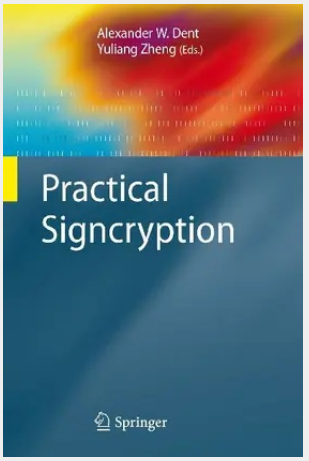
Dent / Zheng

Practical Signcryption



In today's world, data must be sent around the world cheaply and securely, and that requires origin authentication, integrity protection, and confidentiality – the recipient of a message should be able to ascertain who sent the message, be sure that the message has not been changed en route, and be sure that the data arrives without having been read by anyone else. The second editor invented signcryption, an area of cryptography that studies systems that simultaneously provide origin authentication, integrity protection and confidentiality for data. Signcryption schemes combine the features of digital signature schemes with those of public-key encryption schemes and aim to provide security guarantees in a way that is provably correct and significantly less computationally expensive than the "encrypt-then-sign" method most commonly adopted in public-key cryptography. This is the first comprehensive book on signcryption, and brings together leading authors from the field of cryptography in a discussion of the different methods for building efficient and secure signcryption schemes, and the ways in which these schemes can be used in practical systems. Chapters deal with the theory of signcryption, methods for constructing practical signcryption schemes, and the advantages of using such schemes in practical situations. The book will be of benefit to cryptography researchers, graduate students and practitioners.

In today¿s world, data must be sent around the world cheaply and securely, and that requires origin authentication, integrity protection, and confidentiality ¿ the recipient of a message should be able to ascertain who sent the message, be sure that the message has not been changed en route, and be sure that the data arrives without having been read by anyone else.The second editor invented signcryption, an area of cryptography that studies systems that simultaneously provide origin authentication, integrity protection and confidentiality for data. Signcryption schemes combine the features of digital signature schemes with those of public-key encryption schemes and aim to provide security guarantees in a way that is provably correct and significantly less computationally expensive than the ¿encrypt-then-sign¿ method most commonly adopted in public-key cryptography. This is the first comprehensive book on signcryption, and brings together leading authors from the field of cryptography in a discussion of the different methods for building efficient and secure signcryption schemes, and the ways in which these schemes can be used in practical systems. Chapters deal with the theory of signcryption, methods for constructing practical signcryption schemes, and the advantages of using such schemes in practical situations. The book will be of benefit to cryptography researchers, graduate students and practitioners.

106,99 €
99,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783540894094
Medium: Buch
ISBN: 978-3-540-89409-4
Verlag: Springer
Erscheinungstermin: 12.11.2010
Sprache(n): Englisch
Auflage: 1. Auflage. 2010
Serie: Information Security and Cryptography
Produktform: Gebunden
Gewicht: 606 g
Seiten: 274
Format (B x H): 160 x 241 mm