(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
2024 年 10 月 10 日 (10.10.2024)

WIPO | PCT

(10) 国际公布号
WO 2024/207754 A1

(51) 国际专利分类号:
H04L 9/40 (2022.01)

(21) 国际申请号: PCT/CN2023/133558

(22) 国际申请日: 2023 年 11 月 23 日 (23.11.2023)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202310361154.2 2023年4月6日 (06.04.2023) CN

(71) 申请人: 宁德时代新能源科技股份有限公司 (**CONTEMPORARY AMPEREX TECHNOLOGY CO., LIMITED**) [CN/CN]; 中国福建省宁德市蕉城区漳湾镇新港路2号, Fujian 352100 (CN)。

(72) 发明人: 王超 (**WANG, Chao**); 中国福建省宁德市蕉城区漳湾镇新港路2号, Fujian 352100 (CN)。兰椿树 (**LAN, Chunshu**); 中国福建省宁德市蕉城区漳湾镇新港路2号, Fujian 352100 (CN)。谢吉海 (**XIE, Jihai**); 中国福建省宁德市蕉城区漳湾镇新港路2号, Fujian 352100 (CN)。

(74) 代理人: 北京华进京联知识产权代理有限公司 (**ACIP LAW OFFICES**); 中国北京市海淀区知春路7号致真大厦A1403, Beijing 100191 (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF,

(54) **Title:** IDENTITY AUTHENTICATION METHOD, APPARATUS, VEHICLE, ELECTRONIC CONTROL UNIT AND STORAGE MEDIUM

(54) 发明名称: 身份认证方法、装置、车辆、电子控制单元和存储介质

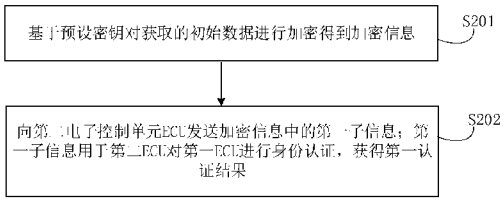


图2

S201 On the basis of a preset key, encrypt acquired initial data to obtain encrypted information

S202 Send first sub-information of the encrypted information to a second electronic control unit (ECU), the first sub-information being used for the second ECU to perform identity authentication on a first ECU so as to obtain a first authentication result

(57) **Abstract:** The present application relates to an identity authentication method, an apparatus, a vehicle, an electronic control unit and a storage medium. The method comprises: on the basis of a preset key, encrypting acquired initial data to obtain encrypted information, and sending first sub-information of the encrypted information to a second electronic control unit (ECU), such that the second ECU performs identity authentication on a first ECU on the basis of the first sub-information so as to obtain a first authentication result. Thus, the second ECU implements identity authentication of the first ECU. Moreover, since the first ECU only sends partial information of the encrypted information to the second ECU, the data volume of the sent information is reduced, thereby reducing the load rate of the identity authentication, and improving the efficiency of communication of the identity authentication.

(57) 摘要: 本申请涉及一种身份认证方法、装置、车辆、电子控制单元和存储介质。所述方法包括：基于预设密钥对获取的初始数据进行加密得到加密信息，并向第二电子控制单元ECU发送加密信息中的第一子信息，从而使第二ECU基于第一子信息对第一ECU进行身份认证，获得第一认证结果，从而实现第二ECU对第一ECU的身份认证。并且，由于第一ECU仅向第二ECU发送加密信息中的部分信息，从而降低了所发送的信息的数据量，降低了身份认证的负载率，提高了身份认证的通信效率。

WO 2024/207754 A1

[见续页]

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))。

身份认证方法、装置、车辆、电子控制单元和存储介质

交叉引用

[0001] 本申请引用于 2023 年 04 月 06 日申请的，申请号为 2023103611542，名称为“身份认证方法、装置、车辆、电子控制单元和存储介质”的中国专利申请的优先权，在此将其全文引入作为参考

技术领域

[0002] 本申请涉及车内网技术领域，特别是涉及一种身份认证方法、装置、车辆、电子控制单元和存储介质。

背景技术

[0003] 车内网是实现单车智能网联的基础技术。车内网是指基于成熟的控制区域网络(controller area network，CAN)、局域互联网络（Local Interconnect Network）或以太网等技术建立的标准化整车网络，实现车内各电子控制单元（Electronic Control Unit，简称 ECU）之间的通信。

[0004] 为了实现两个 ECU 之间的安全通信，需要对 ECU 进行身份认证。然而，目前，车内网中缺少对 ECU 进行身份认证的方案，因此，如何对 ECU 进行身份认证成为本领域亟待解决的技术问题。

发明内容

[0005] 基于此，有必要针对上述技术问题，提供一种能够对 ECU 进行身份认证的身份认证方法、装置、车辆、电子控制单元和存储介质。

[0006] 第一方面，本申请提供了一种身份认证方法。该方法应用于第一电子控制单元 ECU，该方法包括：

[0007] 基于预设密钥对获取的初始数据进行加密得到加密信息；

[0008] 向第二电子控制单元 ECU 发送该加密信息中的第一子信息；该第一子信息用于该第二 ECU 对该第一 ECU 进行身份认证，获得第一认证结果。

[0009] 本申请实施例中，通过基于预设密钥对获取的初始数据进行加密得到加密信息，并向第二电子控制单元 ECU 发送加密信息中的第一子信息，从而使第二 ECU 基于第一子信息对第一 ECU 进行身份认证，获得第一认证结果，从而实现第二 ECU 对第一 ECU 的身份认证。并且，由于第一 ECU 仅向第二 ECU 发送加密信息中的部分信息，从而降低了所发送的信息

的数据量，降低了身份认证的负载率，提高了身份认证的通信效率。

[0010] 在其中一个实施例中，该方法还包括：

[0011] 接收该第二 ECU 发送的第二子信息和该第一认证结果，并基于该第二子信息、以及该加密信息中的第三子信息，对该第二 ECU 进行身份认证，获得第二认证结果；

[0012] 基于该第一认证结果和该第二认证结果，确定该第一 ECU 与该第二 ECU 的双向身份认证结果。

[0013] 本申请实施例中，通过接收第二 ECU 发送的第二子信息和第一认证结果，并基于第二子信息、以及加密信息中的第三子信息，对第二 ECU 进行身份认证，获得第二认证结果，并基于第一认证结果和第二认证结果，确定第一 ECU 与第二 ECU 的双向身份认证结果，从而实现第一 ECU 和第二 ECU 之间的双向身份认证。并且，由于第一 ECU 基于第二子信息、以及加密信息中的第三子信息，对第二 ECU 进行身份认证，获得第二认证结果，即第二 ECU 仅向第一 ECU 发送第二子信息，从而降低了第一 ECU 所接收的信息的数据量，从而降低了双向身份认证的负载率，提高了双向身份认证的通信效率。

[0014] 在其中一个实施例中，该第一子信息为该加密信息中位于第一预设区域范围内的子信息，该第三子信息为该加密信息中位于第二预设区域范围内的子信息。

[0015] 本申请实施例中，第一子信息为该加密信息中位于第一预设区域范围内的子信息，第三子信息为该加密信息中位于第二预设区域范围内的子信息，从而实现第一 ECU 根据第一预设区域范围即可快速确定第一子信息，根据第二预设区域范围即可快速确定第三子信息，从而提高身份认证的效率。

[0016] 在其中一个实施例中，该基于该第二子信息、以及该加密信息中的第三子信息，对该第二 ECU 进行身份认证，获得第二认证结果，包括：

[0017] 将该第二子信息与该第三子信息进行比对得到比对结果；

[0018] 若该比对结果为该第二子信息与该第三子信息一致，则确定该第二认证结果为身份认证通过；

[0019] 若该比对结果为该第二子信息与该第三子信息不一致，则确定该第二认证结果为身份认证未通过。

[0020] 本申请实施例中，通过将第二子信息与第三子信息进行比对得到比对结果，进而根据比较结果确定第二认证结果，将接收到的第二子信息与第一 ECU 计算出的第三子信息进行比对，由于比对的是第二子信息和第三子信息，从而降低了所需比对的数据量，提高比对效率。

[0021] 在其中一个实施例中，该基于该第一认证结果和该第二认证结果，确定该第一 ECU 与该第二 ECU 的双向身份认证结果，包括：

[0022] 若该第一认证结果为身份认证通过、且该第二认证结果为身份认证通过，则确定该双向身份认证结果为双向身份认证通过；

[0023] 若该第一认证结果为身份认证通过、且该第二认证结果为身份认证未通过，则确定该双向身份认证结果为双向身份认证未通过。

[0024] 本实施例中，基于第一认证结果和第二认证结果，从而实现第一 ECU 与第二 ECU 之间的双向身份认证。

[0025] 在其中一个实施例中，该方法还包括：

[0026] 接收该第二 ECU 发送的该第一认证结果；

[0027] 若该第一认证结果为身份认证未通过，则确定该第二 ECU 对该第一 ECU 的身份认证未通过。

[0028] 本申请实施例中，若第一 ECU 接收到第一认证结果，且第一认证结果为身份认证未通过，则第一 ECU 可以确定第二 ECU 对第一 ECU 的身份认证未通过，即第一 ECU 接收到的第一认证结果如果为身份认证未通过，则第一 ECU 后续可以不向第二 ECU 发送通信数据，提高通信数据的安全性。

[0029] 在其中一个实施例中，该方法还包括：

[0030] 向该第二 ECU 发送第一身份认证请求；该第一身份认证请求用于触发该第二 ECU 生成第一随机数；

[0031] 接收该第二 ECU 发送的该第一随机数，并将该第一随机数作为该初始数据。

[0032] 本申请实施例中，通过向第二 ECU 发送第一身份认证请求，并接收第二 ECU 发送的第一随机数，并将第一随机数作为初始数据，从而实现初始数据的不固定性，进而提高第二 ECU 对第一 ECU 进行身份认证得到的第一认证结果的可信度。

[0033] 在其中一个实施例中，该向该第二 ECU 发送第一身份认证请求，包括：

[0034] 每隔预设时长向该第二 ECU 发送该第一身份认证请求。

[0035] 本申请实施例中，本申请实施例提供的方法，第一 ECU 每隔预设时长向第二 ECU 发送第一身份认证请求，从而使第一 ECU 每次接收到的第二 ECU 发送的第一随机数不同，进而基于第一随机数得到的初始数据不同，实现初始数据的不固定性，进而提高第二 ECU 对第一 ECU 进行身份认证得到的第一认证结果的可信度，使得整个通信过程更加安全，能够很好的抵抗重放攻击。并且，由于每隔预设时长向第二 ECU 发送第一身份认证请求，能够降低第一 ECU 发送的第一身份认证请求的次数，降低通信负载率。

[0036] 在其中一个实施例中，该方法还包括：

[0037] 若该双向身份认证结果为双向身份认证通过，则向该第二 ECU 发送通信报文；该通信报文包括通信数据和校验信息，该校验信息根据该加密信息确定，该校验信息用于供该第二 ECU 对该通信数据进行校验。

