

Anne Canteaut  
François-Xavier Standaert (Eds.)

LNCS 12697

# 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 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*

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 II

*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 978-3-030-77885-9              ISBN 978-3-030-77886-6 (eBook)  
<https://doi.org/10.1007/978-3-030-77886-6>

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.<sup>1</sup> 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 Samaradjiska 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

---

<sup>1</sup> 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

IIT Madras, India

Joël Alwen

Wickr, USA

Foteini Baldimtsi

George Mason University, USA

Marshall Ball

Columbia University, USA

Begül Bilgin

Rambus - Cryptography Research, The Netherlands

Nir Bitansky

Tel Aviv University, Israel

Joppe W. Bos

NXP Semiconductors, Belgium

Christina Boura

University of Versailles, France

Wouter Castryck

KU Leuven, Belgium

Kai-Min Chung

Academia Sinica, Taiwan

Jean-Sébastien Coron

University of Luxembourg, Luxembourg

Véronique Cortier

LORIA, CNRS, France

Geoffroy Couteau

CNRS, IRIF, Université de Paris, France

Luca De Feo

IBM Research Europe, Switzerland

Léo Ducas (Area Chair:  
Public-Key Crypto)

CWI, Amsterdam, The Netherlands

Orr Dunkelman

University of Haifa, Israel

Stefan Dziembowski

University of Warsaw, Poland

(Area Chair: Theory)

