



(12) 发明专利申请

(10) 申请公布号 CN 112068528 A

(43) 申请公布日 2020.12.11

(21) 申请号 202010883724.0

(22) 申请日 2020.08.28

(71) 申请人 深圳市元征科技股份有限公司  
地址 518000 广东省深圳市龙岗区坂田街  
道五和大道北4012号元征工业园

(72) 发明人 刘均 吴华武

(74) 专利代理机构 深圳中一联合知识产权代理  
有限公司 44414

代理人 肖遥

(51) Int.Cl.  
G05B 23/02 (2006.01)

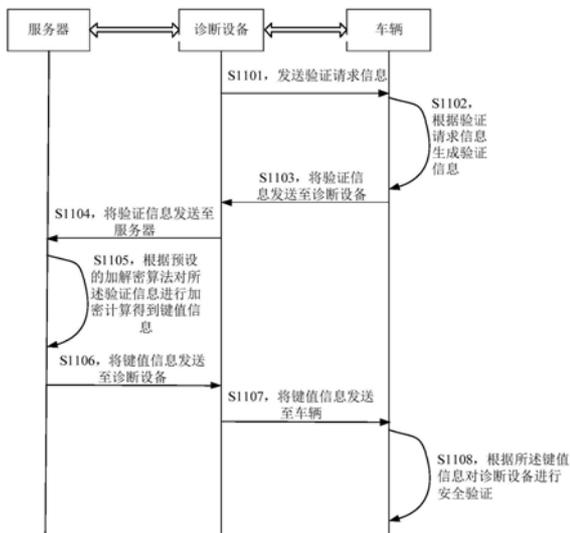
权利要求书2页 说明书10页 附图5页

(54) 发明名称

诊断设备验证方法、车辆、设备及服务器

(57) 摘要

本申请提供一种诊断设备验证方法、车辆、设备及服务器，涉及车辆技术领域，能够提高诊断设备对车辆访问的安全性，解决车辆诊断过程中存在的安全隐患。该方法包括：响应于诊断设备发送的验证请求信息，根据所述验证请求信息生成验证信息；将所述验证信息发送至诊断设备，以指示所述诊断设备将所述验证信息发送至服务器；响应于所述诊断设备返回的键值信息，根据所述键值信息对所述诊断设备进行安全验证。



1. 一种诊断设备验证方法,应用于诊断设备验证系统,所述诊断设备验证系统包括诊断设备、车辆以及服务器,其特征在于,所述方法包括:

所述诊断设备向所述车辆发送验证请求信息;

所述车辆根据所述验证请求信息生成验证信息并发送至所述诊断设备;

所述诊断设备将所述验证信息发送至所述服务器;

所述服务器根据预设的加解密算法对所述验证信息进行加密计算得到键值信息,将所述键值信息发送至所述诊断设备;

所述诊断设备将所述键值信息发送至所述车辆;

所述车辆根据所述键值信息对所述诊断设备进行安全验证。

2. 一种诊断设备验证方法,其特征在于,应用于车辆,所述方法包括:

响应于诊断设备发送的验证请求信息,根据所述验证请求信息生成验证信息;

将所述验证信息发送至诊断设备,以指示所述诊断设备将所述验证信息发送至服务器;

响应于所述诊断设备返回的键值信息,根据所述键值信息对所述诊断设备进行安全验证,所述键值信息为所述服务器根据预设的加解密算法对所述验证信息进行加密计算得到的信息,所述服务器将所述键值信息发送至所述诊断设备,以指示所述诊断设备将所述键值信息返回至所述车辆。

3. 如权利要求2所述的方法,其特征在于,根据所述键值信息对所述诊断设备进行安全验证,包括:

根据所述加解密算法将所述键值信息进行解密,若得到所述验证信息,则确定对所述诊断设备安全验证通过;

根据所述加解密算法将所述键值信息进行解密,若得到所述验证信息,则确定对所述诊断设备安全验证不通过。

4. 一种诊断设备验证方法,其特征在于,应用于诊断设备,所述方法包括:

向车辆发送验证请求信息,所述验证请求信息用于指示所述车辆生成验证信息;

响应于所述车辆发送的所述验证信息,将所述验证信息发送至服务器,所述验证信息用于指示所述服务器根据预设的加解密算法所述验证信息进行加密计算得到键值信息,并将所述键值信息发送至所述诊断设备;

响应于所述服务器发送的所述键值信息,将所述键值信息返回至所述车辆,以指示所述车辆根据所述键值信息对所述诊断设备进行安全验证。

5. 根据权利要求4所述的方法,其特征在于,将所述验证信息发送至服务器,包括:

调用预设的网络接口函数;

通过所述网络接口函数将所述验证信息发送至所述服务器。

6. 根据权利要求4或5所述的方法,其特征在于,将所述键值信息返回至所述车辆,包括:

根据预设的通信协议将所述键值信息进行组帧,生成帧数据;

将所述帧数据返回至所述车辆。

7. 一种诊断设备验证方法,其特征在于,应用于服务器,所述方法包括:

接收诊断设备发送的验证信息,所述验证信息为所述诊断设备向车辆发送验证请求信

息后,以指示所述车辆根据所述验证请求信息生成并返回的验证信息;

根据预设的加解密算法对所述验证信息进行加密计算得到键值信息,将所述键值信息发送至所述诊断设备,以指示所述诊断设备将所述键值信息返回至所述车辆,所述车辆根据所述键值信息对所述诊断设备进行安全验证。

8. 一种车辆,其特征在于,包括:

存储器,用于存储诊断设备验证程序;

处理器,用于执行所述诊断设备验证程序时实现如权利要求2或3所述的诊断设备验证方法。

9. 一种诊断设备,其特征在于,包括:

存储器,用于存储诊断设备验证程序;

处理器,用于执行所述诊断设备验证程序时实现如权利要求4至6任一项所述的诊断设备验证方法。

10. 一种服务器,其特征在于,包括:

存储器,用于存储诊断设备验证程序;

处理器,用于执行所述诊断设备验证程序时实现如权利要求7所述的诊断设备验证方法。

## 诊断设备验证方法、车辆、设备及服务器

### 技术领域

[0001] 本申请涉及车辆技术领域,尤其涉及一种诊断设备验证方法、车辆、设备、及服务器。

### 背景技术

[0002] 目前,由于车辆诊断接口基本都是开放式的,例如OBD (On Board Diagnostics) 接口。使得任何厂家的诊断设备都可以通过开放式的车辆诊断接口与车辆进行通信,导致某些非法分子有机会通过诊断设备对车辆控制器进行修改,甚至进行汽车钥匙匹配等操作。

