

<<量子保密通信协议的设计与分析>>

图书基本信息

书名：<<量子保密通信协议的设计与分析>>

13位ISBN编号：9787030248374

10位ISBN编号：7030248376

出版时间：2009-6

出版时间：科学出版社

作者：温巧燕 等著

页数：293

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>

<<量子保密通信协议的设计与分析>>

前言

人们的生活离不开交流和沟通.从电报、电话等通信工具的出现,到通信网、互联网的飞快发展,人们相互间的交流越来越便利,需要交换的信息也与日俱增.在特定情况下,人们往往只想让期望的人看到自己发送的信息,而不希望其他人也得到这些信息.这一点在军事领域和商业领域尤其突出,一条军事机密的泄漏可能会导致战争的失败,一条商业机密的公开可能会给公司带来巨额经济损失,随着人们对信息保密的要求日益提高,保密通信研究也在不断发展和壮大,其基本目的就是确保用户间的秘密消息能够在公开信道中可靠地传输。

在保密通信中,通常称消息发送者为Alice,接收者为Bob,而窃听者为:Eve.为了达到保密的目的,Alice在发送消息前先利用加密密钥,根据一定的加密算法将要发送的消息M(即明文)加密,得到密文C,然后把密文C通过公开信道传输给Bob.Bob收到这些信息后可以用相应的解密密钥和解密算法由密文C恢复出明文M,从而得到Alice的真实消息.一般地,由于窃听者Eve不知道相应的解密密钥,即使她窃听到传输的密文C,也不能恢复出明文消息M.这就是保密通信的基本原理,其安全性取决于密钥的安全性.现代密码体制主要包括对称密码体制和公钥密码体制两类,它们在应用中各有特点.对称密码体制常用来直接对明文消息进行加密和解密,速度快且对选择密文攻击不敏感;公钥密码体制则主要用于密钥分发及数字签名等.因此在实际应用中一般采用混合密码系统,即用公钥密码体制在通信者之间分发会话密钥,然后用会话密钥通过对称密码体制来对通信消息进行加密。

大多数经典密码体制的安全性是建立在计算复杂性基础上的.也就是说,窃听者要想破译一个密码系统,需要在有限的时间 t (即秘密消息的有效期)内解决某个计算难题.而根据计算复杂性假设,这种任务通常在当前人们的计算能力下很难实现.这正是经典密码体制的安全性基础.但是,随着分布式计算和量子计算的发展,这种密码体制的安全隐患越来越突出.以1994年Shor提出的量子并行算法为例,它能在多项式时间内解决大数因子分解难题.一旦这种算法能够在量子计算机上付诸实施,现行很多基于此类难题的公钥密码体制将毫无安全性可言。

<<量子保密通信协议的设计与分析>>

内容概要

《量子保密通信协议的设计与分析》以作者及其课题组多年的研究成果为主体，结合国内外学者在量子保密通信领域的代表性成果，对这一领域的几个主要研究内容作了系统论述，并提出一些与之紧密相关的新研究课题。

全书分四部分（共8章）。

第一部分为量子保密通信研究所需的量子力学基础知识（第1章）；第二部分为量子密码协议的设计，主要包括量子密钥分发与身份认证、量子秘密共享、量子加密、量子安全直接通信（第2~5章）；第三部分为量子密码协议的分析（第6章）；第四部分为量子隐形传态以及与量子保密通信密切相关的量子纠错码（第7、8章）。

重点从密码学的角度阐述了量子密码协议的设计与分析。

《量子保密通信协议的设计与分析》既可作为对量子保密通信感兴趣的读者的入门教材，也可作为量子保密通信领域研究工作者的参考用书，适合于密码学、信息安全、信息与通信系统、信号与信息处理、物理学、数学及相关学科的高年级本科生、研究生、教师和科研人员阅读参考。

