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

Rebound Attacks on Striboğ .................................................. 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
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>An Anonymous Reputation System with Reputation Secrecy for Manager</td>
<td>363</td>
</tr>
<tr>
<td><em>Toru Nakanishi, Tomoya Nomura, and Nobuo Funabiki</em></td>
<td></td>
</tr>
<tr>
<td><strong>Security Protocol</strong></td>
<td></td>
</tr>
<tr>
<td>Database Outsourcing with Hierarchical Authenticated Data Structures</td>
<td>381</td>
</tr>
<tr>
<td><em>Mohammad Etemad and Alptekin Küçü</em></td>
<td></td>
</tr>
<tr>
<td>Information-Theoretically Secure Entity Authentication in the Multi-user Setting</td>
<td>400</td>
</tr>
<tr>
<td><em>Shogo Hajime, Yohei Watanabe, and Junji Shikata</em></td>
<td></td>
</tr>
<tr>
<td>Practical Receipt-Free Sealed-Bid Auction in the Coercive Environment</td>
<td>418</td>
</tr>
<tr>
<td><em>Jaydeep Howlader, Sanjit Kumar Roy, and Ashis Kumar Mal</em></td>
<td></td>
</tr>
<tr>
<td>Revocable Group Signatures with Compact Revocation List Using Accumulators</td>
<td>435</td>
</tr>
<tr>
<td><em>Toru Nakanishi and Nobuo Funabiki</em></td>
<td></td>
</tr>
<tr>
<td><strong>Cyber Security</strong></td>
<td></td>
</tr>
<tr>
<td>Semantic Feature Selection for Text with Application to Phishing Email Detection</td>
<td>455</td>
</tr>
<tr>
<td><em>Rakesh Verma and Nabil Hossain</em></td>
<td></td>
</tr>
<tr>
<td>Who Is Sending a Spam Email: Clustering and Characterizing Spamming Hosts</td>
<td>469</td>
</tr>
<tr>
<td><em>Jiyoung Woo, Hyun Jae Kang, Ah Reum Kang, Hyukmin Kwon, and Huy Kang Kim</em></td>
<td></td>
</tr>
<tr>
<td>Dark Side of the Shader: Mobile GPU-Aided Malware Delivery</td>
<td>483</td>
</tr>
<tr>
<td><em>Janis Danisevskis, Marta Piekarska, and Jean-Pierre Seifert</em></td>
<td></td>
</tr>
<tr>
<td>Industry-Wide Misunderstandings of HTTPS</td>
<td>496</td>
</tr>
<tr>
<td><em>Stephen Bono and Jacob Thompson</em></td>
<td></td>
</tr>
<tr>
<td><strong>Public Key Cryptography</strong></td>
<td></td>
</tr>
<tr>
<td>Efficient Code Based Hybrid and Deterministic Encryptions in the Standard Model</td>
<td>517</td>
</tr>
<tr>
<td><em>K. Preetha Mathew, Sachin Vasant, and C. Pandu Rangan</em></td>
<td></td>
</tr>
<tr>
<td><strong>Author Index</strong></td>
<td>537</td>
</tr>
</tbody>
</table>
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