



(12)发明专利申请

(10)申请公布号 CN 106487506 A

(43)申请公布日 2017.03.08

(21)申请号 201610876812.1

(22)申请日 2016.10.08

(71)申请人 西安电子科技大学

地址 710071 陕西省西安市太白南路2号西安电子科技大学

(72)发明人 李学俊 吕茂旭 杨诗雨

(74)专利代理机构 北京科亿知识产权代理事务所(普通合伙) 11350

代理人 汤东风

(51) Int. Cl.

H04L 9/08(2006.01)

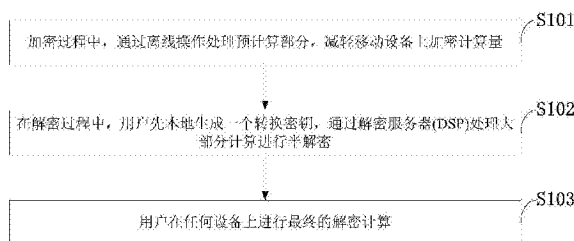
权利要求书3页 说明书7页 附图1页

(54)发明名称

一种支持预加密和外包解密的多机构KP-ABE方法

(57)摘要

本发明公开了一种支持预加密和外包解密的多机构KP-ABE方法,所述支持预加密和外包解密的多机构KP-ABE方法将数据加密、密文解密过程都分为预计算和移动设备计算两部分;在数据加密过程中,通过离线操作处理预计算部分,减轻移动设备上加密计算量;在密文解密过程中,用户先本地生成一个转换密钥,通过解密服务器(DSP)处理大部分计算进行半解密;用户可在任何设备上最终解密计算。本发明实现了多个权威机构共同负责管理用户属性和密钥分发,并有效降低用户端的加密、解密计算开销,使得基于属性加密方案能够适用于低配置的手机等移动设备。



1. 一种支持预加密和外包解密的多机构KP-ABE方法,其特征在于,所述支持预加密和外包解密的多机构KP-ABE方法将数据加密、密文解密过程都分为预计算和移动设备计算两部分;在数据加密过程中,通过离线操作处理预计算部分,减轻移动设备上加密计算量;在密文解密过程中,用户先本地生成一个转换密钥,通过解密服务器处理大部分计算进行半解密;用户在任何设备上进行最终的解密计算。

2. 如权利要求1所述的支持预加密和外包解密的多机构KP-ABE方法,其特征在于,所述数据加密具体包括:

预加密算法:数据拥有者在加密数据时,先在PC端对所有属性密文进行预计算,结合系统参数GP、相关权威机构的公钥 PK_i 以及一个属性集合 $S \subseteq U$,随机选择 $s' \in \mathbb{Z}_p$;进行如下计算:

$$C_j = (g^{u_j})^{s'};$$

$$C_0 = g^{s'};$$

输出中间密文 $IC = (\{C_j\}_{j \in S}, C_1, C_0, s')$,将IC拷贝到移动设备;

线上加密算法:数据拥有者在移动设备对具体数据加密,结合相关属性机构 AA_i 的公钥 PK_i ,一个对称密钥 K_{SE} ;进行以下计算对具体明文数据 m 加密:

$$C_{SE} = \text{SKE.Eec}(K_{SE}, m);$$

$$C = K_{SE} \cdot \left(\prod_{i \in A} e(g, g)^{\alpha_i} \right)^{s'};$$

$$C_2 = s - s';$$

获得密文: $CT = (S, \{C_j\}_{j \in U}, C_1, C_0, C, C_2, C_{SE})$;

数据拥有者计算验证值 $\text{Tag} = H_0(K_{SE})$, $\text{VK}_M = H(\text{Tag} || C_{SE})$;其中, K_{SE} 是一个对称密钥, $C_{SE} = \text{SKE.Eec}(K_{SE}, m)$ 表示用对称加密算法对数据 m 加密得到的密文;然后,将密文CT和验证值 VK_M 上传到云存储服务器CSSP。

3. 如权利要求1所述的支持预加密和外包解密的多机构KP-ABE方法,其特征在于,所述密文解密具体包括:

外包解密算法:用户从云存储服务器CSSP下载密文CT和验证值 VK_M ,并将密文CT、转换密钥 $\text{TK}_{GID, i}$ 发送给DSP, DSP结合系统参数GP计算:

$$C'_j = C_j^{C_2} = (g^{u_j})^s;$$

$$C'_0 = C_0^{C_2} = g^s;$$

然后对于每个 $i \in A$ 选择 $w_x \in \mathbb{Z}_p$ ($x \in S_u$),使得 $\sum_x w_x \cdot \lambda_x = \alpha_i$,并计算:

$$\begin{aligned} E_x &= e(C'_{p(x)}, K_{i,j}) \cdot e(C'_0, K_0) \\ &= e(g^{u_{i,p(x)} \cdot s}, g^{\frac{1}{2\alpha_{i,p(x)}}} \cdot H(\text{GID})^{\frac{\lambda_x}{2\alpha_{i,p(x)}}}) \cdot e(g^s, g^{\frac{-1}{z}}); \\ &= e(g, H(\text{GID}))^{\frac{\lambda_x \cdot s}{z}} \end{aligned}$$

