车载社交网中基于密文属性加密的车队车辆数据共享方案*

杨邵成　蔡英　范艳芳

（北京信息科技大学，北京 100101）

【摘要】针对车载社交网（VSN）中车队车辆数据共享过程中存在的隐私泄露问题，提出一种基于密文属性的加密方案。利用基于属性的加密技术，保证仅授权的车辆可访问数据，防止车队车辆数据共享过程中发生隐私泄露；针对车队车辆数据共享时生成访问策略时间开销大、数据共享效率低的问题，通过构造访问树实现对访问策略的设计，利用路侧单元将访问树转化为访问矩阵，实现访问策略的快速生成。仿真分析结果表明，该方案能够实现对VSN中车队车辆的数据安全共享，所构建的访问策略生成方案能够有效降低车辆的计算开销。

主题词：车载社交网　隐私保护　密文属性加密　访问树　路侧单元

中图分类号：TP309.7　　**文献标志码：**A　　**DOI:** 10.19620/j.cnki.1000-3703.20230685

Ciphertext-Policy Attribute-Based Encryption Scheme for Fleet Vehicle Data Sharing in Vehicular Social Network

Yang Shaocheng, Cai Ying, Fan Yanfang

（Beijing Information Science and Technology University, Beijing 100101）

【Abstract】In response to the privacy leakage issues in the data sharing process among the fleet vehicles in Vehicular Social Network (VSN), this paper proposed a ciphertext policy attribute-based encryption scheme. Firstly, utilizing attribute-based encryption techniques, the scheme ensures that only authorized vehicles can access the data, thereby preventing privacy leakage during the fleet vehicle data sharing process. To address the issue of high time complexity in generating access policies during fleet vehicle data sharing, and low data sharing efficiency, an access tree was constructed to design the access policies. The access tree was then transformed into an access matrix using roadside units, enabling fast generation of access policies. Experimental analysis shows that this scheme achieves secure data sharing among fleet vehicles in VSNs, the proposed access policy generation approach effectively reduces the computational overhead for vehicles.

Key words: Vehicular Social Network (VSN), Privacy preserving, Ciphertext-policy attribute-based encryption, Access tree, Road Side Unit (RSU)

【引用格式】杨邵成, 蔡英, 范艳芳. 车载社交网中基于密文属性加密的车队车辆数据共享方案[J]. 汽车技术, 2024(8): 14-21.

YANG S C, CAI Y, FAN Y F. Ciphertext-Policy Attribute-Based Encryption Scheme for Fleet Vehicle Data Sharing in Vehicular Social Network[J]. Automobile Technology, 2024(8): 14-21.

1　前言

车载社交网（Vehicular Social Network，VSN）是一种特殊的自组织网络[1]，可支持长途运输车队在高速行驶过程中通过数据共享实现车队协作、路线规划和紧急预警等功能。然而，数据共享将泄露诸如行驶路线、驾驶员信息等敏感数据，威胁车辆用户的隐私安全[2]。

在VSN数据共享时隐私泄露问题的解决方法中，基于密文的属性加密（Ciphertext-Policy Attribute Based Encryption，CP-ABE）[3]是目前的研究热点。车队车辆利用CP-ABE将数据密文嵌入访问策略，通过自定义访问策略，实现一对多加密，可在行驶过程中与多个车辆共享数据。然而，生成访问策略的时间与计算开销随属性数量线性增加，车队车辆生成复杂的访问策略将耗费大

*基金项目：国家自然科学基金项目（61672106）；北京市自然科学基金—海淀原始创新联合基金项目（L192023）。

量的时间与计算资源，这影响了CP-ABE在VSN中的广泛应用。

许多学者对VSN中CP-ABE方案展开了研究。Sahai[4]首先提出了模糊身份加密策略，可在具有特定属性集的用户间安全共享数据。Bethencourt等[5]提出了第一个CP-ABE方案，该方案可自定义访问策略，实现访问控制。Zhang等[6]提出了基于CP-ABE和区块链的访问控制方案，以解决VSN中的隐私泄露问题。Cui等[7]提出了一种可隐藏访问结构中用户属性的CP-ABE方案。Yang等[8]利用布隆过滤器过滤用户属性，以降低计算开销。Li等[9]提出了可根据属性值灵活设计访问结构的CP-ABE方案。Xia等[10]利用云服务器对密文进行半解密，以降低用户的计算开销。Kamalakanta等[11]设计了支持追溯数据来源且具有多权限的CP-ABE方案，可对访问策略进行更新和外包解密。Fan等[12]提出了利用区块链记录访问策略的CP-ABE方案。Zhong等[13]提出了一种利用线性秘密共享生成访问策略，并可撤销用户权限的CP-ABE方案。Pu[14]、Shi[15]和Sun等[16]提出了基于区块链的隐私保护方案，确保VSN中数据来源可靠，防止攻击者篡改或伪造数据。

现有研究实现了VSN中的隐私保护，并解决了数据篡改的问题，但还无法解决VSN车队车辆生成复杂访问策略时，计算开销随属性数量线性增加的缺陷。本文利用路侧单元运行外包加密算法，以降低车队车辆计算密文时的计算开销，并利用访问树设计访问策略，由路侧单元将访问树转化为线性访问策略，以降低车队车辆生成访问策略的计算开销。

