

面向卫星互联网的设备跨域轻量级认证

陈操^{1,2,3}, 李凤华^{1,2,3}, 于梦格⁴, 郭超^{1,3,5}, 李子孚^{1,3}, 耿魁^{1,3}

(1. 中国科学院信息工程研究所, 北京 100085; 2. 中国科学院大学网络空间安全学院, 北京 100049;
3. 网络空间安全防御全国重点实验室, 北京 100085; 4. 北京电子科技学院网络空间安全系, 北京 100070;
5. 北京电子科技学院电子与通信工程系, 北京 100070)

摘要: 新一代网络技术演进推动泛在网络的快速发展, 以卫星网络为代表的异构融合架构显著提升了信息服务水平。然而, 开放网络环境衍生的设备身份仿冒、数据链路劫持等安全隐患, 对卫星网络可信接入构成严峻挑战。针对现有认证方案普遍存在的证书管理机制复杂、依赖第三方密钥分发中心等固有缺陷, 提出了基于无证书公钥密码(certificateless public key cryptography, CL-PKC)体制的跨域设备认证方案。该方案通过3重技术突破实现系统优化: 采用密钥参数分离机制消除传统密钥中心的单点故障风险; 设计跨域身份映射协议解决异构网络间的可信身份迁移问题; 引入融合身份的密钥生成方法增强密钥全生命周期管理的隐私保护能力。实验评估表明, 所提方案较传统PKI方案不仅可抵御多种典型安全威胁, 而且在资源受限的卫星网络场景下, 能够在实现同等安全强度的同时将计算成本控制在接受的范围内, 具有显著的工程应用价值。

关键词: 卫星互联网; 泛在网络; 无证书公钥密码; 跨域认证

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2025034

Lightweight cross domain authentication for satellite internet

CHEN Cao^{1,2,3}, LI Fenghua^{1,2,3}, YU Mengge⁴, GUO Chao^{1,3,5}, LI Zifu^{1,3}, GENG Kui^{1,3}

1. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100085, China
2. School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China
3. State Key Laboratory of Cyberspace Security Defense, Beijing 100085, China
4. Department of Cyberspace Security, Beijing Electronic Science and Technology Institute, Beijing 100070, China
5. Department of Electronics and Communication Engineering, Beijing Electronic Science and Technology Institute, Beijing 100070, China

Abstract: With the evolution of next-generation network technologies, ubiquitous networks have developed rapidly, and heterogeneous integrated architectures, particularly satellite networks, have significantly enhanced information service capabilities. However, open network environments have introduced security risks such as device identity spoofing and data link hijacking, which posed severe challenges to trusted access in satellite networks. Traditional au-

收稿日期: 2025-03-15; 修回日期: 2025-04-24

通信作者: 耿魁, gengkui@iie.ac.cn

基金项目: 国家自然科学基金(U23B2024, 62202463)

Foundation Item: The National Natural Science Foundation of China (U23B2024, 62202463)

引用格式: 陈操, 李凤华, 于梦格, 等. 面向卫星互联网的设备跨域轻量级认证[J]. 网络与信息安全学报, 2025, 11(3): 120-133.

Citation Format: CHEN C, LI F H, YU M G, et al. Lightweight cross domain authentication for satellite internet[J]. Chinese Journal of Network and Information Security, 2025, 11(3): 120-133.

thentication schemes have been constrained by complex certificate management mechanisms and reliance on third-party key distribution centers. To address these issues, a cross-domain device authentication framework based on certificateless public key cryptography (CL-PKC) was proposed. The framework achieved system optimization through three key technical breakthroughs. First, a key parameter splitting mechanism was introduced to eliminate single-point failure risks in traditional key centers. Second, a cross-domain identity mapping protocol was developed to resolve trusted identity migration across heterogeneous networks. Third, dynamic anonymous identification technology was applied to enhance privacy protection throughout the key lifecycle management process. Experimental evaluations demonstrate that compared to traditional PKI solutions, the proposed scheme could resist multiple typical security threats. In resource-constrained satellite network scenarios, while maintaining equivalent security strength, the computational cost of the scheme remains within acceptable levels, indicating its significant engineering applicability.

Keywords: satellite internet, ubiquitous networks, CL-PKC, cross-domain authentication

0 引言

随着网络和通信技术的快速发展,以卫星通信^[1]和内容网络^[2]为代表的个性化服务极大地便利了人们的日常生活。这些服务的成功实施需要异构网络的大规模集成,其中移动网络、地面网络和卫星网络共同形成了一个泛在传输环境。事实上,“泛在网络”的概念正成为当代社会通信的重要特征,并被广泛视为一项关键载体和基础设施。因此,各国纷纷将泛在网络的建设提升到国家信息化战略的高度^[3]。

作为泛在网络的重要组成部分,卫星网络可以提供更广泛的覆盖范围和更高的空间利用效率,一旦建成,该网络就可以提供全球网络服务。因此,自卫星网络概念引入以来,它在全球范围内迅速发展^[4]。自然地,由于其高价值性,也成为了攻击目标。换言之,攻击者可能会入侵卫星网络中的设备,来攻击或窃取信息传输。例如,Viasat公司曾披露其民用卫星网络服务遭受了大规模的仿冒攻击,导致数万台设备发送了错误信息^[5]。因此,确保设备之间的信任关系,以防止身份仿冒和信息泄露,已成为业界和学术界的重要议题。

认证是确保可信度的最有效方式之一。通过为设备构建基于密码学的密钥共享方案,数据可以私密传输,难以泄露。为了解决跨网络认证的多样设备问题,学术界已提出了一系列解决方案。具体来说,传统方法集中于基于证书的公钥密码(public key cryptograph, PKC)认证方案^[6-7]。这些方案通常具有良好的可移植性,但涉及复杂的证书管理,并不适用于卫星网络中的低功耗要求。至于改进方案,基于身份的PKC

认证方案^[8-9]通过使用用户身份信息和密钥生成中心(key generation center, KGC)的密钥处理能力简化了证书管理流程。然而,这些方案完全信任KGC的安全性。如果KGC受到破坏,整个方案将不再可信。同时,这些方法的身份匿名性问题也不容忽视。

