一种多认证机构可验证的属性基加密方案 *

陈 勤, 党正芹, 张金漫, 马丹丹
(杭州电子科技大学 计算机学院, 杭州 310018)

摘 要: 针对属性基加密中中央认证机构所带来的安全隐患问题,提出了一种新型的多认证机构可验证的属性基加密方案。该方案采用由各个认证机构独立生成系统主私钥份额和各自公私钥的方法,去除了中央认证机构,避免了因中央认证机构一旦遭破坏将会导致整个系统崩溃的问题,提高了属性基加密的安全性,同时对密文和密钥的正确性进行了验证。最后,给出了可验证性和安全性分析。

关键词: 属性基加密; 多认证机构; 无中央认证机构; 可验证性; 安全性
中图分类号: TP309.2 **文献标志码**: A **文章编号**: 1001-3695(2012)01-0308-04
doi:10.3969/j.issn.1001-3695.2012.01.085

Verifiable attribute base encryption scheme with multi-authority

CHEN Qin, DANG Zheng-qin, ZHANG Jin-man, MA Dan-dan
(*College of Computer*, *Hangzhou Dianzi University*, *Hangzhou* 310018, *China*)

Abstract: Aiming at the security issues caused by the central authority in attribute base encryption, this paper proposed a noble multi-authority verifiable attribute base encryption scheme. Compared with other schemes, the central authority was omitted in this scheme which solved the problem that the whole system would crash once the central authority was destroyed, using the technology of making each authority to generate their own master keys parts as well as their public and private keys independently. So the security of the system was improved. At the same time, it verified the correctness of the ciphertext and the keys. In addition, it gave the verification and security analysis.

Key words: attribute based encryption; multi-authority; without a central authority; verifiability; security

属性基加密是在模糊身份基加密[1]的基础上提出的一种新的公钥加密机制,它用一系列的属性描述了用户的身份,引入了访问控制结构,并将这两者与密文和密钥有机结合,当且仅当属性集合满足了访问控制结构时才能解密。根据访问控制结构位置的不同又可分为密钥策略[2]和密文策略[3,4]的属性基加密。属性基加密可广泛应用于分布式环境下的信息安全,如云计算中的安全存储,已成为公钥加密机制的研究热点之一。

近几年来,国内外研究者陆续提出了一系列的属性基加密方案,如文献[1~6]等,但上述几种方案都采用了单一的认证机构,一旦该认证机构被攻破,将会泄露其中的所有信息,风险性相当大。Chase[7]于 2007 年提出了多认证机构的属性基加密系统,但它还需要一个可信的中央认证机构,管理其他所有认证机构的私密信息,所以一旦该中央认证机构被攻破,信息的安全性将受到威胁。为此,文献[8,9]相继提出了去除中央认证机构的解决办法。

本文基于文献[10]中密钥可验证性的构造思想,并利用离散对数困难问题,提出了一种属性基加密方案。该方案具有以下特点:a)多机构但无须中央认证机构,使每个认证机构独立生成自己的公私钥,并公布系统公钥,独立地生成用户私钥份额和可供验证的信息;b)检验密钥的正确性,使得密钥检验有误时,可以定位到相应的认证机构,要求重新发送相应部分的密钥,不需要所有的认证机构都重新发送;c)可验证密文的正确性,使密文检验出错时无须进行解密直接要求加密者重发密文,提高了效率。

1 预备知识

定义 1 双线性映射。G_1、G_2 和 G_T 是阶为大素数 q 的乘法循环群,设 g_1 和 g_2 分别为 G_1 和 G_2 的生成元;ψ 是从 G_2 到 G_1 的同构映射,并且 $\psi(g_2)=g_1$。$e:G_1\times G_2\rightarrow G_T$ 是双线性映射,又称为双线性对,具有以下特性:

a)双线性。对任意的 $u\in G_1$,$v\in G_2$ 和 $a,b\in Z_q$,有 $e(u^a,v^b)=e(u,v)^{ab}$。

b)非退化性。$e(g_1,g_2)\neq 1$。

c)可计算性。对于所有的 $u\in G_1$,$v\in G_2$,存在一个有效的算法能够计算 $e(u,v)$。

定义 2 离散对数问题。令 G 是一个阶为素数 q 的群,选择 g 为其生成元。离散对数问题即为,给定的随机元素 $y\in G$,求元素 $x\in Z_q$,使其满足 $y=g^x$。

