面向天地一体化网络的终端可信接入认证与密钥协商协议

谢绒娜，周竞，张晨佳，史国振*
（北京电子科技学院，北京 100070）

摘要：面向天地一体化网络中低轨卫星星座具有低时延、高带宽等优势，成为地面终端接入天地一体化网络的核心载体。低轨卫星信道易受非法窃听与干扰、通信链路时断时续，如何实现用户终端可信接入低轨卫星网是当前亟待解决的问题。本文提出一种面向天地一体化网络的终端可信接入认证与密钥协商协议，实现终端用户与低轨卫星之间安全高效的双向认证与密钥协商。协议采用轻量级密码原语，由地面控制中心承担大部分计算任务，降低卫星的计算开销；设计伪身份和身份密码，提高用户终端隐私性；基于初次接入生成的认证参数，协助断线后卫星对用户终端快速认证，提高断线重认证的效率。利用ROR（Real-Or-Random）模型和Tamarin工具对协议进行形式化分析与验证，证明其具有更强的安全性和隐私保护性。性能分析表明，所提协议降低了通信与计算开销，相比现有方案通信效率明显提升，满足天地一体化网络的轻量级需求。

关键词：天地一体化网络；接入认证；断线重连；密钥协商；隐私保护

A Trusted Terminal Access Authentication and Key Agreement Protocol for Space-Air-Ground Integrated Networks

Xie Rongna, Zhou Jing, Zhang Chenjia, Shi Guozhen*
Beijing Electronic Science and Technology Institute, Beijing 100070, China

Abstract: Low Earth Orbit (LEO) satellite constellations feature low latency and high bandwidth, and have become the core carrier for ground terminals to access the integrated space-terrestrial network. Nevertheless, LEO satellite channels are vulnerable to illegal eavesdropping and jamming, and communication links frequently suffer from intermittent outages. Accordingly, enabling trusted access of user terminals to LEO satellite networks has become an urgent challenge to address. This paper proposes a terminal trusted access authentication and key agreement protocol for integrated space-terrestrial networks, which achieves secure and efficient mutual authentication and key agreement between user terminals and LEO satellites. The protocol adopts lightweight cryptographic primitives, and offloads most computational tasks to the ground control center to reduce the computing overhead of satellites. Pseudo-identities and identity passwords are designed to enhance the privacy of user terminals. In addition, the authentication parameters generated during the initial access are reused to support rapid terminal re-authentication after link disconnection, so as to improve the efficiency of re-authentication during reconnection. Formal security analysis and verification are conducted via the Real-Or-Random (ROR) model and the Tamarin prover. The results demonstrate that the proposed protocol achieves improved security and privacy protection. Performance evaluation shows that the protocol reduces communication and computational overhead and obtains a significant improvement in communication efficiency compared with existing schemes, which well satisfies the lightweight requirements of integrated space-terrestrial networks.

Key words: Space-air-ground integrated network, access authentication, re-authentication, key agreement, privacy preservation

收稿日期：2026–05–08；**修回日期：**2026–07–16
通信作者：史国振，1427980882@qq.com
基金项目：国家密码科学基金 (No.2025NCSF02028)；中央高校基本科研业务费基金(No.3282023008)
Foundation Items： National Cryptologic Science Fund of China（No. 2025NCSF02028); the Fundamental Research Funds for the Central Universities(No.3282023008)

0 引言

天地一体化网络由空间段与地面段深度融合构成，是支撑未来广域覆盖、全球互联和多样化业务的新型信息基础设施[1]。其中，低轨卫星（Low Earth Orbit , LEO）星座凭借低时延、高带宽、终端易小型化的独特优势，成为地面终端接入天地一体化网络的核心载体。然而，地面终端与低轨卫星接入点之间的通信链路高度动态、时延与抖动明显、信道开放易受窃听与篡改，同时星上计算与存储资源受限，使得终端可信接入、链路中断后的快速恢复面临严峻的安全与性能挑战。近年来，学术界提出了一系列天地一体化场景下的终端接入认证方案[2-3]，但是大多没有考虑通信中断导致的频繁接入认证问题。本文围绕上述问题，研究如何设计适用于天地一体化网络的终端接入认证与密钥协商协议。本文的主要贡献如下：

（1）采用轻量级密码原语和零知识证明，提出终端可信接入认证与密钥协商协议，实现地面终端与低轨卫星之间的安全高效认证。双方借助地面控制中心完成密钥协商过程，生成共享会话密钥，为后续双方安全会话提供保障。

（2）基于终端接入认证阶段构造快速认证参数，提出轻量级断线重认证协议实现无需重新执行完整接入认证的快速重连，提高了会话的连续性与可靠性。

（3）利用 ROR（Real-Or-Random）模型证明本文协议的安全性，借助 Tamarin 工具验证了协议隐私保护的有效性和安全性。实验仿真与性能评估表明，本文协议具有较低的计算开销和通信开销，适合资源受限的天地一体化环境。

1 相关工作

截止目前，学术界已经设计了大量针对天地一体化网络的认证方案，这些方案涉及多种密码体制和认证方式，为当前协议的设计、安全性提升和适用性增强提供了重要的借鉴意义。Zheng 等[4]针对卫星终端资源受限的特点，创新性地提出了仅依赖哈希函数与异或运算的轻量级认证方案，为低功耗卫星终端认证提供了可行思路。然而，Zhao 等[5]通过安全性分析指出，该方案在身份验证环节存在逻辑缺陷——攻击者可利用伪造的临时凭证绕过卫星中继的校验机制，实施假冒终端接入攻击，暴露了其抗伪造能力的不足。为弥补这一漏洞，Altaf 等[6]提出基于哈希链的改进方案，通过多轮哈希迭代增强身份凭证的时效性与不可伪造性；Xu 等[7]则转向公钥密码体系，利用非对称加密算法实现终端与地面网络的双向认证，试图通过数学难题提升安全性。但 Huang 等[8]与 Ostad-Sharif 等[9]后续研究表明，上述两种方案可能遭受暴力攻击。近年来，量子计算机的快速发展，传统密码体系面临根本性挑战。在此背景下，Kumar 等[10]与 Dharminder 等[11]率先将后量子密码学引入卫星认证领域，提出基于环上带错误学习问题（Ring-LWE）的认证协议，其安全假设在量子计算模型下仍被证明是可靠的，且算法可通过多项式环结构实现高效计算，适配卫星终端的资源约束。尽管上述方案在安全性上逐步提升，但共同局限在于依赖卫星作为“透明中继”。随着卫星计算和存储能力的逐步提升，一些利用卫星直接认证终端的方案逐渐被提出。Cao 等[12]首次提出针对双层卫星网络的认证架构，省去地面中心的参与环节，认证时延降低 60%。此后，Yi 等[13]与 Ma 等[14]进一步结合格密码技术，设计出全链路抗量子的直连认证方案，将单次认证的计算耗时压缩至微秒级。Guan 等[15]则另辟蹊径，引入区块链技术解决传统基于身份认证的密钥托管风险。该方案彻底摆脱地面中心依赖，平均认证时延降至 100ms 以内，但区块链的分布式共识机制带来额外的通信开销和计算开销，在低轨卫星星座的高动态拓扑下仍面临节点同步难题。

