(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 112713989 A
(43)申请公布日 2021.04.27

(21)申请号 201911023614.0

(22)申请日 2019.10.25

(71)申请人 航天信息股份有限公司
地址 100195 北京市海淀区杏石口路甲18号航天信息园

(72)发明人 宁红宙 赵永宽 魏国 龚征 马昌社

(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
代理人 潘雪

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

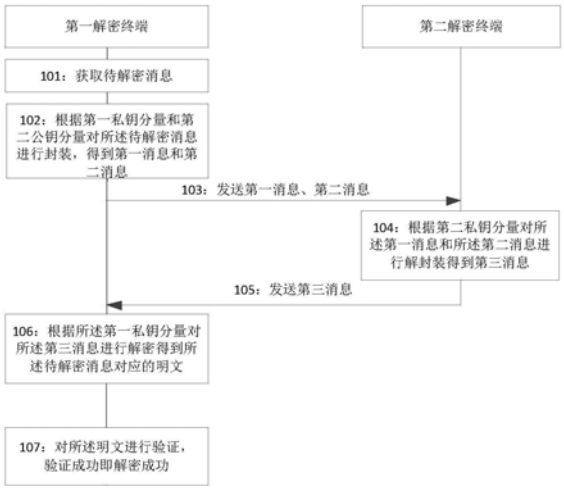
权利要求书3页 说明书9页 附图2页

(54)发明名称

一种解密方法及装置

(57)摘要

本申请实施例中提供了一种解密方法及装置，该方法包括：第一解密终端获取待解密消息；所述第一解密终端根据第一私钥分量和第二公钥分量对所述待解密消息进行封装，得到第一消息和第二消息；将所述第一消息和所述第二消息发送给所述第二解密终端，以使所述第二解密终端根据第二私钥分量对所述第一消息和所述第二消息进行解封装得到第三消息，并将所述第三消息发送给所述第一解密终端；所述第一解密终端根据所述第一私钥分量对所述第三消息进行解密得到所述待解密消息对应的明文。第一解密终端和第二解密终端协同解密，解决了用户私钥单一存储一个解密终端上而易被他人非法盗取的问题，从而提升了用户信息的安全性。



CN 112713989 A

1.一种解密方法,其特征在于,包括:

第一解密终端获取待解密消息;

所述第一解密终端根据第一私钥分量和第二公钥分量对所述待解密消息进行封装,得到第一消息和第二消息;其中,所述第一私钥分量为所述第一解密终端设置的私钥分量,所述第二公钥分量为第二解密终端设置的公钥分量,所述第一解密终端与所述第二解密终端协同解密;

所述第一解密终端将所述第一消息和所述第二消息发送给所述第二解密终端,以使所述第二解密终端根据第二私钥分量对所述第一消息和所述第二消息进行解封装得到第三消息,并将所述第三消息发送给所述第一解密终端,所述第二私钥分量为所述第二解密终端设置的私钥分量;

所述第一解密终端根据所述第一私钥分量对所述第三消息进行解密得到所述待解密消息对应的明文。

2.如权利要求1所述的方法,其特征在于,所述第一解密终端根据第一私钥分量和第二公钥分量对所述待解密消息进行封装,确定第一消息和第二消息,包括:

从所述待解密消息中提取C_1,所述C_1为椭圆曲线上的非无穷远点,所述椭圆曲线是由加密方选择的对所述明文进行加密的曲线;

根据如下公式确定所述第一消息和所述第二消息:

$C_{A1}=C_1+[u]G$,$u\in[1,n-1]$;

$C_{A2}=[u]W_S+[(hd_A)^{-1}\bmod n]C_1$;

其中,所述C_{A1}为所述第一消息,所述C_{A2}为所述第二消息,所述G为所述椭圆曲线上的基点,所述u为随机数发生器产生的随机数,所述n为所述椭圆曲线的基点的阶数,所述[u]G为所述随机数与所述基点的点乘运算,所述W_S为所述第二公钥分量,所述hd_A为所述第一私钥分量;所述$(hd_A)^{-1}\bmod n$为所述hd_A的逆进行求余运算。

3.如权利要求1所述的方法,其特征在于,所述第二解密终端根据所述第二私钥分量对所述第一消息和所述第二消息进行解封装得到第三消息,包括:

根据如下公式得到所述第三消息:

$SC_1=[hd_S]C_{A1}-C_{A2}$;

其中,所述SC_1为所述第三消息,所述hd_s为所述第二私钥分量,所述C_{A1}为所述第一消息,所述C_{A2}为所述第二消息。

4.如权利要求1所述的方法,其特征在于,所述第一解密终端根据所述第一私钥分量对所述第三消息进行解密得到明文,包括:

提取所述待解密消息中的C_3,所述C_3为所述待解密消息中的密文内容;

根据如下公式得到所述明文:

$(x_1,y_1)=[hd_A]SC_1$;

$$M=C_3\oplus KDF(x_1||y_1,klen);$$

所述$KDF(x_1||y_1,klen)$表示根据密钥派生函数对$x_1||y_1$进行处理,所述$x_1||y_1$表示对所述x_1与所述y_1进行拼接处理,所述klen为所述待解密消息的比特长度;所述M为所述明文。

