(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 106453277 A
(43)申请公布日 2017.02.22

(21)申请号 201610847043.2

(22)申请日 2016.09.02

(71)申请人 长城汽车股份有限公司
地址 071000 河北省保定市朝阳南大街2266号

(72)发明人 刘静 郭岩松 李纪玄 李琦

(74)专利代理机构 北京清亦华知识产权代理事务所(普通合伙) 11201
代理人 张大威

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)
G07C 9/00(2006.01)

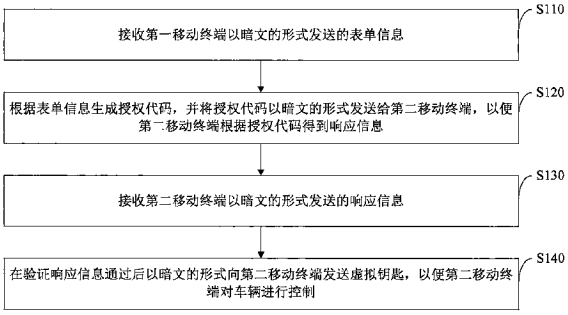
权利要求书2页 说明书5页 附图2页

(54)发明名称

车辆的虚拟钥匙授权方法、系统、移动终端和服务器

(57)摘要

本发明提供了一种车辆的虚拟钥匙授权方法、系统、移动终端和服务器，该方法包括：接收第一移动终端以暗文的形式发送的表单信息；根据表单信息生成授权代码，并将授权代码以暗文的形式发送给第二移动终端，以便第二移动终端根据授权代码得到响应信息；接收第二移动终端以暗文的形式发送的响应信息；在验证响应信息通过后以暗文的形式向第二移动终端发送虚拟钥匙，以便第二移动终端对车辆进行控制。本发明的方法可以在通讯过程进行加密的基础上采用暗文通讯方式，增加了系统的安全性；简化了用户操作的步骤，使分享过程更加简洁，增强了用户体验；通过后台与移动设备之间的三次通信，确保被授权人身份的可靠性，使系统验证过程更加严谨。



CN 106453277 A

1.一种车辆的虚拟钥匙授权方法，其特征在于，包括以下步骤：

接收第一移动终端以暗文的形式发送的表单信息；

根据所述表单信息生成授权代码，并将所述授权代码以暗文的形式发送给第二移动终端，以便所述第二移动终端根据所述授权代码得到响应信息；

接收所述第二移动终端以暗文的形式发送的所述响应信息；

在验证所述响应信息通过后以暗文的形式向所述第二移动终端发送虚拟钥匙，以便所述第二移动终端对所述车辆进行控制。

2.根据权利要求1所述的车辆的虚拟钥匙授权方法，其特征在于，所述表单信息包括分享者信息、车辆授权权限信息和借用人信息。

3.根据权利要求1所述的车辆的虚拟钥匙授权方法，其特征在于，所述响应信息包括第二移动终端发送的借用人信息、第二移动终端信息和所述授权代码。

4.根据权利要求1所述的车辆的虚拟钥匙授权方法，其特征在于，所述虚拟钥匙具有车辆授权权限，以便所述车辆为所述第二移动终端提供对应于所述虚拟钥匙的车辆授权权限的功能。

5.一种移动终端，其特征在于，包括：

第一加密模块，用于对表单信息进行加密；

第一通信模块，用于以暗文的形式向服务器发送所述表单信息。

6.根据权利要求5所述的移动终端，其特征在于，所述表单信息包括分享者信息、车辆授权权限信息和借用人信息。

7.一种移动终端，其特征在于，包括：

第二加密模块，用于对响应信息进行加密；

第二通信模块，用于接收所述服务器发送的授权代码，并以暗文的形式向所述服务器发送所述响应信息，以及接收所述服务器发送的虚拟钥匙，其中，所述虚拟钥匙由所述服务器在验证所述响应信息通过后生成的；

