文章编号：2096-1618(2024)01-0023-05

基于量子技术的跨域数据安全传输研究

林雨生， 昌 燕
(成都信息工程大学网络空间安全学院，四川 成都 610225)

摘要：在大数据时代下，多组织联合办公越来越普遍。数据在跨域传输时的安全共享、数据的分级分类安全管理是目前亟需解决的问题。设计一种基于量子技术的跨域数据安全传输模型，可以保证跨域传输时的数据安全共享及安全管理。将量子网关引入经典跨域传输系统，利用量子网关形成域内用户的身份证书，并完成跨域传输时的身份认证。当进行数据跨域传输时，数据发送方利用量子网关中的量子密钥保护跨域数据，并由量子网关为跨域数据形成数据签名，同时绑定跨域数据的唯一访问权限。当数据访问方的量子网关接收到跨域数据时，首先进行跨域身份的认证及数据完整性查验；然后由域控服务器进行权限的映射，只有权限相匹配的个人或部门才能解密跨域数据，最后数据访问者查看跨域数据，完成多组织的数据共享办公。理论分析表明提出的基于量子技术的跨域数据安全传输模型能够实现跨域数据的保护、用户及数据的分级分类管理、跨域身份认证，并具备更高的密钥安全性。

关 键 词：跨域传输；数据安全共享；量子网关；量子密钥
中图分类号：P751.1 **文献标志码**：A
doi：10.16836/j.cnki.jcuit.2024.01.005

0 引言

在大数据时代下，数据共享是多组织联合办公的需求。为实现多组织的数据共享及数据权限管理，如何构建安全的跨域传输模型是目前亟需解决的问题。目前，经典跨域传输模型的研究主要分为两个方面：数据跨域传输时的安全保护和跨域传输时的安全认证。

在跨域数据的保护研究中，张建辉等[1]提出一种基于数据护照的跨域传输方法，解决了跨域传输时网闸的安全性低等问题，实现跨域数据的安全保护。欧海文等[2]设计了动态授权树，引入关联节点和动态分组节点，解决了数据的实时更新问题，实现数据保护的同时减少数据的交换量。杨晶等[3]分析政务信息跨域传输中的密码支撑技术，并提出建设中国统一的密码支撑体系，为跨域数据安全保护制定加密标准。尹立民[4]为保护跨域数据的安全性，提出基于混沌密钥控制的数据跨域传输方法，在提高数据传输速度的同时增强数据的安全性。肖柳林[5]针对目前的跨域数据的安全需求，分析跨域传输时面临的系统内外部安全威胁，提出数据安全标识绑定及内容过滤等保护技术，实现对跨域数据的安全保护。徐良[6]设计了异构环境下的数据跨域传输控制系统，保证大数据在跨域时的安全性。以上研究能有效解决数据跨域传输时的安全性问题，但随着量子计算的发展，经典跨域传输模型中使用的加密算法不再安全，密钥被泄露的可能性加大，跨域数据传输和共享的安全性面临挑战。

在跨域传输的安全认证研究中，罗义[7]设计了公钥环境中间信息传输的签名方案，实现两个不同密码体制间的跨域签名认证。周波等[8]提出可认证的多层次加密算法，在分散数据计算负载的同时实现身份的认证。徐娟娟[9]引入第三方的认证中心，实现基于代理盲签名的跨域身份认证，减少跨域传输时身份认证的计算负担。潘雪等[10]将区块链技术引入跨域共享模型，设计基于智能合约的跨域访问机制，保证跨域传输时身份认证的安全性。以上研究利用经典公私钥体系或区块链技术保证了跨域传输时身份认证的可靠性与安全性。其可靠性的保证主要来源于经典密码算法的安全性，但随着量子计算的发展，基于公私钥体系的认证将不再安全，从而导致跨域传输的身份认证不再可靠。

随着量子密钥分发网络(QKD 网络)的发展，为经典跨域传输中存在的数据安全和权限问题提供了新的解决思路。量子通信的信息论安全性是由量子力学相关特性保证[11-13]，可以实现量子密钥的安全分发，且量子密钥具备真随机性。因此，可以将量子密钥融入经典公私钥体系和对称加密体系，以量子密钥的真随机性结合一次一密的思想保证对称加密算法或非对称加密算法中密钥的安全性。此外，本文融合密钥管理的思想，以量子密钥作为主密钥，结合不同的加密需求以不同的方式产生各级密钥，并用于数字签名、消息加

