(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 114186251 A
(43)申请公布日 2022.03.15

(21)申请号 202111465919.4

(22)申请日 2021.12.03

(71)申请人 中国科学院大学
地址 100049 北京市石景山区玉泉路19号(甲)

(72)发明人 荆继武 王平建 王跃武 王鹏 雷灵光 刘丽敏 孙思维 寇春静

(74)专利代理机构 北京君尚知识产权代理有限公司 11200
代理人 司立彬

(51)Int.Cl.
G06F 21/60(2013.01)
G06F 21/62(2013.01)
H04L 9/30(2006.01)

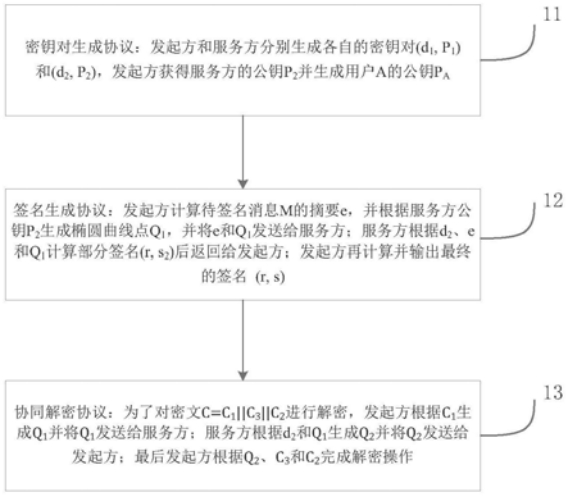
权利要求书2页 说明书7页 附图4页

(54)发明名称

一种保护用户隐私的SM2密码算法协同签名、解密方法

(57)摘要

本发明公开了一种保护用户隐私的SM2密码算法协同签名、解密方法。本发明的签名方法包括:发起方和服务方分别生成各自的密钥对(d_1,P_1)和(d_2,P_2),发起方获得服务方的部分公钥P_2并根据P_2生成用户A的公钥P_A;其中,发起方为用户A所在的终端;发起方计算待签名消息M的摘要e,并根据部分公钥P_2生成椭圆曲线点Q_1;然后将e和Q_1发送给服务方;服务方根据自己的部分私钥d_2、e和Q_1计算得到部分签名(r,s_2)后返回给发起方;发起方根据发起方的部分私钥d_1、r、s_2计算并输出最终的签名(r,s)。本发明不仅提供用户隐私保护,还增强了服务方的性能。



CN 114186251 A

1.一种保护用户隐私的SM2密码算法协同签名方法,其步骤包括:

1)发起方和服务方分别生成各自的密钥对(d_1,P_1)和(d_2,P_2),发起方获得服务方的部分公钥P_2并根据P_2生成用户A的公钥P_A;其中,发起方为用户A所在的终端;

2)发起方计算待签名消息M的摘要e,并根据部分公钥P_2生成椭圆曲线点Q_1;然后将e和Q_1发送给服务方;

3)服务方根据自己的部分私钥d_2、e和Q_1计算得到部分签名(r,s_2)后返回给发起方;

4)发起方根据发起方的部分私钥d_1、r、s_2计算并输出最终的签名(r,s)。

2.根据权利要求1所述的方法,其特征在于,生成密钥对(d_1,P_1)和(d_2,P_2)的方法为:

发起方向服务方发送协同密钥对生成请求;

服务方收到协同密钥对生成请求后,生成随机数$d_2\in[1,n-1]$,其中n为椭圆曲线基点G的阶;计算椭圆曲线点$P_2=[d_2]G$,得到服务方的密钥对(d_2,P_2)并将P_2发送给发起方;

发起方验证P_2是否满足椭圆曲线方程,如果满足则产生随机数$d_1\in[1,n-1]$;然后计算椭圆曲线点$P_1=[d_1]G$,得到发起方的密钥对为(d_1,P_1)。

3.根据权利要求2所述的方法,其特征在于,所述发起方产生随机数$k_1\in[1,n-1]$,通过$Q_1=[k_1]P_2$计算椭圆曲线点Q_1。

4.根据权利要求3所述的方法,其特征在于,得到所述部分签名(r,s_2)的方法为:

31)服务方验证Q_1是否满足椭圆曲线方程,如果满足则产生随机数$k_2\in[1,n-1]$;

32)计算椭圆曲线点$(x_1,y_1)=[k_2]G+Q_1$,将x_1数据类型转换为整数;

33)计算$r=e+x_1 \bmod n$,若$r=0$或$r+k_2=n$,则重新产生随机数k_2返回步骤32);否则计算$s_2=(d_2^{-1}\cdot(r+k_2))\bmod n$;得到所述部分签名$(r,s_2)$。

5.根据权利要求4所述的方法,其特征在于,得到所述签名(r,s)的方法为:

41)发起方根据k_1、s_2进行计算,如果$k_1+s_2=n$则返回步骤2)重新生成椭圆曲线点Q_1,将e和Q_1发送给服务方;

42)计算$s=(d_1^{-1}\cdot(k_1+s_2)-r)\bmod n$,若$s=0$则返回步骤2)重新生成椭圆曲线点$Q_1$,将e和$Q_1$发送给服务方;否则使用公钥$P_A$验证$(r,s)$是否为消息M的签名,如果不是则本次签名失败;否则输出所述签名(r,s)。

6.一种保护用户隐私的SM2密码算法协同解密方法,其步骤包括:

1)发起方和服务方分别生成各自的密钥对(d_1,P_1)和(d_2,P_2),发起方获得服务方的部分公钥P_2;

2)对于待解密的密文C;其中密文C为SM2密码算法加密的密文,由C_1、C_3和C_2三个部分组成;发起方从密文C中提取比特串C_1、C_3和C_2;根据C_1生成椭圆曲线点Q_1并将Q_1发送给服务方;

3)服务方根据d_2和Q_1生成椭圆曲线点Q_2并将Q_2发送给发起方;