5.如权利要求4所述的方法,其特征在于,所述方法还包括:

根据如下公式计算出所述明文的校验码:

$v=Hash(x_1||M||y_1)$；

其中，所述v为所述明文的校验码，所述$Hash(x_1||M||y_1)$为采用哈希函数对拼接之后的所述M和所述x_1及所述y_1进行处理；

获取所述待解密消息中的C_2，所述C_2为所述待解密消息的校验码；

若所述v与所述C_2相同，则输出所述明文。

6.一种解密装置，其特征在于，所述装置包括：

获取模块，用于获取待解密消息；

处理模块，用于根据第一私钥分量和第二公钥分量对所述待解密消息进行封装，得到第一消息和第二消息；其中，所述第一私钥分量为所述第一解密终端设置的私钥分量，所述第二公钥分量为第二解密终端设置的公钥分量，所述第一解密终端与所述第二解密终端协同解密；

通信模块，用于将所述第一消息和所述第二消息发送给所述第二解密终端；

所述处理模块，还用于根据第二私钥分量对所述第一消息和所述第二消息进行解封装得到第三消息，所述第二私钥分量为所述第二解密终端设置的私钥分量；

所述通信模块，还用于将所述第三消息发送给所述第一解密终端；

所述处理模块，还用于根据所述第一私钥分量对所述第三消息进行解密得到所述待解密消息对应的明文。

7.如权利要求6所述的装置，其特征在于，所述处理模块用于根据第一私钥分量和第二公钥分量对所述待解密消息进行封装，得到第一消息和第二消息，具体用于：

从所述待解密消息中提取C_1，所述C_1为椭圆曲线上的非无穷远点，所述椭圆曲线是由加密方选择的对所述明文进行加密的曲线；

根据如下公式确定所述第一消息和所述第二消息：

$C_{A1}=C_1+[u]G, u\in[1,n-1]$；

$C_{A2}=[u]W_S+[(hd_A)^{-1} \bmod n]C_1$；

其中，所述C_{A1}为所述第一消息，所述C_{A2}为所述第二消息，所述G为所述椭圆曲线上的基点，所述u为随机数发生器产生的随机数，所述n为所述椭圆曲线的基点的阶数，所述[u]G为所述随机数与所述基点的点乘运算，所述W_S为所述第二公钥分量，所述hd_A为所述第一私钥分量；所述$(hd_A)^{-1} \bmod n$为所述hd_A的逆进行求余运算。

8.如权利要求6所述的装置，其特征在于，所述处理模块用于根据第二私钥分量对所述第一消息和所述第二消息进行解封装得到第三消息，具体用于：

根据如下公式得到所述第三消息：

$SC_1=[hd_S]C_{A1}-C_{A2}$；

其中，所述SC_1为所述第三消息，所述hd_s为所述第二私钥分量，所述C_{A1}为所述第一消息，所述C_{A2}为所述第二消息。

9.如权利要求6所述的装置，其特征在于，所述处理模块用于根据所述第一私钥分量对所述第三消息进行解密得到所述待解密消息对应的明文，具体用于：

提取所述待解密消息中的C_3，所述C_3为所述待解密消息中的密文内容；

根据如下公式得到所述明文：

$(x_1,y_1)=[hd_A]SC_1$；

$$M = C_3 \oplus KDF(x_1||y_1, klen);$$

所述KDF(x_1||y_1,klen)表示根据密钥派生函数对x_1||y_1进行处理,所述x_1||y_1表示对所述x_1与所述y_1进行拼接处理,所述klen为所述待解密消息的比特长度;所述C_3为所述待解密消息中的密文内容,所述M为所述明文。

10.如权利要求9所述的装置,其特征在于,所述处理模块还用于:

根据如下公式计算出所述明文的校验码:

v＝Hash(x_1||M||y_1);

其中,所述v为所述明文的校验码,所述Hash(x_1||M||y_1)为采用哈希函数对拼接之后的所述M和所述x_1及所述y_1进行处理;

获取所述待解密消息中的C_2,所述C_2为所述待解密消息的校验码;

若所述v与所述C_2相同,则输出所述明文。

一种解密方法及装置

技术领域

[0001] 本发明涉及加解密技术领域，特别涉及一种解密方法及装置。

背景技术

[0002] 随着智能终端技术、移动互联技术和云计算技术的发展，越来越多的互联网络应用开始迁往智能移动终端，如：用于手机终端的支付宝、微信、网银等，使得用户在移动终端过程中，随时随地的都可以使用移动终端进行支付、购物、发送网络消息等。

[0003] 由于移动终端系统的开放性，存储于移动终端系统中的用于解密文件的密钥容易被窃取。因此，如果仅依靠单一移动终端系统存储解密密钥的话，解密密钥被窃取的可能性较大。

发明内容

[0004] 本发明实施例的目的是提供一种解密方法及装置，用以解决现有技术中存在的用户私钥单一存储在移动智能终端的存储卡上，容易被非法人员盗取，导致用户信息安全性不高的问题。

