面向空间信息网络的免配对无证书链上接入认证方法

霍如[1,2]，王志浩[2]，邵子豪[2]，黄韬[2,3]
（1.北京工业大学信息科学技术学院，北京 100124；2.紫金山实验室，江苏 南京 211111；
3.北京邮电大学网络与交换技术国家重点实验室，北京 100876）

摘　要：传统的地面网络接入认证方法存在单点故障和证书分发过程不透明的问题，难以应对空间信息网络中高度复杂和动态多变的拓扑网络，因此提出了一种面向空间信息网络的免配对无证书链上接入认证方法。首先，结合联盟链和无证书公钥密码分发技术，构建了星链通信模型。在此基础上，提出了基于区块链的免配对无证书公钥-椭圆曲线混合加密算法，设计了接入认证机制，以保障接入认证过程的安全性和操作的可追溯性。最后，通过扩展的区块结构记录接入认证清单，设计了批处理机制，实现高效切换。安全分析与仿真结果表明，所提方法与现有方法相比，在提供更强安全性保障的前提下，降低了信令开销约50%、认证时延至少约12.4%、批处理认证时延约23%。

关键词：空间信息网络；区块链；无证书公钥密码分发技术；接入认证
中图分类号：TN309
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2024132

Pairing-free certificateless blockchain-based access authentication method for spatial information network

HUO Ru[1,2], WANG Zhihao[2], SHAO Zihao[2], HUANG Tao[2,3]
1. School of Information Science and Technology, Beijing University of Technology, Beijing 100124, China
2. Purple Mountain Laboratories, Nanjing 211111, China
3. State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract: Due to the single point failure and opaque certificate distribution process of the access authentication methods in a traditional terrestrial network, it was difficult to apply to a spatial information network with a highly complex and dynamic topology. Therefore, pairing-free certificateless blockchain-based access authentication method for spatial information network was proposed. Firstly, a satellite-blockchain network communication model was constructed, combining consortium blockchain and certificateless public key cryptography distribution technology. Furthermore, a certificateless public key without pairing and elliptic curve hybrid encryption algorithm based on blockchain was proposed, and an access authentication mechanism was designed to ensure the security of the access authentication process and the traceability of operations. Finally, the access authentication list was recorded through the extended block structure, and the batch verification mechanism was designed to achieve efficient handover. Security analysis and simulation results show that, compared with existing methods, the proposed method reduces the signaling overhead by about 50%, the authentication delay by at least 12.4%, and the batch authentication delay by about 23%, while providing stronger security guarantees.

Keywords: spatial information network, blockchain, certificateless public key cryptography distribution technology, access authentication

收稿日期：2023–10–12；修回日期：2024–05–24
通信作者：王志浩，wangzhihao01@pmlabs.com.cn
基金项目：国家重点研发计划基金资助项目（No.2023YFB2704200）
Foundation Item：The National Key Research and Development Program of China (No.2023YFB2704200)

0　引言

空间信息网络是以空间平台（如同步卫星或中、低轨道卫星、平流层气球、有人或无人驾驶飞机等）为载体，实时获取、传输和处理空间信息的网络系统。相比其他传统的信息系统而言，空间信息网络具备4个基本特征[1]：1) 空间信息网络是一个立体的、多层次的、全球性的网络系统；2) 空间信息网络是一个多节点、大链路差异的大型异构网络；3) 网络拓扑结构规则性动态变化；4) 业务类型繁多，分布范围广。在空间信息网络中，卫星节点负责提供最终用户请求的服务。一般来说，卫星节点有3种类型的卫星，即静止地球轨道（GEO, geostationary earth orbit）卫星、中地球轨道（MEO, medium earth orbit）卫星和低地球轨道（LEO, low earth orbit）卫星。GEO卫星距离地球较远，具有与地球自转一致的稳定轨道周期。一般来说，GEO卫星可以保证稳定的通信，这对LEO和MEO卫星网络的数据中继起着重要作用。MEO卫星是地球的非同步卫星，可以在LEO和GEO卫星之间传递信息。与MEO和GEO卫星相比，LEO卫星离地面更近，便于发射和维护。由于其物理位置，LEO卫星通常以更短的传输时延实现更高的吞吐量。因此，LEO卫星通常用作接入点，为地面用户（如飞机）提供数据通信和相应的服务。本文中的卫星接入点（SAP, satellite access point）指LEO卫星。

与传统的地面网络不同，空间信息网络可以克服地理限制，提供灵活的、无处不在的接入认证服务，在各种场景（如应急救援、全球定位和导航等）中发挥着重要作用。然而，空间信息网络本身的特性使得其链路暴露程度高、通信时延相对较高、传输速率不稳定、异构网络切换和集成、缺乏统一的标准和管理机制。这些特性使空间信息网络在安全性、隐私性等方面存在着一些问题，并面临如下相关挑战。

1) 密钥管理机制。由于空间信息网络覆盖了广泛的地理空间，建立类似于传统地面网络的集中式密钥管理机制是不现实的。为了适应空间信息网络中各种异构网络的存在和高度复杂的通信环境，设计良好的密钥管理机制是一个亟待解决的问题。

2) 安全通信协议。空间信息网络中复杂的通信环境（如高度暴露的链路）使通信容易受到各种恶意攻击（如窃听、篡改和中间人攻击）。因此，设计一种安全通信协议以确保空间信息网络的安全性，同时保证接入认证服务的服务质量至关重要。

3) 安全切换方案。由于卫星空间与地面空间相对位置的快速变化，需要精心设计安全切换方案，以确保在此过程中信息稳定、快速地传输。

综上所述，需要设计一个安全、高效、可信接入认证方法来实现空间信息网络中有效的密钥管理，保证安全高效的通信与稳定、快速的信息传输，从而实现安全通信与高效切换。

在传统的地面网络中，研究人员已经提出了许多切换认证方案。文献[2]提出了一种基于代理签名算法的统一切换认证方案，只需2次交互即可实现用户与目标接入点之间的双向身份认证方案。文献[3]提出了一种基于凭证高效的切换认证，然后使用秘密共享算法设计并实现了LTE/LTE-A网络的切换认证方案。文献[4]提出了一种轻量级的无线网络切换认证方案，主要利用哈希运算和减少耗时的公钥算法提高该方案的安全性和效率。但是上述方案是为传统地面网络设计的，无法适应复杂的空间信息网络环境。

目前，空间信息网络的接入认证方案已经存在部分研究。文献[5]提出了一种基于椭圆曲线加密（ECC, elliptic curve cryptography）和椭圆曲线数字签名算法（ECDSA, elliptic curve digital signature algorithm）实现非交互式的单向认证。文献[6]提出了基于代理签名的低时延空间信息网络身份认证方法，使用代理签名减少卫星被攻击的风险。文献[7]提出了一种基于ECC算法和对称加密算法的卫星通信认证方法。尽管上述方案基于身份验证机制实现星间以及星地间的安全通信，但上述身份验证机制构建在公钥基础设施（PKI, public key infrastructure）上，需要可信三方证书颁发机构（CA, certificate authority）为所有PKI证书提供信任根。然而，CA存在单点故障问题，会带来沉重的管理成本，无法实现对密钥的有效管理。同时，在上述方案中，用户进行切换认证的安全性也无法得到保障。

区块链是由多个独立节点共同组成的分布式数据库系统，记录节点上发生的所有交易信息。区块链的数据结构可分为3个部分，分别是链、区块和交易，同一个周期内所有被提交的交易构成区块，

区块基于时序连接构成链。区块体内交易数据结构采用Merkle树结构组织，内部任何一个数据改动都会引起交易总哈希值的变化，导致区块链从该区块断开，因此可保证数据不易被篡改、伪造和可追溯。通过区块链技术构建可信分布式系统，能够有效防止单点故障问题，并降低管理成本[8-9]。目前，区块链仍面临着高性能数据交互问题。文献[10]从区块链技术的发展历史出发，给出了高性能数据交互问题的3个方向：1) 链上交互技术，对区块链本身的基础协议和架构进行修改和优化；2) 链下交互技术，将部分数据处理转移到链下，只将最终结果返回链上进行存储和记录，提高了数据处理的效率；3) 跨链交互技术，主要是公证人方案、侧链与链中继、哈希锁定、分布式私钥等。文献[11]设计了一种基于Pedersen承诺与Schnor协议的安全多方计算协议，通过构建该协议架构进行形式化证明演算，表明该协议能够融入区块网络、在匿名情况下合并不同隐私消息并进行高效签署。文献[12]提出了研究一种新型的去中心化阈值签名协议，通过将分布式密钥生成协议与博内-林恩-沙哈姆（BLS, Boneh-Lynn-Shacham）签名结合，设计了一套可多方参与和签名长度固定的阈值签名协议。在协议的实现过程中，采用区块链智能合约作为协议的通信层，确保协议参数的安全交换。

同时，区块链技术能够为空间信息网络中的密钥分发提供可信环境和更加安全的通信，并为切换认证提供可信环境。近期，已有学者使用区块链在空间信息网络接入认证方面进行相关研究。基于卫星不断增长的计算和通信能力，文献[13]设计了一个用于空间信息网络的具有预定义智能合约的区块链架构，并基于智能合约和单轮密钥交换技术构造了Fulgor通信协议，实现了系统内的安全通信。但是该方案默认链上节点可信，忽视了节点本身存在的安全风险。文献[14]结合无密钥签名和区块链数据的不可否认性，实现了基于身份验证和隐私保护的卫星通信网络方案设计。在该方案中，只在地面构建区块链的数据库，其认证的安全性仍依赖于ECC算法的安全性，无法摆脱CA单点故障带来的问题。

