# 移动社交网络中基于属性加密的隐私保护方案

牛淑芬 戈 鹏* 宋 蜜 宿 云
(西北师范大学计算机科学与工程学院 兰州 730070)

**摘 要**：为了保护用户在移动社交网络中的个人信息和交友偏好等隐私，该文提出支持外包解密的基于密文策略的属性基加密(CP-ABE)方案。在该方案中，将用户的交友偏好和自我描述分别生成属性列表，通过将交友偏好转换为密文控制策略，自我描述转化为属性密钥来隐藏属性，从而实现隐私保护。该方案提出了先匹配后解密的算法机制：社交平台对用户信息进行匹配验证，当满足相应的匹配条件时，该算法将计算量较大的双线性对运算外包给交友中心，之后用户再对密文解密。通过快速排除不匹配用户，避免了无效解密。外包解密在保护信息的同时，减少了移动设备的计算负担和通信开销。安全性分析表明，该方案是安全有效的，此外性能评估显示所提方案在计算和通信开销方面是高效且实用的。

**关键词**：社交网络；数据共享；隐私保护；外包解密；属性基加密
**中图分类号**：TN918 **文献标识码**：A **文章编号**：1009-5896(2023)03-0847-09
**DOI**: 10.11999/JEIT221174

# A Privacy Protection Scheme Based on Attribute Encryption in Mobile Social Networks

NIU Shufen GE Peng SONG Mi SU Yun
(*College of Computer Science and Engineering, Northwest Normal University, Lanzhou* 730070, *China*)

**Abstract**: In order to protect the privacy of users′ personal information and friend preferences in social networks, a Ciphertext-Policy Attribute Based Encryption (CP-ABE) scheme that supports outsourced decryption is proposed. In this scheme, attribute lists are generated for the users′ dating preference and self-description respectively, and attributes are hidden by converting the dating preference into ciphertext control policy and self-description into attribute key, thus realizing privacy protection. The proposed algorithm mechanism matches users′ information and then decrypts it. Users′ information is matched and verified by social platform. When the corresponding matching conditions are met, the algorithm outsources the computationally expensive bilinear pairing operation to the dating center. The user then decrypts the ciphertext. Invalid decryption is avoided by quickly eliminating mismatched users. Outsourced decryption reduces the computational burden and communication overhead of mobile devices while protecting information. Security analysis shows that the scheme is safe and effective, furthermore, performance evaluation shows that the proposed scheme is efficient and practical in terms of computational and communication overhead.

**Key words**: Social network; Data sharing; Privacy protection; Outsourced decryption; Attribute Based Encryption (ABE)

收稿日期：2022-09-08；改回日期：2023-01-26；网络出版：2023-02-03
*通信作者： 戈鹏 1851557497@qq.com
基金项目：国家自然科学基金(62241207, 62262060, 61562077)，甘肃省科技计划(22JR5RA158)，甘肃省教育厅产业支撑计划(2022CYZC-17)
Foundation Items: The National Natural Science Foundation of China (62241207, 62262060, 61562077), The Science and Technology Program of Gansu (22JR5RA158), The Industrial Support Plan of Gansu Provincial Department of Education (2022CYZC-17)

## 1 引言

随着移动设备的普及和人际社交的日益发展，移动社交网络[1]在用户的日常生活中发挥着关键作用。各类社交平台(如微信、微博、Facebook, Twitter等)将海量用户信息集成到大数据中，以满足社交网络用户的交友需求。在移动社交网络中，可以通过使用数据加密技术实现对用户隐私的保护。社交平台被认为是诚实的，但也是好奇的。一方面，它诚实地执行系统中分配的任务；另一方面，它也试图尽可能了解更多关于数据的信息，而这很可能会引发隐私泄露问题。因此，如何实现高效的数据访问和细粒度的数据共享，同时保护用户的隐私信息是当前一项重大挑战，也是移动社交活动的重要研究内容。

在移动社交网络中，可以通过数据加密实现对用户的隐私保护。Sahai和Waters[2]在2005年提出了一种新的加密机制，称为属性基加密(Attribute Based Encryption, ABE)。基于密文策略的属性基加密(Ciphertext-Policy Attribute Based Encryption, CP-ABE)[3–5]通过对用户属性指定访问控制策略来加密数据，只有属性满足该策略的用户才能解密相应的数据，CP-ABE适合应用于移动社交网络、智慧医疗等多用户场景中。

Li等人[6]为了实现在云上的物联网数据的细粒度访问控制，提出一种可追踪的密文策略属性基加密(CP-ABE)方案。Wang等人[7]提出了一种高效的基于文件层次属性基加密方案，该方案将分层访问结构集成为一个单独的访问结构，利用集成访问结构对分层文件进行加密，既节省密文的存储空间，又减小了加密的时间开销。文献[8]采用基于属性的条件代理重加密，只有属性满足访问策略的数据传播者才能将数据传播到自己的社交空间。文献[9]提出一种利用属性进行朋友匹配的分层管理方案，旨在促进社交网络用户能够安全高效地寻找好友。为了快速匹配好友，文献[10]设计了一种新的基于CP-ABE的移动社交网络隐私保护属性匹配方案，用户之间几乎不需要交互即可完成高效匹配。

大多数现有的CP-ABE方案[11,12]通常需要多个配对运算，随着访问控制策略复杂性的增加，解密的计算开销变得非常大。具有访问控制权限的用户直接解密数据要承受很大的计算负担，尤其是在进行频繁的数据交互和共享时，例如本文中的移动社交网络应用背景下的用户。

为了解决上述问题，文献[13–16]通过将繁重的计算外包给代理服务器来减少解密的计算开销，允许用户通过“借用”第三方服务器提供商的计算资源来执行繁重的解密工作，而不会泄露数据。传统的ABE外包解密工作中，用户只有经过解密后才知道属性和策略是否匹配。而现有的大多数ABE方案往往需要多次配对操作，先解密后匹配的效率低下，会给用户造成严重的时间滞后。

为了实现用户端的快速解密，同时保障匹配用户的隐私安全和细粒度访问控制，本文提出一种支持外包解密的CP-ABE方案。本方案能够根据用户的自我描述和交友偏好进行精确匹配，同时在匹配过程中有效保护用户隐私。在交友双方信息匹配成功的情况下，交友中心执行大部分解密计算，减轻用户端的计算开销。本文的创新点如下：

(1)提出一种高效的基于CP-ABE的隐私保护好友匹配方案，当有大量用户想要从交友平台中检索数据时，交友中心可以快速排除不匹配的用户，对匹配用户迅速返回相应密文，同时实现了交友数据的高效共享和细粒度访问控制，既保护了用户隐私也提高了交友效率，具有实用性。

(2)在方案的外包解密阶段中，用户密钥被分成两部分，其中用户用于解密的部分私钥长度短且固定，大大节省了用户端的存储开销。将密文外包给交友中心后，用户端的计算成本降低到一个配对运算，提升了计算效率。

(3)实现了机密性，利用对称密钥对隐私文件进行加密，同时采用线性秘密共享方案(Linear Secret-Sharing Schemes, LSSS)对对称密钥进行加密保护，有效避免了匹配好友过程中用户隐私数据的泄露。

## 2 预备知识

### 2.1 双线性映射[9]

设$G_1$, $G_2$和$G_3$是阶为$p$的循环乘法群，$p$为大素数，则存在双线性映射$e: G_1 \times G_2 \to G_3$满足以下条件：

