量子十问之五
量子密码就是量子通信吗?

郭光灿†
(中国科学技术大学　中国科学院量子信息重点实验室　合肥　230026)

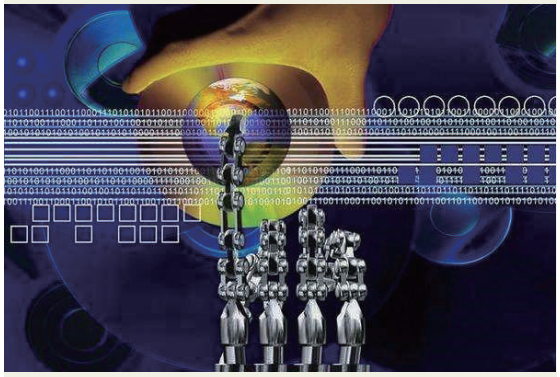
2018－09－12收到
† email: gcguo@ustc.edu.cn
DOI: 10.7693/wl20190206

密码学是内容极其丰富的学科，目前量子信息技术仅仅在“密钥分配”这个具体分支上可望发挥独特的作用。保密通信是密码学的重要内容，其基本原理是，采用密钥K_1 (0，1的随机数列)通过加密算法将甲方要发送的信息(明文)变换成密文，在公开信道上发送到合法用户乙方处，乙方采用密钥K_2从密文中提取所要的明文。

如果甲乙双方采用相同的密钥(即$K_1=K_2$)，称为对称密码或私密密码。如果$K_1\neq K_2$，称为非对称密码或公开密码，其中K_1是公开的密钥，K_2只为乙方私人拥有。

如果任何窃听者在不知晓密钥的情况下，可以从秘文提取出明文，那么这种密码体系就是不安全的。事实上，每个国家，无时无刻都在收集其他国家所发出的秘文，许许多多极其聪明的破译专家日以继夜地企图从各种秘文中提取有用的机密信息，这种精彩的情报战早已成为百姓津津乐道的公开秘密。这时不禁要问，有没有一种令所有专家都无法破解的密码？确实有！早在20世纪40年代，著名的信息论鼻祖香农采用信息论证明，如果密钥长度与明文长度一样长，而且用过后不再重复使用，则这种密文是绝对无法破译的，俗称为“一次一密”。太妙了吧！

量子密码(图片来源于网络)


量子密钥分配(图片来源于网络)

那么为何这种“一次一密”的密码迄今未被广泛推广使用呢？主要原因是，“一次一密”要消耗大量“密钥”，需要甲乙双方不断地更新密码本，而“密码本”的传送(称为“密钥分配”)本质上是不安全的。采用不安全的密钥来实施“一次一密”加密仍然是不安全的。那么是否有什么办法可以确保密钥分配是安全的？有，这就是“量子密钥分配”(缩写为“QKD”)!

“量子密钥分配”应用到量子力学的基本特性(如量子不可克隆性，量子不确定性等)来确保任何企图窃取传送中的密钥都会被合法用户所发现，这是QKD比传统密钥分配所具有的独特优势，后者原则上难以判断手头的密码本是否已被窃听者复制过。QKD的另一个优点是无需保存“密码本”，只是在甲乙双方需要实施保密通信时，实时地进行量子密钥分配，然后使用这个被确认是安全的密钥实现“一次一密”的经典保密通信，这样可避开保存密码本的安全隐患。

量子密钥分配的过程大致如下：单个光子通常作为偏振或相位自由度的量子比特，可以把欲传递的0，1随机数编码到这个量子叠加态上，比如，事先约定，光子的圆偏振代表1，线偏振代表0。光源发出一个光子，甲方随机地将每个光子分别制备成圆偏振态或线偏振态，然后发给合法用户乙方，乙方接收到光子，为确认它的偏振态(即0或1)，便随机地采用圆偏光或线偏光的检偏器测量。如果检偏器的

