# Table of Contents

## Intrusion Avoidance and Detection

Adaptive Detection of Local Scanners  
*Ahren Studer, Chenxi Wang* ............................................ 1

Probabilistic Proof of an Algorithm to Compute TCP Packet Round-Trip Time for Intrusion Detection  
*Jianhua Yang, Yongzhong Zhang* .................................... 18

DSO: Dependable Signing Overlay  
*Guofei Gu, Prahlad Fogla, Wenke Lee, Douglas Blough* ........ 33

## Cryptographic Applications

Do Broken Hash Functions Affect the Security of Time-Stamping Schemes?  
*Ahto Duldas, Sven Laur* ............................................. 50

A Handy Multi-coupon System  
*Sébastien Canard, Aline Gouget, Emeline Hufschmitt* ............. 66

An Efficient Single-Key Pirates Tracing Scheme Using Cover-Free Families  
*Dongvu Tonien, Reihaneh Safavi-Naini* ............................ 82

## DoS: Attacks and Countermeasures

Efficient Memory Bound Puzzles Using Pattern Databases  
*Sujata Doshi, Fabian Monrose, Aviel D. Rubin* ..................... 98

Effect of Malicious Synchronization  
*Mun Choon Chan, Ec-Chien Chang, Liming Lu.  
Peng Song Ngiam* ..................................................... 114

Misusing Unstructured P2P Systems to Perform DoS Attacks: The Network That Never Forgets  
*Elias Athanasopoulos, Kostas G. Anagnostakis,  
Evangelos P. Markatos* ............................................. 130
Key Management

Password Based Server Aided Key Exchange
  Yvonne Cliff, Yiu Shing Terry Tin, Colin Boyd ....................... 146

Secure Password-Based Authenticated Group Key Agreement for
Data-Sharing Peer-to-Peer Networks
  Qiang Tang, Kim-Kwang Raymond Choo ............................... 162

Stateful Subset Cover
  Mattias Johansson, Gunnar Kreitz, Fredrik Lindholm ............... 178

Cryptanalysis

The Rainbow Attack on Stream Ciphers Based on Maiorana-McFarland
Functions
  Khoongming Khoo, Guang Gong, Hian-Kiat Lee ....................... 194

Breaking a New Instance of TTM Cryptosystems
  Xuyin Nie, Lei Hu, Jinyu Li, Crystal Updegrove, Jintai Ding .......... 210

Cryptanalysis of the N-Party Encrypted Diffie-Hellman Key Exchange
Using Different Passwords
  Raphael C.-W. Phan, Bok-Min Goi ................................. 226

Security of Limited Devices

An AES Smart Card Implementation Resistant to Power Analysis
Attacks
  Christoph Herbst, Elisabeth Oswald, Stefan Mangard ............... 239

Physical Security Bounds Against Tampering
  Kerstin Lemke, Christof Paar, Ahmad-Reza Sadeghi ................. 253

Flexible Exponentiation with Resistance to Side Channel Attacks
  Camille Vuillaume, Katsuyuki Okeya ................................ 268

Cryptography

An Improved Poly1305 MAC
  Dayin Wang, Dongdai Lin, Wenling Wu .............................. 284
Certificateless Public-Key Signature: Security Model and Efficient Construction  
Zhenfeng Zhang, Duncan S. Wong, Jing Xu, Dengguo Feng  
293

High Diffusion Cipher: Encryption and Error Correction in a Single Cryptographic Primitive  
Chetan Nanjunda Mathur, Karthik Narayan, K.P. Subbalakshmi  
309

Authentication and Web Security

Authentication for Paranoids: Multi-party Secret Handshakes  
Stanislaw Jarecki, Jihye Kim, Gene Tsudik  
325

Xinghua Li, SangJae Moon, Jianfeng Ma  
340

W3Bcrypt: Encryption as a Stylesheet  
Angelos Stavrou, Michael E. Locasto, Angelos D. Keromytis  
349

Ad Hoc and Sensor Network Security

Combinatorial Structures for Design of Wireless Sensor Networks  
Dibyendu Chakrabarti, Jennifer Seberry  
365

Public Key Cryptography Sans Certificates in Ad Hoc Networks  
Nitesh Saxena  
375

Location-Aware Key Management Using Multi-layer Grids for Wireless Sensor Networks  
JongHyup Lee, TaeKyoung Kwon, Joosook Song  
390

Cryptographic Constructions

A General Methodology for Pipelining the Point Multiplication Operation in Curve Based Cryptography  
Kishan Chand Gupta, Pradeep Kumar Mishra, Pinakpani Pal  
405

Results on Almost Resilient Functions  
Pinhui Ke, Jie Zhang, Qiaoyan Wen  
421

Real Perfect Contrast Visual Secret Sharing Schemes with Reversing  
Ching-Nung Yang, Chung-Chun Wang, Tse-Shih Chen  
433
Security and Privacy

On Optimizing the Security-Throughput Trade-Off in Wireless Networks with Adversaries

Mohamed A. Haleem, Chetan Nanjunda Mathur, R. Chandramouli, K.P. Subbalakshmi ........................................... 448

Improving the Randomized Initial Point Countermeasure Against DPA

Kouichi Itoh, Tetsuya Izu, Masahiko Takenaka ...................... 459

Syntax-Driven Private Evaluation of Quantified Membership Queries

Aggelos Kiayias, Antonina Mitrofanova ................................ 470

Author Index ................................................................. 487