定义 3 BDH 判定假设。假设挑战者随机选择 $a,b,c\in Z_q$,且 $g_1\in G_1$,$g_2\in G_2$,BDH 判定假设就是指不存在攻击者在多项式时间内有不可忽略的优势将元组$(A=g_2^a,B=g_2^b,C=g_2^c,e(g_1,g_2)^{abc})$和$(A=g_2^a,B=g_2^b,C=g_2^c,e(g_1,g_2)^z)$进行区分。

定义 4 q-DDHI 假设。设 G 是一个阶为 q 的群,g 为其生成

收稿日期: 2011-07-03; **修回日期**: 2011-08-22 **基金项目**: 浙江省自然科学基金资助项目(Y1110781)

作者简介:陈勤(1962-),男,浙江义乌人,教授,硕士,主要研究方向为信息安全、密码学(chenqin@hdu.edu.cn);党正芹(1984-),女,硕士研究生,主要研究方向为信息安全、密码学;张金漫(1987-),女,硕士研究生,主要研究方向为信息安全、密码学;马丹丹(1987-),女,硕士研究生,主要研究方向为信息安全、密码学.

元。给出 $k+2$ 元组 $g, g^{x}, g^{x^2}, \cdots, g^{x^k}, g^{z} \in G_1$,不存在攻击者在多项式时间范围内以不可忽略的概率区分 $1/x \in Z_q^*$ 和 $z \in Z_q^*$。

定义 5　访问结构。假设 $\{p_1, p_2, \cdots, p_n\}$ 表示一个主体集合,对于 $\forall B, C$,如果当 $B \in A$ 和 $B \subseteq C$ 时,有 $C \in A$,则称集合 $A \subseteq 2^{\{P_1, P_2, \cdots, P_n\}}$ 是单调的。在 A 中的集合叫做授权集合,而不在 A 中的集合叫做非授权集合。

定义 6　树形结构。本文所用的访问结构为树形结构,令 Γ 表示一个访问结构,其根节点记为 r,对于每一个非叶子节点 x,都拥有一个门限值,记为 $t_x \in (0, \mathrm{num}_x]$,其中,$\mathrm{num}_x$ 表示节点 x 拥有孩子节点的数目。当 $t_x = 1$ 时该节点为或门,当 $t_x = \mathrm{num}_x$ 时,该节点为与门。每一个叶子节点 x 与一个真实属性相对应,记为 $\mathrm{att}(x)$。x 节点的父节点记为 $\mathrm{parent}(x)$。非叶子节点 x 所拥有的子节点,编号从 1 到 num_x,用 $\mathrm{index}(x)$ 返回。

Γ_r 表示以 r 为根节点的访问树,Γ_x 表示以 x 为根节点的子访问树。如果一个属性集合 γ 满足一棵访问树 Γ_x,记为 $\Gamma_x(\gamma) = 1$。如果 x 是一个非叶子节点,则看它的所有子节点 x' 的 $\Gamma_{x'}(\gamma)$,当且仅当至少有 t'_x 个子节点的 $\Gamma_{x'}(\gamma) = 1$ 时,$\Gamma_x(\gamma) = 1$。如果 x 是叶子节点时,当且仅当 $\mathrm{att}(x) \in \gamma$ 时,$\Gamma_x(\gamma) = 1$。

定义 7　可验证性定义。一个属性基加密方案称之为可验证的[10],需满足以下两个条件:

a)假设 Γ_1 和 Γ_2 是访问结构 Γ 的子树结构,分别解密基于属性集 γ 加密的密文,得到 s_1 和 s_2,如果 γ 是 Γ_1 和 Γ_2 的授权子集,即 $\gamma \in \Gamma_1$ 且 $\gamma \in \Gamma_2$,则有 $s_1 = s_2$。

