(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 104038341 B
(45)授权公告日 2017.04.05

(21)申请号 201410280293.3

(22)申请日 2014.06.20

(65)同一申请的已公布的文献号
申请公布号 CN 104038341 A

(43)申请公布日 2014.09.10

(73)专利权人 北京航空航天大学
地址 100191 北京市海淀区学院路37号

(72)发明人 伍前红 邓桦 秦波 刘建伟 周云雅

(74)专利代理机构 北京慧泉知识产权代理有限公司 11232
代理人 王顺荣 唐爱华

(51)Int.Cl.
H04L 9/30(2006.01)
H04L 29/06(2006.01)

(56)对比文件
EP 2372948 A1,2011.10.05,
CN 102624522 A,2012.08.01,
CN 101807991 A,2010.08.18,
CN 103647644 A,2014.03.19,
Weiran Liu, Xiao Liu, Qianhong Wu, Bo Qin."Experimental performance comparisons between (H)IBE schemes over composite-order and prime-order bilinear groups".《Proceedings of 2014 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST)》.2014,全文.

审查员 王卓然

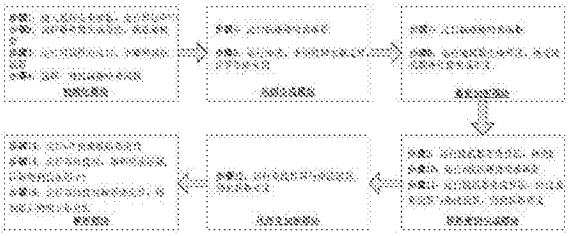
权利要求书4页 说明书11页 附图1页

(54)发明名称

一种基于身份的跨系统代理重加密方法

(57)摘要

一种基于身份的跨系统代理重加密方法，PKG运行的步骤：1、输入系数λ，输出系统参数；2、运行随机数生成算法；3、计算双线性对、求幂和乘法；4、选择一种抗碰撞哈希函数，输出公钥；5、运行抗碰撞哈希函数；6、计算加法、求倒和幂，输出私钥；授权方运行的步骤：7、运行抗碰撞哈希函数；8、运行随机数生成算法、乘法和求幂运算，输出密文；9、选择盲化因子k；10、运行抗碰撞哈希函数；11、运行随机数生成算法、乘法和求幂运算，输出转换密钥；代理方运行的步骤：12、计算双线性对和除法，输出重加密密文；被授权方运行的步骤：13、运行抗碰撞哈希函数；14、计算双线性对、加法、连乘和除法，输出k；15、计算双线性对和乘法，输出明文。



CN 104038341 B

1.一种基于身份的跨系统代理重加密方法，该方法的实施是基于下述模块：

模块一：初始化模块

私钥生成中心即PKG在这一模块中将系统安全参数λ、基于身份的广播加密方法即IBBE系统中被授权用户集合所能包含的用户数量上限m-1作为输入，输出主密钥MSK_{IBE}、MSK_{IBBE}，以及公钥PK_{IBE}、PK_{IBBE}；公钥能公开，而主密钥则须PKG严格保密，不可泄露；

模块二：私钥生成模块

该模块由PKG分别为IBE系统和IBBE系统中的用户分配私钥，模块输入某一用户在系统中的身份ID和主密钥MSK_{IBE}或MSK_{IBBE}，生成对应的私钥SK_{IBE}或SK_{IBBE}，并将输出的私钥发送给各系统用户保管；

模块三：数据加密模块

IBE加密系统中的授权方Delegator在这一模块中将公钥PK_{IBE}和自己的身份ID_{IBE}以及待加密的消息M作为输入，输出加密后的密文CT_{IBE}，并将密文数据上传到文件管理方外包存储；

模块四：转换密钥生成模块

IBE加密系统中的授权方即Delegator在这一模块中根据自己的从PKG处获得的私钥SK_{IBE}、IBBE加密系统中被授权用户即Delegatee的身份集合S以及IBBE加密系统的公钥PK_{IBBE}，计算生成转换密钥——$RK_{IBE\to IBBE}$，并将生成的转换密钥传送给代理重加密方用以重加密时使用；

模块五：代理重加密模块

代理重加密方即Proxy在得到Delegator生成的转换密钥之后，从文件管理方处下载授权方上传的加密数据CT_{IBE}，并根据转换密钥$RK_{IBE\to IBBE}$和需要转换的密文CT_{IBE}，计算方得转换后的密文；

模块六：解密模块

假设某一被授权方即Delegatee在所有被授权方的身份集合S中的身份为ID_{iIBBE}，对应IBBE加密系统中的私钥为SK_{iIBBE}；被授权方即Delegatee收到PKG生成的私钥且从代理重加密方即Proxy处下载获得重加密密文$CT_{IBE\to IBBE}$之后，根据自己的私钥信息SK_{IBBE}和所有被授权方的身份集合S，能解密得到盲化因子k，经一步简单的运算就能得到明文消息M；

其特征在于：该加密方法步骤如下：

步骤1：PKG首先输入系统安全参数λ，然后运行算法$\mathcal{G}(1^{\lambda})$，输出两个阶数为素数p的群$\mathbb{G}$、$\mathbb{G}_T$和一个双线性映射运算$e:\ \mathbb{G}\times\mathbb{G}\to\mathbb{G}_T$；

步骤2：$g\overset{R}{\leftarrow}\mathbb{G}$，$h\overset{R}{\leftarrow}\mathbb{G}$，$\alpha\overset{R}{\leftarrow}Z_p^*$

PKG接下来运行随机数生成算法，随机选择$\mathbb{G}$群中的某个生成元g，$\mathbb{G}$群中的一个元素h，以及Z_p^*域中的一个元素α作为随机指数；

步骤3：PKG运行一次双线性对运算、两次求幂运算和(m-1)次乘法运算，得到$\mathbb{G}_T$群中的一个元素e(g,h)，和$\mathbb{G}$群中的(m+1)个元素g^{α}、h^{α}，...，h^{α^m}；

