

1. Record Nr.	UNINA9910591033603321
Titolo	Security and Cryptography for Networks : 13th International Conference, SCN 2022, Amalfi (SA), Italy, September 12–14, 2022, Proceedings / / edited by Clemente Galdi, Stanislaw Jarecki
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2022
ISBN	9783031147913 303114791X
Edizione	[1st ed. 2022.]
Descrizione fisica	1 online resource (795 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 13409
Disciplina	005.82 005.824
Soggetti	Cryptography Data encryption (Computer science) Application software Data protection Computer networks - Security measures Computer networks Cryptology Computer and Information Systems Applications Security Services Mobile and Network Security Computer Communication Networks
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 -- Invited Talks -- How to Do Cryptography Even When Cryptography Doesn't Exist -- From Galactic PCP Theory to Scaling Blockchains with ZK-STARKs -- Contents -- Ciphers, Cryptanalysis, Defenses -- Decoding McEliece with a Hint - Secret Goppa Key Parts Reveal Everything -- 1 Introduction -- 2 Preliminaries -- 3 Some Parts of a Secret Goppa Key Reveal Everything -- 3.1 Key Recovery from ALL Goppa Points -- 3.2 Goppa Polynomial Recovery from only t_m+1 Goppa Points -- 3.3 Reconstruction of the

Remaining Goppa Points -- 3.4 Full Key Recovery from $tm+1$ Goppa Points -- 4 Correcting Faulty Goppa Points -- References -- Cost-Asymmetric Memory Hard Password Hashing -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Work -- 2 Background and Notations -- 3 Defender's Model -- 4 Attacker's Model -- 4.1 Assumptions of Economics Analysis -- 4.2 Cracking Process -- 4.3 Attacker's Utility -- 4.4 Stackelberg Game -- 5 Computing the Attacker's Optimal Strategy -- 5.1 Marginal Utility -- 5.2 A Superset of the Optimal Checking Sequence -- 5.3 Extension by Concatenation -- 5.4 Local Search in Two Directions -- 5.5 Optimality Test and Globally Optimal Checking Sequence -- 6 Defender's Optimal Strategy -- 7 Experiments -- 7.1 Experiment Setup -- 7.2 Experiment Analysis and Discussion -- 8 Conclusion -- References -- .26em plus .1em minus .1emMemory-Hard Puzzles in the Standard Model with Applications to Memory-Hard Functions and Resource-Bounded Locally Decodable Codes -- 1 Introduction -- 1.1 Our Results -- 1.2 Prior Work -- 2 Technical Overview -- 2.1 Memory-Hard Languages -- 2.2 Memory-Hard Puzzles -- 2.3 Memory-Hard Functions from Memory-Hard Puzzles -- 2.4 Resource-Bounded LDCs from Cryptographic Puzzles -- References -- RAMus- A New Lightweight Block Cipher for RAM Encryption -- 1 Introduction -- 2 Preliminaries. 3 The 2S-Strategy -- 3.1 Notations -- 3.2 The Round Function -- 4 The Description of RAMus -- 5 Design Rationale -- 6 Security Analysis of RAMus -- 6.1 Theoretical Proven Bound -- 6.2 SAT-Based Analysis -- 6.3 The Security of RAMus Against Integral Cryptanalysis and the Division Property Attacks -- 7 Performance -- References -- Higher-Order Masked Saber -- 1 Introduction -- 2 Preliminaries -- 2.1 Notation -- 2.2 Saber -- 2.3 uSaber -- 2.4 Fujisaki-Okamoto Transformation -- 2.5 Higher-Order Masking -- 3 Masking Saber -- 3.1 Arithmetic Operations -- 3.2 Compression -- 3.3 Masked Hashing -- 3.4 Masked Centered Binomial Sampler -- 3.5 Masked Comparison -- 4 Masking uSaber -- 5 Performance Evaluation -- 5.1 Performance Analysis of Comparison Algorithms for Saber -- 5.2 Performance Analysis for Masked Saber Decapsulation -- 5.3 Performance Analysis for Masked uSaber Decapsulation -- 5.4 Comparison with State-of-the-Art -- 6 Conclusions -- References -- Approximate Distance-Comparison-Preserving Symmetric Encryption -- 1 Introduction -- 1.1 Background and Motivation -- 1.2 Our Results -- 1.3 Discussion -- 1.4 Further Related Work -- 2 Preliminaries -- 3 Approximate Distance-Comparison-Preserving Functions and Their Properties -- 3.1 Notions Considered -- 3.2 Accuracy of Nearest Neighbors for -DCP Functions -- 3.3 Impossibility of Ideal Security -- 4 The Scale-and-Perturb (SAP) Scheme -- 4.1 Our Core -DCPE Scheme -- 4.2 Two Preprocessing Algorithms -- 5 Real-or-Replaced Indistinguishability for Neighboring Datasets -- 5.1 -RoR Security Bounds -- 6 Security Against Approximate Frequency-Finding Attacks -- 6.1 Window One-Wayness Security Notion -- 6.2 One-Wayness Bounds -- 6.3 Security Against Freq-Find Adversaries -- 7 Bit Security -- References -- Public Key Encryption -- Key-Policy ABE with Switchable Attributes -- 1 Introduction -- 1.1 Related Work. 1.2 Contributions -- 2 Preliminaries -- 2.1 Dual Pairing Vector Spaces -- 2.2 Change of Basis -- 2.3 Particular Changes -- 3 Key-Policy ABE with Switchable Attributes -- 3.1 Policy Definition -- 3.2 Labeling of Access-Trees -- 3.3 Switchable Leaves and Attributes -- 3.4 Key-Policy Attribute-Based Encapsulation with Switchable Attributes -- 3.5 Security Notions -- 4 Our SA-KP-ABE Scheme -- 4.1 Description of Our KP-ABE with Switchable Attributes -- 4.2 Del-IND-Security of Our SA-KP-ABE for Encaps -- 4.3 Del-IND-Security of Our SA-KP-ABE for

