Lecture Notes in Computer Science 12826

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 II

Springer

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 978-3-030-84244-4 ISBN 978-3-030-84245-1 (eBook)
https://doi.org/10.1007/978-3-030-84245-1

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

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 $\mathtt{EXP} \neq \mathtt{BPP}$" 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
Aarushi Goel
Aayush Jain
Abhishek Jain
Adrien Benamira
Agnes Kiss
Aishwarya Thiruvengadam
Ajith Suresh
Akin Ünal
Akinori Kawachi
Akira Takahashi
Akshay Degwekar
Akshayaram Srinivasan
Akshima
Alain Passelègue
Alex Bienstock
Alex Lombardi
Alexander Golovnev
Alexander Hoover
Alexander May
Alexandre Wallet
Alexandru Cojocaru
Alice Pellet-Mary
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 Lambooij
Eran Omri
Eshan Chattopadhyay
Estuardo Alpirez 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
Ghous 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
Maria Eichlseder
María Naya-Plasencia
Marilyn George
Marios Georgiou
Mark Abspoel
Mark Simkin
Mark Zhandry
Markulf Kohlweiss
Marshall Ball
Marta Mularczyk
Martin Albrecht
Martin Hirt
Mary Wooters
Masayuki Abe
Matteo Campanelli
Matthias Fitzi
Mia Filic
Michael Reichle
Michael Rosenberg
Michael Walter
Michele Orru
Miguel Ambrona
Mingyuan Wang
Miran Kim
Miruna Rosca
Miyako Ohkubo
Mohammad Hajiabadi
Mohammad Hossein Faghihi Sereshgi
Monosij Maitra
Morgan Shirley
Mridul Nandi
Muhammed F. Esgin
Mustafa Khairallah
Naomi Ephraim
Nathan Manohar
Naty Peter
Navid Alamati
Ngoc Khanh Nguyen
Nicholas Spooner
Nicholas-Philip Brandt
Nico Döttling
Nicolas Resch
Nicolas Sendrier
Nikolaos Makriyannis
Nikolas Melissaris
Nils Fleischhacker
Nina Bindel
Nirvan Tyagi
Niv Gilboa
Noah Stephens-Davidowitz
Olivier Blazy
Olivier Bronchain
Omri Shmueli
Orfeas Stefanos Thyfronitis Litos
Orr Dunkelman
Oxana Poburinnaya
Patrick Derbez
Patrick Longa
Patrick Towa
Paul Rösler
Paul Zimmermann
Peter Gazi
Peter Rindal
Philippe Langevin
Pierre Briaud
Pierre Meyer
Pierrick Gaudry
Pierrick Mèaux
Po-Chu Hsu
Prabhanjan Ananth
Prashant Vasudeval
Pratik Sarkar
Pratik Soni
Pratyay Mukherjee
Pratyush Mishra
Qian Li
Qiang Tang
Qipeng Liu
Quan Quan Tan
Rachit Garg
Radu Titiu
Rajeev Raghunath
Rajendra Kumar
Ran Cohen
Raymond K. Zhao
Riad Wahby
Rishab Goyal
Rishabh Bhadauria
Rishiraj Bhattacharyya
Ritam Bhaumik
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 II

Multi-party Computation

Lattice Cryptanalysis