收稿日期：2023-03-28
基金项目：四川省科技厅重点研发计划资助项目(2023YFS0419)

密、身份绑定等,保证密钥层面更高的安全性,便于各级密钥的管理。谭政、韩家伟等[14-15]就量子密钥与经典密码体系的融合展开研究,提出量子密钥与经典对称密码、非对称密码的融合技术,加速了量子通信技术在经典密码体系中的应用。

针对目前经典跨域传输模型存在的问题,本文引入量子网关及量子密钥分发网络,提出一种基于量子技术的跨域数据安全传输模型。该模型首先由两方跨域组织的量子设备产生真随机的对称量子密钥池,并由量子网关管理量子密钥池;然后通过量子网关进行量子密钥编号规则及量子密钥选取长度的协商,形成对称的量子密码本;最后由量子网关和域控服务器实现对数据的分级分类管理、跨域数据的安全防护、跨域身份认证等。本文提出的基于量子技术的跨域数据传输模型,可以实现量子身份认证、数据的权限绑定及安全保护,解决了经典跨域传输模型中密钥易泄露且不是真随机的问题,并且能实现一次一密,保证了跨域数据传输时的安全性。此外,由量子网关实现身份认证的功能,解决公私钥体系认证时密钥存在的安全性问题,保证了跨域传输时的身份合法性。

1 基于量子技术的跨域传输模型

本文提出的基于量子技术的跨域传输模型主要包括:(1)量子密钥分发。两方跨域组织的量子设备产生真随机、对称的量子密钥池。(2)量子网关跨域传输及身份认证。量子网关将量子密钥融入经典加密及认证体系中,实现跨域数据的安全保护及身份认证,并且提供对量子密钥的管理服务。(3)域控服务器的数据及用户权限识别及管理。域控服务器首先进行数据权限及用户权限的划分,然后结合量子网关对数据进行分级分类管理,保证跨域数据传输时用户权限与数据权限的匹配。整体模型结构如图 1 所示。

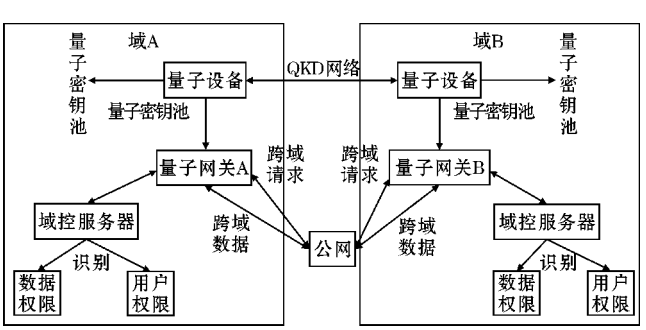

图 1 基于量子技术的跨域传输模型

1.1 量子密钥的生成

两方跨域组织为保证跨域数据加密密钥的安全性,首先通过各自的量子设备产生对称的量子密钥池,然后将量子密钥池交由量子网关进行管理。过程中,量子密钥池中的密钥序列是真随机的,且具有信息论安全性。因此,利用量子密钥分发技术可以保证密钥产生的安全,过程如图 2 所示。

