量子密码术

郭光灿
(中国科技大学物理系)

自从人类有了通信的需要以来,怎样在通信中保密以及如何破译敌方的密码就引起了广泛的兴趣.保密通信不仅在军事、国防等领域发挥独特作用,而且在经济和私人通信等方面也日益重要.随着电信业的全球化,以及多媒体技术在信息领域的广泛应用,在高度串接的宽带光学网络中,信息安全性越来越成为重要的热门课题.例如,未来可使用视频网络来召开重要的会议,如何不让非法接收者从信息网络中窃取会议情况,显然成为至关重要的问题.目前的移动通信很容易被人窃听,这也提醒人们有必要关心信息安全问题.总之,信息交流越发达,信息安全问题就越重要.

一、密码术的概述

提供信息安全的技术有多种多样.最方便的方法是所谓密码术,即将欲传送的信息采用某种方法进行干扰,以致唯有信息通道的合法用户才能从中恢复出传递的信息.密码技术的关键在于信息通道的合法用户掌握一组秘密的随机数码,使用这组数码及某种特殊的算法可以对信息进行加密.这组数码叫做密钥.保密通信的基本思想是唯有掌握密钥的人才可以轻易地重现传递的信息,而没有密钥的人要获得信息却异常的困难.信息的安全性主要依赖于密钥的秘密性.密钥可以是一种信息通道的合法用户共享的秘密信息,也可以是每个用户掌握各自的密钥.密钥每重复使用一次,通道的安全性就会下降一点,因为窃听者多一次机会去分析加密数据,以最终获知合法用户所使用的密钥.随着通信网络中信息交换量的增大,密钥的管理和传输便变成关键性的问题.两个用户必须确保他们所共享或独有的密钥的安全性,并且要经常更换这些密钥,以保证通信体系的安全.

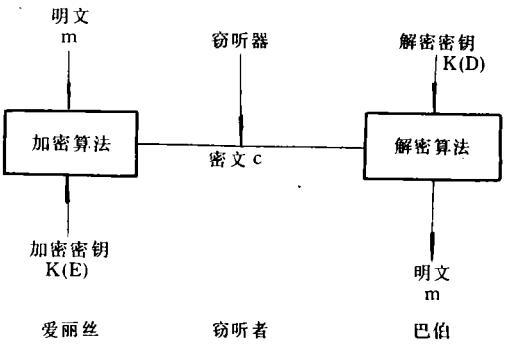


图 1 密码通信技术的基本过程

图 1 是通信中密码技术的基本过程.设想爱丽丝(Alice)小阻与她的男友巴伯(Bob)正在进行秘密通信.爱丽丝想要发送信息 m 给巴伯.在数字通信中 m 是二进制(1,0)的数定串,m 称为明文.爱丽丝拥有一串秘密的随机数码 K(E)(密钥),她使用某种加密算法将明文 m 变换成密码文件 C(称为密文).密文 C 在公开信道中传输.巴伯接收到密文并且应用他的密钥 K(D)和解密算法进行反变换,最终获得明文 m.现有两种密码体系,一种是传统的或对称的密码,在这个体系中很容易从 K(E)得到 K(D),另一种是公开的或非对称的密码,通过计算不可能从 K(E)得到 K(D).假定有第三者企图窃听爱丽丝和巴伯之间所传递的信息,设想这位窃听者已经得知爱丽丝的加密算法和巴伯的解密算法(事实上,在大部分场合中加密和解密算法对窃听者来说也是保密的,但某些密码体系中,主要的加密算法确实是公开的).窃听者从公开信道中获取密文.这时,通道的保密性取决于密钥的保密性.非对称或公开密钥的加密体系尤为重要,因为它可以为事先没有共享密钥的双方提供安全的通信.但是这个体系的安全性是基于诸如把一个大数分解成为两个素

数之积这样的独特数学操作的困难性之上的.虽然这类数学操作目前看来是极其困难的,但在数学上并未严格证明这种操作是绝对不可能的.因此,公开密钥体系的安全性在严格数学的意义上并不可靠.

现在唯一能确保密性(不可破译)的密码体系是所谓 Vernam 密码,这是一种对称加密体系,它要求密钥应与明文一样长,而且密钥只能使用一次(便笺式的).在这个体系中,K(D)必须等于 K(E).这种不可破译的密码体系需要有双方共享的庞大密钥,因此,密钥的传递和管理成为这种密码体系实用化的关键问题.Vernam 密码在它发明之后很长一段时间内并没有得到广泛应用.只有在特别重要的信息通道(例如,莫斯科—华盛顿之间的热线电话)才使用这种技术.目前所使用的大多数对称密码体系,密钥比信息短得多,它只能提供一个最短的破译时间,超过这个时间,密码通信就不安全.当然人们采用许多技术方案不断地增大破译的难度,但原则上它们都是可破译的.

