量子密码和它对我们的启示*

密码的使用可以使得各种需要保密的信息(如国防、经济、商业情报)不致被窃取,以维护国家和个人的利益.今天所使用的密码的确能胜任这一任务.然而,或迟或早,某位数学家就会发现破译密码的方法,从而使得今天的密码技术变得毫无用处.那时,国际安全、商业活动等都会受到黑客的威胁.在信息时代正在来临的今天,人们依靠密码来保护自己,免于间谍、计算机骗子和黑客们窃取信息.一些今天所使用的最安全的密码是建立在如下的事实上的:我们很容易将两个很大的素数相乘求出其乘积,但是,几乎不可能从其乘积反过来求出它是由哪两个素数相乘而来.然而,如果某天一位数学天才发现了求得隐藏在结果背后的素数的捷径,这种密码就会马上失去作用.

人们寻求的是某种新式的密码,一种真正不可能被破译的密码.正是在这里量子世界的基本观念帮助了密码技术.吴令安先生曾在本刊1998年第9期的"量子信息讲座"中对量子密码通信作了清楚而完备的介绍.有兴趣和希望更全面、更深入地了解量子密码学的读者,请参看该文.我们在本文中将以简单易懂的方式介绍与近年量子密码技术的发展有关的一些问题.

量子粒子在与其周围宏观物质相互作用时会丢失它所携带的信息.因而,在具体实现量子密钥的传送时每一步都会遇到技术上的困难.但困难不等于不可能.在过去几年里,科学家和工程师们已经实现了将这种量子密钥利用光纤传送数十公里的距离.而目前他们正在努力实现将量子密钥在空间传送.一旦实验成功,人们就可以通过通信卫星实现迄今最安全的全球通信.

量子密钥的提出和发展过程也是一个最好的例子,说明了人们从基础研究中获得的对自然规律的了解,是怎样和日新月异发展的技术结合,同时又将技术推向更新的高度以实现其生产和社会效益.

1 密码和密钥

在密码学中,常用三个人A,B,C来模拟密码传送中的情景.假定在A要传送一个机密信息给B时,C想要窃取A所传送的信息.为了保密,A必须将信息以密码形式传送给B.A可以用一种理论上不可破译的所谓一次性密码来对他所传送的信息加密.这种一次性密码技术已经在很长时间内被人们用来传送信息.它的密码传送过程是分三步来完成的.首先,A将他要传送的信息编译为二进制码,即以一系列0和1来表示该信息.然后,A再产生一把密钥,它是由一组与信息一样长的随机产生的二进制码,即0和1所组成.第三步,A将信息和随机产生的密钥逐位相加.只不过其有别于通常加法的规则是1+1=0.这样就产生了A的加密信息.A就可以把它用通常的方法传送给B.这类密码原则上是不可破译的,因为A的密钥的每个元素是随机产生的.即使C利用计算机来试验每种可能的密钥,他只能发现其中许多会给出某种对信息的解释.但是,C无法从这些可能的解释中选出真实的信息.而B则可以用A送给他的密钥简单地从获得的加密的信息中减去密钥就可以将密码解密.一般,每个密钥只用一次,用后就将其销毁.下次传递信息时再产生和使用新的密钥编码.这就是将其称为一次性密钥的原因.

尽管理论上一次性密码非常完满,但在实际应用上却存在一些重要的缺陷.正是这些缺陷阻碍着一次性密码的广泛使用.制造一个真正随机的密钥是困难的,而要对每个信息制造一个不同的随机密钥就非常耗费时间.真正的致命之处还在于必须将密钥送到所有接受信息的人的手中.在A制成一个随机密钥并将其要发送的信息编成密码后,他必须将密钥交给B,以使得B可以解开密码.但是,他不能将密钥不加密地传送给B,因为C可能窃获密钥从而将加密的信息解开.但是,A又不能将密钥加密后再送给B,因为如果A将密钥加密,他还必须告诉B解开加密密钥的密钥.这样,就形成了一个解不开的循环.

