(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 108199835 A
(43)申请公布日 2018.06.22

(21)申请号 201810051923.8

(22)申请日 2018.01.19

(71)申请人 北京江南天安科技有限公司
地址 100088 北京市海淀区甸东路17号10层1110室

(72)发明人 闫鸣生 李国 闫申 马晓艳 曲金宝 张钊

(74)专利代理机构 北京科家知识产权代理事务所(普通合伙) 11427
代理人 戴丽伟

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

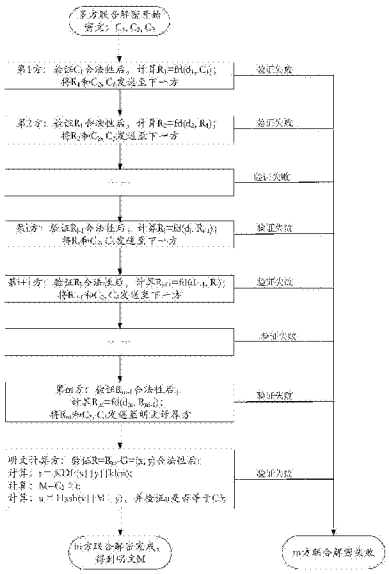
权利要求书2页 说明书11页 附图2页

(54)发明名称

一种多方联合私钥解密方法及系统

(57)摘要

本发明提供一种多方联合私钥解密方法及系统，私钥d由m份私钥因子d_i组成，i＝[1,m]，其中m≥2，m份私钥因子d_i由联合各方在密钥生成时独立秘密产生并秘密保存在各自的设备中；多方联合对密文解密时，需要m个联合方按照一定顺序各自使用自己保存的私钥因子d_i进行运算而共同参与完成对密文的解密。系统包括m个联合方，每个联合方各自具有独立的子系统，每个子系统包括联合密钥生成模块、倍点运算模块和明文计算模块。本发明的多方联合私钥解密方法及系统，改变了过去私钥解密只能由个体进行运算的限制，将私钥解密扩展到由多个独立个体组成的联合体的情况，并在各方联合完成私钥解密运算的情况下，才可以实现该联合体的私钥解密，安全性更高。



CN 108199835 A

1.一种多方联合私钥解密方法，其特征在于，私钥d由m份私钥因子d_i组成，i＝[1,m]，其中m≥2，m份私钥因子d_i由联合各方在密钥生成时独立秘密产生并秘密保存在各自的设备中；多方联合对密文C＝C_1||C_2||C_3解密时，需要m个联合方按照一定顺序各自使用自己保存的私钥因子d_i进行运算而共同参与完成对密文C的解密，其中，C_1为坐标参数，C_2为密文数据，C_3为256比特的数据与公钥结合后的杂凑值，“||”表示前后两个数据串的拼接。

2.根据权利要求1所述的多方联合私钥解密方法，其特征在于，m个联合方按照一定顺序各自使用自己保存的私钥因子d_i进行运算而共同参与完成对密文C的解密，包括如下步骤：

第一顺序方验证C_1是否满足SM2椭圆方程且C_1不是无穷远点，若不满足，则返回错误，联合解密失败；若满足，则恢复本方秘密保存的私钥因子d_1，使用单向函数fd()计算R_1＝fd(d_1,C_1)，并将R_1、C_2和C_3发送至第二顺序方；

第二顺序方验证R_1是否满足SM2椭圆方程且R_1不是无穷远点，若不满足，则返回错误，联合解密失败；若满足，则恢复本方秘密保存的私钥因子d_2，计算R_2＝fd(d_2,R_1)，并将R_2、C_2和C_3发送至下一顺序方；

以此类推，直至到m个联合方的最后顺序方；

最后顺序方验证R_{m-1}是否满足SM2椭圆方程且R_{m-1}不是无穷远点，若不满足，则返回错误，联合解密失败；若满足，则恢复本方秘密保存的私钥因子d_m，计算R_m＝fd(d_m,R_{m-1})＝(x,y)，同时计算t＝KDF(x||y,klen)，最后计算出明文$M = C_2 \oplus t$；其中klen为密文C_2的长度，KDF(x||y,klen)为SM2公钥密码算法的密钥派生函数，(x,y)表示椭圆曲线上的点坐标。

3.根据权利要求2所述的多方联合私钥解密方法，其特征在于，m个联合方中的每个联合方还可以根据各自的私钥因子d_i计算出对应的公钥因子P_i，每个联合方将自己的公钥因子P_i传递给需要的其它联合方，从而可以对传输数据进行加密保护或签名防伪。

4.根据权利要求1所述的多方联合私钥解密方法，其特征在于，m个联合方还可以通过服务中心协调来实现按照一定顺序各自使用自己保存的私钥因子d_i进行运算而共同参与完成对密文C的解密；其中，各联合方仅与服务中心通信，各联合方分别保存各自的私钥因子d_i，同时还保存了服务中心的公钥P，服务中心秘密保存了服务中心的私钥d，同时还保存了各联合方的公钥因子P_i，P_i＝[d_i]G，i＝[1,m]，G为SM2椭圆曲线的基点；具体步骤如下：

服务中心使用第一顺序方的公钥因子P_1对C_1进行SM2加密得到密文C_1”，并将C_1”发送给第一顺序方；

第一顺序方接收服务中心密文数据C_1”，恢复本方的私钥因子d_1，使用私钥因子d_1对密文C_1”进行SM2解密得到C_1，再验证C1是否满足SM2椭圆方程且C1不是无穷远点，若不满足，则返回错误，联合解密失败；若满足，则第一顺序方使用单向函数fd()计算R_1＝fd(d_1,C_1)，并使用服务中心公钥P对数据R_1进行SM2加密得到密文R_1’，将密文R_1’发送给服务中心；

服务中心使用中心私钥d对R_1’进行SM2解密得到R_1，再使用第二顺序方的公钥因子P_2对R_1进行SM2加密得到密文R_1”，并将R_1”发送给第二顺序方；

第二顺序方接收服务中心密文数据R_1”，恢复本方的私钥因子d_2，使用私钥因子d_2对密文R_1”进行SM2解密得到R_1，再验证R_1是否满足SM2椭圆方程且R_1不是无穷远点，若不满足，则返回错误，联合解密失败；若满足，则第二顺序方使用单向函数计算R_2＝fd(d_2,R_1)，并使用服务中心公钥P对数据R_2进行SM2加密得到密文R_2’，将密文R_2’发送给服务中心；

服务中心使用中心私钥d对R_2'进行SM2解密得到R_2,再使用第三顺序方的公钥因子P_3对R_2进行SM2加密得到密文R_2",并将R_2"发送给第三顺序方;

以此类推,直至到m个联合方的最后顺序方将密文R_m'发送给服务中心;

服务中心使用中心私钥d对R_m'进行SM2解密得到R_m,计算t=KDF(x||y,klen),最后计算出明文M=$C_2 \oplus$ t;其中,klen为密文C_2的长度,KDF(x||y,klen)为SM2公钥密码算法的密钥派生函数,(x,y)表示椭圆曲线上的点坐标。