$$\begin{aligned}
 CT' &= \prod_{i \in A} \frac{e(C_0, L)}{\prod_{x \in S_u} E_x^{w_x}} = \prod_{i \in A} \frac{e(g^s, g^z H(GID)^z)^{\frac{\alpha_i}{z}}}{\prod_{x \in S_u} (e(g, H(GID))^{\frac{\lambda_x s}{z}})^{w_x}} \\
 &= \prod_{i \in A} \frac{e(g, g)^{\frac{\alpha_i s}{z}} e(g, H(GID))^{\frac{\alpha_i}{z}}}{e(g, H(GID))^{\frac{s}{z} \sum_{x \in S_u} \lambda_x w_x}} ; \\
 &= \prod_{i \in A} e(g, g)^{\frac{\alpha_i s}{z}}
 \end{aligned}$$

其中, A表示数据拥有者相关权威机构集合, S_u 表示用户属性集, $S_u \subseteq S$;

终端解密算法: 用户结合 DK_s , 首先计算 $K_{SE} = C / (CT')^z$, 然后计算 $Tag = H_0(K_{SE})$, 如果 $H(Tag || C_{SE}) \neq VK_M$, 输出 \perp 并终止算法; 如果 $H(Tag || C_{SE}) = VK_M$, 说明外包计算结果正确, 则计算 $m = SKE.Dec(K_{SE}, C_{SE})$ 进行解密。

4. 一种如权利要求1所述支持预加密和外包解密的多机构KP-ABE方法的多机构KP-ABE系统, 其特征在于, 所述多机构KP-ABE系统包括:

数据拥有者, 在配置较高PC端离线计算预加密部分, 保存计算结果; 在移动设备上调用该结果, 对任意具体明文数据加密, 将密文上传到云存储服务器, 提供给满足策略的用户访问;

可信权威中心, 用于响应用户的注册请求, 负责用户的身份信息管理, 并将已注册的用户身份信息GID发送给各个属性权威机构;

云存储服务器, 用于负责存储数据拥有者的数据密文;

多属性权威机构, 用于负责管理数据拥有者的不同属性集、生成公私钥对、认证用户GID、生成并分发所管理属性的密钥份额;

云解密服务器, 用于接收用户密文和转换密钥, 对密文进行部分解密; 然后将转换密文返给用户, 由访问数据的用户在移动客户端进行最后的解密;

访问数据的用户, 当且仅当他的属性满足访问策略才能解密密文, 每个访问数据的用户有一个互不相同的全局标示符GID。

5. 一种应用权利要求4所述多机构KP-ABE系统的移动设备。

6. 一种应用权利要求4所述多机构KP-ABE系统的移动云终端。

7. 如权利要求6所述移动云终端环境的多机构KP-ABE方法, 其特征在于, 所述多机构KP-ABE方法包括:

首先运行系统初始化算法生成系统参数GP, 各个权威机构结合GP生成权威机构公钥 PK_i 、私钥 SK_i ; 当用户A要通过手机app将数据存储到公共云端的时候, 他先向CA提交注册申请, 生成唯一的身份信息标识GID;

然后将个人的部分属性集 $\{Att_A\}$ 分发给 n ($n \leq N$) 个权威机构, 各个权威机构 AA_i 对所管理属性 $\{Att_i\}$ 生成一个访问策略 (M_i, ρ_i) , 用户A结合相关 PK_i 在PC上对自己所有属性进行预计算, 生成了属性密文, 并将结果存于手机; 在手机端用属性集 $\{Att_A\}$ 对数据加密并计算验证值 VK_M ;

最后将密文CT和验证值 VK_M 上传到云端; 当用户B想要访问A的数据时, 他首先同A一样进

行身份注册;从云端下载A的数据密文CT和验证值VK_M;再发送一个属性集 {Att_{GID}} 以及GID给各权威机构,相关权威机构认证用户信息后,以保留的私钥、用户GID以及 {Att_{GID}} 为输入,生成用户私钥SK_{GID,i};并返给用户B;如果 {Att_{GID}} ∩ {Att_i} ∈ M_i,用户B可利用该私钥SK_{GID,i}正确解密;用户B将SK_{GID,i}进行转换后与密文CT一并发送给代理解密服务器DSP,DSP进行半解密后将结果返给用户B,用户B在手机进行验证,验证正确则进行最终解密。

