



(12) 发明专利申请

(10) 申请公布号 CN 103414559 A

(43) 申请公布日 2013. 11. 27

(21) 申请号 201310188994. X

(22) 申请日 2013. 05. 20

(71) 申请人 广州中长康达信息技术有限公司  
地址 510663 广东省广州市天河区思成路  
19 号宏太智慧谷五号楼  
申请人 广东工业大学

(72) 发明人 江枚元 凌捷 柳毅 钟奇  
郭圣昌

(74) 专利代理机构 广州嘉权专利商标事务所有  
限公司 44205  
代理人 谭英强

(51) Int. Cl.

H04L 9/32(2006. 01)

H04L 29/06(2006. 01)

权利要求书3页 说明书11页

(54) 发明名称

一种云计算环境下的基于类 IBE 系统的身份  
认证方法

(57) 摘要

本发明公开了一种云计算环境下的基于类 IBE 系统的身份认证方法,包括:用户端获取注册用户的身份信息以及口令密码;用户端进行系统参数初始化;将注册数据和签名报文等参数发送到云服务端;云服务端对签名报文进行验证;验证接收到的注册信息;云服务端根据注册数据生成摘要信息;对摘要信息进行综合处理后得到加密密文,并将加密密文发送到用户端;用户端接收加密密文后,进行解密处理及验证。本发明避免了密钥托管、密钥分发等带来的安全问题,具有高可靠性,而且在认证过程中采用了双向签名认证方式进行认证,避免了由于单向认证造成的漏洞,提高了安全性,而且响应速度快,带宽利用率高,可广泛应用在云计算环境下进行身份认证。

1. 一种云计算环境下的基于类 IBE 系统的身份认证方法,其特征在于,包括:

S1、用户端获取注册用户的身份信息  $M_{id}$  以及口令密码  $password$ ,并对口令密码进行哈希散列运算后,获得散列口令密码  $Pwd$ ;

S2、用户端进行系统参数初始化,得到注册用户主密钥  $S$  以及系统参数  $T$ ,进而生成第一公钥  $EID_U$  和第一私钥  $d_{eid}$ ;

S3、将注册用户的注册信息  $M_k$  进行哈希散列运算,生成第一密文摘要  $DK_s$ ,进而结合系统参数  $T$  及第一私钥  $d_{eid}$  生成签名报文  $DK$  后,将注册数据  $M_{reg}$ 、第一公钥  $EID_U$ 、第一密文摘要  $DK_s$  和签名报文  $DK$  发送到云服务端;

S4、云服务端对签名报文  $DK$  进行验证,若验证通过,则继续执行步骤 S5,否则结束;

S5、对接收到的注册信息  $M_k$  进行哈希散列运算后,验证得到的结果是否等于第一密文摘要  $DK_s$ ,若是,则继续执行步骤 S6,否则结束;

S6、云服务端根据注册数据  $M_{reg}$  生成第一加密参数  $RU_{pub}$  和第二私钥  $RU_{PE}$ ,并产生一个用于对该注册用户进行身份标识的标识码  $\lambda$ ,然后对第一加密参数  $RU_{pub}$  和标识码  $\lambda$  进行哈希散列运算后,获得摘要信息  $D$ ;

S7、采用第一加密参数  $RU_{pub}$  和第二私钥  $RU_{PE}$  对摘要信息  $D$  进行加密后得到第二摘要密文  $DS$ ,进而采用第一公钥  $EID_U$  对第二摘要密文  $DS$ 、第一加密参数  $RU_{pub}$  和标识码  $\lambda$  进行加密后,得到加密密文  $FS$ ,并将加密密文  $FS$  发送到用户端;

S8、用户端接收加密密文  $FS$  后,采用第一私钥  $d_{eid}$  对加密密文  $FS$  进行解密,还原得到第二摘要密文  $DS$ 、第一加密参数  $RU_{pub}$  和标识码  $\lambda$ ,然后采用第一加密参数  $RU_{pub}$  和第一公钥  $EID_U$  对第二摘要密文  $DS$  进行解密后,得到摘要信息  $D$ ;

S9、用户端对第一加密参数  $RU_{pub}$  和标识码  $\lambda$  进行哈希散列运算后,验证得到的结果是否等于摘要信息  $D$ ,若是,则认证成功;

所述注册信息  $M_k$  包括身份信息  $M_{id}$  和散列口令密码  $Pwd$ ,所述注册数据  $M_{reg}$  包括身份信息  $M_{id}$ 、散列口令密码  $Pwd$  和系统参数  $T$ 。

2. 根据权利要求 1 所述的一种云计算环境下的基于类 IBE 系统的身份认证方法,其特征在于,所述步骤 S2,包括:

S21、获取一个特征为素数  $p$  的有限域  $F_p$ ,并在有限域  $F_p$  上选取域元素  $a, b$ ,使域元素  $a, b$  满足椭圆曲线  $E(F_p)$  的方程:

$$y^3 = x^2 + a \cdot x + b \pmod{p}, \text{其中 } 4 \cdot a^3 + 27 \cdot b^2 \neq 0 \pmod{p};$$

S22、在椭圆曲线  $E(F_p)$  上选取一个基点  $G$ ,并计算得到基点  $G$  的阶  $q$ ,进而分别计算得到  $G$  点的两个  $q$  阶群  $G_1$  及  $G_2$ ,  $G_1$  及  $G_2$  满足以下双线性映射条件:

$$G_1 \times G_1 \rightarrow G_2;$$

S23、采用下式计算椭圆曲线  $E(F_p)$  的阶  $\#E(F_p)$  除于基点  $G$  的阶  $q$  得到的商  $h$ :

$$h = \#E(F_p) / q$$

其中,商  $h$  满足  $h \leq 4$ ,且  $\#E(F_p)$ 、 $p$ 、 $q$  满足以下条件:

$$\begin{cases} \#E(Fp) \neq p \\ \#p' \neq 1(\text{mod } q) \\ p = 2 \text{ mod } 3 \\ p = 6q - 1 \end{cases}$$

上式中  $t$  为常数, 且  $1 \leq t < 20$ ;

