1. Record Nr. UNINA9910574075903321

Titolo	Advances in Cryptology – EUROCRYPT 2022 : 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 – June 3, 2022, Proceedings, Part II / / edited by Orr Dunkelman, Stefan Dziembowski
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2022
ISBN	3-031-07085-2
Edizione	[1st ed. 2022.]
Descrizione fisica	1 online resource (920 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 13276
Disciplina	929.605 005.82
Soggetti	Cryptography Data encryption (Computer science) Application software Computer networks Coding theory Information theory Cryptology Computer and Information Systems Applications Computer Communication Networks Coding and Information Theory
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 II -- Cryptographic Protocols -- Single-Server Private Information Retrieval with Sublinear Amortized Time -- 1 Introduction -- 1.1 Our Results -- 1.2 Overview of Techniques -- 1.3 Related Work -- 2 Background -- 2.1 Standard Definitions -- 2.2 Definition of Offline/Online PIR -- 3 Two-Server PIR with a Single-Server Online Phase and Sublinear Amortized Time -- Construction 3 -- 4 Single-Server PIR with Sublinear Amortized Time from DCR, QR, DDH, or LWE -- 5 Single-Server PIR with Optimal Amortized Time and Storage from Fully Homomorphic Encryption -- 6 Lower Bounds -- 6.1 Lower Bound for Adaptive Schemes -- 6.2 Lower

Bound for Batch PIR with Advice -- 7 Conclusion -- References -- Anamorphic Encryption: Private Communication Against a Dictator -- 1 Introduction -- 2 Related Works -- 3 Our Approach -- 4 Receiver-Anamorphic Encryption -- 4.1 Syntax -- 4.2 Modes of Operation -- 4.3 Security Notion -- 4.4 Properties of the Anamorphic Mode with Normal Encryption -- 4.5 Security of the Fully Anamorphic Mode -- 5 Constructions -- 5.1 Rejection Sampling -- 5.2 The Naor-Yung Transform -- 5.3 The NY Transform Gives Receive-AM Encryption -- 6 Sender-Anamorphic Encryption -- 6.1 Sufficient Conditions for Sender-AM with No Shared Key -- 6.2 Constructions Based on LWE Encryption Schemes -- 7 Conclusion -- References -- A PCP Theorem for Interactive Proofs and Applications -- 1 Introduction -- 1.1 Main Results -- 1.2 A Cryptographic Application to SNARKs -- 2 Techniques -- 2.1 Towards Transforming IPs to IOPs -- 2.2 Local Access to Randomness -- 2.3 Index-Decodable PCPs -- 2.4 Local Access to Prover Messages -- 2.5 Constructing Index-Decodable PCPs -- 2.6 Commit-and Prove SNARKs from Index-Decodable PCPs -- 2.7 Hardness of Approximation -- References.
Group Signatures and More from Isogenies and Lattices: Generic, Simple, and Efficient -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Technical Overview -- 2 Preliminaries -- 2.1 Non-interactive Zero-Knowledge Proofs of Knowledge in the ROM -- 2.2 Accountable Ring Signatures -- 3 Generic Construction of Accountable Ring Signature and Dynamic Group Signature -- 3.1 Generic Construction of Accountable Ring Signature -- 3.2 Accountable Ring Signature to Dynamic Group Signature -- 3.3 Tightly Secure Variant -- 4 Group-Action-Based Hard Instance Generators and PKEs -- 4.1 Group-Action-Based Hard Instance Generator -- 4.2 Group-Action-Based PKE -- 5 Sigma Protocol for a ``Traceable'' OR Relation -- 5.1 From a Group-Action-Based HIG and PKE to Base Traceable or Sigma Protocol -- 5.2 From Base to Main Traceable or Sigma Protocol -- 5.3 Base Sigma Protocol for the ``Tight'' Relation R-tight -- 6 Multi-proof Online Extractable NIZK from Sigma Protocol main traceable OR sigma protocol -- 7 Instantiations -- References -- Asymmetric PAKE with Low Computation and communication -- 1 Introduction -- 2 Key-Hiding One-Time-Key AKE -- 2.1 2DH as Key-Hiding One-Time-Key AKE -- 2.2 One-Pass HMQV as Key-Hiding One-Time-Key AKE -- 3 Protocol OKAPE: Asymmetric PAKE Construction #1 -- 4 Protocol aEKE: Asymmetric PAKE Construction #2 -- 5 Concrete aPAKE Protocol Instantiations -- 6 Curve Encodings and Ideal Cipher -- A Universally Composable Asymmetric PAKE Model -- B Simulator for Proof of Theorem 3 -- References -- Batch-OT with Optimal Rate -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Related Work -- 2 Technical Overview -- 2.1 Oblivious Transfer from Homomorphic Encryption -- 2.2 Download-Rate Optimal String OT -- 2.3 Our Approach: Recrypting the Receiver's Message -- 2.4 Dealing with LPN Errors -- 2.5 Emulating Small Subgroups -- 3 Preliminaries.
3.1 Lattices and Gaussians -- 3.2 Distributed GGM-PPRF Correlation -- 4 Compression-Friendly Subgroup Emulation via Gaussian Rounding -- 5 Rate-1 Circuit-Private Linearly Homomorphic Encryption -- 5.1 Construction from DDH -- 6 Co-private Information Retrieval -- 6.1 Definition -- 7 Oblivious Transfer with Overall Rate 1 -- 7.1 The Protocol -- 7.2 Security -- 8 Oblivious Matrix-Vector Product and Oblivious Linear Evaluation with Overall Rate 1 -- 8.1 OLE Protocol -- A Additional Preliminaries -- A.1 UC Security -- A.2 Learning Parity with Noise -- References -- Adaptively Secure Computation for RAM Programs -- 1 Introduction -- 1.1 Our Results -- 1.2 Our Techniques -- 2 Equivocal ORAM -- 3 RAM-Efficient Equivocal Encryption -- 3.1

