1.

Record Nr.	UNISALENTO991002593909707536
Autore	Tusiani, Joseph
Titolo	Dialect Poetry of Southern Italy; texts and criticism :(a Trilingual Anthology) / edited by Luigi Bonaffini
Pubbl/distr/stampa	Ottawa : Legas, c1997
ISBN	1881901130
Descrizione fisica	511 p. ; 23 cm.
Soggetti	Poesia dialettale - Italia Meridionale Tusiani, Joseph - Poesie
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliografia: p. 493-506. Indici. Poesie di Joseph Tusiani: 204-214 p.

2.

Record Nr.	UNISA996594167103316
Autore	Joye Marc
Titolo	Advances in Cryptology - EUROCRYPT 2024 : 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zurich, Switzerland, May 26-30, 2024, Proceedings, Part V
Pubbl/distr/stampa	Cham : , : Springer International Publishing AG, , 2024 ©2024
ISBN	3-031-58740-5
Edizione	[1st ed.]
Descrizione fisica	1 online resource (479 pages)
Collana	Lecture Notes in Computer Science Series ; ; v.14655
Altri autori (Persone)	LeanderGregor
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Organization -- Contents - Part V -- Multi-party Computation and Zero-Knowledge (I/II) -- Efficient Arithmetic in Garbled Circuits -- 1 Introduction -- 1.1 Contribution -- 1.2 Background and Related Work -- 1.3 Summary of Our Approach -- 2 Preliminaries -- 2.1 Cryptographic Assumption -- 2.2 Garbling Schemes -- 2.3 Modular Arithmetic -- 2.4 Chinese Remainder Theorem -- 2.5 Barrett's Modular Reduction -- 2.6 Miscellaneous Notation -- 3 Garbled Switch Systems -- 3.1 Generalizing Free XOR -- 3.2 Switch Systems -- 3.3 Garbling Switch Systems -- 4 Generalized One Hot Garbling -- 4.1 Our Approach to One-Hot Garbling -- 4.2 Half Multiplication -- 4.3 Conversions -- 5 Garbled Arithmetic from Switch Systems -- 5.1 Short Integers -- 5.2 Long Integers -- References -- Can Alice and Bob Guarantee Output to Carol? -- 1 Introduction -- 1.1 Our Results -- 1.2 Our Techniques -- 1.3 Organization -- 2 Preliminaries -- 3 Statement of Our Results -- 3.1 An Equivalent Characterization -- 4 Impossibility of Computing Strong Semi-Balanced Functionalities -- 5 A Positive Result for Solitary Output Computation -- 6 Application: Analysis of the Disjointness Functionality -- References -- SPRINT: High-Throughput Robust Distributed Schnorr Signatures -- 1 Introduction -- 1.1 Other Techniques -- 1.2 Prior Work -- 1.3 Subsequent Work -- 1.4 Organization -- 2 Technical Overview -- 2.1 Starting Point: The GJKR Protocol -- 2.2 The Agreement Protocol

-- 2.3 Signing Many Messages in Parallel -- 2.4 Using Super-Invertible Matrices -- 2.5 Using Packed Secret Sharing -- 2.6 More Efficient Signing -- 2.7 The Dynamic Setting -- 2.8 Sub-sampling the Committees -- 2.9 More Optimizations -- 2.10 Parameters and Performance -- 3 The SPRINT Protocols -- 3.1 Static-Committee Setting -- 3.2 The Dynamic/Proactive Setting -- 4 The Agreement Protocol.

