

Orr Dunkelman
Stefan Dziembowski (Eds.)

LNCS 13276

Advances in Cryptology – EUROCRYPT 2022

41st Annual International Conference on the Theory
and Applications of Cryptographic Techniques
Trondheim, Norway, May 30 – June 3, 2022, Proceedings, Part II

2
Part II



 Springer

Founding Editors

Gerhard Goos

Karlsruhe Institute of Technology, Karlsruhe, Germany

Juris Hartmanis

Cornell University, Ithaca, NY, USA

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


More information about this series at <https://link.springer.com/bookseries/558>


Orr Dunkelman · Stefan Dziembowski (Eds.)

Advances in Cryptology – EUROCRYPT 2022

41st Annual International Conference on the Theory
and Applications of Cryptographic Techniques
Trondheim, Norway, May 30 – June 3, 2022
Proceedings, Part II

Editors

Orr Dunkelman 
University of Haifa
Haifa, Haifa, Israel

Stefan Dziembowski 
University of Warsaw
Warsaw, Poland

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-031-07084-6

ISBN 978-3-031-07085-3 (eBook)

<https://doi.org/10.1007/978-3-031-07085-3>

© International Association for Cryptologic Research 2022, corrected publication 2022

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 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Eurocrypt 2022, was held in Trondheim, Norway. Breaking tradition, the conference started on the evening of Monday, May 30, and ended at noon on Friday, June 3, 2022. Eurocrypt is one of the three flagship conferences of the International Association for Cryptologic Research (IACR), which sponsors the event. Colin Boyd (NTNU, Norway) was the general chair of Eurocrypt 2022 who took care of all the local arrangements.

The 372 anonymous submissions we received in the IACR HotCRP system were each reviewed by at least three of the 70 Program Committee members (who were allowed at most two submissions). We used a rebuttal round for all submissions. After a lengthy and thorough review process, 85 submissions were selected for publication. The revised versions of these submissions can be found in these three-volume proceedings.

In addition to these papers, the committee selected the “EpiGRAM: Practical Garbled RAM” by David Heath, Vladimir Kolesnikov, and Rafail Ostrovsky for the best paper award. Two more papers — “On Building Fine-Grained One-Way Functions from Strong Average-Case Hardness” and “Quantum Algorithms for Variants of Average-Case Lattice Problems via Filtering” received an invitation to the Journal of Cryptology. Together with presentations of the 85 accepted papers, the program included two invited talks: The IACR distinguished lecture, carried by Ingrid Verbauwhede, on “Hardware: an essential partner to cryptography”, and “Symmetric Cryptography for Long Term Security” by María Naya-Plasencia.

We would like to take this opportunity to thank numerous people. First of all, the authors of all submitted papers, whether they were accepted or rejected. The Program Committee members who read, commented, and debated the papers generating more than 4,500 comments(!) in addition to a large volume of email communications. The review process also relied on 368 subreviewers (some of which submitted more than one subreview). We cannot thank you all enough for your hard work.

A few individuals were extremely helpful in running the review process. First and foremost, Kevin McCurley, who configured, solved, answered, re-answered, supported, and did all in his (great) power to help with the IACR system. Wkdqn Brx! We are also extremely grateful to Gaëtan Leurent for offering his wonderful tool to make paper assignment an easy task. The wisdom and experience dispensed by Anne Canteaut, Itai Dinur, Bart Preneel, and François-Xavier Standaert are also noteworthy and helped usher the conference into a safe haven. Finally, we wish to thank the area chairs—Sonia Belaïd, Carmit Hazay, Thomas Peyrin, Nigel Smart, and Martijn Stam. You made our work manageable.

Finally, we thank all the people who were involved in the program of Eurocrypt 2022: the rump session chairs, the session chairs, the speakers, and all the technical support staff in Trondheim. We would also like to mention the various sponsors and thank them

for the generous support. We wish to thank the continuous support of the Cryptography Research Fund for supporting student speakers.

