

没有传递信息的量子通信，在传递什么？

摘要：量子通信是量子信息科学的重要分支，其中最重要的两个应用是量子密钥分发和量子隐形传态。量子密钥分发可为通信双方提供无条件安全的对称密钥分发方式，其理论安全性由量子力学规律保证；而量子隐形传态可保密远程转移量子态甚至纠缠态，是未来量子计算机通讯和量子中继的基础。但二者在量子信道中，都没有传递可编码的有序量子比特，而传递的是测量所导致的无序随机态和随机数序列，或转移未知的有序量子态。本文分析了量子密钥分发和量子隐形传态的协议过程，发现二者在量子信道中有一个共同点，即都没有且无法转移已知的有序比特或态序列，因而没有且无法通过量子信道传递确保准确的信息。

1. 经典比特在通信上的局限性

从经典信息学上，一个离散信源产生的消息（单个随机变量的取值序列），所包含的信息熵（平均信息量、平均不确定度），若以 2 为底，则单位（即最小的不可再分的对象）为 bit。

对于以 Bernoulli 分布的单变量的取值序列，所构成的一条消息，当其只包含 1 个符号（事件）时，其信息熵最大为 $-2 \times 0.5 \times \log_2(0.5) = 1$ bit；当其包含 2 个符号时，其最大信息熵为 $-4 \times 0.25 \times \log_2(0.25) = 2$ bit。

因此，在经典信息学中，对于等概率 0-1 分布的单变量取值序列，1 个 bit，对应 1 个符号；而 1 个符号，对应两个取值或状态，即 $0|0\rangle + 1|1\rangle$ 或 $1|0\rangle + 0|1\rangle$ 。

所以在经典信息学中，若不考虑误码^①，则 1 个 bit，不论在接收（测量）之前，还是之后，其值都前后一致地，或为 0，或为 1；对应相应的物理状态，在测量前后，一致地为 $|0\rangle$ 态或 $|1\rangle$ 态。

这意味着，从通信的角度，窃听者 C，总可以从信源 A、信道、信宿 B，这三端中的某一端，截获或复制原始消息，同时可做到不被信源 A 或信宿 B 发现。

2. 量子比特在密钥分发和隐形传态上的物理优势

量子信息科学，是物理上（如比特所对应的具体对象的态）立足于量子力学，

^① 即使对于经典比特，其 01 取值，在物理上也对应某个单元 or 系统的两种状态，比如磁畴或自旋的上下朝向、域值上下的高低电平；而读取、测量等操作，也是一个可能有源的、会与物质相互作用的，输入输出系统，可能会误判，甚至改变储存媒介、传递媒介（如载波）上的原有信号。

但上层建筑（如具体的量子态所代表的比特）构筑于传统信息学的交叉学科。

在量子信息科学中，信息量的单位，以及消息中的单个符号，是量子 bit；与经典信息学不同，由于底层规则受量子力学定律支配，单个量子比特，在测量前后，所处的状态（取值）不同：测量前，每一个量子 bit，都处于各本征态按一定比例^①线性组合的叠加态中；测量后，以一定的几率分布，塌缩到，以各本征态为基矢，所生成的态空间中的，某一个在测量前，并不能确定的态上。

以单光子的偏振态为例，若测量者选用的偏振片是 + 型的，则测量叠加态 $\alpha|\rightarrow\rangle + \beta|\uparrow\rangle$ 后所得的结果，分别以概率 α^2 和 β^2 塌缩到 $|\rightarrow\rangle$ 或 $|\uparrow\rangle$ 态上，分别对应 α^2 的概率得到一个 $|\rightarrow\rangle$ 态光子，有 $\beta^2 = 1 - \alpha^2$ 的概率得到一个 $|\uparrow\rangle$ 态光子。

但若测量者选用的偏振片是 × 型的，则在执行测量后，叠加态 $\alpha|\rightarrow\rangle + \beta|\uparrow\rangle = \alpha'|\nearrow\rangle + \beta'|\nwarrow\rangle$ 会分别以概率 α'^2 和 $\beta'^2 = 1 - \alpha'^2$ 塌缩到 $|\nearrow\rangle$ 或 $|\nwarrow\rangle$ 态上^②。

因此，量子比特额外拥有以下区别于经典比特的特殊性质，即量子力学的 2 大基本假设：量子态叠加原理、量子态被测量后按几率分布随机塌缩为某一确定态，以及由这两者^{③④}导出的量子不可克隆定理：无法克隆一个未知量子态^[1]。

