar-Ilan University, Israel
Susan Hohenberger	Johns Hopkins University, USA
Pavel Hubáček	Charles University Prague, Czech Republic
Abhishek Jain	Johns Hopkins University, USA
Marc Joye	Zama, France
Bhavana Kanukurthi	IISc Bangalore, India
Nathan Keller	Bar-Ilan University, Israel
Susumu Kiyoshima	NTT Research, USA
Eyal Kushilevitz	Technion, Israel
Gregor Leander	Ruhr-Universität Bochum, Germany
Tancrède Lepoint	Google, USA
Tal Malkin	Columbia University, USA
Alexander May	Ruhr-Universität Bochum, Germany
Bart Mennink	Radboud University, The Netherlands
Kazuhiko Minematsu	NEC Corporation, Japan
María Naya-Plasencia	Inria, France
Ryo Nishimaki	NTT Secure Platform Laboratories, Japan
Cécile Pierrot	Inria and Université de Lorraine, France
Sondre Rønjom	University of Bergen, Norway
Ron Rothblum	Technion, Israel
Alessandra Scafuro	North Carolina State University, USA
Peter Schwabe	Radboud University, The Netherlands
Adam Smith	Boston University, USA
François-Xavier Standaert	KU Leuven, Belgium
Yosuke Todo	NTT Secure Platform Laboratories, Japan
Gilles Van Assche	STMicroelectronics, Belgium
Prashant Nalini Vasudevan	UC Berkeley, USA
Muthuramakrishnan Venkitasubramaniam	University of Rochester, USA
Frederik Vercauteren	KU Leuven, Belgium
Damien Vergnaud	Sorbonne Université and Institut Universitaire de France, France
Eylon Yogev	Technion, Israel
Yu Yu	Shanghai Jiao Tong University, China
Gilles Zémor	Université de Bordeaux, France

External Reviewers

Aysajan Abidin
Ittai Abraham
Thomas Agrikola
Navid Alamati
Nils Albartus
Martin Albrecht
Ghada Almashaqbeh
Joël Alwen
Miguel Ambrona
Ghous Amjad
Nicolas Aragon
Gilad Asharov
Tomer Ashur
Thomas Attema
Nuttapong Attrapadung
Daniel Augot
Florian Bache
Christian Badertscher
Saikrishna Badrinarayanan
Shi Bai
Josep Balasch
Foteini Baldimtsi
Marshall Ball
Zhenzhen Bao
James Bartusek
Lejla Batina
Enkhtaivan Batnyam
Carsten Baum
Gabrielle Beck
Christof Beierle
Amos Beimel
Sebastian Berndt
Dan J. Bernstein
Francesco Berti
Ward Beullens
Rishabh Bhadauria
Obbattu Sai Lakshmi Bhavana
Jean-Francois Biasse
Begül Bilgin
Nina Bindel
Nir Bitansky
Olivier Blazy
Naresh Boddu
Koen de Boer
Alexandra Boldyreva
Xavier Bonnetain
Carl Bootland
Jonathan Bootle
Adam Bouland
Christina Boura
Tatiana Bradley
Marek Broll
Olivier Bronchain
Ileana Buhan
Mark Bun
Sergiu Bursuc
Benedikt Bünz
Federico Canale
Sébastien Canard
Ran Canetti
Xavier Caruso
Ignacio Cascudo
David Cash
Gaëtan Cassiers
Guilhem Castagnos
Wouter Castryck
Hervé Chabanne
André Chailloux
Avik Chakraborti
Hubert Chan
Melissa Chase
Cong Chen
Hao Chen
Jie Chen
Ming-Shing Chen
Albert Cheu
Jérémy Chotard
Arka Rai Choudhuri
Kai-Min Chung
Michele Ciampi
Benoit Cogliati
Sandro Coretti-Drayton
Jean-Sébastien Coron
Adriana Suarez Corona
Alain Couvreur
Jan-Pieter D'Anvers
Bernardo David
Thomas Decru
Claire Delaplace
Patrick Derbez
Apoorvaa Deshpande
Siemen Dhooghe
Denis Diemert
Itai Dinur
Christoph Dobraunig
Yevgeniy Dodis
Jack Doerner
Jelle Don
Nico Döttling
Benjamin Dowling
John Schank
Markus Duermuth
Orr Dunkelman
Fréderic Dupuis
Iwan Duursma
Sébastien Duval
Stefan Dziembowski
Aner Moshe Ben Efraim
Naomi Ephraim
Thomas Espitau
Andre Esser
Brett Hemenway Falk
Antonio Faonio
Serge Fehr
Patrick Felke
Rex Fernando
Dario Fiore
Ben Fisch
Marc Fischlin
Nils Fleischhacker
Cody Freitag
Benjamin Fuller
Ariel Gabizon
Philippe Gaborit
Steven Galbraith
Chaya Ganesh
Juan Garay

