量子通信
——量子信息时代到来的前奏

张文卓

（丹麦奥胡斯大学物理与天文系　8000）

1876 年加拿大科学家贝尔发明了电话，使得人类可以利用导体中的电流来传输信息。随后的几十年内电流成为了人类最主要的“有线”通信手段。直到 1966 年高锟发明了光纤，光纤通信成为了电流以外另一个人类主要的有线通信手段。

1865 年，英国著名物理学家麦克斯韦整合了前人的电磁学的定律而提出了名垂史册的麦克斯韦方程组，并据此方程组预言了电磁波的存在。1887 年，德国物理学家赫兹在实验上发现了电磁波。随后的 10 年里，意大利人马可尼，俄罗斯人波波夫，塞尔维亚裔的美国人特斯拉各自实现了利用电磁波的通信。马可尼的团队更将电磁波勇敢地发射向天空，在当时还不知道大气层存在能反射电磁波的电离层的情况下，实现了横跨大西洋的电磁波通信。于是电磁波成为了人类最主要的“无线”通信手段。

1947 年，美国物理学家肖克莱，巴丁和布拉顿发明了晶体管，从而人类可以使用微小的半导体来处理信息。10 年后，德州仪器公司的基尔比和 Intel 公司的创始人诺伊斯在此基础上制造出了集成电路，成为当代各种计算机和电子设备的核心。晶体管和集成电路标志着人类全面步入了信息时代。肖克莱和诺伊斯也顺理成章成为了“硅谷之父”，使我们今天能用上各种各样的计算机和数码产品。

以上就是人类步入信息时代两个最重要的步伐，即“信息传输（通信）”和“信息处理（计算）”，中间相隔约 50 年。我们常常用“数码革命”，“数字化革命”，甚至“信息革命”来直接形容后者这次伟大的变革，但我们不能也不应该忽略前者这次同样伟大的变革。如果后者是高潮，前者就是前奏。后者是主菜，前者就是开胃菜。它们相得益彰，造就了我们今天的互联网：信息处理的设备作为终端，信息传输建立网络，二者缺一不可。

但是无论如何，以上两次变革都是“经典信息”的革命，即信息传输和信息处理符合的都是经典物理学定律。即使我们必须用量子力学才能理解半导体的本质和工作原理，我们用半导体器件所处理的还是经典的二进制信息。同样，无论我们用有线的光纤，导线，还是无线的手机信号，wifi，我们传输的也都是经典信息。

17 ～ 19 世纪经典物理学的建立为我们带来了 20 世纪的经典信息革命。同样 20 世纪量子物理学的建立会给我们带来 21 世纪的“量子信息”革命。因为信息处理的技术难度往往高于信息传输的难度，于是经典信息革命就以经典通信为前奏，以经典信息处理为高潮。同理，量子信息的革命也必然会以“量子通信”为前奏，以“量子计算”为高潮，从而使人类全面进入量子信息时代。如今，这个前奏已经悄然响起。

1. 量子密码分配协议

量子通信按照发展历史，可以分为两个阶段：前一个阶段是利用量子通信方案来传输经典信息——以经典比特为单位的信息。后一个阶段是直接传输量子信息——以量子比特为单位的信息。经典比特即 0 或 1，而量子比特（qubit）可以处于 0 和 1 的量子叠加态（superposition），如 $|\psi\rangle = a|0\rangle + b|1\rangle$ 就是一个量子比特，其中 $a^2+b^2=1$。

物理学家们当然最先提出了用量子通信手段传输经典比特的模式，即用来传输和分配密码的量子通信协议。其中比较著名的是由查尔斯 • 贝内特（Charles Bennett）和吉勒斯 • 布拉萨德（Gilles Brassard）在 1984 年提出的 BB84 协议：

该协议利用光子的偏振态来传输信息。假设量子力学三位主要创始人海森伯，薛定谔和狄拉克各自扮演信息的发送者，接收者和截获者的角色。因为光子的偏振有两个相互线性独立的自由度（即偏振态相互垂直），所以他们可以简单选取“横竖基”，即“+”，和“对角基”，即“×”，作为测量光子偏振的基矢。在“横竖基”中，偏振方向“↑”代表 0，偏振方向“→”代表 1；“对角基”中，偏振方向“↗”代表 0，偏振方向“↘”代表 1。

