软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2018,29(10):3223−3238 [doi: 10.13328/j.cnki.jos.005295]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

移动社交网络中细粒度朋友发现隐私保护机制*

罗恩韬[1,2], 王国军[1], 刘 琴[3], 孟大程[2]

[1](广州大学 计算机科学与教育软件学院,广东 广州 510006)

[2](中南大学 信息科学与工程学院,湖南 长沙 410083)

[3](湖南大学 信息科学与工程学院,湖南 长沙 410082)

通讯作者: 王国军, E-mail: csgjwang@gmail.com

摘 要: 在移动社交网络中,用户可以通过匹配彼此的特征属性进行朋友发现,针对单属性管理中心用户属性密钥更容易被攻击者窃取和服务高峰出现的性能瓶颈问题,提出一种由多个属性管理中心、分级管理用户属性子密钥方案.在该方案中,多个属性中心细粒度地管理用户的不同特征属性,并根据用户特征属性生成属性子密钥,交友请求者只有满足交友发起者设置的交友访问策略,才能正确地将各子密钥组合成完整的解密密钥,进而解密存储在交友中心的用户加密数据文件.通过对属性子密钥进行分级分类管理,不仅避免了单属性管理中心容易被攻击而造成的密钥泄漏以及单点故障风险,而且多属性中心协同工作提高了交友匹配计算效率.通过验证方案是否可挑战明文攻击,证明可达到 CPA 安全,可以有效地保护用户的隐私不被泄露.同时与既有方案进行了充分的对比实验,确保该方案计算开销最小,可以提供良好的用户体验.

关键词: 密文访问控制策略;多授权中心;属性加密;隐私保护;机会计算

中图法分类号: TP309

中文引用格式: 罗恩韬,王国军,刘琴,孟大程.移动社交网络中细粒度朋友发现隐私保护机制.软件学报,2018,29(10):3223−3238. http://www.jos.org.cn/1000-9825/5295.htm

英文引用格式: Luo ET, Wang GJ, Liu Q, Meng DC. Fine-Grained secure friend discovery scheme in mobile social networks. Ruan Jian Xue Bao/Journal of Software, 2018,29(10):3223−3238 (in Chinese). http://www.jos.org.cn/1000-9825/5295.htm

Fine-Grained Secure Friend Discovery Scheme in Mobile Social Networks

LUO En-Tao[1,2], WANG Guo-Jun[1], LIU Qin[3], MENG Da-Cheng[2]

[1](School of Computer Science and Educational Software, Guangzhou University, Guangzhou 510006, China)

[2](School of Information Science and Engineering, Central South University, Changsha 410083, China)

[3](College of Computer Science and Engineering, Hu'nan University, Changsha 410082, China)

Abstract: In mobile social networks, users can look for friends by matching their attributes. In order to solve the problem that the user's attribute is easy to be stolen by the attackers in the single authority center and performance bottleneck occurs in the peak of service, this work proposes a scheme where a multi-attribute management center hierarchically manages user attributes' sub-keys. The scheme involves several attribute centers which perform fine-grained management on different user attributes. After the friend requester's attributes meet the friend access control policy of the friend-making initiator, the friend requester can correctly combine the sub-keys into

*基金项目: 国家自然科学基金(61632009, 61472451, 61402543, 61272151, 61502163); 湖南省自然科学基金(2015JJ3046); 湖南省教育厅科研项目(2015C0589, 110351018002); 中南大学中央高校基本科研业务费专项资金(2016zzts060, 2016zzts339)

Foundation item: National Natural Science Foundation of China (61632009, 61472451, 61402543, 61272151, 61502163); Natural Science Foundation of Hu'nan Province, China (2015JJ3046); Hu'nan Provincial Education Department of China (2015C0589, 110351018002); Fundamental Research Funds for the Central Universities of Central South University (2016zzts060, 2016zzts339)

收稿时间: 2017-01-15; 修改时间: 2017-03-12; 采用时间: 2017-04-24; jos 在线出版时间: 2017-12-01

CNKI 网络优先出版: 2017-12-04 06:46:36, http://kns.cnki.net/kcms/detail/11.2560.TP.20171204.0646.001.html

a complete decryption key and decrypt the user's data file to store in the friend-making server. By introducing hierarchical management in terms of attribute sub-keys, the proposed scheme not only effectively prevents key disclosure when the single-authority management center suffers from attacks, but also improves the computation efficiency of friend profile matching through cooperative work of multiple attribute center. Experiments are conducted to check whether the proposed scheme can challenge the chosen plaintext attack, and certify that the scheme can achieve CPA secure level while effectively protecting the user's privacy security. Extensive comparisons with existing schemes demonstrate the ability of the proposed scheme to entail the lowest computational overheads and provide excellent user experience.

Key words: ciphertext-policy access control; multi-authority; attribute-based encryption; privacy-preserving; opportunity calculation

随着移动社交网络(mobile social network,简称 MSN)和智能手机的飞速发展[1−4],用户利用智能手机在移动社交网络中可以通过匹配彼此的个人属性文件,找到具有共同兴趣爱好的朋友或者具有某类相似属性特征的用户.例如:用户可以通过在社交网络中随时分享心情、照片、活动、兴趣爱好等来不断地发现新的朋友,从而进一步扩大自己的社交范围(例如,微信、智圈、微聚等).

用户个人信息通常蕴含着巨大的商业价值.随着用户交友体验程度的不断加深和范围的不断扩大,用户的真实信息将在远端和终端上海量汇聚.所以常常被其他非法用户在未授权的情况下搜集、分析、挖掘或者出卖,进而威胁到用户的隐私安全.例如,通过发现对方的购物爱好,可以分析用户的消费能力,通过对用户朋友圈的分析,可以定义用户的身份等,而这些隐私信息一旦被泄漏,极有可能被恶意用户所利用进行非法活动(例如,2016 年 8 月发生的轰动全国的山东学生徐**被电信诈骗的案件).

因此,如何在提供良好交友匹配服务的基础上进一步促进移动社交活动的发展,同时又能够保护用户个人隐私安全,是当前交友隐私保护中亟待解决的一个热点问题,也是移动应用服务提供商未来的研究方向.

1 相关工作

1.1 研究背景

目前,国内外很多专家在移动社交网络交友隐私保护的研究上做出了贡献,在文献[5,6]中,通过引入可信第三方(trusted third party,简称 TTP)来保护用户交友过程中的隐私.在此类模型中,单一的可信第三方负责产生和管理用户所有的密钥,因此有可能存在单点故障、密钥失窃风险、服务高峰性能瓶颈问题.文献[7−11]提出了不依赖 TTP 的解决方案,此类方案通过计算用户属性私有交集(private set intersection,简称 PSI)来保证用户的隐私不被泄漏.主要方法是:匹配双方各自持有自己的私有数据集,仅仅通过计算两者共同交集的大小而不泄漏彼此额外的信息来保证用户双方的隐私.但是,此类方法只考虑了用户共同的属性个数,因此无法实现细粒度的访问控制和属性匹配.

Zhang 等人[12]对以上方法进行了改进,提出根据用户的兴趣偏好分配不同的权重,计算匹配的相似度.Niu 等人[13]对用户的属性设置了优先级匹配.Zhu 等人[14]提出高效的混淆矩阵变换算法以实现安全、高效的匹配.但是,上述方案中用户只能对属于公共集合的属性进行设置,因此,应用范围比较有限.例如,当用户更换交友场景时,也许很难找到有共同特征的朋友.

随后,单可信授权中心(trusted authority,简称 TA)结合属性加密方案被提了出来.该方案主要分为基于密钥的加密方案(key policy attribute based encryption,简称 KP-ABE)[15−18]与基于密文的加密方案(ciphertext policy attribute based encryption,简称 CP-ABE)[19−21].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,属性集关联私钥,访问机构关联密文,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.通过比较,相对于 KP-ABE,CP-ABE 更适合应用在移动社交网络用户交友过程中对消息进行加密.

因此,文献[22]提出了基于单授权中心与 CP-ABE 属性加密方案的访问控制策略,可以为属性的匹配和消息共享提供细粒度的访问控制,也可以解决用户交友场景变换的问题.

但是,单独依靠单可信中心的属性加密方案依然存在安全风险.第一,一旦权限实体被攻破,攻击者可以很容易地获得唯一的权威主密钥,进而生成属性子集的子密钥,对加密数据进行解密,造成隐私泄漏风险.第二,一旦唯一的可信中心遭受性能瓶颈或者被攻击者破坏,则系统就完全不能提供服务.第三,依靠单授权中心,用户在更新交友属性时,就需要更新整个访问控制结构,计算开销较大.

1.2 本文贡献

为解决单可信中心的性能瓶颈和密钥托管风险问题,同时又能够达到对匹配用户的细粒度访问权限控制,以及可灵活更新用户的访问控制策略,本文拟通过引入多授权属性中心,对用户的属性进行多层次、细粒度、分级分类管理,本文的贡献如下:

(1) 利用多层次属性中心管理用户子密钥,各级属性中心分管属性私钥,可以有效降低单属性中心密钥泄漏风险;

(2) 利用属性管理中心分层思想,可以有效降低单属性管理中心因为单点故障造成系统不可用和高峰时期的性能计算瓶颈;

(3) 利用细粒度精确匹配思想,各个属性管理中心分别管理某一类属性,用户进行属性更新时,无需更新所有的策略树,在降低开销的同时,对于移动社交网络应用场景的变化,更具有普适性.