2 相关理论

2.1 双线性映射

设G_0、G_1和G_T是阶数为q的循环乘法群，并且q为大素数，则存在双线性映射[17]$e:G_0\times G_1\to G_T$满足以下条件：

a. 双线性。对于$P\in G_0$、$Q\in G_1$、$i,j\in Z_q$，有$e(P^i,Q^j)=e(P,Q)^{ij}$，其中Z_q为有限域。

b. 非退化性。对于$P\in G_0$、$Q\in G_1$、$i,j\in Z_q$，有$e(P,Q)\neq 1$。

c. 可计算性。对于任意的$P\in G_0$、$Q\in G_1$，存在$e(P,Q)$可计算。

2.2 访问结构

在属性域U内建立访问结构Γ[18]，非空属性集合Γ称为授权集合。若存在任何集合D和E，如果$D\in\Gamma$且$D\subseteq E$，则称$E\in\Gamma$，访问结构Γ被称为单调的。

设$U=\{A_1,A_2,\cdots,A_n\}$为属性集，设集合$A_i=\{a_{i,1},a_{i,2},\cdots,a_{i,m_i}\}$，$A_i\in U$。当$A_i$中元素的数量为$m_i$时，构建$L=\{l_1,\cdots,l_n\}$，其中$l_i\in A_i$，$L$为用户属性列表，则访问结构表示为$\Gamma=\{\Gamma_1,\cdots,\Gamma_q\}$，其中$\Gamma_j\in A_j$。

当$l_i=\Gamma_j$且$i,j=1,2,\cdots$时，称用户属性列表L满足访问结构Γ的要求。访问结构也称为访问策略。

2.3 线性秘密共享

在p为素数的有限域Z_p中，满足如下条件的属性集，称为线性秘密共享方案（Linear Secret Sharing Scheme，LSSS），且属性集在属性域U上是线性的：

a. 设定Z_p上的每个向量由属性集中的秘密共享值组成。

b. 全属性域U中的访问策略均有属性映射与共享矩阵$\boldsymbol{M}_{l\times n}$，通过函数$\rho$将$\boldsymbol{M}$中每一行映射到$U$中的属性。对于列向量$\boldsymbol{Z}=[s,z_1,\cdots,z_n]$，其中的元素$z_1,\cdots,z_n$从$Z_p$中随机选取，$s$为秘密共享值，则在访问策略$(\boldsymbol{M},\rho)$中，$\boldsymbol{MZ}$是由$s$关于线性秘密共享方案的$l$个分享份额构成的向量，且$(\boldsymbol{M},\boldsymbol{Z})_j$，$j=1,2,\cdots,l$是映射函数$\rho(j)$分配给对应属性的份额。

设属性集合S为访问策略$(\boldsymbol{M},\rho)$的授权集合，I为矩阵$\boldsymbol{M}$对应行数的集合，即$I=\{i|\rho(i)\in S\cap i\in\{l\}\}$。若存在常数$\{w_i\in Z_p\}_{i\in I}$和秘密值$s$可通过$\lambda_i$进行分享，且$\{\lambda_i\in Z_p\}_{i\in I}$，则可以通过$\sum_{i\in I}w_i\lambda_i=s$恢复$s$，其中$\lambda_i$为对秘密值$s$有效的共享份额，$w_i$为一组用于恢复秘密共享值$s$的常数，满足$\sum_{i\in I}w_i\boldsymbol{M}_i=(1,0,\cdots,0)$，$\boldsymbol{M}_i$为矩阵$\boldsymbol{M}$的第$i$行。

2.4 访问树

访问树（Access Tree）是一种基于层次结构的访问控制模型，它将对象和主体组织成树形结构，并为每个节点分配访问权限。在访问树中，子节点继承父节点的权限，因此可以实现灵活的权限控制。

设T为由节点和边组成的访问树，其中非叶子节点表示门限，由子节点和阈值构成。设节点x有数量为n_x的子节点，阈值为k_x，则$0\leqslant k_x\leqslant n_x$。当$k_x=1$时，该节点表示或门；当$k_x=n_x$时，该节点表示与门。每个叶子节点可以表示一个属性值，且其阈值为$k_x=1$。

定义如下函数来操作访问树：以$p_{\text{arent}}(x)$代表节点x的父节点；对于叶子节点x，$att(x)$表示与x相关的属性值。对访问树T的子节点进行编号，定义函数$index(x)$返回节点x的编号，其中节点x的子节点的编号是1。

满足访问树是指，给定一个访问树T和一个属性集合A^u，如果A^u符合以T中的r为根节点的子树T_r中所有门限节点的阈值要求，则称A^u满足访问树T_r，记为$T_r(A^u)=1$。具体地：对于非叶子节点x，递归计算所有子节点的$T_x(A^u)$，至少k_x个子节点返回1时，$T_x(A^u)$返回1；对于叶子节点，当且仅当其对应的属性在$att(x)\in A^u$中出现时，返回1。

3 本文方案

3.1 系统模型

本方案的系统模型如图1所示，其中包括可信机构（Trusted Authority，TA）、数据拥有者（Data Owner，DO）、数据访问者（Data Visitor，DV）、路侧单元（Road Side Unit，RSU）和云服务器（Cloud Server）6类实体。

