(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111611552 B
(45)授权公告日 2023.04.07

(21)申请号 202010438129.6
(22)申请日 2020.05.21
(65)同一申请的已公布的文献号
申请公布号 CN 111611552 A
(43)申请公布日 2020.09.01
(73)专利权人 浩云科技股份有限公司
地址 511400 广东省广州市番禺区东环街番禺大道北555号天安总部中心22号楼102房
(72)发明人 袁明正
(74)专利代理机构 广州三环专利商标代理有限公司 44202
专利代理师 郭浩辉 麦小婵
(51)Int.Cl.
G06F 21/12(2013.01)
G06F 21/60(2013.01)
(56)对比文件
CN 108268767 A,2018.07.10
CN 109684790 A,2019.04.26
CN 109460639 A,2019.03.12
CN 109328474 A,2019.02.12
CN 108650210 A,2018.10.12
审查员 马莉

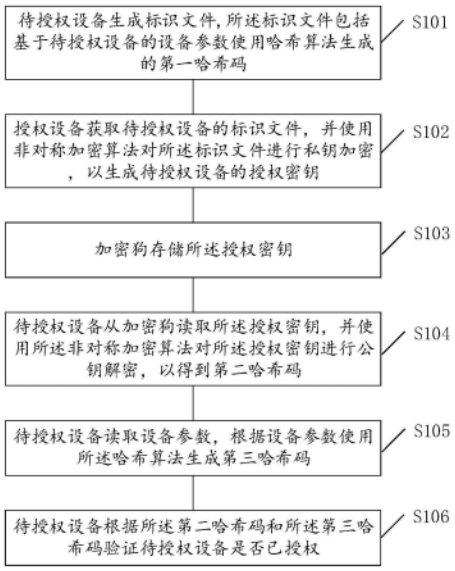
权利要求书2页 说明书7页 附图3页

(54)发明名称

一种软硬结合的license授权方法及装置

(57)摘要

为了解决现有技术中授权易被破解造成授权安全性低的问题,本公开提供了一种软硬结合的license授权方法及装置,提高授权的安全性。方法包括:待授权设备生成标识文件;授权设备获取待授权设备的标识文件,并使用非对称加密算法对所述标识文件进行私钥加密,以生成待授权设备的授权密钥;加密狗存储所述授权密钥;待授权设备从加密狗读取所述授权密钥,并使用所述非对称加密算法对所述授权密钥进行公钥解密,以得到第二哈希码;根据设备参数使用所述哈希算法生成第三哈希码;根据所述第二哈希码和所述第三哈希码验证待授权设备是否已授权。本公开的技术方法中的授权密钥基于常量和变量生成,大大提高了授权的破解难度系数,提高了授权的安全性。



CN 111611552 B

1.一种软硬结合的license授权方法,其特征在于,包括:

待授权设备生成标识文件,所述标识文件包括基于待授权设备的设备参数使用哈希算法生成的第一哈希码,所述设备参数包括设备唯一编码和盐值,所述盐值是由任意字母和数字组合根据MD5算法随机生成的一串字符串;

授权设备获取待授权设备的标识文件,并使用非对称加密算法对所述标识文件进行私钥加密,以生成待授权设备的授权密钥;

加密狗存储所述授权密钥;

待授权设备从加密狗读取所述授权密钥,并使用所述非对称加密算法对所述授权密钥进行公钥解密,以得到第二哈希码;

待授权设备再次读取设备自身的参数,根据读取的设备参数使用所述哈希算法生成第三哈希码;

待授权设备根据所述第二哈希码和所述第三哈希码验证待授权设备是否已授权。

2.如权利要求1所述的方法,其特征在于,所述哈希算法为SHA-256哈希算法,和/或所述非对称加密算法为RSA算法。

3.如权利要求1所述的方法,其特征在于,所述设备参数还包括待授权设备内待授权系统的安装时间,和/或所述唯一编码包括待授权设备的MAC地址和CPUID。

4.一种软硬结合的license授权装置,其特征在于,包括授权设备、加密狗和待授权设备;

所述授权设备包括:

获取模块,用于获取待授权设备的标识文件;

授权密钥生成模块,用于使用非对称加密算法对所述标识文件进行私钥加密,以生成待授权设备的授权密钥。

所述加密狗包括:

存储模块,用于存储待授权设备的授权密钥;

所述待授权设备包括:

标识文件生成模块,用于生成待授权设备的标识文件,所述标识文件包括基于待授权设备的设备参数使用哈希算法生成的第一哈希码,所述设备参数包括设备唯一编码和盐值,所述盐值是由任意字母和数字组合根据MD5算法随机生成的一串字符串;