[0005] 本发明实施例中提供的具体技术方案如下：

[0006] 第一方面，本申请实施例提供了一种解密方法，包括：

[0007] 第一解密终端获取待解密消息；

[0008] 所述第一解密终端根据第一私钥分量和第二公钥分量对所述待解密消息进行封装，得到第一消息和第二消息；其中，所述第一私钥分量为所述第一解密终端设置的私钥分量，所述第二公钥分量为第二解密终端设置的公钥分量，所述第一解密终端与所述第二解密终端协同解密；

[0009] 所述第一解密终端将所述第一消息和所述第二消息发送给所述第二解密终端，以使所述第二解密终端根据第二私钥分量对所述第一消息和所述第二消息进行解封装得到第三消息，并将所述第三消息发送给所述第一解密终端，所述第二私钥分量为所述第二解密终端设置的私钥分量；

[0010] 所述第一解密终端根据所述第一私钥分量对所述第三消息进行解密得到所述待解密消息对应的明文。

[0011] 可选的，所述第一解密终端根据第一私钥分量和第二公钥分量对所述待解密消息进行封装，确定第一消息和第二消息，包括：

[0012] 从所述待解密消息中提取C_1，所述C_1为椭圆曲线上的非无穷远点，所述椭圆曲线是由加密方选择的对所述明文进行加密的曲线；

[0013] 根据如下公式确定所述第一消息和所述第二消息：

[0014] $C_{A1}=C_1+[u]G, u\in[1,n-1]$；

[0015] $C_{A2}=[u]W_S+[(hd_A)^{-1}\bmod n]C_1$；

[0016] 其中，所述C_{A1}为所述第一消息，所述C_{A2}为所述第二消息，所述G为所述椭圆曲线上

的基点，所述u为随机数发生器产生的随机数，所述n为所述椭圆曲线的基点的阶数，所述[u]G为所述随机数与所述基点的点乘运算，所述W_S为所述第二公钥分量，所述hd_A为所述第一私钥分量；所述$(hd_A)^{-1}$mod n为所述hd_A的逆进行求余运算。

[0017] 可选的，所述第二解密终端根据所述第二私钥分量对所述第一消息和所述第二消息进行解封装得到第三消息，包括：

[0018] 根据如下公式得到所述第三消息：

[0019] $SC_1=[hd_S]C_{A1}-C_{A2}$；

[0020] 其中，所述SC_1为所述第三消息，所述hd_S为所述第二私钥分量，所述C_{A1}为所述第一消息，所述C_{A2}为所述第二消息。

[0021] 可选的，所述第一解密终端根据所述第一私钥分量对所述第三消息进行解密得到明文，包括：

[0022] 根据如下公式得到所述明文：

[0023] 提取所述待解密消息中的C_3，所述C_3为所述待解密消息中的密文内容；

[0024] $(x_1,y_1)=[hd_A]SC_1$；

[0025] $$M = C_3 \oplus KDF(x_1||y_1, klen);$$

[0026] 所述KDF(x_1||y_1,klen)表示根据密钥派生函数对x_1||y_1进行处理，所述x_1||y_1表示对所述x_1与所述y_1进行拼接处理，所述klen为所述待解密消息的比特长度；所述M为所述明文。

[0027] 可选的，所述方法还包括：

[0028] 根据如下公式计算出所述明文的校验码：

[0029] v=Hash(x_1||M||y_1)；

[0030] 其中，所述v为所述明文的校验码，所述Hash(x_1||M||y_1)为采用哈希函数对拼接之后的所述M和所述x_1及所述y_1进行处理；

[0031] 获取所述待解密消息中的C_2，所述C_2为所述待解密消息的校验码；

[0032] 若所述v与所述C_2相同，则输出所述明文。

[0033] 第二方面，本申请实施例提供了一种解密装置，所述装置包括：

[0034] 获取模块，用于获取待解密消息；

[0035] 处理模块，用于根据第一私钥分量和第二公钥分量对所述待解密消息进行封装，得到第一消息和第二消息；其中，所述第一私钥分量为所述第一解密终端设置的私钥分量，所述第二公钥分量为第二解密终端设置的公钥分量，所述第一解密终端与所述第二解密终端协同解密；

[0036] 通信模块，用于将所述第一消息和所述第二消息发送给所述第二解密终端；

[0037] 所述处理模块，还用于根据第二私钥分量对所述第一消息和所述第二消息进行解封装得到第三消息，所述第二私钥分量为所述第二解密终端设置的私钥分量；

[0038] 所述通信模块，还用于将所述第三消息发送给所述第一解密终端；

[0039] 所述处理模块，还用于根据所述第一私钥分量对所述第三消息进行解密得到所述待解密消息对应的明文。

[0040] 可选的，所述处理模块用于根据第一私钥分量和第二公钥分量对所述待解密消息进行封装，得到第一消息和第二消息，具体用于：

[0041] 从所述待解密消息中提取C_1,所述C_1为椭圆曲线上的非无穷远点,所述椭圆曲线是由加密方选择的对所述明文进行加密的曲线;

[0042] 根据如下公式确定所述第一消息和所述第二消息:

[0043] $C_{A1}=C_1+[u]G,u\in[1,n-1]$;

[0044] $C_{A2}=[u]W_S+[(hd_A)^{-1}\bmod n]C_1$;

