基于公私属性的多授权中心加密方案

初晓璐 刘培顺

(中国海洋大学信息科学与工程学院 山东 青岛 266001)

摘 要 基于属性的加密方法可以简化云计算环境中的密钥管理和访问控制问题,是适用于云环境的加密方案。文中提出了一种基于公私属性的多授权中心加密方案。该方案将属性分为公有属性和私有属性,将用户的角色权限信息等作为用户的公有属性,将用户登录密码、设备上的标识码等作为用户的私有属性。利用公有属性实现访问控制,在云服务器上安全地共享数据;利用私有属性实现信息流的安全控制,确保只有特定用户在特定设备上使用数据。提出的方案可以实现密钥追踪和属性撤销,基于私有属性的加密还可以实现抗合谋攻击。

关键词 属性加密,云计算,抗合谋攻击,选择安全

中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.11.018

Multi-authority Encryption Scheme Based on Public and Private Attributes

CHU Xiao-lu LIU Pei-shun

(College of Information Science and Engineering, Ocean University of China, Qingdao, Shandong 266001, China)

Abstract The attribute-based encryption method can simplify the problem of key management and access control in cloud computing environment, and it's suitable for cloud environment. This paper proposed a multi-authority encryption scheme based on public and private attributes. In this scheme, the attributes are divided into public attribute and private attribute. The user's public property is constitutive of the user's role authority information, etc. The user's private property is composed of the password and the identification code of devices, etc. By using the public property to implement access control, the data can be shared safely on the cloud server. By using the private property to implement the security control of information flow, it can ensure that only the specific user uses data on a specific device. This scheme can realize key tracing and attribute revocation. Encryption based on private attributes can also achieve anti-conspiracy attacks.

Keywords Attribute-based encryption, Cloud computing, Anti-conspiracy attacks, Selective security

1 引言

当前云计算技术飞速发展,越来越多的企业选择在云环境进行办公。由于云计算环境的开放性和共享性,在云计算环境中用户对私有信息和数据的控制能力减弱,数据安全的一个重要挑战就是既要共享数据又要保护数据安全。在云存储的多用户环境下,共享机密文件将给文件所有者带来密钥存储、更新及维护等难以解决的问题。

Sahai 等[1]在 2005 年的欧密会议上首次提出了基于属性加密的想法。Goyal 等[2]于 2006 年提出将 ABE 分为密钥策略的基于属性的加密方法(KP-ABE)和密文策略的基于属性的加密方法(CP-ABE),并且提供了一个 KP-ABE 方案。Bethencourt 等[3]于 2007 年首次实现了 CP-ABE 方案。此外,Chase[4]提出了一种引入全局标识符与用户键绑定的方法。Goyal 等[5]于 2008 年设计了一种可证明安全的 CP-ABE 方案。Waters[6]于 2011 年给出了一种基于 DBDH 假设的可证明安全的 CP-ABE 方案。至此,基于属性加密的密码体制已基本建立。

在 ABE 的发展过程中,研究人员发现了系统可能存在用户泄密的安全问题和由此产生的撤销密钥的需求。为了解决这些问题,提出了可撤销的基于属性的加密方案和可追踪的基于属性的加密方案。Hinek[7]于 2008 年提出了第一个可追踪选择性安全的系统。Ruj 等[8]提出了一种 DAAC 方案,并为 Lewko 等的方案提出了一种属性撤销方法。在确保安全性的同时,Chen 等[9]根据 Lewko 等[10]的方案,将 DLIN 替换成了标准的 SXDH 假设,大大提高了方案的运行效率。

多授权的基于属性的加密方案(MA-ABE)最先是由 Chase[11]提出的,该加密方案是一种可以实现不同细粒度的加密方案。Cao[12]首先提出了没有中央机构的 MA-ABE 系统,该系统可以解决现有的单授权中心系统问题。Chase 等

到稿日期:2017-10-23 返修日期:2018-01-25 本文受国家重点研发计划资助项目(2017YFC0806200)资助。

初晓璐(1991—),女,硕士,CCF 会员,主要研究方向为密码学;**刘培顺**(1975—),男,博士,讲师,CCF 会员,主要研究方向为信息安全,E-mail:Liups@ouc.edu.cn(通信作者)。

以及 Lewko 等[13]分别于 2009 年和 2011 年对其进行了应用和改进。唐强等[14]提出了一种由单授权中心的可验证的属性加密方案推广而来的,多授权中心的可验证的基于属性的加密方案。Lewko 等[15]提出了一种没有 CA 但是能够提高系统安全性的方案。Yang 等[16-17]提出了一种基于整个 MA-ABE 过程的 MA-ABE 方案。Rouselakis 等[18]于 2015 年提出了在随机预言机模型下支持指数数量集合属性多授权中心的属性的加密方案。Yang 等[19]于 2017 年设计了一个面向社会网络的使用代理重加密技术的 MA-ABE 方案。

基于属性的加密方法将用户的身份表示为一个属性集合,加密数据与访问控制结构相关联,一个用户能否解密密文,取决于密文所关联的属性集合与用户身份对应的访问控制结构是否匹配。基于属性的加密方法能够简化云计算环境中的密钥管理和访问控制问题,是适用于云环境上的加密方案。在云环境中使用属性密码解决访问控制的思路[20]:系统中的权限由属性表示,属性机构对用户的权限属性进行认证并颁发相应的密钥,系统中的资源通过属性加密算法加密后保存在云中,资源的访问策略可根据需要由资源发布者来制定,任何人都能够公开访问加密后的资源,但只有满足访问策略的访问者才可以通过属性加密算法解密该资源。

在使用属性加密的云环境下,用户间存在共享私钥的动机,以获得解密最大范围的加密数据,使自身的利益最大化。在用户密钥泄露之后,得到泄露密钥的用户可以继续将获得的密钥进行传播。在这种情形下,现有的可追踪方案并不能完成对多级泄露中其余密钥的追踪[21]。本文提出的具有公私属性的加密方案可以抵抗合谋攻击,确保了在密钥传输的过程中,即使密钥发生了泄露,获得泄露密文的用户由于没有私有属性的相关密钥,密文也不会被未指定的设备解密,从而保证了密文的安全性。同时,本文方案可以实现属性撤销的相关功能,可以满足绝大多数场景的使用条件。

