计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2019.20190343
56(10):2151-2159,2019

隐藏访问策略的高效 CP-ABE 方案

王 悦[1,2] 樊 凯[2]
[1](西安文理学院信息工程学院 西安 710065)
[2](西安电子科技大学网络与信息安全学院 西安 710071)
(ywang@xawl.edu.cn)

Effective CP-ABE with Hidden Access Policy

Wang Yue[1,2] and Fan Kai[2]
[1](*School of Information Engineering*, *Xi'an University*, *Xi'an* 710065)
[2](*School of Cyber Engineering*, *Xidian University*, *Xi'an* 710071)

Abstract The development of artificial intelligence depends on the development of cloud computing, at the same time, the security of artificial intelligence is closely related to the security of large data in the cloud. At Present, the ciphertext policy attribute-based encryption (CP-ABE) scheme is considered to be one of the most effective methods to achieve fine-grained access control of data in cloud. In the CP-ABE scheme, the access policy is often associated with the ciphertext. But sometimes, the access policy itself is also the important sensitive information, and access policies stored in the cloud in the form of clear text will also cause the users' data revealed. In response to this problem, an efficient improved CP-ABE scheme is presented, which can hide the access policy. It can make both the attribute hiding and the secret sharing be applied to the AND-gate structure at the same time and then according to the composite order bilinear groups. Therefore, the user's specific attribute value will not be disclosed to any other third party, thus we effectively protect the user's privacy. In addition, through the experimental verification and data analysis, our scheme not only achieves the hidden of complex access structure, but also makes the ciphertext time shortened and decryption efficiency improved.

Key words security of large data; attribute based encryption (ABE); access structure; hidden policy; access control

摘 要 人工智能的发展离不开云计算的支撑,同样,人工智能的安全与云上大数据的安全也是密切相关的.目前,基于密文策略的属性基加密(ciphertext policy attribute-based encryption, CP-ABE)被认为是实现云上数据细粒度访问控制最有效的方法之一.在基于密文策略属性基加密方案中,访问策略与密文相关且绑定,但很多时候,访问策略本身就是敏感信息,若以明文形式存放在云端会造成用户数据的泄露.因此,一种隐藏访问策略的高效 CP-ABE 方案被提出以解决这一问题.它可以使得属性隐藏和秘密共享能够同时应用到"与"门结构中,然后利用合数阶双线性群构造了一种基于包含正负及无关值的"与门"的策略隐藏方案,该方案有效地避免了用户的具体属性值泄露给其他第三方,确保了用户隐私的安全.此外,通过实验验证及分析,保证了该方案在实现复杂访问结构的策略隐藏的同时,还满足解密时间短,解密效率高的优点.

收稿日期:2019-06-06;**修回日期**:2019-08-13
基金项目:国家重点研发计划项目(2017YFB0802300);国家自然科学基金项目(61772403,U1401251);西安市科技计划项目(CXY1352WL30)
This work was supported by the National Key Research and Development Program of China (2017YFB0802300), the National Natural Science Foundation of China (61772403, U1401251), and the Science Technology Plan Project in Xi'an of China (CXY1352WL30).

关键词 大数据安全;属性加密;访问结构;策略隐藏;访问控制

中图法分类号 TP393

随着安全意识的提高,人们对人工智能的安全问题也十分重视.基于云计算和人工智能的密切关系,云上大数据的安全也是人工智能安全的一个重要部分.要解决人工智能安全问题,其中一个方面就是要解决云上大数据的安全.

云计算作为一种新兴的数据交互模式极大地改变了人们的生活方式,通过利用互联网资源池及动态可扩展的虚拟化计算资源,越来越多的人对自己的信息数据进行在线存储、远程共享及云端计算.云计算因此成为学术界乃至产业界的热门与焦点.然而,随着云计算的逐步发展,各种各样的信息、资源等都将被存储在云端,敏感的用户数据被存储在互联网上的第三方,即云服务等提供商,将成为一个趋势.例如用户数据、个人邮件以及一些个人喜好等都被存储在各类门户网站上,比如雅虎以及谷歌等.但是,现在存在一个严重的问题,即在实际生活中云服务提供商不能保证完全可信.早在 2009 年 Gartner 的一份调查就已经反映了这个问题,这份调查报告显示现在 70%以上的企业用户对云计算中的用户的隐私性以及数据的安全性表示怀疑.而近些年不断发生地各类存储服务网站瘫痪及用户文件外泄的事件,更使得用户们对云计算及云存储的安全性有了深深的担忧.因此,现阶段安全问题已经成为制约云计算发展的至关重要的因素.如何实现云环境中用户身份的合法性认证、如何确保云服务中信息的保密性以及用户数据的可靠性授权,都是云计算安全领域急需解决的问题.

近些年关于云计算的应用研究日益增多,云存储技术也受到了越来越多的关注及研究.为了向用户提供数据访问以及存储等功能,云存储尽可能地将网络中的各类存储资源集合起来统筹协作,这样不仅极大地节约了用户的成本,也将资源的利用做到了最大化.然而,云存储中的安全问题,比如如何安全有效地共享信息、用户如何得到安全有效的云存储数据访问策略是现阶段云计算技术急需解决的.目前,国内外已经有很多的云存储服务,例如谷歌的 App Engine 和亚马逊的 Simple Storage Service 等.它们在云存储技术方面已经取得了显著的成果,除此之外在加密、完整性、不可否认性、授权以及身份验证等安全性能方面也做出了不少努力.然而,其仅仅只是对通信过程中的相关协议进行了加密处理,对存储的数据却并没有进行加密操作.同时由于用户无法亲自监管其存储在云端的数据,更使得数据的安全性成为限制云存储发展的主要问题.

由于访问控制的固有特性,基于属性的加密(attribute based encryption, ABE)作为可以有效解决数据安全访问控制的措施之一,受到了业内的广泛关注.Sahai 和 Waters[1] 首先在 2005 年引入了 ABE 的概念,其被认为是一种有效的加密和访问控制方式.属性基加密(ABE)方案主要包括密钥策略(KP-ABE)和密文策略(CP-ABE)两种类型,在 KP-ABE[2] 方案中,密钥与访问结构密切关联,密文与属性集合密切关联,具有秘密密钥的用户只能解密由秘密密钥的访问策略指定的密文;而 CP-ABE[3] 方案中,密文与访问结构密切关联,密钥与属性集合关联,只有当属性满足访问结构时,用户才能成功解密密文.由此看来,CP-ABE 方案非常适合分布式云存储及解密方不确定的环境,它利用用户的相关属性以及对象间的相互信任关系作为授权依据,并由此来设计访问结构.

