

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2020 年 7 月 16 日 (16.07.2020)



(10) 国际公布号
WO 2020/143131 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2019/083765

(22) 国际申请日: 2019 年 4 月 23 日 (23.04.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910010904.5 2019 年 1 月 7 日 (07.01.2019) CN

(71) 申请人: 南京航空航天大学 (NANJING UNIVERSITY OF AERONAUTICS AND ASTRONAUTICS) [CN/CN]; 中国江苏省南京市秦淮区御道街 29 号, Jiangsu 210016 (CN)。

(72) 发明人: 刘哲 (LIU, Zhe); 中国江苏省南京市秦淮区御道街 29 号, Jiangsu 210016 (CN)。 葛春鹏 (GE, Chunpeng); 中国江苏省南京市秦淮区御道街 29 号, Jiangsu 210016 (CN)。

(74) 代理人: 南京经纬专利商标代理有限公司 (NANJING JINGWEI PATENT & TRADEMARK AGENCY CO., LTD); 中国江苏省南京市鼓楼区中山路 179 号 12 楼 B 座, Jiangsu 210005 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX,

(54) Title: REVOCABLE CLOUD DATA SECURITY SHARING METHOD

(54) 发明名称: 一种可撤销的云数据安全共享方法

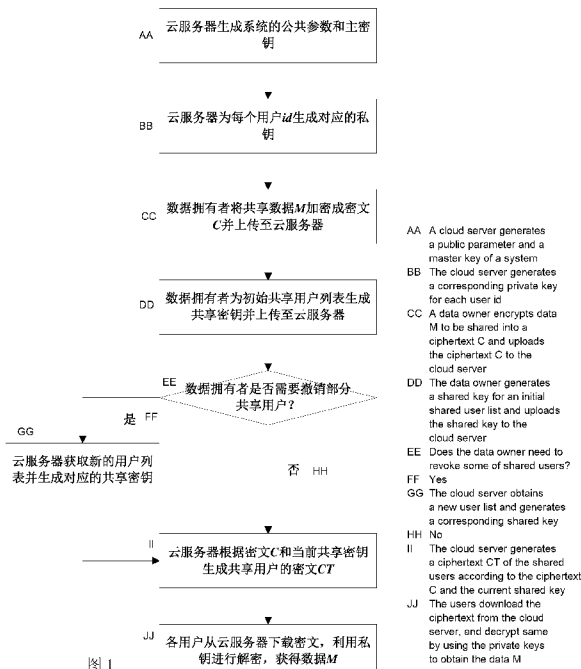


图 1

(57) Abstract: Disclosed in the present invention is a revocable cloud data security sharing method, comprising the steps: a cloud server generates a public parameter and a master key of a system; the cloud server generates a corresponding private key for each user id; a data owner encrypts data M required to be shared into a ciphertext C and uploads the ciphertext C to the cloud server; the data owner generates a shared key for an initial shared user list S and uploads the shared key to the cloud server; the cloud server receives a shared user list R to be revoked from the data owner to obtain a new shared user list S'=S-R, and generates a new shared key corresponding to

MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL,
PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,
SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国(除另有指明, 要求每一种可提供的地区
保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ,
NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM,
AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG,
CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU,
IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT,
RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI,
CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

the shared user list S' ; the cloud server generates a ciphertext CT of shared users according to the ciphertext C and the current shared key; the users download the ciphertext from the cloud server, and decrypt same by using the private keys to obtain the data M. By means of the present invention, the data owner can safely share the data stored in the cloud with other users while being capable of effectively revoking some of the shared users according to own requirements.

(57) 摘要: 本发明公开了一种可撤销的云数据安全共享方法, 步骤: 云服务器生成系统的公共参数和主密钥; 云服务器为每个用户id生成对应的私钥; 数据拥有者将需要共享的数据M加密成密文C, 并上传至云服务器; 数据拥有者为初始的共享用户列表S生成共享密钥, 并上传至云服务器; 云服务器从数据拥有者处接收需要撤销的共享用户列表R, 得到新的共享用户列表 $S' = S - R$, 并生成共享用户列表S'对应的新的共享密钥; 云服务器根据密文C和当前的共享密钥生成共享用户的密文CT; 各用户从云服务器下载密文, 利用私钥进行解密, 获得数据M。通过本发明, 数据拥有者可以将自己存储在云端的数据与其他用户安全共享, 同时可以根据自己的要求高效地撤销部分共享用户。

