(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 107733648 A
(43)申请公布日 2018.02.23

(21)申请号 201711042009.9

(22)申请日 2017.10.30

(71)申请人 武汉大学
地址 430072 湖北省武汉市武昌区珞珈山武汉大学

(72)发明人 何德彪 冯琦 孙金龙

(74)专利代理机构 武汉科皓知识产权代理事务所(特殊普通合伙) 42222
代理人 鲁力

(51)Int.Cl.
H04L 9/30(2006.01)
H04L 9/08(2006.01)
H04L 9/00(2006.01)
H04L 9/32(2006.01)

权利要求书3页 说明书6页

(54)发明名称

一种基于身份的RSA数字签名生成方法及系统

(57)摘要

本发明涉及一种基于身份的RSA数字签名生成方法及系统，具体是：密钥生成中心生成一对RSA的公私钥对，以及一对随机数。将部分签名密钥发送P_1，另一部分签名密钥送给P_2。参于数字签名生成的双方P_1和P_2，分别生成一个随机数r_1和r_2。P_1首先计算r_1，加密r_1得到C_1，随后发送C_1和R_1给P_2。P_2计算r_2返回给P_1。同时P_2计算出密文C_2。P_2将此密文C_2发送给P_1。P_1解密C_2，并利用自己的部分签名密钥$D_{ID}^{(1)}$计算得到签名S和R，在签名验证通过之后，P_1公布完整的基于身份的RSA数字签名(R,S)。本发明保证了签名密钥的安全性，提高了双方参与数字签名的公平性。

CN 107733648 A

1.一种基于身份的两方分布式RSA数字签名生成方法，其特征在于，基于以下定义：公私钥对(e,d)、需要签名的两方P_1和P_2，具体包括：

密钥分发步骤：密钥生成中心首先一对RSA的公私钥对(e,d)，以及满足$d_1 d_2 \equiv d \bmod \varphi(n)$的$d_1$和$d_2$；由$d_1$和$d_2$计算得到满足$(D_{ID}^{(1)})^{D_{ID}^{(2)}} = H(ID)^d \bmod n$的两个部分签名密钥$D_{ID}^{(1)}$和$D_{ID}^{(2)}$，其中H(ID)是基于用户身份生成的哈希值；随后基于同态加密算法生成公私钥对(pk,sk)；将$(e, D_{ID}^{(1)}, pk, sk)$发送给一方$P_1$，将$(e, D_{ID}^{(2)}, pk)$发送给另一方$P_2$；

数字签名生成步骤：P_1和P_2分别生成一个随机数r_1和r_2；P_1首先计算$R_1 = H(ID)^{r_1}$，使用同态加密方法加密r_1得到C_1，随后发送C_1和R_1给P_2；P_2计算$R_2 = H(ID)^{r_2}$返回给P_1；同时P_2通过同态加密的性质，可以计算出$(r_1 r_2 + \alpha) D_{ID}^{(2)}$的密文$C_2$，其中α是基于用户身份，待签名消息以及随机数生成的哈希值；P_2将此密文C_2发送给P_1；P_1解密C_2，并利用自己的部分签名密钥$D_{ID}^{(1)}$计算得到签名$S = H(ID)^{(r_1 r_2 + \alpha)d}$和$R = H(ID)^{r_1 r_2}$，在签名验证通过之后，$P_1$公布完整的基于身份的RSA数字签名(R,S)。

2.根据权利要求1所述的一种基于身份的两方分布式RSA数字签名生成方法，其特征在于，所述密钥分发步骤具体包括：

步骤2.1、产生两个固定长度的大素数p，q，计算模数n＝pq，欧拉函数$\varphi(n) = (p-1)(q-1)$；

步骤2.2、生成一对RSA的公私钥对(e,d)，满足$\gcd(e, \varphi(n)) = 1$并且$ed \equiv 1 \bmod \varphi(n)$，其中e是公钥，d是私钥；

步骤2.3、生成一个随机数d_2，计算d_1使得等式$d_1 d_2 \equiv d \bmod \varphi(n)$成立；

步骤2.4、计算第一部分签名密钥$D_{ID}^{(1)} = H(ID)^{d_1} \bmod n$，第二部分签名密钥$D_{ID}^{(2)} = d_2$；其中H(ID)表示身份ID的哈希值；

