支持大属性空间和安全分级的KP-ABE

康 萍[1],赵开强[1],刘 彬[1],郭 真[1],冯朝胜[1,2],卿 昱[3]
(1. 四川师范大学计算机科学学院,四川成都 610101; 2. 电子科技大学网络与数据安全四川省重点实验室,四川成都 610054;
3. 中国电子科技集团公司第30研究所,四川成都 610041)

摘 要: 现有的KP-ABE(Key-Policy Attribute-Based Encryption)方案主要通过哈希函数实现对大属性空间的支持,安全性建立在随机预言模型下而非标准模型下;计算每个属性对应的密文子项或密钥子项,指数运算次数大于最大加密属性个数;不支持数据和用户安全分级. 针对上述问题,本文提出了一种支持大属性空间和安全分级的KP-ABE方案. 该方案通过编码函数而不是哈希函数将任意"属性名称:属性值"编码映射至有限域中的一个元素,实现对任意"属性名称:属性值"的支持并确保任意两个不同"属性名称:属性值"的编码值不同;结合强制访问控制思想,方案对密文和用户赋予不同的安全等级,只有用户安全等级不低于密文的安全等级时用户才能解密. 最后对本文方案进行了安全性和性能分析,在标准模型下证明了该方案针对选择明文攻击是安全的;性能分析表明,所提出方案只需要进行2次指数运算,就能完成一个属性对应的密文子项或密钥子项的计算.

关键词: KP-ABE;大属性空间;选择明文攻击;强制访问控制;安全分级
基金项目: 国家自然科学基金(No.61373163);国防科技重点实验室基金(No.6142103010709)
中图分类号: TP309.2 **文献标识码:** A **文章编号:** 0372-2112(2023)09-2549-09
电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20210493

A KP-ABE Scheme Supporting Large Universe and Security Classification

KANG Ping[1], ZHAO Kai-qiang[1], LIU Bin[1], GUO Zhen[1], FENG Chao-sheng[1,2], QING Yu[3]
(1. *College of Computer Science, Sichuan Normal University, Chengdu, Sichuan* 610101, *China*;
2. *Network and Data Security Key Laboratory of Sichuan Province, University of Electronic Science and Technology of China, Chengdu, Sichuan* 610054, *China*;
3. *The No.*30 *Institute of China Electronic Technology Corporation, Chengdu, Sichuan* 610041, *China*)

Abstract: The existing KP-ABE (Key-Policy Attribute-Based Encryption) scheme mainly supports large universe by using hash function, and the security is built under the random oracle model instead of the standard model; the number of exponentiation operations is greater than the maximum number of attributes at the time of encryption when calculating the ciphertext components or key components for each attribute; it does not support data and user security classification. To address the above problems, this paper proposes a KP-ABE scheme that supports large universe and security classification. The scheme maps arbitrary "attribute name: attribute value" to an element in the finite field through an encoding function instead of hash function, enabling support for any "attribute name: attribute value" and ensuring that any two different "attribute name: attribute value" combinations are encoded with different values; combined with the idea of mandatory access control, the scheme assigns different security levels to ciphertext and user, and only when the user security level is not lower than the security level of the ciphertext can the user decrypt it. The scheme is proved to be secure against chosen plaintext attacks under the standard model; the performance analysis shows that the proposed scheme only needs to perform two exponential operations to complete the computation of the ciphertext components or key components corresponding to one attribute.

Key words: KP-ABE; large universe; chosen plaintext attack; mandatory access control; security classification
Foundation Item(s): National Natural Science Foundation of China (No.61373163); National Defense Science and Technology Foundation of Key Laboratory (No.6142103010709)

收稿日期:2021-04-16;修回日期:2022-04-10;责任编辑:梅志强

1 引言

云计算技术能够有效解决本地计算能力和存储能力不足的问题[1],但带来新的问题——如何确保外包数据的机密性和隐私性. 加密是解决该问题的一种有效方法[2],然而,传统的加密方法虽然能够保证用户数据的机密性和隐私性,却无法在云环境中实现数据的高效共享和细粒度访问. 针对这一问题,基于属性加密(Attribute-Based Encryption, ABE)方法被提出[3]. 随后,Goyal和Bethencourt针对应用场景的不同,分别提出了密钥策略基于属性加密方案[4](Key-Policy Attribute-Based Encryption, KP-ABE)和密文策略基于属性加密方案[5](Ciphertext-Policy Attribute-Based Encryption, CP-ABE). 现有的KP-ABE方案仍然存在如下问题:(1)安全假设条件较强;(2)不支持安全分级. 针对上述问题,本文设计编码函数重新定义域Z_p到群G_0的映射,解决了安全假设条件较强的问题,使方案在标准模型下能抵御针对性选择明文攻击(selective Chosen Plaintext Attack, sCPA);提出了一种安全分级方法,通过对用户和数据密文赋予不同的安全等级,在密文属性满足共享访问策略且用户安全等级不低于密文安全等级时才能解密.

2006年,Goyal等[4]所构造的大属性空间方案公开参数与n值有关,在密钥生成和加密时计算开销与n值呈正相关. 2010年,Waters等[6]提出的大属性空间构造方案并没有给出使用的散列函数的具体形式,且没有证明方案的正确性与安全性. 2011年,Lewko等[7]首次提出了无界的支持大属性空间构造的KP-ABE方案,该方案构造基于复合阶群,相比素数阶群需要更大的计算开销和存储开销. 2012年,Okamoto等[8]使用特殊的向量子空间(称为对偶向量空间)框架,提出了第一个在标准模型下完全安全的无界的支持大属性空间构造的KP-ABE方案. 2013年,Rouselakis和Waters[9]提出的方案共享访问策略由线性秘密共享方案LSSS[10,11]表示,虽然方案中表示能支持任意属性值,但在具体方案中并没有给出任意字符串到域Z_p的具体映射方式. Lewko等[12]基于文献[13~16],提出的方案表明实际上可以通过创建特殊的向量子空间(称为对偶向量空间)来模拟复合阶群的效果,并在素数阶群上构造一个支持大属性空间构造的KP-ABE方案,虽然能提高效率,但在性能上有明显损失. 2020年,Zhang等[17]通过将任意属性值映射到群G_0中来实现大属性空间构造,但是该方案的安全性证明不全面. 同年,晋云霞等[18]根据解密特点设计并行化解密算法,将大部分解密计算外包到Spark平台,有效提高了云端解密效率. 杨贺昆等[19]将属性相关密钥子项外包,将共享密文子项的一半计算任务外包,并对所有的外包结果进行了验证.

