

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2022 年 7 月 7 日 (07.07.2022)



(10) 国际公布号
WO 2022/140903 A1

- (51) 国际专利分类号:
H04L 9/08 (2006.01) **G06F 8/65** (2018.01)
- (21) 国际申请号: PCT/CN2020/140094
- (22) 国际申请日: 2020 年 12 月 28 日 (28.12.2020)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (71) 申请人: 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。
- (72) 发明人: 王勇 (WANG, Yong); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。
- (74) 代理人: 广州三环专利商标代理有限公司 (SCIHEAD IP LAW FIRM); 中国广东省广州市

越秀区先烈中路 80 号汇华商贸大厦 1508 室, Guangdong 510070 (CN)。

- (81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。
- (84) 指定国(除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT,

(54) Title: OTA UPDATE METHOD AND APPARATUS

(54) 发明名称: 一种OTA升级方法及装置

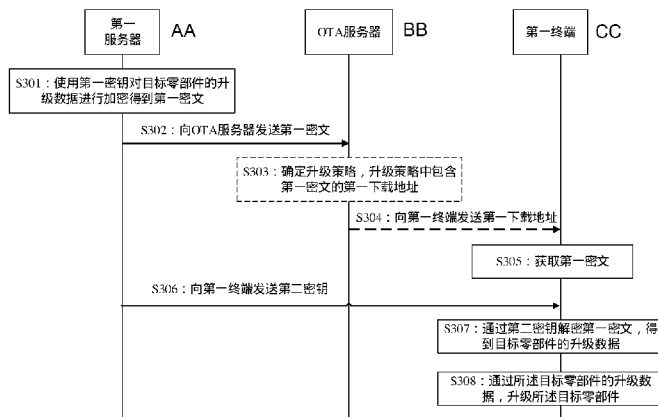


图 3

- S301 Encrypt update data of a target part by using a first key, so as to obtain a first ciphertext
- S302 Send the first ciphertext to an OTA server
- S303 Determine an update policy, the update policy containing a first download address of the first ciphertext
- S304 Send the first download address to a first terminal
- S305 Acquire the first ciphertext
- S306 Send a second key to the first terminal
- S307 Decrypt the first ciphertext by means of the second key, so as to obtain update data of the target part
- S308 Update the target part by using the update data of the target part
- AA First server
- BB OTA server
- CC First terminal

(57) Abstract: The embodiments of the present application provide an OTA update method and apparatus, which are applied to the fields of communication technology and Internet of Vehicles. Said method comprises: a first server encrypting update data of a target part according to a first key, so as to obtain a first ciphertext, the first server being a server for providing update data of the target part; the first server sending the first ciphertext to an OTA server; and the first server sending a second key to a first terminal deployed with the target part, the second key being a decryption key corresponding to the first key. The embodiments of the present application can protect core assets such as secret-related data and key codes in the update data, improving the security of OTA update. The present solution can further be used for improving the capability of autonomous driving or advanced driver assistance systems (ADAS), and can be specifically applied to the fields of vehicle-to-everything (V2X), Long Term Evolution-vehicle (LTE-V) and vehicle-to-vehicle (V2V).

RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布：

— 包括国际检索报告(条约第21条(3))。

(57) 摘要：本申请实施例提供一种OTA升级方法及装置，应用于通信技术、车联网领域，该方法包括：第一服务器根据第一密钥对目标零部件的升级数据进行加密得到第一密文，其中，第一服务器为用于提供目标零部件的升级数据的服务器；第一服务器向OTA服务器发送第一密文；第一服务器向部署有目标零部件的第一终端发送第二密钥，该第二密钥为第一密钥对应的解密密钥。本申请实施例可以保护升级数据中的涉密数据、关键代码等核心资产，提高OTA升级的安全性。该方案进一步可用于提升自动驾驶或高级驾驶辅助系统ADAS能力，具体可以应用于车联网V2X、车路通信长期演进技术LTE-V、车辆-车辆V2V等领域。

一种 OTA 升级方法及装置

技术领域

本申请涉及车联网、通信技术领域，尤其涉及一种 OTA 升级方法及装置。

背景技术

随着计算机技术、网络技术等不断发展，终端的数量越来越多，人们对于终端的智能化要求、安全要求等也越来越高，终端越来越智能化和多媒体化。当前的终端中往往部署了各种各样的硬件、软件（应用），例如，车辆中配置有智能座舱、传感系统、自动驾驶系统，也安装有车载操作系统、导航应用、影音播放应用等等。这些硬件、软件虽然使得终端的功能更加丰富，但是也更容易出现漏洞、或者需要替换为更先进的版本等等。因此，需要对终端的硬件、软件（应用）进行升级更新。

空中下载技术(Over the Air, OTA)是一种通过无线网络进行数据下载的技术，现已被广泛应用于车辆、电视、手机、平板电脑、机顶盒等设备的升级。OTA 技术主要通过下载 OTA 升级包进行自动升级（也支持通过拷贝 OTA 升级包到 SD 卡来升级），OTA 升级速度快、对数据的影响小，因此 OTA 升级成为了终端功能升级的主要方式。例如，对于车辆来说，车辆厂商（Original Equipment Manufacturer, OEM，或者称为原始设备制造商）通过 OTA 技术升级车辆的相关硬件或软件，有利于厂商减少召回成本、快速响应需求、提升用户体验。

现有的 OTA 升级的模式是由 OEM 进行主导，OEM 负责审核升级包的软件版本、分发升级包。但是随着智能网联汽车发展，部分敏感部件、特殊应用等需要升级时，若将升级包交给 OEM 审核后通过 OTA 服务器下载，则可能使得零件供应商的核心技术被泄露或者涉及数据遭到曝光。

因此，如何在 OTA 升级时保护升级数据中的机密性，成为了本领域技术人员亟待解决的技术问题。

发明内容

本申请实施例公开了一种 OTA 升级方法及装置，可以保护升级数据中的涉密数据、关键代码等核心资产，提高了 OTA 升级的安全性。

第一方面，本申请实施例公开了一种 OTA 升级方法，包括：

第一服务器根据第一密钥对目标零部件的升级数据进行加密得到第一密文，其中，所述第一服务器为用于提供所述目标零部件的升级数据的服务器；

所述第一服务器向 OTA 服务器发送所述第一密文；

所述第一服务器向部署有所述目标零部件的第一终端发送第二密钥，所述第二密钥为所述第一密钥对应的解密密钥。

其中，第一服务器为用于提供目标零部件的升级数据的服务器，可以是一个单独的服务器，也可以是多个服务器组成的服务器集群。目标零部件是一个待升级部件。所述第一

密钥与所述第二密钥可以是相同的密钥（例如，第一密钥和所述第二密钥为对称密钥），也可以是不同的密钥（例如第一密钥为公钥，第二密钥为私钥）。

可以看出，第一服务器提供目标零部件的升级数据时，可以将升级数据进行加密得到第一密文，第一终端可以通过 OTA 服务器获取第一密文。后续第一服务器可以将第二密钥发送给第一终端，以便于第一终端解密第一密文后进行升级。由于目标零部件的升级数据是经过加密传输的，只有第一服务器、第一终端可以通过第二密钥得到升级数据，避免了其他中间设备获取升级数据，提高了升级数据的机密性。当升级数据中包含核心代码、关键技术实现的情况下，可以有效保护涉密数据、关键代码等核心资产。

进一步的，由于升级数据是经过加密的，可以避免攻击者篡改升级数据，提高了 OTA 升级的安全性。

结合第一方面，在第一方面的一种可能的实施方式中，上述第一服务器属于目标零部件的供应商用于维护目标零部件的服务器。

结合第一方面，在第一方面的又一种可能的实施方式中，所述第一服务器向部署有所述目标零部件的第一终端发送第二密钥，包括：

所述第一服务器与部署有所述目标零部件的所述第一终端建立安全通道；

所述第一服务器通过所述安全通道向所述第一终端发送所述第二密钥。

其中，安全通道可以是基于安全套接字协议 (Secure Sockets Layer, SSL) 或者传输层安全 (Transport Layer Security, TLS) 的传输通道，用于数据安全传输。由于安全通道是安全可信的信道，第一服务器与第一终端通过安全通道传输第二密钥，可以保证第二密钥的安全性。

可选的，第一服务器具体可以与第一终端中的目标零部件建立安全通道，向第一终端中的目标零部件发送第二密钥。可替换的，第一服务器具体可以与第一终端中的升级控制部件建立安全通道，向第一终端中的升级控制部件发送第二密钥。

结合第一方面，在第一方面的又一种可能的实施方式中，所述第一服务器向部署有所述目标零部件的第一终端发送第二密钥，包括：

所述第一服务器根据第一安全参数加密所述第二密钥得到第二密文，所述第一安全参数为所述第一服务器与所述第一终端之间的共享密钥或者为所述第一终端的第一公钥；

所述第一服务器向部署有所述目标零部件的所述第一终端发送所述第二密文。

其中，第一安全参数可以是公钥、或者对称密钥或者第一服务器与第一终端（或者具体为第一终端中的目标零部件或者第一终端中的升级控制部件等）协商得到的共享密钥。例如，第一终端（具体还可以为第一终端中的目标零部件或者第一终端中的升级控制部件等）可以确定一个私钥对，该公私钥对包含第一公钥和第一私钥，该第一公钥可以发送给第一服务器作为第一安全参数，而第一私钥作为第二安全参数用于第一终端解密第二密文得到第二密钥。

可选的，第一服务器具体可以向第一终端中的目标零部件发送所述第二密文。可替换的，第一服务器具体可以向第一终端中的升级控制部件发送所述第二密文。

可以看出，通过安全参数将第二密钥加密后进行传输，可以提高第二密文的机密性，从而提高升级数据的机密性。

结合第一方面，在第一方面的又一种可能的实施方式中，所述第一服务器根据第一安全参数加密所述第二密钥得到第二密文之前，所述方法还包括：

所述第一服务器接收来自所述第一终端的密钥获取请求。

结合第一方面，在第一方面的又一种可能的实施方式中，所述第一安全参数属于临时密钥或者属于一次性密钥。

其中，一次性密钥可以理解为只使用一次或者使用一次后即失效或被删除的密钥。例如，第一服务器使用第一安全参数加密第二密钥后，则将第一安全参数删除；第一终端使用第二安全参数解密第二密文后，可以将该第二安全参数删除。这样一来，只使用一次第一安全参数进行加密以及只使用一次第二安全参数进行解密，从而使得该第一安全参数和第二安全参数不容易被攻破，提高数据安全性。

结合第一方面，在第一方面的又一种可能的实施方式中，所述第一安全参数为所述第一终端的第一公钥；所述第一服务器根据第一安全参数加密所述第二密钥得到第二密文之前，还包括：

所述第一服务器接收所述第一终端发送的所述第一终端的第一公钥；

所述第一服务器通过所述第一终端的第一数字证书认证所述第一终端的第一公钥。

结合第一方面，在第一方面的又一种可能的实施方式中，所述第一数字证书对应第二公钥和第二私钥；所述第一服务器通过所述第一终端的第一数字证书认证所述第一终端的第一公钥，包括：

所述第一服务器接收来自所述第一终端发送的第一签名，所述第一签名为使用所述第二私钥对所述第一公钥签名得到的；

所述第一服务器根据所述第二公钥、所述第一签名和所述第一公钥确定所述第一公钥认证通过。

结合第一方面，在第一方面的又一种可能的实施方式中，所述第一安全参数为所述第一服务器与所述第一终端之间的共享密钥；所述第一服务器根据第一安全参数加密所述第二密钥得到第二密文之前，还包括：

所述第一服务器通过密钥协商算法，与所述第一终端协商得到所述共享密钥；

所述第一服务器通过所述第一服务器和所述第一终端之间的预共享密钥 PSK 认证所述第一终端的身份，所述 PSK 为所述第一服务器与所述目标零部件之间预设的秘密值。

可以看出，该第一安全参数（以及后续用于解密第二密文的第二安全参数）可以是第一服务器与第一终端通过密钥协商算法确定的。这样一来，不同的终端与第一服务器可以协商得到不同的安全参数，从而使得该第一安全参数和第二安全参数不容易被攻破，提高数据安全性。

结合第一方面，在第一方面的又一种可能的实施方式中，所述第一服务器通过所述第一服务器和所述第一终端之间的预共享密钥 PSK 认证所述第一终端的身份，包括：

所述第一终端接收所述第一终端发送的第一消息，所述第一信息包含第一随机数；

所述第一服务器向所述第一终端发送第二消息，所述第二信息包含第一认证参数和第二随机数；所述第一认证参数为根据所述第一消息、所述第二随机数和所述 PSK 得到的；

所述第一服务器接收所述第一终端发送的第三消息，所述第三信息包含第二认证参数；

所述第一服务器根据所述第二消息、所述第一随机数和所述 PSK 确定所述目标零部件的身份认证通过。

结合第一方面，在第一方面的又一种可能的实施方式中，所述第一服务器向部署有所述目标零部件的第一终端发送第二密钥，包括：

所述第一服务器向所述第一终端的升级控制部件发送所述第二密钥；

或者，所述第一服务器向所述第一终端的所述目标零部件发送所述第二密钥。

第二方面，本申请实施例公开了一种 OTA 升级方法，包括：

第一终端接收 OTA 服务器发送的第一密文，所述第一密文为第一服务器根据第一密钥对所述第一终端上的目标零部件的升级数据加密得到的，所述第一服务器为用于提供所述目标零部件的升级数据的服务器；

所述第一终端接收来自所述第一服务器的第二密钥，所述第二密钥为所述第一密钥对应的解密密钥；

所述第一终端通过所述第二密钥解密所述第一密文，得到所述目标零部件的升级数据；

所述第一终端通过所述目标零部件的升级数据，升级所述目标零部件。

结合第二方面，在第二方面的又一种可能的实施方式中，所述第一终端接收来自所述第一服务器的第二密钥，包括：

所述第一终端与所述第一服务器建立安全通道；

所述第一终端通过所述安全通道接收所述第一服务器的所述第二密钥。

结合第二方面，在第二方面的又一种可能的实施方式中，所述第一终端接收来自所述第一服务器发送的第二密钥，包括：

所述第一终端接收来自所述第一服务器的第二密文；所述第二密文为根据第一安全参数加密第二密钥得到的；

所述第一终端根据第二安全参数解密所述第二密文，得到所述第二密钥，所述第二安全参数为所述第一服务器与所述第一终端之间的共享密钥或者为所述第一终端的第一私钥。

结合第二方面，在第二方面的又一种可能的实施方式中，所述第一终端接收来自所述第一服务器的第二密钥之前，所述方法还包括：

所述第一终端向所述第一服务器发送密钥获取请求。

结合第二方面，在第二方面的又一种可能的实施方式中，所述第二安全参数属于临时密钥或者属于一次性密钥。

结合第二方面，在第二方面的又一种可能的实施方式中，所述第二安全参数为所述第一公钥对应的第一私钥，所述第一安全参数为所述目标零部件的第一公钥；

所述第一公钥通过所述目标零部件的第一数字证书进行认证。

结合第二方面，在第二方面的又一种可能的实施方式中，所述第一数字证书对应第二公钥和第二私钥；所述第一终端接收来自所述第一服务器的第二密文之前，还包括：

所述第一终端确定所述第一公钥和所述第一私钥；

所述第一终端通过所述第二私钥对所述第一公钥进行签名，得到第一签名，

所述第一终端向所述第一服务器发送第一签名和所述第一公钥；所述第一签名用于所

述第一服务器根据所述第一签名证书对应的第二公钥认证所述第一公钥。

结合第二方面，在第二方面的又一种可能的实施方式中，所述第一安全参数为所述第一服务器与所述第一终端之间的共享密钥；所述第一终端根据第二安全参数解密所述第二密文，得到所述第二密钥之前，还包括：

所述第一终端通过密钥协商算法，与所述第一服务器协商得到所述共享密钥；

所述第一终端通过所述第一服务器和所述第一终端之间的预共享密钥 PSK 认证所述第一服务器的身份，所述 PSK 为所述第一服务器与所述第一终端之间预设的秘密值。

结合第二方面，在第二方面的又一种可能的实施方式中，所述第一终端通过所述第一服务器和所述第一终端之间的预共享密钥 PSK 认证所述第一服务器的身份，包括：

所述第一终端向所述第一服务器发送第一消息，所述第一消息包含第一随机数；

所述第一终端接收所述第一服务器发送的第二消息，所述第二消息包含第一认证参数和第二随机数；

所述第一终端根据所述第一认证参数、所述第一消息、所述第二随机数和所述 PSK 确定所述第一服务器的身份认证通过；

所述第一终端向所述第一服务器发送第三消息，所述第三消息包含第二认证参数；所述第二认证参数为根据所述第一随机数、所述第二消息和所述 PSK 得到的。所述第二认证参数用于认证所述第一终端的身份。

结合第二方面，在第二方面的又一种可能的实施方式中，所述 OTA 升级方法具体应用于所述第一终端中的所述目标零部件；

或者，所述第一终端中还包括升级控制部件，所述 OTA 升级方法具体应用于所述升级控制部件。

需要说明的是，本申请第二方面的技术方案与第一方面的方案可能存在对应，相关的有益效果可以参考第一方面的有益效果，此处不再赘述。

第三方面，本申请实施例公开了一种 OTA 升级方法，包括：

OTA 服务器接收来自第一服务器的第一密文，所述第一密文为第一服务器根据第一密钥对所述第一终端上的目标零部件的升级数据加密得到的，所述第一服务器为用于提供所述目标零部件的升级数据的服务器；

所述 OTA 服务器向所述第一终端发送升级策略，所述升级策略包含所述第一密文的第一下载地址。

结合第三方面，在第三方面的一种可能的实施方式中，所述方法还包括：

所述 OTA 服务器通过所述安全通道向所述第一终端发送所述第一密文，所述安全通道为所述第一终端基于所述第一下载地址与所述 OTA 服务器共同建立的。

结合第三方面，在第三方面的又一种可能的实施方式中，所述升级策略中包括升级规则、升级条件、下载规则等等中的一项或者多项。

其中，升级规则用于定义升级的次序、是否需要进行回滚等规则，升级条件可以包含是否供电正常、存储空间、网络状态、有依赖关系的其他设备的状态等，下载规则用于定义下载的顺序、指示哪一个部件进行下载等等。

结合第三方面，在第三方面的又一种可能的实施方式中，所述方法还包括：

所述 OTA 服务器根据所述第一终端的信息和/或所述第一密文的信息，确定所述升级策略。

例如，OTA 服务器根据第一终端的信息和第一密文的文件大小，确定所述第一终端需要的存储空间大小。

第四方面，本申请实施例公开了一种 OTA 升级方法，包括：

第一服务器向 OTA 服务器发送目标零部件的升级数据的元数据，其中，所述第一服务器为用于提供所述目标零部件的升级数据的服务器，所述升级数据的元数据包含所述升级数据的第一下载地址和所述升级数据的版本信息；

所述第一服务器通过安全通道向部署有所述目标零部件的第一终端发送所述目标零部件的升级数据，所述安全通道为所述第一终端根据所述第一下载地址与所述第一服务器共同建立的。

可以看出，第一服务器向 OTA 服务器发送升级数据的元数据，OTA 服务器向第一终端发送升级数据的第一下载地址。第一终端通过第一下载地址从第一服务器下载升级数据，避免了其他中间设备（例如 OTA 服务器）获取目标零部件的升级数据，保证了升级数据的机密性。当升级数据中包含核心代码、关键技术实现的情况下，可以有效保护涉密数据、关键代码等核心资产。

进一步的，由于目标零部件的升级数据是在第一服务器直接获取的，因此避免了中间设备等转存、或者审核等操作，减少了升级流程的复杂度，提高了升级效率。通过本申请实施例还可以满足某些需要快速升级的零部件的需求。

结合第四方面，在第四方面的一种可能的实施方式中，所述第一服务器属于所述目标零部件的供应商用于维护所述目标零部件的服务器。

结合第四方面，在第四方面的又一种可能的实施方式中，所述第一服务器通过安全通道向部署有所述目标零部件的第一终端发送所述目标零部件的升级数据，具体可以为：

所述第一服务器通过所述安全通道向所述第一终端中的所述目标零部件发送所述目标零部件的升级数据；

或者，所述第一服务器通过所述安全通道向所述第一终端中的升级控制部件发送所述目标零部件的升级数据。

第五方面，本申请实施例公开了一种 OTA 升级方法，包括：

第一终端接收 OTA 服务器发送的下载策略，所述下载策略中包含目标零部件的升级数据的第一下载地址；所述目标零部件部署在所述第一终端上；

所述第一终端基于所述第一下载地址，与第一服务器共同建立安全通道，所述第一服务器为用于提供所述目标零部件的升级数据的服务器；

所述第一终端通过所述安全通道接收所述第一服务器发送的所述目标零部件的升级数据；

所述第一终端根据所述目标零部件的升级数据升级所述目标零部件。

结合第五方面，在第五方面的一种可能的实施方式中，所述 OTA 升级方法具体应用于所述目标零部件。

结合第五方面，在第五方面的又一种可能的实施方式中，所述第一终端中还包括升级控制部件，所述 OTA 升级方法具体应用于所述升级控制部件。

第五方面的技术方案可能与第四方面的技术方案对应，相关的有益效果可以参考第四方面的有益效果，此处不再赘述。

第六方面，本申请实施例公开了一种 OTA 升级方法，包括：

OTA 服务器接收第一服务器发送的目标零部件的升级数据的元数据，其中，所述第一服务器为用于提供所述目标零部件的升级数据的服务器，所述升级数据的元数据包含所述升级数据的第一下载地址和所述升级数据的版本信息；

所述 OTA 服务器向所述第一终端发送升级策略，所述升级策略包含所述第一下载地址。

结合第六方面，在第六方面的又一种可能的实施方式中，所述方法还包括：

所述 OTA 服务器根据所述第一终端的信息和/或升级数据的元数据，确定所述升级策略。

结合第六方面，在第六方面的又一种可能的实施方式中，所述升级策略中包括升级规则、升级条件、下载规则等等中的一项或者多项。

结合第六方面，在第六方面的又一种可能的实施方式中，所述元数据中还包括所述目标零部件的升级数据的文件大小。

第七方面，本申请实施例公开了一种 OTA 升级方法，包括：

第一服务器根据第一密钥对目标零部件的升级数据进行加密得到第一密文，其中，所述第一服务器为用于提供所述目标零部件的升级数据的服务器；

所述第一服务器通过第一安全参数的加密第二密钥得到第二密文，其中，所述第一安全参数为所述第一服务器与所述第一终端之间的共享密钥或者为所述第一终端的第一公钥，所述第一终端为部署有第一目标零部件的终端，所述第一目标零部件为所述目标零部件中的一个，所述第二密钥为所述第一密钥的解密密钥；

所述第一服务器向 OTA 服务器发送所述第一密文和所述第二密文，所述第二密文用于所述第一终端解密所述第一密文。

可以看出，由于没有获取第二安全参数则无法解密第二密文得到第二密钥，从而无法解密第一密文得到目标零部件的升级数据，因此保证了目标零部件的升级数据的安全性。

进一步的，由于没有直接对目标零部件的升级数据进行加密，而是使用第一安全参数加密第二密钥，而密钥的数据大小通常小于升级数据的数据大小。因此，对于存在有多个、多种零部件需要升级的供应商来说，考虑多个零部件的安全参数可能不同的情况，相比于直接使用安全参数加密升级数据，本实施例可以显著减少加密过程中的计算量、存储量，提高升级的效率。

结合第七方面，在第七方面的一种可能的实施方式中，所述第一服务器属于所述目标零部件的供应商用于维护所述目标零部件的服务器。

第八方面，本申请实施例公开了一种 OTA 升级方法，包括：

OTA 服务器接收第一服务器发送的第一密文和第二密文，其中，所述第一密文为根据第一密钥对目标零部件的升级数据加密得到的，所述第二密文为根据第一安全参数对第二密钥加密得到的，所述第一安全参数为所述第一服务器与第一终端之间的共享密钥或者为所述第一终端的第一公钥，所述第一终端为部署有第一目标零部件的终端，所述第一目标零部件为所述目标零部件中的一个，所述第二密钥为所述第一密钥的解密密钥；

所述 OTA 服务器向所述第一终端发送所述第一密文和所述第二密文，其中所述第二密文用于所述第一终端解密所述第一密文，以得到所述目标零部件的升级数据。

结合第八方面，在第八方面的一种可能的实施方式中，所述 OTA 服务器向所述第一终端发送所述第一密文和所述第二密文，包括：

所述 OTA 服务器根据所述第一密文所在的升级包的属性和所述第一终端的信息生成升级策略；所述升级策略包括所述第一密文和所述第二密文的第一下载地址；

所述 OTA 服务器向所述第一终端发送所述升级策略；

所述 OTA 服务器通过安全通道向所述第一终端发送所述第一密文和所述第二密文，所述安全通道为所述第一终端根据所述第一下载地址与所述 OTA 服务器共同建立的。

第八方面的技术方案可能与第七方面的技术方案对应，相关的有益效果可以参考第七方面的有益效果，此处不再赘述。

第九方面，本申请实施例公开了一种 OTA 升级方法，应用于部署有第一目标零部件的第一终端，所述第一目标零部件为目标零部件中的一个，所述方法包括：

所述第一终端接收 OTA 服务器发送的第一密文和第二密文，所述第一密文为第一服务器根据第一密钥对所述目标零部件的升级数据加密得到的，其中，所述第一服务器为用于提供所述目标零部件的升级数据的服务器；

所述第一终端根据第二安全参数解密所述第二密文得到第二密钥，所述第二密钥为所述第一密钥的解密密钥，所述第二安全参数为所述第一服务器与所述第一终端之间的共享密钥或者为所述第一终端的第一私钥；

所述第一终端根据所述第二密钥解密所述第一密文，得到所述目标零部件的升级数据；

所述第一终端根据所述目标零部件的升级数据升级所述第一目标零部件。

结合第九方面，在第九方面的一种可能的实施方式中，所述 OTA 升级方法具体应用于所述第一终端中的所述第一目标零部件；

或者，所述 OTA 升级系统中的第一终端中还包括升级控制部件，所述 OTA 升级方法具体应用于所述升级控制部件。

进一步的，所述升级控制部件用于控制所述第一目标零部件的升级。

结合第九方面，在第九方面的又一种可能的实施方式中，所述第一终端接收 OTA 服务器发送的第一密文和第二密文，包括：

所述第一终端通过第一下载地址与所述 OTA 服务器建立安全通道；

所述第一终端通过所述安全通道接收所述 OTA 服务器发送的第一密文和第二密文。

结合第九方面，在第九方面的又一种可能的实施方式中，所述方法还包括：

所述第一终端接收来自所述 OTA 服务器的下载策略，所述下载策略中包含所述第一下载地址。

第十方面，本申请实施例公开了一种 OTA 升级方法，包括：

第一服务器根据第一安全参数对所述目标零部件的升级数据进行加密得到第一密文，所述第一安全参数为预置的所述第一服务器与所述第一终端之间的共享密钥或者为预置的所述第一终端的第一公钥，所述第一服务器为用于提供所述目标零部件的升级数据的服务器；所述第一终端为部署有所述目标零部件的终端；

所述第一服务器向 OTA 服务器发送所述第一密文；所述第一密文用于由所述 OTA 服务器发送给第一终端以对所述第一终端中的所述目标零部件进行升级。

可以看出，第一安全参数和第二安全参数可以是预先配置或者预先获取的，第一服务器使用第一安全参数对目标零部件的升级数据进行加密，第一终端使用第二安全参数对第一密文解密从而获取目标零部件的升级数据。由于目标零部件的升级数据是经过加密传输的，没有获取第二安全参数则无法解密第二密文得到第二密钥，从而无法解密第一密文得到目标零部件的升级数据，因此保证了升级数据的机密性。当升级数据中包含核心代码、关键技术实现的情况下，可以有效保护涉密数据、关键代码等核心资产。

结合第十方面，在第十方面的一种可能的实施方式中，上述第一服务器属于目标零部件的供应商用于维护目标零部件的服务器。

第十一方面，本申请实施例公开了一种 OTA 升级方法，应用于部署有第一目标零部件的第一终端，所述第一目标零部件为目标零部件中的一个，所述方法包括：

第一终端接收 OTA 服务器发送的第一密文，所述第一密文为第一服务器根据第一安全参数对所述目标零部件的升级数据加密得到的，所述第一服务器为用于提供所述目标零部件的升级数据的服务器，所述第一安全参数为所述第一服务器与所述第一终端之间的共享密钥或者为所述第一终端的第一公钥；

所述第一终端根据第二安全参数解密所述升级包中的第一密文，得到所述目标零部件的升级数据，所述第二安全参数为所述共享密钥或者为所述第一终端的第一私钥；

所述第一终端根据所述目标零部件的升级数据升级所述目标零部件。

结合第十一方面，在第十一方面的一种可能的实现方式中，所述 OTA 升级方法具体应用于所述目标零部件。

结合第十一方面，在第十一方面的一种可能的实现方式中，所述第一终端上还部署有升级控制部件，所述 OTA 升级方法具体应用于所述升级控制部件。

第十一方面的技术方案可能与第十方面的技术方案对应，相关的有益效果可以参考第十方面的有益效果，此处不再赘述。

第十二方面，本申请实施例公开了一种 OTA 升级方法，包括：

OTA 服务器接收来自第一服务器的第一密文，所述第一密文为第一服务器根据第一安全参数对所述第一终端上的目标零部件的升级数据加密得到的，所述第一服务器为用于提

供所述目标零部件的升级数据的服务器；

所述 OTA 服务器向所述第一终端发送升级策略，所述升级策略包含所述第一密文的第一下载地址。

结合第十二方面，在第十二方面的一种可能的实施方式中，所述方法还包括：

所述 OTA 服务器通过所述安全通道向所述第一终端发送所述第一密文，所述安全通道为所述第一终端基于所述第一下载地址与所述 OTA 服务器共同建立的。

结合第十二方面，在第十二方面的又一种可能的实施方式中，所述升级策略中包括升级规则、升级条件、下载规则等等中的一项或者多项。

结合第十二方面，在第十二方面的又一种可能的实施方式中，所述方法还包括：

所述 OTA 服务器根据所述第一终端的信息和/或所述第一密文的信息，确定所述升级策略。

第十三方面，本申请实施例公开了一种 OTA 升级装置，所述 OTA 升级装置可以包括处理单元、发送单元，该 OTA 升级装置用于实现第一方面或者第一方面的任意一种可能的实施方式所描述的方法。

