量子信息简介
Brief Introduction to Quantum Information

量子信息是指以量子力学基本原理为基础、通过量子系统的各种相干特性(如量子并行、量子纠缠和量子不可克隆等)，进行计算、编码和信息传输的全新信息方式。

根据摩尔（Moore）定律，每十八个月计算机微处理器的速度就增长一倍，其中单位面积（或体积）上集成的元件数目会相应地增加。可以预见，在不久的将来，芯片元件就会达到它能以经典方式工作的极限尺度。因此，突破这种尺度极限是当代信息科学所面临的一个重大科学问题。量子信息的研究就是充分利用量子物理基本原理的研究成果，发挥量子相干特性的强大作用，探索以全新的方式进行计算、编码和信息传输的可能性，为突破芯片极限提供新概念、新思路和新途径。量子力学与信息科学结合,不仅充分显示了学科交叉的重要性，而且量子信息的最终物理实现，会导致信息科学观念和模式的重大变革。事实上，传统计算机也是量子力学的产物，它的器件也利用了诸如量子隧道现象等量子效应。但仅仅应用量子器件的信息技术，并不等于是现在所说的量子信息。目前的量子信息主要是基于量子力学的相干特征，重构密码、计算和通讯的基本原理。

1. 量子相干性与量子纠缠

在经典信息处理过程中，刻画信息的二进制经典比特（Bit）由经典状态(如电压的高低) 1 和 0 表示。对于量子信息而言，由于微观世界中量子效应会鲜明地凸现出来，经典比特状态的 1 和 0 必须由两个量子态 |1> 和|0> 来取代；处于这样两种不同状态之上的粒子就是量子信息的基本存储单元—量子比特（Qubit）。 任意两态量子体系都可成为量子信息的载体，如二能级原子、分子或离子，光子偏振态或其它等效的自旋 1／2 的粒子。

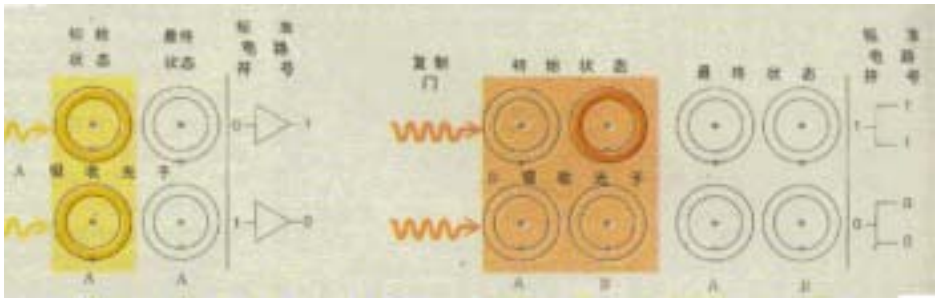

图 1：二能级原子构成量子比特

与经典比特本质不同，一个量子比特可以处在|0>和|1> 的相干叠加态

$$|u\rangle = a|0\rangle+b|1\rangle$$

上。即，量子比特可以随机地存在于状态| 0>和|1>上，且在每种状态上出现的概率 $p=|c|^2$ 由复数系数 c=a ,b 确定。需要指出，这样的叠加态具有明显的量子相干特征，经典概率 $p=|c|^2$ 不足以描写这个叠加态，a 和 b 相对的位相在量子信息过程中，起着至关重要的作用。

由于量子相干性，量子比特在测量过程中会表现出与经典情况完全不同的行为。在经典力学中，至少在理论上可以构造理想的测量，使得测量本身不会本质地改变被测体系的状态。而在量子力学中则不然，测量仪器与被测系统的相互作用会引起所谓的波包塌缩：设|0>和|1>是力学量 A 的本征态，相应的本征值是 a_0 和 a_1 。在|u> 上对 A 进行测量,一旦单一的测量得到了值 a_0，波函数便塌缩到|0> 上。这时|，u>的相干性将被彻底破坏，即发生了所谓的量子退相干。正如在中子干涉问题中，一旦通过测量观测到中子到达屏的路径，干涉条纹将不复存在了。

