

Contents

Encryption

A Tag Based Encoding: An Efficient Encoding for Predicate Encryption in Prime Order Groups	3
<i>Jongkil Kim, Willy Susilo, Fuchun Guo, and Man Ho Au</i>	
Non-zero Inner Product Encryption with Short Ciphertexts and Private Keys.	23
<i>Jie Chen, Benoît Libert, and Somindu C. Ramanna</i>	
Attribute-Based Encryption for Range Attributes.	42
<i>Nuttapong Attrapadung, Goichiro Hanaoka, Kazuto Ogawa, Go Ohtake, Hajime Watanabe, and Shota Yamada</i>	
Naor-Yung Paradigm with Shared Randomness and Applications	62
<i>Silvio Biagioni, Daniel Masny, and Daniele Venturi</i>	

Memory Protection

Provably-Secure Remote Memory Attestation for Heap Overflow Protection	83
<i>Alexandra Boldyreva, Taesoo Kim, Richard Lipton, and Bogdan Warinschi</i>	
Memory Erasability Amplification.	104
<i>Jan Camenisch, Robert R. Enderlein, and Ueli Maurer</i>	

Multi-party Computation

On Adaptively Secure Multiparty Computation with a Short CRS	129
<i>Ran Cohen and Chris Peikert</i>	
Linear Overhead Optimally-Resilient Robust MPC Using Preprocessing.	147
<i>Ashish Choudhury, Emmanuela Orsini, Arpita Patra, and Nigel P. Smart</i>	
High-Precision Secure Computation of Satellite Collision Probabilities.	169
<i>Brett Hemenway, Steve Lu, Rafail Ostrovsky, and William Welser IV</i>	

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
<i>Trotta Gnam</i>	
Fiat–Shamir for Highly Sound Protocols Is Instantiable	198
<i>Arno Mittelbach and Daniele Venturi</i>	
Verifiable Zero-Knowledge Order Queries and Updates for Fully Dynamic Lists and Trees	216
<i>Esha Ghosh, Michael T. Goodrich, Olga Ohrimenko, and Roberto Tamassia</i>	
On the Implausibility of Constant-Round Public-Coin Zero-Knowledge Proofs	237
<i>Yi Deng, Juan Garay, San Ling, Huaxiong Wang, and Moti Yung</i>	

Efficient Protocols

Improving Practical UC-Secure Commitments Based on the DDH Assumption	257
<i>Eiichiro Fujisaki</i>	
The Whole is Less Than the Sum of Its Parts: Constructing More Efficient Lattice-Based AKEs	273
<i>Rafael del Pino, Vadim Lyubashevsky, and David Pointcheval</i>	
Efficient Asynchronous Accumulators for Distributed PKI	292
<i>Leonid Reyzin and Sophia Yakoubov</i>	

Outsourcing Computation

The Feasibility of Outsourced Database Search in the Plain Model	313
<i>Carmit Hazay and Hila Zarosim</i>	
Verifiable Pattern Matching on Outsourced Texts	333
<i>Dario Catalano, Mario Di Raimondo, and Simone Faro</i>	

Digital Signatures

Virtual Smart Cards: How to Sign with a Password and a Server	353
<i>Jan Camenisch, Anja Lehmann, Gregory Neven, and Kai Samelin</i>	
Signatures Resilient to Uninvertible Leakage	372
<i>Yuyu Wang, Takahiro Matsuda, Goichiro Hanaoka, and Keisuke Tanaka</i>	

Practical Round-Optimal Blind Signatures in the Standard Model from Weaker Assumptions	391
<i>Georg Fuchsbauer, Christian Hanser, Chethan Kamath, and Daniel Slamanig</i>	

Cryptanalysis

How (Not) to Instantiate Ring-LWE	411
<i>Chris Peikert</i>	
Pen and Paper Arguments for SIMON and SIMON-like Designs	431
<i>Christof Beierle</i>	

Two-party Computation

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

Secret Sharing

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

Obfuscation

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

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