这样选择测量基的好处就是：“+”和“×”不是线性独立的，相互不正交。于是若选择“+”来测量偏振态“↗”或“↘”时，会得到 50% 的几率为“→”，50% 的几率为“↑”。同理，选择“×”来测量“→”或“↑”时，会得到 50% 的几率为“↗”，50% 的几率为“↘”。

在传输一组二进制信息时，海森伯对每个比特随机选一个基矢，即“+”或者“×”，然后把每个比特（在各自被选的基矢下）对应的偏振光子发送给薛定谔。比如传输一个比特 0，选择的基矢为 +，则对应的光子的偏振态为↑。光子可以通过不破坏偏振态的（保偏）光纤或者自由空间来传输，称为“量子信道”。

薛定谔这边也对接收到的每个比特随机选择“+”或者“×”来测量。在测量出所有的 0 和 1 后，薛定谔和海森伯之间要通过经典信道（电话，短信，QQ 等）建立联系，互相分享各自用过的基矢，然后保留相同的基矢，舍弃不同的基矢。于是保留下来的基矢所对应的比特，就是他们之间通过量子通信传输的密码，见表 1。

通过表 1 我们可以看出，只有当发送方的海森伯和接收方的薛定谔所选择的基矢相同的时候，传输比特才能被保留下来用作密码。如果存在信息截获者狄拉克，那么狄拉克也同样要随机选取“+”或者“×”来测量海森伯发送的比特。比如海森伯选取基矢为“+”，然后发送“→”来代表 1。如果狄拉克选取的基矢也为“+”，他的截获就不会被察觉。但狄拉克是随机选取基矢，那么他就有 50% 的概率选择“×”，于是量子力学的测量特性使光子的偏振就变为 50% 的概率↗和 50% 的概率↘。

作为接收方的薛定谔如果选取了和海森伯同样的基矢“+”，则会把这个比特当做密码。但是薛定谔测量的是经过狄拉克截获的光子的偏振，测量结果是 50% 的概率↑和 50% 的概率→。于是测量这个比特薛定谔跟海森伯的结果不同的概率为 50%×50%=25%。

因此想知道是否存在截获者狄拉克，海森伯和薛定谔只需要拿出一小部分密码来对照。如果发现互相有 25% 的不同，那么就可以断定信息被截获了。同理，如果信息未被截获，那么二者密码的相同率是 100%。于是 BB84 协议可以有效发现窃听，从而关闭通信，或重新分配密码。

随后查尔斯 • 贝内特又在 1992 年提出了作为 BB84 协议简化版的 B92 协议。有兴趣的读者可结合 BB84 协议自行查阅。量子密码分配协议使得通信双方可以生成一串绝对保密的经典二进制密码，用该密码给任何信息加密都会使该信息无法被解密。量子密码协议可以说让人类第一次认识到了量子通信的威力。与此同时，物理学家发现如果传输的是量子比特而不是经典比特，那么量子通信将有根本上的保密性。

2. 量子不可克隆定理

如果来直接传输量子态，如量子比特，那么量子通信就有了它最重要的优势：信息本身的绝对安全性。这个绝对安全性来自于量子“不可克隆定理”。即无法克隆任意的量子态。

量子不可克隆定理可简要证明如下：

“|A〉态和 |B〉态是我们想要克隆的任意量子态，|C〉是我们用做克隆的基矢，U 是克隆算符。量子克隆过程就是 U|A〉|C〉=|A〉|A〉，U|B〉|C〉

表 1　BB84 通信协议

发送的密码比特	0	1	0	0	1	1	0	1
海森伯选择的基矢	+	+	×	×	+	+	×	×
发送的光子偏振	↑	→	↗	↗	→	→	↗	↘
薛定谔选择的基矢	×	+	×	+	×	+	+	×
接收到的光子偏振	↗或↘	→	↗	↑或→	↗或↘	→	↑或→	↘
两者共有的密码		1	0			1		1

=|B〉|B〉。于是能得到等式〈B|A〉=〈C|〈B|U*U|A〉|C〉=〈B|〈B|A〉|A〉。该等式要求|A〉=|B〉或者〈B|A〉=0，即要求|A〉态和|B〉态完全相同，或者正交。这和|A〉和|B〉都是任意态的假设矛盾，因此无法克隆任意量子态。”