多比特系统特有的量子性质是所谓的量子纠缠（Quantum Entanglement）。两个比特的量子系统有 4 种不同的状态， 即两个比特都在|**0**>**上**的状态|0，0>，两个比特都在|1>上的状态|1，1>，第一个比特在|**0**>**上**同时第二个比特在|1>**上**的状态|0，1> 以及第一个比特在|**1**>**上**同时第二个比特在|0>**上**的状态|1，0>。这一点与两个比特经典系统的情况一样。 不同的是，2 比特量子系统可以处在非平凡的双粒子相干叠加态 — 量子纠缠态上，如

$$|EPR\rangle = (1/2)^{1/2}\,(|0,1\rangle + |1,0\rangle)$$

其非平凡性表现在它不能够分解为单个相干叠加态的乘积，从而呈现出比单比特更丰富的、更奇妙的量子力学特性：想象|**EPR**>描述了处在自旋单态上的双电子体系，其中|1>代表电子自旋向上的状态，|0>代表电子自旋向下的状态。 测量第一个电子的自旋，可以 50% 几率得到向上的电子和 50% 向下的电子；当第一个电子被发现向下，整个波函数被塌缩到态 |0,1>上. 这时，再测量第二个电子，必得到自旋向下的确定的结果。即使是两个电子分开得很远，这种不可思议的关联仍然存在。

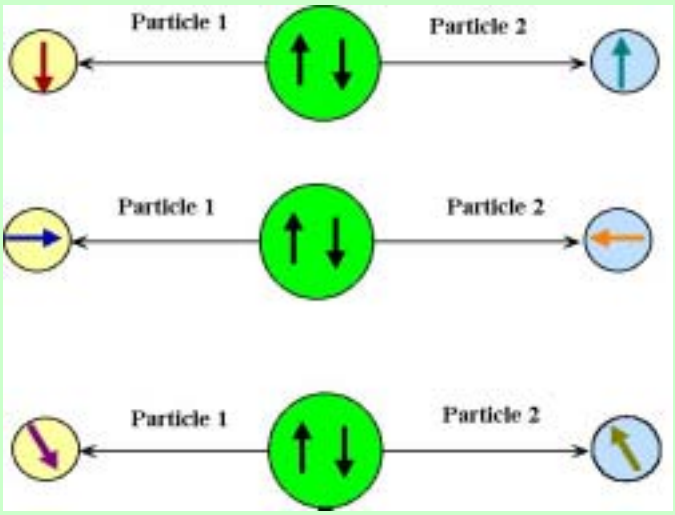

图 2：量子纠缠描述的电子自旋关联的奇妙特性：

电子自旋向上、向下的关联 — 量子纠缠，本质上不同于经典关联：同一个|EPR>态，还可以重新表达为沿任意方向 （如自旋向左、向右）自旋的关联，因而它描述哪一种自旋关联， 依赖于你对第一个电子测量什么。而经典关联具有确定的特征：伸手到一个放了一个白球和一个黑球的黑盒子里，随便摸得黑球和白球的几率各为 50% 。拿到了一只黑球后把盒子拿到远处，再摸你一定得到白球。没有白球和黑球的叠加，这种经典关联是不足为奇的。因此， |EPR>量子纠缠与经典关联的这种基本差异，正是量子通讯的物理基础。

一个黑球。你伸手到盒子里随便摸一个球，得到黑球和白球的几率各为 50% 。但是一旦你拿到了一只黑球，然后把盒子拿开，不管多远，你仍然可以断定盒子里一定是白球。这种事先预置的经典关联是不足为奇的. 但量子情况并非如此简单！由于同一个**|EPR>**态，还可以重新表达为沿任意方向 （如自旋向左、向右）自旋的关联，它描述哪一种自旋关联， 依赖于你对第一个电子测量什么。因此， **|EPR>**描述的这种奇妙的量子纠缠性，本质上不同于经典关联。这种基本差异正是量子通讯的物理基础。