1.3 本文组织结构

本文第 2 节给出方案的预备数学知识.第 3 节给出详细设计,主要包括方案的系统模型和安全模型.第 4 节为方案的具体实施部分.在第 5 节中进行安全性证明以及交友概率分析、计算复杂度分析.详细的实验验证在第 6 节中给出.

2 预备知识

2.1 秘密共享

Shamir[23]、Blakely[24]提出了秘密共享思想.一个秘密被拆分成若干子秘密,每一部分由不同的管理者进行管理,单个管理者不能恢复完整的秘密,只有多个管理者进行协同合作才能恢复完整的秘密信息.

(1) 设 $F(x)$为一项多项式,次数小于 d 次,假设存在 d 个不同的点$(x_i,y_i=F(x_i))$,$\forall x,y$,可以用拉格朗日中值定理求出插值.

(2) 设集合 S 中包含 d 个元素,在整数集中选择 $j\in Z_p$,可以求出 $F(x)$的拉格朗日系数为

$$\Delta_{i,s}(x)=\prod_{x_i\in S,x_i\neq x_j}(x-x_i)/(x_j-x_i).$$

根据 $\Delta_{i,s}(x)$,进而可求出 $F(x)=\sum_{i=1}^{d}(y_i\cdot\Delta_{i,s}(x))$.

2.2 双线性映射

设 G_1,G_2 为循环群,生成阶为 p,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:

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

(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 $g\in G_1,h\in G_2$,可以有效计算 $\hat{e}(g,h)$ 的结果.

2.3 安全性假设

判定性双线性问题及假设(decisional bilinear Diffie-Hellman,简称 DBDH).

给定阶为素数 p 的循环群 G_1,G_2 的五元组$(g,g^a,g^b,g^c,e(g,g)^{abc})$,其中,元素 $a,b,c\in Z_p$,将 $e(g,g)^{abc}$ 发送给攻击者,由攻击者随机选择 $z\in Z_p$ 判定等式 $e(g,g)^z=e(g,g)^{abc}$ 是否成立,则攻击者求解出 DBDH 问题优势可以定义为

$$Adv_{DBDH}=|Pr[A(g,g^a,g^b,g^c,e(g,g)^{abc})=1]-Pr[A(g,g^a,g^b,g^c,e(g,g)^z)=1]|\geqslant\varepsilon.$$

如果针对以上问题,攻击者在任意概率多项式时间内不能以不可忽略的优势ε区分$e(g,g)^z \stackrel{?}{=} e(g,g)^{abc}$,则称群$G_1,G_2$满足 DBDH 假设.

3 方案设计

现给出一个具体的交友过程示例进行说明,假如图 1 中的 Alice 想通过移动社交网络寻找{年龄在 30 岁之内,并且同时具有音乐爱好或者旅游爱好的男性},那么 Alice 会选择一个双线性对随机数加密自身的隐私文件,并将这个隐私文件上传到云交友中心管理.隐私文件中可能包含 Alice 的照片、视频、锻炼数据、联系方式等等.同时,Alice 将自身的访问控制策略提交多属性中心管理;交友中心和属性中心之间可协商访问控制策略对应加密文件的存储编号.如果在移动社交网络中,一个交友请求者 Bob 上传自己的属性到属性管理中心后,正好符合 Alice 的访问策略,那么 Bob 就会得到 Alice 隐私文件的解密密钥和解密对应的文件密文,从而为进一步增进双方的了解提供便利.交友过程的总体架构图如图 1 所示.

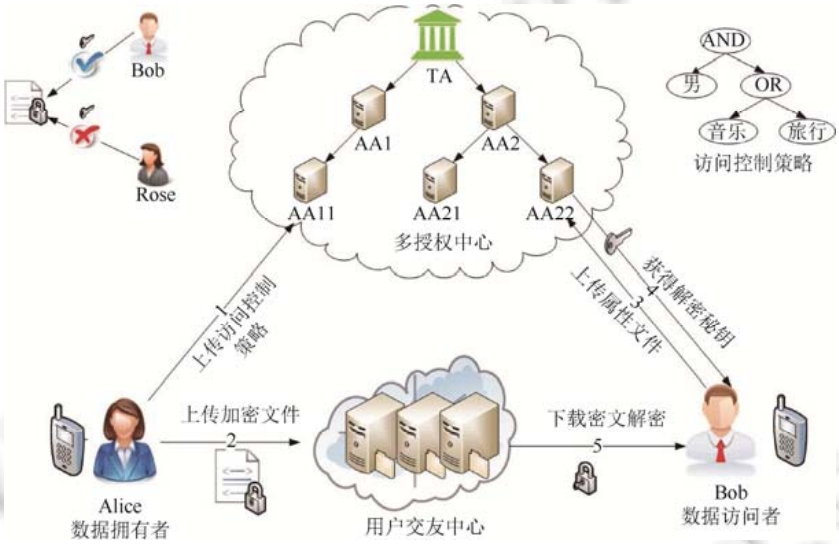


Fig.1 Friend discovery model in mobile social networks

图 1 移动社交网络匹配过程模型图

3.1 系统模型

系统架构由交友中心(friend server,简称 FS)、可信中心安全服务器(trusted authority,简称 TA)、多授权属性管理中心(attributed authority,简称 AA)、交友数据拥有者 Alice、交友数据请求者 Bob 共同组成.

- 交友中心 FS:存储用户的交友隐私数据密文,包括个人照片、个人视频、兴趣爱好、联系方式、身份信息等.
- 可信中心安全服务器 TA:主要负责系统初始化和主密钥的产生,为每一个 AA 授权并分配访问控制策略.
- 多属性管理中心 AA:每一个 AA 负责管理用户某类属性集合,产生相应的属性子密钥和对下级 AA 进行授权等.
- 交友数据拥有者 Alice:拥有对交友隐私数据的所有权利,包括对数据的修改、删除、加密以及对交友请求用户 Bob(或移动网络中的其他用户)指定访问控制策略.
- 交友数据请求者 Bob:交友数据请求者的属性只有满足 Alice 的访问控制策略才能够得到正确的解密密钥,进而正确解密交友请求者的隐私数据.

同时,为了进一步明确他们在模型中的工作角色,假设 TA 和数据拥有者 Alice 是完全可信的,数据请求者 Bob 是完全不可信的,即数据请求者可能串通、共谋、非法访问未经授权的数据.而 FS、AA 是诚实而好奇的[5],

即 FS、AA 会按照既定协议工作,但是不排除他们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.因此,用户在 FS、AA 上存储数据之前,需要对数据进行加密处理.

3.2 安全模型

安全模型可通过定义攻击者 A(非法用户)和挑战者 C(合法用户)之间的攻防过程来达到保证交友隐私安全的目的.如果在游戏中,攻击者给出了正确的猜测,则攻击者赢得了游戏;反之,则挑战者赢得了游戏.如果攻击者猜测正确的优势是可以忽略的,则称方案在选择明文攻击(chosen plaintext attack,简称 CPA)下是不可区分的.

(1) 准备阶段

A 任意选择一个将被挑战的访问控制策略 T^*,发送给挑战者 C.

(2) 系统建立阶段

C 运行密钥生成算法生成系统公钥 PK_0 和系统主密钥 MK_0,C 自身保存 MK_0 并将 PK_0 发送给 A.

(3) 查询第 1 阶段

A 构造属性集合 $\Lambda=\{A_0,A_1,\ldots,A_n\}$向挑战者 C 发出属性私钥请求,但是 Λ 中的元素 $A_i(1\leqslant i\leqslant n)$均不满足 T^*,C 产生属性私钥 SK_i 并发送给 A.

(4) 挑战阶段

A 完成查询第 1 阶段后,将选择两个等长比特长度的明文 M_0 和 M_1 发送给 C.C 任意选择一个比特$\delta\in\{0,1\}$,并利用 T^*对消息 M_δ进行加密,生成密文 $CT^*=Encrypt(T^*,M_\delta)$,最后将 CT^*发送给 A.

(5) 查询第 2 阶段

A 进行解密查询,C 则重复执行查询第 1 阶段的步骤.

(6) 猜测阶段

A 输出比特δ'来猜测在挑战阶段 C 选择的δ是 0 或者是 1,如果敌手猜测正确,即$\delta'=\delta$,那么 A 赢得上述游戏的概率为

$$Adv_A(k)=\left|Pr[\delta=\delta']-\frac{1}{2}\right|.$$

如果对于任意多项式单位 t 时间内攻击者 A 取得的优势 $Adv_A(k)$是可以忽略的,则称该方案是满足 CPA 安全的,CPA 的详细安全证明见文献[25].

4 具体实施

交友过程由 4 个阶段组成,分别为:系统初始化阶段、用户属性私钥生成阶段、用户数据加密阶段、数据解密阶段.其安全性建立于密码学认可的双线性加密安全框架上.相关符号描述可见表 1.

