1. Record Nr. UNINA9910143897103321

Titolo	Advances in Cryptology - ASIACRYPT 2002 : 8th International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, December 1-5, 2002, Proceedings / / edited by Yuliang Zheng
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2002
ISBN	3-540-36178-2
Edizione	[1st ed. 2002.]
Descrizione fisica	1 online resource (XIV, 582 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 2501
Disciplina	005.8
Soggetti	Coding theory Information theory Data encryption (Computer science) Computer networks Operating systems (Computers) Algorithms Computer science—Mathematics Coding and Information Theory Cryptology Computer Communication Networks Operating Systems Algorithm Analysis and Problem Complexity Discrete Mathematics in Computer Science
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Analysis of Bernstein’s Factorization Circuit -- A Variant of the Cramer-Shoup Cryptosystem for Groups of Unknown Order -- Looking beyond XTR -- Bounds for Robust Metering Schemes and Their Relationship with A2-code -- Unconditionally Secure Anonymous Encryption and Group Authentication -- Adapting the Weaknesses of the Random Oracle Model to the Generic Group Model -- On the Impossibilities of Basing One-Way Permutations on Central Cryptographic Primitives -- A

Statistically-Hiding Integer Commitment Scheme Based on Groups with Hidden Order -- Efficient Oblivious Transfer in the Bounded-Storage Model -- In How Many Ways Can You Write Rijndael? -- On the Security of Rijndael-Like Structures against Differential and Linear Cryptanalysis -- Threshold Cryptosystems Based on Factoring -- Non-interactive Distributed-Verifier Proofs and Proving Relations among Commitments -- Asynchronous Secure Communication Tolerating Mixed Adversaries -- Amplified Boomerang Attack against Reduced-Round SHACAL -- Enhancing Differential-Linear Cryptanalysis -- Cryptanalysis of Block Ciphers with Overdefined Systems of Equations -- Analysis of Neural Cryptography -- The Hardness of Hensel Lifting: The Case of RSA and Discrete Logarithm -- A Comparison and a Combination of SST and AGM Algorithms for Counting Points of Elliptic Curves in Characteristic 2 -- A General Formula of the (t, n)-Threshold Visual Secret Sharing Scheme -- On Unconditionally Secure Robust Distributed Key Distribution Centers -- Short Signatures in the Random Oracle Model -- The Provable Security of Graph-Based One-Time Signatures and Extensions to Algebraic Signature Schemes -- Transitive Signatures Based on Factoring and RSA -- 1-out-of-n Signatures from a Variety of Keys -- A Revocation Scheme with Minimal Storage at Receivers -- Optimistic Mixing for Exit-Polls -- Improved Construction of Nonlinear Resilient S-Boxes -- An Upper Bound on the Number of m-Resilient Boolean Functions -- Group Diffie-Hellman Key Exchange Secure against Dictionary Attacks -- Secure Channels Based on Authenticated Encryption Schemes: A Simple Characterization -- ID-Based Blind Signature and Ring Signature from Pairings -- Hierarchical ID-Based Cryptography -- Crypto-integrity -- Gummy and Conductive Silicone Rubber Fingers Importance of Vulnerability Analysis.

Sommario/riassunto

This book constitutes the refereed proceedings of the 8th International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2002, held in Singapore, in December 2002. The 34 revised full papers presented together with two invited contributions were carefully reviewed and selected from 173 submissions on the basis of 875 review reports. The papers are organized in topical sections on public key cryptography, authentication, theory, block ciphers, distributed cryptography, cryptanalysis, public key cryptanalysis, secret sharing, digital signatures, applications, Boolean functions, key management, and ID-based cryptography.