具体来说,在传统跨域认证方面, Lee等^[6]利用属性证书实现了一种普适环境下的跨域认证,但该方案涉及对于证书的复杂管理;丁永善等^[7]设计了一种适用于移动设备的跨域认证方案,该方案中签名的验证结果为常量,保证跨域过程中认证实体的匿名性;朱辉等^[8]提出了一种基于身份的跨域认证,但无法保证用户的匿名性。罗长远等^[9]对此进行了改进,对用户信息进行了匿名化处理,该方案避免使用需要消耗大量计算资源的双线性映射,提高了认证效率,但使用的仍然是基于身份认证的体系;杨小东等^[10]使用了CL-PKC(certificateless public key cryptography)体系,利用双线性映射提出一种云环境下的跨域身份认证方案,并基于无证书签名的合法性和消息的有效性,实现了用户与云服务提供商的身份真实性鉴别。在融合新技术的认证方案方面, Feng等^[11]提出了一种基于区块链的智能5G无人机互联网跨域认证方案,使得无人机能够支持域的加入与退出,并且利用智能合约进行身份验证; Xu等^[12]利用了区块链的去中心化、信任、可追溯性和防篡改等特点,提出了一种针对联盟链中异构成员的跨域认证身份方案,简化了异构跨域认证模型; Yuan等^[13]利用区块链的

群签名技术和分布式系统架构,提出了一种物联网环境下的动态跨域认证方法;Chen等^[14]提出一种高效的隐私保护跨域身份验证方案,并基于区块链设计了一种基于多默克尔哈希树的轻量级正确性验证协议来实现快速响应。

然而,尽管上述方案对跨域接入进行了分析,但由于不同网络环境的限制,这些方案难以在卫星网络中有效应用。具体来说,首先,卫星网络具有动态特性,一个卫星网络中的设备经常需要频繁与另一个卫星网络中的设备通信,这对设备的安全接入与认证机制提出了更高的要求;其次,卫星网络的通信资源受限,数据传输能力有限,因此对低存储占用和高效数据处理的需求尤为突出。总之,认证过程不仅涉及确保设备之间可靠的连接,还包括跨不同网络域的信息传播以及相关资源消耗等因素。到目前为止,仍缺乏同时考虑轻量级和安全性方面的跨域设备认证解决方案。

为解决这些问题,本文提出了一种基于改进的无证书公钥密码系统的卫星网络下新型设备跨域认证方案。该方案利用参数分离来解决基于身份的跨域认证模型中完全信任KGC的问题。这种设计可以降低KGC受到威胁后密钥泄露的风险。同时,该方案将用户的私钥和临时验证值同时纳入计算,使攻击者无法分离它们,从而增强了匿名性。此外,引入CL-PKC避免了基于证书的认证系统中签名证书的复杂管理,并且可以满足当前跨域认证的要求,即较低的存储资源占用和更高的认证速度。

总结来说,本文的贡献如下。

本文提出了一种适用于资源受限的卫星互联网CL-PKC改进算法,实现了一种轻量级的认证方案,该方案利用参数分离技术避免了对KGC的完全信任,不仅避免了单点密钥泄露风险,还无须借助复杂的证书管理流程保障认证安全。

本文还提出了一种新颖的验证和访问方法,将用户的私钥和临时验证值纳入计算流程,通过动态组合这些值的方式为每次跨域认证生成临时身份标识,使得攻击者难以反推实际的用户身份,以此增强认证过程的匿名性。

本文方案通过引入对称加密密钥动态生成、时间戳验签等机制,有效防御重放攻击、中间人

攻击,保障前/后向安全性。

本文对方案的正确性、安全性和效率等进行了评估。与先前的方法相比,所提方案不仅具备更好的安全性,而且认证效率也可接受。

1 预备知识

1.1 卫星互联网

卫星互联网作为一种新型网络,基于卫星通信系统提供跨域网络服务。如图1所示,卫星通信系统一般由地面段、空间段和用户段组成。具体来说,地面段一般包括卫星测控中心及相应的卫星测控网络、系统控制中心及各类信关站(gateway);空间段一般是指提供信息中继服务的卫星,卫星之间可以有或没有星间链路;用户段是指用户端设备,如手机、卫星终端等通信设备^[15]。位于不同地面段的设备需要将数据信号传输到空间段,并经由空间段的数据转发实现交互。过去,卫星网络主要由地球静止轨道(geostationary earth orbit, GEO)卫星构成,由于这类卫星数量少且位置固定,组网与协同管理相对简单,系统的构建和维护成本较低。然而,GEO卫星的通信链路损耗较大,信号传播时延较长,限制了其在低时延、高吞吐量通信需求场景下的应用。随着人类对网络传输速率的要求逐渐提高,能提供更大通信容量和更低传输时延的中低轨道卫星所构成的卫星互联网已经成为了新的发展方向。

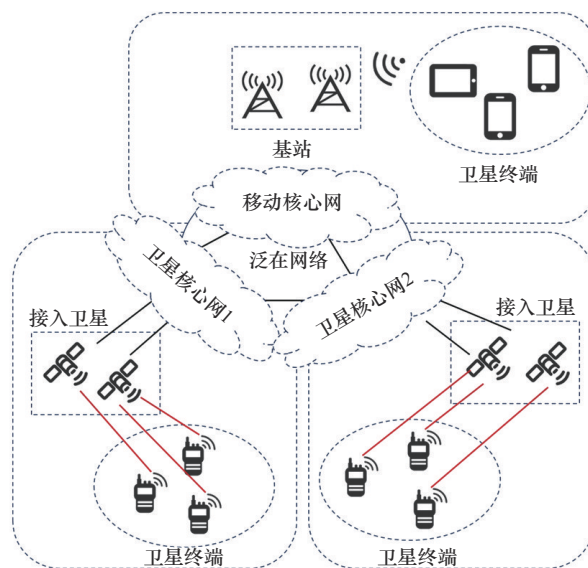


图1 典型卫星网络结构

Figure 1 Typical satellite network structure

1.2 CL-PKC 体制

在传统的公钥密码体制，CA (certificate authority) 需要管理和维护大量的证书^[16]，这就造成了大量存储资源与计算资源的浪费。为了解决这一问题，Shamir 在 1984 年首次提出 ID-PKC (identity-based public key cryptography) 的概念，使得用户的身份信息作为公钥而无须与证书绑定。这一理念解决了传统 PKC 的资源浪费问题，同时其设定了可信的第三方 KGC 作为用户私钥的生成方。然而，该方案假设其 KGC 完全可信，一旦 KGC 被恶意攻破，攻击者就能获取用户的完整私钥信息。

为了解决这一缺陷，Al-Riyami 和 Paterson 提出了无证书公钥密码系统的概念^[17]。具体来说，CL-PKC 在保证 ID-PKC 体制中无须维护额外证书的前提下，解决了 ID-PKC 中私钥托管的问题，使得 KGC 不能完全掌握用户私钥。在 KGC 被攻破的情况下，也能保证用户信息不被泄露。在 CL-PKC 体制中，KGC 拥有系统的主密钥，用户的私钥由用户和 KGC 共同生成。KGC 根据用户的身份和系统主密钥为用户生成部分私钥。用户基于 KGC 为其计算的部分私钥和随机选取的秘密值生成用户完整的私钥；公钥由用户的秘密值、身份和系统参数计算得出，并对外安全公布。这意味着 KGC 对用户私钥仅有部分访问权限，确保即使 KGC 被恶意攻破，攻击者也不能通过 KGC 获取用户的完整私钥信息，也就无法解密用户通信信息。由于这种设计，CL-PKC 方案可进一步保证用户数据的安全性。

