doi:10.3969/j.issn.1000-436x.2014.08.004

面向社交网络的隐私保护方案

吕志泉[1,2]，洪澄[1]，张敏[1]，冯登国[1]，陈开渠[3]
(1. 中国科学院 软件研究所 可信计算与信息保障实验室，北京 100190；
2. 中国科学院大学，北京 100049；3. 国家超级计算深圳中心，广东 深圳 518055)

摘 要：针对社交网络的隐私安全问题，提出了一种新的社交网络隐私保护方案。首先设计了带陷门的属性加密算法，由属性权威机构与数据属主协同完成用户私钥的生成与分发，有效降低了数据属主的密钥管理代价。然后，通过令牌树机制控制用户对属性陷门的获取，实现了高效的属性撤销。安全性分析表明，该方案能够避免社交网络服务提供商与系统内部非授权用户的合谋攻击，且不泄漏用户的任何属性信息。实验结果证实，该方案在计算代价、存储代价等方面比现有方案更有优越性。

关键词：社交网络；隐私保护；属性加密；令牌树；属性撤销
中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2014)08-0023-10

Privacy-perserving scheme for social networks

LV Zhi-quan[1,2], HONG Cheng[1], ZHANG Min[1], FENG Deng-guo[1], CHEN Kai-qu[3]
(1. TCA Institute of Software，Chinese Academy of Sciences，Beijing 100190, China;
2. University of Chinese Academy of Sciences, Beijing 100049, China;
3. National Supercomputing Center in Shenzhen, Shenzhen 518055, China)

Abstract: The security and privacy issues in SNS were studied and a privacy-preserving scheme PPSNS was proposed. PPSNS utilizes attribute-based encryption, allowing the SNS user to set up an enforcement of fine-grained access control upon the data he owns, thus the potential threats from unauthorized parties or even the SNS provider itself could be avoided. A token system in PPSNS is included to address the challenging issue of efficient attribute revocation. In addition, the users in PPSNS don't have to manage as much information as they do in other encryption-based solutions, achieving a much lower cost in the client side. Analyses show that PPSNS is secure, and gives a better performance in computing and storage costs compared to most related works.

Key words: social network; privacy-preserving; attribute-based encryption; token tree; attribute revocation

1 引言

社交网络即社交网络服务(SNS，social network service)，其建立的主旨是帮助人们建立社会性网络的互联网应用服务。以 Facebook、Twitter 为代表的 SNS 网站发展非常迅猛，用户数量也以惊人速度增长，社交网络已经成为当前最热门的互联网应用服务[1]。

但在现有的社交网络中，隐私安全问题一直令人担忧，已经成为阻碍社交网络发展的主要因素之一。社交网络中的隐私数据主要包括个人信息(例如姓名、毕业院校、当前位置等)、发布的敏感数据(例如校友会成员联系信息、敏感照片或视频等)。社交网络中的隐私安全问题源于数据属主(DO，data owner)与社交网络服务提供者(SNSP，SNS provider)不在同一可信域中，存储于社交网络中的隐私数据完全脱离了 DO 的直接物理控制。因此，这些数据将面临着包括 SNSP 在内的安全威胁，承担着隐私

收稿日期：2013-05-06；**修回日期**：2014-03-19
基金项目：国家自然科学基金资助项目(61232005, 61100237, 91118006)；深圳市战略新兴产业发展专项资金基金资助项目(CXZZ20120831113048965)
Foundation Items: The National Natural Science Foundation of China (61232005, 61100237, 91118006); Shenzhen Special Funds for Development of New Industries (CXZZ20120831113048965)

泄漏的风险[2]。事实也证明，包括 Facebook、Twitter 等著名的 SNSP 都曾泄漏或丢失用户的隐私数据，并导致了严重的后果。

加密是解决上述安全问题的一种最常用方法[3~9]。Flybynight[3]采用客户端 JavaScript 加密，但由于密钥由 SNSP 管理，故易遭受 SNSP 发起的攻击。NOYB[4]提出秘密字典的加密方式，但该方案泄漏了用户身份信息以及用户之间的联系信息等。Facecloak[5]设计了一种社交网络隐私保护架构，将伪造数据发布于 SNSP，真实密文数据却存储于第三方。该方案能抵抗 SNSP 发起的攻击，但安全性依赖于第三方且效率较低。基于密文策略的属性加密 (CP-ABE， ciphertext-policy attribute-based encryption)[10]是一种新型的加密技术，由于其支持属性粒度的访问控制策略，近年来被广泛地应用在隐私保护方案中[7~9,11~14]。在 CP-ABE 中，用户的私钥关联一个属性集，密文则关联一个属性策略，当且仅当属性集满足属性策略时，用户才可解密。现有基于 CP-ABE 的社交网络隐私保护方案分为 2 类：一类以 DO 为中心，如 Persona[7]和 EASiER[8]；另一类以属性权威机构(AA，attribute authority)为中心，如 Liang[9]。前者在 DO 与用户建立社交联系时，由 DO 生成并分发用户私钥。对于 DO 发布的数据，仅 DO 的社交成员中满足属性策略的用户才可解密。后者由 AA 生成并分发用户私钥，DO 仅负责加密数据，社交网络中任意满足属性策略的用户均可解密 DO 的数据。然而，上述 2 类方案仍然存在以下 3 方面的不足。

1) 在 Persona[7]和 EASiER[8]中，由于私钥的计算代价与其关联的属性集线性相关，随着社交成员数量增长，易造成 DO 端的瓶颈。另一方面，由于社交成员可能从多个 DO 处获得私钥，将会造成私钥的存储与管理难题。Liang[9]一定程度上缓解了这些问题，但却造成了社交网络上任意非 DO 社交成员的用户也可能访问 DO 数据的可能。

2) 文献[7~9]方案仅支持用户级别的撤销，然而在社交网络中，随着工作环境等因素变化，社交成员的属性亦会发生相应的变化。因此，必须支持属性撤销，即一旦用户某些属性被撤销，若其剩余的属性仍然能满足属性策略，则依然可以解密该数据。这样可避免用户私钥的频繁更换，并降低私钥管理方的代价。虽然文献[11,15,16]提出了属性撤销方法，但文献[11,15]泄漏了用户的属性信息。由于属性信息代表了用户的身份特征，这在社交网络中应予以保护，而文献[16]的实现代价过大，因为 DO 需要为每个属性维护一个用户撤销列表。

3) Persona[7]在权限撤销时，DO 需要对密文进行重加密以及对剩余非撤销用户分更新私钥，因此代价较大。EASiER[8]通过引入半可信代理服务器，有效降低了该代价，但面临着代理服务器与被撤销用户的合谋攻击。事实上，现有 CP-ABE 权限撤销方法(如文献[12,13,15])大都利用代理重加密技术将代价转移到服务器端。但当服务器受利益驱动时，这类方法均面临着上述合谋攻击。例如，服务器不执行密文重加密或仍然对被撤销用户更新私钥。