读取模块,用于从加密狗读取所述授权密钥;

解密模块,用于使用所述非对称加密算法对所述授权密钥进行公钥解密,以得到第二哈希码;

授权验证模块,用于再次读取自身的设备参数,根据读取的设备参数使用所述哈希算法生成第三哈希码;根据所述第二哈希码和所述第三哈希码验证待授权设备是否已授权。

5.license授权方法,其特征在于,包括:

授权设备获取待授权设备的标识文件,所述标识文件包括基于待授权设备的设备参数使用哈希算法生成的第一哈希码,所述设备参数包括设备唯一编码和盐值,所述盐值是由任意字母和数字组合根据MD5算法随机生成的一串字符串;

授权设备使用非对称加密算法对所述标识文件进行私钥加密,以生成待授权设备的授权密钥,以使待授权设备读取所述授权密钥,并使用所述非对称加密算法对所述授权密钥

进行公钥解密,以得到第二哈希码,待授权设备根据再次读取的设备参数使用所述哈希算法生成第三哈希码,待授权设备根据所述第二哈希码和所述第三哈希码验证待授权设备是否已授权。

6.如权利要求5所述的方法,其特征在于,所述设备参数还包括待授权设备内待授权系统的安装时间,和/或所述唯一编码包括待授权设备的MAC地址和CPUID。

7.license授权方法,其特征在于,包括:

待授权设备生成标识文件,以供授权设备使用非对称加密算法的私钥对所述标识文件加密生成待授权设备的授权密钥,其中,所述标识文件包括基于待授权设备的设备参数使用哈希算法生成的第一哈希码,所述设备参数包括设备唯一编码和盐值,所述盐值是由任意字母和数字组合根据MD5算法随机生成的一串字符串;

待授权设备获取所述授权密钥;

待授权设备使用所述非对称加密算法对所述授权密钥进行公钥解密,以得到第二哈希码;

待授权设备再次读取自身的设备参数,根据读取的设备参数使用所述哈希算法生成第三哈希码;

待授权设备根据所述第二哈希码和所述第三哈希码验证待授权设备是否已授权。

8.如权利要求7所述的方法,其特征在于,所述设备参数还包括待授权设备内待授权系统的安装时间,和/或所述唯一编码包括待授权设备的MAC地址和CPUID。

9.一种计算机可读存储介质,所述计算机可读存储介质上存储有计算机程序或指令,其特征在于,所述计算机程序或指令被处理器执行时实现权利要求5至权利要求6任一项所述的license授权方法的步骤。

10.一种计算机设备,其特征在于,所述计算机设备包括处理器和存储器,所述存储器中存储计算机程序或指令,所述计算机程序或指令由所述处理器执行以实现权利要求5至权利要求6任一项所述的license授权方法的步骤。

一种软硬结合的license授权方法及装置

技术领域

[0001] 本公开涉及一种授权技术,尤其涉及一种软硬结合的license授权方法及装置。

背景技术

[0002] 现有license授权方式多为:纯软件license授权且只对单一常量进行加密;其不足在于:易于破解,所生成的license授权文件安全级别较低,当生成的常量被识别或系统被克隆时,即可破解。

发明内容

[0003] 为了解决上述技术问题中的至少一个,本公开提供了一种软硬结合的license授权方法及装置,提高授权的安全性。

[0004] 本公开的第一方面,一种软硬结合的license授权方法,包括:

[0005] 待授权设备生成标识文件,所述标识文件包括基于待授权设备的设备参数使用哈希算法生成的第一哈希码,所述设备参数包括设备唯一编码和盐值;

[0006] 授权设备获取待授权设备的标识文件,并使用非对称加密算法对所述标识文件进行私钥加密,以生成待授权设备的授权密钥;

[0007] 加密狗存储所述授权密钥;

[0008] 待授权设备从加密狗读取所述授权密钥,并使用所述非对称加密算法对所述授权密钥进行公钥解密,以得到第二哈希码;

[0009] 待授权设备读取设备参数,根据设备参数使用所述哈希算法生成第三哈希码;

[0010] 待授权设备根据所述第二哈希码和所述第三哈希码验证待授权设备是否已授权。

[0011] 可选的,所述哈希算法为SHA-256哈希算法,和/或所述非对称加密算法为RSA算法。

[0012] 可选的,所述设备参数还包括待授权设备内待授权系统的安装时间,和/或所述唯一编码包括待授权设备的MAC地址和CPUID。

[0013] 本公开的第二方面,一种软硬结合的license授权装置,包括授权设备、加密狗和待授权设备;

