基于隐私保护的验证

技术领域

[01] 本发明实施例涉及数据处理技术领域，尤其涉及一种基于隐私保护的验证方法、装置、设备及系统。

背景技术

[02] 随着计算机技术的迅速发展，如手机等终端设备成为人们生活和工作的必需品，终端设备可为用户提供的服务越来越多样化，例如，用户可通过终端设备控制汽车，如用户可通过手机启动汽车、为汽车上锁等。

[03] 为保证终端设备发出的控车指令在传输过程中的安全性，终端设备可通过密钥对控车指令进行加密，并将加密后的控车指令发送给汽车，汽车在通过密钥对控车指令进行解密，并执行解密得到的控车指令。但是，在上述过程中，由于对控车指令的加密方式简单，且未对终端设备以及车载设备进行身份验证，导致控车指令在传输过程中的安全性差，因此，需要一种能够提高控车指令在传输过程中的安全性的解决方案。

发明内容

[04] 本说明书实施例的目的是提供一种基于隐私保护的验证方法、装置、设备及系统，以提供一种能够提高控车指令在传输过程中的安全性的解决方案。

[05] 为了实现上述技术方案，本说明书实施例是这样实现的：第一方面，一种基于隐私保护的验证方法，应用于终端设备，包括：将针对控制车载设备的本地的身份验证请求发送给第一服务器，所述第一服务器用于针对所述身份验证请求，生成与所述终端设备、所述车载设备对应的目标验证信息；接收所述第一服务器发送的所述目标验证信息和预先构建的证书链，基于所述终端设备的预设密钥，对所述证书链和所述目标验证信息进行验证，得到验证结果，所述证书链为由所述第一服务器信息、所述第一服务器的预设密钥、所述终端设备的设备信息、所述终端设备的预设密钥、所述车载设备的设备信息和所述车载设备的预设密钥生成的多级证书链；在所述验证结果为验证通过的情况下，基于所述目标验证信息对控车指令进行处理，并将处理后的控车指令发送给所述车载设备，以使所述车载设备基于所述目标验证信息和所述证书链，对所述控车指令进行处理。

[06] 第二方面，本说明书实施例提供的一种基于隐私保护的验证方法，应用于车载设备，包括：接收第一服务器发送的与终端设备、所述车载设备对应的目标验证信息和预先构建的证书链，所述证书链为由所述第一服务器信息、所述第一服务器的预设密钥、所述终端设备的设备信息、所述终端设备的预设密钥、所述车载设备的设备信息和所述车载设备的预设密钥生成的多级证书链；基于所述车载设备的预设密钥，对所述证书链和所述目标验证信息进行验证，得到验证结果；在所述验证结果为验证通过的情况下，基于所述目标验证信息，对所述终端设备发送的处理后的控车指令进行处理，得到控车指令，并执行所述控车指令，所述处理后的控车指令为所述终端设备基于所述目标验证信息对所述控车指令进行处理得到的指令。

[07] 第三方面，本说明书实施例提供的一种基于隐私保护的验证方法，应用于第一服务器，包括：在接收到终端设备发送的针对控制车载设备的本地的身份验证请求的情况下，生成与所述终端设备、所述车载设备对应的目标验证信息；将所述目标验证信息和预先构建的证书链发送给所述终端设备和所述车载设备，以使所述终端设备基于所述终端设备的预设密钥，对所述证书链和所述目标验证信息进行验证通过后，基于所述目标验证信息，对控车指令进行处理，使所述车载设备基于所述车载设备的预设密钥，对所述证书链和所述目标验证信息进行验证通过后，基于所述目标验证信息，对所述终端设备发送的所述处理后的控车指令进行处理，所述证书链为由所述第一服务器信息、所述第一服务器的预设密钥、所述终端设备的设备信息、所述终端设备的预设密钥、所述车载设备的设备信息和所述车载设备的预设密钥生成的多级证书链。

[08] 第四方面，本说明书实施例提供了一种基于隐私保护的验证系统，所述系统包括终端设备、车载设备和第一服务器。其中，所述终端设备，用于将针对控制所述车载设备的本地的身份验证请求发送给所述第一服务器；所述第一服务器，用于生成与所述终端设备、所述车载设备对应的目标验证信息，并将所述目标验证信息和预先构建的证书链

发送给所述终端设备和所述车载设备；所述证书链为由所述第一服务器信息、所述第一服务器的预设密钥、所述终端设备的设备信息、所述终端设备的预设密钥、所述车载设备的设备信息和所述车载设备的预设密钥生成的多级证书链；所述终端设备，用于基于所述终端设备的预设密钥，对所述证书链和所述目标验证信息进行验证，得到第一验证结果；在所述第一验证结果为验证通过的情况下，基于所述目标验证信息对控车指令进行处理，并将处理后的所述控车指令发送给所述车载设备；所述车载设备，用于基于所述车载设备的预设密钥，对所述证书链和所述目标验证信息进行验证，得到第二验证结果；在所述第二验证结果为验证通过的情况下，基于所述目标验证信息对接收到的所述处理后的控车指令进行处理，得到所述控车指令，并执行所述控车指令。

[09] 第五方面，本说明书实施例提供了一种基于隐私保护的验证装置，所述装置包括：请求发送模块，用于将针对控制车载设备的本地的身份验证请求发送给第一服务器，所述第一服务器用于针对所述身份验证请求，生成与所述基于隐私保护的验证装置、所述车载设备对应的目标验证信息；验证模块，用于接收所述第一服务器发送的所述目标验证信息和预先构建的证书链，基于所述终端设备的预设密钥，对所述证书链和所述目标验证信息进行验证，得到验证结果，所述证书链为由所述第一服务器信息、所述第一服务器的预设密钥、所述基于隐私保护的验证装置的设备信息、所述基于隐私保护的验证装置的预设密钥、所述车载设备的设备信息和所述车载设备的预设密钥生成的多级证书链；指令发送模块，用于在所述验证结果为验证通过的情况下，基于所述目标验证信息对控车指令进行处理，并将处理后的控车指令发送给所述车载设备，以使所述车载设备基于所述目标验证信息和所述证书链，对所述控车指令进行处理。

[10] 第六方面，本说明书实施例提供了一种基于隐私保护的验证装置，所述装置包括：信息接收模块，用于接收第一服务器发送的与终端设备、所述基于隐私保护的验证装置对应的目标验证信息和预先构建的证书链，所述证书链为由所述第一服务器信息、所述第一服务器的预设密钥、所述终端设备的设备信息、所述终端设备的预设密钥、所述基于隐私保护的验证装置的设备信息和所述基于隐私保护的验证装置的预设密钥生成的多级证书链；验证模块，用于基于所述基于隐私保护的验证装置的预设密钥，对所述证书链和所述目标验证信息进行验证，得到验证结果；指令处理模块，用于在所述验证结果为验证通过的情况下，基于所述目标验证信息，对所述终端设备发送的处理后的控车指令进行处理，得到控车指令，并执行所述控车指令，所述处理后的控车指令为所述终端设备基于所述目标验证信息对所述控车指令进行处理得到的指令。

[11] 第七方面，本说明书实施例提供了一种基于隐私保护的验证装置，所述装置包括：信息生成模块，用于在接收到终端设备发送的针对控制车载设备的本地的身份验证请求的情况下，生成与所述终端设备、所述车载设备对应的目标验证信息；信息发送模块，用于将所述目标验证信息和预先构建的证书链发送给所述终端设备和所述车载设备，以使所述终端设备基于所述终端设备的预设密钥，对所述证书链和所述目标验证信息进行验证通过后，基于所述目标验证信息，对控车指令进行处理，使所述车载设备基于所述车载设备的预设密钥，对所述证书链和所述目标验证信息进行验证通过后，基于所述目标验证信息，对所述终端设备发送的所述处理后的控车指令进行处理，所述证书链为由所述基于隐私保护的验证装置信息、所述基于隐私保护的验证装置的预设密钥、所述终端设备的设备信息、所述终端设备的预设密钥、所述车载设备的设备信息和所述车载设备的预设密钥生成的多级证书链。

[12] 第八方面，本说明书实施例提供了一种基于隐私保护的验证设备，所述基于隐私保护的验证设备包括：处理器；以及被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器：将针对控制车载设备的本地的身份验证请求发送给第一服务器，所述第一服务器用于针对所述身份验证请求，生成与所述基于隐私保护的验证设备、所述车载设备对应的目标验证信息；接收所述第一服务器发送的所述目标验证信息和预先构建的证书链，基于所述基于隐私保护的验证设备的预设密钥，对所述证书链和所述目标验证信息进行验证，得到验证结果，所述证书链为由所述第一服务器信息、所述第一服务器的预设密钥、所述基于隐私保护的验证设备的设备信息、所述基于隐私保护的验证设备的预设密钥、所述车载设备的设备信息和所述车载设备的预设密钥生成的多级证书链；在所述验证结果为验证通过的情况下，基于所述目标验证信息对控车指令进行处理，并将处理后的控车指令发送给所述车载设备，以使所述车载设备基于所述

目标验证信息和所述证书链，对所述控车指令进行处理。

[13]第九方面，本说明书实施例提供了一种基于隐私保护的验证设备，所述基于隐私保护的验证设备包括处理器以及被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器：接收第一服务器发送的与终端设备、所述基于隐私保护的验证设备对应的目标验证信息和预先构建的证书链，所述证书链为由所述第一服务器信息、所述第一服务器的预设密钥、所述终端设备的设备信息、所述终端设备的预设密钥、所述基于隐私保护的验证设备的设备信息和所述基于隐私保护的验证设备的预设密钥生成的多级证书链；基于所述基于隐私保护的验证设备的预设密钥，对所述证书链和所述目标验证信息进行验证；在验证通过后，基于所述目标验证信息，对所述终端设备发送的处理后的控车指令进行处理，得到控车指令，并执行所述控车指令，所述处理后的控车指令为所述终端设备基于所述目标验证信息对所述控车指令进行处理得到的指令。

[14]第十方面，本说明书实施例提供了一种基于隐私保护的验证设备，所述基于隐私保护的验证设备包括处理器以及被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器：在接收到终端设备发送的针对控制车载设备的本地的身份验证请求的情况下，生成与所述终端设备、所述车载设备对应的目标验证信息；将所述目标验证信息和预先构建的证书链发送给所述终端设备和所述车载设备，以使所述终端设备基于所述终端设备的预设密钥，对所述证书链和所述目标验证信息进行验证通过后，基于所述目标验证信息，对控车指令进行处理，使所述车载设备基于所述车载设备的预设密钥，对所述证书链和所述目标验证信息进行验证通过后，基于所述目标验证信息，对所述终端设备发送的所述处理后的控车指令进行处理，所述证书链为由所述基于隐私保护的验证设备信息、所述基于隐私保护的验证设备的预设密钥、所述终端设备的设备信息、所述终端设备的预设密钥、所述车载设备的设备信息和所述车载设备的预设密钥生成的多级证书链。

附图说明

[15]图 1A 为本说明书一种基于隐私保护的验证方法实施例的流程图；

[16]图 1B 为本说明书一种基于隐私保护的验证方法的处理过程示意图；

[17]图 2A 为本说明书又一种基于隐私保护的验证方法的处理过程示意图；

[18]图 2B 为本说明书又一种基于隐私保护的验证方法的处理过程示意图；

[19]图 3A 为本说明书一种终端设备中配置的可信执行环境的示意图；

[20]图 3B 为本说明书一种终端设备中配置的可信执行环境的示意图；

[21]图 4A 为本说明书又一种基于隐私保护的验证方法实施例的流程图；

[22]图 4B 为本说明书又一种基于隐私保护的验证方法的处理过程示意图；

[23]图 5A 为本说明书又一种基于隐私保护的验证方法的处理过程示意图；

[24]图 5B 为本说明书又一种基于隐私保护的验证方法的处理过程示意图；

[25]图 6 为本说明书又一种基于隐私保护的验证方法的处理过程示意图；

[26]图 7 为本说明书一种基于隐私保护的验证系统的示意图；

[27]图 8 为本说明书一种基于隐私保护的验证装置实施例的结构示意图；

[28]图 9 为本说明书另一种基于隐私保护的验证装置实施例的结构示意图；

[29]图 10 为本说明书另一种基于隐私保护的验证装置实施例的结构示意图；

[30]图 11 为本说明书一种基于隐私保护的验证设备的结构示意图。

具体实施方式

实施例一

[31]如图 1A 和 1B 所示，本说明书实施例提供一种基于隐私保护的验证方法，该方法的执行主体可为终端设备，终端设备可如手机、平板电脑等移动终端设备，也可如个人计算机等设备。该方法具体可包括以下步骤：

[32]在 S102 中，将针对控制车载设备的本地的身份验证请求发送给第一服务器。

[33]车载设备可是待控制车辆中安装的，能够基于预设信息传输方式与终端设备通信的设备，且车载设备还可执行终端设备发送的控车指令（即车载设备可基于终端设备发送的控车指令控制该待控制车辆），第一服务器可用于针对身份验证请求，生成与终端设备、车载设备对应的目标验证信息，目标验证信息可是任意能够用于验证终端设备、车

载设备的信息，例如，第一服务器可基于预设信息生成算法（如预设随机数生成算法、预设哈希值生成算法等），生成与终端设备的设备标识、车载设备的设备标识对应的信息，并将该信息作为目标验证信息，此外，目标验证信息的生成方法还可有多种，可根据实际应用场景的不同而有所不同，本说明书实施例对此不做具体限定。

[34]随着计算机技术的迅速发展，如手机等终端设备成为人们生活和工作的必需品，终端设备可为用户提供的服务越来越多样化，例如，用户可通过终端设备控制汽车，如用户可通过手机启动汽车、为汽车上锁等。为保证终端设备发出的控车指令在传输过程中的安全性，终端设备可通过密钥对控车指令进行加密，并将加密后的控车指令发送给汽车，汽车在通过密钥对控车指令进行解密，并执行解密得到的控车指令。但是，在上述过程中，由于对控车指令的加密方式简单，且未对终端设备以及车载设备进行身份验证，导致控车指令在传输过程中的安全性差，因此，需要一种能够提高控车指令在传输过程中的安全性的解决方案。为此，本说明书实施例提供一种可解决上述问题的技术方案，具体可参见下述内容。

