



(12)发明专利申请

(10)申请公布号 CN 109242591 A

(43)申请公布日 2019.01.18

(21)申请号 201810791705.8

(22)申请日 2018.07.18

(71)申请人 中国联合网络通信集团有限公司
地址 100033 北京市西城区金融大街21号

(72)发明人 刘牧洲 王湘宁 严斌峰

(74)专利代理机构 北京同立钧成知识产权代理有限公司 11205
代理人 孙静 刘芳

(51)Int.Cl.

G06Q 30/06(2012.01)

G07F 17/00(2006.01)

H04L 29/06(2006.01)

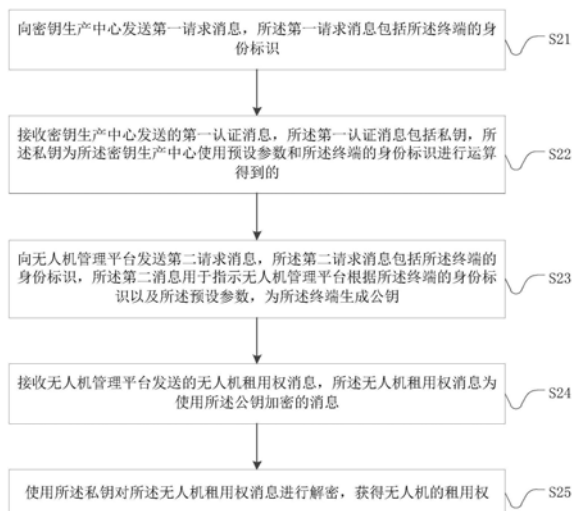
权利要求书3页 说明书11页 附图9页

(54)发明名称

共享无人机的租用方法、设备及系统

(57)摘要

本发明提供一种共享无人机的租用方法、设备及系统,终端通过向密钥生产中心发送第一请求消息,所述第一请求消息中包括所述终端的身份标识,以使密钥生产中心为所述终端生成私钥;通过向无人机管理平台发送第二请求消息,所述第二请求消息包括所述终端的身份标识,以使无人机管理平台可以为所述终端生成公钥;进而无人机管理平台使用公钥对无人机租用权消息进行加密,终端使用私钥对无人机租用权消息进行解密,获得无人机的租用权。通过上述过程,保证了无人机管理平台与终端之间消息的安全性,避免被外界攻击。



1. 一种共享无人机的租用方法,其特征在于,应用于终端,包括:
 - 向密钥生产中心发送第一请求消息,所述第一请求消息包括所述终端的身份标识;
 - 接收密钥生产中心发送的第一认证消息,所述第一认证消息包括私钥,所述私钥为所述密钥生产中心使用预设参数和所述终端的身份标识进行运算得到的;
 - 向无人机管理平台发送第二请求消息,所述第二请求消息包括所述终端的身份标识,所述第二消息用于指示无人机管理平台根据所述终端的身份标识以及所述预设参数,为所述终端生成公钥;
 - 接收无人机管理平台发送的无人机租用权消息,所述无人机租用权消息为使用所述公钥加密的消息;
 - 使用所述私钥对所述无人机租用权消息进行解密,获得无人机的租用权。
2. 根据权利要求1所述的方法,其特征在于,所述第一请求消息还包括携带有效期的令牌,所述令牌用于指示密钥生产中心在所述令牌的有效期内,为所述终端生成私钥;
 - 相应的,所述第一认证消息中还包括所述携带有效期的令牌。
3. 根据权利要求2所述的方法,其特征在于,所述接收密钥生产中心发送的第一认证消息之后,还包括:
 - 向所述密钥生产中心发送确认消息,所述确认消息中包括所述携带有效期的令牌。
4. 一种共享无人机的租用方法,其特征在于,应用于密钥生产中心,包括:
 - 接收终端发送的第一请求消息,所述第一请求消息包括所述终端的身份标识;
 - 使用预设参数和所述终端的身份标识进行运算,为所述终端生成私钥;
 - 向所述终端发送第一认证消息,所述第一认证消息中包括所述私钥,所述私钥用于所述终端对从无人机管理平台接收的无人机租用权消息进行解密。
5. 根据权利要求4所述的方法,其特征在于,所述第一消息中还包括携带有效期的令牌;
 - 相应的,所述使用预设参数和所述终端的身份标识进行运算,为所述终端生成私钥,包括:
 - 在所述令牌的有效期内,使用预设参数和所述终端的身份标识进行运算,为所述终端生成私钥;
 - 所述第一认证消息中还包括所述携带有效期的令牌。
6. 根据权利要求5所述的方法,其特征在于,所述向所述终端发送第一认证消息之后,还包括:
 - 接收所述终端发送的确认消息,所述确认消息中包括所述携带有效期的令牌。
7. 根据权利要求4-6任一项所述的方法,其特征在于,还包括:
 - 向无人机管理平台发送第二认证消息,所述第二认证消息包括所述预设参数。
8. 一种共享无人机的租用方法,其特征在于,应用于无人机管理平台,包括:
 - 接收终端发送的第二请求消息,所述第二请求消息包括所述终端的身份标识;
 - 根据预设参数和所述终端的身份标识,为所述终端生成公钥;
 - 使用所述公钥对无人机租用权消息进行加密;
 - 向所述终端发送所述无人机租用权消息,以使所述终端使用私钥对所述无人机租用权消息进行解密,获取无人机的租用权;其中,所述私钥为所述密钥生产中心使用所述预设参

数和所述终端的身份标识进行运算得到的。

9. 根据权利要求8所述的方法,其特征还在于,还包括:

接收密钥生产中心发送的第二认证消息,所述第二认证消息中包括所述预设参数。

10. 一种共享无人机的租用装置,其特征还在于,应用于终端,包括:

发送模块,用于向密钥生产中心发送第一请求消息,所述第一请求消息包括所述终端的身份标识;

接收模块,用于接收密钥生产中心发送的第一认证消息,所述第一认证消息包括私钥,所述私钥为所述密钥生产中心使用预设参数和所述终端的身份标识进行运算得到的;

所述发送模块,还用于向无人机管理平台发送第二请求消息,所述第二请求消息包括所述终端的身份标识,所述第二消息用于指示无人机管理平台根据所述终端的身份标识以及所述预设参数,为所述终端生成公钥;

所述接收模块,还用于接收无人机管理平台发送的无人机租用权消息,所述无人机租用权消息为使用所述公钥加密的消息;

解密模块,用于使用所述私钥对所述无人机租用权消息进行解密,获得无人机的租用权。

11. 一种共享无人机的租用装置,其特征还在于,应用于密钥生产中心,包括:

接收模块,用于接收终端发送的第一请求消息,所述第一请求消息包括所述终端的身份标识;

处理模块,用于使用预设参数和所述终端的身份标识进行运算,为所述终端生成私钥;

发送模块,用于向所述终端发送第一认证消息,所述第一认证消息中包括所述私钥,所述私钥用于所述终端对从无人机管理平台接收的无人机租用权消息进行解密。

12. 一种共享无人机的租用装置,其特征还在于,应用于无人机管理平台,包括:

接收模块,用于接收终端发送的第二请求消息,所述第二请求消息包括所述终端的身份标识;

处理模块,用于根据预设参数和所述终端的身份标识,为所述终端生成公钥;

加密模块,用于使用所述公钥对无人机租用权消息进行加密;

发送模块,用于向所述终端发送所述无人机租用权消息,以使所述终端使用私钥对所述无人机租用权消息进行解密,获取无人机的租用权;其中,所述私钥为所述密钥生产中心使用所述预设参数和所述终端的身份标识进行运算得到的。

13. 一种终端,其特征还在于,包括:

存储器;

处理器;以及

计算机程序;

其中,所述计算机程序存储在所述存储器中,并被配置为由所述处理器执行以实现如权利要求1-3任一项所述的方法。

14. 一种密钥生产中心,其特征还在于,包括:

存储器;

处理器;以及

计算机程序;

其中,所述计算机程序存储在所述存储器中,并被配置为由所述处理器执行以实现如权利要求4-7任一项所述的方法。

15. 一种无人机管理平台,其特征在于,包括:

存储器;

处理器;以及

计算机程序;