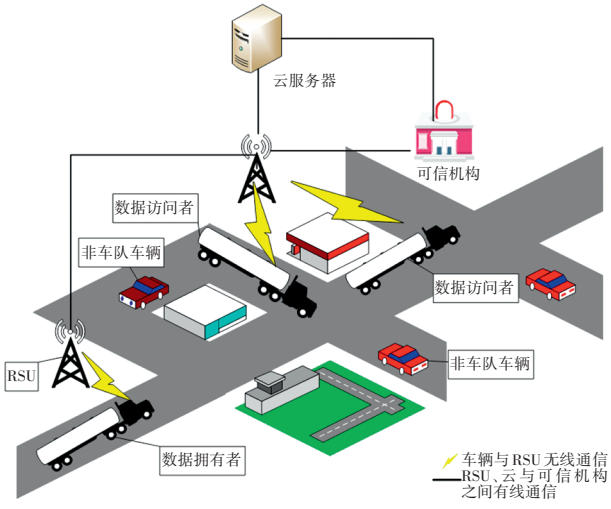

图1 系统模型

其中：TA为车队车辆注册身份生成用户属性集，进行系统初始化，生成系统参数、主密钥和私钥；DO为车队中数据共享的车辆，可设置访问策略并加密数据上传至云服务器；DV为车队中需要获取数据的车辆，通过向云服务器请求数据并验证访问策略得到数据；RSU拥有更加强大的计算和存储资源，作为VSN中间通信节点，在本文方案中其为车队车辆提供外包加密，并将访问树转化为访问矩阵；CS存储和管理数据密文，对数据请求者的请求进行验证。

在数据共享的过程中，假定云服务器与RSU不会合谋。

3.2 基于密文属性加密的车队车辆数据共享方案

本文方案适用于VSN中车队车辆的安全数据共享，由于车队车辆在长途行驶过程中需要进行路线规划与运输任务分配，利用CP-ABE加密密文，不仅能防止车辆的隐私数据泄露，还可以利用其支持自定义访问策略的特点实现细粒度访问控制，满足车队车辆复杂的数据共享需求。然而，计算密文与访问策略需要大量的幂指运算，为了减少资源有限的车队车辆的计算量，利用路侧单元运行外包加密算法，以降低车队车辆计算密文时的计算开销。同时，利用访问树易构造与可读性强的优点生成访问策略，由路侧单元将访问树转化为线性访问策略，以减轻车队车辆生成访问策略的计算开销。

数据共享的流程如图2所示。首先在初始化过程中由TA为车辆生成属性和唯一的身份，并生成方案加密所需的各项参数。DO通过外包加密获得RSU加密得到的密文，并将密文上传至CS，以便于数据共享。DV向CS发送数据请求，当DV属性满足访问策略时，将密文解密得到数据。

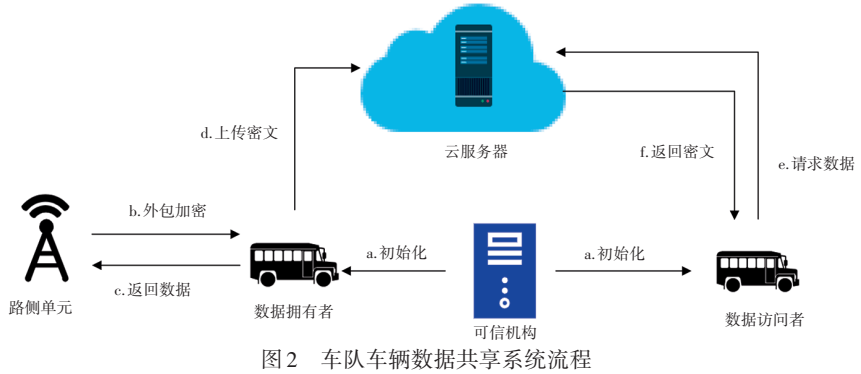

图2 车队车辆数据共享系统流程

3.2.1 初始化算法

$Setup(U)\rightarrow<PK,MSK>$：输入系统属性空间$U$，经过TA的计算最终获得加密数据和生成私钥系统的公钥PK和主密钥MSK。具体过程为：选择2个乘法循环群G和G_T，其阶数均为p，且p为大素数，设双线性映射$e:G\times G\rightarrow G_T$，$g\in G$为群$G$的生成元；随机取一组元素$h_1,\cdots,h_U\in G$，以该组元素表示属性空间$U$中的属性，随机选取参数$\alpha$和$a$，计算得到主密钥$MSK=g^{\alpha}$与公钥$PK$，公钥表示为$PK=[p,G,G_T,e(g,g)^{\alpha},g,g^{a},h_1,\cdots,h_U]$。

3.2.2 密钥生成算法

$KeyGen(PK,MSK,S)\rightarrow<SK>$：在该算法中输入参数$PK$、$MSK$和车队车辆的属性集合$S$，得到私钥$SK$，首先选择对应每个车队车辆用户的唯一随机数$t\in Z_p$，设$x\in S$，$K_x$为在属性空间$U$内的属性参数，$h_x$为在$S$范围内生成的密钥参数，结合公钥参数构造私钥$SK=[S,K=g^{at}g^{a},L=g^{t},\forall x\in S,K_x=h_x^{t}]$。