2 方案设计

2.1 威胁模型和假设

本文设定攻击者可以监听通信信道并获得交互信息，从而获取交互的用户身份，进而开展中间人攻击。此外，攻击者还具备攻击密钥生成中心的能力，因此其有机会获得 KGC 所产生的的公共参数，并可使用这些参数来入侵通信系统。

此外，本文中设定接入卫星 S_A 与接入卫星 S_B 位于不同网络但相互可信，且各自在本安全域的地面 KGC 中注册。各网络内的 KGC 间已相互认证，并且使用相同的用户注册功能模块，同

时，安全域内的用户公钥信息仅能向本域内设备提供，并对外严格保密。

2.2 异构网络接入模型

为了加深对本文所提方案的理解，本节将首先介绍基于无证书体系的设备跨异构网络通信的网络模型以及其中所涉及的必要实体组件，如图 2 所示。普通用户终端的信息将通过卫星终端进行信息转发，并以此与其他网络中的设备交互。在此架构下，安全域 A 中的 KGC_A 设备与用户终端 U_A 均可以通过卫星核心网与安全域 B 进行通信。每个安全域可接入的设备数量有限，且每个安全域需要具备决定其他域的设备是否可以接入的权限，在允许的情况下，一个安全域需要向另一个安全域进行查证，方可进行接入。例如，若设备 U_A 想要接入安全域 B，安全域 B 需要对自己的承载能力进行审查，审查通过，方可接入。相关元素描述如下。

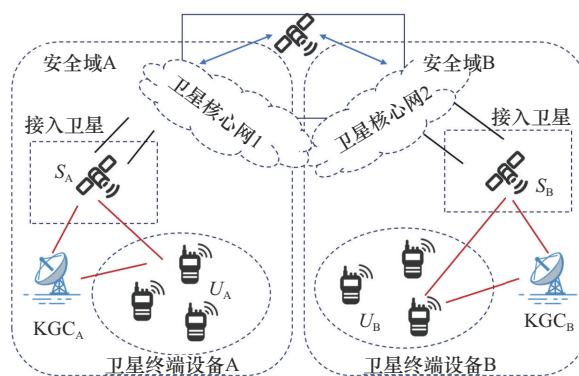


图2 设备接入模型概况

Figure 2 Overview of device access model

安全域。位于同一个网络空间内的实体被认为处于相同的安全域。在某一个安全域内的设备相对于本域内的其他设备都是可信的。换言之，一个区域内所有互相信任的设备，它们信任关系是一张完全无向图，位于这张完全无向图上的所有设备共同构成一个安全域。

KGC。每个安全域将部署一个特定的 KGC。在本文方案中，KGC 是一个关键的实体，用于为域内设备提供密钥生成与分发、密钥管理、用户身份验证以及安全策略实施等服务。公共参数初始化以及用户注册均需通过本域 KGC 进行。

接入卫星。每一个安全域内还将包含一个由若干接入卫星组成的空间段。接入卫星是域内用

户设备的直接通信方, 域内用户的所有通信信息都交由接入卫星转发, 接入卫星是连接域内设备间、设备与 KGC 间、域间设备的唯一通路。

用户设备。按照就近原则, 不同地区的用户设备均会被划定在某一个特定的安全域内。用户设备指手机、车辆、用户等地面终端, 需要通过接入卫星网络获取相应服务。例如, 用户设备作为最终的服务使用者, 只能借助本安全域内接入卫星的广域搜索能力发现位于其他安全域的卫星以及下辖设备, 进而完成跨网络通信。

2.3 跨域认证方案设计

本文方案主要包括系统初始化、本域用户设备注册、跨网接入鉴别以及用户设备跨网接入等 4 个阶段。本文方案涉及符号及含义见表 1。

表 1 符号及含义
Table 1 Symbol and meaning

符号	含义
q	大素数
P	群的生成元
Z_q^*	小于 q 的正整数
s_m	系统主密钥
params	系统公开参数
P_{pub}	系统公钥
$ID_i, i \in \{A, S_A, S_B, KGC_A, KGC_B\}$	域内设备身份标识
$PK_i \leftarrow X_i, Y_i >$	终端 U_i 的公钥对
$sk_i \leftarrow x_i, y_i >$	终端 U_i 的私钥对
H_1, H_2, H_3	单向哈希函数
Ind_i	用户 i 的账户索引
timestamp	用户跨网接入过期时间
U_A, U_B	用户设备 U_A, U_B
S_A, S_B	接入卫星 S_A, S_B
KGC_A, KGC_B	位于安全域 A 和 B 的 KGC

(1) 系统初始化阶段

KGC 首先选取阶数为 q 的循环群 G , 其中 q 为大素数 ($q > 2^k$), P 为 G 的一个生成元。此时, 选取的哈希函数 H_1 、 H_2 和 H_3 分别如式(1)~式(3)所示, 其中 l_A 为用户标识的长度。KGC 随机选取系统主密钥 $s_m \in Z_q^*$ 作为系统主密钥, 利用 $P_{pub} = s_m P$ 计算系统公钥。在获得上述计算结

果的基础上, KGC 将 $\langle q, P, G, P_{pub}, H_1, H_2, H_3 \rangle$ 在所属安全域内作为公共参数进行广播, 为后续认证过程作铺垫。

$$H_1: \{0, 1\}^{l_A} \times G \times G \rightarrow Z_q^* \quad (1)$$

$$H_2: \{0, 1\}^{l_A} \rightarrow Z_q^* \quad (2)$$

$$H_3: Z_q^* \times Z_q^* \rightarrow Z_q^* \quad (3)$$

(2) 本域用户设备注册阶段

① 设备在本地网络内进行注册。具体来说, U_A 将随机选取秘密值 $x_A \in Z_q^*$ 计算公开参数 $X_A = x_A P$, 然后将 X_A 和其身份 ID_A 共同发送给所属安全域 A 的地面密钥生成中心 KGC_A 。KGC_A 在收到 ID_A 和 X_A 后, 随机选取 $r_A \in Z_q^*$, 在计算 $Y_A = r_A P$ 的同时, 基于式(4)计算 y_A 。

$$y_A = r_A + s_m H_1(ID_A, X_A, Y_A) \quad (4)$$

② KGC_A 通过安全信道将 (Y_A, y_A) 返回给终端 U_A 。随后, KGC_A 则根据上述信息为终端 U_A 建立对应的用户账户 (Ind_A, ID_A, X_A, Y_A) , 其中账户索引 Ind_A 如式(5)所示。

