中华博士园地

这是本刊特为海内外正在就读和学成立业的博士、博士后青年学者们开辟的一片科普园地。深学浅著，是一门德识、慧学、素质修养的学问。你们的新知识、新调研、新观察、新目光、新展望，能够用尽可能深入浅出、通俗流畅的语言，汇报给祖国、人民、家乡父老子弟乡亲们吗？中华博士园地，乃耕耘忠孝之地、科教兴国、民族昌盛之地。要用慈母听得懂的语言，写出你们的心声！

量子密码学

陈明奇 毛琼

（北京邮电大学信息安全中心，北京 100876）

1 引 言

在今天的信息时代，大量的敏感信息如资金转移，私人财产，健康状况，法庭记录等常通过公共通信设施或者计算机网络来交换，而且也将有越来越多的公共和私人机构应用电子数据处理，将大量重要而敏感的数据储存在数据库中，因此确保防止这些信息的泄漏，并保证其整体的完整性和真实性是人们所迫切需要的，除了制订相应的法律来保护敏感信息外，密码技术就是一种经济而有效的方法。密码技术对于信息安全而言是如此重要，以至于采用不安全的密码技术甚至比没有采用密码技术还要糟糕。

密码学包括2部分内容：一是加密算法的设计和研究；二是密码分析，所谓密码分析，就是密码破译技术。这两者是矛盾的两方面。密码学的出现虽然可以追溯至遥远的古代，但直到本世纪40年代前，密码技术可以说还是一门艺术而不是一门科学，那时的密码专家常凭着直觉和信念来进行密码设计和分析，而不是靠推理证明。1949年，Claude. E. Shannon发表的“保密系统的信息理论”一文标志着密码学成为了一门科学。此后，密码学得到了迅速的发展。现在密码学的应用已不再局限于军事、政治和外交，其商用价值和社会价值已得到了充分肯定。现在常用的公开加密算法主要可分为两类：以DES (Digital Encryption Standard)算法为代表的密钥算法和以RSA (Rivest-Shamir-Adleman)为代表的公开钥算法。DES密码的保密性是建立在一定长度的密钥基础之上的。RSA密码的保密性则是建立在分

陈明奇 1997年毕业于南京理工大学电子工程系，现为北京邮电大学信息系97级博士生，主要从事信号与信息处理，密码学应用，信息隐藏，图象加密等方面的研究。

解有大素数因子的合数的基础之上。人们尚无法从理论上证明这两种算法的不可破性，换而言之，它们是基于难解的数学问题而不是无法解的问题。事实上，早在 Shannon 给出完善保密系统的证明之前，已有实际应用的 Vernam 密码就是完善保密的，即是不可破的密码。这种密码需要一个与所传递的消息一样长的密码本，并且此密码本绝不再用于另一条消息的传递。这正是 Shannon 所证明的：密钥必须为一长度不少于待加密的明文长度的随机序列，且任何一密钥仅使用一次。这就是所谓的一次一密码体制，理论上它是不可破解的，但由于在实际应用中，其密钥的分配是一个很脆弱的环节，因此未能得到广泛的应用[1]。

近年来，由于量子力学和密码学的结合，出现了量子密码学(Quantum Cryptography)，它可完成单由数学无法完成的完善保密系统。量子密码装置一般采用单个光子实现，根据海森堡的测不准原理，测量这一量子系统会对该系统产生干扰并且会产生出关于该系统测量前状态的不完整信息。因此，窃听一量子通信信道就会产生不可避免的干扰，合法的通信双方则可由此而察觉到有人在窃听。量子密码术利用这一效应，使从未见过面且事先没有共享秘密信息的通信双方建立通信密钥，然后再采用 Shannon 已证明的是完善保密的一次一密钥密码通信，即可确保双方的秘密不泄漏。这样，量子密码学达到了经典密码学所无法达到的 2 个最终目的：一是合法的通信双方可察觉潜在的窃听者并采取相应的措施；二是使窃听者无法破解量子密码，无论企图破译者有多么强大的计算能力[2]。量子密码学的出现是对经典密码学的一重大突破，我们可毫不夸张地说我们正处在信息时代即将发生深刻变化的前夜。

2　量子密码学

在经典物理学中，物体的运动轨迹仅由相应的运动方程所描述和决定，不受外界观察者观测的影响，或者说，这种影响微乎其微可完全被忽略。同样，一个基于经典物理学的密码系统中的信息也不会因窃听者的窃听而改变，这完全是由经典物理学所研究的宏观范围决定的。然而，在微观的量子世界中，情形就完全不同了。因为观察量子系统的状态将不可避免地要破坏量子系统的原有状态，而且这种破坏是不可逆转的。这就意味着：当你用一套精心设计的设备来偷窥量子系统的状态时，你所能看到的仅是在你介入之后的状态，即量子系统改变后的状态，而在此之前的状态则是无法推知的。如果利用量子系统的这种特性来传递密钥，那么窃听者的一举一动都将被量子系统的合法用户所察觉，而且窃听者也不可能获得真正的密钥数据。

