边云协同场景中基于动态属性权限的群组密钥协商协议

张启坤[1],朱 亮[2],韩桂锋[1*],刘梦琪[1],金保华[1],李元章[3]
(1. 郑州轻工业大学计算机与通信工程学院,河南郑州 450002;2. 华东师范大学软件工程学院,上海 200062;
3. 北京理工大学计算机学院,北京 100081)

摘 要: 针对边云协同应用场景中多域间终端的安全通信、信息安全交换及安全资源共享等问题,提出一种基于动态属性权限的群组密钥协商(Group Key Agreement,GKA)协议,为应用场景中的群组终端之间建立了一条安全的通信信道. 协议提出了一种密钥证实算法,解决了传统方案中密钥生成和密钥分发造成的安全隐患;采用隐藏属性认证技术实现对终端身份认证,同时,保障了终端的身份和属性信息不被泄露;采用属性基加密(Attribute-Based Encryption,ABE)与牛顿插值多项式相结合的方式,能够支持安全细粒度的GKA;采用非对称计算,将计算任务转移到边缘服务器上执行,减轻终端的计算量;利用区块链技术不可篡改的特性,实现终端身份和通信信息的完整性验证和数据的可追溯性. 此外,该协议支持属性权限动态更新,保障群组密钥的新鲜性. 通过与应用的文献进行对比分析,本协议在计算时间、计算能耗和通信能耗方面具有较好的性能.

关键词: 边云协同;群组密钥协商;牛顿插值多项式;属性基加密;动态属性权限;隐藏属性认证
基金项目: 国家自然科学基金(No.61971380,No.62072037,No.61772477);郑州市协同创新专项(No.2021ZDPY0206)
中图分类号: TP309.7 **文献标识码:** A **文章编号:** 0372-2112(2024)06-1911-14
电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20220727

Group Key Agreement Protocol Based on Dynamic Attribute Permissions for Edge-Cloud Collaboration Scenarios

ZHANG Qi-kun[1], ZHU Liang[2], HAN Gui-feng[1*], LIU Meng-qi[1], JIN Bao-hua[1], LI Yuan-zhang[3]
(1. *School of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou, Henan* 450002, *China*;
2. *School of Software Engineering, East China Normal University, Shanghai* 200062, *China*;
3. *School of Computer Science and Technology, Beijing Institute of Technology, Beijing* 100081, *China*)

Abstract: In the edge-cloud collaborative application scenario, there are many problems in the secure communication, information security exchange and secure resource sharing of multi domain terminals. In order to solve these problems, a group key agreement (GKA) protocol based on dynamic attribute permissions is proposed. In the protocol, a key verification algorithm is proposed to solve the security problems caused by key generation and key distribution in the traditional scheme. The hidden attribute authentication technology is adopted to realize terminal identity authentication. At the same time, hidden attribute authentication technology ensures that the terminal identity and attribute information are not disclosed. In the protocol, the combination of attribute-based encryption (ABE) and Newton interpolation polynomial is adopted, which can support secure fine-grained group key agreement. By adopting asymmetric computing, the computing tasks are transferred to the edge server for execution to reduce the computing load of the terminal. The tamper-proof characteristics of blockchain technology are applied to realize the integrity verification of terminal identity and communication information so that the data can be traced. In addition, the protocol supports dynamic updating of attribute permissions to ensure the freshness of groups. Compared with the applied literature, this protocol has good performance in computing time, computing energy consumption and communication energy consumption.

收稿日期:2022-06-24;修回日期:2022-11-05;责任编辑:梅志强
*通讯作者:韩桂锋

Key words: edge-cloud collaboration; group key agreement; Newton interpolating polynomial; attribute-based encryption; dynamic attribute permissions; hidden attribute authentication

Foundation Item(s): National Natural Science Foundation of China (No.61971380, No.62072037, No.61772477); Collaborative Innovation Project of Zhengzhou (Major Training Program) (No.2021ZDPY0206)

1 介绍

随着智慧城市,智能交通,智慧医疗等新兴技术的发展,网络的传输能力和数据的处理能力面临巨大的挑战. 为了应对数据指数级增长,满足企业和个人的需求,边云协同计算成为解决这一问题的关键技术. 云计算能够为用户提供高算力,海量存储以及可扩展的可靠性服务,边缘计算具有低时延,高带宽以及敏捷计算的特点. 边云协同则可以继承两者的优点,能够很好的支撑视频、图像处理以及对网络低时延高带宽要求苛刻的各类新应用场景业务的实现. 因此,边云协同融合发展成为了当前的发展趋势. 边云协同场景在为人们工作和生活提供便利的同时,海量的数据传输,频繁的资源交换也给信息安全领域提出了新的要求. 如何在群组数据传输过程中保护终端的隐私,保障终端之间信息交换及通信的安全性是现在研究的热点话题.

GKA(Group Key Agreement)技术是解决该问题的关键技术之一,GKA通过建立一条安全高效的通信信道能够为群组实体提供可靠的数据传输服务,其应用领域非常广泛,涉及到军事、医疗、教育等生活的方方面面,比如军事部队的自组织网络安全通信,医疗数据的加密传输以及大数据环境下的多方协同计算等等,研究GKA技术具有重要的科学意义. 但是随着科学的进步与新型技术的诞生,目前GKA技术面临着新的挑战,如频繁海量的数据交换造成的终端隐私泄露问题,终端参与多群组通信的需求以及终端的能耗受限问题等. 针对上述问题,本文提出了边云协同场景中基于动态属性权限的GKA协议,能够为边云协同环境中的组成员建立一条安全的通信信道,而且支持终端跨域参与GKA. 协议的主要贡献如下:

(1)密钥证实算法. 针对传统的GKA方案中由密钥管理中心生成密钥,权威认证中心CA(Certificate Authority)认证及分发密钥等存在的密钥泄露风险问题,本文提出了一种密钥证实算法. 算法中终端的密钥由终端自己生成,并向CA证实自己的合法身份和公钥,因此不存在密钥生成及密钥分发的密钥泄露风险,提高了系统的安全性.

(2)隐藏属性认证. 为保障GKA的可认证性,终端在参与GKA之前需要进行身份认证. 只有认证通过后才能获得属性权限,进而参与GKA. 本文提出一种隐藏属性认证技术. 终端将属性加密隐藏后进行密文属性认证,不仅保护了终端的身份隐私,而且保证了终端的属性隐私不被泄露.

(3)细粒度的GKA. 具有不同属性的终端能够通过属性基加密认证获得对应的属性权限,终端将属性基加密和牛顿插值多项式相结合,终端能够一次性计算出多组群组密钥,即可同时参与多个群组安全通信,不仅减轻了终端的计算量,而且提高了GKA的灵活性.

(4)动态属性权限更新. 参与GKA的终端可能随时退出群组或者权限变更. 本文提出了一种动态属性权限更新技术,当群组终端退出群组或者权限变更时,群组密钥的计算需要做相应的变更,以确保群组密钥的新鲜性,进而保障群组间通信的安全性.

2 相关工作

近年来,许多专家和学者对GKA技术进行了深入研究. 根据算法的类型可以分为两大类:对称GKA和非对称GKA. 对于对称GKA典型的研究有Roy等人[1]通过引入一组服务器来承担计算任务,同时采用成本较小的哈希函数和对称加密算法,使得协议中的终端能够轻量负载,但对于对称GKA算法虽然设计的协议比较轻量,但是安全性不足. 因此设计更安全的协议,非对称GKA是更优的选择,Cheng等人[2]采用非对称算法通过多项式同时能够生成多个密钥,提高了计算效率的同时降低了计算成本,而且协议不需要密钥生成中心,更适用于复杂的物联网环境. Li等人利用椭圆曲线密码方案通过对原有方案进行改进,提高了系统的安全性[3],同时降低了协议的计算量和通信消耗,对比分析结果表明,该协议的效果较好. Zhang等人采用了多签名技术,使得协议具有不可伪造的特点[4],此外,该协议支持发送方追踪,具有很高的安全性和实用性.

为了应对非法终端参与或破坏群组通信问题,可认证的GKA协议应运而生. Chen等人提出了一种面向物联网的去中心化GKA协议,协议引入了区块链技术解决了传统集中式认证方案中存在的单点故障问题[5]. 此外,还设置了一个设备管理器将终端与区块链联系在一起,使得协议具有很高的可靠性. Yang等人结合切比雪夫多项式对终端的身份进行认证[6],提高了认证的效率. 同时,协议采用了假名技术来保护终端的隐私,通过分析,协议具有较低的计算和通信能耗,具有更高的效率. Chen等人[7]通过对原有的方案进行改进提出一种支持批量认证的协议,协议采用分布式的协议框架,不需要可信的第三方,具有较高的安全性和可靠性. Lee等人设计了一种支持组成员相互认证的方案[8],同时方案不要对私钥进行存储,占用的存储空间

较少,协议主要采用物理不可克隆函数进行设计,具有很高的安全性和计算效率. Xu等人[9]利用令牌技术完成终端的身份验证,计算成本较低,此外第一次认证后终端会获得标记,在以后的认证中会减少认证的时间成本,令牌有时间限制,能够抵抗已知的攻击. Zhang等人提出了一种属性认证方案[10],能够保护终端的隐私,提高了系统的安全性,同时该协议支持终端自己验证计算出的密钥是否正确,在计算和通信方面,该协议都有较好的效果. Sun等人利用假名技术提出了一种匿名认证的GKA协议[11],该协议不需要对终端的身份信息进行存储,节省了存储空间,而且协议中的防干扰设备不存在单点故障问题,此外,协议的计算消耗和通信消耗较低. Zheng等人[12]设计了一种将身份ID作为公钥的认证密钥协商协议,简化了密钥的管理,同时认证的效率被提高.

由于终端自身资源受限,难以完成大量的计算和通信任务,因此GKA协议需不断优化,越来越轻量. Naresh等人提出了一种轻量级GKA协议[13],协议只使用了异或操作和哈希操作,计算量较小,通过安全性分析可以看出,该协议能够抵抗已知的攻击,性能对比分析显示,该协议在各方面都占优. Braeken提出了一种适用于大规模的GKA协议[14],协议具有固定大小的广播消息,因此协议的通信量和参与GKA的终端数量无关,此外协议没有采用配对操作,比较适用于资源受限的场景. Cui等人结合混沌映射提出了一种GKA协议[15],协议分为两种类型,一种是服务器与群组管理员之间的GKA,另一种是群组成员之间的GKA,协议中没有复杂的幂指运算和乘法运算,有效地减少了计算时间. Santhanalakshmi等人结合神经密码学提出了一种GKA协议[16],减少了传统GKA方案的计算量的同时,利用神经网络能够解决密钥的新鲜度和安全性问题. Zhang等人针对终端资源受限问题提出了一种轻量级GKA协议[17],协议采用非对称算法,实现了发送方不受约束的安全机制,采用将复杂的计算任务转移到边缘服务器,实现了终端的轻量负载,此外,协议能够抵抗已知的攻击,具有很高的安全性.

随着新应用技术的产生以及终端需在不同域间移动而导致的随时加入和退出问题,协议不断改进,使其能够适应不同应用场景和动态性的需求. Zhang等人[18]使用区块链的可追溯和不可篡改的特性对关键参数进行记录,能够跟踪终端的非法行为,通过算法平均每个终端的计算量实现了负载均衡. Naresh等人[19]引入了切片技术将网络划分为若干个小型的网络,解决了吞吐量大和延迟高的问题,此外协议结合区块链技术实现了对非法成员恶意行为的追踪,具有较高的安全性. 针对现有方案中伸缩性差和安全性低等问题,Xu等人结合区块链提出了一种GKA协议[20],该协议采用终端对自己的邻居成员进行认证,提高了认证效率,同时解决了单点故障问题. Alwen等人提出了一种连续的GKA协议[21],该协议不需要可信的第三方,允许终端动态的加入或离开群组,协议具有一定的使用价值且安全性较高. Lin等人采用了一种动态更新组密钥的方案[22],当终端动态的加入或离开群组时不需要重新计算密钥,此外协议采用椭圆密码曲线和较短的密钥长度虽然能够降低协议的计算量,但是在安全性方面的问题还需进一步证明. Kamil等人提出了一种面向车载自组织网的GKA协议[23],通过引入路侧单元对消息的来源身份进行批量认证,提高了协议的计算效率,同时采用耗时较短的操作,使得协议更加轻量. Ayad等人为无人机自组织网络设计了一个GKA协议[24],该协议的实现没有配对操作,减轻了计算消耗,协议密钥的计算存在固定的轮数,所以该协议适用于大规模的机群中,此外,该协议的安全性较高. Wang等人针对端到端通信环境提出了一种基于隐私保护的认证密钥协商协议[25],协议能够在不泄露终端信息的情况下完成认证,实现了对终端身份的隐私保护,此外,方案的综合性能较好.

以上文献都对GKA技术进行了深入的研究,涵盖了很多的应用场景,它们都对GKA技术做出了杰出的贡献,但针对边云协同应用场景的群组密钥协商有较少的研究. 边云协同场景的应用较为复杂,群组密钥协商的参与者可能来自于多个不同的安全域,因此,需要跨域进行群组密钥协商. 同时,边云协同网络具有集中式和分布式网络相结合的性能优势,将群组密钥协商过程中大量的终端计算和通信负载迁移到边缘服务器上,以减少资源受限的智能终端的资源消耗. 此外,现有的群组密钥协商在密钥生成方面存在3个问题,(1)仍需要第三方进行密钥生成及密钥分发,存在密钥泄露的风险;(2)采用匿名或者基于属性的身份认证,难以彻底保障个人隐私问题;(3)对群组密钥协商参与者的约束不够灵活,难以对群组密钥协商的非法参与者进行追踪. 针对上述问题,本文提出了一种基于动态属性权限的GKA协议,对传统权威中心分发私钥的协议进行改进,设计了一种密钥证实方法,降低了私钥泄露的风险,提高了系统的安全性;采用了一种隐藏属性认证方案能够保护终端的身份和属性隐私;同时协议还支持终端属性权限的申请和撤销,终端能够同时以不同的权限等级参与多个群组的密钥协商.

