# Lecture Notes in Computer Science 13218

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

Springer

*Editors*
Jong Hwan Park
Sangmyung Universirsity
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

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-Hyouk 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 |
| Kwangsu 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 Universitesi, Turkey |
| Atsuko Miyaji | Osaka University, Japan |
| Bimal Roy | Indian Statistical Institute, Kolkata, India |
| Dongseong Kim | University of Queensland, Australia |
| Donghoon Chang | IIIT-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

## Cryptographic Protocol II

## Cryptographic Protocol in Quantum Computer Age

## Security Analysis

Security Analysis of Hash Algorithm

Security analysis of Symmetric Key Encryption Algorithm

Fault and Side-Channel Attack

Constructions and Designs

## Quantum Circuit

## Efficient Implementation