Neuenschwander

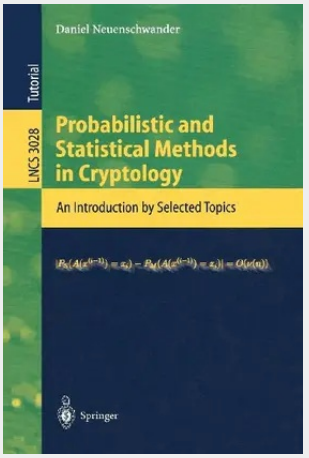
Probabilistic and Statistical Methods in Cryptology

Cryptology nowadays is one of the most important areas of applied mathematics, building on deep results and methods from various areas of mathematics. This text is devoted to the study of stochastic aspects of cryptology.

Besides classical topics from cryptology, the author presents chapters on probabilistic prime number tests, factorization with quantum computers, random-number generators, pseudo-random-number generators, information theory, and the birthday paradox and meet-in-the-middle attack.

In the light of the vast literature on stochastic results relevant for cryptology, this book is intended as an invitation and introduction for students, researchers, and practitioners to probabilistic and statistical issues in cryptology.

Cryptology nowadays is one of the most important areas of applied mathematics, building on deep results and methods from various areas of mathematics. This text is devoted to the study of stochastic aspects of cryptology.Besides classical topics from cryptology, the author presents chapters on probabilistic prime number tests, factorization with quantum computers, random-number generators, pseudo-random-number generators, information theory, and the birthday paradox and meet-in-the-middle attack.In the light of the vast literature on stochastic results relevant for cryptology, this book is intended as an invitation and introduction for students, researchers, and practitioners to probabilistic and statistical issues in cryptology.



53,45 €
49,95 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783540220015
Medium: Buch
ISBN: 978-3-540-22001-5
Verlag: Springer
Erscheinungstermin: 30.04.2004
Sprache(n): Englisch
Auflage: 2004
Serie: Lecture Notes in Computer Science
Produktform: Kartoniert
Gewicht: 277 g
Seiten: 162
Format (B x H): 155 x 235 mm

Kundenservice Verlag Dr. Otto Schmidt KG
Neumannstraße 10, 40235 Düsseldorf | kundenservice@otto-schmidt.de | 0221-93738-997 (Inland)