(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 107483191 A
(43)申请公布日 2017.12.15

(21)申请号 201710701512.4

(22)申请日 2017.08.16

(71)申请人 济南浪潮高新科技投资发展有限公司

地址 250100 山东省济南市高新区孙村镇科航路2877号研发楼一楼

(72)发明人 孙善宝 于治楼 李秀芳

(74)专利代理机构 济南信达专利事务所有限公司 37100

代理人 姜明

(51)Int.Cl.

H04L 9/08(2006.01)
H04L 9/32(2006.01)
H04L 9/30(2006.01)
H04L 29/06(2006.01)

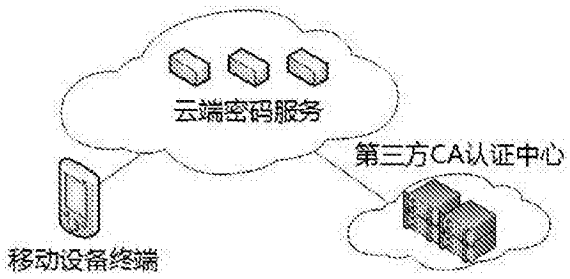
权利要求书2页 说明书5页 附图2页

(54)发明名称

一种SM2算法密钥分割签名系统及方法

(57)摘要

本发明涉及信息安全技术领域，具体设计密钥签名方法技术领域，特别涉及一种SM2算法密钥分割签名系统及方法。其系统结构包括移动设备、云端密码服务和第三方CA中心，所述的移动设备和云端密码服务各自产生随机数，并在移动设备一端完成SM2密钥的合法性验证，确认生成SM2密钥；所述的移动设备和云端密码服务各自完成SM2算法数字签名的一部分，并最终在移动设备一端生成数字签名；本发明的一种SM2算法密钥分割签名方法，实现了基于SM2密钥分割的签名算法，由移动设备和云端共同完成数字签名，保证了签名过程密钥不被泄露，并能有效的保护移动设备端的密钥安全性。



CN 107483191 A

1.一种SM2算法密钥分割签名系统，包括移动设备、云端密码服务和第三方CA中心，所述的移动设备和云端密码服务各自产生随机数，并在移动设备一端完成SM2密钥的合法性验证，确认生成SM2密钥；所述的移动设备和云端密码服务各自完成SM2算法数字签名的一部分，并最终在移动设备一端生成数字签名；

所述的移动设备负责生成随机数、完成SM2密钥的合法性验证以及生成SM2数字签名的部分计算，另外，移动设备会产生临时密钥，用于与云端加密服务的通信；

所述的云端密码服务负责生成随机数，与移动设备端的加密认证数据传输以及实现SM2签名算法的部分计算；

所述的第三方CA中心负责数字证书的签发，一方面为云端密码服务签发证书，确保云端密码服务的合法身份，另一方面为移动设备颁发数字证书，为移动设备的密码应用提供合法身份认证。

2.根据权利要求1所述的一种SM2算法密钥分割签名系统，其特征在于，所述的移动设备采用外接硬件加密终端设备。

3.根据权利要求1所述的一种SM2算法密钥分割签名系统，其特征在于，所述的云端密码服务采用硬件密码机，或使用云密码机来完成加密签名操作。

4.一种SM2算法密钥分割签名方法，包括分割密钥生成的方法和完成数字签名的方法，其中，分割密钥生成的方法包括：

步骤101、第三方CA中心为云端密码服务颁发数字证书；

步骤102、移动设备生成临时密钥对，向所述的云端密码服务提出分割密钥生成请求；

步骤103、所述的云端密码服务生成随机数dc，使用移动设备的公钥进行加密，并使用自身密钥进行签名，发送给所述的移动设备；

步骤104、所述的移动设备先利用临时私钥进行解密，再验证其证书有效性和签名有效性，获得云端密码服务的随机数dc；

步骤105、所述的移动设备产生随机数dm，计算d = dc*dm - 1，d ∈ [1;n - 2]，其中n为SM2椭圆曲线的一个基点的阶；

步骤106、所述的移动设备计算点P = (xP,yP) = [d]G，其中G为基点，(xP,yP)为坐标；如果P满足SM2椭圆曲线的要求，转到步骤107，否则转到步骤108；

