(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
2021 年 11 月 18 日 (18.11.2021)

WIPO | PCT

(10) 国际公布号
WO 2021/226989 A1

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

(21) 国际申请号: PCT/CN2020/090460

(22) 国际申请日: 2020 年 5 月 15 日 (15.05.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: 华为技术有限公司 (**HUAWEI TECHNOLOGIES CO., LTD.**) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: 郭志鹏 (**GUO, Zhipeng**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 北京龙双利达知识产权代理有限公司 (**LONGSUN LEAD IP LTD.**); 中国北京市海淀区北清路68号院3号楼101, Beijing 100094 (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, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ,

WO 2021/226989 A1

(54) **Title:** COMMUNICATION METHOD AND COMMUNICATION APPARATUS

(54) 发明名称: 通信的方法和通信装置

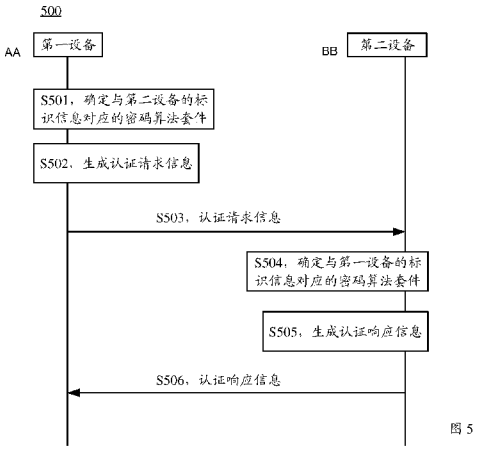

图 5

S501 Determine a cryptographic algorithm suite corresponding to identification information of the second device
S502 Generate authentication request information
S503 Authentication request information
S504 Determine a cryptographic algorithm suite corresponding to identification information of the first device
S505 Generate authentication response information
S506 Authentication response information
AA First device
BB Second device

(57) **Abstract:** Provided are a communication method and a communication apparatus. The method comprises: a second device receiving authentication request information from a first device, wherein the authentication request information comprises identification information of the first device; the second device determining, according to a first mapping relationship, a cryptographic algorithm suite corresponding to the identification information of the first device, wherein the first mapping relationship is used for indicating a correlation between identification information of at least one device and at least one cryptographic algorithm suite; the second device generating authentication response information according to the cryptographic algorithm suite; and the second device sending the authentication response information to the first device. On the basis of the present application, the transmission reliability and communication efficiency of two devices during an authentication process can be improved.

(57) 摘要: 本申请提供了一种通信的方法和通信装置。该方法包括：第二设备接收来自第一设备的认证请求信息，该认证请求信息包括该第一设备的标识信息；该第二设备根据第一映射关系确定与该第一设备的标识信息对应的密码算法套件，该第一映射关系用于指示至少一个设备的标识信息与至少一个密码算法套件之间的对应关系；该第二设备根据该密码算法套件，生成认证响应信息；该第二设备向该第一设备发送该认证响应信息。基于本申请，可以提高两个设备的认证过程的传输可靠性和通信效率。

[见续页]

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))。

通信的方法和通信装置

技术领域

本申请涉及通信领域，并且更具体地，涉及一种通信的方法和通信装置。

背景技术

目前，针对车载以太网（Ethernet，Eth）的安全通信，汽车开放系统架构（automotive open system architecture，AUTOSAR）联盟定义了传输层安全（transport layer security，TLS）协议和数据包传输层安全（datagram transport layer security，DLTS）协议。

不论是基于 TLS 协议还是基于 DTLS 协议，在两个设备的初始握手过程中，或者基于预共享密钥的握手过程中，其中一个设备要向另一个设备传递自身支持的密码算法套件列表。然而密码算法套件列表的数据量比较大，在握手过程中容易造成互联网协议（internet protocol，IP）包分片传输，从而影响传输的可靠性和通信效率。

发明内容

本申请提供一种通信的方法，可以提高设备握手过程中的传输可靠性和通信效率。

第一方面，提供了一种通信的方法，该方法包括：第二设备接收来自第一设备的认证请求信息，该认证请求信息包括该第一设备的标识信息；该第二设备根据第一映射关系确定与该第一设备的标识信息对应的密码算法套件，该第一映射关系用于指示至少一个设备的标识信息与至少一个密码算法套件之间的对应关系；该第二设备根据该密码算法套件，生成认证响应信息；该第二设备向该第一设备发送该认证响应信息。

基于上述技术方案，通过将密码算法套件与设备的标识信息对应的方式，使得第二设备可以根据保存的第一映射关系确定与第一设备通信过程中使用的密码算法套件。因此，第一设备和第二设备在握手过程中，不需要传递支持的密码算法套件列表，从而减小了握手过程中传输的数据量，提高了传输可靠性和通信效率。

结合第一方面，在第一方面的某些实现方式中，在该第二设备向该第一设备发送认证响应信息之前，该方法还包括：该第二设备确定预先配置的第二列表中包含该第一设备的标识信息，该第二列表中包括需要认证的设备的标识信息。

基于上述技术方案，通过在第二设备预先配置第二列表的方式，使得第二设备在确定第一设备的标识信息保存在第二列表的情况下，就可以确定第一设备的来源合法性，即第二列表可以代替原有握手过程中 cookie 字段分配的过程。因此，可以防止恶意设备伪造虚假来源发起认证过程，以及第二设备根据第二列表可以直接忽略不合法设备的认证请求，从而减轻第二设备的处理负担，也可以提高攻击者的攻击难度。

结合第一方面，在第一方面的某些实现方式中，该认证请求信息还包括该第一设备的第一设备证书和/或该第一设备使用的第一签名值；和/或该认证响应信息还包括该第二设备的第二设备证书和/或该第二设备使用的第二签名值。

结合第一方面，在第一方面的某些实现方式中，该认证请求信息还包括该第一设备使用的第一随机数和/或该第一设备使用的第一临时公钥；该认证响应信息还包括该第二设备使用的第二随机数和/或该第二设备使用的第二临时公钥。

结合第一方面，在第一方面的某些实现方式中，该认证请求信息还包括第一密码；和/或该认证响应信息还包括第二密码，该第二密码是该第二设备根据预存的预共享密钥和该密码算法套件生成的。

基于上述方案，第一设备和第二设备基于确定的密码算法套件和预存的预共享密钥可以生成密码来代替设备证书。由于密码的长度远小于设备证书，因此大大减小了握手交互过程中的交互数据量，提高了握手效率和可靠性。

此外，使用密码代替设备证书之后，设备不再需要对设备证书中的根签名进行验签，而是变成了对密码进行对称加密解密运算。而对称加密解密运算速度远远高于验签速度，因此可以提高握手效率。

结合第一方面，在第一方面的某些实现方式中，该认证请求信息还包括该第一设备使用的第一临时公钥；该认证响应信息还包括该第二设备使用的第二临时公钥和该第二设备的标识信息。

结合第一方面，在第一方面的某些实现方式中，该至少一个密码算法套件中的每个密码算法套件满足前向安全性需求。

结合第一方面，在第一方面的某些实现方式中，该方法还包括：该第二设备确定与该第一设备通信使用的报文加密模式，该报文加密模式包括全加密模式和按需加密模式中的一个。

基于上述技术方案，通过定义通信报文的按需加密模式，使得在按需加密模式下，对不需要加密的数据可以明文传输，从而减少了加密载荷的数据量，提高了加密速率，从而提高了通信效率。

结合第一方面，在第一方面的某些实现方式中，该第二设备确定与该第一设备通信使用的报文加密模式，包括：该第二设备根据第二映射关系确定与该第一设备的标识信息对应的该报文加密模式，该第二映射关系用于指示至少一个设备的标识信息与至少一个报文加密模式之间的对应关系。

结合第一方面，在第一方面的某些实现方式中，在该报文加密模式是按需加密模式的情况下时，该方法还包括：该第二设备生成通信报文，该通信报文包括以下字段：明文标识、明文数据、密文标识、密文数据。

结合第一方面，在第一方面的某些实现方式中，该明文数据中包含该密文数据的流加密密钥生成种子。

现有的应用于用户数据报协议的握手过程中，无法使用流加密算法。而基于上述技术方案，在按需加密模式下，可以在明文数据中保存密文数据的流加密密钥生成种子，从而使得用户数据报协议可以支持流加密算法。

第二方面，提供了一种通信的方法，该方法包括：第一设备根据第三映射关系确定与第二设备的标识信息对应的密码算法套件，该第三映射关系用于指示至少一个设备的标识信息与至少一个密码算法套件之间的对应关系；该第一设备根据该密码算法套件生成认证请求信息，该认证请求信息包括该第一设备的标识信息；该第一设备向该第二设备发送该

认证请求信息；该第一设备接收来自该第二设备的认证响应信息。

基于上述技术方案，通过将密码算法套件与设备的标识信息对应的方式，使得第一设备可以根据保存的第三映射关系确定与第二设备通信过程中使用的密码算法套件。因此，第一设备和第二设备在握手过程中，不需要传递支持的密码算法套件列表，从而减小了握手过程中传输的数据量，提高了传输可靠性和通信效率。

结合第二方面，在第二方面的某些实现方式中，在该第一设备向该第二设备发送该认证请求信息之前，该方法还包括：该第一设备确定预先配置的第一列表中包含该第二设备的标识信息，该第一列表中包括需要认证的设备的标识信息。

基于上述技术方案，通过在第一设备预先配置第一列表的方式，使得第一设备在确定第二设备的标识信息保存在第二列表的情况下，就可以确定第二设备的来源合法性。

结合第二方面，在第二方面的某些实现方式中，该认证请求信息还包括该第一设备的设备证书和/或该第一设备使用的第一签名值；和/或该认证响应信息还包括该第二设备的第二设备证书和/或该第二设备使用的第二签名值。

结合第二方面，在第二方面的某些实现方式中，该认证请求信息还包括第一密码，该第一密码是该第一设备根据预存的预共享密钥和该密码算法套件生成的；和/或该认证响应信息还包括第二密码。

基于上述方案，第一设备和第二设备基于确定的密码算法套件和预存的预共享密钥可以生成密码来代替设备证书。由于密码的长度远小于设备证书，因此大大减小了握手交互过程中的交互数据量，提高了握手效率和可靠性。

此外，使用密码代替设备证书之后，设备不再需要对设备证书中的根签名进行验签，而是变成了对密码进行对称加密解密运算。而对称加密解密运算速度远远高于验签速度，因此可以提高握手效率。

结合第二方面，在第二方面的某些实现方式中，该认证请求信息还包括该第一设备使用的第一临时公钥；该认证响应信息还包括该第二设备使用的第二临时公钥和该第二设备的标识信息。

结合第二方面，在第二方面的某些实现方式中，其特征在于，该认证请求信息还包括该第一设备使用的第一随机数和/或该第一设备使用的第一临时公钥；该认证响应信息还包括该第二设备使用的第二随机数和/或该第二设备使用的第二临时公钥。

结合第二方面，在第二方面的某些实现方式中，该至少一个密码算法套件中的每个密码算法套件满足前向安全性需求。

结合第二方面，在第二方面的某些实现方式中，该方法还包括：该第一设备确定与该第二设备通信使用的报文加密模式，该报文加密模式包括全加密模式和按需加密模式中的一个。

基于上述技术方案，通过定义通信报文的按需加密模式，使得在按需加密模式下，对不需要加密的数据可以明文传输，从而减少了加密载荷的数据量，提高了加密速率，从而提高了通信效率。

结合第二方面，在第二方面的某些实现方式中，该第一设备确定与该第二设备通信使用的报文加密模式，包括：该第一设备根据第四映射关系确定与该第二设备的标识信息对应的该报文加密模式，该第四映射关系用于指示至少一个设备的标识信息与至少一个报文

加密模式之间的对应关系。

结合第二方面，在第二方面的某些实现方式中，在该报文加密模式是按需加密模式的情况下，该方法还包括：该第一设备生成通信报文，该通信报文包括以下字段：明文标识、明文数据、密文标识、密文数据。

结合第二方面，在第二方面的某些实现方式中，该明文数据中包含该密文数据的流加密密钥生成种子。

现有的应用于用户数据报协议的握手过程中，无法使用流加密算法。而基于上述技术方案，在按需加密模式下，可以在明文数据中保存密文数据的流加密密钥生成种子，从而使得用户数据报协议可以支持流加密算法。

第三方面，提供一种通信装置，该通信装置包括收发单元和处理单元：该收发单元用于接收来自第一设备的认证请求信息，该认证请求信息包括该第一设备的标识信息；该处理单元用于根据第一映射关系确定与该第一设备的标识信息对应的密码算法套件，该第一映射关系用于指示至少一个设备的标识信息与至少一个密码算法套件之间的对应关系；该处理单元还用于根据该密码算法套件，生成认证响应信息；该收发单元还用于向该第一设备发送该认证响应信息。

结合第三方面，在第三方面的某些实现方式中，该处理单元还用于确定预先配置的第二列表中包含该第一设备的标识信息，该第二列表中包括需要认证的设备的标识信息。

结合第三方面，在第三方面的某些实现方式中，该认证请求信息还包括该第一设备的第一设备证书和/或该第一设备使用的第一签名值；和/或该认证响应信息还包括该通信装置的第二设备证书和/或该通信装置使用的第二签名值。

结合第三方面，在第三方面的某些实现方式中，该认证请求信息还包括第一密码；和/或该认证响应信息还包括第二密码，该第二密码是该处理单元根据预存的预共享密钥和该密码算法套件生成的。

结合第三方面，在第三方面的某些实现方式中，该认证请求信息还包括该第一设备使用的第一随机数和/或该第一设备使用的第一临时公钥；该认证响应信息还包括该通信装置使用的第二随机数和/或该通信装置使用的第二临时公钥。

结合第三方面，在第三方面的某些实现方式中，该认证请求信息还包括该第一设备使用的第一临时公钥；该认证响应信息还包括该通信装置使用的第二临时公钥和该通信装置的标识信息。

结合第三方面，在第三方面的某些实现方式中，该至少一个密码算法套件中的每个密码算法套件满足前向安全性需求。

结合第三方面，在第三方面的某些实现方式中，该处理单元还用于确定与该第一设备通信使用的报文加密模式，该报文加密模式包括全加密模式和按需加密模式中的一个。

结合第三方面，在第三方面的某些实现方式中，该处理单元具体用于根据第二映射关系确定与该第一设备的标识信息对应的该报文加密模式，该第二映射关系用于指示至少一个设备的标识信息与至少一个报文加密模式之间的对应关系。

结合第三方面，在第三方面的某些实现方式中，在该报文加密模式是按需加密模式的情况下时，该处理单元还用于生成通信报文，该通信报文包括以下字段：明文标识、明文数据、密文标识、密文数据。

结合第三方面，在第三方面的某些实现方式中，该明文数据中包含该密文数据的流加密密钥生成种子。

第四方面，提供了一种通信装置，该通信装置包括收发单元和处理单元：该处理单元用于根据第三映射关系确定与第二设备的标识信息对应的密码算法套件，该第三映射关系用于指示至少一个设备的标识信息与至少一个密码算法套件之间的对应关系；该处理单元还用于根据该密码算法套件生成认证请求信息，该认证请求信息包括该通信装置的标识信息；该收发单元用于向该第二设备发送该认证请求信息；该收发单元还用于接收来自该第二设备的认证响应信息。

结合第四方面，在第四方面的某些实现方式中，该处理单元还用于确定预先配置的第一列表中包含该第二设备的标识信息，该第一列表中包括需要认证的设备的标识信息。

结合第四方面，在第四方面的某些实现方式中，该认证请求信息还包括该通信装置的设备证书和/或该通信装置使用的第一签名值；和/或该认证响应信息还包括该第二设备的第二设备证书和/或该第二设备使用的第二签名值。

结合第四方面，在第四方面的某些实现方式中，该认证请求信息还包括第一密码，该第一密码是该通信装置根据预存的预共享密钥和该密码算法套件生成的；和/或该认证响应信息还包括第二密码。

结合第四方面，在第四方面的某些实现方式中，该认证请求信息还包括该通信装置使用的第一随机数和/或该通信装置使用的第一临时公钥；该认证响应信息还包括该第二设备使用的第二随机数和/或该第二设备使用的第二临时公钥。

结合第四方面，在第四方面的某些实现方式中，该认证请求信息还包括该通信装置使用的第一临时公钥；该认证响应信息还包括该第二设备使用的第二临时公钥和该第二设备的标识信息。