在从前,密钥传送问题通常是由可靠的信差直接将密钥交给B的办法来解决.然而,这种解决办法在卫星通信和电子邮件发达的今天并不具有吸引力.而且,在信息时代,传送信息的频次和对信息到达时间的要求愈来愈高,由信差传送密钥的方法显

* 2000-01-17收到初稿,2000-04-19修回

然不能满足要求.

2 量子密钥的概念

正是在密钥的传送问题上量子物理给出了完整的解决方案.20 世纪 80 年代初,美国 IBM 研究所的研究员本内特(Charles Bennett)和蒙特利尔大学的布拉萨特(Gilles Brassard)提出 A 和 B 之间应当用单个光子来交换他们的密钥.他们认为,如果在量子水平操作,A 和 B 可以利用量子规律来保护密钥的安全传送.该方法的基本点是利用在不同方向偏振的光子来代表二进制码中的 1 和 0.如果 C 想拦截密钥,他必须要用有效的方法吸收这些光子.为了使自己的拦截不被 A 和 B 发现,C 还必须要再把光子传送给 B.但是,由于量子物理的特有规律,C 不能够测定出所有 A 送出的光子的正确偏振方向.这样,C 就不能保证送出与 A 相同偏振方向的光子给 B.C 的拦截不可避免地会影响到密钥的传送,因此 A 和 B 就会发现有人拦截,从而舍弃这次的密钥再另外做一个新的密钥.

读者会提出,这一方案听起来是很完美,但是,既然 C 不能准确地读出密钥,B 怎么可能正确地读出密钥呢?这是实现量子密钥中的关键的环节.1984 年,Brassard 在纽约州的某个火车站等候火车回蒙特利尔时,与送行的 Bennett 在火车站聊天.就在这次讨论中,他们发现了第一个可以实际操作的量子密码的工作方案.在他们最初的方案中,A 和 B 各需要 4 个偏振滤波片.到了 1992 年,方案被简化为 A 和 B 各只需要 2 个偏振滤波片的方案所取代.

这种系统是怎样工作的呢?如果 A 需要传送密钥给 B,使他能够对收到的密码正确地进行解码,A 将使用 2 个偏振滤光片,其方向分别放置在 0°和 45°.这两个方向分别代表二进制码的比特值 0 和 1.B 有两个类似的偏振滤光片,他将它们分别放置在 90°和 - 45°方向上.为了传送密钥,A 送给 B 一系列随机的代表 1 和 0 的光子.B 则随机地用他的两个偏振滤光片中的一个来接收 A 所送来的每个光子.由于偏振光子具有的特性,它在遇到与其偏振方向相同的偏振滤光片时总能通过,而在遇到与其偏振方向垂直的偏振滤光片时将不可能通过.但是,在光子遇上与其偏振方向成 45°角的偏振滤光片时,按照量子物理规律,光子通过或被阻拦的可能性各占一半.

假定 B 是用方向在 - 45°的偏振滤光片接收 A 所送来的光子,而他未接收到通过偏振滤光片的光子.这时 B 并不能判定 A 是用 45°方向的偏振滤光片送出光子(它们意味着 1,这种光子将总是被 - 45°的偏振滤光片挡住),或者是用 0°滤光片送出的光子(这种光子表示 0,它只是有时被 - 45°的偏振滤光片阻拦).然而,如果幸而有一个光子通过偏振滤光片而被 B 接收到,他却可以断定 A 是用 0°的偏振滤光片送出这个光子的.可以看出,B 可以确切地判定,如果他用 - 45°的偏振滤光片接收到了 A 所送来的光子,A 必然是传送给他一个 0,类似地,如果他用处于 90°的偏振滤光片接收 A 所传来的光子并接收到了 A 送来的光子,B 就知道 A 必然是送来一个 45°方向的光子,即 1(见图 1).

