

Founding Editors

Gerhard Goos

Karlsruhe Institute of Technology, Karlsruhe, Germany

Juris Hartmanis

Cornell University, Ithaca, NY, USA


Editorial Board Members

Elisa Bertino

Purdue University, West Lafayette, IN, USA

Wen Gao

Peking University, Beijing, China

Bernhard Steffen 

TU Dortmund University, Dortmund, Germany

Gerhard Woeginger 

RWTH Aachen, Aachen, Germany

Moti Yung


Columbia University, New York, NY, USA

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

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

© Springer Nature Switzerland AG 2021

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, expressed 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 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

Wei qi Luo	Jinan University, China
Dong dai 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
Fanguo 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
J��r��mie 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
 Neetesh Saxena
 Hwajeong Seo
 Ling Song
 Chunhua Su
 Willy Susilo
 Qiang Tang
 Ding Wang
 Long Wang
 Zhuo Wei
 Jinming Wen
 Wenling Wu
 Hongjun Wu
 Shouhuai Xu
 Wenyuan Xu
 Wun-She Yap
 Tsz Hon Yuen
 Lu Zhou

Fan Zhang
 Kehuan Zhang

Technical University of Denmark, Denmark
 Cardiff University, UK
 Hansung University, Korea
 Jinan University, China
 The University of Aizu, Japan
 University of Wollongong, Australia
 New Jersey Institute of Technology, USA
 Nankai University, China
 IBM Watson, USA
 Huawei Technologies Research, Singapore
 Jinan University, China
 Chinese Academy of Sciences, China
 Nanyang Technological University, Singapore
 University of Texas at San Antonio, USA
 Zhejiang University, China
 Universiti Tunku Abdul Rahman, Malaysia
 The University of Hong Kong, China
 Nanjing University of Aeronautics and Astronautics,
 China
 Zhejiang University, China
 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

Polytopic Attack on Round-Reduced Simon32/64 Using Deep Learning	3
<i>Heng-Chuan Su, Xuan-Yong Zhu, and Duan Ming</i>	
DAS-AST: Defending Against Model Stealing Attacks Based on Adaptive Softmax Transformation.	21
<i>Jinyin Chen, Changan Wu, Shijing Shen, Xuhong Zhang, and Jianhao Chen</i>	
Bidirectional RNN-Based Few-Shot Training for Detecting Multi-stage Attack.	37
<i>Bowei Jia, Yunzhe Tian, Di Zhao, Xiaojin Wang, Chenyang Li, Wenjia Niu, Endong Tong, and Jiqiang Liu</i>	
An Illumination Modulation-Based Adversarial Attack Against Automated Face Recognition System.	53
<i>Zhaojie Chen, Puxi Lin, Zoe Lin Jiang, Zhanhang Wei, Sichen Yuan, and Junbin Fang</i>	

Asymmetric Cipher

Generic Construction of Server-Aided Revocable Hierarchical Identity-Based Encryption	73
<i>Yanyan Liu and Yiru Sun</i>	
Fully Secure ABE with Outsourced Decryption against Chosen Ciphertext Attack	83
<i>Ti Wang, Yongbin Zhou, Hui Ma, Yuejun Liu, and Rui Zhang</i>	
An Efficient CCA-Secure Access Control Encryption for Any Policy	104
<i>Gaosheng Tan, Rui Zhang, Hui Ma, and Yang Tao</i>	
Distributed Key Generation for SM9-Based Systems	113
<i>Rui Zhang, Huan Zou, Cong Zhang, Yuting Xiao, and Yang Tao</i>	

Post-quantum Crypto

Chosen Ciphertext Attacks Secure Inner-Product Functional Encryption from Learning with Errors Assumption	133
<i>Kelly Yun and Rui Xue</i>	

