

(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 4 月 27 日 (27.04.2017)



(10) 国际公布号
WO 2017/067154 A1

- (51) 国际专利分类号:
H04L 9/32 (2006.01) *H04L 12/66* (2006.01)
- (21) 国际申请号: PCT/CN2016/082074
- (22) 国际申请日: 2016 年 5 月 13 日 (13.05.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510689773.X 2015 年 10 月 21 日 (21.10.2015) CN
- (71) 申请人: 乐视控股(北京)有限公司 (LE HOLDINGS (BEIJING) CO., LTD) [CN/CN]; 中国北京市朝阳区姚家园路 105 号 3 号楼 10 层 1102, Beijing 100025 (CN)。乐卡汽车智能科技(北京)有限公司 (LEAUTO INTELLIGENT TECHNOLOGY (BEIJING) CO. LTD) [CN/CN]; 中国北京市朝阳区姚家园路 105 号观湖国际大厦 11 层, Beijing 100025 (CN)。
- (72) 发明人: 徐勇 (XU, Yong); 中国北京市朝阳区姚家园路 105 号观湖国际大厦 11 层, Beijing 100025 (CN)。陈昆盛 (CHEN, Kunsheng); 中国北京市朝阳区姚家园路 105 号观湖国际大厦 11 层, Beijing 100025 (CN)。李文锐 (LI, Wenrui); 中国北京市朝

阳区姚家园路 105 号观湖国际大厦 11 层, Beijing 100025 (CN)。邹禹 (ZOU, Yu); 中国北京市朝阳区姚家园路 105 号观湖国际大厦 11 层, Beijing 100025 (CN)。李丹 (LI, Dan); 中国北京市朝阳区姚家园路 105 号观湖国际大厦 11 层, Beijing 100025 (CN)。刘鹏 (LIU, Peng); 中国北京市朝阳区姚家园路 105 号观湖国际大厦 11 层, Beijing 100025 (CN)。林伟 (LIN, Wei); 中国北京市朝阳区姚家园路 105 号观湖国际大厦 11 层, Beijing 100025 (CN)。

(74) 代理人: 北京路浩知识产权代理有限公司 (CN-KNOWHOW INTELLECTUAL PROPERTY AGENT LIMITED); 中国北京市海淀区丹棱街 3 号中国电子大厦 B 座 18 层, Beijing 100080 (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, 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, KN, KP, KR, 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。

[见续页]

(54) Title: DATA COMMUNICATION METHOD AND SYSTEM FOR IN-VEHICLE NETWORK COMPRISING MULTIPLE SUBNETWORKS, AND GATEWAY

(54) 发明名称: 用于包括多个子网的车载网络的数据通信方法、系统及网关

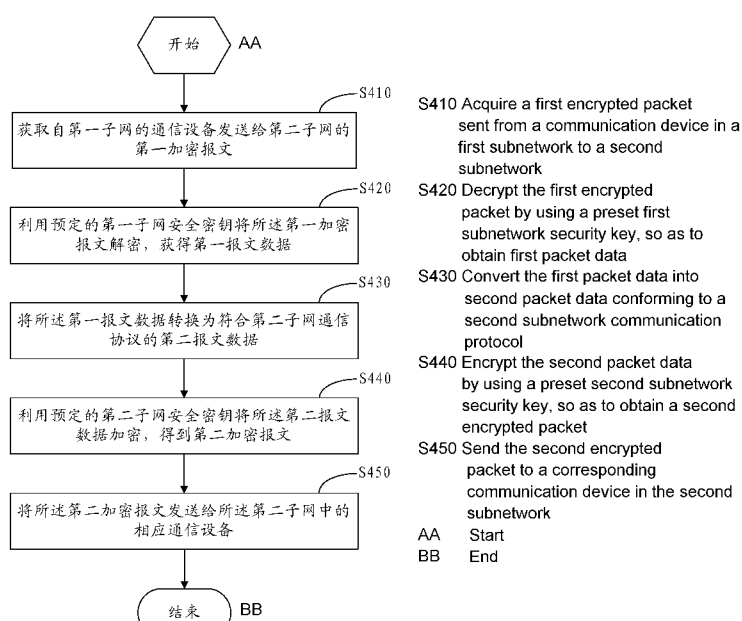


图 4

(57) Abstract: Embodiments of the present invention provide a data communication method and system for an in-vehicle network comprising multiple subnetworks, and a gateway. The data communication method for an in-vehicle network comprising multiple subnetworks comprises: acquiring a first encrypted packet sent from a communication device in a first subnetwork to a second subnetwork; decrypting the first encrypted packet by using a preset first subnetwork security key, so as to obtain first packet data; converting the first packet data into second packet data conforming to a second subnetwork communication protocol; encrypting the second packet data by using a preset second subnetwork security key, so as to obtain a second encrypted packet; and sending the second encrypted packet to a corresponding communication device in the second subnetwork. By means of the data communication method and system for an in-vehicle network comprising multiple subnetworks and the gateway in the present application, data packets transmitted among subnetworks are in communication in a form of ciphertexts, thereby improving the security of an in-vehicle network.

(57) 摘要:

[见续页]

WO 2017/067154 A1



(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, 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)。

根据细则 4.17 的声明:

— 关于申请人有权要求在先申请的优先权(细则 4.17(iii))

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

本发明的实施例提供一种用于包括多个子网的车载网络的数据通信方法、系统及网关。其中, 用于包括多个子网的车载网络的数据通信方法包括: 获取自第一子网的通信设备发送给第二子网的第一加密报文; 利用预定的第一子网安全密钥将所述第一加密报文解密, 获得第一报文数据; 将所述第一报文数据转换为符合第二子网通信协议的第二报文数据; 利用预定的第二子网安全密钥将所述第二报文数据加密, 得到第二加密报文; 将所述第二加密报文发送给所述第二子网中的相应通信设备。本申请实施例的用于包括多个子网的车载网络的数据通信方法、系统及网关, 能够使子网间传递的报文以密文形式进行通信, 从而提高了车载网络的安全性。

用于包括多个子网的车载网络的数据通信方法、系统及网关

交叉引用

- 5 本申请引用于 2015 年 10 月 21 日提交的专利名称为“用于包括多个子网的车载网络的数据通信方法、系统及网关”的第 201510689773X 号中国专利申请，其通过引用被全部并入本申请。

