1. Record Nr. UNISA996464418403316

Titolo	Theory of cryptography : 19th international conference, TCC 2021, Raleigh, NC, USA, November 8-11, 2021 : proceedings : part III / / edited by Kobbi Nissim and Brent Waters
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2021] ©2021
ISBN	3-030-90456-3
Descrizione fisica	1 online resource (525 pages)
Collana	Lecture Notes in Computer Science ; ; v.13044
Disciplina	005.824
Soggetti	Computer security Data encryption (Computer science) Computer 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 -- Contents - Part III -- Covert Learning: How to Learn with an Untrusted Intermediary -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Real World Applications -- 1.3 Related Work -- 2 Covert Learning -- 2.1 Preliminaries -- 2.2 Definition of Covert Learning -- 2.3 A Warm-Up: Covert Learning of Noisy Parity Functions -- 2.4 Covert Learning of Low-Degree Fourier Coefficients -- 2.5 Covert Learning of Polynomial Size Decision Trees -- 3 Covert Verifiable Learning -- 3.1 Definition of Covert Verifiable Learning -- 3.2 Making CLF Verifiable -- 3.3 Making CLDT Verifiable -- 3.4 Verifiability Without Secret Examples -- References -- Random-Index PIR and Applications -- 1 Introduction -- 1.1 Random-Index PIR (RPIR) -- 1.2 Applications -- 1.3 Batch RPIR -- 1.4 Multi-server RPIR -- 1.5 Organization -- 2 Random-Index Private Information Retrieval -- 2.1 Background: Private Information Retrieval -- 2.2 Defining RPIR -- 2.3 Defining Multi-server RPIR -- 2.4 RPIR is equivalent to PIR -- 3 RPIR Protocols -- 3.1 Noninteractive RPIR -- 3.2 Multi-server RPIR Protocols -- 4 Applications to Large-Scale DoS-Resistant Computation -- 4.1 Target Anonymous Communication Channels from RPIR -- 5 Batch RPIR -- 5.1 Definitions -- 5.2 Constructions -- A Random-Index Oblivious-RAM -- A.1 Target Anonymous Channels from RORAM -- B Target

Anonymous Channels from Mix-Nets -- References -- Forward Secret Encrypted RAM: Lower Bounds and Applications -- 1 Introduction -- 1.1 Our Main Result: Lower Bound -- 1.2 ``Bypassing'' the Lower Bound -- 2 Lower Bound Model -- 2.1 Framework for Symbolic Private Data Structure Lower Bounds -- 2.2 Symbolic Definitions for Allowed Primitives -- 2.3 FS eRAM Symbolic Definition -- 3 Forward Secret Encrypted RAM Lower Bound -- 3.1 Minimality and Usefulness -- 3.2 Key-Data Graph -- 3.3 Adversarial Strategy.
4 Stronger Forward Secret Encrypted RAM Definitions -- 5 Oblivious Forward Secret Encrypted RAM -- 5.1 Definitions -- 5.2 Oblivious Forward Secret Encrypted RAM Construction -- 6 Forward Secret Memory Checkers -- 6.1 Forward Secret Memory Checker Definition -- 6.2 Forward Secret Memory Checker Construction -- References -- Laconic Private Set Intersection and Applications -- 1 Introduction -- 1.1 Our Results -- 1.2 Previous Work -- 1.3 Open Problems -- 2 Technical Overview -- 2.1 Semi-Honest PSI from CDH/LWE -- 2.2 Reusable Laconic PSI -- 2.3 DV-NIZK Range Proofs for DJ Ciphertexts -- 2.4 Labeled Laconic PSI and Laconic OT -- 3 Preliminaries -- 3.1 