量子比特的上述 3 个特性，就能保证以量子通信技术中的量子密钥分发(QKD, Quantum key Distribution)为协议的理想通讯过程的无条件安全性。

而利用测量前态叠加、测量后态塌缩，以及一个无法写成其系统态的张量积的、处于纠缠态的系统，这 3 个量子力学特性，传递未知量子态，是量子通信技术中另一大分支——量子隐形传态(QT, Quantum teleportation)技术的基石。

① 比例可以连续调整，以至叠加态的种类，是无穷多的；即叠加态与叠加态之间，可以因系数比例的不同，而互不相同。因此，不像经典比特，在测量之前和之后，只可能有 2 个/种离散的态，且几率比固定为 1:0 或 0:1；量子比特，在测量之前，有无穷多个/种塌缩到不同本征态的几率比的可能。

② 同时，多个量子态，可对应同一个码态 or 值，比如 $|\rightarrow\rangle$ 、 $|\nwarrow\rangle$ 均对应 $|0\rangle$ ，而 $|\nearrow\rangle$ 、 $|\uparrow\rangle$ 均对应 $|1\rangle$ 。

③ 一些资料，如 [科学网—谈谈量子不可克隆原理 - 姬扬的博文 \(sciencenet.cn\)](http://www.sciencenet.cn)，认为量子不可克隆定理，由不确定原理导出，理由是：将“克隆”理解为“复制一个所有属性均与目标对象一样的，第二个对象”，那么首先就需要“知道”“目标对象”的“所有属性”（无需“知道”的克隆看上去也存在，如受激辐射光放大，但这样的克隆仍被禁止，参见参考文献[1]）；而“知道”的途径，只有“测量”；但不确定原理告诉我们，无法同时精确测量得到同一个“目标对象”的“动量”和“位置”等，不对易的每一对物理量，也就无法同时测量得到“目标对象”的“所有属性”；所以当连要复制的对象的“所有属性”都不完全知悉时，是无法复制出另一个“所有属性”全与之一模一样的“对象”的——都不知道要复制出什么样的精确属性的“对象”。总而言之，无法知道量子态的所有信息/属性，则无法复制量子态的所有信息/属性。

④ 我认为，复制量子比特，不需要复制对象的所有属性，毕竟测不准原理约束着；而是只需要复制用于作为量子态的那一个属性，比如对于光子，可以是偏振，也可以是路径；对于原子系统，可以是两个纠缠的能级，而不需要关心作为量子比特的量子系统的其他属性，比如动量、位置等。那么对于一个确定的量子态，即对于一个量子系统的确定的某个属性，是可以被复制的；但对于未知的量子态，仍然没法被复制。因为有且只有通过执行测量的方式，才能知道量子态的状态，或获得塌缩到各个态的几率分布；然而一旦执行测量，则对于单个量子态，则会从叠加态随机塌缩到某个本征态，得到的是改变后的、某个随机的态，并且一次测量不会显示出塌缩到该态的几率，也就更无法推知原叠加态的几率分布，也就无法复制原叠加态。——除非信源发送多个几率分布相同的量子态，这样窃听者就能通过多次测量并验证，相同的多个叠加态的塌缩比例分布，来得知该叠加态塌缩前的几率分布。