[35]终端设备中可安装有用于控制车辆的应用程序，终端设备在检测到用户启动该应用程序，并在检测到用户触发某一控车指令的情况下，可将针对控制车载设备的本地的身份验证请求发送给第一服务器。

[36]在 S104 中，接收第一服务器发送的目标验证信息和预先构建的证书链，基于终端设备的预设密钥，对证书链和目标验证信息进行验证，得到验证结果。

[37]证书链可为由第一服务器信息、第一服务器的预设密钥、终端设备的设备信息、终端设备的预设密钥、车载设备的设备信息和车载设备的预设密钥生成的多级证书链。第一服务器信息可包含用第一服务器的唯一标识信息，终端设备的设备信息也可包含终端设备的唯一标识信息，车载设备的设备信息也可包含车载设备的唯一标识信息。

[38]由于终端设备接收到的证书链是基于第一服务器信息、第一服务器的预设密钥、终端设备的设备信息、终端设备的预设密钥、车载设备的设备信息和车载设备的预设密钥生成的多级证书链，可基于终端设备的预设密钥，对证书链中与终端设备相关的一级或多级证书进行验证，得到验证结果 1。同时，也可根据终端设备的预设密钥，对目标验证信息进行验证，得到验证结果 2，并根据验证结果 1 和验证结果 2，确定验证结果。

[39]在目标验证信息是第一服务器基于终端设备的预设密钥、车载设备的预设密钥，对终端设备的设备信息进行处理得到的信息的情况下，终端设备还可基于证书链、终端设备的预设密钥，获取车载设备的预设密钥，在通过终端设备的预设密钥，以及得到的车载设备的预设密钥，对目标验证信息进行处理，得到对应的终端设备的设备信息，并通过本地存储的终端设备的设备信息，对得到的终端设备的设备信息进行匹配验证，得到验证结果 2。

[40]上述验证结果的确定方法是一种可选地、可实现的确定方法，在实际应用场景中，还可有多种不同的验证结果的确定方法，可根据实际应用场景的不同而有所不同，本说明书实施例对此不做具体限定。

[41]在 S106 中，在验证结果为验证通过的情况下，基于目标验证信息对控车指令进行处理，并将处理后的控车指令发送给车载设备，以使车载设备基于目标验证信息和证书链，对控车指令进行处理。

[42]在验证结果为验证通过的情况下，可基于目标验证信息，对控车指令进行加密处理，并将加密处理后的控车指令发送给车载设备，以使车载设备基于本地存储的目标验证信息，对加密处理后的控车指令进行解密处理，并执行解密处理后的控车指令。

[43]或者，在验证结果为验证通过的情况下，终端设备还可基于终端设备的预设密钥对控车指令进行加密处理，得到加密处理后的控车指令，在通过目标验证信息，对加密处理后的控车指令进行签名处理，得到对应的签名信息，再将签名信息和加密处理后的控车指令发送给车载设备，以使车载设备基于证书链，获取终端设备的预设密钥，并通过终端设备的预设密钥，对接收的签名信息进行验证，同时，车载设备还可通过本地存储的目标验证信息，对加密处理后的控车指令进行解密处理，在签名信息验证通过的情况下，车载设备可执行解密得到的控车指令。

[44]上述控车指令的处理方法是一种可选地、可实现的处理方法，在实际应用场景中，还可有多种不同的处理方法，可根据实际应用场景的不同而有所不同，本说明书实施例对此不做具体限定。

[45]此外，终端设备可如手机、平板电脑等移动终端设备，终端设备可基于预设短距离传输方式（如蓝牙、红外等短距离传输方式），与车载设备进行信息传输。

[46]另外，为保证数据处理的安全性，终端设备中可安装有可信执行环境（如 Trusted Execution Environment，TEE），终端设备可在本地安装的 TEE 中，基于终端设备的预设密钥，对证书链和目标验证信息进行验证，得到验证结果，以及在验证结果为验证通过的情况下，基于目标验证信息对控车指令进行处理。

[47]本说明书实施例提供一种基于隐私保护的验证方法，将针对控制车载设备的本地的身份验证请求发送给第一服务器，第一服务器用于针对身份验证请求，生成与终端设备、车载设备对应的目标验证信息，接收第一服务器发送的目标验证信息和预先构建的证书链，基于终端设备的预设密钥，对证书链和目标验证信息进行验证，得到验证结果，证书链为由第一服务器信息、第一服务器的预设密钥、终端设备的设备信息、终端设备的预设密钥、车载设备的设备信息和车载设备的预设密钥生成的多级证书链，在验证结果为验证通过的情况下，基于目标验证信息对控车指令进行处理，并将处理后的控车指令发送给车载设备，以使车载设备基于目标验证信息和证书链，对控车指令进行处理。这样，由于目标验证信息是第一服务器生成的与终端设备和车载设备对应的验证信息，且证书链也是由第一服务器、终端设备和车载设备的相关信息构成的证书链，所以，终端设备和车载设备可分别通过目标验证信息和证书链，对本地以及另一方（即车载设备）进行身份验证，在验证结果为通过的情况下，在通过目标验证信息对控车指令进行处理，可提高控车指令在传输过程中的安全性。

实施例二

[48]如图 2A 和图 2B 所示，本说明书实施例提供一种基于隐私保护的验证方法，该方法的执行主体可为终端设备，终端设备可如手机、平板电脑等移动终端设备，也可如个人计算机等设备。该方法具体可包括以下步骤：在 S202 中，将针对控制车载设备的本地的身份验证请求发送给第一服务器。

[49]上述 S202 的具体处理过程可参见上述实施例一中 S102 的相关内容，在此不再赘述。

[50]在 S204 中，接收第一服务器的服务器信息以及第一服务器的第一公钥。

[51]第一公钥可为第一服务器基于预设密钥生成算法，生成的与第一服务器对应的密钥，第一服务器的服务器信息可包含第一服务器的标识信息、第一服务器的属性信息等。

[52]在 S206 中，基于预设密钥生成算法，生成与终端设备对应的第二私钥和第二公钥。

[53]终端设备可基于预设非对称密钥生成算法，生成与终端设备的设备信息对应的第二私钥和第二公钥，第二私钥和第二公钥可是终端设备生成的根密钥。

[54]在 S208 中，基于第二私钥，对终端设备的设备信息进行签名，得到第一签名信息。

[55]终端设备可通过预设签名生成算法，基于第二私钥，对终端设备的设备信息进行签名，得到第一签名信息。终端设备的设备信息可包含终端设备的标识信息，如终端设备的设备ID、产品序列号（Serial Number，SN）、局域网地址（Media Access Control Address，MAC）等。

[56]在 S210 中，基于第二公钥、终端设备的设备信息和第一签名信息，生成根证书。

[57]在 S212 中，基于第二私钥，对服务器信息进行签名，得到第二签名信息。

[58]在 S214 中，基于第一公钥、服务器信息和第二签名信息，生成第二证书。

[59]根证书除可包含上述第二公钥、终端设备的设备信息和第一签名信息之外，还可包含该根证书的有效期等相关信息，第二证书中可包含第二证书的有效期等相关信息。

[60]在 S216 中，将根证书和第二证书构成的第一证书链发送给第一服务器，以使第一服务器基于第一证书链、车载设备的设备信息和车载设备的预设密钥，构建证书链。

[61]预先构建的证书链可是包含多级证书的链式结构，可由根证书和第二证书构建第一证书链，第二证书即可作为第一证书链中的二级证书。

[62]第一服务器可基于第一证书链、车载设备的设备信息和车载设备的预设密钥，构建包含三级证书的证书链，即可由车载设备的设备信息和车载设备的预设密钥生成第三证书，并添加到第一证书链中，以构成包含三级证书的证书链，第三证书即为该证书链中的第三级证书。

[63]在 S218 中，基于预设密钥生成算法，生成与用户对应的第四公钥。

[64]可在终端设备的 TEE 中，基于预设密钥生成算法，生成与用户对应的第四公钥。

[65]上述 S218 的处理方式可多种多样，以下提供一种可选的实现方式，具体可参见下

述步骤一~步骤三处理：步骤一，将针对用户的身份验证请求发送给第二服务器。第二服务器可是终端设备中安装的用于控制车载设备的应用程序对应的服务器。
[66]在生成与用户对应的第四公钥之前，可对用户进行身份验证，例如，终端设备在检测到用户运行应用程序，且触发登录请求的情况下，可将针对用户的身份验证请求发送给第二服务器。
[67]步骤二，接收第二服务器基于身份验证请求生成的目标令牌。目标令牌可是第二服务器基于预先存储的用户的相关信息生成的令牌。
[68]步骤三，基于目标令牌，对用户进行身份验证，并在身份验证结果为验证通过的情况下，基于预设密钥生成算法，生成与用户对应的第四公钥。
[69]以目标令牌为第二服务器通过预设哈希值生成算法，生成的与预先存储的用户的生物特征信息对应的令牌为例，终端设备可获取用户的生物特征信息（如指纹信息、虹膜信息等），并基于预设哈希值生成算法，生成与获取的用户的生物特征信息对应的验证信息，再将生成的验证信息与目标令牌进行匹配验证，在验证结果为验证通过的情况下，可在终端设备的 TEE 中，基于预设密钥生成算法，生成与用户对应的第四公钥。
[70]在 S220 中，将第四公钥以及终端设备的设备信息发送给第一服务器，以使第一服务器基于终端设备的设备信息、第四公钥、车载设备的预设密钥以及车载设备的设备信息，生成目标验证信息。
[71]在 S222 中，接收第一服务器发送的目标验证信息和预先构建的证书链。接收到的目标验证信息可包含用户的第四公钥、车载设备的预设密钥等信息。
[72]在 S224 中，接收第一服务器发送的第一可验证信息。第一可验证信息可为第一服务器基于第一服务器的第一私钥，对目标验证信息进行加密处理，得到的与目标验证信息对应的信息。
[73]在 S226 中，基于第一服务器的第一公钥、终端设备的第二公钥，对证书链中的根证书和第二证书进行验证处理，得到第一验证结果。
[74]由于第二证书是基于第一公钥、服务器信息和第二签名信息生成的，而第二签名信息是基于终端设备的第二私钥，对服务器信息进行签名得到的，所以，终端设备可通过第二私钥，对第二证书中的服务器信息进行签名，得到对应的签名信息，并与第二证书中的第二签名信息进行匹配验证，以得到第一验证结果 1。
[75]同样的，由于根证书是由基于第二公钥、终端设备的设备信息和第一签名信息生成的，而第一签名信息是终端设备基于第二私钥，对终端设备的设备信息进行签名得到的，所以，终端设备可基于第二私钥，对根证书中的终端设备的设备信息进行签名，得到对应的签名信息，并与根证书中的第一签名信息进行匹配验证，以得到第一验证结果 2。
[76]然后，终端设备可基于第一验证结果 1 和第一验证结果 2，确定第一验证结果。
[77]上述第一验证结果的确定方法是一种可选地、可实现的确定方法，在实际应用场景中，还可有多种不同的确定方法，可根据实际应用场景的不同而有所不同，本说明书实施例对此不作具体限定。
[78]在 S228 中，基于第一服务器的第一公钥和目标验证信息，对第一可验证信息进行验证，得到第二验证结果。由于第一可验证信息是第一服务器基于第一服务器的第一私钥，对目标验证信息进行加密处理得到的信息，所以，终端设备可通过第一服务器的第一公钥，对第一可验证信息进行解密处理，得到对应的目标验证信息，并与接收到的目标验证信息进行匹配验证，得到第二验证结果。
[79]在 S230 中，基于第一验证结果和第二验证结果，确定验证结果。当第一验证结果和第二验证结果都为验证通过时，可确定验证结果为验证通过，当第一验证结果和/或第二验证结果为验证不通过时，可确定验证结果为验证不通过。
[80]在 S230 之后，在验证结果为验证通过的情况下，可如图 2A 所示，继续执行 S232~S236，以对控车指令进行处理，也可如图 2B 所示，继续执行 S238~S248，以对控车指令进行处理。
[81]在 S232 中，在验证结果为验证通过的情况下，基于用户的第四私钥，对控车指令进行签名处理，得到第二可验证信息。第四私钥可为终端设备基于预设密钥生成算法，生成的与第四公钥对应的私钥。在验证结果为验证通过的情况下，终端设备可获取用户的第四私钥，并基于第四私钥，通过预设签名生成算法，对控车指令进行加密处理，得到第二可验证信息。

[82]在 S234 中，接收车载设备的第三公钥。第三公钥可为车载设备基于预设密钥生成算法，生成的与车载设备对应的密钥。

[83] 在 S236 中，基于车载设备的第三公钥，对控车指令和第二可验证信息进行加密处理，得到加密处理后的控车指令，并将加密处理后的控车指令发送至车载设备，以使车载设备基于第四公钥和第三私钥，对控车指令进行处理，第三私钥为车载设备生成的与第三公钥对应的私钥。由于加密处理后的控车指令是终端设备对控车指令和第二可验证信息进行加密处理得到的，且第二可验证信息是终端设备基于用户的第四私钥对控车指令进行加密得到的验证信息，所以，可保证控车指令在终端设备与车载设备之间的传输安全性。

[84] 在 S238 中，在验证结果为验证通过的情况下，生成针对控车指令的第三可验证信息、与第三可验证信息对应的第一时间戳以及控车指令的有效时间。第三可验证信息可为终端设备基于预设随机数生成算法，生成的与控车指令对应的预设位数的随机数。

[85] 在 S240 中，基于用户的第四私钥，对第三可验证信息、第一时间戳以及有效时间进行签名处理，得到第四可验证信息。

[86] 在 S242 中，接收车载设备的第三公钥。第三公钥可为车载设备基于预设密钥生成算法，生成的与车载设备对应的密钥。

[87] 在 S244 中，基于车载设备的第三公钥，对第三可验证信息、第一时间戳、有效时间以及第四可验证信息进行加密处理，得到目标信息，并将目标信息发送给车载设备。车载设备可对目标信息进行验证，并在验证通过的情况下存储目标信息。

