(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
2017 年 9 月 14 日 (14.09.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/152875 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2017/076295

(22) 国际申请日: 2017 年 3 月 10 日 (10.03.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610141465.8 2016 年 3 月 11 日 (11.03.2016) CN

(71) 申请人: **比亚迪股份有限公司 (BYD COMPANY LIMITED)** [CN/CN]; 中国广东省深圳市坪山新区比亚迪路 3009 号, Guangdong 518118 (CN)。

(72) 发明人: **武新峰 (WU, Xinfeng)**; 中国广东省深圳市坪山新区比亚迪路 3009 号, Guangdong 518118 (CN)。 **尹建银 (YIN, Jianyin)**; 中国广东省深圳市坪山新区比亚迪路 3009 号, Guangdong 518118 (CN)。

(74) 代理人: **北京清亦华知识产权代理事务所（普通合伙） (TSINGYIHUA INTELLECTUAL PROPERTY LLC)**; 中国北京市海淀区清华园清华大学照澜院商业楼 301 室, Beijing 100084 (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, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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,

[见续页]

(54) **Title**: SECURE COMMUNICATION METHOD AND APPARATUS FOR VEHICLE, VEHICLE MULTIMEDIA SYSTEM, AND VEHICLE

(54) **发明名称** : 车辆安全通信方法、装置、车辆多媒体系统及车辆

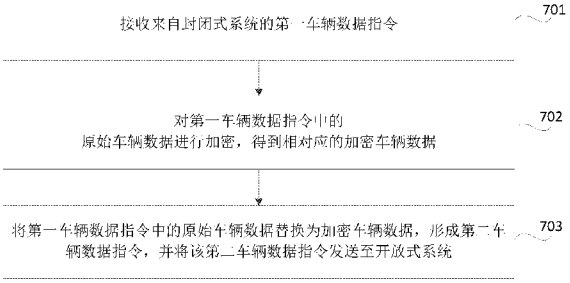


图7

701 Receive a first vehicle data instruction from a closed system
702 Encrypt the original vehicle data in the first vehicle data instruction to obtain the corresponding encrypted vehicle data
703 Replace the original vehicle data in the first vehicle data instruction by using the encrypted vehicle data, so as to form a second vehicle data instruction, and send the second vehicle data instruction to an open system

(57) **Abstract**: Disclosed in the present application are a secure communication method and apparatus for a vehicle, a vehicle multimedia system, and the vehicle. The vehicle comprises an open system, a secure chip, and a closed system. The open system and the closed system are connected by means of the secure chip. The method is applied to the security chip, and the method comprises: receiving a first vehicle data instruction from a closed system, the first vehicle data instruction comprising original vehicle data; encrypting the original vehicle data to obtain the corresponding encrypted vehicle data; and replacing the original vehicle data in the first vehicle data instruction by using the encrypted vehicle data, so as to form a second vehicle data instruction, and sending the second vehicle data instruction to an open system.

(57) **摘要**: 本申请公开了一种车辆安全通信方法、装置、车辆多媒体系统及车辆。车辆包括开放式系统、安全芯片和封闭式系统，开放式系统与封闭式系统之间通过安全芯片连接，方法应用于安全芯片，并且方法包括：接收来自封闭式系统的第一车辆数据指令，其中，第一车辆数据指令包括原始车辆数据；对原始车辆数据进行加密，得到相对应的加密车辆数据；将第一车辆数据指令中的原始车辆数据替换为加密车辆数据，形成第二车辆数据指令，并将第二车辆数据指令发送至开放式系统。

WO 2017/152875 A1

IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, 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))。

车辆安全通信方法、装置、车辆多媒体系统及车辆

相关申请的交叉引用

本申请基于申请号为201610141465.8，申请日为2016年3月11日的中国专利申请提出，并要求该中国专利申请的优先权，该中国专利申请的全部内容在此引入本申请作为参考。

技术领域

本申请涉及车联网领域，具体地，涉及一种车辆安全通信方法、装置、车辆多媒体系统及车辆。

背景技术

随着车载多媒体的大屏化的发展和车联网以及4G、WIFI热点的普及，车载多媒体逐渐成为车主的另一个重要的移动终端系统，原有小屏幕的传统车机封闭式系统渐渐无法满足用户越来越多的娱乐化和多媒体化需求。目前，许多车载多媒体都开始搭载4G模块和WIFI模块，可以接入互联网，并允许客户自行安装偏好的APP应用。另外，随着大数据和云服务的发展，出现了远程控制车机的技术，车载多媒体是接受云服务的载体，但是这样会给客户带来很大的安全隐患，因为车载多媒体和整车其他部件存在通信和互联，车载多媒体会发出很多控制整车其他部件的指令，一旦联网之后，车载多媒体就像电脑和手机一样，容易遭到恶意程序的入侵，不法分子会远程模拟云服务器给汽车发送错误指令。一旦被恶意入侵，可能会导致不法分子获取车辆相关的数据信息，导致车辆数据的泄露，所以对车载多媒体接入互联网时进行必要的信息安全保障是很有必要的。

发明内容

本申请的目的是提供一种车辆安全通信方法、装置、车辆多媒体系统及车辆，以提高车辆联网通信时的安全性。

为了实现上述目的，根据本申请的第一方面，提供了一种车辆安全通信方法，所述车辆包括开放式系统、安全芯片和封闭式系统，所述开放式系统与所述封闭式系统之间通过所述安全芯片连接，所述方法应用于所述安全芯片，并且所述方法包括：接收来自所述封闭式系统的第一车辆数据指令，其中，所述第一车辆数据指令包括原始车辆数据；对所述原始车辆数据进行加密，得到相对应的加密车辆数据；将所述第一车辆数据指令中的所述原始车辆数据替换为所述加密车辆数据，形成第二车辆数据指令，并将所述第二车辆数据指令发送至所述开放式系统。

根据本申请的第二方面，提供了一种车辆安全通信方法，所述车辆包括开放式系统、安

全芯片和封闭式系统，所述开放式系统与所述封闭式系统之间通过所述安全芯片连接，所述开放式系统与服务器连接，所述方法应用于所述服务器，并且所述方法包括：接收来自所述开放式系统的车辆数据指令，其中，所述车辆数据指令是由所述开放式系统从所述安全芯片转发的，并且所述车辆数据指令包括加密车辆数据；对所述车辆数据指令中的所述加密车辆数据进行解密；当解密成功时，得到解密车辆数据；以及处理所述解密车辆数据。

根据本申请的第三方面，提供了一种车辆安全通信装置，所述车辆包括开放式系统、安全芯片和封闭式系统，所述开放式系统与所述封闭式系统之间通过所述安全芯片连接，所述装置配置于所述安全芯片，并且所述装置包括：第一接收模块，被配置为接收来自所述封闭式系统的第一车辆数据指令，其中，所述第一车辆数据指令包括原始车辆数据；加密模块，被配置为对所述原始车辆数据进行加密，得到相对应的加密车辆数据；发送模块，被配置为将所述第一车辆数据指令中的所述原始车辆数据替换为所述加密车辆数据，形成第二车辆数据指令，并将所述第二车辆数据指令发送至所述开放式系统。

根据本申请的第四方面，提供了一种车辆安全通信装置，所述车辆包括开放式系统、安全芯片和封闭式系统，所述开放式系统与所述封闭式系统之间通过所述安全芯片连接，所述开放式系统与服务器连接，所述装置配置于所述服务器，并且所述装置包括：第二接收模块，被配置为接收来自所述开放式系统的车辆数据指令，其中，所述车辆数据指令是由所述开放式系统从所述安全芯片转发的，并且所述车辆数据指令包括加密车辆数据；解密模块，被配置为对所述车辆数据指令中的所述加密车辆数据进行解密，当解密成功时，得到解密车辆数据；以及处理模块，被配置为处理所述解密车辆数据。

根据本申请的第五方面，提供了一种车辆多媒体系统，所述车辆多媒体系统包括：封闭式系统，用于采集原始车辆数据，并发送包括所述原始车辆数据的第一车辆数据指令；安全芯片，该安全芯片包括根据本申请的第三方面提供的所述车辆安全通信装置；开放式系统，所述开放式系统与所述封闭式系统之间通过所述安全芯片通信，并且所述开放式系统还与服务器进行通信，所述开放式系统用于接收来自所述安全芯片的所述第二车辆数据指令，并将所述第二车辆数据指令转发至所述服务器。

根据本申请的第六方面，提供了一种车辆，该车辆包括根据本申请的第五方面提供的车辆多媒体系统。

在上述技术方案中，通过安全芯片对来自封闭式系统的车辆数据进行加密处理，并通过开放式系统将经过加密处理的车辆数据发送至服务器，由服务器进行解密处理，只有在解密成功时，服务器才能获取到来自封闭式系统的车辆数据。由此，能够避免非法的服务器所有者获悉车辆信息，从而确保车辆信息的安全性。