2 属性编码与安全分级

2.1 属性编码

本文设计了一种新的编码方法,通过对"属性名称:属性值"进行特定规则的编码,使用编码函数代替哈希函数,解决了安全性方面安全假设条件较强的问题. 定义系统的具体编码规则如图1所示.

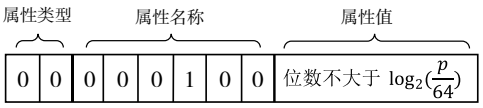

图1 属性编码

(1) 使用一个字节对所有属性名称进行编码,前两位用来标识属性类型,后六位采用000000~111111之间的编码用来唯一表示属性名称:

(a)如果属性为字符串属性,则前两位用00标识.

(b)如果属性为数值属性(例如年龄),则前两位用01标识.

(c)如果属性为布尔属性(例如性别),只有两种状态,则前两位使用10标识.

(2) 针对属性值,采用以下方式进行编码:

(a)如果属性为字符串属性,则系统采用Unicode编码将任意的属性值转换为n位二进制字符串,但需满足$2^{(n+6)}<p$.

(b)如果属性为数值属性,则系统直接将数值属性值转化为二进制字符串,但需满足该数值属性的值小于$p/64$.

(c)如果属性为布尔属性,只有两种状态,则系统只需要一位即可编码该属性值.

(3) 拼接属性名称和属性值的二进制编码,并将其转换为域Z_p内的值;

现就医疗系统应用场景举例说明该编码的使用方式,将系统所有可能用到的属性名称进行编码,如表1所示.

2.2 安全分级

《中华人民共和国保守国家秘密法》规定将国家秘密的密级分为"绝密"、"机密"、"秘密"三个等级,同理,为了保证数据的安全,可以为数据赋予不同的安全等级,如图2所示,安全用户可以是绝密用户、机密用户、秘密用户、敏感用户等具有不同安全等级的用户,数据也可以具有不同的安全等级,只有具有较高安全等级的用户可以访问较低安全等级的数据,而安全等级低于数据安全等级的用户不能访问该数据,即不能向上访问.

针对用户,引入安全等级属性ξ,修改共享访问树,并添加与属性ξ相关联的叶子节点,对属性ξ分配多个

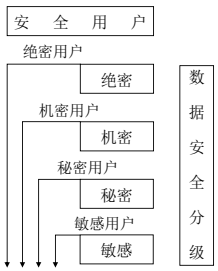

图2　数据安全分级

表1　属性名称编码

属性名称	编码值
姓名	**00**000000
年龄	**01**000000
性别	**10**000000
部门	**00**000100
医疗机构	**00**000001
门诊号	**01**000001
病案号	**01**000010
ID号	**01**000100
职称	**00**000010
科室	**00**000011
日期	**01**000011

与等级相关的密钥子项,当且仅当数据密文相关联属性满足共享访问树且用户安全等级不低于数据密文安全等级时,用户才能解密. 具体的共享访问树修改如图3所示.

3　系统模型

3.1　系统框架

本文的系统框架如图4所示,主要包括4个实体:(1)中央授权机构(Central Authority, CA):一个完全可信的实体,负责初始化和生成用户私钥;(2)云服务提供商(Cloud Service Provider, CSP):半可信实体,接收用户发送过来的存储请求并将数据进行存储;(3)数据所有者(Data Owner, DO):数据的提供者,DO在进行加密前需要定义与密文相关的属性集合,最后将共享密文上传到CSP;(4)数据消费者(Data User, DU):云存储中数据文件的访问者,从CA获取属于自己的私钥,并从CSP中下载需要的共享密文,然后进行解密操作.

3.2　安全模型

sCPA安全模型定义如下.

Init:敌手A声明想要挑战的属性集合S.

Setup:挑战者B运行Setup算法,并把系统公共参数发送给敌手A.

Phase 1:允许敌手A查询属性集合S不满足访问结构T的密钥.

Challenge:敌手A提交两个长度相等的消息M_0, M_1,挑战者B从M_0和M_1中随机选择一条明文消息M_b,并基于属性集合S和系统公钥PK加密M_b得到密文CT^*,然后把密文CT^*传递给敌手A.

Phase 2:重复Phase 1操作.

Guess:敌手A输出b的猜想b'.

在该游戏中敌手A的优势为:

$$\varepsilon = P_r[b' = b] - \frac{1}{2}$$

在上述游戏中,若敌手A在任何概率多项式时间内的攻击优势可忽略,则方案是安全的.

4　方案构造

(1) Setup$(1^\lambda, n)$.