[0014] 所述授权设备包括:

[0015] 获取模块,用于获取待授权设备的标识文件;

[0016] 授权密钥生成模块,用于使用非对称加密算法对所述标识文件进行私钥加密,以生成待授权设备的授权密钥。

[0017] 所述加密狗包括:

[0018] 存储模块,用于存储待授权设备的授权密钥;

[0019] 所述待授权设备包括:

[0020] 标识文件生成模块,用于生成待授权设备的标识文件,所述标识文件包括基于待授权设备的设备参数使用哈希算法生成的第一哈希码,所述设备参数包括设备唯一编码和

盐值；

[0021] 读取模块，用于从加密狗读取所述授权密钥；

[0022] 解密模块，用于使用所述非对称加密算法对所述授权密钥进行公钥解密，以得到第二哈希码；

[0023] 授权验证模块，用于读取设备参数，根据设备参数使用所述哈希算法生成第三哈希码；根据所述第二哈希码和所述第三哈希码验证待授权设备是否已授权。

[0024] 本公开的第三方面，license授权方法，其特征在于，包括：

[0025] 获取待授权设备的标识文件，所述标识文件包括基于待授权设备的设备参数使用哈希算法生成的第一哈希码，所述设备参数包括设备唯一编码和盐值；

[0026] 使用非对称加密算法对所述标识文件进行私钥加密，以生成待授权设备的授权密钥。

[0027] 可选的，其特征在于，所述设备参数还包括待授权设备内待授权系统的安装时间，和/或所述唯一编码包括待授权设备的MAC地址和CPUID。

[0028] 本公开的第四方面，license授权方法，其特征在于，包括：

[0029] 生成标识文件，以供授权设备使用非对称加密算法的私钥对所述标识文件加密生成待授权设备的授权密钥，其中，所述标识文件包括基于待授权设备的设备参数使用哈希算法生成的第一哈希码，所述设备参数包括设备唯一编码和盐值；

[0030] 获取所述授权密钥；

[0031] 使用所述非对称加密算法对所述授权密钥进行公钥解密，以得到第二哈希码；

[0032] 读取设备参数，根据设备参数使用所述哈希算法生成第三哈希码；

[0033] 根据所述第二哈希码和所述第三哈希码验证待授权设备是否已授权。

[0034] 可选的，所述设备参数还包括待授权设备内待授权系统的安装时间，和/或所述唯一编码包括待授权设备的MAC地址和CPUID。

[0035] 本公开的第五方面，一种计算机可读存储介质，所述计算机可读存储介质上存储有计算机程序或指令，其特征在于，所述计算机程序或指令被处理器执行时实现本公开第三或第四方面一项所述方法的步骤。

[0036] 本公开的第六方面，一种计算机设备，其特征在于，所述计算机设备包括处理器和存储器，所述存储器中存储计算机程序或指令，所述计算机程序或指令由所述处理器执行以实现本公开第三或第四方面任一项所述方法的步骤。

[0037] 本公开的技术方案中，授权密钥基于常量和变量生成，大大提高了授权的破解难度系数，提高了授权的安全性；

[0038] 本公开的技术方案中，以加密狗为介质，可防止系统因克隆移植而产生被盗用风险；

[0039] 本公开的技术方案中，采用公钥和私钥分别进行加密解密，降低私钥泄露风险，进一步提高安全性。

附图说明

[0040] 附图示出了本公开的示例性实施方式，并与其说明一起用于解释本公开的原理，其中包括了这些附图以提供对本公开的进一步理解，并且附图包括在本说明书中并构成本

说明书的一部分。

[0041] 图1是本公开的一个实施方式中的一种软硬结合的license授权方法的流程图；

[0042] 图2是本公开的一个实施方式中的一种license授权方法的流程图；

[0043] 图3是本公开的一个实施方式中的另一种license授权方法的流程图；

[0044] 图4是本公开的一个实施方式中的一种软硬结合的license授权装置的框图；

[0045] 图5是本公开的一个实施方式中的授权设备的框图；

[0046] 图6是本公开的一个实施方式中的待授权设备的框图

具体实施方式

[0047] 下面结合附图和实施方式对本公开作进一步的详细说明。可以理解的是，此处所描述的具体实施方式仅用于解释相关内容，而非对本公开的限定。另外还需要说明的是，为了便于描述，附图中仅示出了与本公开相关的部分。