本申请的其他特征和优点将在随后的具体实施方式部分予以详细说明。

附图说明

附图是用来提供对本申请的进一步理解，并且构成说明书的一部分，与下面的具体实施方式一起用于解释本申请，但并不构成对本申请的限制。在附图中：

图 1 是根据一示例性实施例示出的一种实施环境的示意图。

图 2 是根据一示例性实施例示出的一种配置在车辆中的车辆多媒体系统的结构框图。

图 3 是根据一示例性实施例示出的一种车辆安全通信方法的流程图。

图 4 是根据一示例性实施例示出的另一种车辆安全通信方法的流程图。

图 5 是根据一示例性实施例示出的一种在车辆通信过程中，用户终端、服务器、开放式系统、安全芯片、以及封闭式系统之间的信令交互图。

图 6A 是一种示例第一控制指令的组成示意图。

图 6B 是另一种示例第一控制指令的组成示意图。

图 6C 是一种示例第二控制指令的组成示意图。

图 7 是根据另一示例性实施例示出的一种车辆安全通信方法的流程图。

图 8 是一种示例第一车辆数据指令的组成示意图。

图 9 是根据另一示例性实施例示出的另一种车辆安全通信方法的流程图。

图 10 是根据另一示例性实施例示出的一种在车辆通信过程中，服务器、开放式系统、安全芯片、以及封闭式系统之间的信令交互图。

图 11A 是另一种示例第一车辆数据指令的组成示意图。

图 11B 是一种示例第二车辆数据指令的组成示意图。

图 11C 是另一种示例第一车辆数据指令的组成示意图。

图 12 是根据一示例性实施例示出的一种车辆安全通信装置的框图。

图 13 是根据另一示例性实施例示出的一种车辆安全通信装置的框图。

具体实施方式

以下结合附图对本申请的具体实施方式进行详细说明。应当理解的是，此处所描述的具体实施方式仅用于说明和解释本申请，并不用于限制本申请。

图 1 是根据一示例性实施例示出的一种实施环境的示意图。如图 1 所示，该实施环境可以包括用户终端 100、服务器 200 和车辆 300。

在本申请中，服务器 200 可以是为车辆 300 提供服务的电子设备，其可以由车辆 300 的服务提供商所有。用户能够通过用户终端 100 在服务器 200 上进行注册，使用户终端 100 与车辆 300 相关联，这样，用户终端 100 能够经由服务器 200 与车辆 300 进行通信，从而实现用户对车辆 300 的远程控制。另外，车辆 300 也可以将车辆相关的数据反馈给服务器 200，以便服务提供商对车辆 300 进行远程维护，并且如果需要，服务器 200 还可以将该车辆相关的数据反馈给用户终端 100，从而使用户能够随时掌握车辆状况。

在本申请中，用户终端 100 可以是能够联网、与服务器 200 进行通信的电子设备。用户

终端 100 可以例如是智能手机、平板电脑、PC 机、笔记本电脑等等。图 1 中以用户终端 100 是智能手机来示意。

为了提高车辆 300 在联网时的安全性，在本申请的实施例中，在车辆 300 中配置了具有双系统的车辆多媒体系统，图 2 是根据一示例性实施例示出的一种配置在车辆中的车辆多媒体系统的结构框图。如图 2 所示，该车辆多媒体系统可以包括：开放式系统 301 和封闭式系统 302。其中，开放式系统 301 用于车辆 300 联网、与外部设备（例如，服务器 200）进行通信，并且允许用户根据喜好安装各种 APP 应用。示例地，开放式系统 301 中可以配置有开放式核心板 303 和联网模块 304（该联网模块 304 可以例如为 WiFi 模块、GPS 模块、3G 模块、4G 模块等等），其中，开放式核心板 303 与联网模块 304 连接，能够通过该联网模块 304 进行联网操作，以与外部设备（例如，服务器 200）通信。

封闭式系统 302 不被允许接入互联网，其用于与整车进行交互通信。示例地，封闭式系统 302 中可以配置有车辆 300 的微控制单元 MCU 305，该微控制单元 MCU 305 能够与整车 CAN 总线连接，通过 CAN 总线，微控制单元 MCU 305 能够控制整车操作，以及从 CAN 总线获取车辆数据。开放式系统 301 和封闭式系统 302 之间能保持各自独立运行。此外，开放式系统 301 与封闭式系统 302 之间可以通过安全芯片 306 连接，示例地，开放式核心板 303 与 MCU 305 之间通过安全芯片 306 连接。其中，开放式核心板 303 与安全芯片 306 之间可以通过 SDIO（安全数字输入输出）接口连接，安全芯片 306 与 MCU 305 之间可以通过 SPI（串行外设接口）标准口连接。在本申请的一个示例实施方式中，该安全芯片 306 可以选用 SSX1207 型安全芯片，其可提供数据加密、身份认证、有限安全存储等服务。通过该安全芯片 306，可以提升车辆联网时的安全性。

需要说明的是，作为一种示例，本申请所述的开放式系统 301 和封闭式系统 302 都可以为操作系统。例如，开放式系统 301 可以是安卓系统，封闭式系统 302 可以是 Linux 系统。应当理解，该示例仅仅为了说明开放式系统 301 和封闭式系统 302，并不能限定两个系统。例如，开放式系统 301 可以是 Linux 系统，封闭式系统 302 可以是安卓系统；或者都可以是安卓系统；等等。

图 3 是根据一示例性实施例示出的一种车辆安全通信方法的流程图，其中，该方法可以应用于服务器中，例如，图 1 所示的服务器 200。如图 3 所示，该方法可以包括以下步骤。

在步骤 S301 中，接收来自用户终端的原始控制数据，其中，该原始控制数据用于指示车辆要执行的目标操作。

在本申请中，目标操作可以例如包括但不限于以下：解锁、启动、加速、减速、熄火、锁车、车窗升降、多媒体设备控制（启动、音量调节、切换多媒体文件等）等等。

在步骤 S302 中，对原始控制数据进行加密，得到相对应的加密控制数据。

服务器可以预先与安全芯片约定加密协议，这样，服务器可以按照该加密协议，对接收到的原始控制数据进行加密处理，并得到加密控制数据。

在步骤 S303 中，将加密控制数据发送至开放式系统。

开放式系统在接收到该加密控制数据后，可以生成第一控制指令，并且将所接收到的加密控制数据包含在该第一控制指令中。之后，开放式系统将该第一控制指令发送至安全芯片，以由安全芯片对该加密控制数据进行安全性认证。

图 4 是根据一示例性实施例示出的另一种车辆安全通信方法的流程图，其中，该方法可以应用于安全芯片中，例如，图 2 所示的安全芯片 306。如图 4 所示，该方法可以包括以下步骤。

在步骤 S401 中，接收来自开放式系统的第一控制指令，其中，该第一控制指令包括加密控制数据。

在步骤 S402 中，对第一控制指令中的加密控制数据进行解密。

如前所述，服务器可以预先与安全芯片约定一加密协议，这样，安全芯片可以按照该加密协议，对接收到的第一控制指令中的加密控制数据进行解密处理。

在步骤 S403 中，当解密成功时，得到解密控制数据。

在步骤 S404 中，将第一控制指令中的加密控制数据替换为解密控制数据，形成第二控制指令，并将该第二控制指令发送至封闭式系统，以使封闭式系统根据该第二控制指令控制车辆执行目标操作。

例如，假设服务器接收到的来自用户终端的原始控制数据用于指示车辆要进行的目标操作为解锁操作，那么，如果安全芯片解密成功，则其向封闭式系统发送的第二控制指令同样可以指示车辆要进行的目标操作为解锁操作。当封闭式系统（例如，MCU）接收到第二控制指令后，通过对第二控制指令进行解析，能够得知目标操作为解锁操作，之后，封闭式系统能够将解锁指令发送至 CAN 总线中，车辆中的解锁部件能够从 CAN 总线中获取到这一解锁指令，并根据该解锁指令来执行解锁操作，由此，完成对车辆的解锁操作。

图 5 是根据一示例性实施例示出的一种在车辆通信过程中，用户终端、服务器、开放式系统、安全芯片、以及封闭式系统之间的信令交互图。其中，用户终端例如为图 1 所示的用户终端 100，服务器例如为图 1 所示的服务器 200，开放式系统例如为图 2 所示的开放式系统 301，安全芯片例如为图 2 所示的安全芯片 306，封闭式系统例如为图 2 所示的封闭式系统 302。图 5 涉及以上用于服务器和用于安全芯片的车辆安全通信方法中的步骤，因而，其具体的信令交互过程此处不再详细描述。

此外，虽然在图 4 中未示出，但是以上应用于安全芯片的车辆安全通信方法还可以包括：当解密失败时，不向封闭式系统发送任何控制指令。也就是说，一旦解密失败，安全芯片就可以将来自开放式系统的指令拦截。例如，当开放式系统被恶意程序入侵而冒充该开放式系统发送控制指令时，由于安全芯片的防护作用，该控制指令不会被发送至封闭式系统，从而确保封闭式系统及整车的安全性。

在上述技术方案中，通过服务器向车辆的开放式系统发送经过加密处理的控制数据，该

经过加密处理的控制数据能够由开放式系统转发给安全芯片，由安全芯片进行解密处理，只有在解密成功时，经解密得到的控制数据才会被发送至封闭式系统，此时，封闭式系统才会根据该控制数据控制车辆执行相应操作。由此，能够提高车辆联网通信时的安全性，确保只有合法的控制数据才会被发送至封闭式系统，防止因恶意程序的入侵导致对车辆进行错误的控制，从而确保车辆远程控制的安全性。

