

## 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 <https://link.springer.com/bookseries/7410>

Mehdi Tibouchi · Huaxiong Wang (Eds.)

# Advances in Cryptology – ASIACRYPT 2021

27th International Conference on the Theory  
and Application of Cryptology and Information Security  
Singapore, December 6–10, 2021  
Proceedings, Part II

*Editors*

Mehdi Tibouchi   
NTT Corporation  
Tokyo, Japan

Huaxiong Wang   
Nanyang Technological University  
Singapore, Singapore

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-030-92074-6              ISBN 978-3-030-92075-3 (eBook)  
<https://doi.org/10.1007/978-3-030-92075-3>

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

Asiacrypt 2021, the 27th Annual International Conference on Theory and Application of Cryptology and Information Security, was originally planned to be held in Singapore during December 6–10, 2021. Due to the COVID-19 pandemic, it was shifted to an online-only virtual conference.

The conference covered all technical aspects of cryptography, and was sponsored by the International Association for Cryptologic Research (IACR).

We received a total of 341 submissions from all over the world, and the Program Committee (PC) selected 95 papers for publication in the proceedings of the conference. The two program chairs were supported by a PC consisting of 74 leading experts in aspects of cryptography. Each submission was reviewed by at least three PC members (or their sub-reviewers) and five PC members were assigned to submissions co-authored by PC members. The strong conflict of interest rules imposed by IACR ensure that papers are not handled by PC members with a close working relationship with the authors. The two program chairs were not allowed to submit a paper, and PC members were limited to two submissions each. There were approximately 363 external reviewers, whose input was critical to the selection of papers.

The review process was conducted using double-blind peer review. The conference operated a two-round review system with a rebuttal phase. After the reviews and first-round discussions the PC selected 233 submissions to proceed to the second round and the authors were then invited to provide a short rebuttal in response to the referee reports. The second round involved extensive discussions by the PC members.

Alongside the presentations of the accepted papers, the program of Asiacrypt 2021 featured an IACR distinguished lecture by Andrew Chi-Chih Yao and two invited talks by Kazue Sako and Yu Yu. The conference also featured a rump session which contained short presentations on the latest research results of the field.

The four volumes of the conference proceedings contain the revised versions of the 95 papers that were selected, together with the abstracts of the IACR distinguished lecture and the two invited talks. The final revised versions of papers were not reviewed again and the authors are responsible for their contents.

Via a voting-based process that took into account conflicts of interest, the PC selected the three top papers of the conference: “On the Hardness of the NTRU problem” by Alice Pellet-Mary and Damien Stehlé (which received the best paper award); “A Geometric Approach to Linear Cryptanalysis” by Tim Beyne (which received the best student paper award); and “Lattice Enumeration for Tower NFS: a 521-bit Discrete Logarithm Computation” by Gabrielle De Micheli, Pierrick Gaudry, and Cécile Pierrot. The authors of all three papers were invited to submit extended versions of their manuscripts to the *Journal of Cryptology*.

Many people have contributed to the success of Asiacrypt 2021. We would like to thank the authors for submitting their research results to the conference. We are very grateful to the PC members and external reviewers for contributing their knowledge

and expertise, and for the tremendous amount of work that was done with reading papers and contributing to the discussions. We are greatly indebted to Jian Guo, the General Chair, for his efforts and overall organization. We thank San Ling and Josef Pieprzyk, the advisors of Asiacrypt 2021, for their valuable suggestions. We thank Michel Abdalla, Kevin McCurley, Kay McKelly, and members of IACR's emergency pandemic team for their work in designing and running the virtual format. We thank Chitchanok Chuengsatiansup and Khoa Nguyen for expertly organizing and chairing the rump session. We are extremely grateful to Zhenzhen Bao for checking all the L<sup>A</sup>T<sub>E</sub>X files and for assembling the files for submission to Springer. We also thank Alfred Hofmann, Anna Kramer, and their colleagues at Springer for handling the publication of these conference proceedings.

