云环境下SNS隐私保护方案

刘胜杰 王 静
(南京工业大学计算机科学与技术学院 南京 211816)

摘 要 社交网络存储的数据实际都是外包给并不完全可信的云服务商。针对社交网络隐私安全和属性更新问题,提出一种云环境中具有策略隐藏和属性撤销的属性基加密方案。通过分解密钥产生方式降低用户端的计算量,引入合数阶的双线性群实现访问策略隐藏,并利用令牌树和陷门机制灵活且高效地完成属性撤销。而且,该方案在标准假设下可被证明是安全的。因此,将该方案运用于社交网络,将数据加密存储于云服务端是安全可行的。与其他方案相比,该方案既保护了访问策略的隐私,又具有多样的访问控制功能,在计算和存储等方面更有优势。

关键词 隐私保护,属性加密,策略隐藏,属性撤销

中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2019.02.021

Privacy Preserving Scheme for SNS in Cloud Environment

LIU Sheng-jie WANG Jing
(College of Computer Science and Technology, Nanjing Tech University, Nanjing 211816, China)

Abstract In reality, data stored on social networks are often outsourced to the untrusted cloud services providers. Aiming at the problems of privacy and attribute updating of social network, an attribute-based encryption scheme with hidden policy and attribute revocation in cloud environment was proposed. This scheme reduces the computation of client by breaking down the way of key generation. Moreover, the policy is hidden by using the composite order bilinear groups, and a mechanism with token tree and attribute trapdoor is used to achieve an efficient and flexible attribute revocation. In addition, the scheme is proved to be secure under the standard assumption. So, using this encryption in social network service to encrypt data to cloud servers is safe and feasible. Compared to other related works, this scheme protects the privacy of access policy and gives a better performance in computing and storage with access control functions.

Keywords Privacy preserving, Attribute-based encryption, Hidden policy, Attribute revocation

1 引言

随着互联网的深入推进,社交网络(Social Network Service,SNS)发展迅猛,并由此衍生出多种功能,渗透到生活的各方面,例如,在可允许范围内半公开用户的某些资料信息,用户可使用网络交流、交友和评论等服务。尤其是随着移动智能终端的迅速普及,社交网络的数据量快速增长。云计算作为一种新的商业模式,受到学术界和产业界的格外重视。社交网络服务提供商(SNS Provider,SNSP)充分利用云计算的优势将大量的社交网络数据外包存储于并不完全可信的云服务端,而不是建立和维护本地数据中心[1]。云计算确实满足了社交网络的应用部署和数据存储的需求,管理了更多的隐私数据(如姓名、地址、当前位置、私密照片或视频等),这使得大量存储于云端的社交网络外包数据备受用户关注[2]。然而,在社交网络中,隐私安全问题一直不容乐观,社交网络侵犯个人隐私的案例已屡见不鲜[3]。因此,对于社交网络而言,其首要目标是保证数据的安全性。

Sahai等于2005年将属性基加密机制(Attribute-based Encryption,ABE)引入到加密领域,提出了模糊身份加密方案[4],此方案在保证数据机密性的同时实现了灵活的访问控制功能。社交网络在某种程度上是一定范围内数据共享的方案,其数据正在成为探索和吸引不同研究领域的巨大资源[5]。而云计算是一种提供数据共享服务的优秀平台,尤其是基于属性加密技术的使用,云计算实现了细粒度数据共享的策略而受到广泛关注。随着加密技术的发展,一种基于密文策略的属性加密技术CP-ABE(Ciphertext-Policy ABE)被提出,其可由加密者根据自身属性自定义数据的访问策略,此技术保证了在细粒度访问控制的同时还兼具更好的灵活性。例如,通过制定相应的访问策略可以满足社交网络中对不同数据访问者实现不同的访问控制的需求。在现实云计算系统中,CP-ABE拥有如下优点:由于策略是由数据属主(Data-Owner,DO)根据自身的属性来制定的,因此数据拥有者DO

到稿日期:2017-11-22 返修日期:2018-03-23

刘胜杰(1988-),男,硕士,主要研究方向为云计算安全;王 静(1982-),女,博士,副研究员,主要研究方向为无线传感器网络、网络安全,E-mail:wj1982@126.com(通信作者)。

可以为其拥有的文件定义不同的访问策略；所有用户的私钥都不同，这是因为私钥是由用户的属性生成的；如果需要修改访问策略，那么 DO 无需修改公钥和私钥。因此，云环境中 CP-ABE 方案被认为是隐私保护的最佳选择。

