(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112543927 B
(45)授权公告日 2023.03.24

(21)申请号 201980052751.9
(22)申请日 2019.04.17
(65)同一申请的已公布的文献号
申请公布号 CN 112543927 A
(43)申请公布日 2021.03.23
(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/CN2019/083069 2019.04.17
(87)PCT国际申请的公布数据
WO2020/211016 ZH 2020.10.22
(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 杨艳江 魏卓 雅丝敏·瑞哈娜 刘旭涛

(74)专利代理机构 广州三环专利商标代理有限公司 44202
专利代理师 熊永强 李稷芳
(51)Int.Cl.
G06F 21/51(2006.01)

(56)对比文件
CN 108923933 A,2018.11.30
CN 109214168 A,2019.01.15
CN 108196867 A,2018.06.22
CN 108880859 A,2018.11.23
CN 109495307 A,2019.03.19

审查员 翟紫伶

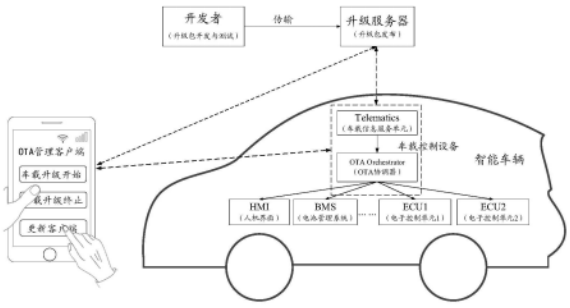
权利要求书4页 说明书36页 附图13页

(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，其中的方法包括控制设备接收通信设备发送的第一升级文件数据，第一升级文件数据为通信设备利用第一密钥对升级文件进行第一安全处理后生成的升级文件数据；控制设备利用第二密钥对第一升级文件数据进行第二安全处理，生成第二升级文件数据，并向待升级设备发送第二升级文件数据；待升级设备接收第二升级文件数据，利用相应的校验密钥对第二升级文件数据进行安全校验，若校验通过，则利用升级文件进行升级。设备升级方法及相关设备可以应用于智能家居、智能驾驶等多个技术领域，用于保障家用设备或车载设备的安全高效的升级。



CN 112543927 B

1.一种设备升级方法,其特征在于,应用于设备升级系统,所述设备升级系统包括控制设备和待升级设备;所述方法包括:

所述控制设备接收通信设备发送的第一升级文件数据,所述第一升级文件数据为所述通信设备利用第一密钥对升级文件进行第一安全处理后生成的升级文件数据;

所述控制设备利用第二密钥对所述第一升级文件数据进行第二安全处理,生成第二升级文件数据,并向所述待升级设备发送所述第二升级文件数据;

所述待升级设备接收所述第二升级文件数据,利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验,若校验通过,则利用所述升级文件进行升级;其中,所述第三密钥为所述第一密钥匹配的校验密钥,所述第四密钥为所述第二密钥匹配的校验密钥;所述第一密钥和所述第三密钥为对称密钥,所述第二密钥和所述第四密钥为对称密钥;

其中,所述控制设备生成目标密钥,将所述目标密钥拆分为所述第一密钥和所述第二密钥,将所述目标密钥发送至所述待升级设备,将所述第一密钥发送至所述通信设备;所述控制设备存储所述第二密钥,并删除所述目标密钥;或者,所述待升级设备生成目标密钥,将所述目标密钥拆分为所述第一密钥和所述第二密钥,将所述第一密钥发送给所述通信设备,以及将所述第二密钥发送给所述控制设备;所述待升级设备存储所述目标密钥,并删除所述第一密钥和所述第二密钥。

2.根据权利要求1所述的方法,其特征在于,所述第一安全处理包括根据所述第一密钥生成所述升级文件的第一消息认证码MAC;所述第一升级文件数据包括所述升级文件和所述第一MAC。

3.根据权利要求2所述的方法,其特征在于,所述第二安全处理包括根据所述第二密钥生成所述升级文件的第二MAC,并将所述第一MAC和所述第二MAC聚合得到第三MAC;所述第二升级文件数据包括所述升级文件和所述第三MAC。

4.根据权利要求2所述的方法,其特征在于,所述第二安全处理包括根据所述第二密钥生成所述第一升级文件数据的第四MAC;所述第二升级文件数据包括所述升级文件和所述第四MAC。

5.根据权利要求1所述的方法,其特征在于,所述方法还包括:

所述待升级设备在利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验之前,将存储的所述目标密钥拆分为所述第三密钥和所述第四密钥。

6.一种设备升级系统,其特征在于,包括通信设备、控制设备和待升级设备;其中,

所述通信设备,用于利用第一密钥对升级文件进行第一安全处理,生成第一升级文件数据,并向所述控制设备发送所述第一升级文件数据;

所述控制设备,用于接收所述通信设备发送的第一升级文件数据,利用第二密钥对所述第一升级文件数据进行第二安全处理,生成第二升级文件数据,并向所述待升级设备发送所述第二升级文件数据;

所述待升级设备,用于接收所述第二升级文件数据,利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验,若校验通过,则利用所述升级文件进行升级;其中,所述第三密钥为所述第一密钥匹配的校验密钥,所述第四密钥为所述第二密钥匹配的校验密钥;

所述第一密钥和所述第三密钥为对称密钥,所述第二密钥和所述第四密钥为对称密

钥；

所述待升级设备，还用于：

生成目标密钥，将所述目标密钥拆分为所述第一密钥和所述第二密钥；

将所述第一密钥发送给所述通信设备，以及将所述第二密钥发送给所述控制设备；

存储所述目标密钥，并删除所述第一密钥和所述第二密钥；

所述通信设备，还用于接收所述待升级设备发送的所述第一密钥，并存储所述第一密钥。

7.根据权利要求6所述的系统，其特征在于，所述第一密钥和所述第三密钥为对称密钥，所述第二密钥和所述第四密钥为对称密钥；

所述控制设备，还用于：

生成目标密钥，将所述目标密钥拆分为所述第一密钥和所述第二密钥；

将所述目标密钥发送至所述待升级设备，将所述第一密钥发送至所述通信设备；

存储所述第二密钥，并删除所述目标密钥；

所述通信设备，还用于接收所述控制设备发送的所述第一密钥，并存储所述第一密钥。

8.根据权利要求6或7所述的系统，其特征在于，

所述待升级设备，还用于在利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验之前，将存储的所述目标密钥拆分为所述第三密钥和所述第四密钥。

9.一种设备升级系统，其特征在于，包括控制设备和待升级设备；其中，

所述控制设备，用于：

接收通信设备发送的第一升级文件数据，所述第一升级文件数据为所述通信设备利用第一密钥对升级文件进行第一安全处理后生成的升级文件数据；

利用第二密钥对所述第一升级文件数据进行第二安全处理，生成第二升级文件数据，并向所述待升级设备发送所述第二升级文件数据；

所述待升级设备，用于接收所述第二升级文件数据，利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验，若校验通过，则利用所述升级文件进行升级；其中，所述第三密钥为所述第一密钥匹配的校验密钥，所述第四密钥为所述第二密钥匹配的校验密钥；

所述第一密钥和所述第三密钥为对称密钥，所述第二密钥和所述第四密钥为对称密钥；

所述控制设备，还用于：

生成目标密钥，将所述目标密钥拆分为所述第一密钥和所述第二密钥；

将所述目标密钥发送至所述待升级设备，将所述第一密钥发送至所述通信设备；

存储所述第二密钥，并删除所述目标密钥。

10.根据权利要求9所述的系统，其特征在于，所述第一密钥和所述第三密钥为对称密钥，所述第二密钥和所述第四密钥为对称密钥；

所述待升级设备，还用于：

生成目标密钥，将所述目标密钥拆分为所述第一密钥和所述第二密钥；

将所述第一密钥发送给所述通信设备，以及将所述第二密钥发送给所述控制设备；

存储所述目标密钥，并删除所述第一密钥和所述第二密钥。

11.根据权利要求9或10所述的系统,其特征在于,

所述待升级设备,还用于在利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验之前,将存储的所述目标密钥拆分为所述第三密钥和所述第四密钥。

12.一种通信设备,其特征在于,包括:

安全处理单元,用于利用第一密钥对升级文件进行第一安全处理,生成第一升级文件数据;

发送单元,用于向控制设备发送所述第一升级文件数据;其中,

所述第一升级文件数据用于所述控制设备利用第二密钥对所述第一升级文件数据进行第二安全处理,生成第二升级文件数据,并向待升级设备发送所述第二升级文件数据;

所述第二升级文件数据用于所述待升级设备利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验,若校验通过,则利用所述升级文件进行升级;其中,所述第三密钥为所述第一密钥匹配的校验密钥,所述第四密钥为所述第二密钥匹配的校验密钥;所述第一密钥和所述第三密钥为对称密钥,所述第二密钥和所述第四密钥为对称密钥;

所述第一密钥和所述第二密钥为所述控制设备将生成的目标密钥拆分后的密钥,其中,所述目标密钥还用于由所述控制设备发送至所述待升级设备进行存储;所述通信设备还包括:接收单元,用于接收所述控制设备发送的所述第一密钥;或者所述第一密钥和所述第二密钥为所述待升级设备将生成的目标密钥拆分后的密钥;所述通信设备还包括:接收单元,用于接收所述待升级设备发送的所述第一密钥。

13.一种控制设备,其特征在于,包括:

第一接收单元,用于接收通信设备发送的第一升级文件数据,所述第一升级文件数据为所述通信设备利用第一密钥对升级文件进行第一安全处理后生成的升级文件数据;

安全处理单元,用于利用第二密钥对所述第一升级文件数据进行第二安全处理,生成第二升级文件数据,并向待升级设备发送所述第二升级文件数据;其中,

所述第二升级文件数据,用于所述待升级设备所述利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验,若校验通过,则利用所述升级文件进行升级;其中,所述第三密钥为所述第一密钥匹配的校验密钥,所述第四密钥为所述第二密钥匹配的校验密钥;所述第一密钥和所述第三密钥为对称密钥,所述第二密钥和所述第四密钥为对称密钥;

所述控制设备还包括:密钥生成单元,用于生成目标密钥,将所述目标密钥拆分为所述第一密钥和所述第二密钥;发送单元,用于将所述目标密钥发送至所述待升级设备,将所述第一密钥发送至所述通信设备;密钥存储单元,用于存储所述第二密钥,并删除所述目标密钥;或者,所述第一密钥和所述第二密钥为所述待升级设备将生成的目标密钥拆分后的密钥;所述控制设备还包括:第二接收单元,用于接收所述待升级设备发送的所述第二密钥。

14.一种待升级设备,其特征在于,包括:

第一接收单元,用于接收控制设备发送的第二升级文件数据,所述第二升级文件数据为所述控制设备利用第二密钥对通信设备发送的第一升级文件数据进行第二安全处理,生成的升级文件数据,所述第一升级文件数据为所述通信设备利用第一密钥对升级文件进行第一安全处理后生成的升级文件数据;

安全校验单元,用于利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验,所述第三密钥为所述第一密钥匹配的校验密钥,所述第四密钥为所述第二密钥匹配的

校验密钥；

升级单元，用于若校验通过，则利用所述升级文件进行升级；

所述第一密钥和所述第三密钥为对称密钥，所述第二密钥和所述第四密钥为对称密钥；

其中，所述第一密钥和所述第二密钥为所述控制设备将生成的目标密钥拆分后的密钥，所述待升级设备还包括：第二接收单元，用于接收所述控制设备发送的所述目标密钥；或者，所述待升级设备还包括：第一密钥生成单元，用于生成目标密钥，将所述目标密钥拆分为所述第一密钥和所述第二密钥；发送单元，用于将所述第一密钥发送给所述通信设备，以及将所述第二密钥发送给所述控制设备；密钥存储单元，用于存储所述目标密钥，并删除所述第一密钥和所述第二密钥。

15.一种智能车辆，其特征在于，应用于车载系统，所述车载系统包括车载控制设备和待升级车载设备；其中，

所述车载控制设备，用于接收通信设备发送的第一升级文件数据，所述第一升级文件数据为所述通信设备利用第一密钥对升级文件进行第一安全处理后生成的升级文件数据；

所述车载控制设备，用于利用第二密钥对所述第一升级文件数据进行第二安全处理，生成第二升级文件数据，并向所述待升级车载设备发送所述第二升级文件数据；

所述待升级车载设备，用于接收所述第二升级文件数据，利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验，若校验通过，则利用所述升级文件进行升级；其中，所述第三密钥为所述第一密钥匹配的校验密钥，所述第四密钥为所述第二密钥匹配的校验密钥；所述第一密钥和所述第三密钥为对称密钥，所述第二密钥和所述第四密钥为对称密钥；

所述车载控制设备，还用于生成目标密钥，将所述目标密钥拆分为所述第一密钥和所述第二密钥；将所述目标密钥发送至所述待升级车载设备，将所述第一密钥发送至所述通信设备；存储所述第二密钥，并删除所述目标密钥；或者，所述待升级车载设备，用于生成目标密钥，将所述目标密钥拆分为所述第一密钥和所述第二密钥；将所述第一密钥发送给所述通信设备，以及将所述第二密钥发送给所述车载控制设备；存储所述目标密钥，并删除所述第一密钥和所述第二密钥。

16.根据权利要求15所述的车辆，其特征在于，

所述待升级车载设备，还用于在利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验之前，将存储的所述目标密钥拆分为所述第三密钥和所述第四密钥。

17.一种芯片系统，其特征在于，所述芯片系统包括至少一个处理器，存储器和接口电路，所述存储器、所述接口电路和所述至少一个处理器通过线路互联，所述至少一个存储器中存储有指令；所述指令被所述处理器执行时，权利要求1－5中任意一项所述的方法得以实现。

18.一种计算机存储介质，其特征在于，所述计算机存储介质存储有计算机程序，该计算机程序被控制设备或升级设备执行时实现上述权利要求1－5任意一项所述的方法。

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。传统待升级车载设备的固件/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,升级文件被非法窃取或者篡改,车载设备内部的安全处理密钥被非法窃取或篡改等,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,可应用于设备升级系统,所述设备升级系统包括控制设备和待升级设备;所述方法可包括:

[0008] 所述控制设备接收通信设备发送的第一升级文件数据,所述第一升级文件数据为所述通信设备利用第一密钥对升级文件进行第一安全处理后生成的升级文件数据;

[0009] 所述控制设备利用第二密钥对所述第一升级文件数据进行第二安全处理,生成第二升级文件数据,并向所述待升级设备发送所述第二升级文件数据;

[0010] 所述待升级设备接收所述第二升级文件数据,利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验,若校验通过,则利用所述升级文件进行升级;其中,所述第三密钥为所述第一密钥匹配的校验密钥,所述第四密钥为所述第二密钥匹配的校验密钥。

[0011] 本发明实施例,通过在设备升级架构中,将设备升级系统中控制设备上用于与待升级设备之间进行安全传输的密钥(不同的待升级设备对应不同的密钥),分散存储到设备

升级系统以外的通信设备上，避免密钥以完整的形式存储在控制设备上，被攻击者轻易窃取或篡改；且由于该通信设备同时也是向设备升级系统传输升级文件的发送方，因此，除了上述分散存储部分密钥，进一步地，通信设备还可以在向控制设备发送升级文件时，利用存储的部分密钥(即第一密钥)对升级文件进行第一安全处理，然后发送给控制设备使其可以利用另一部分密钥(即第二密钥)进行进一步的安全处理，最终将该经过第一密钥和第二密钥共同安全处理的升级文件发送给待升级设备，而待升级设备则使用协商好的第三密钥和第四密钥进行安全校验。使得本应该在控制设备上单独完成的对升级文件的安全处理过程，分布在了通信设备和控制设备上来共完成，即分别由通信设备和控制设备使用各自的部分密钥参与到升级文件的安全处理中来，而无需将上述两个部分密钥恢复成完整密钥才对升级文件进行安全处理，进一步避免了完整密钥出现或存储在控制设备上，使得攻击者无法一次性从控制设备上获取到完整密钥，极大的减小了攻击者截获或篡改完整密钥的几率，从而保证了升级文件在设备升级系统内部传输的安全性。

[0012] 在一种可能的实现方式中，所述第一安全处理包括根据所述第一密钥生成所述升级文件的第一消息认证码MAC；所述第一升级文件数据包括所述升级文件和所述第一MAC。本发明实施例中，由于对升级文件生成消息认证码可以保证升级文件的完整性和来源的真实性，因此可以解决升级文件在设备升级系统中传输时，可能被攻击者篡改和伪造的问题，并且生成MAC的过程使用的是对称密钥，因此可以在保证数据安全性的基础上，减少安全校验的计算量，提升升级效率。

[0013] 在一种可能的实现方式中，所述第二安全处理包括根据所述第二密钥生成所述升级文件的第二MAC，并将所述第一MAC和所述第二MAC聚合得到第三MAC；所述第二升级文件数据包括所述升级文件和所述第三MAC。本发明实施例中，第一安全处理包括通信设备利用自身存储的第一密钥生成升级文件的第一MAC，第二安全处理则包括控制设备先利用自身存储的第二密钥生成升级文件的第二MAC，再对第一MAC和第二MAC进行聚合得到一个与升级文件以及第一密钥和第二密钥都相关的消息认证码，以便于待升级设备利用匹配的第三密钥和第四密钥对聚合后的消息认证码进行安全校验。且由于对升级文件生成消息认证码可以保证升级文件的完整性和来源的真实性，因此可以解决升级文件在设备升级系统中传输时，可能被攻击者篡改和伪造的问题，并且生成MAC的过程使用的是对称密钥，因此可以在保证数据安全性的基础上，减少安全校验的计算量，提升升级效率。

[0014] 在一种可能的实现方式中，所述第二安全处理包括根据所述第二密钥生成所述第一升级文件数据的第四MAC；所述第二升级文件数据包括所述升级文件和所述第四MAC。本发明实施例中，第一安全处理包括通信设备利用自身存储的第一密钥生成升级文件的第一MAC，第二安全处理则包括控制设备利用自身存储的第二密钥生成第一升级文件数据(包括升级文件和第一MAC)的第四MAC，即得到一个与升级文件以及第一密钥和第二密钥都相关的消息认证码，以便于待升级设备利用匹配的第三密钥和第四密钥对聚合后的消息认证码进行安全校验。且由于对升级文件生成消息认证码可以保证升级文件的完整性和来源的真实性，因此可以解决升级文件在设备升级系统中传输时，可能被攻击者篡改和伪造的问题，并且生成MAC的过程使用的是对称密钥，因此可以在保证数据安全性的基础上，减少安全校验的计算量，提升升级效率。

[0015] 在一种可能的实现方式中，所述第一密钥和所述第三密钥为对称密钥，所述第二

密钥和所述第四密钥为对称密钥;所述方法还包括:所述控制设备生成目标密钥,将所述目标密钥拆分为所述第一密钥和所述第二密钥;所述控制设备将所述目标密钥发送至所述待升级设备,将所述第一密钥发送至所述通信设备;所述控制设备存储所述第二密钥,并删除所述目标密钥。在本发明实施例中,第一密钥和第二密钥是由设备升级系统中的控制设备生成的目标密钥进行拆分得到的,且控制设备将拆分后得到的第一密钥发送给通信设备进行存储,以及将目标密钥发送给待升级设备进行存储,以保证完整密钥的分散存储,以及后续的分散使用。

[0016] 在一种可能的实现方式中,所述第一密钥和所述第三密钥为对称密钥,所述第二密钥和所述第四密钥为对称密钥;所述方法还包括:所述待升级设备生成目标密钥,将所述目标密钥拆分为所述第一密钥和所述第二密钥;所述待升级设备将所述第一密钥发送给所述通信设备,以及将所述第二密钥发送给所述控制设备;所述待升级设备存储所述目标密钥,并删除所述第一密钥和所述第二密钥。在本发明实施例中,第一密钥和第二密钥是由设备升级系统中的待升级设备生成的目标密钥进行拆分得到的,且待升级设备将拆分后得到的第一密钥发送给通信设备进行存储,以及将第二密钥发送给控制设备进行存储,以保证完整密钥的分散存储,以及后续的分散使用。

[0017] 在一种可能的实现方式中,所述方法还包括:所述待升级设备在利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验之前,将存储的所述目标密钥拆分为所述第三密钥和所述第四密钥。在本发明实施例中,无论是控制设备生成的目标密钥还是待升级设备生成的目标密钥,待升级设备在使用第三密钥和第四密钥之前,都需要对目标密钥进行拆分,得到第三密钥和第四密钥以进行安全校验。

