计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2017.20170373
54(11):2456-2466,2017

可撤销动静态属性的车联网属性基加密方法

何 倩[1,2] 刘 鹏[1,2] 王 勇[1]
[1](广西云计算与大数据协同创新中心(桂林电子科技大学) 广西桂林 541004)
[2](认知无线电与信息处理教育部重点实验室(桂林电子科技大学) 广西桂林 541004)
(heqian@guet.edu.cn)

Attribute Based Encryption Method with Revocable Dynamic and Static Attributes for VANETs

He Qian[1,2], Liu Peng[1,2], and Wang Yong[1]
[1](*Guangxi Collaborative Innovation Center of Cloud Computing and Big Data* (*Guilin University of Electronic Technology*), *Guilin*, *Guangxi* 541004)
[2](*Key Laboratory of Cognitive Radio and Information Processing* (*Guilin University of Electronic Technology*), *Ministry of Education*, *Guilin*, *Guangxi* 541004)

Abstract The data secure sharing in vehicular ad hoc network (VANET) usually uses group encryption mode. However it is difficult to construct group and to manage group key for vehicular terminal with high mobility. Ciphertext-policy attribute-based encryption (CP-ABE) is a kind of new solution for VANETs' communication security. In the traditional CP-ABE strategy, it has several shortcomings, such as high decryption computation complex, and attributes revoking requires the re-encrypting of the whole cipher-text and the inflexible construction of access policy tree. These shortcomings lead to the limited application of CP-ABE in VANETs. In order to solve these problems, an ABE with revocable dynamic and static attributes (ABE-RDS) is proposed for the data secure sharing of cloud storage in VANETs. In the ABE-RDS, dynamic attribute and static attribute are managed separately, and combination policy tree is constructed, and main decryption part with high computation cost is delegated to servers using decryption proxy. In addition, the vehicular terminal can revoke attributes and refresh dynamic attributes through global and local trusted authority. The proposed ABE-RDS is secure, and it has superiority over traditional CP-ABE in space and time complexity. The performance of ABE-RDS in vehicular terminal decryption, attribute revocation, and system concurrent is evaluated with experiments.

Key words vehicular ad hoc network (VANET); attribute based encryption (ABE); dynamic and static attribute; revocable attribute; decryption proxy

摘 要 车载自组织网络(vehicular ad hoc network, VANET)(也称车联网)数据安全共享通常采用群加密方式,高速移动的车载终端给群组构建和群密钥管理带来困难.密文策略属性基加密(ciphertext-

收稿日期:2017-05-31;**修回日期**:2017-08-07
基金项目:国家自然科学基金项目(61661015,61572148);认知无线电与信息处理教育部重点实验室基金项目(CRKL160101);广西云计算与大数据协同创新中心基金项目(YD16801)
This work was supported by the National Natural Science Foundation of China (61661015, 61572148), the Key Laboratory of Cognitive Radio and Information Processing Fund, Ministry of Education (CRKL160101), and the Guangxi Collaborative Innovation Center of Cloud Computing and Big Data Fund (YD16801).

policy attribute-based encryption, CP-ABE)为车联网通信安全带来了新的解决方案,但是传统的 CP-ABE 方案解密计算复杂度高,属性撤销需要整个密文进行全部更新,策略树的构建不够灵活,导致在车联网中的应用受限.为了解决上述问题,围绕车联网云存储数据安全分享,设计可撤销动静态属性的属性基加密方案.将动态属性和静态属性分开管理,构建组合策略树,引入解密代理将高复杂度的属性基解密过程的主要部分外包到服务端,车辆终端通过中央和本地认证中心进行属性撤销和动态属性更新.可撤销动静态属性的车联网属性基加密方案是安全的,在空间和加解密时间复杂度上较传统 CP-ABE 算法具有优势,实验还分析了车载终端解密、属性撤销和系统并发等性能.

关键词　车联网;属性基加密;动静态属性;可撤销属性;解密代理

中图法分类号　TP393

近年来,随着互联网、物联网、云计算等新兴技术的发展和普及,一种新型的 Ad Hoc 网络应用,即车载自组织网络(vehicular ad hoc network, VANET)(也称车联网),越来越受到人们的关注[1-2].车联网由感知层、网络层和应用层组成,当车辆行驶到某个环境中,通过感知层获取环境和行车状态等信息,然后由网络层实现车与车、车与人和车与应用平台等进行交互,最后分析获取交通、商务等信息,已逐渐成为降低交通事故、提高交通效率和改善驾驶员驾车体验的关键技术[2].

与此同时,车联网中的信息安全问题也逐渐成为阻碍其发展的重要原因.为保证数据安全,应用信息发布者(application service provider, ASP)将数据发布到云存储平台(cloud storage provider, CSP)时通常采用加密的方式存储,只有被授权的用户能够访问数据内容.车联网是一种特殊的自组织网络,同传统的无线网络相比,车联网中车载终端(vehicular terminal, VT)具有数量众多、高度动态性和移动性等特点,当数据分享的数量增多时,这种方案将会带来巨大的管理密钥的开销[3-4],车联网中群组构建、密钥分发和组成员管理都将是比较困难的.在文献[5]中,Sampigethaya 等人提出将相同的车速和保持一定距离的 VT 构成群组,该方式构建群组过于严格,当 VT 高速移动时该方式难以实现.车联网中的数据共享通常采用群加密的方式,由于 VT 高度的动态性,群组成员频繁的变动,使得群组的构建受限以及群密钥的管理开销过大,难以在实际中应用.

Sahai 等人在文献[6-7]中提出属性基加密方法(attribute based encryption, ABE),ABE 是一种非常有效的面向群分享的数据访问控制方法,是基于身份的加密方案[8-9]和门限秘密共享方案[10]的发展.ABE 主要包括密钥策略 ABE(KP-ABE)和密文策略 ABE(ciphertext-policy attribute-based encryption, CP-ABE).CP-ABE 将访问控制策略融入密文,消息的发送者按照一定的访问控制策略树对数据进行加密后传输,消息的接收者所拥有的属性集合如果满足访问控制策略树,则能够进行解密消息.CP-ABE 按照用户所拥有的属性进行群组的划分,提供一种有效的群组构建方式,只有属性集合满足该群组的条件时才能够加入本群组,对接收到该群组的消息进行解密,能够有效地适应用户群组成员多变的特性,非常适合车联网应用.

车联网中 VT 具有高速移动性的特点,将会导致部分属性频繁地更新,如所在城市、街道和行车方向等属性,称为动态属性(dynamic attribute, A_{dyn}).同时车辆还存在一些固有属性,如车辆所属类型、所属单位和注册编号等属性称为静态属性(static attribute, A_{sta}).当系统对权限分配进行更新时,需要撤销用户的部分权限.然而传统的 CP-ABE 的解密过程计算复杂度较大,不适合在车联网中直接应用.Zhang 等人提出了无须双线性对运算的 CP-ABE,但该算法基于 n 元格难问题,其运行效率也不高[11].在文献[12]中提出在线/离线密文策略属性基可搜索加密方案,采用加解密外包技术,降低了解密端的计算开销.

