Lecture Notes in Computer Science 12612

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

Yongdong Wu · Moti Yung (Eds.)

Information Security and Cryptology

16th International Conference, Inscrypt 2020 Guangzhou, China, December 11–14, 2020 Revised Selected Papers

Springer

Editors

Yongdong Wu
Jinan University
Guangzhou, China

Moti Yung
Computer Science Department
Columbia University
New York, NY, USA

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-71851-0 ISBN 978-3-030-71852-7 (eBook)
https://doi.org/10.1007/978-3-030-71852-7

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 16th International Conference on Information Security and Cryptology (Inscrypt 2020) was held in Guangzhou, Guangdong, from December 11 to 14, 2020. It was co-organized by the State Key Laboratory of Information Security, the Chinese Association for Cryptologic Research, and the College of Cyber Security of Jinan University, and in cooperation with the IACR. Due to the COVID-19 pandemic, it was held as a hybrid of physical and online components.

Inscrypt is an annual conference held in China, targeting research advances in all areas of information security, cryptology, and their applications. The 2020 conference instance received a total of 79 submissions from Russia, Korea, Australia, China Hong Kong, and China mainland. The two PC chairs were supported by 45 Program Committee (PC) members and 13 sub-reviewers, who were leading experts on cryptology and security from 13 countries or regions. The PC team selected 24 papers as Full Papers, and 8 papers as Short Papers. In the selecting process, the papers were bid for by the PC members and then automatically assigned to them for reviewing. The reviewing process was conducted using a double-blind peer review process, and each paper was reviewed by at least three PC members or sub-reviewers. All the accepted papers were included in the conference proceedings.

The program of Inscrypt 2020 included six excellent invited academic keynote talks by Professors Danfeng (Daphne) Yao (USA), Yang Liu (Singapore), Aggelos Kiayias (United Kingdom), Orr Dunkelman (Israel), Giuseppe Persiano (Italy), and Chuanming Zong (China), as well as one industrial keynote talk by Dr. Qisen Huang (Nsfocus, China). In addition, the program included nine regular presentation sessions on AI Security, Asymmetric ciphers, Post-quantum Cryptology, Systems security, Privacy Protection, Digital Signatures, etc.

It would have been impossible to have a successful Inscrypt 2020 conference without the significant contribution of many people. First, we would like to thank all the authors for submitting their research results to the conference. We were also very grateful to the PC members and external reviewers for contributing their knowledge and expertise and for their hard reviewing work. Second, we were greatly indebted to the Honorary Chairs, Weiqi Luo and Dongdai Lin, and General Chairs, Jian Weng and Robert H. Deng, for their overall and organization efforts. Third, we thank Kaimin Wei and Shanxiang Lyu for organizing the online and offline conference program, Boyu Gao for checking all the latex files and for assembling the files for submission to Springer, and Mr. Chen and the IACR for setting up and maintaining the Web Submission and Review software for the paper submission and review process. Last but not least, we thank Alfred Hofmann, Anna Kramer, and their Springer colleagues for handling the publication of the conference proceedings.

December 2020

Yongdong Wu
Moti Yung

Organization

Inscrypt 2020

16th China International Conference on Information Security and Cryptology

Guangzhou, China
December 11–14, 2020

Sponsored and organized by

State Key Laboratory of Information Security
(Chinese Academy of Sciences) Jinan University

in cooperation with

International Association for Cryptologic Research
Chinese Association for Cryptologic Research

Honorary Chairs

Weiqi Luo	Jinan University, China
Dongdai Lin	Chinese Academy of Sciences, China

General Chairs

Jian Weng	Jinan University, China
Robert H. Deng	Singapore Management University, Singapore

Technical Program Chairs

Yongdong Wu	Jinan University, China
Moti Yung	Google and Columbia University, USA

