第24卷第7期 小型微型计算机系统 Vol. 24 No. 7
2003年7月 MINI-MICRO SYSTEMS July 2003

量子密码学的研究进展

刘传才

(福州大学 计算机系，福建 福州 350002)

摘 要：量子密码术是一种新的重要加密方法，它利用单光子的量子性质，借助量子密钥分配协议可实现数据传输的可证性安全.量子密码具有无条件安全的特性(即不存在受拥有足够时间和计算机能力的窃听者攻击的危险)，而在实际通信发生之前，不需要交换私钥.本文综述了量子密码学的研究进展，其中包括了量子密码学的物理基础、量子密钥分配、保密增强、量子密钥的实用性以及目前技术限制所存在的缺陷.

关 键 词：量子信息；量子通信；量子计算；量子密码学；量子密钥分配

中图分类号：TP319；TN918 **文献标识码**：A **文 章 编 号**：1000-1220(2003)07-1202-05

Progress in Quantum Cryptography Research

LIU Chuan-cai

(*Department of Computer, Fuzhou University, Fuzhou* 350002, *China*)

Abstract: Quantum cryptology is a new radical approach to the art of cryptography. This new method utilizes the quantum nature of single photon. Data can be transferred with a proven security via the protocols of quantum key distribution. Quantum cryptograph is unconditionally secure (i.e. secure against a spy who has unlimited time and computer power), and it doesn't require a private key exchange before the actual communication takes place. In this paper, the author reviews the recent research progress in quantum cryptography, including the physical foundation of quantum cryptography, quantum key distribution, privacy amplification, practicality of quantum key, and existing defects due to current technology limitation.

Key words: quantum information; quantum communication; quantum computation; quantum cryptography; quantum key distribution

1 引 言

长久以来，人们一直有实施秘密通信的愿望.随着计算机的出现，这种愿望变为一种必然需要(对于 Internet 通信、银行交易等).在过去，人们已开发出能实现这种目标的方法(遗憾的是许多方法性能低劣)，虽然有些方法是无条件安全的(即不存在受有足够时间和计算机能力的对手窃听的危险)，但在实际通信实施之前需要交换私钥.这种交换私钥的方法至少存在两个可能的缺陷：

(1) 面对面的交换极不方便；

(2) 私钥交换过程中存在着泄密和被窃取的可能(即使是面对面的交换私钥，在送达的过程中也有可能因被电子或 x 射线扫描而失密).

此外，还存在严重的密钥分配欺诈问题.一般来说，只要消息保密，Alice 和 Bob 就能共享一个密钥.但在实际工作中无法确保.信任的信使可被贿赂，或者甚至在没有有关他们的知识的情况下侦听到.更普遍的是能区分经典信号.一个窃听者在不改变信号的情况下能可靠地读出它们.因此，在经典物理学中，原则上无法阻止窃听者被动地窃听密钥分配信道.为克服这些缺陷，人们一直在不懈地探索，希望能用新的加密方法来解决这些问题.令人欣慰的是，已有的研究表明，使用量子力学的特征可实现两个陌生人之间通信的完美保密.

量子密码学的研究可追溯到 1970 年.当时，Wiesner 写了一篇很有创意的有关共轭编码的文章，从而奠定了量子密码学的基础.因 Wiesner 的想法太新奇，论文被拒绝刊登，直到 10 多年后的 1983 年才得以发表[1].当时，Charles H. Bennett(Bennett 那个时候知道 Wiesner 的思想)和 Gilles Brassard 拾起这个课题，他们的研究获得了丰硕的成果，先后发表了一系列文章，并最终用一个实验原型展示了概念的技术可靠性[2].量子密码学系统利用 Heisenberg 的不确定性原理：首先，对量子态的测量会干扰量子态本身，因此，这种窃听方式必然会留下痕迹而被合法用户发现.其次避开直接量子测量而采用量子复制机来复制传送信息的量子态，窃听者将原量子态传送给 Bob，而留下复制的量子态进行测量以窃取信息，这样就不会留下任何被发现的痕迹.但是量子不可克隆定理确保窃听者不会成功，任何物理上可行的量子复制机都不可能克隆出与输入量子态完全一样的量子态来.因此，量子密码学原则上可以提供不可破译、不可窃听的保密通信体系.

