后量子密码在卫星互联网中的应用与思考

黄博学，谷 欣，单 超，苏 安
（中国星网网络创新研究院有限公司，北京 100029）

摘 要：随着量子计算机的不断发展，卫星互联网的安全性面临严峻挑战。首先，介绍卫星互联网和后量子密码的基本概念，深入分析卫星互联网在量子计算威胁下的安全需求。然后，通过对国内外后量子密码研究现状的综述，探讨基于格、编码、哈希函数和多变量多项式等后量子密码技术路线的特点及其在卫星互联网中的应用潜力。并通过比较分析，提出适合卫星互联网的后量子安全架构，为应对未来可能的量子计算威胁奠定基础。最后，探讨卫星互联网在量子计算时代所面临的主要安全问题和挑战，并提出相应的应对策略。

关键词：卫星互联网；后量子密码；量子安全
中图分类号：TP393
文献标识码：A
doi：10.11959/j.issn.2096−8930.2025011

Post-Quantum Cryptography in Satellite Internet: Applications and Reflections

HUANG Boxue, GU Xin, SHAN Chao, SU An
China Satellite Network Innovation Co., Ltd., Beijing 100029, China

Abstract: With the ongoing development of quantum computers, the security of satellite Internet faces significant challenges. This paper first introduced the basic concepts of satellite Internet and post-quantum cryptography, thoroughly analyzed the security needs of satellite Internet under the threat of quantum computing. By reviewed the current research status of post-quantum cryptography both domestically and internationally, this paper explored the characteristics and application potential of various post-quantum cryptographic approaches, included lattice-based, code-based, hash-based, and multivariate-based techniques. Through comparative analysis, a post-quantum security architecture suitable for satellite Internet was proposed, laid the groundwork for addressing future quantum computing threats. Finally, the paper discussed the main security issues and challenges that satellite Internet may face in the quantum computing era and proposed corresponding countermeasures.

Keywords: satellite Internet, post-quantum cryptography, quantum security

0 引言

卫星互联网是一种基于卫星通信技术的全球性网络，不仅用于军事、通信和广播等领域，还在卫星导航、气象监测、灾害管理和全球互联网覆盖等方面发挥了关键作用[1]。卫星互联网的重要性在现代社会愈发凸显，其发展不仅对国际通信和信息传播产生了深远影响，还为偏远地区提供了互联网接入的途径，促进了全球信息化进程。然而，卫星互联网也面临各种网络安全威胁，其中之一就是量子计算机的潜在威胁。

在当前以知识经济为基础的信息化社会中，网络信息技术飞速发展，保障网络信息安全无疑成为重中之重。历史上，图灵发明电子计算机破译了密码机，打破了国家之间信息安全的屏障。此后在经典计算机上，人们通过设计基于数学上NP难问题的加解密算法，维护了近50年的网络信息与通信安全。但是，1982年Feynman首次提出将量子力学与计算机相结合的构想[2]，开辟了量子时代的新纪元。1994年Shor[3]给出了一个能够在多项式

收稿日期：2024−10−21；修回日期：2025−01−11

时间内解决大整数分解和离散对数问题的Shor量子算法。至此，人们察觉到在功能强大的量子计算机面前，现有密码技术搭成的“城墙”是如此“不堪一击”。一旦量子计算机广泛应用，传统加密方法将不再足够安全。由于卫星互联网涉及大量的敏感数据传输，这种潜在威胁对于卫星互联网尤为重要，因此，保护卫星互联网免受量子计算机的威胁变得至关重要。

本文探讨后量子密码（Post-Quantum Cryptography，PQC）在卫星互联网中的应用，以有效应对量子计算机威胁。通过分析卫星互联网的安全需求，引出后量子密码学的原理和方法，探讨其在卫星互联网中的实际应用案例。此外，本文还讨论采用后量子密码所面临的挑战，并提供未来工作的展望，希望为卫星互联网领域的网络安全研究和实践提供有价值的参考，以确保卫星互联网的安全性和可靠性。