社交网络是一个以个人为中心的在线门户，现已成为每个人生活的重要组成部分[6]。对于社交网络隐私的保护，Li 等[7]提出了一个在朋友和陌生人之间共享位置的方案。该方案中，用户好友被社交网络服务器随机分成多个子集，且每个位置服务器只能获得一个子集的朋友。这在一定程度上提高了数据访问的效率，但此方案只针对服务提供者发起的内部攻击进行保护，并没有考虑其他攻击类型。在数据分享方面，Fan 等[8]在云环境中对用户进行逻辑上的区域划分，并采用不同的方案来保护数据的隐私性。然而，这并不能很好地应对社交网络即时变化的特性，同时在数据访问控制方面也未考虑灵活性。EASiER[9]是一个成功地将 CP-ABE 运用于社交网络隐私保护的策略，但存在以下不足：私钥计算复杂度与其属性集线性相关，随着社交人数的增长，很可能导致 DO 端的性能急剧下降；未能既支持用户成员属性的动态变化，又可以实现属性层的用户撤销[10-11]；未将访问策略保护起来，因此访问策略中的信息很有可能被窃取。

针对以上问题，本文提出了一种在云计算环境中具有策略隐藏和属性撤销的属性基加密方案，具体工作如下：

1）设计了带陷门的 CP-ABE 算法，只有 DO 的社交成员才可能访问该 DO 数据，同时降低了 DO 和用户端的计算量，节约了用户的存储空间。

2）引入合数阶双线性群，实现对复杂的访问策略结构（与、或、门限）进行隐藏，更好地保护了用户的隐私。

3）运用令牌树和陷门机制灵活且高效地完成属性撤销，且无需更新不撤销属性用户的私钥。

2 预备知识

2.1 属性加密相关定义

定义 1（合数阶的双线性群） 设 p,r 为两个不相同的素数，G 和 G_T 是阶为 N 的循环群，其中 $N=p*r$，$G\times G\rightarrow G_T$ 是双线性映射，合数阶的双线性群满足如下规则：

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

2）非退化性：$e(u,v)\neq 1$。

3）正交性：G_p 和 G_r 分别表示 G 的阶为 p 和 r 的子群，g_p 和 g_r 分别表示 G_p 和 G_r 的生成元，则有 $e(g_p,g_r)=1$。

定义 2（群的阶） 群 G 中元素的总个数称为群的阶，简记为 $|G|$，当 $|G|$ 为合数时，称群 G 为合数阶的群。

定义 3（属性群） 令 $A=\{1,2,\cdots,k\}$ 为全体属性集合，$U=\{u_1,\cdots,u_m\}$ 为全体用户集合，属性群 $G(x)$ 表示拥有属性 x 的全部用户集合。

定义 4（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 才可得到属性 x 对应的属性陷门 TD_x。

定义 5（线性秘密共享（Linear Secret Sharing Scheme，LSSS）[12]） 令 (M,ρ) 代表一个属性策略 p，其中，M 为 $l\times h$ 的矩阵，ρ 为单射函数，对于 $i=1,\cdots,l$，$\rho(i)$ 表示与 M 的第 i 行所关联的属性。S 为满足策略 p 的属性集，$I=\{i|\rho(i)\in S\}$，$\vec{M}_i$ 为 M 第 i 行组成的向量，并由 M 计算得到满足 $\sum_{i\in I}\theta_i\vec{M}_i=\{1,0,\cdots,0\}$ 的一组常系数 $\{\theta_i\in Z_p\}_{i\in I}$。当 S 不满足属性策略 p 时，这组常系数不存在。

2.2 令牌树机制

令牌树是一棵完全二叉树，边对应令牌，节点对应随机密钥，一个叶子节点对应一个用户 u_t，用户私钥的 $TDKey$ 为叶子节点的随机密钥。设二叉树的深度为 D，则第 D 层的所有节点都依次连续在最左边，其他层都是满节点。

令 Φ_x 为令牌树与 $G(x)$ 中用户对应的所有叶子节点的集合，$\Psi_{(x)}$ 为覆盖 Φ_x 节点的最小集合，则令牌树中与 $\Psi_{(x)}$ 对应节点的随机密钥的集合称作属性 x 的最小覆盖密钥集（Minimum Cover Key Set，MCKS），用 $MCKS_x$ 表示。令 n_i 为令牌树中某个叶子节点，则 n_i 到令牌树根途经的一切节点（包括两端的 n_i 和根节点）对应的所有随机密钥的集合称作 n_i 的密钥链集（Key Chain Set，KCS），用 KCS_i 表示，而 n_i 到令牌树根途经的一切令牌的集合称为 n_i 的令牌链集（Token Chain Set，TCS），用 TCS_i 表示。

