doi:10.11959/j.issn.1000-436x.2016271

抵抗 SNS 好友攻击的位置隐私保护方案

林曦，韩益亮，柯彦，杨晓元
（武警工程大学电子技术系，陕西 西安 710086）

摘 要：为了丰富用户的位置信息的表现模式，适应多样化的用户需求，基于属性加密设计了一种支持精确、较精确、模糊以及不公开位置信息共 4 种模式的位置隐私保护方案。以 WT-CP-ABE 算法为基础，将位置信息根据好友的亲密度等级分成 3 个部分。采用属性加密和对称加密的方法分别对密钥信息和位置信息进行加密，在社交网络上发布。对方案的安全性进行分析，表明方案具有用户属性信息机密性、数据机密性和可抵抗合谋攻击的优点。
关键词：社交网络；位置；隐私保护；属性加密
中图分类号：TP309 **文献标识码**：A

Location privacy preserving scheme against attack from friends in SNS

LIN Xi, HAN Yi-liang, KE Yan, YANG Xiao-yuan
(Department of Electronic Technology, Engineering College of the Chinese Armed Police Force, Xi'an 710086, China)

Abstract: In order to enrich the performance of the user's location information and to meet the diverse needs of users, a location privacy protection scheme based on attribute encryption was designed, which provided precise, more accurate, fuzzy and private four modes to manage the location information. The scheme was based on the algorithm of WT-CP-ABE. The location information was divided into three parts according to a close friend of grade, then the key information and position information was encrypted with attribute-based encryption and symmetric encryption method respectively and the ciphertext was published to the social network. The security of the scheme is analyzed, which shows that the scheme has the advantage of user attribute information confidentiality, data confidentiality and can resist the collusion attack.
Key words: social network, location, privacy protection, attribute-based encryption

1 引言

移动社交网络是一个建立在一定社交关系上的在线平台。在移动社交网络中，用户可以与家人、好友分享自己的兴趣、爱好、状态和日常活动等信息，加强彼此联系，维系深厚感情，利用手机等智能设备中的定位技术，分享自己的位置信息，获取各种基于位置的服务(LBS, location based service)。

然而，就在人们享受定位技术带来各种便利的同时，个人位置隐私也遭受着泄露的严重威胁[1]。对于个人位置隐私的保护，目前主要有空间位置隐匿技术和假位置技术[2,3]这 2 类方法。其中，位置 k-匿名模型[4]是最常用的一种空间位置隐匿技术，当需要用户提供个人位置信息时，它将一个足够大的区域(模糊区域)中的 k 个用户的位置都发给 SP(service provider)，因此，服务端无法分辨出用户真正的位置所在。假位置技术则是通过生成一些假位置，然后将真实位置和生成的假位置同时发送给服务器，以达到用户位置信息的隐匿[2]。以上这些位置隐私保护方法都将攻击者定位在 LBS 服务商，没有考虑到攻击者也可能是用户的好友。

事实上，并不是所有的好友都是可信的，用户

收稿日期：2016-09-15
基金项目：国家自然科学基金资助项目（No.61572521, No.61272492, No.61272486）；陕西省自然科学基础研究计划基金资助项目（No.2015JM6353）
Foundation Items: The National Natural Science Foundation of China (No.61572521, No.61272492, No.61272486), The Natural Science Basic Research Program of Shaanxi Province (No.2015JM6353)

的好友列表中也可能存在潜在的攻击者[5]。因此，如果用户对网络中的所有好友都无差别地发布精确位置，则必然会造成个人隐私的泄露，从而有可能使用户受到安全威胁。目前，大多数社交软件（如微信、Twitter）在用户发布状态时，都提供了“可见范围”的选项，但是，它事实上只提供了公开和不公开这 2 个选择，无法实现对一部分好友公开自己精确的位置信息，而对一部分好友公开模糊或者不精确的位置信息。因此，本文提出一种基于属性加密的位置隐私保护方案，移动社交网络用户可以根据好友的不同亲密度级别选择精确、较精确、模糊以及不公开这 4 种模式，让处于不同亲密度等级的好友看到不同精确度的位置。同时，本文方案还具有可撤销性、用户属性信息机密性、数据机密性和可抵抗合谋攻击的优点。

2　预备知识

2.1　双线性映射

如果阶为大素数 p 的乘法群 G_1、G_2，满足：1) 双线性：当 $\forall u$，$v\in G_1$ 和 $\forall a$，$b\in Z_p$，那么有 $e(u^a,v^b)=e(u,v)^{ab}$；2) 非退化性，$\exists u$，$v\in G_1$，使 $e(u,v)\neq 1$；3) 可计算性，$\forall u$，$v\in G_1$，都能在一个多项式时间内计算出 $e(u,v)$。则称映射 $e:G_1\times G_1\rightarrow G_2$ 为双线性映射[6]。

2.2　基于密文策略的属性加密(CP-ABE)