原始 CP-ABE 没有实现属性撤销和更新,已有的具备属性撤销功能的 CP-ABE 都没有将动静态属性进行区分,在单独的属性进行撤销更新时,需要更新整体密文.在车联网中动态属性频繁更新的过程中,将会带来极大的系统消耗.Pirretti 等人在文献[13]中提出一种属性撤销方案,但是该方法不具实时性,需要频繁进行密钥的维护,导致开销较大.Hur 和 Xie 等人在文献[14-15]中提出一种属性即时撤销方案,然而该方案的密钥和密文的更新效率比过低.Fan 等人在文献[16]中提出一种任意状态下属性和用户成员的动态变化,但无法实现用户的属性撤销.

针对以上问题,围绕车联网云存储数据安全分享,本文提出了一种可撤销动静态属性的属性基加密方案.主要创新点包括3点:1)针对车联网的高移动性等特性,根据时间变化快慢,将属性分为动态属性和静态属性,同时引入策略群组的概念,方便群组成员管理,减少密钥管理带来的开销;2)对传统的CP-ABE进行改进,使得在属性进行更新和撤销的过程中,仅需要属性权威和解密代理的参与,进而降低属性撤销对用户的影响,引入解密代理承担大部分的解密运算,从而提高VT的解密效率;3)理论分析了改进方案的安全性以及空间、时间复杂度,构造模拟实验验证了改进方案在车联网应用的可行性.

1 相关知识

1.1 双线性映射

设 G_1,G_2 分别是阶为 p 的加法群和乘法群,g 为群 G_1 的生成元.$e:G_1\times G_1\rightarrow G_2$ 为满足3种性质的双线性对:

1) 双线性.对所有的 $P,Q\in G_1$ 和 $a,b\in Z_q^*$ 有 $e(aP,bQ)=e(abP,Q)=e(P,abQ)=e(P,Q)^{ab}$.

2) 非退化性.$\exists P,Q\in G_1$,满足 $e(P,Q)\neq 1$.

3) 可计算性.对于 $P,Q\in G_1$,存在一个有效的计算方法 $e(P,Q)$.

1.2 车联网的基本模型

车联网主要有移动车载终端如安装有通信单元(on-board unit, OBU)、固定节点如路边基础设施(road-side unit, RSU)和认证中心(trusted authority, TA)这3部分组成.如图1所示,认证中心TA是车联网中的诚实可信的安全中心,是最高权威机构.TA主要负责车联网系统中所有的OBU和RSU的注册、身份认证以及发放证书等.OBU是车联网中的移动终端,并且具有一定的存储和计算能力.车辆在加入到车联网之前需要获得TA认证,并将注册信息存储在存储单元中,未经TA授权无法更改,同时车辆节点是在高速移动中,车载的部分属性信息是在频繁地更新中,如位置、车速和行驶方向等.路边单元RSU接入车联网同样需要获得TA认证,同时可以为OBU提供丰富的行车信息.

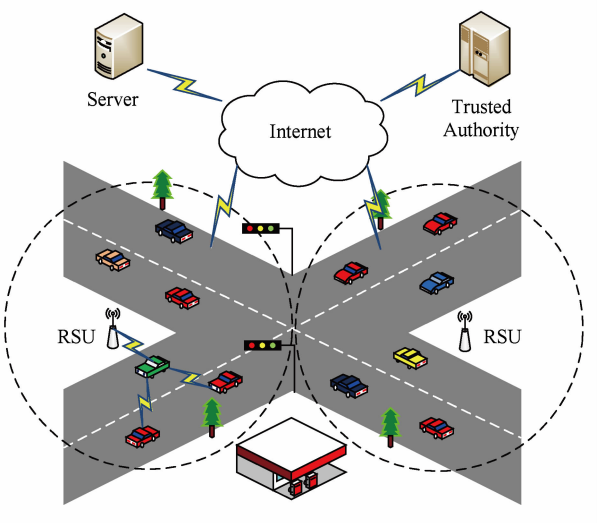

Fig. 1 Basic model of VANET

图1 车联网基本模型

2 动静态属性基加密算法

本文中的属性基加密算法是在文献[7]基础上的改进CP-ABE,结合车联网中VT高速移动的特性,将随时间变化的动态属性引入到算法中;同时,考虑到对时延比较高的要求,引入解密代理提高VT解密速度.主要由5个算法构成:

1) $Setup(\lambda,U)=\{PK,MSK\}$.初始化算法由属性权威执行,算法的输入为安全参数 λ 和属性全集 U.该算法选取阶位 p 的循环群 G_1,生成元为 g 以及随机参数 $\alpha\in Z_p$.对每一属性获取随机参数 $t_{i,v}\in Z_p$,$i\in|U|$,并计算 $h_{i,v}=H(F(t_{i,v},f(t)))$,$i\in|U|$.输出系统主钥为:$MSK=\{a,\alpha,t_{i,v}\}$,$i\in|U|$,系统公钥为:$PK=\{g,e(g,g)^{\alpha},g^{a},h_{i,v}\}$,$i\in|U|$.

2) $Encrypt((M,\rho),PK,\mathcal{M})=CT$.加密算法输入明文 $\mathcal{M}$ 和系统公钥 PK,另外通过函数 ρ 将访问控制策略中的每个属性与LSSS矩阵 $\boldsymbol{M}_{l\times n}$ 中的每一行关联起来.该加密算法首先会生成一个向量 $\boldsymbol{v}=(s,y_2,y_3,\cdots,y_n)^{\perp}$,$s,y_i\in Z_p$,并且计算 $\lambda=\boldsymbol{v}\cdot\boldsymbol{M}$,最后该算法随机选取 $r_1,r_2,\cdots,r_l\in Z_p$,输出密文 $CT=\{C=\mathcal{M}\cdot e(g,g)^{as},C'=g^{s},\{C_i,D_i\}_{1\leqslant i\leqslant l}\}$,其中对于任意的 $1\leqslant i\leqslant l$:$C_i=g^{a\lambda_i}\cdot[h_{\rho(i),v}]^{-r_i}$,$D_i=g^{r_i}$.

3) $Keygen(MSK,PK,S)=\{TK,SK,USP\}$.密钥生成算法由属性权威执行,输入 MSK、PK 和用户属性集合 S,选取随机数 $t\in Z_p$,输出用户转换密钥 $TK=\{K=g^{\alpha/z}\cdot g^{\alpha\beta/z},L=g^{\beta/z},\{K_x=[h_x]^{\beta/z}\}x\in s\}$,用户私钥 $SK=z$,用户保密参数 $USP=\beta/z$.

