经典密码通信与量子密码通信的现状及发展趋势

刘 飞
石家庄市公安局栾城分局，河北 石家庄 051430

[摘要]信息安全一直是通信领域中的一个重要挑战，而密码通信是确保信息安全的关键。传统的经典密码通信方法在过去几十年中取得了巨大的进展，但也面临着越来越严重的安全挑战，尤其是在量子计算机的崭露头角下。为了应对这些挑战，量子密码通信作为一门新兴的领域正在快速发展，利用量子力学的原理来提供前所未有的安全性。本篇文章讨论了经典密码通信与量子密码通信的现状，以及分析未来的发展趋势，量子密码通信作为信息安全的未来方向，将提供更高级别的保障，以确保隐私和数据的安全传输。

[关键词]量子密码术；量子密码分配；量子通信
DOI：10.33142/sca.v6i8.9818 中图分类号：TP91 文献标识码：A

Status and Development Trends of Classical Cryptographic Communication and Quantum Cryptographic Communication

LIU Fei
Luancheng Branch of Shijiazhuang Public Security Bureau, Shijiazhuang, Hebei, 051430, China

Abstract: Information security has always been an important challenge in the field of communication, and password communication is the key to ensuring information security. Traditional classical cryptographic communication methods have made significant progress in the past few decades, but they also face increasingly serious security challenges, especially with the emergence of quantum computers. In order to address these challenges, quantum cryptography communication, as an emerging field, is rapidly developing, utilizing the principles of quantum mechanics to provide unprecedented security. This article discusses the current status of classical cryptographic communication and quantum cryptographic communication, as well as analyzes future development trends. As the future direction of information security, quantum cryptographic communication will provide higher levels of protection to ensure privacy and secure data transmission.

Keywords: quantum cryptography; quantum cryptographic allocation; quantum communication

引言

随着数字化时代的来临，信息的传输和存储变得前所未有的便捷，然而，这也引发了安全性的严重担忧。在这个信息爆炸的时代，保护敏感数据和通信的机密性变得至关重要。传统的经典密码学虽然取得了显著的成就，但随着计算能力的不断增强，经典密码学面临着日益复杂的攻击，如大规模计算和量子计算机的崭露头角。因此，信息安全领域需要更强大的工具和技术，以应对这些威胁。在这个背景下，量子密码通信作为一门融合了量子力学与密码通信的前沿领域正在崭露头角，利用量子力学的原理，如不确定性原理和 EPR 纠缠，提供了前所未有的信息安全性。本文将深入探讨经典密码通信和量子密码通信的现状，以及它们的发展趋势。

1 经典保密通信的现状

1.1 对称密钥通信体系

在对称密钥通信体系中，加密和解密过程都使用相同的密钥，通常表示为“k”。这种体系的特点是在通信双方之间需要事先共享相同的密钥，该密钥用于加密和解密通信中的信息。这里的“k”和“k’”（如果存在）通常是相同的或可以相互推导的，因为加密和解密过程需要使用相同的密钥。为了保证通信的安全性，密钥必须被严格保密，并且在通信双方开始进行通信之前，必须确保双方都拥有相同的密钥，通常需要采取一种安全的密钥分发方法，其中包括以下步骤：第一，在通信双方之间生成一个随机的对称密钥“k”，这个过程需要使用强随机性生成器来确保密钥的随机性和不可预测性。第二，生成的密钥“k”需要安全地传输给通信双方，通常是一项关键任务，因为如果密钥在传输过程中被窃取或泄露，通信将不再安全[1]。第三，通信双方可以在物理上会晤，然后交换密钥，这种方式是最安全的，但也不太便捷，特别是在远距离通信中。第四，双方可以通过安全的信使来交换密钥，确保密钥的安全传递，这也是一种安全的方法，但可能不够高效。在实际应用中，传统的对称密钥通信在一些场景下可能会存在一些挑战。特别是在大规模、分布式或需要频繁更换密钥的通信中，密钥管理和分发可能变得复杂和容易出错。