控制模块，用于根据所述虚拟钥匙对车辆进行控制。

8.根据权利要求7所述的移动终端，其特征在于，所述响应信息包括第二移动终端发送的借用人信息、第二移动终端信息和所述授权代码。

9.一种服务器，其特征在于，包括：

第三加密模块，用于对授权代码和虚拟钥匙进行加密；

第三通信模块，用于接收第一移动终端发送的表单信息，并将所述授权代码以暗文的形式发送给第二移动终端，以及接收所述第二移动终端发送的响应信息，并以暗文的形式向所述第二移动终端发送虚拟钥匙；

处理模块，用于根据所述表单信息生成授权代码，并在验证所述响应信息通过后生成所述虚拟钥匙。

10.根据权利要求9所述的服务器，其特征在于，所述虚拟钥匙具有车辆授权权限，以便所述车辆为所述第二移动终端提供对应于所述虚拟钥匙的车辆授权权限的功能。

11.一种车辆的虚拟钥匙授权系统，其特征在于，包括：

第一移动终端，所述第一移动终端为根据权利要求5或6所述的移动终端；

第二移动终端，所述第二移动终端为根据权利要求7或8所述的移动终端；

服务器，所述服务器为根据权利要求9或10所述的服务器。

车辆的虚拟钥匙授权方法、系统、移动终端和服务器

技术领域

[0001] 本发明涉及汽车技术领域，特别涉及一种车辆的虚拟钥匙授权方法、系统、移动终端和服务器。

背景技术

[0002] 虚拟钥匙在汽车上的应用使得钥匙分享变得更加快速方便，但是虚拟钥匙在分享过程中一直存在着安全隐患。分享给被授权者的信息容易被截获并破译，威胁到汽车安全。

[0003] 相关技术中，分享给被授权者的信息的过程存在如下问题：

[0004] 对被授权的信息仅仅用“加密”二字代表整个机制，未提出针对有效的加密策略，系统安全性没有保障；

[0005] 直接发送授权证书给被授权者，过程中信息容易被截获；

[0006] 后台与车辆连接并能控制和修改车辆自身的授权管理系统，存在系统安全隐患。

发明内容

[0007] 有鉴于此，本发明旨在提出一种车辆的虚拟钥匙授权方法，该方法可以增加系统的安全性，确保被授权人身份的可靠性，简化用户操作，增强用户体验。

[0008] 为达到上述目的，本发明的技术方案是这样实现的：

[0009] 一种车辆的虚拟钥匙授权方法，包括以下步骤：接收第一移动终端以暗文的形式发送的表单信息；根据所述表单信息生成授权代码，并将所述授权代码以暗文的形式发送给第二移动终端，以便所述第二移动终端根据所述授权代码得到响应信息；接收所述第二移动终端以暗文的形式发送的所述响应信息；在验证所述响应信息通过后以暗文的形式向所述第二移动终端发送虚拟钥匙，以便所述第二移动终端对所述车辆进行控制。

[0010] 进一步的，所述表单信息包括分享者信息、车辆授权权限信息和借用人信息。

[0011] 进一步的，所述响应信息包括第二移动终端发送的借用人信息、第二移动终端信息和所述授权代码。

[0012] 进一步的，所述虚拟钥匙具有车辆授权权限，以便所述车辆为所述第二移动终端提供对应于所述虚拟钥匙的车辆授权权限的功能。

[0013] 相对于现有技术，本发明所述的车辆的虚拟钥匙授权方法具有以下优势：

[0014] 本发明所述的车辆的虚拟钥匙授权方法，在通讯过程进行加密的基础上采用暗文通讯方式，增加系统的安全性；通过后台与移动设备之间的三次通信，确保被授权人身份的可靠性，使系统验证过程更加严谨；简化用户操作的步骤，使分享过程更加简洁，增强了用户体验。