针对以上问题，本文提出了一种新的社交网络隐私保护方案 PPSNS，其贡献如下。

1) 设计了带陷门的 CP-ABE 算法，由 AA 负责用户私钥生成与分发，DO 负责属主主私钥的分发(属主主私钥为一与属性集大小无关的常数)。如此，既支持了仅 DO 的社交成员才可能访问该 DO 数据的特点，又降低了 DO 的计算代价和社交成员的存储代价。

2) 通过令牌树机制控制用户对属性陷门的获取，实现了高效的属性撤销。在撤销时，无需更新剩余非撤销用户的私钥，并有效降低了密文的重加密代价。

3) PPSNS 避免了 SNSP 与系统内部非授权用户的合谋攻击，且不泄漏用户任何属性信息。

2 预备知识

2.1 双线性映射

定义 1 双线性映射[17]。假设 G_1 和 G_2 是 2 个阶都为大素数 p 的乘法群，映射 $e:G_1\times G_1\to G_2$ 称为双线性映射，则其满足如下性质。

1) 双线性。对于 $\forall u, v\in G_1$ 和 $\forall a, b\in Z_p$，都有 $e(u^a, v^b) = e(u, v)^{ab}$。

2) 非退化性。$\exists u, v\in G_1$，使得 $e(u, v)\neq 1$。

3) 可计算性。对于 $\forall u, v\in G_1$，都存在一个有效的多项式时间算法来计算 $e(u, v)$。

2.2 基于密文策略的属性加密(CP-ABE)

定义 2 属性。$A=\{1, 2,\cdots, k\}$ 为全体属性集合，则属性集 S 是 A 的一个非空子集，即 $S\subset A$。

定义 3 属性策略。定义在属性之上，由布尔逻辑词“AND”、“OR”等表达的策略 P。

CP-ABE 的构造技术分为 2 类：基于访问结构

树[10]和基于线性秘密共享[18,19]。

定义 4　线性秘密共享[18,19]。令$(\boldsymbol{M},\rho)$代表一个属性策略 P，其中，$\boldsymbol{M}$ 为一个 $l\times h$ 的矩阵，ρ 为一个单射函数，即对于 $i=1,\cdots,l,\rho(i)$表示与 $\boldsymbol{M}$ 的第 i 行关联的属性。令 S 为满足属性策略 P 的属性集，$I=\{i\mid\rho(i)\in S\}$，$\vec{\boldsymbol{M}}_i$ 为 $\boldsymbol{M}$ 第 i 行组成的向量，则可根据 $\boldsymbol{M}$ 计算出一组常系数 $\{\theta_i\in Z_p\}_{i\in I}$ 满足 $\sum_{i\in I}\theta_i\vec{\boldsymbol{M}}_i=\{1,0,\cdots,0\}$。相反，当 S 不满足属性策略 P 时，这组常系数不存在。

因此，假设共享的秘密为 $s\in Z_p$，首先从 Z_p 中随机选取 $h-1$ 个值 $v_2,v_3,\cdots,v_h$，与 s 组成一个 h 维的向量 $\vec{v}=(s,v_2,\cdots,v_h)$，则内积 $\lambda_i=\vec{\boldsymbol{M}}_i\vec{v}$ $(i=1,2,\cdots,l)$为秘密共享值。若属性集 S 满足$(\boldsymbol{M},\rho)$所代表的属性策略 P，则可通过计算 $\sum_{i\in I}\theta_i\lambda_i=s$ 恢复秘密。

3　模型定义

3.1　系统模型

如图 1 所示，PPSNS 主要包括以下 4 个实体：属性权威机构 AA、社交网络服务提供者 SNSP、数据属主 DO 和数据访问者。与文献[9,11]方案类似，AA 完全可信，主要负责初始化系统、生成与分发用户的私钥。此外，AA 还负责撤销用户属性。SNSP 负责存储 DO 发布的数据并提供社交网络应用服务。DO 负责生成与分发属主主私钥，以及加密数据时设定属性策略。数据访问者访问数据时，首先利用 DO 对应的属主主私钥更新自己的私钥，然后再解密。当且仅当私钥关联的属性集满足属性策略并完全拥有属性策略中相关属性陷门后时，才可正确解密。

3.2　攻击模型

在上述系统模型中，AA 完全信任，不会对系统实施任何的攻击行为。因此，系统的攻击者主要分为：1) SNSP，由于 SNSP 存储着所有数据，无法避免其恶意窥窃或分析用户数据，从而获取数据隐私信息；2)非授权用户，这类攻击者通过其已掌握的数据信息，试图访问其他非授权数据；3)合谋攻击者，这类攻击者的威胁最大，包括 SNSP 与非授权用户合谋[8]和非授权用户之间的合谋。

为了不影响数据的正常访问，本文假定 SNSP 不会拒绝用户的合法数据访问请求，亦不会删除和篡改 DO 的数据。此外，本文还假定所有通信信道都建立在安全协议之上(如 SSL 信道)。

4　PPSNS 设计

本节详细描述 PPSNS 方案设计。首先构造了带陷门的 WT-CP-ABE 算法；然后设计了令牌树机制；最后基于二者，描述了 PPSNS 的体系架构。

4.1　属性群

定义 5　属性群。令 $U=\{u_1,\cdots,u_m\}$为全体用户集合，$A=\{1,2,\cdots,k\}$为全体属性集合，则属性群 $G(x)$表示拥有属性 x 的全体用户集合。

定义 6　属性陷门。对于任意属性 $x\in A$，都对应一个属性陷门 TD_x。当且仅当用户 $u_t\in G(x)$时，u_t 才可获得属性 x 对应的属性陷门 TD_x。

4.2　WT-CP-ABE 算法

WT-CP-ABE 算法基于 CP-ABE[19]，并加以改进：1) 改变密钥生成方式，由 AA 与 DO 协同完成，既保证了 DO 仍可对其社交成员加以控制，又降低了其计算代价和社交成员的存储代价；2) 嵌入属性陷门，通过控制用户对属性陷门的获取，实现了

