1.	Record Nr.	UNINA9910741190003321
	Titolo	Advances in Cryptology – CRYPTO 2023 : 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20–24, 2023, Proceedings, Part I / / edited by Helena Handschuh, Anna Lysyanskaya
	Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2023
	ISBN	3-031-38557-8
	Edizione	[1st ed. 2023.]
	Descrizione fisica	1 online resource (XIX, 776 p. 99 illus., 26 illus. in color.)
	Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14081
	Disciplina	005.824
	Soggetti	Cryptography Data encryption (Computer science) Computer engineering Computer networks Computer networks—Security measures Coding theory Information theory Cryptology Computer Engineering and Networks Mobile and Network Security Coding and Information Theory
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di contenuto	Intro -- Preface -- Organization -- Contents - Part I -- Consensus, Secret Sharing, and Multi-party Computation -- Completeness Theorems for Adaptively Secure Broadcast -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Work -- 2 Preliminaries -- 2.1 The Model -- 2.2 Simulation-Based Security -- 2.3 Time-Lock Puzzles -- 3 Broadcast Protocols: Definitions -- 3.1 Property-Based Broadcast -- 3.2 Simulation-Based Broadcast -- 4 Property-Based Adaptively Secure Broadcast -- 4.1 Impossibility of Property-Based Adaptively Secure Broadcast -- 4.2 Property-Based Adaptively Secure Broadcast Protocol -- 5 Simulation-Based Adaptively Secure Broadcast -- 5.1 Impossibility

of Simulation-Based Adaptively Secure Broadcast -- 5.2 Simulation-Based Adaptively Secure Broadcast Protocol -- References -- Bingo: Adaptivity and Asynchrony in Verifiable Secret Sharing and Distributed Key Generation -- 1 Introduction -- 1.1 Technical Overview -- 1.2 Related Work -- 2 Definitions -- 2.1 Preliminaries -- 2.2 Polynomial Commitments -- 2.3 Reliable Broadcast -- 2.4 Packed Asynchronous Verifiable Secret Sharing (PAVSS) -- 3 A Bivariate Polynomial Commitment Scheme -- 3.1 Construction -- 3.2 Commitment and Proof Interpolation -- 4 Bingo: Packed Asynchronous Verifiable Secret Sharing -- 4.1 Design -- 4.2 Security -- 4.3 Efficient Reconstruction -- 5 From Bingo to ADKG -- References -- Network-Agnostic Security Comes (Almost) for Free in DKG and MPC -- 1 Introduction -- 1.1 Background and Starting Point -- 1.2 Technical Overview: DKG -- 1.3 Technical Overview: MPC -- 1.4 Related Work -- 1.5 Paper Organisation -- 2 Preliminaries and Definitions -- 2.1 Cryptographic Primitives -- 2.2 Distributed Primitives -- 2.3 Multi-party Computation -- 3 Communication-Efficient Synchronous Broadcast -- 3.1 Short Message Broadcast Module -- 3.2 Broadcast Extension Protocol.

4 Multivalued Intrusion-Tolerant Consensus -- 5 Communication-Efficient Network-Agnostic DKG -- 6 Multi-party Computation with Asynchronous Fallback -- 6.1 Protocol Compiler -- References -- Practical Settlement Bounds for Longest-Chain Consensus -- 1 Introduction -- 2 Preliminaries and Model -- 2.1 Modeling Blockchains with Network Delay -- 2.2 Ledger Consensus -- 3 Proof-of-Work Settlement -- 3.1 Proof-of-Work Blocktrees -- 3.2 PoW Characteristic Quantity: Margin () -- 3.3 Main PoW Theorem -- 3.4 Existing Tools: Tree Compression and the PoW Restructuring Lemma -- 3.5 Outside of the Critical Region -- 3.6 The Critical Region -- 4 Proof-of-Stake Settlement -- 4.1 Proof-of-Stake Blocktrees -- 4.2 PoS Characteristic Quantities: Reach () and Margin () -- 4.3 Main PoS Theorem -- 4.4 Bounding Reach -- 4.5 Bounding Margin -- 4.6 Crossing Zero -- 4.7 A Practical PoS Adversary -- 5 Numerical Evaluation -- 5.1 Modeling the Slot Leader Distribution -- 5.2 Symbol Distribution in a Phase -- 5.3 Evaluating the Recurrence -- 5.4 Numerical Results -- 6 Conclusions: Practical Relevance -- References -- New Bounds on the Local Leakage Resilience of Shamir's Secret Sharing Scheme -- 1 Introduction -- 1.1 Our Results -- 1.2 Related Work -- 1.3 Main Techniques -- 2 Preliminaries -- 2.1 Coding and Secret Sharing -- 2.2 Entropy and Distances -- 2.3 Leakage Resilient Secret Sharing -- 2.4 Fourier Analysis -- 3 Main Analytical Framework -- 4 Leakage Resilience for -- 5 Balanced Leakage Resilience for -- 6 Unbalanced Leakage Resilience for -- 6.1 A Barrier of Previous Methods -- A Proof of Claim 4.5 -- B Details for a Barrier of Previous Methods -- References -- Arithmetic Sketching -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Work -- 2 A Formalization of Arithmetic Sketching Schemes -- 2.1 Overview -- 2.2 Formal Definitions -- 2.3 Zero Knowledge.