December 2021

Mehdi Tibouchi  
Huaxiong Wang



Wouter Castryck	KU Leuven, Belgium
Rongmao Chen	National University of Defense Technology, China
Jung Hee Cheon	Seoul National University, South Korea
Chitchanok Chuengsatiansup	The University of Adelaide, Australia
Kai-Min Chung	Academia Sinica, Taiwan
Dana Dachman-Soled	University of Maryland, USA
Bernardo David	IT University of Copenhagen, Denmark
Benjamin Fuller	University of Connecticut, USA
Steven Galbraith	The University of Auckland, New Zealand
María Isabel González Vasco	Universidad Rey Juan Carlos, Spain
Robert Granger	University of Surrey, UK
Alex B. Grilo	CNRS, LIP6, Sorbonne Université, France
Aurore Guillevic	Inria, France
Swee-Huay Heng	Multimedia University, Malaysia
Akinori Hosoyamada	NTT Corporation and Nagoya University, Japan
Xinyi Huang	Fujian Normal University, China
Andreas Hülsing	Eindhoven University of Technology, The Netherlands
Tetsu Iwata	Nagoya University, Japan
David Jao	University of Waterloo and evolutionQ, Inc., Canada
Jérémy Jean	ANSSI, France
Shuichi Katsumata	AIST, Japan
Elena Kirshanova	I. Kant Baltic Federal University, Russia
Hyung Tae Lee	Chung-Ang University, South Korea
Dongdai Lin	Institute of Information Engineering, Chinese Academy of Sciences, China
Rongxing Lu	University of New Brunswick, Canada
Xianhui Lu	Institute of Information Engineering, Chinese Academy of Sciences, China
Mary Maller	Ethereum Foundation, UK
Giorgia Azzurra Marson	NEC Labs Europe, Germany
Keith M. Martin	Royal Holloway, University of London, UK
Daniel Masny	Visa Research, USA
Takahiro Matsuda	AIST, Japan
Krystian Matusiewicz	Intel Corporation, Poland
Florian Mendel	Infineon Technologies, Germany
Nele Mentens	Leiden University, The Netherlands, and KU Leuven, Belgium
Atsuko Miyaji	Osaka University, Japan
Michael Naehrig	Microsoft Research, USA
Khoa Nguyen	Nanyang Technological University, Singapore
Miyako Ohkubo	NICT, Japan
Emmanuela Orsini	KU Leuven, Belgium
Jiaxin Pan	NTNU, Norway
Panos Papadimitratos	KTH Royal Institute of Technology, Sweden



Alice Pellet–Mary	CNRS and University of Bordeaux, France
Duong Hieu Phan	Télécom Paris, Institut Polytechnique de Paris, France
Francisco	CINVESTAV, Mexico
Rodríguez-Henríquez	
Olivier Sanders	Orange Labs, France
Jae Hong Seo	Hanyang University, South Korea
Haya Shulman	Fraunhofer SIT, Germany
Daniel Slamanig	AIT Austrian Institute of Technology, Austria
Ron Steinfeld	Monash University, Australia
Willy Susilo	University of Wollongong, Australia
Katsuyuki Takashima	Waseda University, Japan
Qiang Tang	The University of Sydney, Australia
Serge Vaudenay	EPFL, Switzerland
Damien Vergnaud	Sorbonne Université and Institut Universitaire de France, France
Meiqin Wang	Shandong University, China
Xiaoyun Wang	Tsinghua University, China
Yongge Wang	UNC Charlotte, USA
Wenling Wu	Institute of Software, Chinese Academy of Sciences, China
Chaoping Xing	Shanghai Jiao Tong University, China
Sophia Yakubov	Aarhus University, Denmark
Takashi Yamakawa	NTT Corporation, Japan
Bo-Yin Yang	Academia Sinica, Taiwan
Yu Yu	Shanghai Jiao Tong University, China
Hong-Sheng Zhou	Virginia Commonwealth University, USA

