

## 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>

Juan A. Garay (Ed.)

# Public-Key Cryptography – PKC 2021

24th IACR International Conference  
on Practice and Theory of Public Key Cryptography  
Virtual Event, May 10–13, 2021  
Proceedings, Part II

*Editor*

Juan A. Garay 

Texas A&M University

College Station, TX, USA

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-030-75247-7

ISBN 978-3-030-75248-4 (eBook)

<https://doi.org/10.1007/978-3-030-75248-4>

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

The 24th International Conference on Practice and Theory of Public-Key Cryptography (PKC 2021) was held virtually over Zoom from May 10th to May 13th, 2021. It was supposed to take place in Edinburgh, Scotland, but due to COVID-19 this was not possible. The conference is organized annually by the International Association for Cryptologic Research (IACR), and is the main annual conference with an explicit focus on public-key cryptography. Given NIST's efforts on standardization of post-quantum cryptography, this year constructions and cryptanalysis in this area were specially encouraged. These proceedings are comprised of two volumes and include the 52 papers that were selected by the Program Committee (PC), as well as a one-page abstract corresponding to one of the two invited talks, which reflect this year's focus.

The 52 accepted papers were selected out of a total of 156 received submissions. Submissions were assigned to at least three reviewers, while submissions by PC members received at least four reviews. Due to time constraints, the review period this year did not include a rebuttal step, where the authors get a chance to preview their papers' preliminary reviews. The review process, however, was fairly interactive, as in a large number of occasions reviewers posed questions to the authors. Six of the accepted papers were first conditionally accepted and received an additional round of reviewing; in addition, two of the papers were "soft merged" due to the similarity of results and shared one presentation slot.

Given the high number and quality of the submissions, the reviewing and paper selection process was a challenging task and I am deeply grateful to the members of the PC for their high dedication and thorough work. In addition to the PC members, many external reviewers joined the review process in their particular areas of expertise. We were fortunate to have this knowledgeable and energetic team of experts, and I am deeply grateful to all of them for their contributions. The submissions included two papers with which I had a conflict of interest (they were authored by current and/or close collaborators). For these two papers I abstained from the management of the discussion and delegated this task to a PC member. Many thanks to Hoeteck Wee and Vassilis Zikas, respectively, for their help in managing these two papers.

The paper submission, review and discussion processes were effectively and efficiently made possible by the Web-Submission-and-Review software, written by Shai Halevi, and hosted by the IACR. As always, many thanks to Shai for his assistance with the system's various features.

This year the program was further enriched by two invited talks by Léo Ducas (CWI, the Netherlands; "Lattices and Factoring") and Eike Kiltz (Ruhr-Universität Bochum, Germany; "How Provably Secure are (EC)DSA Signatures?"). My special thanks to Léo and Eike for accepting the invitation and great presentations.

I am also grateful for their predisposition, availability, and efforts (unfortunately not fully realized when we decided to go virtual) to Markulf Kohlweiss and Petros Wallden, who served as General Co-chairs, and to Dimitris Karakostas (all from The

University of Edinburgh), who managed the conference's website. I finally thank all the authors who submitted papers to this conference, and all the conference attendees who made this event a truly intellectually stimulating one through their active (albeit remote) participation.

Next time, Edinburgh!

March 2021

Juan A. Garay



Giorgos Panagiotakos	University of Athens, Greece
Alice Pellet-Mary	KUL, Belgium
Christophe Petit	University of Birmingham, UK
Bertram Poettering	IBM Research, Switzerland
Melissa Rossi	ANSSI, France
Olivier Sanders	Orange Labs, France
Berry Schoenmakers	TU Eindhoven, the Netherlands
Fang Song	Portland State University, USA
Akshayaram Srinivasan	Tata Institute of Fundamental Research, India
Qiang Tang	The University of Sydney, Australia
Hoeteck Wee	NTT Research and ENS, France
Vassilis Zikas	Purdue University, USA

