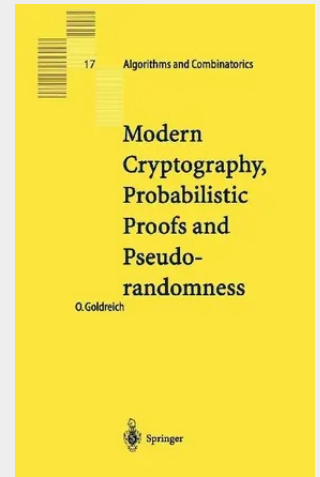


Modern Cryptography, Probabilistic Proofs and Pseudorandomness

You can start by putting the DO NOT DISTURB sign. Cay, in Desert Hearts (1985). The interplay between randomness and computation is one of the most fascinating scientific phenomena uncovered in the last couple of decades. This interplay is at the heart of modern cryptography and plays a fundamental role in complexity theory at large. Specifically, the interplay of randomness and computation is pivotal to several intriguing notions of probabilistic proof systems and is the focal of the computational approach to randomness. This book provides an introduction to these three, somewhat interwoven domains (i.e., cryptography, proofs and randomness). Modern Cryptography. Whereas classical cryptography was confined to the art of designing and breaking encryption schemes (or "secrecy codes"), Modern Cryptography is concerned with the rigorous analysis of any system which should withstand malicious attempts to abuse it. We emphasize two aspects of the transition from classical to modern cryptography: (1) the widening of scope from one specific task to an utmost wide general class of tasks; and (2) the move from an engineering-art which strives on ad-hoc tricks to a scientific discipline based on rigorous approaches and techniques.

You can start by putting the DO NOT DISTURB sign. Cay, in Desert Hearts (1985). The interplay between randomness and computation is one of the most fascinating scientific phenomena uncovered in the last couple of decades. This interplay is at the heart of modern cryptography and plays a fundamental role in complexity theory at large. Specifically, the interplay of randomness and computation is pivotal to several intriguing notions of probabilistic proof systems and is the focal of the computational approach to randomness. This book provides an introduction to these three, somewhat interwoven domains (i.e., cryptography, proofs and randomness). Modern Cryptography. Whereas classical cryptography was confined to the art of designing and breaking encryption schemes (or "secrecy codes"), Modern Cryptography is concerned with the rigorous analysis of any system which should withstand malicious attempts to abuse it. We emphasize two aspects of the transition from classical to modern cryptography: (1) the widening of scope from one specific task to an utmost wide general class of tasks; and (2) the move from an engineering-art which strives on ad-hoc tricks to a scientific discipline based on rigorous approaches and techniques.



139,09 €
129,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783540647669
Medium: Buch
ISBN: 978-3-540-64766-9
Verlag: Springer
Erscheinungstermin: 24.11.1998
Sprache(n): Englisch
Auflage: 1. Auflage 1998
Serie: Algorithms and Combinatorics
Produktform: Gebunden
Gewicht: 1030 g
Seiten: 183
Format (B x H): 160 x 241 mm

