doi:10.11959/j.issn.1000-436x.2017200

# 移动社交网络中跨域代理重加密朋友发现隐私保护方案研究

罗恩韬[1,2]，王国军[2,3]，陈淑红[3,4]，PINIAL Khan-butt[5]

（1. 湖南科技学院电子与信息工程学院, 湖南 永州 425199； 2. 中南大学信息科学与工程学院, 湖南 长沙 410083；
3. 广州大学计算机科学与教育软件学院, 广东 广州 510006；4. 湖南工程学院计算机与通信学院, 湖南 湘潭 411101；
5. 信德农业大学信息技术中心, 巴基斯坦 信德 70060）

**摘 要**：在移动社交网络中，为保证交友过程中的用户隐私，提出跨域环境下的代理重加密交友隐私保护方案。利用跨域多授权中心共享密钥，实现了跨域用户数据的互相访问与共享；利用代理重加密与属性加密技术，对用户属性密钥进行重新加密，实现了以扩充交友访问策略条件的交友匹配；利用用户隐私密文文件与密钥分离技术，增强了用户数据的隐私性。解决了现有方案中存在的用户数据不能跨域跨云共享、交友过少匹配及用户下线不能交友的问题。安全和实验分析表明，方案可以达到选择明文攻击（CPA, chosen plaintext attack）安全，保证交友用户的隐私不被泄露，并且比现有方案更有效。

**关键词**：跨域数据访问；代理重加密；跨域多授权中心；属性加密；隐私保护
**中图分类号**：TP393 **文献标识码**：A

# Privacy preserving friend discovery cross domain scheme using re-encryption in mobile social networks

LUO En-tao[1,2], WANG Guo-jun[2,3], CHEN Shu-hong[3,4], PINIAL Khan-butt[5]

(1. School of Electronics and Information Engineering, Hunan University of Science and Engineering, Yongzhou 425199, China;
2. School of Information Science and Engineering, Central South University, Changsha 410083, China;
3. School of Computer Science and Educational Software, Guangzhou University, Guangzhou 510006, China;
4. School of Computer and Communication, Hunan Institute of Engineering，Xiangtan 411101, China;
5. Information Technology Center, Sindh Agriculture University, Tandojam 70060, Pakistan)

**Abstract:** In order to guarantee the users' privacy in the process of making friends in the mobile social networks, a new scheme of proxy re-encryption privacy protection in the cross-domain environment was introduced. The scheme employed the cross-domain multi-authority to sharing secret keys, so as to realize the access and shave of the cross-domain users data. And the secret keys of users' attributes were re-encrypted, based on the technology of the proxy re-encryption and attribute encryption, to achieve the friends matching under the conditions of extending the access policy. Meanwhile, in purpose of enhancing the privacy of users' data, the technology which contained the separation of users' privacy ciphertext and secret keys was adopted. Based on that, problems in the existing system such as user data's inability to be shared cross-cloud, less matching during the process of making friends and users' inability to make friends when offline had been addressed. Security and experimental analysis show that this scheme can achieve chosen plaintext attack (CPA) security, ensure the privacy of friend discovery, and that is more effective than existing solutions.

**Key words:** cross domain data access, proxy re-encryption, cross domain multi-authority, attribute-based encryption, privacy-preserving

---

**收稿日期**：2017-03-06；**修回日期**：2017-08-07
**通信作者**：王国军，csgiwang@gmail.com
**基金项目**：国家自然科学基金资助项目（No. 61632009, No. 61472451, No.61272151, No.61502163）；湖南省自然科学基金资助项目（No.2016JJ3051）；中央高校基本科研业务费专项基金资助项目（No.2016zzts060）；湖南省教育厅科研基金资助项目（No.2015C0589）；湖南省重点研发计划基金资助项目（No.2017NK2390）；湖南科技学院计算机应用技术重点建设学科基金资助项目（No.128030219-001）

**Foundation Items:** The National Natural Science Foundation of China (No.61632009, No.61472451, No.61272151, No.61502163), The Natural Science Foundation of Hunan Province (No.2016JJ3051), Special Fund for Basic Research and Business Expenses of Central Universities (No.2016zzts060), Research Project of Hunan Provincial Education Department (No.2015C0589), The Hunan Provincal Science and Technology Key Development Project (No.2017NK2390), The Key Construction of Computer Application Technology, Hunan University of Science and Engineering (No.128030219-001)

## 1 引言

随着移动社交网络（MSN, mobile social networks）和云计算的飞速发展[1]，用户之间可以利用APP应用在MSN中随时分享彼此的心情、照片、活动、兴趣爱好等信息，在移动社交网络中不断地发现新的朋友[2,3]，从而进一步扩大自己的社交范围。

但是，通过移动社交网络进行交友发现，给人们生活带来便利的同时，也引发了严重的隐私泄露问题[4]。例如，通过分析对方购物爱好，可以确认用户的消费能力；通过对用户朋友圈的分析，可以确认用户的身份；通过对用户运动数据或轨迹的分析，可以确认用户的身体状况等。而这些个人隐私信息一旦被泄露，极有可能对用户造成不可预测的后果，甚至威胁用户的生命和财产安全。

因此，如何在提供良好交友匹配服务基础上，进一步促进移动社交活动的开展，同时又能够保护用户个人隐私信息安全，是当前交友过程中亟待解决的一个热点问题。

## 2 相关工作

在移动社交网络中，利用加密技术可以对用户的隐私信息进行有效的保护。文献[5~8]通过计算用户属性私有交集（PSI, private set intersection）来保护用户的隐私。主要方法是匹配双方各持自己的私有数据集，通过计算共同交集或2个集合的交集的基数而不泄露任何一方额外的信息来保证双方的隐私。Zhang 等[9]提出根据用户的兴趣偏好分配不同的权重，并计算匹配的相似度。Niu 等[10] 进一步对用户的属性设置了优先级匹配。Zhu 等[11]提出一种改进向量变换算法来保护用户的隐私。但是，在以上方案中，用户只能比较属性集合中每个属性匹配的个数和权重，并没有考虑到用户交友需要属性多元化的组合以及访问控制，因此，应用范围比较有限。

随后，单可信授权中心结合属性加密方案被用来保护用户交友过程中的安全和隐私。这主要分为基于密钥的加密方案（KP-ABE, key policy attribute based encryption）[12~15]和基于密文的加密方案（CP-ABE, ciphertext policy attribute based encryption）[16~18]。在KP-ABE加密方案中，私钥关联访问控制结构，密文与属性集关联，如果数据请求者访问控制结构与数据拥有者的属性集合相匹配，就可以对加密消息进行解密。而在CP-ABE加密方案中，私钥关联属性集，密文与访问结构关联。如果数据请求者的属性集合符合数据拥有者设定的访问控制结构，那么密文就可以被数据请求者解密。

但是，单纯利用单授权中心与属性加密的交友方案，所有用户的密钥均由同一个可信中心生成，且用户特征匹配计算均在授权中心服务器上进行，因此可信中心在高峰服务期，存在性能服务瓶颈和计算瓶颈。

在后续工作中，文献[19]进一步改进了交友隐私保护方案，提出了基于多授权中心的属性加密方案，该方案用户密钥与用户数据由多个授权中心分别管理，可以为属性的匹配和消息的共享提供细粒度的访问控制。该方案在一定程度上解决了性能瓶颈问题，提高了安全性，但是依然存在局限性。

1) 不能解决交友用户数据云端的跨域共享。以前的模型交友用户均假定工作在同一个域中，用户所有公私钥的生成与分发均由同一个域的可信授权中心生成，但是在实际的应用场景中，用户的数据通常存储在不同的云中，由不同的云服务商进行管理，当用户之间互相访问彼此存储在云中的加密数据时，有可能存在两者数据采用的域密钥不一致导致数据不能被访问的问题。

2) 不能解决用户下线之后的交友匹配。在以往模型中，要求用户实时在线参与匹配，一旦用户下线，则不能开展社交交友活动，同时存在交友用户因为设置交友条件的局限性，导致出现交友请求者过少匹配或者无法匹配的问题。

3) 云端服务提供商（CSP, cloud service provider）负责交友用户隐私文件的存储以及属性的匹配。而事实上，完全可信的CSP并不存在，一旦CSP有意窥视用户的隐私数据，只需要监视用户属性的匹配过程，就可以轻易获得用户隐私文件的解密密钥，进而直接解密用户存储在云端的数据文件，造成隐私泄露风险。

4) 在用户交友匹配过程中存在大量需要对加密数据进行转换（先解密再加密）的场景，而如果由不完全可信的云端服务器在云端进行解密又重新加密处理，极有可能产生用户数据泄露的风险。

基于以上问题，本文提出一种在跨云跨域环境

下，引入代理重加密以及密文与密钥分管技术来解决移动社交朋友发现过程中的安全与隐私保护问题。

本文的贡献如下。

1) 提出一种基于属性的跨域加密方案，实现了不同域中用户数据的共享，扩大了交友范围，更具有普适性。

2) 提出一种基于代理重加密技术的交友方案。利用代理用户适当拓宽或灵活修改交友条件，将交友用户访问结构对应的密文转化为代理用户访问结构的密文。当用户下线时，依然可以由代理协助交友，并保证代理用户不掌握用户的任何隐私信息。

