基于格的卫星网络轻量化后量子接入认证方案

王杉杉[1]，赵国锋[1]，徐川[1]，韩珍珍[2]
（1. 重庆邮电大学通信与信息工程学院，重庆 400065；2. 重庆邮电大学网络空间安全与信息法学院，重庆 400065）

摘　要：针对卫星网络的接入认证方案存在量子计算攻击，认证开销大和交互时间长的问题，提出了一种基于格的卫星网络轻量化后量子接入认证方案。在注册阶段，基于近似最短向量问题（SVP）的格密码哈希函数对用户身份进行保密，降低该阶段的计算时间并完成身份注册；在认证阶段，基于盆景树算法设计低维模乘模加的双向认证算法，将其算法复杂度从平方级降至线性级，进一步减少认证过程中的通信开销和卫星上的计算开销。理论证明，所提方案能够抵御量子计算攻击，性能分析表明，与格密码认证方案相比，所提方案至少减少 150% 的认证时间。

关键词：卫星网络；格；双向认证；盆景树算法
中图分类号：TN302
文献标志码：A
DOI：10.11959/j.issn.1000−436x.2024180

Lattice-based lightweight post quantum access authentication scheme for satellite network

WANG Shanshan[1], ZHAO Guofeng[1], XU Chuan[1], HAN Zhenzhen[2]
1. School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
2. School of Cyber Security and Information Law, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

Abstract: Aiming at the problems of quantum computing attacks, high authentication overhead and long interaction time in satellite network access authentication schemes, a lightweight post quantum access authentication scheme based on lattice for a satellite network was proposed. In the registration phase, a lattice Hash function based on the approximate shortest vector problem (SVP) was used to keep the user's identity confidential, which reduced the computation time and completes identity registration. In the authentication phase, a low dimensional modular multiplication modular addition mutual authentication algorithm was designed based on the bonsai tree algorithm, which reduced the algorithm complexity from the quadratic level to the linear level, further decreasing the communication costs during the authentication process and computational costs on satellite. Theoretical proof and performance analysis show that the scheme resists quantum computing attacks and reduces authentication time by at least 150% compared to lattice authentication schemes.

Keywords: satellite network, lattice, mutual authentication, bonsai tree algorithm

0　引言

卫星网络[1]具有广覆盖、高可靠以及灵活部署等优势，可为多种用户提供网络接入服务。但由于卫星节点暴露、无线信道开放、网络动态异

收稿日期：2024–07–02；修回日期：2024–09–24
通信作者：赵国锋，zhaogf@cqupt.edu.cn
基金项目：国家自然科学基金资助项目（No.62171070）；重庆邮电大学博士研究生人才培养基金资助项目（No.BYJS202204）；重庆市博士后科学基金资助项目（No.CSTB2022NSCQ-BHX0043）
Foundation Items：The National Natural Science Foundation of China (No.62171070), Chongqing University of Posts and Telecommunications Ph. D. Post-graduate Talent Cultivation Project (No. BYJS202204), Chongqing Post-Doctoral Science Fund Project (No.CSTB2022NSCQ-BHX0043)

构等特性，与传统地面网络相比在实体通信过程中更容易遭受窃听、拦截、重放等网络攻击[2]，需要在网络实体请求通信前对实体的身份进行认证以检测异常用户。然而，传统卫星网络接入认证方案[3-4]的安全性取决于离散对数或者质数分解的数学问题。随着量子理论的快速发展，Shor[5]指出利用量子计算机和量子算法可在多项式时间内有效解决这些问题，基于数论的接入认证方案难以抵御量子计算攻击，因此亟须研究后量子安全接入认证方案。然而，由于星上资源受限，难以承受大的计算负担，必须设计轻量化的后量子接入认证方案。

为了抵御量子计算攻击，各个领域引入了基于错误学习（LWE, learning with error）和小整数解（SIS, small integer solution）问题的格密码接入认证协议。例如，Khan等[6]提出了一种基于格的公共云计算匿名认证协议，该协议基于LWE加密技术完成实体间的认证。然而，协议中使用了大量的哈希（Hash）函数，在传至其他认证实体时需验证哈希函数的正确性，增加了网络的计算开销。Gulati等[7]结合区块链技术和格密码设计了一种认证和会话密钥交换方案。通过随机加倍函数和交叉舍入函数生成身份验证密钥，同时使用调和函数生成会话密钥，实现车辆之间的相互认证和数据传输。然而，通信实体间需要多次传递参数完成认证流程，导致认证通信开销大。Li等[8]提出了一种基于SIS问题的车载自组网条件隐私保护认证协议，旨在同时实现双向认证和隐私保护。然而，该协议在注册过程中使用额外的密钥生成算法和原像抽样算法生成系统密钥和用户注册参数，使得注册时间增大。

目前，学者们还将这些安全机制扩展到了卫星网络中。Ma等[9]在卫星物联网中提出了一种基于SIS问题的半聚合签名机制，通过将大量签名聚合为单个签名和一些辅助信息来减少传输开销，同时基于Gentry加密机制设计了会话密钥协议为物联网设备与网关之间生成会话密钥。然而，Gentry加密机制需要多次迭代和嵌套才能完成加解密过程，极大地增加了认证时间。Guo等[10]基于环错误学习（RLWE, ring learning with error）提出了一种预协商后量子认证协议，卫星通过提前获取地面管控中心的密钥协商参数以快速实现与用户之间的认证。然而，该协议增加了预协商阶段，导致整个认证流程复杂度的增加。Kumar等[11]基于RLWE问题和概率论中的特征函数提出了一种后量子认证和密钥协商协议，用户和网络控制中心（NCC, network center control）使用格加密算法生成验证和密钥协商参数，并通过卫星转发。Guo等[12]同样结合特征函数和RLWE问题提出了一种身份匿名的认证和密钥协商协议，该协议在网关中使用哈希算法申请临时身份更新，保障用户身份的匿名性。然而，上述2种协议都无法提供后向加密，攻击者可通过现有密钥推算出未来密钥。

尽管现有格密码接入认证方案都可以抵御量子计算攻击，但为保障认证过程中的安全性，方案在注册和认证阶段使用了高复杂度的算法，造成网络开销过大，无法满足轻量化认证的需求。为了解决上述问题，本文提出了一种基于格的卫星网络轻量化后量子接入认证方案。卫星和地面用户基于低计算复杂度的近似最短向量问题（SVP, shortest vector problem）的格密码哈希函数生成不可伪造的注册消息，并在网络控制中心（NCC）上完成注册，降低了注册阶段的计算时间。同时，该方案在地面和卫星上分别采用盆景树算法和原像抽样算法，一次性完成对卫星和地面用户身份合法性的验证，且仅使用了较少的低维模乘运算，将认证算法的计算复杂度从平方级降为线性级，减少卫星上的计算开销。实验结果表明，与现有格接入认证方案相比，本文提出的一种基于格的卫星网络轻量化后量子接入认证方案至少减少150%的认证时间。

1 格密码基础知识

本文所提的一种基于格的卫星网络轻量化后量子接入认证方案主要包括盆景树算法和哈希函数族，本节通过介绍其原理来阐明所提方案的理论基础，特别声明$\log q$是以2为底的对数。

1.1 格理论简介

定义1 格[13]。假设$\boldsymbol{B}=\{\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m\}$由$n$维欧几里得空间$\mathbb{R}^n$中$m$个线性无关向量组成，那么格$L(\boldsymbol{B})$定义为这组向量的所有整数系数的线性组合，记为

$$\Lambda=L(\boldsymbol{B})=\{\sum_{i=1}^{m}a_i\boldsymbol{b}_i:a_i\in\mathbb{Z}\}$$

其中，$\mathbb{R}$和$\mathbb{Z}$分别表示实数域和整数域，n为$L(\boldsymbol{B})$

的维数，m为秩，$\boldsymbol{B}$为格的一组基。

定义 2　格拉姆-施密特（Gram-Schmidt）正交化[13]。设$\boldsymbol{B}=(\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m)\in\mathbb{R}^{n\times m}$是格$\Lambda$的基矩阵，其 Gram-Schmidt 正交化$\tilde{\boldsymbol{B}}=(\tilde{\boldsymbol{b}}_1,\tilde{\boldsymbol{b}}_2,\cdots,\tilde{\boldsymbol{b}}_m)\in\mathbb{R}^{n\times m}$，其中$\tilde{\boldsymbol{b}}_1=\boldsymbol{b}_1,\tilde{\boldsymbol{b}}_{i\geqslant 2}=\boldsymbol{b}_i-\dfrac{\sum_{j=1}^{i=1}\left\langle \boldsymbol{b}_i,\tilde{\boldsymbol{b}}_j\right\rangle}{\left\langle \tilde{\boldsymbol{b}}_j,\tilde{\boldsymbol{b}}_j\right\rangle}\tilde{\boldsymbol{b}}_j$。

定义 3　SIS 问题[14]。给定整数q、矩阵$\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$和实数$\beta$，求解满足齐次线性方程组$\boldsymbol{Az}=0\bmod q$的整数向量$\boldsymbol{z}\in\mathbb{Z}^m$，同时$\|\boldsymbol{z}\|\leqslant\beta$。

值得注意的是，密钥生成算法和原像抽样算法是轻量化后量子方案中使用的2个关键算法。下面将展示关于密钥生成算法和原像抽样算法等的相关引理。

引理 1　格基生成算法[15]。给定一个m维格$\Lambda=L(\boldsymbol{B})$上的满秩向量集合组成矩阵$\boldsymbol{S}$，存在一个确定多项式时间算法 ToBasis( ) 能够输出Λ的一个基$\boldsymbol{T}$，满足$\|\tilde{\boldsymbol{T}}\|\leqslant\|\tilde{\boldsymbol{S}}\|$且$\|\boldsymbol{T}\|\leqslant\|\boldsymbol{S}\|\dfrac{\sqrt{m}}{2}$。

引理 2　密钥生成算法[16]。给定素数$q\geqslant 3$，正整数$m\geqslant 5n\log q$，存在一个概率多项式时间算法 TrapGen( ) 能够输出矩阵$\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$和格$\Lambda(\boldsymbol{A})$的一组基$\boldsymbol{T}\in\mathbb{Z}_q^{m\times m}$，使得矩阵$\boldsymbol{A}$的分布与$\mathbb{Z}_q^{n\times m}$上的均匀分布是统计不可区分的，且以压倒性的概率满足短基$\|\boldsymbol{T}\|\leqslant O(n\log q)$和$\|\tilde{\boldsymbol{T}}\|\leqslant O(n\log q)$。

引理3　高斯抽样算法[17]。在格上按照高斯分布抽取格点的具体过程，即高斯抽样算法 SampleD( )。具体算法如下。

输入　参数$s>0$，向量$\boldsymbol{d}\in\mathbb{R}^n$，$n$维格$\Lambda$及其基矩阵$\boldsymbol{B}=(\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n)$