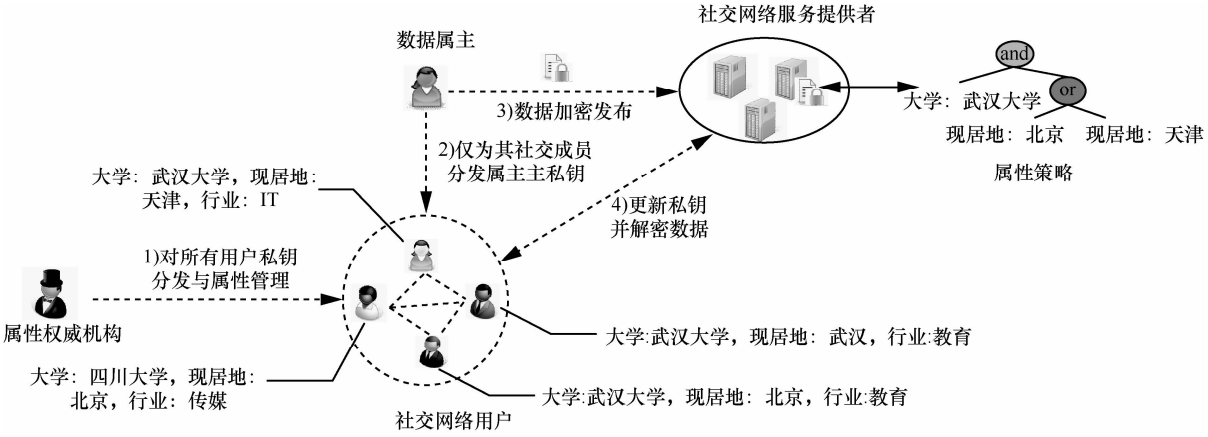


图 1　PPSNS 的系统模型

用户属性撤销功能。WT-CP-ABE 的 5 个子函数可描述如下。

1) *Setup*(1^λ)。首先，AA 根据安全参数1^λ，选定阶为素数 p，生成元为 g 的乘法群 G_1，并定义 e 是 $G_1\times G_1\to G_2$ 的一个双线性映射。其次，定义系统所需的属性空间为 $A=\{1, 2,\cdots, k\}$，对任意属性 $x\in A$ $(1\leqslant x\leqslant k)$, 随机选择 η_x、$TD_x\in Z_p$，并计算 $T_x=g^{\eta_x TD_x}$。最后，随机选择 $\beta\in Z_p$ 生成主私钥 $ASK=<\beta, \{TD_x\}_{x\in A}>$，并发布公开密钥 $APK=<G_1, g, g^\beta, \{T_x\}_{x\in A}>$。其中，$\eta_x$ 用于与属性本身相关的计算，TD_x 用于与属性撤销相关的计算。

此外，每个 DO 随机选择 $\alpha\in Z_p$ 作为主私钥 $OSK=<g^\alpha>$，并发布公开密钥 $OPK=<e(g,g)^\alpha>$。

2) *KeyGen(ASK, S)*。使用主私钥 *ASK* 生成属性集 S 对应的私钥。首先，随机选择 $t\in Z_p$，计算 $D=g^{\beta t}$，$L=g^t$。然后，对于任意属性 $x\in S$，计算 $D_x=T_x^{t/TD_x}=g^{\eta_x t}$。接着，选择一随机的陷门密钥 *TDKey*。最后，输出用户私钥 *SK* 为

$$SK=<D, L, \{D_x\}_{x\in S}, TDKey>$$

其中，t 用于私钥随机化，避免属性合谋攻击，*TDKey* 用于属性陷门恢复。

3) *Encryt*(*APK*, *OPK*, P, m)。使用公开密钥 *APK*、*OPK* 和属性策略 P 加密明文 m。首先，根据文献[18]确定可代表属性策略 P 的$(\boldsymbol{M}, \rho)$，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 $\vec{v}=(s, v_2, \cdots, v_h)\in Z_p$，并计算 $\tilde{C}=m\cdot e(g,g)^{\alpha s}$，$C=g^s$。对于任意 $i\in\{1, 2,\cdots, l\}$，令 $\vec{\boldsymbol{M}}_i$ 为 $\boldsymbol{M}$ 第 i 行所组成的向量，计算 $\lambda_i=\vec{\boldsymbol{M}}_i\vec{v}$。接着，选择随机数 $r_1,\cdots, r_l\in Z_p$，计算 $C_i=g^{\beta\lambda_i}T_{\rho(i)}^{-r_i}$，$C_i^{'}=g^{r_i}$。最终，输出密文 *CT* 如下

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

易见，由于 $T_{\rho(i)}$ 嵌入了属性陷门 $TD_{\rho(i)}$，故密文中与属性相关部分(即每个属性对应的 C_i)都与 $TD_{\rho(i)}$ 相绑定。因此解密时，必须获得密文中的这些属性陷门。

4) *KeyUpdate*(*OSK*, *SK*)。使用 *OSK* 更新私钥 *SK*。更新后的 *SK* 为

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

5) *Decrypt*(*SK*, *CT*)。使用私钥 *SK* 解密密文 *CT*。当且仅当 *SK* 关联的属性集 S 满足 *CT* 中$(\boldsymbol{M}, \rho)$所代表的属性策略 P 时，才可以正确解密。令 $I=\{i \mid \rho(i)\in S\}$，$W=\{\rho(i)\mid \rho(i)\in S\}$，假设对任意属性 $\rho(i)\in W$，已经借助于陷门密钥 *TDKey* 获取了属性陷门 $TD_{\rho(i)}$(详见 4.4 节)。

首先，根据文献[18]所述方法，可计算出一组常系数$\{\theta_i\}_{i\in I}$，使$\sum_{i\in I}\theta_i\lambda_i=s$。接着，计算

$$\begin{aligned}A&=\prod_{i\in I}(e(C_i, L)e(C_i^{'}, D_{\rho(i)}^{TD_{\rho(i)}}))^{\theta_i}\\&=\prod_{i\in I}(e(g^{\beta\lambda_i}g^{-r_i\eta_{\rho(i)}TD_{\rho(i)}}, g^t)e(g^{r_i}, g^{\eta_{\rho(i)}tTD_{\rho(i)}}))^{\theta_i}\\&=e(g,g)^{t\beta\sum_{i\in I}\lambda_i\theta_i}\\&=e(g,g)^{t\beta s}\end{aligned}\tag{1}$$

最后，将式(1)代入，明文可得

$$\begin{aligned}m&=\tilde{C}/(e(C,D)/A)\\&=\tilde{C}/(e(g^s, g^\alpha g^{\beta t})/e(g,g)^{t\beta s})\end{aligned}\tag{2}$$

4.3 令牌树机制

定义 7 令牌树。一颗代表了令牌和随机密钥的完全二叉树。设二叉树的深度为 D，除第 D 层外，其他各层 $(1\sim D-1)$的节点都达到最大数 2^{D-1}，第 D 层的所有节点都连读集中在最左边。为减少边树，还限定除叶子节点外，每一层的所有节点都有 2 个子节点。令牌树的每条边代表一令牌，每个节点都对应一随机密钥，且叶子节点与系统中用户一一映射。根据令牌树的特点可知，对于一颗深度为 D 的令牌树，最多可容纳系统总人数为 2^{D-1}，令牌的最大个数为 2^D-2。

设 $\oplus$ 表示异或操作，$H(\cdot)$表示一公开的单向散列函数，随机对称密钥的长度与 $H(\cdot)$输出的长度相同。令牌树的建立过程如下所述。

1) 初始化。根据系统总人数生成一颗完全二叉树，对任意叶子节点 n_j，选择一随机密钥 RK_j。

2) 内部节点随机密钥设置。以自底向上方式，对任意内部节点 n_j，设其左孩子节点对应的随机密钥为 RK_i，则 n_j 对应的随机密钥为 $RK_j=H(RK_i)$。