本文采用基于密文策略的属性加密（CP-ABE）对对称密钥信息文件进行加密。方案定义全体属性集合 A 为 $\{1,2,\cdots,k\}$，S 为 A 的非空子集，P 为由“AND”“OR”等逻辑词组成的属性策略。CP-ABE 常用的访问控制策略有基于访问树结构[7]以及基于线性秘密共享[8,9]这 2 类。本文采用线性秘密共享进行访问控制，具体过程为：1) 将属性策略 P 用 $(\boldsymbol{M},\rho)$ 表示，$\boldsymbol{M}$ 为 $l\times h$ 的矩阵，ρ 为单射函数，当 $i=1,\cdots,l$，$\rho(i)$ 代表 $\boldsymbol{M}$ 中第 i 行所关联的属性；2) 当集合 S 满足属性策略 P 时，即 $I=\{i|P(i)\in S\}$，则可由此计算出一个满足 $\sum_{i\in I}\theta_i\vec{\boldsymbol{M}}_i=\{1,0,\cdots,0\}$ 常系数组 $\{\theta_i\in Z_p\}$，其中，$\vec{\boldsymbol{M}}_i$ 是 $\boldsymbol{M}$ 第 i 行组成的向量，如果 S 不满足属性策略 P，则不存在这组常系数；3) 隐藏所要共享的秘密，假设 $s\in Z_p$ 为需要共享的秘密，则随机选取 h–1 个值 $v_2,v_3,\cdots,v_h\in Z_p$，与 s 共同构成 h 维的向量 $\vec{\boldsymbol{v}}=(s,v_2,\cdots,v_h)$，计算内积 $\lambda_i=\vec{\boldsymbol{M}}_i\vec{\boldsymbol{v}}$ $(i=1,2,\cdots,l)$，λ_i 为秘密共享值，当且仅当属性集合 S 满足属性策略 P 时，才能计算出秘密 $s=\sum_{i\in I}\theta_i\lambda_i$。

2.3　令牌树机制

2.3.1　令牌树

本文方案构造了一棵深度为 D 的完全二叉树作为令牌树，其中，1~(D−1)每层的节点数都达到最大 2^{D-1}，D 层的节点都集中在最左侧。树的每一条边都对应一个令牌，每个节点都有相应的随机密钥，每个叶子节点对应系统中一个用户。方案定义 Φ_x 为与属性群 $G(x)$中用户对应的令牌树叶子节点的集合，Ψ_x 为能覆盖 Φ_x 的最小节点集合，则与集合 Ψ_x 中节点相对应的所有随机密钥的集合称为属性 x 的最小覆盖密钥集(MCKS，minimum cover key set)，记作 $MCKS_x$。如果 n_i 表示令牌树中的一个叶子节点，方案定义与从 n_i 到根经过的节点（包括根节点以及叶子节点 n_i）所对应的全部随机密钥的集合为节点 n_i 的密钥链集(KCS，key chain set)，记作 KCS_i，定义从 n_i 到根节点所经过的令牌的集合为节点 n_i 的令牌链集(TCS，token chain set)，记作 TCS_i。

2.3.2　令牌树机制

本文方案将令牌树上的每一个叶子节点都对应系统中的一个用户 u_t，将叶子节点的随机密钥作为用户私钥的 TDKey，依靠令牌树中 3 个定理确保令牌树机制的安全性：1) 如果知道叶子节点 n_i 所对应的随机密钥以及它到根所经过的所有边的令牌，那么可以计算得到 n_i 对应的密钥链集 KCS_i；2) 如果只知道叶子节点 n_i 所对应的随机密钥，那么就算得到令牌树的所有令牌，也无法得到除 n_i 到根所经过的节点以外的任意节点所对应的随机密钥；3) 如果 n_t 表示与任意用户 u_t $(1\leqslant t\leqslant m)$相对应的叶子节点，那么当 $u_t\in G(x)(1\leqslant x\leqslant k)$时，有且只有一个元素使 n_t 对应的 KCS_i 与 $G(x)$对应的 $MCKS_x$ 相交。

3　方案设计

3.1　系统模型

隐私保护社交网络系统 PPSNS 如图 1 所示。与文献[10,11]方案类似，假设属性权威机构（AA）是可信的，负责初始化系统，生成与分发用户私钥以及管理用户属性。社交网络服务提供者（SNSP）负责存储数据属主（DO）发布的位置信息以及为用户提供社交网络应用服务。DO 负责生成及分发属主主私钥，确定数据加密所采用的属性策略。当访问者