[0048] 需要说明的是，在不冲突的情况下，本公开中的实施方式及实施方式中的特征可以相互组合。下面将参考附图并结合实施方式来详细说明本公开。

[0049] 参见图1，一种软硬结合的license授权方法，包括：

[0050] 步骤S101：待授权设备生成标识文件，所述标识文件包括基于待授权设备的设备参数使用哈希算法生成的第一哈希码，所述设备参数包括设备唯一编码和盐值；

[0051] 步骤S102：授权设备获取待授权设备的标识文件，并使用非对称加密算法对所述标识文件进行私钥加密，以生成待授权设备的授权密钥；

[0052] 步骤S103：加密狗存储所述授权密钥；

[0053] 步骤S104：待授权设备从加密狗读取所述授权密钥，并使用所述非对称加密算法对所述授权密钥进行公钥解密，以得到第二哈希码；

[0054] 步骤S105：待授权设备读取设备参数，根据设备参数使用所述哈希算法生成第三哈希码；

[0055] 步骤S106：待授权设备根据所述第二哈希码和所述第三哈希码验证待授权设备是否已授权。

[0056] 作为上述方法的一种使用场景，待授权设备是安装待授权系统的设备，如安装业务系统的计算机；授权设备是授权待授权系统所在设备的设备，如安装license管理系统的计算机；上述步骤S101中，可以由待授权设备的待授权系统生成标识文件。

[0057] 本实施方式中，待授权设备生成的标识文件包含第一哈希码，该第一哈希码基于待授权设备的设备参数使用哈希算法生成；授权设备使用非对称加密算法对所述标识文件进行私钥加密得到待授权设备的授权密钥；待授权设备通过载有上述授权密钥的加密狗对授权设备授权；待授权设备在插入加密狗之后，根据使用所述非对称加密算法对所述授权密钥进行公钥解密，得到第二哈希码；根据设备参数得到第三哈希码，基于第二哈希码与第三哈希码确定待授权设备是否已授权。在第二哈希码与第三哈希码一致时可以认为已授权，在第二哈希码与第三哈希码与不一致时可以认为未授权。可以知道的同一个待授权设备被授权后，本公开中的第一哈希码、第二哈希码和第二哈希码应该是相同的。

[0058] 本实施方式中授权密钥基于常量和变量生成，大大提高了授权的破解难度系数，提高了授权的安全性；

[0059] 本实施方式中以加密狗为介质,可防止系统因克隆移植而产生被盗用风险;

[0060] 本实施方式中采用公钥和私钥分别进行加密解密,降低私钥泄露风险,进一步提高安全性。

[0061] 参见图2,用于在授权设备端执行的license授权方法,包括:

[0062] 步骤S201:获取待授权设备的标识文件,所述标识文件包括基于待授权设备的设备参数使用哈希算法生成的第一哈希码,所述设备参数包括设备唯一编码和盐值;

[0063] 步骤S202:使用非对称加密算法对所述标识文件进行私钥加密,以生成待授权设备的授权密钥。

[0064] 本实施方式中,由授权设备端执行,使用非对称加密算法对所述标识文件进行私钥加密得到待授权设备的授权密钥,以便于待授权设备端通过上述授权密钥对授权设备授权

[0065] 本实施方式中授权密钥基于常量和变量生成,大大提高了授权的破解难度系数,提高了授权的安全性;

[0066] 本实施方式中采用私钥进行加密,便于待授权设备端采用公钥解密,降低私钥泄露风险,进一步提高授权的安全性。

[0067] 参见图3,用于在被授权设备端执行的license授权方法,其特征在于,包括:

[0068] 步骤S301:生成标识文件,以供授权设备使用非对称加密算法的私钥对所述标识文件加密生成待授权设备的授权密钥,其中,所述标识文件包括基于待授权设备的设备参数使用哈希算法生成的第一哈希码,所述设备参数包括设备唯一编码和盐值;

[0069] 步骤S302:获取所述授权密钥;

[0070] 步骤S303:使用所述非对称加密算法对所述授权密钥进行公钥解密,以得到第二哈希码;

[0071] 步骤S304:读取设备参数,根据设备参数使用所述哈希算法生成第三哈希码;

[0072] 步骤S305:根据所述第二哈希码和所述第三哈希码验证待授权设备是否已授权。

[0073] 本实施方式中的方法,由待授权设备端执行,待授权设备端生成的标识文件包含第一哈希码,该第一哈希码基于待授权设备的设备参数使用哈希算法生成;以便于授权设备端使用非对称加密算法对所述标识文件进行私钥加密得到待授权设备的授权密钥;待授权设备端根据使用所述非对称加密算法对所述授权密钥进行公钥解密,得到第二哈希码;根据设备参数得到第三哈希码,基于第二哈希码与第三哈希码确定待授权设备是否已授权。