在一些可选的实施方式中，安全芯片可以对解密失败的次数进行计数。当解密失败的次数达到预设次数（例如，≥1）时，则表明开放式系统此时可能存在很大的安全隐患。在这种情况下，安全芯片可以向开放式系统发送重启指令和/或杀毒指令，其中，该重启指令可以用于控制开放式系统进行重启操作，该杀毒指令可以用于控制开放式系统进行杀毒操作。这样，可以在一定程度上解除开放式系统的安全隐患，防止恶意程序长时间威胁开放式系统的安全。

另外，在一些可选的实施方式中，服务器还可以在接收到原始控制数据之后，计算该原始控制数据的奇偶校验码。随后，将该奇偶校验码发送至开放式系统。开放式系统在接收到原始控制数据的奇偶校验码之后，可以将其与加密控制数据一同包含在第一控制指令中，例如，此时的第一控制指令的组成可以如图 6A 所示。安全芯片在接收到这一第一控制指令后，可以首先对其中的加密控制数据进行解密，如果解密成功，则能够得到解密控制数据。之后，安全芯片可以计算该解密控制数据的奇偶校验码。理论上，解密控制数据应当与原始控制数据相同，因此，二者的奇偶校验码应当一致。当第一控制指令中包括的奇偶校验码与解密控制数据的奇偶校验码相一致时，此时，安全芯片可以进一步确定接收到的第一控制指令为合法指令，因此，可以将第一控制指令中的加密控制数据替换为解密控制数据，形成第二控制指令，并将第二控制指令发送至封闭式系统。当第一控制指令中包括的奇偶校验码与解密控制数据的奇偶校验码不一致时，此时，安全芯片可以确定接收到的第一控制指令为非法指令，此时，可以拦截该指令，不向封闭式系统发送任何指令，从而确保整车安全性。

通过以上实施方式，可以进一步提高对合法指令识别的准确性，降低将非法指令错误地识别为合法指令的可能性，从而进一步提高整车安全性。

如前所述，用户可以通过用户终端向服务器发送原始控制数据，该原始控制数据可以用于指示车辆要执行的目标操作。在本申请的一些实施方式中，不同的目标操作可以具有不同的安全等级，目标操作的安全等级能够用于表示该目标操作是否为敏感操作。

在一个实施方式中，服务器可以不管原始控制数据所指示的目标操作的安全等级如何，都直接将原始控制数据进行加密。或者，在另一个实施方式中，服务器可以根据原始控制数据所指示的目标操作是否为敏感操作，来选择性地对原始控制数据进行加密。

例如，服务器在接收到原始控制数据后，可以根据该原始控制数据所指示的目标操作，确定该原始控制数据的安全等级信息，其中，该安全等级信息可以用于表示原始控制数据是否为敏感数据。例如，在服务器中可以预先存储有敏感操作列表，这样，服务器在接收到原

始控制数据后，通过对该原始控制数据进行解析，能够获悉目标操作信息。之后，服务器可以查询敏感操作列表。如果在敏感操作列表中查询到目标操作信息，则表明该目标操作为敏感操作。相应地，原始控制数据为敏感数据。而如果在敏感操作列表中没有查询到目标操作信息，则表明该目标操作为非敏感操作。相应地，原始控制数据为非敏感数据。

当原始控制数据的安全等级信息表示原始控制数据为敏感数据时，服务器才对该原始控制数据进行加密，得到相对应的加密控制数据。也就是说，加密处理操作仅针对敏感数据。而当原始控制数据的安全等级信息表示原始控制数据为非敏感数据时，服务器可以不对该原始控制数据进行加密，直接将原始控制数据发送至开放式系统。

在服务器向开放式系统发送加密控制数据或者原始控制数据时，还可以同时将原始控制数据的安全等级信息发送至开放式系统。例如，将原始控制数据的安全等级信息附加到加密控制数据或者原始控制数据的头部，形成一条信令，然后将该信令发送至开放式系统。这样，开放式系统在接收到该信令之后，通过对头部信息进行解析，能够确定出信令中包括的控制数据是经过加密处理的还是未经过加密处理的（即，原始的）。当原始控制数据的安全等级信息表示原始控制数据为敏感数据时，开放式系统生成并向安全芯片发送第一控制指令，其中，该第一控制指令可以包括：原始控制数据的安全等级信息和加密控制数据。当原始控制数据的安全等级信息表示原始控制数据为非敏感数据时，开放式系统可以生成并向安全芯片发送第三控制指令，其中，该第三控制指令可以包括：原始控制数据的安全等级信息和原始控制数据。安全芯片在接收到来自开放式系统的控制指令后，可以通过其中包括的安全等级信息来获悉该指令中包括的控制数据是否是加密的。如果是，则确定所接收到的是第一控制指令，并按照图 4 所示的方法进行解密处理，如果不是，则确定所接收到的是第三控制指令，此时，可以不进行解密处理，而是直接将该第三控制指令发送至封闭式系统。

当第二控制指令或第三控制指令被发送至封闭式系统之后，封闭式系统中的 MCU 能够通过多种方式来获悉该指令中的控制数据是意图用于控制车辆执行何种目标操作。例如，在一个实施方式中，在封闭式系统中的 MCU 接收到来自安全芯片的第二控制指令后，其可以从其中提取出解密控制数据。在 MCU 中可以预先存储有控制数据-操作映射表，在该映射表中记录有至少一种操作以及每种操作相对应的控制数据。MCU 可以利用提取出的解密控制数据来查询该映射表，以从该映射表中获悉相对应的操作，该操作即为车辆要执行的目标操作。

或者，在另一个实施方式中，服务器可以在通过对原始控制数据进行解析得出目标操作之后，生成第一映射指令数据，其中，该第一映射指令数据可以用于标识该目标操作。之后，服务器能够将该第一映射指令数据发送至开放式系统。这样，开放式系统可以将该第一映射指令数据包含在第一控制指令中，例如，此时所形成的第一控制指令的组成如图 6B 所示。这样，在安全芯片解密成功时，在所形成的第二控制指令中，可以保留该第一映射指令数据，例如，此时所形成的第二控制指令的组成如图 6C 所示。当封闭式系统中的 MCU 接收到该

第二控制指令后，其可以从其中提取出第一映射指令数据，并由此获悉车辆要执行的目标操作。

在获悉车辆要执行的目标操作之后，MCU 能够将第二控制指令中包括的解密控制数据发送至 CAN 总线中，以由相应的执行部件从 CAN 总线中获取该解密控制数据，并随后执行相应的目标操作。

在开放式系统与安全芯片之间的交互过程中，有时可能会受到干扰，这就导致安全芯片接收到的第一控制指令可能不完整，从而导致后续的安全认证失败。为了防止这一情况发生，在本申请的一个可选的实施方式中，安全芯片可以在对第一控制指令中的加密控制数据进行解密之前，首先判断第一控制指令的传输是否正常。当确定第一控制指令的传输正常时，才对第一控制指令中的加密控制数据进行解密。

示例地，开放式系统在向安全芯片发送第一控制指令之前，首先计算该第一控制指令的奇偶校验码，并将该奇偶校验码附加到第一控制指令的尾部，形成一条信令，并发送至安全芯片。安全芯片在接收到该信令之后，可以提取出除尾部信息之外的信息，并计算该信息的奇偶校验码。当所计算出的奇偶校验码与尾部信息中包含的奇偶校验码相一致时，表示第一控制指令的传输正常。否则，表示第一控制指令的传输异常。

当确定第一控制指令的传输异常时，安全芯片可以向开放式系统发送第一重传指令，其中，该第一重传指令可以用于指示开放式系统重新传输第一控制指令。

通过这一实施方式，可以避免原本是合法的第一控制指令因传输干扰而导致安全芯片解密失败的情况发生，从而可以进一步提高安全认证的准确性和可靠性。

以上描述了当用户意图通过用户终端远程控制车辆操作时，用户终端、服务器、开放式系统、安全芯片以及封闭式系统之间的交互过程。在本申请的其他实施方式中，封闭式系统也可以通过安全芯片和开放式系统，向服务器反馈车辆数据，如下面描述的。

图 7 是根据另一示例性实施例示出的一种车辆安全通信方法的流程图，其中，该方法可以应用于安全芯片中，例如，图 2 所示的安全芯片 306。如图 7 所示，该方法可以包括以下步骤。

在步骤 S701 中，接收来自封闭式系统（例如，图 2 所示的封闭式系统 302）的第一车辆数据指令，其中，该第一车辆数据指令包括原始车辆数据。

封闭式系统中的 MCU 可以从 CAN 总线上获取原始车辆数据，该原始车辆数据可以包括多种类型的车辆数据，例如，车辆在执行目标操作后针对该目标操作的执行结果数据，或者，响应于外部请求（例如，来自服务器的数据获取请求）而反馈的整车数据，或者车辆主动向服务器上报的整车数据，等等。例如，当车辆完成解锁操作后，解锁部件可以将解锁结果反馈至 CAN 总线。此时，MCU 可以从 CAN 总线上监听到这一数据，并生成第一车辆数据指令，之后，将该数据作为原始车辆数据包含在第一车辆数据指令当中，并将其发送给安全芯片。

可选地，MCU 还可以在监听到数据之后，生成第二映射指令数据，其中，该第二映射指令数据可以用于标识原始车辆数据的类型。例如，假设 MCU 监听到的是来自解锁部件的解锁结果数据，则 MCU 生成的第二映射指令数据可以用于标识该原始车辆数据的类型为解锁结果。MCU 可以将第二映射指令数据包含在第一车辆数据指令当中，如图 8 所示的第一车辆数据指令，以便日后传输到服务器中时，服务器能够通过该第二映射指令数据，得知该原始车辆数据的类型，从而进行相应处理。