3.2.3 外包加密算法

$OutEncrypt(PK,T)\rightarrow<CT_{OUT}>$：由RSU运行外包加密

算法，由系统公钥 PK 和访问树 T 输出嵌入访问策略 $(\boldsymbol{M},\rho)$ 的密文 CT_{OUT}。设置 $\boldsymbol{M}$ 为 $l\times n$ 规模的矩阵，在RSU中根据定理4将访问树 T 转换为矩阵。随机选择一组元素 $v=\{0,s_2,\cdots,s_n\}\in Z_p^n$，设0为秘密共享值。以上述参数计算得出第 i 组的秘密值集合 $\lambda_i'=\boldsymbol{M}_i v$。对 $\boldsymbol{M}$ 的全部行向量选择随机数 $r_1,\cdots,r_l\in Z_p$，计算 $(\boldsymbol{M},\rho)$ 为LSSS的访问策略，密文参数 C_l、D_l，以减少加密算法中密文的计算量，外包密文 CT_{OUT} 为：

$$CT_{\mathrm{OUT}}=\left[\left(C_1'=g^{\alpha\lambda_1'}h_{\rho(1)}^{-r_1},D_1=g^{r_1}\right),\cdots,\left(C_l'=g^{\alpha\lambda_l'}h_{\rho(l)}^{-r_l},D_l=g^{r_l}\right)\right] \tag{1}$$

式中：C_l' 为在外包算法中加密的密文参数。

3.2.4　加密算法

Encrypt$(PK,(\boldsymbol{M},\rho),m)\rightarrow<CT>$：输入系统公钥 PK、访问策略 $(\boldsymbol{M},\rho)$ 和数据明文 m，输出数据密文 CT。

RSU按照定理4将访问树 T 转变为访问矩阵 $\boldsymbol{M}$，生成线性访问策略 $(\boldsymbol{M},\rho)$。调用 *OutEncrypt* 算法，将得出的 CT_{OUT} 密文送至数据拥有者。车队车辆得到外包密文，继续运行 *Encrypt* 算法，随机选择 $s\in Z_p$ 为秘密共享数，计算 s 的参数 C'，令 $\lambda_i=s+\lambda_i'$，$C_i=g^{\alpha s}C_i'=g^{\alpha\lambda_i}h_{\rho(i)}^{-r_i}$，经计算得出密文为：

$$CT=\left[(\boldsymbol{M},\rho),C=m\cdot e(g,g)^{\alpha s},C'=g^s,\left(C_1=g^{\alpha\lambda_1}h_{\rho(1)}^{-r_1},D_1=g^{r_1}\right),\cdots,\left(C_l=g^{\alpha\lambda_l}h_{\rho(l)}^{-r_l},D_l=g^{r_l}\right)\right] \tag{2}$$

3.2.5　解密算法

Decrypt$(CT,SK)\rightarrow<W>$：输入数据密文 CT、用户私钥 SK，输出数据明文 W。

当数据接收用的户属性集合 S 满足密文的访问策略，得到数据密文后，将解密属性集合表示为 $I\subset\{1,2,\cdots,l\}$ 且 $I=\{i:\rho(i)\in S\}$，随后计算一组常数 $\{w_i\in Z_p\}_{i\in I}$ 使得 $\sum_{i\in I}w_i\lambda_i=s$，其中，$\lambda_i$ 为解密属性在加密时的秘密共享数，K 为用户私钥中包含的参数。进行如下计算：

$$\frac{e(C',K)}{\prod_{i\in I}\left\{\left[e(C_i,L)e(D,K_{\rho(i)})\right]^{w_i}\right\}}=\frac{e(g,g)^{\alpha s}e(g,g)^{\alpha s t}}{\prod_{i\in I}e(g,g)^{t\alpha\lambda_i w_i}}=e(g,g)^{\alpha s} \tag{3}$$

最后得到 W：

$$W=\frac{C}{e(g,g)^{\alpha s}}=\frac{W\cdot e(g,g)^{\alpha s}}{e(g,g)^{\alpha s}} \tag{4}$$

3.3　构造访问树

本节主要将设计的访问树转化为对应的线性访问结构。

定理1：访问树中叶节点的秘密共享数等于该节点的多项式值和其父节点的多项式值之和。

采用定理1计算秘密共享数，可避免在每个节点上分别计算秘密共享数的复杂性，这种方法应用到VSN的数据共享中，可简化密钥生成和解密过程。

设秘密共享数 s 属于访问树的某个叶子节点，设 t_0、t_n 分别为根节点和叶子节点，其路径为 $t_0\rightarrow t_1\rightarrow\cdots\rightarrow t_m$。设节点 $t_i(i\in[0,m])$ 对应多项式 $f_i(x)$，去掉常数项后记作 $f_i'(x)$；定义 $index(x)$ 函数表示兄弟节点中 x 的序号。每个叶子节点的秘密共享数可以通过从根节点到该叶子节点的路径上的每个节点（需要排除访问树的根节点）的父节点多项式值（要求除去该节点的常数项）和该节点的秘密数之和计算，该证明过程表示为：

$$\begin{aligned}&f_0(0)=s,\\&f_1(0)=f_0'(index(t_1))+s,\\&f_2(0)=f_1'(index(t_2))+f_1(0)\\&\quad=f_1'(index(t_2))+f_0'(index(t_1))+s,\\&\cdots,\\&f_m(0)=f_{m-1}'(index(t_m))+f_{m-1}(0)\\&\quad=f_{m-1}'(index(t_m))+\cdots+f_1'(index(t_2))+\\&\quad f_0'(index(t_1))+s\end{aligned} \tag{5}$$

根据该定理，设计一个可以实现快速计算的访问树模型，以便帮助车队车辆快速计算出访问树的叶子节点秘密共享数和数据的密文。

在本文方案中，RSU在计算共享访问树时会采用安全策略，例如将每个节点的多项式常数项设为0，并在获取叶子节点的秘密分量后将其加上1，以有效防止数据泄露。完成计算后，RSU将与属性相关的密文返回给车队车辆，以便进一步计算秘密值 s。

