(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
2022 年 3 月 3 日 (03.03.2022)

WIPO | PCT

(10) 国际公布号
WO 2022/042137 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/CN2021/107277

(22) 国际申请日: 2021 年 7 月 20 日 (20.07.2021)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202010899982.8 2020年8月31日 (31.08.2020) CN

(71) 申请人: **OPPO 广东移动通信有限公司 (GUANGDONG OPPO MOBILE TELECOMMUNICATIONS CORP., LTD.)** [CN/CN]; 中国广东省东莞市长安镇乌沙海滨路 18 号, Guangdong 523860 (CN)。

(72) 发明人: **曾春亮 (ZENG, Chunliang)**; 中国广东省东莞市长安镇乌沙海滨路 18 号, Guangdong 523860 (CN)。 **翟召轩 (ZHAI, Zhaoxuan)**; 中国广东省东莞市长安镇乌沙海滨路 18 号, Guangdong 523860 (CN)。 **杨启昌 (YANG, Qichang)**; 中国广东省东莞市长安镇乌沙海滨路 18 号, Guangdong 523860 (CN)。

(74) 代理人: **北京派特恩知识产权代理有限公司 (CHINA PAT INTELLECTUAL PROPERTY OFFICE)**; 中国北京市海淀区海淀南路21号中关村知识产权大厦B座2层, Beijing 100080 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT,

(54) **Title:** DATA TRANSMISSION METHOD AND APPARATUS, DEVICE, AND STORAGE MEDIUM

(54) **发明名称**: 一种数据传输方法、装置、设备及存储介质

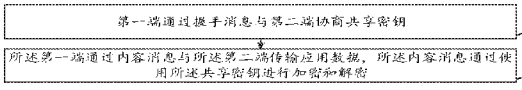

图 16

S1001 A first terminal negotiates a shared key with a second terminal by means of a handshake message

S1002 The first terminal transmits application data to the second terminal by means of a content message, the content message being encrypted and decrypted by using the shared key

(57) **Abstract:** The present application discloses a data transmission method, comprising: a first terminal negotiating a shared key with a second terminal by means of a handshake message; and the first terminal transmitting application data to the second terminal by means of a content message, the content message being encrypted and decrypted by using the shared key, wherein the handshake message and the content message have the same message format, the message format comprises a message serial number and a message load, the message serial number comprises a key epoch identifier and a message seq identifier, and the key epoch identifier is characterized by bit information less than a first number of bits, and the message seq identifier is characterized by bit information less than a second number of bits. The present application further discloses a data transmission apparatus, a device, and a storage medium. By means of the data transmission method and apparatus, and the storage medium provided in the embodiments of the present application, a shared key can be negotiated.

(57) **摘要**: 本申请公开一种数据传输方法，包括：第一端通过握手消息与第二端协商共享密钥；所述第一端通过内容消息与所述第二端传输应用数据，所述内容消息通过使用所述共享密钥进行加密和解密；其中，所述握手消息和所述内容消息具有相同的消息格式，所述消息格式包括：消息序号和消息载荷；所述消息序号包括密钥代数标识和消息计数标识，其中，所述密钥代数标识通过小于第一位数的比特信息进行表征，所述消息计数标识通过小于第二位数的比特信息进行表征。本申请还公开了一种数据传输装置、设备及存储介质；通过本申请实施例提供的数据传输方法、装置及存储介质，可以实现共享密钥的协商。

WO 2022/042137 A1

[见续页]

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, 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))。

一种数据传输方法、装置、设备及存储介质

相关申请的交叉引用

本申请基于申请号为 202010899982.8、申请日为 2020 年 08 月 31 日的中国专利申请提出，并要求该中国专利申请的优先权，该中国专利申请的全部内容在此以全文引入的方式引入本申请。

技术领域

本申请涉及通信安全技术领域，尤其涉及一种数据传输方法、装置、设备及存储介质。

背景技术

物联网设备在进行数据传输之前，考虑到数据传输的安全因素，客户端与服务端需要先通过交互的方式协商共享密钥，进而通过共享密钥进行数据传输。因此，如何协商共享密钥，是需要解决的技术问题。

发明内容

本申请实施例提供一种数据传输方法、装置、设备及存储介质，本申请实施例的技术方案是这样实现的：

第一方面，本申请实施例提供一种数据传输方法，包括：第一端通过握手消息与第二端协商共享密钥；所述第一端通过内容消息与所述第二端传输应用数据，所述内容消息通过使用所述共享密钥进行加密和解密；其中，所述握手消息和所述内容消息具有相同的消息格式，所述消息格式包括：消息序号和消息载荷；所述消息序号包括密钥代数（Epoch）标识和消息计数（Seq）标识，其中，所述密钥代数标识通过小于第一位数的比特信息进行表征，所述消息计数标识通过小于第二位数的比特信息进行表征。

第二方面，本申请实施例提供一种数据传输装置，包括：协商单元，用于通过握手消息与第二端协商共享密钥；应用数据单元，用于通过内容消息与所述第二端传输应用数据，所述内容消息通过使用所述共享密钥进行加密和解密；其中，所述握手消息和所述内容消息具有相同的消息格式，所述消息格式包括：消息序号和消息载荷；所述消息序号包括密钥代数标识和消息计数标识，其中，所述密钥代数标识通过小于第一位数的比特信息进行表征，所述消息计数标识通过小于第二位数的比特信息进行表征。

第三方面，本申请实施例提供一种存储介质，存储有可执行程序，所述可执行程序被处理器执行时，实现本申请实施例所述的数据传输方法。

第四方面，本申请实施例提供一种电子设备，包括存储器、处理器及存储在存储器上并能够由所述处理器运行的可执行程序，所述处理器运行所述可执行程序时执行本申请实施例所述的数据传输方法的步骤。

附图说明

图 1 为相关技术中基于 ECDH 的配网协议的流程示意图；

图 2 为相关技术中基于 ECJPAKE 的配网协议的流程示意图；

图 3 为本申请实施例提供的数据传输方法的客户端侧的一种可选流程示意图；

图 4 为本申请实施例提供的使用 ECDH 的配网协议协商共享密钥的可选流程示意图；

图 5 为本申请实施例提供的使用 ECDH 的配网协议协商共享密钥的详细处理流程示意图；

图 6 为本申请实施例提供的使用 ECJPAKE 的配网协议协商共享密钥的可选流程示意图；

图 7 为本申请实施例提供的使用 ECJPAKE 的配网协议协商共享密钥的详细处理流程示意图；

图 8 为本申请实施例提供的数据传输方法的服务端侧的一种可选流程示意图；

图 9 为本申请实施例提供的数据传输方法的一种可选流程示意图；

图 10 为本申请实施例提供的数据传输方法的一种详细处理流程示意图；

图 11 为本申请实施例提供的数据传输方法的又一种可选流程示意图；

图 12 为本申请实施例提供的数据传输方法的又一种详细处理流程示意图；

图 13 为本申请实施例提供的数据传输方法的再一种可选流程示意图；

图 14 为本申请实施例提供的数据传输方法的再一种详细处理流程示意图；

图 15 为本申请实施例提供的数据传输方法的还一种可选流程示意图；

图 16 为本申请实施例提供的数据传输方法的另一种可选流程示意图；

图 17 为本申请实施例提供的客户端与服务端传输的消息的内容的可选结构示意图；

图 18 为本申请实施例提供的客户端的一种可选结构示意图；

图 19 为本申请实施例提供的服务端的一种可选结构示意图；

图 20 为本申请实施例提供的数据传输装置的一种可选结构示意图；

图 21 为本申请实施例的电子设备的硬件组成结构示意图。

具体实施方式

以下结合附图及实施例，对本申请进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本申请，并不用于限定本申请。

物联网设备在进行功能层面的操作前，出于安全的考虑，往往需要先经过配置，所谓配置，就是通过交互的方式以验证双方身份，并在此过程产生用于数据加密的密钥，由于大部分物联网（Internet of Things，IoT）设备具备通过无线技术，如 WiFi、蓝牙低能耗（Bluetooth Low Energy，BLE）等，进行连接的能力，设备配置后才可以在当前无线网络进行通讯，故将此过程称为配网。

图 1 示出了相关技术中基于 ECDH 的配网协议的流程示意图，如图 1 所示，在第一客户端与服务端建立连接后，分别生成相应的密钥对，然后基于交互的公钥产生共享密钥，在产生共享密钥后即可认为配网完成，然后利用共享密钥对应用层数据（Application Data）进行加密后传输。

图 2 示出了相关技术中基于 ECJPAKE 的配网协议的流程示意图，如图 2 所示，在第一客户端与服务端建立连接，进入握手阶段交换公钥，产生共享密钥，在产生共享密钥后即可认为配网完成，进行应用层数据的传输（用共享密钥进行对称加密）。

但是，在相关技术中基于ECDH的配网协议或者基于ECJPAKE的配网协议，设备的支持不够灵活、全面，同时，标准流程交互过程中数据量高，对BLE设备而言负担大。

随着人们对安全、隐私的意识越来越高，安全技术在物联网产品中显得愈发重要，通常在BLE设备端的做法是，根据BLE设备的安全等级执行不同的协商流程，具体包括：

（1）低安全等级：随机数提供不可预测性，对称密钥，对消息进行对称加密或解密（AES-128）；

（2）高安全等级：随机数提供不可预测性，非对称密钥交换（ECDH密钥交换），对消息进行对称加密或解密（AES-128），在消息头加消息序列号用于防重放，证书认证身份。

在研究过程中发现，对于有个人识别密码（Personal Identification Number，PIN）码的设备，PIN码本身的保护程度不够，容易发生泄露，另外密钥一旦产生将会在整个生命周期使用，没有更新机制。

基于安全通信方法中存在的问题，本申请实施例提出一种数据传输方法，能够解决相关技术方案中无法解决的技术难题和缺点。

图3示出本申请实施例提供的数据传输方法的客户端侧的一种可选流程示意图，根据各个步骤进行说明。

步骤S101，发送第一客户端问候消息。

在一些实施例中，所述客户端向服务端发送第一客户端问候消息，所述第一客户端问候消息包括第一信息，所述第一信息用于指示所述客户端能够支持的第一密钥协商模式。

在一些实施例中，所述第一密钥协商模式包括使用ECDH的配网协议协商密钥和/或使用ECJPAKE的配网协议协商密钥。

在一些实施例中，所述第一信息包括第一加密套件集合；所述第一加密套件集合包括所述客户端能够支持的至少一个加密套件的集合。

在另一些实施例中，所述第一客户端问候消息还可以包括：第一加密套件字段；所述加密套件字段用于指示所述客户端支持的部分或全部加密套件参数。

在一些实施例中，所述第一信息还可以包括第一加密曲线集合；所述第一加密曲线集合包括所述客户端能够支持的至少一个加密曲线的集合。

在另一些实施例中，所述第一客户端问候消息还可以包括：第一加密曲线字段；所述加密曲线字段用于指示所述客户端支持的部分或全部加密曲线参数。

在一些实施例中，所述第一客户端问候消息还包括：第一公钥，所述第一公钥包括：在所述客户端能够支持ECDH的配网协议的情况下，所述第一加密套件集合中任一个加密套件和/或所述第一加密曲线集合中任一个加密曲线确定的公钥。不同加密套件和/或加密曲线确定的公钥不同。

在一些实施例中，所述第一客户端问候消息还包括：第一协议标识集合，所述第一协议标识集合包括至少一个协议版本对应的协议标识，所述协议版本与所述协议标识一一对应，所述第一协议标识集合指示所述客户端支持的协议版本的集合。

在另一些实施例中，所述第一客户端问候消息还可以包括：协议版本字段；所述协议版本字段用于指示所述客户端支持的部分或全部协议版本参数。

在一些实施例中，所述第一客户端问候消息还包括：第一公钥列表，所述第一客户端问候消息的第一公钥列表为NULL。

步骤S102，获取服务端基于所述第一客户端问候消息发送的第一反馈信息。

在一些实施例中，所述客户端可以是主动连接端，所述客户端可以是蓝牙低功耗设备，也可以是如手持终端、可穿戴终端、个人笔记本、平板电脑等电子设备；所述服务端可以是被动连接端，所述服务端可以是蓝牙低功耗设备，如应用于监控护理领域的血压测量装置、温度测量装置、血糖监测装置；或应用于运动和健身领域的健身器材传感器、心律测量装置、定位装置、测速装置、测重装置；或应用于智能家居领域的开关装置、照明装置、智能门锁、电动窗帘、扫地机器人等。

在一些实施例中，所述客户端获取服务端基于所述第一客户端问候消息发送的第一服务端反馈消息；所述第一服务端反馈消息包括第一反馈信息，所述第一反馈信息用于指示所述服务端确定的第二密钥协商模式。

在一些实施例中，在满足所述第一客户端问候消息中包括的第一加密套件集合中包括所述服务端支持的至少一个加密套件、所述第一客户端问候消息中包括的第一加密曲线集合包括所述服务端支持的至少一个加密曲线或所述第一客户端问候消息包括的第一协议标识集合中包括所述服务端支持的至少一个协议版本对应的协议标识，且所述服务端确定第二密钥协商模式为使用ECDH的配网协议协商密钥的情况下，所述第一反馈信息包括以下至少一种：第一加密套件、第一加密曲线、第一协议标识和第二公钥；所述第一加密套件集合包括所述第一加密套件，所述第一加密套件包括所述服务端支持的至少一个加密套件中任一个加密套件；所述第一加密曲线集合包括所述第一加密曲线，所述第一加密曲线包括所述服务端支持的至少一个加密曲线中任一个加密曲线；所述第一协议标识集合包括所述第一协议标识，所述第一协议标识包括所述服务端支持的至少一个协议版本中任一个协议版本对应的协议标识。所述第二公钥基于所述第一加密套件、第一加密曲线和第一协议标识中至少一种确定。所述第一公钥与所述第二公钥相同或不同。

