## Contents

**Secure Multiparty Computation**

Privacy Assurances in Multiple Data-Aggregation Transactions .......................... 3  
  *Kim Le, Parmesh Ramanathan, and Kewal K. Saluja*

A Secure Priority Queue; Or: On Secure Datastructures  
from Multiparty Computation ......................................................... 20  
  *Tomas Toft*

Towards Secure Two-Party Computation from the Wire-Tap Channel .......... 34  
  *Hervé Chabanne, Gérard Cohen, and Alain Patey*

**Proxy Re-encryption**

Combined Proxy Re-encryption ......................................................... 49  
  *Sébastien Canard and Julien Devigne*

Certificateless Proxy Re-Encryption Without Pairings ............................. 67  
  *Kang Yang, Jing Xu, and Zhenfeng Zhang*

**Side Channel Analysis and Its Countermeasures**

Enabling 3-Share Threshold Implementations for all 4-Bit S-Boxes ............ 91  
  *Sebastian Kutzner, Phuong Ha Nguyen, and Axel Poschmann*

Using Principal Component Analysis for Practical Biasing of Power Traces  
to Improve Power Analysis Attacks .............................................. 109  
  *Yongdae Kim and Haengseok Ko*

**Cryptanalysis 1**

Impossible Differential Attack on Reduced-Round TWINE ......................... 123  
  *Xuexin Zheng and Keting Jia*

Optimal Storage for Rainbow Tables ............................................. 144  
  *Gildas Avoine and Xavier Carpent*

First Multidimensional Cryptanalysis on Reduced-Round PRINCE$_{core}$ ...... 158  
  *Xiaoqian Li, Bao Li, Wenling Wu, Xiaoli Yu, Ronglin Hao,  
  and Bingke Ma*
XII  Contents

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 ...................................................... 400
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
Revocable 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
Information Security and Cryptology -- ICISC 2013
16th International Conference, Seoul, Korea, November 27-29, 2013, Revised Selected Papers
Lee, H.-S.; Han, D.-G. (Eds.)
2014, XIII, 538 p. 94 illus., Softcover
ISBN: 978-3-319-12159-8