(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 112585905 B
(45)授权公告日 2021.11.19

(21)申请号 201980053551.5
(22)申请日 2019.11.12
(65)同一申请的已公布的文献号
申请公布号 CN 112585905 A
(43)申请公布日 2021.03.30
(85)PCT国际申请进入国家阶段日
2021.02.08
(86)PCT国际申请的申请数据
PCT/CN2019/117399 2019.11.12
(73)专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼
(72)发明人 林孝盈 摩罗·康帝 安瑞塔·后姜 索比尔·哈尔德
(51)Int.Cl.
H04L 12/24(2006.01)
H04L 29/06(2006.01)
(56)对比文件
CN 108566381 A,2018.09.21
CN 109543439 A,2019.03.29
CN 105933150 A,2016.09.07
CN 102624522 A,2012.08.01
CN 105721448 A,2016.06.29
CN 105991278 A,2016.10.05
CN 110224986 A,2019.09.10
CN 108880796 A,2018.11.23
审查员 丁炜

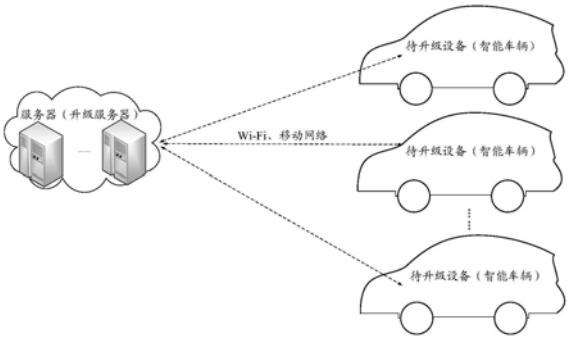
权利要求书4页 说明书34页 附图12页

(54)发明名称

一种设备升级方法及相关设备

(57)摘要

一种设备升级方法及相关设备，具体可以应用于智能车辆以及无人驾驶车辆，保证车辆内部车载设备升级的安全性，其中的方法包括服务器根据待升级设备的属性集合生成针对所述待升级设备的访问策略；所述服务器根据所述访问策略对目标升级包进行加密，生成目标升级包密文；所述服务器将所述目标升级包密文发送至所述待升级设备，所述目标升级包密文用于所述待升级设备根据所述属性集合对应的一个或多个属性密钥进行解密，以获得所述目标升级包。可用于保障家用设备或车载设备的安全高效的升级。



CN 112585905 B

1.一种设备升级方法,其特征在于,包括:

服务器接收终端设备发送的待升级设备的升级请求,所述升级请求包括所述待升级设备的属性集合,所述待升级设备的属性集合包括所述终端设备的一个或多个属性信息以及所述待升级设备的一个或多个属性信息;

所述服务器根据所述待升级设备的属性集合获取所述待升级设备的访问策略,所述访问策略包括所述待升级设备的属性集合中的一个或多个属性信息;

所述服务器根据所述访问策略对目标升级包进行加密,生成目标升级包密文;

所述服务器将所述目标升级包密文发送至所述待升级设备,所述目标升级包密文用于所述待升级设备根据所述访问策略中包括的所述一个或多个属性信息对应的一个或多个属性密钥进行解密,以获得所述目标升级包。

2.根据权利要求1所述的方法,其特征在于,所述服务器根据待升级设备的属性集合获取所述待升级设备的访问策略,包括:

所述服务器根据所述终端设备的一个或多个属性信息以及所述待升级设备的一个或多个属性信息,确定所述待升级设备需要升级的一个或多个升级文件,所述目标升级包包括所述一个或多个升级文件;

所述服务器确定所述一个或多个升级文件对应的升级条件,并基于所述升级条件生成所述访问策略。

3.根据权利要求1或2所述的方法,其特征在于,所述方法还包括:

所述服务器生成公钥和主密钥,所述主密钥为所述公钥对应的私钥;

所述服务器根据所述主密钥以及所述一个或多个属性信息,生成所述一个或多个属性信息对应的一个或多个属性密钥;

所述服务器将所述一个或多个属性密钥发送至所述待升级设备进行预存储;其中,所述一个或多个属性密钥用于所述待升级设备对所述目标升级包密文进行解密以获得所述目标升级包。

4.根据权利要求1或2所述的方法,其特征在于,所述方法还包括:

所述服务器生成公钥和主密钥,所述主密钥为所述公钥对应的私钥;

所述服务器将所述主密钥发送至所述待升级设备上进行预存储,所述主密钥用于所述待升级设备生成所述一个或多个属性信息对应的一个或多个属性密钥,其中,所述一个或多个属性密钥用于所述待升级设备对所述目标升级包密文进行解密以获得所述目标升级包。

5.根据权利要求3或4所述的方法,

所述公钥和所述主密钥对应至少一个属性信息相同的多个不同待升级设备。

6.根据权利要求1-5任意一项所述的方法,其特征在于,所述目标升级包包括所述一个或多个属性信息中至少一个属性信息对应的更新后的属性密钥。

7.根据权利要求1至6任一项所述的方法,所述升级请求还包括所述终端设备的身份信息和所述待升级设备的身份信息,所述终端设备的身份信息和所述待升级设备的身份信息用于所述服务器对所述终端设备和所述待升级设备分别进行身份验证。

8.一种设备升级方法,其特征在于,包括:

待升级设备通过所述终端设备向服务器发送升级请求,所述升级请求包括所述待升级

设备的属性集合；

待升级设备接收所述服务器发送的目标升级包密文，所述目标升级包密文为所述服务器根据访问策略对目标升级包进行加密生成的，所述访问策略是所述服务器根据所述待升级设备的属性集合生成的，所述待升级设备的属性集合包括所述终端设备的一个或多个属性信息以及所述待升级设备的一个或多个属性信息，所述访问策略包括所述待升级设备的属性集合中的一个或多个属性信息；

所述待升级设备获取访问策略中包括的所述一个或多个属性信息对应的一个或多个属性密钥；

所述待升级设备根据所述一个或多个属性密钥对所述目标升级包密文进行解密，获得目标升级包。

9.根据权利要求8所述的方法，其特征在于，所述方法还包括：

所述待升级设备接收所述服务器发送的一个或多个属性密钥，并进行预存储；所述属性密钥为所述服务器生成公钥和主密钥后，根据所述主密钥以及所述一个或多个属性信息，生成的一个或多个属性密钥；所述主密钥为所述公钥对应的私钥。

10.根据权利要求8所述的方法，其特征在于，所述方法还包括：

所述待升级设备接收所述服务器发送的主密钥并进行预存储，所述主密钥为所述服务器生成的；

所述待升级设备根据所述主密钥以及所述一个或多个属性信息，生成所述一个或多个属性信息对应的一个或多个属性密钥。

11.根据权利要求8至10任一项所述的方法，所述目标升级包包括所述一个或多个属性信息中至少一个属性信息对应的更新后的属性密钥。

12.一种设备升级装置，其特征在于，应用于服务器，所述装置包括：

获取单元，用于接收终端设备发送的待升级设备的升级请求，所述升级请求包括所述待升级设备的属性集合，所述待升级设备的属性集合包括所述终端设备的一个或多个属性信息以及所述待升级设备的一个或多个属性信息；

策略生成单元，用于根据所述待升级设备的属性集合获取所述待升级设备的访问策略，所述访问策略包括所述待升级设备的属性集合中的一个或多个属性信息；

加密单元，用于根据所述访问策略对目标升级包进行加密，生成目标升级包密文；

第一发送单元，用于将所述目标升级包密文发送至所述待升级设备，所述目标升级包密文用于所述待升级设备根据所述访问策略中包括的所述一个或多个属性信息对应的一个或多个属性密钥进行解密，以获得所述目标升级包。

13.根据权利要求12所述的装置，其特征在于，所述生成单元，具体用于：

根据所述终端设备的一个或多个属性信息以及所述待升级设备的一个或多个属性信息，确定所述待升级设备需要升级的一个或多个升级文件，所述目标升级包包括所述一个或多个升级文件；

确定所述一个或多个升级文件对应的升级条件，并基于所述升级条件生成所述访问策略。

14.根据权利要求12或13所述的装置，其特征在于，所述装置还包括：

第一密钥生成单元，用于生成公钥和主密钥，所述主密钥为所述公钥对应的私钥；

第二密钥生成单元，根据所述主密钥以及所述一个或多个属性信息，生成所述一个或多个属性信息对应的一个或多个属性密钥；

第二发送单元，用于将所述一个或多个属性密钥发送至所述待升级设备进行预存储；其中，所述一个或多个属性密钥用于所述待升级设备对所述目标升级包密文进行解密以获得所述目标升级包。

15.根据权利要求12或13所述的装置，其特征在于，所述装置还包括：

第三密钥生成单元，用于生成公钥和主密钥，所述主密钥为所述公钥对应的私钥；

第三发送单元，用于将所述主密钥发送至所述待升级设备上进行预存储，所述主密钥用于所述待升级设备生成所述一个或多个属性信息对应的一个或多个属性密钥，其中，所述一个或多个属性密钥用于所述待升级设备对所述目标升级包密文进行解密以获得所述目标升级包。

16.根据权利要求14或15所述的装置，

所述公钥和所述主密钥对应至少一个属性信息相同的多个不同待升级设备。

17.根据权利要求12-16任意一项所述的装置，其特征在于，所述目标升级包包括所述一个或多个属性信息中至少一个属性信息对应的更新后的属性密钥。

18.根据权利要求12至17任一项所述的装置，所述升级请求还包括所述终端设备的身份信息和所述待升级设备的身份信息，所述终端设备的身份信息和所述待升级设备的身份信息用于对所述终端设备和所述待升级设备进行身份验证。

19.一种待升级装置，其特征在于，应用于待升级设备，所述装置包括：

发送单元，用于通过终端设备向服务器发送升级请求，所述升级请求包括所述待升级设备的属性集合；

接收单元，用于接收所述服务器发送的目标升级包密文，所述目标升级包密文为所述服务器根据访问策略对目标升级包进行加密生成的，所述访问策略是根据所述待升级设备的属性集合生成的，所述待升级设备的属性集合包括所述终端设备的一个或多个属性信息以及所述待升级设备的一个或多个属性信息，所述访问策略包括所述待升级设备的属性集合中的一个或多个属性信息；

获取单元，用于获取访问策略中包括的所述一个或多个属性信息对应的一个或多个属性密钥；

解密单元，用于根据所述一个或多个属性密钥对所述目标升级包密文进行解密，获得目标升级包。

20.根据权利要求19所述的装置，其特征在于，所述获取单元，具体用于：

接收所述服务器发送的一个或多个属性密钥，并进行预存储；所述属性密钥为所述服务器生成公钥和主密钥后，根据所述主密钥以及所述一个或多个属性信息，生成的一个或多个属性密钥；所述主密钥为所述公钥对应的私钥。

21.根据权利要求19所述的装置，其特征在于，所述获取单元，具体用于：

接收所述服务器发送主密钥并进行预存储，所述主密钥为所述服务器生成的；

所述待升级设备根据所述主密钥以及所述一个或多个属性信息，生成所述一个或多个属性信息对应的一个或多个属性密钥。

22.根据权利要求19至21任一项所述的装置，所述目标升级包包括所述一个或多个属

性信息中至少一个属性信息对应的更新后的属性密钥。

一种设备升级方法及相关设备

技术领域

[0001] 本申请涉及设备升级技术领域,尤其涉及一种设备升级方法及相关设备。

背景技术

[0002] 远程在线升级通常指在设备(如电脑、手机等)在连接网络的情况下,从服务器下载升级文件以将操作系统、软件等更新至最新状态,无需大量的人工干预,则便可以自主完成设备升级,成本低、且升级效率高。

[0003] 以升级设备为车载设备为例,未来的每辆车都是车联网中的一个网络节点,与电脑,手机等联网设备没有本质的不同。据估计,北美60%到70%车辆招回是由于固件/软件的原因,因此升级车载设备的固件/软件是必不可少的环节。传统待升级车载单元的固件/软件是采用车辆招回的方式,这种办法的缺点是:成本高、周期长。

[0004] 因此,未来车载设备的升级应采用更灵活的远程在线升级方式,如空中下载技术(Over-The-Air,OTA),就像现在的电脑和手机升级一样通过网络来远程升级。对车载设备进行远程固件/软件升级可带来很多好处。例如,便于关键的固件/软件bugs得以快速修复、增加车辆安全性、便于车辆在整个生命周期内及时添加新功能或特色等。因此采用OTA方式不需要车辆招回就可进行固件/软件升级,可为车辆生产商或销售商节省大量成本,同时也为车主带来便利。

[0005] 然而,在车载设备的远程升级过程中,可能存在一些安全隐患。例如,升级文件来源不可靠,升级文件版本、内容不匹配,或者车载设备自身不满足升级条件等,这些都有可能导致车载设备升级的失败或异常,最终导致用户的驾驶安全受到威胁。因此,如何保证包括车载设备等在内的相关设备安全高效的进行固件/软件升级成为亟待解决的问题。

发明内容

[0006] 本发明实施例所要解决的技术问题在于,提供一种设备升级方法及相关设备,解决了升级设备无法安全高效的进行固件/软件升级的问题。

[0007] 第一方面,本发明实施例提供了一种设备升级方法,可包括:

[0008] 服务器根据待升级设备的属性集合生成针对所述待升级设备的访问策略;所述服务器根据所述访问策略对目标升级包进行加密,生成目标升级包密文;所述服务器将所述目标升级包密文发送至所述待升级设备,所述目标升级包密文用于所述待升级设备根据所述属性集合对应的一个或多个属性密钥进行解密,以获得所述目标升级包。

[0009] 本发明实施例中,上述方法为基于属性加密算法来根据访问策略对目标升级包进行加密。而将密文策略属性加密算法(CP-ABE)具体应用到设备升级场景中,服务器可根据待升级设备的属性集合,生成对应的访问策略,并根据该访问策略对待升级设备的升级包进行加密,最终生成只有满足访问策略中所设置的前提条件(即拥有匹配的属性信息所对应的属性密钥)的设备才可以正确解密获得升级包,实现了升级条件的强制检测以及升级包细粒度的访问控制,即非法设备或者不满足升级条件的设备由于没有匹配的属性信息对

应的属性密钥，则无法获得或解密该升级包，保证了设备升级过程的安全性以及准确性。可选的，可以通过在待升级设备的升级请求中携带该待升级设备的属性集合(包含该设备的一个或多个属性信息)的方式，使得服务器获知该待升级设备的属性集合，也可以通过服务器预存储的待升级设备的属性集合或者通过其他途径获得的待升级设备的属性集合进行访问策略的生成。

[0010] 在一种可能的实现方式中，所述方法还包括：所述服务器获取所述待升级设备的升级请求，所述升级请求包括所述待升级设备的属性集合。本发明实施例通过在待升级设备的升级请求中携带待升级设备的属性集合的方式，从而使得服务器可以根据升级请求中的属性集合生成该待升级设备的访问策略。

[0011] 在一种可能的实现方式中，所述服务器获取所述待升级设备的升级请求，包括：所述服务器接收所述待升级设备发送的所述升级请求，所述属性集合包括所述待升级设备的一个或多个属性信息。

[0012] 本发明实施例中，通过待升级设备自身向服务器发送升级请求，且该升级请求中携带了该待升级设备的一个或者多个属性信息。例如，待升级车辆向服务器发送携带有自身的车辆身份码、引擎号、车牌号码、车型流水号、车辆部件的硬件版本号和车辆部件的软件版本号等属性信息的升级请求。

[0013] 在一种可能的实现方式中，所述升级请求还包括所述待升级设备的身份信息；所述方法还包括：所述服务器对所述待升级设备的身份信息进行验证；若验证通过，所述服务器根据所述待升级设备的一个或多个属性信息，确定所述待升级设备需要升级的一个或多个升级文件，所述目标升级包包括所述一个或多个升级文件。

[0014] 本发明实施例中，服务器在获取待升级设备的升级请求后，先对该升级请求做身份验证，若身份验证通过后，则表明该请求者合法，因此根据升级请求中的待升级设备的属性信息确定对应的目标升级包。由于升级包是服务器根据该待升级设备的属性信息确定的，因此可以确保待升级设备可以下载其所精确需要以及符合条件的升级包，避免升级包不符合待升级设备的属性要求，并且，也可以避免不符合该属性信息的待升级设备非法获得升级包，进一步保证了设备升级过程的安全性以及准确性。

[0015] 在一种可能的实现方式中，所述属性集合包括所述待升级设备的一个或多个属性信息；所述服务器根据待升级设备的属性集合生成针对所述待升级设备的访问策略，包括：所述服务器根据所述待升级设备的一个或多个属性信息，确定所述待升级设备需要升级的一个或多个升级文件，所述目标升级包包括所述一个或多个升级文件；所述服务器确定所述一个或多个升级文件对应的升级条件，并基于所述升级条件生成所述访问策略。

[0016] 本发明实施例中，服务器根据待升级设备的一个或者多个属性信息确定一个或多个升级文件，并依据该一个或多个升级文件的升级条件组合后转换为所述访问策略，也即是服务器根据待升级设备的相关属性信息生成针对该待升级设备的升级条件，以限制目标升级包的访问权限。

[0017] 在一种可能的实现方式中，所述服务器获取待升级设备的升级请求，包括：所述服务器接收终端设备发送的所述待升级设备的升级请求，所述属性集合包括所述终端设备的一个或多个属性信息以及所述待升级设备的一个或多个属性信息。

[0018] 本发明实施例中，通过与待升级设备绑定的终端设备向服务器发送升级请求，此

时该升级请求中携带了该终端设备的一个或多个属性信息以及该待升级设备自身的一个或者多个属性信息。例如，与待升级车辆绑定的智能手机向服务器发送携带有自身的手机号、手机识别码和手机的软件版本信息，以及携带有待升级车辆的车辆身份码、引擎号、车牌号码、车型流水号、车辆部件的硬件版本号和车辆部件的软件版本号等属性信息的升级请求。

[0019] 在一种可能的实现方式中，所述升级请求还包括所述终端设备的身份信息和所述待升级设备的身份信息；所述方法还包括：所述服务器对所述终端设备的身份信息和所述终端设备待升级设备的身份信息分别进行验证；若均验证通过，所述服务器根据所述终端设备的一个或多个属性信息以及所述待升级设备的一个或多个属性信息，确定所述待升级设备需要升级的一个或多个升级文件，所述目标升级包包括所述一个或多个升级文件。

[0020] 本发明实施例中，服务器在获取待升级设备的升级请求后，先对该升级请求做身份验证，若身份验证通过后，则表明该请求者合法，因此根据升级请求中的终端设备以及待升级设备的属性信息共同确定对应的目标升级包。由于升级包是服务器根据终端设备和待升级设备的属性信息共同确定的，因此可以确保与对应的终端设备绑定的符合属性信息要求的待升级设备可以下载其所精确需要以及符合条件的升级包，避免升级包不符合终端设备以及待升级设备的属性要求，并且，也可以避免不符合该属性信息的待升级设备非法获得升级包，进一步保证了设备升级过程的安全性以及准确性。

[0021] 在一种可能的实现方式中，所述服务器根据待升级设备的属性集合生成针对所述待升级设备的访问策略，包括：所述服务器根据所述终端设备的一个或多个属性信息以及所述待升级设备的一个或多个属性信息，确定所述待升级设备需要升级的一个或多个升级文件，所述目标升级包包括所述一个或多个升级文件；所述服务器确定所述一个或多个升级文件对应的升级条件，并基于所述升级条件生成所述访问策略。

[0022] 本发明实施例中，由于引入终端设备协助待升级设备进行升级，因此，服务器根据终端设备和待升级设备的多个属性信息确定一个或多个升级文件，并依据该一个或多个升级文件的升级条件组合后转换为所述访问策略，也即是服务器根据终端设备和待升级设备的相关属性信息生成针对该待升级设备的升级条件，以限制目标升级包的访问权限。

[0023] 在一种可能的实现方式中，所述升级请求经过所述公钥的加密；所述方法还包括：所述服务器根据所述公钥对应的私钥对所述升级请求进行解密。

[0024] 本发明实施例中，待升级设备的升级请求本身还可以经过公钥的加密，从而使得服务器可以根据所述公钥对应的私钥对所述升级请求进行解密，保证升级请求发送的安全性。

[0025] 在一种可能的实现方式中，所述属性集合包括一个或多个属性信息；所述方法还包括：所述服务器生成公钥和主密钥，所述主密钥为所述公钥对应的私钥；所述服务器根据所述主密钥以及所述一个或多个属性信息，生成所述属性集合对应的一个或多个属性密钥；所述服务器将所述一个或多个属性密钥发送至所述待升级设备进行预存储；其中，所述一个或多个属性密钥用于所述待升级设备对所述目标升级包密文进行解密以获得所述目标升级包。可选的，所述方法还包括：所述服务器在将一个或多个属性密钥发送至待升级设备上进行预存储时，还将所述公钥发送至所述待升级设备上，以用于所述待升级设备进行升级请求的加密。

[0026] 本发明实施例中，服务器在初始阶段需要生成针对该待升级设备后续安全升级过程中所要使用到的公钥、主密钥(与所述公钥对应的私钥)以及对应的属性密钥，并且将属性密钥发送给拥有对应属性信息的待升级设备，以保证后续的基于密文策略属性加密算法的设备安全升级过程。可选的，还将公钥发送至待升级设备用于待升级设备对升级请求进行加密。

[0027] 在一种可能的实现方式中，所述方法还包括：所述服务器生成公钥和主密钥，所述主密钥为所述公钥对应的私钥；所述服务器将所述主密钥发送至所述待升级设备上进行预存储，所述主密钥用于所述待升级设备生成所述属性集合对应的一个或多个属性密钥，其中，所述一个或多个属性密钥用于所述待升级设备对所述目标升级包密文进行解密以获得所述目标升级包。

[0028] 本方法实施例中，服务器将主密钥发送给待升级设备(可选的，还将公钥与该主密钥一起发送)，用于所述待升级设备在待升级设备的本地，根据满足访问策略中升级条件的属性信息生成对应的属性密钥，进而获得对应的目标升级包。可适用于待升级设备的属性信息变化大的情形，例如，智能车辆为共享车辆，其对应的用户信息或者账户信息等经常变动，导致经常需要不同的属性密钥才能为不同的用户提供设备升级服务等。

[0029] 在一种可能的实现方式中，所述属性集合包括一个或多个属性信息；所述目标升级包包括所述属性集合中至少一个属性信息对应的更新后的属性密钥。

[0030] 本发明实施例中，由于属性密钥可能会存在更新或变更的情况，因此，服务器还可以通过在升级包中携带最新的属性密钥，使得满足属性信息条件的车辆可以根据最新的属性进行升级包的解密，避免需要通过其他额外流程将更新后的属性密钥的发送给待升级设备。

