移动社交网络多密钥混淆的交友隐私保护方案研究

罗恩韬[1],陈淑红[2],王文博[3],张少波[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.广州大学计算机科学与教育软件学院,广东广州 510006;
3.加拿大麦特马斯特大学计算机与软件学院,加拿大汉密尔顿 L8R 5G8;4.湖南科技大学计算机与工程学院,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,为保证交友匹配过程中用户的隐私,提出多密钥混淆隐私保护方案.利用代理重加密技术,对用户密钥密文进行重新加密,实现了以扩充交友访问策略条件的交友匹配,并保证密文转换过程中用户的隐私不被泄露;利用随机密文组件加密技术,实现了对真实明文对应加密文件的信息隐藏,提高了攻击者的破解难度;利用数据摘要签名技术,解决了以往方案未考虑的多加密文件对应的文件解密问题.安全和实验分析表明,本文方案可以达到CPA(Chosen Plaintext Attack)安全,可以保证交友用户的隐私不被泄露,并且比既有的方案更有效.

关键词: 多密钥混淆;代理重加密;数据签名;隐私保护
中图分类号: TP393 **文献标识码:** A **文章编号:** 0372-2112 (2018)09-2123-08
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2018.09.012

A Privacy Preserving Friend Discovery Multi Key Obfuscation Scheme in Mobile Social Networks

LUO En-tao[1],CHEN Shu-hong[2],WANG Wen-bo[3],ZHANG Shao-bo[4],PINIAL Khan-butt[5]
(1. *School of Electronics and Information Engineering, Hunan University of Science and Engineering, Yongzhou, Hunan* 425199, *China*;
2. *School of Computer Science and Educational Software, Guangzhou University, Guangzhou, Guangdong* 510006, *China*;
3. *School of Computer Science and Educational Software, Canada McMaster University, Hamilton L8R 5G8, Canada*;
4. *School of Computer and Engineering, Hunan University of Science and Technology, Xiangtan, Hunan* 411101, *China*;
5. *Information Technology Center, Sindh Agriculture University, Tandojam* 70060, *Pakistan*)

Abstract: In mobile social networks, in order to ensure the privacy of users in the process of friend matching, a privacy protection scheme for multiple keys is proposed. Proxy re-encryption technology is utilized to encrypt the user's key into ciphertext, expand friend matching access policy conditions and ensure no leakage of the ciphertext of user privacy during the process of transformation. The employed encryption technology of random ciphertext components can realize the hidden information of the plainntext, and improve the crack difficulty of the attacker. Multiple encrypted files decryption problem is solved by data signature technology, which are not considered by previous works. Security and experimental analysis show that this scheme can achieve CPA(Chosen Plaintext Attack) security, ensure the privacy of friend discovery, and that is more effective than existing solutions.

Key words: multi-key confusion; proxy re-encryption; data signature; privacy-preserving

收稿日期:2016-09-10;修回日期:2017-11-16;责任编辑:孙瑶
基金项目:国家自然科学基金重点资助项目(No.61632009);国家自然科学基金面上资助项目(No.61472451,No.61272151);国家自然科学基金青年资助项目(No.61502163);湖南省自然科学基金2018面上项目(No.2018JJ2147);湖南省自然科学基金青年项目(No.2016JJ3051);湖南省教育厅科研计划(No.2015C0589);湖南省重点研发计划(No.2017NK2390);湖南科技学院计算机应用技术重点建设学科资助(No.128030219-001)

1 引言

1.1 背景介绍

随着移动社交网络(Mobile Social Networks,MSN)和移动智能终端设备的发展[1~4],基于移动社交网络交友应用的应用软件开始普及.在移动社交网络中,用户可以通过分享自己的特征属性信息,例如购物爱好、旅游照片、学习兴趣、锻炼数据等,找到与自己有相同或者相近特征的交友用户.

但是移动社交网络中用户个人隐私在信息共享过程中存在安全泄露隐患,而一旦用户隐私被泄露,将会给人们的生活带来巨大困扰,甚至可能会危害到用户个人财产与生命安全[5].因此,基于移动社交网络的交友匹配与信息共享通常在较为受限的熟人社交网络中进行,用户并不完全放心将自己的个人敏感信息提交到云端进行匹配,应用范围较为有限.

为了进一步促进交友匹配服务在移动社交网络的多元化纵深拓展,如何在提供不受限的交友匹配服务的同时又能够保护用户个人隐私信息安全方案的相关研究,已经是当前移动社交网络交友过程中亟待解决的一个热点问题.

