Table of Contents

Invited Talks

Pairing-Based Cryptography: Past, Present, and Future 1
Dan Boneh

Some Mathematical Mysteries in Lattices 2
Chuanming Zong

Public-Key Cryptography I

Constant-Size Structure-Preserving Signatures: Generic Constructions and Simple Assumptions 4
Masayuki Abe, Melissa Chase, Bernardo David, Markulf Kohlweiss, Ryo Nishimaki, and Miyako Ohkubo

Dual Form Signatures: An Approach for Proving Security from Static Assumptions 25
Michael Gerbush, Allison Lewko, Adam O'Neill, and Brent Waters

Breaking Pairing-Based Cryptosystems Using η_T Pairing over $GF(3^{97})$ 43
Takuya Hayashi, Takeshi Shimoyama, Naoyuki Shinohara, and Tsuyoshi Takagi

On the (Im)possibility of Projecting Property in Prime-Order Setting . . . 61
Jae Hong Seo

Foundation

Optimal Reductions of Some Decisional Problems to the Rank Problem 80
Jorge Luis Villar

Signature Schemes Secure against Hard-to-Invert Leakage 98
Sebastian Faust, Carmit Hazay, Jesper Buus Nielsen, Peter Sebastian Nordholt, and Angela Zottarel

Completeness for Symmetric Two-Party Functionalities - Revisited 116
Yehuda Lindell, Eran Omri, and Hila Zarosim

Adaptively Secure Garbling with Applications to One-Time Programs and Secure Outsourcing 134
Mihir Bellare, Viet Tung Hoang, and Phillip Rogaway

The Generalized Randomized Iterate and Its Application to New Efficient Constructions of UOWHFs from Regular One-Way Functions 154
Scott Ames, Rosario Gennaro, and Muthuramakrishnan Venkitasubramaniam

Symmetric Cipher

Perfect Algebraic Immune Functions 172
Meicheng Liu, Yin Zhang, and Dongdai Lin

Differential Analysis of the LED Block Cipher 190
Florian Mendel, Vincent Rijmen, Deniz Toz, and Kerem Varıcı

PRINCE – A Low-Latency Block Cipher for Pervasive Computing Applications: Extended Abstract 208
Julia Borghoff, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knezevic, Lars R. Knudsen, Gregor Leander, Ventzislav Nikov, Christof Paar, Christian Rechberger, Peter Rombouts, Søren S. Thomsen, and Tolga Yalçın

Analysis of Differential Attacks in ARX Constructions 226
Gaëtan Leurent

Integral and Multidimensional Linear Distinguishers with Correlation Zero 244
Andrey Bogdanov, Gregor Leander, Kaisa Nyberg, and Meiqin Wang

Differential Attacks against Stream Cipher ZUC 262
Hongjun Wu, Tao Huang, Phuong Ha Nguyen, Huaxiong Wang, and San Ling

Security Proof

An Asymptotically Tight Security Analysis of the Iterated Even-Mansour Cipher 278
Rodolphe Lampe, Jacques Patarin, and Yannick Seurin

3kf9: Enhancing 3GPP-MAC beyond the Birthday Bound 296
Liting Zhang, Wenling Wu, Han Sui, and Peng Wang

Understanding Adaptivity: Random Systems Revisited 313
Dimitar Jetchev, Onur Özen, and Martijn Stam

RKA Security beyond the Linear Barrier: IBE, Encryption and Signatures 331
Mihir Bellare, Kenneth G. Paterson, and Susan Thomson

Public-Key Cryptography II

Fully Secure Unbounded Inner-Product and Attribute-Based Encryption 349
Tatsuaki Okamoto and Katsuyuki Takashima

Computing on Authenticated Data: New Privacy Definitions and Constructions 367
Nuttapong Attrapadung, Benoît Libert, and Thomas Peters

A Coding-Theoretic Approach to Recovering Noisy RSA Keys 386
Kenneth G. Paterson, Antigoni Polychroniadou, and Dale L. Sibborn

Certifying RSA 404
Saqib A. Kakvi, Eike Kiltz, and Alexander May

Lattice-Based Cryptography and Number Theory

Faster Gaussian Lattice Sampling Using Lazy Floating-Point Arithmetic 415
Léo Ducas and Phong Q. Nguyen

Learning a Zonotope and More: Cryptanalysis of NTRUSign Countermeasures 433
Léo Ducas and Phong Q. Nguyen

On Polynomial Systems Arising from a Weil Descent 451
Christophe Petit and Jean-Jacques Quisquater

Public-Key Cryptography III

ECM at Work 467
Joppe W. Bos and Thorsten Kleinjung

IND-CCA Secure Cryptography Based on a Variant of the LPN Problem 485
Nico Döttling, Jörn Müller-Quade, and Anderson C.A. Nascimento

Hash Function

Provable Security of the Knudsen-Preneel Compression Functions 504
Jooyoung Lee

Optimal Collision Security in Double Block Length Hashing with Single Length Key 526
Bart Mennink

Bicliques for Permutations: Collision and Preimage Attacks in Stronger Settings 544
Dmitry Khovratovich

Investigating Fundamental Security Requirements on Whirlpool: Improved Preimage and Collision Attacks 562
Yu Sasaki, Lei Wang, Shuang Wu, and Wenling Wu

Generic Related-Key Attacks for HMAC 580
Thomas Peyrin, Yu Sasaki, and Lei Wang

Cryptographic Protocol I

The Five-Card Trick Can Be Done with Four Cards 598
Takaaki Mizuki, Michihito Kumamoto, and Hideaki Sone

A Mix-Net from Any CCA2 Secure Cryptosystem 607
Shahram Khazaei, Tal Moran, and Douglas Wikström

How Not to Prove Yourself: Pitfalls of the Fiat-Shamir Heuristic and Applications to Helios 626
David Bernhard, Olivier Pereira, and Bogdan Warinschi

Cryptographic Protocol II

Sequential Aggregate Signatures with Lazy Verification from Trapdoor Permutations (Extended Abstract) 644
Kyle Brogle, Sharon Goldberg, and Leonid Reyzin

Commitments and Efficient Zero-Knowledge Proofs from Learning Parity with Noise 663
Abhishek Jain, Stephan Krenn, Krzysztof Pietrzak, and Aris Tentes

Calling Out Cheaters: Covert Security with Public Verifiability 681
Gilad Asharov and Claudio Orlandi

A Unified Framework for UC from Only OT 699
Rafael Pass, Huijia Lin, and Muthuramakrishnan Venkitasubramaniam

Implementation Issues

Four-Dimensional Gallant-Lambert-Vanstone Scalar Multiplication 718
Patrick Longa and Francesco Sica

Shuffling against Side-Channel Attacks: A Comprehensive Study with Cautionary Note 740
Nicolas Veyrat-Charvillon, Marcel Medwed, Stéphanie Kerckhof, and François-Xavier Standaert

Theory and Practice of a Leakage Resilient Masking Scheme 758
Josep Balasch, Sebastian Faust, Benedikt Gierlichs, and Ingrid Verbauwhede

Author Index 777