May 2022

Orr Dunkelman
Stefan Dziembowski

Organization

The 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt 2022)

Sponsored by the *International Association for Cryptologic Research*
Trondheim, Norway
May 30 – June 3, 2022

General Chair

Colin Boyd NTNU, Norway

Program Chairs

Orr Dunkelman University of Haifa, Israel
Stefan Dziembowski University of Warsaw, Poland

Program Committee

Masayuki Abe	NTT Laboratories, Japan
Shashank Agrawal	Western Digital Research, USA
Joël Alwen	AWS Wickr, Austria
Marshall Ball	New York University, USA
Gustavo Banegas	Inria and Institut Polytechnique de Paris, France
Paulo Barreto	University of Washington Tacoma, USA
Sonia Belaïd	CryptoExperts, France
Jean-François Biasse	University of South Florida, USA
Begül Bilgin	Rambus Cryptography Research, The Netherlands
Alex Biryukov	University of Luxembourg, Luxembourg
Olivier Blazy	Ecole Polytechnique, France
Billy Bob Brumley	Tampere University, Finland
Chitchanok Chuengsatiansup	University of Adelaide, Australia
Michele Ciampi	University of Edinburgh, UK
Ran Cohen	IDC Herzliya, Israel
Henry Corrigan-Gibbs	Massachusetts Institute of Technology, USA
Cas Cremers	CISPA Helmholtz Center for Information Security, Germany
Dana Dachman-Soled	University of Maryland, USA
Jean Paul Degabriele	TU Darmstadt, Germany
Itai Dinur	Ben-Gurion University, Israel

Rafael Dowsley	Monash University, Australia
Antonio Faonio	EURECOM, France
Pooya Farshim	Durham University, UK
Sebastian Faust	TU Darmstadt, Germany
Ben Fuller	University of Connecticut, USA
Pierrick Gaudry	Loria, France
Esha Ghosh	Microsoft Research, Redmond, USA
Paul Grubbs	University of Michigan, USA
Divya Gupta	Microsoft Research India, India
Felix Günther	ETH Zurich, Switzerland
Iftach Haitner	Tel Aviv University, Israel
Shai Halevi	Algorand Foundation, USA
Carmit Hazay	Bar-Ilan University, Israel
Pavel Hubáček	Charles University, Czech Republic
Tibor Jager	University of Wuppertal, Germany
Dmitry Khovratovich	Ethereum Foundation, Luxembourg
Gregor Leander	Ruhr University Bochum, Germany
Gaëtan Leurent	Inria, France
Helger Lipmaa	Simula UiB, Norway
Shengli Liu	Shanghai Jiao Tong University, China
Alex Lombardi	Massachusetts Institute of Technology, USA
Hemanta K. Maji	Purdue University, USA
Giulio Malavolta	Max Planck Institute for Security and Privacy, Germany
Peihan Miao	University of Illinois at Chicago, USA
Pratyay Mukherjee	Visa Research, USA
David Naccache	ENS Paris, France
Svetla Nikova	KU Leuven, Belgium
Miyako Ohkubo	National Institute of Information and Communications, Japan
Arpita Patra	Indian Institute of Science, India
Alice Pellet-Mary	CNRS and University of Bordeaux, France
Thomas Peyrin	Nanyang Technological University, Singapore
Josef Pieprzyk	CSIRO Data61, Australia, and Institute of Computer Science, PAS, Poland
Bertram Poettering	IBM Research Europe - Zurich, Switzerland
Peter Rindal	Visa Research, USA
Carla Ràfols	Universitat Pompeu Fabra, Spain
Amin Sakzad	Monash University, Australia
Alessandra Scafuro	North Carolina State University, USA
Nigel Smart	KU Leuven, Belgium
Martijn Stam	Simula UiB, Norway

Meltem Sönmez Turan	National Institute of Standards and Technology, USA
Daniele Venturi	Sapienza University of Rome, Italy
Ivan Visconti	University of Salerno, Italy
Gaoli Wang	East China Normal University, China
Stefan Wolf	University of Italian Switzerland, Switzerland
Sophia Yakoubov	Aarhus University, Denmark
Avishay Yanai	VMware Research, Israel
Bo-Yin Yang	Academia Sinica, Taiwan
Arkady Yerukhimovich	George Washington University, USA
Yu Yu	Shanghai Jiao Tong University, China
Mark Zhandry	NTT Research and Princeton University, USA

Subreviewers

Behzad Abdolmaleki	Christof Beierle
Ittai Abraham	Pascal Bemmam
Damiano Abram	Fabrice Benhamouda
Anasuya Acharya	Francesco Berti
Alexandre Adomnicai	Tim Beyne
Amit Agarwal	Rishabh Bhadauria
Shweta Agrawal	Adithya Bhat
Thomas Agrikola	Sai Lakshmi Bhavana Obbattu
Akshima	Alexander Bienstock
Navid Alapati	Erica Blum
Alejandro Cabrera Aldaya	Jan Bobolz
Bar Alon	Xavier Bonnetain
Miguel Ambrona	Cecilia Boschini
Hiroaki Anada	Raphael Bost
Diego F. Aranha	Vincenzo Botta
Victor Arribas	Katharina Boudgoust
Tomer Ashur	Christina Boura
Gennaro Avitabile	Zvika Brakerski
Matilda Backendal	Luís Brandão
Saikrishna Badrinarayanan	Lennart Braun
Shi Bai	Jacqueline Brendel
Ero Balsa	Gianluca Brian
Augustin Bariant	Anne Broadbent
James Bartusek	Marek Broll
Balthazar Bauer	Christopher Brzuska
Carsten Baum	Chloe Cachet
Ämin Baumeler	Matteo Campanelli
Arthur Beckers	Federico Canale
Charles Bédard	Anne Canteaut

