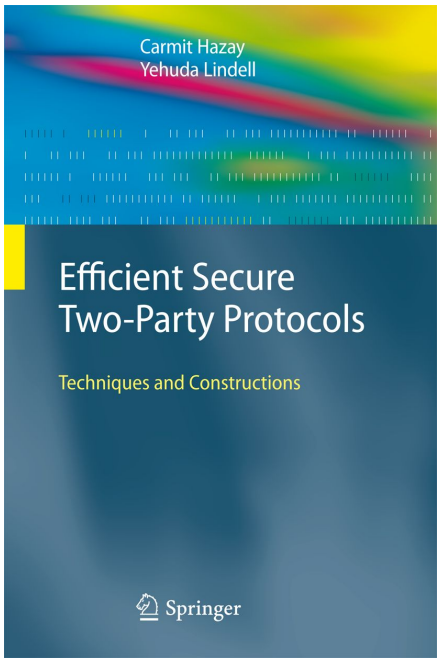

Carmit Hazay, Yehuda Lindell

Efficient Secure Two-Party Protocols

Techniques and Constructions

Series: Information Security and Cryptography

- **Essential reading for researchers in the area of secure protocols The authors compare the efficiencies of different protocols Essential reading for researchers in the area of privacy-preserving data mining**

In the setting of multiparty computation, sets of two or more parties with p- vate inputs wish to jointly compute some (predetermined) function of their inputs. The computation should be such that the outputs received by the parties are correctly distributed, and furthermore, that the privacy of each party's input is preserved as much as possible, even in the presence of - versarial behavior. This encompasses any distributed computing task and includes computations as simple as coin-tossing and broadcast, and as c- plex as electronic voting, electronic auctions, electronic cash schemes and anonymous transactions. The feasibility (and infeasibility) of multiparty c- putation has been extensively studied, resulting in a rather comprehensive understanding of what can and cannot be securely computed, and under what assumptions. The theory of cryptography in general, and secure multiparty computation in particular, is rich and elegant. Indeed, the mere fact that it is possible to actually achieve the aforementioned task is both surprising and intriguing.

2010, XIII, 263 p.

Printed book

Hardcover

129,99 € | £109.99 | $159.99
[1]139,09 € (D) | 142,99 € (A) | CHF 153,50

Softcover

89,99 € | £79.99 | $109.99
[1]96,29 € (D) | 98,99 € (A) | CHF 106,50

eBook

74,89 € | £63.99 | $84.99
[2]74,89 € (D) | 74,89 € (A) | CHF 85,00

Available from your library or springer.com/shop

MyCopy [3]

Printed eBook for just
€ | $ 24.99
springer.com/mycopy