

Contents

Cryptography I: Signatures

Black-Box Separations on Fiat-Shamir-Type Signatures in the Non-Programmable Random Oracle Model	3
<i>Masayuki Fukumitsu and Shingo Hasegawa</i>	
The Generic Transformation from Standard Signatures to Identity-Based Aggregate Signatures.	21
<i>Bei Liang, Hongda Li, and Jinyong Chang</i>	
Leveled Strongly-Unforgeable Identity-Based Fully Homomorphic Signatures	42
<i>Fuqun Wang, Kunpeng Wang, Bao Li, and Yuanyuan Gao</i>	
Graded Signatures.	61
<i>Aggelos Kiayias, Murat Osmanoglu, and Qiang Tang</i>	

System and Software Security

Dynamically Provisioning Isolation in Hierarchical Architectures	83
<i>Kevin Falzon and Eric Bodden</i>	
Factors Impacting the Effort Required to Fix Security Vulnerabilities: An Industrial Case Study.	102
<i>Lotfi ben Othmane, Golriz Chehrazi, Eric Bodden, Petar Tsalovski, Achim D. Brucker, and Philip Miseldine</i>	
Software Security Maturity in Public Organisations	120
<i>Martin Gilje Jaatun, Daniela S. Cruzes, Karin Bernsmed, Inger Anne Tøndel, and Lillian Røstad</i>	

Cryptanalysis I: Block Ciphers

Extending the Applicability of the Mixed-Integer Programming Technique in Automatic Differential Cryptanalysis	141
<i>Siwei Sun, Lei Hu, Meiqin Wang, Qianqian Yang, Kexin Qiao, Xiaoshuang Ma, Ling Song, and Jinyong Shan</i>	
Automatic Search for Linear Trails of the SPECK Family	158
<i>Yuan Yao, Bin Zhang, and Wenling Wu</i>	

From Distinguishers to Key Recovery: Improved Related-Key Attacks on Even-Mansour	177
<i>Pierre Karpman</i>	

Cryptography II: Protocols

Oblivious PAKE: Efficient Handling of Password Trials	191
<i>Franziskus Kiefer and Mark Manulis</i>	
Secure and Efficient Private Set Intersection Cardinality Using Bloom Filter.	209
<i>Sumit Kumar Debnath and Ratna Dutta</i>	
On the Efficiency of Multi-party Contract Signing Protocols	227
<i>Gerard Draper-Gil, Josep-Lluís Ferrer-Gomila, M. Francisca Hinarejos, and Jianying Zhou</i>	
On the Provable Security of the Dragonfly Protocol	244
<i>Jean Lancrenon and Marjan Škrobot</i>	

Network and Cloud Security

Multipath TCP IDS Evasion and Mitigation	265
<i>Zeeshan Afzal and Stefan Lindskog</i>	
Provenance Based Classification Access Policy System Based on Encrypted Search for Cloud Data Storage	283
<i>Xinyu Fan, Vijay Varadharajan, and Michael Hitchens</i>	
Multi-user Searchable Encryption in the Cloud	299
<i>Cédric Van Rompay, Refik Molva, and Melek Önen</i>	

Cryptography III: Encryption and Fundamentals

CCA Secure PKE with Auxiliary Input Security and Leakage Resiliency	319
<i>Zhiwei Wang and Siu Ming Yiu</i>	
General Circuit Realizing Compact Revocable Attribute-Based Encryption from Multilinear Maps.	336
<i>Pratish Datta, Ratna Dutta, and Sourav Mukhopadhyay</i>	
Hashing into Jacobi Quartic Curves.	355
<i>Wei Yu, Kunpeng Wang, Bao Li, Xiaoyang He, and Song Tian</i>	

Cryptanalysis II

Two Generic Methods of Analyzing Stream Ciphers	379
<i>Lin Jiao, Bin Zhang, and Mingsheng Wang</i>	
Key Recovery Attacks Against NTRU-Based Somewhat Homomorphic Encryption Schemes	397
<i>Massimo Chenal and Qiang Tang</i>	

PUFs and Implementation Security

Bit Error Probability Evaluation of RO PUFs	421
<i>Qinglong Zhang, Zongbin Liu, Cunqing Ma, and Jiwu Jing</i>	
Extracting Robust Keys from NAND Flash Physical Unclonable Functions	437
<i>Shijie Jia, Luning Xia, Zhan Wang, Jingqiang Lin, Guozhu Zhang, and Yafei Ji</i>	
On Security of a White-Box Implementation of SHARK	455
<i>Yang Shi and Hongfei Fan</i>	
GPU-Disasm: A GPU-Based X86 Disassembler	472
<i>Evangelos Ladakis, Giorgos Vasiliadis, Michalis Polychronakis, Sotiris Ioannidis, and Georgios Portokalidis</i>	

Key Generation, Biometrics and Image Security

Reasoning about Privacy Properties of Biometric Systems Architectures in the Presence of Information Leakage	493
<i>Julien Bringer, Hervé Chabanne, Daniel Le Métayer, and Roch Lescuyer</i>	
Improvement of Multi-bit Information Embedding Algorithm for Palette-Based Images	511
<i>Anu Aryal, Kazuma Motegi, Shoko Imaizumi, and Naokazu Aoki</i>	
Efficient Ephemeral Elliptic Curve Cryptographic Keys	524
<i>Andrea Miele and Arjen K. Lenstra</i>	
Distributed Parameter Generation for Bilinear Diffie Hellman Exponentiation and Applications	548
<i>Aggelos Kiayias, Ozgur Oksuz, and Qiang Tang</i>	
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