上述基于区块链的空间信息网络接入认证研究并没有合理地利用区块链去中心化的优势，忽视了高度暴露的链路下系统建立时密钥分发的安全风险。因此，本文基于传统的无证书公钥密码（CL-PKC, certificateless public key cryptography）分发技术，设计了免配对无证书公钥密码分发技术，并通过智能合约实现链上监督，构建了星链通信网络。同时，基于区块链的无证书公钥-椭圆曲线混合加密算法，实现用户与地面节点间相互认证，并基于星链系统中记录用户访问认证清单以及时间戳数据，完成链上身份认证智能合约设计，保证了用户与空间信息网络的安全通信。此外，借助区块链中智能合约结合批处理机制的设计，保证处理大量切换请求时的高效性。

1 星链通信模型

本文系统面向空间信息网络，建立星链通信模型，该模型实体主要分为3个部分，即地面基站（GS, ground station）、卫星接入点和移动用户（MU, mobile user）。在该模型中，MU在区块链中完成注册后，通过SAP验证后接入空间信息网络获取服务，模型如图1所示。

首先，地面基站共同完成地面区块链的构建，主要负责SAP、MU注册和相关信息验证，为接入MU提供服务以及保存接入身份列表、访问认证权限列表、ID与身份对应列表和用户操作记录存储工作。一般说来，地面基站分为信关站和地面站，信关站负责卫星管理控制，如星间链路的选取和更改；地面站负责通信转接职能，如将星间网络传输数据转发到地面主干网[15]。地面基站共同构建地面区块链。由于信关站具有网络控制中心（NCC, network control center）职能，能够完成相关管理工作，因此，信关站作为区块节点的候选节点；地面站作为普通节点只作为记账节点，不参与共识过程。同时，SAP共同完成星间分布式存证集群的构建，主要负责对接入MU的验证、数据中继、传输并存储接入身份列表和访问认证权限列表。地球轨道卫星和地球同步轨道卫星离地面距离过远导致传输时延过高，不适合参与认证操作，因此本文讨论的SAP，特指低地球轨道卫星。此外，由于星间载荷能力弱以及存储能力有限，星间分布式存证集群各SAP只同步地面区块链中的接入身份列表和访问认证权限列表。

基于上述星链通信模型，MU需要提前在地面区块链中注册相关信息，获取接入权限，并记录到地面区块链中，星间分布式存证集群才能完成同

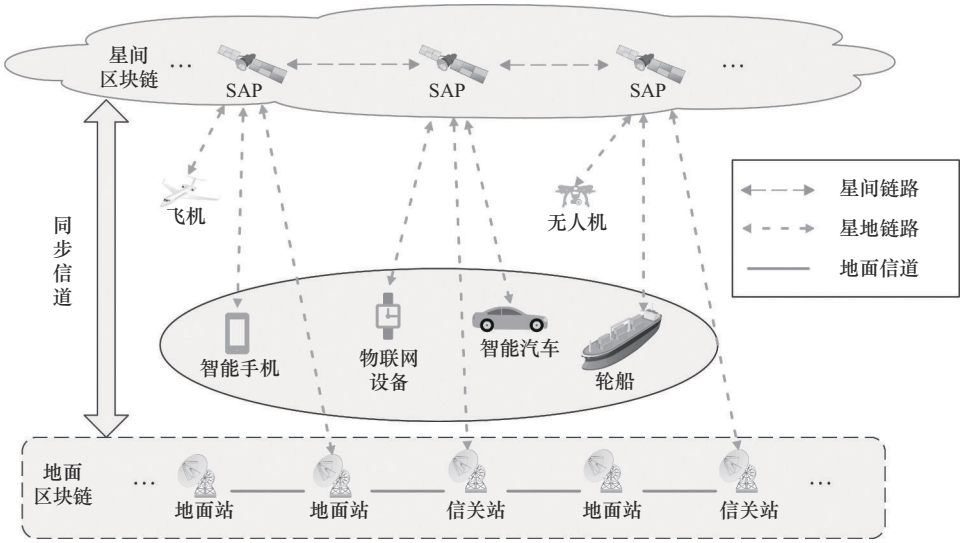

图1　星链通信模型

步。当MU想要获得空间信息网络服务时，需要通过星间分布式存证集群验证，与地面基站建立连接，获取相关服务。其中，MU由不同类型和不同架构的用户设备组成，如智能手机、无人机、物联网设备、智能汽车等。

2　基于区块链的接入认证方案

基于上述星链通信模型，本文设计了从MU接入空间信息网络的完整的接入认证流程，以保证通信的安全，实现相互认证、细粒度接入控制和过程可追溯。具体地，本文将通过基于免配对无证书的星链通信网络构建流程、基于链上无证书-椭圆曲线的接入认证机制以及基于星链通信网络的低/高速移动用户切换机制共同构建空间信息网络的接入与切换认证方案。

2.1　基于免配对无证书的星链通信网络构建流程

本节将通过地面系统初始化、星间分布式存证集群初始化和用户注册3个部分完成星链通信网络的构建。

1) 地面系统初始化。当系统启动时，地面基站完成地面区块链的构建。地面区块链启动共识流程，选出节点。首先，该节点随机生成基点G和素域F_P上的椭圆曲线$E_P(a,b)$，同时生成长期私钥$\mathrm{SK}_{\mathrm{GS}}$和公钥$\mathrm{PK}_{\mathrm{GS}}$，$\mathrm{PK}_{\mathrm{GS}}=\mathrm{SK}_{\mathrm{GS}}G$。该节点选取基点$G$作为生成元生成一个阶为$g$的循环加法群$Z_1$。此外，该节点将确定3个安全的哈希函数$H_1$:$\{0,1\}\rightarrow Z_1^*$、$H_2$:$\{0,1\}\rightarrow Z_1^*$和$H_3$:$\{0,1\}\rightarrow Z_1^*$。随后，该节点将$\mathrm{Sig}_{\mathrm{GS}}(G,a,b,p,g,\mathrm{PK}_{\mathrm{GS}},H_1,H_2,H_3)$存入地面区块链中。其中，$\mathrm{Sig}_{\mathrm{GS}}$为地面系统中对应节点的签名，签名采用SM3算法生成对应公私钥。

2) 星间分布式存证集群初始化。地面基站完成参数初始化和区块链构建后，向SAP发送星间分布式存证集群构建消息。每个SAP接收到消息后，根据自己生成的随机秘密值x_{SAP}，计算部分公钥信息$X_{\mathrm{SAP}}=x_{\mathrm{SAP}}G$，随后向地面区块链发送$\mathrm{Sig}_{\mathrm{SAP}}(\mathrm{ID}_{\mathrm{SAP}},X_{\mathrm{SAP}},T_{\mathrm{SAP}})$。其中，$\mathrm{Sig}_{\mathrm{SAP}}$为对应SAP的签名，$T_{\mathrm{SAP}}$为SAP发送消息时间戳。地面基站接收消息后，验证签名，并计算时延$T_{\mathrm{SAP\text{-}GS}}-T_{\mathrm{SAP}}$，其中$T_{\mathrm{SAP\text{-}GS}}$为该SAP到达地面基站时间戳。若SAP的时间误差为t_1 min，往返时延为t_2 min，本文设置允许最大时延$\Delta T=2t_1+3t_2$。若设定时延$\Delta T<T_{\mathrm{GS}}-T_{\mathrm{SAP}}$，则发送超时消息，并要求SAP重新发送消息（后续时延判定相同）；否则，NCC选取随机数r_{SAP}，并进行如式(1)所示的计算。

$$\begin{aligned}&R_{\mathrm{SAP}}=r_{\mathrm{SAP}}G\\&b_{\mathrm{SAP}}=r_{\mathrm{SAP}}+\mathrm{SK}_{\mathrm{GS}}H_1(\mathrm{ID}_{\mathrm{SAP}},R_{\mathrm{SAP}},X_{\mathrm{SAP}},T_{\mathrm{SAP}})\end{aligned}\tag{1}$$

完成计算后，地面基站将$\mathrm{Sig}_{\mathrm{GS}}(\mathrm{ID}_{\mathrm{GS}},T_{\mathrm{GS}},\mathrm{ID}_{\mathrm{SAP}},R_{\mathrm{SAP}},d_{\mathrm{SAP}})$发送给对应的SAP。同时，地面基站的监控程序监控到地面基站向SAP发送消息的行为，监控程序会主动将地面基站向SAP发送的消息数据$\mathrm{Sig}_{\mathrm{GS}}(\mathrm{ID}_{\mathrm{GS}},T_{\mathrm{GS}},\mathrm{ID}_{\mathrm{SAP}},R_{\mathrm{SAP}},b_{\mathrm{SAP}})$发送给智能合约，此时智能合约会自动化执行，将消息数据存入地面区块链中。其中，$\mathrm{Sig}_{\mathrm{GS}}$为该地面基站的签名，$\mathrm{ID}_{\mathrm{GS}}$为该地面基站的身份信息，$T_{\mathrm{GS}}$为GS发送消息时间戳。SAP收到消息后，对签名和时间戳进行验证。通过验证后，继续验证公式$b_{\mathrm{SAP}}G$与