<<量子保密通信协议的设计与分析>>

书籍目录

第1章 量子力学基础知识1.1 基本概念1.1.1 状态空间和量子态1.1.2 完备正交基1.1.3 量子比特1.1.4 算子1.1.5 测量1.1.6 表象及表象变换1.1.7 密度算子1.1.8 Schmidt分解和纠缠态1.1.9 纠缠交换1.1.10 密集编码1.2 基本原理1.2.1 测不准原理1.2.2 量子不可克隆定理1.2.3 非正交量子态不可区分定理参考文献第2章 量子密钥分发与身份认证2.1 两个基本的密钥分发协议2.1.1 BB84协议2.1.2 GV95协议2.2 两类量子密钥分发协议的共同本质——信息分割2.3 不需要交替测量和旋转的量子密钥分发方案2.3.1 协议描述2.3.2 安全性分析2.3.3 结束语2.4 基于Bell基与其对偶基的量子密钥分发方案2.4.1 两级系统量子密钥分发协议2.4.2 d级系统中的纠缠交换2.4.3 d级系统中Bell基与其对偶基的关系2.4.4 d级系统量子密钥分发协议2.4.5 三级系统中在一对对偶基下进行的纠缠交换2.4.6 结束语2.5 利用不可扩展乘积基和严格纠缠基的量子密钥分发方案2.5.1 3×3 Hilbert空间的UPB和EEB的构造2.5.2 协议描述2.5.3 安全性分析2.5.4 到 $n \times n$ 系统的推广2.5.5 结束语2.6 基于w态的量子密钥分发方案2.6.1 w态的特点2.6.2 协议描述2.6.3 安全性分析2.6.4 结束语2.7 量子密钥分发中身份认证问题的研究现状及方向2.7.1 几种主要的身份认证协议及分析2.7.2 量子身份认证协议的基本要求及发展方向2.8 一种量子密钥分发和身份认证方案2.8.1 协议描述2.8.2 安全性分析及其他性质2.8.3 结束语2.9 一种网络多用户量子认证和密钥分发理论方案2.9.1 分布式客户机/服务器认证结构2.9.2 网络多用户量子认证和密钥分发理论方案2.9.3 安全性分析2.9.4 结束语2.10 注记参考文献第3章 量子秘密共享3.1 HBB协议3.2 基于多粒子纠缠态局域测量的量子秘密共享方案3.2.1 协议描述3.2.2 安全性分析3.2.3 推广到多方秘密共享3.2.4 结束语3.3 基于Bell态局域测量的量子秘密共享方案3.3.1.协议描述3.3.2 安全性分析3.3.3 结束语3.4 基于局域操作的量子秘密共享方案3.4.1 协议描述3.4.2 安全性分析3.4.3 推广到多方秘密共享3.4.4 结束语3.5 基于纠缠交换的环式量子秘密共享方案3.5.1 协议描述3.5.2 安全性分析3.5.3 推广到多方秘密共享3.5.4 结束语3.6 基于经典密钥的高效量子秘密共享方案3.6.1 基于GHZ态的量子秘密共享协议描述3.6.2 安全性分析3.6.3 基于Bell态的量子秘密共享协议3.6.4 结束语3.7 基于Grover算法的门限量子密码方案3.7.1 基于Grover算法的2量子比特操作3.7.2 基于Grover算法的 (t, n) 门限量子方案3.7.3 安全性分析3.7.4 特洛伊木马攻击可以被检测3.7.5 结束语3.8 注记参考文献第4章 量子加密4.1 两种基本加密算法4.1.1 基于经典密钥的量子加密算法4.1.2 基于量子密钥的量子加密算法4.2 d级系统量子加密算法4.2.1 d级系统中的态和门4.2.2 d级系统量子加密算法4.2.3 安全性分析4.2.4 纠错4.2.5 结束语4.3 注记参考文献第5章 量子安全直接通信5.1 BF协议5.2 对BF协议的改进及其安全性分析5.2.1 改进的BF协议5.2.2 安全性分析5.2.3 结束语5.3 注记参考文献第6章 量子密码协议的分析6.1 对一种量子考试协议的窃听与改进6.1.1 量子考试方案简介6.1.2 窃听策略描述6.1.3 改进方案6.1.4 结束语6.2 对基于d级推广Bell态的QKD协议的攻击6.2.1 KBB协议简述6.2.2 窃听策略描述6.2.3 结束语6.3 一次一密乱码本不能用来提高量子通信的效率6.4 重新审视量子对话和双向量子安全直接通信的安全性6.4.1 对NBA和MZL协议的分析6.4.2 对Jz协议的分析6.4.3 对MXN协议的分析6.4.4 信息泄漏与重复使用密钥的OTF'的等价性6.4.5 结束语6.5.共享参考系的一致性需要重新考虑6.6 对基于可重用GHZ载体的量子秘密共享协议的窃听6.6.1 BK协议简述6.6.2 外部攻击6.6.3 参与者攻击6.6.4 结束语第7章 量子隐形传态第8章 量子纠错码

<<量子保密通信协议的设计与分析>>

章节摘录

第6章 量子密码协议的分析 众所周知，密码编码学和密码分析学是密码学的两个重要组成部分。

密码编码学主要研究对数据进行变换的原理、手段和方法，目的是为了设计出安全的密码体制。

密码分析学主要研究消息的破译和消息的伪造，试图发现明文或密钥。

尽管密码编码学和密码分析学表面看来相互对立，但在整个密码学的发展中，它们却是相辅相成、互相促进的。

一般而言，一种先进的密码算法被设计出来后，密码分析家就会对其进行分析，评估其安全性。

一旦该密码算法被破译就需要寻找更安全的密码算法，密码学就是在这种不断的创立和破解中发展的。

就量子密码学而言，大家通常认为：量子密码系统的安全性由量子力学基本原理保证，无论窃听者有多大的计算能力也不能成功攻破它。

具体地，根据量子力学原理，窃听者要想从未知量子信号中提取有用信息，将不可避免地干扰量子信号的状态，进而会在检测窃听过程中被合法通信者发现。

因此，目前人们普遍热衷于提出新的量子密码协议，而对于协议分析却研究很少。

的确，对于一个设计完美的量子密码方案，任何有效的窃听都将被合法通信者发现，因此可以说在理论上量子密码具有无条件安全性。

然而，人们并不是总能提出这种近乎完美的协议。

由于不同的攻击手段对量子态引起的扰动各不相同，而检测窃听的方法又多种多样，所以并不是所有的检测方法都能够检测到任何可能的扰动。

因此，即使经过精心设计的量子密码协议也有可能被某些设计时没有考虑到的特殊攻击方法所攻破。

<<量子保密通信协议的设计与分析>>

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>