(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 108551435 A
(43)申请公布日 2018.09.18

(21)申请号 201810198425.6

(22)申请日 2018.03.12

(71)申请人 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 罗喜伶 王震 周泽全

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)
G06F 21/62(2013.01)

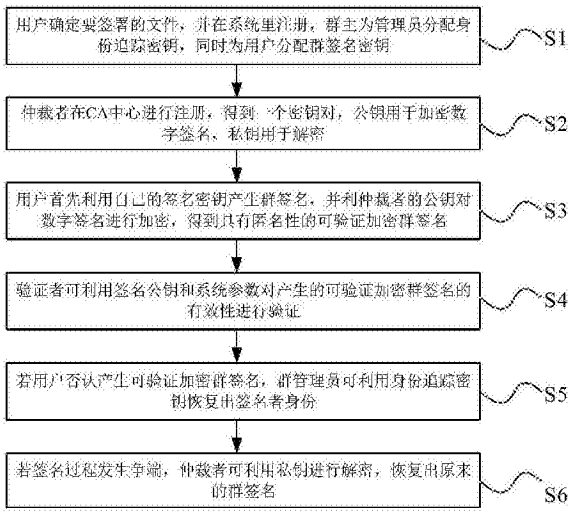
权利要求书1页 说明书5页 附图1页

(54)发明名称

一种具有匿名性的可验证加密群签名方法

(57)摘要

本发明涉及一种具有匿名性的可验证加密群签名方法，主要采用密码学技术手段保护用户在电子文件签约过程中的匿名性。在该方法中，当用户确定要进行文件签约时，其首先在系统中进行注册，得到签名密钥，然后利用签名密钥和仲裁者公钥产生可验证加密群签名。验证者在不解密的情况下可对签名有效性进行验证。群管理员可利用追踪密钥恢复出签名者身份，仲裁者可从可验证加密群签名中恢复出原签名。本发明提出的可验证加密群签名相比大多数签名方案，不仅实现了数字签名的保密性，还实现了签名者的匿名性。



CN 108551435 A

1.一种具有匿名性的可验证加密群签名方法,其特征在于,包括步骤:

S1:用户确认进行文件的签署后,在签名系统里利用身份信息进行注册,接收到注册信息后,群主将用户添加到系统用户所在的群体中,然后产生身份追踪密钥并将其发送给群管理员,同时利用用户身份信息计算用户的群签名密钥,将其发送给用户;

S2:仲裁者在CA(认证中心)中心进行注册,得到一个密钥对,包含一个公钥和一个私钥,公钥用于加密数字签名,私钥用于解密;

S3:用户首先利用自己的签名密钥产生关于文件的群签名,并利用仲裁者的公钥对群签名进行加密,得到具有匿名性的可验证加密群签名;

S4:验证者可利用签名公钥和系统参数在不解密的情况下对可验证加密群签名的有效性进行验证;

S5:若可验证加密群签名产生关于用户身份的纠纷或争端,如某用户否认产生了该签名,则群管理员可利用身份追踪密钥恢复出签名者的真实身份解决争端;

S6:若签名过程发生争端,如某一用户进行合同签署过程中发生欺诈行为,仲裁者可利用私钥解密出原来的群签名以保证合同签订过程的公平性。

2.如权利要求1所述的方法,其特征在于,该发明包含群主、群管理员、用户、验证者和仲裁者5个实体;

群主为群管理员分配身份追踪密钥,为用户分配签名密钥,当有新用户加入系统时,群主为新用户分配签名密钥,同时更新其他成员的签名密钥,当有用户离开时,群主撤销其权限,销毁签名密钥,同时更新其他成员的签名密钥;

群管理员负责追踪用户身份,可利用群追踪密钥从可验证加密群签名中恢复出用户身份;

用户利用签名密钥产生群签名,并利用仲裁者公钥对群签名进行加密,产生具有匿名性的可验证加密群签名;

验证者可在不解密的情况下验证可验证加密群签名的有效性;