在步骤 S702 中，对原始车辆数据进行加密，得到相对应的加密车辆数据。

如前所述，服务器可以预先与安全芯片约定一加密协议，这样，安全芯片可以按照该加密协议，对接收到的第一车辆数据指令中的原始车辆数据进行加密处理，并得到加密车辆数据。

在步骤 S703 中，将第一车辆数据指令中的原始车辆数据替换为加密车辆数据，形成第二车辆数据指令，并将该第二车辆数据指令发送至开放式系统。

开放式系统在接收到来自安全芯片的第二车辆数据指令后，可以将其转发至服务器，以由服务器进行解密处理。

图 9 是根据另一示例性实施例示出的另一种车辆安全通信方法的流程图，其中，该方法可以应用于服务器中，例如，图 1 所示的服务器 200。如图 9 所示，该方法可以包括以下步骤。

在步骤 S901 中，接收来自开放式系统的第二车辆数据指令，其中，该第二车辆数据指令是由开放式系统从安全芯片转发的，并且该第二车辆数据指令包括加密车辆数据。

在步骤 S902 中，对第二车辆数据指令中的加密车辆数据进行解密。

如前所述，服务器可以预先与安全芯片约定一加密协议，这样，服务器可以按照该加密协议，对接收到的第二车辆数据指令中的加密车辆数据进行解密处理。

在步骤 S903 中，当解密成功时，得到解密车辆数据。

在步骤 S904 中，处理该解密车辆数据。其中，所述处理可以例如包括但不限于：存储、显示、向用户终端转发等等。例如，当原始车辆数据为针对目标操作的执行结果数据时，服务器在解密成功得到解密车辆数据后，可以向用户终端发送该解密车辆数据，以向用户告知执行结果。

图 10 是根据另一示例性实施例示出的一种在车辆通信过程中，服务器、开放式系统、安全芯片、以及封闭式系统之间的信令交互图。其中，服务器例如为图 1 所示的服务器 200，开放式系统例如为图 2 所示的开放式系统 301，安全芯片例如为图 2 所示的安全芯片 306，封闭式系统例如为图 2 所示的封闭式系统 302。图 10 涉及以上用于服务器和用于安全芯片的车辆安全通信方法中的步骤，因而，其具体的信令交互过程此处不再详细描述。

在上述技术方案中，通过安全芯片对来自封闭式系统的车辆数据进行加密处理，并通过开放式系统将经过加密处理的车辆数据发送至服务器，由服务器进行解密处理，只有在解密

成功时，服务器才能获取到来自封闭式系统的车辆数据。由此，能够避免非法的服务器所有者获悉车辆信息，从而确保车辆信息的安全性。

在一些可选的实施方式中，封闭式系统中的 MCU 可以在获取到原始车辆数据之后，计算该原始车辆数据的奇偶校验码。随后，封闭式系统可以将其与原始车辆数据一同包含在第一车辆数据指令中，例如，此时的第一车辆数据指令的组成可以如图 11A 所示。安全芯片在接收到这一第一车辆数据指令后，可以首先对其中的原始车辆数据进行加密，得到加密车辆数据。随后，将第一车辆数据指令中的原始车辆数据替换为加密车辆数据，形成第二车辆数据指令，例如，此时的第二车辆数据指令的组成可以如图 11B 所示，并将第二车辆数据指令发送至开放式系统。当开放式系统将第二车辆数据指令转发至服务器后，服务器可以首先对其中的加密车辆数据进行解密，如果解密成功，则能够得到解密车辆数据。理论上，解密车辆数据应当与原始车辆数据相同，因此，二者的奇偶校验码应当一致。当第二车辆数据指令中包括的奇偶校验码与解密车辆数据的奇偶校验码相一致时，此时，服务器可以确定接收到的第二车辆数据指令为合法指令，其中的解密车辆数据是来自于车辆的真实整车数据。此时，可以处理该解密车辆数据。

此外，在一些可选的实施方式中，封闭式系统中的 MCU 所获取到的原始车辆数据可以具有不同的安全等级，其中，该安全等级信息可以用于表示该原始车辆数据是否为敏感数据。在这种情况下，MCU 在生成第一车辆数据指令后，可以将原始车辆数据的安全等级信息包含在第一车辆数据指令中，例如，此时的第一车辆数据指令的组成可以如图 11C 所示。这样，当安全芯片接收到第一车辆数据指令后，可以通过该安全等级信息，判断原始车辆数据是否为敏感数据。在一个实施方式中，安全芯片可以不管原始车辆数据的安全等级如何，都对该原始车辆数据进行加密处理。或者，在另一个实施方式中，当安全等级信息表示原始车辆数据为敏感数据时，安全芯片才对第一车辆数据指令中的原始车辆数据进行加密，得到相对应的加密车辆数据。也就是说，加密处理操作仅针对敏感数据。而当原始车辆数据安全等级信息表示原始车辆数据为非敏感数据时，安全芯片可以不对该原始车辆数据进行加密。

当原始车辆数据的安全等级信息表示原始车辆数据为敏感数据时，安全芯片可以生成第二车辆数据指令，其中，该第二车辆数据指令中可以包括原始车辆数据的安全等级信息、以及加密车辆数据。当原始车辆数据的安全等级信息表示原始车辆数据为非敏感数据时，安全芯片可以直接将第一车辆数据指令转发给开放式系统。服务器在接收到由开放式系统转发的车辆数据指令后，可以通过对其中的安全等级信息进行解析，确定出车辆数据指令中包括的车辆数据是经过加密处理的还是未经过加密处理的（即，原始的）。当安全等级信息表示原始车辆数据为敏感数据时，则服务器能够确定接收到的是第二车辆数据指令，并对其中的加密车辆数据进行解密。当安全等级信息表示原始车辆数据为非敏感数据时，则服务器能够确定接收到的是第一车辆数据指令，并可以直接对其中的原始车辆数据进行处理。

此外，在服务器与开放式系统之间的交互过程中、在开放式系统与安全芯片之间的交互

过程中、以及在安全芯片与封闭式系统中的 MCU 之间的交互过程中，有时可能会受到干扰，这就导致安全芯片接收到的第一车辆数据指令可能不完整，或者服务器接收到的由开放式系统转发的车辆数据指令不完整，从而导致后续的解密失败。为了防止这一情况发生，在本申请的一个可选的实施方式中，安全芯片可以在对第一车辆数据指令中的原始车辆数据进行加密处理之前，先判断第一车辆数据指令的传输是否正常。当确定第一车辆数据指令的传输正常时，才对第一车辆数据指令中的原始车辆数据进行加密。

示例地，封闭式系统在向安全芯片发送第一车辆数据指令之前，首先计算该第一车辆数据指令的奇偶校验码，并将该奇偶校验码附加到第一车辆数据指令的尾部，形成一条信令，并发送至安全芯片。安全芯片在接收到该信令之后，可以提取出除尾部信息之外的信息，并计算该信息的奇偶校验码。当所计算出的奇偶校验码与尾部信息中包含的奇偶校验码相一致时，表示第一车辆数据指令的传输正常。否则，表示第一车辆数据指令的传输异常。

当确定第一车辆数据指令的传输异常时，安全芯片可以向封闭式系统发送第二重传指令，其中，该第二重传指令可以用于指示封闭式系统重新传输第一车辆数据指令。

另外，在服务器侧，其可以在对接收到的第二车辆数据指令中的加密车辆数据进行解密之前，先判断该第二车辆数据指令的传输是否正常。当确定第二车辆数据指令的传输正常时，才对该第二车辆数据指令中的加密车辆数据进行解密。

示例地，安全芯片可以在向开放式系统发送第二车辆数据指令之前，首先计算该第二车辆数据指令的奇偶校验码，并将该奇偶校验码附加到第二车辆数据指令的尾部，形成一条信令，并发送至开放式系统。开放式系统在接收到该信令之后，可以提取出除尾部信息之外的信息，并计算该信息的奇偶校验码。当所计算出的奇偶校验码与尾部信息中包含的奇偶校验码相一致时，表示在安全芯片与开放式系统之间，第二车辆数据指令的传输正常。否则，表示在安全芯片与开放式系统之间，第二车辆数据指令的传输异常。

当在安全芯片与开放式系统之间，第二车辆数据指令的传输正常时，开放式系统可以直接将该信令转发至服务器。服务器在接收到该信令之后，可以提取出除尾部信息之外的信息，并计算该信息的奇偶校验码。当所计算出的奇偶校验码与尾部信息中包含的奇偶校验码相一致时，表示在服务器与开放式系统之间，第二车辆数据指令的传输正常。否则，表示在服务器与开放式系统之间，第二车辆数据指令的传输异常。

当在安全芯片与开放式系统之间，第二车辆数据指令的传输异常时，开放式系统可以向安全芯片发送第三重传指令，其中，该第三重传指令用于指示安全芯片重新传输第二车辆数据指令。当在服务器与开放式系统之间，第二车辆数据指令的传输异常时，服务器可以向开放式系统发送第四重传指令，其中，该第四重传指令用于指示开放式系统重新传输第二车辆数据指令。