在一种可能的实施方案中，所述处理单元，用于根据第一密钥对目标零部件的升级数据进行加密得到第一密文，其中，所述第一服务器为用于提供所述目标零部件的升级数据的服务器；

所述发送单元，用于向 OTA 服务器发送所述第一密文；

所述发送单元，还用于向部署有所述目标零部件的第一终端发送第二密钥，所述第二密钥为所述第一密钥对应的解密密钥。

结合第十三方面，在第十三方面的一种可能的实施方式中，上述 OTA 升级装置属于目标零部件的供应商用于维护目标零部件的装置。

结合第十三方面，在第十三方面的又一种可能的实施方式中，所述处理单元，还用于与部署有所述目标零部件的所述第一终端建立安全通道；

所述发送单元，还用于通过所述安全通道向所述第一终端发送所述第二密钥。

结合第十三方面，在第十三方面的又一种可能的实施方式中，所述处理单元，还用于根据第一安全参数加密所述第二密钥得到第二密文，所述第一安全参数为所述第一服务器与所述第一终端之间的共享密钥或者为所述第一终端的第一公钥；

所述发送单元，还用于向部署有所述目标零部件的所述第一终端发送所述第二密文。

结合第十三方面，在第十三方面的又一种可能的实施方式中，所述装置还包括：

接收单元，用于接收来自所述第一终端的密钥获取请求。

结合第十三方面，在第十三方面的又一种可能的实施方式中，所述第一安全参数属于临时密钥或者属于一次性密钥。

结合第十三方面，在第十三方面的又一种可能的实施方式中，所述第一安全参数为所述第一终端的第一公钥；所述接收单元，还用于接收所述第一终端发送的所述第一终端的第一公钥；

所述处理单元，还用于通过所述第一终端的第一数字证书认证所述第一终端的第一公

钥。

结合第十三方面，在第十三方面的又一种可能的实施方式中，所述第一数字证书对应第二公钥和第二私钥；所述接收单元，还用于接收来自所述第一终端发送的第一签名，所述第一签名为使用所述第二私钥对所述第一公钥签名得到的；

所述处理单元，还用于根据所述第二公钥、所述第一签名和所述第一公钥确定所述第一公钥认证通过。

结合第十三方面，在第十三方面的又一种可能的实施方式中，所述第一安全参数为所述第一服务器与所述第一终端之间的共享密钥；所述处理单元，还用于：

通过密钥协商算法，与所述第一终端协商得到所述共享密钥；

通过所述第一服务器和所述第一终端之间的预共享密钥 PSK 认证所述第一终端的身份，所述 PSK 为所述第一服务器与所述目标零部件之间预设的秘密值。

结合第十三方面，在第十三方面的又一种可能的实施方式中，所述接收单元，还用于接收所述第一终端发送的第一消息，所述第一信息包含第一随机数；

所述发送单元，还用于向所述第一终端发送第二消息，所述第二信息包含第一认证参数和第二随机数；所述第一认证参数为根据所述第一消息、所述第二随机数和所述 PSK 得到的；

所述接收单元，还用于接收所述第一终端发送的第三消息，所述第三信息包含第二认证参数；

所述处理单元，具体用于根据所述第二消息、所述第一随机数和所述 PSK 确定所述目标零部件的身份认证通过。

结合第十三方面，在第十三方面的又一种可能的实施方式中，所述发送单元，具体用于：

向所述第一终端的升级控制部件发送所述第二密钥；

或者，向所述第一终端的所述目标零部件发送所述第二密钥。

第十四方面，本申请实施例公开了一种 OTA 升级装置，包括接收单元、处理单元，所述 OTA 升级装置用于实现第二方面或者第二方面的任意一种可能的实施方式所描述的方法。

在一种可能的实施方式中，所述接收单元，用于接收 OTA 服务器发送的第一密文，所述第一密文为第一服务器根据第一密钥对所述第一终端上的目标零部件的升级数据加密得到的，所述第一服务器为用于提供所述目标零部件的升级数据的服务器；

所述接收单元，还用于接收来自所述第一服务器的第二密钥，所述第二密钥为所述第一密钥对应的解密密钥；

所述处理单元，还用于通过所述第二密钥解密所述第一密文，得到所述目标零部件的升级数据；

所述处理单元，还用于通过所述目标零部件的升级数据，升级所述目标零部件。

结合第十四方面，在第十四方面的又一种可能的实施方式中，所述处理单元，还用于与所述第一服务器建立安全通道；

所述接收单元，具体用于通过所述安全通道接收所述第一服务器的所述第二密钥。

结合第十四方面，在第十四方面的又一种可能的实施方式中，

所述接收单元，具体用于接收来自所述第一服务器的第二密文；所述第二密文为根据第一安全参数加密第二密钥得到的；

所述处理单元，还用于根据第二安全参数解密所述第二密文，得到所述第二密钥，所述第二安全参数为所述第一服务器与所述第一终端之间的共享密钥或者为所述第一终端的第一私钥。

结合第十四方面，在第十四方面的又一种可能的实施方式中，所述装置还包括：

发送单元，用于向所述第一服务器发送密钥获取请求。

结合第十四方面，在第十四方面的又一种可能的实施方式中，所述第二安全参数属于临时密钥或者属于一次性密钥。

结合第十四方面，在第十四方面的又一种可能的实施方式中，

所述第二安全参数为所述第一公钥对应的第一私钥，所述第一安全参数为所述第一终端的第一公钥；

所述第一公钥通过所述第一终端的第一数字证书进行认证。

结合第十四方面，在第十四方面的又一种可能的实施方式中，所述第一数字证书对应第二公钥和第二私钥；

所述处理单元，还用于确定所述第一公钥和所述第一私钥；

所述处理单元，还用于通过所述第二私钥对所述第一公钥进行签名，得到第一签名，

所述发送单元，还用于向所述第一服务器发送第一签名和所述第一公钥；所述第一签名用于所述第一服务器根据所述第一签名证书对应的第二公钥认证所述第一公钥。

结合第十四方面，在第十四方面的又一种可能的实施方式中，所述第一安全参数为所述第一服务器与所述第一终端之间的共享密钥；所述处理单元，还用于：

通过密钥协商算法，与所述第一服务器协商得到所述共享密钥；

通过所述第一服务器和所述第一终端之间的预共享密钥 PSK 认证所述第一服务器的身份，所述 PSK 为所述第一服务器与所述目标零部件之间预设的秘密值。

结合第十四方面，在第十四方面的又一种可能的实施方式中，所述发送单元，还用于向所述第一服务器发送第一消息，所述第一消息包含第一随机数；

所述接收单元，还用于接收所述第一服务器发送的第二消息，所述第二消息包含第一认证参数和第二随机数；

所述处理单元，具体用于根据所述第一认证参数、所述第一消息、所述第二随机数和所述 PSK 确定所述第一服务器的身份认证通过；

所述发送单元，还用于向所述第一服务器发送第三消息，所述第三消息包含第二认证参数；所述第二认证参数为根据所述第一随机数、所述第二消息和所述 PSK 得到的。所述第二认证参数用于认证所述第一终端的身份。

结合第十四方面，在第十四方面的又一种可能的实施方式中，所述 OTA 升级装置具体为第一终端中的所述目标零部件；

或者，所述 OTA 升级装置具体为所述第一终端中的升级控制部件。

第十五方面，本申请实施例公开了一种 OTA 升级装置，包括接收单元和发送单元，所述 OTA 升级装置用于实现第三方面或者第三方面的任意一种可能的实施方式所描述的方法。

在一种可能的实施方式中，所述接收单元，用于接收来自第一服务器的第一密文，所述第一密文为第一服务器根据第一密钥对所述第一终端上的目标零部件的升级数据加密得到的，所述第一服务器为用于提供所述目标零部件的升级数据的服务器；

所述发送单元，用于向所述第一终端发送升级策略，所述升级策略包含所述第一密文的第一下载地址。

结合第十五方面，在第十五方面的一种可能的实施方式中，所述发送单元，具体用于通过所述安全通道向所述第一终端发送所述第一密文，所述安全通道为所述第一终端基于所述第一下载地址与所述 OTA 服务器共同建立的。

结合第十五方面，在第十五方面的又一种可能的实施方式中，所述升级策略中包括升级规则、升级条件、下载规则等等中的一项或者多项。

其中，升级规则用于定义升级的次序、是否需要进行回滚等规则，升级条件可以包含是否供电正常、存储空间、网络状态、有依赖关系的其他设备的状态等，下载规则用于定义下载的顺序、指示哪一个部件进行下载等等。

结合第十五方面，在第十五方面的又一种可能的实施方式中，所述装置还包括：

处理单元 1503，用于根据所述第一终端的信息和/或所述第一密文的信息，确定所述升级策略。

例如，OTA 服务器根据第一终端的信息和第一密文的文件大小，确定所述第一终端需要的存储空间大小。

第十六方面，本申请实施例公开了一种 OTA 升级装置，包括发送单元，所述 OTA 升级装置用于实现第四方面或者第四方面的任意一种可能的实施方式所描述的方法。所述 OTA 升级装置为用于提供所述目标零部件的升级数据的装置，

在一种可能的实施方式中，所述发送单元，用于向 OTA 服务器发送目标零部件的升级数据的元数据，所述升级数据的元数据包含所述升级数据的第一下载地址和所述升级数据的版本信息；

所述发送单元，还用于通过安全通道向部署有所述目标零部件的第一终端发送所述目标零部件的升级数据，所述安全通道为所述第一终端根据所述第一下载地址与所述第一服务器共同建立的。

结合第十六方面，在第十六方面的一种可能的实施方式中，所述 OTA 升级装置属于所述目标零部件的供应商用于维护所述目标零部件的装置。

结合第十六方面，在第十六方面的又一种可能的实施方式中，所述 OTA 升级装置还包括：

处理单元，用于确定所述目标零部件的升级数据的元数据。

结合第十六方面，在第十六方面的又一种可能的实施方式中，所述发送单元，具体用于：

通过所述安全通道向所述第一终端中的所述目标零部件发送所述目标零部件的升级数

据；

或者，通过所述安全通道向所述第一终端中的升级控制部件发送所述目标零部件的升级数据。

第十七方面，本申请实施例公开了一种 OTA 升级装置，所述 OTA 升级装置包括接收单元、处理单元，所述 OTA 升级装置用于实现第五方面或者第五方面的任意一种可能的实施方式所描述的方法。所述 OTA 升级装置中部署有目标零部件。

在一种可能的实现方式中，所述接收单元，用于接收 OTA 服务器发送的下载策略，所述下载策略中包含目标零部件的升级数据的第一下载地址；所述目标零部件部署在所述第一终端上；

所述处理单元，用于基于所述第一下载地址，与第一服务器共同建立安全通道，所述第一服务器为用于提供所述目标零部件的升级数据的服务器；

所述处理单元，还用于通过所述安全通道接收所述第一服务器发送的所述目标零部件的升级数据；

所述处理单元，还用于根据所述目标零部件的升级数据升级所述目标零部件。

结合第十七方面，在第十七方面的又一种可能的实施方式中，所述 OTA 升级装置具体为第一终端中的所述目标零部件；

或者，所述 OTA 升级装置具体为所述第一终端中的升级控制部件。

第十八方面，本申请实施例公开了一种 OTA 升级装置，包括接收单元、发送单元，所述 OTA 升级装置用于实现第六方面或者第六方面的任意一种可能的实施方式所描述的方法。

在一种可能的实施方式中，所述接收单元，用于接收第一服务器发送的目标零部件的升级数据的元数据，其中，所述第一服务器为用于提供所述目标零部件的升级数据的服务器，所述升级数据的元数据包含所述升级数据的第一下载地址和所述升级数据的版本信息；

所述发送单元，用于向所述第一终端发送升级策略，所述升级策略包含所述第一密文的第一下载地址。

结合第十八方面，在第十八方面的又一种可能的实施方式中，所述装置还包括：

处理单元，用于根据所述第一终端的信息和/或升级数据的元数据，确定所述升级策略。

结合第十八方面，在第十八方面的又一种可能的实施方式中，所述升级策略中包含升级规则、升级条件、下载规则等等中的一项或者多项。

结合第十八方面，在第十八方面的又一种可能的实施方式中，所述元数据中还包括所述目标零部件的升级数据的文件大小。

第十九方面，本申请实施例公开了一种 OTA 升级装置，包括处理单元、发送单元，所述 OTA 装置用于实现第七方面或者第七方面的任意一种可能的实施方式所描述的方法。所述 OTA 升级装置可以为用于提供所述目标零部件的升级数据的装置。

在一种可能的实施方案中，所述处理单元，用于根据第一密钥对目标零部件的升级数据进行加密得到第一密文，其中，所述第一服务器为用于提供所述目标零部件的升级数据

的服务器；

所述处理单元，用于通过第一安全参数的加密第二密钥得到第二密文，其中，所述第一安全参数为所述第一服务器与所述第一终端之间的共享密钥或者为所述第一终端的第一公钥，所述第一终端为部署有第一目标零部件的终端，所述第一目标零部件为所述目标零部件中的一个，所述第二密钥为所述第一密钥的解密密钥；

所述发送单元，用于向 OTA 服务器发送所述第一密文和所述第二密文，所述第二密文用于所述第一终端解密所述第一密文。

结合第十九方面，在第十九方面的一种可能的实施方式中，所述 OTA 升级装置属于所述目标零部件的供应商用于维护所述目标零部件的装置。

第二十方面，本申请实施例公开了一种 OTA 升级装置，包括接收单元、发送单元，所述 OTA 升级装置用于实现第八方面或者第八方面的任意一种可能的实施方式所描述的方法。

在一种可能的实施方式中，所述接收单元，用于接收第一服务器发送的第一密文和第二密文，其中，所述第一密文为根据第一密钥对目标零部件的升级数据加密得到的，所述第二密文为根据第一安全参数对第二密钥加密得到的，所述第一安全参数为所述第一服务器与第一终端之间的共享密钥或者为所述第一终端的第一公钥，所述第一终端为部署有第一目标零部件的终端，所述第一目标零部件为所述目标零部件中的一个，所述第二密钥为所述第一密钥的解密密钥；

所述发送单元，用于向所述第一终端发送所述第一密文和所述第二密文，其中所述第二密文用于所述第一终端解密所述第一密文，以得到所述目标零部件的升级数据。

结合第二十方面，在第二十方面的一种可能的实施方式中，所述装置，还包括：

处理单元，用于根据所述第一密文所在的升级包的属性和所述第一终端的信息生成升级策略；所述升级策略包括所述第一密文和所述第二密文的第一下载地址；

所述发送单元，还用于向所述第一终端发送所述升级策略；

所述发送单元，还用于通过安全通道向所述第一终端发送所述第一密文和所述第二密文，所述安全通道为所述第一终端根据所述第一下载地址与所述 OTA 服务器共同建立的。

第二十一方面，本申请实施例公开了一种 OTA 升级装置，包括接收单元、处理单元，所述 OTA 升级装置用于实现第九方面或者第九方面的任意一种可能的实施方式所描述的方法。其中，所述 OTA 升级装置中（或者 OTA 升级装置所在的设备中）部署有第一目标零部件，所述第一目标零部件为目标零部件中的一个。

在一种可能的实施方式中，所述接收单元，用于接收 OTA 服务器发送的第一密文和第二密文，所述第一密文为第一服务器根据第一密钥对所述目标零部件的升级数据加密得到的，其中，所述第一服务器为用于提供所述目标零部件的升级数据的服务器；

所述处理单元，用于根据第二安全参数解密所述第二密文得到第二密钥，所述第二密钥为所述第一密钥的解密密钥，所述第二安全参数为所述第一服务器与所述第一终端之间的共享密钥或者为所述第一终端的第一私钥；

所述处理单元，还用于根据所述第二密钥解密所述第一密文，得到所述目标零部件的

升级数据；

所述处理单元，还用于根据所述目标零部件的升级数据升级所述第一目标零部件。

结合第二十一方面，在第二十一方面的一种可能的实施方式中，所述 OTA 升级装置具体为所述第一终端中的所述第一目标零部件；

或者，所述 OTA 升级装置具体为所述第一终端中的升级控制部件。

结合第二十一方面，在第二十一方面的又一种可能的实施方式中，所述处理单元，还用于通过第一下载地址与所述 OTA 服务器建立安全通道；

所述接收单元，具体用于通过所述安全通道接收所述 OTA 服务器发送的第一密文和第二密文。

结合第二十一方面，在第二十一方面的又一种可能的实施方式中，所述接收单元，还用于接收来自所述 OTA 服务器的下载策略，所述下载策略中包含所述第一下载地址。

第二十二方面，本申请实施例公开了一种 OTA 升级装置，包括处理单元、发送单元，所述 OTA 升级装置用于实现第十方面或者第十方面的任意一种可能的实施方式所描述的方法。所述 OTA 升级装置可以为用于提供所述目标零部件的升级数据的装置。

在一种可能的实施方案中，所述处理单元，用于根据第一安全参数对所述目标零部件的升级数据进行加密得到第一密文，所述第一安全参数为预置的所述第一服务器与所述第一终端之间的共享密钥或者为预置的所述第一终端的第一公钥，所述第一服务器为用于提供所述目标零部件的升级数据的服务器；所述第一终端为部署有所述目标零部件的终端；

所述发送单元，用于向 OTA 服务器发送所述第一密文；所述第一密文用于由所述 OTA 服务器发送给第一终端以对所述第一终端中的所述目标零部件进行升级。

结合第二十二方面，在第二十二方面的一种可能的实施方式中，上述 OTA 升级装置属于目标零部件的供应商用于维护目标零部件的装置。

第二十三方面，本申请实施例公开了一种 OTA 升级装置，包括接收单元、处理单元，所述 OTA 升级装置用于实现第十一方面或者第十一方面的任意一种可能的实施方式所描述的方法。其中，所述 OTA 升级装置中部署有第一目标零部件，所述第一目标零部件为目标零部件中的一个。

在一种可能的实现方式中，所述接收单元，用于接收 OTA 服务器发送的第一密文，所述第一密文为第一服务器根据第一安全参数对所述目标零部件的升级数据加密得到的，所述第一服务器为用于提供所述目标零部件的升级数据的服务器，所述第一安全参数为所述第一服务器与所述第一终端之间的共享密钥或者为所述第一终端的第一公钥；

所述处理单元，用于根据第二安全参数解密所述升级包中的第一密文，得到所述目标零部件的升级数据，所述第二安全参数为所述共享密钥或者为所述第一终端的第一私钥；

所述处理单元，还用于根据所述目标零部件的升级数据升级所述目标零部件。

结合第二十三方面，在第二十三方面的又一种可能的实施方式中，所述 OTA 升级装置具体为第一终端中的所述目标零部件；

或者，所述 OTA 升级装置具体为所述第一终端中的升级控制部件。

第二十四方面，本申请实施例公开了一种 OTA 升级装置，包括接收单元、发送单元，所述 OTA 升级装置用于实现第十二方面或者第十二方面的任意一种可能的实施方式所描述的方法。

在一种可能的实施方式中，所述接收单元，用于接收来自第一服务器的第一密文，所述第一密文为第一服务器根据第一安全参数对所述第一终端上的目标零部件的升级数据加密得到的，所述第一服务器为用于提供所述目标零部件的升级数据的服务器；

所述发送单元，用于向所述第一终端发送升级策略，所述升级策略包含所述第一密文的第一下载地址。

结合第二十四方面，在第二十四方面的一种可能的实施方式中，所述发送单元，具体用于通过所述安全通道向所述第一终端发送所述第一密文，所述安全通道为所述第一终端基于所述第一下载地址与所述 OTA 服务器共同建立的。

结合第二十四方面，在第二十四方面的又一种可能的实施方式中，所述升级策略中包含升级规则、升级条件、下载规则等等中的一项或者多项。

结合第二十四方面，在第二十四方面的又一种可能的实施方式中，所述装置还包括：

处理单元，用于根据所述第一终端的信息和/或所述第一密文的信息，确定所述升级策略。

第二十五方面，本申请实施例还提供一种第一服务器，所述服务器包括至少一个处理器和通信接口，所述通信接口用于发送和/或接收数据，所述至少一个处理器用于调用至少一个存储器中存储的计算机程序，以使得所述第一服务器实现第一方面或第一方面任意一种可能的实施方式所描述的方法；又或者实现第四方面或第四方面的任意一种可能的实施方式所描述的方法；又或者实现第七方面或第七方面的任意一种可能的实施方式所描述的方法；又或者实现第十一方面或第十一方面的任意一种可能的实施方式所描述的方法。

第二十六方面，本申请实施例还提供一种第一终端，所述第一终端包括至少一个处理器和通信接口，所述通信接口用于发送和/或接收数据，所述至少一个处理器用于调用至少一个存储器中存储的计算机程序，以使得所述第一终端实现第二方面或第二方面任意一种可能的实施方式所描述的方法；又或者实现第五方面或第五方面的任意一种可能的实施方式所描述的方法；又或者实现第九方面或第九方面的任意一种可能的实施方式所描述的方法；又或者实现第十一方面或第十一方面的任意一种可能的实施方式所描述的方法。

可选的，所述第一终端可以为网关、整车集成单元、T-box 等装置，也可以为车辆、机器人或者无人机等智能设备或者运输终端。

第二十七方面，本申请实施例还提供一种 OTA 服务器，所述 OTA 服务器包括至少一个处理器和通信接口，所述通信接口用于发送和/或接收数据，所述至少一个处理器用于调用至少一个存储器中存储的计算机程序，以使得所述 OTA 服务器实现第三方面或第三方面任意一种可能的实施方式所描述的方法；又或者实现第六方面或第六方面的任意一种可能的实施方式所描述的方法；又或者实现第八方面或第八方面的任意一种可能的实施方式所描述的方法；又或者实现第十二方面或第十二方面的任意一种可能的实施方式所描述的方法。

第二十八方面，本申请实施例还提供一种 OTA 升级系统，该 OTA 升级系统包括第一服务器和目标零部件。其中，该第一服务器用于实现上述第一方面或者第一方面的又一种可能的实现方式所描述的方法，该目标零部件用于实现上述第二方面或者第二方面的一种可能的实现方式所描述的方法；

或者，该第一服务器用于实现上述第四方面或者第四方面的又一种可能的实现方式所描述的方法，该目标零部件用于实现上述第五方面或者第五方面的一种可能的实现方式所描述的方法；

或者，该第一服务器用于实现上述第七方面或者第七方面的又一种可能的实现方式所描述的方法，该目标零部件用于实现上述第九方面或者第九方面的一种可能的实现方式所描述的方法；

或者，该第一服务器用于实现上述第十方面或者第十方面的又一种可能的实现方式所描述的方法，该目标零部件用于实现上述第十一方面或者第十一方面的一种可能的实现方式所描述的方法。

第二十九方面，本申请实施例还提供一种 OTA 升级系统，该 OTA 升级系统包括 OTA 服务器和第一终端。其中，该 OTA 服务器用于实现上述第三方面或者第三方面的又一种可能的实现方式所描述的方法，该第一终端用于实现上述第二方面或者第二方面的一种可能的实现方式所描述的方法；

或者，该 OTA 服务器用于实现上述第六方面或者第六方面的又一种可能的实现方式所描述的方法，该第一终端用于实现上述第五方面或者第五方面的一种可能的实现方式所描述的方法；

或者，该 OTA 服务器用于实现上述第八方面或者第八方面的又一种可能的实现方式所描述的方法，该第一终端用于实现上述第九方面或者第九方面的一种可能的实现方式所描述的方法；

或者，该 OTA 服务器用于实现上述第十二方面或者第十二方面的又一种可能的实现方式所描述的方法，该第一终端用于实现上述第十一方面或者第十一方面的又一种可能的实现方式所描述的方法。

第三十方面，本申请实施例公开了一种计算机可读存储介质，所述计算机可读存储介质中存储有计算机程序，当所述计算机程序在一个或多个处理器上运行时，实现第一方面至第十二方面（或者还包括其可能的实施方式）所描述的方法。

第三十一方面，本申请实施例公开了一种计算机程序产品，当所述计算机程序产品在一个或多个处理器上运行时，实现第一方面至第十二方面（或者还包括其可能的实施方式）所描述的方法。

可以理解的，本申请实施例装置侧的有益效果可以参考对应的方法侧，此处不再赘述。

附图说明

以下对本申请实施例用到的附图进行介绍。

图 1 是本申请实施例的一种 OTA 升级系统的架构示意图；

图 2 是本申请实施例提供的一种车辆升级系统的架构示意图；

图 3 是本申请实施例提供的一种 OTA 升级方法的流程示意图；
图 4 是本申请实施例提供的一种车辆的架构示意图；
图 5 是本申请实施例提供的一种确定第一安全参数的方法的流程示意图；
图 6 是本申请实施例提供的又一种确定第一安全参数的方法的流程示意图；
图 7 是本申请实施例提供的又一种 OTA 升级系统的架构示意图；
图 8 是本申请实施例提供的又一种 OTA 升级方法的流程示意图；
图 9 是本申请实施例提供的再一种 OTA 升级系统的架构示意图；
图 10 是本申请实施例提供的再一种 OTA 升级方法的流程示意图；
图 11 是本申请实施例提供的再一种 OTA 升级系统的架构示意图；
图 12 是本申请实施例提供的再一种 OTA 升级方法的流程示意图；
图 13 是本申请实施例提供的一种 OTA 升级装置的结构示意图；
图 14 是本申请实施例提供的又一种 OTA 升级装置的结构示意图；
图 15 是本申请实施例提供的再一种 OTA 升级装置的结构示意图；
图 16 是本申请实施例提供的再一种 OTA 升级装置的结构示意图。

具体实施方式

下面结合本申请实施例中的附图对本申请实施例进行描述。需要说明的是，本申请中，“示例性的”或者“例如”等词用于表示作例子、例证或说明。本申请中被描述为“示例性的”或者“例如”的任何实施例或设计方案不应被解释为比其他实施例或设计方案更优选或更具优势。确切而言，使用“示例性的”或者“例如”等词旨在以具体方式呈现相关概念。

本申请中实施例提到的“至少一个”是指一个或者多个，“多个”是指两个或两个以上。“以下至少一项(个)”或其类似表达，是指的这些项中的任意组合，包括单项(个)或复数项(个)的任意组合。例如，a、b、或 c 中的至少一项(个)，可以表示：a、b、c、(a 和 b)、(a 和 c)、(b 和 c)、或 (a 和 b 和 c)，其中 a、b、c 可以是单个，也可以是多个。“和/或”，描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A、同时存在 A 和 B、单独存在 B 这三种情况，其中 A、B 可以是单数或者复数。字符“/”一般表示前后关联对象是一种“或”的关系。

以及，除非有相反的说明，本申请实施例使用“第一”、“第二”等序数词是用于对多个对象进行区分，不用于限定多个对象的顺序、时序、优先级或者重要程度。例如，第一探测装置和第二探测装置，只是为了区分不同的探测装置，而并不是表示这两种装置的结构、探测原理、重要程度等的不同。

为了便于理解，下面先对本申请实施例中的部分用语进行解释说明。

一、安全算法（密码算法）

（1）散列算法

散列算法又称为哈希（hash）函数、哈希算法，散列算法可以将一段数据（例如字符串、数字、文件等）输出为一段预设长度（例如 80 位、或者 128 位等等）的散列值（散列值也可以称为哈希值、摘要值等），且很难找到逆向规律。常见的散列算法主要有安全散列

算法 (secure hash algorithm 1, SHA-1)、信息摘要 (message digest, MD) 算法 (如 MD2、MD4 或 MD5 等) 等。

(2) 加密 (encryption) 算法

加密算法用于保护数据的机密性 (confidentiality), 通常表现为对明文加密得到密文。加密算法既可以包括加密运算 (例如椭圆点加运算、异或运算等), 也可以包括安全性较高的各种算法。常见的加密算法主要有异或运算、数据加密标准 (data encryption standard, DES)、三重数据加密算法 (triple data encryption algorithm, 3DES)、高级加密标准 (advanced encryption standard, AES)、RSA 加密算法、数据结构分析算法 (data structure analysis, DSA) 等。

(3) 完整性保护算法

完整性保护算法是用于保护数据完整性 (data integrity) 的算法, 也可以称为完保算法。在一些具体实现中, 完整性保护算法通常会输出消息认证码 (message authentication code, MAC), 某些场景中也将完整性保护算法称为 MAC 算法。完整性保护算法可以通过多种哈希算法来实现, 通过哈希算法来实现的完整性保护算法称为基于哈希的消息认证码 (hash-based message authentication code, HMAC) 算法, 其中的哈希算法可以为 MD5、SHA-1、SHA-256 等等中的一个, 这些不同的 HMAC 实现通常标记为: HMAC-MD5, HMAC-SHA1, HMAC-SHA256 等等。

在一些具体场景中, 通过认证加密算法, 对与给定的原文既可以加密数据也可以生成消息认证码, 因此认证加密算法既可以作为加密算法也可以作为完保算法。例如, 基于 GMAC 和计数加密模式的 AES 算法 (AES-Galois/counter mode, AES-GCM) 和基于 CMAC 和计数加密模式的 AES 算法 (AES-CMAC/counter Mode, AES-CCM) 等, 既可以对消息进行认证加密, 认证加密的过程中也能够保护消息的完整性。

(4) 密钥派生算法

密钥派生算法用于从一个秘密值中派生出一个或多个秘密值, 又称为密钥导出算法。例如, 通过秘密值 Key 派生的新的秘密值 DK 可以表示为: $DK = KDF(Key)$ 。常用的密钥派生算法有基于密码的密钥派生函数 (password-based key derivation function, PBKDF)、斯克里普特 (scrypt) 算法等, 其中 PBKDF 算法又包括第一代 PBKDF1 和第二代 PBKDF2。可选的, 一些 KDF 算法在派生密钥过程中, 使用哈希算法对输入的秘密值进行哈希变化, 因此 KDF 函数还可以接收算法标识作为输入, 用于指示使用何种哈希算法。