一种支持预加密和外包解密的多机构KP-ABE方法

技术领域

[0001] 本发明属于数据加密技术领域,尤其涉及一种支持预加密和外包解密的多机构KP-ABE方法。

背景技术

[0002] 随着智能手机的快速发展。越来越多的用户通过手机的云应用将个人数据信息存储在云端,通过移动云进行存储和共享。但是,移动云作为一种开放的分布式环境,不能够保证数据的机密性和安全性,云服务提供商也可能出于好奇或者商业利益而窥探用户数据,甚至泄露用户数据。因此,如何实现数据的安全共享也成为云计算发展面临的一大挑战。传统的公钥密码虽然能够实现数据的安全共享,但它仅支持一对一的加密形式,并且不能实现灵活的访问控制。目前,在云环境下,属性基加密ABE被认为是实现数据安全共享及访问控制的最有前景的技术,因为ABE使得用户可以通过访问策略直接控制数据,并且不需要给其他用户分发密钥,就可以实现数据的安全共享。ABE分为基于密文策略的属性加密(CP-ABE)和基于密钥策略的属性加密(KP-ABE)。属性加密能够实现对数据细粒度访问控制,现实中具有很大的应用价值。基于密钥策略的属性加密KP-ABE是指密钥和访问结构相对应,而密文和一个属性集合相结合,当且仅当密文的属性集合满足密钥的访问结构时才能解密密文。针对于单属性权威机构的方案中,单个属性权威机构必须管理所有用户的属性和复杂的密钥分发工作,工作量巨大,很容易不堪重负,影响系统效率问题。目前,很多研究转向了多属性权威机构机制。但是,多机构系统时面临着各权威机构间或者各用户间的串谋攻击问题。假如相关权威机构都不可信,由于各权威机构都知道用户的身份信息,它们就可以合谋冒充该用户,从而获取解密密钥。另外,如果不对解密密钥进行身份信息绑定,不同用户也可能串谋,冒充其他用户。

[0003] 综上所述,现有属性加密方案由于计算开销大,不适用于低配置移动设备。此外,对于大规模环境下单机构属性加密方案,单个权威机构工作量大,可能不堪重负从而带来性能瓶颈问题。

发明内容

[0004] 本发明的目的在于提供一种支持预加密和外包解密的多机构KP-ABE方法,旨在解决现有属性加密方案计算开销大而不适用于低配置移动设备,以及对于大规模环境下单机构属性加密方案可能带来性能瓶颈问题。

[0005] 本发明是这样实现的,一种支持预加密和外包解密的多机构KP-ABE方法,所述支持预加密和外包解密的多机构KP-ABE方法将数据加密、密文解密过程都分为预计算和移动设备计算两部分;在数据加密过程中,通过离线操作处理预计算部分,减轻移动设备上加密计算量;在密文解密过程中,用户先本地生成一个转换密钥,通过解密服务器(DSP)处理大部分计算进行半解密;用户在任何设备上进行最终的解密计算。

[0006] 进一步,所述数据加密具体包括:

[0007] 预加密算法:数据拥有者在加密数据时,先在PC端对所有属性密文进行预计算,结合系统参数GP、相关权威机构的公钥PK_i以及一个属性集合 $S \subseteq U$,随机选择 $s' \in \mathbb{Z}_p$;进行如下计算:

$$[0008] \quad C_j = (g^{u_{i,j}})^{s'};$$

$$[0009] \quad C_0 = g^{s'};$$

[0010] 输出中间密文IC = ($\{C_j\}_{j \in S}, C_1, C_0, s'$),将IC拷贝到移动设备;

[0011] 线上加密算法:数据拥有者在移动设备对具体数据加密,结合相关属性机构AA_i的公钥PK_i,一个对称密钥K_{SE};进行以下计算对具体明文数据m加密:

$$[0012] \quad C_{SE} = \text{SKE.Eec}(K_{SE}, m);$$

$$[0013] \quad C = K_{SE} \cdot \left(\prod_{i \in A} e(g, g)^{\alpha_i} \right)^s;$$

$$[0014] \quad C_2 = s - s';$$

[0015] 获得密文:CT = ($S, \{C_j\}_{j \in U}, C_1, C_0, C, C_2, C_{SE}$).

[0016] 数据拥有者计算验证值Tag = H₀(K_{SE}), VK_M = H(Tag || C_{SE});其中, K_{SE}是一个对称密钥, C_{SE} = SKE.Eec(K_{SE}, m)表示用对称加密算法对数据m加密得到的密文;并将密文CT和验证值VK_M上传到云存储服务器CSSP。

[0017] 进一步,所述密文解密具体包括:

[0018] 外包解密算法:用户从云存储服务器CSSP下载密文CT和验证值VK_M,并将密文CT、转换密钥TK_{GID,i}发送给DSP,DSP结合系统参数GP计算:

$$[0019] \quad C_j^i = C_j^{C_2} = (g^{u_{i,j}})^s;$$

$$[0020] \quad C_0^i = C_0^{C_2} = g^s;$$

[0021] 然后对于每个 $i \in A$ 选择 $w_x \in \mathbb{Z}_p$ ($x \in S_u$),使得 $\sum_x w_x \cdot \lambda_x = \alpha_i$,并计算:

$$[0022] \quad \begin{aligned} E_x &= e(C_{\rho_i(x)}^i, K_{i,j}) \cdot e(C_0^i, K_0) \\ &= e(g^{u_{i,\rho_i(x)} \cdot s}, g^{\frac{1}{z^{u_{i,\rho_i(x)}}} \cdot H(GID)^{\frac{\lambda_x}{z^{u_{i,\rho_i(x)}}}}}) \cdot e(g^s, g^{\frac{-1}{z}}); \\ &= e(g, H(GID))^{\frac{\lambda_x \cdot s}{z}} \end{aligned}$$