步骤107、所述的移动设备向所述的云端密码服务发送生成密钥成功消息，SM2密钥对为SM2密钥对是(dm*dc-1;P)，其中dm作为所述的移动设备的私钥，dc作为所述的云端密码服务的私钥，P为公钥；

步骤108、所述的移动设备向所述的云端密码服务发送生成密钥失败消息，并转到步骤102，重新进行随机数申请；

步骤109、SM2分割密钥对生成成功，所述的第三方CA中心为该密钥颁发数字证书；

完成数字签名的方法包括：

步骤201、所述的移动设备先计算本用户的杂凑值Z，再拼接明文M，计算其摘要值并转换为整数，记作e；

步骤202、所述的移动设备生成临时密钥对，向所述的云端密码服务提出分割密钥生成请求；

步骤203、所述的云端密码服务生成随机数k ∈[1,n-1]，计算SM2椭圆曲线点(x1,y1)=

[k]G，再计算r=(e+x1) mod n，若r=0或r+k=n则重新生成随机数；

步骤204、所述的云端密码服务计算t=(k+r)*dc-1；并将(r，t)使用移动设备的公钥进行加密，并使用自身密钥进行签名，发送给所述的移动设备；

步骤205、所述的移动设备先利用临时私钥进行解密，再验证其证书有效性和签名有效性，获得(r，t)；

步骤206、所述的移动设备产生计算s = (t-r*dm)*dm-1，如果s=0，转到步骤207，否则转到步骤208；

步骤207、所述的移动设备向所述的云端密码服务发送生成密钥失败消息，并转到步骤202，重新进行签名；

步骤208、所述的移动设备向所述的云端密码服务发送生成签名成功消息，SM2签名值为(r，s)。

5.根据权利要求4所述的一种SM2算法密钥分割签名方法，其特征在于，所述的步骤102中，移动设备向所述的云端密码服务提出分割密钥生成的请求，包括移动设备标识，临时密钥对的公钥，申请时间。

6.根据权利要求4所述的一种SM2算法密钥分割签名方法，其特征在于，所述的步骤202中，所述的移动设备向所述的云端密码服务提出分割密钥生成的请求包括移动设备标识，临时密钥对的公钥，摘要值整数e。

7.根据权利要求4所述的一种SM2算法密钥分割签名方法，其特征在于，所述的分割密钥生成的方法还包括：

步骤209、移动设备利用其公钥证书对签名值进行验签。

一种SM2算法密钥分割签名系统及方法

技术领域

[0001] 本发明涉及信息安全技术领域，具体设计密钥签名方法技术领域，特别涉及一种SM2算法密钥分割签名系统及方法。

背景技术

[0002] 近年来，网络安全事件频发，网络攻击已经从信息泄露、资金窃取、电信诈骗及钓鱼网站等个人事件，上升到全社会的安全事件，会影响我们的生活、影响政府的服务、社会稳定甚至社会安全。密码技术是网络信息安全的核心技术，在互联网全球化的大环境下，国产密码技术在国家安全战略上有着重要的地位，是实现国家网络信息自主可控的基础，可以广泛用于电子政务、能源、交通、卫生、教育等涉及民生和基础信息资源的行业系统。

[0003] SM2算法是国家密码管理局于2010年12月17日发布的椭圆曲线公钥密码算法，SM2算法与RSA算法相比在同等密钥强度下，具有安全性高、计算速度快、存储空间小的优点，同时，相对于国际标准的ECC算法，SM2算法在初始状态编码、加密计算效率上都要更好。

