

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

Moti Yung 

Columbia University, New York, NY, USA

More information about this series at <https://link.springer.com/bookseries/558>

Orr Dunkelman · Stefan Dziembowski (Eds.)

Advances in Cryptology – EUROCRYPT 2022

41st Annual International Conference on the Theory
and Applications of Cryptographic Techniques
Trondheim, Norway, May 30 – June 3, 2022
Proceedings, Part III

Editors

Orr Dunkelman 
University of Haifa
Haifa, Haifa, Israel

Stefan Dziembowski 
University of Warsaw
Warsaw, Poland

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-031-07081-5 ISBN 978-3-031-07082-2 (eBook)
<https://doi.org/10.1007/978-3-031-07082-2>

© International Association for Cryptologic Research 2022

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 Annual International Conference on the Theory and Applications of Cryptographic Techniques, Eurocrypt 2022, was held in Trondheim, Norway. Breaking tradition, the conference started on the evening of Monday, May 30, and ended at noon on Friday, June 3, 2022. Eurocrypt is one of the three flagship conferences of the International Association for Cryptologic Research (IACR), which sponsors the event. Colin Boyd (NTNU, Norway) was the general chair of Eurocrypt 2022 who took care of all the local arrangements.

The 372 anonymous submissions we received in the IACR HotCRP system were each reviewed by at least three of the 70 Program Committee members (who were allowed at most two submissions). We used a rebuttal round for all submissions. After a lengthy and thorough review process, 85 submissions were selected for publication. The revised versions of these submissions can be found in these three-volume proceedings.

In addition to these papers, the committee selected the “EpiGRAM: Practical Garbled RAM” by David Heath, Vladimir Kolesnikov, and Rafail Ostrovsky for the best paper award. Two more papers — “On Building Fine-Grained One-Way Functions from Strong Average-Case Hardness” and “Quantum Algorithms for Variants of Average-Case Lattice Problems via Filtering” received an invitation to the Journal of Cryptology. Together with presentations of the 85 accepted papers, the program included two invited talks: The IACR distinguished lecture, carried by Ingrid Verbauwhede, on “Hardware: an essential partner to cryptography”, and “Symmetric Cryptography for Long Term Security” by María Naya-Plasencia.

We would like to take this opportunity to thank numerous people. First of all, the authors of all submitted papers, whether they were accepted or rejected. The Program Committee members who read, commented, and debated the papers generating more than 4,500 comments(!) in addition to a large volume of email communications. The review process also relied on 368 subreviewers (some of which submitted more than one subreview). We cannot thank you all enough for your hard work.

A few individuals were extremely helpful in running the review process. First and foremost, Kevin McCurley, who configured, solved, answered, re-answered, supported, and did all in his (great) power to help with the IACR system. Wkdqn Brx! We are also extremely grateful to Gaëtan Leurent for offering his wonderful tool to make paper assignment an easy task. The wisdom and experience dispensed by Anne Canteaut, Itai Dinur, Bart Preneel, and François-Xavier Standaert are also noteworthy and helped usher the conference into a safe haven. Finally, we wish to thank the area chairs—Sonia Belaïd, Carmit Hazay, Thomas Peyrin, Nigel Smart, and Martijn Stam. You made our work manageable.

Finally, we thank all the people who were involved in the program of Eurocrypt 2022: the rump session chairs, the session chairs, the speakers, and all the technical support staff in Trondheim. We would also like to mention the various sponsors and thank them

for the generous support. We wish to thank the continuous support of the Cryptography Research Fund for supporting student speakers.

May 2022

Orr Dunkelman
Stefan Dziembowski

Organization

The 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt 2022)

Sponsored by the *International Association for Cryptologic Research*
Trondheim, Norway
May 30 – June 3, 2022

