

# Contents

## Side Channel Analysis

Side-Channel Analysis on Blinded Regular Scalar Multiplications . . . . .	3
<i>Benoit Feix, Mylène Roussellet, and Alexandre Venelli</i>	
Online Template Attacks . . . . .	21
<i>Lejla Batina, Łukasz Chmielewski, Louiza Papachristodoulou, Peter Schwabe, and Michael Tunstall</i>	
Improved Multi-bit Differential Fault Analysis of Trivium . . . . .	37
<i>Prakash Dey and Avishek Adhikari</i>	
Recovering CRT-RSA Secret Keys from Message Reduced Values with Side-Channel Analysis . . . . .	53
<i>Benoit Feix, Hugues Thiebauld, and Lucille Tordella</i>	

## Theory

On Constant-Round Concurrent Zero-Knowledge from a Knowledge Assumption . . . . .	71
<i>Divya Gupta and Amit Sahai</i>	
Balancing Output Length and Query Bound in Hardness Preserving Constructions of Pseudorandom Functions . . . . .	89
<i>Nishanth Chandran and Sanjam Garg</i>	

## Block Ciphers

Linear Cryptanalysis of the PP-1 and PP-2 Block Ciphers . . . . .	107
<i>Michael Colburn and Liam Keliher</i>	
On the Key Schedule of Lightweight Block Ciphers . . . . .	124
<i>Jialin Huang, Serge Vaudenay, and Xuejia Lai</i>	
Cryptanalysis of Reduced-Round SIMON32 and SIMON48 . . . . .	143
<i>Qingju Wang, Zhiqiang Liu, Kerem Varıcı, Yu Sasaki, Vincent Rijmen, and Yosuke Todo</i>	
General Application of FFT in Cryptanalysis and Improved Attack on CAST-256 . . . . .	161
<i>Long Wen, Meiqin Wang, Andrey Bogdanov, and Huaifeng Chen</i>	

## Side Channel Analysis

Cryptanalysis of the Double-Feedback XOR-Chain Scheme Proposed in Indocrypt 2013 . . . . .	179
<i>Subhadeep Banik, Anupam Chattopadhyay, and Anusha Chowdhury</i>	
ESCAPE: Diagonal Fault Analysis of APE . . . . .	197
<i>Dhiman Saha, Sukhendu Kuila, and Dipanwita Roy Chowdhury</i>	

## Cryptanalysis

Using Random Error Correcting Codes in Near-Collision Attacks on Generic Hash-Functions . . . . .	219
<i>Inna Polak and Adi Shamir</i>	
Linear Cryptanalysis of FASER128/256 and TriviA-ck . . . . .	237
<i>Chao Xu, Bin Zhang, and Dengguo Feng</i>	
Partial Key Exposure Attack on CRT-RSA . . . . .	255
<i>Santanu Sarkar and Ayineedi Venkateswarlu</i>	
On the Leakage of Information in Biometric Authentication . . . . .	265
<i>Elena Pagnin, Christos Dimitrakakis, Aysajan Abidin, and Aikaterini Mitrokotsa</i>	

## Efficient Hardware Design

One Word/Cycle HC-128 Accelerator via State-Splitting Optimization . . . . .	283
<i>Ayesha Khalid, Prasanna Ravi, Anupam Chattopadhyay, and Goutam Paul</i>	
A Very Compact FPGA Implementation of LED and PHOTON. . . . .	304
<i>N. Nalla Anandakumar, Thomas Peyrin, and Axel Poschmann</i>	
S-box Pipelining Using Genetic Algorithms for High-Throughput AES Implementations: How Fast Can We Go?. . . . .	322
<i>Lejla Batina, Domagoj Jakobovic, Nele Mentens, Stjepan Picek, Antonio de la Piedra, and Dominik Sisejkovic</i>	

## Protected Hardware Design

Wire-Tap Codes as Side-Channel Countermeasure: – An FPGA-Based Experiment – . . . . .	341
<i>Amir Moradi</i>	
Differential Power Analysis in Hamming Weight Model: How to Choose among (Extended) Affine Equivalent S-boxes . . . . .	360
<i>Sumanta Sarkar, Subhamoy Maitra, and Kaushik Chakraborty</i>	

Confused by Confusion: Systematic Evaluation of DPA Resistance of Various S-boxes . . . . .	374
<i>Stjepan Picek, Kostas Papagiannopoulos, Baris Ege, Lejla Batina, and Domagoj Jakobovic</i>	

## Elliptic Curves

Binary Edwards Curves Revisited. . . . .	393
<i>Kwang Ho Kim, Chol Ok Lee, and Christophe Negre</i>	
Summation Polynomial Algorithms for Elliptic Curves in Characteristic Two. . .	409
<i>Steven D. Galbraith and Shishay W. Gebregiyorgis</i>	
A Quantum Algorithm for Computing Isogenies between Supersingular Elliptic Curves . . . . .	428
<i>Jean-François Biasse, David Jao, and Anirudh Sankar</i>	
<b>Author Index</b> . . . . .	443

Progress in Cryptology -- INDOCRYPT 2014  
15th International Conference on Cryptology in India,  
New Delhi, India, December 14-17, 2014, Proceedings  
Meier, W.; Mukhopadhyay, D. (Eds.)  
2014, XXVI, 444 p. 80 illus., Softcover  
ISBN: 978-3-319-13038-5