1.

Record Nr.	UNISA996466472003316
Titolo	Advances in Cryptology – CRYPTO 2017 [[electronic resource]] : 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20–24, 2017, Proceedings, Part II / / edited by Jonathan Katz, Hovav Shacham
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2017
ISBN	3-319-63715-0
Edizione	[1st ed. 2017.]
Descrizione fisica	1 online resource (XV, 735 p. 100 illus.)
Collana	Security and Cryptology ; ; 10402
Disciplina	004
Soggetti	Data encryption (Computer science) Computer security Computer communication systems Software engineering Management information systems Computer science Coding theory Information theory Cryptology Systems and Data Security Computer Communication Networks Software Engineering Management of Computing and Information Systems Coding and Information Theory
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Intro -- Preface -- Crypto 2017 The 37th IACR International Cryptology Conference -- Contents - Part II -- OT and ORAM -- Secure Computation Based on Leaky Correlations: High Resilience Setting -- 1 Introduction -- 1.1 Model -- 1.2 Our Contribution -- 1.3 Prior Relevant Works -- 1.4 Technical Overview -- 2 Preliminaries -- 2.1 Functionalities and Correlations -- 2.2 Toeplitz Matrix Distribution --

2.3 Graph Representation of Correlations -- 3 Extracting One OLE over a Large Field -- 3.1 Extraction of One Secure [K] Correlation -- 3.2 Securely Realizing [K] Using [K] Correlation -- 4 Embedding Multiple s into an over an Extension Field -- 4.1 Intuition of the Embedding -- 4.2 Relevant Prior Work on 3-Free Sets -- 4.3 Generating Explicit Embedding and Proof of Theorem 1 -- 5 Simple Partition Number -- 5.1 Intuition of the Hardness of Computation Result -- 5.2 Relevant Prior Work on Graph Covering Problems -- 5.3 Relation to Leakage Resilience: Proof of Lemma 4 -- 5.4 Estimates of Simple Partition Number and Proof of Theorem 2 -- 5.5 Subsuming the Partition Argument -- 5.6 Relevant Prior Work on Common Information and Assisted Common Information -- 5.7 Analogy of Biclique Partition Number and Wyner's Common Information -- References -- Laconic Oblivious Transfer and Its Applications -- 1 Introduction -- 1.1 Laconic OT -- 1.2 Warm-Up Application: Non-interactive Secure Computation on Large Inputs -- 1.3 Main Application: Multi-hop Homomorphic Encryption for RAM Programs -- 1.4 Roadmap -- 2 Technical Overview -- 2.1 Laconic OT -- 2.2 Non-interactive Secure Computation on Large Inputs -- 2.3 Multi-hop Homomorphic Encryption for RAM Programs -- 3 Laconic Oblivious Transfer -- 3.1 Laconic OT -- 3.2 Updatable Laconic OT -- 4 Laconic Oblivious Transfer with Factor-2 Compression -- 4.1 Somewhere Statistically Binding Hash Functions and Hash Proof Systems.

4.2 HPS-friendly SSB Hashing -- 4.3 A Hash Proof System for Knowledge of Preimage Bits -- 4.4 The Laconic OT Scheme -- 5 Construction of Updatable Laconic OT -- 5.1 Background -- 5.2 Construction Overview -- References -- Black-Box Parallel Garbled RAM -- 1 Introduction -- 1.1 Problem Statement -- 1.2 Comparison with Previous Work -- 1.3 Our Results -- 1.4 Overview of New Ideas for Our Construction -- 1.5 Roadmap -- 2 Preliminaries -- 2.1 Notation -- 2.2 PRAM: Parallel RAM Programs -- 2.3 Garbled Circuits -- 2.4 Oblivious PRAM -- 2.5 Garbled Parallel RAM -- 3 Construction of Black-Box Parallel GRAM -- 3.1 Overview -- 3.2 Data Garbling: (, s) GData(1, D) -- 3.3 Program Garbling: (,sin) GProg(1, 1logN, 1t, , s, told) -- 3.4 Input Garbling: GInput(1, x,sin) -- 3.5 Garbled Evaluation: y GEval(,) -- 4 Cost and Correctness Analysis -- 4.1 Overall Cost -- 4.2 Correctness -- 5 Main Theorem -- References -- A UMA2-security Proof -- B UMA2 to Full Security -- Foundations II -- Non-Malleable Codes for Space-Bounded Tampering -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Additional Related Work -- 2 Preliminaries -- 2.1 Notation -- 2.2 Coding Schemes -- 3 Non-Malleability in Bounded Space -- 3.1 Space-Bounded Tampering -- 3.2 Achievable Parameters -- 4 Building Blocks -- 4.1 Random Oracles -- 4.2 Merkle Commitments -- 4.3 Graph Pebbling and Labeling -- 5 Non-Interactive Proofs of Space -- 5.1 NIPoS Definition -- 5.2 NIPoS Construction -- 6 Our Coding Scheme -- 6.1 Code Construction -- 6.2 Proof of Security -- 6.3 Concrete Instantiation and Parameters -- 7 Trading Leakage for Tamper-Proof Security -- 7.1 Leaky Tamper Simulatability -- 7.2 Analysis -- References -- Four-Round Concurrent Non-Malleable Commitments from One-Way Functions -- 1 Introduction -- 1.1 Our Results -- 1.2 3-Round Concurrent Non-Malleable Commitments -- 1.3 The New State of the Art.

