

Table of Contents

Invited Talks

The State of Hash Functions and the NIST SHA-3 Competition (Extended Abstract)	1
<i>Bart Preneel</i>	
Key Evolution Systems in Untrusted Update Environments	12
<i>Benoît Libert, Jean-Jacques Quisquater, and Moti Yung</i>	
Secure and Privacy-Preserving Information Brokering	22
<i>Peng Liu</i>	

Digital Signature and Signcryption Schemes

Provably Secure Convertible Nominative Signature Scheme	23
<i>Wei Zhao, Changlu Lin, and Dingfeng Ye</i>	
Cryptanalysis of Two Ring Signcryption Schemes	41
<i>Huaqun Wang and Hong Yu</i>	
Efficient Signcryption Key Encapsulation without Random Oracles	47
<i>Fagen Li, Masaaki Shirase, and Tsuyoshi Takagi</i>	

Privacy and Anonymity

Strong Anonymous Signatures	60
<i>Rui Zhang and Hideki Imai</i>	
Publicly Verifiable Privacy-Preserving Group Decryption	72
<i>Bo Qin, Qianhong Wu, Willy Susilo, and Yi Mu</i>	
Privacy for Private Key in Signatures	84
<i>Qianhong Wu, Bo Qin, Yi Mu, and Willy Susilo</i>	

Message Authentication Code and Hash Function

Security of Truncated MACs	96
<i>Peng Wang, Dengguo Feng, Changlu Lin, and Wenling Wu</i>	
Security Analysis of Multivariate Polynomials for Hashing	115
<i>Luk Bettale, Jean-Charles Faugère, and Ludovic Perret</i>	

Secure Protocols

SPVT-II: An Efficient Security Protocol Verifier Based on Logic Programming.....	125
<i>MengJun Li, Ti Zhou, and ZhouJun Li</i>	
Batch ZK Proof and Verification of OR Logic.....	141
<i>Kun Peng and Feng Bao</i>	

Symmetric Cryptography

Constructing Variable-Length PRPs and SPRPs from Fixed-Length PRPs.....	157
<i>Debra L. Cook, Moti Yung, and Angelos Keromytis</i>	
Impossible Differential Analysis of Reduced Round CLEFIA.....	181
<i>Wenyong Zhang and Jing Han</i>	
Reducible Polynomial over \mathbb{F}_2 Constructed by Trinomial σ -LFSR	192
<i>Guang Zeng, Yang Yang, Wenbao Han, and Shuqin Fan</i>	

Certificateless Cryptography

Chosen Ciphertext Secure Certificateless Threshold Encryption in the Standard Model	201
<i>Piqi Yang, Zhenfu Cao, and Xiaolei Dong</i>	
Further Observations on Certificateless Public Key Encryption.....	217
<i>Xu an Wang, Xinyi Huang, and Xiaoyuan Yang</i>	

Hardware Implementation and Side Channel Attack

Efficient Hardware Architecture of SHA-256 Algorithm for Trusted Mobile Computing	240
<i>Mooseop Kim, Jaecheol Ryou, and Sungik Jun</i>	
New Elliptic Curve Multi-scalar Multiplication Algorithm for a Pair of Integers to Resist SPA	253
<i>Duo Liu, Zhiyong Tan, and Yiqi Dai</i>	

Wireless Network Security

A Novel Marking Probability Distribution Using Probability Propagation in Hierarchical WSN	265
<i>Bo-Chao Cheng, Huan Chen, and Guo-Tan Liao</i>	

Key Predistribution Schemes Using Codes in Wireless Sensor Networks	275
<i>Sushmita Ruj and Bimal Roy</i>	
Efficient Multi-PKG ID-Based Signcryption for Ad Hoc Networks	289
<i>Fagen Li, Masaaki Shirase, and Tsuyoshi Takagi</i>	
Public Key and Identity Based Cryptography	
On the Computational Efficiency of XTR+	305
<i>Ningbo Mu, Yupu Hu, and Leyou Zhang</i>	
A Variant of Boneh-Gentry-Hamburg's Pairing-Free Identity Based Encryption Scheme	314
<i>Mahabir Prasad Jhanwar and Rana Barua</i>	
Inter-domain Identity-Based Proxy Re-encryption	332
<i>Qiang Tang, Pieter Hartel, and Willem Jonker</i>	
Access Control and Network Security	
Hardening Botnet by a Rational Botmaster	348
<i>Zonghua Zhang, Ruo Ando, and Youki Kadobayashi</i>	
Separation of Duty in Trust-Based Collaboration	370
<i>Lingli Deng, Yeping He, and Ziyao Xu</i>	
Trusted Computing and Applications	
An Integrity Assurance Mechanism for Run-Time Programs	389
<i>Ziyao Xu, Yeping He, and Lingli Deng</i>	
A Security and Performance Evaluation of Hash-Based RFID Protocols	406
<i>Tong-Lee Lim, Tieyan Li, and Yingjiu Li</i>	
Correction, Optimisation and Secure and Efficient Application of PBD Shuffling	425
<i>Kun Peng and Feng Bao</i>	
Author Index	439