然而,在密文策略属性基加密方案中,访问策略与密文密切相关,十分容易暴露,并可能导致用户敏感信息的泄露.例如一个健康组织想向所有携带某些疾病的患者发送一个信息.其中,属性 Universe 包含所有疾病,访问策略包含"++-**+"这种格式.其中"+"("-")表示特定疾病的阳性(阴性),"*"表示无关紧要.如果 CP-ABE 方案不能隐藏访问策略,那么从一个人是否可以解密该消息,我们就可以直接得到一些用户的敏感信息.因此,隐藏方案的访问结构,对保护用户隐私来说至关重要.

1 相关工作

为了保护用户在访问策略中的隐私,Waters 和 Boneh[4] 提出了一种新的加密方案,通过隐藏向量的谓词加密以实现匿名.随后,Katz, Sahai 和 Waters [5] 又提出了一种新的谓词加密方案,它不仅支持内积加密,而且可以实现匿名的 CP-ABE 方案;Nishide 等人[6] 提出了 2 种隐藏访问策略的密文策略 ABE 方案,他们使用包含无关值的多值属性的"与"门作为方案的访问结构;Balu 和 Kuppusamy[7] 提出了另一种隐藏策略的密文策略 ABE 方案,相比

较而言,其访问策略可以得到更加有效的表达.上述这些方案都使用与文献[6]相同的访问结构,但是几乎所有这些方案都是使用 3 种类型的符号(正,负和无关字符)来表示每个属性的可能值,这样的设计在某种程度上是十分冗余的.后来,Lai 等人[8]提出了一种完全安全的 CP-ABE 方案,且它也支持隐藏的策略和无关值,但在其方案中密文大小会随着所有属性的可能值数量的增加而增长,在一定程度上,这便极大地限制了其扩展出更高的性能;Phuong,Yang 和 Susilo[9]提出了一种新的隐藏策略密文属性基加密方案,他们使用"位置"的概念,并实现了密文大小恒定不变,然而,他们的方案在不同的假设条件下都只能被证明是选择安全的;除此之外,Waters[10]首先提出了一种新的方法用以证明加密系统的安全性,即双系统加密,并且还提出完全安全的 IBE 和 HIBE 系统;然后 Lewko 和 Waters[11]提出了一个支持短密文的完全安全的 HIBE 方案;Lewko 等人[12]在 IPE 结构中使用双系统,提出了一个新的 IPE 方案;Okamoto 和 Takashima 等人[13]在双系统条件下提出了第一个完全安全的 ABE 方案;Freeman[14]提出了一个隐藏访问策略的 CP-ABE 方案,并且使用了双系统证明其是完全安全的,但是它们也采用与文献[6]相同的访问结构,导致了大尺寸密文长度和效率的低下.策略隐藏的属性加密一直以来都是人们关注的焦点,到目前为止,已经不断有科研人员提出了实现方案[15-27].

本文的方案是一个专注于实现高效的隐藏策略的 CP-ABE 方案,并可证明它在静态假设下是完全安全的.基于由 Phuong 等人[9]提出的使用不同符号的位置进行转换的思想,本文的 CP-ABE 方案达到了完全安全并实现了可以隐藏访问策略且密文大小短小、低解密成本等十分高效的性能.

本文方案工作的主要贡献归纳有 3 个方面:

1) 进一步研究了基于无关值与门的隐藏访问策略的 CP-ABE 方案,提出了一个高效的可以隐藏访问策略的 CP-ABE 方案.

2) 针对提出的方案进行了安全性分析,明确其具有数据机密性、访问策略的安全性以及抗共谋攻击的特性,确保了方案的安全可靠.

3) 从理论分析与仿真实验 2 方面对方案的效率进行了分析说明,证明了方案在加解密以及密钥生成方面都有较高的效率.

2　预备知识

2.1　合数阶双线性群

本文构建的方案是基于合数阶双线性群的.现使用双线性组,其阶数是 3 个不同素数的乘积.设 $\mathcal{G}$ 是一个算法,它的输入为一个安全参数 1^{λ},且输出为一个元组 $\mathbb{G}=(p_1,p_2,p_3,G,G_T,e)$,其中,$p_1$,$p_2$,$p_3$ 是不同的素数,G,G_T 是阶为 $N=p_1p_2p_3$ 的循环群,映射 $e:G\times G\rightarrow G_T$ 满足:

1) 双线性.$\forall g,h\in G$,$\forall a,b\in\mathbb{Z}_N$,$e(g^a,h^b)=e(g,h)^{ab}$.

2) 非退化性.$\exists g\in G$,使得 $e(g,g)$ 在 G_T 中阶为 N.

假设在多项式时间内,对于参数 λ,双线性映射 e 的运算以及群 G 与 G_T 中的运算都是可计算的.接着分别用 G_{p_1},G_{p_2},G_{p_3} 表示 G 的 3 个子群,且其阶分别为 p,q,r,X_3 是 G_{p_3} 的一个生成元.注意,如果 $h_i\in G_{p_i}$ 且 $h_j\in G_{p_j}$,$i\neq j$,那么,$e(h_i,h_j)$ 就是群 G_T 的单位元,即 $e(h_i,h_j)=1$.

2.2　复杂性假设

本文方案所依赖的用于证明系统安全性的复杂性假设:第 1 个假设是 3 素数子群判定性假设.这个假设是静态的,且大小固定.

假设 1. 假设一个如上的 $\mathcal{G}$,有定义:$g\leftarrow G_{p_1}$,$Z_2\leftarrow G_{p_2}$,$D=(\mathbb{G},g,Z_2)$,$T_1\leftarrow G_{p_1p_3}$,$T_2\leftarrow G_{p_1}$.

由此定义敌手 A 攻破假设 1 的优势为 $Adv_A^1=|Pr[A(D,T_1)=1]-Pr[A(D,T_2)=1]|$.