2 系统模型

2.1 系统框架

系统框架具体如图 1 所示，图中涉及三个实体：各类用户终端（User Terminal, UT）、低轨卫星 LEO 和地面控制中心（Networks Control Center, NCC）。由于天地一体化网络中星上计算资源紧张，处理能力受限，目前天地一体化网络中资源管理和安全防护都放在地面进行，卫星组网路由阶段大多都经过地面控制中心[16-17]。此外，星地无线链路开放暴露，极易遭受窃听、篡改、伪造及中间人攻击，对协议的轻量性与抗攻击能力提出了双重要求。

因此，本文协议采用星地协同的设计思想，依托地面控制中心完成核心密钥管理与可信支撑，有

效规避星上资源瓶颈，同时适配动态接入场景。

2.2　安全目标

面向天地一体化网络的终端可信接入认证协议是保障星地异构网络可信互联的核心安全机制，旨在实现域内身份认证、资源协同及服务连续性[18]。协议应满足以下安全要求：

（1）双向认证。终端、卫星及网络控制中心三方身份互信，确保通信主体身份合法可信，并支持高动态拓扑下快速、安全的重认证。

（2）身份隐私与可审计性。在保护终端身份隐私、防止长期追踪的同时，实现身份的可控追溯与审计，兼顾匿名性与监管可追溯需求。

（3）端到端数据保护。保障端到端数据传输的机密性与完整性，抵御中间人攻击，实现安全、高效的数据通信保护。

3　方案设计

本节提出了一种天地一体化网络中的终端可信接入认证协议，该方案包括系统初始化、实体注册、初始接入认证与密钥协商和断线重认证与密钥协商四个阶段。协议中部分符号设计如表1所示。

表1　　符号定义

符号	说明
ID	真实身份
TID	伪身份
q,G	大素数/基点
s、P_{pub}	系统私钥/公钥
(sk,PK)	公私钥对
K_{U-L},K_{L-U}	会话密钥
EXP_{time}	有效期
MAC	消息验证码
RE	认证返回值
Tag	快速认证标识
‖	连接运算
⊕	异或运算

3.1　系统初始化

本阶段由NCC完成系统安全参数的初始化配置，具体步骤如下：

Step1：选定椭圆曲线群，该群的阶为素数q，生成元为G。

Step2：生成随机数$s \in Z_q^*$作为系统的主私钥，计算系统公钥$P_{\text{pub}} = s \cdot G$。

Step3：选取抗碰撞的单向哈希函数H:$\{1,0\}^* -> Z_q^*$。向网络公开参数$\{q, G, H, P_{\text{pub}}\}$。

3.2　实体注册

本阶段中，用户终端（UT）与低轨卫星（LEO）需在地面控制中心（NCC）完成注册，整个注册流程通过安全信道执行，具体分为两个子阶段：

（1）用户终端注册阶段：

Step1：UT向NCC发送注册请求，包括真实身份标识ID_U。

Step2：NCC接收到注册请求后，选择随机数$sk_U \in Z_q^*$作为用户私钥，计算对应的用户公钥

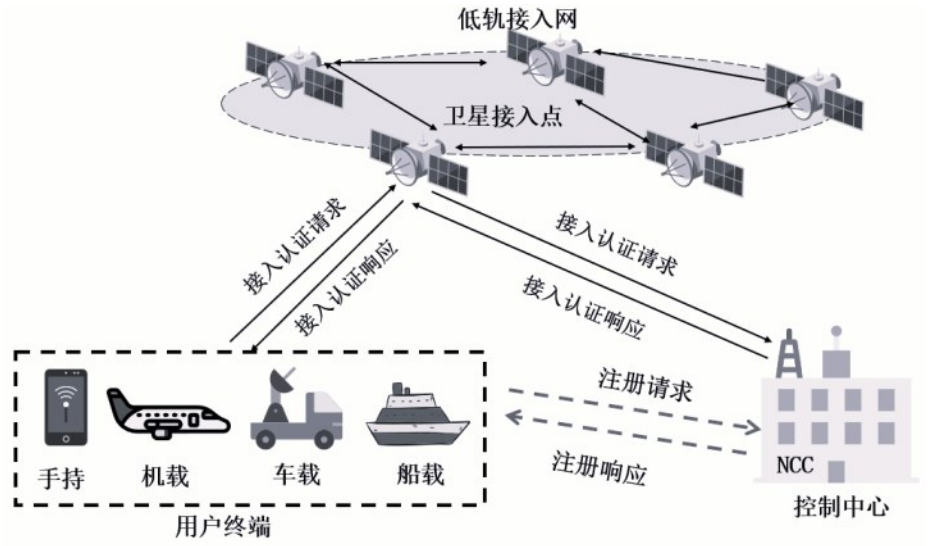

图1　系统框架

$PK_U = sk_U \cdot G$。生成用户密码 PW_U，向 UT 发送 $\{(sk_U, PK_U), PW_U\}$。

Step3：UT 在本地安全存储 $\{(sk_U, PK_U), PW_U\}$。

（2）低轨卫星接入点注册阶段：

Step1：LEO 向 NCC 发送注册请求，包括真实身份标识 ID_L。

Step2：NCC 接收到注册请求后，选择随机数 $sk_L \in Z_q^*$ 作为卫星私钥，计算对应的卫星公钥 $PK_L = sk_L \cdot G$。生成卫星密码 PW_L，向 LEO 发送 $\{(sk_L, PK_L), PW_L\}$。

Step3：LEO 在本地安全存储 $\{(sk_L, PK_L), PW_L\}$。

3.3　认证与密钥协商

本阶段面向终端首次接入低轨卫星网络的场景，完整流程如图2所示，具体步骤如下：

Step1：UT 获取当前时间戳 T_1，选择随机数 $r_U \in Z_q^*$ 作为临时私钥，计算 $R_U = r_U \cdot G$ 作为临时公钥。生成伪身份 $TID_U = ID_U \oplus H(sk_U \| T_1)$，计算消息验证码 $MAC_U = r_U + sk_U \cdot H(TID_U \| R_U \| PW_U \| T_1)$。向 LEO 发送请求消息 $M_1 = \{TID_U, R_U, T_1, MAC_U\}$。