3) 提出一种用户数据加密文件与密钥分管的交友隐私保护模型。利用对称加密和属性加密双重加密技术，有效避免用户数据在云端被窥视，更好地保护了用户的隐私。

## 3　预备知识

### 3.1　线性秘密共享

秘密共享[20,21]是将秘密以适当的方式拆分，拆分后的每一个份额由不同的参与者管理，单个参与者无法恢复秘密信息，只有若干个参与者共同协作才能恢复原秘密。当其中任何相应范围内参与者出现问题时，秘密仍可以完整恢复。

Benaloh 等[22]提出线性秘密共享方案（LSSS, linearity secret sharing scheme），该方案将秘密共享表示为树状结构，而门限值在树节点上提现，具体可以表示为以下 2 点。

1) 每个实体的共享是在 $Z_p$ 上构成的一个矢量。

2) 假设 $\boldsymbol{M}_{l\times n}$ 矩阵是线性秘密共享方案 $\prod$ 的线性秘密共享矩阵，$\rho(i)$ 表示第 $i$ 行的值，$\forall i=1,2,3,\cdots,l$，列矢量可以定义为 $\boldsymbol{v}=\{s,r_2,r_3,\cdots,r_n\}$，其中，$s\in Z_p$ 是需要共享的秘密，$r_2,r_3,\cdots,r_n\in Z_p$，$\boldsymbol{Mv}$ 则是通过 $\prod$ 产生关于秘密 $s$ 的 $l$ 个共享的矢量，共享的 $(\boldsymbol{Mv})_i$ 属于实体 $\rho(i)$。

### 3.2　数学基础

#### 3.2.1　群理论

**定义 1**　群。群 $G$ 可以表示为一个满足封闭性、结合性、存在唯一有单位元、逆元的二元运算的代数结构。

1) 封闭性：$\forall a,b\in G$，有 $(a*b)\in G$。

2) 结合性: $\forall a,b\in G$, 有 $(a*b)*c=a*(b*c)$。

3) 存在唯一单位元 $e$：$\forall a\in G$，使 $a*e=e*a=a$ 成立。

4) 存在逆元 $a^{-1}$：$\forall a\in G$，使得 $a*a^{-1}=a^{-1}*a=e$ 成立。

**定义 2**　阿贝尔群。阿贝尔群又称为交换群或加群，它除了满足一般群的性质，还满足交换律，即：$a*b=b*a$，$a,b\in G$。

**定义 3**　阶。如果群中的元素是有限的，那么该群称为有限群，反之，则称为无限群。有限群 $G$ 中元素的个数，称为群的阶。

**定义 4**　循环群。循环群是由群 $G$ 中的一个元素 $g$ 的幂次构成的群，元素 $g$ 称为群 $G$ 的生成元。

#### 3.2.2　双线性映射

设 $G_1$、$G_2$ 是生成阶为 $p$ 的循环群，$G_T$ 为具有相同阶的循环乘法群，则存在双线性映射 $\hat{e}:G_1\times G_2\to G_T$，满足以下 3 个性质。1) 双线性：对于 $P\in G_1$，　$Q\in G_2$，$a,b\in Z_p$，有 $\hat{e}(P^a,Q^b)=e(P,Q)^{ab}$。2) 非退化性：对于 $g\in G_1,h\in G_2$，$\hat{e}(g,h)\neq 1$。3) 可计算性：对于 $g\in G_1,h\in G_2$，$\hat{e}(g,h)$ 都是可以有效计算的。

#### 3.2.3　安全性假设

判定性 $q$-parallel BDHE（decisional $q$-parallel bilinear Diffie-Hellman exponent）假设[23]。

$$\vec{\boldsymbol{y}}=g,g^s,g^a,\cdots,g^{(a^q)},g^{(a^{q+2})},\cdots,g^{(a^{2q})},$$

$$\forall 1\leqslant j\leqslant q,g^{sb_j},g^{\frac{a}{b_j}},\cdots,g^{\frac{a^q}{b_j}},g^{\frac{a^{q+2}}{b_j}},\cdots,g^{\frac{a^{2q}}{b_j}},$$

$$\forall 1\leqslant j,k\leqslant q,k\neq j,g^{\frac{asb_k}{b_j}},\cdots,g^{\frac{a^qsb_k}{b_j}}$$

判定性 $q$-parallel BDHE 问题是将上述 $\vec{\boldsymbol{y}}$ 提供给攻击者 $A$，攻击者 $A$ 需要来判别出 $T=e(g,g)^{a^{q+1}s}$，还是随机值 $T\in G_T$，其中，$a,s,b_1,\cdots,b_q\in Z_P$，$g$ 为 $G$ 的生成元。则攻击者 $A$ 在 $q$-parallel BDHE 问题上取得的优势为

$$Adv_A^{q-\text{parallel BDHE}}=\left|\begin{matrix}\Pr[B(\vec{\boldsymbol{y}},T=e(g,g)^{a^{q+1}s})=0]\\-\Pr[B(\vec{\boldsymbol{y}},T\in G_T)=0]\end{matrix}\right|\geqslant\varepsilon$$

如果攻击者 $A$ 在多项式时间内不存在以一个不可忽略的优势 $\varepsilon$ 来区分 $T=e(g,g)^{a^{q+1}s}$ 或 $T\in G_T$，则称判定性 $q$-parallel BDHE 假设成立。

## 4　方案模型定义

### 4.1　系统模型

本文方案由以下部分组成：云端交友中心（FS，

friend server)、跨域多授权中心(TA, cross domain multi-authority)，交友发起用户（DO, data owner)、交友代理用户（DP, data proxy)、交友请求用户（DR, data requester)。

云端交友中心 FS：负责用户交友属性的匹配。

跨域多授权中心 TA：负责系统初始化以及该区域属性密钥生成、密钥分发等。

交友发起用户 DO：负责交友文件的加密，访问控制策略的设立。只有交友请求用户的属性满足 DO 的访问控制策略才能获得解密密钥，解密 DO 的隐私文件。本文假设交友发起用户为 Alice。

交友代理用户 DP：由 DO 进行授权，利用自身属性对 DO 的属性密钥进行重新加密，保证 DO 用户加密后数据文件的安全转换，同时可向交友请求用户推荐自身的已有的好友，使交友机制更高效。本文假设 Bob 为属主代理授权用户。

交友请求用户 DR：负责向交友发起用户 DO 或者交友代理用户 DP 发起交友请求，本文假设 Cindy 为交友请求用户。

同时，为明确各用户在方案中的角色，假设 TA 和交友信息属主 DO 是完全可信的，交友请求用户 DR 是完全不可信的，即交友请求用户可能串通、共谋，非法访问未经授权的数据。而 FS、DP 是诚实而好奇的[24]，即 FS、DP 会按照既定协议进行工作，但是不排除它们因为好奇，试图从获取的信息中采用更多的技术手段去窥视用户更多的隐私信息。

交友过程模型如图 1 所示，其中，图 1(a)表示 Alice 与 Cindy 共域的情况，没有代理用户参与匹配交友的应用场景。图 1(b)表示 Alice 与 Cindy 不属于同一个域，需要代理用户 Bob 参与匹配交友的应用场景。

### 4.2 方案设计

本文对所涉及的变量符号进行描述，如表 1 所示。

**表 1 符号描述**

| 符号 | 描述 |
|---|---|
| $\phi_i$、$\phi_j$ | 分别为第 $i$、$j$ 个域 |
| $GP$、$PK_{\phi_i}$、$MSK_{\phi_i}$ | 公共参数、系统公钥、系统主密钥 |
| $U_{\phi_i}$ | 用户属性集 $U_{\phi_i}$ |
| $S$ | 交友发起者属性集 |
| $S'$ | 交友请求者属性集 |
| $SK_S$ | 属性集 $S$ 对应的私钥 |
| $(\boldsymbol{M}, \rho)$ | 交友发起者的属性访问结构 |
| $(\boldsymbol{M}', \rho')$ | 交友代理者的属性访问结构 |
| $(\boldsymbol{M}^*, \rho^*)$ | 假设挑战的访问控制结构 |
| $m$ | 交友明文 |
| $\boldsymbol{M}$ | 访问控制结构矩阵 |
| $CT$ | 输出密钥密文 |
| $CT'$ | 重加密密钥密文 |
| $rk_{S\to(M',\rho')}$ | 代理重加密密钥 |