这里我们认为 T_1 可以被写成是 G_{p_1} 中一个元素和 G_{p_3} 中一个元素的乘积.这 2 个元素分别被称为 T_1 的 G_{p_1} 部分及 T_1 的 G_{p_3} 部分.

定义 1. 若对于任意多项式时间对手 A,Adv_A^1 是可忽略的,则称 $\mathcal{G}$ 是满足假设 1 的.

假设 2. 假设一个如上的 $\mathcal{G}$,有定义:$\mathbb{G}\leftarrow\mathcal{G}$,$g$,$X_1\leftarrow G_{p_1}$,$X_2$,$Y_2\leftarrow G_{p_2}$,$X_3$,$Y_3\leftarrow G_{p_3}$,$D=(\mathbb{G},g,X_1,X_2,X_3,Y_2,Y_3)$,$T_1\leftarrow G_{p_1}$,$T_2\leftarrow G_{p_1p_3}$.

由此定义敌手 A 攻破假设 2 的优势为 $Adv_A^2=|Pr[A(D,T_1)=1]-Pr[A(D,T_2)=1]|$.

本文使用 $G_{p_1p_3}$ 来表示 G 中阶为 p_1p_3 的子群,这里我们可以认为 T_1 是 G_{p_1} 中的一个元素,T_2 是 G_{p_1} 中的一个元素以及 G_{p_3} 中一个元素的乘积.这些元素分别被称为 T_1 的 G_{p_1} 部分,T_2 的 G_{p_1} 部分以及 T_2 的 G_{p_3}.

定义 2. 若对于任意多项式时间对手 A,Adv_A^2 是可忽略的,则称 $\mathcal{G}$ 是满足假设 2 的.

假设 3. 假设一个如上的 $\mathcal{G}$,有定义:$\mathbb{G}\leftarrow\mathcal{G}$,$g\leftarrow G_{p_1}$,$X_2\leftarrow G_{p_2}$,$X_3,Y_3,Z_3\leftarrow G_{p_3}$,$\alpha,s\leftarrow Z_n$,$D=(\mathbb{G},g,g^{\alpha}X_3,X_2,g^{s}Y_3,Z_3)$,$T_1\leftarrow e(g,g)^{\alpha s}$,$T_2\leftarrow G_T$.

由此定义敌手 A 攻破假设 3 的优势为 $Adv_A^3=|Pr[A(D,T_1)]=1-Pr[A(D,T_2)]=1|$.

定义 3. 若对于任意多项式时间对手 A,Adv_A^3 是可忽略的,则称 $\mathcal{G}$ 是满足假设 3 的.

2.3 韦达定理[9]

给定 2 个矢量 $\boldsymbol{v}=(v_1,v_2,\cdots,v_L)$,$\boldsymbol{z}=(z_1,z_2,\cdots,z_L)$,矢量 $\boldsymbol{v}$ 既包含字母也包含无关字符,无关字符的个数是 n,而矢量 $\boldsymbol{z}$ 只包含 L 个字母.设定 $J=\{j_1,j_2,\cdots,j_n\}$,$i\in[1,L]$表示矢量 $\boldsymbol{v}$ 中无关字符的位置.

定义 $\prod_{j\in J}(i-j)=\sum_{k=0}^{n}\lambda_k i^k$,其中 λ_k 是由 J 决定的系数.如果对于 $i=1,2,\cdots,L$,若$(v_i=z_i)\vee(v_i=*)$,则:

$$\sum_{i=1,i\notin J}^{L}v_j\prod_{j\notin J}(i-j)=\sum_{k=0}^{n}\lambda_k\sum_{i=1}^{L}z_i i^k. \tag{1}$$

我们选择一个随机群元素 H_i,且 v_i,Z_i 是 H_i 的指数.如此,式(1)将变成:

$$\prod_{i=1,i\notin J}^{L}H_i^{v_i\prod_{j\in J}(i-j)}=\prod_{k=0}^{n}\left(\prod_{i=1}^{L}H_i^{Z_i i^k}\right)^{\lambda_k}. \tag{2}$$

利用韦达定理,我们可以构建式(1)中的系数 λ_k 为

$$\lambda_{n-k}=(-1)^k\sum_{1\leqslant i_1<i_2<\cdots<i_k\leqslant k}j_{\alpha}j_{\beta},$$
$$\alpha=i_1,i_2,\cdots i_k,$$
$$\beta=i_1,i_2,\cdots i_k,$$
$$0\leqslant k\leqslant n(n=|J|).$$

例如假定 $J=\{j_1,j_2,j_3\}$,多项式为$(x-j_1)\times(x-j_2)\times(x-j_3)$.利用韦达定理我们得到 $\lambda_3=1$,$\lambda_2=-(j_1+j_2+j_3)$,$\lambda_1=(j_1j_2+j_1j_3+j_2j_3)$,$\lambda_0=-j_1j_2j_3$.

3 高效的策略隐藏的 CP-ABE 方案

3.1 系统模型

如图 1 所示,云共享系统模型中主要有 4 种角色:云服务器、数据提供者、用户、可信授权中心.

1) 云服务器.它可以提供数据及信息的存储服务.它既是诚实的同时又是好奇的,所谓诚实是指它会严格执行我们制定的协议,而好奇意味着它会主动泄露我们的数据,这种情况下我们定义云服务器是半可信的.

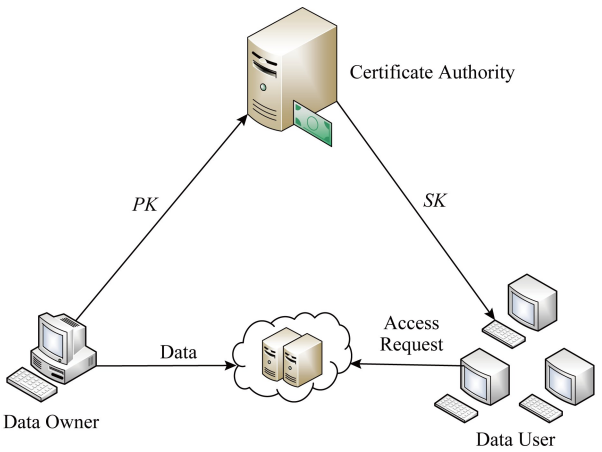

Fig. 1 System model of the effective CP-ABE with hidden access policy

图 1 高效的策略隐藏的 CP-ABE 方案系统模型图

2) 数据提供者.数据提供者需要自己制定访问策略,并且根据制定的访问策略来加密自己想要共享的数据,然后将加密后的数据上传到云服务器进行保管,且数据提供者不依赖于云服务器对数据的访问控制,相反,数据的访问控制是由数据拥有者自己制定且包含在加密数据的内部.系统中的合法用户在理论上均可以对密文进行访问,但是只有当用户的属性集合满足数据提供者定义在密文中的访问策略时,用户才能够解密密文从而得到明文.

