

Table of Contents

Cryptographic Protocol and Schemes I

Improved Garbled Circuit Building Blocks and Applications to Auctions and Computing Minima	1
<i>Vladimir Kolesnikov, Ahmad-Reza Sadeghi, and Thomas Schneider</i>	
Multi Party Distributed Private Matching, Set Disjointness and Cardinality of Set Intersection with Information Theoretic Security	21
<i>G. Sathya Narayanan, T. Aishwarya, Anugrah Agrawal, Arpita Patra, Ashish Choudhary, and C. Pandu Rangan</i>	
On Cryptographic Schemes Based on Discrete Logarithms and Factoring	41
<i>Marc Joye</i>	

Invited Talk 1

Asymptotically Optimal and Private Statistical Estimation	53
<i>Adam Smith</i>	

Cryptanalysis I

Linear (Hull) and Algebraic Cryptanalysis of the Block Cipher PRESENT	58
<i>Jorge Nakahara Jr., Pouyan Sepehrdad, Bingsheng Zhang, and Meiqin Wang</i>	
Saturation Attack on the Block Cipher HIGHT	76
<i>Peng Zhang, Bing Sun, and Chao Li</i>	
Extensions of the Cube Attack Based on Low Degree Annihilators	87
<i>Aileen Zhang, Chu-Wee Lim, Khoongming Khoo, Lei Wei, and Josef Pieprzyk</i>	
An Analysis of the Compact XSL Attack on BES and Embedded SMS4	103
<i>Jiali Choy, Huihui Yap, and Khoongming Khoo</i>	

Wireless and Sensor Network Security I

RFID Distance Bounding Protocol with Mixed Challenges to Prevent Relay Attacks	119
<i>Chong Hee Kim and Gildas Avoine</i>	

Anonymizer-Enabled Security and Privacy for RFID.....	134
<i>Ahmad-Reza Sadeghi, Ivan Visconti, and Christian Wachsmann</i>	
Blink 'Em All: Scalable, User-Friendly and Secure Initialization of Wireless Sensor Nodes	154
<i>Nitesh Saxena and Md. Borhan Uddin</i>	

Network Security

DepenDNS: Dependable Mechanism against DNS Cache Poisoning	174
<i>Hung-Min Sun, Wen-Hsuan Chang, Shih-Ying Chang, and Yue-Hsun Lin</i>	

Privacy and Anonymity

Privacy-Preserving Relationship Path Discovery in Social Networks.....	189
<i>Ghita Mezzour, Adrian Perrig, Virgil Gligor, and Panos Papadimitratos</i>	
Verifying Anonymous Credential Systems in Applied Pi Calculus.....	209
<i>Xiangxi Li, Yu Zhang, and Yuxin Deng</i>	
Transferable Constant-Size Fair E-Cash	226
<i>Georg Fuchsbauer, David Pointcheval, and Damien Vergnaud</i>	

Functional and Searchable Encryption

A Secure Channel Free Public Key Encryption with Keyword Search Scheme without Random Oracle	248
<i>Liming Fang, Willy Susilo, Chunpeng Ge, and Jiandong Wang</i>	
Private-Key Hidden Vector Encryption with Key Confidentiality	259
<i>Carlo Blundo, Vincenzo Iovino, and Giuseppe Persiano</i>	

Invited Talk 2

Building Secure Networked Systems with Code Attestation (Abstract)	278
<i>Adrian Perrig</i>	

Authentication

HPAKE : Password Authentication Secure against Cross-Site User Impersonation	279
<i>Xavier Boyen</i>	

An Efficient and Provably Secure Cross-Realm Client-to-Client Password-Authenticated Key Agreement Protocol with Smart Cards ...	299
<i>Wenting Jin and Jing Xu</i>	

Ensuring Authentication of Digital Information Using Cryptographic Accumulators	315
<i>Christophe Tartary</i>	

Block Cipher Design

MIBS: A New Lightweight Block Cipher	334
<i>Maryam Izadi, Babak Sadeghiyan, Seyed Saeed Sadeghian, and Hossein Arabnezhad Khanooki</i>	

Cryptanalysis II

Distinguishing and Second-Preimage Attacks on CBC-Like MACs	349
<i>Keting Jia, Xiaoyun Wang, Zheng Yuan, and Guangwu Xu</i>	
Improving the Rainbow Attack by Reusing Colours	362
<i>Martin Ågren, Thomas Johansson, and Martin Hell</i>	
Side Channel Cube Attack on PRESENT	379
<i>Lin Yang, Meiqin Wang, and Siyuan Qiao</i>	
Algebraic Attack on the MQQ Public Key Cryptosystem	392
<i>Mohamed Saied Emam Mohamed, Jintai Ding, Johannes Buchmann, and Fabian Werner</i>	

Algebraic and Number-Theoretic Schemes

Construction of Rotation Symmetric Boolean Functions with Maximum Algebraic Immunity	402
<i>Shaoping Fu, Chao Li, Kanta Matsuura, and Longjiang Qu</i>	
Multi-core Implementation of the Tate Pairing over Supersingular Elliptic Curves	413
<i>Jean-Luc Beuchat, Emmanuel López-Trejo, Luis Martínez-Ramos, Shigeo Mitsunari, and Francisco Rodríguez-Henríquez</i>	
On the Complexity of Computing Discrete Logarithms over Algebraic Tori	433
<i>Shuji Isobe, Eisuke Koizumi, Yuji Nishigaki, and Hiroki Shizuya</i>	

Wireless and Sensor Network Security II

On the Usability of Secure Association of Wireless Devices Based on Distance Bounding	443
<i>Mario Cagalj, Nitesh Saxena, and Ersin Uzun</i>	

Short Hash-Based Signatures for Wireless Sensor Networks 463
Erik Dahmen and Christoph Krauß

Invited Talk 3

Computing on Encrypted Data (Abstract) 477
Craig Gentry

Cryptographic Protocol and Schemes II

Fully Robust Tree-Diffie-Hellman Group Key Exchange 478
Timo Brecher, Emmanuel Bresson, and Mark Manulis

Group Signatures with Verifier-Local Revocation and Backward
Unlinkability in the Standard Model..... 498
Benoît Libert and Damien Vergnaud

Relinkable Ring Signature..... 518
Koutarou Suzuki, Fumitaka Hoshino, and Tetsutaro Kobayashi

Author Index 537