1.2 相关工作

利用加密技术可以对用户隐私信息进行有效的保护.而利用属性私有交集思想(Private Set Intersection,PSI)可以粗粒度的计算用户属性特征的相似度[6~9].后继工作中,Zhang[10]、Niu[11]、Zhu[12]等进一步对用户的属性设置了细粒度的优先级匹配.并且 Zhu 提出利用高效的混淆矩阵变换算法结合内积思想来保护用户的隐私安全.但是,在以上方案中,也存在不足.例如:用户在匹配过程中,无法对用户的属性设置多元的 AND/OR 访问控制权限,因此匹配通常是集合间的属性数目匹配,应用范围相对较为有限.

结合单可信授权中心(Trusted Authority,TA)的属性加密方案[13~19]可以用来保护用户交友过程中用户的安全和隐私,同时也可以解决访问控制权限问题.但是,在此类方案中,用户特征匹配计算都在授权中心服务器上进行.因此在服务高峰期,单可信中心性能瓶颈问题一直难以得到缓解.

为了缓解单可信中心的性能瓶颈问题,Luo 等提出了多授权中心结合属性加密的方案(HMCP)[20],在该方案中,用户密钥与用户属性由多层多个授权中心分别管理,各属性中心分别为属性匹配与消息共享提供细粒度的访问控制,同时方案利用秘密共享思想有效降低了密钥失窃风险,在一定程度上解决了单可信授权中心性能瓶颈问题,同时提高了系统的安全性.但是 HMCP 方案依然存在以下 3 个局限性.

(1)多层次属性中心方案对属性子密钥分别进行管理,虽然降低了密钥失窃风险,但是用户属性需要分别提交到多个属性中心进行匹配,用户属性更新与撤销困难.

(2)多层次属性中心方案考虑的是多个参与者匹配一个发起者设置的交友策略,在实际应用中,有可能出现因发起者设置的交友策略受限,造成有效匹配过低的问题.

(3)多层次属性中心方案将加密文件提交到工作于云端的交友中心,由多个参与者进行匹配,但是该方案仅仅只考虑了在同一域中多个参与者解密单个加密文件的问题,并没有考虑到多个交友发起者在不同域中对不同的加密文件的解密,因此应用性较为单一.

基于以上问题,本文提出一种多密钥混淆交友隐私保护方案,通过跨域密钥共享、代理重加密数据转换、多子密钥混淆加密技术来解决移动社交网络用户交友过程中数据的安全与隐私保护问题.

1.3 本文创新

(1)基于随机多密钥组件安全混淆技术,实现加密密文的多元性,在增强攻击者破解难度的同时,与 HMCP 方案相比,可以更有效的管理用户的属性.

(2)基于代理重加密技术,实现了交友访问控制策略密文的扩展,在提高交友成功率的同时,保证交友过程中密钥密文的安全转换.同时利用重加密密钥与密文隐藏技术,实现了不需要云服务提供商(Cloud Service Provider,CSP)参与数据加密和解密过程,可以有效保护用户的隐私不被泄露.

(3)基于加密文件数据摘要签名技术,解决了以往方案未解决的多加密文件的对应解密问题,更具有普适性.

2 方案模型定义

2.1 系统模型

本文模型主要由以下几部分组成:云端交友中心(Friend Server,FS),负责存储用户加密后的交友敏感数据;可信授权中心(Trusted Authority,TA),负责系统的初始化以及该区域的属性密钥生成、密钥分发等;交友发起用户(Data Owner,DO)加密和指定访问控制策略;属主授权代理用户(Data Proxy,DP)负责对交友信息属主的访问控制结构进行重加密,保证 DO 用户加密后数据文件的安全转换;交友请求用户(Data Requester,DR)负责提交交友请求.

在本文中,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[21~23],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. 本文假设 Alice 为交友发起者,Bob 为属主代理授权用户. Cindy 为交友活动请求者. 交友过程模型图如图 1 所示.

