# Table of Contents

## Cryptanalysis

Integral Cryptanalysis of ARIA ..... 1
*Ping Li, Bing Sun, and Chao Li*

Cryptanalysis of the ESSENCE Family of Hash Functions ..... 15
*Nicky Mouha, Gautham Sekar, Jean-Philippe Aumasson, Thomas Peyrin, Søren S. Thomsen, Meltem Sönmez Turan, and Bart Preneel*

Differential-Multiple Linear Cryptanalysis ..... 35
*Zhiqiang Liu, Dawu Gu, Jing Zhang, and Wei Li*

Differential Attack on Five Rounds of the SC2000 Block Cipher ..... 50
*Jiqiang Lu*

## Signature and Signcryption

Pairing-Based Nominative Signatures with Selective and Universal Convertibility ..... 60
*Wei Zhao and Dingfeng Ye*

Cryptanalysis of Certificateless Signcryption Schemes and an Efficient Construction without Pairing ..... 75
*S. Sharmila Deva Selvi, S. Sree Vivek, and C. Pandu Rangan*

Sanitizable Signatures with Strong Transparency in the Standard Model ..... 93
*Shivank Agrawal, Swarun Kumar, Amjed Shareef, and C. Pandu Rangan*

Breaking and Building of Threshold Signcryption Schemes ..... 108
*S. Sharmila Deva Selvi, S. Sree Vivek, Shilpi Nayak, and C. Pandu Rangan*

## Key Exchange

Provably Secure Password-Authenticated Group Key Exchange with Different Passwords under Standard Assumption ..... 124
*Fengjiao Wang and Yuqing Zhang*

An Enhanced Password Authenticated Key Agreement Protocol for Wireless Mobile Network ..... 134
*Zhigang Gao and Dengguo Feng*

Efficient Password-Based Authenticated Key Exchange Protocol in the UC Framework ..... 144
*Xuexian Hu and Wenfen Liu*

## Private Computations

Efficient Generalized Selective Private Function Evaluation with Applications in Biometric Authentication ..... 154
*Helger Lipmaa and Bingsheng Zhang*

Optionally Identifiable Private Handshakes ..... 164
*Yanjiang Yang, Jian Weng, Jianying Zhou, and Ying Qiu*

Communication Efficient Statistical Asynchronous Multiparty Computation with Optimal Resilience ..... 179
*Arpita Patra, Ashish Choudhury, and C. Pandu Rangan*

## Cipher Design and Analysis

Gemstone: A New Stream Cipher Using Coupled Map Lattice ..... 198
*Ruming Yin, Jian Yuan, Qiuhua Yang, Xiuming Shan, and Xiqin Wang*

Proposition of Two Cipher Structures ..... 215
*Lei Zhang, Wenling Wu, and Liting Zhang*

Hardware Framework for the Rabbit Stream Cipher ..... 230
*Deian Stefan*

Linearity within the SMS4 Block Cipher ..... 248
*Muhammad Reza Z'aba, Leonie Simpson, Ed Dawson, and Kenneth Wong*

Algebraic Cryptanalysis of Curry and Flurry Using Correlated Messages ..... 266
*Jean-Charles Faugère and Ludovic Perret*

## Public Key Cryptography

Weak Keys in RSA with Primes Sharing Least Significant Bits ..... 278
*Xianmeng Meng and Jingguo Bi*

Hybrid Proxy Re-encryption Scheme for Attribute-Based Encryption ... 288
*Takeo Mizuno and Hiroshi Doi*

Constructing Better KEMs with Partial Message Recovery ..... 303
*Rui Zhang and Hideki Imai*

## Network and System Security

A Novel Contagion-Like Patch Dissemination Mechanism against Peer-to-Peer File-Sharing Worms ..... 313
*Xiaofeng Nie, Jiwu Jing, and Yuewu Wang*

Remodeling Vulnerability Information ..... 324
*Feng Cheng, Sebastian Roschke, Robert Schuppenies, and Christoph Meinel*

Using Strategy Objectives for Network Security Analysis ..... 337
*Elie Bursztein and John C. Mitchell*

## Hardware Security

A DAA Scheme Requiring Less TPM Resources ..... 350
*Liqun Chen*

Full-Custom VLSI Design of a Unified Multiplier for Elliptic Curve Cryptography on RFID Tags ..... 366
*Johann Großschädl*

Weaknesses in Two Recent Lightweight RFID Authentication Protocols ..... 383
*Pedro Peris-Lopez, Julio C. Hernandez-Castro, Juan M.E. Tapiador, Tieyan Li, and Jan C.A. van der Lubbe*

Algebraic Side-Channel Attacks ..... 393
*Mathieu Renauld and François-Xavier Standaert*

## Web Security

CAPTCHA Phishing: A Practical Attack on Human Interaction Proofing ..... 411
*Le Kang and Ji Xiang*

An Attack and Repair of Secure Web Transaction Protocol for Anonymous Mobile Agents ..... 426
*Saba Jalal and Brian King*

A Formal Language for Specifying Complex XML Authorisations with Temporal Constraints ..... 443
*Sean Policarpio and Yan Zhang*

**Author Index** ..... 459