1. Record Nr. UNINA9910574057603321

Titolo	Advances in Cryptology – EUROCRYPT 2022 : 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 – June 3, 2022, Proceedings, Part I / / edited by Orr Dunkelman, Stefan Dziembowski
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2022
ISBN	3-031-06944-7
Edizione	[1st ed. 2022.]
Descrizione fisica	1 online resource (842 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 13275
Disciplina	005.824
Soggetti	Cryptography Data encryption (Computer science) Cryptology
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 -- Abstracts of Invited Talks -- Hardware: An Essential Partner to Cryptography -- Symmetric Cryptography for Long Term Security -- Contents - Part I -- Contents - Part II -- Contents - Part III -- Best Paper Award -- EpiGRAM: Practical Garbled RAM -- 1 Introduction -- 1.1 Contribution -- 2 Technical Overview -- 2.1 The Language Translation Problem -- 2.2 Lazy Permutations -- 2.3 Pattern-Leaking (Leaky) Arrays -- 2.4 Garbled RAM -- 3 Related Work -- 4 Preliminaries, Notation, and Assumptions -- 4.1 Common Notation -- 4.2 Cryptographic Assumptions -- 4.3 Garbling Schemes -- 4.4 Garblings and Sharings -- 4.5 Oblivious Permutation -- 5 Approach -- 5.1 Avoiding Factor Blowup -- 5.2 Pop-only Oblivious Stacks -- 5.3 Lazy Permutations -- 5.4 Our GRAM -- 6 Evaluation -- References -- Secure Multiparty Computation -- Garbled Circuits with Sublinear Evaluator -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Garbled PIR -- 1.3 Compact 2PC and Garbled PIR -- 1.4 High-Level Intuition for Our Approach -- 2 Related Work -- 3 Preliminaries -- 3.1 Reducing GC Communication -- 3.2 Universal and Set-Universal Circuits -- 3.3 Garbled Circuit Formalization -- 3.4 Circuit Syntax -- 4 Technical Overview -- 5 Our Construction -- 5.1