[0015] 本发明的第二个目的在于提出一种移动终端，该移动终端可以增加虚拟钥匙授权过程的安全性。

[0016] 为达到上述目的，本发明的技术方案是这样实现的：

[0017] 一种移动终端，包括：第一加密模块，用于对表单信息进行加密；第一通信模块，用

于以暗文的形式向服务器发送所述表单信息。

[0018] 进一步的，所述表单信息包括分享者信息、车辆授权权限信息和借用人信息。

[0019] 本发明所述的移动终端，在通讯过程进行加密的基础上采用暗文通讯方式，增加虚拟钥匙授权过程的安全性。

[0020] 本发明的第三个目的在于提出一种移动终端，该移动终端可以增加虚拟钥匙授权过程的安全性，同时可以对车辆进行控制。

[0021] 为达到上述目的，本发明的技术方案是这样实现的：

[0022] 一种移动终端，包括：第二加密模块，用于对响应信息进行加密；第二通信模块，用于接收所述服务器发送的授权代码，并以暗文的形式向所述服务器发送所述响应信息，以及接收所述服务器发送的虚拟钥匙，其中，所述虚拟钥匙由所述服务器在验证所述响应信息通过后生成的；控制模块，用于根据所述虚拟钥匙对车辆进行控制。

[0023] 进一步的，所述响应信息包括第二移动终端发送的借用人信息、第二移动终端信息和所述授权代码。

[0024] 所述的移动终端，在通讯过程进行加密的基础上采用暗文通讯方式，增加虚拟钥匙授权过程的安全性，同时可以接受虚拟钥匙对车辆进行控制。

[0025] 本发明的第四个目的在于提出一种服务器，可以增加虚拟钥匙授权过程的安全性。

[0026] 为达到上述目的，本发明的技术方案是这样实现的：

[0027] 一种服务器，包括：第三加密模块，用于对授权代码和虚拟钥匙进行加密；第三通信模块，用于接收第一移动终端发送的表单信息，并将所述授权代码以暗文的形式发送给第二移动终端，以及接收所述第二移动终端发送的响应信息，并以暗文的形式向所述第二移动终端发送虚拟钥匙；处理模块，用于根据所述表单信息生成授权代码，并在验证所述响应信息通过后生成所述虚拟钥匙。

[0028] 进一步地，所述虚拟钥匙具有车辆授权权限，以便所述车辆为所述第二移动终端提供对应于所述虚拟钥匙的车辆授权权限的功能。

[0029] 本发明所述的服务器，在通讯过程进行加密的基础上采用暗文通讯方式，增加虚拟钥匙授权过程的安全性。

[0030] 本发明的第五个目的在于提出一种车辆的虚拟钥匙授权系统，可以增加虚拟钥匙授权过程的安全性，同时可以对车辆进行控制。

[0031] 为达到上述目的，本发明的技术方案是这样实现的：

[0032] 一种车辆的虚拟钥匙授权系统，包括：第一移动终端，所述第一移动终端为第二实施例所述的移动终端；第二移动终端，所述第二移动终端为第三实施例所述的移动终端；服务器，所述服务器为第四实施例所述的服务器。

[0033] 本发明所述的车辆的虚拟钥匙授权系统，可以增加虚拟钥匙授权过程的安全性，同时可以对车辆进行控制。

附图说明

[0034] 构成本发明的一部分的附图用来提供对本发明的进一步理解，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

[0035] 图1为本发明实施例所述的车辆的虚拟钥匙授权方法的流程图；

[0036] 图2为本发明一个实施例所述的移动终端的结构框图；

[0037] 图3为本发明另一个实施例所述的移动终端的结构框图；

[0038] 图4为本发明另一个实施例所述的服务器的结构框图；

[0039] 图5为本发明实施例所述的车辆的虚拟钥匙授权系统的结构框图。

具体实施方式

[0040] 需要说明的是，在不冲突的情况下，本发明中的实施例及实施例中的特征可以相互组合。

[0041] 下面将参考附图并结合实施例来详细说明本发明。

[0042] 图1为本发明实施例所述的控制车辆与车辆的虚拟钥匙授权方法的流程图。

[0043] 如图1所示，根据本发明一个实施例的车辆的虚拟钥匙授权方法，包括以下步骤：

[0044] S110：接收第一移动终端以暗文的形式发送的表单信息。

[0045] 具体地，服务器接收第一移动终端以暗文发送的表单信息。其中，第一移动终端为原车辆驾驶员预定的移动终端，移动移动终端上设置有生成表单信息的APP。当原车辆驾驶员需要向其他移动终端发送授权信息时，首先向服务器发送表单信息。以暗文形式发送即授权码只在服务器内传输不会展示给用户，用户只需要根据提示操作即可。