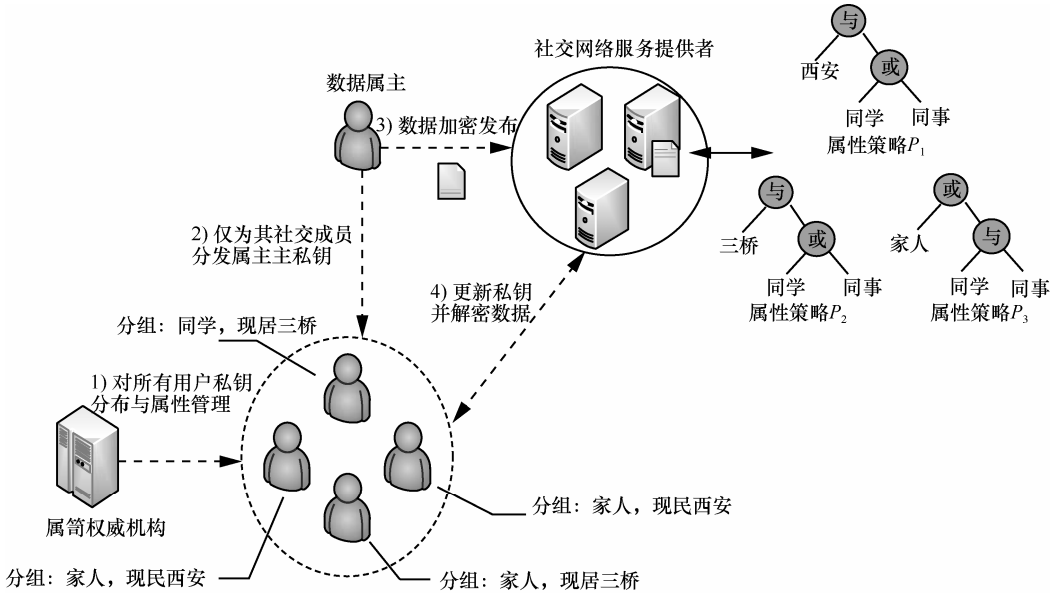

图 1 隐私保护社交网络系统

访问 DO 的数据时，访问者需要用 DO 的属主主私钥更新自己的私钥，当且仅当访问者的属性满足加密的属性策略时，访问者才能正确解密数据。

3.2 定义

定义 1 属性群。用户集合 $U=\{u_1,\cdots,u_m\}$，属性集合 A={1,2,$\cdots$,k}，那么定义属性群 $G(x)$为具有 x 属性的所有用户的集合。

定义 2 属性陷门。如果每个属性 $x\in A$ 都有一个相应的属性陷门 TD_x，那么当且仅当用户 $u_t\in G(x)$ 时，用户才能得到 x 相应的属性陷门 TD_x。

定义 3 位置信息。将 DO 的位置信息 m 分成 m_1、m_2、m_3 共 3 个部分，例如，将 m=陕西省西安市三桥镇七天酒店，划分成 m_1=陕西省西安市、m_2=三桥镇、m_3=七天酒店。

定义 4 亲密度等级。根据用户与 DO 的关系情况（陌生人、普通、友好、亲密），可以划分为 4 个亲密度等级 *rank*，记为 0、1、2、3。设置产生 3 种属性策略 P_1、P_2、P_3，若用户与 DO 的亲密度为普通，则 *rank*=1 且用户的属性集 S 满足策略 P_1，亲密度为友好，则 *rank*=2 且 S 满足策略 P_2，亲密度为亲密，则 *rank*=3 且 S 满足策略 P_3。

3.3 算法设计

本文算法将待加密数据分成位置信息和密钥信息 2 个部分，位置信息使用传统对称加密的方法进行加密，密钥信息使用 WT-CP-ABE[12]算法进行属性加密。其中，WT-CP-ABE 算法是以 CP-ABE 为基础，由 AA 与 DO 协同完成密钥生成，同时嵌入属性陷门，添加了属性撤消的功能。具体算法由 *Setup*() 、 *KeyGen*() 、 *EncryptM*() 、 *EncryptK*() 、 *KeyUpdate* ()、*DecryptK* ()、*DecryptM* ()这 7 个子函数组成。

1) *Setup*(1^λ)

根据给定安全参数 1^λ，AA 选择一个阶为 p，生成元为 g 的乘法群 G_1，则具有双线性映射 e：$G_1\times G_1\to G_2$。定义系统的属性集合 A={1,2,$\cdots$,k}，对于属性 $x\in A$ ($1\leqslant x\leqslant k$)，随机选择 η_x，$TD_x\in Z_p$，计算 $T_x=g^{\eta_x TD_x}$。随机选择 $\beta\in Z_p$，生成系统主私钥 $ASK=<\beta,\{TD_x\}>$，并发布公开密钥 $APK=<G_1, g, g^\beta, \{T_x\}_{x\in A}>$。最后，由 DO 随机选择 $\alpha\in Z_p$，计算用户主私钥 $OSK=<g^\alpha>$，发布用户公开密钥 $OPK=<e(g,g)^\alpha>$。

2) *KeyGen*(*ASK*,*S*)

