量子密码学前沿阅读报告

姓名：叶奕含　　学号 3200103514

所在学院：信息与电子工程学院, 浙江大学
Email: zjuyeyihan@zju.edu.cn

摘要：在今天的互联网时代，机密信息的安全传输是一个亟待解决的问题。随着量子计算领域的发展，利用量子密码学确保密钥的安全性逐渐进入商业应用领域。本文对量子密码学的背景、量子原理和应用做了简单的整合，对量子加密领域进行回顾和展望。

一．背景介绍

从古至今，人们一直有实现秘密通信的愿望。在传统的数字通信系统中，可以被动地监视或复制信息；一些窃听者甚至可以改变信息。经典的密码系统方法（Rivest-Shamir-Adleman, RSA）、数据加密标准（DES）基于数论等。如果双方最初不共享密钥，那么在经典系统中，在双方之间的不安全信道上共享密钥将是不可能的。随着互联网发展，公民的个人信息和国家安全数据都是通过互联网传输，这些传输数据的重要性使得安全秘密通信的愿望变成一种必然需要。在过去，人们通常利用传统加密方式，收发双方必须交换密钥才能顺利实现信息的加密和解密，在传输密钥的过程中就存在许多问题：

（1） 面对面交换极不方便；

（2） 密钥交换过程中存在泄密和被窃取的可能（即使面对面交换密钥，在送达的过程中仍可能被窃取失密）。

在经典系统中原理上总存在窃密手段，保证密钥系统安全的前提是保证密钥的绝对安全，但这个前提是无法实现的。

此外，还存在严重的密钥分配欺诈问题。信使的安全性无法保证，密钥甚至可以在没有有关他们的知识的情况下被侦听。更普遍的是，一个窃听者在不改变信号的情况下可以有效读取经典信号。在经典物理学中，原则上无法阻止窃听者被动窃听密钥分配信道。

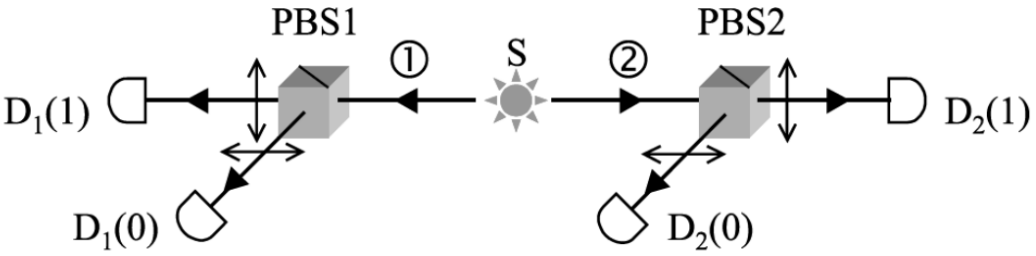
对于安全通信的迫切需要使得人们将目光投向量子领域，量子密码学应运而生，其可以提供完美的一次性密钥解决方案。量子密码学（Quantum cryptography）泛指利用量子力学的特性来加密的科学，其目的是提供一个可靠的方法（或者信道）使得没有人可以截获密钥。量子密码学最著名的例子是量子密钥分发，而量子密钥分发提供了通信两方安全传递密钥的方法，且该方法的安全性可被信息论所证明。目前所使用的公开密钥加密与数字签名（如 ECC 和 RSA）在具规模的量子电脑出现后，都会在短时间内被破解。量子密码学的优势在于，除了经典密码学上的数学难题之外，再加上某些量子力学的特性，可达成经典密码学无法企及的效果。例如，以量子态加密的信息无法被克隆。又例如，任何试图尝试读取量子态的行动，都会改变量子态本身，这使得任何窃听量子态的行动会被发现。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。

量子密码学的研究可以追溯到 1970 年，Wiesner 写了一篇关于共轭编码的文章，奠定了量子密码学的基础。但由于其想法太超前，这篇文章直到 1983 年才得以发表。Charles H.Bennett 和 Gilles Brassard 拾起这个课题，得到了一系列研究成果，最终用一个实验原型展示了概念的技术可靠性。此外，还有 Shor 的量子算法，将 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像 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。

二．原理

1.量子测量的破坏性

爱因斯坦、波多尔斯基和罗森在 1935 年为证明量子力学的不完备性提出了 EPR 佯谬。



在这个实验里，粒子源向两个相反的方向发出一对关联光子，分别经过一个偏振分束器，然后被两对探测器在不同的偏振路径上被接收到。光子的关联性使得 D1(1)和 D2(1)同时观测到光子，或者 D1(0)和 D2(0)同时观测到光子。

由于出射光子的偏振是不同偏振态$|\leftrightarrow\rangle$和$|\updownarrow\rangle$的线性组合，这意味着光子①和光子②无论距离多远都会因为对某一光子的测量，瞬间坍缩到同一本征态上。