输出　向量$\boldsymbol{v}\in\Lambda$

令$v_n\leftarrow 0,d_n\leftarrow d_i$，依次令$i=n,n-1,\cdots,1$。

1) 计算$d_n\leftarrow\dfrac{<d_i,\tilde{\boldsymbol{b}}_i>}{\|\tilde{\boldsymbol{b}}_i\|^2}\in\mathbb{R}$，$s_i\leftarrow\dfrac{s}{\|\tilde{\boldsymbol{b}}_i\|}>0$；

2) 随机挑选整数$z_i\leftarrow D_{\mathbb{Z},s_i,d_i}$，其中$D_{\mathbb{Z},s_i,d_i}$是以实数$d_i$为中心的高斯分布；

3) 令$d_{i-1}\leftarrow d_i-z_i\boldsymbol{b}_i$，$v_{i-1}\leftarrow v_i-z_i\boldsymbol{b}_i$。

引理 4　原像抽样算法[18]。原像抽样算法 Samplepre( ) 是利用单向陷门函数$f(s)=\boldsymbol{As}$中的陷门求任意向量$\boldsymbol{u}\in\mathbb{Z}^n$在函数上的原像过程。具体算法如下。

输入　安全参数n，正整数$m>5n\log q$，矩阵$\boldsymbol{A}\in\mathbb{Z}^{n\times m}$，格基$\boldsymbol{T}\in\mathbb{Z}^{m\times m}$，高斯参数$s\geqslant\|\tilde{\boldsymbol{T}}\|\cdot w(\sqrt{\log n})$，$\|\tilde{\boldsymbol{T}}\|\leqslant O(\sqrt{n\log q})$，$\boldsymbol{u}\in\mathbb{Z}^n$

输出　$\boldsymbol{e}=\boldsymbol{t}+\boldsymbol{v}$

1)选择一个整数向量$\boldsymbol{t}\in\mathbb{Z}^n$，求解线性方程组$\boldsymbol{At}=\boldsymbol{u}\bmod q$；

2)利用高斯抽样算法 SampleD($\boldsymbol{T},s,-t$) 抽样向量$\boldsymbol{v}\sim D_{\Lambda^{\perp},s,-t}$。

1.2　盆景树算法及 Hash 函数族

盆景树模型由 Cash 等[19]提出，作为陷门函数的推广，因其扩展性可用于分布式网络如车联网中[20]。本文主要使用盆景树模型中的扩展控制算法和随机控制算法，其中格上的扩展控制算法可以将较小维数的格和基向量构造成更大维数的格和基向量，随机控制算法用来保障扩展控制算法输出的基向量相互独立。

引理 5　扩展控制算法。给定任意一个格$\Lambda(\boldsymbol{A})$以及它的一组基$\boldsymbol{S}$，其中$\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$，$\boldsymbol{S}\in\mathbb{Z}^{m\times m}$。设矩阵$\tilde{\boldsymbol{A}}\in\mathbb{Z}_q^{n\times m}$，$s$为高斯参数满足$s\geqslant\eta_\varepsilon\left(\Lambda^{\perp}(\boldsymbol{A})\right)$，$\eta_\varepsilon$为平滑参数，存在一个确定的多项式时间算法 ExtBasis$\left(\boldsymbol{S},\boldsymbol{A}'=(\boldsymbol{A}\|\tilde{\boldsymbol{A}}),s\right)$输出格$\Lambda^{\perp}(\boldsymbol{A}')$的基$\boldsymbol{S}'$，满足$\|\tilde{\boldsymbol{S}}\|=\|\tilde{\boldsymbol{S}}'\|$。

引理 6　随机控制算法。给定n维整数格Λ的一组基$\boldsymbol{S}$和高斯参数$s\geqslant\|\tilde{\boldsymbol{S}}\|w(\sqrt{\log n})$，$w(\,)$为渐近函数，存在一个概率多项式时间算法 RandBasis($\boldsymbol{S},s$)，输出格Λ的基$\boldsymbol{S}'$使得$\|\boldsymbol{S}'\|\leqslant s\sqrt{m}$。如果$\boldsymbol{S}_0$、$\boldsymbol{S}_1$是同一个格的2个不同的基且$s\geqslant\max\left\{\|\tilde{\boldsymbol{S}}_0\|,\|\tilde{\boldsymbol{S}}_1\|\right\}w(\sqrt{\log n})$，那么 RandBasis($\boldsymbol{S}_0,s$)和 RandBasis($\boldsymbol{S}_1,s$)的输出不可区分。

Lyubashensky 等[21]定义了一个安全 Hash 函数族，其安全性是基于平均状态下的近似 SVP 问题，该 Hash 函数族由$\mathbb{Z}_q^m$映射到$\mathbb{Z}_q$且满足向量加法和数乘运算的同态性，在本文中用于加密实体的真实身份，防止隐私信息泄露，同时作为验证参数完成实体的身份检验和注册。具体定义如下。

令$\boldsymbol{\alpha}\in\mathbb{Z}_q^m$，则 Hash 函数族的输入为$\boldsymbol{v}\in\mathbb{Z}_q^m$，输出为$(\boldsymbol{\alpha},\boldsymbol{v})\in\mathbb{Z}_q$，记作$h_{\boldsymbol{\alpha}}(\boldsymbol{v})=(\boldsymbol{\alpha},\boldsymbol{v})$。因此，对任意向量$\boldsymbol{v},\boldsymbol{e}\in\mathbb{Z}_q^m$和$c\in\mathbb{Z}_q$，有

1) $h_{\boldsymbol{\alpha}}(\boldsymbol{v}+\boldsymbol{e})=h_{\boldsymbol{\alpha}}(\boldsymbol{v})+h_{\boldsymbol{\alpha}}(\boldsymbol{e})(\bmod q)$；

2) $h_{\boldsymbol{\alpha}}(c\boldsymbol{v})=ch_{\boldsymbol{\alpha}}(\boldsymbol{v})$。

2 方案总体设计

2.1 系统模型组成

常见的认证方案一般分为系统建立、实体注册和实体认证3个阶段，这种分阶段的方法不仅可提高身份验证的可信度，还可有效防止未授权用户的接入访问。基于格的卫星网络轻量化后量子接入认证系统模型如图1所示，由3类实体组成：NCC、卫星实体和地面用户，具体描述如下。

NCC：作为卫星和地面用户的地面指挥部，通过密钥生成算法输出系统公钥，并将公共参数例如哈希函数进行全网公布。然后验证卫星和地面用户发送的注册请求消息的正确性并生成对应的响应消息。若注册响应消息未被攻击者篡改伪造，则表示地面用户和卫星注册成功。

卫星实体：包括多种轨道卫星，如地球同步轨道卫星、中轨道地球卫星和低轨道地球卫星等。由于低轨上的卫星离地面最近，传输时延短，路径损耗小，通常作为卫星接入网络中的一员为地面用户提供服务，因此，基于格的卫星网络轻量化后量子接入认证方案在无特殊说明下在低轨道地球卫星与地面用户之间进行相互认证，且每颗卫星都具有唯一的身份标识。作为认证实体之一，为降低注册阶段的计算开销，卫星基于近似SVP问题的格密码的哈希函数生成注册请求消息。接着采用原像抽样算法输出卫星签名，同时一次性完成地面用户身份合法性的验证。最后生成会话密钥，并将其加密后传输给地面用户。

地面用户：包括车辆、智能设备和船舶等。地面用户同样基于格密码的哈希函数构建注册请求消息降低注册开销。接着使用盆景树算法输出用户签名，同时一次性完成卫星身份合法性的验证。最后生成会话密钥并验证卫星侧会话密钥的正确性，若正确，则表示会话密钥协商成功。

2.2 方案研究思路

当认证实体的注册时间超过注册存活期，或者实体因设备故障长时间未接入网络时，实体之间需重新认证以获得数据传输资格。由于星地距离远，星上资源有限，应采用开销小交互时间短的认证方案。然而，现有方案采用高复杂度的注册算法和认证算法以保障其接入安全性，为此，提出了一种基于格的卫星网络轻量化后量子接入认证方案，具体思路如下。

1) 系统建立阶段，如图1的①所示，NCC需要为实体生成认证过程提供所需要的安全参数。NCC使用密钥生成算法TrapGen(n,q)生成系统公钥$(\boldsymbol{A}_0,\boldsymbol{A}_i),i=1,2,\cdots,k$，以及认证中的其他安全参数，如各种类型的哈希函数或随机矩阵等，并公开所有的系统公共参数。

2) 实体注册阶段，如图1的②所示，卫星和地面用户都需要在NCC上进行注册以获得后续相互认证的资格。首先基于近似SVP问题的格上哈希函数将真实身份ID映射为不可伪造的整数后，结

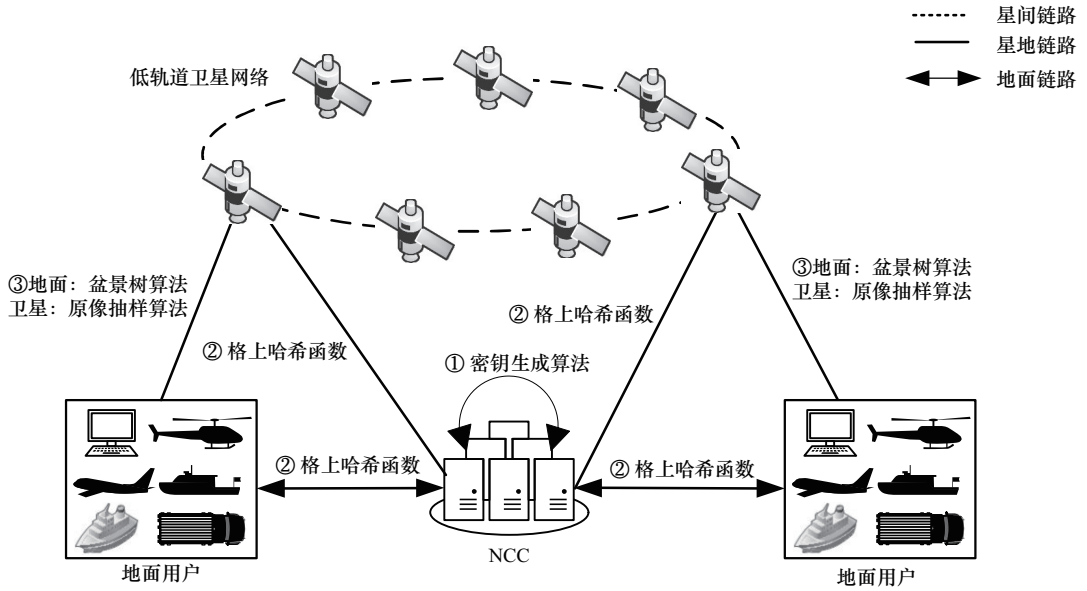


图1 基于格的卫星网络轻量化后量子接入认证系统模型

合注册请求符生成注册请求消息发送给NCC。接着NCC利用格的哈希函数族计算公式 $h_\alpha(c\mathrm{ID}) \stackrel{?}{=} \mathrm{ch}_\alpha(\mathrm{ID})$ 来验证消息 $\left(h_\alpha(\mathrm{ID}),\mathrm{Request}\right)$ 的正确性，其中 $h_\alpha(c\mathrm{ID}),c,h_\alpha(\mathrm{ID}) \in \mathbb{Z}_q$。同时利用自身身份标识符和实体的真实身份生成注册响应消息 $\left(h_\alpha(\mathrm{Ncc}+\mathrm{ID}),\mathrm{Ncc},\mathrm{Responce}\right)$ 返回地面用户和卫星。最后，地面用户和低轨道地球卫星通过计算 $h_\alpha(\mathrm{Ncc}+\mathrm{ID}) \stackrel{?}{=} h_\alpha(\mathrm{Ncc}) + h_\alpha(\mathrm{ID})$ 来验证响应消息的正确性，若验证结果正确，则表示地面用户和卫星注册成功。