4)发起方根据Q_2、C_3和C_2完成对密文C的解密。

7.根据权利要求6所述的方法,其特征在于,步骤2)中,生成椭圆曲线点Q_1的方法为:将C_1的数据类型转换成椭圆曲线上的点,验证C_1是否满足椭圆曲线方程并且$[h]C_1$不为无穷远点,若不满足或$[h]C_1$是无穷远点则结束协同解密流程,否则产生随机数$k_1\in[1,n-1]$,通过$Q_1=[k_1]C_1$计算椭圆曲线点Q_1;其中h为基点G的阶n的余因子。

8.根据权利要求7所述的方法,其特征在于,生成椭圆曲线点Q_2的方法为:验证Q_1是否满足椭圆曲线方程并且$[h]Q_1$不为无穷远点,若不满足或$[h]Q_1$是无穷远点则结束协同解密流

程;否则计算椭圆曲线点$Q_2=[d_2]Q_1$。

9.根据权利要求8所述的方法,其特征在于,步骤4)中,对密文C的解密方法为:验证Q_2是否满足椭圆曲线方程,若不满足则结束协同解密流程,若满足则计算椭圆曲线点$(x_2,y_2)=[d_1 \cdot k^{-1}]Q_2-C_1$,将$x_2$、$y_2$的数据类型转换成比特串;然后计算$t=KDF(x_2||y_2,klen)$,若t为全0比特串,则结束协同解密流程,否则计算$M'=C_2 \oplus t$;然后计算$u=Hash(x_2||M'||y_2)$,若$u \neq C_3$,则结束协同解密流程,否则输出明文$M'$;其中klen为密文中$C_2$的比特长度。

一种保护用户隐私的SM2密码算法协同签名、解密方法

技术领域

[0001] 本发明涉及密码领域，特别涉及适用于需要保护用户隐私的SM2密码算法协同签名、解密方法。

背景技术

[0002] 基于公钥密码学的数字签名技术已经广泛应用于电子商务、身份认证、数字票据等应用中，而私钥的生成及使用的安全性是保证数字签名安全的基础，而硬件密码模块(如U盾等)和移动终端已成为个人身份凭证中的重要载体，但存在容易被盗和丢失的风险。另一方面，针对移动终端的攻击越来越多，许多恶意应用能够窃取用户存储在终端上的私有数据，攻击终端与服务器的通信，因此亟需解决移动终端上的密钥存储和计算安全。基于密钥拆分和协同计算的协同签名技术，在易于推广部署的同时，还能够满足签名私钥的保护要求。

[0003] 已有多种SM2算法的协同签名方法，该类方案的共同特点是：由两个参与方分别存储部分私钥，两方联合才能完成消息的签名操作，我们下面将发起协同签名的一方称为发起方，另一方称为服务方。但是已有的方法普遍存在如下列举中问题的一个或多个：

[0004] 1)密钥对产生协议，服务方能够计算出用户完整私钥对应的公钥，这在需要严格保护用户隐私的场景不适用。

[0005] 2)密钥对产生协议，将发起方部分私钥和服务方部分私钥绑定，服务方存储这种绑定关系，这可能会造成用户关联信息的泄露。

[0006] 3)签名生成协议，需要服务方计算除椭圆曲线基点G的点乘操作，无法优化计算过程。

[0007] 4)缺少协同解密协议，在需要使用用户私钥解密数据时无法解密。

发明内容

[0008] 有鉴于此，本发明公开了一种保护用户隐私的SM2密码算法协同签名、解密方法，定义了密钥对生成协议、签名生成协议和协同解密协议，除了提供用户隐私保护的特性外还通过减少通信次数、减少随机数个数、使用可以优化的计算方法等增强了服务方的性能。

[0009] 为了达到上述目的，本发明的技术方案是这样实现的：

[0010] 1)密钥对生成协议：发起方和服务方分别生成各自的密钥对(d_1,P_1)和(d_2,P_2)，发起方获得服务方的部分公钥P_2并生成用户A的公钥P_A，其中发起方为用户A所在的终端。具体步骤如下：

[0011] 发起方：

[0012] A1：发起方向服务方发送协同密钥对生成请求。

[0013] 服务方：

[0014] B1：产生随机数$d_2\in[1,n-1]$，其中n为椭圆曲线基点G的阶；

[0015] B2：计算椭圆曲线点$P_2=[d_2]G$，服务方的密钥对为(d_2,P_2)；

[0016] B3:将P_2发送给发起方。

[0017] 发起方:

[0018] A2:验证P_2是否满足椭圆曲线方程,若不满足则协同生成密钥对失败;满足则进行A3;

[0019] A3:产生随机数$d_1\in[1,n-1]$;

[0020] A4:计算椭圆曲线点$P_1=[d_1]G$,发起方的密钥对为(d_1,P_1);

[0021] A5:计算椭圆曲线点$P_A=[d_1]P_2-G$,输出用户A的公钥为P_A。

[0022] 2)签名生成协议:发起方计算待签名消息M的摘要e,并根据服务方公钥P_2生成椭圆曲线点Q_1,并将e和Q_1发送给服务方;服务方根据d_2、e和Q_1计算部分签名(r,s_2)后返回给发起方;发起方再根据d_1、r、s_2计算并输出最终的签名(r,s)。具体步骤如下:

[0023] 发起方:

[0024] A1:按GM/T 0003.2中定义的方法计算消息M的摘要e;

[0025] A2:产生随机数$k_1\in[1,n-1]$;

[0026] A3:计算椭圆曲线点$Q_1=[k_1]P_2$;

[0027] A4:将e,Q_1发送给服务方。

[0028] 服务方:

[0029] B1:验证Q_1是否满足椭圆曲线方程,若不满足则终止协同签名流程;满足则进行B2;

[0030] B2:产生随机数$k_2\in[1,n-1]$;

[0031] B3:计算椭圆曲线点$(x_1,y_1)=[k_2]G+Q_1$,将x_1数据类型转换为整数;