(1)双线性：对于$g \in G_1$, $h \in G_2$, $a, b \in Z_p$，有$e(g^a, h^b) = e(g, h)^{ab}$。

(2)非退化性：对于$g \in G_1$，$h \in G_2$，$e(g, h) \neq 1$。

(3)可计算性：对于$g \in G_1$, $h \in G_2$，存在有效算法可在多项式时间内计算$e(g, h) \neq 1$。

### 2.2 访问结构[11]

根据属性域$U$建立一个访问结构$\Lambda$，其中$\Lambda$是一个非空属性集合，$\Lambda$中的集合称为授权集合。访问结构$\Lambda$被称为是单调的，且对于任意集合$B$和$C$，若$B \in \Lambda, B \subseteq C$，则$C \in \Lambda$。本文仅考虑单调访问结构，访问结构在本文中也被称为访问策略。

在CP-ABE方案中，只有拥有授权属性集的用

户才能对密文进行解密。令所有属性集的集合$U=\{A_1,A_2,\cdots,A_n\}$，集合$A_i=\{a_{i,1},a_{i,2},\cdots,a_{i,m_i}\}$，对于$A_i\in U$，有$m_i$个取值。建立用户的属性列表$L=\{l_1,l_2,\cdots,l_n\}$，$l_i\in A_i$，设访问结构$\Lambda=\{\Lambda_1,\Lambda_2,\cdots,\Lambda_q\}$，$\Lambda_j\in A_i$。当且仅当$l_i=\Lambda_j$时，$i,j=1,2,\cdots$，本文称用户的属性列表$L$满足定义的访问结构$\Lambda$。

### 2.3 线性秘密共享[12]

若满足下列条件，则称属性域$U$上的线性秘密共享方案(LSSS)在$Z_p$($p$为素数)上是线性的：

(1)分配给每个属性的秘密共享值构成$Z_p$上的一个向量。

(2)对于域$U$上的访问策略，存在一个$l\times n$的共享矩阵$\boldsymbol{M}$和一个属性映射函数$\rho$，将$\boldsymbol{M}$的每一行映射到$U$中的一个特定属性，它满足以下条件：$\boldsymbol{Z}=\{s,z_2,\cdots,z_n\}$，其中$z_2,\cdots,z_n$是$Z_p$中的随机元素，$\boldsymbol{MZ}$是由秘密值$s$关于线性秘密共享方案的$l$个分享份额构成的向量，其中$(\boldsymbol{MZ})_j$是分配给属性$\rho(j)$的份额，$(\boldsymbol{M},\rho)$被称为访问策略。

线性秘密共享方案满足重构和安全要求。令集合$S$为策略$(\boldsymbol{M},\rho)$的授权集合，$I$为对应属性在$S$中的行数集合，即$I=\{i|\rho(i)\in S\cap i\in[l]\}$。若存在一组常数$\{w_i\in Z_p\}_{i\in I}$以及秘密值$s$的一组有效分享$\{\lambda_i\in Z_p\}_{i\in I}$，则$s$可以通过$\sum_{i\in I}w_i\lambda_i=s$恢复。常数$w_i$满足$\sum_{i\in I}w_i\boldsymbol{M}_i=(1,0,\cdots,0)$，并且可在生成共享矩阵$\boldsymbol{M}$的时间多项式内找到，对任何未授权的集合都不存在满足条件的常量。

### 2.4 困难性假设[12]

判定性$q$-parallel BDHE(decisional q-parallel Bilinear Diffie-Hellman Exponent)假设定义如下：设$G$是一个阶为素数$p$的群，$g$是$G$的一个生成元，随机选择$s,a,b_1,\cdots,b_q\in Z_p$，若给定敌手$\mathcal{A}$式(1)的参数

$$\begin{aligned}\mathrm{PP}=\{&G,p,g,g^s,g^a,\cdots,g^{(a^q)},g^{(a^{q+2})},\cdots,g^{(a^{2q})},g^{s\cdot b_j},\\&g^{a/b_j},\cdots,g^{(a^q/b_j)},g^{(a^{q+2}/b_j)},\cdots,g^{(a^{2q}/b_j)},\\&g^{(a\cdot s\cdot b^k/b_j)},\cdots,g^{(a^q s\cdot b_k/b_j)}\}_{\forall 1\le j,k\le q,k\ne j}\end{aligned}\tag{1}$$

敌手$\mathcal{A}$将无法区分$e(g,g)^{a^{q+1}s}$与随机元素$R\in G_3$。敌手在$q$-parallel BDHE问题上取得的优势为

$$|\Pr[\mathcal{A}(\mathrm{PP},e(g,g)^{a^{q+1}s})=0]-|\Pr[\mathcal{A}(\mathrm{PP},R)=0]|\le\varepsilon\tag{2}$$

如果敌手$\mathcal{A}$在任何多项式时间内不存在以不可忽略的优势$\varepsilon$来解决判定性$q$-parallel BDHE问题，则称判定性$q$-parallel BDHE假设在群$G$上成立。

## 3 方案模型定义

### 3.1 系统模型

本文系统架构由密钥生成中心(Key Generation Center, KGC)、交友中心服务器(Friend Server, FS)、交友数据发布者(Data Owner, DO)、交友数据请求者(Data Receiver, DR)4个实体共同组成。

KGC：它是一个可信任的授权机构，主要负责系统初始化，生成系统参数和主密钥。同时管理系统属性，根据用户属性为其生成属性密钥和私钥。

FS：服务器具有强大的存储和计算资源。FS提供好友匹配服务，存储DO的匹配参考信息，根据DR的请求为其匹配相应的DO，最终帮助匹配双方建立联系。FS也可对原始密文进行部分解密，减少DR的计算量，提高用户端的解密效率。

DO：DO在FS上注册并发布自己的交友匹配参考信息。为了实现对匹配好友的数据进行细粒度的访问控制，DO使用CP-ABE方案对交友数据进行加密，然后再将加密后的数据上传到FS。

DR：DR向FS发起交友请求，只有当DR自身的属性满足DO定义的访问策略时才能成功解密密文。未授权的用户不能恢复明文，也无法猜测出访问策略中涉及的属性。

### 3.2 属性信息与匹配

用户属性：在本文的系统模型中，每条交友发布者的匹配参考信息以及请求者的查询信息中都包含4个域，即用户ID、自我描述$S$、交友偏好$P$和交友文件$F$。ID为用户在FS中注册的唯一标识，自我描述$S$和交友偏好$P$分别描述用户自身特征和交友目标，即用户自身属性和定义的访问控制策略，交友文件$F$中为用户的隐私数据。

匹配条件：对于社交网络系统中的交友数据发布者和请求者，若发布者DO想在网络中搜索朋友，则将生成的交友偏好属性列表$P_{\mathrm{DO}}$上传到服务器，请求者上传自我描述属性列表$S_{\mathrm{DR}}$，在本方案中，如果交友偏好属性集是自我描述属性集的子集，则称匹配成功。DO和DR之间的属性匹配可用以下函数表示

$$\mathrm{Match}(\mathrm{DO},\mathrm{DR})=\begin{cases}1, P_{\mathrm{DO}}\subseteq S_{\mathrm{DR}}\\0, \text{其他}\end{cases}\tag{3}$$