3　群组密钥协商协议框架

云计算擅长全局性、非实时、长周期的大数据处理与分析,而边缘计算更适合局部性、实时、短周期数据

的处理和分析;边缘计算和云计算的协同(Edge-cloud Collaboration),可以大幅度扩展其应用范围、大幅度提升所提供的服务质量,从而放大边缘计算与云计算各自的应用价值.GKA数据资源共享是各应用场景中互联设备间的资源共享,信息交换、协同计算等相互操作的桥梁和纽带,也是边云协同应用场景的核心技术之一.

在本节中面向边云协同的GKA协议的框架被设计,主要思想如下:(1)不同的群组有不同的安全级别,各群组通过设定不同的属性权限组合来限定终端参与密钥协商.(2)具有不同的属性的终端通过注册获得属性权限.只有满足对应属性权限集合的终端才能够加入群组参与密钥协商.(3)如果属性权限不满足要求,终端可以向云服务器申请新的属性权限参与更高级别的GKA,同时当终端收到惩罚时,其属性权限也会被撤销,边云协同网络框架图如图1所示.

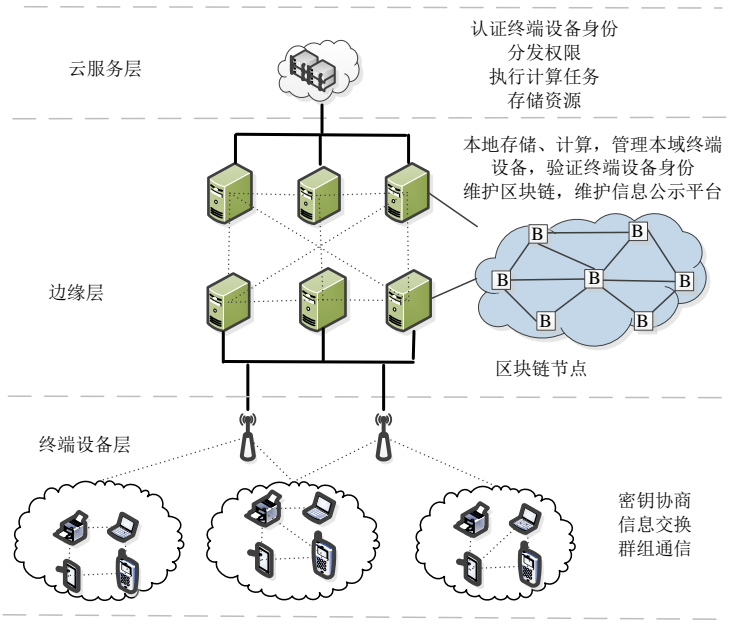

图1 边云协同网络框架图

协议中各实体的结构如下.

云服务层:云服务器拥有丰富的计算算力和存储空间,其能够执行大规模且复杂的计算任务,存储海量的数据资源,此外它还需要制定系统属性的认证策略,对系统中的终端进行身份认证,并为他们分发属性权限.

边缘服务层:相较于云服务器,边缘服务器的计算和存储资源相对匮乏,但其距终端较近,能够为终端提供高带宽、低时延以及高效率的便捷服务.此外,边缘服务器还需管理本域的终端,在终端参与GKA之前验证其身份和权限.

终端层:它由众多的固定或资源受限的移动智能终端组成,终端的主要特点是计算能力弱,存储空间小,通信范围有限.它只有在通过云服务器的认证后才能进行GKA,通过协商的群组密钥进行群组间安全的信息交换及通信.

区块链:该区块链为联盟链,由所有的边缘服务器共同创建和维护.属性权限分发成功后,终端成员的身份、权限以及对应的时间戳等信息会以交易的形式写入区块.如果终端的权限信息发生变化,其上级边缘服务器会及时的更新,并将新的区块链接到区块链中,终端的身份权限信息以最新时间的记录为准.

信息公示平台:该平台公示的信息包括终端的属性权限参数、属性序列号、公钥以及IP地址等信息,信息公示平台由各边缘服务器共同维护.

4 群组密钥协商协议的基础知识

4.1 双线性映射

假设G_1和G_2是两个具有相同的大素数阶q的群,其中G_1是一个加法群,它的生成元为g_1,G_2是一个乘法群,且需满足$q\geqslant 2^{\ell}+1$(ℓ是一个安全参数).H_1:$\{0,1\}^{*}\rightarrow G_1$,$H_2$:$\{0,1\}^{*}\rightarrow \mathbb{Z}_q^{*}$,$H_3$:$G_1\rightarrow \mathbb{Z}_q^{*}$和$H_4$:$G_2\rightarrow \mathbb{Z}_q^{*}$是四个抗碰撞的哈希函数.$e$:$G_1\times G_1\rightarrow G_2$是一个$G_1$到$G_2$的可计算的双线性映射函数,它满足如下性质.

(1)双线性:对于任意的元素$a,b\in \mathbb{Z}_q^{*}$和$\mu,v\in G_1$,等式$e(a\mu,bv)=e(\mu,v)^{ab}$恒成立.

(2)非退化性:对于任意的元素$g\in G_1$,有

$e(g,g)\neq 1$.

(3)可计算性:对于任意给定的$\mu,v\in G_1$,在多项式时间内存在有效的算法可计算$e(\mu,v)$.

推理 1　对于任意给定的元素$\mu_1,\mu_2,v\in G_1$,有$e(\mu_1+\mu_2,v)=e(\mu_1,v)e(\mu_2,v)$.

定义 1　离散对数问题:对于G_1上的任意点$g\in G_1$及任意整数$a\in\mathbb{Z}_q^*$,已知g和a,很容易求解出$Q=ag$,但已知$Q=ag$和g,在多项式时间内无法从Q求解出a的值.

定义 2　系统密钥生成函数 Keygen:Keygen$(1^\lambda)\rightarrow$(PK,MSK)即 CA 输入一个λ长度的二进制串(λ为安全参数),生成系统的公钥 PK$\in G_1$和主密钥 MSK$\in\mathbb{Z}_q^*$,其中,PK=MSKg_1.

定义 3　逆 Diffie-Hellman 问题(IDHP)假设:对于G_1上的任意点$ag,abg\in G_1$及任意正整数$a,b\in\mathbb{Z}_q^*$,已知ag和abg,在多项式时间内无法求解$(ab/a)g$.

定义 4　哈希函数$H_1:\{0,1\}^*\rightarrow G_1$:输入一个任意长度的比特串集合,输出一个加法群$G_1$群中的元素.

定义 5　哈希函数$H_2:\{0,1\}^*\rightarrow\mathbb{Z}_q^*$:输入一个任意长度的比特串集合,输出一个数$\partial$,其中,$\partial\in\mathbb{Z}_q^*$.

定义 6　哈希函数$H_3:G_1\rightarrow\mathbb{Z}_q^*$:输入一个加法群$G_1$群中的元素,输出一个数$\varepsilon$,其中,$\varepsilon\in\mathbb{Z}_q^*$.

定义 7　哈希函数$H_4:G_2\rightarrow\mathbb{Z}_q^*$:输入一个乘法群$G_2$中的元素,输出一个数$\vartheta$,其中,$\vartheta\in\mathbb{Z}_q^*$.

4.2　牛顿插值多项式

给定函数$f(x)$和$n+1$个不同的插值节点$x_0,x_1,\cdots,x_n$. 定义$f(x_m)$为$f(x)$在节点x_m处的零阶差商,$f(x_m,x_n)=(f(x_n)-f(x_m))/(x_n-x_m)$为$f(x)$在节点$x_m$和节点$x_n$处的一阶差商,$f(x_m,x_n,x_k)=(f(x_n,x_k)-f(x_m,x_n))/(x_k-x_m)$为函数$f(x)$在节点$x_m,x_n$以及$x_k$处的二阶差商.

一般的,可用$f(x_0,x_1,\cdots,x_k)$表示$f(x)$在节点$x_0,x_1,\cdots,x_k$处的k阶差商,$f(x_0,x_1,\cdots,x_k)=\dfrac{f(x_1,x_2,\cdots,x_k)-f(x_0,x_1,\cdots,x_{k-1})}{x_k-x_0}$. 也可以表示为函数值的组合$f(x_0,x_1,\cdots,x_k)=\sum_{i=0}^{k}\dfrac{f(x_i)}{\prod_{j=0,j\neq i}^{k}(x_i-x_j)}$.

公式的一般推导形式如下,$f(x)$的各阶差商为

$$\begin{cases} f(x,x_0)=\dfrac{f(x_0)-f(x)}{(x_0-x)} \\ f(x,x_0,x_1)=\dfrac{f(x_0,x_1)-f(x,x_0)}{(x_1-x)} \\ \cdots \\ f(x,x_0,x_1,\cdots,x_k)=\dfrac{f(x_0,x_1,\cdots,x_k)-f(x,x_0,\cdots,x_{k-1})}{(x_k-x)} \end{cases} \tag{1}$$

变形可得

$$\begin{cases} f(x)=f(x_0)+(x-x_0)f(x,x_0) \\ f(x,x_0)=f(x_0,x_1)+(x-x_1)f(x,x_0,x_1) \\ \cdots \\ f(x,x_0,\cdots,x_k)=f(x_0,x_1,\cdots,x_k)+(x-x_k)f(x,x_0,\cdots,x_k) \end{cases} \tag{2}$$

分别带入可以得到牛顿插值公式为

$$\begin{aligned} f(x)=&f(x_0)+(x-x_0)f(x_0,x_1) \\ &+(x-x_0)(x-x_1)f(x_0,x_1,x_2)+\cdots \\ &+(x-x_0)(x-x_1)\cdots(x-x_{k-1})f(x_0,x_1,\cdots,x_n) \end{aligned} \tag{3}$$

4.3　符号及其说明

为了便于理解本文所提出的协议,下面列举了文中用到的符号以及它们对应的解释,具体如表1所示.

表1　符号及其解释

符号	解释
G_1	椭圆曲线上的加法群
G_2	椭圆曲线上的乘法群
g_1	加法群G_1的生成元
ℓ	安全参数
q	足够大的素数
e	双线性映射
H_i	抗碰撞的哈希函数
M^*	明文空间
$\mathrm{pk}_{\mathrm{CS}},\mathrm{sk}_{\mathrm{CS}}$	云服务器的公钥和私钥
$\mathrm{pk}_{\mathrm{ES}_i},\mathrm{sk}_{\mathrm{ES}_i}$	边缘服务器ES_i的公钥和私钥
$\mathrm{pk}_{u_{i,j}},\mathrm{sk}_{u_{i,j}}$	终端$u_{i,j}$的公钥和私钥

5　群组密钥协商过程

5.1　密钥证实算法

为了解决传统 GKA 过程中认证中心 CA 为系统实体分发密钥带来的安全隐患,本文设计了一种密钥证实算法,CA 将实体身份与公钥相关联的方式确定系统实体的真实身份. 假设 CA 知道系统实体u的身份标识为id_u,系统实体包括云服务器,边缘服务器以及终端,密钥证实的具体过程如下:

(1)CA 运行系统密钥生成算法 Keygen 并在网络中广播系统参数$\{g_1,G_1,e,q,H_1,H_2,H_3,H_4,\mathrm{PK}\}$.

(2)u随机选取一个正整数$r\in\mathbb{Z}_q^*$作为私钥,然后计算公钥$\mathrm{pk}=rg_1$和证实密钥所需的参数$w_1=H_2(\mathrm{id}_u)rg_1$,$w_2=r\mathrm{PK}$,$w_3=H_2(\mathrm{id}_u)\mathrm{PK}$和$w_4=H_1(\mathrm{id}_u\|w_1\|w_2\|w_3\|\mathrm{pk})$. 然后将消息$\{\mathrm{id}_u,w_1,w_2,w_3,w_4,\mathrm{pk}\}$发送给 CA.

(3)CA 收到消息$\{\mathrm{id}_u,w_1,w_2,w_3,w_4,\mathrm{pk}\}$后,计算$w_2'=\mathrm{MSK}^{-1}w_2=\mathrm{pk}=rg_1$,$w_3'=\mathrm{MSK}^{-1}w_3=H_2(\mathrm{id}_u)g_1$,$w_4'=H_1(\mathrm{id}_u\|w_1\|w_2\|w_3\|\mathrm{pk})$,并通过计算等式$w_4'=w_4$是否成立来验证消息传输过程中是否被篡改,及等式$e(w_2,w_3')=$

$e(w_3, w_2')$是否成立来验证公钥pk和身份id_u的对应关系,如果等式成立,CA公布实体u的有效公钥pk. 也就是说u生成了自己的公私密钥对(pk, r).

假设通过上述过程云服务器CS(Cloud Server)生成的公私密钥对为$(\mathrm{pk}_{\mathrm{cs}}, \mathrm{sk}_{\mathrm{cs}})$,边缘服务器$\mathrm{ES}_i$的公私密钥对为$(\mathrm{pk}_{\mathrm{ES}_i}, \mathrm{sk}_{\mathrm{ES}_i})$,终端$u_{i,j}$的公私密钥对为$(\mathrm{pk}_{u_{i,j}}, \mathrm{sk}_{u_{i,j}})$其中$\mathrm{ES}_i$表示边云协同网络中的第$i$个边缘服务器,$u_{i,j}$表示第$i$个边缘管理域的第$j$个终端,$u_{i,j}$的身份标识为$\mathrm{id}_{u_{i,j}}$.

