Engineering Secure Two-party Computation Protocols

Secure two-party computation, called secure function evaluation (SFE), enables two mutually mistrusting parties, the client and server, to evaluate an arbitrary function on their respective private inputs while revealing nothing but the result. Originally the technique was considered to be too inefficient for practical privacy-preserving applications, but in recent years rapid speed-up in computers and communication networks, algorithmic improvements, automatic generation, and optimizations have enabled their application in many scenarios.The author offers an extensive overview of the most practical and efficient modern techniques used in the design and implementation of secure computation and related protocols. After an introduction that sets secure computation in its larger context of other privacy-enhancing technologies such as secure channels and trusted computing, he covers the basics of practically efficient secure function evaluation, circuit optimizations and constructions, hardware-assisted garbled circuit protocols, and the modular design of efficient SFE protocols. The goal of the author's research is to use algorithm engineering methods to engineer efficient secure protocols, both as a generic tool and for solving practical applications, and he achieves an excellent balance between the theory and applicability. The book is essential for researchers, students and practitioners in the area of applied cryptography and information security who aim to construct practical cryptographic protocols for privacy-preserving real-world applications. EAN/ISBN : 9783642300424 Publisher(s): Springer, Berlin Discussed keywords: Computersicherheit Format: ePub/PDF Author(s): Schneider, Thomas