3) 令牌设置。令 $Flag=1$ 表示 $H(\cdot)$函数，则对任意左孩子节点，连接其到父节点的边对应的令牌为 $TK_{i\to j}=Flag$；对任意右孩子节点，设其对应的随机密钥为 RK_i，其父节点对应的随机密钥 RK_j，则连接

其到父节点的边对应的令牌为 $TK_{i\to j}=H(RK_i)\oplus RK_j$。

定义 8　最小覆盖密钥集(MCKS，minimum cover key set)。对于任意 $MCKS_x\in MCKS$ $(1\leqslant x\leqslant k)$，令 $\boldsymbol{\Phi}_x$ 为令牌树中与属性群 $G(x)$中用户对应的叶子节点的集合，$\boldsymbol{\Psi}_x$ 为最小覆盖 $\boldsymbol{\Phi}_x$ 的节点集合，则 $MCKS_x$ 表示 $\boldsymbol{\Psi}_x$ 所有节点对应的随机密钥的集合。

定义 9　密钥链集(KCS，key chain set)。对于任意 $KCS_i\in KCS(1\leqslant i\leqslant m)$，令 n_i 为令牌树中某叶子节点，则 KCS_i 表示 n_i 到根节点经过的所有节点(包括 n_i 和根节点)对应的随机密钥的集合。

定义 10　令牌链集(TCS，token chain set)。对于任意 $TCS_i \in TCS\ (1\leqslant i\leqslant m)$，令 n_i 为令牌树中某叶子节点，则 TCS_i 表示 n_i 到根节点经过的所有令牌的集合。

定理 1　若已知某叶子节点对应的随机密钥和其到根节点的所有边上对应的令牌，则可以恢复该叶节点的密钥链集。

证明　以叶子节点 n_i 为例。若 n_i 为左孩子节点，则其父节点 n_j 对应的随机密钥为 $RK_j=H(RK_i)$；若 n_i 为右孩子节点，则其父节点 n_j 对应的随机密钥为 $RK_j=H(RK_i)\oplus TK_{i\to j}=H(RK_i)\oplus H(RK_i)\oplus RK_j$。以此方式，自底向上递归计算，即可恢复 n_i 的 KCS_i。

定理 2　若仅已知某叶子节点对应的随机密钥，即使获得令牌树中所有的令牌，也无法恢复该叶子节点到根节点经过的所有节点以外的任意节点对应的随机密钥。

证明　以叶子节点 n_i 为例。设 NS 表示 n_i 到根节点上经过的所有节点的集合，由定理 1，显然可计算出 NS 中任意节点对应的随机密钥。对于任意节点 $n_j\in NS$，设 n_c 为其孩子节点且 $n_c\notin NS$。若 n_c 为右孩子节点，则可计算出 $RK_j\oplus TK_{c\to j}=RK_j\oplus H(RK_c)\oplus RK_j=H(RK_c)$。由于 $H(\cdot)$的单向性，无法计算出 RK_c；若 n_c 为左孩子节点，同理也无法计算出 RK_c。故对于不属于 NS 的节点，无法计算出其对应的随机密钥。

如图 2 所示，若用户 u_6 已知令牌树中的随机密钥 RK_6 和 TCS_6，则可计算 $RK_{11}=H(RK_6)\oplus TK_{6\to 11}=H(RK_6)\oplus H(RK_6)\oplus RK_{11}$，$RK_{14}=H(RK_{11})$，$RK_{15}=H(RK_{14})\oplus TK_{14\to 15}=H(RK_{14})\oplus H(RK_{14})\oplus RK_{15}$。但是，即使 u_6 知道令牌树中的所有令牌，也无法计算出上述以外的任意随机密钥。

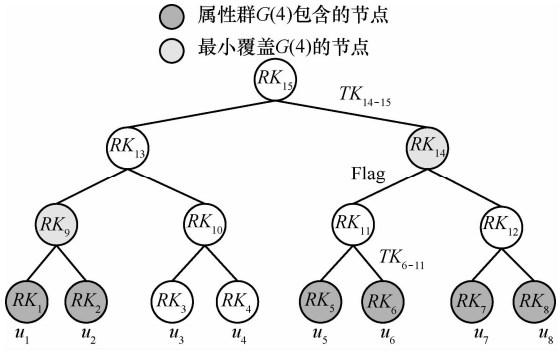


图 2　令牌树示意

定理 3　对于任意用户 $u_t\ (1\leqslant t\leqslant m)$，令 n_t 为其相映射的叶子节点。若 $u_t\in G(x)\ (1\leqslant x\leqslant k)$，则 n_t 对应的 KCS_i 与 $G(x)$对应的 $MCKS_x$ 有且仅有一个元素相交。

证明　1)存在性。假设 n_t 对应的 KCS_i 与 $G(x)$对应的 $MCKS_x$ 没有元素相交，即属于 $MCKS_x$ 的任意节点，均不属于 KCS_i。故 $MCKS_x$ 中的节点均不为 n_t 到根节点所经过的节点，因此 $MCKS_x$ 不包括节点 n_t。而由已知 $u_t\in G(x)$，可推得 $MCKS_x$ 必然包含节点 n_t。故该假设不成立。2)唯一性。假设 n_t 对应的 KCS_i 与 $G(x)$对应的 $MCKS_x$ 有 1 个以上的元素相交，即至少存在 2 个节点同时属于 KCS_i 和 $MCKS_x$。故 $MCKS_x$ 中至少有 2 个节点可同时覆盖 n_t，这与 $MCKS_x$ 为 $G(x)$的最小覆盖集相矛盾，故该假设不成立。

4.4　体系架构

系统建立。在系统初始化阶段，AA 选择一个安全参数 1^λ，运行 $Setup(1^\lambda)$算法生成主私钥 ASK 和公开密钥 APK。每个 DO 与 AA 协作，生成主私钥 OSK 以及公开密钥 OPK。其中，主私钥由各自秘密保存，公开密钥公开发布。

新用户注册。当有一个新用户 u_t 加入社交网络时，AA 根据 u_t 的身份特征，赋予其相应的属性集 S。然后，执行 $KeyGen(ASK, S)$算法生成私钥 SK 并通过安全信道(如 SSL 协议信道)将 SK 发送给 u_t。为了实现属性群管理，AA 还需要将用户添加到相应的属性群中。例如，若用户 u_1、u_2、u_3 对应的属性集依次{1, 2}、{1, 2, 3}、{2, 3}，则 AA 构建的属性群依次为 $G(1)=\{u_1, u_2\}$、$G(2)=\{u_1, u_2, u_3\}$、$G(3)=\{u_2, u_3\}$。