Thomas Eisenbarth

University of Lübeck, Germany

Dario Fiore

IMDEA Software Institute, Spain

Marc Fischlin

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
María 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	Florian Bourse	Leo de Castro
Hamza Abusalah	Xavier Boyen	Thomas Decru
Alexandre Adomnicai	Elette Boyle	Jean Paul Degabriele
Archita Agarwal	Zvika Brakerski	Akshay Degwekar
Divesh Aggarwal	Lennart Braun	Amit Deo
Shashank Agrawal	Gianluca Brian	Patrick Derbez
Gorjan Alagic	Marek Broll	Itai Dinur
Martin R. Albrecht	Olivier Bronchain	Christoph Dobraunig
Ghada Almashaqbeh	Chris Brzuska	Yevgeniy Dodis
Bar Alon	Benedikt Bünz	Jack Doerner
Miguel Ambrona	Chloe Cachet	Jelle Don
Ghous Amjad	Matteo Campanelli	Benjamin Dowling
Prabhanjan Ananth	Federico Canale	Eduoard Dufour Sans
Toshinori Araki	Ignacio Cascudo	Yfke Dulek
Victor Arribas	Gaëtan Cassiers	Frédéric Dupuis
Gilad Asharov	Avik Chakraborti	Sylvain Duquesne
Roberto Avanzi	Benjamin Chan	Avijit Dutta
Melissa Azouaoui	Eshan Chattopadhyay	Ehsan Ebrahimi
Christian Badertscher	Panagiotis Chatzigiannis	Kasra Edalat Nejd
Saikrishna	Shan Chen	Naomi Ephraim
Badrinarayanan	Yanlin Chen	Thomas Espitau
Karim Bagheri	Yilei Chen	Andre Esser
Victor Balcer	Yu Chen	Grzegorz Fabiański
Laasya Bangalore	Alessandro Chiesa	Xiong Fan
Magali Bardet	Ilaria Chillotti	Antonio Faonio
James Bartusek	Seung Geol Choi	Sebastian Faust
Balthazar Bauer	Arka Rai Choudhuri	Serge Fehr
Carsten Baum	Michele Ciampi	Patrick Felke
Christof Beierle	Daniel Coggia	Rune Fiedler
James Bell	Benoît Cogliati	Ben Fisch
Fabrice Benhamouda	Ran Cohen	Matthias Fitz
Iddo Bentov	Andrea Coladangelo	Antonio Flórez-Gutiérrez
Olivier Bernard	Sandro Coretti-Drayton	Cody Freitag
Sebastian Berndt	Craig Costello	Georg Fuchsbauer
Pauline Bert	Daniele Cozzo	Ariel Gabizon
Ward Beullens	Ting Ting Cui	Nicolas Gama
Benjamin Beurdouche	Debajyoti Das	Chaya Ganesh
Ritam Bhaumik	Poulami Das	Rachit Garg
Erica Blum	Bernardo David	Pierrick Gaudry
Alexandra Boldyreva	Alex Davidson	Romain Gay
Jonathan Bootle	Gareth Davies	Peter Gaži
Nicolas Bordes	Lauren De Meyer	Nicholas Genise
Katharina Boudgoust	Thomas Debris-Alazard	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 Gunsing	Elena Kirshanova	Fermi Ma
Chun Guo	Agnes Kiss	Mimi Ma
Qian Guo	Karen Klein	Urmila Mahadev
Felix Günther	Michael Kloof	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
Iliia 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	João Ribeiro	Siwei Sun
Jesper Buus Nielsen	Silas Richelson	Mehrdad Tahmasbi
Ryo Nishimaki	Tania Richmond	Quan Quan Tan
Abderrahmane Nitaj	Doreen Riepel	Stefano Tessaro
Anca Nitulescu	Peter Rindal	Florian Thaeter
Lamine Nouredine	Miruna Rosca	Aishwarya
Adam O'Neill	Michael Rosenberg	Thiruvengadam
Maciej Obremski	Mélissa Rossi	Mehdi Tibouchi
Cristina Onete	Yann Rotella	Radu Titiu
Michele Orru	Alex Russell	Oleksandr Tkachenko
Emmanuela Orsini	Théo Ryffel	Yosuke Todo
Carles Padro	Carla Ràfols	Junichi Tomida
Mahak Pancholi	Paul Rösler	Ni Trieu
Omer Paneth	Rajeev Anand Sahu	Eran Tromer
Dimitris Papachristoudis	Olga Sanina	Daniel Tschudi
Sunoo Park	Pratik Sarkar	Giorgos Tsimos
Anat Paskin-Cherniavsky	Alessandra Scafuro	Ida Tucker
Alice Pellet-Mary	Christian Schaffner	Michael Tunstall
Olivier Pereira	Peter Scholl	Akin Ünäl
Léo Perrin	Tobias Schmalz	Dominique Unruh
Thomas Peters	Phillipp Schoppmann	Bogdan Ursu
Duy-Phuc Pham	André Schrottenloher	Christine van Vredendaal
Krzyszof Pietrzak	Jörg Schwenk	Wessel van Woerden
Jérôme Plût	Adam Sealfon	Marc Vaclair
Bertram Poettering	Okan Seker	Serge Vaudenay
Yuriy Polyakov	Jae Hong Seo	Muthu
Antigoni Polychroniadou	Karn Seth	Venkitasubramaniam
Alexander Poremba	Barak Shani	Damien Vergnaud
Thomas Prest	Abhi Shelat	Gilles Villard
Cassius Puodzius	Omri Shmueli	Fernando Virdia
Willy Quach	Victor Shoup	Satyanarayana Vusirikala
Anaís Querol	Hippolyte Signargout	Riad Wahby
Rahul Rachuri	Tjerand Silde	Hendrik Waldner
Hugues Randriam	Mark Simkin	Alexandre Wallet
Adrian Ranea	Luisa Siniscalchi	Haoyang Wang
Shahram Rasoolzadeh	Daniel Slamanig	Hoeteck Wee
Deevashwer Rathee	Benjamin Smith	WeiQiang Wen
Mayank Rathee	Fang Song	Benjamin Wesolowski
Divya Ravi	Jana Sotáková	Jan Wichelmann
Christian Rechberger	Pierre-Jean Spaenlehauer	Luca Wilke
Michael Reichle	Nicholas Spooner	Mary Wootters
Jean-René Reinhard	Akshayaram Srinivasan	David Wu
Joost Renes	Damien Stehlé	Jiayu Xu
Nicolas Resch	Marc Stevens	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 II

### Symmetric Designs

CIMINION: Symmetric Encryption Based on Toffoli-Gates over Large Finite Fields . . . . .	3
<i>Christoph Dobraunig, Lorenzo Grassi, Anna Guinet, and Daniël Kuijsters</i>	
Mind the Middle Layer: The HADES Design Strategy Revisited. . . . .	35
<i>Nathan Keller and Asaf Rosemarin</i>	
Password Hashing and Preprocessing. . . . .	64
<i>Pooya Farshim and Stefano Tessaro</i>	
Compactness of Hashing Modes and Efficiency Beyond Merkle Tree . . . . .	92
<i>Elena Andreeva, Rishiraj Bhattacharyya, and Arnab Roy</i>	

### Real-World Cryptanalysis

Three Third Generation Attacks on the Format Preserving Encryption Scheme FF3 . . . . .	127
<i>Ohad Amon, Orr Dunkelman, Nathan Keller, Eyal Ronen, and Adi Shamir</i>	
Cryptanalysis of the GPRS Encryption Algorithms GEA-1 and GEA-2 . . . . .	155
<i>Christof Beierle, Patrick Derbez, Gregor Leander, Gaëtan Leurent, Håvard Raddum, Yann Rotella, David Rupprecht, and Lukas Stennes</i>	