3 Sketching via Algebraic Manipulation Detection -- 3.1 Definition -- 3.2 From AMD Distributions to Sketching Schemes -- 3.3 Constructing AMD Distributions from Algebraic Varieties -- 3.4 New Sketching Schemes for Weight-One Vectors -- 3.5 A Sketch with 1/| F |2 Soundness for Binary Weight 1 -- 4 Sketching for Low-Weight Vectors -- 4.1 Refined Definitions: Arithmetic sketching with Private Decision -- 4.2 Weight-w Vectors with Arbitrary Payload -- 4.3 Sketching for Vectors with L1 Norm w -- 4.4 Bounded-Weight Vectors with Arbitrarily Restricted Payloads -- 5 From Arithmetic Sketching to Client-Server Protocols -- 6 Lower Bound on Sketch Size -- 7 Languages Without Arithmetic Sketching Schemes -- 7.1 Lp Norm -- 7.2 Specified Value in Arbitrary Vector -- 7.3 Intervals -- 8 Open Questions -- References --

Additive Randomized Encodings and Their Applications -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Open Questions -- 1.3 Related Work -- 2 Overview of Techniques -- 2.1 Information-Theoretic ARE -- 2.2 Computational ARE -- 2.3 Robust ARE -- 2.4 Applications -- 3 Additive Randomized Encoding: Definitions and Properties -- 3.1 ARE Security -- 3.2 Basic Properties of ARE -- 4 Information-Theoretic ARE -- 4.1 ARE for Capped Sum -- 4.2 Negative Results for Perfectly Secure ARE -- 5 Computational ARE from Bilinear Maps -- 5.1 A Pairing-Based Two-Party Equality Scheme -- 5.2 From Equality to Any Small Function -- 5.3 Computational ARE for General Functions -- 6 From ARE to Multiparty Randomized Encoding -- References -- How to Recover a Secret with O(n) Additions -- 1 Introduction -- 1.1 Motivation -- 1.2 Our Results -- 1.3 Technical Overview -- 1.4 A Practical Instantiation -- 1.5 Related Work -- 2 Preliminaries -- 2.1 Secret Sharing: Definitions -- 2.2 Additive-Only Algorithms and BBSS -- 2.3 Additive-Only Erasure Codes -- 3 The Basic Construction.