Ignacio Cascudo
 Andre Chailloux
 Nishanth Chandran
 Donghoon Chang
 Binyi Chen
 Shan Chen
 Weikeng Chen
 Yilei Chen
 Jung Hee Cheon
 Jesus-Javier Chi-Dominguez
 Seung Geol Choi
 Wutichai Chongchitmate
 Arka Rai Choudhuri
 Sherman S. M. Chow
 Jeremy Clark
 Xavier Coiteux-Roy
 Andrea Coladangelo
 Nan Cui
 Benjamin R. Curtis
 Jan Czajkowski
 Jan-Pieter D'Anvers
 Hila Dahari
 Thinh Dang
 Quang Dao
 Poulami Das
 Pratish Datta
 Bernardo David
 Gareth T. Davies
 Hannah Davis
 Lauren De Meyer
 Gabrielle De Micheli
 Elke De Mulder
 Luke Demarest
 Julien Devevey
 Siemen Dhooghe
 Denis Diemert
 Jintai Ding
 Jack Doerner
 Xiaoyang Dong
 Nico Döttling
 Benjamin Dowling
 Yang Du
 Leo Ducas
 Julien Duman
 Betul Durak

Oğuzhan Ersoy
 Andreas Erwig
 Daniel Escudero
 Muhammed F. Esgin
 Saba Eskandarian
 Prastudy Fauzi
 Patrick Felke
 Thibauld Feneuil
 Peter Fenteany
 Diodato Ferraioli
 Marc Fischlin
 Nils Fleischhacker
 Cody Freitag
 Daniele Friolo
 Tommaso Gagliardoni
 Steven D. Galbraith
 Pierre Galissant
 Chaya Ganesh
 Cesar Pereida García
 Romain Gay
 Kai Gellert
 Craig Gentry
 Marilyn George
 Hossein Ghodosi
 Satrajit Ghosh
 Jan Gilcher
 Aarushi Goel
 Eli Goldin
 Junqing Gong
 Dov Gordon
 Jérôme Govinden
 Lorenzo Grassi
 Johann Großschädl
 Jiaxin Guan
 Daniel Guenther
 Milos Gujic
 Qian Guo
 Cyril Guyot
 Mohammad Hajiabadi
 Ariel Hamlin
 Shuai Han
 Abida Haque
 Patrick Harasser
 Dominik Hartmann
 Phil Hebborn

Alexandra Henzinger
Javier Herranz
Julia Hesse
Justin Holmgren
Akinori Hosoyamada
Kai Hu
Andreas Hülsing
Shih-Han Hung
Vincenzo Iovino
Joseph Jaeger
Aayush Jain
Christian Janson
Samuel Jaques
Stanislaw Jarecki
Corentin Jeudy
Zhengzhong Jin
Daniel Jost
Saqib Kakvi
Vukašin Karadžić
Angshuman Karmakar
Shuichi Katsumata
Jonathan Katz
Mahimna Kelkar
Nathan Keller
John Kelsey
Mustafa Khairallah
Hamidreza Amini Khorasgani
Dongwoo Kim
Miran Kim
Elena Kirshanova
Fuyuki Kitagawa
Michael Kloob
Sebastian Kolby
Lukas Kölsch
Yashvanth Kondi
David Kretzler
Veronika Kuchta
Marie-Sarah Lacharité
Yi-Fu Lai
Baptiste Lambin
Mario Larangeira
Rio LaVigne
Quoc-Huy Le
Jooyoung Lee
Julia Len
Antonin Leroux
Hanjun Li
Jianwei Li
Yiming Li
Xiao Liang
Damien Ligier
Chengyu Lin
Dongxi Liu
Jiahui Liu
Linsheng Liu
Qipeng Liu
Xiangyu Liu
Chen-Da Liu Zhang
Julian Loss
Vadim Lyubashevsky
Lin Lyu
You Lyu
Fermi Ma
Varun Madathil
Akash Madhusudan
Bernardo Magri
Monosij Maitra
Nikolaos Makriyannis
Mary Maller
Giorgia Marson
Christian Matt
Noam Mazor
Nikolas Melissaris
Bart Mennink
Antonis Michalas
Brice Minaud
Kazuhiko Minematsu
Alberto Montina
Amir Moradi
Marta Mularczyk
Varun Narayanan
Jade Nardi
Patrick Neumann
Ruth Ng
Hai H. Nguyen
Kirill Nikitin
Ryo Nishimaki
Anca Nitulescu
Ariel Nof
Julian Nowakowski

