Table of Contents

Homomorphic Encryption and LWE

Better Bootstrapping in Fully Homomorphic Encryption 1
Craig Gentry, Shai Halevi, and Nigel P. Smart

Polly Cracker, Revisited, Revisited 17
Gottfried Herold

Ring-LWE in Polynomial Rings 34
Léo Ducas and Alain Durmus

On Homomorphic Encryption and Chosen-Ciphertext Security 52
Brett Hemenway and Rafail Ostrovsky

Signature Schemes

Waters Signatures with Optimal Security Reduction 66
Dennis Hofheinz, Tibor Jager, and Edward Knapp

Strong Security from Probabilistic Signature Schemes 84
Sven Schäge

Space Efficient Signature Schemes from the RSA Assumption 102
Shota Yamada, Goichiro Hanaoka, and Noboru Kunihiro

The Construction of Ambiguous Optimistic Fair Exchange from Designated Confirmer Signature without Random Oracles 120
Qiong Huang, Duncan S. Wong, and Willy Susilo

Code-Based and Multivariate Crypto

Efficient Implementation of a CCA2-Secure Variant of McEliece Using Generalized Srivastava Codes 138
Pierre-Louis Cayrel, Gerhard Hoffmann, and Edoardo Persichetti

Solving Underdetermined Systems of Multivariate Quadratic Equations Revisited 156
Enrico Thomae and Christopher Wolf

Public-Key Identification Schemes Based on Multivariate Cubic Polynomials 172
Koichi Sakumoto

Bibliografische Informationen
http://d-nb.info/1021598607

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

Public-Key Cryptography from New Multivariate Quadratic Assumptions 190
Yun-Ju Huang, Feng-Hao Liu, and Bo-Yin Yang

Public-Key Encryption: Special Properties

Anonymous Broadcast Encryption: Adaptive Security and Efficient Constructions in the Standard Model 206
Benoît Libert, Kenneth G. Paterson, and Elizabeth A. Quaglia

Outsider-Anonymous Broadcast Encryption with Sublinear Ciphertexts 225
Nelly Fazio and Irippuge Milinda Perera

Verifiable Predicate Encryption and Applications to CCA Security and Anonymous Predicate Authentication 243
Shota Yamada, Nuttapong Attrapadung, Bagus Santoso, Jacob C.N. Schuldt, Goichiro Hanaoka, and Noboru Kunihiro

Public Key Encryption against Related Key Attacks 262
Hoeteck Wee

Identity-Based Encryption

Functional Encryption for Threshold Functions (or Fuzzy IBE) from Lattices 280
Shweta Agrawal, Xavier Boyen, Vinod Vaikuntanathan, Panagiotis Voulgaris, and Hoeteck Wee

Variants of Waters' Dual System Primitives Using Asymmetric Pairings (Extended Abstract) 298
Somindu C. Ramanna, Sanjit Chatterjee, and Palash Sarkar

From Selective to Full Security: Semi-generic Transformations in the Standard Model 316
Michel Abdalla, Dario Fiore, and Vadim Lyubashevsky

Circular and KDM Security for Identity-Based Encryption 334
Jacob Alperin-Sheriff and Chris Peikert

Public-Key Encryption: Constructions

`NTRUCCA`: How to Strengthen `NTRUEncrypt` to Chosen-Ciphertext Security in the Standard Model 353
Ron Steinfeld, San Ling, Josef Pieprzyk, Christophe Tartary, and Huaxiong Wang

Generating Provable Primes Efficiently on Embedded Devices 372
Christophe Clavier, Benoit Feix, Loïc Thierry, and Pascal Paillier

Invited Talk

Password-Based Authenticated Key Exchange 390
David Pointcheval

Secure Two-Party and Multi-party Computations

Constant-Round Multi-party Private Set Union Using Reversed Laurent Series 398
Jae Hong Seo, Jung Hee Cheon, and Jonathan Katz

Policy-Enhanced Private Set Intersection: Sharing Information While Enforcing Privacy Policies 413
Emil Stefanov, Elaine Shi, and Dawn Song

Efficiently Shuffling in Public 431
Udaya Parampalli, Kim Ramchen, and Vanessa Teague

Key Exchange and Secure Sessions

Efficient Password Authenticated Key Exchange via Oblivious Transfer 449
Ran Canetti, Dana Dachman-Soled, Vinod Vaikuntanathan, and Hoeteck Wee

Strongly Secure Authenticated Key Exchange from Factoring, Codes, and Lattices 467
Atsushi Fujioka, Koutarou Suzuki, Keita Xagawa, and Kazuki Yoneyama

Relatively-Sound NIZKs and Password-Based Key-Exchange 485
Charanjit Jutla and Arnab Roy

Multi-location Leakage Resilient Cryptography 504
Ali Juma, Yevgeniy Vahlis, and Moti Yung

Public-Key Encryption: Relationships

On Definitions of Selective Opening Security 522
Florian Böhl, Dennis Hofheinz, and Daniel Kraschewski

New Definitions and Separations for Circular Security 540
David Cash, Matthew Green, and Susan Hohenberger

Correlated Product Security from Any One-Way Function 558
Brett Hemenway, Steve Lu, and Rafail Ostrovsky

Relations between Constrained and Bounded Chosen Ciphertext Security for Key Encapsulation Mechanisms 576
Takahiro Matsuda, Goichiro Hanaoka, and Kanta Matsuura

DL, DDH, and More Number Theory

Solving a Discrete Logarithm Problem with Auxiliary Input on a 160-Bit Elliptic Curve 595
Yumi Sakemi, Goichiro Hanaoka, Tetsuya Izu, Masahiko Takenaka, and Masaya Yasuda

Inferring Sequences Produced by Nonlinear Pseudorandom Number Generators Using Coppersmith's Methods 609
Aurélie Bauer, Damien Vergnaud, and Jean-Christophe Zapalowicz

Extended-DDH and Lossy Trapdoor Functions 627
Brett Hemenway and Rafail Ostrovsky

DDH-Like Assumptions Based on Extension Rings 644
Ronald Cramer, Ivan Damgård, Eike Kiltz, Sarah Zakarias, and Angela Zottarel

Beyond Ordinary Signature Schemes

Security of Blind Signatures Revisited 662
Dominique Schröder and Dominique Unruh

Efficient Network Coding Signatures in the Standard Model 680
Dario Catalano, Dario Fiore, and Bogdan Warinschi

Improved Security for Linearly Homomorphic Signatures: A Generic Framework 697
David Mandell Freeman

On the Security of Dynamic Group Signatures: Preventing Signature Hijacking 715
Yusuke Sakai, Jacob C.N. Schuldt, Keita Emura, Goichiro Hanaoka, and Kazuo Ohta

Author Index 733