1.2 非对称密钥通信体系

非对称密钥通信体系，广泛应用于网络和金融行业，是一种重要的加密通信方式。在这个体系中，存在一对密钥，一个是公开的，称为公钥，另一个是保密的，称为私钥。公钥用于加密消息，私钥用于解密消息。非对称密钥

体系的安全性建立在数学上难以计算的数学问题之上，通常是基于大数因式分解等问题。例如，RSA（一种非对称加密算法）的安全性基于将一个大整数分解成两个素数之积的问题，这是一个在经典计算机上非常耗时的任务[2]。经典计算机几乎无法在合理的时间内破解基于大数因式分解等问题的非对称密钥体系。然而，Shor's 算法（一种量子算法）已经证明，使用量子计算机可以有效地破解这些问题，从而威胁传统的非对称密钥通信安全性。为了应对量子计算的威胁，研究人员正在开发后量子密码学方法，这些方法使用抗量子攻击的加密算法，以确保通信的安全性。除了使用非对称密钥加密，现代安全通信也倾向于采用多因素认证，以增强安全性，要求用户提供多个身份验证因素，而不仅仅依赖于密钥。

1.3 Vernam 密钥体系

Vernam 密钥体系，也被称为一次性便签密码本（One-Time Pad），是一种在保密通信领域具有绝对安全性的加密方法。该方法最早由美国人 Vernam 于 1926 年提出，直到 1949 年，信息理论的奠基人克劳德·香农（Claude Shannon）证明了其绝对安全性。Vernam 密钥体系要求密钥 K 和明文 M 具有相同的长度，这是该方法的关键特点之一。密钥的使用必须是随机的，一次性的，这意味着每个密钥只能用于一次加密操作，不可重复使用。同时，Vernam 密钥体系被证明具有绝对的安全性，也就是说，即使攻击者拥有所有可能的密钥和密文，也无法破解出明文，这是因为每个密钥都可以产生任意的密文，不会泄漏关于明文的任何信息。Vernam 密钥体系的主要挑战之一是密钥的管理，通信双方必须事先共享庞大的密钥群，并能够迅速方便地分配和管理密钥，这在实际通信中通常是非常困难的，因为密钥的分配和管理需要高度的安全性和保密性[3]。由于密钥管理的困难，Vernam 密钥体系从提出到现在一直未能广泛应用于实际通信中，只有在一些特殊情况下，例如军事通信或高度敏感的政府通信中，才可能会考虑使用这种绝对安全的加密方法。总之，Vernam 密钥体系是一种具有绝对安全性的加密方法，但由于密钥管理的挑战，它并没有在广泛的通信领域得到应用。在实际应用中，其他更实用的加密方法，如对称密钥加密和非对称密钥加密，通常更为常见，因为它们能够更好地解决密钥管理和分配的问题。

2 量子密码通信的现状

量子密码通信其理论最早由美国哥伦比亚大学的 S.J. Wiesner 提出。Wiesner 在约 1970 年左右撰写了一篇论文，题为“Conjugate Coding”，其中提出了使用量子物理学原理来传送消息的方案。然而，这个想法当时被认为过于离奇而被拒绝刊登，直到 1983 年才在会议上被发表。第一，量子密码通信的核心特点是其绝对安全性，基于量子力学原理，其中的不确定性和观测干扰性质确保了通信的绝对保密性，即使攻击者使用最先进的技术和设备，也无法破解量子密钥。第二，量子密码通信是用来建立和传输安全的密码（密钥），通信双方使用量子态编码密钥，然后通过量子信道将其传输给接收者，可以用于对后续的通信进行加密和解密[4]。第三，量子密码通信抵御了各种窃听攻击。如果窃听者试图截取传输中的量子态来窃取密钥，根据量子力学的原理，这个过程会被探测到，并且密钥会被重新生成，通信双方会察觉到潜在的攻击。第四，量子密码通信引起了广泛的兴趣，尤其在高度敏感的通信领域，如军事通信和金融交易。虽然目前量子密码通信的实际应用还相对有限，但它已经成为信息安全领域的重要研究方向。总之，量子密码通信是一种具有绝对安全性的通信方式，其基础是量子力学原理，使得窃听者无法窃取通信的密钥或信息。尽管在实际应用中仍面临技术挑战，但它代表了未来信息安全的一个潜在方向，特别是在面对量子计算等新兴威胁时。