3. 量子密钥分发

3.1 量子信道无窃听的 BB84 协议过程

1984 年, Bennett 和 Brassard, 正式提出了量子通信技术中的第一个量子密钥分发(QKD)协议 (图 1): BB84 协议^[2]。

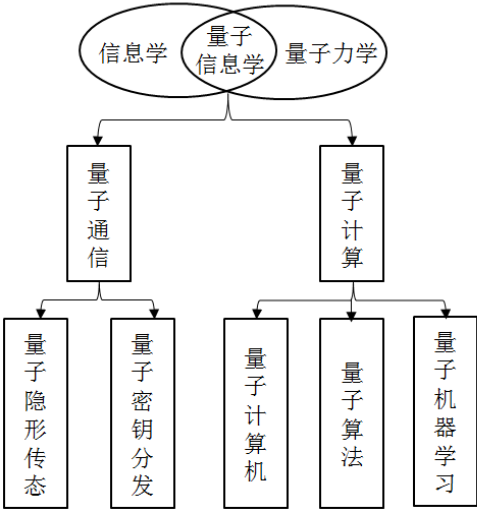


图 1. 量子信息学的研究分支

以传递一条符号数量为 1000 的消息为例，基于光量子偏振态的 BB84 协议的通讯过程如下：

首先，A 用线性起偏器，制备并发送一串随机偏振态序列（图 2 首行），其中每一个态，都是 4 种不同的单光子偏振状态： $0^\circ \rightarrow$ 、 $45^\circ \nearrow$ 、 $90^\circ \uparrow$ 、 $135^\circ \nwarrow$ 之一，并分别对应各自所代表的量子比特取值：0、1、1、0（图 2 末行）。



图 2. A 发送的随机偏振态序列及相应的比特值（前 20 个）和二者的数量分布

接着,暂时不考虑外在原因导致的损耗和误码, B 使用随机的检偏器序列 (图 3), 来测量 A 所发送的偏振态序列 (图 2 首行)。

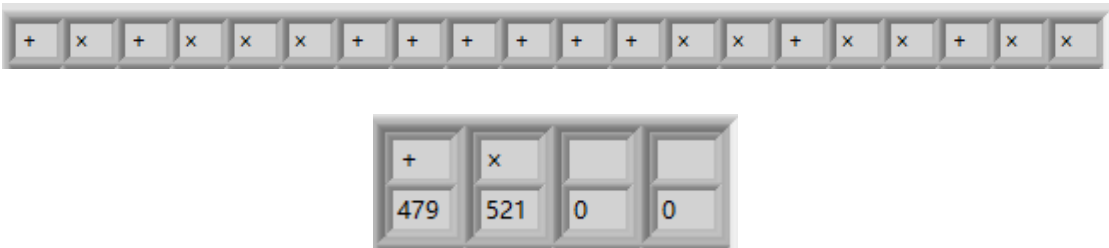


图 3. B 使用的随机检偏器序列 (仍只显示了前 20 个, 下同), 及相应数量分布

其中, $0^{\circ}\rightarrow$ 、 $90^{\circ}\uparrow$ 两个态, 在经过 x 型检偏器后, 会有相同的 50% 的概率塌缩为 $45^{\circ}\nearrow$ 或 $135^{\circ}\nwarrow$ 态; 同时, 其所对应的量子比特的值, 分别有 50% 的概率变得与之前不同或保留之前的值, 即出现 0 和 1 的几率为 1:1; 而在经过 + 型检偏器后, 量子态和量子比特, 都保持原值不变。

因此, 在无窃听的情况下, 即 A,B 间没有 C 存在的条件下, B 直接接收 A 发来的偏振态序列 (图 2 首行), 并用该组随机检偏器序列 (图 3), 进行测量后得到的偏振态序列及其相应的量子密钥, 如图 4 后两行所示:



图 4. 无窃听时, B 使用的随机检偏器相对 A 态的正误序列 & 测量所得的偏振态序列 及其相应的量子比特序列, 和三者的数量分布

此时, B 通过经典信道, 公布自己所用的检偏器序列 (图 3); 接着, A 检验 B 所公布的检偏器序列, 相对于自己制备并发送的态序列 (图 2 首行) 的正误情况, 并通过经典信道, 公布其中的正确部分或正确位置或正误序列 (图 4 首行)。

B 从经典信道中得到 A 公布的正误序列 (图 4 首行), 剔除其中选用错误的检偏器, 所对应的量子态和量子比特, 再次于经典信道中公布, 剔除后所剩下的

量子比特序列（如图 4 中即为 11001100000...）。

A 从经典信道中接收到 B 的第 2 次消息后，对比其之前所公布的位置上的比特序列（如图 2 中即为 11001100000...）—— 如果对比所得的误码率接近 0，或传输过程的本征误码率，则 A 再从经典信道中公布：没有窃听，挑选并确认使用该公有比特序列中特定位置的比特组成的量子密钥。

