Contents

Public-Key Cryptography

Blending FHE-NTRU Keys – The Excalibur Property .......................... 3
Louis Goubin and Francisco José Vial Prado

Approximate-Deterministic Public Key Encryption from Hard Learning Problems .................................................. 25
Yamin Liu, Xianhui Lu, Bao Li, Wenpan Jing, and Fuyang Fang

Adaptively Secure Strong Designated Signature ............................. 43
Neetu Sharma, Rajeev Anand Sahu, Vishal Saraswat, and Birendra Kumar Sharma

The Shortest Signatures Ever ...................................................... 61
Mohamed Saled Emam Mohamed and Albrecht Petzoldt

Cryptographic Protocols

CRT-Based Outsourcing Algorithms for Modular Exponentiations ...... 81
Lakshmi Kuppusamy and Jothi Rangasamy

Verifiable Computation for Randomized Algorithm ........................ 99
Muhua Liu, Ying Wu, and Rui Xue

UC-secure and Contributory Password-Authenticated Group Key Exchange ... 119
Lin Zhang and Zhenfeng Zhang

Side-Channel Attacks

Score-Based vs. Probability-Based Enumeration – A Cautionary Note ....... 137
Marios O. Choudary, Romain Poussier, and François-Xavier Standaert

Analyzing the Shuffling Side-Channel Countermeasure for Lattice-Based Signatures ........................................... 153
Peter Pessl

Implementation of Cryptographic Schemes

Atomic-AES: A Compact Implementation of the AES Encryption/Decryption Core ......................................................... 173
Subhadeep Banik, Andrey Bogdanov, and Francesco Regazzoni
Fast Hardware Architectures for Supersingular Isogeny Diffie-Hellman Key Exchange on FPGA ................................................. 191
   Brian Koziel, Reza Azarderakhsh, and Mehran Mozaffari-Kermani

AEZ: Anything-But EaZy in Hardware ........................................... 207
   Ekawat Homsirikamol and Kris Gaj

Functional Encryption

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

Revocable Decentralized Multi-Authority Functional Encryption ............ 248
   Hikaru Tsuchida, Takashi Nishide, Eiji Okamoto, and Kwangjo Kim

Symmetric-Key Cryptanalysis

On Linear Hulls and Trails .............................................................. 269
   Tomer Ashur and Vincent Rijmen

Related-Key Cryptanalysis of Midori .............................................. 287
   David Gérault and Pascal Lafourcade

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

Practical Low Data-Complexity Subspace-Trail Cryptanalysis of Round-Reduced PRINCE .................................................. 322
   Lorenzo Grassi and Christian Rechberger

Foundations

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

Implicit Quadratic Property of Differentially 4-Uniform Permutations . . . 364
   Theo Fanuela Prabowo and Chik How Tan

Secret Sharing for mNP: Completeness Results .................................. 380
   Mahabir Prasad Jhanwar and Kannan Srinathan

New Cryptographic Constructions

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