Rachit Garg
Pierrick Gaudry
Nicholas Genise
Essam Ghadafi
Satrajit Ghosh
Kristian Gjøsteen
Aarushi Goel
Junqing Gong
Alonso Gonzalez
Lorenzo Grassi
Jens Groth
Aurore Guillevic
Berk Gulmezoglu
Aldo Gunsing
Chun Guo
Qian Guo
Siyao Guo
Shai Halevi
Shuai Han
Abida Haque
Phil Hebborn
Brett Hemenway
Shoichi Hirose
Dennis Hofheinz
Justin Holmgren
Akinori Hosoyamada
Senyang Huang
Paul Huynh
Kathrin Hövelmanns
Andreas Hülsing
Ilia Iliashenko
Laurent Imbert
Takanori Isobe
Tetsu Iwata
Håkon Jacobsen
Tibor Jager
Aayush Jain
Samuel Jaques
Jéremy Jean
Yanxue Jia
Zhengzhong Jin
Thomas Johansson
Kimmo Järvinen
Saqib Kakvi
Daniel Kales
Seny Kamara
Gabe Kaptchuk
Martti Karvonen
Shuichi Katsumata
Raza Ali Kazmi
Florian Kerschbaum
Dakshita Khurana
Jean Kieffer
Ryo Kikuchi
Eike Kiltz
Sam Kim
Elena Kirshanova
Fuyuki Kitagawa
Dima Kogan
Lisa Kohl
Markulf Kohlweiss
Ilan Komargodski
Yashvanth Kondi
Venkata Koppula
Lucas Kowalczyk
Karel Kral
Ralf Kuesters
Ashutosh Kumar
Ranjit Kumaresan
Srijita Kundu
Peter Kutasp
Thijs Laarhoven
Gijs Van Laer
Russell Lai
Virginie Lallemand
Baptiste Lambin
Julien Lavauzelle
Phi Hung Le
Eysa Lee
Hyung Tae Lee
Jooyoung Lee
Antonin Leroux
Gaëtan Leurent
Xin Li
Xiao Liang
Chengyu Lin
Huijia (Rachel) Lin
Wei-Kai Lin
Eik List
Guozhen Liu
Jiahui Liu
Qipeng Liu
Shengli Liu
Tianren Liu
Pierre Loidreau
Alex Lombardi
Patrick Longa
Sébastien Lord
Julian Loss
George Lu
Atul Luykx
Vadim Lyubashevsky
Fermi Ma
Varun Madathil
Roel Maes
Bernardo Magri
Saeed Mahloujifar
Christian Majenz
Eleftheria Makri
Giulio Malavolta
Mary Maller
Alex Malozemoff
Nathan Manohar
Daniel Masny
Simon Masson
Takahiro Matsuda
Noam Mazor
Audra McMillan
Lauren De Meyer
Peihan Miao
Gabrielle De Micheli
Ian Miers
Brice Minaud
Pratyush Mishra
Ahmad Moghimi
Esfandiar Mohammadi
Victor Mollimard
Amir Moradi
Tal Moran
Andrew Morgan
Mathilde de la Morinerie
Nicky Mouha
Tamer Mour
Pratyay Mukherjee
Marta Mularczyk
Koksal Mus
Pierrick Méaux
Jörn Müller-Quade