[0003] 因此,利用开放式的车辆诊断接口对车辆进行诊断存在安全问题。

### 发明内容

[0004] 本申请实施例提供了一种诊断设备验证方法、车辆、设备及服务器,能够有效解决利用开放式的车辆诊断接口对车辆进行诊断时存在的安全问题。

[0005] 第一方面,本申请提供一种诊断设备验证方法,应用于诊断设备验证系统,所述诊断设备验证系统包括诊断设备、车辆以及服务器,所述方法包括:

[0006] 所述诊断设备向所述车辆发送验证请求信息;

[0007] 所述车辆根据所述验证请求信息生成验证信息并发送至所述诊断设备;

[0008] 所述诊断设备将所述验证信息发送至所述服务器;

[0009] 所述服务器根据预设的加解密算法对所述验证信息进行加密计算得到键值信息,将所述键值信息发送至所述诊断设备;

[0010] 所述诊断设备将所述键值信息发送至所述车辆;

[0011] 所述车辆根据所述键值信息对所述诊断设备进行安全验证。

[0012] 第二方面,本申请提供一种诊断设备验证方法,应用于车辆,所述方法包括:

[0013] 响应于诊断设备发送的验证请求信息,根据所述验证请求信息生成验证信息;

[0014] 将所述验证信息发送至诊断设备,以指示所述诊断设备将所述验证信息发送至服务器;

[0015] 响应于所述诊断设备返回的键值信息,根据所述键值信息对所述诊断设备进行安全验证,所述键值信息为所述服务器根据预设的加解密算法对所述验证信息进行加密计算得到的信息,所述服务器将所述键值信息发送至所述诊断设备,以指示所述诊断设备将所述键值信息返回至所述车辆。

[0016] 在一可选的实现方式中,根据所述键值信息对所述诊断设备进行安全验证,包括:

[0017] 根据所述加解密算法将所述键值信息进行解密,若得到所述验证信息,则确定对所述诊断设备安全验证通过;

[0018] 根据所述加解密算法将所述键值信息进行解密,若得到所述验证信息,则确定对所述诊断设备安全验证不通过。

[0019] 第三方面,本申请提供一种诊断设备验证方法,应用于诊断设备,所述方法包括:

- [0020] 向车辆发送验证请求信息,所述验证请求信息用于指示所述车辆生成验证信息;
- [0021] 响应于所述车辆发送的所述验证信息,将所述验证信息发送至服务器,所述验证信息用于指示所述服务器根据预设的加解密算法所述验证信息进行加密计算得到键值信息,并将所述键值信息发送至所述诊断设备;
- [0022] 响应于所述服务器发送的所述键值信息,将所述键值信息返回至所述车辆,以指示所述车辆根据所述键值信息对所述诊断设备进行安全验证。
- [0023] 在一可选的实现方式中,将所述验证信息发送至服务器,包括:
- [0024] 调用预设的网络接口函数;
- [0025] 通过所述网络接口函数将所述验证信息发送至所述服务器。
- [0026] 在一可选的实现方式中,将所述键值信息返回至所述车辆,包括:
- [0027] 根据预设的通信协议将所述键值信息进行组帧,生成帧数据;
- [0028] 将所述帧数据返回至所述车辆。
- [0029] 第四方面,本申请提供一种诊断设备验证方法,应用于服务器,所述方法包括:
- [0030] 接收诊断设备发送的验证信息,所述验证信息为所述诊断设备向车辆发送验证请求信息后,以指示所述车辆根据所述验证请求信息生成并返回的验证信息;
- [0031] 根据预设的加解密算法对所述验证信息进行加密计算得到键值信息,将所述键值信息发送至所述诊断设备,以指示所述诊断设备将所述键值信息返回至所述车辆,所述车辆根据所述键值信息对所述诊断设备进行安全验证。
- [0032] 第五方面,本申请提供一种车辆,包括:
- [0033] 存储器,用于存储诊断设备验证程序;
- [0034] 处理器,用于执行所述诊断设备验证程序时实现如上第一方面所述的诊断设备验证方法。
- [0035] 第六方面,本申请提供一种诊断设备,包括:
- [0036] 存储器,用于存储诊断设备验证程序;
- [0037] 处理器,用于执行所述诊断设备验证程序时实现如上第二方面所述的诊断设备验证方法。
- [0038] 第七方面,本申请提供一种服务器,包括:
- [0039] 存储器,用于存储诊断设备验证程序;
- [0040] 处理器,用于执行所述诊断设备验证程序时实现如上第三方面所述的诊断设备验证方法。
- [0041] 第八方面,本申请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,所述计算机程序被处理器执行时实现如上第一方面所述的诊断设备验证方法,或者所述计算机程序被处理器执行时实现如上第二方面所述的诊断设备验证方法,或者所述计算机程序被处理器执行时实现如上第三方面所述的诊断设备验证方法。
- [0042] 采用本申请第一方面提供的诊断设备验证方法,通过根据诊断设备发送的验证请求信息生成验证信息,并将验证信息发送至诊断设备,以指示诊断设备将验证信息发送至服务器,生成键值信息,进而根据键值信息验证诊断设备的安全性。能够提高诊断设备对车辆访问的安全性,解决车辆诊断过程中存在的安全隐患。
- [0043] 可以理解的是,上述第二方面至第八方面的有益效果可以参见上述第一方面中的

相关描述,在此不再赘述。

### 附图说明

[0044] 为了更清楚地说明本申请实施例中的技术方案,下面将对实施例或现有技术描述中所支持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。

[0045] 图1(a)是本申请第一实施例提供的诊断设备验证系统的示意图;

[0046] 图1(b)是本申请第二实施例提供的诊断设备验证方法的交互流程图;

[0047] 图2是本申请第三实施例提供的诊断设备验证方法的流程图;

[0048] 图3是本申请第四实施例提供的诊断设备验证方法的流程图;

[0049] 图4是本申请第五实施例提供的诊断设备验证方法的流程图;

[0050] 图5是本申请第六实施例提供的车辆的示意图;

[0051] 图6是本申请第七实施例提供的诊断设备的示意图;

[0052] 图7是本申请第八实施例提供的服务器的示意图;

[0053] 图8是本申请第九实施例提供的车辆的示意图;

[0054] 图9是本申请第十实施例提供的诊断设备的示意图;

