

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>

Anne Canteaut · François-Xavier Standaert (Eds.)

Advances in Cryptology – EUROCRYPT 2021

40th Annual International Conference on the Theory
and Applications of Cryptographic Techniques
Zagreb, Croatia, October 17–21, 2021
Proceedings, Part III

Editors

Anne Canteaut 
Inria
Paris, France

François-Xavier Standaert 
UCLouvain
Louvain-la-Neuve, Belgium

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-77882-8 ISBN 978-3-030-77883-5 (eBook)
<https://doi.org/10.1007/978-3-030-77883-5>

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

Eurocrypt 2021, the 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, was held in Zagreb, Croatia, during October 17–21, 2021.¹ 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.

We received a total of 400 submissions. Each submission was anonymized for the reviewing process and was assigned to at least three of the 59 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 78 papers. The revised versions of these papers are included in this three-volume proceedings.

The PC decided to give Best Paper Awards to the papers “*Non-Interactive Zero Knowledge from Sub-exponential DDH*” by Abhishek Jain and Zhengzhong Jin, “*On the (in)security of ROS*” by Fabrice Benhamouda, Tancrede Lepoint, Julian Loss, Michele Orrù, and Mariana Raykova and “*New Representations of the AES Key Schedule*” by Gaëtan Leurent and Clara Pernot. The authors of these three papers received an invitation to submit an extended version of their work to the *Journal of Cryptology*. The program also included invited talks by Craig Gentry (Algorand Foundation) and Sarah Meiklejohn (University College London).

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 good papers which did not find a slot in the sparse number of accepted papers. We sincerely hope that these works will eventually get the attention they deserve.

We are indebted to the PC and the external reviewers for their voluntary work. Selecting papers from 400 submissions covering the many areas of cryptologic research is a huge workload. It has been an honor to work with everyone. We owe a big thank you to Kevin McCurley for his continuous support in solving all the minor issues we had with the HotCRP review system, to Gaëtan Leurent for sharing his MILP programs which made the papers assignments much easier, and to Simona Samardjiska who acted as Eurocrypt 2021 webmaster.

Finally, we thank all the other people (speakers, sessions chairs, rump session chairs...) for their contribution to the program of Eurocrypt 2021. We would also like to thank the many sponsors for their generous support, including the Cryptography Research Fund that supported student speakers.

April 2021

Anne Canteaut
François-Xavier Standaert

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 due to COVID-19.

Eurocrypt 2021

The 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques

Sponsored by the *International Association for Cryptologic Research*
Zagreb, Croatia
October 17–21, 2021

General Co-chairs

Lejla Batina
Stjepan Picek

Radboud University, The Netherlands
Delft University of Technology, The Netherlands

Program Committee Chairs

Anne Canteaut
François-Xavier Standaert

Inria, France
UCLouvain, Belgium

Program Committee

Shweta Agrawal

Joël Alwen

Foteini Baldimtsi

Marshall Ball

Begül Bilgin

Nir Bitansky

Joppe W. Bos

Christina Boura

Wouter Castryck

Kai-Min Chung

Jean-Sébastien Coron

Véronique Cortier

Geoffroy Couteau

Luca De Feo

Léo Ducas (Area Chair:
Public-Key Crypto)

Orr Dunkelman

Stefan Dziembowski
(Area Chair: Theory)