定理2：访问树的秘密值为1或0，叶子节点的秘密分量增加1，该访问树的相同叶子节点将同时增加1的秘密分量。

当共享访问树设置秘密值为1时，由定理1可得，叶子节点 t_m 的秘密分量多项式可表示为：

$$f_{m,1}(0)=f_{m-1}'(index(r_m))+\cdots+f_1'(index(t_2))+f_0'(index(t_1))+1 \tag{6}$$

由定理1可得，设置秘密值为0的访问树叶子节点 t_m 的多项式，其秘密分量为：

$$f_{m,0}(0)=f_{m-1}'(index(t_m))+\cdots+f_1'(index(t_2))+f_0'(index(t_1))+0 \tag{7}$$

将上述多项式中的秘密值加1后可得：

$$f_{m,2}(0)=f_{m,0}(0)+1=f_{m-1}'(index(t_m))+\cdots+f_1'(index(t_2))+f_0'(index(t_1))+1 \tag{8}$$

根据上述证明可得 $f_{m,1}(0)=f_{m,2}(0)$，即定理2成立。

定理3：访问树的秘密值为1，无论该访问树的叶子节点的秘密分量是否乘以秘密值 s，根节点的秘密值都相同。同样地，当访问树的秘密值为 s 时，无论该访问树的

叶子节点是否乘以s，均不会影响该树根节点的秘密值。

由定理1得，设置秘密值为s的访问树叶子节点t_m的多项式秘密分量为：

$$f_{m,1}(0)=f'_{m-1}(index(t_m))+\cdots+f'_1(index(t_2))+f'_0(index(t_1))+s \tag{9}$$

相应地，当访问树的秘密值出现为1的情况时，由定理1可推导得出叶子节点t_m的秘密分量多项式为：

$$f_{m,0}(0)=f'_{m-1}(index(t_m))+\cdots+f'_1(index(t_2))+f'_0(index(t_1))+1 \tag{10}$$

将上述多项式进行乘以s的运算后可得：

$$\begin{aligned}f_{m,2}(0)&=f_{m,0}(0)\cdot s\\&=f'_{m-1}(index(t_m))\cdot s+\cdots+f'_1(index(t_2))\cdot s+f'_0(index(t_1))\cdot s+s\end{aligned} \tag{11}$$

根据定理1可知，加密时访问树根节点秘密值，是加密前秘密分量$f_m(0)$的最后一项。因此，在访问树的秘密值为1且叶子节点秘密分量乘以s的情况下，加密前的秘密分量$f_m(0)$的最后一项为s，根节点的秘密值为s。在该情况下，加密前的秘密分量$f_m(0)$的最后一项也为s，因此根节点的秘密值仍为s，从而定理3命题成立。根据定理2和定理3，在秘密值为0时，将秘密分量加1的叶子节点乘以秘密值s，根节点的秘密值相同。此外，当秘密值为s时，根节点的秘密值相同。

定理4：访问树和$(\boldsymbol{M},\rho)$是等价的，即可以通过访问树转化为线性秘密共享方案。

证明如下：首先将访问树T转换为相应的二叉树，设节点编号次序为1,2,…,m，为访问树T的m个非二叉树叶子节点；同时设定二叉树n个叶子节点，依次编号为1,2,…,n。二叉树中的非叶子节点用i表示，并用函数$f_i(x)=\omega_i x,\omega_i\in Z_p^*$表示。

设定从根节点到叶子节点i依次经过的非叶子节点（简称路径）为$i_1,i_2,\cdots,i_{m_i}$，s_i为访问树第i个叶子节点的秘密共享值，根据定理1可知，将二叉树的第i个叶子节点用多项式表示的秘密共享数为：

$$\begin{aligned}\lambda_i&=s_i=s+\sum_{j=1}^{n_i}f_{i_j}(index(i_{j+1}))\\&=s+\sum_{j=1}^{n}b_{ij}f_j(index(suc(j))),\left(b_{ij}=\begin{cases}1,j\in\{i_1,i_2,\cdots,i_{n_i}\}\\0,\text{else}\end{cases}\right)\\&=s+\sum_{i=1}^{n}\omega_i b_{ij}(index(suc(j))),\\&=s+\sum_{j=1}^{n}\omega_i b_{ij}c_{ij},\left(c_{ij}=index(suc(j))=\begin{cases}1\\2\end{cases}\right)\\&=\left(1,b_{i1}c_{i1},b_{i2}c_{i2},\cdots,b_{im}c_{im}\right)\left(s,\omega_1,\omega_2,\cdots,\omega_m\right)^{\mathrm{T}}\\&=\boldsymbol{M}_i\left(s,\omega_1,\omega_2,\cdots,\omega_m\right)^{\mathrm{T}}\end{aligned} \tag{12}$$

其中，$index(suc(j))$函数结果为1时为左孩子，$index(suc(j))$函数结果为2时为右孩子。当式（12）中的参数$b_{ij}=1$时，可利用$suc(j)$求j在路径上的后继节点，最后转化过程多项式为：

$$\rho(\boldsymbol{M}_i)=att(i),\boldsymbol{M}=(\boldsymbol{M}_1,\boldsymbol{M}_2,\cdots,\boldsymbol{M}_n)^{\mathrm{T}}=\begin{bmatrix}1&\cdots&b_{1m}c_{1m}\\\vdots&&\vdots\\1&\cdots&b_{nm}c_{nm}\end{bmatrix} \tag{13}$$

