

Contents

Recent Advances in Function and Homomorphic Secret Sharing (Invited Talk)	1
<i>Elette Boyle</i>	
A Note on Ring-LWE Security in the Case of Fully Homomorphic Encryption	27
<i>Guillaume Bonnoron and Caroline Fontaine</i>	
Architecture Level Optimizations for Kummer Based HECC on FPGAs.	44
<i>Gabriel Gallin, Turku Ozlum Celik, and Arnaud Tisserand</i>	
Bricklayer Attack: A Side-Channel Analysis on the ChaCha Quarter Round	65
<i>Alexandre Adomnica, Jacques J. A. Fournier, and Laurent Masson</i>	
CCA-secure Predicate Encryption from Pair Encoding in Prime Order Groups: Generic and Efficient.	85
<i>Sanjit Chatterjee, Sayantan Mukherjee, and Tapas Pandit</i>	
Cold Boot Attacks on NTRU	107
<i>Kenneth G. Paterson and Ricardo Villanueva-Polanco</i>	
Differential Cryptanalysis of 18-Round PRIDE.	126
<i>Virginie Lallemand and Shahram Rasoolzadeh</i>	
DSA Signing Key Recovery with Noisy Side Channels and Variable Error Rates	147
<i>Jiji Angel, R. Rahul, C. Ashokkumar, and Bernard Menezes</i>	
Efficient Construction of Diamond Structures	166
<i>Ariel Weizmann, Orr Dunkelman, and Simi Haber</i>	
Efficient Optimal Ate Pairing at 128-Bit Security Level.	186
<i>Md. Al-Amin Khandaker, Yuki Nanjo, Loubna Ghammam, Sylvain Duquesne, Yasuyuki Nogami, and Yuta Kodera</i>	
Fast Scalar Multiplication for Elliptic Curves over Binary Fields by Efficiently Computable Formulas	206
<i>Saud Al Musa and Guangwu Xu</i>	
Field Lifting for Smaller UOV Public Keys	227
<i>Ward Beullens and Bart Preneel</i>	

Gabidulin Matrix Codes and Their Application to Small Ciphertext Size Cryptosystems	247
<i>Thierry P. Berger, Philippe Gaborit, and Olivier Ruatta</i>	
Lightweight Design Choices for LED-like Block Ciphers	267
<i>Sumanta Sarkar, Habeeb Syed, Rajat Sadhukhan, and Debdeep Mukhopadhyay</i>	
Looting the LUTs: FPGA Optimization of AES and AES-like Ciphers for Authenticated Encryption	282
<i>Mustafa Khairallah, Anupam Chattopadhyay, and Thomas Peyrin</i>	
Improved Differential Cryptanalysis on Generalized Feistel Schemes	302
<i>Ivan Tjuawinata, Tao Huang, and Hongjun Wu</i>	
Improvements for Gate-Hiding Garbled Circuits	325
<i>Mike Rosulek</i>	
Recovering Short Generators of Principal Fractional Ideals in Cyclotomic Fields of Conductor $p^z q^\beta$	346
<i>Patrick Holzer, Thomas Wunderer, and Johannes A. Buchmann</i>	
Revisiting a Masked Lookup-Table Compression Scheme	369
<i>Srinivas Vivek</i>	
Several Masked Implementations of the Boyar-Peralta AES S-Box	384
<i>Ashrujit Ghoshal and Thomas De Cnudde</i>	
Author Index	403

Progress in Cryptology – INDOCRYPT 2017

18th International Conference on Cryptology in India,
Chennai, India, December 10–13, 2017, Proceedings

Patra, A.; Smart, N.P. (Eds.)

2017, XII, 403 p. 68 illus., Softcover

ISBN: 978-3-319-71666-4