5.2 终端属性权限的获取

终端在参与GKA之前需要属性权限认证,只有通过认证并获得属性权限的终端才能够参与GKA. 假设边云协同网络中有N个边缘服务器管理域,每个边缘服务器根据IP最多管理n个终端. 云服务器定义系统的有序属性集合为$\mathrm{set}_{\mathrm{attr}}=\{\mathrm{Attr}_1, \mathrm{Attr}_2, \cdots, \mathrm{Attr}_T\}$,对应的属性序列号为$\{S_1, S_2, \cdots, S_T\}$,任意终端$u_{i,j}(1\leqslant i\leqslant N, 1\leqslant j\leqslant n)$的有序属性集合为$\mathrm{set}_{u_{i,j}}=\{\mathrm{attr}_{i,j,1}, \mathrm{attr}_{i,j,2}, \cdots, \mathrm{attr}_{i,j,t}\}(\mathrm{set}_{u_{i,j}}\subseteq\mathrm{set}_{\mathrm{attr}}, 1\leqslant t\leqslant T)$,其中$i$表示$u_{i,j}$属于$\mathrm{ES}_i$边缘域,$j$表示$u_{i,j}$为$\mathrm{ES}_i$边缘域的第$j$个终端,$t$表示为$u_{i,j}$的第$t$个属性,$\mathrm{attr}_{i,j,t}=\mathrm{Attr}_t(1\leqslant t\leqslant T)$. 终端属性认证和属性权限的算法如算法1所示,其获取过程如下:

(1)云服务器CS根据系统的有序属性集合$\mathrm{set}_{\mathrm{attr}}=\{\mathrm{Attr}_1, \mathrm{Attr}_2, \cdots, \mathrm{Attr}_T\}$随机为每个属性选择一个对应的属性参数,假设随机选择的T个属性参数组成的集合为$\mathrm{ap}=\{b_1, b_2, \cdots, b_T\}$,其中,$b_k\in\mathbb{Z}_q^*(1\leqslant k\leqslant T)$,然后广播系统有序属性集及其对应的属性序列号$\{S_1, S_2, \cdots, S_T\}$.

(2)收到CS广播的有序属性集后,$u_{i,j}$随机选择$l_{i,j}\in\mathbb{Z}_q^*$,计算$L_{i,j}=l_{i,j}\mathrm{pk}_{\mathrm{cs}}$,$\gamma_{u_{i,j,1}}=H_2(\mathrm{attr}_{i,j,1})l_{i,j}g_1$,$\gamma_{u_{i,j,2}}=H_2(\mathrm{attr}_{i,j,2})l_{i,j}g_1$,$\cdots$,$\gamma_{u_{i,j,t}}=H_2(\mathrm{attr}_{i,j,t})l_{i,j}g_1$及$\sigma_{u_{i,j}}=\mathrm{sk}_{u_{i,j}}^{-1}H_2(\mathrm{attr}_{i,j,1}\|\mathrm{attr}_{i,j,2}\|\cdots\|\mathrm{attr}_{i,j,t})g_1$,然后将消息$\{L_{i,j}, (\gamma_{u_{i,j,1}}, \gamma_{u_{i,j,2}}, \cdots, \gamma_{u_{i,j,t}}), \sigma_{u_{i,j}}, \mathrm{id}_{u_{i,j}}\}$发送给CS.

(3)CS收到$u_{i,j}$发送的$\{L_{i,j}, (\gamma_{u_{i,j,1}}, \gamma_{u_{i,j,2}}, \cdots, \gamma_{u_{i,j,t}}), \sigma_{u_{i,j}}, \mathrm{id}_{u_{i,j}}\}$后,分别计算$L'_{i,j}=\mathrm{sk}_{\mathrm{cs}}^{-1}L_{i,j}=l_{i,j}g_1$,$\gamma_{\mathrm{cs}_{i,j,1}}=H_2(\mathrm{Attr}_1)L'_{i,j}$,$\gamma_{\mathrm{cs}_{i,j,2}}=H_2(\mathrm{Attr}_2)L'_{i,j}$,$\cdots$,$\gamma_{\mathrm{cs}_{i,j,T}}=H_2(\mathrm{Attr}_T)L'_{i,j}$并计算$\{\gamma_{u_{i,j,1}}, \gamma_{u_{i,j,2}}, \cdots, \gamma_{u_{i,j,t}}\}\cap\{\gamma_{\mathrm{cs}_{i,j,1}}, \gamma_{\mathrm{cs}_{i,j,2}}, \cdots, \gamma_{\mathrm{cs}_{i,j,T}}\}$来确定$u_{i,j}$具有的有序属性集合为$\{\mathrm{Attr}_1, \mathrm{Attr}_2, \cdots, \mathrm{Attr}_t\}(\mathrm{attr}_{i,t}=\mathrm{Attr}_t(1\leqslant t\leqslant T))$,CS计算$H_2(\mathrm{Attr}_1\|\mathrm{Attr}_2\|\cdots\|\mathrm{Attr}_t)g_1$,并通过等式$e(\sigma_{u_{i,j}}, \mathrm{pk}_{u_{i,j}})=e(H_2(\mathrm{Attr}_1\|\mathrm{Attr}_2\|\cdots\|\mathrm{Attr}_t)g_1, g_1)$验证$u_{i,j}$的签名,如果等式成立,则可确定$u_{i,j}$拥有属性集$\{\mathrm{attr}_{i,j,1}, \mathrm{attr}_{i,j,2}, \cdots, \mathrm{attr}_{i,j,t}\}$,CS从集合ap中选择对应的属性参数$\{b_1, b_2, \cdots, b_t\}$,并计算属性权限$\chi_{u_{i,j,1}}=b_1H_2(\mathrm{Attr}_1)L'_{i,j}$,$\chi_{u_{i,j,2}}=b_2H_2(\mathrm{Attr}_2)L'_{i,j}$,$\cdots$,$\chi_{u_{i,j,t}}=b_tH_2(\mathrm{Attr}_t)L'_{i,j}$,$\delta_{\mathrm{cs}_{i,j}}=\mathrm{sk}_{\mathrm{cs}}^{-1}H_3(\chi_{u_{i,j,1}}\|\chi_{u_{i,j,2}}\|\cdots\|\chi_{u_{i,j,t}})g_1$,然后CS将信息$\{\chi_{u_{i,j,1}}, \chi_{u_{i,j,2}}, \cdots, \chi_{u_{i,j,t}}, \delta_{\mathrm{cs}_{i,j}}, \mathrm{pk}_{\mathrm{cs}}\}$发送给$u_{i,j}$.

(4)$u_{i,j}$收到CS发送的$\{\chi_{u_{i,j,1}}, \chi_{u_{i,j,2}}, \cdots, \chi_{u_{i,j,t}}, \delta_{\mathrm{cs}_{i,j}}, \mathrm{pk}_{\mathrm{cs}}\}$消息后,通过等式$e(\delta_{\mathrm{cs}_{i,j}}, \mathrm{pk}_{\mathrm{cs}})=e(H_3(\chi_{u_{i,j,1}}\|\chi_{u_{i,j,2}}\|\cdots\|\chi_{u_{i,j,t}})g_1, g_1)$验证CS的签名身份,如果验证等式成立,则分别计算属性权值$\rho_{u_{i,j,1}}=l_{i,j}^{-1}\chi_{u_{i,j,1}}=b_1H_2(\mathrm{attr}_{i,j,1})g_1$,$\rho_{u_{i,j,2}}=l_{i,j}^{-1}\chi_{u_{i,j,2}}=b_2H_2(\mathrm{attr}_{i,j,2})g_1$,$\cdots$,$\rho_{u_{i,j,t}}=l_{i,j}^{-1}\chi_{u_{i,j,t}}=b_tH_2(\mathrm{attr}_{i,j,t})g_1$,$u_{i,j}$的属性集$\mathrm{attr}_{u_{i,j}}=\{\mathrm{attr}_{i,j,1}, \mathrm{attr}_{i,j,2}, \cdots, \mathrm{attr}_{i,j,t}\}$对应的属性权值为$\{\rho_{u_{i,j,1}}, \rho_{u_{i,j,2}}, \cdots, \rho_{u_{i,j,t}}\}$,具体过程如算法1所示.

(5)由于边缘服务器$\mathrm{ES}_i(1\leqslant i\leqslant N)$的特殊性,被认为具有系统属性集$\mathrm{set}_{\mathrm{attr}}=\{\mathrm{Attr}_1, \mathrm{Attr}_2, \cdots, \mathrm{Attr}_T\}$的所有

算法1 终端属性权限的获取

输入:有序属性集合$\mathrm{set}_{\mathrm{attr}}=\{\mathrm{attr}_{i,j,1}, \mathrm{attr}_{i,j,2}, \cdots, \mathrm{attr}_{i,j,t}\}$、属性参数集合$\mathrm{ap}=\{b_1, b_2, \cdots, b_t\}$和属性序列号$\{S_1, S_2, \cdots, S_t\}$

输出:属性权值$\{\rho_{u_{i,j,1}}, \rho_{u_{i,j,2}}, \cdots, \rho_{u_{i,j,t}}\}$

步骤1:云服务器CS广播有序属性集合$\mathrm{set}_{\mathrm{attr}}=\{\mathrm{Attr}_1, \mathrm{Attr}_2, \cdots, \mathrm{Attr}_T\}$、属性参数$\mathrm{ap}=\{b_1, b_2, \cdots, b_T\}$和属性序列号$\{S_1, S_2, \cdots, S_T\}$

步骤2:$u_{i,j}(1\leqslant j\leqslant n)$随机选择$l_{i,j}\in\mathbb{Z}_q^*$并计算$L_{i,j}=l_{i,j}\mathrm{pk}_{\mathrm{cs}}$和

FOR k=1 to t DO

$\gamma_{u_{i,j,k}}=H_2(\mathrm{attr}_{i,j,k})l_{i,j}g_1$

END FOR

$u_{i,j}$计算签名$\sigma_{u_{i,j}}=\mathrm{sk}_{u_{i,j}}^{-1}H_2(\mathrm{attr}_{i,j,1}\|\mathrm{attr}_{i,j,2}\|\cdots\|\mathrm{attr}_{i,j,t})g_1$并将消息$\{L_{i,j}, (\gamma_{u_{i,j,1}}, \gamma_{u_{i,j,2}}, \cdots, \gamma_{u_{i,j,t}}), \sigma_{u_{i,j}}, \mathrm{id}_{u_{i,j}}\}$发送给CS

步骤3:CS计算$L'_{i,j}=\mathrm{sk}_{\mathrm{cs}}^{-1}L_{i,j}=l_{i,j}g_1$和

FOR k=1 to T DO

$\gamma_{\mathrm{cs}_{i,j,k}}=H_2(\mathrm{Attr}_k)L'_{i,j}$

END FOR

CS计算$\{\gamma_{u_{i,j,1}}, \gamma_{u_{i,j,2}}, \cdots, \gamma_{u_{i,j,t}}\}\cap\{\gamma_{\mathrm{cs}_{i,j,1}}, \gamma_{\mathrm{cs}_{i,j,2}}, \cdots, \gamma_{\mathrm{cs}_{i,j,T}}\}$、$H_2(\mathrm{Attr}_1\|\mathrm{Attr}_2\|\cdots\|\mathrm{Attr}_t)g_1$和$e(\sigma_{u_{i,j}}, \mathrm{pk}_{u_{i,j}})=e(H_2(\mathrm{Attr}_1\|\mathrm{Attr}_2\|\cdots\|\mathrm{Attr}_t)g_1, g_1)$验证签名的合法性,然后根据参数$\{b_1, b_2, \cdots, b_t\}$计算

FOR k=1 to t DO

$\chi_{u_{i,j,k}}=b_kH_2(\mathrm{Attr}_k)L'_{i,j}$

END FOR

CS计算签名$\delta_{\mathrm{cs}_{i,j}}=\mathrm{sk}_{\mathrm{cs}}^{-1}H_3(\chi_{u_{i,j,1}}\|\chi_{u_{i,j,2}}\|\cdots\|\chi_{u_{i,j,t}})g_1$并将消息$\{\chi_{u_{i,j,1}}, \chi_{u_{i,j,2}}, \cdots, \chi_{u_{i,j,t}}, \delta_{\mathrm{cs}_{i,j}}, \mathrm{pk}_{\mathrm{cs}}\}$发送给$u_{i,j}$

步骤4:$u_{i,j}$计算$e(\delta_{\mathrm{cs}_{i,j}}, \mathrm{pk}_{\mathrm{cs}})=e(H_3(\chi_{u_{i,j,1}}\|\chi_{u_{i,j,2}}\|\cdots\|\chi_{u_{i,j,t}})g_1, g_1)$验证CS的身份并计算属性权值

FOR k=1 to t DO

$\rho_{u_{i,j,k}}=l_{i,j}^{-1}\chi_{u_{i,j,k}}=b_1H_2(\mathrm{attr}_{i,j,k})g_1$

END FOR

属性,并根据上述过程计算获得所有的属性权值 $\{\rho_{\mathrm{ES}_{i,1}}=b_1H_2(\mathrm{Attr}_1)g_1,\rho_{\mathrm{ES}_{i,2}}=b_2H_2(\mathrm{Attr}_2)g_1,\cdots,\ \rho_{\mathrm{ES}_{i,T}}=b_TH_2(\mathrm{Attr}_T)g_1\}$.

(6)CS根据 $u_{i,j}$ 的IP地址和边缘服务器 $\mathrm{ES}_i(1\leqslant i\leqslant N)$ 的IP进行管理域的划分,并将 ES_i 所属终端 $u_{i,j}$ 的注册信息 $\{(\chi_{u_{i,j,1}},\chi_{u_{i,j,2}},\cdots,\chi_{u_{i,j,t}}),(S_1,S_2,\cdots,S_t),\mathrm{pk}_{u_{i,j}},\mathrm{id}_{u_{i,j}},\mathrm{IP}_{u_{i,j}}\}$ 发给 ES_i,随后 ES_i 将信息 $\{(\chi_{u_{i,j,1}},\chi_{u_{i,j,2}},\cdots,\chi_{u_{i,j,t}}),\mathrm{pk}_{u_{i,j}},L_{i,j},\mathrm{IP}_{u_{i,j}},\mathrm{time}_{u_{i,j}}\}$ 以交易的形式形成区块,并链接在联盟区块链中,对信息公示平台进行更新,其中 $\mathrm{time}_{u_{i,j}}$ 表示交易的时间戳,区块的结构如图2所示,信息公示平台公布的信息如表2所示.

