

1. Record Nr.	UNINA9910842286403321
Titolo	Applied Cryptography and Network Security : 22nd International Conference, ACNS 2024, Abu Dhabi, United Arab Emirates, March 5–8, 2024, Proceedings, Part I // edited by Christina Pöpper, Lejla Batina
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2024
ISBN	3-031-54770-5
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (509 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14583
Disciplina	005.8
Soggetti	Data protection Data structures (Computer science) Information theory Operating systems (Computers) Application software Cryptography Data encryption (Computer science) Data and Information Security Data Structures and Information Theory Operating Systems Computer and Information Systems Applications Cryptology Security Services
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 Keynote Talks -- Applying Machine Learning to Securing Cellular Networks -- Real-World Cryptanalysis -- CAPTCHAs: What Are They Good For? -- Contents - Part I -- Contents - Part II -- Contents - Part III -- Cryptographic Protocols -- CryptoZoo: A Viewer for Reduction Proofs -- 1 Introduction -- 2 Related Work -- 3 State-Separating Proofs -- 4 A Proof Viewer for SSPs -- 4.1 Proof Viewing Concepts -- 4.2 Implementation Considerations -- 5 Case Study: IND-CPA Vs. Simulation-Based Security -- 6 Case Study: Constant-Depth GGM Tree

-- 7 Case Study: Yao's Garbling Scheme -- 8 Comparison -- 8.1 Yao's Garbling Scheme -- 8.2 SSP Proofs of TLS 1.3 -- 8.3 SSP Proofs of the MLS Key Schedule -- 8.4 Formal Verification Tools for SSPs -- 9 Conclusion and Future Work -- References -- Element Distinctness and Bounded Input Size in Private Set Intersection and Related Protocols -- 1 Introduction -- 2 Related Work and Background -- 2.1 Private Set Intersection (PSI) -- 2.2 PSI Variants -- 2.3 PSI with Restrictions -- 2.4 PSI with Multiset Input -- 2.5 Zero-Knowledge Proofs -- 2.6 Homomorphic Encryption -- 3 Proving Element Distinctness -- 3.1 Puzzle-Based PoED Construction -- 3.2 Analysis of PoED-Puzzle Protocol -- 4 PSI with Element Distinctness Check -- 4.1 Adversary Model -- 4.2 Definition of AD-PSI -- 4.3 A Construction for AD-PSI Based on PoED-puzzle -- 4.4 Alternative AD-PSI and Modified Construction -- 5 AD-PSI Variants -- 5.1 PSI-CA with Element Distinctness (AD-PSI-CA) -- 5.2 PSI-X with Element Distinctness (AD-PSI-X) -- 5.3 PSI-DT with Element Distinctness (AD-PSI-DT) -- 6 Completing Bounded-Size-Hiding-PSI -- 7 Authorized PSI with Element Distinctness -- 7.1 AD-APSI Definition -- 7.2 AD-APSI Construction -- 7.3 Security Analysis -- 8 Conclusion -- A Security Proof for AD-PSI-puzzle -- B AD-PSI Variants. C Security Proof for AD-APSI -- References -- A New Approach to Efficient and Secure Fixed-Point Computation -- 1 Introduction -- 1.1 Related Work -- 1.2 Construction Blueprint -- 2 Preliminaries -- 2.1 UC Functionalities -- 3 Truncation -- 3.1 RNS in MPC -- 3.2 Fixed-Point Arithmetic -- 4 The Construction -- 4.1 Preprocessing -- 4.2 Lifting -- 4.3 Probabilistic Truncation -- 4.4 Error Reduction -- 5 Efficiency -- 5.1 Implementation -- 5.2 Comparison with Related Techniques -- References -- Auditable Attribute-Based Credentials Scheme and Its Application in Contact Tracing -- 1 Introduction -- 2 Preliminaries -- 3 Auditable Attribute-Based Credentials Scheme -- 3.1 Auditable Public Keys -- 3.2 Formal Definitions of Auditable ABC -- 3.3 Our Constructions and Analysis -- 4 Application: Contact Tracing -- 4.1 An Auditable ABC-Based Construction -- 4.2 Security and Analysis -- 4.3 Implementation -- 5 Conclusion -- A The Necessity of Enhancing Contact Tracing Systems -- B The SPS-EQ Scheme from ch4spseqspkpc2022 -- C Extending the BLS Signature ch4bls01 with APK -- References -- Verification Protocol for Stable Matching from Conditional Disclosure of Secrets -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Applications -- 1.3 Organization -- 2 Related Works -- 2.1 Stable Matching -- 2.2 Conditional Disclosure of Secrets -- 2.3 Multi-client Verifiable Computation -- 3 Preliminaries -- 3.1 Stable Matching -- 3.2 Conditional Disclosure of Secrets -- 3.3 Multi-client Verifiable Computation -- 3.4 Secret Sharing -- 4 Proposed CDS Schemes -- 4.1 CDS Scheme for Unstable Matching -- 4.2 CDS Scheme for Stable Matching -- 4.3 Possible Improvements -- 5 Verification Protocol for Stable Matching -- 6 Implementation -- 7 Concluding Remarks -- References -- Non-malleable Fuzzy Extractors -- 1 Introduction -- 1.1 Our Results -- 1.2 Related Work -- 2 Preliminaries. 2.1 (Keyless) Fuzzy Extractors -- 2.2 Non-malleable Codes -- 3 Non-malleable Fuzzy Extractors -- 4 Construction -- 5 Fuzzy Tamper-Resilient Security -- 6 Conclusions -- References -- Upgrading Fuzzy Extractors -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Related Work -- 1.3 Discussion and Future Work -- 2 Preliminaries -- 2.1 Entropy Definitions -- 2.2 Obfuscation Definitions -- 2.3 Fuzzy Extractors -- 3 Weakly-Private Fuzzy Extractors -- 3.1 Weakly Private FE from FE and MBCC Obfuscation -- 3.2 Weakly Private FE from Secure Sketch and MBCC Obfuscation -- 4 Robustness -- 5 Reuse -- A Privacy vs FE Security -- B Reusability from Composable MBCC Obfuscation --