[0018] 在一种可能的实现方式中,所述升级文件经过数字签名;所述第一升级文件数据为所述通信设备在获取所述升级文件,并对所述数字签名进行验签通过后,利用所述第一密钥对所述升级文件进行第一安全处理后生成的升级文件数据。本发明实施例中,通信设备在生成第一升级文件数据的过程中,若通信设备在获取到升级文件时,升级文件经过了数字签名,则还需要对升级文件先进行验签,若验签通过(例如服务器用私钥签名,通信设备用公钥验签),代表该升级文件是安全合法的,再对该升级文件进行第一安全处理,即通信设备需要先确认获取到的升级文件是安全合法的,才会进行进一步的安全处理,否则将放弃升级,以免威胁设备安全。

[0019] 在一种可能的实现方式中,所述第一升级文件数据中的升级文件还经过数字签名;所述控制设备利用第二密钥对所述第一升级文件数据进行第二安全处理之前,还包括:所述控制设备对所述数字签名进行验签,若验签通过,则利用所述第二密钥对所述第一升级文件数据进行第二安全处理。本发明实施例中,当通信设备确认了升级文件的安全合法性且进行了第一安全处理之后,可以在该第一升级文件数据中继续携带该数字签名,以防止在通信设备将第一升级文件数据发送给控制设备的过程中,遭到非法攻击者的篡改和伪造,因此相应地,控制设备也先对该数字签名进行验签,验签通过之后(例如服务器用私钥签名,通信设备用公钥验签),再进行第二安全处理。需要说明的是,由于接下来控制设备和待升级设备之间是通过与第一密钥和第二密钥相关的第二安全处理进行安全验证的,因此当控制设备向待升级设备发送第二升级文件数据时,则可以去掉数字签名,即待升级设备可以无需进行该数字签名的验签。

[0020] 在一种可能的实现方式中，所述方法还包括：所述待升级设备在根据所述升级文件升级成功后，向所述控制设备发送升级成功消息，所述升级成功消息为经过所述第四密钥的安全保护的消息。本发明实施例中，当待升级设备升级成功之后，可以向控制设备反馈升级成功的消息，为了保证该升级成功消息在待升级设备和控制设备之间的安全传输，该升级成功消息可以经过第四密钥的保护，而控制设备则可以利用已存储的第二密钥进行相应的安全校验，以达到复用第二密钥和第四密钥的效果，因而无需重新生成密钥，且节省存储空间。

[0021] 在一种可能的实现方式中，所述方法还包括：所述控制设备在确认所述待升级设备升级成功后，指示所述通信设备更新所述升级文件的回滚文件；和/或所述控制设备在确认所述待升级设备升级失败后，从所述通信设备获取所述升级文件的回滚文件，并发送给所述待升级设备进行回滚操作。本发明实施例，通信设备可以为设备升级系统提供升级文件的回滚文件，无论在待升级设备升级成功或者失败的情况下，通信设备都可以对当前的升级文件进行回滚操作，以便于待升级设备升级过程中有升级文件获取需求时，有回滚文件可以参考。

[0022] 在一种可能的实现方式中，所述第一密钥和所述第二密钥是由服务器生成目标密钥并拆分而来，并由所述服务器分别发送至所述通信设备和所述控制设备的。可选的，所述服务器生成目标密钥之后发送到所述控制设备或所述待升级车载设备上进行拆分。例如，所述服务器为升级服务器、密钥服务器或其它服务器等。本发明实施例中，目标密钥的生成和/或目标密钥的拆分过程可以是由服务器来执行，可减少控制设备和待升级设备的计算量，提升升级效率。

[0023] 在一种可能的实现方式中，所述第三密钥和所述第四密钥是由服务器拆分而来，再发送至所述待升级车载设备的。例如，所述服务器为升级服务器、密钥服务器或其它服务器等。本发明实施例中，第三密钥和第四密钥对应的原始密钥的生成和/或拆分，可以是由服务器来执行，可减少控制设备和待升级设备的计算量，提升升级效率。

[0024] 第二方面，本发明实施例提供了一种设备升级系统，可包括通信设备、控制设备和待升级设备；其中，所述通信设备，用于利用第一密钥对升级文件进行第一安全处理，生成第一升级文件数据，并向所述控制设备发送所述第一升级文件数据；所述控制设备，用于接收所述通信设备发送的第一升级文件数据，利用第二密钥对所述第一升级文件数据进行第二安全处理，生成第二升级文件数据，并向所述待升级设备发送所述第二升级文件数据；所述待升级设备，用于接收所述第二升级文件数据，利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验，若校验通过，则利用所述升级文件进行升级；其中，所述第三密钥为所述第一密钥匹配的校验密钥，所述第四密钥为所述第二密钥匹配的校验密钥。

[0025] 在一种可能的实现方式中，所述第一安全处理包括根据所述第一密钥生成所述升级文件的第一消息认证码MAC；所述第一升级文件数据包括所述升级文件和所述第一MAC。

[0026] 在一种可能的实现方式中，所述第二安全处理包括根据所述第二密钥生成所述升级文件的第二MAC，并将所述第一MAC和所述第二MAC聚合得到第三MAC；所述第二升级文件数据包括所述升级文件和所述第三MAC。

[0027] 在一种可能的实现方式中，所述第二安全处理包括根据所述第二密钥生成所述第一升级文件数据的第四MAC；所述第二升级文件数据包括所述升级文件和所述第四MAC。

[0028] 在一种可能的实现方式中，所述第一密钥和所述第三密钥为对称密钥，所述第二密钥和所述第四密钥为对称密钥；所述控制设备，还用于：生成目标密钥，将所述目标密钥拆分为所述第一密钥和所述第二密钥；将所述目标密钥发送至所述待升级设备，将所述第一密钥发送至所述通信设备；存储所述第二密钥，并删除所述目标密钥；所述通信设备，还用于接收所述控制设备发送的所述第一密钥，并存储所述第一密钥。

[0029] 在一种可能的实现方式中，所述第一密钥和所述第三密钥为对称密钥，所述第二密钥和所述第四密钥为对称密钥；所述待升级设备，还用于：生成目标密钥，将所述目标密钥拆分为所述第一密钥和所述第二密钥；将所述第一密钥发送给所述通信设备，以及将所述第二密钥发送给所述控制设备；存储所述目标密钥，并删除所述第一密钥和所述第二密钥；所述通信设备，还用于接收所述待升级设备发送的所述第一密钥，并存储所述第一密钥。

[0030] 在一种可能的实现方式中，所述待升级设备，还用于在利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验之前，将存储的所述目标密钥拆分为所述第三密钥和所述第四密钥。

[0031] 在一种可能的实现方式中，所述升级文件经过数字签名；所述通信设备，具体用于获取所述升级文件，并对所述数字签名进行验签，若验签通过，则利用所述第一密钥对所述升级文件进行第一安全处理。

[0032] 在一种可能的实现方式中，所述第一升级文件数据中的升级文件还经过数字签名；所述控制设备，还用于在利用第二密钥对所述第一升级文件数据进行第二安全处理之前，对所述数字签名进行验签，若验签通过，则利用所述第二密钥对所述第一升级文件数据进行第二安全处理。

[0033] 在一种可能的实现方式中，所述待升级设备，还用于在根据所述升级文件升级成功后，向所述控制设备发送升级成功消息，所述升级成功消息为经过所述第四密钥的安全保护的消息。

[0034] 在一种可能的实现方式中，所述控制设备，还用于在确认所述待升级设备升级成功后，指示所述通信设备更新所述升级文件的回滚文件；和/或所述控制设备，还用于在确认所述待升级设备升级失败后，从所述通信设备获取所述升级文件的回滚文件，并发送给所述待升级设备进行回滚操作。

[0035] 在一种可能的实现方式中，所述第一密钥和所述第二密钥是由服务器生成目标密钥并拆分而来，并由所述服务器分别发送至所述通信设备和所述控制设备的。可选的，所述服务器生成目标密钥之后发送到所述控制设备或所述待升级车载设备上进行拆分。例如，所述服务器为升级服务器、密钥服务器或其它服务器等。本发明实施例中，目标密钥的生成和/或目标密钥的拆分过程可以是由服务器来执行，可减少控制设备和待升级设备的计算量，提升升级效率。

[0036] 在一种可能的实现方式中，所述第三密钥和所述第四密钥是由服务器拆分而来，再发送至所述待升级车载设备的。例如，所述服务器为升级服务器、密钥服务器或其它服务器等。本发明实施例中，第三密钥和第四密钥对应的原始密钥的生成和/或拆分，可以是由服务器来执行，可减少控制设备和待升级设备的计算量，提升升级效率。

[0037] 第三方面，本发明实施例提供了一种设备升级系统，可包括控制设备和待升级设

备;其中,所述控制设备,用于:接收所述通信设备发送的第一升级文件数据,所述第一升级文件数据为所述通信设备利用第一密钥对升级文件进行第一安全处理后生成的升级文件数据;利用第二密钥对所述第一升级文件数据进行第二安全处理,生成第二升级文件数据,并向所述待升级设备发送所述第二升级文件数据;所述待升级设备,用于接收所述第二升级文件数据,利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验,若校验通过,则利用所述升级文件进行升级;其中,所述第三密钥为所述第一密钥匹配的校验密钥,所述第四密钥为所述第二密钥匹配的校验密钥。

[0038] 在一种可能的实现方式中,所述第一安全处理包括根据所述第一密钥生成所述升级文件的第一消息认证码MAC;所述第一升级文件数据包括所述升级文件和所述第一MAC。

[0039] 在一种可能的实现方式中,所述第二安全处理包括根据所述第二密钥生成所述升级文件的第二MAC,并将所述第一MAC和所述第二MAC聚合得到第三MAC;所述第二升级文件数据包括所述升级文件和所述第三MAC。

[0040] 在一种可能的实现方式中,所述第二安全处理包括根据所述第二密钥生成所述第一升级文件数据的第四MAC;所述第二升级文件数据包括所述升级文件和所述第四MAC。

[0041] 在一种可能的实现方式中,所述第一密钥和所述第三密钥为对称密钥,所述第二密钥和所述第四密钥为对称密钥;所述控制设备,还用于:生成目标密钥,将所述目标密钥拆分为所述第一密钥和所述第二密钥;将所述目标密钥发送至所述待升级设备,将所述第一密钥发送至所述通信设备;存储所述第二密钥,并删除所述目标密钥。

[0042] 在一种可能的实现方式中,所述第一密钥和所述第三密钥为对称密钥,所述第二密钥和所述第四密钥为对称密钥;所述待升级设备,还用于:生成目标密钥,将所述目标密钥拆分为所述第一密钥和所述第二密钥;将所述第一密钥发送给所述通信设备,以及将所述第二密钥发送给所述控制设备;存储所述目标密钥,并删除所述第一密钥和所述第二密钥。

[0043] 在一种可能的实现方式中,所述待升级设备,还用于在利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验之前,将存储的所述目标密钥拆分为所述第三密钥和所述第四密钥。

[0044] 在一种可能的实现方式中,所述升级文件经过数字签名;所述第一升级文件数据为所述通信设备在获取所述升级文件,并对所述数字签名进行验签通过后,利用所述第一密钥对所述升级文件进行第一安全处理后生成的升级文件数据。

[0045] 在一种可能的实现方式中,所述第一升级文件数据中的升级文件还经过数字签名;所述控制设备,还用于在利用第二密钥对所述第一升级文件数据进行第二安全处理之前,对所述数字签名进行验签,若验签通过,则利用所述第二密钥对所述第一升级文件数据进行第二安全处理。

[0046] 在一种可能的实现方式中,所述待升级设备,还用于在根据所述升级文件升级成功后,向所述控制设备发送升级成功消息,所述升级成功消息为经过所述第四密钥的安全保护的消息。

[0047] 在一种可能的实现方式中,所述控制设备,还用于在确认所述待升级设备升级成功后,指示所述通信设备更新所述升级文件的回滚文件;和/或所述控制设备,还用于在确认所述待升级设备升级失败后,从所述通信设备获取所述升级文件的回滚文件,并发送给

所述待升级设备进行回滚操作。

[0048] 在一种可能的实现方式中，所述第一密钥和所述第二密钥是由服务器生成目标密钥并拆分而来，并由所述服务器分别发送至所述通信设备和所述控制设备的。可选的，所述服务器生成目标密钥之后发送到所述控制设备或所述待升级车载设备上进行拆分。例如，所述服务器为升级服务器、密钥服务器或其它服务器等。本发明实施例中，目标密钥的生成和/或目标密钥的拆分过程可以是由服务器来执行，可减少控制设备和待升级设备的计算量，提升升级效率。

[0049] 在一种可能的实现方式中，所述第三密钥和所述第四密钥是由服务器拆分而来，再发送至所述待升级车载设备的。例如，所述服务器为升级服务器、密钥服务器或其它服务器等。本发明实施例中，第三密钥和第四密钥对应的原始密钥的生成和/或拆分，可以是由服务器来执行，可减少控制设备和待升级设备的计算量，提升升级效率。

[0050] 第四方面，本发明实施例提供了一种通信设备，可包括：

[0051] 安全处理单元，用于利用第一密钥对升级文件进行第一安全处理，生成第一升级文件数据；

[0052] 发送单元，用于向控制设备发送所述第一升级文件数据；其中，

[0053] 所述第一升级文件数据用于所述控制设备利用第二密钥对所述第一升级文件数据进行第二安全处理，生成第二升级文件数据，并向待升级设备发送所述第二升级文件数据；

[0054] 所述第二升级文件数据用于所述待升级设备利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验，若校验通过，则利用所述升级文件进行升级；其中，所述第三密钥为所述第一密钥匹配的校验密钥，所述第四密钥为所述第二密钥匹配的校验密钥。

[0055] 在一种可能的实现方式中，所述第一安全处理包括根据所述第一密钥生成所述升级文件的第一消息认证码MAC；所述第一升级文件数据包括所述升级文件和所述第一MAC。

[0056] 在一种可能的实现方式中，所述第二安全处理包括根据所述第二密钥生成所述升级文件的第二MAC，并将所述第一MAC和所述第二MAC聚合得到第三MAC；所述第二升级文件数据包括所述升级文件和所述第三MAC。

[0057] 在一种可能的实现方式中，所述第二安全处理包括根据所述第二密钥生成所述第一升级文件数据的第四MAC；所述第二升级文件数据包括所述升级文件和所述第四MAC。

[0058] 在一种可能的实现方式中，所述第一密钥和所述第三密钥为对称密钥，所述第二密钥和所述第四密钥为对称密钥；所述第一密钥和所述第二密钥为所述控制设备将生成的目标密钥拆分后的密钥，其中，所述目标密钥还用于由所述控制设备发送至所述待升级设备进行存储；所述通信设备还包括：接收单元，用于接收所述控制设备发送的所述第一密钥。

[0059] 在一种可能的实现方式中，所述第一密钥和所述第三密钥为对称密钥，所述第二密钥和所述第四密钥为对称密钥；所述第一密钥和所述第二密钥为所述待升级设备将生成的目标密钥拆分后的密钥；所述通信设备还包括：接收单元，用于接收所述待升级设备发送的所述第一密钥。

[0060] 在一种可能的实现方式中，所述第三密钥和所述第四密钥为所述待升级设备在利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验之前，将存储的所述目标密

钥拆分后的密钥。

[0061] 在一种可能的实现方式中，所述升级文件经过数字签名；所述第一升级文件数据为所述通信设备在获取所述升级文件，并对所述数字签名进行验签通过后，利用所述第一密钥对所述升级文件进行第一安全处理后生成的升级文件数据。

[0062] 在一种可能的实现方式中，所述升级文件经过数字签名；所述安全处理单元，具体用于获取所述升级文件，并对所述数字签名进行验签，若验签通过，则利用所述第一密钥对所述升级文件进行第一安全处理。

[0063] 在一种可能的实现方式中，所述第一升级文件数据中的升级文件还经过数字签名；所述第一升级文件数据具体用于所述控制设备对所述数字签名进行验签，若验签通过，则利用第二密钥对所述第一升级文件数据进行第二安全处理，生成第二升级文件数据。

[0064] 在一种可能的实现方式中，所述通信设备还包括第一回滚单元，用于在所述待升级设备升级成功后，接收所述控制设备发送的更新所述升级文件的回滚文件的指示；和/或，所述通信设备还包括第二回滚单元，用于在所述待升级设备升级失败后，向所述控制设备发送所述升级文件的回滚文件，以用于所述待升级设备进行回滚操作。

[0065] 在一种可能的实现方式中，所述第一密钥和所述第二密钥是由服务器生成目标密钥并拆分而来，并由所述服务器分别发送至所述通信设备和所述控制设备的。可选的，所述服务器生成目标密钥之后发送到所述控制设备或所述待升级车载设备上进行拆分。例如，所述服务器为升级服务器、密钥服务器或其它服务器等。本发明实施例中，目标密钥的生成和/或目标密钥的拆分过程可以是由服务器来执行，可减少控制设备和待升级设备的计算量，提升升级效率。

[0066] 在一种可能的实现方式中，所述第三密钥和所述第四密钥是由服务器拆分而来，再发送至所述待升级车载设备的。例如，所述服务器为升级服务器、密钥服务器或其它服务器等。本发明实施例中，第三密钥和第四密钥对应的原始密钥的生成和/或拆分，可以是由服务器来执行，可减少控制设备和待升级设备的计算量，提升升级效率。

[0067] 第五方面，本发明实施例提供了一种控制设备，可包括：

[0068] 第一接收单元，用于接收通信设备发送的第一升级文件数据，所述第一升级文件数据为所述通信设备利用第一密钥对升级文件进行第一安全处理后生成的升级文件数据；

[0069] 安全处理单元，用于利用第二密钥对所述第一升级文件数据进行第二安全处理，生成第二升级文件数据，并向待升级设备发送所述第二升级文件数据；其中，

[0070] 所述第二升级文件数据，用于所述待升级设备所述利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验，若校验通过，则利用所述升级文件进行升级；其中，所述第三密钥为所述第一密钥匹配的校验密钥，所述第四密钥为所述第二密钥匹配的校验密钥。

[0071] 在一种可能的实现方式中，所述第一安全处理包括根据所述第一密钥生成所述升级文件的第一消息认证码MAC；所述第一升级文件数据包括所述升级文件和所述第一MAC。

[0072] 在一种可能的实现方式中，所述第二安全处理包括根据所述第二密钥生成所述升级文件的第二MAC，并将所述第一MAC和所述第二MAC聚合得到第三MAC；所述第二升级文件数据包括所述升级文件和所述第三MAC。

[0073] 在一种可能的实现方式中，所述第二安全处理包括根据所述第二密钥生成所述第

一升级文件数据的第四MAC;所述第二升级文件数据包括所述升级文件和所述第四MAC。

[0074] 在一种可能的实现方式中,所述第一密钥和所述第三密钥为对称密钥,所述第二密钥和所述第四密钥为对称密钥;所述控制设备还包括:密钥生成单元,用于生成目标密钥,将所述目标密钥拆分为所述第一密钥和所述第二密钥;发送单元,用于将所述目标密钥发送至所述待升级设备,将所述第一密钥发送至所述通信设备;密钥存储单元,用于存储所述第二密钥,并删除所述目标密钥。

[0075] 在一种可能的实现方式中,所述第一密钥和所述第三密钥为对称密钥,所述第二密钥和所述第四密钥为对称密钥;所述第一密钥和所述第二密钥为所述待升级设备将生成的目标密钥拆分后的密钥;所述控制设备还包括:第二接收单元,用于接收所述待升级设备发送的所述第二密钥。

[0076] 在一种可能的实现方式中,所述第三密钥和所述第四密钥为所述待升级设备在对所述第二升级文件数据进行安全校验之前,将存储的所述目标密钥拆分后的密钥。

[0077] 在一种可能的实现方式中,所述升级文件经过数字签名;所述第一升级文件数据为所述通信设备在获取所述升级文件,并对所述数字签名进行验签通过后,利用所述第一密钥对所述升级文件进行第一安全处理后生成的升级文件数据。

[0078] 在一种可能的实现方式中,所述第一升级文件数据中的升级文件还经过数字签名;所述安全处理单元,具体用于在利用第二密钥对所述第一升级文件数据进行第二安全处理之前,对所述数字签名进行验签,若验签通过,则利用所述第二密钥对所述第一升级文件数据进行第二安全处理。

[0079] 在一种可能的实现方式中,所述控制设备,还包括第三接收单元,用于接收所述待升级设备在根据所述升级文件升级成功后发送的升级成功消息,所述升级成功消息为经过所述第四密钥的安全保护的消息。

[0080] 在一种可能的实现方式中,所述控制设备,还包括第一回滚单元,用于在确认所述待升级设备升级成功后,指示所述通信设备更新所述升级文件的回滚文件;和/或所述控制设备,还包括第二回滚单元,用于在确认所述待升级设备升级失败后,从所述通信设备获取所述升级文件的回滚文件,并发送给所述待升级设备进行回滚操作。

