Journal of Computer Applications
计算机应用,2021,41(6):1611 - 1620
ISSN 1001-9081
CODEN JYIIDU
2021-06-10
http://www.joca.cn

文章编号:1001-9081(2021)06-1611-10
DOI:10.11772/j.issn.1001-9081.2020121955

基于云雾计算的可追踪可撤销密文策略属性基加密方案

陈家豪[1],殷新春[1,2*]
(1.扬州大学 信息工程学院,江苏 扬州 225127; 2.扬州大学广陵学院,江苏 扬州 225128)
(*通信作者电子邮箱xcyin@yzu.edu.cn)

摘 要:针对资源受限的边缘设备在属性基加密中存在的解密工作开销较大,以及缺乏有效的用户追踪与撤销的问题,提出了一种支持云雾计算的可追踪可撤销的密文策略属性基加密(CP-ABE)方案。首先,通过对雾节点的引入,使得密文存储、外包解密等工作能够放在距离用户更近的雾节点进行,这样既有效地保护了用户的隐私数据,又减少了用户的计算开销;其次,针对属性基加密系统中用户权限变更、用户有意或无意地泄露自己密钥等行为,加入了用户的追踪和撤销功能;最后,通过算法追踪到做出上述行为的恶意用户身份后,将该用户加入撤销列表,从而取消该用户访问权限。性能分析表明,所提方案用户端的解密开销降低至一次乘法运算和一次指数运算,能够为用户节省大量带宽与解密时间,且该方案支持恶意用户的追踪与撤销。因此所提方案适用于云雾环境下计算资源受限设备的数据共享。

关键词:密文策略属性基加密;云计算;雾计算;外包解密;用户可追踪;用户可撤销
中图分类号:TP309.7 **文献标志码**:A

Traceable and revocable ciphertext-policy attribute-based encryption scheme based on cloud-fog computing

CHEN Jiahao[1], YIN Xinchun[1,2*]
(1. *College of Information Engineering, Yangzhou University, Yangzhou Jiangsu* 225127, *China*;
2. *Guangling College of Yangzhou University, Yangzhou Jiangsu* 225128, *China*)

Abstract: Focusing on the large decryption overhead of the resource limited edge devices and the lack of effective user tracking and revocation in attribute-based encryption, a traceable and revocable Ciphertext-Policy Attribute-Based Encryption (CP-ABE) scheme supporting cloud-fog computing was proposed. Firstly, through the introduction of fog nodes, the ciphertext storage and outsourcing decryption were able to be carried out on fog nodes near the users, which not only effectively protected users' private data, but also reduced users' computing overhead. Then, in response to the behaviors such as user permission changes, users intentionally or unintentionally leaking their own keys in the attribute-based encryption system, user tracking and revocation functions were added. Finally, after the identity of malicious user with the above behaviors was tracked through the algorithm, the user would be added to the revocation list, so that user's access right was cancelled. The performance analysis shows that the decryption overhead at the user end is reduced to one multiplication and one exponential operation, which can save large bandwidth and decryption time for users; at the same time, the proposed scheme supports the tracking and revocation of malicious users. Therefore, the proposed scheme is suitable for data sharing of devices with limited computing resources in cloud-fog environment.

Key words: Ciphertext-Policy Attribute-Based Encryption (CP-ABE); cloud computing; fog computing; outsourcing decryption; user traceable; user revocable

0 引言

云计算[1]的广泛应用使得用户能够以较低的成本存储和共享数据。然而,随着网络边缘设备数量的迅速增加,这些设备产生的数据量越来越大,集中的云服务器已经不能高效地处理边缘设备产生的海量数据。雾计算[2]是对云计算的延伸,它是在边缘设备和远端云之间再扩展的一层,也可以叫作边缘网络层。在物联网应用中有些请求的处理不需要放到远端的云,而是可以直接在距离边缘设备较近的雾端进行处理。雾计算将云提供的服务扩展到网络边缘来提供本地化的服务,这有效满足了边缘设备对低时延、移动性支持、位置感知的服务需求。Statista的报告[3]显示,全世界的雾计算规模将在2022年达到130亿美元。

为了充分利用雾计算技术,Stojmenovic等[4]引入了云雾设备(cloud-fog-device)体系来提供各种应用服务,包括智能城市、智能电网、智能交通和工业自动化。在该体系中,数以千计的云被用来存储数据;数百万个雾节点被用来减少数据传输期间的工作负载和带宽;数十亿个边缘设备用于请求和上

收稿日期:2020-11-04;**修回日期**:2021-03-29;**录用日期**:2021-04-06。 **基金项目**:国家自然科学基金资助项目(61472343)。
作者简介:陈家豪(1997—),男,安徽安庆人,硕士研究生,主要研究方向:密码学、物联网安全、加密算法和协议; 殷新春(1962—),男,江苏姜堰人,教授,博士生导师,博士,CCF会员,主要研究方向:密码学、软件质量保障、高性能计算。

传数据。其中,雾节点在维护高速缓存的数据方面发挥着重要作用,并为数据的智能处理提供了协同合作。雾节点的目的是帮助边缘设备克服资源限制,以减少数据传输期间的带宽成本。以智能交通为例,云雾设备体系实现了应用服务器与车辆之间的高效数据通信。具体而言,云从应用服务器接收消息,并转发到相应的雾节点,雾节点将消息传送到终端设备。

然而,云雾计算并不是完全可信的,如果不能很好地解决其中的安全和隐私保护问题,那么这将严重阻碍云雾计算的发展[5-8]。Stojmenovic等[4]指出,雾节点在分发身份验证信息和收集审核日志时,与远程云的连接不稳定,因此容易遭受中间人攻击。这种脆弱的连接降低了在远程云服务器上执行身份验证协议的可靠性。Huang等[7]随后引入了一种带有独立身份验证(Stand-Alone Authentication, SAA)的新机制,以实现用户身份验证从而适应不稳定的连接情况。但是,要采用SAA,需要保护雾节点与用户之间的身份验证信息,这又带来了额外的存储开销。数据加密是进行安全数据共享的常用方法,但是在传统的云雾计算中,基于公钥基础设施的身份验证困难且效率不高。属性基加密(Attribute-Based Encryption, ABE)[9-11]机制能克服这一障碍,它无需事先知道数据接收者的具体身份,却能够实现灵活的一对多加密,同时能实现对数据的细粒度访问控制。Sahai等[9]首次提出了ABE机制。随后Goyal等[10]首次提出了基于密钥策略的属性基加密(Key-Policy Attribute-Based Encryption, KP-ABE)方案,其中在密钥中指定访问策略,在密文中指定属性集合,只有当密文的属性集合满足密钥所指定的访问策略时才能解密。Bethencourt等[11]首次提出基于密文策略的属性基加密(Ciphertext-Policy Attribute-Based Encryption, CP-ABE)方案,与KP-ABE构造相反,它在密文中指定访问策略,在密钥中指定属性集合,只有当密钥的属性集合满足密文指定的访问策略时才能解密。因为CP-ABE方案不仅可以对数据共享进行细粒度的访问控制,而且数据加密者可以定义访问策略,所以CP-ABE得到了更广泛的应用。

虽然属性基加密具有广阔的应用前景,但是在实际应用中,存在恶意用户将解密密钥泄漏给ABE系统中的第三方的情况。由于解密密钥与属性相关联,因此无法确定泄漏解密密钥的用户。例如,Alice拥有属性集{计算机系,教授,女性}而Bob拥有属性集{计算机系,教授,男性}。假设根据访问策略{计算机系 and 教授}生成一条密文,由于Alice和Bob都具有相同的属性子集{计算机系,教授},他们都能够解密这个密文,如果解密密钥泄露,则无法确定是Alice还是Bob泄漏了密钥。为了解决恶意用户密钥泄露的问题,Liu等[12]提出了第一个白盒可追踪CP-ABE方案,接着,Ning等[13-14]提出了两个白盒可追踪CP-ABE方案,它们分别支持大属性空间和灵活的属性集。尽管上述方案能够追踪到恶意用户,但无法有效地撤销他们的访问权限。为满足这一实际要求,文献[15-18]提出了许多可撤销的基于属性的加密(Revocable Attribute-Based Encryption, RABE)方案。目前主要有两种撤销机制:间接撤销和直接撤销。对于前者,属性权威机构需要与未撤销的用户通信并发送更新信息,系统中存在大量用户时,这将导致大量的通信开销。而对于后者,用户不必与更新撤销列表的属性权威机构进行通信。高嘉昕等[16]提出了一个支持属性撤销的可追踪外包属性加密方案,其中属性撤销需要利用重加密方法更新用户密钥,这导致了大量的通信开销。明洋等[18]提出了一个支持直接撤销的可验证外包的属性加密方案,该方案为每个属性引入了版本密钥,增加了用户的存储开销,且该方案只实现了属性层面的撤销,并未对用户层面进行撤销。目前,文献[19-23]提出了许多可直接撤销的属性基加密方案。Shi等[22]提出了一个有效的撤销方案,其中数据服务管理者只需更新与最新撤销列表R'相关的部分密文。但Shi等[22]只是专注于KP-ABE的撤销,且不支持外包解密。