步骤2.5、生成同态加密算法的一对公私钥对(pk,sk)；将$(e, D_{ID}^{(1)}, pk, sk)$发送给第一参与方$P_1$，将$(e, D_{ID}^{(2)}, pk)$发送给第二参与方$P_2$。

3.根据权利要求1所述的一种基于身份的两方分布式RSA数字签名生成方法，其特征在于，所述数字签名生成步骤包括：

步骤3.1、P_1生成第一个随机数r_1，计算第一个临时公钥$R_1 = H(ID)^{r_1}$，使用同态加密算法的公钥pk对r_1做加密，即第一个密文$C_1 = Enc_{pk}(r_1)$；P_1把(R_1, C_1)发送给P_2；

步骤3.2、P_2生成第二个随机数r_2，计算第二个临时公钥$R_2 = H(ID)^{r_2}$，第一部分签名$R = R_1^{r_2} = H(ID)^{r_1 r_2}$，第二个密文$C_2 = \left((C_1 \odot r2) \oplus Encpk\alpha \odot DID2 = Encpk((r1r2+\alpha)DID(2)\right)$，其中α是身份ID，消息M和R一起做Hash操作得到的值，即α＝H(ID,M,R)；P_2把(R_2, C_2)发送给P_1；

步骤3.3、P_1使用同态加密算法的私钥做解密，计算明文$\sigma = Dec_{sk}(C_2) = (r_1r_2 + \alpha)D_{ID}^{(2)}$，第一部签名$R = R_2^{r_1} = H(ID)^{r_1r_2}$和第二部分签名$S = (D_{ID}^{(1)})^{\sigma} \bmod n$;使用签名验证算法验证签名的正确性，若签名正确则输出签名(R,S)，否则终止协议。

4.一种基于身份的两方分布式RSA数字签名生成系统，其特征在于，基于以下定义：公私钥对(e,d)、需要签名的两方P_1和P_2，具体包括：

密钥生成中心：用于生成一对RSA的公私钥对(e,d)，以及满足$d_1d_2 \equiv d \bmod \varphi(n)$的$d_1$和$d_2$，由$d_1$和$d_2$计算得到满足$(D_{ID}^{(1)})^{D_{ID}^{(2)}} = H(ID)^d \bmod n$的两个部分签名密钥$D_{ID}^{(1)}$和$D_{ID}^{(2)}$，其中H(ID)是基于用户身份生成的哈希值；

密钥分发单元：基于同态加密算法生成公私钥对(pk,sk)；将$(e, D_{ID}^{(1)}, pk, sk)$发送给一方$P_1$，将$(e, D_{ID}^{(2)}, pk)$发送给另一方$P_2$；

数字签名生成单元：P_1和P_2分别生成一个随机数r_1和r_2；P_1首先计算$R_1 = H(ID)^{r_1}$，使用同态加密方法加密r_1得到C_1，随后发送C_1和R_1给P_2；P_2计算$R_2 = H(ID)^{r_2}$返回给P_1；同时P_2通过同态加密的性质，可以计算出$(r_1r_2 + \alpha)D_{ID}^{(2)}$的密文$C_2$，其中α是基于用户身份，待签名消息以及随机数生成的哈希值；P_2将此密文C_2发送给P_1；P_1解密C_2，并利用自己的部分签名密钥$D_{ID}^{(1)}$计算得到签名$S = H(ID)^{(r_1r_2+\alpha)d}$和$R = H(ID)^{r_1r_2}$，在签名验证通过之后，$P_1$公布完整的基于身份的RSA数字签名(R,S)。

5.根据权利要求4所述的一种基于身份的两方分布式RSA数字签名生成系统，其特征在于，所述密钥分发单元的具体分发方法包括：

步骤5.1、产生两个固定长度的大素数p，q，计算模数$n = pq$，欧拉函数$\varphi(n) = (p-1)(q-1)$；

步骤5.2、生成一对RSA的公私钥对(e,d)，满足$\gcd(e, \varphi(n)) = 1$并且$ed \equiv 1 \bmod \varphi(n)$，其中e是公钥，d是私钥；