技术领域

- 10 本发明的实施例涉及车载网络通信技术，尤其涉及一种用于包括多个子网的车载网络的数据通信方法、系统及网关。

背景技术

- 众所周知，汽车由发动机、底盘、车身和电器共四个系统组成。每个系统都包含多个通信设备，每个通信设备内置电子控制单元(Electronic Control Unit, ECU)。从用途上讲，ECU 是汽车专用微机控制器，也称汽车专用单片机。ECU 之间需要通信，并且依赖于各种不同的总线协议。因此，汽车内部具有多种总线协议，例如控制器局域网(Controller Area Network, CAN)总线协议、局部互联网络(Local Interconnect Network, LIN)总线协议、面向媒体的系统传输(Media Oriented System Transport, MOST)总线协议、FLEXRAY 总线协议、以太网(ETHERNET)总线协议等。
- 15
- 20

- 图 1 是示出现有技术中车载网络的示例性示意图之一，图 2 是示出现有技术中车载网络的示例性示意图之二。参照图 1 和图 2，车载网络的中心节点是车载网关。车载网关具有多种接口，可连接适用例如 CAN、LIN、MOST 等协议的多重网络。每种总线协议构成一个独立的子网(如子网 1)，每个子网内包含一定数量的上述通信设备。
- 25

- 随着人们对汽车安全的关注度的不断提高，信息安全问题是车载网络中尚未得到很好解决的问题。基于上述车载网络拓扑结构，如图 1 所示，当子网 1 中的报文传递到子网 2 时，需要在网关进行一次转发。其
- 30

过程中报文 $P(n)$ 全部以明文形式传递。然而，明文形式的报文很容易被监听和被破解，从而给行车带来安全隐患。

发明内容

5

本申请的目的在于，提供一种用于包括多个子网的车载网络的数据通信方法、系统及网关，以使子网间传递的报文以密文形式进行通信，为行车建立更加安全、稳定的网络环境。

10 为实现上述发明目的，本申请的实施例提供了一种用于包括多个子网的车载网络的数据通信方法，包括：获取自第一子网的通信设备发送给第二子网的第一加密报文；利用预定的第一子网安全密钥将所述第一加密报文解密，获得第一报文数据；将所述第一报文数据转换为符合第二子网通信协议的
15 第二报文数据；利用预定的第二子网安全密钥将所述第二报文数据加密，得到第二加密报文；将所述第二加密报文发送给所述第二子网中的相应通信设备。

优选地，所述预定的第一子网安全密钥和所述预定的第二子网安全密钥不同。

20 优选地，所述利用预定的第一子网安全密钥将所述第一加密报文解密，获得第一报文数据的处理包括：根据所述预定的第一子网安全密钥使用对称加密算法对所述第一加密报文进行解密，得到第一报文数据；所述利用预定的第二子网安全密钥将所述第二报文数据加密，得到第二加密报文的处理包括：根据所述预定的第二子网安全密钥使用对称加密算法对所述
25 第二报文数据进行加密，得到第二加密报文。

优选地，所述对称加密算法是数据加密标准 DES 算法或高级加密标准 AES 算法。

优选地，所述方法还包括：根据预设的密钥更新算法更新第一子网安全密钥；将所述更新的第一子网安全密钥发送给所述第一子网中的通信设备。

30 优选地，所述将所述更新的第一子网安全密钥发送给所述第一子网中

的通信设备的处理包括：使用当前的第一子网安全密钥将密钥更新报文加密，所述密钥更新报文包括所述更新的第一子网安全密钥；将加密的密钥更新报文发送至所述第一子网中的通信设备。

优选地，在车载网络的网关上执行所述方法。

5 本申请的实施例还提供了一种车载网络的网关，包括：报文获取模块，用于获取自第一子网的通信设备发送给第二子网的第一加密报文；报文解密模块，用于利用预定的第一子网安全密钥将所述第一加密报文解密，获得第一报文数据；通信协议转换模块，用于将所述第一报文数据转换为符合第二子网通信协议的

10 第二报文数据；报文加密模块，用于利用预定的第二子网安全密钥将所述第二报文数据加密，得到第二加密报文；报文发送模块，用于将所述第二加密报文发送给所述第二子网中的相应通信设备。

优选地，所述预定的第一子网安全密钥和所述预定的第二子网安全密钥不同。

15 优选地，所述报文解密模块用于根据所述预定的第一子网安全密钥使用对称加密算法对所述第一加密报文进行解密，得到第一报文数据；所述报文加密模块用于根据所述预定的第二子网安全密钥使用对称加密算法对所述第二报文数据进行加密，得到第二加密报文。

优选地，所述对称加密算法是数据加密标准 DES 算法或高级加密标准 AES 算法。

20 优选地，所述网关还包括：密钥更新模块，用于根据预设的密钥更新算法获得更新的第一子网安全密钥；密钥发送模块，用于将所述更新的第一子网安全密钥发送给所述第一子网中的通信设备。

25 优选地，所述密钥发送模块包括：密钥更新报文加密单元，用于使用当前的第一子网安全密钥将密钥更新报文加密，所述密钥更新报文包括所述更新的第一子网安全密钥；密钥更新报文发送单元，用于将加密的密钥更新报文发送至所述第一子网中的通信设备。

30 本申请的实施例还提供了一种车载网络的数据通信系统，包括：多个子网和如前述实施例所述的车载网络的网关，其中，每个所述子网包括多个通信设备，所述通信设备用于从所述网关接收加密的第一报文，将所述第一报文解密，并且将发送给所述网关的第二报文加密，将加密的第二报