通过这一实施方式，可以避免原本是合法的第二车辆数据指令因传输干扰而导致服务器解密失败的情况发生，从而可以进一步提高安全认证的准确性和可靠性。

图 12 是根据一示例性实施例示出的一种车辆安全通信装置 1200 的框图，其中，该装置 1200 可以配置于安全芯片中，例如，图 2 所示的安全芯片 306。如图 12 所示，该装置 1200 可以包括：第一接收模块 1201，被配置为接收来自封闭式系统的第一车辆数据指令，其中，该第一车辆数据指令包括原始车辆数据；加密模块 1202，被配置为对原始车辆数据进行加密，得到相对应的加密车辆数据；发送模块 1203，被配置为将第一车辆数据指令中的原始车辆数据替换为加密车辆数据，形成第二车辆数据指令，并将第二车辆数据指令发送至开放式系统。

可选地，该第一车辆数据指令还包括原始车辆数据的安全等级信息，其中，该安全等级信息用于表示原始车辆数据是否为敏感数据；以及，所述加密模块 1202，被配置为当安全等级信息表示原始车辆数据为敏感数据时，对第一车辆数据指令中的原始车辆数据进行加密，得到相对应的加密车辆数据。

可选地，所述装置 1200 还可以包括：第一判断模块，被配置为判断第一车辆数据指令的传输是否正常；所述加密模块 1202，被配置为当确定第一车辆数据指令的传输正常时，对第一车辆数据指令中的原始车辆数据进行加密，得到相对应的加密车辆数据。

图 13 是根据一示例性实施例示出的另一种车辆安全通信装置 1300 的框图，其中，该装置 1300 可以配置于服务器中，例如，图 1 所示的服务器 200。如图 13 所示，该装置 1300 可以包括：第二接收模块 1301，被配置为接收来自开放式系统的车辆数据指令，其中，该车辆数据指令是由开放式系统从安全芯片转发的，并且车辆数据指令包括加密车辆数据；解密模块 1302，被配置为对车辆数据指令中的加密车辆数据进行解密，当解密成功时，得到解密车辆数据；以及处理模块 1303，被配置为处理解密车辆数据。

可选地，所述车辆数据指令还包括与加密车辆数据在加密之前所对应的原始车辆数据相关联的奇偶校验码；所述装置 1300 还可以包括：计算模块，被配置为计算解密车辆数据的奇偶校验码；所述处理模块 1303，被配置为当车辆数据指令中包括的奇偶校验码与解密车辆数据的奇偶校验码相一致时，处理解密车辆数据。

可选地，所述装置 1300 还可以包括：第二判断模块，被配置为判断车辆数据指令的传输是否正常；所述解密模块 1302，被配置为当确定车辆数据指令的传输正常时，对车辆数据指令中的加密车辆数据进行解密。

在上述技术方案中，通过安全芯片对来自封闭式系统的车辆数据进行加密处理，并通过开放式系统将经过加密处理的车辆数据发送至服务器，由服务器进行解密处理，只有在解密成功时，服务器才能获取到来自封闭式系统的原始车辆数据。由此，能够避免非法的服务器所有者获悉车辆信息，从而确保车辆信息的安全性。

关于上述实施例中的装置，其中各个模块执行操作的具体方式已经在有关该方法的实施例中进行了详细描述，此处将不做详细阐述说明。

以上结合附图详细描述了本申请的优选实施方式，但是，本申请并不限于上述实施方式

中的具体细节，在本申请的技术构思范围内，可以对本申请的技术方案进行多种简单变型，这些简单变型均属于本申请的保护范围。

另外需要说明的是，在上述具体实施方式中所描述的各个具体技术特征，在不矛盾的情况下，可以通过任何合适的方式进行组合。为了避免不必要的重复，本申请对各种可能的组合方式不再另行说明。

此外，本申请的各种不同的实施方式之间也可以进行任意组合，只要其不违背本申请的思想，其同样应当视为本申请所公开的内容。

权利要求书

1、一种车辆安全通信方法，其特征在于，所述车辆包括开放式系统、安全芯片和封闭式系统，所述开放式系统与所述封闭式系统之间通过所述安全芯片连接，所述方法应用于所述安全芯片，并且所述方法包括：

接收来自所述封闭式系统的第一车辆数据指令，其中，所述第一车辆数据指令包括原始车辆数据；

对所述原始车辆数据进行加密，得到相对应的加密车辆数据；

将所述第一车辆数据指令中的所述原始车辆数据替换为所述加密车辆数据，形成第二车辆数据指令，并将所述第二车辆数据指令发送至所述开放式系统。

2、根据权利要求 1 所述的方法，其特征在于，所述第一车辆数据指令还包括与所述原始车辆数据相关联的奇偶校验码。

3、根据权利要求 1 所述的方法，其特征在于，所述第一车辆数据指令还包括所述原始车辆数据的安全等级信息，其中，所述安全等级信息用于表示所述原始车辆数据是否为敏感数据；

所述对所述第一车辆数据指令中的所述原始车辆数据进行加密，得到相对应的加密车辆数据，包括：

当所述安全等级信息表示所述原始车辆数据为敏感数据时，对所述原始车辆数据进行加密，得到相对应的加密车辆数据。

4、根据权利要求 1 至 3 中任一项所述的方法，其特征在于，所述方法还包括：

判断所述第一车辆数据指令的传输是否正常；

所述对所述原始车辆数据进行加密，得到相对应的加密车辆数据，包括：

当确定所述第一车辆数据指令的传输正常时，对所述原始车辆数据进行加密，得到相对应的加密车辆数据。

5、一种车辆安全通信方法，其特征在于，所述车辆包括开放式系统、安全芯片和封闭式系统，所述开放式系统与所述封闭式系统之间通过所述安全芯片连接，所述开放式系统与服务器连接，所述方法应用于所述服务器，并且所述方法包括：

接收来自所述开放式系统的车辆数据指令，其中，所述车辆数据指令是由所述开放式系统从所述安全芯片转发的，并且所述车辆数据指令包括加密车辆数据；

对所述车辆数据指令中的所述加密车辆数据进行解密；

当解密成功时，得到解密车辆数据；以及

处理所述解密车辆数据。

6、根据权利要求 5 所述的方法，其特征在于，所述车辆数据指令还包括与所述加密车辆数据在加密之前所对应的原始车辆数据相关联的奇偶校验码；

所述方法还包括：

计算所述解密车辆数据的奇偶校验码；

所述处理所述解密车辆数据，包括：

当所述车辆数据指令中包括的奇偶校验码与所述解密车辆数据的奇偶校验码相一致时，处理所述解密车辆数据。

7、根据权利要求 5 或 6 所述的方法，其特征在于，所述方法还包括：

判断所述车辆数据指令的传输是否正常；

所述对所述车辆数据指令中的所述加密车辆数据进行解密，包括：

当确定所述车辆数据指令的传输正常时，对所述车辆数据指令中的所述加密车辆数据进行解密。

8、一种车辆安全通信装置，其特征在于，所述车辆包括开放式系统、安全芯片和封闭式系统，所述开放式系统与所述封闭式系统之间通过所述安全芯片连接，所述装置配置于所述安全芯片，并且所述装置包括：

第一接收模块，被配置为接收来自所述封闭式系统的第一车辆数据指令，其中，所述第一车辆数据指令包括原始车辆数据；

加密模块，被配置为对所述原始车辆数据进行加密，得到相对应的加密车辆数据；

发送模块，被配置为将所述第一车辆数据指令中的所述原始车辆数据替换为所述加密车辆数据，形成第二车辆数据指令，并将所述第二车辆数据指令发送至所述开放式系统。

9、根据权利要求 8 所述的装置，其特征在于，所述第一车辆数据指令还包括与所述原始车辆数据相关联的奇偶校验码。

10、根据权利要求 8 所述的装置，其特征在于，所述第一车辆数据指令还包括所述原始车辆数据的安全等级信息，其中，所述安全等级信息用于表示所述原始车辆数据是否为敏感数据；

所述加密模块，被配置为当所述安全等级信息表示所述原始车辆数据为敏感数据时，对所述第一车辆数据指令中的所述原始车辆数据进行加密，得到相对应的加密车辆数据。

11、根据权利要求 8 至 10 中任一项所述的装置，其特征在于，所述装置还包括：

第一判断模块，被配置为判断所述第一车辆数据指令的传输是否正常；

所述加密模块，被配置为当确定所述第一车辆数据指令的传输正常时，对所述第一车辆数据指令中的所述原始车辆数据进行加密，得到相对应的加密车辆数据。

12、一种车辆安全通信装置，其特征在于，所述车辆包括开放式系统、安全芯片和封闭式系统，所述开放式系统与所述封闭式系统之间通过所述安全芯片连接，所述开放式系统与服务器连接，所述装置配置于所述服务器，并且所述装置包括：