本文方案由 6 个算法构成，算法定义如下。

假设本文方案中的交友用户属于不同的 $N$ 个域，每个域用 $\phi_i$ 表示，$i \in \{1, \cdots, N\}$。

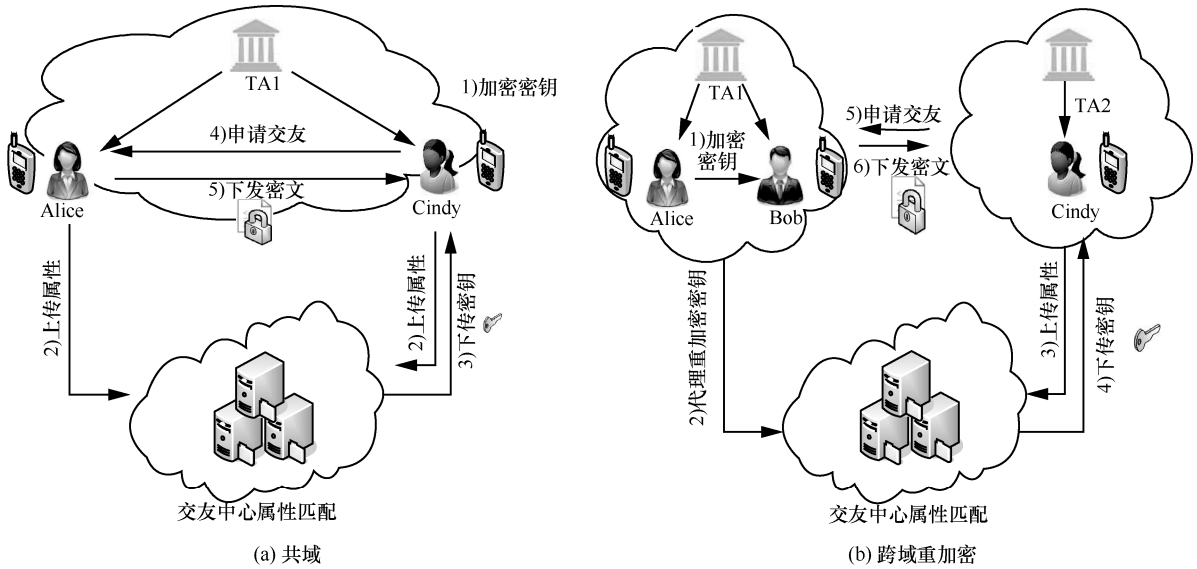


图 1 移动社交网络代理加密匹配过程模型

1) $Setup(1^k, U_{\phi_i}) \to (GP, MSK_{\phi_i}, PK_{\phi_i})$

系统密钥生成算法：$U_{\phi_i}$和$1^k$分别为输入的全体属性集与安全参数，$GP$ 为输出的公共参数，$PK_{\phi_i}$和$MSK_{\phi_i}$分别为系统公钥和系统主密钥。

2) $KeyGen(GP, MSK_{\phi_i}, S) \to SK_S$

密钥生成算法：输入公共参数$GP$、系统主密钥$MSK_{\phi_i}$和域$\phi_i$的属性集$S$，输出属性集$S$对应的私钥$SK_S$。

3) $Enc(m, (\boldsymbol{M}, \rho), PK_{\phi_i}, GP) \to CT$

加密算法：输入明文$m$、交友访问控制策略$(\boldsymbol{M}, \rho)$、系统公钥$PK_{\phi_i}$与公共参数$GP$，输出可被代理用户进行重加密的密钥密文$CT$。

4) $ReKeyGen(GP, S, SK_S, (\boldsymbol{M}', \rho')) \to rk_{S\to(\boldsymbol{M}',\rho')}$

密钥重加密算法：输入代理用户设置的访问控制策略$(\boldsymbol{M}', \rho')$、属性集$S$、私钥$SK_S$和公共参数$GP$，输出$rk_{S\to(\boldsymbol{M}',\rho')}$。

5) $ReEnc(rk_{S\to(\boldsymbol{M}',\rho')}, CT) \to CT'$

密文重加密算法：输入重加密密钥$rk_{S\to(\boldsymbol{M}',\rho')}$，密钥密文$CT$，输出经过重加密的密钥密文$CT'$。

6) $Dec_R(GP, S', SK_{S'}, CT') \to m$

文件解密算法：输入公共参数$GP$，属性集$S'$和私钥$SK_{S'}$，重加密密钥密文$CT'$，若$S'|=(\boldsymbol{M}', \rho')$，则输出明文$m$；否则输出$\perp$。

### 4.3 安全模型

本文安全模型通过定义一个攻击者$A$和挑战者$C$的游戏来保障移动社交网络中的交友过程中的安全与隐私。

1) 初始化阶段

$A$选择任意一个访问控制策略$(\boldsymbol{M}^*, \rho^*)$，并发送给$C$。

2) 系统建立阶段

$C$运行$Setup(1^k, U_{\phi_i})$算法，系统初始化时选择安全参数$K$和域$\phi_i$中的属性集$U_{\phi_i}$，生成相应$GP$与公钥$PK_{\phi_i}$，并将$GP$和$PK_{\phi_i}$发送给$A$。$C$保留系统主密钥$MSK_{\phi_i}$。

3) 查询阶段 1

$A$向$C$提出私钥查询请求$Q_{SK}(S)$。

$C$输入属性集$S$，$C$运行密钥生成算法；

$KeyGen(GP, MSK_{\phi_i}, S) \to SK_S$，然后将私钥$SK_S$发送给$A$。

$A$向$C$发出新属性集$(\boldsymbol{M}', \rho')$的访问查询$Q_{rk}(S, (\boldsymbol{M}', \rho'))$，$rk$为重加密密钥。

$C$执行$ReKeyGen(SK_S, S, (\boldsymbol{M}', \rho')) \to rk_{S\to(\boldsymbol{M}',\rho')}$算法并将重加密密钥发送给$A$。

4) 挑战阶段

$A$随机发送等长的消息$m_0$和$m_1$给$C$，$C$则从$b \in (0,1)$中随机选择 0 或 1，并利用$(\boldsymbol{M}^*, \rho^*)$对$m_b$加密得到$CT$，将$CT$返回给$A$。

5) 查询阶段 2

重复第一阶段的查询工作。

6) 猜测阶段

$A$输出一个比特$b'$来猜测在挑战阶段$C$选择的$b$是 0 或 1，若猜测正确，即$b'=b$，那么$A$赢得这个游戏。$A$的优势被定义为

$$\varepsilon = Adv(1^k, U_{\phi_i}) = |\Pr[b'=b] - \frac{1}{2}|$$

如果对于任意攻击者，赢得以上游戏的概率$Adv_A(k)$都是可以忽略的，则称该方案是可以达到挑战明文攻击（CPA）安全的。

## 5 具体方案

本文方案在各个阶段的工作，其安全性基于CP-ABE[16]方案和双系统加密（dual system encryption）的技术框架，细分如下。

初始化和私钥生成过程。DO 首先定义某一类属性特征的访问控制策略并上传到可信授权中心，每个可信授权中心管理各自域内的属性集，并产生与之对应的公、私钥。同时，在该过程中，DO 为保证自身的交友隐私，需要对数据进行加密。

代理过程。在交友过程中，交友信息属主DO可以向代理进行授权，由代理授权用户进行好友推荐。敏感数据文件的访问结构也可以由DP进行制定，这使DO和DP都能够灵活控制其他用户的访问权限。

加密过程。首先采用密钥加密数据明文，得到数据密文，再利用访问控制策略加密密钥，得到密钥密文。

解密过程。当DR的属性满足DO的属性访问控制策略，则可以首先对密钥密文进行解密，进而利用获得的密钥解密加密数据，最终得到交友数据文件明文，为进一步的社交交友活动提供便利。

具体实施过程如下。

### 5.1 系统初始化阶段

$TA$ 随机选择群 $G$ 和 $G^T$ 以及生成元 $g, g_1 \in G$，$a \in Z_p^*$，其中，双线性映射可表示为 $e: G \times G \to G_T$，生成系统公共参数 $GP$，散列函数 $H_1$和$H_2$。

$$\begin{aligned} &GP = (p, g, G, G_T, e, g_1, g^{\alpha}, H_1, H_2) \\ &H_1 : \{0,1\}^* \to G,\ H_2 : G^T \to Z_p^* \end{aligned} \tag{1}$$

假设交友用户分别属于不同的域 $D_{\phi}$，对于任意一个域 $D_{\phi_i}$ 的可信授权中心 $TA_{\phi_i}$ 均可运行 $setup(\ )$ 算法，随机选择 $\alpha_{\phi_i} \in Z_p^*$，为交友用户生成域公钥 $PK_{\phi_i}$，域主密钥 $MSK_{\phi_i}$。其中，公共参数 $GP$ 和域公钥对外公开，而域主密钥 $MSK_{\phi_i}$ 由工作在该域可信授权中心 $TA_{\phi_i}$ 保存。

$$PK_{\phi_i} = e(g,g)^{\alpha_{\phi_i}},\ MSK_{\phi_i} = g^{\alpha_{\phi_i}} \tag{2}$$