为了解决上述问题,本文提出了一个在云雾环境下的支持用户撤销的可追踪可外包解密的密文策略属性基加密方案。本文的主要工作如下:

1)支持恶意用户的追踪和撤销。在本文的方案中,解密密钥分为两部分:一部分与属性集相关,另一部分与二叉树中叶子节点存储的用户身份有关,与Liu等[12]的方案相比,本文方案不需要额外的身份列表来存储用户的身份。密文分为两部分:一个与访问策略相关,另一个与撤销列表相关。在解密密钥泄露的情况下,可以从解密密钥中追踪到该用户的身份,并将其添加到撤销列表中,以此来撤销其访问权限。

2)支持雾计算与外包解密。本文方案针对实际应用中边缘设备计算能力不足、通信延时较大等缺陷,在云计算技术和传统的属性基加密的基础上,加入了雾计算与外包解密技术。在本文中,雾节点与云服务器进行通信,而边缘设备只需与本地雾节点进行通信,从而能有效降低设备的通信延时与响应时间。同时,利用雾节点进行外包解密,能够显著减少解密的计算量,提高边缘设备的解密效率。

安全性分析表明,本文方案在判定性q-BDHE(decisional q-Bilinear Diffie-Hellman Exponent)假设下是IND-CPA(INDistinguishability Chosen-Plaintext Attack)安全的,且在l-SDH(l-Strong Diffie-Hellman)假设下可抵抗密钥伪造攻击。性能分析表明,本文所提的方案在系统功能和计算开销方面相较其他方案更具有优势。

1 预备知识

1.1 符号介绍

本文方案中使用到的一些符号的定义如表1所示。

1.2 双线性映射

令G和G_T是两个阶为素数p的乘法循环群,g是G的一个生成元。存在一个双线性映射$e: G \times G \rightarrow G_T$,满足如下性质:

1)双线性性:$\forall u, v \in G, \forall a, b \in \mathbf{Z}_p$,有$e(u^a, v^b) = e(u, v)^{ab}$。

2)非退化性:$e(g, g) \neq 1$。

3)可计算性:对$\forall u, v \in G$,都存在有效算法去计算$e(u, v)$。

1.3 访问策略

设$\{P_1, P_2, \cdots, P_n\}$为$n$个参与者的集合。对于集合$A \subseteq 2^{\{P_1, P_2, \cdots, P_n\}}$,如果$\forall B, C \subseteq \{P_1, P_2, \cdots, P_n\}$,$B \in C$,$B \subseteq C \Rightarrow C \in A$,则称集合$A$是单调的。其中属于$A$的集合称为授权集;否则,称为非授权集[24]。

举例来说,对于$\{A,B,C,D\}$,单调集合$\{\{A,B\},\{B,C\},\{C,D\},\{A,B,C\},\{A,B,D\},\{A,C,D\},\{B,C,D\}\}$就是一个单调访问策略,$\{A,B\},\{B,C\},\{C,D\}$是三个授权集合,而$\{A,D\}$则是一个非授权集合。通常来说,单调访问策略可以表示成不包含“非”的布尔公式;非单调的访问策略,可以用包含“非”的布尔公式来表示。

表 1　相关符号及定义

Tab. 1　Related notations and their definitions

符号	定义
p	大素数
G,G_T	p阶循环群
g	群G的生成元
$\mathbf{Z}_p$	不大于p的整数域
e	双线性映射
U	用户集合
$\mathcal{T}$	二叉树
u	用户
A	属性全集
$(\boldsymbol{M},\rho)$	访问策略($\boldsymbol{M}$为一个矩阵,ρ为一个映射函数)
$S\vDash(\boldsymbol{M},\rho)$	属性满足访问策略
$S\nvDash(\boldsymbol{M},\rho)$	属性不满足访问策略
R	撤销列表
List	追踪列表

1.4　线性秘密共享方案

令$\mathcal{V}$表示属性全集,p表示一个素数。秘密空间$\mathbf{Z}_p$上的秘密共享方案Π,实现了$\mathcal{V}$上的访问策略。如果秘密分享方案Π满足以下两个性质[23],则Π是线性的。

1)秘密$s\in\mathbf{Z}_p$分割成的每一个部分对应了$\mathcal{V}$中的一个属性,且每个部分构成$\mathbf{Z}_p$上的一个向量。

2)对于访问策略$S=(\boldsymbol{M},\rho)$,$\boldsymbol{M}$是一个$l\times n$的秘密分享矩阵。函数ρ将$\boldsymbol{M}$的第$i\in\{1,2,\cdots,l\}$行映射到全集$\mathcal{V}$的一个属性$\rho(i)$。通过这样的映射,矩阵$\boldsymbol{M}$的每一行都代表$\mathcal{V}$上的一个属性。例如,构造一个列向量$\boldsymbol{u}=(s,y_2,y_3,\cdots,y_n)^{\mathrm{T}}$,其中$y_2,y_3,\cdots,y_n\in\mathbf{Z}_p$是随机数,用于隐藏要共享的秘密值$s$。则$\boldsymbol{Mu}\in\mathbf{Z}_p^{l\times 1}$是$l$行1列的向量,也就是把秘密值$s$根据$\Pi$分成了$l$个部分。$(\boldsymbol{Mu})_i$对应属性$\rho(i)$,其中$i\in[l]$。

如文献[24]中所示,符合以上定义的线性秘密共享方案(Linear Secret Sharing Scheme, LSSS)可以进行线性重构算法Recon。Recon的具体定义如下:Π为访问策略S上的线性秘密共享方案,$P\in S$为任意授权集合,集合$I=\{i\in[l]\wedge\rho(i)\in P\}$且$I\subseteq\{1,2,\cdots,l\}$。对于秘密$s$的任意合法分享$\{\lambda_i=(\boldsymbol{Mu})_i\}_{i\in I}$,存在常量集合$\{\sigma_i\in\mathbf{Z}_p\}_{i\in I}$可以在多项式时间内计算出来。而对于非授权集合$p'$,则不存在$\{\sigma_i\}_{i\in I}$这样的常量集合。

1.5　二叉树

令U为系统中的用户集合,R为撤销列表,则在二叉树[25]中定义:

1)一个二叉树$\mathcal{T}$的叶子节点只关联一个用户。令*root*为根节点,$|U|$为用户数,则树中的节点数为$2|U|-1$,使用宽度优先搜索为树中节点编号。例如,根节点为1,最后一个节点为$2|U|-1$。

2)$path(i)$定义为从根节点到节点的路径。

3)最小包含集合$cover(R)$是所有未在撤销列表内的用户的最小集合[26]。令u_i为撤销列表R中的用户,x_l和x_r分别为x节点的左右孩子节点,定义一个可以以最少节点表示不在R中节点的算法使得$cover(R)=Covernodes(\mathcal{T},R)$,其中$Covernodes(\mathcal{T},R)$定义如算法1所示。

4)若一个用户不在撤销列表中,则存在一个唯一的节点$j=cover(R)\cap path(u)$。

如图1所示,撤销列表为$R=\{u_5,u_8\}=\{11,14\}$,所以$cover(R)=\{1,12,13\}$。已知u_3的路径$path(u_3)=path(9)=\{0,1,4,9\}$,因此这个唯一的节点$j=cover(R)\cap path(u_8)=\{1\}$。

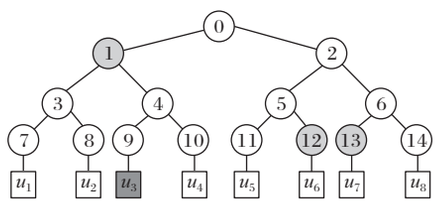

图1　二叉树

Fig. 1　Binary tree

算法1　*Covernodes*。

function *Covernodes*(T,R)
　$X,Y\leftarrow\varnothing$
　for $u_i\in R$ do
　　$X\cup path(U_i)$
　end for
　for $x\in X$ do
　　if $x_l\notin X$ then $Y\leftarrow Y\cup x_l$
　　end if
　　if $x_r\notin X$ then $Y\leftarrow Y\cup x_r$
　　end if
　end for
　if $Y=\varnothing$ then $Y\leftarrow root$
　end if
　return Y
end function

1.6　复杂性假设

q-BDHE(q-Bilinear Diffie-Hellman Exponent)假设[27]:选取阶为素数p的乘法循环群G和G_T,g是群G的生成元,e为双线性映射$e:G\times G\rightarrow G_T$,随机选取$d,s\in\mathbf{Z}_p$,随机选取$F\in G_T$。给定$\boldsymbol{y}=(g,g^s,g^d,\cdots,g^{d^q},g^{d^{q+2}},g^{d^{2q}})$,令$T=e(g,g)^{d^{q+1}s}$,$F$为$G_T$中的随机元素,如果$|\Pr[B(\boldsymbol{y},T=e(g,g)^{d^{q+1}s})=0]-\Pr[B(\boldsymbol{y},T=F)=0]|\geqslant\varepsilon$,即$B$能够在多项式时间内区分$T$和$F$,则称$B$能以优势$\varepsilon$解决$q$-BDHE假设。