在另一些实施例中，在满足所述第一客户端问候消息中包括的第一加密套件集合中包括所述服务端支持的至少一个加密套件、所述第一客户端问候消息中包括的第一加密曲线集合包括所述服务端支持的至少一个加密曲线或所述第一客户端问候消息包括的第一协议标识集合中包括所述服务端支持的至少一个协议版本对应的协议标识，且所述服务端确定第二密钥协商模式为使用ECJPAKE的配网协议协商密钥的情况下，所述第一反馈信息包括：第一加密套件、第一加密曲线、第一协议标识和第一公钥列表；所述第一加密套件集合包括所述第一加密套件，所述第一加密套件包括所述服务端支持的至少一个加密套件中任一个加密套件；所述第一加密曲线集合包括所述第一加密曲线，所述第一加密曲线包括所述服务端支持的至少一个加密曲线中任一个加密曲

线；所述第一协议标识集合包括所述第一协议标识，所述第一协议标识包括所述服务端支持的至少一个协议版本中任一个协议版本对应的协议标识。所述第二公钥基于所述第一加密套件、第一加密曲线和第一协议标识中至少一种确定。所述第一公钥列表包括服务端向客户端发送的，用于确定第一客户端共享密钥的公钥对。

在再一些实施例中，在满足以下至少一种情况：所述第一客户端问候消息中包括的第一加密套件集合中不包括所述服务端支持的至少一个加密套件、所述第一客户端问候消息中包括的第一加密曲线集合不包括所述服务端支持的至少一个加密曲线或所述第一客户端问候消息包括的第一协议标识集合中不包括所述服务端支持的至少一个协议版本对应的协议标识的情况下，所述第一反馈信息包括：第二加密套件、第二加密曲线和第二协议标识。所述第一加密套件集合不包括所述第二加密套件，所述第二加密套件包括所述服务端支持的至少一个加密套件中任一个加密套件；所述第一加密曲线集合不包括所述第二加密曲线，所述第二加密曲线包括所述服务端支持的至少一个加密曲线中任一个加密曲线；所述第一协议标识集合部包括所述第二协议标识，所述第二协议标识包括所述服务端支持的至少一个协议版本中任一个协议版本对应的协议标识。

例如，在所述第一加密套件集合中不包括所述服务端支持的加密套件、所述第一加密曲线集合中不包括所述服务端支持的曲线，且所述第一协议标识集合中不包括所述服务端支持的协议版本对应的协议标识的情况下，所述第一反馈信息包括所述服务端根据所述服务端自身性能确定的第二加密套件、第二加密曲线和第二协议标识。

或者，在所述第一加密套件集合中包括所述服务端支持的加密套件、所述第一加密曲线集合不包括所述服务端支持的加密曲线，且所述第一协议标识集合中不包括所述服务端支持的协议版本对应的协议标识的情况下，所述第一反馈信息包括所述服务端根据所述服务端自身性能确定的第二加密曲线和第二协议标识，以及所述服务端基于所述第一客户端问候消息确定的第一加密套件。

步骤 S103，若所述第一密钥协商模式包括所述第二密钥协商模式，基于所述第二密钥协商模式确定第一客户端共享密钥，根据所述第一客户端共享密钥进行目标数据传输。

在一些实施例中，在所述第一密钥协商模式包括所述第二密钥协商模式的情况下，基于所述第二密钥协商模式确定第一客户端共享密钥，根据所述第一客户端共享密钥进行目标数据传输。

在一些实施例中，所述第一密钥协商模式包括所述第二密钥协商模式包括：所述第一加密套件集合中包括所述第一加密套件、所述第一加密曲线集合包括所述第一加密曲线、所述第一协议标识集合中包括所述第一协议标识的情况下，所述第一密钥协商模式包括所述第一服务端反馈消息中携带的第一加密套件、第一加密曲线和第一协议标识对应的第二密钥协商模式。

在另一些实施例中，所述第一密钥协商模式包括所述第二密钥协商模式，还可以包括：所述第一客户端问候消息的所述协议版本字段的协议版本参数包括所述第一服务端反馈消息的所述协议版本字段的协议版本参数；所述第一客户端问候消息的所述加密套件字段的加密套件参数包括所述第一服务端反馈消息的所述加密套件字段的加密套件参数；所述第一客户端问候消息的所述加密曲线字段的加密曲线参数包括所述第一服务端反馈消息的所述加密套件字段的加密套件参数。

在一些实施例中，基于所述第二密钥协商模式确定第一客户端共享密钥包括情景 1 和情景 2，将在后续实施例中进行详细说明。

在一些实施例中，所述情景 1 包括：所述第二密钥协商模式为使用 ECDH 的配网协议协商密钥；进一步，所述基于所述第二密钥协商模式确定第一客户端共享密钥包括：使用 ECDH 的配网协议协商密钥。

在一些实施例中，所述情景 2 包括所述第二密钥协商模式为 ECJPAKE 的配网协议。进一步，所述基于所述第二密钥协商模式确定第一客户端共享密钥包括：使用 ECJPAKE 的配网协议协商密钥。

步骤 S104，若所述第一密钥协商模式不包括所述第二密钥协商模式，则发送第二客户端问候消息。

在一些实施例中，所述第一密钥协商模式不包括所述第二密钥协商模式，包括：所述第一客户端问候消息包括的第一加密套件集合中不包括所述第一服务端反馈消息中携带的第二加密套件；或者，所述第一客户端问候消息包括的第一加密曲线集合不包括所述第一反馈信息中携带的第二加密曲线；或者，所述第一客户端问候消息包括的第一协议标识集合中不包括所述第一反馈信息中携带的第二协议标识。即所述第一密钥协商模式不包括所述第一服务端反馈消息中携带的加密套件、加密曲线和协议标识对应的第二密钥协商模式。

在一些实施例中，所述客户端发送第二客户端问候消息包括：所述客户端向服务端发送第二客户端问候消息，所述第二客户端问候消息包括第二信息，所述第二信息用于指示所述客户端能够支持的第三密钥协商模式。

在一些实施例中，所述第二信息包括所述客户端能够支持的第二加密套件集合和/或所述客户端能够支持的第二加密曲线集合。所述第一加密套件集合中包括的至少一个加密套件与所述第二加密套件集合中包括的至少一个加密套件完全不相同；所述第一加密曲线集合中包括的至少一个加密曲线与所述第二加密曲线集合中包括的至少一个加密曲线完全不相同。

在一些实施例中，所述第二客户端问候消息还包括：第四公钥，所述第四公钥包括：在所述客户端能够支持 ECDH 的配网协议的情况下，所述第二加密套件集合中任一个加密套件和/或所述第二加密曲线集合中任一个加密曲线确定的公钥。

在一些实施例中，所述第二客户端问候消息还包括：第二协议标识集合，所述第二协议标识集合包括至少一个协议版本对应的协议标识，所述协议版本与所述协议标识一一对应，所述第二协议标识集合指示所述客户端支持的协议版本的集合。

在一些实施例中，所述第二客户端问候消息还包括：第二公钥列表，所述第二客户端问候消息的第二公钥列表为 NULL。

在一些实施例中，在所述服务端能够支持所述第三密钥协商模式的情况下，执行步骤 S105；在所述服务端不能支持所述第三密钥协商模式的情况下，执行步骤 S107。

步骤 S105，获取所述服务端基于所述第二客户问候消息发送的第二服务端反馈消息。

在一些实施例中，所述客户端获取所述服务端基于所述第二客户问候消息发送的第二服务端反馈消息，所述第二服务端反馈消息包括第二反馈信息，所述第二反馈信息用于指示所述服务端确定的第四密钥协商模式的具体步骤流程与步骤 S102 相似，此处不再重复赘述。

步骤 S106，基于所述第四密钥协商模式确定第二客户端共享密钥，根据所述第二客户端共享密钥进行目标数据传输。

在一些实施例中，基于所述第四密钥协商模式确定第二客户端共享密钥，根据所述第二客户端共享密钥进行目标数据传输的具体步骤流程与步骤 S103 相似，此处不再重复赘述。

步骤 S107，获取所述服务端基于所述第二客户端问候消息发送的第一警告消息，基于所述第一警告消息断开连接。

在一些实施例中，所述客户端获取所述服务端基于所述第二客户端问候消息发送的第一警告消息，基于所述第一警告消息断开连接。

在一些实施例中，所述服务端接收所述第二客户端问候消息，并确定所述服务端不支持所述第二加密套件集合中包括的至少一个加密套件；或者所述服务端不支持所述第二加密曲线集合中包括的至少一个加密曲线；或者所述服务端不支持所述第二协议标识集合中包括的至少一个协议标识对应的协议版本的情况下，所述服务端向所述客户端发送第一警告消息，所述第一警告消息用于指示断开所述客户端与所述服务端之间的连接。

在一些实施例中，所述方法还包括：步骤 S108，发送第二警告消息。

在一些实施例中，在所述客户端接收到的第一服务端反馈消息中，所述第一服务端反馈消息中包括 2 个以上加密曲线或者 2 个以上加密套件或者 2 个以上版本标识的情况下，所述客户端向服务端发送第二警告消息，并断开与服务端之间的连接；所述第二警告消息用于指示断开所述客户端和服务端之间的连接。在所述第一服务端反馈消息中包括 2 个以上加密曲线或者 2 个以上加密套件或者 2 个以上版本标识的情况下，说明所述客户端受到第三方的恶意攻击，或者服务端出现错误，所述客户端发送第二警告消息并断开与服务端之间的连接。

在另一些实施例中，在所述客户端接收到的第二服务端反馈消息中，所述第二服务端反馈消息中包括 2 个以上加密曲线或者 2 个以上加密套件或者 2 个以上版本标识的情况下，所述客户端向服务端发送第二警告消息，并断开与服务端之间的连接；所述第二警告消息用于指示断开所述客户端和服务端之间的连接。

如此，本申请实施例提供一种灵活的数据传输方式，对于性能较差且对安全要求不高的客户端，使用 ECDH 的配网协议进行数据传输；对于性能较好且对安全要求高的客户端，使用 ECJPAKE 的配网协议进行数据传输。无需由开发者或提前选择数据传输流程，客户端或服务端可以根据实际需求自行确定传输流程。并且，本申请实施例中，对于安全级别要求高的客户端，将客户端的 PIN 码与传输流程结合，提升了 PIN 码破解的难度，提升了数据传输的安全性。此外，本申请实施例中，所述客户端和/或服务端传输的每一帧消息均参与校验数据的哈希值运算，保证了握手协商数据不被篡改，提升握手协商过程的安全可靠性。

图 4 示出了本申请实施例提供的使用 ECDH 的配网协议协商共享密钥的可选流程示意图；图 5 示出了本申请实施例提供的使用 ECDH 的配网协议协商共享密钥的详细处理流程示意图，将结合图 4、图 5 进行说明。

本实施例对应步骤 S103 中的情景 1。

在一些实施例中，所述客户端基于步骤 S102，从所述服务端获取所述第一服务端反馈消息，并基于所述第一反馈信息确定第二密钥传输模式为使用 ECDH 的配网协议协商共享密钥的情况下，若所述客户端在确定所述第二公钥的第一加密曲线与确定所述第一公钥的加密曲线不相同，执行步骤 S200；若所述客户端在确定所述第二公钥的第一加密曲线与确定所述第一公钥的加密曲线相同，执行步骤 S201。

步骤 S200，客户端向服务端发送第三客户端问候消息。

在一些实施例中，所述第三客户端问候消息包括一下至少一种：第一加密套件、第一加密曲线和第一协议标识。

在一些实施例中，所述第三客户端问候消息还可以包括：第三公钥；所述第三公钥基于所述第一加密套件和/或第一加密曲线确定。

在另一些实施例中，所述第三客户端问候消息还可以包括：第三公钥与第一随机序列组合形成的第一数字序列。所述第一随机序列由所述客户端随机生成。

例如，所述第三公钥可以包括：####，所述第一随机序列可以包括******（所述第一随机序列可以是数字、大小写字母、符号组成的随机序列），所述数字序列可以包括**####****。所述第一随机序列可以只有所述客户端知晓，用于增加第一公钥传输的复杂度，防止所述第一数字序列被第三方截取后，基于所述第一数字序列获得所述第一公钥；所述第一随机序列不参与所述第一密钥的确定；所述服务端接收所述第一数字序列后，去除所述第一数字序列中的第一随机序列，获取所述第三公钥，进而确定所述第一密钥。

在一些实施例中，如图 5 所示，所述第三客户端问候消息通过 ClientHello 信息发送至所述服务端。

步骤 S201，所述客户端基于第二公钥确定第一密钥。

在一些实施例中，所述客户端基于第二公钥确定第一密钥包括：所述客户端基于所述第一服务端反馈消息中的第二公钥确定第一密钥。所述第二客户端去除所述第一服务端反馈消息中，所述服务端产生的第二随机序列，获取所述第二公钥，并基于所述第二公钥确定所述第一密钥。

在一些实施例中，所述基于第二公钥确定第一密钥的方法与相关技术中，基于公钥确定密钥的方法相同，此处不再重复赘述。

在一些实施例中，如图 5 所示，所述第一服务端反馈消息通过 ServerHello 消息发送至所述服务端。

步骤 S202，服务端基于第一公钥或第三公钥确定第一密钥。

在一些实施例中，在确定所述第二公钥的第一加密曲线与确定所述第一公钥的加密曲线相同的情况下，所

述服务端基于第一客户端问候消息中的第一公钥确定第一密钥。所述服务端去除所述第一客户端问候消息中的随机序列，获取所述第一公钥，并基于所述第一公钥确定所述第一密钥。

在另一些实施例中，在确定所述第二公钥的第一加密曲线与确定所述第一公钥的加密曲线不相同的情况下，所述服务端基于第一数字序列中的第三公钥确定第一密钥。所述服务端去除所述第一数字序列中的第一随机序列，获取所述第三公钥，并基于所述第三公钥确定所述第一密钥。