收稿日期：2001-09-26 基金项目：国家 973 项目(G1998030600)资助；福建省自然科学基金项目(F00013)资助；福州大学科技发展基金研究项目(XKJ(QD)-0121)资助 作者简介：刘传才，博士，副教授，主要研究方向为模式识别与智能系统、网络信息安全.

此外,在此值得一提的是 Shor 的量子算法[3~5]. 他将著名的 NP 问题转化为 P 问题,矛头直指 RSA 方法. 此算法证明,采用量子计算机可以轻而易举地破译象 RSA 这样的公开密钥体系,从而在全球掀起了量子计算的研究热潮.

2 量子密码学的物理学基础

信息一旦量子化,量子力学的特性便成为量子信息的物理基础[4,5],这主要有量子纠缠[6,7]、量子不可克隆、量子叠加性和相干性. 因为量子力学的线性特性禁止对任意量子态实行精确的复制,量子不可克隆定理和 Heisenberg 测不准原理构成了量子密码学的物理基础.

2.1 量子不可克隆定理

Wootters 和 Zurek 曾于 1982 年在《自然》杂志上撰文提出了如下问题:是否存在一种物理过程,实现对一个未知量子态的精确复制,使得每个复制态与初始量子态完全相同呢? Wootters 和 Zurek 证明,量子力学的线性特性禁止这样的复制,这就是量子不可复制定理的最初表述[8].

量子不可克隆定理的证明很简单. 以两态量子系统为例,将基矢选为$|0\rangle$和$|1\rangle$,设$|s\rangle$代表此二维空间的任意量子态,量子克隆过程可以表示为

$$|s\rangle|Q\rangle_x \rightarrow |s\rangle|s\rangle|\tilde{Q}\rangle_x \tag{1}$$

式中右端$|s\rangle|s\rangle$表示初始模和复制均处于$|s\rangle$态,$|Q\rangle_x$和$|\tilde{Q}_s\rangle_x$分别为装置在复制前后的量子态,复制后装置的量子态$|\tilde{Q}_s\rangle_x$可能依赖于输入态$|s\rangle$. 若存在(1)式的变换,那么对基矢$|0\rangle$和$|1\rangle$应分别有

$$|0\rangle|Q\rangle_x \rightarrow |0\rangle|0\rangle|\tilde{Q}_0\rangle_x \tag{2a}$$

$$|1\rangle|Q\rangle_x \rightarrow |1\rangle|1\rangle|\tilde{Q}_1\rangle_x \tag{2b}$$

现假设$|s\rangle$是一个任意的叠加态,即

$$|s\rangle=\alpha|0\rangle+\beta|1\rangle,\ |\alpha|^2+|\beta|^2=1 \tag{3}$$

由(2)式及量子操作的线性特征不难导出,在操作后,$|s\rangle$将演变为$|s\rangle|Q\rangle_x=(\alpha|0\rangle+\beta|1\rangle)|Q\rangle_x \rightarrow \alpha|0\rangle|0\rangle|\tilde{Q}_0\rangle_x+\beta|1\rangle|1\rangle|\tilde{Q}_1\rangle_x)$. 若复制机的态$|\tilde{Q}_0\rangle_x$与$|\tilde{Q}_1\rangle_x$不恒等,那么上式给出的初始模和复制模均处于$|0\rangle$与$|1\rangle$的混合态;若态$|\tilde{Q}_0\rangle_x$与$|\tilde{Q}_1\rangle_x$恒等,则初始模和复制模将处于纠缠态$\alpha|0\rangle|0\rangle+\beta|1\rangle|1\rangle$. 无论哪种情况,初始模和复制模都不可能处于直积态$|s\rangle|s\rangle$. 因此,如果一个量子复制机能精确复制态$|0\rangle$和$|1\rangle$,则它不可能复制两态的叠加态$|s\rangle$,这就是量子不可克隆定理的内容.