General Chair

Colin Boyd

NTNU, Norway

Program Chairs

Orr Dunkelman

University of Haifa, Israel

Stefan Dziembowski

University of Warsaw, Poland

Program Committee

Masayuki Abe

NTT Laboratories, Japan

Shashank Agrawal

Western Digital Research, USA

Joël Alwen

AWS Wickr, Austria

Marshall Ball

New York University, USA

Gustavo Banegas

Inria and Institut Polytechnique de Paris, France

Paulo Barreto

University of Washington Tacoma, USA

Sonia Belaïd

CryptoExperts, France

Jean-François Biasse

University of South Florida, USA

Begül Bilgin

Rambus Cryptography Research, The Netherlands

Alex Biryukov

University of Luxembourg, Luxembourg

Olivier Blazy

Ecole Polytechnique, France

Billy Bob Brumley

Tampere University, Finland

Chitchanok Chuengsatiansup

University of Adelaide, Australia

Michele Ciampi

University of Edinburgh, UK

Ran Cohen

IDC Herzliya, Israel

Henry Corrigan-Gibbs

Massachusetts Institute of Technology, USA

Cas Cremers

CISPA Helmholtz Center for Information
Security, Germany

Dana Dachman-Soled

University of Maryland, USA

Jean Paul Degabriele

TU Darmstadt, Germany

Itai Dinur

Ben-Gurion University, Israel

Rafael Dowsley	Monash University, Australia
Antonio Faonio	EURECOM, France
Pooya Farshim	Durham University, UK
Sebastian Faust	TU Darmstadt, Germany
Ben Fuller	University of Connecticut, USA
Pierrick Gaudry	Loria, France
Esha Ghosh	Microsoft Research, Redmond, USA
Paul Grubbs	University of Michigan, USA
Divya Gupta	Microsoft Research India, India
Felix Günther	ETH Zurich, Switzerland
Iftach Haitner	Tel Aviv University, Israel
Shai Halevi	Algorand Foundation, USA
Carmit Hazay	Bar-Ilan University, Israel
Pavel Hubáček	Charles University, Czech Republic
Tibor Jager	University of Wuppertal, Germany
Dmitry Khovratovich	Ethereum Foundation, Luxembourg
Gregor Leander	Ruhr University Bochum, Germany
Gaëtan Leurent	Inria, France
Helger Lipmaa	Simula UiB, Norway
Shengli Liu	Shanghai Jiao Tong University, China
Alex Lombardi	Massachusetts Institute of Technology, USA
Hemanta K. Maji	Purdue University, USA
Giulio Malavolta	Max Planck Institute for Security and Privacy, Germany
Peihan Miao	University of Illinois at Chicago, USA
Pratyay Mukherjee	Visa Research, USA
David Naccache	ENS Paris, France
Svetla Nikova	KU Leuven, Belgium
Miyako Ohkubo	National Institute of Information and Communications, Japan
Arpita Patra	Indian Institute of Science, India
Alice Pellet-Mary	CNRS and University of Bordeaux, France
Thomas Peyrin	Nanyang Technological University, Singapore
Josef Pieprzyk	CSIRO Data61, Australia, and Institute of Computer Science, PAS, Poland
Bertram Poettering	IBM Research Europe - Zurich, Switzerland
Peter Rindal	Visa Research, USA
Carla Ràfols	Universitat Pompeu Fabra, Spain
Amin Sakzad	Monash University, Australia
Alessandra Scafuro	North Carolina State University, USA
Nigel Smart	KU Leuven, Belgium
Martijn Stam	Simula UiB, Norway