## Sponsoring Institutions

The Scottish Informatics and Computer Science Alliance (SICSA) Cyber Nexus  
 INPUT|OUTPUT  
 DFINITY

## External Reviewers

Behzad Abdolmaleki	Jérémy Chotard	Romain Gay
Ojaswi Acharya	Ran Cohen	Nicholas Genise
Thomas Attema	Orel Cosserson	Riddhi Ghosal
Nuttapong Attrapadung	Geoffroy Couteau	Huijing Gong
Reza Azarderakhsh	Daniele Cozzo	Junqing Gong
Karim Bagheri	Gareth Davies	Rishab Goyal
Shi Bai	Yi Deng	Vipul Goyal
James Bartusek	Jintai Ding	François Gérard
Andrea Basso	Ehsan Ebrahimi	Mohammad Hajiabadi
Carsten Baum	Keita Emura	Shai Halevi
Ward Beullens	Thomas Espitau	Mike Hamburg
Olivier Blazy	Leo Fan	Kyoohyung Han
Charlotte Bonte	Antonio Faonio	Patrick Harasser
Jonathan Bootle	Thibault Feneuil	Brett Hemenway
Pedro Branco	Hanwen Feng	Julia Hesse
Konstantinos Brazitikos	Weiqi Feng	Minki Hhan
Xavier Bultel	Luca De Feo	Seungwan Hong
Sébastien Canard	Rex Fernando	Yuncong Hu
Wouter Castryk	Ben Fisch	Andreas Hlsing
Jie Chen	Boris Fouotsa	Muhammad Ishaq
Long Chen	Pierre-Alain Fouque	David Jao
Yu Chen	Phillip Gajland	Sam Jaques
Benoit Chevallier-Mames	Chaya Ganesh	Stanislaw Jarecki
Wonhee Cho	Rachit Garg	Dingding Jia



Zhengzhong Jin	Hiraku Morita	Yongha Son
Daniel Jost	Michael Naehrig	Yongsoo Song
Bhavana Kanukurthi	Anderson Nascimento	Florian Speelman
Harish Karthikeyan	Khoa Nguyen	Martijn Stam
John Kelsey	Ngoc Khanh Nguyen	Yiru Sun
Dongwoo Kim	Anca Nitulescu	Katsuyuki Takashima
Duhyeong Kim	Martha Hovd Norberg	Samuel Tap
Jiseung Kim	Hiroshi Onuki	Aravind Thyagarajan
Fuyuki Kitagawa	Michele Orr	Song Tian
Susumu Kiyoshima	Jiaxin Pan	Jacques Traoré
Michael Klooss	Bo Pang	Yiannis Tselekounis
Yashvanth Kondi	Louiza Papachristodoulou	Bogdan Ursu
Brian Koziel	Sikhar Patranabis	Prashant Vasudevan
Hugo Krawczyk	Geovandro Pereira	Hendrik Waldner
Mukul Kulkarni	Ray Perlner	Alexandre Wallet
Nishant Kumar	Federico Pintore	Hailong Wang
Péter Kutas	Bernardo Portela	Luping Wang
Fabien Laguillaumie	Youming Qiao	Yuyu Wang
Qiqi Lai	Tian Qiu	Zhedong Wang
Russel Lai	Willy Quach	Charlotte Weitkämper
Anja Lehmann	Srinivasan Raghuraman	Weiqiang Wen
Chengyu Lin	Divya Ravi	Benjamin Wesolowski
Xi Lin	Lo Robert	David Wu
Yanyan Liu	Angela Robinson	Keita Xagawa
Chen-Da Liu-Zhang	Miruna Rosca	Tiancheng Xie
George Lu	Paul Rösler	Anshu Yadav
Steve Lu	Yusuke Sakai	Sophia Yakoubov
Yun Lu	Dimitris Sakavalas	Shota Yamada
Zhenliang Lu	Peter Scholl	Takashi Yamakawa
Fermi Ma	Jacob Schuldt	Avishay Yanai
Shunli Ma	Rebecca Schwerdt	Kazuki Yoneyama
Gilles Macario-Rat	Toon Segers	Aaram Yun
Christian Majenz	Gregor Seiler	Thomas Zacharias
Nathan Manohar	Yannick Seurin	Mohammad Zaheri
Ange Martinelli	Akash Shah	Cong Zhang
Simon-Philipp Merz	Sina Shiehian	Jiaheng Zhang
Romy Minko	Luisa Siniscalchi	Kai Zhang
Dustin Moody	Daniel Smith-Tone	Yongjun Zhao