[0045] 其中,所述C_{A1}为所述第一消息,所述C_{A2}为所述第二消息,所述G为所述椭圆曲线上的基点,所述u为随机数发生器产生的随机数,所述n为所述椭圆曲线的基点的阶数,所述[u]G为所述随机数与所述基点的点乘运算,所述W_S为所述第二公钥分量,所述hd_A为所述第一私钥分量;所述$(hd_A)^{-1}\bmod n$为所述hd_A的逆进行求余运算。

[0046] 可选的,所述处理模块用于根据第二私钥分量对所述第一消息和所述第二消息进行解封装得到第三消息,具体用于:

[0047] 根据如下公式得到所述第三消息:

[0048] $SC_1=[hd_S]C_{A1}-C_{A2}$;

[0049] 其中,所述SC_1为所述第三消息,所述hd_S为所述第二私钥分量,所述C_{A1}为所述第一消息,所述C_{A2}为所述第二消息。

[0050] 可选的,所述处理模块用于根据所述第一私钥分量对所述第三消息进行解密得到所述待解密消息对应的明文,具体用于:

[0051] 提取所述待解密消息中的C_3,所述C_3为所述待解密消息中的密文内容;

[0052] 根据如下公式得到所述明文:

[0053] $(x_1,y_1)=[hd_A]SC_1$;

[0054] $$M = C_3 \oplus KDF(x_1||y_1, klen);$$

[0055] 所述$KDF(x_1||y_1,klen)$表示根据密钥派生函数对$x_1||y_1$进行处理,所述$x_1||y_1$表示对所述x_1与所述y_1进行拼接处理,所述klen为所述待解密消息的比特长度;所述C_3为所述待解密消息中的密文内容,所述M为所述明文。

[0056] 可选的,所述处理模块还用于:

[0057] 根据如下公式计算出所述明文的校验码:

[0058] $v=Hash(x_1||M||y_1)$;

[0059] 其中,所述v为所述明文的校验码,所述$Hash(x_1||M||y_1)$为采用哈希函数对拼接之后的所述M和所述x_1及所述y_1进行处理;

[0060] 获取所述待解密消息中的C_2,所述C_2为所述待解密消息的校验码;

[0061] 若所述v与所述C_2相同,则输出所述明文。第三方面,本申请实施例提供一种计算机可读存储介质,所述计算机可读存储介质存储有计算机程序,所述计算机程序包括程序指令,所述程序指令当被计算机执行时,使所述计算机执行如上述方法的一个或多个步骤。

[0062] 第四方面,本申请实施例提供一种程序产品,所述程序产品包括程序指令,所述程序指令当被计算机执行时,使所述计算机执行如上述方法的一个或多个步骤。

[0063] 本发明有益效果如下:

[0064] 在本申请实施例中提供的技术方案中,第一解密终端和第二解密终端协同解密,将各个解密终端自身产生相应的私钥分量,并分别存储在本地,且任何一方解密终端均无法仅根据本地存储的私钥分量推算出另一解密终端本地存储的私钥分量,在采用私钥进行

解密时，需要两个私钥分量共同做计算才能完成解密操作，解决了用户私钥单一存储一个解密终端上而易被他人非法盗取的问题，从而提升了用户信息的安全性。

附图说明

[0065] 为了更清楚地说明本申请实施例或现有技术中的技术方案，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申请的一些实施例。

[0066] 图1为本发明实施例提供的一种解密方法的流程示意图；

[0067] 图2为本发明实施例中的用户手机和服务器双方协同进行解密计算的流程图；

[0068] 图3为本发明实施例提供的一种解密装置的结构示意图。

具体实施方式

[0069] 为使本申请的目的、技术方案和优点更加清楚明白，下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，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，都属于本申请保护的范围。在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互任意组合。并且，虽然在流程图中示出了逻辑顺序，但是在某些情况下，能够以不同于此处的顺序执行所示出或描述的步骤。

[0070] 本申请的说明书和权利要求书及上述附图中的术语“第一”和“第二”是用于区别不同对象，而非用于描述特定顺序。此外，术语“包括”以及它们任何变形，意图在于覆盖不排他的保护。例如包含了一系列步骤或单元的过程、方法、系统、产品或设备没有限定于已列出的步骤或单元，而是可选地还包括没有列出的步骤或单元，或可选地还包括对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0071] 另外，本文中术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A和/或B，可以表示：单独存在A，同时存在A和B，单独存在B这三种情况。另外，本文中字符“/”，在不做特别说明的情况下，一般表示前后关联对象是一种“或”的关系。

[0072] 为了解决现有技术中存在的用户私钥存储在单一解密终端的存储卡上，容易被非法人员盗取的问题，本发明实施例中提供了一种解密方法及装置，该方法为：第一解密终端获取待解密消息；所述第一解密终端根据第一私钥分量和第二公钥分量对所述待解密消息进行封装，得到第一消息和第二消息；其中，所述第一私钥分量为所述第一解密终端设置的私钥分量，所述第二公钥分量为第二解密终端设置的公钥分量，所述第一解密终端与所述第二解密终端协同解密；将所述第一消息和所述第二消息发送给所述第二解密终端，以使所述第二解密终端根据第二私钥分量对所述第一消息和所述第二消息进行解封装得到第三消息，并将所述第三消息发送给所述第一解密终端，所述第二私钥分量为所述第二解密终端设置的私钥分量；所述第一解密终端根据所述第一私钥分量对所述第三消息进行解密得到所述待解密消息对应的明文。

