1. Record Nr. UNISA996464507603316

Titolo	Theory of cryptography . Part I : 19th International Conference, TCC 2021, Raleigh, NC, USA, November 8-11, 2021, Proceedings / / Kobbi Nissim, Brent Waters (editors)
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2021] ©2021
ISBN	3-030-90459-8
Descrizione fisica	1 online resource (799 pages)
Collana	Lecture notes in computer science ; ; 13042
Disciplina	005.82
Soggetti	Data encryption (Computer science) Computer networks - Security measures
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 I -- Contents - Part II -- Contents - Part III -- Secure Quantum Computation with Classical Communication -- 1 Introduction -- 1.1 Results -- 1.2 Technical Overview -- 1.3 Discussion and Open Problems -- 1.4 Other Related Work -- 2 Preliminaries -- 2.1 Delegation of Quantum Computation -- 2.2 Quantum Fully-Homomorphic Encryption -- 2.3 Multi-party Quantum Computation -- 2.4 Classical Non-interactive Secure Computation -- 3 Generalizing the Alagic et al. Parallel Repetition Theorem -- 4 Composable Blind CVQC -- 4.1 CVQC for Quantum-Classical Circuits -- 4.2 Delegation of Quantum-Classical Circuits with Quantum Verifier -- 4.3 Making the Verifier Classical -- 4.4 Four-Message CVQC -- 5 Secure Quantum Computation -- 5.1 A Generic Construction of Multi-party Quantum Computation -- References -- Secure Software Leasing from Standard Assumptions -- 1 Introduction -- 1.1 Background -- 1.2 Our Results -- 1.3 Related Work -- 1.4 Concurrent Work -- 1.5 Technical Overview -- 1.6 Organization -- 2 Preliminaries -- 2.1 Noisy Trapdoor Claw-Free Hash Function -- 2.2 Secure Software Leasing -- 3 Two-Tier Quantum Lightning -- 3.1 Two-Tier Quantum Lightning -- 3.2 Two-Tier Quantum Lightning with Classical Verification -- 3.3 Two-Tier Quantum Lightning with Classical Verification from LWE -- 4 Relaxed Watermarking -- 4.1 Definition of

Relaxed Watermarking -- 4.2 Relaxed Watermarking for PRF -- 5 Secure Software Leasing from Two-Tier Quantum Lightning -- References -- Post-quantum Resettably-Sound Zero Knowledge -- 1 Introduction -- 1.1 Contributions -- 2 Technical Overview -- 2.1 Defining Post-quantum Resettable Soundness -- 2.2 3-Message and Constant-Round-Public-Coin Protocols Can Be Made Resettably Sound -- 2.3 Constructing a Resettably Sound Non-Black-Box Zero-Knowledge Protocol.
2.4 From Resettable Soundness to Quantum Unobfuscatability -- 2.5 Related Work -- 3 Defining Post-Quantum Resettable Soundness -- 3.1 Post-Quantum Resettable Soundness -- 4 Transforming Protocols to Achieve Quantum Resettable Soundness -- 4.1 Quantum Oracle Notations -- 4.2 Transforming 3 Message Private Coin Protocols -- 4.3 Deterministic-Prefix Resetting Provers -- 5 A Post-Quantum Resettably Sound Zero Knowledge Protocol -- 5.1 Protocol Construction -- References -- Secure Software Leasing Without Assumptions -- 1 Introduction -- 1.1 Summary of Contributions -- 1.2 Open Problems -- 1.3 Outline -- 2 Preliminaries -- 2.1 Notation -- 2.2 Quantum Authentication -- 3 Definitions -- 3.1 Quantum Copy Protection -- 3.2 Secure Software Leasing -- 3.3 Distributions for Point Functions -- 4 Generic Results on Definitions -- 4.1 Reusability of the Program -- 4.2 Malicious-Malicious Security and Correctness -- 4.3 Secure Software Leasing and Honest-Malicious Copy Protection -- 4.4 Secure Software Leasing of Compute-and-Compare Circuits -- 5 Authentication-Based Copy Protection Scheme -- 5.1 Construction and Correctness -- 5.2 Honest-Malicious Security -- References -- The Round Complexity of Quantum Zero-Knowledge -- 1 Introduction -- 2 Technical Overview -- 2.1 Witness-Indistinguishable Arguments -- 2.2 Zero Knowledge Arguments -- 2.3 Zero Knowledge in the Timing Model -- 2.4 Related Work -- 3 Preliminaries -- 3.1 Quantum Adversaries -- 3.2 Learning with Errors -- 3.3 Pseudorandom Functions -- 3.4 Interactive Proofs and Sigma Protocols -- 3.5 Statistical ZAPs for NP -- 3.6 Sometimes-Binding Statistically Hiding Commitments -- 3.7 Quantum One-Time Pad -- 3.8 Homomorphic Encryption -- 4 Witness-Indistinguishable Arguments for QMA -- 4.1 Definition -- 4.2 Statistically Zero-Knowledge Sigma Protocol -- 4.3 2-Round Witness-Indistinguishable Arguments for QMA.
References -- Rate-1 Quantum Fully Homomorphic Encryption -- 1 Introduction -- 1.1 Our Results -- 1.2 Related Work -- 2 Technical Overview -- 2.1 Malicious Circuit Privacy -- 2.2 Rate-1 Quantum Fully-Homomorphic Encryption -- 2.3 Putting Things Together -- 3 Preliminaries -- 3.1 Quantum Adversaries -- 3.2 Learning with Errors -- 3.3 Pauli Operators -- 3.4 Quantum One-Time Pad -- 4 Homomorphic Encryption -- 4.1 Classical Homomorphic Encryption -- 4.2 Quantum Homomorphic Encryption -- 5 Malicious Circuit Privacy for Quantum Computation -- 5.1 Semi-Honest Circuit Privacy -- 5.2 Our Bootstrapping Theorem -- 6 Rate-1 Quantum Fully Homomorphic Encryption -- 6.1 Definition -- 6.2 Our Construction -- References -- Unifying Presampling via Concentration Bounds -- 1 Introduction -- 1.1 Our Results -- 1.2 Open Problems -- 2 Preliminaries -- 2.1 Quantum Random Oracle Model -- 2.2 Compressed Oracle -- 2.3 Security Game with Classical Advice -- 2.4 Presampling Techniques for Random Oracles -- 2.5 Aaronson-Ambainis Conjecture -- 2.6 Concentration Bounds -- 3 Barriers for Leveraging Presampling Techniques -- 4 Unifying Presampling via Concentration Bounds -- 4.1 A New Characterization of Bit-Fixing -- 4.2 A Simpler Proof for Theorem 3 -- 5 Applications to AI-QROM -- 5.1 Presampling Techniques for Quantum Random Oracles -- 5.2 Post-quantum Non-