[0074] 本实施方式中授权密钥基于常量和变量生成,大大提高了授权的破解难度系数,提高了授权的安全性;

[0075] 本实施方式中采用公钥和私钥分别进行加密解密,降低私钥泄露风险,进一步提高安全性。

[0076] 作为上述各实施方式的一个可选方案,所述哈希算法为SHA-256哈希算法;SHA安全加密标准,是至今国际上使用最为广泛的较为安全的压缩算法之一,采用SHA-256算法生成哈希码可以进一步提高授权方法的安全性。

[0077] 作为上述各实施方式的一个可选方案,所述非对称加密算法为RSA算法。

[0078] RSA算法是一种非对称加密算法,其加密安全系数高;若结合SHA-256算法生成哈

希码,可以保证本公开的授权方法的安全性。

[0079] 作为上述各实施方式的一个可选方案,设备参数还包括待授权设备内待授权系统的安装时间;

[0080] 待授权设备内待授权系统的安装时间,即需要授权的待授权系统的安装时间,安装时间在待授权系统安装时可以自动获取,而基于所述安装时间生成的哈希码,并基于该哈希码生成的授权密钥;只有在知晓上述待授权系统的安装时间时,才有可能破解授权密钥,进一步提高授权的安全性。

[0081] 作为上述各实施方式的一个可选方案,所述唯一编码包括待授权设备的MAC地址和CPUID。

[0082] CPUID即CPU的ID号;即设备参数包含待授权设备的MAC地址和CPUID;可以进一步防止其他设备使用授权密钥进行授权,提高安全性。

[0083] 实施例2:

[0084] 参见图4～图6,一种软硬结合的license授权装置,包括授权设备1、加密狗2和待授权设备3;

[0085] 授权设备1包括:

[0086] 获取模块101,用于获取待授权设备的标识文件;

[0087] 授权密钥生成模块102,用于使用非对称加密算法对所述标识文件进行私钥加密,以生成待授权设备的授权密钥。

[0088] 加密狗2包括:

[0089] 存储模块,用于存储待授权设备的授权密钥;

[0090] 待授权设备3包括:

[0091] 标识文件生成模块301,用于生成待授权设备的标识文件,所述标识文件包括基于待授权设备的设备参数使用哈希算法生成的第一哈希码,所述设备参数包括设备唯一编码和盐值;

[0092] 读取模块302,用于从加密狗读取所述授权密钥;

[0093] 解密模块303,用于使用所述非对称加密算法对所述授权密钥进行公钥解密,以得到第二哈希码;

[0094] 授权验证模块304,用于读取设备参数,根据设备参数使用所述哈希算法生成第三哈希码;根据所述第二哈希码和所述第三哈希码验证待授权设备是否已授权。

[0095] 作为上述各实施方式的一个可选方案,所述哈希算法为SHA-256哈希算法;

[0096] 作为上述各实施方式的一个可选方案,所述非对称加密算法为RSA算法。

[0097] 作为上述各实施方式的一个可选方案,所述设备参数还包括待授权设备内待授权系统的安装时间;

[0098] 作为上述各实施方式的一个可选方案,所述唯一编码包括待授权设备的MAC地址和CPUID。

[0099] 本实施方式中的装置生成的授权密钥基于常量和变量生成,大大提高了授权的破解难度系数,提高了授权的安全性;

[0100] 本实施方式中的装置采用公钥和私钥分别进行加密解密,降低私钥泄露风险,进一步提高安全性。

[0101] 实施例3：

[0102] 一种计算机可读存储介质，计算机可读存储介质上存储有计算机程序或指令，计算机程序或指令被处理器执行时实现实施例1任一项所述license授权方法的步骤。

[0103] 实施例4：

[0104] 一种计算机设备，计算机设备包括处理器和存储器，存储器中存储计算机程序或指令，计算机程序或指令由所述处理器执行以实现实施例1任一项所述license授权方法的步骤。

[0105] 本实施例以业务系统为例做进一步说明；

[0106] 1、生成标识文件：

[0107] 在业务系统部署完成后，系统默认在安装路径下启动会根据当前设备(即待授权设备)的设备参数使用SHA-256算法生成一个当前设备的标识文件(可以是以txt文件格式存放一串64位哈希码)。由项目运维人员将其取出并发送给公司license管理人员，申请软件授权。其中设备参数包括物理设备MAC地址、盐值(由任意字母、数字组合，根据MD5算法随机生成的一串字符串)、系统安装时间和CPUID；