4) $Transform(CT,TK)=CT'$.代理解密算法由解密代理服务器执行.该算法输入密文 CT 和转换密钥 TK.如果用户属性集合 S 满足访问控制策略,则存在 $\rho(i)\in S$,同时生成向量 $\boldsymbol{W}=(w_1,w_2,\cdots,w_l)$,$w_i\in Z_p$,使得 $\boldsymbol{W}\cdot\boldsymbol{M}=(1,0,0,\cdots,0)$,然后计算

$R=e(C',K)/E$,其中 $E=\prod_{i=1}^{l}e(C_i^{w_i},L)\cdot e(D_i^{w_i},K_{\rho(i)})$,然后输出半解密密文 $CT'=\{R,C\}$,否则直接输出 $CT'=\perp$.

5) $Decrypt(CT',SK)=OUT$. 解密算法由车辆节点执行,输入半解密密文 CT'和用户私钥 SK,输出明文 OUT.

3　车联网属性基加密系统模型

3.1　系统架构

车联网属性基加密系统是动态的属性基加密系统,主要由中央认证中心(global trusted authority, GTA)、本地认证中心(local trusted authority, LTA)、解密代理(decrypt proxy, DP)、应用服务的提供者 ASP、云存储提供者 CSP 和车载终端 VT 这 6 个部分组成,系统架构如图 2 所示:

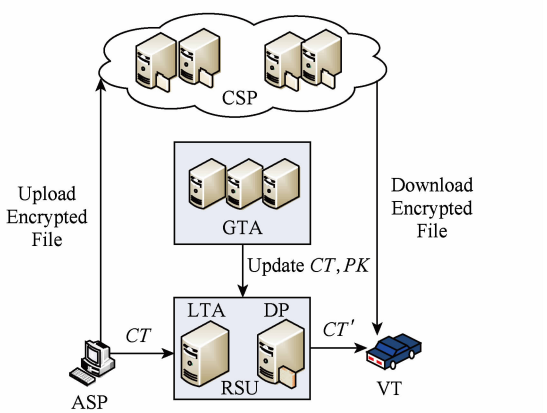

Fig. 2　ABE system architecture for vehicle networking

图 2　车联网属性基加密系统架构

ASP 将数据采用对称加密后上传到 CSP,同时将密钥采用 CP-ABE 加密后存储到密钥管理中心. 车载终端满足访问控制策略则可以解密获得对称密钥. GTA 部署在云端,主要负责 VT 和 RSU 注册、静态属性以及静态密钥生成管理等,并且管理多个 LTA;LTA 部署在 RSU 上,主要负责对车辆动态属性和动态密钥的管理等,需要定时和 GTA 进行同步,保证数据的同步;DP 部署在 RSU 上,主要负责对密文 CT 的预解密和属性的撤销更新等;同时 RSU 的部署时采用分等级和分布式的方式部署. 在系统中车载终端之间和车辆与服务器间均通过无线广播的形式相互通信,其他服务器之间通过高速有线网络通信.

本系统架构中主要涉及 2 种加密算法:1)对密钥进行加密阶段使用的基于密文的 CP-ABE,该加密方式主要是针对密钥进行加密,将加密生成的密文 CT 和对应文件的 FID 存储在本地的 RSU 中;2)利用密钥对消息进行加密阶段使用到的对称加密,将加密生成的数据存储到云平台上. 车载终端根据需求获取存储在 RSU 上的 CT 和 FID,然后将 CT 进行属性基解获得密钥,然后对从云端获取的应用文件进行对称解密获得应用信息.

3.2　动态策略群密钥分发

车联网中当车辆进入一个新的区域,首先 VT 和 LTA 进行相互认证,认证通过后向管理该区域的 LTA 请求动态属性更新,并且生成新的动态密钥,主要过程分为 3 个部分:

1) LTA 和 VT 做相互认证,认证通过后 LTA 获取 VT 新的动态属性集;

2) LTA 使用新的动态属性集执行初始化算法,并且产生动态公钥 PK_{dyn}和动态主密钥 MSK_{dyn};

3) 为该范围内的所有 VT 生成动态密钥 SK_{dyn},然后使用 PK_{dyn}进行签名解密后发送给每个车辆节点.

VT 在进行动态属性基解密时,必须进行属性的同步,例如在时刻 t_1 使用动态属性 $attr_1$ 进行加密数据,则在时刻 t_2 属性未进行更新时,应该是不能够解密消息的. 本文将文献[17]提出的对每个动态属性引入衰退方程应用到方案中,在指定的时间单元 t 中,通过衰退方程计算出该属性的值,从而使属性动态地变化. 不同的动态属性变化的时间单元 t 的大小在本文不做讨论.

3.3　组合策略群组的构建

车联网中动态属性更新频繁,为了方便属性的管理,该系统中静态属性和动态属性分开管理,静态属性由中央认证机构 GTA 在车辆注册的过程中预置到车辆当中,同时为车辆生成静态加密参数;动态属性是在车辆行驶过程中,由本地认证中心 LTA 进行分发,同时为 VT 生成动态参数. 然后通过组合策略树的方式构建整体的访问控制策略.

在方案中首先引入策略群的概念,每一个 LTA 具有固定的管理区域,并且在该区域的车辆的部分动态属性如位置和日期等相同. 当车辆进入一个新的区域,首先 VT 和 LTA 进行相互认证,认证完成后通过 GTA 和 LTA 进行属性同步(attribute synchronization, SYNA),并且分别为车辆节点生成静态密钥和动态密钥. 能够满足相同访问控制策略的车辆构成一个群组,该策略群的构建方式同传统的

群组构建方式相比,该方式在每一个 LTA 管理区域具有相同动态属性的车辆节点构成一个策略群,有效地减少为密钥的管理、群组成员频繁的添加和删除产生额外的开销.

在策略群中只使用动态属性构成动态策略树加密消息时,所有的群组成员都能够进行解密,这将带来极大的不便. 如某出租车公司想在 CSP 上分享的特定应用信息,只对该公司在特定区域内的车辆提供服务,而不希望被其他公司的出租车或者该公司在其他区域内的出租车获取,那么采用组合策略树加密信息将能够很好地解决该问题. 如图 3 所示,在进行数据加密的过程中,采用动态属性和静态属性混合的方式构成访策略树,该方式能够使得策略群再次进行群组的划分,构成子策略群组,即能够提高数据的细粒度访问控制.

