(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
2018 年 5 月 3 日 (03.05.2018)

WIPO | PCT

(10) 国际公布号
WO 2018/076564 A1

(51) 国际专利分类号:
H04L 9/30 (2006.01) *H04L 29/06* (2006.01)
H04L 9/32 (2006.01) *H04L 29/08* (2006.01)

(21) 国际申请号: PCT/CN2017/072672

(22) 国际申请日: 2017 年 1 月 25 日 (25.01.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610933025.6 2016年10月31日 (31.10.2016) CN

(71) 申请人: 宇龙计算机通信科技（深圳）有限公司 (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.) [CN/CN]; 中国广东省深圳市南山区科技园北区梦溪道2号, Guangdong 518057 (CN)。

(72) 发明人: 钟焰涛(ZHONG, Yantao); 中国广东省深圳市南山区科技园北区梦溪道2号, Guangdong 518057 (CN)。 郑倩(ZHENG, Qian); 中国广东省深圳市南山区科技园北区梦溪道2号, Guangdong 518057 (CN)。 邓一伟(DENG, Yiwei); 中国广东省深圳市南山区科技园北区梦溪道2号, Guangdong 518057 (CN)。 高俊鹏(GAO, Junpeng); 中国广东省深圳市南山区科技园北区梦溪道2号, Guangdong 518057 (CN)。 李红威(LI, Hongwei); 中国广东省深圳市南山区科技园北区梦溪道2号, Guangdong 518057 (CN)。

(74) 代理人: 北京友联知识产权代理事务所（普通合伙）(YOULINK INTELLECTUAL PROPERTY LAW FIRM); 中国北京市海淀区学清路8号科技财富中心A座506室尚志峰, Beijing 100192 (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,

(54) **Title:** PRIVACY PROTECTION METHOD AND PRIVACY PROTECTION DEVICE IN VEHICLE COMMUNICATION

(54) **发明名称:** 车辆通信中的隐私保护方法及隐私保护装置

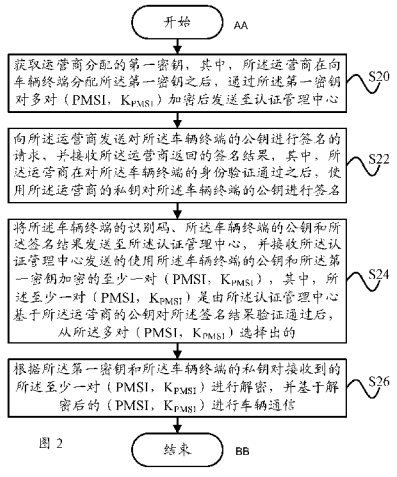

图 2

S20 Acquiring a first secret key allocated by an operator, wherein after the operator allocates the first secret key to a vehicle terminal, a plurality of pairs of (PMSI, KPMSI) are encrypted via the first secret key and are then sent to an authentication management centre

S22 Sending, to the operator, a request for performing signature on a public key of the vehicle terminal, and receiving a signature result returned by the operator, wherein the operator uses a private key of the operator to perform signature on the public key of the vehicle terminal after identity verification of the vehicle terminal is passed

S24 Sending an identification code of the vehicle terminal, the public key of the vehicle terminal and the signature result to the authentication management centre, and receiving at least one pair of (PMSI, KPMSI), sent by the authentication management centre, encrypted using the public key of the vehicle terminal and the first secret key, wherein the at least one pair of (PMSI, KPMSI) is selected from the plurality of pairs of (PMSI, KPMSI) after the verification of the signature result by the authentication management centre based on the public key of the operator is passed

S26 Decrypting the received at least one pair of (PMSI, KPMSI) according to the first secret key and the private key of the vehicle terminal, and performing vehicle communication based on the decrypted (PMSI, KPMSI)

AA Start

BB End

(57) Abstract: Provided are a privacy protection method and a privacy protection device in vehicle communication. The privacy protection method comprises: acquiring a first secret key allocated by an operator, wherein after the operator allocates the first secret key, a plurality of pairs of (PMSI, KPMSI) are encrypted via the first secret key and are then sent to an authentication management centre; sending, to the operator, a request for performing signature on a public key of a vehicle terminal, and receiving a signature result returned by the operator, wherein the operator uses a private key of the operator to perform signature on the public key of the vehicle terminal; sending an identification code of the vehicle terminal, the public key of the vehicle terminal and the signature result to the authentication management centre, and receiving at least one pair of (PMSI, KPMSI), sent by the authentication management centre, encrypted using the public key of the vehicle terminal and the first secret key; and decrypting the received (PMSI, KPMSI) according to the first secret key and the private key of the vehicle terminal, and performing vehicle communication based on the decrypted (PMSI, KPMSI). The present invention significantly improves privacy security during a vehicle communication process.

WO 2018/076564 A1

[见续页]

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, 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))。

(57) 摘要：本发明提供了一种车辆通信中的隐私保护方法及隐私保护装置，隐私保护方法包括：获取运营商分配的第一密钥，其中，运营商在分配第一密钥后，通过第一密钥对多对(PMSI，K_{PMSI})加密后发送至认证管理中心；向运营商发送对车辆终端的公钥进行签名的请求，并接收运营商返回的签名结果，其中，运营商使用运营商的私钥对车辆终端的公钥进行签名；将车辆终端的识别码、车辆终端的公钥和所述签名结果发送至认证管理中心，并接收认证管理中心发送的使用车辆终端的公钥和第一密钥加密的至少一对(PMSI，K_{PMSI})；根据第一密钥和车辆终端的私钥对接收到的(PMSI，K_{PMSI})进行解密，并基于解密后的(PMSI，K_{PMSI})进行车辆通信。本发明极大地提升了车辆通信过程中的隐私安全性。

车辆通信中的隐私保护方法及隐私保护装置

本申请要求于 2016 年 10 月 31 日提交中国专利局、申请号为 201610933025.6、发明名称为“车辆通信中的隐私保护方法及隐私保护装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本发明涉及车辆通信技术领域，具体而言，涉及一种车辆通信中的隐私保护方法和一种车辆通信中的隐私保护装置。

背景技术

目前，LTE（Long Term Evolution，长期演进）已经将车联网通信纳入到了标准化范围，在相关规范中将车辆对外界（对其他车辆、对行人、对路边设施等）的通信简称为 V2X（Vehicle to X，车辆对外界）通信。

在 3GPP 的相关讨论稿中，V2X 规范中制定了以下两个互相矛盾的安全性和隐私性条款:

（1）为保护车辆的隐私，运营商应该不能分辨参与通信的车辆;

（2）为保护网络安全，运营商应该能够识别在车联网中发送恶意消息，或者有其他恶意行为的车辆。

由于运营商的行为不受其他实体控制，因此它完全可以使用条款（2）所赋予的车辆识别能力对条款（1）中的车辆隐私性进行侵犯。

为了解决上述问题，相关技术中提出的解决方案如图 1 所示，其中采用了一个称为假名中心（Pseudonym Certificate Authority）的实体。当 V-UE（vehicle User Equipment，车辆终端，即接入车联网的车辆）与 MNO（Mobile Network Operator，移动网络运营商）之间通信获取到密钥 K_{PERIOD} 之后，MNO 向 PCA 发送多对采用 K_{PERIOD} 加密的假名 ID（Pseudonymous Mobile Subscriber ID，简称 PMSI）和对应的密钥 K_{PMSI}，

即（PMSI，K_{PMSI}），进而由 PCA 来向 V-UE 分配（PMSI，K_{PMSI}），避免 MNO 分辨参与通信的车辆。同时，若 V-UE 在车联网中执行恶意行为被发现后，MNO 通过询问 PCA 可以获得该恶意车辆的身份信息。

此外，在图 1 所示的技术方案中，PCA 与 V-UE 之间需要保持一一对应的长期密钥来保证通信信道的安全，而存储这些密钥的密钥库是由 PCA 维护，随着车联网技术的普及，接入车联网的车辆越来越多，密钥库的维护难度也越来越大，并且密钥库很容易成为黑客攻击的目标，存在较大的安全隐患。

发明内容

本发明正是基于上述技术问题至少之一，提出了一种新的车辆通信中的隐私保护方案，使得车辆终端与认证管理中心之间无需保持一一对应的长期密钥，降低了认证管理中心对密钥的管理负担，同时由于无需维护密钥库，因此也有效避免了密钥库遭到攻击而造成的安全隐患，极大提升了车辆通信过程中的隐私安全性。

有鉴于此，根据本发明的第一方面，提出了一种车辆通信中的隐私保护方法，该隐私保护方法适用于车辆终端，具体包括以下步骤：

获取运营商分配的第一密钥，其中，所述运营商在向车辆终端分配所述第一密钥之后，通过所述第一密钥对多对（PMSI，K_{PMSI}）加密后发送至认证管理中心；

向所述运营商发送对所述车辆终端的公钥进行签名的请求，并接收所述运营商返回的签名结果，其中，所述运营商在对所述车辆终端的身份验证通过之后，使用所述运营商的私钥对所述车辆终端的公钥进行签名；

将所述车辆终端的识别码、所述车辆终端的公钥和所述签名结果发送至所述认证管理中心，并接收所述认证管理中心发送的使用所述车辆终端的公钥和所述第一密钥加密的至少一对（PMSI，K_{PMSI}），其中，所述至少一对（PMSI，K_{PMSI}）是由所述认证管理中心基于所述运营商的公钥对所述签名结果验证通过后，从所述多对（PMSI，K_{PMSI}）选择出的；

根据所述第一密钥和所述车辆终端的私钥对接收到的所述至少一对

（PMSI，K_{PMSI}）进行解密，并基于解密后的（PMSI，K_{PMSI}）进行车辆通信。

在该技术方案中，通过由车辆终端向运营商发送对车辆终端的公钥进行签名的请求，而运营商在对车辆终端的身份验证通过之后，使用运营商的私钥对车辆终端的公钥进行签名，进而由车辆终端将签名结果发送至认证管理中心，由认证管理中心根据运营商设备的公钥来对签名结果进行验证，使得车辆终端与认证管理中心之间进行通信时能够通过公私密钥的方式来保证通信的安全性，无需车辆终端与认证管理中心之间保持一一对应的长期密钥，进而能够降低认证管理中心对密钥的管理负担，同时由于无需维护密钥库，因此也有效避免了密钥库遭到攻击而造成的安全隐患，极大提升了车辆通信过程中的隐私安全性。

其中，车辆终端的识别码可以是 IMSI（International Mobile Subscriber Identification Number，国际移动用户识别码）或 IMEI（International Mobile Equipment Identity，国际移动设备标识）；PMSI 即为假名 ID，K_{PMSI} 是与 PMSI 相对应的密钥，车辆终端在进行车辆通信时使用假名 ID 进行通信，并能够通过 K_{PMSI} 来进行身份识别。当车辆终端在车联网中的恶意行为被发现后，运营商可以通过车辆终端的假名 ID 来询问认证管理中心，以获得相应车辆的真实身份信息，既保证运营商能够识别到在车联网中有恶意行为的车辆，也能够避免运营商肆意获取车联网中的车辆信息而导致车辆隐私泄露的问题。