步骤5.3、生成一个随机数d_2，计算d_1使得等式$d_1d_2 \equiv d \bmod \varphi(n)$成立；

步骤5.4、计算第一部分签名密钥$D_{ID}^{(1)} = H(ID)^{d_1} \bmod n$，第二部分签名密钥$D_{ID}^{(2)} = d_2$；其中H(ID)表示身份ID的哈希值；

步骤2.5、生成同态加密算法的一对公私钥对(pk,sk)；将$(e, D_{ID}^{(1)}, pk, sk)$发送给第一参与方$P_1$，将$(e, D_{ID}^{(2)}, pk)$发送给第二参与方$P_2$。

6.根据权利要求4所述的一种基于身份的两方分布式RSA数字签名生成系统，其特征在于，所述数字签名生成单元进行数字签名的具体步骤包括：

步骤6.1、P_1生成第一个随机数r_1，计算第一个临时公钥$R_1 = H(ID)^{r_1}$，使用同态加密算法的公钥pk对r_1做加密，即第一个密文$C_1 = Enc_{pk}(r_1)$；P_1把(R_1, C_1)发送给P_2；

步骤6.2、P_2生成第二个随机数r_2，计算第二个临时公钥$R_2 = H(ID)^{r_2}$，第一部分签名$R = R_1^{r_2} = H(ID)^{r_1 r_2}$，第二个密文$C_2 = ((C_1 \odot r2) \oplus Encpk(\alpha) \odot DID2 = Encpk((r1r2+\alpha)DID(2))$，其中α是身份ID，消息M和R一起做Hash操作得到的值，即α＝H(ID,M,R)；P_2把(R_2, C_2)发送给P_1；

步骤6.3、P_1使用同态加密算法的私钥做解密，计算明文$\sigma = Dec_{sk}(C_2) = (r_1 r_2 + \alpha) D_{ID}^{(2)}$，第一部签名$R = R_2^{r_1} = H(ID)^{r_1 r_2}$和第二部分签名$S = (D_{ID}^{(1)})^{\sigma} \bmod n$；使用签名验证算法验证签名的正确性，若签名正确则输出签名(R,S)，否则终止协议。

一种基于身份的RSA数字签名生成方法及系统

技术领域

[0001] 本发明属于信息安全领域，特别是基于身份的RSA数字签名生成方法及系统。

背景技术

[0002] 数字签名是数字化环境下对传统手写签名的模拟，可以提供数字信息的不可伪造性、认证性和完整性。数字签名涉及两种密钥：签名密钥和验证公钥。关于验证公钥的安全性和不可替代性，传统的解决办法是使用公钥基础设施，即通过可信机构签发数字证书来对用户的公钥和身份进行捆绑。为了解决这种方法中存在证书管理困难问题，科研人员提出了基于身份的数字签名。在这种签名中，密钥生成中心使用用户身份生成公私钥对，可以在验证数字签名的过程中同时确认用户身份。

[0003] 随着互联网的发展，许多事务在网络上开展，如电子商务、电子证券等。这些电子事务的完成通常涉及多个参与方，需要多个参与者同时对相关消息进行签名，其安全性和参与者的公平性需求催生了多种数字签名体制。一般情况下，用户会使用秘密共享的思想来共同生成数字签名。在这种方法中，签名密钥被分割成t个子密钥，并安全地分给t个参与者掌管，这些参与者中的k个及以上所构成的子集可以重构签名密钥，少于k个参与者则无法获得任何关于完整签名密钥的信息。但是当恢复出完整签名密钥之后，持有完整签名密钥的一方就可以在其他参与方不知情的情况下独立地进行签名，威胁了安全性和公平性。特别是在只有两个参与方的情况下，某一方恢复并持有完整签名密钥，就可以在另一方不知情的情况下，独立地进行数字签名，这在电子货币系统中会造成直接的利益损失。

[0004] 第一个基于身份的RSA数字签名方案由Shamir提出(参见《Identity-based Cryptosystems and Signature Schemes》Crypto.1984,84:47-53)，此算法中，用户的验证公钥由用户身份计算而来，用户的签名密钥则由可信机构生成。基于秘密共享的实现方法对签名密钥的保护较弱，存在密钥泄露的隐患。