步骤4：PKG选择一种抗碰撞哈希函数H(•)，该函数满足抗碰撞哈希函数的所有特性，输入为任意的字符串，输出为映射到域Z_p^*中的某一元素；

经过上述四个步骤得到的参数：

$$PK_{IBBE}=(g^{\alpha},e(g,h),h,h^{\alpha},...,h^{\alpha^{m}},H(\cdot))$$

作为IBBE加密系统的公钥能对外公开；IBE加密系统的公钥与上述公钥不同，为：

$$PK_{IBE}=(g^{\alpha},e(g,h),h,h^{\alpha},h^{\alpha^{2}},H(\cdot))$$

IBE和IBBE加密系统的主密钥相同，为：

$MSK_{IBE}=MSK_{IBBE}=(g,\alpha)$

由PKG保管；

步骤5：PKG运行抗碰撞哈希函数H(•)，计算得到

$$H(ID_{IBE}),H(ID_{IBBE})\in Z_p^*$$

公式中的ID_{IBE}代表IBE加密系统中用户的身份，ID_{IBBE}代表IBBE加密系统中用户的身份，均用一串任意的字符串表示；

步骤6：PKG运行一次加法运算，一次求倒数运算和求指数运算，按照下面公式计算得到IBE加密系统中的用户私钥：

$$SK_{IBE}=g^{\frac{1}{\alpha+H(ID_{IBE})}}$$

以及，IBBE加密系统中用户的私钥：

$$SK_{IBBE}=g^{\frac{1}{\alpha+H(ID_{IBBE})}}$$

步骤7：授权方即Delegator运行抗碰撞哈希函数H(•)，计算得到$H(ID_{IBE})\in Z_p^*$；

步骤8：授权方即Delegator运行随机数生成算法，随机选择域Z_p^*中的一个元素s作为指数，按照下面公式运行两次乘法和三次求幂运算，得到：

$$C_0=M\cdot e(g,h)^{s},C_1=h^{\alpha s}h^{H(ID)s}=h^{s(\alpha+H(ID_{IBE}))}$$

最后的密文输出为：$CT_{IBE}=(C_0,C_1)$，该密文是根据Delegator的身份ID_{IBE}加密，故只有授权方即Delegator自己的私钥SK_{IBE}能解密；

步骤9：授权方即Delegator首先运行随机数生成算法，随机选择$\mathbb{G}$群中的某个元素$k\in\mathbb{G}$，作为盲化因子；

步骤10：针对被授权方即Delegatee身份集合S中的每个身份，授权方即Delegator运行n次抗碰撞哈希函数H(•)，得到：

$H(ID_{1IBBE}),H(ID_{2IBBE})\cdots H(ID_{nIBBE})$

其中n代表用户集合中的身份数量；

步骤11：授权方即Delegator运行随机数生成算法，随机选择域Z_p^*中的一个元素v作为指数；按照下式运行多项式次求幂运算和乘法运算，得到：

$C_0'=k\cdot e(g,h)^{v}$，$C_1'=h^{v(\alpha+H(ID_{1IBBE}))(\alpha+H(ID_{2IBBE}))\cdots(\alpha+H(ID_{nIBBE}))}$将得到的结果表示为：

$R=(C_0',C_1')$

经过最后一步乘法运算$SK_{IBE}\cdot k$，授权方即Delegator便生成了转换密钥：

$RK_{IBE\rightarrow IBBE}=(SK_{IBE}\cdot k,R)$

其中，被授权方即Delegatee的身份集合S默认为所有集合内的用户均知晓；

步骤12：代理重加密方即Proxy按照下式运行一次双线性对和一次除法运算，

得到：$$D_0=\frac{C_0}{e(SK_{IBE}\cdot k,C_1)}=\frac{Me(g,h)^s}{e(g^{\frac{1}{\alpha+H(ID_{IBE})}},h^{s(\alpha+H(ID_{IBE}))})e(k,h^{s(\alpha+H(ID_{IBE}))})}$$

$$=\frac{M}{e(k,h^{s(\alpha+H(ID_{IBE}))})}$$

经过代理重加密后的密文为：

$CT_{IBE\rightarrow IBBE}=(D_0,C_1,R)$；

步骤13：被授权方即Delegatee首先针对被授权用户的身份集合S中的每个身份，运行一次抗碰撞哈希函数H(•)得到：

$H(ID_{1IBBE}),H(ID_{2IBBE})\cdots H(ID_{nIBBE})$

式中的n代表用户集合中的身份数量；

步骤14：被授权方即Delegatee按照下式运行两次双线性对运算和多项式次加法、连乘运算得到：

$$A=(e(g^{-\alpha v},h^{\frac{1}{\alpha}(\prod_{j=1,j\neq i}^{n}(\alpha+H(ID_{jIBBE}))-\prod_{j=1,j\neq i}^{n}H(ID_{jIBBE}))})\cdot e(SK_{iIBBE},C_1'))^{\frac{1}{\prod_{j=1,j\neq i}^{n}H(ID_{jIBBE})}}$$

$$(e(g,h)^{-v(\prod_{j=1,j\neq i}^{n}(\alpha+H(ID_{jIBBE}))-\prod_{j=1,j\neq i}^{n}H(ID_{jIBBE}))}$$

$$\cdot e(g^{\frac{1}{\alpha+H(ID_{iIBBE})}},g^{\frac{1}{v(\prod_{j=1}^{n}\alpha+H(ID_{jIBBE}))}}))^{\frac{1}{\prod_{j=1,j\neq i}^{n}H(ID_{jIBBE})}}$$

$$=e(g,h)^v$$

再进行一次除法运算即能得到盲化因子k：

$$k=\frac{C_0'}{A}A=\frac{ke(g,h)^v}{e(g,h)^v}$$；

步骤15：最后，被授权方即Delegatee按照下式经过一次双线性对和乘法运算，得到最后的明文消息M：

$$M=D_0\cdot e(k,C_1)$$

$$=\frac{M}{e(k,h^{s(\alpha+H(ID_{IBE}))})}\cdot e(k,h^{s(\alpha+H(ID_{IBE}))})$$。

2.根据权利要求1所述的一种基于身份的跨系统代理重加密方法，其特征在于：在步骤1中所述的“算法$\mathcal{G}(1^{\lambda})$”，其运行方法如下：私钥生成中心即PKG输入系统安全参数λ，根据λ的大小，系统选择相应的椭圆曲线：$Y^2=X^3+aX+b$，a和b是系数，再由椭圆曲线上的点构成两个素数p阶的群$\mathbb{G}$、$\mathbb{G}_T$；选择一种函数映射e，将群$\mathbb{G}$中的元素映射到群$\mathbb{G}_T$中去；安全参数数

值越大，所选择椭圆曲线上的点也越多，群也越大。

3.根据权利要求2所述的一种基于身份的跨系统代理重加密方法，其特征在于：步骤1中所选的椭圆曲线：$Y^2=X^3+aX+b$，随机选择自变量X的一个值x_1，计算对应因变量Y的值y_1；若点(x_1,y_1)在想要映射的群中，则成功生成了随机元素；若点(x_1,y_1)不在群中，则继续选择X的值，直到找到出现在群中的点；此外，域Z_p^*表示集合{1,2,...,p-1}，随机选择域Z_p^*中元素的随机数生成函数能从Pairing-BasedCryptosystems函数包中调用库函数运行。