Table 1 Symbol description

表 1 符号描述

符号	描述
G,g	循环群和生成元
G_{id},A_{id}	用户身份标识和属性管理中心标识
TA,AA	可信授权机构和属性管理中心
PK,MK	系统公钥和系统主密钥
SK	AA 上用户属性对应的私钥
$T^{(k)}$	用户访问控制策略树
$\Lambda=(A_0,A_1,\ldots,A_n)$	属性管理集合
$Au^{(k)}_{Alice}$	Alice 在第 k 个 AA 上的属性集合
$a^{(k)}_{Alice_{i,j}}$	属性集合 $Au^{(k)}_{Alice\_i}$ 中第 j 个属性
$CT^{(k)}_{Alice}$	Alice 在第 k 个 AA 上的属性密文
M	数据拥有者的数据明文
$H()$	哈希散列函数

4.1 系统初始化阶段

首先,TA 为所有交友用户和属性管理服务器 AA 分别分配全局唯一身份标识 G_{id} 以及 A_{id},G_{id} 通常是用户身份数字签名字符串,且被用户自身独立保密持有,AA 可验证 G_{id} 的真实性.考虑到实际的计算开销,TA 可对授权属性中心的层次深度 *dep* 进行限定.

其次,TA 计算系统公钥 PK_0 和系统主密钥 MK_0.

$$PK_0=\left(G,g,h_1=g^{\beta_1},h_2=g^{\beta_2},f_1=g^{\frac{1}{\beta_1}},f_2=g^{\frac{1}{\beta_2}},e(g,g)^{\alpha}\right) \tag{1}$$

$$MK_0=\left(\beta_1,\beta_2,g^{\alpha}\right) \tag{2}$$

$$\alpha,\left(\beta_1,\beta_2,...,\beta_{depth}\right)\in Z_p$$

再次,TA 对一级属性管理中心 AA 进行授权.

(1) 假设 AA 管理的属性集合为 $\Lambda=\{A_0,A_1,\ldots,A_n\}$,其中,$A_0$ 表示第 1 层属性,A_i 表示第 i 层属性,$a_{i,j}$ 表示属性子集 A_i 中第 j 个属性.m 表示 A_i 中属性的个数($0\leqslant i\leqslant n$,$1\leqslant j\leqslant m$).TA 随机选择参数 $r,r_i,r_{i,j}\in Z_p$ 分别表示 $\Lambda,A_i,A_{i,j}$,计算第 1 级 AA 的主密钥 MK_1.

$$MK_1=\left(\Lambda,D=g^{\frac{\alpha+r}{\beta_1}},D_{i,j}=g^{r_i}\cdot H(a_{i,j})^{r_{i,j}},D'_{i,j}=g^{r_{i,j}},E_i=g^{\frac{r+r_i}{\beta_2}}\right) \tag{3}$$

在公式(3)中,利用参数 E_i 对节点进行解密转换以保证不同集合中的属性可以匹配.

(2) 设 Λ 为上级 AA 管理的属性集,Λ'为下级 AA 管理的属性集,且满足 Λ'是 Λ 的子集,可计算 AA_{k+1} 层的主密钥 MK_2.

$$MK_2=\left(\Lambda',\tilde{D}=D\cdot f_1^{\tilde{r}},\tilde{D}_{i,j}=D_{i,j}\cdot g^{\tilde{r}}\cdot H(a'_{i,j})^{\tilde{r}_{i,j}},D'_{i,j}=D'_{i,j}\cdot g^{\tilde{r}_{i,j}},\tilde{E}_i=E_i\cdot f_2^{\tilde{r}+\tilde{r}_i}\right) \tag{4}$$

$\tilde{r},\tilde{r}_i,r_{i,j}\in Z_p$ 为 AA_k 随机的选择参数,分别表示 $\Lambda',\Lambda'_i,a'_{i,j}$.

4.2 用户属性私钥生成阶段

假设 Alice 期望通过移动社交网络中的交友中心找到具有某一类特征的用户,那么 Alice 可设置满足一系列的交友属性特征的交友策略树(如图 2 所示),并上传到多授权属性管理中心.为了保证用户的隐私安全和服务的高可用性,依据秘密共享思想,Alice 所有属性特征 Au_{user} 将被拆分成互不相交的 K 份,由属性信任链上的 K 个 AA 共同管理.假设 Alice 在第 k 个($1\leqslant k\leqslant K$)上的属性集合为

$$Au_{user}^{(k)}=\left(Au_{user\_0}^{(k)},Au_{user\_1}^{(k)},...,Au_{user\_n}^{(k)}\right).$$

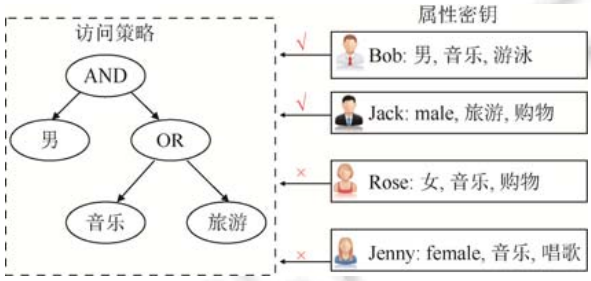


Fig. 2 Access policy tree schematic diagram

图 2 交友访问策略树结构示意图

$Au_{user\_0}^{(k)}$ 表示由单个属性组成的集合,$Au_{user\_i}^{(k)}$ 表示属性子集. $Au_{user\_i}^{(k)}=\left(a_{i,0}^{(k)},a_{i,1}^{(k)},...,a_{i,j}^{(k)},...,a_{i,m}^{(k)}\right)$, $a_{i,j}^{(k)}$ 表示属性子集 $Au_{user\_i}^{(k)}$ 中第 j 个属性.m 表示 $Au_{user\_i}^{(k)}$ 中属性的个数,那么用户的在第 k 个属性管理中心的属性子密钥可按照如下步骤计算.

(1) AA_k 为 $Au_{user}^{(k)}$ 选择随机整数 $ru^{(k)}$,为每个属性子集 $Au_{user\_i}^{(k)}$ 选择 n 个不相同的随机整数 $ru_i^{(k)}(i=1,2,...,n)$.

对于集合 $Au_{user\_0}^{(k)}$, 设 $ru_0^{(k)}=ru^{(k)}$; 同时为 $Au_{user\_i}^{(k)}$ 中的每个属性 $a_{i,j}^{(k)}$ 选择不同的随机整数 $ru_{i,j}^{(k)}$.

(2) AA_k 根据用户的 G_{id} 和 A_{id_k} 计算用户的私钥部件 $P_{SK}(u)=\alpha_{k,u}$.

(3) 计算用户在 AA_k 的子密钥 $SK_{user}^{(k)}$.

$$SK_{user}^{(k)}=\left(D_{user}^{(k)}=g^{\frac{\alpha_{k,u}+ru^{(k)}}{\beta_{k,1}}},D_{i,j}^{(k)}=g^{ru_i^{(k)}}\cdot H(a_{i,j}^{(k)})^{ru_{i,j}^{(k)}},D_{i,j}'^{(k)}=g^{ru_{i,j}^{(k)}},E_i^{(k)}=g^{\frac{ru^{(k)}+ru_i^{(k)}}{\beta_{k,2}}}\right) \tag{5}$$

其中, $\beta_{k,1}=\dfrac{\beta_1}{\alpha+r+\tilde{r}}$, $\beta_{k,2}=\dfrac{\beta_2}{r+r_i+\tilde{r}+\tilde{r}_i}$ 分别是 AA_k 上的两个局部主密钥.

(4) 计算用户在所有 AA 属性的总密钥 SK_{user}.

$$SK_{user}=\left(\left(SK_{user}^{(k)}\right)_{k=1}^{K},D_{user}=g^{\left(\alpha+\sum_{k=1}^{K}\alpha u_{(k)}\right)\Big/\sum_{k=1}^{K}\beta_{k,1}}\right) \tag{6}$$

D_{user} 用于满足访问策略树的用户进行文件解密(见后文公式(18)),由 TA 颁发.

4.3 用户数据加密阶段

实际上,由于不存在完全可信的交友服务提供商,即服务商有可能窥视用户存储在其上的隐私数据,所以 Alice 将明文数据 M 上传至远程的交友中心服务器之前,须选择一个随机数 $\theta\in Z_p$,并利用公布的双线性参数 $e(g,g)^{\alpha}$ 组成加密密钥 $SECRET_{Key}$,对明文 M 进行加密,生成密文 $\tilde{C}_{Alice}$, 并上传到交友中心.双线性的安全性在文献[20]中已有详细的证明.

$$\tilde{C}_{Alice}=M\cdot SECRET_{Key}=M\cdot e(g,g)^{\alpha\theta} \tag{7}$$

同时,Alice 提交访问控制策略 T 到 AA 进行管理,AA 将 T 拆分成 K 个子策略,每一个子策略用 $\left(T_{Alice}^{(k)}\right)_{k=1}^{K}$ 表示,并对应 K 个属性管理中心 AA_k.假设属性管理中心 AA_k 上部署的访问子策略为 $T^{(k)}$,那么 $T^{(k)}$ 上 n 个子节点 $x^{(k)}$ 均存在 n 个多项式 q_x 相对应.

(1) 如果 $x^{(k)}$非叶子节点,q_x 的阶(用 d_x 表示)$d_x=k_x-1$,k_x 为节点 x 的门限值.

(2) 如果 $x^{(k)}$为叶子节点,则 $d_x=0$.

(3) 对于其他任意节点 $x^{(k)}$,设 $q_x(0)=q_{parent}(x)(index(x))$,多项式 q_x 的其他参数可以任意选择.

(4) 对于根节点,设 $q_R(0)=\theta,\theta\in Z_p,q_x$ 门限多项式可利用拉格朗日定理设置.

