

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

Moti Yung 

Columbia University, New York, NY, USA

More information about this series at <https://link.springer.com/bookseries/558>

Jong Hwan Park · Seung-Hyun Seo (Eds.)

Information Security and Cryptology – ICISC 2021

24th International Conference
Seoul, South Korea, December 1–3, 2021
Revised Selected Papers

Editors

Jong Hwan Park
Sangmyung University
Seoul, Korea (Republic of)

Seung-Hyun Seo 
Hanyang University
Ansan, Korea (Republic of)

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-031-08895-7

ISBN 978-3-031-08896-4 (eBook)

<https://doi.org/10.1007/978-3-031-08896-4>

© The Editor(s) (if applicable) and The Author(s), under exclusive license
to Springer Nature Switzerland AG 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 24th International Conference on Information Security and Cryptology (ICISC 2021) was held during December 1–3, 2021. This year’s conference was hosted by the Korea Institute of Information Security and Cryptology (KIISC).

The aim of the ICISC conference is to provide an international forum for the latest results of research, development, and applications within the field of information security and cryptology. This year, we received 63 submissions and were able to accept 23 papers for presentation at the conference. The challenging review and selection processes were successfully conducted by Program Committee (PC) members and external reviewers via the EasyChair review system. For transparency, it is worth noting that each paper underwent a blind review by at least three PC members. Furthermore, to resolve potential conflicts concerning the reviewer’s decisions, individual review reports were open to all PC members and the review phase was followed by detailed interactive discussions on each paper. For this LNCS post-proceedings, the authors of selected papers had a few weeks to prepare for their final versions, based on the comments received from the reviewers.

The conference featured two invited talks, given by Xiuzhen Cheng and Vadin Lyubashevsky. We thank the invited speakers for their kind acceptances and insightful presentations. We would like to thank all authors who submitted their papers to ICISC 2021, as well as all PC members. It was a truly wonderful experience to work with such talented and hardworking researchers. We also appreciate the external reviewers for assisting the PC members. Finally, we would like to thank all attendees for their active participation and the organizing members who successfully managed this conference. We look forward to seeing you again at next year’s ICISC.

December 2021

Jong Hwan Park
Seung-Hyun Seo

Organization

General Chair

Jae-Cheol Ryu

Chung-Nam National University, South Korea

Organizing Chair

Jong-Hyoun Lee

Sejong University, South Korea

Program Chairs

Jong Hwan Park

Sangmyung University, South Korea

Seung-Hyun Seo

Hanyang University, South Korea

Program Committee

Dong-Guk Han

Kookmin University, South Korea

Sungwook Kim

Seoul Women's University, South Korea

Changhoon Lee

Seoul National University of Science and
Technology, South Korea

Kwangsue Lee

Sejong University, South Korea

Mun Kyu Lee

Inha University, South Korea

Jooyoung Lee

KAIST, South Korea

Hyung Tae Lee

Chung-Ang University, South Korea

Dongyoung Roh

National Security Research Institute, South Korea

Seogchung Seo

Kookmin University, South Korea

Jae Hong Seo

Hanyang University, South Korea

Hwajeong Seo

Hansung University, South Korea

Jihye Kim

Kookmin University, South Korea

Changmin Lee

Korea Institute for Advanced Study, South Korea

Jongsung Kim

Kookmin University, South Korea

Yun Aaram

Ewha Womans University, South Korea

Taek-Young Youn

Dankook University, South Korea

Jung Yeon Hwang

Sungshin Women's University, South Korea

Minhye Seo

Duksung Women's University, South Korea

Heeseok Kim

Korea University, South Korea

Wenling Wu

Institute of Software, Chinese Academy of
Sciences, Beijing

Zhenfu Cao

East China Normal University, China

Qiang Tang	University of Sydney, Australia
Shifeng Sun	Monash University, Australia
Swee-Huay Heng	Multimedia University, Malaysia
Toshihiro Yamauchi	Okayama University, Japan
Jiqiang Lu	Beihang University, China
Jonathan Bootle	IBM Research, USA
Joonsang Baek	University of Wollongong, Australia
Josef Pieprzyk	CSIRO, Australia
Katsuyuki Okeya	Hitachi High-Tech Corporation, Japan
Keita Emura	National Institute of Information and Communications Technology, Japan
Khoa Nguyen	Nanyang Technological University, Singapore
Alptekin Küpçü	Koc Üniversitesi, Turkey
Atsuko Miyaji	Osaka University, Japan
Bimal Roy	Indian Statistical Institute, Kolkata, India
Dongseong Kim	University of Queensland, Australia
Donghoon Chang	IIT-Delhi, India
Hung-Min Sun	National Tsing Hua University, Taiwan
Iraklis Leontiadis	Inpher, USA
Baodong Qin	Xi'an University of Posts and Telecommunications, China
Fuchun Guo	University of Wollongong, Australia
Katsuyuki Takashima	Waseda University, Japan
Xinyi Huang	Fujian Normal University, China
Olivier Sanders	Orange Labs, France
Sherman S. M. Chow	Chinese University of Hong Kong, Hong Kong
Daniel Slamanig	Austrian Institute of Technology, Austria