4.根据权利要求1所述的一种基于身份的跨系统代理重加密方法，其特征在于：在步骤3中所述的“运行双线性对运算”，其做法如下：自变量的输入为群$\mathbb{G}$中的元素g、h，输出为群$\mathbb{G}_T$中的元素：e(g,h)。

5.根据权利要求1所述的一种基于身份的跨系统代理重加密方法，其特征在于：在步骤4中所述的“抗碰撞哈希函数H(•)”，同样能从Pairing-Based Cryptosystems函数包中调用库函数运行。

一种基于身份的跨系统代理重加密方法

(一)技术领域:

[0001] 本发明涉及一种基于身份的跨系统代理重加密方法,可实现不同加密系统下密文的代理转换,属于信息安全中密码学领域。

(二)技术背景:

[0002] 随着通信安全性的提高,多种密码体制被提出用以对数据进行加密传输,保证了用户之间的通信隐私安全,基于身份的公钥加密体制就是被广泛应用的一种。根据通信双方所采用的密钥是否相同,将数据加密的体制分为两种:单钥加密体制与公钥加密体制;公钥加密是与单钥加密相对的一种加密体制,两者均强调加密算法可以公开,而解密密钥必须严格保密,一旦密钥泄露则整个加密的数据就不安全了。两者的不同之处在于,单钥加密的加密密钥与解密密钥是相同的,而公钥加密的加密密钥与解密密钥是不同的。在公钥加密体制中,公钥用以对要加密的信息(这里我们称之为明文)加密,而私钥则用来对加密后的信息(这里我们称之为密文)加密。

[0003] 基于身份的加密方法——Identity-Based Encryption(IBE)最开始是由Shamir提出的,属于公钥加密体制。参与方通常为加、解密方和私钥生成中心。在IBE系统中,解密方的身份ID作为加密的公钥,该身份ID可以是解密方的身份证号码、邮箱地址或是电话号码等。加密方根据公钥对明文进行加密,私钥生成中心——Private Key Generator(PKG)负责根据系统中用户的身份对用户发放私钥,只有解密方的身份与公钥一致,方可解密。该加密方法的优势在于,解除了公钥基础设施——Public Key Infrastructure(PKI)对用户发放认证证书的环节,减轻了系统的开销,更具有实用意义。

[0004] 在IBE这种高效快捷的加密算法基础上又衍生出了许多基于身份的多功能加密方法,其中就包括基于身份的广播加密方法——Identity-Based Broadcast Encryption(IBBE)。IBBE加密方法主要用于解决加密用户同时对多解密用户进行广播加密的应用需求,加密用户在加密时使用的公钥为所有解密用户的身份组成的集合,只有在该身份集合中的用户才可以成功对密文解密。譬如,我们参考这样一种应用场景:某医院的主治医生A想与其他各大医院的n位医生共同讨论分析某位病人的病历信息,由于考虑到病人信息的敏感性并出于保护病人隐私的考虑,医生A在发送病历之前对病历信息进行了加密。若此处采用IBE加密方法,首先A需要根据n个医生的身份分别对病历信息加密,生成n份密文;若采用IBBE加密方法,A仅须根据n个医生的身份组成的身份集合对病历信息加密一次,生成一份密文,身份集合中的医生即可对密文解密;该方法大大节省了加密用户的时间与精力,降低了密文存储的开销,方法更加高效。

[0005] 除此之外,我们考虑另一种应用场景:邮箱用户Alice有一封加密邮件想与另一用户Bob共享,但该邮件是以Alice的身份作为公钥,在IBE加密系统下加密的,Bob不知晓Alice的私钥时无法完成解密。而Alice不想泄露自己私钥的前提下,传统的做法是:Alice使用自己的私钥对邮件进行解密,再使用Bob的身份对解密后的明文再次加密。将密文传送给Bob;Bob使用自己的私钥对收到的密文解密,从而完成了邮件内容的共享。无疑上述做法

是繁杂且耗时的，因而衍生出一种称为：“代理重加密”——Proxy re-encryption(PRE)的解决方法。代理重加密的概念最早是由Blaze、Bleumer和Strauss三位科学家在1998年的欧洲密码学年会上提出的，在PRE方案中，通信参与方分别为私钥生成中心——PKG、解密授权方(Delegator)、代理重加密方(Proxy)和被授权方(Delegatee)。在上述应用场景下，若采用代理重加密方法，Alice作为Delegator仅需根据自己的私钥和Bob的身份计算生成一个转换密钥——Re-encryption Key(RK)，并将密文和转换密钥同时发送给代理重加密方；代理重加密方使用转换密钥，在完全不知晓明文内容和Alice私钥信息的前提下将只有Alice的私钥可解密的密文重加密得到Bob的私钥可解密的密文。这样，Bob只需从代理重加密方处下载重加密后的密文，使用自己的私钥完成密文的解密即可。代理重加密方法运行的过程中，省去了Delegator对原始密文先解密再加密的步骤，节约了用户与系统的开支；除此之外，代理重加密方在重加密环节中不可获知任何有关明文与用户私钥的信息，数据在整个外界存储的过程中都是以密文形式存在的，保障了复杂的分布式网络环境下的数据安全。

[0006] 根据代理重加密的加密方向的不同，代理重加密可以分为单向的代理重加密和双向的代理重加密；单向的代理重加密可以实现将Delegator的公钥加密的密文转换成被授权方Delegatee的公钥加密的密文，反向不可以；双向的代理重加密则可以同时实现反向的密文转换。

[0007] 随着代理重加密方法的提出，越来越多的加密方法与代理重加密的思想结合起来形成了不同加密系统下的代理重加密方案。考虑目前已有的代理重加密方案，密文转换前后的加密系统均是相同的；也就是说，若使用IBE加密系统加密的密文经过代理重加密之后仍为IBE加密系统下的密文，这在某些应用场景下局限了用户的适用范围。以云环境下的用户信息加密存储为例，该类用户在自己存储能力不足的限制下，选择将数据上传到云端服务器，出于保护数据的安全性及节省存储开销的目的，将持有分布式存储数据的用户以IBE加密系统组织起来，每个数据持有用户由PKG分配了独一无二的公、私钥对；在数据持有用户将数据上传到云端服务器之前，首先根据自己被分配到的公钥对数据进行加密，再传送至云端存储。加密后的数据只有该用户自己可以解密，避免了数据遭到恶意服务器泄密的危险。

