

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>

Yu Yu · Moti Yung (Eds.)

Information Security and Cryptology

17th International Conference, Inscrypt 2021
Virtual Event, August 12–14, 2021
Revised Selected Papers

Editors

Yu Yu 
Shanghai Jiao Tong University
Shanghai, China

Moti Yung 
Columbia University
New York, NY, USA

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-030-88322-5

ISBN 978-3-030-88323-2 (eBook)

<https://doi.org/10.1007/978-3-030-88323-2>

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer Nature Switzerland AG 2021, corrected publication 2022

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 17th International Conference on Information Security and Cryptology (Inscrypt 2021) was originally planned as a hybrid event to take place in Qingdao, China, during August 12–14, 2021. Due to the COVID-19 pandemic, it was eventually held online (virtually). The conference was organized by the State Key Laboratory of Information Security (SKLOIS) of the Institute of Information Engineering of the Chinese Academy of Sciences and the School of Cyber Science and Technology, Shandong University, in cooperation with the IACR.

Inscrypt is an annual international conference held in China, targeting research advances in all areas of information security, cryptology, and their applications. Inscrypt 2021 received 81 submissions from Canada, China, Japan, Morocco, Romania, Slovenia, Switzerland, and the UK. The program committee (PC) was composed of 58 members, who are leading experts on cryptology and security from six countries or regions. The PC team selected 28 papers as full papers. Each submission underwent a double-blind peer-review process and was scrutinized by at least three PC members or sub-reviewers. All the accepted papers are included in this conference proceedings.

We note that the program of Inscrypt 2021 included four excellent invited academic keynote talks by Shengli Liu (China), Ran Canetti (USA), Sanjam Garg (USA), and François-Xavier Standaert (Belgium); we thank the invited speakers for their important contributions to the program. In addition to these keynotes, the program included nine regular presentation sessions on Signatures, System Security, Symmetric Cryptanalysis, Asymmetric Cryptanalysis, Cryptographic Protocols, Mathematical Foundations, Symmetric Cryptography, Public Key Cryptography, and Real World Cryptography.

It would not have been possible to have a successful Inscrypt 2021 without the significant contributions of many people. First, we would like to thank all the authors for submitting their research results to the conference. We are also very grateful to the PC members and external reviewers for contributing their knowledge, expertise, and hard work to assuring the quality of the conference. Secondly, we are greatly indebted to the honorary chairs, Dongdai Lin and Xiaoyun Wang, and to the general co-chairs, Yu Chen and Chun Guo, for their organizational efforts. Thirdly, we thank Puwen Wei for organizing the online conference program. Last but not least, we thank Anna Kramer, Ronan Nugent, and their Springer colleagues for handling the publication of the conference proceedings.

August 2021

Yu Yu
Moti Yung

Organization

Honorary Chairs

Dongdai Lin	Chinese Academy of Sciences, China
Xiaoyun Wang	Tsinghua University, China

General Chairs

Yu Chen	Shandong University, China
Chun Guo	Shandong University, China

Technical Program Chairs

Yu Yu	Shanghai Jiao Tong University, China
Moti Yung	Google LLC and Columbia University, USA

Organizing Chair

Puwen Wei	Shandong 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 LLC and Columbia University, USA
Fangguo Zhang	Sun Yat-sen University, China
Huanguo Zhang	Wuhan University, China

