1. Record Nr. UNINA9910855378403321

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 IV / / edited by Marc Joye, Gregor Leander
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2024
ISBN	3-031-58737-5
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (424 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14654
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 IV -- Theoretical Foundations (II/II) -- The NISQ Complexity of Collision Finding -- 1 Introduction -- 1.1 Contributions -- 1.2 Related Work -- 2 Hybrid Random Oracle Model -- 2.1 Models for NISQ Algorithms -- 3 Hybrid Compressed Oracle -- 3.1 Construction -- 3.2 Structural Properties -- 3.3 Sampling and Resampling -- 3.4 Progress Measures -- 4 Collision Finding -- 4.1 Progress Measure -- 4.2 Main Result -- 4.3 Progress Overlap Lemmas -- 4.4 Progress Increase Lemmas -- References -- Non-malleable Codes with Optimal Rate for Poly-Size Circuits -- 1 Introduction -- 1.1 Error Correcting Codes and Non-malleable Codes

-- 1.2 Our Results: Non-malleable Codes with Optimal Rate -- 1.3 Overview of the Technique -- 1.4 Other Rate Compilers for Non-Malleable Codes -- 1.5 Organization of This Paper -- References -- Approximate Lower Bound Arguments -- 1 Introduction -- 1.1 Our Setting -- 1.2 Our Results -- 1.3 Applications -- 1.4 Relation to General-Purpose Witness-Succinct Proofs -- 2 Definitions -- 3 Telescope ALBA -- 3.1 Basic Construction -- 3.2 Construction with Prehashing -- 3.3 Implementing Random Oracles with Long Inputs -- 3.4 Optimality of the Certificate Size -- 4 ALBAs with Decentralized Prover -- 4.1 Simple Lottery Construction -- 4.2 Decentralized Telescope -- 4.3 Optimality of the Certificate Size - Communication Tradeoff -- 5 Adding Weights -- 6 Knowledge Extraction for NIROPK -- 7 Replacing the Random Oracle with PRF -- 7.1 Knowledge Extraction For Definition 6/4 -- 8 Performance Comparisons -- References -- Software with Certified Deletion -- 1 Introduction -- 1.1 Our Results -- 2 Technical Overview -- 2.1 Warm-Up Example -- 2.2 General Compiler for Certified Deletion -- 2.3 Discussion -- 2.4 Blind Delegation with Certified Deletion -- 2.5 Obfuscation with Certified Deletion.
3 Related Work -- 3.1 Prior Work -- 3.2 Concurrent and Independent Work -- 4 Delayed Preparation of Coset States -- 4.1 Coset Representatives -- 4.2 Sampling Procedure -- 4.3 Delayed Preparation of Coset States -- 5 General Compiler for Certified Deletion -- 5.1 General Theorem -- References -- Public-Coin, Complexity-Preserving, Succinct Arguments of Knowledge for NP from Collision-Resistance -- 1 Introduction -- 1.1 Our Results -- 1.2 Technical Overview -- 1.3 Related Work on Succinct Arguments -- 2 Preliminaries -- 2.1 Collision-Resistant Hash Functions -- 2.2 Hash Trees -- 2.3 Arguments of Knowledge -- 3 Arguments of Knowledge for Bounded Space Computation -- 3.1 Construction -- 4 Complexity-Preserving Succinct Arguments of Knowledge -- 4.1 Construction -- References -- Unbiasable Verifiable Random Functions -- 1 Introduction -- 2 Preliminaries -- 2.1 Notation -- 2.2 Preprocessing Adversaries -- 2.3 Discrete Logarithm Problem and DDH -- 2.4 Pseudo Random Functions -- 2.5 Verifiable Random Functions -- 3 Unbiasability -- 3.1 Definition -- 3.2 Properties -- 4 Unbiasable VRF in the ROM -- 4.1 From Any VUF -- 4.2 From Weakly Unbiasable VUF -- 5 Constructions in the Standard Model -- 5.1 1st Preliminary Construction: Padded VRF -- 5.2 Verifiable Random Bijection -- 5.3 2nd Preliminary Construction: 2-Feistel Rounds -- 5.4 VRB Compiler -- 5.5 Unbiasable VRF Compiler -- 6 Conclusions -- References -- Monotone-Policy Aggregate Signatures -- 1 Introduction -- 1.1 Our Results -- 1.2 Related Work -- 2 Technical Overview -- 2.1 Aggregate Signatures for Bounded-Space Monotone Policies -- 2.2 Weakly Unforgeable Aggregate Signatures for Polynomial-Size Monotone Policies -- 2.3 Full Version -- 3 Aggregate Signatures for Monotone Policies -- 4 Batch Arguments for Monotone Policies -- 4.1 Batch Arguments with Adaptive Subset Extraction.
4.2 From Adaptive Subset Extraction to Aggregate Signatures -- References -- Leakage-Tolerant Circuits -- 1 Introduction -- 1.1 Our Results -- 1.2 Related Work -- 2 Technical Overview -- 2.1 Application: Stateful Leakage-Resilient Circuits -- 2.2 Overview of Feasibility Results -- 2.3 Leakage Tolerance Against Depth-1 AC0 Leakage -- 2.4 Leakage Tolerance Against Parity Leakage -- 3 Preliminaries -- 4 Sketch of Depth-1 AC0 Leakage Tolerance -- 5 Parity Leakage Tolerance -- 5.1 Parity-to-Probing Implies Parity Tolerance -- 5.2 Feasibility of Parity-Tolerant Circuits -- References -- Pseudorandom Isometries -- 1 Introduction -- 1.1 Our Results -- 1.2 Technical Overview -- 2 Pseudorandom Isometry: Definition -- 2.1

