1. Record Nr. UNISA996503468503316

Titolo	Theory of cryptography : 20th international conference, TCC 2022, Chicago, IL, USA, November 7-10, 2022, proceedings, Part III / / edited by Eike Kiltz and Vinod Vaikuntanathan
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2022] ©2022
ISBN	3-031-22368-3
Descrizione fisica	1 online resource (254 pages)
Collana	Lecture Notes in Computer Science ; ; v.13749
Disciplina	652.8
Soggetti	Cryptography Data encryption (Computer science)
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 III -- ORAM, OT and PIR -- Verifiable Private Information Retrieval -- 1 Introduction -- 1.1 Our Contribution -- 1.2 On the Round Complexity of vPIR -- 1.3 Open Questions -- 2 Technical Overview -- 2.1 vPIR for Local Properties -- 2.2 vPIR for Global Properties -- 3 Preliminaries -- 3.1 Private Information Retrieval -- 3.2 Batch Arguments -- 4 Verifiable PIR -- 4.1 Simulation Security -- 4.2 Local Security -- 5 From Batch Arguments to 1-Local vPIR -- 6 From 1-Local vPIR to vPIR with Constant Locality -- 7 From Local vPIR to Simulation Secure vPIR -- References -- Random-Index Oblivious RAM -- 1 Introduction -- 1.1 Random-Index ORAM -- 1.2 Applications -- 1.3 Our Contributions -- 2 Definitions -- 2.1 RORAM Security -- 2.2 Batch RORAM -- 3 Hierarchical RORAM -- 3.1 Protocol 1 - Future Randomness -- 3.2 Protocol 2 - Randomness -- 4 Tree-Based RORAM -- 4.1 A Class of Tree-RORAM Schemes -- 4.2 The Scheme that We Analyze -- 4.3 Bounding the Prediction Probability -- 5 Discussion and Future Directions -- 5.1 Hybrid ORAM/RORAM Schemes -- 5.2 Refreshing Keys in Large-Scale MPC -- 5.3 Improved Schemes and Analysis -- 5.4 From RORAM to ORAM -- 5.5 Miscellaneous -- A Hierarchical-RORAM: More Details -- B Tree-RORAM: More Details -- B.1 Analysis of the Optimal Strategy -- C Non-independence for a Tree-RORAM

Construction -- References -- On the Optimal Communication Complexity of Error-Correcting Multi-server PIR -- 1 Introduction -- 1.1 Our Results -- 1.2 Related Work -- 2 Technical Overview -- 2.1 Optimal Communication Complexity of Error-Correcting PIR -- 2.2 Instantiation of Our Transformation -- 3 Preliminaries -- 4 Private Information Retrieval (PIR) -- 4.1 Definitions -- 4.2 Robust PIR -- 4.3 Error-Correcting and Error-Detecting PIR -- 5 Transformation from Regular to Error-Detecting PIR.
5.1 Basic Transformation -- 5.2 General Transformation -- 6 Transformation from Error-Detecting to Error-Correcting PIR -- 7 Optimal Communication Complexity of Error-Correcting PIR -- 7.1 The Case of Perfect Error Correction -- 7.2 The Case of Statistical Error Correction -- 8 Instantiation of Our Transformation -- 8.1 Statistical Error-Correcting PIR Based on Homomorphic MAC -- A Definitions -- B Proof of Theorem2 -- C Proof of Lemma1 -- D Proof of Theorem3 -- E Proof of Theorem5 -- References -- .28em plus .1em minus .1emOblivious-Transfer Complexity of Noisy Coin-Toss via Secure Zero Communication Reductions -- 1 Introduction -- 2 Technical Overview -- 3 Preliminaries -- 3.1 Zero-Communication Secure Reductions -- 4 Balanced Embedding -- 5 SZCR from MPC Protocols -- A Basic Constructions -- A.1 Balanced Embedding from Truth Table -- A.2 Constructing Balanced Embedding from Circuit -- References -- Theory II -- One-Time Programs from Commodity Hardware -- 1 Introduction -- 1.1 Our Results -- 2 Technical Overview -- 2.1 Basic Protocol -- 2.2 Reducing the Number of Lockboxes -- 2.3 Reducing Lockboxes Using Laconic OT -- 2.4 Counter Lockboxes with Multiple Password Attempts -- 2.5 Related Work -- 3 Preliminaries -- 3.1 One-Time Programs -- 4 Counter Lockboxes -- 5 Leaky Batch-OT -- 5.1 Definition -- 5.2 Construction -- 6 Robust Garbling -- 6.1 Definitions -- 6.2 Construction -- 7 One-Time Program -- 8 Concrete Analysis -- 8.1 Number of Lockboxes -- 8.2 Instantiating Lockboxes -- 8.3 Applications -- References -- Universal Reductions: Reductions Relative to Stateful Oracles -- 1 Introduction -- 1.1 Universal Reductions in a Nut-shell -- 1.2 Formalizing Universal Reductions -- 1.3 On the Feasibility of Universal Reductions -- 1.4 Restricted Classes of Natures -- 1.5 Universal Reductions Imply Standard Reductions.
1.6 Conclusions, Related and Future Work -- 2 Overview of Techniques -- 2.1 The Dummy Lemma -- 2.2 Straightline Black-Box Reductions and Witness Indistinguishability -- 2.3 Impossibility of Hardness Amplification and Goldreich-Levin -- 2.4 Universal Reductions for Time-Evolving k-Window Natures, from Classical Non-adaptive Reductions -- 3 Defining Universal Reductions -- 3.1 Preliminaries -- 3.2 The Definition and Some Consequences -- References -- Permissionless Clock Synchronization with Public Setup -- 1 Introduction -- 1.1 Overview of Our Results -- 2 Model and Building Blocks -- 2.1 Imperfect Local Clocks -- 2.2 Other Core Functionalities -- 2.3 Dynamic Participation -- 3 The Clock Synchronization Protocol with Public Setup -- 3.1 Timekeeper Timestamps -- 3.2 2-for-1 Proofs of Work and Synchronization Beacons -- 3.3 Clock Synchronization Intervals and the Synchronization Procedure -- 3.4 The Target Recalculation Function -- 3.5 Newly Joining Parties -- 4 Protocol Analysis -- 4.1 Notation, Definitions and Preliminary Propositions -- 4.2 Protocol Parameters and Their Conditions -- 4.3 Typical Executions -- 4.4 Proof Roadmap -- A Glossary -- References -- Beyond Uber: Instantiating Generic Groups via PGGs -- 1 Introduction -- 1.1 Background -- 1.2 Our Approach -- 1.3 Applications of Pseudo-Generic Groups -- 1.4 Other Related Work and Discussions -- 1.5 Structure of the Paper -- 2 Preliminaries -- 3 Pseudo-Generic Groups