

Springer

1st  
edition

2010, XIII, 263 p.

**Printed book**

Hardcover

**Printed book**

Hardcover

ISBN 978-3-642-14302-1

£ 109,99 | CHF 153,50 | 129,99 € |

142,99 € (A) | 139,09 € (D)

Available

**Discount group**

Science (SC)

**Product category**

Monograph

**Series**

Information Security and Cryptography

**Other renditions**

Softcover

ISBN 978-3-642-26576-1

**Computer Science : Programming Techniques**

Hazay, Carmit, Lindell, Yehuda

# Efficient Secure Two-Party Protocols

**Techniques and Constructions**

- **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 private 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 adversarial behavior. This encompasses any distributed computing task and includes computations as simple as coin-tossing and broadcast, and as complex as electronic voting, electronic auctions, electronic cash schemes and anonymous transactions. The feasibility (and infeasibility) of multiparty computation 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.

**Order online at [springer.com/booksellers](http://springer.com/booksellers)****Springer Nature Customer Service Center GmbH**

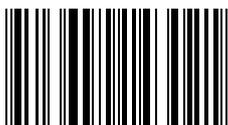
Customer Service

Tiergartenstrasse 15-17

69121 Heidelberg

Germany

T: +49 (0)6221 345-4301

[row-booksellers@springernature.com](mailto:row-booksellers@springernature.com)

ISBN 978-3-642-14302-1 / BIC: UM / SPRINGER NATURE: SCI14010

Prices and other details are subject to change without notice. All errors and omissions excepted. Americas: Tax will be added where applicable. Canadian residents please add PST, QST or GST. Please add \$5.00 for shipping one book and \$ 1.00 for each additional book. Outside the US and Canada add \$ 10.00 for first book, \$5.00 for each additional book. If an order cannot be fulfilled within 90 days, payment will be refunded upon request. Prices are payable in US currency or its equivalent.

Part of **SPRINGER NATURE**