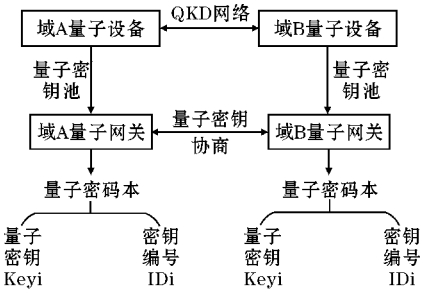

图 2 量子密钥生成

1.2 跨域传输及身份验证

经典跨域传输模型中,数据的加密及身份的验证需由域控服务器完成,加大了服务器的运行负载。此外,经典跨域模型中使用的加密密钥及验证方案存在一定的安全性问题。因此,本文将量子网关引入跨域传输模型中,借助量子网关实现跨域数据的加密保护及跨域身份验证等功能。在进行基于量子技术的跨域数据传输前,域 A 和域 B 已经通过量子密钥分发设备产生对称的量子密钥池,然后域 A 和域 B 的量子网关进行量子密钥协商形成对称的量子密码本,并交换双方量子网关的公钥信息。当进行双方身份认证时,发起跨域数据请求的域 A 成员提供成员信息、域信息、公钥信息给域控服务器;然后由域控服务器转发请求信息(成员信息、域信息、成员公钥信息)到域 A 量子网关;再由域 A 量子网关使用量子密钥编号 ID1 对应的量子密钥 Key1 对当前时间戳 T 使用对称加密算法形成签名密钥 Keys,然后对收到的成员信息及域信息进行签名,形成身份认证信息,同时使用 Keys 对成员公钥信息进行签名形成成员的身份证书;最后由域 A 量子网关使用量子密钥编号 ID2 对应的量子密钥 Key2 使用对称加密算法加密随机数 R 产生会话密钥 Keyc,再使用 Keyc 加密身份认证信息,然后将身份认证数据包(加密身份认证信息、量子密钥编号 ID2、随机数 R)利用域 B 量子网关公钥加密后发送到域 B。其中,利用量子密钥的真随机性保证了量子密钥 Key1 进行数字签名的不可伪造性。此外,根据量子密钥编号 ID2 对应的量子密钥 Key2 和随机数 R 产生会话密钥 Keyc,既保证了对称加密密钥的安全性,又可以实现一次一密。域 B 量子网关接收到域 A 成员的加密身份认证数据包后,首先使用自身私钥进行解密,然后

根据量子密钥编号 ID2 查询量子密码本中对应的量子密钥 Key2;再结合随机数 R 还原会话密钥 Keyc 来解密加密身份认证信息,获取签名使用的量子密钥编号 ID1 及时间戳 T;最后还原签名密钥对签名信息进行验签,验证成员身份是否合法,并将验证结果返回到域控服务器中。身份认证数据包形成过程如图 3 所示。

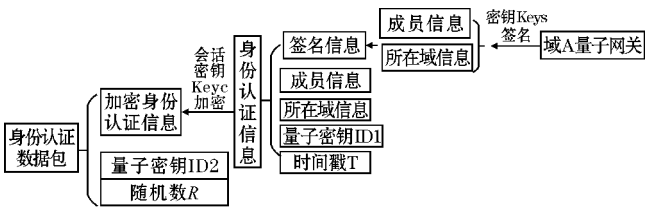

图 3　加密身份认证信息

过程中使用两个量子密钥,其中形成会话密钥的随机数 R 可以每次不同,保证会话密钥的一次一密且降低量子密钥的使用量。此外,用于制作域成员身份认证信息的量子密钥具有一对一及一对多的模式。一对一的模式即一个量子密钥绑定一个用户的信息,一对多的形式则将量子密钥作为主密钥,依次加密不同的随机数产生各个用户的身份绑定密钥,用于两个域成员的身份认证及域成员身份证书制作。

当完成两个域成员的身份认证后,数据持有域 B 即可对跨域数据进行加密传输。首先,域 B 中的域控服务器将跨域数据、数据权限、数据提供者身份信息、数据请求者信息组成的跨域数据信息提交到域 B 的量子网关中,由域 B 量子网关使用数据请求者公钥对跨域数据进行加密,形成加密数据信息;再使用跨域数据发送者自身私钥对加密数据信息进行签名,得到签名信息;然后,域 B 量子网关使用会话密钥 Keyc(会话密钥的产生方法与身份认证时一致)对跨域信息(加密数据信息、数据提供者身份信息、数据权限、接收者、签名信息)进行加密;最后,由域 B 量子网关使用域 A 量子网关公钥加密跨域数据包(加密后的跨域信息、跨域数据发送者公钥证书、随机数 R 及量子密钥编号)后发送到域 A 中。域 A 量子网关接收到跨域信息后,首先使用自身私钥解密跨域数据表,然后对发送方进行身份认证;随后,域 A 量子网关根据量子密钥编号及随机数 R 还原会话密钥 Keyc,再解密跨域信息;域 A 量子网关再使用发送方公钥对跨域信息进行验签,若正确,则将跨域信息中的加密数据信息、数据权限、数据接收者发送到域控服务器;最后,由域控服务器先识别数据权限与数据接收者权限是否匹配,若匹配再将加密数据信息发送到发起数据请求的成员。域成员接收到加密数据信息后,首先使用自身私钥解密数据包获取最终的跨域数据,其过程如图 4 所示。

