Lecture Notes in Computer Science **11443**

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

More information about this series at http://www.springer.com/series/7410

Dongdai Lin · Kazue Sako (Eds.)

Public-Key Cryptography – PKC 2019

22nd IACR International Conference
on Practice and Theory of Public-Key Cryptography
Beijing, China, April 14–17, 2019
Proceedings, Part II

Springer

Editors
Dongdai Lin
SKLOIS, Institute of Information Engineering
Chinese Academy of Sciences
Beijing, China

Kazue Sako
Security Research Laboratories
NEC Corporation
Kawasaki, Japan

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-17258-9 ISBN 978-3-030-17259-6 (eBook)
https://doi.org/10.1007/978-3-030-17259-6

Library of Congress Control Number: 2019936577

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

The 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC 2019) was held April 14–17, 2019, in Beijing, China. The conference is sponsored by the International Association for Cryptologic Research (IACR) and focuses on all technical aspects of public-key cryptography. These proceedings consist of two volumes including 42 papers that were selected by the Program Committee from 173 submissions. Each submission was assigned to at least three reviewers while submissions co-authored by Program Committee members received at least five reviews. During the discussion phase, the Program Committee used quite intensively a recent feature of the review system, which allows Program Committee members to anonymously ask questions to the authors. The reviewing and selection process was a challenging task and we are deeply grateful to the Program Committee members and external reviewers for their hard and thorough work. Many thanks also to Shai Halevi for his assistance with the Web submission and review software. We thank the authors for promptly responding to the questions raised by the committee, which helped us understand the content of their submissions.

The conference program also included an invited talk by Tatsuaki Okamoto (NTT). We would like to thank the invited speaker as well as all the other speakers and the authors of all submissions for their contributions to the program and conference. Finally, we would like to thank Xiaoyun Wang, the general chair, and all the members of local Organizing Committee for organizing a great conference and all the conference attendees for making this conference a truly intellectually stimulating event through their active participation.

April 2019

Dongdai Lin
Kazue Sako

PKC 2019

22nd IACR International Conference on Practice and Theory of Public-Key Cryptography

Beijing, China
April 14–17, 2019

Sponsored and Organized by

International Association for Cryptologic Research
State Key Laboratory of Information Security
State Key Laboratory of Cryptology
TopSec Technologies Inc.
Institute of Information Engineering, Chinese Academy of Sciences
Chinese Association for Cryptologic Research

General Chair

Xiaoyun Wang	Tsinghua University, China

Program Co-chairs

Dongdai Lin	SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences, China
Kazue Sako	Security Research Laboratories, NEC Corporation, Japan

Steering Committee

Michel Abdalla	Ecole Normale Supérieure, France
Yvo Desmedt	University of Texas at Dallas, USA
Goichiro Hanaoka	National Institute of Advanced Industrial Science and Technology, Japan
Aggelos Kiayias	University of Edinburgh, UK
Dongdai Lin	Chinese Academy of Sciences, China
David Naccache	Ecole Normale Supérieure, France
Tatsuaki Okamoto	NTT Labs, Japan
David Pointcheval	Ecole Normale Supérieure, France
Kazue Sako	NEC Security Research Laboratories, Japan
Moti Yung	Google and Columbia University, USA
Yuliang Zheng	University of Alabama at Birmingham, USA