CSURF-TWO: CSIDH for the Ratio (2 : 1)	148
<i>Xuejun Fan, Song Tian, Xiu Xu, and Bao Li</i>	
Group Key Exchange Protocols from Supersingular Isogenies.	157
<i>Xuejun Fan, Xiu Xu, and Bao Li</i>	
System Security	
A Paid Message Forwarding Scheme Based on Social Network	177
<i>Yifu Geng, Bo Qin, Wenchang Shi, and Qianhong Wu</i>	
WebSmell: An Efficient Malicious HTTP Traffic Detection Framework Using Data Augmentation	193
<i>Tieming Chen, Zhengqiu Weng, YunPeng Chen, Chenqiang Jin, Mingqi Lv, Tiantian Zhu, and Jianhong Lin</i>	
Blockchain-Based Efficient Public Integrity Auditing for Cloud Storage Against Malicious Auditors	202
<i>Shanshan Li, Chunxiang Xu, Yuan Zhang, Anjia Yang, Xinsheng Wen, and Kefei Chen</i>	
E-SGX: Effective Cache Side-Channel Protection for Intel SGX on Untrusted OS	221
<i>Fan Lang, Huorong Li, Wei Wang, Jingqiang Lin, Fengwei Zhang, Wuqiong Pan, and Qiong Xiao Wang</i>	
Privacy Protection	
Public Verifiable Private Decision Tree Prediction.	247
<i>Hailong Wang, Yi Deng, and Xiang Xie</i>	
P2A: Privacy Preserving Anonymous Authentication Based on Blockchain and SGX	257
<i>Tianlin Song, Wei Wang, Fan Lang, Wenyi Ouyang, Qiong Xiao Wang, and Jingqiang Lin</i>	
Spectrum Privacy Preserving for Social Networks: A Personalized Differential Privacy Approach.	277
<i>Yang Liu, Yong Zeng, Zhihong Liu, and Jianfeng Ma</i>	
LPPRS: New Location Privacy Preserving Schemes Based on Ring Signature over Mobile Social Networks	288
<i>Cailing Cai, Tsz Hon Yuen, Handong Cui, Mingli Wu, and Siu-Ming Yiu</i>	

Secure Sequence

On the Structure Property of PCR's Adjacency Graph with a Prime Order and Its Application of Constructing M-Sequences	307
<i>Congwei Zhou, Jie Guan, Bin Hu, and Kuan He</i>	
Symmetric 2-Adic Complexity of Ding-Helleseth Generalized Cyclotomic Sequences of Period pq	318
<i>Vladimir Edemskiy and Chenhuang Wu</i>	
A Distinguisher for RNGs with LFSR Post-processing.	328
<i>Xinying Wu, Yuan Ma, Tianyu Chen, and Na Lv</i>	
On the k -Error Linear Complexities of De Bruijn Sequences	344
<i>Ming Li, Yupeng Jiang, and Dongdai Lin</i>	

Digital Signature

A Lattice-Based Fully Dynamic Group Signature Scheme Without NIZK. . . .	359
<i>Yiru Sun and Yanyan Liu</i>	
An Efficient Blind Signature Scheme Based on SM2 Signature Algorithm . . .	368
<i>Yudi Zhang, Debiao He, Fangguo Zhang, Xinyi Huang, and Dawei Li</i>	
A New Efficient Quantum Digital Signature Scheme for Multi-bit Messages.	385
<i>Yukun Wang and Mingqiang Wang</i>	

Mathematical Fundamental

An Improvement of Multi-exponentiation with Encrypted Bases Argument: Smaller and Faster.	397
<i>Yi Liu, Qi Wang, and Siu-Ming Yiu</i>	
Number Theoretic Transform: Generalization, Optimization, Concrete Analysis and Applications	415
<i>Zhichuang Liang, Shiyu Shen, Yuantao Shi, Dongni Sun, Chongxuan Zhang, Guoyun Zhang, Yunlei Zhao, and Zhixiang Zhao</i>	
On Galois NFSRs Equivalent to Fibonacci Ones.	433
<i>Jianghua Zhong, Yingyin Pan, and Dongdai Lin</i>	

Symmetric Cipher

Bagua: A NFSR-Based Stream Cipher Constructed Following Confusion and Diffusion Principles.	453
<i>Lin Tan, Xuanyong Zhu, and Wenfeng Qi</i>	

Provable Related-Key Security of Contracting Feistel Networks 466
 Wenqi Yu, Yuqing Zhao, and Chun Guo

Revisiting Construction of Online Cipher in Hash-ECB-Hash Structure 491
 Gang Liu, Peng Wang, Rong Wei, and Dingfeng Ye

Author Index 505