Thomas Eisenbarth

Dario Fiore

Marc Fischlin

IIT Madras, India

Wickr, USA

George Mason University, USA

Columbia University, USA

Rambus - Cryptography Research, The Netherlands

Tel Aviv University, Israel

NXP Semiconductors, Belgium

University of Versailles, France

KU Leuven, Belgium

Academia Sinica, Taiwan

University of Luxembourg, Luxembourg

LORIA, CNRS, France

CNRS, IRIF, Université de Paris, France

IBM Research Europe, Switzerland

CWI, Amsterdam, The Netherlands

University of Haifa, Israel

University of Warsaw, Poland

University of Lübeck, Germany

IMDEA Software Institute, Spain

TU Darmstadt, Germany

Benjamin Fuller	University of Connecticut, USA
Adrià Gascón	Google, UK
Henri Gilbert	ANSSI, France
Shai Halevi	Algorand Foundation, USA
Annelie Heuser	Univ Rennes, CNRS, IRISA, France
Naofumi Homma	Tohoku University, Japan
Kristina Hostáková	ETH Zürich, Switzerland
Tetsu Iwata	Nagoya University, Japan
Marc Joye	Zama, France
Pascal Junod (Area Chair: Real-World Crypto)	Snap, Switzerland
Pierre Karpman	Université Grenoble-Alpes, France
Gregor Leander (Area Chair: Symmetric Crypto)	Ruhr-Universität Bochum, Germany
Benoît Libert	CNRS and ENS de Lyon, France
Julian Loss	University of Maryland, College Park, USA
Christian Majenz	CWI, Amsterdam, The Netherlands
Daniel Masny	Visa Research, USA
Bart Mennink	Radboud University, The Netherlands
Tarik Moataz	Aroki Systems, USA
Amir Moradi	Ruhr-Universität Bochum, Germany
Michael Naehrig	Microsoft Research, USA
Maria Naya-Plasencia	Inria, France
Claudio Orlandi	Aarhus University, Denmark
Elisabeth Oswald (Area Chair: Implementations)	University of Klagenfurt, Austria
Dan Page	University of Bristol, UK
Rafael Pass	Cornell Tech, USA
Thomas Peyrin	Nanyang Technological University, Singapore
Oxana Poburinnaya	University of Rochester and Ligerio Inc., USA
Matthieu Rivain	CryptoExperts, France
Adeline Roux-Langlois	Univ Rennes, CNRS, IRISA, France
Louis Salvail	Université de Montréal, Canada
Yu Sasaki	NTT Laboratories, Japan
Tobias Schneider	NXP Semiconductors, Austria
Yannick Seurin	ANSSI, France
Emmanuel Thomé	LORIA, Inria Nancy, France
Vinod Vaikuntanathan	MIT, USA
Prashant Nalini Vasudevan	UC Berkeley, USA
Daniele Venturi	Sapienza University of Rome, Italy
Daniel Wichs	Northeastern University and NTT Research Inc., USA
Yu Yu	Shanghai Jiao Tong University, China

Additional Reviewers

Mark Abspoel
 Hamza Abusalah
 Alexandre Adomnicai
 Archita Agarwal
 Divesh Aggarwal
 Shashank Agrawal
 Gorjan Alagic
 Martin R. Albrecht
 Ghada Almashaqbeh
 Bar Alon
 Miguel Ambrona
 Ghous Amjad
 Prabhanjan Ananth
 Toshinori Araki
 Victor Arribas
 Gilad Asharov
 Roberto Avanzi
 Melissa Azouaoui
 Christian Badertscher
 Saikrishna
 Badrinarayanan
 Karim Bagheri
 Victor Balcer
 Laasya Bangalore
 Magali Bardet
 James Bartusek
 Balthazar Bauer
 Carsten Baum
 Christof Beierle
 James Bell
 Fabrice Benhamouda
 Iddo Bentov
 Olivier Bernard
 Sebastian Berndt
 Pauline Bert
 Ward Beullens
 Benjamin Beurdouche
 Ritam Bhaumik
 Erica Blum
 Alexandra Boldyreva
 Jonathan Bootle
 Nicolas Bordes
 Katharina Boudgoust

Florian Bourse
 Xavier Boyen
 Elette Boyle
 Zvika Brakerski
 Lennart Braun
 Gianluca Brian
 Marek Broll
 Olivier Bronchain
 Chris Brzuska
 Benedikt Bünz
 Chloe Cachet
 Matteo Campanelli
 Federico Canale
 Ignacio Cascudo
 Gaëtan Cassiers
 Avik Chakraborti
 Benjamin Chan
 Eshan Chattopadhyay
 Panagiotis Chatzigiannis
 Shan Chen
 Yanlin Chen
 Yilei Chen
 Yu Chen
 Alessandro Chiesa
 Ilaria Chillotti
 Seung Geol Choi
 Arka Rai Choudhuri
 Michele Ciampi
 Daniel Coggia
 Benoît Cogliati
 Ran Cohen
 Andrea Coladangelo
 Sandro Coretti-Drayton
 Craig Costello
 Daniele Cozzo
 Ting Ting Cui
 Debajyoti Das
 Poulami Das
 Bernardo David
 Alex Davidson
 Gareth Davies
 Lauren De Meyer
 Thomas Debris-Alazard