选择阶为素数p的双线性群G_0、G_T,记G_0的生成元为g,定义双线性映射$e: G_0 \times G_0 \to G_T$. 对于任何$A = \left\{a_i \middle| a_i \in Z_p, 1 \leqslant i \leqslant m, i \in Z_p\right\}$,拉格朗日系数定义为:$\Delta_{i,A}(x) = \prod_{j \in A, j \neq i} \frac{x-j}{i-j}$. 设加密数据的属性的数量不超过$n$,随机选择$a, \alpha, \beta_i \in Z_p, g_2 \in G_0$,计算$g_1 = g^\alpha, g_3 = g^a, h_i = g^{\beta_i}$,其中$i \in [1, m]$,$\beta_1$到$\beta_m$代表安全等级. 定义编码函数$h(x)$,将任意属性值映射到域$Z_p$中的一个元素,再定义函数$H(x) = g_2^{\rho(h(x))} g_3^{h(x)}$,其中$\rho(\cdot)$为$n+1$次随机多项式. 算法输出公钥PK和主密钥MSK:

$$\mathrm{PK} = \left(G_0, G_T, g, g_1, g_2, g_3, h, h_i, H, e\right)$$

$$\mathrm{MSK} = (\alpha, a)$$

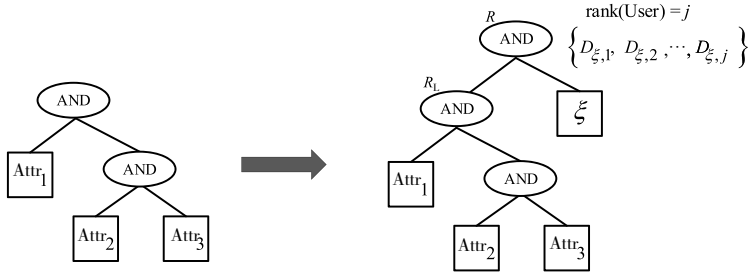

图3　支持安全分级的共享访问树

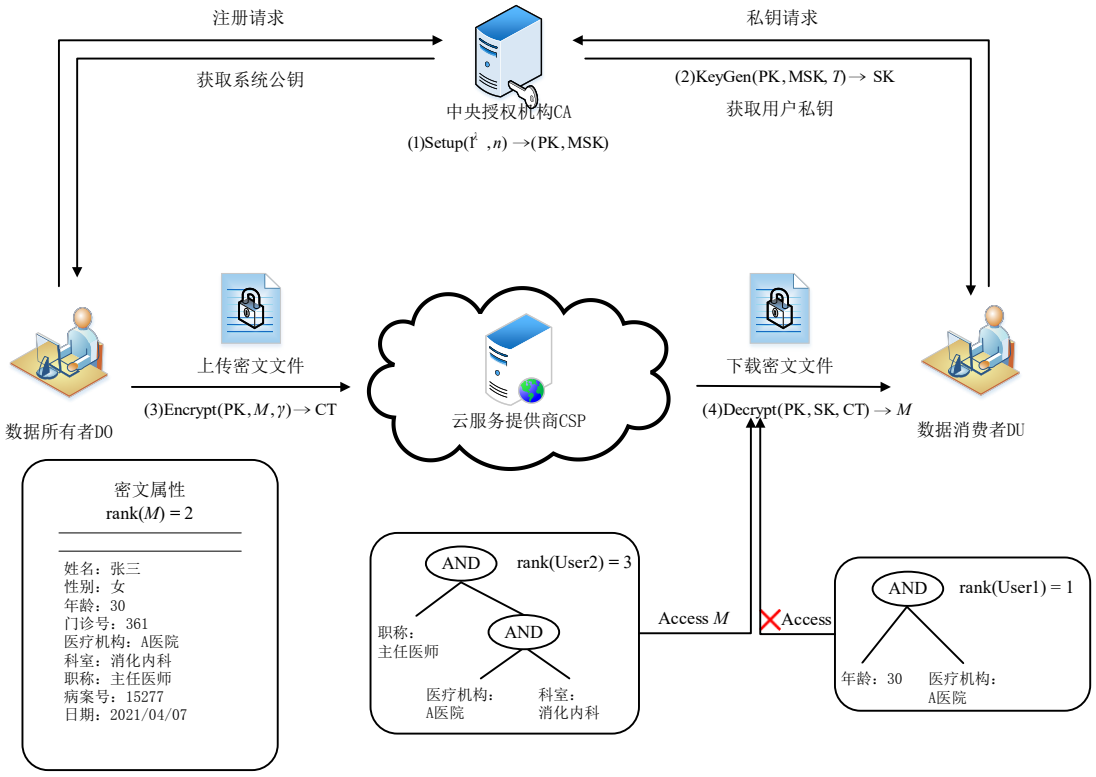

图4 支持大属性空间和安全分级的KP-ABE系统框架

（2）KeyGen(PK, MSK, T).

首先为共享访问树 T 中的每一个节点 x 选择一个随机多项式 q_x，从根节点 R 开始，对于树 T 中每个节点 x，其多项式 q_x 的阶 $q_x=k_x-1$（k_x 表示门限值），令根节点 $q_R(0)=\alpha$，并随机选择 d_R 个点完整定义 q_R. 令 $q_x(0)=q_{\text{parent}(x)}(\text{index}(x))$，并随机选择 d_x 个点完整定义 q_x.

对于具有安全等级的用户，设用户安全等级总共为 m 级，m 代表最高等级，1代表最低等级. 如图3所示，假设用户能够解密到第 $j(j\leqslant m)$ 级文件，即用户安全等级为 j. 对于所有 $i\in[1,j]$，随机选择 $r_{\xi,i}\in Z_p$，计算 $D_{\xi,i}=g_2^{q_\xi(0)}(h_i)^{r_{\xi,i}}$，$D'_{\xi,i}=g^{r_{\xi,i}}$，其中 $q_\xi(0)$ 为安全等级节点所分得的秘密值. 对于每个叶子节点 $y\in L_T$（其中 L_T 为除安全等级节点以外的其他叶子节点集合），随机选择 $r_y\in Z_p$，计算 $D_y=g_2^{q_y(0)}\left(g_2^{\rho(h(x))}g_3^{h(x)}\right)^{r_y}$，$D'_y=g^{r_y}$.