# Lattices and Factoring

## (Abstract of Invited Talk)

Léo Ducas

Cryptology Group, Centrum Wiskunde & Informatica, Amsterdam,  
The Netherlands

**Abstract.** In this talk, I would like to re-popularize two dual ideas that relate Lattices and Factoring. Such a connection may appear surprising at first, but is only one logarithm away: after all, factoring is nothing more than a *multiplicative* knapsack problem, i.e. a subset product problem, where the weights are given by the set of small enough primes.

The first of the two ideas, we owe to Schnorr (1991) and to Adleman (1995). It consists in finding close or short vectors in a carefully crafted lattice, in the hope that they will provide so-called factoring relations. While this idea does not appear to lead to faster factoring algorithms, it remains fascinating and has in fact lead to other major results. Indeed, the Schnorr-Adleman lattice plays a key role in the proof by Ajtai (1998) of the NP-hardness of the shortest vector problem.

The second idea, due to Chor and Rivest (1988) shows a reverse connection: constructing the lattice this time using *discrete* logarithms, they instead solve the bounded distance decoding (BDD) problem through easy factoring instances. Revisiting their idea, Pierrot and I (2018) showed that this was a quite close to an optimal construction for solving BDD in polynomial time. It was in fact the best known such construction until some recent work by Peikert and Mook (2020).

I wish to conclude with an invitation to explore the cryptographic potential of other lattices than the random  $q$ -ary lattices—the lattices underlying the Learning with Error problem (LWE) and the Short Integer Solution problem (SIS). While SIS and LWE have shown to be very convenient for constructing the most advanced schemes and protocols, I believe that more general lattices have a yet untapped potential for cryptography.

## Contents – Part II

More Efficient Digital Signatures with Tight Multi-user Security. . . . .	1
<i>Denis Diemert, Kai Gellert, Tibor Jager, and Lin Lyu</i>	
Multiparty Cardinality Testing for Threshold Private Intersection . . . . .	32
<i>Pedro Branco, Nico Döttling, and Sihang Pu</i>	
Verifiable Random Functions with Optimal Tightness . . . . .	61
<i>David Niehues</i>	
A Geometric Approach to Homomorphic Secret Sharing . . . . .	92
<i>Yuval Ishai, Russell W. F. Lai, and Giulio Malavolta</i>	
Generic Negation of Pair Encodings . . . . .	120
<i>Miguel Ambrona</i>	
On Selective-Opening Security of Deterministic Primitives. . . . .	147
<i>Adam O’Neill and Mohammad Zaheri</i>	
Revisiting (R)CCA Security and Replay Protection . . . . .	173
<i>Christian Badertscher, Ueli Maurer, Christopher Portmann, and Guilherme Rito</i>	
<b>Cryptographic Protocols</b>	
Single-to-Multi-theorem Transformations for Non-interactive Statistical Zero-Knowledge . . . . .	205
<i>Marc Fischlin and Felix Rohrbach</i>	
On the CCA Compatibility of Public-Key Infrastructure. . . . .	235
<i>Dakshita Khurana and Brent Waters</i>	
Round-Optimal Verifiable Oblivious Pseudorandom Functions from Ideal Lattices . . . . .	261
<i>Martin R. Albrecht, Alex Davidson, Amit Deo, and Nigel P. Smart</i>	
BETA: Biometric-Enabled Threshold Authentication . . . . .	290
<i>Shashank Agrawal, Saikrishna Badrinarayanan, Payman Mohassel, Pratyay Mukherjee, and Sikhar Patranabis</i>	
Masked Triples: Amortizing Multiplication Triples Across Conditionals. . . . .	319
<i>David Heath, Vladimir Kolesnikov, and Stanislav Peceny</i>	

