DOI:10.7544/issn1000-1239.2018.20161043
55(4):846-853,2018

支持隐私保护的多机构属性基加密方案

闫玺玺[1] 刘 媛[1] 李子臣[2] 汤永利[1]
[1](河南理工大学计算机科学与技术学院 河南焦作 454003)
[2](北京印刷学院信息工程学院 北京 102600)
(yanxx@hpu.edu.cn)

Multi-Authority Attribute-Based Encryption Scheme with Privacy Protection

Yan Xixi[1], Liu Yuan[1], Li Zichen[2], and Tang Yongli[1]
[1](*School of Computer Science and Technology, Henan Polytechnic University, Jiaozuo, Henan* 454003)
[2](*School of Information Engineering, Beijing Institute of Graphic Communication, Beijing* 102600)

Abstract Attribute based encryption (ABE) is a new cryptographic technique which guarantees fine-grained access control of outsourced encrypted data in the cloud. In order to protect the users' sensitive information in the cloud, a multi-authority attribute based encryption (MA-ABE) scheme with privacy protection is proposed. In the scheme, the users' attribute is divided into two parts: the attribute name and the attribute value. The value of user's attributes would be hidden in the access structure to prevent from revealing to any third parties, so the users' privacy will be effectively preserved. In addition, the attribute name is used to construct the access structure, and the length of our ciphertext is associated with the number of attribute name which belongs to the access policy, rather than the all attributes in the system. Besides, the scheme is secure against chosen plaintext attack under the decision bilinear Diffie-Hellman (DBDH) assumption in the standard model. Compared with the existing related schemes, the size of ciphertext and users' secret key in the scheme are all reduced, and the lower computing cost and storage cost makes the scheme more effective in the practical application, especially the condition in which the scale of user attributes is far smaller than the scale of system attributes.

Key words multi-authority; privacy protection; attribute based encryption (ABE); attribute hidden; standard model

摘 要 针对云环境中用户敏感信息的保护,提出一种支持隐私保护的多机构属性基加密(attribute based encryption, ABE)方案.该方案采用半策略隐藏方式,将属性分为属性名和属性值2部分,通过对用户的属性值进行隐藏,实现对用户的隐私保护,避免用户的具体属性值泄露给其他任何第三方.另外,加密时仅对与访问策略相关的属性名进行加密,而不是对系统所有属性进行加密,改变了已有的隐私保护属性基加密方式,大大减短了密文长度.方案的安全性依赖于DBDH假设,并且在标准模型下满足自适应选择明文攻击安全.同时,通过与其他方案的对比,方案计算代价和存储代价都有明显优势,尤其是

收稿日期:2016-12-27;**修回日期**:2017-08-09
基金项目:"十三五"国家密码发展基金项目(MMJJ20170122);河南省科技厅项目(142300410147);河南省教育厅科研项目(12A520021,16A520013);河南理工大学2015年青年骨干教师资助项目
This work was supported by the "13th Five-Year" National Crypto Development Foundation (MMJJ20170122), the Project of Science and Technology Department of Henan Province (142300410147), the Project of Education Department of Henan Province (12A520021, 16A520013), and the Research Fund for Young Backbone Teachers of Henan Polytechnic University in 2015.
通信作者:汤永利(yltang@hpu.edu.cn)

密文长度仅与访问策略设置的属性相关,更加适用于实际应用中用户属性规模远远小于系统属性规模的情况.

关键词 多机构;隐私保护;属性基加密;属性隐藏;标准模型

中图法分类号 TP309

随着互联网的发展以及云计算的应用,越来越多的人趋于将数据存储在云端,然而在这些数据中可能包含一些敏感信息(比如个人病历),为了保护用户隐私,经常需要对敏感的隐私信息进行加密处理.属性基加密(attribute based encryption, ABE)[1]作为一种新兴的公钥加密技术,将用户的身份用一系列的属性表示,通过对用户的私钥或密文设置属性集或访问结构,只有属性集和访问结构相匹配时才能解密,从而实现了一对多的通信以及对文件的细粒度访问控制,解决了传统公钥密码体制无法满足云环境下的访问控制、安全和效率问题,被认为是云环境中高效的信息分享的最佳选择.但是由于加密者制定访问策略的属性中往往会包含一些敏感的隐私信息,如个人健康病例系统中病人设置访问策略为{人民医院,医生,心脏科},这些属性信息很容易泄露病人的隐私.因此,如何实现云环境数据共享中敏感信息的隐私保护便成为学者们研究的热点.

传统的 ABE 只有一个可信的机构来管理所有的属性,但在实际应用中属性往往是由多个机构管理运行的.单个属性机构的 ABE 机制不能满足大规模分布式环境的需求,属性权威机构易受到集中攻击,另外,属性权威机构需要为所有的用户认证属性分发密钥,工作负荷过重,成为系统的性能瓶颈.在此基础上 Chase[2] 提出第 1 个多机构属性基加密方案(multi-authority attribute based encryption, MA-ABE),多个机构分别管理不同的属性集,并为其权限内的属性用户分发密钥,该方案有一个可信的中央机构及多个属性机构,允许属性机构独立地监控属性及分配密钥,但该方案要求中央机构完全可信,一旦中央机构被破坏,则整个系统都会崩溃.

