1. Record Nr. UNISA996503468703316

Titolo	Theory of cryptography : 20th international conference, TCC 2022, Chicago, IL, USA, November 7-10, 2022, proceedings, Part II / / edited by Eike Kiltz and Vinod Vaikuntanathan
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2023] ©2023
ISBN	3-031-22365-9
Descrizione fisica	1 online resource (813 pages)
Collana	Lecture Notes in Computer Science ; ; v.13748
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 II -- Encryption -- Forward-Secure Encryption with Fast Forwarding -- 1 Introduction -- 1.1 Basic Solutions and a New Dimension -- 1.2 Our Contributions -- 1.3 Related Work -- 2 Preliminaries -- 3 Fast-Forwarding in the Bulletin Board Model -- 3.1 Bulletin Board -- 3.2 Fast-Forwardable Stream Ciphers -- 3.3 Fast-Forwardable Updatable Public-Key Encryption -- 4 Constructing a Fast-Forwardable PRNG -- 4.1 The Basic Construction -- 4.2 Supporting an Unbounded Number of Epochs -- 5 Fast-Forwardable Updatable Public-Key Encryption -- 5.1 Update-Homomorphic UPKE -- 5.2 Update Graphs -- 5.3 A Generic Construction -- 6 Conclusions and Open Problems -- References -- Rate-1 Incompressible Encryption from Standard Assumptions -- 1 Introduction -- 1.1 Our Results -- 1.2 Comparison with Previous Work -- 2 Technical Overview -- 2.1 The Scheme of GWZ -- 2.2 The Big Picture -- 2.3 Rate-1 Incompressible Symmetric-Key Encryption -- 2.4 From Symmetric-Key to Public-Key Incompressible Encryption via Hash Proof Systems -- 2.5 Extension to CCA Security -- 3 Preliminaries -- 3.1 Decisional Diffie-Hellman Assumption -- 3.2 Public-Key Encryption -- 3.3 HILL-Entropic Encodings -- 4 Incompressible Symmetric-Key Encryption -- 4.1 Definition -- 4.2 Construction -- 5 Programmable Hash Proof Systems -- 5.1 Definitions -- 5.2 Programmable Hash Proof

System from DDH -- 5.3 2-Smooth Hash Proof System from DDH -- 6 Incompressible PKE from Incompressible SKE and HPS -- 6.1 CCA Incompressible Encryption -- 6.2 Construction -- References -- Achievable CCA2 Relaxation for Homomorphic Encryption -- 1 Introduction -- 2 Preliminaries -- 3 A Sufficient and Achievable Relaxation of CCA2 -- 3.1 funcCPA-Security: A Sufficient Relaxation of CCA2 -- 3.2 Sanitized HE Schemes are funcCPA-Secure -- 3.3 funcCPA Security of leveled HE Schemes.
3.4 Barriers on Proving funcCPA for Existing HE Schemes -- 4 CPA Insufficiency Against Malicious Adversaries -- 5 CPA Implies Privacy Against Semi-honest Adversaries -- 6 Conclusions -- A Proof of Lemma 2 -- References -- Multi-party Computation I -- Round-Optimal Honest-Majority MPC in Minicrypt and with Everlasting Security -- 1 Introduction -- 1.1 Our Contribution -- 2 Technical Overview -- 2.1 Main Theorem -- 2.2 Strong Honest-Majority MPC with Everlasting Security from OWF -- References -- Sublinear Secure Computation from New Assumptions -- 1 Introduction -- 1.1 Our Results -- 2 Technical Overview -- 2.1 Sublinear 2PC for Layered Circuits from Decomposable Batch OT -- 2.2 Polylogarithmic PIR from CDH -- 3 Sublinear Computation for loglog-Depth Circuits -- 3.1 Decomposable Two-Round Batch Oblivious Transfer -- 3.2 Instantiation Under QR +LPN, Adapted from ch5EC:BBDP22 -- 3.3 Bounded Query Repetitions -- 3.4 Two-Round Batch SPIR with Correlated Queries -- 3.5 Sublinear Computation of loglog-Depth Circuits from corrSPIR -- 3.6 Extension to Layered Circuits -- 4 Polylogarithmic PIR from CDH -- 4.1 Laconic Private Set Intersection -- 4.2 From Laconic PSI to Half-PIR -- 4.3 From Polylogarithmic Half-PIR to Polylogarithmic PIR -- References -- How to Obfuscate MPC Inputs -- 1 Introduction -- 1.1 Overview of Our Results -- 1.2 Related Work -- 2 Preliminaries -- 2.1 Idealized Models -- 2.2 Obfuscation -- 3 Defining io2PC -- 3.1 Simulation Rate -- 3.2 Server Compromise and Offline Evaluation -- 3.3 Preventing Precomputation -- 4 io2PC for Random-Oracle-Model Obfuscation -- 4.1 Oblivious PRF -- 4.2 io2PC Protocol -- 5 io2PC for Generic-Group Obfuscations -- 5.1 Generic Groups -- 5.2 Personalized Generic Group -- 5.3 Protocol for Personalized Generic Groups -- 5.4 io2PC Protocol for Generic-Group Obfuscation -- 6 Compatible Obfuscations.
