

# 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  
*Willem Schroé, Bart Mennink, Elena Andreeva, and Bart Preneel*

Key-Recovery Attacks Against the MAC Algorithm Chaskey . . . . . 205  
*Chrysanthi Mavromati*

Differential Forgery Attack Against LAC . . . . . 217  
*Gaëtan Leurent*

**Privacy Preserving Data Processing**

Private Information Retrieval with Preprocessing Based  
on the Approximate GCD Problem . . . . . 227  
*Thomas Vannet and Noboru Kunihiro*

Dynamic Searchable Symmetric Encryption with Minimal Leakage  
and Efficient Updates on Commodity Hardware . . . . . 241  
*Attila A. Yavuz and Jorge Guajardo*

**Side Channel Attacks and Defenses**

Affine Equivalence and Its Application to Tightening Threshold  
Implementations . . . . . 263  
*Pascal Sasdrich, Amir Moradi, and Tim Güneysu*

Near Collision Side Channel Attacks . . . . . 277  
*Barış Ege, Thomas Eisenbarth, and Lejla Batina*

Masking Large Keys in Hardware: A Masked Implementation of McEliece . . . 293  
*Cong Chen, Thomas Eisenbarth, Ingo von Maurich,  
and Rainer Steinwandt*

Fast and Memory-Efficient Key Recovery in Side-Channel Attacks . . . . . 310  
*Andrey Bogdanov, Ilya Kizhvatov, Kamran Manzoor,  
Elmar Tischhauser, and Marc Witteman*

**New Cryptographic Constructions**

An Efficient Post-Quantum One-Time Signature Scheme . . . . . 331  
*Kassem Kalach and Reihaneh Safavi-Naini*

Constructing Lightweight Optimal Diffusion Primitives  
with Feistel Structure. . . . . 352  
*Zhiyuan Guo, Wenling Wu, and Si Gao*

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

**Authenticated Encryption**

A New Mode of Operation for Incremental Authenticated Encryption  
with Associated Data. . . . . 397  
*Yu Sasaki and Kan Yasuda*

SCOPE: On the Side Channel Vulnerability of Releasing  
Unverified Plaintexts . . . . . 417  
*Dhiman Saha and Dipanwita Roy Chowdhury*

**On the Hardness of Mathematical Problems**

Bit Security of the CDH Problems over Finite Fields. . . . . 441  
*Mingqiang Wang, Tao Zhan, and Haibin Zhang*

Towards Optimal Bounds for Implicit Factorization Problem . . . . . 462  
*Yao Lu, Liqiang Peng, Rui Zhang, Lei Hu, and Dongdai Lin*

**Cryptanalysis of Authenticated Encryption Schemes**

Forgery Attacks on Round-Reduced ICEPOLE-128. . . . . 479  
*Christoph Dobraunig, Maria Eichlseder, and Florian Mendel*

Analysis of the CAESAR Candidate Silver. . . . . 493  
*Jérémy Jean, Yu Sasaki, and Lei Wang*

Cryptanalysis of the Authenticated Encryption Algorithm COFFE. . . . . 510  
*Ivan Tjuawinata, Tao Huang, and Hongjun Wu*

**Author Index** . . . . . 527



<http://www.springer.com/978-3-319-31300-9>

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