Step2：LEO 收到 M_1 后，检查时间戳 T_1 的新鲜度，检验通过后获取当前时间戳 T_2，同时暂存 UT 的临时公钥 R_U。选择随机数 $r_L \in Z_q^*$ 作为临时私钥，计算 $R_L = r_L \cdot G$ 作为临时公钥。生成伪身份 $TID_U = ID_L \oplus H(sk_L \| T_2)$，计算消息验证码 $MAC_L = r_L + sk_L \cdot H(TID_L \| R_L \| PW_L \| T_2)$。将 $\{M_1, M_2\}$ 转发至 NCC，其中 $M_2 = \{TID_L, R_L, T_2, MAC_L\}$。

Step3：NCC 收到消息后，检查时间戳 T_1、T_2 的新鲜度，检验通过后获取当前时间戳 T_3。计算 $ID_U' = TID_U \oplus H(sk_U \| T_1)$、$ID_L' = TID_L \oplus H(sk_L \| T_2)$，通过将 ID_U' 和 ID_L' 与真实身份对比验证合法性。根据身份标识查找对应的密码 PW_U 和 PW_L，计算 $MAC_U \cdot G \stackrel{?}{=} R_U + PK_U \cdot H(TID_U \| R_U \| PW_U \| T_1)$、$MAC_L \cdot G \stackrel{?}{=} R_L + PK_L \cdot H(TID_L \| R_L \| PW_L \| T_2)$ 对消息完整性进行验证。身份认证后，NCC 选择随机数 $r_N \in Z_q^*$ 作为临时私钥，计算 $R_N = r_N \cdot G$ 作为临时公钥；分别生成卫星和用户终端的认证返回值 $RE_L = r_N \cdot PK_L + s \cdot R_L$ 和 $RE_U = r_N \cdot PK_U + s \cdot R_U$。

为提高用户断线后重连效率，初次接入认证时 NCC 同步生成快速认证参数。令 $a = TID_U \| TID_L$，计算 $b = H(a \| R_N)$、$c = r_N + b \cdot s$。NCC 计算保护参数 $d = c \oplus r_N$ 和中介参数 $e = r_N \oplus sk_U$，设定 EXP_{time} 为快速认证参数有效期。构造响应消息 $M_3 = \{PK_U, R_N, T_3, RE_L\}$、$M_4 = \{TID_L, PK_L, R_L, R_N, d, e, T_3, EXP_{time}, RE_U\}$ 并向 LEO 发送。

Step4：LEO 收到消息后，检查时间戳 T_3 的新鲜度，检验通过后获取当前时间戳 T_4。计算认证返回值 $RE_L' = r_L \cdot P_{pub} + sk_L \cdot R_N$，计算 $RE_L' \stackrel{?}{=} RE_L$ 验证 NCC 的身份。认证通过后 LEO 计算会话参数

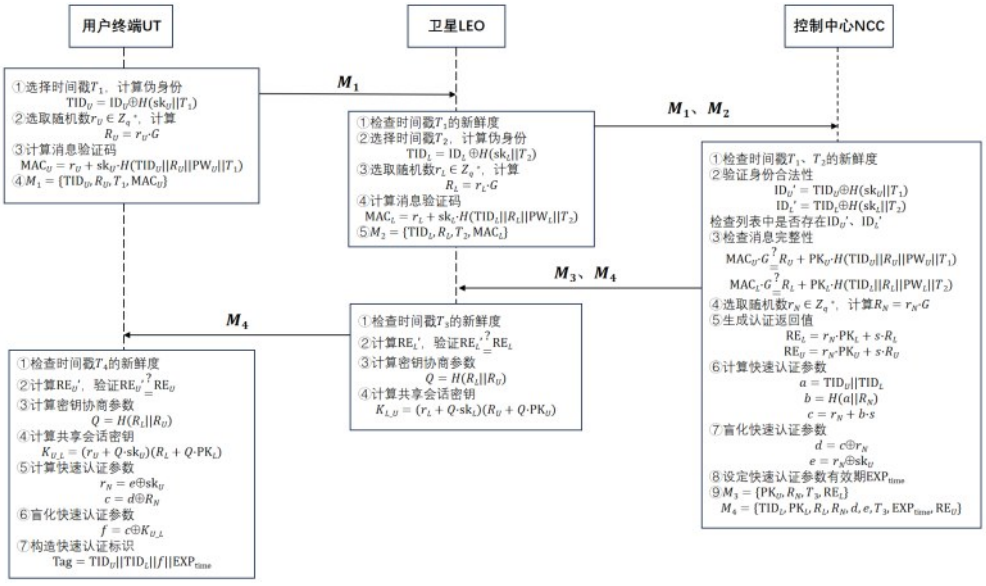

图2　初始接入认证与密钥协商

$Q = H(R_L \| R_U)$，计算共享会话密钥 $K_{L-U} = (r_L + Q \cdot \mathrm{sk}_L)(R_U + Q \cdot \mathrm{PK}_U)$。LEO 存储 $\{\mathrm{TID}_U, P_{\mathrm{pub}}\}$，在参数有效期内暂存 $\{K_{L-U}, R_N\}$，并向 UT 转发 M_4。

Step5：UT 收到 M_4 后，检查时间戳 T_4 的新鲜度，检验通过后计算认证返回值 $\mathrm{RE}_U' = r_U \cdot P_{\mathrm{pub}} + \mathrm{sk}_U \cdot R_N$，计算 $\mathrm{RE}_U' \stackrel{?}{=} \mathrm{RE}_U$ 验证 NCC 的身份。认证通过后 UT 计算会话参数 $Q = H(R_L \| R_U)$，得到共享会话密钥 $K_{U-L} = (r_U + Q \cdot \mathrm{sk}_U)(R_L + Q \cdot \mathrm{PK}_L)$。根据参数 d、e 计算快速认证参数 c，计算保护参数 $f = c \oplus K_{U-L}$。构造快速认证标识 $\mathrm{Tag} = \mathrm{TID}_U \| \mathrm{TID}_L \| f \| \mathrm{EXP}_{\mathrm{time}}$ 用于后续断线重认证。

3.4　断线重认证与密钥协商

星地链路处于开放暴露状态，易遭受安全威胁，在链路发生异常中断后，星地双方依托预存储的快速认证参数，完成轻量级的身份认证与会话密钥协商，确保高动态断连场景下协议安全属性，提高协议的效率。完整流程如图 3 所示，具体步骤如下：

