

## 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*

Gerhard Woeginger 

*RWTH Aachen, Aachen, Germany*

Moti Yung

*Columbia University, New York, NY, USA*

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

Tal Malkin · Chris Peikert (Eds.)

# Advances in Cryptology – CRYPTO 2021

41st Annual International Cryptology Conference, CRYPTO 2021  
Virtual Event, August 16–20, 2021  
Proceedings, Part I

*Editors*

Tal Malkin   
Columbia University  
New York City, NY, USA

Chris Peikert   
University of Michigan  
Ann Arbor, MI, USA

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-030-84241-3              ISBN 978-3-030-84242-0 (eBook)  
<https://doi.org/10.1007/978-3-030-84242-0>

LNCS Sublibrary: SL4 – Security and Cryptology

© International Association for Cryptologic Research 2021

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 International Cryptology Conference (Crypto 2021), sponsored by the International Association of Cryptologic Research (IACR), was held during August 16–20, 2021. Due to the ongoing COVID-19 pandemic, and for the second consecutive year, Crypto was held as an online-only virtual conference, instead of at its usual venue of the University of California, Santa Barbara. In addition, six affiliated workshop events took place during the days immediately prior to the conference.

The Crypto conference continues its substantial growth pattern: this year’s offering received a record-high 430 submissions for consideration, of which 103 (also a record) were accepted to appear in the program. The two program chairs were not allowed to submit a paper, and Program Committee (PC) members were limited to two submissions each. Review and extensive discussion occurred from late February through mid-May, in a double-blind, two-stage process that included an author rebuttal phase (following the initial reviews) and extensive discussion by reviewers. We thank the 58-person PC and the 390 external reviewers for their efforts to ensure that, during the continuing COVID-19 pandemic and unusual work and life circumstances, we nevertheless were able to perform a high-quality review process.

The PC selected four papers to receive recognition via awards, along with invitations to the Journal of Cryptology, via a voting-based process that took into account conflicts of interest (the program chairs did not vote).

- The Best Paper Award went to “On the Possibility of Basing Cryptography on  $\text{EXP} \neq \text{BPP}$ ” by Yanyi Liu and Rafael Pass.
- The Best Paper by Early Career Researchers Award, along with an Honorable Mention for Best Paper, went to “Linear Cryptanalysis of FF3-1 and FEA” by Tim Beyne.
- Honorable Mentions for Best Paper also went to “Efficient Key Recovery for all HFE Signature Variants” by Chengdong Tao, Albrecht Petzoldt, and Jintai Ding; and “Three Halves Make a Whole? Beating the Half-Gates Lower Bound for Garbled Circuits” by Mike Rosulek and Lawrence Roy.

In addition to the regular program, Crypto 2021 included two invited talks, by Vanessa Teague on “Which e-voting problems do we need to solve?” and Jens Groth on “A world of SNARKs.” The conference also carried forward the long-standing tradition of having a rump session, organized in a virtual format.

The chairs would also like to thank the many other people whose hard work helped ensure that Crypto 2021 was a success:

- Vladimir Kolesnikov (Georgia Institute of Technology)—Crypto 2021 general chair.
- Daniele Micciancio (University of California, San Diego), Thomas Ristenpart (Cornell Tech), Yevgeniy Dodis (New York University), and Thomas Shrimpton (University of Florida)—Crypto 2021 Advisory Committee.

- Carmit Hazay (Bar Ilan University)—Crypto 2021 workshop chair.
- Bertram Poettering and Antigoni Polychroniadou—Crypto 2021 rump session chairs.
- Kevin McCurley, for his critical assistance in setting up and managing the HotCRP paper submission and review system, conference website, and other technology.
- Kevin McCurley, Kay McKelly, and members of the IACR’s emergency pandemic team for their work in designing and running the virtual format.
- Anna Kramer and her colleagues at Springer.