最终的用户私钥为：

$$\text{SK}_j^u=\left(\left\{D_{\xi,i}\right\}_{i\in[1,j]},\left\{D'_{\xi,i}\right\}_{i\in[1,j]},\left\{D_y\right\}_{y\in L_T},\left\{D'_y\right\}_{y\in L_T}\right)$$

（3）Encrypt(PK, M, γ).

随机选择 $s\in Z_p$，定义函数 rank(M) 表示 M 的安全等级，因此 rank(M) $\in[1,m]$，计算 $E'=\text{Me}(g_1,g_2)^s$，$\bar{E}=g^s$，$\hat{E}=h^s_{\text{rank}(M)}$. $\forall\tau\in\gamma$，计算 $E_\tau=H(\tau)^s=\left(g_2^{\rho(h(\tau))}g_3^{h(\tau)}\right)^s$，最终的密文为：

$$\text{CT}=\left(\gamma,E',\bar{E},\hat{E},\left\{E_\tau\right\}_{\forall\tau\in\gamma}\right)$$

（4）Decrypt(PK, SK, CT).

定义递归函数 DecryptNode(CT, SK, y)，输出 G_T 上的一个群元素或 $\perp$. 具体解密过程如下：

①如果 y 是除安全等级节点以外的其他叶子节点，令 $\tau=\text{att}(y)$，当 $\tau\in\gamma$ 时，

$$\text{DecryptNode}(\text{CT},\text{SK},y)=\frac{e\left(D_y,\bar{E}\right)}{e\left(D'_y,E_\tau\right)}$$

$$=\frac{e\left(g_2^{q_y(0)}\left(g_2^{\rho\left(h\left(\text{att}(y)\right)\right)}g_3^{h\left(\text{att}(y)\right)}\right)^{r_y},g^s\right)}{e\left(g^{r_y},\left(g_2^{\rho(h(\tau))}g_3^{h(\tau)}\right)^s\right)}=e\left(g_2,g\right)^{sq_y(0)}$$

②如果 y 是非叶子节点，对于 y 的所有孩子节点 z，都调用函数 DecryptNode(CT, SK, z)，并将其输出记为 F_z，设每个 $F_z\neq\perp$，令 S_y 表示任意 k_y 个 y 的孩子节点集合，其中 $S_y'=\left\{\text{index}(z)\middle|z\in S_y\right\}$，$i=\text{index}(z)$，计算：

$$F_y=\prod_{z\in S_y}F_z^{\Delta_{i,S_y'}(0)}=\prod_{z\in S_y}\left(e\left(g_2,g\right)^{sq_z(0)}\right)^{\Delta_{i,S_y'}(0)}$$
$$=\prod_{z\in S_y}\left(e\left(g_2,g\right)^{sq_{\text{parent}(z)}(\text{index}(z))}\right)^{\Delta_{i,S_y'}(0)}$$
$$=\prod_{z\in S_y}\left(e\left(g_2,g\right)^{sq_y(i)}\right)^{\Delta_{i,S_y'}(0)}=e\left(g_2,g\right)^{sq_y(0)}$$

如图3所示,若能解密$F_{R_L}=e\left(g_2,g\right)^{sq_{R_L}(0)}$且用户安全等级能达到密文安全等级,则用户能解密第$t$级的文件,其中$\text{rank}(M)=t(t\leqslant j)$,可计算出:

$$F_\xi=\frac{e\left(D_{\xi,t},\bar{E}\right)}{e\left(D'_{\xi,t},\hat{E}\right)}=\frac{e\left(g_2^{q_\xi(0)}\left(h_t\right)^{r_{\xi,t}},g^s\right)}{e\left(g^{r_{\xi,t}},h^s_{\text{rank}(M)}\right)}=e\left(g_2,g\right)^{sq_\xi(0)}$$

最后,将F_{R_L}与F_ξ进行拉格朗日插值即可得到$F_R=e\left(g_2,g\right)^{\alpha s}=e\left(g_1,g_2\right)^s$,从而解密出$M=\dfrac{E'}{F_R}=\dfrac{\text{Me}\left(g_1,g_2\right)^s}{e\left(g_1,g_2\right)^s}$.

5　安全性证明

定理1　如果敌手能在标准模型下攻破本文方案,那么可以构建出模拟器以不可忽略的优势赢得DBDH(Decisional Bilinear Diffie-Hellman)游戏.

证明　假设存在概率多项式时间敌手(算法)A,能以优势ε在标准模型下攻破本文方案,那么可以构建模拟器B,以$\varepsilon/2$的优势进行DBDH游戏,模拟器B执行过程如下.

首先挑战者设置具有有效双线性映射e的群G_0和G_T,其中G_0的生成元为g,挑战者避开模拟器B的视野抛硬币μ,如果$\mu=0$,挑战者设置$(A,B,C,Z)=\left(g^a,g^b,g^c,e\left(g,g\right)^{abc}\right)$,否则设置$(A,B,C,Z)=\left(g^a,g^b,g^c,e\left(g,g\right)^z\right)$,其中$a,b,c,z$为随机数.

Init:模拟器B运行A,A选择想挑战的属性集$S^*=\left\{s_1,s_2,\cdots,s_n\right\}$(映射到域$Z_p$上的对应集合为$\gamma=\left\{h\left(s_1\right),h\left(s_2\right),\cdots,h\left(s_n\right)\right\}$)和数据安全等级$t^*$.

Setup:模拟器B分配公共参数$g_1=A,g_2=B$,设置函数$H(x)=g_2^{\rho(h(x))}g_3^{h(x)}$,按照下述规则选择$n+1$阶多项式$\rho(\cdot)$:若$x\in S^*$,设置$\rho\left(h(x)\right)=0$,若$x\notin S^*$,则$\rho\left(h(x)\right)\neq0$.因此$H(x)=g_2^{\rho(h(x))}g_3^{h(x)}=g_3^{h(x)}$.设$\rho\left(\beta_{t^*}\right)=0,h_{t^*}=g_2^{\rho\left(\beta_{t^*}\right)}g^{\beta_{t^*}}=g^{\beta_{t^*}}$.