S24、生成第一随机数  $S$  且满足  $S \in Z_q^*$ , 则  $S$  为注册用户的主密钥, 并计算第二加密参数  $P_{\text{pub}} = S \cdot G$ , 进而选取 4 个哈希函数  $H, Q, H_1$  及  $Q_1$ :

$$\begin{aligned} H: F_p^2 &\rightarrow \{0,1\}^n, \\ Q: \{0,1\}^n &\rightarrow F_p^2, \end{aligned}$$

$$H_1: \{0,1\}^n \times \{0,1\}^n \rightarrow F_q,$$

$$Q_1: \{0,1\}^n \rightarrow \{0,1\}^n,$$

其中,  $F_p^2$  是一个有限群且  $F_p^2 \in \{0,1\}^n$ ,  $n$  为自然数;

S25、根据下式可得到系统参数  $T$  为:

$$T = (p, a, b, G, p_{\text{pub}}, q, h, H, Q, H_1, Q_1);$$

同时可得到消息空间  $M$  为  $M = \{0,1\}^n$ , 密文空间  $C$  为  $C = G_1 \times \{0,1\}^n$ ;

S26、根据身份信息  $M_{\text{id}}$  生成第一公钥  $EID_U$ , 进而将第一公钥  $EID_U$  映射到椭圆曲线  $E(Fp)$  上的一个点  $E_p$ , 并计算得到第一公钥  $d_{\text{eid}}: d_{\text{eid}} = s \cdot E_p$ 。

3. 根据权利要求 2 所述的一种云计算环境下的基于类 IBE 系统的身份认证方法, 其特征在于, 所述步骤 S3, 包括:

S31、根据下式将注册用户的注册信息  $M_k$  进行哈希散列运算, 生成第一密文摘要  $DK_s$ :

$$DK_s = \text{Hash}(M_k \langle M_{\text{id}}, \text{Pwd} \rangle);$$

S32、选取一个整数  $k$ ,  $k$  满足条件:  $0 < k < n$ ;

S33、根据下式计算  $\beta$ , 若得到的结果为  $\beta = 0$ , 则返回步骤 S32, 反之执行步骤 S34:

$$\begin{cases} kG = (x_1, y_1) \\ \beta = x_1 \text{ mod } n \end{cases};$$

S34、根据以下公式计算  $\omega$ , 若得到的结果为  $\omega = 0$ , 则返回步骤 S32, 反之执行步骤 S35:

$$\begin{cases} K^* = k^{-1} \text{ mod } n \\ \omega = K^* \{DK_s + d_{\text{eid}}\} \text{ mod } n \end{cases};$$

S35、得到签名报文  $DK = (\beta, \omega)$ , 进而将注册数据  $M_{\text{reg}}$ 、第一公钥  $EID_U$ 、第一密文摘要  $DK_s$  和签名报文  $DK$  发送到云服务端。

4. 根据权利要求 3 所述的一种云计算环境下的基于类 IBE 系统的身份认证方法, 其特征在于, 所述步骤 S4, 包括:

S41、判断签名报文  $DK$  是否满足以下条件:

$$\begin{cases} \beta > 0 \\ \omega < n \end{cases},$$

若是,则继续执行步骤 S42,否则结束;

S42、根据下列公式计算  $w$  :

$$\begin{cases} u = \omega^{-1} \bmod n \\ \mu_1 = (DK_s u) \bmod n \\ \mu_2 = (\beta u) \bmod n \\ \mu_1 G + \mu_2 EID_U = (x_0, y_0) \\ w = x_0 \bmod n \end{cases}$$

S43、判断  $w$  是否等于  $\beta$ ,若是,则验证通过,继续执行步骤 S5, 否则结束。

5. 根据权利要求 4 所述的一种云计算环境下的基于类 IBE 系统的身份认证方法,其特征在于,所述步骤 S6,包括:

S61、云服务端选取第二随机数  $R_c$  作为该注册用户交互认证的主密钥  $S'$  后,采用下式结合注册数据  $M_{reg}$  中的系统参数  $T$  生成第一加密参数  $RU_{pub}$ :  $RU_{pub} = R_c \cdot G$ ;

S62、将第一公钥  $EID_U$  映射到椭圆曲线  $E(F_p)$  上的一个点  $EID_p$  后,根据下式计算得到第二私钥  $RU_{PE}$ :  $RU_{PE} = R_c \cdot EID_p$ ;

S63、云服务端产生一个用于对该注册用户进行身份标识的标识码  $\lambda$ , 然后根据下式对第一加密参数  $RU_{pub}$  和标识码  $\lambda$  进行哈希散列运算后,获得摘要信息  $D$ :

$$D = \text{Hash}(RU_{pub}, \lambda)。$$

6. 根据权利要求 5 所述的一种云计算环境下的基于类 IBE 系统的身份认证方法,其特征在于,所述步骤 S7,包括:

S71、根据下式采用第一加密参数  $RU_{pub}$  和第二私钥  $RU_{PE}$  对摘要信息  $D$  进行加密后得到第二摘要密文  $DS$ :

$$DS = EC(D, r, RU_{pub}, RU_{PE})$$

其中,  $r = H_1(\sigma, D)$ , 而  $\sigma$  为第一随机串;

S72、根据下式采用第一公钥  $EID_U$  对第二摘要密文  $DS$ 、第一加密参数  $RU_{pub}$  和标识码  $\lambda$  进行加密后,得到加密密文  $FS$  后,并将加密密文  $FS$  发送到用户端:

$$FS = EC(DS, RU_{pub}, \lambda, EID_U, R, P_{pub})$$

其中,  $R = H_1(\pi, DS, RU_{pub}, \lambda)$ ,  $\pi$  为第二随机串,  $P_{pub}$  为系统参数  $T$  中的第二加密参数。

7. 根据权利要求 6 所述的一种云计算环境下的基于类 IBE 系统的身份认证方法,其特征在于,所述步骤 S8,包括:

S81、用户端接收加密密文  $FS$  后,根据下式采用第一私钥  $d_{eid}$  对加密密文  $FS$  进行解密,还原得到第二摘要密文  $DS$ 、第一加密参数  $RU_{pub}$  和标识码  $\lambda$ :  $(DS, RU_{pub}, \lambda) = DC(P_{pub}, d_{eid}, FS)$ ;

S82、根据下式采用第一加密参数  $RU_{pub}$  和第一公钥  $EID_U$  对第二摘要密文  $DS$  进行解密后,得到摘要信息  $D$ :  $D = DC(RU_{pub}, DS, EID_U)$ 。