陷门信息发布。为了帮助未被属性撤销的用户解密密文，AA 需要发布陷门信息(TDM，trapdoor message)。该过程描述如下。

1) 根据 4.3 节建立一颗令牌树，树的叶子节点

与用户一一映射，且其对应的随机密钥为该用户私钥中的 *TDKey*。

2) 对于任意的属性 $x \in A$ $(1 \leqslant x \leqslant k)$，根据其对应的属性群 $G(x)$，确定最小覆盖密钥集 $MCKS_x$，并生成陷门信息 $TDM_x = \{E_{RK_j}(TD_x)\}_{RK_j \in MCKS_x}$。其中，$RK_j$ 为随机密钥，TD_x 为属性 x 的陷门，E 为快速的对称加密算法，如异或运算。

如图 2 所示，假设属性 4 对应的属性群 $G(4) = \{u_1, u_2, u_5, u_6, u_7, u_8\}$，则最小覆盖集 $MCKS_4 = \{RK_9, RK_{14}\}$，故属性 4 对应的陷门信息 $TDM_4 = \{E_{RK_9}(TD_4), E_{RK_{14}}(TD_4)\}$。

3) 将 $TDM = \{TDM_x\}_{x \in A}$ 和令牌链 $TCS = \{TCS_i\}_{i \in \{1,2,\cdots,m\}}$ 公开发布于社交网络中。

社交联系建立。当 DO 与社交网络中的用户建立起社交联系时，会通过安全信道将自己的主私钥 *OSK* 发送给这些社交成员。

隐私数据发布。为简洁起见，此处只描述 DO 对单个数据文件的处理，其过程如下。

1) 选择一个随机对称密钥 *DEK* 加密文件 *f*，得到文件密文 $Enc_{DEK}(f)$（*Enc* 为符合要求的对称加密算法）。

2) 根据属性策略 P，运行 *Encryt*(*APK*, *OPK*, P, *m*)算法加密对称密钥 *DEK*，得到密文 CT_f。

3) 令 $V = \{\rho(i) | 1 \leqslant i \leqslant l\}$，则对于任意属性 $x \in V$，获取其对应的陷门信息 TDM_x，组成陷门信息 $TDM_f = \{TDM_x\}_{x \in V}$。

最终，文件以 $ID_f \| TDM_f \| CT_f \| Enc_{DEK}(f)$ 格式存储于社交网络中（ID_f 为文件唯一编号）。

数据访问。当用户 u_t 发起对编号为 ID_f 的文件的访问请求时，SNSP 返回 $TDM_f \| CT_f \| Enc_{DEK}(f)$ 和该用户对应的令牌链 TCS_t。u_t 的解密过程如下。首先，对 TDM_f 解密，得到相关属性陷门。然后，利用属性陷门和私钥 *SK* 解密 CT_f，得到对称密钥 *DEK*。最后，利用 *DEK* 解密文件。前两步过程描述如下。

① TDM_f 解密。由定理 1，用户 u_t 可用私钥 *SK* 中的陷门密钥 *TDKey* 以及令牌链 TCS_t，计算得到其在令牌树中的密钥链集 KCS_t。显然，若 u_t 可解密 CT_f，则其私钥 *SK* 关联的属性集 S 必然满足由($\boldsymbol{M}$, ρ)所代表的属性策略。令 $W = \{\rho(i) | 1 \leqslant i \leqslant l$ 且 $\rho(i) \in S\}$。对于任意属性 $x \in W$，令 $G(x)$ 为其对应的属性群，显然有 $u_t \in G(x)$。令 $MCKS_x$ 为 $G(x)$ 对应的最小覆盖密钥集，由定理 3 可知，必然存在同一随机密钥 $RK_y \in KCS_t$ 且 $RK_y \in MCKS_x$。故 u_t 可用 RK_y 解密 TDM_x，从而得到属性陷门 TD_x。因此，u_t 可从 TDM_f 得到 CT_f 解密时所需的所有属性陷门。

如图 2 所示，用户 u_2 可利用令牌链 $TCS_2 = TK_{2\to 9} \| \text{Flag} \| \text{Flag}$ 依次计算出 RK_9、RK_{13}、RK_{15}，故其可用随机密钥 RK_9 解密属性 4 对应的陷门信息 TDM_4，从而得到陷门 TD_4。

② CT_f 解密。u_t 首先执行 *KeyUpdate*(*OSK*, *SK*)算法更新自己的私钥 *SK*，接着运行 *Decrypt*(*SK*, *CT*)算法解密 CT_f，得到随机对称密钥 *DEK*。

属性撤销。当用户失去属于某属性群的资格时，AA 应当撤销该用户相应的属性。令 R 表示撤销属性集合，u_t 为撤销用户，则该过程可描述如下。

1) AA 执行属性陷门信息更新。对于任意属性 $x \in R$，随机选择新的属性陷门 TD_x'。令 $G(x)$ 为 x 对应的属性群，显然此时 $u_t \notin G(x)$。确定新的最小覆盖密钥集 $MCKS_x'$，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。

如图 2 所示，当 AA 撤销用户 u_2 的属性 4 后，$G(4) = \{u_1, u_5, u_6, u_7, u_8\}$。此时，最小覆盖集 $MCKS_4' = \{RK_1, RK_{14}\}$，陷门信息 $TDM_4' = \{E_{RK_1}(TD_4'), E_{RK_{14}}(TD_4')\}$。根据定理 2，$u_2$ 即使获得了令牌树中所有的令牌链，也只能获得随机密钥 RK_9、RK_{13}、RK_{15}。因此，其被撤销属性 4 后，再也无法获得新的属性陷门 TD_4'。

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 $T_x' = T_x^{TD_x'/TD_x} = h_i^{TD_x'}$，替换 *ASK* 中的 TD_x 为 TD_x'。

3) 当且仅当数据内容修改时，由 DO 执行懒惰的密文重加密。首先，用新的随机对称密钥 *DEK'* 加密数据文件，得到 $E_{DEK'}(f)$。然后，执行 *Encryt*(*APK*, *OPK*, P, *m*)算法加密对称密钥 *DEK'*，得到密文 CT_f'。最后，更新文件对应的属性群信息。其更新规则为：令 $V = \{\rho(i) | 1 \leqslant i \leqslant l\}$，$VR = V \cap R$（$R$ 为撤销属性集合），若 $VR = \varnothing$，则无需更新数据的陷门信息；否则，对任意属性 $x \in VR$，更新 TDM_x 为 TDM_x'。

懒惰重加密方法在文献[20,21]中均被采用。该类方法认为，因为被撤销用户可能保留了旧数据的副本，故即使其仍能够访问旧数据，也并没有威胁

到文件系统的安全性。因此，在权限撤销时，没必要立即执行重加密，而可在数据内容更新时才执行重加密。本文采用懒惰的密文重加密处理，带来了 2 个好处。一方面，可以避免 AA 执行属性撤销时需实时通知 DO 重加密密文的问题；另一方面，当数据文件内容更新不频繁时，可以将多次的属性撤销(密文重加密)聚集为一次密文重加密，这样可显著降低重加密计算代价。