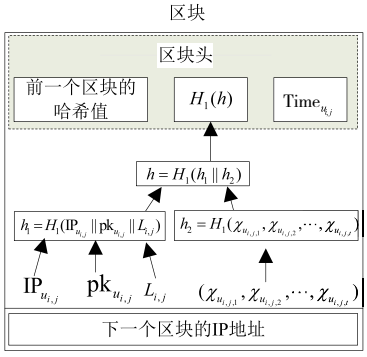

图2　区块的结构

表2　信息公示平台

终端	公钥	属性权限参数	IP地址
$u_{i,1}(1\leqslant i\leqslant N)$	$\mathrm{pk}_{u_{i,1}}$	$\chi_{u_{i,1,1}},\chi_{u_{i,1,2}},\cdots,\chi_{u_{i,1,k}}$	$\mathrm{IP}_{u_{i,1}}$
$u_{i,2}(1\leqslant i\leqslant N)$	$\mathrm{pk}_{u_{i,2}}$	$\chi_{u_{i,2,1}},\chi_{u_{i,2,2}},\cdots,\chi_{u_{i,2,r}}$	$\mathrm{IP}_{u_{i,2}}$
…	…	…	…
$u_{i,j}(1\leqslant i\leqslant N)$	$\mathrm{pk}_{u_{i,j}}$	$\chi_{u_{i,n,1}},\chi_{u_{i,n,2}},\cdots,\chi_{u_{i,n,t}}$	$\mathrm{IP}_{u_{i,j}}$
…	…	…	…
$u_{i,n}(1\leqslant i\leqslant N)$	$\mathrm{pk}_{u_{i,n}}$	$\chi_{u_{i,n,1}},\chi_{u_{i,n,2}},\cdots,\chi_{u_{i,n,t}},\chi_{u_{i,n,v}}$	$\mathrm{IP}_{u_{i,n}}$

5.3　群组密钥计算

信息交换往往需要在具有相同安全等级或者特定权限的群组终端之间进行,因此具有相同属性集的终端才能组成一个群组进行密钥协商. GKA之前,边缘服务器需要进行初始化操作,边缘服务器 ES_i 首先计算 $x_1=H_3(\rho_{\mathrm{ES}_{i,1}})$, $x_2=H_3(\rho_{\mathrm{ES}_{i,2}})$, …, $x_T=H_3(\rho_{\mathrm{ES}_{i,T}})$. 其中 $\rho_{u_{i,k,t}}=\rho_{\mathrm{ES}_{i,t}}(1\leqslant i\leqslant N,1\leqslant j\leqslant n,1\leqslant t\leqslant T)$,然后随机选择 T 个正整数 $d_i\in\mathbb{Z}_q^*(0\leqslant i\leqslant T-1)$ 构造多项式 $f(x)=d_0+d_1x+d_2x^2+\cdots+d_{T-1}x^{T-1}$. $\mathrm{ES}_i(1\leqslant i\leqslant N)$ 将所有属性权值集合的哈希值分别带入多项式求值得到 $\{f(x_1),f(x_2),\cdots,f(x_T)\}$, 然后 $\mathrm{ES}_i(1\leqslant i\leqslant N)$ 根据公式 $f(x_1,x_2,\cdots,x_k)=\sum_{i=1}^{k}\frac{f(x_i)}{\prod_{j=1,j\neq i}^{k}(x_i-x_j)}(1\leqslant k\leqslant T)$ 分别计算 $t(0\leqslant t\leqslant k-1)$ 阶差商 $f(x_1)$, $f(x_1,x_2)=(f(x_2)-f(x_1))/(x_2-x_1)$, …, $f(x_1,x_2,\cdots,x_t)=(f(x_2,x_3,\cdots,x_t)-f(x_1,x_2,\cdots,x_{t-1}))/(x_t-x_1)$. 差商集合 $\{f(x_1),f(x_1,x_2),\cdots,f(x_1,x_2,\cdots,x_t)\}$ 将会作为群组密钥因子发送给参与GKA的终端. 群组密钥计算如算法2所示,其计算过程如下.

5.3.1　身份及权限验证

(1)GKA发起者 $u_{i,\tau}(1\leqslant\tau\leqslant n)$ 广播具有属性权限集或者子集为属性权限集 $\{\chi_{u_{i,\tau,1}},\chi_{u_{i,\tau,2}},\cdots,\chi_{u_{i,\tau,t}}\}$ 的终端进行GKA. $u_{i,\tau}$ 首先计算参与GKA需要的属性及其哈希值 $h_{u_{i,\tau,1}}=H_2(\mathrm{attr}_{i,\tau,1}),h_{u_{i,\tau,2}}=H_2(\mathrm{attr}_{i,\tau,2}),\cdots,h_{u_{i,\tau,t}}=H_2(\mathrm{attr}_{i,\tau,t})$, 假设 $\{\chi_{u_{i,\tau,1}},\chi_{u_{i,\tau,2}},\cdots,\chi_{u_{i,\tau,t}}\}$ 对应的属性哈希值的集合为 $\{h_{u_{i,\tau,1}},h_{u_{i,\tau,2}},\cdots,h_{u_{i,\tau,t}}\}$, $u_{i,\tau}$ 将GKA具有属性哈希值及其身份信息 $\{h_{u_{i,\tau,1}},h_{u_{i,\tau,2}},\cdots,h_{u_{i,\tau,t}},\mathrm{id}_{u_{i,\tau}},\mathrm{pk}_{u_{i,\tau}}\}$ 广播到系统网络上.

(2)其它任意成员 $u_{i,j}(1\leqslant j\leqslant n)$ 及 ES_i 收到 $u_{i,\tau}$ 发起的GKA消息后,分别根据自己的属性计算 $\{h_{u_{i,j,1}}=H_2(\mathrm{attr}_{i,j,1}),\cdots,h_{u_{i,j,t}}=H_2(\mathrm{attr}_{i,j,t})\}$ 和 $\{h_{\mathrm{ES}_{i,1}}=H_2(\mathrm{Attr}_{i,1}),\cdots,h_{\mathrm{ES}_{i,T}}=H_2(\mathrm{Attr}_{i,T})\}$, $u_{i,j}$ 根据自己计算的属性哈希值 $\{h_{u_{i,j,1}},h_{u_{i,j,2}},\cdots,h_{u_{i,j,t}}\}$ 与 $u_{i,\tau}$ 广播的属性哈希值集合 $\{h_{u_{i,\tau,1}},h_{u_{i,\tau,2}},\cdots,h_{u_{i,\tau,t}}\}$ 进行对比,如果有 $\{h_{u_{i,\tau,1}},h_{u_{i,\tau,2}},\cdots,h_{u_{i,\tau,t}}\}\subseteq\{h_{u_{i,j,1}},h_{u_{i,j,2}},\cdots,h_{u_{i,j,t}}\}$, 则可以以判定自己有权限参与该GKA.

(3)有权限参与GKA的任意终端 $u_{i,j}(1\leqslant j\leqslant n)$(包括 $u_{i,\tau}$)根据自己在属性认证过程中的参数 $l_{i,j}\in\mathbb{Z}_q^*$, 计算 $E_{i,j}=l_{i,j}\mathrm{pk}_{\mathrm{ES}_i}$, 属性哈希值的签名 $\delta_{u_{i,j}}=\mathrm{sk}_{u_{i,j}}^{-1}H_3(h_{u_{i,j,1}}\|h_{u_{i,j,2}}\|\cdots\|h_{u_{i,j,t}})g_1$, 哈希值 $h_{u_{i,j}}=H_1(\delta_{u_{i,j}}\|\mathrm{IP}_{u_{i,j}}\|\mathrm{pk}_{u_{i,j}}\|E_{i,j})$, 并将GKA申请信息 $\{(h_{u_{i,\tau,1}},h_{u_{i,\tau,2}},\cdots,h_{u_{i,\tau,t}}),h_{u_{i,j}},\mathrm{pk}_{u_{i,j}},\mathrm{IP}_{u_{i,j}},\delta_{u_{i,j}},E_{i,j}\}$ 发送给本域边缘服务器 ES_i.

(4) ES_i 收到消息 $\{(h_{u_{i,\tau,1}},h_{u_{i,\tau,2}},\cdots,h_{u_{i,\tau,t}}),h_{u_{i,j}},\mathrm{pk}_{u_{i,j}},\mathrm{IP}_{u_{i,j}},\delta_{u_{i,j}},E_{i,j}\}$ 后,首先在区块链中查询 $u_{i,j}$ 的 $\mathrm{IP}_{u_{i,j}}$ 和属性权限集 $\chi_{u_{i,j}}=\{\chi_{u_{i,j,1}},\chi_{u_{i,j,2}},\cdots,\chi_{u_{i,j,t}}\}$, 并计算 $h_{\mathrm{ES}_i}=H_1(\delta_{u_{i,j}}\|\mathrm{IP}_{u_{i,j}}\|\mathrm{pk}_{u_{i,j}}\|E_{i,j})$, 如果 $h_{u_{i,j}}=h_{\mathrm{ES}_i}$, ES_i 分别计算 $E'_{i,j}=\mathrm{sk}_{\mathrm{ES}_i}^{-1}E_{i,j}=l_{i,j}g_1$, $\gamma_{\mathrm{ES}_{i,1}}=H_2(\mathrm{Attr}_{i,1})E'_{i,j}$, $\gamma_{\mathrm{ES}_{i,2}}=H_2(\mathrm{Attr}_{i,2})E'_{i,j},\cdots,\gamma_{\mathrm{ES}_{i,t}}=H_2(\mathrm{Attr}_{i,t})E'_{i,j}$, 如果有 $\chi_{u_{i,j}}=\{\chi_{u_{i,j,1}},\chi_{u_{i,j,2}},\cdots,\chi_{u_{i,j,t}}\}=\{\gamma_{\mathrm{ES}_{i,1}},\gamma_{\mathrm{ES}_{i,2}},\cdots,\gamma_{\mathrm{ES}_{i,t}}\}$ 且 $\{h_{u_{i,\tau,1}},h_{u_{i,\tau,2}},\cdots,h_{u_{i,\tau,t}}\}\subseteq\{h_{u_{i,j,1}},h_{u_{i,j,2}},\cdots,h_{u_{i,j,t}}\}$, ES_i 计算 $H_3(h_{\mathrm{ES}_{i,1}}\|h_{\mathrm{ES}_{i,2}}\|\cdots\|h_{\mathrm{ES}_{i,t}})$

g_1,并通过等式$e(\delta_{u_{i,j}},\mathrm{pk}_{u_{i,j}})=e(H_3(h_{\mathrm{ES}_{i,1}}\|h_{\mathrm{ES}_{i,2}}\|\cdots\|h_{\mathrm{ES}_{i,t}})g_1,g_1)$验证$u_{i,j}$的签名,如果等式成立,$\mathrm{ES}_i$发送密钥因子$\{f(x_1),f(x_1,x_2),\cdots,f(x_1,x_2,\cdots,x_t)\}$给终端$u_{i,j}$.

(5) $u_{i,j}$收到密钥因子$\{f(x_1),f(x_1,x_2),\cdots,f(x_1,x_2,\cdots,x_t)\}$后,$u_{i,j}$用$(x_1=H_3(\rho_{u_{i,j,1}}),x_2=H_3(\rho_{u_{i,j,2}}),\cdots,x_t=H_3(\rho_{u_{i,j,t}}))$和密钥因子还原多项式:

$$\begin{aligned}f(x)=&f(x_1)+(x-x_1)f(x_1,x_2)\\&+(x-x_1)(x-x_2)f(x_1,x_2,x_3)+\cdots\\&+(x-x_1)(x-x_2)\cdots(x-x_{t-1})f(x_1,x_2,\cdots,x_t)\end{aligned}\tag{4}$$

$u_{i,j}$令$x=0$计算得到$x_{u_{i,j}}=f(0)$,并将$\mathrm{dk}_{u_{i,j}}=x_{u_{i,j}}$作为群组解密密钥. 随后,计算群组加密密钥$\mathrm{ek}_{u_{i,j}}=\zeta_{i,j}=\mathrm{sk}_{u_{i,j}}^{-1}x_{u_{i,j}}g_1$.

5.3.2 密钥正确性验证

(1)当群组内的所有终端成员的加密和解密密钥计算完成后,群组密钥发起者$u_{i,\tau}$计算哈希值$\phi=H_3(x_{u_{i,\tau}}g_1)$和签名$\sigma=\mathrm{sk}_{u_{i,\tau}}^{-1}H_3(\rho_{u_{i,\tau,1}}\|\rho_{u_{i,\tau,2}}\|\cdots\|\rho_{u_{i,\tau,t}})g_1$,然后$u_{i,\tau}$在群组内广播消息$\{\mathrm{pk}_{u_{i,\tau}},\phi,\sigma\}$.

(2)群组所有的终端$u_{i,k}(k\neq\tau)$收到消息$\{\mathrm{pk}_{u_{i,\tau}},\phi,\sigma\}$后,计算$\eta=H_3(\rho_{u_{i,k,1}}\|\rho_{u_{i,k,2}}\|\cdots\|\rho_{u_{i,k,t}})$并通过计算公式$e(\sigma,g_1)=e(\eta g_1,\mathrm{pk}_{u_{i,\tau}})$验证$u_{i,\tau}$的身份和属性权限,如果等式成立,$u_{i,k}$计算$\phi'=H_3(x_{u_{i,k}}g_1)$,如果$\phi'=\phi$则说明群组内所有成员的解密密钥是一致的.

同理,具有不同数量属性的群组也采取同样的方式协商加密和解密密钥$(\mathrm{ek}_{u_{i,j}},\mathrm{dk}_{u_{i,j}})$.

5.4 权限升级

如果终端想要加入更高层级的群组,他需要向云服务器CS申请获得对应的新属性来升级权限. 假设终端$u_{i,j}$能够参与L层GKA,L层群组要求终端需要具有属性集$\{\mathrm{Attr}_1,\mathrm{Attr}_2,\cdots,\mathrm{Attr}_t\}$,然而$u_{i,j}$有参与$L+1$层GKA的需求,且$L+1$层要求终端需要具有属性集$\{\mathrm{Attr}_1,\mathrm{Attr}_2,\cdots,\mathrm{Attr}_t,\mathrm{Attr}_{t+1}\}(2\leqslant t+1\leqslant T)$. 终端升级权限过程如下:

(1)终端$u_{i,j}$根据属性权限计算签名$\vartheta_{u_{i,j}}=\mathrm{sk}_{u_{i,j}}^{-1}H_3(S_{t+1}\|\rho_{u_{i,j,1}}\|\rho_{u_{i,j,2}}\|\cdots\|\rho_{u_{i,j,t}})g_1$和哈希值$h_{u_{i,j}}=H_1(\vartheta_{u_{i,j}}\|\mathrm{IP}_{u_{i,j}}\|\mathrm{pk}_{u_{i,j}})$,并将申请属性权限所需的信息$\{\mathrm{pk}_{u_{i,j}},h_{u_{i,j}},\vartheta_{u_{i,j}},\mathrm{IP}_{u_{i,j}},S_{t+1}\}$发送给云服务器.