b)当所有的分享信息都是正确的,用户能够以概率 1 恢复出秘密,即用户能够正常解密密文。

2　方案描述

在本方案中,假设系统中有 N 个认证机构,全部的属性被划分成 N 个互不相交的集合,每个属性集合由不同的认证机构负责管理。

设 G_1、G_2、G_T 是阶为素数 q 的群,g_1 是 G_1 的生成元,g_2 是 G_2 的生成元,双线性映射 $e: G_1 \times G_2 \to G_T$。设 $\psi: G_2 \to G_1$,ψ 是从 G_2 到 G_1 的同构映射,且 $\psi(g_2) = g_1$。抗碰撞函数 $H: \{0,1\}^* \to Z_q$。定义拉格朗日系数表示为 $\Delta_{i,S}$,其中 $i \in S, S \subset Z_q$:$\Delta_{i,S}(x) = \prod_{j \in S, j \neq i} \frac{x-j}{i-j}$。

1)初始化

输入:系统安全参数。

对于每个认证机构 $k(1 \leqslant k \leqslant N)$ 执行如下步骤:

a)根据输入的安全参数生成双线性群参数为 $(q, g_1, g_2, G_1, G_2, G_T, e, \psi)$;

b)随机选取 $f_{k,1}, f_{k,2}, \cdots, f_{k,n_k+1} \in G_2$,其中 n_k 表示认证机构 k 所管理的属性数目,令 $N_k = \{1, 2, \cdots, n_k + 1\}$,定义函数 $F_k(X) = g_2^{X^{n_k}} \prod_{i=1}^{n_k+1} f_{k,i}^{\Delta_{i,N_k}(X)}$;

c)随机选取 $\alpha_k \in Z_q$,计算 $y_k = g_1^{\alpha_k}$,并发送 $Y_k = e(g_1, g_2)^{\alpha_k}$ 给其他认证机构;

d)计算 $Y = \prod_{k=1}^{N} Y_k = e(g_1, g_2)^{\sum_{k=1}^{N} \alpha_k}$;

e)随机选择一个伪随机种子 s_k。

输出:认证机构 k 的私钥为 $\{y_k, s_k\}$;认证机构 k 的公钥为 $\{Y, Y_k, \{f_{k,i}\}_{i \in [1, \cdots, N_k]}\}$;系统公钥 PK 为 $\{q, g_1, g_2, G_1, G_2, G_T, e, \psi, Y_k, Y, \{f_{k,i}\}_{i \in [1, \cdots, N_1], k \in [1, \cdots, N]}\}$。

2)密钥生成

输入:认证机构 $k(1 \leqslant k \leqslant N)$ 的私钥,用户身份标志符及该用户在该认证机构的访问结构 Γ_k。

在认证机构 k 中用户 u 的属性集合为 A_k^u,访问结构为 Γ_k,根节点为 r_k,采用自上而下的方式为访问结构中的每个节点 x 选择一个次数为 $d_{k,x} = t_{k,x} - 1$ 的多项式 $q_{k,x}(\cdot)$,其中 $t_{k,x}$ 为相应节点 x 的门限值。

a)通过伪随机函数计算 $y_{k,u} = P_{sk}(u)$;

b)对根节点 r_k,令 $q_{k,r}(0) = y_{k,u}$,再随机选取剩下的 $d_{k,r}$ 值,完全确定多项式 $q_{k,r}(\cdot)$;

c)计算 $Q_{k,u} = \frac{y_k}{g_1^{y_{k,u}}} = g_1^{\alpha_k - y_{k,u}}$,$Q'_u = e(g_1, g_2)^{\alpha_k - y_{k,u}}$ 和 $Y_{k,u} = e(g_1, g_2)^{y_{k,u}}$,并把 $Q_{k,u}$ 发送给其他认证机构,计算 $Q_u = \prod_{k=1}^{N} Q_{k,u} = g_1^{\sum_{k=1}^{N}(\alpha_k - y_{k,u})}$;

d)对其他节点 x,令 $q_{k,x}(0) = q_{k,\mathrm{parent}(x)}(\mathrm{index}(x))$,再随机选择剩下的 $d_{k,x}$ 个点的值,完全确定多项式 $q_{k,x}(\cdot)$。

e)一旦所有的多项式被确定下来,则对每个叶子节点 x 随机选取 $r_{k,x} \in Z_q$,令:$D_{k,x} = g_1^{q_{k,x}(0)} \cdot F_k(i)^{r_{k,x}}$,其中