3) 用户.用户可以向云服务器发送一个数据访问请求,接着云服务器对密文进行预解密,若该用户具有的属性集合满足数据提供者制定的访问策略,则云服务器将密文发送给用户,用户利用自己的私钥解密密文最终获得想要的数据,否则无法获得相应的数据.

4) 可信授权中心.一般情况下,可信授权中心被认为是可以信任的,它是云共享系统的核心,主要负责用户密码管理和分发以及系统参数生成.

3.2 安全模型

本方案基于选择明文安全模型[28-30],安全模型是通过敌手与挑战者间的一场安全挑战游戏来表述的,具体步骤为:

Setup.挑战者 B 运行初始化算法,并向敌手 A 提供公共参数 PK.

Phase1.敌手 A 根据已掌握的属性 $S_1,S_2,\cdots,S_n$,自适应地向挑战者发出查询请求.对于每一个

S_i,挑战者 B 运行 KeyGen$(PK,MK,L)\rightarrow SK$ 算法,并将 SK_i 发送给 A.

Challenge.敌手 A 向挑战者发送一个访问结构 W 以及 2 个等长的消息 M_0 和 M_1.挑战者 B 抛掷一枚公平硬币 $b\in\{0,1\}$,且在访问结构 W 作用下加密 M_b,并将密文 CT 发送给 A.

Phase2.重复执行询问阶段 1,但限制这些属性中的任何一个都不满足 W.

Guess.敌手 A 输出对 b 的一个猜测 b'.定义敌手 A 在上述游戏中敌手 A 获胜的优势为

$$\left|Pr[b'=b]-\frac{1}{2}\right|.$$

对于一个加密方案,如果在任意多项式时间内,敌手在游戏中的优势是可忽略的,即其赢得游戏的概率都趋近于 0,则称该加密方案在该模型下是安全的.

3.3　方案介绍

本文的方案主要是在文献[9]所述的第 2 个方案的基础上进行改进,以减少解密运算的消耗,提高解密的效率.

Setup1$(1^\lambda,U)\rightarrow(PK,MK)$.这一部分去除参数 $g_2\in G$,增加一个随机指数 d,并改变设定 $Y=e(g,g)^d$,其余部分不变,可得公共密钥为

$$PK=(p,e,g,G,G_T,g_1,Y,\{V_i,X_i\}_{i=1}^2,\{U_{1,i},U_{2,i},T_{1,i},T_{2,i},W_{1,i},W_{2,i},Z_{1,i},Z_{2,i}\}_{i=1}^n). \tag{3}$$

修改主密钥:

$$MK=(d,\{v^i,x_i\}_{i=1}^2,\{u_{1,i},u_{2,i},t_{1,i},t_{2,i},w_{1,i},w_{2,i},z_{1,i},z_{2,i}\}_{i=1}^n). \tag{4}$$

与原方案对比,公共参数 PK 中的 Y 值由原来的 $e(g,g_2)^d$ 变为 $e(g,g)^d$,主密钥 MK 去掉了一个参数 g_2,增加了一个参数 d,这些改变将会在解密算法步骤中起到作用,减小解密算法的运算,提高解密率.

Encrypt$(PK,M,W)\rightarrow CT$.对比原方案,无需对加密算法作修改,因此,密文不变仍为

$$\begin{aligned}CT=(&C_m=MY^{s_2},C_A=g^{s_2},C_B=g_1^{s_1}),\\&\{C_{1,i}=U_{1,i}^{s_1}T_{1,i}^{s_2}V_1^{si^a},\\&C_{2,i}=U_{2,i}^{s_1}T_{2,i}^{s_2}V_2^{v_i\alpha},\\&C_{3,i}=W_{1,i}^{s_1}Z_{1,i}^{s_2}X_1^{v_i\beta},\\&C_{4,i}=W_{2,i}^{s_1}Z_{2,i}^{s_2}X_2^{v_i\beta}\}_{i=1}^n.\end{aligned} \tag{5}$$

KeyGen$(PK,MK,L=\{A_1,A_2,\cdots,A_k\}\subseteq\mathbb{Z}_p)\rightarrow SK$.KeyGen 算法将用户的属性列表 L 作为输入,L 中包含 $n_2'\leqslant N_2$ 个正值属性,它们的位置被标记为 $V'=\{v_1',v_2',\cdots,v_{n_2'}'\}$,$n_3'\leqslant N_3$ 个负值属性,它们的位置标记为 $Z'=\{z_1',z_2',\cdots,z_{n_3'}'\}$.与原方案相同,我们构造 2 个向量 $\boldsymbol{XV}'$ 和 $\boldsymbol{XZ}'$:

$$\begin{aligned}\boldsymbol{XV}'&=(v_0',v_1',\cdots,v_{N_1}',1,0),\\\boldsymbol{XZ}'&=(z_0',z_1',\cdots,z_{N_1}',0,1).\end{aligned} \tag{6}$$

但对比原方案,在随机选择指数 $f_1,f_2,r_{1,i},r_{2,i},\cdots,r_{1,n},r_{2,n}\in\mathbb{Z}_p$ 后,接着选择随机元素 $R_A,R_B,R_{1,i},R_{2,i},R_{3,i},R_{4,i}\in G$.然后计算:

$$\begin{aligned}K_A&=g^d\prod_{i=1}^n K_{1,i}^{-t_{1,i}}K_{2,i}^{-t_{2,i}}K_{3,i}^{-z_{1,i}}K_{4,i}^{-z_{1,i}}\times R_A,\\K_B&=\prod_{i=1}^n g^{-(r_{1,i}+r_{2,i})}\times R_B,\\\{K_{1,i}&=g^{-\gamma_2 r_{1,i}}g^{f_1XV_iu_{2,i}}\times R_{1,i},\\K_{2,i}&=g^{\gamma_2 r_{1,i}}g^{-f_1XV_iu_{1,i}}\times R_{2,i},\\K_{3,i}&=g^{-\theta_2 r_{2,i}}g^{f_2XZ_iw_{2,i}}\times R_{3,i},\\K_{4,i}&=g^{\theta_1 r_{2,i}}g^{-f_2XZ_iw_{1,i}}\times R_{4,i}\}_{i=1}^n,\end{aligned} \tag{7}$$

得到密钥 $SK=(K_A,K_B,\{K_{1,i},K_{2,i},,K_{3,i},K_{4,i}\}_{i=1}^n)$.

