

## <<量子保密通信引论>>

### 图书基本信息

书名：<<量子保密通信引论>>

13位ISBN编号：9787564029289

10位ISBN编号：7564029285

出版时间：2010-1

出版时间：陈晖、祝世雄、朱甫臣 北京理工大学出版社，北京航空航天大学出版社，哈尔滨工程大学出版社，哈尔滨工业大学出版社，西北工业大学出版社 (2010-01出版)

作者：陈晖，朱甫臣 著

页数：169

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>

## <<量子保密通信引论>>

### 前言

在信息技术快速发展的今天，信息安全已不再是单纯的通信保密，而是一个涉及数学、物理、生物、化学、信息论、计算机和通信技术等诸多学科知识的综合学科，是一个融合信息的保密性、完整性、可用性、可控性和不可否认性为一体的综合体系，然而，对于长期困扰信息安全的完全保密、身份识别和窃听检测等问题并未得到彻底解决。

又因为在经典领域不可能有天然的保密信道，也很难实时发现各种入侵攻击，所有这些问题的彻底解决都需要新的保密通信技术。

近年来，随着人们对量子计算和量子信息的深入研究以及对信息系统安全需求的快速增长，科学家们发现了量子现象在信息科学中的许多新的应用，由于量子信息技术在提高信息处理速度、确保信息安全、增大信息容量和提高检测精度等方面有着经典信息技术无法比拟的潜在技术优势，得到了快速发展并且得到了广泛关注。

研究表明，完全保密的、物理安全的保密通信技术——量子密钥分发（QKD）将是最可能首先投入使用的量子信息技术。

为什么要研究量子密钥分发？

为什么要研究量子保密通信？

量子通信能否突破经典通信的距离和速率极限？

假如到2030年左右，量子计算机研究取得重大突破并开始投入使用，256比特密钥的对称密码算法将不安全，RSA等非对称密码算法也将不安全！

经典密码体制已经不能为信息系统提供安全性保证的情况下，人们如何保护他们的通信安全，国家又如何保护国防、军事、金融等重要领域内的信息安全？

这是本书力求回答的主要问题。

## <<量子保密通信引论>>

### 内容概要

《量子保密通信引论》从应用的角度出发，使用通俗的表达方式，系统地论述了量子保密通信的基本原理、体系结构、系统实现等，并探讨了量子保密通信技术在国防领域内的重要应用前景。全书共六章，主要内容包括保密通信概述、量子信息技术基础、量子密钥管理技术、量子保密通信体制、量子保密通信系统工程和量子保密通信与信息安全等。

《量子保密通信引论》内容深入浅出、层次分明、通俗易懂，可作为信息安全、密码学、通信和光通信、量子光学应用等相关学科的科研和工程技术人员的参考书，也可作为相关专业高等学校师生的参考书。

## &lt;&lt;量子保密通信引论&gt;&gt;

## 书籍目录

第1章 保密通信概述1.1 神秘的古代密码术1.2 经典保密通信介绍1.2.1 基于模运算的移位密码1.2.2 替换密码1.2.3 维吉尼亚密码1.2.4 Hill密码1.2.5 一次一密乱码本1.2.6 转轮机1.3 保密通信与战争1.4 经典密码学的发展历程1.4.1 经典密码学文献介绍1.4.2 经典密码学的发展阶段1.4.3 保密通信的基本要求1.5 经典密码理论介绍1.5.1 密码学基础介绍1.5.2 密码通信协议介绍1.5.3 经典信息论简介1.5.4 伪随机序列与序列密码1.5.5 分组密码1.5.6 公钥密码1.6 经典密码的困惑1.7 量子信息的研究背景和现状第2章 量子信息技术基础2.1 数学基础和量子态的表示2.1.1 矢量空间2.1.2 内积空间2.1.3 Hilbert空间2.1.4 Dirac符号2.1.5 Hermite算子与么正算子2.2 量子力学基本理论简介2.2.1 量子力学的基本假设2.2.2 量子测量2.2.3 量子的物理存在2.3 量子信息的形式2.3.1 量子态2.3.2 量子纠缠态2.3.3 GHZ态2.4 量子信息的特性2.4.1 量子不可克隆与概率测量2.4.2 存在隐匿的量子信息2.4.3 稠密编码2.4.4 量子隐形传态2.5 量子纠错码简介2.5.1 量子纠错与经典纠错2.5.2 量子纠错的基本思想和方法2.5.3 量子纠错的基本原理2.5.4 CSS量子纠错码2.6 量子计算简介2.6.1 量子逻辑门2.6.2 量子计算的并行性2.6.3 Deutsch问题算法2.6.4 Simon问题算法2.6.5 Grover量子搜索算法2.6.6 Shor量子因式分解算法2.7 量子信息论简介2.8 量子测不准与量子通信2.8.1 量子通信的特点2.8.2 量子保密通信安全性第3章 量子密钥管理技术3.1 经典密钥管理技术介绍3.1.1 经典密钥的分类和产生3.1.2 经典密钥管理介绍3.1.3 经典密钥分发技术介绍3.1.4 经典密钥管理技术的局限性3.2 量子密钥协商(QKA)3.2.1 基于非正交态的QKA3.2.2 基于纠缠态的QKA3.2.3 基于隐形传态的QKA3.3 QKA模型3.3.1 协议模型3.3.2 协议复杂性3.3.3 密钥的正确性验证3.3.4 QKA安全性分析3.4 量子密钥分发(QKD)3.4.1 基于共享密钥的QKD3.4.2 基于稠密编码的QKD3.4.3 无共享秘密信息的QKD3.5 量子密钥协商 / 分发的局限性3.6 量子密钥分发网络3.6.1 网络中的量子密钥分发3.6.2 量子网络中的数据传传输模式3.7 量子密钥的应用第4章 量子保密通信体制4.1 基于密钥的保密通信方案介绍4.1.1 经典OTP体制4.1.2 量子OTP体制4.2 量子保密直接通信协议介绍4.2.1 “一兵一兵”协议4.2.2 Two-StepQSDC协议4.3 量子保密通信体制模型4.3.1 量子通信的保密原理4.3.2 量子直接通信编码4.3.3 量子保密通信方案4.4 抗干扰量子保密通信4.5 量子保密通信网络4.6 量子身份识别4.6.1 身份识别与零知识证明4.6.2 基于量子隐形传态的身份识别4.6.3 基于量子态身份的身份识别4.7 量子密码介绍4.7.1 量子对称密码算法4.7.2 抗量子计算的非对称密码算法第5章 量子保密通信系统工程5.1 光通信系统5.1.1 光通信概述5.1.2 光纤通信系统简介5.1.3 光传输网络5.2 量子通信系统模型5.3 量子随机数发生器5.3.1 随机序列产生器和随机性检测5.3.2 量子随机数发生器实现原理5.4 量子信号源5.4.1 单光子系统5.4.2 纠缠系统5.5 量子信道与应用环境5.5.1 光纤5.5.2 自由空间5.5.3 深水空间5.6 同步与信号检测5.6.1 同步5.6.2 信号检测5.7 量子中继5.7.1 基于量子隐形传态的中继方案5.7.2 基于量子纠缠交换的中继方案5.8 量子态编码和量子信息处理5.8.1 干涉和消相干5.8.2 偏振态编码方案5.8.3 相位编码方案5.8.4 量子误码率和通信效率5.9 量子保密通信系统实例分析5.9.1 平衡M-Z干涉仪系统5.9.2 双非平衡M-Z干涉仪系统5.9.3 偏振自补偿干涉仪系统5.10 高速量子保密通信系统的应用前景第6章 量子保密通信与信息安全6.1 量子保密通信与完全保密6.2 量子保密通信发展趋势探讨6.3 应用前景与技术挑战附录A 术语和缩略语附录B 量子理论和量子信息的重要突破年代参考文献

