基于量子密钥分发技术的金融网络安全实践研究

张　斌
复旦大学　上海　200433

摘　要：金融数字化转型中，传统加密面临网络攻击与量子破解双重威胁。本研究聚焦QKD技术在金融网络安全的应用可行性与实践价值：先阐述QKD原理及依托量子力学的真随机、高可靠、无条件安全优势；再剖析金融安全的区域失衡、人才匮乏、基建自主可控不足等问题；后论述QKD的多层次防御、提速远程传输、完善防护机制、建跨机构生态等应用路径。研究表明，QKD可有效应对金融安全难题，为建防护体系、御量子攻击提供支撑，对保障金融数据安全与系统稳定具重要价值。

关键词：金融领域；网络安全；量子密钥

引言

在金融科技迅速发展的背景下，网上银行、移动支付和跨境结算等新兴业务已成为现代金融服务的重要组成部分。与此同时，大量敏感金融数据的产生与传播，使网络安全成为维系金融体系稳定运行的关键。当前，传统加密手段正面临双重压力：网络攻击日趋专业化并呈高频态势，黑客通过漏洞利用或社会工程窃取金融信息。2024年中国金融行业数据泄露事件较2023年增加18%，严重威胁客户财产安全并损害金融机构形象；同时，量子计算的快速发展可能对RSA和ECC等主流加密算法构成实质挑战，预计在未来十年内或将具备破解大部分现有密码的能力。量子密钥分发（QKD）技术依托量子力学原理，结合不可克隆定理和测不准原理，实现密钥生成的真随机性、传输的可监控性和信息传递的无条件安全性，为解决金融网络安全问题提供了理论上可靠的保障。深入研究QKD在金融领域的应用路径与优化策略，不仅有助于提升金融机构抵御高级网络攻击和量子计算威胁的能力，还将推动构建符合国家信息安全合规要求的抗量子安全体系，对提升金融系统整体安全水平具有重要的理论意义和实践价值。

一、量子密钥分发技术原理及特点

1.工作原理

量子密钥分发技术属于依靠量子力学原理创建起来的信息保障系统，在这个架构里，各方利用随时生成的随机又安全的密钥来对信息数据执行加密和解密操作，进而达成在信息传输过程中达到最佳保密效果的目的，而且能够显著减少数据泄漏或者遭到破坏的风险，它的具体运作情况可以参考图1。

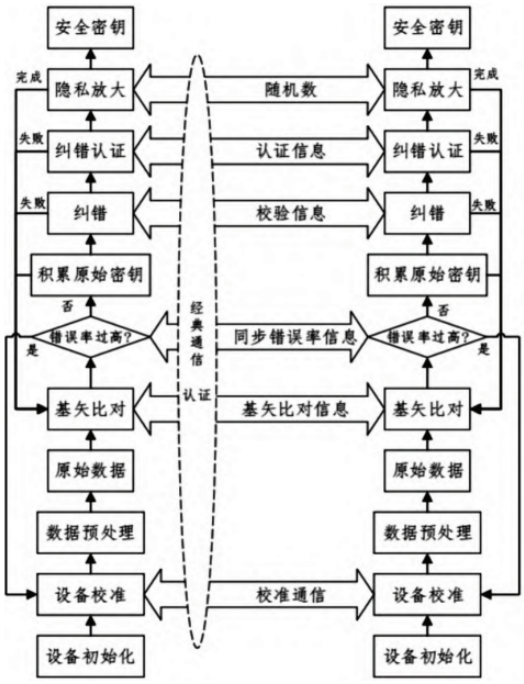

图1　量子密钥分发技术工作原理示意图

2.主要特点

基于对量子密钥分发技术的研究和分析，量子密钥分发技术具有很多突出的特点，主要表现在随机性、安全性高、难以破解等。

（1）真随机性。在通信双方没有建立稳定联系的情况下，量子密钥很难产生，只有经过正式通信之后，才能创建出带有随机性质的量子密钥。这种密钥具有随机性以及不可复制性等特点，对于保障信息安全有着决定

作者简介：张斌（1982年2月－），男，汉，上海静安，硕士，研究方向：信息安全与信息系统管理。

性的保证作用。

（2）高安全性。量子密钥分发（Quantum Key Distribution，QKD）属于一种依靠量子力学原理的新型加密技术，它有着固有的安全属性，在密钥管理方面有着明显的优势，从根本上解决了传统密码学方法所存在的安全隐患，经由比较经典公钥加密算法与QKD技术的安全性特点可以发现，后者在总体防护性能上要优于前者，造成这种现象的根本原因在于，虽然公钥加密利用复杂的数学运算来保障数据传输的保密性，但是仍然存在着被破解的风险，而QKD技术凭借量子态的不可克隆特性创建起了绝对安全的密钥生成与分发机制，在量子计算等先进的攻击手段面前依然能够稳定运行，把QKD技术应用到计算机网络安全防护体系当中有着非常重要的实际意义和应用前景。