3) 实体双向认证与密钥协商阶段，如图1的③所示，卫星和地面用户基于签名机制相互验证对方身份的合法性，并生成各自的会话密钥。当系统中的地面用户需要向低轨道地球卫星请求服务时，地面用户通过盆景树算法设计了一种认证算法，利用哈希函数输出均衡的特性选取随机矩阵 $\boldsymbol{A}_{\mathrm{GUE}} = \boldsymbol{A}_0||\boldsymbol{A}_1||\boldsymbol{A}_2||\cdots||\boldsymbol{A}_j$，并使用原像抽样算法 $\boldsymbol{v}_0 \leftarrow \mathrm{Samplepre}\left(\boldsymbol{T}_{\boldsymbol{A}_0},s,-\sum \boldsymbol{A}_j\boldsymbol{v}_j \ (\mathrm{mod}\,q),\boldsymbol{A}_0\right)$ 得到地面用户的签名消息 $\boldsymbol{v}_{\mathrm{GUE}} = (\boldsymbol{v}_0||\boldsymbol{v}_1||\cdots||\boldsymbol{v}_j)$。接着生成会话密钥参数 $\boldsymbol{e}_{\mathrm{GUE}}$，构造认证请求消息 $\left(\boldsymbol{e}_{\mathrm{GUE}},\boldsymbol{H}(\mathrm{ID}_{\mathrm{GUE}}),\boldsymbol{v}_{\mathrm{GUE}},t_1\right)$ 并发送给卫星。该轻量化后量子认证算法中的运算多为低维模乘模加，降低了地面侧的认证复杂度。卫星收到消息后，首先验证认证请求消息的正确性，完成地面用户的身份合法性检验。随后，使用原像抽样算法 $\boldsymbol{w}_0 \leftarrow \mathrm{Samplepre}(\boldsymbol{T}_{\boldsymbol{A}_0},s,\boldsymbol{A}_0)$ 得到卫星的签名消息 $\boldsymbol{w}_0$，再结合会话密钥参数 $\boldsymbol{e}_{\mathrm{SAT}}$ 生成会话密钥 $\mathrm{SK}_{\mathrm{SAT}} = h_\alpha(\mathrm{Ncc})\boldsymbol{e}_{\mathrm{SAT}}\boldsymbol{e}_{\mathrm{GUE}}$，并构造认证响应消息 $\left(\boldsymbol{e}_{\mathrm{SAT}},\boldsymbol{w}_0,t_3,H_1(\mathrm{SK}_{\mathrm{SAT}})\right)$ 发送给地面。然后地面用户通过计算 $\boldsymbol{A}_0\boldsymbol{w}_0 \stackrel{?}{=} 0\,(\mathrm{mod}\,q)$ 来验证响应消息的正确性，若正确，则地面用户和卫星相互认证成功。最后地面用户计算会话密钥 $\mathrm{SK}_{\mathrm{GUE}} = h_\alpha(\mathrm{Ncc})\boldsymbol{e}_{\mathrm{SAT}}\boldsymbol{e}_{\mathrm{GUE}}$ 用来验证公式 $H_1(\mathrm{SK}_{\mathrm{SAT}}) \stackrel{?}{=} H_1(\mathrm{SK}_{\mathrm{GUE}})$ 是否成立，若成立，则会话密钥协商成功，认证到此结束。在后续通信过程中，卫星和地面用户可分别使用会话密钥对数据加密后进行传输。

3　方案流程

基于格的卫星网络轻量化接入认证方案中的相关符号和定义如表1所示。下面将介绍各个阶段的具体实现。

表1　相关符号和定义

参数	定义
n	安全参数
q	质数
β	多项式函数
s	高斯参数
$(\boldsymbol{A}_0,\boldsymbol{A}_i),i=1,2,\cdots,k$	系统主公钥
H,H_1,h_α	哈希函数
Resquest	注册请求标识符
Response	注册响应标识符
$\mathrm{ID}_{\mathrm{GUE}}$	地面用户真实身份
$\mathrm{ID}_{\mathrm{SAT}}$	低轨道地球卫星真实身份
Ncc	NCC真实身份
$\boldsymbol{e}_{\mathrm{GUE}},\boldsymbol{e}_{\mathrm{SAT}}$	会话密钥参数
SK	会话密钥
t_1,t_2,t_3,t_4	时间戳

3.1　系统建立阶段

在基于格的卫星网络轻量化接入认证方案中，NCC生成系统公共参数，例如安全参数、质数、高斯分布、哈希函数等，然后发布公共参数。为方便表达，低轨道地球卫星表示为SAT，地面用户表示为GUE。NCC选择安全参数 n、质数 q、正整数 b 和 $m = bn\log q$，多项式函数 $\beta = \mathrm{poly}(n)$ 和高斯参数 $s = O(\sqrt{n\log q})w(\sqrt{\log n})$ 以及渐近函数 $w()$，并设 $H{:}\mathbb{Z}_q^m \to \{0,1\}^k$ 和 $H_1{:}\mathbb{Z}_q^{n\times n} \to \{0,1\}^*$，以及基于近似SVP问题的格密码的哈希族 $h_\alpha{:}\ \mathbb{Z}_q^m \to \mathbb{Z}_q,\boldsymbol{\alpha} \in \mathbb{Z}_q^m$ 为安全的哈希函数。NCC运用密钥生成算法 $\mathrm{TrapGen}(n,q)$ 得到矩阵 $\boldsymbol{A}_0 \in \mathbb{Z}_q^{n\times m}$ 以及格 $\Lambda_q^{\perp}(\boldsymbol{A})$ 上的陷门基 $\boldsymbol{T}_{\boldsymbol{A}_0} \in \mathbb{Z}_q^{m\times m}$。同时生成随机独立的 k 个矩阵 $\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_k \in \mathbb{Z}_q^{n\times m}$，并选择系统公钥为 $(\boldsymbol{A}_0,\boldsymbol{A}_i),i=1,2,\cdots,k$。最后，NCC公开生成的系统公共参数：$\left\{(\boldsymbol{A}_0,\boldsymbol{A}_i),\boldsymbol{T}_{\boldsymbol{A}_0},h,H,H_1\right\}$。

3.2　实体注册阶段

GUE与SAT在相互验证各自身份合法性前，都需要在NCC上进行注册以获得后续双向认证的资格。实体注册阶段流程如图2所示。

1) GUE或SAT→NCC

实体使用格上密码哈希函数将唯一身份标识符 $\mathrm{ID} \in \mathbb{Z}_q^m$ 映射为 $h_{\boldsymbol{\alpha}}(\mathrm{ID})$，同时生成注册请求符Request，并将注册请求消息 $\left(h_{\boldsymbol{\alpha}}(\mathrm{ID}),\mathrm{Request}\right)$ 发送给NCC，其中 $\boldsymbol{\alpha} \in \mathbb{Z}_q^m$。

2) NCC→GUE或SAT

由于实体是再次注册，当NCC收到注册请求消息后，可通过计算 $h_{\boldsymbol{\alpha}}(c\mathrm{ID}) \stackrel{?}{=} \mathrm{ch}_{\boldsymbol{\alpha}}(\mathrm{ID})$ 来验证消息的正确性，其中身份标识符是以 $\left((c,\mathrm{ID}),h_{\boldsymbol{\alpha}}(c\mathrm{ID})\right)$ 的形式存储在数据库中且 $c \in \mathbb{Z}_q$。若验证结果不正确，则拒绝该注册请求消息；若验证结果正确，则NCC使用格上哈希函数将唯一身份标识符 $\mathrm{Ncc} \in \mathbb{Z}_q^m$ 和实体身份ID共同映射为 $h_{\boldsymbol{\alpha}}(\mathrm{Ncc}+\mathrm{ID})$，同时生成注册响应符Response，并将注册响应消息 $\left(h_{\boldsymbol{\alpha}}(\mathrm{Ncc}+\mathrm{ID}),\mathrm{Ncc},\mathrm{Response}\right)$ 发给实体。

3) GUE或SAT

实体收到注册响应消息后，同样使用格上哈希函数映射NCC的身份标识符得到 $h_{\boldsymbol{\alpha}}(\mathrm{Ncc})$，再通过计算 $h_{\boldsymbol{\alpha}}(\mathrm{Ncc}+\mathrm{ID}) \stackrel{?}{=} h_{\boldsymbol{\alpha}}(\mathrm{Ncc})+h_{\boldsymbol{\alpha}}(\mathrm{ID})$ 验证消息的正确性，若验证结果不正确，则拒绝该注册响应消息；若验证结果正确，则表示GUE和SAT注册成功。

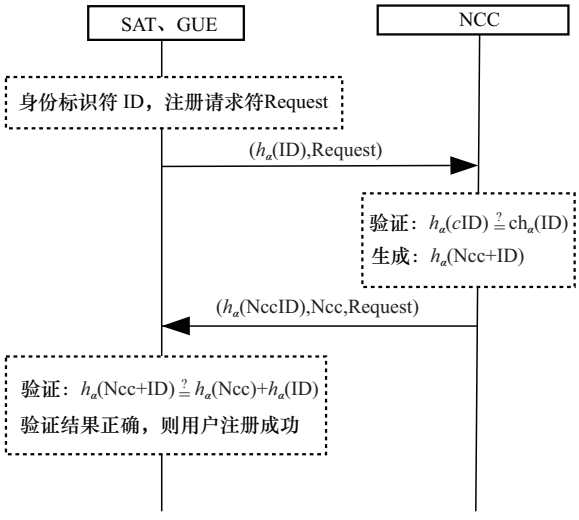


图2　实体注册阶段流程

3.3　实体双向认证和密钥协商阶段

SAT收到GUE发送的认证请求消息后，不仅需要验证GUE的合法性还需要生成卫星侧的会话密钥。当SAT返回认证响应消息给GUE后，GUE同样需要验证SAT的合法性并生成地面侧的会话密钥。实体双向认证和密钥协商阶段的流程如图3所示。