[0031] 在一种可能的实现方式中，所述属性集合包括一个或多个属性信息；其中，至少一个所述属性信息相同的不同待升级设备对应相同的所述公钥和对应的主密钥。

[0032] 本发明实施例中，服务器针对具有相同的某一种或者某几种属性信息的不同待升级设备，使用相同的公钥以及对应的主密钥，可以降低服务器上的存储量以及计算量，提升升级效率。例如具有相同型号的车辆，可以采用相同的公钥和主密钥。

[0033] 在一种可能的实现方式中，所述服务器根据所述属性集合生成针对所述待升级设备的访问策略，包括：所述服务器根据所述属性集合确定所述目标升级包；所述服务器确定所述目标升级包对应的升级条件，并将所述升级条件组合后转换为所述访问策略。

[0034] 本发明实施例中，服务器根据升级请求中的属性集合确定与该待升级设备匹配的目标升级包，并针对该目标升级包定义升级的前提条件，再将升级的前提条件经过组合转换后确定为访问策略，从而使得后续可以根据该访问策略对目标升级包进行加密，以实现对待升级设备的升级条件(例如身份、状态等)的强制力检测。

[0035] 在一种可能的实现方式中，所述待升级设备为智能车辆；所述属性集合包括车辆身份码、引擎号、车牌号码、车型流水号、车辆部件的硬件版本号和车辆部件的软件版本号中的一种或者多种属性信息。

[0036] 本发明实施例中，将上述任意一种设备升级方法应用在车载设备升级场景中，可以保证车辆升级的安全性以及准确性。

[0037] 在一种可能的实现方式中，所述终端设备为智能手机；所述属性集合包括手机号、

手机识别码和手机的软件版本信息中的一种或者多种属性信息。

[0038] 本发明实施例中，通过采用智能手机搭配待升级设备进行升级，提供一种适用于一些特殊场景中的升级系统架构。例如，某个用户可以通过自己的智能手机对与该手绑定的车辆进行安全升级，安全便捷。

[0039] 第二方面，本发明实施例提供了一种设备升级方法，可包括：

[0040] 待升级设备接收服务器发送的目标升级包密文，所述目标升级包密文为所述服务器根据访问策略对目标升级包进行加密生成的，所述访问策略为所述服务器根据所述待升级设备的属性集合生成的；所述待升级设备获取所述属性集合对应的一个或多个属性密钥；所述待升级设备根据所述一个或多个属性密钥对所述目标升级包密文进行解密，获得目标升级包。

[0041] 本发明实施例中，上述方法为基于属性加密算法来根据访问策略对目标升级包进行加密。而将密文策略属性加密算法(CP-ABE)具体应用到设备升级场景中，服务器可根据待升级设备的属性集合，生成对应的访问策略，并根据该访问策略对待升级设备的升级包进行加密，最终生成只有满足访问策略中所设置的前提条件(即拥有匹配的属性信息所对应的属性密钥)的设备才可以正确解密获得升级包，实现了升级条件的强制检测以及升级包细粒度的访问控制，即非法设备或者不满足升级条件的设备由于没有匹配的属性信息对应的属性密钥，则无法获得或解密该升级包，保证了设备升级过程的安全性以及准确性。在一种可能的实现方式中，所述方法还包括：所述待升级设备向所述服务器发送升级请求，所述升级请求包括所述待升级设备的属性集合。

[0042] 在一种可能的实现方式中，所述属性集合包括一个或多个属性信息；所述待升级设备获取所述属性集合对应的一个或多个属性密钥，包括：所述待升级设备接收所述服务器发送的一个或多个属性密钥，并进行预存储；所述属性密钥为所述服务器生成公钥和主密钥后，根据所述主密钥以及所述一个或多个属性信息，生成的一个或多个属性密钥；所述主密钥为所述公钥对应的私钥。

[0043] 在一种可能的实现方式中，所述属性集合包括一个或多个属性信息；所述待升级设备获取所述属性集合对应的一个或多个属性密钥，包括：所述待升级设备接收所述服务器发送的主密钥并进行预存储，所述主密钥为所述服务器生成的；所述待升级设备根据所述主密钥以及所述一个或多个属性信息，生成一个或多个属性密钥。

[0044] 在一种可能的实现方式中，所述升级请求还包括所述待升级设备的身份信息；其中，所述身份信息用于所述服务器进行验证，若验证通过则根据所述待升级设备的一个或多个属性信息，确定所述待升级设备需要升级的一个或多个升级文件，所述目标升级包包括所述一个或多个升级文件。

[0045] 在一种可能的实现方式中，所述升级请求经过所述公钥的加密；其中，加密后的所述升级请求用于所述服务器根据所述公钥对应的私钥对所述升级请求进行解密。

[0046] 在一种可能的实现方式中，所述属性集合包括一个或多个属性信息；所述目标升级包包括所述属性集合中至少一个属性信息对应的更新后的属性密钥。

[0047] 在一种可能的实现方式中，所述属性集合包括一个或多个属性信息；其中，至少一个所述属性信息相同的不同待升级设备对应相同的所述公钥和对应的主密钥。

[0048] 在一种可能的实现方式中，所述待升级设备为智能车辆；所述属性集合包括车辆

身份码、引擎号、车牌号码、车型流水号、车辆部件的硬件版本号和车辆部件的软件版本号中的一种或者多种属性信息。

[0049] 第三方面，本发明实施例提供了一种设备升级方法，可包括：

[0050] 终端设备向服务器发送待升级设备的升级请求，所述升级请求包括所述待升级设备的属性集合，所述属性集合包括所述终端设备的一个或多个属性信息以及所述待升级设备的一个或多个属性信息；所述待升级设备接收所述服务器发送的目标升级包密文，所述目标升级包密文为所述服务器基于属性加密算法，根据访问策略对目标升级包进行加密生成的，所述访问策略为所述服务器根据所述属性集合生成的；

[0051] 所述待升级设备根据所述属性集合对应的一个或多个属性密钥对所述目标升级包密文进行解密，获得目标升级包。

[0052] 在一种可能的实现方式中，所述升级请求还包括所述终端设备的身份信息和所述待升级设备的身份信息；其中，所述终端设备的身份信息和所述待升级设备的身份信息用于所述服务器分别进行验证；若均验证通过则根据所述终端设备的一个或多个属性信息以及所述待升级设备的一个或多个属性信息，确定所述待升级设备需要升级的一个或多个升级文件，所述目标升级包包括所述一个或多个升级文件。

[0053] 在一种可能的实现方式中，所述方法还包括：所述终端设备获取所述终端设备的一个或多个属性信息以及所述待升级设备的一个或多个属性信息。

[0054] 在一种可能的实现方式中，所述方法还包括：所述待升级设备获取所述终端设备的一个或多个属性信息对应的属性密钥，以及所述待升级设备的一个或多个属性信息对应属性密钥。

[0055] 第四方面，本发明实施例提供了一种设备升级装置，可应用于服务器，所述装置可包括：

[0056] 策略生成单元，用于根据待升级设备的属性集合生成针对所述待升级设备的访问策略；

[0057] 加密单元，用于根据所述访问策略对目标升级包进行加密，生成目标升级包密文；

[0058] 第一发送单元，用于将所述目标升级包密文发送至所述待升级设备，所述目标升级包密文用于所述待升级设备根据所述属性集合对应的一个或多个属性密钥进行解密，以获得所述目标升级包。

[0059] 在一种可能的实现方式中，所述装置还包括：

[0060] 获取单元，用于获取所述待升级设备的升级请求，所述升级请求包括所述待升级设备的属性集合。

[0061] 在一种可能的实现方式中，所述获取单元，具体用于：

[0062] 接收所述待升级设备发送的所述升级请求，所述属性集合包括所述待升级设备的一个或多个属性信息。

[0063] 在一种可能的实现方式中，所述属性集合包括所述待升级设备的一个或多个属性信息；所述策略生成单元，具体用于：

[0064] 根据所述待升级设备的一个或多个属性信息，确定所述待升级设备需要升级的一个或多个升级文件，所述目标升级包包括所述一个或多个升级文件；

[0065] 确定所述一个或多个升级文件对应的升级条件，并基于所述升级条件生成所述访

问策略。

[0066] 在一种可能的实现方式中，所述获取单元，具体用于：

[0067] 接收终端设备发送的所述待升级设备的升级请求，所述属性集合包括所述终端设备的一个或多个属性信息以及所述待升级设备的一个或多个属性信息。

[0068] 在一种可能的实现方式中，所述生成单元，具体用于：

[0069] 根据所述终端设备的一个或多个属性信息以及所述待升级设备的一个或多个属性信息，确定所述待升级设备需要升级的一个或多个升级文件，所述目标升级包包括所述一个或多个升级文件；

[0070] 确定所述一个或多个升级文件对应的升级条件，并基于所述升级条件生成所述访问策略。

[0071] 在一种可能的实现方式中，所述属性集合包括一个或多个属性信息；所述装置还包括：

[0072] 第一密钥生成单元，用于生成公钥和主密钥，所述主密钥为所述公钥对应的私钥；

[0073] 第二密钥生成单元，根据所述主密钥以及所述一个或多个属性信息，生成所述属性集合对应的一个或多个属性密钥；

[0074] 第二发送单元，用于将所述一个或多个属性密钥发送至所述待升级设备进行预存储；其中，所述一个或多个属性密钥用于所述待升级设备对所述目标升级包密文进行解密以获得所述目标升级包。

[0075] 在一种可能的实现方式中，所述装置还包括：

[0076] 第三密钥生成单元，用于生成公钥和主密钥，所述主密钥为所述公钥对应的私钥；

[0077] 第三发送单元，用于将所述主密钥发送至所述待升级设备上进行预存储，所述主密钥用于所述待升级设备生成所述属性集合对应的一个或多个属性密钥，其中，所述一个或多个属性密钥用于所述待升级设备对所述目标升级包密文进行解密以获得所述目标升级包。

[0078] 在一种可能的实现方式中，其特征在于，所述属性集合包括一个或多个属性信息；所述目标升级包包括所述属性集合中至少一个属性信息对应的更新后的属性密钥。

[0079] 第五方面，本发明实施例提供了一种待升级装置，可应用于待升级设备，所述装置可包括：

[0080] 接收单元，用于接收服务器发送的目标升级包密文，所述目标升级包密文为所述服务器根据访问策略对目标升级包进行加密生成的，所述访问策略为所述服务器根据所述待升级设备的属性集合生成的；

[0081] 获取单元，用于获取所述属性集合对应的一个或多个属性密钥；

[0082] 解密单元，用于根据所述一个或多个属性密钥对所述目标升级包密文进行解密，获得目标升级包。

[0083] 在一种可能的实现方式中，所述装置还包括：

[0084] 发送单元，用于发送升级请求，所述升级请求包括所述待升级设备的属性集合。

[0085] 在一种可能的实现方式中，所述属性集合包括一个或多个属性信息；所述获取单元，具体用于：

[0086] 接收所述服务器发送的一个或多个属性密钥，并进行预存储；所述属性密钥为所

述服务器生成公钥和主密钥后，根据所述主密钥以及所述一个或多个属性信息，生成的一个或多个属性密钥；所述主密钥为所述公钥对应的私钥。

[0087] 在一种可能的实现方式中，所述属性集合包括一个或多个属性信息；所述获取单元，具体用于：

[0088] 接收所述服务器发送主密钥并进行预存储，所述主密钥为所述服务器生成的；

[0089] 所述待升级设备根据所述主密钥以及所述一个或多个属性信息，生成一个或多个属性密钥。

[0090] 在一种可能的实现方式中，所述升级请求还包括所述待升级设备的身份信息；其中，所述身份信息用于所述服务器进行验证，若验证通过则根据所述待升级设备的一个或多个属性信息，确定所述待升级设备需要升级的一个或多个升级文件，所述目标升级包包括所述一个或多个升级文件。

[0091] 在一种可能的实现方式中，所述升级请求经过所述公钥的加密；其中，加密后的所述升级请求用于所述服务器根据所述公钥对应的私钥对所述升级请求进行解密。

[0092] 在一种可能的实现方式中，所述属性集合包括一个或多个属性信息；所述目标升级包包括所述属性集合中至少一个属性信息对应的更新后的属性密钥。

[0093] 在一种可能的实现方式中，所述属性集合包括一个或多个属性信息；其中，至少一个所述属性信息相同的不同待升级设备对应相同的所述公钥和对应的主密钥。

[0094] 在一种可能的实现方式中，所述待升级设备为智能车辆；所述属性集合包括车辆身份码、引擎号、车牌号码、车型流水号、车辆部件的硬件版本号和车辆部件的软件版本号中的一种或者多种属性信息。

[0095] 第六方面，本发明实施例提供了一种设备升级装置，可应用于终端设备，所述装置可包括：

[0096] 发送单元，用于向服务器发送待升级设备的升级请求，所述升级请求包括所述待升级设备的属性集合，所述属性集合包括所述终端设备的一个或多个属性信息以及所述待升级设备的一个或多个属性信息。

[0097] 在一种可能的实现方式中，所述升级请求还包括所述终端设备的身份信息和所述待升级设备的身份信息；其中，所述终端设备的身份信息和所述待升级设备的身份信息用于所述服务器分别进行验证；若均验证通过则根据所述终端设备的一个或多个属性信息以及所述待升级设备的一个或多个属性信息，确定所述待升级设备需要升级的一个或多个升级文件，所述目标升级包包括所述一个或多个升级文件。

[0098] 在一种可能的实现方式中，所述装置还包括：获取单元，用于获取所述终端设备的一个或多个属性信息以及所述待升级设备的一个或多个属性信息。

[0099] 第七方面，本发明实施例提供了一种服务器，可包括：处理器和存储器；其中，所述存储器用于存储程序代码，所述处理器用于调用所述存储器存储的程序代码执行如下步骤：

[0100] 根据待升级设备的属性集合生成针对所述待升级设备的访问策略；

[0101] 根据所述访问策略对目标升级包进行加密，生成目标升级包密文；

[0102] 将所述目标升级包密文发送至所述待升级设备，所述目标升级包密文用于所述待升级设备根据所述属性集合对应的一个或多个属性密钥进行解密，以获得所述目标升级

包。

[0103] 在一种可能的实现方式中,所述处理器还用于:获取所述待升级设备的升级请求,所述升级请求包括所述待升级设备的属性集合。

[0104] 在一种可能的实现方式中,所述处理器,具体用于:接收所述待升级设备发送的所述升级请求,所述属性集合包括所述待升级设备的一个或多个属性信息。

[0105] 在一种可能的实现方式中,所述属性集合包括所述待升级设备的一个或多个属性信息;所述处理器,具体用于:

[0106] 根据所述待升级设备的一个或多个属性信息,确定所述待升级设备需要升级的一个或多个升级文件,所述目标升级包包括所述一个或多个升级文件;

[0107] 确定所述一个或多个升级文件对应的升级条件,并基于所述升级条件生成所述访问策略。

[0108] 在一种可能的实现方式中,所述处理器,具体用于:

[0109] 接收终端设备发送的所述待升级设备的升级请求,所述属性集合包括所述终端设备的一个或多个属性信息以及所述待升级设备的一个或多个属性信息。

[0110] 在一种可能的实现方式中,所述处理器,具体用于:

[0111] 根据所述终端设备的一个或多个属性信息以及所述待升级设备的一个或多个属性信息,确定所述待升级设备需要升级的一个或多个升级文件,所述目标升级包包括所述一个或多个升级文件;

[0112] 确定所述一个或多个升级文件对应的升级条件,并基于所述升级条件生成所述访问策略。

[0113] 在一种可能的实现方式中,其特征在于,所述属性集合包括一个或多个属性信息;所述处理器还用于:

[0114] 生成公钥和主密钥,所述主密钥为所述公钥对应的私钥;

[0115] 根据所述主密钥以及所述一个或多个属性信息,生成所述属性集合对应的一个或多个属性密钥;

[0116] 将所述一个或多个属性密钥发送至所述待升级设备进行预存储;其中,所述一个或多个属性密钥用于所述待升级设备对所述目标升级包密文进行解密以获得所述目标升级包。

[0117] 在一种可能的实现方式中,所述处理器还用于:

[0118] 生成公钥和主密钥,所述主密钥为所述公钥对应的私钥;

[0119] 将所述主密钥发送至所述待升级设备上进行预存储,所述主密钥用于所述待升级设备生成所述属性集合对应的一个或多个属性密钥,其中,所述一个或多个属性密钥用于所述待升级设备对所述目标升级包密文进行解密以获得所述目标升级包。

[0120] 在一种可能的实现方式中,所述属性集合包括一个或多个属性信息;所述目标升级包包括所述属性集合中至少一个属性信息对应的更新后的属性密钥。

[0121] 在一种可能的实现方式中,所述属性集合包括一个或多个属性信息;其中,至少一个所述属性信息相同的不同待升级设备对应相同的所述公钥和对应的主密钥。

[0122] 在一种可能的实现方式中,所述待升级设备为智能车辆;所述属性集合包括车辆身份码、引擎号、车牌号码、车型流水号、车辆部件的硬件版本号和车辆部件的软件版本号

中的一种或者多种属性信息。

[0123] 在一种可能的实现方式中，所述终端设备为智能手机；所述属性集合包括手机号、手机识别码和手机的软件版本信息中的一种或者多种属性信息。

[0124] 在一种可能的实现方式中，所述处理器具体用于：根据所述属性集合确定所述目标升级包；所述服务器确定所述目标升级包对应的升级条件，并将所述升级条件组合后转换为所述访问策略。

[0125] 第八方面，本发明实施例提供了一种待升级设备，可包括：处理器和存储器；其中，所述存储器用于存储程序代码，所述处理器用于调用所述存储器存储的程序代码执行如下步骤：

[0126] 接收服务器发送的目标升级包密文，所述目标升级包密文为所述服务器根据访问策略对目标升级包进行加密生成的，所述访问策略为所述服务器根据所述待升级设备的属性集合生成的；获取所述属性集合对应的一个或多个属性密钥；根据所述一个或多个属性密钥对所述目标升级包密文进行解密，获得目标升级包。

[0127] 在一种可能的实现方式中，所述属性集合包括一个或多个属性信息；所述处理器，具体用于：接收所述服务器发送的一个或多个属性密钥，并进行预存储；所述属性密钥为所述服务器生成公钥和主密钥后，根据所述主密钥以及所述一个或多个属性信息，生成的一个或多个属性密钥；所述主密钥为所述公钥对应的私钥。

[0128] 在一种可能的实现方式中，所述属性集合包括一个或多个属性信息；所述处理器，具体用于：接收所述服务器发送的主密钥并进行预存储，所述主密钥为所述服务器生成的；所述待升级设备根据所述主密钥以及所述一个或多个属性信息，生成一个或多个属性密钥。

[0129] 在一种可能的实现方式中，所述升级请求还包括所述待升级设备的身份信息；其中，所述身份信息用于所述服务器进行验证，若验证通过则根据所述待升级设备的一个或多个属性信息，确定所述待升级设备需要升级的一个或多个升级文件，所述目标升级包包括所述一个或多个升级文件。

[0130] 在一种可能的实现方式中，所述升级请求经过所述公钥的加密；其中，加密后的所述升级请求用于所述服务器根据所述公钥对应的私钥对所述升级请求进行解密。

[0131] 在一种可能的实现方式中，所述属性集合包括一个或多个属性信息；所述目标升级包包括所述属性集合中至少一个属性信息对应的更新后的属性密钥。

[0132] 在一种可能的实现方式中，所述属性集合包括一个或多个属性信息；其中，至少一个所述属性信息相同的不同待升级设备对应相同的所述公钥和对应的主密钥。

[0133] 在一种可能的实现方式中，所述待升级设备为智能车辆；所述属性集合包括车辆身份码、引擎号、车牌号码、车型流水号、车辆部件的硬件版本号和车辆部件的软件版本号中的一种或者多种属性信息。

[0134] 第九方面，本发明实施例提供了一种终端设备，可包括：处理器和存储器；其中，所述存储器用于存储程序代码，所述处理器用于调用所述存储器存储的程序代码执行如下步骤：

[0135] 向服务器发送待升级设备的升级请求，所述升级请求包括所述待升级设备的属性集合，所述属性集合包括所述终端设备的一个或多个属性信息以及所述待升级设备的一个

或多个属性信息。

[0136] 在一种可能的实现方式中，所述升级请求还包括所述终端设备的身份信息和所述待升级设备的身份信息；其中，所述终端设备的身份信息和所述待升级设备的身份信息用于所述服务器分别进行验证；若均验证通过则根据所述终端设备的一个或多个属性信息以及所述待升级设备的一个或多个属性信息，确定所述待升级设备需要升级的一个或多个升级文件，所述目标升级包包括所述一个或多个升级文件。

[0137] 在一种可能的实现方式中，所述处理器还用于：获取所述终端设备的一个或多个属性信息以及所述待升级设备的一个或多个属性信息。

[0138] 第十方面，本申请提供一种设备升级装置，该设备升级装置具有实现上述第一方面、第二方面或第三方面提供的任意一种设备升级方法的功能。该功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。该硬件或软件包括一个或多个与上述功能相对应的模块。

[0139] 第十一方面，本申请提供一种服务器，该服务器中包括处理器，处理器被配置为支持该服务器执行第一方面提供的任意一种设备升级方法中相应的功能。该服务器还可以包括存储器，存储器用于与处理器耦合，其保存该服务器必要的程序指令和数据。该服务器还可以包括通信接口，用于该服务器与其他设备或通信网络通信。

[0140] 第十二方面，本申请提供一种待升级设备，该待升级设备中包括处理器，处理器被配置为支持该待升级设备执行第二方面提供的任意一种设备升级方法中相应的功能。该待升级设备还可以包括存储器，存储器用于与处理器耦合，其保存该待升级设备必要的程序指令和数据。该待升级设备还可以包括通信接口，用于该待升级设备与其他设备或通信网络通信。

[0141] 第十三方面，本申请提供一种终端设备，该终端设备中包括处理器，处理器被配置为支持该终端设备执行第三方面提供的任意一种设备升级方法中相应的功能。该终端设备还可以包括存储器，存储器用于与处理器耦合，其保存该终端设备必要的程序指令和数据。该终端设备还可以包括通信接口，用于该终端设备与其他设备或通信网络通信。

[0142] 第十四方面，本申请提供一种计算机存储介质，用于储存为上述第一方面、第二方面或第三方面提供的服务器、待升级设备或终端设备所用的计算机软件指令，其包含用于执行上述方面所设计的程序。