[0032] B4:计算$r=e+x_1 \bmod n$,若$r=0$或$r+k_2=n$,则返回B2;否则进行B5;

[0033] B5:计算$s_2=(d_2^{-1}\cdot(r+k_2))\bmod n$;

[0034] B6:将r,s_2发送给发起方。

[0035] 发起方:

[0036] A5:如果$k_1+s_2=n$则返回A2;否则进行A6;

[0037] A6:计算$s=(d_1^{-1}\cdot(k_1+s_2)-r)\bmod n$,若$s=0$则返回A2;否则进行A7;

[0038] A7:使用公钥P_A验证(r,s)是否为消息M的签名,如果不是则本次签名失败;否则输出(r,s)作为消息M的签名。

[0039] 3)协同解密协议:为了对密文$C=C_1||C_3||C_2$进行解密,发起方根据C_1生成Q_1并将Q_1发送给服务方;服务方根据d_2和Q_1生成Q_2并将Q_2发送给发起方;最后发起方根据Q_2、C_3和C_2完成解密操作。具体步骤如下:

[0040] 发起方:

[0041] A1:从C中提取比特串C_1、C_3和C_2,将C_1的数据类型转换成椭圆曲线上的点,验证C_1是否满足椭圆曲线方程并且$[h]C_1$不为无穷远点,若不满足或$[h]C_1$是无穷远点则报错并退出,其中h为基点G的阶n的余因子;从SM2的密文C中提取C1C3C2三部分一个公知的技术,参考《GM/T 0003.4SM2椭圆曲线公钥密码算法第4部分公钥加密算法》。

[0042] A2:产生随机数$k_1\in[1,n-1]$,通过$Q_1=[k_1]C_1$计算椭圆曲线点Q_1,将Q_1发送给服务方。

[0043] 服务方:

[0044] B1:验证Q_1是否满足椭圆曲线方程并且[h]Q_1不为无穷远点,若不满足或[h]Q_1是无穷远点则结束协同解密流程;

[0045] B2:计算椭圆曲线点$Q_2=[d_2]Q_1$;

[0046] B3:将Q_2发送给发起方。

[0047] 发起方:

[0048] A3:验证Q_2是否满足椭圆曲线方程,若不满足则报错并退出;

[0049] A4:计算椭圆曲线点$(x_2,y_2)=[d_1 \cdot k^{-1}]Q_2-C_1$;将$x_2$、$y_2$的数据类型转换成比特串;

[0050] A5:计算$t=KDF(x_2||y_2,klen)$,若t为全0比特串,则报错并退出,其中klen为密文中C_2的比特长度;

[0051] A6:计算$M'=C_2 \oplus t$;

[0052] A7:计算$u=Hash(x_2||M'||y_2)$,若$u \neq C_3$,则报错并退出;

[0053] A8:输出明文M′。

[0054] 可见,本发明所述方案中,服务方不知道用户公钥,不需要关联发起方私钥,从而能够有效保护用户的隐私。同时协议执行过程中发送的数据不包含敏感内容,不需要对通信数据做机密性保护;签名生成协议中,仅需要一个通信流程既可以完成签名,服务方仅需要产生一个随机数,并且对于耗时较多的椭圆曲线点乘运算,服务方仅需要计算基点G和随机数的点乘,还可以在发起方请求前就进行预计算,从而本发明公布的服务方具有更高的性能。

附图说明

[0055] 图1为本发明保护用户隐私的SM2密码算法协同签名方法实施例的流程图。

[0056] 图2为本发明密钥对生成协议的过程示意图。

[0057] 图3为本发明签名生成协议的过程示意图。

[0058] 图4为本发明需要服务方验证或确认消息内容的签名生成协议的过程示意图。

[0059] 图5为本发明协同解密协议的过程示意图。

具体实施方式

[0060] 为了使本发明的技术方案更加清楚、明白,以下参照附图并举实施例,对本发明所述方案作进一步的详细说明。

[0061] 本发明使用以下术语和定义:

[0062] 1)协同数字签名:由两个参与方通过协议交互和使用各自掌握的用户部分私钥完成某输入消息的数字签名计算的过程。

[0063] 2)部分私钥:在协同数字签名过程中由发起方和服务方分别专用的秘密数据项。

[0064] 3)用户公钥:用户私钥对应的公钥,在本文件中是由两个参与方分别掌握的部分私钥共同组成的用户私钥对应的公钥。

[0065] 4)密钥对协同生成:由两个参与方通过协议交互生成各自掌握的部分私钥并输出用户公钥的过程。

[0066] 5)发起方:在协议的操作过程中发送首轮信息的参与方,本文件中一般为用户使用的终端。

[0067] 6)服务方:在协议的操作过程中协助发起方完成密钥对生成或签名的参与方,本文件中一般为服务端或辅助设备。

[0068] 本发明使用下列符号:

[0069] d_1 发起方的部分私钥。

[0070] d_2 服务方的部分私钥。

[0071] $d^{-1}\bmod n$ d模n的逆。

[0072] $E(F_q)$ F_q上椭圆曲线E的所有有理点(包括无穷远点)组成的集合。

[0073] F_q 包含q个元素的有限域。

[0074] e 密码杂凑算法作用于消息M的输出值。

[0075] G 椭圆曲线的一个基点,其阶为素数。

[0076] $H_v()$ 消息摘要长度为v比特的密码杂凑算法。

[0077] KDF() 密钥派生函数。

[0078] h 余因子,$h=\#E(F_q)/n$,其中n是基点G的阶。

[0079] M 待签名或待加密的消息。

[0080] mod n 模n运算。

[0081] n 基点G的阶。

[0082] P_1 发起方的部分公钥。

[0083] P_2 服务方的部分公钥。

[0084] P_A 用户A的公钥。

[0085] x||y x与y的拼接,其中x、y可以是比特串或字节串。

[0086] Z_A 关于用户A的标识、部分椭圆曲线系统参数和用户A公钥的杂凑值。

[0087] [k]P 椭圆曲线上点P的k倍点,k是正整数。

[0088] (r,s) 消息的签名。

[0089] [x,y] 大于或等于x且小于或等于y的整数的集合。

[0090] $\#E(F_q)$ $E(F_q)$上点的数目,称为椭圆曲线$E(F_q)$的阶。

[0091] 图1为本发明保护用户隐私的SM2密码算法协同签名方法实施例的流程图,如图1所示,包括以下步骤11～13。

[0092] 步骤11:发起方和服务方分别生成各自的密钥对(d_1,P_1)和(d_2,P_2),发起方获得服务方的部分公钥P_2并生成用户A的公钥P_A。

[0093] 步骤12:发起方计算待签名消息M的摘要e,并根据服务方部分公钥P_2生成椭圆曲线点Q_1,并将e和Q_1发送给服务方;服务方根据部分私钥d_2、e和Q_1计算部分签名(r,s_2)后返回给发起方;发起方再根据d_1、r、s_2计算并输出最终的签名(r,s)。

[0094] 步骤13:为了对密文$C=C_1||C_3||C_2$进行解密,发起方根据C_1生成Q_1并将Q_1发送给服务方;服务方根据d_2和Q_1生成Q_2并将Q_2发送给发起方;最后发起方根据Q_2、C_3和C_2完成解密操作。

[0095] 图2为本发明密钥对生成协议的过程示意图。如图2所示,包括发起方步骤A1～A5和服务方步骤B1～B3。

[0096] 发起方:

[0097] A1:发起方向服务方发送协同密钥对生成请求。

[0098] 服务方:

[0099] B1:产生随机数$d_2 \in [1,n-1]$;

[0100] B2:计算椭圆曲线点$P_2=[d_2]G$,服务方的密钥对为(d_2,P_2);

[0101] B3:将P_2发送给发起方。

[0102] 发起方:

[0103] A2:验证P_2是否满足椭圆曲线方程,若不满足则协同生成密钥对失败;

[0104] A3:产生随机数$d_1 \in [1,n-1]$;

[0105] A4:计算椭圆曲线点$P_1=[d_1]G$,发起方的密钥对为(d_1,P_1);

[0106] A5:计算椭圆曲线点$P_A=[d_1]P_2-G$,用户A的公钥为P_A。

[0107] 通过上述步骤所示过程,即可生成发起方和服务方各自的部分私钥d_1和d_2,并合成用户公钥P_A。用户实际私钥为$d_A=(d_1d_2-1) \bmod n$,无论是发起方还是服务方,都不能独立计算出用户私钥。

[0108] 需要说明的是,上述步骤表示方式仅为举例说明,并不用于限制各步骤的执行顺序,在实际应用中,可根据实际需要设定各步骤的执行顺序,只要最终能够得到所需的结果即可,后续涉及到的各示意图中同样如此,不再赘述。

[0109] 图3为本发明签名生成协议的过程示意图。如图3所示,包括发起方步骤A1～A7和服务方步骤B1～B6。

[0110] 发起方:

[0111] A1:计算消息摘要$e=H_v(Z_A||M)$,按GM/T 0003.1—2012第1部分4.2节中定义的方法将e的数据类型转换为整数,其中Z_A需按照GM/T 0003.2—2012第2部分5.5节中定义的方法计算得到;

[0112] A2:产生随机数$k_1 \in [1,n-1]$;

[0113] A3:计算椭圆曲线点$Q_1=[k_1]P_2$;

[0114] A4:将e,Q_1发送给服务方。

[0115] 服务方:

[0116] B1:验证Q_1是否满足椭圆曲线方程,若不满足则终止协同签名流程;

[0117] B2:产生随机数$k_2 \in [1,n-1]$;

[0118] B3:计算椭圆曲线点$(x_1,y_1)=[k_2]G+Q_1$,按GM/T 0003.1-2012第1部分4.2节中定义的方法将x_1数据类型转换为整数;

[0119] B4:计算$r=(e+x_1) \bmod n$,若$r=0$或$r+k_2=n$,则返回B2;

[0120] B5:计算$s_2=(d_2^{-1} \cdot (r+k_2)) \bmod n$;

[0121] B6:将r,s_2发送给发起方。

[0122] 发起方:

[0123] A5:如果$k_1+s_2=n$则返回A2;

[0124] A6:计算$s=(d_1^{-1} \cdot (k_1+s_2)-r) \bmod n$,若$s=0$则返回A2;

[0125] A7:使用公钥P_A验证(r,s)是否为消息M的签名,如果不是则本次签名失败;否则输出(r,s)作为消息M的签名。

[0126] 图4为本发明需要服务方验证或确认消息内容的签名生成协议的过程示意图。如

图4所示，包括发起方步骤A1～A6和服务方步骤B1～B8。

[0127] 发起方：

[0128] A1：产生随机数$k_1 \in [1,n-1]$；

[0129] A2：计算椭圆曲线点$Q_1 = [k_1]P_2$；

[0130] A3：将M，Z_A，Q_1发送给服务方，其中Z_A需按照GM/T 0003.2—2012第2部分5.5节中定义的方法计算得到。

[0131] 服务方：

[0132] B1：验证Q_1是否满足椭圆曲线方程，若不满足则终止协同签名流程；

[0133] B2：检查消息M的内容并进行确认，若消息内容不正确则终止协同签名流程；

[0134] B3：计算消息摘要$e = H_v(Z_A||M)$，按GM/T 0003.1-2012第1部分4.2节中定义的方法将e的数据类型转换为整数；

[0135] B4：产生随机数$k_2 \in [1,n-1]$；

[0136] B5：计算椭圆曲线点$(x_1,y_1) = [k_2]G+Q_1$，按GM/T 0003.1-2012第1部分4.2节中定义的方法将x_1数据类型转换为整数；