Yusuke Naito
Mridul Nandi
Samuel Neves
Ngoc Khanh Nguyen
Anca Nitulescu
Ariel Nof
Sai Lakshmi Bhavana Obbattu
Maciej Obremski
Tobias Oder
Frédérique Oggier
Miyako Ohkubo
Mateus de Oliveira Oliveira
Tron Omland
Maximilian Orlt
Michele Orrù
Emmanuela Orsini
Morten Øygarden
Ferruh Ozbudak
Carles Padro
Aurel Page
Jiaxin Pan
Omer Paneth
Lorenz Panny
Anat Paskin-Cherniavsky
Alain Passelègue
Sikhar Patranabis
Michaël Peeters
Chris Peikert
Alice Pellet-Mary
Olivier Pereira
Léo Perrin
Edoardo Persichetti
Thomas Peters
George Petrides
Thi Minh Phuong Pham
Duong-Hieu Phan
Krzysztof Pietrzak
Oxana Poburinnaya
Supartha Podder
Bertram Poettering
Antigoni Polychroniadou
Claudius Pott
Bart Preneel
Robert Primas
Luowen Qian
Willy Quach
Ahmadreza Rahimi
Somindu Ramannai
Matthieu Rambaud
Hugues Randriam
Shahram Rasoolzadeh
Divya Ravi
Mariana P. Raykova
Christian Rechberger
Ling Ren
Joost Renes
Leonid Reyzin
Joao Ribeiro
Silas Richelson
Peter Rindal
Francisco Rodríguez-Henríquez
Schuyler Rosefield
Mélissa Rossi
Mike Rosulek
Dragos Rotaru
Lior Rotem
Arnab Roy
Paul Rösler
Reihaneh Safavi-Naini
Amin Sakzad
Simona Samardjiska
Antonio Sanso
Yu Sasaki
Pascal Sasdrich
Or Sattath
John Schanck
Sarah Scheffler
Tobias Schneider
Markus Schofnegger
Peter Scholl
Jan Schoone
André Schrottenloher
Sven Schäge
Adam Sealfon
Jean-Pierre Seifert
Gregor Seiler
Sruthi Sekar
Okan Seker
Karn Seth
Yannick Seurin
Ido Shahaf
Ronen Shaltiel
Barak Shani
Sina Shiehian
Omri Shmueli
Jad Silbak
Thierry Simon
Luisa Sinischalchi
Veronika Slivova
Benjamin Smith
Yifan Song
Pratik Soni
Jessica Sorrell
Nicholas Spooner
Akshayaram Srinivasan
Damien Stehlé
Ron Steinfeld
Noah Stephens-Davidowitz
Martin Strand
Shifeng Sun
Ridwan Syed
Katsuyuki Takashima
Titouan Tanguy
Stefano Tessaro
Enrico Thomae
Jean-Pierre Tillich
Benjamin Timon
Junichi Tomida
Deniz Toz
Rotem Tsabary
Daniel Tschudi
Yiannis Tselekounis
Yi Tu
Dominique Unruh
Bogdan Ursu
Vinod Vaikuntanathan
Kerem Varici
Philip Vejre
Marloes Venema
Daniele Venturi
Fernando Virdia
Vanessa Vitse
Damian Vizár
Chrysoula Vlachou

Mikhail Volkhov
Satyanarayana Vusirikala
Hendrik Waldner
Alexandre Wallet
Michael Walter
Haoyang Wang
Meiqin Wang
Weijia Wang
Xiao Wang
Yohei Watanabe
Hoeteck Wee
Mor Weiss
Weiqiang Wen
Benjamin Wesolowski
Jan Wichelmann
Daniel Wichs
Friedrich Wiemer
Christopher Williamson
Jonas Wloka
Wessel van Woerden
Lennert Wouters
David J. Wu
Shai Wyborski
Brecht Wyseur
Keita Xagawa
Xiang Xie
Chaoping Xing
Sophia Yakoubov
Shota Yamada
Takashi Yamakawa
Avishay Yanai
Kang Yang
Kevin Yeo
Arkady Yerukhimovich
Øyvind Ytrehus
Aaram Yun
Mohammad Zaheri
Mark Zhandry
Jiayu Zhang
Liangfeng Zhang
Ren Zhang
Zhenfei Zhang
Zhongxiang Zheng
Hong-Sheng Zhou
Vassilis Zikas
Giorgos Zirdelis
Vincent Zucca

Contents – Part III