需要说明的是, KDF 不仅应用于派生得到秘密值得过程, 也可以应用在生成认证信息、身份信息场景中。

(5) 密钥协商算法

密钥协商是通信双方通过交互一部分参数, 从而协商得到密钥的过程。用于密钥协商的算法称为密钥协商算法, 也可以称为密钥交换算法。常用的密钥协商算法有迪菲赫尔曼 (Diffie-Hellman, DH) 算法、基于椭圆曲线密码 (Elliptic Curve Cryptosystems, ECC) 的迪菲赫尔曼 (ECDH) 算法、奥克利 (Oakley) 算法、国密算法 (如 SM1、SM2、SM3 和 SM4) 等。

其中, 以 DH 算法为例, 两个装置使用两个数值较大的素数 p 和随机数 g , 各自产生的随机数 a 和 b 。第二装置将 g 的 a 次方 mod P 产生的数值 $A (A = g^a \text{ mod } p)$ 发送给第一装置,

第一装置将 g 的 b 次方 $\bmod p$ 产生的数值 B ($B=gb \bmod p$) 发送给第二装置, 第二装置再对接收的结果做 a 次方运算 ($K=Ba \bmod p$), 第一装置对接收的结果做 b 次方运算 ($K=Ab \bmod p$), 由于 $K=Ab \bmod p = (ga \bmod p)b \bmod p = gab \bmod p = (gb \bmod p)a \bmod p = Ba \bmod p$, 因此第一装置和第二装置计算出的密钥 K 是相同的。

在这种情况下, 若攻击者通过 A 、 g 、 p , 计算得到 a 的公式为: $a=\log_g A \bmod p$, 由于对数运算没有一个快速计算的算法, 而且素数 p 和随机数 g 通常数值较大, 因此攻击者很难通过 A 、素数 p 和随机数 g 通过对数运算和模运算得到 a 。因此通过 DH 算法得到的密钥 K 是具有安全性的。

其中, ECDH 算法主要基于如下等式来实现: $K=k \times G$, 其中 K 、 G 为椭圆曲线 $E_p(a,b)$ 上的点, n 为 G 的阶 ($nG=O_\infty$, O_∞ 指无穷远点), k 为小于 n 的整数。在 $K=kG$ 中, 对于给定的 k 和 G , 根据加法法则, 计算 K 很容易 (例如使用点加运算进行累加)。但反过来, 对于给定的 K 和 G , 求 k 就非常困难。因为实际使用中的椭圆曲线算法原则上把 p 取得相当大, n 也相当大, 要把 k 个点逐一算出来与 K 进行比较是数学难题。

可以理解的, 前述的关于算法的解释只是用于简单叙述实现的原理, 并不限定使用时一定使用相同的参数进行实现。算法具体实现过程中还可以有其他的改进和变体, 本申请中提到算法可以为经过改进和变体后的算法, 例如 ECC 可以结合在 DSA 算法中, 称为 ECDSA 算法。

二、新鲜性参数

新鲜性参数用于生成密钥和认证参数等, 也可以称为新鲜度或新鲜参数, 可以包括随机数 (number once, NONCE)、计数值 (counter)、序列号 (serial number)、顺序号 (sequence number) 等等中的至少一个。其中, NONCE 是一个只被使用一次的 (或者说非重复的) 随机数值。不同时刻生成的新鲜性参数通常不同, 即新鲜性参数的具体取值, 在每生成一次新鲜性参数时会发生变化, 从而使得这一次生成密钥 (或者认证参数等) 所使用的新鲜性参数与上一次生成密钥 (或者认证参数等) 时所使用的新鲜性参数不同的, 可以提高生成的密钥 (或者认证参数等) 的安全性。

例如, 新鲜性参数可以是节点通过随机数发生器 (random number generator) 获取的随机数。

三、数字证书

数字证书 (也可以称为安全证书) 是标志身份的一个数字认证, 通常是由证书授权 (Certificate Authority, CA) 中心或者受信任的第三方设备所颁发的一种较为权威与公正的证书。

例如, 第一终端中存在一个长期密钥对 (长期公钥 PK 和长期私钥 SK), CA 中心为长期公钥 PK 做认证, CA 中心用自己的私钥 cpk , 对该长期公钥 PK 和一些相关信息 (例如对第二节点的描述信息) 一起加密生成 DC。第一终端使用证书对应的私钥生成第一公钥的签名 (即 “私钥签名”), 将第一公钥、第一公钥的签名以及 DC 发送给第一服务器, 第一服务器使用 CA 中心的公钥 csk 解密证书, 可以确定该 DC 为 CA 颁发的, 以及确定该 DC 中的长期公钥 PK 来自第一终端, 从而认证了长期公钥 PK 的来源。第一服务器使用长期公钥 PK 对第一公钥的签名进行验签 (即 “公钥验签”), 从而确定第一公钥来自第一终端。

下面对本申请实施例的系统架构和业务场景进行描述。需要说明的是，本申请描述的系统架构及业务场景是为了更加清楚的说明本申请的技术方案，并不构成对于本申请提供的技术方案的限定，本领域普通技术人员可知，随着系统架构的演变和新业务场景的出现，本申请提供的技术方案对于类似的技术问题，同样适用。

请参见图 1，图 1 是本申请实施例提供的一种 OTA 升级系统的示意图，包括第一服务器 101、OTA 服务器（server）102、终端 103，其中：

第一服务器 101 是具有数据处理能力的设备，可以是实体设备如主机、服务器等，也可以是虚拟设备如虚拟机、容器等。需要说明的是，此处为了便于描述称为服务器，具体实现过程中可以是服务器，也可以是其他具有数据处理能力的设备。第一服务器 101 为提供目标零部件的升级数据的服务器。例如，第一服务器可以属于目标零部件的供应商维护目标零部件的服务器。

OTA 服务器 102 是 OTA 升级过程中，与终端进行信息交互的服务器。通常来说，OTA 服务器可以指示终端需要进行某一零部件的升级，可选的，OTA 服务器还可以将零部件的升级数据发送给终端。在一些具体的实施场景中，也将 OTA 服务器称为 OTA 云端。

第一终端 103 为部署有目标零部件 104 的终端。第一终端 103 可以通过 OTA 服务器 102 获取升级数据，从而进行升级目标零部件 104。

在一种可能的设计中，目标零部件 104 具有数据收发能力，从而可以从 OTA 服务器 102 中获取升级数据从而进行升级。

在又一种可能的设计中，第一终端 103 上可以部署有升级控制部件 105，该第一终端 103 可以通过升级控制部件 105 从 OTA 服务器 102 中获取升级数据。进一步的，第一终端 103 可以通过升级控制部件 105 对目标零部件 104 进行升级，或者通过升级控制部件 105 控制目标零部件 104 进行升级。例如，升级控制部件 105 用于接收升级数据、指挥升级的次序、检查升级状态、刷写升级数据等等中的一项或者多项都可以看作升级控制部件 105 控制目标零部件 104 进行升级。

在一些具体实施场景中，第一终端 103 的升级控制部件 105 具体又可以包括 OTA 主模块（Master）和 OTA 从模块（slave），OTA 主模块将从 OTA 服务器获取的升级包分发给终端中的一个或者多个 OTA 从模块，该一个或者多个 OTA 从模块指挥终端内的零部件安装和激活升级包，完成升级。以第一终端为车辆为例，请参见图 2，图 2 是本申请实施例例举的一种可能的车辆升级系统的示意图，包括供应商服务器 201、OTA 云端 202 和车辆 203。车辆 203 是基于车辆电子电气（Electrical/Electronic Architecture, E/E）架构的车辆，参见区域 204，车辆 203 可以包括以下部件：移动数据中心（Mobile Data Center, MDC）、人机交互（Human-Machine Interaction, HMI）、网关（gateway, GW）、汽车盒子（Telematics BOX, Tbox 或者称为 TCU）、电子控制单元（Electronic Control Unit, ECU）等模块。其中，GW 是整车电子电气架构中的核心部件，其作为整车网络的数据交互枢纽，可将控制区域网络（Controller Area Network, CAN）、局域互联网络（Local Interconnect Network, LIN）、多媒体数据传输（Media Oriented System Transport, MOST）、FlexRay 等网络数据在不同网络中进行路由。MDC 是汽车的智能车载计算平台。T-BOX 主要用于和汽车外部、后台系

统和手机应用(application, APP)通信。HMI 是汽车的信息娱乐系统。ECU 是汽车专用微机控制器。在车辆203的GW中部署有升级主模块(update master, 可以看作是OTA master), 车辆203的多个零部件中部署有升级从模块(update slave, 可以看作是OTA slave), GW中的升级主模块接收OTA云端202发送的升级包, 将其分发给升级从模块, 使得升级从模块指挥车辆内的零部件安装和激活升级包, 完成对车辆203中的一个或者多个零部件的升级。

但是, 现有的OTA升级时, 升级的过程是由OTA服务器进行主导。该OTA服务器由OEM负责维护, 也即是说, OEM负责审核软件版本、分发升级包。例如, 在图2所示的架构中, 供应商服务器201需要将升级包交由OTA云端202(OTA服务器), 由OTA云端202将升级包分发给需要升级的车辆203。但是随着智能网联汽车发展, 部分敏感部件、特殊应用等需要升级时, 若将升级包交给OEM审核后通过OTA服务器下载, 则可能使得升级包的数据被泄露, 可能导致零部件供应商的核心技术、关键数据被泄露或者涉密数据遭到曝光。

为了解决上述问题, 本申请提出如下实施例。

请参见图3, 图3是本申请实施例提供的一种OTA升级方法的流程示意图, 该方法包括但不限于如下步骤:

步骤S301: 第一服务器根据第一密钥对目标零部件的升级数据进行加密得到第一密文。

其中, 目标零部件是一个待升级的部件。该目标零部件可以部署在一个或者多个终端上, 例如, 以终端为某一车辆为例, 目标零部件可以为车辆中的GW、Tbox、VIU、DC、ECU等等, 或者还可以为车辆中的媒体设备如摄像头、雷达等等, 或者还可以为车辆中的软件, 例如操作系统、导航软件、地图软件、监控软件等等。其中, ECU由处理器、存储器、输入/输出(I/O)接口、模数转换器(A/D)以及整形、驱动等大规模集成电路中的一个或者多个组成, 可以完成多种多样的功能。

第一服务器为用于提供目标零部件的升级数据的服务器。进一步的, 第一服务器可以用于目标零部件的供应商在维护目标零部件的过程中使用。本申请例举一种可能的场景: 第一服务器可以是属于目标零部件的供应商的地图更新服务器, 用于该供应商更新目标零部件的地图数据。

需要说明的是, 本申请各实施例中提到的服务器(例如第一服务器、OTA服务器等), 可以是一个服务器、也可以是多个服务器组成的服务器集群。例如, 第一服务器可以为多个服务器通过分布式架构部署的服务器集群, 集群中可以包括云计算服务器、内容分发网络(Content Delivery Network, CDN)服务器、网络时间协议(Network Time Protocol, NTP)、域名解析系统(Domain Name System, DNS)服务器等等中的一个或者多个。其中, 各个服务器之间可以相互协调, 共同完成计算、数据存储、通信等功能, 为了方便描述, 本申请实施例中将单个服务器、分布式服务器、服务器集群等统称为服务器。

第一密钥可以是对称密钥, 也可以是非对称密钥。具体的, 通过非对称密钥加密算法进行加密的密文, 加密密钥和解密的密钥通常不同。使用对称加密算法进行加密的密文, 加密密钥和解密密钥相同。

目标零部件的升级数据用于对目标零部件进行升级。例如，目标零部件的升级数据可以为操作系统更新、应用软件版本更新、漏洞补丁、对地图数据的更新、标定数据更新等等。可选的，该目标零部件的升级数据可以经过目标零部件的供应商的审核。

第一服务器可以通过加密算法，根据第一密钥对目标零部件的升级数据进行加密。例如，得到的第一密文满足如下式子：第一密文= Enc（升级数据，第一密钥），其中，Enc为加密算法，具体可以为 DES 算法、AES 算法等等中的一个或者多个的组合。

可选的，对于存在多个目标零部件时（例如第一终端上部署了第一目标零部件，第二终端上部署了第二目标零部件），对多个目标零部件的升级数据的加密可以使用相同的密钥进行加密，也可以使用不同的密钥进行加密。

可选的，目标零部件可能存在多项升级数据，第一服务器可以将多项升级数据中的部分升级数据进行加密，得到第一密文。该第一密文可以与其他未加密的升级数据一同打包得到升级包，该升级包用于目标零部件的升级。本申请例举一种可能的场景：第一服务器对目标零部件进行漏洞补丁和地图数据更新，此时可以将地图数据更新加密得到第一密文，而将漏洞补丁和第一密文打包得到升级包。这样一来，第一服务器可以只加密需要进行机密性保护的数据，减轻计算压力。

当然，第一服务器也可以将一项或者多项升级数据先打包得到升级包，然后将升级包进行加密。本申请再例举一种可能的场景：第一服务器对目标零部件进行漏洞补丁和地图数据更新，此时可以将漏洞补丁和地图数据更新打包得到升级包，对升级包进行加密得到第一密文。

步骤 S302：第一服务器向 OTA 服务器发送第一密文。

可以理解的，第一服务器向 OTA 服务器发送第一密文，相应的，OTA 服务器则接收来自第一服务器的第一密文。

在具体实施过程中，若第一密文包含在升级包中，第一服务器可以向 OTA 服务器发送升级包。OTA 服务器接收来自第一服务器的升级包，从而接收到升级包中第一密文。

可选的，第一服务器还可以向 OTA 服务器发送第一密文的元数据或者第一密文所在的升级包的元数据（metadata）。其中，元数据是用于描述第一密文或者升级包的数据属性的数据，例如第一密文的文件大小、第一密文的版本等等。该元数据可以用于 OTA 服务器确定升级策略等。

可选的，图 3 所示的实施例可以包括步骤 S303-步骤 S304 中的一个或者多个步骤，步骤 S303-步骤 S304 具体如下：

步骤 S303：OTA 服务器确定升级策略，该升级策略中包含第一密文的第一下载地址。

具体地，第一下载地址用于下载第一密文或者下载包含第一密文的升级包。可选的，OTA 服务器接收第一密文后，可以为第一密文分配第一下载地址。可选的，第一下载地址可以为统一资源定位符（uniform resource locator，URL）。

可选的，升级策略还可以包括升级规则、升级条件、下载规则等等中的一项或者多项。其中，升级规则用于定义升级的次序、是否需要进行回滚等规则，升级条件可以包含是否供电正常、存储空间、网络状态、有依赖关系的其他设备的状态等，下载规则用于定义下载的顺序、指示哪一个部件进行下载等等。

可选的, OTA 服务器根据第一终端的信息和/或所述第一密文(或者所述第一密文所在的升级包)的信息, 确定升级策略。其中, 第一终端的信息包含第一终端的身份标识(identification, ID)、型号、版本信息、分组信息、地址等等中的一项或者多项。第一密文的信息包含第一密文的元数据(或者说属性), 例如所述第一密文的版本、文件大小、存储地址等等中的一项或者多项。第一密文所在的升级包的信息包含升级包的文件大小、存储地址、升级包中一项或者多项数据的依赖关系等等中的一项或者多项。

例如, OTA 服务器根据第一终端中的目标零部件的版本信息以及第一密文的版本信息, 确定第一终端上的目标零部件需要升级, 进而根据第一密文的存储地址确定第一下载地址。再如, OTA 服务器根据第一密文所在的升级包中的多项升级数据的依赖关系, 确定第一终端中的下载多项升级数据的下载次序。再如, OTA 服务器根据第一密文的文件大小, 确定所述第一终端需要的存储空间大小。

可以理解的, 在实际的处理过程中, OTA 服务器可以确定升级策略, 也可以不确定升级策略, 例如, OTA 服务器可以将第一密文(或者第一密文所在的升级包)的元数据发送给第一终端, 由第一终端确定下载策略。具体情况取决于 OTA 服务器的实现、预先的约定或者标准的定义。

步骤 S304: OTA 服务器向第一终端发送第一下载地址。

其中, 第一下载地址可以用于第一终端从存储该第一密文的设备(例如, OTA 服务器、或者多个服务器中的 CDN 服务器、或者 NAS 设备、又或者分布式数据库等)中下载该第一密文。

可选的, 在第一下载地址包含在升级策略中的情况下, OTA 服务器可以向第一终端发送升级策略, 相应的, 第一终端就接收到来自 OTA 服务器的升级策略, 从而获取第一下载地址。

进一步的可选的, OTA 服务器具体可以向目标零部件发送升级策略, 相应的, 目标零部件则接收来自 OTA 升级主节点的升级策略, 从而获取第一下载地址。

可替代的, OTA 服务器具体可以向第一终端中的升级控制部件发送升级策略(没有确定升级策略的情况下也可以是发送第一下载地址)。进一步的, 第一终端中的升级控制部件可以将升级策略转发给第一终端中的目标零部件。例如, 参见图 2, 升级控制部件可以是 GW, 目标零部件可以为 MDC, OTA 服务器可以向车辆 203 中的 GW 发送升级策略, GW 接收升级策略, 并将升级策略转发给 MDC, 以便于 MDC 按照升级策略进行升级。

在一种可能的设计中, 升级控制部件也可以是其他用于控制车辆的部件组中的待升级部件进行升级的部件。请参见图 4, 图 4 是本申请实施例提供的一种可能的车辆的架构, 车辆 40 存在多个部件组, 每个部件组中包括一个用于升级控制部件组内的待升级部件进行 OTA 升级的升级控制部件。例如, 可以将一个整车集成单元(vehicle integrated/integration unit, VIU)及其连接的部件作为一个部件组, 将 VIU 作为一个部件组的升级控制部件。本申请例举一个可能的部件组 group1: VIU1、座舱域控制器(cockpit domain controller, CDC)、ECU1.1、ECU1.2、ECU2.1、ECU2.2、Tbox, 其中 VIU1 为该部件组 group1 的升级控制部件。若目标零部件为 CDC, 则 OTA 服务器可以将第一下载地址发送给 VIU1, 相应的, VIU1 接收来自 OTA 服务器的第一下载地址。需要说明的是, 当部件组内仅包括一个部件时, 该

部件可以既是该部件组的升级控制部件，也是该部件组的待升级部件。此处的部件组仅为示例，具体的部件组分组情况取决于具体的实现。

步骤 S305：第一终端获取第一密文。

本申请例举两种可能的第一终端获取第一密文的可能情况：

情况一：OTA 服务器向第一终端发送第一密文，相应的，第一终端则接收来自 OTA 服务器的第一密文。具体的，OTA 服务器可以通过有线链路、无线链路等向第一终端发送第一密文。

情况二：第一终端可以通过第一下载地址，从存储第一密文的设备（例如，OTA 服务器、或者多个服务器中的 CDN 服务器、或者 NAS 设备、又或者分布式数据库等）下载第一密文。

进一步的可选的，第一终端可以通过安全通道下载第一密文。其中，安全通道可以是基于安全套接字(Secure Sockets Layer, SSL)协议或者传输层安全(Transport Layer Security, TLS)协议的传输通道，用于数据安全传输。具体的，安全通道可以包括超文本传输安全协议 HTTPs 安全通道、传输层安全协议 TLS 安全通道或数据包传输层安全协议(Datagram Transport Layer Security, DTLS)安全通道等等中的一个或者多个。

可选的，第一终端与存储第一密文的设备建立安全通道时，可能需要执行相关安全配置，以便于安全的传输信息。例如，第一终端与存储第一密文的设备可以通过证书确认对方的身份、确定进行加解密的公私钥对等等中的一项或者多项。

可选的，OTA 服务器（或者其他存储第一密文的设备）对第一密文的内容不进行修改或审核，可以看作 OTA 服务器（或者其他存储第一密文的设备）通过透传方式，将第一密文从第一服务器处透传给第一终端。

步骤 S306：第一服务器向第一终端发送第二密钥。

具体的，第二密钥为第一密钥的解密密钥。经过第一密钥加密的密文，可以通过该第二密钥解密得到明文。第二密钥与前述第一密钥可能是相同的密钥（例如，第一密钥和第二密钥为对称密钥），也可能是不同的密钥（例如第一密钥为公钥，第二密钥为私钥）。

可以理解的，第一服务器向第一终端发送第二密钥，相应的，第一终端则接收来自第一服务器的第二密钥。该第二密钥可以用于第一终端解密第一密文，得到目标零部件的升级数据。可选的，第一服务器具体可以向第一终端中的目标零部件发送第二密钥，或者具体可以向第一终端中的升级控制部件发送第二密钥。

可选的，第一服务器可以通过各种实现方式向第一终端发送第二密钥，本实施例例举两种可能的实现方式：

实现方式一：第一服务器与第一终端建立安全通道，第一服务器通过安全通道向第一终端发送第二密钥。具体的，安全通道包括 HTTPs 安全通道、TLS 安全通道或 DTLS 安全通道等等中的一个或者多个，用于安全数据传输。可选的，第一服务器可以通过 OTA 服务器向第一终端分发用于获取第二密钥的地址，第一终端根据该第二密钥的地址，可以与第一服务器建立安全通道。

进一步可选的，第一终端与第一服务器建立通道时，可能需要执行相关安全配置，以便于安全的传输信息。例如，第一终端与第一服务器可以通过证书确认对方的身份、确定

进行加解密的公私钥对等等。

可选的，在实际的处理过程中，第一服务器还可以通过其他支持加密的通信链路向第一终端发送数据，而无需通过安全通道传输数据。具体可以取决于第一服务器与第一终端的实现、预先的约定或者标准的定义。

需要说明的是，本申请实施例中提到的安全通道具体可以为一段安全通道，也可以为多段安全通道。例如，在第一终端中的目标零部件支持与第一服务器进行通信的情况下，目标零部件可以直接与第一服务器建立安全通道，因此目标零部件可以通过安全通道接收第一服务器发送的第二密钥。在一些具体实施场景中，若目标零部件不支持与第一服务器直接建立安全通道，但是支持与第一终端中的升级控制部件建立安全通道。该控制部件可以与第一服务器建立第一段安全通道，与目标零部件建立第二段安全通道，从而使得目标零部件可以通过第一段安全通道和第二段安全通道，与第一服务器进行通信。

实现方式二：第一服务器通过第一安全参数加密第二密钥，得到第二密文。第一服务器向第一终端发送第二密文。进一步的，第一终端使用第二安全参数解密第二密文，得到第二密钥。具体的，第二安全参数可以用于解密经过第一安全参数加密得到的密文。第一安全参数与第二安全参数可以是相同的参数也可以是不同的参数。可选的，第一安全参数可以是公钥、或者对称密钥或者第一服务器与第一终端协商得到的共享密钥。例如，第一终端（具体可以为第一终端中的目标零部件或者第一终端中的升级控制部件等）可以确定一个私钥对，该公私钥对包含第一公钥和第一私钥，该第一公钥可以发送给第一服务器作为第一安全参数，而第一私钥作为第二安全参数。

可选的，第一安全参数（以及第二安全参数）可以属于临时密钥或者一次性密钥（one time key）。其中，一次性密钥可以理解为只使用一次或者使用一次后即失效或被删除的密钥。例如，第一服务器使用第一安全参数加密第二密钥后，则将第一安全参数删除；第一终端使用第二安全参数解密第二密文后，可以将该第二安全参数删除。这样一来，只使用一次第一安全参数进行加密以及只使用一次第二安全参数进行解密，从而使得该第一安全参数和第二安全参数不容易被攻破，提高数据安全性。

可选的，为了提高安全性，第一服务器加密第二密钥时，可以使用一次一密的形式。也即是说，第一服务器向不同的终端发送第二密钥时，对第二密钥进行加密的安全参数是不同的。

进一步可选的，该第一安全参数（以及后续用于解密第二密文的第二安全参数）可以是第一服务器与第一终端通过协商确定的，为了方便理解，本申请例举两种可能的确定第一安全参数的设计：

设计1：第一终端确定一个公私钥（包含第一公钥和第一私钥），第一终端的第一数字证书可以用于认证第一公钥来源于第一终端。具体的，第一终端可以将第一公钥发送给第一服务器，第一服务器通过第一数字证书认证第一公钥。该第一公钥即作为第一安全参数，用于加密第二密钥。可选的，确定上述公私钥对的具体可以为第一终端中的目标零部件或者升级控制部件等，上述第一数字证书具体可以为第一终端中的目标零部件或者升级控制部件的数字证书。

在一种可能的实施场景中，第一数字证书对应第二公钥和第二私钥。例如，CA可以为

第一终端的第二公钥作公证，将第二公钥和第一终端的信息等封装得到第一数字证书。其他设备（例如第一服务器）可以通过第一数字证书和 CA 确定第二公钥确实来自第一终端。从而使得其他设备（例如第一服务器）通过第一数字证书对应的第二公钥和第二私钥可以认证第一公钥。请参见图 5，图 5 是本申请实施例提供的一种确定第一安全参数（以及第二安全参数）的方法流程图，具体可以包括以下步骤：

步骤 S511：第一终端确定第一公钥（PK1）和第一私钥（SK1）。

可选的，具体可以为第一终端中的目标零部件确定第一公钥和第二私钥，也可以为第一终端中的升级控制部件确定第一公钥和第一私钥。

步骤 S512：第一终端根据第一数字证书对应的第二私钥、第一公钥和第一随机数，得到第一签名。

例如，得到的第一签名 S1 满足如下式子： $S1 = \text{sign}(SK2, PK1, \text{NONCE1})$ ，其中，sign 为签名算法，SK2 为第一数字证书对应的第二私钥，PK1 为第一公钥，NONCE1 为第一随机数（可选的）。

步骤 S513：第一终端向第一服务器发送第一公钥、第一随机数和第一签名。

需要说明的是，第一终端可以在同一条消息中携带第一公钥、第一随机数和第一签名，也可以在多条消息中分别携带第一公钥、第一随机数和第一签名。

第一终端向第一服务器发送第一公钥、第一随机数和第一签名，相应的，第一服务器则接收来自第一终端的第一公钥、第一随机数和第一签名。

步骤 S514：第一服务器根据第一数字证书对应的第二公钥认证第一公钥。

其中，第一数字证书可以是第一终端发送给第一服务器的，也可以是第一服务器中预先配置的，还可以是第一服务器从第三方设备（例如网络侧设备、CA 中心等）获取的。

具体的，第一服务器可以根据第一数字证书对应的第二公钥解签第一签名，将解签后的结果与第一公钥比对，若比对一致则认证第一公钥通过。进一步的，若对比一致，则说明第一公钥确实来源于第一终端，没有被篡改。若比对不一致，则说明第一服务器收到第一公钥可能被篡改或者来源不可信。

可选的，第一服务器可以获取有第二数字证书。第二数字证书可以用于认证第一服务器的身份。例如，第二数字证书可以对应第三公钥和第四公钥。图 5 所示的方法还可以包括如下步骤：

步骤 S515：第一服务器根据第二数字证书对应的第三私钥、第一随机数和第二随机数，得到第二签名。

例如，得到的第二签名 S2 满足如下式子： $S2 = \text{sign}(SK3, \text{NONCE1}, \text{NONCE2})$ ，其中，sign 用于指示签名算法，SK3 为第三数字证书对应的第三私钥，NONCE1 为第一随机数（可选的），NONCE2 为第二随机数（可选的）。

步骤 S516：第一服务器向第一终端发送第二随机数和第二签名。

需要说明的是，第一服务器可以在同一条消息中携带第二随机数（NONCE2）和第二签名（S2），也可以在多条消息中分别携带第二随机数和第二签名。

可选的，第一服务器可以在发送第二签名的消息中携带第二密文（C2）。进一步的可选的，第一服务器还可以根据第二签名、第二密文、第二随机数得到第三签名（S3），该第三

签名用于第一终端验证第二密文。例如,第三签名 $S3$ 满足: $S3 = \text{Sign}(SK3, S2 || C2 || \text{NONCE2})$, 其中“||”可以为字符串连接符号,各项参数的含义可以参考前述的描述。

步骤 S517: 第一终端根据第二数字证书认证第一服务器的身份。

具体的,第一终端可以根据第二数字证书对应的第三公钥解签第二签名,将解签后的结果与第一随机数、第二随机数比对,若比对一致则认证第一服务器的身份通过。

可选的,在包含第三签名时,还可以根据第二数字证书对应的第三公钥解签第三签名。

可选的,若认证第一服务器的身份通过,第一终端可以向第一服务器反馈确认字符(acknowledge character, ACK)或其他确认指示信息。可选的,该 ACK 或其他确认指示信息可以使用第二私钥进行签名。

进一步的,若比对不一致,则说明第一随机数、第二随机数、或者第二密文已经被篡改或者来源不可信。

设计 2: 第一服务器与第一终端通过密钥协商算法确定共享密钥,该共享密钥作为第一安全参数(第二安全参数)。

进一步的,在确定共享密钥的过程中,第一服务器可以通过与第一终端之间的预共享密钥(pre-shared key, PSK)确定对方的身份。其中,PSK 是第一服务器与第一终端之间共享的一个秘密值。第一服务器与第一终端可以通过预先定义、预先配置或者通过互相协商生成等方式得到 PSK。

请参见图 6,图 6 是本申请实施例提供的又一种确定第一安全参数(以及第二安全参数)的方法流程图,具体可以包括以下步骤:

步骤 S6201: 第一终端基于密钥协商算法,确定第一密钥协商参数。

其中,密钥协商算法为第一终端与第一服务器预先约定的密钥协商算法,或者,第一服务器可以通过 OTA 服务器向第一终端转发其支持的密钥协商算法的标识,用于第一终端选择使用何种密钥协商算法。

例如,以密钥协商算法为 DH 算法为例,第一终端与第一服务器可以将较大的素数 p 和随机数 g 作为公钥,第一终端根据自己的私钥(a)和公钥(p 和 g)确定计算值 A (例如: $A = g^a \bmod p$),该计算值 A 可以看做第一密钥协商参数。

再如,以密钥协商算法为 ECDH 算法、以确定的椭圆曲线为 E_p 、基点为 G 为例,第一终端根据自己的私钥(a)和基点 G 得到计算值 A (例如: $A = a \times G$)发送给第一服务器,则该计算值 A 可以看做第一密钥协商参数。