从物理学的角度看,现有的密码通信都属于经典物理的范畴,携带着信息的载体是经典的电磁波(或光波),密钥(俗称为密码本)本身若被非法用户复制时,可以不被觉察,密钥在传递时被他人窃听,合法用户也无法识破.因此,经典密钥本身的安全性得不到绝对的保证,即使采用 Vernam 密码这种不可破译的密码体系,也无法杜绝被窃听的可能性.经典密钥原则上是可以窃听而不被发现的.当然,对密钥采取十分严厉的保安措施,或者通过信使或秘密通道来传送密钥,这些办法都有助于增加密钥的安全性,但却无法保证其绝对安全.

量子密码术是一种能确保密钥传输安全性的新技术,其安全性由物理学定律来保证,这种密码术有能力抵挡住强大的破译技术和计算工具的攻击.现有文献中所说的"量子密码"实质上只是指量子密钥的传递技术.量子密码术属于对称密码体系,但与现有的对称或非对称密码体系不同.它可实现不可破译、不可窃听的保密通信.这种量子技术一旦实用化,那么信息安全领域将会有重要的突破.

1976 年美国哥伦比亚大学的 S. J. Wiesner 最早提出将量子力学与密码术相结合,他撰写了一篇"共轭编码"的论文.或许是由于这种想法显得过于离奇,刊物编辑拒绝发表这篇论文.一直到了十几年之后的 1983 年,该论文才在"SIGACT NEW"上发表.幸运的是 C. H. Bennett 与 G. Brassard 在 70 年代末期了解到了这个思想,并在 1984 年完成了第一个量子密码的原理性实验,现称为 BB84 方案.目前,量子密码术的研究引起了人们广泛的兴趣,并在理论和实验方面取得了重要的进展.采用光纤传输线已实现 30 公里的密码传送并达到了每秒 20 千比特的数据传输率.量子密码术的实用化只是时间的问题,当前的研究方向在如何增大传输距离和提高比特率.

二、量子密码术的基本原理

采用量子通道来传送密钥,其安全性由物理定律本身来保证.因此,甚至在原则上也是不可能窃听到这种量子通道中的信息的.

现在已提出若干实现量子密码的方案,所有这些方案的核心在于应用到量子力学的几率特性,以及任何信息的提取(例如窃听)都会干扰通信通道.

现代科学业已证明,世界是按照量子力学的规律演变的,不管人们喜欢还是不喜欢,也不管人们习惯与否,都是如此.当然,在大多数场合,从我们日常生活的宏观尺度来看,单个量子事件的几率特性很不明显,事物的变化基本上是遵从经典物理的规律,但是在单个粒子(如光子,电子)的水准上,量子规律就发挥出了作用,量子特性不可忽略.量子密码术就是基于量子规律的.因此,为理解量子密码术的基本原理,我们需要熟悉支配着量子世界的规律.在这些规律中,对量子密码术起关键性作用的是海森堡不确定原理.这个原理是量子世界中粒子具有波-粒两象性的必然体现.该原理可以等效地表达为下列的论断:不可能测量某物体而又不干扰这个物体.测量过程本身必然要求被测体系和测量装置之间发生相互作用,这种相互作

用不可避免地会干扰被测体系，除非该体系在测量前被制备在某个特殊的态上.例如，我们想要确定电子的位置和动量，当我们增大测量电子动量的精度时，海森堡不确定性原理会使得我们越来越不能确定电子在那个空间位置上，在测量极限下，电子的动量完全被精确地确定，这时我们绝对不能知道电子的位置.同样地，若精确地测量电子的位置，则完全不可能知道电子的动量.这个结果不是仪器的性能问题，而是受到更深层次的量子规律的制约，任何先进的仪器和测量手段都无法突破海森堡不确定关系所给定的限制.