### Implementation Issues

Pre-computation Scheme of Window $\tau$ NAF for Koblitz Curves Revisited . . .	187
<i>Wei Yu and Guangwu Xu</i>	
Dummy Shuffling Against Algebraic Attacks in White-Box Implementations . . . . .	219
<i>Alex Biryukov and Aleksei Udovenko</i>	
Advanced Lattice Sieving on GPUs, with Tensor Cores . . . . .	249
<i>Léo Ducas, Marc Stevens, and Wessel van Woerden</i>	

**Masking and Secret-Sharing**

Fast Verification of Masking Schemes in Characteristic Two . . . . . 283  
*Nicolas Bordes and Pierre Karpman*

On the Power of Expansion: More Efficient Constructions in the Random Probing Model . . . . . 313  
*Sonia Belaïd, Matthieu Rivain, and Abdul Rahman Taleb*

Leakage-Resilience of the Shamir Secret-Sharing Scheme Against Physical-Bit Leakages . . . . . 344  
*Hemanta K. Maji, Hai H. Nguyen, Anat Paskin-Cherniavsky, Tom Suad, and Mingyuan Wang*

**Leakage, Faults and Tampering**

Leakage Resilient Value Comparison with Application to Message Authentication . . . . . 377  
*Christoph Dobraunig and Bart Mennink*

The Mother of All Leakages: How to Simulate Noisy Leakages via Bounded Leakage (Almost) for Free. . . . . 408  
*Gianluca Brian, Antonio Faonio, Maciej Obremski, João Ribeiro, Mark Simkin, Maciej Skórski, and Daniele Venturi*

Message-Recovery Laser Fault Injection Attack on the *Classic McEliece* Cryptosystem . . . . . 438  
*Pierre-Louis Cayrel, Brice Colombier, Vlad-Florin Drăgoi, Alexandre Menu, and Lilian Bossuet*

Multi-source Non-malleable Extractors and Applications . . . . . 468  
*Vipul Goyal, Akshayaram Srinivasan, and Chenzhi Zhu*

**Quantum Constructions and Proofs**

Secure Software Leasing . . . . . 501  
*Prabhanjan Ananth and Rolando L. La Placa*

Oblivious Transfer Is in MiniQCrypt. . . . . 531  
*Alex B. Grilo, Huijia Lin, Fang Song, and Vinod Vaikuntanathan*

Security Analysis of Quantum Lightning . . . . . 562  
*Bhaskar Roberts*

Classical vs Quantum Random Oracles . . . . . 568  
*Takashi Yamakawa and Mark Zhandry*

On the Compressed-Oracle Technique, and Post-Quantum Security  
of Proofs of Sequential Work . . . . . 598  
*Kai-Min Chung, Serge Fehr, Yu-Hsuan Huang, and Tai-Ning Liao*

Classical Proofs of Quantum Knowledge . . . . . 630  
*Thomas Vidick and Tina Zhang*

**Multiparty Computation**

Order-C Secure Multiparty Computation for Highly Repetitive Circuits . . . . . 663  
*Gabrielle Beck, Aarushi Goel, Abhishek Jain, and Gabriel Kaptchuk*

The More the Merrier: Reducing the Cost of Large Scale MPC . . . . . 694  
*S. Dov Gordon, Daniel Starin, and Arkady Yerukhimovich*

Multiparty Reusable Non-interactive Secure Computation from LWE . . . . . 724  
*Fabrice Benhamouda, Aayush Jain, Ilan Komargodski, and Huijia Lin*

Unbounded Multi-party Computation from Learning with Errors. . . . . 754  
*Prabhanjan Ananth, Abhishek Jain, Zhengzhong Jin,  
and Giulio Malavolta*

Generic Compiler for Publicly Verifiable Covert Multi-Party Computation . . . . . 782  
*Sebastian Faust, Carmit Hazay, David Kretzler, and Benjamin Schlosser*

Constant-Overhead Unconditionally Secure Multiparty Computation Over  
Binary Fields . . . . . 812  
*Antigoni Polychroniadou and Yifan Song*

Breaking the Circuit Size Barrier for Secure Computation Under  
Quasi-Polynomial LPN . . . . . 842  
*Geoffroy Couteau and Pierre Meyer*

Function Secret Sharing for Mixed-Mode and Fixed-Point Secure  
Computation. . . . . 871  
*Elette Boyle, Nishanth Chandran, Niv Gilboa, Divya Gupta, Yuval Ishai,  
Nishant Kumar, and Mayank Rathee*

VOLE-PSI: Fast OPRF and Circuit-PSI from Vector-OLE . . . . . 901  
*Peter Rindal and Phillipp Schoppmann*

**Author Index** . . . . . 931