结合第四方面，在第四方面的某些实现方式中，该至少一个密码算法套件中的每个密码算法套件满足前向安全性需求。

结合第四方面，在第四方面的某些实现方式中，该处理单元还用于确定与该第二设备通信使用的报文加密模式，该报文加密模式包括全加密模式和按需加密模式中的一个。

结合第四方面，在第四方面的某些实现方式中，该处理单元具体用于根据第四映射关系确定与该第二设备的标识信息对应的该报文加密模式，该第四映射关系用于指示至少一个设备的标识信息与至少一个报文加密模式之间的对应关系。

结合第四方面，在第四方面的某些实现方式中，在该报文加密模式是按需加密模式的情况下，该处理单元还用于生成通信报文，该通信报文包括以下字段：明文标识、明文数据、密文标识、密文数据。

结合第四方面，在第四方面的某些实现方式中，该明文数据中包含该密文数据的流加密密钥生成种子。

第五方面，提供了一种通信装置，包括处理器。该处理器与存储器耦合，可用于执行存储器中的指令，以实现上述第一方面至第二方面或第一方面至第二方面中任一种可能实现方式中的方法。

第六方面，提供了一种处理器，包括：输入电路、输出电路和处理电路。处理电路用于通过输入电路接收信号，并通过输出电路发射信号，使得处理器执行上述第一方面至第

二方面或第一方面至第二方面中任一种可能实现方式中的方法。

在具体实现过程中，上述处理器可以为芯片，输入电路可以为输入管脚，输出电路可以为输出管脚，处理电路可以为晶体管、门电路、触发器和各种逻辑电路等。输入电路所接收的输入的信号可以是由例如但不限于接收器接收并输入的，输出电路所输出的信号可以是例如但不限于输出给发射器并由发射器发射的，且输入电路和输出电路可以是同一电路，该电路在不同的时刻分别用作输入电路和输出电路。本申请实施例对处理器及各种电路的具体实现方式不做限定。

第七方面，提供了一种处理装置，包括处理器。还可以包括存储器，存储器用于存储指令，该处理器用于读取存储器中存储的指令，并可通过接收器接收信号，通过发射器发射信号，以执行上述第一方面至第二方面或第一方面至第二方面中任一种可能实现方式中的方法。

可选地，处理器为一个或多个，存储器为一个或多个。

可选地，存储器可以与处理器集成在一起，或者存储器与处理器分离设置。

在具体实现过程中，存储器可以为非瞬时性（non-transitory）存储器，例如只读存储器（read only memory，ROM），其可以与处理器集成在同一块芯片上，也可以分别设置在不同的芯片上，本申请实施例对存储器的类型和存储器与处理器的设置方式不做限定。

应理解，相关的数据交互过程例如发送指示信息可以为从处理器输出指示信息的过程，接收能力信息可以为处理器接收输入能力信息的过程。具体地，处理输出的数据可以输出给发射器，处理器接收的输入数据可以来自接收器。其中，发射器和接收器可以统称为收发器。

上述第七方面中的处理装置可以是一个芯片，该处理器可以通过硬件来实现也可以通过软件来实现，当通过硬件实现时，该处理器可以是逻辑电路、集成电路等；当通过软件来实现时，该处理器可以是一个通用处理器，通过读取存储器中存储的软件代码来实现，该存储器可以集成在处理器中，可以位于该处理器之外，独立存在。

第八方面，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（也可以称为代码，或指令），当计算机程序被运行时，使得计算机执行上述第一方面至第二方面或第一方面至第二方面中任一种可能实现方式中的方法。

第九方面，提供了一种计算机可读存储介质，计算机可读存储介质存储有计算机程序（也可以称为代码，或指令）当其在计算机上运行时，使得计算机执行上述第一方面至第二方面或第一方面至第二方面中任一种可能实现方式中的方法。

第十方面，提供了一种通信系统，包括前述第三方面或第三方面中任一种可能实现方式中的通信装置，和/或，前述第四方面或第四方面中任一种可能实现方式中的通信装置。

附图说明

图 1 是 TLS 协议的示意性流程图。

图 2 是基于预共享密钥的握手过程的示意性流程图。

图 3 和图 4 是适用于本申请实施例提供的方法的通信系统的示意图。

图 5 至图 7 是本申请实施例提供的通信的方法的示意性流程图。

图 8 是本申请实施例提供的按需加密模式下的通信报文的格式示意图。

图 9 是本申请实施例提供的全加密模式下的通信报文的格式示意图。

图 10 至图 12 是本申请实施例提供的通信的方法的示意性流程图。

图 13 和图 14 是本申请实施例提供的通信装置的示意性框图。

具体实施方式

下面将结合附图，对本申请中的技术方案进行描述。

目前，针对车载以太网的安全通信，AUTOSAR 联盟定义了 TLS 协议和 DLTS 协议。AUTOSAR 中定义的 TLS 协议和 DTLS 协议与传统以太网协议中定义的 TLS 协议和 DTLS 协议相同，即 AUTOSAR 定义的 TLS 协议和 DTLS 协议是 TLS 协议和 DTLS 协议在车载以太网上的移植。

图 1 中示出了 TLS 协议的流程。如图 1 所示，TLS 协议包含握手过程和通信过程。车内部件#1 中预置根证书、私钥（secret key，SK）#1 和设备证书#1，设备证书#1 中包括车内部件#1 的标识（identity，ID）#1、公钥（public key，PK）#1 和根签名。车内部件#2 中预置根证书、SK#2 和设备证书#2，设备证书#2 中包括车内部件#2 的 ID#2、PK#2 和根签名。

其中握手过程例如可以包括以下步骤:

S101，车内部件#1 生成随时数（random）#1。

S102，车内部件#1 向车内部件#2 发送连接请求（ClientHello）#1。连接请求#1 中包括随机数#1 和车内部件#1 支持的密码算法套件列表。

S103，车内部件#2 生成一个 cookie 字段。

S104，车内部件#2 向车内部件#1 发送验证请求（HelloVerifyRequest）。验证请求中包括 cookie 字段。

S105，车内部件#1 向车内部件#2 发送连接请求#2。连接请求#2 中包括随机数#1、车内部件#1 支持的密码算法套件列表和 cookie 字段。

S106，车内部件#2 生成随机数#2。

S107，车内部件#2 根据车内部件#1 支持的密码算法套件列表选择支持的密码算法套件。

S108，车内部件#2 根据选择的密码算法套件生成临时公私钥对#2。临时公私钥对#2 包括临时私钥(temporary secret key，tempSK)#2 和临时公钥(temporary public key，tempPK) #2。

S109，车内部件#2 计算签名（Sign）#2。Sign#2=Sign（ID#2||random#2||tempPK#2）。

S110，车内部件#2 向车内部件#1 发送连接响应（ServerHello）。连接响应中包括设备证书#2、随机数#2、tempPK#2 和 Sign#2。

S111，车内部件#1 验证设备证书#2 的合法性。

S112，车内部件#1 验证 Sign#2 的合法性。

S113，车内部件#1 生成临时公私钥对#1。临时公私钥对#1 包括 tempSK#1 和 tempPK#1。

S114，车内部件#1 计算 Sign#1。Sign#1=Sign（ID#1||random#1||tempPK#1）

S115，车内部件#1 向车内部件#2 发送改变密码标准（ChangeCipherSpec）。改变密码标准中包括设备证书#1、tempPK#1 和 Sign#1。

S116，车内部件#1 根据密钥派生函数（key derivation function，KDF）计算预共享密钥（pre-shared key，PSK）#1。PSK#1=KDF（ID#1，ID#2，tempSK#1，tempPK#2）。

S117，车内部件#1 根据 KDF 计算会话密钥（SessionKey）#1。SessionKey#1=KDF（PSK#1，random#1，random#2）。

S118，车内部件#2 验证设备证书#1 的合法性。

S119，车内部件#2 验证 Sign #1 的合法性。

S120，车内部件#2 根据 KDF 计算 PSK#2。PSK#2=KDF（ID#1，ID#2，tempSK#2，tempPK#1）。

S121，车内部件#2 根据 KDF 计算 SessionKey#2。SessionKey#2=KDF（PSK#2，random#1，random#2）。

如上所述，车内部件#1 和车内部件#2 通过握手过程完成双方的身份合法性认证、密码算法套件协商和 SessionKey 协商等步骤。进一步地，在通信过程中：

S122，车内部件#1 和车内部件#2 使用 SessionKey 对通信报文进行加密传输。

如果通信双方之前进行过握手过程，保存有相同的 PSK，那么握手过程可以简化。基于 PSK 的握手过程如图 2 所示。

S201，车内部件#1 生成随时数（random）#1。

S202，车内部件#1 向车内部件#2 发送连接请求#3。连接请求#3 中包括随机数#1、车内部件#1 支持的密码算法套件列表和 PSK_ID。

S203，车内部件#2 生成随机数#2。

S204，车内部件#2 根据车内部件#1 支持的密码算法套件列表选择支持的密码算法套件，根据 PSK_ID 选择 PSK。

S205，车内部件#2 根据选择的密码算法套件生成临时公私钥对#2。临时公私钥对包括 tempSK#2 和 tempPK#2。

S206，车内部件#2 使用 PSK 加密报文。

S207，车内部件#2 向车内部件#1 发送加密的连接响应。连接响应中包括随机数#2 和 tempPK#2。

S208，车内部件#1 解密报文得到随机数#2。

S209，车内部件#1 生成临时公私钥对#1。临时公私钥对#1 包括 tempSK#1 和 tempPK#1。

S210，车内部件#1 使用 PSK 加密报文。

S211，车内部件#1 向车内部件#2 发送加密的改变密码标准。改变密码标准中包括 tempPK#1。

S212，车内部件#1 计算预共享密钥（pre-shared key，PSK）#1。PSK#1=KDF（ID#1，ID#2，tempSK#1，tempPK#2）。

S213，车内部件#1 根据 KDF SessionKey#1。SessionKey#1=KDF（PSK#1，random#1，random#2）。

S214，车内部件#2 根据 KDF 计算 PSK#2。PSK#2=KDF（ID#1，ID#2，tempSK#2，tempPK#1）。

S215，车内部件#2 根据 KDF 计算 SessionKey#2。SessionKey#2=KDF（PSK#2，random#1，random#2）。

S216，车内部件#1 和车内部件#2 使用 SessionKey 对通信报文进行加密传输。

如上所述，基于 PSK 的握手过程无需对设备证书进行合法性验证，因此提高了握手的效率。

然而不论是初始握手过程还是基于 PSK 的握手过程，在密码算法套件协商环节传递的密码算法套件列表的数据量比较大，以及在初始握手过程的身份合法性认证环节传递的证书数据量比较大，因此，在握手过程中容易造成互联网协议（internet protocol，IP）包分片传输，从而影响传输的可靠性和通信效率。

此外，在车内网的场景下，不同车内部件之间传输大量的数据会增加车内转发部件的负担；现有的密码算法套件与车内部件的硬件能力不兼容，因此部署难度大，实时性差；基于传输控制协议（transmission control protocol，TCP），不同车内部件之间需要建立连接，因此在车内上电时大量车内部件建立连接容易造成总线拥堵或中心节点负载过重；TLS 协议无法应用于用户数据报协议（user datagram protocol，UDP）；以及，不同车内部件之间的安全通道建立后，传输的所有数据都要加密，然而车内存在很多无需加密，只需要保证完整性的数据传输（例如，车辆控制指令），因此，对所有数据都加密会造成运算资源浪费，同时会话密钥使用次数过多会增大攻击风险。

DTLS 协议是为了适应 UDP 协议而对 TLS 协议进行改动得到的。由于 UDP 协议是不可靠的，报文有可能丢失和乱序。为了处理这些情况，DTLS 协议在 TLS 协议的基础上做了如下改动:

（1）DTLS 增加了报文超时重传机制，用来处理报文丢失的问题;

（2）DTLS 报文中保存一个不加密的序号值，用来处理报文乱序的问题;

（3）DTLS 移除了流加密算法的支持，也就是说，DTLS 支持的密码算法套件是 TLS 支持的密码算法套件的子集。

除了上述不同之外，DTLS 协议的流程与 TLS 协议的流程相同。

由于 DTLS 协议用于 UDP 协议，存在丢包的可能，因此，在握手过程中传输数据量较大的密码算法套件列表和设备证书，对传输可靠性和通信效率的不利影响会更大。

此外，在车内网场景下，不同车内部件之间传输大量的数据会增加车内转发部件的负担；现有的密码算法套件与车内部件的硬件能力不兼容，因此部署难度大，实时性差；在追求高实时性的车内通信中，流加密算法是常用的高效加密手段，然而 DTLS 协议并不支持流加密算法；以及，不同车内部件之间的安全通道建立后，传输的所有数据都要加密，然而车内存在很多无需加密，只需要保证完整性的数据传输（例如，车辆控制指令），因此，对所有数据都加密会造成运算资源浪费，同时会话密钥使用次数过多会增大攻击风险。

基于此，本申请实施例提供一种通信的方法，以期减少握手过程中的交互过程和通信数据量，从而提高传输效率和通信质量。

图 3 是适用于本申请实施例的通信方法的通信系统的示意图。如图 3 所示，本申请实施例提供的方法可以应用于智能网联车的车内部件之间通过车载以太网进行安全通信的场景。例如，图 3 所示的电子控制单元（electronic control unit，ECU）#1 与 ECU#2 之间通过车载以太网进行通信。

车内部件可以包括与外界通信的远程信息处理器如车联网终端盒子（telematics box，T-Box）、网关（gateway，GW）、高级驾驶辅助系统（advanced driver assistance system，

ADAS）、人机界面（human-machine interface，HMI）、整车控制器（vehicle control unit，VCU）等。

如图 3 所示，两个车内部件之间可以直接连接。或者，两个车内部件之间还可以通过其它车内部件转接，如图 4 所示，ECU#1 和 ECU#2 之间通过 GW 连接。

下面结合附图对本本申请实施例提供的方法进行说明。

图 5 示出了本申请实施例提供的通信的方法的示意性流程图。图 5 所示的方法 500 可以应用于图 3 或图 4 所示的通信系统中，图 5 所示的第一设备可以是图 3 或图 4 中的 ECU#1，第二设备可以是图 3 或图 4 中的 ECU#2。如图 5 所示，该方法 500 可以包括 S501 至 S506，下面详细描述各个步骤。

S501，第一设备根据第三映射关系确定与第二设备的标识信息对应的密码算法套件。

可以理解，与第二设备的标识信息对应的密码算法套件，即第一设备与第二设备之间进行通信所使用的密码算法套件。

其中，第一设备或第二设备可以是 T-Box、GW、ADAS、HMI、或 VCU 等。

其中，第三映射关系用于指示至少一个设备的标识信息与至少一个密码算法套件之间的对应关系。至少一个设备的标识信息可以是第一设备需要认证的设备的标识信息。也就是说，第一设备根据第三映射关系可以确定与需要认证的设备进行通信所使用的密码算法套件。可以理解的，至少一个设备的标识信息包括第二设备的标识信息。

可选地，若第一设备根据第三映射关系可以确定出与第二设备的标识信息对应的密码算法套件，则第一设备可以默认第二设备是需要认证的设备，即可以确定第二设备的真实性。

设备的标识信息可以包括以下一种或多种：设备的类型、设备的标识（identifier，ID）、设备的网际协议（internet protocol，IP）地址、设备的媒体访问控制（media access control，MAC）地址。

本申请实施例对至少一个设备的标识信息与至少一个密码算法套件的对应关系不做限定。

作为一个示例，至少一个设备的标识信息与至少一个密码算法套件之间可能存在一一对应的对应关系。表 1 示出了至少一个设备的标识信息与至少一个密码算法套件之间一一对应的示例。

表 1

设备的标识信息	密码算法套件
设备#A	密码算法套件#A
设备#B	密码算法套件#B
设备#C	密码算法套件#C
设备#D	密码算法套件#D

根据表 1，第一设备可以确定与设备#A 的标识信息对应的是密码算法套件#A，与设备#B 的标识信息对应的是密码算法套件#B，与设备#C 的标识信息对应的是密码算法套件#C，与设备#D 的标识信息对应的是密码算法套件#D。

作为另一示例，至少一个设备的标识信息与至少一个密码算法套件之间可能存在多对一的对应关系。表 2 示出了至少一个设备的标识信息与至少一个密码算法套件之间多对一

的示例。

表 2

设备的标识信息	密码算法套件
设备#A	密码算法套件#A
设备#B	
设备#C	
设备#D	密码算法套件#B

根据表 2，第一设备可以确定与设备#A 的标识信息、设备#B 的标识信息和设备#C 的标识信息对应的都是密码算法套件#A，与设备#D 的标识信息对应的是密码算法套件#B。