Meltem Sönmez Turan

National Institute of Standards and Technology,
USA

Daniele Venturi

Sapienza University of Rome, Italy

Ivan Visconti

University of Salerno, Italy

Gaoli Wang

East China Normal University, China

Stefan Wolf

University of Italian Switzerland, Switzerland

Sophia Yakoubov

Aarhus University, Denmark

Avishay Yanai

VMware Research, Israel

Bo-Yin Yang

Academia Sinica, Taiwan

Arkady Yerukhimovich

George Washington University, USA

Yu Yu

Shanghai Jiao Tong University, China

Mark Zhandry

NTT Research and Princeton University, USA

Subreviewers

Behzad Abdolmaleki

Christof Beierle

Ittai Abraham

Pascal Bemmman

Damiano Abram

Fabrice Benhamouda

Anasuya Acharya

Francesco Berti

Alexandre Adomnicai

Tim Beyne

Amit Agarwal

Rishabh Bhadauria

Shweta Agrawal

Adithya Bhat

Thomas Agrikola

Sai Lakshmi Bhavana Obbattu

Akshima

Alexander Bienstock

Navid Alamati

Erica Blum

Alejandro Cabrera Aldaya

Jan Bobolz

Bar Alon

Xavier Bonnetain

Miguel Ambrona

Cecilia Boschini

Hiroaki Anada

Raphael Bost

Diego F. Aranha

Vincenzo Botta

Victor Arribas

Katharina Boudgoust

Tomer Ashur

Christina Boura

Gennaro Avitabile

Zvika Brakerski

Matilda Backendal

Luís Brandão

Saikrishna Badrinarayanan

Lennart Braun

Shi Bai

Jacqueline Brendel

Ero Balsa

Gianluca Brian

Augustin Bariant

Anne Broadbent

James Bartusek

Marek Broll

Balthazar Bauer

Christopher Brzuska

Carsten Baum

Chloe Cachet

Ämin Baumeler

Matteo Campanelli

Arthur Beckers

Federico Canale

Charles Bédard

Anne Canteaut

Ignacio Cascudo
 Andre Chailloux
 Nishanth Chandran
 Donghoon Chang
 Binyi Chen
 Shan Chen
 Weikeng Chen
 Yilei Chen
 Jung Hee Cheon
 Jesus-Javier Chi-Dominguez
 Seung Geol Choi
 Wutichai Chongchitmate
 Arka Rai Choudhuri
 Sherman S. M. Chow
 Jeremy Clark
 Xavier Coiteux-Roy
 Andrea Coladangelo
 Nan Cui
 Benjamin R. Curtis
 Jan Czajkowski
 Jan-Pieter D’Anvers
 Hila Dahari
 Thinh Dang
 Quang Dao
 Poulami Das
 Pratish Datta
 Bernardo David
 Gareth T. Davies
 Hannah Davis
 Lauren De Meyer
 Gabrielle De Micheli
 Elke De Mulder
 Luke Demarest
 Julien Devevey
 Siemen Dhooghe
 Denis Diemert
 Jintai Ding
 Jack Doerner
 Xiaoyang Dong
 Nico Döttling
 Benjamin Dowling
 Yang Du
 Leo Ducas
 Julien Duman
 Betul Durak

Oğuzhan Ersoy
 Andreas Erwig
 Daniel Escudero
 Muhammed F. Esgin
 Saba Eskandarian
 Prastudy Fauzi
 Patrick Felke
 Thibault Feneuil
 Peter Fenteany
 Diodato Ferraioli
 Marc Fischlin
 Nils Fleischhacker
 Cody Freitag
 Daniele Friolo
 Tommaso Gagliardoni
 Steven D. Galbraith
 Pierre Galissant
 Chaya Ganesh
 Cesar Pereida García
 Romain Gay
 Kai Gellert
 Craig Gentry
 Marilyn George
 Hossein Ghodosi
 Satrajit Ghosh
 Jan Gilcher
 Aarushi Goel
 Eli Goldin
 Junqing Gong
 Dov Gordon
 Jérôme Govinden
 Lorenzo Grassi
 Johann Großschädl
 Jiaxin Guan
 Daniel Guenther
 Milos Gujic
 Qian Guo
 Cyril Guyot
 Mohammad Hajiabadi
 Ariel Hamlin
 Shuai Han
 Abida Haque
 Patrick Harasser
 Dominik Hartmann
 Phil Hebborn

Alexandra Henzinger
 Javier Herranz
 Julia Hesse
 Justin Holmgren
 Akinori Hosoyamada
 Kai Hu
 Andreas Hülsing
 Shih-Han Hung
 Vincenzo Iovino
 Joseph Jaeger
 Aayush Jain
 Christian Janson
 Samuel Jaques
 Stanislaw Jarecki
 Corentin Jeudy
 Zhengzhong Jin
 Daniel Jost
 Saqib Kakvi
 Vukašin Karadžić
 Angshuman Karmakar
 Shuichi Katsumata
 Jonathan Katz
 Mahimna Kelkar
 Nathan Keller
 John Kelsey
 Mustafa Khairallah
 Hamidreza Amini Khorasgani
 Dongwoo Kim
 Miran Kim
 Elena Kirshanova
 Fuyuki Kitagawa
 Michael Klooß
 Sebastian Kolby
 Lukas Kölsch
 Yashvanth Kondi
 David Kretzler
 Veronika Kuchta
 Marie-Sarah Lacharité
 Yi-Fu Lai
 Baptiste Lambin
 Mario Larangeira
 Rio LaVigne
 Quoc-Huy Le
 Jooyoung Lee
 Julia Len

Antonin Leroux
 Hanjun Li
 Jianwei Li
 Yiming Li
 Xiao Liang
 Damien Ligier
 Chengyu Lin
 Dongxi Liu
 Jiahui Liu
 Linsheng Liu
 Qipeng Liu
 Xiangyu Liu
 Chen-Da Liu Zhang
 Julian Loss
 Vadim Lyubashevsky
 Lin Lyu
 You Lyu
 Fermi Ma
 Varun Madathil
 Akash Madhusudan
 Bernardo Magri
 Monosij Maitra
 Nikolaos Makriyannis
 Mary Maller
 Giorgia Marson
 Christian Matt
 Noam Mazor
 Nikolas Melissaris
 Bart Mennink
 Antonis Michalas
 Brice Minaud
 Kazuhiko Minematsu
 Alberto Montina
 Amir Moradi
 Marta Mularczyk
 Varun Narayanan
 Jade Nardi
 Patrick Neumann
 Ruth Ng
 Hai H. Nguyen
 Kirill Nikitin
 Ryo Nishimaki
 Anca Nitulescu
 Ariel Nof
 Julian Nowakowski