## Additional Reviewers

Behzad Abdolmaleki	James Bartusek
Gorjan Alagic	Balthazar Bauer
Orestis Alpos	Rouzbeh Behnia
Miguel Ambrona	Yanis Belkheyar
Diego Aranha	Josh Benaloh
Victor Arribas	Ward Beullens
Nuttapong Attrapadung	Tim Beyne
Benedikt Auerbach	Sarani Bhattacharya
Zeta Avarikioti	Rishiraj Bhattacharyya
Melissa Azouaoui	Nina Bindel
Saikrishna Badrinarayanan	Adam Blatchley Hansen
Joonsang Baek	Olivier Blazy
Karim Bagheri	Charlotte Bonte
Shi Bai	Katharina Boudgoust
Gustavo Banegas	Ioana Boureanu
Subhadeep Banik	Markus Brandt

Anne Broadbent	Samuel Dobson
Ileana Buhan	Luis J. Dominguez Perez
Andrea Caforio	Jelle Don
Eleonora Cagli	Benjamin Dowling
Sébastien Canard	Maria Eichlseder
Ignacio Cascudo	Jesse Elliott
Gaëtan Cassiers	Keita Emura
André Chailloux	Muhammed F. Esgin
Tzu-Hsien Chang	Hulya Evkan
Yilei Chen	Lei Fan
Jie Chen	Antonio Faonio
Yanlin Chen	Hanwen Feng
Albert Cheu	Dario Fiore
Jesús-Javier Chi-Domínguez	Antonio Florez-Gutierrez
Nai-Hui Chia	Georg Fuchsbauer
Ilaria Chillotti	Chaya Ganesh
Ji-Jian Chin	Daniel Gardham
Jérémy Chotard	Rachit Garg
Sherman S. M. Chow	Pierrick Gaudry
Heewon Chung	Romain Gay
Jorge Chávez-Saab	Nicholas Genise
Michele Ciampi	Adela Georgescu
Carlos Cid	David Gerault
Valerio Cini	Satrajit Ghosh
Tristan Claverie	Valerie Gilchrist
Benoît Cogliati	Aron Gohr
Alexandru Cojocaru	Junqing Gong
Daniel Collins	Marc Gourjon
Kelong Cong	Lorenzo Grassi
Craig Costello	Milos Grujic
Geoffroy Couteau	Aldo Gunsing
Daniele Cozzo	Kaiwen Guo
Jan Czajkowski	Chun Guo
Tianxiang Dai	Qian Guo
Wei Dai	Mike Hamburg
Sourav Das	Ben Hamlin
Pratish Datta	Shuai Han
Alex Davidson	Yonglin Hao
Lauren De Meyer	Keisuke Hara
Elke De Mulder	Patrick Harasser
Claire Delaplace	Jingnan He
Cyprien Delpech de Saint Guilhem	David Heath
Patrick Derbez	Chloé Héban
Siemen Dhooghe	Julia Hesse
Daniel Dinu	Ryo Hiromasa
Christoph Dobraunig	Shiqi Hou

Lin Hou  
Yao-Ching Hsieh  
Kexin Hu  
Jingwei Hu  
Zhenyu Huang  
Loïs Huguenin-Dumittan  
Arnie Hung  
Shih-Han Hung  
Kathrin Hövelmanns  
Ilia Iliashenko  
Aayush Jain  
Yanxue Jia  
Dingding Jia  
Yao Jiang  
Floyd Johnson  
Luke Johnson  
Chanyang Ju  
Charanjit S. Jutla  
John Kelsey  
Taechan Kim  
Myungsun Kim  
Jinsu Kim  
Minkyu Kim  
Young-Sik Kim  
Sungwook Kim  
Jiseung Kim  
Kwangjo Kim  
Seungki Kim  
Sunpill Kim  
Fuyuki Kitagawa  
Susumu Kiyoshima  
Michael Kloof  
Dimitris Kolonelos  
Venkata Koppula  
Liliya Kraleva  
Mukul Kulkarni  
Po-Chun Kuo  
Hilder Vitor Lima Pereira  
Russell W. F. Lai  
Jianchang Lai  
Yi-Fu Lai  
Virginie Lallemand  
Jason LeGrow  
Joohee Lee  
Jooyoung Lee  
Changmin Lee