一种可撤销的云数据安全共享方法

技术领域

本发明属于信息共享和信息安全领域，特别涉及了一种可撤销的云数据安全共享方法。

背景技术

随着云技术的发展，越来越多的用户、企业、科研院所将自己的信息保存至云端。云计算给用户便利的数据服务时也带来用户数据安全问题。为了保护用户数据的安全，用户的数据通常在本地加密后再存储在云端。当用户的数据被加密存储在云端后，用户往往需要对数据进行某些操作，而数据共享是最常见的一种操作。然而由于加密使得用户的数据失去了原有的结构，导致了云服务器对数据的共享操作也随之失效。现有的云数据安全共享方法主要基于代理重加密来实现。现有的基于代理重加密的实现方法都无法实现对共享用户的安全、高效撤销。现有的实现方法都是将共享密钥设置在某一个时间段内有效，当每一个新的时间段来临时，无论是否有用户被从共享列表中撤销掉，数据拥有者都需要为共享列表中的用户重新生成一个新的共享密钥。这些方法存在两个问题：（1）数据拥有者在每个新的时间段都需要生成一个新的共享密钥，而新的共享密钥的计算量往往比较大；（2）数据拥有者每次生成新的共享密钥后都需要一个安全信道来将这个共享密钥发送给云服务器，建立安全信道的代价往往比较大。

发明内容

为了解决上述背景技术提出的技术问题，本发明提供一种可撤销的云数据安全共享方法。

为了实现上述技术目的，本发明的技术方案为：

一种可撤销的云数据安全共享方法，包括以下步骤：

- (1) 云服务器生成系统的公共参数和系统的主密钥；
- (2) 云服务器为每个用户 id 生成对应的私钥；
- (3) 数据拥有者将需要共享的数据 M 加密成密文 C ，并上传至云服务器；
- (4) 数据拥有者为初始的共享用户列表 S 生成共享密钥，并上传至云服务器；
- (5) 数据拥有者是否需要撤销部分共享用户，若是，进入步骤 (6)，若否进入步骤 (7)；
- (6) 云服务器从数据拥有者处接收需要撤销的共享用户列表 R ，得到新的共享用户列表 $S'=S-R$ ，并生成共享用户列表 S' 对应的新的共享密钥；
- (7) 云服务器根据密文 C 和当前的共享密钥生成共享用户的密文 CT ；
- (8) 各用户从云服务器下载密文，利用私钥进行解密，获得数据 M 。

进一步地，在步骤 (1) 中，云服务器首先选取一个标准椭圆曲线，并根据该椭圆曲线构造循环群 G 以及群 G 上的双线性运算 $e: G \times G \rightarrow G_T$ ，其中 G_T 是由双线性运算 e 的结果构成的群，群 G 的生成元为 g ，阶数为素数 p ；云服务器随机选取群 G 上的元素 $\mu, Q \in G$ 和整数 $\alpha \in Z_p$ ，其中 Z_p 表示整数集合 $\{0, 1, \dots, p-1\}$ ，计算 $g_1 = g^\alpha, g_2 = g^{\alpha^2}, \dots, g_N = g^{\alpha^N}$ ， $\mu_1 = \mu^\alpha, \mu_2 = \mu^{\alpha^2}, \dots, \mu_N = \mu^{\alpha^N}$ ， $v = e(g, \mu)$ ，其中 N 为系统支持的最大用户数量；云服务器生成两个抗碰撞哈希函数： $H_1: \{0, 1\}^* \rightarrow Z_p$ ， $H_2: G_T \rightarrow G$ ，其中 $\{0, 1\}^*$ 表示任意长度的 0,1 字符串；云服务器生成系统的公共参数 $mpk = (G, G_T, e, p, g, g_1, \dots, g_N, \mu_1, \dots, \mu_N, v, Q, H_1, H_2)$ 以及系统的主密钥 $msk = (\alpha, \mu)$ ；

进一步地，在步骤 (2) 中，每个用户 id 生成对应的私钥 $sk_{id} = \mu^{1/(\alpha + H_1(id))}$ 。

进一步地, 在步骤(3)中, 数据所有者将数据 M 加密成密文 $C = (C_M, C_0, C_1)$, 其中 $C_M = M \cdot v^r$, $C_0 = g^{r(\alpha + (H_1(id)))}$, $C_1 = Q^r$, $r \in Z_p$ 是随机选取的整数。

进一步地, 在步骤(4)中, 数据所有者为初始的共享用户列表 S 生成共享密钥 rk :

$$rk = (rk_1, rk_2, rk_3, rk_4, rk_5, (rk_{6,i})_{i \in \{1, 2, \dots, k+1\}})$$

其中, $rk_1 = sk_{id} \cdot Q^t$, $rk_2 = g^{\alpha t}$, $rk_3 = g^{tH_1(id)} \cdot H_2(\sigma)$,

$$rk_4 = e(g, \mu)^s \cdot \sigma, \quad rk_5 = g^{s \cdot \prod_{id \in S} (\alpha + H_1(id))}, \quad rk_{6,i} = \mu_i^s, i \in \{1, 2, \dots, k+1\};$$