5　安全性

5.1　用户属性信息机密性

文献[11,15]提出的属性撤销方法，对外暴露了用户的属性信息。在 PPSNS 中，属性权威机构 AA 负责用户私钥生成以及属性撤销，故用户属性信息仅 AA 可获得，因此是机密的。

5.2　数据机密性

PPSNS 的数据机密性主要包括数据文件密文的机密性和 WT-CP-ABE 密文的机密性。假设加密数据文件的对称加密算法以及对称密钥长度都是满足安全要求，那么数据机密性就取决于 WT-CP-ABE 加密算法的安全性以及属性撤销机制的安全性。

CP-ABE[19]算法基于判定性 PBDHE 数学难题，在标准模型下被证明是安全的。WT-CP-ABE 算法以 CP-ABE[19]为基础，并加以改进：1) 改变了密钥生成方式，当且仅当用户获得了 DO 的主私钥 *OSK* 时，才可能通过 *OSK* 更新私钥并解密密文；2) 为每个属性 x 设置一个属性陷门 TD_x，通过控制用户对 TD_x 的获取，从而实现属性撤销。由于 TD_x 由令牌树中的随机密钥加密，假定随机密钥长度和对称加密算法都是安全的，由定理 1 和定理 2 可知，本文设计的令牌树机制也是安全的。因此，WT-CP-ABE 加密算法也是在标准模型下是安全的。

属性撤销时，AA 会随机选择新的属性陷门，并由令牌树中被撤销用户无法获得的随机密钥加密，从而保证被撤销用户无法获得该新陷门，故无法正常解密。因此，属性撤销机制亦是安全的。

5.3　抵抗合谋攻击

SNSP 与被撤销用户合谋是最常见的一种攻击[8,11~13,15]。而 PPSNS 设计了令牌树机制，当撤销事件发生时，由 DO 执行懒惰密文重加密，从而避免了 SNSP 与被撤销用户合谋获得更新后数据的可能性。

非授权用户之间合谋是另一种典型的攻击。2 个属性集均不满足解密条件的用户，很有可能通过组合各自的私钥，实现对密文的解密。然而，与文献[10,19]方案类似，PPSNS 通过对每个用户的私钥嵌入随机数，避免了不同私钥间进行组合解密。由于加密数据文件的对称密钥 *DEK* 与 $e(g,g)^{\alpha s}$ 绑定在一起，欲得到 *DEK*，攻击者必先恢复出 $e(g,g)^{\alpha s}$。从 4.2 节的解密过程可知，唯一方法就是计算 $e(C,D)/e(g,g)^{t\beta s}$，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 $e(C_i,L)e(C_i^{'}, D_{\rho(i)}^{TD_{\rho(i)}})$。然而，由于 L 和 D_i 中分别嵌入了每个用户唯一的随机数 t，故即使通过组合私钥，也无法完成上述计算。因此，攻击者不能通过合谋得到对称密钥 *DEK*。

6　性能

6.1　复杂度分析

将 PPSNS 与 EASiER[8]从复杂度角度进行对比，为了方便描述，用 *OSKC* 表示 DO 端生成私钥的计算代价，*OSKS* 表示用户私钥的存储代价，*OENC* 表示 DO 在加密时的计算代价，*ODEC* 表示用户解密时的计算代价。

在 PPSNS 的私钥生成阶段，由于 DO 仅需生成属主主私钥，故 PPSNS 的 *OSKC* 的复杂度为 $O(1)$。EASiER[8]方案中，DO 需要为每个用户都生成私钥，其 *OSKC* 的复杂度为 $O(na)$，其中，n 为 DO 的平均社交成员数，a 为用户私钥关联的平均属性数。在 PPSNS 的私钥存储中，由于用户仅需存储私钥 *SK* 以及每个 DO 分发的属主主私钥，故 *OSKS* 的复杂度为 $O(m)+O(a)$，其中，m 为与用户有社交联系的平均 DO 人数。EASiER[8]方案中，用户需要存储每个 DO 为其发送的私钥 *SK*，故 *OSKS* 的复杂度为 $O(ma)$。

由于 PPSNS 与 EASiER[8]均采用双层加密机制（数据文件用对称加密，对称密钥用 CP-ABE 加密），故二者的 *OENC* 与 *ODEC* 的复杂度均相同。*OENC* 的复杂度为 $O(D)+O(b)$，*ODEC* 的复杂度为 $O(D)+O(c)$，其中，D 表示数据文件的大小，b 表示加密时密文关联的平均属性个数，c 表示密文需要解密的平均属性个数。

综上所述，由表 1 可以看到，PPSNS 尽管在加密与解密过程的计算复杂度与 EASiER[8]相同，但在私钥的生成以及存储方面，复杂度要明显优于后者。

表 1　　**复杂度分析**

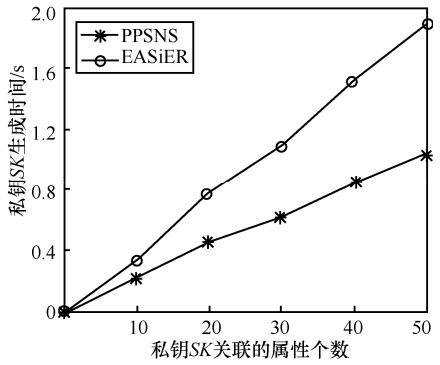
方案	*OSKC*	*OSKS*	*OENC*	*ODEC*
EASiER	*O*(*na*)	*O*(*ma*)	*O*(*D*)+*O*(*b*)	*O*(*D*)+*O*(*c*)
PPSNS	*O*(1)	*O*(*m*)+*O*(*a*)	*O*(*D*)+*O*(*b*)	*O*(*D*)+*O*(*c*)

6.2　实验仿真

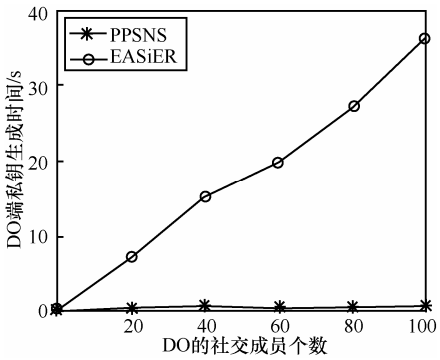
实验环境搭建于 VMware Workstation 8.0.4 虚拟机上的 Red Hat Enterprise 5，分配有 1 GB 内存。实验系统采用 C 语言实现，代码主要分为两部分，其中，WT-CP-ABE 加密算法以 libfenc 库[22]的 WatersCP 模块为基础改写，对称加密算法采用 openssl-1.0.0 库的 192 bit AES 加密算法。

实验 1　私钥生成时间效率。

用户私钥生成时间效率评价系统性能的一个重要指标，特别是考虑在 SNS 环境下，系统人数较多时。图 3(a)展示了私钥 *SK* 生成时间开销，其结果表明，*SK* 生成时间随关联的属性集大小线性增长。此外，生成任意属性对应的私钥组件时，PPSNS 比 EASiER[8]少 2 次连乘操作，故效率高于后者。图 3(b)展示了当私钥 *SK* 关联的属性个数为 10 时，DO 端私钥生成时间开销随 DO 的社交成员数量变化的情况。实验结果表明，由于 DO 仅需生成属主主私钥，故 DO 端代价明显低于 EASiER[8]。