使用主私钥 *ASK* 生成属性集对应的私钥。随机选择 $t\in Z_p$，计算 $D=g^{\beta t}$，$L=g^t$。计算任意属性 $x\in S$ 对应的 $D_x=T_x^{\frac{t}{TD_x}}=g^{\eta_x t}$。随机选择陷门密钥 *TDKey*，组成用户私钥 $SK=<D,L,\{D_x\}_{x\in S}, TDKey>$。其中，为避免属性合谋攻击，在 D_x 中引入随机数 t，随机化用户私钥。使用陷门密钥 *TDKey* 可以恢复相应的属性陷门。

3) *EncryptM*(m,k_1,k_2,k_3)

使用对称加密方法对位置信息 m 进行加密。首先，选择 3 组随机产生的对称密钥 k_1、k_2、k_3，接

着，按照 3.2 节的定义将位置信息 m 分成 m_1、m_2、m_3，分别以 k_1、k_2、k_3 为密钥对 m_1、m_2、m_3 进行对称加密，得到 $E_{k_1}(m_1)$、$E_{k_2}(m_2)$、$E_{k_3}(m_3)$。输出位置信息的密文 CM 如下

$$CM=<E_{k_1}(m_1),E_{k_2}(m_2),E_{k_3}(m_3)>$$

4) *EncryptK*(*APK*,*OPK*, P_{rank}, K_{rank})

使用公开密钥 APK、OPK 和属性策略 P_{rank} 加密对称密钥信息 K_{rank}。首先，DO 可以根据普通、友好、亲密这 3 种亲密度等级，设置 3 种属性策略 P_1、P_2、P_3。

根据文献[8]确定可代表属性策略 P_{rank} 的$(\boldsymbol{M},\rho)$，$rank\in\{1,2,3\}$，其中，$\boldsymbol{M}$ 为 $l\times h$ 的矩阵，ρ 为单射函数。然后，随机选择 h 维向量 $\vec{\boldsymbol{v}}=(s,v_2,\cdots,v_h)\in Z_p$，并计算 $\tilde{C}=K_{rank}e(g,g)^{\alpha s}$，$C=g^s$。对于任意 $i\in\{1,2,\cdots,l\}$，令为 $\vec{\boldsymbol{M}}_i$ 为 $\boldsymbol{M}$ 第 i 行所组成的向量，计算 $\lambda_i=\vec{\boldsymbol{M}}_i\vec{\boldsymbol{v}}$。然后，选择随机数 $r_1,\cdots,r_l\in Z_p$，计算 $C_i=g^{\beta\lambda_i}T_{\rho(i)}^{-r_i}$，$C_i'=g^{r_i}$。输出的密文 CK_{rank} 为

$$CK_{rank}=<(\boldsymbol{M},\rho),\tilde{C},C,\{C_i,C_i'\}_{i\in\{1,2,\cdots,l\}}>$$

在密文中，每个属性对应的 C_i 都由 $T_{\rho(i)}$ 计算得到，而只有得到属性陷门 $TD_{\rho(i)}$ 才能计算出 $T_{\rho(i)}$。因此，当且仅当得到密文中的属性陷门 $TD_{\rho(i)}$ 才能解密密文。

当 *rank* 分别为 1、2、3 时，以属性策略 P_1、P_2、P_3 进行加密，K_1、K_2、K_3 分别为 k_1、$k_1\|k_2$、$k_1\|k_2\|k_3$，经计算可以得到 CK_1、CK_2、CK_3，组成密钥信息的密文为

$$CK=<CK_1,CK_2,CK_3>$$

5) *KeyUpdate*(*OSK*,*SK*)

使用 *OSK* 更新私钥 *SK*。更新后的 *SK* 为

$$SK=<D=g^{\alpha}g^{\beta t},L,\{D_x\}_{x\in S},TDKey>$$

6) *DecryptK*(*SK*,*CK*)

解密密钥信息的密文 CK_{rank}。当且仅当私钥 *SK* 的属性集合 S 满足加密 CK_{rank} 时所采用的属性策略 P_{rank} 时，用户才能解密得到密钥信息。令 $I=\{i|\rho(i)\in S\}$，$W=\{\rho(i)|\rho(i)\in S\}$，假设已经通过陷门密钥 TDKey，计算得到任意属性 $\rho(i)\in$W 对应的属性陷门 $TD_{\rho(i)}$。

首先，使用文献[8]中的方法计算得到一组常系数 $\{\theta_i\}_{i\in I}$，使 $\sum_{i\in I}\theta_i\lambda_i=s$。接着，计算

$$\begin{aligned}&\prod_{i\in I}(e(C_i,L)e(C_i',D_{\rho(i)}^{TD_{\rho(i)}}))^{\theta_i}\\&=\prod_{i\in I}(e(g^{\beta\lambda_i}g^{-r_i\eta_{\rho(i)}TD_{\rho(i)}},g^t)e(g^{r_i},g^{\eta_{\rho(i)}tTD_{\rho(i)}}))^{\theta_i}\\&=e(g,g)^{t\beta\sum_{i\in I}\lambda_i\theta_i}\\&=e(g,g)^{t\beta s}\end{aligned}$$

