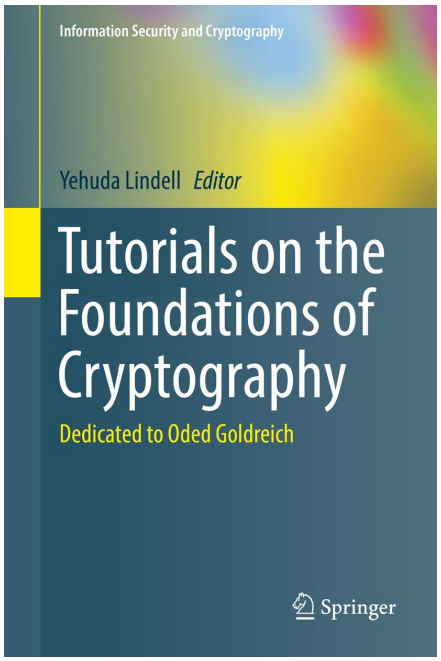

1st ed. 2017, XV, 450 p. 26 illus., 5 illus. in color.

Printed book

Hardcover

79,99 € | £69.99 | $99.99
[1]85,59 € (D) | 87,99 € (A) | CHF 88,00

Softcover

79,99 € | £69.99 | $99.99
[1]85,59 € (D) | 87,99 € (A) | CHF 88,00

eBook

67,82 € | £55.99 | $79.99
[2]67,82 € (D) | 67,82 € (A) | CHF 75,50

Available from your library or springer.com/shop

MyCopy [3]

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

Yehuda Lindell (Ed.)

Tutorials on the Foundations of Cryptography

Dedicated to Oded Goldreich

Series: Information Security and Cryptography

- Advanced tutorials developed by Benny Applebaum, Boaz Barak, Andrej Bogdanov, Iftach Haitner, Shai Halevi, Yehuda Lindell, Alon Rosen, and Salil Vadhan
- Domain and authors inspired by Oded Goldreich, a pioneering scientist, educator and mentor
- Appropriate for graduate tutorials and seminars, and for self-study by experienced researchers

This is a graduate textbook of advanced tutorials on the theory of cryptography and computational complexity. In particular, the chapters explain aspects of garbled circuits, public-key cryptography, pseudorandom functions, one-way functions, homomorphic encryption, the simulation proof technique, and the complexity of differential privacy. Most chapters progress methodically through motivations, foundations, definitions, major results, issues surrounding feasibility, surveys of recent developments, and suggestions for further study. This book honors Professor Oded Goldreich, a pioneering scientist, educator, and mentor. Oded was instrumental in laying down the foundations of cryptography, and he inspired the contributing authors, Benny Applebaum, Boaz Barak, Andrej Bogdanov, Iftach Haitner, Shai Halevi, Yehuda Lindell, Alon Rosen, and Salil Vadhan, themselves leading researchers on the theory of cryptography and computational complexity. The book is appropriate for graduate tutorials and seminars, and for self-study by experienced researchers, assuming prior knowledge of the theory of cryptography.