本文主要对传统的基于属性的加密方法进行进一步的改进,在文献[22]中基于密文属性的加密算法 CP-ABE 的基础上,提出了云存储数据安全访问控制方案。在这个方案中,将属性分为公有属性和私有属性,将用户的角色身份信息等作为用户的公有属性,将用户的云服务器登录密码、用户私有设备上的标识码、WLANMAC、BLUETOOTHMAC 等作为用户的私有属性。利用公有属性实现访问控制,可以实现在云服务器上安全共享数据;利用私有属性实现信息流的安全控制,可以确保只有特定用户在特定设备上使用数据。当用户的条件不满足解密条件时,用户即使获得数据也无法查看。只有用户的所有条件都符合时,用户才可以进行所有操作。

本文第 2 节介绍了加密方案中使用到的双线性映射、双线性对、访问结构和 LSSS 线性秘密共享方案,并对安全模型进行了定义;第 3 节提出了应用于云上的多授权的基于属性的加密方法的系统设置、方案定义和安全模型;第 4 节列出了加密方案的具体运算;第 5 节对提出的方案进行了安全性分析和相关方案对比;最后总结全文。

2　背景知识

定义 1(双线性映射)　假设两个素数阶 p 的循环乘法群为 G_0,G_1。假定 g 是 G_0 的生成元,双线性映射 $e:G_0\times G_0\rightarrow G_1$。

双线性映射 e 有下列性质:

1)双线性:对于所有 $u,v\in G_0$,$a,b\in Z_P$,有 $e(u^a,v^b)=e(u,v)^{ab}$。

2)非退化性:任意 $a,b\in G$,$e(g,g)\neq 1$,其中,1 为 G 单位元。

3)可计算性:用一个多项式时间算法计算 $e(u,v)$。

定义 2(访问结构(Access Structure))　假设 n 个参与者的集合为$\{P_1,P_2,\cdots,P_n\}$,A 是由参与者$\{P_1,P_2,\cdots,P_n\}$的子集构成的集合。若满足对于任意的 $B,C,B\in A$ 并且 $B\subseteq C$,那么 $C\in A$,则 A 是单调的。一个访问结构(单调访问结构)是集合$\{P_1,P_2,\cdots,P_n\}$的非空子集构成的集合(单调集合)。A 中的集合元素称为授权集合,不在 A 中的集合元素称为非授权集合。

定义 3(LSSS 线性秘密共享方案(Linear Secret-Sharing Schemes))[23]　如果对于一个集合 P,集合中的每一个元素所获得的分享部分可以形成一个 Z_P 上的向量。存在一个 L 行 N 列的分享生成矩阵 M,使得对于所有的 $i=1,\cdots,l$,矩阵 M 的第 i 行代表集合 $\rho(i)$中的一个元素,并且可以通过函数找到对应的元素。任何的访问控制策略都可以转换成一个访问矩阵。矩阵 M 的行表示访问主体,列表示访问客体,行与列的交点代表主体对客体应进行的操作。对于向量 $v=(s,r_2,r_3,\cdots,r_n)$,其中 s 是一个 Z_P 上的需要被共享的秘密,$r_2,\cdots,r_n$ 都是在 Z_P 上随机选择的,则 M_v 得到的向量是这 l 个元素所分享的信息,其中$(M_v)_i$ 属于元素 $\rho(i)$。

由文献[24]可知,元素分享的信息具有秘密恢复的属性,即对于某个集合 S 是由矩阵 M 决定的可以恢复出秘密的集合。则对于 $I\subset\{1,2,\cdots,l\}$,$I=\{i:\rho(i)\in S\}$存在这样的常量集合$\{\omega_i\in Z_p\}_{i\in I}$使得对于秘密 s 的有效分享 λ_i 信息有 $\sum_{i\in I}\omega_i\lambda_i=s$。这些常量的集合可以根据矩阵 M 在多项式的时间内获得。

定义 4(判定 q 双线性 Diffie-Hellman 问题 q-BDHE)　令 G 表示一个 q 阶的群,g 是其生成元。判定 q 双线性 Diffie-Hellman 问题是对随机选取的 $a,s\in Z_p$,对于给定的参数 $y=(g,g^a,\cdots,g^{a^q},g^{a^{q+2}},\cdots,g^{a^{2q}},g^s)$ 和 T,判定等式 $T=e(g,g)^{a^{q+1}s}$ 是否成立。

安全假设:

1)假设云服务器对于用户的数据内容是诚实但好奇的。虽然云服务器能够执行访问控制方案,但是它同样希望尽快得到用户的数据。

2)假设数据所有者、用户和属性机构中的密钥交换信道是安全的,不能非法得到密钥。

3　体系结构

3.1　系统设置

本方案设计的系统包含认证机构(CA)、属性机构(AA)、云服务器(Cloud Server)、数据所有者(Owner)、用户(User),它们之间的交互关系如图 1 所示。

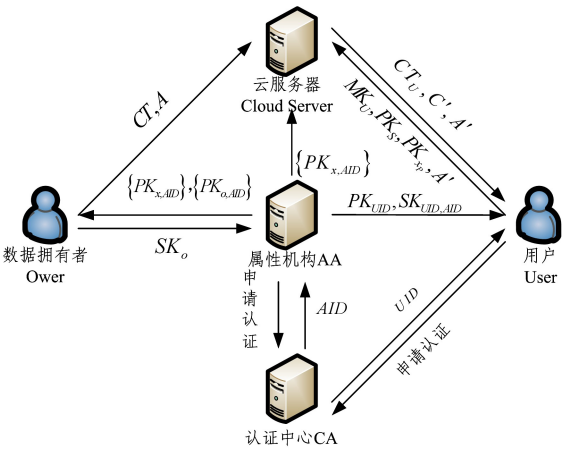

图 1 系统结构示意图

Fig. 1 Schematic diagram of system structure

图 1 中系统结构的功能特点的定义如下：

1)认证机构(CA)。在系统中用于认证属性机构和用户的身份。在建立系统的过程中，属性机构与用户向 CA 申请身份认证。CA 向合法的属性机构与用户颁发证书，并向每个合法属性机构分配全局唯一的标识符 AID，向每个合法用户分配全局唯一的标识符 UID。CA 并不参与属性的管理和相关密钥的建立。

2)属性机构(AA)。按照类别划分所有公有属性，每个 AA 负责管理一种公有属性，它们相互独立，可以有效地保护用户信息，防止隐私泄露。AA 负责生成与属性相关的密钥，当属性更新时，AA 负责更新属性密钥。

3)云服务器(Cloud severs)。云服务器为数据所有者提供存储服务和数据访问服务。数据所有者在将数据传送到云服务器之前，根据访问控制规则使用相应的公有属性密钥对数据进行加密，之后将加密后的数据密文和访问控制结构上传到云服务器。若用户满足访问控制结构的条件，用户可以向对应的属性机构 AA 申请数据访问密钥，然后连同用户自己的私有属性公钥发送到云服务器，云服务器对其进行重新封装操作，并将封装过的密文发送给用户，确保只有该用户才能解密数据。

