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

ICISC 2013, the 16th International Conference on Information Security and Cryptology, was held in Seoul, Korea, during November 27–29, 2013. This year’s conference was hosted by the KIISC (Korea Institute of Information Security and Cryptology) jointly with the NSRI (National Security Research Institute), in cooperation with the Ministry of Science, ICT and Future Planning (MSIP).

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 126 submissions from more than 20 countries and were able to accept 31 papers from 14 countries, with an acceptance rate of 24.6%. The review and selection processes were carried out by the Program Committee (PC) members, 86 prominent experts worldwide, via the IACR review system. Submissions by Program Committee members received at least five reviews. The review process was double-blind, and conflicts of interest were handled carefully.

The conference featured two invited talks: “Making NTRUEncrypt and NTRUSign as Secure as Worst-Case Problems over Ideal Lattices” by Damien Stehlé and “Introduction to Quantum Cryptography and Its Technology Trends” by Jeong Woon Choi. We thank the invited speakers for their kind acceptance and nice presentations.

We would like to thank all authors who submitted their papers to ICISC 2013 and all of the 86 PC members. It was a truly great 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. Finally, we would like to thank all attendees for their active participation and the organizing team who nicely managed this conference. We look forward to seeing you again at next year’s ICISC.

August 2014

Hyang-Sook Lee
Dong-Guk Han
The 16th International Conference on Information Security and Cryptology ICISC 2013

November 27–29, 2013
New Millennium Hall, Konkuk University, Seoul, Korea

Hosted by
Korea Institute of Information Security and Cryptology (KIISC)
National Security Research Institute (NSRI)

Supported by
Ministry of Science, ICT and Future Planning (MSIP)
Electronics and Telecommunications Research Institute (ETRI)
Korea Internet & Security Agency (KISA)
Organization

General Chairs

Sukwoo Kim  Hansei University, Korea
Seok-Yeol Kang  NSRI, Korea

Program Co-chairs

Hyang-Sook Lee  Ewha Womans University, Korea
Dong-Guk Han  Kookmin University, Korea

Program Committee

Gail-Joon Ahn  Arizona State University, USA
Joonsang Baek  Khalifa University, UAE
Yoo-Jin Baek  Woosuk University, Korea
Alex Biryukov  University of Luxembourg, Luxembourg
Andrey Bogdanov  Technical University of Denmark, Denmark
Zhenfu Cao  Shanghai Jiao Tong University, China
Aldar Chan  Institute for Infocomm Research (I2R), A*STAR, Singapore
Kefei Chen  Hangzhou Normal University, China
Dooho Choi  ETRI, Korea
Yongwha Chung  Korea University, Korea
Nora Cuppens  TELECOM Bretagne, France
Paolo D’Arco  Università degli Studi di Salerno, Italy
Rafael Dowsley  Karlsruhe Institute of Technology, Germany
Shaojing Fu  National University of Defence Technology, China
Matthew D. Green  Johns Hopkins University, USA
Johann Großschäd  University of Bristol, UK
JaeCheol Ha  Hoseo University, Korea
Martin Hell  Lund University, Swede
Swee-Huay Heng  Multimedia University, Malaysia
Dowon Hong  Kongju National University, Korea
Jin Hong  Seoul National University, Korea
Jiankun Hu  University of New South Wales, Australia
Jung Yeon Hwang  ETRI, Korea
Eul Gyu Im  Hanyang University, Korea
David Jao  University of Waterloo, Canada
Chong Hee Kim  Brightsight, The Netherlands
Dong Kyue Kim  Hanyang University, Korea
Jorge L. Villar Universitat Politecnica de Catalunya, Spain
Hongxia Wang Southwest Jiaotong University, China
Yongzhuang Wei Guilin University of Electronic Technology, China
Wenling Wu Institute of Software Chinese Academy
            of Sciences, China
Toshihiro Yamauchi Okayama University, Japan
Wei-Chuen Yau Multimedia University, Malaysia
Ching-Hung Yeh Far East University, Taiwan
Sung-Ming Yen National Central University, Taiwan
Yongjin Yeom Kookmin University, Korea
Jeong Hyun Yi Soongsil University, Korea
Kazuki Yoneyama NTT Secure Platform Laboratories, Japan
Myungkeun Yoon Kookmin University, Korea
Dae Hyun Yum Myongji University, Korea
Aaram Yun Ulsan National Institute of Science
            and Technology, Korea
Fangguo Zhang Sun Yat-sen University, China

Organization Chair

Changho Seo Kongju National University, Korea

Organizing Committee

Daesung Kwon NSRI, Korea
Daeyoub Kim Soowon University, Korea
Keecheon Kim Konkuk University, Korea
Kihyo Nam Umlogics, Korea
Heuisu Ryu Gyeongin National University of Education, Korea
Howon Kim Pusan National University, Korea
Junbeom Hur Chung Ang University, Korea
Okyeon Yi Kookmin University, Korea
Seokwon Jeong Mokpo National University, Korea
Sungbeom Pan Chosun University, Korea
Young-Ho Park Sejong Cyber University, Korea
Sanguk Shin Pukyong National University, Korea
## Contents