而若该误码率远高于预期，则 A 再第 2 次从经典信道中公布：存在窃听，并停止使用该序列，甚至停止使用该量子信道。

B 第 3 次从经典信道中收到后，按照 A 的意思做，完成 BB84 协议所规定的对称密钥分发过程。接着用对称密钥对密文按位做一次线性异或运算即可得明文。

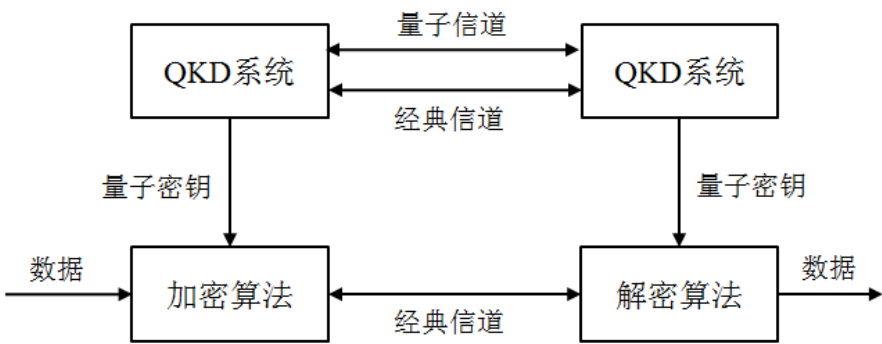


图 5. 基于 QKD 的量子保密通信系统的 2 种信道

可以仿真或计算出，无量子窃听时，B 接收到的比特序列的全局理论误码率为 25%，如下图 6 所示：



图 6. 无窃听时，B 比特序列相对于 A 比特序列的正误序列，及数量分布


安全性分析：对于 C 单从经典信道中窃听的情况，由于量子态不可克隆定理，窃听者 C 无法制备未知量子态及其序列的复制，因此即使从经典信道中 A 发送的消息内，得知了 B 检偏器的正误情况，C 也无法复原 B 测量后所得的量子态及其比特序列，因此 C 从经典信道中，窃听 B 检偏器的正误情况是没有意义的。

进而，C 从经典信道中窃听得到的任何信息，都是没有意义的：不能帮助 C 还原 A 和 B 的在通信过程的任何阶段的态序列和比特序列。

因此，对于理想的 BB84 协议过程，C 窃听经典信道没有用，而伪装信源或信宿在经典信道中阻碍、欺骗对方，或破坏经典信道的行为，最终会被双方发现。

因此，从信道的角度，C 只能选择窃听量子信道。

3.2 量子信道有窃听的 BB84 协议过程

量子信道在无窃听时，信号在量子信道中的流向为 $A \rightarrow B$ ；有窃听时，信号流向为 $A \rightarrow C \rightarrow B$ 。假设 C 也用比特数量个，即  1000 个检偏器来测量单光子序列的偏振态序列：

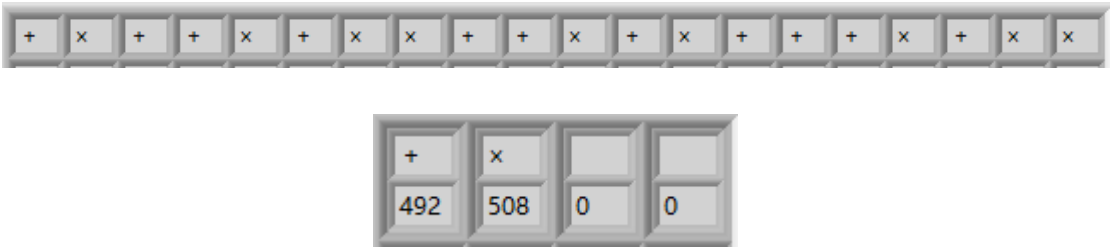


图 7. C 使用的随机检偏器序列，及数量分布

C 用如图 7 所示的检偏器序列测量获得的，且传向 B 的偏振态序列，如下图 8 的中间行所示；C 所得到的比特序列如下图 8 的末行所示：



图 8. C 使用的随机检偏器相对 A 态的正误序列 & 测量所得的偏振态序列及其相应的量子比特序列，和三者的数量分布

经过窃听者 C 后，B 接收到可能被 C 的检偏器改变过的偏振态序列（图 8 中间行），再用与图 3 相同的检偏器序列测量之，得到的偏振态序列，如下图 9 的中间行所示；对应的比特序列如下图 9 的末行所示：



图 9. 有窃听时，B 使用的随机检偏器相对 C 态的正误序列 & 测量所得的偏振态序列及其相应的量子比特序列，和三者的数量分布

可以从下图 10 中发现，经过窃听者 C 后，B 所得到的量子比特序列（图 10 末行），相对于 A 的比特序列（图 2 末行）的全局误码率，从原来的 25%，提高到了 37.5%。