July 2021

Tal Malkin  
Chris Peikert

# Organization

## General Chair

Vladimir Kolesnikov

Georgia Institute of Technology, USA

## Program Committee Chairs

Tal Malkin

Columbia University, USA

Chris Peikert

University of Michigan and Algorand, Inc., USA

## Program Committee

Abhi Shelat

Northeastern University, USA

Andrej Bogdanov

Chinese University of Hong Kong, Hong Kong

Antigoni Polychroniadou

JP Morgan AI Research, USA

Brice Minaud

Inria and École Normale Supérieure, France

Chaya Ganesh

Indian Institute of Science, India

Chris Peikert

University of Michigan and Algorand, Inc., USA

Claudio Orlandi

Aarhus University, Denmark

Daniele Venturi

Sapienza University of Rome, Italy

David Cash

University of Chicago, USA

David Wu

University of Virginia, USA

Dennis Hofheinz

ETH Zurich, Switzerland

Divesh Aggarwal

National University of Singapore, Singapore

Dominique Unruh

University of Tartu, Estonia

Elena Andreeva

Technical University of Vienna, Austria

Elena Kirshanova

Immanuel Kant Baltic Federal University, Russia

Fabrice Benhamouda

Algorand Foundation, USA

Fang Song

Portland State University, USA

Frederik Vercauteren

KU Leuven, Belgium

Ghada Almashaqbeh

University of Connecticut, USA

Itai Dinur

Ben-Gurion University, Israel

Jean-Pierre Tillich

Inria, France

Jeremiah Blocki

Purdue University, USA

John Schanck

University of Waterloo, Canada

Jonathan Bootle

IBM Research, Switzerland

Joseph Jaeger

University of Washington, USA

Junqing Gong

East China Normal University, China

Lisa Kohl

CWI Amsterdam, The Netherlands

Manoj Prabhakaran

IIT Bombay, India

Marcel Keller

CSIRO's Data61, Australia

Mariana Raykova

Google, USA

Mike Rosulek	Oregon State University, USA
Mor Weiss	Bar-Ilan University, Israel
Muthuramakrishnan Venkitasubramaniam	University of Rochester, USA
Ni Trieu	Arizona State University, USA
Nir Bitansky	Tel Aviv University, Israel
Nuttapong Attrapadung	AIST, Japan
Omer Paneth	Tel Aviv University, Israel
Paul Grubbs	NYU, Cornell Tech and University of Michigan, USA
Peihan Miao	University of Illinois at Chicago, USA
Peter Schwabe	Max Planck Institute for Security and Privacy, Germany, and Radboud University, The Netherlands
Ran Canetti	BU, USA, and Tel Aviv University, Israel
Romain Gay	IBM Research, Switzerland
Ron Steinfeld	Monash University, Australia
Rosario Gennaro	City University of New York, USA
Ryo Nishimaki	NTT Secure Platform Laboratories, Japan
Sandro Coretti	IOHK, Switzerland
Sikhar Patranabis	Visa Research, USA
Sina Shiehian	UC Berkeley and Stony Brook University, USA
Siyao Guo	NYU Shanghai, China
Stanislaw Jarecki	University of California, Irvine, USA
Tal Malkin	Columbia University, USA
Tarik Moataz	Aroki Systems, USA
Thomas Peters	UC Louvain, Belgium
Thomas Peyrin	Nanyang Technological University, Singapore
Tianren Liu	University of Washington, USA
Viet Tung Hoang	Florida State University, USA
Xavier Bonnetain	University of Waterloo, Canada
Yu Yu	Shanghai Jiao Tong University, China

## Additional Reviewers

Aaram Yun	Akshayaram Srinivasan
Aarushi Goel	Akshima
Aayush Jain	Alain Passelègue
Abhishek Jain	Alex Bienstock
Adrien Benamira	Alex Lombardi
Agnes Kiss	Alexander Golovnev
Aishwarya Thiruvengadam	Alexander Hoover
Ajith Suresh	Alexander May
Akin Ünal	Alexandre Wallet
Akinori Kawachi	Alexandru Cojocaru
Akira Takahashi	Alice Pellet-Mary
Akshay Degwekar	Alin Tomescu