窃听者在窃听经典信息的时候，等于复制了这份经典信息，使信息的原本接收者和窃听者各获得一份。但是在量子信息传输中，量子比特由量子态携带。因为无法克隆任意量子态，于是在窃听者窃听拦截量子通信的时候，就会销毁他所截获到的这个量子态，即销毁它所携带的量子比特，于是无论是接收者还是窃听者都无法再获得这个信息。通信双方会轻易察觉信息的丢失，因此量子通信的具有绝对的保密性。

细心的读者可能会发现如果想要克隆一个单独的量子态，或者几个相互正交的态，原理上还是可行的。但是这样的态无法提供足够的量子比特，因此不具有任何信息上的意义，也不会用到量子通信中。

量子不可克隆定理使得我们传输量子比特的时候，不用再建立上一节那样的量子密码。但相比于传输经典比特，传输量子比特的难度要大很多。接下来将要就介绍如何利用量子纠缠态来传输量子比特。

3. 量子纠缠态

量子信息学的核心除了量子比特之外，就是量子纠缠态。它是量子力学一种很基本但也很特殊的态，从经典物理学角度你无法理解它的神奇。无论是量子通信还是量子计算，量子纠缠态都会发挥着举足轻重的作用。

量子纠缠态最早得到重视，正是始于爱因斯坦对量子力学的批评。量子力学在20世纪20年代诞生以后，爱因斯坦认为量子力学是不完备的，因为不符合自己基于相对论而提出的“局域实在原理”(local realism)：（1）物质实体独立于任何测量而存在。（2）物质之间的任何影响都是时空局域的，即不能超过光速。

1935年，爱因斯坦和波多尔斯基（Boris Podolsky），罗森（Nathan Rosen）一同提出了著名的EPR（即Einstein–Podolsky–Rosen）佯谬，用来论证量子力学的不完备性：根据海森伯的不确定关系，无法同时测量一个粒子的位置和动量的精确值。于是EPR佯谬设想两个相互作用的粒子A和B，总动量确定（即一个EPR对）。当两个粒子分隔相距很远时，测量A的位置可得到精确值；同时测量B的动量也可得到精确值，从而计算出A的动量的精确值，这就同时精确测量了A的位置和动量，违反了不确定关系。

但现实世界不是这样。因为粒子A和B处于“纠缠态”，即共同组成一个纯的量子态，当你精确测量A的位置时，影响到了B，使你无法精确测量B的动量，反之亦然。因为两个粒子已经相距很远并且无相互作用，于是EPR文章中认为量子纠缠暗示了：（1）要么这两个粒子存在某种超过光速的非局域（non-local）相互作用而违背相对论。（2）要么量子力学的描述是不完备的，存在未知的“隐变量”来抵消这种非局域相互作用，使A和B依然符合局域实在原理。EPR的论文倾向于后者，随后经过美国物理学家波姆（David Bohm）的发展而成为“局域隐变量理论”。1964年爱尔兰物理学家贝尔提出了“贝尔不等式”，用来判定局域隐变量理论是否存在。后来约翰·克劳泽（John Clauser），斯图尔特·弗里德曼（Stuart Freedman）和阿兰·阿斯派克（Alain Aspect）等人的一系列实验证实了量子纠缠系统违反贝尔不等式，从而否定了局域隐变量的存在，即证明量子纠缠是非局域的。

让我们了解一下量子纠缠。公式（1）就是一个量子纠缠态的例子：假设两个粒子A和B相互纠缠，每个粒子只有|0〉和|1〉两个量子态（即携带一个量子比特，可处于|0〉和|1〉任意叠加态）。无论两个粒子相隔多远，当测量得到A的状态为|0〉时，测量|B〉的状态必然为1，总的纠缠态塌缩为|01〉。同理，当测量A的状态为|1〉时，B的状态必然为|0〉，总的纠缠态塌缩为|10〉。也就是说，A和B共享公式（1）所代表的一个单一波函数，波函数塌缩到|01〉和|10〉的概率各为1/2。