$$Ind_A = X_A + Y_A + H_1(ID_A, X_A, Y_A) P_{pub} \quad (5)$$

③ 终端 U_A 收到 KGC_A 返回的域内部分公钥和部分私钥后, 通过式(6)验证密钥的合法性, 若等式成立则说明用户密钥生成成功。最终终端 U_A 与 KGC_A 在域内的认证公钥 PK_A 、私钥 sk_A 的计算式如式(7)和式(8)所示。后续 KGC_A 将拥有 PK_A , 而 U_A 会拥有 PK_A 和 sk_A , 它们可以用此公私钥对协商出当前两方的对称会话密钥。

$$y_A P = Y_A + H_1(ID_A, X_A, Y_A) P_{pub} \quad (6)$$

$$PK_A \leftarrow X_A, Y_A > \quad (7)$$

$$sk_A \leftarrow x_A, y_A > \quad (8)$$

(3) 跨网接入鉴别阶段

在设备成功接入网络的基础上, 设备通信流程即可以展开。具体来说, 如图 3 所示, 随机选择终端 U_A , $r \in Z_q^*$ 通过式(9)计算 R 。同时, U_A 利用当前时间戳 T_A , 根据式(10)计算哈希值 h , 并基于此, 以式(11)计算临时参数 R 。随后, U_A 按照式(12)组合成 M_A , 将 M_A 转发至 B 域的密钥生成中心 KGC_B。此时, KGC_B 和 KGC_A 将分别执行接入请求验证、接入反馈认证以及合法性确认流程, 具体描述如下:

$$R = rP \quad (9)$$

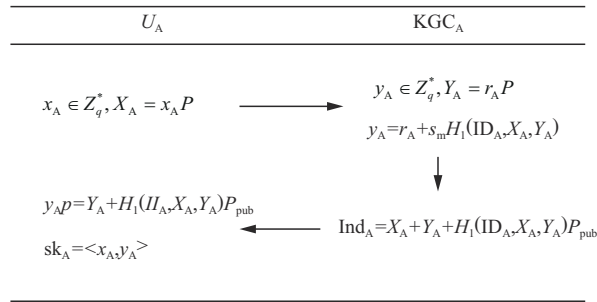


图3 本域用户设备注册阶段

Figure 3 Terminal registration stage in its own domain

$$h = H_2(R, T_A, ID_A, X_A, Y_A) \quad (10)$$

$$u = r + (x_A + y_A)h \quad (11)$$

$$M_A = \langle u, h, R, T_A, ID_{KGC_A} \rangle \quad (12)$$

接入请求验证。在 KGC_B 检查 M_A 中时间戳 T_A 的新鲜性后，同时取 A、B 跨域交互秘密信息的有效期时间戳 T_{AB} 、当前时间戳信息 T_{KB} 以及 KGC_B 用于跨域信息交换的公开密钥 PK_{KGC_B} ，并根据式(13)构造跨网接入鉴别信息 M_{KB} 。随后 KGC_B 将相关信息以式(14)的形式，形成 M_{KGC_B} ，其中， $Sig_B(M_{KB})$ 表示 KGC_B 对 M_{KB} 进行签名。 M_{KGC_B} 将会由 KGC_B 转发给 A 安全域的认证中心 KGC_A ，供其执行接下来的验证。

$$M_{KB} = \{u, h, R, T_A, ID_{KGC_A}, ID_{KGC_B}, T_{KB}, T_{AB}, PK_{KGC_B}\} \quad (13)$$

$$M_{KGC_B} = \langle T_{KB}, T_{AB}, M_{KB}, Sig_B(M_{KB}) \rangle \quad (14)$$

接入反馈认证。在成功验证签名 $Sig_B(M_{KB})$ 的有效性以及 T_{KB} 的新鲜性后， KGC_A 进一步验证 A、B 跨域交互秘密信息的有效期时间戳 T_{AB} ，此时将分为两种情况。

情况1：如果 T_{AB} 在有效期内，则认为过去两个域的设备进行过认证，可以根据收到的 M_{KB} 信息直接来判定具体的待交互设备，以此优化动态环境下的快速接入流程。具体来说， KGC_A 通过式(15)得到 Ind'_A 后，将继续检查本安全域已注册的合法终端列表，并找到与 Ind'_A 相同的注册索引信息，该信息同时关联了终端 U_A 的账户信息 (Ind_A, ID_A, X_A, Y_A) ，当找到注册索引信息时，则判定 Ind'_A 所指代的标识是位于 KGC_A 所述安全域的设备 U_A 。此时， KGC_A 将 $\langle ALLOW_MESSAGE \rangle$ 经由安全通道分发给 U_A ，告知 U_A 可以向 KGC_B 发起消息。

$$Ind'_A = (uP - R)h^{-1} \quad (15)$$

情况2：如果 T_{AB} 不在有效期内（或首次建立 A、B 域内的通信），除了完成情况1中索引值 Ind'_A 的合法性检查外。在验证 Ind'_A 通过的情况下， KGC_A 还需要额外新增一个跨域交互秘密信息 r_{AB} ，并将 KGC_B 注册的允许信息以及跨域交互秘密信息组成的组合消息 $\langle ALLOW_MESSAGE, r_{AB} \rangle$ 通过安全通道分发给 U_A 。同时， KGC_A 将额外通过公钥加密构造加密值 M_{EAB} ，用于将 r_{AB} 传递给 KGC_B ，具体的构造方法如式(16)所示， KGC_A 需要使用 KGC_B 传递的公钥 PK_{KGC_B} 加密 r_{AB} 与 T_{AB} 。

$$M_{EAB} = Enc_{PK_{KGC_B}}(r_{AB}) \quad (16)$$

在上述情况的处理完成后， KGC_A 取当前时间戳 T_{KA} ，在情况1下可根据式(17)构造消息 M_{KA1} ，在情况2下依照式(18)构造消息 M_{KA2} ，并依照式(19)将融合消息 M_{KGC_A} 转发给 KGC_B ，其中， $Sig_B(M_{KA})$ 表示消息签名， M_{KA} 和 M_{EAB} 是否发送以及发送的内容依情况1和情况2而定。

$$M_{KA1} = H_1(Ind_A, R) \oplus T_A \oplus T_{KA} \quad (17)$$

$$M_{KA2} = H_1(Ind_A, R) \oplus T_A \oplus T_{KA} \oplus M_{EAB} \quad (18)$$

$$M_{KGC_A} = \langle T_{KA}, M_{EAB}, M_{KA}, Sig_A(M_{KA}) \rangle \quad (19)$$