$$[0023] \quad \begin{aligned} CT^i &= \prod_{i \in A} \frac{e(C_0^i, L)}{\prod_{x \in S_u} E_x^{w_x}} = \prod_{i \in A} \frac{e(g^s, g^{\frac{\alpha_i}{z} \cdot H(GID)^{\frac{\alpha_i}{z}}})}{\prod_{x \in S_u} (e(g, H(GID))^{\frac{\lambda_x \cdot s}{z}})^{w_x}} \\ &= \prod_{i \in A} \frac{e(g, g)^{\frac{\alpha_i \cdot s}{z}} \cdot e(g, H(GID))^{\frac{\alpha_i \cdot s}{z}}}{e(g, H(GID))^{\sum_{x \in S_u} \lambda_x \cdot w_x}}; \\ &= \prod_{i \in A} e(g, g)^{\frac{\alpha_i \cdot s}{z}} \end{aligned}$$

[0024] 其中,A表示数据拥有者相关权威机构集合, S_u表示用户属性集, S_u ⊆ S;

[0025] 终端解密算法:用户结合 DK_s ,首先计算 $K_{SE}=C/(CT')^z$,然后计算 $Tag=H_0(K_{SE})$,如果 $H(Tag||C_{SE})\neq VK_M$,输出 \perp 并终止算法;如果 $H(Tag||C_{SE})=VK_M$,说明外包计算结果正确,则计算 $m=SKE.Dec(K_{SE},C_{SE})$ 进行解密。

[0026] 本发明的另一目的在于提供一种所述支持预加密和外包解密的多机构KP-ABE方法的多机构KP-ABE系统,所述多机构KP-ABE系统包括:

[0027] 数据所有者,在配置较高PC端离线计算预加密部分,保存计算结果;在移动设备上调用该结果,对任意具体明文数据加密,将密文上传到云存储服务器,提供给满足策略的用户访问;

[0028] 可信权威中心,用于响应用户的注册请求,负责用户的身份信息管理,并将已注册的用户身份信息GID发送给各个属性权威机构;

[0029] 云存储服务器,用于负责存储数据拥有者的数据密文;

[0030] 多属性权威机构,用于负责管理数据拥有者的不同属性集、生成公私钥、认证用户GID、生成并分发所管理属性的密钥份额;

[0031] 云解密服务器,用于接收用户密文和转换密钥,对密文进行部分解密;然后转换密文返给用户,由访问数据的用户在移动客户端进行最后的解密;

[0032] 访问数据的用户,当且仅当他的属性满足访问策略才能解密密文,每个访问数据的用户有一个互不相同的全局标示符GID。

[0033] 本发明的另一目的在于提供一种应用所述多机构KP-ABE系统的移动设备。

[0034] 本发明的另一目的在于提供一种应用所述多机构KP-ABE系统的移动云终端。

[0035] 进一步,所述多机构KP-ABE方法包括:

[0036] 首先运行系统初始化算法生成系统参数GP,各个权威机构结合GP生成权威机构公钥 PK_i 、私钥 SK_i ;当用户A要通过手机app将数据存储到公共云端的时候,他先向CA提交注册申请,生成唯一的身份信息标识GID;

[0037] 然后将个人的部分属性集 $\{Att_A\}$ 分发给 $n(n\leq N)$ 个权威机构,各个权威机构 AA_i 对所管理属性 $\{Att_i\}$ 生成一个访问策略 (M_i,ρ_i) ,用户A结合相关 PK_i 在PC上对自己所有属性进行预计算,生成了属性密文,并将结果存于手机;在手机端用属性集 $\{Att_A\}$ 对数据加密并计算验证值 VK_M ;

[0038] 最后将密文CT和验证值 VK_M 上传到云端;当用户B想要访问A的数据时,他首先同A一样进行身份注册;从云端下载A的数据密文CT和验证值 VK_M ;再发送一个属性集 $\{Att_{GID}\}$ 以及GID给各权威机构,相关权威机构认证用户信息后,以保留的私钥、用户GID以及 $\{Att_{GID}\}$ 为输入,生成用户私钥 $SK_{GID,i}$;并返给用户B;如果 $\{Att_{GID}\}\cap\{Att_i\}\in M_i$,用户B可利用该私钥 $SK_{GID,i}$ 正确解密;户B将 $SK_{GID,i}$ 进行转换后与密文CT一并发送给代理解密服务器DSP,DSP进行半解密后将结果返给用户B,用户B在手机进行验证,验证正确则进行最终解密。

[0039] 本发明提供的支持预加密和外包解密的多机构KP-ABE方法,结合用户全局身份信息GID可防止多机构系统是面临着各权威机构间或者各用户间的串谋攻击问题。此外,由于属性加密方案的计算开销很大,具有较高的配置要求,直接将其应用于低配置的移动设备并不现实。本发明考虑将加密、解密过程都分为预计算和移动设备计算两部分;在加密过程中,通过离线操作处理预计算部分,减轻移动设备上加密计算量;在解密过程中,用户先生成一个转换密钥,通过解密服务器(DSP)处理大部分计算,然后用户在任何设备上都可以轻