仲裁者可利用私钥对可验证加密群签名进行解密,恢复出原来的群签名。

3.如权利要求1所述的方法,其特征在于,该方法采用群签名的方式实现签名者的匿名性,同时采用公钥加密技术对群签名进行加密,实现数字签名的保密性。

4.如权利要求1所述的方法,其特征在于,系统内的用户形成一个群体,群主为群内成员分配签名密钥,群管理员负责追踪用户身份,匿名性主要通过将签名用户的身份隐藏在合法的群体用户身份中而实现,在该群体中,签名用户可代表群体产生自己的群签名,但不能产生其他用户的群签名。

5.如权利要求1所述的方法,其特征在于,CA中心包含一个密钥产生器,为仲裁者分配一对密钥,公钥是公开的,群内成员可利用公钥对群签名进行加密,产生可验证加密群签名,私钥由仲裁者保存,用以解密可验证加密群签名。

6.如权利要求1所述的方法,其特征在于,可验证加密群签名和原群签名的有效性一致,即若可验证加密群签名有效,则原群签名也有效;若可验证加密群签名无效,则原群签名也无效。

一种具有匿名性的可验证加密群签名方法

技术领域

[0001] 本发明涉及信息安全和密码学技术领域，具体是一种具有匿名性的可验证加密群签名方法。

背景技术

[0002] 随着电子商务的飞速发展，电子合同签署、电子数据交换等新型电子商务型式层出不穷。由于互联网中也存在诸多不安全的因素，黑客攻击、信息泄露等事件时有发生，对社会、个人的隐私和利益造成极大的危害，因此安全性是实现电子商务中的前提。可验证加密签名作为一种独特的密码学技术手段，是一种实现安全电子合同签约的重要方式。

[0003] 可验证加密签名是对数字签名进行加密，同时保有数字签名性质的加密签名，验证者可以在不解密的情况下验证原始签名的有效性。当发生争端时，存在一个仲裁者，可以从加密的签名中恢复出原始签名，防止用户欺诈和抵赖。可验证加密签名避免了在电子合同签署或电子交易过程中数字签名的泄露，因此在一定程度上保证了数字签名的安全性。然而，目前大多数可验证加密签名方案未考虑签名者的身份隐私，这些方案虽然能够保证数字签名的安全性，但不能保证签名者的身份隐私安全，一旦电子合同签订过程中发生欺诈行为，用户身份信息可能会遭到泄露，对用户隐私造成极大的危害。

[0004] 因此，针对以上普通可验证加密签名方案的缺陷和不足，本发明提出一种具有匿名性的可验证加密群签名方法，采用可验证加密签名结合群签名的技术，在保证数字签名的安全性的前提下实现对签名者的身份隐私保护，提高了电子合同签署和电子交易过程中的安全性和隐私性。

发明内容

[0005] 本发明提出了一种具有匿名性的可验证加密群签名方法，采用可验证加密签名结合群签名的技术手段，旨在解决目前电子合同签署和电子交易过程中存在的用户身份隐私泄露等问题。

[0006] 一种具有匿名性的可验证加密群签名，包括以下步骤：

[0007] S1：用户确认进行文件的签署后，在签名系统里利用身份信息进行注册，接收到注册信息后，群主将用户添加到系统用户所在的群体中，然后产生身份追踪密钥并将其发送给群管理员，同时利用用户身份信息计算用户的群签名密钥，将其发送给用户；