$t, s \in Z_p, \sigma \in G_T$, k 为系统支持的最大撤销用户数。

进一步地, 在步骤(6)中, 云服务器生成共享用户列表 S' 对应的新的共享密钥 rk' :

$$rk' = (rk_1, rk_2, rk_3, rk_{4'}, rk_{5'}, rk_{6'})$$

其中, $rk_{4'} = rk_4 \cdot e(g, \prod_{i=1}^l rk_{6,i}^{f_i})$, $rk_{5'} = rk_5^{\frac{1}{\prod_{id' \in R} H_1(id')}}^l$, $rk_{6'} = \prod_{i=1}^{l+1} rk_{6,i}^{f_{i-1}}$;

f_i 是多项式 $F(x)$ 的项 x^i 的系数,

$$F(x) = \frac{1}{\prod_{id' \in R} H_1(id')} \prod_{id' \in R} (x + H_1(id')) \square f_l x^l + f_{l-1} x^{l-1} + \dots + f_1 x + f_0.$$

进一步地, 在步骤(7)中, 生成的共享密文 $CT = (C_{M'}, C_{1'}, C_{2'}, C_{3'}, C_{4'}, C_{5'})$; 若当前共享密钥为原共享密钥 rk , 则 $C_{M'} = C_M \cdot e(rk_1, C_0)^{-1} \cdot (rk_2, C_1)$, $C_{1'} = C_1$, $C_{2'} = rk_3$, $C_{3'} = rk_4$, $C_{4'} = rk_5$, $C_{5'} = rk_{6,1}$; 若当前共享密钥为新的共享密钥 rk' , 则 $C_{M'} = C_M \cdot e(rk_1, C_0)^{-1} \cdot (rk_2, C_1)$, $C_{1'} = C_1$, $C_{2'} = rk_3$, $C_{3'} = rk_{4'}$, $C_{4'} = rk_{5'}$, $C_{5'} = rk_{6'}$ 。

进一步地, 在步骤(8)中, 若用户为数据所有者, 从云服务器下载密文 C , 解密得到数据 $M = C_M \cdot e(sk_{id}, C_0)^{-1}$; 若用户不是数据所有者, 从云服务器下载共享密文 CT , 首先计算 $T = \left(e(C_{5'}^{-1}, g^{\rho_{i,S}(\alpha)}) \cdot e(sk_{id}, C_{4'}) \right)^{\prod_{j=1, j \neq i}^S H_1(id_j)}$, 其中 i 表示实施解

密的用户， j 表示 S 中用户 i 以外的用户， id_j 表示用户 j 的 id ，

$$\rho_{i,S}(\alpha) = \frac{1}{\alpha} \cdot \left(\prod_{j=1, j \neq i}^S (\alpha + H_1(id_j)) - \prod_{j=1, j \neq i}^S H_1(id_j) \right) ; \quad \text{再 计 算}$$

$\sigma = C_3 \cdot T^{-1}$, $g^{tH_1(id)} = C_2 \cdot H_2(\sigma)^{-1}$; 最后计算 $M = C_{M'} \cdot e(C_1, g^{tH_1(id)})$ 。

采用上述技术方案带来的有益效果：

通过本发明，数据拥有者在每次需要撤销共享用户时，仅仅需要发送一个撤销的共享用户列表给云服务器，传统方法在 Intel(R) Core(TM) i5-8250U CPU @ 1.60GHZ 8GB RAM 的 PC 机上需要 144 毫秒产生新的共享密钥，采用本发明后几乎是实时的。同时，传统方法无法在智能手机等移动设备上计算生成新的共享密钥，而本发明可以支持数据拥有者在智能手机等移动设备上授权数据共享。