[0143] 第十五方面，本发明实施例提供了一种计算机程序，该计算机程序包括指令，当该计算机程序被执行时，使得服务器、待升级设备或终端设备可以执行上述第一方面、第二方面或第三方面中任意一项的设备升级方法中的流程。

[0144] 第十六方面，本申请提供了一种芯片系统，该芯片系统包括处理器，用于支持服务器、待升级设备或终端设备实现上述第一方面、第二方面或第三方面中所涉及的功能。在一种可能的设计中，所述芯片系统还包括存储器，所述存储器，用于保存服务器、待升级设备或终端设备必要的程序指令和数据。该芯片系统，可以由芯片构成，也可以包含芯片和其他分立器件。

[0145] 以上各方面中，进一步，可选的，上述各方面中所提到的属性集合可以包括待升级设备的属性信息和待升级设备中一个或多个单元模块的属性信息；其中，可选的单元模块的属性信息可以包括有单元模块的软件版本信息。

[0146] 此外,访问策略可以包括所述待升级设备的属性信息和服务器所确定的所述待升级设备的目标升级单元模块的软件版本信息。

[0147] 其中待升级设备中的单元模块可以为待升级设备中需要进行升级的模块,例如可以为车载控制设备;具体可以包括车载信息服务单元(Telematics box,TBox)和车载主控制器(Primary Electronic Control Unit,ECU),进一步还可以包括人机界面(Human Machine Interface,HMI)、电池管理系统(Battery Manage System,BMS)、车载辅助ECU1(Secondary ECU1)、车载辅助ECU2(Secondary ECU2)等,可选的,还可以包括车载自诊断系统II(the Second On-Board Diagnostics,OBDII)、高级驾驶辅助系统主控制器(Advanced Driving Assistant System Main Controller,ADAS Main Controller)、车辆控制器单元(Vehicle Controller Unit,VCU)、车身控制器(Body Controller)等以上车内部件中的一个或多个。

附图说明

[0148] 图1为本发明实施例提供的一种基于物联网的智能家居升级系统的架构图;

[0149] 图2是本发明实施例提供的一种车载设备升级应用场景的示意图;

[0150] 图3是本发明实施例提供的另一种车载设备升级应用场景的示意图;

[0151] 图4是本发明实施例提供的一种设备升级系统架构示意图;

[0152] 图5为本发明实施例提供的另一种设备升级系统架构示意图;

[0153] 图6是本发明实施例提供的一种Primary ECU的结构示意图;

[0154] 图7是本发明实施例提供的一种待升级车载单元的结构示意图

[0155] 图8是本发明实施例提供的一种终端设备的结构示意图;

[0156] 图9是本发明实施例提供的一种设备升级方法的流程示意图;

[0157] 图10是本发明实施例提供的另一种设备升级方法的流程示意图;

[0158] 图11是本发明实施例提供的又一种设备升级方法的流程示意图;

[0159] 图12是本发明实施例提供的一种智能车辆的升级场景示意图;

[0160] 图13是本发明实施例提供的另一种智能车辆的升级场景示意图;

[0161] 图14是本发明实施例提供的又一种智能车辆的升级场景示意图;

[0162] 图15是本发明实施例提供的又一种智能车辆的升级场景示意图;

[0163] 图16是本发明实施例提供的又一种智能车辆的升级场景示意图;

[0164] 图17是本发明实施例提供的又一种智能车辆的升级场景示意图;

[0165] 图18是本发明实施例提供的一种设备升级装置的结构示意图;

[0166] 图19是本发明实施例提供的又一种设备升级装置的结构示意图;

[0167] 图20是本发明实施例提供的一种待升级装置的结构示意图;

[0168] 图21是本发明实施例提供的另一种设备升级装置的结构示意图;

[0169] 图22是本发明实施例提供的一种设备的结构示意图。

具体实施方式

[0170] 下面将结合本发明实施例中的附图,对本发明实施例进行描述。

[0171] 本申请的说明书和权利要求书及所述附图中的术语“第一”、“第二”、“第三”和“第

四”等是用于区别不同对象，而不是用于描述特定顺序。此外，术语“包括”和“具有”以及它们任何变形，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、产品或设备没有限定于已列出的步骤或单元，而是可选地还包括没有列出的步骤或单元，或可选地还包括对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0172] 在本文中提及“实施例”意味着，结合实施例描述的特定特征、结构或特性可以包含在本申请的至少一个实施例中。在说明书中的各个位置出现该短语并不一定均是指相同的实施例，也不是与其它实施例互斥的独立的或备选的实施例。本领域技术人员显式地和隐式地理解的是，本文所描述的实施例可以与其它实施例相结合。

[0173] 在本说明书中使用的术语“部件”、“模块”、“系统”等用于表示计算机相关的实体、硬件、固件、硬件和软件的组合、软件、或执行中的软件。例如，部件可以是但不限于，在处理器上运行的进程、处理器、对象、可执行文件、执行线程、程序和/或计算机。通过图示，在计算设备上运行的应用和计算设备都可以是部件。一个或多个部件可驻留在进程和/或执行线程中，部件可位于一个计算机上和/或分布在2个或更多个计算机之间。此外，这些部件可从在上面存储有各种数据结构的各种计算机可读介质执行。部件可例如根据具有一个或多个数据分组(例如来自与本地系统、分布式系统和/或网络间的另一部件交互的二个部件的数据，例如通过信号与其它系统交互的互联网)的信号通过本地和/或远程进程来通信。

[0174] 首先，对本申请中的部分用语进行解释说明，以便于本领域技术人员理解。

[0175] (1)空中下载技术(Over the Air Technology，OTA)是通过移动通信的空中接口进行远程固件或软件远程升级的技术。

[0176] (2)车载信息服务(Telematics)是远距离通信的电信(Telecommunications)与信息科学(Informatics)的合成词，按字面可定义为通过内置在汽车、航空、船舶、火车等运输工具上的计算机系统、无线通信技术、卫星导航装置、交换文字、语音等信息的互联网技术而提供信息的服务系统。简单的说就通过无线网络将车辆接入互联网，为车主提供驾驶、生活所必需的各种信息。Telematics box，简称车载TBox，TBox是车辆对外部的主要通信部件，车辆升级时，可以通过Telematics box与服务器交互获得升级包。

[0177] (3)电子控制单元(Electronic Control Unit，ECU)，从用途上讲则是汽车专用微机控制器。它和普通的电脑一样，由微处理器(CPU)、存储器(ROM、RAM)、输入/输出接口(I/O)、模数转换器(A/D)以及整形、驱动等大规模集成电路组成。

[0178] (4)车辆控制单元(Vehicle Control Unit，VCU)，也可以称之为电动汽车整车控制器VCU是电动汽车动力系统的总成控制器，负责协调发动机、驱动电机、变速箱、动力电池等各部件的工作，具有提高车辆的动力性能、安全性能和经济性等作用。是电动汽车整车控制系统的核心部件，是用来控制电动车电机的启动、运行、进退、速度、停止以及电动车的其它电子器件的核心控制器件。VCU作为纯电动汽车控制系统核心的部件，其承担了数据交换、安全管理、驾驶员意图解释、能量流管理的任务。VCU采集电机控制系统信号、加速踏板信号、制动踏板信号及其他部件信号，根据驾驶员的驾驶意图综合分析并作出响应判断后，监控下层的各部件控制器的动作，对汽车的正常行驶、电池能量的制动回馈、网络管理、故障诊断与处理、车辆状态监控等功能起着关键作用。

[0179] (5)控制器局域网络(Controller Area Network，CAN)总线，是国际上应用最广泛的现场总线之一。其所具有的高可靠性和良好的错误检测能力受到重视，被广泛应用于汽

车计算机控制系统和环境温度恶劣、电磁辐射强和振动大的工业环境。CAN总线是一种应用广泛的现场总线，在工业测控和工业自动化等领域有很大的应用前景。CAN属于总线式串行通信网络，在数据通信方面具有可靠、实时和灵活的优点。

[0180] (6)消息验证码(Message Authentication Code,MAC)是通信实体双方使用的一种验证机制，是保证消息数据完整性的一种工具。MAC类似于摘要算法，但是它在计算的时候还要采用一个密钥，因此MAC是基于密钥和消息摘要所获得的一个值，实际上是对消息本身产生一个冗余的信息，可用于数据源认证和完整性校验。

[0181] (7)公钥密码(非对称密码)，公钥密码又称为非对称密码，非对称密钥算法是指一个加密算法的加密密钥和解密密钥是不一样的，或者说不能由其中一个密钥推导出另一个密钥。拥有公钥密码的用户分别拥有加密密钥和解密密钥，通过加密密钥不能得到解密密钥。并且加密密钥是公开的。公钥密码就是基于这一原理而设计的，将辅助信息(陷门信息)作为秘密密钥。这类密码的安全强度取决于它所依据的问题的计算复杂度。现在常见的公钥密码有RSA公钥密码、ElGamal公钥密码、椭圆曲线密码。

[0182] (8)对称密码，对称密钥加密又叫专用密钥加密，即发送和接收数据的双方必使用相同的密钥对明文进行加密和解密运算。即加密密钥能够从解密密钥中推算出来，反过来也成立。在大多数对称算法中，加密解密密钥是相同的。这些算法也叫秘密密钥算法或单密钥算法，它要求发送者和接收者在安全通信之前，商定一个密钥。对称算法的安全性依赖于密钥，泄漏密钥就意味着任何人都能对消息进行加密解密。只要通信需要保密，密钥就必须保密。

[0183] 从上述对对称密钥算法和非对称密钥算法的描述中可看出，对称密钥加解密使用的同一个密钥，或者能从加密密钥很容易推出解密密钥;对称密钥算法具有加密处理简单，加解密速度快，密钥较短，发展历史悠久等特点，非对称密钥算法具有加解密速度慢的特点，密钥尺寸大，发展历史较短等特点。

[0184] (9)密码散列函数(Cryptographic hash function)，又译为加密散列函数，是散列函数的一种。它被认为是一种单向函数，也就是说极其难以由散列函数输出的结果，回推输入的数据是什么。这样的单向函数被称为“现代密码学的驮马”。这种散列函数的输入数据，通常被称为消息(message)，而它的输出结果，经常被称为消息摘要(message digest)或摘要(digest)。在信息安全中，有许多重要的应用，都使用了密码散列函数来实现，例如数字签名，消息认证码。

[0185] (10)终端设备，可以为用户设备(User Equipment,UE)、无线局域网(Wireless Local Area Networks,WLAN)中的站点(STAION,ST)、蜂窝电话、无线本地环路(Wireless Local Loop,WLL)站、个人数字处理(Personal Digital Assistant,PDA)设备、具有无线通信功能的手持设备、计算设备或连接到无线调制解调器的其它处理设备、可穿戴设备等。

[0186] (11)原始设备制造商(Original Equipment Manufacturer,OEM)是受托厂商按来样厂商之需求与授权，按照厂家特定的条件而生产，所有的设计图等都完全依照来样厂商的设计来进行制造加工。本申请中的OEM可以为待升级设备的原始制造或生产商，例如，待升级设备为智能车辆，则OEM指车辆制造商。

[0187] (12)车载自动诊断系统(On Board Diagnostics,OBD)，为汽车故障诊断而延伸出来的一种检测系统。OBD能在汽车运行过程中实时监测发动机电控系统及车辆的其它功能

模块的工作状况，如有发现工况异常，则根据特定的算法判断出具体的故障，并以诊断故障代码(Diagnostic Trouble Codes，DTC)的形式存储在系统内的存储器上。系统自诊断后得到的有用信息可以为车辆的维修和保养提供帮助，维修人员可以根据汽车原厂专用仪器读取故障码，从而可以对故障进行快速定位，以便于对车辆的修理，减少人工诊断的时间。

[0188] 首先，为了便于理解本发明实施例，进一步分析并提出本申请所具体要解决的技术问题。在现有技术中，关于设备的安全远程升级(以车辆的远程升级为例)技术，包括多种技术方案，以下示例性的列举如下常用的四种方案。其中，

[0189] 方案一：车辆的升级包开发完成后会包含发行单位的签名(例如用预先协商好的私钥进行签名)；车辆通过车内电子控制单元ECU(也可称之为车内控制器)获取该升级包之后，使用预先协商好的公钥进行验证。该验证流程验证了升级包的源可信，即可以验证该升级包是由合法的发行单位发布的。

[0190] 该方案一的缺点：只是验证了升级包的源可信，并未包含对车辆的身份与状态进行验证(可能导致不符合条件的车辆下载了不合适的升级包，导致升级失败)，也未包含远程升级包传输时的机密性保护。

[0191] 方案二：对于车辆升级包通过白盒加密达到机密性、使用哈希算法保证升级包的完整性、使用签名系统保障源可信。

[0192] 该方案二的缺点：该方案保障了升级包的机密性、完整性与源可信，但没有对车辆身份与状态进行验证。

[0193] 方案三：提出在车辆进行升级前的前提条件检测，包含车辆身份与车辆状态。例如，提出进行软件版本的比较，若车载控制器上的版本较旧，则可进行升级包的下载。又例如，软件更新管理提出较多的前提条件检测，并且下载升级包与安装升级包所需要的前提条件可以不同等。

[0194] 该方案三的缺点：并没有提供具有强制力的条件检测方式，即检测方式不具有高度强制性，容易被绕过。

[0195] 方案四：使用密码工具提供高度强制性的前提条件检测。例如，通过加密算法提供升级包的机密性、通过签名提供源可信验证、计算升级包的哈希值提供完整性校验。

[0196] 该方案四的缺点：通用性的密码算法可以检测的条件种类较少，例如使用公钥加密算法时，有公钥密钥对，检测的条件为是否具有该密钥，无法解决多种升级条件的组合状态。

[0197] 综上，上述四种方案中，均未对车辆的身份和状态进行检测；或者是即使有相关检测，但不是强制性检测，也很容易被绕过；亦或者是即使提供了强制性检测，但是由于是基于通用性的密码算法的检测方式，可提供的检测的条件种类少、不灵活，无法满足车辆升级过程中的实际需求。

[0198] 因此，为了解决当前安全远程升级技术中上述不满足实际业务需求的问题，本申请实际要解决的技术问题包括如下方面：当车辆进行安全远程升级的时候，如何实现一个具有强制力、且可满足多种前提条件检测的升级方案；进一步地，特别是在保障升级包机密性与完整性的前提下，要能够提供具有强制力的车辆身份与状态的前提条件检测。

[0199] 为了便于理解本发明实施例，以下示例性列举本申请中设备升级方法所应用的设备升级系统的场景，可以包括如下三个场景。

[0200] 场景一，通过服务器对智能家居进行升级管理：

[0201] 请参阅图1，图1为本发明实施例提供的一种基于物联网的智能家居升级系统的架构图，该应用场景中包括服务器(图1中以物联网服务器为例)、通信设备(图1中小区网关为例)、控制设备(图1中以家庭网关为例)和多个待升级设备(图1中以智能窗帘、智能窗户、智能电视和智能空调为例)，其中，智能窗帘、智能窗户、智能电视和智能空调和家庭网关之间可以通过蓝牙、NFC、Wi-Fi或移动网络等无线通信方式进行通信，家庭网关则通过互联网接入小区网关和物联网服务器。当多个待升级的智能家居设备中的任意一个智能家居设备有升级需求时，可通过在升级请求中携带自身的属性集合向物联网服务器发起请求。例如，智能空调将携带有自身的型号、固件版本、软件版本的升级请求通过家庭网关以及小区网关发送至物联网服务器之后，物联网服务器则根据该智能空调的型号、固件版本、软件版本等，生成与该空调匹配的访问策略，再基于属性加密算法，根据该访问策略与约定的公钥对升级包进行加密得到升级包密文，再通过小区网关、家庭网关发送至该空调进行升级。由于该升级包密文是基于智能空调的属性集合进行的属性加密处理的。因此，只有拥有该属性集合对应的属性密钥的智能空调才可以正确解密升级包。并且，进一步地，该升级包可以是根据属性集合的特征进行匹配的，因此可以确保该智能空调可以精确下载符合其需求的升级包并升级。

[0202] 场景二，通过服务器对智能车辆进行一对多升级管理，且待升级设备的升级请求由待升级设备自身向服务器发起：

[0203] 请参见图2，图2是本发明实施例提供的一种车载设备升级应用场景的示意图。该应用场景中包括服务器(例如升级服务器)和多个待升级设备(例如智能车辆)，升级服务器和智能车辆之间可以通过Wi-Fi和移动网络等进行通信。其中，升级服务器可以对多个合法注册的智能车辆进行升级管理，完成关于升级包的提供、下载更新等相关服务。当多个待升级的智能车辆中的任意一个智能车辆有升级需求时，可通过在升级请求中携带自身的属性集合向升级服务器发起请求。例如，智能车辆将携带有自身的车辆身份码、引擎号、车型流水号、车辆部件的硬件版本号和软件版本号的升级请求发送至服务器之后，服务器则根据该智能车辆的车辆身份码、引擎号、车型流水号、车辆部件的硬件版本号和软件版本号等，生成与该智能车辆匹配的访问策略，再基于属性加密算法，根据该访问策略与约定的公钥对升级包进行加密得到升级包密文，再发送至该智能车辆进行升级。由于该升级包密文是基于该智能车辆的属性集合进行的属性加密处理的。因此，只有拥有该属性集合对应的属性密钥的智能车辆才可以正确解密升级包。并且，进一步地，该升级包可以是根据属性集合的特征进行匹配的，因此可以确保该智能车辆可以精确下载符合其需求的升级包并升级。

[0204] 而智能车辆除了在向服务器发起升级请求时携带自身的属性集合以外，还可以根据例如升级服务器上新增一个逻辑功能实体，该逻辑功能实体用于存储第一密钥以及执行第一安全处理，对车辆内部的升级文件的存储或传输进行安全强化，保证车辆的升级安全。

[0205] 场景三，通过终端设备对智能车辆进行一对一管理，待升级设备的升级请求由匹配的终端设备向服务器发起：

[0206] 请参见图3，图3是本发明实施例提供的另一种车载设备升级应用场景的示意图，该应用场景中包括终端设备(例如智能手机)、待升级设备(例如智能车辆)和服务器(例如升级服务器)，智能手机和智能车辆之间可以通过蓝牙、NFC、Wi-Fi和移动网络等进行通信，

升级服务器和终端设备之间可以通过Wi-Fi和移动网络等进行通信。其中，智能手机和智能车辆之间可以建立一对一的匹配关系，例如通过智能车辆的车牌或唯一标识与终端设备的身份识别卡或者合法账号进行匹配，匹配完成后，智能手机和智能车辆之间便可以合作执行本申请中发起本申请中的升级请求的流程，从而实现用户通过智能手机对驾驶的车辆进行升级管理，保证车辆的升级安全。在另一种可能的实现方式中，智能手机和智能车辆之间可以建立一对多的匹配关系，例如一个用户可以同时拥有并管理多个车辆，也可以是一个用户对多个不同用户的车辆进行管理。比如4S店的员工，通过专用的终端设备对店内的同一个型号的所有车辆进行系统升级，或者某个用户通过自己的终端设备对附近的与其建立了匹配关系的智能车辆进行升级包的提供或管理等，以实现一个设备同时管理多个智能车辆的应用场景，节省时间、节省网络传输带宽以及存储资源，并且保证车辆的升级安全。可以理解的是，在一对多的管理中，需要该终端设备中预先存储有该多个车辆的相关信息，或者是该多个车辆向终端设备证明其合法性以及与该终端设备之间存在服务关系。在该场景三中的两种实现方式中，例如，智能手机将携带有属性集合如智能手机的手机号、识别码，智能车辆的身份码、引擎号、车型流水号、车辆部件的硬件版本号和软件版本号的升级请求发送至服务器之后，服务器则根据上述属性集合生成与该智能手机和智能车辆匹配的访问策略，再基于属性加密算法，根据该访问策略与约定的公钥对升级包进行加密得到升级包密文，再发送至智能手机或者智能车辆进行升级。由于该升级包密文是基于该智能手机和智能车辆的属性集合进行的属性加密处理的。因此，只有拥有该属性集合对应的属性密钥的智能手机或智能车辆才可以正确解密升级包，也即是通过合法智能手机协助其匹配的智能车辆进行设备升级。并且，进一步地，该升级包可以是根据属性集合的特征进行匹配的，因此可以确保该智能车辆可以精确下载符合其需求的升级包并升级。

[0207] 可以理解的是，图1、图2和图3中的应用场景的只是本发明实施例中的几种示例性的实施方式，本发明实施例中的应用场景包括但不仅限于以上应用场景。本申请中的设备升级方法还可以应用于，例如，服务器管理不同型号的智能手机的批量系统升级、智能手机管理智能穿戴设备进行设备升级、智能医疗服务器管理智能医疗器械进行设备升级、工厂管控服务器管理智能机器的设备升级等场景，其它场景及举例将不再一一列举和赘述。

[0208] 结合上述应用场景，下面先对本发明实施例所基于的其中一种设备升级系统架构进行描述。请参见图4，图4是本发明实施例提供的一种设备升级系统架构示意图(简称为架构一)，对应上述场景二。本申请提供的设备升级方法可以应用于该系统架构。该系统架构中包含了升级服务器、智能车辆。其中，智能车辆包括车载控制设备和一个或多个待升级车载单元，车载控制设备可以包括车载信息服务单元(Telematics box，TBox)和车载主控制器(Primary Electronic Control Unit，ECU)，用于管理和辅助多个待升级车载单元的升级过程。一个或多个待升级车载单元可包括如图4中所示的人机界面(Human Machine Interface，HMI)、电池管理系统(Battery Manage System，BMS)、车载辅助ECU1(Secondary ECU1)、车载辅助ECU2(Secondary ECU2)等，可选的，还可以包括图4中未示出的车载自诊断系统II(the Second On-Board Diagnostics，OBDII)、高级驾驶辅助系统主控制器(Advanced Driving Assistant System Main Controller，ADAS Main Controller)、车辆控制器单元(Vehicle Controller Unit，VCU)、车身控制器(Body Controller)等车内部件。可选的，上述车内各个部件可由各种车内总线相连接。在上述系统架构下，智能车辆远

程升级可以包括以下基本过程:升级包发布,升级包获取,升级包传输,升级与确认等。其中,

[0209] 升级服务器,可以用于从开发者处获取未经过加密的车载升级包,该车载升级包可包括本申请中的目标升级包,可用于对应的待升级车载单元进行升级。可选的,升级服务器还用于生成升级服务器和智能车辆之间所使用的密钥,包括公钥、主密钥和多个属性密钥等。

