1. Record Nr. UNINA9910847584503321

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 III / / edited by Qiang Tang, Vanessa Teague
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2024
ISBN	3-031-57725-6
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (427 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14603
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 -- Contents - Part III -- Theoretical Foundations -- A Refined Hardness Estimation of LWE in Two-Step Mode -- 1 Introduction -- 2 Preliminaries -- 2.1 Notations and Basic Definitions -- 2.2 Lattice Hard Problems -- 2.3 Primal Attack -- 2.4 Core-SVP Model ch1ADPS16 -- 2.5 PnjBKZ -- 2.6 Dimension for Free (d4f) Technique -- 2.7 Leaky-LWE-Estimator -- 2.8 PnjBKZ Simulator -- 3 Efficiency of Two-Step Solving Mode -- 4 A Refined Two-Step Security Estimator for Solving LWE -- 4.1 Two-Step LWE Estimator with Trivial Strategy -- 4.2 Two-Step LWE Estimator with Refined Strategy -- 5 Experiments on Verifying the Accuracy of Two-Step LWE Estimator -- 5.1 Verification Experiments for Success Probability -- 5.2 Verification Experiments for Efficiency of Two-Step Mode -- 5.3 The Comparison of Different Estimation Modes -- 6 Improved Conservative Estimation for LWE -- 6.1 Theoretical Lower-Bound Security Estimation of LWE Hardness -- 7 Two-Step Security Estimation of LWE in NIST Schemes -- 7.1 Security Upper Bound Estimation of LWE in NIST PQC Schemes -- 7.2 Lower Bound Estimation of LWE in NIST PQC Schemes -- 8 Conclusion -- A Appendix. Two-Step LWE Estimator Based on Classical LWE Estimator -- References -- A Simpler and More Efficient Reduction of DLog to CDH for Abelian Group Actions*-8pt -- 1 Introduction*-2pt