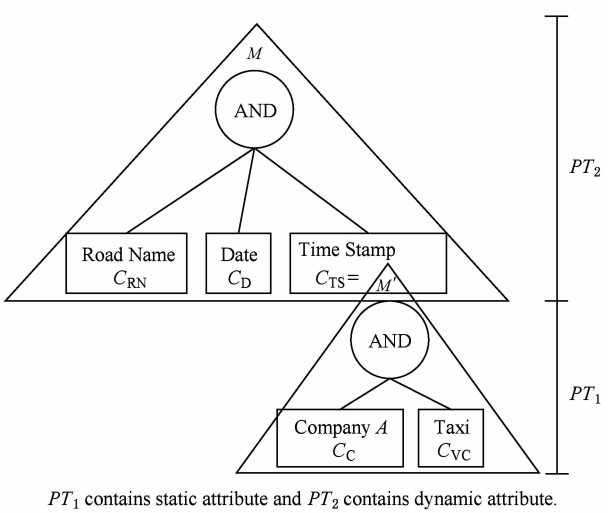

Fig. 3 Combined policy tree

图 3 组合策略树

由于该系统中动静态属性的分开管理,因此动静态属性的加密参数不同. 如图 3 所示,当应用信息的发布者使用组合策略树发布消息时,采用静态属性构建策略树 PT_1 和动态属性构建策略树 PT_2,然后将静态策略树和动态策略树再组合为一个组合策略树,使用组合策略树作为访问策略加密消息. 首先使用动态策略树 PT_2 加密消息 M 生成密文 CT_2;然后将 CT_2 中的 C_y 作为一个秘密,使用静态策略树 PT_1 进行加密;最后生成组合策略树加密的密文 CT. 具体的加密过程如下:

1) 创建静态策略树 PT_1 和动态策略树 PT_2;

2) 使用加密算法 $Encrypt(M, PK, PT_2) = CT_2$,其中 $CT_2 = \{PT_2, C, C', \{C_y, D_y\} y \in A_{dyn}\}$;

3) 随机从 CT_2 选取一个 C 作为秘密,然后使用加密算法 $Encrypt(C_y, PK, PT_1) = CT_1$,其中 $CT_1 = \{PT_1, C', C'', \{C_x, D_x\} x \in A_{sta}\}$;

4) 混合策略树中加密的密文输出为 $CT = \{CT_1; CT_2 \backslash C; PT = \{PT_1; PT_2\}\}$.

将静态策略树和动态策略树分开建立,然后再构建成组合策略树. 一方面将属性分开管理,可降低集中管理对单一节点所带来的压力,同时还可以分散集中攻击的危害性;另一方面可以更加方便地解决动态属性更新问题,减少属性更新开销.

4 关键技术实现

4.1 属性撤销

中央认证中心 GTA 是系统的核心部分,在进行属性撤销更新过程中起主导作用,撤销过程如图 4 所示. 假设 GTA 需要将一个 OBU 的属性 $attr$ 进行撤销,具体过程如下:

1) GTA 根据当前的属性 $attr$ 生成一个新的属性值 $t_{attr,v\_new} \in Z_p$,然后计算其公钥参数 $h_{attr,v_new} = H(F(t_{attr,v_new}, f(t)))$并发送给加密者,再次加密则使用新版本的公钥参数,同时将 t_{attr,v_new} 和 h_{attr,v_new} 发送到解密代理.

2) 解密代理根据 CT 的属性依赖表,从而获得所有依赖该属性 CT 的 FID 与在 CT 中对应的行号,然后通过计算获得 $D_{attr} = g^{r_i}$,并将其返回给 GTA.

3) GTA 根据 D_{attr} 生成 CT 更新密钥 $CUK = D_{attr}^{-(t_{attr\_new} - t_{attr\_old})} = g^{-r_i(t_{attr\_new} - t_{attr\_old})}$ 和用户转换密钥升级密钥 $UUK = g^{(t_{attr\_new} - t_{attr\_old}) \cdot \beta / z}$,然后发送给解密代理.

4) 解密代理对 CT 升级,即 $C_{attr} = C_{attr,old} \cdot CUK = g^{a\lambda_i} \cdot [g^{t_{attr\_new}} \cdot \rho(attr)]^{-r_i}$;对 TK 进行升级即 $K_{attr} = K_{attr,old} \cdot UUK = [g^{t_{attr\_new}} \rho(attr)]^{\beta/z}$.

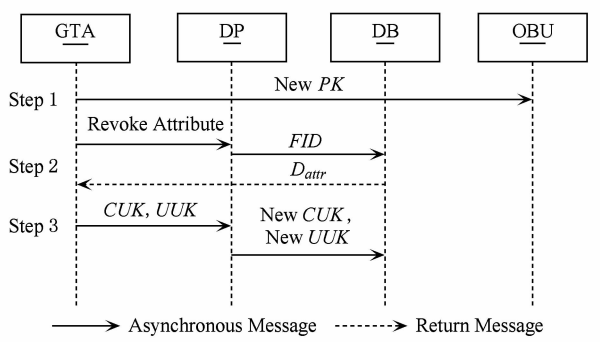

Fig. 4 The process of attribute revocation

图 4 属性撤销过程

在属性撤销的过程中,GTA 为 CT 中 $attr$ 属性的属性参数由 h_{attr,v_old} 升级到 h_{attr,v_new}. 对于未被撤销该属性的用户,GTA 为其 TK 生成升级密钥 UUK,TK 获得升级. 属性被撤销的用户由于未获得升级密钥,所以其转换密钥 TK 失效,即属性被撤销. 更加值得注意的是在属性撤销过程中,只有 GTA 和解密代理参与,并不需要车辆节点参与和对已有的 CT 进行重加密,从而降低属性更新的开销.

4.2　动态属性更新

车辆节点进入 LTA 管理区域后请求更新属性,LTA 为该车辆节点生成动态密钥参数,同时为每个动态属性赋予衰退方程,LTA 和车辆节点拥有相同的衰退方程,并且进行时间同步. 动态属性主要由 LTA 进行管理,当动态属性 A_{dyn} 需要更新时,主要步骤如下:

1) LTA 通过运行衰退方程 $F(t_{A_{\mathrm{dyn}}},f(t))$ 为 A_{dyn} 生成新的属性值,同时车辆节点运行该算法获取新的属性值,并将新的属性值和 $h_{A_{\mathrm{dyn}}}$ 发送到解密代理.

2) 解密代理根据 CT 的属性依赖表,从而获得所有依赖该属性的 CT 与在 FID 中对应的行号,然后通过计算获得 $D_{A_{\mathrm{dyn}}}=g^{r_i}$,并将其返回给 LTA.

3) LTA 根据获取到的 $D_{A_{\mathrm{dyn}}}=g^{r_i}$ 为密文和转换密钥生成更新密钥 CUK 和 UUK,然后发送给解密代理,进行动态属性相关密文和转换密钥的更新.