类型恰好与被测的光子偏振态一致，则测出的随机数与甲所编码的随机数必然相同，否则，乙所测得的随机数就与甲方发射的不同。乙方把甲方发射来的光子逐一测量，记录下测量的结果。然后乙方经由公开信道告诉甲方他所采用的检偏器类型。这时甲方便能知道乙方检测时哪些光子被正确地检测，哪些未被正确地检测，可能出错，于是他告诉乙方仅留下正确检测的结果作为密钥，这样双方就拥有完全一致的0，1随机数序列。

如果有窃听者在此过程中企图骗取这个密钥，他有两种策略：一是将甲发来的量子比特进行克隆，然后再发给乙方。但量子不可克隆性确保窃听者无法克隆出正确的量子比特序列，因而也无法获得最终的密钥；另一种是窃听者随机地选择检偏器，测量每个量子比特所编码的随机数，然后将测量后的量子比特冒充甲方的量子比特发送给乙方。按照量子力学的假定，测量必然会干扰量子态，因此这个“冒充”的量子比特与原始的量子比特可能不一样，这将导致甲乙双方最终形成的随机数序列出现误差，他们经由随机比对，只要发现误码率异常得高，便知有窃听者存在，这样的密钥不安全，弃之不用。只有当他们确认无窃听者存在，其密钥才是安全的。接下来便可用此安全密钥进行“一次一密”的经典保密通信。

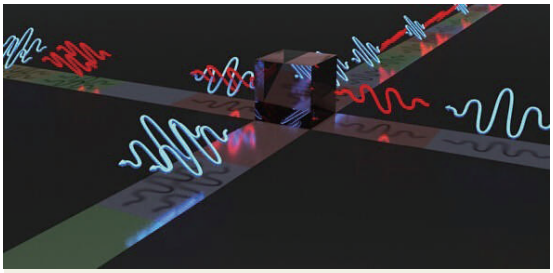
上述这种保密通信，实质上是“一次一密”的经典通信，只是密钥是由QKD生成的，通常也称为量子保密通信。那么有两个问题出现：

一是，如果窃听者不停地窃听，甲乙双方就无法获得安全的密钥，于是保密通信便无法进行。确实如此，QKD对此无能为力！它唯一的优势功能就是断定是否有窃听者存在，所分配的密钥是否安全而已。这点在传统密钥分配原则上做不到。QKD只能用来确保传递信息的安全性，无法抗击“破坏信息传送”的行为。在这种场合只有借助于其他办法进行保密通信，比如，采用网络QKD，若某一路中段，寻找到不被窃听的传输路径可实现安全的密钥分配。如果QKD网络都处于被窃听的状态，那只好采用传统的保密通信办法了。

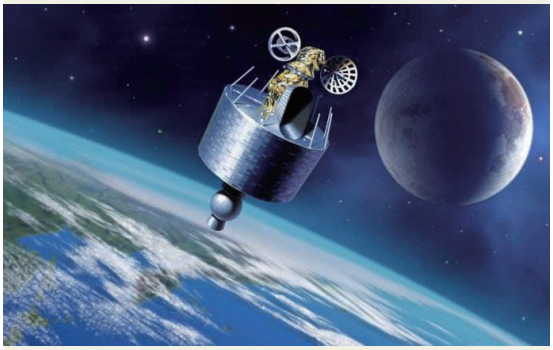
二是采用量子比特所生成的安全密钥比起用传统方法所得到的安全密钥(假定存在这种办法)有优越性吗？回答是否定的。只要密钥是安全的，不管是用何种办法生成的，两者性能完全一样。特别是，如果达不到“一次一密”的加密程度，即使QKD的密钥是绝对安全的。这种密码体系同样可能被聪明的破译者所攻破。

