

Contents

Order Revealing Encryption

Revealing Encryption for Partial Ordering	3
<i>Helene Haagh, Yue Ji, Chenxing Li, Claudio Orlandi, and Yifan Song</i>	

Homomorphic Encryption and Secure Computation

Dynamic Multi Target Homomorphic Attribute-Based Encryption	25
<i>Ryo Hiromasa and Yutaka Kawai</i>	
Practical Homomorphic Encryption Over the Integers for Secure Computation in the Cloud	44
<i>James Dyer, Martin Dyer, and Jie Xu</i>	
When It's All Just Too Much: Outsourcing MPC-Preprocessing	77
<i>Peter Scholl, Nigel P. Smart, and Tim Wood</i>	

Coding Theory

On the Probability of Incorrect Decoding for Linear Codes	103
<i>Marco Frego</i>	
Improvement on Minimum Distance of Symbol-Pair Codes	116
<i>Han Zhang</i>	

Bilinear and Multilinear Maps

Bilinear Cryptography Using Groups of Nilpotency Class 2	127
<i>Ayan Mahalanobis and Pralhad Shinde</i>	
Notes on GGH13 Without the Presence of Ideals	135
<i>Martin R. Albrecht, Alex Davidson, and Enrique Larraia</i>	

Signatures

Attribute-Based Signatures with User-Controlled Linkability Without Random Oracles	161
<i>Ali El Kaafarani and Essam Ghadafi</i>	

How Low Can You Go? Short Structure-Preserving Signatures for Diffie-Hellman Vectors.	185
<i>Essam Ghadafi</i>	

Post-Quantum Cryptography

CAKE: <u>C</u> ode-Based <u>A</u> lgorithm for <u>K</u> ey <u>E</u> ncapsulation.	207
<i>Paulo S. L. M. Barreto, Shay Gueron, Tim Güneysu, Rafael Misoczki, Edoardo Persichetti, Nicolas Sendrier, and Jean-Pierre Tillich</i>	

A Practical Implementation of Identity-Based Encryption Over NTRU Lattices	227
<i>Sarah McCarthy, Neil Smyth, and Elizabeth O'Sullivan</i>	

A Note on the Implementation of the Number Theoretic Transform.	247
<i>Michael Scott</i>	

Homomorphic Signatures

A Linearly Homomorphic Signature Scheme from Weaker Assumptions	261
<i>Lucas Schabhüser, Johannes Buchmann, and Patrick Struck</i>	

Subset Signatures with Controlled Context-Hiding.	280
<i>Essam Ghadafi</i>	

Symmetric Cryptography

Orthogonal MDS Diffusion Matrices over Galois Rings.	307
<i>Chik How Tan and Theo Fanuela Prabowo</i>	

Cryptanalysis

MILP-Based Cube Attack on the Reduced-Round WG-5 Lightweight Stream Cipher.	333
<i>Raghvendra Rohit, Riham AlTawy, and Guang Gong</i>	

Lattice Attacks on Pairing-Based Signatures	352
<i>Thierry Mefenza and Damien Vergnaud</i>	

Lattice Reductions over Euclidean Rings with Applications to Cryptanalysis	371
<i>Taechan Kim and Changmin Lee</i>	

Author Index	393
-------------------------------	-----

Cryptography and Coding

16th IMA International Conference, IMACC 2017, Oxford,

UK, December 12-14, 2017, Proceedings

O'Neill, M. (Ed.)

2017, X, 393 p. 23 illus., Softcover

ISBN: 978-3-319-71044-0