文献[3]中 Lin 等人首次提出无中央机构的安全门限多机构 ABE,该方案采用密钥分配技术和零秘密共享技术,代替了文献[2]中的伪随机函数.文献[4]中 Müller 等人提出密钥策略的多机构 ABE,该方案的中央机构只负责秘密用户的密钥分发,而属性密钥的分发由多个属性机构来完成,每个属性分别和一个单独的属性机构相关.文献[5]中 Chase 等人提出提高隐私和安全的多机构 ABE,该方案移除了可信的中央机构,每个用户都有一个唯一的全域身份标识(global identifier, GID),采用匿名证书技术隐藏用户的 GID,以防止机构累积用户的信息来保护用户的隐私.文献[6]中 Lewko 等人提出分权的多机构 ABE,该方案中任何一方都可以通过为不同的用户生成公钥和发放私钥成为机构,且提出一种将用户的密钥与 GID 相连的技术以抵抗共谋攻击.文献[7]中 Xhafa 等人提出云计算中具有隐私意识的基于属性的个人健康记录共享系统,该方案是一种密钥策略的多机构的 ABE,通过隐藏访问策略保护访问用户的隐私.文献[8]中 Han 等人提出提高隐私和安全的分权的密文策略的多机构 ABE,该方案采用承诺方案和零知识证明技术来保护用户的 GID 和属性,这是第 1 篇保护用户属性的方案.但是,在文献[9]中 Wang 等人指出文献[8]中所提的方案并不能很好地保护用户的属性.文献[10]中 Qian 等人提出基于多机构属性基加密的可撤销属性和隐私保护的个人健康病例系统,该方案提供用户属性的撤销及策略更新.文献[11]中关志涛等人提出面向云存储的基于属性加密的多授权中心访问控制方案,该方案采用最小化属性分组算法大大减少了用户访问文件时所需的密钥量,系统开销较小.文献[12]中陶启等人提出基于密文策略多机构属性基加密方案,该方案去除中央机构,采用访问树策略及 Shamir 秘密共享技术,并支持属性撤销.文献[13]中吴光强提出适合云存储的访问策略可更新多中心 CP-ABE 方案,该方案设置的多授权机构可以防止密钥泄露,增加系统的灵活性和安全性.但文献[11-13]并不提供用户的属性隐私保护.

从上述分析可以看出,多机构 ABE 方案一般通过保护用户 GID 来保护用户隐私,而很少考虑用户的其他属性泄露所引起的隐私问题.例如高校招生系统中,系统将考生的报考档案信息保存至云服务器,高校使用考生的姓名、身份证号、报考院校等加密考生的信息,访问策略如图 1 所示,但在这些属性中,身份证号和报考院校等都是较为敏感的信息,其内容涉及考生隐私,所有的属性信息都需要进行

保护.已有的多机构 ABE 方案[6-11]大多数都是线性秘密共享(linear secret-sharing schemes, LSSS)技术,但是 LSSS 中分享矩阵如何表达访问控制策略并没有进行详细的描述.在标准假设下,LSSS 矩阵和访问树结构都支持属性的与、或、门限操作,但是 LSSS 秘密分享矩阵构造相对复杂.而访问树通常利用拉格朗日多项式插值来实现,构造复杂度相对较低,因此基于访问树的 ABE 方案在应用中更为实用.

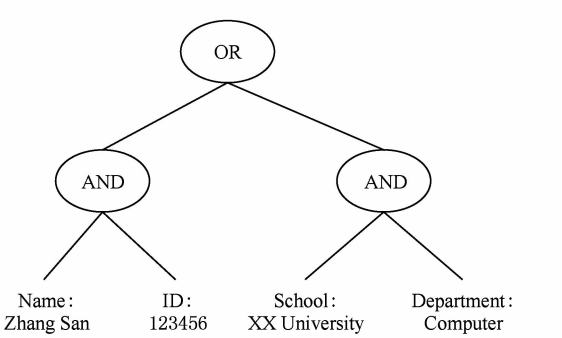

Fig. 1 General access policy

图 1 普通访问策略

结合文献[14]中的思想,本文基于访问树结构,提出一种支持隐私保护的多机构 ABE 方案,实现对用户属性的隐私保护,只利用属性名进行加密,从而有效保护用户的隐私,具体访问策略如图 2 所示:

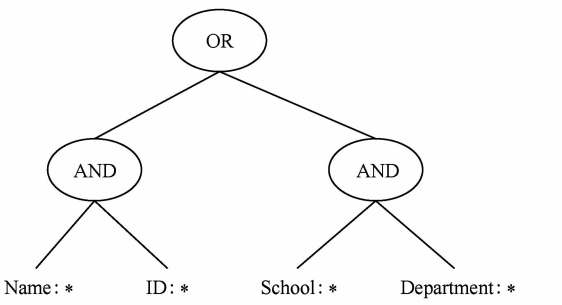

Fig. 2 Partially hidden access policy

图 2 半隐藏访问策略

本文主要包括 3 点创新:

1) 将属性分为属性名和属性值 2 部分,加密时只针对属性名进行加密,而将属性值隐藏,解密时只需提供其属性值,看其是否满足该属性名下的属性值.

