

*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, 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*

Gerhard Weikum

*Max Planck Institute for Informatics, Saarbrücken, Germany*

More information about this series at <http://www.springer.com/series/7410>

Seokhie Hong · Jong Hwan Park (Eds.)

# Information Security and Cryptology – ICISC 2016

19th International Conference

Seoul, South Korea, November 30 – December 2, 2016

Revised Selected Papers

*Editors*

Seokhie Hong  
CIST, Korea University  
Seoul  
Korea (Republic of)

Jong Hwan Park  
Sangmyung University  
Seoul  
Korea (Republic of)

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-319-53176-2

ISBN 978-3-319-53177-9 (eBook)

DOI 10.1007/978-3-319-53177-9

Library of Congress Control Number: 2017930645

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer International Publishing AG 2017

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.

Printed on acid-free paper

This Springer imprint is published by Springer Nature

The registered company is Springer International Publishing AG

The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

# Preface

ICISC 2016, the 19th International Conference on Information Security and Cryptology, was held in Seoul, Korea, from November 30 to December 2, 2016. This year the conference was hosted by the KIISC (Korea Institute of Information Security and Cryptology) jointly with the NSR (National Security Research Institute).

The aim of this conference is to provide an international forum for the latest results of research, development, and applications in the field of information security and cryptology. This year we received 69 submissions, and were able to accept 18 papers from 10 countries, with an acceptance rate of 26%. The review and selection processes were carried out by the Program Committee (PC) members, 44 prominent international experts, via the EasyChair review system. First, each paper was blind reviewed, by at least three PC members for most cases. Second, for resolving conflicts on the reviewers' decisions, the individual review reports were open to all PC members, and detailed interactive discussions on each paper followed.

The conference featured two invited talks: "Multivariate Public Key Cryptography" by Jintai Ding; "On Practical Functional Encryption" by Michel Abdalla. We thank those invited speakers for their kind acceptance and interesting presentations. We would like to thank all authors who submitted their papers to ICISC 2016 and all 44 PC members. It was a truly nice experience to work with such talented and hard-working researchers. We also appreciate the external reviewers for assisting the PC members in their particular areas of expertise.

We would like to thank all attendees for their active participation and the Organizing Committee members who managed this conference. Finally, we thank the sponsors NSR (National Security Research Institute) and KONAI.

December 2016

Seokhie Hong  
Jong Hwan Park

# Organization

ICISC 2016 was organized by the Korea Institute of Information Security and Cryptology (KIISC) and NSR (National Security Research Institute)

## Executive Committee

### General Chair

Im-Yeong Lee                      Soonchunhyang University, Korea

### Program Chairs

Seokhie Hong                      CIST, Korea University, Korea  
Jong Hwan Park                      Sangmyung University, Korea

### Organizing Chair

Okyeon Yi                          Kookmin University, Korea

## Program Committee

Olivier Blazy	XLim, Université de Limoges, France
Andrey Bogdanov	Technical University of Denmark, Denmark
Zhenfu Cao	East China Normal University, China
Donghoon Chang	IIIT-Delhi, India
Paolo D'Arco	University of Salerno, Italy
Keita Emura	NICT, Japan
Dong-Guk Han	Kookmin University, South Korea
Swee-Huay Heng	Multimedia University
Deukjo Hong	Chonbuk National University
Xinyi Huang	Fujian Normal University, China
David Jao	University of Waterloo, Canada
Dong Seong Kim	University of Canterbury, New Zealand
Dong-Chan Kim	Kookmin University, South Korea
Howon Kim	Pusan National University, South Korea
Huy Kang Kim	Korea University, South Korea
Alptekin Küpçü	Koc University, Turkey
Taekyoung Kwon	Yonsei University, South Korea
Hyung Tae Lee	Nanyang Technological University, Singapore
Kwangsu Lee	Sejong University, South Korea

Moon Sung Lee	Seoul National University, South Korea
Mun-Kyu Lee	Inha University, South Korea
Pil Joong Lee	POSTECH, South Korea
Joseph K. Liu	Monash University, Australia
Zhe Liu	Nanjing University of Aeronautics and Astronautics, Singapore
Jiqiang Lu	Institute for Infocomm Research, Singapore
Sjouke Mauw	University of Luxembourg, Luxembourg
Florian Mendel	Graz University of Technology, Austria
Atsuko Miyaji	JAIST, Japan
Tarik Moataz	Brown University, USA
Raphael C.-W. Phan	Multimedia University
Josef Pieprzyk	Queensland University of Technology, Australia
Christian Rechberger	DTU, Denmark and Graz University of Technology, Austria
Kouichi Sakurai	Kyushu University, Japan
Jae Hong Seo	Myongji University, South Korea
Rainer Steinwandt	Florida Atlantic University, USA
Marion Videau	Quarkslab and Loria, France
Wenling Wu	Institute of Software, Chinese Academy of Sciences, China
Shouhuai Xu	University of Texas at San Antonio, USA
Toshihiro Yamauchi	Okayama University, Japan
Masaya Yasuda	Kyushu University, Japan
Wei-Chuen Yau	Xiamen University, Malaysia
Dae Hyun Yum	Myongji University, South Korea
Aaram Yun	UNIST