[0055] 图10是本申请第十一实施例提供的服务器的示意图。

### 具体实施方式

[0056] 以下描述中,为了说明而不是为了限定,提出了诸如特定系统结构、技术之类的具体细节,以便透彻理解本申请实施例。然而,本领域的技术人员应当清楚,在没有这些具体细节的其它实施例中也可以实现本申请。在其它情况中,省略对众所周知的系统、装置、电路以及方法的详细说明,以免不必要的细节妨碍本申请的描述。应当理解,在本申请说明书和所附权利要求书的描述中,术语“第一”、“第二”、“第三”等仅用于区分描述,而不能理解为指示或暗示相对重要性。

[0057] 还应当理解,在本申请说明书中描述的参考“一个实施例”或“一些实施例”等意味着在本申请的一个或多个实施例中包括结合该实施例描述的特定特征、结构或特点。另外还需要说明的是,为了便于描述,附图中仅示出了与本发明相关的部分而非全部内容。在更加详细地讨论示例性实施例之前应当提到的是,一些示例性实施例被描述成作为流程图描绘的处理或方法。虽然流程图将各项操作(或步骤)描述成顺序的处理,但是其中的许多操作可以被并行地、并发地或者同时实施。此外,各项操作的顺序可以被重新安排。当其操作完成时所述处理可以被终止,但是还可以具有未包括在附图中的附加步骤。所述处理可以对应于方法、函数、规程、子例程、子程序等等。

[0058] 首先,在说明本申请实施例提供的诊断设备验证方法之前,结合图1(a),对本申请实施例提供的诊断设备验证方法的原理进行示例性的说明。如图1(a)所示,图1(a)是本申请第一实施例提供的诊断设备验证系统的示意图。由图1(a)可知,本申请实施例提供的诊断设备验证系统100包括诊断设备101、车辆102以及服务器103。其中,诊断设备101分别与车辆102以及服务器103均建立通信连接,例如诊断设备101包括两个通信端口,分别为第一

通信端口和第二通信端口,第一通信端口连接至车辆102的诊断接口OBD,与车辆102连接通信连接,第二通信端口连接至服务器103,与服务器103建立通信连接。

[0059] 示例性地,在诊断设备101分别与车辆102以及服务器103建立通信连接之后,诊断设备101向车辆102发送验证请求信息;车辆102根据诊断设备101发送的验证请求信息生成验证信息,并将该验证信息发送至诊断设备101。诊断设备101将该验证信息发送至服务器103。服务器103在接收到该验证信息后,根据预设的加解密算法对该验证信息进行加密计算得到键值信息,并将该键值信息发送至诊断设备101。诊断设备101进一步将该键值信息发送至车辆102。车辆102可以根据该键值信息对诊断设备101进行安全验证。

[0060] 下面通过具体实施例,对本申请提供的诊断设备验证方法进行示例性的说明。

[0061] 如图1(b)所示,图1(b)是本申请第二实施例提供的诊断设备验证方法的交互流程图。由图1(b)可知,本申请实施例提供的诊断设备验证方法的交换流程包括:

[0062] S1101,诊断设备向车辆发送验证请求信息。

[0063] S1102,车辆根据验证请求信息生成验证信息。

[0064] S1103,车辆将验证信息发送至诊断设备。

[0065] S1104,诊断设备将验证信息发送至服务器。

[0066] S1105,服务器根据预设的加解密算法对所述验证信息进行加密计算得到键值信息。

[0067] S1106,服务器将所述键值信息发送至诊断设备。

[0068] S1107,诊断设备将所述键值信息发送至车辆。

[0069] S1108,车辆根据所述键值信息对诊断设备进行安全验证。

[0070] 通过上述分析可知,本申请实施例提供的诊断设备验证方法,通过根据诊断设备发送的验证请求信息生成验证信息,并将验证信息发送至诊断设备,以指示诊断设备将验证信息发送至服务器,生成键值信息,进而根据键值信息验证诊断设备的安全性。能够提高诊断设备访问开放式车辆诊断接口的安全性,解决车辆诊断过程中存在的安全隐患。

[0071] 请参见图2,图2是本申请第三实施例提供的诊断设备验证方法的流程图。本实施例中的诊断设备验证方法可以由车辆来执行,该车辆具有控制单元以实现本实施例的诊断设备验证方法,其中,所述控制单元可以是例如电子控制单元ECU等。例如,在本申请的实施例中,车辆可以通过电子控制单元实现对诊断设备的验证。如图2所示的诊断设备验证方法可包括:

[0072] S201,响应于诊断设备发送的验证请求信息,根据所述验证请求信息生成验证信息。

[0073] 在本申请实施例中,所述验证请求信息为诊断设备根据预设的车辆诊断协议,例如OBD诊断协议,生成的安全认证请求信息。

[0074] 可以理解地,在诊断设备向车辆发送验证请求信息之前,诊断设备通过车辆的诊断接口,例如OBD接口与车辆建立通信连接。其中,车辆的诊断接口为开放式接口。车辆响应于诊断设备发送的验证请求信息后,作为对验证请求信息的应答,根据所述验证请求信息生成验证信息。例如,所述验证信息为携带有所述验证请求信息的一组字符串。

[0075] 示例性地,车辆通过电子控制单元接收到所述验证请求信息后,根据所述验证请求信息向诊断设备返回所述验证信息。

[0076] S202,将所述验证信息发送至诊断设备,以指示所述诊断设备将所述验证信息发送至服务器。

[0077] 在本申请实施例中,所述服务器为与诊断设备通信连接的服务器,可以是处理诊断数据的后台服务器。

[0078] 示例性地,诊断设备可以通过网络接口函数访问所述服务器。例如,诊断设备通过调用所述网络接口函数,将所述验证信息发送至服务器。

[0079] S203,响应于所述诊断设备返回的键值信息,根据所述键值信息对所述诊断设备进行安全验证,所述键值信息为所述服务器根据预设的加解密算法对所述验证信息进行加密计算得到的信息,所述服务器将所述键值信息发送至所述诊断设备,以指示所述诊断设备将所述键值信息返回至所述车辆。

[0080] 在本申请实施例中,所述加解密算法可以是常见的秘钥生成解密算法,例如数字签名算法和国际数据加密算法等,具体在此不做详细赘述。

[0081] 在本申请的实施例中,所述根据所述键值信息对所述诊断设备进行安全验证,可以包括:根据所述加解密算法将所述键值信息进行解密,若得到所述验证信息,则确定对所述诊断设备安全验证通过;