文发送给所述网关。

本申请的实施例还提供了一种车载网络的网关，包括：

处理器、存储器、通信接口和总线；其中，

所述处理器、存储器、通信接口通过所述总线完成相互间的通信；

5 所述通信接口用于该网关与车辆的通信设备之间的信息传输；

所述处理器用于调用所述存储器中的逻辑指令，以执行如下方法：

获取自第一子网的通信设备发送给第二子网的第一加密报文；利用预

定的第一子网安全密钥将所述第一加密报文解密，获得第一报文数据；将

所述第一报文数据转换为符合第二子网通信协议的第二报文数据；利用预

10 定的第二子网安全密钥将所述第二报文数据加密，得到第二加密报文；将

所述第二加密报文发送给所述第二子网中的相应通信设备。

本申请的实施例还提供了一种计算机程序，包括程序代码，所述程序代码用于执行如下操作：

获取自第一子网的通信设备发送给第二子网的第一加密报文；

15 利用预定的第一子网安全密钥将所述第一加密报文解密，获得第一报文数据；

将所述第一报文数据转换为符合第二子网通信协议的第二报文数据；

利用预定的第二子网安全密钥将所述第二报文数据加密，得到第二加密报文；

20 将所述第二加密报文发送给所述第二子网中的相应通信设备。

本申请的实施例还提供了一种存储介质，用于存储如前所述的计算机程序。

本申请实施例提供的用于包括多个子网的车载网络的数据通信方法、系统及网关，可为执行数据通信的两个子网的通信设备自动、快速地对二者间传递的报文进行加密和解密处理，从而更安全、可靠地进行交互。其中，子网安全密钥极大地保证了子网的通信设备之间交互的安全性和稳定性，极大地提升了用户行车体验。

附图说明

30 图 1 为示出现有技术中车载网络的示例性示意图之一；

图 2 为示出现有技术中车载网络的示例性示意图之二；

图 3 为示出反映本申请的总体发明构思的一个示例的示意图；

图 4 为示出本申请实施例一的用于包括多个子网的车载网络的数据通信方法的流程图；

5 图 5 为示出本申请实施例二的车载网络的网关的逻辑框图；

图 6 为示出本申请实施例三的车载网络的数据通信系统的逻辑框图；

图 7 为示出本申请实施例四的车载网络的网关的结构框图。

具体实施方式

10

本申请的基本构思是，提供一种基于安全密钥为进行数据通信的两个子网间传递的报文进行加密和解密处理，再进行报文传输的技术方案，从而使得子网的通信设备之间更安全、可靠地进行交互。

图 3 是示出反映本申请的总体发明构思的一个示例的示意图。

15 参照图 3，车载网关中存有各个子网相应的密钥，当一个报文需要从子网 1 传递到子网 2 上时，子网 1 的加密报文可能与子网 2 的加密报文所使用的通信协议不同。

例如，车载网关接收来自子网 1 的密文报文 $P(1)K(1)$ ，利用子网 1 的密钥 $K(1)$ 解析所述密文报文 $P(1)K(1)$ 得到报文数据 $P(1)$ ，然后再对报文数据 $P(1)$ 做不同子网的通信协议转换，转换成符合子网 2 的通信协议的报文数据 $P(2)$ ，最后利用子网 2 的密钥 $K(2)$ 将完成通信协议转换的报文数据 $P(2)$ 加密得到密文报文 $P(2)K(2)$ ，并将密文报文 $P(2)K(2)$ 发送到子网 2 上。

20 由此可见，在车载网络内部的数据通信过程中，报文皆是以密文形式传递的，密文形式的报文具有不易被监听和被破解的优势。因此，在车载网络中通过密文形式进行数据通信可保证子网的通信设备之间交互的安全性和稳定性，提高行车安全，进而提升用户行车体验。

此外，因子网的通信设备之间采用不同的密钥，即使某个子网被攻破，并不会影响到其他子网，其他子网仍然是安全的。

下面结合附图详细描述本申请实施例的用于包括多个子网的车载网络的数据通信方法、系统及网关。

30

实施例一

图 4 是示出本申请实施例一的用于包括多个子网的车载网络的数据通信方法的流程图。可例如在车载网络的网关上执行所述方法。

参照图 4，在步骤 S410，获取自第一子网的通信设备发送给第二子网的第一加密报文。

具体地，当第一子网的通信设备需要与第二子网的通信设备进行数据通信时，第一子网的通信设备会使用预存的预定第一子网安全密钥将报文数据加密得到第一加密报文，并且将第一加密报文放在总线上进行发送。相应地，车载网络的网关从总线获取第一加密报文。这里，子网安全密钥的长度可以是 128 比特或 256 比特。

在步骤 S420，利用预定的第一子网安全密钥将所述第一加密报文解密，获得第一报文数据。

在具体的实现方式中，预定的第一子网安全密钥可预先存入车载网络的网关及第一子网的通信设备，在使用时直接获取即可，或者从存储有各个子网安全密钥的服务器下载，再或者从如 U 盘等存储设备直接拷入。同样地，对于包括多个子网的车载网络，其他子网的安全密钥也可运用上述相同的实现方式。

在步骤 S430，将所述第一报文数据转换为符合第二子网通信协议的第二报文数据。

在步骤 S440，利用预定的第二子网安全密钥将所述第二报文数据加密，得到第二加密报文。

在步骤 S450，将所述第二加密报文发送给所述第二子网中的相应通信设备。

本申请实施例的用于包括多个子网的车载网络的数据通信方法，接收通信发起方发送的加密报文，进一步对加密报文进行解密、通信协议转换及加密的处理，从而自动、快速地发送适用于通信接收方的加密报文，极大地保证了子网的通信设备之间交互的安全性、流畅性和稳定性，且提升了用户行车体验。

在此基础上，由于在车载网络的设备中，对系统反馈和资源使用具有较高的要求，因此可考虑对使用的加密解密算法进行优化。在加密解密算法中，

对称加密算法相对简单、系统开销小的优点，适合对大量数据进行加解密。

因此，根据本申请的示例性实施例，在步骤 S420，根据所述预定的第一子网安全密钥使用对称加密算法对所述第一加密报文进行解密，得到第一报文数据。

- 5 同理，根据本申请的示例性实施例，在步骤 S440，根据所述预定的第二子网安全密钥使用对称加密算法对所述第二报文数据进行加密，得到第二加密报文。

需要说明的是，本发明实施例中的对称加密算法不仅可以通过软件实现，也可以通过硬件实现。

- 10 进一步地，所述对称加密算法可以是数据加密标准 DES 算法或高级加密标准 AES 算法，从而进一步对采用的加密算法进行优化。其中，数据加密标准 DES 算法运行速度较快，适用于加密大量数据的场合，而高级加密标准 AES 算法是下一代的加密算法标准，运行速度比数据加密标准 DES 算法还要快，且安全级别高。