[0008] S2：仲裁者在CA(认证中心)中心进行注册，得到一个密钥对，包含一个公钥和一个私钥，公钥用于加密数字签名，私钥用于解密；

[0009] S3：用户首先利用自己的签名密钥产生关于文件的群签名，并利用仲裁者的公钥对群签名进行加密，得到具有匿名性的可验证加密群签名；

[0010] S4：验证者可利用签名公钥和系统参数在不解密的情况下对可验证加密群签名的有效性进行验证；

[0011] S5：若可验证加密群签名产生关于用户身份的纠纷或争端，如某用户否认产生了

该签名，则群管理员可利用身份追踪密钥恢复出签名者的真实身份解决争端；

[0012] S6：若签名过程发生争端，如某一用户进行合同签署过程中发生欺诈行为，仲裁者可利用私钥解密出原来的群签名以保证合同签订过程的公平性。

[0013] 作为本发明的进一步补充，该发明包含群主、群管理员、用户、验证者和仲裁者5个实体：

[0014] 群主为群管理员分配身份追踪密钥，为用户分配签名密钥，当有新用户加入系统时，群主为新用户分配签名密钥，同时更新其他成员的签名密钥，当有用户离开时，群主撤销其权限，销毁签名密钥，同时更新其他成员的签名密钥；

[0015] 群管理员负责追踪用户身份，可利用群追踪密钥从可验证加密群签名中恢复出用户身份；

[0016] 用户利用签名密钥产生群签名，并利用仲裁者公钥对群签名进行加密，产生具有匿名性的可验证加密群签名；

[0017] 验证者可在不解密的情况下验证可验证加密群签名的有效性；

[0018] 仲裁者可利用私钥对可验证加密群签名进行解密，恢复出原来的群签名。

[0019] 作为本发明的进一步补充，该方法采用群签名的方式实现签名者的匿名性，同时采用公钥加密技术对群签名进行加密，实现数字签名的保密性。

[0020] 作为本发明的进一步补充，系统内的用户形成一个群体，群主为群内成员分配签名密钥，群管理员负责追踪用户身份，匿名性主要通过将签名用户的身份隐藏在合法的群体用户身份中实现，在该群体中，签名用户可代表群体产生自己的群签名，但不能产生其他用户的群签名。

[0021] 作为本发明的进一步补充，该发明产生的可验证加密群签名和群签名是基于身份密码体制的，即用户的签名密钥是关于用户的身份信息的，身份信息包括用户身份证号、手机号、邮箱、地址以及生物特征信息(指纹、虹膜)等。用户的签名密钥用于产生群签名和可验证加密群签名，而系统参数和公钥则用于群签名和可验证加密群签名的验证。

[0022] 作为本发明的进一步补充，CA中心包含一个密钥生成器，仲裁者在CA中心注册时，CA 中心为其产生一对密钥，私钥通过短信、邮件或其他私密信道发送给用户，而公钥则配有对应的数字证书，数字证书用于证明密钥的合法性。CA中心负责存储和维护仲裁者的公钥及数字证书，并在一定时间期限内更新仲裁者的公钥和对应的数字证书。而私钥由仲裁者保存，当发生争议或存在欺诈行为时，仲裁者可利用私钥对可验证加密群签名进行解密，得到原来的群签名。

[0023] 作为本发明的进一步补充，若验证者要对原群签名的有效性进行验证，验证者无需解密，只需对可验证加密群签名进行验证，若可验证加密群签名有效，则原群签名也有效；否则，原群签名无效。本发明无需解密就可验证原群签名的有效性，可保证数字签名的安全性。

[0024] 本发明提出的一种具有匿名性的可验证加密群签名方法，采用基于身份的群签名技术和公钥加密技术保证电子合同和电子交易过程中数字签名的安全性和用户身份的隐私性。本发明解决了大多数可验证加密签名方案中存在的缺乏用户匿名性保护的问题，既能够保护数字签名的安全性又能兼顾用户的匿名性，大大提升了电子合同签署和电子交易过程中的安全性，对电子商务的发展起到积极的作用。

