

Table of Contents

Authentication

Security Analysis of a Multi-factor Authenticated Key Exchange Protocol	1
<i>Feng Hao and Dylan Clarke</i>	
Breaking an Animated CAPTCHA Scheme	12
<i>Vu Duc Nguyen, Yang-Wai Chow, and Willy Susilo</i>	
Contextual OTP: Mitigating Emerging Man-in-the-Middle Attacks with Wireless Hardware Tokens	30
<i>Assaf Ben-David, Omer Berkman, Yossi Matias, Sarvar Patel, Cem Paya, and Moti Yung</i>	

Key Management

RIKE: Using Revocable Identities to Support Key Escrow in PKIs	48
<i>Nan Zhang, Jingqiang Lin, Jiwu Jing, and Neng Gao</i>	
TreVisor: OS-Independent Software-Based Full Disk Encryption Secure against Main Memory Attacks	66
<i>Tilo Müller, Benjamin Taubmann, and Felix C. Freiling</i>	

Block Ciphers

Authenticated Encryption: How Reordering Can Impact Performance ...	84
<i>Basel Alomair</i>	
Length-Doubling Ciphers and Tweakable Ciphers	100
<i>Haibin Zhang</i>	
Extending Higher-Order Integral: An Efficient Unified Algorithm of Constructing Integral Distinguishers for Block Ciphers	117
<i>Wentao Zhang, Bozhan Su, Wenling Wu, Dengguo Feng, and Chuankun Wu</i>	

Identity-Based Cryptography

Security Enhancements by OR-Proof in Identity-Based Identification ...	135
<i>Atsushi Fujioka, Taiichi Saito, and Keita Xagawa</i>	

Identity-Based Extractable Hash Proofs and Their Applications	153
<i>Yu Chen, Zongyang Zhang, Dongdai Lin, and Zhenfu Cao</i>	

Cryptographic Primitives

On Structural Signatures for Tree Data Structures	171
<i>Kai Samelin, Henrich C. Pöhls, Arne Bilzhaue, Joachim Posegga, and Hermann de Meer</i>	
Inner-Product Lossy Trapdoor Functions and Applications	188
<i>Xiang Xie, Rui Xue, and Rui Zhang</i>	
On the Joint Security of Signature and Encryption Schemes under Randomness Reuse: Efficiency and Security Amplification	206
<i>Afonso Arriaga, Manuel Barbosa, and Pooya Farshim</i>	
Secure Accumulators from Euclidean Rings without Trusted Setup	224
<i>Helger Lipmaa</i>	

Cryptanalysis

Linear Fault Analysis of Block Ciphers	241
<i>Zhiqiang Liu, Dawu Gu, Ya Liu, and Wei Li</i>	
Cryptanalysis of 256-Bit Key HyRAL via Equivalent Keys	257
<i>Yuki Asano, Shingo Yanagihara, and Tetsu Iwata</i>	
Distinguishers beyond Three Rounds of the RIPEMD-128/-160 Compression Functions	275
<i>Yu Sasaki and Lei Wang</i>	

Side Channel Attacks

Zero-Value Point Attacks on Kummer-Based Cryptosystem	293
<i>Fangguo Zhang, Qiping Lin, and Shengli Liu</i>	
PICARO – A Block Cipher Allowing Efficient Higher-Order Side-Channel Resistance	311
<i>Gilles Piret, Thomas Roche, and Claude Carlet</i>	
Wide Collisions in Practice	329
<i>Xin Ye and Thomas Eisenbarth</i>	

Network Security

A General Construction for 1-Round δ -RMT and $(0, \delta)$ -SMT	344
<i>Reihaneh Safavi-Naini, Mohammed Ashrafal Alam Tuhin, and Pengwei Wang</i>	

A Prefiltering Approach to Regular Expression Matching for Network Security Systems	363
<i>Tingwen Liu, Yong Sun, Alex X. Liu, Li Guo, and Binxing Fang</i>	

Web Security

iHTTP: Efficient Authentication of Non-confidential HTTP Traffic	381
<i>Jason Gionta, Peng Ning, and Xiaolan Zhang</i>	
ARC: Protecting against HTTP Parameter Pollution Attacks Using Application Request Caches	400
<i>Elias Athanasopoulos, Vasileios P. Kemerlis, Michalis Polychronakis, and Evangelos P. Markatos</i>	
Tracking the Trackers: Fast and Scalable Dynamic Analysis of Web Content for Privacy Violations	418
<i>Minh Tran, Xinshu Dong, Zhenkai Liang, and Xuxian Jiang</i>	

Security and Privacy in Social Networks

The Shy Mayor: Private Badges in GeoSocial Networks	436
<i>Bogdan Carbutnar, Radu Sion, Rahul Potharaju, and Moussa Ehsan</i>	
Detecting Social Spam Campaigns on Twitter	455
<i>Zi Chu, Indra Widjaja, and Haining Wang</i>	

Security and Privacy in RFID Systems

A New Framework for Privacy of RFID Path Authentication	473
<i>Shaoying Cai, Robert H. Deng, Yingjiu Li, and Yunlei Zhao</i>	
<i>GHB</i> [#] : A Provably Secure <i>HB</i> -Like Lightweight Authentication Protocol	489
<i>Panagiotis Rizomiliotis and Stefanos Gritzalis</i>	

Security and Privacy in Cloud Systems

Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud	507
<i>Boyang Wang, Baochun Li, and Hui Li</i>	
SPICE – Simple Privacy-Preserving Identity-Management for Cloud Environment	526
<i>Sherman S.M. Chow, Yi-Jun He, Lucas C.K. Hui, and Siu Ming Yiu</i>	

Security and Privacy in Smart Grids

A Practical Smart Metering System Supporting Privacy Preserving Billing and Load Monitoring	544
<i>Hsiao-Ying Lin, Wen-Guey Tzeng, Shiuan-Tzuo Shen, and Bao-Shuh P. Lin</i>	
Private Computation of Spatial and Temporal Power Consumption with Smart Meters	561
<i>Zekeriya Erkin and Gene Tsudik</i>	
Author Index	579