4)数据所有者(Owner)。数据所有者负责加密数据，数据所有者通过访问控制结构让满足条件的用户从云服务器上下载数据。

5)用户(User)。用户具有公有属性和私有属性，用户角色、地理位置等作为公共属性密钥组成部分；用户特有的属性(如登录账号、登录密码、设备标识码、WLANMAC、BLUETOOTHMAC 等)可以作为私有属性密钥的组成部分。

3.2 方案定义

1)系统初始化。在初始化过程中不需要参数。认证机构为每个属性机构生成 AID，为每个用户生成 UID。

2)密钥生成算法。其包括 3 个算法：1)$OwnerGeneration(\beta,\gamma,\alpha_{AID})$，该算法输入随机参数 $\beta,\gamma,\alpha_{AID}$，生成主密钥 MK_o，私钥 SK_o，版本密钥 VK_{AID} 和数据所有者的公钥 $PK_{o,AID}$；2)$UserGeneration(u,SK_o)$，该算法输入随机参数 u，私钥 SK_o，由属性机构负责生成用户的公钥 PK_{UID} 和用户的私钥 $SK_{UID,AID}$；3)$UserPrivateGeneration(\varepsilon,\mu,\delta,u_{UID})$，该算法输入随机参数 $\varepsilon,\mu,\delta,u_{UID}$，由用户生成 $MK_U, PK_U, PK_{x_P}, SK_{x_P}, PK_S$ 和 SK_S。

3)加密。加密算法 $Encryption(s,\{PK_{o,AID_K}\}_{k\in I_A},\{PK_{x,AID_K}\}_{x\in S_{AID_k},k\in I_A},MK_o,m,A)$ 的参数包括：随机参数 s、数据所有者的公钥 $\{PK_{o,AID_K}\}_{k\in I_A}$、公共属性密钥 $\{PK_{x,AID_K}\}_{x\in S_{AID_k},k\in I_A}$、数据所有者的主密钥 MK_o、发送信息 m 和访问结构 A。

4)重新封装。$Repackaging(PK_{x,AID},MK_U,PK_{x_P},PK_S=e(g,g)^{\delta})$：云服务器使用 $PK_{x,AID}=(g\cdot H(x))^{\alpha_{AID}\cdot u}$ 对密文进行操作。如果用户的属性与数据所有者设计的访问控制方案匹配，云服务器将对密文进行重新封装操作。使用 MK_U，PK_{x_P}, PK_S 对信息进行重新封装。

5)解密。$Decryption(CT_U,C',PK_U,SK_{x_P},SK_{UID,AID})$：如果用户的设备属性满足密文 CT_U 中的访问结构 A'，用户将使用 C', PK_U, SK_{x_P} 和 $SK_{UID,AID}$ 对密文进行解密运算，最后获得信息。

3.3 安全模型

基于属性的加密安全模型的定义如下。

1)系统建立阶段：挑战者随机选择一个安全参数，运行系统初始化算法，并向攻击者提供生成的公钥。

2)挑战查询阶段：攻击者向挑战者提问，对属性集合进行查询，并对私有属性部分的密钥进行询问。属性集合不能满足访问结构。

3)挑战阶段：攻击者提交两个相等长度的信息 M_0 和 M_1 给挑战者。挑战者抛出一枚公平的硬币 $b\in\{0,1\}$，然后加密 M_b 并得到输出 C^*，将 C^* 发送给攻击者。

4)猜测阶段：攻击者必须回答 0 或者 1(记为 b')，作为 C^* 的猜测。如果 $b'=b$，攻击者赢得游戏。攻击者在游戏中的优势定义为 $Pr[b'=b]=\frac{1}{2}$。如果攻击者赢得游戏的概率是可以忽略的，那么游戏被称为 IND-CCA 游戏。在选择明文游戏中，称为 IND-CCA 安全。

4 基于属性的加密方案

本节将描述基于属性的加密方案，该方案由以下 6 个阶段组成。

1)系统初始化($Setup$)：初始化阶段，认证机构 CA 验证每个属性机构 AA 和每个用户的身份，验证通过后每个属性机构 AA 将得到认证机构 CA 分配的标识符 AID，每个用户得到全局唯一标识符 UID。

2)密钥生成阶段($Generation$)：包括 3 个算法，分别生成数据所有者的密钥、用户的公有属性密钥、用户的私有属性密钥。

①数据所有者生成算法($OwnerGeneration$)：当数据所有者有数据需要共享到云服务器时，需要生成数据加密所需的密钥。

该算法由数据所有者初始化，随机选择 $\beta,\gamma\in Z_p$ 作为公共参数，生成数据所有者的主密钥 $MK_o=\{\beta,\gamma\}$，私钥 $SK_o=\{g^{\frac{1}{\beta}},\frac{\gamma}{\beta}\}$。数据所有者将 SK_o 通过安全的信道发送给允许访问该数据的访问属性所属的属性机构 AA。

属性机构 AA 随机选择参数 $\alpha_{AID}\in Z_p$，生成数据加密用的版本密钥 $VK_{AID}=\alpha_{AID}$，生成数据所有者的公钥 $PK_{o,AID}=e(g,g)^{\alpha_{AID}}$。设属性机构 AA 控制属性 x（x 为用户的身份属性，符合数据的访问控制要求），生成公共属性密钥 $PK_{x,AID}=(g\cdot H(x))^{\alpha_{AID}\cdot u}$，并把它和 $PK_{o,AID}$ 一起发送给数据所有者。

②用户访问密钥的生成（*UserGeneration*）：当满足访问属性的用户需要访问数据所有者共享到云服务器的数据时，需要到对应的属性管理机构 AA 申请用户访问密钥。

属性机构 AA 随机选择 $u\in Z_p$，g 为生成元，生成用户的公钥 $PK_{UID}=g^u$。属性机构 AA 分配用户的属性，构成个人属性集 $S_{UID,AID}$。使用数据所有者的 SK_o，属性机构 AA 输出用户的私钥 $SK_{UID,AID}=(PK_{UID})^{\frac{\gamma}{\beta}}\cdot g^{\frac{\alpha_{AID}}{\beta}}=g^{u\cdot\frac{\gamma}{\beta}}\cdot g^{\frac{\alpha_{AID}}{\beta}}$。

③用户的私有属性密钥生成（*UserPrivateGeneration*）：为了防止合谋攻击和密钥泄漏导致的非法传播，用户在访问云数据时，还需要生成基于其私有属性的访问密钥。