[0038] 本申请实施例中，在双向身份认证结果为双向身份认证通过的情况下，第一 ECU 向第二 ECU 发送通信报文，并且通信报文中包括的校验信息根据加密信息确定，从而可以提高

整个通信过程的安全性，能够很好的抵抗重放攻击。

[0039] 在其中一个实施例中，该校验信息包括第一校验信息和/或第二校验信息，该第一校验信息为该第一子信息中位于第三预设区域范围内的信息，该第二校验信息为该第三子信息中位于第四预设区域范围的信息。

[0040] 本申请实施例中，通过在通信包括中增加包括第一校验信息和/或第二校验信息的校验信息，从而提高了通信数据的安全性。

[0041] 在其中一个实施例中，该方法还包括：

[0042] 接收该第二 ECU 发送的第二身份认证请求；

[0043] 响应于该第二身份认证请求生成第二随机数，并向该第二 ECU 发送该第二随机数，并将该第二随机数作为该初始数据。

[0044] 本申请实施例中，第一 ECU 可以为主动向第二 ECU 发送第一身份认证请求，实现第二 ECU 对第一 ECU 进行身份认证，也可以同时被动接收第二 ECU 发送的第二身份认证请求，从而实现第一 ECU 对第二 ECU 进行身份认证，提高双向身份认证的效率。

[0045] 第二方面，本申请还提供了一种身份认证装置。该装置设置于第一 ECU，该装置包括：

[0046] 加密模块，用于基于预设密钥对获取的初始数据进行加密得到加密信息；

[0047] 发送模块，用于向第二电子控制单元 ECU 发送该加密信息中的第一子信息；该第一子信息用于该第二 ECU 对该第一 ECU 进行身份认证，获得第一认证结果。

[0048] 第三方面，本申请还提供了一种车辆，其中，该车辆包括第一电子控制单元 ECU 和第二 ECU；

[0049] 该第一 ECU，用于基于预设密钥对获取的初始数据进行加密得到加密信息；

[0050] 该第一 ECU，用于向该第二 ECU 发送该加密信息中的第一子信息；

[0051] 该第二 ECU，用于基于该第一子信息对该第一 ECU 进行身份认证，获得第一认证结果。

[0052] 在其中一个实施例中，该第二 ECU，还用于基于该预设密钥对获取的初始数据进行加密得到认证信息，基于该第一子信息和该认证信息中的第四子信息，对该第一 ECU 进行身份认证，并向该第一 ECU 发送该认证信息中的第二子信息；该第二子信息为该认证信息中位于第二预设区域范围内的子信息，该第四子信息为该认证信息中位于第一预设区域范围内的子信息；

[0053] 该第一 ECU，还用于接收该第二 ECU 发送的该第二子信息，并基于该加密信息中的第三子信息、以及该第二子信息，对该第二 ECU 进行身份认证，获得第二认证结果。

[0054] 第四方面，本申请还提供了一种电子控制单元，包括存储器和处理器，该存储器存储有计算机程序，其中，该处理器执行该计算机程序时实现上述的方法的步骤。

[0055] 第五方面，本申请还提供了一种计算机可读存储介质。该计算机可读存储介质，其上存储有计算机程序，该计算机程序被处理器执行时实现上述的方法的步骤。

[0056] 第六方面，本申请还提供了一种计算机程序产品。该计算机程序产品，包括计算机程序，该计算机程序被处理器执行时实现上述的方法的步骤。

[0057] 上述说明仅是本申请技术方案的概述，为了能够更清楚了解本申请的技术手段，而可依照说明书的内容予以实施，并且为了让本申请的上述和其它目的、特征和优点能够更明显易懂，以下特举本申请的具体实施方式。

附图说明

[0058] 为了更清楚地说明本申请实施例的技术方案，下面将对本申请实施例中所需要使用的附图作简单地介绍，显而易见地，下面所描述的附图仅仅是本申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据附图获得其他的附图：

[0059] 图 1 为一个实施例中身份认证方法的应用环境图；

[0060] 图 2 是本申请实施例提供的一种身份认证方法的流程示意图；

[0061] 图 3 是本申请实施例提供的一种双向身份认证方法的流程示意图；

[0062] 图 4 是本申请实施例提供的一种第二认证结果获得方法的流程示意图；

[0063] 图 5 是本申请实施例提供的另一种身份认证方法的流程示意图；

[0064] 图 6 是本申请实施例提供的一种身份认证请求发送方法的流程示意图；

[0065] 图 7 是本申请实施例提供的一种通信报文格式示意图；

[0066] 图 8 是本申请实施例提供的校验信息格式的示意图；

[0067] 图 9 是本申请实施例提供的一种双向身份认证方法的信令流程图；

[0068] 图 10 是本申请实施例提供的另一种身份认证请求发送方法的流程示意图；

[0069] 图 11 是本申请实施例提供的一种身份认证装置的结构框图。

具体实施方式

[0070] 下面将结合附图对本申请技术方案的实施例进行详细的描述。以下实施例仅用于更加清楚地说明本申请的技术方案，因此只作为示例，而不能以此来限制本申请的保护范围。

[0071] 除非另有定义，本文所使用的所有的技术和科学术语与属于本申请的技术领域的技术人员通常理解的含义相同；本文中所使用的术语只是为了描述具体的实施例的目的，不是旨在于限制本申请；本申请的说明书和权利要求书及上述附图说明中的术语“包括”和“具有”以及它们的任何变形，意图在于覆盖不排他的包含。

[0072] 在本申请实施例的描述中，技术术语“第一”“第二”等仅用于区别不同对象，而不能理解为指示或暗示相对重要性或者隐含指明所指示的技术特征的数量、特定顺序或主次关系。

在本申请实施例的描述中，“多个”的含义是两个以上，除非另有明确具体的限定。

[0073] 在本文中提及“实施例”意味着，结合实施例描述的特定特征、结构或特性可以包含在本申请的至少一个实施例中。在说明书中的各个位置出现该短语并不一定均是指相同的实施例，也不是与其它实施例互斥的独立的或备选的实施例。本领域技术人员显式地和隐式地理解的是，本文所描述的实施例可以与其它实施例相结合。

[0074] 在本申请实施例的描述中，术语“和/或”仅仅是一种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。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系。

[0075] 在本申请实施例的描述中，术语“多个”指的是两个以上（包括两个），同理，“多组”指的是两组以上（包括两组），“多片”指的是两片以上（包括两片）。

[0076] 在本申请实施例的描述中，技术术语“中心”“纵向”“横向”“长度”“宽度”“厚度”“上”“下”“前”“后”“左”“右”“竖直”“水平”“顶”“底”“内”“外”“顺时针”“逆时针”“轴向”“径向”“周向”等指示的方位或位置关系为基于附图所示的方位或位置关系，仅是为了便于描述本申请实施例和简化描述，而不是指示或暗示所指的装置或元件必须具有特定的方位、以特定的方位构造和操作，因此不能理解为对本申请实施例的限制。

[0077] 在本申请实施例的描述中，除非另有明确的规定和限定，技术术语“安装”“相连”“连接”“固定”等术语应做广义理解，例如，可以是固定连接，也可以是可拆卸连接，或成一体；也可以是机械连接，也可以是电连接；可以是直接相连，也可以通过中间媒介间接相连，可以是两个元件内部的连通或两个元件的相互作用关系。对于本领域的普通技术人员而言，可以根据具体情况理解上述术语在本申请实施例中的具体含义。

[0078] 车内网是实现单车智能网联的基础技术。车内网是指基于成熟的 CAN、局域互联网络或以太网等技术建立的标准化整车网络，实现车内各 ECU 之间的通信。

[0079] 为了实现两个 ECU 之间的安全通信，需要对 ECU 进行身份认证。然而，目前，车内网中缺少对 ECU 进行身份认证的方案，因此，如何对 ECU 进行身份认证成为本领域亟待解决的技术问题。

[0080] 本申请实施例中，为了实现对 ECU 进行身份认证，第一 ECU 基于预设密钥对获取的初始数据进行加密得到加密信息，并向第二 ECU 发送加密信息中的第一子信息；第一子信息用于第二 ECU 对第一 ECU 进行身份认证，获得第一认证结果,实现第二 ECU 对第一 ECU 进行身份认证。

[0081] 本申请实施例提供的身份认证方法，可以应用于如图 1 所示的应用环境中。其中，第一 ECU 通过网络与第二 ECU 进行通信。第一 ECU 基于预设密钥对获取的初始数据进行加密得到加密信息，第一 ECU 向第二 ECU 发送加密信息中的第一子信息，第二 ECU 基于第一子信息对第一 ECU 进行身份认证，获得对第一 ECU 进行身份认证的第一认证结果，从而实现

对 ECU 进行身份认证。

[0082] 在一个实施例中，如图 2 所示，图 2 是本申请实施例提供的一种身份认证方法的流程示意图，该方法应用于车辆中的 ECU，在本实施例中以应用于图 1 中的第一 ECU 为例进行说明，该方法包括以下步骤：

[0083] S201、基于预设密钥对获取的初始数据进行加密得到加密信息。

[0084] 其中，第一 ECU 可以采用密码学算法，基于预设密钥对获取的初始数据进行加密得到加密信息。密码学算法数据加密标准（Data Encryption Standard，DES）加密算法、高级加密标准（Advanced Encryption Standard，AES）加密算法、信息摘要算法(message-digest algorithm 5，MD5）加密算法等。预设密钥和密码学算法可以在出厂时集成于第一 ECU 中。

[0085] 初始数据可以为预设数据，第一 ECU 和第二 ECU 中可以预先存储有预设数据，在车辆启动后，双方可以同时基于预设密钥对预先存储的预设数据进行加密得到加密信息。或者，初始数据也可以为第一 ECU 接收的第二 ECU 发送的随机数。

[0086] S202、向第二电子控制单元 ECU 发送加密信息中的第一子信息；第一子信息用于第二 ECU 对第一 ECU 进行身份认证，获得第一认证结果。

[0087] 第一 ECU 得到加密信息后，可以将加密信息中的部分信息发送给第二 ECU，即将加密信息中的第一子信息发送给第二 ECU，从而使第二 ECU 能够基于第一子信息对第一 ECU 进行身份认证，获得第一认证结果。

[0088] 在一种实现方式中，第一 ECU 将加密信息的最高比特位作为起始位置，将第一预设长度的比特位数作为第一子信息，第一预设长度可以等于加密信息的总长度的二分之一，也可以等于其他长度。例如，加密信息的长度为 8 字节，可以将高 4 字节命名为 K1，将低 4 字节命名为 K3，第一 ECU 可以将 K1 作为第一子信息，则第一 ECU 仅将 K1 发送给第二 ECU。

[0089] 在另一种实现方式中，第一 ECU 将加密信息的最低比特位作为起始位置，将第二预设长度的比特位数作为第一子信息，第二预设长度可以等于加密信息的总长度的二分之一，也可以等于其他长度，例如，第一 ECU 可以将 K3 作为第一子信息，则第一 ECU 仅将 K3 发送给第二 ECU。