Einstein, Podolsky 和 Rosen 在二十世纪三十年代提出来的 EPR 态的观念（玻姆后来给出了 EPR 态的上述直观表达），其目的是要通过量子纠缠现象与相对论因果关系表面上的矛盾质疑量子力学的完备性，它引发了许多关于量子力学基本问题的讨论。

量子计算(Quantum Computing)

从原理上讲，经典计算可以被描述为对输入信号序列按一定算法进行变换(逻辑门操作)的物理过程。 基于经典比特的非 0 即 1 的确定特征，经典算法是通过经典计算机(或经典图灵机)的内部逻辑电路加以实现的.而量子计算，则是基于量子比特的既 |0> 又 |1> 相干叠加特征，对可由量子叠加态描述的输入信号,根据量子的算法要求，进行叫做“ 量子逻辑门操作 ”的幺正变换．这是一个被人为控制的、以输入态为初态的量子物理演化过程。对末态 — 输出态进行量子测量，给出量子计算的结果．顾名思义，所谓的量子计算机(quantum computer) 就是实现这种量子计算过程的机器。

量子计算机的概念最早源于二十世纪六、七十年代对克服能耗问题的可逆计算机的研究.计算机芯片的发热，影响芯片的集成度，从而大大限制了计算机的运行速度．Landauer 关于“ 能耗产生于计算过程中的不可逆操作 ”的发现表明，虽然物理原理并没有限制能耗的下限，但必须将不可逆操作改造为可逆操作，才能大大提高芯片的集成度。直观地说，当电路集成密度很大时，Δx 很小时，Δp 就会很大，电子不再被束缚，就会出现量子物理所描述的量子干涉效应，从而破坏传统计算机芯片的功能。对于现有的传统计算机技术，量子力学的限制似乎是一个不可逾越的障碍。只有量子力学中的幺正变换，才能真正地实现可逆操作。从理论观念的角度讲，量子计算的想法与美国著名物理学家 R．Feynman“ 不可能用传统计算机全面模拟量子力学过程 ”的看法直接相关。在此基础上，1985 年，英国牛津大学的 D．Deutsch 初步阐述了量子图灵机的概念，并且指出了量子图灵机可能比经典图灵机具有更强大的功能。1995 年，Shor 提出了大数因子化量子算法,并有其他人演示了量子计算在冷却离子系统中实现的可能性，量子计算机的研究才变成物理学家、计算机专家和数学家共同关心的交叉领域研究课题。

量子并行性是量子计算的关键所在。显而易见，描述有 2 个比特的量子计算机,需要 4 个系数数字 ;描述 n 个量子比特的量子计算机就需要 2^n 个系数数字。例如，如果 n 等于 50，那就需要大约 10^{15} 个数来描述量子计算机的所有可能状态。虽然 n 增大时所有可能状态的数目将迅速变成一个很大的集合，但由于态叠加原理，量子计算机操作 —幺正变换能够对处于叠加态的所有分量同时进行。这就是所谓的量子并行性。由于这一奇妙的内禀并行性，一台量子计算机仅仅靠一个处理器就能够很自然地同时进行非常多的运算。典型的量子计算有 Shor 的大数因子化和 Grover 的数据库量子搜索。

所谓的大数因子化是把一个给定大数分解为素数因子的乘积。破译某些密码（如“ RSA 公共密钥体系 ”），需要在有效的时间内完成这样的计算。然而，在传统计算机中，一个 n 位二进制数是由一串有 n 个 0 或 1 组成的数串描述。任何一个十进制数 $x= a_0 2^0 +a_1 2^1 + a_2 2^2+.....+a_n2^n$ 可以唯一地表达为一个二进制数 $a_n a_{n-1} \ldots a_2 a_1 a_0$,其中 a_I=0,1。存储大数 x 通常约需要 $n=\log_2 x$ 个比特。如果用１，２，３，、、、直到 $\sqrt{x}$ 去试除 x，经典计算过程通过约 $\sqrt{x}$ 步运算，可以最后找到 x 的全部素数因子。显然，计算的步数 $s= e^{n(\ln 2)/2}$ 与这个大数的数据位数呈 e 指数增长关系。因此，随着 n 变大，步数将是一个天文数字。按照现有的算法，对于一个 400 位数字的分解，使用现今世界上最快的超级计算机也要花几十亿年时间才能完成。人类的历史才不过几百万年，这样的计算必定是无效的。然而，令人吃惊的是，美国电报电话公司的 Peter W.Shor 在 1995 年写下了一个量子算法，使得完成 一个 n 位大数的因子分解所用的计算步数只是 n 的多项式函数，而不是 n 的指数函数。这个被称为“ Shor 大数因子化 ”的量子算法，充分发挥了量子并行性的强大作用，原则上可以在一年左右的时间内分解一个 400 位大数。 由于现有的加密系统大多是建立在大数难于分解的基础之上，Shor 的发现有可能使现在所用的大部分复杂加密方案失效，从而在金融和国防的保密方面产生了极大的影响。