系统获取用户的登录密码和用户所用设备的信息作为私有属性 x_P，选择随机参数 $\varepsilon,\mu,\delta,u_{UID}\in Z_P$，生成 User 的 $MK_U=\{\varepsilon,\mu\}$，$PK_U=(g^{\delta}\cdot H(x_P)^{\delta})^{u_{UID}}$，$PK_{x_P}=g^{u_{UID}}$，$SK_{x_P}=g^{u_{UID}\cdot\frac{\mu}{\varepsilon}}\cdot g^{\frac{\delta}{\varepsilon}}$，$PK_S=e(g,g)^{\delta}$，$SK_S=\{g^{\frac{1}{\varepsilon}},\frac{\mu}{\varepsilon}\}$。

3）加密（*Encryption*）：数据上传云服务器前，数据所有者使用申请到的 $PK_{o,AID}$ 和 $PK_{x,AID}$ 密钥进行加密。

加密过程如下：随机选择加密指数 $s\in Z_p$ 和向量 $\vec{v}=(s,y_2,\cdots,y_n)\in Z_p^n$，用来共享加密指数。对于 $i=1,\cdots,l$，生成并分配 $\lambda_i=\vec{v}\cdot M_i$，$M_i$ 是对应于矩阵 M 第 i 行的向量。存在 $\omega_i\in Z_p$，使得 $\sum_{i\in I}\omega_i\lambda_i=s$ 成立。生成密文如下：

$$CT=(C=m\cdot(\prod_{k\in I_A}PK_{o,AID_K})^s,C'=g^{\beta s},C_i=g^{u\gamma\lambda_i}\cdot(PK_{x_i,AID_i})^{-\beta s},i=1,\cdots,l) \tag{1}$$

其中，m 为数据明文。数据所有者把密文传输到云服务器。

4）重新封装（*Repackaging*）：符合访问规则要求的用户申请到用户访问密钥后，可以向云服务器申请数据访问，云服务器在接收到用户请求后，为了防止合谋攻击和密钥泄露导致的非法传播，使用用户的私有属性相关密钥执行重新封装操作，把数据与用户私有属性进行绑定，可以保证只有特定的设备和用户才可以解密消息，获得信息。

用户将 $MK_U=\{\varepsilon,\mu\}$，$PK_{x_P}=g^{u_{UID}}$，$PK_S=e(g,g)^{\delta}$ 和 A' 访问结构上传给云服务器，A' 是由用户根据所选私有属性构成的访问结构。云服务器对密文执行重新封装操作，在重新封装过程中，云服务器并不能得到完整的信息 m。

如果用户的属性与数据所有者设计的访问控制方案匹配，云服务器将根据用户拥有的属性在对应的属性机构 AA 获取 $PK_{x,AID}$，使用 $PK_{x,AID}$ 对密文进行操作，得到密文 M'。

$$\begin{aligned}M'&=Decrypt(CT,PK_{x,AID})\\M'&=C\cdot\prod_{K\in I_A}\prod_{i\in S_{AID_k}}(e(C_i,g)\cdot e(C',PK_{x,AID}))^{w_in_A}\\&=C\cdot\prod_{K\in I_A}\prod_{i\in S_{AID_k}}(e(g^{u\gamma\lambda_i},(g\cdot H(v(i)))^{-\alpha_{AID_k}\beta us},g)\cdot\\&\quad e(g^{\beta s},(g\cdot H(\rho(i)))^{\alpha_{AID_k}\cdot u}))^{w_in_A}\\&=C\cdot\prod_{K\in I_A}\prod_{i\in S_{AID_k}}(e(g,g)^{u\gamma\lambda_i-\alpha_{AID_k}\beta us}\cdot e(g,H(v(i)))^{-\alpha_{AID_k}\beta us}\cdot e(g,g)^{\alpha_{AID_k}\beta us}\cdot e(g\cdot H(\rho(i)))^{\alpha_{AID_k}\beta us})^{w_in_A}\\&=C\cdot\prod_{K\in I_A}\prod_{i\in S_{AID_k}}e(g,g)^{u\gamma\lambda_iw_in_A}\\&=C\cdot e(g,g)^{u\gamma sn_A}\end{aligned} \tag{2}$$

然后，云服务器将对密文进行重新封装操作，云服务器使用 $MK_U=\{\varepsilon,\mu\}$，$PK_{x_P}=g^{u_{UID}}$，$PK_S=e(g,g)^{\delta}$ 对密文 M' 进行运算。首先，随机选择加密指数 $s'\in Z_p$ 和向量 $\vec{v}'=(s',y_2',\cdots,y_n')\in Z_p^n$，用来共享加密指数。对于 $i=1,\cdots,t$，$i\in S_U$，生成并分配 $\lambda_i'=\vec{v}'\cdot M_i'$，$M_i'$ 是对应于矩阵 M' 第 i 行的向量。存在 $\omega_i'\in Z_p$，使得 $\sum_{i\in I}\omega_i'\lambda_i'=s'$ 成立。S_U 是被选中的用户私有属性中的属性，n_A 是参与运算的属性机构 AA 的数量。

重新封装的过程如下：

$$\begin{aligned}&CT_U=(C_U=M'\cdot(\prod_{k\in I_U}PK_S)^{s'},C'=g^{\beta s},C_U'=g^{\varepsilon s'},\\&\quad C_{U,i}=g^{\mu u_{UID}\lambda_i'}(PK_{\tau(i),x_P})^{-\varepsilon S'}(i=1,\cdots,t))\end{aligned} \tag{3}$$

云服务器将访问结构 A' 隐式包含于密文 CT_U 中。

5）解密（*Decryption*）：用户收到云服务器发送过来的重新封装的数据后，执行解密操作。

云服务器将密文 CT_U 发送给用户，如果用户的设备属性满足密文 CT_U 中的访问结构 A'，用户将使用 $C'=g^{\beta s}$，$PK_U=(g^{\delta}\cdot H(x_P)^{\delta})^{u_{UID}}$，$SK_{x_P}=g^{u_{UID}\cdot\frac{\mu}{\varepsilon}}\cdot g^{\frac{\delta}{\varepsilon}}$ 和 $SK_{UID,AID}=g^{u\cdot\frac{\gamma}{\beta}}\cdot g^{\frac{\alpha_{AID}}{\beta}}$ 对密文 C_U 进行解密运算，最后获得信息 m。n_A' 是参与运算的属性数量。

