从量子纠缠到量子信息与量子通信：早期发展简介

谢柏松 北京师范大学

当今物理学的基础在应用方面重大发展的蓬勃潮流中，量子通信、量子离物传态以及量子计算乃至量子计算机技术的研究与实现无疑是弄潮者的先锋。

2019 年，奥地利维也纳大学的 Anton Zeilinger 教授荣获 2018/2019 年度墨子量子奖（量子通信领域实验类）。获奖理由是他在多光子纠缠干涉度量及自由空间量子传输方面的开创性实验，使实现安全的广域量子通信成为可能。无独有偶，2020 年，中国科学技术大学潘建伟教授荣获 2020 年度的德国蔡司研究奖（ZEISS Research Award）。获奖理由是他在量子通信方面的先驱性研究使得安全使用的远距离量子密码技术成为可能；同时他在多光子纠缠等方面的研究也为展示量子计算的优越性奠定了重要基础。

鉴于该研究领域的广泛性和高度的专业性，本文不打算做详细的介绍，而是集中在其早期发展的历史梳理，并对其重要的概念性由来和理论演变，例如EPR佯谬、Bell不等式、量子纠缠与量子信息、量子密码、量子通信与量子传输等做些简单的介绍。原则上所介绍的内容限于20世纪的研究成果。

故事要从上个世纪相对论和量子力学创始人爱因斯坦和玻尔这两大巨头对量子力学的波函数描述是否完备针锋相对的激烈争论说起。

EPR佯谬与Bell不等式

1935 年，爱因斯坦、波多尔斯基和罗森在美国著名期刊《物理评论》上发表了一篇题为“Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?”（《物理实在的量子力学描述能否被认为是完备的？》）的论文[1]，这个后来被广泛称之为 EPR 佯谬或 EPR 悖论的工作，开启了有关量子纠缠和量子非局域关联方面的研究兴趣

和热情，由于这篇文章先验地认为存在局域性的物理实在，对两个被分离得很远的粒子（可以当作是类空间隔，也就是说在光锥之外），自然地假设了其局域性有效的 EPR 建议：“既然在测量的时候这两个系统不再相互作用，那么不管你对第一个系统做过什么，都不应该对第二个系统的物理实在性有任何的改变”。EPR 在论文中提出了两个互为依赖的描述：要么（1）量子力学波函数对实在的描述是不完备的，要么（2）对于共轭的两个非对易物理量（例如位置和动量），这两个物理量不能有同时的实在性。EPR 论文的论证否定了（2），由此只能是（1），即 EPR 得出量子力学波函数不提供物理实在的完备性描述，简言之：量子力学是不完备的。

具体说来，可以这样设想EPR的思想：考察一个系统，它由两个子系统A和B组成，其中A和B仅在一个有限时间内发生相互作用。假定在它们发生相互作用以前，波函数已经给定，薛定谔方程会给出作用发生后的波函数。那么从整个系统的波函数可以得到B的物理量有且只有一个波函数完备描述的实在性。现在由测量尽可能完备地确定子系统A的物理状态，例如动量或者位置，再考虑子系统B，EPR巧妙地证明了或者由A的动量算符给出B的动量P存在的实在性，又或者由A的位置算符给出B的位置Q存在的实在性。但显然这两个实在性的事实（即不依赖于A而只应该在B中独立存在的同时实在性），另一个事实是在整体波函数下它又由A的测量下的单一实在性所决定，上述这两个事实互相抵触，因此这一矛盾性使得爱因斯坦得出EPR悖论：量子力学的波函数描述是不完备的。

但随即这一 EPR 思想实验在同一年遭到了玻尔（Bohr）的有力反驳[2]，连文章的标题都一模一样“Can Quantum-Mechanical Description of Physical Reality be Considered Complete' ?”玻尔指出 EPR 论文包含了关于物理实在的一个本质上的模糊性，特别是当它应用于量子现象时，在这方面，玻尔提出了一种被称为“互补性”的观点来解释物理现象的量子力学描述，并证明在它的范围内，似乎满足了对完备性的所有合理要求。关于量子力学是否完备的争论就此在两大巨头之间展开，并持续了很久。虽然如此，激烈的争论似乎并没有影响到他们的友谊（见图 1）。

