浅谈量子密码术和保密通信

冯向华

密码术是对信息进行编码实现隐藏信息的一门学问。例如你想把信用卡号码告诉商家来买东西，但不希望任何有恶意的第三方截取你的信用卡号码，采用密码方法可以隐藏和保护需要保密的消息，使未受权者不能提取信息。

被隐藏消息称做明文，密码可将明文变换成另一种隐藏的形式，称为密文。这种变换过程称做加密，其逆过程，即由密文恢复出原明文的过程称为解密。对明文进行加密时所采用的一组规则称做加密算法，对密文进行解密时所采用的一组规则称做解密算法。加密和解密算法的操作通常都是在一组密钥控制下进行的，密钥是密码体制安全保密的关键。密码体制分为单钥体制和双钥体制。

单钥体制的加密密码和解密密码相同。例如通信双方爱丽斯和鲍伯共享一个只有他们知道的密钥。密钥可以是一个二进制随机位串，爱丽斯用这个密钥把要传给鲍伯的信息加密，然后把加密信息发给鲍伯。鲍伯收到信息后，利用他知道的密钥，对加密信息施加逆变换，以恢复原始信息。

单钥体制的保密性主要取决于密码的安全性，一个重要的问题是如何将密钥安全可靠地分配给通信对方。恶意的第三方可能在密钥分配时通过各种办法窃听(如搭线窃听、电磁窃听、声音窃听等)，然后用截获的密钥来解密传送的机密信息。传统的物理信道当有人监测窃听时，通信双方不会知道窃听在何时发生。例如，信使所带密码本可能被秘密设置的高分辨率 X 射线扫描，或用先进的成像技术读出，磁带、光盘或无线电波中载荷的信息被复制或截获时都难以发现。现代信息系统还可能遭受另一类攻击，非法入侵者、攻击者或黑客主动向系统窜扰，采用删除、增添、重放、伪造等窜改手段向系统注入假消息，达到利己害人的目的。

量子密码术能够使爱丽斯和鲍伯的秘密不会受到威胁。当信息以量子为载体时，由量子力学的测不准原理知，对任何一个物理量的测量都不可避免地产生对另一物理量的干扰。于是，当爱丽斯和鲍伯要传送密钥时，若有人窃听，窃听者因对爱丽斯和鲍伯用来进行密钥确定的信道带来干扰从而被发现。爱丽斯和鲍伯可以丢弃有窃听者出现时建立的密钥位，并重新确定密钥。

双钥密码体制的最大特点是采用两个密钥将加密和解密能力分开：一个公开作加密密钥；一个为用户专用，作为解密密钥，通信双方无需事先交换密钥就可以进行保密通信。鲍伯公布一个“公钥”，让所有人都可以得到，爱丽斯用这个密钥把送给鲍伯的消息加密。有趣的是，第三方不可能用鲍伯的公钥解密！因为加密变换取得非常巧妙，仅从公开的公钥或密文分析出明文或密钥，在计算上是不可行的。鲍伯有一个与公钥配对的私钥，他用这两个密钥可以很容易地进行解密。这个私钥只有鲍伯知道，故在别人不太可能具有只用公钥就能解密的前提下，鲍伯可以相信，只有他能阅读爱丽斯传来的内容。

公钥密码的安全性的关键在于，仅利用公钥进行解密极其困难。目前最广泛采用的公钥密码体制——RSA 密码体制的安全性是建立在用经典计算机分解因数非常困难的这个信念之上。然而，肖尔(Shor)的在量子计算机上分解因数的快速算法可以用于破解 RSA！类似地，如果知道一个解离散对数问题的快速算法——肖尔针对离散对数问题的量子算法，有些公钥密码就会被破解。量子计算机在攻破密码系统上的这项应用，引发了对量子计算与量子信息研究的很大兴趣。