1　卫星互联网与后量子密码

1.1　卫星互联网概述

卫星互联网具有节点分布广泛、终端随遇接入、信道开放透明、拓扑动态变动、面向全球服务等特点，作为新一代网络服务系统，卫星互联网系统建设本身是一个长期迭代探索的过程，特别是在安全方面，卫星互联网的特点决定其在各个方面会面临更大的挑战和风险。首先，卫星节点和终端广泛分布于全球，使远距离甚至跨国界的攻击变得更加容易。其次，卫星信道的接入开放性在提高网络灵活性的同时，也为攻击者提供更多的入侵路径，使得通信过程更易被窃听和干扰，增加了数据泄露和被篡改的风险。此外，网络拓扑的动态变化进一步加剧了系统安全管理的复杂性。最后，卫星互联网系统的定位，也决定了其面临的对手不是普通网络黑客，而是有组织的境外竞争对手和敌对势力。在面对新技术发展带来的网络安全威胁，尤其是具有颠覆效果的量子攻击时，只有不断加强卫星互联网安全防护能力，研究前沿安全防护技术，创新安全防护体制，才能做到防患于未然。

1.2　后量子密码简介

量子计算机作为量子力学与计算机技术相结合的重要成果而备受关注。传统计算机使用二进制进行运算，而量子计算机则利用量子特性进行计算。与传统计算机相比，量子计算机的特点在于其独特的量子态和量子门操作，使其具有更高的运算速度和更强的计算能力。同时，量子算法充分发挥了量子比特的优势，针对特定的数学困难问题的解决效率实现了指数级提升。例如Grover算法[4]可以在平方根级别的时间内搜索解空间，主要应用于搜索和优化问题，使得对称密码体制中相关算法的安全性减半；Shor算法可以在多项式时间内解决大整数分解和离散对数问题，这意味着基于这些数学难题设计的传统公钥加密算法，如SM2、RSA、Diffie-Hellman等算法的安全性将受到严重破坏，即便是增加参数长度也是无效的。

量子计算机的快速发展减少了高计算量问题的处理时间，解决了大量复杂的数学问题，给当前已经发展成熟并且应用广泛的现代公钥密码体制带来了巨大的威胁与严峻的挑战。因此，为保障网络安全与信息系统后量子安全，密码学家基于新的数学困难问题设计了新的加密算法，目前主流的数学困难问题包括格、编码、多变量多项式以及哈希函数等相关困难问题构造的密码算法。这些算法的构造没有采用量子力学的物理特性，但基于这些数学困难问题所构造的密码算法则可以有效抵抗量子计算攻击，因此被称为后量子密码。

后量子密码延续了传统主流计算上的可证明安全研究方法，仅对算法本身进行修改，对现有的公钥加密体系框架和协议依然适用。因此，后量子密码提供了应对量子威胁的解决方案，确保了数据和通信在未来的计算环境中仍然能够保持隐私和安全，同时允许密码体制逐步、平滑地过渡到更安全的加密标准，而无须立即改变现有加密系统。

1.3　量子安全需求分析

卫星互联网的量子安全需求包括以下几个关键方面。

数据机密性保护：在卫星互联网中，数据的加密和解密至关重要，数据传输中的加密可以保护数据免受窃听和篡改。卫星互联网可能涉及敏感数据的传输，如政府通信、商业数据或军事信息，因此，尤其需要使用强加密算法来保护数据的机密性，但随着量子计算机的发展，传统的数据加密算法将不再安全。

数据完整性保护：在卫星互联网中，数据的完整性同样至关重要。数据的完整性要求保证数据在传输过程中不会被篡改或损坏，数据一旦被篡改，可能会导致信息的错误传播或损害数据的可信度，特别是由地面运行中心上传的运控指令等，一旦遭到篡改和破坏，若无法及时识别错误或恶意指令，则可能对卫星正常运行造成严重影响。

抗攻击性：卫星互联网应该具备一定的抗攻击性，以窃听、篡改、破坏、中间人攻击等为主。在卫星互联网中，中间人攻击是一种潜在威胁，由于卫星互联网信

道开放，攻击者可能试图将自己插入通信双方之间，以窃取、篡改或监视通信数据，从而导致信息泄露和数据被篡改。通信协议中通常通过身份认证和签名的方式避免此类攻击，但量子计算机凭借强大的计算能力很有可能找到哈希碰撞，进而伪造签名、仿冒通信双方的身份，对通信双方乃至整个系统造成严重破坏。

访问控制：卫星互联网应该具备用户资源管理和业务接入过程中的安全防护机制，包括终端接入认证、用户鉴权等。在统一通信过程中需要进行细粒度的忽略控制，并按需对数据进行安全隔离传输。鉴于量子计算机可以对传统的数字签名进行仿冒和篡改，亟须采用后量子密码技术对认证接入协议进行增强，确保访问控制安全可靠。

