1. Record Nr. UNISA996466365603316

Titolo	Cryptology and Network Security [[electronic resource]] : 8th International Conference, CANS 2009, Kanazawa, Japan, December 12-14, 2009, Proceedings / / edited by Juan A. Garay, Akira Otsuka
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2009
ISBN	3-642-10433-9
Edizione	[1st ed. 2009.]
Descrizione fisica	1 online resource (XIV, 538 p.)
Collana	Security and Cryptology ; ; 5888
Classificazione	DAT 461f DAT 465f SS 4800
Disciplina	004n/a
Soggetti	Data encryption (Computer science) Computer communication systems Number theory Coding theory Information theory Mathematical logic Computer science—Mathematics Cryptology Computer Communication Networks Number Theory Coding and Information Theory Mathematical Logic and Formal Languages Mathematics of Computing Kanazawa (2009) Kongress.
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Cryptographic Protocol and Schemes I -- Improved Garbled Circuit Building Blocks and Applications to Auctions and Computing Minima -- Multi Party Distributed Private Matching, Set Disjointness and

Cardinality of Set Intersection with Information Theoretic Security -- On Cryptographic Schemes Based on Discrete Logarithms and Factoring -- Invited Talk 1 -- Asymptotically Optimal and Private Statistical Estimation -- Cryptanalysis I -- Linear (Hull) and Algebraic Cryptanalysis of the Block Cipher PRESENT -- Saturation Attack on the Block Cipher HIGHT -- Extensions of the Cube Attack Based on Low Degree Annihilators -- An Analysis of the Compact XSL Attack on BES and Embedded SMS4 -- Wireless and Sensor Network Security I -- RFID Distance Bounding Protocol with Mixed Challenges to Prevent Relay Attacks -- Anonymizer-Enabled Security and Privacy for RFID -- Blink ' Em All: Scalable, User-Friendly and Secure Initialization of Wireless Sensor Nodes -- Network Security -- DepenDNS: Dependable Mechanism against DNS Cache Poisoning -- Privacy and Anonymity -- Privacy-Preserving Relationship Path Discovery in Social Networks -- Verifying Anonymous Credential Systems in Applied Pi Calculus -- Transferable Constant-Size Fair E-Cash -- Functional and Searchable Encryption -- A Secure Channel Free Public Key Encryption with Keyword Search Scheme without Random Oracle -- Private-Key Hidden Vector Encryption with Key Confidentiality -- Invited Talk 2 -- Building Secure Networked Systems with Code Attestation -- Authentication -- HPAKE : Password Authentication Secure against Cross-Site User Impersonation -- An Efficient and Provably Secure Cross-Realm Client-to-Client Password-Authenticated Key Agreement Protocol with Smart Cards -- Ensuring Authentication of Digital Information Using Cryptographic Accumulators -- Block Cipher Design -- MIBS: A New Lightweight Block Cipher -- Cryptanalysis II -- Distinguishing and Second-Preimage Attacks on CBC-Like MACs -- Improving the Rainbow Attack by Reusing Colours -- Side Channel Cube Attack on PRESENT -- Algebraic Attack on the MQQ Public Key Cryptosystem -- Algebraic and Number-Theoretic Schemes -- Construction of Rotation Symmetric Boolean Functions with Maximum Algebraic Immunity -- Multi-core Implementation of the Tate Pairing over Supersingular Elliptic Curves -- On the Complexity of Computing Discrete Logarithms over Algebraic Tori -- Wireless and Sensor Network Security II -- On the Usability of Secure Association of Wireless Devices Based on Distance Bounding -- Short Hash-Based Signatures for Wireless Sensor Networks -- Invited Talk 3 -- Computing on Encrypted Data -- Cryptographic Protocol and Schemes II -- Fully Robust Tree-Diffie-Hellman Group Key Exchange -- Group Signatures with Verifier-Local Revocation and Backward Unlinkability in the Standard Model -- Relinkable Ring Signature.

Sommario/riassunto

This book constitutes the refereed proceedings of the 8th International Conference on Cryptology and Network Security, CANS 2009, held in Kanazawa, Japan, in December 2009. The 32 revised full papers presented together with 3 invited talks were carefully reviewed and selected from 109 submissions. The papers are organized in topical sections on cryptographic protocols and schemes; cryptanalysis; wireless and sensor security; network security; privacy and anonymity; functional and searchable encryption; authentication; block cipher design; and algebraic and number-theoretic schemes.