Katz

Digital Signatures

As a beginning graduate student, I recall being frustrated by a general lack of acces sible sources from which I could learn about (theoretical) cryptography. I remember wondering: why aren’t there more books presenting the basics of cryptography at an introductory level? Jumping ahead almost a decade later, as a faculty member my graduate students now ask me: what is the best resource for learning about (various topics in) cryptography? This monograph is intended to serve as an answer to these 1 questions — at least with regard to digital signature schemes. Given the above motivation, this book has been written with a beginninggraduate student in mind: a student who is potentially interested in doing research in the ?eld of cryptography, and who has taken an introductory course on the subject, but is not sure where to turn next. Though intended primarily for that audience, I hope that advanced graduate students and researchers will ?nd the book useful as well. In addition to covering various constructions of digital signature schemes in a uni?ed framework, this text also serves as a compendium of various “folklore” results that are, perhaps, not as well known as they should be. This book could also serve as a textbook for a graduate seminar on advanced cryptography; in such a class, I expect the entire book could be covered at a leisurely pace in one semester with perhaps some time left over for excursions into related topics.

Digital Signatures is the first comprehensive account of the theoretical principles and techniques used in the design of provably secure signature schemes. In addition to providing the reader with a better understanding of the security guarantees provided by digital signatures, the book also contains full descriptions and detailed proofs for essentially all known secure signature schemes in the cryptographic literature. A valuable reference for students, professors, and researchers, Digital Signature Schemes can be used for self-study, as a supplement to a course on theoretical cryptography, or as a textbook in a graduate-level seminar.

106,99 €
99,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9780387277110
Medium: Buch
ISBN: 978-0-387-27711-0
Verlag: Springer Nature Singapore
Erscheinungstermin: 03.06.2010
Sprache(n): Englisch
Auflage: 2010. Auflage 2010
Produktform: Gebunden
Gewicht: 1040 g
Seiten: 192
Format (B x H): 163 x 240 mm