2 后量子密码研究现状

2.1 国内研究现状

2016 年 6 月，首届亚洲后量子密码论坛在我国成都顺利召开。鉴于 PQC 算法的飞速发展，原定于 2017 年召开的第二届亚洲后量子密码论坛提前到 2016 年 11 月于韩国首尔大学召开。2020—2021 年，丁津泰所带领的团队先后破解了美国国家标准与技术研究院（NIST）两个抗量子数字签名候选方案，包括 Luov[5] 和 GeMMS[6]，并将研究成果发表在 2020 年欧洲密码学年会和 2021 年美国密码学年会上。2022 年，上海交通大学的谷大武教授领导的 LoCCS 实验室成功破解了 80 维格的容错学习问题（Learning With Errors，LWE），创造了格密码中困难问题求解新的世界纪录，同时该纪录已经在格密码挑战的官方网站 LWE Challenge 上进行了公布。2023 年年初，北京、安徽和江苏等多省市发布政府工作报告，强调发展量子信息和量子科技。

虽然中国在 PQC 标准化的研究中起步较晚，但在 NIST-PQC 算法征集活动中也参与并贡献了一定的力量。参与设计的团队包括密码科学技术国家重点实验室、上海交通大学、复旦大学、中国科学院信息工程研究所等。其中，由中国科学院数据与通信保护研究教育中心设计的 LAC 算法[7]，与欧洲、美国、加拿大等提供的 PQC 算法一起，入选了 NIST 第二轮 PQC 密码算法名单。除此之外，中国在国内 PQC 算法标准的征集活动中也做了一些工作。自 2019 年起，中国密码学会开始举办全国密码算法设计竞赛，该竞赛仅面向中国的密码学者，受到了广大密码学家的青睐，并在公钥密码组的参赛作品中征集到大量的 PQC 算法。该竞赛的成功举办推动了我国密码理论与应用技术的发展，是我国 PQC 算法标准制定的基础，意味着我国 PQC 技术的研究正逐步向国际先进水平看齐，致力于通过充分调动国内各界研究力量，推动国产化研发，保障未来后量子时代下我国的网络空间安全。

2.2 国外研究现状

2015 年 8 月，美国国家安全局（NSA）宣布对当前美国政府所使用的“密码算法 B 套件”进行安全性升级，升级的算法将用于后量子时代过渡期的加密标准。2016 年 4 月，NIST 颁布“后量子密码学”研究报告，并宣布将启动 PQC 算法标准计划，截至 2022 年 7 月，美国已完成 3 轮算法标准化流程筛选，并选中 4 个候选算法进行标准化。

2022 年 9 月，美国国家安全局发布了《商业国家安全算法套件 2.0”(CNSA 2.0) 网络安全咨询 (CSA) 》新指南，新指南中表示，预计国家安全系统的所有者和运营商将在 2035 年之前开始使用后量子算法。

2023 年 3 月，网络安全公司 QuSecure 宣布，该公司已首次通过星链（Starlink）太空卫星传输受 PQC 保护的数据，表明其率先推出美国首个具有量子弹性的实时端到端卫星加密通信链路。几周后，QuSecure 宣布与埃森哲合作，双方在卫星通信领域成功进行了一项使用 PQC 保护的多轨道数据通信测试。此次测试旨在为组织提供更加安全和可靠的卫星通信解决方案。

2023 年 3 月，纳米卫星通信服务供应商 SAS Global 宣布与网络安全公司 CyberProtonics 建立合作伙伴关系。后者将为 SAS 的纳米卫星和地面终端部署端到端的 PQC 技术，以保护客户数据免受网络攻击的威胁。SAS 立即开始嵌入 CyberProtonics 的专有 PQC 技术，为下一次发射做准备。

2023 年 5 月，量子网络安全服务商 Qrypt 宣布与政府 IT 解决方案商 Carahsoft 科技公司建立合作伙伴关系。根据合作协议，Carahsoft 将作为 Qrypt 的政府方面的整合专家，Carahsoft 将通过其经销商合作伙伴、信息技术企业解决方案和国家合作采购联盟订单，向美国联邦政府提供 Qrypt 公司的量子安全加密技术。

2.3 问题与思考

后量子研究成为国内外科技领域的热门话题，吸引了广泛的研究兴趣和巨额投资，正逐渐演变成一场全球竞争。这一研究领域的崛起是因为人们认识到传统的量子技术将对传统的密码学领域带来严重挑战，并且量子计算技术还在快速取得进展和突破中，如何保证国家关键信息基础设施的安全问题变得日益迫切。卫星互联网是一个高度依赖信息传输和通信的领域，随着量子计算