$$|\psi\rangle=\frac{1}{\sqrt{2}}\left(|01\rangle+|10\rangle\right) \qquad (1)$$

图1用薛定谔的两只猫代表两个粒子，形象表述了纠缠态的概念：薛定谔把甲乙两只猫扔到一个“纠

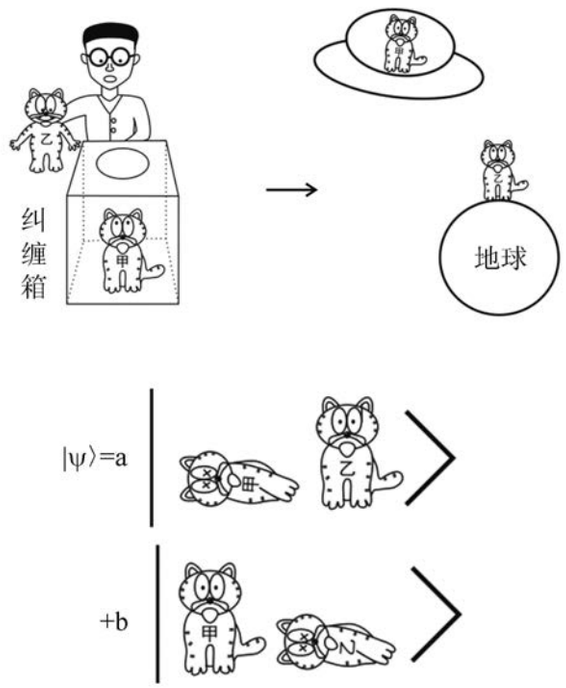

图 1　薛定谔的纠缠猫，$a^2+b^2=1$

缠箱”里，使之相互发生纠缠。后来，甲猫被外星人劫持到了外太空，乙猫还留在薛定谔家里。当薛定谔再用乙猫做实验时，当他测量到乙猫的结果为“活”，那么甲猫在外太空的状态就必然为“死”；同理，当薛定谔测量到乙猫的状态为“死”，那么甲猫在外太空的状态就必然为“活”。即测量操作只能使甲乙两只猫的纠缠态塌缩到“甲死乙活”，或者“甲活乙死”两个态上。

因为量子纠缠是非局域的，即两个纠缠的粒子无论相距多远，测量其中一个的信息（态）必然能同时获得到另一个粒子的信息，这个“信息”的获取是不受光速限制的。于是物理学家自然想到了是否能把这种跨越空间的纠缠态用来进行信息传输？因此，基于量子纠缠态的量子通信便应运而生。这种利用量子纠缠态的量子通信就是“量子隐形传态”（quantum teleportation）。

4. 量子隐形传态

虽然借用了科幻小说中隐形传态（teleportation）这个词，但量子隐形传态实际上和科幻中的隐形传态关系并不大。它是通过跨越空间的量子纠缠（比如EPR 对）来实现对量子比特的传输，即量子通信。

量子隐形传态的过程（即传输协议）一般分如下几步：

（1）制备一个 EPR 对。将其中一个粒子发射到 A 点，另一个发送至 B 点。两个粒子之间的纠缠态为如下四个“贝尔基”（Bell states）之一：

$$|\phi+\rangle=\frac{1}{\sqrt{2}}\left(|0_A0_B\rangle+|1_A1_B\rangle\right)$$

$$|\phi-\rangle=\frac{1}{\sqrt{2}}\left(|0_A0_B\rangle-|1_A1_B\rangle\right)$$

$$|\varphi+\rangle=\frac{1}{\sqrt{2}}\left(|0_A1_B\rangle+|1_A0_B\rangle\right)$$

$$|\varphi-\rangle=\frac{1}{\sqrt{2}}\left(|0_A1_B\rangle-|1_A0_B\rangle\right)$$

（2）在 A 点另一个粒子 C 携带想要传输的量子比特 $|\psi\rangle=a|0_C\rangle+b|1_C\rangle$。假设 A 点和 B 点的 EPR 对处于的纠缠态为 $|\phi+\rangle$，则 EPR 对和粒子 C 形成的总的态，由如下四个态等概率叠加而成：

$$\frac{1}{2}\left(|0_A0_C\rangle+|1_A1_C\rangle\right)\left(a|0_B\rangle+b|1_B\rangle\right)$$

$$\frac{1}{2}\left(|0_A0_C\rangle-|1_A1_C\rangle\right)\left(a|0_B\rangle-b|1_B\rangle\right)$$

$$\frac{1}{2}\left(|0_A1_C\rangle+|1_A0_C\rangle\right)\left(a|0_B\rangle+b|1_B\rangle\right)$$

$$\frac{1}{2}\left(|0_A1_C\rangle-|1_A0_C\rangle\right)\left(a|0_B\rangle-b|1_B\rangle\right)$$