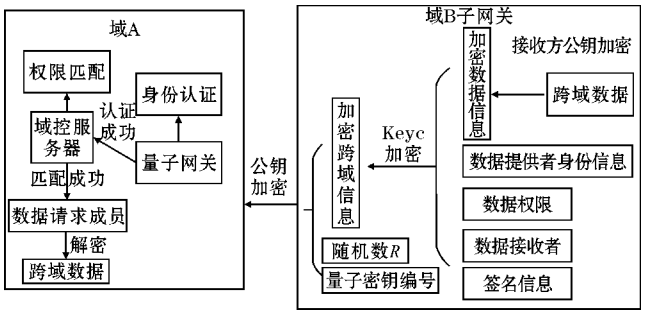

图 4　跨域数据传输

1.3　用户及数据权限管理

为保证跨域数据的分级分类管理,域控服务器需对所在域的用户及数据的权限进行集中管理。根据数据保密级别的不同,域控服务器需定义数据的权限级别,限制数据跨域后的可访问范围。此外,根据域中成员所在的部门、岗位不同,域控服务器需分类分级赋予域成员的数据访问权限。当进行跨域传输时,域控服务器接收到跨域数据后,匹配跨域数据的权限和数据请求者权限是否一致,若一致,则发送到对应的域用户中。反之,则报送用户请求错误,不能查看权限级别以上的数据,最终导致此次跨域数据请求失败,其过程如图 5 所示。

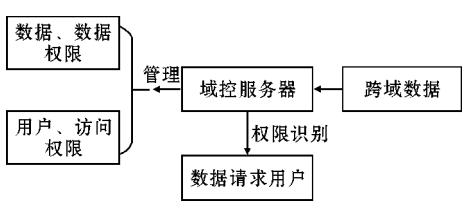

图 5　数据及用户管理

2　模型分析

基于量子技术的跨域传输模型优势可从安全性和效率两个方面对模型进行简要理论分析。

2.1　安全性分析

2.1.1　密钥安全性

跨域传输的安全性保证来源于密钥的安全性。基于量子技术的跨域数据传输模型中,引入量子密钥分发技术及量子网关,能够基于量子力学原理和量子网关特性保证跨域传输中密钥的安全性。

其中,量子密钥分发技术是基于量子力学原理,具有窃听检测、密钥真随机性、信息论安全性等特点。因此,只有拥有量子设备的域才能获取原始的量子密钥池,且量子密钥池一经生成则交由量子网关进行管理,使攻击者无法获取到量子密钥池,从而阻止攻击者获

取密钥。

量子网关是量子通信技术发展的产物,其具有为外部应用提供密码服务、数据包处理、量子密钥管理的功能,量子网关在跨域传输中的核心作用即对数据加密解密传输、密钥管理和跨域用户的身份认证。其中,数据的加密解密传输分为两个部分:(1)两方域中的量子网关进行密钥编号规则及密钥长度的协商,从量子密钥池中形成对称的量子密码本;(2)量子网关从量子密码本中选取量子密钥进行跨域数据的加密解密传输。量子网关的密钥管理主要体现在量子密钥不会出现在量子网关以外的地方,并且量子密钥在量子网关中进行加密存储,量子网关的管理员还可登录管理后台实时查看量子密钥的使用情况。因此,将量子网关引入跨域传输模型中,可以保证跨域数据传输时密钥的安全性,并且可以实时对量子密钥的使用情况进行管理。

2.1.2 *身份认证安全性*

与经典 PKI 体系认证不同,基于量子技术的跨域传输模型中,由量子网关进行认证,为域中的用户使用量子密钥绑定身份认证信息,保证身份认证的唯一性和不可伪造性。相比于经典认证体系,量子网关的认证安全是由量子密钥的安全性保证的,量子密钥只存在于量子网关中,并且在跨域传输时不会出现量子密钥的明文信息,使攻击者无法伪造域用户的身份信息,保证身份认证时更高的安全性。因此,在跨域身份识别中,提出的模型提高了经典认证方式的安全性。

2.2 效率分析

经典跨域传输系统中,用户身份认证、数据加密解密等功能需由域控服务器完成,对服务器的性能要求较高。在基于量子技术的跨域传输模型中,跨域的数据包处理、跨域身份认证、密钥管理可由量子网关完成,域控服务器只需进行域中用户及数据的分级分类管理,降低了服务器的运行负载,更高效地进行跨域传输任务。