量子态不可克隆是量子力学的固有特性,它设置了一个不可逾越的界限. 量子不可克隆定理是量子信息科学的重要理论基础之一. 量子信息是以量子态为信息载体(信息单元). 量子态不可精确复制是量子密码术的重要前提,它确保了量子密码的安全性,近年来人们对它作了进一步的研究,揭示出更丰富的物理内涵.

在 W-Z 的证明中,假设输入态是完全未知的. 但在实际情况中,往往知道输入态属于一个确定的态集合. 例如在基于非正交态的量子密码术中,输入态是两个非正交态的其中一个. W-Z 的证明依据量子叠加原理,该证明至少需要 3 种可能的输入态,如上面$|0\rangle$,$|1\rangle$及$\alpha|0\rangle+\beta|1\rangle$,因此它没有排除克隆两个量子态的可能性. 之后人们推广了量子不可克隆定理,使之适用于两态情况,并指出如果克隆过程可以表示为一幺正演化,则幺正性要求两个态可以被相同的物理过程克隆,当且仅当它们相互正交,亦即非正交态不可以克隆[9]. 该结果在量子密码学中有重要应用,我们知道,一个简单的量子密码方案就是随机地传送两个非正交的量子态,正因为非正交态不可克隆,所以窃听者无法窃取信息.

适用于两态的量子不可克隆定理后来被进一步推广到混合态的情况,并证明了一个更强的定理,文献中称为量子不可播送定理[10]. 近来不可克隆定理又被推广到纠缠态的情况[11]. *Mor* 甚至指出复合系统的正交态不可以被克隆[#1],而这种正交态的不可克隆定理需要狭义相对论做基础.

量子不可克隆定理断言,非正交态不可以克隆,但它并没有排除非精确克隆即复制量子态的可能性. 目前主要有两种克隆机:普适克隆机和概率克隆机.

2.2 Heisenberg 的测不准原理

由测不准原理可知,对任何一个物理量的测量都不可避免地对另一物理量产生干扰. 这就使得通信双方能够检测到信息是否被窃听,这一性质使通信双方无须事先交换密钥即可进行绝密通信. 换句话说,无须通信双方事先交换密钥,量子加密学为人们提供了一种无条件安全的希望. 不依赖问题的计算难度,量子加密学使用基本的物理定律提供了可证的无条件安全. 并且不象一次一密的密钥,任何窃听量子密钥交换和拷贝密钥的人不可能不被检测到. 依据测不准原理,根本不可能知道诸如粒子的动量和它的位置这些辅助变量的准确值[12,13]. 由量子力学施加的这一表观限制可成为一个强有力的捕获窃听者的工具. 其中心思想是使用非正交的量子状态来为信息编码. 更具体地说,量子密码学的本质可理解为如下问题:给定用四个可能的极化状态(↔,↕,↗,或↖↘)之一来描述单个光子,人们是否能肯定地确定它的极化呢?答案是否定的. 直线基(↔和↕)与对角线基(↗和↖↘)是不相容的,因此测不准原理禁止我们同时度量两者,更一般地说,即使仅部分可靠,判别非正交状态的实验将干扰状态.

3 量子密钥分配协议

在量子密码学中,Alice 和 Bob 间的秘密通信是靠量子密钥分配协议的支撑来实现的. 在某一加密系统中,依据协议,Alice 和 Bob 能在一个即将作为密钥的秘密 bit 串问题上达成一致意见. 目前,量子密码的方案主要有四种:

① 基于两种共轭基的四态方案,其代表为BB84协

[1]Mor T. Phys. Lett., 1998, 80: 3137.