[0210] 车载控制设备中的TBox,负责对外通信,例如与终端设备、与升级服务器之间的通信等。在车辆进行远程升级时,可以与服务器交互获得密钥、升级包,以及将密钥、升级包传输给车载主控制器Primary ECU等。

[0211] 车载控制设备中的车载主控制器Primary ECU,负责与车载内的多个待升级车载单元进行通信,其主要功能是管理和辅助待升级车载单元的升级过程。具体来说,Primary ECU可以具有如下功能:密钥获取及管理,例如,经由TBox从服务器处获取公钥、属性密钥(可选的,也可以获取主密钥,并生成属性密钥)等,并进行存储。升级包的获取与解密,例如,经由TBox从服务器处获取目标升级包密文,并根据其所存储的属性密钥对接收到的目标升级包密文进行解密,最终将解密后的目标升级包发送给对应的待升级车载单元进行升级。可选的,Primary ECU是逻辑实体,物理上可以部署任何功能强大的单元或模块上,例如TBox、Gateway、VCU上等。

[0212] 如图5所示,图5为本发明实施例提供的另一种设备升级系统架构示意图(简称为架构二),对应上述场景三。该系统架构中,还包括了终端设备,其中,

[0213] 终端设备,可与升级服务器或者智能车辆之间进行通信,可负责完成升级请求的发送,以及根据自身的存储能力和计算能力参与到公钥、属性密钥的存储,或主密钥的存储、属性密钥的计算,以及目标升级包密文的获取和安全处理等过程,以实现计算扩展和安全强化。进一步地,终端设备还用于从资源扩展以及升级控制等角度,参与到智能车辆的安全升级过程中来。例如,根据自身的存储能力协助储存属性集合(如各个待升级车载单元软/固件信息,当前版本、大小、开发者等),备份文件(如待升级车载单元软/固回滚版)与车机系统状况,以完成储存扩展。另外,终端设备还可以作为软/固件升级的远程控制console端(让用户选择是否升级、升级时间、单点或群组升级模式等),以实现用户远程控制升级。

[0214] 基于上述对本发明实施例提供的架构一和架构二的描述,进一步对上述架构中所涉及的模块或设备的结构进行描述。其中,

[0215] Primary ECU的结构可以如图6所示,图6是本发明实施例提供的一种Primary ECU的结构示意图。其中,Primary ECU可以包括处理器CPU以及相关的易失性存储器RAM和非易时性存储器ROM;用于存放密钥的安全存储,如从服务器处获取的公钥和一个或多个属性密钥,或者主密钥等;用于存储远程升级OTA管理程序的存储器,该OTA管理程序用于实现对升级过程的管理;用于通过CAN bus或其他车内网络与其他车载设备通信的网络接口。可以理解的是,如果Primary ECU实现在TBox上,它还需要有与外部网络通信的网络接口。即Primary ECU应有较强的计算能力和较多资源辅助车载设备完成远程升级,并被其他车载设备信任。从逻辑架构上划分,Primary ECU把该架构分为车外通信部分和车内通信部分。车内部分的各设备无需进行公钥密码操作而只需进行对称密码操作;如涉及公钥密钥操作,则代理给Primary ECU,以减少车载内待升级单元的计算量和计算复杂度。

[0216] 智能车辆中任意一个待升级车载单元的构成可以如图7所示，图7是本发明实施例提供的一种待升级车载单元的结构示意图。待升级车载单元可以包括微型控制器(Micro controlller)，CAN控制器(CAN controller)和收发器(Transceiver)。其中，待升级车载单元通过收发器Transceiver与车内网络如CAN bus通信，CAN controller则用于实现CAN协议，微型控制器则用于实现待升级以及升级后的相关的计算处理。结合上述结构示意图，在本申请中，待升级车载单元基于车内网络如CAN bus，通过收发器(Transceiver)接收车载控制设备发送的解密后的目标升级包，并通过微型控制器(Micro Controlller)进行安全升级。

[0217] 终端设备的构成可以参考图8，图8是本发明实施例提供的一种终端设备的结构示意图。该终端设备可包括处理器CPU以及相关的易失性存储器RAM和非易时性存储器ROM；其中，ROM可用于存储OTA管理程序、属性信息、属性密钥等；该OTA管理程序可用于实现对设备升级过程的管理；无线通信模块可用于与其它设备(包括智能车辆以及升级服务器等)进行通信；显示及输入外设用于为用户提供车载升级交互控制界面的显示及输入，如音频输入输出模块、按键或触摸输入模块以及显示器等。

[0218] 可选的，上述架构一或架构二中还可以包括开发者，开发者在固件/软件发布的开发和测试升级程序后，将车载升级包交付给升级服务器，该交付的车载升级包需要经过数字签名。可选的，在经过数字签名之前，还可以对该车载升级包经过加密。若经过加密则上述系统架构还可以包括密钥服务器，用于提供开发者和升级服务器之间传输所使用的密钥。可以理解的是，图4和图5中的设备升级系统架构只是本发明实施例中的两种示例性的实施方式，本发明实施例中的设备升级系统架构包括但不仅限于以上设备升级系统架构。

[0219] 下面结合上述应用场景、系统架构以及本申请中提供的设备升级方法，以待升级设备为智能车辆/车载系统为例，对本申请中提出的技术问题进行具体分析和解决。

[0220] 请参见图9，图9是本发明实施例提供的一种设备升级方法的流程示意图，该设备升级方法可应用于上述系统架构一或系统架构二，且适用于上述图1、图2或图3中的任意一种应用场景。下面将结合附图9从服务器与待升级设备的交互侧进行描述，该方法可以包括以下步骤S901-步骤S903。

[0221] 步骤S901：服务器根据待升级设备的属性集合生成针对所述待升级设备的访问策略。

[0222] 具体地，以下主要以智能车辆/车载系统升级的场景为例进行描述，即待升级设备可以为智能车辆/车载系统，服务器可以为原始设备制造商OEM(即车厂)的升级服务器。由于本发明实施例中，每个待升级设备都拥有一个反映自身身份和状态的属性集合(该属性集合为非空集合)，以及该属性集合对应的密钥集合。该属性集合可包括该待升级设备的一个或多个属性信息，该属性信息可以为用于表征该待升级设备的身份或者状态的信息，例如属性信息为车辆身份码、引擎号、车牌号码、车型流水号、车辆部件的硬件版本号和车辆部件的软件版本号中的一种或者多种。该属性集合用于后续服务器根据该属性集合进行升级包的处理，进而确保只有身份与状态均符合条件的待升级设备，才可以获得匹配的升级包。既避免了不满足条件的待升级设备非法获得升级包，也避免了不符合升级条件的待升级设备进行错误的下载或升级。相当于不同待升级设备或每一类待升级设备都可以有其个性化的特性及升级需求。在本发明实施例中，服务器需要根据待升级设备的属性集合生成

针对该待升级设备的访问策略(access control policy),也可称之为访问结构、访问控制策略等。也即是访问策略限定了获得目标升级包的前提条件,换句话说,访问策略定义了具备哪些属性信息的设备可以解密目标升级包,或者不具备哪些属性信息的设备无法解密目标升级包。可以理解为,该访问策略是针对目标升级包进行前提条件的设定,并且将该前提条件组合转换成访问策略,用于对目标升级包进行加密。例如,服务器根据属性集合生成针对待升级设备的访问策略具体包括:服务器根据属性集合确定目标升级包;服务器确定目标升级包对应的升级条件,并将升级条件组合后转换为访问策略。即服务器根据升级请求中的属性集合确定与该待升级设备匹配的目标升级包,并针对该目标升级包定义升级的前提条件,再将升级的前提条件经过组合转换后确定为访问策略,从而使得后续可以根据该访问策略对目标升级包进行加密,以实现对待升级设备的升级条件(例如身份、状态等)的强制力检测。

[0223] 例如,当待升级设备的属性集合包括智能车辆的身份码1234、车型流水号12345、引擎号1234567、TBox的软件版本号V1、人机界面HMI软件版本号V3、电池管理系统BMS软件版本V2”。服务器通过属性集合中的车辆的身份码1234确定该车辆为合法的智能车辆,然后基于车型流水号12345获取该型号智能车辆当前对应的最新软件版本,经过比较,发现该车型当前对应的最新版本为TBox的软件版本号V2、人机界面HMI软件版本号V3、电池管理系统BMS软件版本V2,因此确定该智能车辆需要更新的升级包为将TBox的软件版本从V1更新到V2。因此,服务器根据该属性集合生成的访问策略可以为“引擎号码为1234567并且TBox的软件版本号为V1”,也即是强制限定只有满足引擎号码为1234567且TBox的软件版本号为V1的智能车辆才能进行解密,或者,该访问策略也可以为“车型流水号12345并且TBox的软件版本号为V1”,也即是限定车型为12345类型且TBox的软件版本号为V1的一类智能车辆,均可以进行解密。总之,服务器根据待升级设备的属性集合生成的访问策略,可以是只针对该待升级设备的,也可以是针对包括该待升级设备在内的某一个类型的待升级设备。且其具体生成的访问策略的规则依据实际的升级场景以及升级规则不同而不同,本发明实施例对如何根据属性集合生成对应的访问策略不作具体限定。

[0224] 可选的,属性集合中可以包含静态属性信息或动态属性信息,静态属性信息包含智能车辆身份码、引擎编号、生产序号等随着时间不会变化的信息;动态属性信息包含智能车辆的部件的生产序号、部件的身份码、部件所使用的硬件版本、软件版本等随着时间可能会有变化的信息。例如,当如智能车辆需要进行电池管理系统BMS的升级时,则该属性集合可以为包括该智能车辆的静态属性信息:身份码、车型流水号、电池管理系统BMS的硬件版本号,以及动态属性信息:BMS的软件版本号。

[0225] 在一种可能的实现方式中,服务器在生成访问策略之前通过获取包括待升级设备的属性集合的升级请求,来确定上述待升级设备的属性集合。例如,升级请求可以为针对智能车辆/车载系统中的一个或多个待升级车载单元(例如人机界面HMI、电池管理系统BMS、电子控制单元等)的升级请求。即可以通过在待升级设备的升级请求中携带该待升级设备的属性集合(包含该设备的一个或多个属性信息)的方式,使得服务器获知该待升级设备的属性集合。可选的,也可以通过服务器预存储的待升级设备的属性集合或者通过其他途径获得的待升级设备的属性集合进行访问策略的生成。也即是该属性集合可以是待升级设备或者是其他设备发送给服务器的,也可以是服务器预先存储的(例如大数据存储、大数据分

析等),本发明实施例对此不作具体限定。

[0226] 在一种可能的实现方式中,属性集合包括一个或多个属性信息;服务器获取待升级设备的升级请求之前还包括:服务器生成公钥和主密钥,主密钥为公钥对应的私钥;服务器根据主密钥以及一个或多个属性信息,生成一个或多个属性密钥;服务器将一个或多个属性密钥发送至待升级设备进行预存储;其中,一个或多个属性密钥用于待升级设备对目标升级包密文进行解密以获得目标升级包。本发明实施例中,服务器在初始阶段需要生成针对该待升级设备后续安全升级过程中所要使用到的公钥、主密钥(与公钥对应的私钥)以及对应的属性密钥,并且将属性密钥发送给拥有对应属性信息的待升级设备,以保证后续的基于密文策略属性加密算法的设备安全升级过程。例如,原车厂OEM的服务器需要在前期预先生成本发明实施例所基于的属性加密算法中的相关密钥,以及将相关密钥分发给对应的待升级设备。即定义待升级设备的相关属性信息以及对应的属性密钥。具体地,车厂的服务器使用setup算法生成公钥pk_c与主密钥mr_c,该公钥pk_c与主密钥mr_c为一对公私钥对。再使用pk_c与mr_c生成待升级设备的各种不同属性信息对应的属性密钥ar_c;并且将属性密钥预置于相应的智能车辆内部。

[0227] 在一种可能的实现方式中,服务器还预先生成公钥和主密钥,主密钥为公钥对应的私钥;服务器将公钥和主密钥发送至待升级设备上进行预存储,该主密钥可用于待升级设备在待升级设备的本地,根据满足访问策略中升级条件的属性信息生成对应的属性密钥,进而获得对应的目标升级包。本方法实施例中,服务器将公钥和主密钥均发送给待升级设备,用于待升级设备在待升级设备的本地,根据满足访问策略中升级条件的属性信息生成对应的属性密钥,进而获得对应的目标升级包。可适用于待升级设备的属性信息变化大的情形,例如,智能车辆为共享车辆,其对应的用户信息或者账户信息等经常变动,导致经常需要不同的属性密钥才能为不同的用户提供设备升级服务等。

[0228] 可选的,上述升级请求经过所述公钥pk_c的加密;服务器在接收到待升级设备的升级请求后,还根据所述公钥对应的私钥即主密钥mr_c对升级请求进行解密。也即是服务器在将一个或多个属性密钥发送至待升级设备上进行预存储时,还将所述公钥发送至所述待升级设备上,以用于所述待升级设备进行升级请求的加密。本发明实施例中,升级请求本身还可以经过公钥的加密,从而使得服务器可以使用主密钥对升级请求进行解密,以保证升级请求传输的安全性;且可进一步基于解密后的升级请求,以确定该待升级设备的是否有可用的目标升级包,以确保升级的准确性。进一步地,服务器根据解密后的升级请求,核对车辆的身份与属性,判断当前是否有可用的目标升级包(若判断出当前没有可用升级包,也可以向待升级设备指示当前无需进行升级),该目标升级包可以是对于智能车辆内的一个或多个不同待升级车载单元的升级文件的组合。

[0229] 步骤S902:所述服务器基于属性加密算法,根据所述访问策略对目标升级包进行加密,生成目标升级包密文。

[0230] 具体地,服务器基于属性加密算法,输入目标升级包、以及步骤S901中的访问策略,可选的还输入服务器生成的公钥,最终输出该目标升级包的密文即目标升级包密文。待升级设备能够解密该目标升级包密文,当且仅当该待升级设备对应的属性信息(体现在是否拥有对应的属性密钥)满足在该目标升级包密文中部署的访问策略才行。其中,目标升级包可以为智能车辆中任意一个或多个待升级车载单元的系统升级文件、系统补丁或系统同

步信息等,用于为对应的待升级车载单元提供系统升级、维护或更新等服务。本发明实施例基于密文策略的属性加密算法(ciphertext policy attribute based encryption,CP-ABE),在公钥加密体制中引入访问策略,以此部署目标升级包的访问控制策略。与传统的公钥加密体制(如基于身份的加密IBE),本发明实施例不再将待升级设备的身份作为唯一识别信息,而是根据多个属性(即属性集合)来标识待升级设备,增强了描述性,实现了一个具有强制力、且可满足多种前提条件(即可基于升级请求中的属性集合灵活变化)检测的设备升级方案。在保障升级包机密性与完整性的前提下,能够提供具有强制力的待升级设备的身份与状态的前提条件检测。

[0231] 步骤S903:所述服务器将所述目标升级包密文发送至所述待升级设备,所述目标升级包密文用于所述待升级设备根据所述属性集合对应的一个或多个属性密钥进行解密,以获得所述目标升级包。

[0232] 具体地,服务器将目标升级包密文发送至待升级设备,待升级设备接收到该目标升级包密文后,根据其属性集合中与上述访问策略匹配的属性密钥,对目标升级包密文进行解密,以获得目标升级包的明文,并最终根据该目标升级包进行升级。也即是只有拥有符合访问策略中的前提条件的属性信息(也即拥有匹配的属性密钥)的待升级设备才能够解密获得目标升级包。在本发明实施例中,由于服务器和待升级设备之间预先协商好了相关的公钥、主密钥以及属性密钥,并将公钥和属性密钥分发给了具有对应属性信息的待升级设备。因此,经过上述步骤S901-步骤S903的流程后,不仅可以保证目标升级包来源的合法性、传输的机密性和完整性,并且可以实现具有强制力的设备身份与状态的前提条件检测的升级过程,即可满足多种前提条件检测的设备升级方案。本发明实施例应用在车载设备升级场景中时,可以保证车辆升级的安全性以及准确性。

[0233] 在一种可能的实现方式中,所述属性集合包括一个或多个属性信息;所述目标升级包包括所述属性集合中至少一个属性信息对应的更新后的属性密钥。本发明实施例中,由于属性密钥可能会存在更新或变更的情况,因此,服务器还可以通过在目标升级包中携带最新的属性密钥,使得满足属性信息条件的待升级设备可以根据最新的属性密钥进行升级包的解密,避免需要通过其他额外流程将更新后的属性密钥的发送给待升级设备。

[0234] 在一种可能的实现方式中,所述属性集合包括一个或多个属性信息;其中,至少一个所述属性信息相同的不同待升级设备对应相同的所述公钥和对应的主密钥。本发明实施例中,服务器针对具有相同的某一种或者某几种属性信息的不同待升级设备,使用相同的公钥以及对应的主密钥,可以降低服务器上的存储量以及计算量,提升升级效率。例如具有相同型号的车辆,可以采用相同的公钥和主密钥。

[0235] 本发明实施例中,将密文策略属性加密算法(CP-ABE)具体应用到设备升级场景中,通过在待升级设备的升级请求中携带该待升级设备的属性集合(包含该设备的一个或多个属性信息),使得服务器可根据该升级请求中的属性集合,生成对应的访问策略,并根据该访问策略对待升级设备的升级包进行加密,最终生成只有满足访问策略中所设置的前提条件(即拥有匹配的属性信息所对应的属性密钥)的设备才可以正确解密获得升级包,实现了升级条件的强制检测以及升级包细粒度的访问控制,即非法设备或者不满足升级条件的设备由于没有匹配的属性信息对应的属性密钥,则无法获得或解密该升级包,保证了设备升级过程的安全性以及准确性。

[0236] 需要说明的是，虽然上述实施例主要以智能车辆/车载系统升级的场景为例进行描述，但并不代表本申请中的设备升级方法只能应用于以上车载设备的升级场景，如前述，本申请中的设备升级方法还可以应用于，例如服务器管理智能家电进行升级、服务器管理虚拟机进行系统升级、服务器管理终端批量系统升级、智能手机管理智能穿戴设备进行设备升级等等，其它场景及举例将不再一一列举和赘述。

[0237] 请参见图10，图10是本发明实施例提供的另一种设备升级方法的流程示意图，该设备升级方法可应用于上述系统架构一，且适用于上述图1、图2中的任意一种应用场景。下面将结合附图10从服务器和待升级设备的交互侧进行描述，该方法实施例可以包括以下步骤S1001-步骤S1011，其中包括步骤S1004-A-步骤S1007-A。

[0238] S1001：服务器生成公钥和主密钥，主密钥为公钥对应的私钥。

[0239] S1002：服务器根据主密钥以及一个或多个属性信息，生成一个或多个属性密钥。

[0240] S1003：服务器将一个或多个属性密钥发送至待升级设备进行预存储；其中，一个或多个属性密钥用于待升级设备对目标升级包密文进行解密以获得目标升级包。

[0241] S1004-A：待升级设备获取待升级设备的属性集合对应的一个或多个属性密钥。

[0242] S1005-A：待升级设备向服务器发送升级请求，服务器接收待升级设备发送的升级请求，升级请求包括待升级设备的属性集合，属性集合包括待升级设备的一个或多个属性信息。

[0243] S1006-A：服务器对待升级设备的身份信息进行验证。

[0244] S1007-A：若验证通过，服务器根据待升级设备的一个或多个属性信息，确定待升级设备需要升级的一个或多个升级文件，目标升级包包括一个或多个升级文件。

[0245] 可替换地，上述步骤S1004-A-步骤S1007-A可以替换为下面的步骤S1004-B-步骤S1004-B。请参见图11，图11是本发明实施例提供的又一种设备升级方法的流程示意图，该设备升级方法可应用于上述系统架构二，且适用于上述图1、图3中的任意一种应用场景。该方法实施例可以包括以下步骤S1001-步骤S1011，其中包括如下步骤S1004-B-步骤S1007-B。

[0246] S1004-B：待升级设备获取终端设备的一个或多个属性信息对应的属性密钥，以及待升级设备的一个或多个属性信息对应属性密钥。

[0247] S1005-B：终端设备向服务器发送待升级设备的升级请求，服务器接收终端设备发送的待升级设备的升级请求，升级请求包括待升级设备的属性集合，属性集合包括终端设备的一个或多个属性信息以及待升级设备的一个或多个属性信息；

[0248] S1006-B：服务器对终端设备的身份信息和终端设备待升级设备的身份信息分别进行验证；

[0249] S1007-B：若均验证通过，服务器根据终端设备的一个或多个属性信息以及待升级设备的一个或多个属性信息，确定待升级设备需要升级的一个或多个升级文件，目标升级包包括一个或多个升级文件。

[0250] S1008：服务器根据属性集合生成针对待升级设备的访问策略。

[0251] S1009：服务器基于属性加密算法，根据访问策略对目标升级包进行加密，生成目标升级包密文。

[0252] S1010：服务器将目标升级包密文发送至待升级设备。待升级设备接收服务器发送

的目标升级包密文；

[0253] S1011：待升级设备根据一个或多个属性密钥对目标升级包密文进行解密，获得目标升级包。

[0254] 具体地，以下主要以智能车辆/车载系统升级的场景为例进行描述，即待升级设备可以为智能车辆/车载系统。升级请求可以为针对智能车辆/车载系统中的一个或多个待升级车载单元(例如人机界面HMI、电池管理系统BMS、电子控制单元等)的升级请求。

[0255] 在上述步骤S1001-步骤S1003中，服务器生成公钥和主密钥，主密钥为公钥对应的私钥；服务器根据主密钥以及一个或多个属性信息，生成一个或多个属性密钥；服务器将一个或多个属性密钥发送至待升级设备进行预存储；其中，一个或多个属性密钥用于待升级设备对目标升级包密文进行解密以获得目标升级包。也即是服务器在初始阶段需要生成针对该待升级设备后续安全升级过程中所要使用到的公钥、主密钥(与公钥对应的私钥)以及对应的属性密钥，并且将属性密钥发送给拥有对应属性信息的待升级设备，以保证后续的基于密文策略属性加密算法的设备安全升级过程。需要说明的是，若对应图11中所述的实施例，则该一个或多个属性密钥中还包括终端设备的属性信息所对应的属性密钥，也即是后续生成访问策略时，需要基于终端设备的属性信息以及待升级设备的属性信息生成。对应的，服务器接收的升级请求中包括的属性集合包括也包括终端设备的一个或多个属性信息。