[0008] 然而，当数据持有用户想与多个用户进行数据共享时，若采用现有的代理重加密方法，则出现了两点限制：首先被授权用户同样需要在该IBE加密系统之中拥有合法身份；其次授权用户需要根据每一个被授权用户的身份生成转换密钥发送给代理方。当被授权方是以其他加密系统组织起来的情况下，现有的代理重加密便无法成功进行。因此，我们发明了一种适用范围更广、功能更加全面的“跨加密系统代理重加密”方法——可轻松实现从IBE加密系统到IBBE加密系统的代理密文转换。在本发明方法中IBE加密系统和IBBE加密系统是彼此独立存在的，分别具有自己的系统参数，代理方在转换过程中充当了桥梁的作用，将IBE系统与IBBE系统联系起来。通过转换密钥，将IBE系统中公钥加密后的密文转换成IBBE系统中公钥加密后的密文，实现了用户的跨系统解密。

[0009] 由于IBE加密系统和IBBE加密系统不仅所使用的公钥不同，而且IBE加密系统中密文是根据一个身份加密的，IBBE是根据多个身份构成的身份集合加密的，两者加密后的密文结构形式必然有很大的差异，如何成功实现密文转换，是我们的发明主要解决的问题。基

于现有的一种高效简洁的IBBE加密方案，我们构造了一种全新的IBE加密系统。首先，我们令授权方将原始消息使用自己的公钥，按照我们设计出的IBE加密系统加密，只有授权方自己的私钥可以成功解密。随后，授权方方选择随机数，盲化自己的私钥，将该随机数依照被授权用户的身份集合，利用IBBE系统中的系统参数加密。满足身份在被授权用户集合中的用户可以成功解密得到该随机值，最后恢复出明文信息。此外，本发明为单向的代理重加密方法，授权方与代理方无法合谋达到解密被授权方的密文的目的，从而最大程度地保护了被授权人的数据安全。

(三)发明内容：

[0010] 1、目的：一种基于身份的跨系统代理重加密方法

[0011] 本发明的目的是提出一种基于身份的跨系统代理重加密方法，它是一种在不同加密系统下的身份基代理重加密方法，该方法结合了现有身份基加密技术和代理重加密技术的优势，可轻松实现从授权方到被授权方的密文转换，同时保护明文信息在整个重加密过程中不会遭到代理重加密方的恶意泄露；同时我们根据现有的身份基广播加密(IBBE)方案重新设计了新颖的的身份基加密(IBE)系统，在保留了现有IBBE加密系统解密速度快、密文短等特性的同时，使跨IBE到IBBE系统的密文转换成为可能。

[0012] 2、技术方案：

[0013] 本发明包括五个实体：1)私钥生成中心(Private Key Generator,PKG)：具有验证用户身份，计算生成、分发用户私钥功能的机构；2)解密授权方(Delegator)：具有加密、生成转换密钥功能的的个人或社会机构；3)代理重加密方(Proxy)：具有根据重加密密钥Re-encryption Key(RK)转换密文的个人或社会机构；4)解密被授权方(Delegatee)：具有解密功能的的个人或社会机构；5)文件管理方(File Manager)：具有存储数据功能的社会机构。

[0014] 首先，我们定义用户的身份——ID，代表用户在系统中的身份，表示为一串任意的字符串。其次，我们定义IBBE系统中用户身份集合——S，代表广播加密面向的用户身份集合，集合中的元素为IBBE系统中用户的身份。由于本发明所设计的算法中使用了双线性映射和抗碰撞哈希函数这两方面的数学知识。特在此对双线性映射和抗碰撞哈希函数的定义和特性做出解释。

[0015] 2.1双线性对

[0016] 我们定义一种函数映射e(.,.)，将群$\mathbb{G}$中的元素映射到群$\mathbb{G}_T$中去，即：

[0017] $e:\mathbb{G}\times\mathbb{G}\rightarrow\mathbb{G}_T$；

[0018] 双线性对满足的特性有：

[0019] ①双线性特性：对于$g,h\in\mathbb{G}$，$a,b\in\mathbb{Z}_p$，有$e(g^a,h^b)=e(g,h)^{ab}$成立；

[0020] ②非退化性：$\mathbb{G}$群中至少存在一个元素g，使得计算后的e(g,g)为$\mathbb{G}_T$群的某个生成元；

[0021] ③可计算性：存在有效的算法，使得所有的$u,v\in\mathbb{G}$，可以有效计算出e(u,v)的值；

[0022] 其中，Z_p表示集合{0,1,2,...,p-1}。

[0023] 2.2抗碰撞哈希函数

[0024] 本发明中使用的哈希函数具备两个基本特性：单向性和抗碰撞性；单向性是指只

能从哈希函数的输入推导出输出，而不能从哈希函数的输出计算出输入；抗碰撞性是指不能找到两个不同的哈希函数输入使其哈希后的结果相同。本发明中的哈希算法输入是用户的身份ID，以任意字符串形式表示；输出为映射到域Z_p中的元素。

[0025] 2.3方案内容

[0026] 本发明为一种基于身份的跨系统代理重加密方法，该方法由初始化模块、数据加密模块、私钥生成模块、转换密钥生成模块、代理重加密模块和解密模块，六个模块共15个步骤实现其功能，本发明所设计的代理重加密方法的系统架构图如图1所示，现结合图1将本发明所述方法及各模块的功能介绍如下。

[0027] 本发明一种基于身份的跨系统代理重加密方法，其作法如下：

[0028] 模块一：初始化模块

[0029] PKG在这一模块中将系统安全参数λ、IBBE系统中被授权用户集合所能包含的用户数量上限(m-1)作为输入，输出主密钥MSK_{IBE}、MSK_{IBBE}，以及公钥PK_{IBE}、PK_{IBBE}。公钥可以公开，而主密钥则须PKG严格保密，不可泄露。该模块功能的实现具体分为下述四步：

[0030] 步骤1：PKG首先输入系统安全参数λ，然后运行算法$g(1^{\lambda})$，输出两个阶数为素数p的群$\mathbb{G}$、$\mathbb{G}_T$和一个双线性映射运算e: $\mathbb{G}\times\mathbb{G}\rightarrow\mathbb{G}_T$；

[0031] 步骤2：$g\overset{R}{\leftarrow}\mathbb{G}$，$h\overset{R}{\leftarrow}\mathbb{G}$，$\alpha\overset{R}{\leftarrow}Z_p^*$

[0032] PKG接下来运行随机数生成算法，随机选择$\mathbb{G}$群中的某个生成元g，$\mathbb{G}$群中的一个元素h，以及Z_p^*域中的一个元素α作为随机指数；

[0033] 步骤3：PKG运行一次双线性对运算、两次求幂运算和(m-1)次乘法运算，得到$\mathbb{G}_T$群中的一个元素e(g,h)，和$\mathbb{G}$群中的(m+1)个元素g^{α}、h^{α}，...，h^{α^m}；

[0034] 步骤4：最后，PKG选择一种抗碰撞哈希函数H(•)，该函数满足抗碰撞哈希函数的所有特性，输入可以为任意的字符串，输出为映射到域Z_p^*中的某一元素。经过上述四个步骤得到的参数：