根据本发明的第二方面，还提出了一种车辆通信中的隐私保护方法，该隐私保护方法适用于运营商设备，具体包括以下步骤：

向车辆终端分配第一密钥，并通过所述第一密钥对多对（PMSI，K_{PMSI}）加密后发送至认证管理中心；

在接收到所述车辆终端发送的对所述车辆终端的公钥进行签名的请求时，对所述车辆终端的身份进行验证；

在对所述车辆终端的身份验证通过之后，使用运营商设备的私钥对所述车辆终端的公钥进行签名，并将签名结果返回至所述车辆终端；

其中，所述签名结果用于供所述车辆终端发送至所述认证管理中心进

行验证，以使所述认证管理中心在对所述签名结果验证通过后向所述车辆终端发送至少一对（PMSI，K_{PMSI}）进行车辆通信。

在该技术方案中，运营商设备通过在接收到车辆终端发送的对车辆终端的公钥进行签名的请求时，对车辆终端的身份进行验证，并使用运营商的私钥对车辆终端的公钥进行签名后返回至车辆终端，使得车辆终端能够将签名结果发送至认证管理中心，由认证管理中心来进行验证，进而使得车辆终端与认证管理中心之间进行通信时能够通过公私密钥的方式来保证通信的安全性，无需车辆终端与认证管理中心之间保持一一对应的长期密钥，降低了认证管理中心对密钥的管理负担，同时由于无需维护密钥库，因此也有效避免了密钥库遭到攻击而造成的安全隐患，极大提升了车辆通信过程中的隐私安全性。

根据本发明的第三方面，还提出了一种车辆通信中的隐私保护方法，该隐私保护方法适用于认证管理设备，具体包括以下步骤：

接收运营商发送的通过第一密钥加密后的多对（PMSI，K_{PMSI}），其中，所述第一密钥是由所述运营商分配给车辆终端的；

接收所述车辆终端发送的所述车辆终端的识别码、所述车辆终端的公钥和所述运营商对所述车辆终端的公钥的签名结果，其中，所述签名结果是由所述运营商对所述车辆终端的身份验证通过之后，使用所述运营商的私钥对所述车辆终端的公钥进行签名得到的；

基于所述运营商的公钥对所述签名结果进行验证，在对所述签名结果验证通过后，从所述多对（PMSI，K_{PMSI}）中选择至少一对（PMSI，K_{PMSI}），并通过所述车辆终端的公钥对经过所述第一密钥加密后的所述至少一对（PMSI，K_{PMSI}）进行再次加密；

将通过所述车辆终端的公钥和所述第一密钥加密后的所述至少一对（PMSI，K_{PMSI}）发送至所述车辆终端，以供所述车辆终端在解密后使用所述至少一对（PMSI，K_{PMSI}）进行车辆通信。

在该技术方案中，由于运营商在对车辆终端的身份验证通过之后，使用运营商的私钥对车辆终端的公钥进行签名，因此通过由认证管理设备根据运营商的公钥来对签名结果进行验证，使得车辆终端与认证管理设备之

间进行通信时能够通过公私密钥的方式来保证通信的安全性，无需车辆终端与认证管理设备之间保持一一对应的长期密钥，进而能够降低认证管理设备对密钥的管理负担，同时由于无需维护密钥库，因此也有效避免了密钥库遭到攻击而造成的安全隐患，极大提升了车辆通信过程中的隐私安全性。

其中，认证管理设备中维护有车辆终端的识别码和分配给车辆终端的（PMSI，K_{PMSI}）之间的关系，这样使得车辆终端在车联网中的恶意行为被发现后，运营商可以通过车辆终端的假名 ID 来询问认证管理设备，以获得相应车辆的真实身份信息。

根据本发明的第四方面，还提出了一种车辆通信中的隐私保护装置，该隐私保护装置适用于车辆终端，具体包括：

获取单元，用于获取运营商分配的第一密钥，其中，所述运营商在向车辆终端分配所述第一密钥之后，通过所述第一密钥对多对（PMSI，K_{PMSI}）加密后发送至认证管理中心；

第一交互单元，用于向所述运营商发送对所述车辆终端的公钥进行签名的请求，并接收所述运营商返回的签名结果，其中，所述运营商在对所述车辆终端的身份验证通过之后，使用所述运营商的私钥对所述车辆终端的公钥进行签名；

第二交互单元，用于将所述车辆终端的识别码、所述车辆终端的公钥和所述签名结果发送至所述认证管理中心，并接收所述认证管理中心发送的使用所述车辆终端的公钥和所述第一密钥加密的至少一对（PMSI，K_{PMSI}），其中，所述至少一对（PMSI，K_{PMSI}）是由所述认证管理中心基于所述运营商的公钥对所述签名结果验证通过后，从所述多对（PMSI，K_{PMSI}）选择出的；

处理单元，用于根据所述第一密钥和所述车辆终端的私钥对所述第二交互单元接收到的所述至少一对（PMSI，K_{PMSI}）进行解密，并基于解密后的（PMSI，K_{PMSI}）进行车辆通信。

在该技术方案中，通过由车辆终端向运营商发送对车辆终端的公钥进行签名的请求，而运营商在对车辆终端的身份验证通过之后，使用运营商

的私钥对车辆终端的公钥进行签名，进而由车辆终端将签名结果发送至认证管理中心，由认证管理中心根据运营商设备的公钥来对签名结果进行验证，使得车辆终端与认证管理中心之间进行通信时能够通过公私密钥的方式来保证通信的安全性，无需车辆终端与认证管理中心之间保持一一对应的长期密钥，进而能够降低认证管理中心对密钥的管理负担，同时由于无需维护密钥库，因此也有效避免了密钥库遭到攻击而造成的安全隐患，极大提升了车辆通信过程中的隐私安全性。

其中，车辆终端的识别码可以是 IMSI 或 IMEI；PMSI 即为假名 ID，K_{PMSI} 是与 PMSI 相对应的密钥，车辆终端在进行车辆通信时使用假名 ID 进行通信，并能够通过 K_{PMSI} 来进行身份识别。当车辆终端在车联网中的恶意行为被发现后，运营商可以通过车辆终端的假名 ID 来询问认证管理中心，以获得相应车辆的真实身份信息，既保证运营商能够识别到在车联网中有恶意行为的车辆，也能够避免运营商肆意获取车联网中的车辆信息而导致车辆隐私泄露的问题。

根据本发明的第五方面，还提出了一种车辆通信中的隐私保护装置，该隐私保护装置适用于运营商设备，具体包括：

分配单元，用于向车辆终端分配第一密钥；

第一发送单元，用于通过所述第一密钥对多对（PMSI，K_{PMSI}）加密后发送至认证管理中心；

处理单元，用于在接收到所述车辆终端发送的对所述车辆终端的公钥进行签名的请求时，对所述车辆终端的身份进行验证，当对所述车辆终端的身份验证通过之后，使用运营商设备的私钥对所述车辆终端的公钥进行签名，并将签名结果返回至所述车辆终端；

其中，所述签名结果用于供所述车辆终端发送至所述认证管理中心进行验证，以使所述认证管理中心在对所述签名结果验证通过后向所述车辆终端发送至少一对（PMSI，K_{PMSI}）进行车辆通信。

在该技术方案中，运营商设备通过在接收到车辆终端发送的对车辆终端的公钥进行签名的请求时，对车辆终端的身份进行验证，并使用运营商的私钥对车辆终端的公钥进行签名后返回至车辆终端，使得车辆终端能够

将签名结果发送至认证管理中心，由认证管理中心来进行验证，进而使得车辆终端与认证管理中心之间进行通信时能够通过公私密钥的方式来保证通信的安全性，无需车辆终端与认证管理中心之间保持一一对应的长期密钥，降低了认证管理中心对密钥的管理负担，同时由于无需维护密钥库，因此也有效避免了密钥库遭到攻击而造成的安全隐患，极大提升了车辆通信过程中的隐私安全性。

根据本发明的第六方面，还提出了一种车辆通信中的隐私保护装置，该隐私保护装置适用于认证管理设备，具体包括：

第一接收单元，用于接收运营商发送的通过第一密钥加密后的多对（PMSI，K_{PMSI}），其中，所述第一密钥是由所述运营商分配给车辆终端的；

第二接收单元，用于接收所述车辆终端发送的所述车辆终端的识别码、所述车辆终端的公钥和所述运营商对所述车辆终端的公钥的签名结果，其中，所述签名结果是由所述运营商对所述车辆终端的身份验证通过之后，使用所述运营商的私钥对所述车辆终端的公钥进行签名得到的；

处理单元，用于基于所述运营商的公钥对所述签名结果进行验证，在对所述签名结果验证通过后，从所述多对（PMSI，K_{PMSI}）中选择至少一对（PMSI，K_{PMSI}），并通过所述车辆终端的公钥对经过所述第一密钥加密后的所述至少一对（PMSI，K_{PMSI}）进行再次加密；

发送单元，用于将通过所述车辆终端的公钥和所述第一密钥加密后的所述至少一对（PMSI，K_{PMSI}）发送至所述车辆终端，以供所述车辆终端在解密后使用所述至少一对（PMSI，K_{PMSI}）进行车辆通信。

在该技术方案中，由于运营商在对车辆终端的身份验证通过之后，使用运营商的私钥对车辆终端的公钥进行签名，因此通过由认证管理设备根据运营商的公钥来对签名结果进行验证，使得车辆终端与认证管理设备之间进行通信时能够通过公私密钥的方式来保证通信的安全性，无需车辆终端与认证管理设备之间保持一一对应的长期密钥，进而能够降低认证管理设备对密钥的管理负担，同时由于无需维护密钥库，因此也有效避免了密钥库遭到攻击而造成的安全隐患，极大提升了车辆通信过程中的隐私安全

性。

其中，认证管理设备中维护有车辆终端的识别码和分配给车辆终端的（PMSI，K_{PMSI}）之间的关系，这样使得车辆终端在车联网中的恶意行为被发现后，运营商可以通过车辆终端的假名 ID 来询问认证管理设备，以获得相应车辆的真实身份信息。

通过以上技术方案，使得车辆终端与认证管理中心之间无需保持一一对应的长期密钥，降低了认证管理中心对密钥的管理负担，同时由于无需维护密钥库，因此也有效避免了密钥库遭到攻击而造成的安全隐患，极大提升了车辆通信过程中的隐私安全性。