Step1：UT 获取当前时间戳 T_1，生成随机数 $r_1 \in Z_q^*$ 作为重连会话的临时私钥，计算对应的临时公钥 $R_1 = r_1 \cdot G$。向 LEO 发送重连请求信息 $M_1 = \{\mathrm{TID}_U, R_1, T_1, \mathrm{Tag}\}$，触发重认证流程。

Step2：LEO 收到 M_1 后，检查时间戳 T_1 的新鲜度，检验通过后获取当前时间戳 T_2。验证快速认证标识 Tag 中的有效期，检验通过后恢复出快速认证参数 $c = f \oplus K_{L-U}$，计算 $c \cdot G \stackrel{?}{=} R_N + H(\mathrm{TID}_U \| \mathrm{TID}_L \| R_N) \cdot P_{\mathrm{pub}}$ 验证用户终端的身份。

生成随机数 $r_2 \in Z_q^*$ 作为临时私钥，计算对应的临时公钥 $R_2 = r_2 \cdot G$。更新快速认证参数和共享会话密钥：计算 $b' = H(\mathrm{TID}_U \| \mathrm{TID}_L \| R_2)$，得到 $c' = r_2 + b' \cdot \mathrm{sk}_L$ 和 $K_{L-U}' = H(K_{L-U}, r_2 R_1)$。计算保护参数 $d' = c' \oplus K_{L-U}'$，计算消息验证码 $\mathrm{MAC} = H(K_{L-U}', T_2) \oplus c$。构造响应消息 $M_2 = \{\mathrm{TID}_L, R_2, d', T_2, \mathrm{MAC}\}$ 并发送至 UT。

Step3：UT 收到 M_2 后，检查时间戳 T_2 的新鲜度，检验通过后计算更新后的共享会话密钥 $K_{U-L}' = H(K_{U-L}, r_1 R_2)$。计算消息验证码 $\mathrm{MAC}_? = H(K_{U-L}', T_2) \oplus c$ 验证消息的完整性。LEO 恢复出更新后的快速认证参数 $c' = d' \oplus K_{U-L}'$，同时计算保护参数 $f' = c' \oplus K_{U-L}'$。更新快速认证标识 $\mathrm{Tag}' = \mathrm{TID}_U \| \mathrm{TID}_L \| f' \| \mathrm{EXP}_{\mathrm{time}}$。并用新的快速认证参数 c'、d'、f' 替换原有的认证参数 c、d、f，新快速认证标识 Tag' 替换原有的快速认证标识 Tag、新的共享会话密钥 K_{U-L}' 替换共享会话密钥 K_{U-L}。

每次断线重连都生成新的随机数 r_1、r_2，并更新认证参数和快速认证标识，以及用户和卫星之间的共享会话密钥 K_{U-L}，提高了抵抗重放攻击的能力。

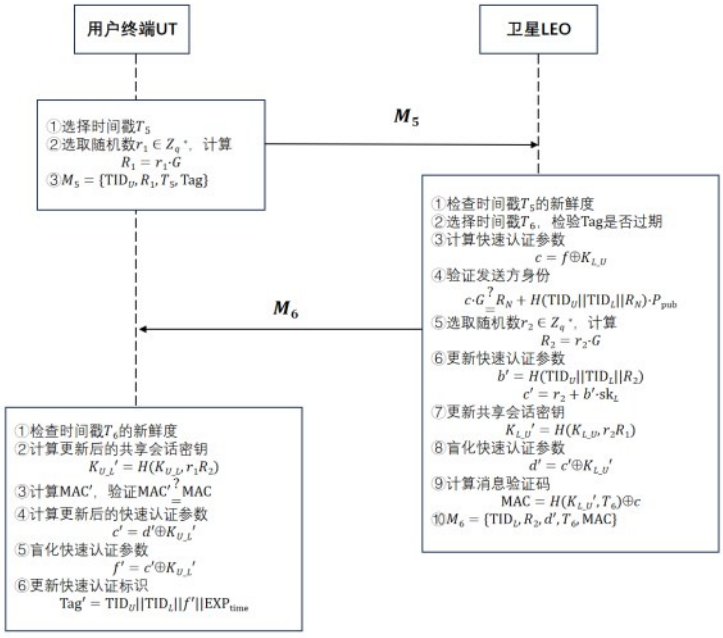

图3　断线重认证与密钥协商

4 安全性分析

4.1 基于ROR的形式化证明

本小节使用ROR（Real-Or-Random）模型来分析评估提出的认证与密钥协商协议是可证明安全的。协议涉及三个参与实体：发起方终端A、响应方卫星B和地面控制中心NCC。使用Π_U^i表示参与者U的第i个协议实例，其中$U \in S_A, S_B,$ NCC。每个实例在协议执行过程中维护自身的内部状态，攻击者A通过以下查询与协议交互：

Execute$(\Pi_A^i,\Pi_{AAS}^k,\Pi_B^j)$：A窃听并记录该会话在星地链路上传输的所有消息。

Send(Π_U^i,m)：A向实例Π_U^i发送消息m并接收响应，以此模拟伪造、重放或篡改攻击。

Hash(m): A输入消息m，若列表中已有记录则返回对应哈希值，否则返回一个新的随机值。

Reveal(Π_U^i): A获得该实例当前已生成的会话密钥SK_{AB}。

Corrupt(U): 模拟设备物理俘获或内部攻击，若A执行此询问能窃取到U设备内存中所有的秘密参数。此查询不泄露当前未结束会话中的临时随机数。

Test(Π_U^i): 用于检验会话密钥的不可区分性。预言机抛掷一枚硬币$b \in \{0,1\}$。若$b=1$，返回真实的会话密钥sk_{AB}；若$b=0$，返回与sk_{AB}等长的随机字符串。

定理4.1 假设A是在多项式时间t内攻击本文提出的方案的敌手。那么，敌手A在推导U^α和L^β之间的共享会话密钥K_{U-L}和K_{L-U}的优势可以估计为：

$$Adv_P^{ake}(\ ) \leqslant \frac{q_h^2}{2^{l_{hash}}} + \frac{(q_{send}+q_h)^2}{2^{l_{nonce}}} \#(1)$$

其中l_{hash}为哈希输出长度，l_{nonce}为随机数长度，q_{send}和q_h分别为*Send*和*Hash*查询次数。

证明： 本方案将设计序列游戏$Game_0 \sim Game_5$来模拟攻击过程。设$Succ_i$为攻击者A在$Game_i$中赢得*Test*()查询的事件。