定义1　若不存在一个算法可以在多项式时间内以不可忽略的优势解决q-BDHE问题,则称q-BDHE假设成立。

l-SDH(l-Strong Deffie-Hellman)假设[19]:选取阶为素数p的乘法循环群G,g是群G的生成元,随机选取$x\in\mathbf{Z}_p$。给定一个$l+1$元组$(g,g^x,g^{x^2},\cdots,g^{x^l})$作为输入,输出一个配对$(c,g^{1/(c+x)})\in\mathbf{Z}_p\times G$,如果$|\Pr[B(g,g^x,g^{x^2},\cdots,g^{x^l})=(c,g^{1/(c+x)})]|\geqslant\varepsilon$,即$B$能够正确输出配对$(c,g^{1/(c+x)})\in\mathbf{Z}_p\times G$,则称$B$能以优势$\varepsilon$解决$l$-SDH假设。

定义2　若不存在一个算法可以在多项式时间内以不可

忽略的优势解决 l-SDH 问题，则称 l-SDH 假设成立。

2 系统和安全模型

在本文中，考虑如下应用场景。某地的汽车销售服务公司（以下简称公司）为其售出的车辆提供基于云雾计算的数据共享服务。为了实现细粒度的访问控制和支持一对多的通信模式，公司需要为加密数据制定灵活的访问策略。在该项服务中，每个车辆会被分配一系列属性，如{“2014 年生产”，“A 品牌”，“SUV”}。作为一种强大的“一对多”加密机制，密文策略属性基加密（CP-ABE）非常适合该应用场景。出于安全考虑，发送方需要先使用 CP-ABE 技术加密其信息，然后再上传至本地的雾节点，雾节点分析密文是否有长期用途（long-term），如果密文有长期用途，则由雾节点上传至云服务器（以分担雾节点存储压力），否则存在本地或者转发给其他雾节点。如公司需要召回一批 2014 年生产的 A 品牌的运动型多用途汽车（Sport Utility Vehicle，SUV），这批车辆的刹车存在重大安全隐患，为了保障用户隐私安全同时避免此安全隐患被不法分子获悉，公司需要加密消息并嵌入访问策略为“2014 年生产∧A 品牌∧SUV”，以确保只有满足此访问策略的车辆才能解密该密文。此密文有长期用途，由公司上传至本地雾节点并由雾节点上传至云服务器。若该公司为了答谢客户，准备在“双十一”举办一个限时优惠活动。为了确保目标客户能够接收到消息且该消息不被其他汽车保养公司所获得，该公司需要加密消息并嵌入访问策略为“B 品牌∧轿车”，以确保只有满足此访问策略的车辆才能解密该密文。此密文仅有短期用途（short-term），由发送方上传至本地雾节点并存储，若本地雾节点存储能力不够，则将此消息发送给相邻的雾节点存储。只要车辆的属性满足密文中嵌入的访问策略，则由雾节点先进行密文的外包解密，之后将半解密密文发送回车辆，车辆利用自己的密钥解密从而获得明文。

2.1 系统模型

本文方案的系统模型一共包含 5 个部分，如图 2 所示：

1）可信权威机构负责生成系统公共参数和主私钥，还负责车辆的注册、密钥分发。一旦发现有密钥被泄露，可信权威机构就调用跟踪算法对该密钥进行追踪，找到泄露解密密钥的恶意用户，并将恶意用户的身份加入撤销列表中。

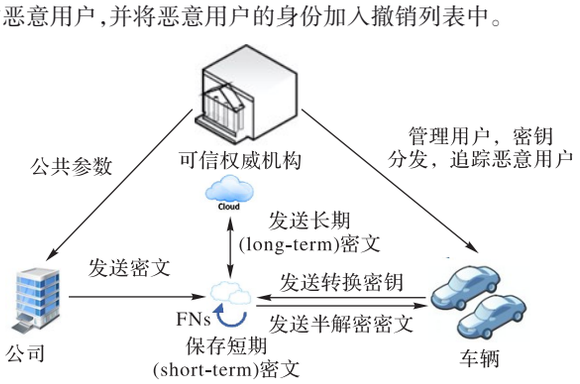

图 2 本文方案的系统模型

Fig. 2 System model of proposed scheme

2）车辆是资源受限的设备，主要进行以下工作：

①车辆向本地雾节点请求相关密文。

②车辆将需要分享的数据进行加密并且传送给本地雾节点。

3）公司根据可信权威机构发布的公共参数和撤销列表，制定相应访问策略，并将消息加密后传送给雾节点。

4）雾节点（Fog Node，FN）是边缘服务器，负责以下工作：

①FNs 充当高速缓存，存储具有短期目的的数据和信息。

②FNs 将具有长期目的的数据转发到云服务器。

③在从车辆接收数据查询之后，FNs 首先搜索本地存储并与其他 FNs 进行交互。如果请求不到查询的密文，则 FNs 向云服务器请求密文。

值得注意的是，尽管允许车辆与云服务器直接通信，但是由于云服务器存在远端而 FNs 在实际情况下更接近车辆，因此车辆与云服务器直接通信会占用更多带宽。

5）云服务器（Cloud Server，CS），具备大量存储空间，可以容纳数据，还可以通过公共通道将加密的数据共享给 FNs。

2.2 形式化定义

本文方案主要由以下 6 个算法组成，分别是系统初始化算法 Setup、加密算法 Encrypt、用户密钥生成算法 KeyGen、外包解密算法 Transform、解密算法 Decrypt 和追踪算法 Trace。各算法分别定义如下：

1）$\mathrm{Setup}(\lambda, A, \mathcal{T}) \rightarrow (PP, MSK, R, List)$：该算法由可信权威机构执行，算法的输入为安全参数 λ、属性全集 A 和二叉树 $\mathcal{T}$，输出系统公共参数 PP 和主私钥 MSK，并将 PP 公开。可信权威机构还初始化一个空的撤销列表 R 和一个空的追踪列表 $List$。

2）$\mathrm{Encrypt}(PP, m, (\boldsymbol{M}, \rho), R) \rightarrow CT$：该算法由发送者执行，算法输入公共参数 PP、要发送的明文消息 m、一个 LSSS 访问策略 $(\boldsymbol{M}, \rho)$ 和撤销列表 R，输出密文 CT。

3）$\mathrm{KeyGen}(MSK, u, S) \rightarrow SK$：该算法由可信权威机构来执行，算法输入主私钥 MSK、用户身份 u、用户属性集 S，输出用户密钥 SK，并将 SK 发送给车辆。SK 包含两部分，分别是用户转换密钥 TK 与用户个人密钥 UK。

4）$\mathrm{Transform}(CT, TK) \rightarrow CT'$：该算法由雾节点执行，该算法输入密文 CT 和用户转换密钥 TK，输出半解密密文 CT'，并将 CT' 发送给车辆。

5）$\mathrm{Decrypt}(UK, CT') \rightarrow m$：该算法由接收者执行，输入用户个人密钥 UK 和半解密密文 CT'，输出明文 m。

6）$\mathrm{Trace}(PP, R, SK) \rightarrow u \text{ or } u_{\varnothing}$：该算法由可信权威机构执行，输入公共参数 PP、撤销列表 R、用户密钥 SK，如果追踪到了恶意用户，则输出该用户的身份 u，否则输出 $u_{\varnothing}$。

2.3 密钥伪造攻击安全模型定义

本文采用文献[28]定义的密钥伪造攻击模型，其中密钥伪造攻击定义可以通过一个挑战者 B 和一个攻击者 Adv 之间的安全游戏来描述，具体步骤如下所示：

1）初始化：挑战者 B 运行 Setup 算法，并将公共参数 PP 发送给攻击者 Adv。

2）密钥询问：攻击者 Adv 向挑战者 B 询问与属性集 $(u_1, S_1)(u_2, S_2)\cdots(u_q, S_q)$ 相关的用户密钥，其中 $u_i \in R$ 或者 $S_l \notin (\boldsymbol{M}, \rho), i = 1, 2, \cdots, q$。$B$ 运行 KeyGen 算法并返回相应的密钥。

3）密钥伪造：攻击者 Adv 输出一个用户密钥 SK^*。如果

$\mathrm{Trace}(PP, R, SK^*) \neq \perp$,并且$\mathrm{Trace}(PP, R, SK^*) \notin \{id_1, id_1, \cdots, id_q\}$,其中$id_i (i = 1, 2, \cdots, q)$为用于询问的用户身份,攻击者$Adv$赢得上述游戏。

攻击者Adv赢得上述游戏的优势定义为:

$\varepsilon = \Pr[\mathrm{Trace}(PP, R, SK^*) \notin \{\perp, id_1, id_2, \cdots, id_q\}]$。