(2)云服务器CS收到终端$u_{i,j}$发送的消息$\{\mathrm{pk}_{u_{i,j}},h_{u_{i,j}},\vartheta_{u_{i,j}},\mathrm{IP}_{u_{i,j}},S_{t+1}\}$后,首先在信息平台中查询$u_{i,j}$的$\mathrm{IP}_{u_{i,j}}$和属性序列号$(S_1,S_2,\cdots,S_t)$并计算$h_{\mathrm{ES}_i}=H_1(\vartheta_{u_{i,j}}\|\mathrm{IP}_{u_{i,j}}\|\mathrm{pk}_{u_{i,j}})$,如果$h_{u_{i,j}}=h_{\mathrm{ES}_i}$,$\mathrm{ES}_i$根据属性序列号$(S_1,S_2,\cdots,S_t)$找到对应的属性权限$\{\rho_{\mathrm{ES}_{i,1}},\rho_{\mathrm{ES}_{i,2}},\cdots,\rho_{\mathrm{ES}_{i,t}}\}$,

算法2 群组密钥计算

输入:属性集$\{\mathrm{attr}_{i,j,1},\mathrm{attr}_{i,j,2},\cdots,\mathrm{attr}_{i,j,t}\}$和属性权值集合$\{\rho_{u_{i,j,1}},\rho_{u_{i,j,2}},\cdots,\rho_{u_{i,j,t}}\}$

输出:群组加密密钥$\mathrm{ek}_{u_{i,j}}$和群组解密密钥$\mathrm{dk}_{u_{i,j}}$

步骤1:GKA发起人$u_{i,\tau}$广播属性权限集合$\{\chi_{u_{i,\tau,1}},\chi_{u_{i,\tau,2}},\cdots,\chi_{u_{i,\tau,t}}\}$并计算参与GKA所需的参数信息:

FOR k=1 to t DO

$h_{u_{i,\tau,k}}=H_2(\mathrm{attr}_{i,\tau,k})$

END FOR

$u_{i,\tau}$广播属性哈希值及其身份信息$\{h_{u_{i,\tau,1}},h_{u_{i,\tau,2}},\cdots,h_{u_{i,\tau,t}},\mathrm{id}_{u_{i,\tau}},\mathrm{pk}_{u_{i,\tau}}\}$

步骤2:其他成员$u_{i,j}(1\leqslant j\leqslant n)$以及边缘服务器$\mathrm{ES}_i$计算属性哈希值

FOR k=1 to t DO

$h_{u_{i,j,k}}=H_2(\mathrm{attr}_{i,j,k})$

END FOR

FOR k=1 to t DO

$h_{\mathrm{ES}_{i,k}}=H_2(\mathrm{Attr}_{i,k})$

END FOR

$u_{i,j}$将自己的属性哈希值$\{h_{u_{i,j,1}},h_{u_{i,j,2}},\cdots,h_{u_{i,j,t}}\}$与$u_{i,\tau}$广播的属性哈希值集合$\{h_{u_{i,\tau,1}},h_{u_{i,\tau,2}},\cdots,h_{u_{i,\tau,t}}\}$进行对比,判断自己是否有权限参与$u_{i,\tau}$发起的GKA

IF $\{h_{u_{i,\tau,1}},h_{u_{i,\tau,2}},\cdots,h_{u_{i,\tau,t}}\}\subseteq\{h_{u_{i,j,1}},h_{u_{i,j,2}},\cdots,h_{u_{i,j,t}}\}$ THEN

步骤3:边缘服务器验证GKA成员$u_{i,j}$的身份并分发密钥因子

$u_{i,j}$计算$E_{i,j}=l_{i,j}\mathrm{pk}_{\mathrm{ES}_i}$、签名$\delta_{u_{i,j}}=\mathrm{sk}_{u_{i,j}}^{-1}H_3(h_{u_{i,j,1}}\|h_{u_{i,j,2}}\|\cdots\|h_{u_{i,j,t}})g_1$以及哈希值$h_{u_{i,j}}=H_1(\delta_{u_{i,j}}\|\mathrm{IP}_{u_{i,j}}\|\mathrm{pk}_{u_{i,j}}\|E_{i,j})$并向$\mathrm{ES}_i$发送申请信息$\{(h_{u_{i,\tau,1}},h_{u_{i,\tau,2}},\cdots,h_{u_{i,\tau,t}}),h_{u_{i,j}},\mathrm{pk}_{u_{i,j}},\mathrm{IP}_{u_{i,j}},\delta_{u_{i,j}},E_{i,j}\}$

ES_i计算$h_{\mathrm{ES}_i}=H_1(\delta_{u_{i,j}}\|\mathrm{IP}_{u_{i,j}}\|\mathrm{pk}_{u_{i,j}}\|E_{i,j})$和验证所需的参数

IF $h_{u_{i,j}}=h_{\mathrm{ES}_i}$ THEN

FOR k=1 to t DO

$\gamma_{\mathrm{ES}_{i,k}}=H_2(\mathrm{Attr}_{i,k})E'_{i,j}$

END FOR

IF $e(\delta_{u_{i,j}},\mathrm{pk}_{u_{i,j}})=e(H_3(h_{\mathrm{ES}_{i,1}}\|h_{\mathrm{ES}_{i,2}}\|\cdots\|h_{\mathrm{ES}_{i,t}})g_1,g_1)$ AND $\{\chi_{u_{i,j,1}},\chi_{u_{i,j,2}},\cdots,\chi_{u_{i,j,t}}\}=\{\gamma_{\mathrm{ES}_{i,1}},\gamma_{\mathrm{ES}_{i,2}},\cdots,\gamma_{\mathrm{ES}_{i,t}}\}$ THEN

ES_i发送密钥因子$\{f(x_1),f(x_1,x_2),\cdots,f(x_1,x_2,\cdots,x_t)\}$给终端$u_{i,j}$

$u_{i,j}$用$(x_1=H_3(\rho_{u_{i,j,1}}),x_2=H_3(\rho_{u_{i,j,2}}),\cdots,x_t=H_3(\rho_{u_{i,j,t}}))$和$\{f(x_1),f(x_1,x_2),\cdots,f(x_1,x_2,\cdots,x_t)\}$还原多项式计算得到$\mathrm{ek}_{u_{i,j}}$和$\mathrm{dk}_{u_{i,j}}$

然后通过计算等式$e(\vartheta_{u_{i,j}},g_1)=e(H_3(S_{t+1}\|\rho_{u_{i,j,1}}\|\rho_{u_{i,j,2}}\|\cdots\|\rho_{u_{i,j,t}})g_1,\mathrm{pk}_{u_{i,j}})$是否成立来验证终端的身份和权限. 如果成立,CS查询区块链计算$L'_{i,j}=\mathrm{sk}_{\mathrm{CS}}^{-1}L_{i,j}$,$\chi_{u_{i,j,t+1}}=b_{t+1}\gamma_{u_{i,j,t+1}}=b_{t+1}H_2(\mathrm{Attr}_{t+1})L'_{i,j}$并将消息$\{\chi_{u_{i,j,t+1}}\}$发送给$u_{i,j}$. 同时将信息$\{\chi_{u_{i,j,t+1}},S_{t+1},\mathrm{pk}_{u_{i,j}},\mathrm{IP}_{u_{i,j}}\}$发送给$u_{i,j}$所在域的边缘服务器$\mathrm{ES}_i$.

(3)$u_{i,j}$收到消息$\{\chi_{u_{i,j,t+1}}\}$后计算获得属性权限

$\rho_{u_{i,j,t+1}}=l_{i,j}^{-1}\chi_{u_{i,j,t+1}}$.

(4)ES_i收到消息$\{\chi_{u_{i,j,t+1}},S_{t+1},\mathrm{pk}_{u_{i,j}},\mathrm{IP}_{u_{i,j}}\}$后,将信息$\{(\chi_{u_{i,j,1}},\chi_{u_{i,j,2}},\cdots,\chi_{u_{i,j,t}},\chi_{u_{i,j,t+1}}),\ \mathrm{pk}_{u_{i,j}},L_{i,j},\mathrm{IP}_{u_{i,j}},\mathrm{time}_{u_{i,j}}\}$以交易的形式写入一个新的区块,并链接在联盟区块链中,然后对信息公示平台进行更新. 权限升级后的信息公示平台如表3所示.

表3　权限升级后的信息公示平台

终端	公钥	属性权限参数	IP地址
$u_{i,1}(1\leqslant i\leqslant N)$	$\mathrm{pk}_{u_{i,1}}$	$\chi_{u_{i,1,1}},\chi_{u_{i,1,2}},\cdots,\chi_{u_{i,1,k}}$	$\mathrm{IP}_{u_{i,1}}$
$u_{i,2}(1\leqslant i\leqslant N)$	$\mathrm{pk}_{u_{i,2}}$	$\chi_{u_{i,2,1}},\chi_{u_{i,2,2}},\cdots,\chi_{u_{i,2,r}}$	$\mathrm{IP}_{u_{i,2}}$
…	…	…	…
$u_{i,j}(1\leqslant i\leqslant N)$	$\mathrm{pk}_{u_{i,j}}$	$\chi_{u_{i,n,1}},\chi_{u_{i,n,2}},\cdots,\chi_{u_{i,n,t}},\chi_{u_{i,j,t+1}}$	$\mathrm{IP}_{u_{i,j}}$
…	…	…	…
$u_{i,n}(1\leqslant i\leqslant N)$	$\mathrm{pk}_{u_{i,n}}$	$\chi_{u_{i,n,1}},\chi_{u_{i,n,2}},\cdots,\chi_{u_{i,n,t}},\chi_{u_{i,n,v}}$	$\mathrm{IP}_{u_{i,n}}$

5.5　权限撤销

当终端$u_{i,j}$受到惩罚时,需要撤销终端的权限. 假设$u_{i,j}$现有的属性权限集合为$\{\rho_{u_{i,j,1}},\rho_{u_{i,j,2}},\cdots,\rho_{u_{i,j,t}}\}(i,j,t\in\mathrm{N}^*,t\leqslant T)$,现需撤销属性权限$\rho_{u_{i,j,t}}$. 属性权限撤销后,$u_{i,j}$只能参与$\{\rho_{u_{i,j,1}},\rho_{u_{i,j,2}},\cdots,\rho_{u_{i,j,t-1}}\}$对应的或更低的GKA. 因此需要对网络中其它终端属性序列号S_t对应的属性权限进行更新. 撤销过程如下:

(1)CS查询网络中其他终端列表$u_{a,k}(1\leqslant a\leqslant N,1\leqslant k\leqslant n)$(且需满足当$a=i$时$k\neq j$),并随机选择$b'_t\in\mathbb{Z}_q^*$,随后查询区块链并计算$L'_{a,k}=\mathrm{sk}_{\mathrm{cs}}^{-1}L_{a,k}$,$\chi'_{u_{a,k,t}}=b'_tH_2(\mathrm{Attr}_t)L'_{a,k}(1\leqslant a\leqslant N,1\leqslant k\leqslant n)$,然后将消息$\{\chi'_{u_{a,k,t}}\}(1\leqslant a\leqslant N,1\leqslant k\leqslant n)$发送给网络中的每一个终端$u_{a,k}(1\leqslant a\leqslant N,1\leqslant k\leqslant n)$,并将消息$\{\chi'_{u_{a,k,t}},S_t,\mathrm{pk}_{u_{a,k}},\mathrm{IP}_{u_{a,k}}\}(1\leqslant a\leqslant N,1\leqslant k\leqslant n)$发送给其它的每个终端对应的边缘服务器$\mathrm{ES}_a(1\leqslant a\leqslant N)$.

(2)网络内其他成员$u_{a,k}(1\leqslant a\leqslant N,1\leqslant k\leqslant n)$收到消息$\{\chi'_{u_{a,k,t}}\}(1\leqslant a\leqslant N,1\leqslant k\leqslant n)$后,计算获得属性权限$\rho'_{u_{a,k,t}}=l_{a,k}^{-1}\chi'_{u_{a,k,t}}$.

(3)$\mathrm{ES}_a(1\leqslant a\leqslant N)$收到消息$\{\chi'_{u_{a,k,t}},S_t,\mathrm{pk}_{u_{a,k}},\mathrm{IP}_{u_{a,k}}\}(1\leqslant a\leqslant N,1\leqslant k\leqslant n)$后,首先计算$\rho'_{ES_{a,t}}=b'_tH_2(\mathrm{Attr}_t)g_1$,将信息$\{(\chi_{u_{a,k,1}},\chi_{u_{a,k,2}},\cdots,\chi'_{u_{a,k,t}}),\mathrm{pk}_{u_{a,k}},L_{a,k},\mathrm{IP}_{u_{a,k}},\mathrm{time}_{u_{a,k}}\}(1\leqslant a\leqslant N,1\leqslant k\leqslant n)$以交易的形式写入一个新的区块,并链接在联盟区块链中,然后对信息公示平台进行更新. 权限撤销后的信息公示平台如表4所示.