第三映射关系所指示的至少一个设备的标识信息和至少一个密码算法套件之间的对应关系，可以根据第一设备与至少一个设备的硬件能力确定。例如，如果第一设备和设备#A 都具有电子安全车辆入侵防护应用（E-safety vehicle intrusion protected application，EVITA）full 级的硬件安全模块（hardware security module，HSM），则可以将第一设备与该设备#A 进行安全通信使用的密码算法套件确定为 ECDHE_ECDSA_AES_128_GCM_Whirlpool。也就是说，可以将设备#A 的标识信息与 ECDHE_ECDSA_AES_128_GCM_Whirlpool 对应起来。其中，临时椭圆曲线 Diffie-Hellman（ephemeral elliptic curve Diffie-Hellman，ECDHE）代表密钥协商算法，椭圆曲线数字签名算法（elliptic curve digital signature algorithm，ECDSA）代表数字签名算法，高级加密标准（advanced encryption standard，AES）_128_（galois/counter mode，GCM）代表认证加密算法，Whirlpool 算法为哈希算法，这些算法都是 EVITA full 级的 HSM 中规定的算法。

第三映射关系可以是预先存储在第一设备中的。例如，第三映射关系可以是设备生产商在生成第一设备的时候预先存储在第一设备中的；或者，第三映射关系可以是用户在使用第一设备之前预先存储在第一设备中的；或者，第三映射关系还可以是软件提供商预先存储在第一设备中的。

在本申请实施例中，通过将密码算法套件与设备的标识信息对应的方式，使得第一设备够可以根据保存的第三映射关系确定与第二设备通信所使用的密码算法套件，因此，第一设备不需要向第二设备传输自身支持的密码算法套件列表，从而减小了传输的数据量。

可选地，至少一个密码算法套件中的每个密码算法套件都满足前向安全性需求。也就是说，在定义第一设备与至少一个其它设备进行通信使用的密码算法套件时，只使用满足前向安全性需求的密钥协商算法，例如，使用临时 Diffie-Hellman（ephemeral Diffie-Hellman，DHE）或 ECDHE。

S502，第一设备根据确定的密码算法套件生成认证请求信息。

第一设备根据确定的密码算法套件生成认证请求信息可以理解为，第一设备根据确定密码算法套件生成认证请求信息中包括的参数。

认证请求信息中包括第一设备的标识信息（下文中以 ID#1 为例进行说明）。认证请求信息还可以包括以下参数中的一种或多种：第一设备使用的第一临时公钥（下文中以 tempPK#1 为例进行说明）、第一设备使用的第一随机数（random）（下文中以 random#1 为例进行说明）、第一设备的设备证书（下文中以设备证书#1 为例进行说明）、第一设备使用的第一签名值（下文中以 Sign#1 为例进行说明）、第一密码（下文中以 cipher#1

为例进行说明）。其中，random#1 和 tempPK#1 用于生成第一设备与第二设备之间通信使用的会话密钥，设备证书#1、Sign#1 和 cipher#1 用于对第一设备的合法性进行验证。

其中，设备证书#1 中包括 ID#1、第一设备使用的第一公钥（下文中以 PK#1 为例进行说明）和根签名。可以理解，由于设备证书#1 中包括 ID#1，因此，认证请求信息中可以不包括第一设备的标识信息，在此情况下，可以理解为，第一设备的标识信息包含在设备证书#1 中。

tempPK#1 是第一设备根据确定的密码算法套件生成的。第一设备根据密码算法套件中的密钥协商算法生成第一临时公私钥对，第一临时公私钥对中包括 tempPK#1 和第一临时私钥（下文中以 tempSK#1 为例进行说明）两个数据。

Sign#1 是第一设备根据确定的密码算法套件生成的。第一设备构造第一消息（下文中以 msg#1 为例进行说明），msg#1 的内容为{ID#1‖random#1‖tempPK#1}；进一步地，第一设备以使用的第一私钥（下文中以 SK#1 为例进行说明）为密钥，根据密码算法套件中规定的数字签名算法对 msg#1 加密得到 Sign#1，Sign#1=Sign（ID#1‖random#1‖tempPK#1），“‖”表示连接，Sign（）表示用数字签名算法进行计算。

cipher#1 是第一设备根据预存的 PSK 和密码算法套件生成的。其中，预存的 PSK 与第二设备对应。

第一设备构造 msg#1，msg#1 的内容为{ID#1‖random#1}；进一步地，第一设备以 PSK 为密钥，根据密码算法套件中的对称加密算法对 msg#1 进行加密，生成 cipher#1，cipher#1=Enc_{PSK}（ID#1‖random#1）。其中，“‖”表示连接，Enc_{PSK}（）表示以 PSK 为密钥，以对称加密算法加密。

预存的 PSK 可以是第一设备在与第二设备在先进行身份认证的过程中生成的。

可以理解，若第一设备与第二设备之前进行过身份认证过程，则第一设备和第二设备可以保存有相同的 PSK。第一设备可以根据第二设备的标识信息（下文中以 ID#2 为例进行说明）从保存的一个或多个 PSK 中确定与第二设备对应的 PSK。

预存的 PSK 还可以是第一设备根据预先配置的第一 PSK 列表中保存的 PSK。预先配置的第一 PSK 列表中可以包括至少一个设备的标识信息对应的 PSK。预先配置的第一 PSK 列表可以理解为第一 PSK 列表是预先存储在第一设备中的。例如，第一 PSK 列表可以是设备生产商在生成第一设备的时候预先存储在第一设备中的；或者，第一 PSK 列表可以是用户在使用第一设备之前预先存储在第一设备中的；或者，第一 PSK 列表还可以是软件提供商预先存储在第一设备中的。

在此情况下，第一设备可以根据预先配置的第一 PSK 列表确定与 ID#2 对应的 PSK。

可选地，如图 6 所示，该方法 500 还可以包括：S507，第一设备确定预先配置的第一列表中包含第二设备的标识信息。预先配置的第一列表可以理解为第一列表是预先存储在第一设备中的。例如，第一列表可以是设备生产商在生成第一设备的时候预先存储在第一设备中的；或者，第一列表可以是用户在使用第一设备之前预先存储在第一设备中的；或者，第一列表还可以是软件提供商预先存储在第一设备中的。

需要说明的是，图中仅以 S507 在 S502 之后为例进行说明，不应对本申请构成限定，S507 还可以在 S502 或者在 S501 之前执行。或者，S507 与 S501 可以是一个步骤。

其中，第一列表中定义了第一设备需要和哪些设备进行安全通信的认证过程，也就是

说，第一列表中包括第一设备需要认证的设备的标识信息。

第一列表的内容可以根据第一设备的应用场景确定。例如，第一设备是 ADAS，则在自动驾驶业务功能中，ADAS 需要和 HMI、VCU、车身域控制器、底盘域控制器、传感器等设备进行安全通信，因此 ADAS 中预先配置的第一列表中可以保存上述设备的标识信息。

在第一设备生成或发送认证请求信息之前，第一设备可以查询预先配置的第一列表中是否保存有第二设备的标识信息。

若第一列表保存有第二设备的标识信息，则表示第一设备需要对第二设备进行身份认证，则第一设备向第二设备发起认证过程。例如，第一设备在确定第一列表中包含第二设备的标识信息的情况下，再生成认证请求信息，或向第二设备发送认证请求信息。

若第一列表中没有保存第二设备的标识信息，则表示第一设备和第二设备之间无需进行身份认证，则第一设备不会向第二设备发起认证过程。例如，第一设备在确定第一列表中不包含第二设备的标识信息的情况下，不生成认证请求信息，或不向第二设备发送认证请求信息。

还需要说明的是，上述第一设备确定第一列表中包含第二设备的标识信息的方案也可以单独实施，即，可以作为独立的实施例，而不必依附于本说明书中的其他实施例。

在本申请实施例中，通过在第一设备预置第一列表的而方式，使得第一设备在确定第二设备的标识信息保存在第一列表的情况下，再向第二设备发送认证请求信息，从而可以避免发起不必要认证请求。

可选地，如图 7 所示，该方法 500 还可以包括：S509，第一设备确定与第二设备通信使用的报文加密模式。

需要说明的是，图中仅以 S509 在 S507 之后为例进行说明，不应对本申请构成限定。S509 还可以在 S507 之前执行，或者可以在 S502 之前执行，或者可以在 S501 之前执行，或者 S509 还可以在 S503 之后执行。或者，S509 与 S507 可以是一个步骤，者 S509 与 S501 可以是一个步骤。

其中，报文加密模式包括全加密模式和按需加密模式中的一个。

若第一设备与第二设备通信使用的报文加密模式是全加密模式，则第一设备与第二设备之间发送的通信报文可以包括：密文数据。

密文数据即第一设备与第二设备根据密码算法套件对通信数据进行加密得到的数据。

图 8 示出了全加密模式下的通信报文格式。如图 8 所示，在全加密模式下，只有报文序号不加密，其他所有数据均为密文数据。

若第一设备与第二设备通信使用的报文加密模式是按需加密模式，则第一设备与第二设备之间发送的通信报文包括：明文标识、明文数据、密文标识、密文数据。

其中，明文标识用于标识明文数据的长度，或者用于指示明文标识之后的字段是明文数据。明文数据即没有加密的数据。

可选地，明文数据中可以包含密文数据的流加密密钥生成种子。

图 9 示出了在按需加密模式下，第一设备与第二设备之间发送的通信报文的格式。从图 9 可以看出，明文标识之后，密文标识之前的数据是明文数据，密文标识之后的数据是密文数据。其中，明文数据可以包括：报文序号、流密钥种子、娱乐数据、车辆控制指令、

哈希值等。密文数据可以包括：定位数据、地图数据、用户隐私等。

本申请实施例对第一设备确定报文加密模式的方式不做限定。

作为一个示例，第一设备可以根据与第二设备之间传输的数据内容确定报文加密模式。例如，若第一设备与第二设备之间传输的是地图数据、定位数据等，则确定报文加密模式为全加密模式。若第一设备与第二设备之间除了传输地图数据等数据，还传输娱乐数据、控制指令等，则确定报文加密模式为按需加密模式，即对地图数据等数据加密，对娱乐数据、控制指令等不加密。

进一步地，第一设备可以向第二设备发送指示信息，指示与第二设备之间通信所使用的报文加密模式。例如，第一设备发送的指示信息可以是布尔型（bool）变量，若布尔型变量的值是“1”，则指示第一设备与第二设备之间通信使用的报文加密模式是全加密模式；若布尔型变量的值是“0”，则指示第一设备与第二设备之间通信使用的报文加密模式是按需加密模式。可选的，该指示信息还可以携带在认证请求信息中。

作为另一个示例，第一设备可以根据第四映射关系确定与第二设备的标识信息对应的报文加密模式，第四映射关系用于指示至少一个设备的标识信息与至少一个报文加密模式之间的对应关系。

本申请实施例对至少一个设备的标识信息与至少一个报文加密模式的对应关系不做限定。

例如，至少一个设备的标识信息与至少一个报文加密模式之间可能存在一一对应的对应关系。表 3 示出了至少一个设备的标识信息与至少一个报文加密模式之间一一对应的示例。

表 3

设备的标识信息	报文加密模式
设备#A	全加密模式
设备#B	全加密模式
设备#C	按需加密模式
设备#D	按需加密模式

根据表 3，第一设备可以确定与设备#A 和设备#B 的标识信息对应的是全加密模式，与设备#C 和设备#D 的标识信息对应的是按需加密模式。

又例如，至少一个设备的标识信息与至少一个报文加密模式之间可能存在多对一的对应关系。表 4 示出了至少一个设备的标识信息与至少一个报文加密模式之间多对一的示例。

根据表 4，第一设备可以确定与设备#A 的标识信息和设备#B 的标识信息对应的都是全加密模式，与设备#C 的标识信息和设备#D 的标识信息对应的是按需加密模式。

表 4

设备的标识信息	报文加密模式
设备#A	全加密模式
设备#B	
设备#C	按需加密模式
设备#D	

还需要说明的是，上述第一设备确定与第二设备通信使用的报文加密模式的方案也可以单独实施，即，可以作为独立的实施例，而不必依附于本说明书中的其他实施例。

在本申请实施例中，通过定义通信报文的按需加密模式，使得在按需加密模式下，对不需要加密的数据可以明文传输，从而减少了加密载荷的数据量，提高了加密速率，从而提高了通信效率。在按需加密模式下，可以在明文数据中保存密文数据的流加密密钥生成种子，从而可以在 UDP 协议上支持流加密算法，进一步提高通信效率。

应理解，上文中以第一设备分别保存了第三映射关系、第一列表、第一 PSK 列表和第四映射关系为例进行说明，不应对本申请实施例构成限定。

第三映射关系指示的信息、第四映射关系指示的信息、第一 PSK 列表包含的内容和第一列表包含的内容可以保存在同一个列表中；或者，第三映射关系指示的信息、第四映射关系指示信息、第一 PSK 列表包含的内容和第一列表包含的内容中的一个或多个可以保存在同一个列表中。

表 5 示出了第三映射关系指示的信息、第四映射关系指示的信息、第一 PSK 列表包含的内容和第一列表包含的内容保存在同一个列表中的示例。

表 5

设备的标识信息	密码算法套件	PSK	报文加密模式
设备#A	密码算法套件#1	PSK#1	全加密模式
设备#B	密码算法套件#2	PSK#2	全加密模式
设备#C	密码算法套件#3	PSK#3	按需加密模式
设备#D	密码算法套件#4	PSK#4	按需加密模式

其中，设备#A 至设备#D 的标识信息即第一设备需要认证的设备的标识信息；以及表 5 中示出了与设备#A 至设备#D 的标识信息分别对应的密码算法套件#1 至密码算法套件#4、PSK#1 至 PSK#4、报文加密模式。

S503，第一设备向第二设备发送认证请求信息。相对应地，在 S503 中，第二设备接收来自第一设备的认证请求信息。

认证请求信息中可以包括以下参数中的一种或多种：ID#1、tempPK#1、random#1、设备证书#1、Sign#1、cipher#1。

例如，在第一设备与第二设备单向认证的场景下，认证请求信息中可以包括：ID#1、tempPK#1 和 random#1。

第一设备和第二设备之间进行单向认证，即第一设备对第二设备的合法性进行认证，第二设备不对第一设备的合法性进行认证。例如，在自动驾驶场景中，假设第一设备是智能驾驶域控制器，第二设备是传感器，则智能驾驶域控制器与域内传感器进行通信之前，智能驾驶域控制器为防止传感器发送伪造数据，需要对传感器进行认证，而传感器无需对智能驾驶域控制器进行认证。

又例如，在第一设备与第二设备进行双向认证的情况下，认证请求信息中可以包括：设备证书#1、Sign#1、tempPK#1 和 random#1。

第一设备与第二设备进行双向认证，即第一设备对第二设备的合法性进行认证，第二设备也对第一设备的合法性进行认证。

再例如，在第一设备预存与第二设备对应的 PSK 的情况下，认证响应信息可以包括：

ID#1、cipher#1 和 tempPK#1。

S504，第二设备根据第一映射关系确定与第一设备的标识信息对应的密码算法套件。

可以理解，与第一设备的标识信息对应的密码算法套件，即第一设备与第二设备之间进行通信所使用的密码算法套件。

其中，第一映射关系用于指示至少一个设备的标识信息与至少一个密码算法套件之间的对应关系。具体地，关于第一映射关系的描述可以参考 S501 中关于第三映射关系的描述，为例简洁，本申请实施例不再详述。

可以理解的，步骤 S504 中确定的密码算法套件与步骤 S501 中确定的密码算法套件相同。

第一映射关系可以是预先存储在第二设备中的。例如，第一映射关系可以是设备生产商在生成第二设备的时候预先存储在第二设备中的；或者，第一映射关系可以是用户在使用第二设备之前预先存储在第二设备中的；或者，第一映射关系还可以是软件提供商预先存储在第二设备中的。

可选地，若第二设备根据第一映射关系可以确定出与第一设备的标识信息对应的密码算法套件，则第二设备可以默认第一设备是需要认证的设备，即可以确定第一设备的真实性。

在本申请实施例中，通过将密码算法套件与设备的标识信息对应的方式，使得第二设备可以根据保存的第一映射关系确定与第一设备通信过程中使用的密码算法套件。因此，第一设备不需要向第二设备传输自身支持的密码算法套件，从而减小了传输过程中的数据量，提高了传输可靠性和通信效率。

可选地，至少一个密码算法套件中的每个密码算法套件都满足前向安全性需求。

如前文所述，在第一设备与第二设备之间进行双向认证的情况下，第一设备向第二设备发送的认证请求信息可以包括设备证书#1 和/或 Sign#1。则第二设备在确定密码算法套件之前，可以先对设备证书#1 的合法性进行验证。