步骤 S6202: 第一终端向第一服务器发送第一密钥协商参数。

具体的,第一终端可以向第一服务器发送第一消息,第一消息中包含第一密钥协商参数。可选的,第一消息中还可以包括第一终端确定的第一新鲜性参数(NONCE1)、第一终端的 ID 等等。

第一终端向第一服务器发送第一密钥协商参数,相应的,第一服务器则接收来自第一终端的第一密钥协商参数。

步骤 S6203: 第一服务器基于密钥协商算法,得到共享密钥(第一安全参数)。

例如,以 DH 算法为例,共享密钥可以满足: $K_{dh} = K_{Ee}^b \bmod p$,其中, K_{Ee} 为第一密钥协商参数(例如,满足: $K_{Ee} = g^a \bmod p$), p 为 DH 密钥交换过程中的公钥。

例如，以 ECDH 算法为例，共享密钥可以满足： $K_{dh} = b \times K_{Ee}$ ，其中， K_{Ee} 为第一密钥协商参数（例如，满足： $K_{Ee} = a \times G$ ）， G 为椭圆曲线的基点。

可选的，第一服务器可以根据共享密钥 K_{dh} 进行推演，推演出的密钥也可以为共享密钥。例如，共享密钥 K_{gt} 可以满足： $K_{gt} = KDF(K_{dh}, NONCE1, NOCNE2)$ 。其中， $NONCE1$ 为第一新鲜性参数， $NOCNE2$ 为第二新鲜性参数。该共享密钥或者通过共享密钥派生得到的其他密钥可以作为前述第一安全参数。

进一步的可选的，第一服务器可以基于共享密钥推演得到加密密钥、身份认证密钥、完整性保护密钥中的一个或者多个。例如，第一服务器确定的加密密钥 K_{enc} 可以满足：

$$K_{enc} = KDF(K_{dh}, NONCE1, NOCNE2, "enc")$$

其中，“enc”为一种可选的密钥标识，具体实施时可以预先配置或者协议规定一段字符串作为密钥标识， $NONCE1$ 为第一新鲜性参数， $NOCNE2$ 为第二新鲜性参数。 $NONCE1$ ， $NOCNE2$ ，“enc”为可选参数，具体实施时还可以包括其他可选参数，例如第一终端的 ID、第一服务器的 ID 等等。再如，第一服务器确定的完整性保护密钥 K_{int} 可以满足：

$$K_{enc} = KDF(K_{dh}, NONCE1, NOCNE2, "int")$$

其中，“int”为一种可选的密钥标识，具体实施时可以预先配置或者协议规定一段字符串作为密钥标识。 $NONCE1$ ， $NOCNE2$ ，“enc”为可选参数，具体实施时还可以包括其他可选参数，例如第一终端的 ID、第一服务器的 ID 等等。该完整性保护密钥进一步可以用于生成消息认证码 MAC，用于保护消息的完整性。

步骤 S6204：第一服务器确定第二密钥协商参数。

例如，以密钥协商算法为 DH 算法为例，第一服务器根据自己的私钥（b）和公钥（p 和 g）确定计算值 B，该计算值 B 可以看做第二密钥协商参数。

再如，以密钥协商算法为 ECDH 算法、以确定的椭圆曲线为 E_p 、基点为 G 为例，第一服务器根据自己的私钥（b）和基点 G 得到计算值 B（例如： $B=b \times G$ ）发送给第一终端，则该计算值 B 可以看做第二密钥协商参数。

可选的，还包括步骤 S6205：第一服务器根据第一服务器与第一终端的 PSK 确定第一认证参数。

可选的，第一认证参数 AUTH1 可以满足如下式子： $AUTH1 = (PSK, NONCE2, \text{第一消息})$ 。进一步的，参与生成第一认证参数的数据还可以有共享密钥、第一终端的 ID、第二终端的 ID、第二消息等等中的一项或者多项。

步骤 S6206：第一服务器向第一终端发送第二密钥协商参数。

具体的，第一终端向第一服务器发送第一密钥协商参数，相应的，第一服务器则接收来自第一终端的第一密钥协商参数。

可选的，第一服务器可以向第一终端发送第二消息，该第二消息中即包含第二密钥协商参数。可选的，第二消息中还可以包括第一服务器确定的第二新鲜性参数（ $NONCE2$ ）、第一身份认证信息 AUTH1、第一消息认证码 MAC1、第一服务器的身份标识（identification，ID）等等。其中，第一消息认证码 MAC1 为根据第二消息的部分或者全部数据，通过完整性保护算法（或者还包括完整性保护密钥）得到的 MAC，用于保护第二消息的完整性。

步骤 S6207：第一终端基于密钥协商算法，根据第二密钥协商参数确定共享密钥（第

二安全参数)。

具体描述可以参考步骤 S6203 中第一服务器侧的详细描述。

步骤 S6208: 第一终端根据第一服务器与第一终端的 PSK, 校验第一认证参数。

在一种可选的方案中, 根据协议规定, 第一服务器使用什么参数生成第一认证参数, 则第一终端也应当使用相同的参数生成校验信息, 如果校验信息与第一认证参数相同, 则认为验证通过。

例如, 若第一认证参数 AUTH1 满足: $AUTH1 = KDF(PSK, NONCE2, \text{第一消息})$, 则第一终端根据 PSK, 则第二节点生成校验信息 $check1 = KDF(PSK, NONCE2, \text{第一消息})$, 若校验信息 check1 与 AUTH1 相同, 则第一认证参数校验通过。进一步的, 若第一认证参数校验通过, 说明第一服务器中的 PSK 与第一终端中的 PSK 一致 (第一服务器的身份可信), 且第一消息、第二随机数没有被篡改。

步骤 S6209: 第一终端根据 PSK 确定第二认证参数。

可选的, 第二认证参数 AUTH2 可以满足如下式子: $AUTH2 = (PSK, NONCE1, \text{第二消息})$ 。进一步的, 参与生成第一认证参数的数据还可以有共享密钥、第一终端的 ID、第二终端的 ID、第二消息等等中的一项或者多项。

步骤 S6210: 第一终端向第一服务器发送第二认证参数。

可选的, 第一服务器可以向第一终端发送第三消息, 该第三消息中即包含第二认证参数。可选的, 第三消息中还可以包括第一服务器确定的第二消息认证码 MAC2 等等。其中, 第二消息认证码 MAC2 用于保护第三消息的完整性。

可选的, 该第二认证参数或者第三消息还可以通过加密密钥进行加密。

步骤 S6211: 第一服务器根据 PSK, 校验第一认证参数。

具体描述可以参考步骤 S6208 中第一终端侧的详细描述。

可选的, 第一服务器向第一终端发送第二密钥之前, 可以接收来自第一终端的密钥获取请求 (具体可以是请求消息、指示请求第二密钥的信息, 本申请对信息的名称不作限定)。进一步的, 第一服务器响应于该密钥获取请求, 向第一终端发送第二密钥或者向第二终端发送第二密文。在一种可能的设计中, 第一服务器接收来自第一终端的密钥获取请求, 从而通过密钥协商算法得到第一安全参数 (第二安全参数)。第一服务器根据第一安全参数加密第二密钥得到第二密文, 向第一终端发送第二密文。

步骤 S307: 第一终端通过第二密钥解密第一密文, 得到目标零部件的升级数据。

可选的, 第一终端可以通过解密算法, 通过第二密钥对第一密文进行解密, 得到升级数据。例如, 得到的升级数据的过程满足如下式子: $\text{升级数据} = \text{Dec}(\text{升级数据}, \text{第二密钥})$, 其中, Dec 为加密算法 Enc 对应的解密算法 (通常来说, 加密算法与解密算法为同一种算法, 或者具体可以为算法中的不同计算流程, 此处为了便于描述使用不同的名称)。

可选的, 第一服务器可以通过 OTA 服务器在升级策略中指示使用的加密算法, 从而使第一终端使用对应的解密算法进行解密。可替换的, 第一服务器可以在发送第二密钥时发送指示信息, 用于指示使用的加密算法, 从而使第一终端使用对应的解密算法进行解密。

步骤 S308: 第一终端通过所述目标零部件的升级数据, 升级所述目标零部件。

在具体实施过程中，具体可以为第一终端中的升级控制部件或者目标零部件对第一密文进行解密，然后通过升级控制部件或者目标零部件根据升级数据进行升级。本申请例举几种可能的实施情况：

情况一：第一终端中的升级控制部件接收 OTA 服务器发送的第一密文，该升级控制部件将第一密文转发给第一终端中的目标零部件。第一终端中的升级控制部件接收第一服务器发送的第二密钥，该升级控制部件将第二密钥转发给第一终端中的目标零部件。目标零部件根据第二密钥解密第一密文，得到升级数据。目标零部件根据升级数据，对自身进行升级。可以理解的，目标零部件自身可能不具备与 OTA 服务器或者与第一服务器进行数据传输的能力，因此可以通过升级控制部件转发第一密文和第二密钥，解密第一密文后使用升级数据进行升级。

情况二：第一终端中的升级控制部件接收 OTA 服务器发送的第一密文。该升级控制部件接收第一服务器发送的第二密钥。该升级控制部件根据第二密钥解密第一密文，得到升级数据，根据升级数据对目标零部件进行升级。可以理解的，目标零部件自身可能不具备解密能力，因此可以通过升级控制部件解密得到升级数据。可选的，升级时，升级控制部件可以通过数据刷写等方式，对目标零部件进行升级。

情况三：第一终端中的目标零部件接收 OTA 服务器发送的第一密文，该目标零部件接收第一服务器发送的第二密钥。该目标零部件根据第二密钥解密第一密文，得到升级数据。该目标零部件根据升级数据，对目标零部件进行升级。可以理解的，目标零部件在具有外部通信能力和解密能力的条件下，可以使用情况三中描述的方法进行升级。例如，参见图 4，目标零部件可以为车辆中的 VIU，该 VIU 可以与 OTA 服务器和第一服务器进行数据传输，因此 VIU 可以通过情况三中描述的方法进行升级。

请参见图 7，图 7 是本申请实施例提供的一种可能的 OTA 升级方法的运行示意图，可以看出，第一服务器 701 将目标零部件的升级数据通过第一密钥加密得到第一密文，将第一密文通过 OTA 服务器 702 透传给第一终端 703（具体可以是目标零部件 704 或者升级控制部件 705）。然后将第二密钥发送给第一终端 703（具体可以是目标零部件 704 或者升级控制部件 705）。其中，发送第二密钥时，具体可以是通过安全通道发送（如图中①所在的线条所示），也可以是将第二密钥使用第一安全参数加密后，将得到的第二密文发送给第一终端（如图中②所在的线条所示，后续第一终端 703 使用第二安全参数解密第二密文得到第二密钥）。

可以看出，在图 3 所示的实施例中，由于目标零部件的升级数据是经过加密传输的，只有第一服务器、第一终端可以通过第二密钥得到升级数据，避免了其他中间设备获取升级数据，提高了升级数据的机密性。当升级数据中包含核心代码、关键技术实现的情况下，可以有效保护涉密数据、关键代码等核心资产。

进一步的，由于升级数据是经过加密的，可以避免攻击者篡改升级数据，提高了 OTA 升级的安全性。

请参见图 8，图 8 是本申请实施例提供的又一种 OTA 升级方法的流程示意图，该方法包括但不限于如下步骤：

步骤 S801：第一服务器向 OTA 服务器发送目标零部件的升级数据的元数据。

其中，元数据，又称中介数据、中继数据，为描述数据的数据（data about data），主要是描述数据属性（property）的信息。目标零部件的升级数据的表头可以包含升级数据的第一下载地址、版本信息、文件大小、存储位置、提供升级数据的设备的标识、目标零部件的标识等等中的一项或者多项。

进一步的，该元数据可以用于 OTA 服务器确定升级策略等。

第一服务器以及目标零部件的相关描述可以参考步骤 S301 中的相关说明，此处不再赘述。

可选的，图 8 所示的实施例可以包括步骤 S802-步骤 S803，具体如下：

步骤 S802：OTA 服务器确定升级策略。

具体的，该升级策略中可以包含第一密文的第一下载地址。相关描述可以参考步骤 S303 中的详细描述，此处不再赘述。

步骤 S803：OTA 服务器向第一终端发送升级策略。

具体的，OTA 服务器向第一终端发送升级策略，相应的，第一终端就接收到来自 OTA 服务器的升级策略。相关描述可以参考步骤 S304 中的详细描述，此处不再赘述。

步骤 S804：第一服务器向第一终端发送目标零部件的升级数据。

具体的，第一服务器向第一终端发送目标零部件的升级数据，相应的，第一终端则接收第一服务器发送的目标零部件的升级数据。具体的，第一服务器可以通过有线链路、无线链路等向第一终端发送目标零部件的升级数据。可以理解的，该第一服务器可以通过 CDN 向第一终端发送目标零部件的升级数据。

进一步的，第一终端可以获取目标零部件的升级数据的第一下载地址，该第一下载地址用于第一终端从第一服务器上接收升级数据。

具体的，第一终端可以通目标零部件的升级数据的下载地址，与第一服务器建立安全通道。第一服务器通过该安全通道向第一终端发送目标零部件的升级数据，相应的，第一终端通过安全通道接收目标零部件的升级数据。其中，安全通道可以包括超文本传输安全协议 HTTPS 安全通道、传输层安全协议 TLS 安全通道或数据包传输层安全性协议 DTLS 安全通道等等中的一个或者多个，用于数据安全传输。

步骤 S805：第一终端通过所述目标零部件的升级数据，升级所述目标零部件。

具体可以参考步骤 S308 中的相关描述，此处不再赘述。

请参见图 9，图 9 是本申请实施例提供的又一种可能的 OTA 升级方法的运行示意图，可以看出，第一服务器 901 向 OTA 服务器 902 发送目标零部件的升级数据的元数据，OTA 服务器 902 向第一终端 903（具体可以是目标零部件 904 或者升级控制部件 905）发送第一下载地址。第一终端 903（具体可以是目标零部件 904 或者升级控制部件 905）通过第一下载地址从第一服务器处下载目标零部件 904 的升级数据，从而对目标零部件 904 进行升级。

可以看出，在图 8 所示的方法中，第一终端通过第一下载地址从第一服务器下载升级数据，从而避免了其他中间设备（例如 OTA 服务器）获取目标零部件的升级数据，保证了升级数据的机密性。当升级数据中包含核心代码、关键技术实现的情况下，可以有效保护涉密数据、关键代码等核心资产。

进一步的，由于目标零部件的升级数据是在第一服务器直接获取的，因此避免了中间设备等转存、或者审核等操作，减少了升级流程的复杂度，提高了升级效率。通过本申请实施例还可以满足某一些需要快速升级的零部件的需求。

请参见图 10，图 10 申请实施例提供的又一种 OTA 升级方法的流程示意图，方法包括但不限于如下步骤：

步骤 S1001：第一服务器根据第一密钥对目标零部件的升级数据进行加密得到第一密文。

具体可以参考步骤 S301 中的相关描述，此处不再赘述。

步骤 S1002：第一服务器通过第一安全参数加密第二密钥得到第二密文。

其中，第一安全参数为第一服务器与第一终端（或者具体为第一终端中的第一目标零部件或者升级控制部件）之间的共享密钥或者为第一终端（或者具体为第一终端中的第一目标零部件或者升级控制部件）的第一公钥。其中，第一目标零部件为目标零部件中的一个。

可选的，第一安全参数可以在是第一服务器中预置的。例如，第一目标零部件中预先配置有第一私钥（或者还包含第一私钥的第一公钥），第一服务器可以预先配置有第一公钥，第一服务器通过该第一公钥加密第二密钥，得到第二密文。后续第一目标零部件可以通过预先配置的第一私钥解密第二密文。

可替代的，第一安全参数还可以是第一服务器与第一终端通过协商的方式预先确定的。例如，第一服务器与第一终端通过图 5 或者图 6 所示的方式确定第一安全参数（第二安全参数）。

第二密钥为第一密钥的解密密钥，经过第一密钥加密的密文，可以使用第二密钥解密得到明文。第一密钥与第二密钥可能是不同的密钥（非对称密钥），也可以是同一个密钥（对称密钥），具体取决于加密第一密文时使用的算法的类型。

可选的，考虑一种可能的情况，第二终端上配置有第二目标零部件，该第二目标零部件可以为目标零部件中的其中一个。第一服务器可以通过第三安全参数加密所述目标零部件的升级数据得到第三密文，该第三密文用于该第二终端升级该第二目标零部件。其中，第三安全参数可以为第一服务器与第二终端（或者具体为第二终端中的目标零部件）之间的共享密钥，或者为第二终端（或者具体为第二终端中的目标零部件）的第四公钥。

需要说明的是，第三安全参数一般与第一安全参数不同，但是在一些实施情况中，第三安全参数与第一安全参数也可以是相同的。例如，供应商在生产目标零部件时，在某一批次的目标零部件（包含第一目标零部件和第二目标零部件）中预先配置了相同的共享密钥或者预先配置了相同的私钥，从而使得加密第二密钥时使用的第三安全参数与第一安全参数是相同的。

步骤 S1003：第一服务器向 OTA 服务器发送第一密文、第二密文。

需要说明的是，第一服务器可以在同一条消息中携带第一密文和第二密文，也可以在多条消息中分别携带第一密文和第二密文。此处为了便于描述故写作一个动作，并不旨在限定一定是在同一条消息中发送的。

可选的，考虑前述的第二终端配置有第二目标零部件的情况，第一服务器还可以 OTA 服务器发送第三密文。

可选的，第一服务器还可以向 OTA 服务器发送第二密文对应的第一终端的指示信息（或者具体为第一终端上的第一目标零部件的指示信息），便于第一服务器将第二密文发送给第一终端。

可选的，图 10 所示的实施例可以包括步骤 S1004-步骤 S105 中的一个或者多个步骤，步骤 S1004-步骤 S1005 具体如下：

步骤 S1004：OTA 服务器确定升级策略，升级策略中包含第一密文和第二密文的第一下载地址。

具体地，第一下载地址用于下载第一密文或者下载包含第一密文的升级包，还可以用于下载第二密文。可选的，第一下载地址可以为统一资源定位符（uniform resource locator, URL）。

可选的，第一下载地址具体可以包含两个地址，其中一个地址用于下载第一密文（或者下载包含第一密文的升级包），另一个地址用于下载第二密文。

关于升级策略的详细描述可以参考步骤 S303 中的详细描述，此处不再赘述。

可选的，考虑前述的第二终端配置有第二目标零部件的情况，OTA 服务器可以根据第二终端中的第二零部件的版本信息，确定第二零部件需要升级。OTA 服务器则向第二终端发送第一密文的下载地址以及第三密文的下载地址。

其他更多内容可以参考步骤 S303 中相关描述，此处不再赘述。

步骤 S1005：OTA 服务器向第一终端发送第一下载地址。

其中，第一下载地址可以用于第一终端从存储该第一密文（第二密文）的设备（例如，OTA 服务器、或者多个服务器中的 CDN 服务器、或者 NAS 设备、又或者分布式数据库等）中下载该第一密文（第二密文）。

可选的，考虑前述的第二终端上配置有第二目标零部件的情况，OTA 服务器还可以向第三终端发送第三密文的第一下载地址，该第二下载地址用于第二终端下载第三密文。进一步的可选的，第一密文的下载地址可以与第一密文的下载地址相同。

步骤 S1006：第一终端获取第一密文和第二密文。

本申请例举两种可能的第一终端获取第一密文和第二密文的情况：

情况一：OTA 服务器向第一终端发送第一密文和第二密文，相应的，第一终端则接收来自 OTA 服务器的第一密文和第二密文。具体的，第一终端可以通过有线链路、无线链路等接收第一服务器发送的第一密文和第二密文。可选的，第一密文和第二密文可以是在同一条消息中携带的，也可以是通过不同的消息分别携带的。

情况二：第一终端可以通过第一下载地址，从存储第一密文的设备（例如，OTA 服务器、或者多个服务器中的 CDN 服务器、或者 NAS 设备、又或者分布式数据库等）下载第一密文和第二密文。

进一步的可选的，第一终端可以通过安全通道下载第一密文（第二密文）。可选的，第一终端与存储第一密文（第二密文）的设备建立安全通道时，可能需要执行相关安全配置，以便于安全的传输信息。

需要说明的是，OTA 服务器（或者其他存储第一密文的设备）对第一密文的内容不进行修改或审核，可以看作 OTA 服务器（或者其他存储第一密文的设备）通过透传方式，将第一密文（第二密文）从第一服务器处透传给第一终端。

具体的描述还可以参考步骤 S306 中的描述，此处不再赘述。

步骤 S1007：第一终端通过第二安全参数解密第二密文，得到第二密钥。

其中，第二安全参数可以解密经过第一安全参数加密的密文。可选的，该第二安全参数与第二安全参数可以是相同的（例如共享密钥），也可以是不同的（例如第一安全参数为公钥，第二安全参数为私钥）。

第一终端可以通过解密算法，通过第二安全参数对第二密文进行解密，得到第二密钥。

步骤 S1008：第一终端通过第二密钥解密第一密文，得到第一目标零部件的升级数据。

具体可以参见步骤 S307 中的相关描述，此处不再赘述。

步骤 S1009：第一终端通过第一目标零部件的升级数据，升级第一目标零部件。

具体可以参见步骤 S308 中的相关描述，此处不再赘述。

可以理解的，可选的，考虑前述的第二终端上配置有第二目标零部件的情况，第三终端可以获取第一密文和第三密文，使用第四安全参数解密第三密文，得到第二密钥。通过第二密钥解密第一密文，得到第二目标零部件的升级数据。

例如，请参见图 11，图 11 是本申请实施例提供的又一种可能的 OTA 升级系统的运行示意图，第一服务器 1101 根据第一密钥加密目标零部件（包含第一目标零部件 1104 和第二目标零部件 1107）的升级数据，得到第一密文。第一服务器 1101 使用第一安全参数加密第二密钥得到第二密文，使用第三安全参数加密第二密钥得到第三密文。第一服务器 1101 向 OTA 服务器 1102 发送第一密文、第二密文（如图中①所在的线条所示）、第三密文（如图中②所在的线条所示）。OTA 服务器 1101 将第一密文发送给第一终端 1103（具体可以是第一目标零部件 1104 或者第一升级控制部件 1105）和第二终端 1106（具体可以是第二目标零部件 1107 或者第二升级控制部件 1108）。OTA 服务器 1101 将第二密文发送给第一终端 1103，以便于第一终端 1103 使用第二安全参数解密第二密文，得到第二密钥。OTA 服务器将第三密文发送给第二终端 1106，以便于第二终端 1106 使用第四安全参数解密第三密文，得到第二密钥。该第二密钥可以用于第一终端和第二终端解密第一密文，以得到升级目标零部件的升级数据。

可以看出，在图 10 所示的方法中，由于没有获取第二安全参数则无法解密第二密文得到第二密钥，从而无法解密第一密文得到目标零部件的升级数据，因此保证了目标零部件的升级数据的安全性。

进一步的，由于没有直接对目标零部件的升级数据进行加密，而是使用第一安全参数加密第二密钥，而密钥的数据大小通常小于升级数据的数据大小。因此，对于存在有多个、多种零部件需要升级的供应商来说，考虑多个零部件的安全参数可能不同的情况，相比于直接使用安全参数加密升级数据，本实施例可以显著减少加密过程中的计算量、存储量，提高升级的效率。

请参见图 12，图 12 是本申请实施例提供的又一种 OTA 升级方法的流程示意图，该方

法包括但不限于如下步骤：

步骤 S1201：第一服务器使用第一安全参数对目标零部件的升级数据进行加密得到第一密文。

其中，第一安全参数为第一服务器与第一终端（或者具体为第一终端中的目标零部件）之间的共享密钥或者为第一终端（或者具体为第一终端中的目标零部件）的第一公钥。可选的，第一安全参数可以为第一服务器中预先配置、预先定义或者通过协商的方式生成的。

例如，供应商在生产目标零部件时在目标零部件中配置了与第一服务器之间的共享密钥（第一安全参数），第一服务器在发送升级数据时，可以使用预置的共享密钥加密目标零部件的升级数据。

再如，第一终端中预先配置有第一私钥（或者还包含第一私钥的第一公钥），第一服务器可以获取第一终端的第一公钥，第一服务器通过该第一公钥加密目标零部件的升级数据，得到第一密文。后续第一终端可以通过预先配置的第一私钥解密第一密文。

需要说明的是，为了减少计算量，同一种或者同一批次的目标零部件对应的安全参数可以是相同的。但是不同的目标零部件对应的安全参数也可以不同，具体取决于第一服务器、第一终端的实现。

目标零部件是第一终端中一个待升级的部件。第一服务器、目标零部件的升级数据等相关描述可以参见步骤 S301 中的描述，此处不再赘述。

第一服务器可以通过加密算法，根据第一安全参数对目标零部件的升级数据进行加密。例如，得到的第一密文满足如下式子：第一密文=Enc（升级数据，第一安全参数），其中，Enc 为加密算法，具体可以为 DES 算法、AES 算法等等中的一个或者多个的组合。

可选的，目标零部件可能存在多项升级数据，第一服务器可以将多项升级数据中的部分升级数据进行加密，得到第一密文。该第一密文可以与其他未加密的升级数据一同打包得到升级包，该升级包用于目标零部件的升级。这样一来，第一服务器可以只加密需要进行机密性保护的数据，减轻服务器的计算压力。

当然，第一服务器也可以将一项或者多项升级数据先打包得到升级包，然后将升级包进行加密。

步骤 S1202：第一服务器向 OTA 服务器发送第一密文。

具体可以参见步骤 S302 中的详细描述，此处不再赘述。

可选的，图 12 所示的实施例可以包括步骤 S1203-步骤 S1204 中的一个或者多个步骤，步骤 S1203-步骤 S1204 具体如下：

步骤 S1203：OTA 服务器确定升级策略，升级策略中包含第一密文的第一下载地址。

具体可以参见步骤 S303 中的详细描述，此处不再赘述。

步骤 S1204：OTA 服务器向第一终端发送第一下载地址。

具体可以参见步骤 S304 中的详细描述，此处不再赘述。

步骤 S1205：第一终端获取第一密文。

具体可以参见步骤 S305 中的详细描述，此处不再赘述。

步骤 S1206：第一终端通过第二安全参数解密第一密文，得到目标零部件的升级数据。

其中，第二安全参数可以解密经过第一安全参数加密的密文。可选的，该第二安全参

数与第二安全参数可以是相同的值（例如共享密钥），也可以是不同的值（例如第一安全参数为公钥，第二安全参数为私钥）。

可选的，第一终端可以通过解密算法，使用第二安全参数对第一密文进行解密，得到升级数据。例如，得到的升级数据的过程满足如下式子：升级数据=Dec（升级数据，第二安全参数），其中，Dec为加密算法Enc对应的解密算法（通常来说，加密算法与解密算法为同一种算法，或者具体可以为算法中的不同计算流程，此处为了便于描述使用不同的名称）。

可选的，OTA服务器可以在升级策略中指示使用的加密算法，从而使得第一终端使用对应的解密算法进行解密。可替换的，第一服务器可以在发送第二密钥时发送指示信息，用于指示使用的加密算法，从而使得第一终端使用对应的解密算法进行解密。

步骤S1207：第一终端通过目标零部件的升级数据，升级目标零部件。

具体可以参见步骤S308中的详细描述，此处不再赘述。

在图12所示的方法中，第一安全参数和第二安全参数可以是预先配置或者预先获取的，第一服务器使用第一安全参数对目标零部件的升级数据进行加密，第一终端使用第二安全参数对第一密文解密从而获取目标零部件的升级数据。由于目标零部件的升级数据是经过加密传输的，没有获取第二安全参数则无法解密第二密文得到第二密钥，从而无法解密第一密文得到目标零部件的升级数据，因此保证了升级数据的机密性。当升级数据中包含核心代码、关键技术实现的情况下，可以有效保护涉密数据、关键代码等核心资产。

上述详细阐述了本申请实施例的方法，下面提供了本申请实施例的装置。

请参见图13，图13是本申请实施例提供的一种OTA升级装置130的结构示意图，该OTA升级装置130可以包括处理单元1301、发送单元1302、接收单元中的一个或者多个。该OTA升级装置130用于实现前述的OTA方法，例如可以用于实现图3、图8、图10或者图12所示的OTA升级方法。

可以理解的，本申请各个装置实施例中，对多个单元或者模块的划分仅是一种根据功能进行的逻辑划分，不作为对装置具体的结构的限定。在具体实现中，其中部分功能模块可能被细分为更多细小的功能模块，部分功能模块也可能组合成一个功能模块，但无论这些功能模块是进行了细分还是组合，在实现OTA升级方法的过程中所执行的大致流程是相同的。例如，上述装置130中的发送单元1302、接收单元1303也可以合并为通信单元，该通信单元用于实现接收、或者发送数据的功能。通常，每个单元都对应有各自的程序代码（或者说程序指令），这些单元各自对应的程序代码在至少一个处理器上运行时，使得该单元执行相应的流程从而实现相应功能。

在一种可能的设计中，图13中所示的OTA升级装置130可以为图3所示实施例中的第一服务器，或者为第一服务器中的一个器件，例如芯片或者集成电路等。

在一种可能的实施方案中，该OTA升级装置130可以包括处理单元1301和发送单元1302，其中：

所述处理单元1301，用于根据第一密钥对目标零部件的升级数据进行加密得到第一密

文，其中，所述第一服务器为用于提供所述目标零部件的升级数据的服务器；

所述发送单元 1302，用于向 OTA 服务器发送所述第一密文；

所述发送单元 1302，还用于向部署有所述目标零部件的第一终端发送第二密钥，所述第二密钥为所述第一密钥对应的解密密钥。

可以看出，上述设计中，由于目标零部件的升级数据是经过加密传输的，只有 OTA 升级装置 130、第一终端可以通过第二密钥得到升级数据，避免了其他中间设备获取升级数据，提高了升级数据的机密性。当升级数据中包含核心代码、关键技术实现的情况下，可以有效保护涉密数据、关键代码等核心资产。