Adam O'Neill
 Maciej Obremski
 Eran Omri
 Maximilian Orlt
 Bijeeta Pal
 Jiaxin Pan
 Omer Paneth
 Lorenz Panny
 Dimitrios Papadopoulos
 Jeongeun Park
 Anat Paskin-Cherniavsky
 Sikhar Patranabis
 Marcin Pawłowski
 Hilder Pereira
 Ray Perlner
 Clara Pernot
 Léo Perrin
 Giuseppe Persiano
 Edoardo Persichetti
 Albrecht Petzoldt
 Duong Hieu Phan
 Krzysztof Pietrzak
 Jeroen Pijnenburg
 Rachel Player
 Antigoni Polychroniadou
 Willy Quach
 Anaïs Querol
 Srinivasan Raghuraman
 Adrián Ranea
 Simon Rastikian
 Divya Ravi
 Francesco Regazzoni
 Maryam Rezapour
 Mir Ali Rezazadeh Bae
 Siavash Riahi
 Joao Ribeiro
 Vincent Rijmen
 Bhaskar Roberts
 Francisco Rodriguez-Henríquez
 Paul Rösler
 Arnab Roy
 Iftekhar Salam
 Paolo Santini
 Roozbeh Sarenche
 Yu Sasaki

Matteo Scarlata
 Tobias Schmalz
 Mahdi Sedaghat
 Vladimir Sedlacek
 Nicolas Sendrier
 Jae Hong Seo
 Srinath Setty
 Yaobin Shen
 Sina Shiehian
 Omri Shmueli
 Janno Siim
 Jad Silbak
 Leonie Simpson
 Rohit Sinha
 Daniel Slamanig
 Fang Song
 Yongsoo Song
 Damien Stehle
 Ron Steinfeld
 Noah Stephens-Davidowitz
 Christoph Striecks
 Fatih Sulak
 Chao Sun
 Ling Sun
 Siwei Sun
 Koutarou Suzuki
 Katsuyuki Takashima
 Hervé Tale Kalachi
 Quan Quan Tan
 Yi Tang
 Je Sen Teh
 Cihangir Tezcan
 Aishwarya Thiruvengadam
 Orfeas Thyfronitis
 Mehdi Tibouchi
 Ni Trieu
 Yiannis Tselekounis
 Michael Tunstall
 Nicola Tuveri
 Nirvan Tyagi
 Sohaib ul Hassan
 Wessel van Woerden
 Kerem Varc
 Prashant Vasudevan
 Damien Vergnaud

Jorge L. Villar
 Giuseppe Vitto
 Sameer Wagh
 Hendrik Waldner
 Alexandre Wallet
 Ming Wan
 Xiao Wang
 Yuyu Wang
 Zhedong Wang
 Hoeteck Wee
 Mor Weiss
 Weiqiang Wen
 Daniel Wicks
 Mathias Wolf
 Lennert Wouters
 Michał Wroński
 David Wu
 Yusai Wu
 Keita Xagawa
 Yu Xia

Zejun Xiang
 Tiancheng Xie
 Shota Yamada
 Takashi Yamakawa
 Lisa Yang
 Kevin Yeo
 Eylon Yogev
 Kazuki Yoneyama
 Yusuke Yoshida
 William Youmans
 Alexandros Zacharakis
 Michał Zając
 Arantxa Zapico
 Greg Zaverucha
 Shang Zehua
 Tina Zhang
 Wentao Zhang
 Yinuo Zhang
 Yu Zhou
 Cong Zuo

Contents – Part III

Symmetric-Key Cryptanalysis

Key Guessing Strategies for Linear Key-Schedule Algorithms in Rectangle Attacks	3
<i>Xiaoyang Dong, Lingyue Qin, Siwei Sun, and Xiaoyun Wang</i>	
A Correlation Attack on Full SNOW-V and SNOW-Vi	34
<i>Zhen Shi, Chenhui Jin, Jiyan Zhang, Ting Cui, Lin Ding, and Yu Jin</i>	
Refined Cryptanalysis of the GPRS Ciphers GEA-1 and GEA-2	57
<i>Dor Amzaleg and Itai Dinur</i>	
Revamped Differential-Linear Cryptanalysis on Reduced Round ChaCha	86
<i>Sabyasachi Dey, Hirendra Kumar Garai, Santanu Sarkar, and Nitin Kumar Sharma</i>	
A Greater GIFT: Strengthening GIFT Against Statistical Cryptanalysis	115
<i>Ling Sun, Bart Preneel, Wei Wang, and Meiqin Wang</i>	

