

*Commenced Publication in 1973*

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board

David Hutchison

*Lancaster University, Lancaster, UK*

Takeo Kanade

*Carnegie Mellon University, Pittsburgh, PA, USA*

Josef Kittler

*University of Surrey, Guildford, UK*

Jon M. Kleinberg

*Cornell University, Ithaca, NY, USA*

Friedemann Mattern

*ETH Zurich, Zurich, Switzerland*

John C. Mitchell

*Stanford University, Stanford, CA, USA*

Moni Naor

*Weizmann Institute of Science, Rehovot, Israel*

C. Pandu Rangan

*Indian Institute of Technology Madras, Chennai, India*

Bernhard Steffen

*TU Dortmund University, Dortmund, Germany*

Demetri Terzopoulos

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

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

*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

© Springer Nature Switzerland AG 2019

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, express 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

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 JUIX ([www.juix.net/en/index.jhtml](http://www.juix.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

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

## Invited Paper

Security Analysis of SM9 Key Agreement and Encryption . . . . .	3
<i>Zhaohui Cheng</i>	

## Blockchain and Crypto Currency

Evaluating CryptoNote-Style Blockchains . . . . .	29
<i>Runchao Han, Jiangshan Yu, Joseph Liu, and Peng Zhang</i>	
Goshawk: A Novel Efficient, Robust and Flexible Blockchain Protocol . . . . .	49
<i>Cencen Wan, Shuyang Tang, Yuncong Zhang, Chen Pan, Zhiqiang Liu, Yu Long, Zhen Liu, and Yu Yu</i>	
AFCoin: A Framework for Digital Fiat Currency of Central Banks Based on Account Model . . . . .	70
<i>Haibo Tian, Xiaofeng Chen, Yong Ding, Xiaoyan Zhu, and Fangguo Zhang</i>	
Anonymity Reduction Attacks to Monero. . . . .	86
<i>Dimaz Ankaa Wijaya, Joseph Liu, Ron Steinfeld, Dongxi Liu, and Tsz Hon Yuen</i>	
Analysis of Variance of Graph-Clique Mining for Scalable Proof of Work . . .	101
<i>Hiroaki Anada, Tomohiro Matsushima, Chunhua Su, Weizhi Meng, Junpei Kawamoto, Samiran Bag, and Kouichi Sakurai</i>	

## Lattice-Based Cryptology

Preprocess-then-NTT Technique and Its Applications to KYBER and NEWHOPE . . . . .	117
<i>Shuai Zhou, Haiyang Xue, Daode Zhang, Kunpeng Wang, Xianhui Lu, Bao Li, and Jingnan He</i>	
Two-Round PAKE Protocol over Lattices Without NIZK. . . . .	138
<i>Zengpeng Li and Ding Wang</i>	

## Symmetric Cryptology

Improved Integral Attacks on PRESENT-80. . . . .	163
<i>Shi Wang, Zejun Xiang, Xiangyong Zeng, and Shasha Zhang</i>	

Improved Differential Fault Analysis on Authenticated Encryption of PAEQ-128 . . . . .	183
<i>Ruyan Wang, Xiaohan Meng, Yang Li, and Jian Wang</i>	
Improved Indifferentiability Security Bound for the Prefix-Free Merkle-Damgård Hash Function . . . . .	200
<i>Kamel Ammour and Lei Wang</i>	
<b>Applied Cryptography</b>	
Privacy-Preserving Data Outsourcing with Integrity Auditing for Lightweight Devices in Cloud Computing. . . . .	223
<i>Dengzhi Liu, Jian Shen, Yuling Chen, Chen Wang, Tianqi Zhou, and Anxi Wang</i>	
Cloud-Based Data-Sharing Scheme Using Verifiable and CCA-Secure Re-encryption from Indistinguishability Obfuscation . . . . .	240
<i>Mingwu Zhang, Yan Jiang, Hua Shen, Bingbing Li, and Willy Susilo</i>	
An Encrypted Database with Enforced Access Control and Blockchain Validation . . . . .	260
<i>Zhimei Sui, Shangqi Lai, Cong Zuo, Xingliang Yuan, Joseph K. Liu, and Haifeng Qian</i>	
Using Blockchain to Control Access to Cloud Data. . . . .	274
<i>Jiale Guo, Wenzhuo Yang, Kwok-Yan Lam, and Xun Yi</i>	
A Multi-client DSSE Scheme Supporting Range Queries . . . . .	289
<i>Randolph Loh, Cong Zuo, Joseph K. Liu, and Shi-Feng Sun</i>	
Image Authentication for Permissible Cropping. . . . .	308
<i>Haixia Chen, Shangpeng Wang, Hongyan Zhang, and Wei Wu</i>	
<b>Information Security</b>	
Chord: Thwarting Relay Attacks Among Near Field Communications . . . . .	329
<i>Yafei Ji, Luning Xia, Jingqiang Lin, Qiongxiao Wang, Lingguang Lei, and Li Song</i>	
Analyzing Use of High Privileges on Android: An Empirical Case Study of Screenshot and Screen Recording Applications . . . . .	349
<i>Mark H. Meng, Guangdong Bai, Joseph K. Liu, Xiapu Luo, and Yu Wang</i>	
Blockchain-Based Privacy Preserving Deep Learning. . . . .	370
<i>Xudong Zhu, Hui Li, and Yang Yu</i>	