[0005] 针对这种情况，本发明设计了一种基于身份的两方分布式RSA数字签名方案，可以实现在两个参与方之间分布式的完成数字签名，数字签名必须由两方共同参与，并且在签名过程中没有恢复完整的签名密钥，保证签名密钥的安全性。

发明内容

[0006] 本发明的目的在于提出两方在不泄露自己的部分签名密钥，并且无法获得完整的签名密钥的情况下共同完成对消息的基于身份的RSA数字签名。

[0007] 针对本发明的目的，本发明提出了一种基于身份的两方分布式RSA数字签名生成方案，下面给出具体描述。

[0008] 一种基于身份的两方分布式RSA数字签名生成方法，其特征在于，基于以下定义：公私钥对(e,d)、需要签名的两方P_1和P_2，具体包括：

[0009] 密钥分发步骤：密钥生成中心首先生成一对RSA的公私钥对(e,d)，以及满足$d_1 d_2 \equiv d \bmod \varphi(n)$的$d_1$和$d_2$；由$d_1$和$d_2$计算得到满足$(D_{ID}^{(1)})^{D_{ID}^{(2)}} = H(ID)^d \bmod n$的两

个部分签名密钥$D_{ID}^{(1)}$和$D_{ID}^{(2)}$，其中H(ID)是基于用户身份生成的哈希值；随后基于同态加密算法生成公私钥对(pk，sk)；将$(e, D_{ID}^{(1)}, pk, sk)$发送给一方$P_1$，将$(e, D_{ID}^{(2)}, pk)$发送给另一方$P_2$；

[0010] 数字签名生成步骤：P_1和P_2分别生成一个随机数r_1和r_2。P_1首先计算$R_1 = H(ID)^{r_1}$，使用同态加密方法加密r_1得到C_1，随后发送C_1和R_1给P_2。P_2计算$R_2 = H(ID)^{r_2}$返回给P_1。同时P_2通过同态加密的性质，可以计算出$(r_1 r_2 + \alpha)D_{ID}^{(2)}$的密文$C_2$，其中α是基于用户身份，待签名消息以及随机数生成的哈希值。P_2将此密文C_2发送给P_1。P_1解密C_2，并利用自己的部分签名密钥$D_{ID}^{(1)}$计算得到签名$S=H(ID)^{(r1r2+\alpha)d} \bmod n$和$R = H(ID)^{r_1 r_2}$，在签名验证通过之后，$P_1$公布完整的基于身份的RSA数字签名(R，S)。

[0011] 在上述的一种基于身份的两方分布式RSA数字签名生成方法，所述密钥分发步骤具体包括：

[0012] 步骤2.1、产生两个固定长度的大素数p，q，计算模数$n=pq$，欧拉函数$\varphi(n) = (p-1)(q-1)$。

[0013] 步骤2.2、生成一对RSA的公私钥对(e，d)，满足$\gcd(e, \varphi(n)) = 1$并且$ed \equiv 1 \bmod \varphi(n)$，其中e是公钥，d是私钥；

[0014] 步骤2.3、生成一个随机数d_2，计算d_1使得等式$d_1 d_2 \equiv d \bmod \varphi(n)$成立；

[0015] 步骤2.4、计算第一部分签名密钥$D_{ID}^{(1)} = H(ID)^{d_1} \bmod n$，第二部分签名密钥$D_{ID}^{(2)} = d_2$；其中H(ID)表示身份ID的哈希值；

[0016] 步骤2.5、生成同态加密算法的一对公私钥对(pk，sk)；将$(e, D_{ID}^{(1)}, pk, sk)$发送给第一参与方$P_1$，将$(e, D_{ID}^{(2)}, pk)$发送给第二参与方$P_2$。

[0017] 在上述的一种基于身份的两方分布式RSA数字签名生成方法，所述数字签名生成步骤包括：

[0018] 步骤3.1、P_1生成第一个随机数r_1，计算第一个临时公钥$R_1 = H(ID)^{r_1}$，使用同态加密算法的公钥pk对r_1做加密，即第一个密文$C_1=Enc_{pk}(r_1)$。P_1把(R_1, C_1)发送给P_2。