$$i = \mathrm{att}(x), R_{k,x} = g_2^{r_{k,x}}$$

$$h_{k,x} = e(g_1, g_2)^{q_{k,x}(0)}$$

$$C_{k,x} = \{e(g_1, g_2)^{a_{k,i}}\}_{i \in [1, \cdots, d_{k,x}]}$$

其中:$a_{k,i}$ 为多项式中非常数部分的系数。

输出:用户的私钥和验证信息为 $\{\{\Gamma_k, D_{k,x}, R_{k,x}\}_{k \in [1, \cdots, N]}, Q_u\}$ 和 $\{h_{k,x}, C_{k,x}, Y_{k,u}\}_{k \in [1, \cdots, N]}$。

3)验证

当用户得到私钥时,执行可验证算法,验证私钥的正确性。

输入:系统公钥 PK,用户私钥 $\{\{\Gamma_k, D_{k,x}, R_{k,x}\}_{k \in [1, \cdots, N]}, Q_u\}$ 和验证信息 $\{h_{k,x}, C_{k,x}, Y_{k,u}\}_{k \in [1, \cdots, N]}$。

对于从认证机构 $k \in [1, \cdots, N]$ 得到的私钥份额,验证过程为:

用户首先从叶子节点出发,对于每个叶子节点 x,验证如下两等式:

$$e(D_{k,x}, g_2) = h_{k,x} \cdot e(F_k(i), R_{k,x}) \tag{1}$$

$$h_{k,x} = h_{k,\mathrm{parent}(x)} \times \prod_{i=1}^{d_{k,x}} (e(g_1, g_2)^{a_{k,i}})^{\mathrm{index}(x)^i} \tag{2}$$

当两等式都成立时,则表示该节点通过验证,如果所有叶子节点都通过验证,则利用式(2)自下而上验证其他各节点信息的正确性,直到根节点 r_k,验证 $h_{k,r_k} = Y_{k,u}$ 是否成立。

然后验证 $Y_k = Q'_u \cdot Y_{k,u}$ 的正确性。在此过程,只要一个节点未通过验证,则表明用户私钥有错,可要求该认证机构重新发送对应部分的密钥。

如果从 N 个认证机构得到的私钥份额都通过了上述验证过程,最后验证式(3)是否成立。

$$Y = \mathrm{e}(Q_u, g_2) \times \prod_{k=1}^{N} Y_{k,u} \tag{3}$$

若式(3)成立,则验证算法输出用户私钥正确,否则输出用户私钥错误。

4)加密

输入:属性集合 $\{A_k^c\}_{k \in [1, \cdots, N]}$,明文 $m \in G_T$,系统公钥。

加密者随机选择 $s \in Z_q$,计算 $E_0 = mY^s$,$E_1 = g_2^s$,$\{E_{k,i} = F_k(i)^s\}_{i \in A_k^c, k \in [1, \cdots, N]}$。

输出:密文为 $\{\{A_k^c\}_{k \in [1, \cdots, N]}, E_0 = mY^s, E_1 = g_2^s, \{E_{k,i} = F_k$

$(i)^s\}_{i\in A_k^c,k\in[1,\cdots N]}\}$。

5)解密

用户得到密文后,首先进行如下验证:

$$e(E_{k,i},g_2)=e(F_k(i),E_1),\forall i\in A_k^c$$

如果等式不成立,则说明密文出错,否则执行以下解密算法:

输入:密文$\{\{A_k^c\}_{k\in[1,\cdots,N]},E_0=mY^s,E_1=g_2^s,\{E_{k,i}=F_k(i)^s\}_{i\in A_k^c,k\in[1,\cdots N]}\}$和密钥$\{\{\Gamma_k,D_{k,x},R_{k,x}\}_{k\in[1,\cdots,N]},Q_u\}$。

当且仅当用户密钥中的访问结构满足密文中的属性集合时方可解密成功。解密过程为:

a)先从叶子节点 x 开始计算

$$\frac{e(D_{k,x},E_1)}{e(R_{k,x},E_{k,i})}=\frac{e(g_1^{q_{k,x}(0)}\cdot F_k(i)^{r_{k,x}},g_2^s)}{e(g_2^{r_{k,x}},F_k(i)^s)}=e(g_1,g_2)^{sq_{k,x}(0)}$$