步骤 S203，服务端向客户端发送第一验证信息。

在一些实施例中，所述服务端向所述客户端发送第一验证信息，所述第一验证信息包括所述服务端的证书；所述第一验证信息用于所述客户端验证所述服务端的身份。

在一些实施例中，如图 5 所示，所述第一验证信息通过 Authenticate 信息发送至所述客户端。

在一些实施例中，所述第一验证信息可以是 X509 证书或者是服务端自定义的整数。

步骤 S204，服务端向客户端发送第一校验数据。

在一些实施例中，所述服务端向客户端发送第一校验数据，所述第一校验数据包括所述客户端发送和/或接收的每一帧消息的哈希值的集合。例如第一校验数据= hash(M1 ‖ M2 ‖...‖Mn)，其中 M1，M2……，Mn 为所述客户端发送和/或接收的每一帧消息。例如，在本实施例中，客户端向服务端发送第一客户端问候消息、服务端向客户端发送第一服务端反馈消息以及服务端向客户端发送第一验证信息的情况下，所述第一校验数据包括：所述第一客户端问候消息的哈希值、所述第一服务端反馈消息的哈希值以及所述第一验证信息的哈希值。

在一些实施例中，如图 5 所示，所述第一校验数据通过 Finished 信息发送至所述客户端。

在另一些实施例中，所述第一校验数据还可以通过：hash（hash（M1 ‖ M2 ‖...‖Mn））确定。

在一些实施例中，所述第一校验数据可以在所述客户端和服务端交换公钥后发送，包括所述第一客户端发送和/或接收的每一帧消息的哈希值的集合；也可以携带在所述服务端向所述客户端发送的每一条消息中。

在一些实施例中，所述第一校验数据携带在所述服务端向所述客户端发送的每一条消息中包括：所述服务端基于最近接收的消息中携带的第一哈希值，与所述服务端即将向客户端发送消息的第二哈希值，确定第一校验数据。所述第一校验数据可以是所述第一哈希值与所述第二哈希值之和。例如，基于第一客户端问候消息获取所述第一客户端问候消息中的第一哈希值；所述服务端基于第一服务端反馈消息确定的所述第一服务端反馈消息的第二哈希值，所述第一反馈信息中，所述第一客户端问候消息和所述第一服务端反馈消息的哈希值集合包括所述第一哈希值与所述第二哈希值的和；所述第一哈希值与所述第二哈希值长度相同。

步骤 S205，客户端向服务端发送第二验证信息。

在一些实施例中，所述客户端向所述服务端发送第二验证信息，所述第二验证信息包括所述客户端的证书；所述第二验证信息用于所述服务端验证所述客户端的身份。

在一些实施例中，如图 5 所示，所述第二验证信息通过 Authenticate 信息发送至所述服务端。

步骤 S206，客户端向服务端发送第二校验数据。

在一些实施例中，所述客户端向服务端发送第二校验数据，所述第二校验数据包括所述服务端发送和/或接收的每一帧消息的哈希值的集合。例如第二校验数据= hash(M1 ‖ M2 ‖...‖Mn)，其中 M1，M2……，Mn 为所述服务端发送和/或接收的每一帧消息。例如，在本实施例中，客户端向服务端发送第一客户端问候消息、服务端向客户端发送第一服务端反馈消息、服务端向客户端发送第一验证信息、服务端向客户端发送第一校验信息以及客户端向服务端发送第二验证信息的情况下，所述第一校验数据包括：所述第一客户端问候消息的哈希值、所述第一服务端反馈消息的哈希值、所述第一验证信息的哈希值、第二验证信息的哈希值以及第一校验数据的哈希值。

在一些实施例中，如图 5 所示，所述第二校验数据通过 Finished 信息发送至所述服务端。

在另一些实施例中，所述第二校验数据还可以通过：hash（hash（M1 ‖ M2 ‖...‖Mn））获得。

在一些实施例中，所述第二校验数据可以在所述客户端和服务端交换公钥后发送，包括所述第一客户端发送和/或接收的每一帧消息的哈希值的集合；也可以携带在所述客户端向所述服务端发送的每一条消息中。

在一些实施例中，所述第二校验数据携带在所述服务端向所述客户端发送的每一条消息中包括：所述客户端基于最近接收的消息中携带的第三哈希值，与所述客户端即将向服务端发送的消息的第四哈希值，确定第二校验数据。所述第二校验数据可以是所述第三哈希值与所述第四哈希值之和。例如，基于第一服务端反馈消息获取所述第一客户端问候消息中的第三哈希值；所述客户器基于第三客户端问候消息确定的所述第三客户端问候消息的第四哈希值，所述第三客户端问候消息中，所述第二校验数据包括所述第三哈希值与所述第四哈希值的和；所述第一哈希值与所述第二哈希值长度相同。

如此，本申请实施例提供的数据传输方式，性能较差或对安全性能要求不高的客户端和/或服务端可以使用 ECDH 的配网协议进行数据传输。无需由开发者或提前选择数据传输流程，客户端或服务端可以根据实际需求自行确定传输流程。并且，本申请实施例中，所述客户端和/或服务端传输的每一帧消息均参与校验数据的哈希值运算，保证了握手协商数据不被篡改，提升握手协商过程的安全可靠性。

图 6 示出了本申请实施例提供的使用 ECJPAKE 的配网协议协商共享密钥的可选流程示意图；图 7 示出了本申请实施例提供的使用 ECJPAKE 的配网协议协商共享密钥的详细处理流程示意图，将结合图 6、图 7 进行说明。

本实施例对应步骤 S103 中的情景 2，所述第二密钥协商模式为使用 ECJPAKE 的配网协议协商共享密钥。

步骤 S301，客户端向服务端发送第三客户端问候消息。

在一些实施例中，所述客户端基于步骤 S102，从所述服务端获取所述第一反馈信息，并基于所述第一反馈信息确定第二密钥传输模式为使用 ECJPAKE 的配网协议协商共享密钥的情况下，所述客户端向所述服务端发送第三客户端问候消息。

在一些实施例中，所述第三客户端问候消息包括一下至少一种：第一加密套件、第一加密曲线和第一协议标识。

在一些实施例中，所述第三客户端问候消息还可以包括：第二公钥列表，所述第二公钥列表包括用于确定第一服务端共享密钥的公钥对。所述第二公钥列表还可以包括所述客户端的 PIN 码。

在一些实施例中，所述第三客户端问候消息还可以包括：第四公钥。所述第四公钥基于所述第一加密套件和/或第一加密曲线确定。所述第四公钥还可以包括所述客户端的 PIN 码。

在另一些实施例中，所述第三客户端问候消息还可以包括：第四公钥与第二随机序列组合形成的第二数字序列。所述第二随机序列由所述客户端随机生成。

例如，所述第四公钥可以包括：####，所述第二随机序列可以包括******（所述第二随机序列可以是数字、大小写字母、符号组成的随机序列），所述第二数字序列可以包括**####****。所述第二随机序列可以只有所述服务端知晓，用于增加第四公钥传输的复杂度，防止所述第二数字序列被第三方截取后，基于所述第二数字序列获得所述第四公钥；所述第二随机序列不参与所述第一密钥的确定；所述服务端接收所述第二数字序列后，去除所述第二数字序列中的第二随机序列，获取所述第四公钥，进而确定所述第一密钥。

在一些实施例中，如图 7 所示，所述第三客户端问候消息通过 ClientHello 信息发送至所述服务端。

相应地，所述服务端接收所述第二公钥列表和第四公钥，基于所述第二公钥列表中包括的公钥对与所述第四公钥确定第一密钥。

步骤 S302，服务端向客户端第一服务端问候消息。

在一些实施例中，所述第一服务端问候消息包括一下至少一种：第一加密套件、第一加密曲线和第一协议标识。

在一些实施例中，所述第一服务端问候消息还可以包括：第五公钥。所述第五公钥基于所述第一加密套件和/或第一加密曲线确定。所述第五公钥列表还可以包括所述服务端的 PIN 码。

在另一些实施例中，所述第一服务端问候消息还可以包括：第五公钥与第三随机序列组合形成的第三数字序列。所述第三随机序列由所述服务端随机生成。

在一些实施例中，如图 7 所示，所述第一服务端问候消息通过 ServerHello 信息发送至所述客户端。

相应地，客户端基于第一服务端反馈消息中第一公钥列表包括的公钥对与所述第五公钥确定第一密钥。

步骤 S303，服务端向客户端发送第一校验数据。

在一些实施例中，所述服务端向所述客户端发送第一校验数据，所述第一校验数据包括所述第一客户端发送和/或接收的每一帧消息的哈希值的集合。例如第一校验数据= hash(M1 ‖ M2 ‖...‖Mn)，其中 M1，M2……，Mn 为所述第一客户端发送和/或接收的每一帧消息。例如，在本实施例中，客户端向服务端发送第一客户端问候消息和第三客户端问候消息、服务端向客户端发送第一服务端反馈消息和第一服务端问候消息的情况下，所述第一校验数据包括：所述第一客户端问候消息的哈希值、所述第三客户端问候消息的哈希值、所述第一服务端反馈消息的哈希值以及所述第一服务端问候消息的哈希值。如图 7 所示，所述第一校验数据通过 Finished 信息发送至所述第一客户端。

在另一些实施例中，所述第一校验数据还可以通过：hash（hash(M1 ‖ M2 ‖...‖Mn)）获得。

在一些实施例中，所述第一校验数据可以在所述客户端和服务端交换公钥后发送，包括所述第一客户端发送和/或接收的每一帧消息的哈希值的集合；也可以携带在所述服务端向所述客户端发送的每一条消息中。

在一些实施例中，所述第一校验数据携带在所述服务端向所述客户端发送的每一条消息中包括：所述服务端基于最近接收的消息中携带的第一哈希值，与所述服务端即将向客户端发送消息的第二哈希值，确定第一校验数据。所述第一校验数据可以是所述第一哈希值与所述第二哈希值之和。例如，基于第一客户端问候消息获取所述第一客户端问候消息中的第一哈希值；所述服务端基于第一服务端反馈消息确定的所述第一服务端反馈消息的第二哈希值，所述第一反馈信息中，所述第一校验数据包括所述第一哈希值与所述第二哈希值的和；所述第一哈希值与所述第二哈希值长度相同。

步骤 S304，客户端向服务端发送第二校验数据。

在一些实施例中，所述客户端向服务端发送第二校验数据，所述第二校验数据包括所述服务端发送和/或接收的每一帧消息的哈希值的集合。例如第二校验数据= hash(M1 ‖ M2 ‖...‖Mn)，其中 M1，M2……，Mn 为所述服务端发送和/或接收的每一帧消息。例如，在本实施例中，客户端向服务端发送第一客户端问候消息、服务端向客户端发送第一服务端反馈消息、服务端向客户端发送第一验证信息、服务端向客户端发送第一校验信息以及客户端向服务端发送第二验证信息的情况下，所述第一校验数据包括：所述第一客户端问候消息的哈希值、所述第一服务端反馈消息的哈希值、所述第一验证信息的哈希值、第二验证信息的哈希值以及第一校验数据的哈希值。

在一些实施例中，如图 7 所示，所述第二校验数据通过 Finished 信息发送至所述服务端。

在另一些实施例中，所述第二校验数据还可以通过：hash（hash（M1 ‖ M2 ‖...‖Mn））获得。

在一些实施例中，所述第二校验数据可以在所述客户端和服务端交换公钥后发送，包括所述第一客户端发送和/或接收的每一帧消息的哈希值的集合；也可以携带在所述客户端向所述服务端发送的每一条消息中。

在一些实施例中，所述第二校验数据携带在所述服务端向所述客户端发送的每一条消息中包括：所述客户端基于最近接收的消息中携带的第三哈希值，与所述客户端即将向服务端发送的消息的第四哈希值，确定第二校验数据。所述第二校验数据可以是所述第三哈希值与所述第四哈希值之和。例如，基于第一服务端反馈消息获取所述第一客户端问候消息中的第三哈希值；所述客户器基于第三客户端问候消息确定的所述第三客户端问候消息的第四哈希值，所述第三客户端问候消息中，所述第二校验数据包括所述第三哈希值与所述第四哈希值的和；所述第一哈希值与所述第二哈希值长度相同。

如此，本申请实施例提供一种灵活的数据传输方式，对于性能较好且对安全要求高的终端设备，使用ECJPAKE 的配网协议进行数据传输。无需由开发者或提前选择数据传输流程，终端设备或服务端可以根据实际需求自行确定传输流程。并且，本申请实施例中，对于安全级别要求高的终端设备，将终端设备的 PIN 码与传输流程结合，提升了 PIN 码破解的难度，提升了数据传输的安全性。此外，本申请实施例中，所述终端设备和/或服务端传输的每一帧消息均参与校验数据的哈希值运算，保证了握手协商数据不被篡改，提升握手协商过程的安全可靠性。