### 5.2 用户密钥生成阶段

Alice 首先启动运行在智能手机上的 APP 交友应用程序，其可选择在云中的某个可信授权中心 $TA_{\phi_i}$ 上进行注册。

1) $TA_{\phi_i}$ 随机选择 $ts \in Z_p^*$，运行 $KeyGen(\ )$ 算法，生成该用户唯一的私钥 $SK_S$

$$SK_S = (K = g^{a \cdot ts} g^{\alpha_{\phi_i}}, L = g^{ts}, \forall x \in S, K_x = H_1(x)^{ts}) \tag{3}$$

2) $TA_{\phi_i}$ 通过安全信道将 Alice 公私钥 $(PK_{\phi_i}, SK_S)$ 以及在 $TA_{\phi_i}$ 上的签名发送给 Alice。

### 5.3 文件加密阶段

为保证自身的交友隐私，Alice 需要将自己的交友文件进行加密，只有满足 Alice 交友访问控制策略的用户才能查看 Alice 的交友信息。Alice 对文件加密采用混合加密方式，步骤如下。

1) Alice 利用加密密钥对交友数据明文加密得到数据密文。

Alice 可以根据实际应用场景的不同建立多个交友文件，每个文件分别使用不同的密钥进行加密。本方案假设 Alice 随机选择一个交友文件，文件编号为 $FID_i, i \in \{1,2,3,\cdots,n\}$，然后从加密密钥集合中随机选择对称密钥 $KF$，加密 $FID_i$ 对应数据明文 $m$ 得到数据密文 $CF$。

2) 基于用户交友特征属性加密，加密密钥 $KF$ 得到密钥密文 $CT$。

Alice 运行加密算法 $Enc(\ )$，假设 Alice 定义的交友访问控制结构是 $(\boldsymbol{M}, \rho)$，那么交友请求用户的属性只有符合 $(\boldsymbol{M}, \rho)$ 设定的条件才能解密密钥密文 $CT$，得到密钥 $KF$，进而利用 $KF$ 解密 $CF$ 得到数据明文 $m$。

密钥密文可以表示为

$$CT = ((\boldsymbol{M}, \rho), A_1, A_2, A_3, (B_1, C_1), \cdots, (B_l, C_l)) \tag{4}$$

$$\begin{cases} A_1 = KF \cdot e(g,g)^{\alpha \cdot s}, A_2 = g^s, A_3 = g_1^s \\ B_1 = (g^{\alpha})^{\lambda_1} \cdot H_1(\rho(1))^{-r_1}, \cdots, B_l = (g^{\alpha})^{\lambda_l} \cdot H_1(\rho(l))^{-r_l} \\ C_1 = g^{r_1}, \cdots, C_l = g^{r_l} \end{cases} \tag{5}$$

其中，$\boldsymbol{M}$ 表示 $l \times n$ 的矩阵，$\rho$ 是关联 $M$ 行到属性的映射，$\{\rho(i) | 1 \leqslant i \leqslant l\}$ 表示访问结构 $(\boldsymbol{M}, \rho)$ 中使用的属性。$s$ 表示 Alice 需要共享的秘密 $s, y_2, \cdots, y_n \in Z_p^*$。对于 $i = 1$ 到 $l$，设置 $\lambda_i = v\boldsymbol{M}_i$，$\boldsymbol{M}_i$ 是对应到矩阵 $\boldsymbol{M}$ 第 $i$ 行的矢量，$v = (s, y_2, \cdots, y_n)$，$r_1, \cdots, r_l \in Z_p^*$。

3) DO 将 $(FID_i, CT)$ 以及签名发送给交友中心 $FS$，$FS$ 接收并验证签名，若正确，则保存 $(FID_i, CT)$。同时，因为本方案假设 $FS$ 是诚实而好奇的，所以密文文件 $CF$ 由 Alice 自己保存。

### 5.4 代理对密钥密文进行重加密阶段

在 4.3 节，Alice 将密钥密文 $CT$ 提交给 $FS$，由 FS 负责匹配交友请求者的属性，但是单独依靠这种机制有可能存在 Alice 设置交友条件局限导致最终不能成功交友的情况。因此本文方案借鉴真实生活中的媒介的思想，引入代理用户，通过代理用户适当拓宽或灵活修改交友条件的匹配方案（对密钥密文进行重加密），从而保证 Alice 的交友效率。另外，也可根据 Alice 的交友条件灵活向其推荐自身好友列表中的好友，减少匹配时间。

假设用户 Bob 是合法授权代理用户（媒介），如果 Alice 选择对 Bob 进行交友授权，那么 Bob 将获得 Alice 发送的密钥密文 $CT$，Bob 将利用自身的访问控制结构 $(\boldsymbol{M}', \rho')$ 对 $CT$ 进行重加密。

Bob 输入自身私钥 $SK = (K, L, K_x)$ 和属性集 $S$，并生成新的访问控制结构为 $(\boldsymbol{M}', \rho')$。

1) 若 Bob 和 Alice 工作在同一域 $D_{\phi_i}$ 中，Bob 随机选择 $\delta \in G_T$，计算

$$C'_{(\boldsymbol{M}', \rho')} = (A_1', A_2', B_{1,}' C_1', \cdots, B_{l,}', C_l') \tag{6}$$

$$\begin{cases} A_1' = \delta e(g,g)^{\alpha_{\phi_i} s'},\ A_2' = g^{s'} \\ B_1' = (g^a)^{\lambda_1'} H_1(\rho(1))^{-r_1'}, \cdots, B_l' = (g^a)^{\lambda_l'} H_1(\rho'(l'))^{-r_l'} \\ C_1' = g^{r_1'}, \cdots, C_{l'}' = g^{r_l'} \end{cases} \tag{7}$$

2) 若 Bob 和 Alice 工作在不同域中，例如，Bob 属于 $D_{\phi_i}$，Alice 属于 $D_{\phi_j}$，那么 Bob 将申请域 $D_{\phi_j}$ 的公钥 $e(g,g)^{\alpha_{\phi_j}}$，计算

$$C'_{(\boldsymbol{M}',\rho')} = (A_1', A_2', B_1', C_1', \cdots, B_l', C_l') \tag{8}$$

$$\begin{cases} A_1' = \delta e(g,g)^{\alpha_{\phi_j} \cdot s'},\ A_2' = g^{s'} \\ B_1' = (g^a)^{\lambda_1'} H_1(\rho(1))^{-r_1'}, \cdots, B_l' = (g^a)^{\lambda_l'} H_1(\rho'(l'))^{-r_l'} \\ C_1' = g^{r_1'}, \cdots, C_{l'}' = g^{r_l'} \end{cases} \tag{9}$$

注意，$C'_{(\boldsymbol{M}',\rho')}$ 为重加密密钥密文的重要参数。

3) Bob 选择 $\theta \in Z_p^*$，计算

$$rk_1 = K^{H_2(\delta)} g_1^{\theta} = (g^{a \cdot ts} g^a) g_1^{\theta}, rk_2 = g^{\theta}, rk_3 = L^{H_2(\delta)},$$
$$\forall x \in S, rk_4 = C'_{(\boldsymbol{M}',\rho')}, R_x = K_x^{H_2(\delta)} \tag{10}$$

Bob 输出重加密密钥

$$rk_{S\to(\boldsymbol{M}',\rho')} = (S, rk_1, rk_2, rk_3, rk_4, R_x) \tag{11}$$

并将重加密密钥 $rk_{S\to(\boldsymbol{M}',\rho')}$ 发送给 *FS*。

4) *FS* 收到 $rk_{S\to(\boldsymbol{M}',\rho')}$ 后，运行 *ReEnc*( ) 算法对 Alice 密钥密文 *CT* 进行重加密得到 *CT*′，并计算

$$A_4 = \frac{\dfrac{e(A_2, rk_1)}{e(A_3, rk_2)}}{\prod_{i\in I}(e(B_i, rk_3)e(C_i, R_{\rho(i)}))^{w_i}} \tag{12}$$

$I = \{i : \rho(i) \in S\}$，当 *S* 符合 $(\boldsymbol{M},\rho)$ 设定的条件时，存在一个常数集合 $\{\omega_i \in Z_p^*\}_{i\in I}$，使 $\sum_{i\in I}\omega_i\lambda_i = s$。其中，$\{\lambda_i\}$ 是对秘密 *s* 的共享。

输出

$$CT' = ((\boldsymbol{M}',\rho'), A_1, A_3, (B_1, C_1), \cdots, (B_l, C_l), A_4, rk_4) \tag{13}$$

### 5.5　文件解密阶段

假如 Cindy 向 *FS* 发起交友查询请求，Cindy 首先要上传自己的交友条件集合 *S*，若 *S* 满足 $(\boldsymbol{M},\rho)$，则 *FS* 可以提供好友列表，由 Cindy 进行选择；若 Cindy 自身属性集合 *S* 不满足 $(\boldsymbol{M},\rho)$，则 *FS* 提示无满足 Cindy 交友条件的交友伙伴，输出 ⊥。