和通信技术的不断发展，卫星互联网的长期安全性面临严峻挑战，我国需要尽快布局后量子密码体制的研究、标准化和商业化，尽快研究并应用适用于卫星互联网的抗量子攻击的密码体制，争取在未来的技术竞争中占据领先地位，推动我国的卫星互联网可持续发展。

3　后量子密码技术分析

3.1　技术路线

（1）基于格的后量子密码

格（Lattice）是一种数学结构，定义为一组线性无关的非0向量（称作格基）的整系数线性组合。格密码的主要数学基础是格中的两个困难问题：格的最短矢量问题[8]（SVP）和格的最近矢量问题[9]（CVP）。SVP是对于给定的一组基，找出其所生成的格中欧氏距离（两点之间的距离）最小的非零向量。即在格上找到一个非零向量$\boldsymbol{v}$，满足对格上的任意非零向量$\boldsymbol{u}$，均有$\|\boldsymbol{v}\|\leqslant\|\boldsymbol{u}\|$。CVP是对于给定的格及任一向量$\boldsymbol{y}$，找出格中与该向量距离最近的向量。即在格上找到一个向量$\boldsymbol{v}$，满足对格上的任意非零向量$\boldsymbol{u}$，均有$\|\boldsymbol{v}\text{-}\boldsymbol{y}\|\leqslant\|\boldsymbol{u}-\boldsymbol{y}\|$。格是一个困难的问题，并且难度还能控制，满足了成为密码学算法核心的必要条件。

在PQC算法中，对格的研究是最活跃、最灵活的。基于格的算法在安全性、公私钥大小、计算速度上可达到较好的平衡。第一，基于格的算法可以实现加密[10]、数字签名[11]、密钥交换[12]、属性加密[13]、函数加密[14]、全同态加密[15]等各类功能的密码学构造[16]。第二，基于格的算法的安全性依赖于求解格中问题的困难性。这些问题在达到相同的安全强度时，基于格的算法的公私钥大小比其他方案更小，计算速度更快，且能被用于构造多种密码学原语，更适用于真实世界中的应用。因此，基于格的算法被认为是最有前景的PQC算法之一[17]。

（2）基于编码的后量子密码

编码理论是数学与计算机科学的一个分支，用来处理在噪声信道中传送信息时的错误倾向。基于编码的密码体制也被认为是在量子计算机中相对安全的密码算法，其核心在于将一定数量的错误码字引入编码中，提升纠正错误码字或计算校验矩阵的伴随式过程的复杂度。一个较早提出且至今仍在使用的基于编码的加密算法是1978年McEliece提出的McEliece公钥加密方案[18]，该方案基于的困难问题是对称群隐藏子群问题[19]。该算法相对于现有公钥密码体制而言加密速度快，但是由于其公钥尺寸过大，该算法并不是很实用，不过针对该算法的改进最终也进入了NIST第3轮的候选算法中。基于编码的公钥密码体制或许可以成为基于数论的公钥密码体制的一个很好的替代[20]。

（3）基于哈希函数的后量子密码

基于哈希函数的签名算法由Ralph Merkel提出[21]，被认为是传统数字签名（RSA、DSA、ECDSA等）的可行代替算法之一。基于哈希函数的签名算法由一次性签名方案演变而来，并使用Merkle的哈希树认证机制。哈希树的根是公钥，一次性的认证密钥是树中的叶子节点。基于哈希函数的签名算法的安全性依赖哈希函数的抗碰撞性。由于没有有效的量子算法能快速找到哈希函数的碰撞，因此基于哈希函数的构造可以抵抗量子计算机攻击。此外，基于哈希函数的数字签名算法的安全性不依赖某一个特定的哈希函数。即使目前使用的某些哈希函数被攻破，还可用更安全的哈希函数直接代替被攻破的哈希函数。

（4）基于多变量多项式的后量子密码

基于多变量多项式的算法使用有限域上具有多个变量的二次多项式组构造加密[22]、签名[23]、密钥交换[24]等算法[25]。多变量密码的安全性依赖于求解非线性方程组的困难程度，即多变量二次多项式问题[26]。该问题被证明为非确定性多项式时间困难。目前没有已知的经典和量子算法可以快速求解有限域上的多变量方程组。与经典的基于数论问题的密码算法相比，基于多变量多项式的算法的计算速度快，但公钥尺寸较大，因此适用于无须频繁进行公钥传输的应用场景。

