Lecture Notes in Computer Science 11449

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

Editorial Board

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

Fuchun Guo · Xinyi Huang
Moti Yung (Eds.)

Information Security and Cryptology

14th International Conference, Inscrypt 2018 Fuzhou, China, December 14–17, 2018 Revised Selected Papers

Springer

Editors
Fuchun Guo
University of Wollongong
Wollongong, NSW, Australia

Moti Yung
Columbia University
New York, NY, USA

Xinyi Huang
Fujian Normal University
Fujian, China

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-14233-9 ISBN 978-3-030-14234-6 (eBook)
https://doi.org/10.1007/978-3-030-14234-6

Library of Congress Control Number: 2019932173

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 14th International Conference on Information Security and Cryptology (Inscrypt 2018) was held during December 14–17, 2018, in Fuzhou, China, with more than 170 attendees. Inscrypt is a well-recognized annual international forum for security researchers and cryptographers to exchange their ideas and present their research results, and is held every year in China. This volume contains all papers accepted by Inscrypt 2018. The program chairs also invited seven distinguished researchers to deliver talks. The keynote speakers were Robert Deng from Singapore Management University, Singapore; Jin Li from Guangzhou University, China; Ron Steinfeld from Monash University, Australia; Huaxiong Wang from Nanyang Technological University, Singapore; Yang Xiang from Swinburne University of Technology, Australia; Moti Yung from Columbia University and Google, USA; and Wanlei Zhou from University of Technology Sydney, Australia.

The conference received 93 submissions. Each submission was reviewed by at least three Program Committee members or external reviewers. The Program Committees accepted 31 full papers and 5 short papers to be included in the conference program. The Program Committees selected two papers as the best papers. They are "Cloud-Based Data-Sharing with White-box Access Security Using Verifiable and CCA-Secure Re-encryption from Indistinguishability Obfuscation" by Mingwu Zhang, Yan Jiang, and Willy Susilo, and "Two-Round PAKE Protocol over Lattices without NIZK" by Zengpeng Li and Ding Wang. The program chairs also invited one paper about the analysis of Chinese cryptographic standards to be included in this volume. The proceedings therefore contain all 32 papers revised after the conference.

Inscrypt 2018 was held in cooperation with the International Association for Cryptologic Research (IACR), and was co-organized by the Fujian Provincial Key Lab of Network Security and Cryptology of the Fujian Normal University, and the State Key Laboratory of Information Security (SKLOIS) of the Chinese Academy of Science. Furthermore, Inscrypt 2018 was sponsored by the JUZIX (www.juzix.net/en/index.jhtml).

We would like to thank all 306 authors who submitted their papers to Inscrypt 2018, and the conference attendees for their interest and support. We thank the Program Committee members and the external reviewers for their hard work in reviewing the submissions. We thank the Organizing Committee and all volunteers from Fujian Normal University for their time and effort dedicated to arranging the conference. Finally, we thank the EasyChair system for making the entire process convenient.

January 2019

Fuchun Guo
Xinyi Huang
Moti Yung

Inscrypt 2018

14th International Conference
on Information Security and Cryptology

Fuzhou, China
December 14–17, 2018

Organized and sponsored by

Fujian Provincial Key Laboratory of Network Security and Cryptology
(Fujian Normal University)
State Key Laboratory of Information Security (SKLOIS)
(Chinese Academy of Sciences)
JUZIX Technology Co., Ltd.

in cooperation with

International Association for Cryptologic Research (IACR)

Honorary Chairs

Dongdai Lin	Chinese Academy of Sciences, China
Yi Mu	Fujian Normal University, China

General Chairs

Xiaofeng Chen	Xidian University, China
Changping Wang	Fujian Normal University, China
Li Xu	Fujian Normal University, China

Technical Program Chairs

Fuchun Guo	University of Wollongong, Australia
Xinyi Huang	Fujian Normal University, China
Moti Yung	Columbia University and Google, USA

Organizing Chairs

Wei Wu	Fujian Normal University, China
Shangpeng Wang	Fujian Normal University, China

Publicity Chairs

Rongmao Chen	National University of Defense Technology, China
Zhe Liu	University of Luxembourg, Luxembourg

Publication Chair

Yuexin Zhang	Swinburne University of Technology, Australia

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
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	Snapchat Inc. and Columbia University, USA
Fangguo Zhang	Sun Yat-Sen University, China
Huanguo Zhang	Wuhan University, China