附图说明

图 1 示出了相关技术中提出的车辆通信中的隐私保护方案的示意图；

图 2 示出了根据本发明的第一个实施例的车辆通信中的隐私保护方法的流程示意图；

图 3 示出了根据本发明的第一个实施例的车辆通信中的隐私保护装置的示意框图；

图 4 示出了根据本发明的第二个实施例的车辆通信中的隐私保护方法的流程示意图；

图 5 示出了根据本发明的第二个实施例的车辆通信中的隐私保护装置的示意框图；

图 6 示出了根据本发明的第三个实施例的车辆通信中的隐私保护方法的流程示意图；

图 7 示出了根据本发明的第三个实施例的车辆通信中的隐私保护装置的示意框图；

图 8 示出了根据本发明的实施例的车辆通信中的隐私保护方案的整体流程示意图；

图 9 示出了根据本发明的实施例的车辆终端的示意框图；

图 10 示出了根据本发明的实施例的运营商设备的示意框图；

图 11 示出了根据本发明的实施例的认证管理设备的示意框图。

具体实施方式

为了能够更清楚地理解本发明的上述目的、特征和优点，下面结合附图和具体实施方式对本发明进行进一步的详细描述。需要说明的是，在不冲突的情况下，本申请的实施例及实施例中的特征可以相互组合。

在下面的描述中阐述了很多具体细节以便于充分理解本发明，但是，本发明还可以采用其他不同于在此描述的其他方式来实施，因此，本发明的保护范围并不受下面公开的具体实施例的限制。

本发明的技术方案主要是采用公私密钥技术来解决车辆终端与认证管理中心之间通信信道的安全性问题，主要涉及到的实体有运营商设备、车辆终端和认证管理设备，以下分别从这三个实体的角度进行说明：

1、车辆终端：

如图 2 所示，根据本发明的第一个实施例的车辆通信中的隐私保护方法，包括以下步骤：

步骤 S20，获取运营商分配的第一密钥，其中，所述运营商在向车辆终端分配所述第一密钥之后，通过所述第一密钥对多对（PMSI，K_{PMSI}）加密后发送至认证管理中心。

进一步地，为了提高密钥的安全性，第一密钥可以为周期性密钥。

步骤 S22，向所述运营商发送对所述车辆终端的公钥进行签名的请求，并接收所述运营商返回的签名结果，其中，所述运营商在对所述车辆终端的身份验证通过之后，使用所述运营商的私钥对所述车辆终端的公钥进行签名。

步骤 S24，将所述车辆终端的识别码、所述车辆终端的公钥和所述签名结果发送至所述认证管理中心，并接收所述认证管理中心发送的使用所述车辆终端的公钥和所述第一密钥加密的至少一对（PMSI，K_{PMSI}），其中，所述至少一对（PMSI，K_{PMSI}）是由所述认证管理中心基于所述运营商的公钥对所述签名结果验证通过后，从所述多对（PMSI，K_{PMSI}）选择出的。

步骤 S26，根据所述第一密钥和所述车辆终端的私钥对接收到的所述至少一对（PMSI，K_{PMSI}）进行解密，并基于解密后的（PMSI，K_{PMSI}）进

行车辆通信。

图 2 所示的技术方案的执行主体是车辆终端。在图 2 所示的技术方案中，通过由车辆终端向运营商发送对车辆终端的公钥进行签名的请求，而运营商在对车辆终端的身份验证通过之后，使用运营商的私钥对车辆终端的公钥进行签名，进而由车辆终端将签名结果发送至认证管理中心，由认证管理中心根据运营商设备的公钥来对签名结果进行验证，使得车辆终端与认证管理中心之间进行通信时能够通过公私密钥的方式来保证通信的安全性，无需车辆终端与认证管理中心之间保持一一对应的长期密钥，进而能够降低认证管理中心对密钥的管理负担，同时由于无需维护密钥库，因此也有效避免了密钥库遭到攻击而造成的安全隐患，极大提升了车辆通信过程中的隐私安全性。

其中，车辆终端的识别码可以是 IMSI 或 IMEI；PMSI 即为假名 ID，K_{PMSI} 是与 PMSI 相对应的密钥，车辆终端在进行车辆通信时使用假名 ID 进行通信，并能够通过 K_{PMSI} 来进行身份识别。当车辆终端在车联网中的恶意行为被发现后，运营商可以通过车辆终端的假名 ID 来询问认证管理中心，以获得相应车辆的真实身份信息，既保证运营商能够识别到在车联网中有恶意行为的车辆，也能够避免运营商肆意获取车联网中的车辆信息而导致车辆隐私泄露的问题。

图 3 示出了根据本发明的第一个实施例的车辆通信中的隐私保护装置的示意框图，该隐私保护装置适用于车辆终端。

如图 3 所示，根据本发明的第一个实施例的车辆通信中的隐私保护装置 300，包括：获取单元 302、第一交互单元 304、第二交互单元 306 和处理单元 308。

其中，获取单元 302 用于获取运营商分配的第一密钥，其中，所述运营商在向车辆终端分配所述第一密钥之后，通过所述第一密钥对多对（PMSI，K_{PMSI}）加密后发送至认证管理中心；

第一交互单元 304 用于向所述运营商发送对所述车辆终端的公钥进行签名的请求，并接收所述运营商返回的签名结果，其中，所述运营商在对所述车辆终端的身份验证通过之后，使用所述运营商的私钥对所述车辆终

端的公钥进行签名；

第二交互单元 306 用于将所述车辆终端的识别码、所述车辆终端的公钥和所述签名结果发送至所述认证管理中心，并接收所述认证管理中心发送的使用所述车辆终端的公钥和所述第一密钥加密的至少一对（PMSI，K_{PMSI}），其中，所述至少一对（PMSI，K_{PMSI}）是由所述认证管理中心基于所述运营商的公钥对所述签名结果验证通过后，从所述多对（PMSI，K_{PMSI}）选择出的；

处理单元 308 用于根据所述第一密钥和所述车辆终端的私钥对所述第二交互单元 306 接收到的所述至少一对（PMSI，K_{PMSI}）进行解密，并基于解密后的（PMSI，K_{PMSI}）进行车辆通信。

在该技术方案中，通过由车辆终端向运营商发送对车辆终端的公钥进行签名的请求，而运营商在对车辆终端的身份验证通过之后，使用运营商的私钥对车辆终端的公钥进行签名，进而由车辆终端将签名结果发送至认证管理中心，由认证管理中心根据运营商设备的公钥来对签名结果进行验证，使得车辆终端与认证管理中心之间进行通信时能够通过公私密钥的方式来保证通信的安全性，无需车辆终端与认证管理中心之间保持一一对应的长期密钥，进而能够降低认证管理中心对密钥的管理负担，同时由于无需维护密钥库，因此也有效避免了密钥库遭到攻击而造成的安全隐患，极大提升了车辆通信过程中的隐私安全性。

其中，车辆终端的识别码可以是 IMSI 或 IMEI；PMSI 即为假名 ID，K_{PMSI} 是与 PMSI 相对应的密钥，车辆终端在进行车辆通信时使用假名 ID 进行通信，并能够通过 K_{PMSI} 来进行身份识别。当车辆终端在车联网中的恶意行为被发现后，运营商可以通过车辆终端的假名 ID 来询问认证管理中心，以获得相应车辆的真实身份信息，既保证运营商能够识别到在车联网中有恶意行为的车辆，也能够避免运营商肆意获取车联网中的车辆信息而导致车辆隐私泄露的问题。

进一步地，为了提高密钥的安全性，第一密钥可以为周期性密钥。

2、运营商设备：

如图 4 所示，根据本发明的第二个实施例的车辆通信中的隐私保护方

法，包括以下步骤：

步骤 S40，向车辆终端分配第一密钥，并通过所述第一密钥对多对（PMSI，K_{PMSI}）加密后发送至认证管理中心；

步骤 S42，在接收到所述车辆终端发送的对所述车辆终端的公钥进行签名的请求时，对所述车辆终端的身份进行验证；

步骤 S44，在对车辆终端的身份验证通过之后，使用运营商设备的私钥对所述车辆终端的公钥进行签名，并将签名结果返回至所述车辆终端；

其中，所述签名结果用于供所述车辆终端发送至所述认证管理中心进行验证，以使所述认证管理中心在对所述签名结果验证通过后向所述车辆终端发送至少一对（PMSI，K_{PMSI}）进行车辆通信。

进一步地，图 4 所示的车辆通信中的隐私保护方法还包括：将运营商设备的公钥发送至所述认证管理中心，以供所述认证管理中心根据所述运营商设备的公钥对所述签名结果进行验证。

具体地，由于是使用运营商设备的私钥对车辆终端的公钥进行签名，因此通过将运营商设备的公钥发送至认证管理中心，使得认证管理中心能够根据运营商设备的公钥来对签名结果进行验证，避免了车辆终端与认证管理中心之间需要维持一一对应的长期密钥而存在的安全隐患和密钥管理负担。

图 4 所示的技术方案的执行主体是运营商设备。在图 4 所示的技术方案中，运营商设备通过在接收到车辆终端发送的对车辆终端的公钥进行签名的请求时，对车辆终端的身份进行验证，并使用运营商的私钥对车辆终端的公钥进行签名后返回至车辆终端，使得车辆终端能够将签名结果发送至认证管理中心，由认证管理中心来进行验证，进而使得车辆终端与认证管理中心之间进行通信时能够通过公私密钥的方式来保证通信的安全性，无需车辆终端与认证管理中心之间保持一一对应的长期密钥，降低了认证管理中心对密钥的管理负担，同时由于无需维护密钥库，因此也有效避免了密钥库遭到攻击而造成的安全隐患，极大提升了车辆通信过程中的隐私安全性。

图 5 示出了根据本发明的第二个实施例的车辆通信中的隐私保护装置

的示意框图，该隐私保护装置适用于运营商设备。

如图 5 所示，根据本发明的第二个实施例的车辆通信中的隐私保护装置 500，包括：分配单元 502、第一发送单元 504 和处理单元 506。

其中，分配单元 502 用于向车辆终端分配第一密钥；

第一发送单元 504 用于通过所述第一密钥对多对（PMSI，K_{PMSI}）加密后发送至认证管理中心；

处理单元 506 用于在接收到所述车辆终端发送的对所述车辆终端的公钥进行签名的请求时，对所述车辆终端的身份进行验证，当对所述车辆终端的身份验证通过之后，使用运营商设备的私钥对所述车辆终端的公钥进行签名，并将签名结果返回至所述车辆终端；

其中，所述签名结果用于供所述车辆终端发送至所述认证管理中心进行验证，以使所述认证管理中心在对所述签名结果验证通过后向所述车辆终端发送至少一对（PMSI，K_{PMSI}）进行车辆通信。

在该技术方案中，运营商设备通过在接收到车辆终端发送的对车辆终端的公钥进行签名的请求时，对车辆终端的身份进行验证，并使用运营商的私钥对车辆终端的公钥进行签名后返回至车辆终端，使得车辆终端能够将签名结果发送至认证管理中心，由认证管理中心来进行验证，进而使得车辆终端与认证管理中心之间进行通信时能够通过公私密钥的方式来保证通信的安全性，无需车辆终端与认证管理中心之间保持一一对应的长期密钥，降低了认证管理中心对密钥的管理负担，同时由于无需维护密钥库，因此也有效避免了密钥库遭到攻击而造成的安全隐患，极大提升了车辆通信过程中的隐私安全性。