6.1 Point Functions -- 6.2 Hyperplane Membership -- References -- Statistical Security in Two-Party Computation Revisited -- 1 Introduction -- 1.1 Our Contributions -- 2 Technical Overview -- 2.1 One-Sided Statistical Two-Party Computation Protocol -- 2.2 Constructing Our Ingredients from eOT -- 3 Preliminaries -- 3.1 Notations -- 3.2 Oblivious Transfer Protocols -- 3.3 Additional Preliminaries -- 4 Three Round Oblivious Transfer Protocols -- 4.1 Statistically Receiver Private Indistinguishability-Based OT -- 4.2 Three Round Statistically Sender Private OT -- 5 One-Sided Statistically Secure 2PC Against Explainable Parties -- 5.1 Protocol exp -- 5.2 Two Round Statistically Hiding Commitment -- 6 One-Sided Statistically Secure 2PC Against Malicious Corruptions -- 6.1 Conditional Disclosure of Secrets in the Preprocessing Model -- 6.2 Protocol mal -- 7 Instantiations of eOT -- References -- Protocols: Key Agreement and Commitments -- On the Worst-Case Inefficiency of CGKA -- 1 Introduction -- 1.1 Our Results -- 1.2 Compact Key Exchange -- 1.3 Standard Security of Continuous Group Key Agreement -- 1.4 Equivalence of CKE and CGKA Worst-Case Communication Complexity -- 1.5 Black-Box Compact Key Exchange Lower Bound -- 1.6 No Single Optimal CGKA Protocol Exists -- 1.7 Lessons Learned for Practice -- 2 Definitions -- 2.1 Continuous Group Key Agreement -- 2.2 Compact Key Exchange -- 3 From CGKA to CKE Tightly -- 3.1 Embedding CGKA

Ciphertexts in CKE Ciphertexts -- 4 CKE Lower Bound from PKE -- 4.1 Proof Outline -- 4.2 Attack for (CRSGeng, Initg, Comme, Derived) -- 5 No Single Optimal CGKA Protocol Exists -- 5.1 Bad Sequences of Operations -- 5.2 Suboptimality of All CGKA Protocols -- References -- Adaptive Multiparty NIKE -- 1 Introduction -- 1.1 Prior Work and Motivation -- 1.2 Technical Challenges -- 1.3 Result Summary -- 1.4 Technical Overview.