令牌树机制的安全性由如下 3 个定理保证。

定理 1 若叶子节点 n_i 的随机密钥及其到根节点途经的边上的令牌已知，则节点 n_i 的密钥链集 KCS_i 可恢复。

定理 2 若只已知叶子节点 n_i 的随机密钥，尽管得到树中的全部令牌，也无法恢复除了 n_i 到根节点途经的节点以外的任何一个节点所对应的随机密钥。

定理 3 n_t 为用户 $u_t(1\leqslant x\leqslant m)$ 相对应的叶子节点。当 $u_t\in G(x)(1\leqslant x\leqslant k)$ 时，有且仅有一个元素使得 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

如图 1 所示，基于云环境的社交网络主要包括 4 个实体：云端社交网络服务提供者 SNSP、可信任的属性权威机构 AA、上传数据的数据属主 DO 和作为数据访问者角色的社交网络用户。

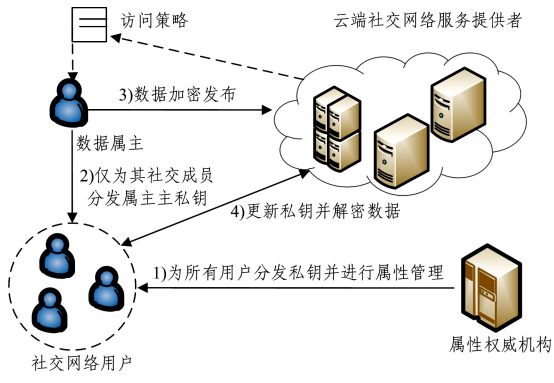

图 1 基于云环境的社交网络的系统模型

Fig. 1 System model of social network based on cloud environment

本方案的系统模型[13-15]中 AA 完全可信，承担系统初始化、用户端私钥的计算及分发、社交系统的属性管理、用户属性撤销的职责。云端社交网络服务提供者为 DO 提供数据的存储、社交网络应用服务以及访问策略生成的主要任务。属主主私钥由 DO 生成与分发，DO 通过云端定义并获取访问策略。数据访问者必须先使用 DO 对应的属主主私钥来更新自己的私钥，再得到相应的属性陷门，最后在符合访问策略的要求后才可以进行解密操作。

3.2　算法设计

本文提出的算法基于 WT-CP-ABE[16]进行改进，以 CP-ABE 为基础改变系统和用户密钥的生成方式，分解了密钥产生功能，引入陷门和令牌树机制实现撤销功能，同时使用合数阶双线性群达到访问策略信息隐藏的目的。本文方案中 5 个主要算法的函数描述如下。

算法 1　$Setup(1^{\lambda},k)$

λ 是一个安全参数，参数 k 表示系统中所管理属性的个数。此算法运用双线性参数生成器计算 $\Theta=(N=p_1p_2p_3,G,G_T,e)$，其中 p_1,p_2,p_3 是 λ 阶的 3 个不相同的素数。选择随机的生成元 $g_1,u_1,\cdots,u_k\in G_{p_1}$，$g_3\in G_{p_3}$，$e$ 是 $G\times G\to G_T$ 的双线性映射，定义一个系统所需的属性空间集合为 $A=\{1,2,\cdots,k\}$，对于任意属性 $x\in A(1\leqslant x\leqslant k)$，随机选择 $\eta_x,TD_x\in Z_p$，选择 $a,y_1,\cdots,y_k\in Z_N$，定义属性集 $A_1=u_1g_3^{y_1},\cdots,A_k=u_kg_3^{y_k}$，并计算 $E_x=g_1^{\eta_x TD_x}$ 生成主公钥 APK 和主私钥 ASK：

$$APK=\langle\Theta,g_1,g_3,g_1^{a},A_1,\cdots,A_k,E_1,\cdots,E_k\rangle$$

$$ASK=\langle\eta_x,\{TD_x\}_{x\in A}\rangle$$

其中，η_x 用于属性相关计算，TD_x 用于属性撤销计算。而 DO 端随机选择 $\alpha\in Z_p$，计算主私钥 $OSK=\langle g_1^{\alpha}\rangle$ 和公开密钥 $OPK=\langle e(g_1,g_1)^{\alpha}\rangle$。

算法 2　$KeyGen(ASK,S)$

运用 ASK 计算生成属性集 S 对应的私钥。首先选择一个随机参数 $t\in Z_p$，计算 $K_1=g_1^{\alpha}g_1^{at}$，$K_2=g_1^{t}$。对于任意属性 $x\in S$，分别计算 $K_x=u_x^{t}$ 和 $D_x=g_1^{\eta_x t}$。然后，选择一随机陷门密钥 $TDKey$。最后，输出用户私钥 SK 为：