Program Committee

Erdem Alkim	Ondokuz Mayis University, Turkey
Diego F. Aranha	Aarhus University, Denmark and University of Campinas, Brazil
Chris Brzuska	Alto University, Finland
Dario Catalano	University of Catania, Italy
Nishanth Chandran	Microsoft, India
Sanjit Chatterjee	Indian Institute of Sciences, India
Jie Chen	East China Normal University, China
Jung Hee Cheon	Seoul National University, Korea
Craig Costello	Microsoft Research, USA
Yi Deng	Chinese Academy of Sciences, China
Leo Ducas	CWI Amsterdam, The Netherlands
Nico Döttling	Cispa Helmholtz Center (i.G.), Germany
Dario Fiore	IMDEA Software Institute, Spain
Pierre-Alain Fouque	Rennes University, France
Feng Hao	University of Warwick, UK
Tibor Jager	Paderborn University, Germany
Marc Joye	OneSpan, Belgium
Tancrède Lepoint	SRI International, USA
Benoît Libert	CNRS and ENS de Lyon, France
Helger Lipmaa	University of Tartu, Estonia
Feng-Hao Liu	Florida Atlantic University, USA
Takahiro Matsuda	AIST, Japan
Pratyay Mukherjee	Visa Research, USA
Satoshi Obana	Hosei University, Japan
Miyako Okubo	NICT, Japan
Arpita Patra	Indian Institute of Science, India
Ludovic Perret	Sorbonne University, France
Thomas Peters	UC Louvain, Belgium
Benny Pinkas	Bar-Ilan University, Israel
Bertram Poettering	Royal Holloway, University of London, UK
Antigoni Polychroniadou	Cornell Tech, USA
Alessandra Scafuro	NC State University, USA
Jae Hong Seo	Hanyang University, South Korea
Qiang Tang	New Jersey Institute of Technology, USA
Huaxiong Wang	Nanyang Technological University, Singapore
Yu Yu	Shanghai Jiaotong University, China

Organizing Committee

Xiaofeng Chen	Xidian University, China
Yu Chen	SKLOIS, Institute of Information Engineering, CAS, China
Shuqin Fan	State Key Laboratory of Cryptology, China

Xinyi Huang	Fujian Normal University, China
Ming Li	SKLOIS, Institute of Information Engineering, CAS, China
Zhe Liu	Nanjing University of Aeronautics and Astronautics, China
Chunming Tang	Guangzhou University, China
Anyu Wang	SKLOIS, Institute of Information Engineering, CAS, China
Jian Weng	Jinan University, China
Baofeng Wu	SKLOIS, Institute of Information Engineering, CAS, China
Fangguo Zhang	Sun Yat-sen University, China
Yunlei Zhao	Fudan University, China

Additional Reviewers

Benjamin Dowling
Behzad Abdolmaleki
Masayuki Abe
Martin R. Albrecht
Pedro G. M. R. Alves
Gilad Asharov
Nuttapong Attrapadung
Karim Baghery
Shi Bai
Marshall Ball
Manuel Barbosa
Hridam Basu
Carsten Baum
Pascal Bemmann
Fabrice Benhamouda
Pauline Bert
Francesco Berti
Ward Beullens
Sauvik Bhattacharya
Olivier Blazy
Katharina Boudgoust
Florian Bourse
Xavier Bultel
Olive Chakraborty
Biniy Chen
Long Chen
Rongmao Chen
Yu Chen
Wonhee Cho
Ashish Choudhury
Peter Chvojka
Sadro Coretti
Geoffroy Couteau
Edouard Cuvelier
Prem Laxman Das
Bernardo David
Amit Deo
Apoorvaa Deshpande
Julien Devigne
Ning Ding
Lucas Enloe
Jieun Eom
Naomi Ephraim
Xiong Fan
Antonio Faonio
Luca De Feo
Daniele Friolo
Georg Fuchsbauer
Ben Fuller
Tommaso Gagliardoni
Steven Galbraith
Tatiana Galibus
Chaya Ganesh
Romain Gay
Peter Gazi
Kai Gellert
Nicholas Genise
Satrajit Ghosh

