量子密钥分发技术在商用密码领域的应用探析

陈济京

（数字广西集团有限公司，广西 南宁 530001）

摘 要 我国科技水平不断提升，互联网系统完善程度不断提高，使互联网信息技术在我国各行各业得到广泛应用，同时也使网络安全问题受到了社会的广泛热议。在商用领域，基于互联网技术的量子密钥分发技术逐渐成熟，其作为一种新兴密钥通信技术，实现了对网络数据安全的有效保障，可以构建起完善程度更高的网络安全防范体系，可以满足保障通信效率的要求，也符合当前我国数据安全管理需求。基于此，本文对量子密钥分发技术特征进行了分析，并对其在商用密码领域的应用路径进行了深入探究，希望可以为今后现代化商用密码体系的完善提供经验参考。

关键词 量子密钥分发技术；商用密码；金融机构；安全评测；身份验证

中图分类号：TN919 **文献标志码**：A **文章编号**：2097-3365(2024)07-0004-03

大数据技术、互联网技术、量子计算等一系列新兴技术在我国商业发展中的应用范围不断扩展，国家法规及行业监管也对网络信息数据安全提出了新要求。对于商用密码而言，可以有效构建信息数据安全的保护体系。因此，要灵活运用商用密码，使其促进现代企业稳定发展，进而最大程度地降低核心商业数据泄露、丢失等问题出现的可能性。在我国颁发的《商用密码管理条例》中，对当前的量子密钥分发技术创新、应用要点等进行了要求。今后，应该以上述条例相关规定为基础，充分发挥出量子密钥分发技术在商用密码领域的应用优势，实现对现有商用密码体系的有效补充，这也可以起到促进我国社会经济稳定发展的作用。可以看出，我国在商用密码体系方面的研究虽然已经取得阶段性成果，但整体来看，依然有较大的进步空间，尤其在成本管控、技术应用前景扩展等方面还需要进一步深耕，应该加大量子密钥分发技术在安全评测、身份验证、防范体系构建等方面的应用力度，这样才能使量子密钥分发技术的应用成效更佳。

1 量子密钥分发技术特征分析

1.1 不可破译性

想要实现对量子密钥分发技术的深度开发与应用，应该对此项技术的特征有具体了解，不可破译性是其最为明显的特征之一。具体而言，由于量子密钥分发过程中，可以实现对字符串长短的随意设定，同时也可以在数据串传输过程中生成新的密钥，进而保证数据传输效率及精准性。因此，对量子密钥分发方式进行妥善利用之后，其形成的字符串体现出了不可破译的特性。

1.2 真随机性

真随机性主要是指量子所具备的不可克隆性特征，由于量子密钥的生产过程可以看作是数据传输过程，因此，需要构建起以通信双方为桥梁的基本结构，这样才能使所产生的一系列数据具有随机性，并且产生的每一串字符往往都具有一次性的特点，因此体现出了真随机性[1]。

1.3 可追溯性

量子密钥分发技术与一般的密钥技术存在一定差异，主要体现为密钥在生成过程中会对形成的字符串进行直接记录，因此，在通信过程中，数据结构之间的可追溯性可得到保证。并且，字符串传输过程中出现通信安全问题的可能性得到了有效控制，更加方便相关检查记录工作人员对特定字符串进行查找，这也使量子密钥技术的应用体现出了数据可追溯性，符合当前互联网时代背景下安全防护需求。

2 量子密钥分发技术在商用密码领域的应用基础

2.1 相关法律法规较为健全

从目前商业金融领域发展情况来看，对量子密码技术的应用重视程度不断提高，对此项技术的研发也越来越深入，其主要目的是更好地适应我国社会现代化发展。之所以量子密钥分发技术在商用密码领域的研发与应用体现出了适用性，与当前良好的法规环境有直接关系，目前来看，我国已经先后出台了《中华

人民共和国网络安全法》《中华人民共和国个人信息保护法》等一系列法律法规，也正是因为相关法规的不断完善，使得商用密码领域的技术研究及实践应用有了更为具体的依据，同时也使得金融领域的相关制度规范程度明显提高，尤其在完善金融行业信息化结构的同时，使得商业金融数据的利用得到保障[2]。

此外，随着我国国家互联网应急中心的建立，使得当前网络金融安全程度明显提高，商用密码的现代化程度不断提高，尤其利用了量子密钥分发技术的商用密码体系，其安全程度更高，并且体现出了真随机性、可追溯性、不可破译性等一系列特征，使得当前的商用网络密码安全性明显提高，为现代企业及金融机构发展确定了新路径。