$$SK=\langle K_1,K_2,\{K_x\}_{x\in S},\{D_x\}_{x\in S},TDKey\rangle$$

其中，t 是用于随机化私钥的一个参数，其功能是避免用户攻击；$TDKey$ 是在属性撤销时用于恢复陷门的参数。

算法 3　$Encrypt(APK,OPK,P,m)$

利用 APK、OPK 和属性策略 P 加密明文 m。首先，生成属性策略 P 的 (M,ρ)，其中，M 为 $l\times h$ 的矩阵，ρ 为一个单射函数。然后随机选择 n 维的向量 $\vec{v}=(s,v_2,\cdots,v_n)\in Z_p^n$，其中 s 表示待分享秘密，计算 $C_1=m\cdot e(g_1,g_1)^{\alpha s}$，$C_2=g_1^{s}R_0$。令 $\vec{M}_i$ 为 M 第 i 行所组成的向量，$i\in\{1,2,\cdots,l\}$，计算 $\lambda_i=\vec{M}_i\vec{v}$。选择随机数 $r_1,\cdots,r_l\in Z_N$，$R_0\in G_{p_3}$，$\{R_i,R_i'\in G_{p_3}\}_{i\in\{1,\cdots,l\}}$，计算 $T_i=g_1^{a\lambda_i}A_{\rho(i)}^{-r_1}R_i'$，$W_i=g_1^{r_i}R_i$，得出密文：

$$CT=\langle C_1,C_2,(\{T_i,W_i\}_{i\in\{1,2,\cdots,l\}})\rangle$$

算法 4　$KeyUpdate(OSK,SK)$

使用 OSK 更新私钥 SK：

$$SK=\langle K_1=g_1^{2\alpha}g_1^{at},K_2,\{D_x\}_{x\in S},TDKey\rangle$$

算法 5　$Decrypt(SK,CT)$

使用私钥 SK 解密密文 CT。只有当 SK 关联的用户属性集 S 满足密文 CT 中的策略 (M,ρ) 且符合 $I=\{i:\rho(i)\in S\}$ 时，$W=\{\rho(i)\mid\rho(i)\in S\}$。若可以在多项式时间内算得一个 $\{\omega_i\in Z_N\}_{i\in I}$ 常数集，使得 $\sum_{i\in I}\omega_i\lambda_i=s$，其中 λ_i 是秘密 s 的有效分享，则可以正确解密。假设对于任意属性 $\rho(i)\in W$，凭借陷门密钥 $TDKey$ 获取了属性陷门 $TD_{\rho(i)}$，则计算：

$$\frac{e(C_2,K_1)}{\prod_{i\in I}(e(T_i,K_2)e(W_i,K_{\rho(i)}))^{\omega_i}}=e(g_1,g_1)^{\alpha s}\tag{1}$$

运用式(1)能将明文 m 恢复。

3.3　方案描述

3.3.1　系统启动并初始化

AA 运行 $Setup(1^{\lambda},k)$，生成系统公钥 APK 和系统主私钥 ASK，DO 与 AA 协作生成主私钥 OSK 和公开密钥 OPK。

3.3.2　用户注册及陷门发布

假设一个新用户 u_t 在云端注册加入社交网络，并能够登录到个人中心，查看、增加和修改自身的隐私数据。AA 根据 u_t 的身份特征，生成相应属性集 S。然后，执行 $KeyGen(ASK,S)$ 并生成私钥 SK，运用安全通道将 SK 发送给 u_t。接着，AA 更新属性群并发布新的陷门信息(Trapdoor Message，TDM)，目的是解决新用户的加入或属性撤销导致其他用户对密文的访问。首先，建立一棵令牌树，对于任意系统中的属性 x，根据其属性群 $G(x)$ 获取最小覆盖密钥集 $MCKS_x$，并计算陷门信息 $TDM_x=\{E_{RK_j}(TD_x)\}_{RK_j\in MCKS_x}$。其中，$TD_x$ 为 x 的陷门，RK_j 为随机密钥，E 为对称加密算法。接着发布 $TDM=\{TDM_x\}_{x\in A}$ 和令牌链 $TCS=\{TCS_i\}_{i\in\{1,2,\cdots,m\}}$。

3.3.3　隐私数据发布

DO 向与其有社交关系的用户发送自己的主私钥 OSK 分享信息。DO 端对数据文件进行处理，ABE 算法具有复杂性，不宜对大文件进行加密，否则会大大降低系统性能，因此采用混合加密方式。先用对称加密算法加密文件数据，再对对称加密密钥 DEK(Data Encryption Key)采用 ABE 算法进行加密，过程如下：

1)选取一对称密钥 DEK 加密文件 f，得到数据密文 $DEK(f)$，并为其分配唯一文件编号 ID_f。

2)定义数据文件访问策略 P，利用 APK 和 OPK，运行 $Encrypt(APK,OPK,P,m)$ 算法加密 DEK，得到密文 CT_f，将密文上传到云服务中心。