用户合法性确认。 KGC_B 接收到来自 KGC_A 的接入反馈响应值，即代表 KGC_A 允许 U_A 进行跨域注册操作，接着， KGC_B 需要同时验证签名以及时间戳 T_{KA} 的新鲜性，在情况2时还需要使用自己的跨域信息交换的私钥 sk_{KGC_B} 解密信息 M_{EAB} 以获得 r_{AB} ，解密方法如式(20)所示。若成立且解密成功，则 KGC_B 通过 KGC_A 和终端 U_A 的认证，换句话说， KGC_B 此时相信终端 U_A 确实为安全域 A 中的合法用户，且已被允许跨域注册，相关流程如图4所示。

$$r_{AB} = Dec_{sk_{KGC_B}}(M_{EAB}) \quad (20)$$

(4) 设备跨网接入阶段

在上述验证过程通过后， KGC_B 根据 KGC_A 的参数情况选择式(21)（对应情况1）或者式(22)（对应情况2）计算得到部分参数值，并使用事先广播的哈希函数 H_3 依照式(23)构造对称加密密钥 K ，这个加密密钥 K 将与 U_A 进行接下来的跨域注册操作，相关的流程如图5所示。


```

5:   ALLOW_MESSAGE ← Generation
Message
6:   if ValidTimestamp( $T_{AB}$ ) Then
7:      $M_{EAB} \leftarrow 0$ 
8:   else
9:      $r_{AB} \leftarrow \text{GetRandomSecretKey}$ 
10:     $M_{EAB} \leftarrow \text{Encrypt}(r_{AB})$ 
11:  end if
12:   $U_A \leftarrow r_{AB}, \text{ALLOW\_MESSAGE}$ 
13:   $T_{KA} \leftarrow \text{CurrentTimestamp}$ 
14:   $H_{temp} \leftarrow \text{Hash}(\text{Ind}_A, R)$ 
15:   $M_{KA} \leftarrow \text{XOR}(H_{temp}, T_{KA}, T_A, M_{EAB})$ 
16:   $M_{KGC_A} \leftarrow T_{KA} || M_{EAB} || M_{KA} || \text{Sign}(M_{KA})$ 
17:  else
18:    Error ← InvalidDevice
19:  end if
20:  return  $M_{KGC_A}$ 

```

第1~4行：签名验证与设备索引计算

本部分验证 KGC_A 签名是否合法，并判定设备是否为本域的合法注册设备。通过 VerifySignature 函数进行签名验证，确保设备信息未被篡改，并通过式(15)计算设备的索引值 Ind_A 来唯一标识设备，随后根据计算出的设备索引值，查询本地已注册设备表，检查该设备是否存在，如果未注册，则在第16行返回非法设备信息。

第5~12行：生成秘密值并通知

KGC_A 验证跨域交互秘密信息的有效期时间戳 T_{AB} ，当时间戳不在有效期时，取一个新的随机秘密值 r_{AB} ，并由式(16)构造秘密值 M_{EAB} 传递给 KGC_B ，将 r_{AB} 与允许跨域认证信息一起由安全信道传递给设备，设备收到这两条信息后，即可使用秘密值进行对称加密和跨域注册操作，而当时间戳位于有效期，则说明设备已有秘密值，此时仅需将允许跨域注册信息传送即可。

第13~16行：鉴别计算与响应返回

取得新的时间戳，使用来自 KGC_B 的公钥加密秘密值经过异或操作计算信息 M_{KA} 并签名， M_{KA} 由不同阶段决定，处于有效期时， M_{KA} 值为空，其他参数信息与其异或操作的结果仍是其他参数本身。最后由式(19)、签名以

及时间戳和其他参数一同构成 M_{KGC_A} 作为返回的响应信息。

第18~20行：异常响应返回

当判定失败后，将直接返回设备信息不一致的异常响应。

算法2 设备跨网注册算法

输入 加密消息 M_{AP} ，对称密钥 K ，秘密密钥 r_{AB} ，初始化的集合 $M_{KP} = \emptyset$

输出 加密消息 M_{KP}

```

1:   Encrypted Data ← Receive Encrypted
Data( $M_{AP}$ )
2:   if DeviceFound = True Then
3:      $ID'_A \leftarrow \text{ExtractDeviceID}(\text{Decrypted}$ 
Data)
4:      $r'_A \leftarrow \text{GenerateRandomSecret}()$ 
5:      $Y'_A, y'_A \leftarrow \text{ComputePartialKeys}(r'_A, r_{AB})$ 
6:      $\text{Ind}'_A \leftarrow \text{ComputeCrossDomainIndex}$ 
( $ID'_A$ )
7:     timestamp ← SetDeviceLifecycle()
8:      $\mathbb{D} \leftarrow \{(ID'_A, \text{Ind}'_A, \text{timestamp})\}$ 
9:     DeviceRegistrationTable ← StoreDev
iceInfo( $\mathbb{D}$ )
10:     $T_{KP} \leftarrow \text{CurrentTimestamp}$ 
11:     $M_{KP} \leftarrow \text{Encrypt}(Y'_A, y'_A, T_{KP})$ 
12:  else
13:    Error ← InvalidData, DiscardRegis-
tration
14:  end if
15:  return  $M_{KP}$ 

```

第1~2行：验证信息解密

收到数据后开始解密，使用秘密值 r_{AB} 对收到的信息进行对称解密，解密失败则在第13行直接返回错误异常信息，解密成功则代表注册设备为合法跨域注册设备，将进入响应信息构造阶段。在后续阶段中， KGC_B 会将设备看作本域的临时设备进行注册。

第3~7行：设备注册参数计算

从解密出的参数信息中，抽取设备 ID'_A ，根据随机选取的秘密值 r'_A 与跨域注册秘密值 r_{AB} 通过式(27)和式(28)计算部分公开密钥和私钥 Y'_A, y'_A ，接着使用设备 ID 值以及其他必要参数，

通过式(29)计算设备位于本域的合法索引值,随后为注册设备计算并分配一个生命周期,确保设备在设置的生命周期内正常响应。

第8~11行:参数持久化与响应返回

设备的ID信息以及索引值和生命周期将做持久化处理,用以后续的鉴别计算,随后,选取当前的响应时间戳、时间戳 T_{KP} 以及形成的部分跨域注册公钥和私钥信息,通过式(30)计算后构成注册响应信息 M_{KP} ,最后将使用对称加密密钥 K 对响应信息进行对称加密,最终经过加密的注册响应信息将会返回给注册终端(如15行)。

第13行:异常信息返回

在判定解密失败后,会返回非法数据异常并取消本次注册。

4 实验结果与分析

为了对本文方案进行评估,本节将从设备跨网认证所必需的认证算法入手,从计算效率和安全属性两方面进行分析,以展示方案的有效性。此外,本节还将对认证方案的正确性进行分析证明,以及使用形式化验证工具Tamarin进行形式化安全性验证,从而表明方案设计的合理性。