解密算法的过程如下：

$$\begin{aligned}&\frac{C_U\cdot\prod_{k\in I_U}\prod_{i\in S_{U_k}}(e(C_U',PK_U)\cdot e(C_{U,i},g))^{w_i'n_A'}}{\prod_{k\in I_U}e(C_U',SK_{x_P})\cdot\prod_{K\in I_A}e(C',SK_{UID,AID_K})}\\&=\frac{C_U\cdot\prod_{k\in I_U}\prod_{i\in S_{U_K}}(e(g^{\varepsilon s'},(g^{\delta_k}\cdot H(\sigma(i))^{\delta_k})^{u_{UID}})\cdot e(g^{\mu u_{UID}\lambda_i'}\cdot(g\cdot H(\tau(i)))^{-\varepsilon\delta_ku_{UID}S'},g))^{w_i'n_A'}}{\prod_{k\in I_U}e(g^{\varepsilon s'},g^{u_{UID}\cdot\frac{\mu}{\varepsilon}}\cdot g^{\frac{\delta_k}{\varepsilon}})\cdot\prod_{K\in I_A}e(g^{\beta s},g^{u\cdot\frac{\gamma}{\beta}}\cdot g^{\frac{\alpha_{AID_k}}{\beta}})}\\&=\frac{C_U\cdot\prod_{i\in S_{U_K}}e(g,g)^{\mu u_{UID}\lambda_i'w_i'n_A'}}{\prod_{k\in I_U}e(g,g)^{\mu u's'+\delta_ks'}\cdot\prod_{K\in I_A}e(g,g)^{u\gamma s+\alpha_{AID_k}s}}=\frac{C_U\cdot e(g,g)^{\mu u_{UID}s'n_A'}}{e(g,g)^{\mu u_{UID}s'n_A'}\cdot\prod_{K\in I_U}e(g,g)^{\delta_ks'}\cdot e(g,g)^{u\gamma sn_A}\cdot\prod_{K\in I_A}e(g,g)^{\alpha_{AID_k}s}}\\&=\frac{C_U}{e(g,g)^{u\gamma sn_A}\cdot\prod_{k\in I_U}e(g,g)^{\delta_ks'}\cdot\prod_{K\in I_A}e(g,g)^{\alpha_{AID_k}s}}=\frac{M'\cdot(\prod_{k\in I_U}PK_S)^{s'}}{e(g,g)^{u\gamma sn_A}\cdot\prod_{k\in I_U}e(g,g)^{\delta_ks'}\cdot\prod_{K\in I_A}e(g,g)^{\alpha_{AID_k}s}}\\&=\frac{C\cdot e(g,g)^{u\gamma sn_A}\cdot(\prod_{k\in I_U}PK_S)^{s'}}{e(g,g)^{u\gamma sn_A}\cdot\prod_{k\in I_U}e(g,g)^{\delta_ks'}\cdot\prod_{K\in I_A}e(g,g)^{\alpha_{AID_k}s}}=\frac{m\cdot(\prod_{k\in I_A}PK_{o,AID_K})^s\cdot e(g,g)^{u\gamma sn_A}\cdot(\prod_{k\in I_U}PK_S)^{s'}}{e(g,g)^{u\gamma sn_A}\cdot\prod_{k\in I_U}e(g,g)^{\delta_ks'}\cdot\prod_{K\in I_A}e(g,g)^{\alpha_{AID_k}s}}=m\end{aligned} \tag{4}$$

6)属性更新(*AttributeUpdate*):对于存放在云服务器上的数据,数据拥有者重新设置访问控制规则可以执行属性更新操作,撤销不需要的属性,增加新属性。

属性更新需要密钥更新和数据重加密 2 个步骤。密钥更新算法的参数包括私钥 $SK_{UID,AID}$ 和新属性设置 $S'_{UID,AID} \in S_{UID,AID}$,生成新的版本密钥 VK'_{AID} 并更新相关密钥。重加密算法的参数包括密文 CT、更新信息 UI_{AID}、更新密钥 UK_{AID}、生成新密文。更新的密钥可以防止被撤销的 User 通过新公钥对数据进行未授权的访问,可以保证当一个新加入的用户的属性满足密文的相关访问策略时,其可以访问以前的数据。

步骤 1 密钥更新

属性机构 AA 通过执行密钥更新算法生成新版本密钥 VK'_{AID},更新密钥 $UK'_{AID'}$ 和用户的新私钥 $SK'_{UID',AID'}$。

属性机构 AA 的属性变更后,数据所有者需要更改相关密钥,保证属性变更后的信息安全,步骤如下:

1)AA 重新生成用户访问密钥

带有 AID' 的属性机构 AA 首先随机选择 $\alpha'_{AID'} \in Z_p$ 作为与之前版本密钥不同的新版本密钥,然后计算 UID' 的用户新的私钥 $SK'_{UID',AID'}$:$SK'_{UID',AID'} = (PK_{UID'})^{\frac{\gamma}{\beta}} \cdot g^{\frac{\alpha'_{AID'}}{\beta}}$,$\forall x \in S'_{UID',AID'}$:$PK'_{x,AID'} = (g \cdot H(x))^{\alpha'_{AID'} \cdot u}$。

新版本密钥 $VK'_{AID'}$ 用来生成更新密钥:

$$UK_{AID'} = (UK1_{AID'} = g^{\frac{\alpha'_{AID'} - \alpha_{AID'}}{\beta}}, UK2_{AID'} = \frac{\alpha'_{AID'}}{\alpha_{AID'}})$$

最后,拥有 AID' 的属性机构 AA 分发新私钥 $SK'_{UID',AID'}$ 给拥有该属性的用户。

2)用户更新用户访问密钥

每个拥有新属性的用户收到更新密钥 $UK'_{AID'}$,更新私钥的过程如下:$SK'_{UID_i,AID'} = (SK'_{UID_i} = SK_{UID_i,AID'} \cdot UK1_{AID'}$,$\forall x \in S_{UID_i,AID'}$:$SK'_{x,UID_i,AID'} = (SK_{x,UID_i,AID'})^{UK2_{AID'}})$。

3)数据所有者更新相关密钥

数据所有者收到属性机构 AA 发送的更新密钥 $UK_{AID'}$,之前的公钥 $PK'_{o,AID'}$ 更新到现有版本 $PK'_{o,AID'} = (PK_{o,AID'})^{UK2_{AID'}}$,并且每个公共属性密钥更新为 $PK'_{x,AID'} = (PK_{x,AID'})^{UK2_{AID'}}$。