进一步地，第一发送单元 504 还用于：将运营商设备的公钥发送至所述认证管理中心，以供所述认证管理中心根据所述运营商设备的公钥对所述签名结果进行验证。

具体地，由于是使用运营商设备的私钥对车辆终端的公钥进行签名，因此通过将运营商设备的公钥发送至认证管理中心，使得认证管理中心能够根据运营商设备的公钥来对签名结果进行验证，避免了车辆终端与认证管理中心之间需要维持一一对应的长期密钥而存在的安全隐患和密钥管理

负担。

3、认证管理设备：

如图 6 所示，根据本发明的第三个实施例的车辆通信中的隐私保护方法，包括以下步骤：

步骤 S60，接收运营商发送的通过第一密钥加密后的多对（PMSI，K_{PMSI}），其中，所述第一密钥是由所述运营商分配给车辆终端的；

步骤 S62，接收所述车辆终端发送的所述车辆终端的识别码、所述车辆终端的公钥和所述运营商对所述车辆终端的公钥的签名结果，其中，所述签名结果是由所述运营商对所述车辆终端的身份验证通过之后，使用所述运营商的私钥对所述车辆终端的公钥进行签名得到的；

步骤 S64，基于所述运营商的公钥对所述签名结果进行验证，在对所述签名结果验证通过后，从所述多对（PMSI，K_{PMSI}）中选择至少一对（PMSI，K_{PMSI}），并通过所述车辆终端的公钥对经过所述第一密钥加密后的所述至少一对（PMSI，K_{PMSI}）进行再次加密；

步骤 S66，将通过所述车辆终端的公钥和所述第一密钥加密后的所述至少一对（PMSI，K_{PMSI}）发送至所述车辆终端，以供所述车辆终端在解密后使用所述至少一对（PMSI，K_{PMSI}）进行车辆通信。

图 6 所示的技术方案的执行主体是认证管理设备。在图 6 所示的技术方案中，由于运营商在对车辆终端的身份验证通过之后，使用运营商的私钥对车辆终端的公钥进行签名，因此通过由认证管理设备根据运营商的公钥来对签名结果进行验证，使得车辆终端与认证管理设备之间进行通信时能够通过公私密钥的方式来保证通信的安全性，无需车辆终端与认证管理设备之间保持一一对应的长期密钥，进而能够降低认证管理设备对密钥的管理负担，同时由于无需维护密钥库，因此也有效避免了密钥库遭到攻击而造成的安全隐患，极大提升了车辆通信过程中的隐私安全性。

其中，认证管理设备中维护有车辆终端的识别码和分配给车辆终端的（PMSI，K_{PMSI}）之间的关系，这样使得车辆终端在车联网中的恶意行为被发现后，运营商可以通过车辆终端的假名 ID 来询问认证管理设备，以获得相应车辆的真实身份信息。

图 7 示出了根据本发明的第三个实施例的车辆通信中的隐私保护装置的示意框图，该隐私保护装置适用于认证管理设备。

如图 7 所示，根据本发明的第三个实施例的车辆通信中的隐私保护装置 700，包括：第一接收单元 702、第二接收单元 704、处理单元 706 和发送单元 708。

其中，第一接收单元 702 用于接收运营商发送的通过第一密钥加密后的多对（PMSI，K_{PMSI}），其中，所述第一密钥是由所述运营商分配给车辆终端的；

第二接收单元 704 用于接收所述车辆终端发送的所述车辆终端的识别码、所述车辆终端的公钥和所述运营商对所述车辆终端的公钥的签名结果，其中，所述签名结果是由所述运营商对所述车辆终端的身份验证通过之后，使用所述运营商的私钥对所述车辆终端的公钥进行签名得到的；

处理单元 706 用于基于所述运营商的公钥对所述签名结果进行验证，在对所述签名结果验证通过后，从所述多对（PMSI，K_{PMSI}）中选择至少一对（PMSI，K_{PMSI}），并通过所述车辆终端的公钥对经过所述第一密钥加密后的所述至少一对（PMSI，K_{PMSI}）进行再次加密；

发送单元 708 用于将通过所述车辆终端的公钥和所述第一密钥加密后的所述至少一对（PMSI，K_{PMSI}）发送至所述车辆终端，以供所述车辆终端在解密后使用所述至少一对（PMSI，K_{PMSI}）进行车辆通信。

在该技术方案中，由于运营商在对车辆终端的身份验证通过之后，使用运营商的私钥对车辆终端的公钥进行签名，因此通过由认证管理设备根据运营商的公钥来对签名结果进行验证，使得车辆终端与认证管理设备之间进行通信时能够通过公私密钥的方式来保证通信的安全性，无需车辆终端与认证管理设备之间保持一一对应的长期密钥，进而能够降低认证管理设备对密钥的管理负担，同时由于无需维护密钥库，因此也有效避免了密钥库遭到攻击而造成的安全隐患，极大提升了车辆通信过程中的隐私安全性。

其中，认证管理设备中维护有车辆终端的识别码和分配给车辆终端的（PMSI，K_{PMSI}）之间的关系，这样使得车辆终端在车联网中的恶意行为

被发现后，运营商可以通过车辆终端的假名 ID 来询问认证管理设备，以获得相应车辆的真实身份信息。

以下分别从运营商设备、车辆终端和认证管理设备三个方面对本发明的技术方案进行了说明，以下结合图 8 对三者之间的具体交互过程进行说明，其中，运营商设备即为 MNO、车辆终端即为 V-UE、认证管理设备可以为 PCA:

在介绍具体的技术方案之前，先介绍本发明提到的以下几个要点:

（1）MNO 持有用于数字签名的公私密钥对（PK_{MNO}，SK_{MNO}），其中，PK_{MNO} 为公钥，SK_{MNO} 为私钥;

（2）V-UE 持有用于加解密的公私密钥对（PK_V，SK_V），其中，PK_V 为公钥，SK_V 私钥;

（3）PCA 通过验证来自 MNO 的数字签名来验证 V-UE 的身份，同时 PCA 选定数个（PMSI，K_{PMSI}），并通过 PK_V 加密后发送给 V-UE。

具体如图 8 所示，包括:

步骤 802，V-UE 从 MNO 处获得密钥 K_{PERIOD}。具体地，V-UE 向 MNO 发送获取 K_{PERIOD} 的请求，之后 MNO 向 V-UE 分配 K_{PERIOD}。其中，K_{PERIOD} 是由 MNO 生成的一个周期性密钥（比如每周换一个），K_{PERIOD} 用来对（PMSI，K_{PMSI}）进行加密。

步骤 804，MNO 向 PCA 发送以 K_{PERIOD} 加密的多对（PMSI，K_{PMSI}），其中，（PMSI，K_{PMSI}）的数量取决于系统的规模，比如可以是 1000000 对。

步骤 806，V-UE 向 MNO 请求对 PK_V 进行签名。

步骤 808，MNO 在验证 V-UE 的身份后使用私钥 SK_{MNO} 对 PK_V 进行签名，并将签名结果返回至 V-UE。其中，MNO 验证 V-UE 的身份类似于 UE 的注册过程。

步骤 810，V-UE 将自身的 IMSI（或 IMEI）、PK_V、MNO 对 PK_V 的签名结果发送至 PCA。

步骤 812，PCA 基于 MNO 的公钥 PK_{MNO} 验证 PK_V 的签名。其中，在步骤 812 之前，MNO 需要将公钥 PK_{MNO} 通知给 PCA，以便于 PCA 在该

步骤中对 PK_V 的签名进行验证。

步骤 814，PCA 在对 PK_V 的签名验证通过之后，选取至少一对通过 K_{PERIOD} 加密的（PMSI，K_{PMSI}），并用 PK_V 加密后发送给 V-UE。

步骤 816，V-UE 对接收到的（PMSI，K_{PMSI}）进行两重解密后得到（PMSI，K_{PMSI}）的值。具体地，V-UE 先用自己的私钥 SK_V 解密，然后再用 K_{PERIOD} 解密。

在 V-UE 解密后获得（PMSI，K_{PMSI}）的值之后，可以基于 PMSI 来进行车辆通信，而 K_{PMSI} 用于进行身份识别时使用。其中，若 PCA 发送了多对通过 K_{PERIOD} 加密的（PMSI，K_{PMSI}），则 V-UE 在解密后的通信过程中，可以每过一段时间更换一次使用的 PMSI。当 V-UE 在车联网中的恶意行为被发现后，MNO 可以通过 V-UE 的 PMSI 来询问 PCA，由于 PCA 维护有 V-UE 的真实身份（IMSI/IMEI）和（PMSI，K_{PMSI}）之间的关系，因此 PCA 可以获得 V-UE 的真实身份信息，进而可以将获得的真实身份返回给 MNO，可见，本发明的技术方案既保证运营商能够识别到在车联网中有恶意行为的车辆，也能够避免运营商肆意获取车联网中的车辆信息而导致车辆隐私泄露的问题。

图 9 示出了根据本发明的实施例的车辆终端的示意框图。

如图 9 所示，根据本发明的实施例的车辆终端，包括：处理器 1、输入装置 2、输出装置 3 和存储器 5。在本发明的一些实施例中，处理器 1、输入装置 2、输出装置 3 和存储器 5 可以通过总线 4 或其他方式连接，图 9 中以通过总线 4 连接为例。

其中，存储器 5 用于存储一组程序代码，处理器 1 调用存储器 5 中存储的程序代码，用于执行以下操作：

通过输入装置 2 获取运营商分配的第一密钥，其中，所述运营商在向车辆终端分配所述第一密钥之后，通过所述第一密钥对多对（PMSI，K_{PMSI}）加密后发送至认证管理中心；

通过输出装置 3 向所述运营商发送对所述车辆终端的公钥进行签名的请求，并通过输入装置 2 接收所述运营商返回的签名结果，其中，所述运营商在对所述车辆终端的身份验证通过之后，使用所述运营商的私钥对所

述车辆终端的公钥进行签名；

通过输出装置 3 将所述车辆终端的识别码、所述车辆终端的公钥和所述签名结果发送至所述认证管理中心，并通过输入装置 2 接收所述认证管理中心发送的使用所述车辆终端的公钥和所述第一密钥加密的至少一对（PMSI，K_{PMSI}），其中，所述至少一对（PMSI，K_{PMSI}）是由所述认证管理中心基于所述运营商的公钥对所述签名结果验证通过后，从所述多对（PMSI，K_{PMSI}）选择出的；

根据所述第一密钥和所述车辆终端的私钥对接收到的所述至少一对（PMSI，K_{PMSI}）进行解密，并基于解密后的（PMSI，K_{PMSI}）进行车辆通信。

图 10 示出了根据本发明的实施例的运营商设备的示意框图。

如图 10 所示，根据本发明的实施例的运营商设备，包括：处理器 1'、输入装置 2'、输出装置 3'和存储器 5'。在本发明的一些实施例中，处理器 1'、输入装置 2'、输出装置 3'和存储器 5'可以通过总线 4'或其他方式连接，图 10 中以通过总线 4'连接为例。