2.1 基于 2 个非正交的两态量子密钥分配方案

B92 协议是一种基于两个非正交的两态量子系统的密钥分发方案，因此它不需要使用四个正交的量子态，与传统的 BB84 协议相比，更加简单，但效率略低。B92 协议基于量子力学的性质，利用光子的偏振态来传输信息，它的核心思想是使用两组非正交的量子态作为编码基础，然后通信双方随机选择其中一个基组进行测量[5]。通信双方通常表示为 A 和 B，分别代表发送方和接收方。密钥建立的详细过程如下：第一，A 选择一个随机的偏振态，可以是 0 度（表示“0”）或 45 度（表示“1”），然后发送相应的光子脉冲给 B。第二，在接收到光子后，随机选择一个测量基准（垂直于 A 的选择方向），可以是 90° 或 135°。如果 B 的测量基准与 A 的偏振态垂直，那么 B 的探测器将无法接收光子。只有当 B 选择的测量基准与 A 的偏振态相匹配时，B 才有 50%的概率接收到光子。这一步骤模糊了 B 对光子偏振态的测量结果。第三，B 将测量结果告知 A，但不公开测量基准的选择，然后 A 和 B 都丢弃那些没有测量到的数据，因为这些数据对于密钥建立无用。第四，接下来，B 将接收到的光子转化为量子位（“0”或“1”），并将其编码为密钥的粗码。第五，B 随机公布一部分位，以供 A 验证通信的完整性和 B 的身份。第六，经过 A 的确认，双方确定没有窃听或干扰后，剩下的位可作为密钥。B92 协议的安全性基于量子力学的性质，即任何企图通过观测传输中的量子位来窃取密钥而不留下窃听的痕迹是绝对不可能的，因为量子力学的不确定性原理确保了 B 的测量结果不会完全与 A 的偏振态匹配。B92 方案的效率仅为 BB84 方案的一半，因为只有当 B 选择的测量基准与 A 的偏振态匹配时，B 才有 50%的概率接收到光子[6]。

2.2 基于 EPR 态的纠缠量子密钥分配方案

基于 EPR 态的纠缠量子密钥分配方案，也称为 EPR

协议或 E91 协议，是由 Andrzej Ekert 于 1991 年提出的一种量子密码通信方案。该方案的核心原理是利用量子力学的非局域性和 EPR 纠缠性质，以 EPR 粒子对作为量子信道来传送密钥。EPR 态是一种特殊的纠缠量子态，最著名的是 Einstein、Podolsky 和 Rosen（EPR）在 1935 年提出的 EPR 纠缠态。这种态具有非常特殊的性质，其中两个粒子之间存在确定的、不变的关联。例如，如果测量其中一个粒子的极化态为向上，那么另一个粒子的极化态一定是朝下，即使它们之间的距离很远。E91 协议的密钥分配过程如下：第一，发送方 A 创建一对 EPR 纠缠光子对，并将其中一个光子发送给接收方 B，对光子对的制备通常涉及到使用一个特殊的量子源来生成 EPR 纠缠态。第二，A 和 B 各自在他们的光子上执行一系列测量，包括极化态的测量，测量的选择是随机的，且在 A 和 B 之间约定好。第三，A 和 B 将他们的测量结果通过一个公共通道进行通信，但不公开测量的具体方式，这个步骤模糊了潜在窃听者对密钥的了解。第四，接下来，A 和 B 比较他们的测量结果，并筛选出一部分数据用于密钥建立，这一步骤通常包括错误检验，以确保通信的完整性和 B 的身份。第五，经过筛选和验证后，A 和 B 共同拥有一套相同的随机序列，这可以用作密钥。E91 协议的安全性基于 EPR 纠缠态的性质，窃听者任何企图窃听通信内容都会破坏 EPR 纠缠态的关联性，这将被 A 和 B 察觉到。因此，E91 协议提供了高度的安全性。基于 EPR 纠缠态的密钥分配可用于远程通信，因为 EPR 纠缠态可以在较长的距离上维持其关联性。此外，一些纠缠技术，如量子隐形传态、纠缠交换、纠缠纯化、量子中继器等，已经应用到了 E91 协议中，增强了量子远程通信的可行性和效率。