第二接收模块，被配置为接收来自所述开放式系统的车辆数据指令，其中，所述车辆数据指令是由所述开放式系统从所述安全芯片转发的，并且所述车辆数据指令包括加密车辆数据；

解密模块，被配置为对所述车辆数据指令中的所述加密车辆数据进行解密，当解密成功时，得到解密车辆数据；以及

处理模块，被配置为处理所述解密车辆数据。

13、根据权利要求 12 所述的装置，其特征在于，所述车辆数据指令还包括与所述加密车辆数据在加密之前所对应的原始车辆数据相关联的奇偶校验码；

所述装置还包括：

计算模块，被配置为计算所述解密车辆数据的奇偶校验码；

所述处理模块，被配置为当所述车辆数据指令中包括的奇偶校验码与所述解密车辆数据的奇偶校验码相一致时，处理所述解密车辆数据。

14、根据权利要求 12 或 13 所述的装置，其特征在于，所述装置还包括：

第二判断模块，被配置为判断所述车辆数据指令的传输是否正常；

所述解密模块，被配置为当确定所述车辆数据指令的传输正常时，对所述车辆数据指令

中的所述加密车辆数据进行解密。

15、一种车辆多媒体系统，其特征在于，所述车辆多媒体系统包括：

封闭式系统，用于采集原始车辆数据，并发送包括所述原始车辆数据的第一车辆数据指令；

安全芯片，该安全芯片包括权利要求 8-11 中任一项所述的车辆安全通信装置；

开放式系统，所述开放式系统与所述封闭式系统之间通过所述安全芯片通信，并且所述开放式系统还与服务器进行通信，所述开放式系统用于接收来自所述安全芯片的所述第二车辆数据指令，并将所述第二车辆数据指令转发至所述服务器。

