

Zeitschrift: L'Enseignement Mathématique
Band: 48 (2002)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Kapitel: Information, communication, circuits

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. [Siehe Rechtliche Hinweise.](#)

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. [Voir Informations légales.](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. [See Legal notice.](#)

Download PDF: 06.10.2024

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>

economic or social considerations, is what constitutes the originality of this work. By presenting the interdisciplinary nature of these topics, the book has added value for scientists who wish to broaden their horizons and avenues of research.

Information, communication, circuits

Kazimierz ALSTER, Jerzy URBANOWICZ, Hugh C. WILLIAMS, (Editors). — **Public-key cryptography and computational number theory.** — Proceedings of the International Conference organized by the Stefan Banach International Mathematical Center Warsaw, Poland, September 11-15, 2000. — Un vol. relié, 18×25, de XII, 331 p. — ISBN 3-11-017046-9. — Prix: DM 256.00. — Walter de Gruyter, Berlin, 2001.

This volume contains articles from leading experts in the world on cryptography and computational number theory, providing an account of the state of research in a wide variety of topics related to the conference theme. It contains fifteen articles on public-key cryptography which are concerned with efficiency and security of DL-cryptosystems, DL-cryptosystems based on elliptic curves, the Jacobian of a hyperelliptic curve, algebraic groups and class groups of imaginary and real quadratic orders, connections between cryptography and error correcting codes, new cryptosystems (NTRU and XTR) and other new ideas in cryptography.

R.J. McELIECE. — **The theory of information and coding.** — Second edition. — Encyclopedia of mathematics and its applications, vol. 86. — Un vol. relié, 16×23,5, de XII, 397 p. — ISBN 0-521-00095-5. — Prix: £60.00. — Cambridge University Press, Cambridge, 2002.

This volume is a self-contained introduction to all basic results in the theory of information and coding. This theory was developed to deal with the fundamental problem of communication, that of reproducing at one point, either exactly or approximately, a message selected at another point. First there is a short and elementary overview that introduces the reader to the concept of coding. Following that part 1 is devoted to Shannon's main results, the channel and source coding theorems, and part 2 is devoted to a study of specific coding schemes which can be used for channel and source coding. The main changes in this edition are in part 2 which has been revised and expanded.

Annette WERNER. — **Elliptische Kurven in der Kryptographie.** — Un vol. broché, 15,5×23,5, de X, 142 p. — ISBN 3-540-42518-7. — Prix: € 22.95. — Springer, Berlin, 2002.

Dieses Lehrbuch bietet eine elementare Einführung in ein mathematisch anspruchsvolles Gebiet der modernen Kryptographie, das zunehmend an praktischer Bedeutung gewinnt. Die relevanten Tatsachen über elliptische Kurven und Public-Key-Kryptographie werden ausführlich erläutert. Dabei werden nur geringe Vorkenntnisse vorausgesetzt, um den Text für Studierende der Mathematik und Informatik ab dem fünften Semester sowie für Praktiker zugänglich zu machen.