

# Table of Contents

## Key Exchange

New Modular Compilers for Authenticated Key Exchange . . . . .	1
<i>Yong Li, Sven Schäge, Zheng Yang, Christoph Bader, and Jörg Schwenk</i>	
Password-Based Authenticated Key Exchange without Centralized Trusted Setup . . . . .	19
<i>Kazuki Yoneyama</i>	
A Linear Algebra Attack to Group-Ring-Based Key Exchange Protocols . . . . .	37
<i>M. Kreuzer, A.D. Myasnikov, and A. Ushakov</i>	

## Primitive Construction

Improved Constructions of PRFs Secure against Related-Key Attacks . . . . .	44
<i>Kevin Lewi, Hart Montgomery, and Ananth Raghunathan</i>	
Verifiable Multi-server Private Information Retrieval . . . . .	62
<i>Liang Feng Zhang and Reihaneh Safavi-Naini</i>	
Certified Bitcoins . . . . .	80
<i>Giuseppe Ateniese, Antonio Faonio, Bernardo Magri, and Breno de Medeiros</i>	
Leakage Resilient Proofs of Ownership in Cloud Storage, Revisited . . . . .	97
<i>Jia Xu and Jianying Zhou</i>	
Private Message Transmission Using Disjoint Paths . . . . .	116
<i>Hadi Ahmadi and Reihaneh Safavi-Naini</i>	

## Attacks (Public-Key Cryptography)

Partial Key Exposure Attacks on Takagi's Variant of RSA . . . . .	134
<i>Zhangjie Huang, Lei Hu, Jun Xu, Liqiang Peng, and Yonghong Xie</i>	
New Partial Key Exposure Attacks on CRT-RSA with Large Public Exponents . . . . .	151
<i>Yao Lu, Rui Zhang, and Dongdai Lin</i>	
Bit-Flip Faults on Elliptic Curve Base Fields, Revisited . . . . .	163
<i>Taechan Kim and Mehdi Tibouchi</i>	

## Hashing

All-but-One Dual Projective Hashing and Its Applications . . . . .	181
<i>Zongyang Zhang, Yu Chen, Sherman S.M. Chow, Goichiro Hanaoka, Zhenfu Cao, and Yunlei Zhao</i>	
Distributed Smooth Projective Hashing and Its Application to Two-Server Password Authenticated Key Exchange . . . . .	199
<i>Franziskus Kiefer and Mark Manulis</i>	
Sakura: A Flexible Coding for Tree Hashing . . . . .	217
<i>Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche</i>	
Reset Indifferentiability from Weakened Random Oracle Salvages One-Pass Hash Functions . . . . .	235
<i>Yusuke Naito, Kazuki Yoneyama, and Kazuo Ohta</i>	

## Cryptanalysis & Attacks (Symmetric Cryptography)

Memoryless Unbalanced Meet-in-the-Middle Attacks: Impossible Results and Applications . . . . .	253
<i>Yu Sasaki</i>	
On the (In)Equivalence of Impossible Differential and Zero-Correlation Distinguishers for Feistel- and Skipjack-Type Ciphers . . . . .	271
<i>Céline Blondeau, Andrey Bogdanov, and Meiqin Wang</i>	
Improved Cryptanalysis on Reduced-Round GOST and Whirlpool Hash Function . . . . .	289
<i>Bingke Ma, Bao Li, Ronglin Hao, and Xiaoqian Li</i>	
Differential Cryptanalysis and Linear Distinguisher of Full-Round Zorro . . . . .	308
<i>Yanfeng Wang, Wenling Wu, Zhiyuan Guo, and Xiaoli Yu</i>	
Detecting Hidden Leakages . . . . .	324
<i>Amir Moradi, Sylvain Guilley, and Annelie Heuser</i>	

## Network Security

Improving Intrusion Detection Systems for Wireless Sensor Networks . . .	343
<i>Andriy Stetsko, Tobiáš Smolka, Vashek Matyáš, and Martin Stehlík</i>	
MoTE-ECC: Energy-Scalable Elliptic Curve Cryptography for Wireless Sensor Networks . . . . .	361
<i>Zhe Liu, Erich Wenger, and Johann Großschädl</i>	

BackRef: Accountability in Anonymous Communication Networks . . . . .	380
<i>Michael Backes, Jeremy Clark, Aniket Kate, Milivoj Simeonovski, and Peter Druschel</i>	

WebTrust – A Comprehensive Authenticity and Integrity Framework for HTTP . . . . .	401
<i>Michael Backes, Rainer W. Gerling, Sebastian Gerling, Stefan Nürnberg, Dominique Schröder, and Mark Simkin</i>	

## Signatures

A Revocable Group Signature Scheme from Identity-Based Revocation Techniques: Achieving Constant-Size Revocation List . . . . .	419
<i>Nuttapong Attrapadung, Keita Emura, Goichiro Hanaoka, and Yusuke Sakai</i>	

Faster Batch Verification of Standard ECDSA Signatures Using Summation Polynomials . . . . .	438
<i>Sabyasachi Karati and Abhijit Das</i>	

On Updatable Redactable Signatures . . . . .	457
<i>Henrich C. Pöhls and Kai Samelin</i>	

Practical Signatures from the Partial Fourier Recovery Problem . . . . .	476
<i>Jeff Hoffstein, Jill Pipher, John M. Schanck, Joseph H. Silverman, and William Whyte</i>	

## System Security

Activity Spoofing and Its Defense in Android Smartphones . . . . .	494
<i>Brett Cooley, Haining Wang, and Angelos Stavrou</i>	

Polymorphism as a Defense for Automated Attack of Websites . . . . .	513
<i>Xinran Wang, Tadayoshi Kohno, and Bob Blakley</i>	

Fragmentation Considered Leaking: Port Inference for DNS Poisoning . . . . .	531
<i>Haya Shulman and Michael Waidner</i>	

## Secure Computation

Delegating a Pairing Can Be Both Secure and Efficient . . . . .	549
<i>Sébastien Canard, Julien Devigne, and Olivier Sanders</i>	

Automatic Protocol Selection in Secure Two-Party Computations . . . . .	566
<i>Florian Kerschbaum, Thomas Schneider, and Axel Schröpfer</i>	

Author Index . . . . .	585
------------------------	-----