2) 采用半策略隐藏的方式进行加密访问策略的设置,加密时仅对与用户相关的属性进行加密,而不是对系统所有属性进行加密,改变了已有的隐私保护属性基加密方式.

3) 实现对用户所有属性的保护,不再单一通过对 GID 隐藏进行隐私保护,而是将 GID 作为用户的一种属性,通过保护属性保护用户的 GID,实现对用户的隐私保护.

1 相关知识

1.1 双线性对

令 G_0,G_1 为 2 个阶为素数 p 的乘法循环群,g_0 为 G_0 的生成元,存在双线性映射 $e:G_0\times G_0\rightarrow G_1$,且有 3 个特征:

1) 双线性. $\forall x,y\in\mathbb{Z}_p$, $\forall m,n\in G_0$,有 $e(m^x,n^y)=e(m,n)^{xy}$.

2) 可计算性. $\forall m,n\in G_0$,存在有效算法计算 $e(m,n)$.

3) 非退化性. $e(g_0,g_0)\neq 1$.

1.2 访问结构

假定$\{p_1,p_2,\cdots,p_n\}$为参与方的集合,集合 $P\subseteq 2^{\{p_1,p_2,\cdots,p_n\}}$,若对于 $\forall X,Y$:若 $X\in P$ 且 $X\subseteq Y$,有 $Y\in P$,则称 P 是单调的;访问结构是$\{p_1,p_2,\cdots,p_n\}$的非空子集 P,即 $P\subseteq 2^{\{p_1,p_2,\cdots,p_n\}}\setminus\{\varnothing\}$,包含在 P 内的集合是授权集合,不包含在 P 内的集合是非授权集合.

1.3 Shamir(t,n)门限秘密共享

Shamir(t,n)门限秘密共享[15]是将秘密 s 按一定的方法分成 n 个共享,任意 t 个共享都可恢复出 s,其中 $t\leqslant n$;它是以一个 $t-1$ 阶的多项式 $y=p(x)$ 为基础的,其具体描述如下:

1) 建立.分享者 D 想要在 t 个用户中分布秘密 s. D 首先选择一个素数 $p>\max(s,n)$,定义 $a_0=s$,并随机选择 $t-1$ 个系数 $a_1,a_2,\cdots,a_{t-1}$,$0<a_j\leqslant p-1$,且在 Z_p 中定义随机多项式 $p(x)=\sum_{j=0}^{t-1}a_jx^j$;然后 D 计算 $s_i=p(x_i)\bmod p$,并将分享 s_i 发送给用户.

2) 合并分享.给定任意 t 个用户的分享$\{(x_i,s_i)\}_{i=1}^t$,可以通过拉格朗日插值法计算 $p(x)$的系数 a_j,从而恢复出 $p(x)=\sum_{i=1}^t s_i\Delta_i(x)$,其中$\Delta_i(x)=\prod_{j=1,j\neq i}^t\frac{x-x_j}{x_i-x_j}$,则分享的秘密为 $p(0)=a_0=s$.

1.4 素数阶群上的判断双线性 Diffie-Hellman 假设(DBDH 假设)

令 G_0,G_1 为 2 个阶为素数 p 的乘法循环群,g_0 为 G_0 的生成元,存在双线性映射 $e:G_0\times G_0\rightarrow G_1$,随机选择 $a,b,c\in\mathbb{Z}_p^*$ 和 $V\in G_1$,给定元组$(g_0,g_0^a,g_0^b,$

$g_0^c, V)$,判断 $V=e(g_0,g_0)^{abc}$ 是否成立. 如果对于任一多项式时间的敌手 $\mathcal{A}$ 的优势

$Adv_{\mathcal{A}}^{\mathrm{DBDH}}=|Pr[\mathcal{A}(g_0^a,g_0^b,g_0^c,e(g_0,g_0)^{abc})=1]-Pr[\mathcal{A}(g_0^a,g_0^b,g_0^c,V)=1]|\leqslant\varepsilon$ 是可忽略的,则在群 (e,p,G_0,G_1) 上的 DBDH 问题是困难的.

2 算法定义与安全模型

2.1 算法定义

本文方案包括系统初始化 $Setup(1^\lambda)$、属性机构初始化 $Authority\text{-}Step(PP)$、密钥生成 $KeyGen(PP,SK_i,A_{\mathrm{user}})$、加密 $Encrypt(PP,m,(A,T))$、解密 $Decrypt(PP,CT,SK_{\mathrm{user}})$ 这 5 个算法,具体如下:

1) 系统初始化 $Setup(1^\lambda)\rightarrow PP$. 系统初始化算法由系统执行,输入安全参数 1^λ,输出系统公共参数 PP.