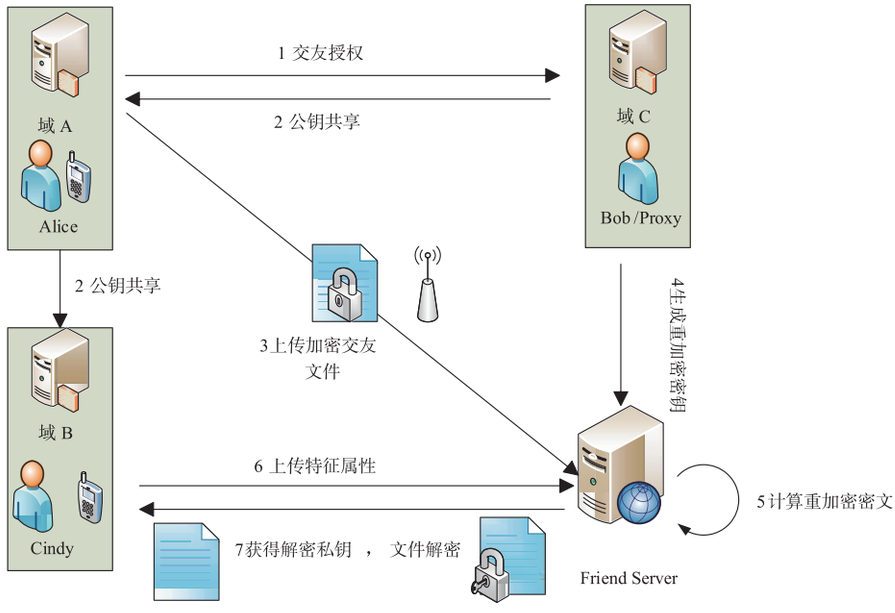


图1　移动社交网络多模式混淆模型匹配过程

2.2　方案设计

本方案包括以下 6 个算法步骤.

假设本方案中(交友用户)属于不同的 N 个域,每个域用 φ_i 表示,$i \in \{1,\cdots,N\}$.

步骤 1　系统密钥生成算法

$$\text{Setup}(1^k, U_{\varphi_i}) \rightarrow (GP, msk_{\varphi_i}, pk_{\varphi_i})$$

U_{φ_i},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_{φ_i},msk_{φ_i} 分别为系统公钥和系统主密钥.

步骤 2　密钥生成算法

$$\text{KeyGen}(GP, msk_{\varphi_i}, S) \rightarrow sk_S$$

输入公共参数 GP,系统主密钥 msk_{φ_i} 和域 φ_i 的属性集 S,输出属性集 S 对应的私钥 sk_S.

步骤 3　加密算法

$$\text{Enc}(m, (M,\rho), pk_{\varphi_i}, GP) \rightarrow CT$$

输入明文 m,交友访问控制策略(M,ρ),系统公钥 pk_{φ_i} 与公共参数 GP,输出可被代理用户重加密的密钥密文 CT.

步骤 4　密钥重加密算法

$$\text{ReKeyGen}(GP, S, sk_s, (M', \rho')) \rightarrow rk_{S\rightarrow(M',\rho')}$$

输入代理用户设置的访问控制策略(M', ρ'),属性集 S,私钥 sk_S 和公共参数 GP,输出重加密密钥 $rk_{S\rightarrow(M',\rho')}$.

步骤 5　密文重加密算法

$$\text{ReEnc}(rk_{S\rightarrow(M',\rho')}, CT) \rightarrow CT'$$

输入重加密密钥 $rk_{S\rightarrow(M',\rho')}$,密钥密文 CT,输出经过重加密的密钥密文 CT'.

步骤 6　文件解密算法

$$\text{Dec}_R(GP, S', SK_{S'}, CT') \rightarrow m$$

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 $S' \models (M', \rho')$,则输出明文 m;否则输出空集 $\perp$.

3　具体方案

3.1　系统初始化阶段

TA 随机选择群 G_1 和 G_2 以及生成元 $g \in G_1$,$a \in \mathbf{Z}_p^*$,其中双线性映射可表示为 $e: G_1 \times G_1 \rightarrow G_2$,生成系统公共参数 GP,哈希函数 H_1, H_2, H_3, H_4, l 为一随机数,其中:

$$H_1: \{0,1\}^* \rightarrow G_1, H_2: \{0,1\}^* \rightarrow Z_p^*,$$
$$H_3: G_2 \rightarrow \{0,1\}^l, H_4: \{0,1\}^* \rightarrow G_1$$
$$GP = (p, g, G_1, G_2, e, H_1, H_2, H_3, H_4) \quad (1)$$