Our Construction -- 4 Equivocal Garbled RAM -- 4.1 Our Construction -- 4.2 Putting It Together -- 5 Adaptive Zero-Knowledge for RAM -- 5.1 Splitable Garbling -- 5.2 Our Adaptive UC ZK Protocol -- References -- Optimal Broadcast Encryption and CP-ABE from Evasive Lattice Assumptions -- 1 Introduction -- 2 Technical Overview -- 2.1 Our CP-ABE Schemes -- 2.2 On Evasive Lattice Assumptions -- 2.3 Additional Related Work -- 3 Preliminaries -- 3.1 Lattices Background -- 3.2 Attribute-Based Encryption -- 4 Evasive LWE -- 5 Main Constructions -- 5.1 Homomorphic Computation on Matrices -- 5.2 CP-ABE for NC1 Circuits -- 5.3 Optimal Broadcast Encryption -- 5.4 CP-ABE for Polynomial-Depth Circuits -- 6 Discussion on Evasive LWE -- References -- Embedding the UC Model into the IITM Model -- 1 Introduction -- 2 A Brief Overview of the UC and IITM Models -- 2.1 The UC Model -- 2.2 The IITM Model -- 3 Embedding the UC Model in the IITM Model -- 3.1 Main Conceptual Differences -- 3.2 Mapping Protocols -- 3.3 UC Security Implies IITM Security -- 3.4 UC Composition Implies IITM Composition.
3.5 Capturing Dynamically Generated Machine Code -- 3.6 Discussion: Beyond UC Protocols -- 4 Impossibility of Embedding the IITM Model into the UC Model -- References -- Zero-Knowledge Proofs -- Zero-Knowledge IOPs with Linear-Time Prover and Polylogarithmic-Time Verifier -- 1 Introduction -- 1.1 Our Results -- 1.2 Related Work on Probabilistic Proofs -- 1.3 Related Work on Succinct Arguments -- 2 Techniques -- 2.1 Approach Overview -- 2.2 Construction Overview -- 2.3 From Tensor-Queries to Point-Queries in Zero-Knowledge -- 2.4 Tensor IOP for R1CS with Semi-honest Verifier Zero Knowledge -- 2.5 Hiding Properties of Linear Codes -- 2.6 On Bounded-Query Zero Knowledge -- 2.7 Linear-Time Succinct Arguments from Linear-Time IOPs -- References -- Non-Interactive Zero-Knowledge Proofs with Fine-Grained Security -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Technical Details -- 2 Preliminaries -- 2.1 Function Families -- 2.2 Sampling Procedure -- 2.3 Proof Systems -- 3 AC0[2]-Protocol for Linear Languages -- 4 Fine-Grained NIZK for Linear Languages -- 5 Fine-Grained OR-Proof -- 6 Fine-Grained NIZK Proof for Circuit SAT -- 7 Fine-Grained NIZK for AC0CM[2] with Short Proofs -- 7.1 Definition of Fine-Grained sFHE -- 7.2 Construction of Fine-Grained sFHE -- 7.3 Generic Construction of NIZK -- 8 Fine-Grained Non-Interactive Zap -- 8.1 Verifiable Correlated Key Generation -- 8.2 Construction of Fine-Grained Non-Interactive Zap -- 9 Fine-Grained NIZK in the URS Model -- References -- On Succinct Non-interactive Arguments in Relativized Worlds -- 1 Introduction -- 1.1 Our Results -- 1.2 Related Work -- 2 Techniques -- 2.1 Linear Code Random Oracles -- 2.2 Accumulation Scheme for Low-Degree Random Oracles -- 2.3 A Forking Lemma for Linear Code Random Oracles -- 2.4 A Zero-Finding Game for Low-Degree Random Oracles -- 2.5 SNARKs for Oracle Computations.
3 Preliminaries -- 3.1 Notations -- 3.2 Non-interactive Arguments in Oracle Models -- 3.3 Accumulation Schemes -- 3.4 Commitment Schemes -- 4 Linear Code Random Oracles -- 4.1 Query Transcripts and Partial Oracles -- 4.2 Constraints -- 4.3 Query Complexity -- 4.4 Low-Degree Random Oracles -- 5 A Forking Lemma for Linear Code Random Oracles -- 6 Oracle Zero-Finding Games -- 7 Accumulation Scheme for Low-Degree Random Oracles -- References -- Families of SNARK-Friendly 2-Chains of Elliptic Curves -- 1 Introduction -- 2 Preliminaries -- 2.1 Background on Bilinear Pairings -- 2.2 zk-SNARKs -- 2.3 SNARK-Friendly Chains -- 3 Inner Curves: Barreto-Lynn-Scott (BLS) Curves -- 3.1 Parameters with a Polynomial Form -- 3.2 Faster Co-factor Multiplication -- 3.3 Subgroup Membership Testing: GT -- 3.4 Choosing a Curve Coefficient b=1 -- 3.5 SNARK-Friendly Inner BLS