3.2　对比分析

上述PQC密码体制均可以为卫星互联网系统提供量子安全保护，但由于算法本身的功能和性能特性，其各自所适用的应用场景有所区别，各密码算法体制在功能和性能方面的对比见表1。

表1　各密码算法体制在功能和性能方面的对比

对比项	基于格的PQC密码算法	基于编码的PQC密码算法	基于哈希函数的PQC密码算法	基于多变量多项式的PQC密码算法
密码构造	密钥交换	密钥交换	签名方案	密钥交换
	加密	加密		签名
	签名			加密
构造技术	容错学习问题	错误纠正码	哈希树	二次多项式组
安全性	最短向量问题	Goppa解码	抗碰撞性	非线性方程组
公钥大小	较小	大	小	较大
密文或签名大小	小	较大	大	较小
计算速度	快	较快	快	较快
功能	很好	不好	不好	较好

3.3　应用分析

基于格的密码体制构造灵活、功能性强，可以实现密钥交换、数据加解密、数字签名等功能，满足卫星互联网中大部分密码应用场景，且在密码体制的改进过程中，密钥尺寸不断缩小、运算速度不断提高，逐步在安全性、密钥尺寸以及计算速度上达到更好的平衡。

基于编码的密码体制可以实现密钥交换[27]和数据加解密[28]功能，但由于密码本身构造的原因无法实现数字签名功能。这使得该密码体制在卫星互联网中的应用受限，仅能对通信数据实现机密性保护，而对于数据的完整性则无法提供有效保护，需要同其他后量子密码体制配合使用。

基于哈希函数的密码体制主要用于数字签名[29]，其优点在于签名生成和验证速度快、公钥尺寸小，具有低时延、低存储成本的特点。可适用于实时性要求较高、计算资源受限的卫星互联网系统。

基于多变量多项式的密码体制同样可以实现密钥交换、加解密和签名等功能，且计算速度较快，但该密码体制的公钥尺寸通常较大，存储成本较高，因此在资源受限的卫星网络中限制条件较大。

综上所述，在多种后量子密码技术路线中，基于格的后量子密码体制具有构造灵活、功能性强、效率高等特点，在卫星互联网系统中具有更多的综合优势和广泛的应用前景。

4　后量子密码技术应用

基于对卫星互联网安全需求以及系统架构的分析和对后量子密码技术的理解，构建后量子时代下的卫星互联网安全架构如图 1 所示。

（1）卫星终端设备：包含手持、车载、机载等多样化体制标准的终端，通过终端安全模块实现入网认证和接入鉴权。

（2）卫星节点：后量子安全模块负责对地面节点完成认证、鉴权和星地、星间链路传输安全，并通过后量子密钥协商算法保障密钥量子安全。

（3）信关站：负责对星地用户数据进行加解密，保证数据的机密性和完整性。

（4）密钥管理中心：通常部署在地面的运控中心，在可信环境中完成各实体部分的身份注册和密钥生成、分发和管理。

（5）数据中心：负责重要数据的安全存储，结合后量子密码技术、分布式存储、冗余备份等方式对重要数据进行安全保护。

（6）通信链路：结合现有通信协议和后量子密码体制建立量子安全链路，确保通信数据在量子攻击下的机密性和完整性。

具体的后量子安全措施与技术应用见表 2。

终端身份认证：基于 5G 标准的终端身份认证方式主要有 EAP-AKA 和 EAP-TLS 两种，其中 EAP-TLS 协议基于 PKI 证书体系实现了传输层安全保护。但随着量子计算的发展，原有的公钥证书体系安全性将受到威胁，攻击者可以通过量子计算机伪造用户签名进而仿冒合法终端，或直接通过破译加密数据进而获取后续的会话密钥。因此，需要通过后量子密码技术对现有安全协议进行增强，从而实现终端身份认证的后量子安全。例如，采用基于格的密钥交换技术可以防止量子攻击者破译加密数