[0004] 随着移动互联网的发展，移动设备成为改变传统计算的一个根本趋势，移动设备已经步入智能化时代，移动智能终端的普及率越来越高。人们利用碎片化的时间来上网，移动办公、移动电子商务、移动电子政务有了巨大的发展，随之而来的是安全问题，需要解决移动端的身份认证和数字签名。在这种情况下，如何能高效的利用移动设备并结合国产密码算法实现数字签名成为一个亟需解决的问题。

发明内容

[0005] 为了解决现有技术的问题，本发明提供了一种SM2算法密钥分割签名系统及方法，其结合移动端的特点，利用移动设备和云端密码服务共同产生SM2密钥，并将密钥分割为两部分，分别由移动设备端和云端密码服务器各自保存，本方法实现了基于SM2密钥分割的签名算法，由移动设备和云端共同完成数字签名，保证了签名过程密钥不被泄露，并能有效的保护移动设备端的密钥安全性。

[0006] 本发明所采用的技术方案如下：

一种SM2算法密钥分割签名系统，包括移动设备、云端密码服务和第三方CA中心，所述的移动设备和云端密码服务各自产生随机数，并在移动设备一端完成SM2密钥的合法性验证，确认生成SM2密钥；所述的移动设备和云端密码服务各自完成SM2算法数字签名的一部分，并最终在移动设备一端生成数字签名；

所述的移动设备负责生成随机数、完成SM2密钥的合法性验证以及生成SM2数字签名的部分计算，另外，移动设备会产生临时密钥，用于与云端加密服务的通信；

所述的云端密码服务负责生成随机数，与移动设备端的加密认证数据传输以及实现SM2签名算法的部分计算；

所述的第三方CA中心负责数字证书的签发，一方面为云端密码服务签发证书，确保云端密码服务的合法身份，另一方面为移动设备颁发数字证书，为移动设备的密码应用提供

合法身份认证。

[0007] 移动设备采用外接硬件加密终端设备。

[0008] 云端密码服务采用硬件密码机，或使用云密码机来完成加密签名操作。

[0009] 一种SM2算法密钥分割签名方法，包括分割密钥生成的方法和完成数字签名的方法，其中，分割密钥生成的方法包括：

步骤101、第三方CA中心为云端密码服务颁发数字证书；

步骤102、移动设备生成临时密钥对，向所述的云端密码服务提出分割密钥生成请求；

步骤103、所述的云端密码服务生成随机数dc，使用移动设备的公钥进行加密，并使用自身密钥进行签名，发送给所述的移动设备；

步骤104、所述的移动设备先利用临时私钥进行解密，再验证其证书有效性和签名有效性，获得云端密码服务的随机数dc；

步骤105、所述的移动设备产生随机数dm，计算d = dc*dm - 1，d ∈ [1;n - 2]，其中n为SM2椭圆曲线的一个基点的阶；

步骤106、所述的移动设备计算点P = (xP,yP) = [d]G，其中G为基点，(xP,yP)为坐标；如果P满足SM2椭圆曲线的要求，转到步骤107，否则转到步骤108；

步骤107、所述的移动设备向所述的云端密码服务发送生成密钥成功消息，SM2密钥对为SM2密钥对是(dm*dc-1;P)，其中dm作为所述的移动设备的私钥，dc作为所述的云端密码服务的私钥，P为公钥；

步骤108、所述的移动设备向所述的云端密码服务发送生成密钥失败消息，并转到步骤102，重新进行随机数申请；

步骤109、SM2分割密钥对生成成功，所述的第三方CA中心为该密钥颁发数字证书；

完成数字签名的方法包括：

步骤201、所述的移动设备先计算本用户的杂凑值Z，再拼接明文M，计算其摘要值并转换为整数，记作e；

步骤202、所述的移动设备生成临时密钥对，向所述的云端密码服务提出分割密钥生成请求；

步骤203、所述的云端密码服务生成随机数k ∈[1,n-1]，计算SM2椭圆曲线点(x1,y1)=[k]G，再计算r=(e+x1) mod n，若r=0或r+k=n则重新生成随机数；