### Secure Multiparty Computation

**Privacy Assurances in Multiple Data-Aggregation Transactions**

*Kim Le, Parmesh Ramanathan, and Kewal K. Saluja*  
3

**A Secure Priority Queue; Or: On Secure Datastructures from Multiparty Computation**

*Tomas Toft*  
20

**Towards Secure Two-Party Computation from the Wire-Tap Channel**

*Hervé Chabanne, Gérard Cohen, and Alain Patey*  
34

### Proxy Re-encryption

**Combined Proxy Re-encryption**

*Sébastien Canard and Julien Devigne*  
49

**Certificateless Proxy Re-Encryption Without Pairings**

*Kang Yang, Jing Xu, and Zhenfeng Zhang*  
67

### Side Channel Analysis and Its Countermeasures

**Enabling 3-Share Threshold Implementations for all 4-Bit S-Boxes**

*Sebastian Kutzner, Phuong Ha Nguyen, and Axel Poschmann*  
91

**Using Principal Component Analysis for Practical Biasing of Power Traces to Improve Power Analysis Attacks**

*Yongdae Kim and Haengseok Ko*  
109

### Cryptanalysis 1

**Impossible Differential Attack on Reduced-Round TWINE.**

*Xuexin Zheng and Keting Jia*  
123

**Optimal Storage for Rainbow Tables**

*Gildas Avoine and Xavier Carpent*  
144

**First Multidimensional Cryptanalysis on Reduced-Round PRINCE$_{core}$**

*Xiaoqian Li, Bao Li, Wenling Wu, Xiaoli Yu, Ronglin Hao, and Bingke Ma*  
158
Cryptanalysis 2

Rebound Attacks on Stribog .................................................. 175
   Riham AlTawy, Aleksandar Kircanski, and Amr M. Youssef

Bitwise Partial-Sum on HIGHT: A New Tool for Integral Analysis Against ARX Designs ........................................ 189
   Yu Sasaki and Lei Wang

General Model of the Single-Key Meet-in-the-Middle Distinguisher on the Word-Oriented Block Cipher .................. 203
   Li Lin, Wenling Wu, Yanfeng Wang, and Lei Zhang

Embedded System Security and Its Implementation

Integral Based Fault Attack on LBlock .................................. 227
   Hua Chen and Limin Fan

Protecting Ring Oscillator Physical Unclonable Functions Against Modeling Attacks .............................................. 241
   Shohreh Sharif Mansouri and Elena Dubrova

Parallel Implementations of LEA ........................................... 256
   Hwajeong Seo, Zhe Liu, Taehwan Park, Hyunjin Kim, Yeoncheol Lee, Jongseok Choi, and Howon Kim

Primitives for Cryptography

Invertible Polynomial Representation for Private Set Operations .................. 277
   Jung Hee Cheon, Hyunsook Hong, and Hyung Tae Lee

On the Efficacy of Solving LWE by Reduction to Unique-SVP .............. 293
   Martin R. Albrecht, Robert Fitzpatrick, and Florian Göpfert

A Family of Cryptographically Significant Boolean Functions Based on the Hidden Weighted Bit Function ............. 311
   Qichun Wang, Chik How Tan, and Timothy Foo

Digital Signature

Ambiguous One-Move Nominative Signature Without Random Oracles .... 325
   Dennis Y.W. Liu, Duncan S. Wong, and Qiong Huang

A Provably Secure Signature and Signcryption Scheme Using the Hardness Assumptions in Coding Theory ............... 342
   K. Preetha Mathew, Sachin Vasant, and C. Pandu Rangan
An Anonymous Reputation System with Reputation Secrecy for Manager... 363

Toru Nakanishi, Tomoya Nomura, and Nobuo Funabiki

Security Protocol

Database Outsourcing with Hierarchical Authenticated Data Structures... 381

Mohammad Etemad and Alptekin Küçü

Information-Theoretically Secure Entity Authentication in the Multi-user Setting

Shogo Hajime, Yohei Watanabe, and Junji Shikata

Practical Receipt-Free Sealed-Bid Auction in the Coercive Environment... 418

Jaydeep Howlader, Sanjit Kumar Roy, and Ashis Kumar Mal

Recoverable Group Signatures with Compact Revocation List Using Accumulators... 435

Toru Nakanishi and Nobuo Funabiki

Cyber Security

Semantic Feature Selection for Text with Application to Phishing Email Detection... 455

Rakesh Verma and Nabil Hossain

Who Is Sending a Spam Email: Clustering and Characterizing Spamming Hosts... 469

Jiyoung Woo, Hyun Jae Kang, Ah Reum Kang, Hyukmin Kwon, and Huy Kang Kim

Dark Side of the Shader: Mobile GPU-Aided Malware Delivery... 483

Janis Danisevskis, Marta Piekarska, and Jean-Pierre Seifert

Industry-Wide Misunderstandings of HTTPS... 496

Stephen Bono and Jacob Thompson

Public Key Cryptography

Efficient Code Based Hybrid and Deterministic Encryptions in the Standard Model... 517

K. Preetha Mathew, Sachin Vasant, and C. Pandu Rangan

Author Index... 537