专题：空天地一体化通信技术

天地一体化网络安全挑战及创新方案

李金慧[1,2]，黄铖斌[1,2]，王锦华[1,2]，刘洋[1]
（1. 中国电信股份有限公司研究院，上海 201315；
2. 云网基础设施安全国家工程研究中心，上海 201315）

摘　要：主要探讨了天地一体化网络在6G时代面临的安全挑战，提出了一种基于量子安全的创新方案。首先，介绍了天地一体化网络的发展背景和组网架构演进趋势，包括透明转发架构和星上再生架构的特点和应用场景。接着，分析了天地一体化网络面临的安全挑战，特别是数据传输安全风险和接入认证风险。针对这些挑战，提出了一种基于量子技术保障天地一体化网络安全的创新方案，利用量子通信的无条件安全性和后量子密码算法的优势，为天地一体化网络提供端到端的安全通信保障。最后，验证了采用量子技术保障天地一体化网络安全创新方案的可行性。

关键词：天地一体化网络；6G；量子；网络安全；后量子密码
中图分类号：TN915.08
文献标志码：A
doi: 10.11959/j.issn.1000−0801.2024170

Challenges and innovative solutions of space-ground integrated network security

LI Jinhui[1,2], HUANG Chengbin[1,2], WANG Jinhua[1,2], LIU Yang[1]
1. Research Institute of China Telecom Co., Ltd., Shanghai 201315, China
2. National Engineering Research Center of Cloud and Network Infrastructure Security, Shanghai 201315, China

Abstract: The security challenges confronting the space-ground integrated network in 6G era were mainly disscussed, and an innovative scheme based on quantum security was proposed. Firstly, the developmental backdrop and evolving trends of the integrated network’s architecture were outlined, highlighting the distinct features and application contexts of both the transparent forwarding and on-board regeneration frameworks. Secondly, the security challenges faced by the space-ground integrated network were analyzed, especially the risks of data transmission security and access authentication. In response to these challenges, the innovative solutions were proposed to ensure the security of the space-ground integrated network based on quantum technology. By leveraging the unconditional security of quantum communication and the advantages of post-quantum cryptographic algorithms, end-to-end secure communication protection for the space-ground integrated network was provided. Finally, the feasibility of using quantum

收稿日期：2024−03−31；修回日期：2024−06−14
基金项目：国家重点研发计划项目（No.2022YFB2902100）
Foundation Item: The National Key Research and Development Program of China (No.2022YFB2902100)

technology was verified to ensure the security of the space-ground integrated network.

Key words: space-ground integrated network, 6G, quantum, network security, post-quantum cryptographic

0 引言

随着物联网、云计算、大数据等技术的快速发展，天地一体化网络已成为连接天地、实现全球信息互联互通的关键。5G技术的商用化推动了天地一体化网络的发展，而未来的6G技术将进一步拓展网络覆盖范围，提升通信速率和服务质量[1]。然而，随着网络的不断扩展和复杂化，天地一体安全问题也日益凸显。黑客攻击、隐私泄露、网络设备的安全性等问题将成为6G天地一体通信面临的挑战。因此，研究6G时代的天地一体化网络安全问题具有重要意义[2-3]。

量子技术以其独特的物理特性，在通信领域展现出了巨大的潜力。量子通信利用量子态的不可克隆性和纠缠性，实现了无条件安全的通信，极大地提高了通信的安全性[4-7]。我国已经建成包括“京沪干线”“武合干线”“沪杭干线”等在内的多个量子通信骨干网络。这些网络利用量子密钥分发技术，为远距离通信提供了高安全性的密钥分发服务，进而通过安全的量子密钥为天地一体化网络通信的端到端安全通信提供保障[8-9]。同时，我国清华大学王小云院士团队、上海交通大学郁昱团队、复旦大学赵运磊团队、中科院路献辉团队等也在后量子密码（PQC）方面积极推进。PQC算法是一种抵抗量子计算对公钥密码算法攻击的新一代密码算法，可具有加解密、数字签名、密钥交换等多种安全能力[10-11]。随着PQC算法逐步标准化，利用PQC算法与现有公钥基础设施（PKI）体系的兼容性和可扩展性，可以为天间与地面之间的网络设备提供基于PQC数字证书的简化认证流程，快速建立安全通信连接。

本文主要梳理了天地一体化网络的组网架构演进趋势，分析了天地一体化网络的安全问题，并提出了一种基于量子技术保障天地一体化网络安全的创新方案。

1 天地一体化网络的组网架构演进

5G、6G天地一体通信网络可以提供和地面移动通信网相同的业务服务，包括语音、短消息、物联、视频等[12]。但由于我国地面网络比较完善，目前天地一体通信网络主要应用在特殊需求场景，如紧急通信、环境监测等。后续随着手机直连卫星技术发展，逐步扩展到普通大众消费者。针对卫星是否融合了移动通信网络能力，以及不同的应用场景和差异化的网络需求，天地一体化网络设计了两大类组网架构及4种组网模式，组网架构分析见表1 [12-18]。