[0046] 在本发明的一个实施例中，表单信息包括分享者信息、车辆授权权限信息和借用人信息。其中，分享者信息即原车辆驾驶员的信息，原车辆的驾驶员将上述信息发送给服务器，以便服务器执行相应的动作。

[0047] S120：根据所述表单信息生成授权代码，并将所述授权代码以暗文的形式发送给第二移动终端，以便所述第二移动终端根据所述授权代码得到响应信息。

[0048] 具体地，服务器收到表单信息后，由于表单信息包括对借用人信息和对借用人的授权信息。服务器根据表单信息生成相应的授权代码，并将授权代码以暗文的形式发送给第二移动终端(即借用人的移动终端)，以便在第二移动终端上根据上述授权代码生成响应信息。其中，第二移动终端上设置有接收授权信息，并根据授权信息生成响应信息的APP，借用者只需对APP进行操作即可。在借用者对APP进行操作时，授权代码不是显示在第二移动终端上。

[0049] S130：接收所述第二移动终端以暗文的形式发送的所述响应信息。

[0050] 在本发明的一个实施例中，响应信息包括第二移动终端发送的借用人信息、第二移动终端信息和所述授权代码。第二移动终端将上述借用人信息、第二移动终端信息和所述授权代码发送给服务器，以便服务器执行相应的动作。

[0051] S140：在验证所述响应信息通过后以暗文的形式向所述第二移动终端发送虚拟钥匙，以便所述第二移动终端对所述车辆进行控制。

[0052] 具体地，服务器对第二移动终端发送的响应信息与第一移动终端发送的表单信息进行验证，验证内容包括第二移动终端发送的借用人信息是否与第一移动终端发送的借用人信息是否一致等。当响应信息通过验证后，服务器生成虚拟钥匙，并以暗文的行驶发送至第二移动终端。第二移动终端收到虚拟钥匙后即可对车辆进行控制。

[0053] 在本发明的一个实施例中，虚拟钥匙具有车辆授权权限，以便所述车辆为所述第

二移动终端提供对应于所述虚拟钥匙的车辆授权权限的功能，即第二移动终端在授权权限内可以对车辆进行相应的控制。在本发明的一个示例中，授权权限为第二移动终端只能对车辆行驶时进行基本操作，同时授权权限还可以包括对第二移动终端对车辆控制的授权时间。

[0054] 根据本发明实施例的车辆的虚拟钥匙授权方法，在通讯过程进行加密的基础上采用暗文通讯方式，增加系统的安全性；通过后台与移动设备之间的三次通信，确保被授权人身份的可靠性，使系统验证过程更加严谨；简化用户操作的步骤，使分享过程更加简洁，增强了用户体验。

[0055] 图2是根据本发明一个实施例的移动终端的结构框图。如图2所示，根据本发明一个实施例的移动终端200，包括：第一加密模块210和第一通信模块220。

[0056] 其中，第一加密模块210用于对表单信息进行加密。第一通信模块220用于以暗文的形式向服务器发送所述表单信息。

[0057] 根据本发明实施例的移动终端，在通讯过程进行加密的基础上采用暗文通讯方式，增加虚拟钥匙授权过程的安全性。

[0058] 在本发明的一个实施例中，表单信息包括分享者信息、车辆授权权限信息和借用人信息。

[0059] 需要说明的是，本发明实施例的移动终端200的具体实现方式与本发明实施例的车辆的虚拟钥匙授权方法中的第一移动终端的具体实现方式类似，具体请参见车辆的虚拟钥匙授权方法中的第一移动终端部分的描述，为了减少冗余，此处不做赘述。

[0060] 图3是根据本发明一个实施例的移动终端的结构框图。如图3所示，根据本发明一个实施例的移动终端300，包括：第二加密模块310和第二通信模块320。

[0061] 其中，第二加密模块310用于对响应信息进行加密。第二通信模块320用于接收所述服务器发送的授权代码，并以暗文的形式向所述服务器发送所述响应信息，以及接收所述服务器发送的虚拟钥匙.其中，所述虚拟钥匙由所述服务器在验证所述响应信息通过后生成的；控制模块，用于根据所述虚拟钥匙对车辆进行控制。