Leo de Castro
 Thomas Decru
 Jean Paul Degabriele
 Akshay Degwekar
 Amit Deo
 Patrick Derbez
 Itai Dinur
 Christoph Dobraunig
 Yevgeniy Dodis
 Jack Doerner
 Jelle Don
 Benjamin Dowling
 Eduoard Dufour Sans
 Yfke Dulek
 Frédéric Dupuis
 Sylvain Duquesne
 Avijit Dutta
 Ehsan Ebrahimi
 Kasra Edalat Nejdlat
 Naomi Ephraim
 Thomas Espitau
 Andre Esser
 Grzegorz Fabiański
 Xiong Fan
 Antonio Faonio
 Sebastian Faust
 Serge Fehr
 Patrick Felke
 Rune Fiedler
 Ben Fisch
 Matthias Fitz
 Antonio Flórez-Gutiérrez
 Cody Freitag
 Georg Fuchsbauer
 Ariel Gabizon
 Nicolas Gama
 Chaya Ganesh
 Rachit Garg
 Pierrick Gaudry
 Romain Gay
 Peter Gaži
 Nicholas Genise
 Craig Gentry

Marilyn George	Daniel Jost	Nikos Leonardos
Adela Georgescu	Kimmo Järvinen	Matthieu Lequesne
David Gerault	Guillaume Kaim	Antonin Leroux
Essam Ghadafi	Chethan Kamath	Gaëtan Leurent
Satrajit Ghosh	Pritish Kamath	Jyun-Jie Liao
Irene Giacomelli	Fredrik Kamphuis	Damien Ligier
Aarushi Goel	Ioanna Karantaidou	Huijia Lin
Junqing Gong	Shuichi Katsumata	Benjamin Lipp
Alonso González	Jonathan Katz	Maciej Liskiewicz
S. Dov Gordon	Tomasz Kazana	Qipeng Liu
Louis Goubin	Marcel Keller	Shengli Liu
Marc Gourjon	Mustafa Khairallah	Tianren Liu
Rishab Goyal	Louiza Khati	Yanyi Liu
Lorenzo Grassi	Hamidreza Khoshakhlagh	Chen-Da Liu-Zhang
Elijah Grubb	Dakshita Khurana	Alex Lombardi
Cyprien de Saint Guilhem	Ryo Kikuchi	Patrick Longa
Aurore Guillevic	Eike Kiltz	Vadim Lyubashevsky
Aldo Günsing	Elena Kirshanova	Fermi Ma
Chun Guo	Agnes Kiss	Mimi Ma
Qian Guo	Karen Klein	Urmila Mahadev
Felix Günther	Michael Klooß	Nikolaos Makriyannis
Iftach Haitner	Alexander Koch	Giulio Malavolta
Mohammad Hajiabadi	Lisa Kohl	Damien Marion
Mathias Hall-Andersen	Vladimir Kolesnikov	Yoann Marquer
Ariel Hamlin	Dimitris Kolonelos	Giorgia Marson
Lucjan Hanzlik	Ilan Komargodski	Chloe Martindale
Patrick Harasser	Yashvanth Kondi	Ange Martinelli
Dominik Hartmann	Venkata Koppula	Michael Meyer
Eduard Hauck	Adrien Koutsos	Pierre Meyer
Phil Hebborn	Hugo Krawczyk	Andrew Miller
Javier Herranz	Stephan Krenn	Brice Minaud
Amir Herzberg	Ashutosh Kumar	Ilya Mironov
Julia Hesse	Ranjit Kumaresan	Tal Moran
Shoichi Hirose	Po-Chun Kuo	Saleet Mossel
Martin Hirt	Rolando L. La Placa	Tamer Mour
Akinori Hosoyamada	Thijs Laarhoven	Pratyay Mukherjee
Kathrin Hövelmanns	Jianchang Lai	Marta Mularczyk
Andreas Hülsing	Virginie Lallemand	Pierrick Méaux
Ilia Iliashenko	Baptiste Lambin	Yusuke Naito
Charlie Jacomme	Eran Lambooj	Joe Neeman
Christian Janson	Philippe Lamontagne	Patrick Neumann
Stanislaw Jarecki	Rio Lavigne	Khoa Nguyen
Ashwin Jha	Jooyoung Lee	Ngoc Khanh Nguyen
Dingding Jia	Alexander Lemmens	Phong Nguyen