其中,所述计算机程序存储在所述存储器中,并被配置为由所述处理器执行以实现如权利要求8或9所述的方法。

16. 一种计算机可读存储介质,其特征在于,其上存储有计算机程序,所述计算机程序被处理器执行以实现如权利要求1-3任一项所述的方法,或者,如权利要求4-7任一项所述的方法,或者,如权利要求8或9所述的方法。

17. 一种共享无人机的租用系统,其特征在于,包括:如权利要求13所述的终端、如权利要求14所述的密钥生产中心、如权利要求15所述的无人机管理平台。

共享无人机的租用方法、设备及系统

技术领域

[0001] 本发明涉及通信技术领域,尤其涉及一种共享无人机的租用方法、设备及系统。

背景技术

[0002] 在众多的应用领域中,无人机展现出了与相关行业相结合的迅猛发展势头。例如,无人机已应用在农林保值、电力及石油管线巡检、应急通讯、气象监测、矿产勘探和边境巡逻等诸多领域中,并且带来了客观的经济效益。目前,随着共享经济的发展,共享无人机也走入人们的生活。例如,在湖北已投入共享无人机开展飞防植保任务,并实现了上万亩次的飞防植保面积。

[0003] 目前,用户在使用共享无人机时,可以通过用户终端APP、扫描二维码等方式登录无人机管理平台,然后将个人信息以及租用信息录入后,无人机管理平台将共享无人机的租用权信息返回给用户。

[0004] 但是,上述的共享无人机租用流程中,用户终端与无人机管理平台的交互信息的安全性无法保障,存在被攻击的可能。

发明内容

[0005] 本发明提供一种共享无人机的租用方法、设备及系统,采用基于标识的加密技术,无人机管理平台使用公钥对无人机租用权消息进行加密,终端使用私钥对无人机租用权消息进行解密,保证了无人机管理平台与终端之间消息的安全性,避免被外界攻击。

[0006] 第一方面,本发明提供的共享无人机的租用方法,应用于终端,包括:

[0007] 向密钥生产中心发送第一请求消息,所述第一请求消息包括所述终端的身份标识;

[0008] 接收密钥生产中心发送的第一认证消息,所述第一认证消息包括私钥,所述私钥为所述密钥生产中心使用预设参数和所述终端的身份标识进行运算得到的;

[0009] 向无人机管理平台发送第二请求消息,所述第二请求消息包括所述终端的身份标识,所述第二消息用于指示无人机管理平台根据所述终端的身份标识以及所述预设参数,为所述终端生成公钥;

[0010] 接收无人机管理平台发送的无人机租用权消息,所述无人机租用权消息为使用所述公钥加密的消息;

[0011] 使用所述私钥对所述无人机租用权消息进行解密,获得无人机的租用权。

[0012] 可选的,所述第一请求消息还包括携带有效期的令牌,所述令牌用于指示密钥生产中心在所述令牌的有效期内,为所述终端生成私钥;

[0013] 相应的,所述第一认证消息中还包括所述携带有效期的令牌。

[0014] 可选的,所述接收密钥生产中心发送的第一认证消息之后,还包括:

[0015] 向所述密钥生产中心发送确认消息,所述确认消息中包括所述携带有效期的令牌。

- [0016] 第二方面,本发明提供的共享无人机的租用方法,应用于密钥生产中心,包括:
- [0017] 接收终端发送的第一请求消息,所述第一请求消息包括所述终端的身份标识;
- [0018] 使用预设参数和所述终端的身份标识进行运算,为所述终端生成私钥;
- [0019] 向所述终端发送第一认证消息,所述第一认证消息中包括所述私钥,所述私钥用于所述终端对从无人机管理平台接收的无人机租用权消息进行解密。
- [0020] 可选的,所述第一消息中还包括携带有效期的令牌;
- [0021] 相应的,所述使用预设参数和所述终端的身份标识进行运算,为所述终端生成私钥,包括:
- [0022] 在所述令牌的有效期内,使用预设参数和所述终端的身份标识进行运算,为所述终端生成私钥;
- [0023] 所述第一认证消息中还包括所述携带有效期的令牌。
- [0024] 可选的,所述向所述终端发送第一认证消息之后,还包括:
- [0025] 接收所述终端发送的确认消息,所述确认消息中包括所述携带有效期的令牌。
- [0026] 可选的,所述方法还包括:
- [0027] 向无人机管理平台发送第二认证消息,所述第二认证消息包括所述预设参数。
- [0028] 第三方面,本发明提供的共享无人机的租用方法,应用于无人机管理平台,包括:
- [0029] 接收终端发送的第二请求消息,所述第二请求消息包括所述终端的身份标识;
- [0030] 根据预设参数和所述终端的身份标识,为所述终端生成公钥;
- [0031] 使用所述公钥对无人机租用权消息进行加密;
- [0032] 向所述终端发送所述无人机租用权消息,以使所述终端使用私钥对所述无人机租用权消息进行解密,获取无人机的租用权;其中,所述私钥为所述密钥生产中心使用所述预设参数和所述终端的身份标识进行运算得到的。
- [0033] 可选的,所述方法还包括:
- [0034] 接收密钥生产中心发送的第二认证消息,所述第二认证消息中包括所述预设参数。
- [0035] 第四方面,本发明提供的共享无人机的租用装置,应用于终端,包括:
- [0036] 发送模块,用于向密钥生产中心发送第一请求消息,所述第一请求消息包括所述终端的身份标识;
- [0037] 接收模块,用于接收密钥生产中心发送的第一认证消息,所述第一认证消息包括私钥,所述私钥为所述密钥生产中心使用预设参数和所述终端的身份标识进行运算得到的;
- [0038] 所述发送模块,还用于向无人机管理平台发送第二请求消息,所述第二请求消息包括所述终端的身份标识,所述第二消息用于指示无人机管理平台根据所述终端的身份标识以及所述预设参数,为所述终端生成公钥;
- [0039] 所述接收模块,还用于接收无人机管理平台发送的无人机租用权消息,所述无人机租用权消息为使用所述公钥加密的消息;
- [0040] 解密模块,用于使用所述私钥对所述无人机租用权消息进行解密,获得无人机的租用权。
- [0041] 可选的,所述第一请求消息还包括携带有效期的令牌,所述令牌用于指示密钥生

产中心在所述令牌的有效期内,为所述终端生成私钥;

[0042] 相应的,所述第一认证消息中还包括所述携带有效期的令牌。

[0043] 可选的,所述发送模块,还用于向所述密钥生产中心发送确认消息,所述确认消息中包括所述携带有效期的令牌。

[0044] 第五方面,本发明提供的共享无人机的租用装置,应用于密钥生产中心,包括:

[0045] 接收模块,用于接收终端发送的第一请求消息,所述第一请求消息包括所述终端的身份标识;

[0046] 处理模块,用于使用预设参数和所述终端的身份标识进行运算,为所述终端生成私钥;

[0047] 发送模块,用于向所述终端发送第一认证消息,所述第一认证消息中包括所述私钥,所述私钥用于所述终端对从无人机管理平台接收的无人机租用权消息进行解密。

[0048] 可选的,所述第一消息中还包括携带有效期的令牌;

[0049] 相应的,所述处理模块,具体用于在所述令牌的有效期内,使用预设参数和所述终端的身份标识进行运算,为所述终端生成私钥;

[0050] 所述第一认证消息中还包括所述携带有效期的令牌。

[0051] 可选的,所述接收模块,还用于接收所述终端发送的确认消息,所述确认消息中包括所述携带有效期的令牌。

[0052] 可选的,所述发送模块,还用于向无人机管理平台发送第二认证消息,所述第二认证消息包括所述预设参数。

[0053] 第六方面,本发明提供的共享无人机的租用装置,应用于无人机管理平台,包括:

[0054] 接收模块,用于接收终端发送的第二请求消息,所述第二请求消息包括所述终端的身份标识;

[0055] 处理模块,用于根据预设参数和所述终端的身份标识,为所述终端生成公钥;

[0056] 加密模块,用于使用所述公钥对无人机租用权消息进行加密;

[0057] 发送模块,用于向所述终端发送所述无人机租用权消息,以使所述终端使用私钥对所述无人机租用权消息进行解密,获取无人机的租用权;其中,所述私钥为所述密钥生产中心使用所述预设参数和所述终端的身份标识进行运算得到的。

[0058] 可选的,所述接收模块,还用于接收密钥生产中心发送的第二认证消息,所述第二认证消息中包括所述预设参数。

[0059] 第七方面,本发明提供的终端,包括:

[0060] 存储器;

[0061] 处理器;以及

[0062] 计算机程序;

[0063] 其中,所述计算机程序存储在所述存储器中,并被配置为由所述处理器执行以实现如第一方面任一项所述的方法。

[0064] 第八方面,本发明提供的密钥生产中心,包括:

[0065] 存储器;

[0066] 处理器;以及

[0067] 计算机程序;

[0068] 其中,所述计算机程序存储在所述存储器中,并被配置为由所述处理器执行以实现如第二方面任一项所述的方法。

[0069] 第九方面,本发明提供的无人机管理平台,包括:

[0070] 存储器;

[0071] 处理器;以及

[0072] 计算机程序;

[0073] 其中,所述计算机程序存储在所述存储器中,并被配置为由所述处理器执行以实现如第三方面任一项所述的方法。

[0074] 第十方面,本发明提供的计算机可读存储介质,其上存储有计算机程序,所述计算机程序被处理器执行以实现如第一方面任一项所述的方法,或者,如第二方面任一项所述的方法,或者,如第三方面任一项所述的方法。

[0075] 第十一方面,本发明提供的共享无人机的租用系统,包括:如第七方面所述的终端、如第八方面所述的密钥生产中心、如第九方面所述的无人机管理平台。

[0076] 本发明提供的共享无人机的租用方法、设备及系统,终端通过向密钥生产中心发送第一请求消息,所述第一请求消息中包括所述终端的身份标识,以使密钥生产中心为所述终端生成私钥;通过向无人机管理平台发送第二请求消息,所述第二请求消息包括所述终端的身份标识,以使无人机管理平台可以为所述终端生成公钥;进而无人机管理平台使用公钥对无人机租用权消息进行加密,终端使用私钥对无人机租用权消息进行解密,获得无人机的租用权。通过上述过程,保证了无人机管理平台与终端之间消息的安全性,避免被外界攻击。

附图说明

[0077] 为了更清楚地说明本发明实施例或现有技术中的技术方案,下面将对实施例或现有技术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性的前提下,还可以根据这些附图获得其他的附图。

[0078] 图1为本发明提供的共享无人机的租用系统的架构图;

[0079] 图2为本发明提供的共享无人机的租用方法实施例一的流程图;

[0080] 图3A为本发明提供的共享无人机的租用方法实施例二的流程图;

[0081] 图3B为本发明提供的共享无人机的租用方法实施例二的信令流程图;

[0082] 图4A为本发明提供的共享无人机的租用方法实施例三的流程;

[0083] 图4B为本发明提供的共享无人机的租用方法实施例三的信令流程图;

[0084] 图5为本发明提供的共享无人机的租用装置实施例一的结构示意图;

[0085] 图6为本发明提供的共享无人机的租用装置实施例二的结构示意图;

[0086] 图7为本发明提供的共享无人机的租用装置实施例三的结构示意图;

[0087] 图8为本发明提供的终端实施例的结构示意图;

[0088] 图9为本发明提供的密钥生产中心实施例的结构示意图;

[0089] 图10为本发明提供的无人机管理平台实施例的结构示意图;

[0090] 图11为本发明提供的共享无人机的租用系统实施例的结构示意图。

具体实施方式

[0091] 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,而不是全部的实施例。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。

[0092] 本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”、“第三”“第四”等(如果存在)是用于区别类似的对象,而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换,以便这里描述的本发明的实施例例如能够以除了在这里图示或描述的那些以外的顺序实施。此外,术语“包括”和“具有”以及他们的任何变形,意图在于覆盖不排他的包含,例如,包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元,而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0093] 本发明提供一种共享无人机的租用方法及系统,采用基于标识的加密技术,无人机管理平台使用公钥对无人机租用权消息进行加密,终端使用私钥对无人机租用权消息进行解密,保证了无人机管理平台与终端之间消息的安全性,避免被外界攻击。

[0094] 下面以具体地实施例对本发明的技术方案进行详细说明。下面这几个具体的实施例可以相互结合,对于相同或相似的概念或过程可能在某些实施例不再赘述。

[0095] 图1为本发明提供的共享无人机的租用系统的架构图,如图1所示,无人机租用系统包括:终端、无人机管理平台和密钥生产中心。其中,终端为用户使用的终端设备,其包括但不限于手机、平板电脑、笔记本电脑等电子设备;无人机管理平台为无人机管理服务器,可以接收终端的无人机租用请求,并向终端提供无人机租用权信息。密钥生产中心可以为密钥管理服务器,用于管理所有终端的公钥和私钥。

[0096] 现有技术中,用户在使用共享无人机时,可以通过用户终端APP、扫描二维码等方式登录无人机管理平台,然后将个人信息以及租用信息录入后,无人机管理平台将共享无人机的租用权信息返回给用户。但是,上述的共享无人机租用流程中,用户终端与无人机管理平台的交互信息的安全性无法保障,存在被攻击的可能。

[0097] 如图1所示,本发明提供的共享无人机的租用系统中,增加了密钥生产中心用于管理终端的公钥和私钥,使得无人机管理平台使用公钥对无人机租用权消息进行加密,终端使用私钥对无人机租用权消息进行解密,在终端与无人机管理平台之间构建安全的信息交互通道,保证了交互信息的安全性。

[0098] 图2为本发明提供的共享无人机的租用方法实施例一的流程图,本实施例的执行主体可以为图1中的终端。如图2所示,本实施例的方法,包括:

[0099] S21:向密钥生产中心发送第一请求消息,所述第一请求消息包括所述终端的身份标识。

[0100] S22:接收密钥生产中心发送的第一认证消息,所述第一认证消息包括私钥,所述私钥为所述密钥生产中心使用预设参数和所述终端的身份标识进行运算得到的。

[0101] 具体的,终端在获取共享无人机的租用权之前,需要首先通过第一请求消息向密钥生产中心获取私钥。其中,密钥生产中心可以为可信的第三方,密钥生产中心可以根据终端提供的身份标识,使用预设参数和预设算法进行运算,得到该终端的私钥,并通过第一认

证消息发送给终端,其中,所述预设参数可以在密钥生产中心初始化阶段根据预设算法生成。

[0102] 其中,终端向密钥生产中心发送第一请求消息的时机不作具体限定,其可以在获取共享无人机的租用权之前任何时刻进行。一种可选的实施方式中,终端在无人机管理平台进行注册时,向密钥生产中心发送第一请求消息。另一种可选的实施方式中,终端获取到无人机管理平台发送的无人机租用权消息后,发现该消息为加密消息且无对应的解密私钥时,向密钥生产中心发送第一请求消息以请求私钥。

[0103] 可选的,所述终端的身份标识为任意一串有意义的字符,包括但不限于:用户的email地址、手机号码、身份号码等。

[0104] S23:向无人机管理平台发送第二请求消息,所述第二请求消息包括所述终端的身份标识,所述第二消息用于指示无人机管理平台根据所述终端的身份标识以及所述预设参数,为所述终端生成公钥。

[0105] 具体的,本实施例中采用基于标识的加密方案,基于标识的加密方案采用的是非对称加密技术,以发送方A和接收方B通信过程为例,发送方A使用接收方B的公钥对明文进行加密得到密文,接收方B接收到密文后,使用接收方B的私钥对密文进行解密,得到明文。因此,本实施例中,终端向无人机管理平台发送第二请求消息,其中包括终端的身份标识,从而无人机管理平台可以根据终端的身份标识得到该终端对应的公钥,进而无人机管理平台可以根据终端的公钥对无人机租用权消息进行加密。

[0106] 其中,无人机管理平台可以根据预设参数和终端的身份标识进行运算,为终端生成公钥。所述预设参数为密钥生产中心为终端生成私钥时所使用的预设参数。本发明对于无人机管理平台获取所述预设参数的方法不作具体限定。一种可选的实施方式中,密钥生产中心在初始化阶段生成所述预设参数后,向无人机管理平台发送所述预设参数。另一种可选的实施方式中,无人机管理平台在需要使用所述预设参数时,向密钥生产中心发送请求消息进行获取。

[0107] 可以理解的,终端需要在向无人机管理平台申请租用权之前,向无人机管理平台发送第二请求消息,使得无人机管理平台能够及时得到该终端对应的公钥,进而能够在向终端发送无人机租用权消息时采用所述公钥进行加密。一种可选的实施方式中,终端在登录无人机管理平台时,向无人机管理平台发送第二请求消息。