车联网高速移动性的特点会导致属性频繁的更新,属性同步是动态属性的重要组成部分. 车辆节点 VT 在进入一个新的 LTA 管理区域后,首先 VT 和本地 LTA 进行相互认证,认证完成后由本地 LTA 为 VT 生成动态参数和进行时钟同步. 本文将文献[17]中为每个动态属性引入的衰退方程应用到本方案中. LTA 和 VT 对同一个动态属性拥有相同的衰退方程,从而实现动态属性同步,由于不同动态属性的衰退方程中的衰退因子不同,所以动态属性的变化快慢不同. 本方案中为每个属性均赋予版本号,在动态属性每次更新的过程中对属性版本号进行递增.

4.3　代理解密

首先,解密代理测试用户的属性基 S 是否满足访问控制策略,如果满足,则在多项式时间内必定可以找到向量 $\boldsymbol{W}=(w_1,w_2,\cdots,w_l)$,$w_i\in Z_p$,并且满足 $\boldsymbol{W}\cdot\boldsymbol{M}=(1,0,0,\cdots,0)$. 由于 $\lambda_i=\boldsymbol{v}\cdot\boldsymbol{M}_i$,其中向量 $\boldsymbol{v}=[s,y_1,y_2,\cdots,y_l]^{\perp}$,因此可以求得 s,即 $\sum_{i=1}^{l}\lambda_i w_i=\sum_{i=1}^{l}\boldsymbol{v}\cdot\boldsymbol{M}_i\cdot w_i=\boldsymbol{v}\cdot\boldsymbol{M}\cdot\boldsymbol{W}=s$,否则直接输出 $CT'=\perp$.

然后,由解密代理计算出 $R=e(C',K)/E$,其中 E 是由所有的 E_i 相乘得到:

$$E=\prod_{i=1}^{l}e(C_i^{w_i},L)\cdot e(D_i^{w_i},K_{\rho(i)})=\prod_{i=1}^{l}e(g^{a\lambda_i w_i}\cdot[h_{\rho(i),v}]^{-r_i w_i},g^{\beta/z})\cdot e(g^{r_i w_i},[h_{\rho(i),v}]^{\beta/z})=e(g,g)^{(a\beta/z)\cdot\sum_{i=1}^{l}\lambda_i w_i},$$

其中,$\rho(i)\in S$ 并且 $C_i^{w_i}$ 和 $K_{\rho(i)}$ 都含有 $h_{\rho(i),v}$,所以只有 $h_{\rho(i),v}$ 的值相同时才能够消除. 由 E 和 s 带入 $R=e(C',K)/K=e(g,g)^{as/z}$,即得 $CT'=(R,C)$.

至此,解密代理的半解密过程完成. 由以上的解密过程和车载终端执行的解密算法可以看出,车辆节点在获得半解密密文后,仅仅执行一次指数运算和一次乘法运算即可完成解密,并且不会受到属性数量的影响.

5　方案分析

5.1　安全性分析

定理 1. 本文提出的可撤销动静态属性的车联网属性基加密方法是 CPA 安全的.

证明. 本文提出的属性基加密算法是文献[7]的改进,同文献[7]的不同之处有 3 点:

1) 系统公钥中与属性相关联的随机群元素,在文献[7]中采用随机数 $h_1,h_2,\cdots,h_{|U|}\in G$,而在本方案中则采用 $h_{1,v},h_{2,v},\cdots,h_{|U|,v}\in G$,其中 $\boldsymbol{v}$ 代表属性的版本号,这完全不会影响该方案的安全性;

2) 增加了属性撤销模块,在该模块中主要由 GTA 生成 CT 的更新密钥 $CUK=g^{-r_i(t_{attr\_\mathrm{new}}-t_{attr\_\mathrm{old}})}$,敌手无法从 CUK 中获取 r_i 的任何信息;

3) 增加 $Transform(CT,TK)$ 算法,该算法由解密代理服务器执行,输出 $CT'=\{R,C\}$,其中 $R=e(g,g)^{as/z}$,$C=PT\cdot e(g,g)^{as}$. 敌手想要从 CT' 中获取用户私钥 z,相当于求解离散对数问题,该求解过程是不可行的.

综上所述本文提出的 ABE-RDS 方案不会降低文献[7]的安全级别,由文献[7]提出的 CP-ABE 方案是 CPA 安全的,故本方案也是 CPA 安全的.

证毕.

定理 2. 所提方案的属性撤销功能满足前向安全性.

证明. 如果敌手拟攻击本方案的属性撤销功能,因为在进行属性撤销过程中,GTA 将为属性未撤销的车辆节点的转换密钥生成升级密钥 $UUK=g^{(t_{attr\_\mathrm{new}}-t_{attr\_\mathrm{old}})\cdot\beta/z}$,由属性撤销过程可知,$UUK$ 通常

是和用户相关的随机参数 β/z 进行绑定,该参数除 GTA 外其他任何车辆节点无法获得.所以,在属性撤销的过程中其他车辆节点无法使用其他用户的转换密钥 UUK 对自身的 TK 进行升级,在属性更新的过程中,主要由 LTA 对属性进行更新,该过程同属性的撤销相似,因此属性的更新和撤销是安全的.

证毕.

定理 3. 所提方案具有防止联合串谋的抵抗性.

证明. 代理解密的过程,通过分析本方案和方案[7]的密钥生成算法可知,本方案的 TK 即为方案[7]私钥的 z 次幂.本方案中私钥 z 由用户持有,当进行代理解密时,输出半解密密文 CT',如果解密代理想要获得明文,必须获得用户私钥,但是这是不可能的.

当解密代理和车辆节点进行串谋时,由密钥生成过程看出,车辆节点的每一个属性同随机数 β/z 进行绑定.假设车辆节点 V_1 拥有属性 $Dattr_1$ 和 V_2 拥有属性 $Dattr_2$,当 V_1 企图获得属性 $Dattr_2$ 时,则通过与 V_2 和解密代理进行串谋获得属性 $Dattr_2$,由转换密钥的结构可知,他们必须获得 h_{Dattr_2},然后计算出 $K_{V_1,Dattr_2}=[h_{Dattr_2}]^{\beta_{V_1}/z_{V_1}}$ 构成 V_1 新的转换密钥.尽管在 V_2 的转换密钥中有 $K_{V_2,Dattr_2}=[h_{Dattr_2}]^{\beta_{V_2}/z_{V_2}}$,同时能够从私钥中获得 z_{V_2} 但是无法获得 β_{V_2},因此该过程无法获得 h_{Dattr_2},则 V_1 无法获得 $Dattr_2$,所以解密代理能够抗串谋攻击.

证毕.

