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 III





Lecture Notes in Computer Science

13092

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

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 III



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 978-3-030-92077-7 ISBN 978-3-030-92078-4 (eBook) https://doi.org/10.1007/978-3-030-92078-4

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

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 cryptology, 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 cryptology. 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

vi Preface

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 IaT_{EX} 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

Organization

General Chair

Jian Guo

Nanyang Technological University, Singapore

Program Committee Co-chairs

Mehdi Tibouchi	NTT Corporation, Japan
Huaxiong Wang	Nanyang Technological University, Singapore

Steering Committee

Masayuki Abe Lynn Batten Jung Hee Cheon Steven Galbraith D. J. Guan Jian Guo Khalid Habib Lucas Hui Nassar Ikram Kwangjo Kim Xuejia Lai Dong Hoon Lee Satya Lokam Mitsuru Matsui (Chair) Tsutomu Matsumoto Phong Nguyen

Dingyi Pei Duong Hieu Phan Raphael Phan Josef Pieprzyk (Vice Chair) C. Pandu Rangan Bimal Roy Leonie Simpson Huaxiong Wang Henry B. Wolfe Duncan Wong Tzong-Chen Wu Bo-Yin Yang Siu-Ming Yiu Yu Yu Jianying Zhou

Program Committee

IIT Madras, India
Royal Holloway, University of London, UK
Nanyang Technological University, Singapore
University of Porto (FCUP) and INESC TEC, Portugal
Radboud University, The Netherlands
CryptoExperts, France
Algorand Foundation, USA
Rambus - Cryptography Research, The Netherlands
University of Waterloo, Canada
NXP Semiconductors, Belgium

Wouter Castryck Rongmao Chen Jung Hee Cheon Chitchanok Chuengsatiansup Kai-Min Chung Dana Dachman-Soled Bernardo David **Benjamin Fuller** Steven Galbraith María Isabel González Vasco Robert Granger Alex B. Grilo Aurore Guillevic Swee-Huay Heng Akinori Hosoyamada Xinyi Huang Andreas Hülsing Tetsu Iwata David Jao Jérémy Jean Shuichi Katsumata Elena Kirshanova Hyung Tae Lee Dongdai Lin Rongxing Lu Xianhui Lu Mary Maller Giorgia Azzurra Marson Keith M. Martin Daniel Masny Takahiro Matsuda Krystian Matusiewicz Florian Mendel Nele Mentens Atsuko Miyaji Michael Naehrig

Michael Naehrig Khoa Nguyen Miyako Ohkubo Emmanuela Orsini Jiaxin Pan Panos Papadimitratos

KU Leuven, Belgium National University of Defense Technology, China Seoul National University, South Korea The University of Adelaide, Australia Academia Sinica, Taiwan University of Marvland, USA IT University of Copenhagen, Denmark University of Connecticut, USA The University of Auckland, New Zealand Universidad Rey Juan Carlos, Spain University of Surrey, UK CNRS, LIP6, Sorbonne Université, France Inria. France Multimedia University, Malaysia NTT Corporation and Nagoya University, Japan Fujian Normal University, China Eindhoven University of Technology, The Netherlands Nagoya University, Japan University of Waterloo and evolutionQ, Inc., Canada ANSSI. France AIST. Japan I. Kant Baltic Federal University, Russia Chung-Ang University, South Korea Institute of Information Engineering, Chinese Academy of Sciences. China University of New Brunswick, Canada Institute of Information Engineering, Chinese Academy of Sciences. China Ethereum Foundation, UK NEC Labs Europe, Germany Royal Holloway, University of London, UK Visa Research, USA AIST, Japan Intel Corporation, Poland Infineon Technologies, Germany Leiden University, The Netherlands, and KU Leuven, Belgium Osaka University, Japan Microsoft Research, USA Nanyang Technological University, Singapore NICT, Japan KU Leuven, Belgium NTNU, Norway KTH Royal Institute of Technology, Sweden