表现量子计算独特能力的另一项算法，是贝尔实验室的 L.K.Grover 设计的量子搜索算法。计算机在搜索藏在有 n 个对象的数据库中的一个特定的对象时，经典的搜索过程要比较每一个对象，平均说来需要进行 n／2 次尝试才有较大的可能找到那个对象。经典搜索的一个日常生活的例子是在一个按人名索引的、共有Ｎ个人的电话簿里，找到确定号码的人，通常要找Ｏ（Ｎ）次才能成功。Grover 把它换成量子力学问题就是：对于Ｎ个态的均匀相干叠加，通过若干次基本的么正变换可以把其中一个特定分量的几率放大为１。令人惊讶的是，Grover 的量子搜索可以通过大约根号 $\sqrt{N}$ 次尝试就找出所需的对象。1998 年初，IBM 公司加洲阿尔马登研究中心的 Issac Chuang 等人利用氯仿核磁共振实现了两个量子数据位的量子搜索实验，成为量子计算的第一个演示实例。

量子通讯与量子离物传态（Quantum Teleportation）

量子通讯是利用量子纠缠效应进行信息传递的一种新型的通讯方式。量子离物传态是这种新型的通讯方式的原理演示。由于量子纠缠代表的关联依赖于对两个纠缠的粒子之一测量什么，直接通过量子纠缠不能传递物体的全部信息。但是，我们却可以设想这样的量子通讯过程：将某物体待传递量子态的信息分成经典和量子两个部分，它们分别经由经典通道和量子通道传送给接收者。经典信息是发送者对原物进行某种测量而提取的，量子信息是发送者在测量中未提取的大量信息；接收者在获得这两种信息后，就可以制备出原来量子态的完全复制品。该过程中传送的仅仅是该物体的量子态，而不是该物体本身。发送者甚至可以对这个待传量子态一无所知，而接收者则能将他持有的粒子处于原物体的量子态上。

利用这种量子纠缠特性，Bennet 和其他 5 位来自不同国家的科学家等在 1993 年提出了演示这种量子通讯的量子离物传态（Teleportation）方案：通过在经典信道中送 2 个比特的信息破坏空间某点的量子态，可以在空间不同点制备出一个相同的量子态. 要指出的是，通常的离物传态（Teleportation）描述了这样一种奇妙的、有点象科幻小说的场景：某人突然消失掉，而在远处莫明其妙地显现出来。 Bennet 等人的量子离物传态方案具体描述如

下：设想 Bob 要将他持有的粒子 B 的未知量子态 $|u\rangle=a|0\rangle+b|1\rangle$ 传给远方的持有粒子 A 的 Alice. 他可以操控他持有的粒子 B 和由 BBO 型量子纠缠源分发给来的粒子 S。由于量子纠缠源产生了粒子 A 和粒子 S 的量子纠缠态 $|ERP\rangle$， Bob 对粒子 B 和粒子 S 的联合测量结果（依赖于对 A 和 S 的 4 个 Bell 基的区分），会导致 Alice 持有的粒子 A 塌缩到一个与 $|u\rangle$ 相联系的状态 $|u'\rangle=W|u\rangle$ 上，其中幺正变换 **W** 完全由 Bob 对 粒子 A 和粒子 S 的联合测量结果的 2 个比特经典信息决定，而与待传的未知量子态无关。 Bob 将即已测到的结果，通过经典通道（打电话、发传真或 e-mail 等）告诉 Alice。远方的 Alice 就知道粒子 A 已经塌缩到$|u'\rangle$上.选取合适的幺正变换 W^+，Alice 便可以将粒子 A 制备在$|u\rangle$上了。

