1. Record Nr. UNINA9910816880803321

Titolo	Secure multi-party computation / / edited by Manoj M. Prabhakaran and Amit Sahai
Pubbl/distr/stampa	Amsterdam ; ; Washington, DC, : IOS Press, 2013
ISBN	1-299-33339-7 1-61499-169-3
Edizione	[1st ed.]
Descrizione fisica	1 online resource (296 p.)
Collana	Cryptology and information security series, , 1871-6431 ; ; v. 10
Altri autori (Persone)	PrabhakaranManoj M SahaiAmit
Disciplina	005.8/2
Soggetti	Computer security - Management Cryptography
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Title Page; Foreword; Preface; Contents; General Cryptographic Protocols: The Very Basics; A Short Tutorial of Zero-Knowledge; Security and Composition of Cryptographic Protocols: A Tutorial; The BGW Protocol for Perfectly-Secure Multiparty Computation; Information-Theoretic Secure Multiparty Computation; The IPS Compiler; Randomization Techniques for Secure Computation; Complexity of Multi-Party Computation Functionalities; Author Index
Sommario/riassunto	Secure Multi-Party Computation (MPC) is one of the most powerful tools developed by modern cryptography: it facilitates collaboration among mutually distrusting parties by implementing a virtual trusted party. Despite the remarkable potential of such a tool, and decades of active research in the theoretical cryptography community, it remains a relatively inaccessible and lesser-known concept outside of this field. Only a handful of resources are available to students and researchers wishing to learn more about MPC. The editors of this book have assembled a comprehensive body of basic and advanced material on MPC, authored by experts in the field. It will serve as a starting point for those interested in pursuing research related to MPC, whether they are students learning about it for the first time or researchers already working in the area. The book begins with tutorials introducing the

concept of MPC and zero-knowledge proofs, an important theoretical platform where many of the concepts central to MPC were shaped. The remaining chapters deal with classical as well as recent MPC protocols, and a variety of related topics. Each chapter is self-contained and can be read independently of the others.