附图说明

[0025] 附图1为本发明实例提供的一种具有匿名性的可验证加密群签名方法的流程图。

具体实施方式

[0026] 为使本发明实施例的目的、方案和效果更加清楚、明确，以下参考附图并举例对本发明进一步详细说明。

[0027] 附图为本发明提出的一种具有匿名性的可验证加密群签名方法流程图。如图1所示，本发明包含以下步骤：

[0028] S1：用户确认进行文件的签署后，在签名系统里利用身份信息进行注册，接收到注册信息后，群主将用户添加到系统用户所在的群体中，然后系统产生如下参数。设G和G_T为两个阶数为n＝pq有限循环群，其中p和q是两个大素数，G_p，G_q为G的p和q阶子群。e:G×G→G_T是一个双线性映射，g为随机选取的循环群G的生成元，h为随机选取的循环群G_q的生成元。设置用户身份追踪密钥为TK＝q，并将追踪密钥发送给群管理员。用户身份长度设为n_u，身份信息记为$u=(k_1^u k_2^u ... k_{n_u}^u)$，其中对于0＜i≤$n_u$，有$k_i^u \in \{0,1\}$。随机选择$n_u$维向量U＝($u_i$)，$n_m$维向量M＝($m_j$)以及元素u′，m′∈G，其中$u_i$，$m_j$为群G中的随机元素。设$Z_n$为n阶整数循环群，随机选择$\alpha_1 \in Z_n$，$g_2 \in G$，设置$g_1 = g^{\alpha_1}$。随机选择$r_u \in Z_n$，则用户的签名密钥为

[0029] $$d_u = (d_1, d_2, d_3) = \left(g_2^{\alpha_1} \left(u' \prod_{i=1}^{n_u} u_i^{k_i^u} \right)^{r_u}, g^{r_u}, h^{r_u} \right).$$

[0030] 其中d_1，d_2，d_3为用户签名密钥的三个组成部分。

[0031] S2：仲裁者在CA(认证中心)中心进行注册，CA中心包含一个密钥生成器，用于生成合同双方和第三方(仲裁者)的密钥对。设Z_n为n阶整数循环群，随机选择$\alpha_T \in Z_n$，则仲裁者的密钥对为$(SK_T, PK_T) = (\alpha_T, g^{\alpha_T})$，其中$PK_T$为公钥，用于加密数字签名，公钥配有CA中心颁发的数字证书，CA中心负责存储和维护仲裁者的公钥及数字证书，并在一定时间期限内更新仲裁者的公钥和对应的数字证书，SK_T为私钥，用于解密数字签名，私钥由仲裁者保存。

[0032] S3：在产生可验证加密群签名时，用户首先利用自己的签名密钥产生关于电子文件的群签名。而在产生群签名时，需先利用数字摘要算法产生n_m长度的电子文件的摘要$m=(k_1^m k_2^m ... k_{n_m}^m)$，其中对于0＜j≤$n_m$，有$m_j \in \{0,1\}$。然后系统随机选择$r_u', r_m, t_1, ..., t_{n_u} \in Z_n$，令$t = \sum_{i=1}^{n_u} t_i$，计算用户的群签名

[0033] $$\sigma_1 = g_2^{\alpha_1} \left(u' \prod_{i=1}^{n_u} u_i^{k_i^u} \right)^{r_u + r_u'} \left(m' \prod_{j=1}^{n_m} m_j^{k_j^m} \right)^{r_m} h^{(r_u + r_u')t}, \sigma_2 = g^{r_u + r_u'}, \sigma_3 = g^{r_m},$$

[0034] $$\sigma_4 = h^t, \sigma_5 = \sigma_2^t = g^{(r_u + r_u')t}, \quad c_i = u_i^{k_i^u} \cdot h^{t_i}, \pi_i = (u_i^{2k_i^u - 1} \cdot h^{t_i})^{t_i},$$

[0035] $$\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, c_1, ..., c_{n_u}, \pi_1, ..., \pi_{n_u})$$

[0036] 令$c = u' \prod_{i=1}^{n_u} c_i$，$M = m' \prod_{j=1}^{n_m} m_j^{k_j^m}$，有$\sigma_1 = g_2^{\alpha_1} c^{r_u + r_u'} M^{r_m}$，其中$\sigma_1$，$\sigma_2$，$\sigma_3$，$\sigma_4$，$\sigma_5$以及

