



西安电子科技大学
XIDIAN UNIVERSITY

雷达信号处理国家级重点实验室
National Laboratory of Radar Signal Processing

量子信息导论

主讲：李军

Email: junli01@mail.xidian.edu.cn

办公室：新科技楼1718室





西安电子科技大学
XIDIAN UNIVERSITY

雷达信号处理国家级重点实验室
National Laboratory of Radar Signal Processing

第七讲

量子通信



- 1. 量子通信基本概念**
- 2. 量子隐形传态技术**
- 3. 量子通信网络构建**

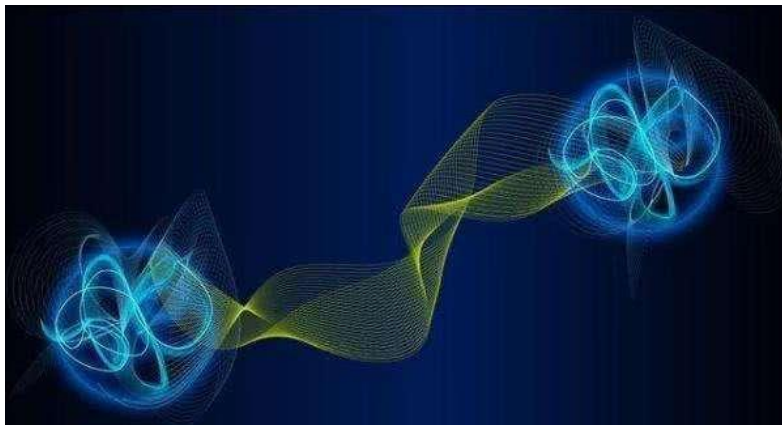


● 量子通信的概念

- 量子通信是利用量子叠加态和纠缠效应进行信息传递的新型通信方式
- 基于量子力学中的不确定性、测量坍缩和不可克隆三大原理提供了无法被窃听和计算破解的绝对安全性保证

物理保障

- 量子隐形传态
- 量子密钥分发
- 量子密集编码
- 量子中继





● 量子隐形传态简介

- 量子隐形传态 (Quantum teleportation) , 又称量子遥传、量子隐形传输、量子隐形传送、量子远距传输或量子远传,
- 是一种利用分散量子缠结与一些物理讯息的转换来传送量子态至任意距离的位置的技术。
- 它传输的不再是经典信息而是量子态携带的量子信息, 在量子纠缠的帮助下, 待传输的量子态如同经历了科幻小说中描写的“超时空传输”, 在一个地方神秘地消失, 不需要任何载体的携带, 又在另一个地方神秘地出现。

◆ 用量子态传递信息, 但需要经典辅助信号

◆ 因此, 信息的传递也不能超光速

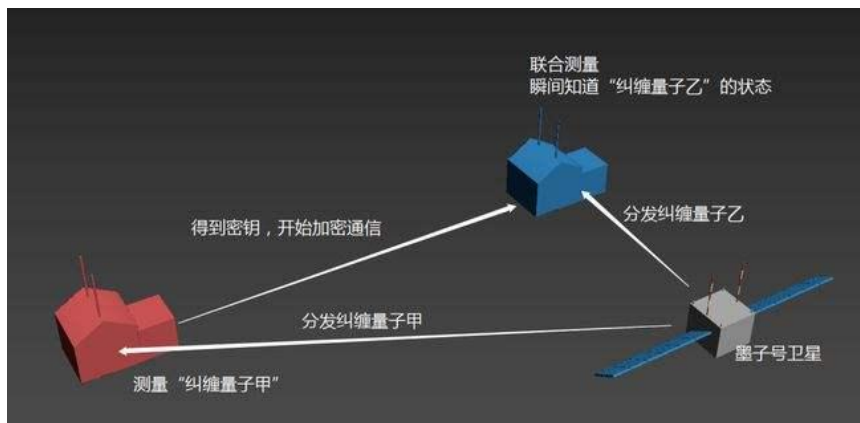


● 量子密钥分发简介

量子密钥分发（英语：quantum key distribution，简称QKD），是利用量子力学特性来保证通信安全性。它使通信的双方能够产生并分享一个随机的、安全的密钥，来加密和解密消息。

量子密钥分发的一个最重要的，也是最独特的性质是：如果有第三方试图窃听密码，则通信的双方会察觉。这种性质基于量子力学的基本原理：任何对量子系统的测量都会对系统产生干扰。第三方试图窃听密码，必须用某种方式测量它，而这些测量就会带来可察觉的异常。