由此，我们假设一微观系统的波函数为$|\psi\rangle$，这时算符$\hat{A}$的平均值为$\langle A\rangle=\left\langle\psi\middle|\hat{A}\middle|\psi\right\rangle$，如果$|\psi\rangle$不是$A$的本征态，那么获得$\langle A\rangle$需要通过多次测量取平均。每次测量随机获得$A$的本征值$A_n$。如果将波函数通过本征波函数展开$|\psi\rangle=\sum_n c_n|\psi_n\rangle$，所以测量得到$A_n$的几率是$|c_n|^2$。如果持续同样的测量，由于系统状态已经坍塌到$|\psi_n\rangle$，所以会一直得到同样的$A_n$。我们无法使用线性代数理论有效地描述波函数坍塌的过程。

2.量子不可克隆原理

量子测量是一种破坏性测量，会导致系统坍塌，由此可以得到量子不可克隆原理。

假设量子可以被克隆，即我们可以通过一种方法使得

$$|\psi\rangle|X\rangle\rightarrow|\psi\rangle|\psi\rangle$$

那么我们可以得到

$$|\psi_1\rangle|X\rangle\rightarrow|\psi_1\rangle|\psi_1\rangle\qquad|\psi_2\rangle|X\rangle\rightarrow|\psi_2\rangle|\psi_2\rangle$$

如果我们希望克隆一个线性组合态$|\psi\rangle=\alpha|\psi_1\rangle+\beta|\psi_2\rangle$，那么

$$|\psi\rangle|X\rangle \to \alpha|\psi_1\rangle|\psi_1\rangle + \beta|\psi_2\rangle|\psi_2\rangle$$

但实际上我们应该得到

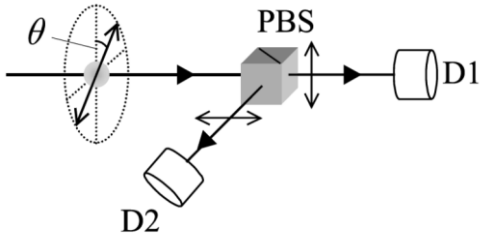
$$|\psi\rangle|X\rangle \to (\alpha|\psi_1\rangle + \beta|\psi_2\rangle)(\alpha|\psi_1\rangle + \beta|\psi_2\rangle)$$
$$= \alpha^2|\psi_1\rangle|\psi_1\rangle + \beta^2|\psi_2\rangle|\psi_2\rangle + \alpha\beta|\psi_1\rangle|\psi_2\rangle + \alpha\beta|\psi_2\rangle|\psi_1\rangle$$

上式可以证明一个非平庸的线性叠加态是无法被克隆的。

量子不可克隆原理是量子力学的固有特性，它设置了一个不可逾越的界限，是量子密码技术的重要前提，它确保了量子密码的安全性。

2.量子密码学应用

量子力学告诉我们，我们无法测量一个处于非平庸的线性叠加态的粒子而不改变其状态。而量子不可克隆原理告诉我们，我们无法截获和测量一个粒子，然后克隆一个完全一样的粒子进入原始信道。所以我们可以利用这一原理，通过量子原理暴露窃听者，进而确保传输信息的安全性。



对光子的偏振态测量是当前实用化量子密钥分发系统的基本手段。如果我们假设入射光子与垂直偏振方向的夹角为θ，当$\theta = 0°$，D1 会探测到光子；当$\theta = 90°$时，D2 会探测到光子。如果我们把偏振态写成垂直偏振态和水平偏振态的线性叠加

$$|\theta\rangle = \cos\theta|\updownarrow\rangle + \sin\theta|\leftrightarrow\rangle$$

对接收端来说，接收到垂直偏振态的几率为$\cos^2\theta$，接收水平偏振态的几率为$\sin^2\theta$。

如果窃听者 Eve 使用同样的偏振分束器进行窃听，那么他只能窃听到垂直或水平偏振态中的一个，然后复制并送出一个本征态，显然，这破坏了原有的量子信息。更一般的，Eve 的目的在于探测出信道中光子的偏振角度θ，然后送出一个同样偏振为θ的光子，但由于量子不可克隆原理，只能送出一个不同偏振角度的新光子，这将改变原有的信息。

三．前沿讨论与分析

1.量子密钥分发的架构协议

在量子密码学中，Alice 和 Bob 问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 协议；

② 基于两个非正交态的两态方案，如 B92 协议；

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；

④ 基于正交态的密钥分配方案，其基础是正交态的不可克隆原理。

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。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。