附图说明

图 1 是本发明的方法流程图。

具体实施方式

以下将结合附图，对本发明的技术方案进行详细说明。

一种可撤销的云数据安全共享方法，如图 1 所述，包括以下步骤：

步骤 1：云服务器生成系统的公共参数和系统的主密钥；

步骤 2：云服务器为每个用户 id 生成对应的私钥；

步骤 3：数据拥有者将需要共享的数据 M 加密成密文 C ，并上传至云服务器；

步骤 4：数据拥有者为初始的共享用户列表 S 生成共享密钥，并上传至云服务器；

步骤 5：数据拥有者是否需要撤销部分共享用户，若是，进入步骤 6，若否进入步骤 7；

步骤 6：云服务器从数据拥有者处接收需要撤销的共享用户列表 R ，得到新

的共享用户列表 $S'=S-R$ ，并生成共享用户列表 S' 对应的新的共享密钥；

步骤 7：云服务器根据密文 C 和当前的共享密钥生成共享用户的密文 CT ；

步骤 8：各用户从云服务器下载密文，利用私钥进行解密，获得数据 M 。

在本实施例中，步骤 1 采用如下优选方案实现：

云服务器首先选取一个标准椭圆曲线，并根据该椭圆曲线构造循环群 G 以及群 G 上的双线性运算 $e:G \times G \rightarrow G_T$ ，其中 G_T 是由双线性运算 e 的结果构成的群，群 G 的生成元为 g ，阶数为素数 p ；云服务器随机选取群 G 上的元素 $\mu, Q \in G$ 和整数 $\alpha \in Z_p$ ，其中 Z_p 表示整数集合 $\{0,1,\dots,p-1\}$ ，计算 $g_1 = g^\alpha, g_2 = g^{\alpha^2}, \dots, g_N = g^{\alpha^N}$ ， $\mu_1 = \mu^\alpha, \mu_2 = \mu^{\alpha^2}, \dots, \mu_N = \mu^{\alpha^N}$ ， $v = e(g, \mu)$ ，其中 N 为系统支持的最大用户数量；云服务器生成两个抗碰撞哈希函数： $H_1: \{0,1\}^* \rightarrow Z_p$ ， $H_2: G_T \rightarrow G$ ，其中 $\{0,1\}^*$ 表示任意长度的 0,1 字符串；云服务器生成系统的公共参数 $mpk = (G, G_T, e, p, g, g_1, \dots, g_N, \mu_1, \dots, \mu_N, v, Q, H_1, H_2)$ 以及系统的主密钥 $msk = (\alpha, \mu)$ ；

在本实施例中，步骤 2 采用如下优选方案实现：

每个用户 id 生成对应的私钥 $sk_{id} = \mu^{1/(\alpha + H_1(id))}$ 。

在本实施例中，步骤 3 采用如下优选方案实现：

数据拥有者将数据 M 加密成密文 $C = (C_M, C_0, C_1)$ ，其中 $C_M = M \cdot v^r$ ， $C_0 = g^{r(\alpha + (H_1(id)))}$ ， $C_1 = Q^r$ ， $r \in Z_p$ 是随机选取的整数。

在本实施例中，步骤 4 采用如下优选方案实现：

数据拥有者为初始的共享用户列表 S 生成共享密钥 rk ：

$$rk = (rk_1, rk_2, rk_3, rk_4, rk_5, (rk_{6,i})_{i \in \{1,2,\dots,k+1\}})$$

其中， $rk_1 = sk_{id} \cdot Q^t$ ， $rk_2 = g^{\alpha t}$ ， $rk_3 = g^{tH_1(id)} \cdot H_2(\sigma)$ ，

$$rk_4 = e(g, \mu)^s \cdot \sigma, \quad rk_5 = g^{s \cdot \prod_{id \in S} (\alpha + H_1(id))}, \quad rk_{6,i} = \mu_i^s, i \in \{1,2,\dots,k+1\};$$

$t, s \in Z_p, \sigma \in G_T$, k 为系统支持的最大撤销用户数。

在本实施例中, 步骤 6 采用如下优选方案实现:

云服务器生成共享用户列表 S' 对应的新的共享密钥 rk' :

$$rk' = (rk_1, rk_2, rk_3, rk_4, rk_5, rk_6)$$

$$\text{其中, } rk_4 = rk_4 \cdot e(g, \prod_{i=1}^l rk_{6,i}^{f_i}), \quad rk_5 = rk_5^{\frac{1}{\prod_{id' \in R} H_1(id')}} , \quad rk_6 = \prod_{i=1}^{l+1} rk_{6,i}^{f_{i-1}} ;$$

f_i 是多项式 $F(x)$ 的项 x^i 的系数,

$$F(x) = \frac{1}{\prod_{id' \in R} H_1(id')} \prod_{id' \in R} (x + H_1(id')) \square f_l x^l + f_{l-1} x^{l-1} + \dots + f_1 x + f_0 .$$

在本实施例中, 步骤 7 采用如下优选方案实现:

生成的共享密文 $CT = (C_{M'}, C_1, C_2, C_3, C_4, C_5)$; 若当前共享密钥为原共享密钥 rk , 则 $C_{M'} = C_M \cdot e(rk_1, C_0)^{-1} \cdot (rk_2, C_1)$, $C_1 = C_1$, $C_2 = rk_3$, $C_3 = rk_4$, $C_4 = rk_5$, $C_5 = rk_{6,1}$; 若当前共享密钥为新的共享密钥 rk' , 则 $C_{M'} = C_M \cdot e(rk_1, C_0)^{-1} \cdot (rk_2, C_1)$, $C_1 = C_1$, $C_2 = rk_3$, $C_3 = rk_4$, $C_4 = rk_5$, $C_5 = rk_{6'}$ 。

