1. Record Nr. UNINA9910855386003321

Titolo	Advances in Cryptology – EUROCRYPT 2024 : 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zurich, Switzerland, May 26–30, 2024, Proceedings, Part VII / / edited by Marc Joye, Gregor Leander
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2024
ISBN	9783031587542 3031587545
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (394 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14657
Disciplina	005.8
Soggetti	Cryptography Data encryption (Computer science) Data protection Computer networks - Security measures Computer networks Information technology - Management Cryptology Security Services Mobile and Network Security Computer Communication Networks Computer Application in Administrative Data Processing
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Intro -- Preface -- Organization -- Contents - Part VII -- Classic Public Key Cryptography (II/II) -- Practical Attack on All Parameters of the DME Signature Scheme -- 1 Introduction -- 2 Notation -- 3 Concise Description of DME -- 4 Structure of DME over Fq2 -- 4.1 Stability by q-Powering -- 4.2 Multi-hamming Weight -- 4.3 Monomial Content over Fq2 -- 5 Algebraic Attack on DME -- 5.1 Using the Big Field Representation -- 5.2 Finding the Monomial Content of the Last Round Input -- 5.3 Finding the Unknown Coefficients -- 5.4 Complexity of Solving Specialized Modeling 1 -- 5.5 Completing an Equivalent Round

Function -- 6 Experimental Results -- A Proof of Lemma 1 -- B Gröbner Bases for Specialized Modeling 1 -- References -- Signatures with Memory-Tight Security in the Quantum Random Oracle Model -- 1 Introduction -- 1.1 Contributions -- 1.2 Organization -- 2 Preliminaries -- 2.1 Lemmas on Quantum Computations -- 2.2 Adversaries with Access to Random Functions -- 2.3 Lossy Identification -- 3 Digital Signature -- 3.1 From CMA1 Security to CMA Security -- 3.2 Signature from Lossy Identification -- 4 Multi-challenge Security of Signature from Lossy Identification -- 4.1 Proof of Theorem -- 5 Plus-One Unforgeability of Signature from Lossy Identification -- 5.1 Proof of Theorem -- References -- Key Exchange with Tight (Full) Forward Secrecy via Key Confirmation -- 1 Introduction -- 1.1 Our Contribution I: Tight Forward Secrecy via Key Confirmation -- 1.2 Our Contribution II: Forward Secrecy via Key Confirmation in the QROM -- 2 Preliminaries -- 3 Three-Message Authenticated Key Exchange -- 4 Verifiable Authenticated Key Exchange -- 5 AKE with Key Confirmation -- 6 Applying Our Results to Existing Protocols -- 6.1 AKE from KEMs -- 6.2 The CCGJJ Protocol and Its Isogeny-Based Variant -- 7 KEM-Based AKE with Key Confirmation in the QROM -- References.
SLAP: Succinct Lattice-Based Polynomial Commitments from Standard Assumptions -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Works -- 1.3 Technical Overview -- 2 Preliminaries -- 3 Power-Ring-BASIS Assumption -- 3.1 h-PRISIS Assumption for =2 -- 3.2 h-PRISIS Assumption for =O(1) -- 4 Merkle-PRISIS Commitment Scheme -- 4.1 Security Analysis -- 5 Proof of Polynomial Evaluation -- 5.1 Compressed -Protocol -- 5.2 Succinct Arguments via Recursion -- 5.3 Succinct Polynomial Commitment Scheme -- References -- Universal Composable Password Authenticated Key Exchange for the Post-Quantum World -- 1 Introduction -- 2 Preliminaries -- 2.1 Hardness Assumptions -- 2.2 UC Framework for PAKE -- 2.3 ROM vs. QROM -- 3 PAKE from Basic LPKE in ROM -- 3.1 Basic Lossy Public Key Encryption (LPKE) -- 3.2 Construction of PAKE from Basic LPKE in ROM -- 4 PAKE from Extractable LPKE in QROM -- 4.1 Definition of Extractable LPKE (eLPKE) -- 4.2 Construction of eLPKE from LPKE+ -- 4.3 Construction of PAKE from eLPKE in QROM -- 5 Instantiations -- 5.1 LPKE and LPKE+ Schemes from LWE -- 5.2 LPKE and LPKE+ Scheme from Group Actions -- 5.3 Instantiations of PAKE -- References -- Asymptotics and Improvements of Sieving for Codes -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Technical Overview -- 2 Preliminaries -- 3 The Information Set Decoding (ISD) Framework -- 4 Nearest Neighbor Search in the Hamming Metric -- 4.1 LSF via Coded Hashing -- 4.2 LSF via Random Product Codes -- 5 Results and Performance Comparisons -- 5.1 Performance of Nearest Neighbor Algorithms -- 5.2 Performance of SievingISD Instantiations -- References -- Isogeny Problems with Level Structure -- 1 Introduction -- 2 Level Structures -- 3 Modular Isogeny Problems -- 4 A Reduction -- 5 -SIDH Problems in the Wild -- 5.1 The Generic Isogeny Problem -- 5.2 The SIDH Problem -- 5.3 M-SIDH.
5.4 Unipotent SIDH a.k.a. SIDH1 -- 5.5 Borel SIDH a.k.a. SIDH0 -- 5.6 Diagonal SIDH -- 6 Conclusion -- References -- Key Recovery Attack on the Partial Vandermonde Knapsack Problem -- 1 Introduction -- 2 Preliminaries -- 2.1 Notations -- 2.2 The PV Knapsack Problem -- 2.3 Lattice Reduction -- 3 Previous Attacks -- 3.1 Direct Primal Attack ch8DBLP:confspsacnsspsHoffsteinPSSW14 -- 3.2 Dual Attack ch8DBLP:confspscryptospsBoudgoustGP22 -- 4 Our Contribution -- 5 Proposed Attack -- 5.1 Analysis of the New Attack -- 6 Experimental Results -- 6.1 PASSRS Signature from ch8DBLP:confspsacnsspsHoffsteinPSSW14 -- 6.2 Signature Scheme from ch8DBLP:confspsacispspsLuZA18 -- 6.3