***Game*$_0$：** ROR模型下的初始游戏，完全模拟攻击者在真实网络环境下的攻击行为。该游戏成功的概率与方案无法抵抗敌手A攻击的概率是一致的。通过语义安全的定义得到如下公式：

$$Adv_P^{ake}(\ ) = \left|2 \cdot Pr[Succ_0] - 1\right| \#(2)$$

***Game*$_1$：** 在此游戏中，A执行*Execute*()查询以被动窃听信道上的所有消息。在UT、LEO、NCC之间通信的消息如下：

Msg1. UT—>LEO：$\{TID_U, R_U, T_1, MAC_U\}$

Msg2. LEO—>NCC：$\{M_2, TID_L, R_L, T_2, MAC_L\}$

Msg3. NCC—>LEO：$\{PK_U, R_N, T_3, RE_L\}$

Msg4. LEO—>UT：$\{TID_L, PK_L, R_L, R_N, d, e, T_3, EXP_{time}, RE_U\}$

消息可以被敌手A读取或拦截，A执行*Test*()查询以检查输出是会话密钥还是随机值。由于A未执行任何主动查询且不知晓任何主密钥，因此，A从窃听中获得的信息不足以区分真实密钥与随机数，其获胜概率与$Game_0$相同：

$$\left|Pr[Succ_1] - Pr[Succ_0]\right| = 0 \#(3)$$

***Game*$_2$：** 模拟*Send*()和*Hash*()查询，排除哈希碰撞和随机数碰撞对安全性的干扰。这轮游戏被视为主动攻击，其中敌手A试图欺骗参与者相信已被篡改或伪造的消息。与在本文提出的方案中，消息{□□□1, □□□2, □□□3, □□□4}与当前时间戳、随机数和参与者身份相关联，因此它们是新鲜的。即使敌手使用篡改或伪造的消息连续执行*Hash*()查询，这些查询中的目标消息也不会发生冲突。因此，基于生日悖论，有如下关系：

$$\left|Pr[Succ_2] - Pr[Succ_1]\right| \leqslant \frac{q_h^2}{2^{l_{hash}}} + \frac{(q_{send}+q_h)^2}{2^{l_{nonce}}} \#(4)$$

***Game*$_3$:** 此游戏模拟设备物理俘获场景，假设敌手A在目标会话结束后执行$Corrupt(S_A)$查询，那么在这轮游戏中，A可以从UT获得所有秘密参数$\{r_U, sk_U, ID_U, c\}$。另外，如果A可以从$\{R_U = r_U \cdot G, PK_U = sk_U \cdot G, TID_U = ID_U \oplus H(sk_U \| T_1), c = r_N + b \cdot s\}$中猜测出用户的秘密参数，那么只有知道共享会话密钥$K_{U-L}$和系统私钥$s$才能实现。而且A可以试图使用物理俘获攻击从卫星接入点LEO中获取秘密参数$\{sk_L, r_L\}$，但通过*Send*()查询从LEO处的秘密参数恢复会话密钥在计算上是不可行的。这证明即使设备被俘获，历史会话密钥依然是安全的：

$$\left|Pr[Succ_3] - Pr[Succ_2]\right| \approx 0 \#(5)$$

***Game*$_4$:** 模拟地面站被攻破或内部恶意卫星的场景，假设A执行*Corrupt*(NCC)，获得卫星接入

点的长期密钥 sk_L，此时 A 可以解密 LEO 与 NCC 的消息并获得 ID_L。但若 A 想计算最终双方的共享会话密钥，须获取星地链路上的随机数 r_L。在消息 M_2 中，r_L 可通过 $R_L \cdot G$ 或 $MAC_L = r_L + sk_L \cdot H(TID_L \| R_L \| PW_L \| T_2)$ 获取，由于密码 PW_L 是在注册阶段离线预置在卫星中的，A 无法获得此凭证，因此无法计算 K_{L-U}。实现对地面站信任的解耦。

$$\left| Pr[Succ_4] - Pr[Succ_3] \right| = 0\#(6)$$

***Game*$_5$:** 在排除上述所有攻击手段后，A 面对 *Test*() 查询时，由于始终缺少计算共享会话密钥的必要参数，他所拥有的信息与随机数在统计上是不可区分的。A 赢得游戏的概率为：

$$Pr[Succ_5] = 1/2\#(7)$$

综合上述公式(1)至(6)，利用三角不等式 $|a \pm b| \leqslant |a| + |b|$ 累加各游戏的优势差，得到：

$$Adv_P^{ake}(A) \leqslant 2 \cdot \left(\frac{q_h^2}{2^{l_{hash}}} + \frac{(q_{send} + q_h)^2}{2^{l_{nonce}}} \right) \#(8)$$

哈希长度 l_{hash} 和随机数长度 l_{nonce} 足够大，该优势是可忽略的。证毕。

4.2　基于 Tamarin 的安全证明

本文的实验平台为 Ubuntu22.04 操作系统，使用的是 Tamarin1.12.0 版本。Tamarin 中对协议安全引理的证明将通过 autoprove 自动进行，Tamarin 会根据已有的规则判断是否存在反例，若不存在则证明正确，标记为绿色，若存在，则标记为红色并在约束系统中展示反例存在的路径。图 4 为协议构建的四个安全引理的证明，包括身份隐私的保护、会话密钥的机密性、断线重连的前提等。下面展示协议中一个安全引理的关键建模过程：

当 UT 与 LEO 完成初始接入认证后，应能协商出共享会话密钥；且若在某时刻建立了共享会话密钥，则在此前必然已发生对应的 UT_Completed (ID_U, ID_L)，即完成认证是建立会话密钥的前提。示例如下：

```
lemma SessionKey_Established:
exists-trace
"Ex ID_U ID_L K #i #j.
SessionKey(ID_U, ID_L, K) @ #i &
UT_Completed(ID_U, ID_L) @ #j &
#j < #i"
```

结果证协议中的各参与实体能够正确解析消息、同步更新密钥、安全保存参数，不存在协议死锁或参数类型不匹配的问题。

4.3　非形式化安全证明

本小节将从以下几方面进行安全性分析。

（1）双向认证。以 LEO 与 NCC 之间的认证为例，LEO 利用私钥计算出消息验证码 MAC，NCC 利用公钥计算其发送的 MAC 是否等于 $R_L + PK_L \cdot H(TID_L \| R_L \| PW_L \| T_2)$ 判断身份合法性。而 NCC 发送认证返回值 RE_L，LEO 计算其是否等于 $r_L \cdot P_{pub} + sk_L \cdot R_N$ 判断身份合法性，以此实现对 NCC 的认证。

（2）前向后向安全性。UT 和 LEO 通过 $(r_L + Q \cdot sk_L)(r_U + Q \cdot sk_U) \cdot G$ 建立会话密钥。由于每次建立会话密钥所使用的随机数 r_L 和 r_U 都是独立生成，因此不同会话之间建立的会话密钥没有直接关联，