4.1 Agreement in SPRINT, the Static Case -- 4.2 Agreement in the Dynamic/Proactive Setting -- References -- Efficient and Generic Methods to Achieve Active Security in Private Information Retrieval and More Advanced Database Search -- 1 Introduction -- 1.1 Our Results -- 1.2 Related Work -- 2 Technical Overview -- 2.1 Non-interactive Actively Secure Protocols -- 2.2 Interactive Actively Secure Protocols -- 3 Preliminaries -- 3.1 Secure Computation in the Client-Servers Setting -- 3.2 Existing Passively Secure Protocols -- 4 Interactive Actively Secure Protocols -- 4.1 Graph Theory -- 4.2 Formalization of Conflict-Finding Protocols -- 4.3 Compiler from Conflict-Finding to Actively Secure Protocols -- 4.4 Compiler from Passively Secure to Conflict-Finding Protocols -- 4.5 Instantiations -- 5 Non-interactive Actively Secure Protocols -- 5.1 Locally Surjective Map Family -- 5.2 Compiler from Passively Secure to Actively Secure Protocols -- 5.3 Instantiations -- References -- Constant-Round Simulation-Secure Coin Tossing Extension with Guaranteed Output -- 1 Introduction -- 2 Technical Overview -- 2.1 The Round Structure of CTE Protocols -- 2.2 Coin Tossing Extension and Explainable Extractors -- 2.3 Computational Coin Tossing Extension with Long Stretch -- 2.4 A Lower Bound for Statistical Coin Tossing Extension -- 2.5 One-Round Unbiased Sampling from Any Distribution -- 3 One-Round, One-Sample Adaptive Coin Tossing Extension from LWE -- References -- Witness Semantic Security -- 1 Introduction -- 1.1 Application: Malicious-CRS Security for Non-interactive Zero-Knowledge -- 1.2 Our Results -- 1.3 Other Related Works -- 2 Technical Overview -- 2.1 Defining Witness Semantic Security -- 2.2 NIZK Satisfying Witness Semantic Security with a Malicious CRS -- 3 Preliminaries -- 4 Witness Semantic Security -- 4.1 Verifiable Witness Semantic Security.

4.2 Malicious CRS Non-uniform Zero-Knowledge with Auxiliary Information -- 4.3 Malicious CRS NUZK Implies Malicious CRS Witness Semantic Security -- 4.4 Malicious CRS NUZK Implies Malicious CRS Verifiable Witness Semantic Security -- 4.5 Malicious Reusable CRS Witness Semantic Security -- 5 NIZK with Malicious CRS Witness Semantic Security from LWE -- 5.1 Building Blocks -- 5.2 The Construction -- References -- Garbled Circuit Lookup Tables with Logarithmic Number of Ciphertexts -- 1 Introduction -- 1.1 Contribution -- 2 Related Work -- 3 Preliminaries -- 3.1 Notation and Assumptions -- 3.2 Garbled Sharing -- 3.3 Garbling Schemes -- 3.4 One-Hot Garbling -- 4 Technical Overview -- 4.1 Reducing Lookup Tables to Random Function Evaluation -- 4.2 Evaluating a Uniformly Random Function -- 5 Approach -- 6 Performance -- 7 Security Theorems and Proofs -- References -- Publicly Verifiable Secret Sharing Over Class Groups and Applications to DKG and YOSO -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Works -- 2 Preliminaries -- 2.1 Publicly Verifiable Secret Sharing(PVSS) -- 2.2 Background on Class Groups -- 2.3 Zero Knowledge Proofs for Class Groups -- 3 PVSS over Class Groups -- 3.1 The PVSS Scheme -- 3.2 Instantiating the Proofs -- 3.3 Complexity -- 4 Application: Distributed Key Generation -- 4.1 Two-Round DKG with Unbiasable Public Key -- 4.2 One-Round Biasable Public-Key Version -- 5 Application: YOSO MPC -- 5.1 Resharing -- 5.2 Realizing Efficient YOSO MPC --

References -- Bulletproofs++: Next Generation Confidential Transactions via Reciprocal Set Membership Arguments -- 1 Introduction -- 1.1 Contributions -- 1.2 Related Work -- 2 Preliminaries -- 2.1 Zero-Knowledge Arguments of Knowledge -- 3 Technical Overview -- 3.1 Recap: Bulletproofs and Bulletproofs+ -- 3.2 Reciprocal Argument -- 3.3 Norm Linear Argument -- 3.4 Arithmetic Circuits.