假设 Cindy 选择 Alice 作为交友伙伴，则 *FS* 利用解密算法对 Alice 存储在 *FS* 上的密文 *CT* 进行解密求解密钥 *KF*。

1) 如果 *CT* 是未经过重加密的原始密文，求解过程为

$$\begin{aligned} &\frac{\dfrac{A_1}{e(A_2,K)}}{(\prod_{i\in I}(e(B_i,L)e(C_i,K_{\rho(i)}))^{w_i})} \\ &= \frac{KF \cdot e(g,g)^{\alpha_{\phi_i} s} e(g, g^{ats})^{\sum_{i\in I}\lambda_i w_i}}{e(g^s, g^{ats} g^{\alpha_{\phi_i}})} \\ &= \frac{KF \cdot e(g,g)^{\alpha s}}{e(g,g)^{\alpha s}} \\ &= KF \end{aligned} \tag{14}$$

2) 如果密文是经过代理重新加密的密钥密文 *CT*′，求解过程如下。

当交友请求用户的属性集 *S*′ 不符合 Alice 预设的条件 $(\boldsymbol{M},\rho)$，但却符合代理用户的条件 $(\boldsymbol{M}',\rho')$ 时，用户 *FS* 可计算 $\delta$，$\delta$ 为求解密钥密文 *KF* 的关键部分

$$\delta = \frac{\dfrac{A_1'}{e(A_2', K')}}{\prod_{i\in I}(e(B_i', L')e(C_i', K'_{\rho(i)}))^{w_i'}} \tag{15}$$

进一步计算得到密钥密文 $KF = \dfrac{A_1}{(A_4)^{\frac{1}{H_2(\delta)}}}$。

正确性验证

$$\begin{aligned} A_4 &= \frac{\dfrac{e(A_2, rk_1)}{e(A_3, rk_2)}}{\prod_{i\in I}(e(B_i, rk_3)e(C_i, R_{\rho(i)}))^{w_i}} \\ &= \frac{\dfrac{e(g^S, (g^{a\cdot t_S} g^{\alpha_{\phi_i}})^{H_2(\delta)})}{e(g_1^S, g^{at_S H_2(\delta)})}}{e(g, g^{at_S H_2(\delta)})^{\sum_{i\in I}\lambda_i w_i}} \\ &= e(g^S, g^{at_{\phi_i} H_2(\delta)}) \end{aligned} \tag{16}$$

$$\frac{A_1}{(A_4)^{\frac{1}{H_2(\delta)}}} = KF \frac{e(g,g)^{\alpha_{\phi_i} S}}{e(g^S, g^{\alpha_{\phi_i}})} = KF$$

3) *FS* 将 Alice 的交友敏感数据文件的解密密钥 *KF* 和对应文件 $FID_i$ 发送给 Cindy，Cindy 可以向 Alice 请求编号为 $FID_i$ 的交友敏感文件 *CF*，并最终对 *CF* 进行解密获得数据文件明文 *m*，从而进

行更深入的交流，例如，了解交友用户发起者音频、视频、联系方式、兴趣爱好等。

## 6 安全性分析

**定理 1** 假设判定性 $q$-parallel BDHE 假设在 $(G,G_T)$ 上成立，那么多项式概率时间内不存在攻击者 $A$ 能选择 $(\boldsymbol{M}^*,\rho^*)$ 访问策略来攻破本文方案，即本文方案在随机预言模型下可证 CPA 安全。

**证明** 假设存在攻击者 $A$ 能在 CPA 游戏中以 $\varepsilon=Adv_A$ 的优势证明本文方案，则本文方案将证明存在不可忽略的概率 $\frac{\varepsilon}{2}$ 解决判定性 q-parallel BDHE 问题。

1) 初始化阶段

$A$ 将需要挑战的访问结构 $(\boldsymbol{M}^*,\rho^*)$ 发送给 $C$，$\boldsymbol{M}^*$ 是一个 $\ell^*\times n^*$ 大小的矩阵（$\ell^*,n^*\leqslant q$）。

2) 系统建立阶段

假设 $(\boldsymbol{M}^*,\rho^*)$ 中的属性属于域 $\phi_i$，$C$ 选择 $\alpha_{\phi_i},\gamma\in Z_p^*$，设置 $g_1=g^{\gamma}$，$e(g,g)^{\alpha_{\phi_i}}=e(g^{\alpha},g^{\alpha^q})\cdot e(g,g^{\alpha_{\phi_i}})$。

同时选择散列函数 $H_1$、$H_2$，并发送公共参数 $GP$ 及公钥 $PK$ 给 $A$。

3) 查询阶段 1

$A$ 向 $C$ 提出询问，$C$ 进行应答。

**情况 1** 对私钥提取询问 $O_{SK}(S)$

$C$ 选择随机值 $r_S\in Z_p^*$，$w=(w_1,w_2,\cdots,w_n)\in Z_p^*$，$w_1=-1$，$\forall i,\rho^*(i)\in S$，$w\boldsymbol{M}_i^*=0$，将元组 $(S,SK_S)$ 添加到 $SK^{\text{List}}$ 中，同时返回 $SK_S$ 给 $A$，假如 $S\models(\boldsymbol{M}^*,\rho^*)$，则 $C$ 从集合 {0,1} 中随机选择一个输出。

**情况 2** 对于重加密密钥提取询问 $O_{rk}(S,(\boldsymbol{M}',\rho'))$

用一个属性集 $S$ 和一个访问结构 $(\boldsymbol{M}',\rho')$ 来询问 $O_{rk}$。根据安全游戏，若 $S$ 不满足 $(\boldsymbol{M}^*,\rho^*)$，那 $C$ 就先执行 $O_{SK}(S)$，获得相应的私钥 $(K,L,K_x)$，然后选择 $\theta,\sigma\in_R Z_p^*,\overline{K}\in_R G$，计算重加密密钥 $rk_1=\overline{K}g_1^{\theta}$，$rk_2=g^{\theta},rk_4=g^{\sigma},R_x=\delta_{2,x}^{\sigma}$，并将 $rk_{S\to(\boldsymbol{M}',\rho')}=(S,rk_1,rk_2,rk_3,rk_4,R_x)$ 发送给 $A$。否则 $C$ 从集合 {0,1} 中任意选择 0 或 1，发送给攻击者 $A$。

4) 挑战阶段

$A$ 选择等长明文消息 $m_0$ 和 $m_1$ 发送给 $C$。$C$ 随机选择比特 $b\in\{0,1\}$，并利用访问策略 $(\boldsymbol{M}^*,\rho^*)$ 加密接收到的明文消息 $m_b$，输出有效密文 $CT^*=((\boldsymbol{M}^*,\rho^*),A^*,A_2^*,A_3^*,(B_1^*,C_1^*),\cdots,(B_{\ell^*}^*,C_{\ell^*}^*))$ 给 $A$。若 $T=e(g,g)^{a^{q+1}\cdot s}$，那么 $CT^*$ 是一个有效密文。

5) 查询阶段 2

重复查询第 1 阶段的操作。

6) 猜测阶段

$A$ 从集合 $b'\in\{0,1\}$ 中随机选择 0 或者 1，假如 $A$ 猜测正确，即 $b'=b$，则 $C$ 可在游戏挑战中得到（$T=e(g,g)^{a^{q+1}\cdot s}$）；否则 $C$ 得到（$T\in G_T$）。

$C$ 成功的概率为当输出为 0 时，即 $T\in G_T$，即 $A$ 得不到关于 $m_b$ 的任何信息，不能恢复明文。因此这时猜测正确的概率为 $\Pr[b'=b\mid(y,T=R)=0]=\frac{1}{2}$。当输出为 1 时，即 $T=e(g,g)^{a^{q+1}s}$，也就是 $A$ 得到的是一个关于 $m_b$ 的有效密文。通过定理 1，$A$ 有不可忽视的优势 $\varepsilon$ 猜测到正确结果，即 $\Pr[b'=b\mid(y,T=e(g,g)^{a^{q+1}s})=0]=\frac{1}{2}+\varepsilon$

因此，本文方案判定性 $q$-parallel BDHE 游戏中正确猜测 $b'=b$ 的优势为

$$\begin{aligned}Adv_c&=\Pr[b'=b]-\frac{1}{2}\\&=\frac{1}{2}\Pr[b'=b\mid b=0]+\frac{1}{2}\Pr[b'=b\mid b=1]-\frac{1}{2}\\&=\frac{1}{2}\cdot\frac{1}{2}+\frac{1}{2}\cdot(\frac{1}{2}+\varepsilon)-\frac{1}{2}\\&=\frac{\varepsilon}{2}\end{aligned}$$

综上可证，如果攻击者 $A$ 能攻破本文方案的概率为 $\varepsilon$，则解决判定性 $q$-parallel BDHE 问题的概率为 $\frac{\varepsilon}{2}$。而这与目前已知 $q$-parallel BDHE 问题难解是相矛盾的，因此，在多项式时间内不存在一种算法能够以不可忽略的优势 $\varepsilon$ 解决本问题，本文方案可以达到挑战明文攻击（CPA）安全，证毕。