（3）不可破译性。量子密钥分发（QKD）最突出的优点就是它固有的信息安全性特性，在每一次传输期间，都会产生长度不同的密钥序列，而且整个分发链路呈现出明显的随机性，按照这样的技术框架，加密后的数据具备很强的抵抗攻击的能力，可以有效地抵挡住像量子计算这样的高级威胁，从而给通信双方的数据隐私保护给予有力的技术保障。

二、金融网络安全领域面临的挑战和问题

1. 金融网络安全发展不平衡不充分

由于金融业对数字化技术的依赖性很强且需要大量存储数据，所以它成了网络攻击的重点目标，如果遭遇安全威胁，就会引发系统性的金融风险，而且给宏观经济稳定和社会秩序带来极大冲击，在这种情形之下，金融网络安全既承受着更为严厉的监管压力，又得到从业机构的高度关注，而且呈现出比其他行业好得多的整体发展水平，近些年，信息技术飞速发展并且深入到金融业转型进程当中，传统的安全防护方法已经跟不上技术变革的步伐，于是造成了行业内部出现明显的分化状况，各个细分领域的网络安全能力存在很大差别，比如商业银行，证券公司以及保险公司等不同类型的金融机构因为各自的业务模式不一样，受到的监管政策也不一样，所以有着各自独特之处的安全防护特性以及风险隐患。同一行业内部各个主体在网络安全防护能力方面存在着明显的差异特征，由于受到组织规模、资源分配和技术储备等因素的不同凡响，它们的安全防护水平呈现出分层的现象，有些机构还存在着重业务轻运维、重外部防御轻内部监管等现象，没有及时适应新技术和新业态所带来的安全威胁，造成整体布局有明显的漏洞且缺乏足够的效能，金融机构应该深刻理解网络安全的战略价值，把其提升到国家安全的关键层面，合理分配资源并准确地填补短板，达成风险防范与业务发展的有机结合，避免局部薄弱成为系统性风险隐患。

2. 金融网络安全人才紧缺

网络攻防竞争本质是技术人才核心能力的较量。随新一代信息技术发展与数字化转型深化，网络安全保障需求爆发式增长，对人才数量、质量要求提升，我国网安人才建设遇困，金融行业尤为突出。虽高校加大培养、企业布局储备，但供求矛盾短期难缓解，高层次人才短缺或长期存在。金融网安领域人才培养需求亟待加强。数字化转型中，新技术广泛应用提更高要求，需金融科技、信息安全与业务实践交叉的复合型人才。当前金融机构普遍缺高级安全专家与实战攻防人员，从业人员跨学科能力欠缺，人才培养滞后于行业与技术发展，亟需系统培训体系提升团队整体能力。

3. 金融关键信息基础设施面临“卡脖子”

国家安全自主可控战略的深入实施，使得ICT企业开始注重核心技术的突破，并且形成协同创新机制，以此来促进信创产业生态的优化发展，在此情况下，各个行业的信息化设备以及产品都在加速实现国产化，信息技术应用创新取得了明显的成果，但是在金融领域还存在着关键基础设施过度依赖进口设备和服务的现象，如果原厂突然停止供应或者缺少技术支持，就会对业务连续性产生重大影响，当下迫切需要提升信息技术自主创新人才的培养力度，完善自主研发体系，加大对于核心平台、组件以及重要信息基础设施的自主运维强度，切实减少对外部供应链的依赖风险，避免核心技术被他人控制。

三、量子密钥分发技术在金融网络安全领域未来应用展望

1. 帮助完善攻击防范体系

在计算机网络遭受黑客攻击的情形之下，传统金融信息系统由于自身的技术架构特点，常常陷入追踪困难、损失难以快速弥补的窘境，这就很容易引发系统运行异常的问题。

当下，计算机网络里病毒的流传速度以及蔓延范围正在出现明显增长态势，每次爆发事件都会造成组织系统陷入完全瘫痪状况，在金融行业遭遇这种威胁之后，其数据安全以及业务连续性会遭受严重破坏，由此造成的经济损失无法估量。

量子密钥分发技术属于信息安全范畴的核心手段，它不但能明显改善病毒防护系统的性能水平，而且对守护网络通信数据安全有着非常重要的意义，传统的加密算法大致包含链路加密，终端加密以及节点加密这三种

形式，它们的运作原理依靠各种加密方法的联合配合，常规密码和公钥密码共同形成了基本结构，常规密码由于具备良好的保密属性而得到广泛采用，表现出不错的可靠性，不过公钥密码虽然比较容易在开放网络环境中部署，但是由于计算过程较为繁杂，所以加密效率相对较低。