[0019] 步骤3.2、P_2生成第二个随机数r_2，计算第二个临时公钥$R_2 = H(ID)^{r_2}$，第一部分签名$R = R_1^{r_2} = H(ID)^{r_1 r_2}$，第二个密文$C_2 = \left((C_1 \odot r_2) \oplus Enc_{pk}(\alpha)\right) \odot D_{ID}^{(2)} = Enc_{pk}((r_1 r_2 + \alpha)D_{ID}^{(2)})$，其中α是身份ID，消息M和R一起做Hash操作得到的值，即$\alpha=H(ID,M,R)$。P_2把(R_2, C_2)发送给P_1。

[0020] 步骤3.3、P_1使用同态加密算法的私钥做解密，计算明文$\sigma = Dec_{sk}(C_2) = (r_1 r_2 + \alpha)D_{ID}^{(2)}$，第一部签名$R = R_2^{r_1} = H(ID)^{r_1 r_2}$和第二部分签名$S = (D_{ID}^{(1)})^{\sigma} \bmod n$。使用签名验证算法验证签名的正确性，若签名正确则输出签名(R，S)，否则终止协议。

[0021] 一种基于身份的两方分布式RSA数字签名生成系统，其特征在于，基于以下定义：公私钥对(e,d)、需要签名的两方P_1和P_2，具体包括：

[0022] 密钥生成中心：用于一对RSA的公私钥对(e,d)，以及满足$d_1 d_2 \equiv d \bmod \varphi(n)$的$d_1$和$d_2$，由$d_1$和$d_2$计算得到满足$(D_{ID}^{(1)})^{D_{ID}^{(2)}} = H(ID)^d \bmod n$的两个部分签名密钥$D_{ID}^{(1)}$和$D_{ID}^{(2)}$，其中H(ID)是基于用户身份生成的哈希值；

[0023] 密钥分发单元：基于同态加密算法生成公私钥对(pk,sk)；将$(e, D_{ID}^{(1)}, pk, sk)$发送给一方$P_1$，将$(e, D_{ID}^{(2)}, pk)$发送给另一方$P_2$；

[0024] 数字签名生成单元：P_1和P_2分别生成一个随机数r_1和r_2。P_1首先计算$R_1 = H(ID)^{r_1}$，使用同态加密方法加密r_1得到C_1，随后发送C_1和R_1给P_2。P_2计算$R_2 = H(ID)^{r_2}$返回给P_1。同时P_2通过同态加密的性质，可以计算出$(r_1 r_2 + \alpha) D_{ID}^{(2)}$的密文$C_2$，其中α是基于用户身份，待签名消息以及随机数生成的哈希值。P_2将此密文C_2发送给P_1。P_1解密C_2，并利用自己的部分签名密钥$D_{ID}^{(1)}$计算得到签名$S = H(ID)^{(r1r2+\alpha)d}$和$R = H(ID)^{r_1 r_2}$，在签名验证通过之后，$P_1$公布完整的基于身份的RSA数字签名(R,S)。

[0025] 在上述的一种基于身份的两方分布式RSA数字签名生成系统，所述密钥分发单元的具体分发方法包括：

[0026] 步骤5.1、产生两个固定长度的大素数p，q，计算模数$n = pq$，欧拉函数$\varphi(n) = (p-1)(q-1)$。

[0027] 步骤5.2、生成一对RSA的公私钥对(e，d)，满足$\gcd(e, \varphi(n)) = 1$并且$ed \equiv 1 \bmod \varphi(n)$，其中e是公钥，d是私钥；

[0028] 步骤5.3、生成一个随机数d_2，计算d_1使得等式$d_1 d_2 \equiv d \bmod \varphi(n)$成立；

[0029] 步骤5.4、计算第一部分签名密钥$D_{ID}^{(1)} = H(ID)^{d_1} \bmod n$，第二部分签名密钥$D_{ID}^{(2)} = d_2$；其中H(ID)表示身份ID的哈希值；

[0030] 步骤2.5、生成同态加密算法的一对公私钥对(pk,sk)；将$(e, D_{ID}^{(1)}, pk, sk)$发送给第一参与方$P_1$，将$(e, D_{ID}^{(2)}, pk)$发送给第二参与方$P_2$。