[0137] B6：计算$r = (e+x_1) \bmod n$，如果$r = 0$或者$r+k_2 = n$，则返回B4；

[0138] B7：计算$s_2 = (d_2^{-1} \cdot (r+k_2)) \bmod n$；

[0139] B8：将r，s_2发送给发起方。

[0140] 发起方：

[0141] A4：如果$k_1+s_2 = n$则返回A1；

[0142] A5：计算$s = (d_1^{-1} \cdot (k_1+s_2)-r) \bmod n$，若$s = 0$则返回A1；

[0143] A6：使用公钥P_A验证(r,s)是否为消息M的签名，如果不是则签名失败；否则输出(r,s)作为消息M的签名。

[0144] 图5为本发明协同解密协议的过程示意图。如图5所示，包括发起方步骤A1～A8和服务方步骤B1～B3。

[0145] 发起方：

[0146] A1：从C中提取比特串C_1、C_3和C_2，按GM/T 0003.1—2012第1部分3.2节中定义的方法将C_1的数据类型转换成椭圆曲线上的点，验证C_1是否满足椭圆曲线方程并且$[h]C_1$不为无穷远点，若不满足或$[h]C_1$是无穷远点则报错并退出，其中h为基点G的阶n的余因子；

[0147] A2：产生随机数$k_1 \in [1,n-1]$，通过$Q_1 = [k_1]C_1$计算椭圆曲线点Q_1，将$Q_1 = C_1$发送给服务方。

[0148] 服务方：

[0149] B1：验证Q_1是否满足椭圆曲线方程并且$[h]Q_1$不为无穷远点，若不满足或$[h]Q_1$是无穷远点则结束协同解密流程；

[0150] B2：计算椭圆曲线点$Q_2 = [d_2]Q_1$；

[0151] B3：将Q_2发送给发起方。

[0152] 发起方：

[0153] A3：验证Q_2是否满足椭圆曲线方程，若不满足则报错并退出；

[0154] A4：计算椭圆曲线点$(x_2,y_2) = [d_1 \cdot k^{-1}]Q_2-C_1$；按GM/T 0003.1—2012第1部分3.2节中定义的方法将x_2、y_2的数据类型转换成比特串；

[0155] A5:计算t＝KDF(x_2||y_2,klen),若t为全0比特串,则报错并退出,其中klen为密文中C_2的比特长度;

[0156] A6:计算M′＝C_2⊕t;

[0157] A7:计算u＝Hash(x_2||M′||y_2),若u≠C_3,则报错并退出;

[0158] A8:输出明文M′。

[0159] 综上所述,以上仅为本发明的较佳实施例而已,并非用于限定本发明的保护范围。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。

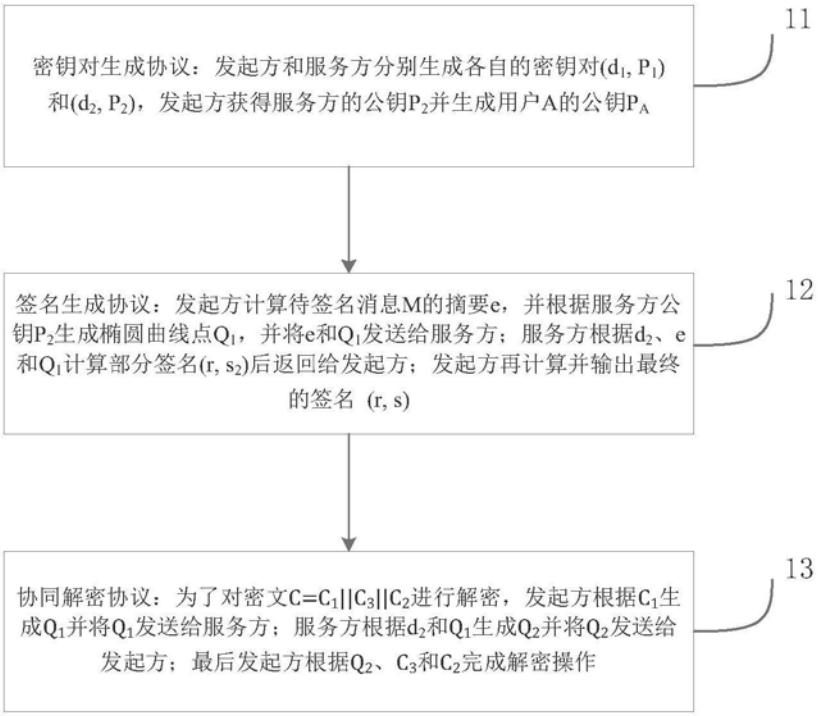

密钥对生成协议：发起方和服务方分别生成各自的密钥对(d_1, P_1)和(d_2, P_2)，发起方获得服务方的公钥P_2并生成用户A的公钥P_A
11
签名生成协议：发起方计算待签名消息M的摘要e，并根据服务方公钥P_2生成椭圆曲线点Q_1，并将e和Q_1发送给服务方；服务方根据d_2、e和Q_1计算部分签名(r, s_2)后返回给发起方；发起方再计算并输出最终的签名 (r, s)
12
协同解密协议：为了对密文$C=C_1||C_3||C_2$进行解密，发起方根据C_1生成Q_1并将Q_1发送给服务方；服务方根据d_2和Q_1生成Q_2并将Q_2发送给发起方；最后发起方根据Q_2、C_3和C_2完成解密操作
13