图1 相对论和量子力学创始人爱因斯坦（左）和玻尔（右）（图片来自百度百科）

从EPR发表的论文中不难看出，EPR的论证建立在两个重要的观点上[3]，一是局域或叫定域因

果性（local causality）；二是物理实在性（physical reality）。由此EPR的核心思想就是所谓的定域实在论：距离遥远的也就是类空间隔的两个系统具有彼此相互独立的物理实在性。

EPR原始论文读起来多少有点绕，1951年Bohm（玻姆）建议了一个更加简洁的版本[4]。简单说就是一个自旋为单态的两个子系统组成的复合系统，不管A和B相距多远，只要测得A的自旋态投影（例如向上），B的不用测量就知道一定与A相反（向下），这与B的独立实在性相矛盾，同时B的三个自旋投影彼此是非对易的，怎么能在不对B做测量前都可以由A的测量同时确定其物理量呢？ 玻尔的反驳主要是阐述了在量子力学下，物理实在论的观点是有问题的，因此量子力学在非定域意义上是完备的。

1964 年 Bell（贝尔）根据爱因斯坦的定域实在论和爱因斯坦暗示以及玻姆发展的隐变量假设，推导出一个不等式 [5]，现在也被称之为 Bell 定理或 Bell 不等式定理。Bell 想法的关键是考虑 A 和 B 两处测量之间的关联。这个不等式是说：对于沿三个不同方向，例如 **a, b, c**, 任何两组方向测量的关联函数，（例如对 (**a, b**) 组，这个量记为 P(**a, b**)），其结果之差的绝对值不会大于另外一组的关联函数加 1，例如 $|P(\mathbf{a},\mathbf{b})-P(\mathbf{a},\mathbf{c})| \leqslant 1+P(\mathbf{b},\mathbf{c})$。显然量子力学的理论和迄今为止的实验结果都是违反 Bell 不等式的，因此隐变量假设不成立，或者说定域实在论在量子力学现象中有问题。一个简单例子是：假定两个粒子 A 和 B 组成了一个统一的纠缠态，对 A 粒子沿 a 方向和 B 粒子沿 b 方向测量所得的平均值就是 (**a, b**）夹角余弦的负值，容易验证，如果 **a, b, c** 在同一个平面内，且 (**a, b**）夹角为 60 度，(**b, c**）夹角为 60 度，(**a, c**）夹角为 120 度，那么 Bell 不等式 $|1/2+1/2| \leqslant 1-1/2$ 是不成立的。

怎么理解或解释Bell定理？一个自然方法就是想象一个场景，其中包含两个“粒子”，它们可能在某个时间点“在一起”（并相互作用），但在当前时间点“分离”（在某种意义上意味着它们不能再相互作用）。假设随后任意选择并对每个粒子执行测量（不一定对两个粒子进行相同的测量）。如果控制系统行为的基础物理是“经典”的，那么这样一个系统的行为可以基于相关的随机变量（通常称为“局部隐藏变量”），反映先前相互作用的可能结果。如果在进行测量时组件之间无法进行通信，则此类系统的可能行为就受到了限制。但如果控制系统行为的基础物理是“量子”（从某种意义上说，它可以基于纠缠的量子态，而不是相关的随机变量），那么一些受限制的行为可能会不受限制而发生，这在经典情况下是不可能的。这便是Bell不等式定理的旨趣所在。

当然后来人们研究了各种不同形式推广了的 Bell 不等式形式，包括克劳瑟－霍恩－希莫尼－霍尔特不等式（Clauser-Horne-Shimony-Holt inequalities，CHSH）[6]、连续变量 Bell 不等式及其最大破坏等，这些问题的研究对后续的量子隔物传输、纠缠交换、量子信息处理及量子计算等都有很重要的意义和价值 [3]。

对Bell不等式的实验验证大部分都在20世纪80年代，最著名的恐怕是1982年著名的Aspect小组的实验[7]（见图2），他们使用偏振光子代替了自旋粒子。在实验中，光子对在钙原子级联辐射下被发射出来。实验结果与量子力学理论一致，但违反了Bell不等式5个标准差。