1.1 透明转发架构

天地一体化网络透明转发架构中，用户设备、卫星、地面网络之间通过服务链路和馈线链

表1 组网架构分析[12-18]

组网架构	卫星	空口	终端	特点
面向普通终端的天地一体化网络透明转发架构	传统卫星	分开	普通终端	限轮船、飞机特定场景 时延高、成本低
面向融合终端的天地一体化网络透明转发架构	传统卫星	合一	融合终端	不限场景 时延高、成本低
天地一体化网络星上再生架构	卫星与基站合一	合一	融合终端	不限场景 时延低、技术复杂、成本高
天地一体化网络星上再生架构	卫星、基站、核心网网元合一	合一	融合终端	不限场景 时延超低、技术复杂、成本高

路连接，卫星提供射频中继转发功能，卫星对数据流转发过程透明。该架构可复用具备透明转发能力的现有卫星资源，无须重新发射定制化卫星，有利于天地一体化网络的快速商业落地。目前，天地一体化网络透明转发架构又可以根据不同场景需求及用户终端支持直连卫星的能力情况细分出2种组网方式。

（1）面向普通终端的天地一体化网络透明转发架构

面向普通终端的天地一体化网络透明转发架构如图1所示，主要针对邮轮、飞机等特殊场景，特别适用于不具备直接连接卫星能力的普通用户终端。这种方式通过在特殊场景内部署的小基站和专用卫星终端，实现汇聚用户数据，并将其发送到卫星。随后，卫星会将数据透传并转发回地面基站网关。

（2）面向融合终端的天地一体化网络透明转发架构

面向融合终端的天地一体化网络透明转发架构如图2所示，主要面向地面移动用户场景，适用于具备直连卫星能力的融合终端。在这种方式下，用户终端可通过非地面网络（non-terrestrial network，NTN）空口实现直连卫星，然后由卫星透传数据并转发回地面基站。这样的组网方式不仅满足了不同场景下的通信需求，也提高了通信的灵活性和效率。

1.2　星上再生架构

在天地一体化网络的星上再生架构中，用户终端与卫星、卫星与地面移动通信核心网之间通过标准化的通信接口实现连接。星上再生架构中卫星作为一种创新的接入方式，根据卫星与移动通信网的深度融合，为地面用户提供高效、稳定的通信服务。因此，与透明转发架构相比，星上再生架构具有诸多优势。目前，天地一体化网络