5.根据权利要求2-4任一项所述的多方联合私钥解密方法,其特征在于,在计算出明文M之后还包括如下步骤:计算u=Hash(x||M||y),并验证u是否等于C_3,若是,则输出明文M;否则返回错误,联合解密失败;其中,Hash表示为预定的哈希函数。

6.一种多方联合私钥解密系统,其特征在于,包括m个联合方,每个联合方各自具有独立的子系统,每个子系统包括:

联合密钥生成模块:用于联合各方生成私钥d,私钥d由m份私钥因子d_i组成,i=[1,m],其中m≥2,该私钥d_i是在密钥生成时由m个联合方各自分别产生并秘密保存在各自的设备中;

倍点运算模块:用于SM2椭圆曲线的倍点运算;

明文计算模块:用于多方联合私钥解密时计算明文M。

一种多方联合私钥解密方法及系统

技术领域

[0001] 本发明涉及信息安全技术领域，尤其涉及一种多方联合私钥解密方法及系统。

背景技术

[0002] 使用SM2公钥密码体系的加解密是基于密钥对(d,P)，包括一个公钥P和一个私钥d。其中私钥d被秘密保存，可应用于对公钥加密数据的解密。

[0003] 传统的方法是解密设备独立秘密生产一组密钥对(d,P)，并秘密保存私钥d。需要解密时，解密设备独立使用私钥d对密文C进行解密运算出明文M。

[0004] 对于SM2椭圆曲线公钥密码算法，使用公钥P对明文M进行加密：

[0005] C＝En(P,k,M)

[0006] 其中，En()表示SM2加密运算，P为公钥，k为随机数，M为明文。

[0007] 得到的密文格式C的格式为：C＝C1||C2||C3；

[0008] 其中C1＝(x,y)为512比特点坐标数据，C2为密文数据(与明文等长)，C3为256比特的数据与公钥结合后的杂凑值；

[0009] 解密需使用私钥d，即：

[0010] M＝De(d,C)

[0011] 其中，De()表示SM2解密运算，d为私钥，C为密文。得到的明文M，关键步骤为：

[0012] 1.计算[d]C1＝(x2,y2)；即使用私钥d对密文C1部分计算。

[0013] 2.计算t＝KDF(x2||y2,klen)；klen为密文C2的长度；

[0014] 3.计算明文M＝C2⊕t；输出明文M。

[0015] 在公钥体系下，私钥解密是使用私钥d对加密数据进行运算的结果。对于诸如：笔记本、智能手机、电视机顶盒等终端设备缺乏专门的安全部件时，私钥将很难做到秘密保存，特别是在使用时，更容易遭到蠕虫、木马等恶意软件的攻击，造成私钥泄露。

发明内容

[0016] 基于此，本发明的目的在于提供一种多方联合私钥解密方法及系统，将私钥解密扩展到由多个独立个体组成的联合体的情况，并在各方联合完成私钥解密运算的情况下，才可以实现该联合体的私钥解密，安全性更高。为实现上述目的，本发明的技术方案如下：

[0017] 一种多方联合私钥解密方法，私钥d由m份私钥因子d_i组成，i＝[1,m]，其中m≥2，m份私钥因子d_i由联合各方在密钥生成时独立秘密产生并秘密保存在各自的设备中；多方联合对密文C＝C_1||C_2||C_3解密时，需要m个联合方按照一定顺序各自使用自己保存的私钥因子d_i进行运算而共同参与完成对密文C的解密，其中，C_1为坐标参数，C_2为密文数据，C_3为256比特的数据与公钥结合后的杂凑值，“||”表示前后两个数据串的拼接。

[0018] 使用私钥解密时，m个联合方各自使用自己保存的私钥因子d_i进行运算，按照1～m顺序，进行运算，其中第i方接收第i-1方的运算结果R_{i-1}，计算得到结果R_i，并将结果发送给第i+1方。直至最后第m方。计算出明文M。

[0019] 优选地，m个联合方按照一定顺序各自使用自己保存的私钥因子d_i进行运算而共同参与完成对密文C的解密，包括如下步骤：

[0020] 第一顺序方验证C_1是否满足SM2椭圆方程且C_1不是无穷远点，若不满足，则返回错误，联合解密失败；若满足，则恢复本方秘密保存的私钥因子d_1，使用单向函数fd()计算$R_1=fd(d_1,C_1)$，并将R_1、C_2和C_3发送至第二顺序方；

[0021] 第二顺序方验证R_1是否满足SM2椭圆方程且R_1不是无穷远点，若不满足，则返回错误，联合解密失败；若满足，则恢复本方秘密保存的私钥因子d_2，计算$R_2=fd(d_2,R_1)$，并将R_2、C_2和C_3发送至下一顺序方；

[0022] 以此类推，直至到m个联合方的最后顺序方；

[0023] 最后顺序方验证R_{m-1}是否满足SM2椭圆方程且R_{m-1}不是无穷远点，若不满足，则返回错误，联合解密失败；若满足，则恢复本方秘密保存的私钥因子d_m，计算$R_m=fd(d_m,R_{m-1})=(x,y)$，同时计算$t=KDF(x||y,klen)$，最后计算出明文$M=C_2\oplus t$；其中klen为密文$C_2$的长度，KDF(x||y,klen)为SM2公钥密码算法的密钥派生函数，(x,y)表示椭圆曲线上的点坐标。

[0024] 进一步地，m个联合方中的每个联合方还可以根据各自的私钥因子d_i计算出对应的公钥因子P_i，每个联合方还将自己的公钥因子P_i传递给需要的其它联合方，从而可以对传输数据进行加密保护或签名防伪。$P_i=[d_i]G$，$i=[1,m]$，G为SM2椭圆曲线的基点。

[0025] 优选地，m个联合方按照一定顺序各自使用自己保存的私钥因子d_i进行运算而共同参与完成对密文C的解密，包括如下步骤：

[0026] 第一顺序方验证C_1是否满足SM2椭圆方程且C_1不是无穷远点，若不满足，则返回错误，联合解密失败；若满足，则恢复本方秘密保存的私钥因子d_1，使用单向函数fd()计算$R_1=fd(d_1,C_1)$，并使用私钥因子d_1对数据$R_1||C_2||C_3$进行数字签名$S_1=(r_1,s_1)$，并将结果$Q_1=R_1||C_2||C_3||r_1||s_1$发送至第二顺序方；

[0027] 第二顺序方使用第一顺序方的公钥因子P_1对数字签名值(r_1,s_1)进行签名验证，如签名验证不通过，则返回错误，联合解密失败；如签名验证通过，则第二顺序方再验证R_1是否满足SM2椭圆方程且R_1不是无穷远点，若不满足，则返回错误，联合解密失败；若满足，则恢复本方秘密保存的私钥因子d_2，计算$R_2=fd(d_2,R_1)$，并使用私钥因子d_2对数据$R_2||C_2||C_3$进行数字签名$S_2=(r_2,s_2)$，并将结果$Q_2=R_2||C_2||C_3||r_2||s_2$发送至下一顺序方；