4.1 效率分析及对比

在分析时将忽略卫星转发等信息传递所需的时间,仅对具体认证算法流程(包括跨网接入鉴别与跨网接入注册阶段)进行计算。与具备代表性的AWAP方案^[8]、IDAS方案^[9]及CBAS方案^[7]进行比较,计算开销主要依赖于认证时产生的群

上的双线性对运算、点乘运算、指数运算、哈希运算、对称加解密的执行次数。令 E_e 表示双线性映射操作, E_M 表示群上的点乘运算, E_Q 表示群上的指数运算, T_H 表示哈希运算, E_P 表示公钥加解密运算, S_E 表示对称加解密运算, P_S 表示公钥签名及验证。其对比结果见表2。其中 $(x/y/z)$ 表示参与该认证过程的3个实体分别执行了 x 、 y 和 z 次专门的密码学运算。

通过对表2中计算所需时间的分析可以看出,4个方案所需对称加解密及公钥签名验证的次数相等。同时,Zhang等^[15]认为在椭圆曲线上的点加运算相对于点乘运算所需的时间基本可以忽略不计,普通的哈希运算所需时间极少,且本文方案(情况1)的哈希计算(4/2/2)相对于前3个方案(1/0/1)、(2/1/2)、(2/1/0)仅为个位数增加,因此可以将其忽略。通过对比可看出,AWAP方案、IDAS方案、CBAS方案所需的认证时间都大于本文方案。综合来看,在5个方案中,本文方案在情况1时的计算效率最高,在情况2时的计算效率与其他3个方案相当。由于本文方案基于密钥参数分离,且在使用跨域共享秘密参数时加入了随机因素和时间变量,在参与密钥生成时引入了哈希计算,因此可根据卫星移动规律周期和认证设备数量,针对跨域共享秘密参数设置一个较长的时间有效期,保证常态化跨域认证时均符合情况1,因此本文方案具有显著的效率优势。安全性方面,其他3个方案都需要额外证书或完全可信的KGC等限制条件,因此本文方案具有显著的安全性优势。

为衡量认证所需计算开销,本文采用3.2 GHz

表2 计算效率 and 安全性对比
Table 2 Comparison of computational efficiency and security

方案	计算次数(发起方设备/接入方认证中心/发起方认证中心)								安全性	
	双线性对运算	点乘运算	指数运算	哈希运算	公钥加解密	对称加解密	公钥签名及验证	总运算次数	额外证书	完全可信的KGC
AWAP	0/0/1	4/1/2	*	1/0/1	0/0/0	1/1/0	0/2/2	$E_e + 7E_M + 2T_H + 2S_E + 4P_S$	×	√
IDAS	0/0/0	3/2/3	*	2/1/2	0/1/1	1/1/0	0/2/2	$8E_M + 2T_H + 2E_P + 2S_E + 4P_S$	×	√
CBAS	0/0/0	*	5/4/4	2/1/0	0/1/1	1/1/0	0/2/2	$13E_Q + 3T_H + 2E_P + 2S_E + 4P_S$	√	√
本文方案(情况1)	0/0/0	4/1/2	*	4/2/2	0/0/0	1/1/0	0/2/2	$7E_M + 8T_H + 2S_E + 4P_S$	×	×
本文方案(情况2)	0/0/0	4/1/2	*	4/2/2	0/1/1	1/1/0	0/2/2	$7E_M + 8T_H + 2E_P + 2S_E + 4P_S$	×	×

的 CPU 模拟密码学操作, 并基于密码原语的时间消耗进行精确计算, 见表 3。

表 3 密码原语的时间消耗

Table 3 Time consuming of cryptographic primitives

运算类型	符号表示	耗时/ms
双线性映射	E_e (MNT224)	3.710 5
群上的点乘	E_M (MNT224)	0.000 5
指数运算	E_Q (MNT224)	4.638
哈希运算	T_H (SM3-256)	0.002 5
对称加密	S_E^1 (SM4-128)	4.6453
对称解密	S_E^2 (SM4-128)	4.513 5
公钥加密	E_P^1 (SM2-256)	12.071 3
公钥解密	E_P^2 (SM2-256)	6.594 8
公钥签名	P_S^1 (SM2-256)	5.386 9
公钥验证	P_S^2 (SM2-256)	10.850 1

在此基础上, 使用完整跨域认证过程所花费的总时间衡量计算开销。对比了 AWAP、IDAS、CBAS 方案和本文方案在用户设备及密钥生成中心端的计算开销, 图 7 给出了认证次数与时间消耗的关系。在一次完整的跨域认证中, 本文方案在用户端侧认证所需的计算成本在情况 1 和情况 2 下均仅需 12.08 ms, 与 AWAP (12.07 ms) 和 IDAS (12.07 ms) 方案基本一致, 但显著低于 CBAS (35.27 ms) 方案。当认证规模扩大时 (如重复执行 10~100 次 KGC 操作), 本文方案 (情况 1) 的计算总开销始终最低。例如, 当进行 10 次认证时, 本文方案计算总时间比其他 3 个方案中较快的 AWAP 方案降低 8.4%; 当进行 100 次认证时, 本文方案计算总时间比 CBAS 方案降低 54.3%。在情况 2 下, 虽然计算开销有所增加, 但整体消耗基本与 IDAS 方案相当, 并且显著优于 CBAS 方案。

为衡量认证所需的带宽消耗和通信时延, 本文将各方案应用于低轨卫星非地面网络场景进行对比。兼顾安全性要求和性能要求, 统一设定椭圆曲线强度、哈希函数、身份标识等相关参数长度。模拟真实的卫星网络, 设定卫星间链路长度约 1500 km, 低轨卫星高度约 550 km, 下载和上传速度分别约为 122.5 Mbit/s 和 12.5 Mbit/s。表 4 展

示了上行数据 (U_{data})、下行数据 (D_{data})、交易时延 (T_{delay}) 以及传播时延 (P_{delay}) 的对比情况。

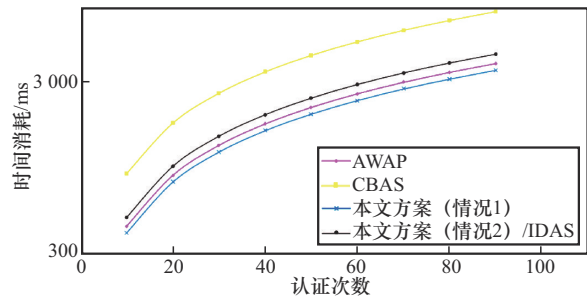


图 7 认证次数与时间消耗的关系

Figure 7 The relationship between the number of authentications and time consumption