定义 3　若不存在多项式时间攻击者能以不可忽略的优势赢得上述游戏,那么称本文提出的方案是可抵抗密钥伪造攻击的。

2.4　选择明文攻击安全模型定义

本文采用文献[27]定义的安全模型,该模型定义为挑战者B与攻击者Adv之间交互的安全游戏,该游戏是选择明文攻击(Chosen Plaintext Attack, CPA)下的不可区分性(INDistinguishability, IND)游戏。具体描述如下:

1)初始化:攻击者Adv选择要挑战的一个访问策略$(\boldsymbol{M}^*, \rho^*)$并将其发送给挑战者$B$,其中$\boldsymbol{M}^*$是一个$l^* \times n^*$的矩阵,函数$\rho^*$把矩阵$\boldsymbol{M}^*$的一行映射成一个属性$\rho^*(i)$。

2)系统建立:挑战者B运行Setup算法,将公共参数PP发送给攻击者Adv。

3)阶段1:攻击者Adv向挑战者B询问与属性集$(u_1, S_1)(u_2, S_2)\cdots(u_q, S_q)$相关的用户密钥。

①若$S_i \models (\boldsymbol{M}^*, \rho^*)$且$u_i \notin R^*$,则不做处理。

②若$S \not\models (\boldsymbol{M}, \rho)$或$u_i \in R^*$,挑战者$B$生成一个与属性$(u_i, S_i)$相关的用户转换密钥,并将它发送给攻击者$Adv$。

4)挑战:攻击者Adv向挑战者B提交2个等长的消息m_0和m_1。挑战者掷一枚均匀的硬币$\eta \in \{0, 1\}$,并在访问策略$(\boldsymbol{M}^*, \rho^*)$和撤销列表$R^*$下加密$m_\eta$生成挑战密文$CT^*$。挑战者$B$将$CT^*$发送给攻击者$Adv$。

5)阶段2:阶段2重复阶段1的步骤。

猜测:攻击者Adv输出对η的猜测η',若$\eta = \eta'$,则攻击者Adv赢得游戏。

攻击者Adv赢得上述游戏的优势定义为:

$\varepsilon = |\Pr[\eta' = \eta] - 1/2|$

定义 4　若不存在多项式时间攻击者能以不可忽略的优势赢得上述游戏,那么认为本文提出的方案是IND-CPA安全的。

3　本文方案

3.1　方案工作流程

本文方案可分为4个阶段:

1)系统初始化。可信权威机构运行Setup算法生成公共参数PP,并将PP发送给各个实体。可信权威机构运行KeyGen算法为每个用户生成密钥SK,并通过安全信道发送给车辆。

2)数据上传。数据发送者将数据加密并上传至本地雾节点。FNs分析密文是否具有长期用途,若密文仅有短期用途,则FNs将此密文存储在本地,若本地节点存储容量不够,则将此密文转存至相邻的FNs。若密文具有长期用途,FNs将密文上传至云服务器保存。

3)数据下载。当车辆向本地FNs请求密文时,$\mathrm{FN_S}$首先在本地寻找符合要求的密文,如果没有找到,则此FNs向其他FNs与CS请求密文,雾节点将获取到的密文进行外包解密,并将半解密密文发送给车辆,由车辆进行最终解密。

4)恶意用户追踪与撤销。在用户密钥泄露的情况下,可信权威机构可以从该密钥中追踪到恶意用户的身份,并将其添加到撤销列表中,以此来撤销其访问权限。

3.2　方案构造

本节主要展示方案的具体构造并对相关参数进行说明。在本文的方案中,二叉树用于实现追踪和撤销,用户密钥分为两个部分:一部分与用户的身份有关,另一部分与用户的属性集有关。密文包含两个部分:一部分与撤销列表相关,另一部分与访问策略相关。当且仅当用户密钥中的属性满足密文中的访问策略并且用户身份不在撤销列表中时,该用户才能解密密文。具体方案如下:

1)$\mathrm{Setup}(\lambda, A, \mathcal{T}) \rightarrow (PP, MSK, R, List)$。

Setup算法由可信权威机构执行,算法的输入为安全参数λ、属性全集A和二叉树$\mathcal{T}$,输出系统公共参数PP、主私钥MSK、撤销列表R和追踪列表$List$。该算法选取阶为p的循环群G和G_T,G的生成元为g,$e: G \times G \rightarrow G_T$为双线性映射。$U$为用户集合,$R$是一个撤销列表(初始化为空),$List$是一个追踪列表(初始化为空),$\mathcal{T}$是一个满二叉树,树上的每一个叶子节点分别对应一个用户u,树的深度为d。因此用户数目最多为$|U| = 2^d$,树中的节点数为$2|U| - 1$。算法做如下运算:

①随机选取$\alpha, \alpha \in \mathbf{Z}_p$,$h \in G$,一个抗碰撞的哈希函数$H: \{0, 1\}^* \rightarrow G$。

②对$\forall x \in A$,选择$A_x \in G$。

③对树中的每一个节点,在$\mathbf{Z}_p$中随机选取$X = \{x_i\}_{i \in [2|U|-1]}$,计算$Y = \{y_i | y_i = g^{x_i}\}_{i \in [2|U|-1]}$。

系统按照以下格式公布公共参数(PP)并保存主私钥和追踪列表$(MSK, List)$:

$$PP = (g, h, e(g, g)^\alpha, g^a, H, R, (A_x)_{x \in A}, A)$$

$$MSK = (\alpha, a, X)$$

$$List = \varnothing$$

2)$\mathrm{Encrypt}(PP, m, (\boldsymbol{M}, \rho), R) \rightarrow CT$。

Encrypt算法由公司执行,算法输入公共参数PP、撤销列表R、要发送的消息明文m和访问策略$(\boldsymbol{M}, \rho)$,输出密文CT。其中$\boldsymbol{M}$是一个$l \times n$的矩阵,函数ρ把矩阵$\boldsymbol{M}$的一行映射成一个属性$\rho(i)$。随机选择$s, v_2, v_3, \cdots, v_n \in \mathbf{Z}_p$,并设置向量$\boldsymbol{\mu} = (s, v_2, v_3, \cdots, v_n)^{\mathrm{T}}$,其中$s$是用于分享的随机秘密值。对所有的$i = 1, 2, \cdots, l$,计算$\lambda_i = \boldsymbol{M}_i \times \boldsymbol{\mu}$,其中$\boldsymbol{M}_i$表示矩阵$\boldsymbol{M}$的第$i$行。

①首先,设置如下与访问策略关联的部分密文:

$$\left(C = me(g, g)^{\alpha s}, C_0 = g^s, C_0' = g^{\alpha s}, \{C_i = h^{\lambda_i} A_{\rho(i)}^{-s}\}_{i \in [l]}\right)$$

②对$\forall j \in cover(R)$,有$path(j) = \{i_0, i_1, \cdots, i_{dept(j)}\}$,其中$i_0 = root$,$i_{dept(j)} = j$。然后,设置如下与撤销列表$R$相关的部分密文:

$$\left(\{W_j = y_j^s\}_{j \in cover(R)}\right)$$

③最后构成完整的密文如下:

$$CT = \left(C, C_0, C_0', \{C_i\}_{i \in [l]}, \{W_j\}_{j \in cover(R)}, (\boldsymbol{M}, \rho), R\right)$$

3)$\mathrm{KeyGen}(MSK, u, S) \rightarrow SK$。

KeyGen算法由可信权威机构来执行,算法输入主私钥

MSK,身份 u,用户属性集 S,输出用户密钥 SK,SK 由用户转换密钥 TK 与用户个人密钥 SK 组成。随机选择 $r,t,z\in\mathbf{Z}_p$。计算 $c=H(i_d)$,其中 i_d 是与用户 u 相关联的叶子节点的值,然后把二元组 (c,i_d) 加入列表 $List$。

①首先,设置如下与用户属性集相对应的部分密钥:

$$\left(K'=c,K=g^{\frac{\alpha+z\alpha r}{za+zc}}h^{rt},L=g^{rt},L'=g^{art},\{K_X=(A_x^{(a+c)rt}\}_{x\in S}\right)$$

②令 $path(id)=\{i_0,i_1,\cdots,i_d\}$,$i_0=root$,$i_d$ 是与用户 u 相关联的叶子节点。随机选取 $b\in\mathbf{Z}_p$,设置与用户身份 u 关联的部分密钥,如下所示:

$$\left(D=g^{ar}y_{id}^{b},E=g^{b}\right)$$

③用户转换密钥 TK 与用户个人密钥 UK 如下所示:

$$TK=\left(K',K,L,L',\{K_x\}_{x\in S},D,E,\{x_i\}_{i\in path(i_d)}\right)$$

$$UK=(z)$$

④最后构成完整用户密钥如下:

$$SK=(TK,UK)$$

4)Transform$(CT,TK)\rightarrow CT'$。

Transform 算法由雾节点执行,该算法输入密文 CT 和用户转换密钥 TK,输出半解密密文 CT'。该算法的输出存在以下两种情况:

情况 1 若用户的身份 $u\in R$ 或者用户属性集 S 不满足密文的访问策略 $(\boldsymbol{M},\rho)$,算法输出 $\perp$。

情况 2 若用户身份 $u\notin R$ 且用户属性集 S 满足密文的访问策略 $(\boldsymbol{M},\rho)$,算法执行如下运算:

①因为 $u\notin R$,所以存在一个节点 $j=cover(R)\cap path(u)$。令 $path(j)=\{i_0,i_1,\cdots,i_{dept(j)},\cdots,i_d\}$,其中,$i_{dept(j)}=j$,$i_d$ 是与用户 u 相关联的叶子节点。计算 $Y_{i_d}=y_{i_d}^{s}$。

②对于 $S\in(\boldsymbol{M},\rho)$,令 $I=\{i:\rho(i)\in S\}\subseteq\{1,2,\cdots,l\}$,存在 $\{c_i|i\in I\}$ 使得 $\{c_iM_i=(1,0,\cdots,0)\}$,因此,有 $\sum_{i\in I}c_i\lambda_i=s$。

③最终,计算:

$$K_1=e(K,C_0^{K'}\cdot C_0')=e(g^{\frac{\alpha+z\alpha r}{za+zc}}h^{rt},g^{(a+c)s})=e(g,g)^{\frac{\alpha s}{z}}e(g,g)^{\alpha rs}e(g,h)^{(a+c)rts}$$

$$K_1'=\sum_{i\in I}(e(L^{K'}\cdot L',C_i)\cdot e(K_{\rho(i)},C_0))^{c_i\lambda_i}=\sum_{i\in I}(e(g,h)^{(a+c)rtc_i})=e(g,h)^{(a+c)rts}$$

$$K_1''=\frac{e(C_0,D)}{e(E,Y_{i_d})}=e(g,g)^{\alpha rs}$$

$$CT'=\frac{K_1}{K_1'\cdot K_1''}=e(g,g)^{\frac{\alpha s}{z}}$$

系统输出半解密密文 CT'。

5)Decrypt$(UK,CT')\rightarrow m$。

Decrypt 算法由车辆执行,输入半解密密文 CT' 和用户个人密钥 UK,输出明文 m:

$$m=\frac{C}{(CT')^{z}}$$

6)Trace$(PP,R,SK)\rightarrow u$ or $u_{\varnothing}$。

Trace 算法由可信权威机构执行,输入公共参数 PP,撤销列 R,用户密钥 SK,输出跟踪到的恶意用户 u 或 $u_{\varnothing}$。

若用户密钥 SK 符合以下三个检测:

1)$K'\in\mathbf{Z}_p,K,L,L',K_x,D,E\in G$。

2)$e(g,L')=e(g^{a},L)\neq 1$。

3)$\exists x\in S,\text{s.t.}\,e(A_x,L^{K'}L)=e(g,K_x)\neq 1$。

那么用户密钥 SK 是完整的,否则算法直接输出符号 $\perp$ 表示密钥不完整,无法进行追踪。对于通过上一步完整性检查的用户密钥,算法在列表 $List$ 中根据密钥中的 K' 查找对应的用户 u。如果找到了 K',算法输出 K' 对应的 i_d,该用户就是被追踪的恶意用户,并将其身份 u 加入撤销列表 R;否则,输出 $u_{\varnothing}$ 表示没有查找到恶意的用户。

4 安全性分析

4.1 密钥伪造攻击

定理 1 令 q 为攻击者 Adv 查询密钥的次数,若 l-SDH 困难性假设成立,则方案在 $q<l$ 的情况下是可抵抗密钥伪造攻击的。

证明 假设存在一个多项式时间的攻击者 Adv 在经过了 $q(l=q+1)$ 次密钥查询之后可以以不可忽略的优势 ε 赢得密钥伪造攻击游戏。那么能够构造一个概率多项式时间算法 B 以不可忽略的优势攻破 l-SDH 困难性假设。选取阶为 p 的乘法循环群 G 和 G_T,G 的生成元为 g,$e:G\times G\rightarrow G_T$ 为双线性映射,$g_1\in G,a\in\mathbf{Z}_p$。给出实例 $IN_{\text{SDH}}=\left(p,G,G_T,E,g_1,g_1^{a},\cdots,g_1^{a^l}\right)$,$B$ 的目标是输出 $c_r\in\mathbf{Z}_p$ 和 $w_r\in G$ 并满足 $w_r=g_1^{\frac{1}{a+c_r}}$,从而解决 l-SDH 假设。令 $A_i=g_1^{a^i}(i=0,1,\cdots,l)$,$B$ 以挑战者的身份与 Adv 进行密钥伪造攻击游戏。

1)初始化。B 随机选取 q 个不同的值 $c_1,c_2,\cdots,c_q\in\mathbf{Z}_p$,随机选取 $\alpha,\theta\in\mathbf{Z}_p,u\in G$。令多项式 $f(y)=\prod_{i=1}^{q}(y+c_i)$。展开 $f(y)$,可以得到形如 $f(y)=\sum_{i=1}^{q}\alpha_iy^i$ 的表达式,其中 $\alpha_i\in\mathbf{Z}_p(i=0,1,\cdots,q)$,是多项式 $f(y)$ 展开式中各项的系数。B 计算 g 和 g^{a}:

$$g=\prod_{i=0}^{q}(A_i)^{\alpha_i}=g_1^{f(a)}$$

$$g^{a}=\prod_{i=1}^{q+1}(A_i)^{\alpha_{i-1}}=g_1^{f(a)\cdot a}$$

对每一个属性 $x\in A$,随机选取 $u_x\in\mathbf{Z}_p$,令 $A_x=g^{u_x}$。对二叉树 $\mathcal{T}$ 中的每个节点,在 $\mathbf{Z}_p$ 中随机选取 $X=\{x_i\}_{i\in[2|U|-1]}$,计算 $Y=\{y_i|y_i=g^{x_i}\}_{i\in[2|U|-1]}$。公共参数如下所示:

$$PP=(g,h,e(g,g)^{\alpha},g^{a},H,(A_x)_{x\in A},Y)$$

2)密钥询问。Adv 提交 (u_i,S_i) 给 B,询问用户 u_i 的密钥 SK_i。假设这是 Adv 的第 i 次询问 $(i\leqslant q)$。令多项式 $f_i(y)=\frac{f(y)}{y+c_i}=\prod_{j=1,j\neq i}^{q}(y+c_j)=\sum_{j=0}^{q-1}\beta_jy^j$,$B$ 计算 $\sigma_i=\prod_{j=0}^{q-1}(A_j)^{\beta_j}=g_1^{f_i(a)}=g_1^{f(a)/(a+c_i)}=g^{1/(a+c_i)}$,然后 B 随机选取 $t,r\in\mathbf{Z}_p$ 并计算:$K'=c_i,K=(\sigma_i)^{\alpha/z+\alpha r}h^{rt},L=g^{rt},L'=(g^{a})^{rt},\{K_x=(g^{a}\cdot g^{c_i})^{u_xrt}\}_{x\in S_i}$。

令 $path(u_i)=\{i_0,i_1,\cdots,i_d\}$,其中 $i_0=root$,i_d 是与用户 u_i 相关联的叶子节点。B 随机选择 $b\in\mathbf{Z}_p$,令 $D=g^{\alpha r}y_{i_d}^{b}$,$E=g^{b}$。最终 B 将密钥 $SK_i=(K',K,L,L',\{K_x\}_{x\in S_i},D,E,\{x_i\}_{i\in path(i_d)})$ 发送给 Adv。SK_i 表示 Adv 第 i 次询问得到的用户密钥。

3)密钥伪造。Adv 将用户密钥 SK^* 提交给 B,令 ε_A 表示 Adv 赢得密钥伪造攻击游戏。即 SK^* 满足用户密钥格式检查的3个条件,并且 $K'\notin\{c_1,c_2,\cdots,c_q\}$。存在以下两种情况:

①假设 ε_A 未发生,则不作处理。

②假设 ε_A 发生了,B 设置一个多项式 $f(y)=\gamma(y)\cdot(y+K')+\gamma-1$,其中 $\gamma(y)=\sum_{i=0}^{q-1}(\gamma_i y^i)$ 且 $\gamma-1\in\mathbf{Z}_p$,由于 $f(y)=\prod_{i=1}^{q}(y+c_i),c_i\in\mathbf{Z}_p,K'\notin\{c_1,c_1,\cdots,c_q\}$,即 $(y+K')$ 不能整除 $f(y)$。假设 $L=g^{rt}(r,t\in\mathbf{Z}_p$ 且未知),可以得到 $L'=g^{art}$。根据 $e(L^{K'}L',\Lambda)=e(L,g^{\alpha})$,得到 $\Lambda=g^{\frac{\alpha}{a+K'}}$,令:

$$\sigma=(\Lambda)^{\alpha^{-1}}=g^{\frac{1}{a+K'}}=g_1^{\frac{f(a)}{a+K'}}=g_1^{\gamma(a)}g_1^{\frac{\gamma-1}{a+K'}}$$