3.1 Privacy Lemmas -- 3.2 Immediate Corollaries -- 4 Analyzing the Basic Construction over All Primes Simultaneously -- 5 Deriving Near-Threshold Schemes -- References -- On Linear Communication Complexity for (Maximally) Fluid MPC -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Related Work -- 2 Technical Overview -- 2.1 Our Starting Point: Le Mans ch9rachuri2021mans -- 2.2 The ``King Idea'' in the Fluid Setting -- 2.3 Fluid Honest Majority MPC with Linear Communication -- 2.4 Technical Overview of SMT Lower Bound -- 3 Security Model and Preliminaries -- 3.1 Modelling Fluid MPC -- 3.2 Security Model -- 3.3 Preliminaries -- 4 Honest Majority -- 4.1 Efficient Resharing for Honest Majority -- 4.2 Incremental Checks -- 4.3 Secure Multiplication -- 4.4 Honest Majority Protocol -- 5 Dishonest Majority Preprocessing Size Is Tight -- 5.1 Secure Message Transmission with Two Committees -- 5.2 Lower Bound on Per-Party Preprocessing for Linear SMT -- References -- Cryptography with Weights: MPC, Encryption and Signatures -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Related Work -- 2 Technical Overview -- 2.1 Challenges in Using the WRSS Scheme -- 2.2 Weighted Threshold Encryption -- 2.3 Weighted MPC -- 2.4 Weighted Threshold Signature -- 3 Preliminaries -- 4 Efficient Weighted Ramp Secret-Sharing Scheme -- 4.1 Unweighted CRT-Based Secret-Sharing -- 4.2 Realizing Efficient WRSS Using CRT-Based Secret-Sharing -- 5 Efficient Weighted MPC -- 5.1 Generating Shares of Random Value FRandom -- 5.2 Degree Reduction Protocol Fdeg -- 5.3 Opening Secret Shares Fopen -- 5.4 Realizing Negation Gate Fneg -- 5.5 Our Protocol -- 6 Efficient Weighted Threshold Encryption Scheme -- 6.1 Building Blocks -- 6.2 Our Construction -- 7 Efficient Weighted Threshold Signature -- 7.1 ECDSA Signatures -- References -- Best of Both Worlds -- 1 Introduction -- 1.1 Our Contributions.

1.2 Related Work -- 1.3 Technical Overview -- 2 Preliminaries -- 3 MPC with Fall-Back Security -- 3.1 Example Protocol with Semi-Honest Fall-Back Security -- 4 Compiling to Semi-Honest Fall-Back Security -- 5 MPC with Fall-Back Security - Malicious Security -- 5.1 Authenticated Triples Generation -- 5.2 Authenticated Triples with Semi-Honest Fall-Back Security -- 5.3 Commitment Protocols with Fall-Back Security -- 5.4 Malicious Fall-Back Secure Protocol for Authenticated Triples -- References -- Perfect MPC over Layered Graphs -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Work -- 1.3 Technical Overview -- 2 Preliminaries -- 2.1 Layered MPC -- 2.2 Adaptivity and Composability in Layered MPC -- 3 Basic Primitives -- 3.1 Future Messaging -- 3.2 Multiparty Addition -- 4 Layered MPC Based on CNF

Secret Sharing -- 4.1 Future Multicast -- 4.2 Verifiable Secret Sharing -- 4.3 Multiplication -- 4.4 Realizing MPC from Layered Multiplication and Addition -- 5 Efficient Layered MPC -- 5.1 Verifiable Shamir Secret Sharing -- 5.2 Multiplication -- 5.3 MPC -- 6 Computational Efficient Layered MPC for t&lt -- n/2 -- References -- Round-Optimal Black-Box MPC in the Plain Model -- 1 Introduction -- 1.1 Related Work -- 2 Technical Overview -- 2.1 Instantiating the IPS Compiler with Three-Round Watchlist -- 2.2 Constructing Three-Round Watchlists with Promise Extraction -- 2.3 Constructing Three-Round 2PC with Special Extraction -- 3 Preliminaries -- 3.1 3-Round Two-Party Computation Protocol with Special Extraction -- 4 The Watchlist Protocol -- 4.1 Definitions -- 4.2 Construction -- 5 4-Round Black-Box MPC Protocol -- 5.1 Building Blocks -- References -- Reusable Secure Computation in the Plain Model -- 1 Introduction -- 1.1 Our Results -- 2 Technical Overview -- 2.1 Reusable Two-Party Computation -- 2.2 Reusable MPC -- 3 Preliminaries.
3.1 Reusable Secure Two-Party Computation Protocol.

Sommario/riassunto

The five-volume set, LNCS 14081, 140825, 14083, 14084, and 14085 constitutes the refereed proceedings of the 43rd Annual International Cryptology Conference, CRYPTO 2023. The conference took place at Santa Barbara, USA, during August 19-24, 2023. The 124 full papers presented in the proceedings were carefully reviewed and selected from a total of 479 submissions. The papers are organized in the following topical sections: Part I: Consensus, secret sharing, and multi-party computation; Part II: Succinctness; anonymous credentials; new paradigms and foundations; Part III: Cryptanalysis; side channels; symmetric constructions; isogenies; Part IV: Faster fully homomorphic encryption; oblivious RAM; obfuscation; secure messaging; functional encryption; correlated pseudorandomness; proof systems in the discrete-logarithm setting. .