1. Record Nr. UNINA9910144928103321

Titolo	Security Protocols [[electronic resource]] : International Workshop Cambridge, United Kingdom April 10-12, 1996 Proceedings / / edited by Mark Lomas
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 1997
ISBN	3-540-68047-0
Edizione	[1st ed. 1997.]
Descrizione fisica	1 online resource (VIII, 203 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 1189
Disciplina	005.8/2
Soggetti	Coding theory Information theory Data encryption (Computer science) Algorithms Computer communication systems Computer mathematics Electrical engineering Coding and Information Theory Cryptology Algorithm Analysis and Problem Complexity Computer Communication Networks Computational Mathematics and Numerical Analysis Communications Engineering, Networks
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	On cryptographic techniques for on-line bankcard payment transactions using open networks -- A certification scheme for electronic commerce -- Practical escrow cash systems -- NetCard — A practical electronic-cash system -- Electronic payments of small amounts -- PayWord and MicroMint: Two simple micropayment schemes -- Transactions using bets -- Protocol failures for RSA-like functions using Lucas sequences and elliptic curves -- Efficient and provable security amplifications -- A comparison of RSA and the

	Naccache-Stern public-key cryptosystem -- IEEE P1363: A standard for RSA, Diffie-Hellman, and Elliptic-Curve cryptography (abstract) -- Efficient and secure conference-key distribution -- Directed signatures and application to threshold cryptosystems -- Key escrow in mutually mistrusting domains -- Automatic event-stream notarization using digital signatures -- Why isn't trust transitive? -- Securing the residential asynchronous transfer mode networks -- Visual cryptography II: Improving the contrast via the cover base.
Sommario/riassunto	This book constitutes the refereed proceedings of the International Workshop on Security Protocols held in Cambridge, UK, in April 1996, in the context of the special program on computer security, cryptology, and coding theory at the Isaac Newton Institute. The 17 revised full papers and one abstract included in the book were carefully selected. Among the topics addressed are several types of public key cryptosystems, digital cash, electronic commerce, digital signatures, and visual cryptography. Besides original theoretical results, the collection of papers show a strong applications-oriented component.