- ◆ 只用于产生和分发密钥，并没有传输任何实质的消息
- ◆ 安全性基于量子力学的基本原理

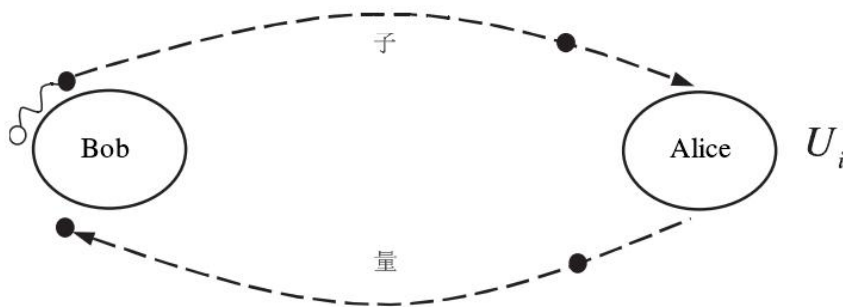




● 量子密集编码简介

- 量子密集编码的思想是Bennett和Wiesner于1992年提出来的。
- 其基本思想是**基于量子纠缠态的非定域空间特性**，对处于纠缠的量子系统的一个子系统做局域量子么正操作，只有在对整个量子系统做联合测量后才能读出局域量子操作的信息。这是与经典信息处理完全不同的事情。
- 在经典通信中，发送 1 个经典比特，只能得到 1 个比特经典信息；
- 而在量子通信中，利用量子纠缠的奇妙特性，发送 1 个量子比特，可以得到 2 个比特经典信息。

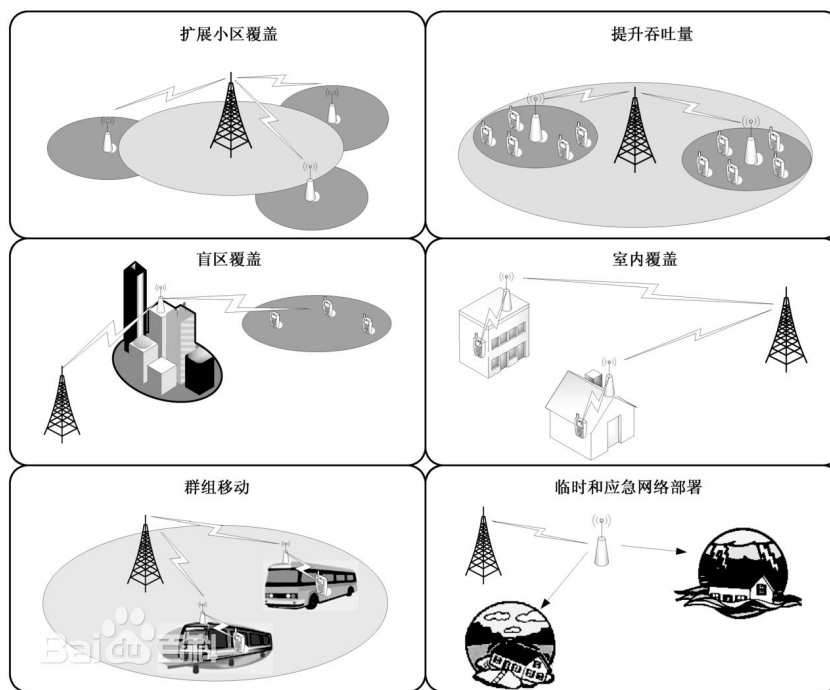
◆ 扩展了信道容量





● 量子中继技术

- 由于信道噪声很难完全消除，在其中**传输的信号将不可避免的**产生衰减和损耗，因此为确保信号的远距离稳定传输，进行信号中继是一个很好的选择。
- 对于基于纠缠态的量子通信来说，**纠缠交换**是量子中继的必备技术





1. 量子通信基本概念
2. 量子隐形传态技术
3. 量子通信网络构建



● 量子隐形传态概念的提出

1993年, Bennett 等来自4个国家的6位科学家联合在国际著名物理期刊《Phys. Rev. Lett. 》上发表了一篇题为“**经由经典和 EPR 通道传送未知量子态**”的开创性文章重新点燃人们研究隐形传物的兴趣并引发一系列富有成果的研究。



(top, left) Richard Jozsa, William K. Wootters, Charles H. Bennett. (bottom, left) Gilles Brassard, Claude Crépeau, Asher Peres. Photo: André Berthiaume.