因此，任意关于秘密共享的访问树均可转化为线性秘密共享中的访问策略$(\boldsymbol{M},\rho)$，从而RSU可将访问树转化为访问矩阵。且根据以上定理，车队车辆可以快速实现基于访问树的访问策略。

3.4 安全模型

初始化阶段。挑战者V初始化生成挑战所需的PK，并将其返回至敌手G。

阶段1：V创建空表N以存储记录，分别设置用于挑战的空集D和整数k，其初始值为0，对于以下查询，G可以重复任意次数。

a. $Create(S)$：挑战者V使用外包私钥生成算法，设置整数$k:=k+1$，以获取属性集S用于挑战，在表N中存储密钥、转换密钥(SK,TK)和参数(k,S,SK,TK)，随后将TK返回给G，G可以不受限地重复查询。

b. $Corrupt(i)$：查询表N的存储记录，如有记录i，则将记录(i,S,SK,TK)发送给V，收到记录后V设置集合$D:=D\cup\{S\}$，并将表N中的私钥SK发送给G，如表N中查询不到记录i，则返回空值（⊥）给V。

c. $Decrypt(i,CT)$：查询表N的存储记录，如存在记录i，将记录(i,S,SK,TK)发送给V，随后以(SK,CT)作为输入解密密文，输出明文给G，如表N中查询不到记录i，则返回⊥给V。

挑战阶段：G提交明文给V，设明文M_0与M_1等长的同时，敌手G继续向挑战者V提交T^*。T^*是一个挑战访问树，任意$S\in D$都不能满足T^*。V收到上述数据，获得随机数b，该随机数通过抛硬币得到。V将计算明文和密文(M_b,CT^*)，最后G收到计算结果。

阶段2：进行有限的重复查询，其限制条件为，查询不能获取解密挑战密文的私钥，且不能进行解密挑战密文的查询。

猜测阶段：在猜测阶段，G给出一个关于b的猜测值b'。

4 性能分析

4.1 安全性分析

在本方案中，DO进行数据共享，而数据的存储则外

包给CS。为确保数据存储的安全性，访问策略的生成工作由RSU完成。RSU作为进行外包加密的实体，能够获得访问树，并将其转化为DO所需的访问策略，无法获得完整密文，本节主要对访问树的安全性进行分析。

初始化阶段：模拟器B激活敌手G，敌手G生成挑战访问树T^*，模拟器B可以根据定理4，将访问树T^*转换成$(\boldsymbol{M}^*,\rho^*)$，并发送给挑战者V，作为被挑战的访问结构。模拟器B成功获取公钥参数$PK=e(g,g)^{\alpha},g,g^{a},\{T_i\}_{i\in U}$，将其发送给G作为系统公钥。

阶段1：由模拟器B生成一些空表，如N、T_1、T_2，此外，仍需一个空的集合D和一个初始值为0的整数k，G还可以进行以下步骤的查询。

a. $H_1(R,M)$算法判断(R,M,s)是否已经在表T_1中，如果存在则返回s，反之则选择一个随机值$s\in Z_p^*$，将(R,M,s)记录在T_1表中并返回s'。

b. $H_2(R)$算法判断(R,r)是否存在表T_2中，如在表中则返回r，否则选择一个随机值$r\in\{0,1\}^k$，将(R,r)记录在T_2中并返回r。

c. *Create*(S)算法中，模拟器B设定$k:=k+1$，并且采用如下步骤处理：

属性集合S满足T^*时，生成伪造的转换密钥，运行算法$KeyGen((d,PK),S)$，随机生成$d\in Z_p^*$，得到SK'，得出转换密钥$TK=SK'$、$SK=(d,TK)$；

属性集合S不满足访问树T^*时，运行私钥生成算法生成私钥，对应属性集合S的私钥为$SK'=(PK,K',L'\{K_x'\}_{x\in S})$，随机选择$z\in Z_p^*$，设置转换密钥$(PK,K=K'^{1/z},L=L'^{1/z},\{K_x\}_{x\in S}=\{K_x'\}_{x\in S})$，私钥为$(z,TK)$；

B将数据(k,S,SK,TK)存储在表N中，并将表中的TK返回给敌手G。

d. *Corrupt*(i)算法：当请求被拒绝，表明G无法挑战T^*的私钥，则属性集合S不满足T^*。若N中存在第i个元素，B获取参数(i,S,SK,TK)并设置$D:=D\cup\{S\}$，敌手G将收到由挑战者V发送的私钥SK，若不存在，则返回$\perp$。

e. *Decrypt*(i,CT)算法中，参数CT已半解密，模拟器B和敌手G已得知SK和TK，对密文CT进行半解密。

密文$CT=(C_0,C_1,C_2)$的访问策略为T^*（访问树），于表格N中获取(i,S,SK,TK)。当表N中不存在(i,S,SK,TK)或属性S不满足T^*时，返回$\perp$给G。此外，当第i个元素满足T^*时，按如下步骤进行：

a. 解析$SK=(z,TK)$，计算$R=C_0/C_2^z$。

b. 遍历表格T_1，获取记录(R,M_i,s_i)，若记录不存在，将$\perp$返回敌手G。

c. 表T_1中$y\neq x$时，将导致记录(R,M_y,s_y)和(R,M_x,s_x)，存在$M_y\neq M_x$且$s_y\neq s_x$的情况，因此B终止仿真。

