1.	Record Nr.	UNINA9910847583103321
	Autore	Tang Qiang
	Titolo	Public-Key Cryptography – PKC 2024 : 27th IACR International Conference on Practice and Theory of Public-Key Cryptography, Sydney, NSW, Australia, April 15–17, 2024, Proceedings, Part IV / / edited by Qiang Tang, Vanessa Teague
	Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2024
	ISBN	3-031-57728-0
	Edizione	[1st ed. 2024.]
	Descrizione fisica	1 online resource (424 pages)
	Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14604
	Altri autori (Persone)	TeagueVanessa
	Disciplina	005.824
	Soggetti	Cryptography Data encryption (Computer science) Cryptology
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di contenuto	Intro -- Preface -- Organization -- One-Shot Signatures: Applications and Design Directions (Invited Talk) -- Contents - Part IV -- Encryption -- More Efficient Public-Key Cryptography with Leakage and Tamper Resilience -- 1 Introduction -- 2 Preliminaries -- 2.1 Digital Signatures -- 2.2 Public-Key Encryption -- 2.3 Collision-Resistant Hash Functions -- 2.4 Pairing Groups and MDDH Assumptions -- 3 More Efficient SIG with Leakage and Tamper-Resilience -- 3.1 Definition of sLTR-CMA Security -- 3.2 Construction of SIG from MDDH -- 3.3 Proof of Theorem 1 -- 4 More Efficient PKE with Leakage and Tamper-Resilience -- 4.1 Definition of sLTR-CCA Security -- 4.2 Construction of PKE from MDDH -- 4.3 Proof of Theorem 2 -- References -- SoK: Public Key Encryption with Openings -- 1 Introduction -- 2 Preliminaries -- 2.1 Notation -- 2.2 PKE Syntax -- 2.3 Security Notions -- 3 Confidentiality with Openings -- 3.1 Four Kinds of Opening -- 3.2 Four Philosophies of Confidentiality -- 3.3 A Priori Indistinguishability with Selective Openings (IND) -- 3.4 A Posteriori Indistinguishability with Selective Opening (ISO) -- 3.5 A Posteriori Simulatability with Selective Opening (SSO) -- 3.6 A Priori Simulatability with Selective Opening (NCE) -- 4 Relations -- References -- Dynamic Collusion Functional Encryption and Multi-Authority Attribute-Based Encryption -- 1 Introduction --

1.1 Multi-Authority Attribute-Based Encryption -- 2 Technical Overview -- 3 Preliminaries -- 4 Functional Encryption: Definitions -- 4.1 Static Collusion Model -- 4.2 Dynamic Collusion Model -- 4.3 Tagged Functional Encryption -- 5 From Static to Dynamic Collusion Model Generically -- 5.1 Tagged FE Accumulator -- 5.2 Security -- 5.3 Central Theorem -- 6 Multi-Authority ABE: Tagged and Dynamic Collusion -- 6.1 Definition and Preliminaries -- 6.2 Statically Secure MA-ABE for CSS Schemes.