$B_{\mathrm{SAP}}=R_{\mathrm{SAP}}+\mathrm{PK}_{\mathrm{GS}}H_1(\mathrm{ID}_{\mathrm{SAP}},R_{\mathrm{SAP}},X_{\mathrm{SAP}},T_{\mathrm{SAP}})$，并进行如式(2)所示的计算。

$$\begin{aligned}\mathrm{SK}_{\mathrm{SAP}}&=(x_{\mathrm{SAP}},b_{\mathrm{SAP}})\\ \mathrm{PK}_{\mathrm{SAP}}&=(X_{\mathrm{SAP}},B_{\mathrm{SAP}})\end{aligned}\tag{2}$$

完成上述计算后，SAP获得自己的私钥$\mathrm{SK}_{\mathrm{SAP}}$和公钥$\mathrm{PK}_{\mathrm{SAP}}$。随后SAP向地面基站发送自己的公钥$\mathrm{PK}_{\mathrm{SAP}}$，地面基站获得SAP的公钥后，进行如式(3)所示的计算。

$$P_{\mathrm{ID}_{\mathrm{SAP}}}=\mathrm{PK}_{\mathrm{SAP}}\|\mathrm{ID}_{\mathrm{SAP}}\|T_{\mathrm{SAP}^*}\tag{3}$$

其中，T_{SAP^*}为SAP发送公钥到地面基站时间戳。完成上述计算后，地面基站将$\mathrm{Sig}_{\mathrm{GS}}(\mathrm{ID}_{\mathrm{SAP}},\mathrm{PK}_{\mathrm{SAP}},T_{\mathrm{SAP}^*},P_{\mathrm{ID}_{\mathrm{SAP}}})$存入地面区块链中，其中，$P_{\mathrm{ID}_{\mathrm{SAP}}}$为该条数据验证参数。地面基站向SAP发送星间分布式存证集群名单，SAP与名单内的SAP共同建立星间分布式存证集群。至此，星间分布式存证集群初始化完成。

3) 用户注册。MU使用空间信息网络服务，需要在地面区块链中完成注册成为合法用户。首先，MU_j需要向地面基站发送注册请求，以便与真实身份ID_j一起注册到空间信息网络。对应地面基站在接收到注册请求后，首先生成n个随机数$N_j^i(i=1,2,3,\cdots,n)$，随机选择第q个随机数Q_{ID_j}计算临时身份，具体如式(4)所示。

$$\mathrm{TID}_j^i=H_{\mathrm{GS}}(\mathrm{ID}_j\|Q_{\mathrm{ID}_j})\tag{4}$$

随后，地面基站向MU发送$\mathrm{Sig}_{\mathrm{GS}}(\mathrm{ID}_{\mathrm{GS}},T_{\mathrm{GS}},\mathrm{TID}_j^i)$。MU对签名进行时间戳验证后，根据自己生成的随机秘密值$x_{\mathrm{TID}_j^i}$，计算部分公钥信息$X_{\mathrm{TID}_j^i}=x_{\mathrm{TID}_j^i}G$，随后向地面基站发送$\mathrm{Sig}_{\mathrm{TID}_j^i}(\mathrm{TID}_j^i,X_{\mathrm{TID}_j^i},T_{\mathrm{TID}_j^i})$。其中，$\mathrm{Sig}_{\mathrm{TID}_j^i}$为对应用户临时身份的签名，$T_{\mathrm{TID}_j^i}$为$\mathrm{TID}_j^i$发送消息时间戳。地面基站接收到消息后，验证签名与时间戳。地面基站选取随机数$r_{\mathrm{TID}_j^i}$，并进行如式(5)所示的计算。

$$\begin{aligned}R_{\mathrm{TID}_j^i}&=r_{\mathrm{TID}_j^i}G\\ b_{\mathrm{TID}_j^i}&=r_{\mathrm{TID}_j^i}+\mathrm{SK}_{\mathrm{GS}}H_1(\mathrm{ID}_{\mathrm{TID}_j^i},R_{\mathrm{TID}_j^i},X_{\mathrm{TID}_j^i},T_{\mathrm{TID}_j^i})\end{aligned}\tag{5}$$

完成计算后，地面基站将$\mathrm{Sig}_{\mathrm{GS}}(\mathrm{ID}_{\mathrm{GS}},\mathrm{T}_{\mathrm{GS}},\mathrm{TID}_j^i,R_{\mathrm{TID}_j^i},d_{\mathrm{TID}_j^i})$发送给对应SAP。同时，负责监督地面基站行为的智能合约会将相关数据自动同步到地面区块链中。其中，$\mathrm{Sig}_{\mathrm{GS}}$为该地面基站的签名，$\mathrm{ID}_{\mathrm{GS}}$为该地面基站的身份信息，$T_{\mathrm{GS}}$为GS发送消息时间戳。MU收到消息后，对签名和时间戳进行验证。通过验证后，继续验证$b_{\mathrm{TID}_j^i}G$与$B_{\mathrm{TID}_j^i}=R_{\mathrm{TID}_j^i}+\mathrm{PK}_{\mathrm{GS}}H_1(\mathrm{ID}_{\mathrm{TID}_j^i},R_{\mathrm{TID}_j^i},X_{\mathrm{TID}_j^i},T_{\mathrm{TID}_j^i})$是否相等，通过验证后，进行如式(6)所示的计算。

$$\begin{aligned}\mathrm{SK}_{\mathrm{TID}_j^i}&=(x_{\mathrm{TID}_j^i},b_{\mathrm{TID}_j^i})\\ \mathrm{PK}_{\mathrm{TID}_j^i}&=(X_{\mathrm{TID}_j^i},B_{\mathrm{TID}_j^i})\end{aligned}\tag{6}$$

随后，MU向地面基站发送自己的公钥$\mathrm{PK}_{\mathrm{TID}_j^i}$。地面基站获得用户公钥后为用户分配访问权限$A_{\mathrm{ID}_j}$，并进行如式(7)所示的计算。

$$\begin{aligned}P_{\mathrm{TID}_j^i}=\mathrm{PK}_{\mathrm{TID}_j^i}\|\mathrm{TID}_j^i\|\mathrm{Enc}_{\mathrm{PK}_{\mathrm{GS}}}(\mathrm{TID}_j^i,\\ \mathrm{ID}_j,A_{\mathrm{ID}_j})\|\mathrm{LT}_{\mathrm{TID}_j^i}\end{aligned}\tag{7}$$

其中，$\mathrm{LT}_{\mathrm{TID}_j^i}$是地面基站定义的第$i$个临时标识的生存期。地面基站完成上述计算后，计算

$$\begin{aligned}&\mathrm{Sig}_{\mathrm{GS}}(\mathrm{PK}_{\mathrm{TID}_j^i},\mathrm{TID}_j^i,A_{\mathrm{ID}_j},\mathrm{LT}_{\mathrm{TID}_j^i},P_{\mathrm{TID}_j^i},\\ &\mathrm{Enc}_{\mathrm{PK}_{\mathrm{GS}}}(\mathrm{TID}_j^i,\mathrm{ID}_j,A_{\mathrm{ID}_j}))\end{aligned}\tag{8}$$

随后，地面基站将式(8)存入地面区块链中，并将$\mathrm{Sig}_{\mathrm{GS}}(\mathrm{PK}_{\mathrm{TID}_j^i},\mathrm{TID}_j^i,A_{\mathrm{ID}_j},\mathrm{LT}_{\mathrm{TID}_j^i},P_{\mathrm{TID}_j^i})$同步至星间分布式存证集群各节点，$P_{\mathrm{TID}_j^i}$为该条数据验证参数。至此，用户注册完成。此外，当$\mathrm{LT}_{\mathrm{TID}_j^i}$耗尽时，地面基站的监控程序会主动向地面区块链中智能合约发送提醒消息，智能合约会自动化执行，赋予用户新的临时身份。

2.2 基于链上无证书-椭圆曲线的接入认证机制

本节将通过预协商和接入认证2个阶段共同完成用户接入认证机制的设计。

2.2.1 预协商阶段

在预协商阶段，地面区块链需要存储所有地面节点的预协商消息，并同步到星间分布式存证集群各节点。预协商消息包含基于对应地面节点签名的一个时间戳和一个密钥协商参数$R_{\mathrm{GS}}=r_{\mathrm{GS}}G$，其中$r_{\mathrm{GS}}$是网关选择的随机数，将用于在身份验证和密钥协商阶段生成会话密钥。在接收到消息后，SAP首先验证签名并检查时间戳以防止重播攻击，然后将此预协商消息存到星间分布式存证集群各节点。为了进一步保证密钥协商的安全性，地面站将定期更新预协商消息，更新密钥协商参数R_{GS}。定期更新R_{GS}可以帮助消除密钥协议的潜在威胁。

2.2.2　接入认证阶段

当用户请求访问空间信息网络中的资源或与其他用户通信时，身份验证交互继续进行。在接入认证阶段，MU_j和NCC将同时协商会话密钥。本文方法的接入认证流程如图2所示。

MU_j生成请求消息m，选取随机数$k_{TID_j^i}$和时间戳$T^1_{TID_j^i}$进行如式(9)所示的计算。

$$\begin{aligned}
&V_{TID_j^i} = k_{TID_j^i}G\\
&h^1_{TID_j^i} = H_1(TID_j^i, V_{TID_j^i}, X_{TID_j^i}, T^1_{TID_j^i})\\
&h^2_{TID_j^i} = H_2(m, TID_j^i, V_{TID_j^i}, X_{TID_j^i}, T^1_{TID_j^i})\\
&h^3_{TID_j^i} = H_3(m, TID_j^i, V_{TID_j^i}, X_{TID_j^i}, T^1_{TID_j^i})\\
&d_{TID_j^i} = k_{TID_j^i} + SK_{TID_j^i}h^1_{TID_j^i}\\
&W_{TID_j^i} = h^3_{TID_j^i}x_{TID_j^i} + d_{TID_j^i} + k_{TID_j^i}h^2_{TID_j^i}
\end{aligned} \tag{9}$$