交友信息属主 Alice 选择在任意一个云中的可信授权中心 TA_{φ_i} 上进行注册. 假设本方案交友用户分别属

于不同的的域 D_φ,对于任意一个域 D_{φ_i}的可信授权中心 TA_{φ_i}均可运行 Setup$(1^k,U_{\varphi_i})\rightarrow(GP,msk_{\varphi_i},pk_{\varphi_i})$算法,随机选择 $\alpha_{\varphi_i},x_i,x_j\in Z_p^*$,为交友用户生成域公钥 pk_{φ_i},域主密钥 msk_{φ_i}. 其中,公共参数 GP 和域公钥对外公开,而域主密钥 msk_{φ_i}由工作在该域可信授权中心 TA_{φ_i}保存.

$$\text{Setup}(1^k,U_{\varphi_i})\rightarrow(GP,msk_{\varphi_i},pk_{\varphi_i}),$$
$$msk_{\varphi_i}=g^{\alpha_{\varphi_i}},pk_{\varphi_i}=g^{x_i\alpha_{\varphi_i}} \tag{2}$$

3.2 用户密钥生成阶段

TA_{φ_i}运行 KeyGen$(GP,msk_{\varphi_i},S)\rightarrow sk_S$ 算法,生成该用户唯一的私钥 sk_{φ_i}

$$sk_{\varphi_i}=x_i \tag{3}$$

同理 $sk_{\varphi_j}=x_j,pk_{\varphi_j}=g^{x_j\alpha_{\varphi_j}}$.

TA_{φ_i}通过安全信道将该用户公私钥$(sk_{\varphi_i},pk_{\varphi_i})$以及在 TA_{φ_i}上的签名发送给该用户.

3.3 密文混淆加密阶段

为保证数据明文的安全性,本文采用随机多密钥组件安全混淆技术,实现密文的多元性,增强攻击者破解难度.

Alice 将根据实际应用场景的不同可以建立多个交友文件,每个文件分别使用不同的密钥进行加密,假设 Alice 随机选择一个交友文件,文件编号为 $FID_i,i\in\{1,2,3,\cdots,n\}$,加密 FID_i 对应数据明文 m 得到数据密文 CT_i,那么多密钥加密算法 $Enc(m,pk_{\varphi_i},GP)\rightarrow CT_i$,可拆分为 i,$(i\leqslant 5)$个部分,步骤如下:

$$\begin{aligned}
&CT_i=(CT_1,CT_2,CT_3,CT_4,CT_5)\\
&CT_1=g^r,r=H_2(m\parallel k),k\in G_2\\
&CT_2=ke(pk_{\varphi_i},H_1(pk_{\varphi_i}))^r\\
&CT_3=m\oplus H_3(k)\\
&CT_4=H_1(pk_{\varphi_i})\\
&CT_5=H_4(CT_1\parallel CT_2\parallel CT_3\parallel CT_4)^r
\end{aligned} \tag{4}$$

在对明文 $CT_3=m\oplus H_3(k)$加密成功后,Alice 将$(H_1(FID_i),FID_i,CT_i)$发送给交友中心 FS,FS 接收后,验证数据摘要 $H_1(FID_i)$,若正确,则进行保存.

3.4 代理对密钥密文进行重加密阶段

在该阶段,本方案将引入代理用户,通过代理用户适当拓宽或者灵活修改交友条件(对密文进行重加密),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_i,同时 Bob 将利用自身的访问控制结构 (M',ρ') 对 CT_i 进行重加密.

(1)Bob 输入自身私钥 sk_j 和属性集 S,生成新的访问控制结构为 (M',ρ').

假设 Bob 和 Alice 在不同域中工作. 例如 Bob 属于 D_{φ_j},Alice 属于 D_{φ_i},那么 Bob 将申请域 D_{φ_i}的公钥 pk_{φ_i},计算重加密密钥 $rk_{S\rightarrow(M',\rho')}$:

$$\begin{aligned}
&rk_{S\rightarrow(M',\rho')}=\\
&(pk_{\varphi_i},pk_{\varphi_i}^r,H_1(pk_{\varphi_i}\parallel(M',\rho'))H_1(pk_{\varphi_i})^{sk_j},g^{-r})
\end{aligned} \tag{5}$$

并将重加密密钥 $rk_{S\rightarrow(M',\rho')}$发送给 FS.