4 Norm Linear Argument -- 4.1 Reducing the Vectors -- 4.2 Norm Linear Argument -- 4.3 Full Protocol Description -- 5 Arithmetic Circuits -- 5.1 Protocol Overview -- 6 Reciprocal Argument -- 6.1 Warmup: Reciprocal Argument Protocol -- 6.2 Reciprocal Form Circuits -- 6.3 Reciprocal Range Proofs -- 6.4 Multi-asset Confidential Transactions -- 7 Implementation and Benchmarks -- References -- Perfect Asynchronous MPC with Linear Communication Overhead -- 1 Introduction -- 1.1 Related Work -- 2 Technical Overview -- 2.1 Basic Asynchronous Verifiable Secret Sharing -- 2.2 Our Asynchronous Weak-Binding Secret Sharing -- 2.3 Our MPC Protocol -- 2.4 Multiplication Triplets with a Dealer -- 3 Preliminaries -- 3.1 Asynchronous Secure Computation and SUC -- 4 Verifying Product Relation -- 4.1 Trivariate Polynomial Verification - Functionality -- 4.2 Verifying Product Relation Using Trivariate Polynomial -- 4.3 Trivariate Polynomial Verification - Protocol -- 5 Rate-1 Asynchronous Weak-Binding Secret Sharing -- 6 Verifiable Triple Sharing -- 6.1 Batching for Linear Overhead per Triple -- 7 The MPC Protocol -- References -- Perfect (Parallel) Broadcast in Constant Expected Rounds via Statistical VSS -- 1 Introduction -- 1.1 Our Results -- 1.2 Related Work -- 2 Technical Overview -- 2.1 Efficient Oblivious Leader Election -- 2.2 Efficient Statistical VSS -- 2.3 Putting It All Together -- 3 Preliminaries -- 4 Statistical Verifiable Secret Sharing -- 4.1 Sharing Attempt -- 4.2 Reconstructing Shares -- 4.3 Statistical VSS Protocol -- 5 Batched Multi-moderated Verifiable Secret Sharing -- 5.1 Reconstruction with Moderators -- 5.2 Batching -- 6 Oblivious Leader Election -- 7 Broadcast, and Parallel Broadcast -- References -- Fuzzy Private Set Intersection with Large Hyperballs -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Work -- 1.3 Applications.

2 Technical Overview -- 2.1 Recap: Apple's PSI Protocol -- 2.2 Fuzzy Matching for Infinity Distance -- 2.3 Generalized Distance Functions -- 2.4 Fuzzy PSI in Low Dimensions -- 2.5 Extending to High Dimensions -- 3 Preliminaries -- 3.1 Oblivious Key-Value Store (OKVS) -- 3.2 Random Self-reductions of DDH Tuples -- 4 Definitions and Functionalities -- 4.1 Definition of Fuzzy Matching -- 4.2 Definition of Fuzzy (Circuit) Private Set Intersection -- 5 Fuzzy Matching -- 5.1 Fuzzy Matching for Infinity Distance -- 5.2 Fuzzy Matching for Minkowski Distance -- 6 Fuzzy PSI in Low-Dimension Space -- 6.1 Spatial Hashing Techniques -- 6.2 Fuzzy PSI-CA for Infinity Distance -- 6.3 Fuzzy PSI-CA for Minkowski Distance -- 7 Fuzzy PSI in High-Dimension Space -- 7.1 Infinity Distance -- 8 Extending to Broader Functionalities -- 9 Performance Evaluation -- 9.1 Concrete Performance -- 10 Conclusion -- References -- Fast Batched Asynchronous Distributed Key Generation -- 1 Introduction -- 1.1 An MPC Engine Geared Towards Schnorr -- 1.2 Two Problems -- 2 Our Contributions -- 2.1 Solution to Problem 1 -- 2.2 Solution to Problem 2 -- 2.3 Combining the Two Solutions -- 2.4 The Rest of the Paper -- 3 Preliminaries -- 3.1 Asynchronous Verifiable Secret Sharing -- 3.2 Group-Oriented AVSS -- 4 Subprotocols -- 4.1 AVSS -- 4.2 Reliable Broadcast -- 4.3 One-Sided Voting -- 4.4 Random Beacon -- 5 Our New GoAVSS Protocol -- 5.1 Security Analysis of Protocol GoAVSS1 -- 5.2 Complexity Analysis of Protocol GoAVSS1 -- 5.3 A Variation for

Large n -- 6 Super-Invertible Matrices from Pascal -- 6.1 The Symmetric Pascal Matrix -- 6.2 The Upper-Triangular Pascal Matrix -- 6.3 Better Super-Invertible Matrices from Hyper-invertible Matrices -- References -- Toward Malicious Constant-Rate 2PC via Arithmetic Garbling -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Technical Overview.

2 Notations and Definitions.