[0028] 以此类推，直至到m个联合方的最后顺序方；

[0029] 最后顺序方使用第m-1方的公钥因子P_{m-1}对数字签名值(r_{m-1},s_{m-1})进行签名验证，如签名验证不通过，则返回错误，联合解密失败；如签名验证通过，则最后顺序方再验证R_{m-1}是否满足SM2椭圆方程且R_{m-1}不是无穷远点，若不满足，则返回错误，联合解密失败；若满足，则恢复本方秘密保存的私钥因子d_m，计算$R_m=fd(d_m,R_{m-1})=(x,y)$，同时计算$t=KDF(x||y,klen)$，最后计算出明文$M=C_2\oplus t$；其中klen为密文$C_2$的长度，KDF(x||y,klen)为SM2公钥密码算法的密钥派生函数，(x,y)表示椭圆曲线上的点坐标。

[0030] 优选地，m个联合方还通过服务中心协调来实现按照一定顺序各自使用自己保存的私钥因子d_i进行运算而共同参与完成对密文C的解密；其中，各联合方仅与服务中心通信，各联合方分别保存各自的私钥因子d_i，同时还保存了服务中心的公钥P，服务中心秘密保存了服务中心的私钥d，同时还保存了各联合方的公钥因子P_i，$P_i=[d_i]G$，$i=[1,m]$，G为SM2椭圆曲线的基点；具体步骤如下：

[0031] 服务中心使用第一顺序方的公钥因子P_1对C_1进行加密得到密文C_1”，并将C_1”发送给第一顺序方；

[0032] 第一顺序方接收服务中心密文数据C_1”，恢复本方的私钥因子d_1，使用私钥因子d_1对密文C_1”进行SM2解密得到C_1，再验证C_1是否满足SM2椭圆方程且C_1不是无穷远点，若不满足，则返回错误，联合解密失败；若满足，则第一顺序方使用单向函数fd()计算$R_1=fd(d_1,C_1)$，并使用服务中心公钥P对数据R_1进行SM2加密得到密文R_1’，将密文R_1’发送给服务中心；

[0033] 服务中心使用中心私钥d对R_1’进行解密得到R_1，再使用第二顺序方的公钥因子P_2加密R_1得到密文R_1”，并将R_1”发送给第二顺序方；

[0034] 第二顺序方接收服务中心密文数据R_1”，恢复本方的私钥因子d_2，使用私钥因子d_2对密文R_1”进行SM2解密得到R_1，再验证R_1是否满足SM2椭圆方程且R_1不是无穷远点，若不满足，则返回错误，联合解密失败；若满足，则第二顺序方使用单向函数计算$R_2=fd(d_2,R_1)$，并使用服务中心公钥P对数据R_2进行SM2加密得到密文R_2’，将密文R_2’发送给服务中心；

[0035] 服务中心使用中心私钥d对R_2’进行SM2解密得到R_2，再使用下一顺序方的公钥因子对R_2进行SM2加密得到密文R_2”，并将R_2”发送给所述下一顺序方；

[0036] 以此类推，直至到m个联合方的最后顺序方将密文R_m’发送给服务中心；

[0037] 服务中心使用中心私钥d对R_m’进行SM2解密得到R_m，计算$t=KDF(x||y,klen)$，最后计算出明文$M=C_2\oplus t$；其中，klen为密文C_2的长度，KDF(x||y,klen)为SM2公钥密码算法的密钥派生函数，(x,y)表示椭圆曲线上的点坐标。

[0038] 优选地，m个联合方还通过服务中心协调来实现按照一定顺序各自使用自己保存的私钥因子d_i进行运算而共同参与完成对密文C的解密；其中，各联合方仅与服务中心通信，各联合方分别保存各自的私钥因子d_i，同时还保存了服务中心的公钥P，服务中心秘密保存了服务中心的私钥d，同时还保存了各联合方的公钥因子P_i，$P_i=[d_i]G$，$i=[1,m]$，G为SM2椭圆曲线的基点；具体步骤如下：

[0039] 服务中心使用第一顺序方的公钥因子P_1对C_1进行SM2加密得到密文C_1”，并将C_1”发送给第一顺序方；

[0040] 第一顺序方接收服务中心密文数据C_1”，恢复本方的私钥因子d_1，使用私钥因子d_1对密文C_1”进行SM2解密得到C_1，再验证C_1是否满足SM2椭圆方程且C_1不是无穷远点，若不满足，则返回错误，联合解密失败；若满足，则第一顺序方使用单向函数fd()计算$R_1=fd(d_1,C_1)$，并使用服务中心公钥P对数据R_1进行SM2加密得到密文R_1’，将密文R_1’发送给服务中心；

[0041] 服务中心使用中心私钥d对R_1’进行SM2解密得到R_1，再使用第二顺序方的公钥因子P_2对R_1进行SM2加密得到密文R_1”，并将R_1”发送给第二顺序方；

[0042] 第二顺序方接收服务中心密文数据R_1”，恢复本方的私钥因子d_2，使用私钥因子d_2对密文R_1”进行SM2解密得到R_1，再验证R_1是否满足SM2椭圆方程且R_1不是无穷远点，若不满足，则返回错误，联合解密失败；若满足，则第二顺序方使用单向函数fd()计算$R_2=fd(d_2,R_1)$，并使用服务中心公钥P对数据R_2进行SM2加密得到密文R_2’，将密文R_2’发送给服务中心；

[0043] 服务中心使用中心私钥d对R_2’进行SM2解密，得到R_2，再使用下一顺序方的公钥因子对R_2进行SM2加密得到密文R_2”，并将R_2”发送给所述下一顺序方；

[0044] 以此类推，直至到m个联合方的最后顺序方将密文R_m’发送给服务中心；

[0045] 服务中心使用中心私钥d对R_m’进行SM2解密得到R_m，再验证$R_m=(x,y)$是否满足SM2

椭圆方程且R_m不是无穷远点，若不满足，则返回错误，联合解密失败；若满足，则服务中心计算t＝KDF(x||y,klen)，最后计算出明文M＝$C_2 \oplus t$；其中，klen为密文C_2的长度，KDF(x||y,klen)为SM2公钥密码算法的密钥派生函数，(x,y)表示椭圆曲线上的点坐标。

[0046] 优选地，在计算出明文M之后还包括如下步骤：计算u＝Hash(x||M||y)，并验证u是否等于C3，若是，则输出明文M；否则返回错误，联合解密失败；其中，Hash表示为预定的哈希函数。

[0047] 根据本发明的另一方面，提供一种多方联合私钥解密系统，包括m个联合方，每个联合方各自具有独立的子系统，每个子系统包括：

[0048] 联合密钥生成模块：用于联合各方生成私钥d，私钥d由m份私钥因子d_i组成，i＝[1,m]，其中m≥2，该私钥d_i是在密钥生成时由m个联合方各自分别产生并秘密保存在各自的设备中；