(2) FS 收到 $rk_{S\rightarrow(M',\rho')}$后,运行 $ReEnc(rk_{S\rightarrow(M',\rho')},CT_i)\rightarrow CT_i'$算法对 Alice 密钥密文 CT_i 进行重加密得到 CT_i',并计算输出:

$$\begin{aligned}
&CT_i'=(CT_1',CT_2',CT_3',CT_4',CT_5')\\
&CT_1'=CT_1\\
&CT_2'=ke(pk_{\varphi_i},H_1(pk_{\varphi_i}\parallel(M',\rho')))\\
&CT_3'=CT_3\\
&CT_4'=H_1(pk_{\varphi_i})\\
&CT_5=H_4(CT_1'\parallel CT_2'\parallel CT_3'\parallel CT_4')^r
\end{aligned} \tag{6}$$

3.5 文件解密阶段

假如交友请求者 Cindy 向 FS 发起交友查询 FID_i 文件的请求,Cindy 首先要上传自己的交友条件集合 S',若 Cindy 自身属性集合 S'不满足(M,ρ),但是却符合代理用户的条件(M',ρ')时,则 FS 根据 Cindy 提交的属性 S'利用解密算法 $Dec_R(GP,S',SK_{S'},CT_i')\rightarrow m$ 求解数据明文 m,进行更深入的进行交流,解密过程如下.

(1)计算

$$k=\frac{CT_2'}{e(CT_1',H_1(pk_{\varphi_i}\parallel(M',\rho')))^{sk_i}} \tag{7}$$

(2)若可以成功计算

$CT_2'=ke(pk_{\varphi_i}^r,H_1(pk_{\varphi_i}\parallel(M',\rho')))$,$CT_1'=g^r$,则可以利用异或计算得出明文 $m=CT_3'\oplus H_3(k)$.

4 安全性分析

定理 1 假设判定性 q-parallel BDHE 假设在(G_1,G_2)上成立,那么多项式概率时间内不存在敌手 A 能选择 (M^*,ρ^*)访问策略来攻破本方案,即本方案在随机预言模型下可达到抵抗选择明文攻击下的算法安全性.

证明 反证法,假设存在敌手 A 能以 $\varepsilon=Adv_A$ 的优势解决本方案,则本方案将证明存在不可忽略的概率 $\varepsilon/2$ 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(M^*,ρ^*)发送给 C.

(2) 系统建立阶段

假设(M^*,ρ^*)中的属性属于域 φ_i,C 选择 $\alpha_{\varphi_i},\gamma\in\mathbf{Z}_p^*$,同时选择哈希函数 H_1,H_2,H_3,H_4,并发送公共参数 GP 及公钥 pk 给敌手 A.

(3) 查询第 1 阶段

A 向 C 提出询问,C 进行应答.

对于重加密密钥提取询问 $Q_{rk}(S',(M',\rho'))$.

用一个属性集 S' 和一个访问结构(M',ρ')来询问 Q_{rk}. 根据安全游戏,若 S' 不满足(M^*,ρ^*),那 C 先执行 $Q_{sk}(S')$,获得相应的私钥 sk_i,然后计算重加密密钥 $rk_{S\to(M',\rho')}$,并将 $rk_{S\to(M',\rho')}$ 发送给 A. 否则 C 从集合$\{0,1\}$中任意选择 0 或者 1,发送给敌手 A.

(4) 挑战阶段

A 选择等长明文消息 m_0,m_1 发送给 C. C 随机选择比特 $b\in\{0,1\}$ 并利用访问策略(M^*,ρ^*)加密接收到的明文消息 m_b,输出有效密文 CT_i^* 给 A.

(5) 查询第 2 阶段

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 猜测成功;否则 C 得到$(T\in G_1)$.

则 C 成功的概率为:

当输出为 0 时,即 $T\in G_1$,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 $\Pr[b'=b|(y,T)=0]=\frac{1}{2}$.

当输出为 1 时,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 能正确猜测结果有不可忽视的优势 ε,有 $\Pr[b'=b|(y,T=1]=\frac{1}{2}+\varepsilon$.

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

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

综上可证,如果敌手 A 能攻破本文方案的概率为 ε,则解决判定性 q-parallel BDHE 问题的概率为 $\varepsilon/2$. 而这与目前公认密码学 q-parallel BDHE 问题难解是相矛盾的. 因此,敌手 A 可以解密密文的假设不成立,本方案可达到抵抗选择明文攻击下的算法安全性,即 CPA 安全,证毕.