量子密码已被实验证明是可行的，但要用于实际商用尚需进一步研究和开发。在未来的光子时代。量子计算机的计算能力可能足以对付现在普遍采用的各种密码体制，用它来分解大整数、进行离散对数、加解密、搜索密钥等运算的速度将提高许多量

级。那时量子密码术可能会提供一种真正安全的密钥分配方式,从而对单钥密码体制提供新的支持。

量子密码术的原理和实现方案

量子密码术基于量子力学理论，它与经典力学最重要的差别是其互补性，其本质是量子系统在被测量时会受到扰动。这可由量子观测的不确定性来表述。令量子算子$\hat{A}$和$\hat{B}$表示量子系统的两个实际观测量,若

$$[\hat{A},\hat{B}]=\hat{A}\hat{B}-\hat{B}\hat{A}\neq 0$$

则称这两个观测量是不可对易的，它们必满足海森伯测不准关系式：

$$\left((\Delta\hat{A})\right)^2\cdot\left((\Delta\hat{B})^2\right)\geqslant\frac{1}{4}\left|\left([\hat{A},\hat{B}]\right)\right|^2$$

和这一性质相联系的是一对物理性质之间的互补性,测量一种性质必将干扰另一性质,任何试图精确测量$\hat{A},\hat{B}$中的一个量,必将以另一个量的“含糊”为代价。

量子密码通信的实现依赖于两点:(1)基本量子力学效应(如测不准原理,贝尔(Bell)原理,量子不可克隆定理);(2)量子密钥分配协议。

量子密码术能提供一种真正安全的密钥分配方式。因为量子密钥分配是通信双方通过交换携带量子信息的物理态、在他们之间建立起一个绝对安全的密钥串的过程。由于一个未知的量子态是不可能被完全克隆的，窃听者艾文在对爱丽斯发出的量子态未知的情况下,无论采取何种窃听方式进行窃听,总会扰动在爱丽斯和鲍伯之间传输的量子态。这样,爱丽斯和鲍伯通过比较他们最初得到密钥串的一小部分结果,计算出他们初步建立的密钥串的误码率,就可以知道他们在通信的时候，艾文有没有进行窃听。如果爱丽斯和鲍伯发现他们所得到的密钥串的误码率太大,他们就放弃此次通信结果,重新开始,再进行一次。如果他们发现所得到的误码率比较小,即理论上可以证明是安全的，那么他们可以利用保密放大的方法,从中提出安全的密钥串。目前实现量子密码的方案主要有如下几种：

基于两种共轭基的四态方案　即由贝内特(C. H. Bennet)和布雷萨德(G. Brassard)在1984年提出来的BB84方案。这是最早的关于量子密钥分配的实验方案。我们用极化光子来说明BB84方案。方案中用到两组基,构成四个态：

$$|+45°\rangle=\frac{1}{\sqrt{2}}(|H\rangle+|V\rangle)$$

$$|-45°\rangle=\frac{1}{\sqrt{2}}(|H\rangle+|V\rangle)\qquad\text{记为}\otimes\text{基,}$$

$$|R\rangle=\frac{1}{\sqrt{2}}(|H\rangle+i|V\rangle)$$

$$|L\rangle=\frac{1}{\sqrt{2}}(|H\rangle+i|V\rangle)\qquad\text{记为}\oplus\text{基。}$$

通信双方事先约定的编码方案为：对于⊗基中的$|+45°\rangle$态(用符号↘表示)和⊕基中的$|R\rangle$态(用符号↕表示)编码为“1”;对于⊗中的$|-45°\rangle$态(用符号↗表示)和⊕基中的$|L\rangle$态(用符号↔表示)编码为“0”。