[0049] 倍点运算模块：用于SM2椭圆曲线的倍点运算；

[0050] 明文计算模块：用于多方联合私钥解密时计算明文M。

[0051] 本发明的有益效果是：

[0052] 本发明的多方联合私钥解密方法及系统，改变了过去私钥解密只能由个体进行运算的限制，将私钥解密扩展到由多个独立个体组成的联合体的情况，并在各方联合完成私钥解密运算的情况下，才可以实现该联合体的私钥解密，安全性更高。

[0053] 在联合私钥解密的过程中，每个个体使用公钥加密或私钥签名的手段，进一步保证信息传递的私密性或真实性，有效防止信息传递过程中的信息泄露或信息伪造等攻击。

[0054] 鉴于互联网应用的日益广泛应用，手机APP、服务中心、解密中心及多个服务实体与终端联合进行私钥解密成为可能。其显著的效果是单个或多个解密单元的信息泄露并不会造成最终用户私钥的泄露。即只要不是所有的解密单元均被攻破，攻击者并不能到达使用用户私钥解密的目的，而相对集中的数据服务中心，由于设施到位，防控措施有效，可以更好地保护用户私钥因子。

附图说明

[0055] 图1为本发明一实施例的多方联合私钥解密方法的解密流程示意图；

[0056] 图2为本发明的多方联合私钥解密方法一实施例的四方有中心联合私钥解密示意图。

具体实施方式

[0057] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例对本发明的多方联合私钥解密方法及系统进行进一步详细说明。需要说明的是，在不冲突的情况下，以下各实施例及实施例中的特征可以相互组合。应当理解，此处所描述的具体实施例仅用于解释本发明，并不用于限定本发明。

[0058] 参照图1，本发明一实施例的多方联合私钥解密方法，私钥d由m份私钥因子d_i组成，i＝[1,m]，其中m≥2，m份私钥因子d_i由联合各方在密钥生成时独立秘密产生并秘密保存在各自的设备中；多方联合对密文C＝$C_1||C_2||C_3$解密时，需要m个联合方按照一定顺序各自使用自己保存的私钥因子d_i进行运算而共同参与完成对密文C的解密，其中，C_1为坐标参

数，优选为512比特的坐标数据，C_2为密文数据(与明文等长)，C_3为256比特的数据与公钥结合后的杂凑值，“||”表示前后两个数据串的拼接。

[0059] 作为一种可优选方式，m个联合方按照一定顺序各自使用自己保存的私钥因子d_i进行运算而共同参与完成对密文C的解密，包括如下步骤：

[0060] 第一顺序方验证C_1是否满足SM2椭圆方程且C_1不是无穷远点，若不满足，则返回错误，联合解密失败；若满足，则恢复本方秘密保存的私钥因子d_1，使用单向函数fd()计算$R_1=fd(d_1,C_1)$，并将R_1、C_2和C_3发送至第二顺序方；

[0061] 第二顺序方验证R_1是否满足SM2椭圆方程且R_1不是无穷远点，若不满足，则返回错误，联合解密失败；若满足，则恢复本方秘密保存的私钥因子d_2，计算$R_2=fd(d_2,R_1)$，并将R_2、C_2和C_3发送至下一顺序方；

[0062] 以此类推，直至到m个联合方的最后顺序方；

[0063] 最后顺序方验证R_{m-1}是否满足SM2椭圆方程且R_{m-1}不是无穷远点，若不满足，则返回错误，联合解密失败；若满足，则恢复本方秘密保存的私钥因子d_m，计算$R_m=fd(d_m,R_{m-1})=(x,y)$，同时计算$t=KDF(x||y,klen)$，最后计算出密文C对应的明文$M=C_2\oplus t$；其中klen为密文$C_2$的长度，KDF(x||y,klen)为SM2公钥密码算法的密钥派生函数，(x,y)表示椭圆曲线上的点坐标。

[0064] 较佳地，在计算出明文M之后还包括如下步骤：计算$u=Hash(x||M||y)$，并验证u是否等于C3，若是，则输出明文M；否则返回错误(报错并退出)，联合解密失败。其中，Hash表示为预定的哈希函数。

[0065] 作为另一种可优选方式，m个联合方按照一定顺序各自使用自己保存的私钥因子d_i进行运算而共同参与完成对密文C的解密，包括如下步骤：

[0066] 第一顺序方验证C_1是否满足SM2椭圆方程且C_1不是无穷远点，若不满足，则返回错误，联合解密失败；若满足，则恢复本方秘密保存的私钥因子d_1，使用单向函数fd()计算$R_1=fd(d_1,C_1)$，并使用私钥因子d_1对数据$R_1||C_2||C_3$进行数字签名$S_1=(r_1,s_1)$，并将结果$Q_1=R_1||C_2||C_3||r_1||s_1$发送至第二顺序方；

[0067] 第二顺序方使用第一顺序方的公钥因子P_1对数字签名值(r_1,s_1)进行签名验证，如签名验证不通过，则返回错误，联合解密失败；如签名验证通过，则第二顺序方再验证R_1是否满足SM2椭圆方程且R_1不是无穷远点，若不满足，则返回错误，联合解密失败；若满足，则恢复本方秘密保存的私钥因子d_2，计算$R_2=fd(d_2,R_1)$，并使用私钥因子d_2对数据$R_2||C_2||C_3$进行数字签名$S_2=(r_2,s_2)$，并将结果$Q_2=R_2||C_2||C_3||r_2||s_2$发送至下一顺序方；

[0068] 以此类推，直至到m个联合方的最后顺序方；

[0069] 最后顺序方使用第m-1方的公钥因子P_{m-1}对数字签名值(r_{m-1},s_{m-1})进行签名验证，如签名验证不通过，则返回错误，联合解密失败；如签名验证通过，则最后顺序方再验证R_{m-1}是否满足SM2椭圆方程且R_{m-1}不是无穷远点，若不满足，则返回错误，联合解密失败；若满足，则恢复本方秘密保存的私钥因子d_m，计算$R_m=fd(d_m,R_{m-1})=(x,y)$，同时计算$t=KDF(x||y,klen)$，最后计算出明文$M=C_2\oplus t$；其中klen为密文$C_2$的长度，KDF(x||y,klen)为SM2公钥密码算法的密钥派生函数，(x,y)表示椭圆曲线上的点坐标。

[0070] 本实施例中，m个联合方中的每个联合方还根据各自的私钥因子d_i计算出对应的公钥因子P_i，每个联合方还将自己的公钥因子P_i传递给需要的其它联合方。

[0071] 如图1所示，对于密文$C=C_1||C_2||C_3$，m个联合方共同完成解密的流程如下：

[0072] 第一方验证C_1合法性，即C_1是否满足椭圆方程及C_1不是无穷远点；如验证成功，恢复秘密保存的私钥因子d_1，计算$R_1=fd(d_1,C_1)$，将R_1、C_2、C_3发送至第二方；如验证失败，返回错误，联合解密失败。