Organizing Chairs

Kaimin Wei	Jinan University, China
Shanxiang Lyu	Jinan University, China

Steering Committee

Feng Bao	Huawei International, Singapore
Kefei Chen	Hangzhou Normal University, China

Dawu Gu	Shanghai Jiao Tong University, China
Xinyi Huang	Fujian Normal University, China
Hui Li	Xidian University, China
Dongdai Lin	Chinese Academy of Sciences, China
Peng Liu	Pennsylvania State University, USA
Zhe Liu	Nanjing University of Aeronautics and Astronautics, China
Wen-Feng Qi	National Digital Switching System Engineering and Technological Research Center, China
Meiqin Wang	Shandong University, China
XiaoFeng Wang	Indiana University at Bloomington, USA
Xiaoyun Wang	Tsinghua University, China
Jian Weng	Jinan University, China
Moti Yung	Google and Columbia University, USA
Fangguo Zhang	Sun Yat-sen University, China
Huanguo Zhang	Wuhan University, China

PC Members

Binbin Chen	Singapore University of Technology and Design, Singapore
Kai Chen	Chinese Academy of Sciences, China
Yu Chen	Shandong University, China
Jorge Cuellar	University of Passau, Germany
Hong-Ning Dai	Macau University of Science and Technology, China
Jérémie Decouchant	University of Luxembourg, Luxembourg
Muhammed Esgin	Monash University, Australia
Liming Fang	Nanjing University of Aeronautics and Astronautics, China
Dawu Gu	Shanghai Jiao Tong University, China
Jian Guo	Nanyang Technological University, Singapore
Chunpeng Ge	University of Wollongong, Australia
Shoichi Hirose	University of Fukui, Japan
Shujun Li	University of Kent, UK
Yingjiu Li	University of Oregon, USA
Kaitai Liang	University of Surrey, UK
Feng Lin	Zhejiang University, China
Jingqiang Lin	Chinese Academy of Sciences, China
Joseph Liu	Monash University, Australia
Zhe Liu	Nanjing University of Aeronautics and Astronautics, China
Peng Liu	Pennsylvania State University, USA
Jiqiang Lu	Beijing University of Aeronautics and Astronautics, China
Xiapu Luo	The Hong Kong Polytechnic University, China
Di Ma	University of Michigan-Dearborn, USA

Weizhi Meng	Technical University of Denmark, Denmark
Neetesh Saxena	Cardiff University, UK
Hwajeong Seo	Hansung University, Korea
Ling Song	Jinan University, China
Chunhua Su	The University of Aizu, Japan
Willy Susilo	University of Wollongong, Australia
Qiang Tang	New Jersey Institute of Technology, USA
Ding Wang	Nankai University, China
Long Wang	IBM Watson, USA
Zhuo Wei	Huawei Technologies Research, Singapore
Jinming Wen	Jinan University, China
Wenling Wu	Chinese Academy of Sciences, China
Hongjun Wu	Nanyang Technological University, Singapore
Shouhuai Xu	University of Texas at San Antonio, USA
Wenyuan Xu	Zhejiang University, China
Wun-She Yap	Universiti Tunku Abdul Rahman, Malaysia
Tsz Hon Yuen	The University of Hong Kong, China
Lu Zhou	Nanjing University of Aeronautics and Astronautics, China
Fan Zhang	Zhejiang University, China
Kehuan Zhang	The Chinese University of Hong Kong, China Hongkong

Sub-reviewers

Zhenzhen Bao
Chun Guo
Zhaoyang Han
Feiran Huang
Zhuotao Lian
Meicheng Liu
Yaobin Shen
Siang Meng
Yi Tu
Xueqiao Xue
Zhichao Yang
Haibin Zheng

Sponsors

NSFOCUS

HUAWEI

Contents

AI Security

Asymmetric Cipher

Post-quantum Crypto

System Security

Privacy Protection

Secure Sequence

Digital Signature

Mathematical Fundamental

Symmetric Cipher