Amin Sakzad  
Amit Singh Bhati  
Amitabh Trehan  
Amos Beimel  
Anat Paskin-Cherniavsky  
Anca Nitulescu  
André Chailloux  
Andre Esser  
André Schrottenloher  
Andrea Coladangelo  
Andreas Hülsing  
Antonin Leroux  
Antonio Florez-Gutierrez  
Archita Agarwal  
Ariel Hamlin  
Arka Rai Choudhuri  
Arnab Roy  
Ashrujit Ghoshal  
Ashutosh Kumar  
Ashwin Jha  
Atsushi Takayasu  
Aurore Guillevic  
Avijit Dutta  
Avishay Yanay  
Baiyu Li  
Balazs Udvarhelyi  
Balthazar Bauer  
Bart Mennink  
Ben Smith  
Benjamin Diamond  
Benjamin Fuller  
Benny Applebaum  
Benoît Cogliati  
Benoit Libert  
Bertram Poettering  
Binyi Chen  
Bo-Yin Yang  
Bogdan Ursu  
Bruno Freitas dos Santos  
Bryan Parno  
Byeonghak Lee  
Carl Bootland  
Carles Padro  
Carmit Hazay  
Carsten Baum  
Cecilia Boschini

Chan Nam Ngo  
Charles Momin  
Charlotte Bonte  
Chen Qian  
Chen-Da Liu-Zhang  
Chenkai Weng  
Chethan Kamath  
Chris Brzuska  
Christian Badertscher  
Christian Janson  
Christian Majenz  
Christian Matt  
Christina Boura  
Christof Paar  
Christoph Egger  
Cody Freitag  
Dahmun Goudarzi  
Dakshita Khurana  
Damian Vizar  
Damiano Abram  
Damien Stehlé  
Damien Vergnaud  
Daniel Escudero  
Daniel Jost  
Daniel Masny  
Daniel Tschudi  
Daniel Wichs  
Dario Catalano  
Dario Fiore  
David Gerault  
David Heath  
Debbie Leung  
Dean Doron  
Debapriya Basu Roy  
Dima Kogan  
Dimitrios Papadopoulos  
Divya Gupta  
Divya Ravi  
Dominique Schröder  
Eduardo Soria-Vazquez  
Eldon Chung  
Emmanuela Orsini  
Eran Lambooi  
Eran Omri  
Eshan Chattopadhyay  
Estuardo Alpírez Bock

Evgenios Kornaropoulos  
 Eysa Lee  
 Fabio Banfi  
 Felix Engelmann  
 Felix Günther  
 Ferdinand Sibleyras  
 Fermi Ma  
 Fernando Virdia  
 Francesco Berti  
 François-Xavier Standaert  
 Fuyuki Kitagawa  
 Gaëtan Cassiers  
 Gaëtan Leurent  
 Gayathri Annapurna Garimella  
 Geoffroy Couteau  
 Georg Fuchsbauer  
 Ghouas Amjad  
 Gildas Avoine  
 Giorgos Panagiotakos  
 Giorgos Zirdelis  
 Giulio Malavolta  
 Guy Rothblum  
 Hamidreza Khoshakhlagh  
 Hamza Abusalah  
 Hanjun Li  
 Hannah Davis  
 Haoyang Wang  
 Hart Montgomery  
 Henry Corrigan-Gibbs  
 Hila Dahari  
 Huijia Lin  
 Ian McQuoid  
 Ignacio Cascudo  
 Igors Stepanovs  
 Ilan Komargodski  
 Ilia Iliashenko  
 Ingrid Verbauwhede  
 Itamar Levi  
 Ittai Abraham  
 Ivan Damgård  
 Jack Doerner  
 Jacob Schuldt  
 James Bartusek  
 Jan Czajkowski  
 Jan-Pieter D’Anvers  
 Jaspal Singh

