

# Contents

## Timing Attacks

Just a Little Bit More . . . . .	3
<i>Joop van de Pol, Nigel P. Smart, and Yuval Yarom</i>	
Cache Storage Attacks. . . . .	22
<i>Billy Bob Brumley</i>	

## Design and Analysis of Block Ciphers

Analyzing Permutations for AES-like Ciphers: Understanding ShiftRows . . .	37
<i>Christof Beierle, Philipp Jovanovic, Martin M. Lauridsen, Gregor Leander, and Christian Rechberger</i>	
Improved Attacks on Reduced-Round Camellia-128/192/256 . . . . .	59
<i>Xiaoyang Dong, Leibo Li, Keting Jia, and Xiaoyun Wang</i>	

## Attribute and Identity Based Encryption

Duality in ABE: Converting Attribute Based Encryption for Dual Predicate and Dual Policy via Computational Encodings. . . . .	87
<i>Nuttapong Attrapadung and Shota Yamada</i>	
Revocable Hierarchical Identity-Based Encryption: History-Free Update, Security Against Insiders, and Short Ciphertexts. . . . .	106
<i>Jae Hong Seo and Keita Emura</i>	

## Membership

Revisiting Cryptographic Accumulators, Additional Properties and Relations to Other Primitives . . . . .	127
<i>David Derler, Christian Hanser, and Daniel Slamanig</i>	
Non-Interactive Zero-Knowledge Proofs of Non-Membership . . . . .	145
<i>Olivier Blazy, Céline Chevalier, and Damien Vergnaud</i>	

## Secure and Efficient Implementation of AES Based Cryptosystems

Implementing GCM on ARMv8 . . . . .	167
<i>Conrado P.L. Gouvêa and Julio López</i>	

Higher-Order Masking in Practice: A Vector Implementation of Masked AES for ARM NEON . . . . .	181
<i>Junwei Wang, Praveen Kumar Vadnala, Johann Großschädl, and Qiuliang Xu</i>	

**Chosen Ciphertext Attacks in Theory and Practice**

Completeness of Single-Bit Projection-KDM Security for Public Key Encryption . . . . .	201
<i>Fuyuki Kitagawa, Takahiro Matsuda, Goichiro Hanaoka, and Keisuke Tanaka</i>	
Format Oracles on OpenPGP . . . . .	220
<i>Florian Maury, Jean-René Reinhard, Olivier Levillain, and Henri Gilbert</i>	

**Algorithms for Solving Hard Problems**

Finding Shortest Lattice Vectors in the Presence of Gaps . . . . .	239
<i>Wei Wei, Mingjie Liu, and Xiaoyun Wang</i>	
A Simple and Improved Algorithm for Integer Factorization with Implicit Hints . . . . .	258
<i>Koji Nuida, Naoto Itakura, and Kaoru Kurosawa</i>	

**Constructions of Hash Functions and Message Authentication Codes**

Hash Functions from Defective Ideal Ciphers. . . . .	273
<i>Jonathan Katz, Stefan Lucks, and Aishwarya Thiruvengadam</i>	
Using an Error-Correction Code for Fast, Beyond-birthday-bound Authentication . . . . .	291
<i>Yusi Zhang</i>	

**Secure Multiparty Computation**

Efficient Leakage Resilient Circuit Compilers . . . . .	311
<i>Marcin Andrychowicz, Ivan Damgård, Stefan Dziembowski, Sebastian Faust, and Antigoni Polychroniadou</i>	
Optimally Efficient Multi-Party Fair Exchange and Fair Secure Multi-Party Computation . . . . .	330
<i>Handan Kılınç and Alptekin Küpçü</i>	

**Authenticated Encryption**

How to Incorporate Associated Data in Sponge-Based Authenticated Encryption . . . . .	353
<i>Yu Sasaki and Kan Yasuda</i>	
Cryptanalysis of Ascon . . . . .	371
<i>Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schl��ffer</i>	

**Detecting and Tracing Malicious Activities**

Stronger Security Notions for Decentralized Traceable Attribute-Based Signatures and More Efficient Constructions . . . . .	389
<i>Essam Ghadafi</i>	
Re-Encryption Verifiability: How to Detect Malicious Activities of a Proxy in Proxy Re-Encryption . . . . .	408
<i>Satsuya Ohata, Yutaka Kawai, Takahiro Matsuda, Goichiro Hanaoka, and Kanta Matsuura</i>	

**Implementation Attacks on Exponentiation Algorithms**

Exploiting Collisions in Addition Chain-Based Exponentiation Algorithms Using a Single Trace. . . . .	429
<i>Neil Hanley, HeeSeok Kim, and Michael Tunstall</i>	
Cold Boot Attacks in the Discrete Logarithm Setting . . . . .	447
<i>Bertram Poettering and Dale L. Sibborn</i>	

**Homomorphic Encryption and Its Applications**

Communication Optimal Tardos-Based Asymmetric Fingerprinting . . . . .	465
<i>Aggelos Kiayias, Nikos Leonardos, Helger Lipmaa, Kateryna Pavlyk, and Qiang Tang</i>	
Linearly Homomorphic Encryption from DDH. . . . .	484
<i>Guilhem Castagnos and Fabien Laguillaumie</i>	

<b>Author Index</b> . . . . .	503
-------------------------------	-----

<http://www.springer.com/978-3-319-16714-5>

Topics in Cryptology -- CT-RSA 2015  
The Cryptographer's Track at the RSA Conference  
2015, San Francisco, CA, USA, April 20-24, 2015.  
Proceedings  
Nyberg, K. (Ed.)  
2015, XIII, 508 p. 79 illus., Softcover  
ISBN: 978-3-319-16714-5