5.2 复杂性分析

本方案所采用的 CP-ABE 是基于文献[7]的改进,下面将本方案的空间复杂度和时间复杂度与文献[7,18-19]进行对比.在 CP-ABE 中配对运算 t_p 和指数运算 t_e 是最为耗时的 2 个运算,因此本文只讨论指数运算和配对运算.为了讨论空间复杂度(即保障加密系统的通信带宽复杂度)消耗,设一个群元素字节数为 l,访问控制策略树中属性的个数为 k,属性全集为 n,车辆节点的属性集为 m.计算本方案和文献[7,18-19]的 PK 和 CT 的空间复杂度,如表 1 所示:

Table 1 Comparison of Space Complexity

表 1 空间复杂度对比

Scheme	PK	CT
Ref[7]	$(n+3)l$	$(2k+2)l$
Ref[18]	$(n+3)l$	$(2k+2)l$
Ref[19]	$(2n+5)l$	$(3k+2)l$
Our Scheme	$(n+3)l$	$(2k+2)l$

由表 1 可以看出本方案 PK 与文献[18-19]的 PK 随着属性全集呈线性增长.在本方案中密文 CT 的长度为 $(2n+2)l$,同文献[18-19]相似,均随着访问控制策略的增加呈线性增长.

另外,车载终端解密时,向解密代理发送密文 CT,使用 $Transform$ 算法将 CT 代理解密为 CT',然后将 CT' 一起返回,用户使用 $Decrypt$ 算法进行解密获得明文信息.则来回通信数据为 $CT+CT'$,空间复杂度为 $(2k+2)l+2l=(2k+4)l$.

由第 2 节的密文生成算法 $Encrypt$ 可知,生成密文 $CT=\{C=\mathcal{M}\cdot e(g,g)^{as}, C'=g^s, \{C_i, D_i\}_{1\leqslant i\leqslant l}\}$,则有:$C=\mathcal{M}\cdot e(g,g)^{as}$ 执行 1 次指数运算,$C'=g^s$ 执行 1 次指数运算,$C_i=g^{a\lambda_i}\cdot[h_{\rho(i),v}]^{-r_i}$ 执行 2 次指数运算,$D_i=g^{r_i}$ 执行 1 次指数运算,所以本方案的解密时间为 $(2+3k)t_e$.

在解密过程中的时间开销主要包括代理解密部分解密开销 $2mt_p+mt_e$ 和车载终端解密开销 t_e.属性基加解密计算复杂度对比如表 2 所示:

Table 2 Comparison of Time Complexity

表 2 时间复杂度对比

Scheme	Encryption	Decryption
Ref[7]	$(2+3k)t_e$	$(m+1)t_p+mt_e$
Ref[18]	$(2+3k)t_e$	$2t_p+2mt_e$
Ref[19]	$(k^2+3k+2)t_e$	$(3m+1)t_p+mt_e$
Our Scheme	$(2+3k)t_e$	t_e

由表 2 可知,本方案的加密性能与文献[18-19]相当;采用代理机制之后,车辆终端的计算复杂度明显降低,与文献[7,18-19]相比具有明显优势.

6 实验与结果

6.1 实验环境

实验软件基于 Java 语言和 JPBC 库,手机端编程采用 Android.考虑到车辆节点的计算性能存在差异,采用笔记本电脑和手机分别模拟高性能和低性能车载终端.实验硬件环境包括 1 台曙光 W5801-G10 服务器(CPU:2 * Intel Xeon E5-2630(6 cores, 2.3 GHz), Memory: 64 GB)、1 台联想 ThinkPad E450c 笔记本电脑和 1 部手机,并且在曙光服务器上配置 3 台 VMware 的虚拟机作为 GTA,LTA 和 DP,具体配置如表 3 所示:

Table 3　Configuration of Device

表 3　设备配置

Component	Device Type	Configuration
GTA	Virtual Machine	CPU:two cores Memory:4 GB
LTA	Virtual Machine	CPU:two cores Memory:4 GB
DP	Virtual Machine	CPU:four cores Memory:8 GB
High-Vehicular	Lenovo ThinkPad E450c	CPU:two cores Memory:4 GB
Low-Vehicular	Huawei Y635-CL00	CPU:Snapdragon 410 Memory:1 GB
Router	TP-Link WR742N	Bandwidth:150 Mbps

6.2　解密性能

解密性能实验在动态策略树以及组合策略树 2 种条件下进行,本方案的解密性能测试包括了完整地从车载终端提交解密请求到代理,代理返回中间结果,然后在车载终端完成最终解密的全过程. 车载终端包括高性能和低性能,比较的 ABE 算法包括传统 CP-ABE 和本方案.

6.2.1　动态策略树下的解密时间对比

车载终端在获取仅有动态属性构成的访问策略树加密的资源时,使用传统 CP-ABE 解密算法和本方案解密的时间对比如图 5 和图 6 所示:

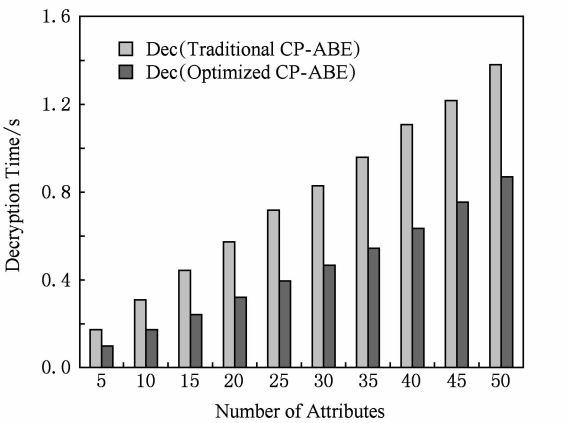

Fig. 5　High-vehicular decryption time comparison under various attributes

图 5　高性能车载终端在不同加密属性数下解密时间比较

由图 5 和图 6 可知,随着 CT 中属性个数的增多,使用代理解密的优势更加突出,在拥有较高计算性能的车载终端,当 CT 中属性个数增加到 50 个时,解密时间降低了 0.6 s;计算能力较差的车载终端随着 CT 中属性个数的增加,则增速更加明显,增速比最高达到将近 27 倍.