松解密密文。有效地降低了用户端的加密、解密计算开销；实现多个权威机构共同负责管理用户属性和密钥分发，并有效降低用户端的加密、解密计算开销，使得基于属性加密方案能够适用于低配置的手机等移动设备。

[0040] 与现有技术相比，本发明具有以下优点：

[0041] 1. 本发明中的多机构KP-ABE方法是多个属性权威机构共同负责用户属性管理和密钥分发工作，减少了每个权威机构的工作量。此外，系统中权威中心只需负责运行系统初始化算法以及管理用户的身份信息，各个权威机构也无需合作，用户只要满足相关的权威机构的访问控制策略，就可以申请正确密钥，最后成功解密密文。

[0042] 2. 本发明中的多机构KP-ABE方法是首个实现加密、解密计算安全外包的多机构密钥策略属性基加密方法。通过在加密过程增加预加密操作，在解密过程由代理解密服务器DSP进行半解密，成功降低了用户端的加密、解密计算开销，使得基于属性加密方案适用于低配置的移动设备成为可能。

[0043] 3. 本发明中的多机构KP-ABE方法在通过代理解密服务器DSP外包半解密后，在用户端可以通过计算验证值，验证外包计算结果的正确性。

[0044] 4. 本发明中的多机构KP-ABE方法能够有效解决多机构方案存在的用户串谋攻击问题，以及权威机构串谋攻击问题，并且方案在基于DBDH假设下是CPA安全的。

附图说明

[0045] 图1是本发明实施例提供的支持预加密和外包解密的多机构KP-ABE方法流程图。

[0046] 图2是本发明实施例提供的模型示意图。

具体实施方式

[0047] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0048] 下面结合附图对本发明的应用原理作详细的描述。

[0049] 如图1所示，本发明实施例提供的支持预加密和外包解密的多机构KP-ABE方法包括以下步骤：

[0050] S101：加密过程中，通过离线操作处理预计算部分，减轻移动设备上加密计算量；

[0051] S102：在解密过程中，用户先本地生成一个转换密钥，通过解密服务器（DSP）处理大部分计算进行半解密；

[0052] S103：用户在任何设备上进行最终的解密计算。

[0053] 下面结合附图对本发明的应用原理作进一步的描述。

[0054] 用户从权威机构获得的密钥份额都绑定其身份信息GID，所以不同用户的密钥不能结合，防止了用户的串谋攻击。具体而言，在加密过程中，通过因子 $\prod_{i \in A} (e(g, g)^{\alpha_i})^s$ 隐藏明文消息，然后依据LSSS矩阵的性质，将 α_i 通过 $\lambda_{i,x}$ 进行分割共享。解密者必须通过属性、身份对 (S_i, GID) 来恢复因子 $\prod_{i \in A} (e(g, g)^{\alpha_i})^s$ 。如果是不同身份信息的用户，将无法计算得到 $e(g, H(GID))^{\lambda_i s/2}$ ，也就无法恢复因子 $\prod_{i \in A} (e(g, g)^{\alpha_i})^s$ ，因此可实现抵抗用户串谋攻击。对于

权威机构,假定数据拥有者的密文与n个权威机构相关,则该方案可以抵抗n-1个权威机构的串谋攻击。令m表示串谋的权威机构数目,如果m=n,它们都知道用户的GID,就可以合谋冒充该用户。如果m≤n-1,也就是说,至少有一个密钥份额是不能得到的,也就不能合谋解密。

[0055] 本发明实施例提供的支持预加密和外包解密的多机构KP-ABE方法的具体步骤如下:

[0056] 步骤1.初始化

[0057] 系统初始化:令X表示N个属性权威机构的集合,A(A∈X)表示每个数据拥有者实际相关的属性权威机构的集合。U表示一个总共有M个属性的全局属性集合,这M个属性被划分成n(n≤N)个互不相交的集合。定义两个阶都为素数p的乘法循环群G、G_T,g是G的一个生成元,再定义一个双线性映射e:G×G→G_T,以及抗碰撞Hash函数,H₀:M→{0,1}^{ℓ_{H0}}和H:{0,1}^{*}→G。则系统全局参数GP为:

[0058] GP = {p, g, G, G_T, e, e(g, g), H₀, H};

[0059] 属性权威机构初始化算法:每个属性权威机构AA_i(i∈X)首先随机选取元素α_i∈Z_p,并对其所管理的各属性Att_j(j∈U)随机选取u_{i,j}∈Z_p。输入GP,输出公钥PK_i和私钥SK_i分别为:

[0060] PK_i = (e(g, g)^{α_i}, {g^{u_{i,j}} }_{j∈U});

[0061] SK_i = (α_i, {u_{i,j} }_{j∈U});

[0062] 步骤2.用户注册

[0063] 用户向用户身份信息库申请身份注册,获得与用户身份信息库唯一对应的用户身份信息GID。用户将身份信息GID提交给各个权威机构。授权机构判断获取的用户身份信息GID与用户身份信息库是否匹配,若是,则执行步骤3,否则,拒绝服务。