[0256] 在上述步骤S1004-A-步骤S1007-A中，通过待升级设备自身向服务器发送升级请求，且该升级请求中携带了该待升级设备的一个或者多个属性信息。例如，待升级车辆向服务器发送携带有自身的车辆身份码、引擎号、车牌号码、车型流水号、车辆部件的硬件版本号和车辆部件的软件版本号等属性信息的升级请求。属性集合包括待升级设备的一个或多个属性信息。目标升级包包括该待升级设备的一个或多个升级文件(例如智能车辆中的多个待升级车载单元分别对应的升级文件)。进一步地，服务器在获取待升级设备的升级请求后，先对该升级请求做身份验证，若身份验证通过后，则表明该待升级设备的身份是合法的。进一步地，服务器可以根据升级请求中的待升级设备的属性信息确定对应的目标升级包，例如，根据属性集合中的硬件版本号和软件版本号确定智能车辆当前需要更行的升级文件。由于，升级包是服务器根据该待升级设备的属性信息确定的，因此可以确保待升级设备可以下载其所精确需要、以及符合条件的升级包，避免升级包不符合待升级设备的属性要求。同时，也可以避免不符合该属性信息的待升级设备非法获得升级包，进一步保证了设备升级过程的安全性以及准确性。

[0257] 可选的，在上述步骤S1001-B-步骤S1003-B中，通过与待升级设备绑定的终端设备向服务器发送升级请求，此时该升级请求中携带了该终端设备的一个或多个属性信息以及该待升级设备自身的一个或者多个属性信息。可选的，在终端设备向服务器发送升级请求之前，还获取终端设备的一个或多个属性信息以及所述待升级设备的一个或多个属性信息。例如，与智能车辆绑定的智能手机向服务器发送携带有自身的手机号、手机识别码和手机的软件版本信息，以及携带有待升级车辆的车辆身份码、引擎号、车牌号码、车型流水号、车辆部件的硬件版本号和车辆部件的软件版本号等属性信息的升级请求。而服务器在获取待升级设备的升级请求后，先对终端设备和待升级设备共同做身份验证，若身份验证均通过后，则表明该请求的终端设备是合法的，且其请求进行设备升级的待升级设备也是合法

的。且由于升级包是服务器根据终端设备和待升级设备的属性信息共同确定的，因此可以确保只有终端设备的属性信息，以及与其绑定的待升级设备的属性信息均符合访问策略中升级条件的情况下，该待升级设备才可以进行安全升级，提供了具有强制力的终端设备和待升级设备的身份与状态的前提条件检测，保证了设备升级过程的安全性以及准确性，避免非法设备或不符合条件的待升级设备非法获得升级包。在一种可能的实现方式中，所述终端设备为智能手机；所述属性集合包括手机号、手机识别码和手机的软件版本信息中的一种或者多种属性信息。即通过采用智能手机搭配待升级设备进行升级，提供一种适用于一些特殊场景中的升级系统架构。例如，某个用户可以通过自己的智能手机对与该手绑定的车辆进行安全升级，安全便捷。

[0258] 在上述步骤S1008中，关于服务器根据属性集合生成针对待升级设备的访问策略的具体方式，针对上述图10或图11的两种架构中，包括两种实现方式：

[0259] 方式一，属性集合包括待升级设备的一个或多个属性信息；服务器根据待升级设备的一个或多个属性信息，确定待升级设备需要升级的一个或多个升级文件，目标升级包包括一个或多个升级文件；服务器确定一个或多个升级文件对应的升级条件，并基于升级条件生成访问策略。本发明实施例中，服务器根据待升级设备的一个或者多个属性信息确定一个或多个升级文件，并依据该一个或多个升级文件的升级条件组合后转换为访问策略，也即是服务器根据待升级设备的相关属性信息生成针对该待升级设备的升级条件，以限制目标升级包的访问权限。

[0260] 方式二，服务器根据终端设备的一个或多个属性信息以及待升级设备的一个或多个属性信息，确定待升级设备需要升级的一个或多个升级文件，目标升级包包括一个或多个升级文件；服务器确定一个或多个升级文件对应的升级条件，并基于升级条件生成访问策略。本发明实施例中，由于引入终端设备协助待升级设备进行升级，因此，服务器根据终端设备和待升级设备的多个属性信息确定一个或多个升级文件，并依据该一个或多个升级文件的升级条件组合后转换为访问策略，也即是服务器根据终端设备和待升级设备的相关属性信息生成针对该待升级设备的升级条件，以限制目标升级包的访问权限。

[0261] 上述步骤S1009至步骤S1011可参考上述图9实施例中的步骤S902至步骤S904的相关描述，此处不再赘述。

[0262] 基于上述，以下结合具体应用场景以及附图，对上述发明实施例进行进一步的描述。

[0263] 请参见图12，图12是本发明实施例提供的一种智能车辆的升级场景示意图，以待升级设备为智能车辆，以服务器为车辆制造商OEM的服务器为例，将本申请中的设备升级流程分为：系统设置阶段(setup phase)和系统升级阶段(update phase)。其中，

[0264] 1、系统设置阶段(setup phase)，主要包括密钥的生成和分发：

[0265] (1)车辆制造商OEM服务器端，针对某特定车型(Car Model)的车进行系统设定，通过系统参数生成公钥(pk_c)和主密钥(mr_c)，该公钥和主密钥为一对公私钥对；

[0266] (2)OEM服务器基于该主密钥(mr_c)以及智能车辆的不同属性信息分别生成不同属性信息对应的属性密钥(ar_c)，然后将上述公钥(pk_c)和属性密钥(ar_c)通过安全通道发送至拥有对应属性信息的智能车辆。

[0267] 2、系统升级阶段(update phase)，主要包括OEM服务器验证车辆身份和状态、OEM

生成相应的升级包：

[0268] (1)智能车辆当前已经拥有系统设置阶段由OEM服务器配置的公钥(pk_c)和一个或多个属性信息对应的属性密钥(ar_c)。

[0269] (2)智能车辆向OEM服务器发送升级请求，且该升级请求中包括经过上述公钥(pk_c)加密的身份信息ID和状态信息attribute(也即是属性集合)，记为Enc_{pk_c}(ID,attribute)。

[0270] (3)OEM服务器根据所述主密钥(mr_c)对接收到的升级请求进行解密和验证，即通过对应的解密算法Dec_{mr_c}(C)以验证车辆身份和状态，其中C则是指上述升级请求。

[0271] (4)OEM服务器根据公钥(pk_c)以及访问策略policy生成目标升级包package的目标升级包密文，也可称之为策略包，记为Enc_{pk_c}(package,policy)。可选的，该策略包可以包含新的属性密钥或者更新后的属性密钥。

[0272] (5)OEM服务器将上述经过访问策略policy和公钥(pk_c)加密后的目标升级包C＝Enc_{pk_c}(package,policy)发送给智能车辆，此处，C是指目标升级包密文。

[0273] (6)智能车辆接收上述目标升级包密文，如果满足访问策略(即使用必要的属性密钥)，则可以通过对应的属性密钥(ar_c)成功解密Dec_{ar_c}(C)。

[0274] 请参见图13，图13是本发明实施例提供的另一种智能车辆的升级场景示意图，以待升级设备为智能车辆，以服务器为车辆制造商OEM的服务器为例，将本申请中的设备升级流程分为：系统设置阶段(setup phase)和系统升级阶段(update phase)。其中，

[0275] 1、系统设置阶段(setup phase)，主要包括密钥的生成和分发：

[0276] (1)车辆制造商OEM服务器端，针对某特定车型(Car Model)的车进行系统设定，通过系统参数生成公钥(pk_c)和主密钥(mr_c)，该公钥和主密钥为一对公私钥对；

[0277] (2)OEM服务器基于该主密钥(mr_c)以及智能车辆的不同属性信息分别生成不同属性信息对应的属性密钥(ar_c)，然后将上述公钥(pk_c)和属性密钥(ar_c)通过安全通道发送至拥有对应属性信息的智能车辆。例如，智能车辆的属性信息包括车辆标识号(VIN)、发动机编号、车牌号、序列号、TBox：硬件版本1，软件版本1、HMI：硬件版本1，软件版本1、动力系统：硬件版本1，软件版本1等。

[0278] 2、系统升级阶段(update phase)，主要包括OEM服务器验证车辆身份和状态、OEM生成相应的升级包：

[0279] (1)智能车辆当前已经拥有系统设置阶段由OEM服务器配置的公钥(pk_c)和一个或多个属性信息对应的属性密钥(ar_c)。

[0280] (2)智能车辆向OEM服务器发送升级请求，且该升级请求中包括经过上述公钥(pk_c)加密的身份信息ID和状态信息attribute(也即是属性集合)，记为Enc_{pk_c}(ID,attribute)。

[0281] (3)OEM服务器根据所述主密钥(mr_c)对接收到的升级请求进行解密和验证，即通过对应的解密算法Dec_{mr_c}(C)以验证车辆身份和状态，其中C则是指上述升级请求。

[0282] (4)OEM服务器根据公钥(pk_c)以及访问策略policy生成目标升级包package的目标升级包密文，也可称之为策略包，记为Enc_{pk_c}(package,policy)。例如，该访问策略为(发动机编号＝1234567)和(TBox软件版本＝1)。

[0283] (5)OEM服务器将上述经过访问策略policy和公钥(pk_c)加密后的目标升级包C＝

Enc_{pk_c}(package,policy)发送给智能车辆,此处,C是指目标升级包密文。

[0284] (6)智能车辆可通过TBox接收上述目标升级包密文,并可通过车载主控制器检测自身是否有引擎号码为1234567的属性密钥(ar_c)与TBox软件版本号码为1的属性密钥(ar_c),若均有,则可以正确解密出目标升级包密文Dec_{ar_c}(C)。若没有,则无法解密出目标升级包密文Dec_{ar_c}(C)。也即是实现了强制力的车辆身份与状态的前提条件检测。

[0285] 本发明实施例与上述图12中的实施例的区别在于,针对智能车辆的属性信息,提供了一种具体的访问策略的示例,以实现升级条件的强制性检测。

[0286] 请参见图14,图14是本发明实施例提供的又一种智能车辆的升级场景示意图,以待升级设备为智能车辆,以服务器为车辆制造商OEM的服务器为例,将本申请中的设备升级流程分为:系统设置阶段(setup phase)和系统升级阶段(update phase)。其中,

[0287] 1、系统设置阶段(setup phase),主要包括密钥的生成和分发:

[0288] (1)车辆制造商OEM服务器端,针对某特定车型(Car Model)的车进行系统设定,通过系统参数生成公钥(pk_c)和主密钥(mr_c),该公钥和主密钥为一对公私钥对;

[0289] (2)OEM服务器基于该主密钥(mr_c)以及该型号的智能车辆的不同属性信息分别生成不同属性信息对应的属性密钥(ar_c),然后将上述公钥(pk_c)和属性密钥(ar_c)通过安全通道发送至拥有对应属性信息的智能车辆。例如,属性信息包括车辆标识号(VIN)、发动机编号、车牌号、序列号、TBox:硬件版本1,软件版本1、HMI:硬件版本1,软件版本1、动力系统:硬件版本1,软件版本1。

[0290] 2、系统升级阶段(update phase),主要包括OEM服务器验证车辆身份和状态、OEM生成相应的升级包:

[0291] (1)智能车辆当前已经拥有系统设置阶段由OEM服务器配置的公钥(pk_c)和一个或多个属性信息对应的属性密钥(ar_c)。

[0292] (2)智能车辆向OEM服务器发送升级请求,且该升级请求中包括经过上述公钥(pk_c)加密的身份信息ID和状态信息attribute(也即是属性集合),记为Enc_{pk_c}(ID,attribute)。

[0293] (3)OEM服务器根据所述主密钥(mr_c)对接收到的升级请求进行解密和验证,即通过对应的解密算法Dec_{mr_c}(C)以验证车辆身份和状态,其中C则是指上述升级请求。

[0294] (4)OEM服务器根据公钥(pk_c)以及访问策略policy生成目标升级包package的目标升级包密文,也可称之为策略包,记为Enc_{pk_c}(package,policy)。例如,该访问策略为(发动机编号=1234567)和(TBox软件版本=1)。在图14中可以看出,车辆原始状态(尚未升级前)有TBox软件版本1,而目标升级包内含有对TBox的软件升级包,且升级后为版本号2,所以升级包中可包含新的属性密钥,该属性密钥相对应于TBox软件版本号2。也即是不仅可以升级智能车辆的软件,同时更新了相对应的属性密钥。

[0295] (5)OEM服务器将上述经过访问策略policy和公钥(pk_c)加密后的目标升级包C=Enc_{pk_c}(package,policy)发送给智能车辆,此处,C是指目标升级包密文。

[0296] (6)智能车辆接收上述目标升级包密文,如果满足访问策略(即使用必要的属性密钥),则可以通过对应的属性密钥(ar_c)成功解密Dec_{ar_c}(C)。例如,当智能车辆上的车载主控制器获得该目标升级包密文后,通过所拥有的属性密钥(例:TBox软件版本号1的属性密钥)进行解密,若属性密钥符合访问策略,则可以正确解出升级包。而此目标升级包中除包

含TBox软件版本号2的升级包,还包含TBox软件版本号2的属性密钥,因此,车载主控制器将TBox软件版本号1的属性密钥更新为TBox软件版本号2的属性密钥。

[0297] 本发明实施例与上述图12中的实施例的区别在于,在系统升级阶段中,在目标升级包中携带某个属性信息(例如此次会变动的动态属性信息)的更新后的属性密钥,以根据升级系统对属性密钥进行升级。

[0298] 请参见图15,图15是本发明实施例提供的又一种智能车辆的升级场景示意图,以待升级设备为智能车辆,以服务器为车辆制造商OEM的服务器为例,将本申请中的设备升级流程分为:系统设置阶段(setup phase)和系统升级阶段(update phase)。其中,

[0299] 1、系统设置阶段(setup phase),主要包括密钥的生成和分发:

[0300] (1)车辆制造商OEM服务器端针对某特定车型(Car Model)的车进行系统设定,通过系统参数生成公钥pk_c与主密钥mr_c。

[0301] (2)OEM服务器预置公钥(pk_c)与主密钥(mr_c)给此车型的车辆。本发明实施例中不特别描述静态属性信息与动态属性信息也即是对应的属性集合。由于主密钥已经预置给车辆,车辆可随需生成相对的属性密钥。

[0302] 2、系统升级阶段(update phase),主要包括OEM服务器验证车辆身份和状态、OEM生成相应的升级包:

[0303] (1)智能车辆当前已经拥有系统设置阶段由OEM服务器配置的公钥(pk_c)和主密钥mr_c。

[0304] (2)智能车辆提出升级需求,使用公钥(pk_c)、身份与状态属性生成加密的身份与状态属性,Enc_{pk_c}(ID attributes,status attributes)。

[0305] (3)智能车辆将包含加密的身份与状态属性的升级请求发送给OEM服务器。

[0306] (4)OEM服务器根据主密钥mr_c解密后(Dec_{mr_c}(C)),核对车辆身份与状态,此处密文C即为上述Enc_{pk_c}(ID attributes,status attributes)。

[0307] (5)OEM服务器根据属性集合中的状态信息找到可以升级的软件组合(package),以及确认升级的前提条件。OEM服务器将前提条件组合成访问策略(access policy),并且通过该访问策略加密升级包Enc_{pk_c}(package,policy)。

[0308] (6)OEM服务器向智能车辆提供该加密的升级包,其包含访问策略(access policy)于其中。

[0309] (7)当智能车辆上的车载主控制器获得该升级包时,通过主密钥mr_c对所拥有的属性生成属性密钥,并根据此属性密钥进行解密,若属性密钥符合访问策略,则可以正确解出升级包。

[0310] 本发明实施例与上述图12中的实施例的区别在于,在系统设置阶段,OEM服务器将主密钥也预置于智能车辆上,其功能是智能车辆可以通过该主密钥动态生成各种属性密钥,支援更广的前提条件,例如行车速度,挡位,网络存取状态等。通过更广的前提条件支援更细致的条件检测,另一方面来说,本发明实施例中需要对智能车辆有更高的信任度。

[0311] 请参见图16,图16是本发明实施例提供的又一种智能车辆的升级场景示意图,以待升级设备为智能车辆,以服务器为车辆制造商OEM的服务器、以终端设备为智能手机为例,将本申请中的设备升级流程分为:系统设置阶段(setup phase)和系统升级阶段(update phase)。其中,

[0312] 1、系统设置阶段(setup phase),主要包括密钥的生成和分发:

[0313] (1)车辆制造商OEM服务器端针对某特定车型(Car Model)的智能车辆进行系统设定,通过系统参数生成公钥pk_c与主密钥mr_c。

[0314] (2)OEM服务器基于该主密钥(mr_c),针对定义好前提条件所对应的属性信息生成属性密钥(ar_c)。然后将上述公钥(pk_c)和属性密钥(ar_c)通过安全通道发送至拥有对应属性信息的智能车辆。例如,智能车辆的属性信息包括车辆标识号(VIN)、发动机编号、车牌号、序列号、TBox:硬件版本1,软件版本1、HMI:硬件版本1,软件版本1、动力系统:硬件版本1,软件版本1。

[0315] (3)进一步地,OEM服务器还需要生成针对匹配的智能手机的属性信息的属性密钥,通过额外的安全通道发布给智能手机。其中,智能手机的属性信息也包含静态属性信息与动态属性信息两部份,例如,静态属性信息为手机号(phone number),动态属性信息为应用程序版本号(application version)。

[0316] 2、系统升级阶段(update phase),主要包括OEM服务器验证车辆身份和状态、OEM生成相应的升级包:

[0317] (1)智能车辆与智能手机联合提出升级需求,使用公钥pk_c,身份与状态属性生成加密的身份与状态属性,i.e.Enc_{pk_c}(ID attributes,status attributes)。

[0318] (2)智能车辆将包含加密的身份与状态属性的升级请求发送给OEM服务器。

[0319] (3)OEM服务器根据所述主密钥(mr_c)对接收到的升级请求进行解密和验证,即通过对应的解密算法Dec_{mr_c}(C)以验证手机和车辆身份与状态,其中C则是指上述升级请求。

[0320] (4)OEM服务器根据属性集合中的状态信息找到可以升级的软件组合(package),以及确认升级的前提条件。OEM服务器将前提条件组合成访问策略(policy),并且通过该访问策略加密升级包Enc_{pk_c}(package,policy)。例如,访问策略为“引擎号码为1234567,手机号码为xxxx且人机界面HMI的软件版本号为1”,其中,对引擎号码的限制可以限制仅有该车辆可以使用该升级包,对手机号码的限制仅有该手机可以限定参与升级过程,对HMI软件版本号码可以限制该车辆的软件条件。

[0321] (5)OEM服务器向待升级设备提供该加密的升级包,其包含访问策略(access policy)于其中。

[0322] (6)当智能手机与智能车辆上的车载主控制器获得该升级包时,通过所拥有的属性密钥(例如:引擎号码,手机号与HMI软件版本号码)联合进行解密,若属性密钥符合访问策略,则可以正确解出升级包。图16中的访问策略为手机具有号码为xxxx的属性密钥,车辆有引擎号码为1234567的属性密钥(ar_c)与HMI软件版本号码为1的属性密钥(ar_c),则可以正确解密出升级包Dec_{ar_c}(C)。

[0323] 本发明实施例与上述图12中的实施例的区别在于,使用了智能手机的协助进行升级。通过智能手机与车载主控制器的协同合作,提出升级要求,并且对收到的升级包进行解密,可以理解的是该系统架构下,可由智能车辆单独对升级包进行解密,也可由智能手机单独对升级包进行解密,还可以由两者共同协作对升级包进行解密。

[0324] 请参见图17,图17是本发明实施例提供的又一种智能车辆的升级场景示意图,以待升级设备为智能车辆,以服务器为车辆制造商OEM的服务器为例,将本申请中的设备升级流程分为:系统设置阶段(setup phase)和系统升级阶段(update phase),其中,关于系统

设置阶段(setup phase)和系统升级阶段的描述,可参考上述图12-图16中任意一种实施例中的相关流程,此处不再赘述。其中,

[0325] 本发明实施例与上述图12中的实施例的区别在于,是在系统设置阶段,通过不同的属性设计,可以减少车厂管理的钥匙对。图17中上半部分显示的是OEM服务器对不同车型的智能车辆分别生成一对钥匙,即车型A对应一个密钥对,车型B对应另一个密钥对。也即是说,对于每一种车型,OEM服务器都需要管理一对钥匙,导致OEM服务器要管理的钥匙对数量与生产的车型数量呈正比。图17的下半部分显示的是当OEM服务器将车型(Car Model)也列为属性信息之一时,则可以使用一对钥匙对管理不同的车型,并且用不同的车型属性密钥进行区别。

[0326] 以上详细阐述了本发明实施例的方法,下面提供了本发明实施例的相关装置。

[0327] 请参见图18,图18是本发明实施例提供的一种设备升级装置的结构示意图,该设备升级装置10可以应用于服务器,如上述图4或图5的系统架构中,设备升级装置10各个单元的详细描述如下。

[0328] 策略生成单元101,用于根据待升级设备的属性集合生成针对所述待升级设备的访问策略;

[0329] 加密单元102,用于基于属性加密算法,根据所述访问策略对目标升级包进行加密,生成目标升级包密文;

[0330] 第一发送单元103,用于将所述目标升级包密文发送至所述待升级设备,所述目标升级包密文用于所述待升级设备根据所述属性集合对应的一个或多个属性密钥进行解密,以获得所述目标升级包。

[0331] 在一种可能的实现方式中,装置10还包括:

[0332] 获取单元104,用于获取所述待升级设备的升级请求,所述升级请求包括所述待升级设备的属性集合。

[0333] 在一种可能的实现方式中,获取单元104,具体用于:

[0334] 接收所述待升级设备发送的所述升级请求,所述属性集合包括所述待升级设备的一个或多个属性信息。

[0335] 在一种可能的实现方式中,所述属性集合包括所述待升级设备的一个或多个属性信息;策略生成单元101,具体用于:

[0336] 根据所述待升级设备的一个或多个属性信息,确定所述待升级设备需要升级的一个或多个升级文件,所述目标升级包包括所述一个或多个升级文件;

[0337] 确定所述一个或多个升级文件对应的升级条件,并基于所述升级条件生成所述访问策略。

[0338] 在一种可能的实现方式中,获取单元104,具体用于:

[0339] 接收终端设备发送的所述待升级设备的升级请求,所述属性集合包括所述终端设备的一个或多个属性信息以及所述待升级设备的一个或多个属性信息。

[0340] 在一种可能的实现方式中,策略生成单元101,具体用于:

[0341] 根据所述终端设备的一个或多个属性信息以及所述待升级设备的一个或多个属性信息,确定所述待升级设备需要升级的一个或多个升级文件,所述目标升级包包括所述一个或多个升级文件;