图 8 示出本申请实施例提供的数据传输方法的服务端侧的一种可选流程示意图，根据各个步骤进行说明。

步骤 S401，接收客户端发送的第一客户端问候消息。

在一些实施例中，所述服务端接收客户端发送的第一客户端问候消息。所述第一客户端问候消息包括第一信息，所述第一信息用于指示所述客户端能够支持的第一密钥协商模式。

在一些实施例中，所述第一密钥协商模式包括使用 ECDH 的配网协议协商密钥和/或使用 ECJPAKE 的配网协议协商密钥。

在一些实施例中，所述第一信息包括第一加密套件集合；所述第一加密套件集合包括所述客户端能够支持的至少一个加密套件的集合。

在另一些实施例中，所述第一客户端问候消息还可以包括：第一加密套件字段；所述加密套件字段用于指示所述客户端支持的部分或全部加密套件参数。

在一些实施例中，所述第一信息还可以包括第一加密曲线集合；所述第一加密曲线集合包括所述客户端能够支持的至少一个加密曲线的集合。

在另一些实施例中，所述第一客户端问候消息还可以包括：第一加密曲线字段；所述加密曲线字段用于指示所述客户端支持的部分或全部加密曲线参数。

在一些实施例中，所述第一客户端问候消息还包括：第一公钥，所述第一公钥包括：在所述客户端能够支持 ECDH 的配网协议的情况下，所述第一加密套件集合中任一个加密套件和/或所述第一加密曲线集合中任一个加密曲线确定的公钥。不同加密套件和/或加密曲线确定的公钥不同。

在一些实施例中，所述第一客户端问候消息还包括：第一协议标识集合，所述第一协议标识集合包括至少一个协议版本对应的协议标识，所述协议版本与所述协议标识一一对应，所述第一协议标识集合指示所述客户端支持的协议版本的集合。

在另一些实施例中，所述第一客户端问候消息还可以包括：协议版本字段；所述协议版本字段用于指示所述客户端支持的部分或全部协议版本参数。

在一些实施例中，所述第一客户端问候消息还包括：第一公钥列表，所述第一客户端问候消息的第一公钥列表为 NULL。

步骤 S402，根据所述第一密钥协商模式确定所述服务端选择的第二密钥协商模式，并通过所述第一服务端反馈消息发送给所述客户端。

在一些实施例中，服务端根据所述第一密钥协商模式确定所述服务端选择的第二密钥协商模式包括：所述服务端基于所述第一客户端问候消息中携带的第一加密套件集合包括的至少一个加密套件、第一加密曲线集合中包括的至少一个加密曲线和第一协议标识集合中包括的至少一个协议版本对应的协议标识，确定所述服务端支持的第二密钥模式。

在一些实施例中，在所述第一客户端问候消息中包括的第一加密套件集合中包括所述服务端支持的至少一个加密套件、所述第一客户端问候消息中包括的第一加密曲线集合包括所述服务端支持的至少一个加密曲线，且所述第一客户端问候消息包括的第一协议标识集合中包括所述服务端支持的至少一个协议版本对应的协议标识的情况下，所述服务端确定所述第二密钥协商模式对应的第一加密套件、第一加密曲线和第一协议标识，并通过第一服务端反馈消息发送给所述客户端。在所述服务端确定第二密钥协商模式为使用 ECDH 的配网协议协商密钥的情况下，所述第一服务端反馈消息还包括：第二公钥，所述第二公钥基于所述第一加密套件、第一加密曲线和第一协议标识中至少一种确定；或者，在所述服务端确定第二密钥协商模式为使用 ECJPAKE 的配网协议协商密钥的情况下，所述第一服务端反馈消息还包括：第一公钥列表，所述第一公钥列表包括服务端向客户端发送的，用于确定第一客户端共享密钥的公钥对。所述第一公钥列表还可以包括所述服务端的 PIN 码。

在另一些实施例中，在所述第一客户端问候消息中不包括的第一加密套件集合中包括所述服务端支持的至少一个加密套件，或者所述第一客户端问候消息中包括的第一加密曲线集合不包括所述服务端支持的至少一个加密曲线，或者所述第一客户端问候消息包括的第一协议标识集合中不包括所述服务端支持的至少一个协议版本对应的协议标识的情况下，所述服务端基于自身能力，向所述客户端发送第一服务端反馈消息；所述第一服务端反馈消息包括：第二加密套件、第二加密曲线和第二协议标识。所述第一加密套件集合不包括所述第二加密套件，所述第二加密套件包括所述服务端支持的至少一个加密套件中任一个加密套件；所述第一加密曲线集合不包括所述第二加密曲线，所述第二加密曲线包括所述服务端支持的至少一个加密曲线中任一个加密曲线；所述第一协议标识集合部包括所述第二协议标识，所述第二协议标识包括所述服务端支持的至少一个协议版本中任一个协议版本对应的协议标识。

步骤 S403，若所述第一密钥协商模式包括所述第二密钥协商模式，基于所述第二密钥协商模式确定第一服务端共享密钥，根据所述第一服务端共享密钥进行目标数据传输。

在一些实施例中，在所述第一密钥协商模式包括所述第二密钥协商模式的情况下，基于所述第二密钥协商模式确定第一客户端共享密钥，根据所述第一客户端共享密钥进行目标数据传输。

在一些实施例中，所述第一密钥协商模式包括所述第二密钥协商模式包括：所述第一加密套件集合中包括所述第一加密套件、所述第一加密曲线集合包括所述第一加密曲线且所述第一协议标识集合中包括所述第一协

议标识的情况下，所述第一密钥协商模式包括所述第一服务端反馈消息中携带的第一加密套件、第一加密曲线和第一协议标识对应的第二密钥协商模式。

在另一些实施例中，所述第一密钥协商模式包括所述第二密钥协商模式，还可以包括：所述第一客户端问候消息的所述协议版本字段的协议版本参数包括所述第一服务端反馈消息的所述协议版本字段的协议版本参数；所述第一客户端问候消息的所述加密套件字段的加密套件参数包括所述第一服务端反馈消息的所述加密套件字段的加密套件参数；所述第一客户端问候消息的所述加密曲线字段的加密曲线参数包括所述第一服务端反馈消息的所述加密套件字段的加密套件参数。

在一些实施例中，基于所述第二密钥协商模式确定第一客户端共享密钥包括情景1（步骤S201至步骤S206）和情景2（步骤S301至步骤S304），此处不再重复赘述。

在一些实施例中，所述情景1包括：所述第二密钥协商模式为使用ECDH的配网协议协商密钥；基于所述第二密钥协商模式确定第一客户端共享密钥包括：使用ECDH的配网协议协商密钥。

在一些实施例中，所述情景2包括所述第二密钥协商模式为ECJPAKE的配网协议。

步骤 S404，若所述第一密钥协商模式不包括所述第二密钥协商模式，接收所述客户端发送第二客户端问候消息。

在一些实施例中，所述第一密钥协商模式不包括所述第二密钥协商模式，包括：所述第一客户端问候消息包括的第一加密套件集合中不包括所述第一服务端反馈消息中携带的第二加密套件；或者，所述第一客户端问候消息包括的第一加密曲线集合不包括所述第一反馈信息中携带的第二加密曲线；或者，所述第一客户端问候消息包括的第一协议标识集合中不包括所述第一反馈信息中携带的第二协议标识。即所述第一密钥协商模式不包括所述第一服务端反馈消息中携带的加密套件、加密曲线和协议标识对应的第二密钥协商模式。

在一些实施例中，所述服务端接收所述客户端发送的第二客户端问候消息，所述客户端发送第二客户端问候消息包括：所述客户端向服务端发送第二客户端问候消息，所述第二客户端问候消息包括第二信息，所述第二信息用于指示所述客户端能够支持的第三密钥协商模式。

在一些实施例中，所述第二信息包括所述客户端能够支持的第二加密套件集合和/或所述客户端能够支持的第二加密曲线集合。所述第一加密套件集合中包括的至少一个加密套件与所述第二加密套件集合中包括的至少一个加密套件完全不相同；所述第一加密曲线集合中包括的至少一个加密曲线与所述第二加密曲线集合中包括的至少一个加密曲线完全不相同。

在一些实施例中，在一些实施例中，所述第二客户端问候消息还包括：第四公钥，所述第四公钥包括：在所述客户端能够支持ECDH的配网协议的情况下，所述第二加密套件集合中任一个加密套件和/或所述第二加密曲线集合中任一个加密曲线确定的公钥。

在一些实施例中，所述第二客户端问候消息还包括：第二协议标识集合，所述第二协议标识集合包括至少一个协议版本对应的协议标识，所述协议版本与所述协议标识一一对应，所述第二协议标识集合指示所述客户端支持的协议版本的集合。

在一些实施例中，所述第二客户端问候消息还包括：第二公钥列表，所述第二客户端问候消息的第二公钥列表为NULL。

在一些实施例中，在所述服务端能够支持所述第三密钥协商模式的情况下，执行步骤 S405；在所述服务端不能支持所述第三密钥协商模式的情况下，执行步骤S407。

步骤 S405，基于所述第二客户端问候消息发送第二服务端反馈消息，所述第二服务端反馈消息用于指示所述服务端确定的第四密钥协商模式。

在一些实施例中，所述第二服务端反馈消息用于指示所述服务端确定的第四密钥协商模式。

在一些实施例中，所述服务端基于所述第二客户端问候消息发送第二服务端反馈消息的具体步骤流程与步骤S402相似，此处不再重复赘述。

步骤 S406，基于所述第四密钥协商模式确定第二服务端共享密钥，根据所述第二客户端共享密钥进行目标数据传输。

在一些实施例中，基于所述服务端第四密钥协商模式确定第二客户端共享密钥，根据所述第二客户端共享密钥进行目标数据传输的具体步骤流程与步骤S203相似，此处不再重复赘述。

步骤S407，发送第一警告消息。

在一些实施例中，所述服务端不能支持所述第三密钥协商模式包括：所述第二客户端问候消息包括的第二加密套件集合中不包括所述服务端支持的加密套件；或者，所述第二客户端问候消息包括的第一加密曲线集合不包括所述服务端支持的加密曲线；或者，所述第二客户端问候消息包括的第一协议标识集合中不包括所述服务端支持的协议标识。

在一些实施例中，所述服务端向所述客户端发送第一告警信息，所述第一警告消息用于指示断开所述客户端和所述服务端之间的连接。

如此，本申请实施例提供一种灵活的数据传输方式，对于性能较好且对安全要求高的客户端，使用ECJPAKE的配网协议进行数据传输。无需由开发者或提前选择数据传输流程，客户端或服务端可以根据实际需求自行确定传输流程。并且，本申请实施例中，对于安全级别要求高的客户端，将客户端的PIN码与传输流程结合，提升了PIN码破解的难度，提升了数据传输的安全性。此外，本申请实施例中，所述客户端和/或服务端传输的每一帧消息均参与校验数据的哈希值运算，保证了握手协商数据不被篡改，提升握手协商过程的安全可靠性。

图9示出了本申请实施例提供的数据传输方法的一种可选流程示意图，图10示出了本申请实施例提供的数据传输方法的一种详细处理流程示意图，将结合图9、图10进行说明。

步骤 S501，客户端向服务端发送第一客户端问候消息。

在一些实施例中，所述客户端向服务端发送第一客户端问候消息，所述第一客户端问候消息包括第一信息，所述第一信息用于指示所述客户端能够支持的第一密钥协商模式。

在一些实施例中，所述第一密钥协商模式包括使用 ECDH 的配网协议协商密钥和/或使用 ECJPAKE 的配网协议协商密钥。

在一些实施例中，所述第一信息包括第一加密套件集合、第一加密曲线集合和第一协议标识集合中至少一种。所述第一加密套件集合包括所述客户端能够支持的至少一个加密套件的集合；所述第一加密曲线集合包括所述客户端能够支持的至少一个加密曲线的集合；所述第一协议标识集合包括至少一个协议版本对应的协议标识，所述协议版本与所述协议标识一一对应，所述第一协议标识集合指示所述客户端支持的协议版本的集合。

在一些实施例中，所述第一客户端问候消息通过图 10 中示出的 ClientHello 消息传输。所述 ClientHello 消息中包括的“supported_version”字段用于指示所述第一协议标识集合；所述 ClientHello 消息中包括的“cipher_suites”字段用于指示所述第一加密套件集合；所述 ClientHello 消息中包括的“supported_group”字段用于指示所述第一加密曲线集合；所述 ClientHello 消息中包括的“key_share”字段用于指示所述第一公钥。

在一些实施例中，所述 ClientHello 消息中还包括“ecjpake_key_kp_pair_list”用于指示 ECJPAKE 的配网协议使用的公钥对，在本实施例中，所述“ecjpake_key_kp_pair_list”为 NULL。

在一些实施例中，所述“key_share”字段还用于指示第四随机序列，所述第四随机序列包括所述客户端随机生成的序列；进一步，所述“key_share”字段用于指示第一公钥与第四随机序列组合形成的第四数字序列。

步骤 S502，服务端向客户端发送第一服务端反馈消息。

在一些实施例中，服务端接收客户端发送的第一客户端问候消息；根据所述第一密钥协商模式确定所述服务端选择的第二密钥协商模式包括：所述服务端基于所述第一客户端问候消息中携带的第一加密套件集合包括的至少一个加密套件、第一加密曲线集合中包括的至少一个加密曲线和第一协议标识集合中包括的至少一个协议版本对应的协议标识，确定所述服务端支持的第二密钥模式。

在一些实施例中，在所述第一客户端问候消息中包括的第一加密套件集合中包括所述服务端支持的至少一个加密套件、所述第一客户端问候消息中包括的第一加密曲线集合包括所述服务端支持的至少一个加密曲线，且所述第一客户端问候消息包括的第一协议标识集合中包括所述服务端支持的至少一个协议版本对应的协议标识的情况下，所述服务端确定所述第二密钥协商模式对应的第一加密套件、第一加密曲线和第一协议标识，并通过第一服务端反馈消息发送给所述客户端。