2.2 机构间可实现数据共享

在以往的商用网络安全领域，企业与企业之间、机构与机构之间的合作往往较为有限，主要由于数据资源的共享程度较低，这也导致资源浪费的情况时常出现，不符合现代化社会经济发展理念。而在当前互联网信息技术全面普及的时代背景下，企业之间、机构之间的合作密切程度更高，主要由于数据共享及利用的及时性得到了保证，符合我国现代商业发展需求。并且，双方的积极合作还可以在实现数据共享的基础上实现资源共享，进而使行业运转规范程度更为可控，也有利于保障机构自身服务质量，使其在当前激烈的行业竞争中获得一席之地[3]。此外，量子密钥分发技术之所以在机构间数据共享中得到广泛应用，还与其具备远距离传输及成本可控等优势有直接关系，当前，量子密钥分发技术主要运用了国密与商密对称的加密算法，因此所形成的传输信道安全性、稳定性更强，在商用领域受到了广泛欢迎。并且，量子密钥分发技术的相关设备体系、质量较小，体现出了小型化、集成化的特点，以2022年我国发射的授课量子微纳卫星为例，其重量仅为98 kg，这也使其安装部署时间更短，并且调试作业更为便捷。

3 量子密钥分发技术在商用密码领域的应用分析

3.1 在金融机构中的应用

当前对量子密钥分发技术的研发越来越深入，尤其在将其应用到金融机构的经营发展中时，体现出了自身独特的优势。当前，金融机构在进行量子安全网络系统构建时需要利用质量密钥分发技术，并且所构建起的量子安全网络系统往往在功能属性方面体现出了自身的独特性，实现了具有共享属性的安全密钥创建。具体而言，将量子密钥分发技术应用到金融机构的量子安全网络构建中主要是利用了此项技术的量子物理原理，进而使得密钥的安全属性得到保障，符合当前金融机构现代化发展需求。构建起量子网络安全系统之后，金融机构在今后的经营发展过程中对于核心数据信息的储存与安防能力会明显提升，尤其在进行敏感的、重要的数据传输时，可以实现对受黑客攻击可能性的有效控制，进而明显降低数据信息出现泄漏现象的可能性。

此外，构建起的量子安全网络系统还为金融机构提供了安全通信通道，对于这一通道而言，可以运用量子密码加密算法来对通信数据进行计算与核准，进而实现由一个数据端到另一个数据端的全过程加密，同时也使数据传输的完整性得到了保证[4]。随着金融机构的现代化运行发展模式逐渐完善，所构建起的量子安全网络还具备抵抗量子计算机攻击的能力，可以有效抵御数据信息系统运行过程中所遇到的多种共计形式，进而保证金融机构自身效益与数据安全。

3.2 在安全评测中的应用

从目前量子密钥分发技术的研发情况来看，由于其技术体系完善程度不断提高，当前已经形成了相应的量子密钥分发标准，通过这一标准体系的构建，使得量子密钥分发技术在安全评测中的应用成效得到了保证。当前我国已经构建起相应的商用密码检测中心等机构，其主要负责对商用密码的安全情况进行评价，并以所得到的评价结果为基础，确定相应的安全测评技术，这样可以实现对特定产业发展的有效促进[5]。可以看出，与安全测评能力形成有关的量子密钥分发标准体系完善程度不断提高，并且形成了相应的理论模型、设备模型等，使得测评工作在开展过程中有了更为系统的理论支持，为今后安全测评工作开展提供了现实助力。并且，由于基于量子密钥分布技术的安全评测体系完善程度不断提高，评测能力越来越强，使得评测工作的开展逐渐体现出自动化、多元化特征，为今后现代企业及机构的稳定发展奠定了基础[6]。

3.3 在身份验证中的应用

在当前的网络信息系统中，如何实现科学的、有针对性的身份验证是行业内部人员关注的要点，可以通过身份验证的方式来使得企业之间、机构之间的交易流程更为清晰具体，同时也使得各环节之间的呼应程度更高，尤其有利于敏感数据信息的传输与保护。对于传统的商用网络身份验证方式而言，其往往验证

环节较为繁琐，并且是以证书的验证形式为主，这也导致其被非法攻击者破解的可能性较大，进而给数据信息持有者造成一定损失，可以看出，传统的商用网络系统身份验证方式安全程度并不高。而利用量子密钥分发技术之后，使得身份验证方式得到优化，可以使通信双方产生一组相同的密钥，也正是因为这组密钥相同，使得二者构建起了通信互动关系，同时也可以实现数据信息共享，使得身份验证的即时性、高效性得以体现[7]。当通信双方形成了共同的密钥组之后，还可以使加密与解密的过程只有双方知晓，这也使身份验证成为二者重要的沟通桥梁之一。此外，还可以借助量子安全云计算的方式来实现身份验证，对于量子安全云计算技术而言，可以将其看作是一种用于保护云环境中敏感核心数据的方式，其主要是利用密钥加密技术的方式来保证数据不会出现泄露或丢失现象，这也更加有利于网络信息系统层面的商业管理工作开展[8]。