同样在 1982 年，Pitowsky 对 EPR 和 Bell 不等式的佯谬问题做了认真研究与分析 [8]。他根据局域性原则的有效性提出了一种自旋为 2 的统计模型。基于观察到单位球面上的某些密度条件与观测频

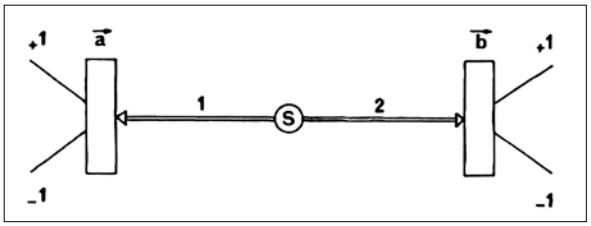

图2 EPR实验原理示意图。处于单重态（或类似态）的两个自旋-2粒子（或光子）分离。1和2的自旋分量（或线性极化方向）分别沿a和b方向。量子力学预言在这些测量中有很强的相关性（取自参考文献[7]）

率一致，由此产生的期望值便违反了贝尔不等式，但这种模式下的 EPR 却不违反局域性原则。测量的单重态的电子对具有统计独立性。这个相对频率违反 Bell 不等式也正是合理地利用了局域性原理。这似乎表明 Bell 不等式的违反反映了某种数学真理，即一定密度条件与现有的概率理论存在不相容的可能性。从概念上讲这是关键点。Bell 不等式的标准解释都假定概率论及其统计独立性和条件化的定义是有效的。换言之，人们相信柯尔莫戈罗夫（Kolmogorov）的公理最终抓住了我们所说的“概率”一词，这种态度类似于康德把欧几里德几何视为先验综合真理的观点。扩展概率概念甚至有很好的独立的数学原因，似乎也有很好的物理原因。因此 Pitowsky 建议类比黎曼和爱因斯坦处理几何学的方法来同样考虑处理概率论的理论。

爱因斯坦在晚年回顾与总结涉及这一EPR问题的量子理论与物理学的基础时[9]写道：“我们这一代的理论物理学家正期待着建立一套新的物理学理论基础。它所运用的基本概念应当大大不同于迄今所考察的场论概念。为表述所谓的量子现象，人们不得不要采用新的思考方法。而玻恩对量子理论的统计解释似乎是唯一可能的解释。这种解释也消除了由我和两位合作者所提出的悖论”（即指上述的EPR悖论）。具体说来，爱因斯坦意识到：波函数不能被理解为单个系统物理状态的一种（完备的）描述，而应该被理解为涉及众多系统，即统计力学意义上的系综的一个可提供测量物理量的统计数据。但显然，爱因斯坦对这种解释还是没有完全满意，他说：虽然量子力学抓住了真理的一部分美妙因素，今后的物理学基础也必须能够推导出它是极限情形，但我不认为量子力学是寻求这个理论基础的起点。正如我们不能指望从热力学或者统计力学就能推出力学基础一样。

1999 年，著名的量子信息物理学家 Zeilinger 教授在《现代物理评论》杂志上发表文章“实验与量子物理基础”综述了当时有关问题的争论与进展[10]，在谈到如何理解玻尔建立的量子力学的互补性原理时说道：“量子互补性就是这样一个事实的表达：为了测量两个互补量，我们必须使用相互排斥的装置。这种在光子记录后很长一段时间内决定波特征或粒子特征表现出来的可能性，是另一种警告，即在考虑量子现象时，人们不应该在头脑中有任何现实的图像。任何关于单个光子的特定个体观测中所发生的事情的详细图像都必须考虑到由两个光子组成的完整量子系统的整个实验装置，并且它只有在事实发生之后才有意义，即在关于互补变量的所有信息被不可恢复地抹去之后。”也就是说量子力学的互补性使得测量是个非定域性的塌缩，而不同的测量会造成不同的塌缩。

量子纠缠与量子信息

EPR直接触发了量子纠缠（Quantum Entanglement）的概念，继而又引起量子信息（Quantum Information）研究的热潮。这也是目前理论物理两个非常重要的研究领域。

