1.

Record Nr.	UNINA9910508455303321
Titolo	Theory of cryptography : 19th international conference, TCC 2021, Raleigh, NC, USA, November 8-11, 2021, proceedings, part II / / edited by Kobbi Nissim and Brent Waters
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2021] ©2021
ISBN	3-030-90453-9
Descrizione fisica	1 online resource (764 pages)
Collana	Lecture Notes in Computer Science ; ; v.13043
Disciplina	005.824
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 II -- Dory: Efficient, Transparent Arguments for Generalised Inner Products and Polynomial Commitments -- 1 Introduction -- 1.1 Limitations of Prior Approaches -- 1.2 Review of LCC-DLOG Techniques -- 1.3 Core Techniques Enabling a Logarithmic Verifier in Dory -- 2 Preliminaries -- 2.1 Notation -- 2.2 Computationally Hard Problems in Type III Pairings -- 2.3 Succinct Interactive Arguments of Knowledge -- 2.4 Commitments -- 2.5 Polynomial Commitments and Evaluation from Vector-Matrix-Vector Products -- 3 An Inner-Product Argument with a Logarithmic Verifier -- 3.1 Scalar-Product -- 3.2 Dory-Reduce -- 3.3 Dory-Innerproduct -- 3.4 Batching Inner Products -- 4 Inner Products with Public Vectors of Scalars -- 4.1 General Reduction with O (n) cost -- 4.2 Extending Dory-Reduce -- 4.3 Extending Dory-Innerproduct -- 4.4 Extending Batch-Innerproduct -- 5 Vector-Matrix-Vector Products -- 5.1 Batching -- 5.2 Concrete Costs -- 6 Dory-PC -- 6.1 Concrete Costs of Dory-PC-RE -- 6.2 Batching -- 7 Implementation -- References -- On Communication-Efficient Asynchronous MPC with Adaptive Security -- 1 Introduction -- 1.1 Communication Complexity of Asynchronous MPC Protocols -- 1.2 Contributions -- 2 Preliminaries -- 2.1 Communication and Adversary Model -- 2.2 Zero-Knowledge Proofs of Knowledge -- 2.3 Universally Composable Commitments --

2.4 Threshold Homomorphic Encryption -- 3 Subprotocols -- 3.1 Agreement Protocols -- 3.2 Decryption Protocols -- 3.3 Multiplication -- 3.4 Triple Generation -- 4 Asynchronous Adaptively Secure MPC Protocol -- 4.1 Ideal Functionality -- 4.2 Informal Explanation of the Protocol -- 4.3 Main Theorem -- 5 Near-Linear MPC in the Atomic Send Model -- 5.1 Model -- 5.2 VACS -- 5.3 Triple Generation -- 5.4 Main Theorem for the Atomic Send Model -- A Details of the Subprotocols.

A.1 Decryption protocols -- A.2 Multiplication -- B Protocol -- References -- Efficient Perfectly Secure Computation with Optimal Resilience -- 1 Introduction -- 1.1 Our Results -- 1.2 Related Work -- 1.3 Open Problems -- 2 Technical Overview -- 2.1 Overview of the BGW Protocol -- 2.2 Our Protocol -- 2.3 Extensions -- 2.4 Organization -- 3 Preliminaries -- 3.1 Definitions of Perfect Security in the Presence of Malicious Adversaries -- 3.2 Robust Secret Sharing -- 3.3 Bivariate Polynomial -- 4 Weak Verifiable Secret Sharing and Extensions -- 4.1 Verifying Shares of a (q,t)-Bivariate Polynomial -- 4.2 Weak Verifiable Secret Sharing -- 4.3 Evaluation with the Help of the Dealer -- 4.4 Strong Verifiable Secret Sharing -- 4.5 Extending Univariate Sharing to Bivariate Sharing with a Dealer -- 5 Multiplication with a Constant Number of VSSs and WSSs -- 5.1 Functionality - Multiplication with a Dealer -- 5.2 The Protocol -- 6 Extension: Arbitrary Gates with Multiplicative Depth-1 -- References -- On Communication Models and Best-Achievable Security in Two-Round MPC -- 1 Introduction -- 1.1 Our Results in Detail -- 1.2 Related Work -- 2 Technical Overview -- 2.1 Lower Bounds in the BC only Model -- 2.2 BC+P2P Model -- 2.3 BC+PKI Model -- 3 Preliminaries -- 3.1 Oblivious Transfer (OT) -- 3.2 Multi-CRS Non-interactive Zero Knowledge (m-NIZK) -- 4 Broadcast Model -- 4.1 Lower Bound for t=1 -- 4.2 Impossibility of Two-Message mR-OT in the Plain Model -- 5 BC+P2P Model -- 5.1 Impossibility Result for Identifiable Result -- 5.2 Fail-Stop Guaranteed Output Delivery -- 6 BC+PKI Model: Guaranteed Output Delivery -- References -- Generalized Pseudorandom Secret Sharing and Efficient Straggler-Resilient Secure Computation -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Work -- 2 Preliminaries -- 2.1 Threshold Secret Sharing.