[2]Li C-F, Zhang Y-S, Guo G-C, et al. unpublished. (可在文献[4]中看到有关的说明);

议[14]；

② 基于两个非正交态的两态方案，如 B92 协议[15]；

③ 基于 EPR 佯谬的 EPR 对方案，由 Ekert 于 1991 年提出，称为 EPR 协议或 E91 协议[16]；

④ 基于正交态的密钥分配方案[17, 18]，其基础为正交态的不可克隆定理.

显然，量子密码(量子密钥分配)实际上是量子辅助的经典密码. 最近，李传锋等建立了真正意义上的量子密码体系#2.

量子密钥分配 QKD (quantum key distribution)的第一个演示性实验由 Bennett 等人完成[19]. 目前有两个实验方向：光纤中的 QKD 和自由空间的 QKD. 光纤中 QKD 实验已逐渐走向成熟[20~23]，目前传输距离已达到 48km#3. 自由空间中的 QKD 也不断取得突破[23]，现在达到的传输距离为 1.5km，而且是在白天进行的实验. 前面的实验都是基于 BB84 或 B92 协议，最近 E91 协议的 QKD 也已取得重大进展[24, 25].

最初的量子密钥分配协议使用单光子的四种不同极化状态作为量子信息的载体[2]，后来相继提出了其它的量子密钥分配协议. 早期的变种有使用 EPR 纠缠对的协议[16]、有仅采用两个非正交态而不是四态的协议[15]、有运用相位调制而不是极化的协议[15, 26]. 即使是在贮藏状态而非传输状态时，使用纠缠对的一个理论好处是允许密钥保留，并受到 Heisenberg 的测不准原理的保护. 最新的变种采用了拒绝的数据协议 (rejected-data protocols)[27, 28]、光子对#4 和亮光 (bright light)#5.

4 保密增强

在实际的量子加密系统中，光子检测器总存在着噪声，因此，即使不存在窃听，Alice 和 Bob 的 bits 也将不一致. 其次，当前的技术还无法可靠地生成单光子. 实际的光子发射器目前只能产生拥有一个特定平均光子数的光脉冲，即平均来说，生成的每个脉冲有 m 个光子，但每次不一定恰好是那个数目. 显然，若 m 比 1 大，以及只要余数不继续干扰 Bob，则 Eve 就能获得分开脉冲和观测一个光子的好机会. 如果 m 比 1 小得多，则一个窃听者能分开脉冲的概率近似为 $m^2/2$[2]. 即使在此情形下，窃听者也能获取此密钥 bits 的常数部分而不被检测到.

文献[2]描述了如何解决这些难点问题. 使用 BB84 协议，Alice 和 Bob 首先通过公开讨论使他们的数据一致. 在量子传输阶段，泄露给 Eve 的信息不过是她可能已获取到的信息. 因此，使用所谓“保密增强(privacy amplification)”，Alice 和 Bob 从他们的部分私钥蒸馏出一个更小而更安全的密钥.

文献[2]描述了使 Alice 和 Bob 的 bits 一致的过程，此过程发生在一个公共信道上. 由于 Eve 有可能监听到所有的公共传输，因此 Alice 和 Bob 为确保他们以相同的密钥结束，就必须尽可能少地泄露信息. 在通信双方的串中，通过两个步骤就可实现此目标：① 首先使 bits 的随机置换一致以便使错误位置随机化；② 其次将最后得到的串分成大小为 b 的块. 选择常数 b 以使每块所包含的错误数不大于 1. 在 BBBSS 的实现中，是通过实验而不是理论来选择 b 的. 最后，Alice 和 Bob 比较每块的奇偶误差. 若发现一对不匹配的奇偶误差块，Alice 和 Bob 就继续将此块二分成越来越小的块，而且每次都要比较奇偶误差，直到发现错误为止. 为防范 Eve 了解此过程，Alice 和 Bob 抛弃掉每个已泄露奇偶误差的块的末尾一位.