[0082] 根据所述加解密算法将所述键值信息进行解密,若得到所述验证信息,则确定对所述诊断设备安全验证不通过。其中,所述键值信息可以是key密钥。

[0083] 可以理解地,如果对所述诊断设备安全验证通过,则确定所述诊断设备对所述车辆的访问合法,可以允许所述诊断设备对车辆各系统进行诊断访问;如果对所述诊断设备安全验证不通过,则确定所述诊断设备对所述车辆的访问不合法,不允许所述诊断设备对车辆各系统进行诊断访问。

[0084] 通过上述分析可知,本申请实施例提供的诊断设备验证方法,通过根据诊断设备发送的验证请求信息生成验证信息,并将验证信息发送至诊断设备,以指示诊断设备将验证信息发送至服务器,生成键值信息,进而根据键值信息验证诊断设备的安全性。能够提高诊断设备访问开放式车辆诊断接口的安全性,解决车辆诊断过程中存在的安全隐患。

[0085] 如图3所示,图3是本申请第四实施例提供的诊断设备验证方法的流程图。本实施例中的诊断设备验证方法可以由诊断设备来执行,诊断设备可以通过硬件和/或软件的方式实现。例如,如图3所示的诊断设备验证方法可包括:

[0086] S301,向车辆发送验证请求信息,所述验证请求信息用于指示所述车辆生成验证信息。

[0087] 在本申请实施例中,所述验证请求信息同样为诊断设备根据预设的车辆诊断协议,例如ODB协议、K线协议或关键字协议等,生成的安全认证请求信息。

[0088] 所述诊断设备在与车辆建立通信连接之后,车辆为了确保接入的诊断设备的合法性,基于所述验证请求信息生成验证信息,对诊断设备的合法性进行验证。

[0089] S302,响应于所述车辆发送的所述验证信息,将所述验证信息发送至服务器,所述验证信息用于指示所述服务器根据预设的加解密算法所述验证信息进行加密计算得到键值信息,并将所述键值信息发送至所述诊断设备。

[0090] 在本申请的实施例中,将所述验证信息发送至服务器,可以包括:调用预设的网络接口函数;通过所述网络接口函数将所述验证信息发送至所述服务器。

[0091] S303, 响应于所述服务器发送的所述键值信息, 将所述键值信息返回至所述车辆, 以指示所述车辆根据所述键值信息对所述诊断设备进行安全验证。

[0092] 在本申请的实施例中, 将所述键值信息返回至所述车辆, 可以包括: 根据预设的通信协议将所述键值信息进行组帧, 生成帧数据; 将所述帧数据返回至所述车辆。

[0093] 示例性地, 预设的通信协议可以是基于K线的诊断协议、关键字协议或OBD协议等。

[0094] 根据上述分析可知, 本申请实施例提供的诊断设备验证方法, 通过根据诊断设备发送的验证请求信息生成验证信息, 并将验证信息发送至诊断设备, 以指示诊断设备将验证信息发送至服务器, 生成键值信息, 进而根据键值信息验证诊断设备的安全性。能够提高诊断设备访问开放式车辆诊断接口的安全性, 解决车辆诊断过程中存在的安全隐患。

[0095] 如图4所示, 图4是本申请第五实施例提供的诊断设备验证方法的流程图。本实施例中的诊断设备验证方法可以由服务器来执行, 服务器可以通过硬件和/或软件的方式实现。例如, 如图4所示的诊断设备验证方法可包括:

[0096] S401, 接收诊断设备发送的验证信息, 所述验证信息为所述诊断设备向车辆发送验证请求信息后, 以指示所述车辆根据所述验证请求信息生成并返回的验证信息。

[0097] S402, 根据预设的加解密算法对所述验证信息进行加密计算得到键值信息, 将所述键值信息发送至所述诊断设备, 以指示所述诊断设备将所述键值信息返回至所述车辆, 所述车辆根据所述键值信息对所述诊断设备进行安全验证。

[0098] 通过上述分析可知, 本申请实施例提供的诊断设备验证方法, 通过根据诊断设备发送的验证请求信息生成验证信息, 并将验证信息发送至诊断设备, 以指示诊断设备将验证信息发送至服务器, 生成键值信息, 进而根据键值信息验证诊断设备的安全性。能够提高诊断设备访问开放式车辆诊断接口的安全性, 解决车辆诊断过程中存在的安全隐患。

[0099] 应理解, 上述实施例中各步骤的序号的大小并不意味着执行顺序的先后, 各过程的执行顺序应以其功能和内在逻辑确定, 而不应对本申请实施例的实施过程构成任何限定。

[0100] 基于上述实施例所提供的诊断设备验证方法, 本发明实施例进一步给出实现上述方法实施例的装置实施例。

[0101] 请参见图5, 图5是本申请第六实施例提供的车辆的示意图。包括的各模块用于执行图2对应的实施例中的各步骤。具体请参阅图2对应的实施例中的相关描述。为了便于说明, 仅示出了与本实施例相关的部分。参见图5, 车辆5包括:

[0102] 生成模块501, 用于响应于诊断设备发送的验证请求信息, 根据所述验证请求信息生成验证信息。

[0103] 第一发送模块502, 用于将所述验证信息发送至诊断设备, 以指示所述诊断设备将所述验证信息发送至服务器。

[0104] 验证模块503, 用于响应于所述诊断设备返回的键值信息, 根据所述键值信息对所述诊断设备进行安全验证, 所述键值信息为所述服务器根据预设的加解密算法对所述验证信息进行加密计算得到的信息, 所述服务器将所述键值信息发送至所述诊断设备, 以指示所述诊断设备将所述键值信息返回至所述车辆。

[0105] 在一可选的实现方式中, 所述验证模块503, 包括:

[0106] 第一确定单元, 用于根据所述加解密算法将所述键值信息进行解密, 若得到所述

验证信息,则确定对所述诊断设备安全验证通过。

[0107] 第二确定单元,用于根据所述加解密算法将所述键值信息进行解密,若得到所述验证信息,则确定对所述诊断设备安全验证不通过。

[0108] 如图6所示,图6是本申请第七实施例提供的诊断设备的示意图。包括的各模块用于执行图3对应的实施例中的各步骤。具体请参阅图3对应的实施例中的相关描述。为了便于说明,仅示出了与本实施例相关的部分。参见图6,诊断设备6包括:

[0109] 第二发送模块601,用于向车辆发送验证请求信息,所述验证请求信息用于指示所述车辆生成验证信息。

[0110] 第三发送模块602,用于响应于所述车辆发送的所述验证信息,将所述验证信息发送至服务器,所述验证信息用于指示所述服务器根据预设的加解密算法所述验证信息进行加密计算得到键值信息,并将所述键值信息发送至所述诊断设备。