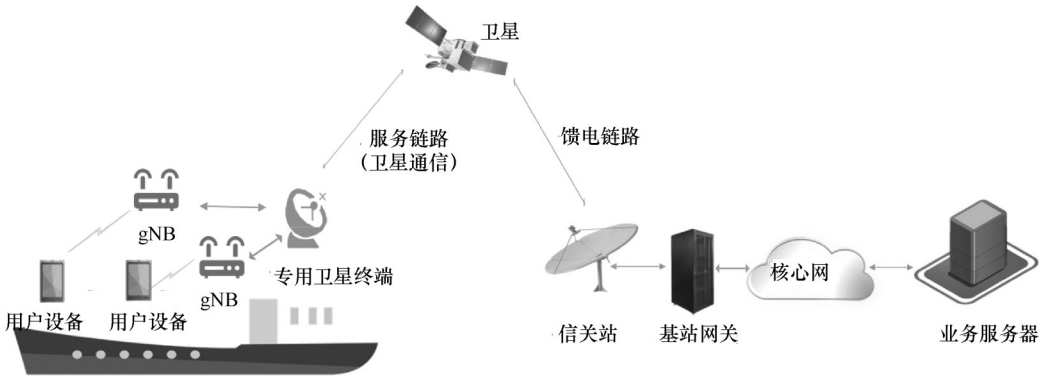


图1　面向普通终端的天地一体化网络透明转发架构

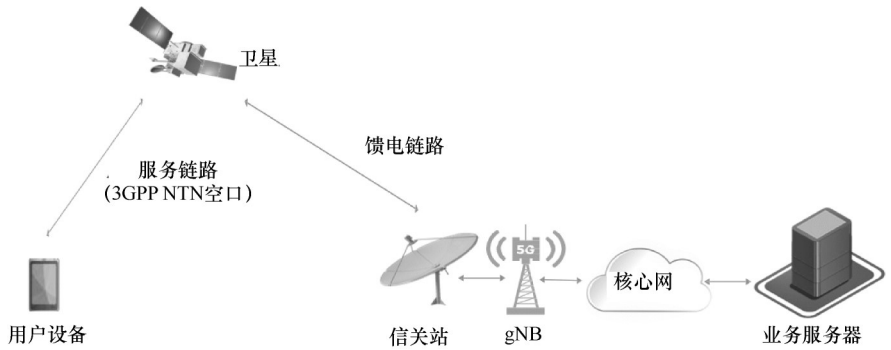


图2　面向融合终端的天地一体化网络透明转发架构

星上再生架构根据卫星与移动通信网的融合程度可细分为2种组网模式。

（1）卫星与基站融合的星上再生架构

卫星与基站融合的天地一体化网络星上再生架构如图3所示，将5G/6G基站功能集成到卫星。这种星载基站能够确保用户无缝接入最佳网络节点，并在星间实现顺畅切换。因此，基于星载基站的星上再生架构可以实现灵活组网，跳波束资源调度灵活，能为用户提供无感知的接入服务。但由于卫星资源受限，卫星计算成本较高，因此星载基站将伴随较高成本。

（2）卫星与基站、核心网网元融合的星上再生架构

这种组网架构需要卫星与基站和核心网网元深度融合，相比于星载基站的星上再生组网模式可以实现更低时延、更加灵活的组网，并为客户提供无感知的接入服务，卫星与基站、核心网网元融合的天地一体化网络星上再生架构如图4所示。将轻量化的5G/6G核心网集成到资源受限的卫星平台，实现星载核心网与地面核心网的互联互通和协同工作，将为万物互联、泛在覆盖提供有力的技术支撑。然而，由于技术复杂度的提升，这种架构也伴随着更高的卫星成本。

从2022年开始，我国已经开始基于海事卫星、天通一号等高轨道卫星开展5G天地一体化网络技术外场实验，2023年已经实现基于天地一体化网络的手机间双向通信测试。当前，由于融合卫星计算能力和存储能力有限，以及星上再生网络架构还不够完善的现状，透明转发模式是更可靠的选择。2024年2月，中国移动将搭载基站和核心网设备的两颗低轨试验卫星成功发射，预示着我国将有越来越多的通信卫星。随着我国低轨卫星的发展，核心网上星的天地一体化网络将是下一代通信技术的赛点。

2　天地一体化网络安全挑战

随着网络攻击手段的不断更新，如中间人攻击、拒绝服务攻击和信息窃取等，天地一体化网

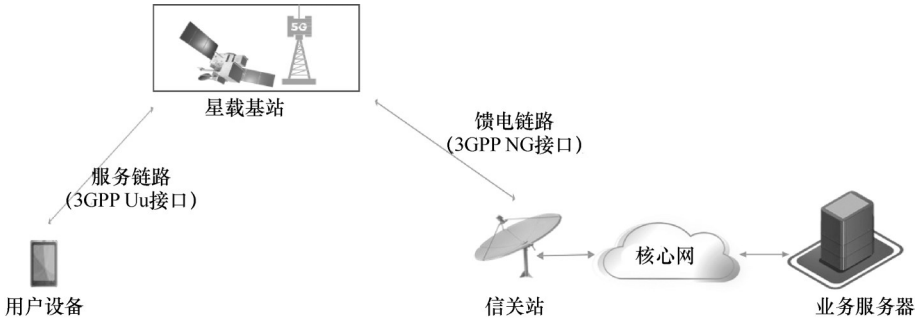


图3　卫星与基站融合的天地一体化网络星上再生架构

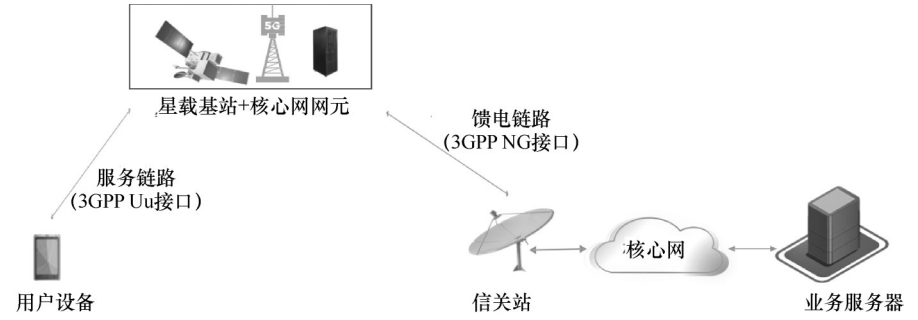


图4　卫星与基站、核心网网元融合的天地一体化网络星上再生架构

络的安全正面临着日益严重的挑战。首先，天地一体化网络由于其跨域、多层、异构的复杂网络架构，面临着多样化的安全风险。其次，由于天地一体化网络涉及空间和地面多个系统之间的信息共享和交互，这也可能引发一系列安全风险，包括信息泄露和非法访问等[19-21]。本文主要分析天地一体化网络在数据传输及接入认证过程存在的核心风险。