[0108] S24:接收无人机管理平台发送的无人机租用权消息,所述无人机租用权消息为使用所述公钥加密的消息。

[0109] S25:使用所述私钥对所述无人机租用权消息进行解密,获得无人机的租用权。

[0110] 无人机管理平台为终端分配无人机的租用权后,使用公钥对无人机租用权消息进行加密发送给终端,终端使用私钥对无人机租用权消息进行解密,从而获取无人机的租用权。由于只有终端才拥有私钥,使得他人无法对无人机租用权消息进行攻击,保证了共享无人机的租用系统的消息交互的安全性。

[0111] 本实施例中,终端通过向密钥生产中心发送第一请求消息,所述第一请求消息中包括所述终端的身份标识,以使密钥生产中心为所述终端生成私钥;通过向无人机管理平台发送第二请求消息,所述第二请求消息包括所述终端的身份标识,以使无人机管理平台可以为所述终端生成公钥;进而无人机管理平台使用公钥对无人机租用权消息进行加密,

终端使用私钥对无人机租用权消息进行解密,获得无人机的租用权。通过上述过程,保证了无人机管理平台与终端之间消息的安全性,避免被外界攻击。

[0112] 图3A为本发明提供的共享无人机的租用方法实施例二的流程图,图3B为本发明提供的共享无人机的租用方法实施例二的信令流程图,结合图3A和图3B,本实施例对共享无人机的租用系统的交互过程进行详细描述。

[0113] 如图3A和图3B所示,本实施例的方法包括:

[0114] S31:终端向密钥生产中心发送第一请求消息,第一请求消息包括终端的身份标识。

[0115] S32:密钥生产中心使用预设参数和终端的身份标识进行运算,为终端生成私钥。

[0116] S33:密钥生产中心向终端发送第一认证消息,第一认证消息中包括私钥。

[0117] S34:终端向无人机管理平台发送第二请求消息,第二请求消息包括终端的身份标识。

[0118] S35:无人机管理平台根据预设参数和终端的身份标识,为终端生成公钥。

[0119] S36:无人机管理平台使用公钥对无人机租用权消息进行加密。

[0120] S37:无人机管理平台向终端发送无人机租用权消息。

[0121] S38:终端使用私钥对无人机租用权消息进行解密,获取无人机的租用权。

[0122] 本实施例的具体实施过程可参见上述实施例一的详细描述,此处不再赘述。

[0123] 另外,需要说明的是,本实施例中示例的是其中一种场景下的共享无人机的租用系统中的消息交互过程。可以理解的,本发明对于上述步骤的执行顺序并不作具体限定,上述各个步骤可以根据具体的应用场景具有不同的执行顺序。

[0124] 可选的,本实施例中的S35之前,还可以包括:密钥生产中心向无人机管理平台发送第二认证消息,所述第二认证消息包括所述预设参数。

[0125] 需要说明的是,上述步骤可以在S25之前的任意位置执行,本发明对此并不作具体限定。

[0126] 本实施例中,终端通过向密钥生产中心发送第一请求消息,所述第一请求消息中包括所述终端的身份标识,以使密钥生产中心为所述终端生成私钥;通过向无人机管理平台发送第二请求消息,所述第二请求消息包括所述终端的身份标识,以使无人机管理平台可以为所述终端生成公钥;进而无人机管理平台使用公钥对无人机租用权消息进行加密,终端使用私钥对无人机租用权消息进行解密,获得无人机的租用权。通过上述过程,保证了无人机管理平台与终端之间消息的安全性,避免被外界攻击。

[0127] 图4A为本发明提供的共享无人机的租用方法实施例三的流程,图4B为本发明提供的共享无人机的租用方法实施例三的信令流程图,在上述实施例的基础上,本实施例对终端获取私钥的过程进行更详细的描述。

[0128] 如图4A和图4B所示,本实施例的方法包括:

[0129] S41:终端向密钥生产中心发送第一请求消息,所述第一请求消息包括所述终端的身份标识以及携带有效期的令牌。

[0130] S42:密钥生产中心在所述令牌的有效期内,使用预设参数和所述终端的身份标识进行运算,为所述终端生成私钥。

[0131] S43:密钥生产中心向所述终端发送第一认证消息,所述第一认证消息中包括所述

私钥以及所述携带有效期的令牌。

[0132] S44:终端向所述密钥生产中心发送确认消息,所述确认消息中包括所述携带有效期的令牌。

[0133] 在上述实施例的基础上,本实施例的方法中,终端在向密钥生产中心发送第一请求消息时,在所述第一请求消息中还包括携带有效期的令牌,使得密钥生产中心在该令牌的有效期内为终端生成私钥,并在该令牌的有效期内向终端发送第一认证消息,进而终端在该令牌的有效期内向密钥生产中心发送确认消息。

[0134] 本实施例中,通过加入令牌机制,能够进一步提高共享无人机租用系统中消息交互的安全性。具体的,一方面,可以通过对令牌有效期的时长进行合理设置,使得在该令牌的有效期内,他人无法进行攻击。例如,终端可以根据网络状态为令牌设置一个较短的有效期,使得他人在该较短的有效期内无法进行网络攻击。另一方面,终端和密钥生产中心还可以根据令牌的有效期,确定网络的安全性。例如,若终端发送第一请求消息后,在令牌的有效期内,没有收到对应的第一认证消息,则可以重新发送第一请求消息,以使密钥生产中心为终端重新分配私钥。

[0135] 图5为本发明提供的共享无人机的租用装置实施例一的结构示意图,本实施例的装置可设置于终端中。如图5所示,本实施例的共享无人机的租用装置500,可以包括:发送模块501、接收模块502和解密模块503。

[0136] 其中,发送模块501,用于向密钥生产中心发送第一请求消息,所述第一请求消息包括所述终端的身份标识。

[0137] 接收模块502,用于接收密钥生产中心发送的第一认证消息,所述第一认证消息包括私钥,所述私钥为所述密钥生产中心使用预设参数和所述终端的身份标识进行运算得到的。

[0138] 发送模块501,还用于向无人机管理平台发送第二请求消息,所述第二请求消息包括所述终端的身份标识,所述第二消息用于指示无人机管理平台根据所述终端的身份标识以及所述预设参数,为所述终端生成公钥。

[0139] 接收模块502,还用于接收无人机管理平台发送的无人机租用权消息,所述无人机租用权消息为使用所述公钥加密的消息。

[0140] 解密模块503,用于使用所述私钥对所述无人机租用权消息进行解密,获得无人机的租用权。

[0141] 可选的,所述第一请求消息还包括携带有效期的令牌,所述令牌用于指示密钥生产中心在所述令牌的有效期内,为所述终端生成私钥;相应的,所述第一认证消息中还包括所述携带有效期的令牌。

[0142] 可选的,发送模块501,还用于向所述密钥生产中心发送确认消息,所述确认消息中包括所述携带有效期的令牌。

[0143] 本实施例的共享无人机的租用装置,可用于执行上述任一方法实施例中终端侧的技术方案,其实现原理和技术效果类似,此处不再赘述。

[0144] 图6为本发明提供的共享无人机的租用装置实施例二的结构示意图,本实施例的装置可设置于密钥生产中心。如图6所示,本实施例的共享无人机的租用装置600,可以包括:接收模块601、处理模块602和发送模块603。

[0145] 其中,接收模块601,用于接收终端发送的第一请求消息,所述第一请求消息包括所述终端的身份标识。

[0146] 处理模块602,用于使用预设参数和所述终端的身份标识进行运算,为所述终端生成私钥。

[0147] 发送模块603,用于向所述终端发送第一认证消息,所述第一认证消息中包括所述私钥,所述私钥用于所述终端对从无人机管理平台接收的无人机租用权消息进行解密。

[0148] 可选的,所述第一消息中还包括携带有效期的令牌;相应的,处理模块602,具体用于在所述令牌的有效期内,使用预设参数和所述终端的身份标识进行运算,为所述终端生成私钥;所述第一认证消息中还包括所述携带有效期的令牌。