3 结束语

本文提出一种基于量子技术的跨域传输模型,借助量子密钥分发技术和量子网关解决经典跨域传输中存在的密钥安全性问题,保证跨域传输时数据及身份认证的安全性,使攻击者无法获取跨域传输时的密钥,且还能降低域控服务器的运行负载,使跨域传输更高效。此外,域管理员可登录量子网关后台对量子密钥的使用情况进行管理,对量子密钥使用过程进行透明监管,及时发现安全问题。经分析表明,本文提出的基于量子技术的跨域传输模型相比于经典跨域传输模型在密钥安全性、效率、身份认证安全性上有较大的提升。

参考文献:

[1] 张建辉,付江,廖竣锴,等. 基于数据护照的跨域传输控制方法设计[J]. 通信技术,2020,53(8):2014-2018.

[2] 欧海文,曾淑娟. 基于数据标识的跨域增量数据交换模型[J]. 北京电子科技学院学报,2012,20(4):53-56.

[3] 杨晶,周海鑫. 政务信息共享数据安全中的密码支撑技术与应用[J]. 信息安全与通信保密,2021(6):16-23.

[4] 尹立民. 大数据环境中数据跨域传输安全控制仿真分析[J]. 计算机仿真,2018,35(11):193-196.

[5] 肖柳林. 面向多级安全的跨域交换技术研究[J]. 通信技术,2014,47(6):658-662.

[6] 徐良. 异构环境下无线传感大数据跨域传输安全控制系统设计[J]. 计算机测量与控制,2020,28(12):117-121.

[7] 罗义. 无证书跨域签密算法及其应用研究[D]. 南昌:南昌大学,2019.

[8] 周波,王树磊. 基于改进 HABE 算法的层次化多中心 SDN 跨域传输系统研究[J]. 高技术通讯,2020,30(11):1122-1132.

[9] 徐娟娟. 云环境下基于密算的异构跨域身份认证方案[D]. 桂林:桂林电子科技大学,2021.

[10] 潘雪,袁凌云,黄敏敏. 主从链下的物联网隐私数据跨域安全共享模型[J]. 计算机应用研究,2022,39(11):3238-3243.

[11] Bennett C H, Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tbssing[C]// IEEE. International Conference on Computers Systems and Signal Processing, September 12, 1984, Baialore, India. NewYork: IEEE, 1984: 175-179.

[12] Elkouss D, Martinez-M J, Ciurana A, et al. Secure Optical Networks Based on Quantum Key Distribution and Weakly Trusted Repeaters[J]. Journal of Optical Communications & Networking, 2013,5(4): 316-328.

[13] Lo H K, Chau H F. Unconditional Security of Quantum Key Distribution over Arbitrarily Long

Distances. Science,1999,283(5410):2050-2056.
[14] 谭政,单欣,孙献平,等. 利用量子密钥的加密/解密实现身份认证[C]. 第十二届全国量子光学学术会议论文摘要集. ,2006:18.
[15] 韩家伟. 量子密钥分发与经典加密方法融合关键技术研究[D]. 长春:吉林大学,2018.

Research on Cross-domain Data Security Transmission based on Quantum Technology

LIN Yusheng,　CHANG Yan
(College of Cyberspace Security Chengdu University of Information Technology, Chengdu 610225, China)

Abstract: In the era of big data, multi-organization co-working has become more and more common. Security sharing of data in cross-domain transmission and security management of data classification are urgent problems to be solved. This paper designs a cross-domain data security transmission model based on quantum technology, which can ensure the security of data sharing and management during cross-domain transmission. In this paper, the quantum gateway is introduced into the classical cross-domain transmission system, the identity certificate of users in the domain is formed by using the quantum gateway, and identity authentication is completed during cross-domain transmission. When the data is transmitted across domains, the data sender uses the quantum key in the quantum gateway to protect the cross-domain data and the quantum gateway forms the data signature for the cross-domain data, and binds the unique access permission of the cross-domain data. When the quantum gateway of the data access party receives the cross-domain data, the cross-domain identity authentication and data integrity check are carried out first. The domain control server maps permissions. Only individuals or departments with matching permissions can decrypt the cross-domain data. Finally, data visitors can view the cross-domain data to complete data sharing. Theoretical analysis shows that the quantum technology-based cross-domain data security transmission model proposed in this paper can realize cross-domain data protection, hierarchical classification management of users and data, cross-domain identity authentication, and higher key security.

Keywords: cross-domain transmission; data security sharing; quantum gateway; quantum key