[0073] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，并不是全部的实施例。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。

[0074] 下面将通过具体实施例对本发明的方案进行详细描述，当然，本发明并不限于以下实施例。

[0075] 参阅图1所示，图1为流程示意图，本发明实施例中，一种解密方法的详细流程如下：

[0076] 101：第一解密终端获取待解密消息。

[0077] 在具体的实施例中，在第一解密终端获取待解密消息之前，加密终端基于椭圆曲线SM2算法中的公钥加密算法部分对明文进行加密。

[0078] 实际应用中，椭圆曲线参数采用国家密码管理局规定的SM2曲线参数，设椭圆曲线为E(Fq)，其中，Fq包含q个元素的素域，E(Fq)为Fq上椭圆曲线E所有有理点(包括无穷远点O)组成的集合，G为椭圆曲线E上的一个基点，存在最小的正整数n使得数乘nG为无穷远点，则将n称为G的阶，n为素数，用[k]P表示椭圆上的点乘运算，k为正整数，P为椭圆曲线上的一个点，椭圆曲线上的P点均可以通过基点与公钥的点乘运算得到。

[0079] 加密终端根据选定的椭圆曲线对消息M加密后取得的密文为$C=C_1||C_2||C_3$。例如，假设第一解密终端是移动端，移动端获取到的待解密消息即是密文$C=C_1||C_2||C_3$。

[0080] 本发明实施例中，各个解密终端预先通过随机数发生器产生自己的私钥分量，并根据各自的私钥分量确定各自的公钥分量，并分别存储至各个解密终端本地。

[0081] 由于在非对称密钥加密系统中，需要使用不同的密钥来分别完成加密和解密操作，一个公开发布，即公开密钥(本发明实施例中简称为公钥)，另一个由用户自己秘密保存，即私用密钥(本发明实施例中简称为私钥)，信息发送者用公钥去加密，而信息接收者则用私钥去解密。

[0082] 具体的，本发明实施例中，解密终端可以包括第一解密终端和第二解密终端，那么，可以将第一解密终端产生的私钥分量、公钥分量分别定义为第一私钥分量，第一公钥分量；第二解密终端产生的私钥分量、公钥分量分别定义为第二私钥分量、第二公钥分量，较佳的，第一解密终端将第一私钥分量、第一公钥分量存储在本地，第二解密终端将第二私钥分量、第二公钥分量存储在本地，本发明实施例中，为了更好的保证用户使用私钥的安全性，第一解密终端和第二解密终端中有一方为不需要满足便携性要求的解密终端(如服务器端)，这样，就能在服务器端采用各种安全技术和手段，以保障存储在服务器端本地的私钥分量的安全性，相应的提高用户使用私钥的安全性。

[0083] 例如，假设第一解密终端是用户手机，第二解密终端是服务器，用户手机通过随机数发生器产生的第一私钥分量，根据第一私钥分量确定第一公钥分量，并存储在用户手机本地；服务器端通过随机数发生器产生的第二私钥分量，并根据第二私钥分量确定第二公钥分量，并存储在服务器端本地；且用户手机和服务器端中任何一方均无法仅根据自身存储的私钥分量推算出另一方存储的私钥分量，用户手机和服务器端可通过第一私钥分量和第二私钥分量共同计算出相应的公共公钥，并公开发布，那么，加密终端在确定需要向用户发送消息时，利用公共公钥采用椭圆曲线公钥加密算法对消息进行加密处理，得到相应的待解密消息，并将密文发送给用户手机，用户手机在接收到密文后，若需要对密文进行解密计算，则需要与服务器端通过第一私钥分量和第二私钥分量共同完成解密计算，进一步的，

由于服务器端不需要满足便携性要求，故可以针对存储在服务器端的第二私钥分量，采用各种安全技术和手段，以保障第二私钥分量的安全性，这样，就相应的提升了用户手机信息的安全性。

[0084] 102：所述第一解密终端根据第一私钥分量和第二公钥分量对所述待解密消息进行封装，得到第一消息和第二消息；其中，所述第一私钥分量为存储在所述第一解密终端的私钥分量，所述第二公钥分量为存储在第二解密终端的公钥分量，所述第一解密终端与所述第二解密终端协同解密；

[0085] 可选的，所述第一解密终端根据第一私钥分量和第二公钥分量对所述待解密消息进行封装，确定第一消息和第二消息，包括：

[0086] 从所述待解密消息中提取C_1；

[0087] 所述C_1为椭圆曲线上的非无穷远点，所述椭圆曲线是由加密方选择的对所述明文进行加密的曲线；

[0088] 根据如下公式确定所述第一消息和所述第二消息：

[0089] $C_{A1}=C_1+[u]G, u\in[1,n-1]$；

[0090] $C_{A2}=[u]W_S+[(hd_A)^{-1} \bmod n]C_1$；

[0091] 其中，所述C_{A1}为所述第一消息，所述C_{A2}为所述第二消息，所述G为所述椭圆曲线上的基点，所述u为随机数发生器产生的随机数，所述n为所述椭圆曲线的基点的阶数，所述[u]G为所述随机数与所述基点的点乘运算，所述W_S为所述第二公钥分量，所述hd_A为所述第一私钥分量；