6.3 Making It Tagged and Handling Dynamic Collusion -- References -- Public-Key Encryption with Keyword Search in Multi-user, Multi-challenge Setting under Adaptive Corruptions -- 1 Introduction -- 1.1 Our Results -- 1.2 Discussion -- 2 Preliminaries -- 2.1 Asymmetric Composite-Order Bilinear Groups -- 3 Definition of MU-PEKS -- 4 The First MU-PEKS Scheme -- 4.1 Construction -- 4.2 Security Proof -- 5 The Second MU-PEKS Scheme -- 5.1 Construction -- 5.2 Security Proof -- References -- Compact Selective Opening Security from LWE -- 1 Introduction -- 1.1 Technical Overview -- 2 Preliminaries -- 2.1 Notation -- 2.2 LWE-Based Trapdoors -- 2.3 Fully Homomorphic Encryption from Lattices -- 2.4 Lossy Trapdoor Functions -- 2.5 All-But-Many Lossy Trapdoor Functions (ABM-LTF) -- 2.6 Lossy Authenticated Encryption -- 2.7 Selective Opening Security -- 3 Lossy Trapdoor Function Construction -- 4 All-But-Many Lossy Trapdoor Function Construction -- 5 IND-SO-CCA Security from ABM-LTFs -- References -- Multi-hop Fine-Grained Proxy Re-encryption -- 1 Introduction -- 2 Preliminaries -- 3 Multi-hop Fine-Grained PRE -- 3.1 Syntax of Multi-hop FPRE and Its CPA and HRA Security -- 3.2 Achieving CPA and HRA Security for Multi-hop FPRE from Weaker Security Notions: IND, wKP and SH -- 3.3 Other Security Notions for Multi-hop FPRE: UNID and CUL -- 4 Constructions of Multi-hop Fine-Grained PRE Scheme -- 4.1 The CPA Secure Multi-hop FPRE Scheme mFPRE1 -- 4.2 The HRA Secure Multi-hop FPRE Scheme mFPRE2 -- References -- Quantum CCA-Secure PKE, Revisited -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Technical Overview -- 2 Preliminaries -- 3 Quantum CCA Security from Hash Proof Systems -- 4 qCCA Security from PKE and KDM-Secure SKE -- 4.1 Quantum CCA-Secure KEM -- 5 Quantum Adaptive Trapdoor Functions -- 5.1 Quantum CCA Security from Quantum ATDFs.

5.2 Quantum ATDFs from Correlated-Product TDFs -- References -- Parameter-Hiding Order-Revealing Encryption Without Pairings -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Technique Overview -- 1.3 Related Work -- 2 Preliminaries -- 2.1 Keyed Hash Function -- 2.2 Property-Preserving Hash -- 2.3 Parameter-Hiding ORE -- 3 Identification Schemes with Map-Invariance -- 3.1 Formal Definitions -- 3.2 An Instance from Schnorr Identification -- 4 PPH from Schnorr Identification -- 4.1 Generic PPH Construction -- 4.2 Security Analysis -- 4.3 PPH Instance from Schnorr Identification -- 5 The Proposed Parameter-Hiding ORE -- 5.1 From PPH to Parameter-Hiding ORE -- 5.2 ORE Instance from Schnorr Identification -- 6 Experimental Evaluation -- 7 Conclusion -- A More on the Leakage of Different ORE Schemes -- References -- Chosen-Ciphertext Secure Dual-Receiver Encryption in the Standard Model Based on Post-quantum Assumptions -- 1 Introduction -- 2 Preliminaries -- 2.1 Definitions -- 2.2 Assumptions and Lemmas -- 3 Applications of Dual-Receiver Encryption -- 3.1 Applications of CCA2 Secure DRE with Soundness -- 3.2 Applications of DRE with Public Verifiability -- 3.3 Applications of CPA secure DRE and the CRS Model -- 3.4 Non-generic Applications -- 4 Related Work on Post-quantum DRE Constructions -- 4.1 IND-CCA2 Secure DRE Schemes Without Soundness -- 4.2 Identity-Based DRE

Schemes Without Soundness -- 5 IND-CCA2DRE Secure and Sound Hybrid DRE -- 5.1 NLWE-Based Construction -- 5.2 Code-Based Construction of a Sound and IND-CCA2DRE Secure DRE -- 6 Discussion -- 7 Conclusion -- References -- Homomorphic Encryption -- SoK: Learning with Errors, Circular Security, and Fully Homomorphic Encryption -- 1 Introduction -- 2 Preliminaries -- 2.1 The Learning with Errors Problem (with Side Information) -- 2.2 LWE Encryption -- 2.3 Key Switching -- 2.4 Gadgets.

