

# Contents

## Secure Key Exchange Schemes

Mitigating Server Breaches in Password-Based Authentication: Secure and Efficient Solutions . . . . .	3
<i>Olivier Blazy, Céline Chevalier, and Damien Vergnaud</i>	
Strongly Leakage-Resilient Authenticated Key Exchange . . . . .	19
<i>Rongmao Chen, Yi Mu, Guomin Yang, Willy Susilo, and Fuchun Guo</i>	

## Authenticated Encryption

INT-RUP Analysis of Block-cipher Based Authenticated Encryption Schemes . . . . .	39
<i>Avik Chakraborti, Nilanjan Datta, and Mridul Nandi</i>	
From Stateless to Stateful: Generic Authentication and Authenticated Encryption Constructions with Application to TLS . . . . .	55
<i>Colin Boyd, Britta Hale, Stig Frode Mjølsnes, and Douglas Stebila</i>	

## Searchable Symmetric Encryption

Dynamic Symmetric Searchable Encryption from Constrained Functional Encryption . . . . .	75
<i>Sebastian Gajek</i>	
Private Large-Scale Databases with Distributed Searchable Symmetric Encryption . . . . .	90
<i>Yuval Ishai, Eyal Kushilevitz, Steve Lu, and Rafail Ostrovsky</i>	

## Digital Signatures with New Functionality

Short Randomizable Signatures . . . . .	111
<i>David Pointcheval and Olivier Sanders</i>	
Non-Interactive Plaintext (In-)Equality Proofs and Group Signatures with Verifiable Controllable Linkability . . . . .	127
<i>Olivier Blazy, David Derler, Daniel Slamanig, and Raphael Spreitzer</i>	

**Secure Multi Party Computation**

Hybrid Publicly Verifiable Computation. . . . .	147
<i>James Alderman, Christian Janson, Carlos Cid, and Jason Crampton</i>	
Efficient Concurrent Covert Computation of String Equality and Set Intersection. . . . .	164
<i>Chongwon Cho, Dana Dachman-Soled, and Stanisław Jarecki</i>	

**How to Verify Procedures**

Secure Audit Logs with Verifiable Excerpts . . . . .	183
<i>Gunnar Hartung</i>	
Efficient Culpably Sound NIZK Shuffle Argument Without Random Oracles . . . . .	200
<i>Prastudy Fauzi and Helger Lipmaa</i>	

**Side-Channel Attacks on Elliptic Curve Cryptography**

ECDH Key-Extraction via Low-Bandwidth Electromagnetic Attacks on PCs . . . . .	219
<i>Daniel Genkin, Lev Pachmanov, Itamar Pipman, and Eran Tromer</i>	
Side-Channel Analysis of Weierstrass and Koblitz Curve ECDSA on Android Smartphones . . . . .	236
<i>Pierre Belgaric, Pierre-Alain Fouque, Gilles Macario-Rat, and Mehdi Tibouchi</i>	

**Hardware Attacks and Security**

Enhancing Side-Channel Analysis of Binary-Field Multiplication with Bit Reliability . . . . .	255
<i>Peter Pessl and Stefan Mangard</i>	
Towards a Unified Security Model for Physically Unclonable Functions . . . .	271
<i>Frederik Armknecht, Daisuke Moriyama, Ahmad-Reza Sadeghi, and Moti Yung</i>	

**Structure-Preserving Signatures**

Cryptanalysis of the Structure-Preserving Signature Scheme on Equivalence Classes from Asiacrypt 2014 . . . . .	291
<i>Yanbin Pan</i>	
Short Structure-Preserving Signatures . . . . .	305
<i>Essam Ghadafi</i>	

## Lattice Cryptography

Which Ring Based Somewhat Homomorphic Encryption Scheme is Best? . . .	325
<i>Ana Costache and Nigel P. Smart</i>	
NFLlib: NTT-Based Fast Lattice Library . . . . .	341
<i>Carlos Aguilar-Melchor, Joris Barrier, Serge Guelton, Adrien Guinet, Marc-Olivier Killijian, and Tancrède Lepoint</i>	

## Cryptanalysis of Symmetric Key Encryption

Optimization of Rainbow Tables for Practically Cracking GSM A5/1 Based on Validated Success Rate Modeling . . . . .	359
<i>Zhen Li</i>	
New Observations on Piccolo Block Cipher . . . . .	378
<i>Yanfeng Wang and Wenling Wu</i>	

## Message Authentication Code and PRF-Security

Replacing SHA-2 with SHA-3 Enhances Generic Security of HMAC . . . . .	397
<i>Yusuke Naito and Lei Wang</i>	
Constrained PRFs for Unbounded Inputs . . . . .	413
<i>Hamza Abusalah, Georg Fuchsbauer, and Krzysztof Pietrzak</i>	

## Security of Public Key Encryption

Construction of Fully CCA-Secure Predicate Encryptions from Pair Encoding Schemes . . . . .	431
<i>Johannes Blömer and Gennadij Liske</i>	
Factoring $N = p^r q^s$ for Large $r$ and $s$ . . . . .	448
<i>Jean-Sébastien Coron, Jean-Charles Faugère, Guénaél Renault, and Rina Zeitoun</i>	

Author Index . . . . .	465
------------------------	-----

Topics in Cryptology - CT-RSA 2016

The Cryptographers' Track at the RSA Conference

2016, San Francisco, CA, USA, February 29 - March 4,

2016, Proceedings

Sako, K. (Ed.)

2016, XI, 465 p. 68 illus. in color., Softcover

ISBN: 978-3-319-29484-1