Hyeonbum Lee  
Moon Sung Lee  
Keewoo Lee  
Dominik Leichtle  
Alexander Lemmens  
Gaëtan Leurent  
Yannan Li  
Shuaishuai Li  
Baiyu Li  
Zhe Li  
Shun Li  
Liang Li  
Jianwei Li  
Trey Li  
Xiao Liang  
Chi-Chang Lin  
Chengjun Lin  
Chao Lin  
Yao-Ting Lin  
Eik List  
Feng-Hao Liu  
Qipeng Liu  
Guozhen Liu  
Yunwen Liu  
Patrick Longa  
Sebastien Lord  
George Lu  
Yuan Lu  
Yibiao Lu  
Xiaojuan Lu  
Ji Luo  
Yiyuan Luo  
Mohammad Mahzoun  
Monosij Maitra  
Christian Majenz  
Ekaterina Malygina  
Mark Manulis  
Varun Maram  
Luca Mariot  
Loïc Masure  
Bart Mennink  
Simon-Philipp Merz  
Peihan Miao  
Kazuhiko Minematsu  
Donika Mirdita  
Pratyush Mishra

Tomoyuki Morimae  
 Pratyay Mukherjee  
 Alex Munch-Hansen  
 Yusuke Naito  
 Ngoc Khanh Nguyen  
 Jianting Ning  
 Ryo Nishimaki  
 Anca Nitulescu  
 Kazuma Ohara  
 Cristina Onete  
 Jean-Baptiste Orfila  
 Michele Orrù  
 Jong Hwan Park  
 Jeongeun Park  
 Robi Pedersen  
 Angel L. Perez del Pozo  
 Léo Perrin  
 Thomas Peters  
 Albrecht Petzoldt  
 Stjepan Picek  
 Rafael del Pino  
 Geong Sen Poh  
 David Pointcheval  
 Bernardo Portela  
 Raluca Postecu  
 Thomas Prest  
 Robert Primas  
 Chen Qian  
 Willy Quach  
 Md Masoom Rabbani  
 Rahul Rachuri  
 Srinivasan Raghuraman  
 Sebastian Ramacher  
 Matthieu Rambaud  
 Shahram Rasoolzadeh  
 Krijn Reijnders  
 Joost Renes  
 Elena Reshetova  
 Mélissa Rossi  
 Mike Rosulek  
 Yann Rotella  
 Joe Rowell  
 Arnab Roy  
 Partha Sarathi Roy  
 Alexander Russell  
 Carla Ráfols

Paul Rösler  
 Yusuke Sakai  
 Amin Sakzad  
 Yu Sasaki  
 Or Sattath  
 John M. Schanck  
 Lars Schlieper  
 Martin Schläfer  
 Carsten Schmidt  
 André Schrottenloher  
 Jacob Schuldt  
 Jean-Pierre Seifert  
 Yannick Seurin  
 Yaobin Shen  
 Yixin Shen  
 Yu-Ching Shen  
 Danping Shi  
 Omri Shmueli  
 Kris Shrishak  
 Hervais Simo Fhom  
 Luisa Siniscalchi  
 Daniel Smith-Tone  
 Fang Song  
 Pratik Soni  
 Claudio Soriente  
 Akshayaram Srinivasan  
 Douglas Stebila  
 Damien Stehlé  
 Bruno Sterner  
 Christoph Striecks  
 Patrick Struck  
 Adriana Suarez Corona  
 Ling Sun  
 Shi-Feng Sun  
 Koutarou Suzuki  
 Aishwarya T.  
 Erkan Tairi  
 Akira Takahashi  
 Atsushi Takayasu  
 Abdul Rahman Taleb  
 Younes Talibi Alaoui  
 Benjamin Hong Meng Tan  
 Syh-Yuan Tan  
 Titouan Tanguy  
 Alexander Tereshchenko  
 Adrian Thillard