第二设备使用根证书中的第二设备使用的第二公钥（下文中以 PK#2 为例进行说明）对设备证书#1 中保存的根签名进行验签。验证通过之后，第二设备再确定密码算法套件。

在确定密码算法套件之后，第二设备继续对 Sign#1 的合法性进行验证。第二设备可以根据设备证书#1 中包括的 ID#1 和认证请求信息中包括的 random#1 和 tempPK#1 构造 msg#1，进一步地，第二设备根据设备证书#1 中包括的 PK#1 对 Sign#1 的合法性进行验证。验证通过之后，第二设备执行后续的认证过程。

若认证请求信息中包括 cipher#2，则第二设备确定密码算法套件之后，以预存的与第一设备的标识信息对应的 PSK 为密钥，以及根据密码算法套件中的对称加密算法解密 cipher#1 得到 ID#1。进一步地，第二设备判断解密 cipher#1 得到的 ID#1 与认证请求信息中的 ID#1 是否一致。如果不一致，则认证失败，如果一致，则继续执行后续的认证过程。

S505，第二设备根据确定的密码算法套件生成认证响应信息。

认证响应信息可以包括以下参数中的一个或多个：

第二设备的标识信息（下文中以 ID#2 为例进行说明）、第二设备使用的第二随机数（下文中 random#2 为例进行说明）、第二设备的第二设备证书（下文中以设备证书#2 为例进行说明）、第二设备使用的第二签名值（下文中以 Sign#1 为例进行说明）、第二设

备使用的第二临时公钥(下文中以 tempPK#2 为例进行说明)、第二密码(下文中以 cipher#2 为例进行说明)。其中,设备证书#2 中包括 ID#2、PK#2 和根签名。random#2 和 tempPK#2 用于生成第一设备与第二设备之间通信使用的会话密钥,设备证书#2、Sign#2 和 cipher#2 用于对第二设备的合法性进行验证。

第二设备可以根据确定的密码算法套件生成认证响应信息,也可以理解为,第二设备生成认证响应信息中包括的参数。

第二设备可以根据确定的密码算法套件生成第二临时公私钥对,第二临时公私钥对中包括 tempPK#2 和第二临时私钥(下文中以 tempSK#2 为例进行说明)两个数据。

第二设备还可以构造第二消息(下文中以 msg#2 为例进行说明),msg#2 的内容为{ID#2‖random#2‖tempPK#2};进一步地,第二设备以使用的第二私钥(下文中以 SK#2 为例进行说明)为密钥,根据密码算法套件中规定的数字签名算法对 msg#2 加密得到 Sign#2,Sign#2=Sign(ID#2‖random#2‖tempPK#2),“‖”表示连接,Sign()表示用数字签名算法进行计算。

第二设备还可以根据预存的 PSK 和密码算法套件生成 cipher#2。第二设备构造 msg#2,msg#2 的内容为{ID#2‖random#2};进一步地,第二设备以 PSK 为密钥,根据密码算法套件中的对称加密算法对 msg#2 进行加密,生成 cipher#2,cipher#2=Enc_{PSK}(ID#2‖random#2)。其中,“‖”表示连接,Enc_{PSK}()表示以 PSK 为密钥,以对称加密算法加密。

预存的 PSK 可以是第一设备在与第二设备在先进行身份认证的过程中生成的。

可以理解,若第一设备与第二设备之前进行过身份认证过程,则第一设备和第二设备保存有相同的 PSK。第二设备可以根据 ID#1 从保存的一个或多个 PSK 中确定与第一设备对应的 PSK。

预存的 PSK 还可以是第二设备根据预先配置的第二 PSK 列表中保存的 PSK。预先配置的第二 PSK 列表中可以包括至少一个设备的标识信息对应的 PSK。预先配置的第二 PSK 列表可以理解为第二 PSK 列表是预先存储在第二设备中的。例如,第一 PSK 列表可以是设备生产商在生成第二设备的时候预先存储在第二设备中的;或者,第二 PSK 列表可以是用户在使用第二设备之前预先存储在第二设备中的;或者,第二 PSK 列表还可以是软件提供商预先存储在第二设备中的。

在此情况下,第二设备可以根据预先配置的第二 PSK 列表确定与 ID#1 对应的 PSK。

若第二设备在确定与第一设备的标识信息对应的密码算法套件之后,仍然不确定第一设备的合法性,则第二设备可以暂时不生成上述参数。

在此情况下,第二设备可以生成一个 cookie 字段,并将生成的 cookie 字段携带在认证响应信息中发送给第一设备。进一步地,第二设备可以在接收到第一设备发送的携带 cookie 字段的认证请求信息之后,根据认证请求信息中的 cookie 字段确定第一设备的真实性和来源合法性。

可选地,如图 6 所示,该方法 500 还可以包括:S508,第二设备确定预先配置的第二列表中包含第一设备的标识信息。预先配置的第二列表可以理解为第二列表是预先存储在第二设备中的。例如,第二列表可以是设备生产商在生成第二设备的时候预先存储在第二设备中的;或者,第二列表可以是用户在使用第二设备之前预先存储在第一设备中的;或者,第二列表还可以是软件提供商预先存储在第二设备中的。

需要说明的是，图中仅以 S508 在 S505 之后为例进行说明，不应对本申请构成限定，S508 还可以在 S505 或者在 S504 之前执行。或者，S508 与 S504 可以是一个步骤。

其中，第二列表中定义了第二设备需要和哪些设备进行安全通信的认证过程，也就是说，第二列表中包括第二设备需要认证的设备的标识信息。具体地，关于第二列表的描述可以参考前文 S507 中关于第一列表的描述，为了简洁，本申请实施例不再详述。

在第二设备生成或发送认证响应信息之前，第二设备可以查询预先配置的第二列表中是否保存有第一设备的标识信息。

若第二列表保存有第一设备的标识信息，则表示第一设备的来源合法，则第二设备响应第一设备的认证请求。例如，第二设备在确定第二列表中包含第一设备的标识信息的情况下，再生成认证响应信息，或向第二设备发送认证响应信息。

若第二列表中没有保存第一设备的标识信息，则表示第一设备的来源不合法，则第二设备不响应第一设备的认证请求。例如，第二设备在确定第二列表中不包含第一设备的标识信息的情况下，不生成认证响应信息，或不向第二设备发送认证响应信息。

还需要说明的是，上述第二设备确定第二列表中包含第一设备的标识信息的方案也可以单独实施，即，可以作为独立的实施例，而不必依附于本说明书中的其他实施例。

在本申请实施例中，通过在第二设备预先配置第二列表的方式，使得第二设备在确定第一设备的标识信息保存在第二列表的情况下，就可以确定第一设备的来源合法性，即第二列表可以代替原有握手过程中 cookie 字段分配的过程。因此，可以防止恶意设备伪造虚假来源发起认证过程，以及第二设备根据第二列表可以直接忽略不合法设备的认证请求，从而减轻第二设备的处理负担，也可以提高攻击者的攻击难度。

可选地，如图 7 所示，该方法 500 还可以包括：S510，第二设备确定与第一设备通信使用的报文加密模式。

需要说明的是，图中仅以 S510 在 S508 之后为例进行说明，不应对本申请构成限定。S510 还可以在 S508 之前执行，或者可以在 S505 之前执行，或者可以在 S504 之前执行，或者 S510 还可以在 S506 之后执行。或者，S510 与 S508 可以是一个步骤，者 S509 与 S504 可以是一个步骤。

其中，报文加密模式包括全加密模式和按需加密模式中的一个。

若第一设备与第二设备通信使用的报文加密模式是全加密模式，则第一设备与第二设备之间发送的通信报文可以包括：密文数据。

密文数据即第一设备与第二设备根据密码算法套件对通信数据进行加密得到的数据。

图 8 示出了全加密模式下的通信报文格式。如图 8 所示，在全加密模式下，只有报文序号不加密，其他所有数据均为密文数据。

若第一设备与第二设备通信使用的报文加密模式是按需加密模式，则第一设备与第二设备之间发送的通信报文包括：明文标识、明文数据、密文标识、密文数据。

其中，明文标识用于标识明文数据的长度，或者用于指示明文标识之后的字段是明文数据。明文数据即没有加密的数据。

可选地，明文数据中可以包含密文数据的流加密密钥生成种子。

图 9 示出了在按需加密模式下的通信报文的格式。从图 9 可以看出，明文标识之后，密文标识之前的数据是明文数据，密文标识之后的数据是密文数据。其中，明文数据可以

包括：报文序号、流密钥种子、娱乐数据、车辆控制指令、哈希值等。密文数据可以包括：定位数据、地图数据、用户隐私等。

本申请实施例对第二设备确定报文加密模式的方式不做限定。

作为一个示例，第二设备可以根据来自第一设备的指示信息确定报文加密模式，该指示信息用于指示第一设备与第二设备之间通信所使用的报文加密模式。例如，第二设备接收的来自第一设备的指示信息可以是布尔型（bool）变量，若布尔型变量的值是“1”，则指示第一设备与第二设备之间通信使用的报文加密模式是全加密模式；若布尔型变量的值是“0”，则指示第一设备与第二设备之间通信使用的报文加密模式是按需加密模式。

作为另一个示例，第二设备可以根据第二映射关系确定与第一设备的标识信息对应的报文加密模式，第二映射关系用于指示至少一个设备的标识信息与至少一个报文加密模式之间的对应关系。具体地，关于第二映射关系的描述可以参考前文 S509 中关于第四映射关系的描述，为了简洁，本申请实施例不再详述。

还需要说明的是，上述第二设备确定与第一设备通信使用的报文加密模式的方案也可以单独实施，即，可以作为独立的实施例，而不必依附于本说明书中的其他实施例。

在本申请实施例中，通过定义通信报文的按需加密模式，使得在按需加密模式下，对不需要加密的数据可以明文传输，从而减少了加密载荷的数据量，提高了加密速率，从而提高了通信效率。在按需加密模式下，可以在明文数据中保存密文数据的流加密密钥生成种子，从而可以在 UDP 协议上支持流加密算法，进一步提高通信效率。

应理解，上文中以第二设备分别保存了第一映射关系、第二列表、第二 PSK 列表和第二映射关系为例进行说明，不应对本申请实施例构成限定。

第一映射关系指示的信息、第二映射关系指示的信息、第二 PSK 列表包含的内容和第二列表包含的内容可以保存在同一个列表中；或者，第一映射关系指示的信息、第二映射关系指示信息、第二 PSK 列表包含的内容和第二列表包含的内容中的一个或多个可以保存在同一个列表中。

表 6 示出了第一映射关系指示的信息、第二映射关系指示的信息、第二 PSK 列表包含的内容和第二列表包含的内容保存在同一个列表中的示例。

表 6

设备的标识信息	密码算法套件	PSK	报文加密模式
设备#E	密码算法套件#1	PSK#1	全加密模式
设备#F	密码算法套件#2	PSK#2	全加密模式
设备#G	密码算法套件#3	PSK#3	按需加密模式
设备#H	密码算法套件#4	PSK#4	按需加密模式

其中，设备#E 至设备#H 的标识信息即第二设备需要认证的设备的标识信息；以及表 6 中示出了与设备#E 至设备#H 的标识信息分别对应的密码算法套件#1 至密码算法套件#4、PSK#1 至 PSK#4、报文加密模式。

S506，第二设备向第一设备发送认证响应信息。

认证响应信息可以包括以下参数中的一个或多个：random#2、设备证书#2、Sign#1、tempPK#2、cipher#2、ID#2。

例如，在第二设备确定第一设备来源合法的情况下，认证响应信息可以包括：

random#2、设备证书#2、Sign#1、tempPK#2。

又例如，第二设备预存与第一设备对应的 PSK 的情况下，认证响应信息可以包括：ID#2、tempPK#2、cipher#2。

相应地，在 S506 中，第一设备接收到来自第二设备的认证响应信息之后，可以对第二设备的合法性进行验证。

若认证响应信息中包括设备证书#2，则第一设备验证设备证书#2 的合法性。第一设备根据设备证书#2 中保存的 ID#2 查询与预先配置的第一列表，确认第二设备是否为需要认证的设备。如果不是，则终止认证；如果是，则第一设备使用根证书中的 PK#1 对设备证书#2 中的根签名进行验签。

若认证响应信息中包括 Sign#2，则第一设备继续验证 Sign#2。第一设备可以根据设备证书#2 中包括的 ID#2 和认证响应信息中包括的 random#2 和 tempPK#2 构造 msg#2，进一步地，第二设备根据设备证书#2 中包括的 PK#2 对 Sign#2 的合法性进行验证。

若认证响应信息中包括 cipher#2，则第一设备以预存的与第二设备对应的 PSK 为密钥，以及根据密码算法套件中的对称加密算法解密 cipher#2 得到 ID#2。进一步地，第一设备判断解密 cipher#2 得到的 ID#2 与认证响应信息中的 ID#2 是否一致，如果不一致，则认证失败，如果一致，则认证成功。

在第一设备与第二设备执行完身份认证流程以及交互了双方使用的随机数和临时公钥之后，则按照现有的流程计算本次安全通信使用的 PSK 和会话密钥。随后进行通信过程。

在本申请实施例中，通过将密码算法套件与设备的标识信息对应的方式，使得第一设备和第二设备可以根据保存的映射关系确定通信过程中使用的密码算法套件。因此，第一设备和第二设备在握手过程中，不需要传递支持的密码算法套件列表，从而减小了握手过程中传输的数据量，提高了传输可靠性和通信效率。在第一设备与第二设备通过转发部件通信的情况下，还可以减轻转发部件的负担。

在本申请实施例中，通过在第二设备预先配置第二列表的方式，使得第二设备在确定第一设备的标识信息保存在第二列表的情况下，就可以确定第一设备的来源合法性，即第二列表可以代替原有握手过程中 cookie 字段分配的过程。因此，可以防止恶意设备伪造虚假来源发起认证过程，以及第二设备根据第二列表可以直接忽略不合法设备的认证请求，从而减轻第二设备的处理负担，也可以提高攻击者的攻击难度。

在本申请实施例中，定义了通信报文的按需加密模式，在按需加密模式下，对不需要加密的数据可以明文传输，从而减少了加密载荷的数据量，提高了加密速率，从而提高了通信效率。

此外，在按需加密模式下，可以在明文数据中保存密文数据的流加密密钥生成种子，从而可以在 UDP 协议上支持流加密算法，进一步提高通信效率。

图 10 是本申请另一实施例提供的方法 600 的示意性流程图，如图 10 所示，该方法 600 可以包括 S601 至 S620，下面详细说明各个步骤。

S601，第一设备确定预先配置的第一列表中包含第二设备的标识信息（ID#2）。

其中，第一列表包括第一设备需要认证的设备的标识信息。

若第一设备确定第一列表中包含 ID#2，则第一设备继续执行认证过程；若第一设备

确定第一列表中没有包含 ID#2，则第一设备不执行与第二设备的认证过程。

S602，第一设备确定与 ID#2 对应的密码算法套件和报文加密模式。

第一设备可以根据第三映射关系确定与 ID#2 对应的密码算法套件。第一设备可以根据第四映射关系确定与 ID#2 对应的报文加密模式。

S603，第一设备生成随机数#1。

S604，第一设备根据密码算法套件中的密钥协商算法生成第一临时公私钥对。

第一临时公私钥对中包括 tempPK#1 和 tempSK#1。

S605，第一设备根据密码算法套件中的数字签名算法生成第一签名值。

第一设备构造 msg#1，msg#1 的内容为{ID#1‖random#1‖tempPK#1}；进一步地，第一设备以 SK#1 为密钥，根据密码算法套件中规定的数字签名算法对 msg#1 加密得到 Sign#1，Sign#1=Sign（ID#1‖random#1‖tempPK#1），“‖”表示连接，Sign（）表示用数字签名算法进行计算。

S606，第一设备向第二设备发送认证请求信息。

认证请求信息中包括：设备证书#1、random#1、tempPK#1 和 Sign#1。设备证书#1 中包括：ID#1、PK#1 和根签名。

S607，第二设备验证设备证书#1 的合法性。

第二设备根据设备证书#1 中的 ID#1，确定预先配置的第二列表中保存 ID#1。若第二列表中保存 ID#1，则第二设备确定第一设备是需要认证的设备；若第二列表中没有保存 ID#1，则第二设备确定第一设备是不需要认证的设备，进而终止认证过程。

在第二设备确定第一设备是需要认证的设备的情况下，第二设备继续使用 PK#2 对设备证书#1 中根签名进行验证。若验证成功，则继续执行验证过程；若验证失败，则终止验证过程。