在一些实施例中，在所述服务端确定第二密钥协商模式为使用 ECDH 的配网协议协商密钥的情况下，所述第一服务端反馈消息还包括：第二公钥，所述第二公钥基于所述第一加密套件、第一加密曲线和第一协议标识中至少一种确定。

在一些实施例中，所述第一服务端反馈消息通过图 10 中示出的 ServerHello 消息传输。所述 ServerHello 消息中包括的“supported_version”字段用于指示所述第一协议标识；所述 ServerHello 消息中包括的“cipher_suites”字段用于指示所述第一加密套件；所述 ServerHello 消息中包括的“supported_group”字段用于指示所述第一加密曲线；所述 ServerHello 消息中包括的“key_share”字段用于指示所述第二公钥。

由于本实施例描述的是使用 ECDH 的配网协议协商密钥的流程，因此，所述 ServerHello 消息中不包括“ecjpake_key_kp_pair_list”。

在一些实施例中，所述“key_share”字段还用于指示第二随机序列，所述第二随机序列包括所述服务端随机生成的序列；进一步，所述“key_share”字段用于指示第二公钥与第二随机序列组合形成的第四数字序列。

步骤 S503，客户端接收所述第一服务端反馈消息。

在一些实施例中，所述客户端接收所述第一服务端反馈消息，判断所述第一反馈消息中包括的第一加密曲线与确定所述第一客户端问候信息中包括的第一公钥的加密曲线是否相同，在所述第一加密曲线与确定所述第一公钥的加密曲线不相同的情况下，执行步骤 S504；或者，在所述第一加密曲线与确定所述第一公钥的加密曲线相同的情况下，执行步骤 S505。

步骤 S504，客户端向服务端发送第二客户端问候消息。

在一些实施例中，所述第二客户端问候消息包括一下至少一种：第一加密套件、第一加密曲线和第一协议标识。

在一些实施例中，所述第二客户端问候消息还可以包括：第三公钥；所述第三公钥基于所述第一加密套件和/或第一加密曲线确定。

在另一些实施例中，所述第二客户端问候消息还可以包括：第三公钥与第一随机序列组合形成的第一数字序列。所述第一随机序列由所述客户端随机生成。

在一些实施例中，所述第二客户端问候消息通过图 10 中示出的 ClientHello 消息传输。所述 ClientHello 消息中包括的“supported_version”字段用于指示所述第一协议标识；所述 ClientHello 消息中包括的“cipher_suites”字段用于指示所述第一加密套件；所述 ClientHello 消息中包括的“supported_group”字段用于指示所述第一加密曲线；所述 ClientHello 消息中包括的“key_share”字段用于指示所述第三公钥。

在一些实施例中，所述 ClientHello 消息中还包括“ecjpake_key_kp_pair_list”用于指示 ECJPAKE 的配网协议使用的公钥对，在本实施例中，所述“ecjpake_key_kp_pair_list”为 NULL。

步骤 S505，服务端基于第一公钥或第三公钥确定第一密钥。

在一些实施例中，所述服务端基于第一公钥确定第一密钥包括：所述第一反馈消息中包括的第一加密曲线与确定所述第一客户端问候信息中包括的第一公钥的加密曲线相同的情况下，所述服务端基于所述第一客户端问候消息确定第一密钥。

在一些实施例中，所述服务端基于第一客户端问候消息中包括的“key_share”字段指示的第一公钥确定第一密钥；或者，所述服务端去除所述“key_share”字段指示的第四数字序列中的第四随机序列，基于所述第四数字序列中包括的第一公钥确定第一密钥。

在另一些实施例中，所述服务端基于第一公钥确定第一密钥包括：所述第一反馈消息中包括的第一加密曲线与确定所述第一客户端问候信息中包括的第一公钥的加密曲线不相同的情况下，所述服务端基于第二客户端问候消息确定第一密钥。

在一些实施例中，所述服务端基于第二客户端问候消息中包括的“key_share”字段指示的第三公钥确定第一密钥；或者，所述服务端去除所述“key_share”字段指示的第一数字序列中的第一随机序列，基于所述第一数字序列中包括的第三公钥确定第一密钥。

在一些实施例中，步骤 S501 至步骤 S505 可以是 Epoch0 阶段执行的流程，所述客户端与所述服务端之间传输的消息不加密。

步骤 S506，服务端向客户端发送第一验证信息。

所述步骤 S506 的具体步骤与步骤 S203 相同，此处不再重复赘述。

步骤 S507，服务端向客户端发送第一校验数据。

所述步骤 S507 的具体步骤与步骤 S204 相同，此处不再重复赘述。

步骤 S508，客户端向服务端发送第二验证信息。

所述步骤 S508 的具体步骤与步骤 S205 相同，此处不再重复赘述。

步骤 S509，客户端向服务端发送第二校验数据。

所述步骤 S509 的具体步骤与步骤 S206 相同，此处不再重复赘述。

客户端向服务端发送第二验证信息。

在一些实施例中，步骤 S506 至步骤 S509 可以是 Epoch1 阶段执行的流程，所述客户端与所述服务端之间传输的消息通过第一密钥加密和/或解密。

步骤 S510，客户端确定第一客户端共享密钥，并根据第一客户端共享密钥进行目标数据传输。

在一些实施例中，所述客户端确定第一客户端共享密钥包括：所述客户端基于第一公钥、第二公钥、第三公钥和第一密钥中至少一种，确定第一客户端共享密钥。

在一些实施例中，所述第一校验数据验证通过，说明所述客户端发送和/或接收的消息未被篡改，所述客户端可以基于第一客户端共享密钥传输目标数据。

步骤 S511，服务端确定第一服务端共享密钥，并根据第一服务端共享密钥进行目标数据传输。

在一些实施例中，所述服务端确定第一服务端共享密钥包括：所述服务端基于第一公钥、第二公钥、第三公钥和第一密钥中至少一种，确定第一服务端共享密钥。

在一些实施例中，所述第二校验数据验证通过，说明所述服务端发送和/或接收的消息未被篡改，所述服务端可以基于第一服务端共享密钥传输目标数据。

在一些实施例中，所述第一客户端共享密钥与所述第一服务端共享密钥相同或不同。

在一些实施例中，所述第一客户端共享密钥基于所述第一密钥确定，例如所述第一客户端共享密钥可以包括所述第一密钥加密后确定的数据。

在一些实施例中，在一些实施例中，步骤 S510 至步骤 S511 可以是 Epoch2 阶段执行的流程，所述客户端传输的消息通过第一客户端共享密钥加密和/或解密；所述服务端传输的消息通过第一服务端共享密钥加密和/或解密。

在一些实施例中，所述方法还包括：所述客户端发送和/或接收的经所述第一客户端共享密钥加密的目标数据的次数大于第一阈值的情况下，所述客户端与服务端重新确定客户端共享密钥。

在一些实施例中，所述客户端发送和/或接收的经所述第一客户端共享密钥加密的目标数据的次数大于第一阈值，包括：第一客户端共享密钥加密次数过多，多次传输会提升所述第一客户端共享密钥被破译的风险，在所述第一客户端共享密钥加密的目标数据的次数大于第一阈值的情况下，所述客户端和所述服务端更新第一密钥和/或第一客户端共享密钥。

如此，本申请实施例提供一种灵活的数据传输方式，无需由开发者或提前选择数据传输流程，客户端或服务端可以根据实际需求自行确定传输流程。此外，本申请实施例中，所述客户端和/或服务端传输的每一帧消息均参与校验数据的哈希值运算，保证了握手协商数据不被篡改，提升握手协商过程的安全可靠性。

图 11 示出了本申请实施例提供的数据传输方法的又一种可选流程示意图，图 12 示出了本申请实施例提供的数据传输方法的又一种详细处理流程示意图，将结合图 11、图 12 进行说明。

步骤 S601，客户端向服务端发送第一客户端问候消息。

所述步骤 S601 的具体流程与步骤 S501 相同，此处不再重复赘述。

步骤 S602，服务端接收客户端发送的第一客户端问候消息。

在一些实施例中，服务端接收客户端发送的第一客户端问候消息；根据所述第一密钥协商模式确定所述服务端选择的第二密钥协商模式，并通过所述第一服务端反馈消息发送给所述客户端。

在一些实施例中，服务端根据所述第一密钥协商模式确定所述服务端选择的第二密钥协商模式包括：所述服务端基于所述第一客户端问候消息中携带的第一加密套件集合包括的至少一个加密套件、第一加密曲线集合中包括的至少一个加密曲线和第一协议标识集合中包括的至少一个协议版本对应的协议标识，确定所述服务端支持的第二密钥模式。

在一些实施例中，在所述第一客户端问候消息中包括的第一加密套件集合中包括所述服务端支持的至少一个加密套件、所述第一客户端问候消息中包括的第一加密曲线集合包括所述服务端支持的至少一个加密曲线，

且所述第一客户端问候消息包括的第一协议标识集合中包括所述服务端支持的至少一个协议版本对应的协议标识的情况下，所述服务端确定所述第二密钥协商模式对应的第一加密套件、第一加密曲线和第一协议标识，并通过第一服务端反馈消息发送给所述客户端。

在一些实施例中，在所述服务端确定第二密钥协商模式为使用 ECJPAKE 的配网协议协商密钥的情况下，所述第一服务端反馈消息还包括：第一公钥列表，所述第一公钥基于所述第一加密套件、第一加密曲线和第一协议标识中至少一种确定。所述第一公钥列表还可以包括所述服务端的 PIN 码。

在一些实施例中，所述第一服务端反馈消息通过图 12 中示出的 HelloRetryRequest 消息传输。所述 HelloRetryRequest 消息中包括的“supported_version”字段用于指示所述第一协议标识；所述 HelloRetryRequest 消息中包括的“cipher_suites”字段用于指示所述第一加密套件；所述 HelloRetryRequest 消息中包括的“supported_group”字段用于指示所述第一加密曲线。

在一些实施例中，所述 HelloRetryRequest 消息中包括的“ecjpake_key_kp_params”字段用于指示所述第二公钥；或者，所述 HelloRetryRequest 消息中包括的“key_share”字段用于指示所述第二公钥。

由于本实施例描述的是使用 ECJPAKE 的配网协议协商密钥的流程，因此，所述 HelloRetryRequest 消息中包括“ecjpake_key_kp_pair_list”，所述“ecjpake_key_kp_pair_list”用于指示第一公钥列表。

步骤 S603，客户端向服务端发送第三客户端问候消息。

在一些实施例中，所述第三客户端问候消息包括一下至少一种：第一加密套件、第一加密曲线和第一协议标识。

在一些实施例中，所述第三客户端问候消息还可以包括：第二公钥列表和第六公钥；所述第六公钥基于所述第一加密套件和/或第一加密曲线确定。所述第二公钥列表还可以包括所述客户端的 PIN 码。

在另一些实施例中，所述第三客户端问候消息还可以包括：第六公钥与第一随机序列组合形成的第一数字序列。所述第一随机序列由所述客户端随机生成。所述第六公钥还可以包括所述客户端的 PIN 码。

在一些实施例中，所述第三客户端问候消息通过图 12 中示出的 ClientHello 消息传输。所述 ClientHello 消息中包括的“supported_version”字段用于指示所述第一协议标识；所述 ClientHello 消息中包括的“cipher_suites”字段用于指示所述第一加密套件；所述 ClientHello 消息中包括的“supported_group”字段用于指示所述第一加密曲线。

在一些实施例中，在一些实施例中，所述 ClientHello 消息中包括的“ecjpake_key_kp_params”字段用于指示所述第六公钥；或者，所述 ClientHello 消息中包括的“key_share”字段用于指示所述第六公钥。

在一些实施例中，所述 ClientHello 消息中还包括“ecjpake_key_kp_pair_list”用于指示 ECJPAKE 的配网协议使用的第二公钥列表。

步骤 S604，服务端向客户端第一服务端问候消息。

在一些实施例中，所述第一服务端问候消息包括一下至少一种：第一加密套件、第一加密曲线和第一协议标识。

在一些实施例中，所述第一服务端问候消息还可以包括：第五公钥。所述第五公钥基于所述第一加密套件和/或第一加密曲线确定。所述第五公钥还可以包括所述服务端的 PIN 码。

在另一些实施例中，所述第一服务端问候消息还可以包括：第五公钥与第三随机序列组合形成的第三数字序列。所述第三随机序列由所述服务端随机生成。

在一些实施例中，所述第一服务端问候消息通过图 12 中示出的 ServerHello 消息传输。所述 ServerHello 消息中包括的“supported_version”字段用于指示所述第一协议标识；所述 ServerHello 消息中包括的“cipher_suites”字段用于指示所述第一加密套件；所述 ServerHello 消息中包括的“supported_group”字段用于指示所述第一加密曲线。

在一些实施例中，在一些实施例中，所述 ServerHello 消息中包括的“ecjpake_key_kp_params”字段用于指示所述第五公钥；或者，所述 ServerHello 消息中包括的“key_share”字段用于指示所述第五公钥。