## 一种云计算环境下的基于类 IBE 系统的身份认证方法

### 技术领域

[0001] 本发明涉及一种身份认证方法,特别是一种云计算环境下的基于类 IBE 系统的身份认证方法。

### 背景技术

[0002] 传统的 IBE 系统中最重要的是 PKG (Private Key Generator),即私钥生成中心,PKG 在接收到用户的身份信息后,根据用户的身份信息使用主密钥为用户产生相应的包括公私钥对的密钥,并通过可信信道将私钥转发给用户。这种模式的身份认证方法,用户私钥是由第三方机构产生并进行转发的,导致了密钥分发和托管的安全信任问题,因而密钥管理成为最棘手的问题。而在云计算环境下,当用户通过用户端与云服务端进行数据交互时,若采用这种模式的身份认证方法,需引入第三方可信机构,将带来庞大的身份认证、密钥分发和密钥托管等问题,提高了云计算过程的复杂性,同时也增大了验证过程的通信量开销,影响云计算的效率和质量,而且,对密钥数据的存储及管理也带来了不安全性。

### 发明内容

[0003] 为了解决上述的技术问题,本发明的目的是提供一种云计算环境下的高效、高可靠性且安全的基于类 IBE 系统的身份认证方法。

[0004] 本发明解决其技术问题所采用的技术方案是:

[0005] 一种云计算环境下的基于类 IBE 系统的身份认证方法,包括:

[0006] S1、用户端获取注册用户的身份信息  $M_{id}$  以及口令密码 password,并对口令密码进行哈希散列运算后,获得散列口令密码 Pwd;

[0007] S2、用户端进行系统参数初始化,得到注册用户主密钥 S 以及系统参数 T,进而生成第一公钥  $EID_U$  和第一私钥  $d_{eid}$ ;

[0008] S3、将注册用户的注册信息  $M_k$  进行哈希散列运算,生成第一密文摘要  $DK_s$ ,进而结合系统参数 T 及第一私钥  $d_{eid}$  生成签名报文 DK 后,将注册数据  $M_{reg}$ 、第一公钥  $EID_U$ 、第一密文摘要  $DK_s$  和签名报文 DK 发送到云服务端;

[0009] S4、云服务端对签名报文 DK 进行验证,若验证通过,则继续执行步骤 S5,否则结束;

[0010] S5、对接收到的注册信息  $M_k$  进行哈希散列运算后,验证得到的结果是否等于第一密文摘要  $DK_s$ ,若是,则继续执行步骤 S6,否则结束;

[0011] S6、云服务端根据注册数据  $M_{reg}$  生成第一加密参数  $RU_{pub}$  和第二私钥  $RU_{PE}$ ,并产生一个用于对该注册用户进行身份标识的标识码  $\lambda$ ,然后对第一加密参数  $RU_{pub}$  和标识码  $\lambda$  进行哈希散列运算后,获得摘要信息 D;

[0012] S7、采用第一加密参数  $RU_{pub}$  和第二私钥  $RU_{PE}$  对摘要信息 D 进行加密后得到第二摘要密文 DS,进而采用第一公钥  $EID_U$  对第二摘要密文 DS、第一加密参数  $RU_{pub}$  和标识码  $\lambda$  进行加密后,得到加密密文 FS,并将加密密文 FS 发送到用户端;

[0013] S8、用户端接收加密密文 FS 后,采用第一私钥  $d_{eid}$  对加密密文 FS 进行解密,还原得到第二摘要密文 DS、第一加密参数  $RU_{pub}$  和标识码  $\lambda$ ,然后采用第一加密参数  $RU_{pub}$  和第一公钥  $EID_U$  对第二摘要密文 DS 进行解密后,得到摘要信息 D;

[0014] S9、用户端对第一加密参数  $RU_{pub}$  和标识码  $\lambda$  进行哈希散列运算后,验证得到的结果是否等于摘要信息 D,若是,则认证成功;

[0015] 所述注册信息  $M_k$  包括身份信息  $M_{id}$  和散列口令密码 Pwd,所述注册数据  $M_{reg}$  包括身份信息  $M_{id}$ 、散列口令密码 Pwd 和系统参数 T。

[0016] 进一步,所述步骤 S2,包括:

[0017] S21、获取一个特征为素数  $p$  的有限域  $F_p$ ,并在有限域  $F_p$  上选取域元素  $a, b$ ,使域元素  $a, b$  满足椭圆曲线  $E(F_p)$  的方程:

[0018]  $y^3 = x^2 + a \cdot x + b \pmod{p}$ ,其中  $4 \cdot a^3 + 27 \cdot b^2 \neq 0 \pmod{p}$ ;

[0019] S22、在椭圆曲线  $E(F_p)$  上选取一个基点  $G$ ,并计算得到基点  $G$  的阶  $q$ ,进而分别计算得到  $G$  点的两个  $q$  阶群  $G_1$  及  $G_2$ , $G_1$  及  $G_2$  满足以下双线性映射条件:

[0020]  $G_1 \times G_1 \rightarrow G_2$ ;

[0021] S23、采用下式计算椭圆曲线  $E(F_p)$  的阶  $\#E(F_p)$  除于基点  $G$  的阶  $q$  得到的商  $h$ :

[0022]  $h = \#E(F_p) / q$

[0023] 其中,商  $h$  满足  $h \leq 4$ ,且  $\#E(F_p)$ 、 $p$ 、 $q$  满足以下条件:

$$[0024] \begin{cases} \#E(F_p) \neq p \\ \#p^t \neq 1 \pmod{q} \\ p = 2 \pmod{3} \\ p = 6q - 1 \end{cases}$$

[0025] 上式中  $t$  为常数,且  $1 \leq t < 20$ ;

[0026] S24、生成第一随机数  $S$  且满足  $S \in \mathbb{Z}_q^*$ ,则  $S$  为注册用户的主密钥,并计算第二加密参数  $P_{pub} = S \cdot G$ ,进而选取 4 个哈希函数  $H, Q, H_1$  及  $Q_1$ :

[0027]  $H: F_p^2 \rightarrow \{0,1\}^n$ ,

[0028]  $Q: \{0,1\}^n \rightarrow F_p^2$ ,

[0029]  $H_1: \{0,1\}^n \times \{0,1\}^n \rightarrow F_q$ ,

[0030]  $Q_1: \{0,1\}^n \rightarrow \{0,1\}^n$ ,

[0031] 其中,  $F_p^2$  是一个有限群且  $F_p^2 \in \{0,1\}^n$ ,  $n$  为自然数;

[0032] S25、根据下式可得到系统参数 T 为:

[0033]  $T = (p, a, b, G, p_{pub}, q, h, H, Q, H_1, Q_1)$ ;

[0034] 同时可得到消息空间  $M$  为  $M = \{0,1\}^n$ ,密文空间  $C$  为  $C = G_1 \times \{0,1\}^n$ ;

