<<混沌加密算法与Hash函数构造研究>>

图书基本信息

书名：<<混沌加密算法与Hash函数构造研究>>

13位ISBN编号：9787121130229

10位ISBN编号：712113022X

出版时间：2011-4

出版时间：电子工业出版社

作者：王永，李昌兵，何波　编著

页数：197

字数：291000

内容概要

本书紧跟混沌密码学的国际前沿，探讨了当前基于混沌理论的加密算法和Hash函数设计两项热点技术。
在混沌基本理论和密码学的基础上，详细介绍了混沌分组密码、混沌流密码、混沌图像加密算法、混沌公钥密码和混沌Hash函数，以及混沌加密算法和Hash函数的安全性分析指标，探析了基于混沌的加密算法和Hash函数的最新国际研究成果，以及混沌密码算法设计的主要思路和发展趋势。

本书可作为高等院校数学、计算机、通信、信息安全等专业从事混沌密码研究的本科生、研究生、教师和科研人员的研究用书或参考资料。

本书可作为高等院校数学、计算机、通信、信息安全等专业从事混沌密码研究的本科生、研究生、教师和科研人员的研究用书或参考资料。

书籍目录

版权说明