3)对于任意属性 $x\in V$，$V=\{\rho(i)\mid 1\leqslant i\leqslant l\}$，运用陷门信息 TDM_x 构成 $TDM_f=\{TDM_x\}_{x\in V}$。

综合以上步骤，存储于社交云服务端中的数据的文件格式如图 2 所示。

ID_f	TDM_f	CT_f	$DEK\{f\}$

图 2　云端文件的存储格式

Fig. 2　Storage format of cloud file

3.3.4　数据访问

当用户 u_t 对编号 ID_f 文件进行访问时，社交云服务端返

回云端对应的存储数据和该用户令牌链 TCS_t，u_t 的解密过程如下：

Step1 通过定理 1 可知，密钥链集 KCS_t 可由用户 u_t 运用 s 中的陷门密钥 $TDKey$ 和令牌链 TCS_t 计算得到。若 u_t 可解密 CT_f，则其私钥 SK 的属性集 S 肯定满足策略 (M,ρ)。根据定理 3 可知，用户 u_i 可根据存在的相同随机密钥 $RK_y \in MCKS_x$ 解密 TDM_x，最终得到属性陷门 TD_x。

Step2 u_t 首先执行 $KeyUpdate(OSK,SK)$ 算法来更新私钥 SK，接着用户将 Step 1 所得结果和私钥 SK 输入到 $Decrypt(SK,CT)$ 算法[17] 中以解密 CT_f，若用户私钥符合密文的访问策略，则获得对称密钥 DEK，从而正确解密并访问文件，否则失败。

3.3.5 属性撤销

当用户属性发生变化时，AA 需要撤销相应属性。u_t 为撤销的用户，R 为撤销的属性集合，则 AA 端属性撤销操作过程如下：

Step1 AA 更新属性陷门信息。对于任意属性 $x \in R$，随机产生新属性陷门 TD_x'，对于与 x 相应的属性群 $G(x)$，更新最小覆盖密钥集 $MCKS'_x$，生成新陷门信息 $TDM_x' = \{E_{RK_j}(TD_x')\}_{RK_j \in MCKS_x'}$，更新属性陷门信息为 TDM_x'。

Step2 更新 APK 与 ASK。对于属性 $x \in R$，更新其在 APK 中对应的组件 $E_x' = E_x^{TD_x'/TD_x}$，替换 ASK 中的 TD_x 为 TD_x'。

Step3 DO 执行密文重加密，用新对称密钥 DEK' 加密文件，得到 $DEK'(f)$。再运行属性加密算法加密 DEK'，得到密文 CT_f'。令 $V=\{\rho(i)\mid 1\leqslant i\leqslant l\}$，$VR=V\cap R$（$R$ 为撤销属性集合），若 $VR=\varnothing$，则不更新陷门信息，否则更新 TDM_x 为 TDM_x'。

4 安全性

4.1 安全性分析

攻击者可获得一随机策略 (M',ρ') 和经 (M,ρ) 加密得到的密文 $CT=\langle C_1,C_2,(T_1,W_1),\cdots,(T_l,W_l)\rangle$。因此，攻击者可根据 M' 选择 $I'\subset\{1,\cdots,l\}$，并进行运算。若 $\{\lambda_i'\}$ 是秘密 s 的有效分享，则在多项式时间内，攻击者可以计算得到常数 $\{\omega_i'\in Z_N\}_{i\in I'}$，使得 $\sum_{i\in I'}\omega_i'\lambda_i'=s$，运算如下：

$$\frac{e(C_2,g_1^a)}{\prod_{i\in I'}(e(T_i,g_1)e(W_i,A_{\rho'(i)}))^{\omega_i'}}=\frac{e(g_1^sR_0,g_1^a)}{\prod_{i\in I'}(e(g_1^{a\lambda_i}(u_{\rho'(i)}g_3^{y_{\rho'(i)}})^{-r_i}R_i',g_1)e(g_1^{r_i}R_i,u_{\rho'(i)}g_3^{y_{\rho'(i)}}))^{\omega_i'}}$$

$$=\frac{e(g_1,g_1)^{as}}{\prod_{i\in I'}(e(g_1^{a\lambda_i},g_1)e(R_i,g_3^{y_{\rho'(i)}}))^{\omega_i'}}=\frac{e(g_1,g_1)^{as}}{e(g_1,g_1)^{a\sum_{i\in I'}\lambda_i\omega_i'}\prod_{i\in I'}(e(R_i,g_3^{y_{\rho'(i)}}))^{\omega_i'}} \tag{2}$$