$c_1,...,c_{n_u}$,$\pi_1,...,\pi_{n_u}$为群签名的组成部分。然后用户利用仲裁者的公钥PK_T对产生的群签名进行加密，随机选择$s\in Z_n$，再计算可验证加密群签名

[0037] $$\omega_1=(PK_T)^s\cdot\sigma_1=(PK_T)^s g_2^{\alpha_1}\left(u'\prod_{i=1}^{n_u}u_i^{k_i^u}\right)^{r_u+r_u'}\left(m'\prod_{j=1}^{n_m}m_j^{k_j^m}\right)^{r_m}h^{(r_u+r_u')t},$$

[0038] $$\omega_2=g^s,\omega_3=\sigma_2=g^{r_u+r_u'},\omega_4=\sigma_3=g^{r_m},\omega_5=\sigma_4=h^t,\omega_6=\sigma_5=g^{(r_u+r_u')t},$$

[0039] $$\omega=(\omega_1,\omega_2,\omega_3,\omega_4,\omega_5,\omega_6,c_1,...,c_{n_u},\pi_1,...,\pi_{n_u})$$

[0040] 其中ω_1，ω_2，ω_3，ω_4，ω_5，ω_6以及$c_1,...,c_{n_u}$，$\pi_1,...,\pi_{n_u}$为可验证加密群签名的组成部分。

[0041] S4：验证者可在不解密的情况下对可验证加密签名和原群签名的有效性进行验证。首先需要验证签名者的身份是否有效，若对于$\forall i=1,...,k$，都有：$e(c_i,u_i^{-1}c_i)=e(h,\pi_i)$，则签名者身份信息有效，否则签名者身份信息无效，其中e为双线性映射。若签名者身份信息有效，则验证下列公式是否成立。

[0042] $e(\omega_1,g)=e(PK_T,\omega_2)e(g_2,g_1)e(c,\omega_3)e(M,\omega_4)$，$e(\omega_3,\omega_5)=e(\omega_6,h)$

[0043]

[0044] 其中e为双线性映射，$c=u'\prod_{i=1}^{n_u}c_i$，$M=m'\prod_{j=1}^{n_m}m_j^{k_j^m}$。若以上公式都成立，则签名有效；否则，签名无效。

[0045] S5：若可验证加密群签名产生关于用户身份的纠纷或争端，如某用户否认产生了该签名，则群管理员可利用身份追踪密钥$TK=q$恢复出签名者的真实身份解决争端。对于$i=1,...,n_u$，若$(c_i)^q=g^0$，则令$k_i^u=0$，否则令$k_i^u=1$，最终得到$u=(k_1^u\cdots k_{n_u}^u)$，其中$k_i^u$为身份信息的第i 位，u为最终得到的签名者的身份信息。群管理员将最终得到的签名者的身份信息和群体中所有用户的身份信息做对比，即可追踪到真实签名者。

[0046] S6：若签名过程发生争端，如某一用户进行合同签署过程中发生欺诈行为，仲裁者可利用私钥SK_T解密出原来的群签名，仲裁者可按下列公式进行计算

[0047] $$\sigma_1=\frac{\omega_1}{\omega_2^{\alpha_T}}=g_2^{\alpha_1}\left(u'\prod_{i=1}^{n_u}u_i^{k_i^u}\right)^{r_u+r_u'}\left(m'\prod_{j=1}^{n_m}m_j^{k_j^m}\right)^{r_m}h^{(r_u+r_u')t},\sigma_2=\omega_3=g^{r_u+r_u'},$$

[0048] $$\sigma_3=\omega_4=g^{r_m},\sigma_4=\omega_5=h^t,\sigma_5=\omega_6=g^{(r_u+r_u')t},$$

[0049] $$\sigma=(\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5,c_1,...,c_{n_u},\pi_1,...,\pi_{n_u})$$

[0050] 最终得到原群签名σ，其中σ_1，σ_2，σ_3，σ_4，σ_5以及$c_1,...,c_{n_u}$，$\pi_1,...,\pi_{n_u}$为群签名的组成部分。最终仲裁者将其发送给仲裁申请方，保证电子合同签署的公平性。