**定理 2** 假设判定性 $q$-parallel BDHE 假设在 $(G,G_T)$ 上成立，那么本文方案在随机预言模型下可抵抗同谋攻击。

**证明** 在本文方案中，因为攻击者 $A$ 可以挑战 $C$ 获得重加密密钥 $rk_{S\to(\boldsymbol{M}',\rho')}$，并且利用 $rk_{S\to(\boldsymbol{M}',\rho')}$ 加密密文 $CT^*=((\boldsymbol{M}^*,\rho^*),A^*,A_2^*,A_3^*,(B_1^*,C_1^*),\cdots,(B_{\ell^*}^*,C_{\ell^*}^*))$ 得到重新加密的密钥密文 $CT'$，如果方案不能抵抗同谋攻击，那么攻击者可利用同谋所提供

的私钥询问 $O_{SK}(S)$ 而获得解密密钥，进而解密重加密密文 $CT'$，得到对 $b$ 的猜测，这显然与已经获得证明的定理 1 相矛盾，故本方案可抵抗同谋攻击。

## 7　实验分析

### 7.1　计算复杂度分析

本节将详细分析方案各阶段的计算开销和通信开销，为简化描述，本文用 $E(G)$ 和 $E(G_T)$ 分别表示 $G$ 和 $G_T$ 的幂运算，$B$ 表示双线性对映射 $e:G\times G\to G_T$，$\gamma$ 表示访问控制策略树的叶子节点，$|A|$ 表示用户的属性集合。$L_G$、$L_{G_T}$、$L_{Z_P}$ 分别表示 $G$、$G_T$、$Z_P$ 的长度。鉴于目前的研究成果中 HMCP 方案与其他方案相比计算开销和通信开销更具优势，因此，本文方案在计算开销和通信开销上与 HMCP[19]交友方案进行了比较，如表 2 所示。

**表 2　　计算开销分析**

| 阶段 | 本文方案计算开销 | HMCP 方案计算开销 |
|---|---|---|
| 系统初始化阶段 | $E(G)+E(G_T)+1B$ | $5E(G)+E(G_T)+B$ |
| 密钥生成阶段 | $(2+\|A\|)E(G)$ | $(k+\|A\|)E(G)$ |
| 加密阶段 | $\|A\|E(G)+1B$ | $(2+3\|A\|)E(G)+1E(G_T)$ |
| 解密阶段 | $\|A\|B+(\gamma)E(G_T)$ | $(\|A\|)B+(\gamma)E(G_T)$ |

1) 系统初始化阶段

本方案生成域主密钥 $MSK_{\phi_i}=g^{\alpha_{\phi_i}}$，域公钥 $PK_{\phi_i}=e(g,g)^{\alpha_{\phi_i}}$ 的计算开销恒定为 $E(G)+E(G_T)+B$，比 HMCP 方案的计算开销 $5E(G)+E(G_T)+B$ 低。

2) 密钥生成阶段

本文方案采用属于不同域的可信中心生成用户私钥，用户私钥的计算开销为 $(2+|A|)E(G)$，其中，$K=g^{ats}g^{\alpha_{\phi_i}}, L=g^{ts}$ 需要 $2E(G)$ 计算，而 $K_x=H_1(x)^{ts}, \forall x\in S$ 计算开销与属性集合 $|A|$ 紧密相关，因此计算开销为 $|A|E(G)$。

而 HMCP 方案因为采用了 $k$ 个属性管理中心分层计算私钥部件，然后再由 $k$ 个私钥部件合并为加密密钥，因此，私钥的生成时间比本文方案高。

3) 加密阶段

本文方案为了保证加密过程的安全，采用了混合加密方式，用户的计算开销为 $|A|E(G)+B$，计算开销比 HMCP 方案稍高，但是值得注意的是，密钥重加密方案主要通过代理执行，因此，不影响交友发起者 Alice 的计算效率。

4) 解密阶段

在本阶段，用户的计算开销为 $|A|B+(\gamma)\ E(G_T)$，可以发现本文方案解密时间与访问策略 $\gamma$、用户的属性集合 $|A|$ 紧密相关，且计算开销与 HMCP 方案持平，说明本方案与 HMCP 方案一样，具有较快的解密速度。

同样地，在表 3 中，本文方案进行了通信和存储开销分析。本文方案系统公钥 $(PK)$ 长度为 $L_{Z_P}+4L_G+L_{G_T}$，用户私钥长度 $(SK)$ 为 $(2+3|A|)L(G)$，与 HMCP 方案的公钥长度 $4L_G+L_{G_T}$ 和私钥长度 $(1+2|A|)L(G)$ 相比，本文方案的密钥强度可以保证有更强的抗攻击能力。本文方案加密后的密文长度为 $|A|L_G+L_{G_T}$，比 HMCP 方案 $5|\gamma|L_G+L_{G_T}$ 更短，因此，当用户上传与下载密文文件时，会有更快的速度和更好的用户体验。

**表 3　　通信开销分析**

| 比较对象 | 本文方案通信开销 | HMCP 方案通信开销 |
|---|---|---|
| 系统公钥 $(PK)$ | $L_{Z_P}+4L_G+L_{G_T}$ | $4L_G+L_{G_T}$ |
| 系统主密钥 $(MK)$ | $L_G$ | $2L_{Z_P}+L_G$ |
| 用户私钥 $(SK)$ | $(2+3\|A\|)L(G)$ | $(1+3\|A\|)L(G)$ |
| 加密密文 $(CT)$ | $\|A\|L_G+L_{G_T}$ | $5\|\gamma\|L_G+L_{G_T}$ |

### 7.2　模拟实验

本文测试环境中利用 HUAWEI 手机 NOVA 版进行群组测试，编程环境使用 Eclipse，利用 Java 作为编程语言进行代码开发。硬件条件为：CPU 骁龙 8X74AC 801 处理器主频 2.5 GHz，使用 LPDDR3 933 MHz 3GB 高速内存，支持蓝牙 4.0 和 Wi-Fi 双频。用户特征属性（兴趣爱好）利用爬虫代码从社交网站进行抓取并进行处理。开发库为（java.math.BigInteger/java.util.Arrays/java.util.Random）。

本文假设用户 Alice 在不同的生活场景中会有不同的交友需求，例如，对音乐、电影、健身的兴趣等。根据微博的调查显示，一般情况下每 100 个常用的属性就能够细粒度地描述用户的兴趣特征，而存储用户交友信息的文件一般在 50 MB 以内。因此，本文假设用户的明文文件固定为 50 MB，特征属性从 0~100 依次递增，系统在初始化时间、密钥生成时间、属性加密和解密时间上与 Chase[25]、Li[26]、Taeho[27]方案以及多可信中心 HMCP 方案比较的差异性。

图 2(a)说明在相同访问策略下，本文方案随着属性数目的递增，系统初始化时间比较稳定, 并且与 HMCP 方案基本持平，但是却比 Chase、Li、Taeho 方案小很多，这是因为在 Chase、Li 方案中使用了大量复杂度较高的双线性计算，而本文方案利用不同域的可信中心分担了计算任务，减少了可信中心的双线性计算的次数。因此，在计算开销上，本文方案更高效。

图 2(b)反映了随着属性数目的递增，每个可信中心产生子密钥时间的变化情况。与其他方案相比，本文方案的在计算时间上增长率很小，属性数目从 20 增加到 100，密钥生成时间基本不变。

图 2(c)反映随着属性数目的递增，文件加密时间的变化情况。在本文方案中，对拥有 100 个特征属性的文件加密仅需要 1.8 s 左右，比 Chase、Li 方案要小很多，这是因为 Chase、Li 方案中为了设计用户签名需要增加相当大的时间开销。

图 2(d)说明随着属性数目的递增，本文方案解密时间的变化情况。本文方案和 HMCP 方案均需要遍历访问控制结构，因此，在属性数目较小的情况下（0~40），Chase、Li、Taeho 方案比本文方案解密时间快。但是随着属性的增加，本文方案在解密速度上体现了很大的优势，这是因为本文方案用户在解密数据时只需要关联解密用户自身的访问控制结构，不需要考虑匹配加密用户的所有属性，因此在计算时间上开销较小。同时，因为上文中 Chase、Li、Taeho 方案的计算效率与本文方案以及 HMCP 方案差距较大，为了进一步区分本方案与 HMCP 方案的差异性，本文扩展了属性数目，固定为 50 个，访问控制策略为 3 层，数据文件大小从 10 MB~100 MB 逐渐递增进行实验，并将本文方案与 HMCP 方案做了补充对比。