[0111] 返回模块603,用于响应于所述服务器发送的所述键值信息,将所述键值信息返回至所述车辆,以指示所述车辆根据所述键值信息对所述诊断设备进行安全验证。

[0112] 在一可选的实现方式中,第三发送模块603,包括:

[0113] 调用单元,用于响应于所述车辆发送的所述验证信息,调用预设的网络接口函数。

[0114] 第一发送单元,用于通过所述网络接口函数将所述验证信息发送至所述服务器。

[0115] 在一可选的实现方式中,返回模块603,包括:

[0116] 生成单元,用于根据预设的通信协议将所述键值信息进行组帧,生成帧数据。

[0117] 返回单元,用于将所述帧数据返回至所述车辆。

[0118] 如图7所示,图7是本申请第八实施例提供的服务器的示意图。包括的各模块用于执行图4对应的实施例中的各步骤。具体请参阅图4对应的实施例中的相关描述。为了便于说明,仅示出了与本实施例相关的部分。参见图7,图7所示的服务器7包括:

[0119] 接收模块701,用于接收诊断设备发送的验证信息,所述验证信息为所述诊断设备向车辆发送验证请求信息后,以指示所述车辆根据所述验证请求信息生成并返回的验证信息。

[0120] 第四发送模块702,用于根据预设的加解密算法对所述验证信息进行加密计算得到键值信息,将所述键值信息发送至所述诊断设备,以指示所述诊断设备将所述键值信息返回至所述车辆,所述车辆根据所述键值信息对所述诊断设备进行安全验证。

[0121] 需要说明的是,上述模块之间的信息交互、执行过程等内容,由于与本申请方法实施例基于同一构思,其具体功能及带来的技术效果,具体可参见方法实施例部分,此处不再赘述。

[0122] 图8是本申请第九实施例提供的车辆的示意图。如图8所示,该实施例的车辆8包括:处理器800、存储器801以及存储在所述存储器801中并可在所述处理器800上运行的计算机程序802,例如诊断设备验证程序。处理器800执行所述计算机程序802时实现上述图2所述诊断设备验证方法实施例中的步骤。或者,所述处理器800执行所述计算机程序802时实现上述图5所示模块501至503的功能。

[0123] 示例性的,所述计算机程序802可以被分割成一个或多个模块/单元,所述一个或者多个模块/单元被存储在所述存储器801中,并由处理器800执行,以完成本申请。所述一个或多个模块/单元可以是能够完成特定功能的一系列计算机程序指令段,该指令段用于

描述所述计算机程序802在所述车辆8中的执行过程。例如,所述计算机程序802可以被分割成生成模块、第一发送模块以及验证模块,各模块具体功能请参阅图5对应地实施例中地相关描述,此处不赘述。

[0124] 所述车辆可包括,但不仅限于,处理器800、存储器801。本领域技术人员可以理解,图8仅仅是车辆8的示例,并不构成对车辆8的限定,可以包括比图示更多或更少的部件,或者组合某些部件,或者不同的部件,例如所述视频处理设备还可以包括输入输出设备、网络接入设备、总线等。

[0125] 所称处理器800可以是中央处理单元(Central Processing Unit,CPU),还可以是其他通用处理器、数字信号处理器(Digital Signal Processor,DSP)、专用集成电路(Application Specific Integrated Circuit,ASIC)、现成可编程门阵列(Field-Programmable Gate Array,FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。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。

[0126] 所述存储器801可以是所述车辆8的内部存储单元,例如车辆8的硬盘或内存。所述存储器801也可以是所述车辆8的外部存储设备,例如所述车辆8上配备的插接式硬盘,智能存储卡(Smart Media Card,SMC),安全数字(Secure Digital,SD)卡,闪存卡(Flash Card)等。进一步地,所述存储器801还可以既包括所述车辆8的内部存储单元也包括外部存储设备。所述存储器801用于存储所述计算机程序802以及所述车辆8所支持的其他程序和数据。所述存储器801还可以用于暂时地存储已经输出或者将要输出的数据。

[0127] 图9是本申请第十实施例提供的诊断设备的示意图。如图9所示,该实施例的诊断设备9包括:处理器900、存储器901以及存储在所述存储器901中并可在所述处理器900上运行的计算机程序902,例如诊断设备验证程序。处理器900执行所述计算机程序902时实现上述图3所述诊断设备验证方法实施例中的步骤。或者,所述处理器900执行所述计算机程序902时实现上述图6所示模块601至603的功能。

[0128] 示例性的,所述计算机程序902可以被分割成一个或多个模块/单元,所述一个或多个模块/单元被存储在所述存储器901中,并由处理器900执行,以完成本申请。所述一个或多个模块/单元可以是能够完成特定功能的一系列计算机程序指令段,该指令段用于描述所述计算机程序902在所述诊断设备9中的执行过程。例如,所述计算机程序902可以被分割成第二发送模块、第三发送模块以及返回模块,各模块具体功能请参阅图6对应地实施例中地相关描述,此处不赘述。

[0129] 所述车辆可包括,但不仅限于,处理器900、存储器901。本领域技术人员可以理解,图9仅仅是诊断设备9的示例,并不构成对诊断设备9的限定,可以包括比图示更多或更少的部件,或者组合某些部件,或者不同的部件,例如所述视频处理设备还可以包括输入输出设备、网络接入设备、总线等。

[0130] 所称处理器900可以是中央处理单元(Central Processing Unit,CPU),还可以是其他通用处理器、数字信号处理器(Digital Signal Processor,DSP)、专用集成电路(Application Specific Integrated Circuit,ASIC)、现成可编程门阵列(Field-Programmable Gate Array,FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。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。

等。

[0131] 所述存储器901可以是所述诊断设备9的内部存储单元,例如诊断设备9的硬盘或内存。所述存储器901也可以是所述诊断设备9的外部存储设备,例如所述诊断设备9上配备的插接式硬盘,智能存储卡(Smart Media Card,SMC),安全数字(Secure Digital,SD)卡,闪存卡(Flash Card)等。进一步地,所述存储器901还可以既包括所述诊断设备9的内部存储单元也包括外部存储设备。所述存储器901用于存储所述计算机程序902以及所述诊断设备9所支持的其他程序和数据。所述存储器901还可以用于暂时地存储已经输出或者将要输出的数据。