Hardness Assumptions -- 3.2 Laconic Private Set Intersection -- 4 Semi-Honest Laconic PSI from CDH/LWE -- 5 Reusable DV-NIZK Range Proofs for DJ Ciphertexts -- 5.1 Equality of Plaintexts in DJ and BGN Ciphertexts -- 5.2 DV-NIZK for Range Proofs of DJ Ciphertexts with Equal Discrete Log -- 6 Reusable Laconic Private Set Intersection -- 7 Self-Detecting Encryption -- References -- Amortizing Rate-1 OT and Applications to PIR and PSI -- 1 Introduction -- 1.1 Our Results -- 1.2 Applications -- 1.3 Comparison with Prior Work -- 2 Technical Overview -- 3 Preliminaries and Definitions -- 3.1 Amortized Rate-1 OT: Definition -- 4 Amortized Rate-1 OT from SXDH -- 4.1 Our Construction -- 4.2 Receiver Privacy -- 5 Amortized Rate-1 OT from Bilinear Power DDH -- 5.1 Receiver Privacy -- 6 Optimization -- 6.1 Delayed Pairing -- 6.2 Increasing Vector Dimension -- 7 Applications -- 7.1 Secure Function Evaluation on Branching Programs -- 7.2 PSI and PIR -- 7.3 Optimization for PSI and PSI-Cardinality -- 7.4 Other Variants of PSI and PIR -- 8 Amortized Rate-1 OT with Strong Sender Privacy -- References -- Ring-Based Identity Based Encryption - Asymptotically Shorter MPK and Tighter Security -- 1 Introduction. 1.1 Our Contributions -- 1.2 Technical Overview -- 2 Preliminaries -- 2.1 Identity-Based Encryption (IBE) -- 2.2 Concrete Bit-Security -- 2.3 Lattices and Gaussian Distributions -- 2.4 Rings and Ideal Lattices -- 3 New Homomorphic Equality Test and Tighter Analysis -- 3.1 Homomorphic Equality Testing -- 3.2 Our Construction -- 3.3 An Optimization with Tighter Analysis -- 3.4 Application to Packing/Unpacking Homomorphic Encodings -- 4 New Partition Function and Homomorphic Evaluation -- 4.1 Our New Hash Function Family -- 4.2 Homomorphic Evaluation of the Partitioning Function -- 5 IBE Design and Analysis -- 5.1 Construction -- 5.2 Security -- 5.3 Asymptotic and Concrete Parameters -- References -- Cryptographic Shallots: A Formal Treatment of Repliable Onion Encryption -- 1 Introduction -- 2 Repliable Onion Encryption: Syntax and Correctness -- 2.1 Onion Evolutions, Forward Paths, Return Paths and Layerings -- 3 FROES: Onion Routing in the SUC Framework -- 3.1 Ideal Functionality FROES -- 3.2 SUC-realizability of FROES -- 4 Repliable-Onion Security: A Game-Based Definition -- 5 Repliable-Onion Security SUC-Realizability of FROES -- 6 Shallot Encryption -- 7 Shallot Encryption Scheme Is Secure -- A Security Game for Variants (b) and (c) -- References -- Grafting Key Trees: Efficient Key Management for Overlapping Groups -- 1 Introduction -- 1.1 The Asymptotic Setting -- 1.2 The Non-asymptotic Setting -- 1.3 Related Work -- 2 Preliminaries

-- 2.1 Notation -- 2.2 Huffman Codes -- 3 Key-Derivation Graphs for Multiple Groups -- 3.1 Continuous Group-Key Agreement and Multicast Encryption -- 3.2 Key-Derivation Graphs -- 3.3 Security -- 3.4 The Trivial Algorithm -- 4 Key-Derivation Graphs in the Asymptotic Setting -- 4.1 Key-Derivation Graphs in the Asymptotic Setting -- 4.2 Update Cost for Concrete Group Systems.