步骤 2 数据重新加密

数据所有者首先生成密钥更新信息 $UI_{AID'}$:$UI_{AID'} = (\forall x \in S_{AID'}$:$UI_{x,AID'} = (\frac{PK_{x,AID'}}{PK'_{x,AID'}})^{\beta s})$。之后,发送更新信息 $UI_{AID'} = \{UI_{i,AID'}\}_{i \in I_{AID'}}$ 和属性机构 AA 的更新密钥 $UK_{AID'} = (UK1_{AID'}, UK2_{AID'})$ 到云服务器。云服务器执行重加密算法,并根据从数据所有者获得的更新信息来重加密密文。计算新密文 CT 为:

$$CT' = (C' = C \cdot e(UK1_{AID'}, C'), C' = g^{\beta s}, (\forall i = 1, \cdots, l), C_i' = C_i (\rho(i) \notin S_{AID'}) / C_i' = C_i \cdot UI_{\rho(i),AID'} (\rho(i) \in S_{AID'}))$$

5 方案分析

此方案的安全性分析如下。

1)在判定性的 q-BDHE 假设成立的条件下,没有攻击者能选择性地用一个规模为 $l^* \times n^*$ ($l^*, n^* \leqslant q$)的挑战矩阵在多项式时间内破坏系统。即,概率 $Adv_A(k) = |Pr[t' = t] - \frac{1}{2}|$ 是可以忽略的。

证明:假设在博弈中,攻击者有不可忽略的优势概率 $\varepsilon = Adv_A(k)$ 可以攻破该方案,而且选择一个行和列大小都不超过 q 的挑战矩阵 M^*。下面给出一个模拟器来证明判定性的 q-BDHE 假设:

①系统建立阶段

攻击者初始化:挑战者初始化 q-BDHE 的挑战向量 $y = (g, g^s, g^a, \cdots, g^{a^q}, g^{a^{q+2}}, \cdots, g^{a^{2q}})$,猜测 T 并选择一个挑战的访问控制结构 $\tau = (M^*, \rho^*)$,其中矩阵 M^* 的列数为 n^*。

系统初始化:挑战者随机选择一个 $\alpha' \in Z_p$ 并令 $\alpha = \alpha' + u^{1+q}$,于是有 $e(g,g)^{\alpha} = e(g^u, g^{u^q}) \cdot e(g,g)^{\alpha'}$。令 X 表示下标 i 的集合,设 $x \in [1, U]$,并随机选取指数值 $z_x \in Z_p$。如果 $H(x)$ 已经存在,则直接输出相应值;否则,群组中的每个元素 $H(x)$,$x \in [1, U]$,并有 $\rho^*(i) = x$,令 $m = z_x + uM^*_{i,1} + u^2 M^*_{i,2} + \cdots + u^{n^*} M^*_{i,n^*}$ 可以用模拟器来进行计算:$H(x) = g^m = g^{z_x + uM^*_{i,1} + u^2 M^*_{i,2} + \cdots + u^{n^*} M^*_{i,n^*}}$。当 $X = \emptyset$ 时,$H(x) = g^{z_x}$。由于 g^{z_x} 的值是随机的,因此计算出的群组元素也是随机的:

$$PK_{x,AID} = (g \cdot H(x))^{\alpha_{AID} \cdot u} = (g \cdot g^{z_x + uM^*_{i,1} + u^2 M^*_{i,2} + \cdots + u^{n^*} M^*_{i,n^*}})^{\alpha \cdot u}$$

②查询阶段

模拟器接受攻击者对私钥的询问,假设攻击者的公有属性为 S,属性 S 不能满足访问结构 M^*。

模拟器首先选择一个随机指数 $r \in Z_p$,由 LSSS 的特性可知,能够找到一个向量 $\vec{\omega} = (\omega_1, \cdots, \omega_{n^*}) \in Z_p^n$,其中 $\omega_1 = -1$,并且对于所有满足 $\rho^*(i) \in S$ 的 i,有 $\vec{\omega} \cdot M_i^* = 0$。模拟器定义一个指数多项式 n,$n = r + \omega_1 a^q + \omega_2 a^{q-1} + \cdots + \omega_{n^*} a^{q-n^*+1} = \frac{1}{\beta}$,可得出 $g^{\frac{1}{\beta}} = g^r \prod_{i=1,\cdots,n^*} (g^{q-i+1})^{\omega_i} = g^n$ 和 $\frac{\gamma}{\beta} = \gamma \cdot (r + \omega_1 a^q + \omega_2 a^{q-1} + \cdots + \omega_{n^*} a^{q-n^*+1}) = n\gamma$,$SK = g^{u \cdot \frac{\gamma}{\beta}} \cdot g^{\frac{\alpha_{AID}}{\beta}} = g^{un\gamma} \cdot g^{n\alpha}$。

模拟器还要计算私有属性部分的密钥,随机选取 ε, μ, δ,$u_{UID} \in Z_P$,分别生成 $PK_U = (g^{\delta} \cdot H(x_P)^{\delta})^{u_{UID}}$,$PK_{x_P} = g^{u_{UID}}$,$SK_{x_P} = g^{u_{UID} \cdot \frac{\mu}{\varepsilon}} \cdot g^{\frac{\delta}{\varepsilon}}$,$PK_S = e(g,g)^{\delta}$,$SK_S = \{g^{\frac{1}{\varepsilon}}, \frac{\mu}{\varepsilon}\}$,$CT_U = (C_U = M^* \cdot (\prod_{k \in I_U} PK_S)^{s'}, C_U' = g^{\varepsilon s'}, C_{U,i} = g^{\mu u_{UID} \lambda_i'} (PK_{\tau(i),x_P})^{-\varepsilon S'} (i = 1, \cdots, t))$。

③挑战阶段

攻击者将两个长度相等的消息 M_0 和 M_1 发送给模拟器,模拟器随机选择 $\beta \in \{0,1\}$,并生成密文 $C = m \cdot (\prod_{k \in I_A} PK_{o,AID_K})^s = m \cdot (\prod_{k \in I_A} e(g,g))^{\alpha s} = m \cdot T \cdot \prod_{k \in I_A} e(g^{a'}, g^s)$,$C' = g^{\frac{s}{n}}$,模拟器选择随机自然数 $y_2', \cdots, y_{n^*}' \in Z_p$,$r_1', \cdots, r_i' \in Z_p$,$i = 1, \cdots, n^*$,并且使用向量 $\vec{v}$ 为 $\vec{v} = (s, sa + y_2', sa^2 + y_3', \cdots, sa^{n-1} + y_{n^*}') \in Z_p^{n^*}$,$\lambda_i = \vec{v} \cdot M_i$。