图1

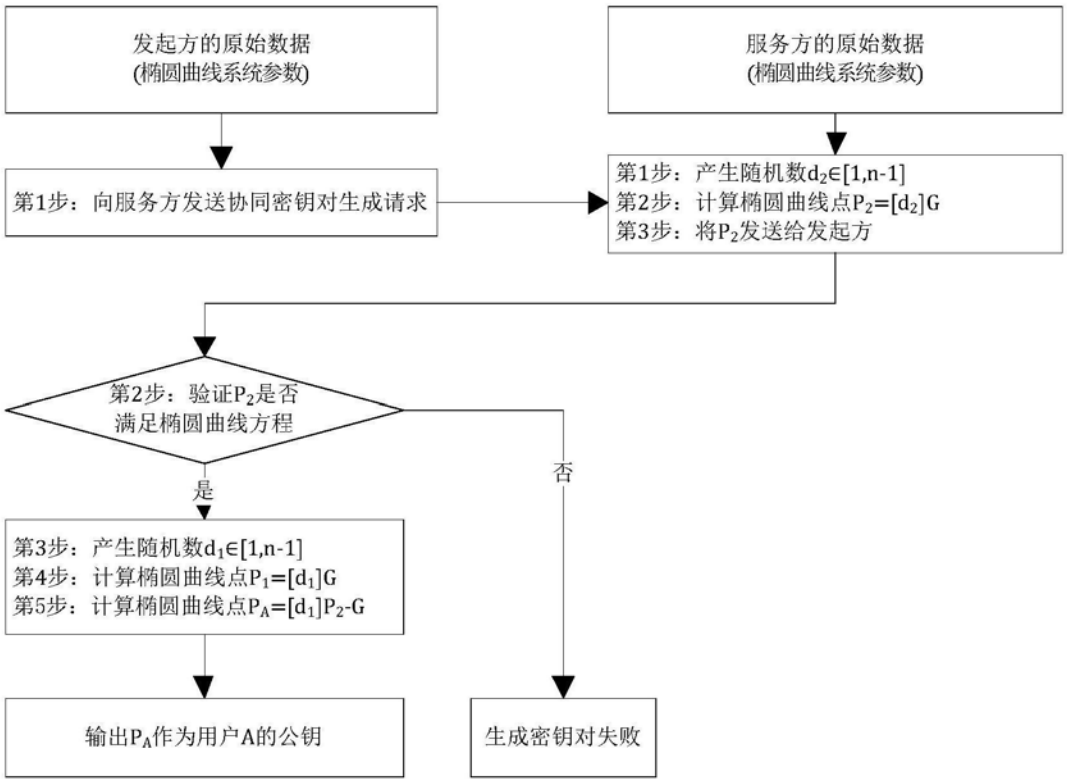

发起方的原始数据
(椭圆曲线系统参数)
服务方的原始数据
(椭圆曲线系统参数)
第1步：向服务方发送协同密钥对生成请求
第1步：产生随机数d_2∈[1,n-1]
第2步：计算椭圆曲线点$P_2=[d_2]G$
第3步：将P_2发送给发起方
第2步：验证P_2是否满足椭圆曲线方程
是
否
第3步：产生随机数d_1∈[1,n-1]
第4步：计算椭圆曲线点$P_1=[d_1]G$
第5步：计算椭圆曲线点$P_A=[d_1]P_2-G$
输出P_A作为用户A的公钥
生成密钥对失败