S608，第二设备确定与 ID#1 对应的密码算法套件和报文加密模式。

第二设备可以根据第一映射关系确定与 ID#1 对应的密码算法套件。第一设备可以根据第二映射关系确定与 ID#1 对应的报文加密模式。

S609，第二设备验证第一签名值。

第二设备可以根据设备证书#1 中包括的 ID#1 和认证请求信息中包括的 random#1 和 tempPK#1 构造 msg#1，进一步地，第二设备根据设备证书#1 中包括的 PK#1 对 Sign#1 的合法性进行验证。验证通过之后，第二设备执行后续的认证过程。验证不通过，则验证失败。

S610，第二设备生成随机数#2。

S611，第二设备根据密码算法套件中的密钥协商算法生成第二临时公私钥对。

第二临时公私钥对中包括 tempPK#2 和 tempSK#2。

S612，第二设备根据密码算法套件中的数字签名算法计算第二签名值。

第二设备构造 msg#2，msg#2 的内容为{ID#2‖random#2‖tempPK#2}；进一步地，第一设备以 SK#2 为密钥，根据密码算法套件中规定的数字签名算法对 msg#2 加密得到 Sign#2，Sign#2=Sign（ID#2‖random#2‖tempPK#2），“‖”表示连接，Sign（）表示用数字签名算法进行计算。

S613，第二设备向第一设备发送认证响应信息。

认证响应信息中包括：设备证书#2、random#2、tempPK#2、Sign#2。设备证书#2 中包括：ID#2、PK#2 和根签名。

S614，第二设备计算 PSK#2。

PSK#2=KDF（ID#1，ID#2，tempSK#2，tempPK#1）。其中，KDF（）表示根据密钥派生函数进行计算。

S615，第二设备计算会话密钥#2。

SessionKey#2=KDF（PSK#2，random#1，random#2）。其中，KDF（）表示根据密钥派生函数进行计算。

S616，第一设备验证设备证书#2 的合法性。

第一设备根据设备证书#2 中的 ID#2，确定预先配置的第一列表中保存 ID#2。若第一列表中保存 ID#2，则第一设备确定第二设备是需要认证的设备；若第一列表中没有保存 ID#2，则第一设备确定第二设备是不需要认证的设备，进而终止认证过程。

在第一设备确定第二设备是需要认证的设备的情况下，第一设备继续使用 PK#1 对设备证书#2 中根签名进行验证。若验证成功，则继续执行验证过程；若验证失败，则终止验证过程。

S617，第一设备验证第二签名值。

第一设备可以根据设备证书#2 中包括的 ID#2 和认证响应信息中包括的 random#2 和 tempPK#2 构造 msg#2，进一步地，第一设备根据设备证书#2 中包括的 PK#2 对 Sign#2 的合法性进行验证。验证通过之后，第一设备执行后续的认证过程。验证不通过，则验证失败。

S618，第一设备计算 PSK#1。

PSK#1=KDF（ID#1，ID#2，tempPK#2，tempSK#1）。其中，KDF（）表示根据密钥派生函数进行计算。

可以理解，虽然本申请实施例中用 PSK#1 和 PSK#2 分别表示第一设备和第二设备生成的 PSK，但这仅仅是为了区分，PSK#1 和 PSK#2 应该认为是等同的。

S619，第一设备计算会话密钥#1。

SessionKey#1=KDF（PSK#1，random#1，random#2）。其中，KDF（）表示根据密钥派生函数进行计算。

可以理解，虽然本申请实施例中用 SessionKey #1 和 SessionKey #2 分别表示第一设备和第二设备生成的 SessionKey，但这仅仅是为了区分，SessionKey#1 和 SessionKey#2 应该认为是等同的。

S620，第一设备与第二设备根据确定的密码算法套件和报文加密模式传输通信报文。

在本申请实施例中，第一设备预先配置的列表中记录了握手来源的合法设备标识列表，可以防止恶意设备伪造虚假来源发起拒绝服务攻击，起到了现有技术中的 cookie 字段的作用。也就是说，可以省去原有 TLS 协议和 DTLS 协议中的 cookie 字段分配的过程，减少了握手过程中的一次交互过程。第二设备根据预先配置的第二列表可以直接忽略不合法设备的握手请求，使第二设备只进行必要的握手，既可以减轻第二设备的处理负担，也可以提高攻击者攻击的难度。

本申请实施例通过将密码算法套件与设备的标识信息对应的方式，使得第一设备和第

二设备可以根据保存的映射关系确定通信过程中使用的密码算法套件，从而省去了原有TLS协议和DTLS协议中密码算法套件协商过程，使得第一设备和第二设备在握手过程中，不需要传递设备支持的密码算法套件列表，从而减小了握手过程中传输的数据量，提高了传输可靠性和通信效率。

此外，在会话密钥协商过程中，使用临时公私钥对，可以满足前向安全性需求。

图 11 是本申请另一实施例提供的方法 700 的示意性流程图，如图 11 所示，该方法 700 可以包括 S701 至 S716，其中，S702 至 S703 与方法 600 中的 S603 至 S604 相同，S706 至 S716 与方法 600 中的 S610 至 S620 相同，为了简洁，本申请实施例不再详述。下面详细说明其余各个步骤。

S701，第一设备确定与 ID#2 对应的密码算法套件和报文加密模式。

第一设备可以根据第三映射关系确定与 ID#2 对应的密码算法套件。第一设备可以根据第四映射关系确定与 ID#2 对应的报文加密模式。

在本申请实施例中，第一设备根据第三映射关系可以确定出与 ID#2 对应的密码算法套件，则第一设备可以默认第二设备是需要认证的设备。

S704，第一设备向第二设备发送认证响应信息。

认证响应信息中包括：ID#1、random#1、tempPK#1。

S705，第二设备确定与 ID#1 对应的密码算法套件和报文加密模式。

第二设备可以根据第一映射关系确定与 ID#1 对应的密码算法套件。第一设备可以根据第二映射关系确定与 ID#1 对应的报文加密模式。

同样，在本申请实施例，第二设备根据第一映射关系可以确定出与 ID#1 对应的密码算法套件，则第二设备可以默认第一设备是需要认证的设备。

在本申请实施例中，只进行了第一设备对第二设备的单向的身份合法认证，进一步减少握手过程中的运算步骤和交互的数据量。尽管第二设备没有对第一设备的身份合法性进行认证，但是第二设备在根据第一映射关系确定密码算法套件的过程中，可以判断第一设备是否是需要认证的设备，这提高了攻击者发送恶意握手请求的难度，相比于目前的单向认证握手过程提高了安全性。

本申请实施例通过将密码算法套件与设备的标识信息对应的方式，使得第一设备和第二设备可以根据保存的映射关系确定通信过程中使用的密码算法套件，从而省去了原有TLS协议和DTLS协议中密码算法套件协商过程，使得第一设备和第二设备在握手过程中，不需要传递设备支持的密码算法套件列表，从而减小了握手过程中传输的数据量，提高了传输可靠性和通信效率。

此外，在会话密钥协商过程中，使用临时公私钥对，可以满足前向安全性需求。

图 12 是本申请另一实施例提供的方法 800 的示意性流程图，如图 12 所示，该方法 800 可以包括 S801 至 S817，其中，S802 至 S803 与方法 600 中的 S603 至 S604 相同，S808 至 S809 与方法 600 中的 S610 至 S611 相同，S812 至 S813 与方法 600 中的 S614 至 S615 相同，S815 至 S817 与方法 600 中的 S618 至 S620 相同，为了简洁，本申请实施例不再详述。下面详细说明其余各个步骤。

S801，第一设备确定与 ID#2 对应的密码算法套件、报文加密模式和 PSK。

第一设备可以根据第三映射关系确定与 ID#2 对应的密码算法套件。第一设备可以根

据第四映射关系确定与 ID#2 对应的报文加密模式。第一设备可以根据预先配置的第一 PSK 列表确定与 ID#2 对应的 PSK。

S804，第一设备计算第一密码。

第一设备构造 msg#1，msg#1 的内容为{ID#1‖random#1}；进一步地，第一设备以 PSK 为密钥，根据密码算法套件中的对称加密算法对 msg#1 进行加密，生成 cipher#1，cipher#1=Enc_{PSK}（ID#1‖random#1）。其中，“‖”表示连接，Enc_{PSK}（）表示以 PSK 为密钥，以对称加密算法加密。

S805，第一设备向第二设备发送认证响应信息。

认证响应信息中包括：ID#1、cipher#1、tempPK#1。

S806，第二设备确定与 ID#1 对应的密码算法套件、报文加密模式和 PSK。

第二设备可以根据第一映射关系确定与 ID#1 对应的密码算法套件。第二设备可以根据第二映射关系确定与 ID#1 对应的报文加密模式。第二设备可以根据预先配置的第二 PSK 列表确定与 ID#1 对应的 PSK。

S807，第二设备解密第一密码。

第二设备确定密码算法套件之后，以确定的 PSK 为密钥，以及根据密码算法套件中的对称加密算法解密 cipher#1 得到 ID#1。进一步地，第二设备判断解密 cipher#1 得到的 ID#1 与认证请求信息中的 ID#1 是否一致，如果不一致，则认证失败，如果一致，则继续执行后续的认证过程。

S810，第二设备计算第二密码。

第二设备构造 msg#2，msg#2 的内容为{ID#2‖random#2}；进一步地，第二设备以 PSK 为密钥，根据密码算法套件中的对称加密算法对 msg#2 进行加密，生成 cipher#2，cipher#2=Enc_{PSK}（ID#2‖random#2）。其中，“‖”表示连接，Enc_{PSK}（）表示以 PSK 为密钥，以对称加密算法加密。

S811，第二设备向第一设备发送认证响应信息。

认证响应信息中包括：ID#2、tempPK#2、cipher#2。

S814，第一设备解密第二密码。

第一设备以确定的 PSK 为密钥，以及根据密码算法套件中的对称加密算法解密 cipher#2 得到 ID#2。进一步地，第二设备判断解密 cipher#2 得到的 ID#2 与认证响应信息中的 ID#2 是否一致，如果不一致，则认证失败，如果一致，则继续执行后续的认证过程。

本申请实施例通过将密码算法套件与设备的标识信息对应的方式，使得第一设备和第二设备可以根据保存的映射关系确定通信过程中使用的密码算法套件，从而省去了原有 TLS 协议和 DTLS 协议中密码算法套件协商过程，使得第一设备和第二设备在握手过程中，不需要传递设备支持的密码算法套件列表，从而减小了握手过程中传输的数据量，提高了传输可靠性和通信效率。

以及，确定了密码算法套件之后，基于预存的 PSK 可以生成 cipher 来代替设备证书。由于 cipher 的长度远小于设备证书，因此大大减小了握手交互过程中的交互数据量，提高了握手效率和可靠性。

此外，使用 cipher 代替设备证书之后，设备不再需要对设备证书中的根签名进行验签，而是变成了对 cipher 进行对称加密解密运算。而对称加密解密运算速度远远高于验签速

度，因此可以提高握手效率。

此外，在会话密钥协商过程中，使用临时公私钥对，可以满足前向安全性需求。

以上，结合图 5 至图 12 详细说明了本申请实施例提供的通信的方法。以下，结合图 13 至图 14 详细说明本申请实施例提供的装置。

图 13 是本申请实施例提供的通信装置 1000 的示意性框图。如图所示，该通信装置 1000 可以包括：收发单元 1010 和处理单元 1020。

在一种可能的设计中，该通信装置 1000 可对应于上文方法实施例中的第一设备。

应理解，该通信装置 1000 可以包括用于执行图 5 至图 7 中的方法 500、图 10 中的方法 600、图 11 中的方法 700 以及图 12 中的方法 800 中的第一设备执行的方法的单元。并且，该通信装置 1000 中的各单元和上述其他操作和/或功能分别为了实现图 5 至图 7 中的方法 500、图 10 中的方法 600、图 11 中的方法 700 以及图 12 中的方法 800 中的第一设备执行的相应流程。应理解，各单元执行上述相应步骤的具体过程在上述方法实施例中已经详细说明，为了简洁，在此不再赘述。

在另一种可能的设计中，该通信装置 1000 可对应于上文方法实施例中的第二设备。

应理解，该通信装置 1000 可以包括用于执行图 5 至图 7 中的方法 500、图 10 中的方法 600、图 11 中的方法 700 以及图 12 中的方法 800 的第二设备执行的方法的单元。并且，该通信装置 1000 中的各单元和上述其他操作和/或功能分别为了实现图 5 至图 7 中的方法 500、图 10 中的方法 600、图 11 中的方法 700 以及图 12 中的方法 800 中的第二设备执行的相应流程。应理解，各单元执行上述相应步骤的具体过程在上述方法实施例中已经详细说明，为了简洁，在此不再赘述。

应理解，该通信装置 1000 中的收发单元 1010 可对应于图 14 中示出的通信装置 2000 中的收发器 2010，该通信装置 1000 中的处理单元 1020 可对应于图 14 中示出的通信装置 2000 中的处理器 2020。

图 14 是本申请实施例提供的通信装置 2000 的示意性框图。如图所示，该通信装置 2000 可以包括：处理器 2020，还可以包括收发器 2010 和存储器 2030。该处理器 2020 与存储器 2030 耦合，用于执行存储器中存储的指令，以控制收发器 2010 发送信号和/或接收信号。

应理解，上述处理器 2020 和存储器 2030 可以合成一个处理装置，处理器 2020 用于执行存储器 2030 中存储的程序代码来实现上述功能。具体实现时，该存储器 2030 也可以集成在处理器 2020 中，或者独立于处理器 2020。

在一种可能的设计中，该通信装置 2000 可对应于上文方法实施例中的第一设备。

具体地，该通信装置 2000 可以包括用于执行图 5 至图 7 中的方法 500、图 10 中的方法 600、图 11 中的方法 700 以及图 12 中的方法 800 中的第一设备执行的方法的单元。并且，该通信装置 2000 中的各单元和上述其他操作和/或功能分别为了实现图 5 至图 7 中的方法 500、图 10 中的方法 600、图 11 中的方法 700 以及图 12 中的方法 800 中第一设备执行的相应流程。应理解，各单元执行上述相应步骤的具体过程在上述方法实施例中已经详细说明，为了简洁，在此不再赘述。

在一种可能的设计中，该通信装置 2000 可对应于上文方法实施例中的第二设备。

具体地，该通信装置 2000 可以包括用于执行图 5 至图 7 中的方法 500、图 10 中的方

法600、图11中的方法700以及图12中的方法800中的第二设备执行的方法的单元。并且，该通信装置2000中的各单元和上述其他操作和/或功能分别为了实现图5至图7中的方法500、图10中的方法600、图11中的方法700以及图12中的方法800中第二设备执行的相应流程。应理解，各单元执行上述相应步骤的具体过程在上述方法实施例中已经详细说明，为了简洁，在此不再赘述。

根据本申请实施例提供的方法，本申请还提供一种计算机程序产品，该计算机程序产品包括：计算机程序代码，当该计算机程序代码在计算机上运行时，使得该计算机执行图5至图7以及图10至图12所示实施例中任意一个实施例的方法。

根据本申请实施例提供的方法，本申请还提供一种计算机可读存储介质，该计算机可读存储介质存储有程序代码，当该程序代码在计算机上运行时，使得该计算机执行图5至图7以及图10至图12所示实施例中任意一个实施例的方法。

根据本申请实施例提供的方法，本申请还提供一种系统，该系统包括前述的第一设备和第二设备。

在上述实施例中，可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时，可以全部或部分地以计算机程序产品的形式实现。计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行计算机指令时，全部或部分地产生按照本申请实施例所述的流程或功能。计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线（例如同轴电缆、光纤、数字用户线（digital subscriber line，DSL））或无线（例如红外、无线、微波等）方式向另一个网站站点、计算机、服务器或数据中心进行传输。计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。可用介质可以是磁性介质（例如，软盘、硬盘、磁带）、光介质（例如，高密度数字视频光盘（digital video disc，DVD））、或者半导体介质（例如，固态硬盘（solid state disk，SSD））等。

上述各个装置实施例中各网元可以和方法实施例中的各网元完全对应，由相应的单元执行相应的步骤，例如收发单元（收发器）执行方法实施例中接收或发送的步骤，除发送、接收外的其它步骤可以由处理单元（处理器）执行。具体单元的功能可以参考相应的方法实施例。其中，处理器可以为一个或多个。

应理解，说明书通篇中提到的“一个实施例”或“一实施例”意味着与实施例有关的特定特征、结构或特性包括在本申请的至少一个实施例中。因此，在整个说明书各处出现的“在一个实施例中”或“在一实施例中”未必一定指相同的实施例。此外，这些特定的特征、结构或特性可以任意适合的方式结合在一个或多个实施例中。应理解，在本申请的各种实施例中，上述各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本申请实施例的实施过程构成任何限定。