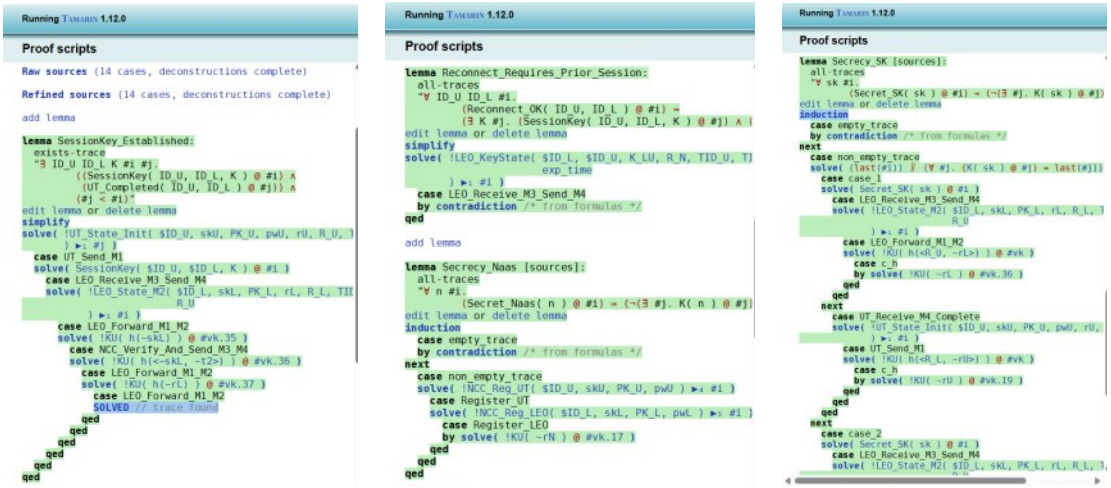

图4　安全引理自动化验证结果

实现了前向后向安全性。

（3）抵抗中间人攻击。UT、LEO 发送的消息 M_1 和 M_2 包含伪身份 TID_U、TID_L 和消息验证码 MAC_U、MAC_L，以修改消息 $M_1=\{\mathrm{TID}_U, R_U, T_1, \mathrm{MAC}_U\}$ 为例，敌手 A 伪造 UT 的临时私钥 r_U'、长期私钥 sk_U' 和密码 PW_U'，计算 $\mathrm{MAC}_U' = r_U' + \mathrm{sk}_U' \cdot H(\mathrm{TID}_U \| R_U \| \mathrm{PW}_U' \| T_1)$。由于临时私钥为随机数，而长期私钥和密码基于注册阶段获得，敌手 A 无法获取，因此敌手 A 计算的 $\mathrm{MAC}_U' \neq \mathrm{MAC}_U$，无法通过 NCC 的认证。故本协议可以抵抗中间人攻击。

（4）抵抗拒绝服务攻击

接收方需要通过消息中的消息验证码 MAC 或认证返回值 RE 计算哈希值进行完整性和间接的身份认证，如 NCC 对 MAC_U 和 MAC_L 的验证、用户终端 UT 和卫星 LEO 对 RE_U 和 RE_L 的验证，使得响应节点能够在协议执行过程中拒绝来自敌手 A 的非法请求，从而有效抵御拒绝服务攻击。

5　性能分析

本节将所提协议与基于 ECC 的协议[8]、基于哈希函数的协议[11]和基于对称密码体制的协议[12]进行安全特性、计算开销、通信开销和时延开销四个方面的性能对比分析。通过与同类协议的比较，证明了本协议适用天地一体化网络中的终端接入认证。

5.1　安全特性

本小节从双向认证等 7 个方面将所提方案中的初始接入认证和断线重连阶段与文献[8,11-12]进行对比，如表 3 和表 4 所示。

表 3　　初始接入认证安全性对比

安全特性	[8]	[11]	[12]	本协议
双向认证	√	√	√	√
身份隐私保护	√	√	√	√
前向后向安全性	×	√	√	√
抵抗中间人攻击	×	×	√	√
抵抗假冒攻击	×	√	×	√
抵抗重放攻击	√	√	√	√
抵抗拒绝服务攻击	√	×	×	√

结果表明，文献[8,11-12]在初始接入认证阶段可以满足大部分安全属性，但不能完全抵抗所有攻击；在断线重连阶段则安全性较差，而本文提出的协议在两个阶段均能够满足表中所述的安全属性要求或抵抗相应攻击，特别是在抵抗中间人攻击、拒绝服务攻击 2 个方面。

表 4　　断线重连安全性对比

安全特性	[8]	[11]	[12]	本协议
双向认证	√	√	√	√
身份隐私保护	√	√	√	√
前向后向安全性	×	√	√	√
抵抗中间人攻击	×	×	√	√
抵抗假冒攻击	×	√	×	√
抵抗重放攻击	√	√	√	√
抵抗拒绝服务攻击	√	×	×	√

5.2　计算开销

本文实验环境操作系统为 Ubuntu 18.04.6 64 bit，在 VMware 虚拟机运行，运行内存为 4GB。硬件环境为 Intel(R) Core(TM) i5-10210U 1.60GHz。随机模拟 1000 次不同密码运行操作进行分析，模拟得出协议中所涉及的密码学运算耗时如表 5 所示（忽略异或运算和级联运算耗时）。

表 5　　密码学运算耗时

运算	T_{h}	T_{mul}	T_{sym}	T_{ecm}	T_{eca}
开销/ms	0.0023	0.0053	0.0046	2.226	0.0288

使用表 5 中的密码学操作执行时间计算本文提出的终端初始接入认证及断线重认证与文献[8,11-12]中相同两个阶段的计算开销进行对比，详情如表 6 及图 5 所示。

文献[8]设计的方案在初始接入认证阶段所需开销较大，因为其频繁使用复杂的双线性对运算，增加了计算量。而本方案在初始接入认证阶段的计算开销略高于文献[11]，这是因为多花费了 1 次椭圆曲线标量乘法，计算出了快速认证参数，能更安全便捷地实现后续断线重连过程。在断线重认证阶段，本方案利用快速认证参数完成双向认证，不再需要 NCC 参与计算，因此计算开销比所有方案都更低。