Multi-party Threshold Private Set Intersection with Sublinear Communication. . . . . 349  
*Saikrishna Badrinarayanan, Peihan Miao, Srinivasan Raghuraman, and Peter Rindal*

On the (In)Security of the Diffie-Hellman Oblivious PRF with Multiplicative Blinding. . . . . 380  
*Stanislaw Jarecki, Hugo Krawczyk, and Jiayu Xu*

An Efficient and Generic Construction for Signal’s Handshake (X3DH): Post-Quantum, State Leakage Secure, and Deniable. . . . . 410  
*Keitaro Hashimoto, Shuichi Katsumata, Kris Kwiatkowski, and Thomas Prest*

Cryptographic Pseudorandom Generators Can Make Cryptosystems Problematic. . . . . 441  
*Koji Nuida*

Publicly Verifiable Zero Knowledge from (Collapsing) Blockchains . . . . . 469  
*Alessandra Scafuro, Luisa Siniscalchi, and Ivan Visconti*

Two-Server Distributed ORAM with Sublinear Computation and Constant Rounds. . . . . 499  
*Ariel Hamlin and Mayank Varia*

Flexible and Efficient Verifiable Computation on Encrypted Data . . . . . 528  
*Alexandre Bois, Ignacio Cascudo, Dario Fiore, and Dongwoo Kim*

Transferable E-Cash: A Cleaner Model and the First Practical Instantiation. . . . . 559  
*Balthazar Bauer, Georg Fuchsbauer, and Chen Qian*

Private Set Operations from Oblivious Switching . . . . . 591  
*Gayathri Garimella, Payman Mohassel, Mike Rosulek, Saeed Sadeghian, and Jaspal Singh*

On Publicly-Accountable Zero-Knowledge and Small Shuffle Arguments. . . . . 618  
*Nils Fleischhacker and Mark Simkin*

Beyond Security and Efficiency: On-Demand Ratcheting with Security Awareness . . . . . 649  
*Andrea Caforio, F. Betül Durak, and Serge Vaudenay*

Group Encryption: Full Dynamicity, Message Filtering and Code-Based Instantiation . . . . . 678  
*Khoa Nguyen, Reihaneh Safavi-Naini, Willy Susilo, Huaxiong Wang, Yanhong Xu, and Neng Zeng*

**Steel: Composable Hardware-Based Stateful and Randomised Functional Encryption** . . . . . 709  
*Pramod Bhatotia, Markulf Kohlweiss, Lorenzo Martinico, and Yiannis Tselekounis*

**Attacks and Cryptanalysis**

Adventures in Crypto Dark Matter: Attacks and Fixes for Weak Pseudorandom Functions . . . . . 739  
*Jung Hee Cheon, Wonhee Cho, Jeong Han Kim, and Jiseung Kim*