[0108] 2、使用RSA算法的私钥对设备的标识文件进行加密生成加密文件，并烧录到加密狗中：

[0109] License管理人员首先将标识文件和申请信息(包括：项目名称、申请人姓名、授权期限、申请时间、申请原因)导入和填写到授权设备的license管理工具上；然后，授权设备的license管理工具根据申请信息确定是否允许授权，若允许授权，则结合RSA对标识文件进行私钥加密(生成一串字符串)；最后，license管理人员利用烧录加密狗工具，将生成的授权密钥烧录到加密狗中。

[0110] 3、通过公钥解析出加密信息并比对验证：

[0111] 项目运维人员拿到公司license管理人员寄送的加密狗硬件后，将其插入安装业务系统的设备上，系统自动识别加密狗并用公钥解密，在解析出加密前的标识hash字符串，然后读取设备参数(物理机MAC地址、盐值、系统安装时间、CPUID)使用SHA-256哈希算法生成hash字符串，与从加密狗解析出的hash字符串进行验证。若验证无误，则授权系统进入下一步运行；若验证有误，则提示授权失败。

[0112] 在本说明书的描述中，参考术语“一个实施例/方式”、“一些实施例/方式”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例/方式或示例描述的具体特征、结构、材料或者特点包含于本申请的至少一个实施例/方式或示例中。在本说明书中，对上述术语的示意性表述不必须针对的是相同的实施例/方式或示例。而且，描述的具体特征、结构、材料或者特点可以在任一个或多个实施例/方式或示例中以合适的方式结合。此外，在不相互矛盾的情况下，本领域的技术人员可以将本说明书中描述的不同实施例/方式或示例以及不同实施例/方式或示例的特征进行结合和组合。

[0113] 此外，术语“第一”、“第二”仅用于描述目的，而不能理解为指示或暗示相对重要性或者隐含指明所指示的技术特征的数量。由此，限定有“第一”、“第二”的特征可以明示或者隐含地包括至少一个该特征。在本申请的描述中，“多个”的含义是至少两个，例如两个，三个等，除非另有明确具体的限定。