[0035] S26、根据身份信息  $M_{id}$  生成第一公钥  $EID_U$ ,进而将第一公钥  $EID_U$  映射到椭圆曲线  $E(F_p)$  上的一个点  $E_p$ ,并计算得到第一公钥  $d_{eid}: d_{eid} = s \cdot E_p$ 。

[0036] 进一步,所述步骤 S3,包括:

[0037] S31、根据下式将注册用户的注册信息  $M_k$  进行哈希散列运算,生成第一密文摘要

$DK_s$  :

[0038]  $DK_s = \text{Hash}(M_k \langle M_{id}, \text{Pwd} \rangle)$  ;

[0039] S32、选取一个整数  $k$ ,  $k$  满足条件 :  $0 < k < n$  ;

[0040] S33、根据下式计算  $\beta$ , 若得到的结果为  $\beta = 0$ , 则返回步骤 S32, 反之执行步骤 S34 :

$$[0041] \begin{cases} kG = (x_1, y_1) \\ \beta = x_1 \bmod n \end{cases};$$

[0042] S34、根据以下公式计算  $\omega$ , 若得到的结果为  $\omega = 0$ , 则返回步骤 S32, 反之执行步骤 S35 :

$$[0043] \begin{cases} K^* = k^{-1} \bmod n \\ \omega = K^* \{DK_s + d_{eid}\} \bmod n \end{cases};$$

[0044] S35、得到签名报文  $DK = (\beta, \omega)$ , 进而将注册数据  $M_{reg}$ 、第一公钥  $EID_U$ 、第一密文摘要  $DK_s$  和签名报文  $DK$  发送到云服务端。

[0045] 进一步, 所述步骤 S4, 包括 :

[0046] S41、判断签名报文  $DK$  是否满足以下条件 :

$$[0047] \begin{cases} \beta > 0 \\ \omega < n \end{cases},$$

[0048] 若是, 则继续执行步骤 S42, 否则结束 ;

[0049] S42、根据下列公式计算  $w$  :

$$[0050] \begin{cases} u = \omega^{-1} \bmod n \\ \mu_1 = (DK_s u) \bmod n \\ \mu_2 = (\beta u) \bmod n \\ \mu_1 G + \mu_2 EID_U = (x_0, y_0) \\ w = x_0 \bmod n \end{cases}$$

[0051] S43、判断  $w$  是否等于  $\beta$ , 若是, 则验证通过, 继续执行步骤 S5, 否则结束。

[0052] 进一步, 所述步骤 S6, 包括 :

[0053] S61、云服务端选取第二随机数  $R_c$  作为该注册用户交互认证的主密钥  $S'$  后, 采用下式结合注册数据  $M_{reg}$  中的系统参数  $T$  生成第一加密参数  $RU_{pub}$  :  $RU_{pub} = R_c \cdot G$  ;

[0054] S62、将第一公钥  $EID_U$  映射到椭圆曲线  $E(F_p)$  上的一个点  $EID_p$  后, 根据下式计算得到第二私钥  $RU_{PE}$  :  $RU_{PE} = R_c \cdot EID_p$  ;

[0055] S63、云服务端产生一个用于对该注册用户进行身份标识的标识码  $\lambda$ , 然后根据下式对第一加密参数  $RU_{pub}$  和标识码  $\lambda$  进行哈希散列运算后, 获得摘要信息  $D$  :

$$[0056] D = \text{Hash}(RU_{pub}, \lambda)$$

[0057] 进一步, 所述步骤 S7, 包括 :

[0058] S71、根据下式采用第一加密参数  $RU_{pub}$  和第二私钥  $RU_{PE}$  对摘要信息  $D$  进行加密后得到第二摘要密文  $DS$  :

[0059]  $DS = EC(D, r, RU_{pub}, RU_{pE})$

[0060] 其中,  $r = H_1(\sigma, D)$ , 而  $\sigma$  为第一随机串;

[0061] S72、根据下式采用第一公钥  $EID_U$  对第二摘要密文  $DS$ 、第一加密参数  $RU_{pub}$  和标识码  $\lambda$  进行加密后, 得到加密密文  $FS$  后, 并将加密密文  $FS$  发送到用户端;

[0062]  $FS = EC(DS, RU_{pub}, \lambda, EID_U, R, P_{pub})$

[0063] 其中,  $R = H_1(\pi, DS, RU_{pub}, \lambda)$ ,  $\pi$  为第二随机串,  $P_{pub}$  为系统参数  $T$  中的第二加密参数。

[0064] 进一步, 所述步骤 S8, 包括:

[0065] S81、用户端接收加密密文  $FS$  后, 根据下式采用第一私钥  $d_{eid}$  对加密密文  $FS$  进行解密, 还原得到第二摘要密文  $DS$ 、第一加密参数  $RU_{pub}$  和标识码  $\lambda$ :  
 $(DS, RU_{pub}, \lambda) = DC(P_{pub}, d_{eid}, FS)$ ;

[0066] S82、根据下式采用第一加密参数  $RU_{pub}$  和第一公钥  $EID_U$  对第二摘要密文  $DS$  进行解密后, 得到摘要信息  $D$ :  $D = DC(RU_{pub}, DS, EID_U)$ 。

[0067] 本发明的有益效果是: 本发明的一种云计算环境下的基于类 IBE 系统的身份认证方法, 不需要 PKG 等第三方可信机构, 采用用户端直接与云服务端进行通讯的方式进行身份认证, 减小了身份认证给云计算过程带来的复杂性, 降低了开销, 避免了密钥托管、密钥分发等带来的安全问题, 具有高可靠性。而且在认证过程中采用了双向签名认证方式进行认证, 避免了由于单向认证造成的漏洞, 提高了安全性, 而且响应速度快, 带宽利用率高。

## 具体实施方式

[0068] 本发明提供了一种云计算环境下的基于类 IBE 系统的身份认证方法, 包括:

[0069] S1、用户端获取注册用户的身份信息  $M_{id}$  以及口令密码  $password$ , 并对口令密码进行哈希散列运算后, 获得散列口令密码  $Pwd$ ;

[0070] S2、用户端进行系统参数初始化, 得到注册用户主密钥  $S$  以及系统参数  $T$ , 进而生成第一公钥  $EID_U$  和第一私钥  $d_{eid}$ ;