Alice Pellet-Mary Duong Hieu Phan Francisco Rodríguez-Henríquez **Olivier Sanders** Orange Labs, France Jae Hong Seo Haya Shulman Daniel Slamanig Ron Steinfeld Willy Susilo Katsuyuki Takashima Qiang Tang Serge Vaudenay Damien Vergnaud Meiqin Wang Xiaoyun Wang Yongge Wang Wenling Wu China Chaoping Xing Sophia Yakoubov Takashi Yamakawa Bo-Yin Yang Yu Yu Hong-Sheng Zhou

CNRS and University of Bordeaux, France Télécom Paris, Institut Polytechnique de Paris, France CINVESTAV, Mexico

Hanyang University, South Korea Fraunhofer SIT, Germany AIT Austrian Institute of Technology, Austria Monash University, Australia University of Wollongong, Australia Waseda University, Japan The University of Sydney, Australia EPFL, Switzerland Sorbonne Université and Institut Universitaire de France. France Shandong University, China Tsinghua University, China UNC Charlotte, USA Institute of Software, Chinese Academy of Sciences, Shanghai Jiao Tong University, China Aarhus University, Denmark NTT Corporation, Japan Academia Sinica, Taiwan Shanghai Jiao Tong University, China Virginia Commonwealth University, USA

Additional Reviewers

Behzad Abdolmaleki Gorjan Alagic Orestis Alpos Miguel Ambrona Diego Aranha Victor Arribas Nuttapong Attrapadung Benedikt Auerbach Zeta Avarikioti Melissa Azouaoui Saikrishna Badrinarayanan Joonsang Baek Karim Baghery Shi Bai Gustavo Banegas Subhadeep Banik

James Bartusek Balthazar Bauer Rouzbeh Behnia Yanis Belkheyar Josh Benaloh Ward Beullens Tim Beyne Sarani Bhattacharya Rishiraj Bhattacharyya Nina Bindel Adam Blatchley Hansen Olivier Blazy Charlotte Bonte Katharina Boudgoust Ioana Boureanu Markus Brandt

Anne Broadbent Ileana Buhan Andrea Caforio Eleonora Cagli Sébastien Canard Ignacio Cascudo Gaëtan Cassiers André Chailloux Tzu-Hsien Chang Yilei Chen Jie Chen Yanlin Chen Albert Cheu Jesús-Javier Chi-Domíguez Nai-Hui Chia Ilaria Chillotti Ji-Jian Chin Jérémy Chotard Sherman S. M. Chow Heewon Chung Jorge Chávez-Saab Michele Ciampi Carlos Cid Valerio Cini Tristan Claverie Benoît Cogliati Alexandru Cojocaru Daniel Collins Kelong Cong Craig Costello Geoffroy Couteau Daniele Cozzo Jan Czajkowski Tianxiang Dai Wei Dai Souray Das Pratish Datta Alex Davidson Lauren De Meyer Elke De Mulder Claire Delaplace Cyprien Delpech de Saint Guilhem Patrick Derbez Siemen Dhooghe Daniel Dinu Christoph Dobraunig

Samuel Dobson Luis J. Dominguez Perez Jelle Don Benjamin Dowling Maria Eichlseder Jesse Elliott Keita Emura Muhammed F. Esgin Hulya Evkan Lei Fan Antonio Faonio Hanwen Feng Dario Fiore Antonio Florez-Gutierrez Georg Fuchsbauer Chava Ganesh Daniel Gardham Rachit Garg Pierrick Gaudry Romain Gav Nicholas Genise Adela Georgescu David Gerault Satrajit Ghosh Valerie Gilchrist Aron Gohr Junqing Gong Marc Gourjon Lorenzo Grassi Milos Grujic Aldo Gunsing Kaiwen Guo Chun Guo Qian Guo Mike Hamburg Ben Hamlin Shuai Han Yonglin Hao Keisuke Hara Patrick Harasser Jingnan He David Heath Chloé Hébant Julia Hesse Ryo Hiromasa 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 Minkvu Kim Young-Sik Kim Sungwook Kim Jiseung Kim Kwangjo Kim Seungki Kim Sunpill Kim Fuyuki Kitagawa Susumu Kiyoshima Michael Klooß **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 Pratvav Mukheriee 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 Posteuca Thomas Prest Robert Primas Chen Oian 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

xiii

Emmanuel Thomé Tyge Tiessen Radu Titiu Ivan Tiuawinata Yosuke Todo Junichi Tomida Bénédikt 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 III