Adam O'Neill
Maciej Obremski
Eran Omri
Maximilian Orlt
Bijeeta Pal
Jiaxin Pan
Omer Paneth
Lorenz Panny
Dimitrios Papadopoulos
Jongeun Park
Anat Paskin-Cherniavsky
Sikhar Patranabis
Marcin Pawłowski
Hilder Pereira
Ray Perlner
Clara Pernot
Léo Perrin
Giuseppe Persiano
Edoardo Persichetti
Albrecht Petzoldt
Duong Hieu Phan
Krzysztof Pietrzak
Jeroen Pijnenburg
Rachel Player
Antigoni Polychroniadou
Willy Quach
Anaïs Querol
Srinivasan Raghuraman
Adrián Ranea
Simon Rastikian
Divya Ravi
Francesco Regazzoni
Maryam Rezapour
Mir Ali Rezazadeh Bae
Siavash Riahi
Joao Ribeiro
Vincent Rijmen
Bhaskar Roberts
Francisco Rodriguez-Henríquez
Paul Rösler
Arnab Roy
Iftekhar Salam
Paolo Santini
Roosbeh Sarenche
Yu Sasaki

Matteo Scarlata
Tobias Schmalz
Mahdi Sedaghat
Vladimir Sedlacek
Nicolas Sendrier
Jae Hong Seo
Srinath Setty
Yaobin Shen
Sina Shiehian
Omri Shmueli
Janno Siim
Jad Silbak
Leonie Simpson
Rohit Sinha
Daniel Slamang
Fang Song
Yongsoo Song
Damien Stehle
Ron Steinfeld
Noah Stephens-Davidowitz
Christoph Striecks
Fatih Sulak
Chao Sun
Ling Sun
Siwei Sun
Koutarou Suzuki
Katsuyuki Takashima
Hervé Tale Kalachi
Quan Quan Tan
Yi Tang
Je Sen Teh
Cihangir Tezcan
Aishwarya Thiruvengadam
Orfeas Thyfronitis
Mehdi Tibouchi
Ni Trieu
Yiannis Tselekounis
Michael Tunstall
Nicola Tuveri
Nirvan Tyagi
Sohaib ul Hassan
Wessel van Woerden
Kerem Varc
Prashant Vasudevan
Damien Vergnaud

Jorge L. Villar
Giuseppe Vitto
Sameer Wagh
Hendrik Waldner
Alexandre Wallet
Ming Wan
Xiao Wang
Yuyu Wang
Zhedong Wang
Hoeteck Wee
Mor Weiss
Weiqiang Wen
Daniel Wichs
Mathias Wolf
Lennert Wouters
Michał Wroński
David Wu
Yusai Wu
Keita Xagawa
Yu Xia

Zejun Xiang
Tiancheng Xie
Shota Yamada
Takashi Yamakawa
Lisa Yang
Kevin Yeo
Eylon Yogev
Kazuki Yoneyama
Yusuke Yoshida
William Youmans
Alexandros Zacharakis
Michał Zając
Arantxa Zapico
Greg Zaverucha
Shang Zehua
Tina Zhang
Wentao Zhang
Yinuo Zhang
Yu Zhou
Cong Zuo

