量子通信的基本原理及其在电力系统中的应用

摘要

量子通信是基于量子力学的通信方式，其核心是量子的叠加性与纠缠性。相比于经典通信方式有着通信效率更高、信道噪声更小等优势，且其通信过程具有绝对安全的特点。目前关于量子通信的研究主要集中在对通信协议、通信中的工程技术以及量子通信应用的研究，在电力系统中已有广泛应用。目前，对量子通信主要存在着远距离通信难以实现、量子密钥产生效率低等问题。为更好了解其在电力系统中的应用前景，本文对量子通信的基本原理、具体通信协议及其在电力系统中的应用现状进行了综述。

关键词：量子通信，原理，协议，电力系统

1.1 引言

量子通信是量子信息学的一个重要分支，它标志着信息传输领域的一次重大突破。这一领域的核心在于量子的叠加性与纠缠性，其常与经典通信技术结合应用。

与经典通信技术相比，量子通信的优势主要体现在其具有高时效性、强抗干扰性能、较好的保密性以及传输较低的信噪比低。而目前对量子通信的研究主要存在着远距离通信难以实现、量子密钥产生效率低等问题。当下，电力系统中多用经典通信技术解决这些难题。

基于前人的研究，本文首先阐释了量子通信的基本原理。接下来，简要介绍了两种重要协议。最后，综述了其在电力系统中的应用现状。

2.1 量子网络基础

2.1.1 量子信息学基础

经典信息学主要基于电磁理论，量子信息学主要基于量子力学。我们知道，在经典频域内，比特是信息的基本储存单元，网络节点是复杂网络拓扑的基本组成单元。因此，我们首先探讨具有基础性的二者在量子域内的映射。

2.1.1.1 量子比特的叠加性与纠缠性

量子比特是量子信息的基本储存单元，同时也是量子信息学中的编码载体。比特是通过某一物理量状态的不同来描述信息的。传统比特的这种物理状态是离散电平；量子比特保留了其离散特性，但是通过量子的状态来描述信息的，也就是所谓的“叠加态”。量子力学中用态矢量描述量子的状态，其可以表示为0和1的叠加态：

其中，常取为矢量与0的夹角。布洛赫球形象地说明了这种叠加（图 1）。因此，一个量子比特在被观测前，其状态是0、1两种状态的相干叠加；观测后，这一比特就以概率塌缩到1态上，或以概率坍缩到0态上。经过观测，量子比特的相干部分就会丢失、变成了一个经典比特。这也就是我们熟知的“测不准”原理。因此，量子比特具体载体可以是电子自旋等，目前较广泛使用的载体是光纤发送的光子，其原理同样是横纵两个方向的偏振。[1]比特，或基本储存单元的不同是量子信息学与经典信息学的主要不同。

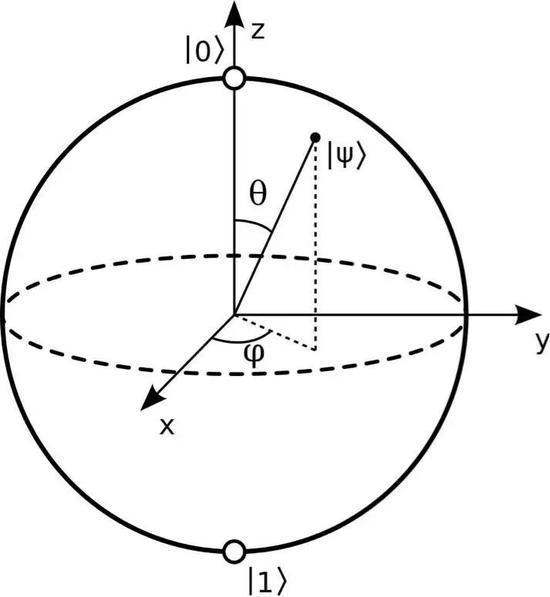


图 1 布洛赫球

除开叠加性，量子态的另一个性质是纠缠性。量子态纠缠指出，虽然单个量子的状态在观测前是不定的，但整个量子系统之间的每一个个体却是“纠缠”相关的。对相关的整个量子系统中的某个子系统进行局域操作，这事实上会影响到其余粒子的状态[2]，而这种相关性是与空间位置无关的。这种无视距离的相干特性构成了量子通信的基础。