[88] 在 S246 中，基于第三可验证信息，对控车指令进行加密处理，得到第一加密指令。

[89] 在 S248 中，将第一加密指令和与控车指令对应的第二时间戳发送给车载设备，以使车载设备基于第一加密指令、第二时间戳以及存储的目标信息，对第一加密指令进行处理。车载设备可基于存储的第三可验证信息，对终端设备发送的第一加密指令进行解密处理，得到对应的控车指令，并基于目标信息中的第一时间戳和有效时间，对第二时间戳进行验证，在验证通过的情况下，车载设备可执行解密得到的控车指令。

[90] 本说明书实施例提供一种基于隐私保护的验证方法，将针对控制车载设备的本地的身份验证请求发送给第一服务器，第一服务器用于针对身份验证请求，生成与终端设备、车载设备对应的目标验证信息，接收第一服务器发送的目标验证信息和预先构建的证书链，基于终端设备的预设密钥，对证书链和目标验证信息进行验证，得到验证结果，证书链为由第一服务器信息、第一服务器的预设密钥、终端设备的设备信息、终端设备的预设密钥、车载设备的设备信息和车载设备的预设密钥生成的多级证书链，在验证结果为验证通过的情况下，基于目标验证信息对控车指令进行处理，并将处理后的控车指令发送给车载设备，以使车载设备基于目标验证信息和证书链，对控车指令进行处理。这样，由于目标验证信息是第一服务器生成的与终端设备和车载设备对应的验证信息，且证书链也是由第一服务器、终端设备和车载设备的相关信息构成的证书链，所以，终端设备和车载设备可分别通过目标验证信息和证书链，对本地以及另一方（即车载设备）进行身份验证，在验证结果为通过的情况下，在通过目标验证信息对控车指令进行处理，可提高控车指令在传输过程中的安全性。

实施例三

[91] 如图 3A 和图 3B 所示，本说明书实施例提供一种基于隐私保护的验证方法，该方法的执行主体可为车载设备，该车载设备可是待控制车辆中安装的，能够基于预设信息传输方式与终端设备通信的设备，且车载设备还可执行终端设备发送的控车指令（即基于终端设备发送的控车指令控制车辆）。该方法具体可包括以下步骤：在 S302 中，接收第一服务器发送的与终端设备、车载设备对应的目标验证信息和预先构建的证书链。

[92] 证书链可为由第一服务器信息、第一服务器的预设密钥、终端设备的设备信息、终端设备的预设密钥、车载设备的设备信息和车载设备的预设密钥生成的多级证书链。

[93] 在 S304 中，基于车载设备的预设密钥，对证书链和目标验证信息进行验证，得到验证结果。

[94] 以证书链包含由终端设备的设备信息、终端设备的预设密钥等信息构成的根证书、由第一服务器信息、第一服务器的预设密钥等信息构成的中间证书，以及由车载设备的设备信息和车载设备的预设密钥构成的第三证书为例，根证书的所有者（即终端设备）可用自己的私钥对中间证书进行签名，中间证书的所有者（即第一服务器）可用自己的

私钥对第三证书进行签名。
[95] 车载设备可通过本地的预设密钥，对上述三级证书链进行逐一验证，即通过本地的私钥，对第三证书包含的签名信息进行验证，在验证通过后，再由第三证书中包含的中间证书所有者的公钥，对中间证书的有效性进行验证，再由中间证书包含的根证书所有者的公钥，对根证书的有效性进行验证，并得到验证结果。
[96] 上述验证结果的确定方法是一种可选地、可实现的确定方法，在实际应用场景中，还可有多种不同的确定方法，可根据实际应用场景的不同而有所不同，本说明书实施例对此不做具体限定。
[97] 在 S306 中，在验证结果为验证通过的情况下，基于目标验证信息，对终端设备发送的处理后的控车指令进行处理，得到控车指令，并执行控车指令。处理后的控车指令可为终端设备基于目标验证信息对控车指令进行处理得到的指令。以处理后的控车指令为终端设备基于目标验证信息对控车指令进行加密处理得到的指令为例，车载设备可基于存储的目标验证信息，对加密处理得到的控车指令进行解密处理，并执行解密处理得到的控车指令。
[98] 车载设备中也可安装有 TEE，用于保证上述数据处理过程中的数据安全性。
[99] 本说明书实施例提供一种基于隐私保护的验证方法，接收第一服务器发送的与终端设备、车载设备对应的目标验证信息和预先构建的证书链，证书链为由第一服务器信息、第一服务器的预设密钥、终端设备的设备信息、终端设备的预设密钥、车载设备的设备信息和车载设备的预设密钥生成的多级证书链，基于车载设备的预设密钥，对证书链和目标验证信息进行验证，得到验证结果，在验证结果为验证通过的情况下，基于目标验证信息，对终端设备发送的处理后的控车指令进行处理，得到控车指令，并执行控车指令，处理后的控车指令为终端设备基于目标验证信息对控车指令进行处理得到的指令。这样，由于目标验证信息是第一服务器生成的与终端设备和车载设备对应的验证信息，且证书链也是由第一服务器、终端设备和车载设备的相关信息构成的证书链，所以，终端设备和车载设备可分别通过目标验证信息和证书链，对本地以及另一方（即终端设备）进行身份验证，在验证结果为通过的情况下，在通过目标验证信息对控车指令进行处理，可提高控车指令在传输过程中的安全性。
实施例四
[100] 如图 4A 和图 4B 所示，本说明书实施例提供一种基于隐私保护的验证方法，该方法的执行主体可为车载设备，该车载设备可是待控制车辆中安装的，能够基于预设信息传输方式与终端设备通信的设备，且车载设备还可执行终端设备发送的控车指令（即基于终端设备发送的控车指令控制车辆）。该方法具体可包括以下步骤：在 S402 中，基于预设密钥生成算法，生成与车载设备对应的第三公钥。
[101] 在 S404 中，将第三公钥和车载设备的设备信息发送给第一服务器，以使第一服务器基于第三公钥、车载设备的设备信息、第一服务器信息、第一服务器的预设密钥、终端设备的设备信息以及终端设备的预设密钥生成证书链。
[102] 在 S406 中，接收第一服务器发送的与终端设备、车载设备对应的目标验证信息和预先构建的证书链。
[103] 在 S408 中，基于车载设备的第三公钥，对证书链进行验证处理，得到第三验证结果。上述 S408 的具体处理过程可参见上述实施例三中 S304 的相关内容，在此不再赘述。
[104] 在 S410 中，接收第一服务器发送的第一公钥和第一可验证信息。
[105] 第一可验证信息可为第一服务器基于第一服务器的第一私钥，对目标验证信息进行加密处理，得到与目标验证信息对应的信息，第一公钥和第一私钥可为第一服务器基于预设密钥生成算法，生成的与第一服务器对应的密钥。
[106] 在 S412 中，基于第一服务器的第一公钥和目标验证信息，对第一可验证信息进行验证，得到第四验证结果。车载设备可基于第一服务器的第一公钥，对第一可验证信息进行解密处理，并将解密处理得到的目标验证信息与接收到的目标验证信息进行匹配验证，以得到第四验证结果。
[107] 在 S414 中，基于第三验证结果和第四验证结果，确定验证结果。在第三验证结果和第四验证结果都为验证通过的情况下，可确定验证结果为验证通过，在第三验证结果和/或第四验证结果为验证不通过的情况下，可确定验证结果为验证不通过。在验证结果为验证通过的情况下，如图 4A 所示，在 S414 后可继续执行 S416~S420，或者可如图

4B 所示，在 S414 后继续执行 S422~S430，以对接收到的处理后的控车指令进行处理。

[108] 在 S416 中，在验证结果为验证通过的情况下，接收终端设备发送的第四公钥。第四公钥可为终端设备基于预设密钥生成算法，生成的与终端设备的用户对应的密钥。

[109] 在 S418 中，基于车载设备的第三私钥，对终端设备发送的处理后的控车指令进行处理，得到控车指令和第二可验证信息。处理后的控车指令可为终端设备基于车载设备的第三公钥对控车指令进行加密处理得到的，第三私钥可为车载设备基于预设密钥生成算法，生成的与第三公钥对应的私钥，第二可验证信息可为终端设备基于用户的第四私钥，对控车指令进行加密处理得到的信息，第四私钥为终端设备基于预设密钥生成算法，生成的与第四公钥对应的私钥。

[110] 在 S420 中，基于控车指令、用户的第四公钥，对第二可验证信息进行验证处理，并在验证通过的情况下，执行控车指令。可基于用户的第四公钥，对第二可验证信息进行解密处理，并将解密处理得到的控车指令与接收到的控车指令进行匹配验证，在验证通过的情况下，执行该控车指令。

[111] 在 S422 中，接收终端设备发送的目标信息。目标信息可为终端设备基于车载设备的第三公钥，对第三可验证信息、与第三可验证信息对应的第一时间戳、控车指令的有效时间以及第四可验证信息进行加密处理得到的信息，第三可验证信息可为终端设备基于预设随机数生成算法，生成的与控车指令对应的预设位数的随机数，第四可验证信息可为终端设备基于用户的第四私钥，对第三可验证信息、第一时间戳以及有效时间进行签名处理得到的信息。

[112] 在 S424 中，基于车载设备的第三私钥，对目标信息进行处理，得到第三可验证信息、第一时间戳、有效时间以及第四可验证信息。

[113] 在 S426 中，基于用户的第四公钥、第三可验证信息、第一时间戳以及有效时间，对第四可验证信息进行处理，在验证通过的情况下，存储第三可验证信息、第一时间戳和有效时间。车载设备可通过第四公钥，对第三可验证信息、第一时间戳以及有效时间进行签名处理，得到对应的签名信息，并将得到的签名信息与接收到的第四可验证信息进行匹配验证，在验证通过的情况下，存储第三可验证信息、第一时间戳和有效时间。

[114] 在 S428 中，基于存储的第三可验证信息，对终端设备发送的第一加密指令进行处理，得到控车指令。第一加密指令可为终端设备基于第三可验证信息，对控车指令进行加密处理得到的指令。

[115] 在 S430 中，基于存储的第一时间戳和有效时间，对第二时间戳进行验证处理，在验证通过的情况下，执行控车指令。例如，可判断第二时间戳是否大于第一时间戳，如果第二时间戳小于第一时间戳，则可认为接收到的控车指令在传输过程中存在被篡改的风险，所以，可向第一服务器或终端设备发送预设告警信息。如果第二时间戳不小于第一时间戳，且第二时间戳位于第一时间戳和有效时间确定的时间范围内，则可确定接收到的控车指令不存在被篡改的风险，可执行该控车指令。

[116] 此外，为保证对第二时间戳的验证有效性，车载设备中还可实时时钟（Real_Time Clock，RTC）。

[117] 本说明书实施例提供一种基于隐私保护的验证方法，接收第一服务器发送的与终端设备、车载设备对应的目标验证信息和预先构建的证书链，证书链为由第一服务器信息、第一服务器的预设密钥、终端设备的设备信息、终端设备的预设密钥、车载设备的设备信息和车载设备的预设密钥生成的多级证书链，基于车载设备的预设密钥，对证书链和目标验证信息进行验证，得到验证结果，在验证结果为验证通过的情况下，基于目标验证信息，对终端设备发送的处理后的控车指令进行处理，得到控车指令，并执行控车指令，处理后的控车指令为终端设备基于目标验证信息对控车指令进行处理得到的指令。这样，由于目标验证信息是第一服务器生成的与终端设备和车载设备对应的验证信息，且证书链也是由第一服务器、终端设备和车载设备的相关信息构成的证书链，所以，终端设备和车载设备可分别通过目标验证信息和证书链，对本地以及另一方（即终端设备）进行身份验证，在验证结果为通过的情况下，在通过目标验证信息对控车指令进行处理，可提高控车指令在传输过程中的安全性。

实施例五

[118] 如图 5A 和图 5B 所示，本说明书实施例提供一种基于隐私保护的验证方法，该方法的执行主体可为第一服务器，服务器可是独立的服务器，也可是由多个服务器组成的

服务器集群。该方法具体可包括以下步骤：在 S502 中，在接收到终端设备发送的针对控制车载设备的本地的身份验证请求的情况下，生成与终端设备、车载设备对应的目标验证信息。

[119] 在 S504 中，将目标验证信息和预先构建的证书链发送给终端设备和车载设备，以使终端设备基于终端设备的预设密钥，对证书链和目标验证信息进行验证通过后，基于目标验证信息，对控车指令进行处理，使车载设备基于车载设备的预设密钥，对证书链和目标验证信息进行验证通过后，基于目标验证信息，对终端设备发送的处理后的控车指令进行处理。

[120] 本说明书实施例提供一种基于隐私保护的验证方法，在接收到终端设备发送的针对控制车载设备的本地的身份验证请求的情况下，生成与终端设备、车载设备对应的目标验证信息，将目标验证信息和预先构建的证书链发送给终端设备和车载设备，以使终端设备基于终端设备的预设密钥，对证书链和目标验证信息进行验证通过后，基于目标验证信息，对控车指令进行处理，使车载设备基于车载设备的预设密钥，对证书链和目标验证信息进行验证通过后，基于目标验证信息，对终端设备发送的处理后的控车指令进行处理。这样，由于目标验证信息是第一服务器生成的与终端设备和车载设备对应的验证信息，且证书链也是由第一服务器、终端设备和车载设备的相关信息构成的证书链，所以，终端设备和车载设备可分别通过目标验证信息和证书链，对本地以及另一方（即车载设备或终端设备）进行身份验证，在验证结果为通过的情况下，在通过目标验证信息对控车指令进行处理，可提高控车指令在传输过程中的安全性。

实施例六

[121] 如图 6 所示，本说明书实施例提供一种基于隐私保护的验证方法，该方法的执行主体可为第一服务器，服务器可是独立的服务器，也可是由多个服务器组成的服务器集群。该方法具体可包括以下步骤：在 S602 中，基于预设密钥生成算法，生成与第一服务器对应的第一私钥和第一公钥。