Tuong-Huy Nguyen
 Jesper Buus Nielsen
 Ryo Nishimaki
 Abderrahmane Nitaj
 Anca Nitulescu
 Lamine Nouredine
 Adam O'Neill
 Maciej Obremski
 Cristina Onete
 Michele Orru
 Emmanuela Orsini
 Carles Padro
 Mahak Pancholi
 Omer Paneth
 Dimitris Papachristoudis
 Sunoo Park
 Anat Paskin-Cherniavsky
 Alice Pellet-Mary
 Olivier Pereira
 Léo Perrin
 Thomas Peters
 Duy-Phuc Pham
 Krzysztof Pietrzak
 Jérôme Plût
 Bertram Poettering
 Yuriy Polyakov
 Antigoni Polychroniadou
 Alexander Poremba
 Thomas Prest
 Cassius Puodzius
 Willy Quach
 Anaïs Querol
 Rahul Rachuri
 Hugues Randriam
 Adrian Ranea
 Shahram Rasoolzadeh
 Deevashwer Rathee
 Mayank Rathee
 Divya Ravi
 Christian Rechberger
 Michael Reichle
 Jean-René Reinhard
 Joost Renes
 Nicolas Resch

João Ribeiro
 Silas Richelson
 Tania Richmond
 Doreen Riepel
 Peter Rindal
 Miruna Rosca
 Michael Rosenberg
 Mélissa Rossi
 Yann Rotella
 Alex Russell
 Théo Ryffel
 Carla Ràfols
 Paul Rösler
 Rajeev Anand Sahu
 Olga Sanina
 Pratik Sarkar
 Alessandra Scafuro
 Christian Schaffner
 Peter Scholl
 Tobias Schmalz
 Phillipp Schoppmann
 André Schrottenloher
 Jörg Schwenk
 Adam Sealfon
 Okan Seker
 Jae Hong Seo
 Karn Seth
 Barak Shani
 Abhi Shelat
 Omri Shmueli
 Victor Shoup
 Hippolyte Signargout
 Tjerand Silde
 Mark Simkin
 Luisa Siniscalchi
 Daniel Slamanig
 Benjamin Smith
 Fang Song
 Jana Sotáková
 Pierre-Jean Spaenlehauer
 Nicholas Spooner
 Akshayaram Srinivasan
 Damien Stehlé
 Marc Stevens

Siwei Sun
 Mehrdad Tahmasbi
 Quan Quan Tan
 Stefano Tessaro
 Florian Thaeter
 Aishwarya
 Thiruvengadam
 Mehdi Tibouchi
 Radu Titiu
 Oleksandr Tkachenko
 Yosuke Todo
 Junichi Tomida
 Ni Trieu
 Eran Tromer
 Daniel Tschudi
 Giorgos Tsimos
 Ida Tucker
 Michael Tunstall
 Akin Ünal
 Dominique Unruh
 Bogdan Ursu
 Christine van Vredendaal
 Wessel van Woerden
 Marc Vaclair
 Serge Vaudenay
 Muthu
 Venkitasubramaniam
 Damien Vergnaud
 Gilles Villard
 Fernando Virdia
 Satyanarayana Vusirikala
 Riad Wahby
 Hendrik Waldner
 Alexandre Wallet
 Haoyang Wang
 Hoeteck Wee
 Weiqiang Wen
 Benjamin Wesolowski
 Jan Wichelmann
 Luca Wilke
 Mary Wootters
 David Wu
 Jiayu Xu
 Sophia Yakoubov

