量子加密技术

摘要

自从 BB84量子密钥分配协议提出以来 ,量子加密技术得到了迅速发展 ,以加密技术为基础的量子信息安全技术也得到了快速发展。 为了更全面地、 系统地了解量子信息安全技术当前的发展状况和以后发展的趋势 ,文中通过资料查新 ,以量子加密技术为基础 ,阐述了量子密钥分配协议及其实现、量子身份认证和量子数字签名、量子比特承诺等多种基于量子特性的信息安全技术的新发展和新动向。

关键词 :信息安全 ;量子态 ;量子加密 ;量子信息安全技术

一、绪论

21 世纪是信息技术高速进步的时代，而互联网技术为我们带来便捷和海量信息服务的同时， 由于我们过多的依赖网络去工作和生活， 网络通信、电子商务、电子金融等等大量敏感信息通过网络去传播。 为了保护个人信息的安全性， 防止被盗和篡改，信息加密成为解决问题的关键。那么是否有绝对可靠的加密方法，保证信息的安全呢？

随着社会信息化的迅猛发展，信息安全问题日益受到世界各国的广泛关注。密码作为信息安全的重要支撑而备受重视， 各国都在努力寻找和建立绝对安全的密码体系。而量子信息尤其是量子计算研究的迅速发展， 使现代密码学的安全性受到了越来越多的挑战。 与现代密码学不同的是， 量子密码在安全性和管理技术方面都具有独特的优势。 因此，量子密码受到世界密码领域的高度关注， 并成为许多发达国家优先支持的重大课题。

二、量子加密技术的相关理论

1、量子加密技术的起源

美国科学家 Wiesner 首先将量子物理用于密码学的研究之中， 他于 1969 年提出可利用单量子态制造不可伪造的“电子钞票” 。1984 年，Bennett 和 Brassard 提出利用单光子偏振态实现第一个 QKD(量子密钥分发）协议— BB84 方案。1992 年，Bennett 又提出 B92 方案。2005 年美国国防部高级研究计划署已引入基于量子通信编码的无线连接网络，包括 BBN办公室、哈佛大学、波士顿大学等 10 个网络节点。2006 年三菱电机、 NEC 东京大学生产技术研究所报道了利用 2 个不同的量子加密通信系统开发出一种新型网络，并公开进行加密文件的传输演示。在确保量子加密安全性的条件下，将密钥传输距离延长到 200km。

2、量子加密技术的概念及原理

量子密码，是以物理学基本定律作为安全模式， 而非传统的数学演算法则或者计算技巧所提供的一种密钥分发方式，量子密码的核心任务是分发安全的密钥，建立安全的密码通信体制，进行安全通讯。量子密码术并不用于传输密文，而是用于建立、传输密码本。量子密码系统基于如下基本原理：量子互补原理(或称量子不确定原理)，量子不可克隆和不可擦除原理，从而保证了量子密码系统的不可破译性。

3、基于单光子技术（即 BB84 协议）的量子密码方案主要过程：

a) 发送方生成一系列光子，这些光子都被随机编码为四个偏振方向；

b) 接收方对接收到的光子进行偏振测量；

c) 接收方在公开信道上公布每次测量基的类型及没测量到任何信号的事件序列，但不公布每次有效测量事件中所测到的具体结果；

d) 如果没有窃听干扰，则双方各自经典二进制数据系列应相同。如果有窃听行为，因而将至少导致发送方和接收方有一半的二进制数据不相符合，得知信息有泄露。

4、量子密码系统的安全性。

在单光子密码系统中，通讯密钥是编码在单光子上的，并且通过量子相干信道传送的。因此任何受经典物理规律支配的密码分析者不可能施行在经典密码系统中常采用的攻击方法：

1) 对加密算法进行分析 , 以找出“ 陷门 ”。

由于量子密码系统的实现所依据的是量子力学原理。而不是数学算法 , 因此无从下手进行算法分析。

2) 截获/ 重发, 并精确复制密钥用于进行穷举攻击。

单个量子不可能克隆的基本原理决定了这样的攻击对信道进行宏观测量都会破坏信道的量子相干性 , 并马上被通讯的合法用户所发现。

三、 量子密码学的几个研究课题

1、量子密钥分配

量子密钥分配是量子密码学中研究最早、 理论和实验成果最多的一个研究领域。量子密钥分配目前主要有两个研究方向：一个是基于连续变量 QKD的理论和实验研究；一个高速率、高性能的 QKD理论和技术研究。量子密钥最早研究得分配协议很多是关于两方之间的点对点的密钥分配。然而 QKD实际的实现要求网络中任意用户之间的密钥分配。 所以后来人们已研究了利用单光子的多用户 QKD方案，也提出了使用非正交基的多用户 QKD方案。

2、量子身份认证

上面所提出的 QKD均是假设通信方为合法用户的前提下，然而在实际的环境中，有可能有假冒者存在， 所以需要考虑通信方的身份认证问题。 基本的量子身份认证方案可分为两类， 即共享信息型和共享纠缠态型。 前者是指通信双方事先共享有一个预定好的比特串， 以此来表明自己是合法通信者； 而后者是双方共享有一组纠缠态粒子， 即双方各自拥有每对纠缠态粒子中的一个， 通过对纠缠对进行相应的操作也可以互相表明身份。这里需要强调一点， “ 共享信息 ”指经典信息，即经典的比特串。另外，与经典密码学中的身份认证类似，量子身份认证中也可以引入仲裁者，双方可以在仲裁者的帮助下验证身份。