[0081] 在一种可能的实现方式中,所述第一密钥和所述第二密钥是由服务器生成目标密钥并拆分而来,并由所述服务器分别发送至所述通信设备和所述控制设备的。可选的,所述服务器生成目标密钥之后发送到所述控制设备或所述待升级车载设备上进行拆分。例如,所述服务器为升级服务器、密钥服务器或其它服务器等。本发明实施例中,目标密钥的生成和/或目标密钥的拆分过程可以是由服务器来执行,可减少控制设备和待升级设备的计算量,提升升级效率。

[0082] 在一种可能的实现方式中,所述第三密钥和所述第四密钥是由服务器拆分而来,再发送至所述待升级车载设备的。例如,所述服务器为升级服务器、密钥服务器或其它服务器等。本发明实施例中,第三密钥和第四密钥对应的原始密钥的生成和/或拆分,可以是由服务器来执行,可减少控制设备和待升级设备的计算量,提升升级效率。

[0083] 第六方面,本发明实施例提供了一种待升级设备,可包括:

[0084] 第一接收单元,用于接收控制设备发送的第二升级文件数据,所述第二升级文件数据为所述控制设备利用第二密钥对通信设备发送的第一升级文件数据进行第二安全处

理，生成的升级文件数据，所述第一升级文件数据为所述通信设备利用第一密钥对升级文件进行第一安全处理后生成的升级文件数据；

[0085] 安全校验单元，用于利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验，所述第三密钥为所述第一密钥匹配的校验密钥，所述第四密钥为所述第二密钥匹配的校验密钥；

[0086] 升级单元，用于若校验通过，则利用所述升级文件进行升级。

[0087] 在一种可能的实现方式中，所述第一安全处理包括根据所述第一密钥生成所述升级文件的第一消息认证码MAC；所述第一升级文件数据包括所述升级文件和所述第一MAC。

[0088] 在一种可能的实现方式中，所述第二安全处理包括根据所述第二密钥生成所述升级文件的第二MAC，并将所述第一MAC和所述第二MAC聚合得到第三MAC；所述第二升级文件数据包括所述升级文件和所述第三MAC。

[0089] 在一种可能的实现方式中，所述第二安全处理包括根据所述第二密钥生成所述第一升级文件数据的第四MAC；所述第二升级文件数据包括所述升级文件和所述第四MAC。

[0090] 在一种可能的实现方式中，所述第一密钥和所述第三密钥为对称密钥，所述第二密钥和所述第四密钥为对称密钥；所述第一密钥和所述第二密钥为所述控制设备将生成的目标密钥拆分后的密钥，所述待升级设备还包括：第二接收单元，用于接收所述控制设备发送的所述目标密钥。

[0091] 在一种可能的实现方式中，所述第一密钥和所述第三密钥为对称密钥，所述第二密钥和所述第四密钥为对称密钥；所述待升级设备还包括：第一密钥生成单元，用于生成目标密钥，将所述目标密钥拆分为所述第一密钥和所述第二密钥；发送单元，用于将所述第一密钥发送给所述通信设备，以及将所述第二密钥发送给所述控制设备；密钥存储单元，用于存储所述目标密钥，并删除所述第一密钥和所述第二密钥。

[0092] 在一种可能的实现方式中，所述待升级设备还包括：第二密钥生成单元，用于在利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验之前，将存储的所述目标密钥拆分为所述第三密钥和所述第四密钥。

[0093] 在一种可能的实现方式中，所述升级文件经过数字签名；所述第一升级文件数据为所述通信设备在获取所述升级文件，并对所述数字签名进行验签通过后，利用所述第一密钥对所述升级文件进行第一安全处理后生成的升级文件数据。

[0094] 在一种可能的实现方式中，所述第一升级文件数据中的升级文件还经过数字签名；所述第二升级文件数据为所述控制设备对通信设备发送的所述第一升级文件数据中的所述数字签名进行验签，并验签通过后，利用第二密钥对所述第一升级文件数据进行第二安全处理生成的升级文件数据。

[0095] 在一种可能的实现方式中，所述待升级设备还包括反馈单元，用于在根据所述升级文件升级成功后，向所述控制设备发送升级成功消息，所述升级成功消息为经过所述第四密钥的安全保护的消息。

[0096] 在一种可能的实现方式中，所述待升级设备还包括回滚单元，用于在确认所述待升级设备升级失败后，从所述控制设备获取所述升级文件的回滚文件，进行回滚操作。

[0097] 在一种可能的实现方式中，所述第一密钥和所述第二密钥是由服务器生成目标密钥并拆分而来，并由所述服务器分别发送至所述通信设备和所述控制设备的。可选的，所述

服务器生成目标密钥之后发送到所述控制设备或所述待升级车载设备上进行拆分。例如，所述服务器为升级服务器、密钥服务器或其它服务器等。本发明实施例中，目标密钥的生成和/或目标密钥的拆分过程可以是由服务器来执行，可减少控制设备和待升级设备的计算量，提升升级效率。

[0098] 在一种可能的实现方式中，所述第三密钥和所述第四密钥是由服务器拆分而来，再发送至所述待升级车载设备的。例如，所述服务器为升级服务器、密钥服务器或其它服务器等。本发明实施例中，第三密钥和第四密钥对应的原始密钥的生成和/或拆分，可以是由服务器来执行，可减少控制设备和待升级设备的计算量，提升升级效率。

[0099] 第七方面，本发明实施例提供了一种智能车辆，可应用于车载系统，所述车载系统包括车载控制设备和待升级车载设备；其中，

[0100] 所述车载控制设备，用于接收通信设备发送的第一升级文件数据，所述第一升级文件数据为所述通信设备利用第一密钥对升级文件进行第一安全处理后生成的升级文件数据；所述车载控制设备，用于利用第二密钥对所述第一升级文件数据进行第二安全处理，生成第二升级文件数据，并向所述待升级车载设备发送所述第二升级文件数据；所述待升级车载设备，用于接收所述第二升级文件数据，利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验，若校验通过，则利用所述升级文件进行升级；其中，所述第三密钥为所述第一密钥匹配的校验密钥，所述第四密钥为所述第二密钥匹配的校验密钥。

[0101] 在一种可能的实现方式中，所述第一安全处理包括根据所述第一密钥生成所述升级文件的第一消息认证码MAC；所述第一升级文件数据包括所述升级文件和所述第一MAC。

[0102] 在一种可能的实现方式中，所述第二安全处理包括根据所述第二密钥生成所述升级文件的第二MAC，并将所述第一MAC和所述第二MAC聚合得到第三MAC；所述第二升级文件数据包括所述升级文件和所述第三MAC。

[0103] 在一种可能的实现方式中，所述第二安全处理包括根据所述第二密钥生成所述第一升级文件数据的第四MAC；所述第二升级文件数据包括所述升级文件和所述第四MAC。

[0104] 在一种可能的实现方式中，所述第一密钥和所述第三密钥为对称密钥，所述第二密钥和所述第四密钥为对称密钥；所述车载控制设备，还用于生成目标密钥，将所述目标密钥拆分为所述第一密钥和所述第二密钥；将所述目标密钥发送至所述待升级车载设备，将所述第一密钥发送至所述通信设备；存储所述第二密钥，并删除所述目标密钥。

[0105] 在一种可能的实现方式中，所述第一密钥和所述第三密钥为对称密钥，所述第二密钥和所述第四密钥为对称密钥；所述待升级车载设备，用于生成目标密钥，将所述目标密钥拆分为所述第一密钥和所述第二密钥；将所述第一密钥发送给所述通信设备，以及将所述第二密钥发送给所述车载控制设备；存储所述目标密钥，并删除所述第一密钥和所述第二密钥。

[0106] 在一种可能的实现方式中，所述待升级车载设备，还用于在利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验之前，将存储的所述目标密钥拆分为所述第三密钥和所述第四密钥。

[0107] 在一种可能的实现方式中，所述升级文件经过数字签名；所述第一升级文件数据为所述通信设备在获取所述升级文件，并对所述数字签名进行验签通过后，利用所述第一密钥对所述升级文件进行第一安全处理后生成的升级文件数据。

[0108] 在一种可能的实现方式中，所述第一升级文件数据中的升级文件还经过数字签名

[0109] 所述车载控制设备，还用于在利用第二密钥对所述第一升级文件数据进行第二安全处理之前，对所述数字签名进行验签，若验签通过，则利用所述第二密钥对所述第一升级文件数据进行第二安全处理。

[0110] 在一种可能的实现方式中，所述待升级车载设备，还用于在根据所述升级文件升级成功后，向所述车载控制设备发送升级成功消息，所述升级成功消息为经过所述第四密钥的安全保护的消息。

[0111] 在一种可能的实现方式中，所述车载控制设备，还用于在确认所述待升级车载设备升级成功后，指示所述通信设备更新所述升级文件的回滚文件；和/或

[0112] 所述车载控制设备，还用于在确认所述待升级车载设备升级失败后，从所述通信设备获取所述升级文件的回滚文件，并发送给所述待升级车载设备进行回滚操作。

[0113] 在一种可能的实现方式中，所述第一密钥和所述第二密钥是由服务器生成目标密钥并拆分而来，并由所述服务器分别发送至所述通信设备和所述车载控制设备的。可选的，所述服务器生成目标密钥之后发送到所述车载控制设备或所述待升级车载设备上进行拆分。例如，所述服务器为升级服务器、密钥服务器或其它服务器等。本发明实施例中，目标密钥的生成和/或目标密钥的拆分过程可以是由服务器来执行，可减少车载控制设备和待升级车载设备的计算量，提升升级效率。

[0114] 在一种可能的实现方式中，所述第三密钥和所述第四密钥是由服务器拆分而来，再发送至所述待升级车载设备的。例如，所述服务器为升级服务器、密钥服务器或其它服务器等。本发明实施例中，第三密钥和第四密钥对应的原始密钥的生成和/或拆分，可以是由服务器来执行，可减少车载控制设备和待升级车载设备的计算量，提升升级效率。

[0115] 第八方面，本发明实施例提供了一种车载设备升级方法，可应用于车载系统，所述车载系统包括车载控制设备和待升级车载设备；所述方法可包括：

[0116] 所述车载控制设备接收所述通信设备发送的第一升级文件数据，所述第一升级文件数据为所述通信设备利用第一密钥对升级文件进行第一安全处理后生成的升级文件数据；

[0117] 所述车载控制设备利用第二密钥对所述第一升级文件数据进行第二安全处理，生成第二升级文件数据，并向所述待升级车载设备发送所述第二升级文件数据；

[0118] 所述待升级车载设备接收所述第二升级文件数据，利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验，若校验通过，则利用所述升级文件进行升级；其中，所述第三密钥为所述第一密钥匹配的校验密钥，所述第四密钥为所述第二密钥匹配的校验密钥。

[0119] 在一种可能的实现方式中，所述第一安全处理包括根据所述第一密钥生成所述升级文件的第一消息认证码MAC；所述第一升级文件数据包括所述升级文件和所述第一MAC。

[0120] 在一种可能的实现方式中，所述第二安全处理包括根据所述第二密钥生成所述升级文件的第二MAC，并将所述第一MAC和所述第二MAC聚合得到第三MAC；所述第二升级文件数据包括所述升级文件和所述第三MAC。

[0121] 在一种可能的实现方式中，所述第二安全处理包括根据所述第二密钥生成所述第一升级文件数据的第四MAC；所述第二升级文件数据包括所述升级文件和所述第四MAC。

[0122] 在一种可能的实现方式中，所述第一密钥和所述第三密钥为对称密钥，所述第二密钥和所述第四密钥为对称密钥；所述方法还包括：所述车载控制设备生成目标密钥，将所述目标密钥拆分为所述第一密钥和所述第二密钥；所述车载控制设备将所述密钥发送至所述待升级车载设备，将所述第一密钥发送至所述通信设备；所述车载控制设备存储所述第二密钥，并删除所述目标密钥。

[0123] 在一种可能的实现方式中，所述第一密钥和所述第三密钥为对称密钥，所述第二密钥和所述第四密钥为对称密钥；所述方法还包括：所述待升级车载设备生成目标密钥，将所述目标密钥拆分为所述第一密钥和所述第二密钥；所述待升级车载设备将所述第一密钥发送给所述通信设备，以及将所述第二密钥发送给所述车载控制设备；所述待升级车载设备存储所述目标密钥，并删除所述第一密钥和所述第二密钥。

[0124] 在一种可能的实现方式中，所述方法还包括：所述待升级车载设备在利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验之前，将存储的所述目标密钥拆分为所述第三密钥和所述第四密钥。

[0125] 在一种可能的实现方式中，所述升级文件经过数字签名；所述第一升级文件数据为所述通信设备在获取所述升级文件，并对所述数字签名进行验签通过后，利用所述第一密钥对所述升级文件进行第一安全处理后生成的升级文件数据。

[0126] 在一种可能的实现方式中，所述第一升级文件数据中的升级文件还经过数字签名；所述车载控制设备利用第二密钥对所述第一升级文件数据进行第二安全处理之前，还包括：对所述数字签名进行验签，若验签通过，则利用所述第二密钥对所述第一升级文件数据进行第二安全处理。

[0127] 在一种可能的实现方式中，所述方法还包括：所述待升级车载设备在根据所述升级文件升级成功后，向所述车载控制设备发送升级成功消息，所述升级成功消息为经过所述第四密钥的安全保护的消息。

[0128] 在一种可能的实现方式中，所述方法还包括：所述车载控制设备在确认所述待升级车载设备升级成功后，指示所述通信设备更新所述升级文件的回滚文件；和/或所述车载控制设备在确认所述待升级车载设备升级失败后，从所述通信设备获取所述升级文件的回滚文件，并发送给所述待升级车载设备进行回滚操作。

[0129] 在一种可能的实现方式中，所述第一密钥和所述第二密钥是由服务器生成目标密钥并拆分而来，并由所述服务器分别发送至所述通信设备和所述车载控制设备的。可选的，所述服务器生成目标密钥之后发送到所述车载控制设备或所述待升级车载设备上进行拆分。例如，所述服务器为升级服务器、密钥服务器或其它服务器等。本发明实施例中，目标密钥的生成和/或目标密钥的拆分过程可以是由服务器来执行，可减少车载控制设备和待升级车载设备的计算量，提升升级效率。

[0130] 在一种可能的实现方式中，所述第三密钥和所述第四密钥是由服务器拆分而来，再发送至所述待升级车载设备的。例如，所述服务器为升级服务器、密钥服务器或其它服务器等。本发明实施例中，第三密钥和第四密钥对应的原始密钥的生成和/或拆分，可以是由服务器来执行，可减少车载控制设备和待升级车载设备的计算量，提升升级效率。

[0131] 第九方面，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。

[0132] 第十方面，本申请提供一种车载设备升级装置，该车载设备升级装置具有实现上述第八方面提供的任意一种车载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。

[0133] 第十一方面，本申请提供一种控制设备，该控制设备中包括处理器，处理器被配置为支持该控制设备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。该控制设备还可以包括存储器，存储器用于与处理器耦合，其保存该控制设备必要的程序指令和数据。该控制设备还可以包括通信接口，用于该控制设备与其他设备或通信网络通信。

[0134] 第十二方面，本申请提供一种车载控制设备，该车载控制设备中包括处理器，处理器被配置为支持该车载控制设备执行第八方面提供的任意一种车载设备升级方法中相应的功能。该车载控制设备还可以包括存储器，存储器用于与处理器耦合，其保存该车载控制设备必要的程序指令和数据。该车载控制设备还可以包括通信接口，用于该车载控制设备与其他设备或通信网络通信。

[0135] 第十三方面，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一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。

[0136] 第十四方面，本申请提供一种待升级车载设备，该待升级车载设备中包括处理器，处理器被配置为支持该待升级车载设备执行第一方面提供的任意一种车载设备升级方法中相应的功能。该待升级车载设备还可以包括存储器，存储器用于与处理器耦合，其保存该待升级车载设备必要的程序指令和数据。该待升级车载设备还可以包括通信接口，用于该待升级车载设备与其他设备或通信网络通信。

[0137] 第十五方面，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提供的控制设备、待升级设备或通信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。

[0138] 第十六方面，本申请提供一种计算机存储介质，用于储存为上述第八方面提供的车载控制设备、待升级车载设备或通信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。

[0139] 第十七方面，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，当该计算机程序被控制设备、待升级设备或通信设备执行时，使得控制设备、待升级设备或通信设备可以执行上述第一方面中任意一项的设备升级方法中控制设备、待升级设备或通信设备所执行的流程。

[0140] 第十八方面，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，当该计算机程序被车载控制设备、待升级车载设备或通信设备执行时，使得车载控制设备、待升级车载设备或通信设备可以执行上述第八方面中任意一项的车载设备升级方法中车载控制设备、待升级车载设备或通信设备所执行的流程。

[0141] 第十九方面，本申请提供了一种芯片系统，该芯片系统包括处理器，用于支持控制设备、待升级设备或通信设备实现上述第一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，用于保存控制设备、待升级设备或通信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。

[0142] 第二十方面，本申请提供了一种芯片系统，该芯片系统包括处理器，用于支持车载控制设备、待升级车载设备或通信设备实现上述第一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，用于保存车载控制设备、待升级车载设备或通信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。

附图说明

[0143] 图1是本发明实施例提供的基于物联网的智能家居升级系统的架构图。

[0144] 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。

[0145] 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。

[0146] 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。

[0147] 图5是本发明实施例提供的一种OTA Orchestrator的结构示意图。

[0148] 图6是本发明实施例提供的一种待升级车载设备的结构示意图。

[0149] 图7是本发明实施例提供的一种终端设备的结构示意图。

[0150] 图8是本发明实施例提供的另一种设备升级系统架构示意图。

[0151] 图9是本发明实施例提供的一种车载设备升级方法的流程示意图。

[0152] 图10是本发明实施例提供的另一种车载设备升级方法的流程示意图。

[0153] 图11是本发明实施例提供的又一种车载设备升级方法的流程示意图。

[0154] 图12是本发明实施例提供的一种通信设备的结构示意图。

[0155] 图13是本发明实施例提供的一种控制设备的结构示意图。

[0156] 图14是本发明实施例提供的另一种控制设备的结构示意图。

[0157] 图15是本发明实施例提供的一种待升级设备的结构示意图。

[0158] 图16是本发明实施例提供的另一种待升级设备的结构示意图。

[0159] 图17是本发明实施例提供的一种智能车辆的结构示意图。

[0160] 图18是本发明实施例提供的一种车载设备升级系统的结构示意图。

[0161] 图19是本发明实施例提供的另一种车载设备升级系统的结构示意图。

[0162] 图20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

[0163] 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。

[0164] 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。

[0165] 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。

[0166] 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。

[0167] 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。

[0168] (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。

[0169] (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。

[0170] (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。

[0171] (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。

[0172] (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。

[0173] (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。

[0174] (7)密钥导出算法(Key Derivation Function,KDF),是加解密过程使用到的密钥派生函数,作用是从一个共享的秘密比特串口派生出密钥数据,在密钥协商过程中,密钥派生函数作用在密钥交换所获动向的秘密比特串上,从中产生所需的会话密钥或进一步加密所需的密钥数据。

[0175] (8)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、El Gamal公钥密码、椭圆曲线密码。

[0176] (9)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。

[0177] 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。

[0178] (10)传输层安全协议(Transport Layer Security,TLS),用于两个应用程序之间提供保密性和数据完整性。该协议由两层组成:TLS记录协议(TLS Record)和TLS握手协议(TLS Handshake)。安全传输层协议(TLS)用于在两个通信应用程序之间提供保密性和数据完整性。

[0179] (11)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。

[0180] (12)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。

[0181] 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。

[0182] 场景一,通过通信设备对智能家居进行升级管理:

[0183] 请参阅图1,图1为本发明实施例提供的基于物联网的智能家居升级系统的架构图,该应用场景中包括升级服务器(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,当物联网服务器中有上述任意一个智能家电更新的升级文件时,则小区网关通过互联网从物联网服务器处下载升级文件,并与家庭网关之间使用本申请中所提供的设备升级方法,在小区网关上完成第一安全处理,以及在家庭网关上完成第二安全处理,最终将经过安全保护的升级文件发送给待升级的智能家电以完成安全升级。

[0184] 场景二,通过通信设备对智能车辆进行一对一管理:

[0185] 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,该应用场景中包括通信设备(图1中以终端设备如智能手机为例)、智能车辆和升级服务器,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提供的设备升级方法的流程,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。在另一种可能的场景中,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。