## &lt;&lt;量子保密通信引论&gt;&gt;

## 章节摘录

插图：人类的各种社会活动都与通信有着密切联系，社会越进步，对通信的依赖程度就越大，尤其是在信息社会，一个国家乃至整个世界的社会、军事、政治、经济的正常运转和秩序维护都离不开通信。

在当今这个纷繁复杂的人类社会，各种邪恶势力、潜在敌人和黑客等为了得到一个国家各个领域内的重要情报，从未间断过针对各种通信的窃听、监控和破译。

在这种情况下，每个国家都不得不采用越来越先进的保密通信技术，以确保国家正常的保密通信不受现实威胁。

保密通信是维护国家安全的一个必要技术手段，也是一个十分重要的科学研究领域，有着十分悠久并且充满神秘的历史，它随着技术的发展和进步不断得到提高和完善。

本章分别对保密通信的几个重要发展阶段、经典密码在战争中所扮演的传奇作用、经典密码学基本理论、经典密码所面临的技术困难与挑战以及量子保密通信的发展契机等进行了介绍。

1.1 神秘的古代密码术“天机不可泄露”在当今是一个被泛用的词语，然而它的真正含义却是十分严肃的，一件东西或者一个消息之所以被称为“天机”，说明它是“神圣”的东西，不能主动或被动地对他人泄露其中的任何秘密，必须用忠诚甚至生命去捍卫它的安全。

在商业竞争中，一个公司或者单位的“天机”意味着能否在竞争中取得主动地位；在战争中，有关军队战略部署和战术的“天机”关系着前沿阵地将士们的生命安全和战争的结局，甚至整个国家的兴衰。

因此，为了确保“天机不可泄露”，从古至今，人们对如何实现这个目标的追求从未间断过，而确保“天机不可泄露”的主要技术手段就是形式多样的密码技术或者保密通信技术。

现实世界里保密的形式随着文明的发展程度、应用群体（士兵、外交官、写日记的人等）和应用目的等因素的不同而变化多样，保密通信的核心技术——密码技术因主要被用于保护一些“不宜”公开的“重要”信息而显得十分神秘，虽然它的起源缺少详细记载，但是密码技术在它几千年发展历程中却始终与人类战争紧密相连。

在公元前5世纪，古希腊的斯巴达人将皮条紧紧缠绕在特定尺寸的木棍子上，再把密信自上而下地写在皮条上；然后再把皮条解开并通过信使或者信鸽等送给目标接收者。

皮条的接收者只需要把皮条重新缠绕在相同尺寸的木棍上，就可以读出其中的信息。

而在不知道木棍尺寸的情况下，这些皮条上的文字是毫无意义的，由此达到保密通信的目的。

这就是有记载的最早使用的保密通信器械，并且称之为“天书”。

由于当时文明程度和技术条件限制，“天书”的应用基本上是手工作业，远距离通信依赖信鸽或信使等。

## <<量子保密通信引论>>

### 编辑推荐

《量子保密通信引论》：国防特色学术专著·信息与通信技术

<<量子保密通信引论>>

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>