[0064] 步骤3.密钥分发

[0065] 密钥生成算法:用户需给每个相关权威机构AA_i发送自己的GID以获得相应属性Att_j的密钥组件。权威机构AA_i认证用户身份后,运行该算法。输入用户GID、保留的SK_i、一个LSSS访问结构(M_i, ρ_i),M_i是一个1×n的矩阵,函数ρ_i是矩阵M_i的每行和属性的一个映射。AA_i首先随机选取列向量 $\vec{v}_i = (\alpha_i, y_2, \dots, y_n) \in \mathbb{Z}_p$,然后计算 $\lambda_{i,x} = M_{i,x} \cdot \vec{v}_i$,其中M_{i,x}表示矩阵M_x的第x行,x∈[1,1]。输出以下形式的密钥组件SK_{GID,i}。

[0066] SK_{GID,i} = ({K_{i,j} = g ^{$\frac{1}{H(GID) \cdot \lambda_{i,\rho_i(x)}}$} · H(GID) ^{$\frac{\lambda_{i,x}}{H(GID)}$} }_{1≤x≤l}, L = g^{α_i} H(GID)^{α_i});

[0067] 密钥转换算法:用户随机选择z∈Z_p,令DK_s=z,计算转换密钥TK_{GID,i}=(SK_{GID,i})^{1/z}和K₀=g^{-1/z},转换密钥TK_{GID,i}的形式如下:

[0068] TK_{GID,i} = ({K_{i,j} = g ^{$\frac{1}{z \cdot H(GID) \cdot \lambda_{i,\rho_i(x)}}$} · H(GID) ^{$\frac{\lambda_{i,x}}{z \cdot H(GID)}$} }_{1≤x≤l}, L = g ^{$\frac{\alpha_i}{z}$} H(GID) ^{$\frac{\alpha_i}{z}$} , K₀ = g ^{$\frac{-1}{z}$});

[0069] 用户将TK_{GID,i}发送给解密服务器(DSP),并保留DK_s。

[0070] 步骤4.数据加密

[0071] 预加密算法:数据拥有者在加密数据时,先在PC端对所有属性密文进行预计算,结

合系统参数GP、相关权威机构的公钥PK_i以及一个属性集合 $S \subseteq U$ ，随机选择 $s' \in \mathbb{Z}_p$ 。然后，进行如下计算：

$$[0072] \quad C_j = (g^{u_j})^{s'};$$

$$[0073] \quad C_0 = g^{s'};$$

[0074] 输出中间密文IC = ($\{C_j\}_{j \in S}, C_1, C_0, s'$)，将IC拷贝到移动设备。

[0075] 线上加密算法：数据拥有者在移动设备上对具体数据加密，结合相关AA_i的公钥PK_i，一个对称密钥K_{SE}。然后进行以下计算对具体明文数据m实现加密：

$$[0076] \quad C_{SE} = \text{SKE.Eec}(K_{SE}, m);$$

$$[0077] \quad C = K_{SE} \cdot \left(\prod_{i \in A} e(g, g)^{\alpha_i} \right)^s;$$

$$[0078] \quad C_2 = s - s';$$

[0079] 获得密文：CT = ($S, \{C_j\}_{j \in S}, C_1, C_0, C, C_2, C_{SE}$)。

[0080] 数据拥有者计算验证值Tag = H₀(K_{SE})，VK_M = H(Tag || C_{SE})。其中，K_{SE}是一个对称密钥，C_{SE} = SKE.Eec(K_{SE}, m)表示用对称加密算法对数据m加密得到的密文。并将密文CT和验证值VK_M上传到云存储服务器CSSP。

[0081] 步骤5. 密文解密

[0082] 外包解密算法：用户从云存储服务器CSSP下载密文CT和验证值VK_M，并将密文CT、转换密钥TK_{GID, i}发送给DSP，DSP结合系统参数GP计算：

$$[0083] \quad C'_j = C_j \cdot C_2 = (g^{u_j})^s;$$

$$[0084] \quad C'_0 = C_0 \cdot C_2 = g^s;$$

[0085] 然后对于每个 $i \in A$ 选择 $w_x \in \mathbb{Z}_p$ ($x \in S_u$)，使得 $\sum_x w_x \cdot \lambda_x = \alpha_i$ ，并计算：

$$[0086] \quad \begin{aligned} E_x &= e(C'_{\rho_i(x)}, K_{i,j}) \cdot e(C'_0, K_0) \\ &= e(g^{u_i \cdot \rho_i(x) \cdot s}, g^{\frac{1}{z \cdot u_i \cdot \rho_i(x)}} \cdot H(GID)^{\frac{\lambda_x}{z \cdot u_i \cdot \rho_i(x)}}) \cdot e(g^s, g^{\frac{-1}{z}}); \\ &= e(g, H(GID))^{\frac{\lambda_x \cdot s}{z}} \end{aligned}$$

$$[0087] \quad \begin{aligned} CT^i &= \prod_{i \in A} \frac{e(C'_0, L)}{\prod_{x \in S_u} E_x^{w_x}} = \prod_{i \in A} \frac{e(g^s, g^{\frac{\alpha_i}{z}} H(GID)^{\frac{\alpha_i}{z}})}{\prod_{x \in S_u} (e(g, H(GID))^{\frac{\lambda_x \cdot s}{z}})^{w_x}} \\ &= \prod_{i \in A} \frac{e(g, g)^{\frac{\alpha_i \cdot s}{z}} \cdot e(g, H(GID))^{\frac{\alpha_i \cdot s}{z}}}{e(g, H(GID))^{\frac{s}{z} \sum_{x \in S_u} \lambda_x \cdot w_x}}; \\ &= \prod_{i \in A} e(g, g)^{\frac{\alpha_i \cdot s}{z}} \end{aligned}$$