2 Definitions and Tools -- 2.1 Preliminaries -- 2.2 2-Round Instance-Dependent Trapdoor Commitments -- 2.3 Non-Malleable Commitments -- 2.4 New Definitions: Weak NM and SimWI -- 3 4-Round One-Many SimWI from OWFs -- 4 4-Round Concurrent NM Commitment Scheme -- 5 3-Round NM Commitments from Strong OWPs -- 5.1 Synchronous NM Commitment Scheme -- 5.2 3-Round

NM Commitment Scheme: NMCom=(NMSen,NMRec) -- References -- Distinguisher-Dependent Simulation in Two Rounds and its Applications -- 1 Introduction -- 1.1 Our Results -- 1.2 Discussion -- 1.3 Related Work -- 1.4 Organization -- 2 Technical Overview -- 2.1 Argument Systems -- 2.2 Applications -- 3 Preliminaries -- 4 Definitions -- 4.1 Proof Systems -- 5 Two Round Argument Systems -- 5.1 Construction -- 5.2 Adaptive Soundness -- 5.3 Witness Indistinguishability -- 5.4 Distributional Weak Zero Knowledge -- 5.5 Strong Witness Indistinguishability -- 5.6 Witness Hiding -- 5.7 Extensions -- References -- Obfuscation II -- Incremental Program Obfuscation -- 1 Introduction -- 1.1 Our Contributions -- 1.2 An Overview of Our Approach -- 1.3 Related Work -- 2 Definitions and Preliminaries -- 2.1 Indistinguishability Obfuscators -- 2.2 Somewhere Statistically Binding Hash -- 2.3 Oblivious RAM -- 2.4 Non-interactive Zero-Knowledge Proofs -- 3 Modeling Incremental Obfuscation -- 3.1 Incremental Indistinguishability Obfuscation -- 3.2 Incremental VGB and VBB Obfuscation -- 4 Our Construction -- 5 Amplifying Security to Increment-Private IIO -- 6 The Lower Bound -- 7 Best Possible Incremental Obfuscation -- 8 Extensions and Future Work -- References -- From Obfuscation to the Security of Fiat-Shamir for Proofs -- 1 Introduction -- 1.1 Our Results -- 1.2 Overview -- 2 Preliminaries -- 2.1 Indistinguishability -- 2.2 Puncturable PRFs -- 2.3 Indistinguishability Obfuscation -- 2.4 Input-Hiding Obfuscation.