B 计算一个二元组 (c_r,w_r) 如下所示:

$$\begin{cases}c_r=K'\\ w_r=\left(\sigma\cdot\prod_{i=0}^{q-1}A_i^{-\gamma_i}\right)^{\frac{1}{\gamma-1}}=g_1^{\frac{1}{a+K'}}\end{cases}$$

由于 $e(g_1^a\cdot g_1^{c_r},w_r)=e\left(g_1^a\cdot g_1^{K'},g_1^{\frac{1}{a+K'}}\right)=e(g_1,g_1)$,所以 (c_r,w_r) 是 l-SDH 问题的一种解决方式。

以下论证 B 攻破 l-SDH 困难性假设的优势。令 ξ 表示 (c_r,w_r) 是 l-SDH 挑战问题的解决方案,可以通过检查 $e(g_1^a\cdot g_1^{c_r},w_r)=e(g_1,g_1)$ 是否成立来进行验证。当 B 随机选择 (c_r,w_r) 时,ξ 的发生概率可以忽略不计。在 $(Adv\cdot wins\wedge\gcd(\gamma-1,p)=1)$ 的情况下,(c_r,w_r) 满足 $e(g_1^a\cdot g_1^{c_r},w_r)=e(g_1,g_1)$ 的概率为1。当 B 输出 (c_r,w_r) 时,假设 Adv 赢得游戏的概率为 ε。

所以,B 以如下概率赢得了 l-SDH 游戏:

$$\begin{aligned}\Pr[\xi]=&\Pr[\xi|\overline{Adv\cdot wins}]\cdot\Pr[\overline{Adv\cdot wins}]+\\&\Pr[\xi|Adv\cdot wins\wedge\gcd(\gamma-1,p)\neq1]\cdot\\&\Pr[Adv\cdot wins\wedge\gcd(\gamma-1,p)\neq1]+\\&\Pr[\xi|Adv\cdot wins\wedge\gcd(\gamma-1,p)=1]\cdot\\&\Pr[Adv\cdot wins\wedge\gcd(\gamma-1,p)=1]=\\&0+0+1\cdot\Pr[Adv\cdot wins\wedge\gcd(\gamma-1,p)=1]=\\&\Pr[Adv.wins]\cdot\Pr[\gcd(\gamma-1,p)=1]=\varepsilon\end{aligned}$$

证毕。

4.2　IND-CPA 安全性分析

定理2　假设判定性 q-BDHE 困难性假设成立,那么在选择访问策略和选择明文攻击下,不存在多项式时间的攻击者 Adv 能以不可忽略的优势攻破本文的系统($q>2|U|-1$,$|U|$ 是系统中用户个数)。

证明　如果存在一个多项式时间攻击者 Adv 能以优势 ε 攻破本文的系统,那么本文能创建一个挑战者 B 以优势 $\varepsilon/2$ 解决 q-BDHE 问题。选取阶为 p 的乘法循环群 G 和 G_T,G 的生成元为 g。令 $e:G\times G\to G_T$ 为双线性映射。证明过程如下:

1)初始化。Adv 选择一个要挑战的访问策略 $(\boldsymbol{M}^*,\rho^*)$,其中 $\boldsymbol{M}^*$ 是一个 $l^*\times n^*$ 的矩阵,$n^*\leqslant q$。

2)系统建立。B 执行如下操作:

①选择 $\alpha\in\mathbf{Z}_p$ 使得 $e(g,g)^{\alpha}=e(g^d,g^{d^q})\cdot e(g,g)^{\alpha'}$,由此可得 $\alpha=\alpha'+d^{q+1}$。

②对 $x\in[|U|]$,随机选择一个值 $z_x\in\mathbf{Z}_p$。每个组元素 $U_x\in G$ 定义如下。

若存在 $i\in\{1,2,\cdots,l^*\}$ 使得 $\rho^*(i)=x$,令 $U_x=g^{z_x}g^{dM_{i,1}^*}g^{d^2M_{i,2}^*}\cdots g^{d^{n^*}M_{i,n^*}^*}$。

若不存在 $i\in\{1,2,\cdots,l^*\}$ 使得 $\rho^*(i)=x$,令 $U_x=g^{z_x}$。

③随机选取 $a\in\mathbf{Z}_p$,计算 g^a,令 $h=g^d$。

④给定撤销列表 R^*,令 $I_{R^*}=\{i\in path(u)|u\in R^*\}$。每个组元素 $y_i\in G(i=1,2,\cdots,2|U|-1)$ 定义如下:

若 $i\in I_{R^*}$,随机选取 $v_i\in\mathbf{Z}_p$,令 $y_i=g^{d^i}\cdot g^{v_i}=g^{d^i+v_i}$,令 $x_i=d^i+v_i$;否则,令 $y_i=g^{d^q}\cdot g^{v_i}=g^{d^q+v_i}$,令 $x_i=d^q+v_i$。

公共参数如下所示:

$PP=(g,h,e(g,g)^{\alpha},g^a,H,(A_x)_{x\in A},Y)$

3)阶段1。在本阶段,Adv 向 B 询问与一系列与 (u,S) 相关的用户密钥。

情况1　如果 $S\models(\boldsymbol{M}^*,\rho^*)$ 且 $u_i\notin R^*$,则不作处理。

情况2　如果 $S\models(\boldsymbol{M},\rho)$ 或 $u_i\in R^*$,B 随机选取 $r,c\in\mathbf{Z}_p$ 并计算 K',K,L,L',K_x。

$$K'=c$$

$$K=(g^{\alpha'})^{\frac{1/z+r}{a+c}}(g^{d^q})^{\frac{(1/z+r)M_{i,1}^*}{(a+c)M_{i,2}^*}}=g^{\frac{\alpha+zr\alpha}{zc+zc}}h^{rt}$$

$$L=\left[(g^{d^q})^{\frac{1/z+r}{a+c}}\right]^{-1}(g^{d^q})^{\frac{(1/z+r)M_{i,1}^*}{(a+c)M_{i,2}^*}}=g^{rt}$$

$$K_x=[(g^{d^q})^{zx(1+r)}]^{-1}(g^{d^{q-1}})^{zx(1+r)}\cdot\left[\prod_{j=2,3,\cdots,n^*}(g^{d(j+q)M_{i,j}^*})\right]^{-(1+r)}\cdot\prod_{j=1,\cdots,n^*,j\neq2}\left(g^{d(j+q-1)M_{i,j}^*}\right)^{\frac{(1+r)M_{i,1}^*}{M_{i,2}^*}}=U_x^{(a+c)rt}$$

$path(u)=\{i_0,i_1,\cdots,i_d\}$,其中 $i_0=root$,i_d 是与用户 u 相关联的叶子节点。由于 $u\in R^*$,可以得到 $i_k\in I_{R^*}$ 和 $x_{i_k}=d^{i_k}+v_{i_k},k=0,1,\cdots,d$,因此 $y_{i_d}=g^{d^{i_d}+v_{i_d}}$。$B$ 选取 $b'\in\mathbf{Z}_p$,并计算 D、E。

$$D=g^{\alpha'r}\cdot(g^{d^{i_d}})^{b'}\cdot g^{v_{i_d}b'}\cdot\left(g^{d^{q+1-i_d}}\right)^{-rv_{i_d}}=g^{\alpha r}y_{i_d}^{b}$$

$$E=\frac{g^{b'}}{\left(g^{d^{q+1}-i_d}\right)^{r}}=g^{b}$$

情况3　如果 $S\not\models(\boldsymbol{M}^*,\rho^*)$ 且 $u_i\in R^*$,B 进行如下运算:

①令 $I=\{i:\rho^*(i)\in S\}\subseteq\{1,2,\cdots,l\}$,$\omega_1=-1$,存在向量 $\boldsymbol{\omega}=(\omega_1,\omega_2,\cdots,\omega_{n^*})\in\mathbf{Z}_p^{n^*}$ 使得 $\boldsymbol{M}_i^*\cdot\boldsymbol{\omega}=0$。

②随机选取 $r,c\in\mathbf{Z}_p$,令 $K'=c$。

③随机选取 $\beta\in\mathbf{Z}_p$,令:

$$t=\frac{1+r}{r(a+c)}(\beta+\omega_1d^q+\omega_2d^{q-1}+\ldots+\omega_{n^*}d^{q-n^*+1})$$

④计算 L,L',K。

$$L = g^{\beta(1+r)/(a+c)}\left[\prod_{i=1,2,\cdots,n^*}\left(g^{a^{q+1-i}}\right)^{\omega_i}\right]^{(1+r)/(a+c)} = g^{rt}$$

$$L' = g^{\alpha\beta(1+r)/(a+c)}\left[\prod_{i=1,2,\cdots,n^*}\left(g^{a^{q+1-i}}\right)^{\omega_i}\right]^{a(1+r)/(a+c)} = g^{art}$$

$$K = \left[g^{\alpha'}g^{d\beta}\prod_{i=2,3,\cdots,n^*}\left(g^{a^{q+2-i}}\right)^{\omega_i}\right]^{(1/z+r)/(a+c)} = g^{(\alpha+2\alpha r)/(z a+z c)}h^{rt}$$