现在假定我们把一个光子制备到某个确定的偏振态上.这种态的制备等同于进行一次完全精确的测量.设想光子被制备在圆偏振态(左旋或右旋)上，由于圆偏振态与线偏振态之间有不确定关系，与电子的位置和动量的不确定关系类似，我们若精确地将光子制备在圆偏振态上，就意味着完全不能精确地了解其线偏振状态，光子处于任意线偏振态的几率完全相同.换句话讲，对处于圆偏振态的光子进行一次精确的线偏振(在水平和垂直两个方向上)测量.如果光子是可分割的，则有半个光子为垂直偏振、半个光子是水平偏振，但理论和实验均已证实，单个光子作为整体是不可分割的，因此这种测量结果决不会出现.按照量子力学的规律，在测量之前，我们可以预计测量结果有 50%几率的垂直偏振，有 50%几率为水平偏振，但无法预言，一次测量的结果应是垂直偏振还是水平偏振.在经典世界中，只要给出初始条件，由物理规律所预言的结果是完全确定的.但在量子世界中，人们能给出的预言是统计性的，无法预测单次测量的结果，除非被测体系事先已经处在特殊态上(例如，光子若事先处于水平偏振态、且采用线偏振装置测量，测量结果必定是水平偏振).

量子力学对测量结果的预言是统计性的，但每次测量的结果却是单一的，对上述圆偏振态的光子测量其线偏振状态，一次测量的结果只能是垂直和水平偏振当中的一个.我们知道，圆偏振可以看成水平偏振和垂直偏振的相干叠加.因此测量过程实质上实现了将这个叠加态投影到其中一个单值态.反过来看，若一次测量的结果是水平偏振，而事先并不知道光子在测量之前处在什么样的偏振状态，那么由一次测量的结果无法知道被测体系在测量之前的状态.换句话讲，单靠一次测量无法获得关于被测体系的信息，而一次测量又会使体系原来的信息消失掉.量子力学的这种几率特性正是量子密码术的物理基础.

现在我们以 BB84 方案为例来阐述量子密钥是如何在公开的信道中传输的.设想爱丽丝和巴伯事先约定：右旋圆偏振和垂直线偏振代表数字码的“1”，左旋圆偏振和水平线偏振代表数字码“0”.假定爱丽丝发出一个右旋圆偏振光子给巴伯(即她发出“1”)，当然巴伯并不知道爱丽丝选择了光子的这个偏振态，他将随意地选择测量圆偏振或者线偏振的装置.假设这次他正好用检偏器来测量光子的圆偏振态，于是他能确切地知道光子处于右旋圆偏振态(即他读出“1”)，正确地得到爱丽丝传送来的比特.现在假定有位窃听者想窃取爱丽丝和巴伯之间的密钥，当然他也不知道爱丽丝所发出光子的偏振态.为了获得编制在光子偏振态中的信息，他必须选择某一种测量偏振的装置——或者圆偏振，或者线偏振，但这两者不能同时测量.我们假定窃听者选择错了装置，他决定测量线偏振，于是他有 50%的几率测到垂直线偏振(即 50%几率读到正确码“1”)，另 50%的几率测到水平线偏振(50%几率读到误码“0”)，当然窃听者并不知道自己选错了测量仪器，他根据自己的测量结果制备一个有确定线偏振态的光子、发送给巴伯.巴伯本来选择了正确的仪器(圆偏振)，若窃听者不出现，他能以 100%的几率读到正确数码“1”.现在窃听者破坏了原来的通道，使得巴伯实际上接收到的不是爱丽丝的圆偏振光子，而是窃听者的线偏振光子.这时，巴伯只有 50%的几率能读出正确的比特(“1”).如果爱丽丝和巴伯事后公开地通报他们的结果，就会发现他们对传送的比特是“1”还是“0”有可能

不一致，也就是说，窃听者的存在使他们之间的误码率不为零.上述结果可由图 2 的示意中看清楚.量子密码方案就是要在爱丽丝和巴伯之间建立这样的关系，一旦有人企图窃听，就会不可避免地出现误码.