在一些实施例中，步骤 S601 至步骤 S604 可以是 Epoch0 阶段执行的流程，所述客户端与所述服务端之间传输的消息不加密。

步骤 S605，服务端向客户端发送第一校验数据。

所述步骤 S605 的具体流程与步骤 S303 相同，此处不再重复赘述。

步骤 S606，客户端向服务端发送第二校验数据。

所述步骤 S606 的具体流程与步骤 S303 相同，此处不再重复赘述。

在一些实施例中，步骤 S605 至步骤 S606 可以是 Epoch1 阶段执行的流程，所述客户端与所述服务端之间传输的消息通过第一密钥加密和/或解密。

步骤 S607，客户端确定第一客户端共享密钥，并根据第一客户端共享密钥进行目标数据传输。

在一些实施例中，所述客户端确定第一客户端共享密钥包括：所述客户端基于第五公钥、第六公钥、第一公钥列表、第二公钥列表和第一密钥中至少一种，确定第一客户端共享密钥。

在一些实施例中，所述第一校验数据验证通过，说明所述客户端发送和/或接收的消息未被篡改，所述客户端可以基于第一客户端共享密钥传输目标数据。

步骤 S608，服务端确定第一服务端共享密钥，并根据第一服务端共享密钥进行目标数据传输。

在一些实施例中，所述服务端确定第一服务端共享密钥包括：所述服务端基于第五公钥、第六公钥、第一公钥列表、第二公钥列表和第一密钥中至少一种，确定第一服务端共享密钥。

在一些实施例中，所述第二校验数据验证通过，说明所述服务端发送和/或接收的消息未被篡改，所述服务端可以基于第一服务端共享密钥传输目标数据。

在一些实施例中，所述第一客户端共享密钥与所述第一服务端共享密钥相同或不同。

在一些实施例中，所述第一客户端共享密钥基于所述第一密钥确定，例如所述第一客户端共享密钥可以包括所述第一密钥加密后确定的数据。

在一些实施例中，在一些实施例中，步骤 S510 至步骤 S511 可以是 Epoch2 阶段执行的流程，所述客户端传输的消息和/或数据通过第一客户端共享密钥加密解密；所述服务端传输的消息和/或数据通过第一服务端共享密钥加密解密

在一些实施例中，所述方法还包括：所述客户端发送和/或接收的经所述第一客户端共享密钥加密的目标数据的次数大于第一阈值的情况下，所述客户端与服务端重新确定客户端共享密钥。

在一些实施例中，所述客户端发送和/或接收的经所述第一客户端共享密钥加密的目标数据的次数大于第一阈值，包括：第一客户端共享密钥加密次数过多，多次传输会提升所述第一客户端共享密钥被破译的风险，在所述第一客户端共享密钥加密的目标数据的次数大于第一阈值的情况下，所述客户端和所述服务端更新第一密钥和/或第一客户端共享密钥。如此，本申请实施例提供一种灵活的数据传输方式，对于性能较好且对安全要求高的客户端，使用 ECJPAKE 的配网协议进行数据传输。无需由开发者或提前选择数据传输流程，客户端或服务端可以根据实际需求自行确定传输流程。并且，本申请实施例中，对于安全级别要求高的客户端，将客户端的 PIN 码与传输流程结合，提升了 PIN 码破解的难度，提升了数据传输的安全性。此外，本申请实施例中，所述客户端和/或服务端传输的每一帧消息均参与校验数据的哈希值运算，保证了握手协商数据不被篡改，提升握手协商过程的安全可靠性。

图 13 示出了本申请实施例提供的数据传输方法的再一种可选流程示意图，图 14 示出了本申请实施例提供的数据传输方法的再一种详细处理流程示意图，将结合图 13、图 14 进行说明。

步骤 S801，客户端向服务端发送第一客户端问候消息。

所述步骤 S801 的具体流程与步骤 S501 相同，此处不再重复赘述。

步骤 S802，服务端向客户端发送第一服务端反馈消息。

在一些实施例中，在所述第一客户端问候消息中不包括的第一加密套件集合中包括所述服务端支持的至少一个加密套件，或者所述第一客户端问候消息中包括的第一加密曲线集合不包括所述服务端支持的至少一个加密曲线，或者所述第一客户端问候消息包括的第一协议标识集合中不包括所述服务端支持的至少一个协议版本对应的协议标识的情况下，所述服务端基于自身能力，向所述客户端发送第一服务端反馈消息；所述第一服务端反馈消息包括：第二加密套件、第二加密曲线和第二协议标识。所述第一加密套件集合不包括所述第二加密套件，所述第二加密套件包括所述服务端支持的至少一个加密套件中任一个加密套件；所述第一加密曲线集合不包括所述第二加密曲线，所述第二加密曲线包括所述服务端支持的至少一个加密曲线中任一个加密曲线；所述第一协议标识集合部包括所述第二协议标识，所述第二协议标识包括所述服务端支持的至少一个协议版本中任一个协议版本对应的协议标识。

在一些实施例中，所述第一服务端反馈消息通过图 14 中示出的 HelloRetryRequest 消息传输。所述 HelloRetryRequest 消息中包括的“supported_version”字段用于指示所述第二协议标识；所述 HelloRetryRequest 消息中包括的“cipher_suites”字段用于指示所述第二加密套件；所述 HelloRetryRequest 消息中包括的“supported_group”字段用于指示所述第二加密曲线。

在一些实施例中，所述 HelloRetryRequest 消息中包括的“ecjpake_key_kp_params”字段用于指示所述第二公钥；或者，所述 HelloRetryRequest 消息中包括的“key_share”字段用于指示所述第二公钥。

在一些实施例中，在所述第一密钥协商模式包括所述第二加密套件、所述第二加密曲线和所述第二协议标识对应的第二密钥协商模式的情况下，执行步骤 S503 至步骤 S511 的流程，或者，执行步骤 S603 至步骤 S608 的流程。在所述第一密钥协商模式不包括所述第二加密套件、所述第二加密曲线和所述第二协议标识对应的第二密钥协商模式的情况下，执行步骤 S803。

步骤 S803，客户端向服务端发送第二客户端问候信息。

在一些实施例中，所述客户端发送第二客户端问候消息包括：所述客户端向服务端发送第二客户端问候消息，所述第二客户端问候消息包括第二信息，所述第二信息用于指示所述客户端能够支持的第三密钥协商模式。

在一些实施例中，所述第二信息包括所述客户端能够支持的第二加密套件集合和/或所述客户端能够支持的第二加密曲线集合。所述第一加密套件集合中包括的至少一个加密套件与所述第二加密套件集合中包括的至少一个加密套件完全不相同；所述第一加密曲线集合中包括的至少一个加密曲线与所述第二加密曲线集合中包括的至少一个加密曲线完全不相同。

在一些实施例中，在一些实施例中，所述第二客户端问候消息还包括：第四公钥，所述第四公钥包括：在所述客户端能够支持 ECDH 的配网协议的情况下，所述第二加密套件集合中任一个加密套件和/或所述第二加密曲线集合中任一个加密曲线确定的公钥。

在一些实施例中，所述第二客户端问候消息还包括：第二协议标识集合，所述第二协议标识集合包括至少一个协议版本对应的协议标识，所述协议版本与所述协议标识一一对应，所述第二协议标识集合指示所述客户端支持的协议版本的集合。

在一些实施例中，所述第二客户端问候消息还包括：第二公钥列表，所述第二客户端问候消息的第二公钥列表为空（NULL）。

在一些实施例中，所述第二客户端问候消息通过图 14 中示出的 ClientHello 消息传输。所述 ClientHello 消息中包括的“supported_version”字段用于指示所述第二协议标识集合；所述 ClientHello 消息中包括的“cipher_suites”字段用于指示所述第二加密套件集合；所述 ClientHello 消息中包括的“supported_group”字段用于指示所述第二加密曲线集合。

在一些实施例中，所述 ClientHello 消息中包括的“ecjpake_key_kp_params”字段用于指示所述第四公钥；或者，所述 ClientHello 消息中包括的“key_share”字段用于指示所述第四公钥。

在一些实施例中，所述 ClientHello 消息中还包括“ecjpake_key_kp_pair_list”用于指示 ECJPAKE 的配网协议使用的公钥对，在本实施例中，所述“ecjpake_key_kp_pair_list”为 NULL。

在一些实施例中，在所述第三密钥协商模式包括所述服务端能够支持的加密套件、加密曲线和协议标识对应的第四密钥协商模式的情况下，执行步骤 S804。在所述第三密钥协商模式不包括所述服务端能够支持的加密套件、加密曲线和协议标识对应的第四密钥协商模式的情况下，执行步骤 S805。

步骤 S804，服务端发送第二服务端反馈信息。

在一些实施例中，在所述第二客户端问候消息中包括的第二加密套件集合中包括所述服务端支持的至少一个加密套件、所述第二客户端问候消息中包括的第二加密曲线集合包括所述服务端支持的至少一个加密曲线，且所述第二客户端问候消息包括的第二协议标识集合中包括所述服务端支持的至少一个协议版本对应的协议标识的情况下，所述服务端确定所述第四密钥协商模式对应的第二加密套件、第二加密曲线和第二协议标识，并通过第二服务端反馈消息发送给所述客户端。在所述服务端确定第四密钥协商模式为使用 ECDH 的配网协议协商密钥的情况下，所述第二服务端反馈消息还包括：第五公钥，所述第五公钥基于所述第二加密套件、第二加密曲线和第二协议标识中至少一种确定；或者，在所述服务端确定第二密钥协商模式为使用 ECJPAKE 的配网协议协商密钥的情况下，所述第二服务端反馈消息还包括：第三公钥列表，所述第三公钥列表包括服务端向客户端发送的，用于确定第一客户端共享密钥的公钥对。

在一些实施例中，所述第一服务端反馈消息通过图 14 中示出的 ServerHello 消息传输。所述 ServerHello 消息中包括的“supported_version”字段用于指示所述第二协议标识；所述 ServerHello 消息中包括的“cipher_suites”字段用于指示所述第二加密套件；所述 ServerHello 消息中包括的“supported_group”字段用于指示所述第二加密曲线。

在一些实施例中，所述 ClientHello 消息中包括的“ecjpake_key_kp_params”字段用于指示所述第五公钥；或者，所述 ClientHello 消息中包括的“key_share”字段用于指示所述第五公钥。

在一些实施例中，若所述客户端与服务端使用 ECDH 的配网协议协商密钥的流程，所述 ServerHello 消息中不包括“ecjpake_key_kp_pair_list”；若所述客户端与服务端使用 ECJPAKE 的配网协议协商密钥的流程，所述 ServerHello 消息中还包括“ecjpake_key_kp_pair_list”，所述“ecjpake_key_kp_pair_list”用于指示第一公钥列表。

在一些实施例中，所述方法还包括：执行步骤 S503 至步骤 S511 的流程，或者，执行步骤 S603 至步骤 S608 的流程。

步骤 S805，服务端发送第一警告消息。

在一些实施例中，所述服务端不能支持所述第三密钥协商模式包括：所述第二客户端问候消息包括的第二加密套件集合中不包括所述服务端支持的加密套件；或者，所述第二客户端问候消息包括的第一加密曲线集合不包括所述服务端支持的加密曲线；或者，所述第二客户端问候消息包括的第一协议标识集合中不包括所述服务端支持的协议标识。

在一些实施例中，所述服务端向所述客户端发送第一告警信息，所述第一警告消息用于指示断开所述客户端和所述服务端之间的连接。

在一些实施例中，所述方法还包括：

步骤 S806，客户端发送第二警告消息。

在一些实施例中，在所述客户端接收到的服务端发送的消息中包括 2 个以上加密曲线或者 2 个以上加密套件或者 2 个以上版本标识的情况下，所述客户端向服务端发送第二警告消息，并断开与服务端之间的连接；所述第二警告消息用于指示断开所述客户端和服务端之间的连接。

在一些实施例中，所述服务端发送的消息包括：第一服务端反馈消息和/或第一服务端问候消息。

如此，本申请实施例提供一种灵活的数据传输方式，对于性能较差且对安全要求不高的客户端，使用 ECDH 的配网协议进行数据传输；对于性能较好且对安全要求高的客户端，使用 ECJPAKE 的配网协议进行数据传输。无需由开发者或提前选择数据传输流程，客户端或服务端可以根据实际需求自行确定传输流程。并且，本申请实施例中，对于安全级别要求高的客户端，将客户端的 PIN 码与传输流程结合，提升了 PIN 码破解的难度，提升了数据传输的安全性。此外，本申请实施例中，所述客户端和/或服务端传输的每一帧消息均参与校验数据的哈希值运算，保证了握手协商数据不被篡改，提升握手协商过程的安全可靠性。

图 15 示出了本申请实施例提供的数据传输方法的还一种可选流程示意图。

步骤 S901，客户端向服务端发送客户端问候消息。

在一些实施例中，在一轮协商中第一次发送所述客户端问候消息时，所述客户端问候消息包括以下至少一项：协议版本字段：用于指示所述客户端支持的部分或全部协议版本参数；所述加密套件字段用于指示所述客户端支持的部分或全部加密套件参数；所述加密曲线字段用于指示所述客户端支持的部分或全部加密曲线参数；所述第一公钥字段用于指示所述客户端的第一公钥；所述第二公钥字段为空或不包括所述第二公钥字段。

步骤 S902，接收服务端基于所述客户端问候消息发送的请求重发问候消息或服务端问候消息或警告消息。

在一些实施例中，当所述请求重发问候消息为所述服务端在一轮协商中第一次发送的请求重发问候消息，则再次发送所述客户端问候消息；和/或，当所述请求重发问候消息为所述服务端在一轮协商中第二次发送的请求重发问候消息，则发送警告消息并断开连接；和/或，接收到所述服务端发送的服务端问候消息缺少任一必选字段时发送警告消息并断开连接；和/或，接收到所述服务端发送的服务端问候消息的协议版本号字段中包括多个协议版本时发送警告消息并断开连接；和/或，接收到所述服务端发送的服务端问候消息的加密套件字段中包括多个加密套件参数或不支持加密套件参数时发送警告消息并断开连接；和/或，接收到所述服务端

发送的服务端问候消息的加密曲线字段中包括多个加密曲线参数或不支持加密曲线参数时发送警告消息并断开连接；和/或，接收到所述服务端发送的服务端问候消息的第一公钥字段中包括多个第一公钥时发送警告消息并断开连接。

