collection informatique dirigée par Jean-Charles Pomerol

Algèbre et protection de l'information

Alain Poli
Philippe Guillot

Hermes
Lavoisier

Table des matières

collection informatique dirigée par Jean-Charles Pomerol

Cet ouvrage couvre l'algèbre classique et l'algèbre discrète ainsi que ses applications à la cryptographie et aux codes correcteurs d'erreurs.

Partant de la théorie des ensembles, il aboutit à la diagonalisation des matrices. Les structures finies sont étudiées, ainsi que certains circuits électroniques utilisés dans la pratique pour effectuer les calculs. Des exemples de complexité d'algorithmes sont donnés.

Ce livre introduit les principales techniques de protection des informations contre les attaques éventuelles. De nombreuses constructions sont proposées. Un exemple concret précède chaque preuve délicate. Plus de cent cinquante exercices et problèmes, avec leurs corrigés complets, illustrent *Algèbre et protection de l'information*.

Les auteurs

Alain Poli, responsable de vingt contrats avec l'industrie, a créé en 1984 la conférence internationale AAECC (Algèbre Appliquée Et Codes Correcteurs). Docteur d'Etat ès Mathématiques, il est professeur à l'université Paul Sabatier de Toulouse où il enseigne l'algèbre et les codes correcteurs.

Philippe Guillot a été successivement responsable des départements de cryptographie de Thales et de Canal+ Technologies. Il est actuellement maître de conférences à l'université Paris 8 où il enseigne la cryptographie.

ISBN 2-7462-1068-1

hermes Science publications

www.hermes-science.com