进一步的，由于升级数据是经过加密的，可以避免攻击者篡改升级数据，提高了 OTA 升级的安全性。

在又一种可能的实施方式中，上述 OTA 升级装置 130 属于目标零部件的供应商用于维护目标零部件的装置。

在又一种可能的实施方式中，所述处理单元 1301，还用于与部署有所述目标零部件的所述第一终端建立安全通道；

所述发送单元 1302，还用于通过所述安全通道向所述第一终端发送所述第二密钥。

在又一种可能的实施方式中，所述处理单元 1301，还用于根据第一安全参数加密所述第二密钥得到第二密文，所述第一安全参数为所述第一服务器与所述第一终端之间的共享密钥或者为所述第一终端的第一公钥；

所述发送单元 1302，还用于向部署有所述目标零部件的所述第一终端发送所述第二密文。

在又一种可能的实施方式中，所述装置 130 还包括：

接收单元 1303，用于接收来自所述第一终端的密钥获取请求。

在又一种可能的实施方式中，所述第一安全参数属于临时密钥或者属于一次性密钥。

在又一种可能的实施方式中，所述第一安全参数为所述第一终端的第一公钥；所述接收单元 1303，还用于接收所述第一终端发送的所述第一终端的第一公钥；

所述处理单元 1301，还用于通过所述第一终端的第一数字证书认证所述第一终端的第一公钥。

在又一种可能的实施方式中，所述第一数字证书对应第二公钥和第二私钥；所述接收单元 1303，还用于接收来自所述第一终端发送的第一签名，所述第一签名为使用所述第二私钥对所述第一公钥签名得到的；

所述处理单元 1301，还用于根据所述第二公钥、所述第一签名和所述第一公钥确定所述第一公钥认证通过。

在又一种可能的实施方式中，所述第一安全参数为所述第一服务器与所述第一终端之间的共享密钥；所述处理单元 1301，还用于：

通过密钥协商算法，与所述第一终端协商得到所述共享密钥；

通过所述第一服务器和所述第一终端之间的预共享密钥 PSK 认证所述第一终端的身份，所述 PSK 为所述第一服务器与所述目标零部件之间预设的秘密值。

在的又一种可能的实施方式中，所述接收单元 1303，还用于接收所述第一终端发送的

第一消息, 所述第一信息包含第一随机数;

所述发送单元 1302, 还用于向所述第一终端发送第二消息, 所述第二信息包含第一认证参数和第二随机数; 所述第一认证参数为根据所述第一消息、所述第二随机数和所述 PSK 得到的;

所述接收单元 1303, 还用于接收所述第一终端发送的第三消息, 所述第三信息包含第二认证参数;

所述处理单元 1301, 具体用于根据所述第二消息、所述第一随机数和所述 PSK 确定所述目标零部件的身份认证通过。

在又一种可能的实施方式中, 所述发送单元 1302, 具体用于:

向所述第一终端的升级控制部件发送所述第二密钥;

或者, 向所述第一终端的所述目标零部件发送所述第二密钥。

需要说明的是, 上述设计中的各个单元的具体实现还可以对应参照图 3 所示的实施例的相应描述。

在一种可能的设计中, 图 13 中所示的 OTA 升级装置 130 可以为图 3 所示实施例中的第一终端, 或者为第一终端中的一个器件, 例如芯片或者集成电路等。

在一种可能的实施方案中, 该 OTA 升级装置 130 可以包括接收单元 1303 和处理单元 1301, 其中:

所述接收单元 1303, 用于接收 OTA 服务器发送的第一密文, 所述第一密文为第一服务器根据第一密钥对所述第一终端上的目标零部件的升级数据加密得到的, 所述第一服务器为用于提供所述目标零部件的升级数据的服务器;

所述接收单元 1303, 还用于接收来自所述第一服务器的第二密钥, 所述第二密钥为所述第一密钥对应的解密密钥;

所述处理单元 1301, 还用于通过所述第二密钥解密所述第一密文, 得到所述目标零部件的升级数据;

所述处理单元 1301, 还用于通过所述目标零部件的升级数据, 升级所述目标零部件。

可以看出, 上述设计中, 由于目标零部件的升级数据是经过加密传输的, 只有第一服务器、OTA 升级装置 130 可以通过第二密钥得到升级数据, 避免了其他中间设备获取升级数据, 提高了升级数据的机密性。当升级数据中包含核心代码、关键技术实现的情况下, 可以有效保护涉密数据、关键代码等核心资产。

进一步的, 由于升级数据是经过加密的, 可以避免攻击者篡改升级数据, 提高了 OTA 升级的安全性。

在又一种可能的实施方式中, 所述处理单元 1301, 还用于与所述第一服务器建立安全通道;

所述接收单元 1303, 具体用于通过所述安全通道接收所述第一服务器的所述第二密钥。

在又一种可能的实施方式中,

所述接收单元 1303, 具体用于接收来自所述第一服务器的第二密文; 所述第二密文为根据第一安全参数加密第二密钥得到的;

所述处理单元 1301,还用于根据第二安全参数解密所述第二密文,得到所述第二密钥,所述第二安全参数为所述第一服务器与所述第一终端之间的共享密钥或者为所述第一终端的第一私钥。

在又一种可能的实施方式中,所述装置 130 还包括:

发送单元 1302,用于向所述第一服务器发送密钥获取请求。

在又一种可能的实施方式中,所述第二安全参数属于临时密钥或者属于一次性密钥。

在又一种可能的实施方式中,所述第二安全参数为所述第一公钥对应的第一私钥,所述第一安全参数为所述第一终端的第一公钥;

所述第一公钥通过所述第一终端的第一数字证书进行认证。

在又一种可能的实施方式中,所述第一数字证书对应第二公钥和第二私钥;

所述处理单元 1301,还用于确定所述第一公钥和所述第一私钥;

所述处理单元 1301,还用于通过所述第二私钥对所述第一公钥进行签名,得到第一签名,

所述发送单元 1302,还用于向所述第一服务器发送第一签名和所述第一公钥;所述第一签名用于所述第一服务器根据所述第一签名证书对应的第二公钥认证所述第一公钥。

在又一种可能的实施方式中,所述第一安全参数为所述第一服务器与所述第一终端之间的共享密钥;所述处理单元 1301,还用于:

通过密钥协商算法,与所述第一服务器协商得到所述共享密钥;

通过所述第一服务器和所述第一终端之间的预共享密钥 PSK 认证所述第一服务器的身份,所述 PSK 为所述第一服务器与所述目标零部件之间预设的秘密值。

在又一种可能的实施方式中,所述发送单元 1302,还用于向所述第一服务器发送第一消息,所述第一消息包含第一随机数;

所述接收单元 1303,还用于接收所述第一服务器发送的第二消息,所述第二消息包含第一认证参数和第二随机数;

所述处理单元 1301,具体用于根据所述第一认证参数、所述第一消息、所述第二随机数和所述 PSK 确定所述第一服务器的身份认证通过;

所述发送单元 1302,还用于向所述第一服务器发送第三消息,所述第三消息包含第二认证参数;所述第二认证参数为根据所述第一随机数、所述第二消息和所述 PSK 得到的。所述第二认证参数用于认证所述第一终端的身份。

在又一种可能的实施方式中,所述 OTA 升级装置 130 具体为第一终端中的所述目标零部件;

或者,所述 OTA 升级装置 130 具体为所述第一终端中的升级控制部件。

需要说明的是,上述设计中的各个单元的具体实现还可以对应参照图 3 所示的实施例的相应描述。

在一种可能的设计中,图 13 中所示的 OTA 升级装置 130 可以为图 3 所示实施例中的 OTA 服务器,或者为 OTA 服务器中的一个器件,例如芯片或者集成电路等。

在一种可能的实施方案中,该 OTA 升级装置 130 可以包括接收单元 1303 和发送单元

1302, 其中:

所述接收单元 1303, 用于接收来自第一服务器的第一密文, 所述第一密文为第一服务器根据第一密钥对所述第一终端上的目标零部件的升级数据加密得到的, 所述第一服务器为用于提供所述目标零部件的升级数据的服务器;

所述发送单元 1302, 用于向所述第一终端发送升级策略, 所述升级策略包含所述第一密文的第一下载地址。

可以看出, 上述设计中, 由于目标零部件的升级数据是经过加密传输的, 上述 OTA 升级装置 130 可以接收密文、转发下载地址以使得第一终端获取第一密文, 但是上述 OTA 升级装置 130 无法获取解密的密钥。当升级数据中包含核心代码、关键技术实现的情况下, 可以有效保护涉密数据、关键代码等核心资产。

进一步的, 由于升级数据是经过加密的, 可以避免攻击者篡改升级数据, 提高了 OTA 升级的安全性。

在又一种可能的实施方式中, 所述发送单元 1302, 具体用于通过所述安全通道向所述第一终端发送所述第一密文, 所述安全通道为所述第一终端基于所述第一下载地址与所述 OTA 服务器共同建立的。

在又一种可能的实施方式中, 所述升级策略中包括升级规则、升级条件、下载规则等等中的一项或者多项。

其中, 升级规则用于定义升级的次序、是否需要进行回滚等规则, 升级条件可以包含是否供电正常、存储空间、网络状态、有依赖关系的其他设备的状态等, 下载规则用于定义下载的顺序、指示哪一个部件进行下载等等。

在又一种可能的实施方式中, 所述装置 130 还包括:

处理单元 1301, 用于根据所述第一终端的信息和/或所述第一密文的信息, 确定所述升级策略。

例如, OTA 服务器根据第一终端的信息和第一密文的文件大小, 确定所述第一终端需要的存储空间大小。

需要说明的是, 上述设计中的各个单元的具体实现还可以对应参照图 3 所示的实施例的相应描述。

请参见图 14, 图 14 是本申请实施例提供的一种 OTA 升级装置 140 的结构示意图, 该 OTA 升级装置 140 可以包括发送单元 1401、处理单元 1402 中的至少一个。该 OTA 升级装置 140 用于实现前述的 OTA 方法, 例如可以用于实现图 3、图 8、图 10 或者图 12 所示的 OTA 升级方法。

在一种可能的设计中, 图 14 中所示的 OTA 升级装置 140 可以为图 8 所示实施例中的第一服务器, 或者为第一服务器中的一个器件, 例如芯片或者集成电路等。

在一种可能的实施方案中, 该 OTA 升级装置 140 可以包括发送单元 1401, 其中:

所述发送单元 1401, 用于向 OTA 服务器发送目标零部件的升级数据的元数据, 所述升级数据的元数据包含所述升级数据的第一下载地址和所述升级数据的版本信息;

所述发送单元 1401，还用于通过安全通道向部署有所述目标零部件的第一终端发送所述目标零部件的升级数据，所述安全通道为所述第一终端根据所述第一下载地址与所述第一服务器共同建立的。

可以看出，上述设计中，OTA 升级装置 140 向 OTA 服务器发送升级数据的元数据，OTA 服务器向第一终端发送升级数据的第一下载地址。第一终端通过第一下载地址下载升级数据，避免了其他中间设备（例如 OTA 服务器）获取目标零部件的升级数据，保证了升级数据的机密性。当升级数据中包含核心代码、关键技术实现的情况下，可以有效保护涉密数据、关键代码等核心资产。

进一步的，由于目标零部件的升级数据是直接从下载地址对应的存储设备上直接获取的，因此避免了中间设备等进行转存、或者审核等操作，减少了升级流程的复杂度，提高了升级效率。通过本申请实施例还可以满足某一些需要快速升级的零部件的需求。

在又一种可能的实施方式中，所述 OTA 升级装置属于所述目标零部件的供应商用于维护所述目标零部件的装置。

在又一种可能的实施方式中，所述 OTA 升级装置还包括：

处理单元 1402，用于确定所述目标零部件的升级数据的元数据。

在又一种可能的实施方式中，所述发送单元 1401，具体用于：

通过所述安全通道向所述第一终端中的所述目标零部件发送所述目标零部件的升级数据；

或者，通过所述安全通道向所述第一终端中的升级控制部件发送所述目标零部件的升级数据。

需要说明的是，上述设计中的各个单元的具体实现还可以对应参照图 8 所示的实施例的相应描述。

请参见图 15，图 15 是本申请实施例提供的一种 OTA 升级装置 150 的结构示意图，该 OTA 升级装置 150 可以包括接收单元 1501、处理单元 1502。该 OTA 升级装置 140 用于实现前述的 OTA 方法，例如可以用于实现图 3、图 8、图 10 或者图 12 所示的 OTA 升级方法。

在一种可能的设计中，图 15 中所示的 OTA 升级装置 150 可以为图 8 所示实施例中的第一终端，或者为第一终端中的一个器件，例如芯片或者集成电路等。

在一种可能的实施方案中，该 OTA 升级装置 150 可以包括接收单元 1501 和处理单元 1502，其中：

所述接收单元 1501，用于接收 OTA 服务器发送的下载策略，所述下载策略中包含目标零部件的升级数据的第一下载地址；所述目标零部件部署在所述第一终端上；

所述处理单元 1502，用于基于所述第一下载地址，与第一服务器共同建立安全通道，所述第一服务器为用于提供所述目标零部件的升级数据的服务器；

所述处理单元 1502，还用于通过所述安全通道接收所述第一服务器发送的所述目标零部件的升级数据；

所述处理单元 1502，还用于根据所述目标零部件的升级数据升级所述目标零部件。

可以看出,上述 OTA 升级装置通过第一下载地址下载升级数据,避免了其他中间设备(例如 OTA 服务器)获取目标零部件的升级数据,保证了升级数据的机密性。当升级数据中包含核心代码、关键技术实现的情况下,可以有效保护涉密数据、关键代码等核心资产。

进一步的,由于目标零部件的升级数据是在第一服务器直接获取的,因此避免了中间设备等进行转存、或者审核等操作,减少了升级流程的复杂度,提高了升级效率。通过本申请实施例还可以满足某一些需要快速升级的零部件的需求。

在又一种可能的实施方式中,所述 OTA 升级装置 150 具体可以为第一终端中的所述目标零部件;

或者,所述 OTA 升级装置 150 具体为所述第一终端中的升级控制部件。

需要说明的是,上述设计中的各个单元的具体实现还可以对应参照图 8 所示的实施例的相应描述。

在一种可能的设计中,图 13 中所示的 OTA 升级装置 130 可以为图 8 所示实施例中的 OTA 服务器,或者为 OTA 服务器中的一个器件,例如芯片或者集成电路等。

在一种可能的实施方案中,该 OTA 升级装置 130 可以包括接收单元 1303 和发送单元 1302,其中:

所述接收单元 1303,用于接收第一服务器发送的目标零部件的升级数据的元数据,其中,所述第一服务器为用于提供所述目标零部件的升级数据的服务器,所述升级数据的元数据包含所述升级数据的第一下载地址和所述升级数据的版本信息;

所述发送单元 1302,用于向所述第一终端发送升级策略,所述升级策略包含所述第一下载地址。

可以看出,上述设计中,上述 OTA 升级装置 130 接收升级数据的元数据,向升级策略转发升级数据的下载地址,而无法获取到升级数据,从而保证了升级数据的机密性。当升级数据中包含核心代码、关键技术实现的情况下,可以有效保护涉密数据、关键代码等核心资产。

进一步的,第一终端可以根据第一下载地址从第一服务器或者其他存储设备上下载升级数据,因此避免了中间设备等进行转存、或者审核等操作,减少了升级流程的复杂度,提高了升级效率。通过本申请实施例还可以满足某一些需要快速升级的零部件的需求。

在又一种可能的实施方式中,所述装置 130 还包括:

处理单元 1301,用于根据所述第一终端的信息和/或升级数据的元数据,确定所述升级策略。

在又一种可能的实施方式中,所述升级策略中包括升级规则、升级条件、下载规则等等中的一项或者多项。

在又一种可能的实施方式中,所述元数据中还包括所述目标零部件的升级数据的文件大小。

需要说明的是,上述设计中的各个单元的具体实现还可以对应参照图 8 所示的实施例的相应描述。

在一种可能的设计中，图 14 中所示的 OTA 升级装置 140 可以为图 10 所示实施例中的第一服务器，或者为第一服务器中的一个器件，例如芯片或者集成电路等。

在一种可能的实施方案中，该 OTA 升级装置 140 可以包括处理单元 1402 和发送单元 1401，其中：

所述处理单元 1402，用于根据第一密钥对目标零部件的升级数据进行加密得到第一密文，其中，所述第一服务器为用于提供所述目标零部件的升级数据的服务器；

所述处理单元 1402，用于通过第一安全参数的加密第二密钥得到第二密文，其中，所述第一安全参数为所述第一服务器与所述第一终端之间的共享密钥或者为所述第一终端的第一公钥，所述第一终端为部署有第一目标零部件的终端，所述第一目标零部件为所述目标零部件中的一个，所述第二密钥为所述第一密钥的解密密钥；

所述发送单元 1401，用于向 OTA 服务器发送所述第一密文和所述第二密文，所述第二密文用于所述第一终端解密所述第一密文。

在又一种可能的实施方式中，所述 OTA 升级装置 140 属于所述目标零部件的供应商用于维护所述目标零部件的装置。

需要说明的是，上述设计中的各个单元的具体实现还可以对应参照图 10 所示的实施例的相应描述。

在一种可能的设计中，图 13 中所示的 OTA 升级装置 130 可以为图 10 所示实施例中的 OTA 服务器，或者为 OTA 服务器中的一个器件，例如芯片或者集成电路等。

在一种可能的实施方案中，该 OTA 升级装置 130 可以包括接收单元 1303 和发送单元 1302，其中：

所述接收单元 1303，用于接收第一服务器发送的第一密文和第二密文，其中，所述第一密文为根据第一密钥对目标零部件的升级数据加密得到的，所述第二密文为根据第一安全参数对第二密钥加密得到的，所述第一安全参数为所述第一服务器与第一终端之间的共享密钥或者为所述第一终端的第一公钥，所述第一终端为部署有第一目标零部件的终端，所述第一目标零部件为所述目标零部件中的一个，所述第二密钥为所述第一密钥的解密密钥；

所述发送单元 1302，用于向所述第一终端发送所述第一密文和所述第二密文，其中所述第二密文用于所述第一终端解密所述第一密文，以得到所述目标零部件的升级数据。

可以看出，上述设计中，将升级数据通过第一密钥进行加密得到第一密文，将第二密钥进行使用第一安全参数进行加密得到第二密文。由于没有获取第二安全参数则无法解密第二密文得到第二密钥，从而无法解密第一密文得到目标零部件的升级数据，因此保证了目标零部件的升级数据的安全性。

进一步的，由于没有直接对目标零部件的升级数据进行加密，而是使用第一安全参数加密第二密钥，而密钥的数据大小通常小于升级数据的数据大小。因此，对于存在有多个、多种零部件需要升级的供应商来说，考虑多个零部件的安全参数可能不同的情况，相比于直接使用安全参数加密升级数据，本实施例可以显著减少加密过程中的计算量、存储量，提高升级的效率。

在又一种可能的实施方式中，所述装置 130，还包括：

处理单元 1301，用于根据所述第一密文所在的升级包的属性和所述第一终端的信息生成升级策略；所述升级策略包括所述第一密文和所述第二密文的第一下载地址；

所述发送单元 1302，还用于向所述第一终端发送所述升级策略；

所述发送单元 1302，还用于通过安全通道向所述第一终端发送所述第一密文和所述第二密文，所述安全通道为所述第一终端根据所述第一下载地址与所述 OTA 服务器共同建立的。

在又一种可能的实施方式中，所述升级策略中包括升级规则、升级条件、下载规则等等中的一项或者多项。

需要说明的是，上述设计中的各个单元的具体实现还可以对应参照图 10 所示的实施例的相应描述。

在一种可能的设计中，图 15 中所示的 OTA 升级装置 150 可以为图 10 所示实施例中的第一终端，或者为第一终端中的一个器件，例如芯片或者集成电路等。其中，所述 OTA 升级装置 150 中（或者 OTA 升级装置 150 所在的设备中）部署有第一目标零部件，所述第一目标零部件为目标零部件中的一个。

在一种可能的实施方案中，该 OTA 升级装置 150 可以包括接收单元 1501 和处理单元 1502，其中：

所述接收单元 1501，用于接收 OTA 服务器发送的第一密文和第二密文，所述第一密文为第一服务器根据第一密钥对所述目标零部件的升级数据加密得到的，其中，所述第一服务器为用于提供所述目标零部件的升级数据的服务器；

所述处理单元 1502，用于根据第二安全参数解密所述第二密文得到第二密钥，所述第二密钥为所述第一密钥的解密密钥，所述第二安全参数为所述第一服务器与所述第一终端之间的共享密钥或者为所述第一终端的第一私钥；

所述处理单元 1502，还用于根据所述第二密钥解密所述第一密文，得到所述目标零部件的升级数据；

所述处理单元 1502，还用于根据所述目标零部件的升级数据升级所述第一目标零部件。

在又一种可能的实施方式中，所述 OTA 升级装置 150 具体为所述第一终端中的所述第一目标零部件；

或者，所述 OTA 升级装置 150 具体为所述第一终端中的升级控制部件。

在又一种可能的实施方式中，所述处理单元 1502，还用于通过第一下载地址与所述 OTA 服务器建立安全通道；

所述接收单元 1501，具体用于通过所述安全通道接收所述 OTA 服务器发送的第一密文和第二密文。

在又一种可能的实施方式中，所述接收单元 1501，还用于接收来自所述 OTA 服务器的下载策略，所述下载策略中包含所述第一下载地址。

需要说明的是，上述设计中的各个单元的具体实现还可以对应参照图 10 所示的实施例的相应描述。

在一种可能的设计中，图 14 中所示的 OTA 升级装置 140 可以为图 12 所示实施例中的第一服务器，或者为第一服务器中的一个器件，例如芯片或者集成电路等。所述 OTA 升级装置可以为用于提供所述目标零部件的升级数据的装置。

在一种可能的实施方案中，该 OTA 升级装置 140 可以包括处理单元 1402 和发送单元 1401，其中：

所述处理单元 1402，用于根据第一安全参数对所述目标零部件的升级数据进行加密得到第一密文，所述第一安全参数为预置的所述第一服务器与所述第一终端之间的共享密钥或者为预置的所述第一终端的第一公钥，所述第一服务器为用于提供所述目标零部件的升级数据的服务器；所述第一终端为部署有所述目标零部件的终端；

所述发送单元 1401，用于向 OTA 服务器发送所述第一密文；所述第一密文用于由所述 OTA 服务器发送给第一终端以对所述第一终端中的所述目标零部件进行升级。

可以看出，上述设计中，第一安全参数和第二安全参数可以是预先配置或者预先获取的，第一服务器使用第一安全参数对目标零部件的升级数据进行加密，第一终端使用第二安全参数对第一密文解密从而获取目标零部件的升级数据。由于目标零部件的升级数据是经过加密传输的，没有获取第二安全参数则无法解密第二密文得到第二密钥，从而无法解密第一密文得到目标零部件的升级数据，因此保证了升级数据的机密性。当升级数据中包含核心代码、关键技术实现的情况下，可以有效保护涉密数据、关键代码等核心资产。

需要说明的是，上述设计中的各个单元的具体实现还可以对应参照图 12 所示的实施例的相应描述。

在一种可能的设计中，图 15 中所示的 OTA 升级装置 150 可以为图 10 所示实施例中的第一终端，或者为第一终端中的一个器件，例如芯片或者集成电路等。其中，所述 OTA 升级装置 150 中（或者 OTA 升级装置 150 所在的设备中）部署有第一目标零部件，所述第一目标零部件为目标零部件中的一个。

在一种可能的实施方案中，该 OTA 升级装置 150 可以包括接收单元 1501 和处理单元 1502，其中：

所述接收单元 1501，用于接收 OTA 服务器发送的第一密文，所述第一密文为第一服务器根据第一安全参数对所述目标零部件的升级数据加密得到的，所述第一服务器为用于提供所述目标零部件的升级数据的服务器，所述第一安全参数为所述第一服务器与所述第一终端之间的共享密钥或者为所述第一终端的第一公钥；

所述处理单元 1502，用于根据第二安全参数解密所述升级包中的第一密文，得到所述目标零部件的升级数据，所述第二安全参数为所述共享密钥或者为所述第一终端的第一私钥；

所述处理单元 1502，还用于根据所述目标零部件的升级数据升级所述目标零部件。

在又一种可能的实施方式中，所述 OTA 升级装置 150 具体为第一终端中的所述目标零部件；

或者，所述 OTA 升级装置 150 具体为所述第一终端中的升级控制部件。

需要说明的是，上述设计中的各个单元的具体实现还可以对应参照图 12 所示的实施例的相应描述。

在一种可能的设计中，图 13 中所示的 OTA 升级装置 130 可以为图 10 所示实施例中的 OTA 服务器，或者为 OTA 服务器中的一个器件，例如芯片或者集成电路等。

在一种可能的实施方案中，该 OTA 升级装置 130 可以包括接收单元 1303 和发送单元 1302，其中：

所述接收单元 1303，用于接收来自第一服务器的第一密文，所述第一密文为第一服务器根据第一安全参数对所述第一终端上的目标零部件的升级数据加密得到的，所述第一服务器为用于提供所述目标零部件的升级数据的服务器；

所述发送单元 1302，用于向所述第一终端发送升级策略，所述升级策略包含所述第一密文的第一下载地址。

在又一种可能的实施方式中，所述发送单元 1302，具体用于通过所述安全通道向所述第一终端发送所述第一密文，所述安全通道为所述第一终端基于所述第一下载地址与所述 OTA 服务器共同建立的。

在又一种可能的实施方式中，所述升级策略中包括升级规则、升级条件、下载规则等等中的一项或者多项。

在又一种可能的实施方式中，所述装置 130 还包括：

处理单元 1301，用于根据所述第一终端的信息和/或所述第一密文的信息，确定所述升级策略。

需要说明的是，上述设计中的各个单元的具体实现还可以对应参照图 12 所示的实施例的相应描述。

请参见图 16，图 16 是本申请实施例提供的一种 OTA 升级装置 160 的结构示意图，该装置 160 可以包括至少一个存储器 1601 和至少一个处理器 1602。可选的，还可以包含总线 1603。进一步可选的，还可以包括通信接口 1604，其中，存储器 1601、处理器 1602 和通信接口 1604 通过总线 1603 相连。

其中，存储器 1601 用于提供存储空间，存储空间中可以存储操作系统和计算机程序等数据。存储器 1601 可以是随机存储记忆体（random access memory，RAM）、只读存储器（read-only memory，ROM）、可擦除可编程只读存储器（erasable programmable read only memory，EPROM）、或便携式只读存储器（compact disc read-only memory，CD-ROM）等等中的一种或者多种的组合。

处理器 1602 是进行算术运算和/或逻辑运算的模块，具体可以是中央处理器（central processing unit，CPU）、图片处理器（graphics processing unit，GPU）、微处理器（microprocessor unit，MPU）、专用集成电路（Application Specific Integrated Circuit，ASIC）、现场可编程逻辑门阵列（Field Programmable Gate Array，FPGA）、复杂可编程逻辑器件（Complex programmable logic device，CPLD）等处理模块中的一种或者多种的组合。

通信接口 1604 用于接收外部发送的数据和/或向外部发送数据，可以为包括诸如以太

网电缆等的有线链路接口，也可以是无线链路（Wi-Fi、蓝牙、通用无线传输等）接口。可选的，通信接口 1604 还可以包括与接口耦合的发射器（如射频发射器、天线等），或者接收器等。

该装置 160 中的处理器 1602 用于读取所述存储器 1601 中存储的计算机程序，用于执行前述的 OTA 升级方法，例如图 3、图 8、图 10 或者图 12 中任意一个实施例所描述的 OTA 升级方法。

在一种可能的设计中，该 OTA 升级装置 160 可以为图 3 所示实施例中的第一服务器，或者第一服务器中的一个模块，例如芯片或者集成电路等。其中，所述 OTA 升级装置 160 可以为用于提供所述目标零部件的升级数据的装置。

该 OTA 升级装置 160 中的处理器 1602 用于读取所述存储器 1601 中存储的计算机程序，用于执行以下操作：

根据第一密钥对目标零部件的升级数据进行加密得到第一密文，其中，所述第一服务器为用于提供所述目标零部件的升级数据的服务器；

通过通信接口 1604 向 OTA 服务器发送所述第一密文；

通过通信接口 1604 向部署有所述目标零部件的第一终端发送第二密钥，所述第二密钥为所述第一密钥对应的解密密钥。

可以看出，上述设计中，由于目标零部件的升级数据是经过加密传输的，只有 OTA 升级装置 160、第一终端可以通过第二密钥得到升级数据，避免了其他中间设备获取升级数据，提高了升级数据的机密性。当升级数据中包含核心代码、关键技术实现的情况下，可以有效保护涉密数据、关键代码等核心资产。

进一步的，由于升级数据是经过加密的，可以避免攻击者篡改升级数据，提高了 OTA 升级的安全性。

在又一种可能的实施方式中，上述 OTA 升级装置 160 属于目标零部件的供应商用于维护目标零部件的装置。

在又一种可能的实施方式中，所述处理器 1602，还用于：

与部署有所述目标零部件的所述第一终端建立安全通道；

通过所述通信接口 1604 通过所述安全通道向所述第一终端发送所述第二密钥。

在又一种可能的实施方式中，所述处理器 1602，还用于：

根据第一安全参数加密所述第二密钥得到第二密文，所述第一安全参数为所述第一服务器与所述第一终端之间的共享密钥或者为所述第一终端的第一公钥；

通过所述通信接口 1604 向部署有所述目标零部件的所述第一终端发送所述第二密文。

在又一种可能的实施方式中，所述处理器 1602，还用于：

通过所述通信接口 1604 接收来自所述第一终端的密钥获取请求。

在又一种可能的实施方式中，所述第一安全参数属于临时密钥或者属于一次性密钥。

在又一种可能的实施方式中，所述第一安全参数为所述第一终端的第一公钥；所述处理器 1602，还用于通过所述第一终端的第一数字证书认证所述第一终端的第一公钥。

在又一种可能的实施方式中，所述第一数字证书对应第二公钥和第二私钥；所述处理

器 1602, 还用于:

通过所述通信接口 1604 接收来自所述第一终端发送的第一签名, 所述第一签名为使用所述第二私钥对所述第一公钥签名得到的;

根据所述第二公钥、所述第一签名和所述第一公钥确定所述第一公钥认证通过。

在又一种可能的实施方式中, 所述第一安全参数为所述第一服务器与所述第一终端之间的共享密钥; 所述处理器 1602, 还用于:

通过密钥协商算法, 与所述第一终端协商得到所述共享密钥;

通过所述第一服务器和所述第一终端之间的预共享密钥 PSK 认证所述第一终端的身份, 所述 PSK 为所述第一服务器与所述目标零部件之间预设的秘密值。

在的又一种可能的实施方式中, 所述处理器 1602, 还用于:

通过所述通信接口 1604 接收所述第一终端发送的第一消息, 所述第一信息包含第一随机数;

通过所述通信接口 1604 向所述第一终端发送第二消息, 所述第二信息包含第一认证参数和第二随机数; 所述第一认证参数为根据所述第一消息、所述第二随机数和所述 PSK 得到的;

通过所述通信接口 1604 接收所述第一终端发送的第三消息, 所述第三信息包含第二认证参数;

根据所述第二消息、所述第一随机数和所述 PSK 确定所述目标零部件的身份认证通过。

在又一种可能的实施方式中, 所述处理器 1602, 还用于:

通过所述通信接口 1604 向所述第一终端的升级控制部件发送所述第二密钥;

或者, 通过所述通信接口 1604 向所述第一终端的所述目标零部件发送所述第二密钥。

需要说明的是, 上述设计中的各个单元的具体实现还可以对应参照图 3 所示的实施例的相应描述。

在一种可能的设计中, 该 OTA 升级装置 160 可以为图 3 所示实施例中的第一终端, 或者第一终端中的一个模块, 例如芯片或者集成电路等。可选的, 所述 OTA 升级装置 160 中 (或者 OTA 升级装置 160 所在的设备中) 部署有目标零部件。

该 OTA 升级装置 160 中的处理器 1602 用于读取所述存储器 1601 中存储的计算机程序, 用于执行以下操作:

通过通信接口 1604 接收 OTA 服务器发送的第一密文, 所述第一密文为第一服务器根据第一密钥对所述第一终端上的目标零部件的升级数据加密得到的, 所述第一服务器为用于提供所述目标零部件的升级数据的服务器;

通过通信接口 1604 接收来自所述第一服务器的第二密钥, 所述第二密钥为所述第一密钥对应的解密密钥;

通过所述第二密钥解密所述第一密文, 得到所述目标零部件的升级数据;

通过所述目标零部件的升级数据, 升级所述目标零部件。

可以看出, 上述设计中, 由于目标零部件的升级数据是经过加密传输的, 只有第一服务器、OTA 升级装置 160 可以通过第二密钥得到升级数据, 避免了其他中间设备获取升级

数据，提高了升级数据的机密性。当升级数据中包含核心代码、关键技术实现的情况下，可以有效保护涉密数据、关键代码等核心资产。

进一步的，由于升级数据是经过加密的，可以避免攻击者篡改升级数据，提高了 OTA 升级的安全性。

在又一种可能的实施方式中，所述处理器 1602，还用于：

与所述第一服务器建立安全通道；

通过通信接口 1604 通过所述安全通道接收所述第一服务器的所述第二密钥。

在又一种可能的实施方式中，所述处理器 1602，还用于：

通过通信接口 1604 接收来自所述第一服务器的第二密文；所述第二密文为根据第一安全参数加密第二密钥得到的；

根据第二安全参数解密所述第二密文，得到所述第二密钥，所述第二安全参数为所述第一服务器与所述第一终端之间的共享密钥或者为所述第一终端的第一私钥。

在又一种可能的实施方式中，所述处理器 1602，还用于：

通过通信接口 1604 向所述第一服务器发送密钥获取请求。

在又一种可能的实施方式中，所述第二安全参数属于临时密钥或者属于一次性密钥。

在又一种可能的实施方式中，所述第二安全参数为所述第一公钥对应的第一私钥，所述第一安全参数为所述第一终端的第一公钥；

所述第一公钥通过所述第一终端的第一数字证书进行认证。

在又一种可能的实施方式中，所述第一数字证书对应第二公钥和第二私钥；所述处理器 1602，还用于：

确定所述第一公钥和所述第一私钥；

通过所述第二私钥对所述第一公钥进行签名，得到第一签名，

通过通信接口 1604 向所述第一服务器发送第一签名和所述第一公钥；所述第一签名用于所述第一服务器根据所述第一签名证书对应的第二公钥认证所述第一公钥。

在又一种可能的实施方式中，所述第一安全参数为所述第一服务器与所述第一终端之间的共享密钥；所述处理器 1602，还用于：

通过密钥协商算法，与所述第一服务器协商得到所述共享密钥；

通过所述第一服务器和所述第一终端之间的预共享密钥 PSK 认证所述第一服务器的身份，所述 PSK 为所述第一服务器与所述目标零部件之间预设的秘密值。

在又一种可能的实施方式中，所述处理器 1602，还用于：

通过通信接口 1604 向所述第一服务器发送第一消息，所述第一消息包含第一随机数；

通过通信接口 1604 接收所述第一服务器发送的第二消息，所述第二消息包含第一认证参数和第二随机数；

根据所述第一认证参数、所述第一消息、所述第二随机数和所述 PSK 确定所述第一服务器的身份认证通过；

通过通信接口 1604 向所述第一服务器发送第三消息，所述第三消息包含第二认证参数；所述第二认证参数为根据所述第一随机数、所述第二消息和所述 PSK 得到的。所述第二认证参数用于认证所述第一终端的身份。

在又一种可能的实施方式中,所述 OTA 升级装置 160 具体为第一终端中的所述目标零部件;

或者,所述 OTA 升级装置 160 具体为所述第一终端中的升级控制部件。

需要说明的是,上述设计中的各个单元的具体实现还可以对应参照图 3 所示的实施例的相应描述。

在一种可能的设计中,该 OTA 升级装置 160 可以为图 3 所示实施例中的 OTA 服务器,或者 OTA 服务器中的一个模块,例如芯片或者集成电路等。

该 OTA 升级装置 160 中的处理器 1602 用于读取所述存储器 1601 中存储的计算机程序,用于执行以下操作:

通过通信接口 1604 接收来自第一服务器的第一密文,所述第一密文为第一服务器根据第一密钥对所述第一终端上的目标零部件的升级数据加密得到的,所述第一服务器为用于提供所述目标零部件的升级数据的服务器;

通过通信接口 1604 向所述第一终端发送升级策略,所述升级策略包含所述第一密文的第一下载地址。

可以看出,上述设计中,由于目标零部件的升级数据是经过加密传输的,上述 OTA 升级装置 160 可以接收密文、转发下载地址以使得第一终端获取第一密文,但是上述 OTA 升级装置 160 无法获取解密的密钥。当升级数据中包含核心代码、关键技术实现的情况下,可以有效保护涉密数据、关键代码等核心资产。

进一步的,由于升级数据是经过加密的,可以避免攻击者篡改升级数据,提高了 OTA 升级的安全性。

在又一种可能的实施方式中,所述处理器 1602,还用于:

通过通信接口 1604 通过所述安全通道向所述第一终端发送所述第一密文,所述安全通道为所述第一终端基于所述第一下载地址与所述 OTA 服务器共同建立的。

在又一种可能的实施方式中,所述升级策略中包括升级规则、升级条件、下载规则等等中的一项或者多项。

其中,升级规则用于定义升级的次序、是否需要回滚等规则,升级条件可以包含是否供电正常、存储空间、网络状态、有依赖关系的其他设备的状态等,下载规则用于定义下载的顺序、指示哪一个部件进行下载等等。

在又一种可能的实施方式中,所述处理器 1602,还用于:

根据所述第一终端的信息和/或所述第一密文的信息,确定所述升级策略。

例如,OTA 服务器根据第一终端的信息和第一密文的文件大小,确定所述第一终端需要的存储空间大小。

需要说明的是,上述设计中的各个单元的具体实现还可以对应参照图 3 所示的实施例的相应描述。

在一种可能的设计中,该 OTA 升级装置 160 可以为图 8 所示实施例中的第一服务器,或者第一服务器中的一个模块,例如芯片或者集成电路等。其中,所述 OTA 升级装置 160

可以为用于提供所述目标零部件的升级数据的装置。

该OTA升级装置160中的处理器1602用于读取所述存储器1601中存储的计算机程序，用于执行以下操作：

通过通信接口1604向OTA服务器发送目标零部件的升级数据的元数据，所述升级数据的元数据包含所述升级数据的第一下载地址和所述升级数据的版本信息；

通过通信接口1604通过安全通道向部署有所述目标零部件的第一终端发送所述目标零部件的升级数据，所述安全通道为所述第一终端根据所述第一下载地址与所述第一服务器共同建立的。

可以看出，上述设计中，OTA升级装置160向OTA服务器发送升级数据的元数据，OTA服务器向第一终端发送升级数据的第一下载地址。第一终端通过第一下载地址下载升级数据，避免了其他中间设备（例如OTA服务器）获取目标零部件的升级数据，保证了升级数据的机密性。当升级数据中包含核心代码、关键技术实现的情况下，可以有效保护涉密数据、关键代码等核心资产。

进一步的，由于目标零部件的升级数据是直接从下载地址对应的存储设备上直接获取的，因此避免了中间设备等进行转存、或者审核等操作，减少了升级流程的复杂度，提高了升级效率。通过本申请实施例还可以满足某一些需要快速升级的零部件的需求。

在又一种可能的实施方式中，所述OTA升级装置属于所述目标零部件的供应商用于维护所述目标零部件的装置。

在又一种可能的实施方式中，所述处理器1602，还用于：

确定所述目标零部件的升级数据的元数据。

在又一种可能的实施方式中，所述处理器1602，还用于：

通过通信接口1604通过所述安全通道向所述第一终端中的所述目标零部件发送所述目标零部件的升级数据；

或者，通过通信接口1604通过所述安全通道向所述第一终端中的升级控制部件发送所述目标零部件的升级数据。

需要说明的是，上述设计中的各个单元的具体实现还可以对应参照图8所示的实施例的相应描述。

在一种可能的设计中，该OTA升级装置160可以为图8所示实施例中的第一终端，或者第一终端中的一个模块，例如芯片或者集成电路等。可选的，所述OTA升级装置160中（或者OTA升级装置160所在的设备中）部署有目标零部件。

该OTA升级装置160中的处理器1602用于读取所述存储器1601中存储的计算机程序，用于执行以下操作：

通过通信接口1604接收OTA服务器发送的下载策略，所述下载策略中包含目标零部件的升级数据的第一下载地址；所述目标零部件部署在所述第一终端上；

基于所述第一下载地址，与第一服务器共同建立安全通道，所述第一服务器为用于提供所述目标零部件的升级数据的服务器；

通过通信接口1604通过所述安全通道接收所述第一服务器发送的所述目标零部件的

升级数据；

根据所述目标零部件的升级数据升级所述目标零部件。

可以看出，上述 OTA 升级装置通过第一下载地址下载升级数据，避免了其他中间设备（例如 OTA 服务器）获取目标零部件的升级数据，保证了升级数据的机密性。当升级数据中包含核心代码、关键技术实现的情况下，可以有效保护涉密数据、关键代码等核心资产。

进一步的，由于目标零部件的升级数据是在第一服务器直接获取的，因此避免了中间设备等进行转存、或者审核等操作，减少了升级流程的复杂度，提高了升级效率。通过本申请实施例还可以满足某一些需要快速升级的零部件的需求。

在又一种可能的实施方式中，所述 OTA 升级装置 160 具体可以为第一终端中的所述目标零部件；

或者，所述 OTA 升级装置 160 具体为所述第一终端中的升级控制部件。

需要说明的是，上述设计中的各个单元的具体实现还可以对应参照图 8 所示的实施例的相应描述。

在一种可能的设计中，该 OTA 升级装置 160 可以为图 8 所示实施例中的 OTA 服务器，或者 OTA 服务器中的一个模块，例如芯片或者集成电路等。

该 OTA 升级装置 160 中的处理器 1602 用于读取所述存储器 1601 中存储的计算机程序，用于执行以下操作：

通过通信接口 1604 接收第一服务器发送的目标零部件的升级数据的元数据，其中，所述第一服务器为用于提供所述目标零部件的升级数据的服务器，所述升级数据的元数据包含所述升级数据的第一下载地址和所述升级数据的版本信息；

通过通信接口 1604 向所述第一终端发送升级策略，所述升级策略包含所述第一下载地址。

可以看出，上述设计中，上述 OTA 升级装置 160 接收升级数据的元数据，向升级策略转发升级数据的下载地址，而无法获取到升级数据，从而保证了升级数据的机密性。当升级数据中包含核心代码、关键技术实现的情况下，可以有效保护涉密数据、关键代码等核心资产。

进一步的，第一终端可以根据第一下载地址从第一服务器或者其他存储设备上下载升级数据，因此避免了中间设备等转存、或者审核等操作，减少了升级流程的复杂度，提高了升级效率。通过本申请实施例还可以满足某一些需要快速升级的零部件的需求。

在又一种可能的实施方式中，所述处理器 1602，还用于：

根据所述第一终端的信息和/或升级数据的元数据，确定所述升级策略。

在又一种可能的实施方式中，所述升级策略中包括升级规则、升级条件、下载规则等等中的一项或者多项。

在又一种可能的实施方式中，所述元数据中还包括所述目标零部件的升级数据的文件大小。

需要说明的是，上述设计中的各个单元的具体实现还可以对应参照图 8 所示的实施例的相应描述。

在一种可能的设计中,该 OTA 升级装置 160 可以为图 10 所示实施例中的第一服务器,或者第一服务器中的一个模块,例如芯片或者集成电路等。其中,所述 OTA 升级装置 160 可以为用于提供所述目标零部件的升级数据的装置。

该 OTA 升级装置 160 中的处理器 1602 用于读取所述存储器 1601 中存储的计算机程序,用于执行以下操作:

根据第一密钥对目标零部件的升级数据进行加密得到第一密文,其中,所述第一服务器为用于提供所述目标零部件的升级数据的服务器;

通过第一安全参数的加密第二密钥得到第二密文,其中,所述第一安全参数为所述第一服务器与所述第一终端之间的共享密钥或者为所述第一终端的第一公钥,所述第一终端为部署有第一目标零部件的终端,所述第一目标零部件为所述目标零部件中的一个,所述第二密钥为所述第一密钥的解密密钥;

通过通信接口 1604 向 OTA 服务器发送所述第一密文和所述第二密文,所述第二密文用于所述第一终端解密所述第一密文。

在又一种可能的实施方式中,所述 OTA 升级装置 160 属于所述目标零部件的供应商用于维护所述目标零部件的装置。

需要说明的是,上述设计中的各个单元的具体实现还可以对应参照图 10 所示的实施例的相应描述。

在一种可能的设计中,该 OTA 升级装置 160 可以为图 10 所示实施例中的 OTA 服务器,或者 OTA 服务器中的一个模块,例如芯片或者集成电路等。

该 OTA 升级装置 160 中的处理器 1602 用于读取所述存储器 1601 中存储的计算机程序,用于执行以下操作:

通过通信接口 1604 接收第一服务器发送的第一密文和第二密文,其中,所述第一密文为根据第一密钥对目标零部件的升级数据加密得到的,所述第二密文为根据第一安全参数对第二密钥加密得到的,所述第一安全参数为所述第一服务器与第一终端之间的共享密钥或者为所述第一终端的第一公钥,所述第一终端为部署有第一目标零部件的终端,所述第一目标零部件为所述目标零部件中的一个,所述第二密钥为所述第一密钥的解密密钥;

通过通信接口 1604 向所述第一终端发送所述第一密文和所述第二密文,其中所述第二密文用于所述第一终端解密所述第一密文,以得到所述目标零部件的升级数据。

可以看出,上述设计中,将升级数据通过第一密钥进行加密得到第一密文,将第二密钥进行使用第一安全参数进行加密得到第二密文。由于没有获取第二安全参数则无法解密第二密文得到第二密钥,从而无法解密第一密文得到目标零部件的升级数据,因此保证了目标零部件的升级数据的安全性。

进一步的,由于没有直接对目标零部件的升级数据进行加密,而是使用第一安全参数加密第二密钥,而密钥的数据大小通常小于升级数据的数据大小。因此,对于存在有多个、多种零部件需要升级的供应商来说,考虑多个零部件的安全参数可能不同的情况,相比于直接使用安全参数加密升级数据,本实施例可以显著减少加密过程中的计算量、存储量,

提高升级的效率。

在又一种可能的实施方式中，所述处理器 1602，还用于：

根据所述第一密文所在的升级包的属性和所述第一终端的信息生成升级策略；所述升级策略包括所述第一密文和所述第二密文的第一下载地址；

通过通信接口 1604 向所述第一终端发送所述升级策略；

通过通信接口 1604 通过安全通道向所述第一终端发送所述第一密文和所述第二密文，所述安全通道为所述第一终端根据所述第一下载地址与所述 OTA 服务器共同建立的。

在又一种可能的实施方式中，所述升级策略中包括升级规则、升级条件、下载规则等等中的一项或者多项。

需要说明的是，上述设计中的各个单元的具体实现还可以对应参照图 10 所示的实施例的相应描述。

在一种可能的设计中，该 OTA 升级装置 160 可以为图 10 所示实施例中的第一终端，或者第一终端中的一个模块，例如芯片或者集成电路等。其中，所述 OTA 升级装置 160 中（或者 OTA 升级装置 160 所在的设备中）部署有第一目标零部件，所述第一目标零部件为目标零部件中的一个。

该 OTA 升级装置 160 中的处理器 1602 用于读取所述存储器 1601 中存储的计算机程序，用于执行以下操作：

接收 OTA 服务器发送的第一密文和第二密文，所述第一密文为第一服务器根据第一密钥对所述目标零部件的升级数据加密得到的，其中，所述第一服务器为用于提供所述目标零部件的升级数据的服务器；

根据第二安全参数解密所述第二密文得到第二密钥，所述第二密钥为所述第一密钥的解密密钥，所述第二安全参数为所述第一服务器与所述第一终端之间的共享密钥或者为所述第一终端的第一私钥；

根据所述第二密钥解密所述第一密文，得到所述目标零部件的升级数据；

根据所述目标零部件的升级数据升级所述第一目标零部件。

在又一种可能的实施方式中，所述 OTA 升级装置 160 具体为所述第一终端中的所述第一目标零部件；

或者，所述 OTA 升级装置 160 具体为所述第一终端中的升级控制部件。

在又一种可能的实施方式中，所述处理器 1602，还用于：

通过第一下载地址与所述 OTA 服务器建立安全通道；

通过通信接口 1604 通过所述安全通道接收所述 OTA 服务器发送的第一密文和第二密文。

在又一种可能的实施方式中，所述处理器 1602，还用于：

通过通信接口 1604 接收来自所述 OTA 服务器的下载策略，所述下载策略中包含所述第一下载地址。

需要说明的是，上述设计中的各个单元的具体实现还可以对应参照图 10 所示的实施例的相应描述。

在一种可能的设计中,该 OTA 升级装置 160 可以为图 12 所示实施例中的第一服务器,或者第一服务器中的一个模块,例如芯片或者集成电路等。其中,所述 OTA 升级装置 160 可以为用于提供所述目标零部件的升级数据的装置。

该 OTA 升级装置 160 中的处理器 1602 用于读取所述存储器 1601 中存储的计算机程序,用于执行以下操作:

根据第一安全参数对所述目标零部件的升级数据进行加密得到第一密文,所述第一安全参数为预置的所述第一服务器与所述第一终端之间的共享密钥或者为预置的所述第一终端的第一公钥,所述第一服务器为用于提供所述目标零部件的升级数据的服务器;所述第一终端为部署有所述目标零部件的终端;

通过通信接口 1604 向 OTA 服务器发送所述第一密文;所述第一密文用于由所述 OTA 服务器发送给第一终端以对所述第一终端中的所述目标零部件进行升级。

可以看出,上述设计中,第一安全参数和第二安全参数可以是预先配置或者预先获取的,第一服务器使用第一安全参数对目标零部件的升级数据进行加密,第一终端使用第二安全参数对第一密文解密从而获取目标零部件的升级数据。由于目标零部件的升级数据是经过加密传输的,没有获取第二安全参数则无法解密第二密文得到第二密钥,从而无法解密第一密文得到目标零部件的升级数据,因此保证了升级数据的机密性。当升级数据中包含核心代码、关键技术实现的情况下,可以有效保护涉密数据、关键代码等核心资产。

需要说明的是,上述设计中的各个单元的具体实现还可以对应参照图 12 所示的实施例的相应描述。

在一种可能的设计中,该 OTA 升级装置 160 可以为图 12 所示实施例中的第一服务器,或者第一服务器中的一个模块,例如芯片或者集成电路等。可选的,所述 OTA 升级装置 160 中(或者 OTA 升级装置 160 所在的设备中)部署有目标零部件。

该 OTA 升级装置 160 中的处理器 1602 用于读取所述存储器 1601 中存储的计算机程序,用于执行以下操作:

通过通信接口 1604 接收 OTA 服务器发送的第一密文,所述第一密文为第一服务器根据第一安全参数对所述目标零部件的升级数据加密得到的,所述第一服务器为用于提供所述目标零部件的升级数据的服务器,所述第一安全参数为所述第一服务器与所述第一终端之间的共享密钥或者为所述第一终端的第一公钥;

根据第二安全参数解密所述升级包中的第一密文,得到所述目标零部件的升级数据,所述第二安全参数为所述共享密钥或者为所述第一终端的第一私钥;

根据所述目标零部件的升级数据升级所述目标零部件。

在又一种可能的实施方式中,所述 OTA 升级装置 160 具体为第一终端中的所述目标零部件;

或者,所述 OTA 升级装置 160 具体为所述第一终端中的升级控制部件。

需要说明的是,上述设计中的各个单元的具体实现还可以对应参照图 12 所示的实施例的相应描述。

在一种可能的设计中,该 OTA 升级装置 160 可以为图 12 所示实施例中的 OTA 服务器,或者 OTA 服务器中的一个模块,例如芯片或者集成电路等。该 OTA 升级装置 160 中的处理器 1602 用于读取所述存储器 1601 中存储的计算机程序,用于执行以下操作:

通过通信接口 1604 接收来自第一服务器的第一密文,所述第一密文为第一服务器根据第一安全参数对所述第一终端上的目标零部件的升级数据加密得到的,所述第一服务器为用于提供所述目标零部件的升级数据的服务器;

通过通信接口 1604 向所述第一终端发送升级策略,所述升级策略包含所述第一密文的第一下载地址。

在又一种可能的实施方式中,所述处理器 1602,还用于:

通过通信接口 1604 通过所述安全通道向所述第一终端发送所述第一密文,所述安全通道为所述第一终端基于所述第一下载地址与所述 OTA 服务器共同建立的。

在又一种可能的实施方式中,所述升级策略中包括升级规则、升级条件、下载规则等等中的一项或者多项。

在又一种可能的实施方式中,所述处理器 1602,还用于:

根据所述第一终端的信息和/或所述第一密文的信息,确定所述升级策略。

需要说明的是,上述设计中的各个单元的具体实现还可以对应参照图 12 所示的实施例的相应描述。

本申请实施例还提供了一种芯片系统,所述芯片系统包括至少一个处理器和通信接口,所述通信接口用于发送和/或接收数据,所述至少一个处理器用于调用至少一个存储器中存储的计算机程序,以使得所述芯片系统所在的装置实现图 3、图 8、图 10 或者图 12 所示的实施例中第一服务器、OTA 服务器或者第一终端侧的方法。

进一步,所述至少一个处理器可以为 CPU、GPU、MPU、ASIC、FPGA、CPLD、协处理器(协助中央处理器完成相应处理和应用)、MCU 等处理模块中的一种或者多种的组合。

本申请实施例还提供了一种 OTA 升级系统,该 OTA 升级系统包括第一服务器和目标零部件。其中,所述第一服务器用于实现图 3、图 8、图 10 或者图 12 所示的实施例中第一服务器侧的方法;

所述目标零部件用于实现图 3、图 8、图 10 或者图 12 所示的实施例中第一终端侧的方法。进一步的,所述第一服务器可以属于所述目标零部件的供应商的服务器。

本申请实施例还提供了一种 OTA 升级系统,该 OTA 升级系统包括 OTA 服务器和第一终端。其中,所述 OTA 服务器用于实现图 3、图 8、图 10 或者图 12 所示的实施例中 OTA 服务器侧的方法;

所述第一终端用于实现图 3、图 8、图 10 或者图 12 所示的实施例中第一终端侧的方法。

本申请实施例还提供了一种 OTA 升级系统,该 OTA 升级系统包括第一服务器、OTA 服务器和第一终端。其中,所述第一服务器用于实现图 3、图 8、图 10 或者图 12 所示的实施例中第一服务器侧的方法;

所述 OTA 服务器用于实现图 3、图 8、图 10 或者图 12 所示的实施例中 OTA 服务器侧

的方法；

所述第一终端用于实现图 3、图 8、图 10 或者图 12 所示的实施例中第一终端侧的方法。

本申请实施例还提供了一种计算机可读存储介质，所述计算机可读存储介质中存储有计算机程序，当所述计算机程序在一个或多个处理器上运行时，实现图 3、图 8、图 10 或者图 12 所示的实施例所描述的方法。

本申请实施例还提供了一种计算机程序产品，当所述计算机程序产品在一个或多个处理器上运行时，实现图 3、图 8、图 10 或者图 12 所示的实施例所描述的方法。

在计算机上加载和执行该计算机指令时，可以全部或部分地实现本申请实施例所描述的流程或功能。该计算机可以是通用计算机、专用计算机、计算机网络、或者其它可编程装置。该计算机指令可以存储在计算机可读存储介质中，或者通过计算机可读存储介质进行传输。该计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。可用介质可以是磁性介质，(例如，软盘、硬盘、磁带)、光介质(例如，DVD)、或者半导体介质(例如，固态硬盘(solid state disk, SSD))等。

本申请方法实施例中的步骤可以根据实际需要进行顺序调整、合并和删减。

本申请装置实施例中的模块可以根据实际需要进行合并、划分和删减。

权利要求

1、一种空中下载技术 OTA 升级方法，其特征在于，包括：

第一服务器根据第一密钥对目标零部件的升级数据进行加密得到第一密文，其中，所述第一服务器为用于提供所述目标零部件的升级数据的服务器；

所述第一服务器向 OTA 服务器发送所述第一密文；

所述第一服务器向部署有所述目标零部件的第一终端发送第二密钥，所述第二密钥为所述第一密钥对应的解密密钥。

2、根据权利要求 1 中所述的方法，其特征在于，所述第一服务器属于所述目标零部件的供应商用于维护所述目标零部件的服务器。

3、根据权利要求 1 或 2 中所述的方法，其特征在于，所述第一服务器向部署有所述目标零部件的第一终端发送第二密钥，包括：

所述第一服务器与部署有所述目标零部件的所述第一终端建立安全通道；

所述第一服务器通过所述安全通道向所述第一终端发送所述第二密钥。

4、根据权利要求 1 或 2 中所述的方法，其特征在于，所述第一服务器向部署有所述目标零部件的第一终端发送第二密钥，包括：

所述第一服务器根据第一安全参数加密所述第二密钥得到第二密文，所述第一安全参数为所述第一服务器与所述第一终端之间的共享密钥或者为所述第一终端的第一公钥；

所述第一服务器向部署有所述目标零部件的所述第一终端发送所述第二密文。

5、根据权利要求 4 中所述的方法，其特征在于，所述第一服务器根据第一安全参数加密所述第二密钥得到第二密文之前，所述方法还包括：

所述第一服务器接收来自所述第一终端的密钥获取请求。

6、根据权利要求 4 或 5 中所述的方法，其特征在于，所述第一安全参数属于临时密钥或者属于一次性密钥。

7、根据权利要求 4-6 任一项中所述的方法，其特征在于，所述第一安全参数为所述目标零部件的第一公钥；所述第一服务器根据第一安全参数加密所述第二密钥得到第二密文之前，还包括：

所述第一服务器接收所述第一终端发送的所述目标零部件的第一公钥；

所述第一服务器通过所述目标零部件的第一数字证书认证所述目标零部件的第一公钥。

8、根据权利要求 4-6 任一项中所述的方法，其特征在于，所述第一安全参数为所述第一服务器与所述第一终端之间的共享密钥；所述第一服务器根据第一安全参数加密所述第二密钥得到第二密文之前，还包括：

所述第一服务器通过密钥协商算法，与所述第一终端协商得到所述共享密钥；

所述第一服务器通过所述第一服务器和所述第一终端之间的预共享密钥 PSK 认证所述第一终端的身份，所述 PSK 为所述第一服务器与所述目标零部件之间预设的秘密值。

9、根据权利要求 1-8 任一项中所述的方法，其特征在于，所述第一服务器向部署有所述目标零部件的第一终端发送第二密钥，包括：

所述第一服务器向所述第一终端的升级控制部件发送所述第二密钥；

或者，所述第一服务器向所述第一终端的所述目标零部件发送所述第二密钥。

10、一种空中下载技术 OTA 升级方法，其特征在于，包括：

第一终端接收 OTA 服务器发送的第一密文，所述第一密文为第一服务器根据第一密钥对所述第一终端上的目标零部件的升级数据加密得到的，所述第一服务器为用于提供所述目标零部件的升级数据的服务器；

