1. Record Nr. UNINA9910146617503321

Titolo	Advances in Cryptology -- ASIACRYPT 2006 : 12th International Conference on the Theory and Application of Cryptology and Information Security, Shanghai, China, December 3-7, 2006, Proceedings / / edited by Xuejia Lai, Kefei Chen
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2006
ISBN	3-540-49476-6
Edizione	[1st ed. 2006.]
Descrizione fisica	1 online resource (XIV, 470 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 4284
Altri autori (Persone)	LaiXuejia ChenKefei <1959->
Disciplina	005.8
Soggetti	Cryptography Data encryption (Computer science) Data protection Algorithms Electronic data processing - Management Computer networks Computer science - Mathematics Discrete mathematics Cryptology Data and Information Security IT Operations Computer Communication Networks 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	Attacks on Hash Functions -- Finding SHA-1 Characteristics: General Results and Applications -- Improved Collision Search for SHA-0 -- Forgery and Partial Key-Recovery Attacks on HMAC and NMAC Using Hash Collisions -- Stream Ciphers and Boolean Functions -- New Guess-and-Determine Attack on the Self-Shrinking Generator -- On the (In)security of Stream Ciphers Based on Arrays and Modular

Addition -- Construction and Analysis of Boolean Functions of 2t+1 Variables with Maximum Algebraic Immunity -- Biometrics and ECC Computation -- Secure Sketch for Biometric Templates -- The 2-Adic CM Method for Genus 2 Curves with Application to Cryptography -- Extending Scalar Multiplication Using Double Bases -- ID-Based Schemes -- HIBE With Short Public Parameters Without Random Oracle -- Forward-Secure and Searchable Broadcast Encryption with Short Ciphertexts and Private Keys -- On the Generic Construction of Identity-Based Signatures with Additional Properties -- Public-Key Schemes -- On the Provable Security of an Efficient RSA-Based Pseudorandom Generator -- On the Security of OAEP -- Relationship Between Standard Model Plaintext Awareness and Message Hiding -- RSA and Factorization -- On the Equivalence of RSA and Factoring Regarding Generic Ring Algorithms -- Trading One-Wayness Against Chosen-Ciphertext Security in Factoring-Based Encryption -- A Strategy for Finding Roots of Multivariate Polynomials with New Applications in Attacking RSA Variants -- Construction of Hash Function -- Indifferentiable Security Analysis of Popular Hash Functions with Prefix-Free Padding -- Multi-Property-Preserving Hash Domain Extension and the EMD Transform -- Combining Compression Functions and Block Cipher-Based Hash Functions -- Protocols -- A Scalable Password-Based Group Key Exchange Protocol in the Standard Model -- AWeakness in Some Oblivious Transfer and Zero-Knowledge Protocols -- Almost Optimum Secret Sharing Schemes Secure Against Cheating for Arbitrary Secret Distribution -- Block Ciphers -- KFC – The Krazy Feistel Cipher -- Generic Attacks on Unbalanced Feistel Schemes with Contracting Functions -- New Cryptanalytic Results on IDEA -- Signatures -- New Approach for Selectively Convertible Undeniable Signature Schemes -- Simulation-Sound NIZK Proofs for a Practical Language and Constant Size Group Signatures -- Analysis of One Popular Group Signature Scheme.

Sommario/riassunto

This book constitutes the refereed proceedings of the 12th International Conference on the Theory and Application of Cryptology and Information Security, held in Shanghai, China, December 2006. The 30 revised full papers cover attacks on hash functions, stream ciphers, biometrics and ECC computation, id-based schemes, public-key schemes, RSA and factorization, construction of hash function, protocols, block ciphers, and signatures.