若 $(M',\rho')=(M,\rho)$，则 $\sum_{i\in I'}\lambda_i\omega_i'=s$，此时式(2)为：

$$\frac{1}{\prod_{i\in I'}(e(R_i,g_3^{y_{\rho'(i)}}))^{\omega_i'}} \tag{3}$$

若 $(M',\rho')\neq(M,\rho)$，则 $\sum_{i\in I'}\lambda_i\omega_i'\neq s$，此时式(2)为：

$$\frac{e(g_1,g_1)^{as}}{e(g_1,g_1)^{a\sum_{i\in I'}\lambda_i\omega_i'}\prod_{i\in I'}(e(R_i,g_3^{y_{\rho'(i)}}))^{\omega_i'}} \tag{4}$$

式(3)和式(4)中都含有 G_T 中的随机元素。因此，攻击者无法确定 CT 是否由 (M',ρ') 加密而成，故本文方案实现的策略隐藏是安全的。

本文算法以 CP-ABE 为基础，在标准模型下被证明是安全的[18]。AA 在属性撤销时随机产生新的 TD_x，并且由被撤销用户未知的随机密钥加密，故被撤销用户无法获取，从而无法正确解密。因此，属性撤销机制也是安全的。

4.2 安全性证明

定理 4 假设 DBDH 成立，若多项式时间内没有攻击者能够以不可忽略的优势破坏所提出的方案，则该方案满足 CPA 安全。

假设攻击者 F 在挑战系统的选择性安全游戏中有不可忽视的优势 $\varepsilon=Adv_F$，那么可以构造一个模拟器 B 以 $\frac{\varepsilon}{2}$ 的优势从一个随机元组中区分 DBDH 元组。定义 $e:G\times G\rightarrow G_T$ 是高效率的双线性映射，G 是由生成元 g 生成的阶为 p 的群。

首先，DBDH 挑战者随机选择以下参数 $a,b,c\in Z_p$，$\mu\in\{0,1\}$，生成元 $g\in G$，随机元素 $R\in G_T$。若 $\mu=0$，则挑战者定义 $T=e(g,g)^{abc}$，否则设置 $T=R$。接着，DBDH 挑战者对模拟器所传递的内容为 $\langle g,g^a,g^b,g^c,T\rangle$，此时模拟器 B 在安全游戏中扮演挑战者角色。为了便于描述，过程仅仅对一个数据文件进行加密。

初始化：攻击者 F 选择具有挑战性的访问结构 F^*，并且发送 F^* 给模拟器 B。

运行建立：向攻击者 F 发送公钥 APK 和 OPK。模拟器 B 选择一个随机数 $\beta\in Z_p$，设置 $\alpha=\beta+ab$，利用规则计算 $e(g,g)^{\alpha}=e(g,g)^{\beta}e(g,g)^{ab}$，同时设置 $h=g^{\beta}=B=g^b$。最后模拟器 B 将 APK 和 OPK 发送给攻击者 F。

询问阶段 1：攻击者 F 可通过提交属性集 $W_j=\{a_j\mid a_j\in F\}$，$W_j\notin F^*$，询问私钥 SK。首先模拟器 B 选择一个随机数 $\eta\in Z_p$，并且设置 $r=\eta-a$，通过计算得到：$D=g^{\alpha}\cdot h^r=g^{\alpha}\cdot g^{\beta r}=g^{\beta+ab}\cdot g^{b(\eta-a)}=g^{(\beta+b\eta)}$。接着对每个属性 $a_j\in W_j$，B 需要选择随机数 $r_j\in Z_p$，最后构造私钥剩下的部分：$D_j=g^{(\eta-a)}\cdot H_1(j)^{r_j}$，$D_j'=h^{r_j}=g^{b\cdot r_j}=B^{r_j}$，并将私钥发给攻击者 F。此外，模拟器 B 还需要计算用户属性生成对应的令牌链 $TCS=\{TCS_j\}_{j\in\{1,2,\cdots,m\}}$，并将令牌链也发给攻击者 F。

挑战：攻击者 F 提交两个等长的信息 m_0 和 m_1。模拟器 B 随机生成一位的 $\hat{\mu}\in\{0,1\}$，在 F^* 下运行加密算法，计算访问结构 F^* 对应的密文 CT^* 部分，$C_1=m_{\hat{\mu}}\cdot e(g,g)^{as}=m_{\hat{\mu}}\cdot e(g,g)^{a\alpha}=m_{\hat{\mu}}\cdot Te(g,g)^{\beta c}$，$C_1=g^s=g^c=C$，使用最小覆盖密钥集生成陷门信息 $TDM_j=\{E_{RK_j}(TD_j)\}_{RK_j\in MCKS_j}$，将 CT^* 和陷门信息都发给攻击者 F。

询问阶段 2：与询问阶段 1 相同。

猜测：攻击者 F 对 $\hat{\mu}$ 进行猜测的结果为 $\hat{\mu}'$，若 $\hat{\mu}=\hat{\mu}'$，则模拟器 B 输出 0，猜想得到 $T=e(g,g)^{abc}$。否则，模拟器 B 输出