我们先来看一段百度[11]词条《量子纠缠》上对这一名词由来的介绍：“薛定谔阅读完毕EPR论文之后，有很多心得感想，他用德文写了一封信给爱因斯坦，在这封信里，他最先使用了术语Verschränkung（他自己将之翻译为“纠缠”），这是为了要形容在EPR思想实验里，两个暂时耦合的粒子，不再耦合之后彼此之间仍旧维持的关联。不久之后，薛定谔发表了一篇重要论文，对于‘量子纠缠’术语给予定义，并且研究探索相关概念。薛定谔体会到该概念的重要性，他表明，量子纠缠不只是量子力学的某个很有意思的性质，而是量子力学的特征性质；量子纠缠在量子力学与经典思路之间做了一个完全切割。如同爱因斯坦一样，薛定谔对于量子纠缠的概念并不满意，因为量子纠缠似乎违反在相对论中对于信息传递所设定的速度极限。后来，爱因斯坦更讥讽量子纠缠为鬼魅般的超距作用。”

一个典型的二粒子的纠缠态如下[11]：假设一个零自旋中性π介子衰变成一个电子与一个正电子。这两个衰变产物各自朝着相反方向移动。电子移动到区域A，在那里的观察者“爱丽丝”会观测电子沿着某特定轴向的自旋；正电子移动到区域B，在那里的观察者“鲍勃”也会观测正电子沿着同样轴向的自旋。在测量之前，这两个纠缠粒子共同形成了零自旋的“纠缠态”它是两个直积态的叠加：A向上与B向下的直积与相反（即A向下B向上）直积的差。

无论对量子理论的基础而言，还是对量子信息论的实际应用而言，对量子纠缠的研究是非常必要而且也非常重要。在早期研究历史与发展中，人们搞清楚了两体量子纠缠、纠缠的度量、量子态的可分离性的充分必要条件。后续的发展是对纠缠研究中遇到的难题，诸如多粒子体系纯态的纠缠和纠缠混合态的结构，最大纠缠态的实现等等，做了众多尝试，也取得了很大进步，但一些根本性的问题仍然没有完全解决。

按照量子信息论的观点，量子纠缠是指不同粒子的量子态之间的纠缠，而不是单个粒子不同自由度之间的耦合，它也不是与态表达方式依赖有关的一个数学形式的存在，而是一种具有测量效应的物理存在[3]。它与量子力学中的态叠加原理以及量子测量的非定域性有密切联系，尽管其量子力学的本质显而易见，但其背后深刻的物理内涵尚未得到完整和很好的认识与了解。

三个粒子及以上的纠缠是实现多比特量子态纠缠、量子通信与量子计算的重要一步，特别是当纠缠度最大时。例如，如果三个粒子的偏振态最大程度地纠缠在一起，但根据量子力学它们中的每一个都是非极化的。20世纪90年代初，Greenberger-Horne-Zeilinger（格林伯格-霍恩-泽林格）就在理论上设计出来这样的纠缠态，后来被称为GHZ态而广为人知[12]。1996年Zeilinger等人又进一步设计了四粒子GHZ纠缠态实现的实验方案[13]。人们借助GHZ态可以实现量子离物传递。当然理论上人们可以通过对纠缠态的再纠缠来实现更加复杂的纠缠态结构从而为真实量子通信或量子离物传递做好准备。

无论从对量子力学概念基础的启示，还是对正确理解量子计算、量子通信和量子密码等新兴领域的基础来看，量子信息论都是一个有巨大潜力的新研究领域。尽管发现了量子无噪声编码定理，对量子噪声信道容量的研究都取得了不少成果，但量子信息在许多方面仍令人困惑。尤其是在量子隐形传态和超密集编码方面。事实上，这些依赖于空间分离的EPR对的两个成员之间的量子关联的对偶过程很难用信息论来解释。

关于量子纠缠与量子信息之间关系的研究，一个重要的工作值得一提，那就是1997年，Cerf

和 Adami对量子纠缠做了新解释[14]，他们的研究使用了著名的香农理论[15]和推广了的信息理论，而后者允许负的条件熵的存在，即使这在经典上是不允许的。这使得他们提出的量子信息过程可以用图表来描述，这就像粒子物理反应中涉及到的粒子那样，携带负的虚拟的信息可以类比于反粒子，而且它们可称之为反比特。

