

Contents – Part III

Asiacrypt 2017 Award Paper II

A Subversion-Resistant SNARK	3
<i>Behzad Abdolmaleki, Karim Bagheri, Helger Lipmaa, and Michał Zając</i>	

Cryptographic Protocols

Two-Round PAKE from Approximate SPH and Instantiations from Lattices	37
<i>Jiang Zhang and Yu Yu</i>	
Tightly-Secure Signatures from Five-Move Identification Protocols	68
<i>Eike Kiltz, Julian Loss, and Jiaxin Pan</i>	
On the Untapped Potential of Encoding Predicates by Arithmetic Circuits and Their Applications.	95
<i>Shuichi Katsumata</i>	
The Minimum Number of Cards in Practical Card-Based Protocols	126
<i>Julia Kastner, Alexander Koch, Stefan Walzer, Daiki Miyahara, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone</i>	

Foundations

Succinct Spooky Free Compilers Are Not Black Box Sound	159
<i>Zvika Brakerski, Yael Tauman Kalai, and Renen Perlman</i>	
Non-Interactive Multiparty Computation Without Correlated Randomness . . .	181
<i>Shai Halevi, Yuval Ishai, Abhishek Jain, Ilan Komargodski, Amit Sahai, and Eylon Yogev</i>	
Optimal-Rate Non-Committing Encryption	212
<i>Ran Canetti, Oxana Poburinnaya, and Mariana Raykova</i>	
Preventing CLT Attacks on Obfuscation with Linear Overhead.	242
<i>Rex Fernando, Peter M. R. Rasmussen, and Amit Sahai</i>	

Zero-Knowledge Proofs

Two-Message Witness Indistinguishability and Secure Computation in the Plain Model from New Assumptions	275
<i>Saikrishna Badrinarayanan, Sanjam Garg, Yuval Ishai, Amit Sahai, and Akshay Wadia</i>	

Zero-Knowledge Arguments for Lattice-Based PRFs and Applications to E-Cash.	304
<i>Benoît Libert, San Ling, Khoa Nguyen, and Huaxiong Wang</i>	
Linear-Time Zero-Knowledge Proofs for Arithmetic Circuit Satisfiability	336
<i>Jonathan Bootle, Andrea Cerulli, Essam Ghadafi, Jens Groth, Mohammad Hajiabadi, and Sune K. Jakobsen</i>	
Symmetric Key Designs	
How to Use Metaheuristics for Design of Symmetric-Key Primitives.	369
<i>Ivica Nikolić</i>	
Cycle Slicer: An Algorithm for Building Permutations on Special Domains.	392
<i>Sarah Miracle and Scott Yilek</i>	
Symmetrically and Asymmetrically Hard Cryptography	417
<i>Alex Biryukov and Léo Perrin</i>	
Blockcipher-Based MACs: Beyond the Birthday Bound Without Message Length	446
<i>Yusuke Naito</i>	
Author Index	471

Advances in Cryptology – ASIACRYPT 2017
23rd International Conference on the Theory and
Applications of Cryptology and Information Security,
Hong Kong, China, December 3–7, 2017, Proceedings,
Part III

Takagi, T.; Peyrin, Th. (Eds.)

2017, XVIII, 473 p. 69 illus., 10 illus. in color., Softcover

ISBN: 978-3-319-70699-3