完成计算后，MU_j向SAP发送$Sig_{TID_j^i}(T^1_{TID_j^i}, ID_{SAP}, V_{TID_j^i}, W_{TID_j^i}, TID_j^i, P_{TID_j^i})$。SAP接收到$MU_j$的消息后，首先基于$TID_j^i$验证公钥签名，确认公钥与身份对应关系，然后进行时延计算。假设消息到达时间为T^*_{SAP}，若$T^*_{SAP} - T^1_{TID_j^i} > \Delta T$，则返回用户拒绝消息；否则，进行如式(10)所示的计算。

$$\begin{aligned}
&h^1_{TID_j^i} = H_1(TID_j^i, V_{TID_j^i}, X_{TID_j^i}, T^1_{TID_j^i})\\
&h^2_{TID_j^i} = H_2(m, TID_j^i, V_{TID_j^i}, X_{TID_j^i}, T^1_{TID_j^i})\\
&h^3_{TID_j^i} = H_3(m, TID_j^i, V_{TID_j^i}, X_{TID_j^i}, T^1_{TID_j^i})\\
&V'_{TID_j^i} = (h^2_{TID_j^i})^{-1}(W_{TID_j^i}G - h^3_{TID_j^i}X_{TID_j^i} -\\
&V_{TID_j^i} - h^1_{TID_j^i}PK_{TID_j^i})
\end{aligned} \tag{10}$$

若$V_{TID_j^i}$与$V'_{TID_j^i}$不相等，则返回用户拒绝消息；否则，检查在节点内存证的接入身份列表中是否有

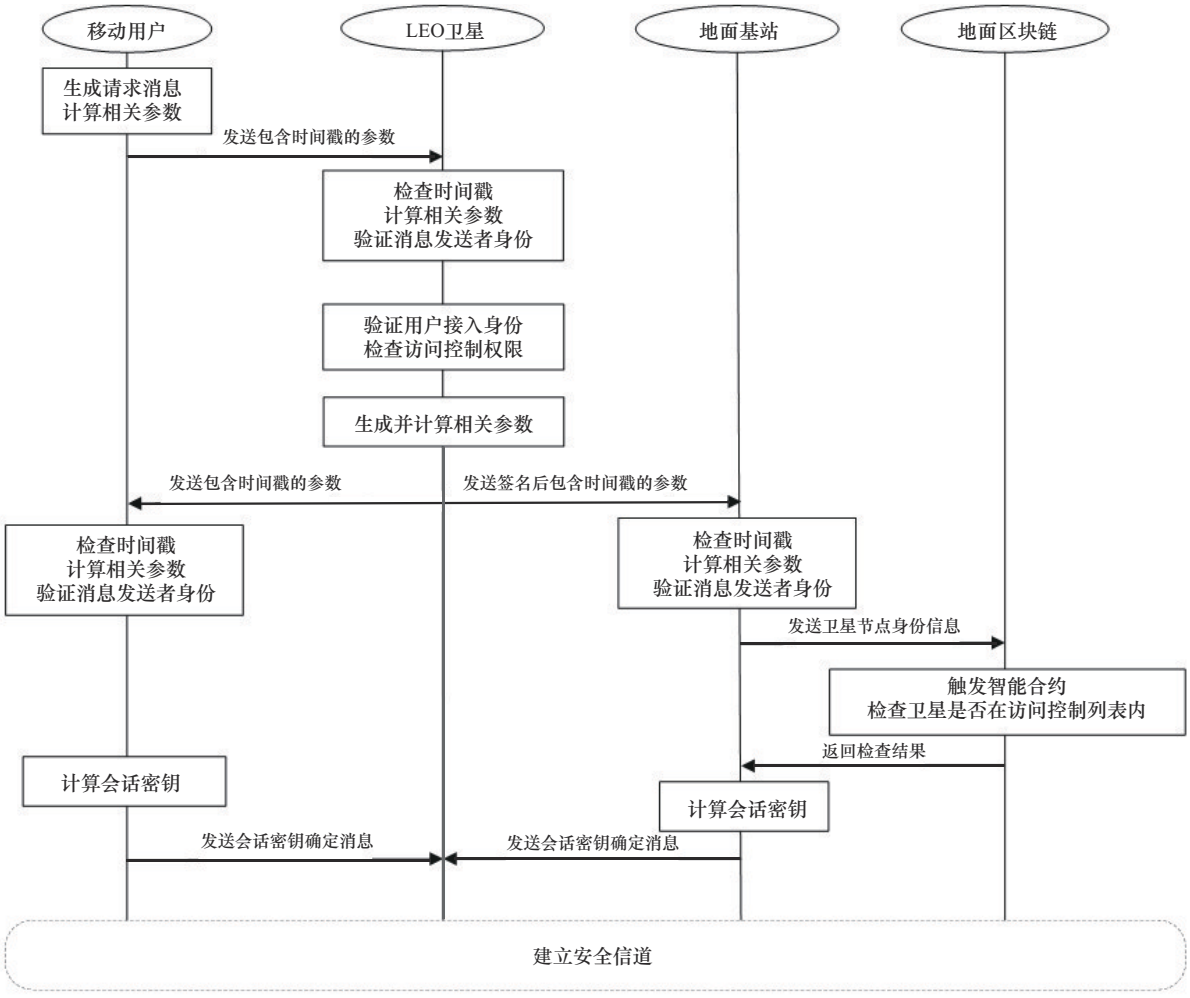

图2　接入认证流程

TID_j^i，并比对包含TID_j^i公钥的访问认证权限列表。通过检查后，SAP则生成随机数k_{SAP}和时间戳T_{SAP}^2，进行如式(11)所示的计算。

$$\begin{aligned}
&V_{\mathrm{SAP}} = k_{\mathrm{SAP}}G\\
&h_{\mathrm{SAP}}^1 = H_1(\mathrm{ID}_{\mathrm{SAP}},V_{\mathrm{SAP}},X_{\mathrm{SAP}},T_{\mathrm{SAP}}^1)\\
&h_{\mathrm{SAP}}^2 = H_2(m,\mathrm{ID}_{\mathrm{SAP}},V_{\mathrm{SAP}},X_{\mathrm{SAP}},T_{\mathrm{SAP}}^1)\\
&h_{\mathrm{SAP}}^3 = H_3(m,\mathrm{ID}_{\mathrm{SAP}},V_{\mathrm{SAP}},X_{\mathrm{SAP}},T_{\mathrm{SAP}}^1)\\
&d_{\mathrm{SAP}} = k_{\mathrm{SAP}} + \mathrm{SK}_{\mathrm{SAP}}h_{\mathrm{SAP}}^1\\
&W_{\mathrm{SAP}} = h_{\mathrm{SAP}}^3 x_{\mathrm{SAP}} + d_{\mathrm{SAP}} + k_{\mathrm{SAP}}h_{\mathrm{SAP}}^2
\end{aligned} \tag{11}$$

SAP将$\mathrm{Sig}_{\mathrm{SAP}}(T_{\mathrm{SAP}}^2,\mathrm{TID}_j^i,V_{\mathrm{SAP}},W_{\mathrm{SAP}},R_{\mathrm{GS}},\mathrm{ID}_{\mathrm{SAP}})$发送给$\mathrm{MU}_j$，并将$\mathrm{Sig}_{\mathrm{SAP}}(T_{\mathrm{SAP}}^2,\mathrm{TID}_j^i,V_{\mathrm{TID}_j^i},\mathrm{ID}_{\mathrm{SAP}},P_{\mathrm{ID}_{\mathrm{SAP}}})$发送给地面节点。$\mathrm{MU}_j$接收到SAP发送的消息后，首先基于SAP验证公钥签名，确认公钥与身份对应关系，然后进行时延计算，验证是否在规定时延ΔT内。假设消息到达时间为T_j^*，若$\Delta T < T_j^* - T_{\mathrm{SAP}}^2$，则返回用户拒绝消息并停止；否则，进行如式(12)所示的计算。

$$\begin{aligned}
&h_{\mathrm{SAP}}^1 = H_1(\mathrm{ID}_{\mathrm{SAP}},V_{\mathrm{SAP}},X_{\mathrm{SAP}},T_{\mathrm{SAP}}^1)\\
&h_{\mathrm{SAP}}^2 = H_2(m,\mathrm{ID}_{\mathrm{SAP}},V_{\mathrm{SAP}},X_{\mathrm{SAP}},T_{\mathrm{SAP}}^1)\\
&h_{\mathrm{SAP}}^3 = H_3(m,\mathrm{ID}_{\mathrm{SAP}},V_{\mathrm{SAP}},X_{\mathrm{SAP}},T_{\mathrm{SAP}}^1)\\
&V'_{\mathrm{SAP}} = (h_{\mathrm{SAP}}^2)^{-1}(W_{\mathrm{SAP}}G - h_{\mathrm{SAP}}^3 X_{\mathrm{SAP}} - V_{\mathrm{SAP}} -\\
&h_{\mathrm{SAP}}^1 \mathrm{PK}_{\mathrm{SAP}})
\end{aligned} \tag{12}$$