图 10. 有窃听时，B 比特序列相对于 A 比特序列 & 无窃听时 B 比特序列的正误序列

接着，A,B 再在经典信道中对比，在 B 使用了正确的检偏器的位置上，所对应的 A,B 量子比特的一致情况。如下图 11 所示，双方会发现，挑选出的局部比特序列的误码率，从无窃听时的接近 0%，提升到有窃听时的 37.5% 左右。



图 11. 有窃听时，检偏器正确的位置上的 B 比特序列，相对于 A 比特序列的正误序列

因此，C 窃听量子信道的行为，也会被发现。

3.3 理论和应用上，QKD 传递随机对称密钥均无条件安全

因此，理想情况下的 BB84 协议，无论是从经典信道，还是从量子信道的角度，理论上都是无条件绝对安全的，其安全性的严格证明已被 Lo、Shor、Mayers 等人完成^{[3][4][5]}。

但在 BB84 的实际应用上，对非理想单光子的弱相干量子光源的光子数分离（photon number splitting attack，简称 PNS attack）的攻击、对探测器终端的瞬态致盲效率控制攻击、甚至高传输损耗，均有可能导致 BB84 协议失效。

针对上述两种攻击和高传输损耗对理论到实际的应用落地带来的挑战，国内外学者分别先后提出了诱骗态协议^[6]、测量器件无关的（MDI）^[7]量子密钥分发方案、量子中继等方案；前者在理论上预言非理想单光子源可拥有与理想单光子源等价的安全性，降低了相干性要求，并大幅延长了安全通信距离到百千米以上；中间者则从理论上彻底解决了探测器攻击问题，包括所有已知和未知的针对探测器的攻击；后者则采用分段纠缠分发与纠缠交换相结合来拓展通信距离。

总之，基于量子力学的 BB84 协议，则从理论上，完全满足香农定理的三个要求：密钥随机，长度不小于明文，一次一密，因此用量子密钥加密后的密文是不可破译的；而结合 BB84 协议+诱骗态协议+MDI 方法，则从实际上，让空间分离的用户共享无条件安全的对称密钥；再加上对称密钥生成方法简单、加密解密过程只需要按位操作，所以基于 BB84 协议的量子密钥分发的效率也很高。

因此，QKD 既实现了高速安全地分发密钥，极大地便利了 B 和 A；又由非数学而纯物理机制保证，在理论和应用层面的安全性上牢不可破，即无限增加了 C 的窃听成本、无限降低了 B 和 A 的损失。

3.4 量子密钥分发的 3 个缺点

3.4.1 缺点一：庞大用户群的多对保密通信成本高

由于 QKD 属于对称加密的私钥体系，则一个 A 端到多个 B 端的 QKD 过程，甚至现今时常出现的，多个 A 端到多个 B 端的，分布式网状加密通信网，会随着终端数目的增加而对整个系统的私钥管理和运营成本提出不小的挑战。

因此 QKD 的第一个缺点就是，只适合一对一、单点对单点的少对用户通信。这种缺点都存在于所有私钥即对称加密体系中。

而非对称公钥体系诸如基于 RSA 的公钥加密算法，尽管面临量子计算机的威胁，其在超大用户数量的密钥管理上，仍具有优势。

针对缺点一的解决办法：PQC 或 PQC+QKD

目前，针对该缺点的解决方法也不是没有。能抵御量子计算威胁的可信赖的信息安全机制主要有两种方式：一是以 QKD 为代表的量子保密通信；二是后量子加密 (PQC, post-quantum cryptography) 算法，比如格密码，已知的量子计算算法无法有效破解。

三是融合 QKD 与 PQC：2021 年 5 月 6 日，国盾量子、中国科大联合团队实现了“QKD+PQC”融合应用^[8]，实验验证了 PQC 技术在 QKD 网络设备认证中的应用，大幅提升了 QKD 认证过程的可操作性和高效性，将 QKD 的简便高效，复制到了多用户对场景中。

3.4.2 缺点二：专门针对穷举进行优化的量子计算

密码学的一个基本原则是，在设计算法时，你必须假设敌人已经知道了算法和密文，唯一不知道的是密钥。而量子计算不窃取密钥，在已知算法和密文的情况下，直接穷举，尝试暴力获取明文。

