Contents

Public-Key Encryption

Simulation-Based Selective Opening CCA Security for PKE from Key Encapsulation Mechanisms . . . 3
Shengli Liu and Kenneth G. Paterson

On the Selective Opening Security of Practical Public-Key Encryption Schemes . . . 27
Felix Heuer, Tibor Jager, Eike Kiltz, and Sven Schäge

How Secure is Deterministic Encryption? . . . 52
Mihir Bellare, Rafael Dowsley, and Sriram Keelveedhi

E-Cash

Divisible E-Cash Made Practical . . . 77
Sébastien Canard, David Pointcheval, Olivier Sanders, and Jacques Traoré

Anonymous Transferable E-Cash . . . 101
Foteini Baldimtsi, Melissa Chase, Georg Fuchsbauer, and Markulf Kohlweiss

Cryptanalysis

Collision of Random Walks and a Refined Analysis of Attacks on the Discrete Logarithm Problem. . . . 127
Shuji Kijima and Ravi Montenegro

A Polynomial-Time Key-Recovery Attack on MQQ Cryptosystems . . . 150
Jean-Charles Faugère, Danilo Gligoroski, Ludovic Perret, Simona Samardjiska, and Enrico Thomae

A Polynomial-Time Attack on the BBCRS Scheme . . . 175
Alain Couvreur, Ayoub Otmani, Jean-Pierre Tillich, and Valérie Gauthier–Umaña

Algebraic Cryptanalysis of a Quantum Money Scheme: The Noise-Free Case. . . 194
Marta Conde Pena, Jean-Charles Faugère, and Ludovic Perret

Bibliografische Informationen
http://d-nb.info/1065469837

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

Digital Signatures I

Digital Signatures from Strong RSA without Prime Generation 217
David Cash, Rafael Dowsley, and Eike Kiltz

Short Signatures with Short Public Keys from Homomorphic Trapdoor Functions 236
Jacob Alperin-Sheriff

Tightly-Secure Signatures from Chameleon Hash Functions 256
Olivier Blazy, Saqib A. Kakvi, Eike Kiltz, and Jiaxin Pan

Password-Based Authentication

Two-Server Password-Authenticated Secret Sharing UC-Secure Against Transient Corruptions 283
Jan Camenisch, Robert R. Enderlein, and Gregory Neven

Adaptive Witness Encryption and Asymmetric Password-Based Cryptography 308
Mihir Bellare and Viet Tung Hoang

Public-Key Encryption Indistinguishable Under Plaintext-Checkable Attacks . . . 332
Michel Abdalla, Fabrice Benhamouda, and David Pointcheval

Pairing-Based Cryptography

Strongly-Optimal Structure Preserving Signatures from Type II Pairings: Synthesis and Lower Bounds 355
Gilles Barthe, Edvard Fagerholm, Dario Fiore, Andre Scedrov, Benedikt Schmidt, and Mehdi Tibouchi

A Profitable Sub-prime Loan: Obtaining the Advantages of Composite Order in Prime-Order Bilinear Groups 377
Allison Lewko and Sarah Meiklejohn

Digital Signatures II

Simpler Efficient Group Signatures from Lattices 401
Phong Q. Nguyen, Jiang Zhang, and Zhenfeng Zhang

Group Signatures from Lattices: Simpler, Tighter, Shorter, Ring-Based 427
San Ling, Khoa Nguyen, and Huaxiong Wang

Secure Efficient History-Hiding Append-Only Signatures in the Standard Model 450
Benoît Libert, Marc Joye, Moti Yung, and Thomas Peters

Efficient Constructions

One-Round Key Exchange with Strong Security: An Efficient and Generic Construction in the Standard Model 477
Florian Bergsma, Tibor Jager, and Jörg Schwenk

Additively Homomorphic UC Commitments with Optimal Amortized Overhead 495
Ignacio Cascudo, Ivan Damgård, Bernardo David, Irene Giacomelli, Jesper Buus Nielsen, and Roberto Trifiletti

Interactive Message-Locked Encryption and Secure Deduplication 516
Mihir Bellare and Sriram Keelveedhi

Faster ECC over $\mathbb{F}_{2^{521}-1}$ 539
Robert Granger and Michael Scott

Cryptography with Imperfect Keys

Continuous Non-malleable Key Derivation and Its Application to Related-Key Security 557
Baodong Qin, Shengli Liu, Tsz Hon Yuen, Robert H. Deng, and Kefei Chen

A Tamper and Leakage Resilient von Neumann Architecture 579
Sebastian Faust, Pratyay Mukherjee, Jesper Buus Nielsen, and Daniele Venturi

Low Noise LPN: KDM Secure Public Key Encryption and Sample Amplification 604
Nico Döttling

Interactive Proofs

Adaptive Proofs of Knowledge in the Random Oracle Model 629
David Bernhard, Marc Fischlin, and Bogdan Warinschi

Making Sigma-Protocols Non-interactive Without Random Oracles 650
Pyrros Chaidos and Jens Groth

Lattice-Based Cryptography

Bootstrapping BGV Ciphertexts with a Wider Choice of p and q 673
Emmanuela Orsini, Joop van de Pol, and Nigel P. Smart

Packing Messages and Optimizing Bootstrapping in GSW-FHE 699
Ryo Hiromasa, Masayuki Abe, and Tatsuaki Okamoto

Simple Lattice Trapdoor Sampling from a Broad Class of Distributions 716
Vadim Lyubashevsky and Daniel Wichs

Identity-Based, Predicate, and Functional Encryption

Simple Functional Encryption Schemes for Inner Products 733
Michel Abdalla, Florian Bourse, Angelo De Caro, and David Pointcheval

Predicate Encryption for Multi-Dimensional Range Queries from Lattices. . . 752
Romain Gay, Pierrick Méaux, and Hoeteck Wee

On the Practical Security of Inner Product Functional Encryption. 777
Shashank Agrawal, Shweta Agrawal, Saikrishna Badrinarayanan, Abishek Kumarasubramanian, Manoj Prabhakaran, and Amit Sahai

Identity-Based Encryption with (almost) Tight Security in the Multi-instance, Multi-ciphertext Setting 799
Dennis Hofheinz, Jessica Koch, and Christoph Striecks

Author Index 823