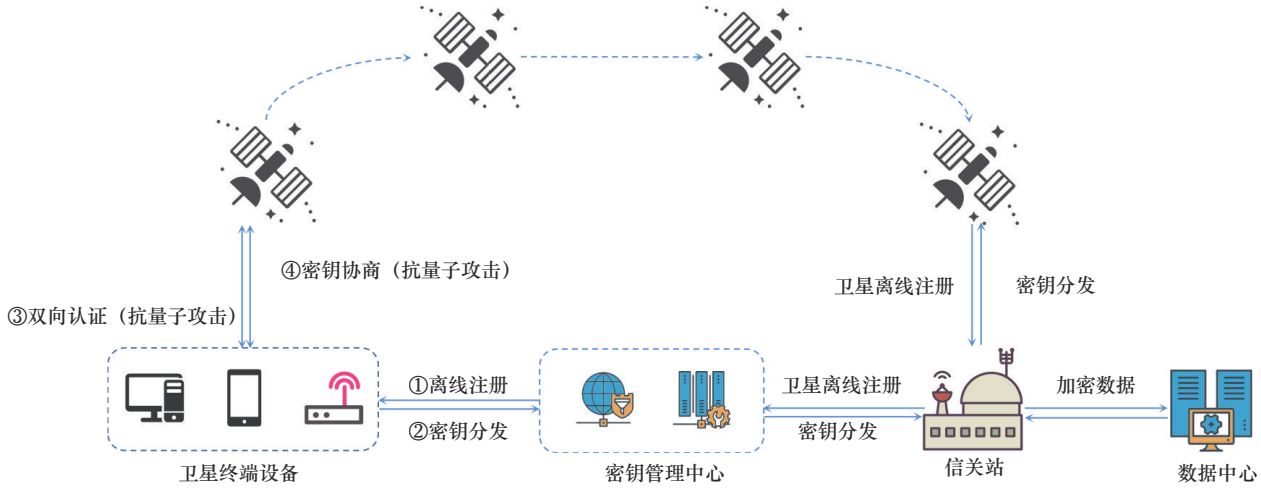

图 1　后量子时代下的卫星互联网安全架构

表2　后量子安全措施与技术应用

应用场景	技术手段	实现效果
终端身份认证	基于格的密钥交换技术； 基于格的签名技术	防止量子攻击者破译加密数据进而获取会话密钥； 防止量子攻击者伪造签名进而仿冒合法终端
端到端的数据加密	基于格的加密技术； 基于格的签名技术	防止量子攻击者窃取、破译用户敏感数据； 防止量子攻击者的中间人攻击
星地重要数据机密性保护	基于格的加密技术	防止量子攻击者窃取、破译重要数据
星地重要数据完整性保护	基于格的签名技术	防止量子攻击者篡改、伪造重要数据
密钥管理	基于格的密钥交换技术； 基于格的加密技术	防止量子攻击者破译加密数据进而获取更新密钥； 防止量子攻击者截获并破译存储的密钥密文信息
重要数据存储	基于格的加密技术； 基于格的签名技术	防止量子攻击者窃取、破坏重要数据信息

据进而获取会话密钥，采用基于格的签名技术可以防止量子攻击者伪造签名进而仿冒合法终端。

端到端的数据加密：通过基于格的加密技术，在终端进行加解密，为用户提供端到端的量子安全通信，同时采用基于格的签名技术保证通信数据的完整性，并防止中间人攻击。

星地重要数据机密性保护：通过基于格的加密技术，在信关站和运控中心对重要数据进行加密，保证数据的机密性，防止重要数据在通信过程中被量子攻击者窃取、破译。

星地重要数据完整性保护：通过基于格的签名技术，在信关站和运控中心对重要数据进行签名，保证数据的完整性，防止重要数据被量子攻击者篡改、伪造。

密钥管理：在密钥更新阶段，密钥管理中心通过基于格的密钥交换技术对系统中各个安全网元中的密钥进行更新，防止量子攻击者在此期间破译加密数据进而获取最新版本的密钥。此外，通过基于格的加密技术对密钥进行加密可以防止量子攻击者截获并破译存储的密钥密文信息。

重要数据存储：通过基于格的加密技术和签名技术对存储在数据中心的重要数据进行数据机密性和完整性保护。

5　卫星互联网后量子安全的应对策略

5.1　问题与挑战

（1）政策层面

第一，后量子密码标准化需要时间。目前后量子密码技术领域研究还处于百花齐放的阶段，尚未形成统一的标准，不同的算法和方案存在互操作性问题。确保不同卫星终端设备和地面站设备之间的互操作性，以及不同卫星互联网系统的互操作性是一个挑战。

第二，隐私和数据保护面临新的挑战。PQC 技术可能会对数据隐私和保护提出新的问题，包括如何处理加密密钥和用户身份验证信息等方面的问题。如何适用现有的数据隐私和保护政策，以确保用户数据在使用 PQC 技术时得到妥善处理是一个挑战。