图2

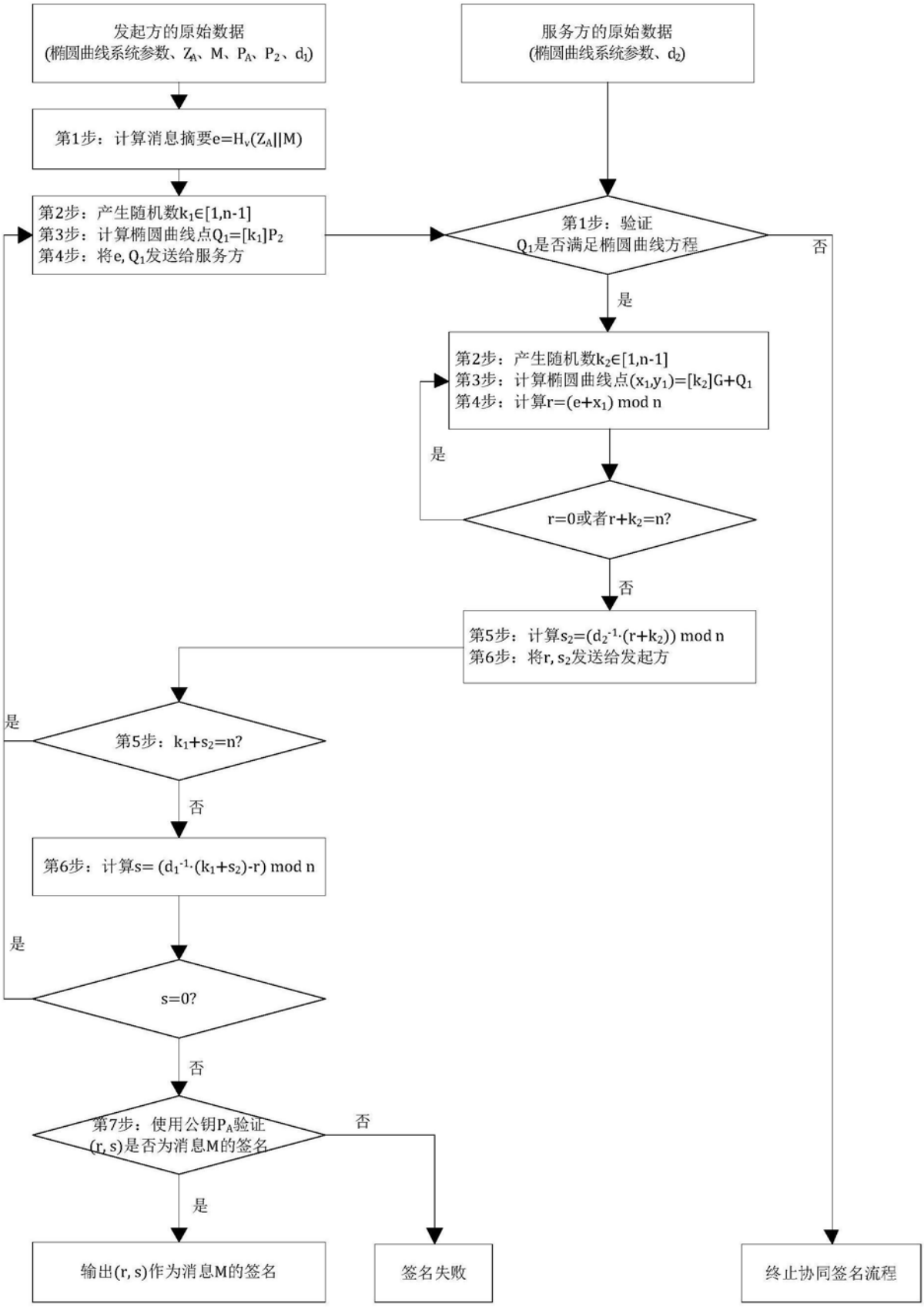

发起方的原始数据
(椭圆曲线系统参数、Z_A、M、P_A、P_2、d_1)
第1步：计算消息摘要$e=H_v(Z_A||M)$
第2步：产生随机数$k_1\in[1,n-1]$
第3步：计算椭圆曲线点$Q_1=[k_1]P_2$
第4步：将e, Q_1发送给服务方
服务方的原始数据
(椭圆曲线系统参数、d_2)
第1步：验证
Q_1是否满足椭圆曲线方程
否
是
第2步：产生随机数$k_2\in[1,n-1]$
第3步：计算椭圆曲线点$(x_1,y_1)=[k_2]G+Q_1$
第4步：计算$r=(e+x_1) \bmod n$
是
r=0或者$r+k_2=n$?
否
第5步：计算$s_2=(d_2^{-1}\cdot(r+k_2)) \bmod n$
第6步：将r, s_2发送给发起方
是
第5步：$k_1+s_2=n$?
否
第6步：计算$s=(d_1^{-1}\cdot(k_1+s_2)-r) \bmod n$
是
s=0?
否
第7步：使用公钥P_A验证
(r, s)是否为消息M的签名
否
是
输出(r, s)作为消息M的签名
签名失败
终止协同签名流程