2.1.1.2 量子域内的网络节点

网络节点是指具有独立地址并接入网络的一台网络设备。量子通信中的网络节点称量子节点。量子信息在量子节点中进行本地生成、处理和存储的操作，这些节点彼此通过量子通道连接，量子通道将量子态从某站点传输到另一站点，并在整个网络中纠缠相干。

量子通道有一个重要的优势：容量。我们假定一个k个节点组成、每个节点存有n个比特的网络。如果这个网络是由经典信道链接的，则其存储的信息量为；而如果是量子通道，其网络的状态数将指数级增长为。这也解释了我们熟知的量子计算机远快于经典计算机的事实。

2.1.2 量子通信的基本原理及主要问题

有了量子比特与量子节点作为基础，我们便可以探讨量子通信的基本实现及其主要问题了。我们知道，经典信息的传输载体主要是电磁波。量子信息的传递则利用了量子的纠缠性，信息的接收类似“解调”。其流程如下：

（1）发送方准备一组量子态A、B，并将其量子纠缠起来。

（2）发送方将其中一个量子粒子A发送给接收方。

（3）对A、B进行联合测量，B的测量结果由经典信道发送给接收方。接收方对A进行幺正变换（一种逆变换，类似解调）。

（4）双方利用公开信道比对测量结果，并纠正测量误差。若接收方得到了与发送方相同的量子态，则完成了信息的可靠传输。

需要注意的是，由于测量会导致坍缩，因此一次量子通信只能传递一次信息[3]。由于更细一步的通信涉及到了具体协议，将在下文深入讨论。

目前，电力系统中量子通信主要存在着以下问题。经典电磁信息通过某种方式进行调制编码，损耗和噪声则在中继站中被再放大来处理。然而，对于量子信息来说，这样的处理模式是不可能的，因为使用经典方法无法放大信号。因此，我们需要重新考虑一种处理方式。

同时，由于损耗、误差，量子通信的距离通常被限制在几百公里左右，这使得我们很难构建起一张广域的量子网络。目前，克服非放大的局限性并实现远距离通信主要有两种途径：其一是量子纠错，其二是中继站与卫星通信。后文将具体地讨论这两种技术。

2.1.3 量子通信技术研究分类

量子通信的相关技术主要可分为三方面：协议、通信技术、具体应用。下文将着重探讨这三方面。

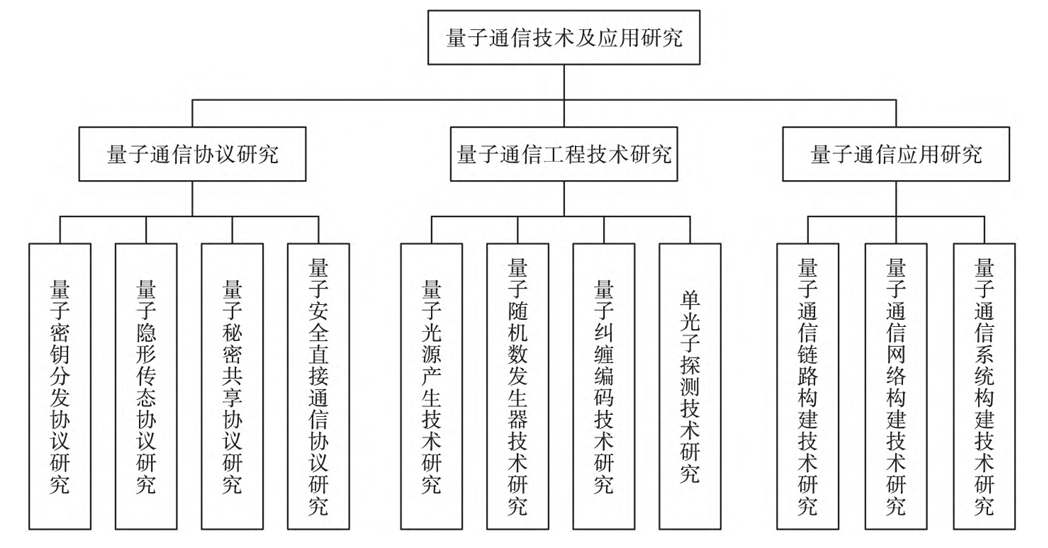


图 2 量子通信技术及其应用研究分类

2.2 量子通信协议

2.2.1 量子通信的安全性

量子通信的安全性其实非常简单，其本质就是量子的叠加性。由于“测不准”原理，窃听者是无法通过测量的手段获得量子态矢量的完整信息的；同时，经由测量，粒子的状态还会坍缩至0或1，这使得窃听行为被发现。那么，既然不能窃听，我们能否将物理信息完整地复制下来再解读呢？W.K.Wootters和W.H.Zurek于1982 年提出并完善了量子不可克隆原理[4]，指出未知的量子态不能被精确复制。因此，窃听者是无法通过克隆的方式获得量子态信息的。所以，我们说，量子通信是目前我们所知的唯一安全的通信方式。