1) GUE生成认证请求消息并发给SAT

首先，GUE对自身 $\mathrm{ID}_{\mathrm{GUE}}$ 进行哈希运算生成 $\boldsymbol{H}(\mathrm{ID}_{\mathrm{GUE}}) \in \{0,1\}^k$，并将 $\boldsymbol{H}(\mathrm{ID}_{\mathrm{GUE}})$ 划分为 k 个子向量 $\boldsymbol{H}(\mathrm{ID}_{\mathrm{GUE}})=(h_1,h_2,\cdots,h_k)$，其中 $h(i)$ 为第 i 个分量。GUE利用 $h(i)$ 的值决定是否选择矩阵 $\boldsymbol{A}_i$：若 $h_i=1$ 则选 $\boldsymbol{A}_i, i=1,2,\cdots,k$，若 $h_i=0$ 则放弃选择矩阵 $\boldsymbol{A}_i$。因此，一共选择了 k^* 个矩阵 $\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_j, j=1,2,\cdots,k^*$。其次，将 $\boldsymbol{A}_0$ 和 k^* 个矩阵级联得到一个新的矩阵 $\boldsymbol{A}_{\mathrm{GUE}}=\boldsymbol{A}_0\|\boldsymbol{A}_1\|\boldsymbol{A}_2\|\cdots\|\boldsymbol{A}_j$，再从高斯分布 D_s^m 中随机选取 k^* 个整数向量 $\boldsymbol{v}_1,\boldsymbol{v}_2,\cdots,\boldsymbol{v}_j, \|\boldsymbol{v}_j\| \leqslant s\sqrt{m}, j=1,2,\cdots,k^*$，其中 $k^*=\dfrac{k}{2}$，同时计算 $\sum \boldsymbol{A}_j\boldsymbol{v}_j \pmod q$。接着，采用原像抽样算法生成部分签名消息 $\boldsymbol{v}_0 \leftarrow \mathrm{Samplepre}\left(\boldsymbol{T}_{\boldsymbol{A}_0},s,-\sum \boldsymbol{A}_j\boldsymbol{v}_j \pmod q,\boldsymbol{A}_0\right)$，并令签名消息 $\boldsymbol{v}_{\mathrm{GUE}}=(\boldsymbol{v}_0\|\boldsymbol{v}_1\|\cdots\|\boldsymbol{v}_j)$，会话密钥参数 $\boldsymbol{e}_{\mathrm{GUE}} \in \mathbb{Z}_q^n$。最后，GUE构造认证请求消息 $\left(\boldsymbol{e}_{\mathrm{GUE}},\boldsymbol{H}(\mathrm{ID}_{\mathrm{GUE}}),\boldsymbol{v}_{\mathrm{GUE}},t_1\right)$ 发送给SAT，其中 t_1 为当前认证请求消息的时间戳。

2) SAT生成会话密钥并将认证响应消息发给GUE

首先，SAT接收认证请求消息之后记录下时间戳 t_2，对时间戳 t_1 进行验证，计算 $t_2-t_1<\Delta t$ 是否满足，其中 Δt 表示系统允许的最大时间。若不满足，则丢弃该认证请求消息；若满足，则SAT通过 $\boldsymbol{H}(\mathrm{ID}_{\mathrm{GUE}})$ 构建级联矩阵 $\boldsymbol{A}_{\mathrm{GUE}}=\boldsymbol{A}_0\|\boldsymbol{A}_1\|\boldsymbol{A}_2\|\cdots\|\boldsymbol{A}_j$，同时计算 $\|\boldsymbol{v}_{\mathrm{GUE}}\| \leqslant s\sqrt{(k^*+1)m}$ 和 $\boldsymbol{A}_{\mathrm{GUE}}\boldsymbol{v}_{\mathrm{GUE}} \stackrel{?}{=} 0 \pmod q$ 来验证认证请求消息的正确性，完成对GUE身份的合法性检验。其次，验证通过后，SAT采用原像抽样算法生成签名消息 $\boldsymbol{w}_0 \leftarrow \mathrm{Samplepre}(\boldsymbol{T}_{\boldsymbol{A}_0},s,\boldsymbol{A}_0)$，令会话密钥参数 $\boldsymbol{e}_{\mathrm{SAT}} \in \mathbb{Z}_q^n$。接着，SAT利用上述参数生成卫星侧会话密钥，计算如下：$\mathrm{SK}_{\mathrm{SAT}}=h_{\boldsymbol{\alpha}}(\mathrm{Ncc})\boldsymbol{e}_{\mathrm{GUE}}\boldsymbol{e}_{\mathrm{SAT}}$。最后，SAT构造认证响应消息 $\left(\boldsymbol{e}_{\mathrm{SAT}},\boldsymbol{w}_0,t_3,H_1(\mathrm{SK}_{\mathrm{SAT}})\right)$ 发送给GUE，其中 t_3 为当前时间戳。

3) GUE接收认证请求响应消息并生成会话密钥

GUE接收认证响应消息之后首先记录下时间戳 t_4，然后对时间戳 t_3 进行验证，计算 $t_4-t_3<\Delta t$

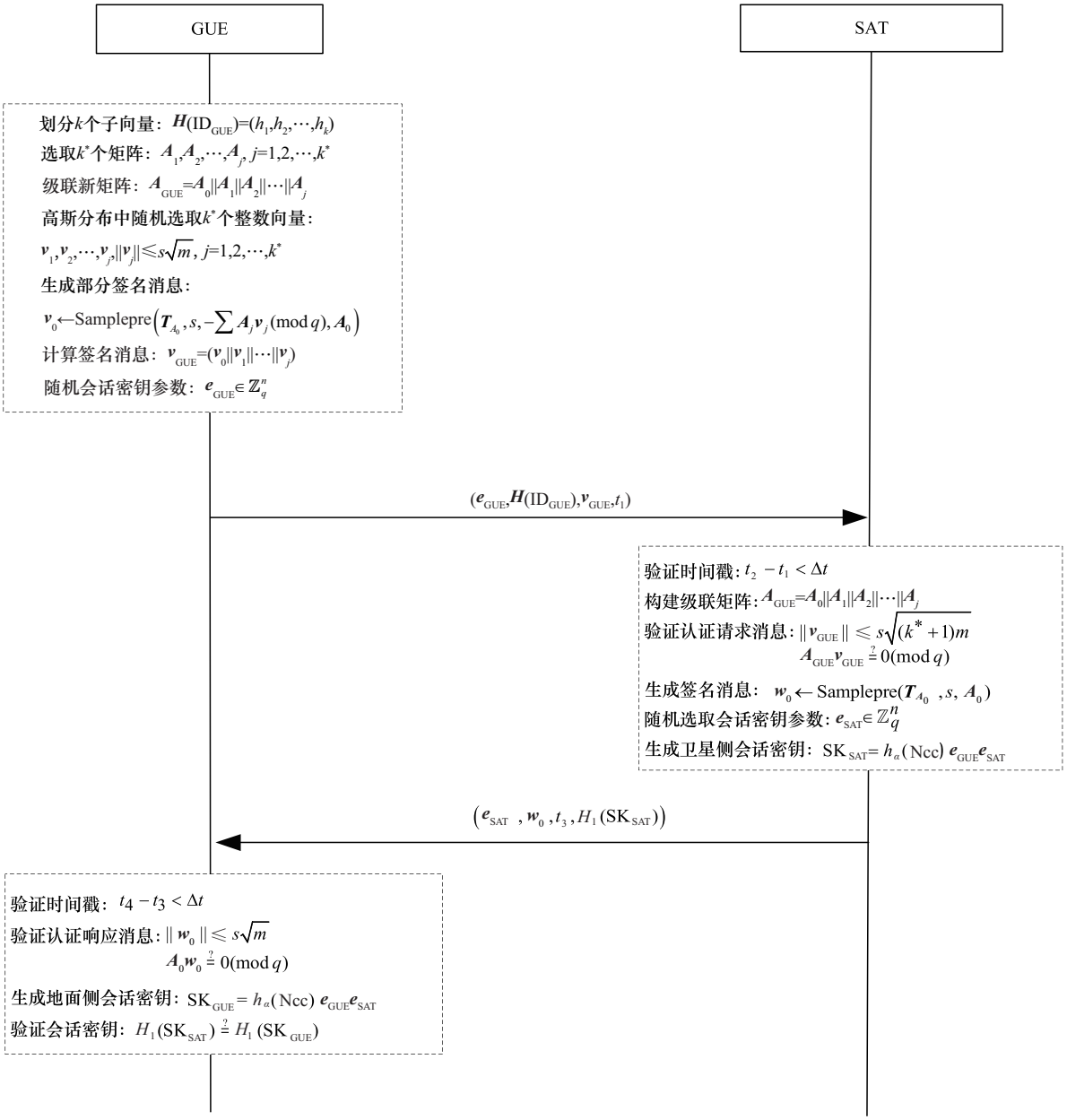


图3　实体双向认证和密钥协商阶段的流程

是否满足，其中Δt表示系统允许的最大时间。若不满足，则丢弃该认证响应消息；若满足，则GUE通过计算$\|\boldsymbol{w}_0\|\leqslant s\sqrt{m}$和$\boldsymbol{A}_0\boldsymbol{w}_0\stackrel{?}{=}0(\mathrm{mod}\,q)$来验证认证响应消息的正确性，完成对SAT身份的合法性检验。其次，验证通过后，GUE利用会话密钥参数生成地面侧的会话密钥，计算如下：$\mathrm{SK}_{\mathrm{GUE}}=h_\alpha(\mathrm{Ncc})\boldsymbol{e}_{\mathrm{GUE}}\boldsymbol{e}_{\mathrm{SAT}}$。最后，GUE验证$H_1(\mathrm{SK}_{\mathrm{SAT}})\stackrel{?}{=}H_1(\mathrm{SK}_{\mathrm{GUE}})$是否成立。如果成立，则会话密钥协商成功；如果不成立，则会话密钥协商失败。

4　正确性分析与安全性证明

4.1　正确性分析

对GUE而言，原像抽样算法输出的向量$\boldsymbol{v}_0$，其近似服从高斯分布且$\boldsymbol{A}_0\boldsymbol{v}_0=-\sum\boldsymbol{A}_j\boldsymbol{v}_j(\mathrm{mod}\,q)$，即$\boldsymbol{A}_{\mathrm{GUE}}\boldsymbol{v}_{\mathrm{GUE}}=0(\mathrm{mod}\,q)$。由于$\|\boldsymbol{v}_0\|\leqslant s\sqrt{m}$以至少$1-2^{-n}$的概率成立，且$\|\boldsymbol{v}_j\|\leqslant s\sqrt{m},j=1,2,\cdots,k^*$，则$\|\boldsymbol{v}_{\mathrm{GUE}}\|\leqslant s\sqrt{(k^*+1)m}$。因此，一个合法的GUE签名以极大概率被SAT所接受。同样的，对SAT而言，向量$\boldsymbol{w}_0$作为原像抽样算法的输出，其近似服