3、量子签名

在量子保密通信的过程中， 像经典保密通信一样也会涉及到签名的问题， 目前量子通信和量子计算机的研究取得了迅速的进展， 特别是量子计算机， 它的出现使得对量子比签名成为重要的课题； 目前已提出了若干种量子签名方案， 主要有基于单向函数的量子签名方案，基于纠缠交换的量子签名方案，基于 GHZ三重态的量子签名方案。

4、量子加密算法

由量子态叠加原理可知， 一个有 n 个量子位的系统可以制备出 2n 个不同的叠加态, 即量子系统有强大的信息存储能力， 因此研究量子加密算法有重要意义。量子加密算法经典加密相比具有特殊的优点： 密钥可以重用。 如果发现通信错误小于一定阈值， 则可以将密钥经过保密放大处理后重复使用。 目前最多的量子加密算法有：基于经典密钥的量子加密算法和基于量子密钥的量子加密算法。

5、量子秘密共享

把一个秘密消息分割使得单个人不能重构该秘密消息是信息处理特别是高安全应用中常见的任务。现代密码学提供了解决方案 -- 秘密共享。随着 QKD的发展, 人们开始研究多方密钥分配问题， 于是很自然的提出了量子秘密共享 (QSS)这一新的方向。 QSS协议有三个主要目标： ① 在多方之间分发秘密密钥； ② 共享经典秘密信息；③ 共享量子秘密 (未知量子态)。另外对于如何提高秘密共享方案的效率也是人们研究的热点

四、阻碍量子密码学实用化的因素

（1）制造高效的单光子源比较困难

目前量子信道主要建立在光纤中，信息载体采用单光子，但是制造高效的单光子源比较困难。单光子源是将脉冲激光大幅度衰减且其光子统计服从泊松分布，当脉冲激光衰减到平均每个脉冲 0.1 个光子时，每个脉冲含 2 个以上光子的概率才降为 0.5%，当平均光子继续减少时单光子速率也相应降低，这将导致量子密码传输系统的带宽窄和传输速率慢。由于光纤的吸收，单光子无法实现远距离传输。

(2) 需要工作在所需波长高效单光子探测器还未成熟。

目前，常用的探测单光子的仪器有光电倍增管 (PMT)和雪崩光电二极管(APD)。但这两种器件的共同缺点是：需通过高压来获得放大。此外，PMT 在红外波段的量子效率太低以及其玻璃外壳使器件过大而易碎和 APD 需要液氮来降低噪声，这需要庞大的设备来维护且成本很高，同时为挫败潜在窃听者的企图，就必须采用高效的光子探测器以减少系统自身错误。

(3) 防窃听技术。

前面已经说明，量子在传输过程中，（3）～（5）三个过程采取的都是非量子方法。这在一定程度上也减弱了量子密码术在技术上的优势。这些问题都有待于整个量子信息技术的发展，例如量子存储器的技术等。

(4) 量子放大

量子通道的放大将不可避免地失去其量子特性，这使得量子信息传输的距离受到限制。

(5) 市场竞争

因为量子通信技术必须与传统的通信技术竞争以获得市场，而这些传统方法在长距离上以及成本费用上更低，从而使量子密码通信技术处于不利地位。这也是目前量子密码术难以立即转化为实用技术的原因之一。但是从总的发展趋势看，经典保密通信的成本是逐年提高，而量子密码通信的成本正随量子密码术的发展在降低。

(6) 自身的原因

量子密码系统即使在没有窃听者窃听的情况下，由于系统自身的不稳定性也会造成一定的长期误码率。还有在实际量子通信系统传输过程中，由于调制、采集数据过程中速度太慢和光探测器暗计数误码、信道噪声所产生的误码，从而导致实际的通信速度太慢和造成一定的误码率。

五、量子密码的前景

量子加密是一种前沿性、战略性的信息安全技术，随着量子计算机的研究与发展使得基于大数的因子分解的经典密码学越来越受到威胁，人们预测，当量子计算机成为现实，经典密码体制将无安全可言。而量子密码术和量子计算机都是根植于量子力学的，只有量子密码术能够抵挡量子计算机的攻击。所以，量子信息安全系统将成为保护数据安全的最佳选择之一。

六、我的几点思考

但是再趋近于完美的东西，也会有他致命的弱点。量子密码在理论上是无可挑剔的，但在实际应用上却存在许多问题，如：

1、如何保证信道的通信安全；

2、怎样提高抗干扰性；

3、量子密码要有一个初始密钥，且该方法的安全性很大程度上依赖于密钥的保密程度，密钥的选定方法及如何远距离保密协商密钥是目前面临的一个重要问题。

以上是本人对量子密码技术的研究成果，　水平有限，内容肤浅，望批评斧正！

七、参考文献

（1）量子密码学的应用研究 ---------- 何湘初 广东工贸职业技术学院

（2）量子加密技术探讨 ---------- 孟　洋　徐向阳　刘英娜

（3）基于量子理论的保密通信研究 ---------- 刘斌　刘涛　刘伟彦

（4）量子密码技术的前沿跟踪与研究 -------- 邵博闻 西安电子科技大学

（5）量子密码　可以保护你我网络信息 -------- 中国妇女报 /2011 年/2 月/10 日/ 第 B04 版

（6）量子信息安全技术 ---------- 赵生妹　姚佳　李飞　郑宝玉