Contents – Part II

Cryptographic Protocols

Single-Server Private Information Retrieval with Sublinear Amortized Time ...	3
<i>Henry Corrigan-Gibbs, Alexandra Henzinger, and Dmitry Kogan</i>	
Anamorphic Encryption: Private Communication Against a Dictator	34
<i>Giuseppe Persiano, Duong Hieu Phan, and Moti Yung</i>	
A PCP Theorem for Interactive Proofs and Applications	64
<i>Gal Arnon, Alessandro Chiesa, and Eylon Yogev</i>	
Group Signatures and More from Isogenies and Lattices: Generic, Simple, and Efficient	95
<i>Ward Beullens, Samuel Dobson, Shuichi Katsumata, Yi-Fu Lai, and Federico Pintore</i>	
Asymmetric PAKE with Low Computation <i>and</i> communication	127
<i>Bruno Freitas Dos Santos, Yanqi Gu, Stanislaw Jarecki, and Hugo Krawczyk</i>	
Batch-OT with Optimal Rate	157
<i>Zvika Brakerski, Pedro Branco, Nico Döttling, and Sihang Pu</i>	
Adaptively Secure Computation for RAM Programs	187
<i>Laasya Bangalore, Rafail Ostrovsky, Oxana Poburinnaya, and Muthuramakrishnan Venkatasubramanian</i>	
Optimal Broadcast Encryption and CP-ABE from Evasive Lattice Assumptions	217
<i>Hoeteck Wee</i>	
Embedding the UC Model into the IITM Model	242
<i>Daniel Rausch, Ralf Küsters, and Céline Chevalier</i>	
Zero-Knowledge Proofs	
Zero-Knowledge IOPs with Linear-Time Prover and Polylogarithmic-Time Verifier	275
<i>Jonathan Bootle, Alessandro Chiesa, and Siqi Liu</i>	

Non-Interactive Zero-Knowledge Proofs with Fine-Grained Security	305
<i>Yuyu Wang and Jiaxin Pan</i>	
On Succinct Non-interactive Arguments in Relativized Worlds	336
<i>Megan Chen, Alessandro Chiesa, and Nicholas Spooner</i>	
Families of SNARK-Friendly 2-Chains of Elliptic Curves	367
<i>Youssef El Housni and Aurore Guillevic</i>	
Fiat–Shamir Bulletproofs are Non-Malleable (in the Algebraic Group Model)	397
<i>Chaya Ganesh, Claudio Orlandi, Mahak Pancholi, Akira Takahashi, and Daniel Tschudi</i>	
Gemini: Elastic SNARKs for Diverse Environments	427
<i>Jonathan Bootle, Alessandro Chiesa, Yuncong Hu, and Michele Orrù</i>	
Stacking Sigmas: A Framework to Compose Σ -Protocols for Disjunctions	458
<i>Aarushi Goel, Matthew Green, Mathias Hall-Andersen, and Gabriel Kaptchuk</i>	
One-Shot Fiat-Shamir-Based NIZK Arguments of Composite Residuosity and Logarithmic-Size Ring Signatures in the Standard Model	488
<i>Benôit Libert, Khoa Nguyen, Thomas Peters, and Moti Yung</i>	
SNARGs for P from Sub-exponential DDH and QR	520
<i>James Hulett, Ruta Jawale, Dakshita Khurana, and Akshayaram Srinivasan</i>	
Cryptographic Primitives	
Optimal Tightness for Chain-Based Unique Signatures	553
<i>Fuchun Guo and Willy Susilo</i>	
On Building Fine-Grained One-Way Functions from Strong Average-Case Hardness	584
<i>Chris Brzuska and Geoffroy Couteau</i>	
On the Multi-user Security of Short Schnorr Signatures with Preprocessing	614
<i>Jeremiah Blocki and Seunghoon Lee</i>	
Multi-Designated Receiver Signed Public Key Encryption	644
<i>Ueli Maurer, Christopher Portmann, and Guilherme Rito</i>	

A Fast and Simple Partially Oblivious PRF, with Applications 674
*Nirvan Tyagi, Sofia Celi, Thomas Ristenpart, Nick Sullivan,
Stefano Tessaro, and Christopher A. Wood*

Hiding in Plain Sight: Memory-Tight Proofs via Randomness Programming ... 706
Ashruijit Ghoshal, Riddhi Ghosal, Joseph Jaeger, and Stefano Tessaro

Dynamic Collusion Bounded Functional Encryption from Identity-Based Encryption 736
Rachit Garg, Rishab Goyal, George Lu, and Brent Waters

Property-Preserving Hash Functions for Hamming Distance from Standard Assumptions 764
Nils Fleischhacker, Kasper Green Larsen, and Mark Simkin

Short Pairing-Free Blind Signatures with Exponential Security 782
Stefano Tessaro and Chenzhi Zhu

Real-World Systems

CoCoA: Concurrent Continuous Group Key Agreement 815
*Joël Alwen, Benedikt Auerbach, Miguel Cueto Noval, Karen Klein,
Guillermo Pascual-Perez, Krzysztof Pietrzak, and Michael Walter*

Efficient Schemes for Committing Authenticated Encryption 845
Mihir Bellare and Viet Tung Hoang

On the Concrete Security of TLS 1.3 PSK Mode 876
Hannah Davis, Denis Diemert, Felix Günther, and Tibor Jager

Correction to: Non-Interactive Zero-Knowledge Proofs with Fine-Grained Security C1
Yuyu Wang and Jiaxin Pan

Author Index 907