1. Record Nr. UNICASRML0295433

Autore	Occorsio, Mario Rosario
Titolo	Lezioni di calcolo numerico / Mario Rosario Occorsio
Pubbl/distr/stampa	Napoli, : Liguori, 1978
Descrizione fisica	258 p. ; 23 cm.
Disciplina	515
Lingua di pubblicazione	Italiano
Formato	Materiale a stampa
Livello bibliografico	Monografia

2. Record Nr. UNISA996601563703316

Autore	Oswald Elisabeth
Titolo	Topics in Cryptology - CT-RSA 2024 : Cryptographers' Track at the RSA Conference 2024, San Francisco, CA, USA, May 6-9, 2024, Proceedings
Pubbl/distr/stampa	Cham : , : Springer International Publishing AG, , 2024 ©2024
ISBN	3-031-58868-1
Edizione	[1st ed.]
Descrizione fisica	1 online resource (490 pages)
Collana	Lecture Notes in Computer Science Series ; ; v.14643
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Organization -- Contents -- Public Key Cryptography -- A Public Key Identity-Based Revocation Scheme: -- 1 Introduction -- 1.1 Related Works -- 1.2 Our Contributions -- 1.3 Technical Overview -- 1.4 Comparison with Existing Pairing-Based Schemes -- 1.5 Organization of the Paper -- 2 Mathematical Tools and Preliminaries -- 2.1 Predicate Encryption -- 2.2 Min-Entropy Computational Assumptions -- 3 Generic Transformations Between

IPEs -- 3.1 Transformation Between PO-IPEs -- 3.2 Extending Transformation for PO-IPEs n Data-Attribute Vectors -- 3.3 Transformation Between n-PO-ZIPE and NIPE -- 4 Constructing a PO-ZIPE Scheme for n Data-Vectors -- 4.1 Instantiating nPOZIPE -- 5 Constructing an IBR Scheme -- 5.1 Instantiating IBR -- 6 Conclusion -- References -- Computational Security Analysis of the Full EDHOC Protocol -- 1 Introduction -- 1.1 Context -- 1.2 Related Work -- 1.3 Contributions -- 2 Security Model -- 2.1 Overview -- 2.2 Execution Environment -- 2.3 Assumptions and Building Blocks -- 3 Description of the EDHOC Protocol -- 4 Security Proofs -- 4.1 Security Bounds -- 4.2 Sketch of Proof -- 5 Concrete Evaluation -- 5.1 Bounds for Multi-user Security -- 5.2 Parameters and Concrete Advantages -- 6 Observations -- 7 Conclusion -- References -- Symmetric Cryptography -- The Multi-user Security of MACs via Universal Hashing in the Ideal Cipher Model -- 1 Introduction -- 1.1 Mu-PRF Security of HtE -- 1.2 Mu-PRF Security of XCBC/TMAC-Type HtE -- 1.3 Related Works -- 1.4 Comparison -- 1.5 Organization -- 2 Preliminaries -- 2.1 Notations -- 2.2 Multi-user PRF Security in the Ideal-Cipher (IC) Model -- 2.3 Mu-PRF Bound with Coefficient H Technique -- 3 Multi-user Security of HtE -- 3.1 Security Notions for Keyed Hash Functions in the IC Model -- 3.2 Specification of HtE -- 3.3 Security of HtE in the IC Model.
3.4 Intuition of the mu-PRF Security of HtE -- 4 Multi-user Security of XCBC/TMAC-Type HtE -- 4.1 Specification of HtXE -- 4.2 Security of HtXE -- 4.3 Intuition of the Security of HtXE in Theorem 2 -- 5 Regular and AXU Bounds for CBC and Applications -- 5.1 Specification of CBC -- 5.2 Regular and AXU Bounds of CBC in the IC Model -- 5.3 Mu-Security of HtE with CBC (EMAC) -- 5.4 Mu-Security of HtXE with CBC (XCBC and TMAC) -- 5.5 Outline of the Proof of Theorem 3 -- 6 Proof of Theorem 1 (Proof for HtE) -- 6.1 Overview -- 6.2 Definition -- 6.3 Adversary's View -- 6.4 Good and Bad Transcripts -- 6.5 Upper-Bounding Pr[TITbad] -- 6.6 Lower-Bounding Pr[TR=]/Pr[TI=] for Tgood -- 6.7 Conclusion of the Proof -- 7 Proof of Theorem 3 (Proof for CBC) -- 7.1 Notations -- 7.2 Super Query -- 7.3 The Upper-Bound 2 -- 7.4 Upper-Bounding Pr[collE1] -- 7.5 Upper-Bounding Pr[E2] -- 7.6 Upper-Bounding Pr[collE3] -- References -- Automated-Based Rebound Attacks on ACE Permutation -- 1 Introduction -- 2 Preliminaries -- 2.1 The ACE Permutation -- 2.2 Rebound Attack -- 3 SMT/SAT-Based Automatic Model -- 3.1 SMT-Based Model for Searching Differential Characteristics with the Minimum Number of Active SB-64s -- 3.2 SAT-Based Model for Searching Differential Characteristics with the Optimal Probability -- 4 Application to ACE Permutation -- 4.1 Differential Characteristics of ACE Permutation -- 4.2 The Algorithm for Searching Rebound Distinguisher of ACE Permutation -- 5 Rebound Attacks on ACE Permutation -- 5.1 11-Step Rebound Attacks Against ACE Permutation -- 5.2 14-Step Rebound Attacks Against ACE Permutation -- 5.3 13-Step Rebound Attacks Against ACE Permutation -- 6 Conclusions -- A The Experimental Results on ACE -- References -- The Exact Multi-user Security of 2-Key Triple DES -- 1 Introduction -- 1.1 Contributions -- 1.2 Organization -- 2 Basic Notation.
3 Mu-Security of 2kTE -- 3.1 Specification of 2kTE -- 3.2 Security Definition: Mu-SPRP Security in Ideal Cipher Model -- 3.3 Mu-SPRP Security of 2kTE -- 4 Overview and Tool for Proof of Theorem 1 -- 4.1 Proof Overview -- 4.2 Methodology for Proving the Mu-SPRP Security -- 4.3 Re-sampling Method -- 5 Proof of Theorem 1 -- 5.1 Definitions -- 5.2 Lazy Sampled Ideal Cipher -- 5.3 Adversary's View -- 5.4 Good and Bad Transcripts -- 5.5 Upper-Bounding Pr[TI Tbad] -- 5.6 Overview of Deriving the Lower-Bound of Pr[TR=]Pr[TI=] -- 5.7 Lower-