[0149] 可选的,接收模块601,还用于接收所述终端发送的确认消息,所述确认消息中包括所述携带有效期的令牌。

[0150] 可选的,发送模块603,还用于向无人机管理平台发送第二认证消息,所述第二认证消息包括所述预设参数。

[0151] 本实施例的共享无人机的租用装置,可用于执行上述任一方法实施例中密钥生产中心侧的技术方案,其实现原理和技术效果类似,此处不再赘述。

[0152] 图7为本发明提供的共享无人机的租用装置实施例三的结构示意图,本实施例的装置可设置于无人机管理平台中。如图7所示,本实施例的共享无人机的租用装置700,可以包括:接收模块701、处理模块702、加密模块703和发送模块704。

[0153] 接收模块701,用于接收终端发送的第二请求消息,所述第二请求消息包括所述终端的身份标识。

[0154] 处理模块702,用于根据预设参数和所述终端的身份标识,为所述终端生成公钥。

[0155] 加密模块703,用于使用所述公钥对无人机租用权消息进行加密。

[0156] 发送模块704,用于向所述终端发送所述无人机租用权消息,以使所述终端使用私钥对所述无人机租用权消息进行解密,获取无人机的租用权;其中,所述私钥为所述密钥生产中心使用所述预设参数和所述终端的身份标识进行运算得到的。

[0157] 可选的,接收模块701,还用于接收密钥生产中心发送的第二认证消息,所述第二认证消息中包括所述预设参数。

[0158] 本实施例的共享无人机的租用装置,可用于执行上述任一方法实施例中的无人机管理平台侧的技术方案,其实现原理和技术效果类似,此处不再赘述。

[0159] 图8为本发明提供的终端实施例的结构示意图,如图8所示,本实施例的终端800,可以包括:存储器801、处理器802和计算机程序,其中,所述计算机程序存储在存储器801中,并被配置为由处理器802执行以实现上述任一方法实施例中终端侧的技术方案,其实现原理和技术效果类似,此处不再赘述。

[0160] 图9为本发明提供的密钥生产中心实施例的结构示意图,如图9所示,本实施例的密钥生产中心900,可以包括:存储器901、处理器902和计算机程序,其中,所述计算机程序存储在存储器901中,并被配置为由处理器902执行以实现上述任一方法实施例中密钥生产中心侧的技术方案,其实现原理和技术效果类似,此处不再赘述。

[0161] 图10为本发明提供的无人机管理平台实施例的结构示意图,如图10所示,本实施例的无人机管理平台1000,可以包括:存储器1001、处理器1002和计算机程序,其中,所述计

计算机程序存储在存储器1001中,并被配置为由处理器1002执行以实现上述任一方法实施例中无人机管理平台侧的技术方案,其实现原理和技术效果类似,此处不再赘述。

[0162] 本发明实施例还提供一种计算机可读存储介质,其上存储有计算机程序,所述计算机程序被处理器执行,可以实现上述任一方法实施例中终端侧的技术方案,或者,可以实现上述任一方法实施例中密钥生产中心侧的技术方案,或者,可以实现上述任一方法实施例中无人机管理平台侧的技术方案,其实现原理和技术效果类似,此处不再赘述。

[0163] 图11为本发明提供的共享无人机的租用系统实施例的结构示意图,如图11所示,本实施例的共享无人机的租用系统1100,可以包括:终端1101、密钥生产中心1102和无人机管理平台1103,其中,终端1101可以采用如图8所示的结构,密钥生产中心1102可以采用如图9所示的结构,无人机管理平台1103可以采用如图10所示的结构。本实施例的共享无人机的租用系统,可用于执行上述任一方法实施例的技术方案,其实现原理和技术效果类似,此处不再赘述。

[0164] 本实施例的手语翻译的系统,可用于执行上述任一方法实施例中的技术方案,其实现原理和技术效果类似,此处不再赘述。

[0165] 在本发明所提供的几个实施例中,应该理解到,所揭露的装置和方法,可以通过其它的方式实现。例如,以上所描述的装置实施例仅仅是示意性的,例如,单元的划分,仅仅为一种逻辑功能划分,实际实现时可以有另外的划分方式,例如多个单元或组件可以结合或者可以集成到另一个系统,或一些特征可以忽略,或不执行。另一点,所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口,装置或单元的间接耦合或通信连接,可以是电性,机械或其它的形式。

[0166] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0167] 另外,在本发明各个实施例中的各功能单元可以集成在一个处理单元中,也可以是各个单元单独物理存在,也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现,也可以采用硬件加软件功能单元的形式实现。

[0168] 上述以软件功能单元的形式实现的集成的单元,可以存储在一个计算机可读存储介质中。上述软件功能单元存储在一个存储介质中,包括若干指令用以使得一台计算机设备(可以是个人计算机,服务器,或者网络设备等)或处理器(英文:processor)执行本发明各个实施例所述方法的部分步骤。而前述的存储介质包括:U盘、移动硬盘、只读存储器(英文:Read-Only Memory,简称:ROM)、随机存取存储器(英文:Random Access Memory,简称:RAM)、磁碟或者光盘等各种可以存储程序代码的介质。

[0169] 在上述网络设备或者终端设备的实施例中,应理解,处理器可以是中央处理单元(英文:Central Processing Unit,简称:CPU),还可以是其他通用处理器、数字信号处理器(英文:Digital Signal Processor,简称:DSP)、专用集成电路(英文:Application Specific Integrated Circuit,简称:ASIC)等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本申请所公开的方法的步骤可以直接体现为硬件处理器执行完成,或者用处理器中的硬件及软件模块组合执行完成。

[0170] 最后应说明的是：以上各实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述各实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分或者全部技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的范围。