- 15 此外，根据本申请的优选实施例，所述预定的第一子网安全密钥和所述预定的第二子网安全密钥不同。

- 举例来说，第二加密报文被发送到第二子网的总线上进行传递。第二子网中的相应通信设备从总线上获取即可。即使第二加密报文被非法的节点监听，但由于该节点没有第二子网的密钥，因此也不能够解析报文数据，更不能反推报文中每个字段的含义。由此，监听到的第二加密报文没有任何价值。

- 20 在具体的实现方式中，各个子网使用不同的安全密钥。这些安全密钥作为初始密钥在汽车出厂前，第一次被植入车载网络的网关和通信设备中的 ECU。由于汽车厂内部出现密钥泄露的机会很小，从而确保初始密钥的安全性。

- 25 但在后续行车过程中安全性存在隐患，因此，需要对不同子网所使用的安全密钥进行定期更新，更新的过程由车载网络的网关管理。例如，在安全密钥到期之后，网关需要向子网发送密钥更新报文，密钥更新报文中携带有新密钥。该密钥更新报文的发送同样需要以密文形式传递，可利用旧密钥对密钥更新报文进行加密，然后通过例如广播的方式发送到子网的总线上。子网
30 网内通信设备中的 ECU 从所属子网的总线获取密钥更新报文，再利用旧密钥

对密钥更新报文进行解密得到新密钥，进一步存储新密钥即可。以此类推，网关依次对不同子网逐个进行上述密钥更新处理过程。

为此，所述方法可还包括：根据预设的密钥更新算法更新第一子网安全密钥；将所述更新的第一子网安全密钥发送给所述第一子网中的通信设备。

- 5 具体地，利用密钥更新算法获得更新的第一子网安全密钥；其次，可使用当前的第一子网安全密钥将密钥更新报文加密，所述密钥更新报文包括所述更新的第一子网安全密钥；将加密的密钥更新报文发送至所述第一子网中的通信设备。

实施例二

- 10 图 5 是示出本申请实施例二的车载网络的网关的逻辑框图。可用于执行如图 4 所示实施例的方法步骤。

参照图 5，车载网络的网关包括报文获取模块 510、报文解密模块 520、通信协议转换模块 530、报文加密模块 540 和报文发送模块 550。

- 15 报文获取模块 510 用于获取自第一子网的通信设备发送给第二子网的第一加密报文。

报文解密模块 520 用于利用预定的第一子网安全密钥将所述第一加密报文解密，获得第一报文数据。

具体地，所述报文解密模块 520 可用于根据所述预定的第一子网安全密钥使用对称加密算法对所述第一加密报文进行解密，得到第一报文数据。

- 20 这里，所述对称加密算法可以是数据加密标准 DES 算法或高级加密标准 AES 算法。

通信协议转换模块 530 用于将所述第一报文数据转换为符合第二子网通信协议的第二报文数据。

- 25 报文加密模块 540 用于利用预定的第二子网安全密钥将所述第二报文数据加密，得到第二加密报文。

具体地，所述报文加密模块 540 可用于根据所述预定的第二子网安全密钥使用对称加密算法对所述第二报文数据进行加密，得到第二加密报文。

报文发送模块 550 用于将所述第二加密报文发送给所述第二子网中的相应通信设备。

- 30 优选地，所述预定的第一子网安全密钥和所述预定的第二子网安全密钥

不同。

进一步地，所述网关还可以包括：密钥更新模块（未示出），用于根据预设的密钥更新算法获得更新的第一子网安全密钥；密钥发送模块（未示出），用于将所述更新的第一子网安全密钥发送给所述第一子网中的通信设备。

- 5 更进一步地，所述密钥发送模块可包括：密钥更新报文加密单元（未示出），用于使用当前的第一子网安全密钥将密钥更新报文加密，所述密钥更新报文包括所述更新的第一子网安全密钥；密钥更新报文发送单元（未示出），用于将加密的密钥更新报文发送至所述第一子网中的通信设备。

10 本申请实施例提供的车载网络的网关，可根据通信发起方的通信设备所属子网安全密钥对其发送的加密报文进行解密，然后对解密得到报文数据进行通信协议转换，并利用通信接收方的通信设备所属子网安全密钥将转换后的报文数据加密，再发送给通信接收方的通信设备，从而使得交互过程更加安全、可靠。尤其是子网安全密钥极大地保证了子网的通信设备之间交互的安全性和稳定性，提升了用户行车体验。

15 实施例三

图 6 是示出本申请实施例三的车载网络的数据通信系统的逻辑框图。

参照图 6，所述数据通信系统包括：多个子网 610 和如前述实施例二的车载网络的网关 620，其中，每个所述子网 610 包括多个通信设备 630。

20 通信设备 630 用于从所述网关接收加密的第一报文，将所述第一报文解密，并且将发送给所述网关的第二报文加密，将加密的第二报文发送给所述网关。

25 本申请实施例提供的车载网络的数据通信系统，可为执行数据通信的两个子网的通信设备，自动、快速地对通信发起方传递给网关的报文，以及网关传递给通信接收方的报文进行加密和解密处理，从而为车载网络的网关和多个子网提供更加安全、可靠的数据通信环境，极大地提升了用户行车体验。

实施例四

图 7 是示出本申请实施例四的车载网络的网关的结构框图。

参照图 7，所述网关，包括：

30 处理器(processor)101、存储器(memory)102、通信接口(Communications Interface)103 和总线 104；其中，

所述处理器 101、存储器 102、通信接口 103 通过所述总线 104 完成相互间的通信；

所述通信接口 103 用于该网关与车辆的通信设备之间的信息传输；

所述处理器 101 用于调用所述存储器 102 中的逻辑指令，以执行如下

5 方法；

获取自第一子网的通信设备发送给第二子网的第一加密报文；利用预定的第一子网安全密钥将所述第一加密报文解密，获得第一报文数据；将所述第一报文数据转换为符合第二子网通信协议的第二报文数据；利用预定的第二子网安全密钥将所述第二报文数据加密，得到第二加密报文；将
10 所述第二加密报文发送给所述第二子网中的相应通信设备。