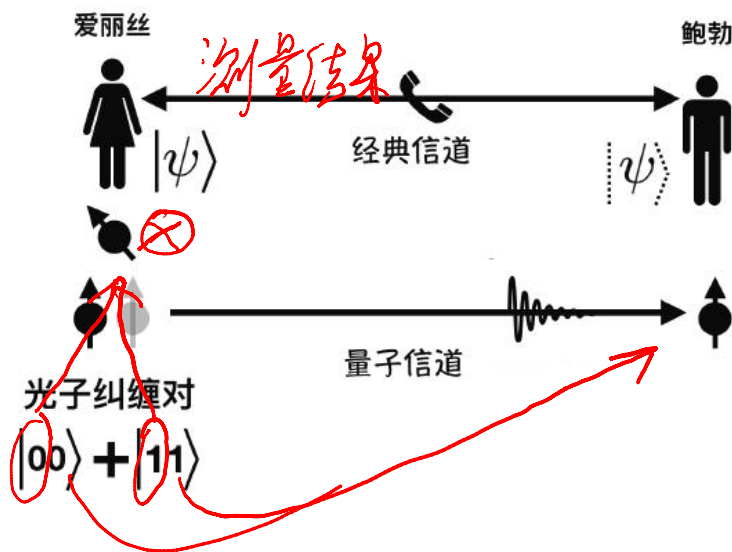


查尔斯·本内特 (Charles H. Bennett), 量子信息论的主要创立者, 国际商业机器公司 (IBM) 院士、美国物理学会院士、美国国家科学院院士, 2020年度香农奖 (Claude E. Shannon Award) 得主。



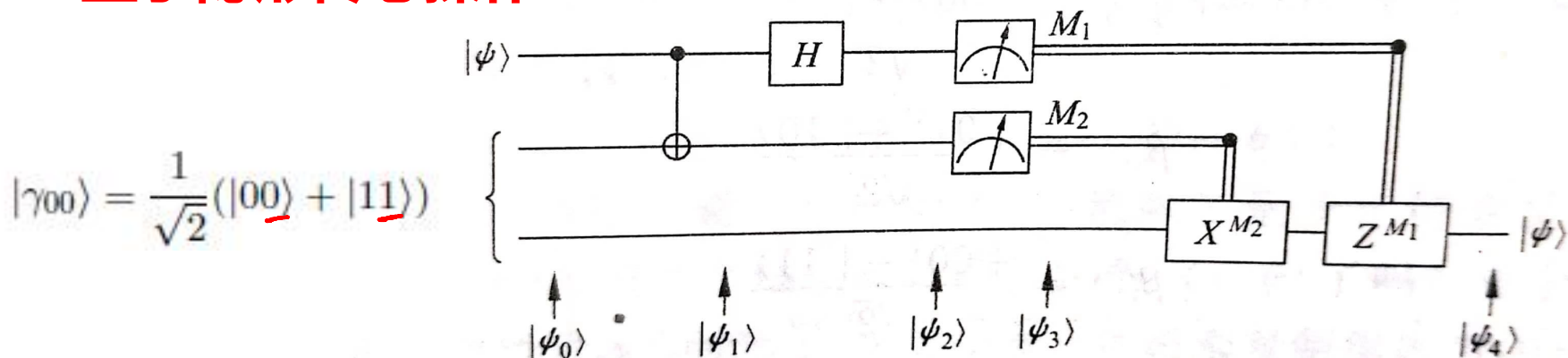
● 量子隐形传态基本思想

- 将两个粒子A和B制备一个纠缠态。而A粒子在甲地，B粒子在乙地。
- 信息分为经典和量子信息。分别经由经典通道和量子通道传送给接受者。
- 甲地的人对粒子A和携带信息粒子C构成的纠缠态，完成纠缠交换，或将C信息附加到A上时，由于A与B之间原来具有纠缠性，因而粒子B也具有这一信息。这时甲地对A和携带信息粒子C构成的纠缠态测量，并将测量结果通过经典通道传送给乙地，乙地根据这一结果还原出C所提供的信息。从而获得全面的量子信息。
- 而这时的经典信息的发送者可以对量子信息一无所知。





● 量子隐形传态操作



$$\begin{aligned}
 |\Phi\rangle_0 &= |\psi\rangle \otimes |\gamma_{00}\rangle = \frac{1}{\sqrt{2}} \left\{ \alpha |0\rangle \otimes (|\underline{00}\rangle + |\underline{11}\rangle) + \beta |1\rangle \otimes (|\underline{00}\rangle + |\underline{11}\rangle) \right\} \\
 &= \frac{1}{\sqrt{2}} \left\{ \alpha (|\underline{000}\rangle + |\underline{011}\rangle) + \beta (|\underline{100}\rangle + |\underline{111}\rangle) \right\} \quad (10.2)
 \end{aligned}$$