例如图1中的Alice想通过移动社交网络寻找{年龄在18～30岁之间，并且爱好音乐的男性}，那么Alice会利用对称密钥加密自身的隐私文件，并将其上传到交友中心，交友中心对文件设置存储编号。同时，Alice将自身的访问控制策略提交至交友中心；如果在移动社交网络中，一个交友请求者Bob(如表1)的自我描述正好符合Alice的交友偏好，那么Bob就会获得Alice的文件，从而交友成功。

### 3.3 算法模型定义

本方案由7个算法构成，算法定义如下：

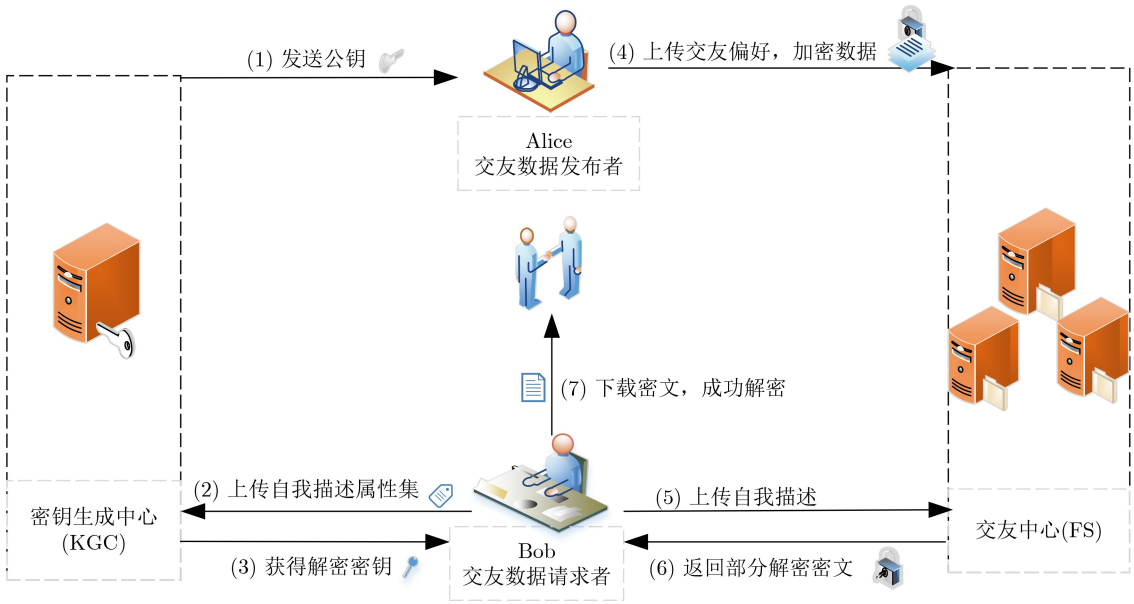


图 1 交友系统模型

**表 1 数据请求者的自我描述列表**

| 列表名 | 用户名 | 年龄 | 性别 | 血型 | 职业 | 住址 | 爱好 |
|---|---|---|---|---|---|---|---|
| $S_{\text{Bob}}$ | Bob | 26 | 男 | AB | 教师 | 北京 | 音乐、旅游、打羽毛球…… |
| $S_{\text{Ada}}$ | Ada | 22 | 女 | O | 空姐 | 上海 | 游泳、瑜伽、音乐、电影…… |
| $S_{\text{Leo}}$ | Leo | 35 | 男 | B | 警察 | 深圳 | 跑步、健身、做饭、画画…… |

(1) $\text{Setup}(1^{\kappa}, U) \to (\text{PK}, \text{MK})$：系统初始化算法。给定安全参数$\kappa$和系统属性集$U$，KGC运行该算法输出系统公钥PK和主密钥MK。

(2) $\text{KeyGen}(\text{PK}, \text{MK}, S) \to (\text{AK}, \text{SK})$：密钥生成算法。以PK, MK和一个用户属性集$S$作为输入，KGC运行该算法为用户生成与属性集$S$相关联的密钥AK和私钥SK。

(3) $\text{Enc}_1(\text{PK}, K, F) \to \text{CF}$：文件加密算法。输入系统公钥PK、对称密钥$K$和交友文件$F$，交友发布者DO输出文件的密文CF。

(4) $\text{Enc}_2(\text{PK}, K, (\boldsymbol{M}, \rho)) \to \text{CT}$：密钥加密算法。以系统公钥PK，对称密钥$K$和发布者定义的访问策略$(\boldsymbol{M}, \rho)$作为输入，交友发布者输出对称密钥的密文CT。

(5) $\text{Match}(\mathbf{RP}_{\text{DO}}, \mathbf{RS}_{\text{DR}}) \to 1/0$：匹配算法。输入用户$U_{\text{DO}}$的交友偏好提示向量$\mathbf{RP}_{\text{DO}}$，用户$U_{\text{DR}}$的自我描述提示向量$\mathbf{RS}_{\text{DR}}$，交友中心对用户$U_{\text{DO}}$和$U_{\text{DR}}$进行信息匹配，若匹配成功，输出结果为1，否则输出0。

(6) $\text{Dec}_1(\text{AK}, \text{CT}) \to \text{CT}'$：部分解密算法。FS输入交友请求者的属性密钥AK和密文CT，再对密文进行部分解密，得到部分解密密文$\text{CT}'$。

(7) $\text{Dec}_2(\text{SK}, \text{CT}') \to F$：文件解密算法。输入交友请求者DR的私钥SK和密文$\text{CT}'$，DR对FS发送过来的密文进行解密，最终得到交友数据发布者的隐私文件$F$。

本方案的基本数据流程如图2所示。在初始化阶段，KGC运行Setup算法生成系统公钥和主密钥。同时，利用KeyGen算法为系统中的用户生成私钥和属性密钥。交友数据发布者定义访问策略，运行Enc算法，为交友数据请求者生成可访问的密文。然后数据发布者将加密数据外包给交友中心服务器。交友数据请求用户向交友中心发送访问密文的请求。交友中心接收到请求后，运行Match算法进行信息匹配，检查请求者的属性是否满足发布者定义的好友访问策略，若查询者的自我描述符合发布者的交友偏好，说明请求者是预期的目标好友，交友中心运行$\text{Dec}_1$算法，用请求者的属性私钥对密文进行部分解密，并将部分解密后的密文发送给数据请求者。接着请求者运行$\text{Dec}_2$算法，用自己的私钥解密密文，最终获得发布者的隐私文件，从而交友成功。

### 3.4 安全模型

本方案的安全性主要依赖于判定性$q$-parallel BDHE假设，为了证明该方案的安全性，本文设计了一个关于攻击者$\mathcal{A}$和挑战者$\mathcal{C}$之间的游戏：针对选择访问策略和选择明文攻击下的不可区分性游戏