一旦完成此过程之后，在那些碰巧包含偶数错误的块中，将仍存在不匹配. 因此随着块大小的增加，Alice 和 Bob 要重复此过程多次直到确信错误总数足够低为止. 此外，由于 Alice 和 Bob 必须抛弃所比较的每一块的一位，因而上述策略的效率低. 为此，Alice 和 Bob 转换到一个需再执行多次的新策略上. 每次，在他们的完整串中，选择一个 bit 位置的随机子集，并比较奇偶误差. 如果子集串不相同，则不一致的概率正好为 1/2. 如果不一致发生，则执行一个二分搜索来发现错误. 在二分搜索中使用的是随机子集而不是块，并抛弃掉每个子集的末尾 bit，最后消除掉所有的错误. 在未发现假定的相同串的任何错误的情况下，Alice 和 Bob 仍将仔细实施相当多的奇偶检验.

此处，Alice 和 Bob 所实施拥有的相同串不完全是私有的. 对部分串或者，分束，或者实施截获/重送，在此过程中 Eve 可能会获得某些有关 Alice 和 Bob 的信息. 虽然第二种策略在 Bob 的串中可能引起某些错误，如果 Eve 仅在少数 bits 上使用此策略，则在探测器和别的物理问题中，诱发的错误将会由噪声引起的错误所湮没. 在通信双方数据一致的阶段，因抛弃掉每个奇偶检验集的末尾 bit，故 Eve 就不会获得任何信息. 然而，Eve 的某些有关特定 bits 的最初信息可能已转变成奇偶位的信息. 例如，在串 y 中，如果 Eve 知道位(bit)x 的值，以及 Alice 和 Bob 泄露了 y 的奇偶误差和抛弃掉 x，那么 Eve 就会知道 y 的保留 bits 的奇偶误差. 如果 Eve 知道一个串的奇偶检验位是她所知道的那个串的一个非空子集的奇偶误差，以及如果 Eve 开始至多只知道密钥的 k 个物理比特，则在协调一致之后，Eve 也只能至多知道密钥的 k 个物理比特[2].

在任何情形下，Alice 和 Bob 共享一个 n-bit 的串 S，并且假定 Eve 至多知道 S 的 k 个确定性(即奇偶或物理的)的 bits. Alice 和 Bob 希望计算一个 r-bit 的密钥 K，而且 $r<n$，这样 Eve 期望的有关 K 的信息就在某个特定的范围之外. 为实现此目标，Alice 和 Bob 将选择一个降维函数 $g:\{0,1\}^n\to\{0,1\}^r$，并计算 $K=g(S)$. 问题是哪类函数适合这样的用途？那就是说，当应用于 S 时，哪些函数能生成一个 Eve 几乎不知道的密钥 K 呢？

定义[29]：对 A 中任何性质不同的 x_1 和 x_2，如果 $g(x_1)=g(x_2)$ 的概率至多为 $1/|B|$(依据均匀分布从 G 中随机地选择

#Hughes R J, et al., J. Mod. Opt., 2000, 47(3): 533~547;

#Huttner S M, Peres A. Quantum cryptography with photon pairs. J. of Modern Optics, to appear;

#Wiesner S. Quantum cryptography with bright light. manuscript, 1993.

g),那么函数 $A\to B$ 类 G 是普适的.

一个普适类的例子是 A 本身的置换集合,既然适用于此集合中的任意 g,那么 $g(x_1)=g(x_2)$ 的概率为 0,显然此概率值比 $1/|A|$ 小.文献[29]指出,如果 *Eve* 知道 S 的 k 个确定性的 bits,以及 Alice 和 Bob 随机地从通用的散列函数 $\{0,1\}^n\to\{0,1\}^r$ 类中选择降维函数 g (其中对于某些安全参数 $0<s<n-k$,有 $r=n-k-s$),那么 Eve 有关 $K=g(S)$ 的期望信息小于或等于 $2^{-s}/\ln 2$ bits.按这样的方式构造的散列函数[2]既可用于生成密钥 K,又可用于 Alice 和 Bob 计算 S 的 r 个随机子集的奇偶误差,这样就保留了结果的秘密.r 个奇偶误差结果将为最终的 r-bit 密钥.