爱丽丝对自己的两个光子进行一个CNOT 门操作

$$|\Phi\rangle_1 = \frac{1}{\sqrt{2}} \left\{ \alpha (|\underline{000}\rangle + |\underline{011}\rangle) + \beta (|\underline{110}\rangle + |\underline{101}\rangle) \right\}$$



$$|\Phi\rangle_1 = \frac{1}{\sqrt{2}} \left\{ \alpha (|00\rangle + |01\rangle) + \beta (|11\rangle + |10\rangle) \right\}$$

爱丽丝然后对第一个光子进行哈达玛门操作

$$|\Phi\rangle_2 = \frac{1}{2} \left\{ \alpha (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) + \beta (|0\rangle - |1\rangle) \otimes (|1\rangle + |0\rangle) \right\}$$

将爱丽丝的两个比特和鲍勃的比特分开，重新安排一下这些项

$$\begin{aligned} |\Phi\rangle_2 = \frac{1}{2} \left\{ |00\rangle \otimes (\alpha |0\rangle + \beta |1\rangle) + |01\rangle \otimes (\alpha |1\rangle + \beta |0\rangle) \right. \\ \left. + |10\rangle \otimes (\alpha |0\rangle - \beta |1\rangle) + |11\rangle \otimes (\alpha |1\rangle - \beta |0\rangle) \right\} \end{aligned}$$

最后爱丽丝对自己的两个光子进行测量，并把测量结果通过电话等经典信道告诉鲍勃



● Bob的操作

1. 如果测量结果是 $|00\rangle$ ，鲍勃的光子正好处于 $|\Phi\rangle_3 = \alpha|0\rangle + \beta|1\rangle = |\psi\rangle$;
2. 如果测量结果是 $|01\rangle$ ，鲍勃的光子处于态 $|\Phi\rangle_3 = \alpha|1\rangle + \beta|0\rangle$ ，鲍勃作用 X 门后得到 $|\psi\rangle$;
3. 如果测量结果是 $|10\rangle$ ，鲍勃的光子处于态 $|\Phi\rangle_3 = \alpha|0\rangle - \beta|1\rangle$ ，鲍勃作用 Z 门后得到 $|\psi\rangle$;
4. 如果测量结果是 $|11\rangle$ ，鲍勃的光子处于态 $|\Phi\rangle_3 = \alpha|1\rangle - \beta|0\rangle$ ，鲍勃作用 Z 门和 X 门后得到 $|\psi\rangle$;



● 量子隐形传态的一个重要说明

- 量子隐形传态需要借助经典信道才能实现，因此**并不能实现超光速通信**；
- 在这个过程中，原物始终留在发送者处，被传送的仅仅是原物的量子态，而且**发送者对这个量子态始终一无所知**；
- 接受者是将别的物质单元(如粒子)制备成为与原物完全相同的量子态，他对这个量子态也始终一无所知；
- 原物的量子态在测量时已被破坏掉——**不违背“量子不可克隆定理”**；
- 未知量子态的传送，需要经典信道传送经典信息(即发送者的测量结果)，传送速度不可能超过光速——**不违背相对论的原理**。

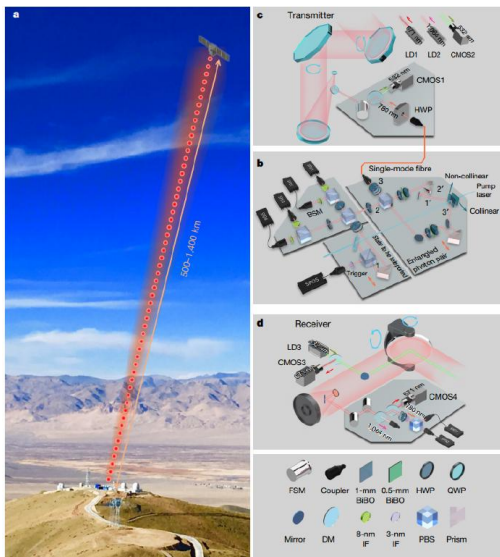
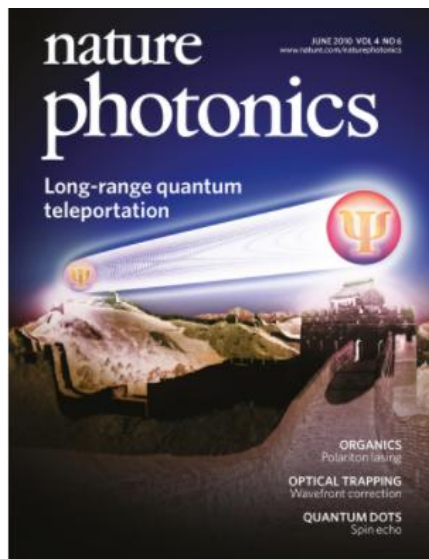