[0035] $$PK_{IBBE}=(g^{\alpha},e(g,h),h,h^{\alpha},...,h^{\alpha^m},H(\cdot))$$

[0036] 作为IBBE加密系统的公钥可以对外公开；IBE加密系统的公钥与上述公钥不同，为：

[0037] $$PK_{IBE}=(g^{\alpha},e(g,h),h,h^{\alpha},h^{\alpha^2},H(\cdot))$$

[0038] IBE和IBBE加密系统的主密钥相同，为：

[0039] $MSK_{IBE}=MSK_{IBBE}=(g,\alpha)$

[0040] 由PKG保管；

[0041] 其中，在步骤1中所述的“算法$g(1^{\lambda})$”，其运行方法如下：私钥生成中心(PKG)输入系统安全参数λ，根据λ的大小，系统选择相应的椭圆曲线：$Y^2=X^3+aX+b$(a和b是系数)，再由椭圆曲线上的点构成两个素数p阶的群$\mathbb{G}$、$\mathbb{G}_T$。选择一种函数映射e，将群$\mathbb{G}$中的元素映射到群$\mathbb{G}_T$中去；安全参数数值越大，所选择椭圆曲线上的点也越多，群也越大。

[0042] 其中，在步骤2中所述的“随机数生成算法”，其做法如下：根据步骤1中所选的椭圆

曲线：$Y^2=X^3+aX+b$，随机选择自变量X的一个值x_1，计算对应因变量Y的值y_1；若点(x_1,y_1)在我们想要映射的群中，则成功生成了随机元素。若点(x_1,y_1)不在群中，则继续选择X的值，直到找到出现在群中的点。此外，域Z_p^*表示集合{1,2,...,p-1}，随机选择域Z_p^*中元素的随机数生成函数可以从Pairing-Based Cryptosystems函数包中调用库函数运行。下文中提到的随机数生成算法皆按上述方法运行。

[0043] 其中，在步骤3中所述的“运行双线性对运算”，其做法如下：自变量的输入为群$\mathbb{G}$中的元素g、h，输出为群$\mathbb{G}_T$中的元素：e(g,h)。

[0044] 其中，在步骤4中所述的“抗碰撞哈希函数H(·)”，同样可以从Pairing-Based Cryptosystems函数包中调用库函数运行。

[0045] 模块二：私钥生成模块

[0046] 该模块由PKG分别为IBE系统和IBBE系统中的用户分配私钥，模块输入某一用户在系统中的身份ID和主密钥MSK_{IBE}或MSK_{IBBE}，生成对应的私钥SK_{IBE}或SK_{IBBE}，并将输出的私钥发送给各系统用户保管。该模块功能的实现为下述两步：

[0047] 步骤5：PKG运行抗碰撞哈希函数H(·)，计算得到

[0048] $$H(ID_{IBE}),H(ID_{IBBE})\in Z_p^*;$$

[0049] 公式中的ID_{IBE}代表IBE加密系统中用户的身份，ID_{IBBE}代表IBBE加密系统中用户的身份，均用一串任意的字符串表示；

[0050] 步骤6：PKG运行一次加法运算，一次求倒数运算和求指数运算，按照下面公式计算得到IBE加密系统中的用户私钥：

[0051] $$SK_{IBE}=g^{\frac{1}{\alpha+H(ID_{IBE})}}$$

[0052] 以及，IBBE加密系统中用户的私钥：

[0053] $$SK_{IBBE}=g^{\frac{1}{\alpha+H(ID_{IBBE})}};$$

[0054] 模块三：数据加密模块

[0055] IBE加密系统中的授权方(Delegator)在这一模块中将公钥PK_{IBE}和自己的身份ID_{IBE}以及待加密的消息M作为输入，输出加密后的密文CT_{IBE}，并将密文数据上传到文件管理方外包存储。该模块功能的实现分下述两步：

[0056] 步骤7：授权方即Delegator运行抗碰撞哈希函数H(·)，计算得到$H(ID_{IBE})\in Z_p^*$；

[0057] 步骤8：授权方即Delegator运行随机数生成算法，随机选择域Z_p^*中的一个元素s作为指数，按照下面公式运行两次乘法和三次求幂运算，得到：

[0058] $C_0=M\cdot e(g,h)^s$，$C_1=h^{\alpha s}h^{H(ID)s}=h^{s(\alpha+H(ID_{IBE}))}$

[0059] 最后的密文输出为：$CT_{IBE}=(C_0,C_1)$，该密文是根据Delegator的身份ID_{IBE}加密，故只有Delegator自己的私钥SK_{IBE}可以解密；

[0060] 模块四：转换密钥生成模块

[0061] IBE加密系统中的授权方(Delegator)在这一模块中根据自己的从PKG处获得的私

钥SK_{IBE}、IBBE加密系统中被授权用户(Delegatee)的身份集合S以及IBBE加密系统的公钥PK_{IBBE},计算生成转换密钥——$RK_{IBE\rightarrow IBBE}$,并将生成的转换密钥传送给代理重加密方用以重加密时使用。该模块功能的实现具体分为下述三步:

[0062] 步骤9:授权方即Delegator首先运行随机数生成算法,随机选择$\mathbb{G}$群中的某个元素$k\in\mathbb{G}$,作为盲化因子;

[0063] 步骤10:针对被授权用户(Delegatee)身份集合S中的每个身份,Delegator运行n次抗碰撞哈希函数H(·),得到:

[0064] $H(ID_{1IBBE})$,$H(ID_{2IBBE})\cdots H(ID_{nIBBE})$

[0065] 其中n代表用户集合中的身份数量;

[0066] 步骤11:授权方即Delegator运行随机数生成算法,随机选择域Z_p^*中的一个元素v作为指数;按照下式运行多项式次求幂运算和乘法运算,得到:

[0067] $C_0'=k\cdot e(g,h)^v$,$C_1'=h^{v(\alpha+H(ID_{1IBBE}))(\alpha+H(ID_{2IBBE}))\cdots(\alpha+H(ID_{nIBBE}))}$

[0068] 我们将得到的结果表示为:

[0069] $R=(C_0',C_1')$

[0070] 经过最后一步乘法运算$SK_{IBE}\cdot k$,授权方便生成了转换密钥:

[0071] $RK_{IBE\rightarrow IBBE}=(SK_{IBE}\cdot k,R)$

[0072] 其中,被授权用户(Delegatee)的身份集合S默认为所有集合内的用户均知晓。

[0073] 模块五:代理重加密模块

[0074] 代理重加密方(Proxy)在得到Delegator生成的转换密钥之后,从文件管理方处下载授权方上传的加密数据CT_{IBE},并根据转换密钥$RK_{IBE\rightarrow IBBE}$和需要转换的密文CT_{IBE},计算方得转换后的密文,该模块的功能由下述一步计算实现:

[0075] 步骤12:Proxy按照下式运行一次双线性对和一次除法运算,得到:

[0076]
$$D_0=\frac{C_0}{e(SK_{IBE}\cdot k,C_1)}=\frac{Me(g,h)^s}{e(g^{\frac{1}{\alpha+H(ID_{IBE})}},h^{s(\alpha+H(ID_{IBE}))})e(k,h^{s(\alpha+H(ID_{IBE}))})}$$
$$=\frac{M}{e(k,h^{s(\alpha+H(ID_{IBE}))})}$$

[0077] 经过代理重加密后的密文为:

[0078] $CT_{IBE\rightarrow IBBE}=(D_0,C_1,R)$;

[0079] 模块六:解密模块

[0080] 我们假设某一被授权方(Delegatee)在被授权用户的身份集合S中的身份为ID_{iIBBE},对应IBBE加密系统中的私钥为SK_{iIBBE}。Delegatee收到PKG生成的私钥且从代理重加密方(Proxy)处下载获得重加密密文$CT_{IBE\rightarrow IBBE}$之后,根据自己的私钥信息SK_{IBBE}和被授权用户的身份集合S,可以解密得到盲化因子k,经一步简单的运算就可得到明文消息M,该模块的功能实现具体分为下述3步:

[0081] 步骤13:被授权方即Delegatee首先针对被授权用户的身份集合S中的每个身份,运行一次抗碰撞哈希函数H(·)得到:

[0082] $H(ID_{1IBBE}),H(ID_{2IBBE})\cdots H(ID_{nIBBE})$

[0083] 式中的n代表用户集合中的身份数量；

[0084] 步骤14：被授权方即Delegatee按照下式运行两次双线性对运算和多项式次加法、连乘运算得到：

$$A=\left(e(g^{-\alpha v},h^{\frac{1}{\alpha}(\prod_{j=1,j\neq i}^{n}(\alpha+H(ID_{jIBBE}))-\prod_{j=1,j\neq i}^{n}H(ID_{jIBBE}))})\cdot e(SK_{iIBBE},C_1')\right)^{\frac{1}{\prod_{j=1,j\neq i}^{n}H(ID_{jIBBE})}}$$

$$(e(g,h)^{-v(\prod_{j=1,j\neq i}^{n}(\alpha+H(ID_{jIBBE}))-\prod_{j=1,j\neq i}^{n}H(ID_{jIBBE}))}$$

[0085]

$$\cdot e(g^{\frac{1}{\alpha+H(ID_{iIBBE})}},g^{\frac{1}{v(\prod_{j=1}^{n}\alpha+H(ID_{jIBBE}))}}))^{\frac{1}{\prod_{j=1,j\neq i}^{n}H(ID_{jIBBE})}}$$

$$=e(g,h)^{v}$$

[0086] 再进行一次除法运算即可得到盲化因子k：

[0087] $$k=\frac{C_0'}{A}A=\frac{ke(g,h)^{v}}{e(g,h)^{v}}$$；

[0088] 步骤15：最后，被授权方即Delegatee按照下式经过一次双线性对和乘法运算，得到最后的明文消息M：

$$M=D_0\cdot e(k,C_1)$$

[0089]

$$=\frac{M}{e(k,h^{s(\alpha+H(ID_{IBE}))})}\cdot e(k,h^{s(\alpha+H(ID_{IBE}))})$$

[0090] 3、优点及功效：

[0091] 本发明提供一种基于身份的跨系统代理重加密方法，可用于授权方与被授权方处于不同加密系统下的密文转换，其优点和功效是：

[0092] 1)本发明方法首先在已有身份基广播加密(IBBE)方案基础上，构造了一种身份基加密(IBE)方案，该方案具有密钥小、密文短的优点。

[0093] 2)本发明方法引入了代理重加密方，将用授权方的公钥加密的密文转换成用被授权方的公钥加密的密文，使得重加密之前只能用授权方的私钥解密的密文转换成了被授权方的私钥也可以解密的密文，使得加密信息的共享既节约了繁琐的解密再加密的步骤，同时保障了分享信息的安全性。

[0094] 3)本发明方法与以往的代理重加密方法最大的优势与创新点在于：该方法通过代理重加密的思想将不同加密系统下的用户联系起来，轻松地实现加密信息的共享；现有的代理重加密方法只适用于授权方和被授权方处于相同加密系统下的情况，这大大限制了用户的适用范围。本发明方法结合现今已广泛投入使用的身份基加密和身份基广播加密方法，通过代理方的参与使得跨系统的加密文件共享成为可能。

[0095] 4)本发明方法中的授权方在代理加密之前只需根据自己的私钥和IBBE加密系统

下的用户身份集合S，根据IBBE系统的公钥信息即可生成转换密钥；首先盲化授权方自己的私钥，再对盲化信息使用IBBE系统加密，保证了只有身份在S中的用户可以解密出盲化信息从而恢复出最终的明文。

[0096] 5)本发明方法中的代理重加密方在得到IBE系统下的密文和转换密钥后对密文进行重加密的过程中，不可知晓有关用户私钥及明文的任何信息，该方法特别适用在代理重加密方不完全可信的应用环境中。

(四)附图说明：

[0097] 图1为本发明所述方法的系统架构图。

[0098] 图2为本发明所述方法的流程框图。

(五)具体实施方式

[0099] 本发明为一种基于身份的跨系统代理重加密方法，见图1、2所示，该方法由初始化模块、私钥生成模块、数据加密模块、转换密钥生成模块、代理重加密模块和解密模块这六个模块实现。整个代理重加密方法运行的系统流程见图2，结合流程框图，将该方法的具体实现步骤介绍如下：

[0100] 模块一：初始化模块

[0101] 该模块功能的实现具体分为四步：

[0102] 步骤1：PKG首先输入系统安全参数λ，运行算法$g(1^{\lambda})$，输出两个阶数为素数p的群$\mathbb{G}$、$\mathbb{G}_T$和一个双线性映射运算e: $\mathbb{G}\times\mathbb{G}\to\mathbb{G}_T$。

[0103] 步骤2：$g\overset{R}{\leftarrow}\mathbb{G}$，$h\overset{R}{\leftarrow}\mathbb{G}$，$\alpha\overset{R}{\leftarrow}Z_p^*$

[0104] PKG接下来运行随机数生成算法，随机选择$\mathbb{G}$群中的某个生成元g，$\mathbb{G}$群中的一个元素h，以及Z_p^*域中的一个元素α作为随机指数。

