1. Record Nr. UNISA996465295103316

Autore	Pfitzmann Birgit
Titolo	Digital Signature Schemes [[electronic resource]] : General Framework and Fail-Stop Signatures / / by Birgit Pfitzmann
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 1996
ISBN	3-540-68712-2
Edizione	[1st ed. 1996.]
Descrizione fisica	1 online resource (XVI, 404 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 1100
Disciplina	005.8
Soggetti	Data structures (Computer science) Data encryption (Computer science) Algorithms Computer communication systems Data Storage Representation Cryptology 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	Requirements on digital signature schemes -- History of digital signature schemes -- Information-theoretic security for signers: Introduction -- Terminology -- Properties of digital signature schemes -- Overview of existing schemes with other than ordinary security -- Conventional definitions of fail-stop signature schemes and general reductions -- Building blocks -- Constructions for one message block -- Signing many long messages -- Lower bounds.
Sommario/riassunto	This book, based on the author's Ph.D. thesis, was selected during the 1995 GI Doctoral Dissertation Competition as the winning thesis in the foundations-of-informatics track. Securing integrity for digital communications in the age of global electronic information exchange and electronic commerce is vital to democratic societies and a central technical challenge for cryptologists. As core contribution to advancing the state of the art, the author develops the new class of digital fail-stop signatures. This monograph is self-contained regarding the

historical background and cryptographic primitives used. For the first time, a general and sophisticated framework is introduced in which innovative fail-stop signatures are systematically presented and evaluated, from theoretical foundations to engineering aspects.