Decrypt$(PK,SK,CT)\rightarrow M$.由原方案可得,如果 SK 的属性列表满足访问结构 W,则内积$(\boldsymbol{v},\boldsymbol{XV})$和$(\boldsymbol{v},\boldsymbol{XZ})$返回 0.则可用解密密钥 SK 解密密文 CT.

通过对初始化算法以及密钥生成算法的改变操作,可得:

$$e(C_A,K_A)=e(g^{s_2},g^d\times\prod_{i=1}^n K_{1,i}^{-t_{1,i}}\times K_{2,i}^{-t_{2,i}}\times K_{3,i}^{-z_{1,i}}\times K_{4,i}^{-z_{2,i}}\times R_A), \tag{8}$$

$$e(C_B,K_B)=e(g^{s_1\Delta},\prod_{i=1}^n g^{-(r_{1,i}+r_{2,i})}\times R_B). \tag{9}$$

因此我们知道:

$$e(C_A,K_A)\times e(C_B,K_B)\times\prod_{j=1}^4\prod_{i=1}^n e(C_{j,i},K_{j,i})=e(g,g)^{ds_2}=DEC. \tag{10}$$

而通过对之前方案的了解,我们知道:

$$\frac{C_m}{DEC}=\frac{M}{e(g,g)^{((\sum v_i\boldsymbol{XV}_i)f_1a\Delta)+((\sum v_i\boldsymbol{XZ}_i)f_2\beta\Delta)}}. \tag{11}$$

所以当用户属性满足访问结构时,即$(\boldsymbol{v},\boldsymbol{XV})=0$且$(\boldsymbol{v},\boldsymbol{XZ})=0$时,可以得到消息 $M=C_m/e(g,g)^{ds_2}$.

4　高效的策略隐藏 CP-ABE 方案分析

4.1　安全性分析

1) 数据机密性.这是保证本方案安全的一个最基本的安全特性.对于一个一般用户而言,当他不满足访问策略时,他就无法得到 $e(g,g)^{ds_2}$ 的值,因此

也无法进行解密操作,无法获得对应的明文.在本方案中,云服务器被认为是诚实但好奇的,它有可能去试图恢复用户的明文信息,但它最多只能得到 $e(g,g)^{ds_2}$ 的值,却无法获取相应但密文 CT,因此,它也无法进行解密操作,进而无法获得相应的明文消息.

2) 访问策略的安全性.当用户的加密信息发送给云服务器时,会通过计算然后以 $\{C_{1,i},C_{2,i},C_{3,i},C_{4,i}\}$ 来代替策略中的每个属性值,以 $\{K_{1,i},K_{2,i},K_{3,i},K_{4,i}\}$ 代替用户的属性值,而这些值只有对应属性的用户才可以被允许计算.因此,对于云服务器以及其他未授权用户无法进行计算得到它们相应的数据值,因此也无法对各个属性进行区分,避免了它们从访问策略中获得额外的信息,如此就确保了方案访问策略的安全性.

3) 抵抗共谋攻击.对于一个属性基加密方案来说,防止用户间的共谋攻击是十分重要的.在本方案中,一个用户或者攻击者要想解密密文,就必须要得到 $e(g,g)^{ds_2}$.而为了得到 $e(g,g)^{ds_2}$,对于一个攻击者 A 来说,当他不具备的特定属性时,他需要和另一名具备该属性的用户 B 联手共谋,这时要首先先计算它的密钥 $SK=(K_A,K_B,\{K_{1,i},K_{2,i},,K_{3,i},K_{4,i}\}_{i=1}^{n})$,但由于在密钥生成算法中加入了随机数 $R_A,R_B,R_{1,i},R_{2,i},R_{3,i},R_{4,i}\in G$,因此不同用户的这些随机数都不相同,这样一来,用户 A 和用户 B 就无法得到 $e(g,g)^{ds_2}$ 的值,也因此无法实现共谋破解密文.

4) CPA 安全性证明.假设存在攻击者 A 具备概率优势 ε,可以在选择明文攻击安全游戏中攻破本方案构造的系统,将其记为 $adv_A=\varepsilon$.

令 $a=s_2,b=d,g_T=e(g,g)\in G_T,v\in(0,1)$,如果 $v=0$,则 $Z=g_T^{ab}=e(g,g)^{ds_2}$,否则 $v=1$,则 $Z=g_T^{z}=e(g,g)^{z}$.对于群元素组 (g_T,g_T^a,g_T^b,Z),模拟器可以获得 g_T^a 和 g_T^b,然后输出对 Z 的猜测 v'.

模拟器的构造过程:

① 初始化.模拟器进行系统初始化,完成初始参数设置,生成全局公共参数 GP 以及公钥 $PK=(p,e,g,G,G_T,g_1,Y)$ 并发送给攻击者,攻击者由此获得 $g_T^b=e(g,g)^d$.

② 第 1 阶段.攻击者向挑战者询问密钥语言机 O_{key}.

攻击者向模拟器发送 (uid,S_{uid}),并向模拟器询问密钥预言机,其中 uid 为用户身份标识,S_{uid} 为对应身份标识所拥有的属性集合.

模拟器运行密钥生成算法,并将相应的属性私钥 $SK=(K_A,K_B,\{K_{1,i},K_{2,i},K_{3,i},K_{4,i}\}_{i=1}^{n})$ 发送给攻击者.