2.5 Interactive Proofs and Arguments -- 2.6 The Fiat-Shamir Paradigm -- 3 Security of Fiat-Shamir for 3-Message Proofs -- 4 Security of Fiat-Shamir for Multi-round Proofs -- References -- Indistinguishability Obfuscation for Turing Machines: Constant Overhead and Amortization -- 1 Introduction -- 1.1 Our Results -- 1.2 Technical Overview: New Template for Succinct iO -- 1.3 Technical Overview: Boostrapping Theorem -- 1.4 Related Work -- 2 Attribute-Based Encryption for TMs with Additive Overhead -- 2.1 Definition -- 2.2 Construction of 1-Key ABE -- 2.3 1-Key Two-Outcome ABE for TMs -- 3 Oblivious Evaluation Encodings -- 3.1 Definition -- References -- Quantum -- Quantum Security of NMAC and Related Constructions -- 1 Introduction -- 1.1 Our Contributions -- 2 Preliminaries -- 2.1 Notations and Conventions -- 2.2 I.i.d Samples of Functions -- 2.3 Various Security Notions of PRFs -- 2.4 NMAC and Related Constructions -- 2.5 Implementing Oracles -- 3 Relative Oracle Indistinguishability of Functions -- 4 Security Against Key Recovery and Security Under Random Leakage -- 4.1 Security of PRFs Against Key Recovery -- 4.2 Security of PRFs Under Random Leakage -- 4.3 Oracle-Secure PRF Under Random Leakage -- 5 Security of NMAC and Other Constructions -- 5.1 Security of the Cascade -- 5.2 Security of NMAC -- 5.3 Security of HMAC -- 5.4 Security of the Augmented Cascade and AMAC -- References -- Quantum Non-malleability and Authentication -- 1 Introduction -- 1.1 Summary of Contributions -- 2 Preliminaries -- 2.1 Quantum States, Registers, and Channels -- 2.2 Unitary Designs -- 3 The Zero-Error Setting -- 3.1 Perfect Secrecy -- 3.2 A New Notion of Non-malleability -- 4 The Approximate Setting -- 4.1 Approximate Non-malleability -- 4.2 Authentication -- References -- A Technical lemmas -- B Proof of characterization theorem.

New Security Notions and Feasibility Results for Authentication of Quantum Data -- 1 Introduction -- 1.1 Quantum Attacks on Classical Protocols -- 1.2 Quantum Authentication of Quantum Data -- 2 Our Contributions -- 2.1 A New Security Definition for Classical Authentication -- 2.2 Definitions for Quantum Authentication -- 2.3 Subsequent Work -- 3 Preliminaries -- 3.1 Notation -- 3.2 Basic Definitions for Authentication -- 4 Security Framework for Quantum

Authentication -- 4.1 Basis-Dependent Authentication -- 4.2 Total Authentication -- 4.3 Total Authentication with Key Leakage -- 4.4 A Remark About Efficiency -- 4.5 Comparison with security definition in -- 5 Properties of Security Definitions -- 5.1 Properties of Basis-Dependent Authentication -- 5.2 Properties of Total Authentication -- 6 Quantum MACs from 3-universal Hashing -- 7 Total Authentication (with Key Leakage) from Complementary Classical Authentication -- 7.1 The Auth-QFT-Auth Scheme -- 8 Total Authentication from Approximate Unitary Designs -- 8.1 The Unitary Design Scheme -- 9 A Lifting Theorem for Authentication -- 10 Open Problems -- References -- Hash Functions -- Time-Memory Tradeoff Attacks on the MTP Proof-of-Work Scheme -- 1 Introduction -- 2 Egalitarian Computing Framework -- 3 Description and Previous Analysis of MTP -- 3.1 Previous Tradeoff analysis of MTP -- 3.2 Instantiation of MTP -- 4 Overview of the Attack on MTP -- 4.1 A Trivial Attack -- 4.2 Weaknesses of MTP -- 4.3 General Description of the Attack -- 5 Details of the Attack -- 5.1 Balancing the Phases -- 5.2 Using Preprocessing -- 6 Analysis of the Full Attack -- 6.1 Concrete Parameters -- 6.2 Comparison with the Analysis of -- 7 Extensions of the Attack -- 8 Countermeasures -- 9 Conclusion -- References -- A Merkle Hash Trees -- B The Indexing Function of Argon2d -- C Optimizing Phase 1 for Argon2d.
Functional Graph Revisited: Updates on (Second) Preimage Attacks on Hash Combiners.

Sommario/riassunto

The three volume-set, LNCS 10401, LNCS 10402, and LNCS 10403, constitutes the refereed proceedings of the 37th Annual International Cryptology Conference, CRYPTO 2017, held in Santa Barbara, CA, USA, in August 2017. The 72 revised full papers presented were carefully reviewed and selected from 311 submissions. The papers are organized in the following topical sections: functional encryption; foundations; two-party computation; bitcoin; multiparty computation; award papers; obfuscation; conditional disclosure of secrets; OT and ORAM; quantum; hash functions; lattices; signatures; block ciphers; authenticated encryption; public-key encryption, stream ciphers, lattice crypto; leakage and subversion; symmetric-key crypto, and real-world crypto.