现在我们可以回答标题所问的问题：量子密码是量子通信吗？答案是否定的！所谓“通信”简单地说就是传递信息(即“明文”)。量子密码只是传送经典随机数而已，不包含有任何信息内容，因此，与“通信”无关。量子保密通信实际上包括由QKD生成的安全密码和“一次一密”经典通信两个部分，本质上仍然是经典通信。现在媒体、学术界所说的“量子通信”就是量子密码或者量子保密通信，是某些人概念不清的误导，再由媒体炒作放大而形成的。真正的“量子通信”有其确切的内涵，即将信息编码在量子比特上，在量子通道上将量子比特从甲方传给乙方，直接实现信息的传递。这种真正的“量子通信”目前仍处于基础研究阶段，离实际应用还相当遥远。

下面我们来回答另一个问题，即量子密码是绝对安全的吗？或者问，量子保密通信果真能做到不可窃听、不可破译的绝对安全吗？保密通信的安全性同时受到两个因素制约：密钥的安全性和“一次一密”的真实性。量子密码在理想状态下可以确保密钥的安全性，但实际上，量子密码系统绝对达不到理想状态，例如单粒子探测效率不是百分百的，它会产生传输损耗、各种器件不完善等问题，这些非理想漏洞就可能被窃听者用来窃取密钥，但却不会被合法用户发现。就



量子密码是绝对安全的吗？(图片来源于网络)



通过卫星实现“天地一体化”的量子保密通信网络？(图片来源于网络)

算人们能设计出与设备完全无关的量子密码协议，但因随机数的真伪、合法用户的识别等问题仍然难以做到密钥的绝对安全。只能是“相对安全”。另一方面，量子密码体系必须确保安全密钥的生成率足够高，以达到视频信息“一次一密”加密的需求，否则，即使密钥是安全的，保密通信仍然是不安全的。

量子密码的研究已有30多年历程，目前达到的实际水平是：在百公里范围的城域网，量子密码体系可以做到密钥分配在现有技术保证的各种攻击下是安全的，安全密钥生成率在25公里可确保高清视频“一次一密”，在100公里内能确保音频、文字、图片等的“一次一密”。因此可以制定“量子密码标准”，推广应用。随着攻击技术水平的提高，现有相对安全的量子密码可能会被攻击，到那时将会随之更新“量子密码标准”。因此，结论是：实际上，量子密码是相对安全的!

至于超过城域而筑建的任何城际量子密码网络，目前仍无法确保其安全性。现在通常使用的是“可信中继”，其安全性依赖于人的因素，所以安全程度不会超越现有的传统加密。远程量子密码只有采用“量子中继”才能确保其安全性，而“量子中继”的研制受到可实用的量子存储器和确定性纠缠光子源的限制，目前仍然处于基础研究阶段。

说得更远些，能否通过卫星等实现“天地一体化”的量子保密通信网络呢？理论上可行，但实际上难以做到。而且，是否非这样做不可也值得探讨。暂不说覆盖地面的网络有多难，就说“地空之间”的量子密码，必须确保在各种恶劣条件下全天候实现安全的密钥分配，而且它的密钥分配要达到“一次一密”的需求，就目前人类所达到的技术而言，这些条件都是可望不可及的。

上面提到的量子密码是在私密密码体系中，至于另种公钥密码体系在量子信息技术时代处境如何呢？现有公钥体系的安全性是基于难求解的数学难题，如大数因子分解等。业已证明，量子计算机的并行运算能力可以攻破RSA，DSA和ECDSA密码。因此，现有的公钥体系将面临巨大的挑战。但是量子计算机并不能解决电子计算机难以求解的所有数学问题，这也意味着，量子计算机并不能攻破所有密码体系，特别是10年前密码学界就开始着手研究“抗量子计算攻击的新型密码”，而且不断取得进展。一旦这种新型的安全密码体系的研究得以成功，量子时代的信息安全将得到保证，而且这种抗量子计算密码显然比起目前研究的量子密码无论从造价上还是使用上都具有更大优势，相信会获得更广泛应用。