实施例五

参看图 4，本实施例公开一种计算机程序，包括程序代码，所述程序代码用于执行如下操作：

获取自第一子网的通信设备发送给第二子网的第一加密报文；

15 利用预定的第一子网安全密钥将所述第一加密报文解密，获得第一报文数据；

将所述第一报文数据转换为符合第二子网通信协议的第二报文数据；

利用预定的第二子网安全密钥将所述第二报文数据加密，得到第二加密报文；

20 将所述第二加密报文发送给所述第二子网中的相应通信设备。

实施例六

本实施例公开一种存储介质，用于存储如前述实施例所述的计算机程序。

本领域普通技术人员可以理解：实现上述方法实施例的全部或部分步骤
25 可以通过程序指令相关的硬件来完成，前述的程序可以存储于一计算机可读取存储介质中，该程序在执行时，执行包括上述方法实施例的步骤；而前述的存储介质包括：ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

最后应说明的是：以上各实施例仅用以说明本发明的实施例的技术方案，
30 而非对其限制；尽管参照前述各实施例对本发明的实施例进行了详细的说明，

本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分或者全部技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质的脱离本发明的实施例各实施例技术方案的范围。

权 利 要 求 书

1、一种用于包括多个子网的车载网络的数据通信方法，其特征在于，包括：

获取自第一子网的通信设备发送给第二子网的第一加密报文；

5 利用预定的第一子网安全密钥将所述第一加密报文解密，获得第一报文数据；

将所述第一报文数据转换为符合第二子网通信协议的第二报文数据；

利用预定的第二子网安全密钥将所述第二报文数据加密，得到第二加密报文；

10 将所述第二加密报文发送给所述第二子网中的相应通信设备。

2、根据权利要求 1 所述的方法，其特征在于，所述预定的第一子网安全密钥与所述预定的第二子网安全密钥不同。

3、根据权利要求 2 所述的方法，其特征在于，所述利用预定的第一子网安全密钥将所述第一加密报文解密，获得第一报文数据的处理包括：

15 根据所述预定的第一子网安全密钥使用对称加密算法对所述第一加密报文进行解密，得到第一报文数据；

所述利用预定的第二子网安全密钥将所述第二报文数据加密，得到第二加密报文的处理包括：

20 根据所述预定的第二子网安全密钥使用对称加密算法对所述第二报文数据进行加密，得到第二加密报文。

4、根据权利要求 3 所述的方法，其特征在于，所述对称加密算法是数据加密标准 DES 算法或高级加密标准 AES 算法。

5、根据权利要求 1~4 中任一所述的方法，其特征在于，所述方法还包括：

25 根据预设的密钥更新算法更新第一子网安全密钥；

将所述更新的第一子网安全密钥发送给所述第一子网中的通信设备。

6、根据权利要求 5 所述的方法，其特征在于，所述将所述更新的第一子网安全密钥发送给所述第一子网中的通信设备的处理包括：

30 使用当前的第一子网安全密钥将密钥更新报文加密，所述密钥更新报文包括所述更新的第一子网安全密钥；

将加密的密钥更新报文发送至所述第一子网中的通信设备。

7、根据权利要求 6 所述的方法，其特征在于，在车载网络的网关上执行所述方法。

8、一种车载网络的网关，其特征在于，包括：

5 报文获取模块，用于获取自第一子网的通信设备发送给第二子网的第一加密报文；

报文解密模块，用于利用预定的第一子网安全密钥将所述第一加密报文解密，获得第一报文数据；

10 通信协议转换模块，用于将所述第一报文数据转换为符合第二子网通信协议的第二报文数据；

报文加密模块，用于利用预定的第二子网安全密钥将所述第二报文数据加密，得到第二加密报文；

报文发送模块，用于将所述第二加密报文发送给所述第二子网中的相应通信设备。

15 9、根据权利要求 8 所述的网关，其特征在于，所述预定的第一子网安全密钥和所述预定的第二子网安全密钥不同。

10、根据权利要求 9 所述的网关，其特征在于，所述报文解密模块用于根据所述预定的第一子网安全密钥使用对称加密算法对所述第一加密报文进行解密，得到第一报文数据；

20 所述报文加密模块用于根据所述预定的第二子网安全密钥使用对称加密算法对所述第二报文数据进行加密，得到第二加密报文。

11、根据权利要求 10 所述的网关，其特征在于，所述对称加密算法是数据加密标准 DES 算法或高级加密标准 AES 算法。

25 12、根据权利要求 8~11 中任一所述的网关，其特征在于，所述网关还包括：

密钥更新模块，用于根据预设的密钥更新算法获得更新的第一子网安全密钥；

密钥发送模块，用于将所述更新的第一子网安全密钥发送给所述第一子网中的通信设备。

30 13、根据权利要求 12 所述的网关，其特征在于，所述密钥发送模块

包括：

密钥更新报文加密单元，用于使用当前的第一子网安全密钥将密钥更新报文加密，所述密钥更新报文包括所述更新的第一子网安全密钥；

5 密钥更新报文发送单元，用于将加密的密钥更新报文发送至所述第一子网中的通信设备。

14、一种车载网络的数据通信系统，其特征在于，包括：多个子网和如权利要求 8~13 中任一项所述的车载网络的网关，其中，每个所述子网包括多个通信设备，所述通信设备用于从所述网关接收加密的第一报文，将所述第一报文解密，并且将发送给所述网关的第二报文加密，将加密的
10 第二报文发送给所述网关。

15、一种车载网络的网关，其特征在于，包括：
处理器、存储器、通信接口和总线；其中，
所述处理器、存储器、通信接口通过所述总线完成相互间的通信；
所述通信接口用于该网关与车辆的通信设备之间的信息传输；
15 所述处理器用于调用所述存储器中的逻辑指令，以执行如下方法：
获取自第一子网的通信设备发送给第二子网的第一加密报文；利用预定的第一子网安全密钥将所述第一加密报文解密，获得第一报文数据；将所述第一报文数据转换为符合第二子网通信协议的第二报文数据；利用预定的第二子网安全密钥将所述第二报文数据加密，得到第二加密报文；将
20 所述第二加密报文发送给所述第二子网中的相应通信设备。

