Mehdi Tibouchi
Huaxiong Wang (Eds.)

LNCS 13092

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

3 Part III

INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH
i a c r

Springer

Lecture Notes in Computer Science 13092

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 III

Springer

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

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 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 LaTeX 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

Shweta Agrawal	IIT Madras, India
Martin R. Albrecht	Royal Holloway, University of London, UK
Zhenzhen Bao	Nanyang Technological University, Singapore
Manuel Barbosa	University of Porto (FCUP) and INESC TEC, Portugal
Lejla Batina	Radboud University, The Netherlands
Sonia Belaïd	CryptoExperts, France
Fabrice Benhamouda	Algorand Foundation, USA
Begül Bilgin	Rambus - Cryptography Research, The Netherlands
Xavier Bonnetain	University of Waterloo, Canada
Joppe W. Bos	NXP Semiconductors, Belgium

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 Rodríguez-Henríquez	CINVESTAV, Mexico
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 Yakoubov	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
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
Sourav 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
Chaya Ganesh
Daniel Gardham
Rachit Garg
Pierrick Gaudry
Romain Gay
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
Minkyu 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
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 Posteuca
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
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

Theory

Symmetric-Key Constructions

Homomorphic Encryption and Encrypted Search