Invertibility -- 3 Construction -- 3.1 Main Results -- 4 Applications -- 4.1 PRI Implies PRSG and PRFSG -- 4.2 Quantum Message Authentication Codes -- 4.3 Length Extension of Pseudorandom States -- References -- New Limits of Provable Security and Applications to ElGamal Encryption -- 1 Introduction -- 2 Related Work and Overview -- 3 Preliminaries -- 4 Notions for PKE and CHOWBs -- 4.1 Public-Key Encryption -- 4.2 Semi-Homomorphic PKE -- 4.3 Certified Homomorphic One-Way Bijections -- 5 Random Self-Reducible and Re-Randomizable Relations (RRRs) -- 5.1 Algorithms -- 6 Important RRRs -- 6.1 RRRs from Semi-Homomorphic PKE -- 6.2 Strong RRRs from Semi-Homomorphic PKE -- 7 A New Weak Security Notion for Relations -- 8 Interactive Complexity Assumption -- 9 First Result: Impossibility of Simple Reductions for General RRR Systems -- 9.1 Simple Reductions -- 9.2 First Main Result -- 9.3 Proof of Theorem 1 -- 9.4 The Ideal Attacker A -- 9.5 The Meta-Reduction M Can Rewind Reduction B -- 9.6 The Simulated Attacker -- 9.7 Analysis -- 10 Second Main Result -- References.
Constructing Leakage-Resilient Shamir's Secret Sharing: Over Composite Order Fields -- 1 Introduction -- 1.1 Basic Preliminaries -- 1.2 Our Results -- 1.3 Prior Related Works -- 1.4 Technical Overview: Randomized Construction -- 1.5 Technical Overview: Classification Algorithm -- 1.6 Discussion: Jacobian Test &amp -- the Number of Isolated Zeroes -- 2 Preliminaries -- 2.1 Secret Sharing Schemes -- 2.2 Physical-Bit Leakages and Leakage-Resilient Secret Sharing -- 2.3 Generalized Reed-Solomon Codes and Vandermonde Matrices -- 2.4 Field Trace -- 2.5 Fourier Analysis -- 2.6 Counting Isolated Roots -- 3 Bounding the Number of Solutions of an Equation -- 3.1 Over Finite Fields with Large Characteristics -- 3.2 Over Finite Fields with Characteristic Two -- 3.3 Over Finite Fields with Small Characteristic -- 4 Bounding 1-Fourier Norms of Physical-Bit Leakages -- 5 Leakage Resilience: Characteristic Two Finite Fields -- 5.1 Claims Needed for Theorem 1 -- 5.2 Proof of Theorem 1 -- 6 Leakage Resilience: Large Characteristic Fields -- 7 Our Classification Algorithm -- 7.1 Proof of Theorem 5 -- 7.2 Technical Results -- References -- Connecting Leakage-Resilient Secret Sharing to Practice: Scaling Trends and Physical Dependencies of Prime Field Masking -- 1 Introduction -- 2 Background -- 2.1 Quantifying the Distance to Uniform -- 2.2 The Limits of Generic Noise Amplification Bounds -- 2.3 Refined Bounds Through Fourier Analysis -- 3 Bit Leakages -- 3.1 Worst-Case Characterization -- 3.2 Average-Case Characterization -- 3.3 Discussion -- 4 Hamming Weight Leakages -- 4.1 Worst-Case Characterization -- 4.2 Average-Case Characterization -- 4.3 Discussion -- 5 Empirical Evaluation -- 6 Conclusions and Open Problems -- A Proofs of Section 2 -- B Proofs of Section 4 -- References -- From Random Probing to Noisy Leakages Without Field-Size Dependence -- 1 Introduction.
1.1 Our Contribution -- 1.2 Technical Overview -- 2 Preliminaries -- 2.1 Simple Facts -- 3 Composable Gadgets Against Average Probing -- 3.1 Basic Arithmetic Gadgets -- 3.2 Multiplication Gadget -- 3.3 Copy Gadget -- 3.4 Putting Everything Together -- 4 The Circuit Compiler -- 5 Conclusions and Open Problems -- References -- A Direct PRF Construction from Kolmogorov Complexity -- 1 Introduction -- 1.1 Construction Overview -- 1.2 Proof Overview -- 2 Preliminaries -- 2.1 Time-Bounded Kolmogorov Complexity -- 2.2 Average-Case* Hardness -- 2.3 One-Way Functions and MKtP[s] -- 2.4 Pseudorandom Generators and Pseudorandom Functions -- 3 Weak Family of PRGs and Security Amplification -- 4 Unapproximability of Random Strings for Small Programs -- 5 PRF Construction from MKtP -- 5.1 Tools -- 5.2

	The PRF Construction -- 5.3 Security of the PRF Construction -- 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.