[0114] 本领域的技术人员应当理解，上述实施方式仅仅是为了清楚地说明本公开，而并

非是对本公开的范围进行限定。对于所属领域的技术人员而言，在上述公开的基础上还可以做出其它变化或变型，并且这些变化或变型仍处于本公开的范围内。

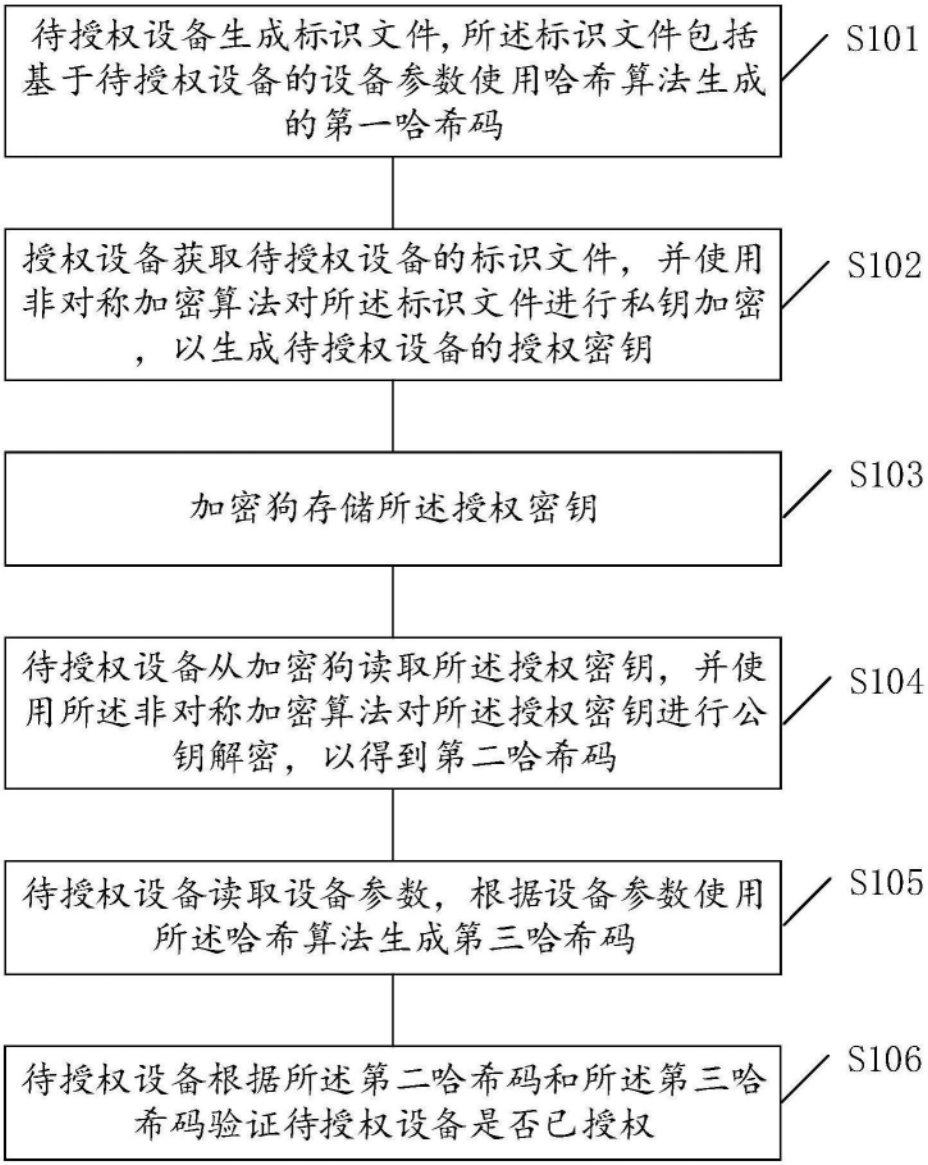

待授权设备生成标识文件，所述标识文件包括基于待授权设备的设备参数使用哈希算法生成的第一哈希码
S101
授权设备获取待授权设备的标识文件，并使用非对称加密算法对所述标识文件进行私钥加密，以生成待授权设备的授权密钥
S102
加密狗存储所述授权密钥
S103
待授权设备从加密狗读取所述授权密钥，并使用所述非对称加密算法对所述授权密钥进行公钥解密，以得到第二哈希码
S104
待授权设备读取设备参数，根据设备参数使用所述哈希算法生成第三哈希码
S105
待授权设备根据所述第二哈希码和所述第三哈希码验证待授权设备是否已授权
S106

图1

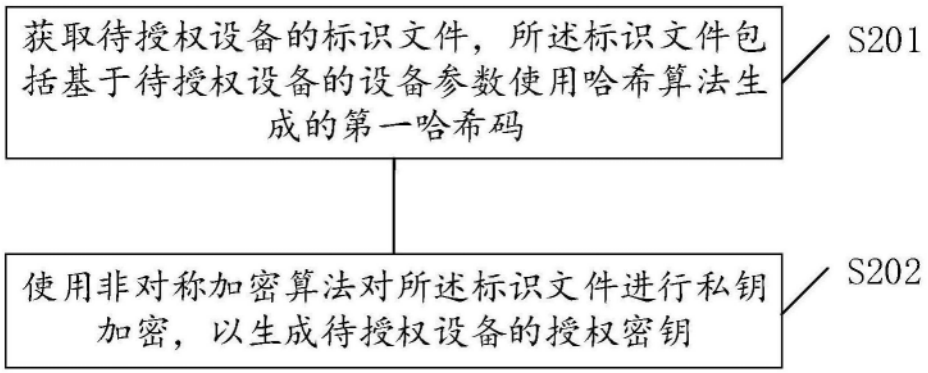

获取待授权设备的标识文件，所述标识文件包括基于待授权设备的设备参数使用哈希算法生成的第一哈希码
S201
使用非对称加密算法对所述标识文件进行私钥加密，以生成待授权设备的授权密钥
S202