对于所有的 $i = 1, \cdots, n^*$,$C_i = g^{u\gamma\lambda_i} (g \cdot H(x))^{-\alpha_{AID} \cdot u\beta s} = g^{u\gamma\lambda_i} \cdot (g \cdot g^{z_x + uM^*_{i,1} + u^2 M^*_{i,2} + \cdots + u^j M^*_{i,2} + \cdots + u^{n^*} M^*_{i,n}})^{-\alpha \cdot u\beta s}$。

以上步骤可以重复执行。

④猜测阶段

攻击者最后输出一个对 β 的猜测 β'。如果 $\beta=\beta'$，那么模拟器猜测计算值 $T=e(g,g)^{a^{q+1}s}$ 的结果为 0；反之，结果输出为 1，说明 T 是随机群组 G_T 中的元素。当 $\beta=0$ 时，模拟器猜测正确的概率为：$Pr[\beta(\vec{y},T=e(g,g)^{a^{q+1}s})=0]=\frac{1}{2}+Adv_A$；当 $\beta=1$ 时，T 是随机群组元素，那么消息 M_β 就可以被完全隐藏，模拟器猜测正确的概率大小为：$Pr[\beta(\vec{y},T=R)=0]=\frac{1}{2}$。因此，模拟器能够以不可忽略的优势 ε' 解决 q-BDHE 问题：

$$\begin{aligned}\varepsilon'&=\frac{1}{2}\cdot Pr[\beta(\vec{y},T=e(g,g)^{a^{q+1}s})=0]+\frac{1}{2}\cdot Pr[\beta(\vec{y},T=R)=0]-\frac{1}{2}\\&=\frac{1}{2}\cdot(\frac{1}{2}+Adv_A)+\frac{1}{2}\cdot\frac{1}{2}-\frac{1}{2}\\&=\frac{1}{2}Adv_A=\frac{1}{2}\varepsilon\end{aligned}$$

因此，本方案中没有攻击者能在多项式时间内破坏系统。

2）在此方案中，用户的数据是安全的，不能被窃取。

①用户的私钥 SK_o 不能通过 $\{SK_{UID,AID_K}\}_{K\in I_A}$ 计算得出

在这个方案中，假设用于传输密钥的信道是安全的，SK_o 由数据所有者计算得出，不能通过 $\{SK_{UID,AID_K}\}_{K\in I_A}$ 计算得出，从而保证了数据所有者私钥的安全性。

②云服务器无法得到信息 m

云服务器从数据所有者处获得密文后，虽然可以从属性机构 AA 获得 $PK_{x,AID}$，但是无法获得 $\{SK_{UID,AID_K}\}_{K\in I_A}$，因此云服务器并不能获得明文。

③私有属性密钥安全

用户的所有私有属性密钥都是自行生成的，而解密过程中需要的密钥并没有对外传输，可以保证用户私有属性密钥的安全。

3）抗合谋攻击

在基于属性的加密系统中，抗合谋攻击是最为重要的安全特性之一。合谋攻击指系统中的属性机构中部分属性机构 AA 或者用户串通起来，彼此进行信息的交换，共享这些机构所具有的属性值，将密钥拼凑起来，试图获取更多的密文。在本方案中，由于每个用户的私钥 $SK_{UID,AID}=(PK_{UID})^{\frac{\gamma}{\beta}}\cdot g^{\frac{\alpha_{AID}}{\beta}}=g^{u\cdot\frac{\gamma}{\beta}}\cdot g^{\frac{\alpha_{AID}}{\beta}}$ 中都有不同的随机化参数，主密钥 $MK_o=\{\beta,\gamma\}$ 保存在数据所有者处，并没有对外传送，属性机构并不能通过运算获得随机参数 u。因此，即使用户或者属性机构 AA 进行串通，也无法通过拼凑密钥来对密文进行解密。因此，本方案是抗合谋攻击的。

4）前向安全

在基于属性加密的系统中，前向安全指任何已经被撤销权限的用户不能再对系统进行访问及任何操作，除非该用户未被撤销的剩余有效属性依旧能够满足访问结构的条件。在这个系统中，实现了属性更新机制，使得密钥和密文在用户的属性被撤销之后，都进行了更新，防止已经失去访问权限的用户对系统中的数据造成威胁。

本方案主要在文献[22]和文献[16]的基础上进行更改，取消原有方案中预解密的步骤，加入了重新封装的步骤，从而将私有属性的想法加入到了方案中。

在本方案中，重新封装步骤在云服务器上完成，最后的加密步骤在用户端完成，可以在保证密文安全的同时，提高用户端的计算效率。将与基于属性的加密方案相关的文献[22]中的方法和文献[16]中的方法与本方案进行比较，结果如表 1 所列。其中，n 是密文中属性的数量。可以看到，本文的方案在增强安全性的同时，并没有增加计算量。

表 1　算法的复杂度对比

Table 1　Comparison of complexity of algorithms

方案	访问策略	加密过程	解密过程
文献[22]方案	LSSS	$O(n)$	$O(n)$
文献[16]方案	LSSS	$O(n)$	$O(1)$
本文方案	LSSS	$O(n)$	$O(n)$

将本文的方案与当前主流的基于属性的密码方案在授权中心、可追踪性、可撤销性和基于属性加密方案类型方面进行对比，结果如表 2 所列，可以看出本文方案的安全属性比较全面。

表 2　相关方案的比较

Table 2　Comparison of relevant schemes

方案	多授权中心	可追踪	可撤销	CP-ABE	KP-ABE
文献[2]方案	×	×	×	×	√
文献[5]方案	×	×	×	√	×
文献[6]方案	×	×	×	√	×
文献[25]方案	×	√	√	√	×
文献[22]方案	√	×	√	√	×
文献[16]方案	√	×	√	√	×
本文方案	√	√	√	√	×

结束语　本文提出了一种应用于云服务器上多授权的基于属性的加密方法。在这个方案中，用户的身份和权限构成公有属性，公有属性实现对密文的访问控制，将用户的登录密码、设备的标识码作为私有属性参与用户私有属性密钥的生成，可以对密文的流转进行控制，使得指定用户在指定设备才能查看公文。并且提供了属性更新机制，确保了已失去权限的用户无法查阅公文，不会对公文造成任何危害。在整个方案的运行过程中，能够实现抗合谋攻击，防止用户或者属性机构通过获得的密钥进行串谋得到需要的密钥，危害系统安全。

参 考 文 献

[1] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]// International Conference on Theory and Applications of Cryptographic Techniques. Springer-Verlag, 2005: 457-473.