16、一种计算机程序，其特征在于，包括程序代码，所述程序代码用于执行如下操作：

获取自第一子网的通信设备发送给第二子网的第一加密报文；
利用预定的第一子网安全密钥将所述第一加密报文解密，获得第一报
25 文数据；

将所述第一报文数据转换为符合第二子网通信协议的第二报文数据；
利用预定的第二子网安全密钥将所述第二报文数据加密，得到第二加密报文；

将所述第二加密报文发送给所述第二子网中的相应通信设备。

30 17、一种存储介质，用于存储如权利要求 16 所述的计算机程序。

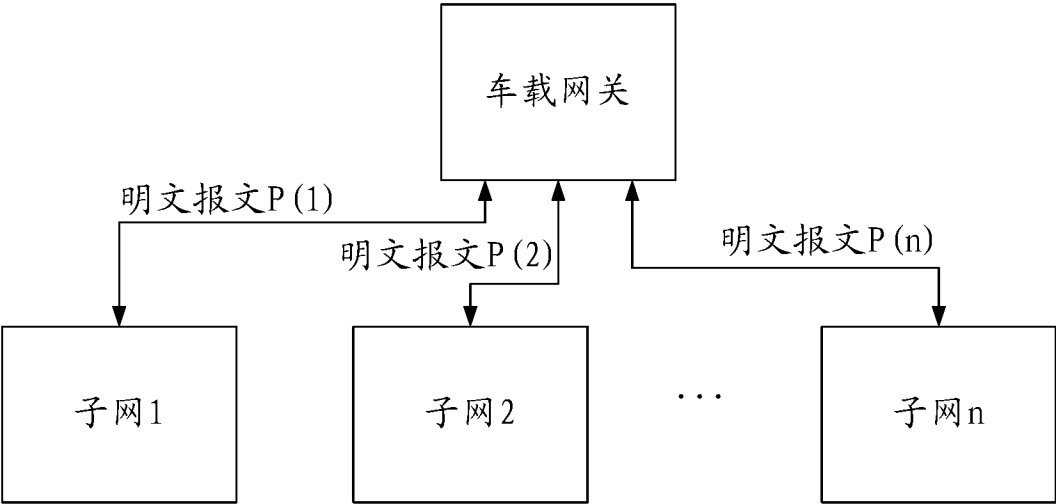


图 1

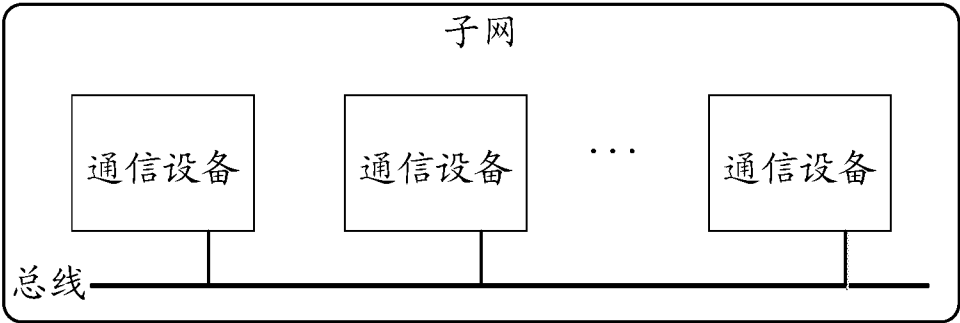


图 2

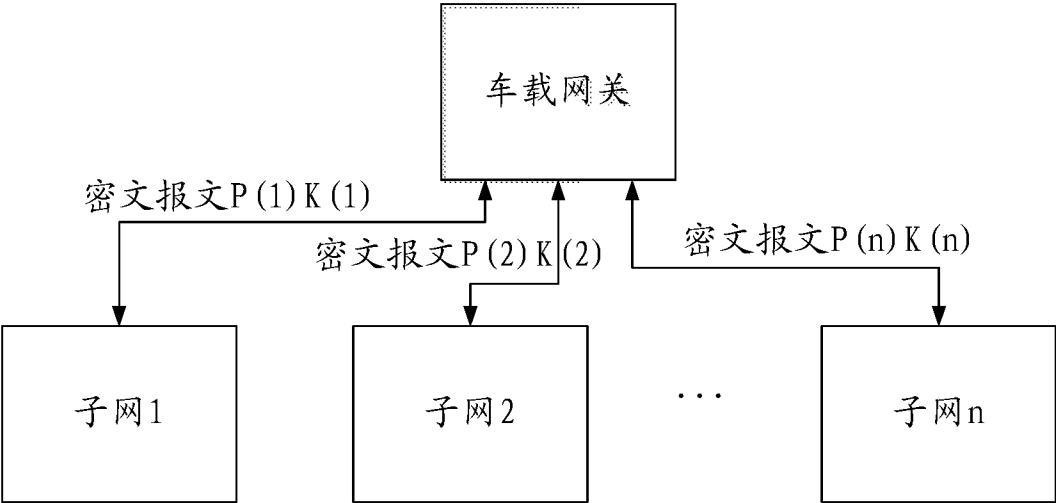


图 3

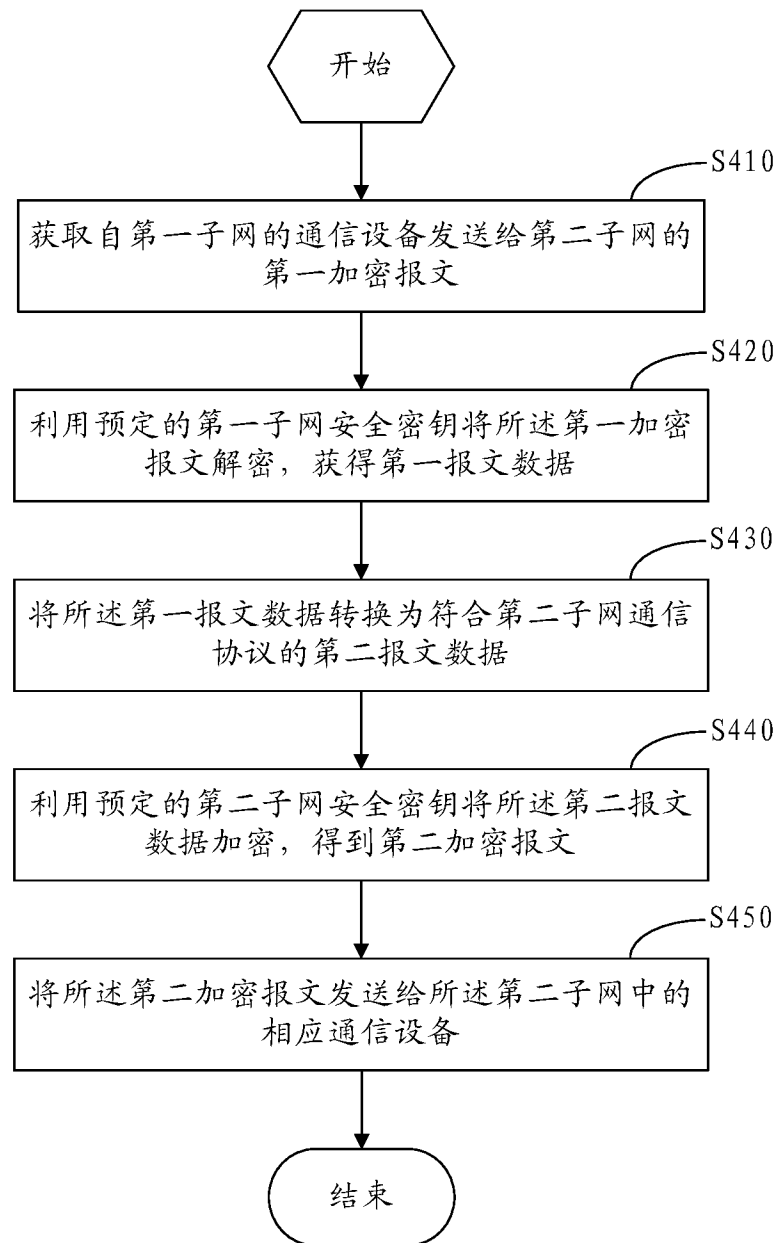


图 4

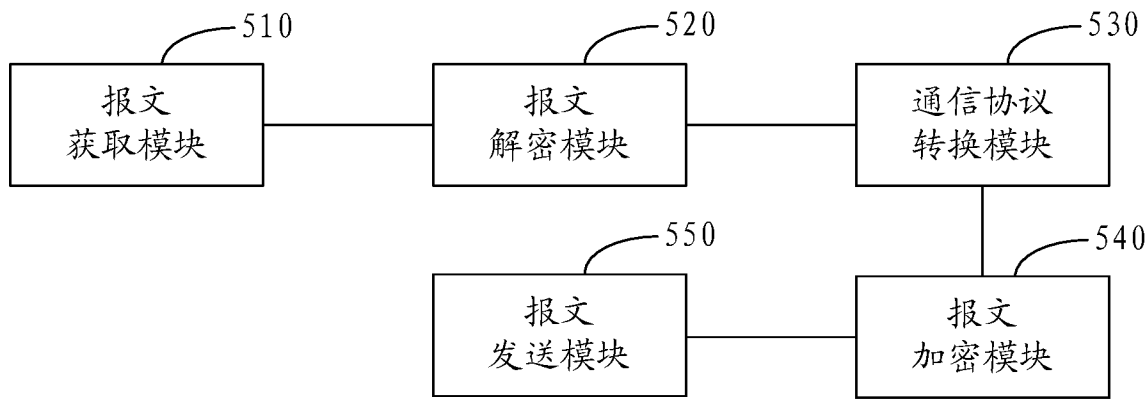


图 5

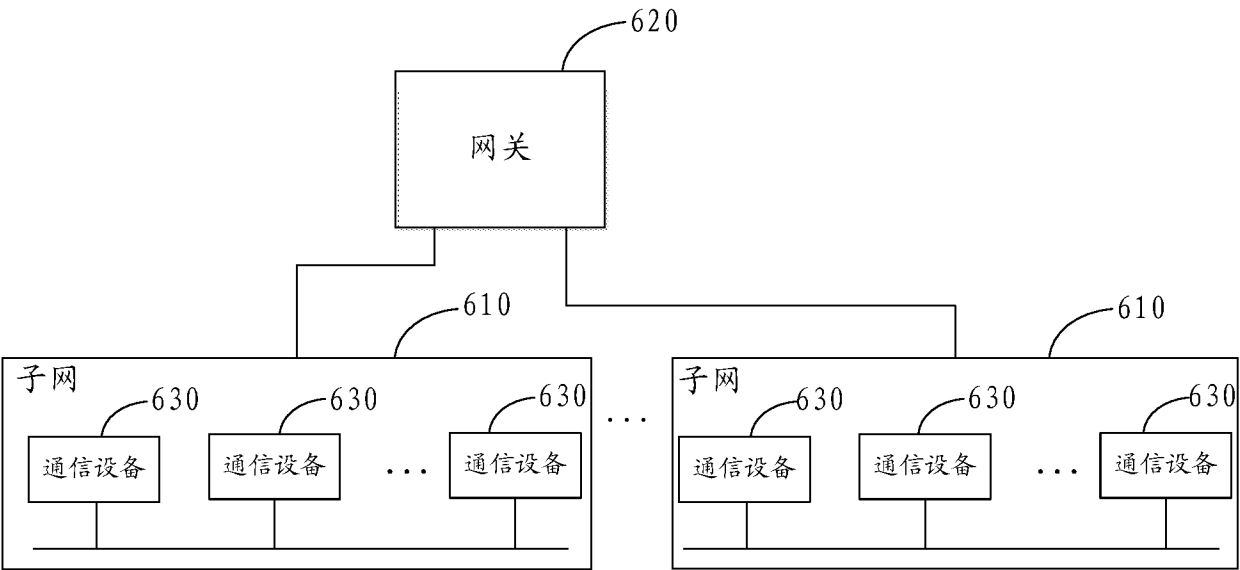


图 6

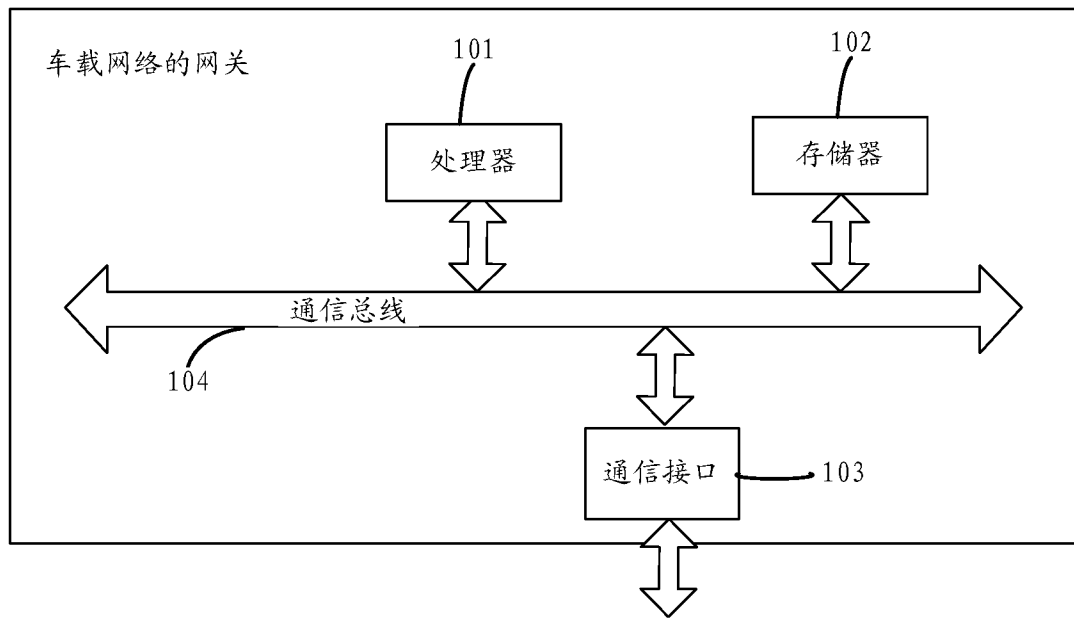


图 7

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/082074

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32 (2006.01) i; H04L 12/66 (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

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)

CNKI, CNPAT, WPI, EPODOC, IEEE, GOOGLE SCHOLAR: gateway, decode, private key, encryption, public key, vehicle, bus, car, network, subnet, ???cipher???, security, key, region, domain

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 103685000 A (ROBERT BOSCH GMBH), 26 March 2014 (26.03.2014), claim 1, and description, paragraphs [0041]-[0074], and figures 3-6	1-17
Y	CN 102546184 A (BEIJING MT-HIRISUN TECHNOLOGY CO., LTD.), 04 July 2012 (04.07.2012), claim 1, and description, paragraph [0026]	1-17
A	US 2008065289 A1 (SPX CORPORATION), 13 March 2008 (13.03.2008), the whole document	1-17
A	CN 103067166 A (HAIER ELECTRONICS GROUP CO., LTD. et al.), 24 April 2013 (24.04.2013), the whole document	1-17