在本实施例中, 步骤 8 采用如下优选方案实现:

若用户为数据拥有者, 从云服务器下载密文 C , 解密得到数据 $M = C_M \cdot e(sk_{id}, C_0)^{-1}$; 若用户不是数据拥有者, 从云服务器下载共享密文 CT ,

首先计算 $T = \left(e(C_5^{-1}, g^{\rho_{i,S}(\alpha)}) \cdot e(sk_{id}, C_4) \right)^{1/\prod_{j=1, j \neq i}^S H_1(id_j)}$, 其中 i 表示实施解密的用户, j 表示 S 中用户 i 以外的用户, id_j 表示用户 j 的 id ,

$$\rho_{i,S}(\alpha) = \frac{1}{\alpha} \cdot \left(\prod_{j=1, j \neq i}^S (\alpha + H_1(id_j)) - \prod_{j=1, j \neq i}^S H_1(id_j) \right) ; \quad \text{再 计 算}$$

$$\sigma = C_3 \cdot T^{-1}, \quad g^{tH_1(id)} = C_2 \cdot H_2(\sigma)^{-1}; \quad \text{最后计算 } M = C_{M'} \cdot e(C_1, g^{tH_1(id)}) .$$

实施例仅为说明本发明的技术思想, 不能以此限定本发明的保护范围, 凡是

按照本发明提出的技术思想，在技术方案基础上所做的任何改动，均落入本发明保护范围之内。

权 利 要 求 书

1、一种可撤销的云数据安全共享方法，其特征在于，包括以下步骤：

- (1) 云服务器生成系统的公共参数和系统的主密钥；
- (2) 云服务器为每个用户 id 生成对应的私钥；
- (3) 数据拥有者将需要共享的数据 M 加密成密文 C ，并上传至云服务器；
- (4) 数据拥有者为初始的共享用户列表 S 生成共享密钥，并上传至云服务器；
- (5) 数据拥有者是否需要撤销部分共享用户，若是，进入步骤 (6)，若否进入步骤 (7)；
- (6) 云服务器从数据拥有者处接收需要撤销的共享用户列表 R ，得到新的共享用户列表 $S'=S-R$ ，并生成共享用户列表 S' 对应的新的共享密钥；
- (7) 云服务器根据密文 C 和当前的共享密钥生成共享用户的密文 CT ；
- (8) 各用户从云服务器下载密文，利用私钥进行解密，获得数据 M 。

2、根据权利要求 1 所述可撤销的云数据安全共享方法，其特征在于，在步骤 (1) 中，云服务器首先选取一个标准椭圆曲线，并根据该椭圆曲线构造循环群 G 以及群 G 上的双线性运算 $e:G \times G \rightarrow G_T$ ，其中 G_T 是由双线性运算 e 的结果构成的群，群 G 的生成元为 g ，阶数为素数 p ；云服务器随机选取群 G 上的元素 $\mu, Q \in G$ 和整数 $\alpha \in Z_p$ ，其中 Z_p 表示整数集合 $\{0,1,\dots,p-1\}$ ，计算 $g_1 = g^\alpha, g_2 = g^{\alpha^2}, \dots, g_N = g^{\alpha^N}$ ， $\mu_1 = \mu^\alpha, \mu_2 = \mu^{\alpha^2}, \dots, \mu_N = \mu^{\alpha^N}$ ， $v = e(g, \mu)$ ，其中 N 为系统支持的最大用户数量；云服务器生成两个抗碰撞哈希函数：

$H_1: \{0,1\}^* \rightarrow Z_p$ ， $H_2: G_T \rightarrow G$ ，其中 $\{0,1\}^*$ 表示任意长度的 0,1 字符串；云服务器生成系统的公共参数 $mpk = (G, G_T, e, p, g, g_1, \dots, g_N, \mu_1, \dots, \mu_N, v, Q, H_1, H_2)$ 以及系统的主密钥 $msk = (\alpha, \mu)$ ；

3、根据权利要求 2 所述可撤销的云数据安全共享方法，其特征在于，在步

骤 (2) 中, 每个用户 id 生成对应的私钥 $sk_{id} = \mu^{1/(\alpha+H_1(id))}$ 。

4、根据权利要求 3 所述可撤销的云数据安全共享方法, 其特征在于, 在步骤 (3) 中, 数据拥有者将数据 M 加密成密文 $C=(C_M, C_0, C_1)$, 其中 $C_M = M \cdot v^r$, $C_0 = g^{r(\alpha+(H_1(id)))}$, $C_1 = Q^r$, $r \in Z_p$ 是随机选取的整数。

