

Table of Contents

Public-Key Cryptanalysis

A Heuristic Quasi-Polynomial Algorithm for Discrete Logarithm in Finite Fields of Small Characteristic	1
<i>Razvan Barbulescu, Pierrick Gaudry, Antoine Joux, and Emmanuel Thomé</i>	
Polynomial Time Attack on Wild McEliece over Quadratic Extensions	17
<i>Alain Couvreur, Ayoub Otmani, and Jean-Pierre Tillich</i>	
Symmetrized Summation Polynomials: Using Small Order Torsion Points to Speed Up Elliptic Curve Index Calculus	40
<i>Jean-Charles Faugère, Louise Huot, Antoine Joux, Guénaél Renault, and Vanessa Vitse</i>	

Identity-Based Encryption

Why Proving HIBE Systems Secure Is Difficult	58
<i>Allison Lewko and Brent Waters</i>	
Identity-Based Encryption Secure against Selective Opening Chosen-Ciphertext Attack	77
<i>Junzuo Lai, Robert H. Deng, Shengli Liu, Jian Weng, and Yunlei Zhao</i>	

Key Derivation and Quantum Computing

Key Derivation without Entropy Waste	93
<i>Yevgeniy Dodis, Krzysztof Pietrzak, and Daniel Wichs</i>	
Efficient Non-malleable Codes and Key-Derivation for Poly-size Tampering Circuits	111
<i>Sebastian Faust, Pratyay Mukherjee, Daniele Venturi, and Daniel Wichs</i>	
Revocable Quantum Timed-Release Encryption	129
<i>Dominique Unruh</i>	

Secret-Key Analysis and Implementations

Generic Universal Forgery Attack on Iterative Hash-Based MACs	147
<i>Thomas Peyrin and Lei Wang</i>	

Links between Truncated Differential and Multidimensional Linear Properties of Block Ciphers and Underlying Attack Complexities	165
<i>Céline Blondeau and Kaisa Nyberg</i>	

Faster Compact Diffie–Hellman: Endomorphisms on the x -Line	183
<i>Craig Costello, Huseyin Hisil, and Benjamin Smith</i>	

Obfuscation and Multilinear Maps

Replacing a Random Oracle: Full Domain Hash from Indistinguishability Obfuscation	201
<i>Susan Hohenberger, Amit Sahai, and Brent Waters</i>	

Protecting Obfuscation against Algebraic Attacks	221
<i>Boaz Barak, Sanjam Garg, Yael Tauman Kalai, Omer Paneth, and Amit Sahai</i>	

GGHlite: More Efficient Multilinear Maps from Ideal Lattices	239
<i>Adeline Langlois, Damien Stehlé, and Ron Steinfeld</i>	

Authenticated Encryption

Reconsidering Generic Composition	257
<i>Chanathip Namprempre, Phillip Rogaway, and Thomas Shrimpton</i>	

Parallelizable Rate-1 Authenticated Encryption from Pseudorandom Functions	275
<i>Kazuhiko Minematsu</i>	

Symmetric Encryption

Honey Encryption: Security Beyond the Brute-Force Bound	293
<i>Ari Juels and Thomas Ristenpart</i>	

Sometimes-Recurse Shuffle: Almost-Random Permutations in Logarithmic Expected Time	311
<i>Ben Morris and Phillip Rogaway</i>	

Tight Security Bounds for Key-Alternating Ciphers	327
<i>Shan Chen and John Steinberger</i>	

The Locality of Searchable Symmetric Encryption	351
<i>David Cash and Stefano Tessaro</i>	

Multi-party Computation

A Bound for Multiparty Secret Key Agreement and Implications for a Problem of Secure Computing	369
<i>Himanshu Tyagi and Shun Watanabe</i>	
Non-Interactive Secure Computation Based on Cut-and-Choose	387
<i>Arash Afshar, Payman Mohassel, Benny Pinkas, and Ben Riva</i>	
Garbled RAM Revisited	405
<i>Craig Gentry, Shai Halevi, Steve Lu, Rafail Ostrovsky, Mariana Raykova, and Daniel Wichs</i>	

Side-Channel Attacks

Unifying Leakage Models: From Probing Attacks to Noisy Leakage	423
<i>Alexandre Duc, Stefan Dziembowski, and Sebastian Faust</i>	
Higher Order Masking of Look-Up Tables	441
<i>Jean-Sébastien Coron</i>	
How to Certify the Leakage of a Chip?	459
<i>François Durvaux, François-Xavier Standaert, and Nicolas Veyrat-Charvillon</i>	

Signatures and Public-Key Encryption

Efficient Round Optimal Blind Signatures	477
<i>Sanjam Garg and Divya Gupta</i>	
Key-Versatile Signatures and Applications: RKA, KDM and Joint Enc/Sig	496
<i>Mihir Bellare, Sarah Meiklejohn, and Susan Thomson</i>	
Non-malleability from Malleability: Simulation-Sound Quasi-Adaptive NIZK Proofs and CCA2-Secure Encryption from Homomorphic Signatures	514
<i>Benoît Libert, Thomas Peters, Marc Joye, and Moti Yung</i>	

Functional Encryption

Fully Key-Homomorphic Encryption, Arithmetic Circuit ABE and Compact Garbled Circuits	533
<i>Dan Boneh, Craig Gentry, Sergey Gorbunov, Shai Halevi, Valeria Nikolaenko, Gil Segev, Vinod Vaikuntanathan, and Dhinakaran Vinayagamurthy</i>	

Dual System Encryption via Doubly Selective Security: Framework, Fully Secure Functional Encryption for Regular Languages, and More	557
<i>Nuttapong Attrapadung</i>	

Multi-input Functional Encryption	578
<i>Shafi Goldwasser, S. Dov Gordon, Vipul Goyal, Abhishek Jain, Jonathan Katz, Feng-Hao Liu, Amit Sahai, Elaine Shi, and Hong-Sheng Zhou</i>	

Foundations

Salvaging Indifferentiability in a Multi-stage Setting	603
<i>Arno Mittelbach</i>	
Déjà Q: Using Dual Systems to Revisit q -Type Assumptions	622
<i>Melissa Chase and Sarah Meiklejohn</i>	
Distributed Point Functions and Their Applications	640
<i>Niv Gilboa and Yuval Ishai</i>	

Multi-party Computation

A Full Characterization of Completeness for Two-Party Randomized Function Evaluation	659
<i>Daniel Kraschewski, Hemanta K. Maji, Manoj Prabhakaran, and Amit Sahai</i>	
On the Complexity of UC Commitments	677
<i>Juan A. Garay, Yuval Ishai, Ranjit Kumaresan, and Hoeteck Wee</i>	
Universally Composable Symbolic Analysis for Two-Party Protocols Based on Homomorphic Encryption	695
<i>Morten Dahl and Ivan Damgård</i>	

Author Index	713
------------------------	-----