图3

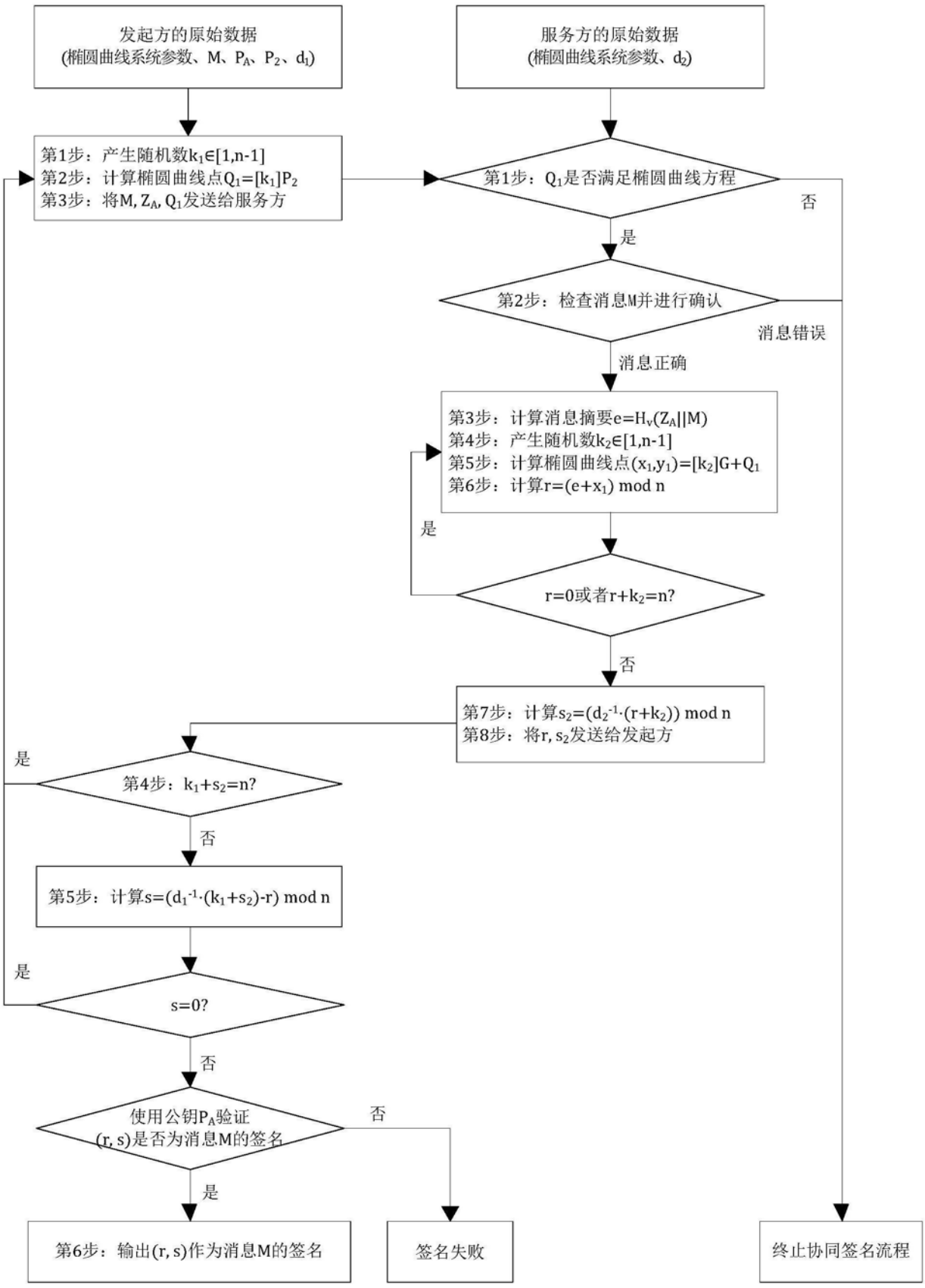

发起方的原始数据
(椭圆曲线系统参数、M、P_A、P_2、d_1)
服务方的原始数据
(椭圆曲线系统参数、d_2)
第1步：产生随机数k_1∈[1,n-1]
第2步：计算椭圆曲线点$Q_1=[k_1]P_2$
第3步：将M, Z_A, Q_1发送给服务方
第1步：Q_1是否满足椭圆曲线方程
否
是
第2步：检查消息M并进行确认
消息错误
消息正确
第3步：计算消息摘要$e=H_v(Z_A||M)$
第4步：产生随机数k_2∈[1,n-1]
第5步：计算椭圆曲线点$(x_1,y_1)=[k_2]G+Q_1$
第6步：计算$r=(e+x_1)$ mod n
是
r=0或者$r+k_2=n$?
否
第7步：计算$s_2=(d_2^{-1}\cdot(r+k_2))$ mod n
第8步：将r, s_2发送给发起方
是
第4步：$k_1+s_2=n$?
否
第5步：计算$s=(d_1^{-1}\cdot(k_1+s_2)-r)$ mod n
是
s=0?
否
使用公钥P_A验证
(r, s)是否为消息M的签名
否
是
第6步：输出(r, s)作为消息M的签名
签名失败
终止协同签名流程

图4

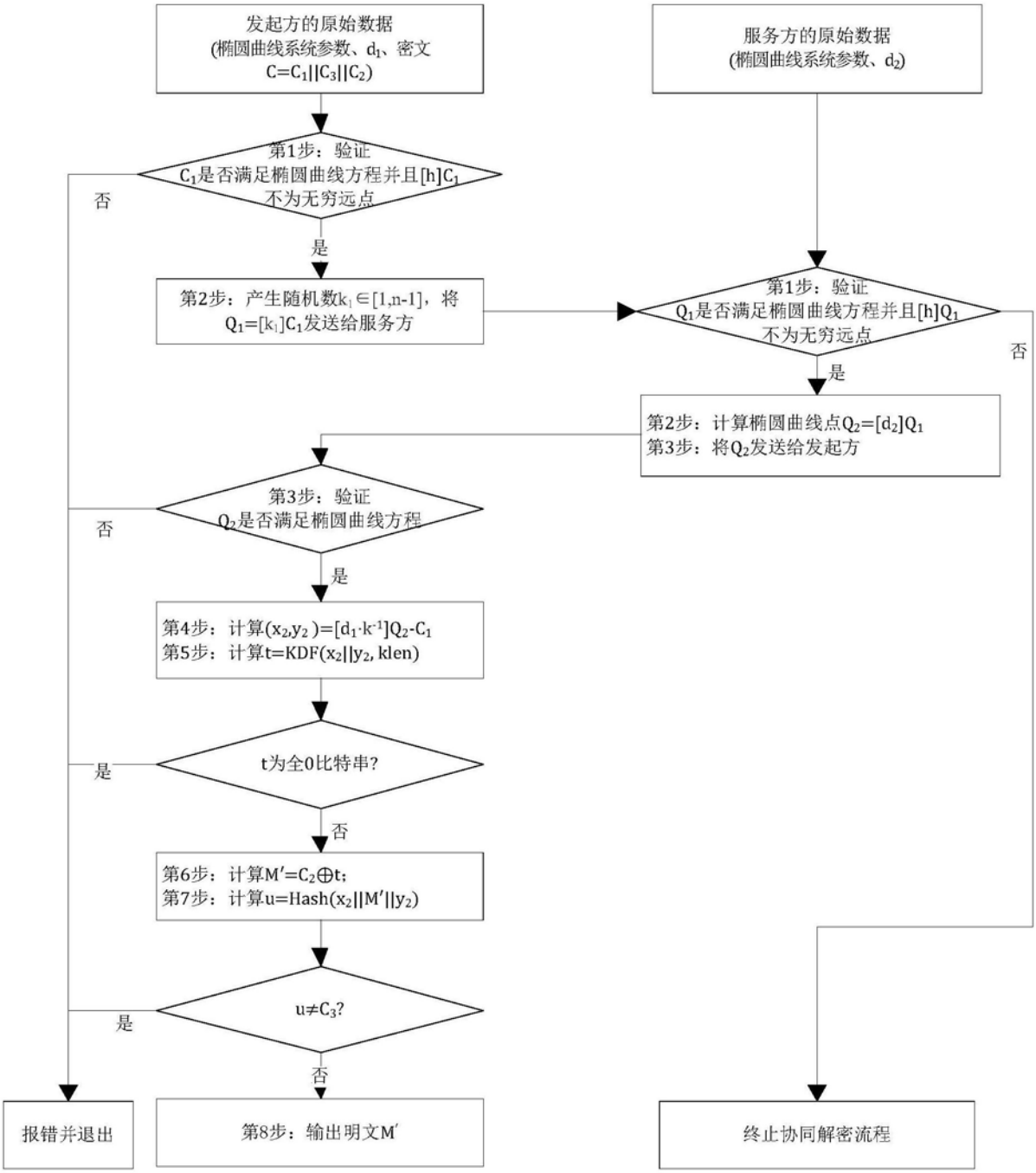

发起方的原始数据
(椭圆曲线系统参数、d_1、密文
$C=C_1||C_3||C_2$)
服务方的原始数据
(椭圆曲线系统参数、d_2)
第1步：验证
C_1是否满足椭圆曲线方程并且$[h]C_1$
不为无穷远点
否
是
第2步：产生随机数$k_1 \in [1,n-1]$，将
$Q_1=[k_1]C_1$发送给服务方
第1步：验证
Q_1是否满足椭圆曲线方程并且$[h]Q_1$
不为无穷远点
否
是
第2步：计算椭圆曲线点$Q_2=[d_2]Q_1$
第3步：将Q_2发送给发起方
第3步：验证
Q_2是否满足椭圆曲线方程
否
是
第4步：计算$(x_2,y_2)=[d_1 \cdot k^{-1}]Q_2-C_1$
第5步：计算$t=KDF(x_2||y_2, klen)$
t为全0比特串?
是
否
第6步：计算$M'=C_2 \oplus t$;
第7步：计算$u=Hash(x_2||M'||y_2)$
$u \neq C_3$?
是
否
报错并退出
第8步：输出明文M'
终止协同解密流程

图5