Encaps* -- 4.4 Distinct Indistinguishability Properties -- 4.5 Attribute-Indistinguishability -- 5 Application to Tracing -- 6 Conclusion -- References -- Mix-Nets from Re-randomizable and Replayable CCA-Secure Public-Key Encryption -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Related Work -- 2 Preliminaries -- 3 Definitions -- 4 Mix-Net -- 5 A Concrete Mix-Net Protocol from RCCA-PKE -- 5.1 Split PKE -- 5.2 A Protocol for Verify-then-Decrypt for Verifiable Split PKE -- 5.3 Our Concrete Verifiable Split PKE -- 5.4 Putting All Together -- References -- New and Improved Constructions for Partially Equivocal Public Key Encryption -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Technical Overview -- 2 Preliminaries -- 2.1 Reminders on Standard Assumptions -- 2.2 Non-Committing Encryption -- 3 PEPE Constructions -- 3.1 PEPE from LWE -- 3.2 PEPE from DDH -- 3.3 PEPE from Subgroup Decision -- References -- On Access Control Encryption Without Sanitization -- 1 Introduction -- 2 Our Results -- 2.1 Modeling ACE Without Sanitization -- 2.2 Instantiating ACEnoS and VACE -- 2.3 Concurrent Work -- 2.4 Future Directions -- 3 Access Control Encryption Without Sanitization -- 4 Linear ACE Without Sanitizer from PKE -- 5 Compact ACE from Hybrid Encryption -- 6 Game-Specific Obfuscation -- 7 ACE with Ciphertext Verifiability. 7.1 Ciphertext Verifiability -- 7.2 VACE from Game Specific Obfuscation -- 7.3 No Secret Write Rule of VACE -- References -- Watermarkable Public Key Encryption with Efficient Extraction Under Standard Assumptions -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Technical Overview of Our Construction -- 1.3 Relations to Prior Work -- 2 Preliminaries -- 3 Watermarkable Public Key Encryption -- 4 Our Watermarkable PKE Scheme -- 5 Security Analysis -- 5.1 Encryption Correctness and IND-CPA Security -- 5.2 Extraction Correctness -- 5.3 Proving Unremovability and Unforgeability Properties -- References -- Authentication and Signatures -- A Provably Secure, Lightweight Protocol for Anonymous Authentication -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Outline of the Paper -- 2 Model and Definitions -- 2.1 Preliminaries -- 2.2 Desynchronization Resilience -- 2.3 Mutual Authentication -- 2.4 Tag Anonymity -- 3 Protocol Description -- 4 Proofs of Security -- 4.1 Mutual Authentication -- 4.2 Desynchronization Resilience -- 4.3 Tag Anonymity -- References -- Anonymous Authenticated Communication -- 1 Introduction -- 1.1 Background and Motivation -- 1.2 Related Work -- 1.3 Contributions -- 1.4 Outline -- 2 Preliminaries -- 2.1 Notation -- 2.2 Constructive Cryptography -- 2.3 Anonymous and Authentic Resources -- 3 Achieving Anonymous Authenticity -- 3.1 Game-Based Security of Bilateral Signatures -- 3.2 Composability Security of Bilateral Signatures -- 4 Achieving De-anonymizable Authenticity -- 4.1 Game-Based Security of Partial Signatures -- 4.2 Composability Security of Partial Signatures -- 5 Achieving Receiver-Side Anonymous Authenticity -- 5.1 Game-Based Security of Ring Signatures -- 5.2 Composability Security of Ring Signatures -- 6 Concluding Remarks and Future Work -- References -- Credential Transparency System -- 1 Introduction. 1.1 Definitional Framework for Diverse Credential Systems -- 2 Credential Transparency System (CTS) -- 2.1 Security Properties -- 3 CTS Construction -- 3.1 Overview of Our Construction -- 3.2 Construction Description -- 3.3 Simulation Algorithms -- 4 Security Proof -- 4.1 Intuition for the Proof of Soundness -- 4.2 Intuition for the Proof of Privacy -- References -- Cumulatively All-Lossy-But-One Trapdoor Functions from Standard Assumptions -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Technical Overview -- 1.3 Related Work -- 2 Background -- 2.1 Cumulatively All-Lossy-But-One Trapdoor Functions -- 2.2 Lattices -- 2.3 Composite Residuosity -- 3