[0088] 其中，A表示数据拥有者相关权威机构集合，S_u表示用户属性集，S_u ⊆ S。

[0089] 终端解密算法：用户结合DK_s，首先计算K_{SE} = C / (CT')^z，然后计算Tag = H₀(K_{SE})，如

果 $H(\text{Tag} || C_{SE}) \neq VK_M$, 输出 \perp 并终止算法。如果 $H(\text{Tag} || C_{SE}) = VK_M$, 说明外包计算结果正确, 则计算 $m = \text{SKE}.\text{Dec}(K_{SE}, C_{SE})$ 进行解密;

[0090] 参照图2中本发明的系统模型:

[0091] 系统主要包括六个部分: 数据所有者DO (Data Owner)、权威中心CA (Central Authority)、云储存服务器CSSP (Cloud Storage Server Provider)、多个属性权威机构MA (Muti-Authority)、解密服务器DSP (Decryption Server Provider) 以及数据用户DU (Data User)。

[0092] DO: 表示数据所有者, DO首先在配置较高PC端离线计算预加密部分, 保存计算结果。然后在移动设备上调用该结果, 对任意具体明文数据加密, 将密文上传到CSSP, 提供给满足策略的用户访问。

[0093] CA: 表示可信权威中心, 响应用户的注册请求, 负责用户的身份信息管理, 并将已注册的用户身份信息GID发送给各个属性权威机构。

[0094] CSSP: 表示一个云存储服务器, 负责存储DO的数据密文。系统中CSSP是不可信的, 并且可能试图窥探用户数据。

[0095] MA: 表示多属性权威机构, 各个权威机构负责管理数据拥有者的不同属性集、生成公私钥对、认证用户GID、生成并分发所管理属性的密钥份额。

[0096] DSP: 是一个云解密服务器, 接收用户密文和转换密钥, 对密文进行部分解密。然后转换密文返给用户, 由DU在移动客户端进行最后的解密。

[0097] DU: 是要访问数据的用户, 当且仅当他的属性满足访问策略才能解密密文, 每个DU有一个互不相同的全局标示符GID。

[0098] 本发明的系统模型中的DO、DU主要指持手机等移动设备的用户, DO可以在任何时间、任何地点通过手机等设备将数据上传云端进行共享, 满足DO密钥访问策略的用户, 可直接通过手机等设备来访问DO的数据信息。

[0099] 下面结合系统模型, 对本发明所述方案应用于移动云环境的情形进行说明。

[0100] 依照本发明的步骤, 首先运行系统初始化算法生成系统参数GP, 各个权威机构结合GP生成权威机构公钥 PK_i 、私钥 SK_i 。当用户A要通过手机app将数据存储到公共云端的时候, 他先向CA提交注册申请, 生成唯一的身份信息标识GID。然后将个人的部分属性集 $\{Att_A\}$ 分发给 n ($n \leq N$) 个权威机构, 各个权威机构 AA_i 对所管理属性 $\{Att_i\}$ 生成一个访问策略 (M_i, ρ_i) , 用户A结合相关 PK_i 在PC上对自己所有属性进行预计算, 生成了属性密文, 并将结果存于手机。然后在手机端用属性集 $\{Att_A\}$ 对数据加密并计算验证值 VK_M , 最后将密文CT和验证值 VK_M 上传到云端。当用户B想要访问A的数据时, 他首先同A一样进行身份注册, 然后从云端下载A的数据密文CT和验证值 VK_M , 再发送一个属性集 $\{Att_{GID}\}$ 以及GID给各权威机构, 相关权威机构认证用户信息后, 以保留的私钥、用户GID以及 $\{Att_{GID}\}$ 为输入, 生成用户私钥 $SK_{GID,i}$ 并返给用户B。这里, 如果 $\{Att_{GID}\} \cap \{Att_i\} \in M_i$, 用户B可利用该私钥 $SK_{GID,i}$ 正确解密。用户B将 $SK_{GID,i}$ 进行转换后与密文CT一并发送给代理解密服务器DSP, DSP进行半解密后将结果返给用户B, 用户B在手机进行验证, 验证正确则进行最终解密。

[0101] 以上所述仅为本发明的较佳实施例而已, 并不用以限制本发明, 凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等, 均应包含在本发明的保护范围之内。