步骤 S903，基于服务端发送的公钥生成客户端共享密钥。

在一些实施例中，当所述客户端能够支持所述服务端发送的所述请求重发反馈消息或所述服务端问候消息指示的密钥协商模式时，基于所述请求重发反馈消息或所述服务端问候消息携带的所述服务端公钥生成客户端共享密钥。

如此，本申请实施例提供一种灵活的数据传输方式，无需由开发者或提前选择数据传输流程，客户端或服务端可以根据实际需求自行确定传输流程。并且，本申请实施例中，所述客户端和/或服务端传输的每一帧消息均参与校验数据的哈希值运算，保证了握手协商数据不被篡改，提升握手协商过程的安全可靠性。

图 16 示出了本申请实施例提供的数据传输方法的另一种可选流程示意图，将根据各个步骤进行说明。

步骤 S1001，第一端通过握手消息与第二端协商共享密钥。

在一些实施例中，所述第一端为客户端的情况下，所述第二端为服务端；或者，所述第一端为服务端的情况下，所述第二端为客户端。

所述客户端通过握手消息与服务端协商共享密钥包括步骤 S101 至步骤 S108，或者包括步骤 S200 至步骤 S206，或者包括步骤 S301 至步骤 S304，或者包括步骤 S401 至步骤 S407，或者包括步骤 S501 至步骤 S511，或者包括步骤 S601 至步骤 S608，或者包括步骤 S801 至步骤 S806，或者包括步骤 S901 至步骤 S903 以及图 5、图 7、图 10、图 12 和图 14 中示出的具体流程，此处不再重复赘述。相应地，所述握手消息包括第一客户端问候消息、第一服务端反馈消息、第二客户端问候消息、第一服务端问候消息、第三客户端问候消息、第一警告消息和第二警告消息至少一种。

在一些实施例中，所述握手消息包括握手问候消息和握手应答消息；所述握手问候消息包括：第一客户端问候消息、第二客户端问候消息和第三客户端问候消息中至少一种；所述握手应答消息包括：第一服务端问候消息；所述重发请求消息包括第一服务端反馈消息。

所述握手问候消息或所述握手应答消息的消息载荷中包括公钥列表字段，所述公钥列表字段的值为空 NULL，所述空值用于确定所述第二端是否支持目标加密套件。所述公钥列表字段通过“ecjpake_key_kp_pair_list”字段指示。

在一些实施例中，所述方法还包括：在协商密钥过程中，所述第一端对所述握手消息进行校验得到校验值。

在一些实施例中，所述握手消息包括握手完成消息，用于指示完成所述密钥的协商流程，其中，所述握手完成消息携带所述校验值。

在一些实施例中，所述握手完成消息可以包括步骤 S204、步骤 S303、步骤 S507、步骤 S605 中的第一校验数据，和/或步骤 S205、步骤 S304、步骤 S509、步骤 S606 中的第二校验数据；相应地所述校验值可以是所述第一校验数据和/或所述第二校验数据中携带的哈希值。

步骤 S1002，所述第一端通过内容消息与所述第二端传输应用数据，所述内容消息通过使用所述共享密钥进行加密和解密。

在本申请实施例中，第一端通过握手消息与第二端协商共享密钥；所述第一端通过内容消息与所述第二端传输应用数据，所述内容消息通过使用所述共享密钥进行加密和解密；其中，所述握手消息和所述内容消息具有相同的消息格式，所述消息格式包括：消息序号和消息载荷；所述消息序号包括密钥代数标识和消息计数标识，其中，所述密钥代数标识通过小于第一位数的比特信息进行表征，所述消息计数标识通过小于第二位数的比特信息进行表征；如此，可以灵活地确定密钥协商模式，进行共享密钥协商，进而通过协商的共享密钥传输目标数据。

在一些实施例中，所述内容消息包括所述第一端和所述第二端传输的目标数据。所述第一端和所述第二端通过使用所述共享密钥对所述第一端和第二端传输的内容消息进行加密和解密。比如，第一端利用共享密钥对待传输的内容消息进行加密，然后将加密后的内容消息传输给第二端，第二端接收到该加密的内容消息后，利用共享密钥对该加密的内容消息进行解密。

在一些实施例中，所述内容消息通过使用所述共享密钥进行加密，包括：使用所述共享密钥对所述内容消息中的消息载荷进行加密。所述消息载荷包括：协议版本字段、加密套件字段、共享密钥字段、加密曲线字段。所述协议版本字段包括图 3 至图 16 的流程中的“supported_version”字段；所述加密套件字段包括图 3 至图 16 的流程中的“cipher_suites”字段；所述共享密钥字段包括图 3 至图 16 的流程中的“key_share”字段、“ecjpake_key_kp_pair_list”字段和“ecjpake_key_kp_params”字段中至少一种；所述加密曲线字段包括图 3 至图 16 的流程中的“supported_group”字段。

在一些实施例中，所述握手问候消息包括图 3 至图 16 的流程中包括的第一客户端问候消息、第二客户端问候消息、第三客户端问候消息；所述握手应答消息包括图 3 至图 16 的流程中包括的第一服务端问候消息；所述重发请求消息包括图 3 至图 16 的流程中包括的第一服务端反馈消息和/或第二服务端反馈消息；所述认证数据消息包括图 3 至图 16 的流程中包括的第一验证信息和/或第二验证信息；所述握手完成消息包括图 3 至图 16 的流程中包括的第一校验数据和/或第二校验数据。

在一些实施例中，如图 3 至图 16 的流程中包括的第一客户端问候消息、第一服务端反馈消息、第二客户端问候消息、第一服务端问候消息、第三服务端问候消息具有相同的消息格式，所述消息格式包括：消息计数和消息载荷；所述消息计数包括密钥代数（Epoch）标识和消息计数（Seq），其中，所述密钥代数通过小于第一位数的比特信息进行表征，所述消息计数通过小于第二位数的比特信息进行表征。

在本申请实施例中，对于第一位数和第二位数的大小不做限定，可以是任意值。在一些实施例中，所述第

一位数可以是 2；所述第二位数可以是 8。

在一些实施例中，所述第一客户端问候消息、第一服务端反馈消息、第二客户端问候消息、第一服务端问候消息和第三服务端问候消息的消息载荷中至少包括以下字段中的一种或多种：协议版本字段、加密套件字段、共享密钥字段、以及加密曲线字段。

其中，所述密钥代数使用 E 表示，所述 E 表征 Epoch 的最低位；所述 Epoch 用于指示当前使用的对称密钥的形式，如表 1 所示，Epoch 0 的情况下，不使用密钥；Epoch 1 的情况下，使用第一密钥；Epoch 2 的情况下，使用第二密钥等。

在一些实施例中，所述第一端通过所述握手问候消息、所述握手应答消息或所述重发请求消息与所述第二端协商密钥时，所述密钥代数标识为 a；所述第一端通过所述认证数据消息或所述握手完成消息与所述第二端协商密钥时，所述密钥代数标识为 a+1；所述第一端通过所述内容消息与所述第二端传输应用数据时，所述密钥代数标识为 a+2 至 a+N；其中，a 为整数，N 为大于或等于 2 的整数。传输在先的应用数据的密钥代数小于传输在后的应用数据的密钥代数。

例如，在 a=0 的情况下，步骤 S501 至步骤 S505 可以是 Epoch0 阶段执行的流程，所述客户端与所述服务端之间传输的消息不加密；步骤 S506 至步骤 S509 可以是 Epoch1 阶段执行的流程，所述客户端与所述服务端之间传输的消息通过第一密钥加密和/或解密；传输所述应用数据可以是 Epoch2 至 EpochN，所述客户端与所述服务端之间传输的消息通过共享密钥加密和/或解密。

在一些实施例中，所述消息计数包括 8 个字节，每个字节占 8 位（8 比特信息），其中，所述消息计数的前 2 个字节表征 Epoch（占 16 位），本申请实施例中，E 通过小于第一位数的比特信息表征；所述 E 可以是对应 Epoch 的最低 1 位（占用 1 比特），或者，所述 E 可以是对应 Epoch 的最低 0 位（不占用比特信息）。

在一些实施例中，所述握手问候消息或所述握手应答消息的消息载荷中包括 ecjpake_key_kp_pair_list 字段，所述公钥列表字段的值为空 NULL，所述空值用于确定所述第二端是否支持目标加密套件。

在一些实施例中，所述第二端基于所述握手问候消息返回所述重发请求消息，其中，所述重发请求消息中的加密套件字段配置为所述目标加密套件。

表 1

Epoch	阶段（Stage）	客户端密钥	服务端密钥
0	Hello	不加密	不加密
1	Handshake	ClientHandshake Key	ServerHandshake Key
2	Application	ClientHandshake Key0	ServerHandshake Key0
……	……	……	……
N	Application	ClientHandshake KeyN	ServerHandshake KeyN

在不同的阶段，所述客户端和服务端端发送和/或接收的数据，使用不同的密钥进行加密、解密。当握手完成后，进入 Epoch 2，后续如果需要更新密钥，可以由客户端和服务端端同步更新，即进入 Epoch N。

图 17 示出了本申请实施例提供的客户端与服务端传输的消息的内容的可选结构示意图。

图 17 中，Seq 为消息计数，用于所述 Seq 对应的消息是所述客户端和/或服务端传输的信息的序号（即所述 Seq 对应的消息是所述客户端和/或服务端传输的第几条消息）。

在一些实施例中，所述消息计数包括 8 个字节，每个字节占 8 位（8 比特信息），其中，所述消息计数的后 6 个字节表征 Seq（占 48 位），本申请实施例中，所述消息计数标识通过所述消息计数的最低第三位数的比特信息表征；消息计数标识的值等于在前传输的相邻的消息计数标识的值与 1 的和。所述第三位数小于所述第二位数。在所述第二位数为 8 的情况下，所述第三位数可以是 7，相应地，所述消息计数标识为所述消息计数的最低 7 位；或者，在所述第二位数为 8 的情况下，所述第三位数可以是 6，相应地，所述消息计数标识为所述消息计数的最低 6 位。也就是说，本申请实施例中，使用小于或等于 8 位比特信息表征所述消息序号，相比目前标准 ECJPAKE 的配网协议的字节长度，消息序号减少了 1-2 字节，更加精简，可以减少传输数据量。

在一些实施例中，所述消息载荷包括实际数据和消息类型，所述消息类型包括填充类型、应用数据类型、警告类型和握手类型。

图 17 中，Payload 为实际数据，包括：经所述第一密钥加密的所述校验数据中携带的传输数据；或者，经共享密钥加密的所述应用数据携带中的传输数据；或者，所述握手信息携带的传输数据。其中，所述经所述第一密钥加密的所述校验数据中携带的传输数据可以是所述校验数据包括的哈希值的集合；所述经所述第一密钥加密的所述应用数据携带中的传输数据可以是待传输的应用数据（如开灯、关灯、开始扫地、打开窗帘等）；所述握手信息携带的传输数据可以是公钥、随机序列、加密曲线、加密套件、协议标识、公钥列表中至少一种。

图 17 中，“+”表示消息所附带的的 extension；“{}”表示 Epoch 1，即消息使用[sender]HandshakeTraffic 派生的密钥功能进行加密；“[]”表示 Epoch 2，即消息使用[sender]ApplicationTraffic 派生的密钥进行加密。

图 17 中，所述消息格式包括：E、Seq 和 Payload；所述 Payload 包括 Content 和 Type。

其中，所述 Payload 包括消息载荷，除第 0 代密钥（Epoch 0）外，Payload 数据被加密。

所述消息载荷包括实际数据和消息类型，所述消息类型包括填充类型、应用数据类型、警告类型和握手类型。所述消息类型（Type）的定义如表 2 所示：

表 2

消息类型（Type）	符号（Sym）	信息（Info）
0	Padding	填充字节 0
1	Application Data	应用层消息
2	Alter	通知消息

3	Handshake	握手协商消息

其中，所述填充类型包括表 2 中的 Padding，用于填充 Payload 至合适的长度。Padding 对应的 Content 部分仍然是 Payload 格式，即最后一个字节需要根据消息类型重新判断。解析时，可以直接掉过 Payload 结尾的 Padding。

如表 2 所示，所述应用数据类型包括表 2 中的 Application Data，包括传输所述第一客户端和/或服务端之间的应用数据，可以是开灯、关灯、环境信息采集、生物特征采集等数据。

所述警告类型包括表 2 中的通知消息，具体包括握手成功、握手失败等告知 ECDH 的配网协议或 ECJPAKE 的配网协议的消息，如第一警告消息、第二警告消息等。

所述握手类型包括表 2 中的握手协商消息，具体包括第一信息、第二序列、第一校验数据、第一验证信息、第二校验数据、第二验证信息、第三序列、第一重传请求、第一问候信息中至少一种。

如表 2 所示，Alert 用于发送告警消息，代码包括：

```
enum {
close_notify(0),
    unexpected_message(10),
    handshake_failure(40),
    protocol_version(70),
    decrypt_error(51),
}AlertCode;
struct{
    uint8 code;
}Alert;
```

其中，所述客户端和或服务端在接收到告警消息的情况下，必须断开连接。

在一些实施例中，Payload 内容为 Handshake 的情况下，Handshake 消息的代码包括：

```
enum: uint8 {
Client_hello(1),
Server_hello (2),
hello_retry_request(3),
authenticate (4),
finished(20),
MAX(255)
} Handshaketype;
struct {
Handshaketype hs_type;        /握手消息类型
uint16 len;                        /*握手消息长度*/
switch(hs_type) {
case Client_hello;                Clienthello
case Server_hello;                Serverhello
case hello_retry_request:        Helloretryrequest;
case authenticate;            Authenticate
case finished;                Finished
}
} Handshake
struct {
Handshake[ ] handshakes;
}    Handshakepayload;
```