表 4 带宽消耗与通信时延

Table 4 Bandwidth consumption and communication delay

方案	U_{data}/bit	D_{data}/bit	T_{delay}/ms	P_{delay}/ms	T_{total}/ms
AWAP	4 148	2 660	0.352	5.566	5.918
IDAS	3 364	3 604	0.296	6.298	6.594
CBAS	3 364	3 604	0.296	5.566	5.862
本文方案 (情况 1)	3 936	2 888	0.338	5.433	5.771
本文方案 (情况 2)	4 352	2 857	0.371	5.934	6.305

通过对比分析, 本文方案较好地平衡了认证过程的数据传输量与时延, 与其他方案相当。综合来看, 本文方案在没有增加通信开销和时延的情况下, 显著降低了计算开销, 从而降低了认证过程的总时间消耗, 在卫星互联网等计算资源条件受限条件下具有较显著优势, 能够较好适用于卫星高速移动、拓扑动态变化情况下的快速认证需求。

4.2 正确性证明

正确性分析主要应用在跨网身份鉴别阶段, 当验证方返回验证消息后, 发送方 KGC 需要帮助验证方, 验证返回信息中的信息标签, 经过计算判断是否为隶属于发送方的某一个合法用户设备。判定是否成立的正确性分析过程示例如下。

在从验证方 KGC_B 接收到验证信息后, 发送方 KGC_A 需要对用户身份是否为 U_A 进行验证。

如果用户隶属于 KGC_A ，则需要满足下式：

$$\text{Ind}_A = (uP - R)h^{-1} \quad (33)$$

上式成立的证明如下：在跨网接入鉴别初始阶段，终端 U_A 经计算得到 R 、 h 和 u ，其迭代计算式可表示为： $R = rP$ ， $h = H_2(R, T_A, \text{ID}_A, X_A, Y_A)$ ， $u = r + (x_A, y_A)h$ 。KGC 收到鉴别信息后，进行如下计算，经由式(34)至式(36)即可验证式(33)的正确性。

$$uP = rP + (x_A + y_A)hP \quad (34)$$

$$uP = R + (X_A + Y_A + H_1(\text{ID}_A, X_A, Y_A)P_{\text{pub}})h \quad (35)$$

$$(uP - R)h^{-1} = X_A + Y_A + H_1(\text{ID}_A, X_A, Y_A)P_{\text{pub}} \quad (36)$$

具体来说，若用户未在 KGC_A 中注册（即，安全域 A 内的非法用户），其公钥 X_A 、 Y_A 和终端身份信息 ID_A 在 KGC_A 的用户注册表中将不存在，自然上述等式无法进行计算。通过式(36)和式(37)，在计算 $(uP - R)h^{-1}$ 后，根据式(15)，可以得到 Ind'_A ，此时，若为 KGC_A 所属终端设备，则两者相等。因此， KGC_A 只需要使用等式(34)进行验证，即可确定相应的用户终端是否是该域内的合法注册用户。

$$X_A + Y_A + H_1(\text{ID}_A, X_A, Y_A)P_{\text{pub}} = \text{Ind}_A \quad (37)$$

4.3 安全性分析

前/后向安全性。在本文方案中，因为跨域认证阶段的会话密钥中的随机参数 $R = rP$ 是基于椭圆曲线上的离散对数难题生成的，本身并不依赖于用户的私钥信息，会话密钥具有随机性和新鲜性。即使用户终端的私钥信息 $\text{sk}_A = \langle x_A, y_A \rangle$ 遭到泄露，也不会影响到先前建立的会话密钥信息。当用户终端开启新的跨域认证时，基于数学难题选取新的随机参数，即使攻击者获取到当前的跨域认证密钥，也无法通过当前密钥推算以前的密钥，也不能计算出后续的跨域认证会话密钥。因此，本文方案满足前/后向安全性。

抗重放攻击能力。在认证过程中，认证中心 KGC 和终端设备之间的认证以及双方认证中心之间的信息验证都会根据当前的时间戳来判断消息的新鲜性，当大于系统所允许的最大差值时，会直接丢弃该信息，从而使攻击者对消息的重放攻击无效。

抵御中间人或假冒攻击能力。在认证过程中，即使终端用户的跨域认证消息 $M_A = \langle u, h, R,$

$T_A, \text{ID}_{KGC_A} \rangle$ 被截获，攻击者也无法对该消息进行改造或伪造。因为验证参数 r 是基于椭圆曲线上的离散对数难题问题随机选取的秘密值，且用户私钥信息由用户秘密保存并且仅部分依赖于认证中心 KGC_A 。想要成功伪造消息，需要同时知道用户的私钥 $\text{sk}_A = \langle x_A, y_A \rangle$ 和秘密值 r 。这就保证了本文协议足以抵御中间人或假冒攻击。

用户匿名性与不可追踪性。在认证鉴别的过程中，用户的标识信息 ID_A 并未出现，而是以哈希的形式存在于认证消息中，只有其所属安全域的认证中心能够通过跨域认证计算来得到用户的索引账户，而目标域的认证中心并不能得到用户的真实信息标识。在跨域认证过程中，用户使用新生成的临时身份信息，且该临时身份信息随每次接入认证而变化，目标域内设备并不能通过该临时身份信息推断其真实身份信息，这就保证了用户的匿名性与不可追踪性。

密钥/共享秘密信息安全。在接入认证过程中，生成的对称加密密钥 K 为一次一密，仅在每次传输认证相关参数时使用，每次认证时重新生成。跨网认证账户公钥 PK'_A 及私钥 sk'_A 主要用于协商临时会话密钥，根据接入认证的有效期 timestamp 进行更新，该有效期可通过卫星互联网的周期性变化规律及跨域通信数据量进行设定，从而保障跨网认证账户私钥安全。跨域交互秘密信息 r_{AB} 主要用于派生对称加密密钥，派生时引入不同终端设备的标识和随机数，并通过哈希函数计算，可以根据终端设备跨域接入有效期、接入数量和频次、卫星互联网的变化周期，平衡好安全和效率，合理设定更新周期，保障秘密信息安全。

4.4 形式化安全性验证

本文使用形式化验证工具 Tamarin，建立了 Dolev-Yao 敌手模型，对所提方案进行了形式化安全性分析和验证。Tamarin 是一种基于多集重写规则和一阶逻辑的符号分析工具，通过脚本自动化方式结合密码功能安全理论，用于分析复杂安全协议的安全性。模型使用 rule（规则）定义系统初始化、本域用户设备注册及设备跨网鉴别与接入过程。为确保协议符合既定的安全目标，模型通过定义 Aliveness（存活性）、AuthRequest