在本说明书中使用的术语“单元”、“系统”等用于表示计算机相关的实体、硬件、固件、硬件和软件的组合、软件、或执行中的软件。例如，部件可以是但不限于，在处理器上运行的进程、处理器、对象、可执行文件、执行线程、程序和/或计算机。通过图示，在计算设备上运行的应用和计算设备都可以是部件。一个或多个部件可驻留在进程和/或

执行线程中，部件可位于一个计算机上和/或分布在 2 个或更多个计算机之间。此外，这些部件可从在上面存储有各种数据结构的各种计算机可读介质执行。部件可例如根据具有一个或多个数据分组（例如来自与本地系统、分布式系统和/或网络间的另一部件交互的二个部件的数据，例如通过信号与其它系统交互的互联网）的信号通过本地和/或远程进程来通信。

本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及方法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统、装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

在本申请所提供的几个实施例中，应该理解到，所揭露的系统、装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，上述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

上述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

另外，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。

上述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（read-only memory，ROM）、随机存取存储器（random access memory，RAM）、磁碟或者光盘等各种可以存储程序代码的介质。

以上所述，仅为本申请的具体实施方式，但本申请的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本申请揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应以权利要求的保护范围为准。

权 利 要 求 书

1、一种通信的方法，其特征在于，包括:

第二设备接收来自第一设备的认证请求信息，所述认证请求信息包括所述第一设备的标识信息;

所述第二设备根据第一映射关系确定与所述第一设备的标识信息对应的密码算法套件，所述第一映射关系用于指示至少一个设备的标识信息与至少一个密码算法套件之间的对应关系;

所述第二设备根据所述密码算法套件，生成认证响应信息;

所述第二设备向所述第一设备发送所述认证响应信息。

2、根据权利要求 1 所述的方法，其特征在于，在所述第二设备向所述第一设备发送认证响应信息之前，所述方法还包括:

所述第二设备确定预先配置的第二列表中包含所述第一设备的标识信息，所述第二列表中包括需要认证的设备的标识信息。

3、根据权利要求 1 或 2 所述的方法，其特征在于，所述认证请求信息还包括所述第一设备的第一设备证书和/或所述第一设备使用的第一签名值; 和/或

所述认证响应信息还包括所述第二设备的第二设备证书和/或所述第二设备使用的第二签名值。

4、根据权利要求 1 至 3 中任一项所述的方法，其特征在于，

所述认证请求信息还包括所述第一设备使用的第一随机数和/或所述第一设备使用的第一临时公钥;

所述认证响应信息还包括所述第二设备使用的第二随机数和/或所述第二设备使用的第二临时公钥。

5、根据权利要求 1 或 2 所述的方法，其特征在于，所述认证请求信息还包括第一密码; 和/或

所述认证响应信息还包括第二密码，所述第二密码是所述第二设备根据预存的预共享密钥和所述密码算法套件生成的。

6、根据权利要求 5 所述的方法，其特征在于，所述认证请求信息还包括所述第一设备使用的第一临时公钥;

所述认证响应信息还包括所述第二设备使用的第二临时公钥和所述第二设备的标识信息。

7、根据权利要求 1 至 6 中任一项所述的方法，其特征在于，所述至少一个密码算法套件中的每个密码算法套件满足前向安全性需求。

8、根据权利要求 1 至 7 中任一项所述的方法，其特征在于，所述方法还包括:

所述第二设备确定与所述第一设备通信使用的报文加密模式，所述报文加密模式包括全加密模式和按需加密模式中的一个。

9、根据权利要求 8 所述的方法，其特征在于，所述第二设备确定与所述第一设备通信使用的报文加密模式，包括:

所述第二设备根据第二映射关系确定与所述第一设备的标识信息对应的所述报文加密模式，所述第二映射关系用于指示至少一个设备的标识信息与至少一个报文加密模式之间的对应关系。

10、根据权利要求 8 或 9 所述的方法，其特征在于，在所述报文加密模式是按需加密模式的情况下时，所述方法还包括:

所述第二设备生成通信报文，所述通信报文包括以下字段：明文标识、明文数据、密文标识、密文数据。

11、根据权利要求 10 所述的方法，其特征在于，所述明文数据中包含所述密文数据的流加密密钥生成种子。

12、一种通信的方法，其特征在于，包括:

第一设备根据第三映射关系确定与第二设备的标识信息对应的密码算法套件，所述第三映射关系用于指示至少一个设备的标识信息与至少一个密码算法套件之间的对应关系;

所述第一设备根据所述密码算法套件生成认证请求信息，所述认证请求信息包括所述第一设备的标识信息;

所述第一设备向所述第二设备发送所述认证请求信息;

所述第一设备接收来自所述第二设备的认证响应信息。

13、根据权利要求 12 所述的方法，其特征在于，在所述第一设备向所述第二设备发送所述认证请求信息之前，所述方法还包括:

所述第一设备确定预先配置的第一列表中包含所述第二设备的标识信息，所述第一列表中包括需要认证的设备的标识信息。

14、根据权利要求 12 或 13 所述的方法，其特征在于，所述认证请求信息还包括所述第一设备的设备证书和/或所述第一设备使用的第一签名值；和/或

所述认证响应信息还包括所述第二设备的第二设备证书和/或所述第二设备使用的第二签名值。

15、根据权利要求 12 或 13 所述的方法，其特征在于，所述认证请求信息还包括第一密码，所述第一密码是所述第一设备根据预存的预共享密钥和所述密码算法套件生成的;和/或

所述认证响应信息还包括第二密码。

16、根据权利要求 15 所述的方法，其特征在于，所述认证请求信息还包括所述第一设备使用的第一临时公钥;

所述认证响应信息还包括所述第二设备使用的第二临时公钥和所述第二设备的标识信息。

17、根据权利要求 12 至 14 中任一项所述的方法，其特征在于，所述认证请求信息还包括所述第一设备使用的第一随机数和/或所述第一设备使用的第一临时公钥;

所述认证响应信息还包括所述第二设备使用的第二随机数和/或所述第二设备使用的第二临时公钥。

18、根据权利要求 12 至 17 中任一项所述的方法，其特征在于，所述至少一个密码算法套件中的每个密码算法套件满足前向安全性需求。

19、根据权利要求 12 至 18 中任一项所述的方法，其特征在于，所述方法还包括:

所述第一设备确定与所述第二设备通信使用的报文加密模式，所述报文加密模式包括全加密模式和按需加密模式中的一个。

20、根据权利要求 19 所述的方法，其特征在于，所述第一设备确定与所述第二设备通信使用的报文加密模式，包括：

所述第一设备根据第四映射关系确定与所述第二设备的标识信息对应的所述报文加密模式，所述第四映射关系用于指示至少一个设备的标识信息与至少一个报文加密模式之间的对应关系。

21、根据权利要求 19 或 20 所述的方法，其特征在于，在所述报文加密模式是按需加密模式的情况下，所述方法还包括：

所述第一设备生成通信报文，所述通信报文包括以下字段：明文标识、明文数据、密文标识、密文数据。

22、根据权利要求 21 所述的方法，其特征在于，所述明文数据中包含所述密文数据的流加密密钥生成种子。

23、一种通信装置，其特征在于，包括用于实现如权利要求 1 至 11 中任一项所述的方法的单元。

24、一种通信装置，其特征在于，包括用于实现如权利要求 12 至 22 中任一项所述的方法的单元。

25、一种通信装置，其特征在于，包括：

处理器，用于执行存储器中存储的计算机指令，以使得所述通信装置执行：如权利要求 1 至 11 中任一项所述的方法。

26、一种通信装置，其特征在于，包括：

处理器，用于执行存储器中存储的计算机指令，以使得所述通信装置执行：如权利要求 12 至 22 中任一项所述的方法。

27、一种计算机可读存储介质，其特征在于，其上存储有计算机程序，所述计算机程序被执行时，以使得如权利要求 1 至 11 中任一项所述的方法被执行。

28、一种计算机可读存储介质，其特征在于，其上存储有计算机程序，所述计算机程序被执行时，以使得如权利要求 12 至 22 中任一项所述的方法被执行。

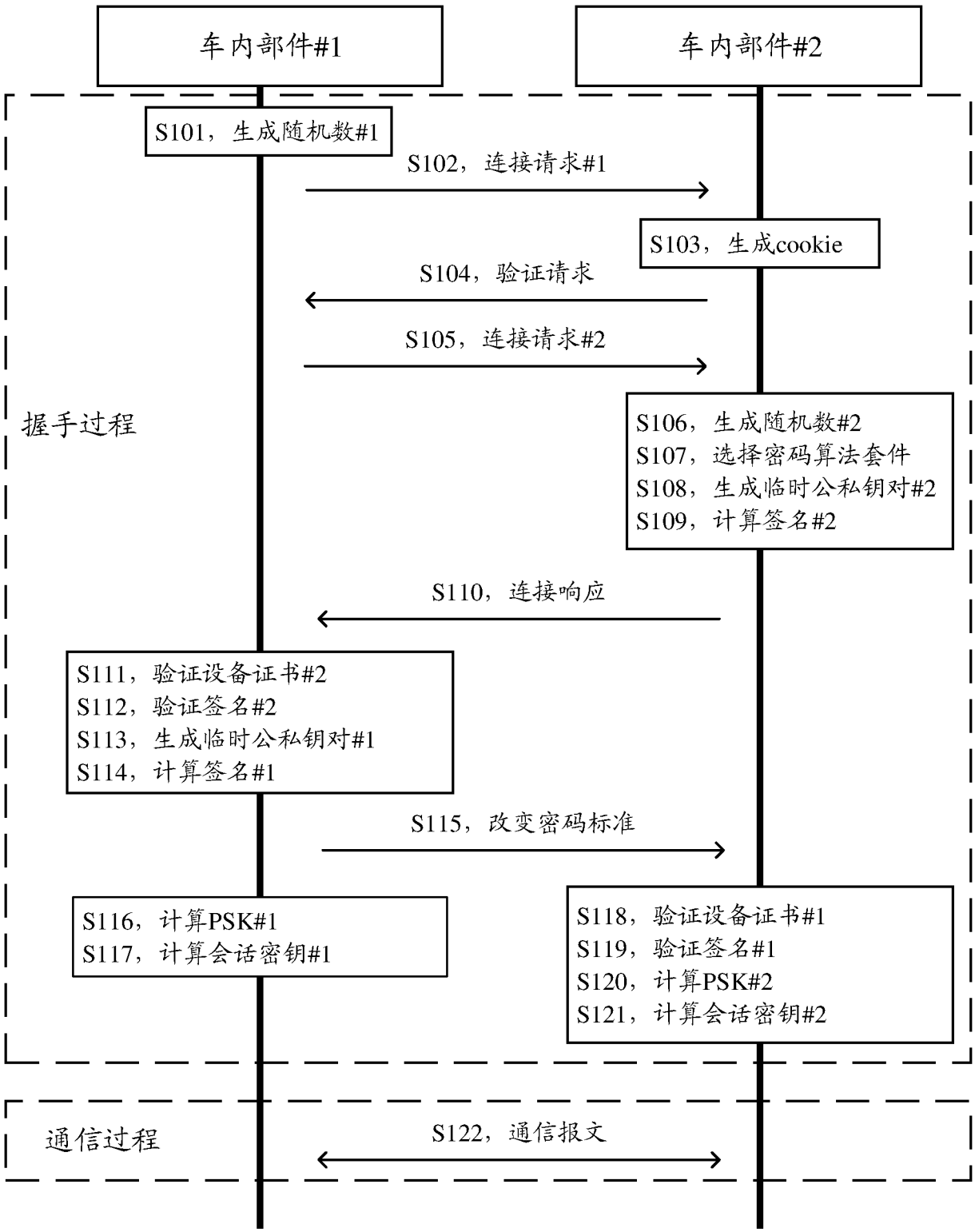
车内部件#1
车内部件#2
S101，生成随机数#1
S102，连接请求#1
S103，生成cookie
S104，验证请求
S105，连接请求#2
握手过程
S106，生成随机数#2
S107，选择密码算法套件
S108，生成临时公私钥对#2
S109，计算签名#2
S110，连接响应
S111，验证设备证书#2
S112，验证签名#2
S113，生成临时公私钥对#1
S114，计算签名#1
S115，改变密码标准
S116，计算PSK#1
S117，计算会话密钥#1
S118，验证设备证书#1
S119，验证签名#1
S120，计算PSK#2
S121，计算会话密钥#2
通信过程
S122，通信报文

图 1

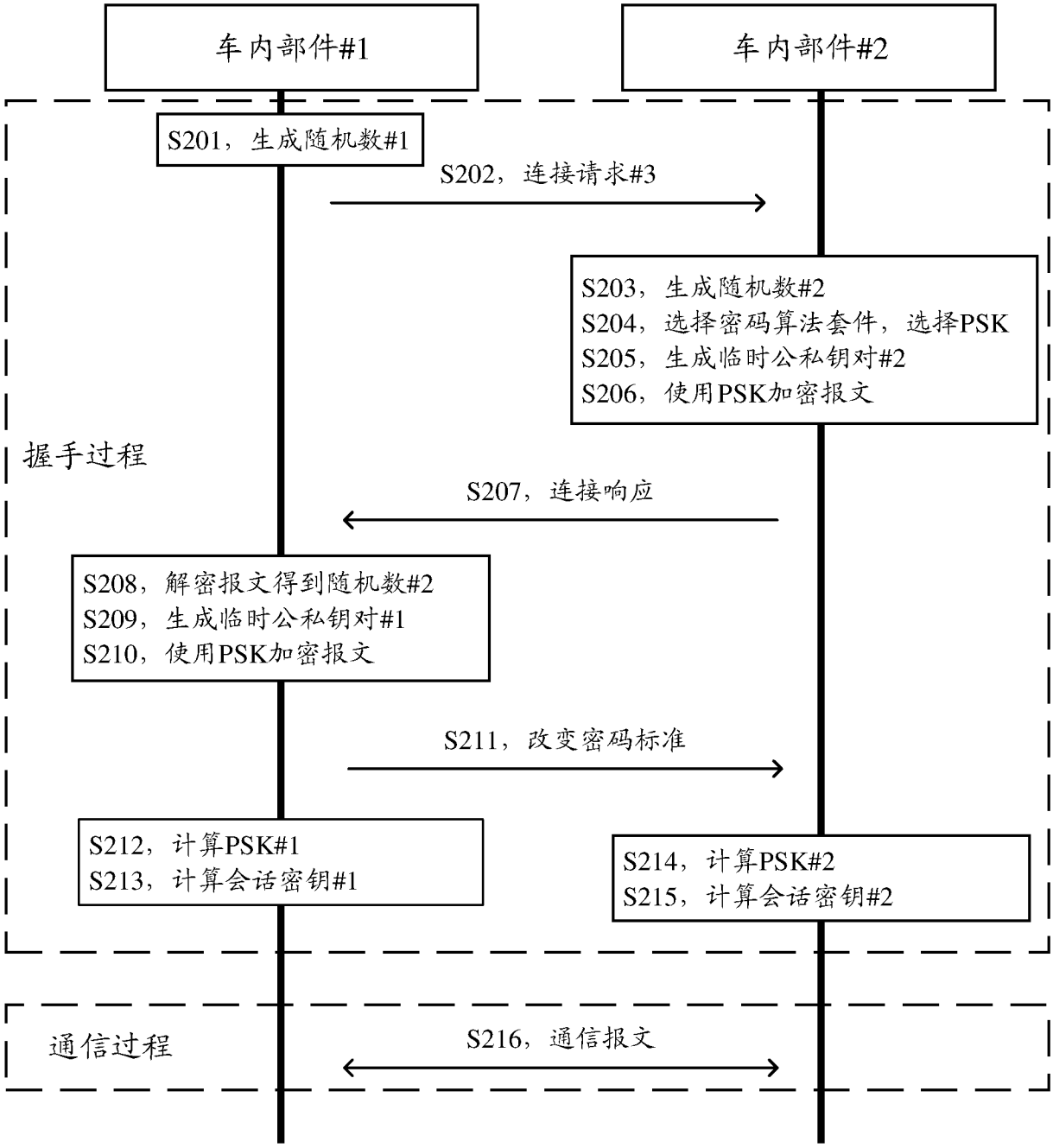
车内部件#1
车内部件#2
S201，生成随机数#1
S202，连接请求#3
S203，生成随机数#2
S204，选择密码算法套件，选择PSK
S205，生成临时公私钥对#2
S206，使用PSK加密报文
握手过程
S207，连接响应
S208，解密报文得到随机数#2
S209，生成临时公私钥对#1
S210，使用PSK加密报文
S211，改变密码标准
S212，计算PSK#1
S213，计算会话密钥#1
S214，计算PSK#2
S215，计算会话密钥#2
通信过程
S216，通信报文