基于上述，我们可以探讨量子通信中的具体协议了。目前，量子通信协议的架构已经基本成型，可划分为量子秘密共享、量子隐形传态、量子密钥分发和量子安全直接通信等协议。本文主要探讨后两种。

2.2.2 量子密钥分发协议

量子通信的过程可分为量子密钥分发、量子态传输两步。

首先是量子密钥分发。量子密钥分发是利用量子纠缠的特性实现密钥共享和保密传输的过程，其流程如下：

（1）通信双方各自准备一组纠缠的量子态。

（2）发送方随机选择一个量子态作为基，将此量子态发送给接收方。

（3）接收方测量接收到的量子态，将测量结果返回给发送方。

（4）发送方和接收方利用公开信道（如互联网）进行公开比对，去除测量中的误差，得到一致的密钥。

（5）发送方和接收方利用量子密钥进行加密和解密，实现消息的安全保密传输。

基于上述原理，一种较为经典的密钥分发协议是QKD协议。其具体内容如下：

（1）发送方随机生成一个量子密钥。

（2）发送方随机选择一个基。

（3）发送方根据所选基调制的单光子信号。

（4）接收方也随机选择一个基，用于接收。

（5）接收方根据单光子偏振态测量转换出的密钥。当双方选择的是同一偏振基时，能够测出正确的密钥，反之不能。

（6）接收方通过公开信道将自己选择的基发送给发送方，发送方将正确的基选择的子集通过公开信道返回给接收方。

（7）双方把相同基选择对应的密钥选择一段进行公布。如果双方公布的序列中出现不同，说明有人在窃听，此次通信作废。

（8）反之，则以密钥未公布的部分作为最终的密钥。[3]

我们会发现，这个过程并不是完全隐秘的，存在两次公开行为：第一次公开的是双方随机选择的基的情况；第二次公开的是密钥的一部分。通信过程的安全性主要与二次公布相关，下面分析有窃听的情况。

由前文可知，未知的量子态是无法复制的，但这并不代表着窃听者没有概率随机到与原量子态相同的量子态。窃听者可以测量发送方发送的量子状态，然后发送一个同样状态的量子态给接收方。首先，接收方选择一组偏振基，如果这组基与发送方使用的偏振基一致，则测量正确；反之，则测量正确和错误的概率各为50%。然后窃听者将与自己测量状态相同的量子态发给接收方[5]。

因此，在有窃听者的情况下，接收方接受收到量子态与发送方不一致的概率是25%（窃听者偏振基错误、测量错误各50%），量子通信的“绝对安全”是对于窃听行为而言的。

2.2.3 量子安全直接通信协议

量子安全直接通信适用于既对通信安全提出要求、又对通信效率提出要求的场景，如投票、谈判等任务，必须同时解决窃听和通信速度的问题。量子安全直接通信可分为单光子类和纠缠光子类。其原理图如下：

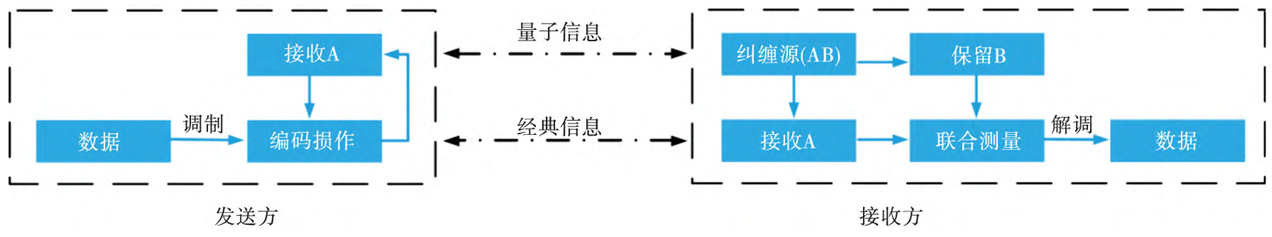


图 3 量子安全直接通信原理图[2]