[0062] 根据本发明实施例的移动终端，在通讯过程进行加密的基础上采用暗文通讯方式，增加虚拟钥匙授权过程的安全性，同时可以接受虚拟钥匙对车辆进行控制。

[0063] 在本发明的一个实施例中，所述响应信息包括第二移动终端发送的借用人信息、第二移动终端信息和所述授权代码。

[0064] 需要说明的是，本发明实施例的移动终端300的具体实现方式与本发明实施例的车辆的虚拟钥匙授权方法中的第二移动终端的具体实现方式类似，具体请参见车辆的虚拟钥匙授权方法中的第二移动终端部分的描述，为了减少冗余，此处不做赘述。

[0065] 图4是根据本发明一个实施例的服务器的结构框图。如图4所示，根据本发明一个实施例的服务器400，包括：第三加密模块410、第三通信模块420和处理模块430。

[0066] 其中，第三加密模块410用于对授权代码和虚拟钥匙进行加密。第三通信模块420用于接收第一移动终端发送的表单信息，并将所述授权代码以暗文的形式发送给第二移动终端，以及接收所述第二移动终端发送的响应信息，并以暗文的形式向所述第二移动终端发送虚拟钥匙。处理模块430用于根据所述表单信息生成授权代码，并在验证所述响应信息通过后生成所述虚拟钥匙。

[0067] 根据本发明实施例的服务器，在通讯过程进行加密的基础上采用暗文通讯方式，增加虚拟钥匙授权过程的安全性。

[0068] 在本发明的一个实施例中，所述虚拟钥匙具有车辆授权权限，以便所述车辆为所述第二移动终端提供对应于所述虚拟钥匙的车辆授权权限的功能。

[0069] 需要说明的是，本发明实施例的服务器400的具体实现方式与本发明实施例的车辆的虚拟钥匙授权方法中的服务器的具体实现方式类似，具体请参见车辆的虚拟钥匙授权方法中的服务器部分的描述，为了减少冗余，此处不做赘述。

[0070] 图5是根据本发明一个实施例的车辆的虚拟钥匙授权系统的结构框图。如图5所示，根据本发明一个实施例车辆的虚拟钥匙授权系统500，包括：第一移动终端510、第二移动终端520和服务器530。

[0071] 其中，第一移动终端510为上述实施例所述的移动终端200。第二移动终端520为上述实施例所述的移动终端300。服务器为上述实施例所述的服务器400。

[0072] 需要说明的是，本发明实施例的车辆的虚拟钥匙授权系统500的具体实现方式与本发明实施例的车辆的虚拟钥匙授权方法的具体实现方式类似，具体请参见方法部分的描述，为了减少冗余，此处不做赘述。

[0073] 以上仅为本发明的较佳实施例而已，并不用以限制本发明，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。

