1. Record Nr. UNISA996495571903316

Autore	Dodis Yevgeniy
Titolo	Advances in cryptology - CRYPTO 2022 . Part I : 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, proceedings / / Yevgeniy Dodis and Thomas Shrimpton
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2022] ©2022
ISBN	3-031-15802-4
Descrizione fisica	1 online resource (822 pages)
Collana	Lecture Notes in Computer Science
Disciplina	005.8
Soggetti	Computer security Data encryption (Computer science)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Organization -- Contents - Part I -- Cryptanalysis I -- Rotational Differential-Linear Distinguishers of ARX Ciphers with Arbitrary Output Linear Masks -- 1 Introduction -- 2 Notations and Preliminaries -- 2.1 Modulo Addition with an Initial Carry Bit -- 2.2 Useful Partitions of F2k F2k -- 3 Ordinary Differential-Linear Correlation of -- 4 Rotational Differential-Linear Correlation of -- 5 Computing the (Rotational) Differential-Linear Correlation of Iterative ARX Primitives -- 6 Applications to ARX Primitives -- 6.1 Cryptanalysis of Alzette -- 6.2 Cryptanalysis of SipHash -- 6.3 Cryptanalysis of SPECK -- 6.4 Cryptanalysis of ChaCha -- 7 Conclusion, Discussion, and Open Problems -- References -- Implicit White-Box Implementations: White-Boxing ARX Ciphers -- 1 Introduction -- 1.1 Contributions -- 2 Preliminaries -- 2.1 Implicit Functions, Self-equivalences and Graph Automorphisms -- 2.2 Encoded Implementations -- 3 Implicit White-Box Implementations -- 3.1 Quasilinear Implicit Round Functions -- 4 Security Analysis -- 4.1 Previous Generic Attacks -- 4.2 Reducing Implicit Implementations to Self-equivalence Implementations -- 5 Self-equivalences of Modular Addition -- 5.1 Computing Self-equivalences from a CCZ-Equivalent Function -- 5.2 Self-equivalences and Graph Automorphisms of the Permuted Modular Addition -- 6 An

Implicit Implementation of an ARX Cipher -- 7 Conclusion -- A Affine Self-equivalences of the Permuted Modular Addition with Wordsize 4 -- References -- Superposition Meet-in-the-Middle Attacks: Updates on Fundamental Security of AES-like Hashing -- 1 Introduction -- 1.1 Our Contribution -- 2 AES-like Hashing and MITM Preimage Attacks -- 3 MILP Model for the Configuration Search -- 3.1 Basic MILP Model for MITM -- 3.2 Superposition States and Separate Attribute-Propagation. 3.3 Multiple Ways of AddRoundKey (MulAK) -- 3.4 Enhanced Model with Guess-and-Determine (GnD) -- 3.5 Transforming to Models for Searching for Collision Attacks -- 3.6 Exploit Symmetry of the Ciphers -- 4 Application to Preimage Attacks on Whirlpool -- 4.1 New Attacks Resulted from Applying the MILP Modeling -- 4.2 Discussions on the New Attacks -- 5 Application to Preimage Attacks on Grøstl -- 5.1 New Attacks Resulted from Applying the MILP Modeling -- 5.2 Discussions on the New Attacks -- 6 Applications to Collision and Key-Recovery Attacks -- References -- Triangulating Rebound Attack on AES-like Hashing -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Novelty and Comparison with Previous Works -- 2 Preliminaries -- 2.1 AES-like Hashing -- 2.2 The Rebound Attack -- 2.3 The Super-Sbox Technique -- 2.4 Triangulation Algorithm -- 2.5 Collision Attacks and Its Variants -- 3 Triangulating Rebound Attack -- 3.1 Solving Non-full-active Super-Sbox by Key Bytes -- 3.2 Connecting Multiple Inbound Phases by Key Bytes -- 3.3 The Triangulating Rebound Attack -- 4 Improved Collision Attacks on AES-128-MMO -- 4.1 Semi-free-start Collision Attack on 7-Round AES-128 -- 4.2 Semi-free-start Collision Attack on 8-Round AES-128-MMO -- 4.3 Quantum Collision Attack on 8-Round AES-128 -- 5 Improved Quantum Attacks on Saturnin-Hash -- 5.1 Improved 8-Round Quantum Free-Start Collision -- 5.2 Extend the Attack to 10-round Free-Start Collision -- 6 Quantum Collision Attack on SKINNY-128-384-MMO -- 6.1 21-Round Quantum Free-Start Collision Attack -- 6.2 Classic Free-Start Collision Attack on 19-Round -- 7 Discussion and Conclusion -- 7.1 Possible Generalization of Triangulating Rebound -- 7.2 Conclusion -- References -- Randomness -- Public Randomness Extraction with Ephemeral Roles and Worst-Case Corruptions -- 1 Introduction -- 1.1 The Motivation Behind Our Setting.