Curves -- 4 Outer Curves: Brezing-Weng, Cocks-Pinch -- 4.1 Generic BW6 Curve Parameters -- 4.2 BW6 with BLS-12 -- 4.3 BW6 with BLS-24 -- 4.4 Two-Chains with Inner BLS and Outer Cocks-Pinch -- 4.5 Comparison of BW6, CP8 and CP12 Outer Curve Performances -- 5 Implementation and Benchmarking -- 5.1 SageMath Library: Derive the Curves -- 5.2 Our Short-List of Curves -- 5.3 Estimated Complexity of a DL Computation in GF(qk) -- 5.4 Golang Library: Implement the Short-List Curves -- 5.5 Benchmarking -- 6 Conclusion -- References -- Fiat-Shamir Bulletproofs are Non-Malleable (in the Algebraic Group Model) -- 1 Introduction -- 1.1 Technical Overview -- 1.2 Related Work -- 2 Preliminaries -- 3 Simulation-Extractability from State-Restoration Unique Response -- 3.1 Simulation-Extractability in the AGM -- 3.2 From Weak Unique Response to Simulation-extractability -- 3.3 Generic Result on Simulation-Extractability -- 4 Non-Malleability of Bulletproofs - Arithmetic Circuits -- 4.1 Algebraic Simulation.
4.2 State-Restoration Unique Responses.

Sommario/riassunto

The 3-volume-set LNCS 13275, 13276 and 13277 constitutes the refereed proceedings of the 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Eurocrypt 2022, which was held in Trondheim, Norway, during 30 May – 3 June, 2022. The 85 full papers included in these proceedings were accepted from a total of 372 submissions. They were organized in topical sections as follows: Part I: Best Paper Award; Secure Multiparty Computation; Homomorphic Encryption; Obfuscation; Part II: Cryptographic Protocols; Cryptographic Primitives; Real-World Systems Part III: Symmetric-Key Cryptanalysis; Side Channel Attacks and Masking, Post-Quantum Cryptography; Information-Theoretic Security.