从高斯分布且$\boldsymbol{A}_0\boldsymbol{w}_0 = 0(\bmod q)$，$\|\boldsymbol{w}_0\| \leqslant s\sqrt{m}$以至少$1-2^{-n}$的概率成立。因此，一个合法的SAT签名以极大概率被GUE所接受。

4.2 安全性证明：存在不可伪造性

定理1 假设存在概率多项式时间的静态选择消息攻击者A经过Q次签名询问后能够以不可忽略概率$\mathrm{Adv}_{\mathrm{SIG}}(A)-\mathrm{negl}(n)$伪造一个合法签名，则可构造一个算法$F$以近似概率$\dfrac{\mathrm{Adv}_{\mathrm{SIG}}(A)}{kQ}-\mathrm{negl}(n)$解决SIS问题，其中$k$是哈希函数$H$的输出长度。

证明 假设算法F得到一个SIS问题的实例如$\left(\overline{\boldsymbol{A}_{\mathrm{GUE}}},s,(k+1)m,q\right)$，其中$s$是高斯参数，$q$为质数，$\overline{\boldsymbol{A}_{\mathrm{GUE}}} = \overline{\boldsymbol{A}_0}\|\overline{\boldsymbol{A}_1}\|\overline{\boldsymbol{A}_2}\|\cdots\|\overline{\boldsymbol{A}_j},\overline{\boldsymbol{A}_j} \in \mathbb{Z}_q^{n\times m},j = 0,1,\cdots,k$。$F$希望得到一个范数小于或等于$2s\sqrt{(k+1)m}$的向量$\boldsymbol{v}_{\mathrm{GUE}}$满足$\overline{\boldsymbol{A}_{\mathrm{GUE}}}\boldsymbol{v}_{\mathrm{GUE}} = 0(\bmod q)$。为此，算法$F$充当模拟者求解SIS问题。

假设消息攻击者A已经获得Q个真实的Hash值$h_1,h_2,\cdots,h_Q \in \{0,1\}^k$，$F$计算比特串$p$的集合$P$，其中$p$取不是$h_1,h_2,\cdots,h_Q$前缀中的最小字符串。由于$|p| \leqslant k$，每个$h_i$最多有$k$个值，因此，在多项式时间内集合$P$中至多有$kQ$个值。算法$F$在$P$中任意选取一个$p$，设$p$中一共有$c$个位置为1，分别用$c_1,c_2,\cdots,c_c$表示1的位置，则算法$F$执行以下操作生成系统公钥。

1)控制生长：随机抽取$|p|-c$个陷门格$\Lambda_q^{\perp}(\boldsymbol{B}_i)$及其格基$\boldsymbol{T}_i \in \mathbb{Z}_q^{m\times m}$，其中$\boldsymbol{B}_i \in \mathbb{Z}_q^{n\times m}$，$i<|p|$且$i \neq t_l,l = 1,2,\cdots,c$，并令$\boldsymbol{A} = \overline{\boldsymbol{A}_0}$。

2)非控制生长：当$j<|p|$时，令$\boldsymbol{A}_{c_j} = \overline{\boldsymbol{A}_{c_j}}$，其中$0<c_1,c_2,\cdots,c_c<|p|$且$p_{c_j} = 1$。其他位置按照下标顺序依次定义$\boldsymbol{A}_i = \boldsymbol{B}_i$。当$j>|p|$时，依次令$\boldsymbol{A}_j = \overline{\boldsymbol{A}_j}$。

因此，可得到公钥为$\boldsymbol{A},\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_k$，算法$F$将公钥以及公共参数$n,m,q,s,k$一起发送给攻击者A并开始进行询问应答游戏。同时，算法F维护列表L用于记录签名询问的回答。

签名询问：对哈希值为$h_1,h_2,\cdots,h_Q$进行询问时，算法F首先查看列表L，如果在表中找到h_i，则返回相应的记录$\boldsymbol{v}_i$，否则，算法F生成签名。

由于p不是h_i的前缀，且h_i的输出具有随机性，可在前$|p|$个位置中除去$c_1,c_2,\cdots,c_c$，但这些位置仍然存在结果为1的值（概率为$1-\dfrac{1}{2^{|p|-c}}$），设该位置为c'，则c'对应公钥为$\boldsymbol{A}_{c'} = \boldsymbol{B}_{c'}$，算法$F$掌握了陷门$\Lambda_q^{\perp}(\boldsymbol{B}_{c'})$的格基，并借助$\Lambda_q^{\perp}(\boldsymbol{B}_{c'})$的格基生成消息的签名$\boldsymbol{v}_i$。算法$F$发送$\boldsymbol{v}_i$给攻击者A，同时将$(\boldsymbol{v}_i,h_i)$存入列表$L$。

在攻击者A完成Q次签名询问后，攻击者A以概率$\mathrm{Adv}_{\mathrm{SIG}}^{\text{eu-scma}}(\mathrm{A})-\mathrm{negl}(n)$输出一个新哈希值$\overline{h}$的伪造签名$\boldsymbol{v}^*$，满足$\boldsymbol{A}_{\overline{h}}\boldsymbol{v}^* = 0(\bmod q)$和$\|\boldsymbol{v}^*\| \leqslant s\sqrt{(j^*+1)m}$，其中$\mathrm{Adv}_{\mathrm{SIG}}^{\text{eu-scma}}(\mathrm{A})$为攻击者A成功伪造签名的概率，$\mathrm{negl}(n)$为可忽略函数，$j^*$是$\overline{h}$的汉明重量，矩阵$\boldsymbol{A}_{\overline{h}}$的含义同上述签名算法。算法$F$检查$p$是不是$\overline{h}$的前缀，如果不是，则算法$F$终止并宣布失败。否则，$p$是$\overline{h}$的前缀，则矩阵$\boldsymbol{A}_{\overline{h}}$是由$\overline{\boldsymbol{A}_0},\overline{\boldsymbol{A}_{t_1}},\cdots,\overline{\boldsymbol{A}_{t_t}},\overline{\boldsymbol{A}_{|p|}},\overline{\boldsymbol{A}_{|p|+1}},\cdots,\overline{\boldsymbol{A}_k}$这些矩阵中的部分矩阵是级联而成的。根据矩阵$\boldsymbol{A}_{\overline{h}}$和$\overline{\boldsymbol{A}_{\mathrm{GUE}}}$之间的关系，算法F可以在相应位置级联矩阵将$\boldsymbol{A}_{\overline{h}}$变为$\overline{\boldsymbol{A}_{\mathrm{GUE}}}$。同时，向量$\boldsymbol{v}^*$向上级联0向量有$\overline{\boldsymbol{v}^*}$，可得出$\|\overline{\boldsymbol{v}^*}\| = s\sqrt{(j^*+1)}\,m \leqslant s\sqrt{(k+1)m}$以及$\overline{\boldsymbol{A}_{\mathrm{GUE}}}\overline{\boldsymbol{v}^*} = 0(\bmod q)$，从而算法$F$得到SIS实例的一个合法解。

算法F伪造的公钥矩阵以不可忽略概率接近均匀，其签名分布与实际攻击中的分布完全相同，因此算法F是否伪造成功仅仅取决于比特串p是不是$\overline{h}$的前缀。又由于算法F输出有效的伪造概率为$\mathrm{Adv}_{\mathrm{SIG}}(A)-\mathrm{negl}(n)$，随机选择的字符串$p \in P$接近于均匀分布。可推出，$p$是$\overline{h}$前缀的概率至少为$\dfrac{1}{kQ}-\mathrm{negl}(n)$，则算法$F$成功的概率接近为$\dfrac{\mathrm{Adv}_{\mathrm{SIG}}(A)}{kQ}-\mathrm{negl}(n)$。在此事件中，构造的$\overline{\boldsymbol{A}_{\mathrm{GUE}}}\overline{\boldsymbol{v}^*} = 0(\bmod q)$且$\|\overline{\boldsymbol{v}^*}\| \leqslant s\sqrt{(k+1)m}$中的$\overline{\boldsymbol{v}^*}$是给定SIS实例的有效解决方案。证毕。

4.3 安全性证明：基于信念的模态逻辑（BAN）证明

在本节中，基于BAN逻辑的形式化分析方法来确保GUE和SAT之间相互认证的安全性以及会话密钥的一致性。在认证过程中所涉及的消息可以简化如下。

认证请求消息

$$\mathrm{GUE}\rightarrow\mathrm{SAT}:\left(\boldsymbol{e}_{\mathrm{GUE}},\boldsymbol{H}(\mathrm{ID}_{\mathrm{GUE}}),\boldsymbol{v}_{\mathrm{GUE}}\right)$$

认证响应消息

$$\mathrm{SAT}\rightarrow\mathrm{GUE}:\left(\boldsymbol{e}_{\mathrm{SAT}},\boldsymbol{w}_0,H_1\left(\mathrm{SK}_{\mathrm{SAT}}\right)\right)$$

会话密钥分别在GUE端和SAT端

$$\mathrm{SK}_{\mathrm{GUE}},\mathrm{SK}_{\mathrm{SAT}}$$

为了验证实体身份的合法性和会话密钥的正确性，还需证明以下安全目标。

$$G_1: SAT| \equiv \left(\boldsymbol{e}_{GUE},\boldsymbol{H}(ID_{GUE}),\boldsymbol{v}_{GUE}\right)$$

$$G_2: ID_{GUE}| \equiv \left(\boldsymbol{e}_{SAT},\boldsymbol{w}_0,H_1\left(SK_{SAT}\right)\right)$$

$$G_3: ID_{GUE}| \equiv ID_{GUE} \overset{SK_{GUE}}{\leftrightarrow} SAT$$

$$G_4: SAT| \equiv SAT \overset{SK_{SAT}}{\leftrightarrow} ID_{GUE}$$

为实现上述目标还需要做出如下假设。

$$A_1: SAT| \equiv ID_{GUE}| \Rightarrow \left(\boldsymbol{e}_{GUE},\boldsymbol{H}(ID_{GUE}),\boldsymbol{v}_{GUE}\right)$$

$$A_2: ID_{GUE}| \equiv SAT| \Rightarrow \left(\boldsymbol{e}_{SAT},\boldsymbol{w}_0,H_1\left(SK_{SAT}\right)\right)$$

接着将基于BAN逻辑的假设和规则，详细说明轻量化后量子认证方案是如何实现安全目标的。

1)通过认证请求消息得

$$SAT \lhd \left(\boldsymbol{e}_{GUE},\boldsymbol{H}(ID_{GUE}),\boldsymbol{v}_{GUE}\right)$$