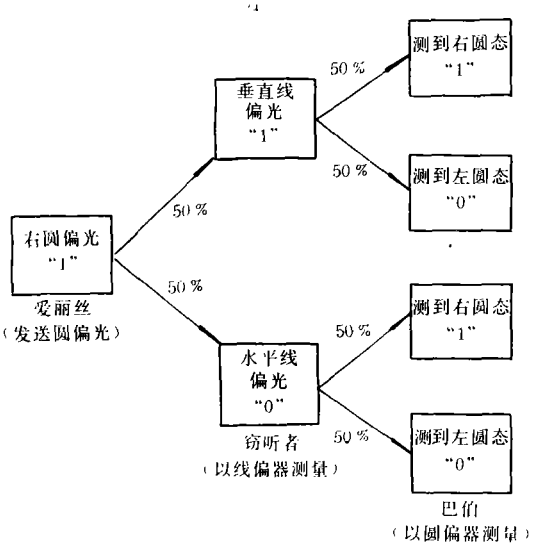


图 2　爱丽丝和巴伯之间某次量子通信的几率树

在图 2 所示的场合：爱丽丝发送圆偏振，巴伯选用正确的检偏仪器，窃听者选对检偏仪器和选错检偏仪器的几率各 50%.窃听者若选对检偏仪器测量圆偏振，则爱丽丝和巴伯通过比较测量的结果便无法发现窃听者的存在，即使窃听者选错检偏仪器，根据图 2 的几率树，这时窃听者仍然有一半几率不被发现.因此综合两种可能性，爱丽丝和巴伯比较一个比特，窃听者逃脱被发现的几率为 3／4.若在一系列的传送之后，爱丽丝和巴伯比较 $3M$ 个比特，窃听者不被发觉的几率为 $(3/4)^M$，当 M 很大时，这个几率就很小，例如，$M=100$，窃听者逃脱的几率为 3.2×10^{-13}，也就是说窃听者在十亿次中只有三次机会能侥幸地不触动警报器.

爱丽丝和巴伯基于单光子偏振特性的量子密码传输方案如下：

(1)爱丽丝发送一系列的单个光子，每发射一个光子时，随机地选取下列四个不同偏振态之中的一个：右旋＝“1”，左旋＝“0”，垂直＝“1”，水平＝“0”.她记录下她每次所选择的偏振态和编制在其中的比特(“1”或“0”).

(2)巴伯独立随机地选择圆偏振或线偏振的检偏仪器来测量每一个进来的光子的偏振并记录下测量结果(“0”或“1”).

(3)在全部传送和测量结束之后，巴伯通过公共通道告诉爱丽丝，他每次所选择的是哪一种检偏仪，但不公布他的测量结果.随后，爱丽丝根据巴伯选择的检偏仪就能确定巴伯在哪些测量中使用了正确的仪器，于是他们两人就约定抛弃巴伯选错仪器的事件，而把选对仪器的比特留下来作为他们共享的密钥 K.这样，量子密钥在他们之间就建立起来，这种密钥事先并不存在，只有在两人共同参与下才得以存在.

(4)在没有窃听者存在时，爱丽丝和巴伯各自拥有一组完全相同的随机比特序列作为密钥.如果在他们的通信通道中有窃听者存在，他们所选定的数据将会因窃听者干扰而出现不一致.为了检知密钥的传输过程是否被窃听，他们公开比较各自的某些数据，由这些数据是否一致就可以发现是否有窃听者存在.如果确信他们所比较的比特是完全一致，则意味着通信未被窃听，余下尚未公开的比特便可用来作为共享的密钥.若发现有窃听者存在，则由所传递的比特就将被抛弃，不做为密钥.因此这种密钥有极高的安全性.

IBM 实验室的第一个量子密码原理性实验(BB84)如图 3 所示，爱丽丝的光源是发出绿光的发光二极管，它以几千赫兹的重复率发出脉宽为 5 微秒的非相干脉冲系列，此光束经准直通过一个特殊的滤波器和起偏器，光强度很低，每个脉冲平均只有 0.1 个光子.爱丽丝随机地使每个脉冲处于上述四种不同偏振态中的一个，从而实现了脉冲的偏码.这依靠随机地调整施加在普克尔盒上的不同电压来完成.巴伯的接收装置由另一套普克尔盒和起偏器构成，普克尔盒由随机和独立的电压所控制，巴伯改变施加在盒上的电压就可以选择不同偏振(圆偏振或线偏振)的检偏仪器.偏振分光器把光束分成水平和垂直偏振，这两束光分别入射到其灵敏度足以探测到单个光子的光电倍

增管.比特的类型"0"或"1"由光电倍增管的输出所确定.

