1. Record Nr. UNISA996465963103316

Autore	Lindell Yehuda
Titolo	Composition of Secure Multi-Party Protocols [[electronic resource]] : A Comprehensive Study / / by Yehuda Lindell
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2003
ISBN	3-540-39819-8
Edizione	[1st ed. 2003.]
Descrizione fisica	1 online resource (XVI, 200 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 2815
Disciplina	005.8
Soggetti	Data encryption (Computer science) Computer communication systems Operating systems (Computers) Computers and civilization Management information systems Computer science Cryptology Computer Communication Networks Operating Systems Computers and Society 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 bibliografia	Includes bibliographical references and index.
Nota di contenuto	1. Introduction -- 2. The Composition of Authenticated Byzantine Agreement -- 3. Secure Computation without Agreement -- 4. Universally Composable Multi-party Computation.
Sommario/riassunto	In the setting of multi-party computation, sets of two or more parties with private inputs wish to jointly compute some (predetermined) function of their inputs. General results concerning secure two-party or multi-party computation were first announced in the 1980s. Put briefly, these results assert that under certain assumptions one can construct protocols for securely computing any desired multi-party functionality. However, this research relates only to a setting where a single protocol execution is carried out. In contrast, in modern networks, many

different protocol executions are run at the same time. This book is devoted to the general and systematic study of secure multi-party computation under composition. Despite its emphasis on a theoretically well-founded treatment of the subject, general techniques for designing secure protocols are developed that may even result in schemes or modules to be incorporated in practical systems. The book clarifies fundamental issues regarding security in a multi-execution environment and gives a comprehensive and unique treatment of the composition of secure multi-party protocols.