16、一种车辆，其特征在于，所述车辆包括根据权利要求 15 所述的车辆多媒体系统。

附图

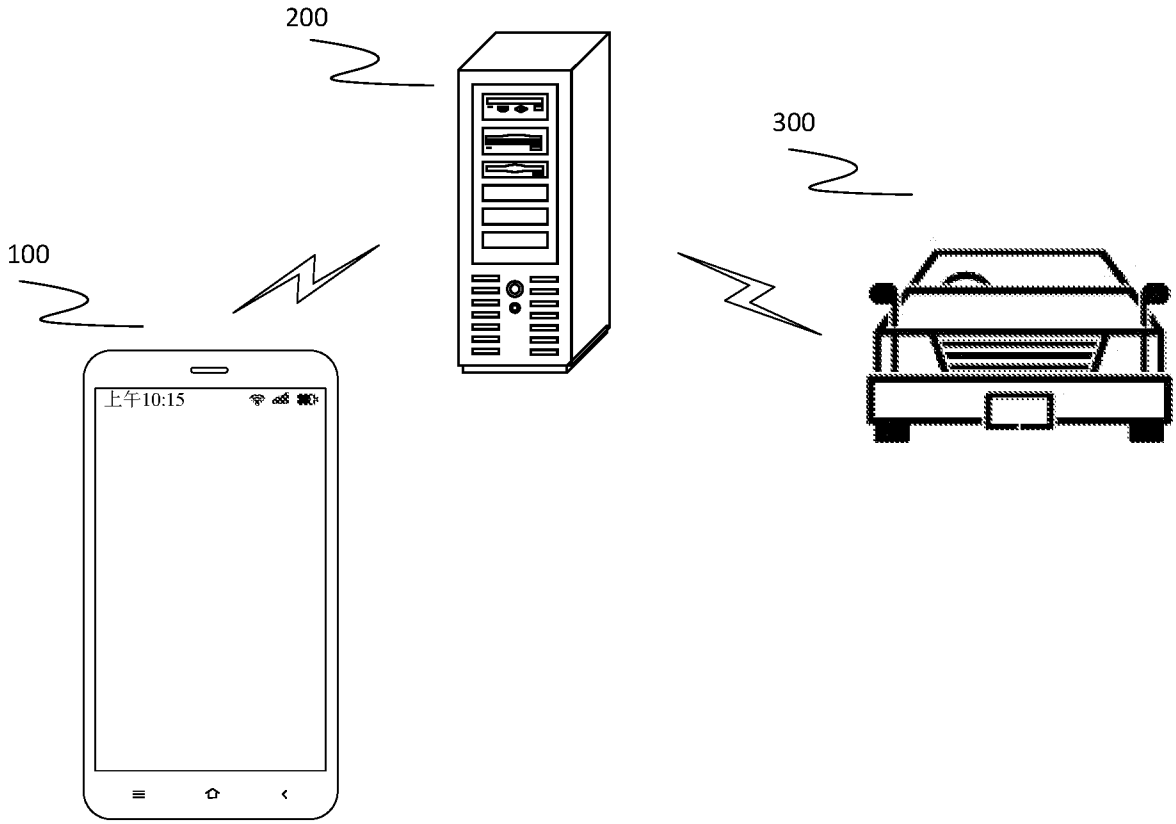

200
300
100
上午10:15

图 1

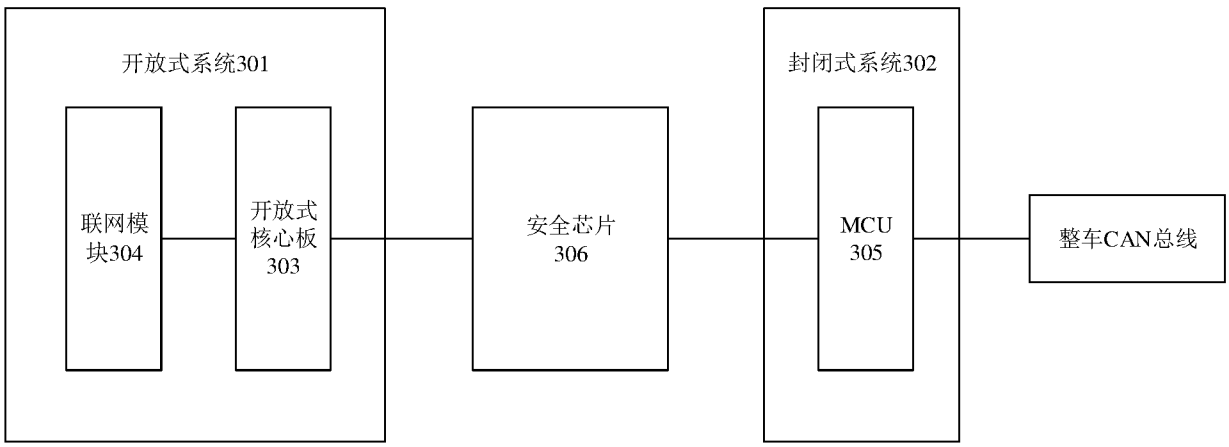

开放式系统301
联网模块304
开放式核心板303
安全芯片306
封闭式系统302
MCU305
整车CAN总线

图 2

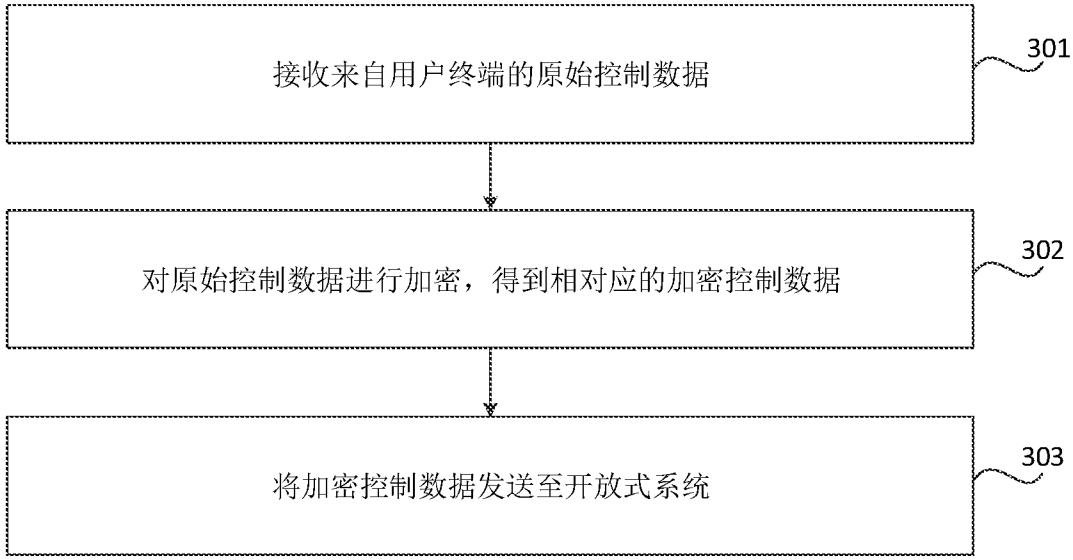

接收来自用户终端的原始控制数据
301
对原始控制数据进行加密，得到相对应的加密控制数据
302
将加密控制数据发送至开放式系统
303

图3

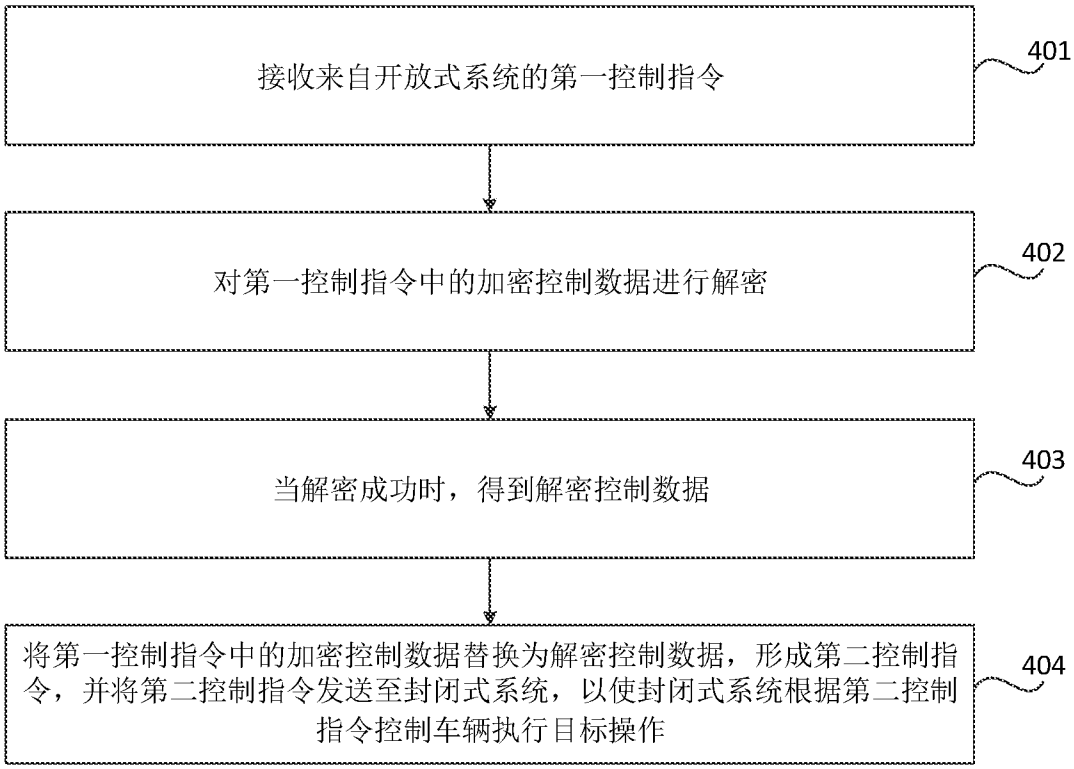

接收来自开放式系统的第一控制指令
401
对第一控制指令中的加密控制数据进行解密
402
当解密成功时，得到解密控制数据
403
将第一控制指令中的加密控制数据替换为解密控制数据，形成第二控制指令，并将第二控制指令发送至封闭式系统，以使封闭式系统根据第二控制指令控制车辆执行目标操作
404

图 4

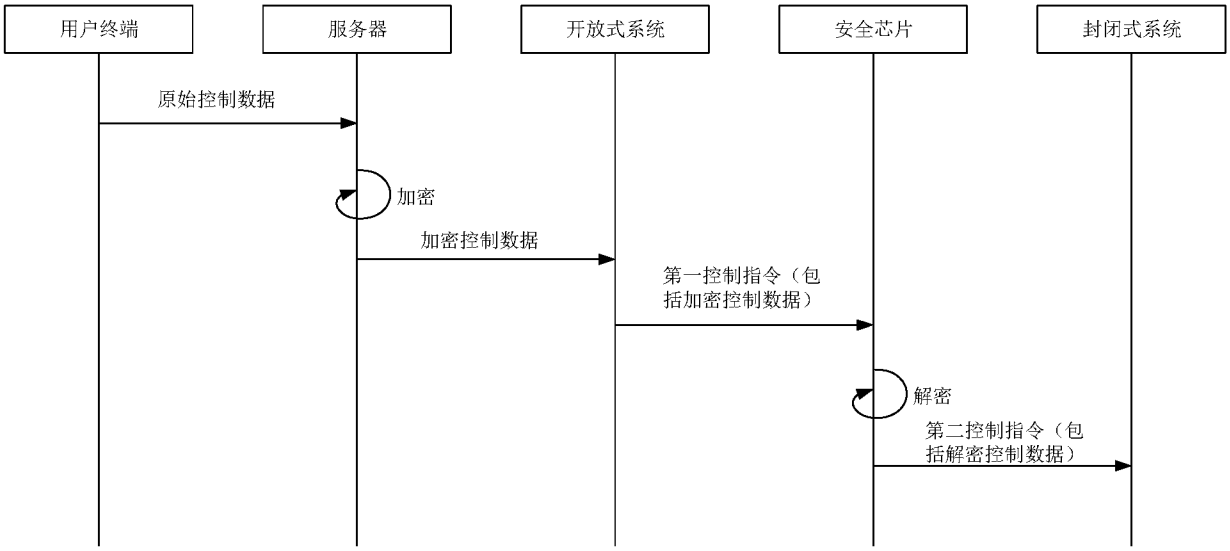


图5



图6A



图6B

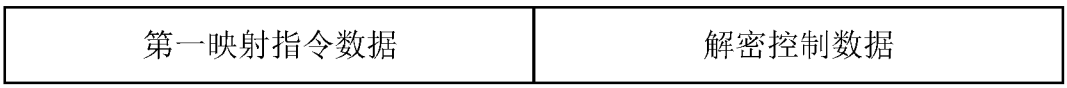


图6C

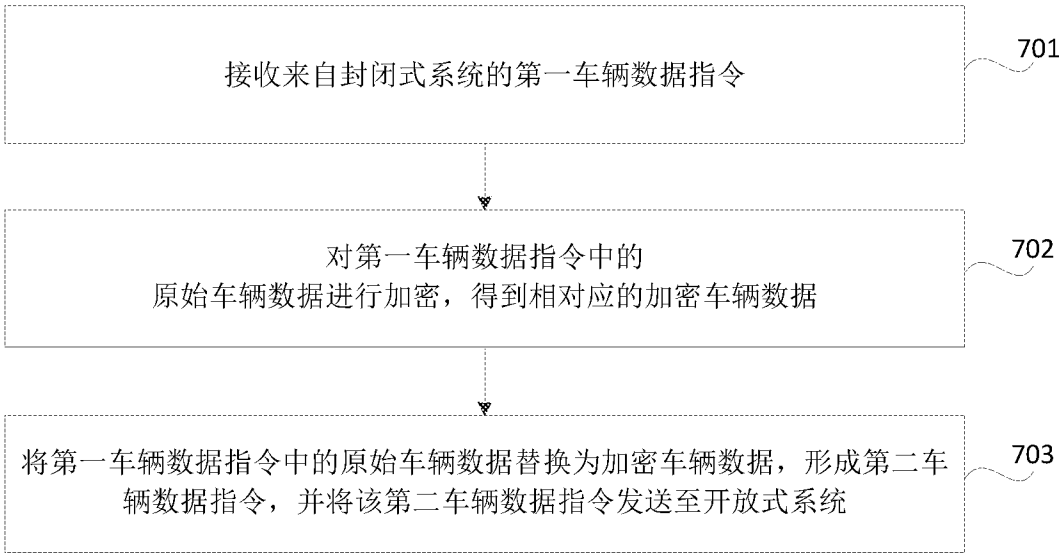

接收来自封闭式系统的第一车辆数据指令
701
对第一车辆数据指令中的
原始车辆数据进行加密，得到相对应的加密车辆数据
702
将第一车辆数据指令中的原始车辆数据替换为加密车辆数据，形成第二车辆数据指令，并将该第二车辆数据指令发送至开放式系统
703

图7


第二映射指令数据
原始车辆数据

图8

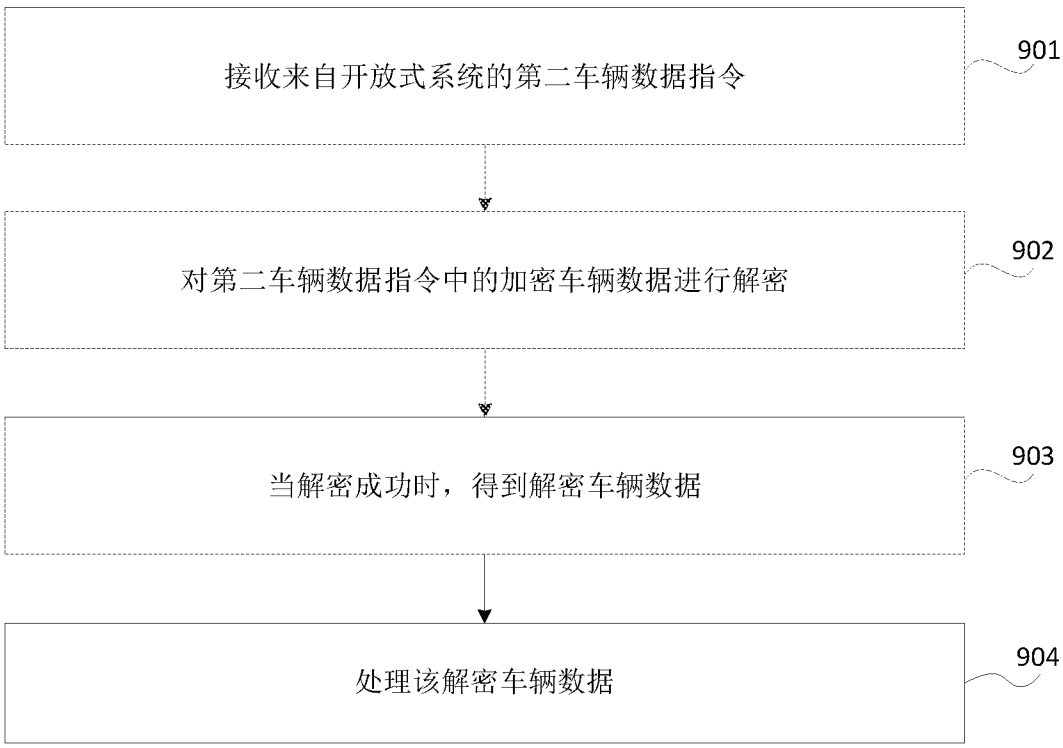

接收来自开放式系统的第二车辆数据指令
901
对第二车辆数据指令中的加密车辆数据进行解密
902
当解密成功时，得到解密车辆数据
903
处理该解密车辆数据
904