其中，存储器 5'用于存储一组程序代码，处理器 1'调用存储器 5'中存储的程序代码，用于执行以下操作：

向车辆终端分配第一密钥，并由输出装置 3'通过所述第一密钥对多对（PMSI，K_{PMSI}）加密后发送至认证管理中心；

在输入装置 2'接收到所述车辆终端发送的对所述车辆终端的公钥进行签名的请求时，对所述车辆终端的身份进行验证；

在对所述车辆终端的身份验证通过之后，使用运营商设备的私钥对所述车辆终端的公钥进行签名，并通过输出装置 3'将签名结果返回至所述车辆终端；

其中，所述签名结果用于供所述车辆终端发送至所述认证管理中心进行验证，以使所述认证管理中心在对所述签名结果验证通过后向所述车辆终端发送至少一对（PMSI，K_{PMSI}）进行车辆通信。

作为一种可选的实施方式，处理器 1'调用存储器 5'中存储的程序代码，还用于执行以下操作：

通过输出装置 3'将运营商设备的公钥发送至所述认证管理中心，以供所述认证管理中心根据所述运营商设备的公钥对所述签名结果进行验证。

图 11 示出了根据本发明的实施例的认证管理设备的示意框图。

如图 11 所示，根据本发明的实施例的认证管理设备，包括：处理器 1"、输入装置 2"、输出装置 3"和存储器 5"。在本发明的一些实施例中，处理器 1"、输入装置 2"、输出装置 3"和存储器 5"可以通过总线 4"或其他方式连接，图 11 中以通过总线 4"连接为例。

其中，存储器 5"用于存储一组程序代码，处理器 1"调用存储器 5"中存储的程序代码，用于执行以下操作：

通过输入装置 2"接收运营商发送的通过第一密钥加密后的多对（PMSI，K_{PMSI}），其中，所述第一密钥是由运营商分配给车辆终端的；

通过输入装置 2"接收所述车辆终端发送的所述车辆终端的识别码、所述车辆终端的公钥和所述运营商对所述车辆终端的公钥的签名结果，其中，所述签名结果是由所述运营商对所述车辆终端的身份验证通过之后，使用所述运营商的私钥对所述车辆终端的公钥进行签名得到的；

基于所述运营商的公钥对所述签名结果进行验证，在对所述签名结果验证通过后，从所述多对（PMSI，K_{PMSI}）中选择至少一对（PMSI，K_{PMSI}），并通过所述车辆终端的公钥对经过所述第一密钥加密后的所述至少一对（PMSI，K_{PMSI}）进行再次加密；

通过输出装置 3"将通过所述车辆终端的公钥和所述第一密钥加密后的所述至少一对（PMSI，K_{PMSI}）发送至所述车辆终端，以供所述车辆终端在解密后使用所述至少一对（PMSI，K_{PMSI}）进行车辆通信。

本发明实施例的方法中的步骤可以根据实际需要进行顺序调整、合并和删减。

本发明实施例的车辆通信中的隐私保护装置、车辆终端、运营商设备和认证管理设备中的单元可以根据实际需要进行合并、划分和删减。

本领域普通技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成，该程序可以存储于一计算机可读存储介质中，存储介质包括只读存储器（Read-Only Memory，

ROM）、随机存储器（Random Access Memory，RAM）、可编程只读存储器（Programmable Read-only Memory，PROM）、可擦除可编程只读存储器（Erasable Programmable Read Only Memory，EPROM）、一次可编程只读存储器（One-time Programmable Read-Only Memory，OTPROM）、电子抹除式可复写只读存储器（Electrically-Erasable Programmable Read-Only Memory，EEPROM）、只读光盘（Compact Disc Read-Only Memory，CD-ROM）或其他光盘存储器、磁盘存储器、磁带存储器、或者能够用于携带或存储数据的计算机可读的任何其他介质。

以上结合附图详细说明了本发明的技术方案，本发明提出了一种新的车辆通信中的隐私保护方案，使得车辆终端与认证管理中心之间无需保持一一对应的长期密钥，降低了认证管理中心对密钥的管理负担，同时由于无需维护密钥库，因此也有效避免了密钥库遭到攻击而造成的安全隐患，极大提升了车辆通信过程中的隐私安全性。

以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

权 利 要 求 书

1. 一种车辆通信中的隐私保护方法，适用于车辆终端，其特征在于，包括:

获取运营商分配的第一密钥，其中，所述运营商在向车辆终端分配所述第一密钥之后，通过所述第一密钥对多对（PMSI，K_{PMSI}）加密后发送至认证管理中心;

向所述运营商发送对所述车辆终端的公钥进行签名的请求，并接收所述运营商返回的签名结果，其中，所述运营商在对所述车辆终端的身份验证通过之后，使用所述运营商的私钥对所述车辆终端的公钥进行签名;

将所述车辆终端的识别码、所述车辆终端的公钥和所述签名结果发送至所述认证管理中心，并接收所述认证管理中心发送的使用所述车辆终端的公钥和所述第一密钥加密的至少一对（PMSI，K_{PMSI}），其中，所述至少一对（PMSI，K_{PMSI}）是由所述认证管理中心基于所述运营商的公钥对所述签名结果验证通过后，从所述多对（PMSI，K_{PMSI}）选择出的;

根据所述第一密钥和所述车辆终端的私钥对接收到的所述至少一对（PMSI，K_{PMSI}）进行解密，并基于解密后的（PMSI，K_{PMSI}）进行车辆通信。

2. 根据权利要求 1 所述的车辆通信中的隐私保护方法，其特征在于，所述第一密钥为周期性密钥。

3. 一种车辆通信中的隐私保护方法，适用于运营商设备，其特征在于，包括:

向车辆终端分配第一密钥，并通过所述第一密钥对多对（PMSI，K_{PMSI}）加密后发送至认证管理中心;

在接收到所述车辆终端发送的对所述车辆终端的公钥进行签名的请求时，对所述车辆终端的身份进行验证;

在对所述车辆终端的身份验证通过之后，使用运营商设备的私钥对所述车辆终端的公钥进行签名，并将签名结果返回至所述车辆终端;

其中，所述签名结果用于供所述车辆终端发送至所述认证管理中心进

行验证，以使所述认证管理中心在对所述签名结果验证通过后向所述车辆终端发送至少一对（PMSI，K_{PMSI}）进行车辆通信。

4．根据权利要求 3 所述的车辆通信中的隐私保护方法，其特征在于，还包括:

将运营商设备的公钥发送至所述认证管理中心，以供所述认证管理中心根据所述运营商设备的公钥对所述签名结果进行验证。

5．一种车辆通信中的隐私保护方法，适用于认证管理设备，其特征在于，包括:

接收运营商发送的通过第一密钥加密后的多对（PMSI，K_{PMSI}），其中，所述第一密钥是由所述运营商分配给车辆终端的;

接收所述车辆终端发送的所述车辆终端的识别码、所述车辆终端的公钥和所述运营商对所述车辆终端的公钥的签名结果，其中，所述签名结果是由所述运营商对所述车辆终端的身份验证通过之后，使用所述运营商的私钥对所述车辆终端的公钥进行签名得到的;

基于所述运营商的公钥对所述签名结果进行验证，在对所述签名结果验证通过后，从所述多对（PMSI，K_{PMSI}）中选择至少一对（PMSI，K_{PMSI}），并通过所述车辆终端的公钥对经过所述第一密钥加密后的所述至少一对（PMSI，K_{PMSI}）进行再次加密;

将通过所述车辆终端的公钥和所述第一密钥加密后的所述至少一对（PMSI，K_{PMSI}）发送至所述车辆终端，以供所述车辆终端在解密后使用所述至少一对（PMSI，K_{PMSI}）进行车辆通信。

6．一种车辆通信中的隐私保护装置，适用于车辆终端，其特征在于，包括:

获取单元，用于获取运营商分配的第一密钥，其中，所述运营商在向车辆终端分配所述第一密钥之后，通过所述第一密钥对多对（PMSI，K_{PMSI}）加密后发送至认证管理中心;

第一交互单元，用于向所述运营商发送对所述车辆终端的公钥进行签名的请求，并接收所述运营商返回的签名结果，其中，所述运营商在对所述车辆终端的身份验证通过之后，使用所述运营商的私钥对所述车辆终端

的公钥进行签名;

第二交互单元，用于将所述车辆终端的识别码、所述车辆终端的公钥和所述签名结果发送至所述认证管理中心，并接收所述认证管理中心发送的使用所述车辆终端的公钥和所述第一密钥加密的至少一对（PMSI，K_{PMSI}），其中，所述至少一对（PMSI，K_{PMSI}）是由所述认证管理中心基于所述运营商的公钥对所述签名结果验证通过后，从所述多对（PMSI，K_{PMSI}）选择出的;

处理单元，用于根据所述第一密钥和所述车辆终端的私钥对所述第二交互单元接收到的所述至少一对（PMSI，K_{PMSI}）进行解密，并基于解密后的（PMSI，K_{PMSI}）进行车辆通信。

7. 根据权利要求 6 所述的车辆通信中的隐私保护装置，其特征在于，所述第一密钥为周期性密钥。

8. 一种车辆通信中的隐私保护装置，适用于运营商设备，其特征在于，包括:

分配单元，用于向车辆终端分配第一密钥;

第一发送单元，用于通过所述第一密钥对多对（PMSI，K_{PMSI}）加密后发送至认证管理中心;

处理单元，用于在接收到所述车辆终端发送的对所述车辆终端的公钥进行签名的请求时，对所述车辆终端的身份进行验证，当对所述车辆终端的身份验证通过之后，使用运营商设备的私钥对所述车辆终端的公钥进行签名，并将签名结果返回至所述车辆终端;

其中，所述签名结果用于供所述车辆终端发送至所述认证管理中心进行验证，以使所述认证管理中心在对所述签名结果验证通过后向所述车辆终端发送至少一对（PMSI，K_{PMSI}）进行车辆通信。

9. 根据权利要求 8 所述的车辆通信中的隐私保护装置，其特征在于，所述第一发送单元还用于:

将运营商设备的公钥发送至所述认证管理中心，以供所述认证管理中心根据所述运营商设备的公钥对所述签名结果进行验证。

10. 一种车辆通信中的隐私保护装置，适用于认证管理设备，其特征

在于，包括：

第一接收单元，用于接收运营商发送的通过第一密钥加密后的多对（PMSI，K_{PMSI}），其中，所述第一密钥是由所述运营商分配给车辆终端的；

第二接收单元，用于接收所述车辆终端发送的所述车辆终端的识别码、所述车辆终端的公钥和所述运营商对所述车辆终端的公钥的签名结果，其中，所述签名结果是由所述运营商对所述车辆终端的身份验证通过之后，使用所述运营商的私钥对所述车辆终端的公钥进行签名得到的；