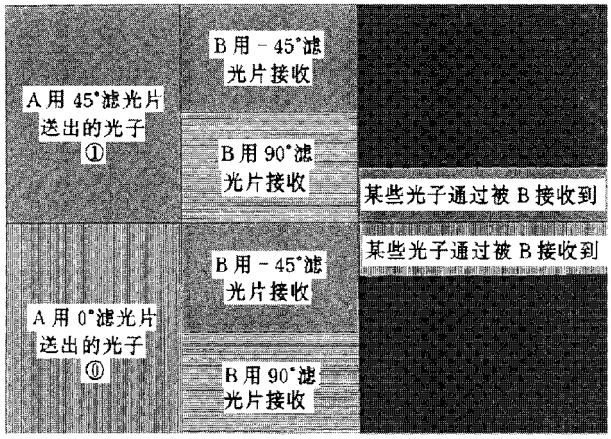

图 1 能够通过 B 的 90°和 - 45°滤光片的光子必定分别是 A 送出的比特值为 1 和 0 的光子

因此,当 A 向 B 传送偏振光子时,B 可以确切地知道被他接收到的那部分光子的比特值.A 可以送出一系列成百上千的偏振光子,每个光子的偏振方向(0 或 1)都是随机选取的.而 B 也随机地转换其偏振滤光片以接收 A 所发来的偏振光子.平均而言,有四分之三的光子将不能被 B 接收到,但是,B 却可以确切地知道那少数通过偏振滤光片而被他接收到的光子的比特值.在接收完 A 所发来的偏振光子后,B 可以用电话告诉 A 哪些光子被他接收到了.这些光子组成的一组值就形成一个密钥,可以用于对以后传送的信息进行加密.

表 1 中给出一个简单的例子来说明密钥是怎么在 A 和 B 之间建立起来的.表中的第一行给出了 A 发送光子时随机采用的他的两个滤光片的组合.因而也就决定了发送出的光子所带的比特值.第二行给出这些光子的比特值.第三行是 B 在接收 A 发送来的每个光子时所用的滤光片,它们是在 B 的两个滤光片间随机选取的.第四行是 B 接收的结果,

“无”表示未接收到光子,“有”表示接收到了 A 发送来的光子.第五行给出的是由 B 接收到的光子所建立起的密钥.在这个例子中,密钥就是 010.当然,我们在这里给出的只是一个很简单的例子.实际应用的密钥要长得多.但是,这个例子说明了量子密钥建立的基本道理.

表 1　A 和 B 建立密钥的例子

A 发送光子时所用的滤光片	/	|	/	/	|	/	|	|	/
A 发送的光子具有的比特值	1	0	1	1	0	1	0	0	1
B 接收光子时所用的滤光片	\	\	—	—	\	\	\	—	\
B 是否接收到 A 送来的光子	无	有	无	有	无	无	有	无	无
A 和 B 间建立的密钥		0		1			0		

3　量子密钥为何是可以安全传送的密钥

在 B 接收完 A 所传送来的光子后,并用任何公开的方式告知 A 他所接收到的光子,密钥就建立起来.即使 C 窃听了 B 的电话,知道 B 接收到了 A 所来的那些光子,他仍然不可能知道组成密钥数码.这是由于 B 并未(也不需要)在电话上告诉 A 他是用什么偏振滤光片对每个光子进行测量的.

更为关键的一点是,如果 C 在 A 向 B 传送光子时企图进行拦截,以获取密钥的情报,他的拦截将会自然地暴露他自己.假定 A 送一个 0°光子给 B,它代表的值是 0.C 用 - 45°的偏振滤光片接收它.当光子未能通过偏振滤光片时,C 并不知道究竟是因为 A 送来的是 45°的光子,因此不可能被接收到,还是送来的是 0°的光子但正好未能通过偏振滤光片.C 必须在这两种可能性间进行猜测.如果他猜这个光子是 45°的光子,并送给 B 一个 45°的光子.假若 B 是用他的 90°的偏振滤光片进行接收,光子有可能被 B 接收到.如果情况真的如此,B 将会将 A 送来的光子错误地解释为表示比特值为 1.