[0105] 步骤3：PKG运行一次双线性对运算、两次求幂运算和(m-1)次乘法运算，得到$\mathbb{G}_T$群中的一个元素e(g,h)，和$\mathbb{G}$群中的(m+1)个元素g^{α}、h^{α}，...，h^{α^m}。

[0106] 步骤4：最后，PKG选择一种抗碰撞哈希函数H(•)，该函数满足抗碰撞哈希函数的所有特性，输入可以为任意长度的字符串，输出为映射到域Z_p^*中的某一元素。

[0107] 经过上述四个步骤得到的参数：

[0108] $PK_{IBBE}=(g^{\alpha},e(g,h),h,h^{\alpha},...,h^{\alpha^m},H(\cdot))$

[0109] 作为IBBE加密系统的公钥可以对外公开；IBE加密系统的公钥与上述公钥不同，为：

[0110] $PK_{IBE}=(g^{\alpha},e(g,h),h,h^{\alpha},h^{\alpha^2},H(\cdot))$

[0111] IBE和IBBE加密系统的主密钥相同，为：

[0112] $MSK_{IBE}=MSK_{IBBE}=(g,\alpha)$

[0113] 由PKG保管。

[0114] 其中，在步骤1中所述的“算法g(1^{λ})”，其运行方法如下：私钥生成中心(PKG)输入系统安全参数λ，根据λ的大小，系统选择相应的椭圆曲线：$Y^2=X^3+aX+b$(a和b是系数)，再由椭圆曲线上的点构成两个素数p阶的群$\mathbb{G}$、$\mathbb{G}_T$。选择一种函数映射e，将群$\mathbb{G}$中的元素映射到群$\mathbb{G}_T$中去；安全参数数值越大，所选择椭圆曲线上的点也越多，群也越大。

[0115] 其中，步骤2中所述的“随机数生成算法”，其做法如下：根据步骤1中所选的椭圆曲线：$Y^2=X^3+aX+b$，随机选择自变量X的一个值x_1，计算对应因变量Y的值y_1；若点(x_1,y_1)在我们想要映射的群中，则成功生成了随机元素。若点(x_1,y_1)不在群中，则继续选择X的值，直到找到出现在群中的点。此外，域Z_p^*表示集合{1,2,...,p-1}，随机选择域Z_p^*中元素的随机数生成函数可以从Pairing-Based Cryptosystems函数包中调用库函数运行。下文中提到的随机数生成算法皆按上述方法运行。

[0116] 其中，步骤3中所述的“运行双线性对运算”，其做法如下：自变量的输入为群$\mathbb{G}$中的元素g、h，输出为群$\mathbb{G}_T$中的元素：e(g,h)。

[0117] 其中，步骤4中所述的抗碰撞哈希函数H(•)同样可以从Pairing-Based Cryptosystems函数包中调用库函数运行。

[0118] 模块二：私钥生成模块

[0119] 该模块功能的实现为两步：

[0120] 步骤5：PKG运行抗碰撞哈希函数H(•)，计算得到：

[0121] $$H(ID_{IBE}),H(ID_{IBBE})\in Z_p^*;$$

[0122] 公式中的ID_{IBE}代表IBE加密系统中用户的身份，ID_{IBBE}代表IBBE加密系统中用户的身份，均用一串任意的字符串表示。

[0123] 步骤6：PKG运行一次加法运算，一次求倒数运算和求指数运算，按照下面公式计算得到IBE加密系统中的用户私钥：

[0124] $$SK_{IBE}=g^{\frac{1}{\alpha+H(ID_{IBE})}}$$

[0125] 以及，IBBE加密系统中用户的私钥：

[0126] $$SK_{IBBE}=g^{\frac{1}{\alpha+H(ID_{IBBE})}}$$

[0127] 模块三：数据加密模块

[0128] 该模块功能的实现分三步：

[0129] 步骤7：Delegator运行抗碰撞哈希函数H(•)，计算得到$H(ID_{IBE})\in Z_p^*$。

[0130] 步骤8：Delegator运行随机数生成算法，随机选择域Z_p^*中的一个元素s作为指数，按照下面公式运行两次乘法和三次求幂运算，得到：

[0131] $$C_0=M\cdot e(g,h)^s,C_1=h^{\alpha s}h^{H(ID)s}=h^{s(\alpha+H(ID_{IBE}))}$$

[0132] 最后的密文输出为：$CT_{IBE}=(C_0,C_1)$，该密文是根据Delegator的身份ID_{IBE}加密，故只有Delegator自己的私钥SK_{IBE}可以解密。

[0133] 模块四：转换密钥生成模块

[0134] 该模块功能的实现具体分为三步：

[0135] 步骤9：Delegator首先运行随机数生成算法，随机选择$\mathbb{G}$群中的某个元素$k \in \mathbb{G}$，作为盲化因子。

[0136] 步骤10：针对被授权用户(Delegatee)身份集合S中的每个身份，Delegator运行n次抗碰撞哈希函数H(•)，得到：

[0137] $H(ID_{1IBBE})$，$H(ID_{2IBBE})\cdots H(ID_{nIBBE})$

[0138] 其中n代表用户集合中的身份数量。

[0139] 步骤11：Delegator运行随机数生成算法，随机选择域Z_p^*中的一个元素v作为指数；按照下式运行多项式次求幂运算和乘法运算，得到：

[0140] $C_0' = k \cdot e(g,h)^v$，$C_1' = h^{v(\alpha+H(ID_{1IBBE}))(\alpha+H(ID_{2IBBE}))\cdots(\alpha+H(ID_{nIBBE}))}$

[0141] 我们将得到的结果表示为：

[0142] $R = (C_0', C_1')$

[0143] 经过最后一步乘法运算$SK_{IBE} \cdot k$，授权方便生成了转换密钥：

[0144] $RK_{IBE \to IBBE} = (SK_{IBE} \cdot k, R)$

[0145] 其中，被授权用户(Delegatee)的身份集合S默认为所有集合内的用户均知晓。

[0146] 模块五：代理重加密模块

[0147] 该模块的功能由一步计算实现：

[0148] 步骤12：Proxy按照下式运行一次双线性对和一次除法运算，得到：

[0149]
$$D_0 = \frac{C_0}{e(SK_{IBE} \cdot k, C_1)} = \frac{Me(g,h)^s}{e(g^{\frac{1}{\alpha+H(ID_{IBE})}}, h^{s(\alpha+H(ID_{IBE}))})e(k, h^{s(\alpha+H(ID_{IBE}))})}$$
$$= \frac{M}{e(k, h^{s(\alpha+H(ID_{IBE}))})}$$