如果获得这样的结果,人们可能要问 Alice 和 Bob 是如何确定 k 的值的,即有多少信息已泄露给 Eve 了.作一个保守的估计,他们可能只假定所有的传输错误都是由窃听引起的(虽然某些错误不见得起源于检测错误).

窃听错误或者可能源于截获/重送,或者源于分束.Alice 和 Bob 可使用束强度 m 和比特错误率来计算 Eve 已获取到的 S 的期望部分.如果 Alice 和 Bob 的假设是保守的,并添加多个标准偏差到他们的结果中,则可获得一个关于泄露给 Eve 的 bits 数的安全上界[2].

上述的讨论假定 Eve 仅知道确定的 bits,人们自然要问它是否可能对 Eve 获得有关 S 的概率信息更有帮助.换言之,不象 Alice 和 Bob 那样在同样的基上测量光子,Eve 可以在它们中间选择一个基.不管 Alice 使用哪个基,将会给 Eve 创造匹配 Alice 基的机会,而且其匹配的概率近似为 85%[30].即使当 Bob 泄露他的测量选择时,Eve 也将不会获得任何信息,因此使用这种策略,她的所有信息是随机的而不是确定的.可以想象,这种随机信息比确定性的信息更抗保密增强.然而,结果并不是这样的情况[30],因此,如果 Eve 希望最优化她关于最终密钥的期望信息,她应象 Alice 和 Bob 那样使用同样的基,方可获得确定的 bits.

5 实用性

很自然,人们要问是否有可能实际地实施上述量子密钥分配系统.答案是肯定的,但要受到实际条件的制约.实际上,Bennett 等制造的装置实现了他们所描述的协议[2],并说明协议是行得通的.然而,量子信道仅 32cm 长.在长距离上实现他们的系统出现的问题是光缆瓦解了光的极化,因此,光子需要通过一个真空直管发送.因干涉模式在光缆中生存得更长[31],Zimmer 在 1992 年采用干涉技术建造了一个 200 码的量子信道.就在次年,采用干涉技术建立了一条 10km 长的量子信道[32,33].尽管如此,将量子信道延伸到更远的距离仍存在较大的问题.沿商用光缆传送消息经过一段距离后会衰减,并且必须周期地通过转播站来放大信号,若不以窃听瓦解信号的方式来瓦解信号,就不能放大量子信号.

在第一个量子密钥分配协议的基础上,相继开发出其他的量子密码协议,而且这些协议在短距离上更有意义.尤其是已提出了隐形传态[30]和比特承诺[34]的量子协议,此协议采用了同样的传输技术、一致(econciliation)技术和保密增强技术.在零知识证据中和其它有协同操作而互不信任的两方的情形下采用隐形传态和比特承诺.这样的情形即使在面对面的谈判中也可能发生,在此场合下,桌面量子设备可能是有用的.