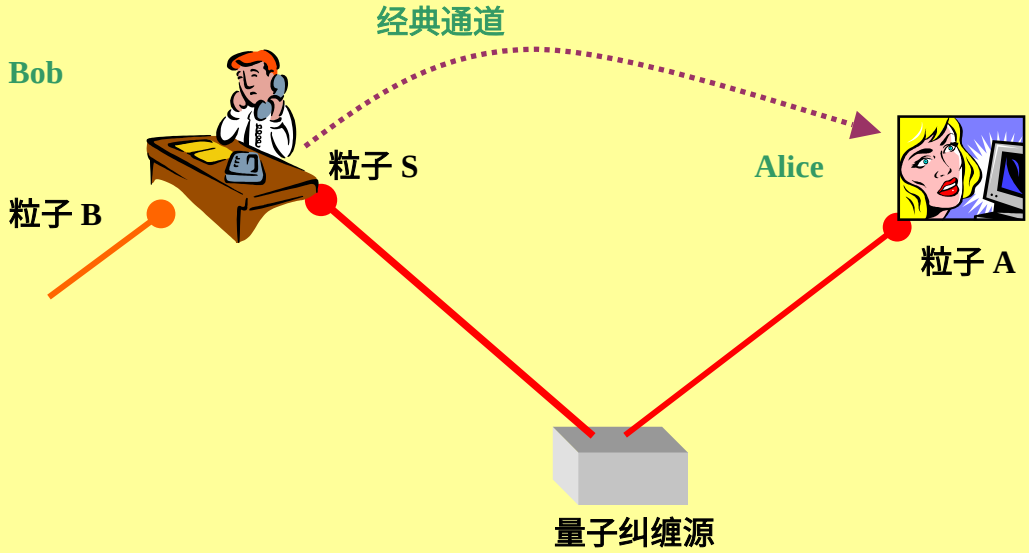

图 3　Bennet 等量子离物传态方案：*设想 Bob 要将他持有的粒子 B 的未知量子态 $|u\rangle=a|0\rangle+b|1\rangle$ 传给远方的持有粒子 A 的 Alice. 他可以操控他持有的粒子 B 和由 BBO 型量子纠缠源分发给来的粒子 S。由于量子纠缠源产生了粒子 A 和粒子 S 的量子纠缠态 $|ERP\rangle$， Bob 对粒子 B 和粒子 S 的联合测量结果（依赖于对 A 和 S 的 4 个 Bell 基的区分），会导致 Alice 持有的粒子 A 塌缩到一个与 $|u\rangle$ 相联系的状态 $|u'\rangle=W|u\rangle$ 上，其中幺正变换 W 完全由 Bob 对 粒子 A 和粒子 S 的联合测量结果的 2 个比特经典信息决定，而与待传的未知量子态无关。 Bob 将即已测到的结果，通过经典通道（打电话、发传真或 e-mail 等）告诉 Alice。远方的 Alice 就知道粒子 A 已经塌缩到$|u'\rangle$上. 选取合适的幺正变换 W^+，Alice 便可以将粒子 A 制备在$|u\rangle$上了。*

在实验上，实现量子通讯与量子离物传态的关键技术是制备理想的 EPR 纠缠态和进行 Bell 基测量。二十世纪八十年代末，史砚华和 Mandel 等研究小组利用ＢＢＯ晶体非线性效应—参量下转换 ，成功地演示了纠缠光子对的存在。1997 年 12 月，奥地利因斯布鲁克

