**Zeitschrift:** L'Enseignement Mathématique
**Herausgeber:** Commission Internationale de l'Enseignement Mathématique
**Band:** 47 (2001)
**Heft:** 3-4: L'ENSEIGNEMENT MATHÉMATIQUE

**Kapitel:** Information, communication, circuits

## *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.