目前，我国已实现距离为100km的量子安全直接通信[6]，使得在地球-卫星通信、城市间点对点通信等无法进行中继的场景中能够实现量子安全可靠通信。目前量子安全直接通信在电力系统中应用较为广泛。

3.1 量子通信在电力系统中的应用

由于电力系统是能量行业，其主要的优化方向包括功率与效率。目前一种应用广泛的效率优化方案是负载优化，闭环地检测负载，并相应调整输出阻抗，使得二者匹配（电电路知识）。这种闭环控制的成效与信息的传输效率直接相关，因此，量子通信能够很好地优化电力系统中的自动化过程。

3.1.1 电力系统面临的通信挑战

电力系统具有特殊性。首先，电网是面向所有人服务的行业，其覆盖面不仅大、而且全。其次，电力系统主要以宏电网、微电网相耦合为拓扑，是一种塔形拓扑，具有多主体的特性。因此，目前，电力系统中量子通信所面临的挑战主要有两类：

1）远距离信息传输。上文提到，量子通信中存在的一大问题是通信距离。我国幅员辽阔，电网规模稳居世界第一，这无疑对远距离通信提出了要求。

2）多主体通信。目前一种实现各电网间信息传输的数据结构是知识图谱，较流行的自动优化方案是负载优化。这二者的成效都与通信效率直接相关。现有的量子密钥技术成码率较低，满足多主体之间的通信需求不失为一种挑战。

3.1.2 远距离信息传输

前文提到，目前主流的远距离传输方案包括了量子纠错与中继站、卫星。由于量子纠错涉及到出错率、纠错原理、纠错码等方面，内容较为繁复，本文主要综述量子中继站与卫星。

为了规避整体距离较远的问题，我们可以将整个信道分成短距离段，并在这些段之间建立纠缠对。这就是量子中继站的基本原理。每个中间中继站使用纠缠交换可以生成长距离纠缠对，但若纠缠交换操作有噪声，则保真度会下降。

对于洲际远程通信，我们可以采用纠缠钝化的方案。我们可以从许多相同的噪声纠缠对拷贝生成少量拷贝，以此提高信息的保真率，这个过程就是纠缠纯化[7]。由于所需状态是已知的，因此我们能够规避未知量子态不可被克隆的定理。纠缠交换和纠缠纯化的彼此嵌套应用已经可以基本允许任意地点的远程量子通信。

卫星是远距离通信中非常重要的一环，而在量子通信中，除开卫星通信中典型的受大气影响大、定位困难、视野半径小等工程难题，另一大问题是保密程度。[8]目前的卫星量子通信的方案均要求信任卫星的提供商。

3.1.3 多用户量子通信

目前多用户通信的主要解决手段是对量子密钥的产生和分配的优化，即：统计通信的密钥需求与信号源的密钥生成效率，并按照量子密钥协议最大限度生成密钥，以有限的密钥满足尽可能多终端的通信需求。

目前量子多用户通信中仍未解决的技术问题还包括量子密钥成码率低，提供的密钥数量小于需求。这是并非电气工程研究的问题，而电力系统提出了自己的解决方案。电力系统约定，发送端对有限的量子密钥进行变换操作，得到数量未变、但量子性质不同的密钥，从而分发给终端[7]。目前应用较广的是连续变量协议。这种方案本质未涉及量子原理，且操作简单，因此具备实用价值。

参考文献

[1] W. Dür, R. Lamprecht, S. Heusler, European Journal of Physics, 38 (2017).

[2] 李冲霄, 李卓, 空间电子技术, 21 (2024) 72-80.

[3] S.R. Hasan, M.Z. Chowdhury, M. Saiam, Y.M. Jang, IEEE Access, 11 (2023) 15855-15877.

[4] ZHANG Haoran，SUN Zhen，QI Ruoyang，et al． Realization of quantum secure direct communication over 100km fiber with time-bin and phase quantum states[J]． Light：Science & Applications，2022，11(1)：83．

[5] H.J. Kimble, Nature, 453 (2008) 1023-1030.

[6] WOOTTERS W K，ZUREK W H．A single quantum cannot be cloned[J]．Nature，1982，299(5886)：802-803．

[7] 谢海鹏, 钱雨琦, 付炜, 王信, 别朝红, 中国电机工程学报, 43 (2023) 4485-4508.

[8] 彭柏语, 袁晨智, 张瑞明, 沈思, 张子昌, 李加睿, 林毅, 邓光伟, 王浟, 宋海智, 周强, 光学学报, 42 (2022) 119-134.