[0092] 所述$(hd_A)^{-1} \bmod n$为所述hd_A的逆进行求余运算。

[0093] 在本申请的实施例中，第一解密终端通过随机数发生器确定第一私钥分量，第二解密终端通过随机数发生器确定第二私钥分量和第二公钥分量之后，第二解密终端将第二公钥分量发送给第一解密终端，第一解密终端根据第一私钥分量和第二公钥分量对点C_1进行处理得到C_{A1}和C_{A2}。第一解密终端从所述待解密消息即密文C中提取出比特串C_1，并将C_1的数据类型转换为在椭圆曲线上的点C_1的坐标，并计算第一解密终端随机数发生器产生的随机数与所述基点的点乘运算，进一步得到第一消息C_{A1}；对所述C_1与所述第一私钥分量的模逆运算值的进行点乘运算得到$[(hd_A)^{-1} \bmod n]C_1$，进一步根据第二公钥分量得到第二消息C_{A2}。

[0094] 103：将所述第一消息和所述第二消息发送给所述第二解密终端；

[0095] 具体的，第一解密终端将上述第一消息和第二消息发送至第二解密终端，即将C_{A1}和C_{A2}发送给第二解密终端。假设第一解密终端是用户手机，第二解密终端是服务器端，即用户手机将封装得到的第一消息和第二消息发送服务器端，以使服务器端进行进一步解密计算。

[0096] 104：所述第二解密终端根据第二私钥分量对所述第一消息和所述第二消息进行解封装得到第三消息，所述第二私钥分量为存储在所述第二解密终端的私钥分量；

[0097] 可选的，所述第二解密终端根据所述第二私钥分量对所述第一消息和所述第二消息进行解封装得到第三消息，包括：根据如下公式得到所述第三消息：

[0098] $SC_1=[hd_S]C_{A1}-C_{A2}$；

[0099] 其中，所述SC_1为所述第三消息，所述hd_S为所述第二私钥分量，所述C_{A1}为所述第一

消息，所述C_{A2}为所述第二消息。

[0100] 具体的，第二解密终端采用上述第二私钥分量对上述第一消息和第二消息进行解封装计算得到第三消息，例如，利用hd_S与C_{A1}的点乘运算减C_{A2}得到SC_1。

[0101] 105：将所述第三消息发送给所述第一解密终端；

[0102] 具体的，在第二解密终端根据第二私钥分量对所述第一消息和第二消息进行解封装之后得到SC_1，将SC_1发送给第一解密终端。

[0103] 106：所述第一解密终端根据所述第一私钥分量对所述第三消息进行解密得到所述待解密消息对应的明文。

[0104] 可选的，所述第一解密终端根据所述第一私钥分量对所述第三消息进行解密得到明文，具体根据以下公式得到：

[0105] $(x_1,y_1)=[hd_A]SC_1$；

[0106] $$M = C_3 \oplus KDF(x_1||y_1, klen);$$

[0107] 所述KDF($x_1||y_1$,klen)表示根据密钥派生函数对$x_1||y_1$进行处理，所述$x_1||y_1$表示对所述x_1所述y_1进行拼接处理，klen为所述待解密消息的比特长度；所述C_3为所述待解密消息中的密文内容，所述M为所述明文。

[0108] 示例性的，例如，假设x_1是1101，y_1是0010，x_1和y_1拼接之后是11010010。

[0109] 107：对所述明文进行验证，验证成功即解密成功。

[0110] 可选的，所述第一解密终端根据所述第一私钥分量对所述第三消息进行解密得到所述待解密消息对应的明文，还包括：根据如下公式计算出所述明文的校验码：

[0111] $v=Hash(x_1||M||y_1)$；

[0112] 其中，所述v为所述明文的校验码，所述$Hash(x_1||M||y_1)$采用密码杂凑函数对拼接之后的所述M和所述x_1及所述y_1进行相应处理；

[0113] 若所述明文的校验码与所述待解密消息的校验码相同，则输出所述明文。

[0114] 具体的，在本申请的实施例中，所述第一解密终端根据所述第一私钥分量对所述第三消息进行解密得到所述待解密消息对应的明文，具体包括：第一解密终端在接收到第二解密终端发送的第三消息SC_1后，将第一私钥分量hd_A和第三消息SC_1的点乘，作为椭圆曲线上的点坐标$(x_1,y_1)=[hd_A]SC_1$，并将坐标x_1，y_1的数据类型转换为比特串；采用密钥派生函数对拼接之后的x_1与y_1进行处理，得到t，其中，$t=KDF(x_1||y_1,klen)$；从密文中提取出密文内容C_3，并将C_3和t做异或处理，得到解密后的明文M，其中，$M = C_3 \oplus KDF(x_1||y_1, klen)$即采用哈希函数对拼接之后的所述M和所述$x_1$及所述$y_1$进行相应处理，计算出验证码v，其中，$v=Hash(x_1||M||y_1)$从密文C中提取出验证码$C_2$，并判断v与$C_2$是否相同，并在判定结果为是时，确定解密成功，输出明文M。

