1. Record Nr. UNISA996466249803316

Titolo	Advances in Cryptology -- ASIACRYPT 2011 [[electronic resource]] : 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011, Proceedings / / edited by Dong Hoon Lee, Xiaoyun Wang
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2011
ISBN	3-642-25385-7
Edizione	[1st ed. 2011.]
Descrizione fisica	1 online resource (XIV, 760 p.)
Collana	Security and Cryptology ; ; 7073
Disciplina	005.8
Soggetti	Data encryption (Computer science) Algorithms Management information systems Computer science Computer science—Mathematics Computer security Applied mathematics Engineering mathematics Cryptology Algorithm Analysis and Problem Complexity Management of Computing and Information Systems Discrete Mathematics in Computer Science Systems and Data Security Applications of Mathematics
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Intro -- Title -- Preface -- Table of Contents -- Lattices and Quantum Cryptography -- BKZ 2.0: Better Lattice Security Estimates -- Introduction -- Preliminaries -- The Blockwise Korkine-Zolotarev (BKZ) Algorithm -- Description -- Enumeration Subroutine -- Analysis -- BKZ 2.0 -- Sound Pruning -- Preprocessing of Local Blocks -- Optimizing the Enumeration Radius -- New Lattice Records --

Darmstadt's Lattice Challenge -- SVP Challenges -- Predicting BKZ 2.0 by Simulation -- Description -- Consistency with Experiments -- Enumeration Subroutine -- Revising Security Estimates -- NTRU Lattices -- Gentry-Halevi's Fully-Homomorphic Encryption Challenges -- References -- Functional Encryption for Inner Product Predicates from Learning with Errors -- Introduction -- Overview of the Construction -- Predicate Encryption -- Security -- Lattice Preliminaries -- Lattices -- Sampling Algorithms -- The LWE Problem -- A Functional Encryption Scheme for Inner Product Predicates -- The Construction -- Correctness -- Security -- Parameter Selection -- Conclusion and Open Questions -- References -- Random Oracles in a Quantum World -- Introduction -- Our Contributions -- Preliminaries -- Quantum Computation -- Quantum-Accessible Random Oracles -- Hard Problems for Quantum Computers -- Cryptographic Primitives -- Separation Result -- Construction -- Signature Schemes in the Quantum-Accessible Random Oracle Model -- Secure Signatures from Preimage Sampleable Trapdoor Functions (PSF) -- Secure Signatures from Claw-Free Permutations -- Encryption Schemes in the Quantum-Accessible Random Oracle Model -- CPA Security of BR Encryption -- CCA Security of Hybrid Encryption -- Conclusion -- References -- Public Key Encryption I -- Lossy Encryption: Constructions from General Assumptions and Efficient Selective Opening Chosen Ciphertext Security -- Introduction -- Background.
Selective Opening Secure Encryption -- Lossy Encryption -- Constructing Lossy Encryption Schemes -- Re-Randomizable Encryption Implies Lossy Encryption -- Statistically-Hiding {Catalog} &lt -- &lt -- /PageLabels&lt -- &lt -- /Nums[0&lt -- &lt -- /S/D /St 70&gt -- &gt --]&gt -- &gt -- &gt -- &gt -- ()21-OT Implies Lossy Encryption -- Chosen-Ciphertext Security -- Chosen-Ciphertext Security: Indistinguishability -- Chameleon Hash Functions -- A Special Use of the Canetti-Halevi-Katz Paradigm -- Lossy and All-But-n Trapdoor Functions -- An IND-SO-stag-wCCA2 TBE Construction -- An All-But-n Function with Short Outputs -- References -- Structure Preserving CCA Secure Encryption and Applications -- Introduction -- Structure Preserving Encryption -- Basic Notation -- Construction -- Correctness and Security -- Secure Joint Ciphertext Computation -- Preliminaries -- Construction -- Oblivious Third Parties -- Conclusion -- References -- Decoding Random Linear Codes in (20.054n) -- Introduction -- Notation -- Information Set Decoding Algorithms -- Information Set Decoding -- Stern's Algorithm -- The Finiasz-Sendrier ISD Algorithm -- Ball-collision Decoding -- How to Solve the Submatrix Problem -- The ColumnMatch Algorithm -- Our New Decoding Algorithm -- Experiments -- References -- Lower and Upper Bounds for Deniable Public-Key Encryption -- Introduction -- Deniable Public-Key Encryption -- Security Notions -- Full Bi-deniablity Implies Full Sender/Receiver-Deniability -- Impossibility of Fully Receiver/Bi-deniable Encryption -- Security of Parallel Self-composition -- Lower Bound -- From Multi-distributional to Poly Deniability -- Poly-Sender-Deniability -- Poly-Receiver-Deniability -- Poly-Bi-Deniability -- References -- Public Key Encryption II -- Bridging Broadcast Encryption and Group Key Agreement -- Introduction -- Our Contributions.
Related Work -- Paper Organization -- Modeling Contributory Broadcast Encryption -- Syntax -- Security Definitions -- Remarks on Complexity Bounds of CBE and BE Schemes -- An Aggregatable BE Scheme -- Review of Aggregatable Signature-Based Broadcast -- An Aggregatable BE Scheme Based on ASBB -- Useful Properties -- Proposed CBE Scheme -- High-Level Description -- The Proposal -- Discussion -- Conclusions -- References -- On the Joint Security of