图 2

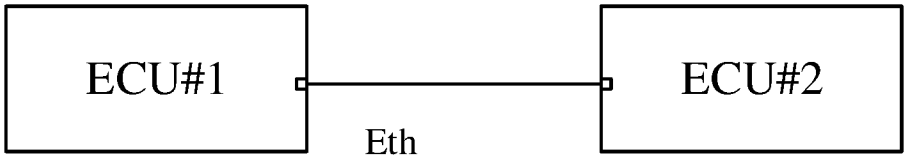
ECU#1
ECU#2
Eth

图 3

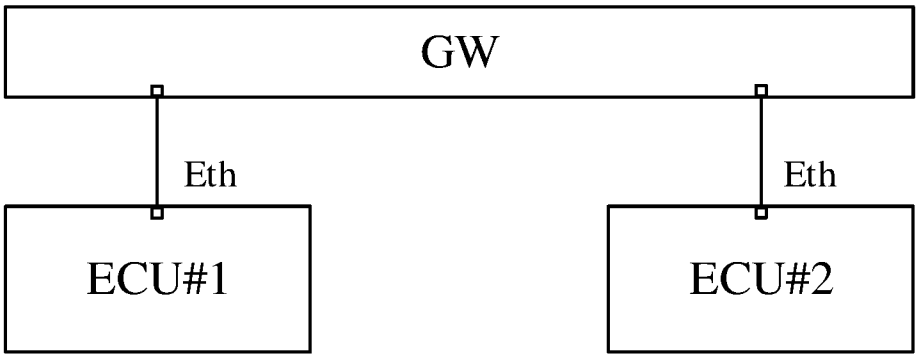
GW
Eth
Eth
ECU#1
ECU#2

图 4

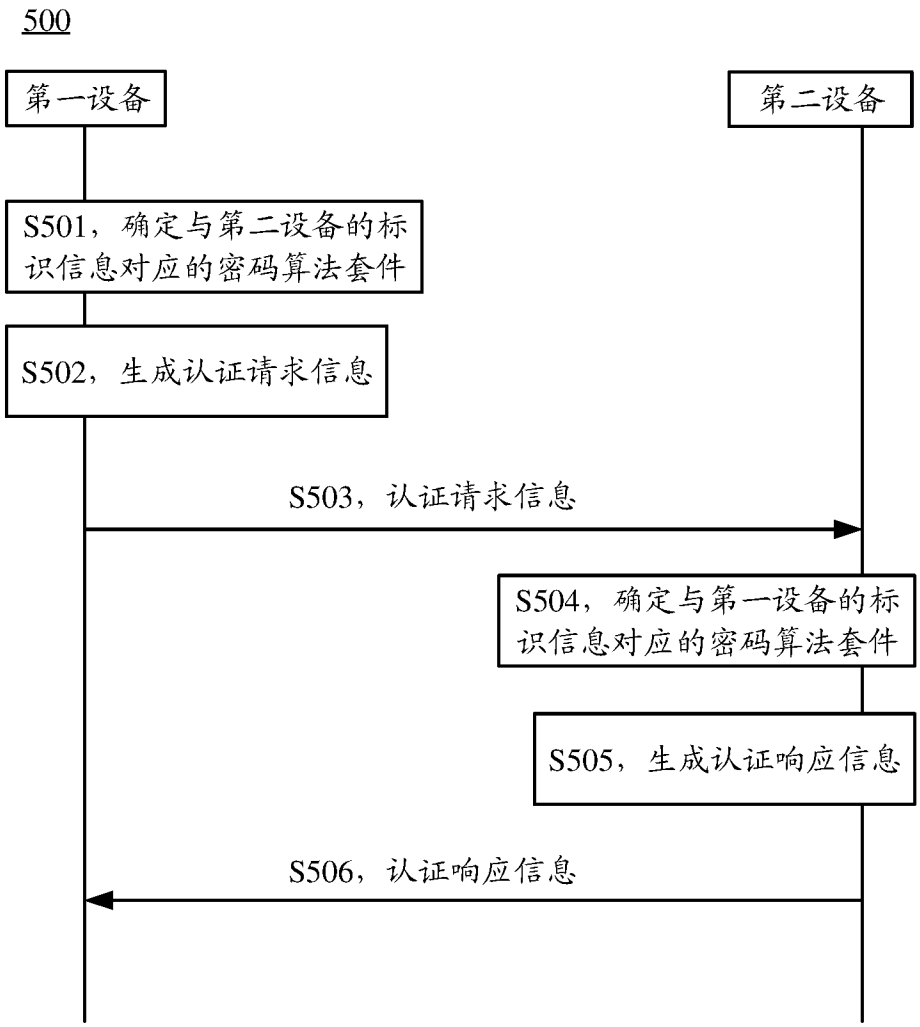
500
第一设备
第二设备
S501，确定与第二设备的标识信息对应的密码算法套件
S502，生成认证请求信息
S503，认证请求信息
S504，确定与第一设备的标识信息对应的密码算法套件
S505，生成认证响应信息
S506，认证响应信息

图 5

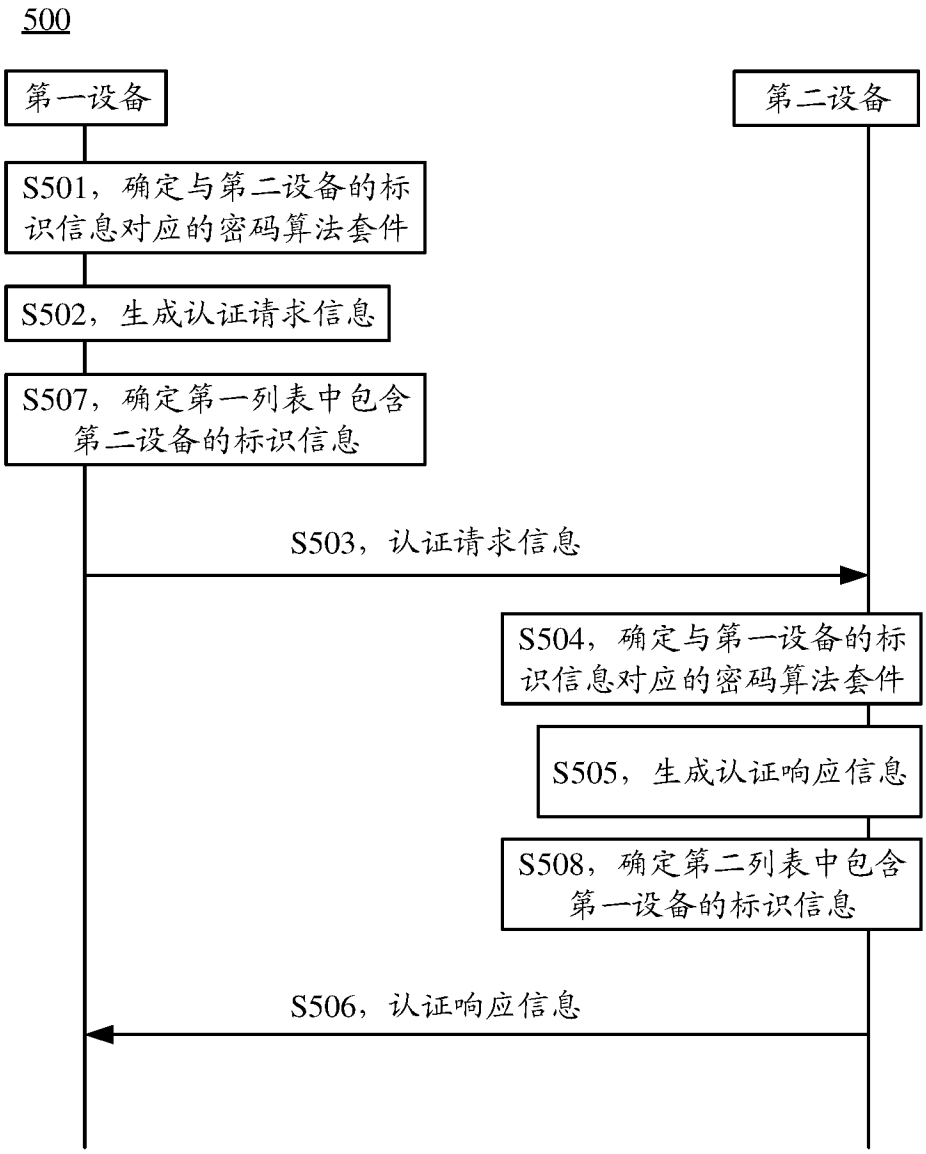
500
第一设备
第二设备
S501，确定与第二设备的标识信息对应的密码算法套件
S502，生成认证请求信息
S507，确定第一列表中包含第二设备的标识信息
S503，认证请求信息
S504，确定与第一设备的标识信息对应的密码算法套件
S505，生成认证响应信息
S508，确定第二列表中包含第一设备的标识信息
S506，认证响应信息

图 6

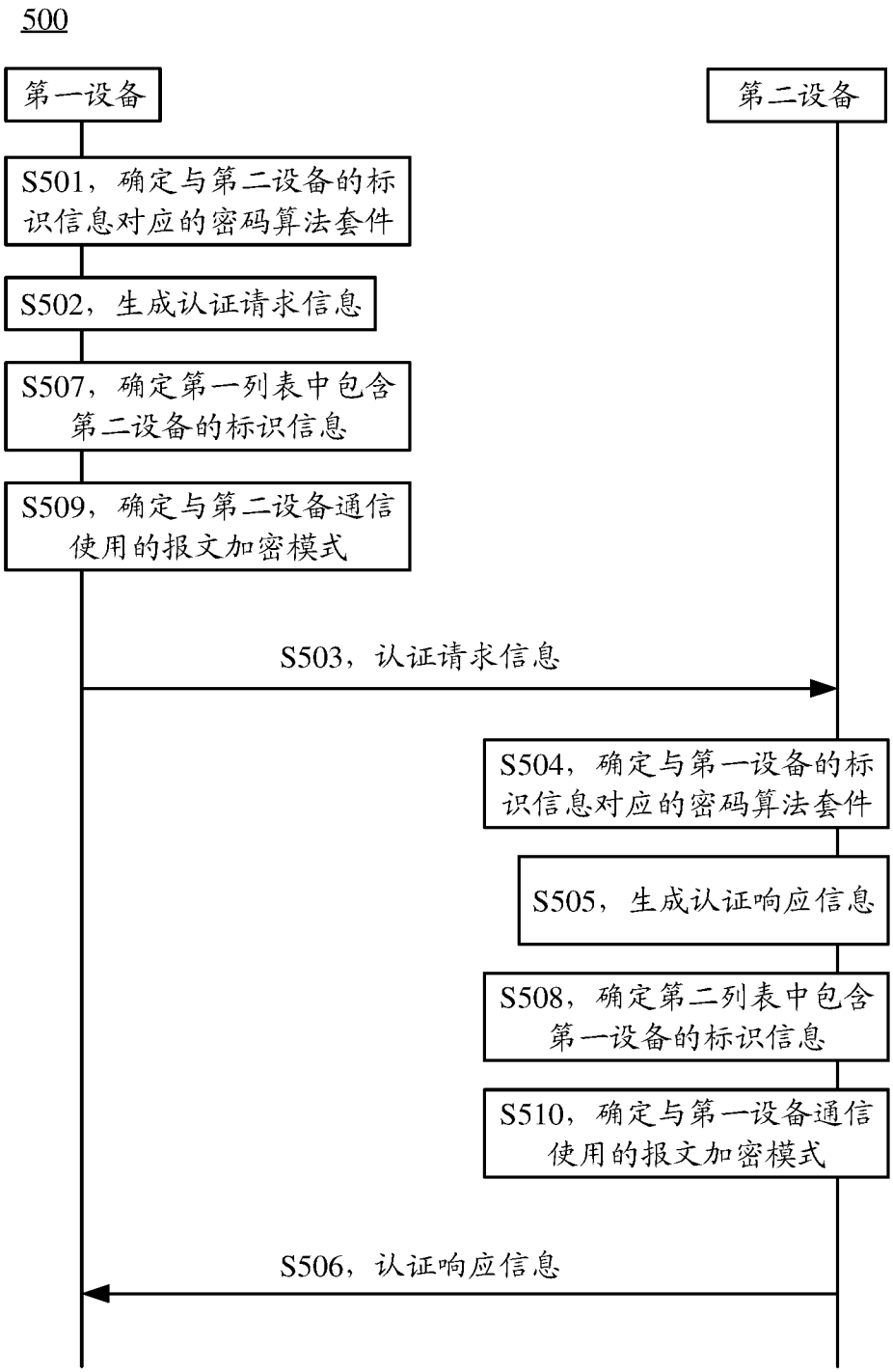
500
第一设备
第二设备
S501，确定与第二设备的标识信息对应的密码算法套件
S502，生成认证请求信息
S507，确定第一列表中包含第二设备的标识信息
S509，确定与第二设备通信使用的报文加密模式
S503，认证请求信息
S504，确定与第一设备的标识信息对应的密码算法套件
S505，生成认证响应信息
S508，确定第二列表中包含第一设备的标识信息
S510，确定与第一设备通信使用的报文加密模式
S506，认证响应信息

图 7

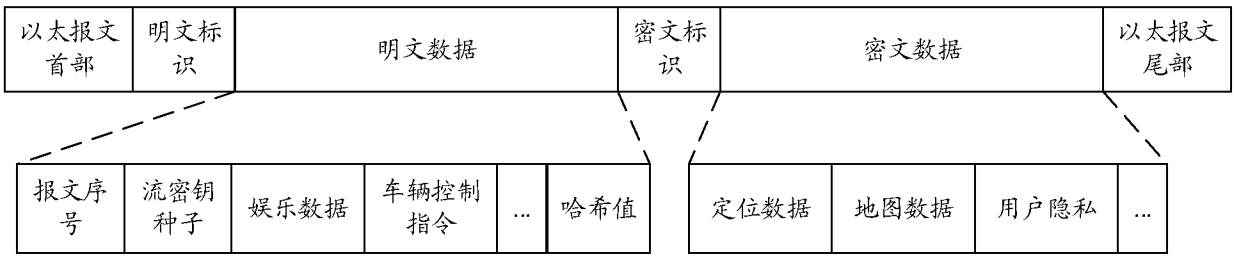
以太报文首部
明文标识
明文数据
密文标识
密文数据
以太报文尾部
报文序号
流密钥种子
娱乐数据
车辆控制指令
...
哈希值
定位数据
地图数据
用户隐私
...