Phase 1:敌手发起如下查询.敌手A对多个共享访问策略发出密钥查询请求,且要求属性集S^*和$\left\{t^*\right\}$的并集不满足任何一个共享访问策略.假设A请求共享访问策略T的密钥且$T_x\left(S^*\cup\left\{t^*\right\}\right)=0$,为了生成密钥,B需要为$T$的每个非叶子节点分配多项式$q_x$,使用文献[4]的小属性空间构造证明中的函数PolySat和PolyUnsat,模拟器运行$\text{PolyUnsat}\left(T,S^*\cup\left\{t^*\right\},A\right)$,该函数为$T$的每一个节点$x$定义一个多项式$q_x$且$q_r(0)=a$.对于每个叶子节点$x$,如果$x$对应属性满足共享访问树,则可得到$q_x(0)$,不满足则至少可得到$g^{q_x(0)}$.

(1)如果与叶子节点x关联的是普通属性,令$i=\text{att}(x)$,x的密钥项为:

如果$i\in S^*$,$D_x=g_2^{q_x(0)}H(i)^{r_x}=g_2^{q_x(0)}g_3^{h(x)r_x}$,$R_x=g^{r_x}$,其中$r_x$从$Z_p$中随机选择.

如果$i\notin S^*$,设$g_4=g^{q_x(0)}$,$D_x=g_4^{\frac{-ah(i)}{\rho(h(i))}}\left(g_2^{\rho(h(i))}g_3^{h(i)}\right)^{r_x'}$
$=g_4^{\frac{-ah(i)}{\rho(h(i))}}\left(g_2^{\rho(h(i))}g^{ah(i)}\right)^{r_x'}=g^{\frac{-q_x(0)ah(i)}{\rho(h(i))}}\left(g_2^{\rho(h(i))}g^{ah(i)}\right)^{r_x'}$
$=g_2^{q_x(0)}\left(g_2^{\rho(h(i))}g^{ah(i)}\right)^{\frac{-q_x(0)}{\rho(h(i))}}\left(g_2^{\rho(h(i))}g^{ah(i)}\right)^{r_x'}$
$=g_2^{q_x(0)}\left(g_2^{\rho(h(i))}g^{ah(i)}\right)^{r_x'-\frac{q_x(0)}{\rho(h(i))}}=g_2^{q_x(0)}\left(H(i)\right)^{r_x}$,
$R_x=g_4^{\frac{-1}{\rho(h(i))}}g^{r_x'}=g^{r_x'-\frac{q_x(0)}{\rho(h(i))}}=g^{r_x}$,其中$r_x'$从$Z_p$中随机选择且$r_x=r_x'-\dfrac{q_x(0)}{\rho\left(h(i)\right)}$.

(2)如果与叶子节点x关联的是安全等级属性,对应的安全等级为t,x的密钥项为:

如果$t\geqslant t^*$,$\rho\left(\beta_t\right)=0$,$D_x=g_2^{q_x(0)}\left(h_t\right)^{r_x}=g_2^{q_x(0)}\left(g_2^{\rho(\beta_t)}g^{\beta_t}\right)^{r_x}$
$=g_2^{q_x(0)}g^{\beta_t r_x}$,$R_x=g^{r_x}$,其中$r_x$从$Z_p$中随机选择.

如果$t<t^*$,$\rho\left(\beta_t\right)\neq0$,设$g_4=g^{q_x(0)}$,$D_x=g_4^{\frac{-\beta_t}{\rho(\beta_t)}}\left(g_2^{\rho(\beta_t)}g^{\beta_t}\right)^{r_x'}$
$=g^{\frac{-q_x(0)\beta_t}{\rho(\beta_t)}}\left(g_2^{\rho(\beta_t)}g^{\beta_t}\right)^{r_x'}=g_2^{q_x(0)}\left(g_2^{\rho(\beta_t)}g^{\beta_t}\right)^{\frac{-q_x(0)}{\rho(\beta_t)}}\left(g_2^{\rho(\beta_t)}g^{\beta_t}\right)^{r_x'}$
$=g_2^{q_x(0)}\left(g_2^{\rho(\beta_t)}g^{\beta_t}\right)^{r_x'-\frac{q_x(0)}{\rho(\beta_t)}}=g_2^{q_x(0)}\left(h_t\right)^{r_x}$,$R_x=g_4^{\frac{-1}{\rho(\beta_t)}}g^{r_x'}=$
$g^{r_x'-\frac{q_x(0)}{\rho(\beta_t)}}=g^{r_x}$,其中$r_x'$从$Z_p$中随机选择且$r_x=r_x'-\dfrac{q_x(0)}{\rho\left(\beta_t\right)}$.

因此,模拟器B可以构造一个关联共享访问树T的密钥,且密钥分布与本文原始方案一致.

Challenge:敌手A向模拟器B提交两个长度相等的明文消息m_0,m_1,然后B抛硬币选择$b\in\{0,1\}$,返回待加密消息m_b,输出密文:

$\text{CT}=(S^*\cup\left\{t^*\right\},\ \widetilde{C}=m_bZ,\bar{C}=g^s=C,\hat{C}=h_{t^*}^s=g^{\beta_{t^*}s}=C^{\beta_{t^*}}$,
$\forall x\in S^*:\tilde{C}_x=H(x)^s=\left(g^{ah(x)}\right)^s=C^{ah(x)})$

随机选择$\mu\in\{0,1\}$,如果$\mu=0,Z=e(g,g)^{abc}$,否则$\mu=1,Z=e(g,g)^{z}$.

Phase 2:模拟器B重复Phase 1的操作.