B 的这种错误解释可以用来探知 C 的拦截.为了看是否 C 拦截了 A 传送给 B 的光子,A 和 B 只需核对发送和接收到的码之间是否存在错误.在他们建立了第一步的密钥之后,他们可以从其中随机地选出某些比特值通过电话进行核对,看看是否一致.如果这些比特值间有误,他们就可以知道 C 进行了拦截从而舍弃这次的密钥,再建立新的密钥.如果一致,他们就可以认为密钥是安全的.在舍弃用来核对的那些比特值后,密钥就可以用于对以后的信息进行加密.当然,C 总有可能猜对他所拦截到的光子的偏振.如果这些光子被用于错误的核对,A 和 B 将不可能发现 C 窃获了传送的光子.然而,当 A 和 B 核对许多光子所代表的比特值时,C 的拦截不被察觉的可能性将变得几乎为 0.

直到 Bennett 和 Brassard 发明量子密码学之后过了五年,他们进行了第一次实验.实验是由一台计算机 A 在空气中传送一系列光子给相距 32cm 的另一台计算机 B.他们成功地实现了世界上最安全的密钥的传送.此后,其他的实验室很快开始了设计能够在更适用的距离上工作的系统.

4　量子密钥技术的发展

关键的技术问题是如何在光子传播中保持其偏振方向.如果光子的偏振在传送过程中由于各种原因发生变化,即使 C 未进行拦截,A 和 B 会在核对错误时也会发现不一致.这样将不可能形成有效的密钥.

一个解决这一问题的途径是用光纤来传送光子.光子在光纤中传播时可以保持其偏振方向不变.这一途径已经被用来使量子密码信息可以在有实际意义的距离上被传送.1995 年,日内瓦大学的研究人员成功地用光纤将量子密码信息传送到在它北面 20 多公里的尼翁.同年,洛斯阿拉莫斯(Los Alamos)的研究人员又创造了新纪录,他们实现了通过一条长 48 公里的光纤传送量子密钥.这个长度已经足可以让一所银行和它的分支机构或者政府各部门的办公室之间建立量子密码通信的网络.但是,要将这一技术扩展到更远距离遇到了困难.这是因为光子在光纤中传输更远距离时难免要被吸收.而在传输成百上千公里距离时信号将衰减到几乎为零.

在卫星通信已经发展和普及的今天,理想的解决办法是寻求某种方法将量子密钥通过大气传送到卫星,并通过卫星进行传送.休斯(Richard Hughes)领导的洛斯阿拉莫斯的量子信息组目前是全世界在“空间量子密码学”研究上的领先者.在过去的两年内,这个小组克服了一个个技术上的困难将通过大气的传送距离一步步的向前推进.最终,他们计划将单个光子传送到距地面约 300km 的卫星上的一个直径仅有几厘米的接收器上,并且要求,光子在穿过大气时不被吸收,不然信号将会丢失,而且,它们的

偏振方向也不改变.

要求光子在传送过程中不被吸收是比较容易的.我们只需选择光子的波长使得大气中的分子对它的吸收可以忽略.休斯小组选择了波长为 770nm 的光子,虽然波长更长的光子也不会被大气吸收,但是它们对大气的扰动比较敏感.大气湍流会改变局域大气的折射系数,从而导致光子偏振方向的歪曲.大气湍流的典型尺度为几十厘米,因此,770nm 已足够短,足以避免这种影响.除此之外还有不少问题.例如,当卫星在接收 A 送来的光子时,信号有被直接从太阳来的,或被地球或月亮反射来的太阳光线淹没的危险.为了防止这种情况的发生,洛斯阿拉莫斯小组设计了一种高度定向的接收器,它只接收从 A 方向传来的光子.接收器还包含了一个滤波系统,它保证只有正确频率的光子能够通过并为接收器所接收.

