1、量子信息优势

之前说过，比特信息是开关，量子信息是旋钮，它包含了无穷多的信息，并且，它在计算速度上也是惊人的快，譬如想要知道一个函数在这个 n 比特体系上的效果，需要 2^n 次操作，而在量子比特中，只需一次操作就能得到结果，不过由于它独特的测量性，导致它一次测量，会决定所有的量子位，所以如要得到我们想要的结果，需要非常巧妙的运算。

2、应用

或许学到现在，你我感觉量子计算离普通人还很遥远，确实，很多应用尚处于演示阶段，还未真正造出使用价值的量子计算机，它的应用在量子计算方面，有量子因数分解（破解最常用的密码体系）和量子搜索（用途最广泛的量子算法）。在量子通信方面，有量子隐形传态和量子密码术。

A、量子因数分解

量子因数分解就是把一个合数分解成质因数的乘积，例如 21 = 3 × 7。如何分解一个数字 N。最容易想到的算法，是从 2 开始往上，一个一个地试验能否整除 N，一直到 N 的平方根为止。如果 N 用二进制表示是个 n 位数，即 N 约等于 2^n，那么尝试的次数大致就是 $2^{n/2}$，任何指数增长的计算量都是不可计算的（多项式问题归为可计算的）由此可以看出因数分解的一个特点：它的逆操作，**即算出两个质数的乘积，是非常容易的；而计算质数，却是非常困难的。**这种"易守难攻"的特性，使它在密码学中得到了重要的应用。

因数分解的困难性，是现在世界上最常用的密码系统"RSA"的基础。RSA 是一种"公开密钥密码体系"，它的公钥（即加密时用到的参数）是对全世界所有人公开的。为什么敢公开？因为这个**公钥是一个很大的合数，解密需要把它分解成两个质数**，而发布者相信别人在正常的时间内解不开。但 RSA 有很大的隐患，第一，也许某些国家已经掌握了更好的解密算法，只是未公开；第二，量子计算机可以轻而易举的破解密码。但仍有大部分在使用 RSA 密钥体系，因为真正使用的量子算法是非常难以实现的。

它目前的发展状况与经典计算机比起，还处于早期阶段，在实验上分解的最大的数是 291311 = 523 × 557，是由中国科学技术大学的杜江峰和彭新华等人在 2017 年实现的。你可能会问，只能分解这么小的数，为何还要用它？然而，量子计算代表着未来，它所能实现的目标远超经典计算机，所以有很多科学家不惜辛苦的研究它。另外，量子计算机是一种统称，它也需要载体，就好比经典计算机有石墨烯、单晶硅一样，我国最先进的单光子量子计算机是以光子为运算载体的。

B、量子搜索

一本花名册，无规律排序，要想找到某个特定名字，需要 2^{n-1} 运算，而量子算法的基本思路是：把所有的解（搜索问题的解可能不止一个）对应的态矢量记为$|\omega\rangle$，初始状态对应的态矢量记为$|s\rangle$。我们不知道$|\omega\rangle$是什么，但算法可以把态矢量向$|\omega\rangle$的方向旋转，每次旋转都靠近一点。经过 N 的平方根量级的步数，就可以以 50%的置信度找到解。量子搜索算法付出的代价，是结果不再是完全确定的。有可能你本来想找张三丰，实际找到的却是张无忌。**无格式搜索的量子算法对经典算法只是平方级的改进**，

√N = 2n/2 还是指数增长，没有发生质的变化，仍然是不可计算。但是这个改进已经非常大了。如果 N 等于一亿，这就是一万倍的节约。

以上是量子计算方面的应用，接下来是量子通信方面的运用。

C、量子隐形传态

量子隐形传态到底是什么呢？它是 1993 年设计出来的一种实验方案，把粒子 A 的量子状态（不需要事先测量 A 的状态）传输给远处的粒子 B，让粒子 B 的状态变成粒子 A 最初的状态，需要注意的是，它传的是状态而不是粒子，并且，在 A 的状态传送给 B 以后，A 的状态将不复存在，换句话说，量子隐形传态是状态的移动，不是复制，总而言之，**量子隐形传态是以不高于光速的速度、破坏性地把一个体系的未知状态传输给另一个体系**。

D、量子密码术

在学习量子密码术之前，先来上一堂简短的密码学课程。

把明文变化成密文，需要算法和密钥，譬如说 fly at once 是明文，而“在英文字母表上前进 x 步”是算法，这里 x=1 是密钥，因此得到密文“gmz bu podf”。保密学中重要的一点是隐藏信息，但是别依托隐藏算法，算法是极易遭泄露的，而是设计好的密钥，所以人们在设计密码时，假设敌方已经知道算法，接下来就是想法设法隐藏密钥。

在**对称密码体制**，A 和 B 用的是同一套算法和密钥，A 用密钥将其转换为密文，B 用密钥将密文反解出明文。关于密钥的设计，这里就不做过多阐述了，现在密钥的设计已经很完善了，真正的难题在于密钥分发上，即怎么把密钥从 A 传给 B，因此引入了**非对称密码体制**（**公钥密码体制**）A 只负责发送密文，B 只负责解密，因此，B 在接受之前，先向 A 发送一个公钥，A 收到公钥后，将密文打包进去，B 收到之后，再用私钥解开公钥，最后用密钥解开密文，相比之前，多了公钥和私钥体系，公钥是大家都可以知道的，但私钥只有 B 一方知道，因此中间信息的传递变得更加安全了。这里公私钥体系可以用 RSA 因数密码，即公钥是一个很大的合数，私钥是两个质数，但之前也说过，这种 RSA 算法也不是绝对的安全，只是不知道是否有人掌握了量子解密算法。

一句话总结目前密码学的困境，**对称密码体制本身是安全的，但分发密钥是漏洞。非对称密码体制不需要信使，但你又会担心它被数学方法破解**。

量子密码术可以解决这个矛盾，回归到对称密码体制，这里的难点是密钥分发问题，现在不需要传输密钥了，因为量子的叠加、测量和纠缠三大特性使得 EPR 粒子对的态矢量可以同时转换成同一状态，即 A 和 B 可以不约而同的获得密钥！这样的过程被称为量子密钥分发。实现该过程有很多方法，最简单也最常用的是不使用量子纠缠的单粒子实现方案，即使用三大特性的前两个。