最后，将 $e(g,g)^{t\beta s}$ 代入，可得

$$K_{rank}=\frac{\tilde{C}}{\dfrac{e(g^s,g^{\alpha}g^{\beta t})}{e(g,g)^{t\beta s}}}$$

当 *SK* 关联的属性集 S 都不满足 CK_1、CK_2、CK_3 中 $(\boldsymbol{M},\rho)$ 所代表的属性策略 P_1、P_2、P_3 时，此时无法得到 K_{rank}；当 *SK* 关联的属性集 S 满足 CK_1 中 $(\boldsymbol{M},\rho)$所代表的属性策略 P_1 时，此时可以得到 K_1；当 *SK* 关联的属性集 S 满足 CK_2 中$(\boldsymbol{M},\rho)$所代表的属性策略 P_2 时，此时可以得到 K_2；当 *SK* 关联的属性集 S 满足 CK_3 中$(\boldsymbol{M},\rho)$所代表的属性策略 P_3 时，此时可以得到 K_3。

7) *DecryptM*(K_{rank},*CM*)

从密钥信息 K_{rank} 中得到的对称密钥 k_1、k_2、k_3，解密位置信息密文 *CM*。当得到 K_1 时，由于 $K_1=k_1$，因此，可以用密钥 k_1 解密 *CM* 中的 $E_{k_1}(m_1)$。使用 $D_{k_1}(E_{k_1}(m_1))$ 得到模糊位置信息 m_1；当得到 K_2 时，由于 $K_2=k_1\|k_2$，因此可以用密钥 k_1、k_2 解密 *CM* 中的 $E_{k_1}(m_1)$ 和 $E_{k_2}(m_2)$。使用 $D_{k_1}(E_{k_1}(m_1))$，$D_{k_2}(E_{k_2}(m_2))$ 得到较精确位置信息 $m_1\|m_2$；当得到 K_3 时，由于 $K_3=k_1\|k_2\|k_3$，因此可以用密钥 k_1、k_2、k_3 解密 *CM* 中的 $E_{k_1}(m_1)$、$E_{k_2}(m_2)$ 和 $E_{k_3}(m_3)$。使用 $D_{k_1}(E_{k_1}(m_1))$，$D_{k_2}(E_{k_2}(m_2))$，$D_{k_3}(E_{k_3}(m_3))$ 得到精确位置信息 $m_1\|m_2\|m_3$。

3.4　方案描述

系统初始化。AA 根据所选择的安全参数 1^{λ}，运行 *Setup*(1^{λ})，得到系统主私钥 *ASK* 和公开密钥 *APK*。然后，由各个 DO 与 AA 共同生成自己的主私钥 *OSK* 以及公开密钥 *OPK*。

新用户注册。当新用户 u_t 加入社交网络时，AA 根据 u_t 的信息生成对应的属性集 S，执行 *KeyGen*(*ASK*,*S*)生成与属性集 S 相关联的私钥 *SK*，然后将 *SK* 分发给 u_t。此外，AA 还需要根据用户的属性情况，构建相应的属性群。若用户 u_1、u_2、u_3 的属性集分别为{1,2}、{1,2,3}、{2,3}，那么相应的属性群

为 $G(1)=\{u_1, u_2\}$、$G(2)=\{u_1, u_2, u_3\}$、$G(3)=\{u_2, u_3\}$。

陷门信息发布。AA 根据第 2.3 节的方法建立一棵令牌树，树上的每一个叶子节点都对应系统中的一个用户，叶子节点的随机密钥为用户私钥的 *TDKey*。根据属性 $x\in A(1\leqslant x\leqslant k)$的属性群 $G(x)$确定最小覆盖密钥集 $MCKS_x$，计算得到陷门信息

$$TDM_x=\{E_{RK_j}(TD_x)\}_{RK_j\in MCKS_x}$$

其中，RK_j为随机密钥，TD_x为 x 对应的属性陷门，E 为一种快速的对称加密算法（如异或运算）。公开发布陷门信息 $TDM=\{TDM_x\}_{x\in A}$ 以及令牌链 $TCS=\{TCS_i\}_{i\in\{1,2,\cdots,m\}}$。

社交联系建立。DO 通过安全信道（如 SSL 协议信道）向自己的社交成员分发主私钥 *OSK*。

隐私数据发布。这里只描述 DO 对单个位置信息 m 的处理，其过程为：1) 选择 3 组随机产生的对称密钥 k_1、k_2、k_3 加密位置信息 m 的 3 个部分 m_1、m_2、m_3 得到 $E_{k_1}(m_1)$、$E_{k_2}(m_2)$、$E_{k_3}(m_3)$ (E 为符合要求的对称加密算法)，组成位置信息的密文 *CM*；2) 根据亲密度等级对应的 3 种属性策略 P_1、P_2、P_3，运行算法 *EncryptK*(*APK*,*OPK*, P_{rank}，K_{rank}) 加密对称密钥信息 K_1、K_2、K_3 得到 CK_1、CK_2、CK_3，组成密钥信息的密文 *CK*；3) 令 $V=\{\rho(i)|1\leqslant i\leqslant l\}$，计算任意属性 $x\in V$ 相应的陷门 TDM_x，组成陷门信息 $TDM_{\mathrm{DO}}=\{TDM_x\}_{x\in V}$；4) 以位置信息文件 $ID_m\|ID_{\mathrm{DO}}\|CM$ 和密钥信息文件 $ID_{\mathrm{DO}}\|TDM_{\mathrm{DO}}\|CK$ 的形式发布在社交网络中。其中，为位置信息 m 创建唯一的编号，记为 ID_m，为 DO 创建唯一的编号，记为 ID_{DO}。