Emmanuel Thomé  
Tyge Tiessen  
Radu Titiu  
Ivan Tjuawinata  
Yosuke Todo  
Junichi Tomida  
Bénédict Tran  
Jacques Traoré  
Ni Trieu  
Ida Tucker  
Michael Tunstall  
Dominique Unruh  
Thomas Unterluggauer  
Thomas van Himbeeck  
Daniele Venturi  
Jorge Villar  
Mikhail Volkhov  
Christine van Vredendaal  
Benedikt Wagner  
Riad Wahby  
Hendrik Waldner  
Alexandre Wallet  
Junwei Wang  
Qingju Wang  
Yuyu Wang  
Lei Wang  
Senpeng Wang  
Peng Wang  
Weijia Wang  
Yi Wang

Han Wang  
Xuzi Wang  
Yohei Watanabe  
Florian Weber  
Weiqiang Wen  
Nils Wisiol  
Mathias Wolf  
Harry H. W. Wong  
Keita Xagawa  
Zejun Xiang  
Jiayu Xu  
Luyao Xu  
Yaqi Xu  
Shota Yamada  
Hailun Yan  
Wenjie Yang  
Shaojun Yang  
Masaya Yasuda  
Wei-Chuen Yau  
Kazuki Yoneyama  
Weijing You  
Chen Yuan  
Tsz Hon Yuen  
Runzhi Zeng  
Cong Zhang  
Zhifang Zhang  
Bingsheng Zhang  
Zhelei Zhou  
Paul Zimmermann  
Lukas Zobernig

## Contents – Part II

### Physical Attacks, Leakage and Countermeasures

Secure and Efficient Software Masking on Superscalar Pipelined Processors . . . . .	3
<i>Barbara Gigerl, Robert Primas, and Stefan Mangard</i>	
Fault-Injection Attacks Against NIST’s Post-Quantum Cryptography Round 3 KEM Candidates . . . . .	33
<i>Keita Xagawa, Akira Ito, Rei Ueno, Junko Takahashi, and Naofumi Homma</i>	
Divided We Stand, United We Fall: Security Analysis of Some SCA+SIFA Countermeasures Against SCA-Enhanced Fault Template Attacks . . . . .	62
<i>Sayandeep Saha, Arnab Bag, Dirmanto Jap, Debdeep Mukhopadhyay, and Shivam Bhasin</i>	
Efficient Leakage-Resilient MACs Without Idealized Assumptions . . . . .	95
<i>Francesco Berti, Chun Guo, Thomas Peters, and François-Xavier Standaert</i>	
DEFAULT: Cipher Level Resistance Against Differential Fault Attack . . . . .	124
<i>Anubhab Baksi, Shivam Bhasin, Jakub Breier, Mustafa Khairallah, Thomas Peyrin, Sumanta Sarkar, and Siang Meng Sim</i>	
Dynamic Random Probing Expansion with Quasi Linear Asymptotic Complexity . . . . .	157
<i>Sonia Belaïd, Matthieu Rivain, Abdul Rahman Taleb, and Damien Vergnaud</i>	

### Multiparty Computation

Homomorphic Secret Sharing for Multipartite and General Adversary Structures Supporting Parallel Evaluation of Low-Degree Polynomials. . . . .	191
<i>Reo Eriguchi and Koji Nuida</i>	
Improved Single-Round Secure Multiplication Using Regenerating Codes . . .	222
<i>Mark Abspoel, Ronald Cramer, Daniel Escudero, Ivan Damgård, and Chaoping Xing</i>	
Garbling, Stacked and Staggered: Faster $k$ -out-of- $n$ Garbled Function Evaluation. . . . .	245
<i>David Heath, Vladimir Kolesnikov, and Stanislav Peceny</i>	