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search 08 July 2016 (08.07.2016)	Date of mailing of the international search report 26 July 2016 (26.07.2016)
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 XIONG, Jin'an Telephone No.: (86-10) 62413381

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2016/082074

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103685000 A	26 March 2014	US 2014133350 A1	15 May 2014
		FR 2995161 A1	07 March 2014
		IT MI20131430 A1	06 March 2014
		KR 20140031812 A	13 March 2014
		DE 102012215765 A1	15 May 2014
		IN2510DEL2013 A	20 February 2015
CN 102546184 A	04 July 2012	None	
US 2008065289 A1	13 March 2008	US 2011257837 A1	20 October 2011
CN 103067166 A	24 April 2013	WO 2013056502 A1	25 April 2013

A. 主题的分类 H04L 9/32(2006.01)i; H04L 12/66(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 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)) CNKI, CNPAT, WPI, EPODOC, IEEE, GOOGLE SCHOLAR: 车, 子网, 域, 网关, 解密, 私钥, 总线, 加密, 公钥, 安全, 密码, 密钥, vehicle, bus, car, network, subnet, ???cipher???, security, key, region, domain																	
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>Y</td> <td>CN 103685000 A (罗伯特. 博世有限公司) 2014年 3月 26日 (2014 - 03 - 26) 权利要求1、说明书[0041]-[0074]段, 附图3-6</td> <td>1-17</td> </tr> <tr> <td>Y</td> <td>CN 102546184 A (北京海联捷讯信息科技发展有限公司) 2012年 7月 4日 (2012 - 07 - 04) 权利要求1、说明书[0026]段</td> <td>1-17</td> </tr> <tr> <td>A</td> <td>US 2008065289 A1 (SPX CORPORATION) 2008年 3月 13日 (2008 - 03 - 13) 全文</td> <td>1-17</td> </tr> <tr> <td>A</td> <td>CN 103067166 A (海尔集团公司等) 2013年 4月 24日 (2013 - 04 - 24) 全文</td> <td>1-17</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	Y	CN 103685000 A (罗伯特. 