(a)生成私钥 *SK* 时间对比



(b)DO 端生成私钥时间对比

图 3　私钥生成时间对比

实验 2　用户私钥存储代价。

假设用户私钥 *SK* 关联的属性个数为 10，图 4 展示了用户私钥的存储开销随与该用户有社交联系的 DO 人数变化的情况。由于 PPSNS 中用户仅需存储私钥 *SK* 以及每个 DO 分发的属主主私钥，而 EASiER[8]中需存储每个 DO 分发的私钥 *SK*，故 PPSNS 的用户私钥存储代价明显低于 EASiER[8]。

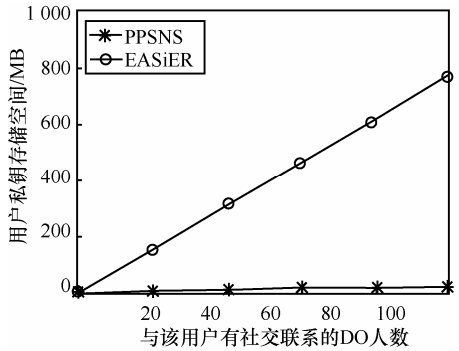


图 4　用户私钥存储代价对比

实验 3　数据加密时间效率。

数据加密是 DO 的主要计算代价，包括对称加密和 CP-ABE 算法加密。当数据文件相同大小时，显然前者的代价对于所有的方案均相当。后者的代价对比结果如图 5 所示。结果显示，WT-CP-ABE 加密时间随属性策略中属性个数线性增加，且与 EASiER[8]中 CP-ABE 加密算法效率相当。

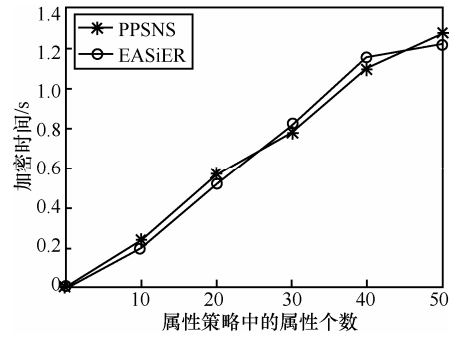


图 5　加密时间对比

实验 4　用户解密数据时间效率。

用户在客户端的解密任务主要包括对陷门信息 *TDM*、密文 *CT* 以及数据文件密文的解密。由于随机密钥一般很短(如 192 bit AES 密钥)，且是被快速对称加密算法加密，故对 *TDM* 的解密时间可忽略。图 6 展示了密文 *CT* 的解密时间对比。由图 6 可知，WT-CP-ABE 解密时间亦随属性策略中属性个数线性增加，且由于少 1 次配对操作，故效率要

稍微高于 EASiER[8]。当数据文件密文大小相同时，各方案对其解密代价相当。

实验 5　令牌相关效率。

本实验考察了 SNSP 向用户发送令牌链集的通信代价、用户通过该令牌链集获得密钥链集的计算代价以及 SNSP 端所有令牌的存储代价，结果如表 2 所示。其中，*Depth* 表示令牌树深度，N_s 表示可容纳的系统最大人数，*OTC* 表示传输令牌链集的通信开销，*OKC* 表示计算密钥链的时间开销，*OTS* 表示存储所有令牌的存储开销。结果显示，随着令牌树的深度增加，这三者的开销均会随之增加。由于获得密链钥的计算是 192 bit 的异或操作，故其计算代价可忽略不计。考虑到 SNSP 的存储能力，所有令牌的存储代价也是可以接受的。

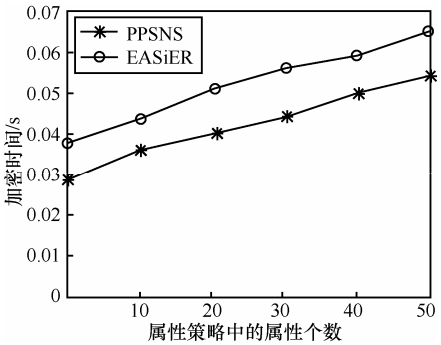


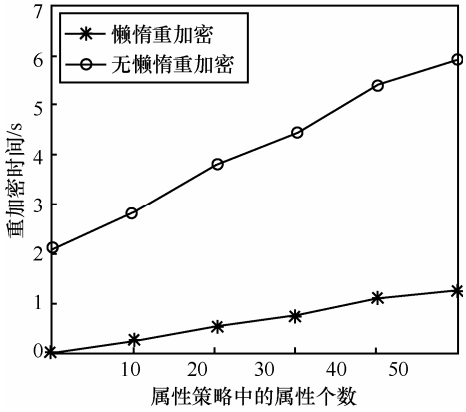
图 6　解密时间对比

表 2　令牌相关效率分析

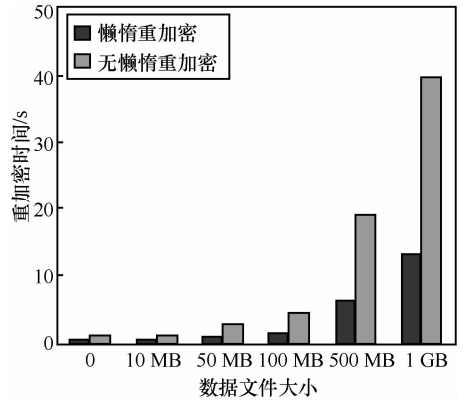
Depth	N_S	*OTC*/byte	*OKC*/ms	*OTS*/MB
10	512	120	5	12
12	2048	144	6	48
14	8192	168	8	192
16	32768	192	9	768

实验 6　密文重加密时间效率。

密文重加密代价是衡量访问控制系统性能的至关重要指标。在 PPSNS 中，该代价包括 WT-CP-ABE 密文重加密和数据文件重加密。鉴于懒惰重加密思想，假定化 3 次属性撤销操作(3 次密文重加密)为一次密文重加密。图 7(a)展示了当数据文件大小为 50 MB 时，密文重加密时间随属性策略中属性个数变化的对比结果；图 7(b)展示了当属性策略中属性个数为 10 时，密文重加密时间随数据文件大小变化的对比结果。结果显示，PPSNS 采用懒惰重加密后，重加密代价显著降低。



(a)密文重加密随属性策略中的属性个数变化的时间对比



(b)密文重加密随数据文件大小变化的时间对比

图 7　重加密时间对比

7　结束语

近年来，社交网络的隐私数据保护成为一热点研究问题。针对现有方案的不足，通过设计带陷门的属性加密算法 WT-CP-ABE 和令牌树机制，提出了一种新的社交网络隐私保护方案 PPSNS。该方案既支持了仅 DO 的社交成员才可能访问该 DO 的数据的特点，又降低了 DO 的计算代价和社交成员的存储代价。在属性撤销时，无需更新剩余非撤销用户的私钥，并有效降低了密文重加密代价。该方案还能够避免 SNSP 与系统内部非授权用户的合谋攻击，且不泄漏用户任何属性信息。实验结果显示，该方案在计算代价、存储代价等方面比现有方案有明显优势。