量子密码学是基于量子物理学中的下述两个基本概念：超状态(Superposition State)和测不准原理(Uncertainty Principle)。正如经典物理学中物体的状态由其位移、速度等物理量决定一样，在量子物理世界中，量子系统是通过量子状态——超状态[3]来描述的，它是抽象 Hilbert 空间中的表示系统未来可能状态的一个矢量。任何一个量子状态可被展开为：

$$|\Psi\rangle = a|0\rangle + b|1\rangle$$

其中$|1\rangle$和$|0\rangle$代表量子的状态，这两种状态是空间中单位正交基(我们仅考虑最简单常用的情形)，是单个量子实际赖以存在的状态，系数 a 和 b 用来表征状态的概率。

假设有观察者在观察该量子系统，那么他所得到的测量结果是不定的，其中获得$|0\rangle$状态的概率为 $a*a$，获得$|1\rangle$状态的概率为 $b*b$。由此可见，量子的超状态记录的是量子系统和外界作用前的状态，这个状态可用来预测观察者各种可能的观察结果的概率。一个量子超状态并不能告诉我们该量子此刻处于何种确定状态，因为不经过观测我们无法得知，然而它却包含了非常重要的信息：预知未来可能状态的概率。在量子物理学中，一些成对的物理性质是互补的，因此，测量一种性质则必然会干扰另一种性质。例如，位置测量的不确定量∇x和动量测量的不确定量∇p的乘积决不能小于约为 h 的数，它们之间有关系式$\nabla x \nabla p \geqslant h$，即位置和动量不可能同时有完全确定的值。这一原理被称为测不准原理，它并不是仅涉及某一特定测量技术的限制，而是适合于所有可能的测量。

量子的超状态和测不准原理使得量子系统在密钥传输过程中具有任何经典信道所无法替代的优势：轻而易举地检测窃听者的存在。但是敏感的量子系统在外界环境变化及监听者的介入下会改变其状态，那么，我们如何在量子信道中传递公共的密钥信息呢？下面，我们来看一个例子——被命名为“BB84”量子密码本分配方案[4]：

量子密码系统将允许原来未共享有秘密信息的通信双方交换一个密码本。该系统包括一个发射装置和一个接收装置。发送方 A 使用发射装置以 4 种

偏振状态(0度,45度,90度,或135度)中的一种接收状态发送光子(光子可被视为是一个微小的振荡电场,其振荡方位被称为该光子的偏振状态)。接收方B则使用接收装置测量其偏振状态。根据量子力学定律,接收装置能区分直线偏振(0度和90度偏振)或者能迅速地改变结构以区分斜线偏振(45度和135度);然而接收装置却无法同时区分两种类型的偏振状态。其密码本发布需要进行下述步骤:

(1) 发送方A发送出有4种偏振状态中的一种偏振光的光子,而这种偏振状态是由A本人随机选定的。

(2) 对于每个接收到的光子而言,接收者B随机地选择这种类型的测量:或者直线型(+)或者斜线型(×)。

(3) 接收者B记录下其测量结果但是密而不宣。

(4) B公开宣布他所采用的测量类型,而且A告诉他哪种测量是正确的测量类型。

(5) A和B保留下B测量出的正确偏振类型的所有事件。然后将这些事件转换成比特(1和0),并以此成为密码本。(下图1中的(1)～(5)对应于上述步骤)

