# Contents

**Cryptography I: Signatures**

Black-Box Separations on Fiat-Shamir-Type Signatures in the Non-Programmable Random Oracle Model .......................... 3  
*Masayuki Fukumitsu and Shingo Hasegawa*

The Generic Transformation from Standard Signatures to Identity-Based Aggregate Signatures ........................................... 21  
*Bei Liang, Hongda Li, and Jinyong Chang*

Leveled Strongly-Unforgeable Identity-Based Fully Homomorphic Signatures ................................................................. 42  
*Fuqun Wang, Kunpeng Wang, Bao Li, and Yuanyuan Gao*

Graded Signatures ................................................................................................................................................................. 61  
*Aggelos Kiayias, Murat Osmanoglu, and Qiang Tang*

**System and Software Security**

Dynamically Provisioning Isolation in Hierarchical Architectures ............ 83  
*Kevin Falzon and Eric Bodden*

Factors Impacting the Effort Required to Fix Security Vulnerabilities: An Industrial Case Study ............................................. 102  
*Lotfi ben Othmane, Golriz Chehrazi, Eric Bodden, Petar Tsakovski, Achim D. Brucker, and Philip Miseldine*

Software Security Maturity in Public Organisations ............................... 120  
*Martin Gilje Jaatun, Daniela S. Cruzes, Karin Bernsmed, Inger Anne Tøndel, and Lillian Røstad*

**Cryptanalysis I: Block Ciphers**

Extending the Applicability of the Mixed-Integer Programming Technique in Automatic Differential Cryptanalysis ............................................... 141  
*Siwei Sun, Lei Hu, Meiqin Wang, Qiangian Yang, Kexin Qiao, Xiaoshuang Ma, Ling Song, and Jinyong Shan*

Automatic Search for Linear Trails of the SPECK Family .......................... 158  
*Yuan Yao, Bin Zhang, and Wenling Wu*
From Distinguishers to Key Recovery: Improved Related-Key Attacks on Even-Mansour ................................................................. 177
Pierre Karpman

Cryptography II: Protocols

Oblivious PAKE: Efficient Handling of Password Trials ..................... 191
Franziskus Kiefer and Mark Manulis

Secure and Efficient Private Set Intersection Cardinality Using Bloom Filter ........................................................................... 209
Sumit Kumar Debnath and Ratna Dutta

On the Efficiency of Multi-party Contract Signing Protocols .............. 227
Gerard Draper-Gil, Josep-Lluís Ferrer-Gomila, M. Francisca Hinarejos, and Jianying Zhou

On the Provable Security of the Dragonfly Protocol ......................... 244
Jean Lancrenon and Marjan Škrobot

Network and Cloud Security

Multipath TCP IDS Evasion and Mitigation ........................................ 265
Zeeshan Afzal and Stefan Lindskog

Provenance Based Classification Access Policy System Based on Encrypted Search for Cloud Data Storage ............................................ 283
Xinyu Fan, Vijay Varadharajan, and Michael Hitchens

Multi-user Searchable Encryption in the Cloud .................................. 299
Cédric Van Rompay, Refik Molva, and Melek Önen

Cryptography III: Encryption and Fundamentals

CCA Secure PKE with Auxiliary Input Security and Leakage Resiliency . . 319
Zhiwei Wang and Siu Ming Yiu

General Circuit Realizing Compact Revocable Attribute-Based Encryption from Multilinear Maps ........................................... 336
Pratish Datta, Ratna Dutta, and Sourav Mukhopadhyay

Hashing into Jacobi Quartic Curves .................................................. 355
Wei Yu, Kunpeng Wang, Bao Li, Xiaoyang He, and Song Tian
Cryptanalysis II

Two Generic Methods of Analyzing Stream Ciphers .......................... 379
   Lin Jiao, Bin Zhang, and Mingsheng Wang

Key Recovery Attacks Against NTRU-Based Somewhat Homomorphic
Encryption Schemes .......................................................... 397
   Massimo Chenal and Qiang Tang

PUFs and Implementation Security

Bit Error Probability Evaluation of RO PUFs ............................. 421
   Qinglong Zhang, Zongbin Liu, Cunqing Ma, and Jiwu Jing

Extracting Robust Keys from NAND Flash Physical Unclonable
Functions ................................................................. 437
   Shijie Jia, Luning Xia, Zhan Wang, Jingqiang Lin,
   Guozhu Zhang, and Yafei Ji

On Security of a White-Box Implementation of SHARK ................. 455
   Yang Shi and Hongfei Fan

GPU-Disasm: A GPU-Based X86 Disassembler ............................ 472
   Evangelos Ladakis, Giorgos Vasiliadis, Michalis Polychronakis,
   Sotiris Ioannidis, and Georgios Portokalidis

Key Generation, Biometrics and Image Security

Reasoning about Privacy Properties of Biometric Systems Architectures
in the Presence of Information Leakage ................................. 493
   Julien Bringer, Hervé Chabanne, Daniel Le Métayer, and Roch Lescuyer

Improvement of Multi-bit Information Embedding Algorithm
for Palette-Based Images ................................................. 511
   Anu Aryal, Kazuma Motegi, Shoko Imaizumi, and Naokazu Aoki

Efficient Ephemeral Elliptic Curve Cryptographic Keys ............... 524
   Andrea Miele and Arjen K. Lenstra

Distributed Parameter Generation for Bilinear Diffie Hellman
Exponentiation and Applications ....................................... 548
   Aggelos Kiayias, Ozgur Oksuz, and Qiang Tang

Author Index ............................................................ 569
Information Security
18th International Conference, ISC 2015, Trondheim, Norway, September 9-11, 2015, Proceedings
Lopez, J.; Mitchell, C.J. (Eds.)
2015, XIII, 570 p. 110 illus., Softcover
ISBN: 978-3-319-23317-8