d. 表T_1中$y=x$时，B从表T_2中获取记录(R,r)，反之B输出$\perp$。

e. 对于T^*中每个密钥i，测试参数$C_0=R\cdot e(g,g)^{\alpha s_i}$、$C_1=M_i\oplus r$、$C_2=e(g,g)^{\alpha s_i/z}$是否成立。

f. B通过了上述测试，将输出消息M_i，反之B输出$\perp$。

挑战阶段：敌手G提交2个消息$(M_0^*,M_1^*)\in\{0,1\}^{2\times k}$，同时要求这2个消息等长，B进行如下处理步骤。

a. B选择随机值$(R_0,R_1)\in G_T^2$，发送给V以获取满足$(\boldsymbol{M}^*,\rho^*)$的密文$CT=(C,C',\{C_i\}_{i\in[i,l]})$。

b. B随机选择$C''\in\{0,1\}^k$。

c. B将挑战密文$CT=(C,C',\{C_i\}_{i\in[i,l]})$发送给敌手G。

阶段2：G不断重复阶段1中的步骤，当返回M_0^*或M_1^*时结束，此时B将响应给G消息Test。

猜测阶段：G的输出结果只能为1或0，除此之外只有放弃攻击。以上情况B将不回应，并继续检索遍历表T_1或T_2，若仅出现1次随机值$R_b(b\in[0,1])$，则b作为B的猜测值，若随机值$R_b(b\in[0,1])$出现多次，将随机选择(0,1)作为猜测值。

因此敌手G的优势为$P_r[b=b']=1/2$。

4.2 仿真分析

本文方案在Pycharm中基于Python2.7语言实现了密钥生成、加密和解密，仿真环境为Ubuntu 14.04 64位系统。主要对比方案的密钥生成、数据加密和解密的计算开销。

表1展示了各方案的理论计算量，其中，单个配对、群上的单个指数运算、乘法运算和哈希的计算开销分别为T_p、T_e、T_m和T_h，u、l分别为用户属性的数量和生成访问策略所使用的属性数量。仿真结果如图3~图5所示。

表1 计算开销分析

方案	密钥生成	数据加密	数据解密
文献[7]	$(u+2)T_e+T_m$	$(8l+2)T_e+(l+3)T_m$	$uT_e+(6u+1)T_p+(5u+1)T_m$
文献[8]	$(u+2)T_e$	$(2l+2)T_e+(l+1)T_m$	$uT_e+(2u+1)T_p+(u+2)T_m$
文献[9]	$(5u+3)T_e+4T_m$	$(2l+6)T_e+(2l+4)T_m+2T_h$	$8T_p+8T_m$
本方案	$(u+l+2)T_e$	$2T_e+T_p$	$lT_e+(2l+1)T_p$

在图3中可以看出，在加密阶段，文献[8]方案的加密时间随着属性数量的增加而快速增长。但文献[7]方案、文献[9]方案与本文方案的加密时间随着属性数量

的增加并未产生较大的变化。由于本文方案与文献[7]、文献[9]均采取了外包加密算法，将访问策略的生成外包给其他实体，车辆用户仅需要根据自己的需求设计访问树，由RSU将访问树转化为访问矩阵从而生成访问策略，故本文方案的加密计算开销最小，仿真数据表明，平均加密时间为70 ms。

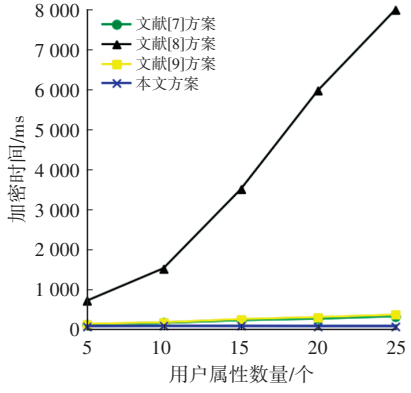

图3　属性数量对密文生成时间的影响

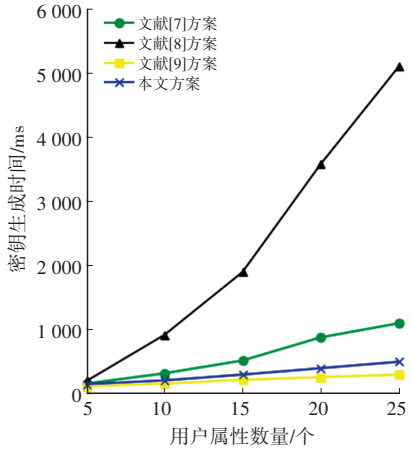

图4　属性数量对密钥生成时间的影响

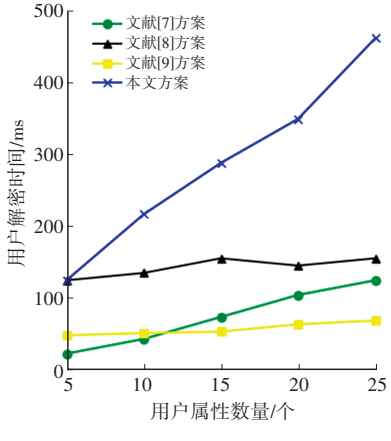

图5　属性数量对用户解密时间的影响

本文方案在密钥生成阶段的计算量仅略高于文献[9]方案，低于其他方案，这与表1中的分析一致。由图4可知，所有方案的密钥生成时间均随着属性数量的增加而增长，本文方案将访问策略的生成外包，使得方案增长幅度仅稍微高于文献[9]方案，这是由于需要车队车辆设计访问树，这部分的开销会随着属性数量的增加而线性增长。