图 3(a)说明在属性数目和访问控制策略层数相同的情况下，文件大小递增时，对本文方案系统初始化时间影响不大，与 HMCP 方案持平。

图 3(b)的实验结果中验证了密钥生成时间不受文件大小变化的影响。本文密钥生成时间稳定，不

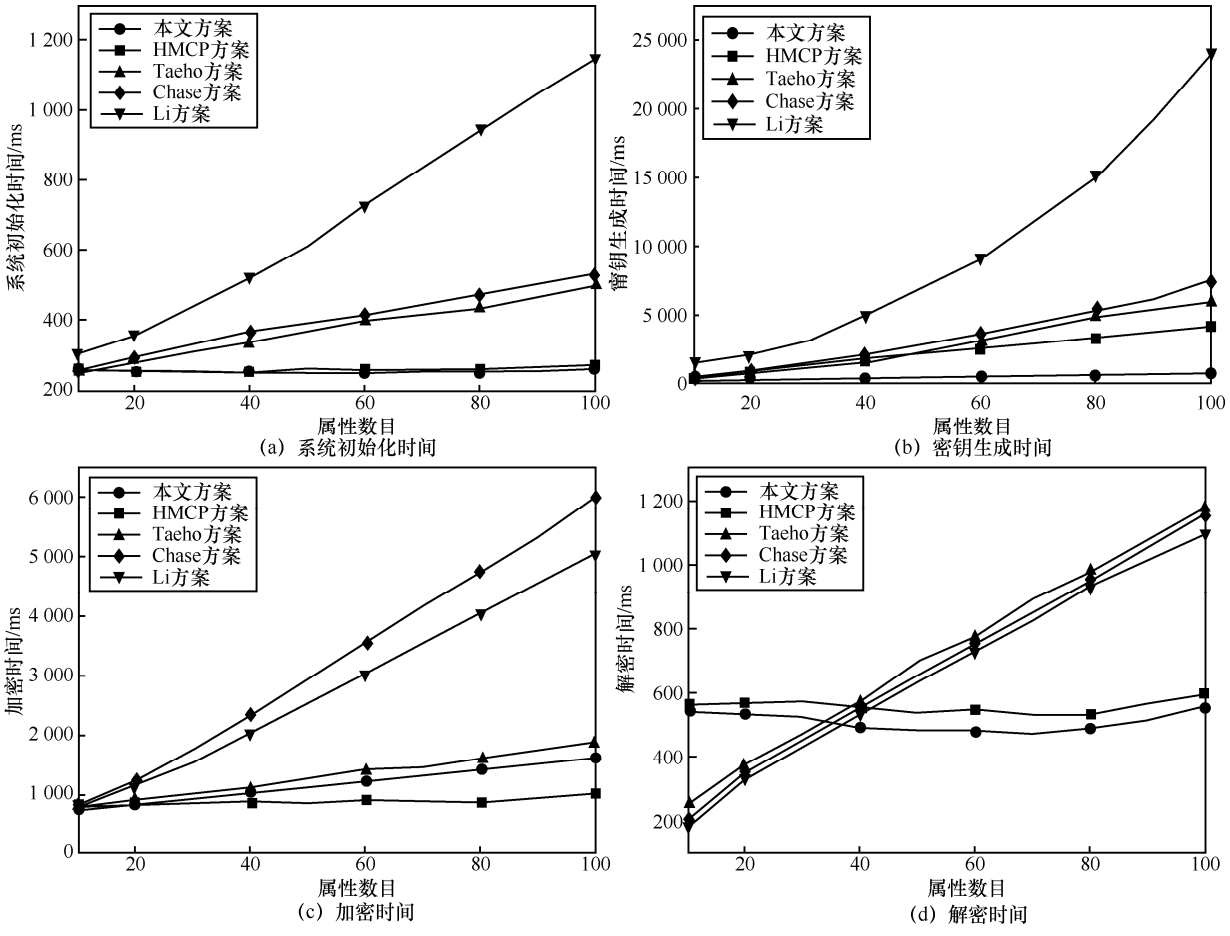


图 2　属性数目对性能的影响

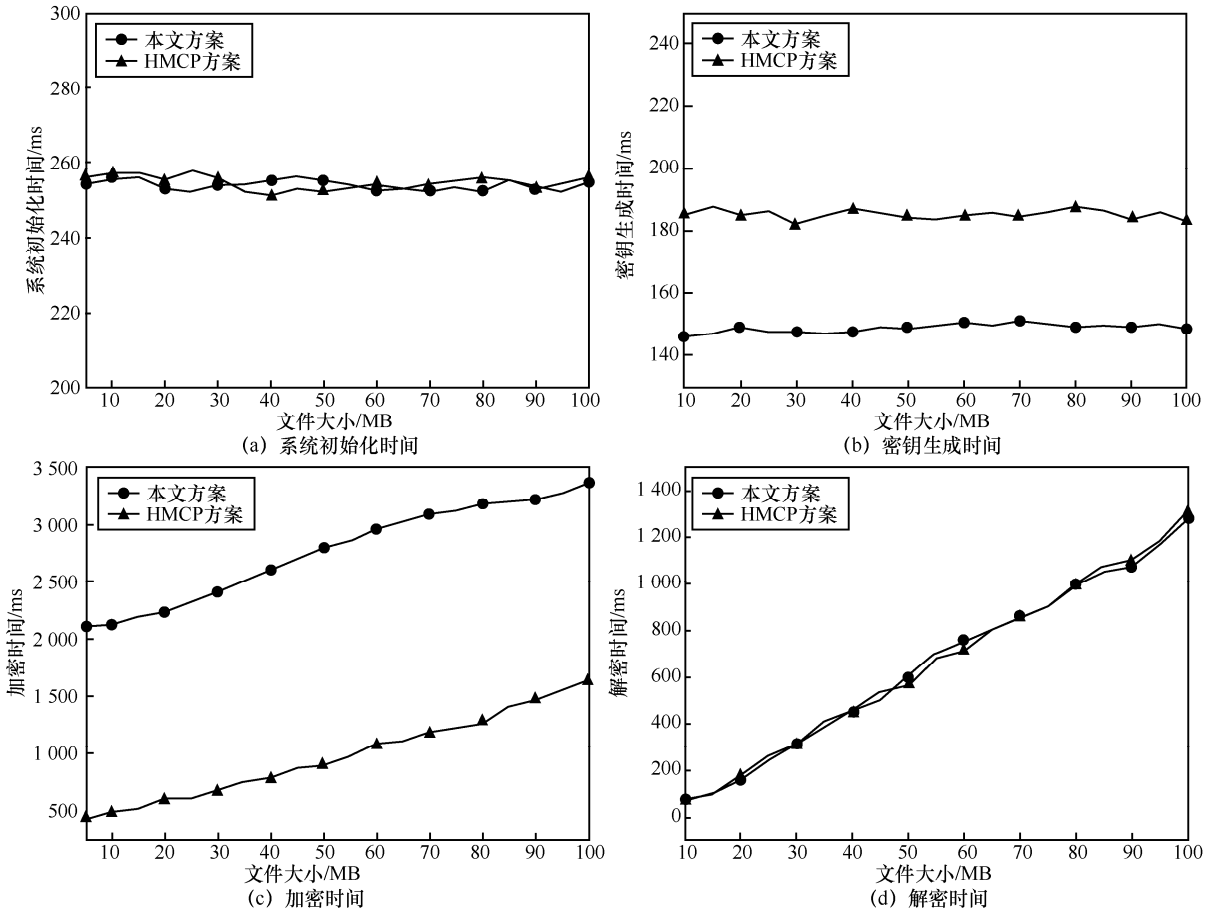


图 3　文件大小对性能的影响

会因为数据文件大小的递增而线性增长，实验时间均在 140 ms 左右轻微浮动，没有出现大的跳跃。同样地，在 HMCP 方案中，密钥生成时间也与数据大小的递增没有关系，也均在 180 ms 波动。进一步验证了表 2 中理论分析的正确性。

图 3(c)说明 HMCP 方案在针对大文件的加密时，加密时间比本文方案低，这是因为 HMCP 方案将用户的特征属性集合划分成 $W$ 个子属性，对应着 $k$ 个下级属性管理中心，多个属性管理中心并行工作，因此，加密时间较快。但是，HMCP 方案没有考虑到用户设置交友条件的局限性，而本文方案通过代理重加密扩充了交友条件，更具有普适性，同时，HMCP 不适用跨域的应用场景，灵活性没有本文方案高。

图 3(d)说明解密时间的变化，本文方案与 HMCP 方案一样，随着文件大小的增加而线性增长，变化趋势相同，对于大文件的处理，依然有很快的速度，例如，解密 100 MB 的文件在 1.4 s 之内，不会影响到用户的实际应用体验。

最后，本文方案与其他方案进行了适应性比较，如表 4 所示，通过比较发现本文方案在循环群计算上只应用了一次 $p$ 运算，在访问控制结构上本方案适应 AND-gates +/− on multi-valued attributes、通配符以及隐藏访问控制结构，体现了比其他方案更好的适应性。

## 8　结束语

在移动社交网络中，最大化增强彼此之间的联系和交流，同时又保护用户的个人隐私问题是当前隐私保护方向的一个研究热点。本文在基于密码学的研究基础上，提出了跨域代理重加密隐私保护协议。在交友过程中，通过跨域思想和引入代理用户既分担了用户的计算开销，又解决了交友应用场景局限、交友过少匹配的问题。用户密钥由多个授权中心分别计算，既降低了性能瓶颈，提高了移动社交网络中的交友效率，又能提高安全性，因此比以往方案更具有普适性和灵活性。本文的下一步工作将会考虑结合用户兴趣权重与安全内积算法来更