处理单元，用于基于所述运营商的公钥对所述签名结果进行验证，在对所述签名结果验证通过后，从所述多对（PMSI，K_{PMSI}）中选择至少一对（PMSI，K_{PMSI}），并通过所述车辆终端的公钥对经过所述第一密钥加密后的所述至少一对（PMSI，K_{PMSI}）进行再次加密；

发送单元，用于将通过所述车辆终端的公钥和所述第一密钥加密后的所述至少一对（PMSI，K_{PMSI}）发送至所述车辆终端，以供所述车辆终端在解密后使用所述至少一对（PMSI，K_{PMSI}）进行车辆通信。

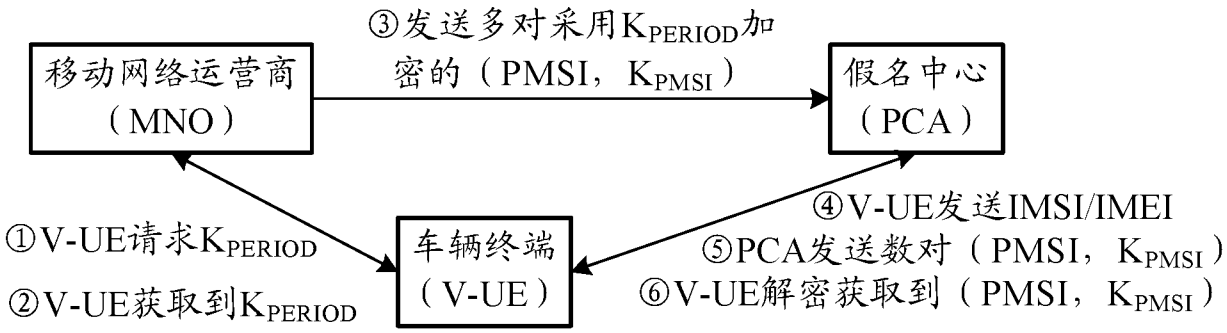
移动网络运营商
（MNO）
③发送多对采用K_{PERIOD}加密的（PMSI，K_{PMSI}）
假名中心
（PCA）
①V-UE请求K_{PERIOD}
②V-UE获取到K_{PERIOD}
车辆终端
（V-UE）
④V-UE发送IMSI/IMEI
⑤PCA发送数对（PMSI，K_{PMSI}）
⑥V-UE解密获取到（PMSI，K_{PMSI}）

图 1

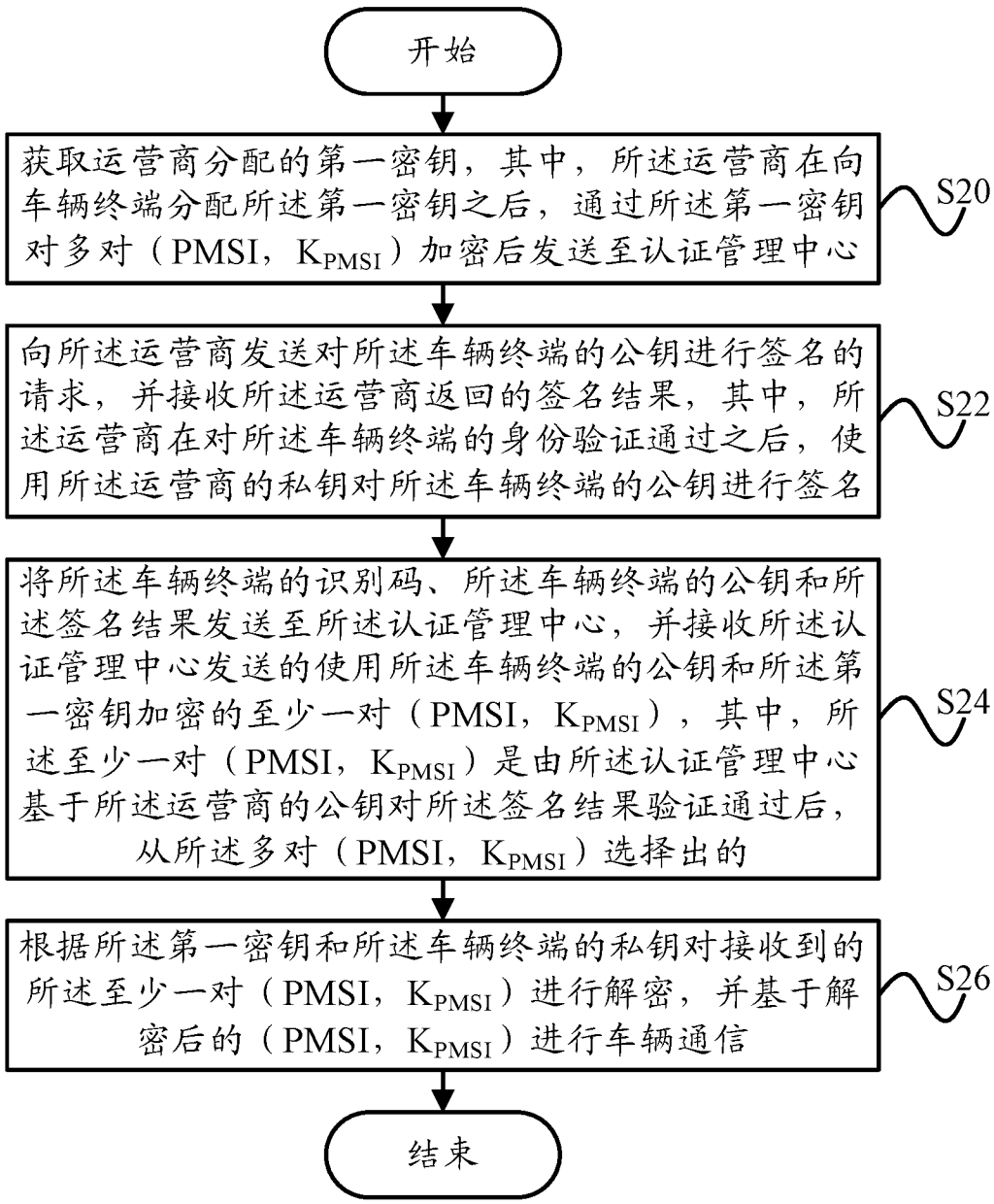
开始
获取运营商分配的第一密钥，其中，所述运营商在向车辆终端分配所述第一密钥之后，通过所述第一密钥对多对（PMSI，K_{PMSI}）加密后发送至认证管理中心
S20
向所述运营商发送对所述车辆终端的公钥进行签名的请求，并接收所述运营商返回的签名结果，其中，所述运营商在对所述车辆终端的身份验证通过之后，使用所述运营商的私钥对所述车辆终端的公钥进行签名
S22
将所述车辆终端的识别码、所述车辆终端的公钥和所述签名结果发送至所述认证管理中心，并接收所述认证管理中心发送的使用所述车辆终端的公钥和所述第一密钥加密的至少一对（PMSI，K_{PMSI}），其中，所述至少一对（PMSI，K_{PMSI}）是由所述认证管理中心基于所述运营商的公钥对所述签名结果验证通过后，从所述多对（PMSI，K_{PMSI}）选择出的
S24
根据所述第一密钥和所述车辆终端的私钥对接收到的所述至少一对（PMSI，K_{PMSI}）进行解密，并基于解密后的（PMSI，K_{PMSI}）进行车辆通信
S26
结束

图 2

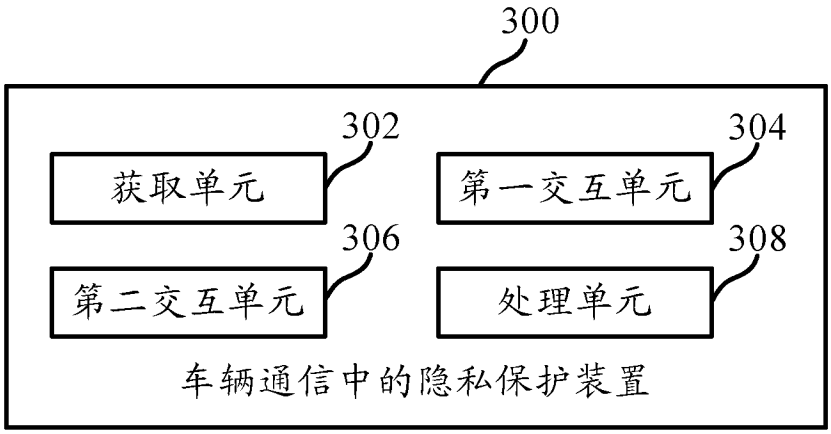
300
302
获取单元
304
第一交互单元
306
第二交互单元
308
处理单元
车辆通信中的隐私保护装置

图 3

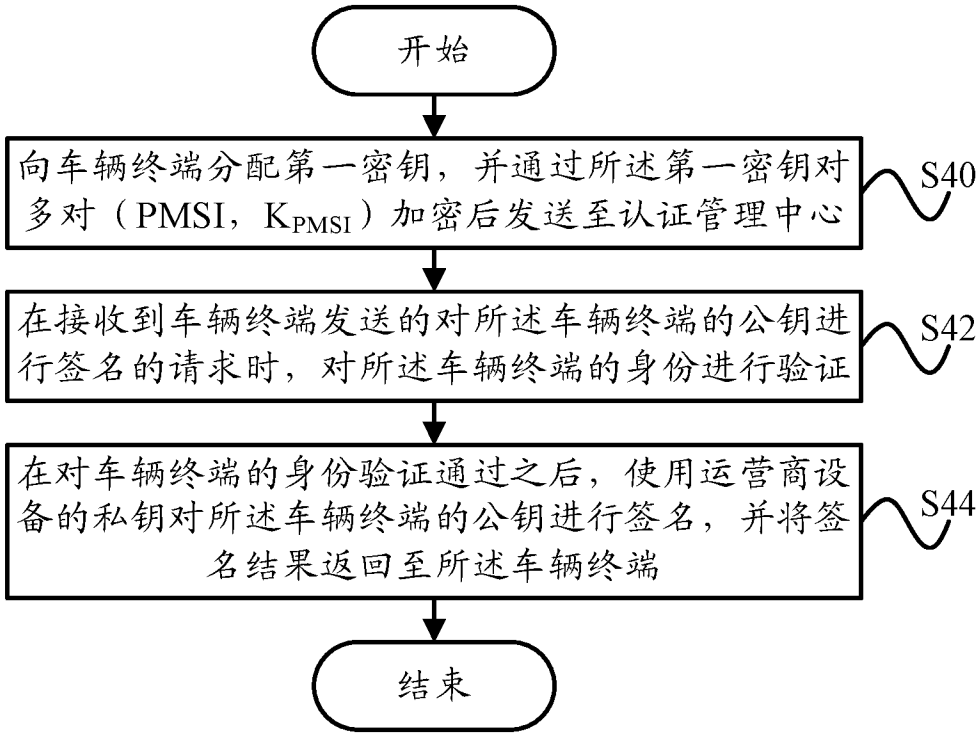
开始
向车辆终端分配第一密钥，并通过所述第一密钥对多对（PMSI，K_{PMSI}）加密后发送至认证管理中心
S40
在接收到车辆终端发送的对所述车辆终端的公钥进行签名的请求时，对所述车辆终端的身份进行验证
S42
在对车辆终端的身份验证通过之后，使用运营商设备的私钥对所述车辆终端的公钥进行签名，并将签名结果返回至所述车辆终端
S44
结束