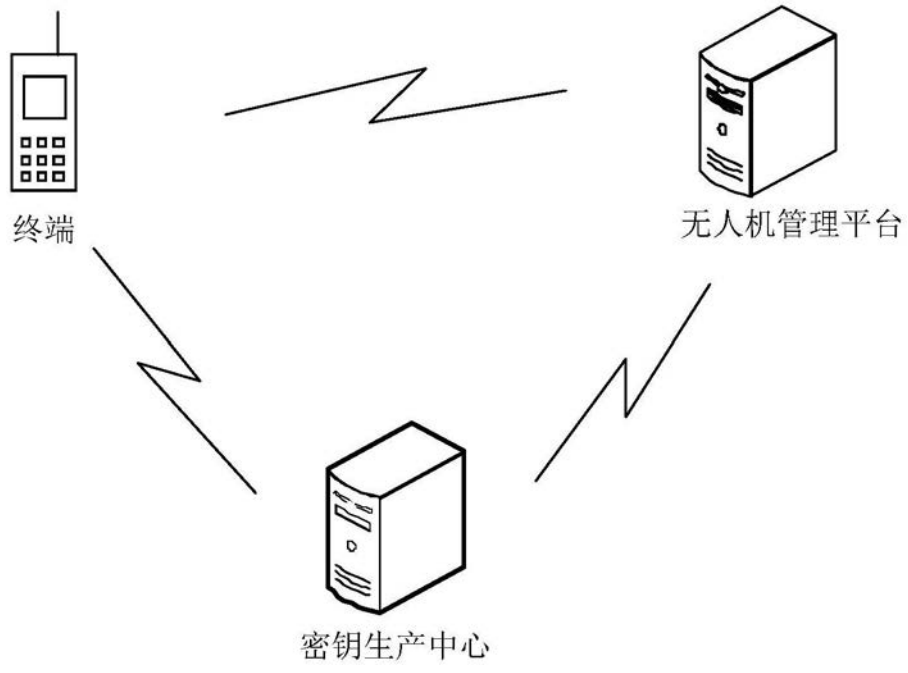


图1

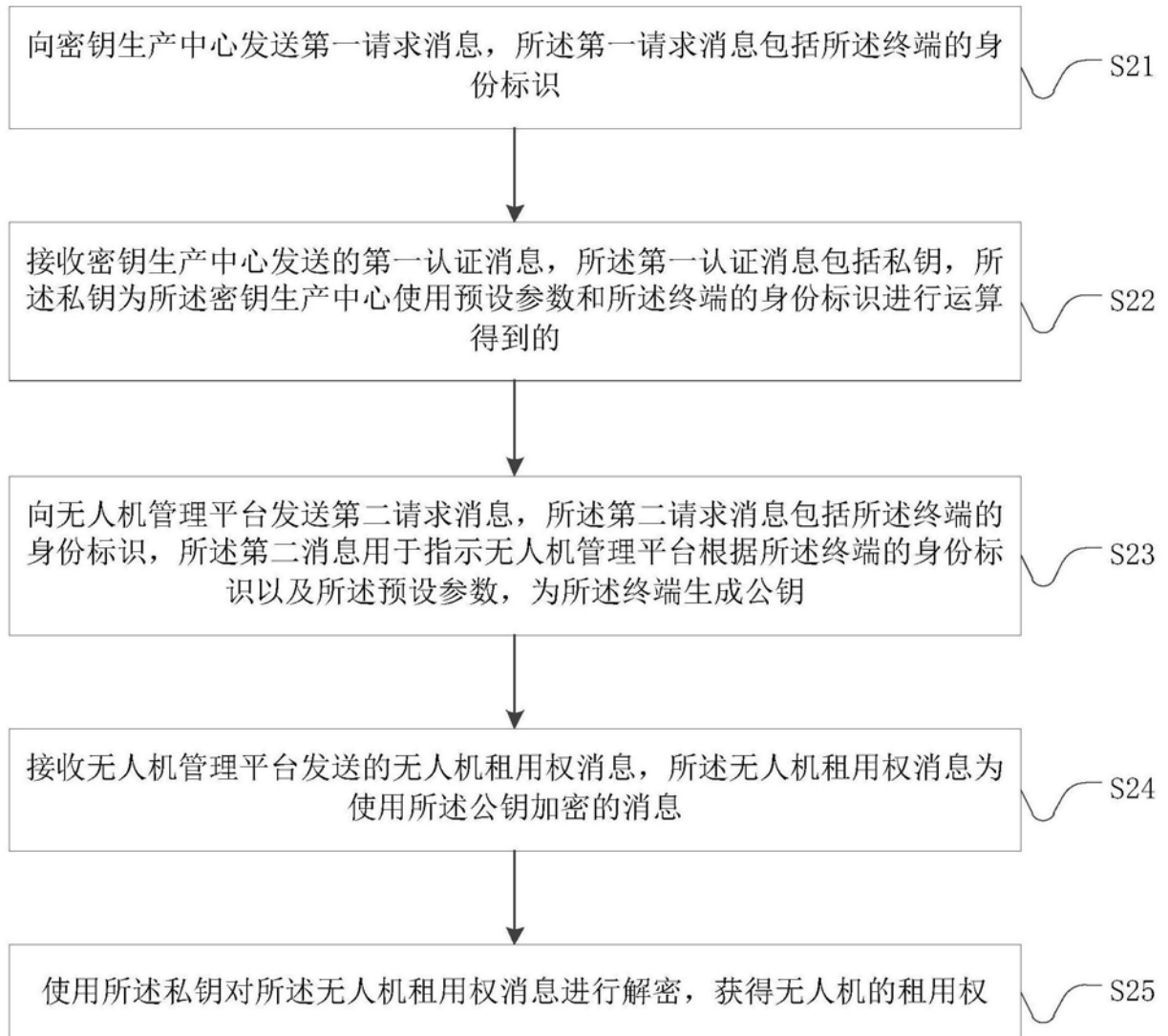


图2



图3A

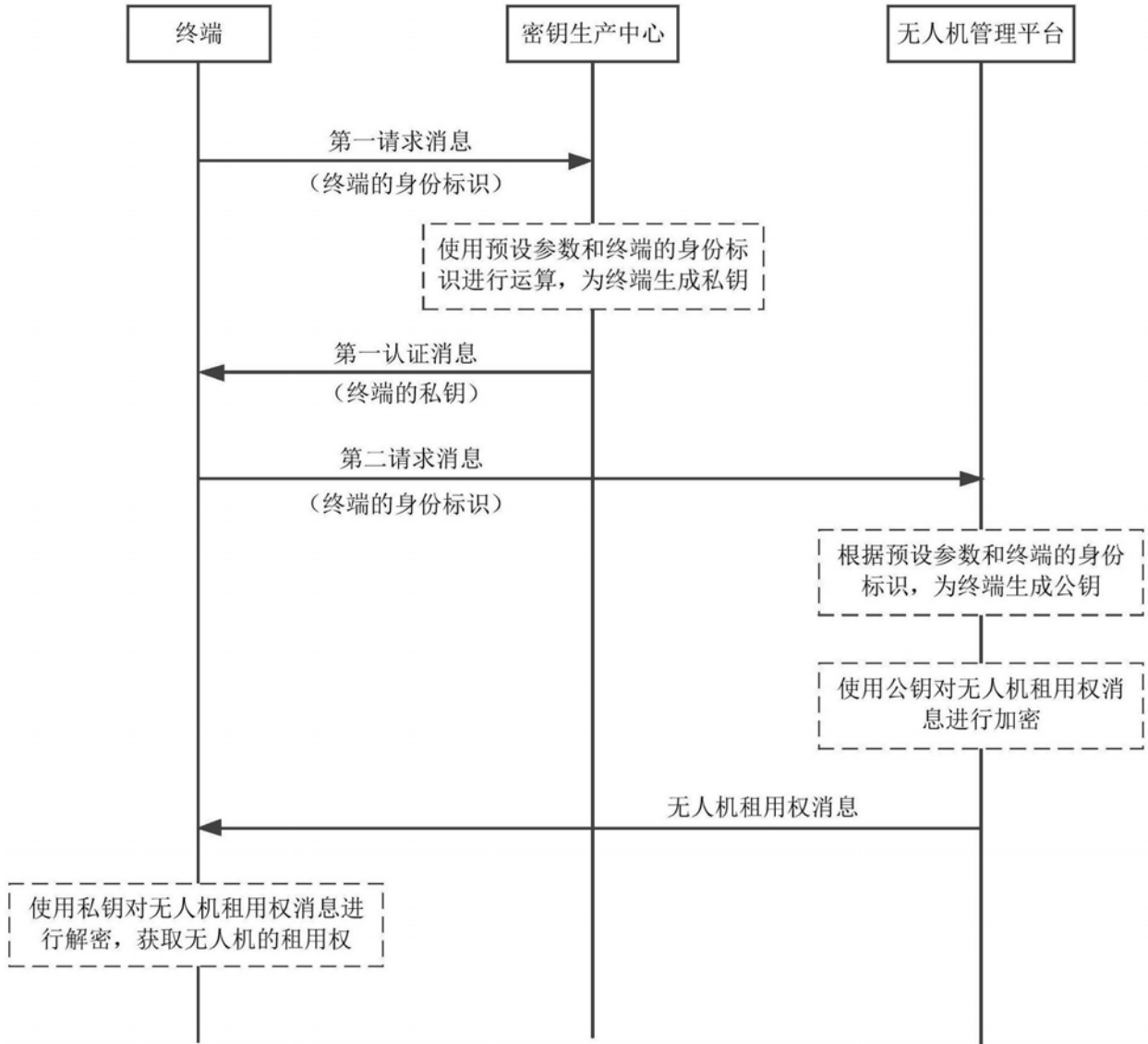


图3B

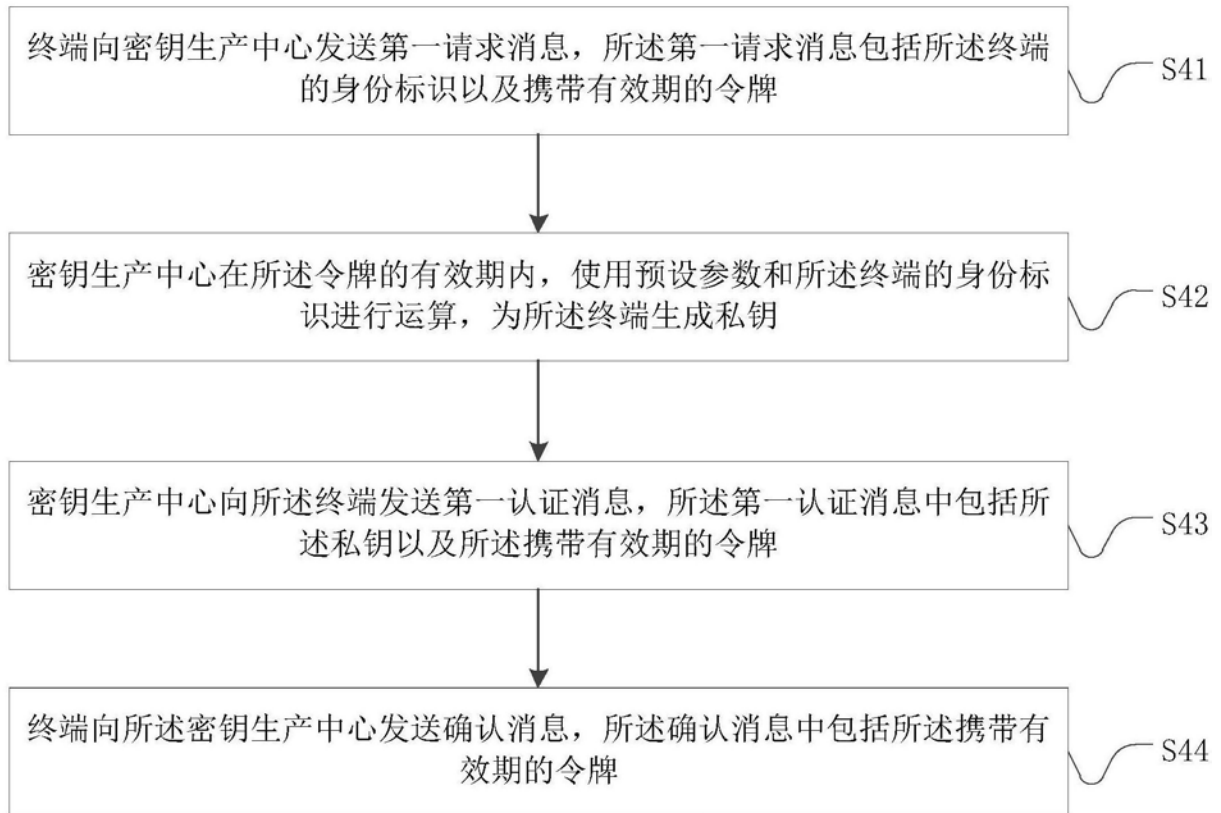


