<<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

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f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Shot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。

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

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。

版权说明