[122] 在 S604 中，将第一公钥和服务器信息发送给终端设备。

[123] 在 S606 中，接收终端设备发送的由根证书和第二证书构成的第一证书链。根证书可为终端设备基于第二公钥、终端设备的设备信息和第一签名信息确定的，第一签名信息可为终端设备基于第二私钥，对终端设备的设备信息进行签名得到的，第二公钥和第二私钥可为终端设备基于预设密钥生成算法，生成的与终端设备对应的密钥，第二证书可为终端设备基于第一公钥、服务器信息和第二签名信息确定的，第二签名信息可为终端设备基于第二私钥，对服务器信息进行签名得到的。

[124] 在 S608 中，接收车载设备发送的第三公钥和车载设备的设备信息。第三公钥可为车载设备基于预设密钥生成算法，生成的与车载设备对应的密钥。

[125] 在 S610 中，基于第一私钥，对车载设备的设备信息进行签名，得到第三签名信息。

[126] 在 S612 中，将第三公钥、车载设备的设备信息和第三签名信息，确定为第三证书。

[127] 在 S614 中，存储由第三证书和第一证书链构成的证书链。

[128] 在 S616 中，在接收到终端设备发送的针对控制车载设备的本地的身份验证请求的情况下，生成与终端设备、车载设备对应的目标验证信息。

[129] 在 S618 中，基于第一服务器的第一私钥，对目标验证信息进行签名处理，得到与目标验证信息对应的第一可验证信息，并将目标验证信息、证书链和第一可验证信息分别发送给终端设备和车载设备，以使终端设备在对目标验证信息、证书链和第一可验证信息验证通过的情况下，基于目标验证信息，对控车指令进行处理，使车载设备基于车载设备的预设密钥，对第一可验证信息、证书链和目标验证信息进行验证通过后，基于目标验证信息，对终端设备发送的处理后的控车指令进行处理。

[130] 本说明书实施例提供一种基于隐私保护的验证方法，在接收到终端设备发送的针对控制车载设备的本地的身份验证请求的情况下，生成与终端设备、车载设备对应的目标验证信息，将目标验证信息和预先构建的证书链发送给终端设备和车载设备，以使终端设备基于终端设备的预设密钥，对证书链和目标验证信息进行验证通过后，基于目标验证信息，对控车指令进行处理，使车载设备基于车载设备的预设密钥，对证书链和目标验证信息进行验证通过后，基于目标验证信息，对终端设备发送的处理后的控车指令进行处理。这样，由于目标验证信息是第一服务器生成的与终端设备和车载设备对应的验证信息，且证书链也是由第一服务器、终端设备和车载设备的相关信息构成的证书链，

所以，终端设备和车载设备可分别通过目标验证信息和证书链，对本地以及另一方（即车载设备或终端设备）进行身份验证，在验证结果为通过的情况下，在通过目标验证信息对控车指令进行处理，可提高控车指令在传输过程中的安全性。

实施例七

[131] 本说明书实施例提供一种基于隐私保护的验证系统，该基于隐私保护的验证系统包括终端设备、车载设备和第一服务器，终端设备可用于将针对控制车载设备的本地的身份验证请求发送给第一服务器。

[132] 第一服务器，可用于生成与终端设备、车载设备对应的目标验证信息，并将目标验证信息和预先构建的证书链发送给终端设备和车载设备；证书链可为由第一服务器信息、第一服务器的预设密钥、终端设备的设备信息、终端设备的预设密钥、车载设备的设备信息和车载设备的预设密钥生成的多级证书链。

[133] 终端设备，可用于基于终端设备的预设密钥，对证书链和目标验证信息进行验证，得到第一验证结果；在第一验证结果为验证通过的情况下，基于目标验证信息对控车指令进行处理，并将处理后的控车指令发送给车载设备。

[134] 车载设备，可用于基于车载设备的预设密钥，对证书链和目标验证信息进行验证，得到第二验证结果；在第二验证结果为验证通过的情况下，基于目标验证信息对接收到的处理后的控车指令进行处理，得到控车指令，并执行控车指令。

[135] 本说明书实施例提供一种基于隐私保护的验证系统，由于目标验证信息是第一服务器生成的与终端设备和车载设备对应的验证信息，且证书链也是由第一服务器、终端设备和车载设备的相关信息构成的证书链，所以，终端设备和车载设备可分别通过目标验证信息和证书链，对本地以及另一方（即车载设备或终端设备）进行身份验证，在验证结果为通过的情况下，在通过目标验证信息对控车指令进行处理，可提高控车指令在传输过程中的安全性。

实施例八

[136] 本说明书实施例提供又一种基于隐私保护的验证系统，该基于隐私保护的验证系统包含了上述实施例七的基于隐私保护的验证系统的全部功能单元，并在其基础上，对其进行了改进，改进内容如下：如图 7 所示，以终端设备为移动终端设备、第一服务器为数字钥匙管理平台服务器为例。

[137] 在终端设备中可安装有用于控制车辆的应用程序（或搭载在应用程序中的可用于控制车辆的小程序），用户可通过终端设备运行该应用程序，以通过待控制车辆安装的车载设备控制该待控制车辆（如启动车辆、为车辆上锁、开启车内空调、音响等设备）。

[138] 车载设备在产线阶段，可在待控制车辆中预先配置有软件开发工具包（Software Development Kit，SDK）。

[139] 第一服务器可基于预设密钥生成算法，生成与第一服务器对应的第一私钥和第一公钥，并将第一公钥和服务器信息发送给终端设备。

[140] 终端设备可基于预设密钥生成算法，生成与终端设备对应的第二私钥和第二公钥，第二私钥和第二公钥可为根密钥。终端设备可基于第二私钥，对终端设备的设备信息进行签名，得到第一签名信息，在基于第二公钥、终端设备的设备信息和第一签名信息，生成根证书。终端设备在基于第二私钥，对服务器信息进行签名，得到第二签名信息。在基于第一公钥、服务器信息和第二签名信息，生成第二证书，最后将根证书和第二证书构成的第一证书链发送给第一服务器。

[141] 车载设备可获取生产待控制车辆的生产厂商信息、车载设备的产品型号、待控制车辆的车辆信息（如车辆型号、车辆品牌等）等产品信息，并将该产品信息发送给终端设备，终端设备可基于该该产品信息生成并存储车载设备的设备信息。同时，车载设备还可获取终端设备的设备 ID、SN、MAC 地址等标识信息，并由该标识信息生成终端设备的设备信息。车载设备还可根据预设标识信息生成规则，基于终端设备的设备 ID、SN、MAC 地址等标识信息，生成与终端设备对应的设备信息，并将该终端设备的设备信息发送给第一服务器，第一服务器可将终端设备的设备信息、SDK 以及终端设备的第二公钥，烧录到车载设备。

[142] 此外，第一服务器可基于车载设备发送的终端设备的设备信息，生成对应的令牌信息，并将该令牌信息发送给车载设备，车载设备可基于该令牌信息生成二维码，待控制车辆的生产厂商可将该二维码放置于该待控制车辆内。

[143] 在待控制车辆首次上电时，车载设备可基于预设密钥生成算法，生成与车载设备对应的第三公钥和第三私钥，车载设备可将第三公钥、车载设备的设备信息（如国际移动设备识别码（International Mobile Equipment Identity，IMEI）、MAC 地址等）发送给第一服务器。

[144] 第一服务器可基于第一私钥，对车载设备的设备信息进行签名，得到第三签名信息，在将第三公钥、车载设备的设备信息和第三签名信息，确定为所第三证书，并存储由第三证书和第一证书链构成的证书链。

[145] 终端设备在首次通过应用程序控制该待控制车辆时，可通过待控制车辆内的二维码，实现终端设备与该待控制车辆之间的绑定。例如，用户可通过终端设备扫描待控制车辆内的二维码，终端设备可对该二维码进行识别，并在获取到二维码中包含的终端设备的设备信息后，将针对用户的身份验证请求发送给第二服务器（第二服务器可是与终端设备的应用程序对应的服务器），并接收第二服务器基于身份验证请求生成的目标令牌，在基于目标令牌，对用户进行身份验证，并在身份验证结果为验证通过的情况下，基于预设密钥生成算法，生成与用户对应的第四公钥和第四私钥。

[146] 终端设备可将第四公钥和二维码中识别到的终端设备的设备信息发送给第一服务器，第一服务器可通过存储的终端设备的设备信息与接收到的种蒜设备的设备信息进行匹配验证，并在验证通过后，保存用户的第四公钥。

[147] 终端设备可基于用户的第四公钥、车载设备的第三公钥以及车载设备的设备信息，生成目标验证信息，并通过第一服务器的第一私钥，对目标验证信息进行加密处理，得到第一可验证信息，并将第一可验证信息以及证书链，分别发送给车载设备和终端设备。

[148] 终端设备可基于第一服务器的第一公钥、终端设备的第二公钥，对证书链中的根证书和第二证书进行验证处理，得到第一验证结果。基于第一服务器的第一公钥和目标验证信息，对第一可验证信息进行验证，得到第二验证结果。最后，基于第一验证结果和第二验证结果，确定验证结果。

[149] 在验证结果为验证通过的情况下，终端设备可存储目标验证信息，即终端设备可存储车载设备的设备信息以及车载设备的第三公钥。

[150] 同时，车载设备也可基于车载设备的第三公钥，对证书链进行验证处理，得到第三验证结果，在基于第一服务器的第一公钥和目标验证信息，对第一可验证信息进行验证，得到第四验证结果，最后，基于第三验证结果和第四验证结果，确定验证结果。并在验证结果为验证通过的情况下，存储用户的第四公钥。

[151] 终端设备可生成针对控车指令的第三可验证信息、与第三可验证信息对应的第一时间戳以及控车指令的有效时间，第三可验证信息可为终端设备基于预设随机数生成算法，生成的与控车指令对应的预设位数的随机数。

[152] 终端设备可基于用户的第四私钥，对第三可验证信息、第一时间戳以及有效时间进行签名处理，得到第四可验证信息。

[153] 终端设备在基于存储的车载设备的第三公钥，对第三可验证信息、第一时间戳、有效时间以及第四可验证信息进行加密处理，得到目标信息，并将目标信息发送给车载设备。

[154] 车载设备可基于本地的第三私钥，对目标信息进行处理，得到第三可验证信息、第一时间戳、有效时间以及第四可验证信息。

[155] 车载设备可基于用户的第四公钥、第三可验证信息、第一时间戳以及有效时间，对第四可验证信息进行处理，在验证通过的情况下，存储第三可验证信息、第一时间戳和有效时间。

[156] 终端设备可基于第三可验证信息，对控车指令进行加密处理，得到第一加密指令，并将第一加密指令和与控车指令对应的第二时间戳发送给车载设备。

[157] 车载设备可根据存储的第三可验证信息，对第一加密指令进行处理，得到控车指令，在基于存储的第一时间戳和有效时间，对第二时间戳进行验证处理，在验证通过的情况下，执行控车指令。此外，还可通过 HMAC 算法，对第一时间戳、第二时间戳进行加密，以提高数据传输过程中的安全性。

[158] 这样，由于第三可验证信息是基于预设随机数生成算法，生成的与控车指令对应的预设位数的随机数，所以，可通过第三可验证信息提高信息传输过重中的安全性。此外，终端设备还可通过第二服务器实现与第一服务器之间的数据传输，即第二服务器可

通过开放数据调用接口，将接收到的终端设备发送的信息，传输至第一服务器。
[159] 本说明书实施例提供一种基于隐私保护的验证系统，由于目标验证信息是第一服务器生成的与终端设备和车载设备对应的验证信息，且证书链也是由第一服务器、终端设备和车载设备的相关信息构成的证书链，所以，终端设备和车载设备可分别通过目标验证信息和证书链，对本地以及另一方（即车载设备或终端设备）进行身份验证，在验证结果为通过的情况下，在通过目标验证信息对控车指令进行处理，可提高控车指令在传输过程中的安全性。
实施例九
[160] 以上为本说明书实施例提供的基于隐私保护的验证方法，基于同样的思路，本说明书实施例还提供一种基于隐私保护的验证装置，如图 8 所示。该基于隐私保护的验证装置包括：请求发送模块 801、验证模块 802 和指令发送模块 803，其中：请求发送模块 801，用于将针对控制车载设备的本地的身份验证请求发送给第一服务器，所述第一服务器用于针对所述身份验证请求，生成与所述基于隐私保护的验证装置、所述车载设备对应的目标验证信息；验证模块 802，用于接收所述第一服务器发送的所述目标验证信息和预先构建的证书链，基于所述基于隐私保护的验证装置的预设密钥，对所述证书链和所述目标验证信息进行验证，得到验证结果，所述证书链为由所述第一服务器信息、所述第一服务器的预设密钥、所述基于隐私保护的验证装置的设备信息、所述基于隐私保护的验证装置的预设密钥、所述车载设备的设备信息和所述车载设备的预设密钥生成的多级证书链；指令发送模块 803，用于在所述验证结果为验证通过的情况下，基于所述目标验证信息对控车指令进行处理，并将处理后的控车指令发送给所述车载设备，以使所述车载设备基于所述目标验证信息和所述证书链，对所述控车指令进行处理。
[161] 本说明书实施例中，所述装置还包括：信息接收模块，用于接收所述第一服务器的服务器信息以及所述第一服务器的第一公钥，所述第一公钥为所述第一服务器基于预设密钥生成算法，生成的与所述第一服务器对应的密钥；第一生成模块，用于基于所述预设密钥生成算法，生成与所述基于隐私保护的验证装置对应的第二私钥和第二公钥；第一处理模块，用于基于所述第二私钥，对所述基于隐私保护的验证装置的设备信息进行签名，得到第一签名信息；第二生成模块，用于基于所述第二公钥、所述基于隐私保护的验证装置的设备信息和所述第一签名信息，生成根证书；第二处理模块，用于基于所述第二私钥，对所述服务器信息进行签名，得到第二签名信息；第三生成模块，用于基于所述第一公钥、所述服务器信息和所述第二签名信息，生成第二证书；证书发送模块，用于将所述根证书和所述第二证书构成的第一证书链发送给所述第一服务器，以使所述第一服务器基于所述第一证书链、所述车载设备的设备信息和所述车载设备的预设密钥，构建所述证书链。
[162] 本说明书实施例中，所述装置还包括：第四生成模块，用于基于所述预设密钥生成算法，生成与用户对应的第四公钥；信息发送模块，用于将所述第四公钥以及所述基于隐私保护的验证装置的设备信息发送给所述第一服务器，以使所述第一服务器基于所述基于隐私保护的验证装置的设备信息、所述第四公钥、所述车载设备的预设密钥以及所述车载设备的设备信息，生成所述目标验证信息。
[163] 本说明书实施例中，所述验证模块 802，用于：接收所述第一服务器发送的第一可验证信息，所述第一可验证信息为所述第一服务器基于所述第一服务器的第一私钥，对所述目标验证信息进行加密处理，得到的与所述目标验证信息对应的信息；基于所述第一服务器的第一公钥、所述基于隐私保护的验证装置的第二公钥，对所述证书链中的根证书和所述第二证书进行验证处理，得到第一验证结果；基于所述第一服务器的第一公钥和所述目标验证信息，对所述第一可验证信息进行验证，得到第二验证结果；基于所述第一验证结果和所述第二验证结果，确定所述验证结果。
[164] 本说明书实施例中，所述指令发送模块 803，用于：基于所述用户的第四私钥，对所述控车指令进行加密处理，得到第二可验证信息，所述第四私钥为所述基于隐私保护的验证装置基于所述预设密钥生成算法，生成的与所述第四公钥对应的私钥；接收所述车载设备的第三公钥，所述第三公钥为所述车载设备基于所述预设密钥生成算法，生成的与所述车载设备对应的密钥；基于所述车载设备的第三公钥，对所述控车指令和所述第二可验证信息进行加密处理，得到加密处理后的控车指令，并将所述加密处理后的控车指令发送至所述车载设备，以使所述车载设备基于所述第四公钥和第三私钥，对所述