表1

爱丽斯随机位	1	0	1	1	0	0	1	0	1	1	1
爱丽斯的基	⊗	⊕	⊕	⊕	⊕	⊕	⊗	⊗	⊕	⊗	⊕
爱丽斯发射的极化光子	↘	↔	↕	↕	↔	↔	↘	↗	↕	↘	↕
鲍伯的基	⊗	⊕	⊕	⊗	⊗	⊕	⊗	⊕	⊗	⊗	⊕
鲍伯接收的位	1		1	0	0	0		1	1	1	1
爱丽斯说正确的基	y		y	n	n	y		n	n	y	y
保留的位	1		1			0				1	1
位的比较			1								
爱丽斯确认			y							y	
密钥	1					0					1

表1详细说明如下：

(1)、爱丽斯发送一系列编码的光子，编码方法为把要发送的光子制备在随机选取的4个光子极化态之一上,编码光子的发送按时序进行,即一个时间间隔发送一个光子。

(2)、鲍伯的时序与爱丽斯相同。在每一个时间间隔鲍伯随机选取两种测量基之一（⊗基或⊕基）对接收到的光子进行测量,并记录测量结果。

(3)、当传输完毕，爱丽斯和鲍伯通过经典信道(如电话、因特网等)公开通信。鲍伯告诉爱丽斯在哪一个时间空挡接收到了光子（有可能接收不到),并告诉爱丽斯用哪一个基对接收到的光子进行测量,但是不公布测量结果(0或1)。同时,爱丽斯告诉鲍伯哪一次测量选用了正确的基。

(4)、双方丢弃使用不同基的情况，保留使用相同基的结果,如果通信不存在窃听,那么保留的测量结果就是双方共享的密钥。

(5)、爱丽斯和鲍伯随机选取一小部分密钥来验证通信误码率,如果误码率在允许范围之内,就可以确信没有窃听者存在,保证通信是成功的,去除用来

验证的小段密钥剩下的就是“绝对安全”的密钥;如果误码率超出允许的范围，则可能是信道噪声或者窃听者造成的,舍弃这一次通信生成的密钥。

基于两个非正交量子态性质的贝内特(Bennett)B92 方案　由于量子不可克隆定律的限制,如果测量不会扰动两个非正交量子态，那么这个测量就不可能获取任何可区分这两个非正交量子态的信息,因此,贝内特提出了只需要利用两个非正交量子态来实现量子密钥分配的 B92 方案。首先,合法通信者爱丽斯和鲍伯选择光子的任何两套共轭的测量基(这里我们取偏振方向为 0° 和 90°、45°和 135°的两组线偏振态,并定义 0°编码为“0”、45° 编码为“1”),但只测量其中两个非正交的量子态 (这里取 0°和 45°)，即从互为共轭的两组量子态中各选一个进行测量。

表 2

	1	0	1	0	1	0	0	1	1	0	1	1	1
a	↗	↔	↗	↔	↗	↔	↔	↗	↗	↔	↗	↗	↗
b	↕	↘	↘	↕	↕	↘	↘	↕	↘	↘	↕	↕	↘
c	y	n	n	n	y	y	y	n	n	y	y	n	n
d	1									0	1		
e										0			
f	1					0	0				1		

与表 2 对应建立密钥的具体步骤如下：

(a)　爱丽斯以 0°或 45°光子线偏振态随机向鲍伯发射选定的光子脉冲。

(b)　鲍伯随机选取 90°或 135° 的方向的检偏基检测,当鲍伯的检测方向与爱丽斯所选方向垂直,探测器完全接收不到光子。当成 45° 时则有 50%的概率接受到光子,一旦鲍伯测到光子,鲍伯就可推测出爱丽斯发出的光子的偏振态。

(c)　然后鲍伯通过公共信道告诉爱丽斯所接收到光子的情况,但不公布测量基,并双方放弃没有测量到的数据.此时如无窃听或干扰.爱丽斯和鲍伯双方则共同拥有一套相同的随机序列数。