在理想状况下,爱丽丝发送一系列的光子,每个光子用四个偏振态之一加以编码并给定某个确切的时间位置.巴伯使用与爱丽丝同一个时钟,并且在每个规定的时间间隙内随机地选择两个不同类型(圆偏振和线偏振)的检偏器(即不同的电压),他记录下测量的结果.在传输之后爱丽丝和巴伯公开商谈(在实验室中这由通过控制微机的软件来执行,在实际体系中这可用窃听者可能接触到的公用电话线来进行),巴伯告诉爱丽丝在每一个时间位置上他所使用的测量装置的类型,但是不通报他的测量结果("0"或"1"),然后爱丽丝告诉巴伯应当保留那些时间位置上的比特作为他们共享的密钥,在这些时间上,巴伯选对了检偏器的类型,而巴伯选错检偏器的比特将被抛弃不用.这样就完成了爱丽丝和巴伯之间的密钥传输.为了确定是否有窃听者存在,他们商定取出某些(设 M 个)时间位置上的比特在公开的信道上进行比较.如果双方的比特类型一致,则他们可使用剩下尚未公开的比特作为密钥.

表 1 综述了上述过程.(a)标出 14 个时间位置,(b)栏为爱丽丝发出的随机编码的光子,(c)为巴伯所使用的检偏器;+代表线偏振检偏器,0 代表圆偏振检偏器.巴伯测量的结果标示在(d)栏中,(e)栏是爱丽丝和巴伯保留下来作为密钥之用的事件,然后他们随机地取出 3、6 和 14 上的数据进行公开比较,若没有发现差错(即无窃听者存在),则用剩下的数据(f 栏)来产生一个二进制的密钥(g 栏).

当然,在实际的量子密码系统中还必须考虑到其他因素的影响,诸如光脉冲并不是单个光子的态,光探测器的量子效率不为 1 等等,这促进许多科学家进一步开展了一系列富有成果的研究.

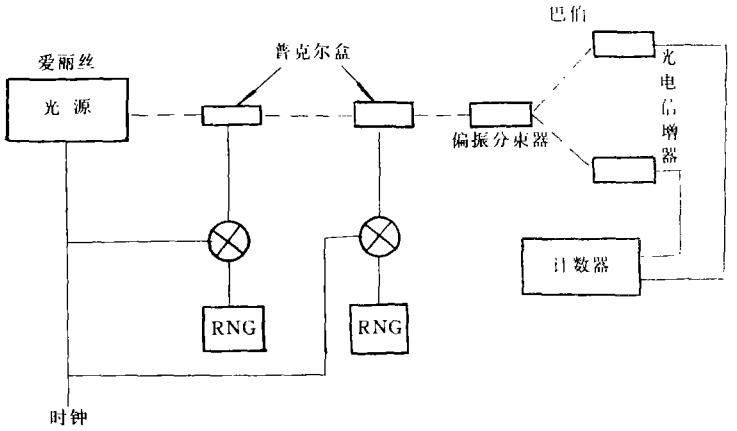


图 3 IBM 量子密钥传输装置(RNG 为随机数发生器)

三、量子密码系统

现在人们已经提出许多不同类型的量子密码方案,这些方案大致可分为两大类,一类是基于量子光学的纠缠态,两个有确定关联的光场用来作为建立爱丽丝和巴伯之间共享密钥的信息载体,任何窃听都会因破坏这种关联而被发现,另一类应用两个非正交量子态来实现量子密钥的传送,窃听者因干扰量子态而被识破.限于篇幅,这里仅介绍两种应用光纤作为传输线路的量子密码系统.

(1)EPR 方案

EPR 效应是指非局域的量子相关效应,它是爱因斯坦等人在与玻尔为代表的哥本哈根学派争论"量子力学是否是完备的理论体系"而提出来的.虽然近年来一系列的实验结果并不支持爱因斯坦的观点,但 EPR 效应确实体现出量子世界中奇特的性质,量子密码就是这种特性的一种应用.

EPR 效应是量子纠缠态的特性之一,以电子自旋为例,假设利用某一物理过程产生一对电子,它们满足总自旋为 0 的条件.然后它们沿着不同的方向传输,无论它们在空间上相距多远,它们的自旋总是相关的.若单独测量其中一个电子的自旋,则发现自旋向上或向下的几率各为 50%,但若测得其中一个电子的自旋向上(向下),则另一个电子的自旋将以 100%的几率取向下(向上)值.这是由于这对电子处于纠缠态,其自旋因满足总自旋为 0 而相互关联.