控车指令进行处理，所述第三私钥为所述车载设备生成的与所述第三公钥对应的私钥。

[165] 本说明书实施例中，所述指令发送模块 803，用于：生成针对所述控车指令的第三可验证信息、与所述第三可验证信息对应的第一时间戳以及所述控车指令的有效时间，所述第三可验证信息为所述基于隐私保护的验证装置基于预设随机数生成算法，生成的与所述控车指令对应的预设位数的随机数；基于所述用户的第四私钥，对所述第三可验证信息、所述第一时间戳以及所述有效时间进行签名处理，得到第四可验证信息；接收所述车载设备的第三公钥，所述第三公钥为所述车载设备基于所述预设密钥生成算法，生成的与所述车载设备对应的密钥；基于所述车载设备的第三公钥，对所述第三可验证信息、所述第一时间戳、所述有效时间以及所述第四可验证信息进行加密处理，得到目标信息，并将所述目标信息发送给所述车载设备；基于所述第三可验证信息，对所述控车指令进行加密处理，得到第一加密指令；将所述第一加密指令和与所述控车指令对应的第二时间戳发送给所述车载设备，以使所述车载设备基于所述第一加密指令、所述第二时间戳以及存储的所述目标信息，对所述第一加密指令进行处理。

[166] 本说明书实施例中，所述指令发送模块 803，用于：将针对所述用户的身份验证请求发送给第二服务器；接收所述第二服务器基于所述身份验证请求生成的目标令牌；基于所述目标令牌，对所述用户进行身份验证，并在身份验证结果为验证通过的情况下，基于所述预设密钥生成算法，生成与所述用户对应的所述第四公钥。

[167] 本说明书实施例提供一种基于隐私保护的验证装置，将针对控制车载设备的本地的身份验证请求发送给第一服务器，第一服务器用于针对身份验证请求，生成与终端设备、车载设备对应的目标验证信息，接收第一服务器发送的目标验证信息和预先构建的证书链，基于终端设备的预设密钥，对证书链和目标验证信息进行验证，得到验证结果，证书链为由第一服务器信息、第一服务器的预设密钥、终端设备的设备信息、终端设备的预设密钥、车载设备的设备信息和车载设备的预设密钥生成的多级证书链，在验证结果为验证通过的情况下，基于目标验证信息对控车指令进行处理，并将处理后的控车指令发送给车载设备，以使车载设备基于目标验证信息和所述证书链，对控车指令进行处理。这样，由于目标验证信息是第一服务器生成的与终端设备和车载设备对应的验证信息，且证书链也是由第一服务器、终端设备和车载设备的相关信息构成的证书链，所以，终端设备和车载设备可分别通过目标验证信息和证书链，对本地以及另一方（即车载设备）进行身份验证，在验证结果为通过的情况下，在通过目标验证信息对控车指令进行处理，可提高控车指令在传输过程中的安全性。

实施例十

[168] 基于同样的思路，本说明书实施例还提供一种基于隐私保护的验证装置，如图 9 所示。该基于隐私保护的验证装置包括：信息接收模块 901、验证模块 902 和指令处理模块 903，其中：信息接收模块，用于接收第一服务器发送的与终端设备、所述基于隐私保护的验证装置对应的目标验证信息和预先构建的证书链，所述证书链为由所述第一服务器信息、所述第一服务器的预设密钥、所述终端设备的设备信息、所述终端设备的预设密钥、所述基于隐私保护的验证装置的设备信息和所述基于隐私保护的验证装置的预设密钥生成的多级证书链；验证模块，用于基于所述基于隐私保护的验证装置的预设密钥，对所述证书链和所述目标验证信息进行验证，得到验证结果；指令处理模块，用于在所述验证结果为验证通过的情况下，基于所述目标验证信息，对所述终端设备发送的处理后的控车指令进行处理，得到控车指令，并执行所述控车指令，所述处理后的控车指令为所述终端设备基于所述目标验证信息对所述控车指令进行处理得到的指令。

[169] 本说明书实施例中，所述装置还包括：生成模块，用于基于预设密钥生成算法，生成与所述基于隐私保护的验证装置对应的第三公钥；信息发送模块，用于将所述第三公钥和所述基于隐私保护的验证装置的设备信息发送给所述第一服务器，以使所述第一服务器基于所述第三公钥、所述基于隐私保护的验证装置的设备信息、所述第一服务器信息、所述第一服务器的预设密钥、所述终端设备的设备信息以及所述终端设备的预设密钥生成所述证书链。

[170] 本说明书实施例中，所述指令处理模块 903，用于：接收所述终端设备发送的第四公钥，所述第四公钥为所述终端设备基于预设密钥生成算法，生成的与所述终端设备的用户对应的密钥；基于所述基于隐私保护的验证装置的第三私钥，对所述终端设备发送的处理后的控车指令进行处理，得到所述控车指令和第二可验证信息，所述处理后的控

车指令为所述终端设备基于所述基于隐私保护的验证装置的第三公钥对所述控车指令进行加密处理得到的，所述第三私钥为所述基于隐私保护的验证装置基于预设密钥生成算法，生成的与所述第三公钥对应的私钥，所述第二可验证信息为所述终端设备基于所述用户的第四私钥，对所述控车指令进行加密处理得到的信息，所述第四私钥为所述终端设备基于所述预设密钥生成算法，生成的与所述第四公钥对应的私钥；基于所述控车指令、所述用户的第四公钥，对所述第二可验证信息进行验证处理，并在验证通过的情况下，执行所述控车指令。

[171] 本说明书实施例中，所述指令处理模块 903，用于：接收所述终端设备发送的第四公钥，所述第四公钥为所述终端设备基于预设密钥生成算法，生成的与所述终端设备的用户对应的密钥；接收所述终端设备发送的目标信息，所述目标信息为所述终端设备基于所述基于隐私保护的验证装置的第三公钥，对第三可验证信息、与所述第三可验证信息对应的第一时间戳、所述控车指令的有效时间以及第四可验证信息进行加密处理得到的信息，所述第三可验证信息为所述终端设备基于预设随机数生成算法，生成的与所述控车指令对应的预设位数的随机数，所述第四可验证信息为所述终端设备基于所述用户的第四私钥，对所述第三可验证信息、所述第一时间戳以及所述有效时间进行签名处理得到的信息；基于所述基于隐私保护的验证装置的第三私钥，对所述目标信息进行处理，得到所述第三可验证信息、所述第一时间戳、所述有效时间以及所述第四可验证信息；基于所述用户的第四公钥、所述第三可验证信息、所述第一时间戳以及所述有效时间，对所述第四可验证信息进行处理，在验证通过的情况下，存储所述第三可验证信息、所述第一时间戳和所述有效时间；基于存储的所述第三可验证信息，对所述终端设备发送的第一加密指令进行处理，得到所述控车指令，所述第一加密指令为所述终端设备基于所述第三可验证信息，对所述控车指令进行加密处理得到的指令；基于存储的所述第一时间戳和所述有效时间，对所述第二时间戳进行验证处理，在验证通过的情况下，执行所述控车指令。

[172] 本说明书实施例提供一种基于隐私保护的验证装置，接收第一服务器发送的与终端设备、车载设备对应的目标验证信息和预先构建的证书链，证书链为由第一服务器信息、第一服务器的预设密钥、终端设备的设备信息、终端设备的预设密钥、车载设备的设备信息和车载设备的预设密钥生成的多级证书链，基于车载设备的预设密钥，对证书链和目标验证信息进行验证，得到验证结果，在验证结果为验证通过的情况下，基于目标验证信息，对终端设备发送的处理后的控车指令进行处理，得到控车指令，并执行控车指令，处理后的控车指令为终端设备基于目标验证信息对控车指令进行处理得到的指令。这样，由于目标验证信息是第一服务器生成的与终端设备和车载设备对应的验证信息，且证书链也是由第一服务器、终端设备和车载设备的相关信息构成的证书链，所以，终端设备和车载设备可分别通过目标验证信息和证书链，对本地以及另一方（即终端设备）进行身份验证，在验证结果为通过的情况下，在通过目标验证信息对控车指令进行处理，可提高控车指令在传输过程中的安全性。

实施例十一

[173] 基于同样的思路，本说明书实施例还提供一种基于隐私保护的验证装置，如图 10 所示。该基于隐私保护的验证装置包括：信息生成模块 1001 和信息发送模块 1002，其中：信息生成模块 1001，用于在接收到终端设备发送的针对控制车载设备的本地的身份验证请求的情况下，生成与所述终端设备、所述车载设备对应的目标验证信息；信息发送模块 1002，用于将所述目标验证信息和预先构建的证书链发送给所述终端设备和所述车载设备，以使所述终端设备基于所述终端设备的预设密钥，对所述证书链和所述目标验证信息进行验证通过后，基于所述目标验证信息，对控车指令进行处理，使所述车载设备基于所述车载设备的预设密钥，对所述证书链和所述目标验证信息进行验证通过后，基于所述目标验证信息，对所述终端设备发送的所述处理后的控车指令进行处理，所述证书链为由所述基于隐私保护的验证装置信息、所述基于隐私保护的验证装置的预设密钥、所述终端设备的设备信息、所述终端设备的预设密钥、所述车载设备的设备信息和所述车载设备的预设密钥生成的多级证书链。

[174] 本说明书实施例中，所述装置还包括：第一生成模块，用于基于预设密钥生成算法，生成与所述基于隐私保护的验证装置对应的第一私钥和第一公钥；数据发送模块，用于将所述第一公钥和所述服务器信息发送给所述终端设备；证书接收模块，用于接收

所述终端设备发送的由根证书和第二证书构成的第一证书链，所述根证书为所述终端设备基于第二公钥、所述终端设备的设备信息和第一签名信息确定的，所述第一签名信息为所述终端设备基于第二私钥，对所述终端设备的设备信息进行签名得到的，所述第二公钥和第二私钥为所述终端设备基于所述预设密钥生成算法，生成的与所述终端设备对应的密钥，所述第二证书为所述终端设备基于所述第一公钥、所述服务器信息和第二签名信息确定的，所述第二签名信息为所述终端设备基于所述第二私钥，对所述服务器信息进行签名得到的；信息接收模块，用于接收所述车载设备发送的第三公钥和所述车载设备的设备信息，所述第三公钥为所述车载设备基于所述预设密钥生成算法，生成的与所述车载设备对应的密钥；第二生成模块，用于基于所述第一私钥，对所述车载设备的设备信息进行签名，得到第三签名信息；第三生成模块，用于将所述第三公钥、所述车载设备的设备信息和所述第三签名信息，确定为所述第三证书；存储模块，用于存储由所述第三证书和所述第一证书链构成的所述证书链。

[175] 本说明书实施例中，所述信息发送模块 1002，用于：基于所述基于隐私保护的验证装置的第一私钥，对所述目标验证信息进行签名处理，得到与所述目标验证信息对应的第一可验证信息，并将所述目标验证信息、所述证书链和所述第一可验证信息分别发送给所述终端设备和所述车载设备，以使所述终端设备在对所述目标验证信息、所述证书链和所述第一可验证信息验证通过的情况下，基于所述目标验证信息，对所述控车指令进行处理，使所述车载设备基于所述车载设备的预设密钥，对所述第一可验证信息、所述证书链和所述目标验证信息进行验证通过后，基于所述目标验证信息，对所述终端设备发送的所述处理后的控车指令进行处理。

[176] 本说明书实施例提供一种基于隐私保护的验证装置，在接收到终端设备发送的针对控制车载设备的本地的身份验证请求的情况下，生成与终端设备、车载设备对应的目标验证信息，将目标验证信息和预先构建的证书链发送给终端设备和车载设备，以使终端设备基于终端设备的预设密钥，对证书链和目标验证信息进行验证通过后，基于目标验证信息，对控车指令进行处理，使车载设备基于车载设备的预设密钥，对证书链和目标验证信息进行验证通过后，基于目标验证信息，对终端设备发送的处理后的控车指令进行处理。这样，由于目标验证信息是第一服务器生成的与终端设备和车载设备对应的验证信息，且证书链也是由第一服务器、终端设备和车载设备的相关信息构成的证书链，所以，终端设备和车载设备可分别通过目标验证信息和证书链，对本地以及另一方（即车载设备或终端设备）进行身份验证，在验证结果为通过的情况下，在通过目标验证信息对控车指令进行处理，可提高控车指令在传输过程中的安全性。