[0132] 图10是本申请第十一实施例提供的服务器的示意图。如图10所示,该实施例的服务器10包括:处理器1000、存储器1001以及存储在所述存储器1001中并可在所述处理器1000上运行的计算机程序1002,例如诊断设备验证程序。处理器1000执行所述计算机程序1002时实现上述图4所述诊断设备验证方法实施例中的步骤。或者,所述处理器1000执行所述计算机程序1002时实现上述图7所示模块701至702的功能。

[0133] 示例性的,所述计算机程序1002可以被分割成一个或多个模块/单元,所述一个或多个模块/单元被存储在所述存储器1001中,并由处理器1000执行,以完成本申请。所述一个或多个模块/单元可以是能够完成特定功能的一系列计算机程序指令段,该指令段用于描述所述计算机程序1002在所述服务器10中的执行过程。例如,所述计算机程序1002可以被分割成接收模块和第四发送模块,各模块具体功能请参阅图7对应地实施例中地相关描述,此处不赘述。

[0134] 所述服务器可包括,但不仅限于,处理器1000、存储器1001。本领域技术人员可以理解,图10仅仅是服务器10的示例,并不构成对服务器10的限定,可以包括比图示更多或更少的部件,或者组合某些部件,或者不同的部件,例如所述视频处理设备还可以包括输入输出设备、网络接入设备、总线等。

[0135] 所称处理器1000可以是中央处理单元(Central Processing Unit,CPU),还可以是其他通用处理器、数字信号处理器(Digital Signal Processor,DSP)、专用集成电路(Application Specific Integrated Circuit,ASIC)、现成可编程门阵列(Field-Programmable Gate Array,FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。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。

[0136] 所述存储器1001可以是所述服务器10的内部存储单元,例如服务器10的硬盘或内存。所述存储器1001也可以是所述服务器10的外部存储设备,例如所述服务器10上配备的插接式硬盘,智能存储卡(Smart Media Card,SMC),安全数字(Secure Digital,SD)卡,闪存卡(Flash Card)等。进一步地,所述存储器1001还可以既包括所述服务器10的内部存储单元也包括外部存储设备。所述存储器1001用于存储所述计算机程序1002以及所述服务器10所支持的其他程序和数据。所述存储器1001还可以用于暂时地存储已经输出或者将要输出的数据。

[0137] 本申请实施例还提供了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,所述计算机程序被处理器执行时可实现上述诊断设备验证方法。

[0138] 所属领域的技术人员可以清楚地了解到,为了描述的方便和简洁,仅以上述各功

能单元、模块的划分进行举例说明,实际应用中,可以根据需要而将上述功能分配由不同的功能单元、模块完成,即将所述装置的内部结构划分成不同的功能单元或模块,以完成以上描述的全部或者部分功能。实施例中的各功能单元、模块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,也可以采用软件功能单元的形式实现。另外,各功能单元、模块的具体名称也只是为了便于相互区分,并不用于限制本申请的保护范围。上述系统中单元、模块的具体工作过程,可以参考前述方法实施例中的对应过程,在此不再赘述。

[0139] 在上述实施例中,对各个实施例的描述都各有侧重,某个实施例中沒有详述或记载的部分,可以参见其它实施例的相关描述。

[0140] 本领域普通技术人员可以意识到,结合本文中所公开的实施例描述的各示例的单元及算法步骤,能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行,取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能,但是这种实现不应认为超出本申请的范围。

[0141] 以上所述实施例仅用以说明本申请的技术方案,而非对其限制;尽管参照前述实施例对本申请进行了详细的说明,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申请各实施例技术方案的精神和范围,均应包含在本申请的保护范围之内。

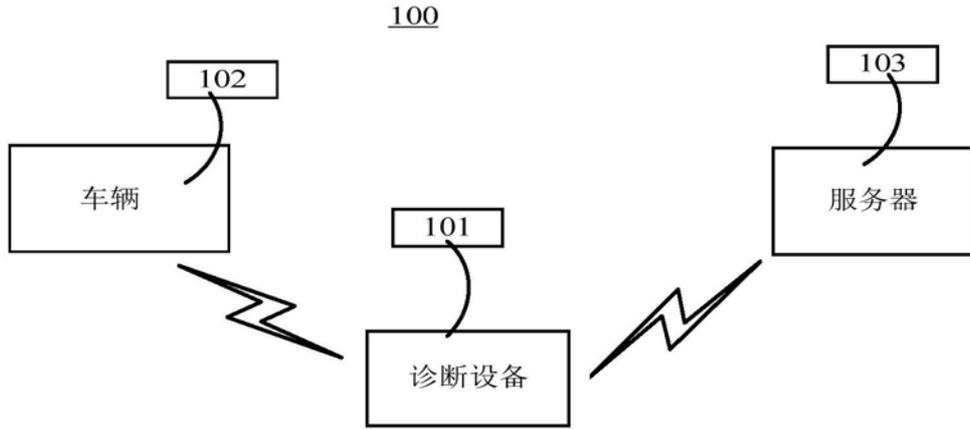


图1 (a)