众所周知，以前描述量子信息过程的尝试通常依赖于经典信息理论的公式，并辅以量子概率，而不是振幅。然而，后来人们认识到冯 · 诺依曼熵具有信息理论意义，它是描述（渐近地）编码量子态系综所需的最小量子资源量。这表明可以定义一个扩展的信息理论，并且明确地把量子相位考虑进来。在 [14] 里，他们只使用密度算符和冯 · 诺依曼熵就能描述多粒子量子系统。这能把香农理论作为该理论考虑下的一个特例，同时也描述了量子纠缠，从而提供了一个经典和量子信息的统一处理方法。这个思想与在超强场下从真空中产生正负电子对 [16] 有异曲同工之妙。

关于虚信息的含义，他们给出了这样的解释：如果信息的提取违反了因果关系，我们将其定义为虚拟信息。换句话说，虚拟信息不能引起EPR对中两个粒子之间的超光速通信。正虚信息或负虚信息是由EPR对的一个成员携带的，这不是粒子的固有属性，而是在信息动力学完成后才可以分配的。在隐形传态或超密集编码中，正（虚）信息由被测粒子携带。如果两个粒子都被测量（例如，在贝尔实验中），则不能进行信息传输，也不能将虚拟信息内容分配给任何一个粒子。

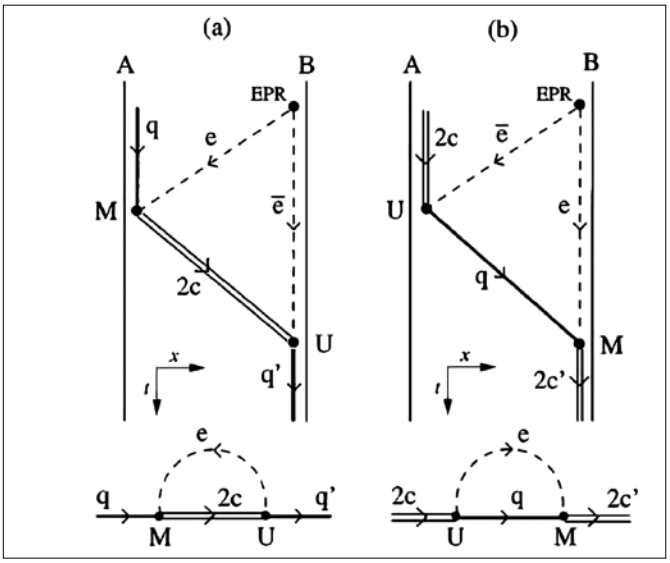

图3 量子隐形传态的物理时空图和超密编码的量子信息动力学图（取自参考文献[14]）

为区别于最大纠缠时使用的 qubit, 在描述两个粒子的“共享纠缠”时，1996 年 Bennett 等人创造了 ebit 一词，它作为“不定向信息资源”,可以提供传输信息的能力（尽管它本身不是信息）。因此 ebit 或 antiebit 也就是 EPR 对中携带了正或负的虚拟信息的那个成员。

这一量子信息理论的拓展几乎与量子场论中对虚粒子的引入与发展如出一撤，就连信息动力学的图（图 3）都与费曼图极为类似，只不过费曼图中的能量 - 动量守恒被信息熵守恒所取代。

量子密码与量子通信

既然量子信息和量子通信不得不需要密码，下面我们就来谈谈量子密码问题。密码学，尽管有着丰富多彩的历史，可以追溯到公元前400年，但直到20世纪40年代末才成为数学和信息理论的一部分，这主要是由于香农的开创性论文[15]。密码学可以简单地被定义为一个转换信息的数学系统，它对那些不打算使用的人来说是无用的。然而，由于与信息转换相关的计算过程总是通过物

理方法来执行，因此不能将数学结构与控制计算过程的基本物理定律分离[17]。1980年代Deutsch已经证明量子物理学丰富了我们的计算能力，它远远超过了经典的图灵机器，由Bennett和Brassard发起的量子密码学工作的确提供了一个很好的先例。