[0186] 场景三,通信设备为服务器,通过服务器对智能车辆进行一对多管理:

[0187] 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。该应用场景中包括智能车辆和升级服务器,升级服务器和智能车辆之间则可以通过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,且该升级服务器中除了可以完成关于升级包的提供、下载更新等相关服务以外,还作为本申请中的通信设备与智能车辆合作执行本申请中提供的车载设备升级方法的流程。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。

[0188] 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,例如主机管理虚拟机进行系统升级、路由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、智能医疗管理设备管理智能医疗器械进行设备升级、工厂管控设备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。

[0189] 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),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、智能车辆和通信设备(图4中以通信设备为终端设备如智能手机为例),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设备,例如HMI(人机界面)、BMS(电池管理系统)、电子控制单元1ECU1和电子控制单元2ECU2,而车载控制设备可以包括车载信息服务单元(Telematics)和OTA协调器(OTA Orchestrator),用于管理和辅助多个待升级车载设备的升级过程。在上述系统架构下,车载设备远程升级可以包括以下基本过程:升级包发布,升级包获取,升级包车内传输,升级与确认。其中,

[0190] 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,该车载升级包包括本申请中的升级文件,可用于本申请中的待升级车载设备进行升级。

[0191] 通信设备,本申请中的通信设备可以为终端设备,负责与升级服务器之间通信,完成车载升级包的获取,以及利用自身的存储能力和计算能力参与到第一密钥的存储、第一安全处理、生成第一升级文件数据的过程,以实现计算扩展和安全强化。进一步地,通信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,利用自身的存储能力协助储存中间档案(如各个待升级车载设备软/固件信息,当前版本、大小、开发者等),备份文件(如待升级车载设备软/固回滚版)与车机系统状况,以完成储存扩展。当通信设备为终端设备时,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。

[0192] 车载控制设备中的Telematics,负责对外通信,例如与通信设备之间的通信、与升级服务器之间的通信等,以及车载升级包的部分传输动作(发送给OTA Orchestrator)。

[0193] 车载控制设备中的OTA Orchestrator,负责与车载内的待升级车载设备进行通信,其主要功能是管理和辅助车载设备的升级过程。具体来说,OTA Orchestrator可以具有如下功能:密钥分发及管理(例如,生成目标密钥、拆分生成第一密钥和第二密钥等);管理OTA过程;与通信设备共同帮助较弱的待升级车载设备分担计算量大的操作,如校验升级包的数字签名等;与通信设备共同作为较弱的待升级车载设备的备份点,以便升级失败时回滚。OTA Orchestrator是个逻辑实体,物理上可以部署任何功能强大的单元或模块上,例如Telematics、Gateway、VCU上等。

[0194] OTA Orchestrator的结构可以如图5所示,图5是本发明实施例提供的一种OTA Orchestrator的结构示意图。其中,OTA Orchestrator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,如与待升级车载设备共享的静态密钥(本申请中的第一密钥、第二密钥)等;用于存储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OTA Orchestrator实现在Telematics上,它还需要有与外部网络通信的网络接口。即OTA Orchestrator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,OTA Orchestrator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OTA Orchestrator,以减少车载内待升级设备的计算量和计算复杂度。

[0195] 待升级车载设备,智能车辆中任意一个待升级车载设备(包括本申请中的所述待

升级车载设备)的构成可以如图6所示,图6是本发明实施例提供的一种待升级车载设备的结构示意图。待升级车载设备可以包括微型控制器(Micro controlller),CAN控制器(CAN controller)和收发器(Transceiver)。其中,待升级车载设备通过收发器Transceiver与车内网络如CANbus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,例如,可以实现本申请中关于待升级车载设备所执行的车载设备升级方法流程。结合上述结构示意图,在本申请中,待升级车载设备基于车内网络如CAN bus,通过收发器(Transceiver)接收车载控制设备发送的第二升级文件数据,并通过微型控制器(Micro Controlller)使用第三密钥和第四密钥对第二升级文件数据进行安全校验,以进行安全升级。可选的,待升级车载设备也可以实现利用微型控制器(Micro Controlller)生成目标密钥以及拆分成为第一密钥和第二密钥等功能,更具体的功能可以参照后续实施例中关于待升级车载设备相关功能的描述。

[0196] 当通信设备为终端设备时,该终端设备的构成可以参考图7,图7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;用于存储OTA管理程序的存储器,该OTA管理程序用于实现对设备升级过程的管理;用于与其它设备(包括智能车辆以及升级服务器等)进行通信的无线通信模块;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。需要说明的是,当通信设备为服务器且该服务器和本申请中的升级服务器在同一个物理实体上时,则该升级服务器中可以包含一个实现上述通信设备所实现的功能的逻辑功能实体,因此,关于通信设备具体的实际结构本申请不作具体限定。且当通信设备为终端设备时,则可以对应图2中的应用场景,当通信设备为服务器时,则可以对应图3中的应用场景。

[0197] 可选的,本申请中的车载系统升级架构还可以包括开发者,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。如图8所示,图8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),该系统架构中,还包括了密钥服务器,可用于生成升级服务器和开发者之间所使用的密钥,也可以生成升级服务器和通信设备或车载控制设备之间签名和验签的公私钥对,进一步可选的,也可以参与本发明实施例中的目标密钥、第一密钥、第二密钥等的生成,本发明实施例对此不作具体限定。

[0198] 可以理解的是,图4和图8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。

[0199] 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。

[0200] 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从通信设备、控制设备和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S906。

[0201] 步骤S901:通信设备利用第一密钥对升级文件进行第一安全处理,生成第一升级

文件数据。

[0202] 步骤S902:通信设备向所述控制设备发送所述第一升级文件数据;控制设备接收通信设备发送的第一升级文件数据。

[0203] 步骤S903:控制设备利用第二密钥对所述第一升级文件数据进行第二安全处理,生成第二升级文件数据。

[0204] 步骤S904:控制设备向所述待升级设备发送所述第二升级文件数据;待升级设备接收所述第二升级文件数据。

[0205] 步骤S905:待升级设备利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验。

[0206] 步骤S906:若校验通过,待升级设备则利用所述升级文件进行升级;其中,所述第三密钥为所述第一密钥匹配的校验密钥,所述第四密钥为所述第二密钥匹配的校验密钥。

[0207] 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,即所述控制设备和待升级设备可以为智能车辆/车载系统中的车载控制设备和待升级车载设备。所述升级文件可以为智能车辆中任意一个待升级车载设备的系统升级文件、系统补丁或系统同步信息等,用于为对应的待升级车载设备提供系统升级、维护或更新等服务。例如,当升级程序开发者测试完成后,将智能车辆的升级包交由升级服务器发布,该升级包可以包括多个待升级车载设备的升级包,而针对某个待升级车载设备来说,一个完整的升级包可为如下格式[MetaD,M,σ],其中,MetaD是升级包的元数据(metadata),可包括升级对象(如待升级车载设备的具体型号)、升级文件类型(如\delta,complete)、当前版本信息、历史版本信息和操作系统信息等,M是用于执行升级的文件,σ=Sign(MetaD||M)是签于MetaD和M(记为MetaD||M)之上的数字签名,可由升级程序经开发者或是升级服务器提供。可选的,所述升级文件可以为上述MetaD||M,进一步可选的,所述升级文件可以经过数字签名,即为携带上述数字签名的升级文件[MetaD,M,σ]。在本发明实施例中,通信设备利用第一密钥对升级文件进行第一安全处理,可以是对升级文件MetaD||M进行第一安全处理,假如升级文件经过数字签名,则通信设备需要先对[MetaD,M,σ]中的数字签名σ进行验签,如果验签通过,再对MetaD||M进行第一安全处理。即无论所述升级文件是否经过数字签名或者其它安全保护,本发明实施例中的第一安全处理所针对的升级文件都可以是针对升级文件本身,而不包含上述签名信息或保护信息。进一步可选的,通信设备可以将该数字签名σ与第一升级文件数据一起发送给车载控制设备,使得车载控制设备在对第一升级文件数据进行第二安全处理之前,先验证该第一升级文件数据中的升级文件是否是安全合法的,若是,才继续进行第二安全处理,否则放弃升级过程。在一种可能的实现方式中,本发明实施例中的通信设备、车载控制设备均可以通过上述升级文件中的MetaD中的升级对象(如待升级车载设备的具体型号)来确定该升级文件具体是针对哪个待升级车载设备的,以便于通信设备使用与之匹配的第一密钥,以及车载控制设备使用与之匹配的第二密钥和将第二升级文件数据发送到对应的待升级车载设备上。

[0208] 在上述步骤S901-S903中,通信设备存储并使用的第一密钥和车载控制设备存储并使用的第二密钥可以是由智能车辆内部生成的目标密钥拆分而来,也可以是智能车辆内部初始生成的两个密钥。可选的,第一密钥和第二密钥也可以是由相关服务器(如升级服务器、密钥服务器或其它服务器等)生成目标密钥并拆分而来,再分别发送给对应设备;还可

以是相关服务器生成目标密钥之后发送到车载控制设备或待升级车载设备上进行拆分的。而无论是拆分而来还是初始生成的，该第一密钥和第二密钥均是作为完整密钥的一部分，共同参与车载控制设备和待升级车载设备之间的安全处理过程，若攻击者只获得了第一密钥或第二密钥，都无法对升级文件进行伪造或篡改。因此，通信设备利用完整密钥中的一部分密钥即第一密钥对升级文件进行第一安全处理，从而生成第一升级文件数据并发送给车载控制设备，目的是使用该部分密钥生成升级文件的部分验证信息，即作为完整验证信息中的一部分，使得车载控制设备无需利用第一密钥和第二密钥进行密钥还原得到完整密钥后才能生成完整验证信息，避免第一密钥和第二密钥同时以明文形式出现在车载控制设备上导致的完整密钥容易被窃取或篡改的情况。而车载控制设备利用第二密钥对上述第一升级文件数据进行第二安全处理，其目的则是让利用第一密钥进行安全处理过的第一升级文件数据，作为第二升级文件数据中的部分验证信息，并利用第二密钥对该部分验证信息和升级文件进行进一步的安全处理，最终发送给待升级车载设备使其需要经过与第一密钥和第二密钥分别匹配的校验密钥共同参与进行安全校验，才可以验证升级文件的安全性。

[0209] 其中，第一安全处理可以是利用第一密钥生成升级文件的消息认证码MAC，也可以是利用第一密钥生成数字签名或者加密处理等；第二安全处理可以是利用第二密钥生成第一升级文件数据的MAC，也可以是利用第二密钥生成第一升级文件数据的数字签名或者加密处理等。即第一安全处理和第二安全处理的具体方式可以根据车载控制设备和待升级车载设备之间的实际安全传输需求，设置不同的安全处理方式，本发明实施例对此不作具体限定。例如，当需要保证升级文件的完整性、来源的真实性时，则安全处理方式可以为生成MAC；当需要保证升级文件的完整性、来源真实性以及不可抵赖性时，则安全处理方式可以为生成数字签名，当需要保证升级文件的保密性时，则安全处理方式可以为对称加密或非对称加密。可选的，第一安全处理和第二安全处理可以是上述方式的任意组合。例如，第一安全处理可以为利用第一密钥生成升级文件的MAC，第二安全处理为利用第二密钥生成第一升级文件数据的MAC，即保证了升级文件在智能车辆内部传输的完整性、来源的真实性。又例如，第一安全处理为利用第一密钥生成升级文件的MAC，第二安全处理则是利用第二密钥对第一升级文件数据进行加密，即保证了升级文件在智能车辆内部传输的完整性、来源的真实性以及保密性。

[0210] 在上述步骤S904-S906中，待升级车载设备利用与第一密钥匹配的第三密钥，和与第二密钥匹配的第四密钥来对第二升级文件数据进行安全校验，原因在于第二升级文件数据本质上是经过了第一密钥和第二密钥的两次安全处理的升级文件，对应地，待升级车载设备也需要经过两次校验来验证该第二升级文件数据的安全性。可选的，待升级车载设备上可以是预先存储了第三密钥和第四密钥，也可以是存储了第三密钥和第四密钥拆分前的目标密钥(前提是第一密钥和第二密钥也是由与目标密钥所匹配的密钥拆分而来)，在需要使用时再进行拆分。可选的，第三密钥和第四密钥也可以是由相关服务器(如升级服务器、密钥服务器或其它服务器等)拆分而来，再发送给待升级车载设备的。并且，可以理解的是，车载控制设备和待升级车载设备之间需要预先协商好安全处理方式即对应的校验方式。且第一密钥和第三密钥，以及第二密钥和第四密钥之间的关系，取决于第一安全处理、第二安全处理的具体方式，例如，当第一安全处理为生成MAC，那么第一密钥和第三密钥之间为对称密钥，即第一密钥和第三密钥相同；当第一安全处理方式为生成数字签名，则第一密钥和

第二密钥之间为非对称密钥，即第一密钥和第三密钥之间为公私钥对；当第一安全处理为加密时，则第一密钥和第三密钥之间既可以为对称密钥也可以为非对称密钥。同理第三密钥和第四密钥之间的关系也与第二安全处理的具体方式相关，此处不再赘述。

[0211] 需要说明的是，本发明实施例中，不同的待升级车载设备分别对应的完整密钥(即第一密钥、第二密钥)不同，并且当同一个待升级车载设备上对应多个升级文件时(如进行不同功能模块的升级时)，其不同升级文件分别对应的完整密钥可以相同也可以不同，本发明实施例对此不作具体限定。还需要说明的是，当通信设备是终端设备，则该终端设备需要与智能车辆之间建立匹配关系；若为升级服务器，则该服务器可以是为智能车辆提供升级文件的升级服务器。

[0212] 本发明实施例，通过在智能车辆中车载控制设备上用于与待升级车载设备之间进行安全传输的密钥(不同的待升级车载设备对应不同的密钥)，分散存储到设备升级系统以外的通信设备上，避免密钥以完整的形式存储在车载控制设备上，被攻击者轻易窃取或篡改；且由于该通信设备同时也是向设备升级系统传输升级文件的发送方，因此，除了上述分散存储部分密钥，进一步地，通信设备还可以在向车载控制设备发送升级文件时，利用存储的部分密钥(即第一密钥)对升级文件进行第一安全处理，然后发送给车载控制设备使其可以利用另一部分密钥(即第二密钥)进行进一步的安全处理，最终将该经过第一密钥和第二密钥共同安全处理的升级文件发送给待升级车载设备，而待升级车载设备则使用协商好的第三密钥和第四密钥进行安全校验。使得本应该在车载控制设备上单独完成的对升级文件的安全处理过程，分布在了通信设备和车载控制设备上来共同完成，即分别由通信设备和车载控制设备使用各自的部分密钥参与到升级文件的安全处理中来，而无需将上述两个部分密钥恢复成完整密钥才对升级文件进行安全处理，避免完整密钥出现或存储在车载控制设备上，使得攻击者无法一次性从车载控制设备上获取到完整密钥，极大的减小了攻击者截获或篡改完整密钥的几率，从而保证了升级文件在设备升级系统内部传输的安全性。

[0213] 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，如前述所述，本申请中的设备升级方法还可以应用于，例如小区网关-家庭网关管理智能家电进行升级、服务器-主机管理虚拟机进行系统升级、服务器-路由器管理终端批量系统升级、服务器-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。

[0214] 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10从通信设备、控制设备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S1001A-步骤S1013。

[0215] S1001-A：控制设备生成目标密钥，将所述目标密钥拆分为所述第一密钥和所述第二密钥。

[0216] S1002-A：控制设备将所述第一密钥发送至所述通信设备；并将所述目标密钥发送至所述待升级设备。

[0217] S1003-A：控制设备存储所述第二密钥，并删除所述目标密钥。

[0218] 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，可

替换地，上述步骤S1001-A-步骤S1003-A可以替换为下面的步骤S1001-B-步骤S1003-B，即该方法实施例可以包括以下步骤S100B-步骤S1013。

[0219] S1001-B：待升级设备生成目标密钥，将所述目标密钥拆分为所述第一密钥和所述第二密钥。

[0220] S1002-B：待升级设备将所述第二密钥发送给所述通信设备；将所述第一密钥发送至所述通信设备。

[0221] S1003-B：待升级设备存储所述第二密钥，并删除所述目标密钥。

[0222] S1004：通信设备获取升级文件，并对所述数字签名进行验签，若验签通过，则利用所述第一密钥对所述升级文件进行第一安全处理。

[0223] S1005：通信设备向所述控制设备发送所述第一升级文件数据；控制设备接收通信设备发送的第一升级文件数据。

[0224] S1006：控制设备对所述数字签名进行验签，若验签通过，则利用所述第二密钥对所述第一升级文件数据进行第二安全处理生成第二升级文件数据。

[0225] S1007：控制设备向所述待升级设备发送所述第二升级文件数据；待升级设备接收所述第二升级文件数据。

[0226] S1008：待升级设备将存储的所述目标密钥拆分为所述第三密钥和所述第四密钥。

[0227] S1009：待升级设备利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验。

[0228] S1010：若校验通过，待升级设备则利用所述升级文件进行升级。

[0229] S1011：待升级设备根据所述升级文件升级成功后，向控制设备发送升级成功消息。

[0230] S1012：在待升级设备升级成功后，控制设备指示所述通信设备更新所述升级文件的回滚文件。

[0231] S1013：在待升级设备升级失败后，控制设备从所述通信设备获得所述升级文件的回滚文件，并发送给所述待升级设备进行回滚操作。

[0232] 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，即所述控制设备和待升级设备可以为智能车辆/车载系统中的车载控制设备和待升级车载设备。在上述步骤S1001-A-步骤S1003-A中，车载控制设备生成目标密钥(比如利用密钥生成器生成目标密钥)，并将目标密钥拆分为第一密钥和第二密钥，然后将第一密钥发送给通信设备，并存储第二密钥，其中，由于在本发明实施例中，该目标密钥为对称密钥(即第三密钥与第一密钥相同，第四密钥和第二密钥相同)。因此，车载控制设备需要将该目标密钥发送给待升级车载设备以进行后续的安全校验，可选的，该车载控制设备也可以将第一密钥和第二密钥发送给待升级车载设备。车载控制设备上只需要存储其后续要进行第二安全处理的第二密钥，而将目标密钥发送给了待升级车载设备之后，则可以将该目标密钥进行删除，避免目标密钥在车载控制设备上存储的时间过久，容易被攻击者窃取或篡改。

[0233] 而上述两种发送方式包括以下区别：一方面，若车载控制设备发送的是目标密钥，则待升级设备在进行安全校验之前需要进行目标密钥的拆分；若发送的是第一密钥和第二密钥，则待升级车载设备无需进行目标密钥的拆分，直接使用即可；另一方面，若车载控制设备发送的是目标密钥，则待升级车载设备只需要按照与车载控制设备协商好的密钥拆分

方式进行拆分，即可以具体获知第一密钥和第二密钥；而若发送的是第一密钥和第二密钥，则车载控制设备需要在发送密钥时明确指示两个密钥中哪个是第一密钥哪个是第二密钥；又一方面，对于待升级车载设备来说，若接收到目标密钥，则只需要存储一个密钥即可，若接收到两个密钥则需要存储两份，当该待升级车载设备中有多个升级文件对应的不同的密钥时，则可能会导致存储两份密钥的情况对应的存储量成倍增加。因此，本发明实施例中所提供的上述两种方式可以在不同的场景中根据不同的实际需求，选择采用不同的发送方式。

[0234] 例如，车载控制设备生成一随机密钥k即为目标密钥，车载控制设备利用密码散列函数(cryptographic hash function)“h(.)”计算得到第一密钥k_1，即k_1＝h(k)，进一步地，通过异或运算“⊕”计算第二密钥$k_2 = k \oplus k_1$.;车载设备分别传送k_1给通信设备(移动设备)，以及k给OTA Orchestrator，并保存k_2为自己的密钥(假设传送通道是安全的)。又例如，在另一种可能的实现方式中，k_1＝h(k,a)，k_2＝h(k,b)，其中“h(.)”为密码散列函数，a、b为常数，表示在“h(.)”之后分别叠加对应的二进制值。本发明实施例还可以利用其它的拆分函数或推演算法对目标密钥进行拆分，此处不再一一列举。

[0235] 可选的，在上述步骤S1001-B-步骤S1003-B中，目标密钥也可以由待升级车载设备来生成并拆分。具体地密钥生成过程以及拆分方法可以参照上述S1001-A-步骤S1003-A中车载控制设备生成目标密钥和拆分密钥的具体方式，在此不再赘述。最终，待升级车载设备需要将第一密钥和第二密钥分别发送给通信设备和车载控制设备，而自己存储目标密钥，可选的，也可以存储第一密钥和第二密钥。其中，待升级车载设备可以根据自己的通信能力，将第一密钥直接发送给通信设备，也可以将第一密钥通过车载控制设备转发至通信设备处。例如，若待升级车载设备有较强的通信能力可与通信设备直接通信，则可以将第一密钥发送至通信设备；若待升级车载设备通信能力较弱，无法直接与通信设备直接通信，则可以通过车载控制设备进行转发。