-- 1.1 Group Actions and Computational Problems -- 1.2 The Montgomery-Zhandry Approach -- 1.3 Technical Overview -- 2 Preliminaries -- 2.1 Cryptographic Group Actions -- 2.2 Computational Problems -- 2.3 Chernoff Bounds -- 3 The Main Reduction -- 3.1 Preparation -- 3.2 Estimating -- 3.3 Thresholding -- 3.4 Finding a Gap -- 3.5 Using the Fixed Set of Elements -- 3.6 Proof of Finding the Subgroup -- 3.7 Putting It All Together -- 3.8 Using the Subgroup -- 3.9 Extending to Non-regular Group Actions -- References.
R3PO: Reach-Restricted Reactive Program Obfuscation and Its Applications -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Work -- 2 Technical Overview -- 2.1 Motivating Examples -- 2.2 Defining R3PO -- 2.3 R3PO Composition Theorem -- 2.4 R3PO Library -- 2.5 Applications: The Different Ways of Using R3PO -- 2.6 Private Multi-Authority ABE -- 2.7 Comparison of R3PO with Existing Primitives -- 3 The R3PO Framework -- 3.1 Reactive Programs and Generators -- 3.2 Reach Extractor -- 3.3 Reach-Restricted Reactive Program Obfuscation -- 4 A Composition Theorem for R3PO -- 4.1 Decomposition -- 4.2 Composition Theorem -- 5 Private Multi-Authority ABE -- 5.1 Definition for Private Multi-Authority ABE -- 5.2 Construction for Private Multi-Authority ABE -- References -- Selective Opening Security in the Quantum Random Oracle Model, Revisited -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Technical Details -- 2 Preliminaries -- 2.1 Public-Key Encryption -- 2.2 Quantum Computation -- 3 Computational Adaptive Reprogramming in the QROM -- 4 Selective Opening Security of Fujisaki-Okamoto's PKE in the QROM -- 4.1 Selective Opening Security Against Chosen-Plaintext Attacks -- 4.2 Selective Opening Security Against Chosen-Ciphertext Attacks -- 5 Tight SO-CCA Security from Lossy Encryption -- 5.1 Construction -- 6 Bi-sO Security in the QROM -- 6.1 Bi-sO Security of TEXT -- 6.2 Bi-sO Security of TEXT -- A Review of Adaptive One-Way-to-Hiding -- References -- On Algebraic Embedding for Unstructured Lattices -- 1 Introduction -- 1.1 This Work: General Lattices as Ideals -- 1.2 Technical Overview -- 2 Preliminaries -- 2.1 The Space H -- 2.2 Lattices -- 2.3 Lattices in Number Fields: Orders and Ideals -- 2.4 The LWE Problem -- 2.5 The Order LWE Problem -- 3 New Hardness Results for O-LWE -- 3.1 Worst-Case Hardness for All O-Ideals.
3.2 Ring-LWE Hardness for Some Non OK-Ideal Lattices -- 4 Gradients of Hardness Between Ring-LWE and LWE -- References -- Isogenies and Applications -- An Algorithm for Efficient Detection of (N,N)-Splittings and Its Application to the Isogeny Problem in Dimension 2 -- 1 Introduction -- 2 Background -- 2.1 Superspecial Abelian Surfaces -- 2.2 The Superspecial Isogeny Graph -- 2.3 Attacking the General Isogeny Problem in Dimension 2 -- 3 Optimised Product Finding in 2(2 -- p) -- 3.1 Taking a Step in 2(2 -- p) -- 3.2 Walking in the Superspecial Subgraph of 2(2 -- p) -- 4 Explicit Moduli Spaces for Genus 2 Curves with Split Jacobians -- 4.1 The Igusa-Clebsch Invariants of a Genus 2 Curve -- 4.2 Optimal Splittings of Jacobians of a Genus 2 Curves -- 4.3 The Surfaces tilde{L}N and {L}N -- 4.4 The Image of the Morphism LN to M2 -- 5 Efficient Detection of (N,N)-Splittings -- 5.1 The Resultants of fj and fk -- 5.2 An Algorithm to Detect (N,N)-Split Jacobians -- 6 The Full Algorithm -- 6.1 SplitSearcher -- 6.2 Determining the Optimal Set N -- 6.3 A Bound on the Cost of the SplitSearcher Algorithm -- 7 Experimental Results -- References -- SCALLOP-HD: Group Action from 2-Dimensional Isogenies -- 1 Introduction -- 1.1 Contribution -- 2 Preliminaries -- 2.1 Quaternion Algebras, Supersingular Elliptic Curves, Isogenies and the Deuring Correspondence -- 2.2 Quadratic Orders and Orientations on Supersingular Elliptic Curves -- 2.3 New Isogeny Representation in