3.4 在防范体系中的应用

量子密钥分发技术在防范体系中的应用主要是指在完善攻击防范体系中的利用，由于计算机网络信息系统在运行过程中有受到外界病毒攻击的可能性，因此要做好相应的防范措施。但对于以往的商用领域计算机网络系统而言，由于其功能存在局限性，因此难以实现对黑客、病毒的追击，一旦因为数据丢失产生损失，往往很难及时对其进行补救，这也加大了系统运转失常的可能性。而借助量子密钥分发技术构建起相应的商用网络安全防范体系，可实现对以往信息加密策略的有效优化，形成针对性更强的病毒防范体系，进而保证数据传输的稳定性、安全性[9]。

就当前情况来看，基于量子密钥分发技术的商用网络病毒防范体系加密方式主要包括节点加密、链路加密等，其信息加密效果更佳，主要由于在加密系统背后有大量的算法对其进行支撑，实现了对以往加密体系的有效优化。并且，还可以通过常规密码、公钥密码的方式来对当前所应用的加密算法进行区分，这也实现了对以往加密形式的有效优化，符合当前企业或机构商用需求[10]。

4 结束语

由于我国互联网信息技术的普及程度不断提高，其在商业领域的应用越来越广泛，这也使得商业数据安全问题受到了人们的关注，如果不能保障核心商业数据的安全性，势必会对相关企业或机构利益产生影响。整体来看，当前我国的商用安全密钥方式依然存在一些不足之处，主要体现为传统的密钥方式依然较为常见，由于传统的非量子加密算法在应用过程中往往体现出属性单一的弊端，导致其容易受到外界因素、人为因素的干扰，进而无法保障目标数据安全性，不能满足现代化企业经营发展需求。而对于量子密钥分发技术而言，其特征明显，主要体现为具备真随机性、可追溯性及不可破译性，也正是因为具备上述优势，将此种密钥技术应用到商用密码领域，可使数据信息的机密性及完整性得到保障，更加有利于数据发挥其应有价值。对于当前的商业数据信息而言，其在信息传输过程中往往会涉及较多的敏感信息，可以利用量子纠缠的特征来保证信息不会被窃取，同时也实现了对安全通信渠道的有效构建。可以看出，量子密钥分发技术的应用为当前的商用密码领域技术体系构建与完善提供了新的可能性，同时也实现了对商用网络系统运行安全性的有效保障。今后应该结合当前商用金融属性敏感信息保护需求，构建起抵御外界病毒及黑客能力更强的防范系统，这样才能使密钥分发技术的应用真正促进我国商业金融领域的稳定发展。

参考文献：

[1] 张一辰，边一铭，王恒，等．面向城域接入的连续变量量子密钥分发技术[J]．信息通信技术与政策，2023,49(07):53-59.
[2] 赵于康，李霞，周雷，等．量子密钥分发技术在商用密码领域的应用路线分析[J]．中国信息安全，2023,20(07):56-58.
[3] 《量子“Q波”技术白皮书》发布，量子无线密钥分发技术得到初步验证[J]．信息网络安全，2022,22(08):91.
[4] 中国科学技术大学潘建伟团队首次实现设备无关量子密钥分发[J]．信息网络安全，2022,22(08):93.
[5] 杜珊娜．纠缠态连续变量量子密钥分发的量子—经典信道复用技术及源无关安全性研究[D]．太原：山西大学，2021.
[6] 左颖敏．量子密钥分发网络中基于机器学习的资源分配技术研究[D]．北京：北京邮电大学，2021.
[7] 邹兴裕．基于部分可信中继的量子密钥分发网络路由与资源分配技术研究[D]．北京：北京邮电大学，2021.
[8] 杨申申．基于FPGA的高速连续变量量子密钥分发后处理技术的研究[D]．太原：山西大学，2020.
[9] 王天一．基于连续变量的量子密钥分发系统中长距离传输技术与安全性研究[D]．北京：北京邮电大学，2017.
[10] 刘友明，汪超，黄端，等．高速连续变量量子密钥分发系统同步技术研究[J]．光学学报，2018,35(01):96-105.