[0073] 第二方验证R_1合法性，即R_1是否满足椭圆方程及R_1不是无穷远点；如验证成功，恢复秘密保存的私钥因子d_2，计算$R_2=fd(d_2,R_1)$，将R_2、C_2、C_3发送至第三方；如验证失败，返回错误，联合解密失败。

[0074] 一般地：

[0075] 第i方验证R_{i-1}合法性，即R_{i-1}是否满足椭圆方程及R_{i-1}不是无穷远点；如验证成功，恢复秘密保存的私钥因子d_i，计算$R_i=fd(d_i,R_{i-1})$，将R_i、C_2、C_3发送至第i+1方；如验证失败，返回错误，联合解密失败。(报错并退出)

[0076] $i=1,2,\cdots m$，$R_0=C_1$

[0077] 至最后第m方：

[0078] 第m方验证R_{m-1}合法性，即R_{m-1}是否满足椭圆方程及R_{m-1}不是无穷远点；如验证成功，恢复秘密保存的私钥因子d_m，计算$R_m=fd(d_m,R_{m-1})=(x,y)$。

[0079] 第m方计算：

[0080] 计算$t=KDF(x||y,klen)$；其中klen为密文C_2的长度，(x,y)表示椭圆曲线上的点坐标；

[0081] 计算明文$M=C_2\oplus t$；输出明文M。

[0082] 上述解密流程的主要特征是，多个联合各方分别秘密保存自己的私钥因子，并使用该私钥因子进行部分解密运算。每个联合方均进行一次，且仅进行一次私钥因子参与的运算，即可得到对密文C解密后的明文M，其中密文C是使用公钥P加密的密文。

[0083] 由于函数fd()为单向函数，所以各联合方使用私钥因子进行函数fd()运算的结果R_i，不会泄露私钥d_i的内容。即，无论是联合方还是网络窃听者，均无法仅通过传递的数据R_i、C_2、C_3来获取私钥因子d_i，从而保证了私钥的安全性。

[0084] 较佳地，在计算出明文M之后还包括如下步骤：计算$u=Hash(x||M||y)$，并验证u是否等于C3，若是，则输出明文M；否则返回错误(报错并退出)，联合解密失败。其中，Hash表示为预定的哈希函数。

[0085] 作为再一种可优选方式，m个联合方还通过服务中心协调来实现按照一定顺序各自使用自己保存的私钥因子d_i进行运算而共同参与完成对密文C的解密；其中，各联合方仅与服务中心通信，各联合方分别保存各自的私钥因子d_i，同时还保存了服务中心的公钥P，服务中心秘密保存了服务中心的私钥d，同时还保存了各联合方的公钥因子P_i，$P_i=[d_i]G$，$i=[1,m]$，G为SM2椭圆曲线的基点；具体步骤如下：

[0086] 服务中心使用第一顺序方的公钥因子P_1对C_1进行SM2加密得到密文C_1”，并将C_1”发送给第一顺序方；

[0087] 第一顺序方接收服务中心密文数据C_1”，恢复本方的私钥因子d_1，使用私钥因子d_1对密文C_1”进行SM2解密得到C_1，使用单向函数fd()计算$R_1=fd(d_1,C_1)$，并使用服务中心公钥P对数据R_1进行SM2加密得到密文R_1’，将密文R_1’发送给服务中心；

[0088] 服务中心使用中心私钥d对R_1’进行SM2解密得到R_1，再使用第二顺序方的公钥因子

P_2对R_1进行SM2加密得到密文R_1”，并将R_1”发送给第二顺序方；

[0089] 第二顺序方接收服务中心密文数据R_1”，恢复本方的私钥因子d_2，使用私钥因子d_2对密文R_1”进行SM2解密得到R_1，计算$R_2=fd(d_2,R_1)$，并使用服务中心公钥P对数据R_2进行SM2加密得到密文R_2’，将密文R_2’发送给服务中心。

[0090] 服务中心使用中心私钥d对R_2’进行SM2解密得到R_2，再使用下一顺序方的公钥因子对R_2进行SM2加密得到密文R_2”，并将R_2”发送给所述下一顺序方；

[0091] 以此类推，直至到m个联合方的最后顺序方将密文R_m’发送给服务中心；

[0092] 服务中心使用中心私钥d对R_m’进行SM2解密得到R_m，计算$t=KDF(x||y,klen)$，最后计算出明文$M=C_2\oplus t$；其中，klen为密文C_2的长度，KDF(x||y,klen)为SM2公钥密码算法的密钥派生函数。

[0093] 较佳地，在计算出明文M之后还包括如下步骤：计算$u=Hash(x||M||y)$，并验证u是否等于C3，若是，则输出明文M；否则返回错误(报错并退出)，联合解密失败。其中，Hash表示为预定的哈希函数。

[0094] 作为再一种可优选方式，m个联合方还通过服务中心协调来实现按照一定顺序各自使用自己保存的私钥因子d_i进行运算而共同参与完成对密文C的解密；其中，各联合方仅与服务中心通信，各联合方分别保存各自的私钥因子d_i，同时还保存了服务中心的公钥P，服务中心秘密保存了服务中心的私钥d，同时还保存了各联合方的公钥因子P_i，$P_i=[d_i]G$，$i=[1,m]$，G为SM2椭圆曲线的基点；具体步骤如下：

[0095] 服务中心使用第一顺序方的公钥因子P_1对C_1进行SM2加密得到密文C_1”，并将C_1”发送给第一顺序方；

[0096] 第一顺序方接收服务中心密文数据C_1”，恢复本方的私钥因子d_1，使用私钥因子d_1对密文C_1”进行SM2解密得到C_1，再验证C1是否满足SM2椭圆方程且C1不是无穷远点，若不满足，则返回错误，联合解密失败；若满足，则第一顺序方使用单向函数fd()计算$R_1=fd(d_1,C_1)$，并使用服务中心公钥P对数据R_1进行SM2加密得到密文R_1’，将密文R_1’发送给服务中心；

[0097] 服务中心使用中心私钥d对R_1’进行SM2解密得到R_1，再使用第二顺序方的公钥因子P_2对R_1进行SM2加密得到密文R_1”，并将R_1”发送给第二顺序方；

[0098] 第二顺序方接收服务中心密文数据R_1”，恢复本方的私钥因子d_2，使用私钥因子d_2对密文R_1”进行SM2解密得到R_1，再验证R_1是否满足SM2椭圆方程且R_1不是无穷远点，若不满足，则返回错误，联合解密失败；若满足，则第二顺序方使用单向函数fd()计算$R_2=fd(d_2,R_1)$，并使用服务中心公钥P对数据R_2进行SM2加密得到密文R_2’，将密文R_2’发送服务中心；

[0099] 服务中心使用中心私钥d对R_2’进行SM2解密得到R_2，再使用下一顺序方的公钥因子对R_2进行SM2加密得到密文R_2”，并将R_2”发送给所述下一顺序方；

