

# Contents

## Privacy Enhancing Technologies

Formal Treatment of Privacy-Enhancing Credential Systems. . . . .	3
<i>Jan Camenisch, Stephan Krenn, Anja Lehmann, Gert Læssøe Mikkelsen, Gregory Neven, and Michael Østergaard Pedersen</i>	
Minimizing the Number of Bootstrappings in Fully Homomorphic Encryption . . . . .	25
<i>Marie Paindavoine and Bastien Vialla</i>	
Privacy-Preserving Fingerprint Authentication Resistant to Hill-Climbing Attacks . . . . .	44
<i>Haruna Higo, Toshiyuki Isshiki, Kengo Mori, and Satoshi Obana</i>	

## Cryptanalysis of Symmetric-Key Primitives

Practical Cryptanalysis of Full Sprout with TMD Tradeoff Attacks . . . . .	67
<i>Muhammed F. Esgin and Orhun Kara</i>	
Related-Key Attack on Full-Round PICARO . . . . .	86
<i>Anne Canteaut, Virginie Lallemand, and María Naya-Plasencia</i>	
Cryptanalysis of Feistel Networks with Secret Round Functions . . . . .	102
<i>Alex Biryukov, Gaëtan Leurent, and Léo Perrin</i>	
Improved Meet-in-the-Middle Distinguisher on Feistel Schemes . . . . .	122
<i>Li Lin, Wenling Wu, and Yafei Zheng</i>	

## Implementation of Cryptographic Schemes

Sandy2x: New Curve25519 Speed Records . . . . .	145
<i>Tung Chou</i>	
ECC on Your Fingertips: A Single Instruction Approach for Lightweight ECC Design in $GF(p)$ . . . . .	161
<i>Debapriya Basu Roy, Poulami Das, and Debdeep Mukhopadhyay</i>	
Exploring Energy Efficiency of Lightweight Block Ciphers . . . . .	178
<i>Subhadeep Banik, Andrey Bogdanov, and Francesco Regazzoni</i>	

## Short Papers

Forgery and Subkey Recovery on CAESAR Candidate iFeed . . . . .	197
<i>Willem Schroé, Bart Mennink, Elena Andreeva, and Bart Preneel</i>	
Key-Recovery Attacks Against the MAC Algorithm Chaskey . . . . .	205
<i>Chrysanthi Mavromati</i>	
Differential Forgery Attack Against LAC . . . . .	217
<i>Gaëtan Leurent</i>	

## Privacy Preserving Data Processing

Private Information Retrieval with Preprocessing Based on the Approximate GCD Problem . . . . .	227
<i>Thomas Vannet and Noboru Kunihiro</i>	
Dynamic Searchable Symmetric Encryption with Minimal Leakage and Efficient Updates on Commodity Hardware . . . . .	241
<i>Attila A. Yavuz and Jorge Guajardo</i>	

## Side Channel Attacks and Defenses

Affine Equivalence and Its Application to Tightening Threshold Implementations . . . . .	263
<i>Pascal Sasdrich, Amir Moradi, and Tim Güneysu</i>	
Near Collision Side Channel Attacks . . . . .	277
<i>Barış Ege, Thomas Eisenbarth, and Lejla Batina</i>	
Masking Large Keys in Hardware: A Masked Implementation of McEliece . . .	293
<i>Cong Chen, Thomas Eisenbarth, Ingo von Maurich, and Rainer Steinwandt</i>	
Fast and Memory-Efficient Key Recovery in Side-Channel Attacks . . . . .	310
<i>Andrey Bogdanov, Ilya Kizhvatov, Kamran Manzoor, Elmar Tischhauser, and Marc Wittenman</i>	

## New Cryptographic Constructions

An Efficient Post-Quantum One-Time Signature Scheme . . . . .	331
<i>Kassem Kalach and Reihaneh Safavi-Naini</i>	
Constructing Lightweight Optimal Diffusion Primitives with Feistel Structure. . . . .	352
<i>Zhiyuan Guo, Wenling Wu, and Si Gao</i>	

Construction of Lightweight S-Boxes Using Feistel and MISTY Structures. . . .	373
<i>Anne Canteaut, Sébastien Duval, and Gaëtan Leurent</i>	

### **Authenticated Encryption**

A New Mode of Operation for Incremental Authenticated Encryption with Associated Data. . . . .	397
<i>Yu Sasaki and Kan Yasuda</i>	

SCOPE: On the Side Channel Vulnerability of Releasing Unverified Plaintexts . . . . .	417
<i>Dhiman Saha and Dipanwita Roy Chowdhury</i>	

### **On the Hardness of Mathematical Problems**

Bit Security of the CDH Problems over Finite Fields. . . . .	441
<i>Mingqiang Wang, Tao Zhan, and Haibin Zhang</i>	
Towards Optimal Bounds for Implicit Factorization Problem . . . . .	462
<i>Yao Lu, Liqiang Peng, Rui Zhang, Lei Hu, and Dongdai Lin</i>	

### **Cryptanalysis of Authenticated Encryption Schemes**

Forgery Attacks on Round-Reduced ICEPOLE-128. . . . .	479
<i>Christoph Dobraunig, Maria Eichlseder, and Florian Mendel</i>	
Analysis of the CAESAR Candidate Silver. . . . .	493
<i>Jérémy Jean, Yu Sasaki, and Lei Wang</i>	
Cryptanalysis of the Authenticated Encryption Algorithm COFFE. . . . .	510
<i>Ivan Tjuawinata, Tao Huang, and Hongjun Wu</i>	

<b>Author Index</b> . . . . .	527
-------------------------------	-----

Selected Areas in Cryptography - SAC 2015  
22nd International Conference, Sackville, NB, Canada,  
August 12-14, 2015, Revised Selected Papers  
Dunkelman, O.; Keliher, L. (Eds.)  
2016, XIX, 528 p. 117 illus., Softcover  
ISBN: 978-3-319-31300-9