Contents

Public Key Implementations

Choosing Parameters for NTRUEncrypt ........................................... 3
   Jeff Hoffstein, Jill Pipher, John M. Schanck, Joseph H. Silverman,
   William Whyte, and Zhenfei Zhang

Encoding-Free ElGamal-Type Encryption Schemes on Elliptic Curves .... 19
   Marc Joye and Benoît Libert

Lattice-Based Cryptanalysis

Gauss Sieve Algorithm on GPUs .................................................. 39
   Shang-Yi Yang, Po-Chun Kuo, Bo-Yin Yang, and Chen-Mou Cheng

A Tool Kit for Partial Key Exposure Attacks on RSA .......................... 58
   Atsushi Takayasu and Noboru Kunihiro

Fault and Glitch Resistant Implementations

Feeding Two Cats with One Bowl: On Designing a Fault and Side-Channel
   Resistant Software Encoding Scheme ......................................... 77
   Jakub Breier and Xiaolu Hou

An Efficient Side-Channel Protected AES Implementation
   with Arbitrary Protection Order ................................................. 95
   Hannes Gross, Stefan Mangard, and Thomas Korak

Side-channel Resistant Implementations

Time-Memory Trade-Offs for Side-Channel Resistant Implementations
   of Block Ciphers ........................................................................ 115
   Praveen Kumar Vadnala

Hiding Higher-Order Side-Channel Leakage: Randomizing Cryptographic
   Implementations in Reconfigurable Hardware ................................ 131
   Pascal Sasdrich, Amir Moradi, and Tim Güneysu

Digital Signatures and Random Numbers

Surnaming Schemes, Fast Verification, and Applications
   to SGX Technology ...................................................................... 149
   Dan Boneh and Shay Gueron
On the Entropy of Oscillator-Based True Random Number Generators .......................... 165
  *Yuan Ma, Jingqiang Lin, and Jiwu Jing*

**Post-quantum Cryptography**

Provably Secure Password Authenticated Key Exchange Based on RLWE for the Post-Quantum World ................................................................. 183
  *Jintai Ding, Saed Alsayigh, Jean Lancrenon, Saraswathy RV, and Michael Snook*

**Symmetric Key Cryptanalysis**

Impossible-Differential and Boomerang Cryptanalysis of Round-Reduced Kiasu-BC ................................................................. 207
  *Christoph Dobraunig and Eik List*

Weak Keys for AEZ, and the External Key Padding Attack ........................................ 223
  *Bart Mennink*

**Symmetric Key Constructions**

Full Disk Encryption: Bridging Theory and Practice .............................................. 241
  *Louiza Khati, Nicky Mouha, and Damien Vergnaud*

Revisiting Full-PRF-Secure PMAC and Using It for Beyond-Birthday Authenticated Encryption .............................................. 258
  *Eik List and Mridul Nandi*

**2017 Selected Topics**

Publish or Perish: A Backward-Compatible Defense Against Selfish Mining in Bitcoin ................................................................. 277
  *Ren Zhang and Bart Preneel*

WEM: A New Family of White-Box Block Ciphers Based on the Even-Mansour Construction ................................................................. 293
  *Jihoon Cho, Kyu Young Choi, Itai Dinur, Orr Dunkelman, Nathan Keller, Dukjae Moon, and Aviya Veidberg*

**Improved Key Recovery Algorithms**

A Bounded-Space Near-Optimal Key Enumeration Algorithm for Multi-subkey Side-Channel Attacks ................................................................. 311
  *Liron David and Avishai Wool*
Improved Key Recovery Algorithms from Noisy RSA Secret Keys
with Analog Noise .......................................................... 328

Noboru Kunihiro and Yuki Takahashi

Side-channel Analysis

Ridge-Based Profiled Differential Power Analysis .................. 347
Weijia Wang, Yu Yu, François-Xavier Standaert, Dawu Gu, Xu Sen,
and Chi Zhang

My Traces Learn What You Did in the Dark: Recovering Secret
Signals Without Key Guesses ........................................... 363
Si Gao, Hua Chen, Wenling Wu, Limin Fan, Weiqiong Cao,
and Xiangliang Ma

Cryptographic Protocols

Actively Secure 1-out-of-N OT Extension with Application to Private
Set Intersection ............................................................. 381
Michele Orrù, Emmanuela Orsini, and Peter Scholl

Low-Leakage Secure Search for Boolean Expressions ............... 397
Fernando Krell, Gabriela Ciocarlie, Ashish Gehani,
and Mariana Raykova

Public Key Algorithms

Constructions Secure Against Receiver Selective Opening
and Chosen Ciphertext Attacks ........................................... 417
Dingding Jia, Xianhui Lu, and Bao Li

New Revocable IBE in Prime-Order Groups: Adaptively Secure, Decryption
Key Exposure Resistant, and with Short Public Parameters ........... 432
Yohei Watanabe, Keita Emura, and Jae Hong Seo

Author Index ................................................................. 451
http://www.springer.com/978-3-319-52152-7

Topics in Cryptology – CT-RSA 2017
The Cryptographers’ Track at the RSA Conference 2017, San Francisco, CA, USA, February 14-17, 2017, Proceedings
Handschuh, H. (Ed.)
2017, XIII, 452 p. 78 illus., Softcover
ISBN: 978-3-319-52152-7