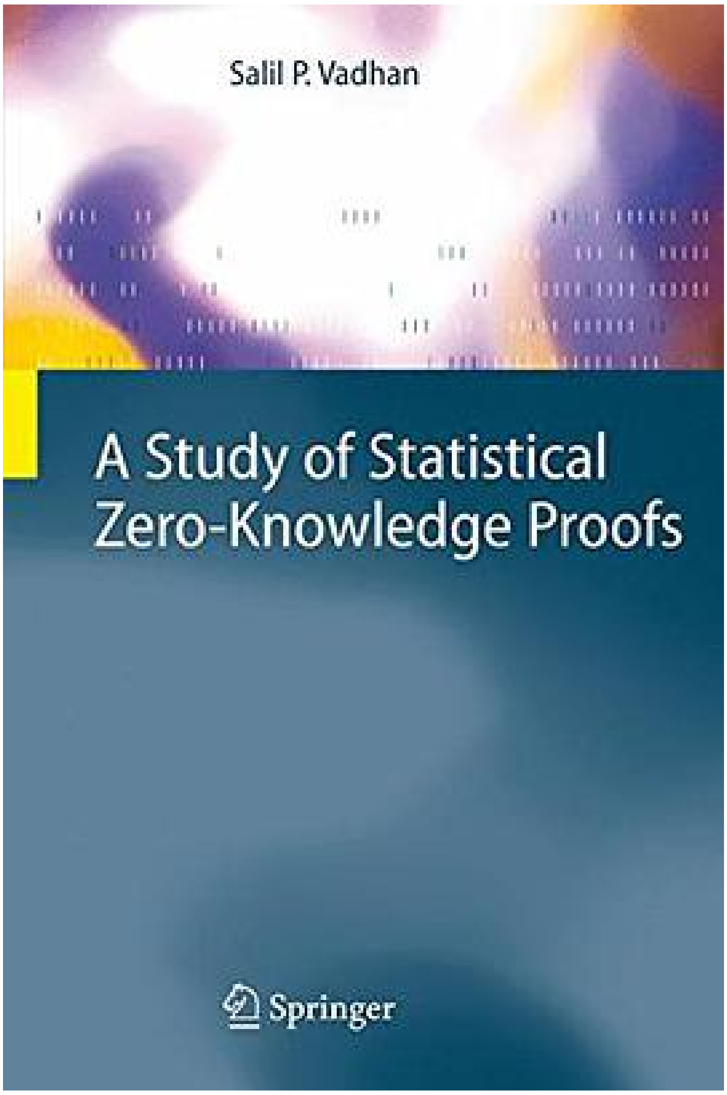
A Study of Statistical Zero-Knowledge Proofs



著者:Salil P. Vadhan

出版者:Springer

出版时间:2018-12-12

装帧:Hardcover

isbn:9783540713739

Zero-knowledge interactive proofs play a central role in the design and study of cryptographic protocols and are rich objects for complexity-theoretic study. Statistical zero-knowledge (SZK) proofs achieve strong information-theoretic 'security', and can provide a clean test bed for the study of more general notions that incorporate computational security. This monograph is a revised and extended version of the author's PhD thesis, the winning thesis of the 2000 ACM Doctoral Dissertation Competition. It is a comprehensive investigation of statistical zero-knowledge (SZK) proofs. It begins by showing that SZK has two natural complete problems, and then uses these complete problems to address a wide variety of fundamental questions about SZK. It also includes a chapter that surveys recent developments in the area, in particular how the results and techniques of this thesis have been extended to computational zero-knowledge proofs and arguments. The presentation offers clarity and intuition, assuming only a basic background in computational complexity and cryptography, and thus the book can bring a graduate student or a researcher in a related area up to date on this topic. At the same time, it includes clear statements of numerous open problems and research directions, which are likely to interest experts in the area.

作者介绍:

目录:

标签

评论

书评