● 量子隐形传态的研究进展

2010年，中国科技大学的潘建伟等人又进行了自由空间 16km的量子隐形传态实验，成功地登上了《Nature Photonics》杂志的封面[8]。

2015年，有工作利用高效率的超导纳米线探测器实现了光纤信道中超过100km 的 Teleportation[9]

2017年，中国科技大学的潘建伟团队在“墨子号”卫星上，有工作实现了从地面到卫星超过 1400km 的 Teleportation.[10]



[8] X. M. Jin, J. G. Ren, B. Yang, et al. Experimental free-space quantum teleportation[J]. **Nature Photonics**, 2010

[9] Takesue H, Dyer S D, Stevens M J, et al. Quantum teleportation over 100 km of fiber using highly efficient superconducting nanowire single-photon detectors[J]. **Optica**, 2015

[10] Ren J G, Xu P, Yong H L, et al. Ground-to-satellite quantum teleportation[J]. **Nature**, 2017



1. 量子通信基本概念
2. 量子隐形传态技术
3. 量子通信网络构建



随着量子通信技术的发展，点对点的通信方式已经逐渐不能满足需求。为了以有限的资源给更多的用户提供安全通信服务，量子通信也逐渐走向了网络化发展的方向。

构建量子通信网络的基本架构主要包括四种方式：

- (1) 基于主动光交换的不可信网络，如光开关；
- (2) 基于被动光学器件的不可信网络，如光分束器(BS)、波分复用器(WDM)；
- (3) 基于信任节点的可信中继网络；
- (4) 基于量子中继的纯量子网络。

量子通信网络的基本拓扑结构主要有三种：

- (1) 星形拓扑结构；
- (2) 环形拓扑结构；
- (3) 总线型拓扑结构。



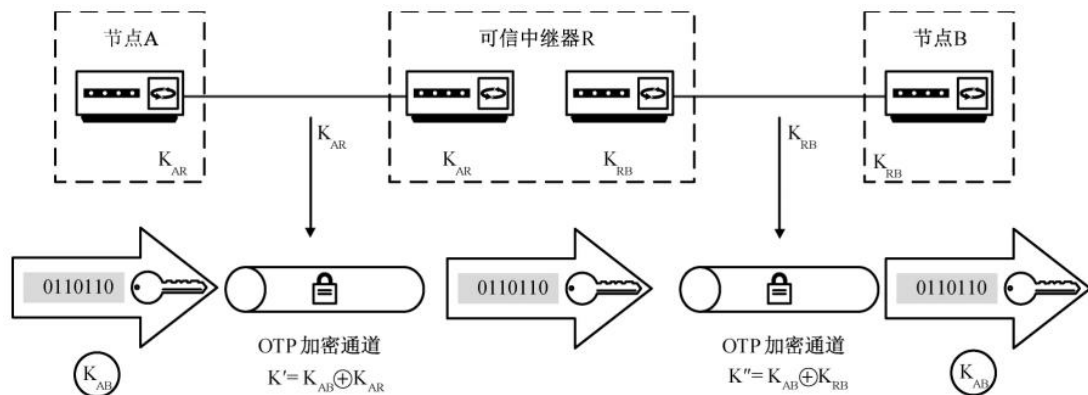


■ 基于光开关或无源光器件的架构

基于光开关或无源光器件实现多用户间的QKD 的基本思想是通过有源的光开关或者无源的光分路器、波分复用器，将多路量子信道复用传输，以实现多用户通信。在同一时隙内，当网络中只有一对用户建立量子链路，即可通过点对点 QKD 技术生成密钥。但是这种网络架构不具备可扩展性。这种网络与点对点 QKD 类似，最大的密钥分发距离仍受限于量子信道的损耗。