**Author Index** . . . . . 761

# Contents – Part I

## Post-Quantum Constructions and Cryptanalysis

QCCA-Secure Generic Key Encapsulation Mechanism with Tighter Security in the Quantum Random Oracle Model . . . . .	3
<i>Xu Liu and Mingqiang Wang</i>	
An Alternative Approach for SIDH Arithmetic . . . . .	27
<i>Cyril Bouvier and Laurent Imbert</i>	
The Convergence of Slide-Type Reductions . . . . .	45
<i>Michael Walter</i>	
On the Success Probability of Solving Unique SVP via BKZ . . . . .	68
<i>Eamonn W. Postlethwaite and Fernando Virdia</i>	
Two-Round $n$ -out-of- $n$ and Multi-signatures and Trapdoor Commitment from Lattices . . . . .	99
<i>Ivan Damgård, Claudio Orlandi, Akira Takahashi, and Mehdi Tibouchi</i>	
Isogeny-Based Key Compression Without Pairings . . . . .	131
<i>Geovandro C. C. F. Pereira and Paulo S. L. M. Barreto</i>	
Analysis of Multivariate Encryption Schemes: Application to Dob . . . . .	155
<i>Morten Øygarden, Patrick Felke, and Håvard Raddum</i>	
On the Integer Polynomial Learning with Errors Problem. . . . .	184
<i>Julien Devevey, Amin Sakzad, Damien Stehlé, and Ron Steinfeld</i>	
Shorter Lattice-Based Zero-Knowledge Proofs via One-Time Commitments. . . . .	215
<i>Vadim Lyubashevsky, Ngoc Khanh Nguyen, and Gregor Seiler</i>	
Multivariate Public Key Cryptosystem from Sidon Spaces . . . . .	242
<i>Netanel Raviv, Ben Langton, and Itzhak Tamo</i>	
Banquet: Short and Fast Signatures from AES . . . . .	266
<i>Carsten Baum, Cyrien Delpèch de Saint Guilhem, Daniel Kales, Emmanuela Orsini, Peter Scholl, and Greg Zaverucha</i>	

## Cryptographic Primitives and Schemes

Improving Revocation for Group Signature with Redactable Signature . . . . .	301
<i>Olivier Sanders</i>	
Bootstrapping Fully Homomorphic Encryption over the Integers in Less than One Second. . . . .	331
<i>Hilder Vitor Lima Pereira</i>	
Group Signatures with User-Controlled and Sequential Linkability . . . . .	360
<i>Jesus Diaz and Anja Lehmann</i>	
Impossibility on Tamper-Resilient Cryptography with Uniqueness Properties. . . . .	389
<i>Yuyu Wang, Takahiro Matsuda, Goichiro Hanaoka, and Keisuke Tanaka</i>	
Rate-1 Key-Dependent Message Security via Reusable Homomorphic Extractor Against Correlated-Source Attacks. . . . .	421
<i>Qiqi Lai, Feng-Hao Liu, and Zhedong Wang</i>	
Two-Party Adaptor Signatures from Identification Schemes . . . . .	451
<i>Andreas Erwig, Sebastian Faust, Kristina Hostáková, Monosij Maitra, and Siavash Riahi</i>	
Compact Zero-Knowledge Proofs for Threshold ECDSA with Trustless Setup . . . . .	481
<i>Tsz Hon Yuen, Handong Cui, and Xiang Xie</i>	
Universal Proxy Re-Encryption. . . . .	512
<i>Nico Döttling and Ryo Nishimaki</i>	
Master-Key KDM-Secure ABE via Predicate Encoding . . . . .	543
<i>Shengyuan Feng, Junqing Gong, and Jie Chen</i>	
Exact Lattice Sampling from Non-Gaussian Distributions. . . . .	573
<i>Maxime Plançon and Thomas Prest</i>	
Efficient Adaptively-Secure IB-KEMs and VRFs via Near-Collision Resistance . . . . .	596
<i>Tibor Jager, Rafael Kurek, and David Niehues</i>	
Subversion-Resilient Public Key Encryption with Practical Watchdogs . . . . .	627
<i>Pascal Bemmman, Rongmao Chen, and Tibor Jager</i>	
Non-interactive CCA2-Secure Threshold Cryptosystems: Achieving Adaptive Security in the Standard Model Without Pairings. . . . .	659
<i>Julien Devevey, Benoît Libert, Khoa Nguyen, Thomas Peters, and Moti Yung</i>	

**Updatable Signatures and Message Authentication Codes** . . . . . 691  
*Valerio Cini, Sebastian Ramacher, Daniel Slamanig, Christoph Striecks,  
and Erkan Tairi*

**Multi-Client Functional Encryption for Separable Functions** . . . . . 724  
*Michele Ciampi, Luisa Siniscalchi, and Hendrik Waldner*

**Author Index** . . . . . 755