（2）技术层面

第一，性能和计算复杂性：后量子密码通常比传统的对称和非对称密码学算法计算更复杂，需要消耗的计算资源较传统密码算法更为庞大，进而可能导致卫星和终端设备性能下降。因此需要寻找高效的 PQC 算法以满足卫星互联网通信的性能需求。

第二，密钥管理：PQC 通常需要更长的密钥长度来提供相同的安全性，这可能导致更大的密钥管理和存储需求。如何有效地生成、分发、存储和更新 PQC 密钥是一个重要的问题。

第三，实时性要求：卫星互联网通信通常需要低时延和实时性。某些 PQC 算法的计算复杂性可能会增加通信时延，这对某些应用场景可能不太适用。

第四，可伸缩性：卫星互联网系统通常包括大量的终端设备和用户，需要确保 PQC 算法在大规模使用时仍然有效。

5.2　应对策略

（1）加强顶层设计

第一，加快我国卫星互联网密码应用向后量子迁移，推动国内后量子密码技术的研究和标准化进程，鼓励国内电信运营商、互联网运营商、网络安全厂商等企业同高校联合开展后量子密码相关的技术研究、产业推进和人才培养。

第二，在体制、系统、商业模式设计阶段充分考虑后量子时代卫星互联网安全建设发展思路，构建引领后量子安全的卫星网络总体发展布局。

（2）加强技术研究

第一，针对卫星互联网星上计算资源消耗大的问题，研究更适用于卫星互联网环境的轻量化后量子密码体制，并通过编译器优化、并行计算、专用加密芯片和硬件加速等技术，减少加解密时计算资源的消耗和计算时延。

第二，针对卫星互联网密钥管理问题，研究高效的密钥生成算法以减小密钥生成的计算负担，并通过预置密钥的方式，在卫星和地面站之间建立初始的密钥材料，然后在通信链路上安全地传输这些材料。这可以减少频繁的密钥分发操作。

第三，加强轻量化加解密、无证书接入认证、快速星间切换等新型网络安全技术研究，简化安全协议的交互过程，降低通信成本和时延。

第四，采用分布式系统架构，提高系统的扩展性，使用云计算或边缘计算资源，根据需求动态分配计算资源。根据流量负荷进行伸缩，以满足大规模用户的使用需求。

6 结束语

卫星互联网的快速发展为全球通信带来了前所未有的便利，然而，随着量子计算技术的迅猛发展，传统加密方法的安全性将难以保证。本文旨在引发后量子时代对卫星互联网通信安全性的重视。只有提前布局后量子安全防护体系，创新研究后量子安全技术，才能更好地保护卫星互联网通信的安全性，继续推动数字社会的发展，促进全球信息交流的繁荣。

参考文献：

[1] 沈学民, 承楠, 周海波, 等. 空天地一体化网络技术: 探索与展望[J]. 物联网学报, 2020, 4(3): 3-19.
SHEN X M, CHENG N, ZHOU H B, et al. Space-air-ground integrated networks: review and prospect[J]. Chinese Journal on Internet of Things, 2020, 4(3): 3-19.

[2] ROSSBY C G, COLLABORATOR S. Relation between variations in the intensity of the zonal circulation of the atmosphere and the displacements of the semi-permanent centers of action[J]. Journal of Marine Research, 1939, 2(1): 38-55.

[3] SHOR P W. Algorithms for quantum computation: discrete logarithms and factoring[C]//Proceedings 35th Annual Symposium on Foundations of Computer Science. Piscataway: IEEE Press, 1994: 124-134.

[4] GROVER L K, GROVER L K. A fast quantum mechanical algorithm for database search[C]//Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing. New York: ACM, 1996: 212-219.

[5] DING J T, DEATON J, SCHMIDT K, et al. Cryptanalysis of the lifted unbalanced oil vinegar signature scheme[M]//Advances in Cryptology - CRYPTO 2020. Cham: Springer International Publishing, 2020: 279-298.

[6] TAO C D, PETZOLDT A, DING J T. Efficient key recovery for all HFE signature variants[M]//Advances in Cryptology - CRYPTO 2021. Cham: Springer International Publishing, 2021: 70-93.

[7] LU X, LIU Y, ZHANG Z, et al. LAC: Practical ring-LWE based public-key encryption with byte-level modulus[J]. Cryptology ePrint Archive, 2018.