■ 基于可信中继的架构

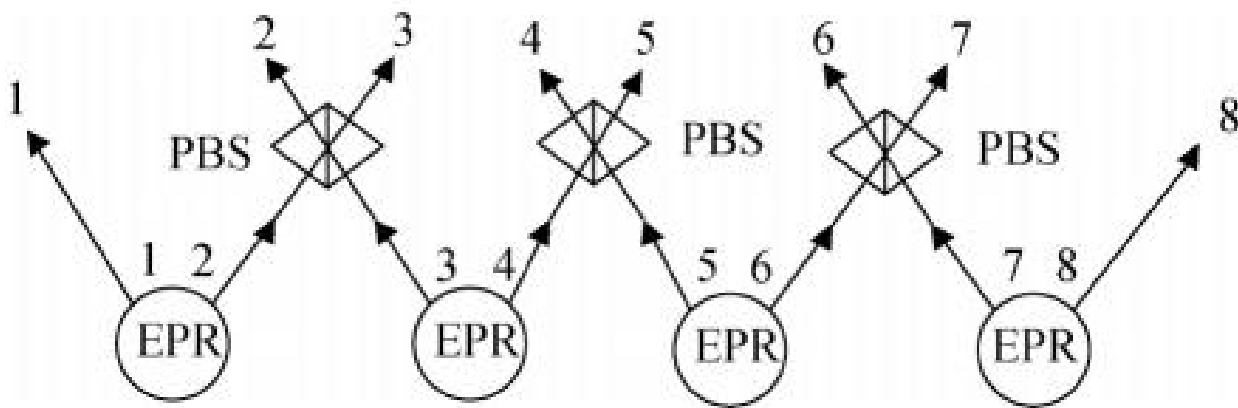
基于纠缠交换的量子中继难度较大，目前还难以应用。为构建远距离量子密钥分发基础设施采用的过渡方案是可信中继器方案。





■ 基于量子中继的架构

量子中继器将基于量子纠缠原理来实现，通过使用纠缠交换和纠缠纯化来实现量子纠缠效应的远距离中继延伸。通过迭代的纠缠交换，可以在任意长的距离上建立可用于生成安全密钥的纠缠在这个方案中，中继没有任何关于最终密钥的信息，因此其不必是可信节点。量子中继器涉及非常精细的量子操作和量子存储器，虽然已有多种技术方案，但距离实用还很遥远。



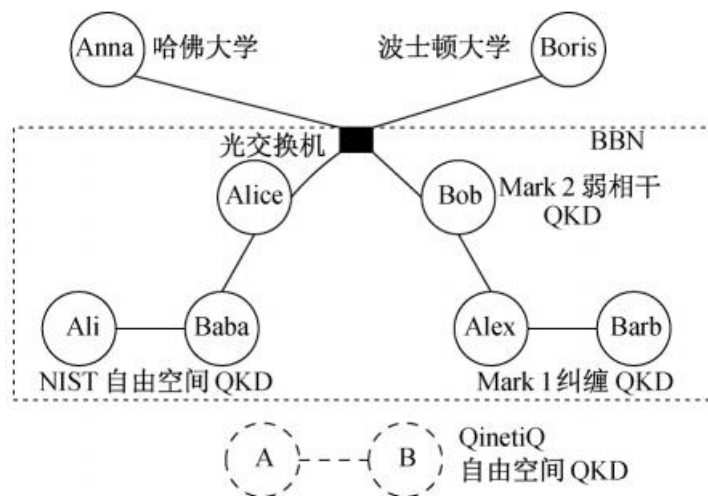
拓扑结构



● 美国 DARPA 量子通信网络

- 2002 年至 2007 年，在美国国防部高级研究计划局(Defense Advanced Research Projects Agency, DARPA) 的资助下，美国 BBN 技术公司、哈佛大学和波士顿大学联合研发了世界上第一个实地建设的量子保密通信网络。

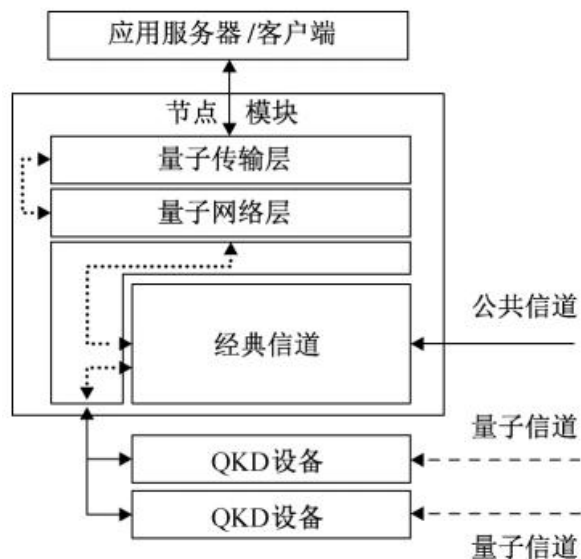
- DARPA 量子密钥分发网络采用多种 QKD 技术，支持光纤和自由空间两种信道。
- DARPA 网络中 4 个节点之间使用光纤弱相干态相位编码 BB84 方案，采用光开关切换方案构成无中继的QKD网络。其他线路则通过可信中继接入。