[0051] 在以上的实施例中，所有计算均由可验证加密群签名系统完成，用户只需在相应平台上进行相应的操作，因此本发明具有良好的实用性。系统内的用户形成一个群体，群主为群内成员分配签名密钥，群管理员负责追踪用户身份，匿名性主要通过将签名用户的身份隐藏在合法的群体用户身份中而实现，在该群体中，签名用户可代表群体产生自己的群签名，但不能产生其他用户的群签名。

[0052] 在整个产生可验证加密群签名和验证的过程中，签名者的身份是受到保护的，只

有在签名用户试图进行恶意行为时，群管理员才会揭示恶意签名者的真实身份，因此本发明能够为诚实用户提供匿名性和安全性。

[0053] 以上内容是结合具体实施方式对本发明的进一步详细说明，显然，所描述的实施例是本发明的一部分实例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

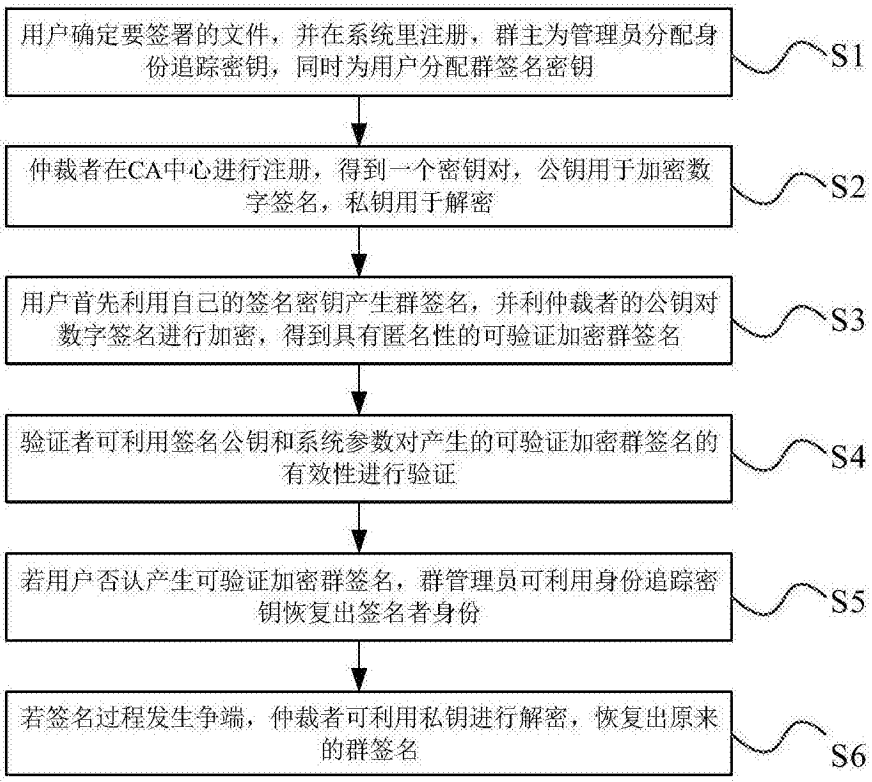

用户确定要签署的文件，并在系统里注册，群主为管理员分配身份追踪密钥，同时为用户分配群签名密钥
S1
仲裁者在CA中心进行注册，得到一个密钥对，公钥用于加密数字签名，私钥用于解密
S2
用户首先利用自己的签名密钥产生群签名，并利仲裁者的公钥对数字签名进行加密，得到具有匿名性的可验证加密群签名
S3
验证者可利用签名公钥和系统参数对产生的可验证加密群签名的有效性进行验证
S4
若用户否认产生可验证加密群签名，群管理员可利用身份追踪密钥恢复出签名者身份
S5
若签名过程发生争端，仲裁者可利用私钥进行解密，恢复出原来的群签名
S6

图1