5.6　终端成员间安全信道的建立

假设任意的终端$u_{i,j}$经过协商获得了群组的加密密钥$\mathrm{ek}_{u_{i,j}}$和解密密钥$\mathrm{dk}_{u_{i,j}}$. 它可以通过建立一个安全的信道将消息$m\in M^*$(M^*表示明文空间)发送给群组内的其他终端. 具体过程如下:

表4　权限撤销后的信息公示平台

终端	公钥	属性权限参数	IP地址
$u_{i,1}(1\leqslant i\leqslant N)$	$\mathrm{pk}_{u_{i,1}}$	$\chi_{u_{i,1,1}},\chi_{u_{i,1,2}},\cdots,\chi_{u_{i,1,k}}$	$\mathrm{IP}_{u_{i,1}}$
$u_{i,2}(1\leqslant i\leqslant N)$	$\mathrm{pk}_{u_{i,2}}$	$\chi_{u_{i,2,1}},\chi_{u_{i,2,2}},\cdots,\chi_{u_{i,2,r}}$	$\mathrm{IP}_{u_{i,2}}$
…	…	…	…
$u_{i,j}(1\leqslant i\leqslant N)$	$\mathrm{pk}_{u_{i,j}}$	$\chi_{u_{i,n,1}},\chi_{u_{i,n,2}},\cdots,\chi_{u_{i,n,t-1}}$	$\mathrm{IP}_{u_{i,j}}$
…	…	…	…
$u_{i,n}(1\leqslant i\leqslant N)$	$\mathrm{pk}_{u_{i,n}}$	$\chi_{u_{i,n,1}},\chi_{u_{i,n,2}},\cdots,\chi'_{u_{i,n,t}},\chi_{u_{i,n,v}}$	$\mathrm{IP}_{u_{i,n}}$

(1)加密:终端$u_{i,j}$选择一个随机数$\lambda\in\mathbb{Z}_q^*$并计算$\omega=\lambda\mathrm{pk}_{u_{i,j}}$,$V=m\oplus H_4(e(\zeta_{i,j},g_1)^{\lambda})$. 然后$u_{i,j}$在群组内广播消息密文$c=<\omega,V>$.

(2)解密:群组成员$u_{i,k}$收到消息$c=<\omega,V>$后,$u_{i,k}$使用协商出的解密密钥$x_{u_{i,j}}$解密出明文$m=V\oplus H_4(e(\omega,g_1)^{x_{u_{i,j}}})$.

6　安全性分析

安全性分析是评估GKA协议的重要指标. 本文采用可证明安全性理论的标准模型对提出的协议进行全面的评估.

6.1　协议的正确性

定理1　如果等式$e(w_2,w'_3)=e(w_3,w'_2)$成立,CA就可以验证实体u的合法身份id_u和公钥pk,并将实体u的身份id_u和公钥pk绑定在一起.

证明　由于$w_2=r\mathrm{PK}$,$w_3=H_2(\mathrm{id}_u)\mathrm{PK}$,$w'_2=\mathrm{MSK}^{-1}w_2=\mathrm{pk}=rg_1$和$w'_3=\mathrm{MSK}^{-1}w_3=H_2(\mathrm{id}_u)g_1$,根据双线性配对的性质,我们可以进行如下的推导:

$$\begin{aligned}e(w_2,w'_3)&=e(r\mathrm{PK},H_2(\mathrm{id}_u)g_1)\\&=e(H_2(\mathrm{id}_u)\mathrm{PK},rg_1)\\&=e(w_3,w'_2)\end{aligned}\tag{5}$$

从上述推导可以看出,等式$e(w_2,w'_3)=e(w_3,w'_2)$成立,因此实体u的身份id_u和公钥pk能够通过认证,CA则会将实体u的身份id_u和公钥pk绑定在一起.

定理2　如果等式$e(\sigma_{u_{i,j}},\mathrm{pk}_{u_{i,j}})=e(H_2(\mathrm{Attr}_1\|\mathrm{Attr}_2\|\cdots\|\mathrm{Attr}_t)g_1,g_1)$成立,CS可以验证终端$u_{i,j}$合法签名并确定终端具有的属性数量.

证明　由于$\sigma_{u_{i,j}}=\mathrm{sk}_{u_{i,j}}^{-1}H_2(\mathrm{attr}_{i,j,1}\|\mathrm{attr}_{i,j,2}\|\cdots\|\mathrm{attr}_{i,j,t})g_1$,根据双线性对的性质,我们可以进行如下推导:

$$\begin{aligned}&e(\sigma_{u_{i,j}},\mathrm{pk}_{u_{i,j}})\\&=e(\mathrm{sk}_{u_{i,j}}^{-1}H_2(\mathrm{attr}_{i,j,1}\|\mathrm{attr}_{i,j,2}\|\cdots\|\mathrm{attr}_{i,j,t})g_1,\mathrm{pk}_{u_{i,j}})\\&=e(H_2(\mathrm{attr}_{i,j,1}\|\mathrm{attr}_{i,j,2}\|\cdots\|\mathrm{attr}_{i,j,t})g_1,\mathrm{pk}_{u_{i,j}})^{\mathrm{sk}_{u_{i,j}}^{-1}}\\&=e(H_2(\mathrm{attr}_{i,j,1}\|\mathrm{attr}_{i,j,2}\|\cdots\|\mathrm{attr}_{i,j,t})g_1,\mathrm{sk}_{u_{i,j}}^{-1}\mathrm{pk}_{u_{i,j}})\\&=e(H_2(\mathrm{Attr}_1\|\mathrm{Attr}_2\|\cdots\|\mathrm{Attr}_t)g_1,g_1)\end{aligned}\tag{6}$$

从上述推导可以看出，等式 $e(\sigma_{u_{i,j}},\mathrm{pk}_{u_{i,j}})=e(H_2(\mathrm{Attr}_1\|\mathrm{Attr}_2\|\cdots\|\mathrm{Attr}_t)g_1,g_1)$ 相等，$u_{i,j}$ 的签名合法并且 $u_{i,j}$ 拥有属性集 $\{\mathrm{attr}_{i,j,1},\mathrm{attr}_{i,j,2},\cdots,\mathrm{attr}_{i,j,t}\}$.

定理 3 如果等式 $e(\delta_{\mathrm{cs}_{i,j}},\mathrm{pk}_{\mathrm{cs}})=e(H_3(\chi_{u_{i,j,1}}\|\chi_{u_{i,j,2}}\|\cdots\|\chi_{u_{i,j,t}})g_1,g_1)$ 相等，终端 $u_{i,j}$ 可以验证 CS 的签名和身份.

证明 由于 $\delta_{\mathrm{cs}_{i,j}}=\mathrm{sk}_{\mathrm{cs}}^{-1}H_3(\chi_{u_{i,j,1}}\|\chi_{u_{i,j,2}}\|\cdots\|\chi_{u_{i,j,t}})g_1$，根据双线对的性质，我们可以进行如下推导：

$$\begin{aligned}e(\delta_{\mathrm{cs}_{i,j}},\mathrm{pk}_{\mathrm{cs}})&=e(\mathrm{sk}_{\mathrm{cs}}^{-1}H_3(\chi_{u_{i,j,1}}\|\chi_{u_{i,j,2}}\|\cdots\|\chi_{u_{i,j,t}})g_1,\mathrm{pk}_{\mathrm{cs}})\\&=e(H_3(\chi_{u_{i,j,1}}\|\chi_{u_{i,j,2}}\|\cdots\|\chi_{u_{i,j,t}})g_1,\mathrm{pk}_{\mathrm{cs}})^{\mathrm{sk}_{\mathrm{cs}}^{-1}}\\&=e(H_3(\chi_{u_{i,j,1}}\|\chi_{u_{i,j,2}}\|\cdots\|\chi_{u_{i,j,t}})g_1,\mathrm{sk}_{\mathrm{cs}}^{-1}\mathrm{pk}_{\mathrm{cs}})\\&=e(H_3(\chi_{u_{i,j,1}}\|\chi_{u_{i,j,2}}\|\cdots\|\chi_{u_{i,j,t}})g_1,g_1)\end{aligned}\tag{7}$$

从上述推导可以看出，等式 $e(\delta_{\mathrm{cs}_{i,j}},\mathrm{pk}_{\mathrm{cs}})=e(H_3(\chi_{u_{i,j,1}}\|\chi_{u_{i,j,2}}\|\cdots\|\chi_{u_{i,j,t}})g_1,g_1)$ 成立，CS 的签名和身份合法.

定理 4 如果等式 $e(\delta_{u_{i,j}},\mathrm{pk}_{u_{i,j}})=e(H_3(h_{\mathrm{ES}_{i,1}}\|h_{\mathrm{ES}_{i,2}}\|\cdots\|h_{\mathrm{ES}_{i,t}})g_1,g_1)$ 成立，ES_i 可以验证终端 $u_{i,j}$ 的身份签名和属性集合.

证明 由于 $\delta_{u_{i,j}}=\mathrm{sk}_{u_{i,j}}^{-1}H_3(h_{u_{i,j,1}}\|h_{u_{i,j,2}}\|\cdots\|h_{u_{i,j,t}})g_1$，根据双线性对的性质，我们可以进行如下推导：

$$\begin{aligned}e(\delta_{u_{i,j}},\mathrm{pk}_{u_{i,j}})&=e(\mathrm{sk}_{u_{i,j}}^{-1}H_3(h_{u_{i,j,1}}\|h_{u_{i,j,2}}\|\cdots\|h_{u_{i,j,t}})g_1,\mathrm{pk}_{u_{i,j}})\\&=e(H_3(h_{u_{i,j,1}}\|h_{u_{i,j,2}}\|\cdots\|h_{u_{i,j,t}})g_1,\mathrm{pk}_{u_{i,j}})^{\mathrm{sk}_{u_{i,j}}^{-1}}\\&=e(H_3(h_{u_{i,j,1}}\|h_{u_{i,j,2}}\|\cdots\|h_{u_{i,j,t}})g_1,\mathrm{sk}_{u_{i,j}}^{-1}\mathrm{pk}_{u_{i,j}})\\&=e(H_3(h_{\mathrm{ES}_{i,1}}\|h_{\mathrm{ES}_{i,2}}\|\cdots\|h_{\mathrm{ES}_{i,t}})g_1,g_1)\end{aligned}\tag{8}$$

从上述推导可以看出，等式 $e(\delta_{u_{i,j}},\mathrm{pk}_{u_{i,j}})=e(H_3(h_{\mathrm{ES}_{i,1}}\|h_{\mathrm{ES}_{i,2}}\|\cdots\|h_{\mathrm{ES}_{i,t}})g_1,g_1)$ 成立，终端 $u_{i,j}$ 的身份签名合法并具有满足参与 GKA 条件的属性集合.

6.2 协议的安全性

定理 5 基于 IDHP 困难性假设，非法终端无法伪造签名通过身份认证，也无法破解出属性权限，也就是说非法终端无法通过伪造签名参与 GKA.

证明 (1)具有属性 $\mathrm{attr}_{i,j,t}(1\leqslant t\leqslant T)$ 的终端 $u_{i,j}(1\leqslant i\leqslant N,1\leqslant j\leqslant n)$ 随机选择 $l_{i,j}\in\mathbb{Z}_q^*$ 并能够计算 $L_{i,j}=l_{i,j}\mathrm{pk}_{\mathrm{cs}}$，$\gamma_{u_{i,j,t}}=H_2(\mathrm{attr}_{i,j,t})l_{i,j}g_1$ 和 $\sigma_{u_{i,j}}=\mathrm{sk}_{u_{i,j}}^{-1}H_2(\mathrm{attr}_{i,j,1}\|\mathrm{attr}_{i,j,2}\|\cdots\|\mathrm{attr}_{i,j,t})g_1$. CS 能够计算 $H_2(\mathrm{Attr}_1\|\mathrm{Attr}_2\|\cdots\|\mathrm{Attr}_t)g_1$ 并通过等式 $e(\sigma_{u_{i,j}},\mathrm{pk}_{u_{i,j}})=e(H_2(\mathrm{Attr}_1\|\mathrm{Attr}_2\|\cdots\|\mathrm{Attr}_t)g_1,g_1)$ 验证 $u_{i,j}$ 的签名，如果相等，CS 则将属性权限参数 $\chi_{u_{i,j,t}}$ 发送给 $u_{i,j}$. $u_{i,j}$ 根据属性权限参数 $\chi_{u_{i,j,t}}$ 计算获得属性权限 $\rho_{u_{i,j,t}}=l_{i,j}^{-1}\chi_{u_{i,j,t}}$.

(2)如果终端 $u_{i,j}$ 没有属性 $\mathrm{attr}_{i,j,t}$，它就无法计算有效的签名来通过认证，也就无法通过合法的手段获得属性权限 $\rho_{u_{i,j,t}}$. 因此 $u_{i,j}$ 尝试在 $u_{i,k}$ 和 CS 的公共信道上截取参数 $\gamma_{u_{i,k,t}}$，$L_{i,j}$ 和 $\chi_{u_{i,k,t}}$ 并破解 $\rho_{u_{i,k,t}}=l_{i,k}^{-1}\chi_{u_{i,k,t}}=b_tH_2(\mathrm{attr}_{i,k,t})g_1$，其中 $\rho_{u_{i,j,t}}=\rho_{u_{i,k,t}}$. 但是 $l_{i,k}$ 是终端 $u_{i,k}$ 的私有参数，b_t 是 CS 的私有参数，因此无法直接破解出属性权限 $\rho_{u_{i,j,t}}$. 从上述证明可以看出 $u_{i,j}$ 想要非法破解属性权限 $\rho_{u_{i,j,t}}$，需要先破解私有参数 $l_{i,k}$ 和 b_t. 由于 $\chi_{u_{i,k,t}}=b_t\gamma_{u_{i,k,t}}$ 和 $\gamma_{u_{i,k,t}}=H_2(\mathrm{attr}_{i,k,t})l_{i,k}g_1$，则有 $\rho_{u_{i,k,t}}=l_{i,k}^{-1}\chi_{u_{i,k,t}}=l_{i,k}^{-1}l_{i,k}b_tH_2(\mathrm{attr}_{i,k,t})g_1$. 我们令 $a=l_{i,k}$，$b=b_tH_2(\mathrm{attr}_{i,k,t})$，则有 $ag_1=l_{i,k}g_1$，$abg_1=l_{i,k}b_tH_2(\mathrm{attr}_{i,k,t})g_1=\chi_{u_{i,k,t}}$. 如果我们构造算法 $\mathcal{A}$ 计算 $\rho_{u_{i,k,t}}=l_{i,k}^{-1}\chi_{u_{i,k,t}}=l_{i,k}^{-1}l_{i,k}b_tH_2(\mathrm{attr}_{i,k,t})g_1=(ab/a)g_1$，计算 $\mathcal{A}$ 是一个 IDHP 困难性假设，因此 $\rho_{u_{i,k,t}}$ 无法被破解.