图 4

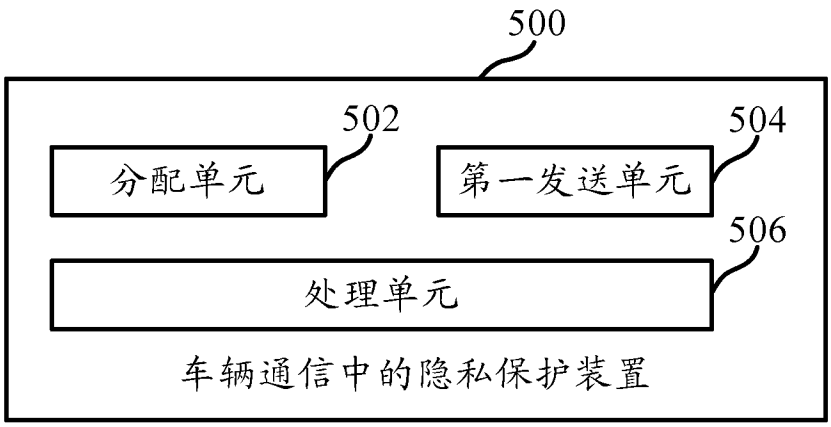
500
502
分配单元
504
第一发送单元
506
处理单元
车辆通信中的隐私保护装置

图 5

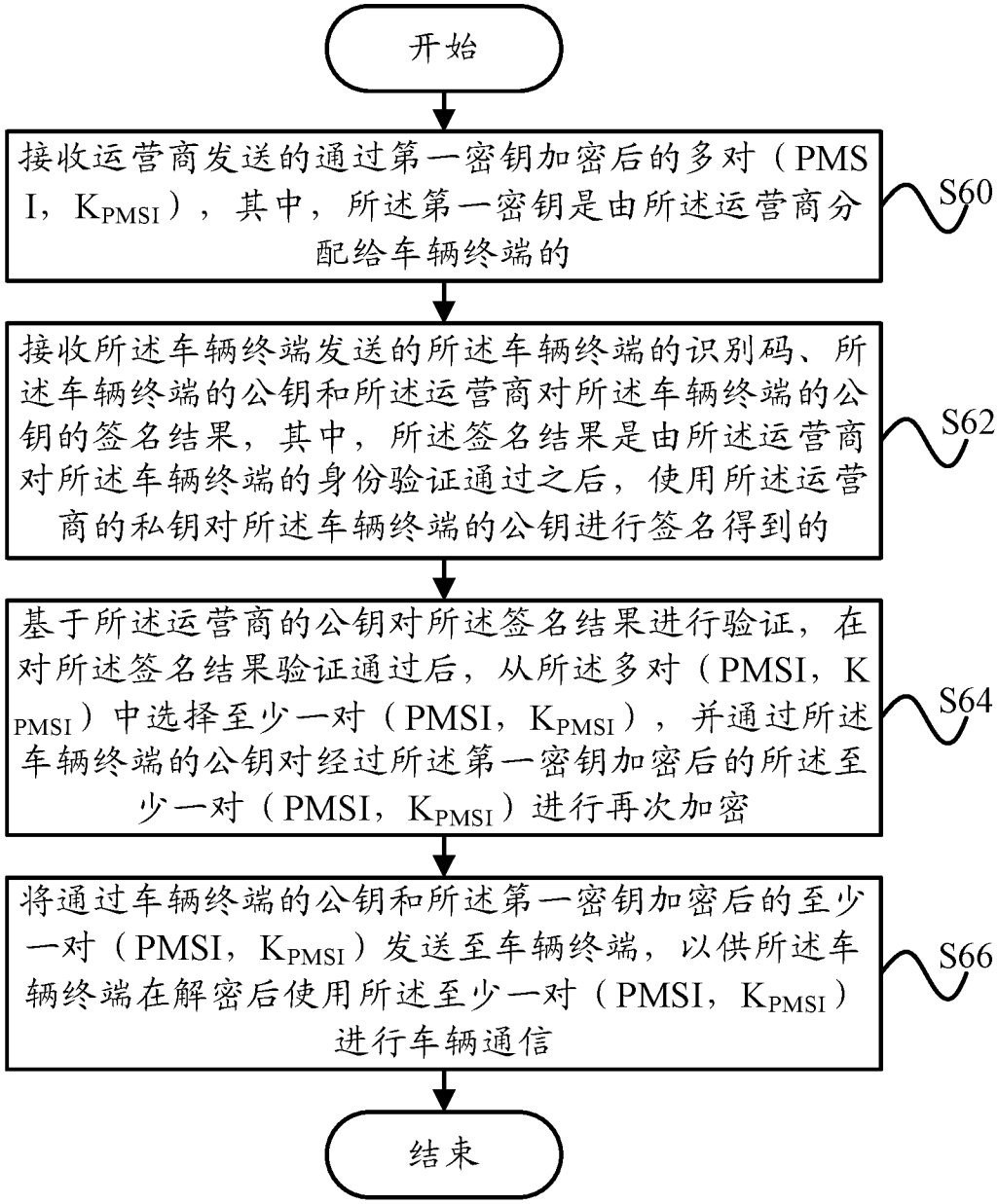
开始
接收运营商发送的通过第一密钥加密后的多对（PMSI，K_{PMSI}），其中，所述第一密钥是由所述运营商分配给车辆终端的
S60
接收所述车辆终端发送的所述车辆终端的识别码、所述车辆终端的公钥和所述运营商对所述车辆终端的公钥的签名结果，其中，所述签名结果是由所述运营商对所述车辆终端的身份验证通过之后，使用所述运营商的私钥对所述车辆终端的公钥进行签名得到的
S62
基于所述运营商的公钥对所述签名结果进行验证，在对所述签名结果验证通过后，从所述多对（PMSI，K_{PMSI}）中选择至少一对（PMSI，K_{PMSI}），并通过所述车辆终端的公钥对经过所述第一密钥加密后的所述至少一对（PMSI，K_{PMSI}）进行再次加密
S64
将通过车辆终端的公钥和所述第一密钥加密后的至少一对（PMSI，K_{PMSI}）发送至车辆终端，以供所述车辆终端在解密后使用所述至少一对（PMSI，K_{PMSI}）进行车辆通信
S66
结束

图 6

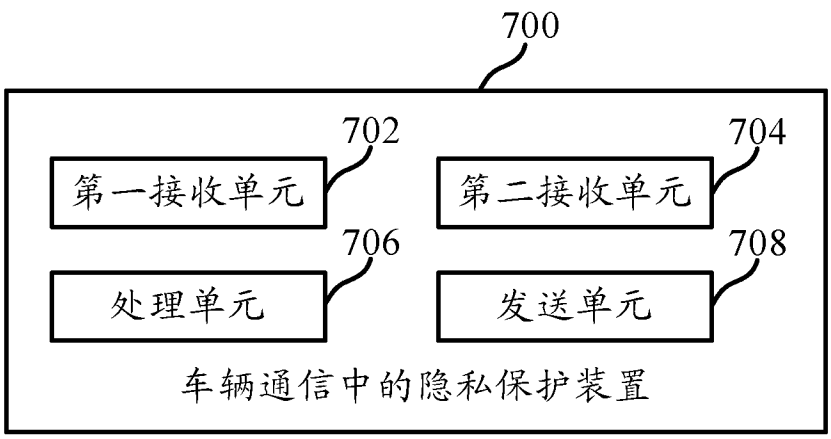
700
702
第一接收单元
704
第二接收单元
706
处理单元
708
发送单元
车辆通信中的隐私保护装置

图 7

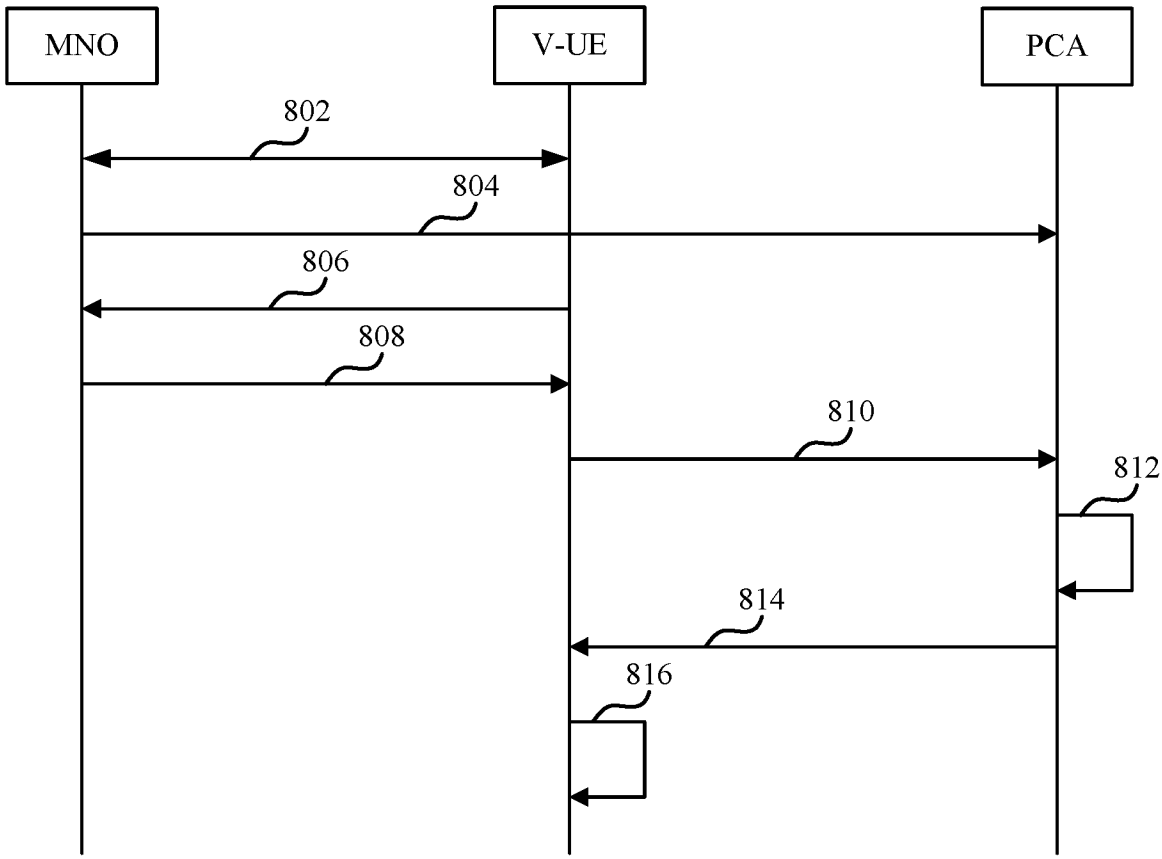
MNO
V-UE
PCA
802
804
806
808
810
812
814
816

