

Table of Contents

Digital Signatures

Forward Secure Ring Signature without Random Oracles.....	1
<i>Joseph K. Liu, Tsz Hon Yuen, and Jianying Zhou</i>	
Ring Signature Schemes from Lattice Basis Delegation.....	15
<i>Jin Wang and Bo Sun</i>	

Public Key Encryption

Computational Soundness about Formal Encryption in the Presence of Secret Shares and Key Cycles	29
<i>Xinfeng Lei, Rui Xue, and Ting Yu</i>	
A Variant of Boyen-Waters Anonymous IBE Scheme	42
<i>Song Luo, Qingni Shen, Yongming Jin, Yu Chen, Zhong Chen, and Sihang Qing</i>	
Non-interactive Opening for Ciphertexts Encrypted by Shared Keys	57
<i>Jiageng Chen, Keita Emura, and Atsuko Miyaji</i>	

Cryptographic Protocols

Lightweight RFID Mutual Authentication Protocol against Feasible Problems	69
<i>Yongming Jin, Huiping Sun, Wei Xin, Song Luo, and Zhong Chen</i>	
A Note on a Privacy-Preserving Distance-Bounding Protocol	78
<i>Jean-Philippe Aumasson, Aikaterini Mitrokotsa, and Pedro Peris-Lopez</i>	
Delegable Provable Data Possession for Remote Data in the Clouds	93
<i>Shiuan-Tzuo Shen and Wen-Guey Tzeng</i>	
Unconditionally Secure Oblivious Transfer Based on Channel Delays ...	112
<i>Kai-Yuen Cheong and Atsuko Miyaji</i>	

Applied Cryptography

Preserving Security and Privacy in Large-Scale VANETs	121
<i>Bo Qin, Qianhong Wu, Josep Domingo-Ferrer, and Lei Zhang</i>	

A Probabilistic Secret Sharing Scheme for a Compartmented Access Structure	136
<i>Yuyin Yu and Mingsheng Wang</i>	
Ideal Secret Sharing Schemes with Share Selectability	143
<i>Keita Emura, Atsuko Miyaji, Akito Nomura, Mohammad Shahriar Rahman, and Masakazu Soshi</i>	

Multimedia Security

A Novel Pyramidal Dual-Tree Directional Filter Bank Domain Color Image Watermarking Algorithm	158
<i>Panpan Niu, Xiangyang Wang, and Mingyu Lu</i>	
Detection for Multiplicative Watermarking in DCT Domain by Cauchy Model	173
<i>Xiang Yin, Shuoling Peng, and Xinshan Zhu</i>	

Algorithms and Evaluation

Extension of Barreto-Voloch Root Extraction Method	184
<i>Zhengjun Cao and Xiao Fan</i>	
Two Applications of an Incomplete Additive Character Sum to Estimating Nonlinearity of Boolean Functions	190
<i>Yusong Du and Fangguo Zhang</i>	
Evaluating Optimized Implementations of Stream Cipher ZUC Algorithm on FPGA	202
<i>Lei Wang, Jiwu Jing, Zongbin Liu, Lingchen Zhang, and Wuqiong Pan</i>	

Cryptanalysis

First Differential Attack on Full 32-Round GOST	216
<i>Nicolas T. Courtois and Michal Misztal</i>	
Collision Attack for the Hash Function Extended MD4	228
<i>Gaoli Wang</i>	
Linear Cryptanalysis of ARIA Block Cipher	242
<i>Zhiqiang Liu, Dawu Gu, Ya Liu, Juanru Li, and Wei Li</i>	
Latin Dances Revisited: New Analytic Results of Salsa20 and ChaCha	255
<i>Tsukasa Ishiguro, Shinsaku Kiyomoto, and Yutaka Miyake</i>	

Security Applications

Behavior Analysis-Based Dynamic Trust Measurement Model.....	267
<i>Dan Wang, Xiaodong Zhou, and Wenbing Zhao</i>	
Improvement and Analysis of VDP Method in Time/Memory Tradeoff Applications.....	282
<i>Wenhao Wang, Dongdai Lin, Zhenqi Li, and Tianze Wang</i>	
Analyzing the Performance of Dither Modulation in Presence of Composite Attacks	297
<i>Xinshan Zhu</i>	

Wireless Network Security

Applying Time-Bound Hierarchical Key Assignment in Wireless Sensor Networks	306
<i>Wen Tao Zhu, Robert H. Deng, Jianying Zhou, and Feng Bao</i>	
A Unified Security Framework for Multi-domain Wireless Mesh Networks	319
<i>Ze Wang, Maode Ma, Wenju Liu, and Xixi Wei</i>	

System Security

Ontology Model-Based Static Analysis of Security Vulnerabilities	330
<i>Lian Yu, Shi-Zhong Wu, Tao Guo, Guo-Wei Dong, Cheng-Cheng Wan, and Yin-Hang Jing</i>	
A Multi-compositional Enforcement on Information Flow Security.....	345
<i>Cong Sun, Ennan Zhai, Zhong Chen, and Jianfeng Ma</i>	
HyperCrop: A Hypervisor-Based Countermeasure for Return Oriented Programming.....	360
<i>Jun Jiang, Xiaoqi Jia, Dengguo Feng, Shengzhi Zhang, and Peng Liu</i>	
An Efficient Finger-Knuckle-Print Based Recognition System Fusing SIFT and SURF Matching Scores	374
<i>G.S. Badrinath, Aditya Nigam, and Phalguni Gupta</i>	

Network Security

Multivariate Correlation Analysis Technique Based on Euclidean Distance Map for Network Traffic Characterization	388
<i>Zhiyuan Tan, Aruna Jamdagni, Xiangjian He, Priyadarsi Nanda, and Ren Ping Liu</i>	

Situational Assessment of Intrusion Alerts: A Multi Attack Scenario Evaluation	399
<i>Hadi Shiravi, Ali Shiravi, and Ali A. Ghorbani</i>	
Minimising Anonymity Loss in Anonymity Networks under DoS Attacks	414
<i>Mu Yang and Vladimiro Sassone</i>	
Author Index	431