(5) 根据上述(1)~(4)可生成属性中心 $\{AA_1,AA_2,...,AA_k\}$ 上访问控制策略的密文 CT_{Alice}^{k}.

$$CT_{Alice}^{k}=\begin{pmatrix}T^{(k)},C^{(k)}=\left(h_1^{\theta}\right),\overline{C}^{(k)}=\left(h_2^{\theta}\right),\forall y^{(k)}\in Y^{(k)}:C_y^{(k)}=g^{q_{y^{(k)}}(0)}\\ C_y^k=H(att(y^{(k)}))^{q_{y^{(k)}}(0)},\forall x^{(k)}\in X^{(k)}:\hat{C}_x^k=h_2^{q_{x^{(k)}}(0)}\end{pmatrix} \tag{8}$$

$X^{(k)}$为所有非叶子节点 $x^{(k)}$的集合,$Y^{(k)}$为所有叶子节点 $y^{(k)}$的集合.Alice 在执行完所有属性管理中心 $\{AA_1,AA_2,\ldots,AA_k\}$的操作后,可以得到访问总策略 C_{Tree}.

$$C_{Tree}=\left(\left(T_{Alice}^{(k)}\right)_{k=1}^{K},\left(CT_{Alice}^{(k)}\right)_{k=1}^{K}\right) \tag{9}$$

C_{Tree} 由多授权属性管理中心进行保存,方便对其他交友请求用户进行属性匹配.

4.4 用户数据解密阶段

假设用户 Bob 想通过社交交友平台找到具有某一类特征的朋友,那么 Bob 需要设置一组属性集合 $Au_{Bob}^{(k)}$, 并上传到属性管理中心 $\{AA_1,AA_2,\ldots,AA_k\}$ 上用来申请解密密钥 $SECRET_{Key}$.解密密钥 $SECRET_{Key}$ 的计算过程如下.

假设 Alice 在第 k 个属性管理中心 AA_k 的密文为 CT_{Alice}^{k}, Bob 在该 AA_k 上的私钥部件为 $SK_{Bob}^{(k)}$,那么 AA_k 将调用 $Tree(Au_{Bob}^{(k)})$ 来验证 Bob 的私钥部件中的属性 $Au_{Bob}^{(k)}$ 是否满足 $CT_{Alice}^{(k)}$ 中所包含的访问控制策略 $T_{Alice}^{(k)}$, $Tree(Au_{Bob}^{(k)})$ 的递归计算过程如下.

对于访问控制结构中的任意节点 x, $Tree(Au_{Bob}^{(k)})$ 返回一个集合 S_x.如果 $Au_{Bob}^{(k)}$ 不满足 $T_{Alice}^{(k)}$, 则 $Tree(Au_{Bob}^{(k)})=$

⊥,⊥为空集.如果 $Au_{Bob}^{(k)}$ 满足 $T_{Alice}^{(k)}$, 则从集合 $Tree(Au_{Bob}^{(k)})$ 选择一个 $i\in S$,递归地从根节点调用解密节点函数 $DecryptNode(CT_{Alice}^{(k)}, SK_{Bob}^{k}, x, i)$, 函数定义如下.

(1) x 是叶子节点

- 当 $att(x)_{Bob}\notin Au_{Alice\_i}^{k}$ 时, $DecryptNode(CT_{Alice}^{(k)}, SK_{Bob}^{k}, x, i)=\perp$.
- 当 $att(x)_{Bob}\in Au_{Alice\_i}^{k}$, 因为 $H(a_{i,j}^{(k)})$ 是 G 上的元素,因此假设 $H(a_{i,j}^{(k)})=g^{t}$, 则:

$$\left.\begin{aligned} DecryptNode(CT_{Alice}^{(k)}, SK_{Bob}^{k}, x, i) &= e(D_{i,j}^{(k)}, C_x^{(k)})\Big/e(D_{i,j}^{\prime(k)}, C_x^{\prime(k)}) \\ &= e\left(g^{ru_i^{(k)}}\cdot H(a_{Alice_{i,j}}^{(k)})^{ru_{i,j}^{(k)}}, g^{q_{x(0)}}\right)\Big/e\left(g^{ru_{i,j}^{(k)}}, H(att(x^{(k)}))^{q_{x(0)}}\right) \\ &= e\left(g^{ru_i^{(k)}}\cdot H(a_{Alice_{i,j}}^{(k)})^{ru_{i,j}^{(k)}}, g^{q_{x(0)}}\right)\Big/e\left(g^{ru_{i,j}^{(k)}}, H(a_{Bob_{i,j}}^{(k)}))^{q_{x(0)}}\right) \\ &= e\left(g^{ru_i^{(k)}}\cdot H(g^{t})^{ru_{i,j}^{(k)}}, g^{q_{x(0)}}\right)\Big/e\left(g^{ru_{i,j}^{(k)}}, H(g^{t}))^{q_{x(0)}}\right) \\ &= e(g,g)^{ru_i^{k}\cdot q_{x(0)}} \end{aligned}\right\} \tag{10}$$

(2) x 非叶子节点

集合 N_x 由任意 k_x 个节点 x 的子节点构成,假设存在任意子节点 $z\in N_x$.

若 $i\in S_Z$,则调用函数 $DecryptNode(CT_{Alice}^{(k)}, SK_{Bob}^{k}, z, i)$, 返回值保存在 F_Z 中.

若 $i'\in S_Z, i'\neq i$,则调用函数 $DecryptNode(CT_{Alice}^{(k)}, SK_{Bob}^{k}, z, i')$, 返回值保存在 F_Z' 中.

- 若 i=0,可直接计算.

$$F_Z^{(k)}=\frac{e(\hat{C}_z^{(k)}, E_{i'}^{(k)})}{F_Z'}=\frac{e\left(g^{\beta_{k,2}\cdot q_{z(0)}}, g^{\frac{ru^{(k)}+ru_{i'}^{(k)}}{\beta_{k,2}}}\right)}{e(g,g)^{ru_{i'}^{k}\cdot q_{z(0)}}}=e(g,g)^{ru^{(k)}\cdot q_{z(0)}} \tag{11}$$

- 若 $i\neq 0$,需要对节点进行转换.

$$\left.\begin{aligned} F_Z^{(k)} &= e\left(\hat{C}_z^{(k)}, \frac{E_i^{(k)}}{E_{i'}^{(k)}}\right)\cdot F_Z' \\ &= e\left(g^{\beta_{k,2}\cdot q_{z(0)}}, g^{\frac{ru^{(k)}+ru_i^{(k)}-ru^{k}-ru_{i'}^{(k)}}{\beta_{k,2}}}\right)\cdot e(g,g)^{ru_{i'}^{k}\cdot q_{z(0)}} \\ &= e(g,g)^{(ru_i^{(k)}-ru_{i'}^{(k)})\cdot q_{z(0)}}\cdot e(g,g)^{ru_{i'}^{k}\cdot q_{z(0)}} \\ &= e(g,g)^{(ru_i^{(k)})\cdot q_{z(0)}} \end{aligned}\right\} \tag{12}$$

计算完所有 F_z 结果后,利用拉格朗日插值法可以求得: $F_x^{(k)}=\prod_{z\in N_x}F_z^{\Delta iz, S_z'}$, 其中,$iz=index(z)$, $S_z'=(index(z): z\in N_x)$, 拉格朗日系数为

$$\Delta iz, S_z'(0)=\prod_{jz\in S_z', jz\neq iz}\frac{0-jz}{iz-jz} \tag{13}$$

最后利用 $DecryptNode(CT_{Alice}^{(k)}, SK_{Bob}^{k}, x, i)$ 解得节点 x 处的函数值为

$$F_x^{(k)}=\begin{cases}\dfrac{e(g,g)^{ru_i^{(k)}\cdot q_x(0)}, i\neq 0}{e(g,g)^{ru^{(k)}\cdot q_x(0)}, i=0\end{cases} \tag{14}$$

同理,递归计算可得到根节点 R 处的函数值为

$$F_R^{(k)}=\begin{cases}\dfrac{e(g,g)^{ru_i^{(k)}\cdot q_x(0)}=e(g,g)^{ru_i^{(k)}\cdot\theta}, i\neq 0}{e(g,g)^{ru^{(k)}\cdot q_x(0)}=e(g,g)^{ru_i^{(k)}\cdot\theta}, i=0\end{cases} \tag{15}$$

当 $i\neq 0$ 时,对 $F_R^{(k)}$ 进行转换,可求得:

$$F^{(k)}=\frac{e(\hat{C}_r^{(k)},E_i^{(k)})}{F_R^{(k)}}=\frac{e\left(g^{\beta_{k,2}\cdot q_R(0)},g^{\frac{ru^{(k)}+ru_i^{(k)}}{\beta_{k,2}}}\right)}{e(g,g)^{ru_i^{(k)}\cdot q_R(0)}}=e(g,g)^{ru^{(k)}\cdot q_R(0)}=e(g,g)^{ru^{(k)}\cdot\theta} \tag{16}$$