表 1　爱丽丝和巴伯使用圆偏振和线偏振进行局域的密钥传输

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14
b	∩	∩	∩	|	—	∩	—	|	|	∩	∩	—	∩	|
c	+	○	○	+	○	○	+	○	○	○	+	+	+	+
d	|	∩	∩	|	∩	∩	—	∩	∩	∩	|	—	|	|
e		∩	∩	|		∩	—			∩		—		|
f		∩		|			—			∩		—		
g		1		1			0			1		0		

在量子光学中应用参量下转换的非线性光学可以制备一对光子的纠缠态，无论这对光子(俗称孪生光子对)其后分离多远，它们彼此总是相关，基于这种 EPR 效应可以实现量子密钥的传输.图 4 是采用光纤传输孪生光子的量子密码系统.激光器发射频率为 ω_P 的激光束(泵浦光)，入射到频率下转换晶体上，一个泵浦光子会同时产生一对孪生光子，分别称为信号光子(频率 ω_S)和空闲光子(频率 ω_I)，这个非线性光学过程要求能量守恒和动量守恒，即

$$\omega_S+\omega_I=\omega_P \tag{1}$$

$$\vec{k}_S+\vec{k}_I=\vec{k}_P \tag{2}$$

式中$\vec{k}$为光的波矢.信号光子 ω_S 和空闲光子 ω_I 是相关的.两个光子分别通过光纤传输到远处的 Mach-Zehnder 干涉仪，每个干涉仪包含一条长的和短的路径.设光在长、短路径传播的时间差为 ΔT.设 Φ_S 和 Φ_I 分别表示在两个干涉仪中独立加入的相移.每个干涉仪的两个输出口分别连接到单光子探测器 S_0、S_1 和 I_0、I_1.

单个光子经过干涉仪后会发生干涉，两个光子探测器接收到这个光子的几率依赖于两个光程的相位差，这个探测几率可以按照经典光学的干涉公式来计算.在目前的系统，我们关心的是两个输出端的联合几率分布，即 $P(i,j)$，i，$j=0$ 或 1，其物理意义如下：$P(1,1)$ 表示 S 光子进入探测器 S_1，而它的孪生 I 光子进入探测器 I_1 的几率，$P(1,0)$ 表示 S 光子进入 S_1 而 I 光子进入 I_0 的几率，$P(0,0)$ 和 $P(0,1)$ 的意义类似.计算的结果为

$$P(1,1)=P(0,0)=\frac{1}{4}[1+\cos(\Phi_I+\Phi_S+\theta)] \tag{3}$$

$$P(0,1)=P(1,0)=\frac{1}{4}[1-\cos(\Phi_I+\Phi_S+\theta)] \tag{4}$$

式中 $\theta=(\omega_S+\omega_I)\Delta T=\omega_P\Delta T$，选择合适的干涉仪光程差可以使 $\theta=2n\pi$，n 为整数.现在引入如下的相关函数：

$$J(\Phi_S,\Phi_I)=P(1,1)+P(0,0)-P(0,1)-P(1,0) \tag{5}$$

在 $\theta=2n\pi$ 时，将式(3)和(4)代入上式便可得到

$$J(\Phi_S,\Phi_I)=\cos(\Phi_S+\Phi_I) \tag{6}$$

下面我们考察一下爱丽丝和巴伯如何使用这个系统来实现密钥传输.设他们分别用干涉

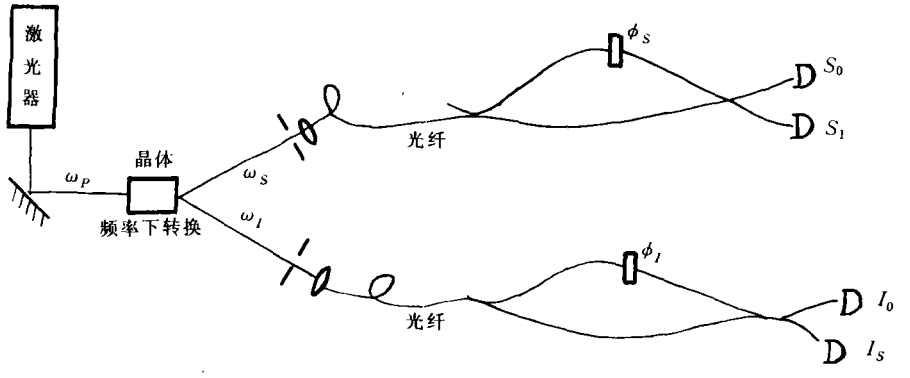


图 4　孪生光子干涉的量子密码系统

仪接收 S 光子和 I 光子，每次测量时，爱丽丝随机地选取相移 Φ_S 为 0 或者 $\pi/2$，巴伯随机地选取 Φ_I 为 0 或者 $\frac{\pi}{2}$.在光源发出一系列的孪生光子而爱丽丝和巴伯随机地选取 Φ_S 和 Φ_I，并用探测器进行测量之后，他们两人在公开的信道上宣布每次测量所选取的相移值 Φ_S 和 Φ_I，但不公布哪一个探测器接收到光子.然后他们决定抛弃 $\Phi_S+\Phi_I\neq 0$ 的事例，而将 $\Phi_S+\Phi_I=0$ 的事例保留下来作为密钥，在保留下来的事例中，按照方程(3,4,6)有

