

Contents – Part I

CCA Security

Trading Plaintext-Awareness for Simulatability to Achieve Chosen Ciphertext Security	3
<i>Takahiro Matsuda and Goichiro Hanaoka</i>	
Chosen-Ciphertext Security from Subset Sum	35
<i>Sebastian Faust, Daniel Masny, and Daniele Venturi</i>	
On the Hardness of Proving CCA-Security of Signed ElGamal	47
<i>David Bernhard, Marc Fischlin, and Bogdan Warinschi</i>	
CCA-Secure Keyed-Fully Homomorphic Encryption	70
<i>Junzuo Lai, Robert H. Deng, Changshe Ma, Kouichi Sakurai, and Jian Weng</i>	
On the Key Dependent Message Security of the Fujisaki-Okamoto Constructions	99
<i>Fuyuki Kitagawa, Takahiro Matsuda, Goichiro Hanaoka, and Keisuke Tanaka</i>	

Functional Encryption

Extended Nested Dual System Groups, Revisited	133
<i>Junqing Gong, Jie Chen, Xiaolei Dong, Zhenfu Cao, and Shaohua Tang</i>	
Functional Encryption for Inner Product with Full Function Privacy	164
<i>Pratish Datta, Ratna Dutta, and Sourav Mukhopadhyay</i>	
Deniable Functional Encryption	196
<i>Angelo De Caro, Vincenzo Iovino, and Adam O'Neill</i>	

Identity-Based Encryption

Identity-Based Cryptosystems and Quadratic Residuosity	225
<i>Marc Joye</i>	
Identity-Based Hierarchical Key-Insulated Encryption Without Random Oracles	255
<i>Yohei Watanabe and Junji Shikata</i>	

Signatures

Attribute-Based Signatures for Circuits from Bilinear Map	283
<i>Yusuke Sakai, Nuttapong Attrapadung, and Goichiro Hanaoka</i>	
Efficient Unlinkable Sanitizable Signatures from Signatures with Re-randomizable Keys	301
<i>Nils Fleischhacker, Johannes Krupp, Giulio Malavolta, Jonas Schneider, Dominique Schröder, and Mark Simkin</i>	
Fault-Tolerant Aggregate Signatures	331
<i>Gunnar Hartung, Björn Kaidel, Alexander Koch, Jessica Koch, and Andy Rupp</i>	
Delegatable Functional Signatures	357
<i>Michael Backes, Sebastian Meiser, and Dominique Schröder</i>	
Mitigating Multi-target Attacks in Hash-Based Signatures	387
<i>Andreas Hülsing, Joost Rijneveld, and Fang Song</i>	
Nearly Optimal Verifiable Data Streaming	417
<i>Johannes Krupp, Dominique Schröder, Mark Simkin, Dario Fiore, Giuseppe Ateniese, and Stefan Nuernberger</i>	
ARMed SPHINCS: Computing a 41 KB Signature in 16 KB of RAM	446
<i>Andreas Hülsing, Joost Rijneveld, and Peter Schwabe</i>	
Author Index	471