

# Contents – Part III

## Authenticated Encryption

Boosting Authenticated Encryption Robustness with Minimal Modifications . . . . .	3
<i>Tomer Ashur, Orr Dunkelman, and Atul Luykx</i>	
ZMAC: A Fast Tweakable Block Cipher Mode for Highly Secure Message Authentication . . . . .	34
<i>Tetsu Iwata, Kazuhiko Minematsu, Thomas Peyrin, and Yannick Seurin</i>	
Message Franking via Committing Authenticated Encryption . . . . .	66
<i>Paul Grubbs, Jiahui Lu, and Thomas Ristenpart</i>	
Key Rotation for Authenticated Encryption . . . . .	98
<i>Adam Everspaugh, Kenneth Paterson, Thomas Ristenpart, and Sam Scott</i>	

## Public-Key Encryption

Kurosawa-Desmedt Meets Tight Security . . . . .	133
<i>Romain Gay, Dennis Hofheinz, and Lisa Kohl</i>	
Asymptotically Compact Adaptively Secure Lattice IBEs and Verifiable Random Functions via Generalized Partitioning Techniques . . . . .	161
<i>Shota Yamada</i>	
Identity-Based Encryption from Codes with Rank Metric . . . . .	194
<i>Philippe Gaborit, Adrien Hauteville, Duong Hieu Phan, and Jean-Pierre Tillich</i>	

## Stream Ciphers

Degree Evaluation of NFSR-Based Cryptosystems . . . . .	227
<i>Meicheng Liu</i>	
Cube Attacks on Non-Blackbox Polynomials Based on Division Property . . .	250
<i>Yosuke Todo, Takanori Isobe, Yonglin Hao, and Willi Meier</i>	

## Lattice Crypto

Middle-Product Learning with Errors . . . . .	283
<i>Miruna Roşca, Amin Sakzad, Damien Stehlé, and Ron Steinfeld</i>	

All-But-Many Lossy Trapdoor Functions from Lattices and Applications . . . .	298
<i>Xavier Boyen and Qinyi Li</i>	

All-But-Many Lossy Trapdoor Functions and Selective Opening Chosen-Ciphertext Security from LWE . . . . .	332
<i>Benoît Libert, Amin Sakzad, Damien Stehlé, and Ron Steinfeld</i>	

Amortization with Fewer Equations for Proving Knowledge of Small Secrets . . . . .	365
<i>Rafael del Pino and Vadim Lyubashevsky</i>	

## Leakage and Subversion

Private Multiplication over Finite Fields. . . . .	397
<i>Sonia Belaïd, Fabrice Benhamouda, Alain Passelègue, Emmanuel Prouff, Adrian Thillard, and Damien Vergnaud</i>	

Anonymous Attestation with Subverted TPMs . . . . .	427
<i>Jan Camenisch, Manu Drijvers, and Anja Lehmann</i>	

Hedging Public-Key Encryption in the Real World . . . . .	462
<i>Alexandra Boldyreva, Christopher Patton, and Thomas Shrimpton</i>	

## Symmetric-Key Crypto

Information-Theoretic Indistinguishability via the Chi-Squared Method . . . .	497
<i>Wei Dai, Viet Tung Hoang, and Stefano Tessaro</i>	

Indifferentiability of Iterated Even-Mansour Ciphers with Non-idealized Key-Schedules: Five Rounds Are Necessary and Sufficient . . . . .	524
<i>Yuanxi Dai, Yannick Seurin, John Steinberger, and Aishwarya Thiruvengadam</i>	

Encrypted Davies-Meyer and Its Dual: Towards Optimal Security Using Mirror Theory . . . . .	556
<i>Bart Mennink and Samuel Neves</i>	

## Real-World Crypto

A Formal Treatment of Multi-key Channels . . . . .	587
<i>Felix Günther and Sogol Mazaheri</i>	

Ratcheted Encryption and Key Exchange: The Security of Messaging . . . .	619
<i>Mihir Bellare, Asha Camper Singh, Joseph Jaeger, Maya Nyayapati, and Igors Stepanovs</i>	

PRF-ODH: Relations, Instantiations, and Impossibility Results . . . . .	651
<i>Jacqueline Brendel, Marc Fischlin, Felix Günther, and Christian Janson</i>	
A New Distribution-Sensitive Secure Sketch and Popularity-Proportional Hashing . . . . .	682
<i>Joanne Woodage, Rahul Chatterjee, Yevgeniy Dodis, Ari Juels, and Thomas Ristenpart</i>	
<b>Author Index</b> . . . . .	711

<http://www.springer.com/978-3-319-63696-2>

Advances in Cryptology – CRYPTO 2017

37th Annual International Cryptology Conference, Santa  
Barbara, CA, USA, August 20–24, 2017, Proceedings,

Part III

Katz, J.; Shacham, H. (Eds.)

2017, XV, 713 p. 95 illus., Softcover

ISBN: 978-3-319-63696-2