PASS Encrypt, PV Regev Encrypt Schemes from ch8DBLP: journalsspsdccspsBoudgoustSS22 -- 7 Symmetries of Higher Order -- References -- Cryptanalysis of Rank-2 Module-LIP in Totally Real Number Fields -- 1 Introduction -- 2 Preliminaries -- 2.1 Lattices -- 2.2 Number Fields -- 2.3 Algorithmic Considerations -- 3 Definition of Module-LIP -- 3.1 Pseudo-Gram Matrices -- 3.2 Module-LIP -- 4 An Algorithm for Module-LIP in Rank 2 over Totally Real Fields -- 4.1 Gram Ideal -- 4.2 The Assumption -- 4.3 The Algorithm -- 5 Implementation of the Algorithm -- References -- Provable Dual Attacks on Learning with Errors -- 1 Introduction -- 1.1 Contributions -- 1.2 Comparison with ch10DP23's Contradictory Regime -- 1.3 Organisation of the Paper -- 2 Preliminaries -- 2.1 LWE -- 2.2 Discrete Gaussian Distribution -- 2.3 Lattices -- 2.4 Short Vector Sampling -- 3 Basic Dual Attack -- 4 Modern Dual Attack -- 4.1 Intuition -- 4.2 Formal Analysis -- 4.3 Informal Application -- 4.4 Complexity Estimates -- 5 Quantum Dual Attack -- 5.1 Algorithm and Analysis -- 5.2 Applications -- 6 Comparison with ch10DP23's Contradictory Regime -- 6.1 Almost Complementary Regimes -- 6.2 On the Distribution of Targets.
7 Open Questions -- References -- Reduction from Sparse LPN to LPN, Dual Attack 3.0 -- 1 Introduction -- 1.1 Background -- 1.2 Our Contribution -- 2 Notation and Coding Theory Background -- 3 Reduction from Sparse to Plain LPN -- 3.1 The Approach -- 3.2 Estimating the New Noise -- 4 The double-RLPN Algorithm -- 5 Estimating the Number of False Candidates -- 5.1 Main Duality Tool -- 5.2 Intuition on How This Formula Allows to Estimate | S | -- 5.3 Main Proposition -- 6 Experimental Evidence for Our Analysis -- 7 Instantiating the Auxiliary Code with an Efficient Decoder -- 8 Links with Dual Attacks in Lattice Based Cryptography -- References -- Plover: Masking-Friendly Hash-and-Sign Lattice Signatures -- 1 Introduction -- 1.1 Our Solution -- 1.2 Technical Overview -- 2 Preliminaries -- 2.1 Notations -- 2.2 Distributions -- 2.3 Hardness Assumptions -- 2.4 Masking -- 2.5 Probing Model -- 3 Plover-RLWE : Our RLWE-Based Maskable Signature -- 3.1 Description of Unmasked Plover-RLWE -- 3.2 EUF-CMA Security of Unmasked Plover-RLWE -- 3.3 Description of Masked Plover-RLWE -- 3.4 Security of Masked Plover-RLWE -- 3.5 Cryptanalysis and Parameter Selection -- 3.6 Implementation -- References -- Updatable Public-Key Encryption, Revisited -- 1 Introduction -- 2 Preliminaries -- 3 Updatable Key Encapsulation (UKEM) -- 3.1 Functionality -- 3.2 Security -- 4 Construction -- 5 Security of the Construction -- 5.1 Member Security -- 5.2 Joiner Security -- References -- Author Index.

Sommario/riassunto

The 7-volume set LNCS 14651 - 14657 conference volume constitutes the proceedings of the 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2024, held in in Zurich, Switzerland, in May 2024. The 105 papers included in these proceedings were carefully reviewed and selected from 500 submissions. They were organized in topical sections as follows: Part I: Awarded papers; symmetric cryptology; public key primitives with advanced functionalities; Part II: Public key primitives with advances functionalities; Part III: AI and blockchain; secure and efficient implementation, cryptographic engineering, and real-world cryptography; theoretical foundations; Part IV: Theoretical foundations; Part V: Multi-party computation and zero-knowledge; Part VI: Multi-party computation and zero-knowledge; classic public key cryptography, Part VII: Classic public key cryptography.