(d)　鲍伯再把接收到的光子转化为量子位(0 或 1),他们获得了密码的粗码。

(e)　鲍伯随便公布某些位，供爱丽斯确定有无错误(验证鲍伯的身份)。

(f)　经爱丽斯确认无误断定无人窃听后，剩下的位就可留下建立为密钥。这种方法比 BB84 协议简单,但代价是有 50%正确测量将得不到结果,B92 方案的效率仅为 BB84 方案的一半。

基于量子纠缠态的爱克特(Ekert)的 E91 方案　爱因斯坦关于量子力学不完备的结论被称为“EPR 佯谬”,实际上 EPR 佯谬利用的是二粒子体系的一个纠缠态。E91 方案的原理是利用 EPR 效应(量子力学非局域性),即制备一对 EPR 关联光子,对通信双方具有确定、不变的关联,如测得其中一个光子的极化态向上，同时遥远的另一个光子的极化态一定朝下,且不随时间和空间的变化而改变。因此，用两个具有确定关联的光场来建立通信双方间共享密钥的信息载体，任何窃听都会破坏这种关联而被发现。

其通信过程如图 1 所示:首先,由 EPR 源产生的光子对分别朝±Z 方向发送到合法的用户爱丽斯和鲍伯,爱丽斯任意选择检偏基(线偏振基或圆偏振基)对 EPR 对中的其中一个光子进行测量,由 EPR 对的关联特性，爱丽斯的测量结果将会使另一个光子投影到特定的极化光子态上；同时鲍伯也随机用检偏基测量接收到的 EPR 关联对的另一个光子,并记录测量结果；然后鲍伯通过公共信道公开其使用的测量基,但不公布测量结果,爱丽斯告诉鲍伯那些检偏基选对了，双方保留采用正确测量基测量光子态的结果;再根据双方约定的编码方案,对保存的光子态进行编码,从而建立密钥。

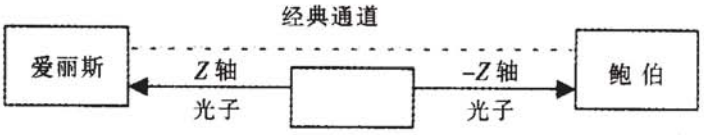

图 1　基于贝尔理论的量子密码通信示意图

E91 方案与 BB84 不同的是，发送方通过测量 EPR 对中的一个光子从而制备了接受方的光子态,而 BB84 方案则由发送方先制备光子态再发送给接收方。利用纠缠光子对进行量子密钥分配在远距离通信上比利用单光子态要好，操纵纠缠态的技术可以引入到基于 EPR 关联态的密钥分配中,如量子隐形传态、纠缠交换、纠缠纯化、量子中继器等。这些技术大大加强了量子远程通信的可行性。

量子密码通信未来的发展前景

目前，阻碍量子密码术走向实用还存在一些技术问题:首先,制造出高效的单光子源比较困难;其次，需要工作在所需波长高效的单光子探测器还未

发射“引力探测器 B”验证广义相对论

奇 云

只有不断向既有学说发起挑战，才是不断带来革命性发现的科学探索精神。美国东部时间 2004 年 4 月 20 日 13 时，美国宇航局“引力探测器 B”卫星成功升空，它的使命就是对世界著名科学家爱因斯坦 1916 年提出的广义相对论进行进一步验证。