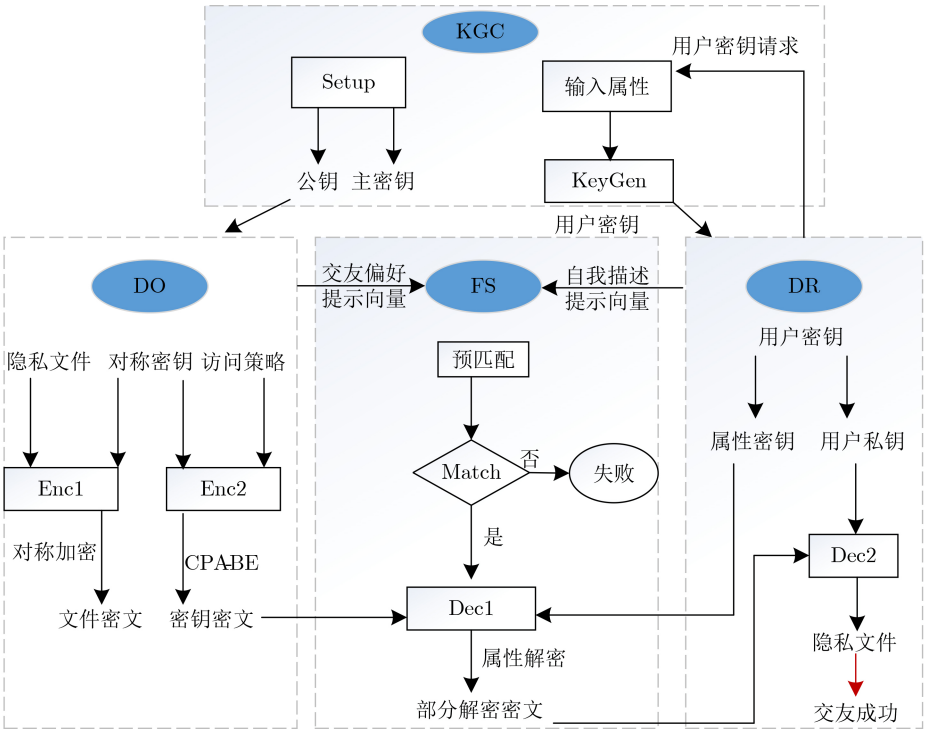


图 2 算法流程图

(INDistinguishability against Selective Access Policy and Chosen Plaintext Attacks, IND-SAP-CPA)。

(1)初始化阶段：$\mathcal{A}$选择一个任意的挑战访问策略$(\boldsymbol{M}^*, \rho*)$并将其提交给$\mathcal{C}$。

(2)系统建立阶段：$\mathcal{C}$运行$\text{Setup}(1^\kappa, U)$算法生成系统公钥PK和主密钥MK，$\mathcal{C}$将公钥PK发送给$\mathcal{A}$，保留主密钥MK。

(3)查询阶段1：在该阶段，$\mathcal{C}$回答$\mathcal{A}$提出的私钥查询。给定一个属性集$S$，$\mathcal{C}$运行算返回相应的解密密钥给$\mathcal{A}$，其中属性集$S$不满足访问策略$(\boldsymbol{M}^*, \rho*)$。

(4)挑战阶段：在这个阶段构建挑战密文CT*。$\mathcal{A}$向$\mathcal{C}$提供长度相等的消息$K_0$和$K_1$，$\mathcal{C}$随机选择$b \in \{0,1\}$，用$(\boldsymbol{M}^*, \rho*)$加密$K_b$，然后将挑战密文$\text{CT}^* = \text{Enc}(\text{PK}, K_b, (\boldsymbol{M}*, \rho*))$发送给$\mathcal{A}$。

(5)查询阶段2：重复查询阶段1的工作。

(6)猜测阶段：$\mathcal{A}$输出一个猜测$b'$，如果$b' = b$，则$\mathcal{A}$获胜。$\mathcal{A}$在本次游戏中的优势定义为

$$\varepsilon = \text{Adv}_{\mathcal{A}}^{\text{IND-SAP-CPA}} = \left| \Pr[b' = b] - \frac{1}{2} \right| \tag{4}$$

如果在所有多项式时间内攻击者$\mathcal{A}$在上述游戏中获胜的概率可忽略，那么本文方案是IND-SAP-CPA安全的。

## 4　具体方案

在本文中，用户在社交网络中的交友过程主要包括5个阶段：系统初始化阶段、用户密钥生成阶段、信息匹配阶段、数据加密阶段和数据解密阶段。各阶段的运算描述如下：

### 4.1　系统初始化阶段

KGC输入安全参数$\kappa$和属性域$U=\{\text{att}_1, \text{att}_2, \cdots, \text{att}_{|U|}\}$，设$G$和$G_1$是阶为素数$p$的乘法循环群，$g$是$G$的生成元，$e: G \times G \to G_1$是一个双线性映射。KGC随机选择$\alpha, \beta \in Z_p^*$，令$\gamma = (\alpha + \beta) \bmod p$，对于$U$中的每个属性，随机选择群元素$h_{\text{att}_1}, h_{\text{att}_2}, \cdots, h_{\text{att}_{|U|}} \in G$，KGC计算系统公钥PK和主密钥MK：$\text{PK}=\{g, e(g,g)^\gamma, g^\gamma, h_{\text{att}_1}, h_{\text{att}_2}, \cdots, h_{\text{att}_{|U|}}\}$，$\text{MK}=\{\alpha, \beta, \gamma\}$。

公开系统公钥PK，KGC秘密保存主密钥MK。

### 4.2　用户密钥生成阶段

如果交友请求者想要在移动社交网络上搜索心仪类型的好友，他/她首先在交友平台上进行注册，随后将自己的属性$S$(自我描述)提交给KGC, KGC再运行算法生成相应的安全密钥。

KGC随机选择$t, z \in Z_p^*$，令$\tilde{t} = t/z$，将用户密钥创建为两部分，一部分是可与交友中心服务器共享的“属性密钥”AK，另一部分是用户的私有“安全密钥”SK，KGC计算属性密钥AK和用户私钥SK：$\text{AK} = \{V_1 = g^{\alpha/z} g^{\gamma\tilde{t}}, E = g^{\tilde{t}}, \forall \text{att}_x \in S : V_x = h_{\text{att}_x}^{\tilde{t}}\}$, $\text{SK} = \{z, V_2 = g^{\beta/z} g^{\gamma\tilde{t}}\}$。

KGC通过安全信道将密钥(AK, SK)发送给交友数据请求者。

### 4.3　数据加密阶段

由于服务器不完全可信，为了保护敏感隐私

信息，数据发布者对数据进行两次加密，具体如下：

(1)DO根据需求建立多个不同的交友文件并使用不同的密钥进行加密。DO选择一个交友文件，设置编号为$F_i, i \in \{1,2,\cdots,n\}$，随机选择对称密钥$K$，对文件$F_i$进行对称加密，得到文件密文CF。

(2)DO将自己的交友偏好作为访问控制策略来加密对称密钥$K$，得到对称密钥密文CT。

DO将交友偏好设置为LSSS访问结构$(\boldsymbol{M},\rho)$的形式，构造一个向量$\boldsymbol{v}=(s,z_2,\cdots,z_n)$。对于$i=1$到$l$，计算$\lambda_i=\boldsymbol{M}_i\boldsymbol{v}$，得到一组秘密值的有效分享集合$\{\lambda_i\}$，$\boldsymbol{M}_i$表示矩阵$\boldsymbol{M}$中的第$i$行。此外，DO随机选择$r_1,r_2,\cdots,r_n\in Z_p$，得到密文$\mathrm{CT}=\{(\boldsymbol{M},\rho), C,C',\{C_i,D_i\}_{i\in[l]}\}$，其中，$C=K\cdot e(g,g)^{\gamma s}, C'=g^s$，$\{C_i=g^{\gamma\lambda_i}h_{\rho(i)}^{-r_i}, D_i=g^{r_i}\}_{i\in[l]}$。