[0115] 以下介绍一个完整的实施例。

[0116] 假设第一解密终端是用户手机，第二解密终端是服务器端，参见图2所示，图2为本发明实施例中的手机和服务器双方协同进行解密计算的流程图；

[0117] 用户手机和服务器需要根据第一私钥分量和第二私钥分量预先计算出相应的公钥。假设用户手机通过随机数发生器产生的第一私钥分量为hd_A，并根据第一私钥分量确定第一公钥分量$W_A=[hd_A]G$，并将第一私钥分量和第一公钥分量存储在本地的；服务器通过随

机数发生器产生的第二私钥分量$hd_S \in [1,n-1]$，根据第二私钥分量确定第二公钥分量$W_S = [hd_S]G$，并将第二私钥分量和第二公钥分量存储在本地；其中，$hd_A, hd_S \in [1,n-1]$；用户手机根据第一私钥分量hd_A及第二公钥分量计算公共公钥$P_A = [hd_A]W_S - G$。

[0118] 用户手机通过随机数发生器确定第一私钥分量，服务器通过随机数发生器确定第二私钥分量和第二公钥分量之后，服务器将第二公钥分量发送给用户手机。

[0119] 步骤1：获取待解密消息。

[0120] 加密终端基于椭圆曲线公钥加密算法对消息M进行加密处理，输出密文$C = C_1||C_2||C_3$，密文C包括椭圆曲线上的点C_1，校验码C_2和密文内容C_3。

[0121] 步骤2：从待解密消息中提取出C_1，用户手机根据第一私钥分量和第二公钥分量对点C_1进行处理得到C_{A1}和C_{A2}。

[0122] 用户手机获取密文C，用户手机从所述待解密消息即密文C中提取出比特串C_1，并将C_1的数据类型转换为在椭圆曲线上的点C_1的坐标。

[0123] 步骤3：用户手机将上述第一消息和第二消息发送至服务器，即将C_{A1}和C_{A2}发送给服务器。

[0124] 步骤4：服务器采用上述第二私钥分量对上述第一消息和第二消息进行解封装计算得到第三消息，例如，利用hd_S与C_{A1}的点乘运算减C_{A2}得到SC_1。

[0125] 步骤5：将SC_1发送给用户手机。

[0126] 步骤6：所述用户手机根据所述第一私钥分量对所述第三消息进行解密得到所述待解密消息对应的明文，具体包括：用户手机在接收到服务器发送的第三消息SC_1后，将第一私钥分量hd_A和第三消息SC_1的点乘，作为椭圆曲线上的点坐标$(x_1,y_1) = [hd_A]SC_1$，并将坐标x_1, y_1的数据类型转换为比特串；采用密钥派生函数对$x_1||y_1$进行处理，得到t，其中，$t = KDF(x_1||y_1, klen)$，$x_1||y_1$表示所述x_1与所述y_1拼接在一起，klen为C_3的比特长度；从密文C中提取出C_3，并将C_3和t做异或处理，得到解密后的明文M，其中，$M = C_3 \oplus KDF(x_1||y_1, klen)$。

[0127] 步骤7：对所述明文进行验证。

[0128] 采用哈希函数对拼接之后的所述M和所述x_1及所述y_1进行相应处理，计算出验证码v，其中，$v = Hash(x_1||M||y1)$；从密文C中提取出校验码C_2，并判断v与C_2是否相同，并在判定结果为是时，确定解密成功，输出明文M。

[0129] 基于同一发明构思，本发明实施例还提供了一种基于椭圆曲线的解密计算装置(如，第一解密终端)，请参见图3，图3为本申请提供基于椭圆曲线的解密计算装置的结构示意图，该装置包括接获取模块301，处理模块302，通信模块303；

[0130] 获取模块301，用于获取待解密消息；

[0131] 处理模块302，用于根据第一私钥分量和第二公钥分量对所述待解密消息进行封装，得到第一消息和第二消息；其中，所述第一私钥分量为所述第一解密终端设置的私钥分量，所述第二公钥分量为第二解密终端设置的公钥分量，所述第一解密终端与所述第二解密终端协同解密；

[0132] 通信模块303，用于将所述第一消息和所述第二消息发送给所述第二解密终端；

[0133] 所述处理模块302，还用于根据第二私钥分量对所述第一消息和所述第二消息进行解封装得到第三消息，所述第二私钥分量为所述第二解密终端设置的私钥分量；

[0134] 所述通信模块303，还用于将所述第三消息发送给所述第一解密终端；

[0135] 所述处理模块302，还用于根据所述第一私钥分量对所述第三消息进行解密得到所述待解密消息对应的明文。

[0136] 本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0137] 本发明是参照根据本发明实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0138] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0139] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0140] 尽管已描述了本发明的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本发明范围的所有变更和修改。

[0141] 显然，本领域的技术人员可以对本发明实施例进行各种改动和变型而不脱离本发明实施例的精神和范围。这样，倘若本发明实施例的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