若 K 个访问子策略均能达成匹配,即 $\left(F^{(k)}\right)_{k=1}^{K}\neq\perp$, 则:

$$Q=\prod_{k=1}^{K}\frac{e(C^{(k)},Du^{(k)})}{F^{(k)}}=\prod_{k=1}^{K}\frac{e\left(g^{\beta_{k,1}\cdot\theta},g^{\frac{\alpha u^{(k)}+ru^{(k)}}{\beta_{k,1}}}\right)}{e(g,g)^{ru^{(k)}\cdot\theta}}=\prod_{k=1}^{K}\frac{e(g,g)^{(\alpha u^{(k)}+ru^{(k)})\cdot\theta}}{e(g,g)^{ru^{(k)}\cdot\theta}}=e(g,g)^{\theta\cdot\sum_{k=1}^{K}\alpha u^{(k)}} \tag{17}$$

由此可得解密密钥 $SECRET_{Key}$:

$$SECRET_{Key}=\frac{e\left(\prod_{k=1}^{K}C^{(k)},D_{user}\right)}{Q}=\frac{e\left(g^{\theta\cdot\sum_{k=1}^{K}\beta_{k,1}},g^{\left(\alpha+\sum_{k=1}^{K}\alpha u^{(k)}\right)/\sum_{k=1}^{K}\beta_{k,1}}\right)}{e(g,g)^{\theta\cdot\sum_{k=1}^{K}\alpha u^{(k)}}}=e(g,g)^{\alpha\theta} \tag{18}$$

利用公式(18)得到的密钥 $SECRET_{Key}=e(g,g)^{\alpha\theta}$ 可以解密密文 $\tilde{C}_{Alice}=M\cdot e(g,g)^{\alpha\theta}$, 最终得到明文 M.

$$M=\frac{\tilde{C}}{e(g,g)^{\alpha\theta}}=\frac{M\cdot e(g,g)^{\alpha\theta}}{e(g,g)^{\alpha\theta}}=M \tag{19}$$

当 Bob 成功解密 Alice 在用户交友中心中加密的密文时,Bob 就可以进一步开展与 Alice 进行交友互动和兴趣分享.

5 安全证明

定理 1. 现有密码体制内,如果攻击者在多项式时间内不存在不可忽略的优势来解决 DBDH 难题,则方案可以达到抵抗选择明文攻击下的算法安全性[26].

证明:反证法,假设存在敌手 A 能够以不可忽略的优势 ε 解密密文,则将证明敌手 A 存在不可忽略的优势 $\varepsilon/2$ 可以解决 DBDH 问题.

挑战者 C 选择比特 δ,设置五元组 (g,A,B,C,∂).

$$(g,A,B,C,\partial):=\begin{cases}(g,g^a,g^b,g^c,e(g,g)^{abc}),\ \delta=0\\(g,g^a,g^b,g^c,e(g,g)^z),\ \ \delta=1\end{cases},$$

其中,$a,b,c,z\in Z_p$ 是随机选取的.挑战者 C 随后将元组 (g,A,B,C,∂) 发送给模拟器,后继工作模拟器将模拟挑战者的工作.

(1) 准备阶段

A 任意挑选一个将被挑战的访问控制结构 T^*.

(2) 系统建立阶段

模拟器 C 计算系统公钥 PK_0 和系统主密钥 MK_0,模拟器 C 保留 MK_0,并将 PK_0 发送给敌手 A.

(3) 查询第 1 阶段

敌手 A 根据 $A_1,A_2,...,A_q$ 生成私钥部件,但是私钥部件不满足 T^* 上的访问策略,因此模拟器 C 构造私钥 SK_i,并将私钥 SK_i 发送给敌手 A.

$$SK_i=\left(Du^{(k)}=g^{\frac{\alpha u_{(k)}+ru^{(k)}}{\beta_{k,1}}},D_{i,j}^{(k)}=g^{ru_i^{(k)}}\cdot H(a_{i,j}^{(k)})^{ru_{i,j}^{(k)}},Du_{i,j}'^{k}=g^{ru_{i,j}^{(k)}}\right).$$

(4) 挑战阶段

模拟器 C 接收敌手 A 选择的等长明文消息 M_0 和 M_1,模拟器 C 利用 T^* 加密 $M_\mu(\mu\in\{0,1\})$ 得到密文 CT',并将其发送给敌手 A.

$$CT'=\left(T^*,\tilde{C}=M_\delta\cdot Z,\begin{pmatrix}C^{(k)}=h_{k,1}^{\theta},\bar{C}^{(w)}=h_{k,2}^{\theta},\\ \forall y^{(k)}\in Y^{(k)}:C_y^{(k)}=g^{q_y(0)},C_y'^{(k)}=H(attr(y^{(k)}))^{q_y(0)},\\ \forall x^{(k)}\in X^{(k)}:\hat{C}_x^{(k)}=h_{k,2}^{q_x(0)}\end{pmatrix}_{k=1}^{K}\right)$$

当δ=0 时,可定义 $Z=e(g,g)^{abc}$,设 $c=\theta$,可得:

$\tilde{C}=M_\delta\cdot Z=M_\delta\cdot e(g,g)^{abc}=M_\delta\cdot e(g,g)^{\alpha\theta}$. 因此 CT^*是一个密文.

当δ=1 时,$\tilde{C}=M_\delta\cdot Z=M_\delta\cdot e(g,g)^{z}$, 因为 z 为一个随机数,所以 $\tilde{C}$ 中不包含密文信息.

(5) 查询第 2 阶段

重复查询第 1 阶段的操作.

(6) 猜测阶段

敌手 A 猜测μ',如果 A 猜测正确,即$\mu=\mu'$,模拟器输出 δ'=0,表明获得的是 $e(g,g)^{abc}$ 密文;如果 A 猜测错误,即$\mu\neq\mu'$,模拟器输出δ'=1,表明获得的是随机值 $e(g,g)^{z}$.

在上述游戏中,当δ=1 时,敌手 A 接收的是一个随机值,不能恢复明文.因此,有 $Pr[\mu\neq\mu'\mid\delta=1]=\frac{1}{2}$.

当δ=0 时,敌手 A 将获得密文 M_μ,根据本节定理 1,敌手有不可忽略的优势解密密文 $e(g,g)^{abc}$,所以有

$$Pr[\mu'=\mu\mid\delta=0]=\frac{1}{2}+\varepsilon.$$

因此,在上述 DBDH 游戏中可以正确猜测$\mu=\mu'$的优势为

$$Adv_c=Pr[\mu=\mu']-\frac{1}{2}=\frac{1}{2}Pr[\mu=\mu'\mid\delta=1]+\frac{1}{2}Pr[\mu=\mu'\mid\delta=0]-\frac{1}{2}=\frac{1}{2}\cdot\frac{1}{2}+\frac{1}{2}\cdot\left(\frac{1}{2}+\varepsilon\right)-\frac{1}{2}=\frac{\varepsilon}{2}.$$

综上可证,假如存在敌手 A 能够以ε的概率优势解密密文,则可以得到解决 DBDH 问题概率为 $\frac{\varepsilon}{2}$ 的结论.而该结论与目前已知公认密码学 DBDH 问题难解是相矛盾的.即在多项式时间内不存在一种算法可以有不可忽略的优势解决 DBDH 难题.因此,敌手 A 可以解密密文的假设不成立,即方案可以达到抵抗选择明文攻击下的算法安全性,证毕. □

定理 2. 数据机密性.

交友发起者利用双线性参数 $e(g,g)^{\alpha\theta}$ 加密交友数据明文 M,同时将访问控制策略 T 上传至 AA 上生成访问控制策略密文 $C_{Tree}=\left(\left(T_{Alice}^{(k)}\right)_{k=1}^{K},\left(CT_{Alice}^{(k)}\right)_{k=1}^{K}\right)$, 保证了访问策略 T的安全性;在解密过程中,只有满足访问控制策略的交友请求者才能够获得正确的解密密钥,从而解密数据密文 $\tilde{C}_{Alice}$, 得到对应的明文 M.

定理 3. 密钥安全性.

方案采用了秘密共享机制,将用户的访问控制策略 T 分配给 k 个 AA 进行管理,只有 k 个 AA 进行合作才能将存储在其上的属性子密钥合并为解密总密钥,暴露其中一个 AA 或者多到 k–1 个 AA 份额的子密钥都不会威胁到总密钥的泄漏,因此,方案可以保证最多抵御 k–2 个 AA 合谋时的密钥安全.

6 分析和实验

6.1 交友机会分析

为衡量真实移动社交网络中交友匹配的参与用户,假设时间 t 内出现在发起者周围应答者的人数服从泊松分布$\{N(t),t\geqslant 0\}$,参数为λ,$N_q(t)=n$ 和 $N_{\bar{q}}(t)=m$ 分别表示[0,t]时间段内出现在发起者周围的合格的可信用户和不合格的用户.

定理 4. 假设$\tau(\tau\in[0,t])$时间到达通信区域的任意用户交友匹配概率是 $P(\tau)$.在[0,t]时间内参与交友匹配的预期人数为 $E(N_q(t))=\lambda tp$,其中, $p=\frac{1}{t}\int_0^t p(\tau)\mathrm{d}\tau$.