与文献[11]方案类似，PPSNS 也可能存在着密钥泄密问题。例如用户将某 DO 分发的属主主私钥泄漏给非该 DO 的社交成员，或者是用户将属性陷门泄漏给非该属性群中的人员。为解决这一问题，可考虑采用文献[23,24]方案中的责任认定方法。在后续的工作中，一方面可考虑融合密文检索技术，将对隐私数据

的检索与访问有机的统一起来，实现一个功能更加完备的社交网络隐私保护系统；另一方面考虑到单一属性权威机构的性能瓶颈，可根据文献[25]方案的思想，设计多属性权威机构的社交网络隐私保护系统。

参考文献：

[1] KWAK H, LEE C, PARK H, *et al*. What is Twitter, a social network or a news media[A]. Proceedings of the 19th International Conference on World Wide Web[C]. Raleigh, NC, USA, 2010. 591-600.

[2] FOGEL J, NEHMAD E. Internet social network communities: risk taking, trust, and privacy concerns[J]. Computers in Human Behavior, 2009, 25(1): 153-160.

[3] LUCAS M, BORISOV N. Flybynight: mitigating the privacy risks of social networking[A]. Proceedings of the 7th ACM Workshop on Privacy in the Electronic Society[C]. Alexandria, VA, USA, 2008. 1-8.

[4] GUHA S, TANG K, FRANCIS P. NOYB: privacy in online social networks[A]. Proceedings of the First Workshop on Online Social Networks[C]. Seattle, WA, USA, 2008. 49-54.

[5] LUO W, XIE Q, HENGARTNER U. Facecloak: an architecture for user privacy on social networking sites[A]. Proceedings of the 12th International Conference on Computational Science and Engineering (CSE 2009)[C]. Vancouver, BS, Canada, 2009. 26-33.

[6] SUN J, ZHU X, FANG Y. A privacy-preserving scheme for online social networks with efficient revocation[A]. Proceedings of the 29th International Conference on Computer Communications (INFOCOM 2010)[C]. SanDiego, CA, USA, 2010. 1-9.

[7] BADEN R, BENDER A, SPRING N, *et al*. Persona: an online social network with user-defined privacy[A]. Proceedings of the ACM SIGCOMM 2009 Conference on Data Communication (SIGCOMM 2009)[C]. Barcelona, Spain, 2009. 135-146.

[8] JAHID S, MITTAL P, BORISOV N. EASiER: encryption-based access control in social networks with efficient revocation[A]. Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2011)[C]. HongKong, China, 2011. 411-415.

[9] LIANG X, LI X, LU R, *et al*. An efficient and secure user revocation scheme in mobile social networks[A]. Proceedings of International Conference on Global Telecommunications Conference (GLOBECOM 2011)[C]. Houston, TX, USA, 2011. 1-5.

[10] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[A]. Proceedings of the 28th International Symposium on Security and Privacy (S&P 2007)[C]. Berkeley, CA, USA, 2007. 321-334.

[11] HUR J, NOH D. Attribute-based access control with efficient revocation in data outsourcing systems[J]. IEEE Transactions on Parallel and Distributed Systems, 2011, 22(7): 1214-1221.

[12] LV Z, HONG C, ZHANG M, *et al*. A secure and efficient revocation scheme for fine-grained access control in cloud storage[A]. Proceedings of the 4th International Conference on Cloud Computing Technology and Science (CloudCom 2012)[C]. Taiwan, China, 2012. 545-550.

[13] 吕志泉，张敏，冯登国. 云存储密文访问控制方案[J]. 计算机科学与探索, 2011, 5(9): 835-844.
LV Z Q, ZHANG M, FENG D G. Cryptographic access control scheme for cloud storage[J]. Journal of Frontiers Computer Science and Technology, 2011, 5(9): 835-844.

[14] 孙国梓, 董宇, 李云. 基于 CP-ABE 算法的云存储数据访问控制[J]. 通信学报, 2011, 32(7): 146-152.
SUN G Z, DONG Y, LI Y. CP-ABE based data access control for cloud storage[J]. Journal on Communications, 2011, 32(7): 146-152.

[15] YU S, WANG C, REN K, *et al*. Attribute based data sharing with attribute revocation[A]. Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2010)[C]. Beijing, China, 2010. 261-270.

[16] 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.

[17] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[A]. Proceedings of the 21th Annual International Cryptology (CRYPTO 2001)[C]. Santa Rarbara, California, USA, 2001. 213-29.

[18] BEIMEL A. Secure Schemes for Secret Sharing and Key Distribution[D]. PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.

[19] WATERS B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization[A]. Proceedings of the 14th IACR International Conference on Practice and Theory of Public Key Cryptography (PKC 2011)[C]. Taormina, Italy,2011.53-70.

[20] KALLAHALLA M, RIEDEL E, SWAMINATHAN R, *et al*. Plutus: scalable secure file sharing on untrusted storage[A]. Proceedings of the 2nd USENIX Conference on File and Storage Technologies[C]. San Francisco, CR, USA, 2003. 29-42.

[21] FU K. Group Sharing and Random Access in Cryptographic Storage File Systems[D]. Massachusetts Institute of Technology, 1999.

[22] The functional encryption library[EB/OL]. http://code.google.com/p/libfenc/.

[23] LI J, ZHAO G, CHEN X, *et al*. Fine-grained data access control systems with user accountability in cloud computing[A]. Proceedings of the 2th International Conference on Cloud Computing Technology and Science (CloudCom 2010)[C]. Indianapolis, IN, USA, 2010.89-96.

[24] LI J, REN K, ZHU B, *et al*. Privacy-Aware Attribute-Based Encryption with User Accountability[M]. Information Security. Springer Berlin Heidelberg, 2009.347-362.

[25] CHASE M, CHOW S. Improving privacy and security in multi- authority attribute-based encryption[A]. Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS 2009)[C]. Chicago, IL, USA, 2009. 121-130.

作者简介：

吕志泉（1986-），男，湖北赤壁人，中国科学院博士生，主要研究方向为数据库与云计算安全。

洪澄（1985-），男，江西余干人，博士，中国科学院助理研究员，主要研究方向为数据库安全理论与技术。

张敏（1975-），女，安徽萧县人，博士，中国科学院副研究员、硕士生导师，主要研究方向为数据安全与隐私保护。

冯登国（1965-），男，陕西靖边人，博士，中国科学院研究员、博士生导师，主要研究方向为密码学与信息安全。

陈开渠（1976-），男，福建泉州人，硕士，国家超级计算深圳中心高级工程师，主要研究方向为网络安全、云计算安全。