2) 属性机构初始化 $Authority\text{-}Step(PP)\rightarrow(PK_i,SK_i)$. 算法由属性机构执行,输入公共参数 PP,输出属性机构的公私钥对.

3) 密钥生成 $KeyGen(PP,SK_i,A_{\mathrm{user}})\rightarrow SK_{\mathrm{user}}$. 算法由机构与用户交互完成,输入公共参数 PP、属性机构私钥 SK_i、用户属性值 A_{user},输出用户私钥 SK_{user}.

4) 加密 $Encrypt(PP,m,(A,T))\rightarrow CT$. 算法由用户执行,输入公共参数 PP、明文 m、访问结构 (A,T),输出密文 CT.

5) 解密 $Decrypt(PP,CT,SK_{\mathrm{user}})\rightarrow m$. 算法由用户执行,输入公共参数 PP、用户私钥 SK_{user}、密文 CT,输出明文 m.

2.2 安全模型

本方案的安全模型是选择属性和选择明文攻击下的不可区分性(indistinguishability against selective attribute and chosen-plaintext attack, IND-sAtt-CPA)游戏,游戏中包含一个挑战者和一个敌手,挑战者模拟系统运行并回答敌手的询问. 具体游戏如下:

1) 初始化. 敌手选择要挑战的访问结构树 (A,T^*),并将它发送给挑战者.

2) 建立. 挑战者执行 $Setup(1^\lambda)$ 和 $Authority\text{-}Setup(PP)$ 算法,生成公共参数 PP 及属性机构的公私钥 (PK_i,SK_i),并将 PP 及 PK_i 发送给敌手.

3) 阶段 1. 敌手为其属性集合 A_{D} 发出私钥请求,且 $A_{\mathrm{D}}\not\subset(A,T^*)$,挑战者返回其私钥 SK_{D}.

4) 挑战. 敌手发送 2 个等长的消息 m_0,m_1 给挑战者,挑战者随机选取 $c\in\{0,1\}$,对 m_c 进行加密,返回 $C_c=Encrypt(PP,m_c,(A,T^*))$.

5) 阶段 2. 敌手继续如阶段 1 一样地限制查询私钥.

6) 猜想. 敌手输出对 c 的猜想 $c'\in\{0,1\}$.

定义 1. 如果对于所有的任意多项式时间的敌手以一个可忽略的优势 ε 攻击 IND-sAtt-CPA 游戏,则本方案是自适应性选择明文攻击安全的,且优势 $\varepsilon=\left|Pr[c=c']-\frac{1}{2}\right|$.

3 本文方案

方案将属性分为属性名和属性值 2 部分,假设系统的全部属性包括 n 个不同的属性名,且 $n=(a_1,a_2,\cdots,a_n)$,每个属性名 a_i 下有 n_i 个不同的属性值 $A_i=(a_{i,1},a_{i,2},\cdots,a_{i,n_i})$,用户的属性集合为 $A_{\mathrm{user}}=(a_1:a_{1,t_1},a_2:a_{2,t_2},\cdots,a_n:a_{n,t_n})$,其中 $a_{i,t_i}\in A_i$. 假设系统有 n 个不同的属性机构 $AA_1,AA_2,\cdots,AA_n$,属性机构 AA_i 管理属性名为 a_i 下的 n_i 个属性值,a_{i,n_i} 表示由机构 AA_i 管理的属性名为 a_i 的属性值.

1) 系统初始化. 该算法输入安全参数 1^λ,输出系统公共参数 $PP=\{e,G,G_1,g_1,g_2,p\}$,其中 g_1,g_2 是循环群 G 的生成元,p 为群的素数阶,双线性映射 $e:G\times G\rightarrow G_1$.

2) 属性机构初始化. 该算法输入 PP,输出机构 AA_i 的公私钥对;属性机构 AA_i 随机选择 $\alpha_i\in\mathbb{Z}_p^*$,计算:$X_i=e(g_1,g_1)^{\alpha_i}$;对其管理的属性名 a_i,随机选取 $\omega_i\in\mathbb{Z}_p^*$,计算:$Y_i=g_1^{\omega_i}$;对其下的每个属性值 a_{i,n_i},随机选择 $\omega_{i,n_i}\in\mathbb{Z}_p^*$,计算:$W_{i,n_i}=g_1^{\omega_{i,n_i}}$.

则:属性机构公钥 $PK_i=\{X_i,Y_i,(W_{i,n_i})_{\forall a_{i,n_i}\in A_i}\}$,

属性机构私钥 $SK_i=\{\alpha_i,\omega_i,(\omega_{i,n_i})_{\forall a_{i,n_i}\in A_i}\}$.