然后利用拉格朗日插值,逐步向上插值,最后到根节点,计算得到 $e(g_1,g_2)^{sq_{k,r}(0)}=e(g_1,g_2)^{sy_{k,u}(u)}$;

b)计算 $P=\prod_{k=1}^{N}e(g_1,g_2)^{sy_{k,u}(u)}$;

c)计算 $Y_u=e(Q_u,E_1)$;

d)计算 $E_0/(P\cdot Y_u)=m$。

输出:明文 m。

3　方案构造的分析

3.1　正确性

用户想要解密密文,需输入访问结构$\{\Gamma_k\}_{k\in[1,\cdots,N]}$,当$\{\Gamma_k\}_{k\in[1,\cdots,N]}$满足了密文中属性集合$\{A_k^c\}_{k\in[1,\cdots,N]}$时,用户用解密密钥进行解密,过程如下:

$$\frac{E_0}{P\cdot Y_u}=\frac{mY^s}{\prod_{k=1}^{N}e(g_1,g_2)^{sy_{k,u}(u)}\cdot e(Q_u,E_1)}=$$

$$\frac{m\cdot e(g_1,g_2)^{s\cdot\sum_{k=1}^{N}\alpha_k}}{\prod_{k=1}^{N}e(g_1,g_2)^{sy_{k,u}(u)}\cdot e(g_1^{\sum_{k=1}^{N}(\alpha_k-y_{k,u})},g_2^s)}=$$

$$\frac{me(g_1,g_2)^{s\cdot\sum_{k=1}^{N}\alpha_k}}{e(g_1,g_2)^{s\sum_{k=1}^{N}y_{k,u}}\cdot e(g_1^{\sum_{k=1}^{N}(\alpha_k-y_{k,u})},g_2^s)}=$$

$$\frac{me(g_1,g_2)^{s\cdot\sum_{k=1}^{N}\alpha_k}}{e(g_1,g_2)^{s\sum_{k=1}^{N}y_{k,u}}\cdot e(g_1,g_2)^{s\cdot\sum_{k=1}^{N}(\alpha_k-y_{k,u})}}=$$

$$\frac{me(g_1,g_2)^{s\cdot\sum_{k=1}^{N}\alpha_k}}{e(g_1,g_2)^{s\cdot\sum_{k=1}^{N}\alpha_k}}=m$$

如果用户密钥中的访问结构$\{\Gamma_k\}_{k\in[1,\cdots,N]}$不满足密文中属性集合$\{A_k^c\}_{k\in[1,\cdots,N]}$,则用户无法进行有效的解密,恢复不出明文。

3.2　密钥可验证性分析

在每个认证机构 $k\in[1,\cdots,N]$中,对其每个叶子节点提供的验证信息,是在密钥生成过程中用来分享该认证机构的秘密的多项式系数,而该认证机构真正的秘密是 $y_{k,u}$,但用户不能直接获得 $y_{k,u}$的分享,所以第一步要验证式(1)是否成立,目的是确保每个 $D_{k,x}$和 $h_{k,x}$中的 $q_{k,x}(0)$是相同的。然后验证

$$h_{k,x}=h_{k,\text{parent}(x)}\times\prod_{i=1}^{d_{k,x}}(e(g_1,g_2)^{a_{k,i}})^{\text{index}(x)^i}$$

是否成立。如果成立,那么就能够确保每个节点提供的验证信息 $h_{k,x}$确实是由其父节点 $\text{parent}_k(x)$的多项式计算得到的,即 $q_{k,x}(0)=q_{k,\text{parent}(x)}(\text{index}(x))$,保证了 $q_{k,\text{parent}(x)}(0)$是被正确分享的。

如果同根节点的两个授权子结构,以不可忽略的概率恢复出了两个不同的秘密,也就是说,两个授权子结构在重构秘密时,至少有一个是错误的,却通过了以上的验证方程。假设这个根节点为 x,则认证机构 k 构造可计算值为 a_k,满足

$$J_k=e(g_1,g_2)^{a_k}=e(g_1,g_2)^{q_{k,x}(0)}=$$

$$h_{k,\text{parent}(x)}\times\prod_{i=1}^{d_{k,x}}(e(g_1,g_2)^{a_{k,i}})^{\text{index}(x)^i}$$

