Information, communication, circuits

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **47 (2001)**

Heft 3-4: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **25.05.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

Information, communication, circuits

Oded GOLDREICH. — **Foundations of cryptography: basic tools.** — Un vol. relié, 18×26, de XIX, 372 p. — ISBN 0-521-79172-3. — Prix: £40.00. — Cambridge University Press, Cambridge, 2001.

This book presents a rigorous and systematic treatment of the foundational issues: defining cryptographic tasks and solving new cryptographic problems using existing tools. It focuses on the basic mathematical tools: computational difficulty (one-way functions), pseudorandomness, and zero-knowledge proofs. The emphasis is on the clarification of fundamental concepts and on demonstrating the feasibility of solving cryptographic problems rather than on describing ad hoc approaches. The book is suitable for use in a graduate course on cryptography and as a reference book for experts.

Vyacheslav P. TUZLUKOV. — **Signal detection theory.** — Un vol. relié, 17×24, de XVIII, 725 p. — ISBN 0-8176-4152-1. — Prix: SFr. 148.00. — Birkhäuser, Boston, 2001.

The problem of noise immunity is a key problem for complex signal processing systems research in science and engineering. New approaches and problems of such complexity study allows the development of a better quality of signal detection in noise. This book is devoted to a new generalized approach to signal detection theory. The main purpose is to present the basic fundamental concepts of the generalized approach to signal processing in noise and to show how it may be applied in various areas of signal processing. The generalized approach allows extension of the well-known boundaries of the potential noise immunity set up by classical and modern signal detection theories. New approaches for construction of detectors with the amplitude, frequency and phase tracking systems based on the generalized approach are presented.