3) 密钥生成. 该算法由用户与属性机构 AA_i 交互,属性机构首先检查用户的属性值 a_{i,t_i} 是否是其权限下的属性值,若不是,则输出 $\perp$;否则,随机选择 $\gamma_i\in\mathbb{Z}_p^*$,计算:

$$D_i=g_1^{\alpha_i}g_2^{\gamma_i},$$

$$D_{i,t_i}=g_2^{\gamma_i}Y_i^{\omega_{i,t_i}}\ (1\leqslant i\leqslant n).$$

则用户私钥 $SK_{\mathrm{user}}=\{D_i,D_{i,t_i}\}_{(1\leqslant i\leqslant n)}$.

4) 加密. 该算法输入明文 m、访问结构 (A,T),输出密文 CT. 利用 Shamir 门限秘密共享构造访问树,将叶子节点与加密者设置的属性名 a_i 相对应,秘密共享如下:随机选取 $s\in\mathbb{Z}_p^*$,设置访问树根节点为 s,并标记该节点已分配,其孩子节点标记为未分配,对所有未分配的非叶子节点做 3 个操作.

① 若操作符为 $\vee$,且其孩子节点未分配,则为其孩子节点赋值 s,并标记已分配;

② 若操作符为 $\wedge$,且其孩子节点未分配,则随机选择 $s_i\in\mathbb{Z}_p^*$ $(i=1,2,\cdots,n-1)$,其中 n 为其孩子节点个数,第 n 个孩子节点赋值 $s_n=s-\sum_{i=1}^{n-1}s_i$,并标记已分配;

③ 若操作符为 of,且其孩子节点未分配,则随机选取一个 $t-1$ 阶的多项式 $p(x)$,令 $p(0)=s$,利用 Shamir(t,n)对 s 进行分割,其中 t 为门限值,n 为孩子节点数,对其孩子节点赋值 $s_i=p(i)$,并标记为已分配.

同样,随机选取 $s'\in\mathbb{Z}_p^*$,按上述方法进行分割,对叶子节点赋值 s_i'.

令 A_τ 为叶子节点表示的属性名集合,I_A 为被选属性机构的索引集,对访问树的每个叶子节点进行计算:

$$CT=\{C_0=m\times\prod_{i\in I_A}e(g_1,g_1)^{\alpha_i s},$$

$$C_1=g_1^s,(C_2=Y_i^{s_i},C_3=g_1^{s_i})_{\forall a_i\in A_\tau}\},$$

$$CT'=\{C_0'=\prod_{i\in I_A}e(g_1,g_1)^{\alpha_i s'},$$

$$C_1'=g_1^{s'},(C_2'=Y_i^{s_i'},C_3'=g_1^{s_i'})_{\forall a_i\in A_\tau}\},$$

则密文 $C=(CT,CT')$.

5) 解密. 解密时,算法首先计算满足访问结构(A,T)的最小子树 $\min(A,T)$,确定解密者是否存在与最小访问子树相匹配的属性值,使得:

$$\frac{C_0'\times\prod_{i\in I_A}\prod_{a_i\in\min(A,T)}\left(\frac{e(D_{i,t_i},C_3')}{e(W_{i,t_i},C_2')}\right)^{\Delta_i(0)}}{\prod_{i\in I_A}e(D_i,C_1')}=1.$$

$\Delta_i(0)$为拉格朗日系数,若存在,则计算:

$$\frac{C_0\times\prod_{i\in I_A}\prod_{a_i\in\min(A,T)}\left(\frac{e(D_{i,t_i},C_3)}{e(W_{i,t_i},C_2)}\right)^{\Delta_i(0)}}{\prod_{i\in I_A}e(D_i,C_1)}=m,$$

否则,判断解密失败.

4 方案分析

4.1 安全性证明

定义 2. 如果 DBDH 假设成立,则不存在任何多项式时间内的敌手攻击成功.

游戏开始前挑战者生成双线性群(e,p,G,G_1),随机选择生成元 $g_1\in G$,$a,b,c\in\mathbb{Z}_p^*$,抛掷一枚均匀的硬币,得到数 $\theta\in\{0,1\}$,如果 $\theta=0$,将$(A,B,C,V)=(g_1^a,g_1^b,g_1^c,e(g_1,g_1)^{abc})$发送给敌手,否则,发送$(A,B,C,V)=(g_1^a,g_1^b,g_1^c,e(g_1,g_1)^v)$给敌手,其中 $a,b,c,v\in\mathbb{Z}_p^*$. 挑战者与敌手的游戏如下:

1) 初始化. 敌手选择要挑战的访问结构树(A,T^*),并发送给挑战者.