⑤对 $\forall x \in S$，计算 K_x。若不存在 i 使得 $\rho^*(i) = x$，令 $K_x = L^{(a+c)z_x}$；否则，存在 i，使得 $\rho^*(i) = x$，设置 K_x 如下：

$$K_x = L^{(a+c)z_x}\left[\prod_{j=1,2,\cdots,n^*}\left(g^{d^j\beta}\prod_{k=1,2,\cdots,n^*,k\neq j}\left(g^{d^{q+1+j-k}}\right)^{\omega_k}\right)M_{i,j}^*\right]^{(1+r)}$$

⑥按照情况 2 的步骤计算 D、E。

情况 4　如果 $S \models (\boldsymbol{M}^*, \rho^*)$ 且 $u_i \notin R^*$，B 按照情况 3 的步骤计算 K', K, L, L', K_x，假设 $path(u) = \{i_0, i_1, \cdots, i_d\}$，其中 $i_0 = root$，i_d 是与用户 u 相关联的叶子节点。由于 $u \notin R^*$，则 $i_k \notin I_{R^*}$ 和 $x_{i_k} = d^q + v_i, k = 0, 1, \cdots, d$。因此，$y_{i_d} = g^{d^q + v_{i_d}}$。$B$ 随机选取 $b' \in \mathbf{Z}_p$ 并计算 D、E。

$$D = g^{\alpha' r}\cdot(g^{d^q})^{b'}\cdot g^{v_{i_d}b'}\cdot(g^d)^{-rv_{i_d}} = g^{\alpha r}y_{i_d}^b$$

$$E = \frac{g^{b'}}{(g^d)^r} = g^b$$

4）挑战。Adv 向 B 提交 2 个等长的消息 m_0, m_1，B 做如下运算：

①B 掷一枚均匀的硬币 $\eta \in \{0, 1\}$ 并计算 C_η, C_0, C_0'：

$C_\eta = m_\eta \cdot W \cdot e(g^s, g^{\alpha'})$

$C_0 = g^s$

$C_0' = (g^a)^s$

②随机选取 $r_2', r_3', \cdots, r_{n^*}' \in \mathbf{Z}_p$，并计算 v。

$v = (s, sd + r_2', sd^2 + r_3', \cdots, sd^{n^*-1} + r_{n^*}') \in \mathbf{Z}_p^{n^*}$。

③计算 $C_i = \prod_{j=2,3,\cdots,n^*}(g^d)^{M_{i,j}^* r_j'}\cdot(g^s)^{-x\rho^*(i)}, i = 1, 2, \cdots, l$。

④对 $\forall j \in cover(R^*)$，定义 $path(j) = \{i_0, i_1, \cdots, i_{depth(j)}\}$，$i_0 = root$，$i_{depth(j)} = j$。由于 $\forall j \in cover(R^*)$，可得 $x_j = a^q + v_{i_k}$，$y_j = g^{a^q + v_j}$。令 $T_j = (g^s)^{x_j} = y_j^s$。

最终，B 输出密文 CT 并将它发送给 Adv。

$CT = (C_\eta, C_0, C_0', \{C_i\}_{i\in[l]}, \{W_j\}_{j\in cover(R)})$。

5）阶段 2。阶段 2 重复阶段 1 的步骤。

6）猜测。Adv 输出对 η 的猜测 η'，若 $\eta' = \eta$，B 输出对 v 的猜测 $v' = 1$；否则，B 输出对 v 的猜测 $v' = 1$。

①当 $v = 0$ 时，$Z = e(g, g)^{d^{q+1}s}$ 且 Adv 获取到了一个合法的密文。假定 Adv 的优势 $\varepsilon = \Pr[\eta = \eta' | v = 0] - \frac{1}{2}$。由于 $\Pr[\eta = \eta' | v = 0] = \Pr[v = v' | v = 0]$，因此 B 赢得游戏的概率是 $\Pr[v = v' | v = 0] = \varepsilon + \frac{1}{2}$。

②当 $v = 1$ 时，Z 是 G_T 中的随机元素，因此，Adv 无法获得 η 的任何信息。在此情况下，Adv 没有任何优势，所以 $\Pr[\eta \neq \eta' | v = 1] = \frac{1}{2}$。由于 $\Pr[\eta \neq \eta' | v = 1] = \Pr[v = v' | v = 1]$，因此 B 赢得游戏的概率是 $\Pr[v = v' | v = 1] = \frac{1}{2}$。

最终，B 解决 q-BDHE 困难性假设的总体优势为：

$$\Pr[v = v'] = \Pr[v = v' | v = 0]\cdot\Pr[v = 0] + \Pr[v = v' | v = 1]\cdot\Pr[v = 1] - \frac{1}{2} = \left(\varepsilon + \frac{1}{2}\right)\times\frac{1}{2} + \frac{1}{2}\times\frac{1}{2} - \frac{1}{2} = \frac{1}{2}\varepsilon$$

证毕。

5　方案对比

对本文方案和文献[22]方案、文献[29]方案、文献[30]方案、文献[31]方案、文献[32]方案的功能和效率进行了评估和比较，由于此 5 个方案与本文方案在系统功能上有部分相似点，故选择此 5 个方案进行对比。具体对比情况如表 2~3 所示。

在表 2 中，进行了功能的对比，其中文献[22]方案提出了一个可追踪的属性基加密方案。然而，该方案仅支持密钥策略属性基加密，且未实现用户撤销与外包解密的功能。文献[29]方案虽然支持用户的撤销，与本文方案相比，文献[29]方案仅通过密钥更新来实现撤销，发生撤销时，需要更新所有未被撤销的用户的密钥，这增加了系统的计算开销与通信开销。文献[30]方案实现了支持外包解密的属性基加密方案，但没有实现用户追踪，当用户泄露自己的密钥给第三方时，无法有效追踪到恶意的用户。文献[29]方案与文献[31]方案实现了可追踪可撤销的属性基加密方案，与本文方案相比，文献[29]方案与文献[31]的方案不支持外包解密。文献[32]方案虽然也实现了云雾计算下的可撤销属性基加密方案，但是不支持恶意用户追踪，且仅可以抵抗选择明文攻击。本文方案可以抵抗选择明文攻击和密钥伪造攻击。考虑到本文应用场景中，车辆作为一个边缘设备，并不具备强大的计算能力。因此，本文方案在保证数据机密性的前提下将部分解密计算外包给计算能力较强的雾节点，能够有效减轻车辆的计算开销。

表 2　不同方案系统功能对比

Tab. 2　System function comparison of different schemes

方案	用户撤销	可追踪	选择模型安全	外包解密	支持雾计算
文献[22]方案	×	√	√	×	×
文献[29]方案	√	√	√	×	×
文献[30]方案	√	×	√	√	×
文献[31]方案	√	√	√	×	×
文献[32]方案	√	×	√	√	√
本文方案	√	√	√	√	√

表3　不同方案系统效率对比

Tab. 3　System efficiency comparison of different schemes

方案	密钥生成	加密	外包解密	用户解密	追踪
文献[22]方案	$(2+2s)E+sM$	$(2+3l)E+2M$	—	$(1+2n)P+nE+(2+2n)M$	$(5+3s)P+(2+s)E+(3+2s)M$
文献[29]方案	$(1+2s)E+sM$	$(2+3l)E+2M$	—	$(1+2n)P+nE+(2+2n)M$	$(5+3s)P+(2+s)E+(3+2s)M$
文献[30]方案	$(3+2s)E+(1+s)M$	$(5+6l)E+(4l+1)M$	$(3+4n)P+3nE+(3+2n)M$	$E+M$	—
文献[31]方案	$(4+4s)E+M$	$(3+4l+lr)E+(l+1)M$	—	$(1+4n)P+(3+n)E+(3+3n)M$	$(4+2s)P+4E+3sM$
文献[32]方案	$(4+4s)E+(2+5s)M$	$(6+4l)E+(4l+1)M$	$(2+4n)P+2nE+(2+3n)M$	$P+2M$	—
本文方案	$(6+s)E+(1+s)M$	$(3+2l+r)E+(l+1)M$	$(2+4n)P+2nE+(3+2n)M$	$E+M$	$(2+2s)P+(1+s)E+sM$

表3显示了本文方案与其他方案在性能方面的比较。方便起见,令E表示G、G_T中的指数运算;P表示双线性配对操作;M表示G、G_T中的乘法运算;l表示访问策略中属性的数目;r表示$cover(R)$的长度;s表示用户属性的数量;n表示解密密钥中满足访问策略的属性数。在密钥生成和加密算法中,本文方案的指数运算和乘法运算的复杂度比其他方案低,因此效率更高。在解密算法中,由于文献[22]方案、文献[29]方案和文献[31]方案不支持外包解密,所以用户解密的计算开销比本文方案要大得多,文献[30]方案的用户解密计算开销与本文方案持平,皆为一个指数运算与一个乘法运算,文献[32]方案的用户解密由一个配对运算与两个乘法运算组成,故本文的用户解密计算开销较小。与文献[22]方案、文献[29]方案和文献[31]方案相比,由于本文方案在跟踪方面具有更少的乘法运算与指数运算,因此本文方案在追踪方面的效率更高。