实施例十二

[177] 基于同样的思路，本说明书实施例还提供一种基于隐私保护的验证设备，如图 11 所示。所述基于隐私保护的验证设备可为上述实施例提供的区块链节点设备。基于隐私保护的验证设备可因配置或性能不同而产生比较大的差异，可包括一个或一个以上的处理器 1101 和存储器 1102，存储器 1102 中可存储有一个或一个以上存储应用程序或数据。存储器 1102 可是短暂存储或持久存储。存储在存储器 1102 的应用程序可包括一个或一个以上模块（图示未示出），每个模块可包括对基于隐私保护的验证设备中的一系列计算机可执行指令。更进一步地，处理器 1101 可设置为与存储器 1102 通信，在基于隐私保护的验证设备上执行存储器 1102 中的一系列计算机可执行指令。基于隐私保护的验证设备还可包括一个或一个以上电源 1103，一个或一个以上有线或无线网络接口 1104，一个或一个以上输入输出接口 1105，一个或一个以上键盘 1106。

[178] 具体在本实施例中，基于隐私保护的验证设备包括有存储器，以及一个或一个以上的程序，其中一个或者一个以上程序存储于存储器中，且一个或者一个以上程序可包括一个或一个以上模块，且每个模块可包括对基于隐私保护的验证设备中的一系列计算机可执行指令，且经配置以由一个或者一个以上处理器执行该一个或者一个以上程序包含用于进行以下计算机可执行指令：将针对控制车载设备的本地的身份验证请求发送给第一服务器，所述第一服务器用于针对所述身份验证请求，生成与所述基于隐私保护的验证设备、所述车载设备对应的目标验证信息；接收所述第一服务器发送的所述目标验证信息和预先构建的证书链，基于所述基于隐私保护的验证设备的预设密钥，对所述证书链和所述目标验证信息进行验证，得到验证结果，所述证书链为由所述第一服务器信息、所述第一服务器的预设密钥、所述基于隐私保护的验证设备的设备信息、所述基于

隐私保护的验证设备的预设密钥、所述车载设备的设备信息和所述车载设备的预设密钥生成的多级证书链；在所述验证结果为验证通过的情况下，基于所述目标验证信息对控车指令进行处理，并将处理后的控车指令发送给所述车载设备，以使所述车载设备基于所述目标验证信息和所述证书链，对所述控车指令进行处理。

[179] 可选地，在所述接收所述第一服务器发送的所述目标验证信息和预先构建的证书链之前，所述方法还包括：接收所述第一服务器的服务器信息以及所述第一服务器的第一公钥，所述第一公钥为所述第一服务器基于预设密钥生成算法，生成的与所述第一服务器对应的密钥；基于所述预设密钥生成算法，生成与所述基于隐私保护的验证设备对应的第二私钥和第二公钥；基于所述第二私钥，对所述基于隐私保护的验证设备的设备信息进行签名，得到第一签名信息；基于所述第二公钥、所述基于隐私保护的验证设备的设备信息和所述第一签名信息，生成根证书；基于所述第二私钥，对所述服务器信息进行签名，得到第二签名信息；基于所述第一公钥、所述服务器信息和所述第二签名信息，生成第二证书；将所述根证书和所述第二证书构成的第一证书链发送给所述第一服务器，以使所述第一服务器基于所述第一证书链、所述车载设备的设备信息和所述车载设备的预设密钥，构建所述证书链。

[180] 可选地，在所述接收所述第一服务器发送的所述目标验证信息和预先构建的证书链之前，还包括：基于所述预设密钥生成算法，生成与用户对应的第四公钥；将所述第四公钥以及所述基于隐私保护的验证设备的设备信息发送给所述第一服务器，以使所述第一服务器基于所述基于隐私保护的验证设备的设备信息、所述第四公钥、所述车载设备的预设密钥以及所述车载设备的设备信息，生成所述目标验证信息。

[181] 可选地，所述基于所述基于隐私保护的验证设备的预设密钥，对所述证书链和所述目标验证信息进行验证，得到验证结果，包括：接收所述第一服务器发送的第一可验证信息，所述第一可验证信息为所述第一服务器基于所述第一服务器的第一私钥，对所述目标验证信息进行加密处理，得到的与所述目标验证信息对应的信息；基于所述第一服务器的第一公钥、所述基于隐私保护的验证设备的第二公钥，对所述证书链中的根证书和所述第二证书进行验证处理，得到第一验证结果；基于所述第一服务器的第一公钥和所述目标验证信息，对所述第一可验证信息进行验证，得到第二验证结果；基于所述第一验证结果和所述第二验证结果，确定所述验证结果。

[182] 可选地，所述基于所述目标验证信息对控车指令进行处理，并将处理后的控车指令发送给所述车载设备，包括：基于所述用户的第四私钥，对所述控车指令进行加密处理，得到第二可验证信息，所述第四私钥为所述基于隐私保护的验证设备基于所述预设密钥生成算法，生成的与所述第四公钥对应的私钥；接收所述车载设备的第三公钥，所述第三公钥为所述车载设备基于所述预设密钥生成算法，生成的与所述车载设备对应的密钥；基于所述车载设备的第三公钥，对所述控车指令和所述第二可验证信息进行加密处理，得到加密处理后的控车指令，并将所述加密处理后的控车指令发送至所述车载设备，以使所述车载设备基于所述第四公钥和第三私钥，对所述控车指令进行处理，所述第三私钥为所述车载设备生成的与所述第三公钥对应的私钥。

[183] 可选地，基于所述目标验证信息对控车指令进行处理，并将处理后的控车指令发送给所述车载设备，包括：生成针对所述控车指令的第三可验证信息、与所述第三可验证信息对应的第一时间戳以及所述控车指令的有效时间，所述第三可验证信息为所述基于隐私保护的验证设备基于预设随机数生成算法，生成的与所述控车指令对应的预设位数的随机数；基于所述用户的第四私钥，对所述第三可验证信息、所述第一时间戳以及所述有效时间进行签名处理，得到第四可验证信息；接收所述车载设备的第三公钥，所述第三公钥为所述车载设备基于所述预设密钥生成算法，生成的与所述车载设备对应的密钥；基于所述车载设备的第三公钥，对所述第三可验证信息、所述第一时间戳、所述有效时间以及所述第四可验证信息进行加密处理，得到目标信息，并将所述目标信息发送给所述车载设备；基于所述第三可验证信息，对所述控车指令进行加密处理，得到第一加密指令；将所述第一加密指令和与所述控车指令对应的第二时间戳发送给所述车载设备，以使所述车载设备基于所述第一加密指令、所述第二时间戳以及存储的所述目标信息，对所述第一加密指令进行处理。

[184] 可选地，基于所述预设密钥生成算法，生成与用户对应的第四公钥，包括：将针对所述用户的身份验证请求发送给第二服务器；接收所述第二服务器基于所述身份验证

请求生成的目标令牌；基于所述目标令牌对所述用户进行身份验证，并在身份验证结果为验证通过的情况下，基于所述预设密钥生成算法生成与所述用户对应的所述第四公钥。
[185] 另外，基于隐私保护的验证设备包括有存储器，以及一个或一个以上的程序，其中一个或者一个以上程序存储于存储器中，且一个或者一个以上程序可包括一个或一个以上模块，且每个模块可包括对基于隐私保护的验证设备中的一系列计算机可执行指令，且经配置以由一个或者一个以上处理器执行该一个或者一个以上程序包含用于进行以下计算机可执行指令：接收第一服务器发送的与终端设备、所述基于隐私保护的验证设备对应的目标验证信息和预先构建的证书链，所述证书链为由所述第一服务器信息、所述第一服务器的预设密钥、所述终端设备的设备信息、所述终端设备的预设密钥、所述基于隐私保护的验证设备的设备信息和所述基于隐私保护的验证设备的预设密钥生成的多级证书链；基于所述基于隐私保护的验证设备的预设密钥，对所述证书链和所述目标验证信息进行验证；在验证通过后，基于所述目标验证信息，对所述终端设备发送的处理后的控车指令进行处理，得到控车指令，并执行所述控车指令，所述处理后的控车指令为所述终端设备基于所述目标验证信息对所述控车指令进行处理得到的指令。
[186] 可选地，在所述基于所述基于隐私保护的验证设备的预设密钥，对所述证书链和所述目标验证信息进行验证之前，还包括：基于预设密钥生成算法，生成与所述基于隐私保护的验证设备对应的第三公钥；将所述第三公钥和所述基于隐私保护的验证设备的设备信息发送给所述第一服务器，以使所述第一服务器基于所述第三公钥、所述基于隐私保护的验证设备的设备信息、所述第一服务器信息、所述第一服务器的预设密钥、所述终端设备的设备信息以及所述终端设备的预设密钥生成所述证书链。
[187] 可选地，所述基于所述基于隐私保护的验证设备的预设密钥，对所述证书链和所述目标验证信息进行验证，得到验证结果，包括：基于所述基于隐私保护的验证设备的第三公钥，对所述证书链进行验证处理，得到第三验证结果；接收所述第一服务器发送的第一公钥和第一可验证信息，所述第一可验证信息为所述第一服务器基于所述第一服务器的第一私钥，对所述目标验证信息进行签名处理，得到与所述目标验证信息对应的信息，所述第一公钥和第一私钥为所述第一服务器基于预设密钥生成算法，生成的与所述第一服务器对应的密钥；基于所述第一服务器的第一公钥和所述目标验证信息，对所述第一可验证信息进行验证，得到第四验证结果；基于所述第三验证结果和所述第四验证结果，确定所述验证结果。
[188] 可选地，基于所述目标验证信息，对所述终端设备发送的处理后的控车指令进行处理，得到控车指令，并执行所述控车指令，包括：接收所述终端设备发送的第四公钥，所述第四公钥为所述终端设备基于预设密钥生成算法，生成的与所述终端设备的用户对应的密钥；基于所述基于隐私保护的验证设备的第三私钥，对所述处理后的控车指令进行处理，得到所述控车指令和第二可验证信息，所述处理后的控车指令为所述终端设备基于所述基于隐私保护的验证设备的第三公钥对所述控车指令进行加密处理得到的，所述第三私钥为所述基于隐私保护的验证设备基于预设密钥生成算法，生成的与所述第三公钥对应的私钥，所述第二可验证信息为所述终端设备基于所述用户的第四私钥，对所述控车指令进行加密处理得到的信息，所述第四私钥为所述终端设备基于所述预设密钥生成算法，生成的与所述第四公钥对应的私钥；基于所述控车指令、所述用户的第四公钥，对所述第二可验证信息进行验证处理，并在验证通过的情况下，执行所述控车指令。
[189] 可选地，所述基于所述目标验证信息，对所述终端设备发送的处理后的控车指令进行处理，得到控车指令，并执行所述控车指令，包括：接收所述终端设备发送的第四公钥，所述第四公钥为所述终端设备基于预设密钥生成算法，生成的与所述终端设备的用户对应的密钥；接收所述终端设备发送的目标信息，所述目标信息为所述终端设备基于所述基于隐私保护的验证设备的第三公钥，对第三可验证信息、与所述第三可验证信息对应的第一时间戳、所述控车指令的有效时间以及第四可验证信息进行加密处理得到的信息，所述第三可验证信息为所述终端设备基于预设随机数生成算法，生成的与所述控车指令对应的预设位数的随机数，所述第四可验证信息为所述终端设备基于所述用户的第四私钥，对所述第三可验证信息、所述第一时间戳以及所述有效时间进行签名处理得到的信息；基于所述基于隐私保护的验证设备的第三私钥，对所述终端设备发送的目标信息进行处理，得到所述第三可验证信息、所述第一时间戳、所述有效时间以及所述第四可验证信息；基于所述用户的第四公钥、所述第三可验证信息、所述第一时间戳以

及所述有效时间，对所述第四可验证信息进行处理，在验证通过的情况下，存储所述第三可验证信息、所述第一时间戳和所述有效时间；基于存储的所述第三可验证信息，对所述终端设备发送的第一加密指令进行处理，得到所述控车指令，所述第一加密指令为所述终端设备基于所述第三可验证信息，对所述控车指令进行加密处理得到的指令；基于存储的所述第一时间戳和所述有效时间，对所述第二时间戳进行验证处理，在验证通过的情况下，执行所述控车指令。

[190] 另外，基于隐私保护的验证设备包括有存储器及一个或一个以上的程序，其中一个或者一个以上程序存储于存储器中，且一个或者一个以上程序可包括一个或一个以上模块，且每个模块可包括对基于隐私保护的验证设备中的一系列计算机可执行指令，且经配置以由一个或者一个以上处理器执行该一个或者一个以上程序包含用于进行以下计算机可执行指令：在接收到终端设备发送的针对控制车载设备的本地的身份验证请求的情况下，生成与所述终端设备、所述车载设备对应的目标验证信息；将所述目标验证信息和预先构建的证书链发送给所述终端设备和所述车载设备，以使所述终端设备基于所述终端设备的预设密钥，对所述证书链和所述目标验证信息进行验证通过后，基于所述目标验证信息，对控车指令进行处理，使所述车载设备基于所述车载设备的预设密钥，对所述证书链和所述目标验证信息进行验证通过后，基于所述目标验证信息，对所述终端设备发送的所述处理后的控车指令进行处理，所述证书链为由所述基于隐私保护的验证设备信息、所述基于隐私保护的验证设备的预设密钥、所述终端设备的设备信息、所述终端设备的预设密钥、所述车载设备的设备信息和所述车载设备的预设密钥生成的多级证书链。

