

Table of Contents

Homomorphic Encryption

Packed Ciphertexts in LWE-Based Homomorphic Encryption	1
<i>Zvika Brakerski, Craig Gentry, and Shai Halevi</i>	
Feasibility and Infeasibility of Adaptively Secure Fully Homomorphic Encryption	14
<i>Jonathan Katz, Aishwarya Thiruvengadam, and Hong-Sheng Zhou</i>	
Chosen Ciphertext Secure Keyed-Homomorphic Public-Key Encryption	32
<i>Keita Emura, Goichiro Hanaoka, Go Ohtake, Takahiro Matsuda, and Shota Yamada</i>	

Invited Talk (1)

Functional Encryption: Origins and Recent Developments	51
<i>Brent Waters</i>	

Primitives

Vector Commitments and Their Applications	55
<i>Dario Catalano and Dario Fiore</i>	
Efficient, Adaptively Secure, and Composable Oblivious Transfer with a Single, Global CRS	73
<i>Seung Geol Choi, Jonathan Katz, Hoeteck Wee, and Hong-Sheng Zhou</i>	
Cryptography Using Captcha Puzzles	89
<i>Abishek Kumarasubramanian, Rafail Ostrovsky, Omkant Pandey, and Akshay Wadia</i>	
Improved Zero-Knowledge Proofs of Knowledge for the ISIS Problem, and Applications	107
<i>San Ling, Khoa Nguyen, Damien Stehlé, and Huaxiong Wang</i>	

Functional Encryption/Signatures

Decentralized Attribute-Based Signatures	125
<i>Tatsuaki Okamoto and Katsuyuki Takashima</i>	

On the Semantic Security of Functional Encryption Schemes	143
<i>Manuel Barbosa and Pooya Farshim</i>	
Attribute-Based Encryption with Fast Decryption	162
<i>Susan Hohenberger and Brent Waters</i>	

On RSA

Recovering RSA Secret Keys from Noisy Key Bits with Erasures and Errors	180
<i>Noboru Kunihiro, Naoyuki Shinohara, and Tetsuya Izu</i>	
Combined Attack on CRT-RSA: Why Public Verification Must Not Be Public?	198
<i>Guillaume Barbu, Alberto Battistello, Guillaume Dabosville, Christophe Giraud, Guénaél Renault, Soline Renner, and Rina Zeitoun</i>	

IBE and IPE

Revocable Identity-Based Encryption Revisited: Security Model and Construction	216
<i>Jae Hong Seo and Keita Emura</i>	
Improved (Hierarchical) Inner-Product Encryption from Lattices	235
<i>Keita Xagawa</i>	

Invited Talk (2)

Techniques for Efficient Secure Computation Based on Yao's Protocol	253
<i>Yehuda Lindell</i>	

Key Exchange

Non-Interactive Key Exchange	254
<i>Eduarda S.V. Freire, Dennis Hofheinz, Eike Kiltz, and Kenneth G. Paterson</i>	
Efficient UC-Secure Authenticated Key-Exchange for Algebraic Languages	272
<i>Fabrice Ben Hamouda, Olivier Blazy, Céline Chevalier, David Pointcheval, and Damien Vergnaud</i>	

Signature Schemes I

Tighter Reductions for Forward-Secure Signature Schemes	292
<i>Michel Abdalla, Fabrice Ben Hamouda, and David Pointcheval</i>	
Tagged One-Time Signatures: Tight Security and Optimal Tag Size	312
<i>Masayuki Abe, Bernardo David, Markulf Kohlweiss, Ryo Nishimaki, and Miyako Ohkubo</i>	

Encryption

Key Encapsulation Mechanisms from Extractable Hash Proof Systems, Revisited	332
<i>Takahiro Matsuda and Goichiro Hanaoka</i>	
Robust Encryption, Revisited	352
<i>Pooya Farshim, Benoît Libert, Kenneth G. Paterson, and Elizabeth A. Quaglia</i>	
Sender-Equivocable Encryption Schemes Secure against Chosen- Ciphertext Attacks Revisited	369
<i>Zhengan Huang, Shengli Liu, and Baodong Qin</i>	

Signature Schemes II

Efficient Completely Context-Hiding Quotable and Linearly Homomorphic Signatures	386
<i>Nuttapong Attrapadung, Benoît Libert, and Thomas Peters</i>	
Verifiably Encrypted Signatures with Short Keys Based on the Decisional Linear Problem and Obfuscation for Encrypted VES	405
<i>Ryo Nishimaki and Keita Xagawa</i>	
Sequential Aggregate Signatures with Short Public Keys: Design, Analysis and Implementation Studies	423
<i>Kwangsue Lee, Dong Hoon Lee, and Moti Yung</i>	
New Constructions and Applications of Trapdoor DDH Groups	443
<i>Yannick Seurin</i>	

Protocols

Rate-Limited Secure Function Evaluation: Definitions and Constructions	461
<i>Özgür Dagdelen, Payman Mohassel, and Daniele Venturi</i>	

Verifiable Elections That Scale for Free 479
 Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, and Sarah Meiklejohn

On the Connection between Leakage Tolerance and Adaptive Security 497
 Jesper Buus Nielsen, Daniele Venturi, and Angela Zottarel

Author Index 517