2)由于$\boldsymbol{e}_{GUE},\boldsymbol{v}_{GUE}$都带有随机性因子，有

$$SAT| \equiv \#\left(\boldsymbol{e}_{GUE},\boldsymbol{H}(ID_{GUE}),\boldsymbol{v}_{GUE}\right)$$

3)SAT通过验证GUE发送的认证请求消息来验证GUE的合法性，若验证通过有

$$SAT| \equiv ID_{GUE}| \sim \left(\boldsymbol{e}_{GUE},\boldsymbol{H}(ID_{GUE}),\boldsymbol{v}_{GUE}\right)$$

4)由临时值验证规则$\dfrac{P| \equiv \#(X),P| \equiv Q| \sim X}{P| \equiv Q| \equiv X}$，有

$$SAT| \equiv ID_{GUE}| \equiv \left(\boldsymbol{e}_{GUE},\boldsymbol{H}(ID_{GUE}),\boldsymbol{v}_{GUE}\right)$$

5)由$|A_1$与仲裁规则$\dfrac{P| \equiv \Rightarrow (X),P| \equiv Q| \equiv X}{P| \equiv X}$，可得$SAT| \equiv \left(\boldsymbol{e}_{GUE},\boldsymbol{H}(ID_{GUE}),\boldsymbol{v}_{GUE}\right)$，满足目标1。

6)由认证响应消息得

$$ID_{GUE} \lhd \left(\boldsymbol{e}_{SAT},\boldsymbol{w}_0,H_1\left(SK_{SAT}\right)\right)$$

7)$\boldsymbol{w}_0$由原像抽样算法得出具有统计均匀的特性，且$\boldsymbol{e}_{SAT}$和$H_1\left(SK_{SAT}\right)$具有随机性，所以

$$ID_{GUE}| \equiv \#\left(\boldsymbol{e}_{SAT},\boldsymbol{w}_0,H_1\left(SK_{SAT}\right)\right)$$

8)GUE通过验证SAT发送的认证响应消息来验证目标卫星的合法性，若验证通过

$$ID_{GUE}| \equiv SAT| \sim \left(\boldsymbol{e}_{SAT},\boldsymbol{w}_0,H_1\left(SK_{SAT}\right)\right)$$

9)由临时值验证规则$\dfrac{P| \equiv \#(X),P| \equiv Q| \sim X}{P| \equiv Q| \equiv X}$，有

$$ID_{GUE}| \equiv SAT| \equiv \left(\boldsymbol{e}_{SAT},\boldsymbol{w}_0,H_1\left(SK_{SAT}\right)\right)$$

10)结合假设A_2与仲裁规则$\dfrac{P| \equiv \Rightarrow (X),P| \equiv Q| \equiv X}{P| \equiv X}$，$ID_{GUE}| \equiv \left(\boldsymbol{e}_{SAT},\boldsymbol{w}_0,H_1\left(SK_{SAT}\right)\right)$，满足目标2。

11)由于$\boldsymbol{e}_{SAT},\boldsymbol{e}_{GUE} \in \mathbb{Z}_q^n$是随机选择的，因此$ID_{GUE}| \equiv \#(\boldsymbol{e}_{SAT}\boldsymbol{e}_{GUE})$。

12)由新鲜性原则$\dfrac{P| \equiv \#(X)}{P| \equiv \#(X,Y)}$可得$ID_{GUE}| \equiv \#\left(h_\alpha(Ncc)(\boldsymbol{e}_{SAT},\boldsymbol{e}_{GUE})\right)$，其中$h_\alpha(Ncc)$在注册阶段获得。

13)最后得出$ID_{GUE}| \equiv \#(SK_{GUE})$。

14)由步骤8)和会话密钥规则$\dfrac{P| \equiv \#(k),P| \equiv Q| \sim X}{P| \equiv P \overset{k}{\leftrightarrow} Q}$可得$ID_{GUE}| \equiv ID_{GUE} \overset{SK_{GUE}}{\leftrightarrow} SAT$，目标3得证。

15)相同地，有

$$SAT| \equiv \#\left(h_\alpha(Ncc)(\boldsymbol{e}_{SAT},\boldsymbol{e}_{GUE})\right) = \#(SK_{SAT})$$

16)由步骤3)和会话密钥规则$\dfrac{P| \equiv \#(k),P| \equiv Q| \sim X}{P| \equiv P \overset{k}{\leftrightarrow} Q}$可得$SAT| \equiv SAT \overset{SK_{SAT}}{\leftrightarrow} ID_{GUE}$，目标4得证。

根据步骤5)、步骤10)、步骤14)和步骤16)，所有目标均证明结束。

4.4　形式化安全性证明

本节将详细分析基于格的卫星网络轻量化接入认证方案满足的几种安全需求，具体如下。

1)双向认证：双向认证主要是在SAT和GUE之间实现。一方面，SAT通过检验认证请求消息的正确性来验证地面用户身份的合法性。首先，SAT验证认证请求消息中的时间戳t_1，接着计算$\|\boldsymbol{v}_{GUE}\| \leqslant s\sqrt{(k^*+1)m}$和$\boldsymbol{A}_{GUE}\boldsymbol{v}_{GUE} \overset{?}{=} 0(\mathrm{mod}\,q)$，验证通过盆景树算法得到签名消息$\boldsymbol{v}_{GUE}$。若验证成功，则GUE身份合法。另一方面，GUE通过检验认证响应消息的正确性来验证SAT身份的合法性。首先，GUE验证认证请求消息中的时间戳t_3，接着计算$\|\boldsymbol{w}_0\| \leqslant s\sqrt{m}$和$\boldsymbol{A}_0\boldsymbol{w}_0 \overset{?}{=} 0(\mathrm{mod}\,q)$，验证通过原像抽样函数得到的签名消息$\boldsymbol{w}_0$。若满足，则目标卫星身份合法。

2)密钥协商：$h_\alpha(Ncc)$在注册阶段获得，是NCC的唯一身份标识符。$\boldsymbol{e}_{GUE}$和$\boldsymbol{e}_{SAT}$是GUE和SAT在本地生成的随机向量，可分别通过这些参数生成会话密钥$SK_{SAT} = h_\alpha(Ncc)\boldsymbol{e}_{SAT}\boldsymbol{e}_{GUE}$以及$SK_{GUE} = h_\alpha(Ncc)\boldsymbol{e}_{SAT}\boldsymbol{e}_{GUE}$，完成密钥的协商。

3)抗量子计算攻击：基于格的卫星网络轻量化接入认证方案主要分为注册阶段和认证阶段。在注

册阶段，该方案基于近似SVP问题的格密码哈希函数完成卫星和地面用户的身份注册，其中近似SVP问题可规约到SIS问题中[19]；在认证阶段，该方案基于盆景树算法生成签名消息并完成身份验证。根据该方案的安全性分析可知，该认证算法的不可伪造性同样基于SIS问题[8,21]。一般认为，SIS问题目前不能用任何多项式时间算法来解决。因此，该方案整体是可以抵御量子计算攻击的。

4)防恶意实体攻击：该方案在交互消息中添加了时间戳来抵御重放攻击，通过实体间的相互认证抵御身份篡改和中间人攻击，而且只有合法的SAT和GUE生成的交互消息才可成功被通信方验证，所以攻击者无法伪造合法的消息。

5)密钥前后向安全性：为了保障认证后的通信安全，需要使用会话密钥对交互数据进行加密，再将加密后的通信内容传输到网络中。会话密钥由h_a(Ncc)、$\boldsymbol{e}_{\mathrm{GUE}}$和$\boldsymbol{e}_{\mathrm{SAT}}$组成，攻击者可以在网络中获取NCC的唯一身份标识符，但是却很难获取$\boldsymbol{e}_{\mathrm{GUE}}$和$\boldsymbol{e}_{\mathrm{SAT}}$，因为$\boldsymbol{e}_{\mathrm{GUE}}$和$\boldsymbol{e}_{\mathrm{SAT}}$均是地面用户和卫星在本地随机生成，每一次会话后便丢弃当前密钥生成新的会话密钥开始下一轮的数据传输。因此，会话密钥具有前后向安全性。

6)实体隐私信息保护：由于实体采用的是基于格密码的哈希函数而不是真实身份完成注册，因此实体的身份信息得到保护，且身份信息不可伪造。另外，网络中只有NCC知道实体的真实身份，因此该方案还具有恶意实体追踪的功能。

5　性能仿真与分析

本节分3个方面与文献[3-4,8-9]进行对比，进而分析本文所提方案的性能，并给出仿真结果，其中文献[3-4]方案基于椭圆曲线的离散对数问题来提供安全性保障，文献[8-9]方案使用格密码中的SIS问题来保证认证方案的安全性。为了更方便地显示实验结果，所有方案均在3.4 GHz Intel Core i7-6700处理器和8 GB RAM的台式计算机上使用LatticeCrypto库来模拟方案中涉及的密码操作，其中$R_q=\dfrac{\mathbb{Z}_q[x]}{x^n+1}$，椭圆曲线为$y^2=x^3-x$，同时在给定安全参数$k=8$的情况下，设$q=k^2$，$m=n=k\log q$以保证SIS问题难度的成立[14,18]。假设低轨道地球卫星与地面的距离约为1 500 km，单条交互消息的往返时延约为10 ms，同时令卫星下行速度为5 Mbit/s，上行速度为200 kbit/s。接着在VS2022上分别创建卫星模块和地面用户模块，并通过前述的认证方案进行参数交互。当卫星或用户收到认证参数后，分别调用LatticeCrypto库模拟密码算法。

5.1　计算时间对比

本节将本文所提方案与其他相关方案在计算时间方面进行比较。表2中给出了所有认证方案中需要使用的各种密码符号和定义以及各个操作的具体时间。

表2　　密码符号定义及操作时间

参数	时间/ms
抽样函数T_{ge}	7.177 47
哈希函数T_{h}	3.5
格中乘加操作T_{lma}	31.360 55
格中标乘操作T_{lsmul}	29.278
格中乘操作T_{lpma}	37.174
椭圆曲线中乘操作T_{mul}	0.063 2
椭圆曲线中点加操作T_{pa}	0.000 3

在计算时间时，方案中不包括串联和异或的运算时间，因为这2个操作都占用很少的执行时间。本文所提方案中的计算时间主要由注册阶段和认证阶段2个阶段的计算时间组成，2个阶段的计算时间如表3和表4所示，下面将分别对表3和表4进行分析。