5.3　通信开销

设定所有方案涉及的同类通信开销大小一致，

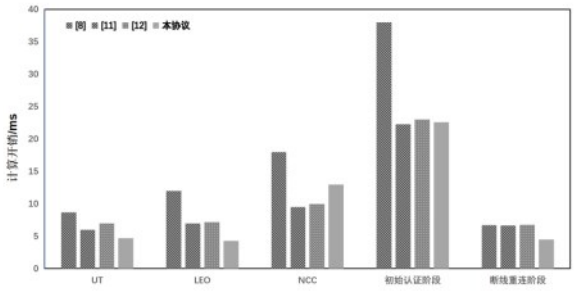

图5　协议计算开销对比

使用元数据的长度如表7所示。

使用表7中的元数据通信长度，计算本文提出的终端初始接入认证阶段及断线重认证通信开销，并与文献[8,11-12]中提出的方案通信开销进行对比，结果见表8和图6。本协议在初始接入认证阶段总的通信开销略高于文献[11]和[12]的方案，相较于这二者而言，协议在初始接入认证阶段传递的消息中包含了快速认证参数的协商信息，该参数为后续安全快捷地实现断线重认证提供基础。在断线重认证阶段，LEO只需要验证快速认证参数即可实现相互验证，该阶段的总通信开销远小于其他方案。

5.4　时延开销

天地一体化网络实际场景中，星地无线传输存在传播时延、NCC跨网转发引入额外排队时延，卫星切换产生状态同步开销。本小节结合低轨卫星典型轨道参数、天地一体化组网工程实测参数，量化协议总时延为：

$$T_{total} = T_{calc} + N \cdot T_{prop} + T_{NCC} + T_{sync} \#(9)$$

其中 T_{calc} 为星载处理器运算时延，T_{prop} 为星地传播时延，T_{NCC} 为NCC排队转发时延，T_{sync} 为参数同步时延，N 为交互轮次，T_{calc}' 为5.2小节计算的桌面处理器计算开销，具体开销如表9所示。

根据公式9和表9的数据，计算本文提出的终端初始接入认证及断线重认证总时延开销，并与文献[8,11-12]进行对比，结果见表10和图7。本协议在认证时延上的优势主要体现在断线重连阶段，由于提前预置了快速认证参数，无需NCC参与认证，减少了消息交互轮次，避免了NCC转发时延，降低了通信实体的运算量。

根据LEO轨道参数标准[19]，单星有效通信窗口约764s，本文方案时延开销远低于链路可用时长，可在链路失效前完成密钥协商。综合来看，天地一体化网络中终端断线重连为高频业务，本方案在高频场景时延优势抵消初次接入微小开销，整体满足LEO卫星高动态、链路时变、资源受限的轻量化部署需求。

6　结束语

本文针对天地一体化网络中终端与卫星接入点的可信接入认证、断线重认证效率及通信与计算开销优化的问题，提出了一种终端可信接入认证与密钥协商协议。本文协议轻量级密码原语和零知识证明，实现了终端与卫星的双向身份认证、会话密钥协商，同时实现了用户身份隐私与通信数据的安全保护。NCC作为半可信第三方，通过初始认证阶段完成终端与卫星的间接身份认证并生成快速认证参数，实现了断线场景下快速重认证，有效降低了协议的整体通信与计算负担。通过ROR模型和Tamarin形式化验证工具，证明了协议在初次接入认证、会话密钥协商及断线重连场景下的安全性。实验与分析结果表明，本文协议在计算与通信上的综合开销较低，总体认证时延较少，能够在保证高安全特性的同时显著降低系统开销，适配天地一体化网络的动态接入需求。

表6　协议计算开销对比

协议	初始接入认证阶段			初始认证阶段/ms	断线重连阶段/ms
	UT/ms	LEO/ms	NCC/ms		
[8]	$7T_h+4T_{ecm}$	$5T_h+T_{eca}+5T_{ecm}$	$10T_h+3T_{eca}+8T_{ecm}$	$22T_h+4T_{eca}+17T_{ecm}$=38.0078	$4T_h+2T_{eca}+3T_{ecm}$ =6.7448
[11]	$6T_h+2T_{sym}+3T_{ecm}$	$4T_h+1T_{sym}+3T_{ecm}$	$9T_h+2T_{sym}+4T_{ecm}$	$19T_h+5T_{sym}+10T_{ecm}$=22.3267	$4T_h+2T_{sym}+3T_{ecm}$ =6.6964
[12]	$2T_h+2T_{eca}+3T_{ecm}$	$2T_h+2T_{eca}+3T_{ecm}$	$5T_h+2T_c+3T_{ecm}$	$9T_h+4T_{eca}+2T_c+9T_{ecm}$=23.0799	$2T_h+2T_{sym}+2T_{eca}+3T_{ecm}$=6.7494
本协议	$4T_h+4T_{eca}+2T_{ecm}$	$4T_h+2T_{eca}+2T_{ecm}$	$6T_h+4T_{eca}+6T_{ecm}$	$14T_h+10T_{eca}+10T_{ecm}$=22.5802	$2T_h+2T_{eca}+2T_{ecm}$ =4.5142

表 7　　元数据长度

元数据	L_{id}	L_h	L_t	L_p	L_n	L_c	L_{ecm}	L_{sym}
长度/bit	32	160	32	512	512	480	320	256

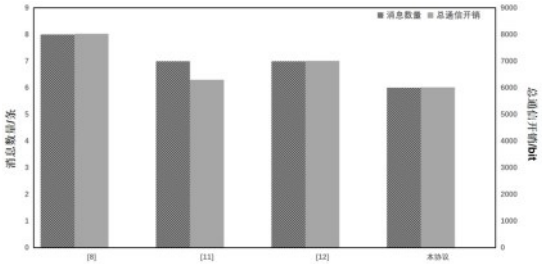

图 6　协议通信开销对比

表 8　　协议通信开销对比

协议	消息数量/条		总通信开销/bit		
	初始接入		断线重连	初始接入	断线重连
[8]	5	3	$5L_{id}+5L_t+2L_{ecm}+8L_n=5568$		$5L_{id}+2L_h+2L_{sym}+6L_t+4L_{ecm}=2464$
[11]	4	3	$7L_{id}+6L_h+4L_t+8L_{ecm}=4256$		$3L_{id}+4L_h+2L_{sym}+4L_t+2L_{ecm}=2016$
[12]	4	3	$4L_{id}+8L_h+5L_t+2L_p+6L_{ecm}=4512$		$4L_{id}+2L_h+4L_t+6L_{ecm}=2496$
本协议	4	2	$3L_{id}+7L_h+5L_t+10L_{ecm}=4576$		$2L_{id}+2L_t+4L_{ecm}=1436$