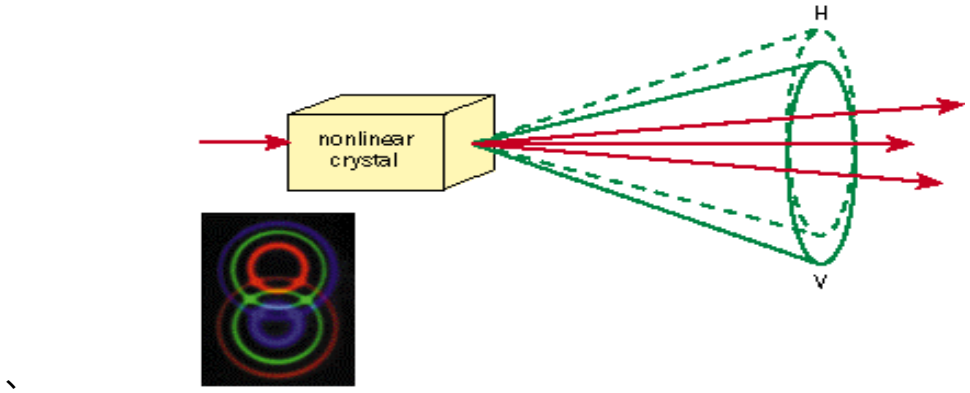

图 3: ＢＢＯ晶体参量下转换产生纠缠光子对

大学的 A. Zeilinger 研究小组利用这种纠缠光子对，对量子离物传态进行了一次的重要的实验演示。 1998 年初，意大利学者也报导了另一个成功的实验。在这些实验中，纠缠态的非定域性起着至关重要的作用，而量子力学非定域效应已被违背贝尔不等式的实验结果所证实。因此，量子离物传态的实验实现，不仅在物理学领域对人们认识与揭示自然界的量子特性具有重要意义，而且可以用量子态作为信息载体，通过量子态的传送完成大容量信息的传输，实现原则上不可破译的量子保密通信。然而，由于实验中不能进行完整的 Bell 基测量－区分四个 Bell 基，学术界有人对这些实验持不同的观点，这些争论均涉及对基本量子测量问题的不同理解。另外，由于存在各种不可避免的环境噪声，量子纠缠态的品质会随着传送距离的增加而变得越来越差。因此，量子离物传态的实验实现离实用量子通讯的要求还有相当的距离。

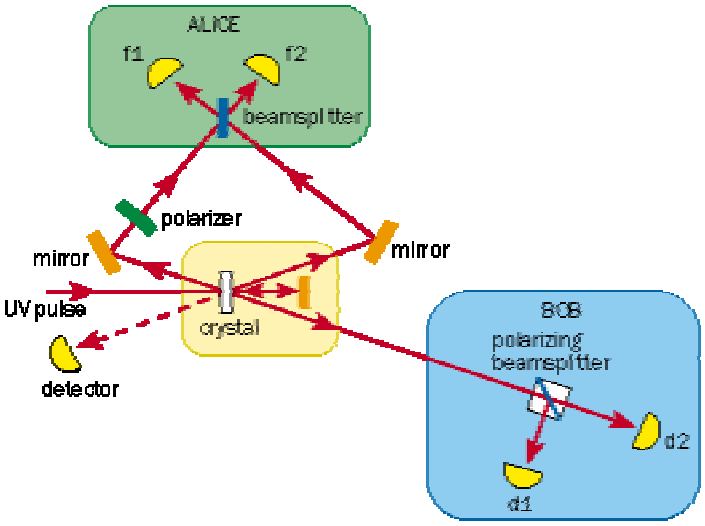

图 4：Zeilinger 小组量子离物传态实验原理示意图

量子密码学（Quantum Cryptography）

经典的密码学是一门古老的学科，它的起源可以追溯到几千年前的古埃及、古罗马时代。 早在四千年前，古埃及一些贵族墓碑上的铭文就已经具备了密码的两个基本要素：秘密性和信息的有意变形。尽管如此，密码学作为一门严格的科学建立起来还仅仅是近五十年的事。可以说，直到 1949 年以前， 密码研究更象是一门艺术而非科学。主要原因在于，在这个时期没有任何公认的客观标准衡量各种密码体制的安全性，因此也就无法从理论上深入研究信息安全问题。1949 年，C.E.Shannon 发表了《保密系统的通信理论》，首次把密码学建立在严格的数学基础之上。密码学从此才成为真正意义上的科学。