5　实验分析

5.1　计算复杂度分析

在本节的性能对比中,本文忽略 hash 运算,异或操作,因为它们的计算开销远比循环群上的乘法,加法运算,以及双线性对的计算要小. 为简化描述,本文用 $E(G)$ 和 $E(G_1)$ 分别表示 G 和 G_T 的幂运算,B 表示双线性对映射 $e:G\times G\to G_T$,γ 表示访问控制策略树的叶子节点,$|A|$表示用户的属性集合,z 表示 Z_P 上的一次整数运算. L_G,L_{G_T},L_{Z_P} 分别表示 G,G_T,Z_P 的长度. 表 1 为本方案与 HMCP 方案的计算开销与通信开销比较.

表 1　计算开销分析

	本方案计算开销	HMCP[20] 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	z	$(k+\|A\|)\cdot E(G)$
加密阶段	$1\cdot B+8E(G_1)$	$(2+3\|A\|)\cdot E(G)+1\cdot E(G_T)$
解密阶段	$1\cdot B+3E(G_1)$	$(\|A\|)\cdot B+(\gamma)\cdot E(G_T)$

(1) 系统初始化阶段

本方案生成域主密钥 $msk_{\varphi_i}=g^{\alpha_\varphi}$,域公钥 $pk_{\varphi_i}=g^{x\alpha_\varphi}$ 计算开销恒定为 $1\cdot E(G)+1\cdot E(G_T)+1\cdot B$,比 HMCP 方案的的计算开销 $5\cdot E(G)+1\cdot E(G_T)+1\cdot B$ 低.

(2) 密钥生成阶段

本方案的私钥采用了较短的随机数运算 $sk_{\varphi_i}=x_i$,与 HMCP 方案相比,计算开销更小,这是因为 HMCP 方案中,私钥与属性集合 $|A|$ 以及多属性中心紧密相关,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方案高.

(3) 多密钥加密阶段

本方案为了保证加密过程的安全,采用了多密钥安全混淆技术,实现密文的多元性,增强攻击者破解难度,用户的计算开销为 $1\cdot B+8E(G_1)$,比 HMCP 方案稍高;但是值得注意的是,本方案线性计算主要通过代理执行,因此不影响交友发起者的计算效率.

(4) 解密阶段

在本阶段,用户的计算开销为 $1\cdot B+3E(G_1)$,可以发现本方案解密时间计算开销与 HMCP 方案相比更有优势,因此可以获得很快的解密速度.

5.2　通信开销分析

同样地,在表 2 中,本方案进行了通信开销分析. 本方案系统公钥长度为 $1\cdot L_{G_1}$,用户私钥长度为 L_{Z_P},与 HMCP 方案的公钥长度 $4\cdot L_G+1\cdot L_{G_T}$ 和私钥长度$(1+2|A|)\cdot L(G)$相比,本方案的密钥更短,更适合移动计算环境. 本方案加密后的密文长度为 $8L_{G_1}$,比 HMCP 方案 $5\cdot|\gamma|\cdot L_G+L_{G_T}$ 更小. 因此,当用户上传与下载密文文件时,用户可以获得更快的速度与更好的用户

体验.