证明:在[0,t]时间内,假设某一移动社交网络中的总人数为

$$N_q(t)+N_{\bar{q}}(t)=n+m \tag{20}$$

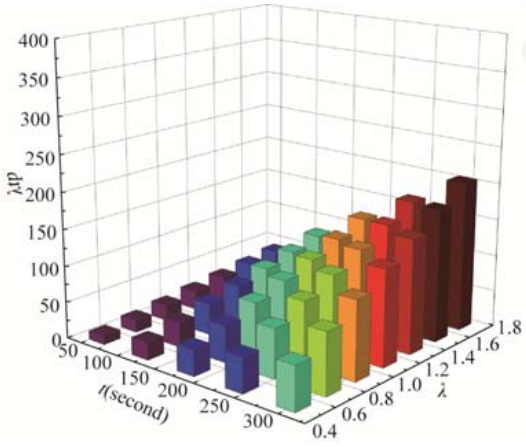
假设单位时间内$\tau\in[0,t]$分布的人数是均匀的,因此,在总人数为 $n+m$ 的条件下,某用户在[0,t]时间段内有意愿参与交友匹配,并且是可信用户的概率为 $p=\frac{1}{t}\int_0^t p(\tau)\mathrm{d}\tau$.同时,因为所有用户到达时间都是独立的,因此可得:

$$\left.\begin{aligned}P\{N_q(t)=n,N_{\bar{q}}(t)=m\}&=P\{N_q(t)=n,N_{\bar{q}}(t)=m\mid N(t)=n+m\}\cdot P\{N(t)=n+m\}\\&=\binom{n+m}{n}p^n(1-p)^m e^{-\lambda t}\frac{(\lambda t)^{n+m}}{(n+m)!}\\&=e^{-\lambda tp}\frac{(\lambda tp)^n}{n!}\cdot e^{-\lambda t(1-p)}\frac{(\lambda t(1-p))^m}{m!}\end{aligned}\right\} \tag{21}$$

由公式(21)可以看出,$N_q(t)$和 $N_{\bar{q}}(t)$ 是分布率分别为λtp 和 $\lambda t(1–p)$的相互独立的泊松分布,因此,在时间[0,t]内到达通信区域参与交友属性匹配的真实人数预期为 $E(N_q(t))=\lambda tp$.

本文进行了模拟实验,从图 3 可以看出,在移动社交活动密集的时刻或者人口密度较高的区域,可以通过降低参与计算应答者的概率 p,做到有效控制参与社交交友参与人数 $E(N_q(t))$.

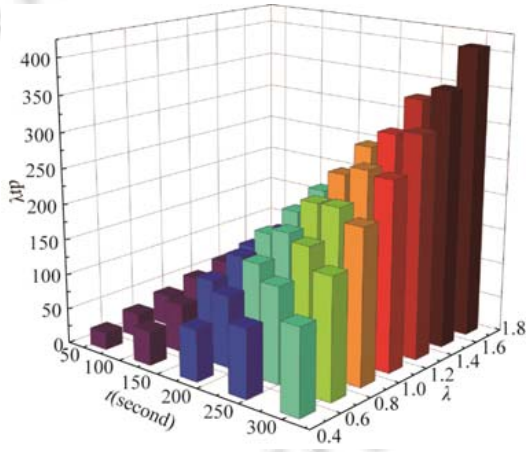
从图 4 可以看出,在移动社交活动稀疏时刻或者人口密度较低的区域,可以通过提高参与计算应答者的概率 p,做到有效增加参与社交交友参与人数 $E(N_q(t))$.



设定阈值为 P=0.4 时,预期愿意参加匹配的应答者人数

Fig.3 Friend matching person number (sparse moment)

图 3 稀疏时刻交友参与匹配人数



设定阈值为 P=0.8 时,预期愿意参加匹配的应答者人数

Fig.4 Friend matching person number (dense moment)

图 4 稠密时刻交友参与匹配人数

6.2 计算复杂度分析

面对移动社交网络大量用户的交友属性匹配问题,需要讨论方案的有效性.假设单授权方案[27]与本文方案的数据结构均按照二叉树结构进行存储,$Au_{Alice}^{(k)}=\left(Au_{Alice_0}^{(k)},Au_{Alice_1}^{(k)},\ldots,Au_{Alice_n}^{(k)}\right)$为 Alice 特征属性的集合,那么传统的单授权方案中心服务器需要承担所有的计算任务,在进行属性匹配的递归遍历时,遍历 $Au_{Alice}^{(k)}$ 中所有节点其计算时间复杂度是 $O(N)$,而在本方案中,$Au_{Alice}^{(k)}$ 中的若干属性组成若干个任务 T 并分布到 k 个属性中心执行,k 个属性中心分担了计算任务,因此,计算时间复杂度为 $O\left(\frac{N}{k}\right)$.显然,我们的计算速度更有优势.

同时,为了进一步比较单授权方案与本文方案的区别,本节将详细分析两种方案中每一阶段的计算开销和通信开销,我们用 $E(G)$和 $E(G_T)$分别表示 G 和 G_T 的幂运算时间,用 B 来表示执行双线性对映射 e:$G\times G\to G_T$ 的时间,T 代表访问控制策略树的叶子节点,$|A|$代表用户属性集合. L_G,L_{G_T},L_{Z_P} 分别表示 G,G_T,Z_P 的长度.

在表 2 中,系统初始化阶段,计算开销恒定为 $5\cdot E(G)+1\cdot E(G_T)+1\cdot B$;密钥生成阶段,密钥生成计算开销由 k 个

AA 共同承担,计算开销为$(k+|A|)\cdot E(G)/k$;加密阶段,可发现,计算开销与属性$|A|$相关,为$(2+3|A|)\cdot E(G)+1\cdot E(G_T)$;解密阶段,解密时间与访问策略 T、用户的属性集合$|A|$以及属性管理中心 AA 的个数 k 紧密相关,其中访问策略 T 的复杂度计算由 k 个 AA 共同承担,因此,计算开销为$(|A|)\cdot B+(T/k)\cdot E(G_T)$.通过以上分析,本方案的计算开销在系统初始化阶段是一个常量,在密钥生成阶段和解密阶段,属性密钥的产生和解密由 k 个 AA 所分担,所以较单授权(单一可信授权中心)方案更有优势.

同样地,在表 3 中,对通信和存储开销进行了分析.系统初始化阶段,系统公钥(PK)和系统主密钥(MK)分别为 $4\cdot L_G+1\cdot L_{G_T}$ 和 $2\cdot L_{Z_p}+L_G$, 私钥长度(SK)和密文长度分别为$(1+3|A|)\cdot L(G)$和$5\cdot|T|\cdot L_G+L_{G_T}$, 与单授权方案的私钥长度$(2+3|A|)\cdot L(G)$和密文长度$1\cdot|A|\cdot L_G+L_{G_T}$ 相比,虽然本方案密文稍长,在一定程度上增加了系统的通信开销,但却降低了系统的工作风险,提高了安全性.

Table 2 Complexity analysis

表 2 计算开销分析

	单授权方案计算开销	本方案计算开销
系统初始化阶段	$1\cdot E(G)+1\cdot E(G_T)+1\cdot B$	$5\cdot E(G)+1\cdot E(G_T)+1\cdot B$
密钥生成阶段	$(2+\|A\|)\cdot E(G)$	$(k+\|A\|)\cdot E(G)$
加密阶段	$\|A\|\cdot E(G)+1\cdot B$	$(2+3\|A\|)\cdot E(G)+1\cdot E(G_T)$
解密阶段	$\|A\|\cdot B+(T)\cdot E(G_T)$	$(\|A\|)\cdot B+(T/k)\cdot E(G_T)$

Table 3 Communication/Storage analysis

表 3 通信开销分析

	单授权方案通信开销	本方案通信开销
系统公钥(PK)	$1\cdot L_{Z_p}+4\cdot L_G+1\cdot L_{G_T}$	$4\cdot L_G+1\cdot L_{G_T}$
系统主密钥(MK)	$1\cdot L_G$	$2\cdot L_{Z_p}+L_G$
用户私钥(SK)	$(2+3\|A\|)\cdot L(G)$	$(1+3\|A\|)\cdot L(G)$
加密密文(CT)	$1\cdot\|A\|\cdot L_G+L_{G_T}$	$5\cdot T\cdot L_G+L_{G_T}$

6.3 实验验证

本文测试环境中利用小米手机 NOTE 版进行群组测试,编程环境为 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 3G 高速内存,支持蓝牙 4.0 和 Wi-Fi 双频,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特征属性,例如对音乐、电影、健身、旅游、购物的兴趣等.根据微博的调查显示,一般情况下,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 50MB 以内,因此,实验假设用户的明文文件固定为 50MB,特征属性从 0~100 依次递增,在初始化时间、密钥生成时间、属性加密和解密时间上与 Chase[28]、Li[29]方案以及单授权方案相比的差异性.

图 5 表明,在相同访问策略下,随着属性数目的递增,初始化时间比较稳定,与单授权方案基本持平,但却比 Chase、Li 方案要小很多,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,而我们采用了更加灵活的分层结构和访问控制策略,减少了双线性计算的次数.因此,在计算开销上更高效.

图 6 反映了随着属性数目的递增,每个属性管理中心产生子密钥的时间变化情况.由于单授权方案是一个属性集合对应生成一个私钥,因此,在密钥生成的计算时间上最小,但是也存在密钥复杂度不高的缺陷.同时,在处理大规模用户属性集合的问题上,存在性能瓶颈和密钥托管不安全等问题.与 Chase、Li 方案相比,我们设计的分层结构中,用户的属性集合被拆分成 k 个子集合,每个 AA 为子集合生成对应的私钥部件,由多个属性中心 AA 共同管理,因此,多个 AA 分担了计算密钥的开销,所以本文的密钥生成时间更有优势.