若V_{SAP}与V'_{SAP}不相等，则返回用户拒绝消息；否则，确定SAP合法且可信，然后计算与地面站共享的会话密钥，如式(13)所示。

$$\mathrm{SK}_{\mathrm{TID}_j^i - \mathrm{GS}} = k_{\mathrm{TID}_j^i}R_{\mathrm{GS}} \tag{13}$$

同时地面节点接收到SAP的消息后，首先验证签名，然后进行时延计算，验证是否在规定时延ΔT内。假设消息到达时间为T_{GS}^*，若$\Delta T < T_{\mathrm{GS}}^* - T_{\mathrm{SAP}}^2$，则返回用户拒绝消息并停止；否则，地面节点进行式(14)计算并通过地面区块链验证SAP的身份信息。若V_{SAP}与V'_{SAP}不相等或地面区块链中SAP未注册，则返回用户拒绝消息；否则，确定SAP合法且可信。通过检查计算与MU_j共享的会话密钥，如式(14)所示。

$$\mathrm{SK}_{\mathrm{TID}_j^i - \mathrm{GS}} = r_{\mathrm{GS}}V_{\mathrm{TID}_j^i} \tag{14}$$

最终会话密钥将在地面节点和MU_j之间安全共享。因此，在SAP中建立MU_j和地面节点之间的安全信道，会话中的通信分组由其中一个（用户/地面节点）加密，当接收到分组时由另一个解密。

2.3 基于星链通信网络的低/高速用户切换机制

本节将给出切换阶段的方案。在空间信息网络中，卫星相对于地球表面以更高的速度移动，导致网络拓扑的高动态特性。这种特性给连续和安全的通信带来了重大挑战。因此，提供一个无缝和安全的切换方案来保证某些业务的服务质量，尤其是实时业务的服务质量是非常必要的。虽然网络拓扑变化很快，但这种变化是周期性和可预测的，因为卫星有严格的运动轨道。同时，接入同一卫星的用户在切换时有很强的相似性，比如相同的原SAP具有相同的切换时间。因此，以群组方式为这些用户执行切换是合理的。本文在设计切换方案时考虑了上述特性。接下来，将介绍2种可能的切换场景，并分别针对这2种切换场景提出2种切换机制。

2.3.1 低速移动用户切换机制

低速MU相对于高速卫星是静止的，所以卫星覆盖的转移是切换的主要原因。这种切换场景经常发生，如图3所示，对低速MU而言，建立的连接只是从C-SAP切换到N-SAP，地面站不变。因此，MU和地面站之间共享的会话密钥不需要重新协商。考虑到这种情况，给出当这种切换场景发生时服务质量保证问题的可用解决方案如下。

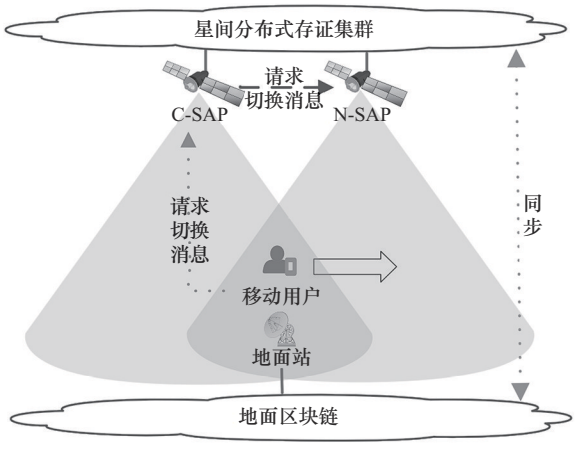

图3 低速MU切换场景

1) 准备阶段。地面站具有卫星星座拓扑和卫星的运动，因此它可以预测即将到来的卫星N-SAP。然后地面站将白名单存入地面区块链，并通知星间分布式存证集群各节点完成同步操作，N-SAP将白名单同步至本地。白名单存储信息为$\mathrm{Sig}_{\mathrm{GS}}(\mathrm{TID}_j^i,\mathrm{ID}_{\mathrm{C\text{-}SAP}})$。其中，$\mathrm{TID}_j^i$为$\mathrm{MU}_j$的第$i$个临

时身份ID，$\mathrm{ID}_{\text{C-SAP}}$为C-SAP的ID。

2) 请求切换阶段。当MU_j位于C-SAP和N-SAP覆盖的重叠区域时，根据接收到的信号强度决定是否切换。当决定切换时，MU_j将请求切换消息连同数据一起发送给C-SAP，该请求切换消息包括MU_j的临时身份和N-SAP的ID，即$\mathrm{Sig}_{\mathrm{GS}}(\mathrm{TID}_j^i,\mathrm{ID}_{\text{N-SAP}})$。然后，C-SAP主动将相关消息发送至N-SAP。

3) 切换完成阶段。接收到请求切换消息后，N-SAP将从本地提取出白名单信息，并与C-SAP发送过来的请求切换消息进行比对，验证通过后，将完成切换。

2.3.2　高速移动用户切换机制

对于高速MU，如各种飞机，切换的原因不仅是卫星覆盖的转移，还有MU的移动。如图4所示，MU不仅从C-SAP切换到N-SAP，而且从当前地面站切换到新地面站。因此，必须更改会话密钥确保管理部门和新地面站之间的安全通信。在这种情况下，MU和新卫星可以使用预认证方法来完成认证和密钥协商。

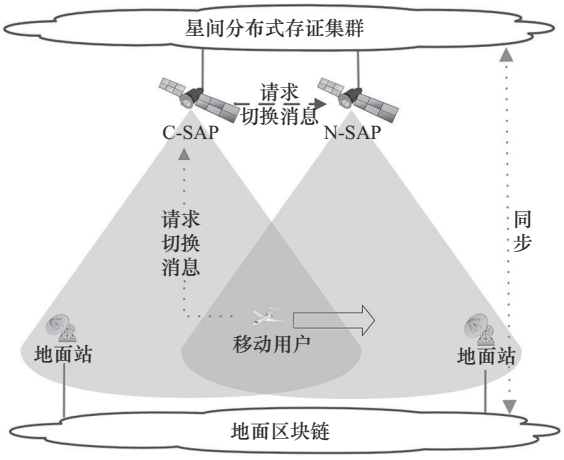

图4　高速MU切换场景

1) 准备阶段。当进入N-SAP的覆盖区域和新地面站覆盖区域时，将在MU_j和新地面站之间执行预协商阶段。

2) 请求切换阶段。在重叠区域中，根据接收到的信号强度决定是否切换。当决定切换时，向C-SAP发送请求切换消息$\mathrm{Sig}_{\mathrm{TID}_j^i}(\mathrm{TID}_j^i,\mathrm{ID}_{\text{N-SAP}},V_{\mathrm{TID}_j^i},W_{\mathrm{TID}_j^i},P_{\mathrm{TID}_j^i})$。然后，C-SAP主动将请求切换消息发送至N-SAP。

3) 切换完成阶段。当N-SAP接收到L个请求切换消息后，可采用批处理机制来验证请求切换消息的合法性，具体验证过程如式(15)所示。

$$G\sum_{j=1}^{L}k_{\mathrm{TID}_j^i}\overset{?}{=}\sum_{j=1}^{L}(h_{\mathrm{TID}_j^i}^2)^{-1}\,(W_{\mathrm{TID}_j^i}G-h_{\mathrm{TID}_j^i}^3X_{\mathrm{TID}_j^i}-V_{\mathrm{TID}_j^i}-h_{\mathrm{TID}_j^i}^1\mathrm{PK}_{\mathrm{GS}}) \tag{15}$$

其中，L最大值为10。如果式(15)成立，从本地中比对白名单，若验证通过，则切换认证完成，并且N-SAP接受所有切换请求，并将确认消息发送回相应的管理单元；否则，通过“分而治之”的方法检测无效的请求切换消息。若验证未通过，则发送“拒绝”消息。同时，N-SAP将消息，即$\mathrm{Sig}_{\mathrm{SAP}}(T_{\mathrm{SAP}}^2,\mathrm{TID}_j^i,V_{\mathrm{SAP}},W_{\mathrm{SAP}},R_{\mathrm{GS}})$发回，以实现相互认证和密钥协商。最后，完成身份验证的MU_j成功与新地面站共享一个会话密钥，并且实现安全和可靠的验证。