Guess:敌手A输出对b的猜想b'.$\mu=1$时,敌手得不到关于b的信息,因此有$\Pr[b\neq b'|\mu=1]=\frac{1}{2}$. 由于当$b\neq b'$时,模拟器猜测$\mu'=1$,有$\Pr[\mu'=\mu|\mu=1]=\frac{1}{2}$.$\mu=0$时,敌手可以知道$m_b$的密文,敌手在此情形赢得游戏的优势为$\varepsilon$,因此有$\Pr[b=b'|\mu=0]=\frac{1}{2}+\varepsilon$. 由于当$b=b'$时,模拟器猜测$\mu'=0$,有$\Pr[\mu'=\mu|\mu=0]=\frac{1}{2}+\varepsilon$. 因此模拟器在DBDH游戏中总优势为$\frac{1}{2}\Pr[\mu'=\mu|\mu=0]+\frac{1}{2}\Pr[\mu'=\mu|\mu=1]-\frac{1}{2}=\frac{1}{2}\left(\frac{1}{2}+\varepsilon\right)+\frac{1}{2}\cdot\frac{1}{2}-\frac{1}{2}=\frac{1}{2}\varepsilon$.

6 性能分析

6.1 特性分析

对四个方案的特性分析由表2所示.

6.2 性能分析

6.2.1 计算性能分析

授权中心生成用户私钥时,针对关联普通属性的叶子节点,其计算开销为$5N_{\mathrm{p}}E_{G_0}+N_{\mathrm{p}}H_{Z_p}$($N_{\mathrm{p}}$表示共享访问策略的普通属性个数). 设用户的安全等级为l,故授权中心生成一个用户私钥的计算开销为$(5N_{\mathrm{p}}+3l)E_{G_0}+N_pH_{Z_p}$. 数据所有者加密数据时,计算非属性密文子项的计算开销为$2E_{G_0}+E_{G_T}$,计算属性密文子项的计算开销为$3N_{\mathrm{s}}E_{G_0}+N_{\mathrm{s}}H_{Z_p}$($N_{\mathrm{s}}$表示加密属性集合包含的属性个数),因此数据所有者加密时的总计算开销为$(2+3N_{\mathrm{s}})E_{G_0}+E_{G_T}+N_{\mathrm{s}}H_{Z_p}$. 数据消费者在解密时,共享访问树的每个叶子节点需要两次双线性配对运算(假设共享访问策略仅含“AND”门限),其计算开销为$2(N_{\mathrm{p}}+1)B$,对于除根节点的所有节点(包括所有叶子节点)都需要一次指数运算,其计算开销为$(|T|+1)E_{G_T}$($|T|$表示不引入安全叶子节点时共享访问树T的节点个数),故整个解密过程的总计算开销为$(|T|+1)E_{G_T}+2(N_{\mathrm{p}}+1)B$. 本文与其他方案的计算开销对比如表3所示.

6.2.2 存储性能分析

本文主要对用户私钥和密文进行存储性能分析,用$|G_0|$和$|G_T|$表示一个群元素所需存储空间. 对于授权中心生成的私钥,其总密钥存储开销为$2(N_{\mathrm{p}}+l)|G_0|$. 分析数据所有者加密生成的密文,对于非属性密文子项,存储开销为$|G_T|+2|G_0|$,对于与密文属性相关的密文子项,存储开销为$N_{\mathrm{s}}|G_0|$,故总密文存储开销为$|G_T|+(N_{\mathrm{s}}+2)|G_0|$. 本文与其他方案的存储开销对比如表4所示.

表2 特性对比

方案	大属性空间	安全分级	访问结构
文献[4]	√	×	访问树
文献[9]	√	×	LSSS
文献[17]	√	×	访问树
本文方案	√	√	访问树

表3 计算开销对比

方案	私钥生成	加密	解密
文献[4]	$(n+5)N_{\mathrm{p}}E_{G_0}$	$(1+(n+3)N_{\mathrm{s}})E_{G_0}+E_{G_T}$	$(\|T\|-1)E_{G_T}+2N_{\mathrm{p}}B$
文献[9]	$5N_{\mathrm{p}}E_{G_0}$	$(1+4N_{\mathrm{s}})E_{G_0}+E_{G_T}$	$N_{\mathrm{p}}E_{G_T}+3N_{\mathrm{p}}B$
文献[17]	$3N_{\mathrm{p}}E_{G_0}+N_{\mathrm{p}}H_{G_0}$	$(1+N_{\mathrm{s}})E_{G_0}+E_{G_T}+N_{\mathrm{s}}H_{G_0}$	$(\|T\|-1)E_{G_T}+2N_{\mathrm{p}}B$
本文方案	$(5N_{\mathrm{p}}+3l)E_{G_0}+N_{\mathrm{p}}H_{Z_p}$	$(2+3N_{\mathrm{s}})E_{G_0}+E_{G_T}+N_{\mathrm{s}}H_{Z_p}$	$(\|T\|+1)E_{G_T}+2(N_{\mathrm{p}}+1)B$

表4 存储开销对比

方案	用户私钥	数据密文
文献[4]	$2N_{\mathrm{p}}\|G_0\|$	$\|G_T\|+(N_{\mathrm{s}}+1)\|G_0\|$
文献[9]	$3N_{\mathrm{p}}\|G_0\|$	$\|G_T\|+(2N_{\mathrm{s}}+1)\|G_0\|$
文献[17]	$2N_{\mathrm{p}}\|G_0\|$	$\|G_T\|+(N_{\mathrm{s}}+1)\|G_0\|$
本文方案	$2(N_{\mathrm{p}}+l)\|G_0\|$	$\|G_T\|+(N_{\mathrm{s}}+2)\|G_0\|$

6.3 实验分析

实验基于JPBC密码库,使用Eclipse集成开发工具进行,实验平台采用512 bit的A类奇异曲线$y^2=x^3+x$构造160 bit的椭圆曲线群. 实验环境配置为:操作系统Windows 10、内存16 GB、处理器Core™ i5-1035G1(1.19 GHz). 对文献[4,9,17]和本文方案进行了对比,固定加密属性集的属性个数上限$n=50$,哈希函数采用SHA-512,且共享访问策略的每个属性之间的关系都是“AND”,固定用户的安全等级为10来探讨密钥生成时间受共享访问策略中属性增加的影响.