密码学的目的是改变信息的原有形式使得局外人难以读懂。密码学中的信息代码称为密码，尚未转换成密码的文字信息称为明文，由密码表示的信息称为密文，从明文到密文的转换过程称为加密，相反的过程称为解密， 解密要通过所谓的密钥进行。因此，一个密码体制的安全性只依赖于其密钥的保密性。在设计、建立一个密码体制时，必须假定破译对手能够知道关于密码体制的一切信息，而唯一不知道的是具体的一段密文到底是用哪一个密钥所对应的加密映射加密的。在传统的密码体制中，只要知道了加密映射也就知道了解密映射。因此，传统密码体制要求通信双方在进行保密通信之前必须先约定并通过“ 安全通道 ”传递密钥。此外，在传统的密码体制下，每一对用户都需要有一个密钥。这样，在 n 个用户的通讯网络中，要保证任意两个 用户都能进行保密通信，就需要很多“ 安全通道 ”传送 n(n-1)/2 个密钥。如果 n 很大，保证安全将是很困难的。

为解决上述难题，人们另辟蹊径，于 1976 年提出了公开密钥密码体制的思想：将密钥分成公开密钥和秘密密钥两部分，分别决定互逆的加密映射和解密映射。在这种密码体制下，每个用户均有自己的公开密钥和秘密密钥。公开密钥是公开的，可以象电话号码一样供人查阅，这样，通信双方不必事先约定即可进行保密通信，也不存在需要“ 安全通道 ”传送密钥的问题； 秘密密钥则是秘密的，由每个用户自己保存，供解密之用。典型的一个公钥密码体系是 RSA 密码体制，它主要是基于经典计算机几乎无法完成大数分解有效计算这一事实。从这个意义上讲，如果人们能够在实际中实现“ Shor 大数因子化 ”的量子算法，RSA 保密体制完成的任何加密就会被解密。因此，量子计算会对由传统密码体系保护的信息安全构成致命的打击，对现有保密通讯提出了严峻挑战。要预防这种打击，必须采取量子的方式加密。虽然量子密码体系当初并非因此而生，但它的确是解决这个问题的有效途径。

量子密码体系采用量子态作为信息载体，经由量子通道在合法的用户之间传送密钥。量子密码的安全性由量子力学原理所保证。所谓绝对安全性是指：即使在窃听者可能拥有极高的智商、可能采用最高明的窃听措施、可能使用最先进的测量手段，密钥的传送仍然是安全的。通常，窃听者采用截获密钥的方法有两类：一种方法是通过对携带信息的量子态进行测量，从其测量的结果来提取密钥的信息。但是，量子力学的基本原理告诉我们，对量子态的测量会引起波函数塌缩，本质上改变量子态的性质，发送者和接受者通过信息校验就会发现他们的通讯被窃听，因为这种窃听方式必然会留下具有明显量子测量特征的痕迹，合法用户之间便因此终止正在进行的通讯。第二种方法则是避开直接的量子测量，采用具有复制功能的装置，先截获和复制传送信息的量子态。然后，窃听者再将原来的量子态传送给要接受密钥的合法用户，留下复制的量子态可供窃听者测量分析，以窃取信息。

这样，窃听原则上不会留下任何痕迹。但是，由量子相干性决定的量子不可克隆定理告诉人们，任何物理上允许的量子复制装置都不可能克隆出与输入态完全一样的量子态来。这一重要的量子物理效应，确保了窃听者不会完整地复制出传送信息的量子态。因而，第二种窃听方法也无法成功。量子密码术原则上提供了不可破译、不可窃听和大容量的保密通讯体系。

量子博弈(Quantum Game)