[2] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-Based Encryption for Fine-Grained Access Control of Encryption Data[C]// ACM Conference on Computer and Communication Security (CCS 2006). New York: ACM Press, 2006: 89-98.

[3] BETHENCOURTJ, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]// 2017 IEEE Symposium on Security and Privacy. Berkeley: IEEE Press, 2018(4): 321-334.

[4] CHASE M. Multi-authority attribute based encryption [C]// Theory of Cryptography. Berlin, Heidelberg: Springer Press, 2007: 515-534.

（下转第 168 页）

[13] TARTAKOVSKY A G,POLUNCHENKO A S,SOKOLOV G. Efficient Computer Network Anomaly Detection by Changepoint Detection Methods [J]. IEEE Journal of Selected Topics in Signal Processing,2013,7(1):4-11.

[14] YANG Y H,HUANG H Z,SHEN Q N,et al. Reserch on intrusion detection based on Incremental GHSOM[J]. Chinese Journal of Computers,2014,37(5):1217-1224. (in Chinese)
杨雅辉,黄海珍,沈晴霓,等. 基于增量式 GHSOM 神经网络模型的入侵检测研究[J]. 计算机学报,2014,37(5):1217-1224.

[15] FU M B. A Intrusion Detection System Based on Cluster Analysis[J]. Software Engineering,2016,19(4):10-12. (in Chinese)
付明柏. 一种基于聚类分析的入侵检测模型[J]. 软件工程,2016,19(4):10-12.

[16] LI J,DENG G,LI H,et al. The relationship between similarity measure and entropy of intuitionistic fuzzy sets[J]. Information Sciences,2012,188(1):314-321.

[17] ASKARI S,MONTAZERIN N. A high-order multi-variable Fuzzy Time Series forecasting algorithm based on fuzzy clustering[J]. Expert Systems with Applications,2015,42(9):2121-2135.

(上接第 129 页)

[5] GOYAL V,JIAN A,PANDEY O,et al. Bounded ciphertext policy attribute based encryption[C]// International Colloquium on Automata, Languages, and Programming. Berlin, Heidelberg: Springer Press,2008:579-591.

[6] WATER B. Ciphertext-policy attribute-based encryption:An expressive,efficient,and provably secure realization[C]// International Workshop on Public Key Cryptography. Taormina: Springer,2011:53-70.

[7] HINEK M J. Attribute-Based Encryption with Key Cloning Protection[J]. Cryptology Eprint Archive Report,2006,2008(4):803-819.

[8] RUJ S,NAYAK A,STOJMENOVIC I. DACC:Distributed Access. Control in Clouds[C]// 2011 IEEE 10th International Conference on Trust,Security and Privacy in Computing and Communications. Changsha:IEEE Press,2011:91-98.

[9] CHEN J,LIM H W,LING S,et al. Shorter IBE and signatures via asymmetric pairings [C]// International Conference on Pairing-Based Cryptography. Cologne: Springer Press, 2012: 122-140.

[10] LEWKO A B,WATERS B. New proof methods for attribute-based encryption:Achieving full security through selective techniques [C]// Advances in Cryptology-CRYPTO. Santa Barbara: Springer Press,2012:180-198.

[11] CHASE M. Multi-authority attribute-based encryption[C]// The Fourth Theory of Cryptography Conference (TCC 2007). Berlin,Heidelberg:Springer Press,2007:515-534.

[12] CAOZ F. New directions of modern cryptography [M]. Boca Raton:CRC Press,2012.

[13] LEWKO A B,Waters B. Decentralizing attribute-based encryption [C]// Annual International Conference on the Theory and Applications of Cryptographic Techniques. Tallinn: Springer, 2011:568-588.

[14] TANG Q,JI D Y. Multi-authority verifiable attribute based encryption[J]. Journal of Wuhan University(Science Edition), 2008,54(5):607-610. (in Chinese)
唐强,姬东耀. 多授权中心可验证的基于属性的加密方案[J]. 武汉大学学报(理学版),2008,54(5):607-610.

[15] LEWKO A,WATERS B. Decentralizing attribute-based encryption[C]// Advances in Cryptology-EUROCRYPT. 2011: 568-588.

[16] YANG K,JIA X H. Attributed-based Access Control for Multi-authority System in Cloud Storage[C]// 2012 IEEE 32nd International Conference on Distributed Computing Systems. Macau: IEEE Press,2012:536-545.

[17] YANG K,JIA X H. Expressive,Efficient and Revocable Data Access Control for Multi-Authority Cloud Storage[C]// IEEE Transactions on Parallel and Distributed Systems. IEEE Computer Society:IEEE Press,2013:1735-1744.

[18] ROUSELAKIS Y,WATERS B. Efficient statically-secure largeuniverse multi-authority attribute-based encryption [C]// International Conference on Financial Cryptography and Data Security. Berlin,Heidelberg:Springer Press,2015:315-332.

[19] YANG X D,YANG M M,YANG P,et al. A Multi-authority Attribute-Based Encryption Access Control for Social Network [C]// 2017 3rd IEEE International Conference on Control Science and Systems Engineering (ICCSSE). Beijing: IEEE Press, 2017:671-674.

[20] FENG D G,CHEN C. Research on Attribute-based Cryptography[J]. Journal of Cryptologic Research,2014,1(1):1-12. (in Chinese)
冯登国,陈成. 属性密码学研究[J]. 密码学报,2014,1(1):1-12.

[21] CAO Z F. New Development of Cryptography[J]. Journal of Sichuan University,2015,1(47):1-12. (in Chinese)
曹珍富. 密码学的新发展[J]. 四川大学学报,2015,1(47):1-12.

[22] CHEND W,WANL Q,WANG C,et al. A Multi-authority Attribute-based Encryption Scheme with Pre-decryption[C]// 2015 Seventh International Symposium on Parallel Architectures,Algorithms and Programming (PAAP). Nanjing: IEEE Press, 2015:223-228.

[23] HU P,GAO H Y. Key-Policy Attribute-Based Encryption Scheme for General Circuits[J]. Journal of Software,2016,27(6): 1498-1510. (in Chinese)
胡鹏,高海英. 一种实现一般电路的密钥策略的属性加密方案[J]. 软件学报,2016,27(6):1498-1510.

[24] BEIMEL A. Secure schemes for secret sharing and key distribution[J/OL]. Phd Thesis Israel Institute of Technology Technion, 1996. http://www. dphu. org/uploads/attachements/books/books_1542_0. pdf.

[25] LIU Z,CAO Z F,WONG D S. White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures[C]// IEEE Transaction on Information Forensics and Security. IEEE Signal Processing Society:IEEE Press, 2013:76-88.