1. Record Nr. UNISA996466253903316

Titolo	Cryptology and Network Security [[electronic resource]] : 10th International Conference, CANS 2011, Sanya, China, December 10-12, 2011, Proceedings / / edited by Dongdai Lin, Gene Tsudik, Xiaoyun Wang
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2011
ISBN	3-642-25513-2
Edizione	[1st ed. 2011.]
Descrizione fisica	1 online resource (XII, 313 p.)
Collana	Security and Cryptology ; ; 7092
Disciplina	003.54
Soggetti	Data encryption (Computer science) Computer communication systems Computer science—Mathematics Coding theory Information theory Data structures (Computer science) Computer security Cryptology Computer Communication Networks Discrete Mathematics in Computer Science Coding and Information Theory Data Structures and Information Theory Systems and Data Security
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 -- Invited Talks -- Expressive Encryption Systems from Lattices -- Introduction -- Background -- Lattice Notions -- Discrete Gaussians -- Sampling and Preimage Sampling -- Hardness Assumption -- Classic Constructions -- Regev Public-Key Encryption -- GPV Identity-Based Encryption -- Techniques and Refinements -- Bit-by-Bit Standard-Model IBE -- All-at-Once Standard-Model IBE -- Adaptive or ``Full'' Security --

Delegation and Hierarchies -- Concatenation-Based Delegation -- Multiplicative In-Place Delegation -- Attributes and Predicates -- Conclusion -- References -- Breaking Fully-Homomorphic-Encryption Challenges -- References -- Symmetric Cryptanalysis -- Cube Cryptanalysis of Hitag2 Stream Cipher -- Introduction -- Hitag2 Stream Cipher -- Cube Attack -- Cube Attack on Hitag2 -- First Phase: Black-Box Attack -- Second Phase: White-Box Attack -- Third Phase: Exhaustive Search Attack -- Experimental Results -- Conclusion -- References -- New Impossible Differential Cryptanalysis of Reduced-Round Camellia -- Introduction -- Preliminaries -- Notations -- A Brief Description of Camellia -- 7-Round Impossible Differential of Camellia -- Impossible Differential Attack on 10-Round Camellia-128 -- Attack on 10-Round Camellia-192 and 11-Round Camellia-256 -- Attack on 10-Round Camellia-192 -- Attack on 11-Round Camellia-256 -- Conclusion -- References -- The Initialization Stage Analysis of ZUC v1.5 -- Introduction -- Preliminaries -- ZUC v1.5 -- S-Functions -- The Chosen-IV Attack of ZUC v1.5 -- The Definition of Differences -- An Chosen-IV Differential Path of ZUC v1.5 -- The Differential Properties of Operations in ZUC v1.5 -- The Probability of the Differential -- Conclusion -- References -- Algebraic Cryptanalysis of the Round-Reduced and Side Channel Analysis of the Full PRINTCipher-48 -- Introduction.
PRINTCipher -- Algebraic Description -- SAT Techniques for Algebraic System Solving -- Conversion Techniques -- Optimal Tools and Strategies for the Attacks -- Algebraic Analysis of PRINTCipher-48 -- Attack on Round-Reduced PRINTCipher-48 -- Additional Bits at Round Four -- Side Channel Analysis of the Full PRINTCipher-48 -- Conclusion and Future Work -- References -- Symmetric Ciphers -- EPCBC - A Block Cipher Suitable for Electronic Product Code Encryption -- Introduction -- The Electronic Product Code - EPC -- A New Block Cipher Suitable for EPC Encryption: EPCBC -- EPCBC(48,96) - EPCBC with 48-Bit Block Size and 96-Bit Key Size -- EPCBC(96,96) - EPCBC with 96-Bit Block Size and 96-Bit Key Size -- Improved Differential and Linear Cryptanalyis of PR-n -- Brief Description of PR-n -- Improved Differential and Linear Cryptanalysis -- Security Analysis of EPCBC -- Differential, Linear and Related-Key Differential Cryptanalysis -- Other Attacks on EPCBC -- Implementation of EPCBC -- Conclusion -- References -- On Permutation Layer of Type 1, Source-Heavy, and Target-Heavy Generalized Feistel Structures -- Introduction -- Preliminaries -- Generalized Feistel Structure (GFS) -- Diffusion of GFS -- Equivalence of GFSs -- Analysis on DRmax() -- Type 1 GFS -- Source-Heavy GFS -- Target-Heavy GFS -- Experimental Results -- Conclusions -- References -- Public Key Cryptography -- Security Analysis of an Improved MFE Public Key Cryptosystem -- Introduction -- MFE and Its Improvement -- MFE Cryptosystem -- Improvement of MFE -- Linearization Equation Attack -- First Order Linearnation Equation -- Second Order Linearization Equation -- Conclusion -- References -- A New Lattice-Based Public-Key Cryptosystem Mixed with a Knapsack -- Introduction -- Preliminaries -- Knapsack Problem -- Lattice -- Description of Our Cryptosystem -- The Basic Cryptosystem.
Implementations of Our Cryptosystem -- Choosing the Superincreasing Sequence and -- Finding Integer Linear Combination with Small Coefficients -- Some Experimental Results -- Security Analysis -- Knapsack Structure -- Message Security -- Key Security -- Remarks -- Conclusion -- References -- Achieving Short Ciphertexts or Short Secret-Keys for Adaptively Secure General Inner-Product Encryption -- Introduction -- Background -- Our Results -- Related Works -- Key