DO将数据包$(F_i,\mathrm{CF},\mathrm{CT})$上传到交友中心FS。

### 4.4 信息匹配阶段

考虑到社交网络中潜在的匹配用户数量通常远小于用户总数，本文设计了一种快速过滤无效用户的机制。在本机制中，交友发起者将属性列表$P$中的属性数量和特征设置成提示向量**RP**发送给交友平台。请求匹配的用户，同样生成自己的查询属性向量**RS**，并上传至交友中心。交友中心在接收到查询包后，将请求者的属性列表与发布者的提醒向量进行比较，确定其是否是发起者的潜在好友。若预匹配成功，则进行下一步的匹配计算；否则，匹配终止。具体操作如下：

(1)对于交友偏好属性列表$P=\{p_1,p_2,\cdots,p_m\}$，$1\le i\le m$，DO计算$\mathrm{rp}_i\equiv\mathrm{Hash}(p_i)\mathrm{mod}\delta$，生成交友偏好提示向量$\mathbf{RP}=\{\mathrm{rp}_1,\mathrm{rp}_2,\cdots,\mathrm{rp}_m\}$，并上传至交友平台。同样地，DR对自我描述$S=\{s_1,s_2,\cdots,s_q\}$计算$\mathrm{rs}_j\equiv\mathrm{Hash}(s_j)\mathrm{mod}\delta$，生成自我描述提示向量$\mathbf{RS}=\{\mathrm{rs}_1,\mathrm{rs}_2,\cdots,\mathrm{rs}_q\}$, $1\le j\le q$。参数$\delta$的值越小，生成的提示向量越模糊，值越大，生成的提示向量越精确。显然，提示向量越精确，系统的安全性越低。在本系统模型中，不同用户的属性数量不一定相同。交友中心收到DR的属性列表后，比较**RP**和**RS**的长度，若$|\mathbf{RP}|>|\mathbf{RS}|$或属性类别相同时$\mathrm{rp}_i$与$\mathrm{rs}_j$的取值不同，则说明DR不符合DO的交友偏好，匹配终止；否则进入下一步匹配算法。

(2)第1步的预匹配之后，交友中心检查DR是否满足解密密文的条件。令$I=\{i:\rho_i\in S\}$，当DR的自我描述$S$满足DO定义的访问策略$(\boldsymbol{M},\rho)$时，存在一组常数$\{w_i\in Z_p^*\}_{i\in I}$使得$\sum_{i\in I}w_i\lambda_i=s$。交友中心计算是否存在一组正确的常数$w_i$使得$\sum_{i\in I}w_i\boldsymbol{M}_i=(1,0,\cdots,0)$，其中$\boldsymbol{M}_i$表示DR提交的属性值所对应的行向量，若能成功求得$w_i$的值，说明匹配成功，再进行之后的解密操作。

### 4.5 数据解密阶段

若DR向交友中心FS发起好友搜索请求，FS首先对DR进行信息匹配，检查其是否满足DO的交友条件。若预匹配成功，DR向交友中心FS发送密钥AK，利用交友平台进行部分解密。如果DR完全符合DO的交友目标，则可成功解密。求解过程如下：

(1)FS输入DR的AK和DO上传的密文CT，进行部分解密，计算$\mathrm{CT}'$

$$\mathrm{CT}'=\frac{e(C',V_1)}{\left(\prod\limits_{i\in I}\left(e(C_i,E)e(D_i,V_{\rho(i)})\right)^{w_i}\right)^2} \tag{5}$$

FS将计算出的$\mathrm{CT}'$以及DO的敏感数据文件密文CF发送给DR。

(2)DR收到FS传过来的部分解密密文$\mathrm{CT}'$和数据文件密文CF后，输入私钥$\mathrm{SK}=\{z,V_2\}$和$\mathrm{CT}'$，计算参数$B=e(V_2,C')\cdot\mathrm{CT}'$，再进一步计算出对称密钥

$$K=\frac{C}{B^z} \tag{6}$$

DR利用对称密钥$K$对DO的隐私文件进行解密，最终获得文件明文，即获得了交友发布者DO的联系方式、照片、音频等个人敏感数据，从而交友成功。

## 5 方案分析

### 5.1 正确性分析

为了证明式(6)正确性，先分析用于计算对称密钥的部分解密密文$\mathrm{CT}'$，再分析参数$B$。假设DR与DO匹配成功，即FS找到一组常数$\{w_i\in Z_p^*\}_{i\in I}$使得$\sum_{i\in I}w_i\lambda_i=s$，FS对密文进行部分解密后得到$\mathrm{CT}'$

$$\begin{aligned}\mathrm{CT}'&=\frac{e(C',V_1)}{\left(\prod\limits_{i\in I}\left(e(C_i,E)e\left(D_i,V_{\rho(i)}\right)\right)^{w_i}\right)^2}\\&=\frac{e(g^s,g^{\alpha/z}g^{\gamma\tilde{t}})}{\left(\prod\limits_{i\in I}\left(e(g^{\gamma\lambda_i}h_{\rho(i)}^{-r_i},g^{\tilde{t}})e(g^{r_i},h_{\rho(i)}^{\tilde{t}})\right)^{w_i}\right)^2}\\&=\frac{e(g,g)^{s\alpha/z}e(g,g)^{s\gamma\tilde{t}}}{\left(e(g^{\gamma},g^{\tilde{t}})^{\sum\limits_{i\in I}w_i\lambda_i}\right)^2}=\frac{e(g,g)^{s\alpha/z}}{e(g,g)^{s\gamma\tilde{t}}}\end{aligned} \tag{7}$$

所以$B=e(V_2,C')\cdot\mathrm{CT}'=e(g,g)^{s\gamma/z}$，从而$C/B^z=\dfrac{K\cdot e(g,g)^{\gamma s}}{\left(e(g,g)^{s\gamma/z}\right)^z}=\dfrac{K\cdot e(g,g)^{\gamma s}}{e(g,g)^{s\gamma}}=K$。

### 5.2 安全性分析

**定理1** 假设判定性$q$-parallel BDHE假设在群

$G$和$G_1$中成立，则在多项式概率时间内不存在敌手$\mathcal{A}$能以可忽略的优势赢得IND-SAP-CPA游戏。

**证明**　在本文定义的安全模型下，模拟敌手$\mathcal{A}$和挑战者$\mathcal{C}$之间的安全游戏。假设存在一个多项式时间敌手$\mathcal{A}$，它能够以$\varepsilon$的优势破坏本文方案的IND-SAP-CPA安全性。定义一个模拟器$\mathcal{B}$来试图解决判定性$q$-parallel BDHE问题，则存在$\mathcal{B}$以$\varepsilon/2$的概率来解决判定性$q$-parallel BDHE问题。模拟过程如下：