有必要回过头来对密码学的一些基本概念有个简单地认识和了解[17]。早期密文的安全性取决于整个加密和解密过程的保密性；然而，今天我们使用的密码，加密和解密的算法可以在不损害特定安全性的情况下把密码透露给任何人。在这种密码中，一组称为密钥的特定参数与明文一起作为加密算法的输入，与密码一起作为解密算法的输入。加密和解密算法可以是公开宣布的，而密码的安全性完全取决于密钥的保密性，所以这个密钥就变得非常重要，原则上它可以由随机选择的充分长的比特串组成。一旦密钥建立，随后的通信包括发送公共信道上的密码，易受拦截。所以为了建立密钥，两个最初不共享秘密信息的用户必须在通信的某个阶段使用可靠且非常安全的信道。对于拦截来说，不管从技术角度来说有多困难，因为毕竟是窃听者在这个频道上进行的一组测量，所以原则上，任何经典频道都可以被监控，而合法用户又意识不到发生了任何窃听，这就带来了通信的不安全性。但量子信道的情况并非如此[3]。其中一个主要原因是量子信道在没有任何与密钥相关联的“现实元素”的情况下分发了密钥，这一特性受到了量子力学完备性的保护。因此相比与经典信道，量子密码的安全性大大提高。

1991 年英国牛津大学的 Ekert 提出一种有趣的新方法[17]，表明在密码学中所谓的密钥分配过程的安全性取决于量子力学的完备性。这里的完完备性意味着量子描述提供了所考虑的任何系统的最大可能信息。该方案基于玻姆版的 EPR 思想性的实验[4]并使用广义的 Bell 定理，即 CHSH 不等式[6]做测试窃听。从理论上讲，这个方案扩展了 Bennett 和 Brassard 的原始思想，从实验的角度出发，通过对为验证 Bell 定理而建立的实验进行一点小小的修改，做到了能具有实际应用可能性的实现。例如在 1982 年 Aspect 小组在声光开关实验基础上[7]再加一些具体的设置，再结合一些软件来模拟信息发送者爱丽丝、信息接收者鲍勃和可能的某个窃听者，那么实验上就能模拟和检验所谓的量子信道及其密码的安全性。

总的说来 Ekert 描述了一种密码方案，其中 EPR 粒子对被用来在遥远的地方产生相同的随机数，而贝尔定理证明了窃听者没有在传输过程中测量到这些粒子。但随后不久，1992 年 Bennett、Brassard 和 Mermin 他们描述了一个相关但更简单的 EPR 方案[18]，并且在不调用 Bell 定理的情况下，证明了它对更一般的攻击是安全的，包括替换假的 EPR 源。他们证明了该方案与原来 1984 年 Bennett 和 Brassard[19] 提出的密钥分配方案（也就是研究历史上那个著名的 BB84 协议）是等价的，当时使用的是单粒子而不是 EPR 对。这表明，Bell 不等式和 EPR 相关态都不是产生和证明这种共享随机数密钥匙的重要部分。

再来看下物理学家如何利用EPR量子纠缠等属性来实现可能的量子通信或量子离物隐形传态的。

众所周知，不确定性原理阻止了量子态共轭变量的同时精确测量。这似乎排除了以经典方式发送足够信息以完全重建测量量子态的可能性。然而，1993年在Bennett等人的一项研究中[20]，发现自旋1/2粒子的未知态可以通过传输经典信息“传送”到远程站，前提是发送者和接收者共享一个EPR纠缠量子对，但光子计数固有的低效率

却限制了实验的实现。

20 世纪 90 年代中后期 Vaidman 和 Kimble 等人提出了连续量子变量的隐形传态的可能性 [21]，例如利用电磁场的正交振幅，这使得使用高效的零差检测技术成为可能。作为一个具体的例子，他们讨论了使用参量下转换作为 EPR 源的光学状态的隐形传态 [22]。

1998 年，Ralph 等研究了明亮压缩光的隐形传态 [23]，他们从小信号通信的角度研究连续量子变量的隐形传态。发现混合的明亮压缩光束可以提供隐形传态所需的纠缠。从信息传递和状态重建的角度提出了明亮光束隐形传态的具体实验准则。