[0342] 确定所述一个或多个升级文件对应的升级条件，并基于所述升级条件生成所述访问策略。

[0343] 在一种可能的实现方式中，所述属性集合包括一个或多个属性信息；装置10还包括：

[0344] 第一密钥生成单元105，用于生成公钥和主密钥，所述主密钥为所述公钥对应的私钥；

[0345] 第二密钥生成单元106，根据所述主密钥以及所述一个或多个属性信息，生成所述属性集合对应的一个或多个属性密钥；

[0346] 第二发送单元107，用于将所述一个或多个属性密钥发送至所述待升级设备进行预存储；其中，所述一个或多个属性密钥用于所述待升级设备对所述目标升级包密文进行解密以获得所述目标升级包。

[0347] 在一种可能的实现方式中，请参见图19，图19是本发明实施例提供的另一种设备升级装置的结构示意图，装置10还包括：

[0348] 第三密钥生成单元108，用于生成公钥和主密钥，所述主密钥为所述公钥对应的私钥；

[0349] 第三发送单元109，用于将所述主密钥发送至所述待升级设备上进行预存储，所述主密钥用于所述待升级设备生成所述属性集合对应的一个或多个属性密钥，其中，所述一个或多个属性密钥用于所述待升级设备对所述目标升级包密文进行解密以获得所述目标升级包。

[0350] 在一种可能的实现方式中，所述属性集合包括一个或多个属性信息；所述目标升级包包括所述属性集合中至少一个属性信息对应的更新后的属性密钥。

[0351] 在一种可能的实现方式中，所述属性集合包括一个或多个属性信息；其中，至少一个所述属性信息相同的不同待升级设备对应相同的所述公钥和对应的主密钥。

[0352] 在一种可能的实现方式中，所述待升级设备为智能车辆；所述属性集合包括车辆身份码、引擎号、车牌号码、车型流水号、车辆部件的硬件版本号和车辆部件的软件版本号中的一种或者多种属性信息。

[0353] 在一种可能的实现方式中，所述终端设备为智能手机；所述属性集合包括手机号、手机识别码和手机的软件版本信息中的一种或者多种属性信息。

[0354] 需要说明的是，本发明实施例中所描述的设备升级装置10中各功能单元的功能可参见上述图1-图17所述的方法实施例中服务器的相关描述，此处不再赘述。

[0355] 请参见图20，图20是本发明实施例提供的一种待升级装置的结构示意图，该待升级装置20可应用于待升级设备，如上述图4或图5的系统架构中，待升级装置20各个单元的详细描述如下。

[0356] 接收单元201，用于接收服务器发送的目标升级包密文，所述目标升级包密文为所述服务器基于属性加密算法，根据访问策略对目标升级包进行加密生成的，所述访问策略为所述服务器根据所述待升级设备的属性集合生成的；

[0357] 获取单元202，用于获取所述属性集合对应的一个或多个属性密钥；

[0358] 解密单元203，用于根据所述一个或多个属性密钥对所述目标升级包密文进行解密，获得目标升级包。

[0359] 在一种可能的实现方式中，装置20还包括：

[0360] 发送单元204，用于发送升级请求，所述升级请求包括所述待升级设备的属性集合。

[0361] 在一种可能的实现方式中，所述属性集合包括一个或多个属性信息；获取单元202，具体用于：

[0362] 接收所述服务器发送的一个或多个属性密钥，并进行预存储；所述属性密钥为所述服务器生成公钥和主密钥后，根据所述主密钥以及所述一个或多个属性信息，生成的一个或多个属性密钥；所述主密钥为所述公钥对应的私钥。

[0363] 在一种可能的实现方式中，所述属性集合包括一个或多个属性信息；获取单元202，具体用于：

[0364] 接收所述服务器发送主密钥并进行预存储，所述主密钥为所述服务器生成的；

[0365] 所述待升级设备根据所述主密钥以及所述一个或多个属性信息，生成一个或多个属性密钥。

[0366] 在一种可能的实现方式中，所述属性集合包括一个或多个属性信息；所述目标升级包包括所述属性集合中至少一个属性信息对应的更新后的属性密钥。

[0367] 在一种可能的实现方式中，所述属性集合包括一个或多个属性信息；其中，至少一个所述属性信息相同的不同待升级设备对应相同的所述公钥和对应的主密钥。

[0368] 在一种可能的实现方式中，所述待升级设备为智能车辆；所述属性集合包括车辆身份码、引擎号、车牌号码、车型流水号、车辆部件的硬件版本号和车辆部件的软件版本号中的一种或者多种属性信息。

[0369] 需要说明的是，本发明实施例中所描述的待升级装置20中各功能单元的功能可参见上述图1-图17所述的方法实施例中待升级设备的相关描述，此处不再赘述。

[0370] 请参见图21，图21是本发明实施例提供的另一种设备升级装置的结构示意图，该待升级设备30可应用于终端设备，如上述图5的系统架构中，设备升级装置30各个单元的详细描述如下。

[0371] 发送单元301，用于向服务器发送待升级设备的升级请求，所述升级请求包括所述待升级设备的属性集合，所述属性集合包括所述终端设备的一个或多个属性信息以及所述待升级设备的一个或多个属性信息。

[0372] 在一种可能的实现方式中，所述升级请求还包括所述终端设备的身份信息和所述待升级设备的身份信息；其中，所述终端设备的身份信息和所述待升级设备的身份信息用于所述服务器分别进行验证；若均验证通过则根据所述终端设备的一个或多个属性信息以及所述待升级设备的一个或多个属性信息，确定所述待升级设备需要升级的一个或多个升级文件，所述目标升级包包括所述一个或多个升级文件。

[0373] 在一种可能的实现方式中，所述装置还包括：获取单元302，用于获取所述终端设备的一个或多个属性信息以及所述待升级设备的一个或多个属性信息。

[0374] 需要说明的是，本发明实施例中所描述的设备升级装置30中各功能单元的功能可参见上述图1-图17所述的方法实施例中终端设备的相关描述，此处不再赘述。

[0375] 如图22所示，图22是本发明实施例提供的一种设备的结构示意图。本申请中的服务器、待升级设备和终端设备均可以以图20中的结构来实现，该设备40包括至少一个处理

器401,至少一个存储器402、至少一个通信接口403。此外,该设备还可以包括天线等通用部件,在此不再详述。

[0376] 处理器401可以是通用中央处理器(CPU),微处理器,特定应用集成电路(application-specific integrated circuit,ASIC),或一个或多个用于控制以上方案程序执行的集成电路。

[0377] 通信接口403,用于与其他设备或通信网络通信,如升级服务器、密钥服务器、车载内部的设备等。

[0378] 存储器402可以是只读存储器(read-only memory,ROM)或可存储静态信息和指令的其他类型的静态存储设备,随机存取存储器(random access memory,RAM)或者可存储信息和指令的其他类型的动态存储设备,也可以是电可擦可编程只读存储器(Electrically Erasable Programmable Read-Only Memory,EEPROM)、只读光盘(Compact Disc Read-Only Memory,CD-ROM)或其他光盘存储、光碟存储(包括压缩光碟、激光碟、光碟、数字通用光碟、蓝光光碟等)、磁盘存储介质或者其他磁存储设备、或者能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质,但不限于此。存储器可以是独立存在,通过总线与处理器相连接。存储器也可以和处理器集成在一起。

[0379] 其中,所述存储器402用于存储执行以上方案的应用程序代码,并由处理器401来控制执行。所述处理器401用于执行所述存储器402中存储的应用程序代码以实现本申请中服务器、待升级设备以终端设备的相关功能。

[0380] 需要说明的是,本发明实施例中所描述的服务器、待升级设备和终端设备的功能可参见上述图1至图17中的所述的方法实施例中的相关描述,此处不再赘述。

[0381] 本发明实施例还提供一种计算机存储介质,其中,该计算机存储介质可存储有程序,该程序执行时包括上述方法实施例中记载的任意一种设备升级方法的部分或全部步骤。

[0382] 本发明实施例还提供一种计算机程序,该计算机程序包括指令,当该计算机程序被计算机执行时,使得计算机可以执行任意一种设备升级方法的部分或全部步骤。

[0383] 在上述实施例中,对各个实施例的描述都各有侧重,某个实施例中没有详述的部分,可以参见其他实施例的相关描述。

[0384] 需要说明的是,对于前述的各方法实施例,为了简单描述,故将其都表述为一系列的动作组合,但是本领域技术人员应该知悉,本申请并不受所描述的动作顺序的限制,因为依据本申请,某些步骤可能可以采用其他顺序或者同时进行。其次,本领域技术人员也应该知悉,说明书中所描述的实施例均属于优选实施例,所涉及的动作和模块并不一定是本申请所必须的。

[0385] 在本申请所提供的几个实施例中,应该理解到,所揭露的装置,可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,例如上述单元的划分,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,可以是电性或其它的形式。

[0386] 上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。

[0387] 另外,在本申请各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,也可以采用软件功能单元的形式实现。

[0388] 上述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时,可以存储在一个计算机可读取存储介质中。基于这样的理解,本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来,该计算机软件产品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(可以为个人计算机、服务器或者网络设备等,具体可以是计算机设备中的处理器)执行本申请各个实施例上述方法的全部或部分步骤。其中,而前述的存储介质可包括:U盘、移动硬盘、磁碟、光盘、只读存储器(Read-Only Memory,缩写:ROM)或者随机存取存储器(Random Access Memory,缩写:RAM)等各种可以存储程序代码的介质。

[0389] 以上所述,以上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。

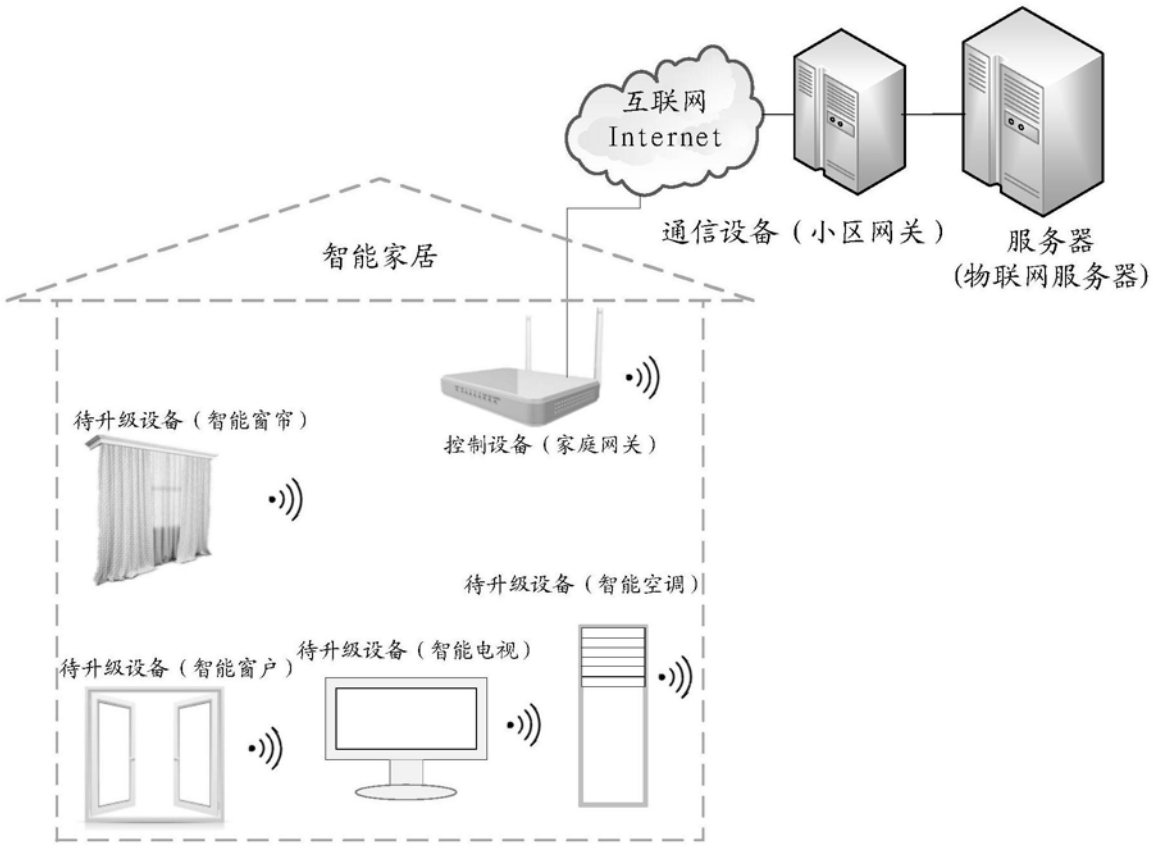

互联网
Internet
通信设备（小区网关）
服务器
(物联网服务器)
智能家居
控制设备（家庭网关）
待升级设备（智能窗帘）
待升级设备（智能空调）
待升级设备（智能窗户）
待升级设备（智能电视）

图1

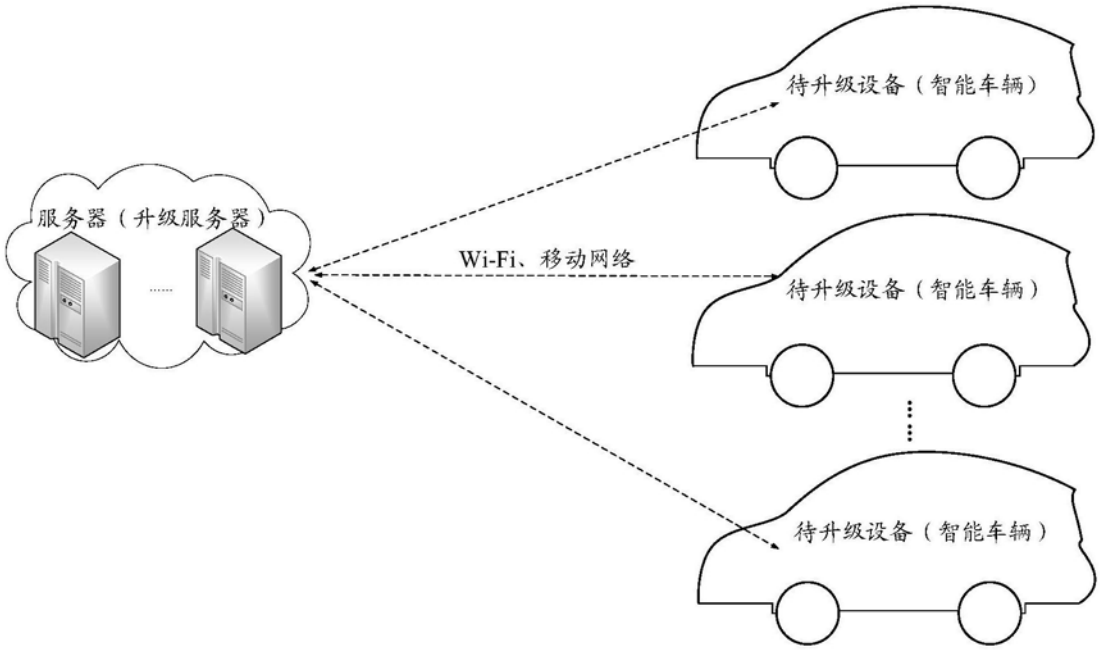

服务器（升级服务器）
Wi-Fi、移动网络
待升级设备（智能车辆）
待升级设备（智能车辆）
待升级设备（智能车辆）

图2

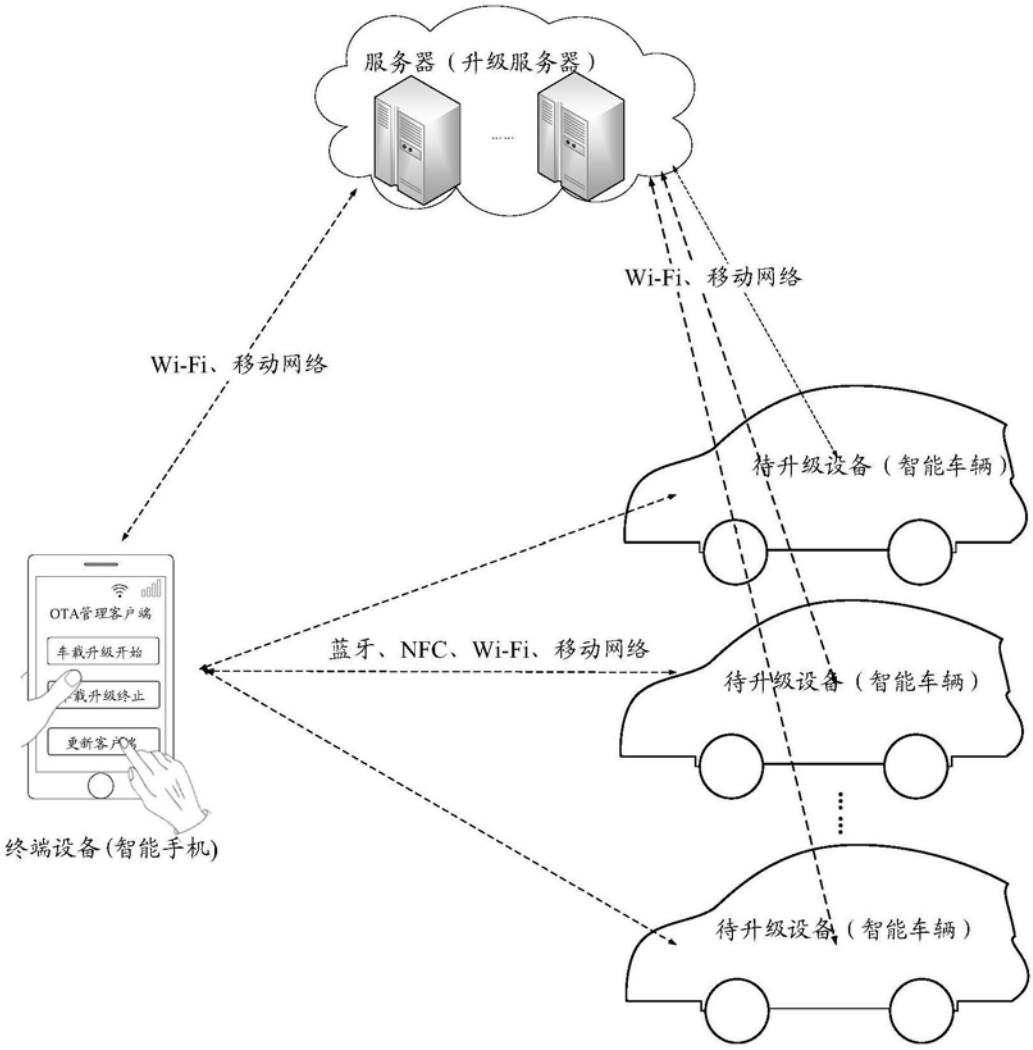

服务器（升级服务器）
Wi-Fi、移动网络
Wi-Fi、移动网络
待升级设备（智能车辆）
OTA管理客户端
车载升级开始
蓝牙、NFC、Wi-Fi、移动网络
待升级设备（智能车辆）
待升级设备（智能车辆）
终端设备(智能手机)

图3

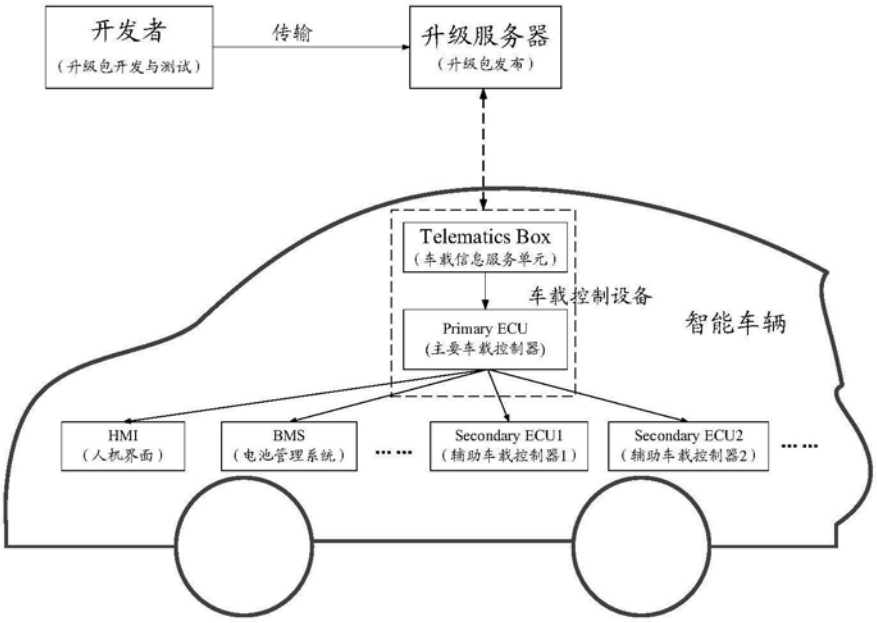

开发者
（升级包开发与测试）
传输
升级服务器
（升级包发布）
Telematics Box
（车载信息服务单元）
车载控制设备
智能车辆
Primary ECU
(主要车载控制器)
HMI
（人机界面）
BMS
（电池管理系统）
Secondary ECU1
（辅助车载控制器1）
Secondary ECU2
（辅助车载控制器2）

