

可证明安全的社交网络隐私保护方案

何建琼^{1,2,3}, 田有亮^{1,2,3}, 周凯^{1,2,3}

(1. 贵州大学计算机科学与技术学院, 贵州 贵阳 550025;

2. 贵州省公共大数据重点实验室, 贵州 贵阳 550025;

3. 贵州大学密码学与数据安全研究所, 贵州 贵阳 550025)

摘要: 针对社交网络隐私保护方案的安全性证明问题, 提出了一种可证明安全的社交网络隐私保护方案。首先, 通过分析社交网络中节点隐私的安全需求(不可区分的节点结构和不可区分的发送消息), 分别建立其安全模型; 其次, 基于该安全模型运用双线性映射构造社交网络节点隐私保护方案; 最后, 证明了该方案是可证明安全的, 并且分析和对比了该方案的安全性, 分析结果表明, 该方案除了具有可证明安全性外, 还能抵抗再识别攻击、推理攻击和信息聚集攻击。

关键词: 可证明安全; 社交网络; 隐私保护; 双线性映射

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00082

Provably secure social network privacy-preserving scheme

HE Jian-qiong^{1,2,3}, TIAN You-liang^{1,2,3}, ZHOU Kai^{1,2,3}

(1. College of Computer Science and Technology, Guizhou University, Guiyang 550025, China;

2. Guizhou Provincial Key Laboratory of Public Big Data, Guiyang 550025, China;

3. Institute of Cryptography and Data Security, Guizhou University, Guiyang 550025, China)

Abstract: A provable secure social network privacy-preserving scheme was proposed to solve the problem of social network privacy-preserving scheme's security proof. Firstly, through analyzing the security requirements about the node's privacy (indistinguishable node structure and indistinguishable sending messages), the security model were established separately. Secondly, the bilinear mapping was used to construct the social network privacy-preserving scheme. Finally, it was proved that the scheme was provable secure, the security of the schemes were analyzed and compared. The analysis results show that the scheme not only has provable security, but also can resist re-identify attack, inference attack and information aggregation attack.

Key words: provable secure, social network, privacy-preserving, bilinear mapping

1 引言

社交网络的迅速发展, 给社交网络用户的隐私保护带来了严重挑战。人们在享受社交网络提供服务的同时, 个人发布的隐私信息却未

能得到很好的保护, 如果在社交网络发布之前不进行相应的隐私保护, 攻击者就很容易获得用户的隐私信息, 可能会给用户造成一定的经济损失。现有的隐私保护技术主要集中在匿名化技术、泛化技术、随机扰动技术、聚类这几

收稿日期: 2016-04-16; 修回日期: 2016-07-07。通信作者: 田有亮, youliangtian@163.com

基金项目: 国家自然科学基金资助项目(No.61363068); 贵州大学研究生创新基金资助项目(No.2016050)

Foundation Items: The National Natural Science Foundation of China (No.61363068), Graduate Innovation Foundation of Guizhou University (No.2016050)

方面^[1], 尽管应用这些隐私保护技术可以防止攻击者轻而易举获得目标用户的隐私信息, 但是应用这些隐私保护技术后的安全性并没有得到证明。针对隐私保护方案安全性的证明问题, 可以运用可证明安全理论解决。可证明安全理论是从破译密码方案等价于解数学难题的角度间接证明密码方案的安全性, 这将密码方案的安全性最终归结为某个经过深入研究也无法解决的数学难题。

社交网络的隐私信息主要有节点隐私、边隐私和图性质隐私^[2]。本文考虑的节点隐私信息, 目前很多研究者已经做了一些研究。针对节点隐私的保护, 文献[3~5]针对攻击者的背景知识是目标节点的图结构信息, 采用修改图的方式实现节点的隐私保护, 并且分析了匿名后社交网络的有用性。文献[6,7]针对攻击者以目标节点邻接的子图结构为背景信息, 通过泛化顶点标签和扰乱图的结构特征实现隐私保护。文献[8~10]采用顶点进行聚类的匿名技术, 把顶点间结构的差异性隐藏在等价类中。文献[11]考虑到社交网络隐私保护的个性化需求, 提出一种个性化的 (P, α, K) 匿名模型。文献[12]通过增加、删除边以及添加噪声节点的方式, 实现目标节点的属性匿名。文献[13]采用节点分割的隐私属性匿名算法, 通过分割节点的属性连接和关系连接, 提高了节点的匿名性, 降低了目标节点隐私属性泄露的风险。文献[14]提出一种带陷门的属性加密算法, 由属性权威机构与数据属主协同完成用户私钥的生成与分发, 有效降低了数据属主的密钥管理代价, 然后, 通过令牌树机制控制用户对属性陷门的获取, 实现了高效的属性撤销。