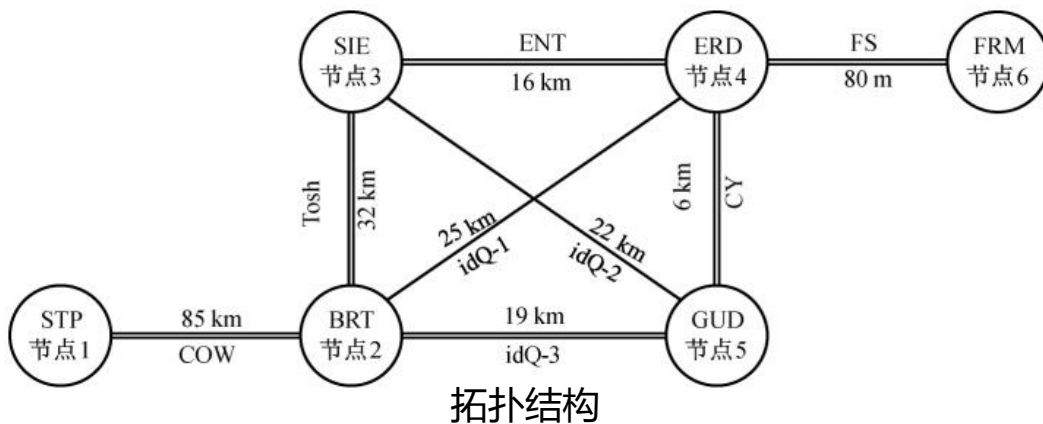


● 欧洲 SECOQC 量子通信网络

2004 年，欧盟基于量子密码的安全通信(Secure Communication based on Quantum Cryptography, SECOQC) 项目启动。2008 年，由英国、法国、德国、意大利等国的研发团队共同研发了 SECOQC QKD 网络。



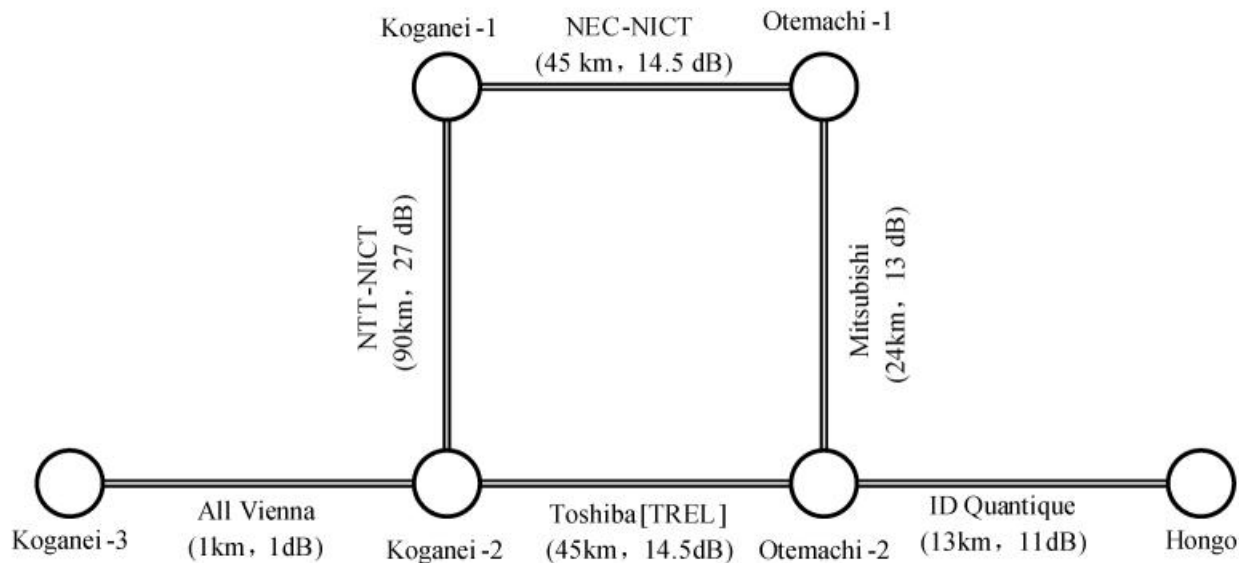
网络节点模型





● 日本东京量子通信网络

2010年,日本国家信息与通信研究院(National Institute of Information and Communication Technology, NICT) 与一些外国量子保密通信领域的研究机构合作, 成功在东京建成 6 节点的城域量子通信网络。东京 QKD 网络融合了六套量子密钥分发系统。