3 量子密码通信的发展前景

自从 Bennett 提出第一个量子密钥分发协议以来，量子密码通信领域已经取得了显著的进展，不仅在理论研究上有长足的发展，而且在实验研究方面也取得了令人瞩目的成果。以下是量子密码通信的发展前景：①光纤中的量子密钥分发（QKD）。光纤中的 QKD 是量子密码通信的主要实验方向之一，已逐渐走向成熟。目前，国际上的研究团队已经在光纤中实现了长距离的 QKD，最新的记录达到了 150km。中国科学院物理研究所与中国科学院研究生院合作创造的 160km 光纤中 QKD 传输距离是一个重要突破。②自由空间的 QKD。自由空间的 QKD 也取得了重要突破，目前已经实现了传输距离达到 23.4km，自由空间的 QKD 技术在一些特定应用场景中具有潜在的价值，如卫星通信等。③量子密钥传输距离的增加。未来的发展方向之一是如何进一步增加量子密钥传输的距离，以实现更广泛的安全通信覆盖范围，涉及到改进量子信道的性能和抗噪声技术的研究。④量子密钥共享。量子密钥共享是一个重要的研究方向，允许多方之间共享量子密钥，以实现更复杂的多方通信安全性。⑤网络量子密码。发展网络量子密码体系结构是量子密码通信的未来方向之一，将涉及到构建更复杂的量子通信网络，以满足不同应用的需求。⑥身份认证、数字签名和量子指纹。量子密码通信领域还将继续研究安全性相关的问题，包括身份认证、数字签名和量子指纹等，以提供更全面的安全解决方案。总的来说，尽管量子密码通信领域仍然面临许多挑战，如传输距离的增加、抗噪声技术、多方通信安全性等问题，但它仍具有巨大的发展潜力。随着技术的不断进步和理论的深入研究，量子密码通信将在信息安全领域发挥越来越重要的作用，为信息保护和安全通信提供更高级别的保障，其发展和应用前景将更加灿烂辉煌。

4 结论

总之，经典密码通信和量子密码通信代表了信息安全领域的两个不同方向，各自具有独特的特点和应用前景。经典密码通信在长期的发展中积累了丰富的理论和实践经验，广泛应用于各个领域。然而，随着计算能力的增强和新型攻击技术的涌现，传统的经典密码学正面临着越来越大的挑战，需要不断创新和升级以保持安全性。与此同时，量子密码通信作为一门新兴的领域，利用量子力学的原理为信息安全提供了更高级别的保障，尤其是在量子计算机的崭露和发展下，量子密码通信显得尤为重要。

[参考文献]

[1]王栋,李国春,俞学豪,等.基于量子保密通信的国产密码服务云平台建设思路[J].电信科学,2018,34(7):171-178.
[2]陈杰建.基于 SDN 的量子密码通信网络设计[J].信息记录材料,2022,23(9):165-167.
[3]张英.对量子密码通信的展望[J].中国新通信,2020,22(22):7-8.
[4]孙刚.关于网络安全技术中的量子密码通信分析[J].数字通信世界,2020(9):97-98.
[5]高鹏,周华旭,于国际等.量子通信技术与当前应用分析[J].电子设计工程,2020,28(16):115-118.
[6]赵鑫,李恺.基于 SDN 的量子密码通信网络设计与研究[J].通信技术,2020,53(4):898-902.

作者简介：刘飞（1980.8—），男，本科毕业于河北科技师范学院计算机科学与技术教育专业，后进修法学硕士学位，现就职于河北省石家庄市公安局栾城分局情报中心主任，二级警务技术主管。