1，也就是 T 是 G_T 中的一随机元素。若 $T=e(g,g)^{abc}$，则 CT 是有效的密文，这种情况下攻击者的优势是 ε。

$$Pr[B(g,g^a,g^b,g^c,T=e(g,g)^{abc})=0]=\frac{1}{2}+\varepsilon$$

若 $T=R$，则攻击者 F 认为 C_1 是完全随机的。无论怎样对 $\hat{\mu}'$ 计算，$\hat{\mu}\neq\hat{\mu}'$ 的概率都是 $\frac{1}{2}$。

$$Pr[B(g,g^a,g^b,g^c,T=R)=0]=\frac{1}{2}$$

最终，在此安全游戏中模拟器 B 的优势结果如下：

$$Adv_B=\frac{1}{2}Pr[B(g,g^a,g^b,g^c,T=e(g,g)^{abc})=0]+\frac{1}{2}Pr[B(g,g^a,g^b,g^c,T=R)=0]-\frac{1}{2}$$

$$=\frac{1}{2}\cdot(\frac{1}{2}+\varepsilon)+\frac{1}{2}\cdot\frac{1}{2}-\frac{1}{2}=\frac{\varepsilon}{2}$$

由此可见，本方案满足 CPA 安全。

5　实验分析

具体实验环境如下：由于硬件环境有限，没有真正的云计算系统可供使用，因此只有通过模拟的方式进行实验。实验计算机的内存为 8GB，处理器为 Intel(R) Core™ i5-3470，3.2 GHz，系统为 Red Hat Enterprise Linux 6.5 64，运用 OpenStack 模仿云计算服务端环境。再用 3 台计算机分别模拟属性权威机构、数据属主、社交访问者。另外，需要在计算机系统环境中安装一些库文件，如 PBC，libfenc 等。实验中，对称加密算法采用 openssl-1.1.0c 库的 128 bit AES 算法。

5.1　加密时间对比

从图 3 可以看出，无论是 EASiER 方案[9]还是本文方案，当属性数量不断增加时，系统的加密时间也随之变长。对比两种方案在图 3 中的同一属性数量处的加密时间不难发现，本文方案的耗时相对来说更长，但差距非常小，影响不大，属于同一数量级的时间开销。其原因是本文方案在加密过程中需要对访问策略以及属性陷门进行处理，增加了少量的计算步骤。

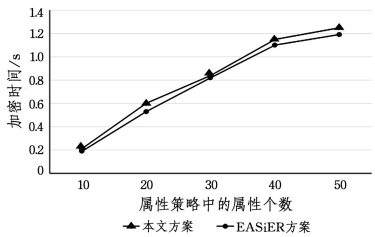

图 3　加密时间对比

Fig. 3　Comparison of encryption time

5.2　用户解密数据时间对比

图 4 展示了 EASiER 方案[9]和本文方案在用户端解密密文 CT 的时间变化情况。由图可知，两种方案的时间也都是随着策略中属性数量的增加而变长。由于本文方案在算法解密的操作中减少了一些计算量，因此解密时间相对于 EASiER 方案[9]更短，略微提高了性能。综合实验可发现，相比于另一种方案，本文方案在完善系统功能、保证系统数据隐私安全性的同时没有降低系统的性能，因此更有优势。

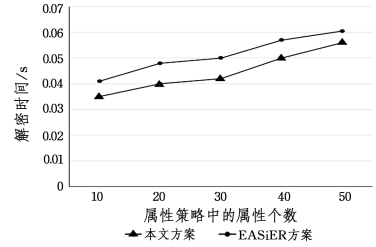

图 4　解密时间对比

Fig. 4　Comparison of decryption time

5.3　用户私钥存储代价对比

图 5 展示了 EASiER 方案[9]和本文方案在单个用户端的私钥存储代价情况。通过观察不难发现，随着与该用户有社交关系的 DO 人数的增长，EASiER 方案[9]存储代价的增长非常明显，几乎呈线性增长，而本文方案几乎保持不变，始终处于同一数量级，没有明显的增长趋势。这是因为本文方案中用户只需存储自己的私钥 SK 和 DO 发送的 OSK，但是在 EASiER 方案中[9]用户需要存储所有与其有社交关系的 DO 发送的私钥 SK，这显然增加了用户端的存储量。相比之下，本文方案在用户端私钥存储的开销很小，有绝对的优势。