References -- X-Lock: A Secure XOR-Based Fuzzy Extractor for Resource Constrained Devices -- 1 Introduction -- 2 Related Works -- 3 Background -- 4 X-Lock: Construction Details -- 5 X-Lock: Algorithm Analysis -- 5.1 Security Analysis -- 5.2 Bias and Correlation Analysis -- 5.3 Costs Analysis -- 6 Implementation and Comparison -- 7 Conclusion -- References -- Encrypted Data -- Efficient Clustering on Encrypted Data -- 1 Introduction -- 2 Related Works -- 3 Background -- 3.1 Approximate Homomorphic Encryption CKKS -- 3.2 Newton's Method -- 4 System Architecture and Threat Model -- 4.1 System Architecture -- 4.2 Threat Model -- 4.3 Security -- 5 Fully Privacy-Preserving Clustering Scheme Based on FHE -- 5.1 Preliminaries -- 5.2 Ciphertext Comparison -- 5.3 Ciphertext Division -- 5.4 Converting the One-Hot Vectors to Label in Plaintexts -- 5.5 The Complete Algorithm for Privacy-Preserving Clustering -- 5.6 Security Proof -- 6 An Optimized Algorithm -- 6.1 Block Clustering Scheme -- 6.2 Block Clustering Scheme with Cluster Selection -- 7 Experiment Results -- 7.1 Experiment Setup -- 7.2 Clustering Accuracy -- 7.3 Run Time -- 7.4 Performance of Block Clustering Scheme with Cluster Selection.

