1

Introduction

Secure multi-party computation (MPC) enable a group to jointly perform a computation without disclosing any participant's private inputs. The participants agree on a function to compute, and then can use an MPC protocol to jointly compute the output of that function on their secret inputs without revealing them. Since its introduction by Andrew Yao in the 1980s, multi-party computation has developed from a theoretical curiosity to an important tool for building large-scale privacy-preserving applications.

This book provides an introduction to multi-party computation for practitioners interested in building privacy-preserving applications and researchers who want to work in the area. We provide an introduction to the foundations of MPC and describe the current state of the art. Our goal is to enable readers to understand what is possible today, and what may be possible in the future, and to provide a starting point for building applications using MPC and for developing MPC protocols, implementations, tools, and applications. As such, we focus on practical aspects, and do not provide formal proofs.

The term *secure computation* is used to broadly encompass all methods for performing computation on data while keeping that data secret. A computation method may also allow participants to confirm the result is indeed the output of the function on the provided inputs, which is known as *verifiable computation*.