图2

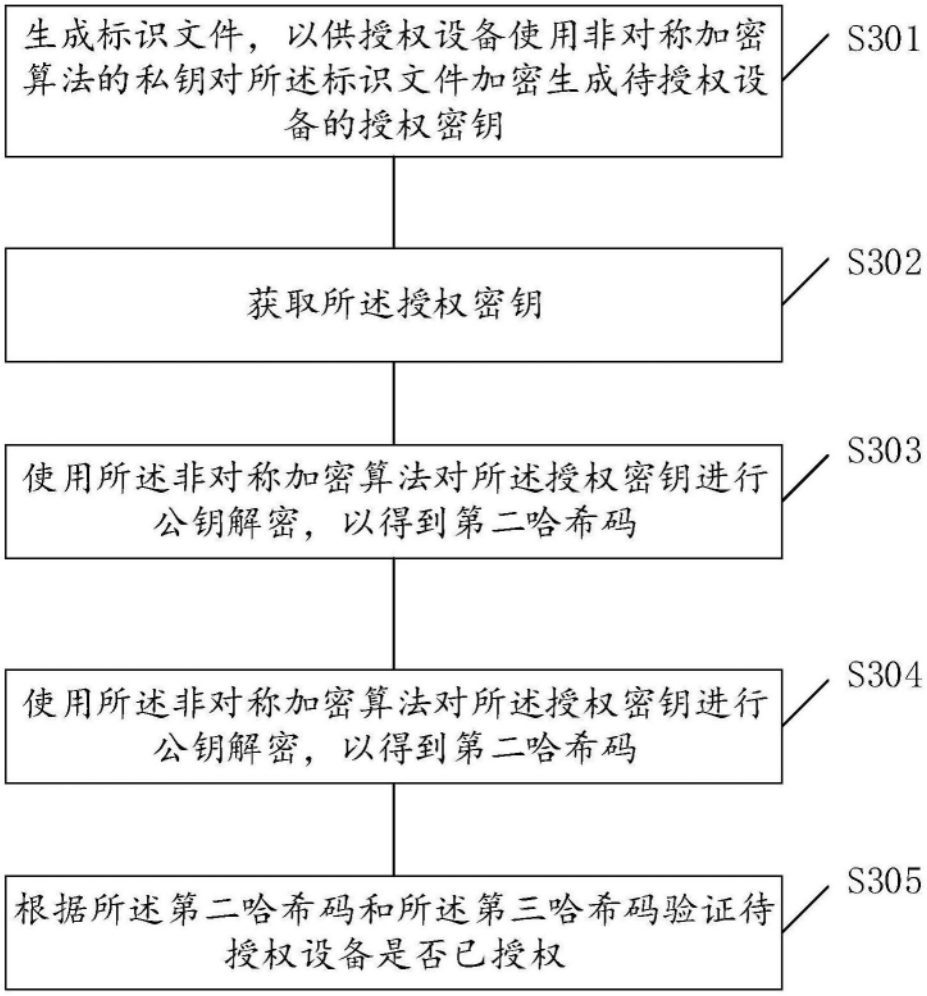

生成标识文件，以供授权设备使用非对称加密算法的私钥对所述标识文件加密生成待授权设备的授权密钥
S301
获取所述授权密钥
S302
使用所述非对称加密算法对所述授权密钥进行公钥解密，以得到第二哈希码
S303
使用所述非对称加密算法对所述授权密钥进行公钥解密，以得到第二哈希码
S304
根据所述第二哈希码和所述第三哈希码验证待授权设备是否已授权
S305

图3

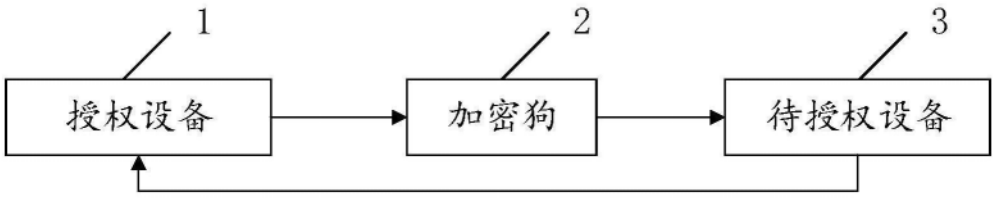

1
2
3
授权设备
加密狗
待授权设备

图4

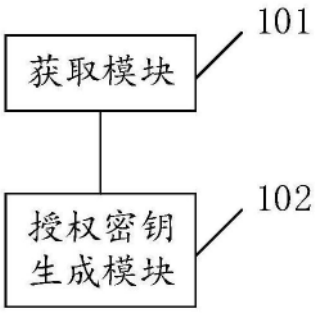

101
获取模块
102
授权密钥
生成模块

图5

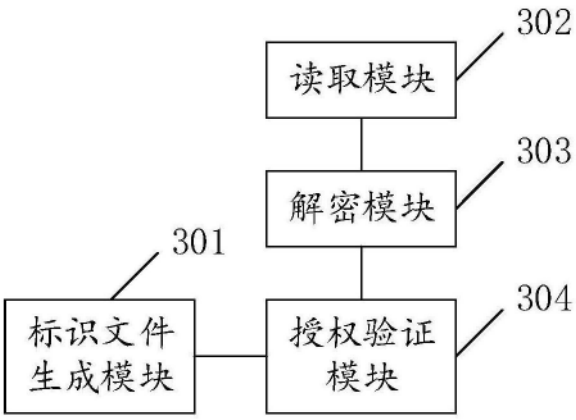

302
读取模块
303
解密模块
301
标识文件
生成模块
304
授权验证
模块

图6