3 Circular LWE Conjectures -- 3.1 How About Linear Circular LWE? -- 3.2 Search to Decision Reduction -- 3.3 Key Cliques -- 3.4 Other Gadgets -- 4 Homomorphic Encryption Schemes -- 4.1 BV 2011, BGV 2012 and Brakerski 2012 -- 4.2 GSW 2013 and BV 2014 -- 4.3 AP14 and GINX16 -- 4.4 HAO15 -- References -- Faster Amortized FHEW Bootstrapping Using Ring Automorphisms -- 1 Introduction -- 2 Preliminaries -- 2.1 Cyclotomic Rings and Embeddings -- 2.2 Encryption Schemes and Operations -- 2.3 Using Ring Automorphisms -- 2.4 Homomorphic Operations on Registers -- 2.5 Standard and Primitive (Inverse) FFT -- 2.6 Summary of Notations -- 3 Novel Techniques -- 3.1 RLWE' to RGSW Scheme Switching -- 3.2 Error Growth in Prime Cyclotomics -- 4 Description of the Algorithm -- 4.1 Packing -- 4.2 Linear Step -- 4.3 msbExtract -- 5 Analysis -- 5.1 Counting Homomorphic Operations -- 5.2 Error Growth -- 5.3 Asymptotic Analysis -- 5.4 Comparison with Previous and Concurrent Work -- 6 Conclusion and Future Work -- References -- Towards Practical Multi-key TFHE: Parallelizable, Key-Compatible, Quasi-linear Complexity -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Works -- 2 Background -- 2.1 Notation -- 2.2 LWE and RLWE Assumptions -- 2.3 Multi-key Homomorphic Encryption -- 2.4 Gadget Decomposition -- 2.5 RLEV and RGSW -- 3 Overview of Chen et al. (2019) -- 3.1 Uni-Encryption and Hybrid Product -- 3.2 Gate Bootstrapping -- 4 Accelerating Multi-key TFHE -- 4.1 Improved Hybrid Product -- 4.2 Generalized External Product -- 4.3 Our Scheme -- 4.4 Using Different Gadget Decompositions -- 4.5 Distributed Decryption -- 5 Performance Analysis -- 5.1 Time and Space Complexity -- 5.2 Noise Growth -- 6 Implementation -- A Multi-key TFHE Variant Using Different Gadget Decompositions -- B Proofs for the Noise Analysis -- References -- Implementation.

Fast and Simple Point Operations on Edwards448 and E448 -- 1 Introduction -- 2 Twisted Edwards Curve -- 2.1 Ed448 and E448 -- 2.2 Affine Addition and Doubling Laws on Twisted Edwards Curves -- 2.3 Extended Twisted Edwards Coordinates -- 3 Unified Addition in Ee for d = -1 -- 3.1 The Unified Addition Law -- 3.2 The Unified Addition Formula -- 4 Clearing Denominators and Scalar Multiplication in Parallel Environments -- 4.1 Clearing Denominators for d = -1 -- 4.2 Clearing Denominators for a = -1 -- 5 Fast Formulae in Ee -- 5.1 Fast Addition in Ee for d = -1 -- 5.2 Modified Projective Coordinates E -- 5.3 Doubling in Ee -- 5.4 Tripling in Ee -- 5.5 Doubling in E -- 5.6 Tripling in E -- 6 Exceptional Case Analysis and Handling Strategies -- 6.1 Unified Addition Formula on 2q-Order Subgroup -- 6.2 Strategy for Single-Scalar Multiplication -- 6.3 Strategy for Multi-scalar Multiplication -- 7 Fast Scalar Multiplication -- 7.1 Parallelization for Unified Addition Formulae -- 7.2 Speedup by Mixing Different Coordinates -- 8 Conclusion -- References -- Author Index.

Sommario/riassunto

The four-volume proceedings set LNCS 14601-14604 constitutes the refereed proceedings of the 27th IACR International Conference on Practice and Theory of Public Key Cryptography, PKC 2024, held in Sydney, NSW, Australia, April 15–17, 2024. The 54 papers included in these proceedings were carefully reviewed and selected from 176

submissions. They focus on all aspects of signatures; attacks; commitments; multiparty computation; zero knowledge proofs; theoretical foundations; isogenies and applications; lattices and applications; Diffie Hellman and applications; encryption; homomorphic encryption; and implementation.