Bounding Pr[TR=]Pr[TI=] -- 6 Limited Security Enhancement by FX with 2kTE -- 6.1 Attacks on 2kTE-FX -- 7 Conclusion -- References -- Improved Meet-in-the-Middle Attacks on Nine Rounds of the AES-192 Block Cipher -- 1 Introduction -- 2 Preliminaries -- 2.1 Notation -- 2.2 The AES Block Cipher -- 2.3 Definitions and Properties About AES -- 3 Flaws in Li et al.'s MitM Attacks on 9-Round AES-192 -- 4 Correcting Li et al.'s 9-Round AES-192 Attacks Under Their Ideas -- 4.1 Corrected 5-Round MitM Distinguisher on AES-192 -- 4.2 Corrected Basic 9-Round AES-192 Attack -- 4.3 Corrected 9-Round AES-192 Attack Under Their Weak-Key Approach -- 4.4 A Remark -- 5 Improved 9-Round AES-192 Attacks with a New Trick -- 5.1 A 9-Round AES-192 Attack Using 4-Byte Key Relations -- 5.2 A 6-Round MitM Distinguisher and a 9-Round AES-192 Attack -- 5.3 A Note -- 6 Conclusion -- References -- Signatures -- Batch Signatures, Revisited -- 1 Introduction -- 1.1 Contributions -- 1.2 Discussion -- 2 Preliminaries -- 2.1 Hash Functions -- 2.2 Digital Signatures -- 2.3 Falcon Signature Scheme -- 3 Batch Signatures -- 4 Construction -- 5 Security Proof -- 6 Applications -- 6.1 Computation -- 6.2 Communication -- 6.3 Use-Cases -- 7 Implementation and Benchmark Setup -- 7.1 Implementation Details -- 7.2 Benchmark Setup -- References.
History-Free Sequential Aggregation of Hash-and-Sign Signatures -- 1 Introduction -- 2 Notation and Preliminaries -- 2.1 Trapdoor Functions -- 2.2 Digital Signatures -- 2.3 Hash-and-Sign Schemes -- 2.4 History-Free Sequential Aggregate Signature -- 3 Sequential Aggregation of Hash-and-Sign Signatures -- 3.1 Security Proof -- 4 Instantiation and Evaluation -- 4.1 Single-Signature Optimizations -- 5 Security of Existing Multivariate SAS Schemes -- 5.1 Multivariate FH-SAS -- 5.2 Description of the Forgery -- 5.3 Discussion -- 6 Conclusions -- A Missing Proofs -- A.1 Proof for strong PS-HF-UF-CMA security (Theorem 1) -- B Trapdoor Functions in Hash-and-Sign Signature Schemes -- B.1 UOV Trapdoor Function -- B.2 Original Unbalanced Oil and Vinegar -- B.3 Provable Unbalanced Oil and Vinegar -- B.4 MAYO -- B.5 Wave -- C PSF-Based Signatures -- References -- Attribute-Based Signatures with Advanced Delegation, and Tracing -- 1 Introduction -- 2 Preliminaries -- 2.1 Dual Pairing Vector Spaces -- 2.2 Change of Basis -- 2.3 Attribute-Based Signature -- 2.4 Security Model -- 2.5 Policies and Access-Trees -- 3 ABS with Attribute and Policy Delegation -- 3.1 Description of Our ABS Scheme -- 3.2 Security Results -- 4 Sketches of the Security Proofs -- 4.1 Perfect Anonymity -- 4.2 Existential Unforgeability -- 5 ABS with Traceability -- 5.1 Traceable ABS -- 5.2 Construction of Traceable ABS -- 5.3 Correctness -- 5.4 Security Results -- References -- Lattice-Based Threshold, Accountable, and Private Signature -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Technical Overview -- 1.3 Related Works -- 2 Preliminaries -- 2.1 Notations -- 2.2 Cyclotomic Rings -- 2.3 Module-SIS and Module-LWE Problems -- 2.4 Rejection Sampling -- 2.5 Commitment Schemes -- 2.6 TAPS -- 3 Lattice-Based TAPS -- 3.1 Building Blocks -- 3.2 An Accountable Threshold Signature.
3.3 Our Lattice-Based TAPS Scheme -- 4 The Underlying Zero-Knowledge Argument -- 4.1 Basic Relation -- 4.2 Instantiating the Proofs -- 4.3 The Underlying t-out-of-N Proof in Our Construction -- 5 Parameters and Sizes -- 6 Conclusion and Future Work -- References -- Homomorphic Encryption -- TFHE Public-Key Encryption Revisited -- 1 Introduction -- 2 Smaller Public Keys, Less Noisy Ciphertexts -- 2.1 Description -- 2.2 Correctness -- 2.3 Security -- 2.4 Performance -- 3 Generalization -- 3.1 General Construction -- 3.2 Basic Scheme -- 3.3 Higher-Order Convolutions and More -- 3.4 Variants -- 4

