1.

Record Nr.	UNINA9910767583803321
Titolo	Advances in Cryptology - CRYPTO '98 [[electronic resource]] : 18th Annual International Cryptology Conference, Santa Barbara, California, USA, August 23-27, 1998, Proceedings / / edited by Hugo Krawczyk
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 1998
ISBN	3-540-68462-X
Edizione	[1st ed. 1998.]
Descrizione fisica	1 online resource (XII, 524 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 1462
Disciplina	005.82
Soggetti	Data encryption (Computer science) Computer security Computers Computer science—Mathematics Computer communication systems Management information systems Computer science Cryptology Systems and Data Security Theory of Computation Discrete Mathematics in Computer Science Computer Communication Networks Management of Computing and Information Systems
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS #1 -- A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack -- Relations among notions of security for public-key encryption schemes -- Cryptography and the internet -- Differential collisions in SHA-0 -- From differential cryptanalysis to ciphertext-only attacks -- A simplified approach to threshold and proactive RSA -- New efficient and secure protocols for verifiable signature sharing and other

applications -- Trading correctness for privacy in unconditional multi-party computation -- Fast digital identity revocation -- Self-delegation with controlled propagation — or — What if you lose your laptop -- Identity escrow -- Generalized birthday attacks on unbalanced Feistel networks -- Quadratic relation of S-box and its application to the linear attack of full round DES -- Cryptanalysis of block ciphers with probabilistic non-linear relations of low degree -- Cryptanalysis of the Ajtai-Dwork cryptosystem -- Cryptanalysis of the Chor-Rivest cryptosystem -- Cryptanalysis of the oil and vinegar signature scheme -- From unpredictability to indistinguishability: A simple construction of pseudo-random functions from MACs -- Many-to-one trapdoor functions and their relation to public-key cryptosystems -- Authentication, enhanced security and error correcting codes -- An efficient discrete log pseudo random generator -- Fast RSA-type cryptosystem modulo p k q -- An elliptic curve implementation of the finite field digital signature algorithm -- Quantum bit commitment from a physical assumption -- On concrete security treatment of signatures derived from identification -- Building PRFs from PRPs -- Security amplification by composition: The case of doubly-iterated, ideal ciphers -- On the existence of 3-round zero-knowledge protocols -- Zero-knowledge proofs for finite field arithmetic, or: Can zero-knowledge be for free? -- Concurrent zero-knowledge: Reducing the need for timing constraints -- The solution of McCurley's discrete log challenge -- Optimal extension fields for fast arithmetic in public-key algorithms -- Time-stamping with binary linking schemes -- Threshold traitor tracing.

Sommario/riassunto

This book constitutes the refereed proceedings of the 18th Annual International Cryptology Conference, CRYPTO'98, held in Santa Barbara, California, USA, in August 1998. The book presents 33 revised full papers selected from a total of 144 submissions received. Also included are two invited presentations. The papers are organized in topical sections on chosen ciphertext security, cryptanalysis of hash functions and block ciphers, distributed cryptography, zero knowledge, and implementation.