图 8

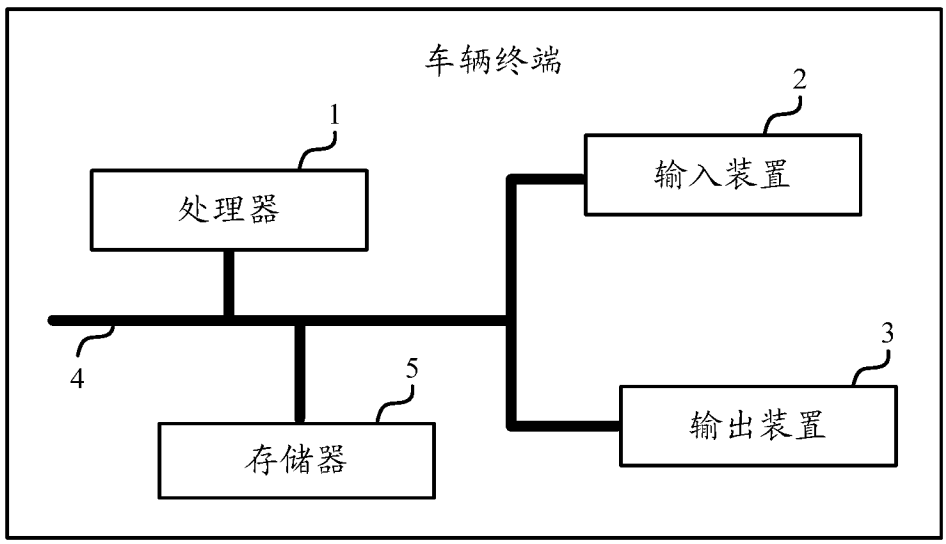
车辆终端
1
处理器
2
输入装置
3
输出装置
4
5
存储器

图 9

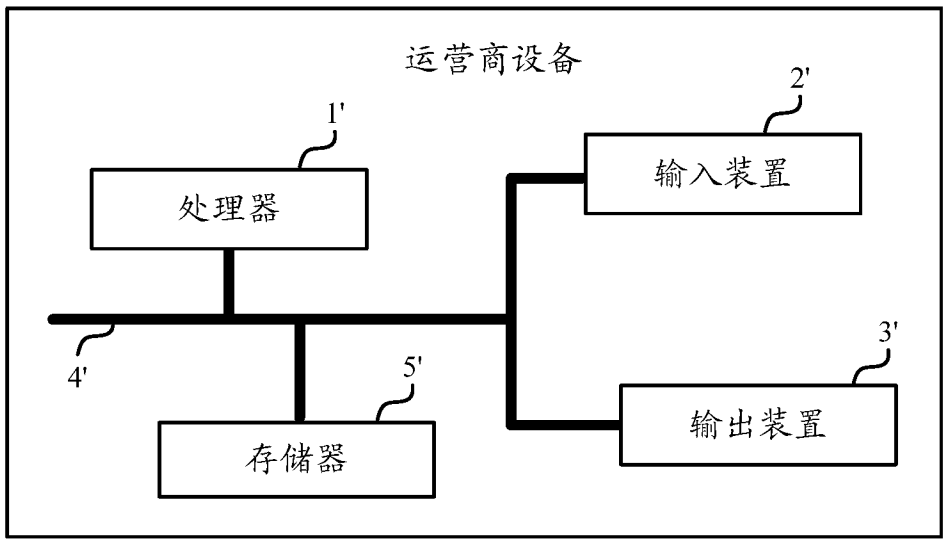

图 10

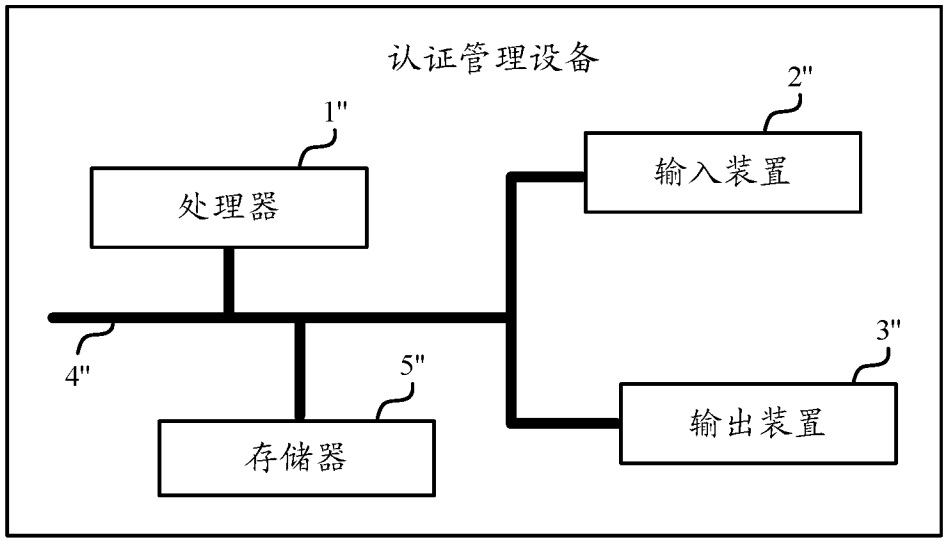

图 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/072672

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/30 (2006.01) i; H04L 9/32 (2006.01) i; H04L 29/06 (2006.01) i; H04L 29/08 (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)

VEN, CPRSABS, CNTXT, USTXT, CNKI, 3GPP: 车辆, 车联网, 车载网, 隐私, 终端, 用户, UE, 运营商, 服务商, 认证, 可信, 验证, 密钥, 秘密, 加密, 签名, 假名, 虚拟名, 虚名, 化名, PMSI, 公钥, 私钥, 身份, vehicular, vehicle, VANET, privacy, secret, terminal, user, operator, server, authentication, certification, security, trusted, key, signature, pseudonymous, pseudonym, public, identification

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	LG Electronics, Update of V2X Attach Identifier Obfuscation Solution in 6.3, 3GPP TSG SA WG3 (Security) Meeting #84, S3-160996, 29 July 2016 (29.07.2016), pages 2-4, section 4, and figure 6.3.2-1	3, 4, 8, 9
A	LG Electronics, Update of V2X Attach Identifier Obfuscation Solution in 6.3, 3GPP TSG SA WG3 (Security) Meeting #84, S3-160996, 29 July 2016 (29.07.2016), pages 2-4, section 4, and figure 6.3.2-1	1, 2, 5-7, 10
A	CN 103618995 A (XIDIAN UNIVERSITY), 05 March 2014 (05.03.2014), entire document	1-10
A	CN 105847235 A (ANHUI UNIVERSITY), 10 August 2016 (10.08.2016), entire document	1-10
A	CN 105554105 A (ANHUI UNIVERSITY), 04 May 2016 (04.05.2016), entire document	1-10

☒ 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
06 July 2017	04 August 2017
Name and mailing address of the ISA 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 WANG, Guixia Telephone No. (86-10) 62411262

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/072672

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 104753680 A (BEIJING UNIVERSITY OF AERONAUTICS AND ASTRONAUTICS), 01 July 2015 (01.07.2015), entire document	1-10
A	JP 2008312213 A (NTT DOCOMO INC.), 25 December 2008 (25.12.2008), entire document	1-10

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/072672

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103618995 A	05 March 2014	CN 103618995 B	18 January 2017
CN 105847235 A	10 August 2016	None	
CN 105554105 A	04 May 2016	None	
CN 104753680 A	01 July 2015	None	
JP 2008312213 A	25 December 2008	EP 2003813 A1	17 December 2008
		JP 4742120 B2	10 August 2011
		EP 2003813 B1	18 March 2009
		DE 602007000729 D1	30 April 2009

国际检索报告

国际申请号
PCT/CN2017/072672

A. 主题的分类

H04L 9/30(2006.01)i; H04L 9/32(2006.01)i; H04L 29/06(2006.01)i; H04L 29/08(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）)

VEN, CPRSABS, CNTXT, USTXT, CNKI, 3GPP: 车辆，车联网，车载网，隐私，终端，用户，UE，运营商，服务商，认证，可信，验证，密钥，秘密，加密，签名，假名，虚拟名，虚名，化名， PMSI，公钥，私钥，身份，vehicular, vehicle, VANET, privacy, secret, terminal, user, operator, server, authentication, certification, security, trusted, key, signature, pseudonymous, pseudonym, public, identification

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	LG Electronics. "Update of V2X attach identifier obfuscation solution in 6.3" 3GPP TSG SA WG3 (Security) Meeting #84, S3-160996, 2016年 7月 29日 (2016-07-29), 第2-4页 第4节，图6.3.2-1	3, 4, 8, 9
A	LG Electronics. "Update of V2X attach identifier obfuscation solution in 6.3" 3GPP TSG SA WG3 (Security) Meeting #84, S3-160996, 2016年 7月 29日 (2016-07-29), 第2-4页 第4节，图6.3.2-1	1, 2, 5-7, 10
A	CN 103618995 A (西安电子科技大学) 2014年 3月 5日 (2014-03-05) 全文	1-10
A	CN 105847235 A (安徽大学) 2016年 8月 10日 (2016-08-10) 全文	1-10
A	CN 105554105 A (安徽大学) 2016年 5月 4日 (2016-05-04) 全文	1-10

☑ 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 7月 6日	2017年 8月 4日

ISA/CN的名称和邮寄地址	受权官员
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	王桂霞
传真号 (86-10)62019451	电话号码 (86-10)62411262

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告

国际申请号
PCT/CN2017/072672

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
A	CN 104753680 A (北京航空航天大学) 2015年 7月 1日 (2015 - 07 - 01) 全文	1-10
A	JP 2008312213 A (NTT DOCOMO INC) 2008年 12月 25日 (2008 - 12 - 25) 全文	1-10

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2017/072672

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	103618995	A	2014年 3月 5日	CN	103618995	B	2017年 1月 18日
CN	105847235	A	2016年 8月 10日		无		
CN	105554105	A	2016年 5月 4日		无		
CN	104753680	A	2015年 7月 1日		无		
JP	2008312213	A	2008年 12月 25日	EP	2003813	A1	2008年 12月 17日
				JP	4742120	B2	2011年 8月 10日
				EP	2003813	B1	2009年 3月 18日
				DE	602007000729	D1	2009年 4月 30日