

Contents

Cryptographic Schemes

RingRainbow – An Efficient Multivariate Ring Signature Scheme.	3
<i>Mohamed Saied Emam Mohamed and Albrecht Petzoldt</i>	
Pinocchio-Based Adaptive zk-SNARKs and Secure/Correct Adaptive Function Evaluation.	21
<i>Mei of Veeningen</i>	
Revisiting and Extending the AONT-RS Scheme: A Robust Computationally Secure Secret Sharing Scheme	40
<i>Liqun Chen, Thalia M. Laing, and Keith M. Martin</i>	

Side-Channel Analysis

Climbing Down the Hierarchy: Hierarchical Classification for Machine Learning Side-Channel Attacks	61
<i>Stjepan Picek, Annelie Heuser, Alan Jovic, and Axel Legay</i>	
Multivariate Analysis Exploiting Static Power on Nanoscale CMOS Circuits for Cryptographic Applications	79
<i>Milena Djukanovic, Davide Bellizia, Giuseppe Scotti, and Alessandro Trifiletti</i>	
Differential Bias Attack for Block Cipher Under Randomized Leakage with Key Enumeration.	95
<i>Haruhisa Kosuge and Hidema Tanaka</i>	

Differential Cryptanalysis

Impossible Differential Cryptanalysis of Reduced-Round SKINNY	117
<i>Mohamed Tolba, Ahmed Abdelkhalek, and Amr M. Youssef</i>	
Impossible Differential Attack on Reduced Round SPARX-64/128	135
<i>Ahmed Abdelkhalek, Mohamed Tolba, and Amr M. Youssef</i>	

Applications

Private Conjunctive Query over Encrypted Data	149
<i>Tushar Kanti Saha and Takeshi Koshihira</i>	

Efficient Oblivious Transfer from Lossy Threshold Homomorphic Encryption 165
Isheeta Nargis

Privacy-Friendly Forecasting for the Smart Grid Using Homomorphic Encryption and the Group Method of Data Handling 184
Joppe W. Bos, Wouter Castryck, Ilia Iliashenko, and Frederik Vercauteren

Number Theory

On Indifferentiable Hashing into the Jacobian of Hyperelliptic Curves of Genus 2. 205
Michel Seck, Hortense Boudjou, Nafissatou Diarra, and Ahmed Youssef Ould Cheikh Khilil

Cryptanalysis of Some Protocols Using Matrices over Group Rings. 223
Mohammad Eftekhari

Author Index 231



<http://www.springer.com/978-3-319-57338-0>

Progress in Cryptology - AFRICACRYPT 2017
9th International Conference on Cryptology in Africa,
Dakar, Senegal, May 24-26, 2017, Proceedings
Joye, M.; Nitaj, A. (Eds.)
2017, X, 231 p. 42 illus., Softcover
ISBN: 978-3-319-57338-0