

Contents

Timing Attacks

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

Design and Analysis of Block Ciphers

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

Attribute and Identity Based Encryption

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

Membership

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

Secure and Efficient Implementation of AES Based Cryptosystems

- Implementing GCM on ARMv8 167
Conrado P.L. Gouvêa and Julio López

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

Chosen Ciphertext Attacks in Theory and Practice

Completeness of Single-Bit Projection-KDM Security for Public
Key Encryption 201
*Fuyuki Kitagawa, Takahiro Matsuda, Goichiro Hanaoka,
and Keisuke Tanaka*

Format Oracles on OpenPGP 220
Florian Maury, Jean-René Reinhard, Olivier Levillain, and Henri Gilbert

Algorithms for Solving Hard Problems

Finding Shortest Lattice Vectors in the Presence of Gaps 239
Wei Wei, Mingjie Liu, and Xiaoyun Wang

A Simple and Improved Algorithm for Integer Factorization
with Implicit Hints 258
Koji Nuida, Naoto Itakura, and Kaoru Kurosawa

Constructions of Hash Functions and Message Authentication Codes

Hash Functions from Defective Ideal Ciphers. 273
Jonathan Katz, Stefan Lucks, and Aishwarya Thiruvengadam

Using an Error-Correction Code for Fast, Beyond-birthday-bound
Authentication 291
Yusi Zhang

Secure Multiparty Computation

Efficient Leakage Resilient Circuit Compilers 311
*Marcin Andrychowicz, Ivan Damgård, Stefan Dziembowski,
Sebastian Faust, and Antigoni Polychroniadou*

Optimally Efficient Multi-Party Fair Exchange and Fair Secure
Multi-Party Computation 330
Handan Kılınç and Alptekin Küpçü

Authenticated Encryption

How to Incorporate Associated Data in Sponge-Based Authenticated Encryption 353
Yu Sasaki and Kan Yasuda

Cryptanalysis of Ascon 371
Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schl affer

Detecting and Tracing Malicious Activities

Stronger Security Notions for Decentralized Traceable Attribute-Based Signatures and More Efficient Constructions 389
Essam Ghadafi

Re-Encryption Verifiability: How to Detect Malicious Activities of a Proxy in Proxy Re-Encryption 408
Satsuya Ohata, Yutaka Kawai, Takahiro Matsuda, Goichiro Hanaoka, and Kanta Matsuura

Implementation Attacks on Exponentiation Algorithms

Exploiting Collisions in Addition Chain-Based Exponentiation Algorithms Using a Single Trace. 429
Neil Hanley, HeeSeok Kim, and Michael Tunstall

Cold Boot Attacks in the Discrete Logarithm Setting 447
Bertram Poettering and Dale L. Sibborn

Homomorphic Encryption and Its Applications

Communication Optimal Tardos-Based Asymmetric Fingerprinting 465
Aggelos Kiayias, Nikos Leonardos, Helger Lipmaa, Kateryna Pavlyk, and Qiang Tang

Linearly Homomorphic Encryption from DDH. 484
Guilhem Castagnos and Fabien Laguillaumie

Author Index 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