[0236] 可选的，上述目标密钥也可以是由架构二中的密钥服务器生成之后发送给车载控制设备或待升级车载设备的，即基于密钥服务器的专有能力为智能车辆拓展密钥的生成服务。进一步地，目标密钥的拆分或者是初始生成的两个密钥(第一密钥、第二密钥等)，也可以是在该密钥服务器上进行，本发明实施例对此不作具体限定。

[0237] 需要说明的是，车载控制设备将第一密钥发送给通信设备，以及将目标密钥(或第一密钥和第二密钥)发送给待升级车载设备之间；或者，待升级车载设备将第一密钥发送给通信设备，以及将第二密钥发送给车载控制设备之间，没有严格的先后顺序，且本发明实施例对此不作具体限定。

[0238] 在上述步骤S1004至步骤S1007中，通信设备从升级服务器处获取升级文件，由于升级服务器需要证明自己提供的升级文件是安全合法的，因此需要提前对发布的升级文件进行数字签名，例如升级服务器利用私钥签名，而接收到该经过数字签名的升级文件的通信设备则可利用公开的公钥对其进行校验，当校验通过后，证明该升级文件是安全合法的，再进行进一步的安全处理即第一安全处理，若未验证通过，则证明该升级文件已经被攻击者攻击，因此放弃升级。

[0239] 在上述步骤S1004至步骤S1007中，关于通信设备的第一安全处理和车载控制设备的第二安全处理的具体实施方式，可以根据实际的安全传输需求有多种可能的实现方式，

以下提供两种示例性的实施方式：

[0240] 方式一：所述第一安全处理包括根据所述第一密钥生成所述升级文件的第一消息认证码MAC；所述第一升级文件数据包括所述升级文件和所述第一MAC。所述第二安全处理包括根据所述第二密钥生成所述升级文件的第二MAC，并将所述第一MAC和所述第二MAC聚合得到第三MAC；所述第二升级文件数据包括所述升级文件和所述第三MAC。

[0241] 具体地，当通信设备在确认车载设备升级系统需要升级后(例如，接收到车载控制设备的升级系统请求，或者接收到用户发起的升级指令)，则从升级服务器处获取升级文件，可选的，该升级文件经过升级服务器的私钥的数字签名，通信设备在获取升级文件之后，首先对升级文件的数字签名进行验签，若验签通过后，则表示该升级文件为安全合法的，然后通信设备再利用第一密钥对所述升级文件生成第一MAC，得到的(升级文件+第一MAC)即为第一升级文件数据，并发送给车载控制设备，车载控制设备接收到之后，先对(升级文件+第一MAC)中的升级文件生成第二MAC，然后将第一MAC和第二MAC通过预设的聚合算法进行聚合，得到聚合后的验证信息即第三MAC，并将包含(升级文件+第三MAC)的第二升级文件数据发送给待升级车载设备进行验证及升级。可选的，通信设备发送的第一升级文件数据中的升级文件还经过数字签名，此时第一升级文件数据包括(升级文件+数字签名+第一MAC)，车载控制设备接收到该第一升级文件数据之后，则需要先对上述数字签名进行验签，若验签通过则证明该从通信设备发送过来的升级文件，是由升级服务器所提供的安全合法的升级文件，且中途没有被非法篡改，然后再对验签后的第一升级文件数据(升级文件+第一MAC)进行第二安全处理，具体可以参照上述有关第二安全处理的相关描述，在此不再赘述。

[0242] 例如，移动设备获取升级包，并验证数字签名σ，如验证失败则放弃升级，如验证成功，则提示用户进行升级，若用户允许，则过蓝牙连接车载OTA Orchestrator，；然后，移动设备利用密钥k_1，计算升级文件MetaD||M的MAC值即为第一MAC，为τ_1＝MAC(k_1,MetaD||M)，并将第一升级文件数据[MetaD,M,σ,τ_1]发送给OTA Orchestrator；OTA Orchestrator验证σ，如验证失败则放弃升级，如验证成功，则OTA Orchestrator利用k_2计算升级文件的聚合验证信息，首先计算第二MAC，为τ_2＝MAC(k_2,MetaD||M)，再计算聚合验证信息第三MAC，为$\tau = \tau_1 \oplus \tau_2$，最终，车载OTA Orchestrator将第二升级文件数据[MetaD,M,τ]发送给待升级车载设备进行安全升级。

[0243] 方式二：所述第一安全处理包括根据所述第一密钥生成所述升级文件的第一消息认证码MAC；所述第一升级文件数据包括所述升级文件和所述第一MAC。所述第二安全处理包括根据所述第二密钥生成所述第一升级文件数据的第四MAC；所述第二升级文件数据包括所述升级文件和所述第四MAC。

[0244] 具体地，该方式中的第一安全处理与上述方式一中的第一安全处理相同，在此不再赘述，而针对第二安全处理方式，则是对整个第一升级文件数据(升级文件+第一MAC)生成第四MAC，而该第四MAC即为聚合后的验证信息，与升级文件、第一密钥和第二密钥均相关，因此车载控制设备将包含(升级文件+第四MAC)的第二升级文件数据发送给待升级车载设备进行安全升级。可选的，关于通信设备发送的第一升级文件数据中的升级文件还经过数字签名，车载控制设备的验签处理过程可参考上述方式一中的相关处理流程，在此不再赘述。

[0245] 例如，移动设备获取升级包，并验证数字签名σ，如验证失败则放弃升级，如验证成功，则提示用户进行升级，若用户允许，则过蓝牙连接车载OTA Orchestrator，；然后，移动设备利用密钥k_1，计算升级文件MetaD||M的MAC值即为第一MAC，为τ_1＝MAC(k_1,MetaD||M)，并将第一升级文件数据[MetaD,M,σ,τ_1]发送给OTA Orchestrator；OTA Orchestrator验证σ，如验证失败则放弃升级，如验证成功，则OTA Orchestrator利用k_2计算升级文件的聚合验证信息，即第四MAC为，τ＝MAC(k_2,MetaD||M||τ_1)，最终，车载OTA Orchestrator将第二升级文件数据[MetaD,M,τ]发送给待升级车载设备进行安全升级。

[0246] 上述两种方式，由于对升级文件生成消息认证码可以保证升级文件的完整性和来源的真实性，因此可以解决升级文件在设备升级系统中传输时，可能被攻击者篡改和伪造的问题，并且生成MAC的过程使用的是对称密钥，因此可以在保证数据安全性的基础上，减少安全校验的计算量，提升升级效率。

[0247] 在上述步骤S1009至步骤S1010中，待升级车载设备先将存储的目标密钥拆分为第三密钥和第四密钥，并对第二升级文件数据进行安全校验，若校验通过则进行升级，若校验未通过则放弃升级。

[0248] 对应上述方式一中的第一安全处理和第二安全处理的实施方式时，待升级车载设备则需要利用第三密钥(由于目标密钥为对称密钥，因此与第一密钥相同)对第二升级文件数据(升级文件+第三MAC)中的升级文件生成一个MAC，与此同时，利用第四密钥(由于目标密钥为对称密钥，因此与第二密钥相同)对第二升级文件数据(升级文件+第三MAC)中的升级文件生成另一个MAC，然后再将该生成的两个MAC按照车载控制设备上的聚合方式进行聚合，得到一个MAC，然后将该一个MAC与第三MAC进行比对，若相同，则表示安全校验通过，即可以进行安全升级。

[0249] 对应上述方式二中的第一安全处理和第二安全处理的实施方式时，待升级车载设备则需要利用第三密钥对第二升级文件数据(升级文件+第三MAC)中的升级文件生成一个MAC，进一步地，利用第四密钥对第二升级文件数据(升级文件+该生成的一个MAC)生成一个聚合MAC，然后再将该聚合MAC与第三MAC进行比对，若相同，则表示安全校验通过，即可以进行安全升级。

[0250] 在上述步骤S1011至步骤S1013中，当待升级车载设备升级成功，则可以向车载控制设备反馈升级成功消息，所述升级成功消息为经过所述第四密钥的安全保护的消息，如此一来，车载控制设备则可以通过存储的第二密钥进行安全校验，以达到安全传输和复用第二密钥和第四密钥的目的。进一步地，当待升级车载设备升级成功，车载控制设备可以指示通信设备更新当前升级成功的回滚文件，以便于下次需要重新获取该升级文件时有回滚文件可以获取，达到通过通信设备的存储能力对智能车辆进行存储扩展。当待升级车载设备升级失败了，则可以向车载控制设备反馈升级失败消息，此时车载控制设备可以从通信设备处(可以理解的是，通信设备上需要保管有升级文件的回滚文件)获取升级文件的回滚文件并发送给待升级车载设备进行回滚操作。本发明实施例，通信设备可以为智能车辆提供升级文件的回滚文件，无论在待升级车载设备升级成功或者失败的情况下，通信设备都可以对当前的升级文件进行回滚操作，以便于待升级车载设备后续升级时有回滚文件可以参考。

[0251] 在一种可能的实现方式中，待升级车载设备在升级之前，还检验升级文件中的升

级包的元数据MetaD,并根据升级包及设备的类型进行升级。例如,如果升级文件是\delta文件,则需先生成全二进制(full binary);如升级文件是full binary,则可直接开始刷新;对于强设备可用A/B系统更新(A/B System Updates)升级模式,即目标待升级车载设备有A区和B区,待升级程序(固件或软件)运行于A区,新的升级程序则写入B区,升级完成后再切换到B去执行,不影响车载升级过程中,旧版系统的正常运行,而对弱设备需要就地升级(in place)模式升级,即直接用新的升级文件替换现有升级文件。

[0252] 本申请基于上述设备升级方法实施例,还提供一种车载控制设备获取升级文件的方式,在一种可能的实现方式中,通信设备从升级服务器处获取升级文件时,车载控制设备也从升级服务器处获取升级文件,如此一来,通信设备发送给车载控制设备的第一升级文件数据中可以不包含升级文件本身,而是只包含了利用第一密钥对升级文件生成的验证信息如第一MAC,而车载控制设备则利用第二密钥对从服务器获取的升级文件、第一升级文件数据生成第二升级文件数据,最终完成后续的安全升级过程。需要说明的是,在上述实现方式中,通信设备和车载控制设备均需要对从升级服务器处获取的升级文件进行数据签名的验签,以证明第一安全处理和第二安全处理所针对的是相同的升级文件。

[0253] 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,如前述所述,本申请中的设备升级方法还可以应用于,例如小区网关-家庭网关管理智能家电进行升级、服务器-主机管理虚拟机进行系统升级、服务器-路由器管理终端批量系统升级、服务器-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。

[0254] 本发明实施例还提供一种车载设备升级方法,可应用于车载系统,所述车载系统包括车载控制设备和待升级车载设备。关于车载控制设备和待升级车载设备所执行的方法流程,可参见上述图1-图11所述的方法实施例中控制设备和待升级设备所执行的方法流程的相关描述,此处不再赘述。

[0255] 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。

[0256] 请参见图12,图12是本发明实施例提供的一种通信设备的结构示意图,该通信设备10可以应用于设备升级系统,如上述图4或图8的系统架构中,通信设备10各个单元的详细描述如下。

[0257] 安全处理单元101,用于利用第一密钥对升级文件进行第一安全处理,生成第一升级文件数据;

[0258] 发送单元102,用于向控制设备发送所述第一升级文件数据;其中,

[0259] 所述第一升级文件数据用于所述控制设备利用第二密钥对所述第一升级文件数据进行第二安全处理,生成第二升级文件数据,并向待升级设备发送所述第二升级文件数据;

[0260] 所述第二升级文件数据用于所述待升级设备利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验,若校验通过,则利用所述升级文件进行升级;其中,所述第三密钥为所述第一密钥匹配的校验密钥,所述第四密钥为所述第二密钥匹配的校验密钥。

[0261] 在一种可能的实现方式中,所述第一安全处理包括根据所述第一密钥生成所述升级文件的第一消息认证码MAC;所述第一升级文件数据包括所述升级文件和所述第一MAC。

[0262] 在一种可能的实现方式中，所述第二安全处理包括根据所述第二密钥生成所述升级文件的第二MAC，并将所述第一MAC和所述第二MAC聚合得到第三MAC；所述第二升级文件数据包括所述升级文件和所述第三MAC。

[0263] 在一种可能的实现方式中，所述第二安全处理包括根据所述第二密钥生成所述第一升级文件数据的第四MAC；所述第二升级文件数据包括所述升级文件和所述第四MAC。

[0264] 在一种可能的实现方式中，所述第一密钥和所述第三密钥为对称密钥，所述第二密钥和所述第四密钥为对称密钥；所述第一密钥和所述第二密钥为所述控制设备将生成的目标密钥拆分后的密钥，其中，所述目标密钥还用于由所述控制设备发送至所述待升级设备进行存储；所述通信设备还包括：接收单元103，用于接收所述控制设备发送的所述第一密钥。

[0265] 在一种可能的实现方式中，所述第一密钥和所述第三密钥为对称密钥，所述第二密钥和所述第四密钥为对称密钥；所述第一密钥和所述第二密钥为所述待升级设备将生成的目标密钥拆分后的密钥；所述通信设备还包括：接收单元103，用于接收所述待升级设备发送的所述第一密钥。

[0266] 在一种可能的实现方式中，所述第三密钥和所述第四密钥为所述待升级设备在利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验之前，将存储的所述目标密钥拆分后的密钥。

[0267] 在一种可能的实现方式中，所述升级文件经过数字签名；所述第一升级文件数据为所述通信设备在获取所述升级文件，并对所述数字签名进行验签通过后，利用所述第一密钥对所述升级文件进行第一安全处理后生成的升级文件数据。

[0268] 在一种可能的实现方式中，所述升级文件经过数字签名；所述安全处理单元，具体用于获取所述升级文件，并对所述数字签名进行验签，若验签通过，则利用所述第一密钥对所述升级文件进行第一安全处理。

[0269] 在一种可能的实现方式中，所述第一升级文件数据中的升级文件还经过数字签名；所述第一升级文件数据具体用于所述控制设备对所述数字签名进行验签，若验签通过，则利用第二密钥对所述第一升级文件数据进行第二安全处理，生成第二升级文件数据。

[0270] 在一种可能的实现方式中，所述通信设备还包括第一回滚单元104，用于在所述待升级设备升级成功后，接收所述控制设备发送的更新所述升级文件的回滚文件的指示；和/或，所述通信设备还包括第二回滚单元105，用于在所述待升级设备升级失败后，向所述控制设备发送所述升级文件的回滚文件，以用于所述待升级设备进行回滚操作。

[0271] 在一种可能的实现方式中，所述第一密钥和所述第二密钥是由服务器生成目标密钥并拆分而来，并由所述服务器分别发送至所述通信设备和所述控制设备的。可选的，所述服务器生成目标密钥之后发送到所述控制设备或所述待升级车载设备上进行拆分。例如，所述服务器为升级服务器、密钥服务器或其它服务器等。本发明实施例中，目标密钥的生成和/或目标密钥的拆分过程可以是由服务器来执行，可减少控制设备和待升级设备的计算量，提升升级效率。

[0272] 在一种可能的实现方式中，所述第三密钥和所述第四密钥是由服务器拆分而来，再发送至所述待升级车载设备的。例如，所述服务器为升级服务器、密钥服务器或其它服务器等。本发明实施例中，第三密钥和第四密钥对应的原始密钥的生成和/或拆分，可以是由

服务器来执行,可减少控制设备和待升级设备的计算量,提升升级效率。

[0273] 需要说明的是,本发明实施例中所描述的通信设备10中各功能单元的功能可参见上述图1-图11所述的方法实施例中通信设备的相关描述,此处不再赘述。

[0274] 请参见图13,图13是本发明实施例提供的一种控制设备的结构示意图,该控制设备20可应用于设备升级系统,如上述图4或图8的系统架构中,控制设备20各个单元的详细描述如下。

[0275] 第一接收单元201,用于接收通信设备发送的第一升级文件数据,所述第一升级文件数据为所述通信设备利用第一密钥对升级文件进行第一安全处理后生成的升级文件数据;

[0276] 安全处理单元202,用于利用第二密钥对所述第一升级文件数据进行第二安全处理,生成第二升级文件数据,并向待升级设备发送所述第二升级文件数据;其中,

[0277] 所述第二升级文件数据,用于所述待升级设备所述利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验,若校验通过,则利用所述升级文件进行升级;其中,所述第三密钥为所述第一密钥匹配的校验密钥,所述第四密钥为所述第二密钥匹配的校验密钥。

[0278] 在一种可能的实现方式中,所述第一安全处理包括根据所述第一密钥生成所述升级文件的第一消息认证码MAC;所述第一升级文件数据包括所述升级文件和所述第一MAC。

[0279] 在一种可能的实现方式中,所述第二安全处理包括根据所述第二密钥生成所述升级文件的第二MAC,并将所述第一MAC和所述第二MAC聚合得到第三MAC;所述第二升级文件数据包括所述升级文件和所述第三MAC。

[0280] 在一种可能的实现方式中,所述第二安全处理包括根据所述第二密钥生成所述第一升级文件数据的第四MAC;所述第二升级文件数据包括所述升级文件和所述第四MAC。

[0281] 在一种可能的实现方式中,所述第一密钥和所述第三密钥为对称密钥,所述第二密钥和所述第四密钥为对称密钥;所述控制设备还包括:密钥生成单元203,用于生成目标密钥,将所述目标密钥拆分为所述第一密钥和所述第二密钥;发送单元204,用于将所述目标密钥发送至所述待升级设备,将所述第一密钥发送至所述通信设备;密钥存储单元205,用于存储所述第二密钥,并删除所述目标密钥。

[0282] 在一种可能的实现方式中,如图14所示,图14是本发明实施例提供的另一种控制设备的结构示意图,所述第一密钥和所述第三密钥为对称密钥,所述第二密钥和所述第四密钥为对称密钥;所述第一密钥和所述第二密钥为所述待升级设备将生成的目标密钥拆分后的密钥;所述控制设备还包括:第二接收单元206,用于接收所述待升级设备发送的所述第二密钥。

[0283] 在一种可能的实现方式中,所述第三密钥和所述第四密钥为所述待升级设备在对所述第二升级文件数据进行安全校验之前,将存储的所述目标密钥拆分后的密钥。

[0284] 在一种可能的实现方式中,所述升级文件经过数字签名;所述第一升级文件数据为所述通信设备在获取所述升级文件,并对所述数字签名进行验签通过后,利用所述第一密钥对所述升级文件进行第一安全处理后生成的升级文件数据。

[0285] 在一种可能的实现方式中,所述第一升级文件数据中的升级文件还经过数字签名;所述安全处理单元,具体用于在利用第二密钥对所述第一升级文件数据进行第二安全

处理之前，对所述数字签名进行验签，若验签通过，则利用所述第二密钥对所述第一升级文件数据进行第二安全处理。

[0286] 在一种可能的实现方式中，所述控制设备，还包括第三接收单元207，用于接收所述待升级设备在根据所述升级文件升级成功后发送的升级成功消息，所述升级成功消息为经过所述第四密钥的安全保护的消息。

[0287] 在一种可能的实现方式中，所述控制设备，还包括第一回滚单元208，用于在确认所述待升级设备升级成功后，指示所述通信设备更新所述升级文件的回滚文件；和/或所述控制设备，还包括第二回滚单元209，用于在确认所述待升级设备升级失败后，从所述通信设备获取所述升级文件的回滚文件，并发送给所述待升级设备进行回滚操作。

[0288] 在一种可能的实现方式中，所述第一密钥和所述第二密钥是由服务器生成目标密钥并拆分而来，并由所述服务器分别发送至所述通信设备和所述控制设备的。可选的，所述服务器生成目标密钥之后发送到所述控制设备或所述待升级车载设备上进行拆分。例如，所述服务器为升级服务器、密钥服务器或其它服务器等。本发明实施例中，目标密钥的生成和/或目标密钥的拆分过程可以是由服务器来执行，可减少控制设备和待升级设备的计算量，提升升级效率。

[0289] 在一种可能的实现方式中，所述第三密钥和所述第四密钥是由服务器拆分而来，再发送至所述待升级车载设备的。例如，所述服务器为升级服务器、密钥服务器或其它服务器等。本发明实施例中，第三密钥和第四密钥对应的原始密钥的生成和/或拆分，可以是由服务器来执行，可减少控制设备和待升级设备的计算量，提升升级效率。