5、根据权利要求 4 所述可撤销的云数据安全共享方法, 其特征在于, 在步骤 (4) 中, 数据拥有者为初始的共享用户列表 S 生成共享密钥 rk :

$$rk = (rk_1, rk_2, rk_3, rk_4, rk_5, (rk_{6,i})_{i \in \{1,2,\dots,k+1\}})$$

其中, $rk_1 = sk_{id} \cdot Q^t$, $rk_2 = g^{\alpha t}$, $rk_3 = g^{tH_1(id)} \cdot H_2(\sigma)$,

$$rk_4 = e(g, \mu)^s \cdot \sigma, \quad rk_5 = g^{s \cdot \prod_{id \in S} (\alpha + H_1(id))}, \quad rk_{6,i} = \mu_i^s, i \in \{1,2,\dots,k+1\};$$

$t, s \in Z_p, \sigma \in G_T$, k 为系统支持的最大撤销用户数。

6、根据权利要求 5 所述可撤销的云数据安全共享方法, 其特征在于, 在步骤 (6) 中, 云服务器生成共享用户列表 S' 对应的新的共享密钥 rk' :

$$rk' = (rk_1, rk_2, rk_3, rk_{4'}, rk_{5'}, rk_{6'})$$

其中, $rk_{4'} = rk_4 \cdot e(g, \prod_{i=1}^l rk_{6,i}^{f_i})$, $rk_{5'} = rk_5^{\frac{1}{\prod_{id' \in R} H_1(id')}}$, $rk_{6'} = \prod_{i=1}^{l+1} rk_{6,i}^{f_{i-1}}$;

f_i 是多项式 $F(x)$ 的项 x^i 的系数,

$$F(x) = \frac{1}{\prod_{id' \in R} H_1(id')} \prod_{id' \in R} (x + H_1(id')) \square f_l x^l + f_{l-1} x^{l-1} + \dots + f_1 x + f_0.$$

7、根据权利要求 6 所述可撤销的云数据安全共享方法, 其特征在于, 在步骤 (7) 中, 生成的共享密文 $CT=(C_{M'}, C_{1'}, C_{2'}, C_{3'}, C_{4'}, C_{5'})$; 若当前共享密钥为原共享密钥 rk , 则 $C_{M'} = C_M \cdot e(rk_1, C_0)^{-1} \cdot (rk_2, C_1)$, $C_{1'} = C_1$, $C_{2'} = rk_3$, $C_{3'} = rk_4$, $C_{4'} = rk_5$, $C_{5'} = rk_{6,1}$; 若当前共享密钥为新的共享密钥 rk' , 则 $C_{M'} = C_M \cdot e(rk_1, C_0)^{-1} \cdot (rk_2, C_1)$, $C_{1'} = C_1$, $C_{2'} = rk_3$, $C_{3'} = rk_{4'}$, $C_{4'} = rk_{5'}$, $C_{5'} = rk_{6'}$ 。

8、根据权利要求 7 所述可撤销的云数据安全共享方法, 其特征在于, 在步

骤 (8) 中, 若用户为数据拥有者, 从云服务器下载密文 C , 解密得到数据 $M = C_M \cdot e(sk_{id}, C_0)^{-1}$; 若用户不是数据拥有者, 从云服务器下载共享密文 CT , 首先计算 $T = \left(e(C_{S'}^{-1}, g^{\rho_{i,S}(\alpha)}) \cdot e(sk_{id}, C_{4'}) \right)^{1/\prod_{j=1, j \neq i}^S H_1(id_j)}$, 其中 i 表示实施解密的用户, j 表示 S 中用户 i 以外的用户, id_j 表示用户 j 的 id , $\rho_{i,S}(\alpha) = \frac{1}{\alpha} \cdot \left(\prod_{j=1, j \neq i}^S (\alpha + H_1(id_j)) - \prod_{j=1, j \neq i}^S H_1(id_j) \right)$; 再计算 $\sigma = C_{3'} \cdot T^{-1}$, $g^{tH_1(id)} = C_{2'} \cdot H_2(\sigma)^{-1}$; 最后计算 $M = C_M \cdot e(C_1, g^{tH_1(id)})$ 。