对于理解量子隐形传态方案来说，最重要的是认识到最大纠缠态（如Bell基）的特征是纠缠态的任何单个成员都不能单独携带任何信息。所有信息只在联合属性中编码。因此，纠缠态是对纠缠对的两个成员的两个可能测量值之间关系的描述。非常有趣和有用的是传送的状态不仅仅是未知的，而且是未定义的。这种可能性导致纠缠交换，即纠缠两个完全独立产生且从未相互作用的粒子，1998年潘建伟等人就研究了这一问题[24]，他们首次实验实现了这一惊人的应用投影假设的纠缠交换方案（见图4），这也是中国学者对量子通信研究做出的重要贡献之一。

最后对量子通信安全性问题笔者做下总结，并且我们要再提一下其他中国人的贡献[25]。显然量子计算机为现代通信安全带来了严重挑战，量子保密通信是应对这一挑战的重要技术。一般认为20世纪80年代Bennett和Brassard提出的量子密钥分发，90年代Hillery等提出的量子秘密共享和中国学者龙桂鲁等提出的量子安全直接通信（Quantum Secure Direct Communication，简称QSDC即量子直通）是三个最主要的量子保密通信理论。

窃听光量子会改变其状态而被检测发现。量子密钥分发和量子秘密共享通过检测传输的随机数是否被窃听，决定放弃传输数据或者将其升级为密钥，再通过经典信道传输信息。经典通信没有窃听感知能力，两个交谈的人感知不到他们的谈话已被躲在暗处的窃听者偷听。量子密钥分发和秘密共享拥有窃听感知能力，但是无法阻止窃听者窃取信息，不能直接进行通信或共享信息。为此，他们就先传输一队随机数，检测是否被窃听，如果发现被窃听则丢弃传输的随机数，如果确认没有被窃听则将传输的随机数作为密钥。量子直通在感知窃听的基础上，更进一步有了抵抗窃听的能力，不仅能发现有人窃听而且让窃听者得不到任何信息，从而实现直接安全的通信。之所以能够这样，是因为量子直通采用了“数据块传输”的方式，在传输过程中在块内发现窃听，不使信息泄露，从而实现直接通信。

量子直通似乎是经典通信在量子领域的发展，香农理论保证了在噪声信道下信息的可靠传输，而Wyner搭线信道理论则保证了量子直通在

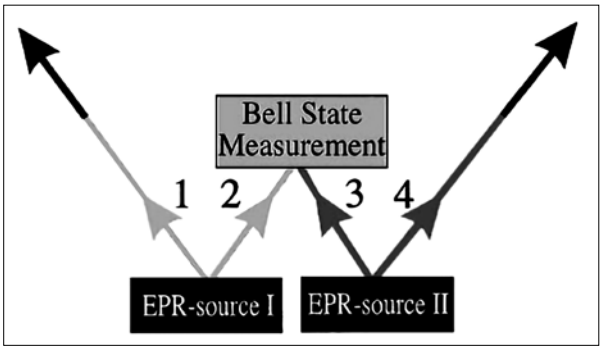

图4 纠缠交换原理图。两个EPR源产生两对纠缠光子，一对1−2，一对3−4。对每对光子中的一个影的变化表示可以进行的可能预测性的改变。（取自参考文献[24]）。

既有噪声又有窃听的信道中信息的可靠和安全通信。由于减少了密钥分发和管理等环节，量子直通的安全性得到进一步提高，并且可以在多方面应用。美国国土安全部战略局主任John Costello指出，量子直通可在整体上提高量子通信的安全和价值。有关详细情况可进一步参考[25]。

由于篇幅所限，就简单介绍这些，事实上，进入21世纪以来，这方面的研究获得了长足的发展与进步。后续更多的研究成果和取得的实际应用等有机会再给大家介绍。值得一提的是2019年，具有实用价值的量子直通样机已经成功研制。通过几代人不懈的努力，我们有理由期待真正的量子通信和量子计算机将在不久的将来得到实现，或许在EPR发表100周年之际，这是奉献给那些伟大先驱者们最好的礼物。

（2020年5月5日稿）

参考文献

[1] Einstein A, Podolsky B and Rosen N. Can Quantum–Mechanical Description of Physical Reality Be Considered Complete' ? Phys. Rev. 47: 777–780 (1935).