[0031] 在上述的一种基于身份的两方分布式RSA数字签名生成系统，所述数字签名生成单元进行数字签名的具体步骤包括：

[0032] 步骤6.1、P_1生成第一个随机数r_1，计算第一个临时公钥$R_1 = H(ID)^{r_1}$，使用同态加密算法的公钥pk对r_1做加密，即第一个密文$C_1 = Enc_{pk}(r_1)$。P_1把(R_1, C_1)发送给P_2。

[0033] 步骤6.2、P_2生成第二个随机数r_2，计算第二个临时公钥$R_2 = H(ID)^{r_2}$，第一部分签名$R = R_1^{r_2} = H(ID)^{r_1 r_2}$，第二个密文$C_2 = ((C_1 \odot r_2) \oplus Enc_{pk}(\alpha)) \odot D_{ID}^{(2)} = Enc_{pk}((r_1 r_2 + \alpha) D_{ID}^{(2)})$，其中α是身份ID，消息M和R一起做Hash操作得到的值，即$\alpha = H(ID, M, R)$。P_2把$(R_2,$

C_2)发送给P_1。

[0034] 步骤6.3、P_1使用同态加密算法的私钥做解密，计算明文$\sigma = Dec_{sk}(C_2) = (r_1r_2 + \alpha)D_{ID}^{(2)}$，第一部签名$R = R_2^{r_1} = H(ID)^{r_1r_2}$和第二部分签名$S = (D_{ID}^{(1)})^{\sigma} \bmod n$。使用签名验证算法验证签名的正确性，若签名正确则输出签名(R,S)，否则终止协议。

[0035] 本发明与现有技术相比具有如下有益效果：1、关于签名密钥的安全性，目前现有的门限秘密共享方案，虽然可以将签名密钥进行分割，但在签名阶段，密钥会被恢复并被某一方掌握，造成了签名密钥的泄露，这样降低了多方签名的安全性。2、关于签名的公平性，目前现有的门限秘密共享方案，最终持有完整签名密钥的一方可以独立进行签名，不需要全部参与方共同参加，这样降低了多方签名的公平性。3、本发明实现了基于身份的分布式RSA数字签名，签名过程中保证双方不会暴露部分签名密钥，同时数字签名必须由双方同时参与，这样实现了多方签名的安全性和公平性。4、本发明基于数学难题，保证即使有一方的签名密钥丢失，也不会泄露关于完整签名密钥或另外一方持有的部分签名密钥的任何信息。

具体实施方式

[0036] 下面结合实例对本发明做详细的描述，以下实施方案只表示本发明是一种可能的实施方式，不是全部可能的实施方案，不作为对本发明的限定。

[0037] 一、首先阐述本发明的方法原理。

[0038] 密钥生成中心生成一对RSA的公私钥对(e，d)，以及一对随机数满足$d_1d_2 \equiv d \bmod \varphi(n)$。将部分签名密钥$D_{ID}^{(1)} = H(ID)^{d_1} \bmod n$发送$P_1$，$D_{ID}^{(2)} = d_2$发送给$P_2$，其中H(ID)是基于用户身份生成的哈希值。同时选择并生成一组同态加密算法的公私钥对(pk，sk)，并将(pk，sk)发送给P_1，pk发送给P_2。参加数字签名生成的双方P_1和P_2，分别生成一个随机数r_1和r_2。P_1首先计算$R_1 = H(ID)^{r_1}$，使用同态加密方法加密r_1得到C_1，随后发送C_1和R_1给P_2。P_2计算$R_2 = H(ID)^{r_2}$返回给P_1。同时P_2通过同态加密的性质，可以计算出$(r_1r_2 + \alpha)D_{ID}^{(2)}$的密文$C_2$，其中α是基于用户身份，待签名消息以及随机数生成的哈希值。P_2将此密文C_2发送给P_1。P_1解密C_2，并利用自己的部分签名密钥$D_{ID}^{(1)}$计算得到签名S＝H(ID)$^{(r1r2+\alpha)d}$和$R = H(ID)^{r_1r_2}$，在签名验证通过之后，P_1公布完整的基于身份的RSA数字签名(R,S)。