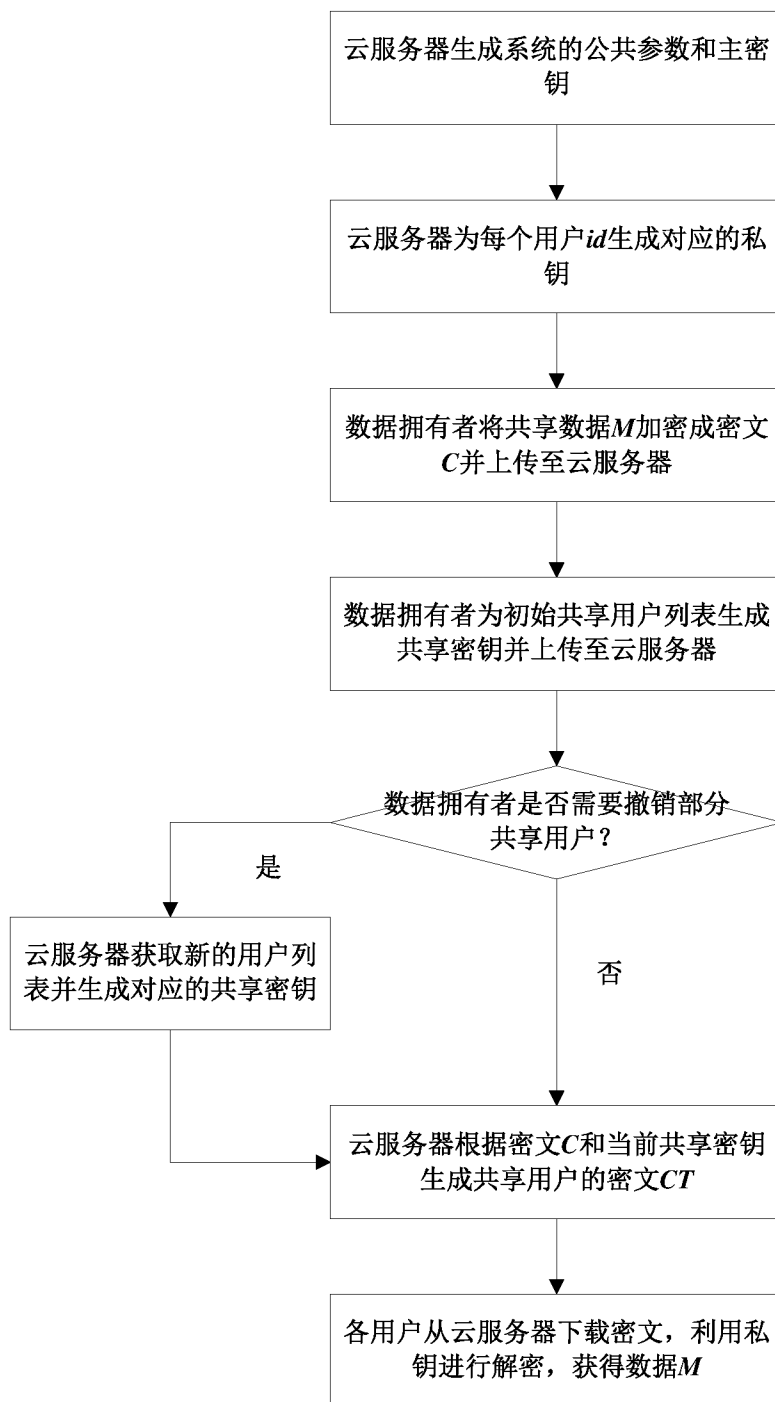


图 1

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/083765

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC, ISI, IEEE: 云服务器, 云端, 数据, 共享, 撤销, 秘钥, 密钥, 群, 组, 列表, 名单, 新, 更新, 重新, 加密, 解密, cloud, server, data, sharing, share, revoke, revocation, user, group, list, update, new, key, decryption, encrypt

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 109889494 A (NANJING UNIVERSITY OF AERONAUTICS AND ASTRONAUTICS) 14 June 2019 (2019-06-14) claims 1-8	1-8
A	CN 105933345 A (UNIVERSITY OF ELECTRONIC SCIENCE AND TECHNOLOGY OF CHINA) 07 September 2016 (2016-09-07) description, paragraphs [0007]-[0019]	1-8
A	CN 104901968 A (HUAZHONG UNIVERSITY OF SCIENCE AND TECHNOLOGY) 09 September 2015 (2015-09-09) entire document	1-8
A	CN 104022869 A (XIDIAN UNIVERSITY) 03 September 2014 (2014-09-03) entire document	1-8
A	Jaya Rao Gudeme et al. "Public Integrity Auditing for Shared Data with Efficient and Secure User Revocation in Cloud Computing" <i>2018 International Conference On Advances in Communication and Computing Technology (ICACCT)</i> , 09 February 2018 (2018-02-09), entire document	1-8



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

20 September 2019

Date of mailing of the international search report

09 October 2019

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing
100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/083765

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WEI, Jianghong et al. "Secure and Efficient Attribute-Based Access Control for Multiauthority Cloud Storage" <i>IEEE SYSTEMS JOURNAL</i> , Vol. 12, No. 2, 30 June 2018 (2018-06-30), entire document	1-8

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2019/083765

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	109889494	A	14 June 2019	None	
CN	105933345	A	07 September 2016	None	
CN	104901968	A	09 September 2015	None	
CN	104022869	A	03 September 2014	None	