[0071] S3、将注册用户的注册信息  $M_k$  进行哈希散列运算, 生成第一密文摘要  $DK_s$ , 进而结合系统参数  $T$  及第一私钥  $d_{eid}$  生成签名报文  $DK$  后, 将注册数据  $M_{reg}$ 、第一公钥  $EID_U$ 、第一密文摘要  $DK_s$  和签名报文  $DK$  发送到云服务端;

[0072] S4、云服务端对签名报文  $DK$  进行验证, 若验证通过, 则继续执行步骤 S5, 否则结束;

[0073] S5、对接收到的注册信息  $M_k$  进行哈希散列运算后, 验证得到的结果是否等于第一密文摘要  $DK_s$ , 若是, 则继续执行步骤 S6, 否则结束;

[0074] S6、云服务端根据注册数据  $M_{reg}$  生成第一加密参数  $RU_{pub}$  和第二私钥  $RU_{pE}$ , 并产生一个用于对该注册用户进行身份标识的标识码  $\lambda$ , 然后对第一加密参数  $RU_{pub}$  和标识码  $\lambda$  进行哈希散列运算后, 获得摘要信息  $D$ ;

[0075] S7、采用第一加密参数  $RU_{pub}$  和第二私钥  $RU_{pE}$  对摘要信息  $D$  进行加密后得到第二摘要密文  $DS$ , 进而采用第一公钥  $EID_U$  对第二摘要密文  $DS$ 、第一加密参数  $RU_{pub}$  和标识码  $\lambda$  进行加密后, 得到加密密文  $FS$ , 并将加密密文  $FS$  发送到用户端;

[0076] S8、用户端接收加密密文 FS 后,采用第一私钥  $d_{\text{eid}}$  对加密密文 FS 进行解密,还原得到第二摘要密文 DS、第一加密参数  $RU_{\text{pub}}$  和标识码  $\lambda$ ,然后采用第一加密参数  $RU_{\text{pub}}$  和第一公钥  $EID_0$  对第二摘要密文 DS 进行解密后,得到摘要信息 D;

[0077] S9、用户端对第一加密参数  $RU_{\text{pub}}$  和标识码  $\lambda$  进行哈希散列运算后,验证得到的结果是否等于摘要信息 D,若是,则认证成功;

[0078] 所述注册信息  $M_k$  包括身份信息  $M_{\text{id}}$  和散列口令密码 Pwd,所述注册数据  $M_{\text{reg}}$  包括身份信息  $M_{\text{id}}$ 、散列口令密码 Pwd 和系统参数 T。

[0079] 进一步作为优选的实施方式,所述步骤 S2,包括:

[0080] S21、获取一个特征为素数  $p$  的有限域  $F_p$ ,并在有限域  $F_p$  上选取域元素  $a, b$ ,使域元素  $a, b$  满足椭圆曲线  $E(F_p)$  的方程:

[0081]  $y^3 = x^2 + a \cdot x + b \pmod{p}$ ,其中  $4 \cdot a^3 + 27 \cdot b^2 \neq 0 \pmod{p}$ ;

[0082] S22、在椭圆曲线  $E(F_p)$  上选取一个基点  $G$ ,并计算得到基点  $G$  的阶  $q$ ,进而分别计算得到  $G$  点的两个  $q$  阶群  $G_1$  及  $G_2$ , $G_1$  及  $G_2$  满足以下双线性映射条件:

[0083]  $G_1 \times G_1 \rightarrow G_2$ ;

[0084] S23、采用下式计算椭圆曲线  $E(F_p)$  的阶  $\#E(F_p)$  除于基点  $G$  的阶  $q$  得到的商  $h$ :

[0085]  $h = \#E(F_p) / q$

[0086] 其中,商  $h$  满足  $h \leq 4$ ,且  $\#E(F_p)$ 、 $p$ 、 $q$  满足以下条件:

$$[0087] \begin{cases} \#E(F_p) \neq p \\ \#p^t \neq 1 \pmod{q} \\ p = 2 \pmod{3} \\ p = 6q - 1 \end{cases}$$

[0088] 上式中  $t$  为常数,且  $1 \leq t < 20$ ;

[0089] S24、生成第一随机数  $S$  且满足  $S \in \mathbb{Z}_q^*$ ,则  $S$  为注册用户的主密钥,并计算第二加密参数  $P_{\text{pub}} = S \cdot G$ ,进而选取 4 个哈希函数  $H, Q, H_1$  及  $Q_1$ :

[0090]  $H: F_p^2 \rightarrow \{0,1\}^n$ ,

[0091]  $Q: \{0,1\}^n \rightarrow F_p^2$ ,

[0092]  $H_1: \{0,1\}^n \times \{0,1\}^n \rightarrow F_q$ ,

[0093]  $Q_1: \{0,1\}^n \rightarrow \{0,1\}^n$ ,

[0094] 其中,  $F_p^2$  是一个有限群且  $F_p^2 \in \{0,1\}^n$ ,  $n$  为自然数;

[0095] S25、根据下式可得到系统参数  $T$  为:

[0096]  $T = (p, a, b, G, P_{\text{pub}}, q, h, H, Q, H_1, Q_1)$ ;

[0097] 同时可得到消息空间  $M$  为  $M = \{0,1\}^n$ ,密文空间  $C$  为  $C = G_1 \times \{0,1\}^n$ ;

[0098] S26、根据身份信息  $M_{\text{id}}$  生成第一公钥  $EID_0$ ,进而将第一公钥  $EID_0$  映射到椭圆曲线  $E(F_p)$  上的一个点  $E_p$ ,并计算得到第一公钥  $d_{\text{eid}}: d_{\text{eid}} = s \cdot E_p$ 。

[0099] 进一步作为优选的实施方式,所述步骤 S3,包括:

[0100] S31、根据下式将注册用户的注册信息  $M_k$  进行哈希散列运算,生成第一密文摘要

DK<sub>s</sub> :

[0101] DK<sub>s</sub>=Hash (M<sub>k</sub><M<sub>id</sub>, Pwd>) ;

[0102] S32、选取一个整数 k, k 满足条件 :0<k<n ;

[0103] S33、根据下式计算 β, 若得到的结果为 β=0, 则返回步骤 S32, 反之执行步骤 S34 :

$$[0104] \begin{cases} kG = (x_1, y_1) \\ \beta = x_1 \bmod n \end{cases};$$

[0105] S34、根据以下公式计算 ω, 若得到的结果为 ω=0, 则返回步骤 S32, 反之执行步骤 S35 :

$$[0106] \begin{cases} K^* = k^{-1} \bmod n \\ \omega = K^* \{DK_s + d_{sid}\} \bmod n \end{cases};$$

