collection informatique dirigée par Jean-Charles Pomerol

Quels sont les enjeux de la cryptographie moderne ? Quels sont ses objets, son langage ? Quelles sont les solutions actuelles aux problèmes de confidentialité, d'authentification et d'anonymat ? Quel degré de confiance peut-on accorder à ces solutions ?

Cette seconde édition, enrichie et mise à jour, propose un panorama des outils et procédés de la cryptographie. Après avoir présenté et analysé les méthodes, cet ouvrage offre une description précise des techniques mathématiques indispensables et des principales primitives cryptographiques. Les fonctionnalités de base comme le chiffrement, la signature ou l'authentification, sont étudiées dans le cadre de la cryptographie à clé publique ou secrète.

Cryptographie analyse également l'interaction entre ces notions ainsi que leurs mises en œuvre dans des protocoles généraux et dans des applications concrètes. Il s'intéresse aux attaques contre les systèmes cryptographiques y compris celles par canaux cachés et par injection de fautes. Il aborde le domaine désormais indispensable des preuves de sécurité.

Les auteurs

Pierre Barthélemy est ingénieur de recherches au CNRS (Institut de Mathématiques de Luminy). Il s'intéresse plus particulièrement aux services de l'internet et à leur sécurisation.

Robert Rolland est chercheur associé à l'Institut de Mathématiques de Luminy et au laboratoire ERISCS (Aix-Marseille Université). Son domaine de recherche est centré sur les mathématiques et leurs applications à la cryptographie et au codage.

Pascal Véron est enseignant à l'Université du Sud Toulon-Var et chercheur au sein de l'Institut de Mathématiques de Toulon et du Var. Ses domaines de recherche sont la cryptographie, la théorie algébrique du codage et les liens entre ces deux disciplines.

978-2-7462-3816-9

hermes Science publications

www.hermes-science.com

Pierre Barthélemy
Robert Rolland
Pascal Véron

Cryptographie

collection informatique dirigée par Jean-Charles Pomerol

Cryptographie

principes et mise en œuvre

2e édition revue et augmentée

Pierre Barthélemy
Robert Rolland
Pascal Véron

hermes Lavoisier