Program Committee

Man Ho Au	The University of Hong Kong, China
Shi Bai	Florida Atlantic University, USA
Davide Bellizia	Université catholique de Louvain, Belgium
Zhenzhen Bao	Nanyang Technological University, Singapore
Qi Chen	Guangzhou University, China
Long Chen	New Jersey Institute of Technology, USA
Rongmao Chen	National University of Defense Technology, China
Xiaofeng Chen	Xidian University, China
Yi Deng	Chinese Academy of Sciences, China
Haixin Duan	Tsinghua University, China
Thanassis Giannetsos	Ubiquitous Technologies Limited, USA
Jian Guo	Nanyang Technological University, Singapore
Qian Guo	Lund University, Sweden
Shuai Han	Shanghai Jiao Tong University, China
Itamar Levi	Bar Ilan University, Israel
Jian Liu	Zhe Jiang University, China
Kaitai Liang	TU Delft, Netherlands
Jingqiang Lin	University of Science and Technology of China, China
Joseph Liu	Monash University, Australia
Juanru Li	Shanghai Jiao Tong University, China
Zhen Ling	Southeast University, China
Meicheng Liu	Chinese Academy of Sciences, China
Qipeng Liu	Princeton University, USA
Junzuo Lai	Jinan University, China
Abe Masayuki	NTT and Kyoto University, Japan
Weizhi Meng	Technical University of Denmark, Denmark
Khoa Nguyen	Nanyang Technological University, Singapore
Jianting Ning	National University of Singapore, Singapore
Emmanouil Panaousis	University of Greenwich, UK
Christophe Petit	Université libre de Bruxelles, Belgium
Thomas Peters	UCLouvain, Belgium
Longjiang Qu	National University of Defense Technology, China
Chao Shen	Xi'an Jiaotong University, China
Ron Steinfeld	Monash University, Australia
Ling Song	Jinan University, China
Ling Sun	Shandong University, China
Siwei Sun	Chinese Academy of Sciences, China
Qiang Tang	The University of Sydney, Australia
Anyu Wang	Tsinghua University, China
Qian Wang	Wuhan University, China
Qingju Wang	University of Luxembourg, Luxembourg
Weijia Wang	Shandong University, China
Xiao Wang	Northwestern University, USA

Xiang Xie	Shanghai Key Laboratory of Privacy-Preserving Computation, China
Peng Xu	Huazhong University of Science and Technology, China
Liang Xiao	Xiamen University, China
Moti Yung	Google LLC and Columbia University, USA
Yu Yu	Shanghai Jiao Tong University, China
Yang Yu	Tsinghua University, China
Bingsheng Zhang	Zhejiang University, China
Jiaheng Zhang	UC Berkeley, USA
Jiang Zhang	State Key Laboratory of Cryptology, China
Lei Zhang	Fudan University, China
Yupeng Zhang	Texas A&M University, USA
Yang Zhang	CISPA Helmholtz Center for Information Security, Germany
Xiaohan Zhang	Fudan University, China
Zhenfeng Zhang	Chinese Academy of Sciences, China
Hong-Sheng Zhou	Virginia Commonwealth University, USA

Sub-reviewers

Weihao Bai	Ming Li	Yi Wang
Alessandro Budroni	Shun Li	Haiyang Xue
Hongrui Cui	Xiangxue Li	Jing Yang
Nan Cui	Yiming Li	Kang Yang
Xiaoyang Dong	Guozhen Liu	Qianqian Yang
Xuejun Fan	Hanlin Liu	Rupeng Yang
Boris Fouotsa	Xiangyu Liu	Li Yao
Junqing Gong	Zhen Liu	Bin Zhang
Haihua Gu	Yonglin Hao	Lulu Zhang
Kaiwen Guo	Guifang Huang	Shuoyao Zhao
Xiaojie Guo	Erik Mårtensson	Zhongxiang Zheng
Debiao He	Phuong Pham	Tanping Zhou
Haodong Jiang	Joost Renes	Yu Zhou
Mingming Jiang	Yao Sun	Yuqing Zhu
Peter Kutas	Phuc Thai	
Chunlei Li	Song Tian	

Sponsor



上海市数据隐私安全计算企业重点实验室
Shanghai Key Laboratory of Privacy-Preserving Computation

Contents

Signatures

Concurrent Signatures from a Variety of Keys	3
<i>George Teşeleanu</i>	
A Generic Construction of Fuzzy Signature	23
<i>Jie Song and Yunhua Wen</i>	
Identity Based Linkable Ring Signature with Logarithmic Size	42
<i>Mohamed Nassurdine, Huang Zhang, and Fangguo Zhang</i>	
Security Analysis of DGM and GM Group Signature Schemes Instantiated with XMSS-T	61
<i>Mahmoud Yehia, Riham AlTawy, and T. Aaron Gulliver</i>	

System Security

UC-Secure Cryptographic Reverse Firewall–Guarding Corrupted Systems with the Minimum Trusted Module	85
<i>Geng Li, Jianwei Liu, Zongyang Zhang, and Yanting Zhang</i>	
A Message Franking Channel	111
<i>Loïs Huguenin-Dumittan and Iraklis Leontiadis</i>	
SPARROWHAWK: Memory Safety Flaw Detection via Data-Driven Source Code Annotation	129
<i>Yunlong Lyu, Wang Gao, Siqu Ma, Qibin Sun, and Juanru Li</i>	

