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

Springer

Lecture Notes in Computer Science 12697

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

Springer

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

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, Tancrède 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	Radboud University, The Netherlands
Stjepan Picek	Delft University of Technology, The Netherlands

Program Committee Chairs

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

Tuong-Huy Nguyen
Jesper Buus Nielsen
Ryo Nishimaki
Abderrahmane Nitaj
Anca Nitulescu
Lamine Noureddine
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
Krzyszof 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 Vauclair
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 II

Masking and Secret-Sharing

Leakage, Faults and Tampering

Quantum Constructions and Proofs