如果量子计算有专门针对穷举进行优化的算法，则由于并行计算以及量子比特的加持，在算力上远远超过经典计算机的量子计算，可能通过将算力集中于穷举所有密钥，利用相同的算法和密文，生成不同密钥解密后明文，再设计判断机制筛选出可能有意义的明文，再进一步过滤出正确的明文。

因此 QKD 及所有经典或非经典的保密机制都会受到：不对密钥求解、窃取，而对密钥进行穷举的，量子计算的威胁；除非密钥与明文均设定得很长。

3.4.3 缺点三：无法高保真地传递信息

正因为是物理机制保证，而非数学难度保证，QKD 才具有绝对的安全性。而同样正是由于物理机制的缘故，QKD 过程中，哪怕没有窃听者 C，即对于发送的量子态序列，只有 B 端的一次测量（以得到比特序列），而不是加上窃听者 C 后的多次测量，则每次测量也都会改变一半的量子态的状态，以至于经测量后只有一半的量子态不发生改变。

而经测量后塌缩的那一半的量子态，又分别有二分之一的几率，塌缩到 2 个

取值不同的量子比特所对应的新量子态上。因此哪怕 A 传递的量子态，及其相应的量子比特，不是随机的，则 B 在测量后，必然随机改变一半的量子态，同时随机改变 1/4 的量子比特值。

因此在 BB84 协议的 QKD 过程中，若 B 进行测量一次，则 B 获得的信息，会随机改变 25%；而若 B 不进行测量，又无法获得信息。

所以即使 A 不传递密钥，不传递随机量子态序列，而是通过诸如先后选用有序的起偏器序列，制备和传递有序量子态序列给 B，B 也没法测量后保持信息的完整性和确定性。

3.5 量子密钥分发中，信宿 B 的测量，总可能改变信息

哪怕没有窃听者 C，以 QKD 为代表的量子通信，也没法传递高保真的信息，以至于 QKD 只能传随机比特序列，而不传信息。

从信息论的角度，B 获得 A 传递的消息后，若 A 消息中的某些成分，帮助接收者 B 消除了其所不知道的领域中的某些不确定性，则 B 获得了信息。

B 从 A 的消息中，获得的信息量的大小，和该消息对 B 的既有认知的不确定性消除的程度有关。A 的消息帮助 B 消除了 B 认知上的不确定性程度^①，即为 B 获得的信息量。

对 QKD 稍作修改，使 A 传递一条消息（一则有序的比特序列），而非传递一则随机比特序列；对于经典信道，不考虑窃听、拦截或损耗等带来的误码，B 会收到与 A 发出时相同的消息，只要消息不是完全无序的符号序列，B 会从中获得一定的信息量，比如解码后为“明天将要下雨”。

但对于同样一则消息，若 B 从 QKD 的量子信道，测量得到 A 发送的这则消息，则解码后可能为“后天不要下雪”。

因此即使传递的信息量可能没变，甚至还可能变多了，由于 BB84 协议本征存在的每次测量所带来的 25% 的误码率，最终 B 收到的信息，与 A 发出的信息，可能会完全不同。

虽然可能可以通过增加冗余度，以及一定强度的恢复编码、纠错编码(1995)，来减少信息量的丢失，和信息准确度的下降，但除开其他干扰以外，仅测量带来的，至少 25% 的理论误码率，对于通信双方都是无法接受的，增加冗余度和恢复编码，也是无法保证一定能 work 的。

① 不确定的对象变为确定，导致 B 认知中，确定的对象更多，不确定的对象更少。

因此，由于以 BB84 协议为代表的 QKD 过程，总涉及信宿 B 的测量，而无法避免因测量而导致的对信息的改变的可能，因此总无法实现 100% 传输准确的信息，因此理论上不能用于一般意义上的通讯^①，而只能用于密钥分发，即传递随机数序列。

4 量子隐形传态

4.1 量子信道无窃听的 QT 过程

除了量子密钥分发，量子通信技术的另一个重要分支，是仍由 Bennett 和 Brassard，于 1993 年提出的量子隐形传态^[9]。

在不违背量子不可克隆定理的前提下，量子隐形传态可以通过处于最大纠缠态（4 个贝尔态/基^②之一）的粒子 B 与粒子 C，以之为媒介，转移/传递而非克隆一个未知量子态的粒子 A 的未知量子态 $|a\rangle$ ，到粒子 C 上，使得 $|c\rangle = |a\rangle$ ；同时，粒子 A 的量子态 $|a\rangle$ ，塌缩为另一未知量子态（图 12）。