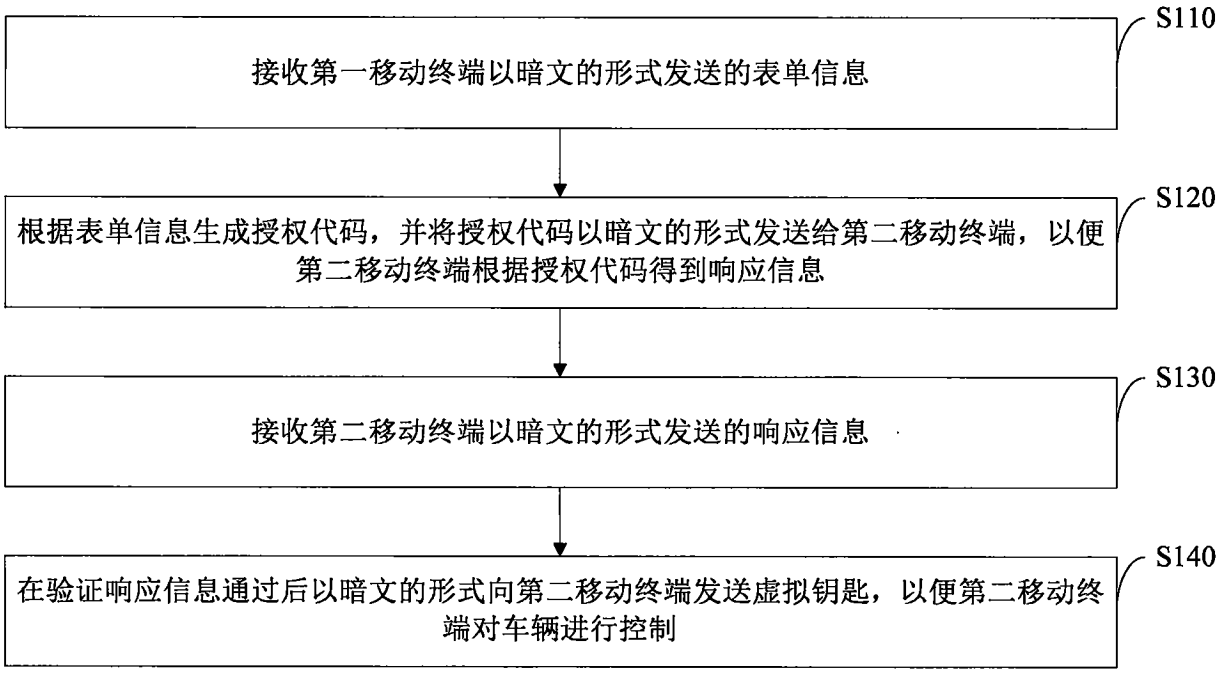

S110
接收第一移动终端以暗文的形式发送的表单信息
S120
根据表单信息生成授权代码，并将授权代码以暗文的形式发送给第二移动终端，以便第二移动终端根据授权代码得到响应信息
S130
接收第二移动终端以暗文的形式发送的响应信息
S140
在验证响应信息通过后以暗文的形式向第二移动终端发送虚拟钥匙，以便第二移动终端对车辆进行控制