[0107] S35、得到签名报文 DK=(β, ω), 进而将注册数据 M<sub>reg</sub>、第一公钥 EID<sub>U</sub>、第一密文摘要 DK<sub>s</sub> 和签名报文 DK 发送到云服务端。

[0108] 进一步作为优选的实施方式, 所述步骤 S4, 包括 :

[0109] S41、判断签名报文 DK 是否满足以下条件 :

$$[0110] \begin{cases} \beta > 0 \\ \omega < n \end{cases};$$

[0111] 若是, 则继续执行步骤 S42, 否则结束 ;

[0112] S42、根据下列公式计算 w :

$$[0113] \begin{cases} u = \omega^{-1} \bmod n \\ \mu_1 = (DK_s u) \bmod n \\ \mu_2 = (\beta u) \bmod n \\ \mu_1 G + \mu_2 EID_U = (x_0, y_0) \\ w = x_0 \bmod n \end{cases}$$

[0114] S43、判断 w 是否等于 β, 若是, 则验证通过, 继续执行步骤 S5, 否则结束。

[0115] 进一步作为优选的实施方式, 所述步骤 S6, 包括 :

[0116] S61、云服务端选取第二随机数 R<sub>c</sub> 作为该注册用户交互认证的主密钥 S' 后, 采用下式结合注册数据 M<sub>reg</sub> 中的系统参数 T 生成第一加密参数 RU<sub>pub</sub> :RU<sub>pub</sub>=R<sub>c</sub> • G ;

[0117] S62、将第一公钥 EID<sub>U</sub> 映射到椭圆曲线 E(F<sub>p</sub>) 上的一个点 EID<sub>p</sub> 后, 根据下式计算得到第二私钥 RU<sub>PE</sub> :RU<sub>PE</sub>=R<sub>c</sub> • EID<sub>p</sub> ;

[0118] S63、云服务端产生一个用于对该注册用户进行身份标识的标识码 λ, 然后根据下式对第一加密参数 RU<sub>pub</sub> 和标识码 λ 进行哈希散列运算后, 获得摘要信息 D :

[0119] D=Hash (RU<sub>pub</sub>, λ) 。

[0120] 进一步作为优选的实施方式, 所述步骤 S7, 包括 :

[0121] S71、根据下式采用第一加密参数 RU<sub>pub</sub> 和第二私钥 RU<sub>PE</sub> 对摘要信息 D 进行加密后得到第二摘要密文 DS :

[0122]  $DS=EC(D, r, RU_{pub}, RU_{pE})$

[0123] 其中,  $r=H_1(\sigma, D)$ , 而  $\sigma$  为第一随机串;

[0124] S72、根据下式采用第一公钥  $EID_U$  对第二摘要密文  $DS$ 、第一加密参数  $RU_{pub}$  和标识码  $\lambda$  进行加密后, 得到加密密文  $FS$  后, 并将加密密文  $FS$  发送到用户端:

[0125]  $FS=EC(DS, RU_{pub}, \lambda, EID_U, R, P_{pub})$

[0126] 其中,  $R=H_1(\pi, DS, RU_{pub}, \lambda)$ ,  $\pi$  为第二随机串,  $P_{pub}$  为系统参数  $T$  中的第二加密参数。

[0127] 进一步作为优选的实施方式, 所述步骤  $S8$ , 包括:

[0128]  $S81$ 、用户端接收加密密文  $FS$  后, 根据下式采用第一私钥  $d_{eid}$  对加密密文  $FS$  进行解密, 还原得到第二摘要密文  $DS$ 、第一加密参数  $RU_{pub}$  和标识码  $\lambda$ :  
 $(DS, RU_{pub}, \lambda)=DC(P_{pub}, d_{eid}, FS)$ ;

[0129]  $S82$ 、根据下式采用第一加密参数  $RU_{pub}$  和第一公钥  $EID_U$  对第二摘要密文  $DS$  进行解密后, 得到摘要信息  $D$ :  $D=DC(RU_{pub}, DS, EID_U)$ 。

[0130] 本发明的一具体实施例如下:

[0131] 一种云计算环境下的基于类  $IBE$  系统的身份认证方法, 包括:

[0132]  $S1$ 、用户端获取注册用户的身份信息  $M_{id}$  以及口令密码  $password$ , 并对口令密码进行哈希散列运算后, 获得散列口令密码  $Pwd$ ;  $Pwd=Hash(password)$ 。

[0133]  $S2$ 、用户端进行系统参数初始化, 得到注册用户主密钥  $S$  以及系统参数  $T$ , 进而生成第一公钥  $EID_U$  和第一私钥  $d_{eid}$ :

[0134]  $S21$ 、获取一个特征为素数  $p$  的有限域  $F_p$ , 并在有限域  $F_p$  上选取域元素  $a, b$ , 使域元素  $a, b$  满足椭圆曲线  $E(F_p)$  的方程:

[0135]  $y^3 = x^2 + a \cdot x + b \pmod{p}$ , 其中  $4 \cdot a^3 + 27 \cdot b^2 \neq 0 \pmod{p}$ ;

[0136]  $S22$ 、在椭圆曲线  $E(F_p)$  上选取一个基点  $G$ , 并计算得到基点  $G$  的阶  $q$ , 进而分别计算得到  $G$  点的两个  $q$  阶群  $G_1$  及  $G_2$ ,  $G_1$  及  $G_2$  满足以下双线性映射条件:

[0137]  $G_1 \times G_1 \rightarrow G_2$ ;

[0138]  $G$  点坐标为:  $G=(x_G, y_G)$ ;

[0139]  $S23$ 、采用下式计算椭圆曲线  $E(F_p)$  的阶  $\#E(F_p)$  除于基点  $G$  的阶  $q$  得到的商  $h$ :

[0140]  $h=\#E(F_p)/q$

[0141] 其中, 商  $h$  满足  $h \leq 4$ , 且  $\#E(F_p)$ 、 $p$ 、 $q$  满足以下条件:

$$[0142] \begin{cases} \#E(F_p) \neq p \\ \#p^t \neq 1 \pmod{q} \\ p = 2 \pmod{3} \\ p = 6q - 1 \end{cases}$$

[0143] 上式中  $t$  为常数, 且  $1 \leq t < 20$ ;