在量子密码学中,已有研究者探索出用不同方法来实施已建立起的协议.一个可供选择的实现[31,16]包括使用所谓的"纠缠对",而纠缠对是通过一定的粒子反应产生的光子对.每个纠缠对包含两个相反极化的光子.在此系统中,在 Alice 和 Bob 之间的某些点上发射纠缠对,Alice 和 Bob 每人都用随机选取的基来测量光子.然后比较他们使用过的那些基,而仅保存那些用同样基测量的光子作为他们的密钥.在光子到达 Alice 或 Bob 之前,如果 Eve 试图读出某个光子,而 Eve 用的一个基与通信双方所用的基不同,则 Alice 和 Bob 将不会再测量到相反的极化.此外,通过比较少的 bits,Alice 和 Bob 就能判断出是否有窃听事件发生.与 BB84 协议比较,这一系统的理论优点如下:就使用 BB84 协议而言,Alice 和 Bob 对密钥取得一致意见之后,必须将密钥存储在他们的计算机(或某些别的非量子装置)中,并且 Eve 有可能闯入和窥探到密钥而不被发觉.但理论上可将光子纠缠对无限地存储起来而不曾被观测到.仅当 Alice 和 Bob 实际上需要使用此密钥时,他们才会去测量它们.如果 Eve 窥探密钥,则 Alice 和 Bob 就会发觉.当然,目前的技术还无法实现任意时间长度的光子存储,因此,现在这种方法并不比 BB84 更好.

虽然量子加密现在还不是很实用,但仍值得我们去研究它.量子加密不象公钥加密系统,其安全性是可证明的,并且无论计算机运算速度多快,或者即使 P=NP,也不会损害它的安全.当前,量子加密系统仅在短距离上奏效,但存在即使短距离传输也有用的情形.此外,随着技术进步,未来有可能在长距离上实施量子加密,因此,私钥系统将不再需面对面地交换密钥.我们知道,保密增强的概念最初是在量子加密学中发展起来的.最终,可将这一概念扩展到 Eve 掌握 Alice 和 Bob 共享一个串的部分知识的任何情形.

References:

1 Wiesner S. Conjugate coding[J]. Sigact News, 1983, 15(1): 78~88.

2 Bennett C H, Bessette F, Brassard G, Salvail L, Smolin J. Experimental quantum cryptography[J]. Journal of Cryptology, 1992, 5(1): 3~28.

3 Shor P W. Algorithms for quantum computation: Discrete logarithms and factoring[A]. Proceedings of the 35th Annual Symposium on the Foundations of Computer Science[M]. Shafi Goldwasser ed., IEEE Computer Society Press, Los Alamitos, 1994: 124~133.

4 Li Chuan-feng, Guo Guang-can. Progress in quantum information research[J]. Progress in Physics, 2000, 20(4): 407~431

5 Zhao Zhi, Feng Mang, Zhan Ming-sheng. Quantum algorithm and quantum computing experiments[J]. Progress in Physics, 2001, 21(2): 183~215

6 Einstein A, Podolsky B and Rosen N. Can quantum-mechanical description of physical reality be considered complete[D]. Phys.

Rev., 1935, 47, 777～780, Reprinted in Quantum theory and measurement, J. A. Wheeler and W. Z. Zurek, eds., Princeton University Press, 1983.

7 Milburn Gerard J. The feynman processor (Guo Guangcan et al. translate) [M]. Nanchang: Publishing House of Jiangxi Education, 1999, 49～55

8 Wootters W K, Zurek W. A single quantum cannot be done[J]. Nature, 1982, 299(28): 802～803.

9 D' Ariano G M, Yuen H P. Impossible of measuring the wave function of a single quantum system [D]. Phys. Rev. Lett., 1996, 76(16): 2832～2835.

10 Barnum H, Caves M. et al. Noncommuting mixed states cannot be broadcast [D]. Phys. Rev. Lett., 1996, 76(15): 2818～2821.

11 Koashi M, Imoto N. No-cloning theorem of entangled states [D]. Phys. Rev. Lett., 1998, 81(9): 4264～4267.

12 Goldwater Sharon. Quantum cryptography and privacy amplification [EB/OL]. http://www.ai.sri.com/～goldwate/quantum.html

13 Gottesman Daniel, Lo Hoi-Kwong. From quantum cheating to quantum security [EB/OL]. Physics Today (online), http://www.physicstoday.org/pt/vol-53/iss-11/p22.html.

14 Bennett C H, Brassard G. Quantum cryptography: public-key distribution and coin tossing [C]. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, Dec. 1984, 175～179.