数据访问。当用户 u_t 想要访问编号为 ID_m 的位置信息文件时，SNSP 根据编号 ID_{DO} 寻找对应的密钥信息文件，返回位置信息 *CM*、密钥信息 $TDM_{\mathrm{DO}}\|CK$ 和该用户的令牌链 TCS_t。用户 u_t 先对 TDM_{DO} 进行解密，得到属性陷门信息，然后，用自身的私钥 *SK* 以及解密 TDM_{DO} 得到的属性陷门对 *CK* 中的 CK_{rank} 进行解密，得到对称密钥 K_{rank}。之后，用对称密钥 K_{rank} 对位置信息文件 *CM* 进行解密，得到属主的位置信息。用户具体的解密过程如下所示。1) TDM_{DO} 解密。由 2.3 节令牌树的第一个定理可知，令牌树中的密钥链集 KCS_t 可以由用户 u_t 的私钥 *SK* 中的陷门密钥 *TDKey* 以及令牌链 TCS_t 计算得到。显然，当且仅当用户 u_t 的私钥 *SK* 的属性集合满足由($\boldsymbol{M}$,ρ)所代表的属性策略时，用户才能解密 *CK*，即对于 $W=\{\rho(i)|1\leqslant i\leqslant l$ 且 $\rho(i)\in S\}$，任意属性 $x\in W$ 以及它对应的属性群 $G(x)$，一定有 $u_t\in G(x)$。由 2.3 节令牌树的第 3 个定理可知，对于 $G(x)$的最少覆盖密钥集 $MCKS_x$，一定存在随机密钥 RK_y 满足 $RK_y\in KCS_t$ 且 $RK_y\in MCKS_x$，即用户可以用 RK_y 对 TDM_x 进行解密得到属性 x 对应的属性陷门 TD_x。因此，用户 u_t 能够解密 TDM_{DO} 得到所有属性陷门，从而可以对 *CK* 进行解密。2) *CK* 解密。用户 u_t 根据属主的 *OSK*，运行 *KeyUpdate*(*OSK*,*SK*)对私钥 *SK* 进行更新，然后，用更新后的私钥运行 *DecryptK*(*SK*,*CK*)对 *CK* 进行解密得到 K_{rank}。3) *CM* 解密。u_t 用得到的 K_{rank} 执行 *DecryptM*(K_{rank},*CM*) 对 *CM* 进行解密得到对应的位置信息。

属性撤销。当用户属性发生改变时，由 AA 实现属性撤销。定义撤销属性集合为 R，被撤销属性的用户为 u_t，具体的撤销过程如下所示。

1) AA 对属性陷门信息进行更新。对于任意属性 $x\in R$，AA 随机产生新的属性陷门 TD_x'，形成 x 新的属性群 $G(x)$，显然一定有被撤销属性的用户 $u_t\notin G(x)$。然后，重新确定最小覆盖密钥集 $MCKS_x'$，生成

$$TDM_x'=\{E_{RK_j}(TD_x')\}_{RK_j\in MCKS_x'}$$

并将 TDM_x' 代替原有的 TDM_x。

2) AA 执行 *APK* 与 *ASK* 更新。对于任意属性 $x\in R$，更新其在 *APK* 中对应的组件

$$T_x'=T_x^{\frac{TD_x'}{TD_x}}$$

替换 *ASK* 中的 TD_x 为 TD_x'。

3) DO 执行密钥信息的密文重加密。首先，随机产生新的 3 组对称加密密钥 k_1'、k_2'、k_3'，组成 K_1'、K_2'、K_3'。执行 3 次 *EncryptK*()计算得到 CK_1'、CK_2'、CK_3'，组成新的 CK'，代替原来的 *CK*。然后，更新属性群信息。更新过程为：令 $V=\{\rho(i)\,|\,1\leqslant i\leqslant l\}$，$VR=V\cap R$($R$ 为撤销属性集合)，如果 $VR=\varnothing$，那么不更新；如果 $VR\neq\varnothing$，那么对任意 $x\in VR$，计算 x 对应的 TDM_x'，替代原来的 TDM_x，组成新的陷门信息

$$TDM_{\mathrm{DO}}'=\{TDM_x'\}_{x\in V}$$

4) 重新发布密钥信息文件 $ID_{\mathrm{DO}} \| TDM'_{\mathrm{DO}} \| CK'$。

4 安全性

4.1 用户属性信息机密性

文献[11, 13]所描述的实现属性撤销的方法，都不可避免地泄露了用户的属性信息。本文方案由 AA 独立完成用户私钥的生成以及用户属性的管理，因此，如果假设 AA 是完全可信的，那么用户的属性信息是机密的。