## Additional Reviewers

Hiroaki Anada	Saqib A. Kakvi
Selcuk Baktir	İpek Kızıl
Sanaz Taheri Boshrooyeh	Stefan Koelbl
Ji-Jian Chin	Thomas Korak
Emmanuel Conchon	Mario Larangeira
Deepak Dalai	Zhen Liu
Christoph Dobraunig	Willi Meier
Mohammad Etemad	Kirill Morozov
Olga Gadyatskaya	Johannes Mueller
Yiwen Gao	Koji Nuida
Junqing Gong	Cristina Onete
Feng Hao	Jiaxin Pan
Yahya Hassanzadeh-Nazarabadi	Geovandro Pereira
Shoichi Hirose	Somindu C. Ramanna
Zhi Hu	Arnab Roy
Devriş İşler	Sushmita Ruj
Ravi Jhawar	Yumi Sakemi

Pinaki Sarkar  
Sumanta Sarkar  
Masaya Sato  
Peter Scholl  
Hwajeong Seo  
Jun Shao  
Koutarou Suzuki

Syh-Yuan Tan  
Tyge Tiessen  
Jorge Toro-Pozo  
Rolando Trujillo  
Berkant Ustaoglu  
Licheng Wang



## **Abstracts of Invited Talks**

# Multivariate Public Key Cryptography

Jintai Ding

University of Cincinnati, Cincinnati, US  
jintai.ding@uc.edu

**Abstract.** Multivariate public key cryptosystems (MPKC) are one of the four main families of post-quantum public key cryptosystems. In a MPKC, the public key is given by a set of quadratic polynomials and its security is based on the hardness of solving a set of multivariate polynomials. In this tutorial, we will give a general introduction to the multivariate public key cryptosystems including the main designs, the main attack tools and the mathematical theory behind. We will also present state of the art research in the area.

# Can Functional Encryption Be Practical?

Michel Abdalla

ENS and PSL Research University, Paris, France  
`michel.abdalla@ens.fr`

**Abstract.** Functional encryption is a paradigm that allows users to finely control the amount of information that is revealed by a ciphertext to a given receiver. In this talk, we will discuss some of the main results in the area for both general and specific functionalities. While constructions for general functionalities tend to be quite inefficient, we will see how one can significantly improve the efficiency of such schemes by focusing on specific functionalities, such as inner products. Though less general, such functionalities still seem expressive enough for use in practical settings.

# Contents

## Protocols

A Secure Group-Based AKA Protocol for Machine-Type Communications . . . . .	3
<i>Rosario Giustolisi, Christian Gehrman, Markus Ahlström, and Simon Holmberg</i>	
Secure and Private, yet Lightweight, Authentication for the IoT via PUF and CBKA . . . . .	28
<i>Christopher Huth, Aydin Aysu, Jorge Guajardo, Paul Duplys, and Tim Güneysu</i>	

## Lattice Cryptography

A Practical Post-Quantum Public-Key Cryptosystem Based on spLWE . . . . .	51
<i>Jung Hee Cheon, Kyoohyung Han, Jinsu Kim, Changmin Lee, and Yongha Son</i>	
Analysis of Error Terms of Signatures Based on Learning with Errors . . . . .	75
<i>Jeongsu Kim, Suyong Park, Seonggeun Kim, Busik Jang, Sang Geun Hahn, Sangim Jung, and Dongyoung Roh</i>	

## Encryption

Transforming Hidden Vector Encryption Schemes from Composite to Prime Order Groups . . . . .	101
<i>Kwangsu Lee</i>	
Lossy Key Encapsulation Mechanism and Its Applications . . . . .	126
<i>Yamin Liu, Xianhui Lu, Bao Li, and Haiyang Xue</i>	
Expanded Framework for Dual System Encryption and Its Application . . . . .	145
<i>Minqian Wang and Zhenfeng Zhang</i>	
Adaptively Secure Broadcast Encryption with Dealership . . . . .	161
<i>Kamalesh Acharya and Ratna Dutta</i>	

## Implementation and Algorithms

A New Algorithm for Residue Multiplication Modulo $2^{521} - 1$ . . . . .	181
<i>Shoukat Ali and Murat Cenk</i>	

Enhancing Data Parallelism of Fully Homomorphic Encryption . . . . .	194
<i>Paulo Martins and Leonel Sousa</i>	
An Improvement of Optimal Ate Pairing on KSS Curve with Pseudo 12-Sparse Multiplication . . . . .	208
<i>Md. Al-Amin Khandaker, Hirotaka Ono, Yasuyuki Nogami, Masaaki Shirase, and Sylvain Duquesne</i>	
<b>Signatures (and Protocol)</b>	
Revisiting the Cubic UOV Signature Scheme . . . . .	223
<i>Dung H. Duong, Albrecht Petzoldt, Yacheng Wang, and Tsuyoshi Takagi</i>	
Network Coding Signature Schemes Against Related-Key Attacks in the Random Oracle Model . . . . .	239
<i>Jinyong Chang, Honglong Dai, Maozhi Xu, and Rui Xue</i>	
New Realizations of Efficient and Secure Private Set Intersection Protocols Preserving Fairness . . . . .	254
<i>Sumit Kumar Debnath and Ratna Dutta</i>	
<b>Analysis</b>	
Improved Results on Cryptanalysis of Prime Power RSA . . . . .	287
<i>Liqiang Peng, Lei Hu, and Yao Lu</i>	
On Computing the Immunity of Boolean Power Functions Against Fast Algebraic Attacks . . . . .	304
<i>Yusong Du and Baodian Wei</i>	
Improved Fault Analysis on the Block Cipher SPECK by Injecting Faults in the Same Round . . . . .	317
<i>Jingyi Feng, Hua Chen, Si Gao, Limin Fan, and Dengguo Feng</i>	
On the Effectiveness of Code-Reuse-Based Android Application Obfuscation. . . . .	333
<i>Xiaoxiao Tang, Yu Liang, Xinjie Ma, Yan Lin, and Debin Gao</i>	
<b>Author Index</b> . . . . .	351