在图5可知，文献[7]方案与文献[9]方案的解密开销受用户属性增长影响更小，这是由于这2种方案采用外包解密。本方案具有较高解密密文开销，后续工作可以考虑引入外包解密，以降低解密计算开销。

5　结束语

本文针对VSN中车队车辆数据共享时存在的隐私泄露问题，提出基于CP-ABE的车队车辆数据共享方案，采用外包加密算法由RSU将数据加密，减轻了车队车辆加密密文的计算压力。由车队车辆通过访问树设计访问策略，RSU将访问树转化为线性访问矩阵来进一步降低车队车辆的计算开销。理论分析和仿真分析结果表明，本文方案实现了高效、安全的数据共享。

参　考　文　献

[1] WANG X J, NING Z L, ZHOU M C, et al. Privacy-Preserving Content Dissemination for Vehicular Social Networks: Challenges and Solutions[J]. IEEE Communications Surveys & Tutorials, 2019, 21(2): 1314-1345.

[2] 周启扬, 李飞, 章嘉彦, 等. 基于区块链技术的车联网匿名身份认证技术研究[J]. 汽车技术, 2020(10): 58-62.
ZHOU Q Y, LI F, ZHANG J Y, et al Research on Anonymous Identity Authentication Technology of Vehicle-to-Everything Based on Blockchain Technology[J]. Automotive Technology, 2020(10): 58-62.

[3] 王经纬, 宁建廷, 许胜民, 等. 面向可变用户群体的可搜索属性基加密方案[J]. 软件学报, 2023, 34(4): 1907-1925.
WANG J W, NING J T, XU S M, et al. A Searchable Attribute Based Encryption Scheme for Variable User Groups[J]. Journal of Software, 2023, 34 (4): 1907-1925.

[4] SAHAI A, WATERS B R. Fuzzy Identity-Based Encryption [C]// 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Aarhus, Denmark: Springer Berlin Heidelberg, 2005: 457-473.

[5] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-Policy Attribute-Based Encryption[C]// 2007 IEEE Symposium on Security & Privacy. Berkeley, CA, USA: IEEE, 2007: 321-334.

[6] ZHANG L Y, ZHANG Y, WU Q, et al. A Secure and Efficient Decentralized Access Control Scheme Based on Blockchain for Vehicular Social Networks[J]. IEEE Internet of Things Journal, 2022, 9(18): 17938-17952.

[7] CUI H, ROBERT H D, WU G, et al. An Efficient and Expressive Ciphertext-Policy Attribute-Based Encryption Scheme with Partially Hidden Access Structures, Revisited [J]. Computer Networks, 2018, 133: 157-165.

[8] YANG K, HAN Q, LI H, et al. An Efficient and Fine-Grained Big Data Access Control Scheme with Privacy-Preserving Policy[J]. IEEE Internet of Things Journal, 2017, 4(2): 563-571.

[9] LI J G, SHA F J, ZHANG Y C, et al. Verifiable Outsourced Decryption of Attribute-Based Encryption with Constant Ciphertext Length[J]. Security and Communication Networks, 2017(2): 1-11.

[10] XIA F, WANG L M. S2PD: A Selective Sharing Scheme for Privacy Data in Vehicular Social Networks[J]. IEEE Access, 2018, 6: 55139-55148.

[11] SETHI K, PRADHAN A, BERA P. Practical Traceable Multi-Authority CP-ABE with Outsourcing Decryption and Access Policy Updation[J]. Journal of Information Security and Applications, 2020, 51.

[12] FAN K, PAN Q, ZHANG K et al. A Secure and Verifiable Data Sharing Scheme Based on Blockchain in Vehicular Social Networks[J]. IEEE Transactions on Vehicular Technology, 2020, 69(6): 5826-5835.

[13] ZHONG H, ZHU W L, XU Y, et al. Multi-Authority Attribute-Based Encryption Access Control Scheme with Policy Hidden for Cloud Storage[J]. Soft Computing A Fusion of Foundations Methodologies & Applications, 2018, 22: 243-251.

[14] PU Y W, XIANG T, HU C Q, et al. An Efficient Blockchain-Based Privacy Preserving Scheme for Vehicular Social Networks[J]. Information Sciences, 2020, 540: 308-324.

[15] SHI K X, ZHU L H, ZHANG C, et al. Blockchain-Based Multimedia Sharing in Vehicular Social Networks with Privacy Protection[J]. Multimedia Tools and Applications, 2020, 9(11): 8085-8105.

[16] SUN J F, XIONG H, ZHANG S F, et al. A Secure Flexible an Tampering-Resistant Data Sharing System for Vehicular Social Networks[J]. IEEE Transaction on Vehicular Technology, 2020, 69(11): 12938-12950.

[17] ZHOU L, LUO E T, WANG G J, et al. Secure Finegrained Friend-Making Scheme Based on Hierarchical Management in Mobile Social Networks[J]. Information Sciences, 2021, 554: 15-32.

[18] BEIMEL A. Secret-Sharing Schemes: A Survey[C]// International Conference on Coding and Cryptology. Berlin, Heidelberg: Springer, 2011: 11-46.

（责任编辑 斛 畔）

修改稿收到日期为2023年7月27日。