步骤204、所述的云端密码服务计算t=(k+r)*dc-1;并将(r,t)使用移动设备的公钥进行加密，并使用自身密钥进行签名，发送给所述的移动设备；

步骤205、所述的移动设备先利用临时私钥进行解密，再验证其证书有效性和签名有效性，获得(r,t)；

步骤206、所述的移动设备产生计算s = (t-r*dm)*dm-1，如果s=0，转到步骤207，否则转到步骤208；

步骤207、所述的移动设备向所述的云端密码服务发送生成密钥失败消息，并转到步骤202，重新进行签名；

步骤208、所述的移动设备向所述的云端密码服务发送生成签名成功消息，SM2签名值为(r,s)。

[0010] 步骤102中，移动设备向所述的云端密码服务提出分割密钥生成的请求，包括移动

设备标识，临时密钥对的公钥，申请时间。

[0011] 步骤202中，所述的移动设备向所述的云端密码服务提出分割密钥生成的请求包括移动设备标识，临时密钥对的公钥，摘要值整数e。

[0012] 分割密钥生成的方法还包括：

步骤209、移动设备利用其公钥证书对签名值进行验签。

[0013] 本发明实施例提供的技术方案带来的有益效果是：

本发明提供了一种SM2算法密钥分割签名系统及方法，结合移动端的特点，利用移动设备和云端密码服务共同产生SM2密钥，并将密钥分割为两部分，分别由移动设备端和云端密码服务器各自保存。生成密钥的过程采用了加密签名来实现设备端和云端的数据交互，保证了传输安全性。基于密钥分割的SM签名算法，将计算分别交由移动设备端和云端来完成，签名过程中随机数的产生利用了云端硬件设备实现，这也保证了随机数的产生强度；密钥和签名生成都在移动设备端完成，云端无法获得移动设备端的密钥部分，甚至连经过计算后的密钥内容也无法获得，这样保证了移动设备端的密钥安全。另一方面，密钥进行分割，即使部分密钥泄露，恶意攻击者也无法伪造数字签名，有效的保护了密钥安全性。另外，移动设备端还可以接入外部密码加密硬件设备来增强其产生SM2密钥的强度。

附图说明

[0014] 为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0015] 图1为本发明的一种SM2算法密钥分割签名系统的系统构成结构图；

图2为本发明的一种SM2算法密钥分割签名方法的密钥生成方法流程图；

图3为本发明的一种SM2算法密钥分割签名方法的数字签名方法流程图。

具体实施方式

[0016] 为使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明实施方式作进一步地详细描述。

[0017] 实施例一

如附图1所示，本实施例的一种SM2算法密钥分割签名系统，包括移动设备、云端密码服务和第三方CA中心。移动设备和云端密码服务各自产生随机数，并在移动设备端完成SM2密钥的合法性验证，确认生成SM2密钥；移动设备和云端密码服务各自完成SM2算法数字签名的一部分，并最终在移动设备端生成数字签名；基于本方法的SM2数字签名验证操作与标准的SM2算法相同。其中，所述的移动设备负责生成随机数、SM2密钥的合法性验证以及生成SM2数字签名的部分计算，另外，移动设备会产生临时密钥用于与云端加密服务的通信，这里的移动设备还可以通过采用外接硬件加密终端设备来提高其安全性。所述的云端密码服务负责生成随机数，与移动设备端的加密认证数据传输以及实现SM2签名算法的部分计算，云端密码服务可以采用硬件密码机，也可以使用云密码机来完成加密签名等操作。所述的第三方CA中心主要负责数字证书的签发，一方面为云端密码服务签发证书，确保云端密码

服务的合法身份，另一方面为移动设备颁发数字证书，为移动设备的密码应用提供合法身份认证。

[0018] 为了描述清楚，假设在本实施例中，云端和设备端进行消息传输均采用国密标准SM2算法，加密密钥算法为SM2国密算法，SM3国密算法作为摘要算法，SM3SM2国密算法作为签名算法，数字证书采用X509格式。移动设备端密钥生成请求的数据格式如下：