3　方案分析

针对本文方法在接入认证过程中的具体实现，本节从正确性与安全性的角度对其进行验证和分析。

3.1　正确性分析

本节将分析在消息认证过程中涉及的接入认证和批量认证的正确性。在接入认证过程中，SAP通过检查来自MU签名后的消息$\mathrm{Sig}_{\mathrm{TID}_j^i}(T_{\mathrm{TID}_j^i}^1,\mathrm{ID}_{\mathrm{SAP}},V_{\mathrm{TID}_j^i},W_{\mathrm{TID}_j^i},\mathrm{TID}_j^i,P_{\mathrm{TID}_j^i})$来确认接入用户消息的有效性和接入身份的合法性。在接入认证过程中，基于下述表达式

$$X_{\mathrm{TID}_j^i}=x_{\mathrm{TID}_j^i}G$$

$$\mathrm{PK}_{\mathrm{TID}_j^i}=\mathrm{SK}_{\mathrm{TID}_j^i}G$$

$$V_{\mathrm{TID}_j^i}=k_{\mathrm{TID}_j^i}G$$

$$h_{\mathrm{TID}_j^i}^1=H_1(\mathrm{TID}_j^i,V_{\mathrm{TID}_j^i},X_{\mathrm{TID}_j^i},T_{\mathrm{TID}_j^i}^1)$$

$$h_{\mathrm{TID}_j^i}^2=H_2(m,\mathrm{TID}_j^i,V_{\mathrm{TID}_j^i},X_{\mathrm{TID}_j^i},T_{\mathrm{TID}_j^i}^1)$$

$$h_{\mathrm{TID}_j^i}^3=H_3(m,\mathrm{TID}_j^i,V_{\mathrm{TID}_j^i},X_{\mathrm{TID}_j^i},T_{\mathrm{TID}_j^i}^1)$$

$$d_{\mathrm{TID}_j^i}=k_{\mathrm{TID}_j^i}+\mathrm{SK}_{\mathrm{TID}_j^i}h_{\mathrm{TID}_j^i}^1$$

$$W_{\mathrm{TID}_j^i}=h_{\mathrm{TID}_j^i}^3x_{\mathrm{TID}_j^i}+d_{\mathrm{TID}_j^i}+k_{\mathrm{TID}_j^i}h_{\mathrm{TID}_j^i}^2$$

$$V'_{\mathrm{TID}_j^i}=(h_{\mathrm{TID}_j^i}^2)^{-1}(W_{\mathrm{TID}_j^i}G-h_{\mathrm{TID}_j^i}^3X_{\mathrm{TID}_j^i}-V_{\mathrm{TID}_j^i}-h_{\mathrm{TID}_j^i}^1\mathrm{PK}_{\mathrm{TID}_j^i})$$

可以验证$V_{\mathrm{TID}_j^i}$与$V'_{\mathrm{TID}_j^i}$相等，即

$$V'_{\mathrm{TID}_j^i}=(h^2_{\mathrm{TID}_j^i})^{-1}(W_{\mathrm{TID}_j^i}G-h^3_{\mathrm{TID}_j^i}X_{\mathrm{TID}_j^i}-V_{\mathrm{TID}_j^i}-h^1_{\mathrm{TID}_j^i}\mathrm{PK}_{\mathrm{TID}_j^i})=$$
$$(h^2_{\mathrm{TID}_j^i})^{-1}[(h^3_{\mathrm{TID}_j^i}x_{\mathrm{TID}_j^i}+d_{\mathrm{TID}_j^i}+k_{\mathrm{TID}_j^i}h^2_{\mathrm{TID}_j^i})G-h^3_{\mathrm{TID}_j^i}X_{\mathrm{TID}_j^i}-$$
$$V_{\mathrm{TID}_j^i}-h^1_{\mathrm{TID}_j^i}\mathrm{PK}_{\mathrm{TID}_j^i}]=$$
$$(h^2_{\mathrm{TID}_j^i})^{-1}(h^3_{\mathrm{TID}_j^i}x_{\mathrm{TID}_j^i}G+d_{\mathrm{TID}_j^i}G+k_{\mathrm{TID}_j^i}h^2_{\mathrm{TID}_j^i}G-$$
$$h^3_{\mathrm{TID}_j^i}X_{\mathrm{TID}_j^i}-V_{\mathrm{TID}_j^i}-h^1_{\mathrm{TID}_j^i}\mathrm{PK}_{\mathrm{TID}_j^i})=$$
$$(h^2_{\mathrm{TID}_j^i})^{-1}[h^2_{\mathrm{TID}_j^i}k_{\mathrm{TID}_j^i}G+(k_{\mathrm{TID}_j^i}+\mathrm{SK}_{\mathrm{TID}_j^i}h^1_{\mathrm{TID}_j^i})G-$$
$$V_{\mathrm{TID}_j^i}-h^1_{\mathrm{TID}_j^i}\mathrm{PK}_{\mathrm{TID}_j^i}]=$$
$$(h^2_{\mathrm{TID}_j^i})^{-1}h^2_{\mathrm{TID}_j^i}k_{\mathrm{TID}_j^i}G=$$
$$k_{\mathrm{TID}_j^i}G=V_{\mathrm{TID}_j^i}$$

在接入认证过程中，MU 对 SAP 验证 V_{SAP} 与 V'_{SAP} 是否相等的计算过程同上，这里不再展开说明。

在批处理过程中，本文使用的基础前提仍然是本节最开始给出的一组表达式。式(15)的具体计算过程如下。

$$\sum_{j=1}^{L}(h^2_{\mathrm{TID}_j^i})^{-1}(W_{\mathrm{TID}_j^i}G-h^3_{\mathrm{TID}_j^i}X_{\mathrm{TID}_j^i}-V_{\mathrm{TID}_j^i}-h^1_{\mathrm{TID}_j^i}$$
$$\mathrm{PK}_{\mathrm{GS}})=\sum_{j=1}^{L}(h^2_{\mathrm{TID}_j^i})^{-1}[(h^3_{\mathrm{TID}_j^i}x_{\mathrm{TID}_j^i}+d_{\mathrm{TID}_j^i}+k_{\mathrm{TID}_j^i}h^2_{\mathrm{TID}_j^i})$$
$$G-h^3_{\mathrm{TID}_j^i}X_{\mathrm{TID}_j^i}-V_{\mathrm{TID}_j^i}-h^1_{\mathrm{TID}_j^i}\mathrm{PK}_{\mathrm{TID}_j^i}]=$$
$$\sum_{j=1}^{L}(h^2_{\mathrm{TID}_j^i})^{-1}(h^3_{\mathrm{TID}_j^i}x_{\mathrm{TID}_j^i}G+d_{\mathrm{TID}_j^i}G+k_{\mathrm{TID}_j^i}h^2_{\mathrm{TID}_j^i}G-$$
$$h^3_{\mathrm{TID}_j^i}X_{\mathrm{TID}_j^i}-V_{\mathrm{TID}_j^i}-h^1_{\mathrm{TID}_j^i}\mathrm{PK}_{\mathrm{TID}_j^i})=$$
$$\sum_{j=1}^{L}(h^2_{\mathrm{TID}_j^i})^{-1}[h^2_{\mathrm{TID}_j^i}k_{\mathrm{TID}_j^i}G+(k_{\mathrm{TID}_j^i}+\mathrm{SK}_{\mathrm{TID}_j^i}h^1_{\mathrm{TID}_j^i})G-$$
$$V_{\mathrm{TID}_j^i}-h^1_{\mathrm{TID}_j^i}\mathrm{PK}_{\mathrm{TID}_j^i}]=$$
$$\sum_{j=1}^{L}(h^2_{\mathrm{TID}_j^i})^{-1}h^2_{\mathrm{TID}_j^i}k_{\mathrm{TID}_j^i}G=G\sum_{j=1}^{L}k_{\mathrm{TID}_j^i}$$

3.2 安全性分析

本节将从安全要求与抵御攻击两方面对本文方法进行安全性分析，并与文献[9,16-20]方案进行安全性比较。

为了证明本文方法的安全性，假设存在恶意攻击者可以访问接入认证过程中双方之间传输的所有消息，并且知道所有的公共参数。

系统在运行过程中可能会面临多种恶意攻击，本文威胁模型考虑的潜在威胁如下。

1) 恶意攻击者伪装成用户，将合法用户的身份认证请求替换成自己生成的身份认证请求，试图非法通过身份认证。

2) 恶意攻击者通过常见的攻击方式，如重放攻击、伪造攻击、替换公钥攻击、篡改攻击和中间人攻击等，试图伪装成合法用户欺骗 SAP。

3) 在合法用户通信过程中，恶意攻击者通过窃听攻击和身份链接攻击推测接入用户的真实身份。

针对安全性要求，首先从相互认证、匿名性、不可链接性和可追溯性等方面展开分析。同时，考虑到密钥更新的安全性，本文还对密钥生成过程中涉及的前后向保密性进行分析。针对安全性要求的分析细节如下。

1) 相互认证。在上述认证方案中，实现了用户与 SAP、SAP 和地面基站之间的相互认证。认证过程可以从验证 $V_{\mathrm{TID}_j^i}$ 与 $V'_{\mathrm{TID}_j^i}$ 以及 V_{SAP} 与 V'_{SAP} 是否相等来完成。攻击者必须同时破解 H_1、H_2 和 H_3 这 3 个哈希函数，假设单个哈希函数的抗碰撞和抗预象性质使得攻击成功概率为 2^{-m}，则攻击成功概率为 2^{-3m}，攻击成功概率随着消息长度增加呈指数下降。通过免配对的 CL-PKC 密钥分发技术与哈希函数保证了 SAP 私钥和用户私钥不会泄露，同时使得被分发的密钥不会受到中心化密钥管理的限制。而在 SAP 与用户私钥未知的情况下，对消息进行伪造是不可行的。

2) 匿名性。在本文方法中，MU_j 的真实身份 ID_j 不会在通信中暴露，通信中的用户身份为地面节点结合当前随机数为其确定的临时身份 $\mathrm{TID}_j^i=H_{\mathrm{GS}}(\mathrm{ID}_j\|Q_{\mathrm{ID}_j})$。此外，由于哈希函数的特性，攻击者无法从临时身份标识中提取真实身份标识，保障了用户的匿名性。

3) 不可链接性。在本文方法中，当生成访问请求消息时，临时身份 TID_j^i 依赖的随机数组生成是随机的，选择随机数的位置也是随机的，因此可以保障用户无法被交易的对方追踪。