图9

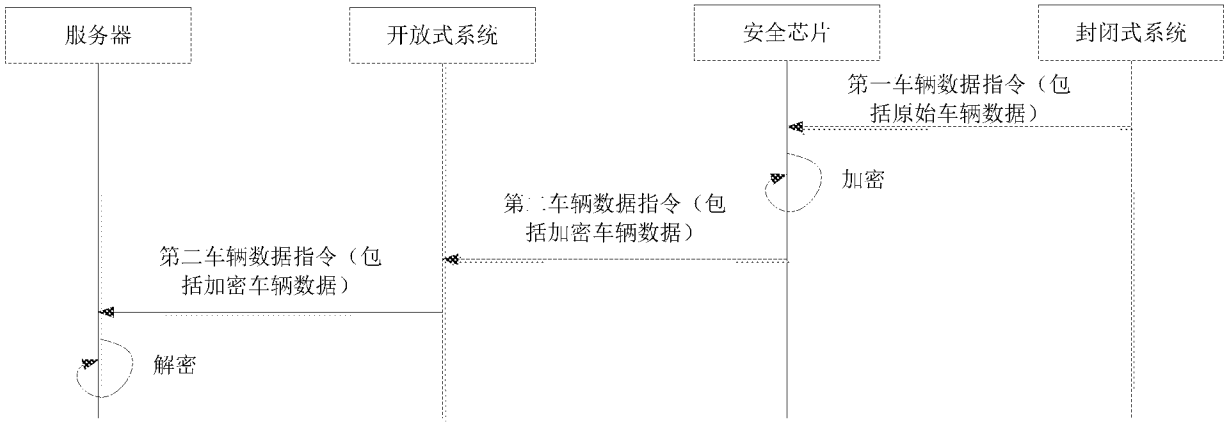


图10

原始车辆数据	奇偶校验码

图11A

加密车辆数据	奇偶校验码

图11B

安全等级信息	原始车辆数据

图11C

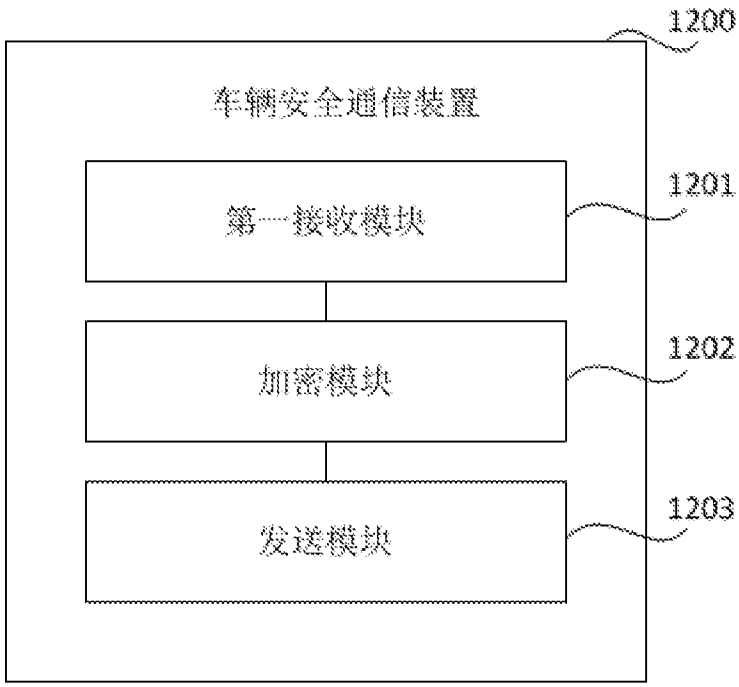

1200
车辆安全通信装置
第一接收模块
1201
加密模块
1202
发送模块
1203

图12

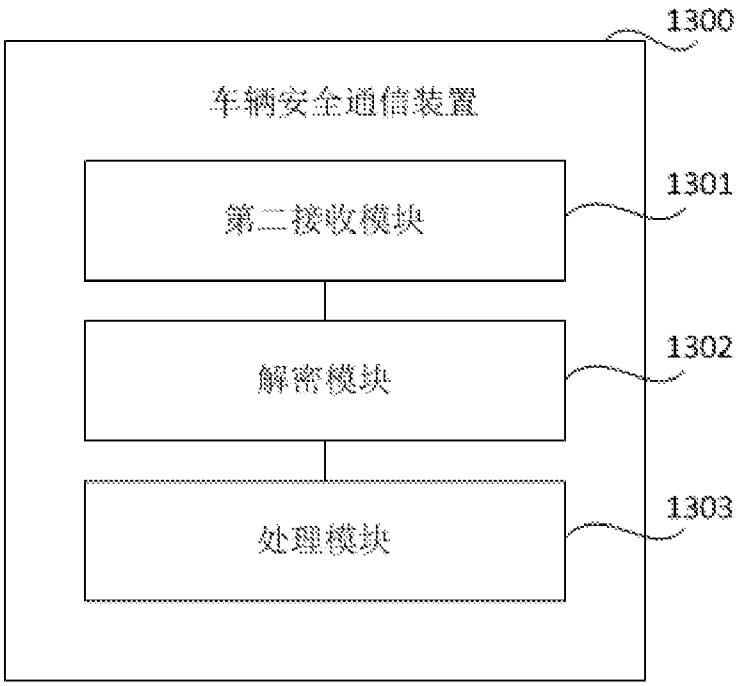

1300
车辆安全通信装置
第二接收模块
1301
解密模块
1302
处理模块
1303

图13

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/076295

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) 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; H04W

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; WPI; EPODOC; CNKI; GOOGLE: sensitive, vehicle data, safe, server, encry+, vehicle, outside, inside, open, close

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 104700469 A (GUANGZHOU TONGHUI TECHNOLOGY CO., LTD.), 10 June 2015 (10.06.2015), description, paragraphs [0005]-[0014]	1-16
X	CN 201509315 U (ZHAO, Yang et al.), 16 June 2010 (16.06.2010), description, paragraphs [0025]-[0034] and [0046]-[0065]	1-16
A	CN 104050421 A (FORD GLOBAL TECHNOLOGIES, LLC), 17 September 2014 (17.09.2014), the whole document	1-16
A	US 2015134142 A1 (GOGORO INC.), 14 May 2015 (14.05.2015), the whole document	1-16

☐ 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	Date of mailing of the international search report
18 April 2017 (18.04.2017)	**04 May 2017 (04.05.2017)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **GONG, Lei** Telephone No.: (86-10) **62413375**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/076295

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104700469 A	10 June 2015	None	
CN 201509315 U	16 June 2010	None	
CN 104050421 A	17 September 2014	DE 102014204589 A1	18 September 2014
		US 2014282827 A1	18 September 2014
US 2015134142 A1	14 May 2015	PH 12016500857 A1	27 June 2016
		EP 3065977 A1	14 September 2016
		TW 201527158 A	16 July 2015
		JP 2017501069 A	12 January 2017
		CN 105873797 A	17 August 2016
		US 2016292937 A1	06 October 2016
		WO 2015070057 A1	14 May 2015

国际检索报告

国际申请号
PCT/CN2017/076295

A. 主题的分类

H04L 29/06(2006.01)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; H04W

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; WPI; EPODOC; CNKI; GOOGLE:敏感，外部，内部，服务器，加密，封闭，开放，车辆数据，安全,server, encry+, vehicle, outside, inside, open, close

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN 104700469 A (广州市通汇科技有限公司) 2015年 6月 10日 (2015-06-10) 说明书第[0005]-[0014]段	1-16
X	CN 201509315 U (赵阳 等) 2010年 6月 16日 (2010-06-16) 说明书第[0025]-[0034]，[0046]-[0065]段	1-16
A	CN 104050421 A (福特全球技术公司) 2014年 9月 17日 (2014-09-17) 全文	1-16
A	US 2015134142 A1 (GOGORO INC.) 2015年 5月 14日 (2015-05-14) 全文	1-16

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 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	国际检索报告邮寄日期
2017年 4月 18日	2017年 5月 4日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(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	受权官员 宫磊 电话号码 (86-10)62413375

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2017/076295

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)
CN	104700469	A	2015年 6月 10日	无			
CN	201509315	U	2010年 6月 16日	无			
CN	104050421	A	2014年 9月 17日	DE	102014204589	A1	2014年 9月 18日
				US	2014282827	A1	2014年 9月 18日
US	2015134142	A1	2015年 5月 14日	PH	12016500857	A1	2016年 6月 27日
				EP	3065977	A1	2016年 9月 14日
				TW	201527158	A	2015年 7月 16日
				JP	2017501069	A	2017年 1月 12日
				CN	105873797	A	2016年 8月 17日
				US	2016292937	A1	2016年 10月 6日
				WO	2015070057	A1	2015年 5月 14日