[0100] 以此类推，直至到m个联合方的最后顺序方将密文R_m’发送给服务中心；

[0101] 服务中心使用中心私钥d对R_m’进行SM2解密得到R_m，再验证$R_m=(x,y)$是否满足SM2椭圆方程且R_m不是无穷远点，若不满足，则返回错误，联合解密失败；若满足，则服务中心计算$t=KDF(x||y,klen)$，最后计算出明文$M=C_2\oplus t$；其中，klen为密文C_2的长度，KDF(x||y,klen)为SM2公钥密码算法的密钥派生函数，(x,y)表示椭圆曲线上的点坐标。

[0102] 较佳地，在计算出明文M之后还包括如下步骤：计算$u=Hash(x||M||y)$，并验证u是否等于C_3，若是，则输出明文M；否则返回错误(报错并退出)，联合解密失败。其中，Hash表示

为预定的哈希函数。

[0103] 根据本发明的另一方面，还提供了一种多方联合私钥解密系统，包括m个联合方，每个联合方各自具有独立的子系统，每个子系统包括：

[0104] 联合密钥生成模块，用于联合各方生成私钥d，私钥d由m份私钥因子d_i组成，i＝[1,m]，其中m≥2，该私钥d_i是在密钥生成时由m个联合方各自分别产生并秘密保存在各自的设备中；

[0105] 倍点运算模块，用于SM2椭圆曲线的倍点运算；

[0106] 明文计算模块，用于多方联合私钥解密时计算明文M。

[0107] 对于系统实施例而言，由于其基本相似于方法实施例，所以描述得比较简单，相关之处参见方法实施例的部分说明即可。显然，本领域的技术人员应该明白，上述的本发明的各模块或各步骤可以用通用的计算装置来实现，它们可以集中在单个的计算装置上，或者分布在多个计算装置所组成的网络上，可选地，它们可以用计算装置可执行的程序代码来实现，从而，可以将它们存储在存储装置中由计算装置来执行，或者将它们分别制作成各个集成电路模块，或者将它们中的多个模块或步骤制作成单个集成电路模块来实现。这样，本发明不限制于任何特定的硬件和软件结合。

[0108] 实例一

[0109] 本实施例涉及的是三方联合解密的实现，一种典型的应用是一个合伙人公司有三个主要领导，分别是第一方：市场总监，第二方：总经理和第三方：董事长。公司重要数据M使用公司的公钥P进行了加密(密文为C)，该密文文件C解密需使用公司私钥d进行解密。为安全起见，公司私钥d分别由三个私钥因子d_i(i＝1,2,3)组成，即：$d=g(d_1,d_2,d_3)$。三方各保管公司私钥的一个私钥因子，只有三方联合解密才会解密该文件C。并约定最后一方为明文获取方。三方的解密设备可以是他们使用的个人电脑、手机或专用解密设备，如USB-KEY。

[0110] 以下实例以SM2非对称密码算法为例，说明三方(m＝3)联合解密的实现。

[0111] 同时，为保障消息来源的真实性，多方解密消息过程中增加了消息签名，以确定消息的真伪。

[0112] 1、联合解密前提

[0113] 第一方(市场总监)：

[0114] 秘密保存了第一方的加密密钥因子d_1，同时保存了第二方和第三方的公钥因子P_2、P_3，其中$P_i=[d_i]G$，i＝1,2,3；G为SM2的椭圆曲线基点。

[0115] 第二方(总经理)：

[0116] 秘密保存了第二方的加密密钥因子d_2，同时保存了第一方和第三方的公钥因子P_1、P_3。

[0117] 第二方(董事长)：

[0118] 秘密保存了第三方的加密密钥因子d_3，同时保存了第一方和第二方的公钥因子P_1、P_2。

[0119] 密文$C=C_1||C_2||C_3$。

[0120] 2、联合解密过程

[0121] 令函数fd(d,R)为SM2椭圆曲线的倍点运算，即：

[0122] $X=fd(d,R)=[d]R$

[0123] 其中X、R为SM2定义的椭圆曲线上的点，X是点R的d倍点，G为SM2的椭圆曲线基点。

[0124] 步骤1：第一方对密文C进行合法性验证，即验证C_1是否满足SM2椭圆方程及C_1不是无穷远点，如验证成功，恢复秘密保存的私钥因子d_1，计算$R_1=fd(d_1,C_1)$，并使用私钥因子d_1对数据$R_1||C_2||C_3$进行数字签名$S_1=(r_1,s_1)$，并将结果$Q_1=R_1||C_2||C_3||r_1||s_1$发送至第2方；

[0125] 如验证失败，返回错误，联合解密失败。

[0126] 步骤2：第2方对使用第1方的公钥因子P_1对数字签名值(r_1,s_1)进行签名验证。如验证不通过，说明数据Q_1是非法的，返回错误，联合解密失败。如验证通过，说明数据Q_1是合法的，则进行如下步骤：

[0127] 对数据R_1进行合法性验证，即验证R_1是否满足SM2椭圆方程及R_1不是无穷远点，如验证成功，恢复秘密保存的私钥因子d_2，计算$R_2=fd(d_2,R_1)$，并使用私钥因子d_2对数据$R_2||C_2||C_3$进行数字签名$S_2=(r_2,s_2)$，并将结果$Q_2=R_2||C_2||C_3||r_2||s_2$发送至第3方；

[0128] 如验证失败，返回错误，联合解密失败。

[0129] 步骤3：第3方对使用第2方的公钥因子P_2对数字签名值(r_2,s_2)进行签名验证。如验证不通过，说明数据Q_2是非法的，返回错误，联合解密失败。如验证通过，说明数据Q_2是合法的，则进行如下步骤：

[0130] 对数据R_2进行合法性验证，即验证R_2是否满足SM2椭圆方程及R_2不是无穷远点，如验证失败，返回错误，联合解密失败。

[0131] 如验证成功，恢复秘密保存的私钥因子d_2，计算$R_3=fd(d_3,R_2)=(x,y)$；同时计算：

[0132] 计算$t=KDF(x||y,klen)$；其中klen为密文C_2的长度，(x,y)表示椭圆曲线上的点坐标；

[0133] 计算明文$M=C_2\oplus t$。

[0134] 这样，通过三方的联合解密过程，最终第三方获得解密的明文M。

[0135] 在联合解密过程中，对传送的数据进行了数字签名，有效避免了数据被篡改或假冒数据的发生。

[0136] 实例二

[0137] 本实施例涉及的是有中心四方联合解密的实现，多方联合私钥解密方法，也可以是有中心的系统构成，其特点是中心负责与联合的各个联络及通信，使得各方不需相互发送消息或结果。在中心的协调下，各方使用各自的私钥因子完成联合解密过程。

[0138] 在有中心的情况下，联合解密的各方与中心之间还可以具有相互独有的加密密钥对即可以对各方与中心之间的信息进行加密，也可以对该信息进行签名以保证各方与中心之间信息的机密性和真实性。