ID ：移动设备标识

PubKey：临时密钥对的公钥

T1：申请时间

Nonce ：一次性数字标识

SigAlg ：签名算法

Signature ：签名值

移动设备端的数字签名请求的数据格式如下：

ID ：移动设备标识

e ：处理后的明文摘要值

PubKey：临时密钥对的公钥

T1：申请时间

Nonce ：一次性数字标识

SigAlg ：签名算法

Signature ：签名值

本领域技术人员将理解的是，除了使用以上数据格式之外，根据本发明的实施方式的构造也能够应用于其他数据格式之上。

[0019] 实施例2：

本实施例的一种SM2算法密钥分割签名方法，包括分割密钥生成的方法和完成数字签名的方法，其中，密钥生成方法参考图2，包括以下步骤：

步骤101、所述的第三方CA中心为所述的云端密码服务颁发数字证书；

步骤102、所述的移动设备生成临时密钥对，向所述的云端密码服务提出分割密钥生成请求(包括移动设备标识，临时密钥对的公钥，申请时间等)；

步骤103、所述的云端密码服务生成随机数dc，使用移动设备的公钥进行加密，并使用自身密钥进行签名，发送给所述的移动设备；

步骤104、所述的移动设备先利用临时私钥进行解密，再验证其证书有效性和签名有效性，获得云端密码服务的随机数dc。

[0020] 步骤105、所述的移动设备产生随机数dm，计算d = dc*dm - 1 ，d ∈ [1;n - 2]，其中n为SM2椭圆曲线的一个基点的阶。

[0021] 步骤106、所述的移动设备计算点P = (xP,yP) = [d]G，其中G为基点，(xP,yP)为坐标；如果P满足SM2椭圆曲线的要求，转到步骤107，否则转到步骤108；

步骤107、所述的移动设备向所述的云端密码服务发送生成密钥成功消息，SM2密钥对为SM2密钥对是(dm*dc-1;P)，其中dm作为所述的移动设备的私钥，dc作为所述的云端密码服务的私钥，P为公钥；

步骤108、所述的移动设备向所述的云端密码服务发送生成密钥失败消息，并转到步骤

102，重新进行随机数申请。

[0022] 步骤109、SM2分割密钥对生成成功，所述的第三方CA中心为该密钥颁发数字证书。

[0023] 完成数字签名的方法参考图3，包括以下步骤：

步骤201、所述的移动设备先计算本用户的杂凑值Z，再拼接明文M，计算其摘要值并转换为整数，记作e；

步骤202、所述的移动设备生成临时密钥对，向所述的云端密码服务提出分割密钥生成请求(包括移动设备标识，临时密钥对的公钥，摘要值整数e等)；

步骤203、所述的云端密码服务生成随机数k ∈[1,n-1]，计算SM2椭圆曲线点(x1,y1)=[k]G，再计算r=(e+x1) mod n，若r=0或r+k=n则重新生成随机数；

步骤204、所述的云端密码服务计算t=(k+r)*dc-1；并将(r,t)使用移动设备的公钥进行加密，并使用自身密钥进行签名，发送给所述的移动设备；

步骤205、所述的移动设备先利用临时私钥进行解密，再验证其证书有效性和签名有效性，获得(r,t)；

步骤206、所述的移动设备产生，计算s = (t-r*dm)*dm-1 ，如果s=0，转到步骤207，否则转到步骤208；

步骤207、所述的移动设备向所述的云端密码服务发送生成密钥失败消息，并转到步骤202，重新进行签名。

[0024] 步骤208、所述的移动设备向所述的云端密码服务发送生成签名成功消息，SM2签名值为(r,s)；

步骤209、所述的移动设备利用其公钥证书对签名值进行验签。

[0025] 以上所述仅为本发明的较佳实施例，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、改进等，均应包含在本发明的保护范围之内。