表3　　注册阶段计算时间

方案	地面用户	低轨道地球卫星	NCC	总时间/ms
文献[3]	—	—	$4T_{\mathrm{mul}}+3T_{\mathrm{h}}$	10.752 8
文献[4]	$2T_{\mathrm{mul}}+2T_{\mathrm{h}}$	$2T_{\mathrm{mul}}+2T_{\mathrm{h}}$	$T_{\mathrm{pa}}+2T_{\mathrm{h}}$	21.253 1
文献[8]	—	—	$T_{\mathrm{h}}+T_{\mathrm{ge}}+T_{\mathrm{lpma}}$	47.851 47
文献[9]	$T_{\mathrm{lma}}+T_{\mathrm{lpma}}+2T_{\mathrm{h}}$	$T_{\mathrm{lma}}+T_{\mathrm{lpma}}+2T_{\mathrm{h}}$	$T_{\mathrm{lpma}}+2T_{\mathrm{h}}$	195.243 1
本文	$2T_{\mathrm{h}}$	$2T_{\mathrm{h}}$	T_{h}	17.5

表 4　　**认证阶段计算时间**

方案	地面用户	低轨道地球卫星	NCC	总时间/ms
文献[3]	$5T_{\text{mul}} + 2T_{\text{pa}} + 4T_{\text{h}}$	$4T_{\text{mul}} + 2T_{\text{pa}} + 4T_{\text{h}}$	—	28.57
文献[4]	$2T_{\text{mul}} + 6T_{\text{h}} + 2T_{\text{pa}}$	$2T_{\text{mul}} + 6T_{\text{h}} + 2T_{\text{pa}}$	—	42.254
文献[8]	$3T_{\text{h}} + T_{\text{lsmul}} + 2T_{\text{lma}} + T_{\text{lpma}}$	$T_{\text{h}} + T_{\text{lpma}} + T_{\text{lma}}$	—	211.707 65
文献[9]	$T_{\text{lma}} + 4T_{\text{h}} + T_{\text{ge}}$	$T_{\text{lpma}} + 3T_{\text{h}}$	—	100.212 02
本文	$2T_{\text{h}} + T_{\text{ge}} + T_{\text{lsmul}}$	$T_{\text{h}} + T_{\text{ge}} + T_{\text{lsmul}}$	—	83.410 94

表3中，地面用户和低轨道地球卫星使用格上哈希函数映射身份标识符得到$h_{\alpha}(\text{ID})$，同时验证NCC返回的注册响应消息$\left(h_{\alpha}(\text{Ncc} + \text{ID}),\text{Ncc},\text{Responce}\right)$的正确性。NCC同样需验证实体发送的注册请求消息$\left(h_{\alpha}(c\text{ID}),\text{Request}\right)$的正确性，并生成响应消息发给实体。因此，注册阶段的计算时间为$5T_{\text{h}}$，约17.5 ms。本文使用相同的方法计算了其他认证方案在注册阶段的计算时间。对于文献[3,8]，地面用户和卫星只需向NCC发送身份信息，并且大多数密码操作都放在了NCC上，因此，注册阶段的计算时间分别为$4T_{\text{mul}} + 3T_{\text{h}}$和$T_{\text{h}} + T_{\text{ge}} + T_{\text{lpma}}$，约为10.752 8 ms和47.851 47 ms。与本文所提方案的注册流程类似，文献[4,9]中的实体都需要在NCC上完成身份注册，因此，注册阶段的计算时间分别为$4T_{\text{lpma mul}} + 6T_{\text{lpma h}} + T_{\text{lpma pa}}$和$3T_{\text{lpma lma}} + 2T_{\text{lpma lpma}} + 6T_{\text{lpma h}}$，约为21.253 1 ms和195.243 1 ms。由于本文所提方案中的卫星和地面用户除了发送身份信息外，还需要发送注册参数等，从而需要较多的时间完成注册。同时，本文所提方案基于格密码完成身份注册，且具有恶意实体追踪功能，在注册阶段的安全性高于其他使用普通哈希函数的文献[3-4]方案，与同样基于格的文献[8-9]方案相比分别缩短了约30 ms和177 ms。

表4中，本文所提方案的认证阶段由盆景树算法和原像抽样算法组成。地面用户首先将哈希后的身份向量$\boldsymbol{H}(\text{ID}_{\text{GUE}})$分成$k$个子向量，其值的大小作为随机矩阵的选取规则。接着使用原像抽样算法$\boldsymbol{v}_0 \leftarrow \text{Samplepre}\left(\boldsymbol{T}_{\boldsymbol{A}_0},s,-\sum \boldsymbol{A}_j\boldsymbol{v}_j \ (\text{mod}\, q),\boldsymbol{A}_0\right)$得到地面用户的签名消息，并传输给卫星。卫星收到消息后，通过计算$\boldsymbol{A}_{\text{GUE}}\boldsymbol{v}_{\text{GUE}} \overset{?}{=} 0(\text{mod}\, q)$来验证认证请求消息的正确性，完成对地面用户身份的合法性检验。然后，卫星同样使用原像抽样算法$\boldsymbol{w}_0 \leftarrow \text{Samplepre}(\boldsymbol{T}_{\boldsymbol{A}_0},s,\boldsymbol{A}_0)$得到卫星的签名消息，并生成认证响应消息传输给用户。最后用户通过计算$\boldsymbol{A}_0\boldsymbol{w}_0 \overset{?}{=} 0(\text{mod}\, q)$来验证消息的正确性，完成对卫星身份的合法性检验，同时计算$H_1(\text{SK}_{\text{SAT}}) \overset{?}{=} H_1(\text{SK}_{\text{GUE}})$验证会话密钥的正确性。因此，认证阶段的计算时间为$3T_{\text{h}} + 2T_{\text{ge}} + 2T_{\text{lsmul}}$，约83.410 94 ms。随后使用相同的方法计算其他方案在认证阶段的计算时间。文献[3-4]方案基于椭圆曲线密码实现地面用户和卫星的双向认证，分别得到计算时间$9T_{\text{mul}} + 4T_{\text{pa}} + 8T_{\text{h}}$和$4T_{\text{mul}} + 12T_{\text{h}} + 4T_{\text{pa}}$，约为28.57 ms和42.254 ms。文献[8-9]方案基于格密码完成对地面用户和卫星各自的身份认证，得到计算时间$4T_{\text{h}} + T_{\text{lsmul}} + 2T_{\text{lpma}} + 3T_{\text{lma}}$、$T_{\text{lma}} + 7T_{\text{h}} + T_{\text{ge}} + T_{\text{lpma}}$，约为211.707 65 ms和100.212 02 ms。由于文献[3-4]中的方案在椭圆曲线上使用点乘或点加运算，计算复杂度低，而本文所提方案中多用了矩阵乘向量运算，在认证阶段的时间比文献[3-4]方案的更大。然而，本文基于格密码中的SIS问题实现相互认证，可以抵抗量子计算攻击。相比之下，文献[3-4]方案是基于椭圆曲线密码完成身份验证，不具备抵御量子计算攻击的功能。此外，文献[8-9]方案使用了高维运算解密消息，导致认证阶段的计算时间较长。本文所提方案考虑了卫星容量有限和处理能力低的缺点，简化了认证流程，卫星只需要验证地面用户的合法性和生成会话密钥，所以认证阶段的计算时间与文献[8-9]方案的相比分别缩短了约128 ms和17 ms。

5.2　认证时间对比

本节将本文所提方案与基于格的认证方案在总认证时间方面进行比较，其中总认证时间由计算时间、通信时延、传播时延组成。考虑文献[3-4]方案中的注册和认证算法由点乘和点加操作组成，通信时延可忽略不计，因此，本文与文献[8-9]方案在认证时间上进行对比分析。下面将介绍各方案

表5　　不同方案的通信时延对比

方案	注册阶段	认证阶段	大小/bit	通信时延/ms
文献[8]	(RID,PWD), (RID,PWD,$\boldsymbol{S}$)	($\mathbf{ANS}$,t,$\mathbf{sk}$),($\mathbf{ANS}$,T,M,$\boldsymbol{Z}$,$\mathbf{sig}$)	$(2+k)(m+n)\lvert q\rvert+7k$ $\approx 8k(2+k)\log^2 k+7k$	15.5
文献[9]	($\boldsymbol{C}_i$),($\boldsymbol{C}_N$)	($\boldsymbol{C}_i$,$\boldsymbol{e}_i$),($\mathbf{MA}\,\mathbf{C}_s$,$\boldsymbol{U}_G$,$\boldsymbol{M}_S$)	$[2mk+(m+1)(m+n+2)]\lvert q\rvert+(m+1)k\log 2+k\approx$ $16k^2\log^3 k+8\log^2 k(k^2+2k)+$ $2\log k(2+k^2\log 2)+k+k\log 2$	166.2
本文	$\left(h_\alpha(\mathrm{ID}),\mathrm{Request}\right)$, $\left(h_\alpha(\mathrm{Ncc}+\mathrm{ID}),\mathrm{Ncc},\mathrm{Responce}\right)$	$\left(\boldsymbol{e}_{\mathrm{GUE}},\boldsymbol{H}(\mathrm{ID}_{\mathrm{GUE}}),\boldsymbol{v}_{\mathrm{GUE}},t_1\right)$, $\left(\boldsymbol{e}_{\mathrm{SAT}},\boldsymbol{w}_0,t_3,H_1(\mathrm{SK}_{\mathrm{SAT}})\right)$	$7k+2+2n\lvert q\rvert+(\frac{k}{2}+2)m\lvert q\rvert$ $\approx 7k+2+2\log^2 k(k^2+8k)$	9.1

的总认证时间的实现细节。

由于地面用户距离NCC较近，且地面数据传输速率快，通信时延短，因此只考虑卫星上数据的传输。各方案的通信时延具体对比结果如表5所示。在注册阶段，卫星基于格密码的哈希函数生成注册请求消息$\left(h_\alpha(\mathrm{ID}),\mathrm{Request}\right)$发送给NCC，NCC则返回响应消息$\left(h_\alpha(\mathrm{Ncc}+\mathrm{ID}),\mathrm{Ncc},\mathrm{Responce}\right)$给卫星完成身份注册。在认证阶段中，卫星和地面用户基于盆景树算法和原像抽样算法生成认证请求消息$\left(\boldsymbol{e}_{\mathrm{GUE}},\boldsymbol{H}(\mathrm{ID}_{\mathrm{GUE}}),\boldsymbol{v}_{\mathrm{GUE}},t_1\right)$和认证响应消息$\left(\boldsymbol{e}_{\mathrm{SAT}},\boldsymbol{w}_0,t_3,H_1(\mathrm{SK}_{\mathrm{SAT}})\right)$，并通过验证消息的正确性实现实体间的双向认证，因此，利用公式通信数据量/通信速率=通信时延，得到本文的通信时延，约为9.1 ms。文献[8]的方案主要通过原像抽样算法和拒绝抽样算法生成通信数据(RID,PWD),(RID,PWD,$\boldsymbol{S}$),($\mathbf{ANS}$,T,M,$\boldsymbol{Z}$,$\mathbf{sig}$)、($\mathbf{ANS}$,t,$\mathbf{sk}$)完成认证参数的传递，因此，通信时延约为15.5 ms。文献[9]的方案利用Gentry加密机制生成交互消息($\boldsymbol{C}_i$),($\boldsymbol{C}_N$)、($\boldsymbol{C}_i$,$\boldsymbol{e}_i$)($\mathbf{MA}\,\mathbf{C}_s$,$\boldsymbol{U}_G$,$\boldsymbol{M}_S$)实现实体的身份认证，通信时延约为166.2 ms。