Higher Dimensions -- 3 Group Action in Isogeny-Based Cryptography -- 4 2dim-Representation of Orientations and Endomorphisms -- 4.1 2dim-Representation -- 4.2 Computing a 2dim-Representation -- 4.3 Class Group Action Evaluation -- 5 SCALLOP-HD Group Action -- 5.1 Outline of SCALLOP-HD -- 5.2 Set Up the Group Action -- 5.3 Set Up a Starting Curve -- 5.4 Offline Phase -- 5.5 Online Phase.
5.6 Implementation Results -- 6 Some Remarks on Security -- 7 Conclusion and Future Work -- References -- New Proof Systems and an OPRF from CSIDH -- 1 Introduction -- 2 Background -- 2.1 Isogeny-Based Cryptography -- 2.2 Zero-Knowledge Proofs -- 3 Towards Multiplication from Addition -- 3.1 Tuple Generation Functionality -- 3.2 Two-Party Multiplication Protocol -- 4 Zero-Knowledge Proof Systems -- 4.1 Languages and Security Assumptions -- 4.2 Addition and Scalar Multiplication -- 4.3 Multiplication with Trusted Setup -- 4.4 MPC-in-the-Head Protocols -- 4.5 New Signatures -- 5 An Oblivious Pseudo-random Function -- 5.1 Choosing the Polynomial -- 5.2 Adding Verifiability -- 5.3 Comparison to the Literature -- 5.4 Removing the Trusted Setup -- References -- Lattices and Applications -- On Structure-Preserving Cryptography and Lattices -- 1 Introduction -- 1.1 Technical Overview -- 1.2 Roadmap -- 2 Preliminaries -- 2.1 Notation -- 2.2 Lattices -- 2.3 Cryptographic Primitives -- 3 Structure-Preserving Sets -- 4 Lattice-Based Structure-Preserving Signatures -- 4.1 SPS Instantiation -- 5 Lattice-Based Structure-Preserving Encryption -- 5.1 SPE Instantiation -- 6 -Protocol Constructions -- 7 Lattice-Based Structure-Preserving NIZK Arguments -- 8 Verifiably Encrypted Signatures (VES) -- 8.1 The VES Construction -- 8.2 Efficiency Considerations -- References -- Tagged Chameleon Hash from Lattices and Application to Redactable Blockchain -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Works -- 1.3 Technique Overview -- 2 Preliminaries -- 2.1 Lattice Background -- 2.2 Computational Assumption -- 2.3 Pseudorandom Function -- 3 Tagged Chameleon Hash -- 4 Lattice-Based Tagged Chameleon Hash -- 4.1 tCH in the Standard Model -- 4.2 tCH with Tight Security in ROM -- 5 Application of tCH to the Redactable Blockchain -- 5.1 Redactable Blockchain.
5.2 Redacting Blocks -- 5.3 Security Analysis -- References -- Diffie Hellman and Applications -- Laconic Branching Programs from the Diffie-Hellman Assumption -- 1 Introduction -- 1.1 Our Results -- 2 Technical Overview -- 3 Preliminaries -- 4 Semi-honest Laconic 2PC with Branching Programs -- 4.1 The BP-2PC Construction -- 5 Applications -- 5.1 Private Set Intersection (PSI) -- 5.2 Private Set Union (PSU) -- 5.3 Wildcards -- 5.4 Fuzzy Matching -- 6 Proof of Lemma 3 -- 7 Proof of Theorem 1 -- 7.1 Proof of Lemma 4 -- 7.2 Proof of Lemma 5 -- References -- Rate-1 Fully Local Somewhere Extractable Hashing from DDH -- 1 Introduction -- 1.1 Our Results -- 1.2 Technical Outline -- 2 Preliminaries -- 2.1 Somewhere Extractable Hash Families -- 2.2 Somewhere Extractable Batch Arguments -- 3 Fully Local SEH from DDH -- 3.1 Definition -- 3.2 Construction -- 3.3 Security Analysis -- 4 Applications -- 4.1 Rate-1 seBARGs -- 4.2 Rate-1 BARGs with Short CRS -- 4.3 RAM SNARGs with Partial Input Soundness -- References -- Private Set Operations from Multi-query Reverse Private Membership Test -- 1 Introduction -- 1.1 Motivation -- 1.2 Our Contribution -- 1.3 Technical Overview -- 1.4 Related Works -- 1.5 Roadmap -- 2 Preliminaries -- 2.1 MPC in the Semi-honest Model -- 2.2 Private Set Operation -- 3 Protocol Building Blocks -- 3.1 Oblivious Transfer -- 3.2 Multi-query Reverse Private Membership Test -- 4 The First Generic Construction of mqRPMT -- 4.1 Definition of Commutative Weak PRF -- 4.2 Construction of Commutative Weak PRF -- 4.3 mqRPMT from

Commutative Weak PRF -- 5 The Second Generic Construction of mqRPMT -- 5.1 Definition of Permuted OPRF -- 5.2 Construction of Permuted OPRF -- 5.3 mqRPMT from Permuted OPRF -- 6 Applications of mqRPMT -- 6.1 PSO Framework from mqRPMT -- 6.2 Private-ID -- 7 Performance -- 7.1 Implementation Details -- 7.2 Experimental Setup. 7.3 Evaluation of mqRPMT.

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. .