图4

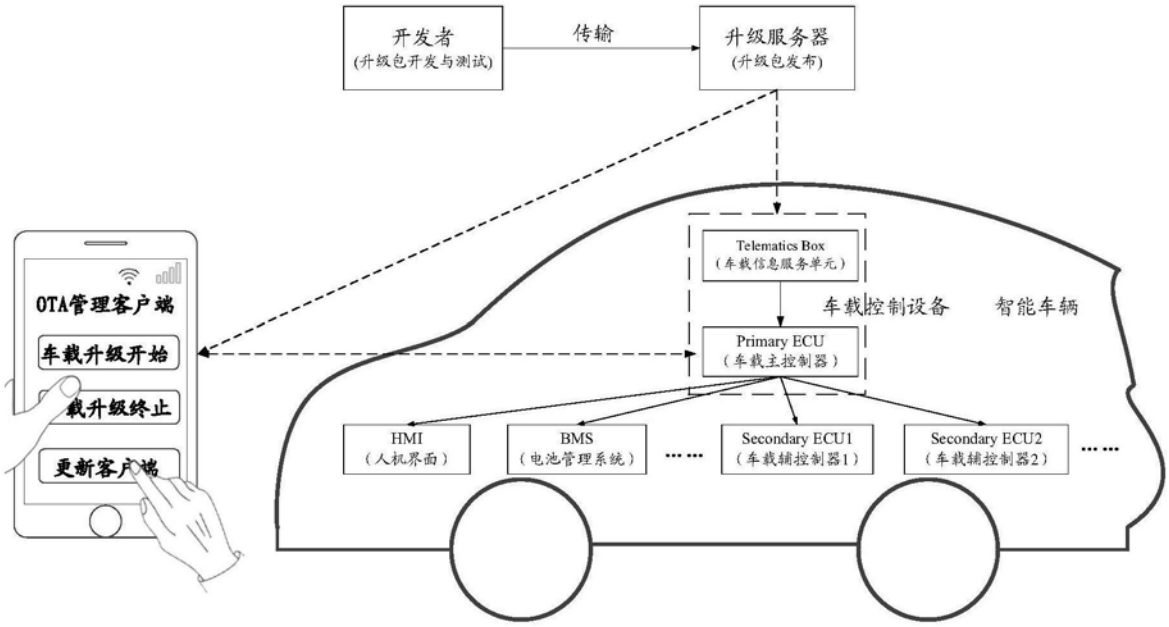

开发者
(升级包开发与测试)
传输
升级服务器
(升级包发布)
OTA管理客户端
车载升级开始
载升级终止
更新客户端
Telematics Box
（车载信息服务单元）
车载控制设备
智能车辆
Primary ECU
（车载主控制器）
HMI
（人机界面）
BMS
（电池管理系统）
Secondary ECU1
（车载辅控制器1）
Secondary ECU2
（车载辅控制器2）

图5

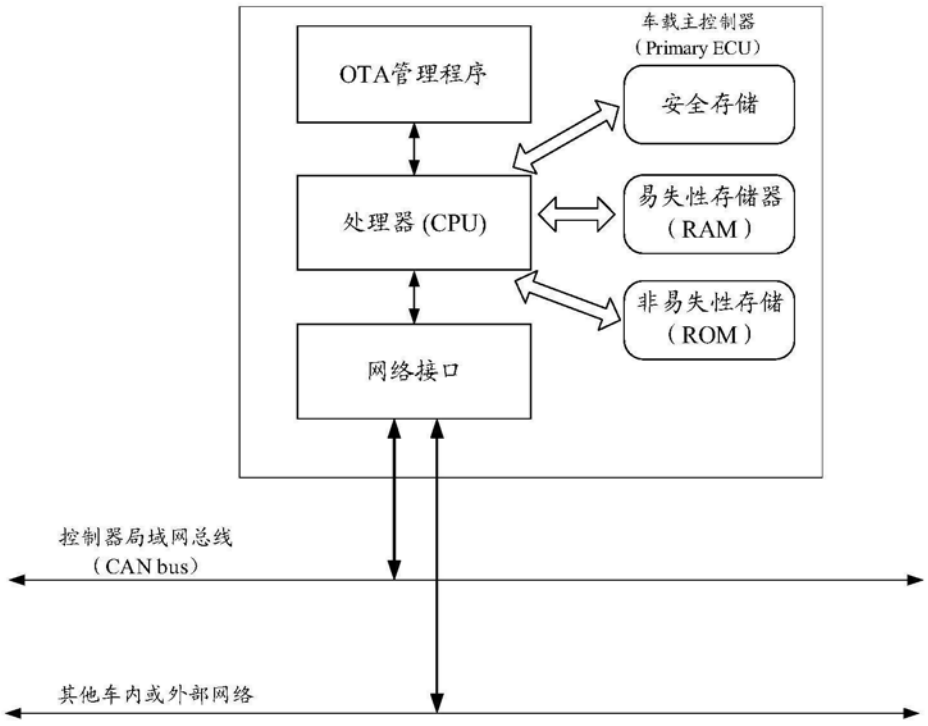

车载主控制器
（Primary ECU）
OTA管理程序
安全存储
处理器 (CPU)
易失性存储器
（RAM）
非易失性存储
（ROM）
网络接口
控制器局域网总线
（CAN bus）
其他车内或外部网络

图6

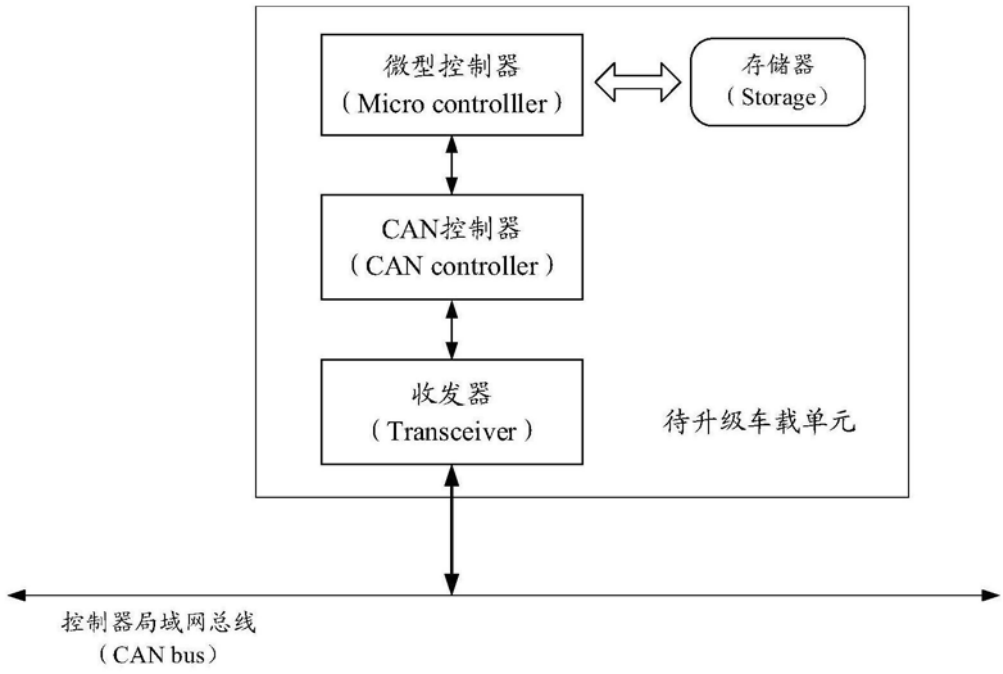

微型控制器
（Micro controlller）
存储器
（Storage）
CAN控制器
（CAN controller）
收发器
（Transceiver）
待升级车载单元
控制器局域网总线
（CAN bus）

图7

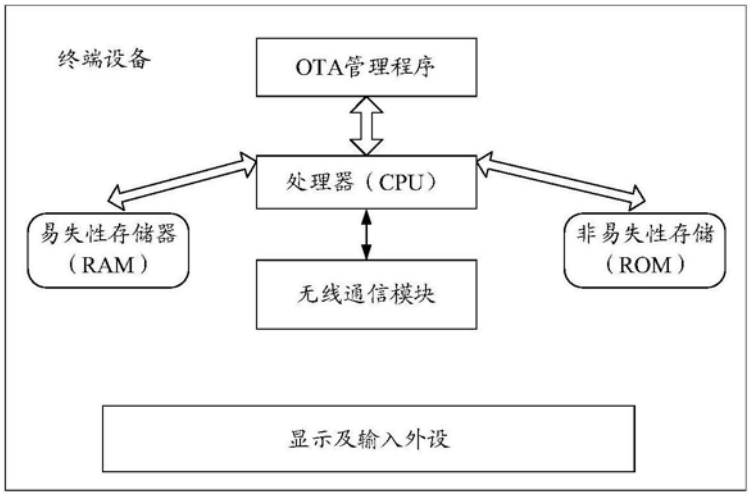

终端设备
OTA管理程序
处理器（CPU）
易失性存储器（RAM）
非易失性存储（ROM）
无线通信模块
显示及输入外设

图8

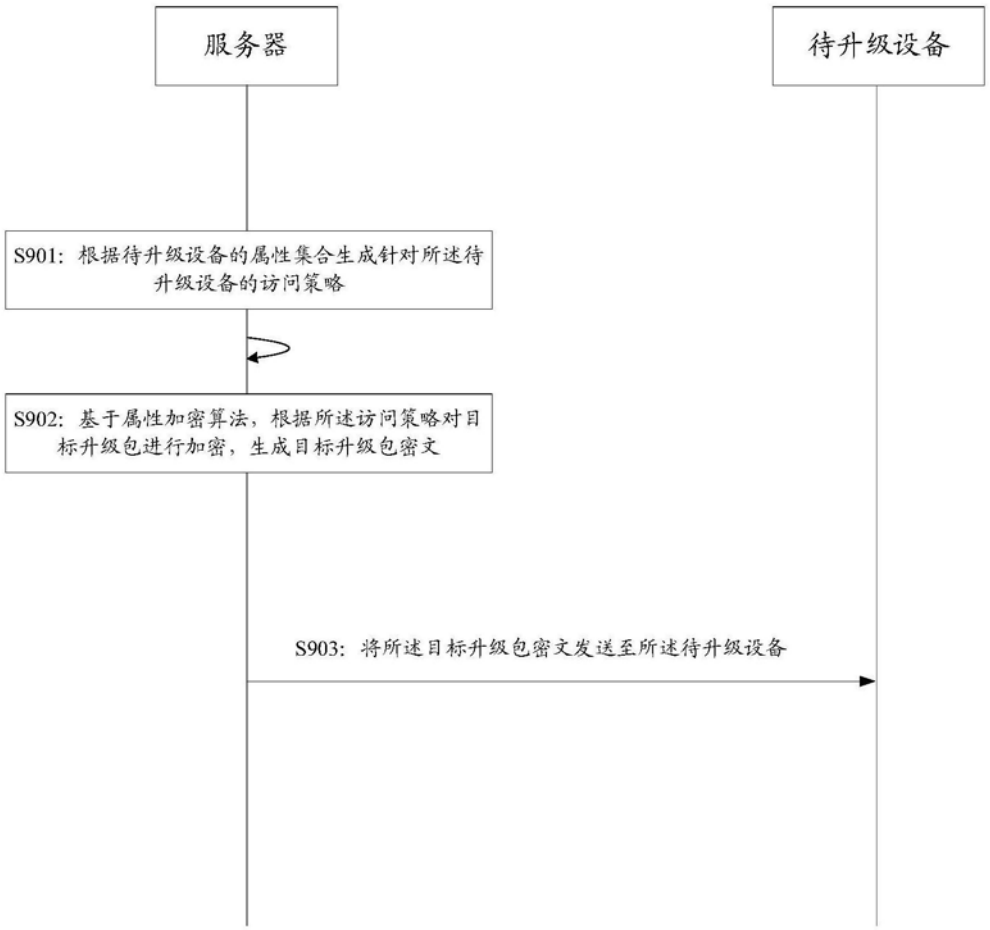

服务器
待升级设备
S901：根据待升级设备的属性集合生成针对所述待升级设备的访问策略
S902：基于属性加密算法，根据所述访问策略对目标升级包进行加密，生成目标升级包密文
S903：将所述目标升级包密文发送至所述待升级设备

图9

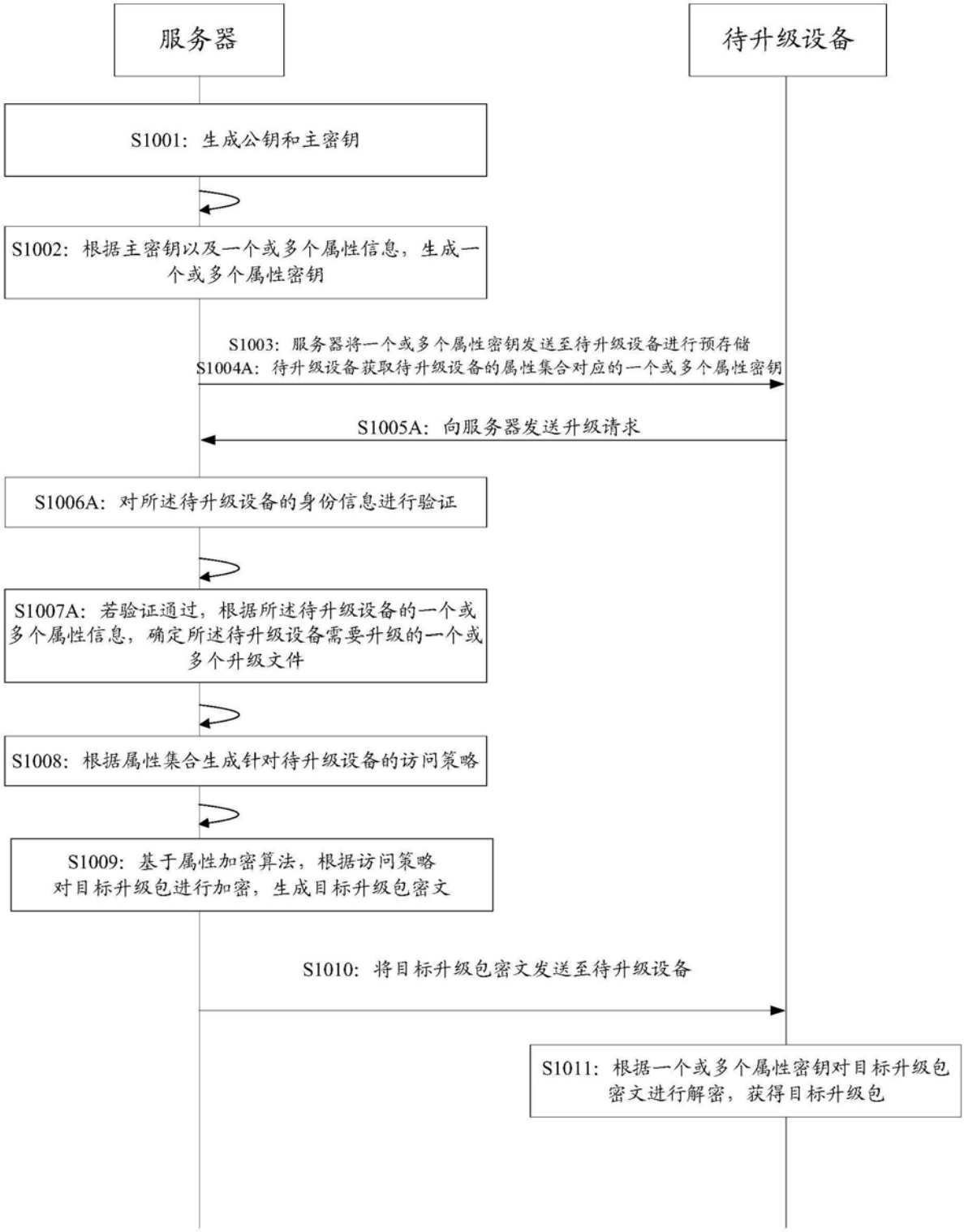

服务器
待升级设备
S1001：生成公钥和主密钥
S1002：根据主密钥以及一个或多个属性信息，生成一个或多个属性密钥
S1003：服务器将一个或多个属性密钥发送至待升级设备进行预存储
S1004A：待升级设备获取待升级设备的属性集合对应的一个或多个属性密钥
S1005A：向服务器发送升级请求
S1006A：对所述待升级设备的身份信息进行验证
S1007A：若验证通过，根据所述待升级设备的一个或多个属性信息，确定所述待升级设备需要升级的一个或多个升级文件
S1008：根据属性集合生成针对待升级设备的访问策略
S1009：基于属性加密算法，根据访问策略对目标升级包进行加密，生成目标升级包密文
S1010：将目标升级包密文发送至待升级设备
S1011：根据一个或多个属性密钥对目标升级包密文进行解密，获得目标升级包

图10

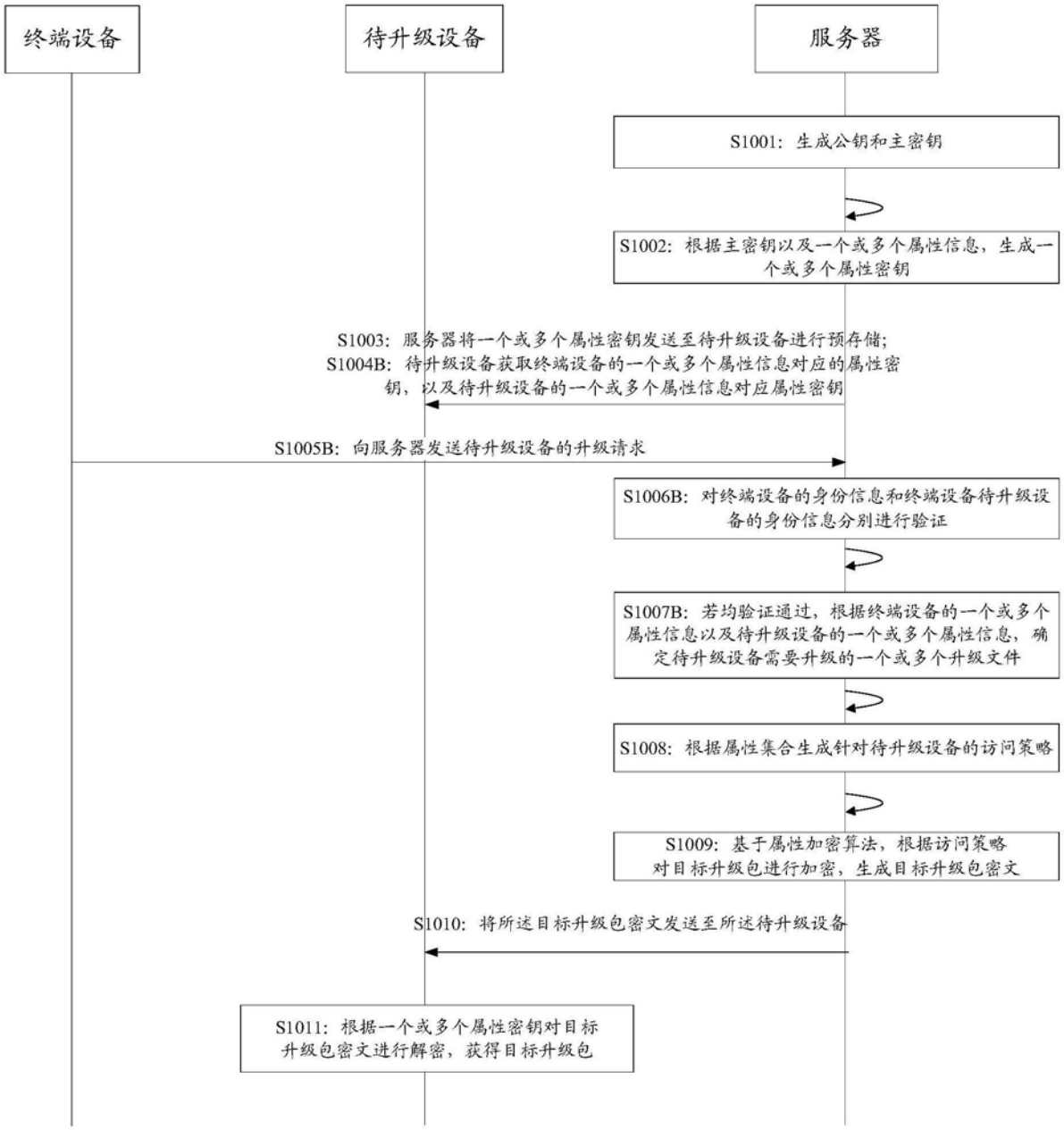

终端设备
待升级设备
服务器
S1001：生成公钥和主密钥
S1002：根据主密钥以及一个或多个属性信息，生成一个或多个属性密钥
S1003：服务器将一个或多个属性密钥发送至待升级设备进行预存储；
S1004B：待升级设备获取终端设备的一个或多个属性信息对应的属性密钥，以及待升级设备的一个或多个属性信息对应属性密钥
S1005B：向服务器发送待升级设备的升级请求
S1006B：对终端设备的身份信息和终端设备待升级设备的身份信息分别进行验证
S1007B：若均验证通过，根据终端设备的一个或多个属性信息以及待升级设备的一个或多个属性信息，确定待升级设备需要升级的一个或多个升级文件
S1008：根据属性集合生成针对待升级设备的访问策略
S1009：基于属性加密算法，根据访问策略对目标升级包进行加密，生成目标升级包密文
S1010：将所述目标升级包密文发送至所述待升级设备
S1011：根据一个或多个属性密钥对目标升级包密文进行解密，获得目标升级包

图11

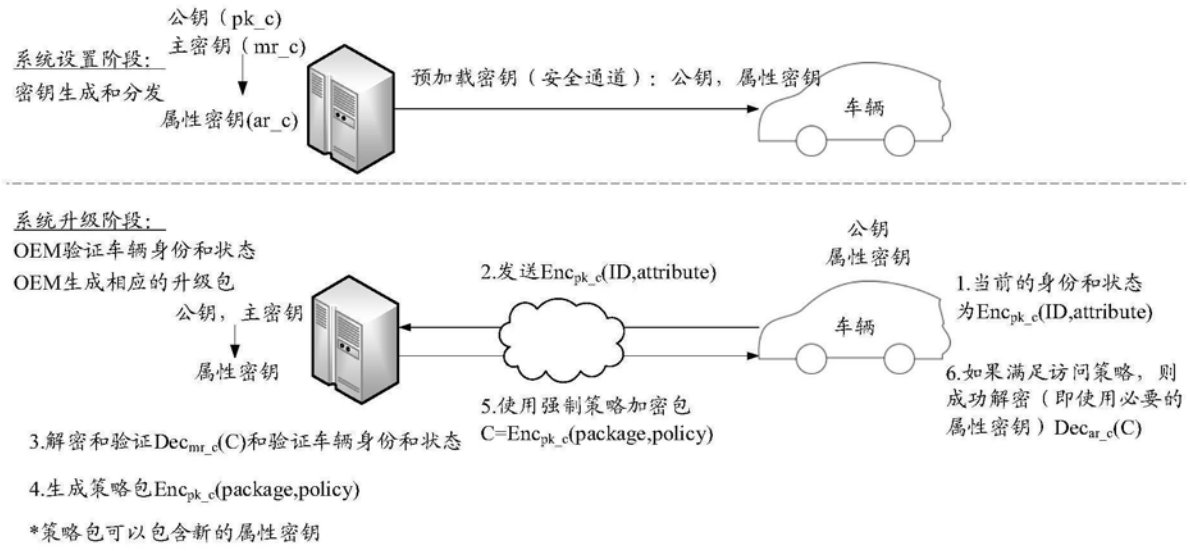

公钥（pk_c）
主密钥（mr_c）
系统设置阶段：
密钥生成和分发
属性密钥(ar_c)
预加载密钥（安全通道）：公钥，属性密钥
车辆
系统升级阶段：
OEM验证车辆身份和状态
OEM生成相应的升级包
公钥，主密钥
属性密钥
2.发送Enc_pk_c(ID,attribute)
公钥
属性密钥
1.当前的身份和状态为Enc_pk_c(ID,attribute)
车辆
6.如果满足访问策略，则成功解密（即使用必要的属性密钥）Dec_ar_c(C)
5.使用强制策略加密包
C=Enc_pk_c(package,policy)
3.解密和验证Dec_mr_c(C)和验证车辆身份和状态
4.生成策略包Enc_pk_c(package,policy)
*策略包可以包含新的属性密钥