当前的研究者较少关心可证明安全理论在社交网络隐私保护中的应用, 未见可证明安全的社交网络隐私保护方案。本文通过分析社交网络中节点隐私保护的安全需求, 建立社交网络节点隐私保护安全模型, 并基于该安全模型运用双线性映射构造社交网络节点隐私保护方案。最后, 证明和分析了该方案的安全性。

2 基础知识

定义 1 双线性映射。

设 G_1 、 G_2 是 2 个相同大素数阶为 q 的群,

其中, G_1 是加法群, G_2 是乘法群。令 P 为 G_1 的任一生成元, aP 记为 a 个 P 相加。若满足下列 3 个性质, 则称映射 $e: G_1 \times G_1 \rightarrow G_2$ 为双线性映射。

1) 双线性。 $\forall P, Q \in G_1$ 和 $a, b \in \mathbb{Z}_q^*$, $e(aP, bQ) = e(P, Q)^{ab}$ 。

2) 非退化性。如果 P 是 G_1 的生成元, 则 $e(P, P)$ 是 G_2 的生成元, 即 $e(P, P) \neq 1$ 。

3) 可计算性。对任何 $\forall P, Q \in G_1$, 都存在有效的算法来计算 $e(P, Q)$ 。

定义 2 询问。

给定一个社交网络 G , 称询问 Q 为攻击者可以用任何背景知识从 G 中获取隐私信息, 询问的结果是顶点集合 V' , 其中 $V' \subseteq V$, V' 中的每个顶点称为一个匹配顶点。

定义 3 结构化攻击。

给定一个已经发布的社交网络 G^* , 如果攻击者对 G^* 发起询问 Q 并获得有限数量的顶点集, 那么目标 x 可能被唯一识别。如果 Q 是基于 G^* 中目标 x 的结构化信息的询问, 这种攻击就称为结构化攻击。

定义 4 访问结构。

令 $\{P_1, P_2, \dots, P_n\}$ 为参与者的集合, 对于聚集 $A \in 2^{\{P_1, P_2, \dots, P_n\}}$, 对 $\forall B, C$: 若 $B \in A$ 且 $B \subseteq C$, 有 $C \in A$, 则称 A 是单调的。访问结构 A 是非空参与者的子集构成的集合。设 D 表示参与者的任一子集, 如果 $D \in A$, 叫做授权集合, 如果 $D \notin A$, 则叫做非授权集合。

定义 5 判定双线性 Diffie-Hellman 指数假设。

根据系统输入的安全参数选择素数阶为 p 的循环群 G 。令 a, s 为 $\mathbb{Z}_q^*$ 上随机选择的参数, g 为群 G 的生成元。当 $y = (g, g^a, \dots, g^{a^q}, g^{a^{q+2}}, \dots, g^{a^{2q}}, g^s)$ 给敌手, 敌手必须可以将 $e(g, g)^{a^{q+1}s} \in G$ 与 G 中的任意一个元素进行区分。

模拟器 B 以优势在 G 中解决 DBDHE 问题并输出, 若

$$\left| \Pr \left[B(y, T = e(g, g)^{a^{q+1}s}) = 0 \right] - \Pr \left[B(y, T = R) = 0 \right] \right| \geq \varepsilon$$

且没有多项式时间的算法以不可忽略的优势解决 DBDHE 问题, 则称 DBDHE 假设成立。

3 节点隐私保护算法框架与安全模型

本文把社交网络建模为一个无向无标签的图，图模型为 $G=(V,E)$ ，其中， V 是图 G 的顶点集合， E 是图 G 的边集合。本节通过对社交网络节点隐私保护的安全需求分析，形式化社交网络节点隐私保护安全需求，构建社交网络节点隐私保护安全模型。

3.1 算法框架

节点隐私保护的安全需求：不可区分的节点结构和不可区分的发送消息。节点隐私保护算法采用 KM 算法^[5]对节点进行匿名，实现不可区分的节点结构；用基于密文策略属性基加密^[15]对节点发送的消息进行加密，实现不可区分的发送消息。因此，本节提出的节点隐私保护方案

