

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

**Kapitel:** Information, communication, circuits

### **Nutzungsbedingungen**

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. 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. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

### **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. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

### **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. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

**Download PDF:** 27.04.2026

**ETH-Bibliothek Zürich, E-Periodica, <https://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.