表 2 通信开销分析

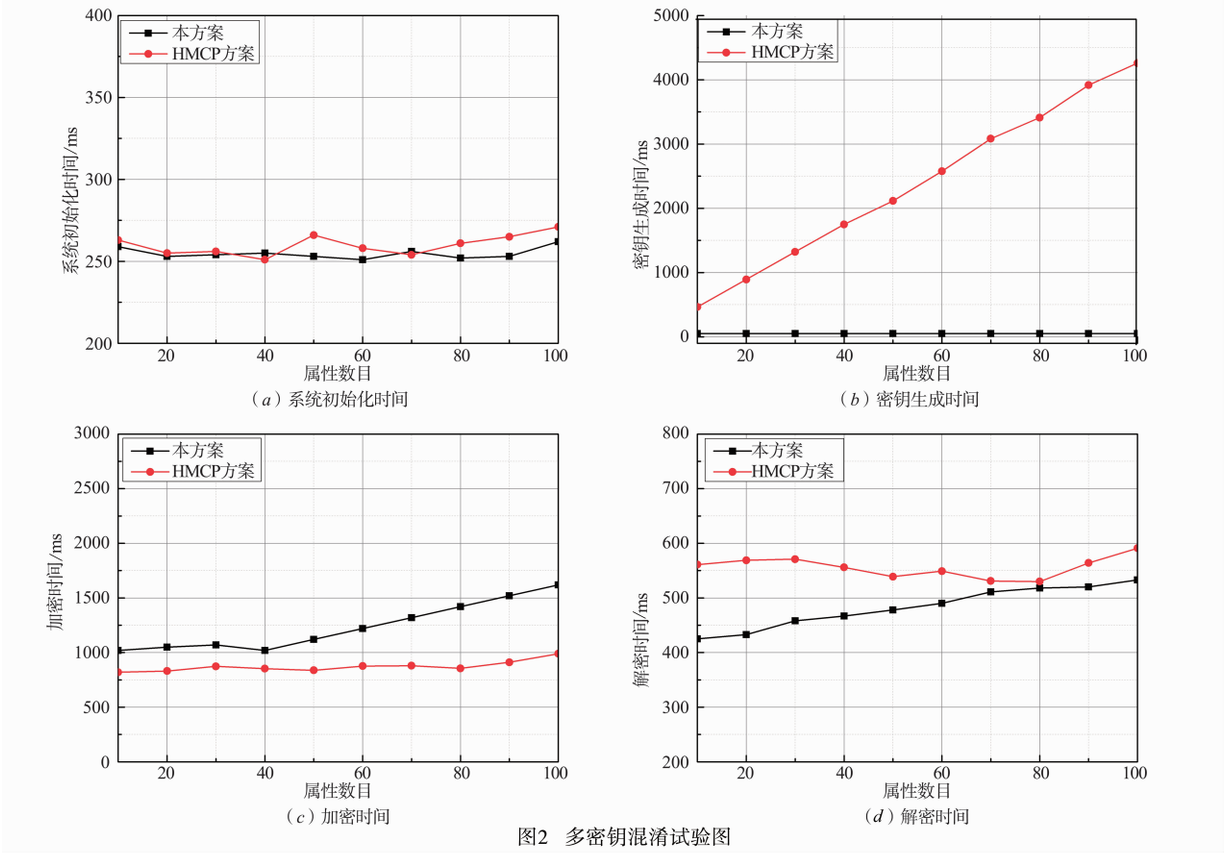
	本方案通信开销	HMCP 方案通信开销
系统公钥(PK)	$1 \cdot L_{G_1}$	$4 \cdot L_G + 1 \cdot L_{G_T}$
系统主密钥(MK)	$1 \cdot L_{G_1}$	$2 \cdot L_{Z_P} + L_G$
用户私钥(SK)	L_{Z_P}	$(1+3\lvert A\rvert) \cdot L(G)$
加密密文(CT)	$8L_{G_1}$	$5 \cdot \lvert\gamma\rvert \cdot L_G + L_{G_T}$

5.3 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 2.5GHz,使用 LPDDR3-933MHz-3G 高速内存,支持蓝牙 4.0 和 Wi-Fi 双频.

本文假设用户的明文文件固定为 50MB,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 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. 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变化情况. 与 HMCP 方案相比,本方案的在计算时间上恒定,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. 在本方案中,对拥有 100 个特征属性的文件加密仅需要 1.5s 左右,比 HMCP 方案加密时间为 1s 稍高,这是因为本方案为保证更安全,增强攻击者破解难度,采用了多子密钥安全混淆技术,实现密文的多元性,因此加密时间稍高. 图 2(d)说明随着属性数目的递增,本方案解密时间的依然比 HMCP 方案低,在保证方案更安全的同时,体现了方案的优越性.



(a) 系统初始化时间 (b) 密钥生成时间

(c) 加密时间 (d) 解密时间

图2 多密钥混淆试验图

6 结束语

本文在基于密码学的研究基础之上,提出了移动社交网络中多密钥交友隐私保护方案. 在交友过程中,利用多密钥技术进行密文隐藏,既提高了对用户属性的灵活性管理,又提高了安全性,解决了交友应用场景局限、交友过少匹配的问题,因此比以往方案更具有普适性.

参考文献

[1] Guo L, Zhang C, Sun J. A privacy-preserving attribute-based authentication system for mobile health networks

[J]. IEEE Transactions on Mobile Computing, 2014, 13(9):1927 – 1941.

[2] Colman-Meixner C, Develder C, Tornatore M. A Survey on resiliency techniques in cloud computing infrastructures and applications[J]. IEEE Communications Surveys & Tutorials, 2016, 18(3):2244 – 2281.