博世有限公司) 2014年 3月 26日 (2014 - 03 - 26) 权利要求1、说明书[0041]-[0074]段, 附图3-6	1-17	Y	CN 102546184 A (北京海联捷讯信息科技发展有限公司) 2012年 7月 4日 (2012 - 07 - 04) 权利要求1、说明书[0026]段	1-17	A	US 2008065289 A1 (SPX CORPORATION) 2008年 3月 13日 (2008 - 03 - 13) 全文	1-17	A	CN 103067166 A (海尔集团公司等) 2013年 4月 24日 (2013 - 04 - 24) 全文	1-17
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求															
Y	CN 103685000 A (罗伯特. 博世有限公司) 2014年 3月 26日 (2014 - 03 - 26) 权利要求1、说明书[0041]-[0074]段, 附图3-6	1-17															
Y	CN 102546184 A (北京海联捷讯信息科技发展有限公司) 2012年 7月 4日 (2012 - 07 - 04) 权利要求1、说明书[0026]段	1-17															
A	US 2008065289 A1 (SPX CORPORATION) 2008年 3月 13日 (2008 - 03 - 13) 全文	1-17															
A	CN 103067166 A (海尔集团公司等) 2013年 4月 24日 (2013 - 04 - 24) 全文	1-17															
☐ 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 2016年 7月 8日		国际检索报告邮寄日期 2016年 7月 26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		授权官员 熊金安 电话号码 (86-10)62413381															

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/082074

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	103685000	A	2014年 3月 26日	US	2014133350	A1	2014年 5月 15日
				FR	2995161	A1	2014年 3月 7日
				IT	MI20131430	A1	2014年 3月 6日
				KR	20140031812	A	2014年 3月 13日
				DE	102012215765	A1	2014年 5月 15日
					IN2510DEL2013	A	2015年 2月 20日
CN	102546184	A	2012年 7月 4日	无			
US	2008065289	A1	2008年 3月 13日	US	2011257837	A1	2011年 10月 20日
CN	103067166	A	2013年 4月 24日	WO	2013056502	A1	2013年 4月 25日