[0290] 需要说明的是，本发明实施例中所描述的控制设备20中各功能单元的功能可参见上述图1-图11所述的方法实施例中控制设备的相关描述，此处不再赘述。

[0291] 请参见图15，图15是本发明实施例提供的一种待升级设备的结构示意图，该待升级设备30可应用于设备升级系统，如上述图4或图8的系统架构中，待升级设备30各个单元的详细描述如下。

[0292] 第一接收单元301，用于接收控制设备发送的第二升级文件数据，所述第二升级文件数据为所述控制设备利用第二密钥对通信设备发送的第一升级文件数据进行第二安全处理，生成的升级文件数据，所述第一升级文件数据为所述通信设备利用第一密钥对升级文件进行第一安全处理后生成的升级文件数据；

[0293] 安全校验单元302，用于利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验，所述第三密钥为所述第一密钥匹配的校验密钥，所述第四密钥为所述第二密钥匹配的校验密钥；

[0294] 升级单元303，用于若校验通过，则利用所述升级文件进行升级。

[0295] 在一种可能的实现方式中，所述第一安全处理包括根据所述第一密钥生成所述升级文件的第一消息认证码MAC；所述第一升级文件数据包括所述升级文件和所述第一MAC。

[0296] 在一种可能的实现方式中，所述第二安全处理包括根据所述第二密钥生成所述升级文件的第二MAC，并将所述第一MAC和所述第二MAC聚合得到第三MAC；所述第二升级文件数据包括所述升级文件和所述第三MAC。

[0297] 在一种可能的实现方式中，所述第二安全处理包括根据所述第二密钥生成所述第一升级文件数据的第四MAC；所述第二升级文件数据包括所述升级文件和所述第四MAC。

[0298] 请参见图16,图16是本发明实施例提供的另一种待升级设备的结构示意图,在一种可能的实现方式中,所述第一密钥和所述第三密钥为对称密钥,所述第二密钥和所述第四密钥为对称密钥;所述第一密钥和所述第二密钥为所述控制设备将生成的目标密钥拆分后的密钥,所述待升级设备还包括:第二接收单元304,用于接收所述控制设备发送的所述目标密钥。

[0299] 在一种可能的实现方式中,所述第一密钥和所述第三密钥为对称密钥,所述第二密钥和所述第四密钥为对称密钥;所述待升级设备还包括:第一密钥生成单元305,用于生成目标密钥,将所述目标密钥拆分为所述第一密钥和所述第二密钥;发送单元306,用于将所述第一密钥发送给所述通信设备,以及将所述第二密钥发送给所述控制设备;密钥存储单元307,用于存储所述目标密钥,并删除所述第一密钥和所述第二密钥。

[0300] 在一种可能的实现方式中,所述待升级设备还包括:第二密钥生成单元308,用于在利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验之前,将存储的所述目标密钥拆分为所述第三密钥和所述第四密钥。

[0301] 在一种可能的实现方式中,所述升级文件经过数字签名;所述第一升级文件数据为所述通信设备在获取所述升级文件,并对所述数字签名进行验签通过后,利用所述第一密钥对所述升级文件进行第一安全处理后生成的升级文件数据。

[0302] 在一种可能的实现方式中,所述第一升级文件数据中的升级文件还经过数字签名;所述第二升级文件数据为所述控制设备对通信设备发送的所述第一升级文件数据中的所述数字签名进行验签,并验签通过后,利用第二密钥对所述第一升级文件数据进行第二安全处理生成的升级文件数据。

[0303] 在一种可能的实现方式中,所述待升级设备还包括反馈单元309,用于在根据所述升级文件升级成功后,向所述控制设备发送升级成功消息,所述升级成功消息为经过所述第四密钥的安全保护的消息。

[0304] 在一种可能的实现方式中,所述待升级设备还包括回滚单元310,用于在确认所述待升级设备升级失败后,从所述控制设备获取所述升级文件的回滚文件,进行回滚操作。

[0305] 在一种可能的实现方式中,所述第一密钥和所述第二密钥是由服务器生成目标密钥并拆分而来,并由所述服务器分别发送至所述通信设备和所述控制设备的。可选的,所述服务器生成目标密钥之后发送到所述控制设备或所述待升级车载设备上进行拆分。例如,所述服务器为升级服务器、密钥服务器或其它服务器等。本发明实施例中,目标密钥的生成和/或目标密钥的拆分过程可以是由服务器来执行,可减少控制设备和待升级设备的计算量,提升升级效率。

[0306] 在一种可能的实现方式中,所述第三密钥和所述第四密钥是由服务器拆分而来,再发送至所述待升级车载设备的。例如,所述服务器为升级服务器、密钥服务器或其它服务器等。本发明实施例中,第三密钥和第四密钥对应的原始密钥的生成和/或拆分,可以是由服务器来执行,可减少控制设备和待升级设备的计算量,提升升级效率。

[0307] 需要说明的是,本发明实施例中所描述的待升级设备30中各功能单元的功能可参见上述图1-图11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。

[0308] 请参见图17,图17是本发明实施例提供的一种智能车辆的结构示意图,该智能车辆40包括车载控制设备50和至少一个第一待升级车载设备60(图11中以多个为例);

[0309] 所述车载控制设备50，用于接收通信设备发送的第一升级文件数据，所述第一升级文件数据为所述通信设备利用第一密钥对升级文件进行第一安全处理后生成的升级文件数据；所述车载控制设备50，用于利用第二密钥对所述第一升级文件数据进行第二安全处理，生成第二升级文件数据，并向所述待升级车载设备发送所述第二升级文件数据；所述待升级车载设备60，用于接收所述第二升级文件数据，利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验，若校验通过，则利用所述升级文件进行升级；其中，所述第三密钥为所述第一密钥匹配的校验密钥，所述第四密钥为所述第二密钥匹配的校验密钥。

[0310] 在一种可能的实现方式中，所述第一安全处理包括根据所述第一密钥生成所述升级文件的第一消息认证码MAC；所述第一升级文件数据包括所述升级文件和所述第一MAC。

[0311] 在一种可能的实现方式中，所述第二安全处理包括根据所述第二密钥生成所述升级文件的第二MAC，并将所述第一MAC和所述第二MAC聚合得到第三MAC；所述第二升级文件数据包括所述升级文件和所述第三MAC。

[0312] 在一种可能的实现方式中，所述第二安全处理包括根据所述第二密钥生成所述第一升级文件数据的第四MAC；所述第二升级文件数据包括所述升级文件和所述第四MAC。

[0313] 在一种可能的实现方式中，所述第一密钥和所述第三密钥为对称密钥，所述第二密钥和所述第四密钥为对称密钥；所述车载控制设备50，还用于生成目标密钥，将所述目标密钥拆分为所述第一密钥和所述第二密钥；将所述目标密钥发送至所述待升级车载设备，将所述第一密钥发送至所述通信设备；存储所述第二密钥，并删除所述目标密钥。

[0314] 在一种可能的实现方式中，所述第一密钥和所述第三密钥为对称密钥，所述第二密钥和所述第四密钥为对称密钥；所述待升级车载设备60，用于生成目标密钥，将所述目标密钥拆分为所述第一密钥和所述第二密钥；将所述第一密钥发送给所述通信设备，以及将所述第二密钥发送给所述车载控制设备；存储所述目标密钥，并删除所述第一密钥和所述第二密钥。

[0315] 在一种可能的实现方式中，所述待升级车载设备60，还用于在利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验之前，将存储的所述目标密钥拆分为所述第三密钥和所述第四密钥。

[0316] 在一种可能的实现方式中，所述升级文件经过数字签名；所述第一升级文件数据为所述通信设备在获取所述升级文件，并对所述数字签名进行验签通过后，利用所述第一密钥对所述升级文件进行第一安全处理后生成的升级文件数据。

[0317] 在一种可能的实现方式中，所述第一升级文件数据中的升级文件还经过数字签名

[0318] 所述车载控制设备50，还用于在利用第二密钥对所述第一升级文件数据进行第二安全处理之前，对所述数字签名进行验签，若验签通过，则利用所述第二密钥对所述第一升级文件数据进行第二安全处理。

[0319] 在一种可能的实现方式中，所述待升级车载设备60，还用于在根据所述升级文件升级成功后，向所述车载控制设备发送升级成功消息，所述升级成功消息为经过所述第四密钥的安全保护的消息。

[0320] 在一种可能的实现方式中，所述车载控制设备50，还用于在确认所述待升级车载设备升级成功后，指示所述通信设备更新所述升级文件的回滚文件；和/或

[0321] 所述车载控制设备50，还用于在确认所述待升级车载设备升级失败后，从所述通

信设备获取所述升级文件的回滚文件，并发送给所述待升级车载设备进行回滚操作。

[0322] 在一种可能的实现方式中，所述第一密钥和所述第二密钥是由服务器生成目标密钥并拆分而来，并由所述服务器分别发送至所述通信设备和所述车载控制设备的。可选的，所述服务器生成目标密钥之后发送到所述车载控制设备或所述待升级车载设备上进行拆分。例如，所述服务器为升级服务器、密钥服务器或其它服务器等。本发明实施例中，目标密钥的生成和/或目标密钥的拆分过程可以是由服务器来执行，可减少车载控制设备和待升级车载设备的计算量，提升升级效率。

[0323] 在一种可能的实现方式中，所述第三密钥和所述第四密钥是由服务器拆分而来，再发送至所述待升级车载设备的。例如，所述服务器为升级服务器、密钥服务器或其它服务器等。本发明实施例中，第三密钥和第四密钥对应的原始密钥的生成和/或拆分，可以是由服务器来执行，可减少车载控制设备和待升级车载设备的计算量，提升升级效率。

[0324] 需要说明的是，本发明实施例中所描述的智能车辆10中的车载控制设备50和待升级车载设备60可参见上述图1和图11中所述的方法实施例中的车载控制设备和待升级车载设备相关描述，此处不再赘述。

[0325] 可以理解的是，智能车辆10还可以运用计算机、现代传感、信息融合、通讯、人工智能及自动控制等技术，集成智能驾驶系统、生活服务系统、安全防护系统、位置服务系统以及用车服务系统等功能，本申请对此不作具体限定，也不再赘述。

[0326] 请参见图18，图18是本发明实施例提供的一种车载设备升级系统的结构示意图，该车载设备升级系统70包括通信设备10、车载控制设备50和至少一个待升级车载设备60(图18中以多个为例)；请参见图19，图19是本发明实施例提供的另一种车载设备升级系统的结构示意图，该车载设备升级系统80包括车载控制设备50和至少一个待升级车载设备60(图19中以多个为例)。具体地，车载设备升级系统70和车载设备升级系统80的相关功能可参见上述图1至图11中所述的方法实施例中的相关描述，此处不再赘述。

[0327] 如图20所示，图20是本发明实施例提供的一种设备的结构示意图。智能车辆40中的车载控制设备50和待升级车载设备60，以及通信设备10，均可以以图20中的结构来实现，该设备90包括至少一个处理器901，至少一个存储器902、至少一个通信接口903。此外，该设备还可以包括天线等通用部件，在此不再详述。

[0328] 处理器901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。

[0329] 通信接口903，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。

[0330] 存储器902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。

[0331] 其中，所述存储器902用于存储执行以上方案的应用程序代码，并由处理器901来控制执行。所述处理器901用于执行所述存储器902中存储的应用程序代码以实现车载控制设备50和待升级车载设备60，以及通信设备10的相关功能。

[0332] 需要说明的是，本发明实施例中所描述的车载控制设备50和待升级车载设备60，以及通信设备10的功能可参见上述图1至图11中的所述的方法实施例中的相关描述，此处不再赘述。

[0333] 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。

[0334] 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。

[0335] 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。

[0336] 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。

[0337] 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。

[0338] 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。

[0339] 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。

[0340] 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。

[0341] 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。

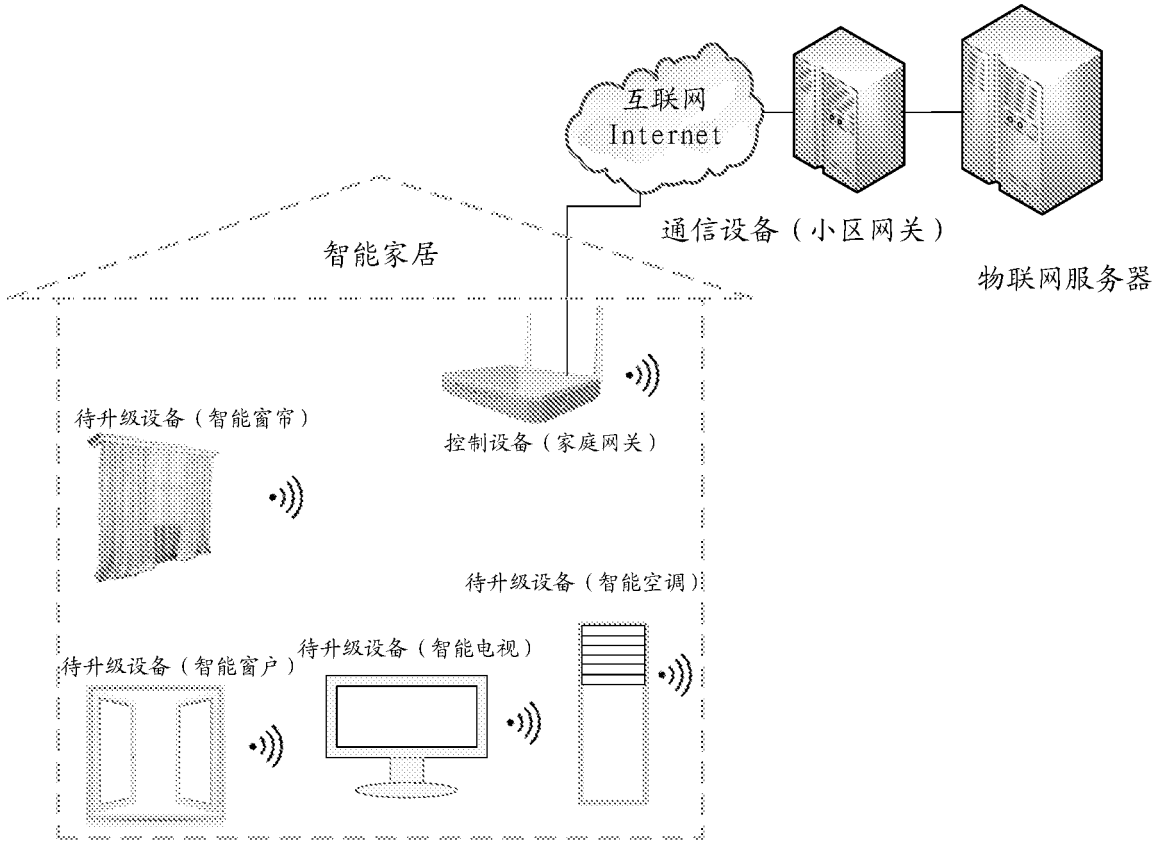

互联网
Internet
通信设备（小区网关）
物联网服务器
智能家居
控制设备（家庭网关）
待升级设备（智能窗帘）
待升级设备（智能空调）
待升级设备（智能窗户）
待升级设备（智能电视）

图1

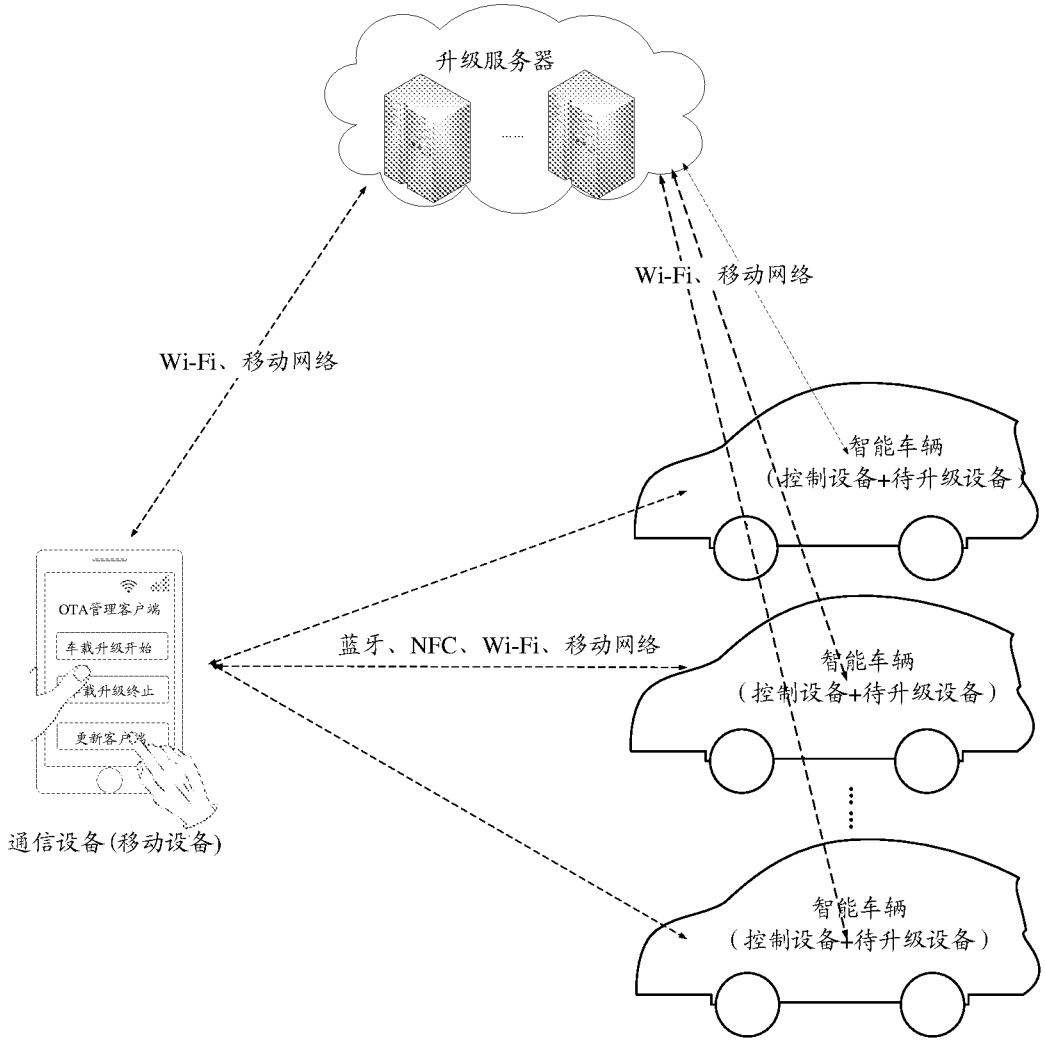

升级服务器
Wi-Fi、移动网络
Wi-Fi、移动网络
智能车辆
（控制设备+待升级设备）
OTA管理客户端
车载升级开始
车载升级终止
更新客户端
蓝牙、NFC、Wi-Fi、移动网络
智能车辆
（控制设备+待升级设备）
智能车辆
（控制设备+待升级设备）
通信设备(移动设备)