[0144] 公式  $p = 2 \pmod{3}$  表示  $p$  对  $3$  求模的结果等于  $2$ , 在椭圆曲线的相关运算中, 求模运算符是放在公式最后处, 本申请也采用这种形式, 例如, 前面公式  $4 \cdot a^3 + 27 \cdot b^2 \neq 0 \pmod{p}$  表示  $(4 \cdot a^3 + 27 \cdot b^2)$  的对  $p$  求模的结果不等于  $0$ ;

[0145]  $S24$ 、生成第一随机数  $S$  且满足  $S \in Z_q^*$ , 则  $S$  为注册用户的主密钥, 并计算第二加密

参数 : $P_{pub} = S \cdot G$ , 进而选取 4 个哈希函数  $H$ 、 $Q$ 、 $H_1$  及  $Q_1$  :

$$[0146] \quad H: F_p^2 \rightarrow \{0,1\}^n,$$

$$[0147] \quad Q: \{0,1\}^n \rightarrow F_p^2,$$

$$[0148] \quad H_1: \{0,1\}^n \times \{0,1\}^n \rightarrow F_q,$$

$$[0149] \quad Q_1: \{0,1\}^n \rightarrow \{0,1\}^n,$$

[0150] 其中,  $Z_q^*$  为随机数域,  $F_p^2$  是一个有限群且  $F_p^2 \in \{0,1\}^n$ ,  $n$  为自然数;

[0151] S25、根据下式可得到系统参数  $T$  为:

$$[0152] \quad T = (p, a, b, G, p_{pub}, q, h, H, Q, H_1, Q_1);$$

[0153] 同时可得到消息空间  $M$  为  $M = \{0,1\}^n$ , 密文空间  $C$  为  $C = G_1 \times \{0,1\}^n$ ;

[0154] 消息空间  $M$  以及密文空间  $C$  是验证过程中用户端需要用到的中间变量, 用于进行加解密运算, 这里不做详细描述;

[0155] S26、根据身份信息  $M_{id}$  生成第一公钥  $EID_U$ , 进而将第一公钥  $EID_U$  映射到椭圆曲线  $E(F_p)$  上的一个点  $E_p$ , 并计算得到第一公钥  $d_{eid}: d_{eid} = s \cdot E_p$ 。

[0156] 身份信息  $M_{id}$  包括注册用户的电子邮箱地址、身份证号、电话号码、手机号码、用户名等属性信息, 可直接在以上属性信息中选取一个作为第一公钥  $EID_U$ 。

[0157] S3、将注册用户的注册信息  $M_k$  进行哈希散列运算, 生成第一密文摘要  $DK_s$ , 进而结合系统参数  $T$  及第一私钥  $d_{eid}$  生成签名报文  $DK$  后, 将注册数据  $M_{reg}$ 、第一公钥  $EID_U$ 、第一密文摘要  $DK_s$  和签名报文  $DK$  发送到云服务端:

[0158] S31、根据下式将注册用户的注册信息  $M_k$  进行哈希散列运算, 生成第一密文摘要  $DK_s$  :

$$[0159] \quad DK_s = \text{Hash}(M_k \langle M_{id}, Pwd \rangle);$$

[0160] S32、选取一个整数  $k$ ,  $k$  满足条件:  $0 < k < n$ ;

[0161] S33、根据下式计算  $\beta$ , 若得到的结果为  $\beta = 0$ , 则返回步骤 S32, 反之执行步骤 S34:

$$[0162] \quad \begin{cases} kG = (x_1, y_1) \\ \beta = x_1 \bmod n; \end{cases}$$

[0163] S34、根据以下公式计算  $\omega$ , 若得到的结果为  $\omega = 0$ , 则返回步骤 S32, 反之执行步骤 S35:

$$[0164] \quad \begin{cases} K^* = k^{-1} \bmod n \\ \omega = K^* \{DK_s + d_{eid}\} \bmod n; \end{cases}$$

[0165] 上式中,  $K^*$  为计算过程中的中间变量。

[0166] S35、得到签名报文  $DK = (\beta, \omega)$ , 进而将注册数据  $M_{reg}$ 、第一公钥  $EID_U$ 、第一密文摘要  $DK_s$  和签名报文  $DK$  发送到云服务端。

[0167] S4、云服务端对签名报文  $DK$  进行验证, 若验证通过, 则继续执行步骤 S5, 否则结束:

[0168] S41、判断签名报文  $DK$  是否满足以下条件:

$$[0169] \quad \begin{cases} \beta > 0 \\ \omega < n \end{cases},$$

[0170] 若是,则继续执行步骤 S42,否则结束;

[0171] S42、根据下列公式计算  $w$  :

$$[0172] \quad \begin{cases} u = \omega^{-1} \bmod n \\ \mu_1 = (DK_s u) \bmod n \\ \mu_2 = (\beta u) \bmod n \\ \mu_1 G + \mu_2 EID_U = (x_0, y_0) \\ w = x_0 \bmod n \end{cases}$$

[0173] 上式中,  $u$ ,  $\mu_1$ ,  $\mu_2$  以及  $w$  均为计算过程的中间变量。

[0174] S43、判断  $w$  是否等于  $\beta$ ,若是,则验证通过,继续执行步骤 S5,否则结束。

[0175] 这里,云服务端首先对用户端发送的签名报文  $DK$  进行验证,若验证通过,则证明用户端发送的该签名报文  $DK$  等消息属于该注册用户,因此继续执行下一步骤。

[0176] S5、对接收到的注册信息  $M_k$  进行哈希散列运算后,验证得到的结果是否等于第一密文摘要  $DK_s$ ,若是,则继续执行步骤 S6,否则结束;这里,验证注册用户的注册信息  $M_k$  属实后,云服务端允许用户端的访问等操作,若验证注册用户的注册信息  $M_k$  不属实,则拒绝用户端的操作请求。

[0177] S6、云服务端根据注册数据  $M_{reg}$  生成第一加密参数  $RU_{pub}$  和第二私钥  $RU_{PE}$ ,并产生一个用于对该注册用户进行身份标识的标识码  $\lambda$ ,然后对第一加密参数  $RU_{pub}$  和标识码  $\lambda$  进行哈希散列运算后,获得摘要信息  $D$  :

[0178] S61、云服务端选取第二随机数  $R_c$  作为该注册用户交互认证的主密钥  $S'$  后,采用下式结合注册数据  $M_{reg}$  中的系统参数  $T$  生成第一加密参数  $RU_{pub}$  :  $RU_{pub} = R_c \cdot G$  ;