Technical Program Committee

Erman Ayday	Bilkent University, Turkey
Mauro Barni	University of Siena, Italy
Donghoon Chang	NIST, USA
Kai Chen	Chinese Academy of Sciences, China
Yu Chen	Chinese Academy of Sciences, China
Ilyong Chung	Chosun University, South Korea
Ashok Kumar Das	International Institute of Information Technology, India
Jintai Ding	University of Cincinnati, USA
Debin Gao	Singapore Management University, Singapore
Dawu Gu	Shanghai Jiao Tong University, China
Feng Hao	Newcastle University, UK
He Debiao	Wuhan University, China
Vincenzo Iovino	University of Luxembourg, Luxembourg
Peng Jiang	Beijing Institute of Technology, China
Dae-Young Kim	Daegu Catholic University, South Korea
Neeraj Kumar	Deemed University, India
Jianchang Lai	Nanjian Normal University, China
Yingjiu Li	Singapore Management University, Singapore
Kaitai Liang	University of Surrey, UK
Joseph Liu	Monash University, Australia
Yang Liu	Nanyang Technological University, Singapore

Zhe Liu	University of Luxembourg, Luxembourg
Florian Mendel	TU Graz, Austria
Jianting Ning	National University of Singapore, Singapore
Kazumasa Omote	University of Tsukuba, Japan
Giuseppe Persiano	Università degli Studi di Salerno, Italy
Josef Pieprzyk	Queensland University of Technology, Australia
Bertram Poettering	Ruhr-Universität Bochum, Germany
Kouichi Sakurai	Kyushu University, Japan
Jian Shen	Nanjing University of Information Science and Technology, China
Chunhua Su	The University of Aizu, Japan
Siwei Sun	State Key Lab of Information Security, China
Qiang Tang	Cornell University, USA
Tian Tian	National Digital Switching System Engineering and Technological Research Center, China
Ding Wang	Peking University, China
Hao Wang	Shandong Normal University, China
Jianfeng Wang	Xidian University, China
Meiqin Wang	Shandong University, China
Wenling Wu	Chinese Academy of Science, China
Shouhuai Xu	University of Texas at San Antonio, USA
Xun Yi	RMIT University, Australia
Ting Yu	Qatar Computing Research Institute, Qatar
Yu Yu	Shanghai Jiao Tong University, China
Fan Zhang	Zhejiang University, China
Fangguo Zhang	Sun Yat-sen University, China
Rui Zhang	Chinese Academy of Sciences, Chian
Yuexin Zhang	Swinburne University of Technology, Australia
Xianfeng Zhao	Chinese Academy of Sciences, China
Cliff Zou	University of Central Florida, USA

Additional Reviewers

Agrawal, Megha
Anada, Hiroaki
Araujo, Roberto
Bag, Samiran
Bao, Zhenzhen
Bi, Jingguo
Biswas, Koushik
Bu, Kai
Chen, Chien-Ning
Chen, Haoyu
Chen, Hua
Chen, Huashan
Chen, Rongmao
Choi, Rakyong
Ding, Ning
Dobraunig, Christoph
Eichlseder, Maria
Erkin, Zekeriya
Fan, Lei
Feng, Qi
Gao, Guanjun
Ge, Chunpeng
Gong, Zheng
Guo, Chun

Guo, Jiale
Hasan, Munawar
He, Yingzhe
Hu, Chunya
Huang, Tao
Huang, Yan
Huang, Zhengan
Jap, Dirmanto
Jianlong, Tan
Kelarev, Andrei
Kim, Kee Sung
Koide, Hiroshi
Krawczyk, Jacek
Kuchta, Veronika
Lee, Jeeun
Li, Huige
Li, Wei
Li, Wenting
Li, Xiangxue
Li, Zhen
Li, Zhi
Lin, Chao
Lin, Chengjun
Liu, Guozhen
Liu, Yunwen
Liu, Zhen
Long, Yu
Lu, Xianhui
Luo, Yiyuan
Ma, Xuecheng
Meng, Weizhi
Paulet, Russell
Poussier, Romain
Pöppelmann, Thomas
Qiu, Tian
Quaglia, Elizabeth
Ravi, Prasanna
Roy, Partha Sarathi
Santoso, Bagus
Sengupta, Binanda
Singh, Ajit Pratap
Singh, Monika
Sun, Ling
Syalim, Amril
Tang, Yongkang
Tang, Zixin
Tian, Yangguang
Wang, Daibin
Wang, Haijun
Wang, Haoyang
Wang, Huaqun
Wang, Jing
Wang, Lei
Wu, Ge
Xiang, Zejun
Xie, Shaohao
Xu, Jiayun
Xu, Ke
Xue, Haiyang
Yang, Wenzhuo
Yang, Xu
Yuan, Lun-Pin
Zhang, Hailong
Zhang, Huang
Zhang, Kai
Zhang, Lei
Zhang, Mingwu
Zhang, Peng
Zhang, Wenying
Zhang, Yinghui
Zhang, Zhenfei
Zhang, Zheng
Zhang, Zhuoran
Zhao, Shengnan
Zhao, Xinjie
Zheng, Yafei
Zhuang, Jincheng

Contents