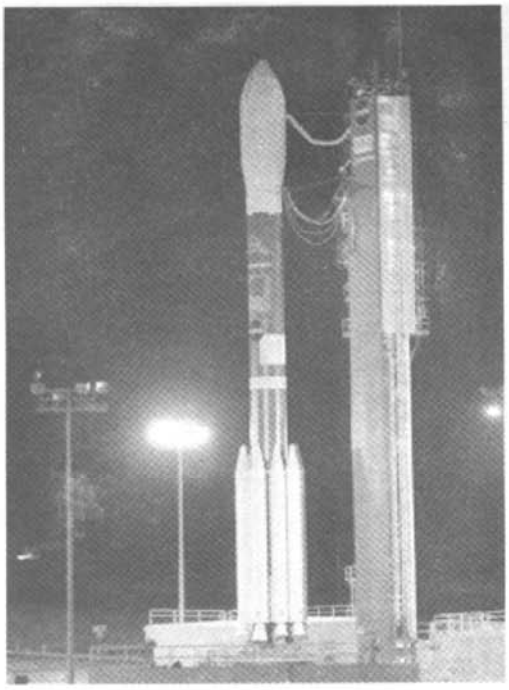

图 1 发射

一个命运多舛的探测卫星

20 世纪 30 年代，英国著名剧作家肖伯纳曾说过一段名言：古希腊天文学家托勒密创立地心宇宙学说，其统治地位延续了 2000 年；英国物理学家牛顿提出万有引力学说，200 年后受到质疑；爱因斯坦发表相对论学说，究竟能维持多久则不得而知。美国东部时间 2004 年 4 月 20 日 13 时（北京时间 21 日凌晨 1 时），美国宇航局（NASA）的“引力探测器 B”（Gravity Probe B，简称 GP-B）卫星从加利福尼亚州范登堡（Vandenberg）空军基地火箭发射场成功升空（图 1），其使命就是对爱因斯坦 1916 年提出的广义相对论进行进一步验证。

引力探测器 B 原定于 2004 年 4 月 19 日由波音德尔塔 2 号（Delta 2）火箭发射升空。但由于地面控制人员不能证实搭载引力探测器 B 发射的火箭是否装备了所有正确的飞行软件，发射总监在最后一秒钟终止了火箭的发射。

引力探测器 B 由美国宇航局出资，斯坦福大学负责设计，洛克希德-马丁公司负责制造。

引力探测器 B 的历史可以追溯到将近半个世纪前。1959 年，斯坦福大学的物理系主任莱昂纳德·席夫（Leonard Schiff）和国防部的普（George Pugh）各自提出了用陀螺仪检验广义相对论的方案。1963 年，美国宇航局第一次为这个项目拨款。然而，当时的条件根本不足以实施这项计划。整个六七十年代，斯坦福的研究组都在进行 GP-A 的前期研究工作。

在这期间，1976 年，美国宇航局发射了引力探测 A 卫星（GP-A）。探测器携带了一只原子钟。这个只持续了 1 小时 55 分的实验检验了广义相对论所预言的引力红移效应--引力场的强度会影响时钟

成熟；第三，要防止窃听者假扮合法通信者来非法获取通信信息，必须结合一些经典技术如保密加强纠错及认证技术等，这在一定程度上也减弱了量子密码术在技术上的优势；第四，量子密码系统即使没有窃听者窃听的情况下，由于系统自身的不稳定性也会造成一定的长期误码率，使通信的质量受到影响；最后，阻碍量子密码术走向实用很重要的非技术问题则是经济问题，因为量子通信技术必须与传统的通信技术来竞争以获得市场，而这些传统方法在长距离上以及成本费用上更低，从而使量子密码通信技术处于不利地位。但是从总的发展趋势看，经典保密通信的成本是逐年提高，而量子密码通信正随量子密码技术的发展其成本在降低。

虽然现在量子密码技术的理论和实验条件还不成熟，但从理论设想到现在已实现在常规光缆线路上传输达几十千米的量子密码通信系统只用了短短几年的时间，发展如此之迅速，这足以证明量子密码通信技术的强大生命力，它的前途是不可限量的。期望在不久的将来，随着单光子探测等技术的不断发展，量子密码通信技术在全光网络和卫星通信等领域的应用潜力会不断挖掘并成为现实。量子密码已是密码学领域的一个新的成员，可能成为光通信网络中数据保护的有力工具。而且在将来，要对付拥有量子计算能力的密码破译者，量子密码可能是唯一的选择。

（郑州信息工程大学理学院数理系 450001）