挑战者$\mathcal{C}$首先做如下设置：随机选择$s,a,b_1,\cdots,b_q\in Z_p$，公开参数

$$\begin{aligned}\mathrm{PP}=\{&G,p,g,g^s,g^a,\cdots,g^{(a^q)},g^{(a^{q+2})},\cdots,g^{(a^{2q})},g^{s\cdot b_j},\\&g^{a/b_j},\cdots,g^{(a^q/b_j)},g^{(a^{q+2}/b_j)},\cdots,g^{(a^{2q}/b_j)},\\&g^{(a\cdot s\cdot b^k/b_j)},\cdots,g^{(a^q s\cdot b_k/b_j)}\}_{\forall 1\le j,k\le q,k\ne j}\end{aligned}\tag{8}$$

$\mathcal{C}$随机选取$\mu\in\{0,1\}$，若$\mu=0$，令$T=e(g,g)^{a^{q+1}s}$；若$\mu=1$，$\mathcal{C}$随机选择元素$T\in Z_p$。

(1)初始化阶段。$\mathcal{A}$将欲挑战的访问策略$(\boldsymbol{M}^*,\rho*)$发送给$\mathcal{B}$，其中$\boldsymbol{M}^*$有$n^*$列。

(2)系统建立阶段。$\mathcal{B}$随机选择$\gamma'\in Z_p$，设置$e(g,g)^{\gamma}=e(g^a,g^{a^q})e(g,g)^{\gamma'}$。$\mathcal{B}$对群元素$h_{\mathrm{att}_1},h_{\mathrm{att}_2},\cdots,h_{\mathrm{att}_{|U|}}\in G$做如下设置：对于$1\le x\le U$的每个$x$，都有随机值$z_x\in Z_p$与之对应。令$X$表示索引$i$的集合，其中$\rho^*(i)=x$。$\mathcal{B}$计算$h_{\mathrm{att}_x}=g^{z_x}\prod_{i\in X}g^{aM^*_{i,1}/b_i}\cdot g^{a^2M^*_{i,2}/b_i}\cdots g^{a^{n*}M^*_{i,n*}/b_i}$。若$X=\varnothing$，则$h_{\mathrm{att}_x}=g^{z_x}$。需要注意的是，$h_{\mathrm{att}_x}$是随机分布的，因为$g^{z_x}$具有随机性。

(3)查询阶段1。$\mathcal{B}$构建一个元组列表$L_{\mathrm{SK}}=(S,\mathrm{SK},\mathrm{AK})$，列表最初为空。假设$\mathcal{A}$对不满足访问策略$(\boldsymbol{M}^*,\rho*)$的属性集$S$进行密钥查询请求，$\mathcal{B}$将回答$\mathcal{A}$的私钥查询。

如果属性集$S$已经被查询过，$\mathcal{B}$从列表$L_{\mathrm{SK}}$中检索密钥，然后返回$(\mathrm{SK},\mathrm{AK})$给$\mathcal{A}$。否则，$\mathcal{B}$设置向量$\boldsymbol{\beta}=(\beta_1,\beta_2,\cdots,\beta_{n*})\in Z_p^{n*}$，令$\beta_1=-1$，且对所有满足$\rho*(i)\in S$的$i$，$\boldsymbol{\beta}\cdot\boldsymbol{M}_i^*=0$。由LSSS的定义可得满足该条件的向量一定存在。$\mathcal{B}$随机选取$\alpha',\beta'\in Z_p$，令$\gamma'=(\alpha'+\beta')\mathrm{mod}p$，设$\alpha=\alpha'+a^{q+1}$，$\boldsymbol{\beta}=\boldsymbol{\beta}'$。然后$\mathcal{B}$计算$V_2=g^{\boldsymbol{\beta}'/z}g^{\gamma\widetilde{t}}=g^{\boldsymbol{\beta}/z}g^{\gamma\widetilde{t}}$。$\mathcal{B}$随机选择$r\in Z_p$，计算$E=g^r\prod_{i\in[1,n*]}(g^{a^{q+1-i}})^{\beta_i}=g^{\widetilde{t}}$，相当于隐含地定义了$\widetilde{t}=r+\beta_1a^q+\beta_2a^{q-1}+\cdots+\beta_{n*}a^{q-n*+1}$。

根据该定义，可使项$g^{-a^{q+1}}$包含在$g^{a\widetilde{t}}$中，即可在构造$V_1$时即可消掉未知项$g^{\alpha}$，$\mathcal{B}$计算$V_1$，$V_1=g^{\alpha'/z}g^{\gamma r}\prod_{i\in[2,n*]}(g^{a^{q+2-i}})^{\beta_i}=g^{\alpha/z}g^{\gamma\widetilde{t}}$。

接下来$\mathcal{B}$开始计算$\{V_x\}_{\mathrm{att}_x\in S}$。对于每个$\mathrm{att}_x\in S$，如果没有$i$使得$\rho^*(i)=x$，则$\mathcal{B}$可设置$V_x=h_{\mathrm{att}_x}^{\widetilde{t}}=(g^{z_x})^t=(g^{\widetilde{t}})^{z_x}=E^{z_x}$。如果有多个$i$使得$\rho^*(i)=x$，由于$\mathcal{B}$不能模拟$g^{a^{q+1}/b_i}$，所以对$V_x$需要满足不含有项$g^{a^{q+1}/b_i}$，由$\boldsymbol{\beta}\cdot\boldsymbol{M}_i^*=0$，$\mathcal{B}$可构造$V_x=E^{z_x}\prod_{i\in X}\prod_{j\in[1,n*]}(g^{(a^j/b_i)r}\prod_{k\in[1,n*],k\ne j}(g^{a^{(q+1+j-k)}/b_i})^{w_k})^{M^*_{i,j}}$；$\mathcal{B}$最后将生成的密钥添加到列表$L_{\mathrm{SK}}=(S,\mathrm{SK},\mathrm{AK})$中并发送给$\mathcal{A}$。

(4)挑战阶段。$\mathcal{A}$向$\mathcal{B}$提供两条长度相等的挑战信息$K_0$和$K_1$。$\mathcal{B}$随机选择$b\in\{0,1\}$，并计算出密文：$C*=K_b\cdot T\cdot e(g,g)^{\gamma's}, C'*=g^s$，接着$\mathcal{B}$选择随机数$y'_2,\cdots,y'_{n*}$，用向量$\eta=(s,sa+y'_2,sa^2+y'_3,\cdots,sa^{n-1}+y'_n)$对秘密值$s$进行分割。

此外，$\mathcal{B}$选择随机数$r'_1,r'_2,\cdots,r'_l\in Z_p$，定义$A_i$为满足$\rho^*(i)=\rho^*(k)$且$k\ne i$的所有$k$的集合，设置挑战密文中的$C_i,D_i$，其中$C_i=h_{\rho*(i)}^{r'_i}\left(\prod_{j\in[2,n]}(g^a)^{M^*_{i,j}y'_j}\right)\cdot(g^{b_is})^{-z_{\rho*(i)}}\cdot\left(\prod_{k\in A_i}\prod_{j\in[1,n]}(g^{a_j\cdot s\cdot(b_i/b_k)})^{M^*_{k,j}}\right)$，$D_i=g^{r'_i}g^{-sb_i}$。