(认证请求)、SecrecyMessage (消息机密性)、Secrecykey (密钥机密性) 和 ExecutableRequest (可执行请求) 5 个引理来模拟所需的安全属性, 并使用 Equality (等式约束) 限制验证签名的正确性, 跨网认证方案 Tamarin 的运行结果如图 8 所示。从中可以看出, 该方案能够在保证认证双方存活性的情况下成功地实现认证, 保障系统主密钥和对称加密密钥的机密性。

```
=====
summary of summaries:

analyzed: 0317.spthy

Aliveness (all-traces): verified (2 steps)
AuthRequest (all-traces): verified (7 steps)
SecrecyMessage (all-traces): verified (12 steps)
FunctionalCorrectness (exists-trace): verified (3 steps)
ExecutableRequest (exists-trace): verified (7 steps)
=====
```

图 8 跨网认证方案 Tamarin 的运行结果
Figure 8 Running output of the cross-network authentication scheme in Tamarin

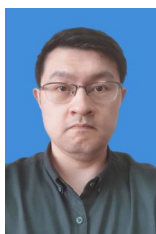
5 结束语

作为泛在网络重要组成部分, 卫星互联网在社会生产应用中逐渐展现出其相对于地面网络的巨大优势, 然而, 其安全性问题也对当前的设备跨网接入提出了更高的要求。传统的公钥密码体制由于其需要维护和管理大量证书, 并不适用于资源受限的卫星网络场景。而传统的基于身份的方案则依赖于完全可信的 KGC。针对上述问题, 本文提出了基于无证书公钥密码系统的轻量级设备认证方案, 该方案不仅解决了传统方案中存在的问题, 还显著提升了认证效率。因此本文方案将更能够适应新一代卫星网络下的设备跨网认证需求。

参考文献:

- [1] FONTANESI G, ORTÍZ F, LAGUNAS E, et al. Artificial intelligence for satellite communication and non-terrestrial networks: A survey[EB]. 2023.
- [2] DHARMAPAL P, CHANNAKRISHNARAJU C, KRISHNAMUR C B. A novel cost-based replica server placement for optimal service quality in cloud-based content delivery network[J]. International Journal of Electrical and Computer Engineering (IJECE), 2023, 13(5): 5588.
- [3] 张平, 苗杰, 胡铮, 等. 泛在网络研究综述[J]. 北京邮电大学学报, 2010, 33(5): 1-6.
- [4] ZHANG P, MIAO J, HU Z, et al. A survey of ubiquitous network[J]. Journal of Beijing University of Posts and Telecommunications, 2010, 33(5): 1-6.
- [5] JIANG W W. Software defined satellite networks: A survey[J]. Digital Communications and Networks, 2023, 9(6): 1243-1264.
- [6] GREIG J. Nsa, viasat say 2022 hack was two incidents; Russian sanctions resulted from investigation[EB]. 2023.
- [7] LEE D G, KANG S I, SEO D H, et al. Authentication for single/multi domain in ubiquitous computing using attribute certification[M]// Computational Science and Its Applications - ICCSA 2006. Heidelberg: Springer Berlin Heidelberg, 2006: 326-335.
- [8] 丁永善, 李立新, 李作辉. 基于证书的匿名跨域认证方案[J]. 网络与信息安全学报, 2018, 4(5): 32-38.
- [9] DING Y S, LI L X, LI Z H. Certificate-based cross-domain authentication scheme with anonymity[J]. Chinese Journal of Network and Information Security, 2018, 4(5): 32-38.
- [10] 朱辉, 李晖, 苏万力, 等. 基于身份的匿名无线认证方案[J]. 通信学报, 2009, 30(4): 130-136.
- [11] ZHU H, LI H, SU W L, et al. ID-based wireless authentication scheme with anonymity[J]. Journal on Communications, 2009, 30(4): 130-136.
- [12] 罗长远, 霍士伟, 邢洪智. 普适环境中基于身份的跨域认证方案[J]. 通信学报, 2011, 32(9): 111-115, 122.
- [13] LUO C Y, HUO S W, XING H Z. Identity-based cross-domain authentication scheme in pervasive computing environments[J]. Journal on Communications, 2011, 32(9): 111-115, 122.
- [14] 杨小东, 安发英, 杨平, 等. 基于无证书签名的云端跨域身份认证方案[J]. 计算机工程, 2017, 43(11): 128-133, 145.
- [15] YANG X D, AN F Y, YANG P, et al. Cross-domain identity authentication scheme in cloud based on certificateless signature[J]. Computer Engineering, 2017, 43(11): 128-133, 145.
- [16] FENG C S, LIU B, GUO Z, et al. Blockchain-based cross-domain authentication for intelligent 5G-enabled Internet of drones[J]. IEEE Internet of Things Journal, 2022, 9(8): 6224-6238.
- [17] XU J J, QIU C H. Authentication scheme based on alliance chain cross-system[C]//Proceedings of the 2023 IEEE 5th International Conference on Power, Intelligent Computing and Systems (ICPICS). Piscataway: IEEE Press, 2023: 624-627.
- [18] YUAN W H, LI X Y, LI M Y, et al. DCAGS-IoT: dynamic cross-domain authentication scheme using group signature in IoT[J]. Applied Sciences, 2023, 13(10): 5847.
- [19] CHEN J, ZHAN Z Y, HE K, et al. XAuth: efficient privacy-preserving cross-domain authentication[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 19(5): 3301-3311.
- [20] ZHANG G X, WANG Y F, DIGN X, et al. Research on several key technologies of satellite Internet[J]. Journal on Communications, 2021, 42(8): 1-14.
- [21] GUTMANN P. PKI: it's not dead, just resting[J]. Computer, 2002, 35(8): 41-49.
- [22] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography[C]//Advances in Cryptology - ASIACRYPT 2003. Heidelberg: Springer Berlin Heidelberg, 2003: 452-473.

[作者简介]



陈操（1988-），男，河南南阳人，中国科学院信息工程研究所博士生，主要研究方向为网络与系统安全。



郭超（1987-），女，江西九江人，博士，北京电子科技学院副教授、硕士生导师，主要研究方向为卫星通信网络安全。



李凤华（1966-），男，湖北浠水人，博士，中国科学院信息工程研究所研究员、博士生导师，主要研究方向为网络与系统安全、信息保护、隐私计算。



李子孚（1992-），女，内蒙古赤峰人，博士，中国科学院信息工程研究所高级工程师、硕士生导师，主要研究方向为网络与系统安全。



于梦格（2000-），女，山东淄博人，中国科学院信息工程研究所硕士生，主要研究方向为网络认证协议。



耿魁（1989-），男，湖北红安人，博士，中国科学院信息工程研究所高级工程师、硕士生导师，主要研究方向为网络安全、信息保护。