

Table of Contents

Chosen Ciphertext Security

Simple Chosen-Ciphertext Security from Low-Noise LPN	1
<i>Eike Kiltz, Daniel Masny, and Krzysztof Pietrzak</i>	
Leakage-Flexible CCA-secure Public-Key Encryption: Simple Construction and Free of Pairing	19
<i>Baodong Qin and Shengli Liu</i>	
A Black-Box Construction of a CCA2 Encryption Scheme from a Plaintext Aware (sPA1) Encryption Scheme	37
<i>Dana Dachman-Soled</i>	
Chosen Ciphertext Security via UCE	56
<i>Takahiro Matsuda and Goichiro Hanaoka</i>	

Re-encryption

Proxy Re-encryption from Lattices	77
<i>Elena Kirshanova</i>	
Re-encryption, Functional Re-encryption, and Multi-hop Re-encryption: A Framework for Achieving Obfuscation-Based Security and Instantiations from Lattices	95
<i>Nishanth Chandran, Melissa Chase, Feng-Hao Liu, Ryo Nishimaki, and Keita Xagawa</i>	

Verifiable Outsourcing

Verifiable Set Operations over Outsourced Databases	113
<i>Ran Canetti, Omer Paneth, Dimitrios Papadopoulos, and Nikos Tsiandopoulos</i>	
Verifiable Oblivious Storage	131
<i>Daniel Apon, Jonathan Katz, Elaine Shi, and Aishwarya Thiruvengadam</i>	
Achieving Privacy in Verifiable Computation with Multiple Servers – Without FHE and without Pre-processing	149
<i>Prabhanjan Ananth, Nishanth Chandran, Vipul Goyal, Bhavana Kanukurthi, and Rafail Ostrovsky</i>	

Efficient Delegation of Zero-Knowledge Proofs of Knowledge in a Pairing-Friendly Setting	167
<i>Sébastien Canard, David Pointcheval, and Olivier Sanders</i>	

Cryptanalysis I

Rounding and Chaining LLL: Finding Faster Small Roots of Univariate Polynomial Congruences	185
--	-----

Jingguo Bi, Jean-Sébastien Coron, Jean-Charles Faugère, Phong Q. Nguyen, Guénaël Renault, and Rina Zeitoun

Elliptic and Hyperelliptic Curves: A Practical Security Analysis	203
<i>Joppe W. Bos, Craig Costello, and Andrea Miele</i>	

Discrete Logarithm in $GF(2^{809})$ with FFS	221
--	-----

Razvan Barbulescu, Cyril Bouvier, Jérémie Detrey, Pierrick Gaudry, Hamza Jeljeli, Emmanuel Thomé, Marion Videau, and Paul Zimmermann

Identity- and Attribute-Based Encryption

Identity-Based Lossy Trapdoor Functions: New Definitions, Hierarchical Extensions, and Implications	239
---	-----

Alex Escala, Javier Herranz, Benoît Libert, and Carla Ràfols

Bounded-Collusion Identity-Based Encryption from Semantically-Secure Public-Key Encryption: Generic Constructions with Short Ciphertexts	257
--	-----

Stefano Tessaro and David A. Wilson

A Framework and Compact Constructions for Non-monotonic Attribute-Based Encryption	275
--	-----

Shota Yamada, Nuttapong Attrapadung, Goichiro Hanaoka, and Noboru Kunihiro

Online/Offline Attribute-Based Encryption	293
---	-----

Susan Hohenberger and Brent Waters

Enhanced Encryption

Scale-Invariant Fully Homomorphic Encryption over the Integers	311
--	-----

Jean-Sébastien Coron, Tancrède Lepoint, and Mehdi Tibouchi

Enhanced Chosen-Ciphertext Security and Applications	329
--	-----

Dana Dachman-Soled, Georg Fuchsbauer, Payman Mohassel, and Adam O'Neill

Signature Schemes

Lattice-Based Group Signature Scheme with Verifier-Local Revocation	345
<i>Adeline Langlois, San Ling, Khoa Nguyen, and Huaxiong Wang</i>	

Leakage-Resilient Signatures with Graceful Degradation	362
<i>Jesper Buus Nielsen, Daniele Venturi, and Angela Zottarel</i>	

On the Lossiness of the Rabin Trapdoor Function	380
<i>Yannick Seurin</i>	

Cryptanalysis II

Solving Random Subset Sum Problem by l_p -norm SVP Oracle	399
<i>Gengran Hu, Yanbin Pan, and Feng Zhang</i>	

Parallel Gauss Sieve Algorithm: Solving the SVP Challenge over a 128-Dimensional Ideal Lattice	411
<i>Tsukasa Ishiguro, Shinsaku Kiyomoto, Yutaka Miyake, and Tsuyoshi Takagi</i>	

Lazy Modulus Switching for the BKW Algorithm on LWE	429
<i>Martin R. Albrecht, Jean-Charles Faugère, Robert Fitzpatrick, and Ludovic Perret</i>	

Practical Cryptanalysis of a Public-Key Encryption Scheme Based on New Multivariate Quadratic Assumptions	446
<i>Martin R. Albrecht, Jean-Charles Faugère, Robert Fitzpatrick, Ludovic Perret, Yosuke Todo, and Keita Xagawa</i>	

Related-Key Security

Related Randomness Attacks for Public Key Encryption	465
<i>Kenneth G. Paterson, Jacob C.N. Schuldt, and Dale L. Sibborn</i>	

Encryption Schemes Secure under Related-Key and Key-Dependent Message Attacks	483
<i>Florian Böhl, Gareth T. Davies, and Dennis Hofheinz</i>	

Functional Authentication

Functional Signatures and Pseudorandom Functions	501
<i>Elette Boyle, Shafi Goldwasser, and Ioana Ivan</i>	

Policy-Based Signatures	520
<i>Mihir Bellare and Georg Fuchsbauer</i>	

Generalizing Homomorphic MACs for Arithmetic Circuits	538
<i>Dario Catalano, Dario Fiore, Rosario Gennaro, and Luca Nizzardo</i>	

Quantum Impossibility

General Impossibility of Group Homomorphic Encryption in the Quantum World	556
<i>Frederik Armknecht, Tommaso Gagliardoni, Stefan Katzenbeisser, and Andreas Peter</i>	

Privacy

On Minimal Assumptions for Sender-Deniable Public Key Encryption	574
<i>Dana Dachman-Soled</i>	
Traceable Group Encryption	592
<i>Benoît Libert, Moti Yung, Marc Joye, and Thomas Peters</i>	
Practical Covert Authentication	611
<i>Stanislaw Jarecki</i>	

Protocols

Fine-Tuning Groth-Sahai Proofs	630
<i>Alex Escala and Jens Groth</i>	
Cross-Domain Secure Computation	650
<i>Chongwon Cho, Sanjam Garg, and Rafail Ostrovsky</i>	
On the Security of the Pre-shared Key Ciphersuites of TLS	669
<i>Yong Li, Sven Schäge, Zheng Yang, Florian Kohlar, and Jörg Schwenk</i>	

Author Index	685
------------------------	-----