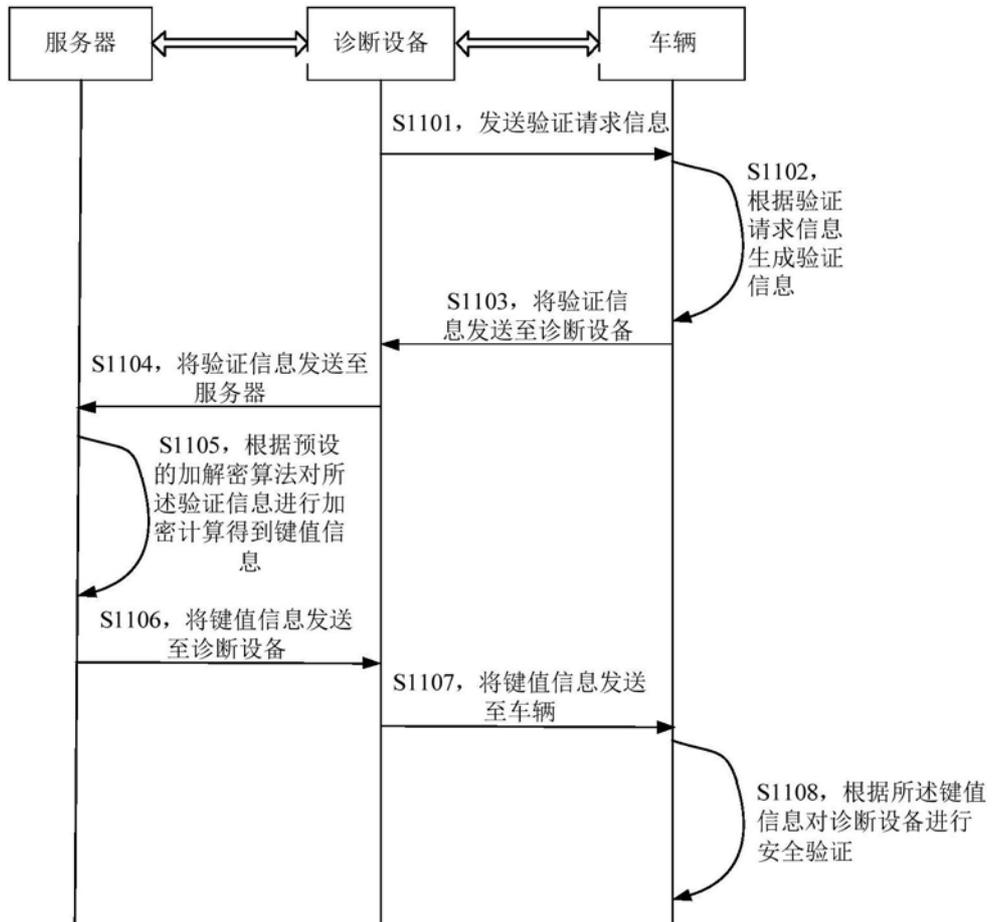


图1 (b)