4.2 数据机密性

本文方案数据的机密性依赖于位置信息文件密文的机密性和密钥信息文件密文的机密性。由于本文采取混合加密的方法对文件进行加密，因此，当假设加密位置信息文件的对称加密算法是安全时，数据机密性就只依赖于加密密钥信息文件的属性加密算法和属性撤销过程的安全性。本文方案采用 WT-CP-ABE 加密算法，它以 CP-ABE 为基础，并加以改进。1) 改变了其以往的密钥生成模式。本文方案中的用户在获得 DO 的主私钥 *OSK* 后，还需要通过 *OSK* 更新自己的私钥，然后才能正确解密。2) 加入了令牌树机制。本文方案构造了一棵完全二叉树，引入令牌树机制控制用户对属性的陷门 TD_x 的获取，从而实现属性的管理。其中，属性的陷门 TD_x 由令牌树中的随机密钥进行加密，即当加密所采用的对称算法以及随机密钥的长度都满足安全性要求时，由 2.3 节可以证明，令牌树机制是安全的。由于 CP-ABE[9]算法是判定性 PBDHE 数学难题，并且被证明在标准模型下是安全的，因此，WT-CP-ABE 加密算法在标准模型下是安全的。

本文方案通过更新陷门信息实现用户的属性撤销。其中，AA 随机生成新的 TD_x，然后从令牌树中选择新的随机密钥对 TD_x 进行对称加密。假设对称加密是安全时，被撤销属性的用户无法解密得到新的 TD_x。因此，被撤销的用户无法进行正常解密，保证了属性撤销机制的安全性。

4.3 抵抗合谋攻击

SNSP 与被撤销用户合谋是最常见的一种攻击[11,13~15]。本文方案采用了令牌树机制，在属性撤销时，由 DO 直接重新加密密钥信息的密文，因此，即使被撤销用户与 SNSP 合谋也无法获得更新之后的数据。

非授权用户之间的合谋攻击。如果 2 个用户合谋，当他们拥有的属性集都不满足解密条件时，在正常情况下是无法对密文进行解密的，但是他们可能通过对各自私钥的组合，获得一些非授权的密钥信息。与文献[7, 9]所采用的方法类似，本文方案通过在每个用户的私钥中嵌入随机数，使合谋者不能通过组合用户私钥进行非法的解密。从 3.3 节的解密过程可知，K_1、K_2、K_3 与 $e(g,g)^{\alpha s}$ 绑定在一起，攻击者想要得到 K_1、K_2、K_3 必须先得到 $e(g,g)^{\alpha s}$。然而，得到 $e(g,g)^{\alpha s}$ 必须计算 $\dfrac{e(C,D)}{e(g,g)^{t\beta s}}$，即计算 $e(g,g)^{t\beta s}$。因此，攻击者必须对任意属性 $\rho(i)(i \in I)$，计算

$$e(C_i, L)e(C'_i, D_{\rho(i)}^{TD_{\rho(i)}})$$

由于本文方案在 L 和 D_i 中嵌入了用户唯一的随机数 t，所以，通过组合不同用户的私钥无法完成上述计算。因此，合谋者无法得到对称密钥信息 K_1、K_2、K_3。

5 性能分析

将本文方案与 EASiER[14]方案进行对比分析。其中，OSKC、OSKS、OENC、ODEC 分别代表 DO 生成私钥的时间复杂度、储存用户私钥的空间复杂度、DO 数据加密的时间复杂度以及用户数据解密的时间复杂度。

生成私钥时，本方案中的 DO 只需要生成 *OSK*，因此 OSKC 的复杂度为 $O(1)$。然而，在 EASiER 方案中，DO 需要计算每个用户的用户私钥，因此，它的 OSKC 复杂度为 $O(na)$，其中，n 表示 DO 拥有社交成员的平均人数，a 表示与用户私钥相关联属性的个数。在私钥存储时，本文方案的用户只需要各自保存私钥 *SK* 和从 DO 处获得的 *OSK*，因此，OSKS 的复杂度为 $O(m)+O(a)$，其中，m 表示与用户建立关系的 DO 的平均人数。然而，在 EASiER 方案中，每个 DO 给用户分发的的私钥 *SK*，用户都要进行存储，因此，它的 OSKS 的复杂度为 $O(ma)$。

本文方案与 EASiER 均采用混合加密方法，但是，本文方案在加密对称密钥信息文件时需要进行 3 次属性加密。因此，EASiER 的 OENC 的复杂度为 $O(D)+O(b)$、ODEC 的复杂度为 $O(D)+O(c)$、本文方案的 OENC 的复杂度为 $O(D)+O(3b)$、ODEC 的复杂度为 $O(D)+O(3c)$、其中，D、b、c 分别表示位置信息文件的大小，加密时密文相关的平均属性个数以及密文解密时需要的平均属性个数。

