

Table of Contents

Invited Talk

Tools over Bilinear Groups for Modular Design of Cryptographic Tasks.....	1
<i>Masayuki Abe</i>	

Signature Schemes

One-Move Convertible Nominative Signature in the Standard Model....	2
<i>Dennis Y.W. Liu and Duncan S. Wong</i>	
Efficient and Random Oracle-Free Conditionally Anonymous Ring Signature	21
<i>Shengke Zeng, Zhiguang Qin, Qing Lu, and Qinyi Li</i>	
ID Based Signcryption Scheme in Standard Model	35
<i>S. Sharmila Deva Selvi, S. Sree Vivek, Dhinakaran Vinayagamurthy, and C. Pandu Rangan</i>	
Combined Public-Key Schemes: The Case of ABE and ABS	53
<i>Cheng Chen, Jie Chen, Hoon Wei Lim, Zhenfeng Zhang, and Dengguo Feng</i>	

Foundations

Several Weak Bit-Commitments Using Seal-Once Tamper-Evident Devices	70
<i>Ioana Boureanu and Serge Vaudenay</i>	
Deterministic Random Oracles.....	88
<i>Margus Nüttsoo</i>	
On the (Non-)Equivalence of UC Security Notions	104
<i>Oana Ciobotaru</i>	

Leakage Resilience and Key Escrow

LR-UESDE: A Continual-Leakage Resilient Encryption with Unbounded Extensible Set Delegation	125
<i>Bo Yang and Mingwu Zhang</i>	

Anonymous Identity-Based Hash Proof System and Its Applications 143
Yu Chen, Zongyang Zhang, Dongdai Lin, and Zhenfu Cao

Efficient Escrow-Free Identity-Based Signature 161
Yunmei Zhang, Joseph K. Liu, Xinyi Huang, Man Ho Au, and Willy Susilo

Encryption Schemes

Perfect Keyword Privacy in PEKS Systems 175
Mototsugu Nishioka

Efficient Fully Secure Attribute-Based Encryption Schemes for General Access Structures 193
Tapas Pandit and Rana Barua

Symmetric Inner-Product Predicate Encryption Based on Three Groups 215
Masayuki Yoshino, Noboru Kunihiro, Ken Naganuma, and Hisayoshi Sato

Secure Keyword Search Using Bloom Filter with Specified Character Positions 235
Takanori Suga, Takashi Nishide, and Kouichi Sakurai

Short Papers

Fully Secure Doubly-Spatial Encryption under Simple Assumptions 253
Cheng Chen, Zhenfeng Zhang, and Dengguo Feng

Strongly Authenticated Key Exchange Protocol from Bilinear Groups without Random Oracles 264
Zheng Yang and Jörg Schwenk

Authenticated Key Exchange with Entities from Different Settings and Varied Groups 276
Yanfei Guo and Zhenfeng Zhang

On Capabilities of Hash Domain Extenders to Preserve Enhanced Security Properties 288
Mohammad Reza Reyhanitabar and Willy Susilo

Information Theoretical Security

Revisiting a Secret Sharing Approach to Network Codes	300
<i>Zhaohui Tang, Hoon Wei Lim, and Huaxiong Wang</i>	
Codes Based Tracing and Revoking Scheme with Constant Ciphertext	318
<i>Xingwen Zhao and Hui Li</i>	
Author Index	337