2.量子密钥分配技术

量子密钥分配（QKD）主要有两个实验方向：光纤中的 QKD 和自由空间 QKD。目前光纤中的 QKD 实验已经逐渐走向成熟。

如今，在“墨子号”量子通信实验卫星和“京沪干线”的交互下，经过两年多稳定性、安全性测试，中国已经实现了 4600 公里的量子保密通信网络，并为超过 150 名用户提供服务。与此同时，科学家们也在探索一些更为前沿的新技术以解决距离问题。例如，双场量子密钥分发（TF-QKD）。在这方面，潘建伟团队与其合作者将真实环境中光纤的双场量子密钥分发距离从 300 公里拓展到了 509 公里。另一方面，高轨道的卫星可以作为天基中继站点。对于长距离或洲际用户来说，由于自由空间内量子信号衰减水平低、退相干效应可以忽略，星地 QKD 成了最具吸引力的方案。目前，“京沪干线”地面量子通信光纤网络已在为 150 多名用户提供服务，在这方面，潘建伟团队演示了上转换单光子探测器、密集波分复用、高效顶底传输、实时后处理和监控等核心关键技术，最重要的是对抗已知的量子攻击。关于星地链路，他们则通过大幅提升系统软硬件设计实现了高速星地 QKD。硬件方面，优化了地面接收器的光学系统，提高了 QKD 系统的时钟速率；软件方面，采用更高效的 QKD 协议来生成密钥。

此外，他们还将星地 QKD 距离从 1200 公里提升到 2000 公里，相应的覆盖角度为 170 度，几乎是整个天空。南山地面站里的远程用户可以与“京沪干线”上的任一节点进行 QKD，无需额外的地面站或光纤链路。光纤 QKD 链路长达 2000 公里，而星地 QKD 链路长达 2600 公里，两相结合，网络内任意一个用户可以实现最长达到 4600 公里的量子保密通信。基于这些技术突破，由一个包括 700 多个 QKD 链路的大规模光纤网络和两段星地自由空间 QKD 链路组成的、一个集成的星地量子通信网络已经成形。

据介绍，该网络平均成码率比此前的“墨子号”实验高出 40 多倍。光纤 QKD 链路长达 2000 公里，而星地 QKD 链路长达 2600 公里，两相结合，网络内任意一个用户可以实现最长达到 4600 公里的量子保密通信。

今年，王爽及其团队展示了如何在 833.8 公里的距离内以 140dB 的信道损耗实现基于光纤的量子密钥分配。

新的设置在容忍信道损耗和基于光纤的 QKD 的长传输距离方面创造了记录，同时实现了优于以前双场量子密钥分配的安全密钥速率相似距离的实验。设置中没有光放大器有助于降低复杂性和成本，在现场和网络应用中具有巨大潜力。该研究提供了一种实用的格式来扩展传输距离并为更广泛的 QKD 实验铺平道路。

四．总结与展望

就目前而言，经典密码学仍然是安全的，因为经典计算机无法破解密码算法。在 BB84 协议设计后，量子密码学的概念迅速商业化。有关量子密码学的研究论文逐年增加。量子计算机的发展将极大地提高计算速度。各种研究组织和公司正在广泛致力于开发后量子算法。与此同时，更多的攻击、算法设计和实现页层出不穷。量子密码学的无条件安全性将使其成为一种长期的安全解决方案。

同时，确定量子硬件的性能也是一个问题。目前，人们已经在开发 QKD 设备方面做出重大努力，然而低成本、稳定、高效、远距离的 QKD 仍具有挑战性。基于卫星的 QKD 迅速出现，而基于地面方法的 QKD 因为光纤衰减和大气损耗等原因，距离有限。为了克服量子密码学中的挑战（如量子攻击、量子通信中的缺陷、成本、距离、密钥率等），并实现量子互联网的目标，量子密码学领域的研究将在未来几年快速发展。

参考文献：

[1] Kumar, A., Garhwal, S. State-of-the-Art Survey of Quantum Cryptography. Arch Computat Methods Eng 28, 3831–3868 (2021).

[2] David J. Griffiths, and Darrell F. Schroeter, Introduction to Quantum Mechanics (3rd Edition), Cambridge University Press (2018).

[3] Wang, S., Yin, ZQ., He, DY. et al. Twin-field quantum key distribution over 830-km fibre. Nat. Photon. 16, 154–161 (2022).

[4] Zimmer C． Perfect gibberish [J] ． Discover． September l992，(1)：92～99.

[5] Mark Fox, Quntum Optics - An Introduction, Oxford University Press (2006).

[6] Broadbent A (2018) How to verify a quantum computation. Theory Comput 14(11):1–37

[7] Gheorghiu A, Kashefi E, Wallden P (2015) Robustness and device independence of verifiable blind quantum computing. New J Phys 17(8):083040

[8] Klarreich E (2018) Graduate student solves quantum verification problem. QuantaMagazine