图 8

以太报文首部	报文序号	密文数据	以太报文尾部

图 9

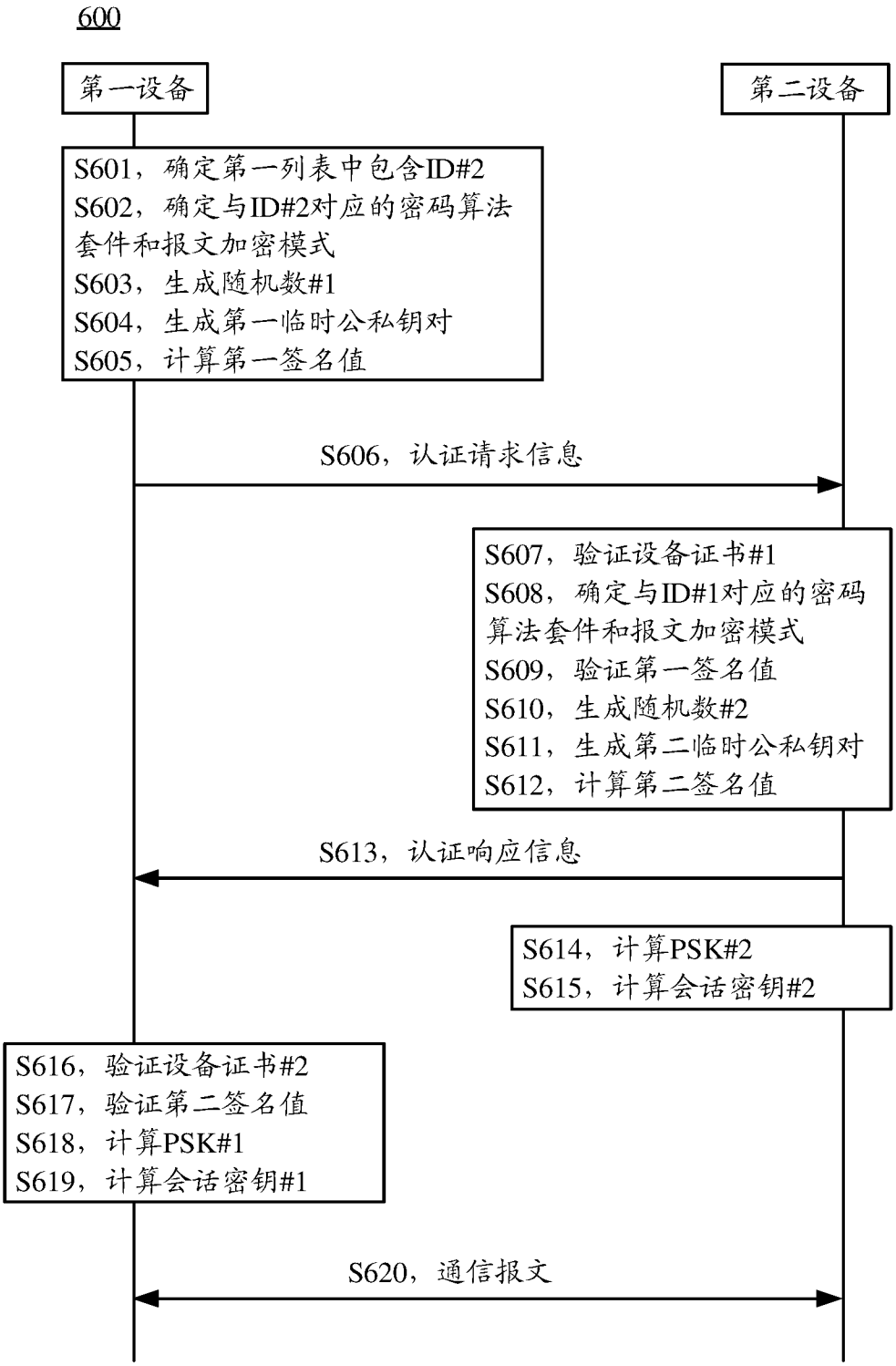

图 10

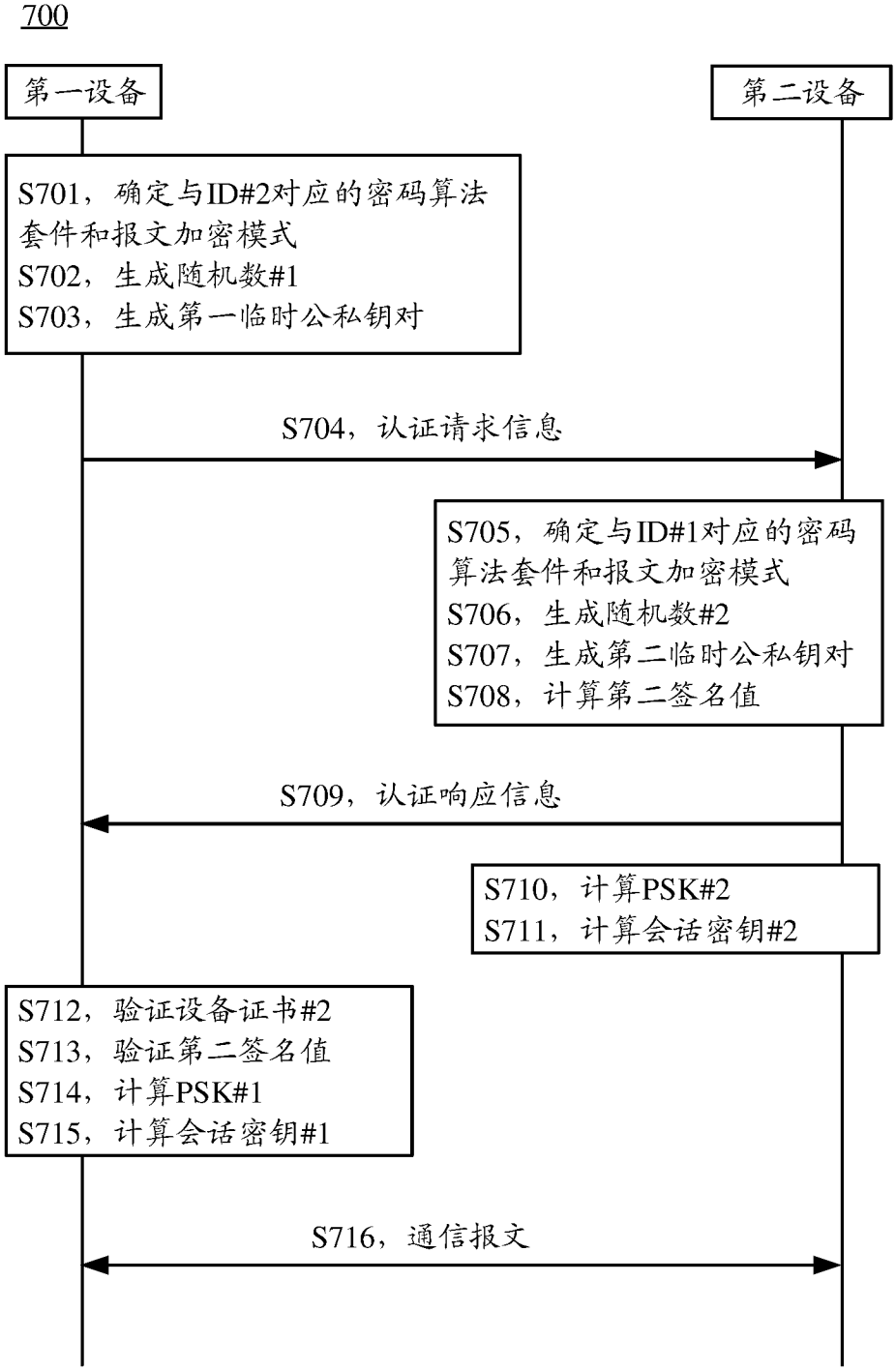
700
第一设备
第二设备
S701，确定与ID#2对应的密码算法套件和报文加密模式
S702，生成随机数#1
S703，生成第一临时公私钥对
S704，认证请求信息
S705，确定与ID#1对应的密码算法套件和报文加密模式
S706，生成随机数#2
S707，生成第二临时公私钥对
S708，计算第二签名值
S709，认证响应信息
S710，计算PSK#2
S711，计算会话密钥#2
S712，验证设备证书#2
S713，验证第二签名值
S714，计算PSK#1
S715，计算会话密钥#1
S716，通信报文

图 11

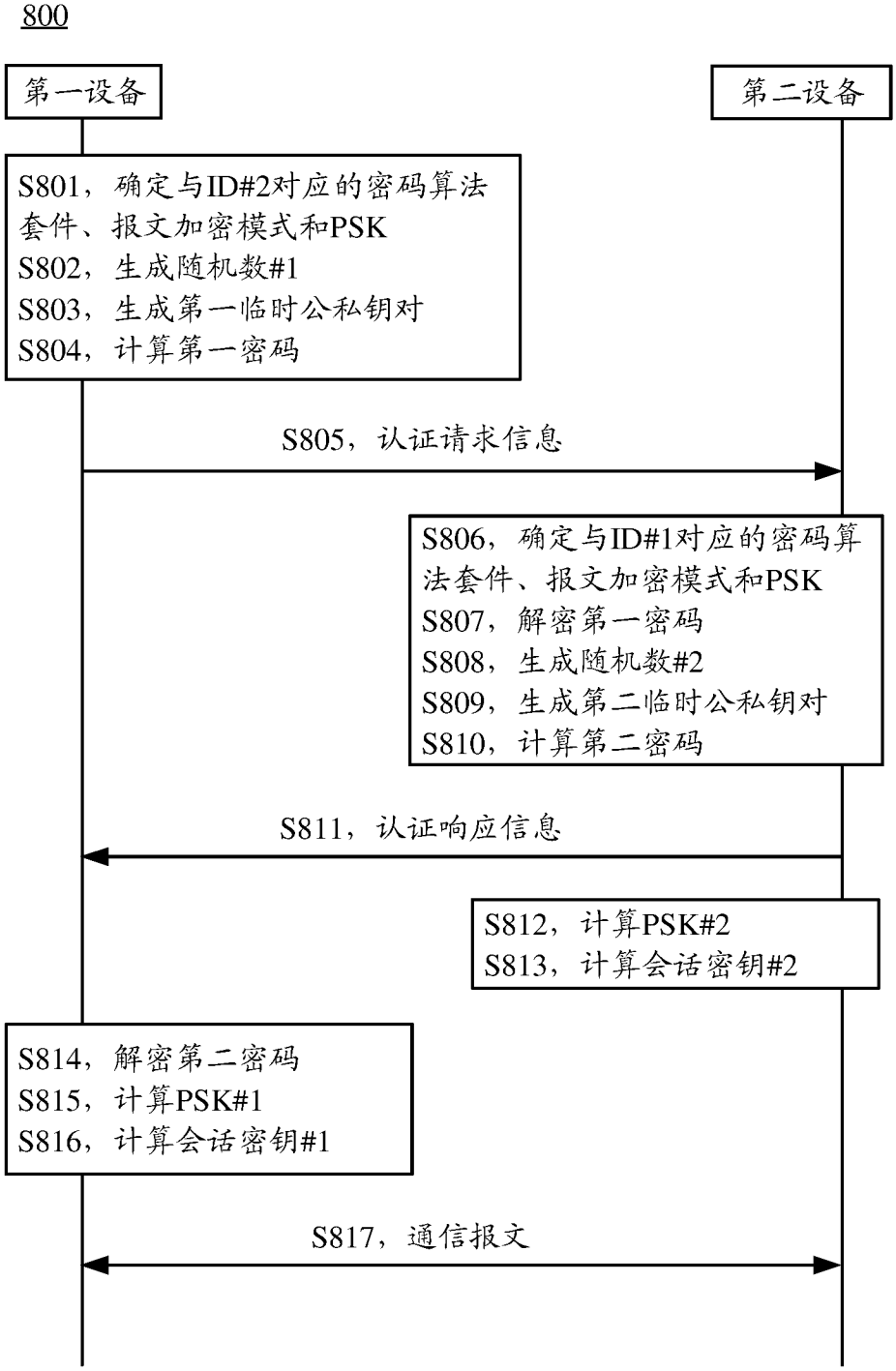
800
第一设备
第二设备
S801，确定与ID#2对应的密码算法套件、报文加密模式和PSK
S802，生成随机数#1
S803，生成第一临时公私钥对
S804，计算第一密码
S805，认证请求信息
S806，确定与ID#1对应的密码算法套件、报文加密模式和PSK
S807，解密第一密码
S808，生成随机数#2
S809，生成第二临时公私钥对
S810，计算第二密码
S811，认证响应信息
S812，计算PSK#2
S813，计算会话密钥#2
S814，解密第二密码
S815，计算PSK#1
S816，计算会话密钥#1
S817，通信报文

图 12

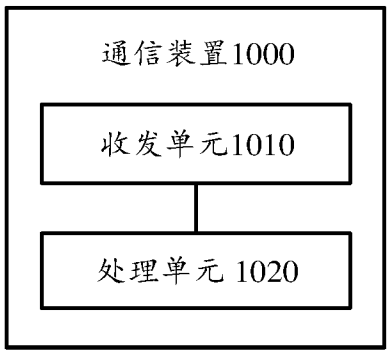
通信装置1000
收发单元1010
处理单元 1020

图 13

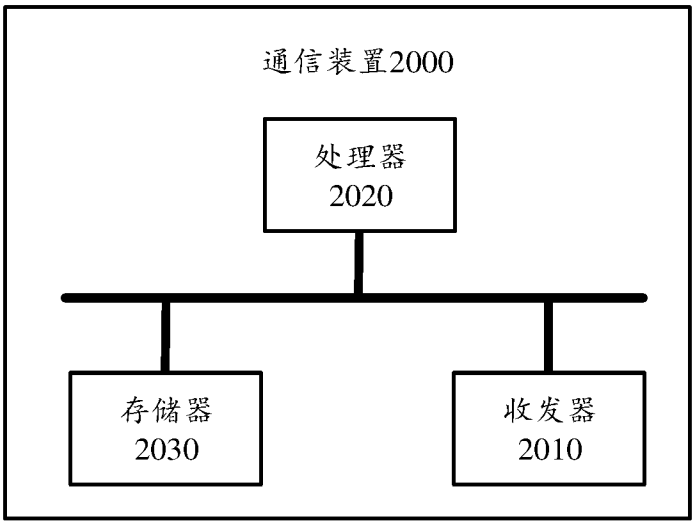
通信装置2000
处理器
2020
存储器
2030
收发器
2010

图 14

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/090460

A. CLASSIFICATION OF SUBJECT MATTER

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

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC: 密钥, 网元, 网络功能, 终端, 标识, 请求, 指示, 安全, 密码套件, 认证, 协商, 量子, 传输层安全, 安全套接字层; key, NE, NF, UE, identifier, request, indication, security, cipher suite, authentication, negotiation, quantum, TLS, SSL

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 108809633 A (GUANGDONG GUODUN QUANTUM TECHNOLOGY CO., LTD.) 13 November 2018 (2018-11-13) description paragraphs 0089-0128	1-28
X	CN 103763356 A (SHENZHEN UNIVERSITY) 30 April 2014 (2014-04-30) description, paragraphs 0004-0043	1-28
X	CN 107612899 A (ZHEJIANG QUSENJOY NETWORK TECHNOLOGY CO., LTD.) 19 January 2018 (2018-01-19) description paragraphs 0041-0118	1-28
A	EP 2207302 A1 (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) 14 July 2010 (2010-07-14) entire document	1-28
A	WO 2010049673 A1 (QINETIQ LIMITED REGISTERED OFFICE) 06 May 2010 (2010-05-06) entire document	1-28
A	US 2013195274 A1 (OKI ELECTRIC INDUSTRY CO., LTD.) 01 August 2013 (2013-08-01) entire document	1-28

☐ 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
05 February 2021	**18 February 2021**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2020/090460

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	108809633	A	13 November 2018	None			
CN	103763356	A	30 April 2014	None			
CN	107612899	A	19 January 2018	None			
EP	2207302	A1	14 July 2010	US	2010250951	A1	30 September 2010
				WO	2009060899	A1	14 May 2009
				JP	WO2009060899	A1	24 March 2011
WO	2010049673	A1	06 May 2010	US	2011213979	A1	01 September 2011
				GB	0819665	D0	03 December 2008
				EP	2356772	A1	17 August 2011
US	2013195274	A1	01 August 2013	JP	2013156330	A	15 August 2013

国际检索报告

国际申请号
PCT/CN2020/090460

A. 主题的分类

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

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNPAT,CNKI,WPI,EPODOC：密钥，网元，网络功能，终端，标识，请求，指示，安全，密码套件，认证，协商，量子，传输层安全，安全套接字层；key, NE, NF, UE, identifier, request, indication, security, cipher suite, authentication, negotiation, quantum, TLS, SSL

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 108809633 A (广东国盾量子科技有限公司) 2018年 11月 13日 (2018-11-13) 说明书第0089-0128段	1-28
X	CN 103763356 A (深圳大学) 2014年 4月 30日 (2014-04-30) 说明书第0004-0043段	1-28
X	CN 107612899 A (浙江神州量子网络科技有限公司) 2018年 1月 19日 (2018-01-19) 说明书第0041-0118段	1-28
A	EP 2207302 A1 (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) 2010年 7月 14日 (2010-07-14) 全文	1-28
A	WO 2010049673 A1 (QINETIQ LIMITED REGISTERED OFFICE) 2010年 5月 6日 (2010-05-06) 全文	1-28
A	US 2013195274 A1 (OKI ELECTRIC INDUSTRY CO., LTD.) 2013年 8月 1日 (2013-08-01) 全文	1-28

☐ 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
2021年 2月 5日	2021年 2月 18日

ISA/CN的名称和邮寄地址	受权官员
中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	彭亮
传真号 (86-10)62019451	电话号码 86-10-53961652

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2020/090460

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	108809633	A	2018年 11月 13日	无			
CN	103763356	A	2014年 4月 30日	无			
CN	107612899	A	2018年 1月 19日	无			
EP	2207302	A1	2010年 7月 14日	US	2010250951	A1	2010年 9月 30日
				WO	2009060899	A1	2009年 5月 14日
				JP	WO2009060899	A1	2011年 3月 24日
WO	2010049673	A1	2010年 5月 6日	US	2011213979	A1	2011年 9月 1日
				GB	0819665	D0	2008年 12月 3日
				EP	2356772	A1	2011年 8月 17日
US	2013195274	A1	2013年 8月 1日	JP	2013156330	A	2013年 8月 15日