2.1　数据传输安全风险

天地一体化网络在数据传输过程中，因其开放信道、长距离传输及网络拓扑的动态变化等特性，面临着诸多挑战。这些特殊的网络结构不仅涉及跨域部署和远程运维，还增加了安全风险。首要的风险来自无线链路的数据传输，其空中信道更易遭受人为干扰、窃听、数据篡改、重放等威胁。其次，互联互通网元之间的数据传输也存在安全隐患，跨域部署使得网元间的数据传输面临潜在风险。再者，天地一体化网络开放的传输信道和大距离跨度加剧了数据窃听和数据仿冒等威胁，进一步增加了数据传输的安全风险。因此，必须高度重视这些安全风险，借助成熟的安全措施、有效的安全手段和创新的安全技术，持续应对挑战，确保天地一体化网络数据传输的安全稳定。

2.2　接入认证风险

在天地一体化网络架构中，不同网络运营方管理的“卫星—信关站—地面网络”要求特别关注网络边界的互联互通接口安全和访问安全。在星上再生架构中，尽管星上和地面网络基础设施可能属于同一运营方，但因物理位置差异仍需要划分不同安全域。特别考虑卫星节点长期运行在暴露空间，且网络拓扑高度动态变化，这增加了被假冒或劫持的风险，因此跨域互联网元的认证鉴权尤为关键。此外，多运营方融合组网还需确保各方间的互信。近年来，随着量子计算机的发展，窃听、篡改、重放等攻击变得更加容易。为了防止天地一体化不同域间的网络设备遭受网络攻击，同时降低身份认证过程中的计算负载，需要考虑一种高效且可靠的认证方案。

3　天地一体化网络安全创新方案

量子通信以其无条件安全性及高效的信息传输等独特优势，将为天体一体化网络通信注入新的活力。通过应用量子密钥分发（QKD）技术，可以保障天地一体化网络各节点间获得安全可靠的共享密钥，有效防范密钥被检测和窃听的风险，从而确保数据在传输过程中的机密性和完整性。此外，PQC算法具备抵抗量子计算攻击的能力，基于PQC算法的签名验签功能，可以保障天地一体化网络不同域间设备的身份真实性。这些技术共同为天地一体化网络通信提供更全面的安全保障。

3.1　透明转发架构安全创新方案

天地一体化网络透明转发架构安全创新方案如图5所示，可以利用我国地面QKD网络为天地一体化网络各节点系统安全地分发量子共享密钥。以面向普通终端的场景为例，可以在小基站与专用卫星终端之间增设量子加密网关。量子加密网关通过量子密钥充注的方式，从QKD网络末端的量子密钥充注平台获取量子密钥及密钥标识。同时，在信关站与核心网之间的基站网关内也集成量子安全能力，以便从QKD网络获取量子密钥及密钥标识。

量子加密网关是服务器设备，可以增加安全存储模块存储充注的量子密钥。根据业务需求，可按需扩展存储空间。同时，可根据业务需求及使用频率，设置具体的量子密钥使用及更新策略。其中，量子密钥可以直接作为会话密钥，也可以作为会话密钥的加密密钥，即通信双方在通信前随机生成或从密钥管理设备获取密钥作为本次会话密钥，用量子密钥加密会话密钥传递给通信对象，实现双方同步会话密钥。根据不同的使用策略及业务需求选择每次量子密钥充注量。以

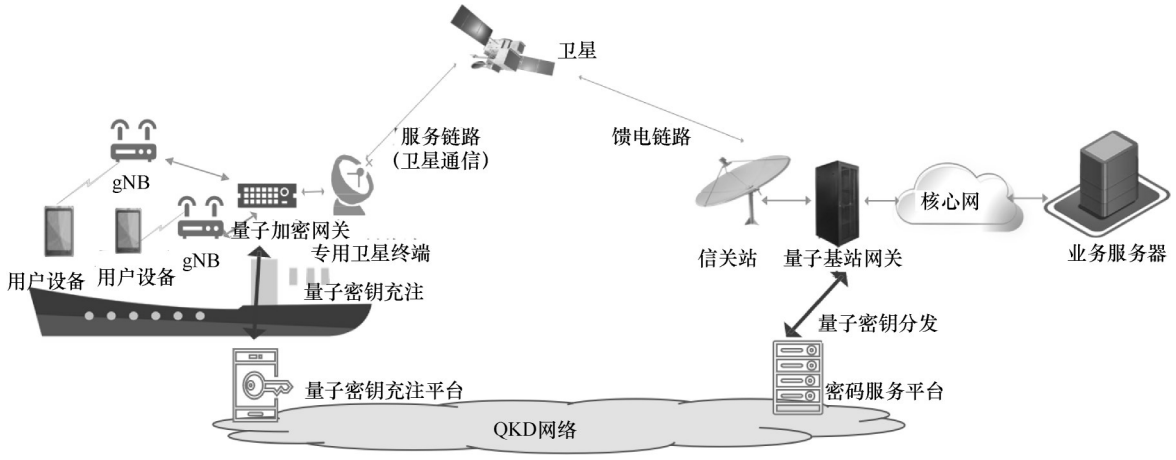


图5　天地一体化网络透明转发架构安全创新方案

量子密钥直接作为会话密钥使用为例，每个量子密钥128 bit，则每次充注1 TB的量子密钥则可进行量子密钥加密687亿次会话。所以可以根据具体的业务量，按需充注足量的密钥，并定期进行新的量子密钥充注即可。