[191] 可选地，在所述将所述目标验证信息和预先构建的证书链发送给所述终端设备和所述车载设备之前，还包括：基于预设密钥生成算法，生成与所述基于隐私保护的验证设备对应的第一私钥和第一公钥；将所述第一公钥和所述服务器信息发送给所述终端设备；接收所述终端设备发送的由根证书和第二证书构成的第一证书链，所述根证书为所述终端设备基于第二公钥、所述终端设备的设备信息和第一签名信息确定的，所述第一签名信息为所述终端设备基于第二私钥，对所述终端设备的设备信息进行签名得到的，所述第二公钥和第二私钥为所述终端设备基于所述预设密钥生成算法，生成的与所述终端设备对应的密钥，所述第二证书为所述终端设备基于所述第一公钥、所述服务器信息和第二签名信息确定的，所述第二签名信息为所述终端设备基于所述第二私钥，对所述服务器信息进行签名得到的；接收所述车载设备发送的第三公钥和所述车载设备的设备信息，所述第三公钥为所述车载设备基于所述预设密钥生成算法，生成的与所述车载设备对应的密钥；基于所述第一私钥，对所述车载设备的设备信息进行签名，得到第三签名信息；将所述第三公钥、所述车载设备的设备信息和所述第三签名信息，确定为所述第三证书；存储由所述第三证书和所述第一证书链构成的所述证书链。

[192] 可选地，将所述目标验证信息和预先构建的证书链发送给所述终端设备和所述车载设备，包括：基于所述基于隐私保护的验证设备的第一私钥，对所述目标验证信息进行签名处理，得到与所述目标验证信息对应的第一可验证信息，并将所述目标验证信息、所述证书链和所述第一可验证信息分别发送给所述终端设备和所述车载设备，以使所述终端设备在对所述目标验证信息、所述证书链和所述第一可验证信息验证通过的情况下，基于所述目标验证信息，对所述控车指令进行处理，使所述车载设备基于所述车载设备的预设密钥，对所述第一可验证信息、所述证书链和所述目标验证信息进行验证通过后，基于所述目标验证信息，对所述终端设备发送的所述处理后的控车指令进行处理。

[193] 本说明书实施例提供一种基于隐私保护的验证设备，由于目标验证信息是第一服务器生成的与终端设备和车载设备对应的验证信息，且证书链也是由第一服务器、终端设备和车载设备的相关信息构成的证书链，所以，终端设备和车载设备可分别通过目标验证信息和证书链，对本地以及另一方（即车载设备或终端设备）进行身份验证，在验证结果为通过的情况下，在通过目标验证信息对控车指令进行处理，可提高控车指令在传输过程中的安全性。

实施例十三

[194] 本说明书实施例还提供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，该计算机程序被处理器执行时实现上述基于隐私保护的验证方法实施例的各个过程，且能达到相同的技术效果，为避免重复，这里不再赘述。所述的计算机可读

存储介质，如只读存储器（Read-Only Memory，简称 ROM）、随机存取存储器（Random Access Memory，简称 RAM）、磁碟或者光盘等。

[195] 本说明书实施例提供一种计算机可读存储介质，由于目标验证信息是第一服务器生成的与终端设备和车载设备对应的验证信息，且证书链也是由第一服务器、终端设备和车载设备的相关信息构成的证书链，所以，终端设备和车载设备可分别通过目标验证信息和证书链，对本地以及另一方（即车载设备或终端设备）进行身份验证，在验证结果为通过的情况下，在通过目标验证信息对控车指令进行处理，可提高控车指令在传输过程中的安全性。

[196] 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可按照不同于实施例中的顺序来执行并且仍然可实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可的或者可能是有利的。

[197] 在 20 世纪 90 年代，对于一个技术的改进可很明显地区分是硬件上的改进（例如，对二极管、晶体管、开关等电路结构的改进）还是软件上的改进（对于方法流程的改进）。然而，随着技术的发展，当今的很多方法流程的改进已经可视为硬件电路结构的直接改进。设计人员几乎都通过将改进的方法流程编程到硬件电路中来得到相应的硬件电路结构。因此，不能说一个方法流程的改进就不能用硬件实体模块来实现。例如，可编程逻辑器件（Programmable Logic Device，PLD）（例如现场可编程门阵列（Field Programmable Gate Array，FPGA））就是这样一种集成电路，其逻辑功能由用户对器件编程来确定。由设计人员自行编程来把一个数字系统“集成”在一片 PLD 上，而不需要请芯片制造厂商来设计和制作专用的集成电路芯片。而且，如今，取代手工地制作集成电路芯片，这种编程也多半改用“逻辑编译器（logic compiler）”软件来实现，它与程序开发撰写时所用的软件编译器相类似，而要编译之前的原始代码也得用特定的编程语言来撰写，此称之为硬件描述语言（Hardware Description Language，HDL），而 HDL 也并非仅有一种，而是有许多种，如 ABEL（Advanced Boolean Expression Language）、AHDL（Altera Hardware Description Language）、Confluence、CUPL（Cornell University Programming Language）、HDCal、JHDL（Java Hardware Description Language）、Lava、Lola、MyHDL、PALASM、RHDL（Ruby Hardware Description Language）等，目前最普遍使用的是 VHDL（Very-High-Speed Integrated Circuit Hardware Description Language）与 Verilog。本领域技术人员也应该清楚，只需要将方法流程用上述几种硬件描述语言稍作逻辑编程并编程到集成电路中，就可很容易得到实现该逻辑方法流程的硬件电路。

[198] 控制器可按任何适当的方式实现，例如，控制器可采取例如微处理器或处理器以及存储可由该（微）处理器执行的计算机可读程序代码（例如软件或固件）的计算机可读介质、逻辑门、开关、专用集成电路（Application Specific Integrated Circuit，ASIC）、可编程逻辑控制器和嵌入微控制器的形式，控制器的例子包括但不限于以下微控制器：ARC 625D、Atmel AT91SAM、Microchip PIC18F26K20 以及 Silicone Labs C8051F320，存储器控制器还可被实现为存储器的控制逻辑的一部分。本领域技术人员也知道，除了以纯计算机可读程序代码方式实现控制器以外，完全可通过将方法步骤进行逻辑编程来使得控制器以逻辑门、开关、专用集成电路、可编程逻辑控制器和嵌入微控制器等的形式来实现相同功能。因此这种控制器可被认为是一种硬件部件，而对其内包括的用于实现各种功能的装置也可视为硬件部件内的结构。或者甚至，可将用于实现各种功能的装置视为既可是实现方法的软件模块又可是硬件部件内的结构。

[199] 上述实施例阐明的系统、装置、模块或单元，具体可由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机。具体的，计算机例如可为个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任何设备的组合。为了描述的方便，描述以上装置时以功能分为各种单元分别描述。当然，在实施本说明书一个或多个实施例时可把各单元的功能在同一个或多个软件和/或硬件中实现。

[200] 本领域内的技术人员应明白，本说明书的实施例可提供为方法、系统、或计算机程序产品。因此，本说明书一个或多个实施例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，本说明书一个或多个实施例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。

[201] 本说明书的实施例是参照根据本说明书实施例的方法、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。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。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。

[202] 在一个典型的配置中，计算设备包括一个或多个处理器（CPU）、输入/输出接口、网络接口和内存。内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器（RAM）和/或非易失性内存等形式，如只读存储器（ROM）或闪存（flash RAM）。内存是计算机可读介质的示例。计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可由任何方法或技术来实现信息存储。信息可是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存（PRAM）、静态随机存取存储器（SRAM）、动态随机存取存储器（DRAM）、其他类型的随机存取存储器（RAM）、只读存储器（ROM）、电可擦除可编程只读存储器（EEPROM）、快闪记忆体或其他内存技术、只读光盘只读存储器（CD-ROM）、数字多功能光盘（DVD）或其他光学存储、磁盒式磁带，磁带磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体（transitory media），如调制的数据信号和载波。

[203] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[204] 本领域技术人员应明白，本说明书的实施例可提供为方法、系统或计算机程序产品。因此，本说明书一个或多个实施例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，本说明书一个或多个实施例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。

[205] 本说明书一个或多个实施例可在由计算机执行的计算机可执行指令的一般上下文中描述，例如程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可在分布式计算环境中实践本说明书一个或多个实施例，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可位于包括存储设备在内的本地和远程计算机存储介质中。

[206] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于系统实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[207] 以上所述仅为本说明书的实施例而已，并不用于限制本说明书。对于本领域技术人员来说，本说明书可有各种更改和变化。凡在本说明书的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本说明书的权利要求范围之内。

权利要求书

1、一种基于隐私保护的验证方法，应用于终端设备，包括：

将针对控制车载设备的本地的身份验证请求发送给第一服务器，所述第一服务器用于针对所述身份验证请求，生成与所述终端设备、所述车载设备对应的目标验证信息；

接收所述第一服务器发送的所述目标验证信息和预先构建的证书链，基于所述终端设备的预设密钥，对所述证书链和所述目标验证信息进行验证，得到验证结果，所述证书链为由所述第一服务器信息、所述第一服务器的预设密钥、所述终端设备的设备信息、所述终端设备的预设密钥、所述车载设备的设备信息和所述车载设备的预设密钥生成的多级证书链；

在所述验证结果为验证通过的情况下，基于所述目标验证信息对控车指令进行处理，并将处理后的控车指令发送给所述车载设备，以使所述车载设备基于所述目标验证信息和所述证书链，对所述控车指令进行处理。

2、根据权利要求 1 所述的方法，在所述接收所述第一服务器发送的所述目标验证信息和预先构建的证书链之前，所述方法还包括：

接收所述第一服务器的服务器信息以及所述第一服务器的第一公钥，所述第一公钥为所述第一服务器基于预设密钥生成算法，生成的与所述第一服务器对应的密钥；

基于所述预设密钥生成算法，生成与所述终端设备对应的第二私钥和第二公钥；

基于所述第二私钥，对所述终端设备的设备信息进行签名，得到第一签名信息；

基于所述第二公钥、所述终端设备的设备信息和所述第一签名信息，生成根证书；

基于所述第二私钥，对所述服务器信息进行签名，得到第二签名信息；

基于所述第一公钥、所述服务器信息和所述第二签名信息，生成第二证书；

将所述根证书和所述第二证书构成的第一证书链发送给所述第一服务器，以使所述第一服务器基于所述第一证书链、所述车载设备的设备信息和所述车载设备的预设密钥，构建所述证书链。

3、根据权利要求 2 所述的方法，在所述接收所述第一服务器发送的所述目标验证信息和预先构建的证书链之前，还包括：

基于所述预设密钥生成算法，生成与用户对应的第四公钥；

将所述第四公钥以及所述终端设备的设备信息发送给所述第一服务器，以使所述第一服务器基于所述终端设备的设备信息、所述第四公钥、所述车载设备的预设密钥以及所述车载设备的设备信息，生成所述目标验证信息。

4、根据权利要求 3 所述的方法，所述基于所述终端设备的预设密钥，对所述证书链和所述目标验证信息进行验证，得到验证结果，包括：

接收所述第一服务器发送的第一可验证信息，所述第一可验证信息为所述第一服务器基于所述第一服务器的第一私钥，对所述目标验证信息进行加密处理，得到的与所述目标验证信息对应的信息；

基于所述第一服务器的第一公钥、所述终端设备的第二公钥，对所述证书链中的根证书和所述第二证书进行验证处理，得到第一验证结果；

基于所述第一服务器的第一公钥和所述目标验证信息，对所述第一可验证信息进行验证，得到第二验证结果；

基于所述第一验证结果和所述第二验证结果，确定所述验证结果。

5、根据权利要求 4 所述的方法，所述基于所述目标验证信息对控车指令进行处理，并将处理后的控车指令发送给所述车载设备，包括：

基于所述用户的第四私钥，对所述控车指令进行加密处理，得到第二可验证信息，所述第四私钥为所述终端设备基于所述预设密钥生成算法，生成的与所述第四公钥对应的私钥；

接收所述车载设备的第三公钥，所述第三公钥为所述车载设备基于所述预设密钥生成算法，生成的与所述车载设备对应的密钥；

基于所述车载设备的第三公钥，对所述控车指令和所述第二可验证信息进行加密处理，得到加密处理后的控车指令，并将所述加密处理后的控车指令发送至所述车载设备，以使所述车载设备基于所述第四公钥和第三私钥，对所述控车指令进行处理，所述第三私钥为所述车载设备生成的与所述第三公钥对应的私钥。

6、根据权利要求 4 所述的方法，所述基于所述目标验证信息对控车指令进行处理，

并将处理后的控车指令发送给所述车载设备，包括：

生成针对所述控车指令的第三可验证信息、与所述第三可验证信息对应的第一时间戳以及所述控车指令的有效时间，所述第三可验证信息为所述终端设备基于预设随机数生成算法，生成的与所述控车指令对应的预设位数的随机数；

基于所述用户的第四私钥，对所述第三可验证信息、所述第一时间戳以及所述有效时间进行签名处理，得到第四可验证信息；

接收所述车载设备的第三公钥，所述第三公钥为所述车载设备基于所述预设密钥生成算法，生成的与所述车载设备对应的密钥；

基于所述车载设备的第三公钥，对所述第三可验证信息、所述第一时间戳、所述有效时间以及所述第四可验证信息进行加密处理，得到目标信息，并将所述目标信息发送给所述车载设备；

基于所述第三可验证信息，对所述控车指令进行加密处理，得到第一加密指令；

将所述第一加密指令和与所述控车指令对应的第二时间戳发送给所述车载设备，以使所述车载设备基于所述第一加密指令、所述第二时间戳以及存储的所述目标信息，对所述第一加密指令进行处理。

7、根据权利要求 3 所述的方法，所述基于所述预设密钥生成算法，生成与用户对应的第四公钥，包括：

将针对所述用户的身份验证请求发送给第二服务器；

接收所述第二服务器基于所述身份验证请求生成的目标令牌；

基于所述目标令牌，对所述用户进行身份验证，并在身份验证结果为验证通过的情况下，基于所述预设密钥生成算法，生成与所述用户对应的所述第四公钥。

8、一种基于隐私保护的验证方法，应用于车载设备，包括：

接收第一服务器发送的与终端设备、所述车载设备对应的目标验证信息和预先构建的证书链，所述证书链为由所述第一服务器信息、所述第一服务器的预设密钥、所述终端设备的设备信息、所述终端设备的预设密钥、所述车载设备的设备信息和所述车载设备的预设密钥生成的多级证书链；