[0179] S62、将第一公钥  $EID_U$  映射到椭圆曲线  $E(F_p)$  上的一个点  $EID_p$  后,根据下式计算得到第二私钥  $RU_{PE}$  :  $RU_{PE} = R_c \cdot EID_p$  ;

[0180] S63、云服务端产生一个用于对该注册用户进行身份标识的标识码  $\lambda$ ,然后根据下式对第一加密参数  $RU_{pub}$  和标识码  $\lambda$  进行哈希散列运算后,获得摘要信息  $D$  :

[0181]  $D = \text{Hash}(RU_{pub}, \lambda)$ 。

[0182] 步骤 S4、S5 确保了对云服务端进行操作的客户端是合法的。而为了保证用户端不被非云服务端欺骗并进行相关操作,用户端还需对云服务端进行验证,如步骤 S7 ~ S9 所述。

[0183] S7、采用第一加密参数  $RU_{pub}$  和第二私钥  $RU_{PE}$  对摘要信息  $D$  进行加密后得到第二摘要密文  $DS$ ,进而采用第一公钥  $EID_U$  对第二摘要密文  $DS$ 、第一加密参数  $RU_{pub}$  和标识码  $\lambda$  进行加密后,得到加密密文  $FS$ ,并将加密密文  $FS$  发送到用户端:

[0184] S71、根据下式采用第一加密参数  $RU_{pub}$  和第二私钥  $RU_{PE}$  对摘要信息  $D$  进行加密后得到第二摘要密文  $DS$  :

[0185]  $DS = EC(D, r, RU_{pub}, RU_{PE})$

[0186] 其中,  $r = H_1(\sigma, D)$ ,而  $\sigma$  为第一随机串;

[0187] S72、根据下式采用第一公钥  $EID_U$  对第二摘要密文  $DS$ 、第一加密参数  $RU_{pub}$  和标识

码  $\lambda$  进行加密后,得到加密密文 FS 后,并将加密密文 FS 发送到用户端:

[0188]  $FS=EC(DS, RU_{pub}, \lambda, EID_U, R, P_{pub})$

[0189] 其中, R 为中间变量且  $R=H_1(\pi, DS, RU_{pub}, \lambda)$ ,  $\pi$  为第二随机串,  $P_{pub}$  为系统参数 T 中的第二加密参数,同样的, EC 代表进行加密运算,可以采用目前常用的方法进行加密,这里不对加密运算的详细算法进行描述。

[0190] S8、用户端接收加密密文 FS 后,采用第一私钥  $d_{eid}$  对加密密文 FS 进行解密,还原得到第二摘要密文 DS、第一加密参数  $RU_{pub}$  和标识码  $\lambda$ ,然后采用第一加密参数  $RU_{pub}$  和第一公钥  $EID_U$  对第二摘要密文 DS 进行解密后,得到摘要信息 D:

[0191] S81、用户端接收加密密文 FS 后,根据下式采用第一私钥  $d_{eid}$  对加密密文 FS 进行解密,还原得到第二摘要密文 DS、第一加密参数  $RU_{pub}$  和标识码  $\lambda$ :  
 $(DS, RU_{pub}, \lambda)=DC(P_{pub}, d_{eid}, FS)$ ;

[0192] S82、根据下式采用第一加密参数  $RU_{pub}$  和第一公钥  $EID_U$  对第二摘要密文 DS 进行解密后,得到摘要信息 D: $D=DC(RU_{pub}, DS, EID_U)$ 。DC 代表进行解密运算,可以采用目前常用的方法进行解密,这里不对解密运算的详细算法进行描述。

[0193] S9、用户端对第一加密参数  $RU_{pub}$  和标识码  $\lambda$  进行哈希散列运算后,验证得到的结果  $Hash(RU_{pub}, \lambda)$  是否等于摘要信息 D,若是,则认证成功,则验证了云服务端的合法性,防止了云服务端身份仿冒。

[0194] 第一加密参数  $RU_{pub}$  和第二加密参数  $P_{pub}$  均为系统参数 T 中可应用在加密或解密过程中的参数。

[0195] 本申请中所述注册信息  $M_k$  包括身份信息  $M_{id}$  和散列口令密码 Pwd: $M_k=\langle M_{id}, Pwd \rangle$ ,所述注册数据  $M_{reg}$  包括身份信息  $M_{id}$ 、散列口令密码 Pwd 和系统参数 T: $M_{reg}=\langle M_{id}, Pwd, T \rangle$ 。

[0196] 本发明不需要 PKG 等第三方可信机构,采用用户端直接与云服务端进行通讯的方式进行身份认证,减小了身份认证给云计算过程带来的复杂性,降低了开销,避免了密钥托管、密钥分发等带来的安全问题。第一私钥  $d_{eid}$  主要用于身份认证和审核,仅供用户端登录云服务端时认证用,认证结束后,便不再利用第一私钥  $d_{eid}$  进行操作,不会造成用户端权限过大的问题。

[0197] 本发明在身份认证过程中采用了椭圆曲线,根据椭圆曲线的离散性特征,本身份认证方法可抵抗冒充攻击。而且,本发明在用户端认证与云服务端认证过程中采用了随机数,可以很好的防止重放攻击。同时,对用户端及云服务端利用了双向签名认证方式进行认证,用户签名时采用第一私钥  $d_{eid}$ ,对应地云服务端采用第一公钥  $EID_U$  进行验证,确保进行访问的用户端的合法性。当云服务端验证进行访问的用户端的合法性后,采用第一加密参数  $RU_{pub}$  和第二私钥  $RU_{pr}$  对用户端发送的信息进行签名,再利用用户端发送的第一公钥  $EID_U$  加密后发送到用户端进行认证,本方法实现了用户端与云服务端的双向安全认证,避免了由于单向认证造成的漏洞,提高了安全性。

[0198] 本方法在认证过程中利用了椭圆曲线,虽然椭圆曲线密码算法计算量相对较大,但是相对于其他公钥体制算法,在密钥长度相等的情况下,其安全性更高,因而在满足同样安全强度的条件下,本方法计算量反而更少。而且由于本方法未采用第三方可信机构,因而协议结构简单,不需要密钥协商、分发等操作,用户端和云服务端直接交互信息,减少了请求和响应的通信消耗,端到端的通信方式使得响应速度更快,网络带宽利用率更高。

[0199] 以上是对本发明的较佳实施进行了具体说明,但本发明创造并不限于所述实施例,熟悉本领域的技术人员在不违背本发明精神的前提下还可作出种种的等同变形或替换,这些等同的变型或替换均包含在本申请权利要求所限定的范围内。