图4A

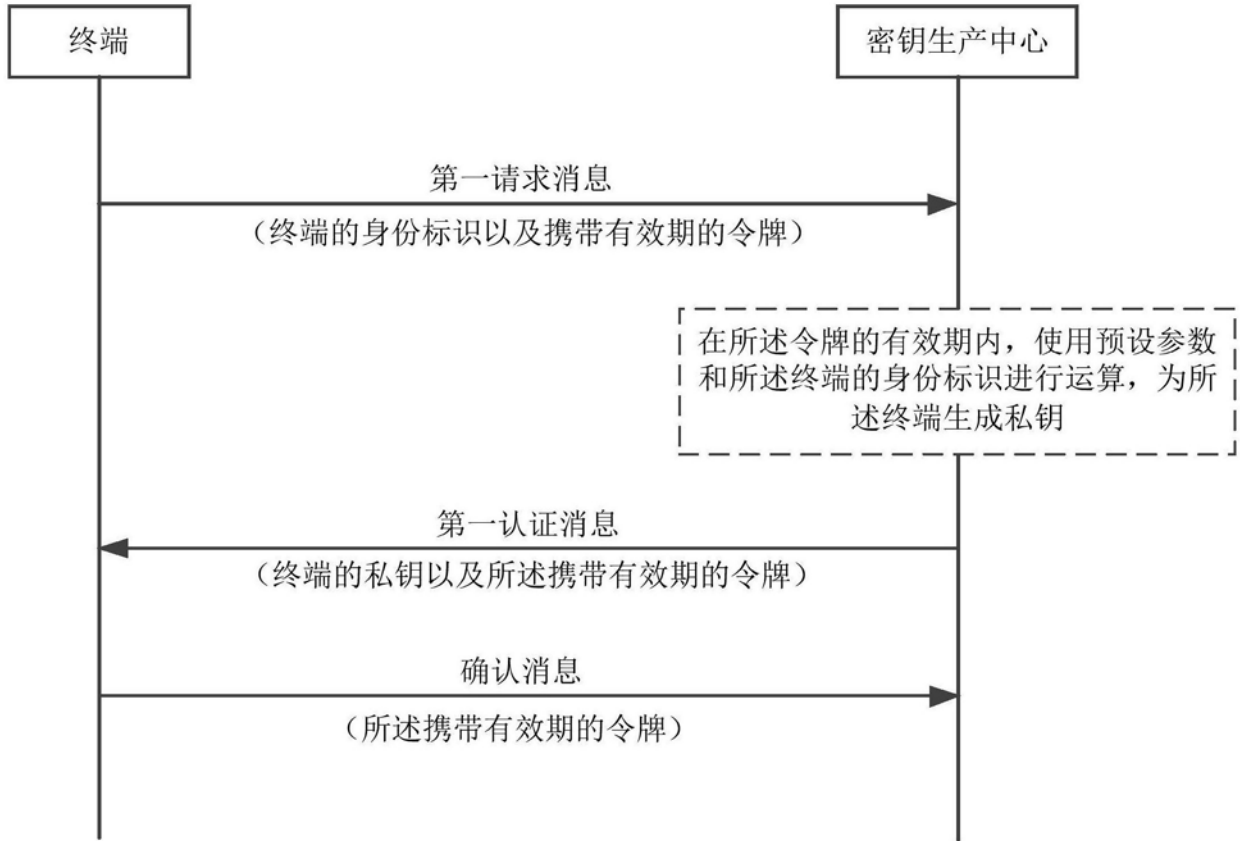


图4B

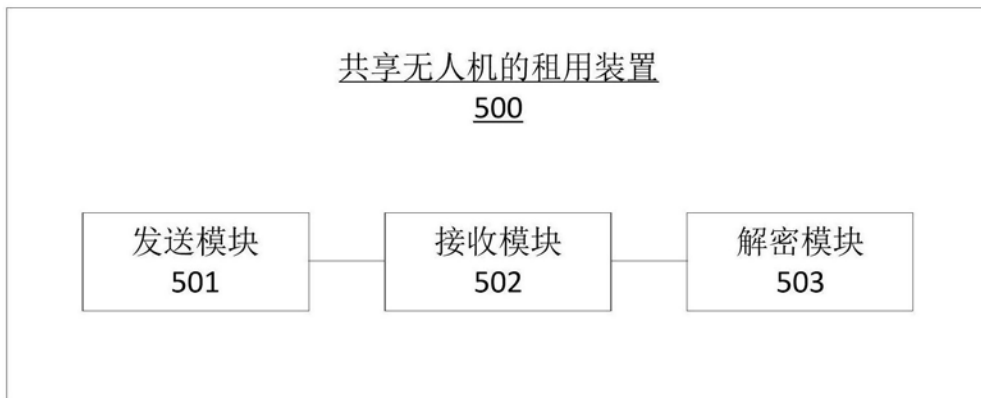


图5

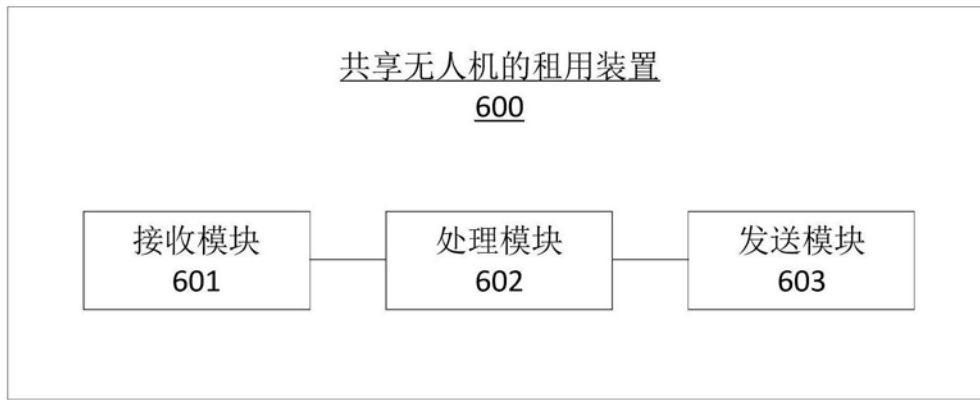


图6

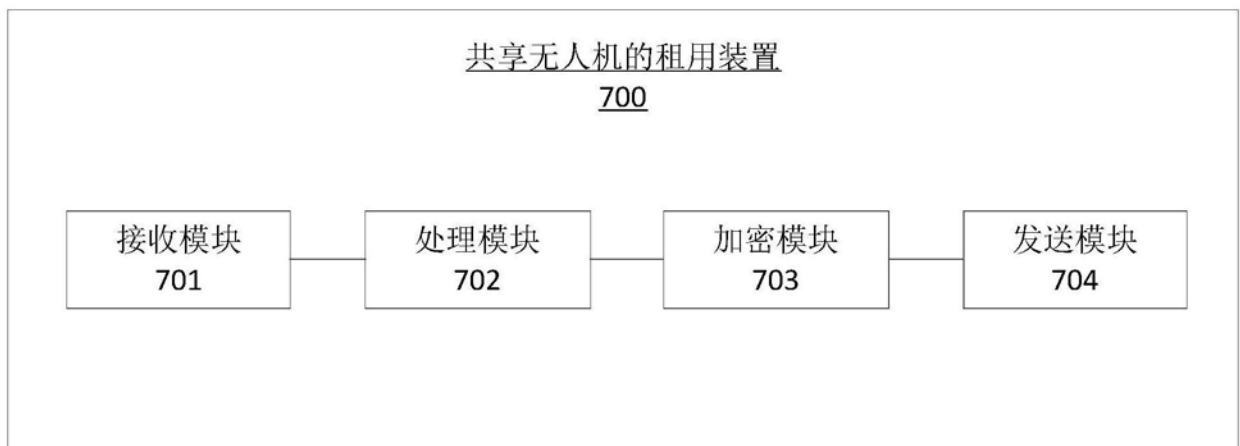