NIZK and SNARKs

Lunar: A Toolbox for More Efficient Universal and Updatable zkSNARKs and Commit-and-Prove Extensions	3
Matteo Campanelli, Antonio Faonio, Dario Fiore, Anaïs Querol, and Hadrián Rodríguez	
Gentry-Wichs is Tight: a Falsifiable Non-adaptively Sound SNARG Helger Lipmaa and Kateryna Pavlyk	34
Proofs for Inner Pairing Products and Applications Benedikt Bünz, Mary Maller, Pratyush Mishra, Nirvan Tyagi, and Psi Vesely	65
Snarky Ceremonies	98
Efficient NIZKs for Algebraic Sets	128
Theory	
Bit Security as Computational Cost for Winning Games with High Probability	161
Giving an Adversary Guarantees (Or: How to Model Designated Verifier Signatures in a Composable Framework) Ueli Maurer, Christopher Portmann, and Guilherme Rito	189
How to Build a Trapdoor Function from an Encryption Scheme Sanjam Garg, Mohammad Hajiabadi, Giulio Malavolta, and Rafail Ostrovsky	220
Beyond Software Watermarking: Traitor-Tracing for Pseudorandom Functions	250
Batching Base Oblivious Transfers Ian McQuoid, Mike Rosulek, and Lawrence Roy	281

Algebraic Adversaries in the Universal Composability Framework	311
Michel Abdalla, Manuel Barbosa, Jonathan Katz, Julian Loss,	
and Jiayu Xu	

Symmetric-Key Constructions

Luby-Rackoff Backwards with More Users and More Security Srimanta Bhattacharya and Mridul Nandi	345
Double-Block-Length Hash Function for Minimum Memory Size Yusuke Naito, Yu Sasaki, and Takeshi Sugawara	376
Toward a Fully Secure Authenticated Encryption Scheme from a Pseudorandom Permutation Wonseok Choi, Byeonghak Lee, Jooyoung Lee, and Yeongmin Lee	407
Tight Security for Key-Alternating Ciphers with Correlated Sub-keys Stefano Tessaro and Xihu Zhang	435
FAST: Secure and High Performance Format-Preserving Encryption and Tokenization.F. Betül Durak, Henning Horst, Michael Horst, and Serge Vaudenay	465
Fine-Tuning the ISO/IEC Standard LightMAC Soumya Chattopadhyay, Ashwin Jha, and Mridul Nandi	490
Categorization of Faulty Nonce Misuse Resistant Message Authentication Yu Long Chen, Bart Mennink, and Bart Preneel	520
Homomorphic Encryption and Encrypted Search	
Balanced Non-adjacent Forms	553
Efficient Boolean Search over Encrypted Data with Reduced Leakage Sarvar Patel, Giuseppe Persiano, Joon Young Seo, and Kevin Yeo	577
Revisiting Homomorphic Encryption Schemes for Finite Fields Andrey Kim, Yuriy Polyakov, and Vincent Zucca	608
Transciphering Framework for Approximate Homomorphic Encryption Jihoon Cho, Jincheol Ha, Seongkwang Kim, Byeonghak Lee, Joohee Lee, Jooyoung Lee, Dukjae Moon, and Hyojin Yoon	640

Improved Programmable Bootstrapping with Larger Precision and Efficient Arithmetic Circuits for TFHE	
Author Index Author Samuel Control	701