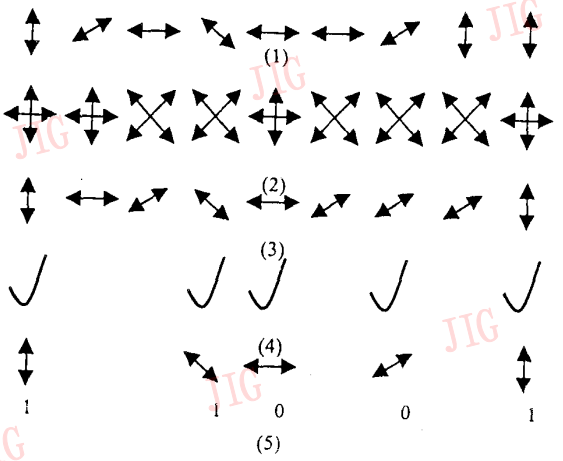

图1 量子密码本的发布过程

在此过程中,为了制造一个量子信道发送光子,发送方首先需要一种偏振滤光片或其它装置,制备已选定偏振方向的光子,而接收者则需要一种测量这些光子偏振方向的方法。接收者的工作可通过另一个偏振滤光片来完成,该滤光片将吸收撞击到其上的一些光子。但是这项工作采用一种双折射晶体(比如方解石)来进行则最方便。双折射晶体能依据入射光子的偏振状态将入射光子送入2个光程中的一个,而不吸收任何光子。碰撞到方解石晶体上的光子可能直接通过晶体并呈现出垂直晶体光轴方向的偏振,或者可能发生偏移并出现沿晶体光轴方向的偏振。光子会表现出两种行为方式中的一种,这取决于它的偏振状态与该晶体的关系。因此,如果接收者知道一给定光子在两个直线方向中的某一方向偏振,即水平(0度)或垂直(90度)方向偏振,则接收者可以用垂直取向的方解石晶体准确地分辨出该光子是由从哪个方向发送入垂直取向的方解石晶体,但是这样的装置不能区分沿对角线方向(45度或135度)偏振的光子。此时沿对角线方向偏振的光子能由一种将上述装置原始取向转动45度的类似装置来准确地加以区分。同样,这种转动45度的装置也不能用来区分垂直偏振与水平偏振的光子。也就是说直线偏振和对角线偏振具有互补的性质,根据测不准原理,这些局限性不仅仅适用于这里所介绍的特定的测量装置而且还适用于任何一种测量装置。

假设有一个窃听者E,他可设法测出量子信道中光子的状态,但由于他不知道每个光子正确的测量类型,由测不准原理,他不可能同时测量到一个光子的直线偏振和对角线偏振状态。因此他所得的测量结果有相当一部分改变了光子的原状态,那么在合法的通信双方A和B处所提取的共享比特信息将不会一致。A和B通过公共信道比较量子信道发出的信号,从而可发现是否有人窃听。如果这种比较检验表明有窃听迹象,那么A和B就放弃他们所有的数据并用一批新光子重新开始通信。如果没有人窃听,则通信双方可从各自的数据中提取出共享比特,从而完成密钥的传送,建立起双方的会话密钥。

3 量子密码的现状及其面临的问题

3.1 量子密码的现状

在过去的几年中,国际上科技界和工业界均对量子密码术显示出了极大的兴趣,量子密码术已被引入了计算机科学和物理学的前沿,量子密码学正在以很快的速度走向实际应用。量子密码学主要应用在下述几方面[2,5]:

(1) 量子密钥的分配和存储。这是量子密码的主要应用。世界上第1个量子密钥分配原型样机在1989年研制成功,它的工作距离仅为32厘米。然而,它的出现标志着量子密码开始初步走向实用。此后,人们在设计及建造实用的量子密钥分配系统方

面作了不懈努力。最近的进展则是由英国电信做出的;据报道,1995 年他们在长达 30 公里的光纤上实现了量子密钥的传送,差错率仅为 1.2～4%。1997 年,他们又利用波分复用(WDM)技术在常规的 1.2Gbit/s 的光纤数据信道(lambda＝1 300nm)上实现了量子密钥的安全传送,工作距离也达到了 28 公里。

Artur K. Ekerth 还利用 EPR(Einstein-Podolsky-Rosen)效应创造出一种保证密码本分配和密码本存储都安全可靠的密码系统。通信双方中的发送方 A 生成一些 EPR 光子对,即一个球型对称原子沿着两个相反方向发射两个光子时,我们称这一对光子为 EPR 光子,EPR 效应就会在这一对光子上发生,EPR 光子对以一个未确定偏振初始状态产生出来,但由于这初始状态的对称性,所以在测量时这两个光子的偏振状态一定是有相反值,只要这些测量是同一类型的。然后 A 将每对中的一个光子留给自己,而将另一个光子传送给接收方 B,收发双方同时测量他们的一些光子以检验是否有窃听,但存储剩余的光子不对进行任何测量,仅在需要密码本之前对所存储的光子进行测量和比较。如果没有人改动所存储的光子,那么当 A 获得 0 时 B 将总是获得 1,反之亦然。如果没有发现差异,A 和 B 就对剩余的存储光子进行测量以获得所需要的密码本。虽然这种系统在理论上是可行的,但它目前还不能用于实际,因为将光子存储零点几秒以上在技术上是不可能的。因此,目前 EPR 效应并不是一种可保证密码本存储安全性的实用工具。

