<<密钥共享体制和安全多方计算>>

图书基本信息

书名：<<密钥共享体制和安全多方计算>>

13位ISBN编号：9787121057922

10位ISBN编号：7121057921

出版时间：2008-2

出版时间：电子工业

作者：刘木兰

页数：238

字数：358000

<<密钥共享体制和安全多方计算>>

内容概要

本书共分5章。
第1章讲述密钥共享体制的基本概念和数学模型。
第2章系统讲述线性密钥共享体制和线性多密钥共享体制。
第3章讲述密钥共享体制的几个应用。
第4章讲述密钥共享体制的信息率。
第5章从密钥共享体制应用的角度讲述安全多方计算理论，特别给出了几个典型的安全多方计算协议安全性的详细证明。
本书可作为密码学和信息安全、网络安全、电子商务、计算机科学和信息科学等专业研究生和大学本科高年级学生的教学参考书，也可作为有关科研人员、工程技术人员的参考书。

<<密钥共享体制和安全多方计算>>

书籍目录

版权说明