4) 可追溯性。一旦用户的不当行为被检测到，网关站就会向 NCC 发送恶意行为的证据。本文方法在注册阶段对 ID_j 和 TID_j 进行了绑定，基于地面节点对公钥进行了加密，并存入区块链。只有 NCC 能够从 $P_{\mathrm{TID}_j^i}$ 中获取用户的真实身份。因此，当发生争议时，NCC 可以追踪恶意用户的真实身份。由于区块链的不可篡改性，该对应列表不会遭

到第三方的恶意篡改，ElGamal加密技术保证了非NCC节点无法获得身份对应列表。

5) 前后向保密性。为了在MU_j和地面基站之间提供密钥前向保密和后向保密，本文采用椭圆曲线Diffie-Hellman密钥交换算法完成对会话密钥的确定。若攻击者想获取会话密钥，他/她必须分别从MU_j和空间信息网络中获取$k_{TID_j^i}$和r_{GS}，这和ECC破解难度是相同的。显然，由于$SK_{TID_j^i\text{-}GS}=k_{TID_j^i}R_G=r_{GS}V_{TID_j^i}=k_{TID_j^i}r_{GS}G$，其中$r_{TID_j^i}$和$r_{GS}$是随机选取的，即使当前会话密钥被攻击者获取，攻击者仍然不能猜测出先前建立的会话密钥。此外，当前会话密钥的泄露也不会导致将来会话密钥的泄露。因此，本文可以实现密钥前向保密和后向保密，从而保证会话密钥的安全性。

本节对常见的抵御攻击进行分析，主要包括重放攻击、伪造攻击、篡改攻击、替换公钥攻击和中间人攻击，分析细节如下。

1) 重放攻击。用户在验证消息中添加了时间戳$T_{TID_j^i}^1$，即$Sig_{TID_j^i}(T_{TID_j^i}^1,ID_{SAP},V_{TID_j^i},W_{TID_j^i},TID_j^i,P_{TID_j^i})$，并确保其签名为最新消息。SAP能够基于时间戳检测重放攻击。因此，本文方法能够有效抵御重放攻击。

2) 伪造攻击。根据前文的证明，攻击者无法获取SAP或签名者的私钥。因此，攻击者无法通过假冒签名者的身份来伪造验证消息$Sig_{TID_j^i}(T_{TID_j^i}^1,ID_{SAP},V_{TID_j^i},W_{TID_j^i},TID_j^i,P_{TID_j^i})$，并使$V_{TID_j^i}$与$V'_{TID_j^i}$相等。

3) 篡改攻击。在消息的验证过程中，攻击者篡改消息$Sig_{TID_j^i}(T_{TID_j^i}^1,ID_{SAP},V_{TID_j^i},W_{TID_j^i},TID_j^i,P_{TID_j^i})$，使得$V_{TID_j^i}$与$V'_{TID_j^i}$无法相等。验证者能够通过计算该等式来检查验证消息是否被篡改。因此，本文方法能够有效抵御篡改攻击。

4) 替换公钥攻击。本文方法在地面区块链和星间分布式存证集群中，实现了用户公钥与临时身份信息的同步存储。MU和SAP验证公钥签名时会验证公钥与身份对应关系。攻击者无法通过替换公钥攻击完成接入认证过程。

5) 中间人攻击。当攻击者在SAP与MU之间进行中间人攻击时，需要假冒成SAP向MU发送验证消息，同时假冒成MU向SAP发送反馈消息。然而，由于本文方法能够有效抵御伪造攻击，因此攻击者无法假冒为其他合法实体。另外，由于消息签名的存在，攻击者只能截获和转发消息，而无法篡改消息。

本文选取了文献[9,16-20]方案，主要在相互认证、匿名性、不可链接性、可追溯性等方面与本文方法进行比较，安全性对比如表1所示。在安全要求上，文献[9,16-20]方案均能满足相互认证、可追溯性和前后向保密性要求。由于区块链的特性，文献[9,16,19-20]未进行额外设计，无法保障用户的匿名性。文献[16-17]为用户设计了临时身份，进行通信时未使用随机身份，容易被追踪到用户隐私信息。文献[9,16-18]由于场景和方案的局限性，未设计批量认证方案。在抵御攻击方面，文献[19]使用无证书密钥分发技术，但是未采取手段解决替换公钥攻击。与其他方案相比，本文方法满足常见的安全需求，且能够实现高效的批量认证。

4　性能分析

本节首先对比了本文方法与文献[9,16-20]方案

表1　　**安全性对比**

方案	相互认证	匿名性	不可链接性	可追溯性	前后向保密性	批量认证	重放攻击	伪造攻击	替换公钥攻击	篡改攻击	中间人攻击
文献[9]	√	×	×	√	√	×	√	√	√	√	√
文献[16]	√	×	×	√	√	×	√	√	√	√	√
文献[17]	√	√	×	√	√	×	√	√	√	√	√
文献[18]	√	√	×	√	√	×	√	√	√	√	√
文献[19]	√	×	×	√	√	√	√	√	×	√	√
文献[20]	√	×	×	√	√	√	√	√	√	√	√
本文方法	√	√	√	√	√	√	√	√	√	√	√

的性能，重点是信令开销、认证时延以及切换验证时延。此外，分析了本文使用批处理的开销优势。

1) 信令开销

在信令开销部分，本文通过与文献[9,16-20]方案进行比较，根据信令消息的数量来评估本文方法。表2列出了不同认证方案在信令开销方面的比较。在文献[9,16-18]方案中，MU和SAP、SAP和GS、GS和NCC之间需要2个信令消息完成相互认证。在本文方法与文献[19-20]方案中，MU和SAP、SAP和GS之间只需要一条信令消息，GS和NCC之间不需要信令消息。尽管文献[9]声明其方案可以在星间完成验证，但是考虑到其在星间使用的是轻节点，所以仍需要与地面的全节点进行交互。因此，本文方法在信令开销上比现有的所有方案具有更好的性能。此外，本文方法可以减轻NCC的负担，因为本文方法不需要NCC参与认证过程。

表2 不同认证方案在信令开销方面的比较

方案	MU ↔ SAP	SAP ↔ GS	GS ↔ NCC
文献[9]	2	2	2
文献[16]	2	2	2
文献[17]	2	2	2
文献[18]	2	2	2
文献[19]	1	1	0
文献[20]	1	1	0
本文方法	1	1	0

2) 认证时延

在认证时延部分，本文将总时延定义为计算开销与传输时延之和。为了便于计算认证时延，本文定义以下符号：TG_{mul}代表椭圆曲线密码机制中点乘运算；TG_{add}代表椭圆曲线密码机制中加法运算；TG_{exp}代表椭圆曲线密码机制中幂运算；$TG_{\wedge_e}$代表进行一次双线性配对花费的时间；TG_H代表进行一次Hash运算花费的时间；TG_{BC}代表完成一次上链过程花费的时间。本文采用了嵌入度k=6和p~170位宫地－中林－高野（MNT, Miyaji-Nakabayashi-Takano）曲线[8]，测试的区块链平台为自行搭建的具备10个节点的联盟链平台，fabric版本为1.4。本次实验的仿真环境CPU为Intel i5-9400F 2.90 GHz、16 GB内存以及Windows10操作系统。仿真实验结果显示，签名生成/验证操作以及区块链的查询操作相对其他操作的时间计算开销可以忽略不计，此处不再列出。各密码操作的执行时间如表3所示。

表3 各密码操作的执行时间

操作	时间/ms
TG_{mul}	2.163
TG_{add}	0.013
TG_{exp}	0.339
$TG_{\wedge_e}$	5.427
TG_H	0.007
TG_{BC}	23.12

本文论述场景基于低轨通信场景，对典型商业低轨卫星通信星座基本技术参数进行调研，将$TG_{MU\text{-}SAP}$设定为20 ms，$TG_{GS\text{-}NCC}$设定为10 ms。具体认证时延如表4所示。在计算开销部分，本文采用优化后的免配对无证书密钥分发技术，在相互认证过程中避免了双线性运算和模幂运算，与采用同类型的文献[17-20]方案相比，计算开销降低19.171 ms、6.269 ms、15.023 ms和6.646 ms。同时通过将区块链应用于注册时对密钥分发的监督，认证时仅进行查询比对操作，避免了区块链中耗时的上链带来的时延影响，对比同类型文献[9]方案，时延降低了60.032 ms。在传输时延部分，相比文献[16-18]方案而言，文献[9]方案避免了GS和NCC的传输时延，时延降低了20 ms。同时，由于采用SAP作为中间验证部分，相比文献[16-18]方案而言，本文方法以及文献[19-20]方案时延降低了60 ms。在总认证时延上，由于计算开销和传输时延均获得了最佳效果，因此本文方法的认证时延最低。

3) 切换验证时延

在切换验证时延部分，上述方案均未对切换策略进行额外研究，仅文献[19]在单卫星节点覆盖内的波束切换时采用了本地缓存查询的方式，而卫星节点以及基站切换时仍然采用无特殊设计的接入认证方案，因此本节主要对本文方法中高/低速切换认证机制的单次切换验证进行分析。由于切换的可预见性，在低速切换认证中，时延主要取决于C-SAP和N-SAP消息传输时延$TG_{SAP\text{-}SAP}$，无计算时延；在高速切换认证中，需重新进行验证，只是不需要额外初始化过程。具体切换验证时延如表5所示。