(2) 公共决定(Public Decisions)。量子密码除了可用于保密通信外,还可在保护专用信息的同时将这些信息用于作出公共决定。由 Claue Creapu 提出了这样的技术:允许 2 个人事先约定好一个函数 $f(x,y)$,它仅依赖于 2 个专有输入 x 和 y,其中一个人仅知道自己的专有输入 x,而另一个仅知道自己的专有输入 y,他们都不会透漏任何有关于自己的输入信息给对方,只能通过自己的输入和函数输出来推知对方的输入。这种决策的经典例子是"约会问题",在约会问题中,如果并且仅仅 2 个人互相喜欢时,他们才寻找一种决定约会时间的方式,而用不着泄漏任何详细的信息,如果 2 个人中的 A 喜欢 B 而 B 不喜欢 A,则 B 就用不着去弄清楚 A 是否喜欢自己而放弃约会,另一方面,A 则不可避免地会了解到 B 不喜欢自己。还有许多其它的情况,在这些情况下公司或政府组织之间或者在个人和组织之间作出的共同决定取决于各方不愿完全泄漏的保密信息,量子密码在这些场合也可得到应用。

(3) 消息认证(Message Authentication)。量子密码术也可用于证明一条消息确是出自某人且在传送过程中未被改动过。Wegman-Carter 的认证术和量子密码术的分配能给通信双方带来好处,一方面,量子技术提供由这种认证方法所使用的密码本比特信息,另一方面,Wegman-Cater 认证术又能成功地用于进行量子密码本的发布,即使在对手更为强有力(比如,能更改公共信道传送的消息及偷听这些消息)的情况下也能如此。

(4) 比特承诺(Bit Commitment)。量子密码术还可用于比特承诺,即量子比特承诺,可用来得到任意 NP 问题表述的零知识证明(Zero-Knowledge Proofs)。此外,量子忘记传输(Quantum Oblivious Transfer)——这是一种奇特的信息处理程序可用来实现谨慎决定。该技术以这样的一种方式来传送 2 条消息,以便使接收者能够读出其中的任何一条消息但不能同时读出 2 条消息。相信随着量子物理及计算机科学的进展,量子密码还将会有更多的应用。

3.2　量子密码面临的问题

目前,阻碍量子密码术走向实用的技术问题主要是制造出工作在所需波长上的高效的单光子检测器比较困难,而这对基于光子的量子密码术的实现则是很关键的。因为为了防止窃听者通过一个半镀银镜之类的装置来窃听传送量子信息的光束,即窃听者将每一个闪光分解成 2 个强度较低的闪光,然后读取一个闪光而让另一个闪光继续通过送至接收方,在此过程中闪光的偏振状态未受干扰。如果窃听者仅移走该光束中的适当部分,则接收方可能就察觉不到信号正在减弱。因此,必须以减少量子信道数据传送的速率为代价,让发送方发送极其微弱的闪光:平均而言其强度为每个闪光小于一个光子,以有效地挫败这种窃听。所以,在量子密码术中必须采用高效的光子检测器以减少系统自身错误,同时挫败潜在的窃听者的企图。

另外,由于量子密码系统即使在没有窃听者窃听时,由于系统自身错误,接收方接收的信息也会有一些误差。此外,我们还要防止窃听者假扮合法通信双方中的一方而欺骗另一方,以使对方相信他是合法通信双方中的对方。因此,量子密码术要走向实用,必须结合一些经典技术,如:保密增强,纠错及认

证技术等。这在一定程度上也减弱了量子密码在技术上的优势。

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，因为量子密钥分配技术不得不同一些传统的方法竞争以获得市场，而这些传统方法在长距离上以及在成本费用上更低，从而使量子密码的密钥分配技术处于不利地位。这也是目前量子密码术难于立即转化为实用技术的原因之一。

4 结 语

当前，量子密码术实用还有相当一段距离，但是英国电信试验系统的成功充分说明了这一技术的进展是如何迅速。一旦在长距离的传统光纤信道上实现了量子密钥的传输，则量子密码在技术上及成本上就完全压倒了经典的密码技术。我们也完全有理由相信，一旦量子密码术得以在实际中得到应用，这一定会在21世纪的信息时代中产生不可估量的影响。目前，国内在此领域内还几乎是一片空白，我们也希望国内的量子物理学专家和密码学专家携手合作，在这一全新的有着光明前景的技术领域内做出应有的贡献。

参考文献

1 杨义先，林须端. 编码密码学. 北京：人民邮电出版社，1992：460～514.

2 Bennett C H, Brassard G, Ekert A K. Quantum Cryptography, Scientific American, 1992：50～57.

3 Timothy P Spilier. Quantum Information Processing：Cryptography, Computation and Teleportation. Proceedings of IEEE, 84 (12)：1719～1746.

4 Bennett C H, Brassard G. Quantum public key distribution system. IBM Technical Disclosure Bulletin, 28(7)：175～179.

5 Gilles Brassard. A Bibliography of Quantum Cryptography. http://www.itr.ch:8000/～phinzma/