Contents

Encryption

A Tag Based Encoding: An Efficient Encoding for Predicate Encryption in Prime Order Groups .................................................. 3
  Jongkil Kim, Willy Susilo, Fuchun Guo, and Man Ho Au

Non-zero Inner Product Encryption with Short Ciphertexts and Private Keys ................................................................. 23
  Jie Chen, Benoît Libert, and Somindu C. Ramanna

Attribute-Based Encryption for Range Attributes .................................................. 42
  Nuttapong Attrapadung, Goichiro Hanaoka, Kazuto Ogawa, Go Ohtake, Hajime Watanabe, and Shota Yamada

Naor-Yung Paradigm with Shared Randomness and Applications .............. 62
  Silvio Biagioni, Daniel Masny, and Daniele Venturi

Memory Protection

Provably-Secure Remote Memory Attestation for Heap Overflow Protection .............................................................................. 83
  Alexandra Boldyreva, Taesoo Kim, Richard Lipton, and Bogdan Warinschi

Memory Erasability Amplification ................................................................. 104
  Jan Camenisch, Robert R. Enderlein, and Ueli Maurer

Multi-party Computation

On Adaptively Secure Multiparty Computation with a Short CRS .............. 129
  Ran Cohen and Chris Peikert

Linear Overhead Optimally-Resilient Robust MPC Using Preprocessing ..... 147
  Ashish Choudhury, Emmanuela Orsini, Arpita Patra, and Nigel P. Smart

High-Precision Secure Computation of Satellite Collision Probabilities .... 169
  Brett Hemenway, Steve Lu, Rafail Ostrovsky, and William Welser IV
Zero-Knowledge Proofs

Zero-Knowledge Made Easy so It Won’t Make You Dizzy (A Tale of Transaction Put in Verse About an Illicit Kind of Commerce) ............ 191
   Trotta Gnam

Fiat–Shamir for Highly Sound Protocols Is Instantiable ....................... 198
   Arno Mittelbach and Daniele Venturi

Verifiable Zero-Knowledge Order Queries and Updates for Fully Dynamic Lists and Trees ................................................................. 216
   Esha Ghosh, Michael T. Goodrich, Olga Ohrimenko, and Roberto Tamassia

On the Implausibility of Constant-Round Public-Coin Zero-Knowledge Proofs .......................................................... 237
   Yi Deng, Juan Garay, San Ling, Huaxiong Wang, and Moti Yung

Efficient Protocols

Improving Practical UC-Secure Commitments Based on the DDH Assumption ............................................................................. 257
   Eiichiro Fujisaki

The Whole is Less Than the Sum of Its Parts: Constructing More Efficient Lattice-Based AKEs .............................................................. 273
   Rafael del Pino, Vadim Lyubashevsky, and David Pointcheval

Efficient Asynchronous Accumulators for Distributed PKI .................. 292
   Leonid Reyzin and Sophia Yakoubov

Outsourcing Computation

The Feasibility of Outsourced Database Search in the Plain Model ....... 313
   Carmit Hazay and Hila Zarosim

Verifiable Pattern Matching on Outsourced Texts .............................. 333
   Dario Catalano, Mario Di Raimondo, and Simone Faro

Digital Signatures

Virtual Smart Cards: How to Sign with a Password and a Server .......... 353
   Jan Camenisch, Anja Lehmann, Gregory Neven, and Kai Samelin

Signatures Resilient to Uninvertible Leakage .................................... 372
   Yuyu Wang, Takahiro Matsuda, Goichiro Hanaoka, and Keisuke Tanaka
Practical Round-Optimal Blind Signatures in the Standard Model from Weaker Assumptions .......................................................... 391
Georg Fuchsbauer, Christian Hanser, Chethan Kamath, and Daniel Slamanig

Cryptanalysis
How (Not) to Instantiate Ring-LWE .................................................. 411
Chris Peikert
Pen and Paper Arguments for SIMON and SIMON-like Designs ............. 431
Christof Beierle

Two-party Computation
Bounded Size-Hiding Private Set Intersection .................................. 449
Tatiana Bradley, Sky Faber, and Gene Tsudik
On Garbling Schemes with and Without Privacy ................................ 468
Carsten Baum
What Security Can We Achieve Within 4 Rounds? ............................. 486
Carmit Hazay and Muthuramakrishnan Venkitasubramaniam

Secret Sharing
Secret Sharing Schemes for Dense Forbidden Graphs .......................... 509
Amos Beimel, Oriol Farràs, and Naty Peter
Proactive Secret Sharing with a Dishonest Majority ............................ 529
Shlomi Dolev, Karim ElDefrawy, Joshua Lampkins, Rafail Ostrovsky, and Motti Yung

Obfuscation
Shorter Circuit Obfuscation in Challenging Security Models ............... 551
Zvika Brakerski and Or Dagmi
Bounded KDM Security from iO and OWF ...................................... 571
Antonio Marcedone, Rafael Pass, and Abhi Shelat
A Unified Approach to Idealized Model Separations via Indistinguishability Obfuscation ............................................................... 587
Matthew D. Green, Jonathan Katz, Alex J. Malozemoff, and Hong-Sheng Zhou

Author Index ................................................................. 605
Security and Cryptography for Networks
10th International Conference, SCN 2016, Amalfi, Italy,
August 31 – September 2, 2016, Proceedings
Zikas, V.; De Prisco, R. (Eds.)
2016, XIX, 606 p. 75 illus., Softcover
ISBN: 978-3-319-44617-2