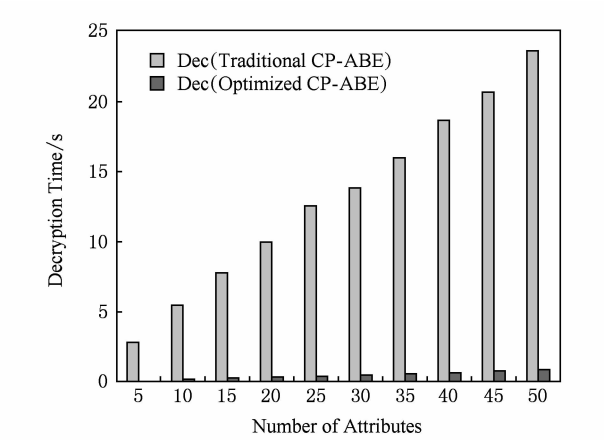

Fig. 6　Low-vehicular decryption time comparison under various attributes

图 6　低性能车载终端在不同加密属性个数下解密时间比较

6.2.2　组合策略树下的解密时间对比

如果车辆获取到的应用资源采用组合策略树构成的访问控制策略,在解密过程中使用传统 CP-ABE 解密和使用本方案的解密时间对比如图 7 和图 8 所示:

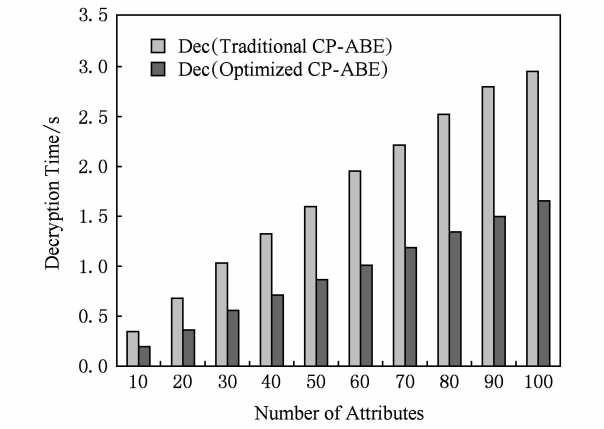

Fig. 7　High-vehicular decryption time comparison under various attributes

图 7　高性能车载终端在不同加密属性数下解密时间比较

由图 7 和图 8 可以看出,同策略群中仅使用动态属性加密的资源相似. 当 CT 中属性个数增加时,采用解密代理进行解密的优势越发显得突出,尤其是在计算性能较低的车辆节点中,当 CT 中相关的属性个数达到 100 个时,在性能较低的车辆节点中的解密加速比将近 30 倍.

通过分析 CP-ABE 的解密算法可知,传统的属性基解密算法中进行配对运算的次数同 CT 中属性的个数成正比,在 CT 中随着属性个数的增加,解密

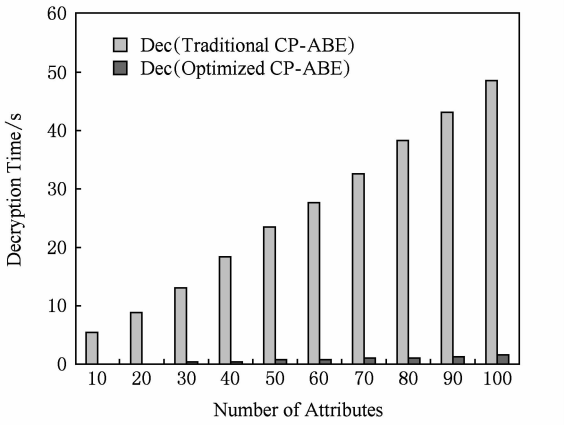

Fig. 8 Low-vehicular decryption time comparison under various attributes

图 8 低性能车载终端在不同加密属性个数下解密时间比较

时间将会呈线性增长,但是在本方案中采用解密代理对 CT 预解密后获得 CT',之后所有的配对运算等复杂运算都将在解密代理上执行,而在车辆节点上只需进行简单的乘法等运算即可对 CT' 进行解密获得对称加密密钥,所以随着属性个数的增加,采用解密代理的 CP-ABE 解密优势将会更加明显,尤其是在当计算能力较差的车辆节点中,使用该方案将会有更明显的加速效果.

6.3 属性撤销性能

改变车辆节点数目和属性数,分析属性撤销的性能如表 4 所示:

Table 4 Attribute Revocation Time Under Various Vehiculars and CTs

表 4 不同用户和 CT 数的属性撤销时间

CT: Vehicular	Revocation Time/s	CT: Vehicular	Revocation Time/s
20:10	1.474	120:60	3.597
40:20	1.647	140:70	3.863
60:30	2.021	160:80	4.262
80:40	2.509	180:90	4.676
100:50	3.172	200:100	5.117

通过表 4 可以看出,随着 CT 和用户数量的增加,属性撤销的时间呈线性增长.通过分析以上属性撤销算法可知,在属性撤销过程中,GTA 要为密文 CT 和解密代理的 TK 生成更新密钥,由于生成更新密钥的算法的时间复杂度是固定的,所以随着车辆节点和 CT 数的增加,属性撤销时间定会呈线性增长,这同实验结果是一致的.该过程对于车辆节点来说几乎是透明的,极大地方便了属性的撤销.

6.4 并发性能分析

使用 LoadRunner 测试工具对解密代理和动态属性密钥参数生成的并发处理能力进行测试.

6.4.1 动态密钥生成并发

动态密钥参数生成并发测试是针对车辆进入到一个新的 LTA 管理范围,同时向 LTA 请求同步新的动态属性并且生成新的动态密钥.该并发测试的并发用户有 5～25,并且分别拥有 10 个动态属性,在不同的并发用户情况下,LTA 的响应时间如表 5 所示:

Table 5 Dynamic Key Generation Time Under Various Concurrent Numbers

表 5 不同并发数下动态密钥生成时间

Concurrent	Generation Time/s	Concurrent	Generation Time/s
5	1.474	20	2.509
10	1.647	25	3.172
15	2.021		

当同时由 15 个车辆节点请求更新动态属性时,LTA 的响应时间为 2.021 s,在实际情况中,双向八车道能够同时有 8 车辆节点请求更新属性,LTA 的响应时间将在 1.5 s 以内,如果设定一个 LTA 管理区域通过时间在 30 min 左右,显然单个 LTA 就能满足管理要求.另外,因为整个系统是采用分布式的方式部署,可以分散 LTA 节点计算压力,有效解决 LTA 的高并发问题.

6.4.2 解密并发

解密代理并发测试针对并发车辆数有 5～25,并且密文 CT 中包含有 10 个属性,在不同并发用户的情况下,解密代理的响应时间如表 6 所示:

Table 6 Decryption Time Under Various Concurrent Numbers

表 6 不同并发数下解密时间

Concurrent	Decryption Time/s	Concurrent	Decryption Time/s
5	0.279	20	0.925
10	0.494	25	1.039
15	0.705		

由表 6 可知,当同时有 5 个车辆节点向同一个解密代理请求解密时,响应时间仅为 279 ms,随着请求解密代理的车辆节点的增多,当并发解密请求

达到25时,响应时间也在1s左右.考虑到解密代理的部署也是按分布式的方式部署,当单个解密代理性能不足时,可以增加新的解密代理,即可认为解密代理的计算资源是巨大的,具有良好的可扩展性.因此解密代理通过分散节点压力,可以进一步提高并发解密速度,满足更多车辆节点的解密任务.