国际检索报告

国际申请号

PCT/CN2019/083765

A. 主题的分类 H04L 29/06 (2006.01) i 按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类																				
B. 检索领域 检索的最低限度文献 (标明分类系统和分类号) H04L 包含在检索领域中的除最低限度文献以外的检索文献 在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用)) CNPAT, CNKI, WPI, EPDOC, ISI, IEEE: 云服务器, 云端, 数据, 共享, 撤销, 秘钥, 密钥, 群, 组, 列表, 名单, 新, 更新, 重新, 加密, 解密, cloud, server, data, sharing, share, revoke, revocation, user, group, list, update, new, key, decryption, encrypt																				
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>PX</td> <td>CN 109889494 A (南京航空航天大学) 2019年 6月 14日 (2019 - 06 - 14) 权利要求1-8</td> <td>1-8</td> </tr> <tr> <td>A</td> <td>CN 105933345 A (电子科技大学) 2016年 9月 7日 (2016 - 09 - 07) 说明书第[0007]-[0019]段</td> <td>1-8</td> </tr> <tr> <td>A</td> <td>CN 104901968 A (华中科技大学) 2015年 9月 9日 (2015 - 09 - 09) 全文</td> <td>1-8</td> </tr> <tr> <td>A</td> <td>CN 104022869 A (西安电子科技大学) 2014年 9月 3日 (2014 - 09 - 03) 全文</td> <td>1-8</td> </tr> <tr> <td>A</td> <td>Jaya Rao Gudeme 等. "Public Integrity Auditing for Shared Data with Efficient and Secure User Revocation in Cloud Computing" 2018 International Conference On Advances in Communication and Computing Technology (ICACCT), 2018年 2月 9日 (2018 - 02 - 09), 全文</td> <td>1-8</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	PX	CN 109889494 A (南京航空航天大学) 2019年 6月 14日 (2019 - 06 - 14) 权利要求1-8	1-8	A	CN 105933345 A (电子科技大学) 2016年 9月 7日 (2016 - 09 - 07) 说明书第[0007]-[0019]段	1-8	A	CN 104901968 A (华中科技大学) 2015年 9月 9日 (2015 - 09 - 09) 全文	1-8	A	CN 104022869 A (西安电子科技大学) 2014年 9月 3日 (2014 - 09 - 03) 全文	1-8	A	Jaya Rao Gudeme 等. "Public Integrity Auditing for Shared Data with Efficient and Secure User Revocation in Cloud Computing" 2018 International Conference On Advances in Communication and Computing Technology (ICACCT), 2018年 2月 9日 (2018 - 02 - 09), 全文	1-8
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求																		
PX	CN 109889494 A (南京航空航天大学) 2019年 6月 14日 (2019 - 06 - 14) 权利要求1-8	1-8																		
A	CN 105933345 A (电子科技大学) 2016年 9月 7日 (2016 - 09 - 07) 说明书第[0007]-[0019]段	1-8																		
A	CN 104901968 A (华中科技大学) 2015年 9月 9日 (2015 - 09 - 09) 全文	1-8																		
A	CN 104022869 A (西安电子科技大学) 2014年 9月 3日 (2014 - 09 - 03) 全文	1-8																		
A	Jaya Rao Gudeme 等. "Public Integrity Auditing for Shared Data with Efficient and Secure User Revocation in Cloud Computing" 2018 International Conference On Advances in Communication and Computing Technology (ICACCT), 2018年 2月 9日 (2018 - 02 - 09), 全文	1-8																		
☒ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。																				
* 引用文件的具体类型: "A" 认为不特别相关的表示了现有技术一般状态的文件 "E" 在国际申请日的当天或之后公布的在先申请或专利 "L" 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的) "O" 涉及口头公开、使用、展览或其他方式公开的文件 "P" 公布日先于国际申请日但迟于所要求的优先权日的文件 "T" 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 "X" 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 "Y" 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 "&" 同族专利的文件																				
国际检索实际完成的日期 2019年 9月 20日		国际检索报告邮寄日期 2019年 10月 9日																		
ISA/CN的名称和邮寄地址 中国国家知识产权局 (ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451		受权官员 王小千 电话号码 (86-10)-53961683																		

C. 相关文件		
类 型*	引用文件，必要时，指明相关段落	相关的权利要求
A	WEI, Jianghong等. "Secure and Efficient Attribute-Based Access Control for Multiauthority Cloud Storage" IEEE SYSTEMS JOURNAL, 第12卷, 第2期, 2018年 6月 30日 (2018 - 06 - 30), 全文	1-8

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2019/083765

检索报告引用的专利文件			公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN	109889494	A	2019年 6月 14日	无	
CN	105933345	A	2016年 9月 7日	无	
CN	104901968	A	2015年 9月 9日	无	
CN	104022869	A	2014年 9月 3日	无	