在密钥生成阶段,由于文献[4]受到n值的影响,其计算开销明显高于其他三个方案. 同理,加密趋势和密钥生成一致. 在进行解密时,安全等级属性的引

入导致共享访问树增加了一个叶子节点和一个内部节点,本文方案比文献[4]和文献[17]的解密开销略高但不明显,而文献[9]基于LSSS访问结构,对于每个属性都需要进行三次双线性配对运算,因此文献[9]的解密开销最高. 所有的计算开销对比依次如图5~7所示. 实验在测试密钥存储随共享访问策略属性个数变化时固定用户等级为10,此时本文方案相较于其他方案会多生成20个密钥子项,因此在属性个数较少时本文方案的密钥存储开销是大于其他方案,又由于文献[9]中与属性相关的密钥子项和密文子项都比其他方案多出一项,因此随着属性的增加,文献[9]的存储开销会超过本文方案. 所有的存储开销对比依次如图8和图9所示.

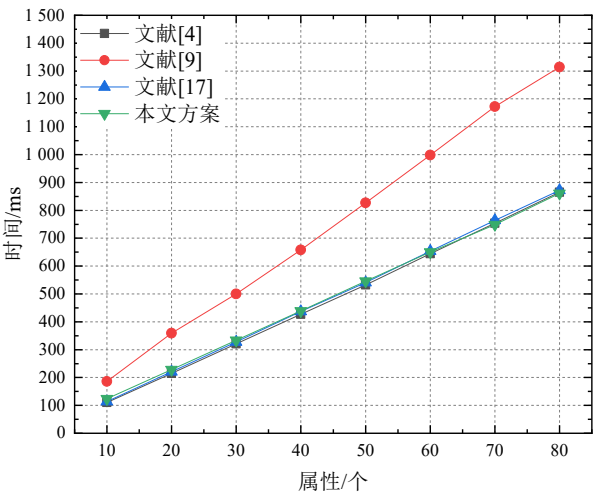

图7　解密计算时间对比图

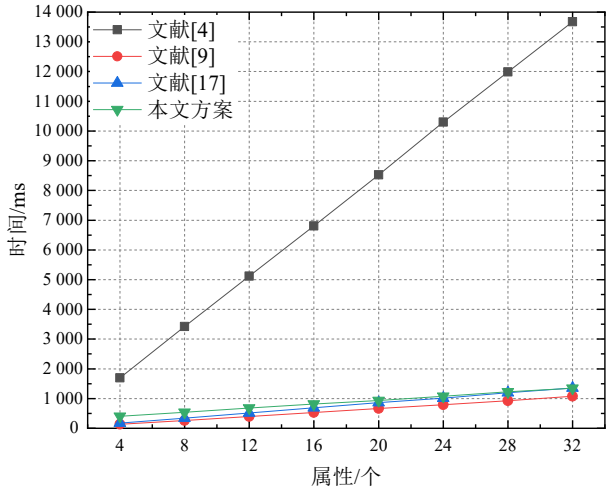

图5　密钥生成计算时间对比图

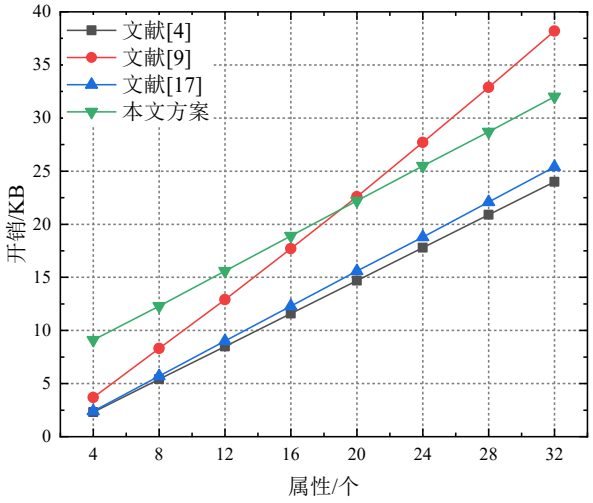

图8　密钥存储开销对比图

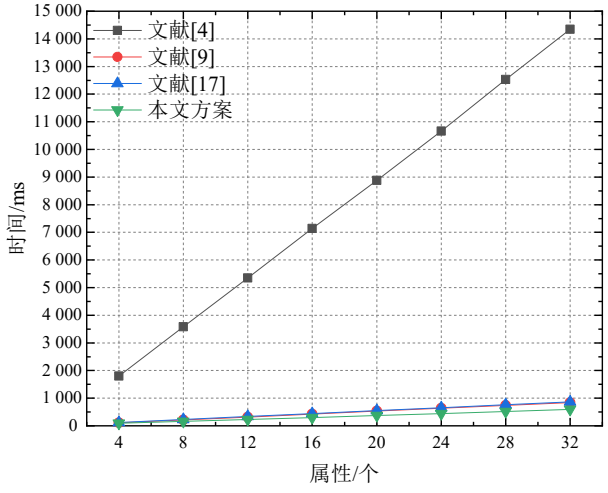

图6　加密计算时间对比图

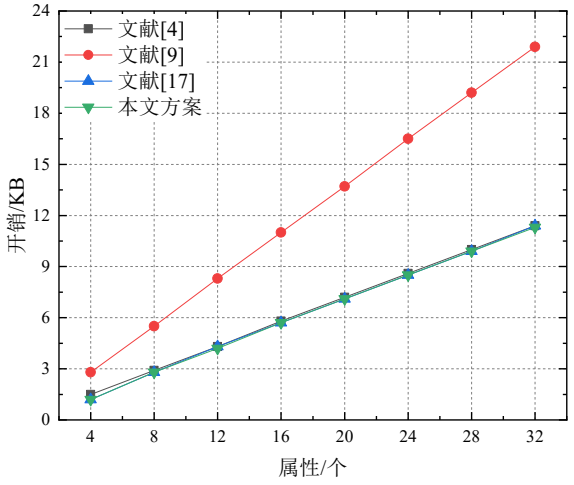

图9　密文存储开销对比图

7 结语

本文采用编码函数代替哈希函数将任意“属性名称:属性值”编码映射至域Z_p中的一个元素,使任意两个不同“属性名称:属性值”的编码值不同,解决了安全性方面安全假设较强的问题. 结合强制访问控制思想,方案引入安全等级属性实现了用户和数据的安全分级. 安全性分析、理论分析和实验分析均表明该方案在不影响效率的同时能在标准模型下抵御针对性选择明文攻击,综合效率更高.

参考文献

[1] 冯朝胜, 秦志光, 袁丁. 云数据安全存储技术[J]. 计算机学报, 2015, 38(1): 150-163.
FENG C S, QIN Z G, YUAN D. Techniques of secure storage for cloud data[J]. Chinese Journal of Computers, 2015, 38(1): 150-163. (in Chinese)

[2] 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, QIN 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)

[3] SAHAI A, WATERS B. Fuzzy identity-based encryption [M]//Lecture Notes in Computer Science. Berlin: Springer Berlin Heidelberg, 2005: 457-473.

[4] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data [C]//CCS' 06: Proceedings of the 13th ACM conference on Computer and communications security. New York: ACM, 2006: 89-98.

[5] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]//2007 IEEE Symposium on Security and Privacy. Piscataway: IEEE, 2007: 321-334.

[6] PIRRETTI M, TRAYNOR P, MCDANIEL P, et al. Secure attribute-based systems[J]. Journal of Computer Security, 2010, 18(5): 799-837.

[7] LEWKO A, WATERS B. Unbounded HIBE and attribute-based encryption[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin,: Springer, 2011: 547-567.

[8] OKAMOTO T, TAKASHIMA K. Fully secure unbounded inner-product and attribute-based encryption[C]//International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2012: 349-366.

[9] ROUSELAKIS Y, WATERS B. New constructions and proof methods for large universe attribute-based encryption [C]//Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. New York: ACM, 2013: 463-474.