图2

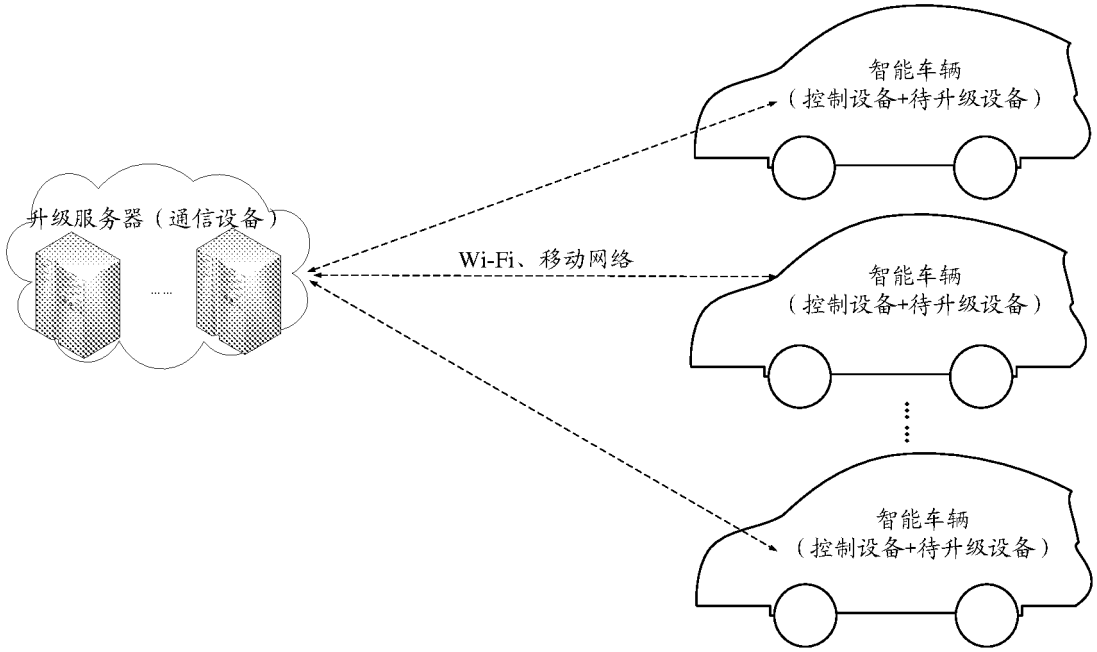

智能车辆
（控制设备+待升级设备）
升级服务器（通信设备）
Wi-Fi、移动网络
智能车辆
（控制设备+待升级设备）
智能车辆
（控制设备+待升级设备）

图3

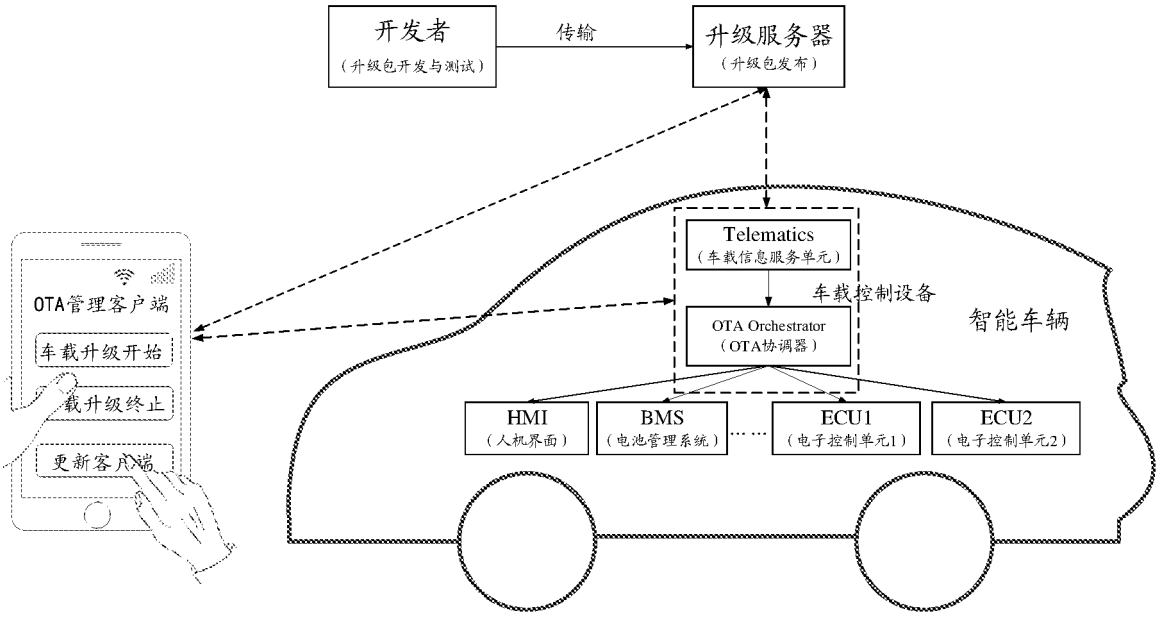

开发者
（升级包开发与测试）
传输
升级服务器
（升级包发布）
OTA管理客户端
车载升级开始
载升级终止
更新客户端
Telematics
（车载信息服务单元）
车载控制设备
OTA Orchestrator
（OTA协调器）
智能车辆
HMI
（人机界面）
BMS
（电池管理系统）
ECU1
（电子控制单元1）
ECU2
（电子控制单元2）

图4

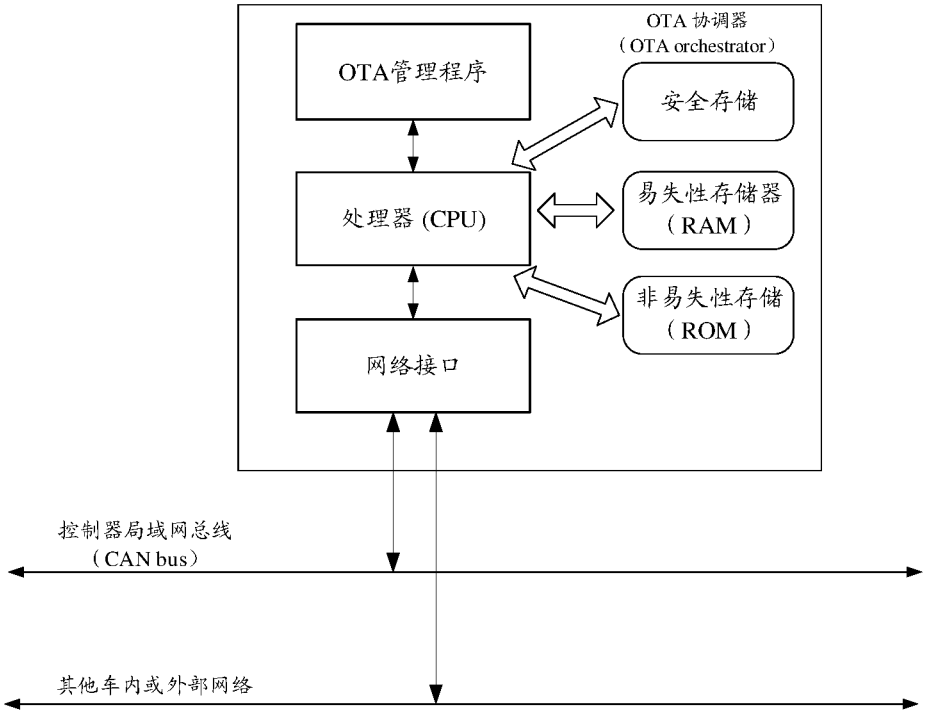

OTA 协调器
（OTA orchestrator）
OTA管理程序
安全存储
处理器 (CPU)
易失性存储器
（RAM）
非易失性存储
（ROM）
网络接口
控制器局域网总线
（CAN bus）
其他车内或外部网络

图5

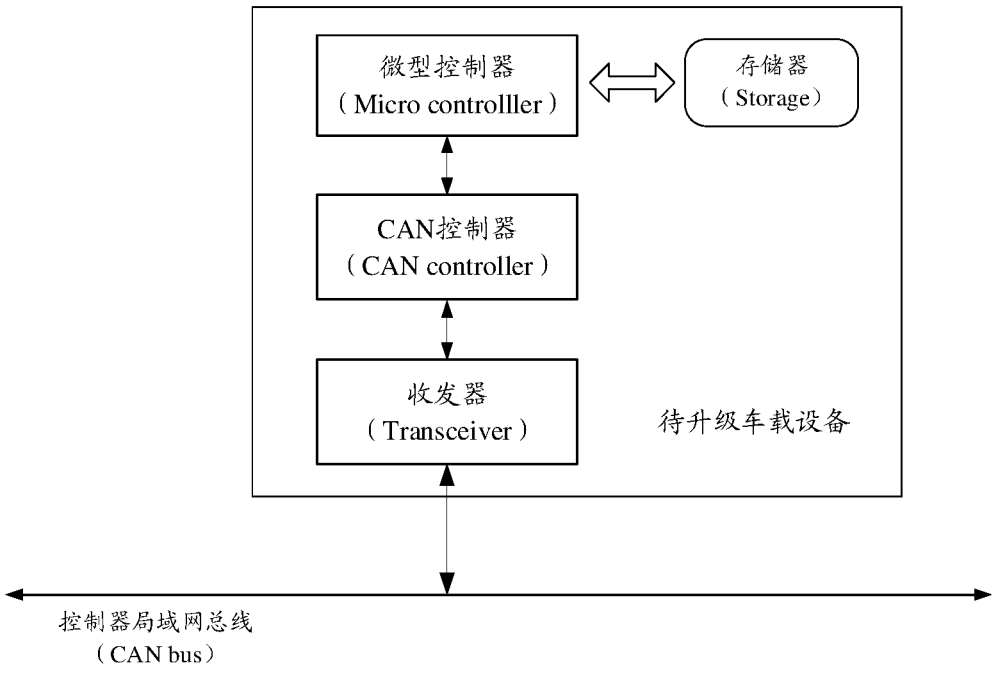

微型控制器
（Micro controlller）
存储器
（Storage）
CAN控制器
（CAN controller）
收发器
（Transceiver）
待升级车载设备
控制器局域网总线
（CAN bus）

图6

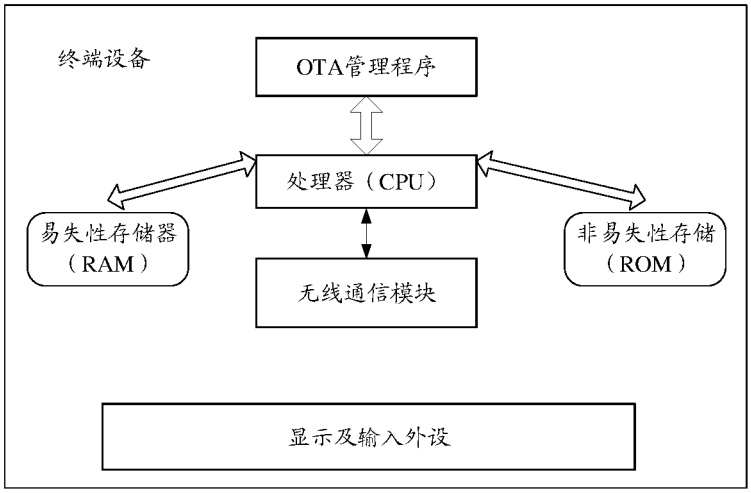

终端设备
OTA管理程序
处理器（CPU）
易失性存储器
（RAM）
非易失性存储
（ROM）
无线通信模块
显示及输入外设

图7

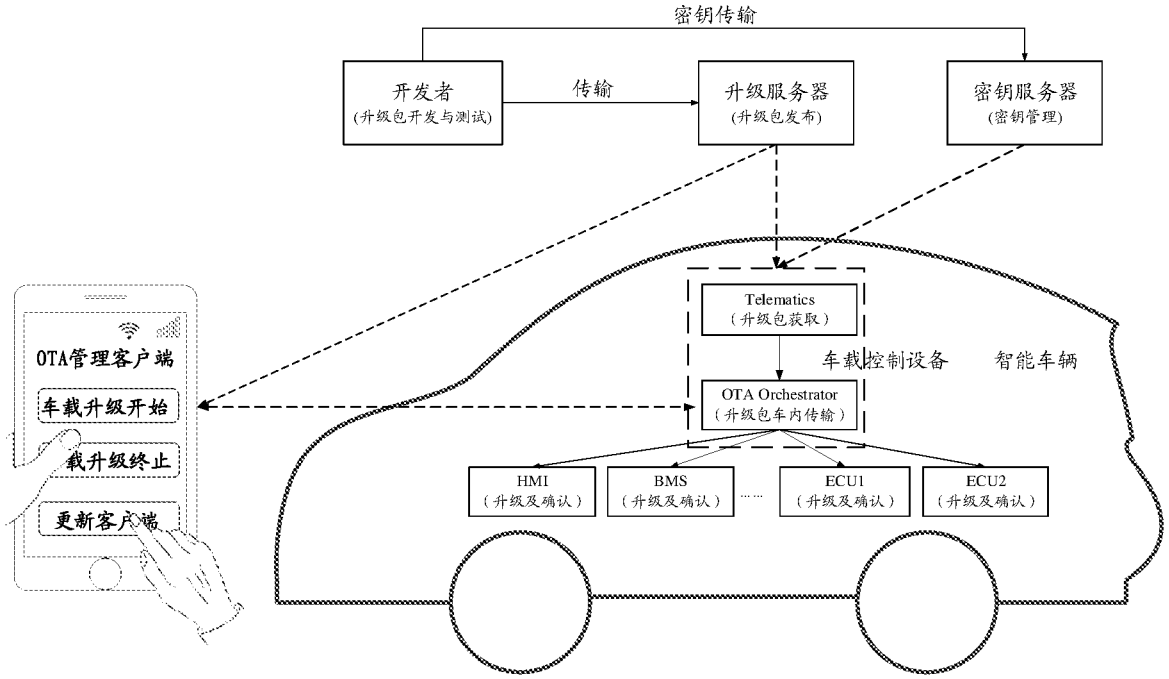

密钥传输
开发者
(升级包开发与测试)
传输
升级服务器
(升级包发布)
密钥服务器
(密钥管理)
OTA管理客户端
车载升级开始
载升级终止
更新客户端
Telematics
（升级包获取）
车载控制设备
智能车辆
OTA Orchestrator
（升级包车内传输）
HMI
（升级及确认）
BMS
（升级及确认）
ECU1
（升级及确认）
ECU2
（升级及确认）

图8

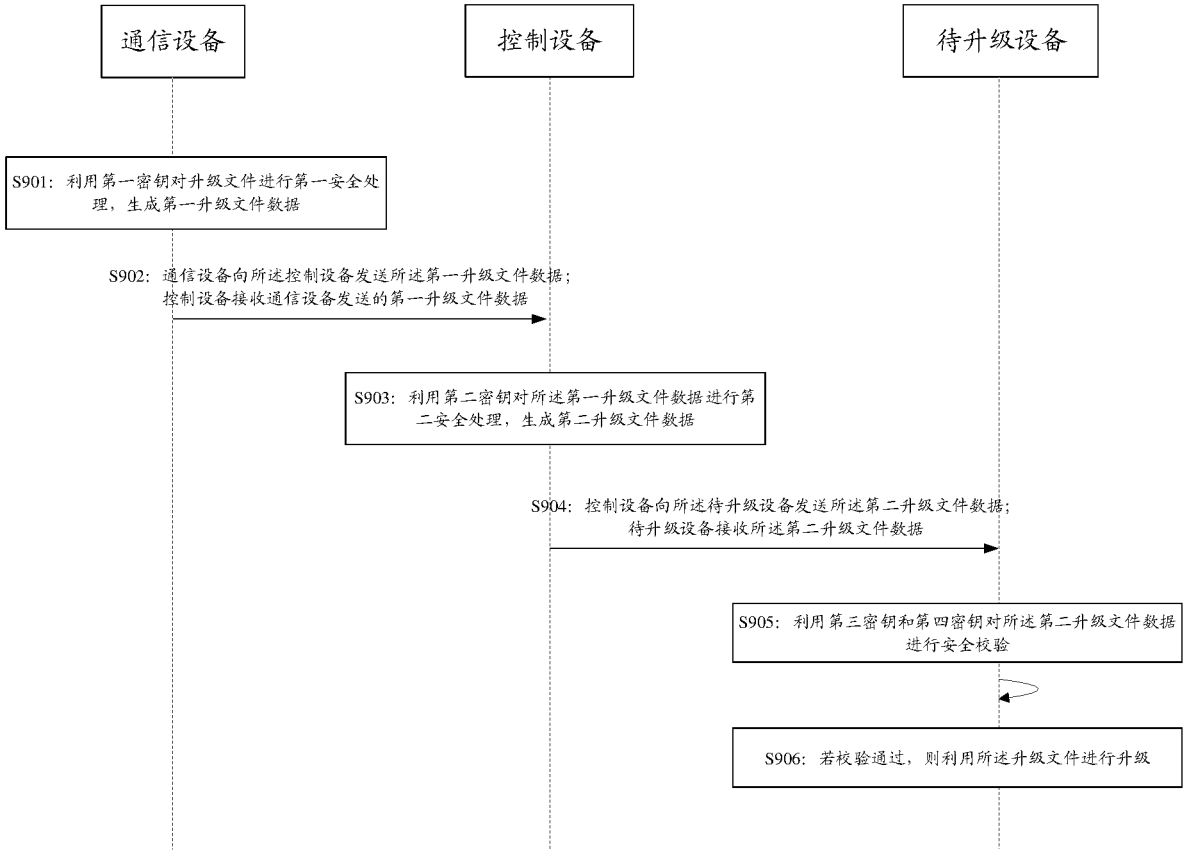

通信设备
控制设备
待升级设备
S901：利用第一密钥对升级文件进行第一安全处理，生成第一升级文件数据
S902：通信设备向所述控制设备发送所述第一升级文件数据；
控制设备接收通信设备发送的第一升级文件数据
S903：利用第二密钥对所述第一升级文件数据进行第二安全处理，生成第二升级文件数据
S904：控制设备向所述待升级设备发送所述第二升级文件数据；
待升级设备接收所述第二升级文件数据
S905：利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验
S906：若校验通过，则利用所述升级文件进行升级

图9

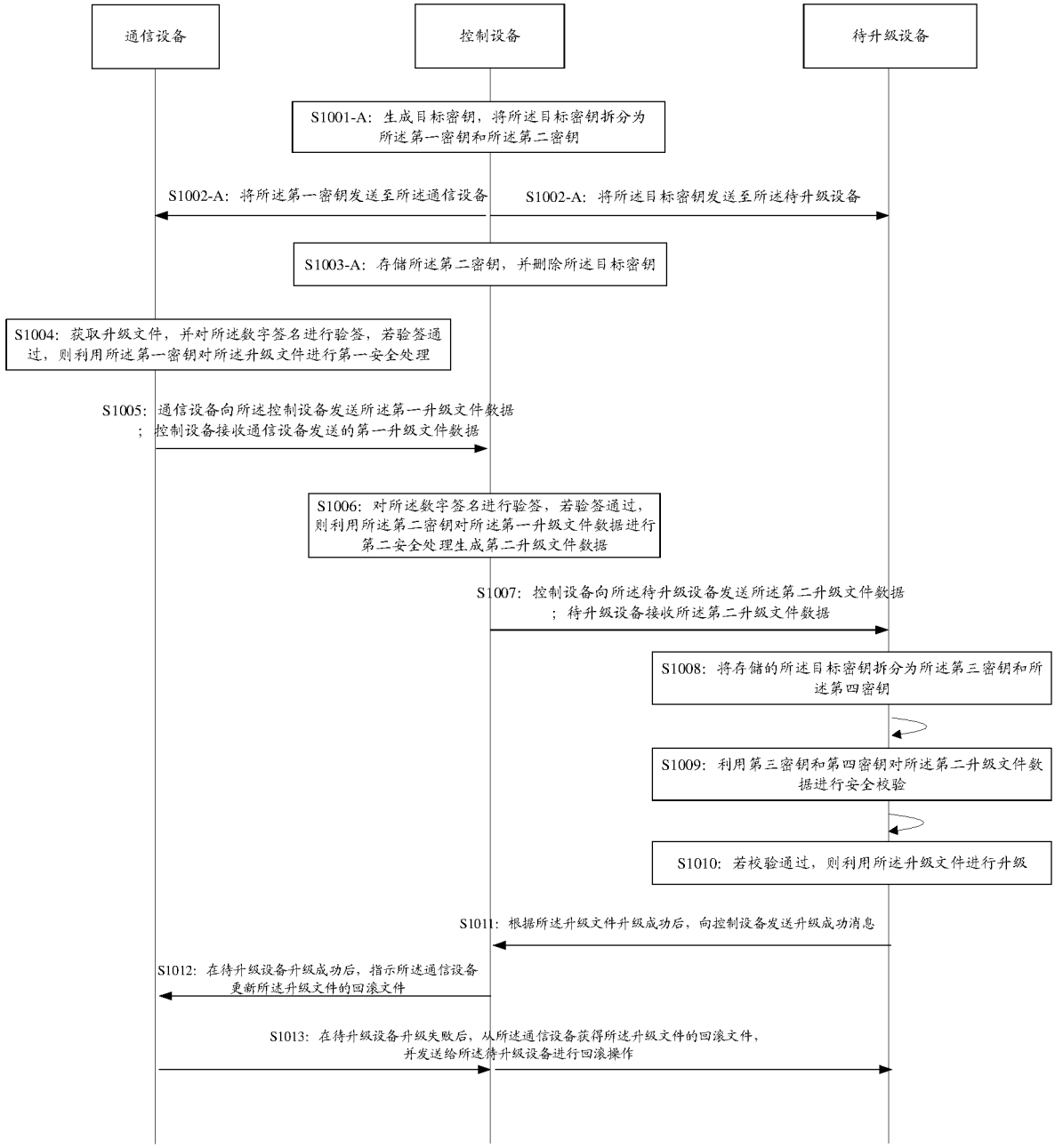

通信设备
控制设备
待升级设备
S1001-A：生成目标密钥，将所述目标密钥拆分为所述第一密钥和所述第二密钥
S1002-A：将所述第一密钥发送至所述通信设备
S1002-A：将所述目标密钥发送至所述待升级设备
S1003-A：存储所述第二密钥，并删除所述目标密钥
S1004：获取升级文件，并对所述数字签名进行验签，若验签通过，则利用所述第一密钥对所述升级文件进行第一安全处理
S1005：通信设备向所述控制设备发送所述第一升级文件数据；控制设备接收通信设备发送的第一升级文件数据
S1006：对所述数字签名进行验签，若验签通过，则利用所述第二密钥对所述第一升级文件数据进行第二安全处理生成第二升级文件数据
S1007：控制设备向所述待升级设备发送所述第二升级文件数据；待升级设备接收所述第二升级文件数据
S1008：将存储的所述目标密钥拆分为所述第三密钥和所述第四密钥
S1009：利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验
S1010：若校验通过，则利用所述升级文件进行升级
S1011：根据所述升级文件升级成功后，向控制设备发送升级成功消息
S1012：在待升级设备升级成功后，指示所述通信设备更新所述升级文件的回滚文件
S1013：在待升级设备升级失败后，从所述通信设备获得所述升级文件的回滚文件，并发送给所述待升级设备进行回滚操作