表9　　时延取值

时延	T_{calc}	T_{prop}	T_{NCC}	T_{sync}
开销/ms	$3.2T_{calc}'$	3.66	5.5	4

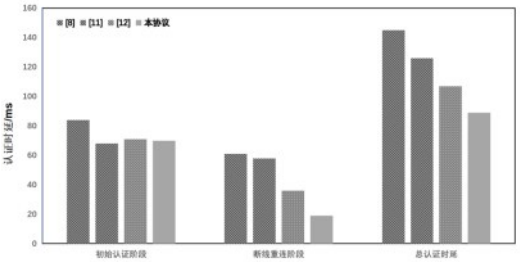

图7　协议时延开销对比

表10　　时延开销对比

协议	初始接入认证阶段/ms	断线重连阶段/ms	总认证时延/ms
[8]	$38.4T_{h}+7.2T_{eca}+27.8T_{ecm}+5T_{prop}+T_{NCC}$	$8.4T_{h}+2T_{eca}+17.4T_{ecm}+3T_{prop}+T_{NCC}+T_{sync}$	$46.8T_{h}+9.2T_{eca}+45.2T_{ecm}+8T_{prop}+2T_{NCC}+T_{sync}=145.2678$
[11]	$41T_{h}+11.6T_{sym}+21.2T_{ecm}+4T_{prop}+T_{NCC}$	$8.4T_{h}+2T_{sym}+17.4T_{ecm}+3T_{prop}+T_{NCC}+T_{sync}$	$49.4T_{h}+13.6T_{sym}+38.6T_{ecm}+7T_{prop}+2T_{NCC}+T_{sync}=126.7198$
[12]	$17.8T_{h}+12.8T_{eca}+2T_{c}+22.2T_{ecm}+4T_{prop}+T_{NCC}$	$2T_{h}+6.4T_{sym}+4.2T_{eca}+7.4T_{ecm}+3T_{prop}+T_{NCC}+T_{sync}$	$19.8T_{h}+6.4T_{sym}+17T_{eca}+29.6T_{ecm}+2T_{c}+7T_{prop}+2T_{NCC}+T_{sync}=107.0742$
本协议	$31.6T_{h}+23.2T_{eca}+22.2T_{ecm}+4T_{prop}+T_{NCC}$	$6.4T_{h}+6.4T_{eca}+3.2T_{ecm}+2T_{prop}+T_{sync}$	$38T_{h}+29.6T_{eca}+25.4T_{ecm}+6T_{prop}+T_{NCC}+T_{sync}=88.9351$

参考文献：

[1] 李凤华, 殷丽华, 吴巍, 等. 天地一体化信息网络安全保障技术研究进展及发展趋势[J]. 通信学报, 2016, 37(11): 156-168.

[2] 李贺武，吴茜，徐恪，等. 天地一体化网络研究进展与趋势 [J]. 科技导报，2016, 34 (14): 95-106.

[3] 谢绒娜, 谭莉, 武佳卉, 等. 面向天地一体化网络的认证与密钥协商协议[J]. 密码学报, 2023, 10(5): 1035-1051.

[4] Zheng G, Ma H T, Cheng C, et al. Design and logical analysis on the access authentication scheme for satellite mobile communication networks [J]. IET Information Security, 2012, 6(1): 6-13.

[5] Zhao W, Zhang A, Li J, et al. Analysis and design of an authentication protocol for space information network[C]//MILCOM 2016 IEEE Military Communications Conference. Baltimore, MD: IEEE, 2016: 43-48.

[6] Altaf I, Saleem M A, Mahmood K, et al. A lightweight key agreement and authentication scheme for satellite communication systems[J]. IEEE Access, 2020, 8: 46278-46287.

[7] Xu S, Liu X, Ma M, et al. An improved mutual authentication protocol based on perfect forward secrecy for satellite communications[J]. International Journal of Satellite Communications and Networking, 2020, 38 (1): 62-73.

[8] Huang H, Miao X, Wu Z, et al. An efficient ECC-based authentication scheme against clock asynchronous for spatial information network[J]. Mathematical Problems in Engineering, 2021: 1-14.

[9] Ostad-sharif A, Abbasinezhad-mood D, Nikooghadam M. Efficient utilization of elliptic curve cryptography in design of a three-factor authentication protocol for satellite communications[J]. Computer Communications, 2019, 147: 85-97.

[10] 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.

[11] Dharminder D, Dadsena P K, Gupta P, et al. A post quantum secure construction of an authentication protocol for satellite communication [J]. International Journal of Satellite Communications and Networking, 2023, 41(1): 14-28.

[12] Cao J, Shi X P, Ma R H, et al. Fusion of satellite-ground and inter-satellite AKA protocols for double-layer satellite networks[J]. Chinese Journal of Network and Information Security, 2023, 9(1): 18-31. doi: 10.11959/j.issn.2096-109x.2023004.

[13] Yi Z, Du X, Liao Y, et al. An access authentication algorithm based on a hierarchical identity-based signature over lattice for the space-ground integrated network[C]//2019 International Conference on Advanced Communication Technologies and Networking (CommNet). Rabat, Morocco: IEEE, 2019: 1-9.

[14] Ma R, Cao J, Feng D, et al. LAA: lattice-based access authentication scheme for IoT in space information networks[J]. IEEE Internet of Things Journal, 2019, 7(4): 2791-2805.

[15] Guan J, Wu Y, Yao S, et al. BSLA: blockchain-assisted secure and lightweight authentication for SGIN[J]. Computer Communications, 2021, 176: 46-55.

[16] Cascudo I, Cozzo D, Giunta E. Verifiable secret sharing from symmetric key cryptography with improved optimistic complexity[C]//Advances in Cryptology – ASIACRYPT 2024. Kolkata, India: Springer, 2024.

[17] Zia M, Obaidat M S, Mahmood K, et al. A provably secure lightweight key agreement protocol for wireless body area networks in healthcare system[J]. IEEE Transactions on Industrial Informatics, 2023, 19(2): 1683-1690.

[18] Wang S, Zhou X, Wen K, et al. Security analysis of a user authentication scheme for IoT-based healthcare[J]. IEEE Internet of Things Journal, 2023, 10(7): 6527-6530.

[19] Cakaj S, Fischer M, Scholtz A L. Practical horizon plane and communication duration for Low Earth Orbiting (LEO) satellite ground stations [J]. WSEAS Transactions on Communications,2009,8(4):378-384.

谢绒娜（1976– ），女，博士，北京电子科技学院教授、博士生导师，主要研究方向为密码理论与应用、数据安全与隐私保护。

周竞（2001– ），男，主要研究方向为密钥管理、密钥协商。

张晨佳（2002– ），女，主要研究方向为密钥管理、密钥协商。

史国振（1974– ），男，博士，北京电子科技学院教授、博士生导师，主要研究方向为密码工程与应用、安全体系结构与系统安全。