图7

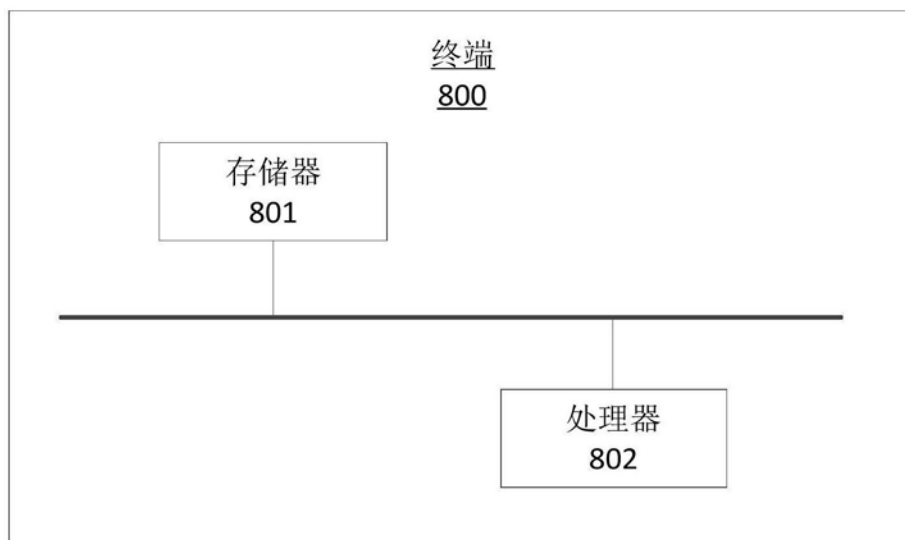


图8

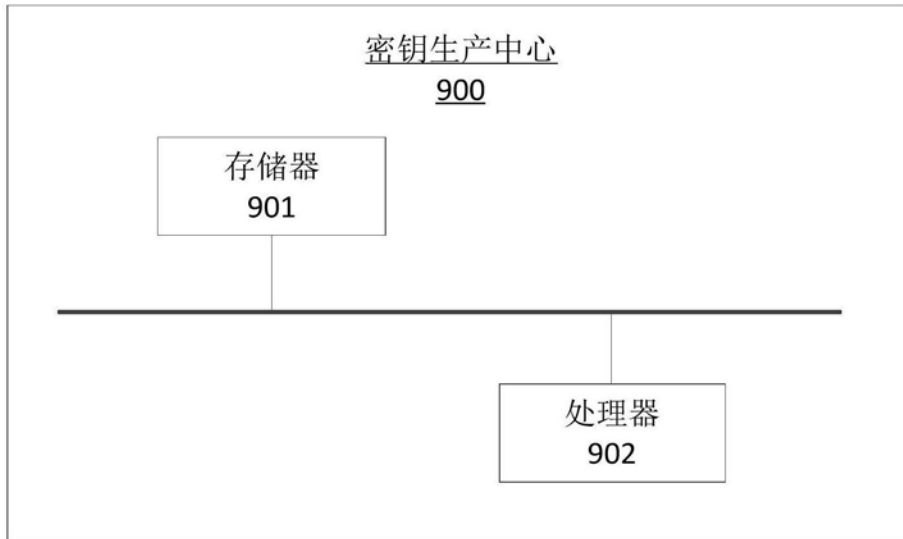


图9

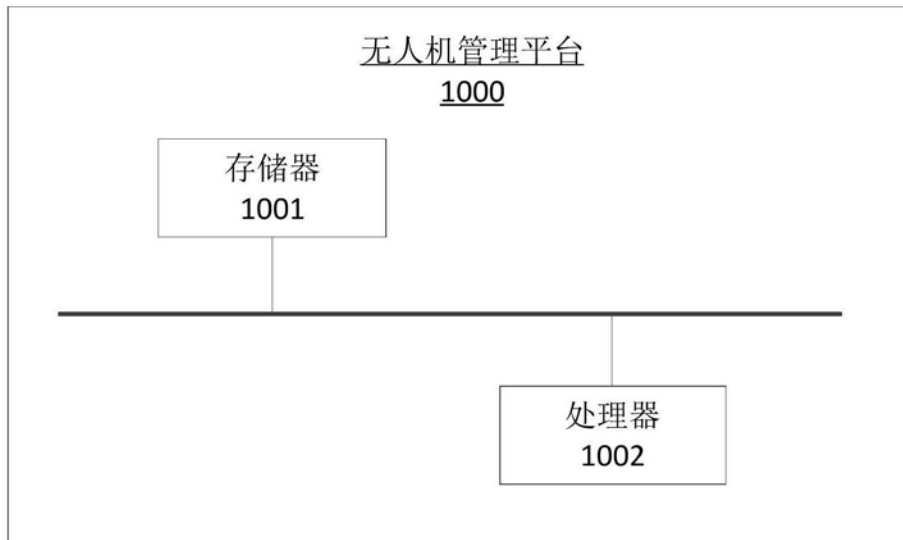


图10

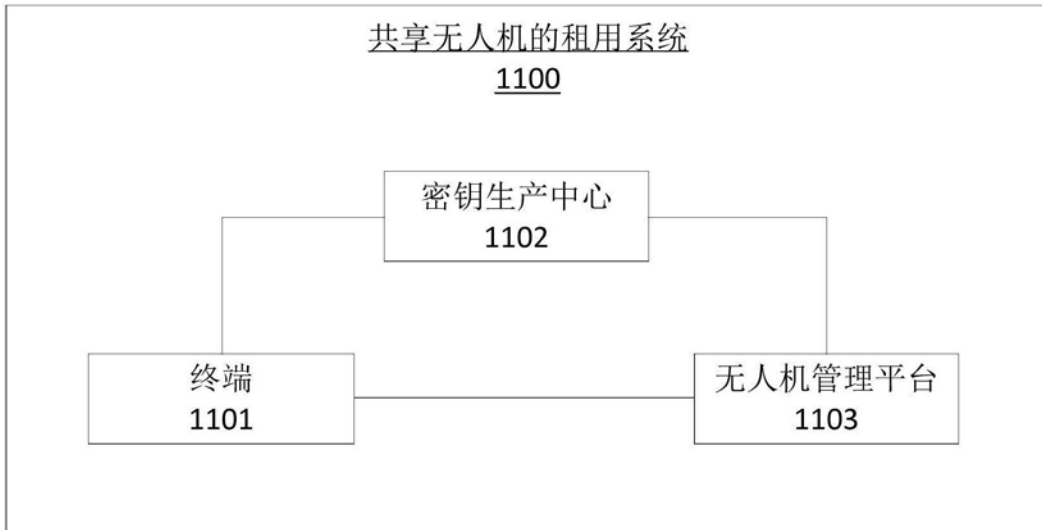


图11