Shota Yamada
Takashi Yamakawa
Sravya Yandamuri
Kang Yang
Lisa Yang

Kevin Yeo
Eylon Yogev
Greg Zaverucha
Mark Zhandry
Jiayu Zhang

Ruizhe Zhang
Yupeng Zhang
Vassilis Zikas
Paul Zimmermann
Dionysis Zindros

Contents – Part III

Garbled Circuits

LogStack: Stacked Garbling with $O(b \log b)$ Computation	3
<i>David Heath and Vladimir Kolesnikov</i>	
Large Scale, Actively Secure Computation from LPN and Free-XOR Garbled Circuits	33
<i>Aner Ben-Efraim, Kelong Cong, Eran Omri, Emmanuela Orsini, Nigel P. Smart, and Eduardo Soria-Vazquez</i>	
Threshold Garbled Circuits and Ad Hoc Secure Computation	64
<i>Michele Ciampi, Vipul Goyal, and Rafail Ostrovsky</i>	

Indistinguishability Obfuscation

Indistinguishability Obfuscation from Simple-to-State Hard Problems: New Assumptions, New Techniques, and Simplification	97
<i>Romain Gay, Aayush Jain, Huijia Lin, and Amit Sahai</i>	
Candidate Obfuscation via Oblivious LWE Sampling	127
<i>Hoeteck Wee and Daniel Wichs</i>	

Non-Malleable Commitments

Black-Box Non-interactive Non-malleable Commitments	159
<i>Rachit Garg, Dakshita Khurana, George Lu, and Brent Waters</i>	
Non-interactive Distributional Indistinguishability (NIDI) and Non-malleable Commitments	186
<i>Dakshita Khurana</i>	

Zero-Knowledge Proofs

Public-Coin Statistical Zero-Knowledge Batch Verification Against Malicious Verifiers	219
<i>Inbar Kaslasi, Ron D. Rothblum, and Prashant Nalini Vasudevan</i>	
Efficient Range Proofs with Transparent Setup from Bounded Integer Commitments.	247
<i>Geoffroy Couteau, Michael Klooß, Huang Lin, and Michael Reichle</i>	

Towards Accountability in CRS Generation	278
<i>Prabhanjan Ananth, Gilad Asharov, Hila Dahari, and Vipul Goyal</i>	

Property-Preserving Hash Functions and ORAM

Robust Property-Preserving Hash Functions for Hamming Distance and More	311
<i>Nils Fleischhacker and Mark Simkin</i>	

Alibi: A Flaw in Cuckoo-Hashing Based Hierarchical ORAM Schemes and a Solution	338
<i>Brett Hemenway Falk, Daniel Noble, and Rafail Ostrovsky</i>	

Structured Encryption and Dynamic Leakage Suppression	370
<i>Marilyn George, Seny Kamara, and Tarik Moataz</i>	

Blockchain

Dynamic Ad Hoc Clock Synchronization	399
<i>Christian Badertscher, Peter Gazi, Aggelos Kiayias, Alexander Russell, and Vassilis Zikas</i>	

TARDIS: A Foundation of Time-Lock Puzzles in UC	429
<i>Carsten Baum, Bernardo David, Rafael Dowsley, Jesper Buus Nielsen, and Sabine Oechsner</i>	

Privacy and Law Enforcement

On the Power of Multiple Anonymous Messages: Frequency Estimation and Selection in the Shuffle Model of Differential Privacy	463
<i>Badih Ghazi, Noah Golowich, Ravi Kumar, Rasmus Pagh, and Ameya Velingker</i>	

Non-Interactive Anonymous Router	489
<i>Elaine Shi and Ke Wu</i>	

Bifurcated Signatures: Folding the Accountability vs. Anonymity Dilemma into a Single Private Signing Scheme	521
<i>Benoît Libert, Khoa Nguyen, Thomas Peters, and Moti Yung</i>	

Abuse Resistant Law Enforcement Access Systems	553
<i>Matthew Green, Gabriel Kaptchuk, and Gijs Van Laer</i>	

Author Index	585
------------------------	-----