5 A Greedy Algorithm Based on Huffman Codes -- 5.1 Algorithm Description -- 5.2 Total Update Cost -- 5.3 Asymptotic Optimality of Boolean-Lattice Based Graphs -- 6 Lower Bound on the Update Cost of CGKA -- 6.1 Symbolic Model -- 6.2 Lower Bound on the Average Update Cost -- 7 Open Problems -- 7.1 Optimal Key-Derivation Graphs -- 7.2 Security -- 7.3 Efficiency of Dynamic Operations -- References -- Updatable Public Key Encryption in the Standard Model -- 1 Introduction -- 1.1 Our Technique: Using Circular Security and Leakage-Resilience -- 1.2 Additional Theoretical Contributions -- 1.3 Related Work -- 2 Preliminaries -- 3 Updatable Public Key Encryption (UPKE) -- 3.1 IND-CR-CPA Security of UPKE -- 4 Key-Dependent-Message-Secure Encryption Scheme -- 5 DDH Based Construction -- 5.1 The BHHO Cryptosystem -- 5.2 CS+LR Security of BHHO Cryptosystem -- 5.3 UPKE Construction -- 5.4 Security of the UPKE Construction -- 6 Constructions Based on LWE -- 6.1 The Dual Regev or GPV Cryptosystem -- 6.2 CS+LR Security of the Dual-Regev Cryptosystem -- 6.3 UPKE Construction -- 6.4 Security of the UPKE Construction -- 7 Towards Stronger Security -- References -- Towards Tight Adaptive Security of Non-interactive Key Exchange -- 1 Introduction -- 1.1 Technical Overview -- 2 Preliminaries -- 2.1 Pairing Group Assumptions -- 2.2 Non-Interactive Key Exchange -- 3 An Inner-Product-Based NIKE Scheme -- 4 Lower Bound -- 4.1 Lower Bound for Inner-product NIKEs -- References -- On the Impossibility of Purely Algebraic Signatures -- 1 Introduction -- 1.1 Related Work -- 1.2 Technical Outline -- 2 Preliminaries -- 2.1 Notation -- 2.2 Generic Group Model -- 2.3 Signatures -- 3 Signature Schemes over Groups of Prime Order -- 3.1 Algebraic Signatures -- 3.2 Preparation -- 3.3 Impossibility of Secure Algebraic Signatures -- 4 Signature Schemes over Groups of Unknown Order.
4.1 Simplified Algebraic Signatures -- 4.2 Hermite Normal Form -- 4.3 An Inefficient AddColumn Procedure for Matrices in HNF -- 4.4 Impossibility of Simplified Algebraic Signatures -- 5 Extension: BLS Signatures Instantiated with Algebraic Hash Functions Are Insecure -- References -- Policy-Compliant Signatures -- 1 Introduction -- 1.1 Applications of PCS -- 1.2 Our Contributions and Organization of this Paper -- 1.3 Related Work -- 2 Preliminaries -- 3 Policy-Compliant Signatures -- 3.1 Adversarial Capabilities in the Security Games -- 3.2 Existential Unforgeability -- 3.3 Indistinguishability-Based Attribute Hiding -- 4 Construction of a Policy-Compliant Signature Scheme -- 4.1 The Scheme -- 4.2 Correctness -- 4.3 Existential Unforgeability -- 4.4 Indistinguishability-Based Attribute Hiding -- 4.5 Efficient Instantiations Based on Inner-Product PE -- 5 Universal Composability and SIM-Based PCS -- 5.1 Simulation-Based Attribute Hiding -- 5.2 On the SIM-Based Security of our Generic Scheme -- References -- Simple and Efficient Batch Verification Techniques for Verifiable Delay Functions -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Additional Related Work and Open Problems -- 1.3 Technical Overview -- 1.4 Paper Organization -- 2 Preliminaries -- 3 Succinct Proofs of Correct Exponentiation -- 3.1 The Basic Definition -- 3.2 Batch Proofs of Correct Exponentiation -- 4 Warm-Up: The Random Subset Compiler -- 5 Amplifying Soundness and Reducing Communication -- 6 An Improved Compiler from the Low Order Assumption -- 6.1 The

Compiler -- 6.2 Soundness Analysis Based on the Low Order Assumption -- References -- Non-malleable Vector Commitments via Local Equivocability -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Applications -- 1.3 Overview of Our Approach -- 1.4 Open Problems -- 1.5 Paper Organization -- 2 Preliminaries.
2.1 Equivocable Commitment Schemes.