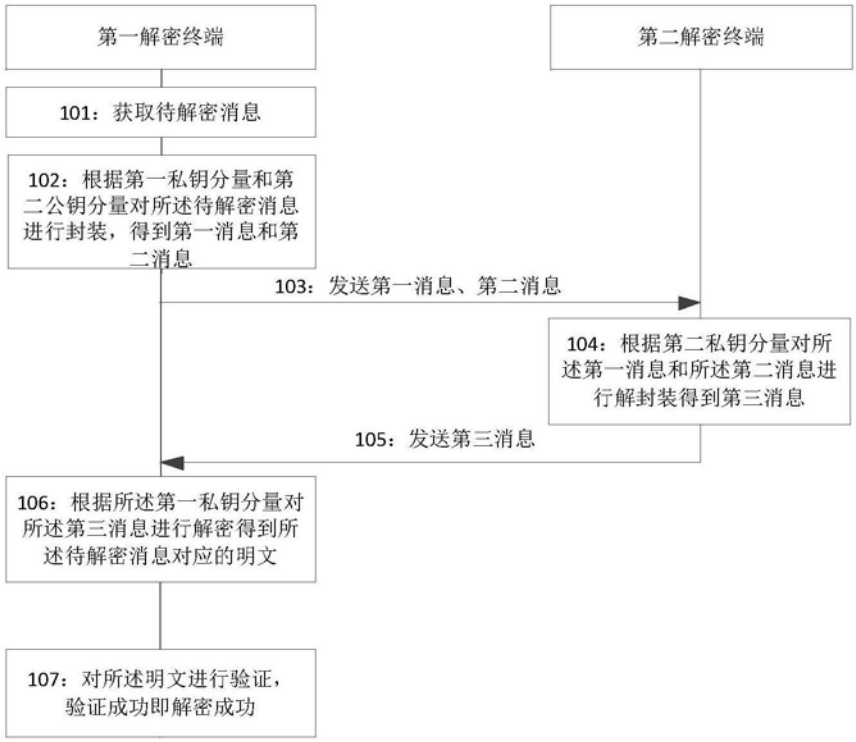

第一解密终端
第二解密终端
101：获取待解密消息
102：根据第一私钥分量和第二公钥分量对所述待解密消息进行封装，得到第一消息和第二消息
103：发送第一消息、第二消息
104：根据第二私钥分量对所述第一消息和所述第二消息进行解封装得到第三消息
105：发送第三消息
106：根据所述第一私钥分量对所述第三消息进行解密得到所述待解密消息对应的明文
107：对所述明文进行验证，验证成功即解密成功

图1

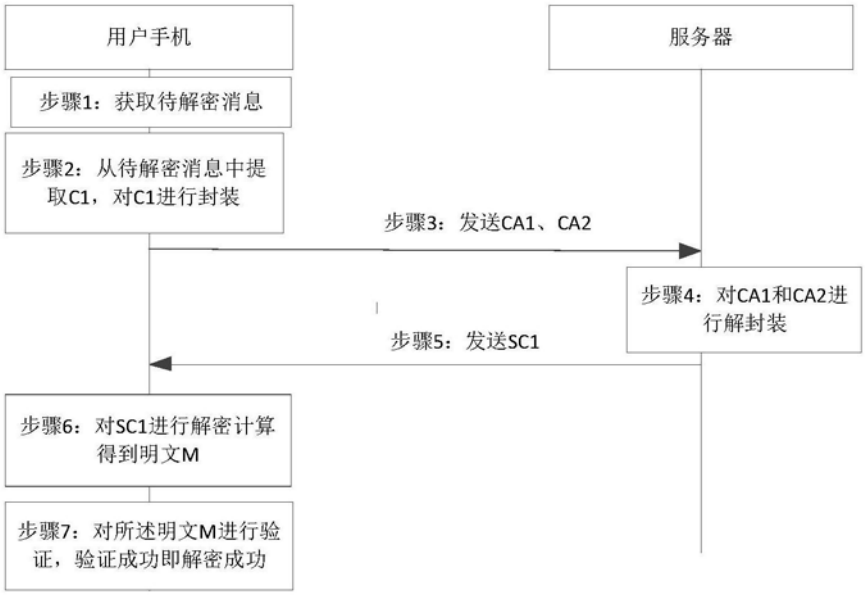

用户手机
服务器
步骤1：获取待解密消息
步骤2：从待解密消息中提取C1，对C1进行封装
步骤3：发送CA1、CA2
步骤4：对CA1和CA2进行解封装
步骤5：发送SC1
步骤6：对SC1进行解密计算得到明文M
步骤7：对所述明文M进行验证，验证成功即解密成功

图2

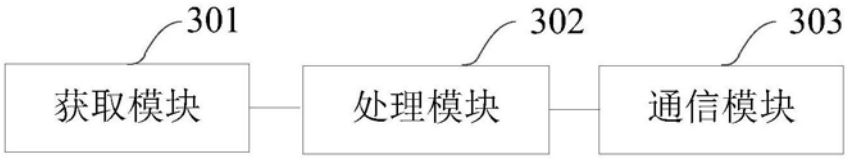


图3