# 第 11 章 现代光学的兴起

## 11.9 量子信息光学

量子特性在信息领域中有着独特的功能，有可能在提高运算速度、确保信息安全、增大信息容量和提高检测精度等方面突破现有经典信息系统的极限，于是便诞生了一门新的学科分支量子信息光学。它是量子力学与信息光学相结合的产物。在 20 世纪 70—90 年代里，这门学科在理论和实验上已经取得了重要突破，引起了广泛重视。人们普遍相信，量子信息光学必将在 21 世纪发挥巨大威力。

### 11.9.1 量子计算机与量子算法

1982 年费因曼（R.Feynman）最先指出，采用经典计算机不可能有效地模拟量子力学系统。他建议，要有效地模拟量子力学系统，惟一的途径就是运用另一量子力学系统。他的意思就是，只有建立在量子力学定律的计算机，才能用于模拟量子力学系统。我们知道，经典计算机与量子系统遵从不同的物理规律，用于描述量子态演化所需要的经典信息量，远远大于用来以同样精度描述相应的经典系统所需的经典信息量。量子计算则可以精确而方便地实现这种模拟。采用少数量子比特的量子计算机可以进行有效的量子模拟。

1985 年，道奇（D.Deutsch）第一个明确地提出，在量子计算机上运算比在经典计算机上有可能更有效地计算。在提出这个问题的同时，他进一步推广了量子计算理论，发展了普适量子计算机和量子图灵机；1989 年，道奇又进一步提出了量子计算网络的概念，还设计了第一种量子算法。

1994 年，肖尔（P.W.Shor）提出量子平行算法[[1]](#footnote-1)，证明量子计算机可以破译目前广泛使用的 RSA（Rivest-Shamir-Adleman）密码体系。肖尔算法可以有效地用来进行大数因子分解。大数因子分解是现在广泛用于电子银行、网络等领域的公开密钥体系 RSA 安全性的依据。采用现有计算机对数 *N*（二进制长度为 lg*N*）做因子分解，其运算步骤（时间）随输入长度（lg*N*）指数增长。目前已经成功被分解的最大数为 129 位，是 1994 年同时使用 1 600 个工作站，花了 8 个月才完成的。用同样的计算能力来分解 1 000 位的数，则要花 1 025 年。将来如果有了量子计算机，采用肖尔算法，就可以在几分之一秒内实现 1 000 位数的因子分解。可见肖尔量子算法的威力。

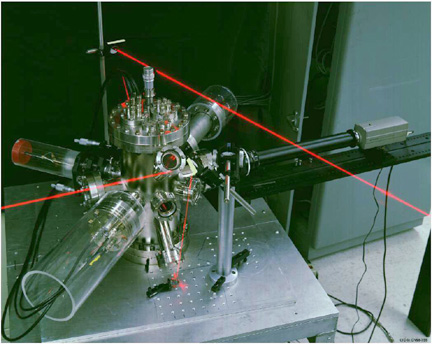


图 11 – 33 用于量子计算的激光设备，可以使钙离子在两态之间变换

随着激光与光电子技术的成熟以及非线性光学与量子光学的发展，已经能够在单量子水平上产生、控制和操纵光，加之光学器件易于集成，量子计算机已经是指日可待了。

### 11.9.2 量子态的制备与操作

在量子信息处理系统中，量子态是信息的携带者，量子信息的提取、传送和处理实质上就是量子态的制备和操作过程。目前，已设计出诸多新的原理和方法实现对量子态的制备与操作，特别是采用腔量子电动力学与量子测量相结合的方法，可以实现众多光场量子态和原子量子态的制备。量子光学实验科学家正积极探究实现单光子福克（Fock）态，光量缠态、光场与原子纠缠态及其他任意量子态的产生、测量、控制与传输方法，并已取得很大进展。这些研究为以光子作为信息载体的光量子信息系统奠定了基础。它们是量子逻辑门、量子网络等硬件设备的基本单元。在量子信息中，用一定量子体系的量子态对信息进行编码，即以量子态作为信息的载体，按照量子力学的态叠加原理等规律对量子态进行传送或逻辑操作，从而达到量子信息处理的目的。

### 11.9.3 量子离物传态

1993 年，IBM 研究所的本内特（C.Bennett）和他的研究小组发明了一种特殊的方法，称为量子离物传态（quantum teleportation）。他们在介绍自己的发明时[[2]](#footnote-2)，用了两个人作为发送方和接受方的代表。爱利斯（Alice）和博布（Bob）分处两地，想要传递一些量子信息。他们只需送出少量的经典信息，就可以传输量子信息。其好处在于“经典的”信息非常强劲，对于环境的相互作用很不敏感。要做出这件事，爱利斯和博布还必须持有一些分享的纠缠。更精确地说，博布在过去的某一刻创建了量子比特的纠缠对

| *χ* 〉 = | 0 〉 | 0 〉 + | 1 〉 | 1 〉

并仔细地把其中一半交给爱利斯。爱利斯有了这一资源，以后在任何时候都可以给博布传送量子态 | *ψ* 〉，方法就是对 | *ψ* 〉 和她的那份 | *χ* 〉 进行一次特殊的量子测量，然后用经典方法把测量的结果传送给博布。博布可以复制 *ψ* 〉，而爱利斯再也没有她那一份量子态。

光态的量子离物传态已经在世界上好几个实验室得到了实现。例如，1997 年底到 1998 年初奥地利与意大利的试验小组分别利用 Ⅱ 类相位匹配下转换过程自发辐射产生的孪生光子对作为 EPR 粒子对，把单光子偏振态作为待传送的量子态，成功地实现了单光子偏振态的离物传态。1997 年美国加州理工学院的金布尔小组利用运转于阈值以下的连续光学参量振荡器产生的两个压缩真空态组成 EPR 纠缠源，从实验上实现了任意量子态的传输。

### 11.9.4 量子密码术

量子密码的安全性可以从量子力学的基本原理得到保证。窃听者的策略无非两类：一是通过对携带着经典信息的量子态进行测量，从测量结果获取所需的信息。但是量子力学的基本原理告诉我们，对量子态的测量会干扰量子态本身，因此，这种窃听方式必然会留下痕迹而被合法用户所发现。二是避开直接量子测量而采用量子复制机来复制传送信息的量子态，窃听者将原量子态传送给乙，而留下复制的量子态进行测量以窃取信息，这样就不会留下任何会被发现的痕迹。但是量子不可克隆定理确保窃听者不会成功，任何物理上可行的量子复制机都不可能克隆出与输入量子态完全一样的量子态来。

目前世界各国正致力于这方面的研究并在实验上取得重要进展，已经在自由空间中实现了 10 公里的密钥传送，在光纤上实现了 67 公里的密钥传送。

1. Shor P W.In：Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science.IEEE Computer Society Press，Los Alamitos，CA，1994.124 ~ 134 [↑](#footnote-ref-1)
2. Bennett C H，et al.Phys.Rev.Lett.，1993，70：1895 ~ 1899 [↑](#footnote-ref-2)