Cumulatively All-Lossy-But-One Trapdoor Functions -- 3.1 Relaxed CALBO-TDFs from LWE -- 3.2 CALBO-TDFs from DCR -- References -- On the Related-Key Attack Security of Authenticated Encryption Schemes -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Related Work -- 2 Preliminaries -- 2.1 Notation -- 2.2 Primitives -- 2.3 Security Notions Against Related-Key Attacks -- 3 RKA Security Notions for Nonce-Based AEAD -- 3.1 Nonce Selection -- 3.2 RKA-Security Notions for AEAD Schemes -- 3.3 RKA-Security Against Nonce Misuse -- 3.4 RKA-Security Notions for Encryption -- 4 RKA Security of the N1, N2, and N3 Constructions -- 4.1 N1 - Instantiation of Encrypt-and-MAC -- 4.2 N2 - Instantiation of Encrypt-then-MAC -- 4.3 N3 - Instantiation of MAC-then-Encrypt -- 5 RKA Nonce-Misuse-Resistant AEAD -- References -- The State of the Union: Union-Only Signatures for Data Aggregation -- 1 Introduction -- 2 Syntax -- 3 Security Definitions -- 3.1 Notation -- 3.2 Unforgeability -- 3.3 History Hiding -- 4 A UOS Scheme -- 4.1 Initial Construction -- 4.2 Secure Variant from Groups of Unknown Order -- 4.3 Secure Variant from Lattices -- 4.4 Security Analysis -- 5 Performance -- 6 Conclusion -- References. Traceable Constant-Size Multi-authority Credentials.

Sommario/riassunto

This book constitutes the proceedings of the 13th International Conference on Security and Cryptography for Networks, SCN 2022, held in Amalfi, Italy, in September 2022. The 33 full papers presented in this volume were carefully reviewed and selected from 101 submissions. They are organized in topical sections: Ciphers, Cryptanalysis, Defenses; Public Key Encryption; Authentication and Signatures, Multiparty Computation; Zero-Knowledge Proofs and Applications.