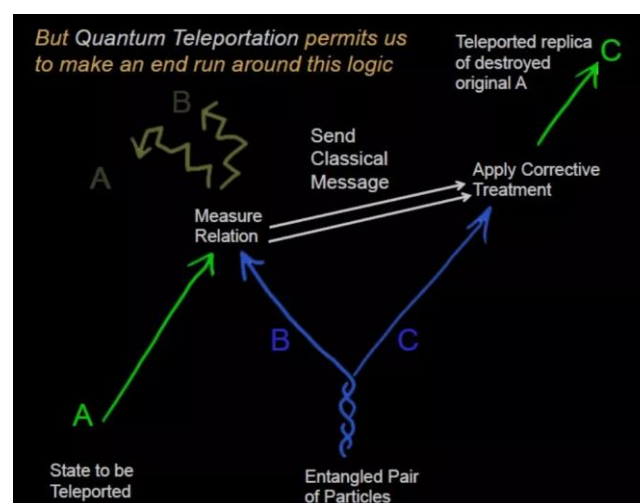


图 12. 量子密码学——量子纠缠 | Charles Bennett（中）^[10]

量子隐形传态也用到了经典信道与量子信道两种信道，其操作过程如下：

制备一对在观测前处于 $|b\rangle, |c\rangle$ 所构成的 4 个贝尔态之一的粒子 B, C 所构成的系统，并分别发送给通信双方 Alice, Bob；同时，Alice 有个粒子 A，处在待复制的未知态 $|a\rangle$ 。

- ① 如果利用上经典信道，BB84 仍可能可以实现通讯：无窃听情况下，A 对比 B 所使用的检偏器后，让 A 与 B 均保留相同位置的比特，然后 A 另拿出其所想传递的消息的 2 进制格式，思考 or 推算、制作：什么样的函数 f ，能使得 f （公有的 50% 的比特）= 所传递的消息，再把这个函数 f 发送给 B，B 将该函数作用于 A, B 所公有的 50% 的比特，即可还原出 A 想传递的消息。
- ② 四个贝尔基构成：两个量子，每个量子两态的态空间的一组完备基矢，且是系统的四个最大纠缠态。

接着, Alice 用 $|a\rangle, |b\rangle$ 所构成的 4 个贝尔基, 联合测量 A,B 所构成的复合系统, 使其塌缩到 $|a\rangle, |b\rangle$ 构成的 4 个贝尔态之一; 同时, $|a\rangle, |b\rangle$ 均塌缩为某未知量子态, 但 A,B 整体的量子态确定, 为 $|a\rangle, |b\rangle$ 构成的 4 个贝尔态之一。

同时, 由于 B,C 也一直处于制备出的 $|b\rangle, |c\rangle$ 构成的 4 个贝尔态之一, 则当 $|b\rangle$ 均塌缩为某未知量子态时, $|c\rangle$ 也塌缩为某未知量子态, 但 B,C 整体的量子态确定, 仍为之前制备出的 $|b\rangle, |c\rangle$ 构成的 4 个贝尔态之一。

Alice 把对 A,B 系统的联合测量结果^①, 通过经典信道告诉接收者 Bob; Bob 根据 A,B 所构成的复合系统具体塌缩到了 $|a\rangle, |b\rangle$ 所构成的哪个贝尔基上, 对其手上已经塌缩到某未知态 $|c\rangle$ 的粒子 C 的态 $|c\rangle$, 进行相应的酉变换, 就可得到/知道, 粒子 A 在与 B 一起被联合测量前, 未塌缩之前初始未知量子态 $|a\rangle$ 。

由于要经过经典信道传递联合测量结果, 且根据该结果操作一次酉变换, Bob 才能“剪切-粘贴”^②出 $|a\rangle$ 态, 所以 QT 传态的速度, 仍受限于光速。

4.2 量子隐形传态中, 信源 A 的联合测量, 总可能改变所传的态

量子隐形传态的最大优点, 就在于其名称本身: 可以通过该手段, 实现态的远程转移, 且不需要知道, 以至于不需要去单独测量所转移的态对应的粒子的态。但问题恰恰也出在这里: 不仅不需要知道, 也不能够、没法知道想要转移的态。以至于只能远程转移未知的、而不能远程转移已知的, 量子态 (序列)。