$$P(1,1)=P(0,0)=\frac{1}{2} \qquad (7\cdot a)$$

$$P(1,0)=P(0,1)=\frac{1}{2} \qquad (7\cdot b)$$

$$J(\Phi_S,\Phi_I)=1 \qquad (8)$$

这表明爱丽丝和巴伯的测量结果完全相关，在每个事例中，他们必定在同类(1 和 0)探测器中测到一个光子，亦即他们得到完全相同的比特串，这便是他们共享的密钥.

在没有窃听者干扰的场合，关联函数 $J(\Phi_S,\Phi_I)=1$.若有第三者进行窃听，必然会破坏爱丽丝和巴伯测量结果的相关性，$J(\Phi_S,\Phi_I)$ 不再等于 1.在传输结束之后，公开比较部分比特，看看两人的比特类型是否一致，便可判断是否有窃听.

(2)非 EPR 型

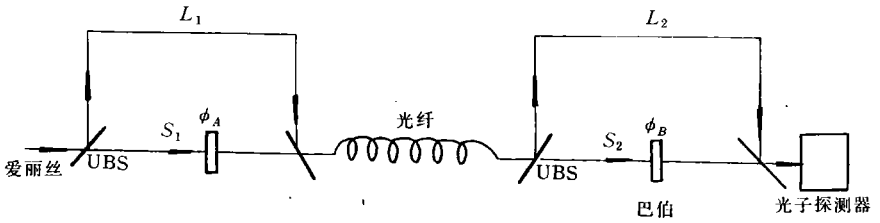
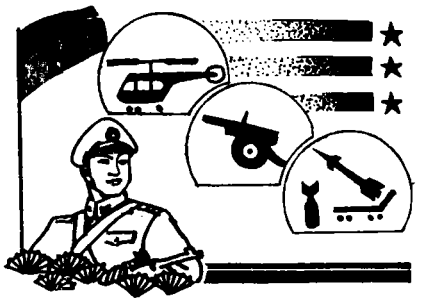


图 5 非 EPR 型的量子密码系统

图 5 是种非 EPR 型的量子密码方案，其原理说明如下：爱丽丝(A)输入一个相干光脉冲，其平均光子数 $M>1$，非对称分束器(UBS)将此光束分成强度不同的两束光，较强的参考光进入路径 L_1，较弱的光脉冲(平均光子数 $m<1$)通过路径 S_1.设 L_1 路径比 S_1 路径长，使得强脉冲落后于弱脉冲的时间为 Δt.在 S_1 路径中安置一个相移器 Φ_A.然后，两个光脉冲通过同一根光纤传输给巴伯(B).巴伯使用与爱丽丝同样的装置对输入两个光脉冲进行分束，较强的光脉冲沿 L_2 传输，它滞后于沿 S_2 传输的弱脉冲的时间为 Δt，在 S_2 路径中同样设置有相移器 Φ_B.所有光脉冲最后到达同一个光子探测器进行检测.

在光脉冲传输过程中，爱丽丝和巴伯分别随机地取 Φ_A、Φ_B 为 0 或 π.由于 L_1 和 L_2 路径相对于 S_1 和 S_2 的时间延迟相同，爱丽丝每发出一个光脉冲，到达探测器则有 3 个脉冲，它们相距 Δt 而先后到达探测器.第一个到达的光脉冲来自于 S_1-S_2 路径，由于经历了两次 UBS 的衰减，此脉冲极其微弱，不予考虑.第二个脉冲实际上是两个脉冲相叠加，一个是经 A 减弱、B 延迟，传输过 S_1L_2 的脉冲，另一个是 A 延迟、B 减弱、经由 L_1S_2 传输而来的脉冲，这两个脉冲强度相同，但前者经过相移器 Φ_A，后者经过相移器 Φ_B.两脉冲叠加之后所形成的第二个脉冲的强度依赖于 Φ_A、Φ_B 的选择，若 $\Phi_A+\Phi_B=0,2\pi$，则第二个脉冲会因相长干涉而增强，若 $\Phi_A+\Phi_B=\pi$，则第二个脉冲会因相消干涉而消失.最后到达探测器的第三个脉冲是经历 A、B 延迟的强脉冲，可以作为每个比特传输结束标志的参考光.