[0090] 需要说明的是，ECU 之间可以通过协议确定发送 K1 还是 K3，若协议第一 ECU 得到加密信息后发送 K1，则第一 ECU 向第二 ECU 发送 K1。若协议第一 ECU 得到加密信息后发送 K3，则第一 ECU 向第二 ECU 发送 K3。为了便于介绍，本实施例中以第一 ECU 向第二 ECU 发送 K1 为例进行说明。

[0091] 第二 ECU 在出厂时也集成有预设密钥和密码学算法，车辆启动后，第二 ECU 可以采用集成的密码学算法对预设密钥进行加密得到认证信息，该认证信息的长度为 8 字节，将认证信息中的高 4 字节命名为 K4，将认证信息中的低 4 字节命名为 K2。第二 ECU 接收到 K1 后，第二 ECU 对第一 ECU 进行身份认证的过程例如为：第二 ECU 将 K1 与自身计算得到的

K4 进行比对，若 K1 与 K4 一致，则确定第一认证结果为身份认证通过；若 K1 与 K4 不一致，则确定第一认证结果为身份认证未通过。其中，若第二 ECU 在出厂时也集成的预设密钥与第一 ECU 相同,且第二 ECU 集成的密码学算法与第一 ECU 的相同，则第二 ECU 将 K1 与自身计算得到的 K4 进行比对得到的第一认证结果为身份认证通过的结果，否则，得到的第一认证结果为身份认证未通过的结果。

[0092] 本申请实施例提供的方法，通过基于预设密钥对获取的初始数据进行加密得到加密信息，并向第二电子控制单元 ECU 发送加密信息中的第一子信息，从而使第二 ECU 基于第一子信息对第一 ECU 进行身份认证，获得第一认证结果，从而实现第二 ECU 对第一 ECU 的身份认证。并且，由于第一 ECU 仅向第二 ECU 发送加密信息中的部分信息，从而降低了所发送的信息的数据量，降低了身份认证的负载率，提高了身份认证的通信效率。

[0093] 在一个实施例中，如图 3 所示，图 3 是本申请实施例提供的一种双向身份认证方法的流程示意图。该方法包括如下步骤：

[0094] S301、基于预设密钥对获取的初始数据进行加密得到加密信息。

[0095] S302、向第二电子控制单元 ECU 发送加密信息中的第一子信息；第一子信息用于第二 ECU 对第一 ECU 进行身份认证，获得第一认证结果。

[0096] S303、接收第二 ECU 发送的第二子信息和第一认证结果，并基于第二子信息、以及加密信息中的第三子信息，对第二 ECU 进行身份认证，获得第二认证结果。

[0097] 以第一子信息为 K1 为例，则第二子信息例如为上述实施例中的 K2。若第二 ECU 得到的第一认真结果为身份认证通过，即第二 ECU 确定第一 ECU 为可信的 ECU，则第二 ECU 可以向第一 ECU 发送 K2 和第一认证结果，相应的，第一 ECU 接收到 K2 和第一认证结果，并基于 K2 以及加密信息中的第三子信息，对第二 ECU 进行身份认证，获得第二认证结果。其中，第三子信息为 K3。

[0098] 若 K2 与 K3 一致，则第一 ECU 确定第二认证结果为身份认证通过，即第一 ECU 确定第二 ECU 为可信的 ECU。若 K2 与 K3 一致，则第一 ECU 确定第二认证结果为身份认证未通过，即第一 ECU 确定第二 ECU 为不可信的 ECU。

[0099] 需要说明的是，第二 ECU 对第一 ECU 的认证、第一 ECU 对第二 ECU 的认证可以同时进行，即车辆启动后，第一 ECU 得到加密信息，第二 ECU 得到认证信息，并且，第一 ECU 向第二 ECU 发送 K1,第二 ECU 向第一 ECU 发送 K2。其中，第一 ECU 向第二 ECU 发送 K1，从而使第二 ECU 基于 K1 和 K4 实现对第一 ECU 的身份认证；第二 ECU 向第一 ECU 发送 K2,从而使第一 ECU 基于 K2 和 K3 实现对第二 ECU 的身份认证。

[00100] S304、基于第一认证结果和第二认证结果，确定第一 ECU 与第二 ECU 的双向身份认证结果。

[00101] 其中，若第一认证结果为身份认证未通过、且第二认证结果为身份认证通过，则确定

双向身份认证结果为双向身份认证未通过；

[00102] 若第一认证结果为身份认证未通过、且第二认证结果为身份认证未通过，则确定双向身份认证结果为双向身份认证未通过。

[00103] 本实施例提供的方法，通过接收第二 ECU 发送的第二子信息和第一认证结果，并基于第二子信息、以及加密信息中的第三子信息，对第二 ECU 进行身份认证，获得第二认证结果，并基于第一认证结果和第二认证结果，确定第一 ECU 与第二 ECU 的双向身份认证结果，从而实现第一 ECU 和第二 ECU 之间的双向身份认证。并且，由于第一 ECU 基于第二子信息、以及加密信息中的第三子信息，对第二 ECU 进行身份认证，获得第二认证结果，即第二 ECU 仅向第一 ECU 发送第二子信息，从而降低了第一 ECU 所接收的信息的数据量，从而降低了双向身份认证的负载率，提高了双向身份认证的通信效率。

[00104] 在一个实施例中，第一子信息为加密信息中位于第一预设区域范围内的子信息，第三子信息为加密信息中位于第二预设区域范围内的子信息。

[00105] 例如，若加密信息的长度为 8 字节，可以将加密信息的一个最高字节的信息作为第一子信息，将加密信息的一个最低字节的信息作为第三子信息，该最高字节即为第一预设区域范围，该最低字节为第二预设区域范围。

[00106] 或者，将加密信息的最高字节和最低字节作为第一子信息，将加密信息中除第一子信息之外的其他子信息作为第三子信息。

[00107] 本申请实施例中，第一子信息为该加密信息中位于第一预设区域范围内的子信息，第三子信息为该加密信息中位于第二预设区域范围内的子信息，从而实现第一 ECU 根据第一预设区域范围即可快速确定第一子信息，根据第二预设区域范围即可快速确定第三子信息，从而提高身份认证的效率。

[00108] 在一个实施例中，如图 4 所示，图 4 是本申请实施例提供的一种第二认证结果获得方法的流程示意图。本实施例涉及的是如何基于第二子信息、以及加密信息中的第三子信息，对第二 ECU 进行身份认证，获得第二认证结果的一种可能的实现方式。在上述实施例的基础上，上述的 S303 中的“基于第二子信息、以及加密信息中的第三子信息，对第二 ECU 进行身份认证，获得第二认证结果”可以包括如下步骤：

[00109] S401、将第二子信息与第三子信息进行比对得到比对结果。

[00110] S402、若比对结果为第二子信息与第三子信息一致，则确定第二认证结果为身份认证通过。

[00111] S403、若比对结果为第二子信息与第三子信息不一致，则确定第二认证结果为身份认证未通过。

[00112] 以第二子信息为 K2，第三子信息为 K3 为例，则 K2 与 K3 一致，则确定第二认证结果为身份认证通过。若 K2 与 K3 不一致，则确定第二认证结果为身份认证未通过。

[00113] 第二子信息与第三子信息一致可以指第二子信息与第三子信息相同。或者第二子信息与第三子信息的相似度大于等于预设阈值，例如，预设阈值为 99.8%,第二子信息与第三子信息的相似度等于 99.9%，则认为第二子信息与第三子信息一致。

[00114] 本申请实施例中，通过将第二子信息与第三子信息进行比对得到比对结果，进而根据比较结果确定第二认证结果，将接收到的第二子信息与第一 ECU 计算出的第三子信息进行比对，由于比对的是第二子信息和第三子信息，从而降低了所需比对的数据量，提高比对效率。

[00115] 在一个实施例中，上述的 S302、基于第一认证结果和第二认证结果，确定第一 ECU 与第二 ECU 的双向身份认证结果，可以通过如下方式实现：

[00116] 若第一认证结果为身份认证通过、且第二认证结果为身份认证通过，则确定双向身份认证结果为双向身份认证通过；

[00117] 若第一认证结果为身份认证通过、且第二认证结果为身份认证未通过，则确定双向身份认证结果为双向身份认证未通过。

[00118] 本实施例中，基于第一认证结果和第二认证结果，从而实现第一 ECU 与第二 ECU 之间的双向身份认证。

[00119] 在一个实施例中，如图 5 所示，图 5 是本申请实施例提供的另一种身份认证方法的流程示意图。本实施例涉及的是第一 ECU 如何确定第二 ECU 是否对第一 ECU 的身份认证通过的流程示意图。在上述实施例的基础上，该方法包括如下步骤：

[00120] S501、接收第二 ECU 发送的第一认证结果。

[00121] S502、若第一认证结果为身份认证未通过，则确定第二 ECU 对第一 ECU 的身份认证未通过。

[00122] 本申请实施例中，若第一 ECU 接收到第一认证结果，且第一认证结果为身份认证未通过，则第一 ECU 可以确定第二 ECU 对第一 ECU 的身份认证未通过，即第一 ECU 接收到的第一认证结果如果为身份认证未通过，则第一 ECU 后续不向第二 ECU 发送通信数据，提高通信数据的安全性。

[00123] 需要说明的是，若第一 ECU 接收到的第一认证结果为身份认证未通过，则第一 ECU 即使已经接收到第二 ECU 发送的第二子信息，也不用将第二子信息与第三子信息进行比对，即无需对第二 ECU 的身份进行认证，可以接着对其他 ECU 进行身份认证，从而提高通信认证效率。

[00124] 在一些实施例中，第一 ECU 可以是主动发起身份认证请求的 ECU，主动发起身份认证请求的 ECU 可以为主动向另一个 ECU 发送数据的 ECU。例如如图 6 所示，图 6 是本申请实施例提供的一种身份认证请求发送方法的流程示意图。在上述实施例的基础上，该方法包括如下步骤：

[00125] S601、向第二 ECU 发送第一身份认证请求；第一身份认证请求用于触发第二 ECU 生

成第一随机数。

[00126] 其中，第一 ECU 可以实时向第二 ECU 发送第一身份认证请求。

[00127] S602、接收第二 ECU 发送的第一随机数，并将第一随机数作为初始数据。

[00128] 第二 ECU 可以向第一 ECU 发送自身产生的第一随机数，相应的，第一 ECU 将接收到的第一随机数作为初始数据。第一 ECU 获取到初始数据后，可以基于预设密钥对初始数据进行加密得到新的加密信息，也即针对每个第一身份认证请求，第一 ECU 得到的加密信息可能不同，即第一 ECU 每次得到的加密信息中的 K1 可能不同，以及 K3 可能不同。

[00129] 本申请实施例提供的方法，通过向第二 ECU 发送第一身份认证请求，并接收第二 ECU 发送的第一随机数，并将第一随机数作为初始数据，从而实现初始数据的不固定性，进而提高第二 ECU 对第一 ECU 进行身份认证得到的第一认证结果的可信度。