以至于如果将 QT 视为通信的话, 信宿 B 接收到的量子态序列, 确实是信源 A 发送出的量子态序列, 但 A 并不知道自己发送的是什么, 也没法知道。因此, A 不应该被看作信源, 而只能被看作一个中继: 中继就可以不知道消息内容具体是什么, 但同时正确地传递消息内容给下一个对象。

5 结语

量子通信技术中, 最大的两个分支, 量子密钥分发和量子隐形传态, 前者只能传递信源 A 已知的无序比特, 后者只能转移信源 A 未知的有序比特, 二者都不能传信源 A 已知的有序比特, 导致信源 A 无法传递信息给 B。

因此可以说, 量子通信, 没有传信息。或者直接就“没有通信”, 更准确的说是: 在量子信道中没有进行任何通信, 通信过程都发生在经典信道内。

所以, “量子通信”还能叫“通信”, 主要是因为, 用了量子的手段, 即通过

① 即测量所导致的, A,B 所构成的复合系统, 塌缩到的 $|a\rangle, |b\rangle$ 所构成的 4 个贝尔基之一

② 而非“复制-粘贴”

量子信道中进行的态或比特序列的传递，从目的和结果上，为“经典信道中的通信”这种通常意义上（人与人之间）的“通信”、或“量子密钥分发的态序列转移”、“量子计算机间的通信”这两种特殊意义上（非人类间）的“通信”，服务的缘故：比如 QKD 主要用于保证经典信道中的通信，所用到的对称密钥的绝对安全；而 QT 则作为量子中继，用于态转移，以延长量子信道中的密钥分发距离，和实现量子计算机间的通讯，并延长其通讯距离。

以 BB84 为代表的 QKD，与 QT 一起，作为量子通信的两大基石，已经被证明无法通过量子信道传递信息，因为测量将导致态随机塌缩，对应比特可能改变；若不测量，连一个比特都无法得到，更别谈信息即有序比特序列了。1992 年，Bennett 提出了通过量子信道传送经典信息的可能性，但其实就是 1993 年 QT 的前身，主要用于的是量子计算机间的态转移，即计算机间的通信，而非人与人间的通信。因此，量子通信是否能直接通过量子信道通信，还待进一步考察。

6 参考文献

-
- [1] WOOTTERS W K, ZUREK W H. A Single Quantum Cannot Be Cloned[J]. *Nature*, 1982, 299(5886): 802–803. DOI:10.1038/299802a0.
 - [2] BENNETT C H, BRASSARD G. Quantum Cryptography: Public Key Distribution and Coin Tossing[J]. *Theoretical Computer Science*, 2014, 560: 7–11. DOI:10.1016/j.tcs.2014.05.025.
 - [3] LO H-K, CHAU H F. Unconditional Security Of Quantum Key Distribution Over Arbitrarily Long Distances[J]. *Science*, 1999, 283(5410): 2050–2056. DOI:10.1126/science.283.5410.2050.
 - [4] SHOR P W, PRESKILL J. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol[J]. *Physical Review Letters*, 2000, 85(2): 441–444. DOI:10.1103/PhysRevLett.85.441.
 - [5] MAYERS D. Unconditional Security in Quantum Cryptography[J]. *Journal of the ACM*, 2001, 48(3): 351–406. DOI:10.1145/382780.382781.
 - [6] WANG X-B. Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography[J]. *Physical Review Letters*, 2005, 94(23): 230503. DOI:10.1103/PhysRevLett.94.230503.
 - [7] LO H-K, CURTY M, QI B. Measurement-Device-Independent Quantum Key Distribution[J]. *Physical Review Letters*, 2012, 108(13): 130503. DOI:10.1103/PhysRevLett.108.130503.
 - [8] WANG L-J, ZHANG K-Y, WANG J-Y, et al. Experimental Authentication of Quantum Key Distribution with Post-Quantum Cryptography[J]. *Npj Quantum Information*, 2021, 7(1): 67. DOI:10.1038/s41534-021-00400-7.
 - [9] BENNETT C H, BRASSARD G, CRÉPEAU C, et al. Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels[J]. *Physical Review Letters*, 1993, 70(13): 1895–1899. DOI:10.1103/PhysRevLett.70.1895.
 - [10] 墨子沙龙. 量子密码学——量子纠缠 | Charles Bennett（中）[EB](2018–11–22).