7 总　　结

为保护车联网通信安全,特别是为了实现车联网中的云存储数据安全分享,本文面向车联网设计了一种可撤销动静态属性的属性基加密算法.针对车联网的高移动等特点,将动态属性和静态属性分开管理,构建组合策略树,能够方便群组的构建和管理.引入解密代理将高复杂度的属性基解密过程的大量计算放在服务端,降低了车辆节点的解密时间,满足车联网的实际要求.车辆节点通过中央认证中心可以方便地进行属性撤销,进入LTA管理区域后可以进行动态属性更新.通过与其他CP-ABE方案进行时间复杂度和空间复杂度分析,证明本方案解密速度要优于其他CP-ABE方案,进一步构建实验系统,模拟高、低性能车载终端,验证了系统的有效性,适合在车联网中应用.

参 考 文 献

[1] Xie Yong, Wu Libing, Zhang Yubo, et al. Anonymous mutual authentication and key agreement protocol in multi-server architecture for VANETs [J]. Journal of Computer Research and Development, 2016, 53(10): 2323-2333 (in Chinese)
(谢永,吴黎兵,张宇波,等. 面向车联网的多服务器架构的匿名双向认证与密钥协商协议[J]. 计算机研究与发展, 2016, 53(10): 2323-2333)

[2] Lin Hongliang, Huang Xiaopeng. Summarization of vehicle networking technology [J]. Mechatronics Engineering, 2014, 31(9): 1235-1238 (in Chinese)
(蔺宏良,黄晓鹏. 车联网技术研究综述[J]. 机电工程, 2014, 31(9): 1235-1238)

[3] Feng Dengguo, Zhang Min, Zhang Yan, et al. Study on cloud computing security [J]. Journal of Software, 2011, 22(1): 71-83 (in Chinese)
(冯登国,张敏,张妍,等. 云计算安全研究[J]. 软件学报, 2011, 22(1): 71-83)

[4] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data [C] //Proc of the 13th ACM Conf on Computer and Communications Security. New York: ACM, 2006: 89-98

[5] Sampigethaya K, Huang L, Li M, et al. CARAVAN: Providing location privacy for VANET [C] //Proc of the 3rd Workshop on Embedded Security in Cars (ESCAR 2005). Cologne, Germany: ESCAR, 2005 [2017-05-10]. https://www.ee.washington.edu/research/nsl/papers/ESCAR-05.pdf

[6] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption [C] //Proc of the 2007 IEEE Symp on Security and Privacy. Los Alamitos, CA: IEEE, 2007: 321-334

[7] Waters B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization [C]// Proc of the 14th Int Conf on Practice and Theory in Public Key Cryptography. Berlin: Springer, 2011: 53-70

[8] Shamir A. Identity-based cryptosystems and signature schemes [G] //LNCS 196: Proc of CRYPTO'84. Berlin: Springer, 1984: 47-53

[9] Dan B, Franklin M K. Identity-based encryption from the Weil pairing [C] //Proc of CRYPTO 2001. Berlin: Springer, 2001: 213-229

[10] Shamir A. How to share a secret [J]. Communications of the ACM, 1979, 22(11): 612-613

[11] Zhang Jiang, Zhang Zhenfeng. A ciphertext policy attribute-based encryption scheme without pairings [C] //Proc of Int Conf on Information Security and Cryptology. Berlin: Springer, 2012: 324-340

[12] Chen Dongdong, Cao Zhenfu, Dong Xiaolei. Online/offline ciphertext-policy attribute-based searchable encryption [J]. Journal of Computer Research and Development, 2016, 53(10): 2365-2375 (in Chinese)
(陈冬冬,曹珍富,董晓蕾. 在线/离线密文策略属性基可搜索加密[J]. 计算机研究与发展, 2016, 53(10): 2365-2375)

[13] Pirretti M, Traynor P, Mcdaniel P, et al. Secure attribute-based systems [J]. Journal of Computer Security, 2010, 18(5): 799-837

[14] Hur J, Noh D K. Attribute-based access control with efficient revocation in data outsourcing systems [J]. IEEE Trans on Parallel & Distributed Systems, 2010, 22(7): 1214-1221

[15] Xie Xingxing, Ma Hua, Li Jin, et al. An efficient ciphertext-policy attribute-based access control towards revocation in cloud computing [J]. Journal of Universal Computerence, 2013, 19(16): 2349-2367

[16] Fan Chunyi, Huang Shiming, Rung Heming. Arbitrary-state attribute-based encryption with dynamic membership [J]. IEEE Trans on Computers, 2013, 63(8): 1951-1961

[17] Chen Nanxi, Gerla M, Huang Dijiang, et al. Secure, selective group broadcast in vehicular networks using dynamic attribute based encryption [C] //Proc of Ad Hoc Netw Workshop. Piscataway, NJ: IEEE, 2010: 1-8

[18] Hohenberger S, Waters B. Attribute-based encryption with fast decryption [C] //Proc of Public-Key Cryptography (PKC 2013). Berlin: Springer, 2013: 162-179

[19] Deng Hua, Wu Qinghong, Qin Bo, et al. Ciphertext-policy hierarchical attribute-based encryption with short ciphertexts [J]. Information Sciences, 2014, 275(11): 370-384

He Qian, born in 1979. PhD, professor. Senior member of CCF. His main research interests include cloud service, distributed computing, and information security.

Liu Peng, born in 1990. MSc candidate. Student member of CCF. His main research interests include distribution computing, and information security.

Wang Yong, born in 1963. PhD, professor, PhD supervisor. Member of CCF. His main research interests include computer network technology and application, cloud computing, information security.

《计算机研究与发展》征订启事

《计算机研究与发展》(Journal of Computer Research and Development)是中国科学院计算技术研究所和中国计算机学会联合主办、科学出版社出版的学术性刊物,中国计算机学会会刊. 主要刊登计算机科学技术领域高水平的学术论文、最新科研成果和重大应用成果. 读者对象为从事计算机研究与开发的研究人员、工程技术人员、各大专院校计算机相关专业的师生以及高新企业研发人员等.

《计算机研究与发展》于 1958 年创刊,是我国第一个计算机刊物,现已成为我国计算机领域权威性的学术期刊之一. 并历次被评为我国计算机类核心期刊,多次被评为“中国百种杰出学术期刊”. 此外,还被《中国学术期刊文摘》、《中国科学引文索引》、“中国科学引文数据库”、“中国科技论文统计源数据库”、美国工程索引(Ei)检索系统、日本《科学技术文献速报》、俄罗斯《文摘杂志》、英国《科学文摘》(SA)等国内外重要检索机构收录.

国内邮发代号:2-654;国外发行代号:M603

国内统一连续出版物号:CN11-1777/TP

国际标准连续出版物号:ISSN1000-1239

联系方式:

100190 北京中关村科学院南路 6 号《计算机研究与发展》编辑部

电话: +86(10)62620696(兼传真);+86(10)62600350

Email:crad@ict.ac.cn

http://crad.ict.ac.cn