从上述证明可以看出，基于 IDHP 困难性假设，本协议在身份认证过程中是安全的，敌手无法以非法的方式获取属性权限 $\rho_{u_{i,j,t}}$.

定理 6 当群组 L_t 设置的最低属性集要求为 $\{\mathrm{Attr}_1,\mathrm{Attr}_2,\cdots,\mathrm{Attr}_t\}$，参与该群组的所有终端 $u_{i,j}$ 都应具有属性集 $\mathrm{set}_{u_{i,j}}$ 且 $\{\mathrm{Attr}_1,\mathrm{Attr}_2,\cdots,\mathrm{Attr}_t\}\subseteq\mathrm{set}_{u_{i,j}}$ 才能计算出正确的加密密钥 $\mathrm{ek}_{u_{i,j}}$ 和解密密钥 $\mathrm{dk}_{u_{i,j}}$. 相反，如果终端 $u_{i,k}$ 的属性集不满足要求，则无法参与该群组的密钥协商，更无法计算出正确的密钥.

证明

(1)如果终端 $u_{i,j}$ 拥有属性 $\{\mathrm{attr}_{i,j,1},\mathrm{attr}_{i,j,2},\cdots,\mathrm{attr}_{i,j,t}\}$，它能够根据定理 5 获得属性权限. 然后 $u_{i,j}$ 计算属性哈希值判定自己是否满足参与 GKA 的条件，如果满足，$u_{i,j}$ 根据属性权限计算 $E_{i,j}=l_{i,j}\mathrm{pk}_{\mathrm{ES}_i}$、签名 $\delta_{u_{i,j}}=\mathrm{sk}_{u_{i,j}}^{-1}H_3(h_{u_{i,j,1}}\|h_{u_{i,j,2}}\|\cdots\|h_{u_{i,j,t}})g_1$ 以及哈希值 $h_{u_{i,j}}=H_1(\delta_{u_{i,j}}\|\mathrm{IP}_{u_{i,j}}\|\mathrm{pk}_{u_{i,j}}\|E_{i,j})$，然后将申请信息发送给本域边缘服务器 ES_i. ES_i 首先计算哈希值 $h_{\mathrm{ES}_i}=H_1(\delta_{u_{i,j}}\|\mathrm{IP}_{u_{i,j}}\|\mathrm{pk}_{u_{i,j}}\|E_{i,j})$ 判断信息是否被篡改，然后通过计算 $\chi_{u_{i,j}}=\{\chi_{u_{i,j,1}},\chi_{u_{i,j,2}},\cdots,\chi_{u_{i,j,t}}\}=\{\gamma_{\mathrm{ES}_{i,1}},\gamma_{\mathrm{ES}_{i,2}},\cdots,\gamma_{\mathrm{ES}_{i,t}}\}$ 和等式 $e(\delta_{u_{i,j}},\mathrm{pk}_{u_{i,j}})=e(H_3(h_{\mathrm{ES}_{i,1}}\|h_{\mathrm{ES}_{i,2}}\|\cdots\|h_{\mathrm{ES}_{i,t}})g_1,g_1)$ 验证终端 $u_{i,j}$ 的身份和权限. 如果成立，$u_{i,j}$ 才能够得到密钥因子 $\{f(x_1),f(x_1,x_2),\cdots,f(x_1,x_2,\cdots,x_t)\}$ 并根据属性权限的哈

希值 $(x_1=H_3(\rho_{u_{i,j,1}}),x_2=H_3(\rho_{u_{i,j,2}}),\cdots,x_t=H_3(\rho_{u_{i,j,t}}))$ 还原牛顿插值多项式 $f(x)$. 然后 $u_{i,j}$ 令 $x=0$ 得到解密密钥 $\mathrm{dk}_{u_{i,j}}=x_{u_{i,j}}=f(0)$ 并计算加密密钥 $\mathrm{ek}_{u_{i,j}}=\zeta_{i,j}=\mathrm{sk}_{u_{i,j}}^{-1}x_{u_{i,j}}g_1$.

(2)如果具有属性集为 $\{\mathrm{attr}_{i,k,1},\mathrm{attr}_{i,k,2},\cdots,\mathrm{attr}_{i,k,t-1}\}$ 的终端 $u_{i,k}$ 不满足群组 L_t 的要求,它通过伪造属性 $\mathrm{attr}'_{i,k,t-1}$ 并计算 $E_{i,k}=l_{i,k}\mathrm{pk}_{\mathrm{ES}_i}$, $h_{u_{i,k,1}}=H_2(\mathrm{attr}_{i,k,1})$, $h_{u_{i,k,2}}=H_2(\mathrm{attr}_{i,k,2})$, $\cdots$, $h'_{u_{i,k,t}}=H_2(\mathrm{attr}_{i,k,t})$, 签名 $\delta'_{u_{i,k}}=\mathrm{sk}_{u_{i,k}}^{-1}H_3(h_{u_{i,k,1}}\|h_{u_{i,k,2}}\|\cdots\|h'_{u_{i,k,t}})g_1$ 和哈希值 $h_{u_{i,k}}=H_1(\delta'_{u_{i,k}}\|\mathrm{IP}_{u_{i,k}}\|\mathrm{pk}_{u_{i,k}}\|E_{i,k})$,然后向 ES_i 申请参与 L_t 层 GKA, ES_i 首先计算哈希值 $h_{\mathrm{ES}_i}=H_1(\delta_{u_{i,k}}\|\mathrm{IP}_{u_{i,k}}\|\mathrm{pk}_{u_{i,k}})$ 验证签名完整性,并计算 $E'_{i,k}=\mathrm{sk}_{\mathrm{ES}_i}^{-1}E_{i,k}=l_{i,k}g_1$, $\gamma_{\mathrm{ES}_{i,1}}=H_2(\mathrm{Attr}_1)E'_{i,k}$, $\gamma_{\mathrm{ES}_{i,2}}=H_2(\mathrm{Attr}_2)E'_{i,k}$, $\cdots$, $\gamma'_{\mathrm{ES}_{i,t}}=H_2(\mathrm{Attr}_t)E'_{i,k}$, 但是计算 $\chi_{u_{i,j}}=\{\chi_{u_{i,j,1}},\chi_{u_{i,j,2}},\cdots,\chi_{u_{i,j,t}}\}\neq\{\gamma_{\mathrm{ES}_{i,1}},\gamma_{\mathrm{ES}_{i,2}},\cdots,\gamma'_{\mathrm{ES}_{i,t}}\}$ 结果不成立,也就是说 $u_{i,k}$ 不满足参与该 GKA 的条件;同时, ES_i 计算等式 $e(\delta'_{u_{i,k}},\mathrm{pk}_{u_{i,k}})=e(H_3(h_{\mathrm{ES}_{i,1}}\|h_{\mathrm{ES}_{i,2}}\|\cdots\|h_{\mathrm{ES}_{i,t}})g_1,g_1)$, 由于 $\rho'_{u_{i,k,t}}\neq\rho_{u_{i,k,t}}$,等式不成立. 因此 $u_{i,k}$ 也无法参与 L_t 层 GKA. 此外,假设 $u_{i,k}$ 能够通过非法手段截取密钥因子 $\{f(x_1),f(x_1,x_2),\cdots,f(x_1,x_2,\cdots,x_t)\}$, 并使用 $(x_1=H_3(\rho_{u_{i,k,1}}),x_2=H_3(\rho_{u_{i,k,2}}),\cdots,x_t=H_3(\rho'_{u_{i,k,t}}))$ 还原牛顿插值多项式. 由于 $\rho'_{u_{i,k,t}}\neq\rho_{u_{i,k,t}}$, $u_{i,k}$ 计算得到的解密密钥 $\mathrm{dk}'_{u_{i,k}}\neq\mathrm{dk}_{u_{i,j}}$,因此 $u_{i,k}$ 也无法非法获取群组通信消息.

从上述证明可以看出,只有具有满足属性条件的终端才能够加入群组并正确的计算出密钥,非法终端无法通过伪造或暴力破解获取正确的密钥.

定理 7　本文所提出的 GKA 协议能够抵抗两个或两个以上非法终端的共谋攻击.

证明　假设终端 $u_{i,k}$ 具有属性 $\{\mathrm{attr}_{i,k,1},\mathrm{attr}_{i,k,2},\cdots,\mathrm{attr}_{i,k,t-1}\}$ 想要与具有属性 $\mathrm{attr}_{i,j,t}$ 的终端 $u_{i,j}$ 合谋参与属性哈希值集合为 $\{h_{u_{i,\tau,1}},h_{u_{i,\tau,2}},\cdots,h_{u_{i,\tau,t}}\}$ 的 GKA, $u_{i,k}$ 计算 $E_{i,k}=l_{i,k}\mathrm{pk}_{\mathrm{ES}_i}$ 和属性哈希值 $h_{u_{i,k}}=H_1(\delta_{u_{i,k}}\|\mathrm{IP}_{u_{i,k}}\|\mathrm{pk}_{u_{i,k}}\|E_{i,k})$, 并向 ES_i 申请参与 $\{h_{u_{i,\tau,1}},h_{u_{i,\tau,2}},\cdots,h_{u_{i,\tau,t}}\}$ 群组的密钥协商. ES_i 收到消息后首先在区块链中查询 $u_{i,j}$ 的 $\mathrm{IP}_{u_{i,j}}$ 和属性权限集 $\chi_{u_{i,j}}=\{\chi_{u_{i,j,1}},\chi_{u_{i,j,2}},\cdots,\chi_{u_{i,j,t}}\}$, 并计算 $h_{\mathrm{ES}_i}=H_1(\delta_{u_{i,j}}\|\mathrm{IP}_{u_{i,j}}\|\mathrm{pk}_{u_{i,j}}\|E_{i,j})$, 如果 $h_{u_{i,j}}=h_{\mathrm{ES}_i}$, ES_i 分别计算 $E'_{i,j}=\mathrm{sk}_{\mathrm{ES}_i}^{-1}E_{i,j}=l_{i,j}g_1$, $\gamma_{\mathrm{ES}_{i,1}}=H_2(\mathrm{Attr}_1)E'_{i,j}$, $\gamma_{\mathrm{ES}_{i,2}}=H_2(\mathrm{Attr}_2)E'_{i,j}$, $\cdots$, $\gamma_{\mathrm{ES}_{i,t}}=H_2(\mathrm{Attr}_t)E'_{i,j}$. ES_i 计算 $\chi_{u_{i,j}}=\{\chi_{u_{i,j,1}},\chi_{u_{i,j,2}},\cdots,\chi_{u_{i,j,t}}\}\neq\{\gamma_{\mathrm{ES}_{i,1}},\gamma_{\mathrm{ES}_{i,2}},\cdots,\gamma_{\mathrm{ES}_{i,t}}\}$, 因此 ES_i 判定 $u_{i,k}$ 为非法终端,终止与其通信.

定理 8　本文提出的协议不仅能够保护终端的身份和属性隐私,而且能够对非法终端进行追溯.

证明　实体 u 在密钥证实阶段向 CA 申请将公钥 pk_u 与身份 id_u 进行绑定,因此认证中心能够通过公钥查询终端的身份信息. 在终端注册阶段终端 $u_{i,j}$ $(1\leqslant i\leqslant N,1\leqslant j\leqslant n)$ 使用私钥进行了签名,通过与 CS 交互的等式 $e(\sigma_{u_{i,j}},\mathrm{pk}_{u_{i,j}})=e(H_2(\mathrm{Attr}_1\|\mathrm{Attr}_2\|\cdots\|\mathrm{Attr}_t)g_1,g_1)$ 能够追溯 $u_{i,j}$ 的身份,此外 $u_{i,j}$ 的公钥 $\mathrm{pk}_{u_{i,j}}$, $\mathrm{IP}_{u_{i,j}}$ 地址以及属性权限等信息在认证成功后被写入区块链中,使得 $u_{i,j}$ 的身份信息能够被追溯且具有不可否认性.

7　性能评估

由于移动终端的资源受限,除了安全性之外,性能也是评估协议优劣的重要指标. 本节从计算花费以及通信花费方面将我们的协议与参考文献[12, 20, 25]进行对比分析,这些文献都是近些年来提出的具有代表性的优秀文献. 根据文献中的数据,我们对比分析了四种协议的计算复杂度和通信复杂度,具体如表 5 所示.

表 5　四种协议的计算复杂度和通信复杂度

算法类型	Zheng 等人的协议[12]	Wang 等人的协议[25]	Xu 等人的协议[20]	Ours
哈希运算	$n+9$	$n+3$	$n+3$	$2t+4$
标量乘法运算	—	—	—	$t+1$
椭圆曲线上的点加	$3n+1$	—	$3n+1$	2
椭圆曲线上的点乘	$n+6$	$2n-2$	$n+7$	—
幂指运算	—	3	—	—
双线性配对运算	6	—	4	2
每个终端发送的消息长度	$9\|q\|$	$12\|q\|$	$7\|q\|$	$(t+5)\|q\|$
每个终端接收的消息长度	$(9n-9)\|q\|$	$(12n-12)\|q\|$	$(4n-1)\|q\|$	$(2t+5)\|q\|$

在计算时间花费方面,我们采用处理器为 Intel(R) Core (TM) i5-8500, 3.0 GHz, 内存为 2 GB, 操作系统为 Windows 10 专业版 64 位的计算机设备,使用 Java 编程语言的 JPBC-2.0.0 加密库运行相关算法得到的数据对四种方案进行量化评价,算法数据如表 6 所示.

由于在实际的边云协同场景中,终端 n 的数量远大于终端属性 t 的数量,为了便于统一量化分析,我们假设 $n=t$ 并将我们的方案与前期的三种方案进行了对比分析.

