## Contents

### Hardware Security

M-ORAM: A Matrix ORAM with Log N Bandwidth Cost .................. 3  
*Steven Gordon, Atsuko Miyaji, Chunhua Su, and Karin Sumongkayothin*

Process Variation Evaluation Using RO PUF for Enhancing SCA-Resistant Dual-Rail Implementation .......................... 16  
*Wei He, Dirmanto Jap, and Alexander Herrmann*

Compact Implementations of LEA Block Cipher for Low-End Microprocessors .............................................. 28  
*Hwajeong Seo, Zhe Liu, Jongseok Choi, Taehwan Park, and Howon Kim*

Compact Implementations of LSH ..................................... 41  
*Taehwan Park, Hwajeong Seo, Zhe Liu, Jongseok Choi, and Howon Kim*

Detection of Rogue Devices in WLAN by Analyzing RF Features and Indoor Location of the Device ............................ 54  
*Hyeokchan Kwon, Kwang-Il Lee, Gaeil An, Byung-Ho Chung, and Jeong-Nyeo Kim*

### Cryptography

Security Analysis on RFID Mutual Authentication Protocol .............. 65  
*You Sung Kang, Elizabeth O’Sullivan, Dooho Choi, and Maire O’Neill*

How Much Randomness Can Be Extracted from Memoryless Shannon Entropy Sources? ........................................ 75  
*Maciej Skorski*

Two Types of Special Bases for Integral Lattices .......................... 87  
*Renzhang Liu and Yanbin Pan*

Keyword Updatable PEKS ............................................. 96  
*Hyun Sook Rhee and Dong Hoon Lee*

On Partitioning Secret Data Based on Concept of Functional Safety .... 110  
*Seira Hidano and Shinsaku Kiyomoto*

Unbounded Hierarchical Identity-Based Encryption with Efficient Revocation ................................................ 122  
*Geumsook Ryu, Kwangsu Lee, Seunghwan Park, and Dong Hoon Lee*
Publishing Graph Data with Subgraph Differential Privacy. . . . . . . . . . . . . . 134
   Binh P. Nguyen, Hoa Ngo, Jihun Kim, and Jong Kim

An Improved Analysis of Broadcast Attacks on the GGH Cryptosystem . . . . 146
   Maoning Wang

Side Channel Attacks and Countermeasures

Secure Binary Field Multiplication . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 161
   Hwajeong Seo, Chien-Ning Chen, Zhe Liu, Yasuyuki Nogami,
   Taehwan Park, Jongseok Choi, and Howon Kim

An Improved Second-Order Power Analysis Attack Based on a New
Refined Expecter: - Case Study on Protected AES - . . . . . . . . . . . . . . . . 174
   Hyunjin Ahn, Neil Hanley, Maire O’Neill, and Dong-Guk Han

Various Threat Models to Circumvent Air-Gapped Systems for Preventing
Network Attack . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 187
   Eunchong Lee, Hyunsoo Kim, and Ji Won Yoon

An Improved Masking Scheme for S-Box Software Implementations. . . . . 200
   Sungjun Ahn and Dooho Choi

Security and Threat Analysis

Open Sesame! Hacking the Password . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 215
   Hwajeong Seo, Zhe Liu, Gyuwon Seo, Taehwan Park, Jongseok Choi,
   and Howon Kim

BurnFit: Analyzing and Exploiting Wearable Devices . . . . . . . . . . . . . . . . 227
   Dongkwan Kim, Suwan Park, Kibum Choi, and Yongdae Kim

Security Analysis of FHSS-type Drone Controller . . . . . . . . . . . . . . . . . . . 240
   Hocheol Shin, Kibum Choi, Youngseok Park, Jaeyeong Choi,
   and Yongdae Kim

Encryption is Not Enough: Inferring User Activities on KakaoTalk
with Traffic Analysis . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 254
   Kyungwon Park and Hyoungshick Kim

IoT Security

Challenges in Deploying CoAP Over DTLS in Resource Constrained
Environments . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 269
   Hyeokjin Kwon, Jiye Park, and Namhi Kang
A Study of OAuth 2.0 Risk Notification and Token Revocation from Resource Server
Jungsoo Park, Jinouk Kim, Minho Park, and Souhwan Jung

Cyber Security Considerations for Designing IoT-Based Control Systems
Kwangho Kim

Frying PAN: Dissecting Customized Protocol for Personal Area Network
Kibum Choi, Yunmok Son, Jangjun Lee, Suryeon Kim, and Yongdae Kim

Structured Design Approach for an Optimal Programmable Synchronous Security Processor
Mahmoud El-Hadidi, Hany El-Sayed, Heba Aslan, and Karim Osama

On Zero Knowledge Argument with PQT Soundness
Guifang Huang and Hongda Li

Network Security

Performance Analysis of Multiple Classifier System in DoS Attack
Bayu Adhi Tama and Kyung Hyune Rhee

Changes of Cybersecurity Legal System in East Asia: Focusing on Comparison Between Korea and Japan
Kwangho Kim, Sangdon Park, and Jongin Lim

Applying Recurrent Neural Network to Intrusion Detection with Hessian Free Optimization
Jihyun Kim and Howon Kim

Application Security

Cost-Effective Modeling for Authentication and Its Application to Activity Tracker
Hiroya Susuki and Rie Shigetomi Yamaguchi

Fully Batch Processing Enabled Memory Integrity Verification Algorithm Based on Merkle Tree
Se Hwan Kim, Yonggon Kim, Ohmin Kwon, and Hyunsoo Yoon

Automatic Security Classification with Lasso
Paal E. Engelstad, Hugo Hammer, Kyrre Wahl Kongsgård, Anis Yazidi, Nils Agne Nordbotten, and Aleksander Bai

Constructing Efficient PAKE Protocols from Identity-Based KEM/DEM
Kyu Young Choi, Jihoon Cho, Jung Yeon Hwang, and Taekyoung Kwon
How to Demonstrate Our Presence Without Disclosing Identity? Evidence from a Grouping-Proof Protocol .......................... 423
   Yunhui Zhuang, Gerhard P. Hancke, and Duncan S. Wong

Author Index .................................................. 437
Information Security Applications
16th International Workshop, WISA 2015, Jeju Island, Korea, August 20-22, 2015, Revised Selected Papers
Kim, H.-w.; Choi, D. (Eds.)
2016, XVI, 438 p. 127 illus., Softcover
ISBN: 978-3-319-31874-5