(5)查询阶段2。重复查询阶段1的工作。

(6)猜测阶段。$\mathcal{A}$输出对$b$的猜测值$b'$，如果$b'=b$，$\mathcal{B}$输出$\mu'=0$，$T=e(g,g)^{a^{q+1}s}$，如果$b'\ne b$，$\mathcal{B}$输出$\mu'=1$，$T\in G_1$。当$\mu=0$时，$\mathcal{A}$得到一个有效密文$K_b$。根据定义，$\mathcal{A}$在这种情况下的优势是$\varepsilon$，因此$\Pr[b'=b|\mu=0]=1/2+\varepsilon$。当$b'=b$时，$\mathcal{B}$猜测$\mu'=0$，所以$\Pr[\mu'=\mu|\mu=0]=12+\varepsilon$。$\mu=1$意味着$\mathcal{A}$得不到$b$的任何信息，因此$\Pr[b'=b|\mu=1]=1/2$。当$b'\ne b$时，$\mathcal{B}$猜测$\mu'=1$，所以$\Pr[\mu'=\mu|\mu=1]=1/2$。$\mathcal{B}$解决判定性$q$-parallel BDHE问题的优势为：$\frac{1}{2}\Pr[\mu'=\mu|\mu=0]-\frac{1}{2}\Pr[\mu'=\mu|\mu=1]=\frac{\varepsilon}{2}$。

因此，$\mathcal{B}$能够以$\varepsilon/2$的优势解决判定性$q$-parallel BDHE难题，而该结论明显与目前已公认的判定性$q$-parallel BDHE假设相矛盾，因此，假设不成立，即该方案可以达到IND-SAP-CPA安全性。　证毕

交友发布者随机选择对称密钥对隐私文件加密，再利用CP-ABE加密对称密钥。由于对称加密和CP-ABE方案是安全的，有效保证了用户隐私信息的安全。其次，用户上传的提示向量**RP**和**RS**仅显示了属性的长度和对参数$\delta$的求余特征，由于存在不同属性值对$\delta$求余后的结果相同，所以交友中心无法通过提示向量推断出具体属性信息，从而便有效保证了用户数据的隐私保护。

本方案中交友发布者根据自身需求设置数据访问控制策略。发布者根据自己制定的访问策略(即交友偏好)来加密文件，然后将初始密文外包给社交网络交友中心。数据访问控制策略支持“与门”和“或门”逻辑操作，能够涵盖所有复杂条件。当数据请求者的自我描述属性满足发布者定义的交友

偏好属性时，请求者才能成功解密发布者的数据密文。因此，这种构造实现了对社交数据的细粒度访问控制。

### 5.3 性能分析

为进一步了解本方案在社交网络系统中的有效性和实用性，本文将本方案与文献[11,12,16]的方案进行了通信和计算开销方面的比较，这些方案和本文方案都使用了LSSS访问策略的CP-ABE方法来实现隐私保护。

#### 5.3.1 通信量分析

如表2所示，本文对方案的通信开销进行了比较分析，主要从系统公钥、系统主密钥、用户密钥和加密密文的存储量方面进行分析。令$|G|$, $|G_1|$ , $|Z_p|$ 和$|H|$ 分别为群$G$、群$G_1$ 、域$Z_p$ 和哈希函数的比特长度，$N$为系统中包含的属性数目。分析发现，本方案生成系统公钥的存储空间为$(2+N)|G|+|G_1|$，比其他方案存储负担低。本文系统主密钥的存储量为$3|G|$，用户密钥的存储量为$(3+u)|G|$，密文的存储长度为$(2l+1)|G|+|G_1|+|(\boldsymbol{M},\rho)|$，虽然本方案存储量高于文献[16]，但是从安全角度分析，本方案加大了攻击者的破坏难度，提高了系统的安全性。

#### 5.3.2 计算量分析

本文主要从密钥生成、数据加密和数据解密3个阶段对方案进行计算量的比较分析。

各方案的理论计算量如表3所示，其中，$T_{\mathrm{e}}$表示在群上的单个指数运算，$T_{\mathrm{p}}$ , $T_{\mathrm{h}}$和$T_{\mathrm{m}}$分别表示单个配对、哈希和乘法运算的计算开销，$u$表示用户提交的属性数目，$l$表示访问策略中的属性数目。

本文在一台惠普笔记本电脑的Linux系统上模拟了本文方案，设备处理器为Intel(R) Core(TM) i5-7200U CPU @2.50 GHz 2.70 GHz，利用PBC (Pairing-Based Cryptography)库实现所有算法。以用户的属性和访问策略的属性个数为变量，测试各个方案的运行时间。图3中的所有结果都是取50次实验的平均运行时间。

从图3(a)、图3(b)可以看出，在密钥生成和加密阶段，本文方案的计算量仅略高于文献[12]方案，这与表3中的分析一致。图3(c)和表3中都能看出，本文方案的解密效率最高，这是因为本文引用了外包解密技术，将大量繁琐的计算任务交给交友服务器，移动用户端仅需执行简单的解密操作，转换后的密文使解密效率更高，体积更小，且与访问控制策略的复杂度无关。

显然，通过对比分析发现，本文方案的效率整体高于其他方案，非常适合社交网络等多用户环境。

## 6 结论

针对移动社交网络中好友匹配的隐私保护问题，本文提出一种基于属性加密的私有数据共享方案，其中交友数据发布者可以根据实际需要灵活设置自己的访问控制策略，以保证只有属性满足访问策略的数据请求者才能够访问自己的社交空间。为了在资源有限的移动客户端上实现高效、安全的数据共享，本文在解密之前引入“匹配”算法，以快速过滤不匹配用户，使原有的CP-ABE结构适用于我们的应用场景，提高了匹配效率。同时为了减少用户的解密开销，本文将大量解密配对操作外包给交友中心提供商，极大地提升了用户端的解密效率。性能分析表明，本文方案是安全有效的，可适用于多种应用场景，例如在线医疗网络中的患者匹配、招聘网站中的求职者和职位匹配等。

**表 2 通信量分析**

| 方案 | 系统公钥 | 系统主密钥 | 用户密钥 | 加密密文 |
|---|---|---|---|---|
| 文献[11] | $9\|G\|+\|G_1\|+\|H\|$ | $\|G\|+4\|Z_p\|$ | $(2+5u)\|G\|$ | $(6l+1)\|G\|+\|G_1\|+\|(\boldsymbol{M},\rho)\|$ |
| 文献[12] | $(2+N)\|G\|+\|G_1\|$ | $\|G\|$ | $(2+u)\|G\|$ | $(l+1)\|G\|+\|G_1\|+\|(\boldsymbol{M},\rho)\|$ |
| 文献[16] | $(5+N)\|G\|+\|G_1\|$ | $(1+N)\|Z_p\|$ | $2\|G\|$ | $5\|G\|+2\|G_1\|$ |
| 本文 | $(2+N)\|G\|+\|G_1\|$ | $3\|G\|$ | $(3+u)\|G\|$ | $(2l+1)\|G\|+\|G_1\|+\|(\boldsymbol{M},\rho)\|$ |