可得 $\log_{e(g_1,g_2)}J_k=\alpha_k=q_{k,x}(o)$,从而满足可验证性的第一个条件成立。

验证等式 $Y_k=Q'_u\cdot Y_{k,u}$,保证了私钥份额 $Q_{k,u}$的正确性。最后验证 $Y=e(Q_u,g_2)\times\prod_{k=1}^{N}Y_{k,u}$,保证最后恢复出的秘密同 Y 中的指数是相同的。如果所有的验证都通过,则用户私钥正确,可以用来解密密文,满足可验证性的第二个条件。

3.3　安全性分析

1)抗共谋攻击

在本文方案中,系统主密钥直接由各个认证机构产生的主密钥份额组成,不影响系统的抗共谋能力,使不合法用户共谋时,仍无法解密密文。

分析:假设系统中只有两个认证机构,1 号和 2 号。用户甲有足够的属性可以从 1 号认证机构获得解密密钥份额:

$$D_{1,x}=g_1^{q_{1,x}(0)}\cdot F_1(i)^{r_{1,x}},i=\text{att}(x)$$

$$R_{1,x}=g_2^{r_{1,x}}$$

但没有足够的属性从 2 号认证机构获得解密密钥份额;类似的用户乙有足够的属性可以从 2 号认证机构获得解密密钥份额

$$D_{2,x}=g_1^{q_{2,x}(0)}\cdot F_2(i)^{r_{2,x}},i=\text{att}(x)$$

$$R_{2,x}=g_2^{r_{2,x}}$$

但没有足够的属性从 1 号认证机构获得解密密钥份额。

甲乙共谋想要来解密密文,则必须要求出 $Y^s=e(g_1,g_2)^{s(\alpha_1+\alpha_2)}$才能成功解密。甲可以进行解密得 $e(g_1,g_2)^{sq_{1,r}(0)}=e(g_1,g_2)^{sy_{1,甲}(u)}$;乙可以进行解密得 $e(g_1,g_2)^{sq_{2,r}(0)}=e(g_1,g_2)^{sy_{2,甲}(u)}$。双方共谋可得 $P=e(g_1,g_2)^{sy_{1,甲}(u)}\cdot e(g_1,g_2)^{sy_{2,乙}(u)}=e(g_1,g_2)^{s(y_{1,甲}(u)+y_{2,乙}(u))}$。

此时,即使用户甲获得 $Q_甲=g_1^{(\alpha_1+\alpha_2-y_{1,甲}(u)-y_{2,甲}(u))}$,用户乙获得了 $Q_乙=g_1^{(\alpha_1+\alpha_2-y_{1,乙}(u)-y_{2,乙}(u))}$,能够计算得到

$$Y_甲=e(Q_甲,E_1)=e(g_1,g_2)^{s(\alpha_1+\alpha_2-y_{1,甲}(u)-y_{2,甲}(u))}$$

$$Y_乙=e(Q_乙,E_1)=e(g_1,g_2)^{s(\alpha_1+\alpha_2-y_{1,乙}(u)-y_{2,乙}(u))}$$

但用户仍无法求得 $e(g_1,g_2)^{sy_{2,甲}}$和 $e(g_1,g_2)^{sy_{1,乙}}$,从而无法得到 $Y^s=e(g_1,g_2)^{s(\alpha_1+\alpha_2)}$,无法共谋来解密密文。

同理可得,N 个认证机构的多个用户共谋时,无法求得 Y^s不能解密密文。综上,本文方案具有抗共谋攻击的安全性。

2)在本文方案中,N 个认证机构只要保证其中一个是诚实可靠的,该系统就能达到安全,最多能容忍 $N-1$ 个认证中心被破坏。

分析:假设这个诚实可信的认证中心为 1 号认证中心,拥有的私钥为$\{y_1,s_1\}$,其他认证中心被破坏,泄露出其私密信息$\{y_k,s_k\}_{k\in[2,\cdots,N]}$。