量子密钥充注到网关设备后，网关设备会生成每个量子密钥的密钥标识符。用户设备进行安全的天地一体化网络通信关键流程如下。第一步，在用户设备发起通信请求后，用户数据首先会通过小基站汇聚到量子加密网关。第二步，量子加密网关会基于量子密钥使用策略和更新策略采用已经充注的量子密钥基于对称加密算法（如AES、SM4算法）对用户数据进行加密，加密后的数据和量子密钥标识通过专用卫星终端以射频信号的方式发送到卫星，卫星将量子密钥加密后的数据和量子密钥标识透明转发至地面信关站。到达信关站后，量子密钥加密后的数据和量子密钥标识以专线的方式转发给量子基站网关。第三步，量子基站网关基于接收到的量子密钥标识进行本地量子密钥检索或向密码服务平台申请该量子密钥。获得该量子密钥后，量子基站网关解密用户数据并通过核心网转发到相应的业务系统。整个过程实现了用户数据端到端的安全加密保障。

为了解决天体一体化网络域间设备身份认证问题，可以在用户侧、卫星侧以及地面网络侧不同域之间的设备在建立连接前采用Dilithium、FALCON、SPHINCS+等主流的PQC数字签名算法对设备身份进行签名验签，以实现通信双方的身份认证，从而确保通信的安全性。在设备间进行签名验证以确定设备身份时，通常采用签名算法对设备商提供的设备特定身份信息（如MAC地址、设备ID、设备型号等）进行签名，以保证身份的真实性。但在天地一体化网络中，设备身份不仅有硬件属性还有网络属性。其中网络属性包括FQDN、IP地址等，由设备的部署和运营机构提供。同时，为了保证每次对设备进行签名的唯一性，本方案设计对设备进行签名的身份信息不仅包括设备硬件属性和网络属性，还包括时间戳信息。

3.2　星上再生架构安全创新方案

天地一体化网络星上再生架构安全创新方案如图6所示，可以在用户设备内部增加量子加密软模块（如APP或SDK），同时在地面网络侧增设量子加密网关，以实现基于量子密钥的数据安全传输创新方案。在这种组网架构中，用户设备的量子加密模块和量子加密网关能够分别通过量子密钥充注方法和量子密钥分发等方式获取共享的量子密钥，从而在底层构建起端到端的量子安全通道，确保数据传输的安全性。

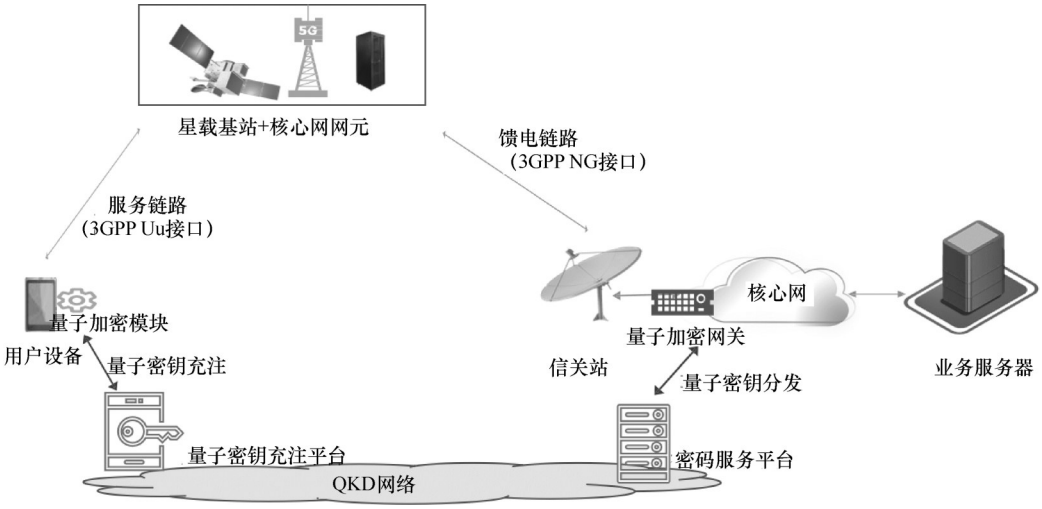


图6　天地一体化网络星上再生架构安全创新方案

量子加密模块集成到用户设备，由于用户设备的存储空间有限，充注的量子密钥量一般在几十Mbit左右。以用户设备每次充注10 Mbit量子密钥为例，每支量子密钥128 bit，则存储65万支量子密钥。根据量子密钥使用及更新策略，如每次会话使用一次密钥，可进行65万次会话；如每10 min更新一次密钥，则可使用12年以上。