2) 建立. 挑战者随机选择 $x_i\in\mathbb{Z}_p^*$,令 $X_i=e(g_1,g_1)^{\alpha_i}=e(g_1,g_1)^{ab}e(g_1,g_1)^{x_i}$,显然 $\alpha_i=ab+x_i$,对于机构 AA_i,对其管理的属性名 a_i,随机选取 $k_i\in\mathbb{Z}_p^*$,若 $\alpha_i\in(A,T^*)$,计算:$Y_i=g_1^{k_i}$,其中 $k_i=\omega_i$;若 $\alpha_i\notin(A,T^*)$,计算:$Y_i=B^{\frac{1}{k_i}}=g_1^{\frac{b}{k_i}}$,其中 $\frac{b}{k_i}=\omega_i$,对其下的每个属性值 a_{i,n_i},随机选择 $k_{i,n_i}\in\mathbb{Z}_p^*$,若 $a_{i,n_i}\in\alpha_i\in(A,T^*)$,计算:$W_{i,n_i}=g_1^{k_{i,n_i}}$,其中 $k_{i,n_i}=\omega_{i,n_i}$;若 $a_{i,n_i}\in\alpha_i\notin(A,T^*)$,计算:$W_{i,n_i}=B^{\frac{1}{k_{i,n_i}}}=g^{\frac{b}{k_{i,n_i}}}$,其中$\frac{b}{k_{i,n_i}}=\omega_{i,n_i}$. 则属性机构公钥 $PK_i=\{X_i,(Y_i)_{\forall a_i},(W_{i,n_i})_{\forall a_{i,n_i}}\}$,属性机构私钥 $SK_i=\{x_i,(k_i)_{\forall a_i},(k_{i,n_i})_{\forall a_{i,n_i}}\}$;挑战者将属性机构公钥 PK_i 发送给敌手.

3) 阶段 1. 敌手为其属性集合 A_D 发出私钥请求,且限定 $A_D\not\subset(A,T^*)$,挑战者随机选择 $\gamma_i'\in\mathbb{Z}_p^*$,计算 $D_i=g_1^{ab+x_i}g_2^{\gamma' i}$,对其属性值,计算 $D_{i,t_i}=g_2^{\gamma' i}Y_{i,n_i}^{\frac{b}{k}}$,并将生成的敌手私钥 $SK_D=\{D_i,D_{i,t_i}\}$发送给敌手.

4) 挑战. 敌手随机选择 2 个等长的消息 m_0,m_1 给挑战者,挑战者随机选取 $c\in\{0,1\}$,对 m_c 进行加密.

① 计算:

$$C_1=g_1^c,$$

$$C_0=m_c\times\prod_{i\in I_A}e(g_1,g_1)^{\alpha_i c}=$$

$$m_c\times\prod_{i\in I_A}e(g_1,g_1)^{(ab+x_i)c}=$$

$$m_c\times\prod_{i\in I_A}e(g_1,g_1)^{abc}\times e(g_1,g_1)^{x_i c}=$$

$$m_c\times V\times\prod_{i\in I_A}e(g_1,g_1)^{x_i c}.$$

② 将访问树的根节点设置为 g_1^c,并标记该节点已分配,其孩子节点标记为未分配,对所有未分配的非叶子节点做以下操作:若操作符为 $\vee$,且其孩子节点未分配,则为其孩子节点赋值 g_1^c,并标记已分配;若操作符为 $\wedge$,且其孩子节点未分配,则随机选择 $\lambda_i\in\mathbb{Z}_p^*$,并分配 $g_1^{\lambda_i}$,最后一个孩子节点分配 $g_1^{\lambda_n}=g_1^c\Big/\sum_{i=1}^{n-1}g_1^{\lambda_i}$,并标记已分配;若操作符为 of,且其孩子

节点未分配,则随机选取一个 $t-1$ 阶的多项式 $p(x)$,令 $p(0)=g_1^c$,利用 Shamir(t,n)对 g_1^c 进行分割,其中 t 为门限值,n 为孩子节点数,对其孩子节点赋值 $g_1^{\lambda_i}=p(i)$,并标记为已分配.

③ 对于每一个叶子节点属性名 $\alpha_i\in(A,T^*)$,计算 $C_2=Y_i^{\lambda_i}$,$C_3=g_1^{\lambda_i}$.

挑战者将密文 $C_c=(C_0,C_1,C_2,C_3)$发送给敌手.

5) 阶段 2. 敌手继续如阶段 1 同样地限制查询私钥.

6) 猜想. 敌手输出对 c 的猜想 $c'\in\{0,1\}$. 如果 $c'\neq c$,则输出 $\theta=1$,$V=e(g_1,g_1)^v$,此时敌手不能得到任何有用的信息,即敌手输出 $c'\neq c$ 的优势为 $Pr[c'\neq c|\theta=1]=1/2$,所以敌手输出 $c'=c$ 即猜出明文的优势为 $Pr[c'=c|\theta=1]=1-Pr[c'\neq c|\theta=1]=1/2$. 如果 $c'=c$,则输出 $\theta=0$,$V=e(g_1,g_1)^{abc}$,挑战者挑战成功,此时敌手的优势 $Pr[c'=c|\theta=0]=\frac{1}{2}+\varepsilon$.

因此,敌手攻击 DBDH 假设的优势为

$$\left|\frac{1}{2}Pr[c'=c|\theta=0]+\frac{1}{2}Pr[c'=c|\theta=1]-\frac{1}{2}\right|=\frac{1}{2}\times\frac{1}{2}+\frac{1}{2}\times\left(\frac{1}{2}+\varepsilon\right)-\frac{1}{2}=\frac{1}{2}\varepsilon.$$

任何多项式时间内敌手赢得 IND-sAtt-CPA 游戏的优势是可忽略的,因此本文是选择明文攻击安全的.