Better Security-Efficiency Trade-Offs in Permutation-Based Two-Party Computation. . . . .	275
<i>Yu Long Chen and Stefano Tessaro</i>	
Two-Round Adaptively Secure MPC from Isogenies, LPN, or CDH . . . . .	305
<i>Navid Alamati, Hart Montgomery, Sikhar Patranabis, and Pratik Sarkar</i>	
Reverse Firewalls for Adaptively Secure MPC Without Setup. . . . .	335
<i>Suvradip Chakraborty, Chaya Ganesh, Mahak Pancholi, and Pratik Sarkar</i>	
<b>Enhanced Public-Key Encryption and Time-Lock Puzzles</b>	
On Time-Lock Cryptographic Assumptions in Abelian Hidden-Order Groups . . . . .	367
<i>Aron van Baarsen and Marc Stevens</i>	
Astrolabous: A Universally Composable Time-Lock Encryption Scheme . . . .	398
<i>Myrto Arapinis, Nikolaos Lamprou, and Thomas Zacharias</i>	
Identity-Based Encryption for Fair Anonymity Applications: Defining, Implementing, and Applying Rerandomizable RCCA-Secure IBE . . . . .	427
<i>Yi Wang, Rongmao Chen, Xinyi Huang, Jianting Ning, Baosheng Wang, and Moti Yung</i>	
Simulation-Based Bi-Selective Opening Security for Public Key Encryption. . . . .	456
<i>Junzuo Lai, Rupeng Yang, Zhengnan Huang, and Jian Weng</i>	
Key Encapsulation Mechanism with Tight Enhanced Security in the Multi-user Setting: Impossibility Result and Optimal Tightness . . . . .	483
<i>Shuai Han, Shengli Liu, and Dawu Gu</i>	
Hierarchical Integrated Signature and Encryption: (or: Key Separation vs. Key Reuse: Enjoy the Best of both Worlds). . . . .	514
<i>Yu Chen, Qiang Tang, and Yuyu Wang</i>	
<b>Real-World Protocols</b>	
TARDIGRADE: An Atomic Broadcast Protocol for Arbitrary Network Conditions . . . . .	547
<i>Erica Blum, Jonathan Katz, and Julian Loss</i>	
Onion Routing with Replies . . . . .	573
<i>Christiane Kuhn, Dennis Hofheinz, Andy Rupp, and Thorsten Strufe</i>	

<b>Private Join and Compute from PIR with Default . . . . .</b>	<b>605</b>
<i>Tancrède Lepoint, Sarvar Patel, Mariana Raykova, Karn Seth, and Ni Trieu</i>	
<b>Generalized Channels from Limited Blockchain Scripts and Adaptor Signatures . . . . .</b>	<b>635</b>
<i>Lukas Aumayr, Oguzhan Ersoy, Andreas Erwig, Sebastian Faust, Kristina Hostáková, Matteo Maffei, Pedro Moreno-Sanchez, and Siavash Riahi</i>	
<b>ConTra Corona: Contact Tracing against the Coronavirus by Bridging the Centralized–Decentralized Divide for Stronger Privacy . . . . .</b>	<b>665</b>
<i>Wasilij Beskorovajnov, Felix Dörre, Gunnar Hartung, Alexander Koch, Jörn Müller-Quade, and Thorsten Strufe</i>	
<b>Cryptographic Analysis of the Bluetooth Secure Connection Protocol Suite . . . . .</b>	<b>696</b>
<i>Marc Fischlin and Olga Sanina</i>	
<b>Author Index . . . . .</b>	<b>727</b>