从表 1 可以看出，虽然本文方案加密与解密过程的时间复杂度大于 EASiER 方案，但是在私钥生成时间复杂度与私钥存储的空间复杂度上具有明显优势。

表 1　　复杂度分析

方案	OSKC	OSKS	OENC	ODEC
EASiER	$O(na)$	$O(ma)$	$O(D)+O(b)$	$O(D)+O(c)$
本文方案	$O(1)$	$O(m)+O(a)$	$O(D)+O(3b)$	$O(D)+O(3c)$

6　结束语

本文以社交网络为应用背景，基于属性加密提出一种支持公开精确、较精确、模糊以及不公开位置信息 4 种模式的位置隐私保护方案。DO 可以根据亲密度等级将位置信息分为 3 个部分，利用对称加密和 WT-CP-ABE 算法对位置信息和密钥信息数据文件进行加密处理并将密文发布到社交网络。通过使用对称加密和公钥加密相结合的方法使加密位置信息更加高效。当且仅当密钥发生变化时，用户需要对密钥信息密文进行重加密。但是，本文方案为了实现对位置信息的分层次解密，需要对密钥信息进行 3 次属性加密，增加了计算量。因此，今后将进一步研究如何更好地将对称加密和属性加密相结合，减少繁琐的加密步骤，提高效率。

参考文献：

[1] CHOW C Y, MOKBEL M F, AREF W G. Casper: query processing for location services without compromising privacy[C]//32nd International Conference on Very Large Data Bases. 2006: 763-774.

[2] KIDO H, YANAGISAWA Y, SATOH T. An anonymous communication technique using dummies for location-based services[C]//Pervasive Services. 2005: 88-97.

[3] MAN L Y, JENSEN C S, HUANG X, et al. SpaceTwist: managing the trade-offs among location privacy, query performance, and query accuracy in mobile services[J]. Icde, 2008: 366-375.

[4] GRUTESER M, GRUNWALD D. Anonymous usage of location-based services through spatial and temporal cloaking[C]//International Conference on Mobile Systems, Applications, and Services. 2003: 31-42.

[5] 陈伟鹤, 李文静, 朱江. 基于社交网络好友攻击的位置隐私保护模型[J]. 计算机工程与科学, 2015, 37(4): 692-698.
CHEN W H, LI W J, ZHU J. A model for protecting location privacy against attacks from friends in SNS[J]. Computer Engineering & Science, 2015, 37(4): 692-698.

[6] BONEH D, FRANKLIN F. Identity-based encryption from the Wail pairing[J]. Advances in Cryptology-Crypt, 2001, 32(3): 586-615.

[7] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]//28th International Symposium on Security and Privacy(S＆P2007). Berkeley, CA, USA, 2007: 321-334.

[8] BEIMEL A. Secure schemes for secret sharing and key distribution[J]. International Journal of Pure & Applied Mathematics, 1996.

[9] WATERS B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization[J]. Lecture Notes in Computer Science, 2011: 321-334.

[10] LIANG X, LI X, LU R, et al. An efficient and secure user revocation scheme in mobile social networks[C]//Global Telecommunications Conference (GLOBECOM 2011). 2011: 1-5.

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

[12] 吕志泉, 洪澄, 张敏, 等. 面向社交网络的隐私保护方案[J]. 通信学报, 2014, 35(8): 23-32.
LYU Z Q, HONG C, ZHANG M, et al. Privacy-perserving scheme for social networks[J]. Journal on Communications, 2014, 35(8): 23-32.

[13] YU S, WANG C, REN K, et al. Attribute based data sharing with attribute revocation[C]//5th ACM Symposium on Information, Computer and Communications Security. Beijing, China, 2010: 261-270.

[14] JAHID S, MITTAL P, BORISOV N. EASiER: Encryption-based access control in social networks with efficient revocation[C]//ACM Symposium on Information, Computer and Communications Security. 2011: 411-415.

[15] ZHANG M, LYU Z, FENG D, et al. A secure and efficient revocation scheme for fine-grained access control in cloud storage[C]//2012 IEEE 4th International Conference on Cloud Computing Technology and Science (CloudCom). 2012: 545-550.

作者简介：

林曦（1992-），男，福建福清人，武警工程大学硕士生，主要研究方向为公钥密码学。

韩益亮（1977-），男，甘肃会宁人，博士，武警工程大学副教授、博士生导师，主要研究方向为公钥密码学与数据安全技术。

柯彦（1991-），男，河南南阳人，武警工程大学硕士生，主要研究方向为信息安全与信息隐藏。

杨晓元（1959-），男，湖南湘潭人，武警工程大学教授、博士生导师，主要研究方向为密码学与信息隐藏。