攻击者任意选取同样长度的明文 M_0 和 M_1 以及 2 个挑战访问结构 A_0 和 A_1,其中挑战访问结构都不能与第 1 阶段选择的属性集合 S_{uid} 匹配,然后攻击者将明文和挑战访问结构发送给挑战者.挑战者收到后,投掷一枚公平硬币,均匀地选择一个随机数 $\beta\in\{0,1\}$,然后按照访问结构 A_β 对 M_β 进行加密.

模拟器选择一个秘密的随机数 $s_2\in\mathbb{Z}_p$,计算得到挑战密文 $CT=(C_m,C_A,C_B,\{C_{1,i},C_{2,i},C_{3,i},C_{4,i}\}_{i=1}^{n})$.

然后,模拟器将挑战密文发送给攻击者.攻击者可以根据 $C_A=g^{s_2}$ 计算得到 $g_T^a=e(g,g)^{s_2}$.

③ 第 2 阶段.重复执行第 1 阶段,但是访问请求中的用户属性集不能满足挑战访问结构.

猜测:攻击者对 β 进行猜测,输出 $\beta'\in\{0,1\}$,如果 $\beta=\beta'$,模拟器输出 $v'=0$,否则模拟器输出 $v'=1$.

分析:在上述安全游戏中,攻击者遵循限制,访问请求中的用户属性集不能满足挑战访问结构.但是攻击者通过密钥询问获得了 g_T^a 和 g_T^b,从而可以对挑战密文进行猜测.

如果 $Z=g_T^{ab}=e(g,g)^{ds_2}$,那么 $C_0=M_\beta Z=M_\beta e(g,g)^{ds_2}$.根据假设,攻击者 A 拥有概率优势 ε,可以在选择明文攻击安全游戏中区分 β:

$$Pr[S(g_T^a,g_T^b,Z)=0|Z=g_T^{ab}]=\frac{1}{2}+adv_A=\frac{1}{2}+\varepsilon. \tag{12}$$

如果 $Z=g_T^{z}=e(g,g)^{z}$,那么攻击者无法猜测出明文 M_β,其概率是:

$$Pr[S(g_T^a,g_T^b,Z)=0|Z=g_T^{z}]=\frac{1}{2}. \tag{13}$$

那么,模拟器完成前面假设 3 的概率优势为

$$Pr[S(g_T^a,g_T^b,Z)=0]=\frac{1}{2}Pr[S(g_T^a,g_T^b,Z)=0|Z=g_T^{ab}]+\frac{1}{2}Pr[S(g_T^a,g_T^b,Z)=0|Z=g_T^{z}]=\frac{1}{2}\times(\frac{1}{2}+\varepsilon)+\frac{1}{2}\times\frac{1}{2}=\frac{1}{2}+\frac{\varepsilon}{2}. \tag{14}$$

在多项式时间内,任何攻击者无法以不可忽略的概率优势攻破假设 3.因此该模拟器拥有的概率优势 $\varepsilon/2$ 是可以忽略的.那么,攻击者 A 在安全游戏中攻破本方案所构造系统的概率优势 ε 也是可以忽略的.

4.2 理论分析

现将本文提出的方案与已有的 8 种属性基加密

方案在性能和安全性 2 个方面进行比较,主要考虑群阶的性质、密文长度、解密运算、安全模型、引用假设、访问结构、是否包含无关值、是否策略隐藏.如表 1 所示,对基于"与"门访问结构的或者具有固定长度的密文的 CP-ABE 方案进行了一个详细的对比.其中 p 表示双线性配对操作,n 是访问结构或属性列表中的属性数量,m 是每个属性的所有可能值的数量,w 是访问结构中无关属性的数量.由此我们可以看到,在所有可以支持无关属性并可以隐藏访问策略的方案中,由于密文大小和解密开销仅取决于访问结构中的无关值的数量,所以由表 1 对比看出,在满足隐藏访问策略且支持无关值的条件下,虽然无法保证本文方案有最小的解密成本,但本文方案有最短的密文长度,保证了解密效率.且本方案是基于完全安全的模型构建,确保了其安全性.因此,综合来讲,本文所述的方案具有最佳的性能.

Table 1　Comparison of CP-ABE Schemes

表 1　CP-ABE 方案比较

Scheme	Order Groups	Ciphertext Size	Decryption Cost	Security Models	Assumption	Wildcard	Hidden Policy
Ref [6]	p	$\|G_T\|+(2mn+1)\|G\|$	$(3n+1)p$	Selective	DBDH+DLIN	Yes	Yes
Ref [8]	pqr	$\|G_T\|+(2mn+1)\|G\|$	$(n+1)p$	Fully	Subgroup Assumption	Yes	Yes
Ref [15]	p	$\|G_T\|+2\|G\|$	$3p$	Selective	aMSN-DDH	No	No
Ref [16]	p	$\|G_T\|+2\|G\|$	$2p$	Selective	n-DBDH	No	No
Ref [17]	pqr	$\|G_T\|+2\|G\|$	$2p$	Fully	Subgroup Assumption	No	No
Ref [18]	p	$\|G_T\|+2\|G\|$	$2p$	Selective	n-DBDH	No	No
Ref [19]	p	$G_T\|+(n+1)\|G\|$	$(n+1)p$	Selective	DBDHE	No	Yes
Ref [20]	p	$2\|G_T\|+3\|G\|$	$(n+4)p$	Selective	n-DBDH	No	Yes
Our Scheme	p	$\|G_T\|+(4w+2)\|G\|$	$(4w+2)p$	Fully	DBDH+DLIN	Yes	Yes

4.3　实验分析

本节将通过实验对方案进行评估,选取文献[21-22]的方案进行对比.实验中使用的环境为 32 b 的 Linux 操作系统,CPU 频率为 3.0 GHz,内存为 3 GB,软件使用 MATLAB.因为 ABE 算法的加解密操作的主要耗时都与访问策略中的属性个数有关.因此,为了不失一般性,我们实验选取了 20 个策略集合$(A_1 \& A_2 \& \cdots \& A_N)$,$A_1$ 代表一个属性,$N \in [1,2,\cdots,20]$.对每个策略,计算同一条件下加解密的耗时.为了保证最终结论的准确性,我们采取了多次测量求取平均值的方法.