图 7 反映了随着属性数目的递增,文件加密时间的变化情况.通过对拥有 100 个特征属性的文件进行加密比较,Chase、Li 方案中因为需要验证用户签名,因此,增加了相当大的时间开销,而在我们的设计加密算法中,用户的特征属性集合被划分成 k 个子属性,对应着 k 个下级授权中心,多个属性之间并行工作,因此,加密时间比其

他方案都快,仅需要 1s 左右.

图 8 反映了解密时间的变化情况.单授权方案与本方案因为均需遍历所有的访问控制结构,因此在属性数目较小的情况下(0~40),Chase、Li 方案的计算时间更快,但是随着属性的增加,多属性中心在解密速度上更快,反映了一定的适应性.

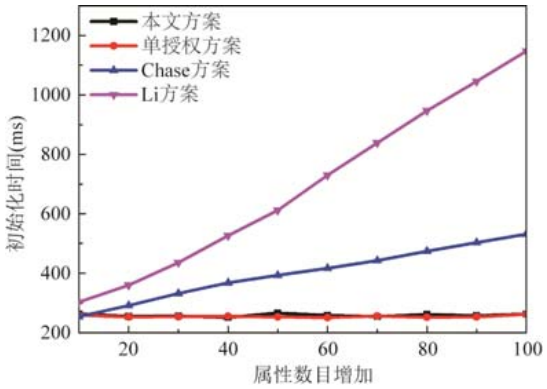


Fig.5 System initialization time (attribute change)

图 5 属性数目递增系统初始化时间图

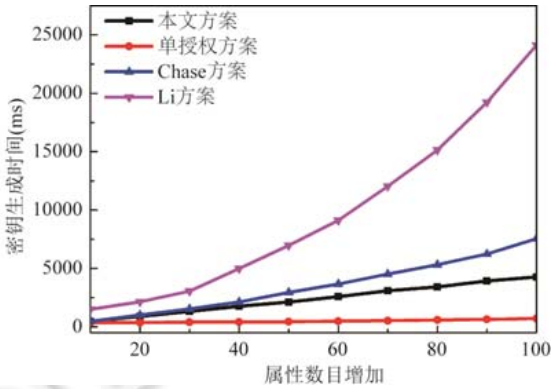


Fig.6 System key generation time (attribute change)

图 6 属性数目递增密钥生成时间图

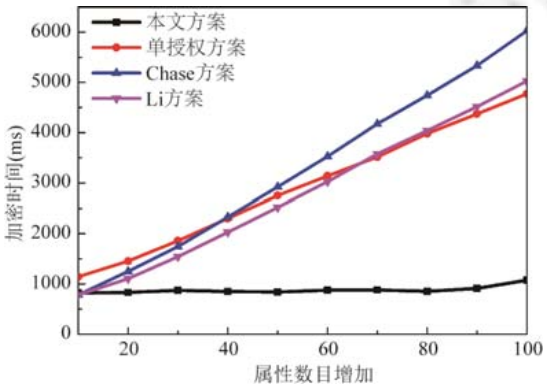


Fig.7 System encryption time (attribute change)

图 7 属性数目递增加密时间图

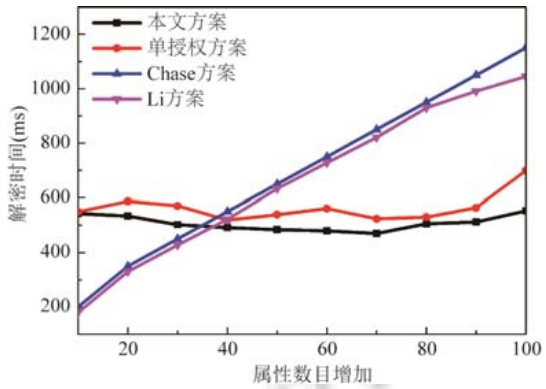


Fig.8 System decryption time (attribute change)

图 8 属性数目递增解密时间图

同时,因为上文中 Chase、Li 方案的计算效率与多授权以及单授权方案相比,差距较大,为了进一步区分与单授权中心计算的差异性并验证第 6.2 节计算开销和通信开销分析的正确性,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 10M~100M 逐渐递增的实验,进行了补充对比.

图 9 说明,在同样属性数目和访问控制策略下,随着文件大小的递增,系统初始化时间基本稳定,与单授权方案持平.

图 10 说明单授权中心在产生密钥的速度上具有优势,这是因为,多授权中心为了解决单授权中心密钥托管的风险问题,子密钥由多个属性中心分别计算,因此时间开销较大.但是多授权中心在加密时间上体现了较大的优越性,如图 11 所示,虽然两者在密钥生成时间上相差 30ms 左右,但在加密时间上却快了 1 000 多 ms,因此,非常适合应用在移动终端的工作环境.

图 12 反映了解密时间的变化情况,解密 100M 的文件在 1.4s 之内,依然有很快的速度,不会影响到用户的实际体验.总的看来,本方案在系统初始化、密钥生成、属性加密和解密的总时间上优于单授权中心方案.

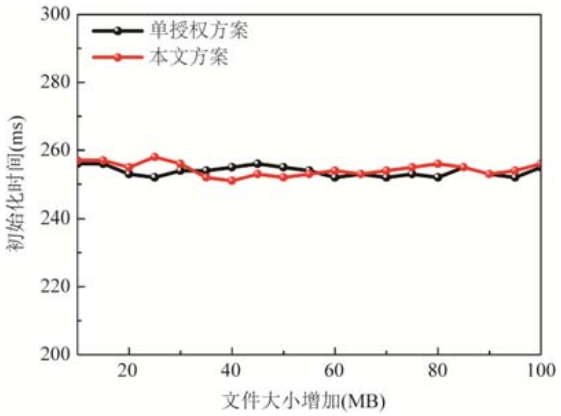


Fig.9 System initialization time (file change)

图 9 文件大小递增初始化时间图

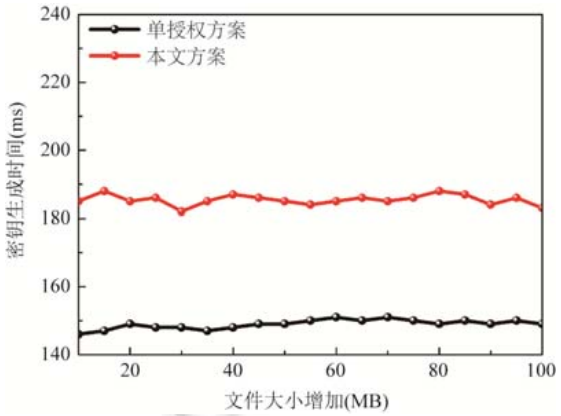


Fig.10 System key generation time (file change)

图 10 文件大小递增密钥生成时间图

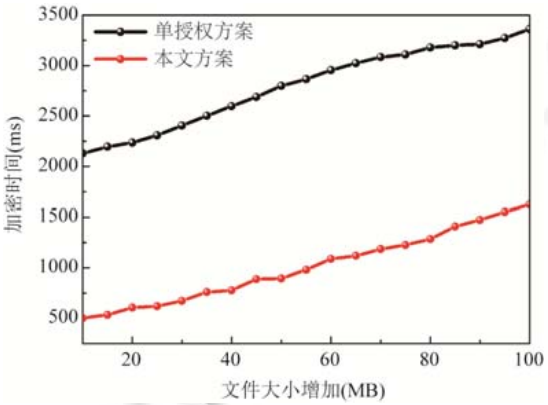


Fig.11 System encryption time (file change)

图 11 文件大小递增加密时间图

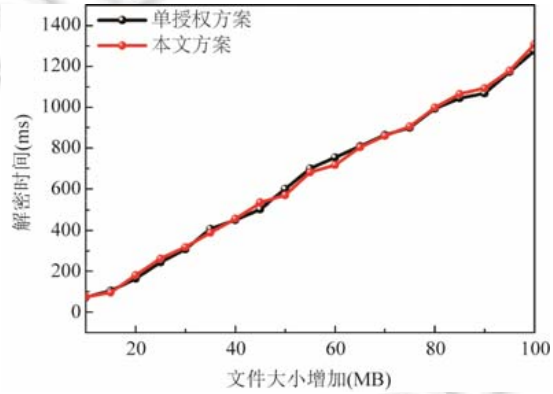


Fig.12 System decryption time (file change)

图 12 文件大小递增解密时间图

最后,我们与其他方案进行了适应性比较.通过比较发现,在我们的方案中,循环群计算次数只应用了一次 p 运算,在访问控制结构上适应多属性的门限方案(AND-gates +/–支持多属性)、通配符计算以及可以隐藏访问控制结构(hidden policy),体现了更好的适应性.见表 4.

Table 4 Comparions among CP-ABE schemes

表 4 与其他 CP-ABE 方案的适应性比较

方案	循环群计算次数	门限方案	通配符	隐藏访问控制策略
Lai, *et al*.[30]	*pqr*	AND-gates +/– on	√	×
Chen, *et al*.[31]	*pqr*	Threshold gates	×	×
Li, *et al*.[32]	*pq*	AND-gates +/– on multi-valued attributes	×	√
本方案	*p*	AND-gates +/– on multi-valued attributes	√	√

7 结束语

在移动社交网络中,用户之间最大化地增强彼此之间的联系和交流,同时又要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.本文基于密码学的研究,提出了多授权中心基于属性的加密方案,该方案提高了移动社交网络中的交友效率,解决了以往单一授权中心的性能瓶颈和密钥管理问题,使得用户能够细粒度地发现与自身设定访问控制策略相匹配的用户,同时可以保证用户交友过程中的隐私不被泄漏.