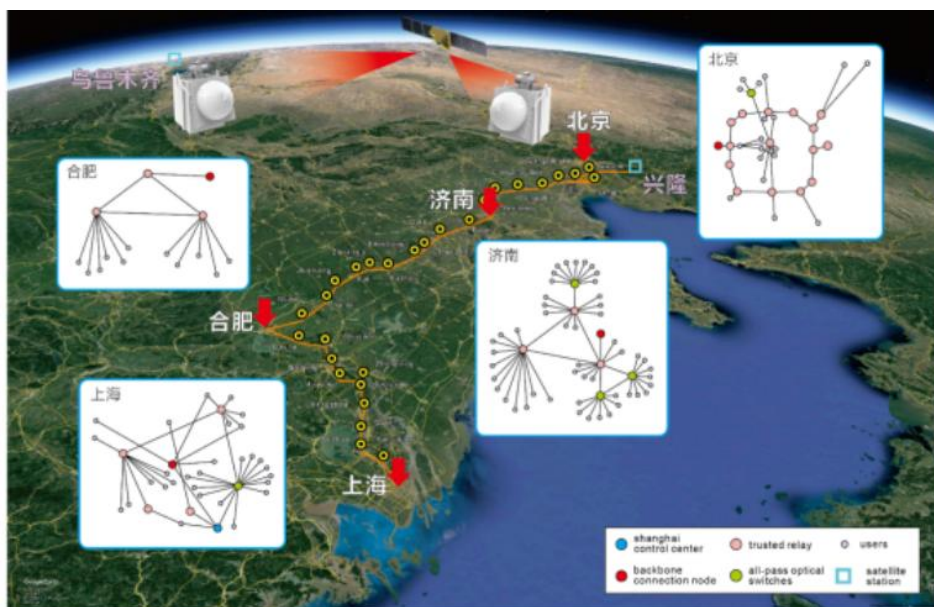


拓扑结构



● 中国天地一体量子通信网络

2021 年，基于量子保密通信“京沪干线”与“墨子号”量子科学实验卫星，中国构建了世界首个天地一体的广域量子通信网络，实现地面跨度 4600 公里、天地一体的大范围、多用户量子密钥分发，证明广域量子通信技术实际应用已经初步成熟，国盾量子为上述保密通信网络提供核心量子设备和技术支持。

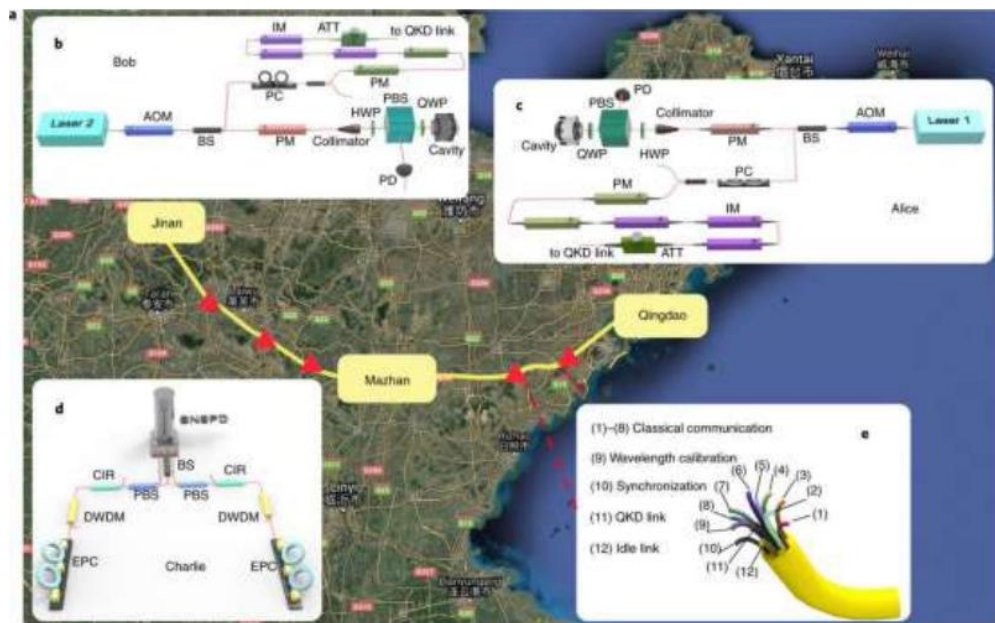


中国天地一体量子通信网络示意图



● 中国500 公里无中继光纤量子通信网络

2021年6月，中国科学技术大学、济南量子技术研究院、国盾量子联合研究团队使用已有商用光纤链路，突破现场远距离高性能单光子干涉技术，分别采用两种技术方案实现 500 公里量级双场量子密钥分发（TF-QKD），创造了现场无中继光纤量子密钥分发传输距离的新世界纪录。



中国500 公里无中继光纤量子通信网络示意图



课后问题

简答题：

- 1、量子通信技术分为哪几类？分别是什么含义？
- 2、写出量子隐形传态的过程。

拓展思考

- 1、要构建星地一体大规模量子通信网络，有哪些关键节点设备？简要说明这些节点设备如何组网。