表 4　　与其他协议适应性对比

| 方案 | 循环群 | 安全模型 | 安全假设 | 访问控制策略适应性 | 通配符 | 是否可隐藏访问控制策略 |
|---|---|---|---|---|---|---|
| 文献[28] | $p$ | selective | DBDH | AND-gates on +/− | √ | × |
| 文献[29] | $p$ | selective | DBDH | AND-gates on multi-valued attributes | × | × |
| 文献[30] | $p$ | selective | $n$-DBDH | AND-gates on multi-valued attributes | √ | × |
| 文献[31] | $p$ | selective | Amse-DDH | Threshold Gates | × | × |
| 文献[32] | $pqr$ | fully | Subgroup Assumption | AND-gates on multi-valued attributes | √ | √ |
| 文献[33] | $pq$ | fully | DBDH | AND-gates on multi-valued attributes | × | √ |
| 文献[34] | $P$ | selective | $n$-DBDH | Threshold Gates | × | × |
| 文献[35] | $pqr$ | fully | Subgroup Assumption | Threshold Gates | × | × |
| 本文方案 | $p$ | selective | DBDH | AND-gates on multi-valued | × | √ |

精确的计算用户之间的相似度，同时考虑利用大素数混淆矩阵来代理传统的加密算法，从而获得更快的加解密速度，提升移动智能终端的用户体验。

## 参考文献：


[1] 付艳艳, 张敏, 冯登国, 等. 基于节点分割的社交网络属性隐私保护[J]. 软件学报, 2014, 25(4): 768-780.
FU Y Y, ZHANG M, FENG D G, et al. Attribute privacy preservation in social networks based on node anatoncy[J]. Journal of Software, 2014, 25(4): 768-780.

[2] DONG W, DAVE V, QIU L. Secure friend discovery in mobile social networks[J]. IEEE Global Communications Conference (INFOCOM), 2015,34(17) : 1647-1655.

[3] LI M, GAO Z, DU S, et al. PriMatch: fairness-aware secure friend discovery protocol in mobile social network[C]//IEEE Global Communications Conference (GLOBECOM). 2013:738-743.

[4] 程瑶, 应凌云, 焦四辈. 移动社交应用的用户隐私泄露问题研究[J]. 计算机学报, 2014, 37(1):87-100.
CHENG Y, YING L Y, JIAO S B. Research an user privacy leakage in mobile social messaging applications[J].Chinese Journal of Computers, 2014, 37(1):87-100.

[5] SARPONG S, XU C. A secure and efficient privacy-preserving attribute matchmaking protocol in proximity-based mobile social networks[J]. Advanced Data Mining and Applications, 2014,8933: 305-318.

[6] LI M, CAO N, YU S, et al. Findu: privacy-preserving personal profile matching in mobile social networks[C]//IEEE International Conference on Computer Communications (INFOCOM). 2011,2(3): 2435-2443.

[7] YAN Z, DING W, NIEMI V. Two schemes of privacy-preserving trust evaluation[J]. Future Generation Computer Systems, 2016, 62(C): 175-189.

[8] KIRAZ M S, GENC Z A, KARDAS S. Security and efficiency analysis of the hamming distance computation protocol based on oblivious transfer[J]. Security & Communication Networks, 2015, 8(18): 4123-4135.

[9] ZHANG R, ZHANG J, ZHANG Y, et al. Privacy-preserving profile matching for proximity-based mobile social networking[J]. IEEE Journal on Selected Areas in Communications, 2013, 31(9):656-668.

[10] NIU B, ZHU X, LIU J. Weight-aware private matching scheme for proximity-based mobile social networks[C]//IEEE Global Communications Conf (GLOBECOM). 2013: 3170-3175.

[11] ZHU X, CHEN Z, CHI H. Two-party and multi-party private matching for proximity-based mobile social networks[C]//IEEE International Conference on Communications (ICC). 2014: 926-931.

[12] HAN J, SUSILO W, MU Y. Privacy-preserving decentralized key-policy attribute-based encryption[J]. IEEE Transactions on Parallel & Distributed Systems, 2012, 23(11):2150-2162.

[13] OSTROVSKY R, SAHAI A, WATERS B. Attribute-based encryption with non-monotonic access structures[C]//CCS 07 ACM Conference on Computer and Communications Security. 2007: 195-203.

[14] LEWKO A, OKAMOTO T, SAHAI A. Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption[J]. Springer Berlin Heidelberg, 2010, 6110:62-91.

[15] TAN S F, SAMSUDIN A. Key policy-attribute based fully homomorphic encryption (KP-ABFHE) scheme for securing cloud application in multi-users environment[J]. Springer Singapore, 2017.

[16] WATERS B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization[J]. Lecture Notes in Computer Science, 2011, 2008: 321-334.

[17] RAO Y S. A secure and efficient ciphertext-policy attribute-based signcryption for personal health records sharing in cloud computing[J]. Future Generation Computer Systems, 2017, 67:133-151.

[18] ZHOU Z, HUANG D, WANG Z. Efficient privacy-preserving ciphertext-policy attribute based-encryption and broadcast encryption[J]. IEEE Transactions on Computers, 2014, 64(1): 126-138.

[19] LUO E, LIU Q, WANG G. Hierachical multi-authority and attribute-based encryption friend discovery scheme in mobile social networks[J]. IEEE Communications Letters, 2016, 20(9):1772-1775.

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

[21] BLAKLEY G R. Safeguarding cryptographic keys[J]. IEEE Computer Society Digital Library, 1979: 313-317.

[22] BENALOH J C, YUNG M. Distributing the power of a government to enhance the privacy of voters[J]. Principles of Distributed Computing Symposium, 1986:52-62.

[23] WATERS B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization[J]. Lectures Notes in Computer Science, 2011, 2008: 321-334.

[24] CURTMOLA R, GARAY J, KAMARA S, et al. Searchable symmetric encryption: improved definitions and efficient constructions[J]. Journal of Computer Security, 2011, 19(5):895-934.

[25] CHASE M, CHOW S S. Improving privacy and security in multi-authority attribute-based encryption[C]//ACM Conference on Computer and Communications Security. 2009: 121-130.

[26] LI J, HUANG Q, CHEN X. Multi-authority ciphertext-policy attribute-based encryption with accountability[J]. ACM Symposium on Information, 2011:386-390.

[27] JUNG T, LI X, WAN Z. Control cloud data access privilege and anonymity with fully anonymous attribute-based encryption[J]. IEEE Transactions on Information Forensics & Security, 2014, 10(1): 190-199.

[28] CHEUNG L, NEWPORT C. Provably secure ciphertext policy ABE[C]//ACM Conference on Computer and Communications Security. 2007:456-465.

[29] EMURA K, MIYAJI A, OMOTE K. A ciphertext-policy attribute-based encryption scheme with constant ciphertext length[C]// International Conference on Information Security Practice and Experience. 2009: 13-23.

[30] ZHOU Z, HUANG D. On efficient ciphertext-policy attribute based encryption and broadcast encryption: extended abstract[J]. IEEE Transactions on Computers, 2010(1).

[31] HERRANZ J, LAGUILLAUMIE F, RÀFols C. Constant size ciphertexts in threshold attribute-based encryption[C]//International Conference on Practice and Theory in Public Key Cryptography. 2010: 19-34.

[32] LAI J, DENG R H, LI Y. Fully secure cipertext-policy hiding CP-ABE[J]. International Conference on Information Security Practice and Experience, 2011, 6672(2): 24-39.

[33] LI X, GU D, REN Y. Efficient ciphertext-policy attribute based encryption with hidden policy[C]// International Conference on Internet & Distributed Computing Systems. 2012: 146-159.

[34] GE A, ZHANG R, CHEN C. Threshold ciphertext policy attribute- based encryption with constant size ciphertexts[C]//Australasian Conference on Information Security and Privacy, 2012: 336-349.

[35] CHEN C, CHEN J, LIM H W. Fully secure attribute-based systems with short ciphertexts/signatures and threshold access structures[M]. Springer Berlin Heidelbag. 2013: 50-67.

**作者简介：**

**罗恩韬**（1978-），男，湖南永州人，博士，湖南科技学院副教授，主要研究方向为可信计算、云安全、隐私保护、大数据等。

**王国军**（1970-），男，湖南长沙人，中南大学教授、博士生导师，主要研究方向为信息安全、可信计算、净室计算、信任推荐等。

**陈淑红**（1975-），女，湖南祁东人，博士，广州大学副教授，主要研究方向为可信计算、社交网络分析、社区发现等。

**PINIAL Khan-butt**（1979-），男，巴基斯坦卡拉奇人，巴基斯坦信德农业大学助理教授，主要研究方向为绿色手机计算、节能计算等。