[2] Bohr N. Can Quantum–Mechanical Description of Physical Reality Be Considered Complete? Phys. Rev. 48: 696–702 (1935).

[3] 曾谨言 裴寿镛 龙贵鲁 主编. 量子力学新进展（第二辑）. 北京大学出版社，北京，2001：p288，p282，.

[4] Bohm D. Quantum Theory. Prentice Hall, Englewood Cliffs, NJ, 1951.

[5] Bell J S. On the Einstein–Podolsky–Rosen Paradox. Physics (Long Island City, N. Y.) 1: 195–200 (1964).

[6] Clauser J F, Horne M A, Shimony S and Holt R A. Proposed Experiment to Test Local Hidden–Variable Theories. Phys. Rev. Lett. 23: 880–884 (1969).

[7] Aspect A, Grangier P and Roger G. Experimental Realization of Einstein– Podolsky–Rosen–Bohm Gedankenexperiment: A New Violation of Bell's Inequalities. Phys. Rev. Lett. 49: 91–94 (1982)

[8] Pitowsky I. Resolution of the Einstein–Podolsky–Rosen and Bell Paradoxes. Phys. Rev. Lett. 48: 1299–1302 (1982).

[9] 阿尔伯特·爱因斯坦 著，方在庆 韩文博 何维国 译. 爱因斯坦晚年文集. 海南出版社，海口，2014：p75–p83..

[10] Zeilinger A. Experiment and the foundations of quantum physics. Rev. Mod. Phys. 71: S288–S297 (1999).

[11] https://www.baidu.com/

[12] Greenberger D M, Horne M A and Zeilinger A. in Bell’s Theorem, Quantum Theory, and Conceptions of the Universe, edited by Kafatos M (Kluwer, Dordrecht, 1989).

[13] Zeilinger A, Horne M A, Weinfurter H and Zukowski1M. Three–Particle Entanglements from Two Entangled Pairs. Phys. Rev. Lett. 78: 3031–3034 (1997).

[14] Cerf N J and Adami C. Negative Entropy and

Information in Quantum Mechanics Phys. Rev. Lett. 79: 5194–5197 (1997).

[15] Shannon C E. Communication Theory of Secrecy Systems. Bell System Technical Journal 28: 656–715 (1949).

[16] 谢柏松 李子良 唐琐 刘杰. 超强场下的正负电子对产生. 物理46: 713–720 (2017).

[17] Ekert A K. Quantum Cryptography Based on Bell's Theorem. Phys. Rev. Lett. 67: 661–663 (1991).

[18] [18] Bennett C H, Brassard G and Mermin N D. Quantum Cryptography without Bell's Theorem. Phys. Rev. Lett. 68: 557–559 (1992).

[19] Bennett C H and Brassard G. Iin Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India (IEEE, New York, 1984), p. 175–179.

[20] Bennett C H, Brassard G, Crepeau C, Jozsa R, Peres A and Wootters W K. Teleporting an Unknown Quantum State via Dual Classical and Einstein–Podolsky–Rosen Channels. Phys. Rev. Lett. 70: 1895–1899 (1993).

[21] Vaidman L. Teleportation of quantum states. Phys. Rev. A 49: 1473–1476 (1994); Braunstein S L and Kimble H J. Teleportation of Continuous Quantum Variables. Phys. Rev. Lett. 80: 869–872 (1998).

[22] Ou Z Y, Pereira S F, Kimble, H J and Peng K C. Realization of the Einstein– Podolsky–Rosen Paradox for continuous Variables. Phys. Rev. Lett. 68: 3663–3666 (1992).

[23] Ralph T C and Lam P K. Teleportation with Bright Squeezed Light. Phys. Rev. Lett. 81: 5668–5671 (1998).

[24] Pan J W, Bouwmeester D, Weinfurter H, and Zeilinger A. Experimental Entanglement Swapping: Entangling Photons That Never Interacted. Phys. Rev. Lett. 80:3891–3894 (1998).

[25] http://www.scichina.com/