

Table of Contents

Public Key Encryption

On the Broadcast and Validity-Checking Security of PKCS#1 v1.5 Encryption	1
<i>Aurélie Bauer, Jean-Sébastien Coron, David Naccache, Mehdi Tibouchi, and Damien Vergnaud</i>	
How to Construct Interval Encryption from Binary Tree Encryption . . .	19
<i>Huang Lin, Zhenfu Cao, Xiaohui Liang, Muxin Zhou, Haojin Zhu, and Dongsheng Xing</i>	
Shrinking the Keys of Discrete-Log-Type Lossy Trapdoor Functions . . .	35
<i>Xavier Boyen and Brent Waters</i>	

Digital Signature

Trapdoor Sanitizable Signatures Made Easy	53
<i>Dae Hyun Yum, Jae Woo Seo, and Pil Joong Lee</i>	
Generic Constructions for Verifiably Encrypted Signatures without Random Oracles or NIZKs	69
<i>Markus Rückert, Michael Schneider, and Dominique Schröder</i>	
Redactable Signatures for Tree-Structured Data: Definitions and Constructions	87
<i>Christina Brzuska, Heike Busch, Oezguer Dagdelen, Marc Fischlin, Martin Franz, Stefan Katzenbeisser, Mark Manulis, Cristina Onete, Andreas Peter, Bertram Poettering, and Dominique Schröder</i>	

Block Ciphers and Hash Functions

Impossible Differential Cryptanalysis on Feistel Ciphers with <i>SP</i> and <i>SPS</i> Round Functions	105
<i>Yuechuan Wei, Ping Li, Bing Sun, and Chao Li</i>	
Multi-trail Statistical Saturation Attacks	123
<i>Baudoin Collard and Francois-Xavier Standaert</i>	
Multiset Collision Attacks on Reduced-Round SNOW 3G and SNOW 3G [Ⓢ]	139
<i>Alex Biryukov, Deike Priemuth-Schmid, and Bin Zhang</i>	
High Performance GHASH Function for Long Messages	154
<i>Nicolas Méloni, Christophe Nègre, and M. Anwar Hasan</i>	

Side-Channel Attacks

Principles on the Security of AES against First and Second-Order
Differential Power Analysis 168
 Jiqiang Lu, Jing Pan, and Jerry den Hartog

Adaptive Chosen-Message Side-Channel Attacks 186
 Nicolas Veyrat-Charvillon and François-Xavier Standaert

Secure Multiplicative Masking of Power Functions 200
 Laurie Genelle, Emmanuel Prouff, and Michaël Quisquater

Zero Knowledge and Multi-party Protocols

Batch Groth-Sahai 218
 *Olivier Blazy, Georg Fuchsbauer, Malika Izabachène,
 Amandine Jambert, Hervé Sibert, and Damien Vergnaud*

Efficient and Secure Evaluation of Multivariate Polynomials and
Applications 236
 Matthew Franklin and Payman Mohassel

Efficient Implementation of the Orlandi Protocol 255
 Thomas P. Jakobsen, Marc X. Makkes, and Janus Dam Nielsen

Improving the Round Complexity of Traitor Tracing Schemes 273
 Aggelos Kiayias and Serdar Pehlivanoglu

Key Management

Password Based Key Exchange Protocols on Elliptic Curves Which
Conceal the Public Parameters 291
 Julien Bringer, Hervé Chabanne, and Thomas Icart

Okamoto-Tanaka Revisited: Fully Authenticated Diffie-Hellman with
Minimal Overhead 309
 Rosario Gennaro, Hugo Krawczyk, and Tal Rabin

Deniable Internet Key Exchange 329
 Andrew C. Yao and Yunlei Zhao

Authentication and Identification

A New Human Identification Protocol and Coppersmith’s Baby-Step
Giant-Step Algorithm 349
 Hassan Jameel Asghar, Josef Pieprzyk, and Huaxiong Wang

Secure Sketch for Multiple Secrets.....	367
<i>Chengfang Fang, Qiming Li, and Ee-Chien Chang</i>	
A Message Recognition Protocol Based on Standard Assumptions.....	384
<i>Atefeh Mashatan and Serge Vaudenay</i>	

Privacy and Anonymity

Affiliation-Hiding Key Exchange with Untrusted Group Authorities	402
<i>Mark Manulis, Bertram Poettering, and Gene Tsudik</i>	
Privacy-Preserving Group Discovery with Linear Complexity	420
<i>Mark Manulis, Benny Pinkas, and Bertram Poettering</i>	
Two New Efficient PIR-Writing Protocols	438
<i>Helger Lipmaa and Bingsheng Zhang</i>	
Regulatory Compliant Oblivious RAM.....	456
<i>Bogdan Carbunar and Radu Sion</i>	

RFID Security and Privacy

Revisiting Unpredictability-Based RFID Privacy Models	475
<i>Junzuo Lai, Robert H. Deng, and Yingjiu Li</i>	
On RFID Privacy with Mutual Authentication and Tag Corruption	493
<i>Frederik Armknecht, Ahmad-Reza Sadeghi, Ivan Visconti, and Christian Wachsmann</i>	

Internet Security

Social Network-Based Botnet Command-and-Control: Emerging Threats and Countermeasures	511
<i>Erhan J. Kartaltepe, Jose Andre Morales, Shouhuai Xu, and Ravi Sandhu</i>	
COP: A Step toward Children Online Privacy	529
<i>Wei Xu, Sencun Zhu, and Heng Xu</i>	
A Hybrid Method to Detect Deflation Fraud in Cost-Per-Action Online Advertising	545
<i>Xuhua Ding</i>	

Author Index.....	563
-------------------	-----