Jean Paul Degabriele  
 Jesper Buus Nielsen  
 Jesús-Javier Chi-Domínguez  
 Ji Luo  
 Jian Guo  
 Jiaxin Pan  
 Jiayu Xu  
 Joanne Adams-Woodage  
 João Ribeiro  
 Joël Alwen  
 Julia Hesse  
 Julia Len  
 Julian Loss  
 Junichi Tomida  
 Justin Holmgren  
 Justin Thaler  
 Kai-Min Chung  
 Katerina Sotiraki  
 Katharina Boudgoust  
 Kathrin Hövelmanns  
 Katsuyuki Takashima  
 Kazuhiko Minematsu  
 Keita Xagawa  
 Kevin Yeo  
 Kewen Wu  
 Khoa Nguyen  
 Koji Nuida  
 Kristina Hostáková  
 Laasya Bangalore  
 Lars Knudsen  
 Lawrence Roy  
 Lejla Batina  
 Lennart Braun  
 Léo Colisson  
 Leo de Castro  
 Léo Ducas  
 Léo Perrin  
 Lin Lyu  
 Ling Song  
 Luca De Feo  
 Luca Nizzardo  
 Lucjan Hanzlik  
 Luisa Siniscalchi  
 Łukasz Chmielewski  
 Maciej Obremski  
 Madalina Bolboceanu

Mahimna Kelkar	Nils Fleischhacker
Maria Eichlseder	Nina Bindel
María Naya-Plasencia	Nirvan Tyagi
Marilyn George	Niv Gilboa
Marios Georgiou	Noah Stephens-Davidowitz
Mark Abspoel	Olivier Blazy
Mark Simkin	Olivier Bronchain
Mark Zhandry	Omri Shmueli
Markulf Kohlweiss	Orfeas Stefanos Thyfronitis Litos
Marshall Ball	Orr Dunkelman
Marta Mularczyk	Oxana Poburinnaya
Martin Albrecht	Patrick Derbez
Martin Hirt	Patrick Longa
Mary Wooters	Patrick Towa
Masayuki Abe	Paul Rösler
Matteo Campanelli	Paul Zimmermann
Matthias Fitzi	Peter Gazi
Mia Filic	Peter Rindal
Michael Reichle	Philippe Langevin
Michael Rosenberg	Pierre Briaud
Michael Walter	Pierre Meyer
Michele Orru	Pierrick Gaudry
Miguel Ambrona	Pierrick Mèaux
Mingyuan Wang	Po-Chu Hsu
Miran Kim	Prabhanjan Ananth
Miruna Rosca	Prashant Vasudeval
Miyako Ohkubo	Pratik Sarkar
Mohammad Hajiabadi	Pratik Soni
Mohammad Hossein Faghihi Sereshgi	Pratyay Mukherjee
Monosij Maitra	Pratyush Mishra
Morgan Shirley	Qian Li
Mridul Nandi	Qiang Tang
Muhammed F. Esgin	Qipeng Liu
Mustafa Khairallah	Quan Quan Tan
Naomi Ephraim	Rachit Garg
Nathan Manohar	Radu Titiu
Naty Peter	Rajeev Raghunath
Navid Alapati	Rajendra Kumar
Ngoc Khanh Nguyen	Ran Cohen
Nicholas Spooner	Raymond K. Zhao
Nicholas-Philip Brandt	Riad Wahby
Nico Döttling	Rishab Goyal
Nicolas Resch	Rishabh Bhadauria
Nicolas Sendrier	Rishiraj Bhattacharyya
Nikolaos Makriyannis	Ritam Bhaumik
Nikolas Melissaris	Robi Pedersen