(NPPS, node privacy-preserving scheme) 包含 5 个算法：节点匿名 (NodeAnony) 算法、初始化 (Setup) 算法、加密 (Encrypt) 算法、密钥生成 (KeyGen) 算法、解密 (Decrypt) 算法，算法的功能描述如下。

1) $NodeAnony(G, k)$ 算法：输入社交网络图 G 、参数 k ，对 G 采用 KM 算法后生成图 G^* ，输出图 G^* 。

2) $Setup(1^k, G^*)$ 算法：输入系统安全参数 k 和发布后的社交网络图 G^* ，生成公钥 PK 和主密钥 MK 。

3) $Encrypt(PK, M, A)$ 算法：输入系统公钥 PK 、消息 M 和访问结构 A ，用公钥 PK 加密消息 M ，生成密文 CT ，其中，密文中包含了访问结构 A 。只有当用户具有的属性集满足访问结构时，才能正确解密消息。

4) $KeyGen(MK, S)$ 算法：输出系统主密钥 MK 和用户属性集 S ，生成私钥 sk 。

5) $Decrypt(sk, CT)$ 算法：输入私钥 sk 和密文 CT ，当私钥中包含的属性基 S 满足密文访问结构 A 时，就能正确解密恢复出消息 M 。

3.2 安全模型

本节给出节点隐私保护的标准模型来抵御节点结构攻击和发送消息攻击，下面通过 2 个实验来说明这 2 个安全需求，如图 1 和图 2 所示。

在图 1、图 2 的实验中， O_K 、 O_E 代表密钥

生成 Oracle 和加密 Oracle， $Q(x)$ 表示敌手对目标节点 x 进行结构化查询， $D(x)$ 表示敌手通过获取目标节点 x 发送的消息为背景知识进行目标节点身份的推断。图 1 实验关注的是不可区分的节点结构，采用节点匿名算法的安全概念 IND-NPPS-CNA，如果该实验以不可忽略的概率返回 1，则敌手 $\mathcal{A}$ 胜利。图 2 实验关注的是不可区分的发送消息，采用基于密文策略属性基加密方案的安全概念 IND-NPPS-CSMA，若该实验以不可忽略的概率返回 1，则敌手 $\mathcal{A}$ 胜利。

$$Exp_{NPPS, \mathcal{A}}^{IND-CNA}(G, k)$$

$$G^* \leftarrow NodeAnony(G, k)$$

$$(V_1, V_2, \dots, V_k) \leftarrow A_1^{Q(x)}(G^*, X)$$

$$k \leftarrow A_2(V_1, V_2, \dots, V_k)$$
 如果 $k=1$ ，则返回 1，否则返回 0

图 1 不可区分的节点结构的安全模型

$$Exp_{NPPS, \mathcal{A}}^{IND-CSMA}(1^k)$$

$$(PK, MK) \leftarrow Setup(1^k, G)$$

$$(sk_s) \leftarrow KeyGen(MK, S_s)$$

$$(sk_r) \leftarrow KeyGen(MK, S_r)$$

$$(M_0, M_1) \leftarrow A_1^{O_K, O_E}(S_s, S_r)$$

$$b \leftarrow \{0, 1\}$$

$$CT \leftarrow Encrypt(PK, M_b, A)$$

$$S_b \leftarrow A_2^{D(x)}(CT, M_0, M_1)$$
 如果 $b=S_b$ ，则返回 1，否则返回 0

图 2 不可区分的发送消息的安全模型

接下来，定义敌手 $\mathcal{A}$ 在 IND-NPPS-CNA 安全性概念下攻破社交网络节点隐私保护方案的优势为 $A_{adv} = \Pr[k=1]$ 。

定义 6 当敌手 $\mathcal{A}$ 攻击能力和查询 Oracle 的次数是关于 ϵ 多项式界定时，如果攻击该 NPPS 方案成功的优势是关于 ϵ 可忽略的，则称这个社交网络节点隐私保护方案是 IND-NPPS-CNA 安全的。

定义敌手 $\mathcal{A}$ 在 IND-NPPS-CSMA 安全性概念下攻破社交网络节点隐私保护方案的优势为 $A_{adv} = \Pr[Exp_{NPPS, \mathcal{A}}^{IND-CSMA}(1^k) = 1]$ 。

定义 7 当敌手 $\mathcal{A}$ 攻击能力和查询 Oracle 的次数是关于 ϵ 多项式界定的，如果攻击该方案成功的优势是关于 ϵ 可忽略的，则称这个社交网络节点隐私保护方案是 IND-NPPS-CSMA 安全的。