[8] MICCIANCIO D, GOLDWASSER S. The springer international series in engineering and computer science[Z]. 2002.

[9] HANROT G, PUJOL X, STEHLÉ D. Algorithms for the shortest and closest lattice vector problems[M]//Coding and Cryptology. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011: 159-190.

[10] AGRAWAL S, YAMADA S. Optimal broadcast encryption from pairings and LWE[C]//Advances in Cryptology - EUROCRYPT 2020. Cham: Springer International Publishing, 2020: 13-43.

[11] ALKIM E, BARRETO P S L M, BINDEL N, et al. The lattice-based digital signature scheme qTESLA[M]//Applied Cryptography and Network Security. Cham: Springer International Publishing, 2020: 441-460.

[12] SINGH V. A practical key exchange for the Internet using lattice cryptography[J]. IACR Cryptology EPrint Archive, 2015: 138.

[13] ZHANG J, ZHANG Z F, GE A J, et al. Ciphertext policy attribute-based encryption from lattices[C]//Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security. New York: ACM, 2012: 16-17.

[14] MERA J M B, KARMAKAR A, MARC T, et al. Efficient lattice-based inner-product functional encryption[M]//Public-Key Cryptography - PKC 2022. Cham: Springer International Publishing, 2022: 163-193.

[15] PATHAK V. Lattices, homomorphic encryption, and CKKS[EB]. 2022.

[16] BERNSTEIN D J, LANGE T. Post-quantum cryptography[J]. Nature, 2017, 549(7671): 188-194.

[17] NEJATOLLAHI H, SHAHHOSSEINI S, CAMMAROTA R, et al. Exploring energy efficient architectures for RLWE lattice-based cryptography[J]. Journal of Signal Processing Systems, 2021, 93 (10): 1139-1148.

[18] MCELIECE R J. A public-key cryptosystem based on algebraic[J]. Coding Thv, 1978, 4244:114-116.

[19] SHOR P W. Algorithms for quantum computation: discrete logarithms and factoring[C]//Proceedings 35th Annual Symposium on Foundations of Computer Science. Piscataway: IEEE Press, 1994: 124-134.

[20] 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.
[21] MERKLE R. Secrecy, authentication, and public key systems[Z]. 2019.
[22] DEBNATH S K, MESNAGER S, DEY K, et al. Post-quantum secure inner product functional encryption using multivariate public key cryptography[J]. Mediterranean Journal of Mathematics, 2021, 18(5): 204.
[23] SMITH-TONE D. New practical multivariate signatures from a nonlinear modifier[M]//Post-Quantum Cryptography. Cham: Springer International Publishing, 2021: 79-97.
[24] KUANG R, PEREPECHAENKO M, BARBEAU M. A new post-quantum multivariate polynomial public key encapsulation algorithm[J]. Quantum Information Processing, 2022, 21(10): 360.
[25] DING J T, GOWER J E, SCHMIDT D S. Multivariate public key cryptosystems[M]. New York: Springer, 2006.
[26] MATSUMOTO T, IMAI H. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption[M]//Advances in Cryptology — EUROCRYPT ’88. Heidelberg: Springer Berlin Heidelberg, 1988: 419-453.
[27] ZHANG Z, ZHANG F. Code-based non-interactive key exchange can be made[J]. Cryptology ePrint Archive, 2021.
[28] SINGH M K. Code-based cryptography: a comparative study of key sizes[M]//Advanced Communication and Intelligent Systems. Cham: Springer Nature Switzerland, 2023: 359-368.
[29] IFTIKHAR Z, IFTIKHAR M, ALI SHAH M. Quantum safe cloud computing using hash-based digital signatures[C]//Proceedings of the 2021 26th International Conference on Automation and Computing (ICAC). Piscataway: IEEE Press, 2021: 1-6.

[作者简介]

黄博学（1998– ），男，硕士，中国星网网络创新研究院有限公司助理工程师，主要研究方向为卫星互联网网络安全技术、后量子密码等。

谷欣（1980– ），男，硕士，中国星网网络创新研究院有限公司高级工程师，主要研究方向为卫星互联网网络安全架构、网络安全标准等。

单超（1977– ），男，博士，中国星网网络创新研究院高级工程师，主要研究方向为卫星通信以及卫星互联网技术，长期从事总体论证工作。

苏安（1997– ），男，硕士，中国星网网络创新研究院有限公司助理工程师，主要研究方向为卫星互联网网络安全、数据安全等。