4.2 性能分析

本文通过属性机构公钥长度、用户密钥、密文长度、加解密代价、隐私保护和安全性假设 6 个方面进行比较,结果如表 1 所示. 其中 n 表示属性机构的个数,N 表示系统属性个数,n_i 表示属性机构 AA_i 所管理的属性个数,L_G 和 L_{G_1} 分别群 G 和群 G_1 中一个元素的比特长度,L_{ver} 表示版本号的长度(文献[10]中引入了版本号),A_{user} 和 A_{cip} 分别表示用户和密文的属性个数,I_{cip} 表示加密时使用的属性所属的属性机构个数,ρ 表示用户 GID 的大小,exp 表示指数运算,e 表示双线性映射,解密代价指解密运算的双线性对的次数.

Table 1 Comparison of Multi-Authority ABE Schemes

表 1 多机构 ABE 方案对比

Scheme	Storage Cost			Computation Cost		Privacy Protection	Security Assumption
	Size of Attribute Authority's Public Key	Size of User's Privacy Key	Size of Ciphertext	Encryption Cost	Decryption Cost		
Ref[6]	$n_iL_G+n_iL_{G_1}$	$(2A_{\text{user}})L_G$	$(3A_{\text{cip}})L_G+(3A_{\text{cip}})L_{G_1}$	$(3A_{\text{cip}})\exp+(2A_{\text{cip}}+1)e$	$2A_{\text{user}}$	Protect User's GID	Group Model
Ref[7]	$n_iL_G+n_iL_{G_1}$	$(2A_{\text{user}}+5)L_G$	$(4N+5)L_G+L_{G_1}$	$(4n+4)\exp+e$	$\sum_{i\in I_{\text{cip}}}4n_i+4\rho+1$	Hide the Access Policy to Protect Privacy	DBDH
Ref[8]	$(2n_i+4)L_G+L_{G_1}$	$(9A_{\text{user}})L_G$	$(3A_{\text{cip}}+3I_{\text{cip}})L_G+A_{\text{cip}}L_{G_1}$	$(3I_{\text{cip}}+3A_{\text{cip}})\exp+(I_{\text{cip}})e$	$\sum_{i\in I_{\text{cip}}}2n_i+4I_{\text{cip}}$	Protect User's GID and Attributes	q-Parallel BDHE
Ref[10]	$(n_i+1)L_G+L_{G_1}+L_{\text{ver}}$	$(A_{\text{user}}+1)L_G+L_{\text{ver}}$	$(A_{\text{cip}}+1)L_G+nL_{G_1}$	$(A_{\text{cip}}+1)\exp+(n+1)e$	$A_{\text{user}}+n+1$	Protect User's GID	DBDH
Our Scheme	$(n_i+1)L_G+L_{G_1}$	$(2A_{\text{user}})L_G$	$(4A_{\text{cip}}+2)L_G+I_{\text{cip}}L_{G_1}$	$(4A_{\text{cip}}+2)\exp+(I_{\text{cip}})e$	$4A_{\text{user}}+4I_{\text{cip}}$	Protect User's GID and Attributes	DBDH

从表 1 可以看出,本文方案提供对用户属性和 GID 进行保护;文献[6,10]仅仅是保护用户 GID;文献[7]通过隐藏访问策略保护用户的隐私;文献[8]保护用户的 GID 及属性,这是首次提出保护用户属性的思想,但文献[9]证明其并不能很好地保护属性,本文方案将用户的属性分为属性名和属性值 2 部分,通过隐藏属性值保护用户的隐私,并将 GID 作为属性进行保护. 从安全方面来看,文献[6]仅仅满足一般群模型下安全,而本文方案和文献[7,10]是满足 DBDH 假设的.

性能方面,本文在通信代价及计算代价两方面,与其他方案相比相对较优. 通过对属性机构公钥长度比较,本文方案比文献[6-8]缩短了近乎一半,比文献[10]减少了 1 个版本号的长度. 用户密钥长度方面,本文方案比文献[7-8]大大缩短,达到了文献[6]相同的长度. 文献[10]中用户密钥尽管较短,但用户密钥的生成需要用户与 n 个属性机构运行匿名密钥生成协议生成,大部分计算由用户执行,计算量

较大.密文长度方面,本文方案相比其他方案长度得到优化,仅与加密访问策略中属性个数和属性机构个数相关,而文献[7]与属性总个数呈线性相关,文献[10]与属性机构总个数相关,都远远大于本文方案.计算代价方面从加密计算和解密计算2部分进行分析,加密代价本文方案减少了指数运算和双线性映射的计算次数,比其他方案更显优势.解密代价方面,本文方案远远小于同样保护隐私的文献[7-8],仅和用户的属性个数相关,而文献[7-8]中如果每个属性机构管理的属性个数比较大,用户解密所付出的代价太大.虽然本文方案解密代价相比文献[6,10]略高,但是文献[6,10]并不提供对用户所有属性的保护.

