

<<量子签名及应用>>

图书基本信息

书名：<<量子签名及应用>>

13位ISBN编号：9787516500064

10位ISBN编号：7516500062

出版时间：2012-7

出版时间：航空工业出版社

作者：温晓军，陈永志 著

页数：188

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>

<<量子签名及应用>>

内容概要

《量子签名及应用》以课题组近年的研究成果为主体，结合量子签名在国内外的研究进展，经过归纳整理构建了量子签名的框架体系，并探讨了量子签名在电子支付系统和电子选举系统中的应用。

《量子签名及应用》分4部分（共9章）。

第一部分（即第1章）深入浅出地介绍了量子签名研究所必需的量子力学基础知识；第二部分（即第2章）简要地介绍了信息签名的基本知识以及量子签名的研究进展；第三部分（第3章~第7章）为量子签名协议的设计与分析，主要包括单用户量子签名、多用户量子签名和盲签名、群签名、代理签名等各种特殊用途的量子签名协议的设计及其安全性分析；第四部分（第8章、第9章）是量子签名在电子支付系统、电子投票系统中的应用。

<<量子签名及应用>>

书籍目录

第1章 量子信息学基础知识1.1 量子力学的基本概念和原理1.1.1 量子力学五大基本假设1.1.2 Hilbert空间与态矢量1.1.3 算符(算子)1.1.4 线性厄米算符及其本征值和本征矢表象1.1.5 量子态的演化么正变换1.1.6 量子测量1.2 量子信息的重要特性1.2.1 量子比特及其叠加特性1.2.2 量子测不准性1.2.3 量子不可克隆性1.2.4 量子纠缠性1.2.5 量子相干性1.3 量子纠缠交换1.4 量子密钥分配1.4.1 BB84协议1.4.2 892协议1.4.3 EPR协议1.5 量子逻辑门1.5.1 单比特量子逻辑门1.5.2 多比特量子逻辑门1.6 量子稠密编码1.7 量子隐形传态1.7.1 量子隐形传态1.7.2 可控量子隐形传态1.8 量子秘密共享1.8.1 方案依据的基本原理——GHZ三重态的量子关联性1.8.2 协议描述1.9 量子交换测试电路1.10 量子单向函数和量子指纹1.10.1 量子单向函数1.10.2 量子指纹第2章 信息签名基础2.1 经典数字签名基础2.1.1 数字签名的概念2.1.2 数字签名的分类2.1.3 计算复杂性问题及单向函数2.1.4 经典数字签名协议示例2.1.5 经典数字签名协议的弱点2.2 Zeng协议第3章 单用户量子签名协议3.1 基于量子纠缠交换的数字签名协议3.1.1 基本原理3.1.2 签名算法描述3.1.3 安全性分析3.1.4 结论3.2 基于EPR光子对的信息签名协议3.2.1 基于测量结果比较的签名协议3.2.2 基于量子远程通信的签名协议3.2.3 结论3.3 基于量子相干性的可信数字签名3.3.1 基本原理3.3.2 签名方案描述3.3.3 安全性分析与讨论3.3.4 结论3.4 不依赖于仲裁的量子信息签名协议3.4.1 签名协议描述3.4.2 安全性分析与讨论3.4.3 结论3.5 本章小结第4章 多用户量子签名协议第5章 量子群签名第6章 量子盲签名第7章 量子代理签名第8章 量子签名在电子支付系统中的应用第9章 量子签名在电子投票系统中的应用参考文献

<<量子签名及应用>>

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>