[0039] 在以下对本发明的描述中，两个整数相乘(或整数符号相乘)，在不产生二义性的情况下，省略乘号“·”，例如a·b简化为ab。mod n表示模n运算，模n运算的优先级是最低的，例如a+bmod n等同于(a+b)mod n，ab mod n等同于(ab)mod n。“≡”表示同余式，即a≡bmod n等同于amod n＝b mod n。gcd(a,b)表示求整数a，b的最大公因子，若gcd(a,b)＝1代表a，b互素。

[0040] 在以下对本发明签名阶段的描述中，P_1使用同态加密算法对消息做加密，使用的公私钥对为(pk，sk)。定义Enc_{pk}为加密运算，Dec_{sk}为解密运算。定义$c_1 \oplus c_2$为c_1，c_2两个密文的“同态加”运算，定义$a \odot c$运算为密文c与明文a的“同态乘”运算。该同态加密算法有如

下性质：

[0041] 1.公钥pk做消息加密，只有唯一对应的私钥sk才可以解密，即$DeC_{sk}(Enc_{pk}(m))=m$；

[0042] 2.密文之间的相乘运算可以映射到明文之间的相加运算，即

[0043] $$Enc_{pk}(m_1)\oplus Enc_{pk}(m_2)=Enc_{pk}(m_1+m_2);$$

[0044] 3.密文与某明文的指数运算可以映射到密文对应明文与该明文的相乘运算，即$Enc_{pk}(m1)\odot m2=Enc_{pk}(m1m2)$。

[0045] (一)密钥分发算法：

[0046] 在本发明中，基于身份的签名密钥由密钥生成中心生成。针对参与数字签名的两方，分别产生部分签名私钥，操作如下：

[0047] 1.产生两个固定长度的大素数p，q，计算模数$n=pq$，欧拉函数$\varphi(n)=(p-1)(q-1)$。

[0048] 2.生成一对RSA的公私钥对(e，d)，满足$\gcd\left(e,\varphi(n)\right)=1$并且$ed\equiv 1 \bmod \varphi(n)$，其中e是公钥，d是私钥；

[0049] 3.生成一个随机数d_2，计算d_1使得等式$d_1d_2\equiv d \bmod \varphi(n)$成立；

[0050] 4.计算第一部分签名密钥$D_{ID}^{(1)}=H(ID)^{d_1}\bmod n$，第二部分签名密钥$D_{ID}^{(2)}=d_2$；其中H(ID)表示身份ID的哈希值；

[0051] 5.生成同态加密算法的一对公私钥对(pk，sk)；将$(e,\ D_{ID}^{(1)},pk,sk)$发送给第一参与方P_1，将$(e,\ D_{ID}^{(2)},pk)$发送给第二参与方P_2；

[0052] (二)分布式签名算法：

[0053] 在本发明中，基于身份的RSA数字签名由两方P_1和P_2共同完成，具体操作如下：

[0054] 1.P_1生成第一个随机数r_1，计算第一个临时公钥$R_1=H(ID)^{r_1}$，使用同态加密算法的公钥pk对r_1做加密，即第一个密文$C_1=Enc_{pk}(r_1)$。P_1把(R_1,C_1)发送给P_2。

[0055] 2.P_2生成第二个随机数r_2，计算第二个临时公钥$R_2=H(ID)^{r_2}$，第一部分签名$R=R_1{}^{r_2}=H(ID)^{r_1r_2}$，第二个密文$C_2=\left((C_1\odot r_2)\oplus Enc_{pk}(\alpha)\right)\odot D_{ID}^{(2)}=Enc_{pk}((r_1r_2+\alpha)D_{ID}^{(2)})$，其中α是身份ID，消息M和R一起做Hash操作得到的值，即$\alpha=H(ID,M,R)$。P_2把(R_2,C_2)发送给P_1。

[0056] 3.P_1使用同态加密算法的私钥做解密，计算明文$\sigma=Dec_{sk}(C_2)=(r_1r_2+\alpha)D_{ID}^{(2)}$，第一部签名$R=R_2{}^{r_1}=H(ID)^{r_1r_2}$和第二部分签名$S=(D_{ID}^{(1)})^{\sigma}\bmod n$。使用签名验证算法验证签名的正确性，若签名正确则输出签名(R，S)，否则终止协议。