8 Conclusions -- References -- Generic Construction of Forward Secure Public Key Authenticated Encryption with Keyword Search -- 1 Introduction -- 2 Preliminaries -- 2.1 PAEKS -- 2.2 0/1 Encodings -- 3 Definition of FS-PAEKS -- 4 Our Generic Construction of FS-PAEKS -- 5 Security Analysis -- 6 Vulnerability of the Jiang Et Al. FS-PAEKS Scheme -- 7 Conclusion -- References -- Encryption Mechanisms for Receipt-Free and Perfectly Private Verifiable Elections -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Our Techniques -- 1.3 Related Work -- 1.4 Overview of Paper -- 2 Background -- 2.1 Assumptions and Primitives -- 2.2 Traceable Receipt-Free Encryption (TREnc) -- 2.3 Commitment Consistent Encryption (CCE) -- 3 The Construction of Our Scheme -- 3.1 Description -- 3.2 Verification Equations -- 3.3 Security Analysis -- 3.4 Efficiency -- 4 Application to E-Voting -- 4.1 Voting Scheme with a Homomorphic Tally -- 4.2 Voting Scheme with a Mixnet Tally -- 5 Conclusion -- A Scheme Description for Complex Ballots -- B Deferred Proofs -- B.1 Correctness -- B.2 Strong Randomizability -- B.3 TCCA Security -- B.4 Traceability -- B.5 Verifiability -- References -- Two-Party Decision Tree Training from Updatable Order-Revealing Encryption -- 1 Introduction -- 1.1 Related Work -- 1.2 Our Contribution -- 1.3 Outline -- 2 Preliminaries -- 2.1 The Universal Composability Model -- 2.2 Order-Revealing Encryption -- 2.3 Decision Tree Training -- 3 Updatable Order-Revealing Encryption -- 4 Secure Decision Tree Training -- 4.1 Variations of the Training Process -- 4.2 Graceful Degradation Using Enclaves -- 5 Analysis of the Leakage -- 5.1 Leakage for Random Message Selection -- 5.2 Additional Leakage for Malicious Message Selection -- 5.3 Transformation for Non-uniform Distributions -- 6 Implementation and Evaluation -- 6.1 Evaluation of the Updatable ORE Scheme. 6.2 Evaluation of the Protocol -- 7 Conclusion -- A A Brief Introduction to the UC Framework -- References -- KIVR: Committing Authenticated Encryption Using Redundancy and Application to GCM, CCM, and More -- 1 Introduction -- 1.1 Research Challenges -- 1.2 Contributions -- 1.3 Organization -- 2 Preliminaries -- 3 Committing Security with Plaintext Redundancy -- 3.1 Plaintext with Redundancy -- 3.2 Definitions for Committing Security with Redundancy -- 4 KIVR Transform -- 4.1 Specification of KIVR -- 4.2 Security of KIVR -- 5 Committing Security of KIVR with CTR-Based AE -- 5.1 Specification of CTR-Based AE -- 5.2 CMT-4-Security of KIVR[CTRAE] -- 6 Proof of Theorem 1 -- 6.1 Tools -- 6.2 Symbol Definitions -- 6.3 Deriving the

CMT-4-Security Bound -- 6.4 Bounding $\Pr[(C,T)=(C,T) \text{ coll}]$ -- 7
Committing Security of KIVR with GCM, GCM-SIV, and CCM -- 7.1
Specifications of GCM, GCM-SIV, and CCM -- 7.2 CMT-4-Security of
KIVR[GCM], KIVR[GCM-SIV], and KIVR[CCM] -- 7.3 Tightness of the
CMT-4-Security of KIVR[GCM] and KIVR[GCM-SIV] -- 7.4 On the
Tightness of CMT-4-Security of KIVR[CCM] -- 8 Committing Security of
KIVR with CTR-HMAC -- 8.1 Specification of CTR-HMAC -- 8.2 CMT-
4-Security Bound of KIVR[CTR-HMAC] -- 8.3 Tightness of the CMT-4-
Security of KIVR[CTR-HMAC] -- 9 Conclusion -- A Multi-user Security
for AE -- B Multi-user PRF Security -- C μ -AE Security of AE
Schemes with KIVR -- D Proof of Theorem 2 for KIVR[GCM-SIV] -- E
Proof of Theorem 3 -- References -- Signatures -- Subversion-
Resilient Signatures Without Random Oracles -- 1 Introduction -- 1.1
Subversion-Resilient Signatures with Watchdogs -- 1.2 Technical
Challenges -- 1.3 Our Contributions -- 1.4 Alternative Models -- 2
Model and Preliminaries -- 2.1 Notation and Model -- 2.2 Subversion-
Resilience -- 2.3 Achieving Subversion-Resilience -- 2.4 Assumptions
-- 2.5 Pseudorandom Functions.
3 Subversion-Resilient One-Way Functions.

Sommario/riassunto

The 3-volume set LNCS 14583-14585 constitutes the proceedings of the 22nd International Conference on Applied Cryptography and Network Security, ACNS 2024, which took place in Abu Dhabi, UAE, in March 2024. The 54 full papers included in these proceedings were carefully reviewed and selected from 230 submissions. They have been organized in topical sections as follows: Part I: Cryptographic protocols; encrypted data; signatures; Part II: Post-quantum; lattices; wireless and networks; privacy and homomorphic encryption; symmetric crypto; Part III: Blockchain; smart infrastructures, systems and software; attacks; users and usability.