References:

[1] Fu YY, Zhang M, Feng DG, Chen KQ. Attribute privacy preservation in social networks based on node anatomy. Ruan Jian Xue Bao/Journal of Software, 2014,25(4):768−780 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4565.htm [doi: 10.13328/j.cnki.jos.004565]

[2] Zhang L, Li XY, Liu Y. Message in a sealed bottle: Privacy preserving friending in social networks. IEEE Trans. on Mobile Computing, 2015,14(9):1888−1902. [doi: 10.1109/TMC.2014.2366773]

[3] Wang Y, Vasilakos AV, Jin Q. Survey on mobile social networking in proximity (MSNP): Approaches, challenges and architecture. Wireless Networks, 2013,20(6):1295−1311. [doi :10.1007/s11276-013-0677-7]

[4] Guo L, Zhang C, Sun J. A privacy-preserving attribute-based authentication system for mobile health networks. IEEE Trans. on Mobile Computing, 2014,13(9):1927−1941. [doi: 10.1109/TMC.2013.84]

[5] Guo L, Zhu X, Zhang C. Privacy-Preserving attribute-based friend search in geosocial networks with untrusted servers. In: Proc. of the Int'l Conf. Global Communications Conf. 2013. 629−634. [doi: 10.1109/GLOCOM.2013.6831142]

[6] Lu R, Lin X, Liang X, Shen X. A secure handshake scheme with symptoms-matching for healthcare social network. Mobile Networks and Applications, 2011,16(6):683−694. [doi: 10.1007/s11036-010-0274-2]

[7] Sarpong S, Xu C. A secure and efficient privacy-preserving attribute matchmaking protocol in proximity-based mobile social networks. In: Proc. of the Int'l Conf. Advanced Data Mining and Applications. 2014. 305−318.

[8] Li M, Cao N, Yu S, Lou W. Findu: Privacy-Preserving personal profile matching in mobile social networks. In: Proc. of the Int'l Conf. Computer Communications (INFOCOM). 2011. 2435−2443. [doi: 10.1109/INFCOM.2011.5935065]

[9] Yan Z, Ding W, Niemi V. Two schemes of privacy-preserving trust evaluation. Future Generation Computer Systems, 2015,62(C): 175−189. [doi: 10.1016/j.future.2015.11.006]

[10] Kiraz MS, Genc ZA, Kardas S. Security and efficiency analysis of the Hamming distance computation protocol based on oblivious transfer. Security & Communication Networks, 2015,8(18):4123−4135. [doi: 10.1002/sec.1329]

[11] Ozdemir S, Peng M, Xiao Y. PRDA: Polynomial regression-based privacy-preserving data aggregation for wireless sensor networks. Wireless Communications & Mobile Computing, 2013,15(4):615−628. [doi: 10.1002/wcm.2369]

[12] Zhang R, Zhang J, Zhang Y, Sun J. Privacy-Preserving profile matching for proximity-based mobile social networking. IEEE Journal on Selected Areas in Communications, 2013,31(9):656−668. [doi: 10.1109/JSAC.2013.SUP.0513057]

[13] Niu B, Zhu X, Liu J. Weight-Aware private matching scheme for proximity-based mobile social networks. In: Proc. of the IEEE Global Communications Conf. (GLOBECOM). 2013. 3170−3175. [doi: 10.1109/GLOCOM.2013.6831559]

[14] Zhu X, Chen Z, Chi H. Two-Party and multi-party private matching for proximity-based mobile social networks. In: Proc. of the Int'l Conf. Communications (ICC). 2014. 926−931. [doi: 10.1109/ICC.2014.6883438]

[15] Han J, Susilo W, Mu Y. Privacy-Preserving decentralized key-policy attribute-based encryption. IEEE Trans. on Parallel & Distributed Systems, 2012,23(11):2150−2162. [doi: 10.1109/TPDS.2012.50]

[16] Lewko A, Ostrovsky R, Sahai A, Waters B. Attribute-Based encryption with non-monotonic access structures. In: Proc. of the Int'l Conf. Computer and Communications Security. 2007. 195−203. [doi: 10.1145/1315245.1315270]

[17] Lewko A, Okamoto T, Sahai A, Waters B. Fully secure functional encryption: Attribute-Based encryption and (hierarchical) inner product encryption. In: Proc. of the Int'l Conf. Theory and Applications of Cryptographic Techniques. 2010. 62−91. [doi: 10.1007/978-3-642-13190-5_4]

[18] Lewko A, Okamoto T, Takashima K, Waters B. Fully secure functional encryption with general relations from the decisional linear assumption. In: Proc. of the Int'l Conf.CRYPTO. 2010. 191−208. [doi: 10.1007/978-3-642-14623-7_11]

[19] Waters B. Ciphertext-Policy attribute-based encryption: An expressive, efficient, and provably secure realization. In: Proc. of the Int'l Conf. Practice and Theory in Public Key Cryptography. 2011. 53−70. [doi: 10.1007/978-3-642-19379-8_4]

[20] Bethencourt J, Sahai A, Waters B. Ciphertext-Policy attribute-based encryption. In: Proc. of the Int'l Conf .Symp. on Security and Privacy. 2007. 321−334. [doi: 10.1109/SP.2007.11]

[21] Cheung L, Newport C. Provably secure ciphertext policy ABE. In: Proc. of the Int'l Conf. Computer and Communications Security. 2007. 456−465. [doi: 10.1145/1315245.1315302]

[22] Zhou Z, Huang D, Wang Z. Efficient privacy-preserving ciphertext-policy attribute based-encryption and broadcast encryption. IEEE Trans. on Computers, 2015,64(1):126–138. [doi: 10.1109/TC.2013.200]

[23] Shamir A. How to share a secret. Communications of the ACM, 1979,22(11):612–613. [doi: 10.1145/359168.359176]

[24] Blakley GR. Safeguarding cryptographic keys. In: Proc. of the Int'l Conf. Computer Society. 1979. 313–317. [doi: 10.1109/AFIPS.1979.98]

[25] Cramer R, Shoup V. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In: Proc. of the Int'l Conf. Advances in Cryptology—CRYPTO'98. 1998. 13–25. [doi: 10.1007/BFb0055717]

[26] Wei FS, Zhang G, Ma JF, Ma CG. Privacy-Preserving multi-factor key exchange protocol in the standard model. Ruan Jian Xue Bao/Journal of Software, 2016,27(6):1511–1522 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5001.htm [doi: 10.13328/j.cnki.jos.005001]

[27] Luo E, Wang W, Meng D. A privacy preserving friend discovery strategy using proxy re-encryption in mobile social networks. In: Proc. of the Int'l Conf. Security, Privacy, and Anonymity in Computation, Communication, and Storage. 2016. 190–203. [doi: 10.1007/978-3-319-49148-6_17]

[28] Chase M, Chow SSM. Improving privacy and security in multi-authority attribute-based encryption. In: Proc. of the Int'l Conf. Computer and Communications Security. 2009. 121–130. [doi: 10.1145/1653662.1653678]

[29] Li J, Huang Q, Chen X. Multi-Authority ciphertext-policy attribute-based encryption with accountability. In: Proc. of the Int'l Conf. Symp. on Information, Computer and Communications Security. 2011. 386–390. [doi: 10.1145/1966913.1966964]

[30] Lai J, Deng R, Li Y. Fully secure cipertext-policy hiding CP-ABE. In: Proc. of the Int'l Conf. Information Security Practice and Experience. 2011. 24–39. [doi: 10.1007/978-3-642-21031-0_3]

[31] Chen C, Chen J, Lim HW, Zhang Z, Feng D. Fully secure attribute-based systems with short ciphertexts/signatures and threshold access structures. In: Proc. of the Int'l Conf. Cryptographers Track at the RSA. 2013. 50–60. [doi: 10.1007/978-3-642-36095-4_4]

[32] Li X, Gu D, Ren Y, Ding NK. Efficient ciphertextpolicy attribute based encryption with hidden policy. In: Proc. of the Int'l Conf. Internet and Distributed Computing Systems. 2012. 146–159. [doi: 10.1007/978-3-642-34883-9_12]

附中文参考文献:

[1] 付艳艳,张敏,冯登国,陈开渠.基于节点分割的社交网络属性隐私保护.软件学报,2014,25(4):768–780. http://www.jos.org.cn/1000-9825/4565.htm [doi: 10.13328/j.cnki.jos.004565]

[26] 魏福山,张刚,马建峰,马传贵.标准模型下隐私保护的多因素密钥交换协议.软件学报,2016,27(6):1511–1522. http://www.jos.org.cn/1000-9825/5001.htm [doi: 10.13328/j.cnki.jos.005001]

罗恩韬(1978－),男,湖南永州人,博士,副教授,主要研究领域为移动社交网络隐私保护,云安全,大数据聚类分析.

刘琴(1982－),女,博士,助理教授,CCF 专业会员,主要研究领域为云安全,信息安全,隐私保护.

王国军(1970－),男,博士,教授,博士生导师,CCF 杰出会员,主要研究领域为可信计算,净室安全计算,网络空间安全.

孟大程(1994－),男,硕士,主要研究领域为移动医疗网络隐私保护,大数据安全.