所述第一终端接收来自所述第一服务器的第二密钥，所述第二密钥为所述第一密钥对应的解密密钥；

所述第一终端通过所述第二密钥解密所述第一密文，得到所述目标零部件的升级数据；
所述第一终端通过所述目标零部件的升级数据，升级所述目标零部件。

11、根据权利要求 10 中所述的方法，其特征在于，所述第一终端接收来自所述第一服务器的第二密钥，包括：

所述第一终端与所述第一服务器建立安全通道；

所述第一终端通过所述安全通道接收所述第一服务器的所述第二密钥。

12、根据权利要求 10 中所述的方法，其特征在于，所述第一终端接收来自所述第一服务器发送的第二密钥，包括：

所述第一终端接收来自所述第一服务器的第二密文；所述第二密文为根据第一安全参数加密第二密钥得到的；

所述第一终端根据第二安全参数解密所述第二密文，得到所述第二密钥，所述第二安全参数为所述第一服务器与所述第一终端之间的共享密钥或者为所述第一终端的第一私钥。

13、根据权利要求 12 中所述的方法，其特征在于，所述第一终端接收来自所述第一服务器的第二密钥之前，所述方法还包括：

所述第一终端向所述第一服务器发送密钥获取请求。

14、根据权利要求 12 或 13 中所述的方法，其特征在于，所述第二安全参数属于临时

密钥或者属于一次性密钥。

15、根据权利要求 12-14 任一项中所述的方法，其特征在于，

所述第二安全参数为所述第一公钥对应的第一私钥，所述第一安全参数为所述目标零部件的第一公钥；

所述第一公钥通过所述目标零部件的第一数字证书进行认证。

16、根据权利要求 12-14 任一项中所述的方法，其特征在于，所述第一安全参数为所述第一服务器与所述第一终端之间的共享密钥；所述第一终端根据第二安全参数解密所述第二密文，得到所述第二密钥之前，还包括：

所述第一终端通过密钥协商算法，与所述第一服务器协商得到所述共享密钥；

所述第一终端通过所述第一服务器和所述目标零部件之间的预共享密钥 PSK 认证所述第一服务器的身份，所述 PSK 为所述第一服务器与所述目标零部件之间预设的秘密值。

17、根据权利要求 10-16 中任一项所述的方法，其特征在于，

所述 OTA 升级方法具体应用于所述第一终端中的所述目标零部件；

或者，所述第一终端中还包括升级控制部件，所述 OTA 升级方法具体应用于所述升级控制部件。

18、一种 OTA 升级方法，其特征在于，包括：

第一服务器向 OTA 服务器发送目标零部件的升级数据的元数据，其中，所述第一服务器为用于提供所述目标零部件的升级数据的服务器，所述升级数据的元数据包含所述升级数据的第一下载地址和所述升级数据的版本信息；

所述第一服务器通过安全通道向部署有所述目标零部件的第一终端发送所述目标零部件的升级数据，所述安全通道为所述第一终端根据所述第一下载地址与所述第一服务器共同建立的。

19、根据权利要求 18 中所述的方法，其特征在于，所述第一服务器属于所述目标零部件的供应商用于维护所述目标零部件的服务器。

20、一种空中下载技术 OTA 升级方法，其特征在于，应用于部署有目标零部件的第一终端，所述方法包括：

所述第一终端接收 OTA 服务器发送的下载策略，所述下载策略中包含所述目标零部件的升级数据的第一下载地址；

所述第一终端基于所述第一下载地址，与第一服务器共同建立安全通道，所述第一服务器为用于提供所述目标零部件的升级数据的服务器；

所述第一终端通过所述安全通道接收所述第一服务器发送的所述目标零部件的升级数据；

所述第一终端根据所述目标零部件的升级数据升级所述目标零部件。

21、一种空中下载技术 OTA 升级方法，其特征在于，包括：

第一服务器根据第一密钥对目标零部件的升级数据进行加密得到第一密文，其中，所述第一服务器为用于提供所述目标零部件的升级数据的服务器；

所述第一服务器通过第一安全参数的加密第二密钥得到第二密文，其中，所述第一安全参数为所述第一服务器与第一终端之间的共享密钥或者为所述第一终端的第一公钥，所述第一终端为部署有第一目标零部件的终端，所述第一目标零部件为所述目标零部件中的一个，所述第二密钥为所述第一密钥的解密密钥；

所述第一服务器向 OTA 服务器发送所述第一密文和所述第二密文，所述第二密文用于所述第一终端解密所述第一密文。

22、根据权利要求 21 中所述的方法，其特征在于，所述第一服务器属于所述目标零部件的供应商用于维护所述目标零部件的服务器。

23、一种空中下载技术 OTA 升级方法，其特征在于，包括：

OTA 服务器接收第一服务器发送的第一密文和第二密文，其中，所述第一密文为根据第一密钥对目标零部件的升级数据加密得到的，所述第二密文为根据第一安全参数对第二密钥加密得到的，所述第一安全参数为所述第一服务器与第一终端之间的共享密钥或者为所述第一终端的第一公钥，所述第一终端为部署有第一目标零部件的终端，所述第一目标零部件为所述目标零部件中的一个，所述第二密钥为所述第一密钥的解密密钥；

所述 OTA 服务器向所述第一终端发送所述第一密文和所述第二密文，其中所述第二密文用于所述第一终端解密所述第一密文，以得到所述目标零部件的升级数据。

24、根据权利要求 23 中所述的方法，其特征在于，所述 OTA 服务器向所述第一终端发送所述第一密文和所述第二密文，包括：

所述 OTA 服务器根据所述第一密文所在的升级包的属性和所述第一终端的信息生成升级策略；所述升级策略包括所述第一密文和所述第二密文的第一下载地址；

所述 OTA 服务器向所述第一终端发送所述升级策略；

所述 OTA 服务器通过安全通道向所述第一终端发送所述第一密文和所述第二密文，所述安全通道为所述第一终端根据所述第一下载地址与所述 OTA 服务器共同建立的。

25、一种空中下载技术 OTA 升级方法，其特征在于，应用于部署有第一目标零部件的第一终端，所述第一目标零部件为目标零部件中的一个，所述方法包括：

所述第一终端接收 OTA 服务器发送的第一密文和第二密文，所述第一密文为第一服务器根据第一密钥对所述目标零部件的升级数据加密得到的，其中，所述第一服务器为用于提供所述目标零部件的升级数据的服务器；

所述第一终端根据第二安全参数解密所述第二密文得到第二密钥，所述第二密钥为所

述第一密钥的解密密钥，所述第二安全参数为所述第一服务器与所述第一终端之间的共享密钥或者为所述第一终端的第一私钥；

所述第一终端根据所述第二密钥解密所述第一密文，得到所述目标零部件的升级数据；
所述第一终端根据所述目标零部件的升级数据升级所述第一目标零部件。

26、根据权利要求 25 中所述的方法，其特征在于，

所述 OTA 升级方法具体应用于所述第一终端中的所述第一目标零部件；

或者，所述 OTA 升级系统中的第一终端中还包括升级控制部件，所述 OTA 升级方法具体应用于所述升级控制部件。

27、一种 OTA 升级方法，其特征在于，包括：

第一服务器根据第一安全参数对所述目标零部件的升级数据进行加密得到第一密文，所述第一安全参数为预置的所述第一服务器与所述第一终端之间的共享密钥或者为预置的所述第一终端的第一公钥，所述第一服务器为用于提供所述目标零部件的升级数据的服务器；所述第一终端为部署有所述目标零部件的终端；

所述第一服务器向 OTA 服务器发送所述第一密文；所述第一密文用于由所述 OTA 服务器发送给第一终端以对所述第一终端中的所述目标零部件进行升级。

28、一种空中下载技术 OTA 升级方法，其特征在于，应用于部署有第一目标零部件的第一终端，所述第一目标零部件为目标零部件中的一个，所述方法包括：

第一终端接收 OTA 服务器发送的第一密文，所述第一密文为第一服务器根据第一安全参数对所述目标零部件的升级数据加密得到的，所述第一服务器为用于提供所述目标零部件的升级数据的服务器，所述第一安全参数为所述第一服务器与所述第一终端之间的共享密钥或者为所述第一终端的第一公钥；

所述第一终端根据第二安全参数解密所述升级包中的第一密文，得到所述目标零部件的升级数据，所述第二安全参数为所述共享密钥或者为所述第一终端的第一私钥；

所述第一终端根据所述目标零部件的升级数据升级所述目标零部件。

29、一种空中下载技术 OTA 升级装置，其特征在于，所述 OTA 升级装置用于提供所述目标零部件的升级数据的装置，所述 OTA 升级装置包括：

处理单元，用于根据第一密钥对目标零部件的升级数据进行加密得到第一密文；

发送单元，用于向 OTA 服务器发送所述第一密文；

所述发送单元，还用于向部署有所述目标零部件的第一终端发送第二密钥，所述第二密钥为所述第一密钥对应的解密密钥。

30、根据权利要求 29 中所述的装置，其特征在于，所述 OTA 升级装置属于所述目标零部件的供应商用于维护所述目标零部件的装置。

31、根据权利要求 29 或 30 中所述的装置，其特征在于，所述发送单元，具体用于：
与部署有所述目标零部件的所述第一终端建立安全通道；
通过所述安全通道向所述第一终端发送所述第二密钥。

32、根据权利要求 29 或 30 中所述的装置，其特征在于，所述处理单元，还用于根据第一安全参数加密所述第二密钥得到第二密文，所述第一安全参数为第一服务器与所述第一终端之间的共享密钥或者为所述第一终端的第一公钥；

所述发送单元，具体用于向部署有所述目标零部件的所述第一终端发送所述第二密文。

33、根据权利要求 32 中所述的装置，其特征在于，所述装置还包括：
接收单元，用于接收来自所述第一终端的密钥获取请求。

34、根据权利要求 32 或 33 中所述的装置，其特征在于，所述第一安全参数属于临时密钥或者属于一次性密钥。

35、根据权利要求 32-34 任一项中所述的装置，其特征在于，所述第一安全参数为所述第一终端的第一公钥；所述接收单元，还用于接收所述第一终端发送的所述目标零部件的第一公钥；

所述处理单元，还用于通过所述第一终端的第一数字证书认证所述第一公钥。

36、根据权利要求 32-34 任一项中所述的装置，其特征在于，所述第一安全参数为所述第一服务器与所述第一终端之间的共享密钥；所述处理单元，还用于：

通过密钥协商算法，与所述第一终端协商得到所述共享密钥；

通过第一服务器和所述第一终端之间的预共享密钥 PSK 认证所述第一终端的身份，所述 PSK 为所述第一服务器与所述目标零部件之间预设的秘密值。

37、根据权利要求 30-36 任一项中所述的装置，其特征在于，所述发送单元，具体用于：

向所述第一终端的升级控制部件发送所述第二密钥；

或者，向所述第一终端的所述目标零部件发送所述第二密钥。

38、一种空中下载技术 OTA 升级装置，其特征在于，包括：

接收单元，用于接收 OTA 服务器发送的第一密文，所述第一密文为第一服务器根据第一密钥对目标零部件的升级数据加密得到的，所述第一服务器为用于提供所述目标零部件的升级数据的服务器；

所述接收单元，还用于接收来自所述第一服务器的第二密钥，所述第二密钥为所述第一密钥对应的解密密钥；

处理单元，用于通过所述第二密钥解密所述第一密文，得到所述目标零部件的升级数

据；

所述处理单元，还用于通过所述目标零部件的升级数据，升级所述目标零部件。

39、根据权利要求 38 中所述的装置，其特征在于，所述处理单元，还用于与所述第一服务器建立安全通道；

所述接收单元，具体用于通过所述安全通道接收所述第一服务器的所述第二密钥。

40、根据权利要求 38 中所述的装置，其特征在于，

所述接收单元，具体用于接收来自所述第一服务器的第二密文；所述第二密文为根据第一安全参数加密第二密钥得到的；

所述处理单元，还用于根据第二安全参数解密所述第二密文，得到所述第二密钥，所述第二安全参数为所述第一服务器与所述第一终端之间的共享密钥或者为所述第一终端的第一私钥。

41、根据权利要求 40 中所述的装置，其特征在于，所述装置还包括：

发送单元，用于向所述第一服务器发送密钥获取请求。

42、根据权利要求 40 或 41 中所述的装置，其特征在于，所述第二安全参数属于临时密钥或者属于一次性密钥。

43、根据权利要求 41-42 任一项中所述的装置，其特征在于，

所述第二安全参数为所述第一公钥对应的第一私钥，所述第一安全参数为所述第一终端的第一公钥；

所述第一公钥通过所述第一终端的第一数字证书进行认证。

44、根据权利要求 41-42 任一项中所述的装置，其特征在于，所述第一安全参数为所述第一服务器与所述第一终端之间的共享密钥；所述处理单元，还用于：

通过密钥协商算法，与所述第一服务器协商得到所述共享密钥；

通过所述第一服务器和所述第一终端之间的预共享密钥 PSK 认证所述第一服务器的身份，所述 PSK 为所述第一服务器与所述目标零部件之间预设的秘密值。

45、根据权利要求 38-44 中任一项所述的装置，其特征在于，所述 OTA 升级装置具体为第一终端中的所述目标零部件；

或者，所述 OTA 升级装置具体为所述第一终端中的升级控制部件。

46、一种 OTA 升级装置，其特征在于，所述 OTA 升级装置为用于提供所述目标零部件的升级数据的装置，所述 OTA 升级装置包括：

发送单元，用于向 OTA 服务器发送目标零部件的升级数据的元数据，所述升级数据的

元数据包含所述升级数据的第一下载地址和所述升级数据的版本信息；

所述发送单元，还用于通过安全通道向部署有所述目标零部件的第一终端发送所述目标零部件的升级数据，所述安全通道为所述第一终端根据所述第一下载地址与第一服务器共同建立的。

47、根据权利要求46中所述的装置，其特征在于，所述OTA升级装置属于所述目标零部件的供应商用于维护所述目标零部件的装置。

48、一种空中下载技术OTA升级装置，其特征在于，所述OTA升级装置中部署有目标零部件，所述OTA升级装置包括：

接收单元，用于接收OTA服务器发送的下载策略，所述下载策略中包含所述目标零部件的升级数据的第一下载地址；

所述处理单元，还用于基于所述第一下载地址，与第一服务器共同建立安全通道，所述第一服务器为用于提供所述目标零部件的升级数据的服务器；

接收单元，用于通过所述安全通道接收所述第一服务器发送的所述目标零部件的升级数据；

所述处理单元，还用于根据所述目标零部件的升级数据升级所述目标零部件。

49、一种空中下载技术OTA升级装置，其特征在于，所述OTA升级装置用于提供所述目标零部件的升级数据的装置，所述OTA升级装置包括：

处理单元，用于根据第一密钥对目标零部件的升级数据进行加密得到第一密文；

所述处理单元，还用于根据第一安全参数的加密第二密钥得到第二密文，其中，所述第一安全参数为第一服务器与所述第一终端之间的共享密钥或者为所述第一终端的第一公钥，所述第一终端为部署有第一目标零部件的终端，所述第一目标零部件为所述目标零部件中的一个，所述第二密钥为所述第一密钥的解密密钥；

发送单元，用于向OTA服务器发送所述第一密文和所述第二密文，所述第二密文用于部署有所述第一目标零部件的第一终端解密所述第一密文。

50、根据权利要求49中所述的装置，其特征在于，所述OTA升级装置属于所述目标零部件的供应商用于维护所述目标零部件的装置。

51、一种空中下载技术OTA升级装置，其特征在于，包括：

接收单元，用于接收第一服务器发送的第一密文和第二密文，其中，所述第一密文为根据第一密钥对目标零部件的升级数据加密得到的，所述第二密文为根据第一安全参数对第二密钥加密得到的，所述第一安全参数为所述第一服务器与第一终端之间的共享密钥或者为所述第一终端的第一公钥，所述第一终端为部署有第一目标零部件的终端，所述第一目标零部件为所述目标零部件中的一个，所述第二密钥为所述第一密钥的解密密钥，所述第一服务器为用于提供所述目标零部件的升级数据的服务器；

发送单元，用于向所述第一终端发送所述第一密文和所述第二密文，其中所述第二密文用于所述第一终端解密所述第一密文，以得到所述目标零部件的升级数据。

52、根据权利要求 51 中所述的装置，其特征在于，所述装置，还包括：

处理单元，用于根据所述第一密文所在的升级包的属性和所述第一终端的信息生成升级策略；所述升级策略包括所述第一密文和所述第二密文的第一下载地址；

所述发送单元，还用于向所述第一终端发送所述升级策略；

所述发送单元，还用于通过安全通道向所述第一终端发送所述第一密文和所述第二密文，所述安全通道为所述第一终端根据所述第一下载地址与所述 OTA 服务器共同建立的。

53、一种空中下载技术 OTA 升级装置，其特征在于，所述 OTA 升级装置中部署有第一目标零部件，所述第一目标零部件为目标零部件中的一个，所述 OTA 升级装置包括：

接收单元，用于接收 OTA 服务器发送的第一密文和第二密文，所述第一密文为第一服务器根据第一密钥对所述目标零部件的升级数据加密得到的，其中所述第一服务器为用于提供所述目标零部件的升级数据的服务器；

处理单元，用于根据第二安全参数解密所述第二密文得到第二密钥，所述第二密钥为所述第一密钥的解密密钥，所述第二安全参数为所述第一服务器与所述第一终端之间的共享密钥或者为所述第一终端的第一私钥；

所述处理单元，还用于根据所述第二密钥解密所述第一密文，得到所述目标零部件的升级数据；

所述处理单元，还用于根据所述目标零部件的升级数据升级所述第一目标零部件。

54、根据权利要求 53 中所述的装置，其特征在于，

所述 OTA 升级装置具体为所述第一终端中的所述目标零部件；

或者，所述 OTA 升级装置具体为所述第一终端中的所述升级控制部件。

55、一种 OTA 升级装置，其特征在于，所述 OTA 升级装置为用于提供所述目标零部件的升级数据的装置，所述 OTA 升级装置包括：

处理单元，用于根据第一安全参数对目标零部件的升级数据进行加密得到第一密文，所述第一安全参数为预置的第一服务器与部署有所述目标零部件的第一终端之间的共享密钥或者为预置的部署有所述目标零部件的第一终端的第一公钥；

发送单元，用于向 OTA 服务器发送所述第一密文；所述第一密文用于由所述 OTA 服务器发送给第一终端以对所述第一终端中的所述目标零部件进行升级。

56、一种空中下载技术 OTA 升级装置，其特征在于，所述 OTA 升级装置中部署有第一目标零部件，所述第一目标零部件为目标零部件中的一个，所述 OTA 升级装置包括：

接收单元，用于接收 OTA 服务器发送的第一密文，所述第一密文为第一服务器根据第一安全参数对所述目标零部件的升级数据加密得到的，所述第一服务器为用于提供所述目

标零部件的升级数据的服务器，所述第一安全参数为所述第一服务器与所述第一终端之间的共享密钥或者为所述第一终端的第一公钥；

所述接收单元，还用于根据第二安全参数解密所述升级包中的第一密文，得到所述目标零部件的升级数据，所述第二安全参数为所述共享密钥或者为所述第一终端的第一私钥；

所述处理单元，还用于根据所述目标零部件的升级数据升级所述目标零部件。

57、一种空中下载技术 OTA 升级装置，其特征在于，所述装置包括至少一个处理器和通信接口，所述通信接口用于发送和/或接收数据，所述至少一个处理器用于调用至少一个存储器中存储的计算机程序，以使得所述装置实现如权利要求 1-28 中任一项所述的方法。

58、一种空中下载技术 OTA 升级系统，其特征在于，所述系统包括第一服务器和目标零部件，其中：

所述第一服务器用于实现如权利要求 1-9 中任一项所述的 OTA 升级方法，所述目标零部件用于实现包含权利要求 10-17 中任一项所述的 OTA 升级方法；

或者，第一服务器用于实现如权利要求 18 或者 19 中所述的 OTA 升级方法，所述目标零部件用于实现如权利要求 20 所述的 OTA 升级方法；

或者，第一服务器用于实现如权利要求 21 或者 22 中任一项所述的 OTA 升级方法，所述目标零部件用于实现如权利要求 25 或者 26 中任一项所述的 OTA 升级方法；

或者，第一服务器用于实现如权利要求 27 中所述的 OTA 升级方法，所述目标零部件用于实现如包含权利要求 28 中所述的 OTA 升级方法。

59、一种空中下载技术 OTA 升级系统，其特征在于，所述系统包括 OTA 服务器和第一终端，其中：

所述 OTA 服务器用于实现如权利要求 23 或者 24 中所述的 OTA 升级方法，所述第一终端包含权利要求 25 或者 26 中所述的 OTA 升级方法。

60、一种计算机可读存储介质，其特征在于，所述计算机可读存储介质中存储有计算机程序，当所述计算机程序在一个或多个处理器上运行时，执行如权利要求 1-28 中任一项所述的方法。