4 方案构造

基于以上安全模型，构建如下方案。

1) $NodeAnony(G, k)$ ：输入社交网络图 G 和

参数 k , 通过朴素匿名后转变为 G' 图。把 G' 划分为 n 个块并且把这些块聚类为 m 个组 $U_1, \dots, U_m$, 每个 U_i 至少有 k 个块 P_{ij} ($i=1, \dots, m, j=1, \dots, k_i, k_i \geq k$)。对每个 U_i 中的所有块 P_{ij} 执行图对齐后得到 P'_{ij} , 用对齐后的块 P'_{ij} 替换块 P_{ij} 得到图 G'' 。对所有的交叉边执行边复制, 得到 k -自同构社交网络图 G^* , 输出图 G^* 。

2) *Setup*($1^k, G^*$): 输入系统的安全参数 1^k 和发布后的社交网络图 G^* , 选取 2 个阶为 q 的加法群 G_1 , 乘法群 G_2 , g 为 G_1 的任一生元, $e: G_1 \times G_1 \rightarrow G_2$ 是双线性映射, 随机选取 $a \in Z_q^*$, 计算 $g_1 = g^a$, 随机选择一个长度为 n 的行向量 $U = (u_i)$, 其中, $u_i \in G_1$ ($1 \leq i \leq n$), 则公钥 $PK = \{g, e(g, g)^a\}$, 主密钥 $MK = \{g_1, U\}$ 。

3) *Encrypt*(PK, M, A): 输入公钥 PK 、消息 M 和访问结构 $A = (n_i)$ ($n_i \in G_1, 1 \leq i \leq n$), 计算 $w = U^T A$ (其中, U^T 是行向量 U 的转置), 随机选择 $s \in Z_q^*$, 公布 $CT = \{C = Me(g, g)^{as}, C^* = g^s, C' = g^{ws}\}$ 。

4) *KeyGen*(MK, S): 输入主密钥 MK 和用户的身份 $S = (d_i)$, 其中, $d_i \in G_1$ ($1 \leq i \leq n$), 随机选取 $t \in Z_q^*$, 然后计算私钥

$$sk = \left\{ D_1 = g^a \left(g^{\sum_1^n u_i d_i} \right)^t, D_2 = g^t \right\}.$$

5) *Decrypt*(sk, CT): 输入匿名后的节点 CT 、用户的私钥 sk , 如果用户的属性 S 满足访问结构 A , 即当 $\sum_1^n u_i d_i = w$ 时, 则可计算 $T = \frac{e(C^*, D_1)}{e(C', D_2)} =$

$$\frac{e\left(g^s, g^a \left(g^{\sum_1^n u_i d_i} \right)^t\right)}{e(g^{ws}, g^t)} = e(g, g)^{as}, \text{ 通过 } S \text{ 可以解匿}$$

名 C 得到消息 $M = \frac{C}{T}$ 。

5 安全性证明

定理 1 假定 DBDHE 假设成立, 那么没有多项式时间的敌手以目标节点的图结构信息和发送的消息来选择性攻击本文系统。

证明 假设敌手 $\mathcal{A}$ 有不可忽略的优势 ε 攻破本文方案。构建一个模拟器 B , 模拟器 B 输入

DBDHE 挑战 $y = (g, g^a, \dots, g^{a^{q+2}}, \dots, g^{a^{2q}})$ 和 T 。敌手将挑战结构 $A^* = (n_i^*)$ ($1 \leq i \leq n^*$) 输入算法中, 其中, $n^* \leq q$ 。

1) 节点匿名算法: 输入社交网络图 G 和参数, 通过朴素匿名转变为图 G' 。把 G' 划分为 n 个块并且把这些块聚类为 m 个组 $U_1, \dots, U_m$, 每个 U_i 至少有 k 个块 P_{ij} ($i=1, \dots, m, j=1, \dots, k_i, k_i \geq k$)。对每个 U_i 中的所有块 P_{ij} 执行图对齐后得到 P'_{ij} , 用对齐后的块 P'_{ij} 替换块得到图 G'' 。对所有的交叉边执行边复制, 得到 k -自同构社交网络图 G^* , 输出图 G^* 。