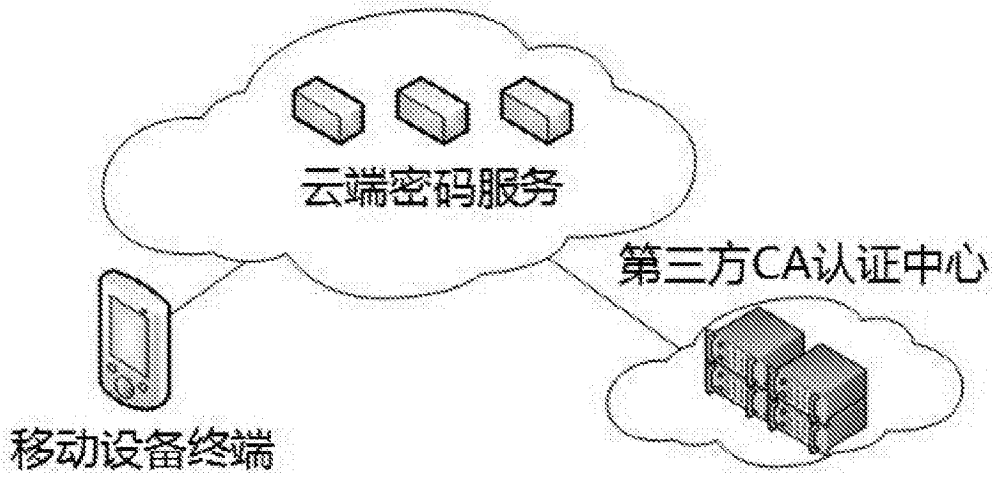

云端密码服务
第三方CA认证中心
移动设备终端

图1

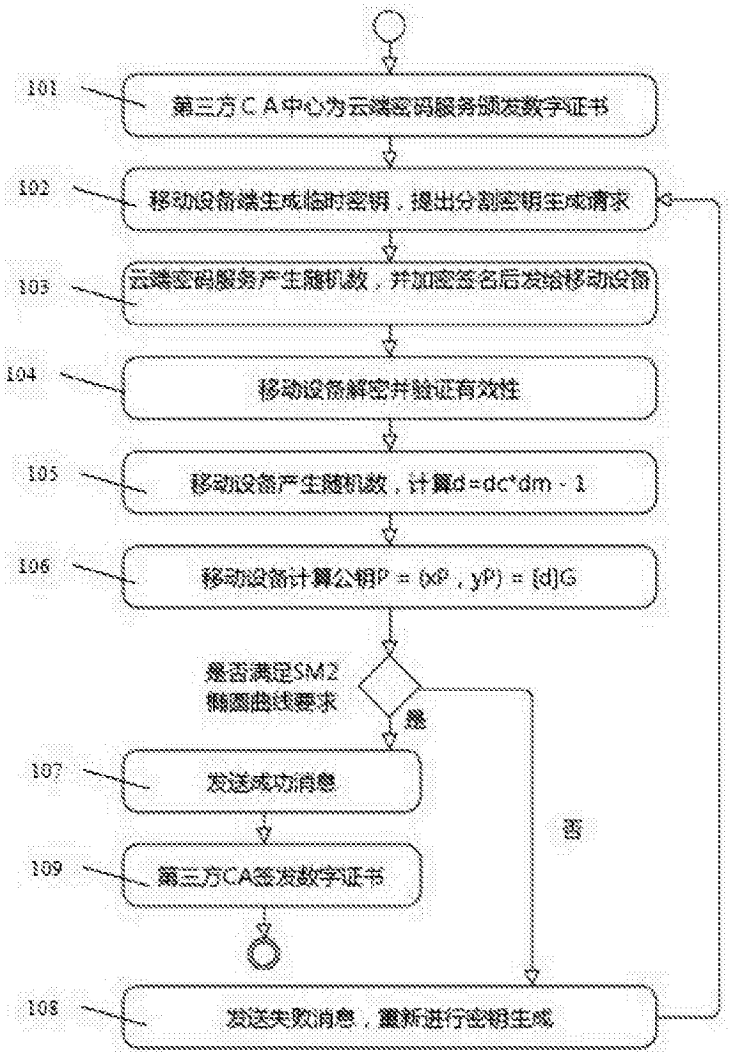

101
第三方CA中心为云端密码服务颁发数字证书
102
移动设备端生成临时密钥，提出分割密钥生成请求
103
云端密码服务产生随机数，并加密签名后发给移动设备
104
移动设备解密并验证有效性
105
移动设备产生随机数，计算d=dc*dm-1
106
移动设备计算公钥P=(xP，yP)=[d]G
是否满足SM2
椭圆曲线要求
是
否
107
发送成功消息