1.5 Organization -- 2 Preliminaries -- 2.1 Multiparty NIKE -- 2.2 Constrained PRFs -- 3 Enhancing Multi-party NIKE -- 3.1 Achieving Adversarial Correctness -- 3.2 Removing the CRS -- 3.3 Adding Shared Key Queries -- 3.4 Putting It All Together -- 4 The Equivalence of Multiparty NIKE and 1-SF-PRF -- 4.1 From 1-SF-PRF to Special Constrained PRF -- 4.2 From Special Constrained PRF to Multiparty NIKE with Setup -- 5 Construction of 1-SF-PRFs -- 5.1 Construction -- 5.2 Security Proof -- References -- On the Impossibility of Algebraic Vector Commitments in Pairing-Free Groups -- 1 Introduction -- 1.1 Our Results -- 1.2 Our Techniques -- 1.3 Interpretation of Our Impossibility and Further Implications -- 1.4 Related Work -- 1.5 Organization of the Paper -- 2 Preliminaries -- 2.1 Vector Commitments -- 2.2 Digital Signatures -- 3 Algebraic Vector Commitments -- 3.1 Generic Transformation from VCs to Signatures -- 3.2 -Unforgeability -- 4 Algebraic Signatures -- 4.1 Attack to Schemes with Strictly Linear Verification -- 4.2 Attack to Schemes with Generic Verification -- 5 Conclusions -- 5.1 Impossibility of Algebraic Vector Commitments -- 5.2 Impossibility of Algebraic Signatures -- References -- Four-Round Black-Box Non-malleable Schemes from One-Way Permutations -- 1 Introduction -- 1.1 Our Contributions -- 2 Overview of Techniques -- 2.1 Our NMZKC Protocol and New Commitment Schemes -- 2.2 4-Round Non-malleable Commitment nmc -- 3 Preliminaries -- 3.1 Commitment Schemes -- 3.2 Non-malleable Commitments -- 3.3 -Commitments -- 3.4 Adaptive-Input SHVZK -- 3.5 One-of-Two Binding Commitments -- 3.6 MPC Definitions -- 3.7 Verifiable Secret Sharing (VSS) -- 4 Non-malleable HVZK with Respect to Commitment -- 5 Our Delayed-Input MPC-in-the-Head Protocol AI -- 6 The Building Blocks of the 4-Round Black-Box Non-malleable Commitment Scheme.
6.1 Commitment from Verifiable Secret Sharing -- 6.2 Commit-and-Prove -- 6.3 The 4-Round Non-malleable Commitment Scheme of ch11FOCS:GRRV14 -- 7 Our 4-Round Black-Box Non-malleable Commitment Scheme -- 7.1 Formal Description of nmc = ((Snmc , Rnmc), Decnmc) -- 8 Comparison with Previous Non-black-box Approaches to Four-Round Non-malleable Commitments -- References -- Theory I: Sampling and Friends -- A Tight Computational Indistinguishability Bound for Product Distributions -- 1 Introduction -- 1.1 Related Work -- 1.2 Organization -- 2 Definitions -- 2.1 Notation -- 3 The Non-uniform Bounds and Tightness -- 3.1 The N-Fold Case -- 3.2 Tightness -- 4 The Uniform Variant -- 5 Applications -- 6 Open Questions -- References -- Secure Sampling with Sublinear Communication -- 1 Introduction -- 1.1 Our Work -- 1.2 Technical Overview -- 1.3 Related Work -- 2 Two-Party L1 Sampling -- 2.1 A Toy Protocol Towards Securely Realizing FL1 -- 2.2 Secure L1 Sampling Protocol -- 3 Two Party L2 Sampling -- 3.1 A Non-private L2 Sampling Protocol with (1) Communication -- 3.2 Secure L2 Sampling from FHE -- 3.3 A Non-private Lp Sampling Protocol with (1) Communication -- 4 Two-Party Product Sampling -- 4.1 Impossibility of Sublinear Product Sampling -- 4.2 Product Sampling While Leaking at Most the Inner Product -- 5 Product Sampling in Constant Rounds -- 5.1 Secure Approximation of the Inner Product -- 5.2 Constant-Round Protocol

for Product Sampling -- References -- Secure Non-interactive Simulation from Arbitrary Joint Distributions -- 1 Introduction -- 2 Overview of Our Contributions -- 2.1 Overview of Our Results -- 2.2 Overview of Our Technical Contributions -- 3 Preliminaries -- 3.1 Notation -- 3.2 Maximal Correlation -- 3.3 Fourier Analysis Basics -- 3.4 Markov Operator -- 3.5 Efron-Stein Decomposition -- 3.6 Imported Theorems.
4 Characterization of SNIS from Arbitrary Sources.