但是,仍然有可能有的光子虽然并不是由 A 所发送,却碰巧有正确的频率并从正确的方向到达接收器.为了避免这样的光子的干扰,接收器还加上了时间窗口.在每微秒时间内,时间窗口仅开启 5ns.只有在此期间到达的光子才能够被接收.可以控制窗口仅在 A 的光子到达时才开启.这一设想当然非常好,但是,时间窗口建立后会遇到另一个问题.这个问题同样与大气湍流有关.尽管我们选取了适当波长的光子,避免了在传播中被大气吸收或影响其偏振方向,可是,局域折射系数的变化却会影响光子传播的速度.大气湍流将会造成光子从 A 传播到 B 所需时间的跳变.这会使得光子的到达时间与时间窗口不能相互吻合.为了解决这一问题,A 在每个光子之前 100ns 发送一个光脉冲.这一光脉冲将会受到由于大气湍流产生的与信号光子同样的影响.因此,每当有一个脉冲到达,卫星上的接收器就知道有一个 A 发送来的光子会在 100ns 后到达.并由此确定开启窗口的时间.

大气湍流还造成另外一个头疼的问题.局域折射率的改变还会使光子传播的轨道晃动.这会使得光子有可能偏离卫星上的接收天线.为了保持光子循正确的轨道到达接收器,A 必须监测前导的光脉冲所产生的极微弱的反射,并利用由此得来的信息调整光子的发送方向.

5 量子密码的进展和它给我们的启示

1999 年初,休斯创造了一个通过大气传送量子密码的新纪录.他们成功地在相距 500m 距离远处交换了量子密钥.在他们的实验中,B 是一个配有直径为 3.5in 望远镜的接收器.入射光子被接收器内的光束分离器随机地将它反射或让其透过,这样使光子分别进入到不同的偏振滤光片.此后,A 和 B 通过以太网核对密钥中的误码.由于没有 C 进行拦截,密钥中应当没有误码.但是,由于背景光子、探测器的噪声等会引入 1.6%的错误率.这并不严重,因为如果有 C 进行拦截,他将造成大致 25%的误码率.因此,A 和 B 仍然能够确信密钥是安全的.

粗看起来,休斯完成的 500m 距离上量子密钥的交换和要将量子密钥送到 300km 外的通信卫星之间尚有很大的距离.但是,实际上休斯和实际目标之间的距离比表面上看来的要接近得多.原因是,休斯是沿水平面传送他的密钥.在水平面上大气密度最高,大气的扰动也最大.休斯估计,沿水平面将量子密钥传送 2km 等价于将它传送到一颗低轨道卫星.他计划晚些时候还要进行 2km 距离上传送量子密钥的实验.他还希望在两年内实现与一颗真正的卫星之间进行密钥的传送.如果休斯的计划如期实现,在 10 年内就有可能实现用这种不可能被破译的量子密码来保护全球卫星通信.而现在,通过光纤已经可以利用量子密码保护在较短距离上的通信.或许现在已经有了这种通信系统.

我们可以清楚地看到,量子密码的发明和研究进展是基础研究与高新技术结合的产物.量子密码学概念的提出是基于基础研究的成果.没有对量子规律的了解,量子密码的想法根本不可能出现.而把设想变成现实却离不开现有的高新技术的帮助.而在实现这种技术的过程中,更不断地将技术推向更新更高.我们看到,基础、实验和已有高新技术的有机结合才会不断推动经济、社会的发展.任何只要一头舍弃其他的做法必然会在发展中遇到不可克服的阻碍.

(中国科学技术大学研究生院　邓祖淦　编译自《New Scientist》,1999 年 10 月 2 日出版)