Encryption and Signature, Revisited -- Introduction -- Our Contribution -- Further Related Work -- Preliminaries -- Combined Signature and Encryption Schemes -- A Cartesian Product Construction -- An Insecure CSE Scheme whose Components are Secure -- A Generic Construction from IBE -- A More Efficient Construction -- Comparison of Schemes -- Conclusions and Future Research -- References -- Polly Cracker, Revisited -- Introduction -- Related Work -- Preliminaries -- Gr bner Basis and Ideal Membership Problems -- Symmetric Polly Cracker: Noise-Free Version -- Homomorphic Symmetric Encryption -- The Scheme -- Security -- Symmetric-to-Asymmetric Conversion -- Gr\"{o} bner Bases with Noise -- Hardness Assumptions and Justifications -- Polly Cracker with Noise -- References -- Database Privacy -- Oblivious RAM with O((logN)3)Worst-Case Cost -- Introduction -- Our Contributions -- Related Work -- Preliminaries -- Defining O-RAM with Enriched Operations -- Relationship with the Standard O-RAM Definition -- Implementing Enriched Semantics -- Encryption and Authentication -- Two Simple O-RAM Constructions with Deterministic Guarantees -- Basic Construction -- Overview of the Binary Tree Construction -- Detailed Construction -- Security Analysis -- Asymptotic Performance of the Basic Construction -- Recursive Construction and How to Achieve the Desired Asymptotics. Recursive O-RAM Construction: O(1) Client-Side Storage -- References -- Noiseless Database Privacy -- Introduction -- Our Privacy Notion -- Boolean Queries -- The No Auxiliary Information Setting -- Handling Auxiliary Information -- Handling Multiple Queries in Adversarial Refreshment Model -- Real Queries -- Sums of Functions of Database Rows -- Privacy Analysis of fin(T)=j[n]aij tj -- Privacy under Multiple Queries on Changing Databases -- References -- Hash Function -- The Preimage Security of Double-Block-Length Compression Functions -- Introduction -- The Model -- An Example Case -- Preimage Security Results for Hirose's Scheme -- Preimage Security Results for Abreast-DM -- Preimage Security Results for Tandem-DM -- Conclusion -- References -- Rebound Attack on JH42 -- Introduction -- Preliminaries -- The JH42 Hash Function -- Properties of the Linear Transformation L -- Observations on the Compression Function -- The Rebound Attack -- Semi-free-start Internal Near-Collisions -- Matching the Active Bytes -- Matching the Passive Bytes -- Outbound Phase -- Distinguishers on JH -- Distinguishers on the Reduced Round Internal Permutation -- Distinguishers on the Full Internal Permutation -- Distinguishers on the Full Compression Function -- Conclusion -- References -- Second-Order Differential Collisions for Reduced SHA-256 -- Introduction -- Higher-Order Differential Collisions for Compression Functions -- Second-Order Differential Collision for Block-Cipher-Based Compression Functions -- Related Work -- Application to SHA-256 -- Description of SHA-256 -- Differential Characteristics -- Complexity of the Attack -- Applications to Related Primitives -- Application to SHA-512 -- Application to SHACAL-2 -- Conclusions -- References -- Finding SHA-2 Characteristics: Searching through a Minefield of Contradictions -- Introduction. Description of SHA-256 -- Basic Attack Strategy -- Determining a Starting Point -- Searching for Valid Differential Characteristics and Conforming Message Pairs in SHA-2 -- Difference and Condition Propagation in SHA-2 -- Alternative Description of SHA-2 -- Generalized Conditions -- Efficiently Implementing the Propagation of Generalized Conditions -- Two-Bit Conditions -- Inconsistency Checks -- Searching for Differential Characteristics -- Search Strategy -- Results -- Conclusions and Future Work -- References -- Symmetric Key Encryption -- Cryptanalysis of ARMADILLO2 -- Introduction --

Description of ARMADILLO2 -- Description -- A Multi-purpose Cryptographic Primitive -- Inverting the ARMADILLO2 Function -- The Meet-in-the-Middle Technique -- ARMADILLO2 Matching Problem: Matching Non-random Elements -- Applying the Parallel Matching Algorithm to ARMADILLO2 -- Meet in the Middle Key Recovery Attacks -- Key Recovery Attack in the FIL-MAC Setting -- Key Recovery Attack in the Stream Cipher Setting -- (Second) Preimage Attack on the Hashing Applications -- Meet-in-the-Middle (Second) Preimage Attack -- Inverting the Compression Function -- Experimental Verifications -- Generalization of the Parallel Matching Algorithm -- The Generalized Problem 1 -- Generalized Parallel Matching Algorithm -- Link with Formulas in the Case of ARMADILLO -- Conclusion -- References -- An Experimentally Verified Attack on Full Grain-128 Using Dedicated Reconfigurable Hardware -- Introduction -- Preliminaries -- Description on Grain-128 -- Previous Results on Grain-128 -- Cube Testers -- Dynamic Cube Attacks -- A Partial Simulation Phase -- A New Approach for Attacking Grain-128 -- Description of the Dedicated Hardware Used to Attack Grain-128 -- Architectural Considerations -- Hardware Implementation Results -- Conclusions -- References. Biclique Cryptanalysis of the Full AES.

Sommario/riassunto

This book constitutes the proceedings of the 17th International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2011, held in Seoul, Korea, in December 2011. The 40 revised papers included in this volume were carefully reviewed and selected from 266 submissions. The contributions are organized in topical sections on lattices and quantum cryptography; public key encryption; database privacy; hash function; symmetric key encryption; zero knowledge proof; universal composability; foundation; secure computation and secret sharing; public key signature; and leakage resilient cryptography.