**表 3 计算量分析**

| 方案 | 密钥生成 | 数据加密 | 数据解密 |
|---|---|---|---|
| 文献[11] | $(u+2)T_{\mathrm{e}}+T_{\mathrm{m}}$ | $(8l+2)T_{\mathrm{e}}+(l+3)T_{\mathrm{m}}$ | $uT_{\mathrm{e}}+(6u+1)T_{\mathrm{p}}+(5u+1)T_{\mathrm{m}}$ |
| 文献[12] | $(u+2)T_{\mathrm{e}}$ | $(2l+2)T_{\mathrm{e}}+(l+1)T_{\mathrm{m}}$ | $uT_{\mathrm{e}}+(2u+1)T_{\mathrm{p}}+(u+2)T_{\mathrm{m}}$ |
| 文献[16] | $(5u+3)T_{\mathrm{e}}+4T_{\mathrm{m}}$ | $(2l+6)T_{\mathrm{e}}+(2l+4)T_{\mathrm{m}}+2T_{\mathrm{h}}$ | $8T_{\mathrm{p}}+8T_{\mathrm{m}}$ |
| 本文 | $(u+3)T_{\mathrm{e}}$ | $(3l+2)T_{\mathrm{e}}+(l+1)T_{\mathrm{m}}$ | $T_{\mathrm{e}}+T_{\mathrm{p}}$ |

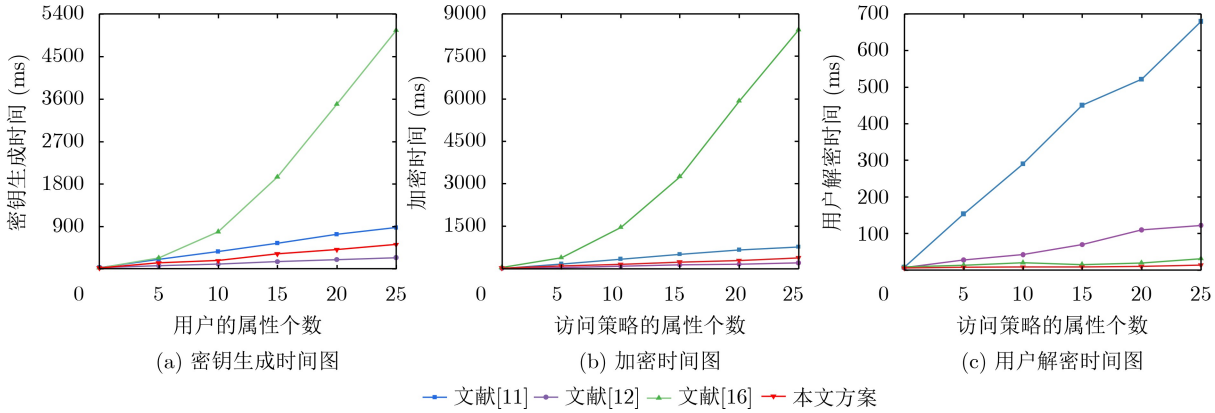


图 3 算法运行时间图

## 参 考 文 献


[1] QIU Tie, CHEN Baochao, SANGAIAH A K, *et al*. A survey of mobile social networks: Applications, social characteristics, and challenges[J]. *IEEE Systems Journal*, 2018, 12(4): 3932–3947. doi: 10.1109/JSYST.2017.2764479.

[2] SAHAI A and WATERS B. Fuzzy identity-based encryption[C]. The 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, 2005: 457–473. doi: 10.1007/11426639_27.

[3] SAIDI A, NOUALI O, and AMIRA A. SHARE-ABE: An efficient and secure data sharing framework based on ciphertext-policy attribute-based encryption and Fog computing[J]. *Cluster Computing*, 2022, 25(1): 167–185. doi: 10.1007/s10586-021-03382-5.

[4] FU Xingbing, WANG Yinglun, YOU Lin, *et al*. Offline/Online lattice-based ciphertext policy attribute-based encryption[J]. *Journal of Systems Architecture*, 2022, 130: 102684. doi: 10.1016/j.sysarc.2022.102684.

[5] DENG Shijie, YANG Gaobo, DONG Wen, *et al*. Flexible revocation in ciphertext-policy attribute-based encryption with verifiable ciphertext delegation[J/OL]. *Multimedia Tools and Applications*, 2022. doi: 10.1007/s11042-022-13537-0.

[6] LI Jiguo, ZHANG Yichen, NING Jianting, *et al*. Attribute based encryption with privacy protection and accountability for CloudIoT[J]. *IEEE Transactions on Cloud Computing*, 2022, 10(2): 762–773. doi: 10.1109/TCC.2020.2975184.

[7] WANG Shulan, ZHOU Junwei, LIU J K, *et al*. An efficient file hierarchy attribute-based encryption scheme in cloud computing[J]. *IEEE Transactions on Information Forensics and Security*, 2016, 11(6): 1265–1277. doi: 10.1109/TIFS.2016.2523941.

[8] HUANG Qinlong, YANG Yixian, and FU Jingyi. PRECISE: Identity-based private data sharing with conditional proxy re-encryption in online social networks[J]. *Future Generation Computer Systems*, 2018, 86: 1523–1533. doi: 10.1016/j.future.2017.05.026.

[9] ZHOU Lei, LUO Entao, WANG Guojun, *et al*. Secure fine-grained friend-making scheme based on hierarchical management in mobile social networks[J]. *Information Sciences*, 2021, 554: 15–32. doi: 10.1016/j.ins.2020.12.012.

[10] CUI Weirong, DU Chenglie, CHEN Jinchao, *et al*. CP-ABE based privacy-preserving user profile matching in mobile social networks[J]. *PLoS One*, 2016, 11(6): e0157933. doi: 10.1371/journal.pone.0157933.

[11] CUI Hui, DENG R H, LAI Junzuo, *et al*. An efficient and expressive ciphertext-policy attribute-based encryption scheme with partially hidden access structures, revisited[J]. *Computer Networks*, 2018, 133: 157–165. doi: 10.1016/j.comnet.2018.01.034.

[12] YANG Kan, HAN Qi, LI Hui, *et al*. An efficient and fine-grained big data access control scheme with privacy-preserving policy[J]. *IEEE Internet of Things Journal*, 2017, 4(2): 563–571. doi: 10.1109/JIOT.2016.2571718.

[13] PREMKAMAL P K, PASUPULETI S K, and ALPHONSE P J A. A new verifiable outsourced ciphertext-policy attribute based encryption for big data privacy and access control in cloud[J]. *Journal of Ambient Intelligence and Humanized Computing*, 2019, 10(7): 2693–2707. doi: 10.1007/s12652-018-0967-0.

[14] ZHANG Zhishuo and ZHOU Shijie. A decentralized strongly secure attribute-based encryption and authentication scheme for distributed Internet of Mobile Things[J]. *Computer Networks*, 2021, 201: 108553. doi: 10.1016/j.comnet.2021.108553.

[15] FENG Chaosheng, YU Keping, ALOQAILY M, *et al*. Attribute-based encryption with parallel outsourced decryption for edge intelligent IoV[J]. *IEEE Transactions on Vehicular Technology*, 2020, 69(11): 13784–13795. doi: 10.1109/TVT.2020.3027568.

[16] LI Jiguo, SHA Fengjie, ZHANG Yichen, *et al*. Verifiable outsourced decryption of attribute-based encryption with constant ciphertext length[J]. *Security and Communication Networks*, 2017, 2017: 3596205. doi: 10.1155/2017/3596205.



牛淑芬：女，博士，教授，研究方向为云计算和大数据网络的隐私保护.

戈　鹏：女，硕士生，研究方向为网络与信息安全.

宋　蜜：女，硕士，研究方向为网络与信息安全.

宿　云：女，博士，副教授，研究方向为情感计算.


责任编辑：余　蓉