图1

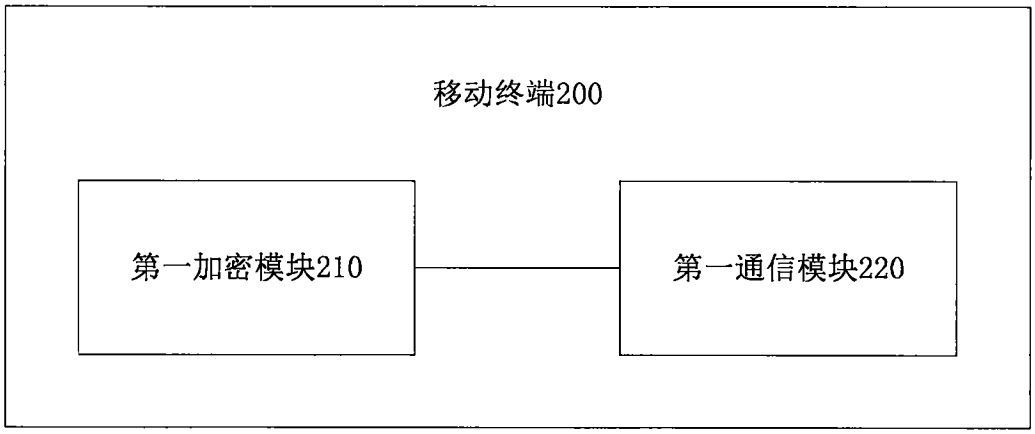

移动终端200
第一加密模块210
第一通信模块220

图2

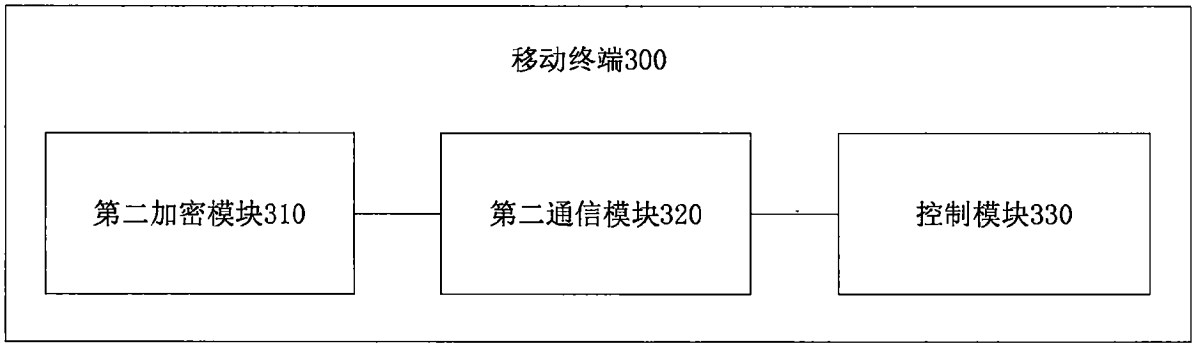

移动终端300
第二加密模块310
第二通信模块320
控制模块330

图3

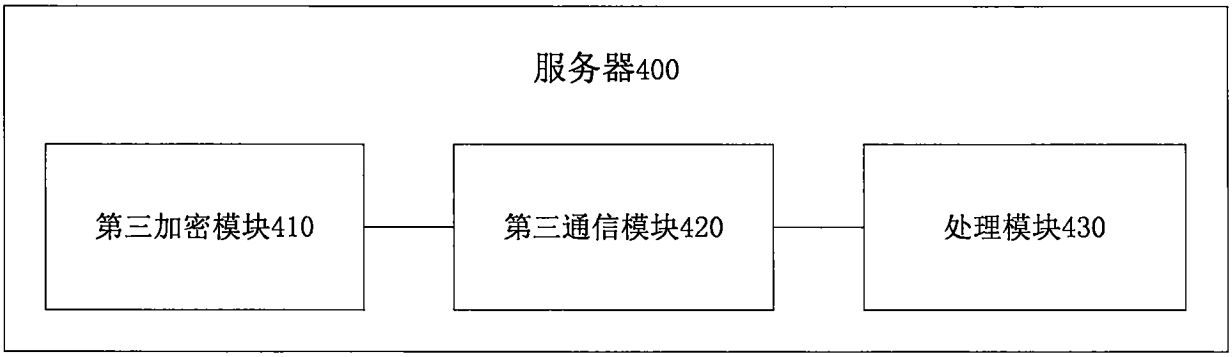

服务器400
第三加密模块410
第三通信模块420
处理模块430

图4

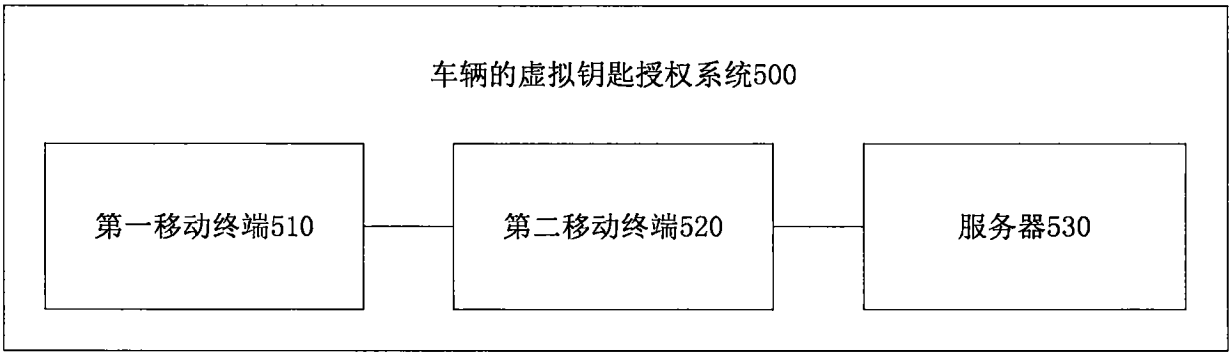

车辆的虚拟钥匙授权系统500
第一移动终端510
第二移动终端520
服务器530

图5