[3] 张涛,马建峰,习宁,等. 面向服务移动社交网络中基于信任的分布式服务组合方法[J]. 电子学报,2016,44(2):258 – 267.
Zhang T, Ma J-F, Xi N, et al. Trust-based decentralized service composition approach in service-oriented mobile social networks[J]. Acta Electronica Sinica, 2016, 44(2): 258 – 267. (in Chinese)

[4] 冯朝胜,秦志光,袁丁,等. 云计算环境下访问控制关键技术[J]. 电子学报,2015,43(2):312 – 319.
Feng C-S, Qing Z-G, Yuan D, et al. Key techniques of access control for cloud computing[J]. Acta Electronica Sinica, 2015, 43(2):312 – 319. (in Chinese)

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

[6] Sarpong S, Xu C. A secure and efficient privacy-preserving attribute matchmaking protocol in proximity-based mobile social networks[A]. Proceedings of Advanced Data Mining and Applications[C]. Berlin: Springer International Publishing, 2014. 305 – 318.

[7] Li M, Cao N, Yu S, Lou W. Findu: Privacy-preserving personal profile matching in mobile social networks[A]. Proceedings of 30th IEEE International Conference on Computer Communications (INFOCOM)[C]. USA: IEEE, 2011. 2435 – 2443.

[8] Yan Z, Ding W, Niemi V. Two Schemes of privacy-preserving trust evaluation[J]. Future Generation Computer Systems, 2015, 62(C):175 – 189.

[9] 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.

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

[11] Niu B, Zhu X, Liu J. Weight-aware private matching scheme for proximity-based mobile social networks[A]. Proceedings of IEEE Global Communications Conference (GLOBECOM)[C]. USA: IEEE, 2013. 3170 – 3175.

[12] Zhu X, Chen Z, Chi H. Two-party and multi-party private matching for proximity-based mobile social networks [A]. Proceedings of IEEE International Conference on Communications (ICC)[C]. USA: IEEE, 2014. 926 – 931.

[13] 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.

[14] Ostrovsky R, Sahai A, Waters B. Attribute-based encryption with non-monotonic access structures[A]. Proceedings of the 14th ACM Conference on Computer and Communications Security[C]. USA: ACM, 2007. 195 – 203.

[15] Lewko A, Okamoto T, Sahai A. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption[A]. Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques[C]. USA: IACR, 2010. 62 – 91.

[16] Tan S F, Samsudin A. Key policy-attribute based fully homomorphic encryption (KP-ABFHE) scheme for securing cloud application in multi-users environment[A]. Proceedings of the 9th International Conference on Robotic, Vision, Signal Processing and Power Applications[C]. Berlin: Springer Singapore, 2017. 77 – 86.

[17] Xu P, Tang Y, Jiang W. Ciphertext-policy attribute-based encryption with short keys[J]. Chinese Journal of Electronics, 2014, 23(4):655 – 660.

[18] 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.

[19] Zhou Z, Huang D, Wang Z. Efficient privacy-preserving ciphertext-policy attribute based-encryption and broadcast encryption[J]. IEEE Transactions on Computers, 2015, 64(1):126 – 138.

[20] 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.

[21] WATERS B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization [A]. Lectnres Notes in Computer Science[C]. Berlin: Springer, 2011, vol 6571. 321 – 334.

[22] 刘梦君,刘树波,等. 基于 LSSS 共享矩阵无授权策略的属性密码解密效率提高方案[J]. 电子学报,2015,43(6):1066 – 1072.
LIU Meng-jun, LIU Shu-bo, et al. Optimizing the decryption efficiency in LSSS matrix-based attribute-based encryption without given policy[J]. Acta Electronica Sini-

ca,2015,43(6):1065 – 1072. (in Chinese)
[23] Cramer R, Shoup V. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack [A]. Proceedings of International Conference on Advances in Cryptology[C] USA:IACR,1998. 13-25.

作者简介

罗恩韬 男. 1978 年生,湖南永州人. 博士、湖南科技学院电子与信息工程学院副教授,主要研究方向为移动社交网络、可信计算、云安全、隐私保护、大数据等.

陈淑红(通讯作者) 女. 1975 年生,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.
E-mail:shuhongchen@ gzhu. edu. cn

王文博 女. 1992 年生,湖南长沙人. 博士,主要研究方向为移动社交网络、隐私保护、信息安全等.

张少波 男. 1979 年生,湖南邵阳人. 博士,主要研究方向为移动社交网络、隐私保护、云计算安全、大数据安全和隐私等.

Pinial Khan Butt 男. 1979 年生,巴基斯坦卡拉奇人. 博士,巴基斯信德省农业大学助理教授,主要研究方向为绿色手机计算,节能计算等.