

<<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

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<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

第1章 密钥共享体制的基本概念和模型 1.1 门限密钥共享体制 1.2 存取结构和一般密钥共享体制 1.3 完美、统计和计算密钥共享体制 1.4 理想的存取结构和拟阵 1.5 存取结构的信息率 1.6 图存取结构 1.6.1 图的基本概念 1.6.2 图存取结构 1.7 同态密钥共享体制 1.8 动态的密钥共享体制 1.9 可验证的密钥共享体制第2章 线性密钥共享体制 2.1 单调张成方案 2.2 线性密钥共享体制模型 2.3 线性密钥共享体制的例子 2.4 对偶线性密钥共享体制 2.5 存取结构的重组 2.6 线性多密钥共享体制模型 2.7 基于安全多方计算的线性多密钥共享体制 2.7.1 重构线性多密钥共享体制的主密钥 2.7.2 线性多密钥共享体制与直和线性多密钥共享体制 2.8 最优线性多密钥共享体制 2.9 非线性密钥共享体制 2.9.1 基于二次剩余的非线性密钥共享体制 2.9.2 拟线性密钥共享体制第3章 密钥共享体制的应用 3.1 密钥共享和数字签名 3.2 密钥共享用于电子拍卖 3.3 密钥共享用于电子选举 3.4 密钥共享用于承诺方案 3.4.1 门限结构攻击者情形 3.4.2 一般结构攻击者情形 3.5 密钥共享体制和线性码 3.5.1 线性单密钥共享体制和线性码 3.5.2 线性多密钥共享体制和线性码 3.6 黑盒密钥共享体制第4章 密钥共享体制的信息率 4.1 理想的图存取结构 4.1.1 密钥共享体制的矩阵表示 4.1.2 秩为2的理想密钥共享体制 4.2 图的分解结构和信息率 4.3 存取结构信息率的界 4.4 $|P|=5$ 时存取结构的信息率 4.5 有效密钥共享体制和计算有效的密钥共享体制 4.5.1 有效线性密钥共享体制 4.5.2 计算有效密钥共享体制和成员判定问题第5章 安全多方计算 5.1 安全多方计算的基本概念 5.1.1 什么是安全多方计算 5.1.2 攻击者及通信模型 5.2 安全多方计算的已知结果 5.3 安全多方计算的安全性定义 5.4 安全多方计算的一般实现方法 5.4.1 基于不经意传输协议的安全多方计算协议 5.4.2 基于同态密码体制的安全多方计算协议 5.4.3 基于线性密钥共享体制的安全多方计算协议 5.5 乘性单调张成方案与安全多方计算 5.6 基于双射标号映射的乘性单调张成方案 5.7 乘性单调张成方案的例子 5.7.1 基于图的连通性的存取结构 5.7.2 乘性单调张成方案的构造 5.8 一般乘性单调张成方案的构造 5.9 统计的安全多方计算 5.9.1 存取结构的定义和线性实现 5.9.2 图上的随机游动算法 5.9.3 一个统计的安全多方计算协议 5.10 并行的安全多方计算 5.10.1 什么是并行安全多方计算 5.10.2 并行安全多方计算协议 ……参考文献符号说明名词索引

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>