6　结语

为了满足资源受限的边缘设备的数据访问需求,同时保证安全的数据共享,本文将云雾计算与密文策略属性基加密相结合,设计了一个安全的云雾设备数据共享方案,并实现了细粒度的访问控制。在本文方案中,车辆直接与本地雾节点进行通信,并将解密任务外包给雾节点执行,从而有效降低了用户的计算开销。由于雾节点只拥有外包解密密钥,因此无法获取明文,进而能够保证用户的隐私安全。本文方案还支持恶意用户的追踪与撤销,在解密密钥泄露的情况下,系统能够根据密钥追踪到用户的身份,进而将他加入撤销列表,使其失去数据访问权限。由于使用了直接撤销的方法,所以相较于间接撤销,本文方案能有效降低通信开销。此外,本文方案在选择明文攻击和密钥伪造攻击下被证明是安全的。由于本文的方案只能实现白盒可追踪性,不如黑盒可追踪性强。因此,我们的未来工作是构建具有黑盒可追踪性的基于密文策略的属性基加密方案。

参考文献 (References)

[1] WOOD T, RAMAKRISHNAN K, SHENOY P, et al. CloudNet: dynamic pooling of cloud resources by live WAN migration of virtual machines [J]. IEEE/ACM Transactions on Networking, 2015, 23(5): 1568-1583.

[2] YI S, QIN Z, LI Q. Security and privacy issues of fog computing: a survey [C]// Proceedings of the 2015 International Conference on Wireless Algorithms, Systems, and Applications, LNCS 9204. Cham: Springer, 2015: 685-695.

[3] Statista. Forecast of fog computing market revenue worldwide from 2018 to 2022 [EB/OL]. [2020-08-12]. https://www.statista.com/statistics/830485/world-fog-computing- revenue-by-vertical/.

[4] STOJMENOVIC I, WEN S. The fog computing paradigm: scenarios and security issues [C]// Proceedings of the 2014 Federated Conference on Computer Science and Information Systems. Piscataway: IEEE, 2014: 1-8.

[5] ROMAN R, LOPEZ J, MAMBO M. Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges [J]. Future Generation Computer Systems, 2018, 78(Pt 2): 680-698.

[6] STOJMENOVIC I, WEN S, HUANG X, et al. An overview of fog computing and its security issues [J]. Concurrency and Computation: Practice and Experience, 2016, 28(10): 2991-3005.

[7] HUANG X, XIANG Y, BERTINO E, et al. Robust multi-factor authentication for fragile communications [J]. IEEE Transactions on Dependable and Secure Computing, 2014, 11(6): 568-581.

[8] CHOO K K R, DOMINGO-FERRER J, ZHANG L. Cloud cryptography: theory, practice and future research directions [J]. Future Generation Computer Systems, 2016, 62: 51-53.

[9] SAHAI A, WATERS B. Fuzzy identity-based encryption [C]// Proceedings of the 2005 Annual International Conference on the Theory and Applications of Cryptographic Techniques, LNCS 3494. Berlin: Springer, 2005: 457-473.

[10] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data [C]// Proceedings of the 2006 13th ACM Conference on Computer and Communications Security. New York: ACM, 2006: 89-98.

[11] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption [C]// Proceedings of the 2007 IEEE Symposium on Security and Privacy. Piscataway: IEEE, 2007: 321-334.

[12] LIU Z, CAO Z, WONG D S. White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures [J]. IEEE Transactions on Information Forensics and Security, 2013, 8(1): 76-88.

[13] NING J, CAO Z, DONG X, et al. Large universe ciphertext-policy attribute-based encryption with white-box traceability [C]// Proceedings of the 2014 European Symposium on Research in Computer Security, LNCS 8713. Cham: Springer, 2014: 55-72.

[14] NING J, DONG X, CAO Z, et al. White-box traceable ciphertext-policy attribute-based encryption supporting flexible attributes [J]. IEEE Transactions on Information Forensics and Security, 2015, 10(6): 1274-1288.

[15] YANG K, JIA X, REN K. Attribute-based fine-grained access control with efficient revocation in cloud storage systems [C]// Proceedings of the 2013 8th ACM SIGSAC Symposium on

Information, Computer and Communications Security. New York: ACM, 2013: 523-528.

[16] 高嘉昕,孙加萌,秦静. 支持属性撤销的可追踪外包属性加密方案[J]. 计算机研究与发展,2019,56(10):2160-2169. (GAO J X, SUN J M, QIN J. Traceable outsourcing attribute-based encryption with attribute revocation [J]. Journal of Computer Research and Development, 2019, 56(10): 2160-2169.)

[17] 王鹏翩,冯登国,张立武. 一种支持完全细粒度属性撤销的CP-ABE方案[J]. 软件学报,2012,23(10):2805-2816. (WANG P P, FENG D G, ZHANG L W. CP-ABE scheme supporting fully fine-grained attribute revocation [J]. Journal of Software, 2012, 23(10): 2805-2816.)

[18] 明洋,何宝康. 支持属性撤销的可验证外包的多授权属性加密方案[J]. 计算机应用,2019,39(12):3556-3562. (MING Y, HE B K. Attribute revocation and verifiable outsourcing supported multi-authority attribute-based encryption scheme [J]. Journal of Computer Applications, 2019, 39(12): 3556-3562.)

[19] YU S, WANG C, REN K, et al. Attribute based data sharing with attribute revocation [C]// Proceedings of the 2010 5th ACM Symposium on Information, Computer and Communications Security. New York: ACM, 2010: 261-270.

[20] LI Y, ZHU J, WANG X, et al. Optimized ciphertext-policy attribute-based encryption with efficient revocation [J]. International Journal of Security and Its Applications, 2013, 7(6): 385-394.

[21] LI Q, XIONG H, ZHANG F. Broadcast revocation scheme in composite-order bilinear group and its application to attribute-based encryption [J]. International Journal of Security and Networks, 2013, 8(1): 1-12.

[22] SHI Y, ZHENG Q, LIU J, et al. Directly revocable key-policy attribute-based encryption with verifiable ciphertext delegation [J]. Information Sciences, 2015, 295: 221-231.

[23] 林娟,薛庆水,曹珍富. 基于代理的即时属性撤销KP-ABE方案[J]. 计算机工程,2014,40(10):20-24. (LING J, XUE Q S, CAO Z F. Proxy-based immediate attribute revocation KP-ABE scheme [J]. Computer Engineering, 2014, 40(10): 20-24.)

[24] XU S, NING J, LI Y, et al. Match in my way: fine-grained bilateral access control for secure cloud-fog computing [J]. IEEE Transaction on Dependable and Secure Computing, 2020 (Early Access): 1-15.

[25] LIU Z, DUAN S, ZHOU P, et al. Traceable-then-revocable ciphertext-policy attribute-based encryption scheme [J]. Future Generation Computer Systems, 2019, 93: 903-913.

[26] XU S, YANG G, MU Y, et al. Secure fine-grained access control and data sharing for dynamic groups in the cloud [J] IEEE Transactions on Information Forensics and Security, 2018, 13(8): 2101-2113.

[27] WATERS B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization [C]// Proceedings of the 2011 International Workshop on Public Key Cryptography, LNCS 6571. Berlin: Springer, 2011: 53-70.

[28] JIANG Y, SUSILO W, MU Y, et al. Ciphertext-policy attribute-based encryption against key-delegation abuse in fog computing [J]. Future Generation Computer Systems, 2018, 78(Pt2): 720-729.

[29] HOANG V H, LEHTIHET E, GHAMRI-DOUDANE Y. Forward-secure data outsourcing based on revocable attribute-based encryption [C]// Proceedings of the 2019 15th International Wireless Communications and Mobile Computing Conference. Piscataway: IEEE, 2019: 1839-1846.

[30] ZHANG Y, ZHENG D, DENG R H. Security and privacy in smart health: efficient policy-hiding attribute-based access control [J]. IEEE Internet of Things Journal, 2018, 5(3): 2130-2145.

[31] WANG S, GUO K, ZHANG Y. Traceable ciphertext-policy attribute-based encryption scheme with attribute level user revocation for cloud storage [J]. PLoS ONE, 2018, 13(9): Article No. e0203225.

[32] LI L, WANG Z, LI N. Efficient attribute-based encryption outsourcing scheme with user and attribute revocation for fog-enabled IoT [J]. IEEE Access, 2020, 8: 176738-176749.

This work is partially supported by the National Natural Science Foundation of China (61472343).

CHEN Jiahao, born in 1997, M. S. candidate. His research interests include cryptography, internet of things security, encryption algorithms and protocols.

YIN Xinchun, born in 1962, Ph. D., professor. His research interests include cryptography, software quality assurance, high-performance computing.