[00130] 在一些实施例中，上述的 S601、向第二 ECU 发送第一身份认证请求可以通过如下方式实现：

[00131] 第一 ECU 可以每隔预设时长向第二 ECU 发送第一身份认证请求，例如，第一 ECU 每隔 5 秒重复向第二 ECU 发送一次第一身份认证请求，即车辆启动到熄火之间的一次驾驶时间段内，可以进行多次身份认证。针对第一 ECU 发送的每次第一身份认证请求，第二 ECU 会产生新的第一随机数 S。

[00132] 本申请实施例提供的方法，第一 ECU 每隔预设时长向第二 ECU 发送第一身份认证请求，从而使第一 ECU 每次接收到的第二 ECU 发送的第一随机数不同，进而基于第一随机数得到的初始数据不同，实现初始数据的不固定性，进而提高第二 ECU 对第一 ECU 进行身份认证得到的第一认证结果的可信度，使得整个通信过程更加安全，能够很好的抵抗重放攻击。并且，由于每隔预设时长向第二 ECU 发送第一身份认证请求，能够降低第一 ECU 发送的第一身份认证请求的次数，降低通信负载率。

[00133] 在一些实施例中，若第一 ECU 为主动发起身份认证请求的 ECU，则在第一 ECU 和第二 ECU 之间的双向身份认证结果为双向身份认证通过的情况下，第一 ECU 可以主动向第二 ECU 发送通信报文，向第二 ECU 发送通信报文的步骤如下：

[00134] 若双向身份认证结果为双向身份认证通过，则向第二 ECU 发送通信报文；通信报文包括通信数据和校验信息，校验信息根据加密信息确定，校验信息用于供第二 ECU 对通信数据进行校验。其中，一帧通信报文的格式如图 7 所示，图 7 是本申请实施例提供的一种通信报文格式示意图。

[00135] 本申请实施例中，在双向身份认证结果为双向身份认证通过的情况下，第一 ECU 向第二 ECU 发送通信报文，并且通信报文中包括的校验信息根据加密信息确定，从而可以提高整个通信过程的安全性，能够很好的抵抗重放攻击。

[00136] 例如，若加密信息为上述实施例介绍的 8 字节的加密信息，该加密信息包括第一子信

息 K1 和第三子信息 K3，则校验信息可以包括 K1 中的部分信息和/或 K3 中的部分信息。例如，校验信息包括中第一子信息 K1 中的高 4 比特位和第三子信息 K3 中的低 4 比特位。

[00137] 需要说明的是，若第一 ECU 将接收的第二 ECU 发送的第一随机数作为初始数据，由于每次的第一认证请求对应的第一随机数可能不同，因此，初始数据可能不同，使得每次的第一认证请求对应的加密信息不同，校验信息也会随加密信息变化二变化，这样可以使得整个通信过程更加安全，能够很好的抵抗重放攻击。

[00138] 在一些实施例中，校验信息包括第一校验信息和/或第二校验信息，第一校验信息为第一子信息中位于第三预设区域范围内的信息，第二校验信息为第三子信息中位于第四预设区域范围的信息。

[00139] 其中，第三预设区域范围可以为第一子信息中的部分区域或全部区域，第四预设区域范围可以为第三子信息中的部分区域或全部区域。

[00140] 例如，以第三预设区域范围为第一子信息中的部分区域，第四预设区域范围为第三子信息中的部分区域为例，则第一校验信息可以为由第一子信息的高 4 比特位组成，第三预设区域范围指第一子信息中高 4 比特位所在的区域范围；第二校验信息可以为第三子信息的低 4 比特位组成，第四预设区域范围指第三子信息中低 4 比特位所在的区域范围，此种情况下，可以减少校验信息的数据量，提高校验效率。如图 8 所示，图 8 是本申请实施例提供的校验信息格式的示意图，图 8 中示出的校验信息为 1 字节，该 1 字节的高 4 比特位作为第一校验信息，该 1 字节的低 4 比特位作为第二校验信息，该高 4 比特位为第一子信息中的高 4 比特位，该低 4 比特位为第三子信息中的低 4 比特位。

[00141] 或者，第一校验信息可以为由第一子信息的高 4 比特位组成，第三预设区域范围指第一子信息中高 4 比特位所在的区域范围；第二校验信息可以为第三子信息的高 4 比特位组成，第四预设区域范围指第三子信息中高 4 比特位所在的区域范围。

[00142] 本申请实施例中，通过在通信包括中增加包括第一校验信息和/或第二校验信息的校验信息，从而提高了通信数据的安全性。

[00143] 为了对第一 ECU 和第二 ECU 之间的双向身份认证过程进行更清楚的介绍，下面结合图 9 进行说明，图 9 是本申请实施例提供的一种双向身份认证方法的信令流程图。本实施例中以第一 ECU 主动向第二 ECU 发送身份认证请求为例。

[00144] S901、第一 ECU 向第二 ECU 发送第一身份认证请求。

[00145] 相应的，第二 ECU 接收第一 ECU 发送的第一身份认证请求。

[00146] S902、第二 ECU 响应于第一身份认证请求生成第一随机数。

[00147] S903、第二 ECU 向第一 ECU 发送第一随机数。

[00148] 第二 ECU 向第一 ECU 发送第一随机数,向第一 ECU 发起挑战。

[00149] S904、第二 ECU 将第一随机数作为初始数据，采用预先存储的预设密钥对初始数据

进行加密得到认证信息，并将认证信息分为第四子信息和第二子信息。

[00150] 其中，第四子信息可以为从认证信息的最高比特位开始的预设长度的子信息，第二子信息 K 可以为从认证信息的最低比特位开始的预设长度的子信息。例如，第四子信息为上述实施例中举例介绍的 K4，第二子信息为 K2，即第二 ECU 将认证信息分为高 4 字节的 K4 和低 4 字节的 K2。

[00151] S905、第一 ECU 将第一随机数作为初始数据，基于预设密钥对获取的初始数据进行加密得到加密信息，并将加密信息分解为第一子信息和第三子信息。

[00152] 其中，第一子信息可以为上述实施例中介绍的 K1，第三子信息可以为上述实施例中介绍的 K3。

[00153] S906、第一 ECU 向第二 ECU 发送第一子信息。

[00154] 相应的，第二 ECU 接收第一 ECU 发送的第一子信息。

[00155] S907、第二 ECU 将接收到的第一子信息与第四子信息进行比对，得到第一认证结果。

[00156] 若第一子信息与第四子信息一致，则确定第一认证结果为身份认证通过。若第一子信息与第四子信息不一致，则确定第一认证结果为身份认证未通过。若第一认证结果为身份认证通过，则可以第二 ECU 可以向第一 ECU 发送第一认证结果和第二子信息。

[00157] S908、第二 ECU 向第一 ECU 发送第一认证结果和第二子信息。

[00158] 相应的，第一 ECU 接收第二 ECU 发送的第一认证结果和第二子信息。

[00159] S909、第一 ECU 将第二子信息与加密信息中的第三子信息进行比对。

[00160] 若第二子信息与第三子信息一致，则第一 ECU 确定第二 ECU 为可信的 ECU。

[00161] S910、第一 ECU 向第二 ECU 发送通信报文。

[00162] S911、第二 ECU 基于认证信息和校验信息对通信报文中的通信数据进行校验。

[00163] 相应的，第二 ECU 接收到通信报文，并基于自身计算得到的认证信息对通信报文中包括的校验信息进行校验。例如，若第一校验信息由第一子信息的高 4 比特位组成，第二校验信息由第三子信息的低 4 比特位组成，则第二 ECU 可以采用第四子信息中的高 4 比特位与第一校验信息进行比对得到第一比对结果，并采用第二子信息中的低 4 比特位与第二校验信息进行比对得到第二比对结果，进而根据第一比对结果和第二比对结果，确定接收到的通信报文是否为可信报文。

[00164] 例如，第一比对结果为第二子信息中的低 4 比特位与第二校验信息一致，且第二比对结果为第二子信息中的低 4 比特位与第二校验信息一致，则确定接收到的通信报文为可信报文；若第一比对结果为第二子信息中的低 4 比特位与第二校验信息不一致，和/或，第二比对结果为第二子信息中的低 4 比特位与第二校验信息不一致，则确定接收到的通信报文为不可信报文。

[00165] 需要说明的是，在一些实施例中，第一 ECU 可以是被动进行身份认证请求的 ECU，

被动进行身份认证请求的 ECU 可以为接收第二 ECU 发送的数据的 ECU，即第二 ECU 若需要主动向第一 ECU 发送数据，则第二 ECU 可以向第一 ECU 发送第二身份认证请求。例如如图 10 所示，图 10 是本申请实施例提供的另一种身份认证请求发送方法的流程示意图。在上述实施例的基础上，该方法包括如下步骤：

[00166] S1001、接收第二 ECU 发送的第二身份认证请求。

[00167] S1002、响应于第二身份认证请求生成第二随机数，并向第二 ECU 发送第二随机数，并将第二随机数作为初始数据。

[00168] 若第一 ECU 接收到第二 ECU 发送的第二身份认证请求，则可以响应于第二身份认证请求生成第二随机数，并向第二 ECU 发送第二随机数，并将第二随机数作为初始数据，第一 ECU 采用预设密钥对初始数据进行加密得到加密信息，并且第一 ECU 后续执行的流程与上述实施例中介绍的第二 ECU 的执行流程相同,为避免重复，此处不再赘述。

[00169] 本申请实施例中，第一 ECU 可以为主动向第二 ECU 发送第一身份认证请求，实现第二 ECU 对第一 ECU 进行身份认证，也可以同时被动接收第二 ECU 发送的第二身份认证请求，从而实现第一 ECU 对第二 ECU 进行身份认证，提高双向身份认证的效率。

[00170] 在本申请实施例中，还提供了一种车辆，车辆包括如图 1 示出的第一 ECU 和第二 ECU；

[00171] 第一 ECU，用于基于预设密钥对获取的初始数据进行加密得到加密信息；

[00172] 第一 ECU，用于向第二 ECU 发送加密信息中的第一子信息；

[00173] 第二 ECU，用于基于第一子信息对第一 ECU 进行身份认证，获得第一认证结果。

[00174] 在一些实施例中，第二 ECU，还用于基于预设密钥对获取的初始数据进行加密得到认证信息，基于第一子信息和认证信息中的第四子信息，对第一 ECU 进行身份认证，并向第一 ECU 发送认证信息中的第二子信息；第二子信息为认证信息中位于第二预设区域范围内的子信息，第四子信息为认证信息中位于第一预设区域范围内的子信息；

[00175] 第一 ECU，还用于接收第二 ECU 发送的第二子信息，并基于加密信息中的第三子信息、以及第二子信息，对第二 ECU 进行身份认证，获得第二认证结果。

[00176] 其中，第二子信息为认证信息中位于第二预设区域范围内的子信息，即第二子信息在认证信息中所处的区域与第三子信息在加密信息中所处的区域对应。例如，第三子信息为加密信息的一个最低字节的信息的情况下，第二子信息为认证信息中一个最低字节的信息。

[00177] 第四子信息为认证信息中位于第一预设区域范围内的子信息，即第四子信息在认证信息中所处的区域与第一子信息在加密信息中所处的区域对应。例如，第一子信息为加密信息的一个最高字节的信息的情况下，第四子信息为认证信息中一个最高字节的信息。

