

Contents

Public-Key Cryptography

Blending FHE-NTRU Keys – The Excalibur Property	3
<i>Louis Goubin and Francisco José Vial Prado</i>	
Approximate-Deterministic Public Key Encryption from Hard Learning Problems	25
<i>Yamin Liu, Xianhui Lu, Bao Li, Wenpan Jing, and Fuyang Fang</i>	
Adaptively Secure Strong Designated Signature	43
<i>Neetu Sharma, Rajeev Anand Sahu, Vishal Saraswat, and Birendra Kumar Sharma</i>	
The Shortest Signatures Ever	61
<i>Mohamed Saied Emam Mohamed and Albrecht Petzoldt</i>	

Cryptographic Protocols

CRT-Based Outsourcing Algorithms for Modular Exponentiations.	81
<i>Lakshmi Kuppusamy and Jothi Rangasamy</i>	
Verifiable Computation for Randomized Algorithm.	99
<i>Muhua Liu, Ying Wu, and Rui Xue</i>	
UC-secure and Contributory Password-Authenticated Group Key Exchange . . .	119
<i>Lin Zhang and Zhenfeng Zhang</i>	

Side-Channel Attacks

Score-Based vs. Probability-Based Enumeration – A Cautionary Note	137
<i>Marios O. Choudary, Romain Poussier, and François-Xavier Standaert</i>	
Analyzing the Shuffling Side-Channel Countermeasure for Lattice-Based Signatures	153
<i>Peter Pessl</i>	

Implementation of Cryptographic Schemes

Atomic-AES: A Compact Implementation of the AES Encryption/Decryption Core	173
<i>Subhadeep Banik, Andrey Bogdanov, and Francesco Regazzoni</i>	

Fast Hardware Architectures for Supersingular Isogeny Diffie-Hellman Key Exchange on FPGA	191
<i>Brian Koziel, Reza Azarderakhsh, and Mehran Mozaffari-Kermani</i>	

AEZ: Anything-But EaZy in Hardware	207
<i>Ekawat Homsirikamol and Kris Gaj</i>	

Functional Encryption

Private Functional Encryption: Indistinguishability-Based Definitions and Constructions from Obfuscation	227
<i>Afonso Arriaga, Manuel Barbosa, and Pooya Farshim</i>	

Revocable Decentralized Multi-Authority Functional Encryption	248
<i>Hikaru Tsuchida, Takashi Nishide, Eiji Okamoto, and Kwangjo Kim</i>	

Symmetric-Key Cryptanalysis

On Linear Hulls and Trails.	269
<i>Tomer Ashur and Vincent Rijmen</i>	

Related-Key Cryptanalysis of Midori.	287
<i>David G�rault and Pascal Lafourcade</i>	

Some Proofs of Joint Distributions of Keystream Biases in RC4	305
<i>Sonu Jha, Subhadeep Banik, Takanori Isobe, and Toshihiro Ohigashi</i>	

Practical Low Data-Complexity Subspace-Trail Cryptanalysis of Round-Reduced PRINCE	322
<i>Lorenzo Grassi and Christian Rechberger</i>	

Foundations

On Negation Complexity of Injections, Surjections and Collision-Resistance in Cryptography	345
<i>Douglas Miller, Adam Scrivener, Jesse Stern, and Muthuramakrishnan Venkitasubramaniam</i>	

Implicit Quadratic Property of Differentially 4-Uniform Permutations	364
<i>Theo Fanuela Prabowo and Chik How Tan</i>	

Secret Sharing for mNP: Completeness Results.	380
<i>Mahabir Prasad Jhanwar and Kannan Srinathan</i>	

New Cryptographic Constructions

Receiver Selective Opening Security from Indistinguishability Obfuscation. . .	393
<i>Dingding Jia, Xianhui Lu, and Bao Li</i>	

Format Preserving Sets: On Diffusion Layers of Format Preserving Encryption Schemes	411
<i>Kishan Chand Gupta, Sumit Kumar Pandey, and Indranil Ghosh Ray</i>	
Author Index	429

Progress in Cryptology – INDOCRYPT 2016
17th International Conference on Cryptology in India,
Kolkata, India, December 11–14, 2016, Proceedings
Dunkelman, O.; Sanadhya, S. (Eds.)
2016, XVII, 429 p. 66 illus., Softcover
ISBN: 978-3-319-49889-8