综合分析,本文方案实现对用户所有属性的隐私保护,性能方面也有很大的提高,适用于实际应用中用户属性规模远远小于系统属性规模的情况.

5 结束语

针对云存储环境中敏感信息保护需求,本文提出一种支持隐私保护的多机构ABE方案,并证明其在标准模型下满足自适应性选择明文安全.本文方案中将属性分为属性名和属性值两部分,通过对属性值进行隐藏,仅仅对属性名进行加密,有效保护了用户的隐私,避免用户的具体属性值泄露给其他任何第三方,恶意的用户无法分析出任何潜在的隐私信息.与其他方案对比结果显示,该方案在计算代价和存储代价方面都有明显优势.

云环境中数据拥有者经常需要动态地更新访问策略,这种策略半隐藏方式有利于用户属性的动态更新,只需要对用户的属性值进行更新,属性名保持不变,下一步工作我们将针对策略更新进行深入地研究.

参 考 文 献

[1] Sahai A, Waters B. Fuzzy identity-based encryption [C] // Proc of the 24th Int Conf on Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2005: 457-473

[2] Chase M. Multi-authority attribute based encryption [C] // Proc of Theory of Cryptography Conf. Berlin: Springer, 2007: 515-534

[3] Lin Huang, Cao Zhenfu, Liang Xiaohui, et al. Secure threshold multi-authority attribute based encryption without a central authority [C] //Proc of Int Conf on Cryptology in India. Berlin: Springer, 2008: 426-436

[4] Müller S, Katzenbeissior S, Eckert C. On multi-authority ciphertext-policy attribute-based encryption [J]. Bulletin of the Korean Mathematical Society, 2009, 46(4): 803-819

[5] Chase M, Chow S S. Improving privacy and security in multi-authority attribute-based encryption [C] //Proc of the 16th ACM Conf of Computer and Communication Security. New York: ACM, 2009: 121-130

[6] Lewko A, Waters B. Decentralizing attribute-based encryption[G] //LNCS 6632: Proc of the 30th Int Conf on Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2011: 568-588

[7] Xhafa F, Feng Jianglang, Zhang Yinghui, et al. Privacy-aware attribute-based PHR sharing with user accountability in cloud computing [J]. Journal of Supercomputing, 2015, 71(5): 1607-1619

[8] Han Jinguang, Susilo W, Mu Yi, et al. Improving privacy and security in decentralized ciphertext-policy attribute-based encryption [J]. IEEE Trans on Information Forensics and Security, 2015, 10 (3): 665-678

[9] Wang Minqian, Zhang Zhenfeng, Chen Cheng. Security analysis of a privacy-preserving decentralized ciphertext-policy attribute-based encryption scheme [J]. Concurrency & Computation Practice & Experience, 2016, 28(4): 1237-1245

[10] Qian Huiling, Li Jiguo, Zhang Yichen, et al. Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation [J]. International Journal of Information Security, 2015, 14(6): 487-497

[11] Guan Zhitao, Yang Tingting, Xu Ruzhi, et al. Multi-authority attribute-based encryption access control model for cloud storage [J]. Journal on Communications, 2015, 36(6): 116-126 (in Chinese)
(关志涛, 杨亭亭, 徐茹枝, 等. 面向云存储的基于属性加密的多授权中心访问控制方案[J]. 通信学报, 2015, 36(6): 116-126)

[12] Tao Qi, Huang Xiaofang. Multi-authority ciphertext-policy attribute-based encryption scheme [J]. Journal of Wuhan University: Nature Science, 2015, 61(6): 545-548 (in Chinese)
(陶启, 黄晓芳. 基于密文策略多机构属性基加密方案[J]. 武汉大学学报: 理学版, 2015, 61(6): 545-548)

[13] Wu Guangqiang. Multi-authority CP-ABE with policy update in cloud storage [J]. Journal of Computer Research and Development, 2016, 53(10): 2393-2399 (in Chinese)
(吴光强. 适合云存储的访问策略可更新多中心CP-ABE方案[J]. 计算机研究与发展, 2016, 53(10): 2393-2399)

[14] Lai Junzuo, Deng Huijie, Li Yingjiu. Expressive CP-ABE with partially hidden access structures [C] //Proc of the 7th ACM Symp on Information, Computer and Communications Security. New York: ACM, 2012: 18-19

[15] Ibraimi L, Tang Qiang, Hartal P. Efficient and provable secure ciphertext-policy attribute-based encryption schemes [C] //Proc of the 5th Int Conf on Information Security Practice and Experience. Berlin: Springer, 2009: 1-12

Yan Xixi, born in 1985. PhD. Member of CCF. Her main research interests include the digital rights management, digital content security.

Li Zichen, born in 1965. PhD. Professor. His main research interests include information security, electronic commerce, and cryptography.

Liu Yuan, born in 1989. Master candidate. Her main research interests include network and information security, cryptography.

Tang Yongli, born in 1972. PhD. Professor. Senior member of CCF. His main research interests include the cryptography algorithm detection, network and information security.