攻击者想要解密密文,就必须要知道 Y^s,因 $Y^S=e(g_1,g_2)^{s\sum_k y_{k,u}}\cdot e(g_1,g_2)^{s\sum_k(\alpha_k-y_{k,u})}$,其中 $e(g_1,g_2)^{s\sum_k(\alpha_k-y_{k,u})}$可以由 E_1 和 Q_u 计算得到,要求 $e(g_1,g_2)^{s\sum_k y_{k,u}}$,即只需知道 $g_1^{\sum_{k=1}^{N}y_{k,u}}$便可解密密文。其中 $\sum_{k=2}^{N}y_{k,u}$已获得,则只要知道

$g_1^{y1,u}$ 即可解密。因 1 号认证中心是诚实可靠的,攻击者无法得知 y_1,即便可得到 $g_u^{\alpha_k - y_{k,u}}$,但基于离散对数困难问题,无法求出 $\alpha_k - y_{k,u}$,从而无法计算出 $g_1^{y1,u}$,因此攻击者求不出 Y^*,恢复不出明文。

另外,本方案的安全证明游戏基于的假设为不存在多项式时间 t 内以大于 $\varepsilon/2$ 的概率解决 DBDH 或 q-DDHI 问题。

证明　利用类似文献[7]中的证明方法,并基于其安全模型进行了适当的修正:因本方案无中央认证机构,所以在密钥查询阶段无须对中央认证机构进行密钥查询;同时需在密钥查询阶段增加验证信息查询和验证查询。当挑战者在构造合法密钥时,在各个认证机构中,类似单认证机构[5]中的方法,可以计算出与密钥

$$Q_u = \prod_{k=1}^{N} Q_{k,u} = g_1^{\sum_{k=1}^{N}(\alpha_k - y_{k,u})}$$

$$D_{k,x} = g_1^{q_{k,x}(0)} \cdot F_k(i)^{\gamma_{k,x}} \quad i = \mathrm{att}(x)$$

$$R_{k,x} = g_2^{r_{k,x}}$$

不可区分的值。同时,在各个认证机构中,多项式的系数是一定有的,相应地,$g_1^{q_{k,x}(0)}$ 也能被计算得到,从而在各个认证机构模拟合法密钥时所需要的验证信息都可被模拟出来,并通过验证,因而在本方案安全模型下需要模拟的信息都可被挑战者模拟出来。最后类似文献[7]能以不可忽略的概率赢得 DBDH 游戏,导致矛盾,从而本方案达到 DBDH 下的语义安全。

4　结束语

本文给出了一种无中央认证机构的多认证机构可验证的属性基加密方案,克服了单一的认证机构被攻破将会泄露其中所有信息的风险,且不需要中央认证机构,增强了安全性,当系统在增加新的认证机构时,所有旧的认证机构都无须更改用户的私钥,减少了开销;同时该方案可验证密钥和密文的正确性,当检验出错时可准确定位到出错方并要求重发相应部分的信息。

参考文献:

[1] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]//Advances in Cryptology-EUROCRYPT 2005. Berlin: Springer-Verlag, 2005: 457-473.

[2] GOYAL V, PANDEY O, SAHAI A, *et al*. Attribute-based encryption for fine-grained access control of encrypted data[C]//Proc of ACM Conference on Computer and Communications Security. New York: ACM Press, 2006:89-98.

[3] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]//Proc of IEEE Symposium on Security and Privacy. Oakland:IEEE Computer Society, 2007: 321-334.

[4] WATERS B. Ciphertext-policy attribute-based encryption:an expressive, efficient, and provably secure realization[C]//Proc of Public Key Cryptography-PKC 2011. New York: Springer-Verlag, 2011:53-70.

[5] 陈和风. 基于特征的加密方案[D]. 厦门:厦门大学,2008.

[6] ATTRAPADUNG N, IMAI H. Dual-policy attribute based encryption[C]//Proc of Applied Cryptography and Network Security Conference. Berlin: Springer-Verlag, 2009:168-185.

[7] CHASE M. Multi-authority attribute based encryption[C]//Proc of Theory of Cryptography. Berlin: Springer-Verlag, 2007:515-534.