1.2 Other Related Work -- 1.3 Our Contributions -- 1.4 Technical Overview -- 1.5 Directions for Future Research -- 2 Network Models for Randomness Extraction -- 2.1 The Sending-Leaks Adversarial Model -- 2.2 The Execution-Leaks Adversarial Model -- 3 Zero-Error Randomness Extraction Protocols -- 3.1 Zero-Error Randomness Extraction in the Sending-Leaks Model -- 3.2 Improved Zero-Error Randomness Extraction in the Execution-Leaks Model -- 4 Low-Error Randomness Extraction Is Impossible with n/4 Corruptions -- References -- (Nondeterministic) Hardness vs. Non-malleability -- 1 Introduction -- 1.1 Hardness Assumptions for Nondeterministic and i-Circuits -- 1.2 Our Results-Included in This Work -- 1.3 Our Results-Included in the Full Version ch6ePrint:BalDacLos22 -- 1.4 Technical Overview -- 1.5 Related Work -- 2 Preliminaries -- 2.1 Complexity Classes and Assumptions -- 2.2 Non-malleable Codes -- 2.3 Seed-Extending Pseudorandom Generators -- 3 A Non-malleable Code for Small Circuit Tampering -- References -- Short Leakage Resilient and Non-malleable Secret Sharing Schemes -- 1 Introduction -- 1.1 Our Results -- 1.2 Technical Overview -- 1.3 Related Work -- 1.4 Organization of the Paper -- 2 Preliminaries -- 2.1 Notation -- 2.2 Statistical Distance and Entropy - Definitions and Lemmata -- 2.3 Randomness Extractors -- 2.4 Secret Sharing Schemes -- 3 Leakage Resilient Secret Sharing Schemes -- 3.1 Local Leakage Family -- 3.2

Construction -- 3.3 Security Proof -- 3.4 Parameters -- 4 Non-malleable Secret Sharing Schemes -- 4.1 Building Blocks -- 4.2 Our Construction -- 4.3 Instantiation of Our Scheme -- References -- *-6ptCryptography from Pseudorandom Quantum States -- 1 Introduction -- 1.1 Our Results -- 1.2 Discussion: Why Explore a World Without One-Way Functions? -- 1.3 Technical Overview -- 1.4 Future Directions -- 2 Pseudorandom States.
