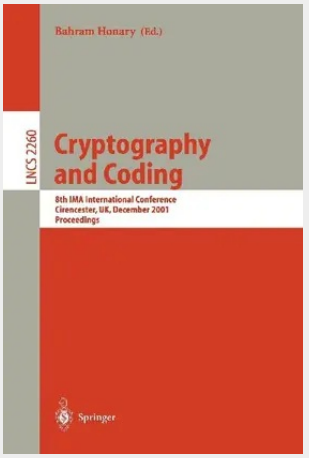
Honary

Cryptography and Coding

8th IMA International Conference Cirencester, UK, December 17-19, 2001 Proceedings

The mathematical theory and practice of cryptography and coding underpins the provision of effective security and reliability for data communication, processing, and storage. Theoretical and implementational advances in the fields of cryptography and coding are therefore a key factor in facilitating the growth of data communications and data networks of various types. Thus, this Eight International Conference in an established and successful IMA series on the theme of “Cryptography and Coding” was both timely and relevant. The theme of this conference was the future of coding and cryptography, which was touched upon in presentations by a number of invited speakers and researchers. The papers that appear in this book include recent research and development in error control coding and cryptography. These start with mathematical bounds, statistical decoding schemes for error correcting codes, and undetected error probabilities and continue with the theoretical aspects of error correction coding such as graph and trellis decoding, multifunctional and multiple access communication systems, low density parity check codes, and iterative decoding. These are followed by some papers on key recovery attack, authentication, stream cipher design, and analysis of ECIES algorithms, and lattice attacks on IP based protocols.

The mathematical theory and practice of cryptography and coding underpins the provision of effective security and reliability for data communication, processing, and storage. Theoretical and implementational advances in the fields of cryptography and coding are therefore a key factor in facilitating the growth of data communications and data networks of various types. Thus, this Eight International Conference in an established and successful IMA series on the theme of "Cryptography and Coding" was both timely and relevant. The theme of this conference was the future of coding and cryptography, which was touched upon in presentations by a number of invited speakers and researchers. The papers that appear in this book include recent research and development in error control coding and cryptography. These start with mathematical bounds, statistical decoding schemes for error correcting codes, and undetected error probabilities and continue with the theoretical aspects of error correction coding such as graph and trellis decoding, multifunctional and multiple access communication systems, low density parity check codes, and iterative decoding. These are followed by some papers on key recovery attack, authentication, stream cipher design, and analysis of ECIES algorithms, and lattice attacks on IP based protocols.



53,49 €
49,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783540430261
Medium: Buch
ISBN: 978-3-540-43026-1
Verlag: Springer
Erscheinungstermin: 10.12.2001
Sprache(n): Englisch
Auflage: 1. Auflage 2001
Serie: Lecture Notes in Computer Science
Produktform: Kartoniert
Gewicht: 1330 g
Seiten: 419
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)