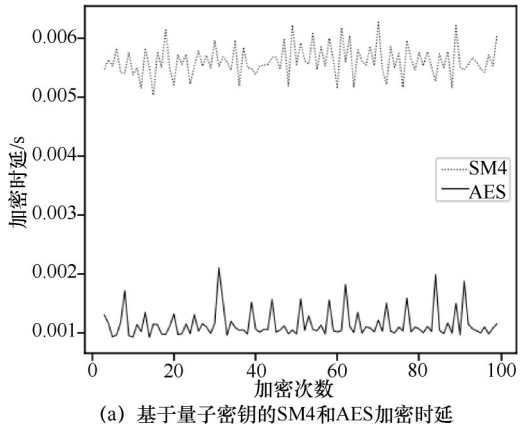
量子密钥充注到用户设备后，用户设备需要计算出每个量子密钥的密钥标识。用户设备进行安全的天地一体化网络通信关键流程如下。第一步，在用户设备发起通信请求前，对基于量子密钥使用策略和更新策略采用已充注的量子密钥基于对称加密算法（如AES、SM4算法）对用户的关键业务数据进行加密，并将加密后的数据和量子密钥标识打包通过NTN空口协议发送给融合卫星。第二步，融合卫星收到携带加密数据包的消息后，对消息进行解析，通过星间路由等服务将加密数据包通过地面信关站转发到地面核心网。第三步，地面核心网通过前置量子加密网关对接收到的加密数据包进行解密，具体解密步骤与透明转发架构量子加密网关相同。

在接入认证方面，星上再生架构与透明转发架构的安全方案相似，在用户侧、卫星侧以及地面网络侧不同域之间的系统在建立连接前可以采用Dilithium、FALCON、SPHINCS+等主流的PQC数字签名算法对设备身份进行签名验签，以实现通信双方的身份认证，为整个通信过程提供坚实的安全保障。设备身份信息包括设备硬件属性、网络属性以及时间戳信息。这一方案不仅提升了天地一体化网络的安全性，也为未来的网络通信提供了更可靠的技术支持。

4　可行性验证

为了验证本创新方案的可用性，本节分别对使用量子密钥实现通信数据加解密以及使用PQC签名算法实现设备间身份认证进行了性能测试分析。本次实验采用4核CPU及8 GB内存的计算机完成。首先，用随机数生成器生成128 bit随机数模拟量子密钥，采用当前比较常用的对称密码算法AES算法和国产SM4算法进行本次通信数据加密性能测试。实验记录了模拟量子密钥分别采用AES算法和SM4算法对200 kbit数据包进行加密的计算时间。同时记录了数据包进行分组对称加密后加密的数据包大小，基于量子密钥的加密传输测试如图7所示。

实验结果显示模拟量子密钥采用AES算法对



(a) 基于量子密钥的SM4和AES加密时延

```
ngth: 204800
Iteration 96: SM4: 0.004881143569946289 seconds, sm4 encryption data l
ength: 204800, AES: 0.001962423324584961 seconds, aes encryption data
length: 204800
Iteration 97: SM4: 0.004870414733886719 seconds, sm4 encryption data l
ength: 204800, AES: 0.0009756088256835938 seconds, aes encryption data
 length: 204800
Iteration 98: SM4: 0.004880189895629883 seconds, sm4 encryption data l
ength: 204800, AES: 0.0009775161743164062 seconds, aes encryption data
 length: 204800
Iteration 99: SM4: 0.00487828254699707 seconds, sm4 encryption data le
ngth: 204800, AES: 0.0009763240814208984 seconds, aes encryption data
length: 204800
Iteration 100: SM4: 0.004877567291259766 seconds, sm4 encryption data
length: 204800, AES: 0.0009756088256835938 seconds, aes encryption dat
a length: 204800
```

(b) 基于量子密钥的SM4和AES加密数据包大小

图7 基于量子密钥的加密传输测试

200 kbit的数据包加密平均时延仅0.001 3 s，数据包大小不变；模拟量子密钥采用SM4算法对200 kbit的数据包加密平均时延为0.005 8 s，数据包大小不变。因国产SM4算法的迭代次数相对较多，应用SM4算法时延相对高。模拟量子密钥采用这2种对称密码算法均不影响电信级通信服务质量，客户基本无感知。可以按照客户服务质量需求，按需选择对称加密算法基于量子密钥对用户数据加密保护。

针对用户侧、卫星侧以及地面网络侧不同域的设备间身份认证性能测试，本实验采用Dilithium算法为本次天地一体化网络不同系统间身份认证的PQC签名验签算法，实现设备间的身份认证。本次实验设计设备签名的身份信息为256 bit，包括设备MAC地址、IP地址以及时间戳信息，剩余位以0填充。本实验分别记录了1 000次Dilithium算法对256 bit设备身份信息进行签名和验签的平均时间，基于Dilithium算法进行签名验签的时延如图8所示。