Techniques -- Notations -- Dual Pairing Vector Spaces by Direct Product of Symmetric Pairing Groups -- Definitions of Zero and Non-zero Inner-Product Encryption (ZIPE / NIPE) -- Decisional Linear (DLIN) Assumption -- Proposed NIPE Scheme with Constant-SizeCiphertexts -- Key Ideas in Constructing the Proposed NIPE Scheme -- Dual Orthonormal Basis Generator -- Construction -- Security -- Proposed NIPE Scheme withConstant-SizeSecret-Keys -- Dual Orthonormal Basis Generator -- Construction and Security -- Proposed ZIPE Scheme with Constant-Size Ciphertexts -- Dual Orthonormal Basis Generator -- Construction and Security -- Performance -- Concluding Remarks -- References -- Protocol Attacks -- Comments on the SM2 Key Exchange Protocol -- Introduction -- Security Attributes -- Related Works and Our Contribution -- Organization -- Review of SM2 Key Exchange Protocol -- Formal Model for Key Exchange Protocols -- Weaknesses of SM2 Key Exchange Protocol -- UKS Attack I -- UKS Attack II -- Formal Attack Description -- Countermeasure -- Conclusion -- References -- Cryptanalysis of a Provably Secure Cross-Realm Client-to-Client Password-Authenticated Key Agreement Protocol of CANS '09 -- Introduction -- Related Work and Motivation -- The C2C-PAKA-SC Protocol -- Adversarial Capability in the C2C-PAKA-SC Security Model -- Cryptanalysis of the C2C-PAKA-SC -- By any Outsider C Impersonating A to B.
By Any Outsider C Impersonating B to A -- By Any Insider Client B=A Impersonating A to KDCA -- Concluding Remarks -- References -- Passive Attack on RFID LMAP++ Authentication Protocol -- Introduction -- LMAP++ Authentication Protocol -- Passive Attack on LMAP++ -- The Least Significant Bit of Identifier 0 [ID] -- The Least Significant Bit of Random Number [r]0 -- Algorithm to Obtain the Identifier and Secrets -- Conclusions -- References -- Privacy Techniques -- Multi-show Anonymous Credentials with Encrypted Attributes in the Standard Model -- Introduction -- A Model for Anonymous Credential Systems with Encrypted Attributes -- Protocols -- Security Properties -- Cryptographic Tools -- Randomizable and Extractable Commitment Schemes -- (SXDH) Groth-Sahai Proofs -- GS Proof of Equality under Different Commitment Keys -- Automorphic Signatures -- Commuting Signatures and Some New Extensions -- Additional Commitments -- Simple Commuting Signature: One Committed Message and One Commitment Key -- Vector of Committed Messages and One Commitment Key -- Vector of Committed Messages and Several Commitment Keys -- Commuting Signatures in Privacy Enhancing Cryptography -- A Multi-show Anonymous Credential Scheme with Encrypted Attributes -- Overview of Our Solution -- Algorithms and Protocols -- References -- Group Signature with Constant Revocation Costs for Signers and Verifiers -- Introduction -- PriorWork on Revocable Group Signatures -- Our Results and Organization -- Preliminaries -- Bilinear Groups -- Hardness Assumptions -- Security Model and Definitions for Revocable Group Signatures -- Our RGS Scheme with Constant Costs for Signers and Verifiers -- High-Level Intuition -- Specification of RGS Algorithms -- Security Analysis -- Conclusion -- References -- Fast Computation on Encrypted Polynomials and Applications -- Introduction -- Our Contribution. Homomorphic Encryption and Hardness Assumptions -- Additive Variant of El Gamal -- Paillier's Encryption Scheme -- Non-interactive Computation on Encrypted Polynomials -- Applications -- Batch Oblivious Polynomial Evaluation -- Private Set Intersection via OPE -- Private Set Intersection via Polynomial Multiplication -- References -- Varia -- AniCAP: An Animated 3D CAPTCHA Scheme Based on Motion Parallax -- Introduction -- Background -- Security and Usability --

Animated CAPTCHAs -- CAPTCHA: Formal Definition and Notation -- AniCAP -- Design and Implementation -- New AI Problem Family -- Security Considerations for AniCAP -- Image Processing and Computer Vision Attacks -- Brute Force Attacks -- Machine Learning Attacks -- Conclusion -- References -- Towards Attribute Revocation in Key-Policy Attribute Based Encryption -- Introduction -- Background -- Bilinear Groups -- Access Structure and Access Tree -- Lagrange Coefficient -- Decision q-BDHE Assumption -- Definition -- Construction -- Small Universe Construction -- Large Universe Construction -- Efficiency -- Security -- Discussion -- Conclusion and Future Work -- References -- A Note on (Im)Possibilities of Obfuscating Programs of Zero-Knowledge Proofs of Knowledge -- Introduction -- Our Results -- Organizations -- Preliminaries -- Point Functions and Their Obfuscation -- Zero-Knowledge -- Witness Indistinguishability -- Proofs of Knowledge -- Definitions of Obfuscation for Interactive Probabilistic Programs -- Considerations -- Definitions -- Impossibilities of Obfuscating Provers -- Impossibilities for Zero Knowledge and Witness Indistinguishability -- Extending the Impossibilities to t-Composition Setting -- Possibilities of Obfuscating Verifiers -- Motivation for Obfuscating Verifiers -- Obfuscation for Verifiers -- Conclusions -- References -- Author Index.

Sommario/riassunto

This book constitutes the refereed proceedings of the 10th International Conference on Cryptology and Network Security, CANS 2011, held in Sanya, China, in December 2011. The 18 revised full papers, presented were carefully reviewed and selected from 65 submissions. The book also includes two invited talks. The papers are organized in topical sections on symmetric cryptanalysis, symmetric ciphers, public key cryptography, protocol attacks, and privacy techniques.