uniform Security of Merkle-Damgard Hash Functions (MDHF) -- 5.3 Post-quantum Non-uniform Security of One-Way Functions (OWF) -- References -- Quantum Key-Length Extension -- 1 Introduction -- 1.1 The FX Construction -- 1.2 Double Encryption -- 1.3 Overview -- 2 Preliminaries -- 2.1 Quantum Background -- 3 The FX Construction -- 3.1 Security of FX Against Non-adaptive Attacks -- 3.2 Adaptive Security of FFX -- 4 Double Encryption -- 4.1 Security Result -- 4.2 The Hardness of List Disjointness -- References.
Relationships Between Quantum IND-CPA Notions -- 1 Introduction -- 1.1 Previous Works -- 1.2 Our Contribution -- 1.3 Organization of the Paper -- 2 Preliminaries -- 3 Definitions -- 3.1 Syntax of l - The Learning Queries -- 3.2 Syntax of c - The Challenge Queries -- 3.3 Instantiation of Learning and Challenge Query Models -- 4 Decoherence Lemmas -- 5 Impossible Security Notions -- 6 Implications -- 7 Separations -- 7.1 Separations by Quasi-Length-Preserving Encryptions -- 7.2 Separations by Simon's Algorithm -- 7.3 Separations by Shi's SetEquality Problem -- 7.4 Separations by Other Arguments -- 8 Encryption Secure in All Notions -- References -- Classical Binding for Quantum Commitments -- 1 Introduction -- 1.1 Overview of Our Results and Techniques -- 1.2 Related Work -- 2 Preliminaries and Basic Tools -- 2.1 Quantum Formalism -- 2.2 Standard Tools -- 3 Classically Binding Quantum Commitments -- 3.1 Composition and Application -- 4 Construction -- 4.1 Split Classical Binding -- 4.2 Split Binding Amplification -- 4.3 SCBQC from Any One-Way Function -- 5 Classical Binding Is Impossible with Statistical Hiding -- References -- Unclonable Encryption, Revisited -- 1 Introduction -- 1.1 Our Work -- 1.2 Technical Overview -- 1.3 Structure of This Paper -- 2 Preliminaries -- 2.1 Notation -- 2.2 Quantum Computing -- 2.3 Post-Quantum Digital Signatures -- 2.4 Functional Encryption -- 2.5 Quantum Copy-Protection -- 2.6 Copy-Protection of Point Functions -- 3 Private-Key and Public-Key Unclonable Encryption: Definition -- 3.1 Unclonable Encryption -- 3.2 Private-Key and Public-Key Unclonable Encryption -- 4 Private-Key Unclonable Encryption (PK-UE) -- 4.1 Private-Key Encryption with Fake-Key Property -- 4.2 Construction -- 5 Public-Key Unclonable Encryption -- 5.1 Construction -- 6 Additional Results on Unclonable Encryption.
6.1 Generalized Conjugate Encryption -- 6.2 A Lower Bound for Conjugate Encryption -- 7 Construction of Copy-Protection from Unclonable Encryption -- References -- Somewhere Statistical Soundness, Post-Quantum Security, and SNARGs -- 1 Introduction -- 1.1 Multi-extractable Somewhere Statistically Binding (meSSB) Hash Families -- 1.2 Somewhere Statistically Sound (SSS) Interactive Arguments -- 1.3 SNARGs: From BatchNP to ¶ and Beyond -- 2 Preliminaries -- 2.1 Straight-Line Reductions -- 2.2 Probabilistically Checkable Proofs (PCP) -- 2.3 Hash Function Families with Local Opening -- 2.4 Kilian's Protocol -- 2.5 The BMW Heuristic -- 3 Somewhere Statistically Binding Hash Functions -- 3.1 Extractable Somewhere Statistically Binding (eSSB) Hash Functions -- 3.2 Multi-Extractable SSB (meSSB) Hash Functions -- 3.3 The BMW Protocol with meSSB Hash Families -- 4 Somewhere Statistically Sound Interactive Arguments -- 4.1 Defining SSS Arguments -- 4.2 SSS Implies Straight-Line Soundness -- 4.3 SSS Implies Post-Quantum Soundness -- 5 Kilian's Protocol Is Somewhere Statistically Sound -- 6 SNARG for Languages with Non-Signaling PCPs -- 6.1 BatchNP -- 6.2 SNARG for Languages with a Non-Signaling PCP -- A Proof of Theorem7 -- References -- Black-Box Impossibilities of Obtaining 2-Round Weak ZK and Strong WI from Polynomial Hardness -- 1 Introduction -- 1.1 Our Results -- 2 Our Techniques -- 2.1 BB Impossibility of 2-Round