2.1 Pseudorandom Function-Like State (PRFS) Generators -- 2.2 Testing Pseudorandom States -- 3 Constructing PRFS from PRS -- 4 Quantum Pseudo One-Time Pad from PRFS -- 5 Quantum Bit Commitments from PRFS -- 5.1 Definition -- 5.2 Construction -- 5.3 Application: Secure Computation -- References -- Quantum Cryptography I -- .26em plus .1em minus .1emCertified Everlasting Zero-Knowledge Proof for QMA*-10pt -- 1 Introduction -- 1.1 Background -- 1.2 Our Results -- 1.3 Technical Overview -- 1.4 Related Works -- 2 Preliminaries -- 2.1 Notations -- 2.2 Quantum Computation -- 2.3 QMA and k-SimQMA -- 2.4 Cryptographic Tools -- 3 Commitment with Certified Everlasting Hiding and Classical-Extractor-Based Binding -- 3.1 Definition -- 3.2 Construction -- 4 Certified Everlasting Zero-Knowledge Proof for QMA -- 4.1 Definition -- 4.2 Construction of Three Round Protocol -- 4.3 Sequential Repetition for Certified Everlasting Zero-Knowledge Proof for QMA -- References -- Quantum Commitments and Signatures Without One-Way Functions -- 1 Introduction -- 1.1 Background -- 1.2 Our Results -- 1.3 Technical Overviews -- 1.4 Concurrent Work -- 2 Preliminaries -- 2.1 Basic Notations -- 2.2 Pseudorandom Quantum States Generators -- 3 Commitments -- 3.1 Definition -- 3.2 Construction -- 3.3 Computational Hiding -- 3.4 Statistical Binding -- 4 Digital Signatures -- 4.1 One-Way Quantum States Generators -- 4.2 Definition of Digital Signatures with Quantum Public Keys -- 4.3 Construction -- 4.4 Security -- A Making Opening Message Classical -- B Equivalence of Binding Properties -- References -- Semi-quantum Tokenized Signatures -- 1 Introduction -- 1.1 The Advantages of Quantum Signature Tokens -- 1.2 Semi-quantum Tokenized Signatures -- 1.3 Results -- 2 Technical Overview -- 2.1 Semi-quantum CCD Tokens and Fully-quantum Signature Tokens -- 2.2 Signing Coset States by Splitting.
2.3 Proving CCD Security Versus Proving Tokenized Signing Security -- 2.4 Hardness of Concentration in Dual of Obfuscated Subspace -- 3 Semi-quantum Tokenized Signatures Construction -- 3.1 Correctness and Security Against Sabotage -- References -- Secure Multiparty Computation I -- Structure-Aware Private Set Intersection, with Applications to Fuzzy Matching -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Work -- 2 Preliminaries -- 2.1 Hamming Correlation Robustness -- 3 Building Blocks -- 3.1 2PC Ideal Functionalities -- 3.2 Function Secret Sharing -- 3.3 Oblivious Key Value Store -- 4 bFSS Constructions -- 4.1 Existing Schemes -- 4.2 New concat Technique for Cross Products -- 4.3 New Spatial Hashing Technique -- 4.4 xor-share Technique -- 5 Structure-Aware PSI from bFSS -- 5.1 Costs -- 5.2 Other Protocols as Instances of Our Framework -- 5.3 bFSS Performance -- 6 Fuzzy PSI Application and Performance -- 6.1 Performance Comparison -- 6.2 Implementation -- 7 Limitation and Open Problems -- References -- .28em plus .1em minus .1emTwo-Round MPC Without Round Collapsing Revisited - Towards Efficient Malicious Protocols*-12pt -- 1 Introduction -- 2 Technical Overview -- 2.1 Multi-party Randomized Encoding -- 2.2 Semi-Malicious Effective-Degree-2 MPRE -- 2.3 MPC for Effective-Degree-2 Functions -- 2.4 Lift Security with Output Substitution -- 2.5

Tensor OLE Correlated Randomness Generation from OT -- 3 Definition of Multi-Party Randomized Encoding -- 4 MPRE for Degree-3 Functions -- 4.1 Background: Semi-honest MPRE for Degree-3 Functions -- 4.2 CDS Encoding -- 4.3 Semi-Malicious MPRE for Degree-3 Functions -- 5 Putting Pieces Together -- References -- More Efficient Dishonest Majority Secure Computation over Z2k via Galois Rings -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Overview of Our Techniques -- 1.3 Related Work.
1.4 Organization of the Paper.