[00178] 应该理解的是，虽然如上的各实施例所涉及的流程图中的各个步骤按照箭头的指示依次显示，但是这些步骤并不是必然按照箭头指示的顺序依次执行。除非本文中有明确的说明，这些步骤的执行并没有严格的顺序限制，这些步骤可以以其它的顺序执行。而且，如上的各

实施例所涉及的流程图中的至少一部分步骤可以包括多个步骤或者多个阶段，这些步骤或者阶段并不必然是在同一时刻执行完成，而是可以在不同的时刻执行，这些步骤或者阶段的执行顺序也不必然是依次进行，而是可以与其它步骤或者其它步骤中的步骤或者阶段的至少一部分轮流或者交替地执行。

[00179] 基于同样的发明构思，本申请实施例还提供了一种用于实现上述所涉及的身份认证方法的身份认证装置。该装置所提供的解决问题的实现方案与上述方法中所记载的实现方案相似，故下面所提供的一个或多个身份认证装置实施例中的具体限定可以参见上文中对于身份认证方法的限定，在此不再赘述。

[00180] 在一个实施例中，如图 11 所示，图 11 是本申请实施例提供的一种身份认证装置的结构框图，该装置 1100 设置于第一 ECU，该装置 1100 包括：

[00181] 加密模块 1101，用于基于预设密钥对获取的初始数据进行加密得到加密信息；

[00182] 第一发送模块 1102，用于向第二电子控制单元 ECU 发送加密信息中的第一子信息；第一子信息用于第二 ECU 对第一 ECU 进行身份认证，获得第一认证结果。

[00183] 在一个实施例中，方法还包括：

[00184] 第一接收模块，用于接收第二 ECU 发送的第二子信息和第一认证结果，并基于第二子信息、以及加密信息中的第三子信息，对第二 ECU 进行身份认证，获得第二认证结果；

[00185] 第一确定模块，用于基于第一认证结果和第二认证结果，确定第一 ECU 与第二 ECU 的双向身份认证结果。

[00186] 在一个实施例中，第一子信息为加密信息中位于第一预设区域范围内的子信息，第三子信息为加密信息中位于第二预设区域范围内的子信息。

[00187] 在一个实施例中，第一接收模块，具体用于将第二子信息与第三子信息进行比对得到比对结果；若比对结果为第二子信息与第三子信息一致，则确定第二认证结果为身份认证通过；若比对结果为第二子信息与第三子信息不一致，则确定第二认证结果为身份认证未通过。

[00188] 在一个实施例中，第一确定模块，具体用于若第一认证结果为身份认证通过、且第二认证结果为身份认证通过，则确定双向身份认证结果为双向身份认证通过；若第一认证结果为身份认证通过、且第二认证结果为身份认证未通过，则确定双向身份认证结果为双向身份认证未通过。

[00189] 在一个实施例中，装置 1100 还可以包括：

[00190] 第二接收模块，用于接收第二 ECU 发送的第一认证结果；若第一认证结果为身份认证未通过，则确定第二 ECU 对第一 ECU 的身份认证未通过。

[00191] 在一个实施例中，装置 1100 还可以包括：

[00192] 第二发送模块，用于向第二 ECU 发送第一身份认证请求；第一身份认证请求用于触发第二 ECU 生成第一随机数；

[00193] 第三接收模块，用于接收第二 ECU 发送的第一随机数，并将第一随机数作为初始数据。

[00194] 在一个实施例中，第二发送模块，具体用于每隔预设时长向第二 ECU 发送第一身份认证请求。

[00195] 在一个实施例中，装置 1100 还可以包括：

[00196] 第三发送模块，用于若双向身份认证结果为双向身份认证通过，则向第二 ECU 发送通信报文；通信报文包括通信数据和校验信息，校验信息根据加密信息确定，校验信息用于供第二 ECU 对通信数据进行校验。

[00197] 在一个实施例中，校验信息包括第一校验信息和/或第二校验信息，第一校验信息为第一子信息中位于第三预设区域范围内的信息，第二校验信息为第三子信息中位于第四预设区域范围的信息。

[00198] 在一个实施例中，装置 1100 还可以包括：

[00199] 第四接收模块，用于接收第二 ECU 发送的第二身份认证请求；

[00200] 第四发送模块，用于响应于第二身份认证请求生成第二随机数，并向第二 ECU 发送第二随机数，并将第二随机数作为初始数据。

[00201] 上述身份认证装置中的各个模块可全部或部分通过软件、硬件及其组合来实现。上述各模块可以硬件形式内嵌于或独立于计算机设备中的处理器中，也可以以软件形式存储于计算机设备中的存储器中，以便于处理器调用执行以上各个模块对应的操作。

[00202] 在一个实施例中，提供了一种电子控制单元，包括存储器和处理器，存储器中存储有计算机程序，该处理器执行计算机程序时实现以下步骤：

[00203] 基于预设密钥对获取的初始数据进行加密得到加密信息；

[00204] 向第二电子控制单元 ECU 发送加密信息中的第一子信息；第一子信息用于第二 ECU 对第一 ECU 进行身份认证，获得第一认证结果。

[00205] 在一个实施例中，处理器执行计算机程序时还实现以下步骤：

[00206] 接收第二 ECU 发送的第二子信息和第一认证结果，并基于第二子信息、以及加密信息中的第三子信息，对第二 ECU 进行身份认证，获得第二认证结果；

[00207] 基于第一认证结果和第二认证结果，确定第一 ECU 与第二 ECU 的双向身份认证结果。

[00208] 在一个实施例中，第一子信息为加密信息中位于第一预设区域范围内的子信息，第三子信息为加密信息中位于第二预设区域范围内的子信息。

[00209] 在一个实施例中，处理器执行计算机程序时还实现以下步骤：

[00210] 将第二子信息与第三子信息进行比对得到比对结果；

[00211] 若比对结果为第二子信息与第三子信息一致，则确定第二认证结果为身份认证通过；

[00212] 若比对结果为第二子信息与第三子信息不一致，则确定第二认证结果为身份认证未通

过。

[00213] 在一个实施例中，处理器执行计算机程序时还实现以下步骤：

[00214] 若第一认证结果为身份认证通过、且第二认证结果为身份认证通过，则确定双向身份认证结果为双向身份认证通过；

[00215] 若第一认证结果为身份认证通过、且第二认证结果为身份认证未通过，则确定双向身份认证结果为双向身份认证未通过。

[00216] 在一个实施例中，处理器执行计算机程序时还实现以下步骤：

[00217] 接收第二 ECU 发送的第一认证结果；

[00218] 若第一认证结果为身份认证未通过，则确定第二 ECU 对第一 ECU 的身份认证未通过。

[00219] 在一个实施例中，处理器执行计算机程序时还实现以下步骤：

[00220] 向第二 ECU 发送第一身份认证请求；第一身份认证请求用于触发第二 ECU 生成第一随机数；

[00221] 接收第二 ECU 发送的第一随机数，并将第一随机数作为初始数据。

[00222] 在一个实施例中，处理器执行计算机程序时还实现以下步骤：

[00223] 每隔预设时长向第二 ECU 发送第一身份认证请求。

[00224] 在一个实施例中，处理器执行计算机程序时还实现以下步骤：

[00225] 若双向身份认证结果为双向身份认证通过，则向第二 ECU 发送通信报文；通信报文包括通信数据和校验信息，校验信息根据加密信息确定，校验信息用于供第二 ECU 对通信数据进行校验。

[00226] 在一个实施例中，校验信息包括第一子信息中位于第三预设区域范围内的第一校验信息和/或第三子信息中位于第四预设区域范围的第二校验信息。

[00227] 在一个实施例中，处理器执行计算机程序时还实现以下步骤：

[00228] 接收第二 ECU 发送的第二身份认证请求；

[00229] 响应于第二身份认证请求生成第二随机数，并向第二 ECU 发送第二随机数，并将第二随机数作为初始数据。

[00230] 在一个实施例中，提供了一种计算机可读存储介质，其上存储有计算机程序，计算机程序被处理器执行时实现以下步骤：

[00231] 基于预设密钥对获取的初始数据进行加密得到加密信息；

[00232] 向第二电子控制单元 ECU 发送加密信息中的第一子信息；第一子信息用于第二 ECU 对第一 ECU 进行身份认证，获得第一认证结果。

[00233] 在一个实施例中，计算机程序被处理器执行时还实现以下步骤：

[00234] 接收第二 ECU 发送的第二子信息和第一认证结果，并基于第二子信息、以及加密信息中的第三子信息，对第二 ECU 进行身份认证，获得第二认证结果；

[00235] 基于第一认证结果和第二认证结果，确定第一ECU与第二ECU的双向身份认证结果。

[00236] 在一个实施例中，第一子信息为加密信息中位于第一预设区域范围内的子信息，第三子信息为加密信息中位于第二预设区域范围内的子信息。

[00237] 在一个实施例中，计算机程序被处理器执行时还实现以下步骤：

[00238] 将第二子信息与第三子信息进行比对得到比对结果；

[00239] 若比对结果为第二子信息与第三子信息一致，则确定第二认证结果为身份认证通过；

[00240] 若比对结果为第二子信息与第三子信息不一致，则确定第二认证结果为身份认证未通过。

[00241] 在一个实施例中，计算机程序被处理器执行时还实现以下步骤：

[00242] 若第一认证结果为身份认证通过、且第二认证结果为身份认证通过，则确定双向身份认证结果为双向身份认证通过；

[00243] 若第一认证结果为身份认证通过、且第二认证结果为身份认证未通过，则确定双向身份认证结果为双向身份认证未通过。

[00244] 在一个实施例中，计算机程序被处理器执行时还实现以下步骤：

[00245] 接收第二ECU发送的第一认证结果；

[00246] 若第一认证结果为身份认证未通过，则确定第二ECU对第一ECU的身份认证未通过。

[00247] 在一个实施例中，计算机程序被处理器执行时还实现以下步骤：

[00248] 向第二ECU发送第一身份认证请求；第一身份认证请求用于触发第二ECU生成第一随机数；

[00249] 接收第二ECU发送的第一随机数，并将第一随机数作为初始数据。

[00250] 在一个实施例中，计算机程序被处理器执行时还实现以下步骤：

[00251] 每隔预设时长向第二ECU发送第一身份认证请求。

[00252] 在一个实施例中，计算机程序被处理器执行时还实现以下步骤：

[00253] 若双向身份认证结果为双向身份认证通过，则向第二ECU发送通信报文；通信报文包括通信数据和校验信息，校验信息根据加密信息确定，校验信息用于供第二ECU对通信数据进行校验。

[00254] 在一个实施例中，校验信息包括第一校验信息和/或第二校验信息，第一校验信息为第一子信息中位于第三预设区域范围内的信息，第二校验信息为第三子信息中位于第四预设区域范围的信息。