Symmetric Cryptanalysis

A New Approach for Finding Low-Weight Polynomial Multiples	151
<i>Laila El Aïmani</i>	
Differential-Linear Cryptanalysis of the Lightweight Cryptographic Algorithm KNOT	171
<i>Shichang Wang, Shiqi Hou, Meicheng Liu, and Dongdai Lin</i>	
Revisit Two Memoryless State-Recovery Cryptanalysis Methods on A5/1	191
<i>Mingxing Wang and Yonglin Hao</i>	

More Accurate Division Property Propagations Based on Optimized
Implementations of Linear Layers 212
Chunlei Hong, Shasha Zhang, Siwei Chen, Da Lin, and Zejun Xiang

Asymmetric Cryptanalysis

Security Analysis on an ElGamal-Like Multivariate Encryption Scheme
Based on Isomorphism of Polynomials 235
*Yasuhiko Ikematsu, Shuhei Nakamura, Bagus Santoso,
and Takanori Yasuda*

Attacking ECDSA Leaking Discrete Bits with a More Efficient Lattice 251
Shuaigang Li, Shuqin Fan, and Xianhui Lu

Cryptographic Protocols

A Simple Post-Quantum Non-interactive Zero-Knowledge Proof
from Garbled Circuits 269
Hongrui Cui and Kaiyi Zhang

Improved Zero-Knowledge Argument of Encrypted Extended Permutation 281
Yi Liu, Qi Wang, and Siu-Ming Yiu

Mathematical Foundations

Isomorphism and Equivalence of Galois Nonlinear Feedback Shift
Registers 301
Wenhui Kong, Jianghua Zhong, and Dongdai Lin

Elliptic Curve and Integer Factorization 316
Zhizhong Pan and Xiao Li

On the Linear Complexity of Feedforward Clock-Controlled Sequence 331
Yangpan Zhang and Maozhi Xu

Symmetric Cryptography

On Characterization of Transparency Order for (n, m) -functions 351
*Yu Zhou, Yongzhuang Wei, Hailong Zhang, Luyang Li, Enes Pasalic,
and Wenling Wu*

Binary Sequences Derived from Monomial Permutation Polynomials
over $\text{GF}(2^p)$ 371
Qun-Xiong Zheng, Yupeng Jiang, Dongdai Lin, and Wen-Feng Qi

On the Provable Security Against Truncated Impossible Differential Cryptanalysis for AES in the Master-Key Setting	384
<i>Xueping Yan, Lin Tan, Hong Xu, and Wenfeng Qi</i>	
Adaptive Side-Channel Analysis Model and Its Applications to White-Box Block Cipher Implementations	399
<i>Yufeng Tang, Zheng Gong, Tao Sun, Jinhai Chen, and Fan Zhang</i>	
Public Key Cryptography	
Fully Secure Lattice-Based ABE from Noisy Linear Functional Encryption	421
<i>Geng Wang, Ming Wan, Zhen Liu, and Dawu Gu</i>	
Revocable Identity-Based Encryption with Server-Aided Ciphertext Evolution from Lattices	442
<i>Yanhua Zhang, Ximeng Liu, Yupu Hu, and Huiwen Jia</i>	
Homomorphic Modular Reduction and Improved Bootstrapping for BGV Scheme	466
<i>Ruiqi Li and Chunfu Jia</i>	
Real World Cryptography	
Privacy Preserving OpenPGP Public Key Distribution with Spamming Resistance	487
<i>Wenyuan Li, Wei Wang, Jingqiang Lin, Qiong Xiao Wang, and Wenjie Wang</i>	
Collaborative Verifiable Delay Functions	507
<i>Liam Medley and Elizabeth A. Quaglia</i>	
SMCOS: Fast and Parallel Modular Multiplication on ARM NEON Architecture for ECC	531
<i>Wenjie Wang, Wei Wang, Jingqiang Lin, Yu Fu, Lingjia Meng, and Qiong Xiao Wang</i>	
Correction to: Differential-Linear Cryptanalysis of the Lightweight Cryptographic Algorithm KNOT	C1
<i>Shichang Wang, Shiqi Hou, Meicheng Liu, and Dongdai Lin</i>	
Author Index	551