实验结果显示采用的Dilithium算法的签名和验签运算的平均时延分别为0.003 9 s和0.001 3 s。一般只有设备初始连接或重启系统才会进行设备间身份认证，设备间已经建立连接并进行业务传输过程不会进行身份认证，所以不会对通信业的服务质量造成影响。

5 结束语

随着6G技术的快速发展，天地一体化网络将迎来更为广阔的应用前景。然而，网络安全问题始终是制约其发展的关键因素。本文通过对天地一体化网络的安全挑战进行深入分析，提出了一种基于量子技术保障天地一体化网络安全的创新方案，并验证了方案的可行性，为天地一体化网络的安全发展提供了新的思路。然而，网络安全是一个持续演进的过程，我们仍需不断探索和完善安全策略，以应对未来可能出现的各种安全威胁。期待未来的研究中，能够进一步挖掘量子

```
length: 256, interation: 990, sign time consume: 0.001674s, verify time comsume: 0
length: 256, interation: 991, sign time consume: 0.001872s, verify time comsume: 0
length: 256, interation: 992, sign time consume: 0.002628s, verify time comsume: 0
length: 256, interation: 993, sign time consume: 0.003071s, verify time comsume: 0
length: 256, interation: 994, sign time consume: 0.001146s, verify time comsume: 0
length: 256, interation: 995, sign time consume: 0.002925s, verify time comsume: 0
length: 256, interation: 996, sign time consume: 0.001992s, verify time comsume: 0
length: 256, interation: 997, sign time consume: 0.003744s, verify time comsume: 0
length: 256, interation: 998, sign time consume: 0.003277s, verify time comsume: 0
length: 256, interation: 999, sign time consume: 0.002769s, verify time comsume: 0
length: 256, interation: 1000, sign time consume: 0.005948s, verify time comsume:
length: 256, sign time consume: 0.003907s, verify time comsume: 0.001329s
root@ml-vm:~/PQClean/test/crypto_sign#
```

图8 基于Dilithium算法进行签名验签的时延

卫星（如墨子号、济南一号）在天地一体化网络中的应用潜力，为天地一体化网络的安全、高效、可靠运行提供有力保障。

参考文献：

[1] AZARI M M, SOLANKI S, CHATZINOTAS S, et al. Evolution of non-terrestrial networks from 5G to 6G: a survey[J]. IEEE Communications Surveys & Tutorials, 2022, 24(4): 2633-2672.

[2] GUO H Z, LI J Y, LIU J J, et al. A survey on space-air-ground-sea integrated network security in 6G[J]. IEEE Communications Surveys & Tutorials, 2022, 24(1): 53-87.

[3] 吴晓文, 焦侦丰. 面向6G的星地融合标准化研究进展[J]. 移动通信, 2024, 48(1): 2-12.
WU X W, JIAO Z F. Progress in standardization of satellite-terrestrial integration for 6G[J]. Mobile Communications, 2024, 48(1): 2-12.

[4] 龙桂鲁, 潘栋. 量子直接通信新进展与应用展望[J]. 信息通信技术与政策, 2022(7): 9-13.
LONG G L, PAN D. Recent advances in quantum secure direct communication and its perspectives of application[J]. Information and Communications Technology and Policy, 2022(7): 9-13.

[5] 黄钊龙, 韩召颖. 量子信息技术发展与国家安全[J]. 武汉大学学报(哲学社会科学版), 2024, 77(2): 51-60.
HUANG Z L, HAN Z Y. An analysis of the impact of quantum information technology on national security[J]. Wuhan University Journal (Philosophy & Social Science), 2024, 77(2): 51-60.

[6] 田野, 何申, 李德志, 等. 量子保密通信应用服务体系研究[J]. 电信科学, 2023, 39(12): 100-109.
TIAN Y, HE S, LI D Z, et al. Research on quantum secure communication application service system[J]. Telecommunications Science, 2023, 39(12): 100-109.

[7] 朱宏峰, 陈柳伊, 王学颖, 等. 量子密钥分发网络架构、进展及应用[J]. 沈阳师范大学学报(自然科学版), 2023, 41(6): 515-525.
ZHU H F, CHEN L Y, WANG X Y, et al. Architecture, progress, and applications of quantum key distribution networks[J]. Journal of Shenyang Normal University (Natural Science Edition), 2023, 41(6): 515-525.

[8] IMT-2030(6G)推进组 . 6G可信内生安全架构研究报告[R]. 2023.
IMT-2030 (6G) Promotion Group. Research report on 6G trustworthy endogenous security architecture[R]. 2023.