Side Channel Attacks and Masking

Approximate Divisor Multiples – Factoring with Only a Third of the Secret CRT-Exponents	147
<i>Alexander May, Julian Nowakowski, and Santanu Sarkar</i>	
Information-Combining Differential Fault Attacks on DEFAULT	168
<i>Marcel Nageler, Christoph Dobraunig, and Maria Eichlseder</i>	
Private Circuits with Quasilinear Randomness	192
<i>Vipul Goyal, Yuval Ishai, and Yifan Song</i>	
MITAKA: A Simpler, Parallelizable, Maskable Variant of FALCON	222
<i>Thomas Espitau, Pierre-Alain Fouque, François Gérard, Mélissa Rossi, Akira Takahashi, Mehdi Tibouchi, Alexandre Wallet, and Yang Yu</i>	
A Novel Completeness Test for Leakage Models and Its Application to Side Channel Attacks and Responsibly Engineered Simulators	254
<i>Si Gao and Elisabeth Oswald</i>	

Towards Micro-architectural Leakage Simulators: Reverse Engineering Micro-architectural Leakage Features Is Practical	284
<i>Si Gao, Elisabeth Oswald, and Dan Page</i>	

Post-Quantum Cryptography

Beyond Quadratic Speedups in Quantum Attacks on Symmetric Schemes	315
<i>Xavier Bonnetain, André Schrottenloher, and Ferdinand Sibleyras</i>	

Orientations and the Supersingular Endomorphism Ring Problem	345
<i>Benjamin Wesolowski</i>	

Quantum Algorithms for Variants of Average-Case Lattice Problems via Filtering	372
<i>Yilei Chen, Qipeng Liu, and Mark Zhandry</i>	

Anonymous, Robust Post-quantum Public Key Encryption	402
<i>Paul Grubbs, Varun Maram, and Kenneth G. Paterson</i>	

McEliece Needs a Break – Solving McEliece-1284 and Quasi-Cyclic-2918 with Modern ISD	433
<i>Andre Esser, Alexander May, and Floyd Zveydinger</i>	

Post-Quantum Security of the Even-Mansour Cipher	458
<i>Gorjan Alagic, Chen Bai, Jonathan Katz, and Christian Majenz</i>	

Watermarking PRFs Against Quantum Adversaries	488
<i>Fuyuki Kitagawa and Ryo Nishimaki</i>	

Non-malleable Commitments Against Quantum Attacks	519
<i>Nir Bitansky, Huijia Lin, and Omri Shmueli</i>	

Anonymity of NIST PQC Round 3 KEMs	551
<i>Keita Xagawa</i>	

Practical Post-Quantum Signature Schemes from Isomorphism Problems of Trilinear Forms	582
<i>Gang Tang, Dung Hoang Duong, Antoine Joux, Thomas Plantard, Youming Qiao, and Willy Susilo</i>	

On IND-qCCA Security in the ROM and Its Applications: CPA Security Is Sufficient for TLS 1.3	613
<i>Loïs Huguénin-Dumittan and Serge Vaudenay</i>	

On the Lattice Isomorphism Problem, Quadratic Forms, Remarkable Lattices, and Cryptography	643
<i>Léo Ducas and Wessel van Woerden</i>	

Information-Theoretic Security

Online-Extractability in the Quantum Random-Oracle Model	677
<i>Jelle Don, Serge Fehr, Christian Majenz, and Christian Schaffner</i>	
Constant-Round Blind Classical Verification of Quantum Sampling	707
<i>Kai-Min Chung, Yi Lee, Han-Hsuan Lin, and Xiaodi Wu</i>	
Authentication in the Bounded Storage Model	737
<i>Yevgeniy Dodis, Willy Quach, and Daniel Wichs</i>	
Secure Non-interactive Simulation: Feasibility and Rate	767
<i>Hamidreza Amini Khorasgani, Hemanta K. Maji, and Hai H. Nguyen</i>	
Secure Non-interactive Reduction and Spectral Analysis of Correlations	797
<i>Pratyush Agarwal, Varun Narayanan, Shreya Pathak, Manoj Prabhakaran, Vinod M. Prabhakaran, and Mohammad Ali Rehan</i>	
Author Index	829