根据表 5 可知, Zheng 等人的协议[12]有 $(n+9)$ 个哈

表6 各种算法的时间消耗 单位:ms

算法类型	时间花费
模逆运算(T_{inv})	$T_{inv}\approx 0.004\,7$
标量乘法运算(T_{mul})	$T_{mul}\approx 0.000\,3$
哈希运算(T_h)	$T_h\approx 0.000\,2$
椭圆曲线上的点加(T_{pa_ec})	$T_{pa\_ec}\approx 0.032\,8$
椭圆曲线上的点乘(T_{sm_ec})	$T_{sm\_ec}\approx 0.033\,4$
双线性配对运算(T_{bp})	$T_{bp}\approx 4.080\,9$
幂指运算(T_{exp})	$T_{exp}\approx 6.959$

表7 每种算法的能量消耗 单位:mJ

算法类型	能量花费
幂指运算	9.1
标量乘法	8.8
双线性配对运算	47.0
椭圆曲线上的点加运算	0.001 085
椭圆曲线上的点乘运算	8.8
哈希运算	0.000 108
发送1 bit数据	0.000 66
接收1 bit数据	0.000 31

希运算,$(3n+1)$个椭圆曲线上的点加运算,$(n+6)$个椭圆曲线上的点乘运算以及6个配对运算;Wang等人的协议[25]有$(n+3)$个哈希运算,$(2n-2)$个椭圆曲线上的点乘运算以及3个幂指运算;Xu等人的协议[20]有$(n+3)$个哈希运算,$(3n+1)$个椭圆曲线上的点加运算,$(n+7)$个椭圆曲线上的点乘运算以及4个配对运算;本协议有$(2t+4)$个哈希运算,$(t+1)$个标量乘法运算,2个椭圆曲线上的加法运算以及2个配对运算. 同时根据表7,每个哈希运算的运行时间为$T_h\approx 0.000\,2$ ms,每个标量乘法的运行时间为$T_{mul}\approx 0.000\,3$ ms,每个椭圆曲线上的点加和点乘运算的运行时间分别为$T_{pa_ec}\approx 0.032\,8$ ms和$T_{sm_ec}\approx 0.033\,4$ ms,每个幂指运算的运行时间为$T_{exp}\approx 6.959$ ms,以及每个双线性配对的运行时间为$T_{bp}\approx 4.080\,9$ ms. 根据两表的数据计算出四种协议的计算时间消耗,如图3所示.

从图3可以看出,四种协议的每个终端的计算时间消耗中,Zheng等人提出的协议[12]计算时间消耗最多,其次是Xu等人提出的协议[20]和Wang等人提出的协议[25],本文提出的协议的计算时间消耗最少.

在能量消耗方面,根据文献[20]和文献[26]中提供的资料,一个型号为"Strong ARM"的133 MHz微处理器执行各种运算所需的能量如表7所示.

根据表7可知,每个幂指运算需要消耗9.1 mJ的能量,每个标量乘法运算需要消耗8.8 mJ的能量,每个双线性配对运算需要消耗47 mJ的能量,每个椭圆曲线的点加和点乘运算需要消耗的能量分别为0.001 085 mJ和8.8 mJ,以及每个乘法运算需要消耗0.000 108 mJ. 基于此,本文分别对四种协议的计算能量消耗进行了分析,结果如图4所示.

从图4可以看出,四种方案的每个终端的计算能量消耗中Wang等人提出的协议[25]计算消耗的能量最多,其次是Zheng等人提出的协议[12]和Xu等人提出的协议[20],本文提出的协议具有最低的计算能量消耗.

根据表5,Zheng等人的协议[12]中每个终端的平均发送消息长度和接收消息长度分别为$9|q|$和$(9n-9)|q|$,Wang等人的协议[25]中每个终端的平均发送消息长度和接收消息长度分别为$12|q|$和$(12n-12)|q|$,Xu等人的协议[20]中每个终端的平均发送消息长度和接收消息长度分别为$7|q|$和$(4n-1)|q|$,本协议每个终端的平均发送消息长度和接收消息长度分别为$(t+5)|q|$和$(2t+5)|q|$;根据表7,发送1 bit数据需要消耗0.000 66 mJ能量,接收1 bit数据需要消耗0.000 31mJ能量;同时假设$|q|$的长度为256 bits. 基于此,本文分别对四种协议的通信能量消耗进行了分析,结果如图5所示.

从图5可以看出,四种方案的每个终端的计算能量消耗中,Wang等人的提出的协议[25]通信能量消耗最多,其次是Zheng等人提出的协议[12],本文提出的协议和Xu等人提出的协议[20]的通信能量消耗最少,两种协议的直线几乎重合,但是在实际应用场景中,属性的数量要远小于终端的数量,因此在实际应用时,本文提出的协议的通信能量消耗要低于Xu等人提出的协议[20].

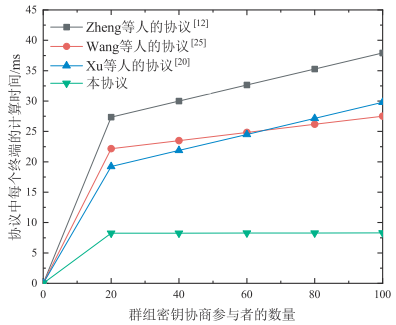

图3 四种协议的计算时间消耗

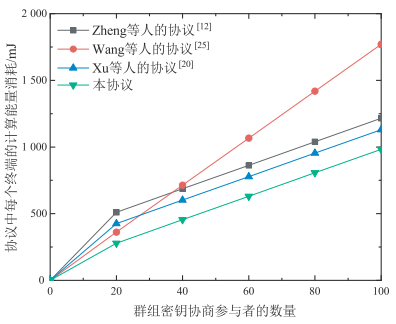

图4 四种协议的计算能量消耗

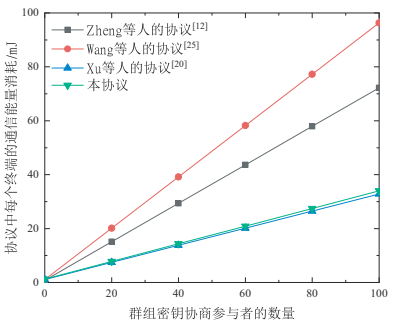

图5 四种协议的通信能量消耗

8 结论

为了解决现有GKA协议中存在的问题,提出了一种适用于边云协同环境的基于动态属性权限的GKA协议. 协议提出了密钥证实算法,解决了传统方案中CA在分发密钥时容易造成的私钥泄露问题;在终端身份信息隐私保护方面,虽然也采用基于隐私的身份认证,但本文采用密文属性身份认证技术,防止通过属性信息挖掘,泄漏个人隐私信息,具有更加安全和隐蔽的身份认证技术;采用属性权限组合技术和牛顿插值多项式相结合实现了细粒度的群组密钥协商;采用区块链技术能够实现终端的可追踪性,提高了系统的安全性与可靠性. 实验结果表明,本方案在计算花费和通信花费方面具有较高的优势.

后续的工作中,我们将所提出的群组密钥协商技术与安全数据共享技术相结合,通过群组密钥协商使得数据共享的多方在线计算出联盟密钥,并将该联盟密钥用于多方共享数据的加密与解密,保障共享数据的安全性. 此外,结合区块链和云计算技术,实现云安全数据存储,以及通过属性权限的约束,研究具有隐私保护的动态访问控制技术.

参考文献

[1] ROY P K, BHATTACHARYA A. A group key-based lightweight mutual authentication and key agreement (MAKA) protocol for multi-server environment[J]. The Journal of Supercomputing, 2022, 78(4): 5903-5930.

[2] CHENG Q, ZHAO Z, HSU C, et al. Practical KGC-free polynomial-based multiple group keys agreement for IoT health care systems[J]. Mathematical Problems in Engineering, 2021, 2021: 1-10.

[3] LI X, LIU P, ZHANG S S, et al. An improved secure and efficient group key agreement scheme in VANETs[J]. International Journal of Communication Systems, 2022, 35 (3): e5025.

[4] ZHANG R, ZHANG L, CHOO K K R, et al. Dynamic authenticated asymmetric group key agreement with sender non-repudiation and privacy for group-oriented applications[J]. IEEE Transactions on Dependable and Secure Computing, 2023, 20(1): 492-505.

[5] CHEN C M, DENG X T, GAN W S, et al. A secure blockchain-based group key agreement protocol for IoT[J]. The Journal of Supercomputing, 2021, 77(8): 9046-9068.

[6] YANG J Y, DENG J M, XIANG T, et al. A Chebyshev polynomial-based conditional privacy-preserving authentication and group-key agreement scheme for VANET[J]. Nonlinear Dynamics, 2021, 106(3): 2655-2666.

[7] CHEN Q N, WU T, HU C N, et al. An identity-based cross-domain authenticated asymmetric group key agreement[J]. Information, 2021, 12(3): 112.

[8] LEE T F, YE X C, LIN S H. Anonymous dynamic group authenticated key agreements using physical unclonable functions for Internet of medical things[J]. IEEE Internet of Things Journal, 2022, 9(16): 15336-15348.

[9] XU Z S, LIANG W, LI K C, et al. A time-sensitive token-based anonymous authentication and dynamic group key agreement scheme for industry 5.0[J]. IEEE Transactions on Industrial Informatics, 2022, 18(10): 7118-7127.

[10] ZHANG Q K, ZHU L, LI Y J, et al. A group key agreement protocol for intelligent Internet of Things system[J]. International Journal of Intelligent Systems, 2022, 37(1): 699-722.

[11] SUN M, GUO Y Y, ZHANG D B, et al. Anonymous authentication and key agreement scheme combining the group key for vehicular ad hoc networks[J]. Complexity, 2021, 2021: 1-13.

[12] ZHENG J, YANG C, XUE J R, et al. A dynamic ID-based authenticated group key agreement protocol[C]// Proceedings of the 2015 4th National Conference on Electrical, Electronics and Computer Engineering. Pari: Atlantis Press, 2016: 1079-1084.

[13] NARESH V S, REDDI S, DIVAKAR ALLAVARPU V. Provable secure dynamic lightweight group communication in VANETs[J]. Transactions on Emerging Telecommunications Technologies, 2021,35(4):e4273.

[14] BRAEKEN A. Pairing free asymmetric group key agreement protocol[J]. Computer Communications, 2022, 181: 267-273.

[15] CUI J, WANG Y L, ZHANG J, et al. Full session key agreement scheme based on chaotic map in vehicular ad hoc networks[J]. IEEE Transactions on Vehicular Technology, 2020, 69(8): 8914-8924.

[16] SANTHANALAKSHMI S, SANGEETA K, PATRA G K. Design of group key agreement protocol using neural key synchronization[J]. Journal of Interdisciplinary Mathematics, 2020, 23(2): 435-451.

[17] ZHANG Q K, ZHU L, WANG R F, et al. Group key agreement protocol among terminals of the intelligent information system for mobile edge computing[J]. International Journal of Intelligent Systems, 2022, 37(12): 10442-10461.

[18] ZHANG Q K, LI Y, WANG R, et al. Blockchain-based asymmetric group key agreement protocol for Internet of

vehicles[J]. Computers & Electrical Engineering, 2020, 86: 106713.
[19] NARESH V S, DIVAKAR ALLAVARPU V V L, REDDI S, et al. A provably secure sharding based blockchain smart contract centric hierarchical group key agreement for large wireless ad-hoc networks[J]. Concurrency and Computation: Practice and Experience, 2022, 34(3): e6553.
[20] XU Z S, LI F, DENG H, et al. A blockchain-based authentication and dynamic group key agreement protocol[J]. Sensors, 2020, 20(17): 4835.
[21] ALWEN J, CORETTI S, JOST D, et al. Continuous group key agreement with active security[C]//Theory of Cryptography. Cham: Springer International Publishing, 2020: 261-290.
[22] LIN H Y. Integrate the hierarchical cluster elliptic curve key agreement with multiple secure data transfer modes into wireless sensor networks[J]. Connection Science, 2022, 34(1): 274-300.
[23] KAMIL I A, OGUNDOYIN S O. A lightweight certificateless authentication scheme and group key agreement with dynamic updating mechanism for LTE-V-based Internet of vehicles in smart cities[J]. Journal of Information Security and Applications, 2021, 63: 102994.
[24] AYAD A, HAMMAL Y. An efficient authenticated group key agreement protocol for dynamic UAV fleets in untrusted environments[C]//2021 International Conference on Networking and Advanced Systems (ICNAS). Piscataway: IEEE, 2021: 1-8.
[25] WANG M J, YAN Z. Privacy-preserving authentication and key agreement protocols for D2D group communications[J]. IEEE Transactions on Industrial Informatics, 2018, 14(8): 3637-3647.
[26] 张启坤, 甘勇, 王锐芳, 等. 簇间非对称群组密钥协商协议[J]. 计算机研究与发展, 2018, 55(12): 2651-2663
ZHANG Q K, GAN Y, WANG R F, et al. Inter-cluster asymmetric group key agreement[J]. Journal of Computer Research and Development, 2018, 55(12): 2651-2663 (in Chinese)

作者简介

张启坤 男, 1980 年 3 月出生, 河南信阳人. 现为郑州轻工业大学计算机与通信工程学院教授、硕士生导师. 主要研究方向为密码学、信息安全.
E-mail: zhangqikun04@163.com

朱 亮 男, 1996 年 11 月出生, 河南正阳人. 现为华东师范大学博士研究生. 主要研究方向为密码学、信息安全.
E-mail: zhuliang_9@163.com

韩桂锋 男, 2002 年 5 月出生, 山东聊城人. 现为郑州轻工业大学本科生. 主要研究方向为密码学、信息安全.
E-mail: 864068879@qq.com

刘梦琪 女, 1999 年 8 月出生, 河南安阳人. 现为郑州轻工业大学硕士研究生. 主要研究方向为密码学、信息安全.
E-mail: liu_confidence@163.com

金保华 男, 1966 年 9 月出生, 河南郑州人. 现为郑州轻工业大学计算机与通信工程学院院长、教授, 硕士生导师. 主要研究方向为人工智能、信息安全.
E-mail: jinbh@zzuli.edu.cn

李元章 男, 1978 年 9 月出生, 江苏盐城人. 现为北京理工大学副教授、博士生导师. 主要研究方向为人工智能对抗、信息安全.
E-mail: popular@bit.edu.cn