2.2 Computation Model: Layered Straight-Line Programs -- 3 Generalized Pseudorandom Secret Sharing -- 3.1 Overview -- 3.2 The Gilboa-Ishai Framework -- 3.3 Technical Tool: Covering Designs -- 3.4 Generalized PRSS for Degree-d Polynomials -- 3.5 Double Shamir Sharing -- 3.6 Beyond Double Sharing -- 4 Constructions for Semi-honest Security -- 4.1 Baseline Protocol (with =1) -- 4.2 Straggler Resilience -- 4.3 Reducing Communication and Computation -- 5 From Semi-honest to Malicious Security -- 5.1 Privacy in the Presence of Malicious Adversaries -- 5.2 Verifying Correctness of the Computation -- 5.3 Putting It All Together - The Main Protocol -- References -- Blockchains Enable Non-interactive MPC -- 1 Introduction -- 1.1 Our Results -- 1.2 Technical Overview -- 1.3 Related Work -- 2 Preliminaries - CSaRs -- 3 Our Non-interactive MPC Construction -- 3.1 Construction Overview -- 4 Optimizations -- 5 Optimizing Communication and State Complexity in MPC -- 5.1 Step. 1: MPC with Semi-malicious Security -- 5.2 Step. 2: MPC with Fully Malicious Security -- 5.3 Properties of the Resulting MPC Construction -- 6 Guaranteed Output Delivery -- References -- Multi-party PSM, Revisited: -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Proof Overview -- 1.3 Related Works -- 2 Preliminaries -- 2.1 Tensor -- 2.2 Private Simultaneous Messages -- 2.3 Randomized Encoding -- 3 New Multi-party PSM Protocols -- 3.1 A Framework for Multi-party PSM --

3.2 The Induced PSM Protocol -- 3.3 When k is Small -- 3.4 When k+1 is a Prime Power -- 4 Unbalanced 2-Party PSM Protocols -- 4.1 A Framework for 2-Party PSM -- 4.2 The Induced PSM Protocol -- 4.3 When Has a Small Denominator -- 5 Open Problems -- A Proof of Eq. (9) and (10) -- B Auxiliary PSM Protocols for "426830A x1 …xk, Y "526930B + s -- B.1 The Multi-party Variant -- B.2 The 2-party Variant -- References.

Multi-Party Functional Encryption -- 1 Introduction -- 1.1 Unifying the View: Multi-Party Functional Encryption -- 1.2 Comparison with Prior Work -- 1.3 New Constructions -- 1.4 Technical Overview -- 1.5 Predicting New and Useful Primitives via MPFE -- 2 Multi-Party Functional Encryption -- 3 Multi-Authority ABE IPFE for LSSS Access Structures -- 3.1 Specializing the MPFE Syntax -- 3.2 Construction -- 3.3 Correctness and Security -- 4 Function-Hiding DDFE for Inner Products -- 4.1 Specializing the MPFE Syntax -- 4.2 Construction of Function-Hiding IP-MCFE -- 4.3 Construction of Function-Hiding IP-DDFE -- References -- Succinct LWE Sampling, Random Polynomials, and Obfuscation -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Technical Overview -- 1.3 Discussion -- 2 Preliminaries -- 2.1 Notations -- 2.2 Learning with Errors -- 2.3 Lattice Tools -- 2.4 Homomorphic Operations -- 2.5 Succinct Randomized Encodings -- 3 Succinct LWE Sampler: Definition and Amplification -- 3.1 Definition and Discussion -- 3.2 Weak Succinct LWE Samplers -- 3.3 Amplification -- 4 Candidate Succinct LWE Sampler -- 4.1 A Basic Framework -- 4.2 Correctness, Succinctness, and LWE with Respect to A* -- 4.3 Instantiating the Parameters -- 4.4 Alternate Candidate Construction -- 4.5 Cryptanalysis -- 4.6 Cryptanalytic Challenges -- 5 Our Succinct Randomized Encoding Construction -- 5.1 Security -- References -- ABE for DFA from LWE Against Bounded Collusions, Revisited*-8pt -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Technical Overview I: T1/2 -- 1.3 Technical Overview II: ABE for DFA -- 1.4 Prior Works -- 1.5 Discussion -- 2 Preliminaries -- 2.1 Attribute-Based Encryption -- 2.2 Lattices Background -- 3 Trapdoor Sampling with T1/2 and a Computational Lemma -- 3.1 LWE Implies T1/2-LWE -- 3.2 Trapdoor Sampling with T1/2 -- 4 ABE for DFA Against Bounded Collusions.
4.1 Our Scheme -- 4.2 sk-Selective Security -- 5 Candidate ABE for DFA Against Unbounded Collusions -- References -- Distributed Merkle's Puzzles -- 1 Introduction -- 1.1 Distributed Key Agreement Based on Symmetric-Key Primitives -- 1.2 Our Results -- 1.3 Overview of the Protocol and Its Analysis -- 1.4 Previous Work -- 2 Preliminaries -- 2.1 Graphs -- 2.2 Random Functions and Encryption -- 3 Distributed Key Agreement Protocols Based on Random Oracles -- 4 The Setup Protocol -- 4.1 Correctness -- 4.2 Query and Communication Complexity -- 4.3 Connectivity -- 4.4 Security -- 5 The Distributed Key Agreement Protocol -- 5.1 Security Analysis -- 5.2 Main Theorem -- 6 Optimality of the Distributed Key Agreement Protocol -- 7 Extensions -- 7.1 The Semi-honest Model -- 7.2 Communication-Security Tradeoff -- References -- Continuously Non-malleable Secret Sharing: Joint Tampering, Plain Model and Capacity -- 1 Introduction -- 1.1 Non-malleability Against Joint Tampering -- 1.2 Our Results -- 1.3 Overview of Techniques -- 1.4 Related Work -- 2 Standard Definitions -- 2.1 Non-interactive Commitment Schemes -- 2.2 Symmetric Encryption -- 2.3 Information Dispersal -- 3 Secret Sharing Schemes -- 3.1 Tampering and Leakage Model -- 3.2 Related Notions -- 4 Rate-Zero Continuously Non-malleable Secret Sharing -- 4.1 Induction Basis -- 4.2 Inductive Step -- 4.3 Putting It Together -- 5 Rate Compilers and Capacity Upper Bounds -- 5.1 Capacity Upper Bounds -- 5.2 Rate Compiler (Plain Model) -- 6 Instantiations -- 6.1