图 2 表示的是用户加密时所需要的时长,从图 2 中可以很明显地看出 3 个方案加密时间的开销都随着属性增加呈现线性增长,这是因为每个方案的加密计算都与密文长度有线性相关关系.因此,其密文的长度也都会随属性数目的增长而线性增长,这

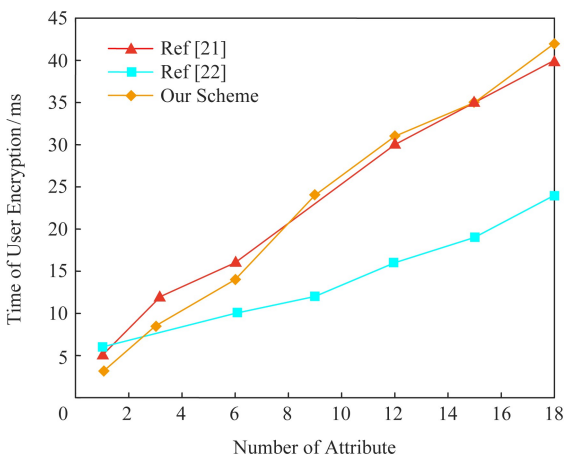

Fig. 2　Comparison of user encryption time for the effective CP-ABE with hidden access policy

图 2　高效的策略隐藏的 CP-ABE 方案用户加密时间比较

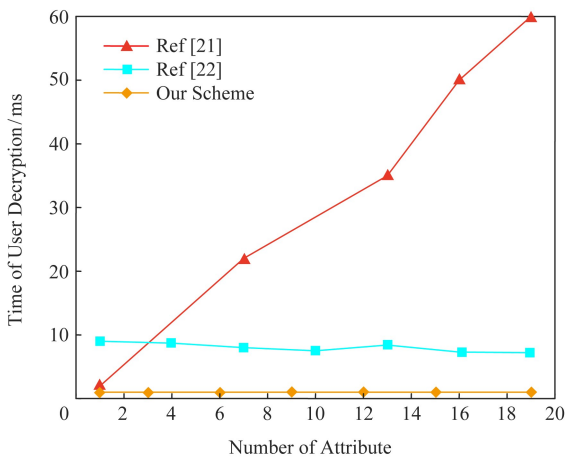

Fig. 3　Comparison of user decryption time for the effective CP-ABE with hidden access policy

图 3　高效的策略隐藏的 CP-ABE 方案用户解密时间比较

是因为每个方案的加密计算都与密文长度有线性相关关系,因此,其密文的长度也都会随属性数目的增长而线性增长.其中,文献[22]的加密计算耗时最短,但其却并未对密文中的访问策略进行加密操作,而与之对比,文献[21]方案以及本文方案虽然耗时多但支持了访问策略的隐藏.

图 3 展现了解密者在解密操作时的时间开销.其中本文方案以及文献[22]的方案在用户解密时的时间开销基本维持在常量水平,而文献[21]的方案因为需要进行对运算操作,因此它的解密时长则会随着访问策略中属性数量的增加而呈现线性增长.而对比与文献[22]方案而言,本方案生成密文更加短小,因此极大地加快了解密的速度,缩短了解密时长.

图 4 表现了用户产生私钥时所需要的时间开销,显而易见,随着用户属性数量的增加,这 3 个方案的计算开销都呈现出线性增加.这是由于每个存在于用户私钥中的属性都要进行相应的运算,因而属性的个数越多,计算开销就会越大.而对于每个属性,文献[21]方案的计算开销都相对而言比较大,所以其耗时也就比较多.

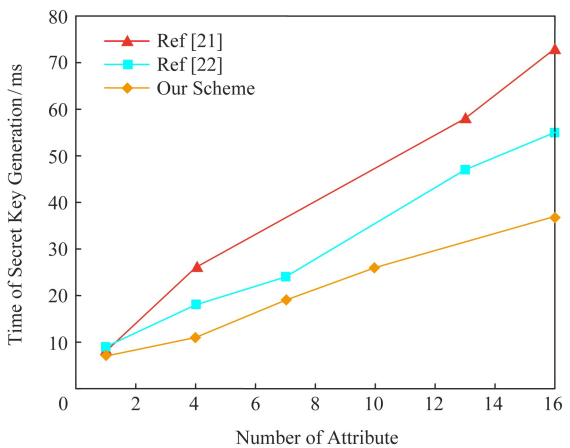

Fig. 4 Comparison of secret key generation time for the effective CP-ABE with hidden access policy

图 4 高效的策略隐藏的 CP-ABE 方案私钥生成时长比较

5 总 结

本文提出了一种隐藏访问策略的高效 CP-ABE 方案,它可以使得属性隐藏和秘密共享能够同时应用到“与”门结构中,然后利用合数阶双线性群构造了一种基于包含正负及无关值的“与门”的策略隐藏方案.本方案有效地避免了用户的具体属性值泄露给其他第三方,确保了用户隐私的安全.此外,通过实验验证及分析,保证了本文方案在实现复杂访问结构的策略隐藏的同时,还满足解密时间短、解密效率高的优点.

参 考 文 献

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

[2] Si Xiaolin, Wang Pengpian, Zhang Liwu. KP-ABE based verifiable cloud access control scheme [C] //Proc of the 12th IEEE Int Conf on Trust, Security and Privacy in Computing and Communications Melbourne. Piscataway, NJ: IEEE, 2013: 34-41

[3] Sun Guozi, Dong Yu, Li Yun. CP-ABE based data access control for cloud storage [J]. Journal on Communications, 2011, 32(7): 146-152 (in Chinese)
(孙国梓, 董宇, 李云. 基于 CP-ABE 算法的云存储数据访问控制[J]. 通信学报, 2011, 32(7): 146-152)

[4] Boneh D, Waters B. Conjunctive, subset, and range queries on encrypted data [C] //Proc of the 4th Conf on Theory of Cryptography. Berlin: Springer, 2007

[5] Katz J, Sahai A, Waters B. Predicate encryption supporting disjunctions, polynomial equations, and inner products [C] // Proc of the 27th Annual Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2008: 191-224