Irene Giacomelli
Junqing Gong
Alonso Gonzalez
Jens Groth
Fabrice Ben Hammouda
Kyoohyung Han
Abida Haque
Javier Herranz
Clemens Heuberger
Minki Hhan
Hyunsook Hong
Seungwan Hong
Jingwei Hu
Qiong Huang
Xinyi Huang
Huisu Jang
Christian Janson
Jinhyuck Jeong
Yun-Seong Ji
Shaoquan Jiang
Zhang Jiang
Charanjit Jutla
R. Kabaleeshwaran
Saqib A. Kakvi
Koray Karabina
Shuichi Katsumata
Yutaka Kawai
Hamidreza Khoshakhlagh
Dongwoo Kim
Duhyeong Kim
Jaeyun Kim
Jiseung Kim
Minkyu Kim
Fuyuki Kitagawa
Susumu Kiyoshima
Kamil Kluczniak
François Koeune
Yashvanth Kondi
Toomas Krips
Shravan Kumar
Rafael Kurek
Fabien Laguillaumie
Junzuo Lai
Qiqi Lai
Hyung Tae Lee
Joohee Lee
Kiwoo Lee
Jiangtao Li
Jie Li
Changlu Lin
Fuchun Lin
Qipeng Liu
Shengli Liu
Zhe Liu
Zhen Liu
Patrick Longa
Steve Lu
Yuan Lu
Lin Lyu
Shunli Ma
Varun Madathil
Monosij Maitra
Giulio Malavolta
Mark Manulis
Chloe Martindale
Daniel Masny
Peihan Miao
Rafael Misoczki
Payman Mohassel
Fabrice Mouhartem
Yi Mu
Sayantan Mukherjee
Pierrick Méaux
Michael Naehrig
Kartik Nayak
Khoa Nguyen
David Niehues
Ryo Nishimaki
Luca Nizzardo
Ariel Nof
Koji Nuida
Sai Lakshmi Bhavana Obbattu
Cristina Onete
Emmanuella Orsini
Jiaxin Pan
Tapas Pandit
Lorenz Panny
Jong Hwan Park
Alain Passelègue
Sikhar Patranabis
Alice Pellet–Mary
Geovandro Pereira

Olivier Pereira
Rachel Player
S. Puria
Erick Purwanto
Baodong Qin
Chen Qian
Mario Di Raimondo
Somindu C. Ramanna
Divya Ravi
Joost Renes
Amanda Cristina Davi Resende
Melissa Rossi
Arnab Roy
Paul Rösler
Mohamed Sabt
Yusuke Sakai
Jonas Schneider
Peter Scholl
Jacob Schuldt
Sven Schäge
Adam Sealfon
Sruthi Sekar
Minhye Seo
Akash Shah
Kazumasa Shinagawa
Adam Shull
Janno Siim
Luisa Siniscalchi
Benjamin Smith
Azam Soleimanian
Yongha Son
Katerina Sotiraki
Shifeng Sun
Willy Susilo
Koutarou Suzuki
Benjamin Hong Meng Tan
Radu Titiu
Junichi Tomida
Rotem Tsabary
Daniel Tschudi
Anselme Tueno
Dominque Unruh
Muthuramakrishnan Venkitasubramaniam
Daniele Venturi
Sameer Wagh
Michael Walter
Hailong Wang
Liping Wang
Luping Wang
Yu-chen Wang
Yuyu Wang
Zhedong Wang
Weiqiang Wen
Joanne Woodage
Shota Yamada
Takashi Yamakawa
Avishay Yanay
Guomin Yang
Kang Yang
Rupeng Yang
Xu Yanhong
Donggeon Yhee
Jingyue Yu
Yang Yu
Zuoxia Yu
Aaram Yun
Michal Zajac
Ming Zeng
Cong Zhang
Jiang Zhang
Juanyang Zhang
Kai Zhang
Liang Feng Zhang
Mingwu Zhang
Rui Zhang
Xiaojun Zhang
Qian Zhao
Yunlei Zhao
Linfeng Zhou
Giorgos Zirdelis

Contents – Part II

Re-encryption Schemes

Fundamental Primitives (II)

Post Quantum Cryptography

Contents – Part I