[0139] 一种典型的应用是公司A的机密文件有四个掌管人，四个掌管人各自具有公司解密私钥的一个私钥因子，只有四个掌管人联合私钥解密才会完成公司的文件的解密。服务中心是一个对外提供服务的机构，在该服务中心的配合下完成各方的联合私钥解密工作。

[0140] 机密文件被公司A的公钥加密成密文C，密文C托管在服务中心保管。当服务中心收到买方客户B需要该秘密文件的采购协议，并按照约定将相关款项支付给公司A后，A公司即对密文C进行解密。解密过程由四个掌管人联合解密完成。

[0141] 以下实例以SM2非对称密码算法为例，说明有中心的四方联合私钥解密的实现。

[0142] 参照图2,图2是四方有中心联合私钥解密示意图。

[0143] 1、有中心的四方联合私钥解密前提

[0144] 四个联合私钥解密方:

[0145] 分别保存各自的私钥因子d_i,(i=1,2,3,4)。四方同时保存了服务中心的公钥P。

[0146] 服务中心:

[0147] 秘密保存了服务中心的私钥d,同时保存了四个联合解密的公钥因子P_i,其中$P_i=[d_i]G$,i=1,2,3,4;G为SM2的椭圆曲线基点。

[0148] 密文$C=C_1||C_2||C_3$。

[0149] 2、有中心四方联合私钥解密流程

[0150] 有中心的多方私钥解密流程需在服务中心的指挥下完成,由于各联合方地位平等,所以服务中心流程可以任意制定该流程中各方的先后次序。为方便起见,假定服务中心按照1-2-3-4的顺序进行。其步骤为:

[0151] 步骤1a:服务中心使用第1方的公钥因子P_1对C_1进行加密,得到密文C_1”,并将C_1”发送给第1方;

[0152] 步骤1b:第1方接收服务中密文数据C_1”,恢复本方的私钥因子d_1,使用私钥因子d_1对密文C_1”进行解密得到C_1。验证验证C_1是否满足SM2椭圆方程及C_1不是无穷远点。如验证成功,则计算$R_1=fd(d_1,C_1)$,并使用服务中心公钥P对数据R_1进行加密得到密文R_1’,将密文R_1’发送服务中心。

[0153] 如C_1验证失败,返回错误,联合解密失败。

[0154] 步骤2a:服务中心使用中心私钥d对R_1’进行解密得到R_1,再使用第2方的公钥因子P_2加密R_1,得到密文R_1”,并将R_1”发送给第2方;

[0155] 步骤2b:第2方接收服务中心密文数据R_1”,恢复本方的私钥因子d_2,使用私钥因子d_2对密文R_1”进行解密得到R_1。验证验证R_1是否满足SM2椭圆方程及R_1不是无穷远点。如验证成功,则计算$R_2=fd(d_2,R_1)$,并使用服务中心公钥P对数据R_2进行加密得到密文R_2’,将密文R_2’发送服务中心。

[0156] 如R_1验证失败,返回错误,联合解密失败。

[0157] 步骤3a:服务中心使用中心私钥d对R_2’进行解密,得到R_2,再使用第3方的公钥因子P_3加密R_2,得到密文R_2”,并将R_2”发送给第3方;

[0158] 步骤3b:第3方接收服务中心密文数据R_2”,恢复本方的私钥因子d_3,使用私钥因子d_3对密文R_2”进行解密,得到R_2。验证验证R_2是否满足SM2椭圆方程及R_2不是无穷远点。如验证成功,则计算$R_3=fd(d_3,R_2)$,并使用服务中心公钥P对数据R_3进行加密得到密文R_3’,将密文R_3’发送服务中心。

[0159] 如R_2验证失败,返回错误,联合解密失败。

[0160] 步骤4a:服务中心使用中心私钥d对R_3’进行解密,得到R_3,再使用第4方的公钥因子P_4加密R_3,得到密文R_3”,并将R_3”发送给第4方;

[0161] 步骤4b:第4方接收服务中心密文数据R_3”,恢复本方的私钥因子d_4,使用私钥因子d_4对密文R_3”进行解密,得到R_3。验证验证R_3是否满足SM2椭圆方程及R_3不是无穷远点。如验证成功,则计算$R_4=fd(d_4,R_3)$,并使用服务中心公钥P对数据R_4进行加密,将密文R_4’发送服务中心。

[0162] 如R_2验证失败，返回错误，联合解密失败。

[0163] 步骤5a：服务中心使用中心私钥d对R_4'进行解密，得到R_4，验证验证R_4＝(x,y)是否满足SM2椭圆方程及R_4不是无穷远点。如验证成功，则：

[0164] 计算t＝KDF(x||y,klen)；其中klen为密文C_2的长度，(x,y)表示椭圆曲线上的点坐标；

[0165] 计算明文M＝$C_2 \oplus t$。

[0166] 通过以上步骤，在服务中心指挥下，四方联合完成私钥的解密。解密后的明文M由服务中心通过安全途径提供给买方客户B。

[0167] 上述通信过程均使用了非对称密码算法对通信内容进行了加密，其优点是，由于使用了公钥加密，只有具有私钥的一方才可以正确解密并获得正确明文。

[0168] 以上各实施方式的多方联合私钥解密的方法及系统，改变了过去私钥解密只能由个体进行运算的限制，将私钥解密扩展到由多个独立个体组成的联合体的情况，并在各方联合完成私钥解密运算的情况下，才可以实现该联合体的私钥解密。在联合私钥解密的过程中，每个个体使用公钥加密或私钥签名的手段，进一步保证信息传递的私密性或真实性，有效防止信息传递过程中的信息泄露或信息伪造等攻击。

[0169] 鉴于互联网应用的日益广泛应用，手机APP，服务中心、解密中心及多个服务实体与终端联合进行用户解密成为可能。以上各实施例的多方联合私钥解密的方法及系统，其显著的效果是单个或多个解密单元的信息泄露并不会造成最终用户私钥的泄露。即只要不是所有的解密单元均被攻破，攻击者并不能到达使用用户私钥解密的目的，而相对集中的数据服务中心，由于设施到位，防控措施有效，可以更好地保护用户私钥因子。

[0170] 本发明的主要特点为：

[0171] 多方各自秘密保管自己的私钥因子d_i，私钥d可以表述为私钥因子的函数，即d＝g(d_1,d_2,…d_m)。任何一方、多方或网络监听者均不能获取完整私钥d。任何一方的私钥因子d_i，网络监听者及其它方均不能获取。

[0172] 联合解密时需由多方共同联合进行运算，各自按照一定顺序使用自己秘密保存的私钥d_i进行运算，相互配合最终结果完成解密过程，最终得到多方联合联合私钥解密的明文M。多方联合解密由多方分别使用各自的私钥因子d_i共同运算才可以完成，缺失任何一方都无法完成联合解密；各方使用相同的单向函数fd()进行运算；

[0173] 各方根据各自的私钥因子d_i计算对应的公钥因子P_i，并将公钥因子P_i传递给需要的其它方。私钥因子d_i可以进行本方的独立的数字签名或数据解密，具有其公钥因子的其它方可以使用公钥因子P_i进行签名验证或数据加密。