[6] Nishide T, Yoneyama K, Ohta K. Attribute-based encryption with partially hidden encryptor-specified access structures [C] //Proc of IEEE ACNS'08. Berlin: Springer, 2008: 111-129

[7] Balu A, Kuppusamy K. Privacy preserving ciphertext policy attribute based encryption [C] //Proc of the 3rd Int Conf on Recent Trends in Network Security and Applications. Berlin: Springer, 2010

[8] Lai Junzuo, Deng R, Li Yingjiu. Fully secure cipertext-policy hiding CP-ABE [C] //Proc of ISPEC'11. Berlin: Springer, 2011: 24-39

[9] Phuong T, Yang G, Susilo W. Hidden ciphertext policy attribute based encryption under standard assumptions [J]. IEEE Transactions on Information Forensics & Security, 2015, 11(1): 35-45

[10] Waters B. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions [C] //Proc of Int Cryptology Conf on Advances in Cryptology. Berlin: Springer, 2009: 619-636

[11] Lewko A, Waters B. New techniques for dual system encryption and fully secure HIBE with short ciphertexts [C] //Proc of the 7th Theory of Cryptography Conf. Berlin: Springer, 2010: 455-479

[12] Lewko A, Okamoto T, Sahai A, et al. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption [C] //Proc of EUROCRYPT'10. Berlin: Springer, 2010: 62-91

[13] Okamoto T, Takashima K. Fully secure functional encryption with general relations from the decisional linear assumption [C] //Proc of the 30th Annual Cryptology Conf on Advances in Cryptology (CRYPTO 2010). Berlin: Springer, 2010: 191-208

[14] Freeman D M. Converting pairing-based cryptosystems from composite-order groups to prime-order groups [C] // Advances in Cryptology (EUROCRYPT 2010). Berlin: Springer, 2010: 44-61

[15] Herranz J, Laguillaumie F, Carla Ràfols. Constant size ciphertexts in threshold attribute-based encryption [C] //Proc of PKC'10. Berlin: Springer, 2010: 19-34

[16] Chen Cheng, Chen Jie, Lim H W, et al. Fully secure attribute-based systems with short ciphertexts/signatures and threshold access structures [C] //Topics in Cryptology (CT-RSA 2013). Berlin: Springer, 2013: 50-67

[17] Chen Cheng, Chen Jie, et al. Fully secure attribute-based systems with short cipher-texts/signatures and threshold access structures [C] //Proc of CT-RSA'13. Berlin: Springer, 2013: 50-67

[18] Zhang Yinghui, Zheng Dong, Chen Xiaofeng. Computationally efficient ciphertext-policy attribute-based encryption with constant-size ciphertexts [C] //Proc of ProvSec'14. Berlin: Springer, 2014: 259-273

[19] Khuntia S, Kuma P S. New hidden policy CP-ABE for big data access control with privacy-preserving policy in cloud computing [C] //Proc of ICCCNT'18. Berlin: Springer, 2018: 1-7

[20] Zhang Yichen, Li Jiguo, Yan Hao. Constant size ciphertext distributed CP-ABE scheme with privacy protection and fully hiding access structure [J]. IEEE Access, 2019, 7: 47982-47990

[21] Hur J. Attribute-based secure data sharing with hidden policies in smart grid [J]. IEEE Transactions on Parallel & Distributed Systems, 2013, 24(11): 2171-2180

[22] Li Jin, Chen Xiaofeng, Li Jingwei. Fine-grained access control system based on outsourced attribute-based encryption [C] //Proc of European Symp on Research in Computer Security. Berlin: Springer, 2013: 592-609

[23] Wang Wei, Zhang Ge, Shen Yong. A CP-ABE scheme supporting attribute revocation and policy hiding in outsourced environment [C] //Proc of the 9th 2018 IEEE Int Conf on Software Engineering and Service Science. Piscataway, NJ: IEEE, 2018: 96-99

[24] Lei Linan, Li Yong. CP-ABE based data access control scheme with multi-authorities [J]. Application Research of Computers, 2018, 35(1): 248-252, 276 (in Chinese)
(雷丽楠, 李勇. 基于密文策略属性基加密的多授权中心访问控制方案[J]. 计算机应用研究, 2018, 35(1): 248-252, 276)

[25] Ling Julia, Weng Anxiang. A scheme of hidden-structure attribute-based encryption with multiple authorities [C] // Proc of CIAE'18. Berlin: Springer, 2018: 1-7

[26] Wang Guangbo, Liu Haitao, Wang Chenlu, et al. Revocable attribute based encryption in cloud storage [J]. Journal of Computer Research and Development, 2018, 55(6): 76-86 (in Chinese)
(王光波, 刘海涛, 王晨露, 等. 云存储环境下可撤销属性加密[J]. 计算机研究与发展, 2018, 55(6): 76-86)

[27] Zhang Kai, Ma Jianfeng, Zhang Junwei, et al. Online/offline traceable attribute-based encryption [J]. Journal of Computer Research and Development, 2018, 55(1): 216-224 (in Chinese)
(张凯, 马建峰, 张俊伟, 等. 在线/离线的可追责属性加密方案[J]. 计算机研究与发展, 2018, 55(1): 216-224)

[28] Wang Jinxiao. A study on the revocation mechanism of attribute-based ecryption [D]. Hangzhou: Hangzhou Dianzi University, 2012 (in Chinese)
(王锦晓. 属性基加密中撤销机制的研究[D]. 杭州: 杭州电子科技大学, 2012)

[29] Li Yuhan. Verifiable outsourcing encryption and decryption CP-ABE scheme [J]. Information & Communications, 2018, 191(11): 28-38 (in Chinese)
(李宇涵. 可验证外包加解密 CP-ABE 方案[J]. 信息通信, 2018, 191(11): 28-38)

[30] Lai Junzuo, Deng R, Li Yingjiu. Expressive CP-ABE with partially hidden access structures [C] //Proc of AsiaCCS'12. Berlin: Springer, 2012: 18-19

Wang Yue, born in 1982. Master, engineer. Her main research interests include information security, information and telecommunication engineering.

Fan Kai, born in 1978. PhD, professor. His main research interests include cloud security, information security. (kfan@mail.xidian.edu.cn)