[00255] 在一个实施例中，计算机程序被处理器执行时还实现以下步骤：

[00256] 接收第二ECU发送的第二身份认证请求；

[00257] 响应于第二身份认证请求生成第二随机数，并向第二ECU发送第二随机数，并将第二随机数作为初始数据。

[00258] 在一个实施例中，提供了一种计算机程序产品，包括计算机程序，该计算机程序被处理器执行时实现以下步骤：

[00259] 基于预设密钥对获取的初始数据进行加密得到加密信息；

[00260] 向第二电子控制单元 ECU 发送加密信息中的第一子信息；第一子信息用于第二 ECU 对第一 ECU 进行身份认证，获得第一认证结果。

[00261] 在一个实施例中，计算机程序被处理器执行时还实现以下步骤：

[00262] 接收第二 ECU 发送的第二子信息和第一认证结果，并基于第二子信息、以及加密信息中的第三子信息，对第二 ECU 进行身份认证，获得第二认证结果；

[00263] 基于第一认证结果和第二认证结果，确定第一 ECU 与第二 ECU 的双向身份认证结果。

[00264] 在一个实施例中，第一子信息为加密信息中位于第一预设区域范围内的子信息，第三子信息为加密信息中位于第二预设区域范围内的子信息。

[00265] 在一个实施例中，计算机程序被处理器执行时还实现以下步骤：

[00266] 将第二子信息与第三子信息进行比对得到比对结果；

[00267] 若比对结果为第二子信息与第三子信息一致，则确定第二认证结果为身份认证通过；

[00268] 若比对结果为第二子信息与第三子信息不一致，则确定第二认证结果为身份认证未通过。

[00269] 在一个实施例中，计算机程序被处理器执行时还实现以下步骤：

[00270] 若第一认证结果为身份认证通过、且第二认证结果为身份认证通过，则确定双向身份认证结果为双向身份认证通过；

[00271] 若第一认证结果为身份认证通过、且第二认证结果为身份认证未通过，则确定双向身份认证结果为双向身份认证未通过。

[00272]

[00273] 在一个实施例中，计算机程序被处理器执行时还实现以下步骤：

[00274] 接收第二 ECU 发送的第一认证结果；

[00275] 若第一认证结果为身份认证未通过，则确定第二 ECU 对第一 ECU 的身份认证未通过。

[00276] 在一个实施例中，计算机程序被处理器执行时还实现以下步骤：

[00277] 向第二 ECU 发送第一身份认证请求；第一身份认证请求用于触发第二 ECU 生成第一随机数；

[00278] 接收第二 ECU 发送的第一随机数，并将第一随机数作为初始数据。

[00279] 在一个实施例中，计算机程序被处理器执行时还实现以下步骤：

[00280] 每隔预设时长向第二 ECU 发送第一身份认证请求。

[00281] 在一个实施例中，计算机程序被处理器执行时还实现以下步骤：

[00282] 若双向身份认证结果为双向身份认证通过，则向第二 ECU 发送通信报文；通信报文

包括通信数据和校验信息，校验信息根据加密信息确定，校验信息用于供第二 ECU 对通信数据进行校验。

[00283] 在一个实施例中，校验信息包括第一校验信息和/或第二校验信息，第一校验信息为第一子信息中位于第三预设区域范围内的信息，第二校验信息为第三子信息中位于第四预设区域范围的信息。

[00284] 在一个实施例中，计算机程序被处理器执行时还实现以下步骤：

[00285] 接收第二 ECU 发送的第二身份认证请求；

[00286] 响应于第二身份认证请求生成第二随机数，并向第二 ECU 发送第二随机数，并将第二随机数作为初始数据。

[00287] 需要说明的是，本申请所涉及的用户信息（包括但不限于用户设备信息、用户个人信息等）和数据（包括但不限于用于分析的数据、存储的数据、展示的数据等），均为经用户授权或者经过各方充分授权的信息和数据。

[00288] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的计算机程序可存储于一非易失性计算机可读取存储介质中，该计算机程序在执行时，可包括如上述各方法的实施例的流程。其中，本申请所提供的各实施例中所使用的对存储器、数据库或其它介质的任何引用，均可包括非易失性和易失性存储器中的至少一种。非易失性存储器可包括只读存储器（Read-Only Memory，ROM）、磁带、软盘、闪存、光存储器、高密度嵌入式非易失性存储器、阻变存储器（ReRAM）、磁变存储器（Magnetoresistive Random Access Memory，MRAM）、铁电存储器（Ferroelectric Random Access Memory，FRAM）、相变存储器（Phase Change Memory，PCM）、石墨烯存储器等。易失性存储器可包括随机存取存储器（Random Access Memory，RAM）或外部高速缓冲存储器等。作为说明而非局限，RAM 可以是多种形式，比如静态随机存取存储器（Static Random Access Memory，SRAM）或动态随机存取存储器（Dynamic Random Access Memory，DRAM）等。本申请所提供的各实施例中所涉及的数据库可包括关系型数据库和非关系型数据库中至少一种。非关系型数据库可包括基于区块链的分布式数据库等，不限于此。本申请所提供的各实施例中所涉及的处理器可为通用处理器、中央处理器、图形处理器、数字信号处理器、可编程逻辑器、基于量子计算的数据处理逻辑器等，不限于此。

[00289] 以上实施例的各技术特征可以进行任意的组合，为使描述简洁，未对上述实施例中的各个技术特征所有可能的组合都进行描述，然而，只要这些技术特征的组合不存在矛盾，都应当认为是本说明书记载的范围。

[00290] 最后应说明的是：以上各实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述各实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分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脱离本申请各实施例技术方案的范围，其均应涵盖在本申请的权利要求和说明书的范围当中。尤其是，只要不存在结构冲突，各个实施例中所提到的各项技术特征均可以任意方式组合起来。本申请并不局限于文中公开的特定实施例，而是包括落入权利要求的范围内的所有技术方案。

权利要求书

1、一种身份认证方法，其中，所述方法应用于第一电子控制单元 ECU，所述方法包括：

基于预设密钥对获取的初始数据进行加密得到加密信息；

向第二电子控制单元 ECU 发送所述加密信息中的第一子信息；所述第一子信息用于所述第二 ECU 对所述第一 ECU 进行身份认证，获得第一认证结果。

2、根据权利要求 1 所述的方法，其中，所述方法还包括：

接收所述第二 ECU 发送的第二子信息和所述第一认证结果，并基于所述第二子信息、以及所述加密信息中的第三子信息，对所述第二 ECU 进行身份认证，获得第二认证结果；

基于所述第一认证结果和所述第二认证结果，确定所述第一 ECU 与所述第二 ECU 的双向身份认证结果。

3、根据权利要求 2 所述的方法，其中，所述第一子信息为所述加密信息中位于第一预设区域范围内的子信息，所述第三子信息为所述加密信息中位于第二预设区域范围内的子信息。

4、根据权利要求 2 或 3 所述的方法，其中，所述基于所述第二子信息、以及所述加密信息中的第三子信息，对所述第二 ECU 进行身份认证，获得第二认证结果，包括：

将所述第二子信息与所述第三子信息进行比对得到比对结果；

若所述比对结果为所述第二子信息与所述第三子信息一致，则确定所述第二认证结果为身份认证通过；

若所述比对结果为所述第二子信息与所述第三子信息不一致，则确定所述第二认证结果为身份认证未通过。

5、根据权利要求 2-4 任一项所述的方法，其中，所述基于所述第一认证结果和所述第二认证结果，确定所述第一 ECU 与所述第二 ECU 的双向身份认证结果，包括：

若所述第一认证结果为身份认证通过、且所述第二认证结果为身份认证通过，则确定所述双向身份认证结果为双向身份认证通过；

若所述第一认证结果为身份认证通过、且所述第二认证结果为身份认证未通过，则确定所述双向身份认证结果为双向身份认证未通过。

6、根据权利要求 1 所述的方法，其中，所述方法还包括：

接收所述第二 ECU 发送的所述第一认证结果；

若所述第一认证结果为身份认证未通过，则确定所述第二 ECU 对所述第一 ECU 的身份认证未通过。

7、根据权利要求 1-6 任一项所述的方法，其中，所述方法还包括：

向所述第二 ECU 发送第一身份认证请求；所述第一身份认证请求用于触发所述第二 ECU 生成第一随机数；

接收所述第二 ECU 发送的所述第一随机数，并将所述第一随机数作为所述初始数据。

8、根据权利要求 7 所述的方法，其中，所述向所述第二 ECU 发送第一身份认证请求，包括：

每隔预设时长向所述第二 ECU 发送所述第一身份认证请求。

9、根据权利要求 2-5 任一项所述的方法，其中，所述方法还包括：

若所述双向身份认证结果为双向身份认证通过，则向所述第二 ECU 发送通信报文；所述通信报文包括通信数据和校验信息，所述校验信息根据所述加密信息确定，所述校验信息用于供所述第二 ECU 对所述通信数据进行校验。

10、根据权利要求 9 所述的方法，其中，所述校验信息包括第一校验信息和/或第二校验信息，所述第一校验信息为所述第一子信息中位于第三预设区域范围内的信息，所述第二校验信息为所述第三子信息中位于第四预设区域范围的信息。

11、根据权利要求 1-6 任一项所述的方法，其中，所述方法还包括：

接收所述第二 ECU 发送的第二身份认证请求；

响应于所述第二身份认证请求生成第二随机数，并向所述第二 ECU 发送所述第二随机数，并将所述第二随机数作为所述初始数据。

12、一种身份认证装置，其中，所述装置设置于第一 ECU，所述装置包括：

加密模块，用于基于预设密钥对获取的初始数据进行加密得到加密信息；

发送模块，用于向第二电子控制单元 ECU 发送所述加密信息中的第一子信息；所述第一子信息用于所述第二 ECU 对所述第一 ECU 进行身份认证，获得第一认证结果。

13、一种车辆，其中，所述车辆包括第一电子控制单元 ECU 和第二 ECU；

所述第一 ECU，用于基于预设密钥对获取的初始数据进行加密得到加密信息；

所述第一 ECU，用于向所述第二 ECU 发送所述加密信息中的第一子信息；

所述第二 ECU，用于基于所述第一子信息对所述第一 ECU 进行身份认证，获得第一认证结果。

14、根据权利要求 13 所述的车辆，其中，

所述第二 ECU，还用于基于所述预设密钥对获取的初始数据进行加密得到认证信息，基于所述第一子信息和所述认证信息中的第四子信息，对所述第一 ECU 进行身份认证，并向所述第一 ECU 发送所述认证信息中的第二子信息；所述第二子信息为所述认证信息中位于第二预设区域范围内的子信息，所述第四子信息为所述认证信息中位于第一预设区域范围内的子信息；

所述第一 ECU，还用于接收所述第二 ECU 发送的所述第二子信息，并基于所述加密信息中的第三子信息、以及所述第二子信息，对所述第二 ECU 进行身份认证，获得第二认证结果。

15、一种电子控制单元，包括存储器和处理器，所述存储器存储有计算机程序，其中，所述处理器执行所述计算机程序时实现权利要求 1 至 11 中任一项所述的方法的步骤。