基于所述车载设备的预设密钥，对所述证书链和所述目标验证信息进行验证，得到验证结果；

在所述验证结果为验证通过的情况下，基于所述目标验证信息，对所述终端设备发送的处理后的控车指令进行处理，得到控车指令，并执行所述控车指令，所述处理后的控车指令为所述终端设备基于所述目标验证信息对所述控车指令进行处理得到的指令。

9、根据权利要求 8 所述的方法，在所述基于所述车载设备的预设密钥，对所述证书链和所述目标验证信息进行验证之前，还包括：

基于预设密钥生成算法，生成与所述车载设备对应的第三公钥；

将所述第三公钥和所述车载设备的设备信息发送给所述第一服务器，以使所述第一服务器基于所述第三公钥、所述车载设备的设备信息、所述第一服务器信息、所述第一服务器的预设密钥、所述终端设备的设备信息以及所述终端设备的预设密钥生成所述证书链。

10、根据权利要求 9 所述的方法，所述基于所述车载设备的预设密钥，对所述证书链和所述目标验证信息进行验证，得到验证结果，包括：

基于所述车载设备的第三公钥，对所述证书链进行验证处理，得到第三验证结果；

接收所述第一服务器发送的第一公钥和第一可验证信息，所述第一可验证信息为所述第一服务器基于所述第一服务器的第一私钥，对所述目标验证信息进行签名处理，得到与所述目标验证信息对应的信息，所述第一公钥和第一私钥为所述第一服务器基于预设密钥生成算法，生成的与所述第一服务器对应的密钥；

基于所述第一服务器的第一公钥和所述目标验证信息，对所述第一可验证信息进行验证，得到第四验证结果；

基于所述第三验证结果和所述第四验证结果，确定所述验证结果。

11、根据权利要求 9 所述的方法，所述基于所述目标验证信息，对所述终端设备发送的处理后的控车指令进行处理，得到控车指令，并执行所述控车指令，包括：

接收所述终端设备发送的第四公钥，所述第四公钥为所述终端设备基于预设密钥生成算法，生成的与所述终端设备的用户对应的密钥；

基于所述车载设备的第三私钥，对所述终端设备发送的处理后的控车指令进行处理，得到所述控车指令和第二可验证信息，所述处理后的控车指令为所述终端设备基于所述车载设备的第三公钥对所述控车指令进行加密处理得到的，所述第三私钥为所述车载设备基于预设密钥生成算法，生成的与所述第三公钥对应的私钥，所述第二可验证信息为所述终端设备基于所述用户的第四私钥，对所述控车指令进行加密处理得到的信息，所述第四私钥为所述终端设备基于所述预设密钥生成算法，生成的与所述第四公钥对应的私钥；

基于所述控车指令、所述用户的第四公钥，对所述第二可验证信息进行验证处理，并在验证通过的情况下，执行所述控车指令。

12、根据权利要求 9 所述的方法，所述基于所述目标验证信息，对所述终端设备发送的处理后的控车指令进行处理，得到控车指令，并执行所述控车指令，包括：

接收所述终端设备发送的第四公钥，所述第四公钥为所述终端设备基于预设密钥生成算法，生成的与所述终端设备的用户对应的密钥；

接收所述终端设备发送的目标信息，所述目标信息为所述终端设备基于所述车载设备的第三公钥，对第三可验证信息、与所述第三可验证信息对应的第一时间戳、所述控车指令的有效时间以及第四可验证信息进行加密处理得到的信息，所述第三可验证信息为所述终端设备基于预设随机数生成算法，生成的与所述控车指令对应的预设位数的随机数，所述第四可验证信息为所述终端设备基于所述用户的第四私钥，对所述第三可验证信息、所述第一时间戳以及所述有效时间进行签名处理得到的信息；

基于所述车载设备的第三私钥，对所述目标信息进行处理，得到所述第三可验证信息、所述第一时间戳、所述有效时间以及所述第四可验证信息；

基于所述用户的第四公钥、所述第三可验证信息、所述第一时间戳以及所述有效时间，对所述第四可验证信息进行处理，在验证通过的情况下，存储所述第三可验证信息、所述第一时间戳和所述有效时间；

基于存储的所述第三可验证信息，对所述终端设备发送的第一加密指令进行处理，得到所述控车指令，所述第一加密指令为所述终端设备基于所述第三可验证信息，对所述控车指令进行加密处理得到的指令；

基于存储的所述第一时间戳和所述有效时间，对所述第二时间戳进行验证处理，在验证通过的情况下，执行所述控车指令。

13、一种基于隐私保护的验证方法，应用于第一服务器，包括：

在接收到终端设备发送的针对控制车载设备的本地的身份验证请求的情况下，生成与所述终端设备、所述车载设备对应的目标验证信息；

将所述目标验证信息和预先构建的证书链发送给所述终端设备和所述车载设备，以使所述终端设备基于所述终端设备的预设密钥，对所述证书链和所述目标验证信息进行验证通过后，基于所述目标验证信息，对控车指令进行处理，使所述车载设备基于所述车载设备的预设密钥，对所述证书链和所述目标验证信息进行验证通过后，基于所述目标验证信息，对所述终端设备发送的所述处理后的控车指令进行处理，所述证书链为由所述第一服务器信息、所述第一服务器的预设密钥、所述终端设备的设备信息、所述终端设备的预设密钥、所述车载设备的设备信息和所述车载设备的预设密钥生成的多级证书链。

14、根据权利要求 13 所述的方法，在所述将所述目标验证信息和预先构建的证书链发送给所述终端设备和所述车载设备之前，还包括：

基于预设密钥生成算法，生成与所述第一服务器对应的第一私钥和第一公钥；

将所述第一公钥和所述服务器信息发送给所述终端设备；

接收所述终端设备发送的由根证书和第二证书构成的第一证书链，所述根证书为所述终端设备基于第二公钥、所述终端设备的设备信息和第一签名信息确定的，所述第一签名信息为所述终端设备基于第二私钥，对所述终端设备的设备信息进行签名得到的，所述第二公钥和第二私钥为所述终端设备基于所述预设密钥生成算法，生成的与所述终端设备对应的密钥，所述第二证书为所述终端设备基于所述第一公钥、所述服务器信息和第二签名信息确定的，所述第二签名信息为所述终端设备基于所述第二私钥，对所述服务器信息进行签名得到的；

接收所述车载设备发送的第三公钥和所述车载设备的设备信息，所述第三公钥为

所述车载设备基于所述预设密钥生成算法，生成的与所述车载设备对应的密钥；

基于所述第一私钥，对所述车载设备的设备信息进行签名，得到第三签名信息；

将所述第三公钥、所述车载设备的设备信息和所述第三签名信息，确定为所述第三证书；

存储由所述第三证书和所述第一证书链构成的所述证书链。

15、根据权利要求 14 所述的方法，所述将所述目标验证信息和预先构建的证书链发送给所述终端设备和所述车载设备，包括：

基于所述第一服务器的第一私钥，对所述目标验证信息进行签名处理，得到与所述目标验证信息对应的第一可验证信息，并将所述目标验证信息、所述证书链和所述第一可验证信息分别发送给所述终端设备和所述车载设备，以使所述终端设备在对所述目标验证信息、所述证书链和所述第一可验证信息验证通过的情况下，基于所述目标验证信息，对所述控车指令进行处理，使所述车载设备基于所述车载设备的预设密钥，对所述第一可验证信息、所述证书链和所述目标验证信息进行验证通过后，基于所述目标验证信息，对所述终端设备发送的所述处理后的控车指令进行处理。

16、一种基于隐私保护的验证系统，包括终端设备、车载设备和第一服务器，其中，

所述终端设备，用于将针对控制所述车载设备的本地的身份验证请求发送给所述第一服务器；

所述第一服务器，用于生成与所述终端设备、所述车载设备对应的目标验证信息，并将所述目标验证信息和预先构建的证书链发送给所述终端设备和所述车载设备；所述证书链为由所述第一服务器信息、所述第一服务器的预设密钥、所述终端设备的设备信息、所述终端设备的预设密钥、所述车载设备的设备信息和所述车载设备的预设密钥生成的多级证书链；

所述终端设备，用于基于所述终端设备的预设密钥对所述证书链和所述目标验证信息进行验证，得到第一验证结果；在所述第一验证结果为验证通过的情况下，基于所述目标验证信息对控车指令进行处理，并将处理后的所述控车指令发送给所述车载设备；

所述车载设备，用于基于所述车载设备的预设密钥，对所述证书链和所述目标验证信息进行验证，得到第二验证结果；在所述第二验证结果为验证通过的情况下，基于所述目标验证信息对接收到的所述处理后的控车指令进行处理，得到所述控车指令，并执行所述控车指令。

17、一种基于隐私保护的验证装置，包括：

请求发送模块，用于将针对控制车载设备的本地的身份验证请求发送给第一服务器，所述第一服务器用于针对所述身份验证请求，生成与所述基于隐私保护的验证装置、所述车载设备对应的目标验证信息；

验证模块，用于接收所述第一服务器发送的所述目标验证信息和预先构建的证书链，基于所述终端设备的预设密钥，对所述证书链和所述目标验证信息进行验证，得到验证结果，所述证书链为由所述第一服务器信息、所述第一服务器的预设密钥、所述基于隐私保护的验证装置的设备信息、所述基于隐私保护的验证装置的预设密钥、所述车载设备的设备信息和所述车载设备的预设密钥生成的多级证书链；

指令发送模块，用于在所述验证结果为验证通过的情况下，基于所述目标验证信息对控车指令进行处理，并将处理后的控车指令发送给所述车载设备，以使所述车载设备基于所述目标验证信息和所述证书链，对所述控车指令进行处理。

18、一种基于隐私保护的验证装置，包括：

信息接收模块，用于接收第一服务器发送的与终端设备、所述基于隐私保护的验证装置对应的目标验证信息和预先构建的证书链，所述证书链为由所述第一服务器信息、所述第一服务器的预设密钥、所述终端设备的设备信息、所述终端设备的预设密钥、所述基于隐私保护的验证装置的设备信息和所述基于隐私保护的验证装置的预设密钥生成的多级证书链；

验证模块，用于基于所述基于隐私保护的验证装置的预设密钥，对所述证书链和所述目标验证信息进行验证，得到验证结果；

指令处理模块，用于在所述验证结果为验证通过的情况下，基于所述目标验证信息，对所述终端设备发送的处理后的控车指令进行处理，得到控车指令，并执行所述控车指令，所述处理后的控车指令为所述终端设备基于所述目标验证信息对所述控车指令进行

处理得到的指令。

19、一种基于隐私保护的验证装置，包括：

信息生成模块，用于在接收到终端设备发送的针对控制车载设备的本地的身份验证请求的情况下，生成与所述终端设备、所述车载设备对应的目标验证信息；

信息发送模块，用于将所述目标验证信息和预先构建的证书链发送给所述终端设备和所述车载设备，以使所述终端设备基于所述终端设备的预设密钥，对所述证书链和所述目标验证信息进行验证通过后，基于所述目标验证信息，对控车指令进行处理，使所述车载设备基于所述车载设备的预设密钥，对所述证书链和所述目标验证信息进行验证通过后，基于所述目标验证信息，对所述终端设备发送的所述处理后的控车指令进行处理，所述证书链为由所述基于隐私保护的验证装置信息、所述基于隐私保护的验证装置的预设密钥、所述终端设备的设备信息、所述终端设备的预设密钥、所述车载设备的设备信息和所述车载设备的预设密钥生成的多级证书链。

20、一种基于隐私保护的验证设备，所述基于隐私保护的验证设备包括处理器以及被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器：

将针对控制车载设备的本地的身份验证请求发送给第一服务器，所述第一服务器用于针对所述身份验证请求，生成与所述基于隐私保护的验证设备、所述车载设备对应的目标验证信息；

接收所述第一服务器发送的所述目标验证信息和预先构建的证书链，基于所述基于隐私保护的验证设备的预设密钥，对所述证书链和所述目标验证信息进行验证，得到验证结果，所述证书链为由所述第一服务器信息、所述第一服务器的预设密钥、所述基于隐私保护的验证设备的设备信息、所述基于隐私保护的验证设备的预设密钥、所述车载设备的设备信息和所述车载设备的预设密钥生成的多级证书链；

在所述验证结果为验证通过的情况下，基于所述目标验证信息对控车指令进行处理，并将处理后的控车指令发送给所述车载设备，以使所述车载设备基于所述目标验证信息和所述证书链，对所述控车指令进行处理。

21、一种基于隐私保护的验证设备，所述基于隐私保护的验证设备包括处理器以及被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器：

接收第一服务器发送的与终端设备、所述基于隐私保护的验证设备对应的目标验证信息和预先构建的证书链，所述证书链为由所述第一服务器信息、所述第一服务器的预设密钥、所述终端设备的设备信息、所述终端设备的预设密钥、所述基于隐私保护的验证设备的设备信息和所述基于隐私保护的验证设备的预设密钥生成的多级证书链；

基于所述基于隐私保护的验证设备的预设密钥，对所述证书链和所述目标验证信息进行验证；

在验证通过后，基于所述目标验证信息，对所述终端设备发送的处理后的控车指令进行处理，得到控车指令，并执行所述控车指令，所述处理后的控车指令为所述终端设备基于所述目标验证信息对所述控车指令进行处理得到的指令。

22、一种基于隐私保护的验证设备，所述基于隐私保护的验证设备包括处理器以及被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器：

在接收到终端设备发送的针对控制车载设备的本地的身份验证请求的情况下，生成与所述终端设备、所述车载设备对应的目标验证信息；

将所述目标验证信息和预先构建的证书链发送给所述终端设备和所述车载设备，以使所述终端设备基于所述终端设备的预设密钥，对所述证书链和所述目标验证信息进行验证通过后，基于所述目标验证信息，对控车指令进行处理，使所述车载设备基于所述车载设备的预设密钥，对所述证书链和所述目标验证信息进行验证通过后，基于所述目标验证信息，对所述终端设备发送的所述处理后的控车指令进行处理，所述证书链为由所述基于隐私保护的验证设备信息、所述基于隐私保护的验证设备的预设密钥、所述终端设备的设备信息、所述终端设备的预设密钥、所述车载设备的设备信息和所述车载设备的预设密钥生成的多级证书链。