SpamTracer: Manual Fake Review Detection for O2O Commercial Platforms by Using Geolocation Features . . . . .	384
<i>Ruoyu Deng, Na Ruan, Ruidong Jin, Yu Lu, Weijia Jia, Chunhua Su, and Dandan Xu</i>	
A Light-Weight and Accurate Method of Static Integer-Overflow-to-Buffer-Overflow Vulnerability Detection . . . . .	404
<i>Mingjie Xu, Shengnan Li, Lili Xu, Feng Li, Wei Huo, Jing Ma, Xinhua Li, and Qingjia Huang</i>	
<b>Asymmetric Encryption</b>	
Fully Secure Decentralized Ciphertext-Policy Attribute-Based Encryption in Standard Model . . . . .	427
<i>Chuangui Ma, Aijun Ge, and Jie Zhang</i>	
Outsourced Ciphertext-Policy Attribute-Based Encryption with Equality Test. . . . .	448
<i>Yuzhao Cui, Qiong Huang, Jianye Huang, Hongbo Li, and Guomin Yang</i>	
Efficient Adaptively Secure Public-Key Trace and Revoke from Subset Cover Using <i>Déjà Q</i> Framework. . . . .	468
<i>Mriganka Mandal and Ratna Dutta</i>	
Attribute-Based Encryption with Efficient Keyword Search and User Revocation . . . . .	490
<i>Jingwei Wang, Xinchun Yin, Jianting Ning, and Geong Sen Poh</i>	
Public-Key Encryption with Selective Opening Security from General Assumptions. . . . .	510
<i>Dali Zhu, Renjun Zhang, Shuang Hu, and Gongliang Chen</i>	
<b>Foundations</b>	
<i>Confused yet Successful: Theoretical Comparison of Distinguishers for Monobit Leakages in Terms of Confusion Coefficient and SNR. . . . .</i>	533
<i>Eloi de Chérisey, Sylvain Guilley, and Olivier Rioul</i>	
Searching BN Curves for SM9 . . . . .	554
<i>Guiwen Luo and Xiao Chen</i>	
Distribution Properties of Binary Sequences Derived from Primitive Sequences Modulo Square-free Odd Integers . . . . .	568
<i>Qun-Xiong Zheng, Dongdai Lin, and Wen-Feng Qi</i>	

Towards Malicious Security of Private Coin Honest Verifier Zero Knowledge for NP via Witness Encryption. . . . .	586
<i>Jingyue Yu</i>	
Faster Homomorphic Permutation and Optimizing Bootstrapping in Matrix GSW-FHE. . . . .	607
<i>Shuai Liu and Bin Hu</i>	
<b>Short Papers</b>	
A Note on the Sidelnikov-Shestakov Attack of Niederreiter Scheme . . . . .	621
<i>Dingyi Pei and Jingang Liu</i>	
An Efficient Anonymous Authentication Scheme Based on Double Authentication Preventing Signature for Mobile Healthcare Crowd Sensing . . .	626
<i>Jinhui Liu, Yong Yu, Yannan Li, Yanqi Zhao, and Xiaojiang Du</i>	
Understanding User Behavior in Online Banking System . . . . .	637
<i>Yuan Wang, Liming Wang, Zhen Xu, and Wei An</i>	
Privacy-Preserving Remote User Authentication with $k$ -Times Untraceability. . . . .	647
<i>Yangguang Tian, Yingjiu Li, Binanda Sengupta, Robert Huijie Deng, Albert Ching, and Weiwei Liu</i>	
Early Detection of Remote Access Trojan by Software Network Behavior . . .	658
<i>Masatsugu Oya and Kazumasa Omote</i>	
<b>Author Index</b> . . . . .	673