16、一种计算机可读存储介质，其上存储有计算机程序，其中，所述计算机程序被处理器执行时实现权利要求 1 至 11 中任一项所述的方法的步骤。

17、一种计算机程序产品，包括计算机程序，其中，该计算机程序被处理器执行时实现权利要求 1 至 11 中任一项所述的方法的步骤。

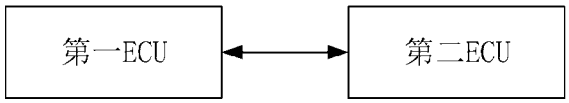

第一ECU
第二ECU

图 1

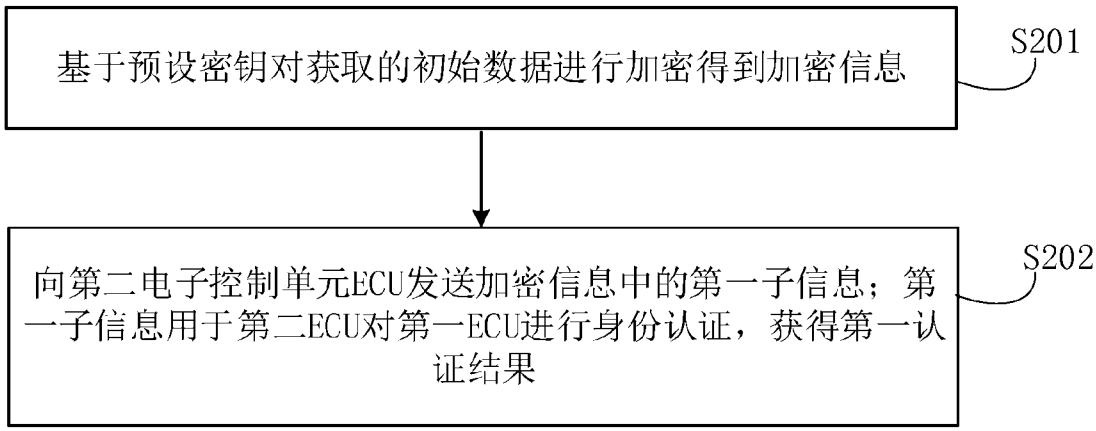

基于预设密钥对获取的初始数据进行加密得到加密信息
S201
向第二电子控制单元ECU发送加密信息中的第一子信息；第一子信息用于第二ECU对第一ECU进行身份认证，获得第一认证结果
S202

图 2

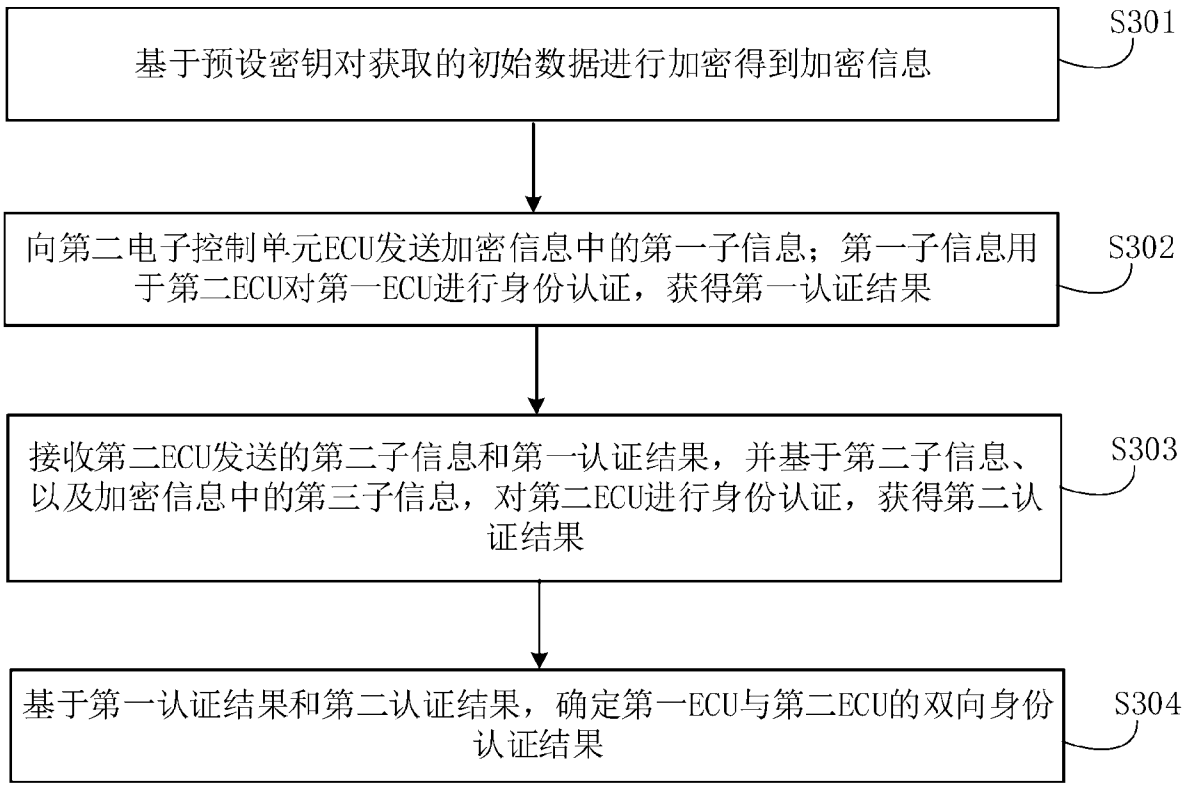

基于预设密钥对获取的初始数据进行加密得到加密信息
S301
向第二电子控制单元ECU发送加密信息中的第一子信息；第一子信息用于第二ECU对第一ECU进行身份认证，获得第一认证结果
S302
接收第二ECU发送的第二子信息和第一认证结果，并基于第二子信息、以及加密信息中的第三子信息，对第二ECU进行身份认证，获得第二认证结果
S303
基于第一认证结果和第二认证结果，确定第一ECU与第二ECU的双向身份认证结果
S304

图 3

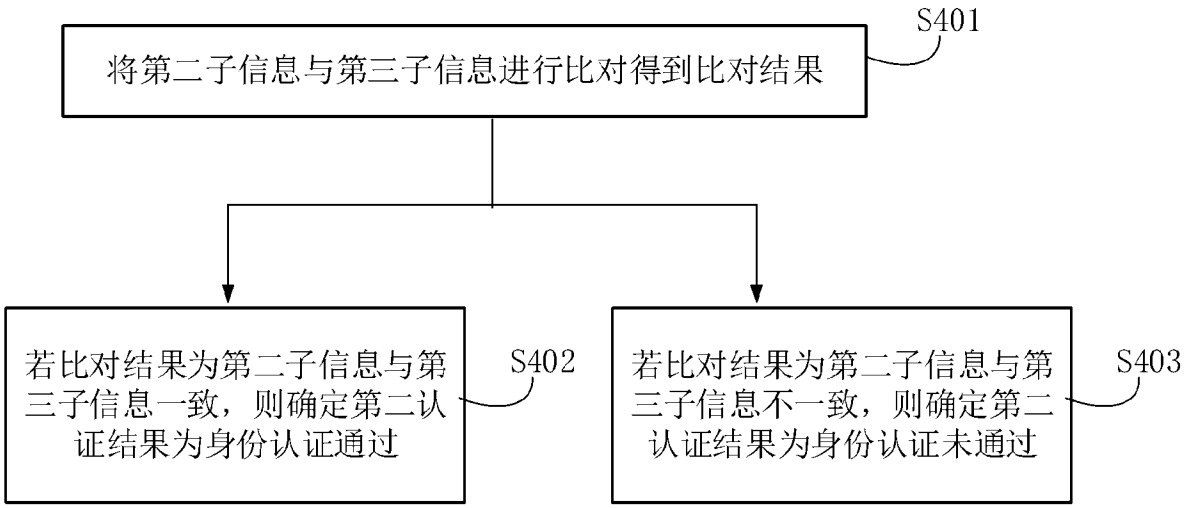

S401
将第二子信息与第三子信息进行比对得到比对结果
若比对结果为第二子信息与第三子信息一致，则确定第二认证结果为身份认证通过
S402
若比对结果为第二子信息与第三子信息不一致，则确定第二认证结果为身份认证未通过
S403

图 4

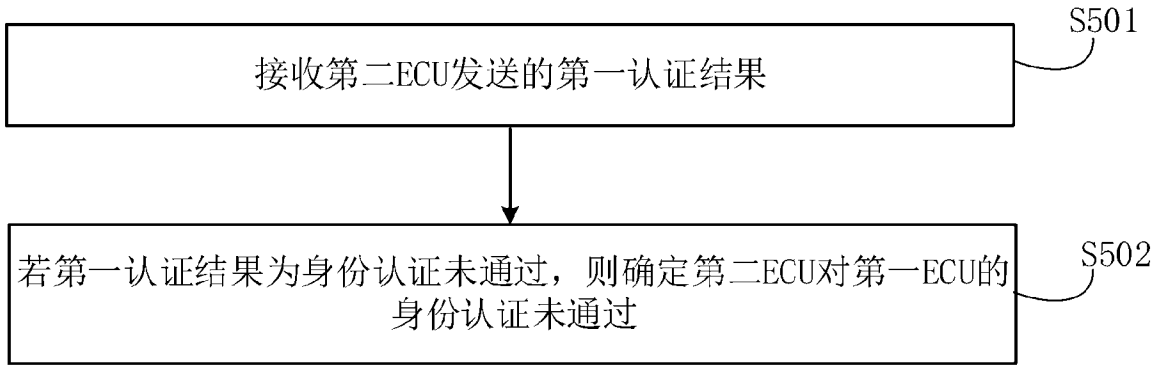

S501
接收第二ECU发送的第一认证结果
若第一认证结果为身份认证未通过，则确定第二ECU对第一ECU的身份认证未通过
S502

图 5

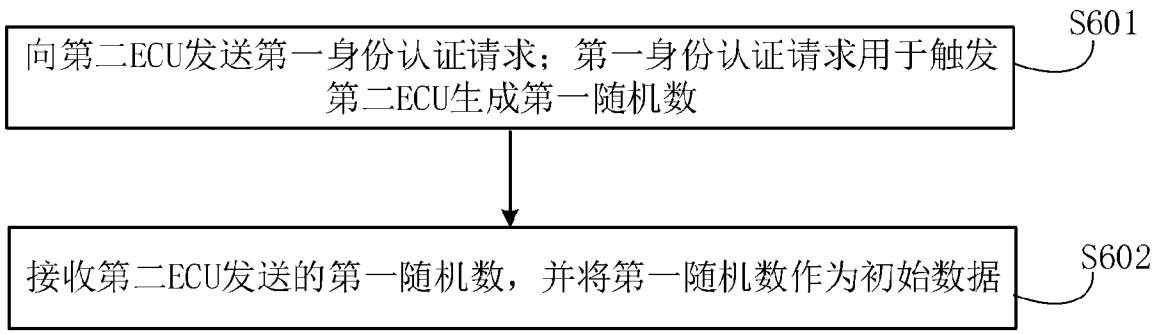

S601
向第二ECU发送第一身份认证请求；第一身份认证请求用于触发第二ECU生成第一随机数
接收第二ECU发送的第一随机数，并将第一随机数作为初始数据
S602