[10] BEIMEL A. Secure Schemes for Secret Sharing and Key Distribution[D]. Haifa: Israel Institute of Techono logy, 1996.

[11] KARCHMER M, WIGDERSON A. On span programs [C]//Proceedings of the Eigth Annual Structure in Complexity Theory Conference. Piscataway: IEEE, 1993: 102-111.

[12] LEWKO A. Tools for simulating features of composite order bilinear groups in the prime order setting[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2012: 318-335.

[13] OKAMOTO T, TAKASHIMA K. Homomorphic encryption and signatures from vector decomposition[C]//International Conference on Pairing-Based Cryptography. Berlin: Springer, 2008: 57-74.

[14] OKAMOTO T, TAKASHIMA K. Fully secure functional encryption with general relations from the decisional linear assumption[C]//Annual Cryptology Conference. Berlin: Springer, 2010: 191-208.

[15] LEWKO A, OKAMOTO T, SAHAI A, et al. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2010: 62-91.

[16] FREEMAN D M. Converting pairing-based cryptosystems from composite-order groups to prime-order groups [C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2010: 44-61.

[17] ZHANG K, LIU X M, LI Y P, et al. A secure enhanced key-policy attribute-based temporary keyword search scheme in the cloud[J]. IEEE Access, 2020, 8: 127845-127855.

[18] 晋云霞, 杨贺昆, 冯朝胜, 等. 一种支持解密外包的KP-ABE方案[J]. 电子学报, 2020, 48(3): 561-567.
JIN Y X, YANG H K, FENG C S, et al. A KP-ABE scheme with outsourced decryption[J]. Acta Electronica Sinica, 2020, 48(3): 561-567. (in Chinese)

[19] 杨贺昆, 冯朝胜, 晋云霞, 等. 支持可验证加解密外包的

CP-ABE方案[J]. 电子学报, 2020, 48(8): 1545-1551.
YANG H K, FENG C S, JIN Y X, et al. ACP-ABE scheme with verifiable outsourced encryption and decryption[J]. Acta Electronica Sinica, 2020, 48(8): 1545-1551. (in Chinese)

作者简介

康　萍　女,1998年3月出生于四川南充,四川师范大学在读研究生. 研究方向为信息安全与云计算.
E-mail: iskangping@foxmail.com

赵开强　男,1996年1月出生于四川巴中,四川师范大学在读研究生. 研究方向为信息安全与云计算.
E-mail: 18483621260@163.com

刘　彬　男,1996年10月出生于四川宜宾,四川师范大学在读研究生. 研究方向为区块链、联邦学习与信息安全.
E-mail: liubin10@foxmail.com

郭　真　女,1997年9月出生于四川成都,四川师范大学在读研究生. 研究方向为信息安全与云计算.
E-mail: ssbguo@foxmail.com

冯朝胜(通讯作者)　男,1971年生于四川广元,博士后,教授,硕士生导师. 2010年获得电子科技大学信息与通信工程博士学位. 研究方向为云计算安全.
E-mail: csfenggy@126.com

卿　昱　女,1970年出生于四川,中国电子科技集团公司第三十研究所研究员,硕士生导师. 研究方向为网络与信息安全. 中国电子学会会员编号:E190026299M.