109
第三方CA签发数字证书
108
发送失败消息，重新进行密钥生成

图2

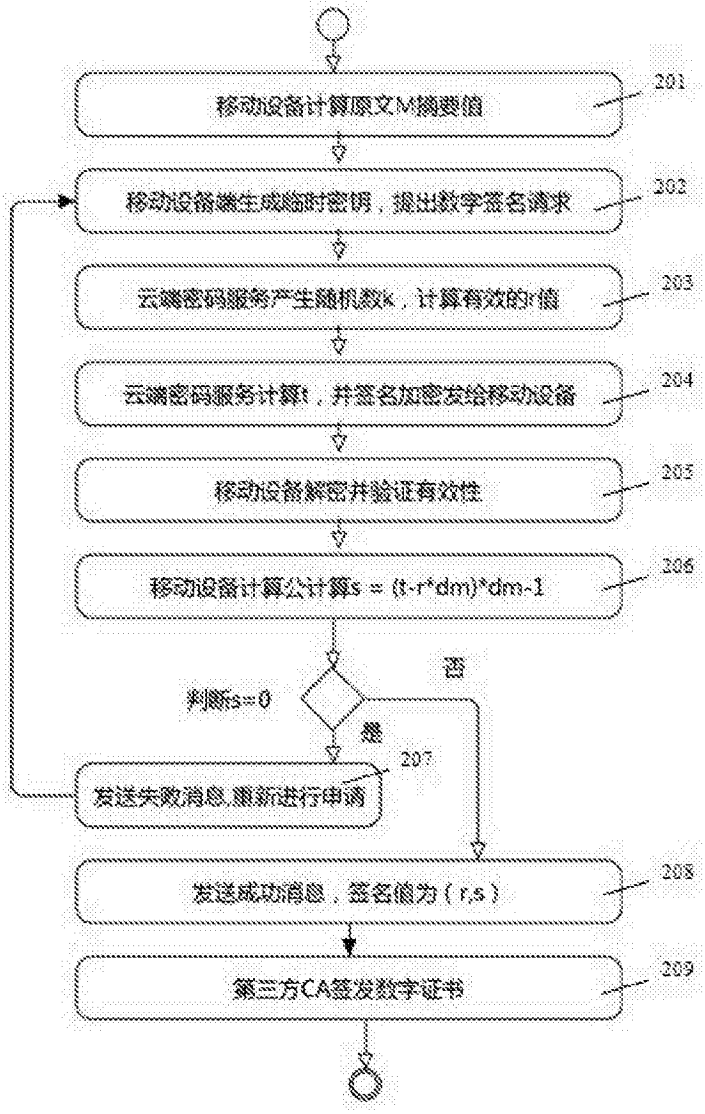

移动设备计算原文M摘要值
201
移动设备端生成临时密钥，提出数字签名请求
202
云端密码服务产生随机数k，计算有效的r值
203
云端密码服务计算t，并签名加密发给移动设备
204
移动设备解密并验证有效性
205
移动设备计算公计算s = (t-r*dm)*dm-1
206
判断s=0
否
是
207
发送失败消息，重新进行申请
发送成功消息，签名值为（r,s）
208
第三方CA签发数字证书
209

图3