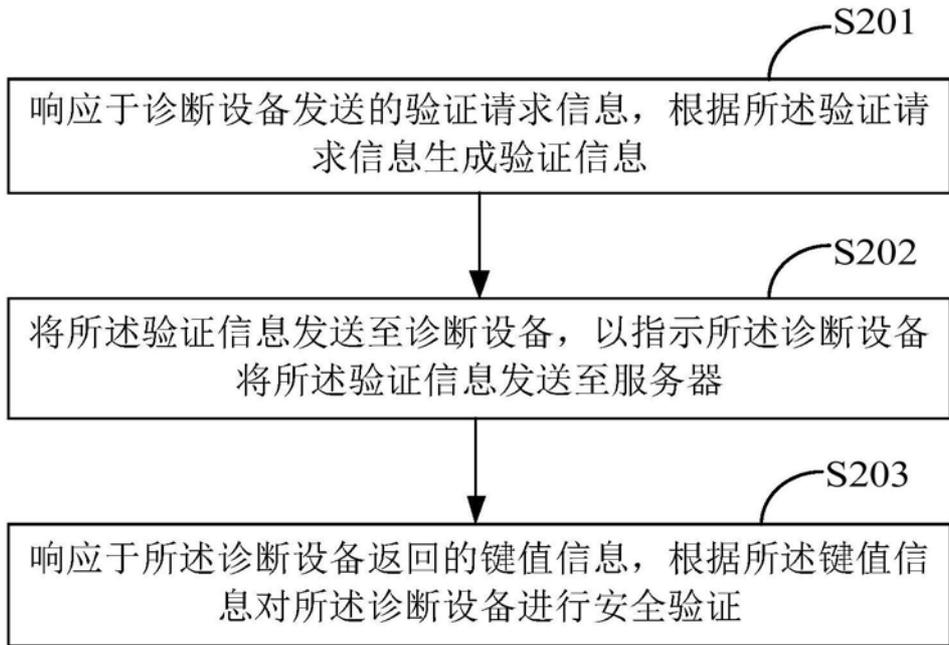


图2

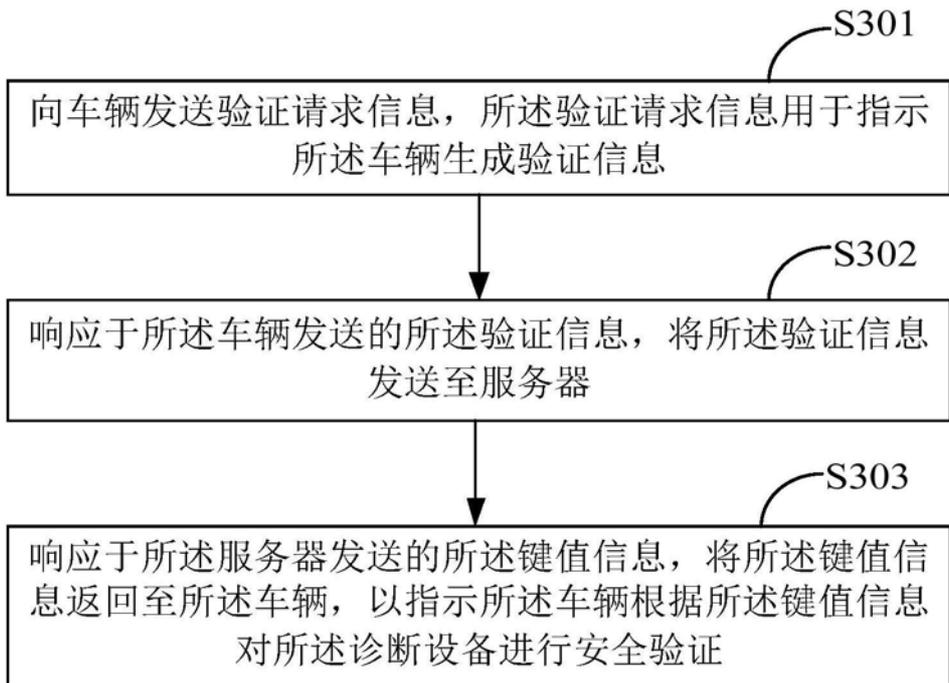


图3

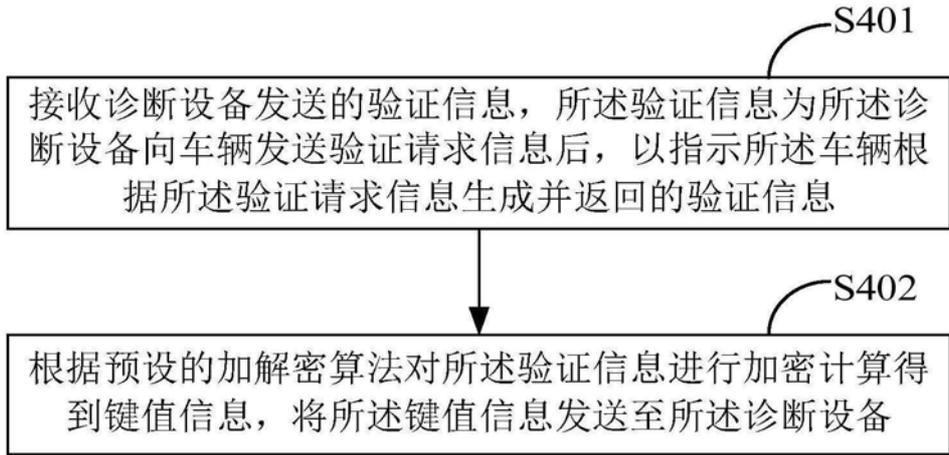


图4

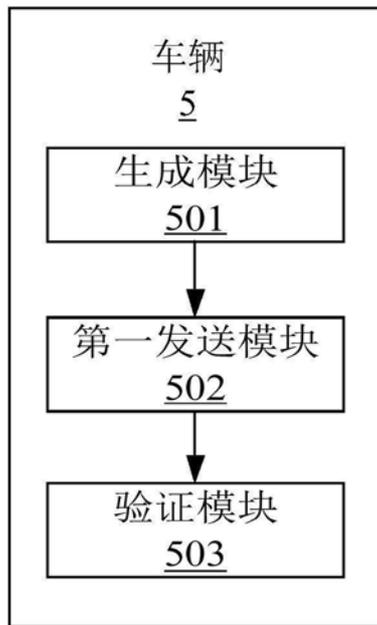


图5

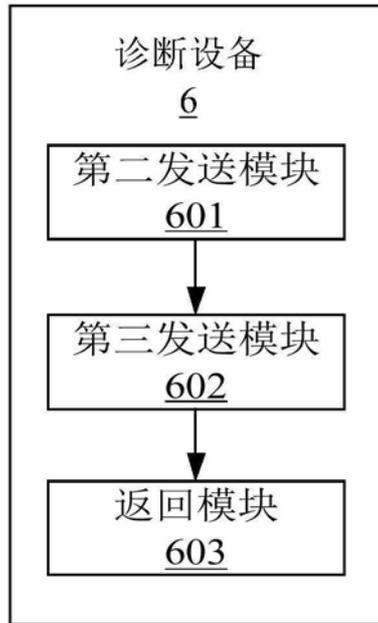


图6

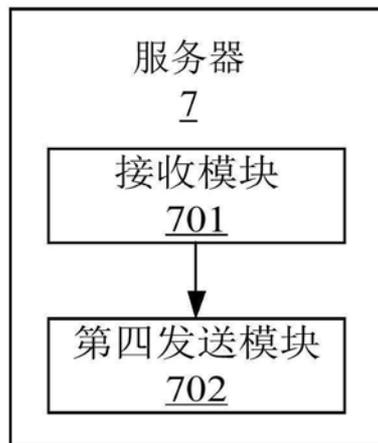


图7

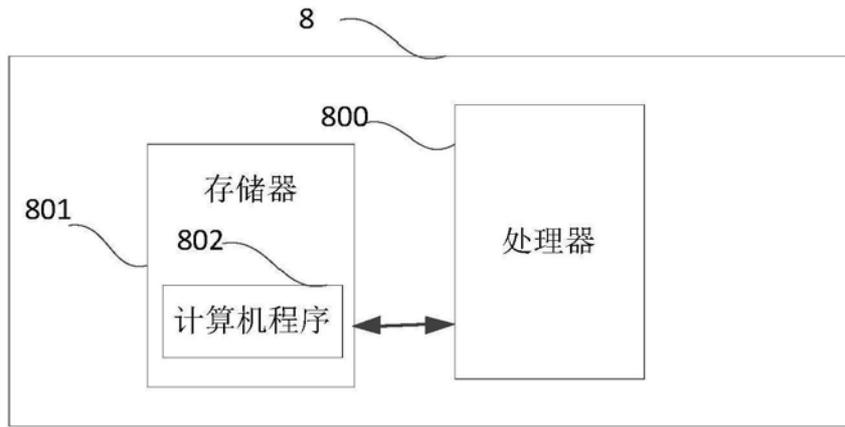


图8

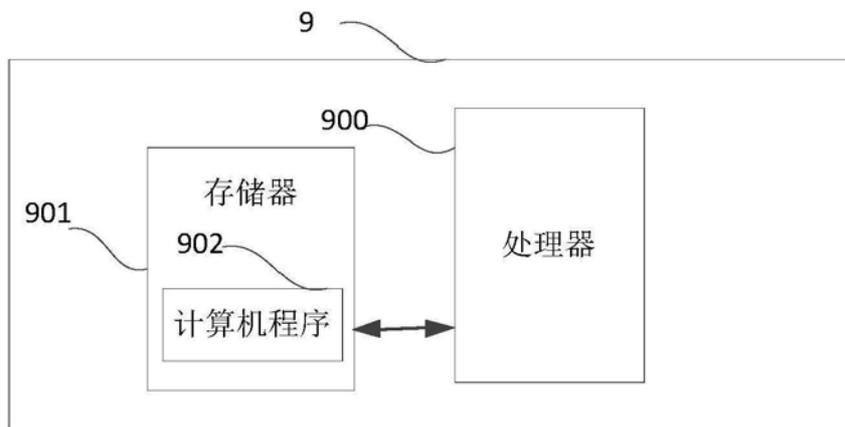


图9

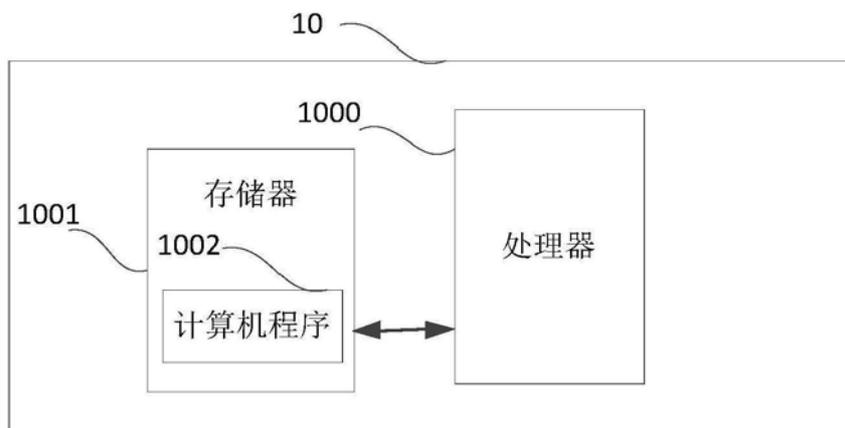


图10