

Contents

Secure Multiparty Computation

Privacy Assurances in Multiple Data-Aggregation Transactions.	3
<i>Kim Le, Parmesh Ramanathan, and Kewal K. Saluja</i>	
A Secure Priority Queue; Or: On Secure Datastructures from Multiparty Computation	20
<i>Tomas Toft</i>	
Towards Secure Two-Party Computation from the Wire-Tap Channel	34
<i>Hervé Chabanne, Gérard Cohen, and Alain Patey</i>	

Proxy Re-encryption

Combined Proxy Re-encryption	49
<i>Sébastien Canard and Julien Devigne</i>	
Certificateless Proxy Re-Encryption Without Pairings	67
<i>Kang Yang, Jing Xu, and Zhenfeng Zhang</i>	

Side Channel Analysis and Its Countermeasures

Enabling 3-Share Threshold Implementations for all 4-Bit S-Boxes	91
<i>Sebastian Kutzner, Phuong Ha Nguyen, and Axel Poschmann</i>	
Using Principal Component Analysis for Practical Biasing of Power Traces to Improve Power Analysis Attacks.	109
<i>Yongdae Kim and Haengseok Ko</i>	

Cryptanalysis 1

Impossible Differential Attack on Reduced-Round TWINE.	123
<i>Xuexin Zheng and Keting Jia</i>	
Optimal Storage for Rainbow Tables	144
<i>Gildas Avoine and Xavier Carpent</i>	
First Multidimensional Cryptanalysis on Reduced-Round PRINCE _{core}	158
<i>Xiaoqian Li, Bao Li, Wenling Wu, Xiaoli Yu, Ronglin Hao, and Bingke Ma</i>	

Cryptanalysis 2

Rebound Attacks on Stribog	175
<i>Riham AlTawy, Aleksandar Kircanski, and Amr M. Youssef</i>	
Bitwise Partial-Sum on HIGHT: A New Tool for Integral Analysis Against ARX Designs	189
<i>Yu Sasaki and Lei Wang</i>	
General Model of the Single-Key Meet-in-the-Middle Distinguisher on the Word-Oriented Block Cipher	203
<i>Li Lin, Wenling Wu, Yanfeng Wang, and Lei Zhang</i>	

Embedded System Security and Its Implementation

Integral Based Fault Attack on LBlock	227
<i>Hua Chen and Limin Fan</i>	
Protecting Ring Oscillator Physical Unclonable Functions Against Modeling Attacks	241
<i>Shohreh Sharif Mansouri and Elena Dubrova</i>	
Parallel Implementations of LEA.	256
<i>Hwajeong Seo, Zhe Liu, Taehwan Park, Hyunjin Kim, Yeoncheol Lee, Jongseok Choi, and Howon Kim</i>	

Primitives for Cryptography

Invertible Polynomial Representation for Private Set Operations	277
<i>Jung Hee Cheon, Hyunsook Hong, and Hyung Tae Lee</i>	
On the Efficacy of Solving LWE by Reduction to Unique-SVP	293
<i>Martin R. Albrecht, Robert Fitzpatrick, and Florian Göpfert</i>	
A Family of Cryptographically Significant Boolean Functions Based on the Hidden Weighted Bit Function	311
<i>Qichun Wang, Chik How Tan, and Timothy Foo</i>	

Digital Signature

Ambiguous One-Move Nominative Signature Without Random Oracles.	325
<i>Dennis Y.W. Liu, Duncan S. Wong, and Qiong Huang</i>	
A Provably Secure Signature and Signcryption Scheme Using the Hardness Assumptions in Coding Theory	342
<i>K. Preetha Mathew, Sachin Vasant, and C. Pandu Rangan</i>	

An Anonymous Reputation System with Reputation Secrecy for Manager . . .	363
<i>Toru Nakanishi, Tomoya Nomura, and Nobuo Funabiki</i>	

Security Protocol

Database Outsourcing with Hierarchical Authenticated Data Structures	381
<i>Mohammad Etemad and Alptekin Küpçü</i>	
Information-Theoretically Secure Entity Authentication in the Multi-user Setting	400
<i>Shogo Hajime, Yohei Watanabe, and Junji Shikata</i>	
Practical Receipt-Free Sealed-Bid Auction in the Coercive Environment	418
<i>Jaydeep Howlader, Sanjit Kumar Roy, and Ashis Kumar Mal</i>	
Revocable Group Signatures with Compact Revocation List Using Accumulators	435
<i>Toru Nakanishi and Nobuo Funabiki</i>	

Cyber Security

Semantic Feature Selection for Text with Application to Phishing Email Detection	455
<i>Rakesh Verma and Nabil Hossain</i>	
Who Is Sending a Spam Email: Clustering and Characterizing Spamming Hosts.	469
<i>Jiyoung Woo, Hyun Jae Kang, Ah Reum Kang, Hyukmin Kwon, and Huy Kang Kim</i>	
Dark Side of the Shader: Mobile GPU-Aided Malware Delivery	483
<i>Janis Danisevskis, Marta Piekarska, and Jean-Pierre Seifert</i>	
Industry-Wide Misunderstandings of HTTPS	496
<i>Stephen Bono and Jacob Thompson</i>	

Public Key Cryptography

Efficient Code Based Hybrid and Deterministic Encryptions in the Standard Model	517
<i>K. Preetha Mathew, Sachin Vasant, and C. Pandu Rangan</i>	

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