考虑星地链路长度远超于地面用户到NCC的距离，本文只考虑星地间的传播时延。具体时延如表6所示。结合注册阶段和认证阶段的通信时延、计算时间以及传播时延，可以得到各个方案总认证时间。图4展示的是当安全参数$k=8$时各方案的总认证时间。从图4中可以看出，与文献[8-9]方案相比，本文所提方案在注册阶段的计算时间缩短了173%，在认证阶段的计算时间缩短了20%，总认证时间缩短了150%。从图5可以看出，随着k值的增加，各个方案的通信开销逐渐变大，但本文所提方案的增长幅度要小于其他2个格密码认证方案，因此，本文不仅为通信实体提供了高安全低开销的快速认证，还提高了卫星上的资源利用率。

表6　　星地传播时延

方案	交互次数/次	传播时延/ms
文献[8]	4	20
文献[9]	4	20
本文	4	20

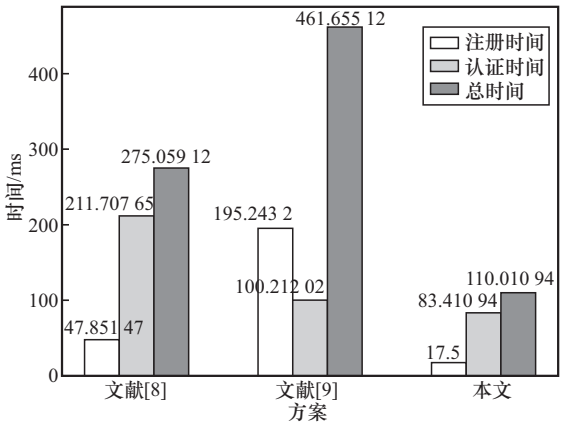


图4　当$k=8$时各个方案的总认证时间

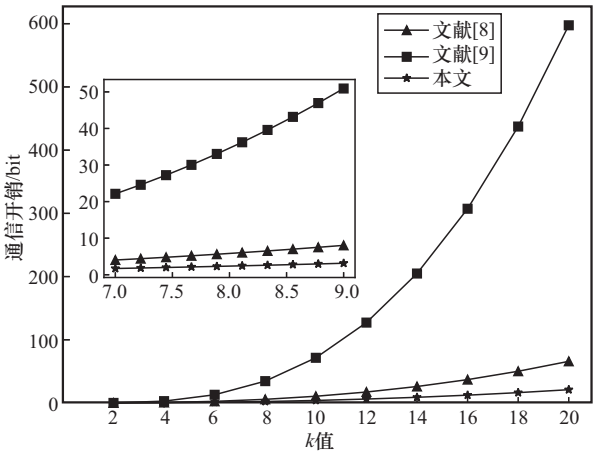


图5　不同k值的通信开销对比

表7　不同方案的安全属性对比

方案	双向认证	密钥协商	抗传统网络攻击	密钥前后向安全	隐私信息保护	抗量子计算攻击
文献[3]	√	√	√	√	×	×
文献[4]	√	√	√	×	×	×
文献[8]	√	×	√	×	×	√
文献[9]	√	√	√	√	×	√
本文	√	√	√	√	√	√

5.3　安全属性对比

本节将本文所提方案与其他相关方案在安全属性方面进行比较，具体对比结果如表7所示，其中√代表存在该安全属性，×代表不存在该安全属性。

从表7中可以看出，现有的认证协议不能满足所有的安全要求。文献[4]方案使用椭圆曲线加密算法生成会话密钥，该密钥不具有随机性，若密钥被攻击者截获且密钥未定时更新，则攻击者有较高概率根据当前会话密钥推断出原始数据。而文献[8]方案中没有考虑密钥协商阶段，只是完成实体间的相互认证，因此没有密钥前后向安全需求。除本文外，其他几种认证方案皆无法实现隐私信息保护，这是因为文献[3-4,8-9]方案在注册或认证阶段使用简单的哈希函数对实体的真实身份进行加密，无法抵御量子计算攻击。此外，由于文献[3-4]方案的安全性是基于离散对数问题，可在多项式时间内被量子算法破解。随着量子计算机的发展，2种认证协议都会存在安全风险。本文通过在密钥生成过程中添加随机因子保障密钥的前后向安全。同时本文基于格密码的哈希函数生成不可伪造的注册请求消息在NCC上完成注册，保护用户的隐私信息不被泄露。因此，本文所提方案不仅满足了常规的各种安全属性，而且还在后量子时代里基于SIS难题有效抵御了量子计算攻击，比其他方案更安全。因此，结合注册阶段和认证阶段的计算时间、认证时间以及安全属性，所提方案满足所有的设计需求，相比其他4种方案，是最优认证方案。

6　结束语

本文针对卫星网络的特点，设计了一种基于格的卫星网络轻量化后量子接入认证方案，该方案在注册阶段基于近似SVP问题的格密码的哈希函数完成了卫星和地面用户的注册。同时，在认证阶段分别在地面和卫星上使用了盆景树算法和原像抽样算法实现了卫星和地面用户的双向认证。安全性理论证明，该方案基于格中的SIS问题可以抵御量子计算攻击。性能结果分析表明，该方案花费了更少的时间便完成了通信实体间的注册和认证。此外，该方案在低轨、中轨、高轨卫星网络中均适用，通信距离越远越能体现本文所提方案的优势。

参考文献：

[1] 蒋长林, 李清, 王羽, 等. 天地一体化网络关键技术研究综述[J]. 软件学报, 2024, 35(1): 266-287.
JIANG C L, LI Q, WANG Y, et al. Survey on key technologies in space-ground integrated network[J]. Journal of Software, 2024, 35(1): 266-287.

[2] 徐国愚, 徐刚, 姜涛, 等. 天地一体化网络认证机制性能定量分析方法[J]. 计算机工程与应用, 2020, 56(21): 108-114.
XU G Y, XU G, JIANG T, et al. Research on quantitative analysis of authentication mechanism performance for space-ground integrated information network[J]. Computer Engineering and Applications, 2020, 56 (21): 108-114.

[3] XUE K P, MENG W, LI S H, et al. A secure and efficient access and handover authentication protocol for Internet of Things in space information networks[J]. IEEE Internet of Things Journal, 2019, 6(3): 5485-5499.

[4] CHEN Y R, YIN F M, HU S F, et al. ECC-based authenticated key agreement protocol for industrial control system[J]. IEEE Internet of Things Journal, 2023, 10(6): 4688-4697.

[5] SHOR P W. Algorithms for quantum computation: discrete logarithms and factoring[C]//Proceedings of the 35th Annual Symposium on Foundations of Computer Science. Piscataway: IEEE Press, 2002: 124-134.

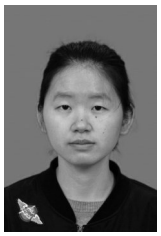
[6] KHAN N, ZHANG J B, ULLAH I, et al. Lattice-based authentication scheme to prevent quantum attack in public cloud environment[J]. Computers, Materials & Continua, 2023, 75(1): 35-49.

[7] GULATI A, AUJLA G S, CHAUDHARY R, et al. DiLSe: lattice-based secure and dependable data dissemination scheme for social Internet of vehicles[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(6): 2520-2534.

[8] LI Q R, HE D B, YANG Z C, et al. Lattice-based conditional privacy-preserving authentication protocol for the vehicular ad hoc network[J].

IEEE Transactions on Vehicular Technology, 2022, 71(4): 4336-4347.
[9] MA R H, CAO J, FENG D G, et al. LAA: lattice-based access authentication scheme for IoT in space information networks[J]. IEEE Internet of Things Journal, 2020, 7(4): 2791-2805.
[10] GUO J Y, DU Y, WU X S, et al. An anti-quantum authentication protocol for space information networks based on ring learning with errors[J]. Journal of Communications and Information Networks, 2021, 6(3): 301-311.
[11] KUMAR U, GARG M. Learning with error-based key agreement and authentication scheme for satellite communication[J]. International Journal of Satellite Communications and Networking, 2022, 40(2): 83-95.
[12] GUO J Y, DU Y. A novel RLWE-based anonymous mutual authentication protocol for space information network[J]. Security and Communication Networks, 2020, 6: 1-12.
[13] LI Q R, LUO M, HSU C, et al. A quantum secure and noninteractive identity-based aggregate signature protocol from lattices[J]. IEEE Systems Journal, 2022, 16(3): 4816-4826.
[14] SHIM K A. A survey on post-quantum public-key signature schemes for secure vehicular communications[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(9): 14025-14042.
[15] WANG F H, WANG J Q, SHI S Q. Efficient data sharing with privacy preservation over lattices for secure cloud storage[J]. IEEE Systems Journal, 2022, 16(2): 2507-2517.
[16] KARABULUT E, ALKIM E, AYSU A. Efficient, flexible, and constant-time Gaussian sampling hardware for lattice cryptography[J]. IEEE Transactions on Computers, 2022, 71(8): 1810-1823.
[17] GUPTA D S, ISLAM S H, OBAIDAT M S, et al. LAAC: lightweight lattice-based authentication and access control protocol for E-health systems in IoT environments[J]. IEEE Systems Journal, 2021, 15(3): 3620-3627.
[18] GUPTA D S, KARATI A, SAAD W, et al. Quantum-defended blockchain-assisted data authentication protocol for Internet of vehicles [J]. IEEE Transactions on Vehicular Technology, 2022, 71(3): 3255-3266.
[19] CASH D, HOFHEINZ D, KILTZ E, et al. Bonsai trees, or how to delegate a lattice basis[C]//Proceedings of the 29th Annual International Conference on Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2010:523-552.
[20] CAO Y B, XU S Y, CHEN X, et al. A forward-secure and efficient authentication protocol through lattice-based group signature in VANETs scenarios[J]. Computer Networks, 2022, 214: 109-149.
[21] LYUBASHEVSKY V, MICCIANCIO D. Asymptotically efficient lattice-based digital signatures[C]//Theory of Cryptography Conference. Berlin: Springer, 2008: 37-54.

[作者简介]



王杉杉（1996– ），女，重庆人，重庆邮电大学博士生，主要研究方向为天地一体化网络安全。

赵国锋（1972– ），男，陕西西安人，博士，重庆邮电大学教授、博士生导师，主要研究方向为天地一体化网络体系结构、工业物联网、网络安全。

徐川（1980– ），男，重庆人，博士，重庆邮电大学教授、博士生导师，主要研究方向为网络体系结构、网络安全、网络建模。

韩珍珍（1989– ），女，河南商丘人，博士，重庆邮电大学讲师，主要研究方向为天地一体化网络体系结构、跨层路由、网络安全。