Bucket Table Gadget -- 5.2 Demultiplexer and Multiplexer -- 5.3 Our Garbling Scheme -- 6 Security -- 6.1 Proofs -- References -- Round-Optimal and Communication-Efficient Multiparty Computation -- 1 Introduction -- 1.1 Related Work -- 1.2 Overview of Our Results -- 2 Technical Overview -- 3 Preliminaries -- 3.1 Functional Encryption -- 3.2 Decomposable Functional Encryption Combiner -- 3.3 Multi Key Fully Homomorphic Encryption -- 3.4 Secure Multiparty Computation -- 4 k-Delayed-Input Function MPC -- 5 Our Compiler: Circuit-Scalable MPC -- 6 Our Compiler: Circuit-Independent MPC -- References.
Round-Optimal Byzantine Agreement -- 1 Introduction -- 1.1 Technical Overview -- 1.2 Related Work -- 2 Model and Definitions -- 2.1 Communication and Adversary Model -- 2.2 Cryptographic Primitives -- 2.3 Agreement Primitives -- 3 Expand-and-Extract Paradigm -- 4 Conditional Graded Broadcast -- 5 Round-Optimal Proxcensus -- 5.1 Protocol Description -- 6 Technical Combinatorial Lemma -- 7 Putting It All Together -- 7.1 Comparison to Previous Protocols -- 7.2 Open Problems -- References -- A Complete Characterization of Game-Theoretically Fair, Multi-Party Coin Toss -- 1 Introduction -- 1.1 Our Results and Contributions -- 1.2 Related Work -- 2 Technical Overview -- 2.1 Upper Bound -- 2.2 Lower Bound -- 3 Definitions -- 4 Upper Bound -- 4.1 Our Final Protocol for Malicious Coalitions -- 5 Lower Bound -- 5.1 Parameter Constraints -- 5.2 Constraint System Implies the Lone-Wolf, Wolf-Minion, and T2-Equality Conditions -- 5.3 Minimizing t Subject to Constraints -- 6 Complete Characterization of Maximin Fairness -- 6.1 Lower Bound -- 6.2 Upper Bound -- A Visualization of the Resilience Parameter -- References -- Lightweight, Maliciously Secure Verifiable Function Secret Sharing -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Work -- 1.3 Technical Overview -- 2 Background -- 2.1 Notation -- 2.2 Function Secret Sharing -- 3 Lightweight, Verifiable DPF -- 3.1 Definitions -- 3.2 Our Construction -- 3.3 VDPF Security Proof -- 4 Verifiable Distributed Multi-Point Function -- 4.1 Cuckoo-hashing from PRPs -- 4.2 Verifiable Distributed MPFs via PRP Hashing -- 5 Implementation &amp -- Performance -- A Match-Mode VDMPF: Point Matching -- References -- Highly Efficient OT-Based Multiplication Protocols -- 1 Introduction -- 1.1 Background on OT-Based Two-Party Multiplication -- 1.2 Our Contributions -- 1.3 Applications -- 1.4 Related Work -- 2 Our Techniques.
3 Preliminaries -- 3.1 Notations -- 3.2 Distributions and Random Variables -- 3.3 Two-Party Protocols and Functionalities -- 3.4 Some Inequalities -- 4 Multiplication with Unpredictable Output Under Attack -- 4.1 The Ideal Functionality -- 4.2 The OT-Based Protocol -- 5 Batching -- 5.1 The Ideal Functionality -- 5.2 The OT-Based Protocol -- 6 Applications -- 6.1 Realizing Perfect Multiplication -- 6.2 Generating Correlated Data in the Preprocessing Model -- References -- Round-Optimal Black-Box Protocol Compilers -- 1 Introduction -- 1.1 Our Results -- 2 Technical Overview -- 2.1 IPS Compiler -- 2.2 A New Compiler: Removing Equivocality -- 2.3 Protocol Compiler in the Random Oracle Model -- 2.4 Two-Sided NISC -- 2.5 The Multiparty Setting -- 3 Preliminaries -- 3.1 Semi-honest Two-Round Two-Party Computation -- 3.2 Semi-malicious Two-Round Two-Party Computation -- 3.3 Extractable Commitments in ROM -- 3.4 Pairwise Verifiable Secret Sharing -- 4 Two-Round Client-Server Protocol with Pairwise Verifiability -- 4.1 Definition -- 5 Black-Box Protocol Compilers in the Two-Party Setting -- 5.1 Protocol Compiler in the Random Oracle Model -- 5.2 Protocol Compiler in the OT Correlations Model -- 5.3 Extension to the Two-Sided Setting -- 6 Black-Box