表 4　　认证时延

方案	计算开销/ms	传输时延/ms	认证时延/ms
文献[9]	$17TG_H + 22TG_{exp} + 6TG_{mul} + 2TG_{BC}(\approx 66.795)$	$4TG_{MU\text{-}SAP}(\approx 80)$	146.795
文献[16]	$2TG_H(\approx 0.014)$	$4TG_{MU\text{-}SAP}+2TG_{GS\text{-}NCC}(\approx 100)$	100.014
文献[17]	$6TG_H + 6TG_{mul} + 6TG_{exp} + 2TG_{add} + 2TG_{\hat{e}}(\approx 25.934)$	$4TG_{MU\text{-}SAP}+2TG_{GS\text{-}NCC}(\approx 100)$	125.934
文献[18]	$6TG_{mul} + 4TG_H + 2TG_{add}(\approx 13.032)$	$4TG_{MU\text{-}SAP}+2TG_{GS\text{-}NCC}(\approx 100)$	113.032
文献[19]	$6TG_{add} + 4TG_{\hat{e}} \approx (21.786)$	$2TG_{MU\text{-}SAP}(\approx 40)$	61.786
文献[20]	$2TG_H + TG_{mul} + TG_{exp} + 3TG_{add} + 2TG_{\hat{e}}(\approx 13.409)$	$2TG_{MU\text{-}SAP}(\approx 40)$	53.409
本文方法	$3TG_{mul} + 10TG_{add} + 12TG_H(\approx 6.763)$	$2TG_{MU\text{-}SAP}(\approx 40)$	46.763

表 5　　切换验证时延

机制	切换验证时延
低速切换验证	$TG_{SAP\text{-}SAP}$
高速切换验证	$3TG_{mul}+10TG_{add}+12TG_H+2TG_{MU\text{-}SAP}$

4) 批处理

在批处理阶段，SAP可能收到多个用户的切换请求，在不考虑无效切换请求的情况下，本文方法在执行批量身份验证时，能显著减少卫星的计算开销。通过分析处理单一身份验证、未使用批处理的 n 个身份验证和使用批处理的 n 个身份验证的计算成本，可知本文提出的批量身份验证机制能够有效减少计算成本，具体批处理开销分析如表 6 所示。未使用批处理的 n 个身份验证和使用批处理的 n 个身份验证的计算开销随请求数量增加的变化如图 5 所示。

表 6　　批处理开销

	批处理开销
单一身份验证	$3TG_{mul} + 10TG_{add} + 12TG_H$
n 个身份验证(未使用批处理)	$3nTG_{mul} + 10nTG_{add} + 12nTG_H$
n 个身份验证(使用批处理)	$2nTG_H + nTG_{\hat{e}} + nTG_{add} + TG_{mul}$

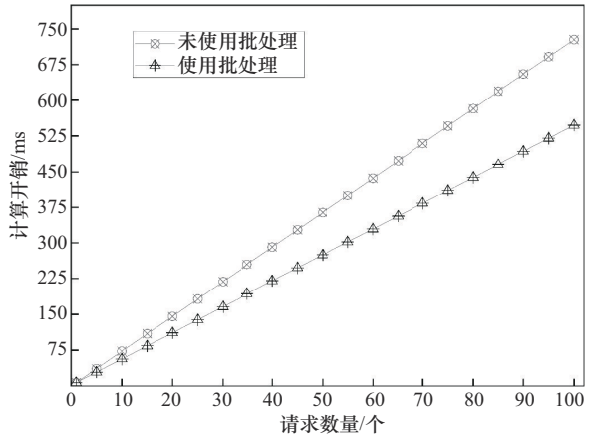

图 5　未使用批处理和使用批处理的身份验证计算开销

5　结束语

本文提出了面向空间信息网络的免配对无证书链上接入认证方法。该方法借助免配对的CL-PKC完成系统初始密钥分发过程，通过区块链技术构建星链通信模型，实现对初始密钥的加密储存以及对密钥分发中心的监督，保证了初始密钥分发过程的安全性。在星链通信模型下，借助智能合约实现了接入认证过程中可信环境的构建，通过免配对的CL-PKC以及ECC混合加密机制设计，并结合密钥交换实现了信息传输过程中会话密钥的安全性，保证了数据难以窃听、不可篡改和不可抵赖。此外，通过设计批处理机制以及ECC加密算法，在多用户场景下实现了高效切换。安全性分析与仿真实验结果表明，与现有的空间信息网络的接入认证方案相比，本文方法具有更低的信令开销、认证时延和批处理认证时延。

参考文献:

[1] 孟祥利, 吴玲达, 于少波, 等. 基于分层、分域控制的空间信息网络体系结构研究[J]. 中国电子科学研究院学报, 2019, 14(11): 1214-1220.
MENG X L, WU L D, YU S B, et al. Research on space information network architecture based on hierarchical and domain-based control[J]. Journal of China Academy of Electronics and Information Technology, 2019, 14(11): 1214-1220.

[2] CAO J, LI H, MA M D, et al. A simple and robust handover authentication between HeNB and eNB in LTE networks[J]. Computer Networks, 2012, 56(8): 2119-2131.

[3] FENG M, XU H. MSNET-blockchain: a new framework for securing mobile satellite communication network[C]//Proceedings of the 2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON). Piscataway: IEEE Press, 2019: 1-9.

[4] ANDROULAKI E, BARGER A, BORTNIKOV V, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains[C]// Proceedings of the Thirteenth EuroSys Conference. New York: ACM

Press, 2018: 1-15.

[5] IBRAHIM M H, KUMARI S, DAS A K, et al. Jamming resistant non-interactive anonymous and unlinkable authentication scheme for mobile satellite networks[J]. Security and Communication Networks, 2016, 9(18): 5563-5580.

[6] MENG W, XUE K P, XU J, et al. Low-latency authentication against satellite compromising for space information network[C]//Proceedings of the 2018 IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems (MASS). Piscataway: IEEE Press, 2018: 237-244.

[7] QI M P, CHEN J H, CHEN Y T. A secure authentication with key agreement scheme using ECC for satellite communication systems[J]. International Journal of Satellite Communications and Networking, 2019, 37(3): 234-244.

[8] 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.

[9] BOYEN X, HERATH U, MCKAGUE M, et al. Associative blockchain for decentralized PKI transparency[J]. Cryptography, 2021, 5(2): 14.

[10] LIU F, HE S H, LI Z H, et al. An overview of blockchain efficient interaction technologies[J]. Frontiers in Blockchain, 2023, 6: 996070.

[11] 刘峰, 杨杰, 李志斌, 等. 一种基于区块链的泛用型数据隐私保护的安全多方计算协议[J]. 计算机研究与发展, 2021, 58(2): 281-290.
LIU F, YANG J, LI Z B, et al. A secure multi-party computation protocol for universal data privacy protection based on blockchain[J]. Journal of Computer Research and Development, 2021, 58(2): 281-290.

[12] 刘峰, 王一帆, 杨杰, 等. 一种基于区块链的融合DKG与BLS的高阈值签名协议[J]. 计算机科学, 2021, 48(11): 46-53.
LIU F, WANG Y F, YANG J, et al. Blockchain-based high-threshold signature protocol integrating DKG and BLS[J]. Computer Science, 2021, 48(11): 46-53.

[13] BAO Z J, LUO M, WANG H Q, et al. Blockchain-based secure communication for space information networks[J]. IEEE Network, 2021, 35(4): 50-57.

[14] LI C J, ZHU L D, LUGLIO M, et al. Research on satellite network security mechanism based on blockchain technology[C]//Proceedings of the 2021 International Symposium on Networks, Computers and Communications (ISNCC). Piscataway: IEEE Press, 2021: 1-6.

[15] 崔新雨, 伍杰, 周一青, 等. 空天地一体化融合组网的挑战与关键技术[J]. 西安电子科技大学学报, 2023, 50(1): 1-11.
CUI X Y, WU J, ZHOU Y Q, et al. Challenges of and key technologies for the air-space-ground integrated network[J]. Journal of Xidian University, 2023, 50(1): 1-11.

[16] WEI S J, LI S, LIU P L, et al. BAVP: blockchain-based access verification protocol in LEO constellation using IBE keys[J]. Security and Communication Networks, 2018, 2018: 7202806.

[17] SHEN M, LIU H S, ZHU L H, et al. Blockchain-assisted secure device authentication for cross-domain industrial IoT[J]. IEEE Journal on Selected Areas in Communications, 2020, 38(5): 942-954.

[18] XIONG T, ZHANG R, LIU J, et al. A blockchain-based and privacy-preserved authentication scheme for inter-constellation collaboration in space-ground integrated networks[J]. Computer Networks, 2022, 206: 108793.

[19] WANG B Y, CHANG Z, LI S C, et al. An efficient and privacy-preserving blockchain-based authentication scheme for low earth orbit satellite-assisted Internet of things[J]. IEEE Transactions on Aerospace and Electronic Systems, 2022, 58(6): 5153-5164.

[20] WU Z J, LIANG C, ZHANG Y. Blockchain-based authentication of GNSS civil navigation message[J]. IEEE Transactions on Aerospace and Electronic Systems, 2023, 59(4): 4380-4392.

[作者简介]

霍如（1988– ），女，黑龙江哈尔滨人，博士，北京工业大学副教授，主要研究方向为未来网络、工业互联网、网络资源管理、区块链等。

王志浩（1997– ），男，安徽池州人，紫金山实验室工程师，主要研究方向为密码学、区块链、工业互联网、算力网络等。

邵子豪（1992– ），男，江苏南京人，博士，紫金山实验室研究员，主要研究方向为区块链、移动群智感知、工业互联网等。

黄韬（1980– ），男，重庆人，博士，北京邮电大学教授，主要研究方向为路由与交换、软件定义网络、空间信息网络、网络试验设施等。