图10

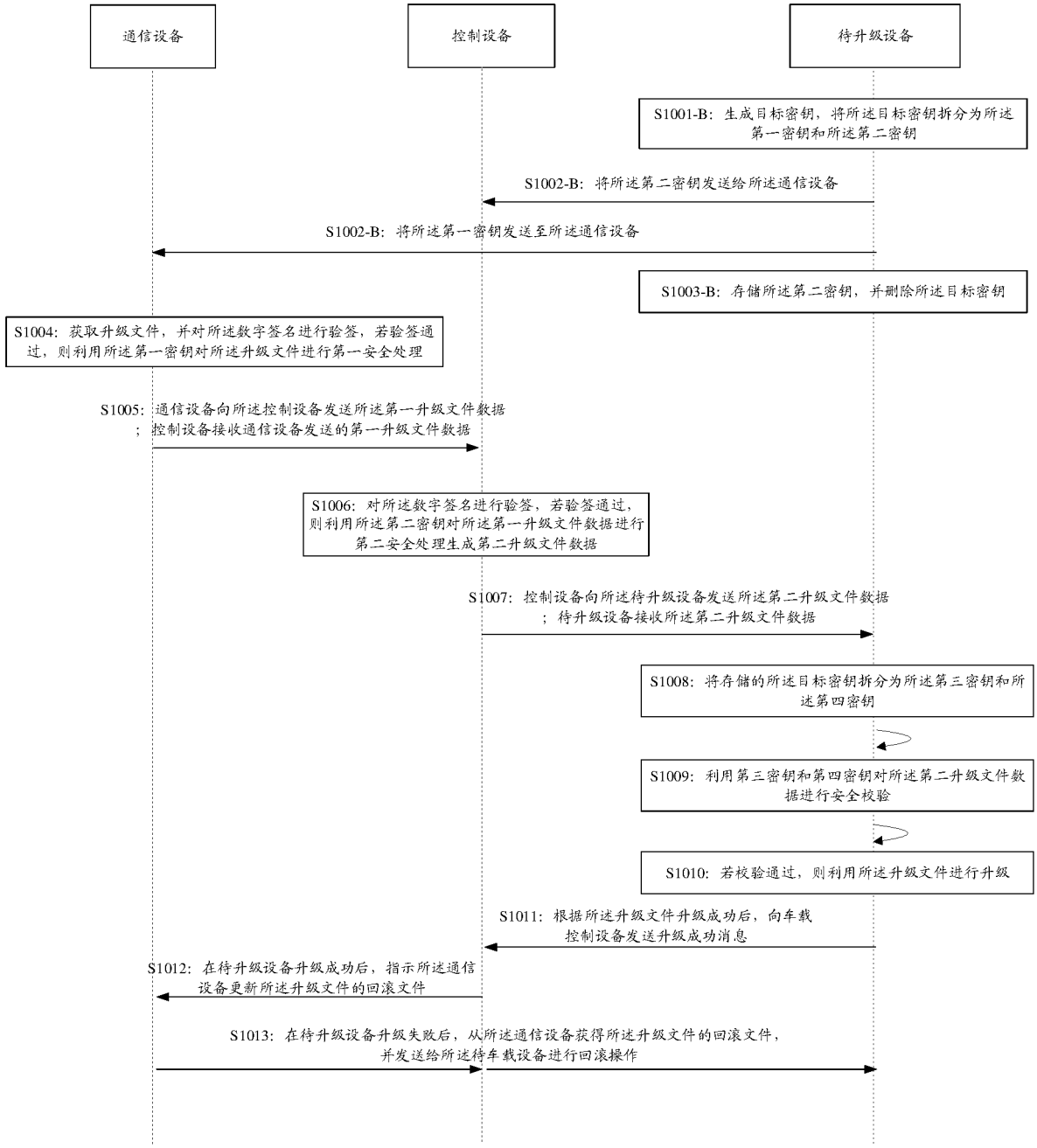

通信设备
控制设备
待升级设备
S1001-B：生成目标密钥，将所述目标密钥拆分为所述第一密钥和所述第二密钥
S1002-B：将所述第二密钥发送给所述通信设备
S1002-B：将所述第一密钥发送至所述通信设备
S1003-B：存储所述第二密钥，并删除所述目标密钥
S1004：获取升级文件，并对所述数字签名进行验签，若验签通过，则利用所述第一密钥对所述升级文件进行第一安全处理
S1005：通信设备向所述控制设备发送所述第一升级文件数据；控制设备接收通信设备发送的第一升级文件数据
S1006：对所述数字签名进行验签，若验签通过，则利用所述第二密钥对所述第一升级文件数据进行第二安全处理生成第二升级文件数据
S1007：控制设备向所述待升级设备发送所述第二升级文件数据；待升级设备接收所述第二升级文件数据
S1008：将存储的所述目标密钥拆分为所述第三密钥和所述第四密钥
S1009：利用第三密钥和第四密钥对所述第二升级文件数据进行安全校验
S1010：若校验通过，则利用所述升级文件进行升级
S1011：根据所述升级文件升级成功后，向车载控制设备发送升级成功消息
S1012：在待升级设备升级成功后，指示所述通信设备更新所述升级文件的回滚文件
S1013：在待升级设备升级失败后，从所述通信设备获得所述升级文件的回滚文件，并发送给所述待车载设备进行回滚操作

图11

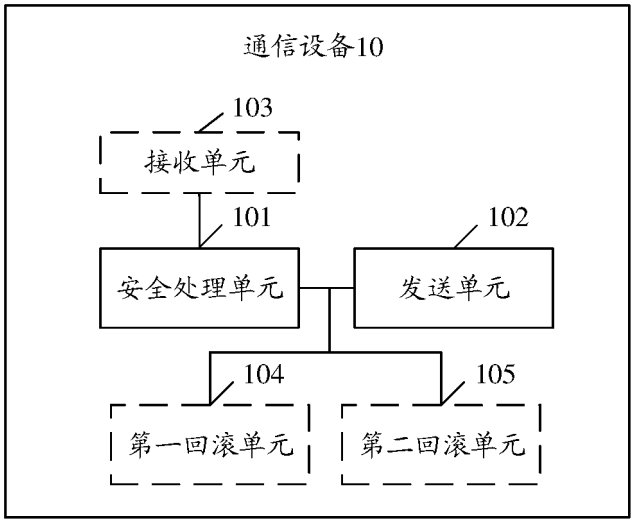

通信设备10
103
接收单元
101
102
安全处理单元
发送单元
104
105
第一回滚单元
第二回滚单元

图12

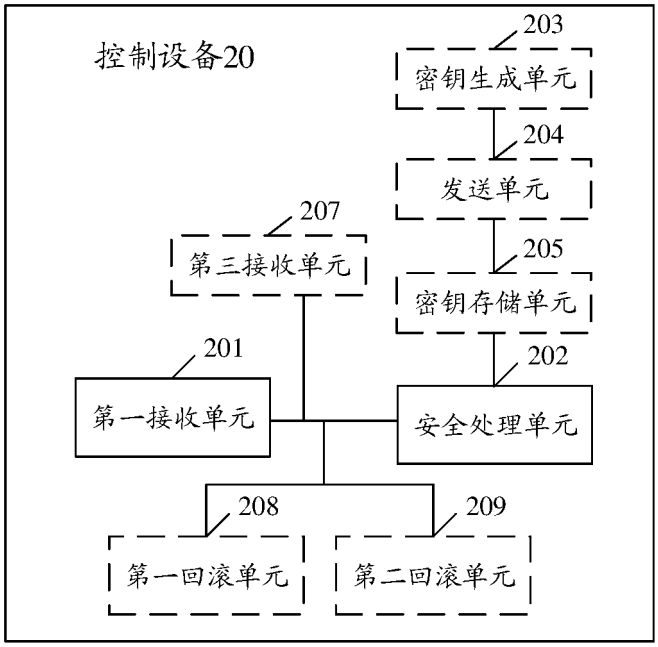

控制设备20
203
密钥生成单元
204
发送单元
207
205
第三接收单元
密钥存储单元
201
202
第一接收单元
安全处理单元
208
209
第一回滚单元
第二回滚单元

图13

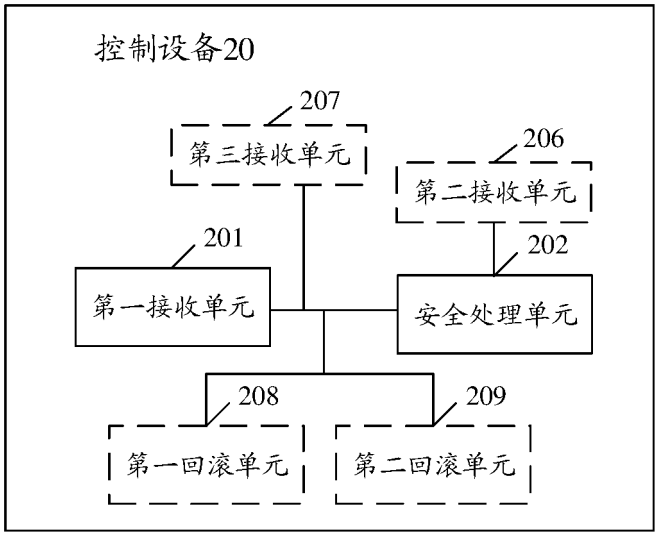

控制设备20
207
第三接收单元
206
第二接收单元
201
第一接收单元
202
安全处理单元
208
第一回滚单元
209
第二回滚单元

图14

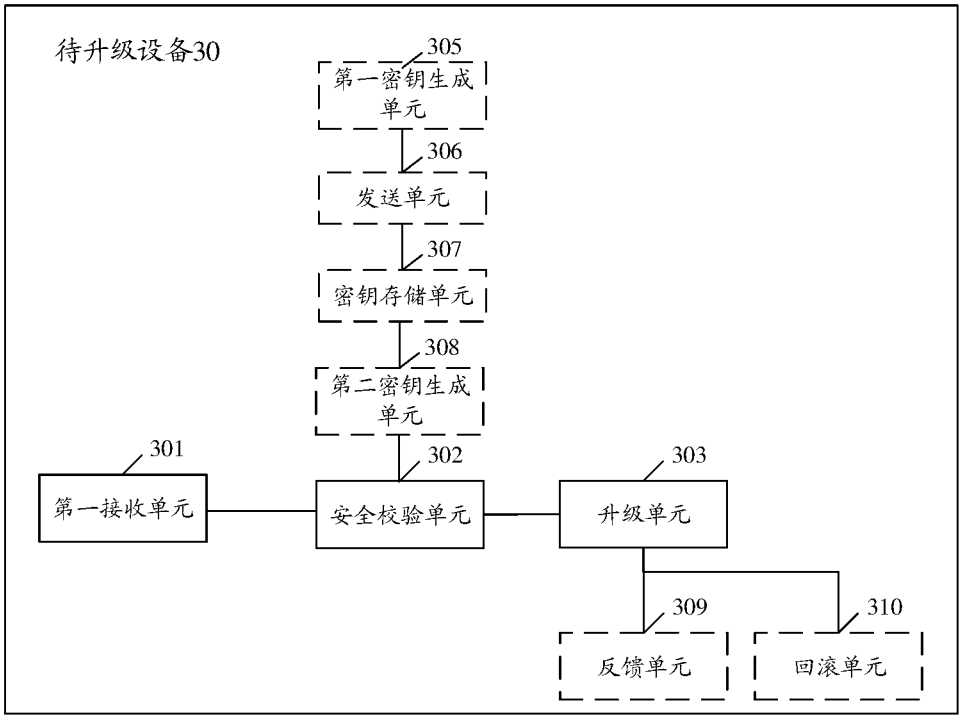

待升级设备30
305
第一密钥生成单元
306
发送单元
307
密钥存储单元
308
第二密钥生成单元
301
第一接收单元
302
安全校验单元
303
升级单元
309
反馈单元
310
回滚单元

图15

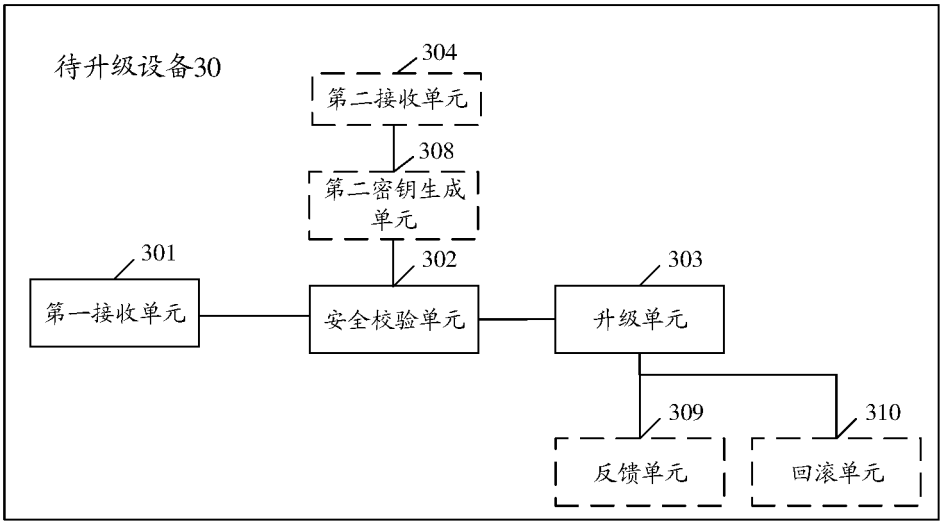

待升级设备30
304
第二接收单元
308
第二密钥生成单元
301
第一接收单元
302
安全校验单元
303
升级单元
309
反馈单元
310
回滚单元

图16

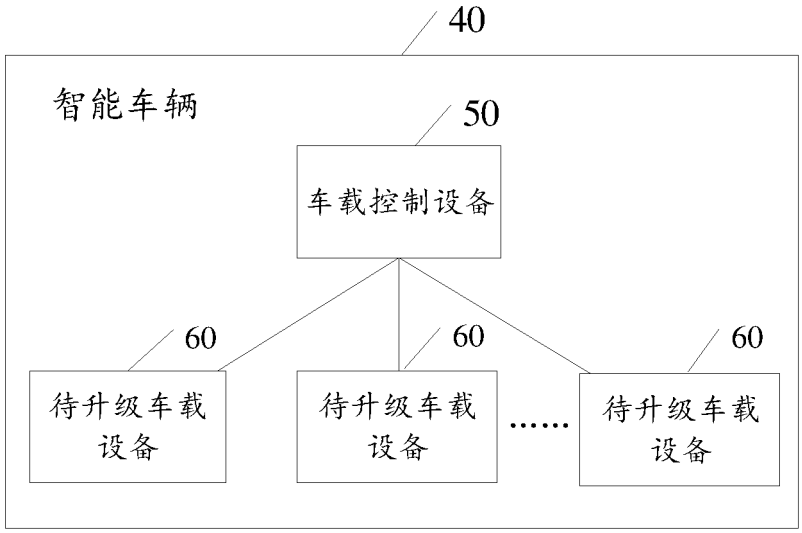

40
智能车辆
50
车载控制设备
60
待升级车载设备
60
待升级车载设备
.....
60
待升级车载设备

图17

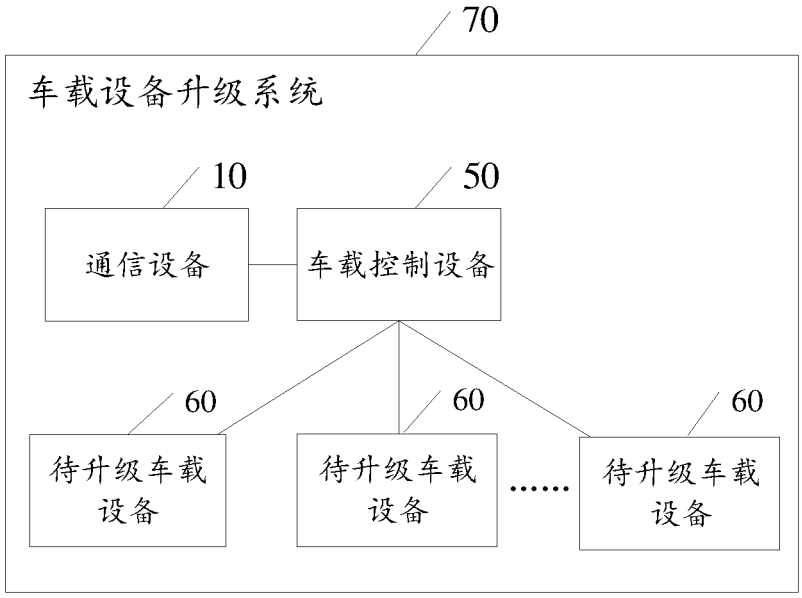

70
车载设备升级系统
10
50
通信设备
车载控制设备
60
60
60
待升级车载设备
待升级车载设备
.....
待升级车载设备

图18

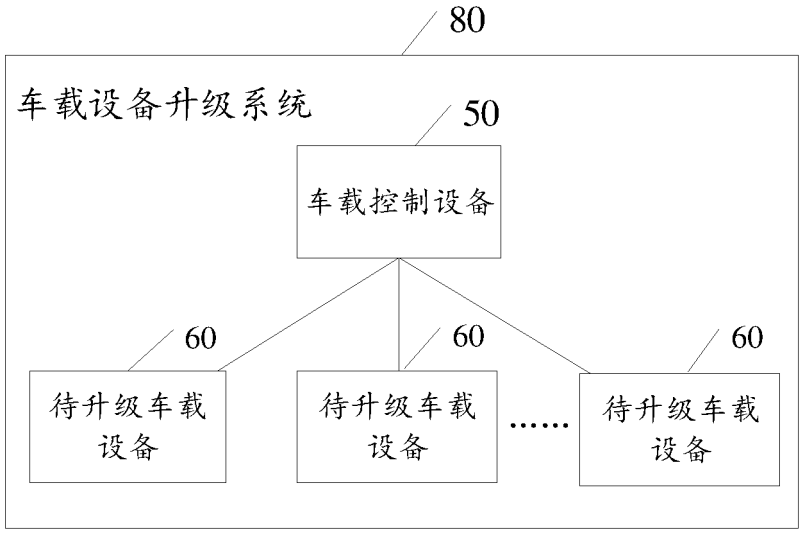

80
车载设备升级系统
50
车载控制设备
60
60
60
待升级车载设备
待升级车载设备
.....
待升级车载设备

图19

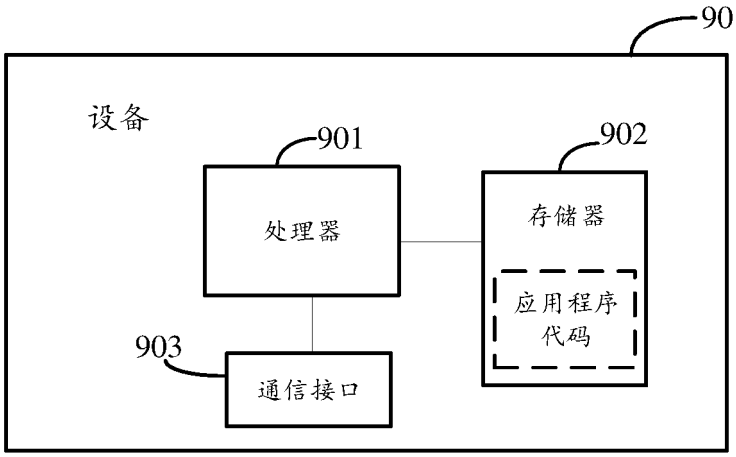


图20