[0150] 经过代理重加密后的密文为：

[0151] $CT_{IBE \to IBBE} = (D_0, C_1, R)$

[0152] 模块六：解密模块

[0153] 该模块的功能实现具体分为3步：

[0154] 步骤13：Delegatee首先针对被授权用户的身份集合S中的每个身份，运行一次抗碰撞哈希函数H(•)得到：

[0155] $H(ID_{1IBBE})$，$H(ID_{2IBBE})\cdots H(ID_{nIBBE})$

[0156] 式中的n代表用户集合中的身份数量。

[0157] 步骤14：Delegatee按照下式运行两次双线性对运算和多项式次加法、连乘运算得到：

$$A = (e(g^{-\alpha v}, h^{\frac{1}{\alpha}(\prod_{j=1,j\neq i}^{n}(\alpha+H(ID_{jIBBE}))-\prod_{j=1,j\neq i}^{n}H(ID_{jIBBE}))}) \cdot e(SK_{iIBBE}, C_1'))^{\frac{1}{\prod_{j=1,j\neq i}^{n}H(ID_{jIBBE})}}$$

$$= (e(g,h)^{-v(\prod_{j=1,j\neq i}^{n}(\alpha+H(ID_{jIBBE}))-\prod_{j=1,j\neq i}^{n}H(ID_{jIBBE}))}$$

[0158]

$$\cdot e(g^{\frac{1}{\alpha+H(ID_{iIBBE})}}, g^{\frac{1}{v(\prod_{j=1}^{n}\alpha+H(ID_{jIBBE}))}}))^{\frac{1}{\prod_{j=1,j\neq i}^{n}H(ID_{jIBBE})}}$$

$$= e(g,h)^{v}$$

[0159] 再进行一次除法运算即可得到盲化因子k：

[0160] $$k = \frac{C_0'}{A} A = \frac{ke(g,h)^v}{e(g,h)^v}$$

[0161] 步骤15：最后，Delegatee按照下式经过一次双线性对和乘法运算，得到最后的明文消息M：

$$M = D_0 \cdot e(k, C_1)$$

[0162]

$$= \frac{M}{e(k, h^{s(\alpha+H(ID_{iBE}))})} \cdot e(k, h^{s(\alpha+H(ID_{jBE}))})$$

。

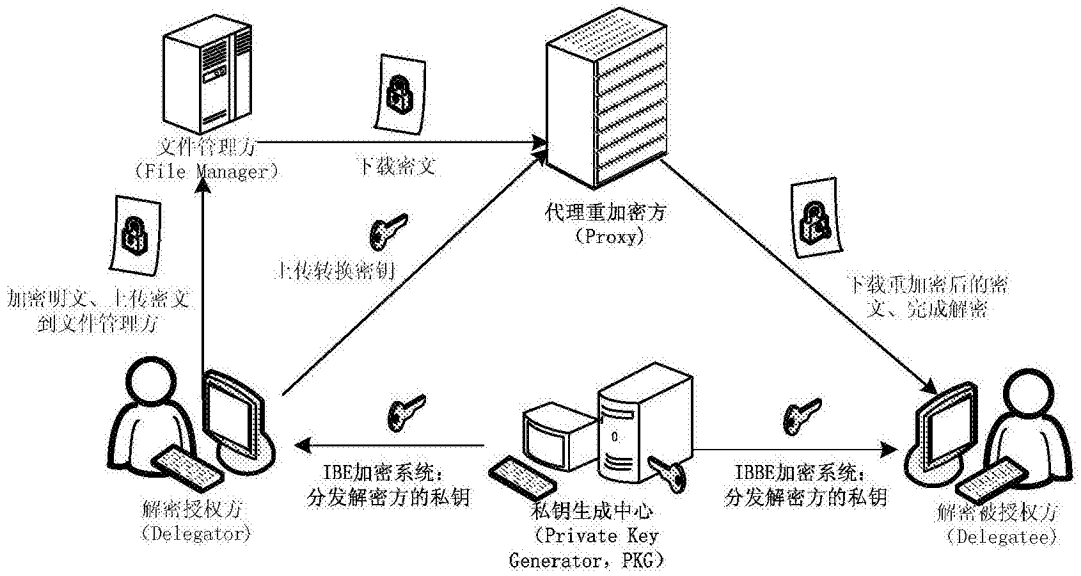

文件管理方
(File Manager)
下载密文
代理重加密方
(Proxy)
上传转换密钥
加密明文、上传密文
到文件管理方
下载重加密后的密
文、完成解密
IBE加密系统：
分发解密方的私钥
IBBE加密系统：
分发解密方的私钥
解密授权方
(Delegator)
私钥生成中心
(Private Key
Generator，PKG)
解密被授权方
(Delegatee)

图1

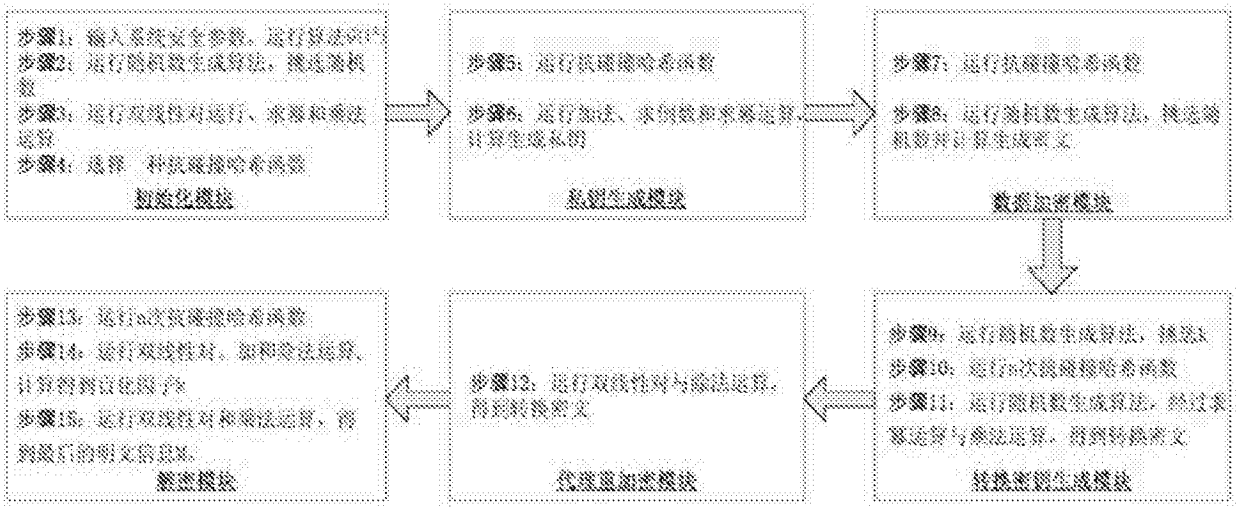


图2