[8] LIN Huang, CAO Zhen-fu, LIANG Xiao-hui, *et al*. Secure threshold multi-authority attribute based encry ption without a central authority [C]//Proc of Cryptology in India-INDOCRYPT 2008. Berlin:Springer-Verlag, 2008:426-436.

[9] CHASE M, CHOW S S M. Improving privacy and security in multi-authority attribute-based encryption[C]//Proc of the ACM Conference on Computer and Communications Security. New York: ACM Press, 2009:121-130.

[10] TANG Qiang, JI Dong-yao. Verifiable attribute based encryption[J]. International Journal of Network Security,2010,10(2):114-120.

(上接第 304 页)接信任度、推荐信任度、风险信任因子、激励因子、惩罚因子、实体活跃度六个因素作为综合信任关系的典型属性,提出了一种基于动态信息增益的多维属性融合方法。根据信息熵和信息增益,客观地从样本获取信任决策对各属性依赖的程度差异,使总体信任度计算模型中各决策属性权值保持相对固定。同时,通过新的交易样本,对属性权值自适应地更新,以适应网络节点行为的动态变化。算法分析表明:直接信任度、推荐信任度、风险信任因子、激励因子、惩罚因子、实体活跃度在 OTD 模型中的权重近似服从6:2:6:1:1:2的比例关系,在此相对比例基础上可动态调节;OTD 模型对决策属性能够进行有效区分。

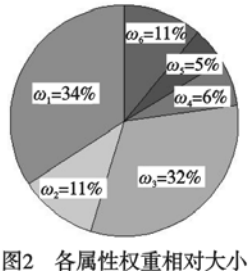

图2　各属性权重相对大小

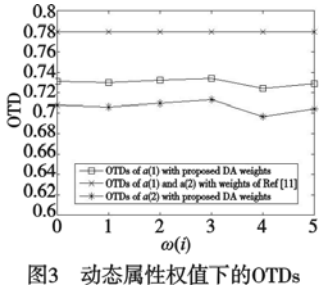

图3　动态属性权值下的OTDs

参考文献:

[1] 李勇军,代亚非. 对等网络信任机制研究[J]. 计算机学报,2010,33(3):390-405.

[2] 李小勇,桂小林. 大规模分布式环境下动态信任模型研究[J]. 软件学报,2007,18(6):1510-1521.

[3] ZHOU Rong-fang, HWANG K. Power-Trust: a robust and scalable reputation system for trusted peer-to-peer computing[J]. IEEE Trans on Parallel and Distributed Systems,2007,18(4):450-473.

[4] JAMEEL H, HANG L X, KALIM U, *et al*. A trust model for ubiquitous systems based on vectors of trust values[C]//Proc of the 7th IEEE International Symposium on Multimedia. Washington DC: IEEE Computer Society Press,2005:674-679.

[5] THEODORAKOPOULOS G, BARAS J S. On trust models and trust evaluation metrics for Ad-hoc networks[J]. IEEE Journal on Selected Areas in Communications,2006,24(2):318-328.

[6] SUN Yan, YU Wei, HAN Zhu, *et al*. Trust modeling and evaluation in Ad hoc networks[C]//Proc of Global Telecommunications Conference. Washington DC: IEEE Computer Society Press,2005:1-10.

[7] 田春岐,邹仕洪,田慧蓉,等. 一种基于信誉和风险评价的分布式 P2P 信任模型[J]. 电子与信息学报,2007,29(7):1628-1682.

[8] HE R, NIU J W, ZHANG G W. CBTW: a trust model with uncertainty quantification and reasoning for pervasive computing[C]//Proc of the 3rd International Symposium on Parallel and Distributed Processing and Applications-ISPA 2005 Workshops. Berlin:Springer-Verlag,2005:541-552.

[9] 田春岐,邹仕洪,王文东,等. 一种基于推荐证据的有效抗攻击 P2P 网络信任模型[J]. 计算机学报,2008,31(2): 270-281.

[10] 李明楚,杨彬,钟炜,等. 基于反馈机制的网格动态授权新模型[J]. 计算机学报,2009,32(11):2187-2199.

[11] 李小勇,桂小林. 可信网络中基于多维决策属性的信任量化模型[J]. 计算机学报,2009,32(3):405-416.