Table of Contents

Block Ciphers

Cryptanalysis of Reduced-Round MIBS Block Cipher 1
Asli Bay, Jorge Nakahara Jr., and Serge Vaudenay

Impossible Differential Cryptanalysis of ARIA Reduced to 7 Rounds ... 20
Chenghang Du and Jiazhe Chen

An Algorithm Based Concurrent Error Detection Scheme for AES..... 31
Chang N. Zhang, Qian Yu, and Xiao Wei Liu

Invited Talk I

Cryptography for Unconditionally Secure Message Transmission in Networks (Abstract)..... 43
Kaoru Kurosawa

Wireless Network Security

Performance and Security Aspects of Client-Side SSL/TLS Processing on Mobile Devices..... 44
Johann Großschädl and Ilya Kizhvatov

A Practical Cryptographic Denial of Service Attack against 802.11i TKIP and CCMP 62
Martin Eian

User Tracking Based on Behavioral Fingerprints 76
Günther Lackner, Peter Teufl, and Roman Weinberger

Hash Functions

On the Collision and Preimage Resistance of Certain Two-Call Hash Functions 96
Nasour Bagheri, Praveen Gauravaram, Majid Naderi, and Søren S. Thomsen

Integral Distinguishers of Some SHA-3 Candidates 106
Marine Minier, Raphael C.-W. Phan, and Benjamin Pousse

Near-Collisions on the Reduced-Round Compression Functions of Skein and BLAKE..... 124
Bozhan Su, Wenling Wu, Shuang Wu, and Le Dong

Public Key Cryptography

Practical Algebraic Cryptanalysis for Dragon-Based Cryptosystems 140
Johannes Buchmann, Stanislav Bulygin, Jintai Ding, Wael Said Abd Elmageed Mohamed, and Fabian Werner

Generating Parameters for Algebraic Torus-Based Cryptosystems 156
Tomoko Yonemura, Yoshikazu Hanatani, Taichi Isogai, Kenji Ohkuma, and Hirofumi Muratani

Analysis of the MQQ Public Key Cryptosystem 169
Jean-Charles Faugère, Rune Steinsmo Ødegård, Ludovic Perret, and Danilo Gligoroski

Efficient Scalar Multiplications for Elliptic Curve Cryptosystems Using Mixed Coordinates Strategy and Direct Computations 184
Roghaie Mahdavi and Abolghasem Saiadian

Invited Talk II

Cryptography Meets Hardware: Selected Topics of Hardware-Based Cryptography (Abstract) 199
Ahmad-Reza Sadeghi

Secure Mechanisms

Towards a Cryptographic Treatment of Publish/Subscribe Systems 201
Tsz Hon Yuen, Willy Susilo, and Yi Mu

STE3D-CAP: Stereoscopic 3D CAPTCHA 221
Willy Susilo, Yang-Wai Chow, and Hua-Yu Zhou

TRIOB: A Trusted Virtual Computing Environment Based on Remote I/O Binding Mechanism 241
Haifeng Fang, Hui Wang, Yiqiang Zhao, Yuzhong Sun, and Zhiyong Liu

Cryptographic Protocols

Dynamic Group Key Exchange Revisited 261
Guomin Yang and Chik How Tan

Towards Practical and Secure Coercion-Resistant Electronic Elections 278
Roberto Araújo, Narjes Ben Rajeb, Riadh Robbana, Jacques Traoré, and Souheib Yousfi

Anonymous Credentials

Predicate Encryption with Partial Public Keys 298
Carlo Blundo, Vincenzo Iovino, and Giuseppe Persiano

Anonymous Credential Schemes with Encrypted Attributes..... 314
Jorge Guajardo, Bart Mennink, and Berry Schoenmakers

One Time Anonymous Certificate: X.509 Supporting Anonymity 334
Aymen Abed and Sébastien Canard

Author Index 355