经典的博弈论是现代数学的重要分支，在经济学等领域中有着广泛的应用。博弈论考虑的问题是：在一个游戏中当游戏的参加者采取不同的策略时，他们会得到不同的收益。那么，为了提高各自的收益，他们应该采取什么样的策略。“ 囚徒困境 ”是博弈论的一个生动的例子。在这个例子中，假定游戏的两个参加者都可以采取 A 或 B 两种策略。如果他们都选择 A，那么每人都会得到三个单位的收益；相反，如果两个人都选择 B，那么每人只能得到一个单位的收益。如果有一个游戏者选择 A，而另一个选择 B，那么后者会得到五个单位的收益，前者则什么也得不到。博弈论告诉我们，如果两个游戏者之间不能互通消息，那么由于对于他们每个人而言无论对方的策略是什么，自己选择 B 所获得的收益总比选择 A 来的多，所以他们都会选择 B。而这样一来他们每人只能得到一个单位的收益，这显然不如两人都选择 A 给他们带来的收益多。对于两个游戏者来说，这是一个无法避免的困境。在这个的例子中，当两个游戏者都采取 B 这个策略时，他们中的任何人独自改变自己的策略都只会使自己收益降低。这种情况称为“ 纳什均衡 ”。在博弈论中，寻找一个游戏的“ 纳什均衡 ”点往往是进行各种分析的核心步骤。不难看出，在上面的例子中，“ 两人都选择 B ”是游戏中唯一的纳什均衡点。

“ 量子博弈 ”是 1999 年由 Eisert 等人提出的。在他们文章所描述的游戏中，游戏者手持服从量子规律的粒子，游戏时所能采取的策略即是对手中的粒子施行自己选定的量子操作。而操作结束后各位游戏者手中粒子的状态将决定这些游戏者的收益。Eisert 的文章指出，在“ 囚徒困境 ”的游戏中，一旦允许两个游戏者手持处在“ 最大纠缠态 ”的粒子，并且以各种么正变换作为自己的策略，那么对于他们来说，能使自己收益最大的策略将不是前面提到的策略 B。对局中将出现一个新的纳什均衡点。这个均衡点所对应的情况是两个游戏者对自己手中的粒子施行一个特定的么正变换。在这个均衡点上，两个游戏者都将得到 3 个单位的收益。这种“ 双赢 ”局面的出现意味着在“ 量子博弈 ”中游戏者摆脱了前面所说的困境。

去年年初，中国科技大学杜江峰博士的科研小组利用核磁共振系统在国际上率先实现了量子博弈实验。杜江峰小组首先在理论上研究了“ 囚徒困境 ”对局中两个游戏者手持粒子相互间的量子纠缠程度与对局中纳什均衡点的关系。他们发现，当这个纠缠程度较小时，对局与经典博弈的情况没什么不同，“ 两个游戏者都采取策略 B ”仍然是局中唯一的纳什均衡点。当纠缠程度增大一些时，对局中将出现两个纳什均衡点，从某种意义上说，这时的对局处在一种不稳定的状态。而当游戏者手中粒子的纠缠大到一定程度时，对局中将只

有 Eisert 文章中所给出的那一个纳什均衡点。杜江峰小组利用核磁共振设备实现了量子博弈。在他们的实验中，氢原子的核自旋状态充当了两个游戏者手中的粒子。科学家们使用一系列射频磁脉冲对这些粒子的状态进行测控。他们成功的制备了不同纠缠程度的粒子态，并模拟两个游戏者按照不同情况下对局中纳什均衡所对应的策略对这些粒子进行了相应的么正变换。之后，实验者测量了一个游戏者的收益。实验测得的收益与理论预言吻合的相当好。

杜江峰研究小组“量子博弈”实验实现工作四月初在 Physical Review Letter 发表后短短几周，就受到了国际量子信息界的广泛关注。英国《自然杂志》发表了题为《两原子计算机博奕每一个人都是赢家》的专题文章，指出了杜江峰及其合作者演示了量子博奕的新现象：如果使用量子策略，在博奕中能够出现双赢的局面。 他们的工作显示了量子博奕中的奇特性质：随着纠缠程度从零增加，博奕将被重复两次：第一次两个游戏者中的一个可能得到更好的结果，而不是像在经典博奕他们的收益都很差。第二次， 完全量子博奕出现，两个博奕者都同时取得最大收益。