61、一种计算机产品，其特征在于，当所述计算机产品在一个或多个处理器上运行时，执行如权利要求 1-28 中任一项所述的方法。

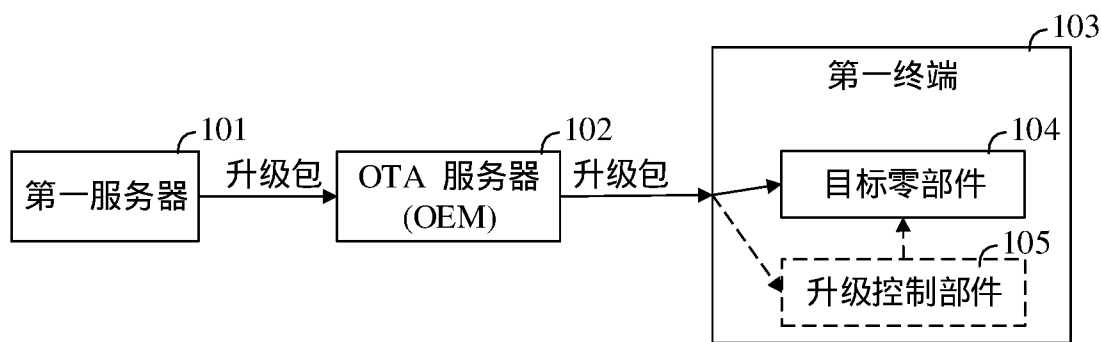


图 1

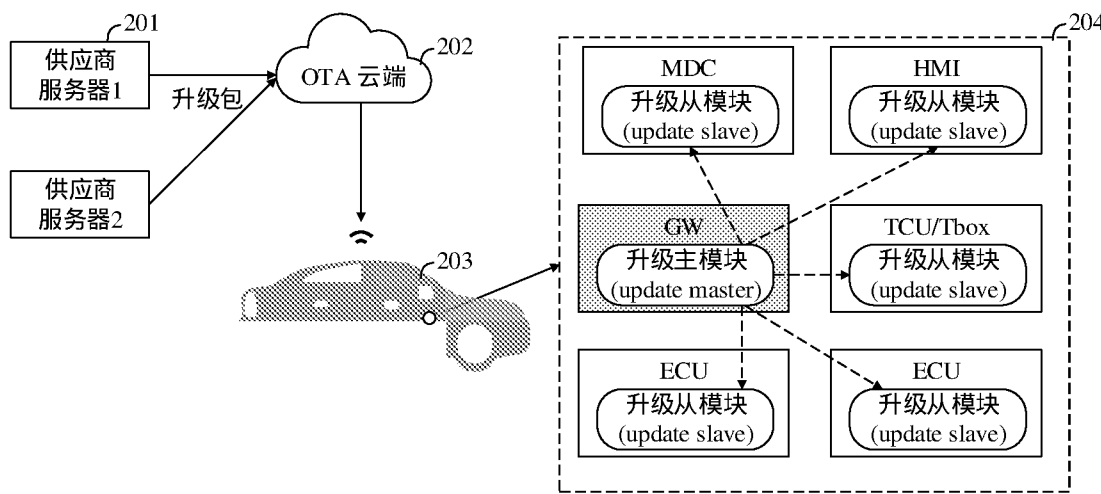


图 2

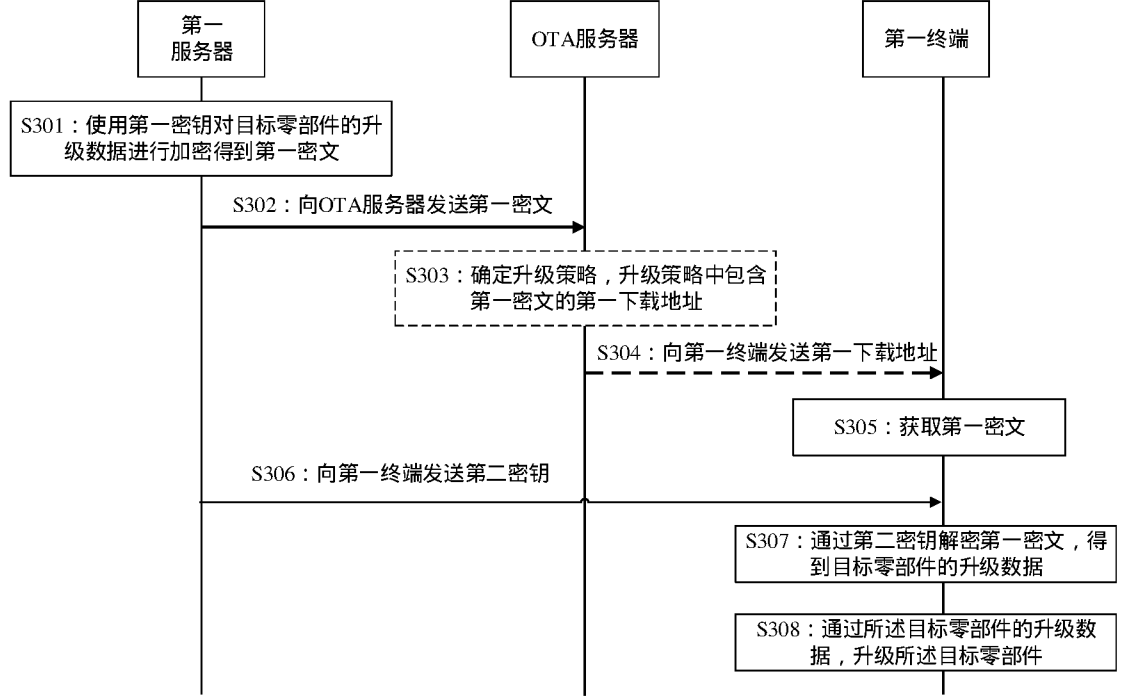


图 3

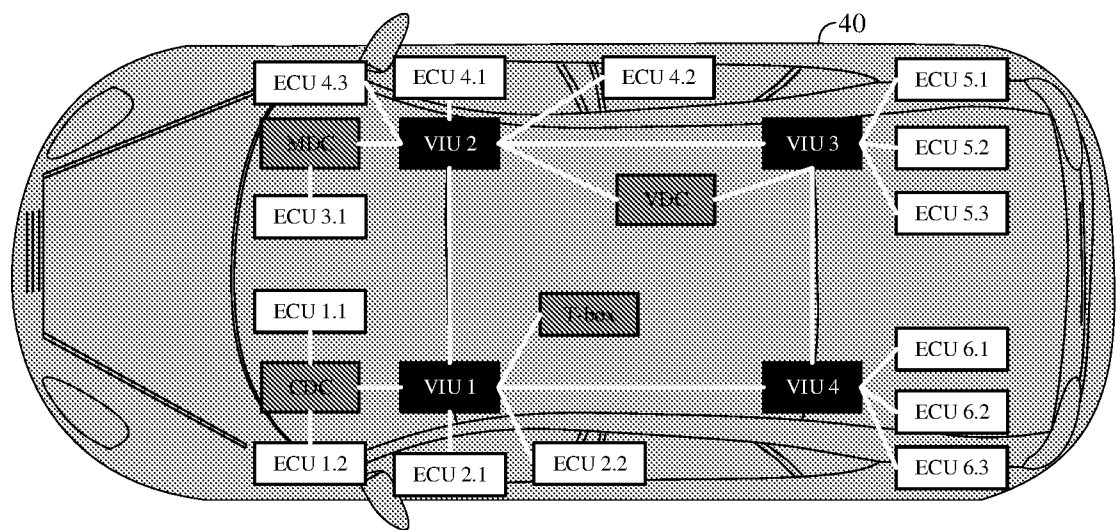


图 4

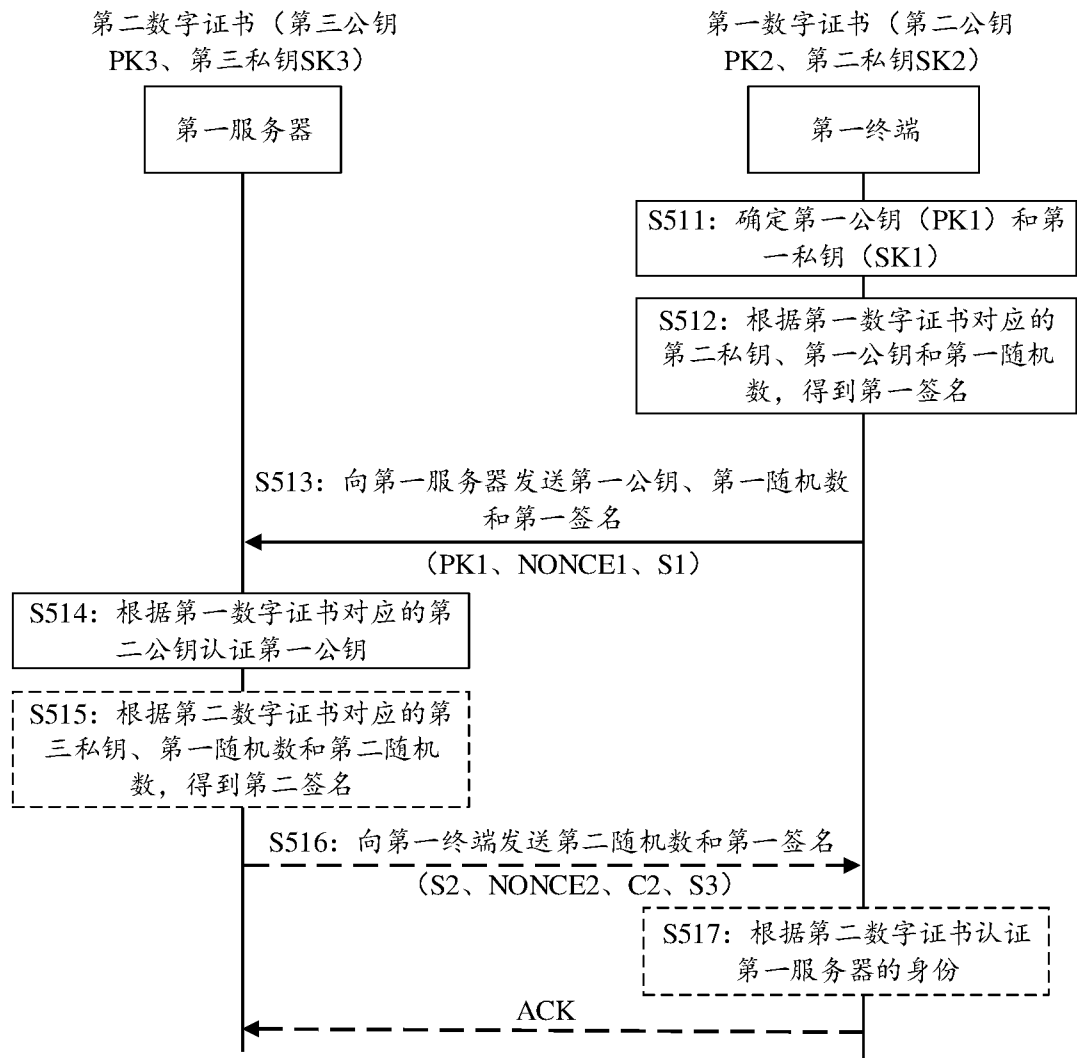


图 5

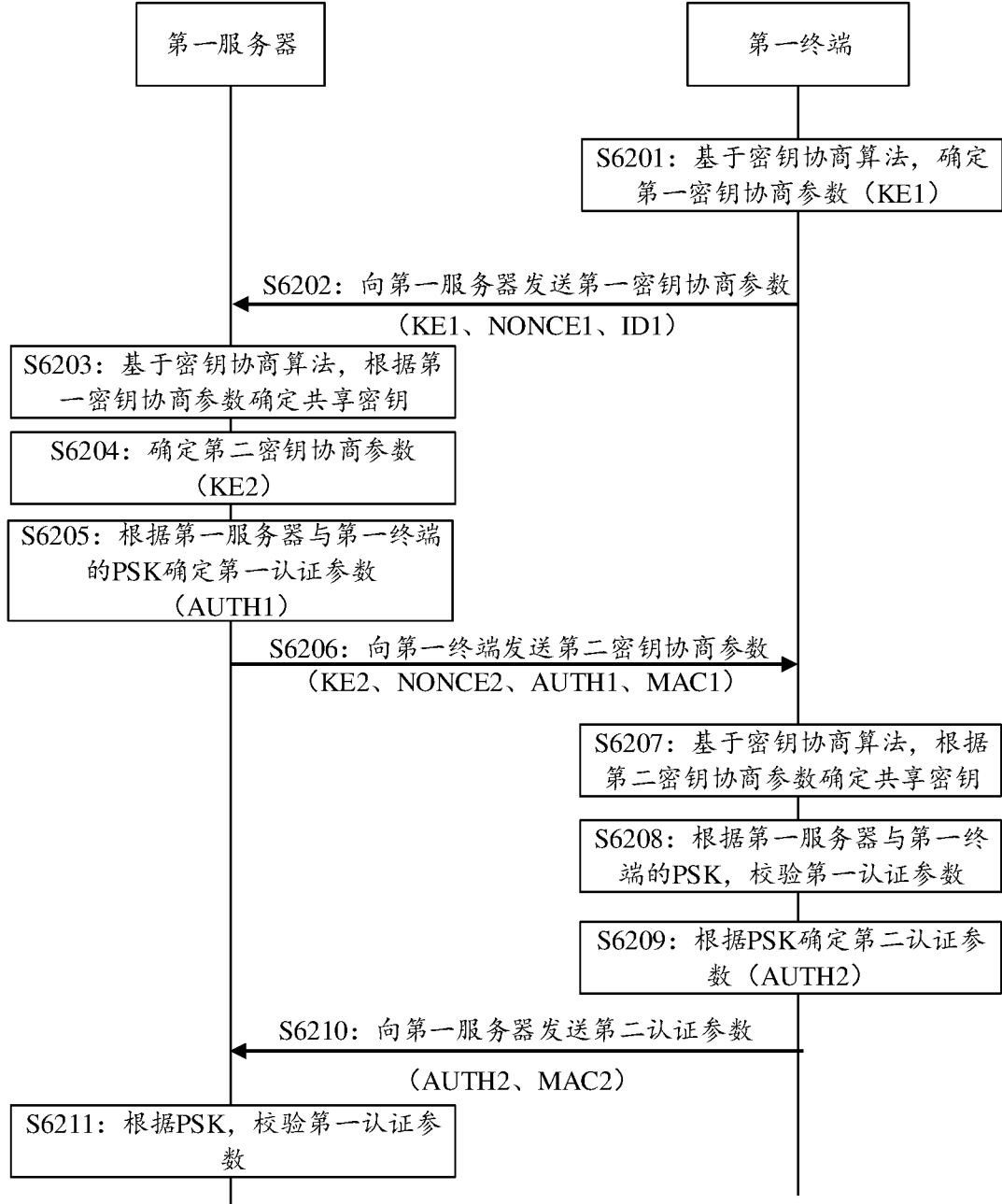


图 6

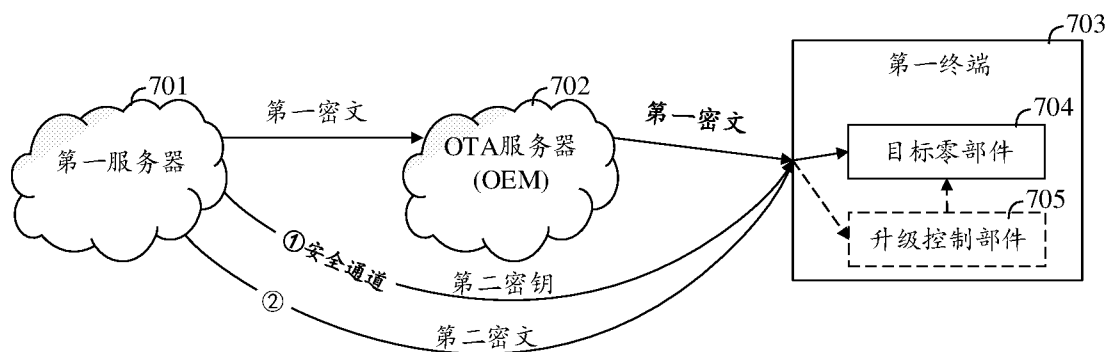


图 7

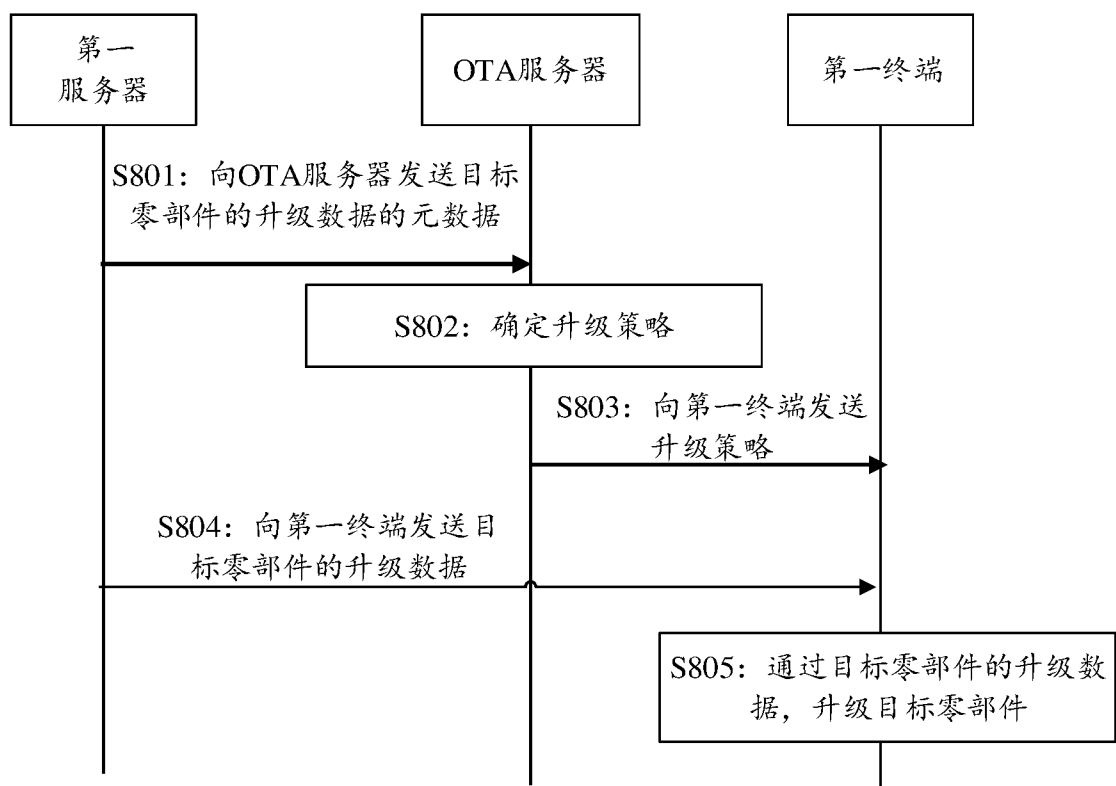


图 8

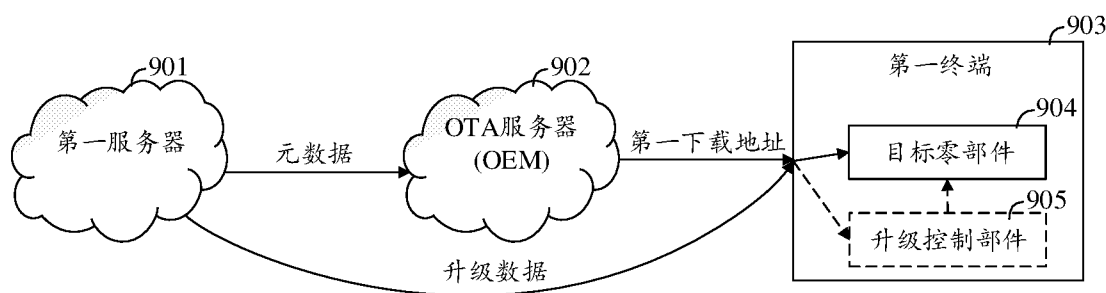


图 9

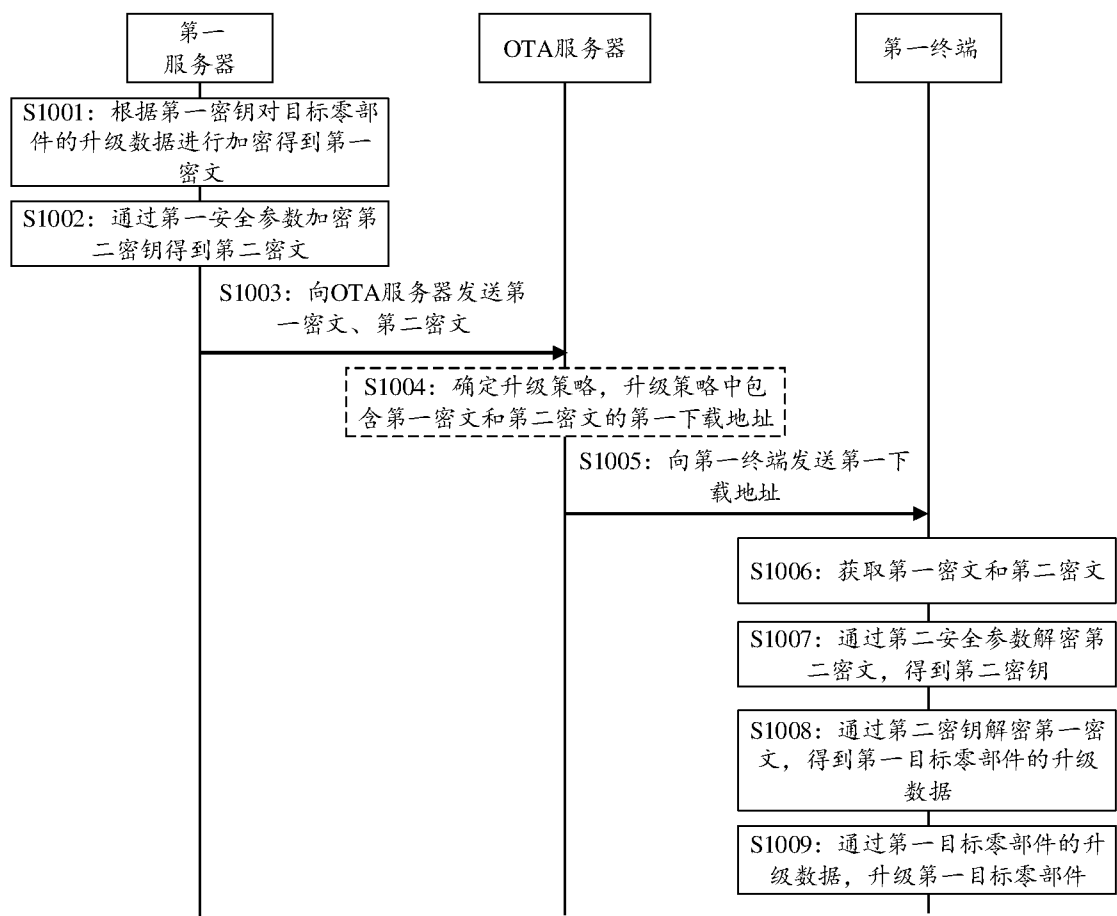


图 10

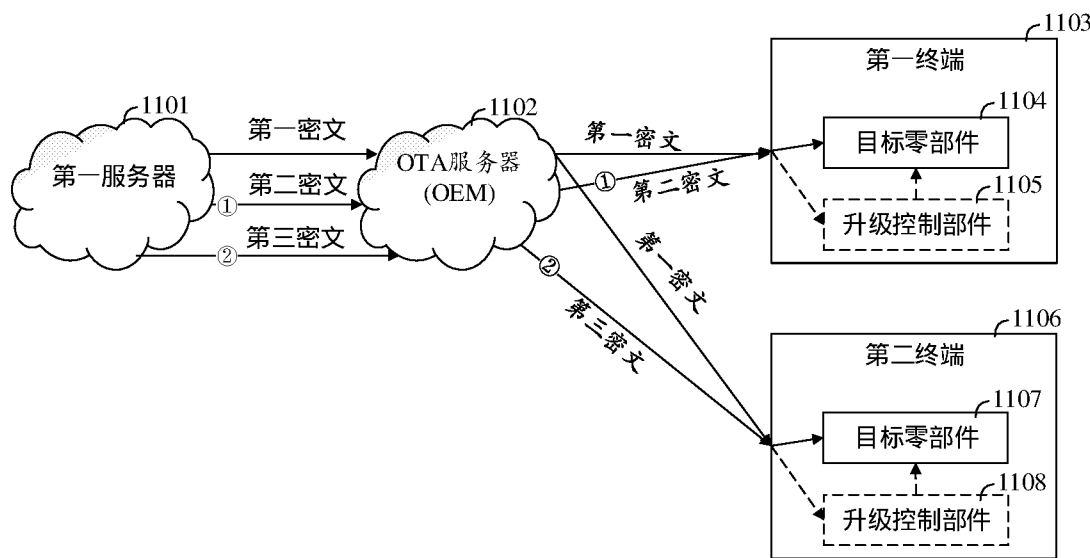


图 11

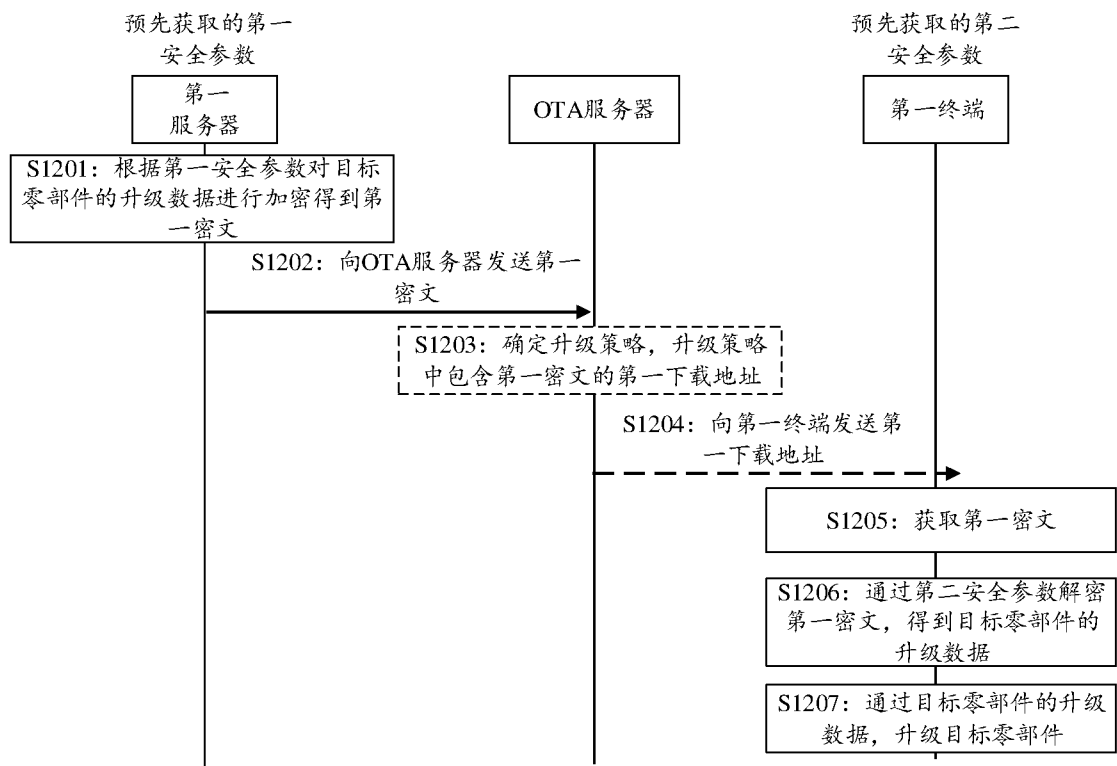


图 12

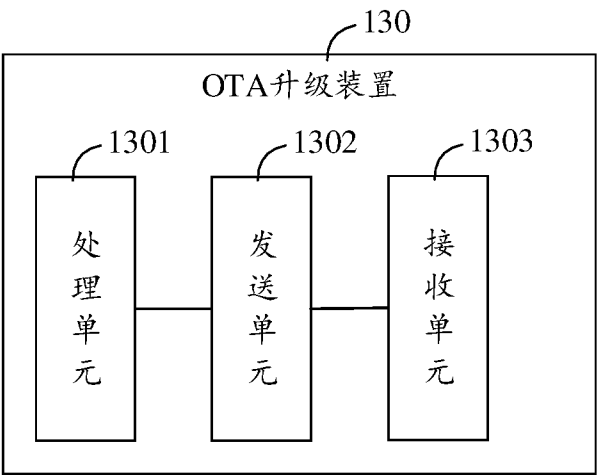


图 13

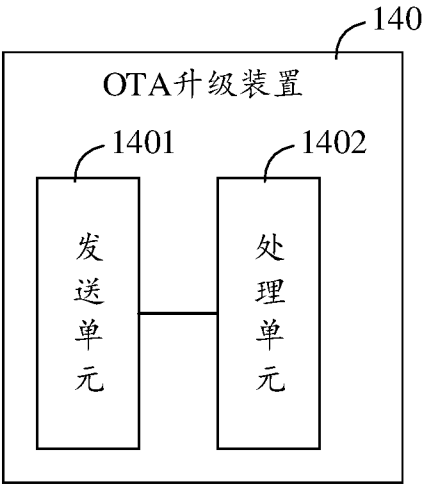


图 14

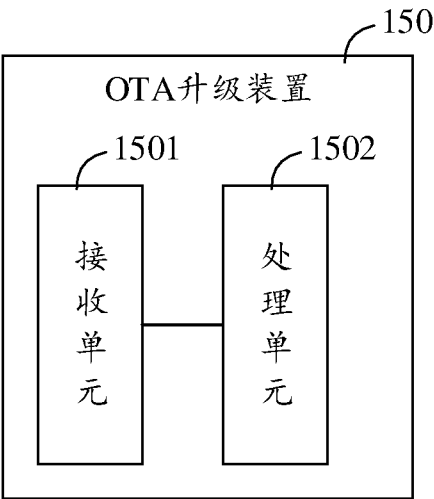


图 15

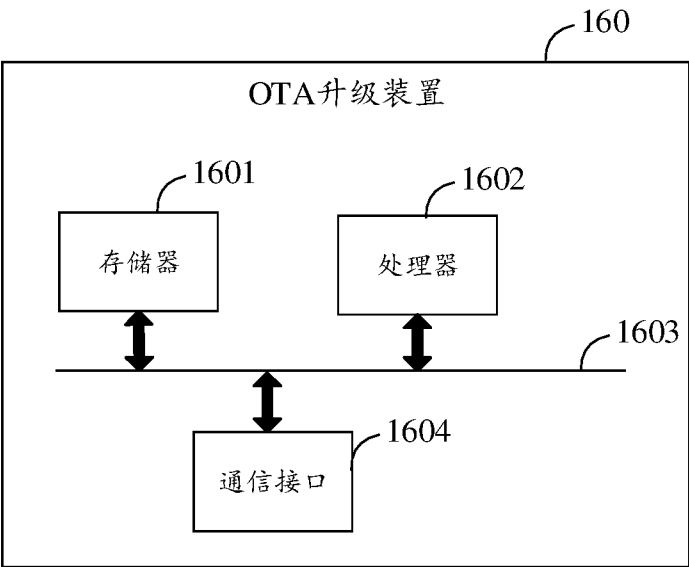


图 16

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2020/140094

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/08(2006.01)i; G06F 8/65(2018.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, EPODOC, WPI: OTA, 加密, 解密, 秘钥, 密钥, 公钥, 私钥, 密文, PSK, 请求, 值, 算法, 协商, 安全通道, 升级, 服务器, encryption, decryption, key, public key, private key, ciphertext, request, value, algorithm, negotiation, secure channel, upgrade, server

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2019083440 A2 (HUAWEI INTERNATIONAL PTE. LTD.) 02 May 2019 (2019-05-02) description, page 7, fifth-to-last paragraph to page 20, paragraph 1, and page 24, fifth-to-last paragraph to the end, and figures 1, 4, and 5	1-17, 21-45, 49-61
A	CN 111079163 A (STATE GRID SHANDONG ELECTRIC POWER COMPANY WEIHAI CITY WENDENG DISTRICT POWER SUPPLY COMPANY et al.) 28 April 2020 (2020-04-28) entire document	1-17, 21-45, 49-61
A	CN 110597538 A (GUANGZHOU XIAOPENG MOTORS TECHNOLOGY CO., LTD.) 20 December 2019 (2019-12-20) entire document	1-17, 21-45, 49-61
A	WO 2020101936 A1 (THIRDWAYV, INC.) 22 May 2020 (2020-05-22) entire document	1-17, 21-45, 49-61



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

24 August 2021

Date of mailing of the international search report

28 September 2021

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing
100088, China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

- [1] First group: related solutions in claims 1-17, 21-45, 49-56, and 59 and claims 57, 58, 60, and 61;
- [2] Second group: related solutions in claims 18-20 and 46-48 and claims 57, 58, 60, and 61.
- [3] The first group of technical solutions relate to encrypting and decrypting data by using a key in OTA upgrade, and the second group of technical solutions relate to sending/receiving upgrade data by means of a secure channel in OTA upgrade. A corresponding technical feature between the two groups of technical solutions is only that OTA upgrade is implemented by using a server. However, the feature is commonly known in the art. Therefore, the two groups of technical solutions do not belong to a single inventive concept.

- 1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
- 2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.
- 3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
- 4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.: **1-17, 21-45, 49-61**

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
- ☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
- ☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2020/140094

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
WO	2019083440	A2	02 May 2019	CN	111279310	A	12 June 2020
				JP	2021500816	A	07 January 2021
				US	2020264864	A1	20 August 2020
				EP	3690643	A2	05 August 2020
CN	111079163	A	28 April 2020	None			
CN	110597538	A	20 December 2019	None			
WO	2020101936	A1	22 May 2020	US	2020151335	A1	14 May 2020

国际检索报告

国际申请号

PCT/CN2020/140094

A. 主题的分类 H04L 9/08(2006.01)i; G06F 8/65(2018.01)i 按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类																	
B. 检索领域 检索的最低限度文献(标明分类系统和分类号) H04L G06F 包含在检索领域中的除最低限度文献以外的检索文献 在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用)) CNPAT, CNKI, EPDOC, WPI:OTA, 加密, 解密, 秘钥, 密钥, 公钥, 私钥, 密文, PSK, 请求, 值, 算法, 协商, 安全通道, 升级, 服务器, encryption, decryption, key, public key, private key, ciphertext, request, value, algorithm, negotiation, secure channel, upgrade, server																	
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>X</td> <td>WO 2019083440 A2 (HUAWEI INTERNATIONAL PTE. LTD.) 2019年 5月 2日 (2019 - 05 - 02) 说明书第7页倒数第5段-第20页第1段, 第24页倒数第5段-结尾, 附图1、4、5</td> <td>1-17, 21-45, 49-61</td> </tr> <tr> <td>A</td> <td>CN 111079163 A (国网山东省电力公司威海市文登区供电公司等) 2020年 4月 28日 (2020 - 04 - 28) 全文</td> <td>1-17, 21-45, 49-61</td> </tr> <tr> <td>A</td> <td>CN 110597538 A (广州小鹏汽车科技有限公司) 2019年 12月 20日 (2019 - 12 - 20) 全文</td> <td>1-17, 21-45, 49-61</td> </tr> <tr> <td>A</td> <td>WO 2020101936 A1 (THIRDWAYV, INC.) 2020年 5月 22日 (2020 - 05 - 22) 全文</td> <td>1-17, 21-45, 49-61</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	X	WO 2019083440 A2 (HUAWEI INTERNATIONAL PTE. LTD.) 2019年 5月 2日 (2019 - 05 - 02) 说明书第7页倒数第5段-第20页第1段, 第24页倒数第5段-结尾, 附图1、4、5	1-17, 21-45, 49-61	A	CN 111079163 A (国网山东省电力公司威海市文登区供电公司等) 2020年 4月 28日 (2020 - 04 - 28) 全文	1-17, 21-45, 49-61	A	CN 110597538 A (广州小鹏汽车科技有限公司) 2019年 12月 20日 (2019 - 12 - 20) 全文	1-17, 21-45, 49-61	A	WO 2020101936 A1 (THIRDWAYV, INC.) 2020年 5月 22日 (2020 - 05 - 22) 全文	1-17, 21-45, 49-61
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求															
X	WO 2019083440 A2 (HUAWEI INTERNATIONAL PTE. LTD.) 2019年 5月 2日 (2019 - 05 - 02) 说明书第7页倒数第5段-第20页第1段, 第24页倒数第5段-结尾, 附图1、4、5	1-17, 21-45, 49-61															
A	CN 111079163 A (国网山东省电力公司威海市文登区供电公司等) 2020年 4月 28日 (2020 - 04 - 28) 全文	1-17, 21-45, 49-61															
A	CN 110597538 A (广州小鹏汽车科技有限公司) 2019年 12月 20日 (2019 - 12 - 20) 全文	1-17, 21-45, 49-61															
A	WO 2020101936 A1 (THIRDWAYV, INC.) 2020年 5月 22日 (2020 - 05 - 22) 全文	1-17, 21-45, 49-61															
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。																	
<table border="0"> <tr> <td> * 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件 </td> <td> “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件 </td> </tr> </table>			* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件	“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件													
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件	“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件																
国际检索实际完成的日期 2021年 8月 24日		国际检索报告邮寄日期 2021年 9月 28日															
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国 北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451		授权官员 张嘉凯 电话号码 86-(10)-53961760															

第III栏 缺乏发明单一性的意见(续第1页第3项)

本国际检索单位在该国际申请中发现多项发明, 即:

- [1] 第1组: 权利要求1-17, 21-45, 49-56, 59及权利要求57, 58, 60, 61中的相关方案;
- [2] 第2组: 权利要求18-20, 46-48及权利要求57, 58, 60, 61中的相关方案。
- [3] 第1组技术方案涉及在OTA升级中对数据用密钥进行加密和解密, 第2组技术方案涉及在OTA升级中通过安全通道发送 / 接收升级数据。二组技术方案中相应的技术特征只有用服务器实现OTA升级。然而该特征是本领域公知的。因此上述两组技术方案不属于一个发明构思。

1. ☐ 由于申请人按时缴纳了被要求缴纳的全部附加检索费, 本国际检索报告涉及全部可作检索的权利要求。
2. ☐ 由于无需付出有理由要求附加费的劳动即能对全部可检索的权利要求进行检索, 本单位未通知缴纳任何加费。
3. ☐ 由于申请人仅按时缴纳了部分被要求缴纳的附加检索费, 本国际检索报告仅涉及已缴费的那些权利要求, 具体地说, 是权利要求:
4. ☒ 申请人未按时缴纳被要求缴纳的附加检索费。因此, 本国际检索报告仅涉及权利要求书中首先提及的发明; 包含该发明的权利要求是: 1-17, 21-45, 49-61

对异议的意见

- ☐ 申请人缴纳了附加检索费, 同时提交了异议书, 适用时, 缴纳了异议费。
- ☐ 申请人缴纳了附加检索费, 同时提交了异议书, 但未在通知书规定的时间期限内缴纳异议费。
- ☐ 缴纳附加检索费时未提交异议书。

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2020/140094

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
WO	2019083440	A2	2019年 5月 2日	CN	111279310	A	2020年 6月 12日
				JP	2021500816	A	2021年 1月 7日
				US	2020264864	A1	2020年 8月 20日
				EP	3690643	A2	2020年 8月 5日
CN	111079163	A	2020年 4月 28日	无			
CN	110597538	A	2019年 12月 20日	无			
WO	2020101936	A1	2020年 5月 22日	US	2020151335	A1	2020年 5月 14日