Protocol Compilers in the Multiparty Setting -- 6.1 Protocol Compiler in the Random Oracle Model -- 6.2 Protocol Compiler in the OT Correlations Model -- References -- Guaranteed Output in O(n) Rounds for Round-Robin Sampling Protocols -- 1 Introduction -- 1.1 Our Contributions -- 2 Preliminaries -- 3 A Round-Reducing Compiler -- 3.1 The Compiler -- 3.2 Proof of Security -- 4 A Round-Robin Protocol -- 4.1 The Protocol -- 4.2 Proof of Security -- 4.3 Application: Powers of Tau and Polynomial Commitments -- 4.4 Application: Sampling Updateable SRSes -- 4.5 Application: Verifiable Mixnets -- 5 With Concrete Efficiency.
References -- Universally Composable Subversion-Resilient Cryptography -- 1 Introduction -- 1.1 Subversion-Resilient Cryptography -- 1.2 Our Contributions -- 1.3 Technical Overview -- 2 A UC Model of Reverse Firewalls -- 2.1 Quick and Dirty Recap of UC -- 2.2 Modeling Reverse Firewalls -- 2.3 Specious Corruptions -- 2.4 Sanitizing Protocols Implementing Regular Ideal Functionalities -- 2.5 General Case -- 2.6 Composition -- 2.7 Computational Transparency -- 2.8 Strong Sanitation -- 3 String Commitment -- 3.1 Sanitizable Commitment Functionality -- 3.2 Protocol from DDH -- 4 Coin Tossing -- 4.1 The Coin Tossing Functionality -- 4.2 Sanitizing Blum's Protocol -- 5 Completeness Theorem -- 5.1 Sanitizable Commit and Prove -- 5.2 Sanitizing the GMW Compiler -- 6 Conclusions and Future Work -- References -- Asymptotically Quasi-Optimal Cryptography -- 1 Introduction -- 1.1 Our Results and Techniques -- 1.2 Perspectives and Open Problems -- 2 Preliminaries -- 2.1 Asymptotic Quasi-Optimality -- 2.2 Ring Learning with Errors -- 2.3 Ring-LWE Encryption -- 2.4 Entropy and Extraction -- 3 AQO Semi-Honest Batch-OLE and Batch-OT -- 3.1 Gentle Noise-Flooding -- 3.2 Entropically Secure Batch-OLE Protocol -- 3.3 Our Batch-OLE and Batch-OT Schemes -- 4 AQO Batch-OLE: The Malicious Setting -- 4.1 Entropically Secure OLE Against a Malicious Receiver -- 5 AQO Zero-Knowledge Arguments -- 5.1 AQO-Honest Verifier ZK from AQO-Honest Verifier ZKPCP -- References -- Round-Optimal Multi-party Computation with Identifiable Abort -- 1 Introduction -- 1.1 Our Results -- 1.2 Technical Overview -- 1.3 Related Work -- 2 Preliminaries and Standard Definitions -- 2.1 Non-malleable Commitments Scheme -- 2.2 Trapdoor Generation Protocol with Bounded Rewind Security -- 3 Rewind-Secure OT and MPC -- 4 From MPC with Unanimous Abort to B-rewindable MPC with Unanimous Abort.
5 Our Construction: MPC with Identifiable Abort -- 6 Special BOT-Rewindable Secure Oblivious Transfer -- References -- On the Security of ECDSA with Additive Key Derivation and Presignatures -- 1 Introduction -- 1.1 Our Contributions -- 2 The EC-GGM -- 3 Properties of the ECDSA Conversion Function -- 4 Notions of Security -- 5 Proof of Security of ECDSA in the EC-GGM -- 6 ECDSA with Additive Key Derivation -- 7 ECDSA with Presignatures -- 7.1 ECDSA with Presignatures and Additive Key Derivation -- 8 ECDSA with Re-randomized Presignatures -- 8.1 ECDSA with Re-randomized Presignatures and Additive Key Derivation -- 9 Homogeneous Key Derivation -- 9.1 Homogeneous Key Derivation Without Presignatures -- 9.2 Homogeneous Key Derivation with Presignatures -- 9.3 Homogeneous Key Derivation with Re-randomized Presignatures -- References -- Secure Multiparty Computation with Free Branching -- 1 Introduction -- 1.1 Our Contributions -- 2 Technical Overview -- 2.1 Non-constant Round Branching MPC -- 2.2 Constant Round (Semi-honest) Protocol -- 3 Oblivious Inner Product -- 4 MPC Interface -- 5 Non-constant Round Semi-honest Branching MPC -- 6 Constant Round Semi-honest Branching MPC -- 7 Implementation -- 7.1 How We

Benchmark -- 7.2 Comparison of Communication Complexity -- 7.3 Comparison of Running Time -- References -- Secure Multiparty Computation with Sublinear Preprocessing -- 1 Introduction -- 1.1 Our Results -- 1.2 Technical Overview -- 2 Preliminaries -- 2.1 Security Definitions -- 2.2 Fully Linear Proof Systems -- 2.3 Additively-Homomorphic Encryption (AHE) -- 2.4 Ideal Functionalities and Basic Building Blocks -- 3 The BGIN Compiler ch15BoyleGIN21 -- 4 A New Simplified Verification Protocol -- 4.1 A Concrete Instantiation for the Zk-FLIOP Protocol -- 4.2 The Dealer's Ideal Functionality FDealer -- 5 Online Computation with a Trusted Dealer.
6 Distributing the Dealer with Sublinear Communication.

Sommario/riassunto

The 3-volume-set LNCS 13275, 13276 and 13277 constitutes the refereed proceedings of the 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Eurocrypt 2022, which was held in Trondheim, Norway, during 30 May – 3 June, 2022. The 85 full papers included in these proceedings were accepted from a total of 372 submissions. They were organized in topical sections as follows: Part I: Best Paper Award; Secure Multiparty Computation; Homomorphic Encryption; Obfuscation; Part II: Cryptographic Protocols; Cryptographic Primitives; Real-World Systems Part III: Symmetric-Key Cryptanalysis; Side Channel Attacks and Masking, Post-Quantum Cryptography; Information-Theoretic Security.