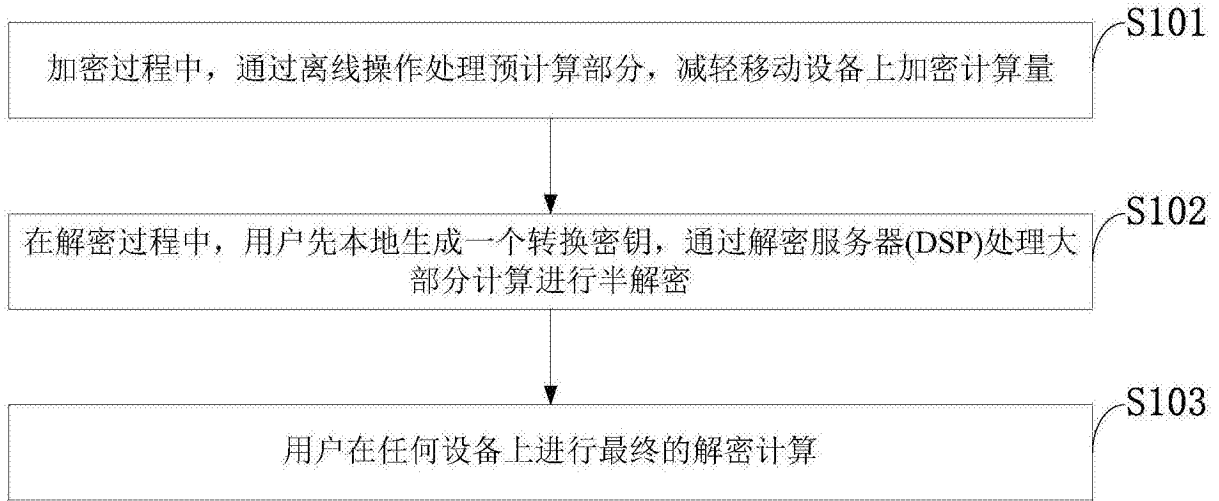


图1

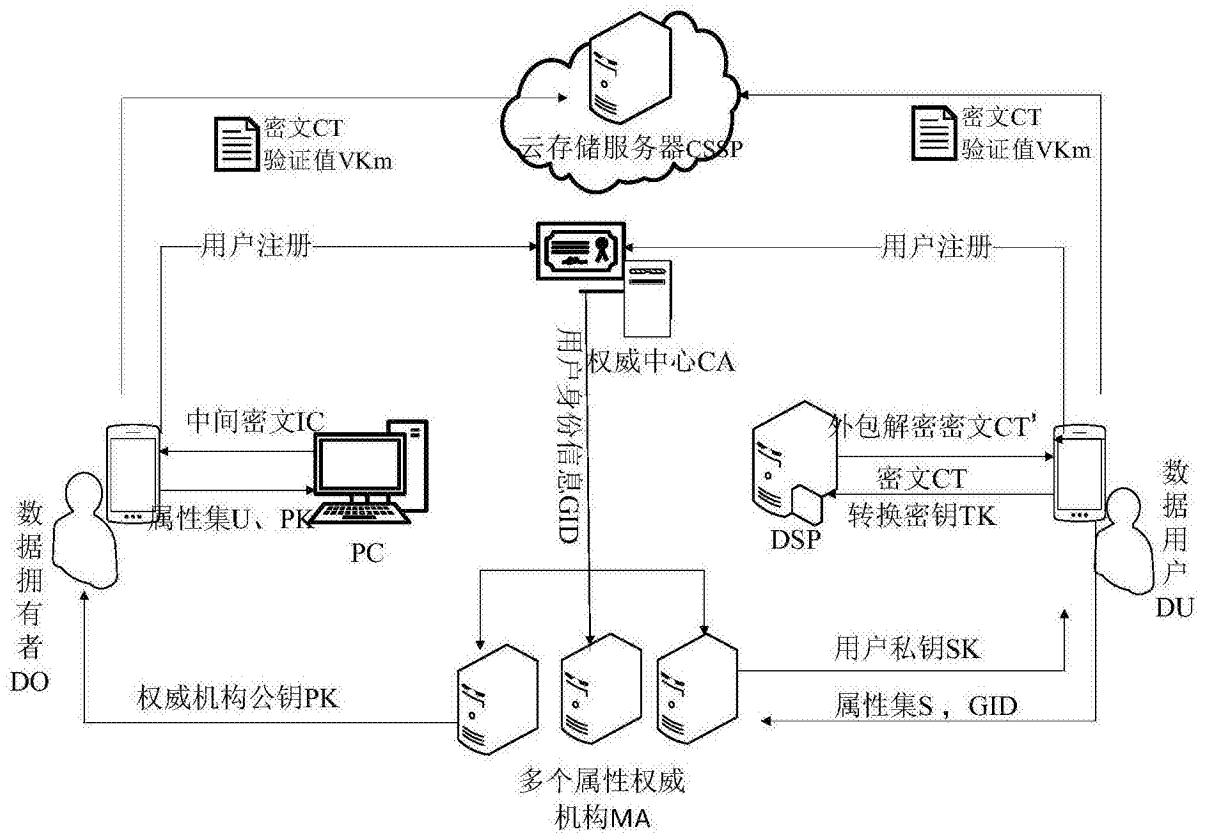


图2