

Table of Contents

Invited Talks

A Brief History of Security Models for Confidentiality	1
<i>Alexander W. Dent</i>	
Symbolic Methods for Provable Security	2
<i>Bogdan Warinschi</i>	

Encryption

Efficient Non-interactive Universally Composable String-Commitment Schemes	3
<i>Ryo Nishimaki, Eiichiro Fujisaki, and Keisuke Tanaka</i>	
Spatial Encryption under Simpler Assumption	19
<i>Muxin Zhou and Zhenfu Cao</i>	
Chosen-Ciphertext Secure RSA-Type Cryptosystems	32
<i>Benoît Chevallier-Mames and Marc Joye</i>	
Anonymous Conditional Proxy Re-encryption without Random Oracle	47
<i>Liming Fang, Willy Susilo, and Jiandong Wang</i>	
Breaking and Fixing of an Identity Based Multi-signcryption Scheme ...	61
<i>S. Sharmila Deva Selvi, S. Sree Vivek, and C. Pandu Rangan</i>	

Digital Signatures

Identity-Based Verifiably Encrypted Signatures without Random Oracles	76
<i>Lei Zhang, Qianhong Wu, and Bo Qin</i>	
How to Prove Security of a Signature with a Tighter Security Reduction	90
<i>Fuchun Guo, Yi Mu, and Willy Susilo</i>	
Twin Signature Schemes, Revisited	104
<i>Sven Schäge</i>	
On the Insecurity of the Fiat-Shamir Signatures with Iterative Hash Functions	118
<i>Eiichiro Fujisaki, Ryo Nishimaki, and Keisuke Tanaka</i>	

Is the Notion of Divisible On-Line/Off-Line Signatures Stronger than On-Line/Off-Line Signatures?	129
<i>Man Ho Au, Willy Susilo, and Yi Mu</i>	
Anonymous Signatures Revisited	140
<i>Vishal Saraswat and Aaram Yun</i>	

Cryptographic Protocols

An eCK-Secure Authenticated Key Exchange Protocol without Random Oracles	154
<i>Daisuke Moriyama and Tatsuaki Okamoto</i>	
Password Authenticated Key Exchange Based on RSA in the Three-Party Settings	168
<i>E. Dongna, Qingfeng Cheng, and Chuanguai Ma</i>	
Comparing <i>SessionStateReveal</i> and <i>EphemeralKeyReveal</i> for Diffie-Hellman Protocols	183
<i>Berkant Ustaoglu</i>	
Zero-Knowledge Protocols for NTRU: Application to Identification and Proof of Plaintext Knowledge	198
<i>Keita Xagawa and Keisuke Tanaka</i>	
Server-Controlled Identity-Based Authenticated Key Exchange	214
<i>Hua Guo, Yi Mu, Xiyong Zhang, and Zhoujun Li</i>	

Reductions and Privacy

Oracle Separation in the Non-uniform Model	230
<i>Ahto Buldas, Sven Laur, and Margus Niiitsoo</i>	
GUC-Secure Set-Intersection Computation	245
<i>Yuan Tian and Hao Zhang</i>	
Self-enforcing Private Inference Control	260
<i>Yanjiang Yang, Yingjiu Li, Jian Weng, Jianying Zhou, and Feng Bao</i>	
Author Index	275