图 6

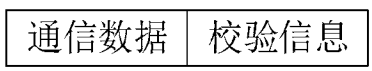

通信数据
校验信息

图 7

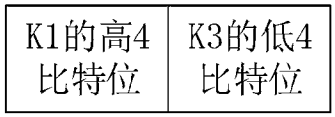

K1的高4比特位
K3的低4比特位

图 8

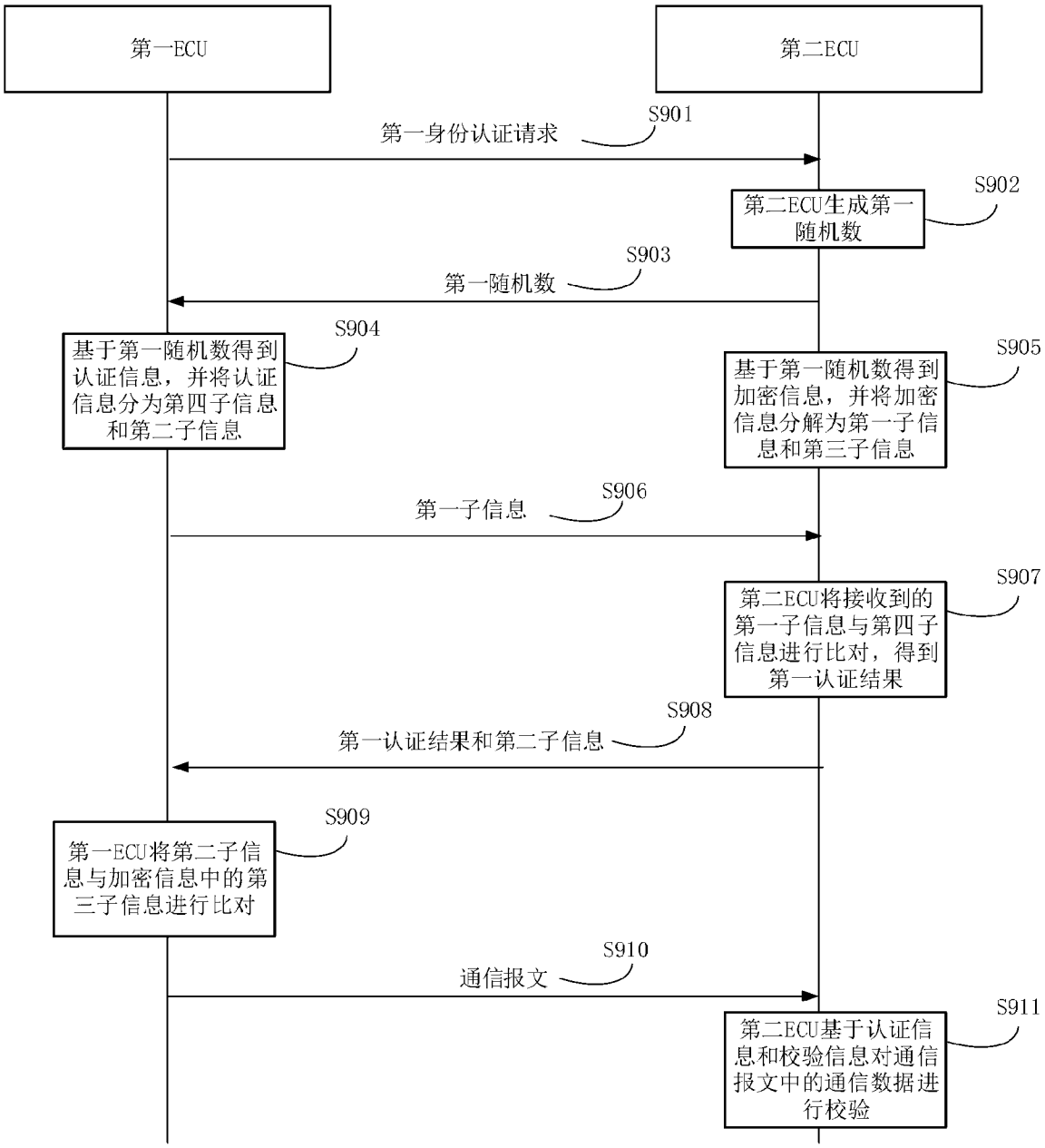

第一ECU
第二ECU
S901
第一身份认证请求
S902
第二ECU生成第一随机数
S903
第一随机数
S904
基于第一随机数得到认证信息，并将认证信息分为第四子信息和第二子信息
S905
基于第一随机数得到加密信息，并将加密信息分解为第一子信息和第三子信息
S906
第一子信息
S907
第二ECU将接收到的第一子信息与第四子信息进行比对，得到第一认证结果
S908
第一认证结果和第二子信息
S909
第一ECU将第二子信息与加密信息中的第三子信息进行比对
S910
通信报文
S911
第二ECU基于认证信息和校验信息对通信报文中的通信数据进行校验

图 9

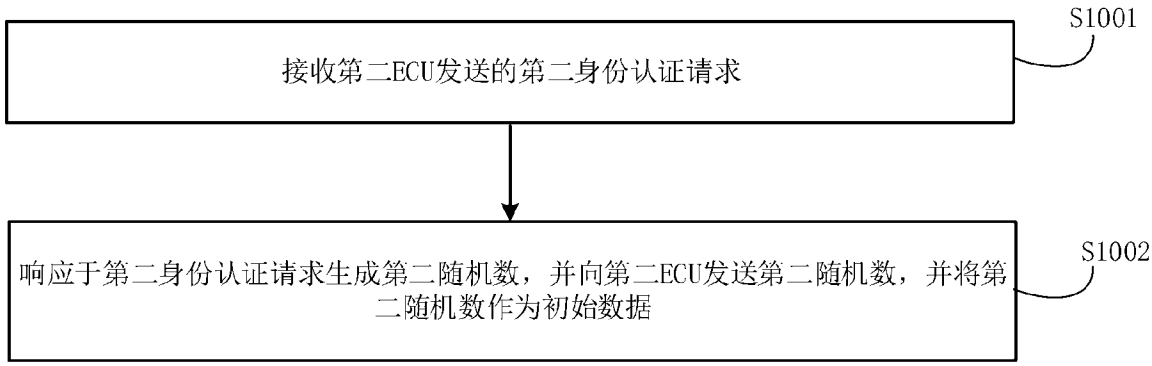

S1001
接收第二ECU发送的第二身份认证请求
响应于第二身份认证请求生成第二随机数，并向第二ECU发送第二随机数，并将第二随机数作为初始数据
S1002

图 10

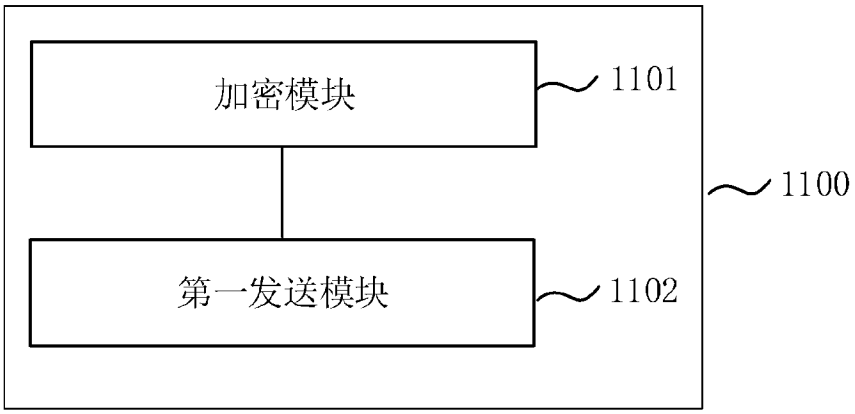


图 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2023/133558

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/40(2022.01)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)

IPC: 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)

CNTXT; ENTXT; ENTXTC; VEN; DWPI; CNKI; IEEE: 电子控制单元, ECU, 密钥, 加密, 随机数, 身份, 认证, 子信息, 部分, 比特, Electronic Control Unit, key, encryption, random number, identity, authentication, Sub-info, part, bit

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 109921908 A (BEIJING RENXINZHENG TECHNOLOGY CO., LTD.) 21 June 2019 (2019-06-21) description, paragraphs [0049]-[0087]	1-17
X	CN 111813078 A (BEIJING TOPSEC NETWORK SECURITY TECHNOLOGY CO., LTD. et al.) 23 October 2020 (2020-10-23) description, paragraphs [0036]-[0125]	1-17
A	CN 111865922 A (GUOQI (BEIJING) INTELLIGENT NETWORK UNITED AUTOMOBILE RESEARCH INSTITUTE CO., LTD.) 30 October 2020 (2020-10-30) entire document	1-17
A	CN 113132098 A (BEIHANG UNIVERSITY) 16 July 2021 (2021-07-16) entire document	1-17
A	US 2019288849 A1 (THE REGENTS OF THE UNIVERSITY OF MICHIGAN) 19 September 2019 (2019-09-19) entire document	1-17

☐ 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
"D" document cited by the applicant in the international application
"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
17 February 2024	**22 February 2024**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **China No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2023/133558

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 109921908 A	21 June 2019	None	
CN 111813078 A	23 October 2020	None	
CN 111865922 A	30 October 2020	None	
CN 113132098 A	16 July 2021	None	
US 2019288849 A1	19 September 2019	WO 2018017566 A1	25 January 2018

国际检索报告

国际申请号
PCT/CN2023/133558

A. 主题的分类

H04L 9/40(2022.01)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)

IPC：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））

CNTXT;ENTXT;ENTXTC;VEN;DWPI;CNKI;IEEE:电子控制单元，ECU，密钥，加密，随机数，身份，认证，子信息，部分，比特，Electronic Control Unit，key，encryption, random number, identity, authentication, Sub-info, part, bit

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 109921908 A (北京仁信证科技有限公司) 2019年6月21日 (2019 - 06 - 21) 说明书第[0049]-[0087]段	1-17
X	CN 111813078 A (北京天融信网络安全技术有限公司 等) 2020年10月23日 (2020 - 10 - 23) 说明书第[0036]-[0125]段	1-17
A	CN 111865922 A (国汽（北京）智能网联汽车研究院有限公司) 2020年10月30日 (2020 - 10 - 30) 全文	1-17
A	CN 113132098 A (北京航空航天大学) 2021年7月16日 (2021 - 07 - 16) 全文	1-17
A	US 2019288849 A1 (THE REGENTS OF THE UNIVERSITY OF MICHIGAN) 2019年9月19日 (2019 - 09 - 19) 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

“D” 申请人在国际申请中引证的文件

“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
2024年2月17日	2024年2月22日
ISA/CN的名称和邮寄地址 中国国家知识产权局 中国北京市海淀区蓟门桥西土城路6号 100088	受权官员 张倩 电话号码 (+86) 010-53961574

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2023/133558

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 109921908 A	2019年6月21日	无	
CN 111813078 A	2020年10月23日	无	
CN 111865922 A	2020年10月30日	无	
CN 113132098 A	2021年7月16日	无	
US 2019288849 A1	2019年9月19日	WO 2018017566 A1	2018年1月25日