

# Table of Contents

## Invited Talk

On Modeling Terrorist Frauds: Addressing Collusion in Distance Bounding Protocols .....	1
<i>Serge Vaudenay</i>	

## Key Exchange Protocols

Authenticated Key Exchange Protocols Based on Factoring Assumption .....	21
<i>Hai Huang</i>	
Efficient, Pairing-Free, Authenticated Identity Based Key Agreement in a Single Round .....	38
<i>S. Sree Vivek, S. Sharmila Deva Selvi, Layamrudhaa Renganathan Venkatesan, and C. Pandu Rangan</i>	
CIL Security Proof for a Password-Based Key Exchange .....	59
<i>Cristian Ene, Cl��mentine Gritti, and Yassine Lakhnech</i>	

## Security Models

Non Observability in the Random Oracle Model .....	86
<i>Prabhanjan Ananth and Raghav Bhaskar</i>	
Indistinguishability against Chosen Ciphertext Verification Attack Revisited: The Complete Picture .....	104
<i>Angsuman Das, Sabyasachi Dutta, and Avishek Adhikari</i>	
Input-Aware Equivocable Commitments and UC-secure Commitments with Atomic Exchanges .....	121
<i>Ioana Boureanu and Serge Vaudenay</i>	
Towards Anonymous Ciphertext Indistinguishability with Identity Leakage .....	139
<i>Tsz Hon Yuen, Cong Zhang, Sherman S.M. Chow, and Joseph K. Liu</i>	

## Signature and Signcryption Schemes

$k$ -Time Proxy Signature: Formal Definition and Efficient Construction .....	154
<i>Weiwei Liu, Guomin Yang, Yi Mu, and Jiannan Wei</i>	

Anonymous Signcryption against Linear Related-Key Attacks . . . . .	165
<i>Hui Cui, Yi Mu, and Man Ho Au</i>	
<b>Authenticated Encryption</b>	
Improved Authenticity Bound of EAX, and Refinements . . . . .	184
<i>Kazuhiko Minematsu, Stefan Lucks, and Tetsu Iwata</i>	
The Security of the OCB Mode of Operation without the SPRP Assumption . . . . .	202
<i>Kazumaro Aoki and Kan Yasuda</i>	
A Short Universal Hash Function from Bit Rotation, and Applications to Blockcipher Modes . . . . .	221
<i>Kazuhiko Minematsu</i>	
<b>Theory</b>	
How to Remove the Exponent GCD in HK09 . . . . .	239
<i>Xianhui Lu, Bao Li, and Yamin Liu</i>	
Translation-Randomizable Distributions via Random Walks . . . . .	249
<i>Nirattaya Khamsemanan and William E. Skeith III</i>	
<b>Public Key Encryption</b>	
RKA Secure PKE Based on the DDH and HR Assumptions . . . . .	271
<i>Dingding Jia, Xianhui Lu, Bao Li, and Qixiang Mei</i>	
Computationally Efficient Dual-Policy Attribute Based Encryption with Short Ciphertext . . . . .	288
<i>Y. Sreenivasa Rao and Ratna Dutta</i>	
Factoring-Based Proxy Re-Encryption Schemes . . . . .	309
<i>Toshiyuki Ishiki, Manh Ha Nguyen, and Keisuke Tanaka</i>	
Towards a Secure Certificateless Proxy Re-Encryption Scheme . . . . .	330
<i>Hui Guo, Zhenfeng Zhang, Jiang Zhang, and Cheng Chen</i>	
<b>Author Index</b> . . . . .	347