2.提供远距离通信安全保障手段

当下金融科技迅猛发展时，金融机构对跨越区域的数据传送需求日益增多，传统通讯安全防护技术由于本身固有的技术限制因素，难以符合当下面临着繁杂业务情形下的安全保障需求，量子密钥流传送技术依靠其独有的物理性质，在远程单独光源协同效应下可有效地防御也许会发生的窃听入侵现象，进而可以给打造高效又安全的数据网络交流系统带来有力的技术保障支撑，在金融核心业务范畴内，这种技术的应用大大改善了金融数据安全水平情况，尤其针对银行、证券这类高度信赖于敏感资讯资料的企业来说，在防止信息泄露事件以及诈骗风险方面尤为突出地表现出明显优点特性。

3.有效提升通信效率

量子密钥分发技术依靠“量子互联网”架构来达成其主要功能，这种架构把远程量子通信链路当作根基，目的在于创建起全球范围内的量子计算网络，进而支撑起跨越大都市区的长距离量子加密数据传送，从而极大地改进金融信息系统之间的信息交流速率，凭借这样的技术途径，既可明显加强数据的安全防护水准，又可改善传输性能，随着量子科技不断发展更新，量子密钥分发系统所达到的传输速率以及涵盖范围都在不断扩大，正在朝着高速度，大容量的量子通信时代迈进，这样一来就能更加符合实际应用环境中的需求。

4.建立金融机构间的量子安全网络

金融机构创建量子安全网络（QSN）的时候，利用量子密钥分发协议可以高效地产生并安全地传送密钥，这种技术依靠量子力学的基本原理来保证密钥交换过程的安全性，进而保证通信数据的保密性和完整性，经由部署QSN，金融机构就能在内部信息交流以及数据传递的过程中明显降低敏感信息外泄的风险，并且能够抵御外部可能存在的危险。

量子安全网络（QSN）属于一种创新性的通讯基础设施，利用量子密钥分发技术达成对信息传输及数据存储的全程加密，保证通讯过程中信息的保密性与完整性，它独有的抵抗量子计算攻击的能力，给金融行业应对将来可能的量子计算安全威胁赋予了稳固的技术支撑，进而改善了抵御潜在安全风险的水平。

量子安全网络（QSN）的部署能显著改善金融机构内部网络安全状况，传统网络通信存在黑客入侵、数据泄露的风险，QSN凭借量子密钥技术给予更高层次的安全保障，量子密钥保证数据传输过程中的信息保密性，还能够防止被窃听和篡改，量子安全网络结合量子加密认证与身份验证机制，从而提升通信主体的身份可信度以及系统运行的可靠性。

总结

本研究关注量子密钥分发（QKD）技术同金融网络安全的紧密结合之处，想突破传统加密方法于金融数字化转型进程中暴露的安全短处和功能局限，文章里先是讲述QKD技术凭借量子力学原理所具有的随机性，可靠性，还有无条件安全特性，并着重突出它在抵御量子计算攻击和防止信息被盗用方面所具有的革命性的意义；接下来对于金融网络安全存在的一些地区涵盖不够全面，缺少专业技术人才和核心设备极度依靠国外的情况，从改良多层次防卫系统，改善远程通信保护机制，提高数据加工效能，形成跨越域的量子安全网络等众多层面着手，深入分析QKD技术应用前景和发展潜力。研究显示，量子密钥分发（QKD）技术可以很好地解决金融领域的数据泄露、信息安全等问题，而且它还能为应对量子计算带来的安全威胁提供技术保障，有利于形成自主可控的金融安全保障体系，今后要着重推进QKD技术同传统金融系统融合，加快复合型人才培育和行业标准制订速度，促使科研成果快速转化为实际生产力，以保证金融系统稳定运行并可靠安全。

参考文献

[1]卢璐.面向数据中心的量子密钥分发策略研究[D].北京邮电大学，2023.

[2]吕嘉琪.多域量子密钥分发网络生存性技术研究[D].北京邮电大学，2023.

[3]董道远，卫宏儒.量子密钥分发技术在希尔加密中的可行性研究[J].网络空间安全，2022（10）.DOI：10.3969/j.issn.1674-9456.2017.10.005.

[4]王思佳，董鹏，耿欣，等.量子密钥分发技术在城市轨道交通通信系统中的应用方案研究[J].铁道通信信号，2024，60（6）：8-14.

[5]何芯逸.量子卫星网络路由与密钥资源分配技术研究[D].北京邮电大学，2023.

[6]网络空间安全.量子密钥分发系统中电光调制器驱动芯片的研究[D].[2025-09-27].

[7]江燕燕，王建秋，嵇英华.基于量子化的网络通信安全性研究[J].电子技术（上海），2008（8）：3.DOI：10.3969/j.issn.1000-0755.2008.08.022.