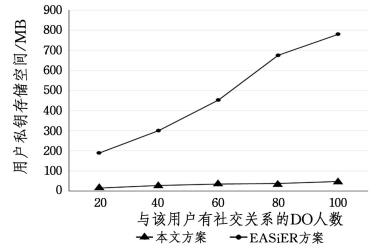

图 5　用户私钥存储代价对比

Fig. 5　Comparison of user's private key storage cost

结束语　社交网络的发展是社会的重要热点之一。本文方案针对现有方案的不足，将社交网络功能与云计算紧密结合，同时针对 CP-ABE 算法进行改进，引入陷门和令牌树机制实现属性撤销，同时使用合数阶的双线性群实现用户访问策略的隐藏。在没有降低系统性能的同时很好地保护了访问结构中的敏感信息，极大地提高了系统的安全性，保护了用户的隐私。实验分析结果显示，该方案在计算代价、访问灵活性以及隐私保护等方面比现有方案更优。

由于属性权威机构承担属性更新、系统及主私钥的分发的任务，因此承担的任务较重，而且使用合数阶的双线性群也在一定程度上增加了计算量。因此，今后应进一步研究更高效的算法，减少繁琐的计算步骤，从而更好地实现社交网络的功能。

参 考 文 献

[1]　NING J T，CAO Z F，DONG X L，et al. Auditable σ-Time Outsourced Attribute-Based Encryption for Access Control in Cloud Computing [J]. IEEE Transactions on Information Forensics

and Security,2018,13(1):94-105.

[2] LI J G,YAO W,ZHANG Y C,et al. Flexible and fine-grained attribute-based data storage in cloud computing [J]. IEEE Transactions on Services Computing,2017,10(5):785-796.

[3] HU X P,CHU T H S,LEUNG V C M,et al. A Survey on Mobile Social Networks:Applications,Platforms,System Architectures,and Future Research Directions [J]. IEEE Communication Surveys & Tutorials,2015,17(3):1557-1581.

[4] SAHAI A,WATERS B. Fuzzy identity-based encryption[C]// International Conference on Tecony & Applications of Cryptographic Techniques. 2005:457-473.

[5] ZHU Y Q,LI D Y,YAN R D,et al. Maximizing the Influence and Profit in Social Networks [J]. IEEE Transactions on Computational Social Systems,2017,4(3):54-64.

[6] DEEPALI V,DEEPALI N. Privacy preservation in SMAC-social networking,mobile network,analytics and cloud computing[C]// 2017 International Conference on I-SMAC (IoT in Social,Mobile,Analytics and Cloud) (I-SMAC). Palladam,India:IEEE,2017:801-807.

[7] LI J,YAN H,LIU Z,et al. Location-Sharing Systems With Enhanced Privacy in Mobile Online Social Networks [J]. IEEE Systems Journal,2017,11(2):439-448.

[8] FAN K,TIAN Q,WANG J X,et al. Privacy protection based access control scheme in cloud-based services [J]. China Communications,2017,14(1):61-71.

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

[10] RUJ S,STOJMENOVIC M,NAYAK A. Decentralized access control with anonymous authentication of data stored in clouds [J]. IEEE Transactions on Parallel and Distributed Systems,2014,25(2):384-394.

[11] HUR J,KANG K. Secure data retrieval for decentralized disruption-tolerant military networks [J]. IEEE/ACM Transactions on Networking,2014,22(1):16-26.

[12] WATERS B. Ciphertext-policy attribute-based encryption:An expressive,efficient,and provably secure realization[C]// Public Key Cryptography-PKC 2011. Berlin Heidelberg: Springer,2011:53-70.

[13] WAN Z,LIU J E,DENG R H. HASBE:a hierarchical attribute-based solution for flexible and scalable access control in cloud computing [J]. Information Forensics and Security,2012,7(2):743-754.

[14] CHEN Y L,SONG L L,YANG G. Efficient Access Control Scheme Combining CP-ABE and SD in Cloud Computing [J]. Computer Science,2014,41(9):152-157,168. (in Chinese)
陈燕俐,宋玲玲,杨庚. 基于 CP-ABE 和 SD 的高效云计算访问控制方案 [J]. 计算机科学,2014,41(9):152-157,168.

[15] ZHOU Z,HUANG D,WANG Z. Efficient Privacy-Preserving Ciphertext-Policy Attribute Based-Encryption and Broadcast Encryption [J]. IEEE Transactions on Computers,2015,1(64):126-138.

[16] LV Z Q,HONG C,ZHANG M,et al. Privacy-perserving scheme for social networks [J]. Journal on Communications,2014,35(8):23-32. (in Chinese)
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.

[17] ZHOU S G,DU R Y,CHEN J,et al. FACOR:flexible access control with outsourceable revocation in mobile clouds [J]. China Communications,2016,13(4):136-150.

[18] TRAN V X P,YANG G M,SUSILO W. Hidden Ciphertext Policy Attribute-Based Encryption Under Standard Assumptions [J]. IEEE Transactions on Information Forensics and Security,2016,11(1):35-45.