

Contents

Public Key Encryption

Compact Attribute-Based Encryption and Signcryption for General Circuits from Multilinear Maps	3
<i>Pratish Datta, Ratna Dutta, and Sourav Mukhopadhyay</i>	
Dynamic Key-Aggregate Cryptosystem on Elliptic Curves for Online Data Sharing	25
<i>Sikhar Patranabis, Yash Shrivastava, and Debdeep Mukhopadhyay</i>	
Lite-Rainbow: Lightweight Signature Schemes Based on Multivariate Quadratic Equations and Their Secure Implementations	45
<i>Kyung-Ah Shim, Cheol-Min Park, and Yoo-Jin Baek</i>	
Lossy Projective Hashing and Its Applications	64
<i>Haiyang Xue, Yamin Liu, Xianhui Lu, and Bao Li</i>	
(De-)Constructing TLS 1.3	85
<i>Markulf Kohlweiss, Ueli Maurer, Cristina Onete, Björn Tackmann, and Daniele Venturi</i>	

Cryptanalysis

Cryptanalysis of Variants of RSA with Multiple Small Secret Exponents	105
<i>Liqiang Peng, Lei Hu, Yao Lu, Santanu Sarkar, Jun Xu, and Zhangjie Huang</i>	
Some Results on Sprout	124
<i>Subhadeep Banik</i>	
Linear Cryptanalysis of Reduced-Round SIMECK Variants	140
<i>Nasour Bagheri</i>	
Improved Linear Cryptanalysis of Reduced-Round SIMON-32 and SIMON-48	153
<i>Mohamed Ahmed Abdelraheem, Javad Alizadeh, Hoda A. Alkhzaimi, Mohammad Reza Aref, Nasour Bagheri, and Praveen Gauravaram</i>	
Some Results Using the Matrix Methods on Impossible, Integral and Zero-Correlation Distinguishers for Feistel-Like Ciphers	180
<i>Thierry P. Berger and Marine Minier</i>	

Improved Meet-in-the-Middle Attacks on 7 and 8-Round ARIA-192 and ARIA-256	198
<i>Akshima, Donghoon Chang, Mohona Ghosh, Aarushi Goel, and Somitra Kumar Sanadhya</i>	
Structural Evaluation for Generalized Feistel Structures and Applications to LBlock and TWINE	218
<i>Huiling Zhang and Wenling Wu</i>	
Side Channel Attacks	
Cryptanalysis of Two Fault Countermeasure Schemes	241
<i>Subhadeep Banik and Andrey Bogdanov</i>	
Differential Fault Analysis of SHA-3.	253
<i>Nasour Bagheri, Navid Ghaedi, and Somitra Kumar Sanadhya</i>	
A Key to Success: Success Exponents for Side-Channel Distinguishers	270
<i>Sylvain Guilley, Annelie Heuser, and Olivier Rioul</i>	
Information Theoretic Cryptography	
Non-malleable Extractors with Shorter Seeds and Their Applications.	293
<i>Yanqing Yao and Zhoujun Li</i>	
Efficiently Simulating High Min-entropy Sources in the Presence of Side Information	312
<i>Maciej Skórski</i>	
Lightweight Cryptography	
BitCryptor: Bit-Serialized Flexible Crypto Engine for Lightweight Applications	329
<i>Ege Gulcan, Aydin Aysu, and Patrick Schaumont</i>	
Low-Resource and Fast Binary Edwards Curves Cryptography	347
<i>Brian Koziel, Reza Azarderakhsh, and Mehran Mozaffari-Kermani</i>	
Author Index	371

Progress in Cryptology -- INDOCRYPT 2015
16th International Conference on Cryptology in India,
Bangalore, India, December 6-9, 2015, Proceedings
Biryukov, A.; Goyal, V. (Eds.)
2015, XX, 371 p. 53 illus. in color., Softcover
ISBN: 978-3-319-26616-9