[9] AKHTAR M W, ALI HASSAN S, GHAFFAR R, et al. The shift to 6G communications: vision and requirements[J]. Human-Centric Computing and Information Sciences, 2020, 10(1): 53.

[10] 张然, 李丽香, 彭海朋. 后量子密码的发展趋势研究[J]. 信息安全与通信保密, 2023, 21(3): 64-81.
ZHANG R, LI L X, PENG H P. Research on the development trend of post-quantum cryptography[J]. Information Security and Communications Privacy, 2023, 21(3): 64-81.

[11] 孙奥, 何银, 李海波, 等. 后量子密码发展综述[J]. 信息安全与通信保密, 2023(9): 27-35.
SUN A, HE Y, LI H B, et al. Overview of post-quantum cryptography development [J]. Information Security and Communications Privacy, 2023(9): 27-35.

[12] 中国电信. 中国电信 5G NTN 技术白皮书—天地一体、手机直连[R]. 2023.
China Telecom. China Telecom 5G NTN technology white paper - integration of space and earth, direct connection of mobile phones[R]. 2023.

[13] 中国移动. 面向 6G 的天地一体融合网络技术白皮书[R]. 2024.
China Mobile. White paper on the technology of integrated space-ground network for 6G[R]. 2024.

[14] 刘会, 叶阳, 丁志东, 等. 星地融合下的手机直连关键技术研究[J]. 电信科学,2024,40(4):10-17.
LIU H, YE Y, DING Z D, et al. Research on key technologies of direct-to-handset under satellite-terrestrial integrated network[J]. Telecommunications Science, 2024, 40(4):10-17.

[15] 缪德山, 柴丽, 孙建成, 等. 5G NTN关键技术研究与演进展望[J]. 电信科学, 2022, 38(3): 10-21.
MIAO D S, CHAI L, SUN J C, et al. Key technologies and evolution of 5G non-terrestrial network[J]. Telecommunications Science, 2022, 38(3): 10-21.

[16] 王胡成, 徐晖, 孙韶辉. 融合卫星通信的5G网络技术研究[J]. 无线电通信技术, 2021, 47(5): 535-542.
WANG H C, XU H, SUN S H. Research of network technologies of 5G integrating satellite communication[J]. Radio Communications Technology, 2021, 47(5): 535-542.

[17] 孙韶辉, 戴翠琴, 徐晖, 等. 面向6G的星地融合一体化组网研究[J]. 重庆邮电大学学报(自然科学版), 2021, 33(6): 891-901.
SUN S H, DAI C Q, XU H, et al. Survey on satellite-terrestrial integration networking towards 6G[J]. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition), 2021, 33(6): 891-901.

[18] 刁兆坤, 杨丽, 王振章. 6G空天地一体化网络架构及其构建[J]. 通信世界, 2024(4): 36-39.
DIAO Z K, YANG L, WANG Z Z. 6G integrated network architecture of space, space and earth and its construction[J]. Communications World, 2024(4): 36-39.

[19] 曹欢, 陈岩, 周一青, 等. 空天地网络确定性服务架构、挑战及关键技术[J]. 西安电子科技大学学报, 2023, 50(3): 1-18.

CAO H, CHEN Y, ZHOU Y Q, et al. Deterministic service of space-air-ground integrated networks: architecture, challenges and key technologies[J]. Journal of Xidian University, 2023, 50(3): 1-18.

[20] 赵晨斌, 王蕴实. 基于5G/5G-A的天地一体化网络安全风险及策略研究[J]. 通信世界, 2023(12): 46-49.
ZHAO C B, WANG Y S. Research on network security risks and strategies of integration of heaven and earth based on 5G/5G-A[J]. Communications World, 2023(12): 46-49.

[21] 王蕴实, 张曼君, 徐雷, 等. 天地一体化网络安全使能技术研究[J]. 邮电设计技术, 2023(8): 1-4.
WANG Y S, ZHANG M J, XU L, et al. Research on security enabling technologies of space-ground integrated network[J]. Designing Techniques of Posts and Telecommunications, 2023(8): 1-4.

作者简介]

李金慧（1994– ），女，中国电信股份有限公司研究院工程师，云网基础设施安全国家工程研究中心工程师，主要研究方向为密码应用安全、5G/6G网络关键技术、网络安全、终端安全、量子安全等。

黄铖斌（1982– ），男，中国电信股份有限公司研究院工程师，云网基础设施安全国家工程研究中心工程师，主要研究方向为5G/6G网络安全、密码应用安全、终端安全、物联网安全、量子安全等。

王锦华（1982– ），男，中国电信股份有限公司研究院工程师，云网基础设施安全国家工程研究中心工程师，主要研究方向为云计算、大数据安全、终端安全、密码应用、量子安全等。

刘洋（1983– ），女，博士，中国电信股份有限公司研究院高级工程师，主要研究方向为5G/6G无线网络关键技术、网络架构及关键技术、网络自治技术等。