Rohit Chatterjee  
Rolando La Placa  
Roman Langrehr  
Rongmao Chen  
Rupeng Yang  
Ruth Ng  
Saba Eskandarian  
Sabine Oechsner  
Sahar Mazloom  
Saikrishna Badrinarayanan  
Sam Kim  
Samir Hodzic  
Sanjam Garg  
Sayandeep Saha  
Schuyler Rosefield  
Semyon Novoselov  
Serge Fehr  
Shai Halevi  
Shashank Agrawal  
Sherman S. M. Chow  
Shi Bai  
Shifeng Sun  
Shivam Bhasin  
Shota Yamada  
Shuai Han  
Shuichi Katsumata  
Siang Meng Sim  
Somitra Sanadhya  
Sonia Belaïd  
Sophia Yakoubov  
Srinivas Vivek  
Srinivasan Raghuraman  
Sruthi Sekar  
Stefano Tessaro  
Steve Lu  
Steven Galbraith  
Stjepan Picek  
Sumegha Garg  
Susumu Kiyoshima  
Sven Maier  
Takahiro Matsuda  
Takashi Yamakawa  
Tal Moran  
Tamer Mour  
Thom Wiggers

Thomas Agrikola  
Thomas Attema  
Thomas Debris-Alazard  
Thomas Decru  
Tiancheng Xie  
Tim Beyne  
Titouan Tanguy  
Tommaso Gagliardoni  
Varun Maram  
Vassilis Zikas  
Venkata Koppula  
Vincent Zucca  
Virginie Lallemand  
Ward Beullens  
Wei Dai  
Willy Quach  
Wouter Castryck  
Xiao Liang  
Xiao Wang  
Xiong Fan  
Yael Kalai  
Yan Bo Ti  
Yann Rotella  
Yannick Seurin  
Yaobin Shen  
Yashvanth Kondi  
Yfke Dulek  
Yiannis Tselekounis  
Yifan Song  
Yilei Chen  
Yixin Shen  
Yongsoo Song  
Yu Long Chen  
Yu Sa  
Yue Guo  
Yuncong Hu  
Yupeng Zhang  
Yuriy Polyakov  
Yuval Ishai  
Zahra Jafargholi  
Zeyong Li  
Zhengfeng Ji  
Zichen Gui  
Zuoxia Yu  
Zvika Brakerski

# Contents – Part I

## Invited Talk

Which E-Voting Problems Do We Need to Solve? . . . . .	3
<i>Vanessa Teague</i>	

## Award Papers

On the Possibility of Basing Cryptography on $\text{EXP} \neq \text{BPP}$ . . . . .	11
<i>Yanyi Liu and Rafael Pass</i>	
Linear Cryptanalysis of FF3-1 and FEA. . . . .	41
<i>Tim Beyne</i>	
Efficient Key Recovery for All HFE Signature Variants. . . . .	70
<i>Chengdong Tao, Albrecht Petzoldt, and Jintai Ding</i>	
Three Halves Make a Whole? Beating the Half-Gates Lower Bound for Garbled Circuits. . . . .	94
<i>Mike Rosulek and Lawrence Roy</i>	

## Signatures

Threshold Schnorr with Stateless Deterministic Signing from Standard Assumptions. . . . .	127
<i>François Garillot, Yashvanth Kondi, Payman Mohassel, and Valeria Nikolaenko</i>	
Two-Round Trip Schnorr Multi-signatures via Delinearized Witnesses. . . . .	157
<i>Handan Kılınç Alper and Jeffrey Burdges</i>	
MuSig2: Simple Two-Round Schnorr Multi-signatures. . . . .	189
<i>Jonas Nick, Tim Ruffing, and Yannick Seurin</i>	
Tighter Security for Schnorr Identification and Signatures: A High-Moment Forking Lemma for $\Sigma$ -Protocols . . . . .	222
<i>Lior Rotem and Gil Segev</i>	
DualRing: Generic Construction of Ring Signatures with Efficient Instantiations . . . . .	251
<i>Tsz Hon Yuen, Muhammed F. Esgin, Joseph K. Liu, Man Ho Au, and Zhimin Ding</i>	