薛定谔在 A 点用某个贝尔基同时测量 EPR 粒子和粒子 C，得到测量结果为以上四个态之一。这个测量使得 EPR 对的纠缠解除，而 A 点的 EPR 粒子和粒子 C 则纠缠到了一起。

（3）薛定谔利用经典信道（就是经典通信方式，如电话或短信等）通知 B 点的海森伯自己的测量结果。

（4）B 点的海森伯收到 A 点的薛定谔的测量结果后，就知道了 B 点剩下的 EPR 粒子处于哪个态。如果薛定谔的测量结果是四个态里的 1 或 3，则海森伯不需要任何操作，A 点到 B 点的隐形传态实现。如果测量结果是 2 或 4，则海森伯需要对 B 点的 EPR 粒子做一个幺正变换，将其变为 $a|0_B\rangle+b|1_B\rangle$，于是隐形传态实现。

以上就是通过量子纠缠实现量子隐形传态的方法，即通过量子纠缠把一个量子比特无损地从一个地点传到另一个地点。这也是量子通信目前最主要的方式。需要注意的是，由于步骤 3 是经典信息传输而且不可忽略，因此它限制了整个量子隐形传态的速度，使得量子隐形传态的信息传输速度无法超过光速。

因为量子计算需要直接处理量子比特，于是像“量子隐形传态”这种直接的量子比特传输会使得量子通信和量子计算可以形成一个纯粹的量子信息传输和处理系统，即纯粹的量子互联网。这也将是未来量子信息时代最显著的标志。

5. 量子通信的现状及未来

正如文章开头讲到，经典信息技术（IT）主要由通信和计算两大部分组成，时间上也有着先实现大规模通信，后实现大规模计算的两步走关系，最后形成了我们今天的互联网。而量子信息学正沿着这条道路在前进。量子通信技术已经日渐成熟，正在慢慢进入应用领域。而量子计算的突破才刚刚开始，还要经过很多年的努力才能大规模应用。我们现在就像大约一百年前，电磁波通信刚刚实现，电子计算机还没有出现的时候。如今小范围的量子密码分配已经走出实验室并得到应用，量子隐形传态技术也早已在实验室实现。但是量子计算方面，还仅仅在实验室实现了十几个量子比特的计算，真正的量子计算机还没有出现。

量子通信目前已经进入应用领域的，是本文最先提到的量子密码分配方案。它可以由人类已应用多年的激光器，光纤，以及偏振分光棱镜等光学器件实现。目前国际上投入应用的量子密码分配网络有位于美国波士顿的 DAPRA 量子网络（DAPRA Quantum Network），由哈佛大学和波士顿大学联合几家公司在 2004 年建成；同年，瑞士的 ID Quantique 公司已经开始将量子密码分配网络投入商业化；第一个量子密码分配的计算机网络位于奥地利维也纳的 SECOQC，由量子信息技术世界顶尖的奥地利科学院量子光学与量子信息研究所（IQOQI）和维也纳大学在 2008 年建成。中国这方面的产业化也已经走入世界前列。中国科学技术大学的团队在合肥于 2012 年建立了中国第一个量子密码分配的安全网络。

如我们前文提到，量子密码分配毕竟还是用量子通信技术传输经典信息。而利用量子纠缠态的量子通信才是真正在传输量子比特。这里不得不提到中国科学技术大学潘建伟院士领导的团队。该团队在世界上首次实现了：量子隐形传态，量子纠缠态交换，自由空间的量子隐形传态，三光子、四光子、五光子和六光子纠缠，使中国在量子通信研究的竞争中超越奥地利，成为如今全世界的领跑者。

量子隐形传态在 2012 年已经实现了 143 km 的记录，下一步将是建立地面和卫星之间的传输。毫无疑问量子隐形传态将成为下一个投入应用的量子通信技术，而且直接传输量子比特的优势，会使它和量子计算机能一起构建起量子互联网，即量子信息时代的互联网。

多年以前我在选修《量子信息》研究生课的时候，任课老师曾以这样一句话作为整个课程的结尾：“昨天的梦想，是今天的希望，也可能是明天的现实。”如今，我们看到了量子通信技术正一步一步从实验室走向应用和商业化。我们正处于经典信息时代和量子信息时代的转换过程中，成为历史的见证者。也许不久的将来，量子通信就会像今天的无线通信技术一样，进入到我们生活的每个角落。在那之后，随之而来的将是以量子计算机为标志的整个量子信息时代。