1.	Record Nr.	UNISA996466112803316
	Titolo	Public Key Cryptography [[electronic resource]] : First International Workshop on Practice and Theory in Public Key Cryptography, PKC'98, Pacifico Yokohama, Japan, February 5-6, 1998, Proceedings / / edited by Hideki Imai, Yuliang Zheng
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 1998
	ISBN	3-540-69105-7
	Edizione	[1st ed. 1998.]
	Descrizione fisica	1 online resource (XIII, 271 p.)
	Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 1431
	Disciplina	005.8/2
	Soggetti	Data encryption (Computer science) Computers Algorithms Computer communication systems Cryptology Theory of Computation Algorithm Analysis and Problem Complexity Computer Communication Networks
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Bibliographic Level Mode of Issuance: Monograph
	Nota di contenuto	Distributed public key cryptosystems -- How (not) to design RSA signature schemes -- Overview of elliptic curve cryptography -- Lattices and cryptography: An overview -- A signcryption scheme with signature directly verifiable by public key -- Guaranteed correct sharing of integer factorization with off-line shareholders -- Lower bounds on term-based divisible cash systems -- Certifying trust -- On the security of server-aided RSA protocols -- On the security of ElGamal based encryption -- An authenticated Diffie-Hellman key agreement protocol secure against active attacks -- On the security of Girault's identification scheme -- A scheme for obtaining a message from the digital multisignature -- Secure hyperelliptic cryptosystems and their performance -- A practical implementation of elliptic curve cryptosystems over GF(p) on a 16-bit microcomputer -- Two efficient

algorithms for arithmetic of elliptic curves using Frobenius map -- Public-key cryptosystems using the modular group -- A cellular automaton based fast one-way hash function suitable for hardware implementation -- A new hash function based on MDx-family and its application to MAC -- Security issues for contactless smart cards -- Parameters for secure elliptic curve cryptosystem -improvements on Schoof s algorithm -- A note on the complexity of breaking Okamoto-Tanaka ID-based key exchange scheme.

Sommario/riassunto

This book constitutes the refereed proceedings of the First International Workshop on Practice and Theory in Public Key Cryptography, PKC'98, held in Pacifico Yokohama, Japan, in February 1998. The volume presents four invited contributions together with 18 revised full papers selected from 30 submissions. The papers address all current issues in research and design in the area including digital signature schemes, digital payment systems, electronic commerce, cryptographic protocols, as well as foundational issues like integer factorization, elliptic curve aspects, hash functions, finite fields, etc.