阶段 1 这个阶段敌手 $\mathcal{A}$ 以目标节点 x 的图结构信息为背景知识, 对发布的图 G^* 进行结构化查询 Q , 由于图 G^* 是一个自同构的图, 所以 $\forall x \in G^*, Q(x) = \{V_1, \dots, V_k\}, V_i \in V^*, i=1, \dots, k$, 则敌手 $\mathcal{A}$ 识别出目标节点 x 的概率为 $\frac{1}{k}$ 。

2) 初始化算法: 模拟器 B 在 Z_q^* 上随机地选择元素 a' , 并且令 $a = a' + a^{q+1}$, 则有 $e(g, g)^a = e(g^a, g^{a'})e(g, g)^{aa'}$ 。另外, 用模拟器 B 来模拟随机行向量 $U' = (u'_i)$, 其中, $u'_i \in G_1$ ($1 \leq i \leq n^*$), u'_i 随机从 Z_q^* 中选取。

阶段 2 这个阶段, 模拟器 B 模拟生成私钥。假定模拟器被给予一个对与用户身份的集合 S 相对应的私钥的询问, 其中, S 不满足访问结构 A^* 。模拟器 B 随机选取 $r \in Z_q^*$, 定义

$$t = r + u'_1 a^q + u'_2 a^{q-1} + \dots + u'_{n^*} a^{q-n^*+1}$$

那么

$$S_1 = g^a \left(g^{\sum_1^n u_i d_i} \right)^t = g^{a'} \left(g^{\sum_1^n u_i d_i} \right)^{r + \sum_1^n u'_i a^{q-i+1}}$$

$$S_2 = g^t = g^r \prod_{i=1, \dots, n^*} (a^{q-i+1})^{u'_i}$$

挑战: 敌手 $\mathcal{A}$ 将 2 个消息 M_0, M_1 给模拟器。模拟器通过抛掷硬币的方式选取 $b \leftarrow \{0, 1\}$, 产生 $C = M_b e(g, g)^{as} = M_b Te(g, g)^{a's}, C^* = g^s$ 。使用模拟器 B 来模拟 $C' = g^{ws}$, 用 $U' = (u'_i)$, 其中 $u'_i \in G_1$ ($1 \leq i \leq n^*$) 来模拟随机行向量, 则 $C' = g^{\left(\sum_1^n u'_i n_i^* \right)^s}$ 。

阶段3 与阶段2相同。

猜测: 敌手最终输出猜测 b' 。若 $b = b'$, 模拟器 B 输出 0 并且回答 $T = e(g, g)^{a^{q+1}}$, 否则, 模拟器输出 1 并且回答 G 中的一个随机值。当 T 是 DBDHE 元组时, $\Pr[B(y, T = e(g, g)^{a^{q+1}}) = 0] = \frac{1}{2} + A_{\text{adv}}$, 当 T 是随机时, $\Pr[B(y, T = R) = 0] = \frac{1}{2}$ 。由于敌手 $\mathcal{A}$ 以不可忽略的优势攻破方案, 那么 B 也以不可忽略的优势来模拟 DBDHE 游戏。

6 方案分析

下面将本文提出的社交网络隐私保护方案与现有的方案进行比较。表1给出了各种方案间安全性的比较, 其中“√”表示满足该安全性, “×”表示不满足该安全性。

从表1可以看出, 文献[5,8,9,13]提出的方案只能抵抗基于属性的再识别攻击和基于结构的再识别攻击, 而不能抵抗推理攻击和信息聚集攻击, 也未能证明其具备可证明安全性。相比已有的社交网络隐私保护方案, 本文提出的方案采用 KM 算法对节点进行匿名, 实现不可区分的节点结构, 用基于密文策略属性基加密对发送的消息进行加密, 实现不可区分的发送消息, 从而能抵抗再识别攻击、推理攻击和信息聚集攻击。此外, 本文运用可证明安全理论对方案的安全性进行了证明, 使方案具有可证明安全性。

7 结束语

本文研究了社交网络节点隐私保护的可证明安全问题, 并建立社交网络节点隐私保护安全模型, 基于该模型, 提出可证明安全的社交网络隐私保护方案。该方案通过用匿名算法实现节点身份的隐藏和图结构的匿名, 防止敌手

基于目标节点的结构化攻击。同时, 采用基于密文策略属性基加密实现对节点发送消息的加密, 防止敌手基于目标节点发送的消息推理出目标节点的身份信息。最后, 证明和分析该方案的安全性。

参考文献:

- [1] BHAGAT S, CORMODE G, KRISHNAMURTHY B, et al. Class-based graph anonymization for social network data[EB/OL]. <http://www.vldb.org/pvldb/2/vldb09-pvldb26.pdf>.
- [2] 刘向宇, 王斌, 杨晓春. 社会网络数据发布隐私保护技术综述[J]. 软件学报, 2014, 25(3):576-590.
LIU X Y, WANG B, YANG X C. Social network data privacy protection technology review [J]. Journal of Software, 2014, 25 (3) : 576-590.
- [3] HAY M, MIKLAU G, JENSEN D, et al. Anonymizing social networks[R]. University of Massachusetts, 2007.
- [4] LIU K, TERZI E. Towards identity anonymization on graphs[C]//The ACM Sigmod International Conference on Management of Data. c2008.
- [5] ZOU L, CHEN L. K-automorphism: a general framework for privacy preserving network publication [C]//The 35th International Conference on Very Large Data Base. c2009:946-957.
- [6] ZHOU B, PEI J. Preserving privacy in social networks against neighborhood attacks[C]//The 24th IEEE International Conference on Data Engineering (ICDE). c2008.
- [7] 宋喜忠, 刘康明. 基于 k -subgrap 算法的社交网络隐私保护研究[J]. 科技通报, 2015 (1):155-157.
SONG X Z, LIU K M. Social network privacy protection study based on k -subgrap algorithm[J]. Bulletin Science and Technology, 2015 (1) : 155-157.
- [8] HAY M, MIKLAU G, JENSEN D, et al. Resisting structural re-identification in anonymized social networks [J]. VLDB Journal, 2010, 19(6): 797-823.
- [9] 韦伟, 李杨, 张为群. 一种基于 GSNPP 算法的社交网络隐私保护方法研究[J]. 计算机科学, 2012, 39(3):104-106.
WEI W, LI Y, ZHANG W Q. A GSNPP algorithm based on the social network privacy protection method research[J]. Journal of Computer Science, 2012, 39 (3): 104-106.

表1 社交网络隐私保护方案安全性比较

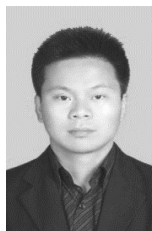
方案	再识别攻击	推理攻击	信息聚集攻击	可证明安全
文献[5]方案	√	×	×	×
文献[8]方案	√	×	×	×
文献[9]方案	√	×	×	×
文献[13]方案	√	×	×	×
本文方案	√	√	√	√

- [10] THOMPSON B, YAO D F. The union-split algorithm and cluster-based anonymization of social networks [C]//The 4th International Symposium on Information, Computer, and Communications Security. c2013:218-227.
- [11] 孔庆江. 社交网络中个人信息与人际关系的隐私保护研究[D]. 杭州: 浙江工业大学, 2011.
- KONG Q J. Personal information and relationships in the social network privacy protection research[D]. Hangzhou: Zhejiang University of Technology, 2011.
- [12] YUAN M X, CHEN L, YU PS, YU T. Protecting sensitive labels in social network data anonymization[J]. IEEE Transactions on Knowledge and Data Engineering, 2013, 25(3):633-647.
- [13] 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, 4: 768-780.
- FU Y Y, ZHANG M, FENG D G, et al. Social network privacy protection based on the node split attributes[J]. Journal of Software, 2014, 4:68-780.
- [14] 吕志泉, 洪澄, 张敏, 等. 面向社交网络的隐私保护方案[J]. 通信学报, 2014, 35(8): 23-32.
- LV Z Q, HONG C, ZHANG M, et al. Privacy protection scheme for social network [J]. Journal on Communications, 2014, 35 (8): 23-32.
- [15] LING C, NEWPORT C. Provably secure ciphertext policy ABE[C]//The 14th ACM Conference on Computer and Communications Security. c2007: 456-465.

作者简介:



何建琼 (1991-), 女, 贵州遵义人, 贵州大学硕士生, 主要研究方向为密码学与安全协议。



田有亮 (1982-), 男, 贵州盘县人, 博士, 贵州大学教授, 主要研究方向为博弈论、密码学与安全协议。



周凯 (1991-), 男, 浙江衢州人, 贵州大学硕士生, 主要研究方向为密码学与可信计算。

《网络与信息安全学报》2016 年第 7 期刊登的《面向差分调制解调的编码码率研究》一文通信作者徐亚冲邮箱 chongge006@163.com 已停用, 现更新为: 18633018050@wo.cn, 特此说明。