包含密钥信息的是第二个脉冲，我们称之为信息脉冲.爱丽丝输入一系列脉冲，并记下她每次随机选取的相移 Φ_A，巴伯测量每次信息脉冲的光强，并记下他每次随机选取的相移 Φ_B.在信息传输和测量结束之后，巴伯通过公开信道告诉爱丽丝，那些次信息脉冲测到了光子，但他不宣布他在测量中所用的相移 Φ_B.随后两人约定抛弃测不到光子的信息脉冲，而只将巴伯



几种新型武器的物理基础

南 秀 华

(石家庄军械工程学院)

随着经济的发展和科学技术现代化程度的不断提高，武器装备的现代化也不断地得到加强，陆续出现了一些新型武器．本文就几种正在开发阶段的新型武器的物理基础，作些简要的介绍．

一、次声武器

利用频率低于 20 赫兹的次声波与人体发生共振，使共振的器官或部位发生形变或位移而造成损伤的武器，叫做次声武器．

次声波与人体发生共振的频率和强度不同，对人体器官和部位的损伤程度也就不同．在强度相同的条件下，不同频率的次声波可以对不同的器官和不同的部位造成损伤；在频率相同的条件下，次声波的强度越大，则对人体的杀伤程度也就越大．次声波与人体发生共振以后，对人体产生精神的和机械的损伤．其主要症状是：全身性不适、头晕目眩、恶心呕吐、眼球震颤、腹部疼痛，严重的可发生神志失常、内脏破裂．实验表明，10 赫兹 135 分贝的次声波，可以使老鼠的内脏坏死；0.5 赫兹 170 分贝的次声波，可以使狗的呼吸困难或停止．次声实验舱由次声发生器、动力装置和控制部分组成，其中次声发生器是关键．次声武器的作用距离，由次声发生器的辐射声功率、声波传播的条件、指向性图案等因素决定．

次声波不易被人察觉，人耳也听不到，而且在大气中传播时衰减很小，因此与大气沟通的掩体和工事难以防御，这是次声武器的优点．但次声波不易集聚成束，在空旷环境中很难产生高强度次声波，而且次声波的波长很长，要使它定向传播，其聚集系统的尺寸将会很大，直径需达几十米或几百米，这实际上很难实现．因此，有的国家考虑采用两个频率相近的可听见的声波，使其频率差处于次声波的频率范围之内，这样比较容易实现次声波的定向辐射．另外还有人提出了利用爆炸产生高强度次声波的“次声弹”的设想．对此都还处于研究阶段．

二、电磁炮

利用洛仑兹力沿导轨发射炮弹的装置，称为电磁炮．它主要由能源、加速器、开关三部分组成．能源部分通常采用可蓄存 10～100 兆焦耳能量的装置．目前实验用的能源有蓄电池组、磁通压缩装置、单极发电机等，其中单极发电机是近期内最有发展前途的能源．加速器是把电磁能量转换成炮弹动能、从而使炮弹达到高速飞行的装置．目前有两大类：一是使用低压直流单极发电机供电的轨道炮加速器；二是使用线圈结构的同轴同步加速器．开关是接通能源和加速器的装置，能在几毫秒之内把兆安

测到了光子的信息脉冲保留下来，按照事先的约定，将相移值转化密码本（如 $\Phi_A=\Phi_B=\pi$ 代表“1”，$\Phi_A=\Phi_B=0$ 代表“0”）．

当然，即使对于 $\Phi_A=\Phi_B$ 的事件，由于平均光子数小于 1，巴伯也有可能探到光子，这些事件也归属于被抛弃的范围．类似于前面的分析，当有第三者窃听时，他的存在会破坏 Φ_A 和 Φ_B 之间的相关性，亦即在 $\Phi_A\neq\Phi_B$ 的事例中，巴伯依然有可能测到光子．通过公开比较部分密码本就能判断窃听者存在与否．

量子密码的理论和实验研究已经取得重要突破．最近我们提出基于相干态的量子密码体系即将发表在 Chin.Phys.Lett.．量子密码的诱人前景激发人们的广泛兴趣，许多国家的科学家竞相投入此领域的研究，相信量子密码术实用化的日子不会太远了．