Contents

Secure Key Exchange Schemes

Mitigating Server Breaches in Password-Based Authentication: Secure and Efficient Solutions. .................................................. 3

Olivier Blazy, Céline Chevalier, and Damien Vergnaud

Strongly Leakage-Resilient Authenticated Key Exchange ............... 19

Rongmao Chen, Yi Mu, Guomin Yang, Willy Susilo, and Fuchun Guo

Authenticated Encryption

INT-RUP Analysis of Block-cipher Based Authenticated Encryption Schemes ................................................................. 39

Avik Chakraborti, Nilanjan Datta, and Mridul Nandi

From Stateless to Stateful: Generic Authentication and Authenticated Encryption Constructions with Application to TLS ..................... 55

Colin Boyd, Britta Hale, Stig Frode Mjølsnes, and Douglas Stebila

Searchable Symmetric Encryption

Dynamic Symmetric Searchable Encryption from Constrained Functional Encryption ............................................................. 75

Sebastian Gajek

Private Large-Scale Databases with Distributed Searchable Symmetric Encryption ............................................................ 90

Yuval Ishai, Eyal Kushilevitz, Steve Lu, and Rafail Ostrovsky

Digital Signatures with New Functionality

Short Randomizable Signatures ............................................. 111

David Pointcheval and Olivier Sanders

Non-Interactive Plaintext (In-)Equality Proofs and Group Signatures with Verifiable Controllable Linkability ......................... 127

Olivier Blazy, David Derler, Daniel Slamanig, and Raphael Spreitzer
Secure Multi Party Computation

Hybrid Publicly Verifiable Computation ................................. 147
James Alderman, Christian Janson, Carlos Cid, and Jason Crampton

Efficient Concurrent Covert Computation of String Equality and Set Intersection ................................. 164
Chongwon Cho, Dana Dachman-Soled, and Stanislaw Jarecki

How to Verify Procedures

Secure Audit Logs with Verifiable Excerpts ................................. 183
Gunnar Hartung

Efficient Culpably Sound NIZK Shuffle Argument Without Random Oracles ................................................. 200
Prastudy Fauzi and Helger Lipmaa

Side-Channel Attacks on Elliptic Curve Cryptography

ECDH Key-Extraction via Low-Bandwidth Electromagnetic Attacks on PCs ................................................. 219
Daniel Genkin, Lev Pachmanov, Itamar Pipman, and Eran Tromer

Side-Channel Analysis of Weierstrass and Koblitz Curve ECDSA on Android Smartphones ................................................. 236
Pierre Belgarric, Pierre-Alain Fouque, Gilles Macario-Rat, and Mehdi Tibouchi

Hardware Attacks and Security

Enhancing Side-Channel Analysis of Binary-Field Multiplication with Bit Reliability ................................................. 255
Peter Pessl and Stefan Mangard

Towards a Unified Security Model for Physically Unclonable Functions ................................................. 271
Frederik Armknecht, Daisuke Moriyama, Ahmad-Reza Sadeghi, and Moti Yung

Structure-Preserving Signatures

Cryptanalysis of the Structure-Preserving Signature Scheme on Equivalence Classes from Asiacrypt 2014 ................................................. 291
Yanbin Pan

Short Structure-Preserving Signatures ................................................. 305
Essam Ghadafi
Lattice Cryptography

Which Ring Based Somewhat Homomorphic Encryption Scheme is Best? . . . 325
Ana Costache and Nigel P. Smart

NFLlib: NTT-Based Fast Lattice Library . . . . . . . . . . . . . . . . . . . . . . . . 341
Carlos Aguilar-Melchor, Joris Barrier, Serge Guelton, Adrien Guinet,
Marc-Olivier Killijian, and Tancrède Lepoint

Cryptanalysis of Symmetric Key Encryption

Optimization of Rainbow Tables for Practically Cracking GSM A5/1
Based on Validated Success Rate Modeling . . . . . . . . . . . . . . . . . . . . . . 359
Zhen Li

New Observations on Piccolo Block Cipher . . . . . . . . . . . . . . . . . . . . . . . . 378
Yanfeng Wang and Wenling Wu

Message Authentication Code and PRF-Security

Replacing SHA-2 with SHA-3 Enhances Generic Security of HMAC . . . . . . 397
Yusuke Naito and Lei Wang

Constrained PRFs for Unbounded Inputs . . . . . . . . . . . . . . . . . . . . . . . . . 413
Hamza Abusalah, Georg Fuchsbauer, and Krzysztof Pietrzak

Security of Public Key Encryption

Construction of Fully CCA-Secure Predicate Encryptions
from Pair Encoding Schemes . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 431
Johannes Blömer and Gennadij Liske

Factoring $N = p^r q^s$ for Large $r$ and $s$ . . . . . . . . . . . . . . . . . . . . . . . . 448
Jean-Sébastien Coron, Jean-Charles Faugère, Guénaël Renault,
and Rina Zeitoun

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