[0057] 本发明在P_1和P_2通信中，加入了零知识证明机制，用来证明发送的数据确实是来自发送方的，从而降低数据被篡改的风险，提高方案的安全性。

[0058] 二、下面结合具体实施例阐述本发明的具体案例。

[0059] 对于本发明，需要密钥生成中心作为可信第三方，对需要签名的两方P_1和P_2的计算

设备(如个人电脑,智能移动设备)生成部分签名密钥$D_{ID}^{(1)}$和$D_{ID}^{(2)}$。P_1或P_2其中任何一方可以在不得到完整签名密钥的情况下对消息进行签名,并可以验证签名的正确性。双方均各自保存且不公开自己的部分签名密钥。

[0060] 在密钥分发阶段,密钥生成中心首先生成(e,d),以及满足$d_1 d_2 \equiv d \bmod \varphi(n)$的$d_1$和$d_2$。由$d_1$和$d_2$计算得到满足$(D_{ID}^{(1)})^{D_{ID}^{(2)}} = H(ID)^d \bmod n$的两个部分签名密钥$D_{ID}^{(1)}$和$D_{ID}^{(2)}$,其中H(ID)是基于用户身份生成的哈希值。选择同态加密算法,例如Paillier加密算法,并生成公私钥对(pk,sk);将$(e, D_{ID}^{(1)}, pk, sk)$发送给一方$P_1$,将$(e, D_{ID}^{(2)}, pk)$发送给另一方$P_2$。

[0061] 在分布式RSA数字签名生成的阶段:

[0062] 1.P_1首先生成r_1,计算$R_1 = H(ID)^{r_1}$,使用pk对r_1做同态加密得到$C_1 = Enc_{pk}(r_1)$,生成第一个零知识证明π_1,即证明R_1是关于r_1的一个离散对数。P_1把(R_1, C_1, π_1)发送给P_2;

[0063] 2.P_2检验π_1是否合法,如果不合法,P_2退出协议;否则P_2生成r_2,计算$R_2 = H(ID)^{r_2}$, $R = R_1^{r_2} = H(ID)^{r_1 r_2}$,生成第二个零知识证明$\pi_2$,即证明$R_2$是关于$r_2$的一个离散对数,并利用ID,M,和R计算出$\alpha = H(ID, M, R)$。$P_2$使用$C_1$,$r_2$和$\alpha$计算出$\gamma = (C_1 \odot r_2) \oplus Enc_{pk}(\alpha)$,通过$\gamma$和$D_{ID}^{(2)}$计算得到$C_2 = \gamma \odot D_{ID}^{(2)}$,即$C_2 = Enc_{pk}((r_1 r_2 + \alpha) D_{ID}^{(2)})$。$P_2$把$(R_2, C_2, \pi_2)$发送给$P_1$;

[0064] 3.P_1检验π_2是否合法,如果不合法,P_1退出协议;否则,P_1对C_2做同态解密,计算得到$\sigma = Dec_{sk}(C_2) = (r_1 r_2 + \alpha) D_{ID}^{(2)}$,$P_1$计算$S = (D_{ID}^{(1)})^{\sigma} \bmod n$,以及$R = R_2^{r_1} = H(ID)^{r_1 r_2}$。并对签名的正确性进行验证,若验证通过$P_1$则公布签名(R,S),否则终止协议。

[0065] 基于本发明的方法,很容易实施本发明方法的系统。

[0066] 基于本发明构造的基于身份的分布式RSA数字签名生成系统包括1台服务器作为密钥生成中心,2台设备。密钥生成中心按照本发明的密钥分发算法,向2台设备分发部分签名密钥。2台设备按照本发明的分布式签名算法,生成对消息M的分布式数字签名。

[0067] 其他未说明的具体技术实施,对于相关领域技术人员而言是众所周知,不言自明的。

[0068] 本文中所描述的具体实施例仅仅是对本发明精神作举例说明。本发明所属技术领域的技术人员可以对所描述的具体实施例做各种各样的修改或补充或采用类似的方式替代,但并不会偏离本发明的精神或者超越所附权利要求书所定义的范围。