[0174] 以上所述实施例仅表达了本发明的几种实施方式，其描述较为具体和详细，但并不能因此而理解为对本发明专利范围的限制。应当指出的是，对于本领域的普通技术人员来说，在不脱离本发明构思的前提下，还可以做出若干变形和改进，凡未脱离本发明技艺精神所作的等效实施方式或变更均应包含在本发明的保护范围之内。

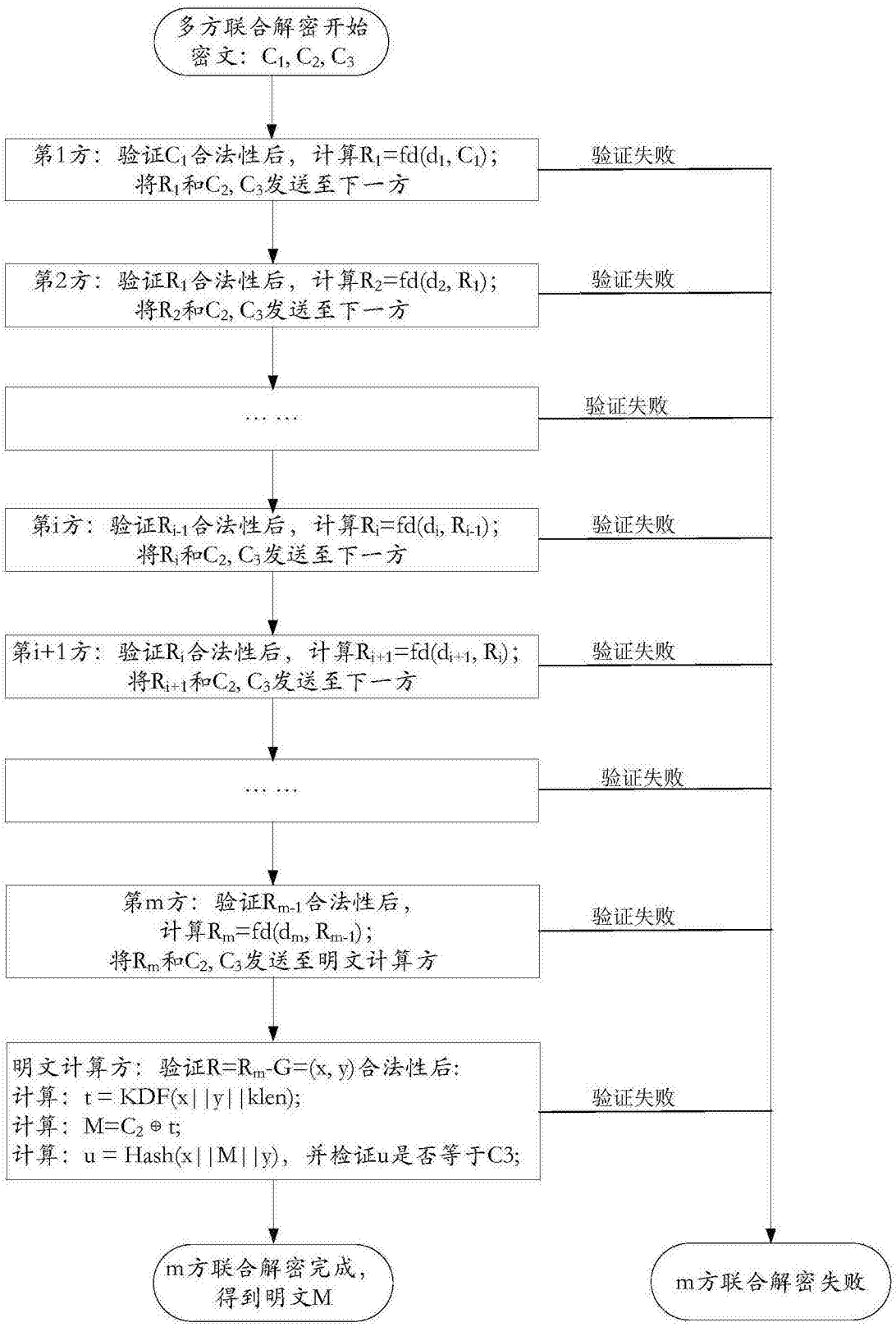

多方联合解密开始
密文：C1, C2, C3
第1方：验证C1合法性后，计算R1=fd(d1, C1)；
将R1和C2, C3发送至下一方
验证失败
第2方：验证R1合法性后，计算R2=fd(d2, R1)；
将R2和C2, C3发送至下一方
验证失败
… …
验证失败
第i方：验证Ri-1合法性后，计算Ri=fd(di, Ri-1)；
将Ri和C2, C3发送至下一方
验证失败
第i+1方：验证Ri合法性后，计算Ri+1=fd(di+1, Ri)；
将Ri+1和C2, C3发送至下一方
验证失败
… …
验证失败
第m方：验证Rm-1合法性后，
计算Rm=fd(dm, Rm-1)；
将Rm和C2, C3发送至明文计算方
验证失败
明文计算方：验证R=Rm-G=(x, y)合法性后：
计算：t = KDF(x||y||klen);
计算：M=C2 ⊕ t;
计算：u = Hash(x||M||y)，并检证u是否等于C3;
验证失败
m方联合解密完成，
得到明文M
m方联合解密失败

图1

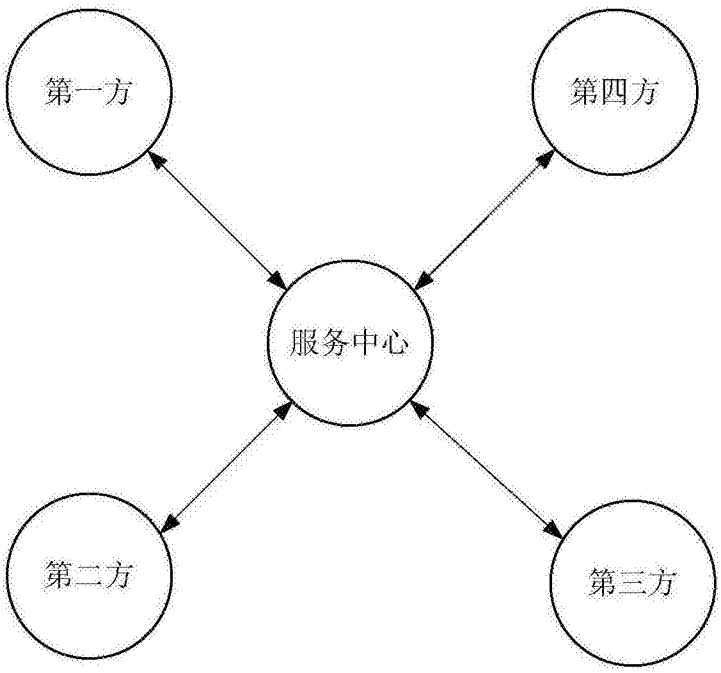


图2