图12

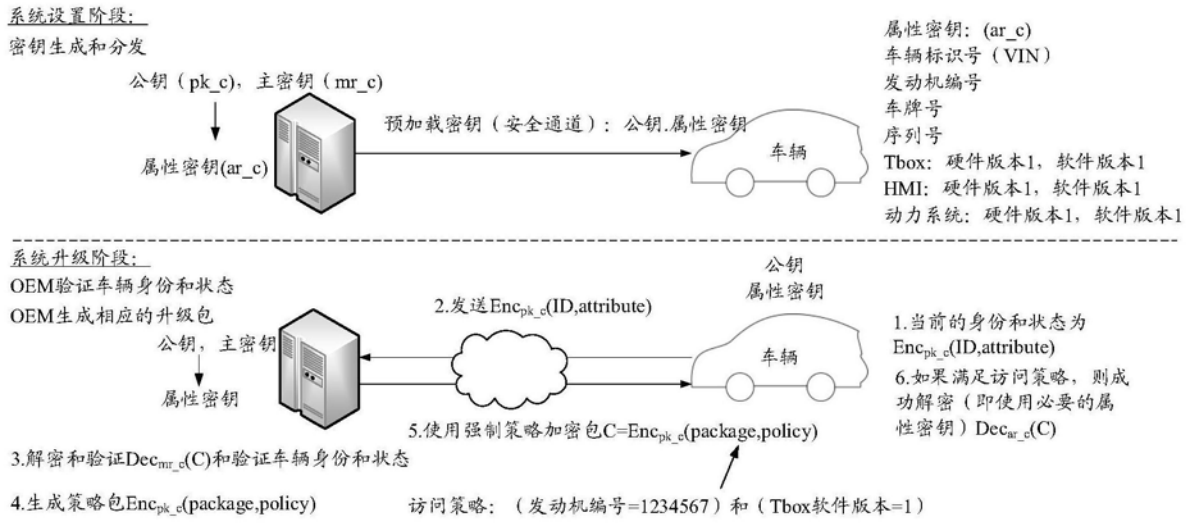

系统设置阶段：
密钥生成和分发
公钥（pk_c），主密钥（mr_c）
属性密钥(ar_c)
预加载密钥（安全通道）：公钥.属性密钥
车辆
属性密钥：(ar_c)
车辆标识号（VIN）
发动机编号
车牌号
序列号
Tbox：硬件版本1，软件版本1
HMI：硬件版本1，软件版本1
动力系统：硬件版本1，软件版本1
系统升级阶段：
OEM验证车辆身份和状态
OEM生成相应的升级包
公钥，主密钥
属性密钥
2.发送Enc_pk_c(ID,attribute)
公钥
属性密钥
车辆
1.当前的身份和状态为Enc_pk_c(ID,attribute)
6.如果满足访问策略，则成功解密（即使用必要的属性密钥）Dec_ar_c(C)
5.使用强制策略加密包C=Enc_pk_c(package,policy)
3.解密和验证Dec_mr_c(C)和验证车辆身份和状态
4.生成策略包Enc_pk_c(package,policy)
访问策略：（发动机编号=1234567）和（Tbox软件版本=1）

图13

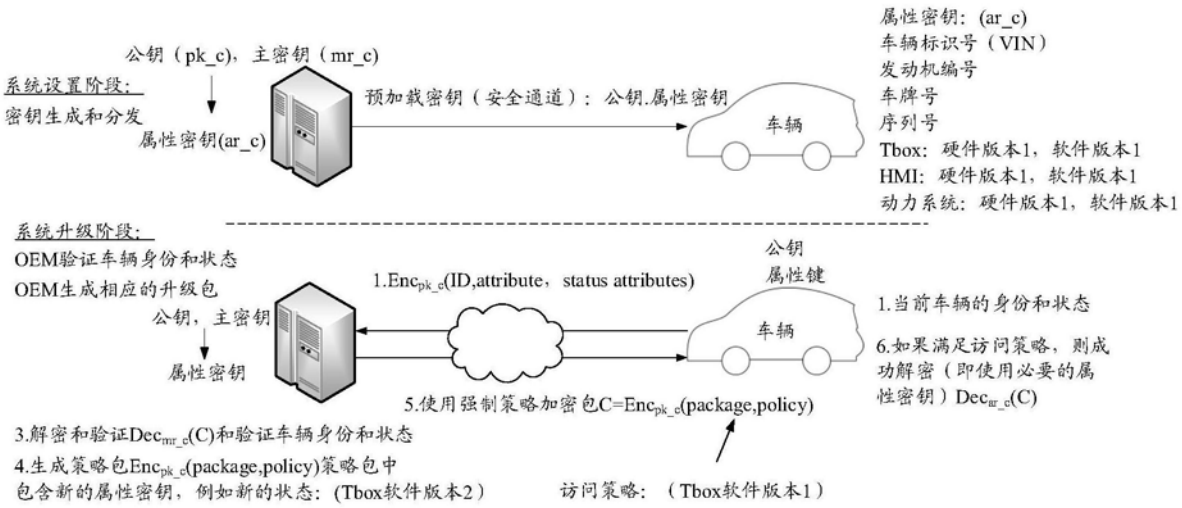

公钥（pk_c），主密钥（mr_c）
系统设置阶段：
密钥生成和分发
属性密钥(ar_c)
预加载密钥（安全通道）：公钥.属性密钥
车辆
属性密钥：(ar_c)
车辆标识号（VIN）
发动机编号
车牌号
序列号
Tbox：硬件版本1，软件版本1
HMI：硬件版本1，软件版本1
动力系统：硬件版本1，软件版本1
系统升级阶段：
OEM验证车辆身份和状态
OEM生成相应的升级包
公钥，主密钥
属性密钥
1.Enc_pk_c(ID,attribute，status attributes)
公钥
属性键
车辆
1.当前车辆的身份和状态
6.如果满足访问策略，则成功解密（即使用必要的属性密钥）Dec_ar_c(C)
5.使用强制策略加密包C=Enc_pk_c(package,policy)
3.解密和验证Dec_mr_c(C)和验证车辆身份和状态
4.生成策略包Enc_pk_c(package,policy)策略包中包含新的属性密钥，例如新的状态：(Tbox软件版本2）
访问策略：（Tbox软件版本1）

图14

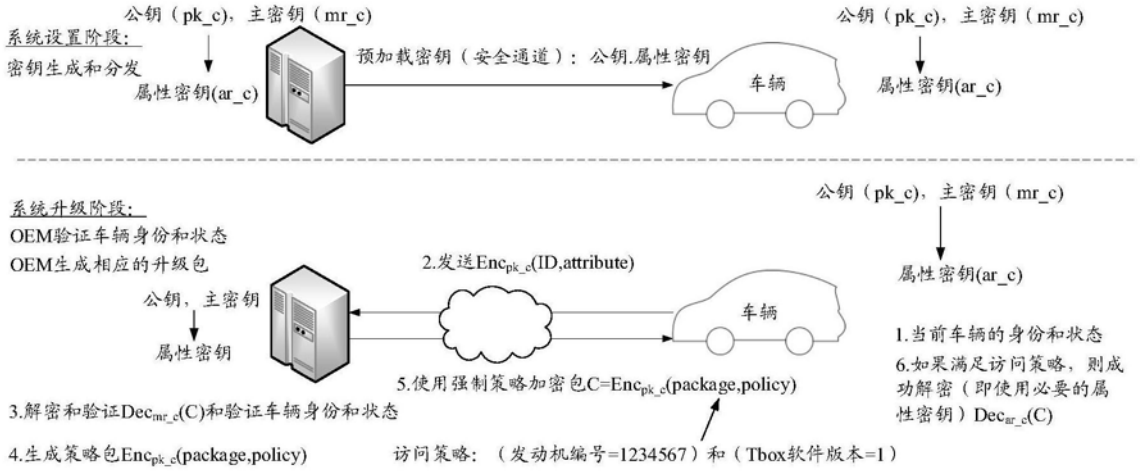

公钥（pk_c），主密钥（mr_c）
系统设置阶段：
密钥生成和分发
属性密钥(ar_c)
预加载密钥（安全通道）：公钥.属性密钥
车辆
公钥（pk_c），主密钥（mr_c）
属性密钥(ar_c)
系统升级阶段：
OEM验证车辆身份和状态
OEM生成相应的升级包
公钥，主密钥
属性密钥
2.发送Enc_pk_c(ID,attribute)
车辆
公钥（pk_c），主密钥（mr_c）
属性密钥(ar_c)
1.当前车辆的身份和状态
6.如果满足访问策略，则成功解密（即使用必要的属性密钥）Dec_ar_c(C)
5.使用强制策略加密包C=Enc_pk_c(package,policy)
3.解密和验证Dec_mr_c(C)和验证车辆身份和状态
4.生成策略包Enc_pk_c(package,policy)
访问策略：（发动机编号=1234567）和（Tbox软件版本=1）

图15

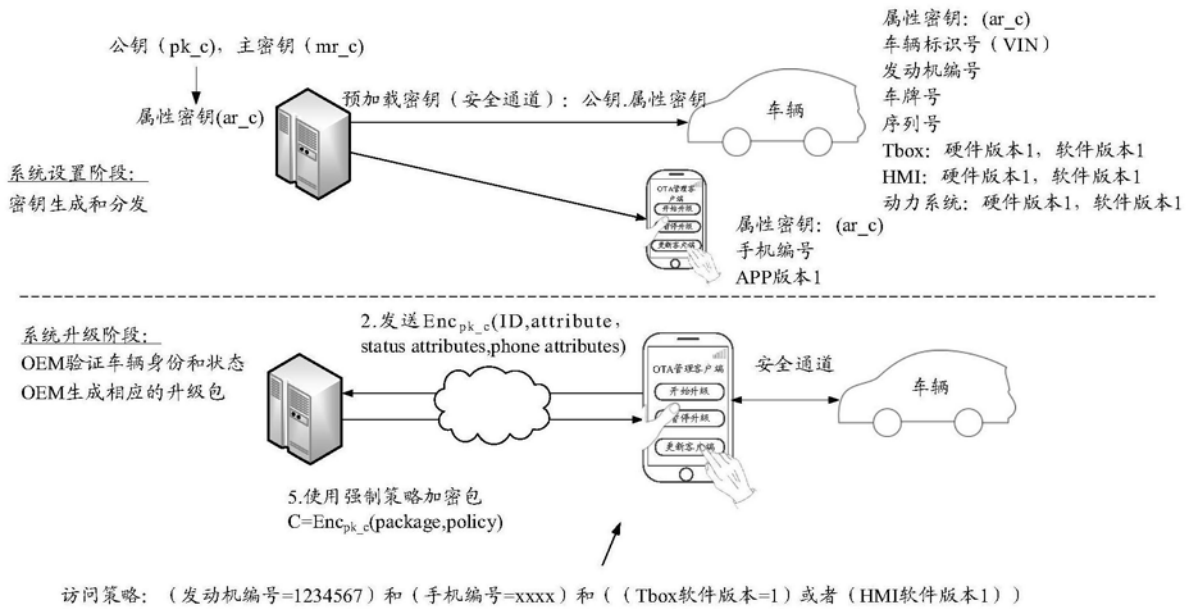

公钥（pk_c），主密钥（mr_c）
属性密钥(ar_c)
预加载密钥（安全通道）：公钥.属性密钥
车辆
属性密钥：(ar_c)
车辆标识号（VIN）
发动机编号
车牌号
序列号
Tbox：硬件版本1，软件版本1
HMI：硬件版本1，软件版本1
动力系统：硬件版本1，软件版本1
系统设置阶段：
密钥生成和分发
属性密钥：(ar_c)
手机编号
APP版本1
系统升级阶段：
OEM验证车辆身份和状态
OEM生成相应的升级包
2.发送Enc pk_c(ID,attribute，
status attributes,phone attributes)
安全通道
车辆
5.使用强制策略加密包
C=Enc pk_c(package,policy)
访问策略：（发动机编号=1234567）和（手机编号=xxxx）和（（Tbox软件版本=1）或者（HMI软件版本1））

图16

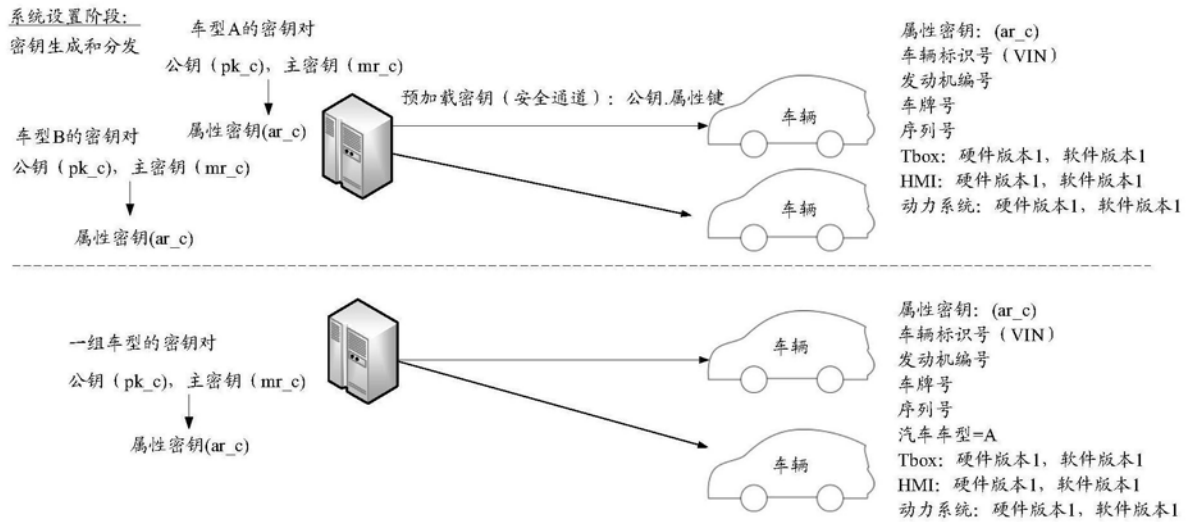

系统设置阶段：
密钥生成和分发
车型A的密钥对
公钥（pk_c），主密钥（mr_c）
属性密钥(ar_c)
预加载密钥（安全通道）：公钥.属性键
车辆
车辆
属性密钥：(ar_c)
车辆标识号（VIN）
发动机编号
车牌号
序列号
Tbox：硬件版本1，软件版本1
HMI：硬件版本1，软件版本1
动力系统：硬件版本1，软件版本1
车型B的密钥对
公钥（pk_c），主密钥（mr_c）
属性密钥(ar_c)
一组车型的密钥对
公钥（pk_c），主密钥（mr_c）
属性密钥(ar_c)
车辆
车辆
属性密钥：(ar_c)
车辆标识号（VIN）
发动机编号
车牌号
序列号
汽车车型=A
Tbox：硬件版本1，软件版本1
HMI：硬件版本1，软件版本1
动力系统：硬件版本1，软件版本1

图17

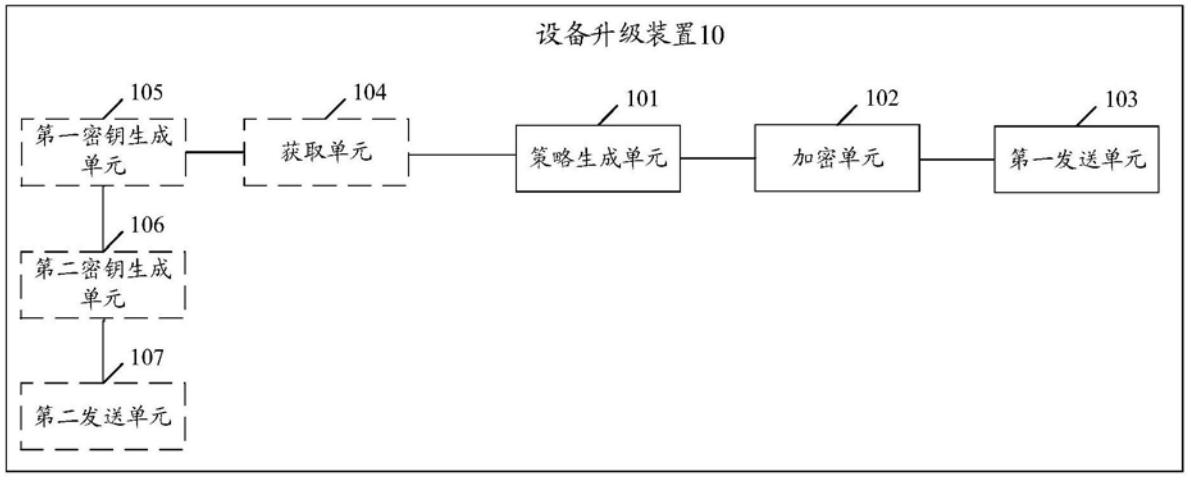

设备升级装置10
105
第一密钥生成单元
104
获取单元
101
策略生成单元
102
加密单元
103
第一发送单元
106
第二密钥生成单元
107
第二发送单元

图18

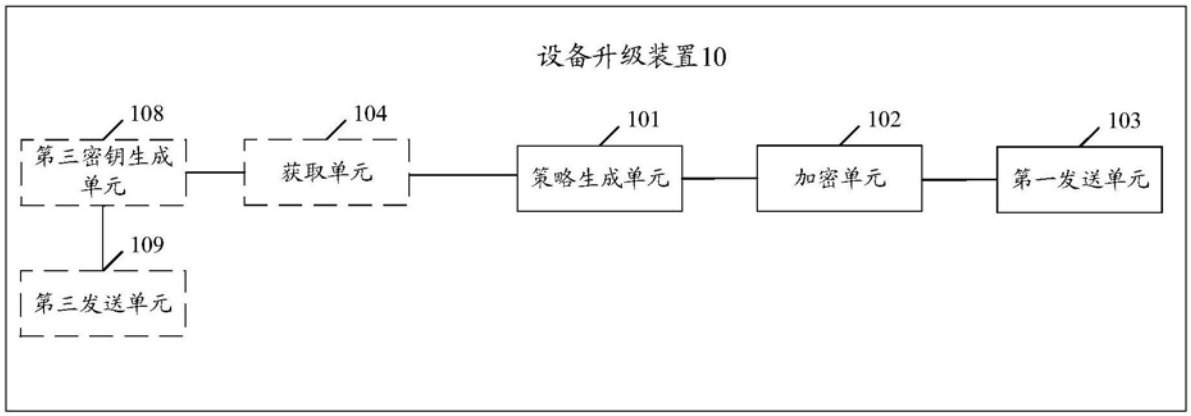

设备升级装置10
108
第三密钥生成单元
104
获取单元
101
策略生成单元
102
加密单元
103
第一发送单元
109
第三发送单元

图19

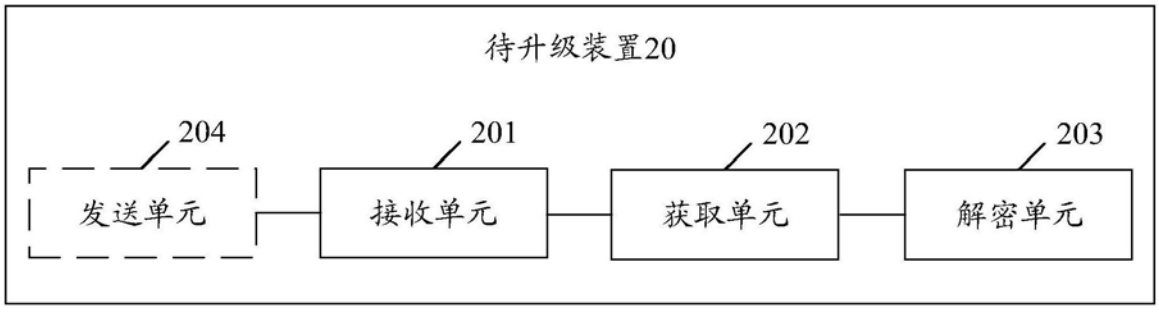

待升级装置20
204
发送单元
201
接收单元
202
获取单元
203
解密单元

图20

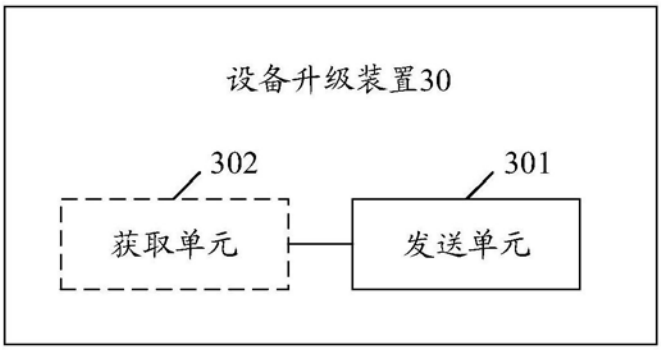

设备升级装置30
302
301
获取单元
发送单元

图21

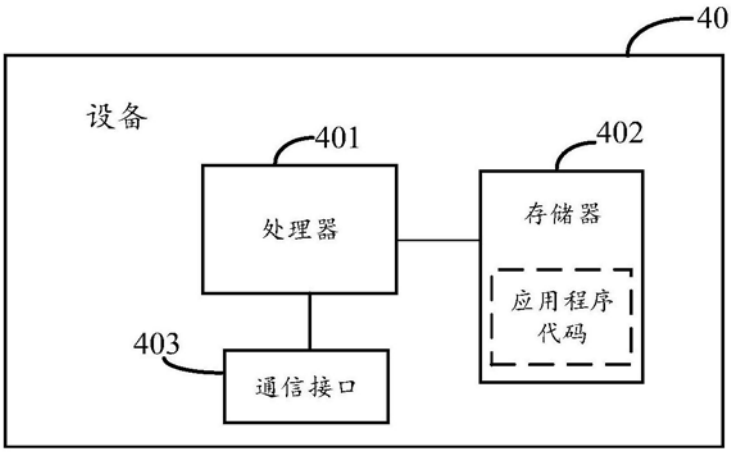

40
设备
401
402
处理器
存储器
应用程序
代码
403
通信接口

图22