Encrypting Multiple Plaintexts -- 5 Conclusion -- A Variance and Covariance -- References -- Differential Privacy for Free? Harnessing the Noise in Approximate Homomorphic Encryption -- 1 Introduction -- 1.1 Contributions -- 1.2 Related Work -- 1.3 Paper Outline -- 2 Background -- 2.1 Basic Notation -- 2.2 CKKS -- 2.3 Differential Privacy -- 2.4 Update Rules -- 2.5 Ridge Regression Case Study -- 2.6 Notation Key -- 3 Differential Privacy Analysis -- 4 Case Study -- 4.1 Sensitivity -- 4.2 Experiments -- 5 Relationship to IND-CPAD Security -- 6 Conclusion -- 7 Further Work -- References -- Identity-Based Encryption -- Identity-Based Encryption from LWE with More Compact Master Public Key -- 1 Introduction -- 1.1 Challenges and Our Contributions -- 1.2 Overview of Our Techniques -- 2 Preliminaries -- 2.1 Identity Based Encryption -- 2.2 Lattices, Gaussian and LWE -- 2.3 Lattice Trapdoors -- 2.4 Homomorphic Computations -- 3 Semi-homomorphic Equality Testing -- 3.1 The Construction -- 3.2 Homomorphic Equality Testing for Larger Ranges -- 4 Partition Function -- 4.1 Design of Partition Function -- 4.2 Homomorphic Evaluation of Partition Function -- 5 Our IBE Scheme -- 5.1 The Construction -- 5.2 Correctness and Security -- 6 Parameters. 6.1 Asymptotic Parameterization.