Contents

Cryptographic Protocol I

Revocable Hierarchical Identity-Based Authenticated Key Exchange	3
<i>Yuki Okano, Junichi Tomida, Akira Nagai, Kazuki Yoneyama, Atsushi Fujioka, and Koutarou Suzuki</i>	
Towards Witness Encryption Without Multilinear Maps	28
<i>Gwangbae Choi and Serge Vaudenay</i>	

Cryptographic Protocol II

Designated-Verifier Linkable Ring Signatures	51
<i>Pourandokht Behrouz, Panagiotis Grontas, Vangelis Konstantakatos, Aris Pagourtzis, and Marianna Spyrou</i>	
ATSSIA: Asynchronous Truly-Threshold Schnorr Signing for Inconsistent Availability	71
<i>Snehil Joshi, Durgesh Pandey, and Kannan Srinathan</i>	

Cryptographic Protocol in Quantum Computer Age

Delegating Supersingular Isogenies over \mathbb{F}_{p^2} with Cryptographic Applications	95
<i>Robi Pedersen and Osmanbey Uzunkol</i>	
Improved Lattice-Based Mix-Nets for Electronic Voting	119
<i>Valeh Farzaliyev, Jan Willemson, and Jaan Kristjan Kaasik</i>	
Practical Post-quantum Password-Authenticated Key Exchange Based-on Module-Lattice	137
<i>Peixin Ren and Xiaozhuo Gu</i>	

Security Analysis

Improved Lattice Enumeration Algorithms by Primal and Dual Reordering Methods	159
<i>Kazuki Yamamura, Yuntao Wang, and Eiichiro Fujisaki</i>	
Compiler-based Attack Origin Tracking with Dynamic Taint Analysis	175
<i>Oliver Braunsdorf, Stefan Sessinghaus, and Julian Horsch</i>	

Security Analysis of Hash Algorithm

Preimage Attacks on 4-Round Keccak by Solving Multivariate Quadratic Systems	195
<i>Congming Wei, Chenhao Wu, Ximing Fu, Xiaoyang Dong, Kai He, Jue Hong, and Xiaoyun Wang</i>	

A Preimage Attack on Reduced GIMLI- HASH	217
<i>Yongseong Lee, Jinkeon Kang, Donghoon Chang, and Seokhie Hong</i>	

Security analysis of Symmetric Key Encryption Algorithm

Algebraic Attacks on Grain-Like Keystream Generators	241
<i>Matthew Beighton, Harry Bartlett, Leonie Simpson, and Kenneth Koon-Ho Wong</i>	

Improved See-In-The-Middle Attacks on AES	271
<i>Jonghyun Park, Hangi Kim, and Jongsung Kim</i>	

Fault and Side-Channel Attack

Differential Fault Attack on Rocca	283
<i>Ravi Anand and Takanori Isobe</i>	

Differential Fault Attack on Lightweight Block Cipher PIPO	296
<i>Seonghyuck Lim, Jaeseung Han, Tae-Ho Lee, and Dong-Guk Han</i>	

Learning-based Side-Channel Analysis on PIPO	308
<i>Ji-Eun Woo, Jaeseung Han, Yeon-Jae Kim, Hye-Won Mun, Seonghyuck Lim, Tae-Ho Lee, Seong-Hyun An, Soo-Jin Kim, and Dong-Guk Han</i>	

Constructions and Designs

Collision-Resistant and Pseudorandom Function Based on Merkle-Damgård Hash Function	325
<i>Shoichi Hirose</i>	

Forward Secure Message Franking	339
<i>Hiroki Yamamuro, Keisuke Hara, Masayuki Tezuka, Yusuke Yoshida, and Keisuke Tanaka</i>	

New General Framework for Algebraic Degree Evaluation of NFSR-Based Cryptosystems	359
<i>Lin Ding and Zheng Wu</i>	

Quantum Circuit

T–depth Reduction Method for Efficient SHA–256 Quantum Circuit Construction 379
Jongheon Lee, Sokjoon Lee, You-Seok Lee, and Dooho Choi

Efficient Quantum Circuit of Proth Number Modular Multiplication 403
Chanho Jeon, Donghoe Heo, MyeongHoon Lee, Sunyeop Kim, and Seokhie Hong

Efficient Implementation

Grover on SM3 421
Gyeongju Song, Kyungbae Jang, Hyunji Kim, Wai-Kong Lee, Zhi Hu, and Hwajeong Seo

SPEEDY on Cortex–M3: Efficient Software Implementation of SPEEDY on ARM Cortex–M3 434
Hyunjun Kim, Kyungbae Jang, Gyeongju Song, Minjoo Sim, Siwoo Eum, Hyunji Kim, Hyeokdong Kwon, Wai-Kong Lee, and Hwajeong Seo

Author Index 445