15 Bennett C H. Quantum cryptography using any two nonorthogonal states[D]. Phys. Rev. Lett., 1992, 68(21): 3121～3124.

16 Ekert A K. Quantum cryptography based on Bell's theorem[D]. Phys. Rev. Lett., 1991, 67(6): 661～663.

17 Goldenberg L, Vaidman L. Quantum cryptography based on orthogonal states [D]. Phys. Rev. Lett., 1995, 75(7): 1239～1243.

18 Masato, Imoto N. Quantum cryptography based on split Transmission of one-bit information in two steps [D]. Phys. Rev. Lett., 1997, 79(12): 2383～2387.

19 Bennett C H, Brassard G. The Down of a new era in quantum cryptography: the experimental prototype is working [J]. SIGACT news, Stein ed., Addison-Wesley, 1989, 20: 78～83.

20 Townsend P D. Quantum cryptography on multiuser optical fiber networks[J]. Nature (London), 1997, 385(6611): 47～49.

21 Muller A, Breguet J, Gisin N. Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1 km[J]. Europhys. Lett., 1993, 23(6): 383～388.

22 Franson J D, Ilives H. Quantum cryptography using optical fibers[J]. Appl. Optics, 1994, 33(14): 2949～2954.

23 Butter W T, et al. Free-space quantum-key distribution [D]. Phys. Rev. A, 1998, 57(4): 2379～2382.

24 Jennewein T, Simon C, Wejns G, Weinfurter H, Zeilinger A. Quantum cryptography with polarization entangled photons[D]. Phys. Rev. Lett., 2000, 84: 4729～4732.

25 Naik D S, Peterson C G, White A G, Berglund A J. Entangled state quantum cryptography: eavesdropping on the Ekert protocol[D]. Phys. Rev. Lett., 2000, 84: 4733～4736.

26 Ekert A K, Rarity J G, Tapster P R, Palma G M. Practical quantum cryptography based on two-photon interferometry[D]. Phys. Rev. Lett., 1992, 69(9): 1293～1295.

27 Barnett S M, Phoenix S J D. Information-theoretic limits to quantum cryptography [D]. Physical Review A, 1993, 48(1): R5～R8.

28 Barnett S M, Phoenix S J D. Bell's inequality and rejected-data protocols for quantum cryptography [J]. J. of Modern Optics, 1993, 40(8): 1443～1448.

29 Bennett C H, Brassard G, Crepeau C, Maurer U M. Generalized privacy amplification [J]. IEEE Trans. on Information Theory, 1995, 41(6): 1915～1923.

30 Bennett C H, Brassard G, Crepeau C, Skubiszewska M -H. Practical quantum oblivious transfer[C]. Advances in Cryptology - Proceedings of Crypto '91, Lecture Notes in Computer Science, Springer-Verlag, Berlin, 1992, 576, 351～366.

31 Zimmer C. Perfect gibberish [J]. Discover. September 1992, (1): 92～99.

32 Townsend P D, Rarity J G, Tapster P R. Single photon interference in a 10 km long optical fiber interferometer[J]. Electronics Letters, April 1993, 29(7): 634～635.

33 Townsend P D, Rarity J G, Tapster P R. Enhanced single photon fringe visibility in a 10 km-long prototype quantum cryptology channel[J]. Electronics Letters, July 1993, 29(14): 1291～1293.

34 Brassard G, Crepeau C, Jozsa R, Langlois D. A quantum bit commitment scheme provably unbreakable by both parties [C]. Proceedings of the 34th IEEE Symposium on Foundations of Computer Science, November 1993, 362～371.

附中文参考文献：

4 李传锋，郭光灿. 量子信息研究进展[J]. 物理学进展，2000，20(4)：407～431.

5 赵志，冯芒，詹明生. 量子算法与量子计算实验[M]. 物理学进展，2001，21(2)：183～215.

8 Milburn G J. 费曼处理器(郭光灿等译)[M]. 南昌：江西教育出版社，1999，49～55.