<b>Compact Ring Signatures from Learning with Errors . . . . .</b>	<b>282</b>
<i>Rohit Chatterjee, Sanjam Garg, Mohammad Hajiabadi, Dakshita Khurana, Xiao Liang, Giulio Malavolta, Omkant Pandey, and Sina Shiehian</i>	
<b>Quantum Cryptography</b>	
<b>A Black-Box Approach to Post-Quantum Zero-Knowledge in Constant Rounds . . . . .</b>	<b>315</b>
<i>Nai-Hui Chia, Kai-Min Chung, and Takashi Yamakawa</i>	
<b>On the Concurrent Composition of Quantum Zero-Knowledge . . . . .</b>	<b>346</b>
<i>Prabhanjan Ananth, Kai-Min Chung, and Rolando L. La Placa</i>	
<b>Multi-theorem Designated-Verifier NIZK for QMA . . . . .</b>	<b>375</b>
<i>Omri Shmueli</i>	
<b>On the Round Complexity of Secure Quantum Computation . . . . .</b>	<b>406</b>
<i>James Bartusek, Andrea Coladangelo, Dakshita Khurana, and Fermi Ma</i>	
<b>Round Efficient Secure Multiparty Quantum Computation with Identifiable Abort. . . . .</b>	<b>436</b>
<i>Bar Alon, Hao Chung, Kai-Min Chung, Mi-Ying Huang, Yi Lee, and Yu-Ching Shen</i>	
<b>One-Way Functions Imply Secure Computation in a Quantum World . . . . .</b>	<b>467</b>
<i>James Bartusek, Andrea Coladangelo, Dakshita Khurana, and Fermi Ma</i>	
<b>Impossibility of Quantum Virtual Black-Box Obfuscation of Classical Circuits . . . . .</b>	<b>497</b>
<i>Gorjan Alagic, Zvika Brakerski, Yfke Dulek, and Christian Schaffner</i>	
<b>New Approaches for Quantum Copy-Protection . . . . .</b>	<b>526</b>
<i>Scott Aaronson, Jiahui Liu, Qipeng Liu, Mark Zhandry, and Ruizhe Zhang</i>	
<b>Hidden Cosets and Applications to Unclonable Cryptography . . . . .</b>	<b>556</b>
<i>Andrea Coladangelo, Jiahui Liu, Qipeng Liu, and Mark Zhandry</i>	
<b>On Tight Quantum Security of HMAC and NMAC in the Quantum Random Oracle Model. . . . .</b>	<b>585</b>
<i>Akinori Hosoyamada and Tetsu Iwata</i>	
<b>Quantum Collision Attacks on Reduced SHA-256 and SHA-512 . . . . .</b>	<b>616</b>
<i>Akinori Hosoyamada and Yu Sasaki</i>	

**Succinct Arguments**

<b>Halo Infinite: Proof-Carrying Data from Additive Polynomial Commitments . . . . .</b>	<b>649</b>
<i>Dan Boneh, Justin Drake, Ben Fisch, and Ariel Gabizon</i>	
<b>Proof-Carrying Data Without Succinct Arguments . . . . .</b>	<b>681</b>
<i>Benedikt Bünz, Alessandro Chiesa, William Lin, Pratyush Mishra, and Nicholas Spooner</i>	
<b>Subquadratic SNARGs in the Random Oracle Model. . . . .</b>	<b>711</b>
<i>Alessandro Chiesa and Eylon Yogev</i>	
<b>Sumcheck Arguments and Their Applications . . . . .</b>	<b>742</b>
<i>Jonathan Bootle, Alessandro Chiesa, and Katerina Sotiraki</i>	
<b>An Algebraic Framework for Universal and Updatable SNARKs . . . . .</b>	<b>774</b>
<i>Carla Ràfols and Arantxa Zapico</i>	
<b>Author Index . . . . .</b>	<b>805</b>