在一些实施例中，所述 Handshake 用于发送握手消息，所述握手消息包括：第一信息、第二序列、第一校验数据、第一验证信息、第二校验数据、第二验证信息、第三序列、第一重传请求、第一问候信息中至少一种。

在一些实施例中，至少一个 Handshake 消息的 Epoch 相同，则发送所述至少一个 Handshake 消息的一端可以将所述至少一个 Handshake 消息合并，如此只需要加密一次。

相应地，在接收所述消息的一端解密数据时，通过 Handshake.len 确定每个 Handshake 消息的边界，通过整条消息长度确定一条消息中包含的所有 Handshake。

图 14 中，客户端发送的 ClientHello 的代码包括：

```
Opaque Random[8];
Struct {
Random random;
Extension[ ] extensions;
} ClientHello;
```

其中，random 包括 8 字节的随机数据，用于防止重放攻击。extension 为扩展，用于描述所述客户端的自身能力和相关参数。Extension 中所有扩展必须按照扩展类型从小到大的顺序排列。

ClientHello 是协议协商的第一条消息，由客户端（Client）向服务端（Server）发送。用于向 Server 告知所

述 Client 的认证能力以及自定义参数。

图 14 中，服务端发送的 ServerHello 的代码包括：

```
opaque Random[8];
struct {
Random random;
Extension[ ] extensions;
} ServerHello;
```

其中，random 包括 32 字节的随机数据，用于防止重放攻击。extension 为扩展，用于描述所述服务端的自身能力和相关参数。Extension 中所有扩展必须按照扩展类型从小到大的顺序排列。只有当 ClientHello 中给出了某个扩展时（代表 Client 支持所述某个扩展），在 ServerHello 的应答中才允许应答对应的扩展。

ServerHello 由 Server 向 Client 发送，用于确定会话的连接参数。

ClientHello 是协议协商的第一条消息，由 Client 向 Server 发送。用于向 Server 告知所述 Client 的认证能力以及自定义参数。

在 Client 处理 ServerHello 时，若发现其中存在任何不支持的扩展，必须向 Server 发送 unexpected_message 警告并断开连接。Server 发现必选扩展不存在是，必须向 Client 发送 unexpected_message 警告并断开连接。

图 14 中，HelloRetryRequest 消息的代码包括：

```
struct {
Extension[ ] extensions;
} HelloRetryRequest;
```

其中，extensions 表征扩展，用于描述所述服务端的自身能力和相关参数。在所述 Client 第一次向 Server 发送 ClientHello 以后，Server 可能发送 HelloRetryRequest 要求 Client 重新发起协商。比较常见的情况是 Client 提供的 key_share 曲线 Server 不支持，比如 Client 提供 secp256r1 曲线，但 Server 只支持 C25519 曲线，此时，Server 需要从 ClientHello 中找到 supported_group 扩展，从 supported_group 中找到能够进行协商的曲线，然后使用 HelloRetryRequest 消息通知 Client 重新协商。

在客户端和服务端协商共享密钥的过程中，Retryrequest 只允许发起一次。对于 Server，若第二次 Clienthello 发送的参数仍然无法接受时，Server 必须发送 handshake_ failure 警告并关闭连接。对于 Client，若收到第二个 HelloRetryrequest，Client 必须发送 unexpected_ message 并断开连接。

HelloRetryRequest 消息在 ECDH 的配网协议中用于对错误 ClientHello 消息的应答；或者，在 ECJPAKE 的配网协议中用于传输 ECJPAKE Round 1 数据。

在一些实施例中，所述在 ECDH 的配网协议中对错误 ClientHello 消息的应答包括步骤 S301 至步骤 S302，此处不再重复赘述；所述在 ECJPAKE 的配网协议中传输 ECJPAKE Round 1 数据包括步骤 S401 至步骤 S402，此处不再重复赘述。

图 14 中，Authenticate 消息的代码包括：

```
struct {
Select（Authentication）{
        Case ECJPAKE：ECJPAKEParams;
        Case Certificate：CertificateAuth;
    };
Extension[ ] extensions;
} Authenticate;
```

其中，所述 Authenticate 消息用于传输认证数据。消息格式会根据 cipher_ suites 定义的 Authentication 列的取值变化。特殊的，当 Authentication 取值为 None 时，该消息必须被省略。不同的认证方式下， Authenticate 构造方式不同。

在认证方式使用 ECDH 的配网协议的情况下，Authenticate 消息的代码包括：

```
enum {
X509(0),
HeyThingsDomainCertificate(242),
(255)
} CertificateType;
struct {
CertificateType type;
Uint16 cert_len;
opaque[sig_len] signature;
} CertificateAuth;
struct {
struct CertificateAuth Cert;
Extension[ ] extensions;
} Authenticate;
```

其中，所述 Authenticate 消息用于对 ECDH 的证书认证，支持两种证书：X509 证书与自定义证书。

图 14 中，Finished 消息的代码包括：

```
struct {
opaque[Hash.length] verify_data
} Finished;
```

其中，verify_data 为使用当前 Transcripthash 值计算 HMAC。计算方法包括：

```
Verify_data=HMAC(key=FinishedKey,message=TranscriptHash)
```

其中，TranscriptHash：Server：TranscriptHash(ClientHello1……Server Authenticate)。

Client：TranscriptHash(ClientHello1…Server Authenticate,Server Finished,Client Authenticate)。

Finished Key: Server: Expand(PRK=ServerHandshakeTraffic, |abe|="htbts finished",len=Hash Length)。

Client: Expand(PRK=ClientHandshakeTraffic, |abe|="htbts finished",len=Hash Length)

图 14 中，Application Data 消息的 Content 部分为完整的用户数据。

所述消息代码中，extension 是对消息的补充说明，代码包括：

```
struct {
extensionType extension_type;
uint16 data_size;
opaque[data_size] extension_data;
} Extension;
```

其中，extension_data 表征各扩展类型内，定义的扩展数据；data_size 表征数据长度。编码方式可以参考变长整数。data_size 不大于 16383 字节，即 data_size 编码后只可能为 1 字节或 2 字节。当编码为 2 字节时，第一字节最高位为 1，第二字节最高位不为 1。解码时，若发现 data_size 不符合要求，则应发送 unexpected_ message 告并关闭连接；extension_type 表征 Extension 的消息类型如表 3 所示：

表 3

Type	Sym	适用于
0	supported_version	CR（必选），SR（必选），HRR（必选）
1	cipher_suits	CR（必选），SR（必选），HRR（必选）
2	supported_group	CR，SR，HRR
4	key_share	CR（必选），SR（必选）
5	Ecjpake_key_kp_pair_list	CR，SR
6	Ecjpake_key_kp_params	CR，SR

其中，所述“适用于”用于标识允许使用相应扩展的我受消息。消息名称通过缩写表示：CR（ClientHello），SR（ServerHello），HRR（HelloRetryRequest），AU（Authenticate）。

其中，“必选”表示响应的消息中必须存在。在对端发送的消息中，缺少某个必选扩展，必须发送 unexpected_ message 并断开连接。

表 3 中，Type 0 表征版本号；Type1 表征加密套件，可以是 ECDH、(Diffle-Hellman，DH）等；Type2 表征使用的曲线类型，如椭圆曲线；Type4 表征交互公钥；Type5 和 Type6 分别表征不同阶段的公钥。

图 14 中，supported_version 的代码包括：

```
uint8 Version;
struct{
    Version [0..255] versions;
} ExtensionSupportedVersion;
```

其中，supported_version 指示所述客户端或服务端支持的协议版本。目前协议版本为 1。

supported_version 必须被添加到 ClientHello、ServerHello、HelloRetryRequest 中。并填写一个 Version。Server 填写的 Version 将作为本次连接的协议版本。

在一些实施例中，当 Client 在收到的 ServerHello 中，发现 supported_version 扩展中存在多个 Version 或发现 Version 自己不支持时，clent 应该发送 protocol_version 警告并关闭连接。

图 14 中，cipher_suites 的代码包括：

```
uint8 CipherSuite;
struct{
    CipherSuite[0..255] cipher_suites;
} ExtensionCipherSuites;
```

其中，所述 cipher_suites 指示所述客户端或服务端支持的加密套件。所述 cipher_suites 包括 CipherSuite、Sym、KeyExchange、Authentication、Cipher、MAC Tag、和 Hash。

CipherSuite 用于指示加密套件的 uint8 的取值；Sym 用于指示加密套件名称，用于统一个实现的命名。KeyExchange 用于指示密钥交换方式，影响 key_share 扩展。Authentication 用于指示认证方式，影响 Authenticate 消息；Cipher 用于指示数据加密方式，在加密时需要使用；MAC Tag 用于指示加密套件的 MAC Tag 长度。Hash 用于指示在协议运行过程中使用的 HKDF、HMAC 等函数所使用的散列函数。

在一些实施例中，Client 在 ClientHello 中填写一个或多个 CipherSuite。由 Server 在 ServerHello 和 HelloRetryRequest 中选中并填写一个 CipherSuite。Server 填写的 CipherSuite 将作为本次连接使用的加密套件。

在一些实施例中，非调试目的不允许使用 0x00(None)加密套件。

在一些实施例中，当 Client 在收到的 ServerHello 中，发现 cipher_suites 扩展中存在多个 cipher_suites 或发现 cipher_suites 自己不支持时，Client 应该发送 unexpected_message 警告并关闭连接。

图 14 中，supported_group 的代码包括：

```
uint8 NamedGroup
struct {
    NamedGroup[0..255] named_group_list;
} ExtensionSupportedGroup;
```

在一些实施例中，支持的 EC 曲线参数。定义如表 4：

表 4

NamedGroup	sym
0x17	secp256r1
0x18	secp384r1
0x19	secp521r1
0x1D	x25519
0x1E	x448

其中，Client 在 ClientHello 中填写一个或多个自己支持的 NamedGroup，但 Server 在 ServerHello 和 HelloRetryRequest 中，选中并填写一个 NamedGroup。Server 填写的 NamedGroup 将作为本次连接使用的 EC 曲线。

在一些实施例中，当 Client 在收到的 ServerHello 中，发现 supported_group 扩展中存在多个 NamedGroup 或发现 NamedGroup 自己不支持时，Client 应该发送 unexpected_message 警告并关闭连接。

图 14 中，key_share 的代码包括：

```
struct {
    NamedGroup group;
    uint8 len
    opaque[len] key_exchange;
} KeyShareEntry;
struct {
    KeyShareEntry[] key_shares;
} ExtensionKeyShare;
```

其中，key_share 用于向对方共享密钥。用于密钥协商。key_share 在 ClientHello、ServerHello、HelloRetryRequest 消息中可能使用。

在一些实施例中，ClientHello 中，key_shares 允许出现多个，用于供 Server 挑选。ServerHell 中，key_shares 仅能出现一个，用于选择密钥协商。HelloRetryRequest 中，key_shares 仅能出现一个，并且 len 为 0。仅用于告知 Client 重新发起 ClientHello。

在一些实施例中，当 Client 在收到的 ServerHello 中，发现扩展中存在多个 key_shareEntry 或发现 NamedGroup 自己不支持时，Client 应该发送 unexpected_message 警告并关闭连接。

图 14 中，ecjpake_key_kp_pair_list 的代码包括：

```
struct {
    ECJPAKEKeyKP ecjpake_key_kp_list[2];
}ExtensionECJPAKEKeyKPPairList;
```

在一些实施例中，如果不确定 Server 端是否支持 ECJPAKE 认证，Client 端在第一个 ClientHello1 中应该携带空的 ecjpake_key_pair_list。若 Server 端选择 ECJPAKE 进行认证，则 Server 端需要选择 ECJPAKE 类 cipher_suites，填写自己的 ECJPAKE Round1 数据并发送 HelloRetryRequest 要求 Client 重新认证。

在一些实施例中，所述握手问候消息或所述握手应答消息的消息载荷中包括 ecjpake_key_kp_pair_list 字段，所述 ecjpake_key_kp_pair_list 字段的值为空 NULL，所述空值用于确定所述第二端是否支持目标加密套件。

在一些实施例中，格式定义与 Elliptic Curve J-PAKE Cipher for Transport Layer (TLS) Section 7.2.2[17] 中定义相同。对应 ClientHello/ServerHello 中的“ECJPAKEKeyKPPairList”扩展。identtity 字段被删除，使用 mbedTLS 实现中预定义的“Client”/“Server”。

图 14 中，ecjpake_key_kp_params 的代码包括：

```
// ServerHello 中的数据结构
struct {
    ECParameters curve_params;
    ECJPAKEKeyKP ecjpake_key_kp;
} ServerECJPAKEParams;
// ClientHello 中的数据结构
struct {
    ECJPAKEKeyKP ecjpake_key_kp;
} ClientECJPAKEParams;
```

其中，格式定义与 Elliptic Curve J-PAKE Cipher for Transport Layer (TLS) Section 7.3[18] 中定义相同。对应

ServerKeyExchange/ClientKeyExchange 中的“ServerECJPAKEParams”或“ClientECJPAKEParams”。

在一些实施例中，所述“ecjpake_key_kp_params”用于指示 ECJPAKE 的协议中的公钥，如第五公钥、第六公钥等。

图 14 中，TrainscriptHash 是握手过程中需要保持的 Hash 上下文，用于保障握手过程数据的完整性。Client、Server 每发送、接收一条消息，都需要将消息内容写入 Hash 上下文。Client 在收到 ServerHello 或 HelloRetryRequest 时初始化 TranscriptHash。Server 在收到第一包 ClientHello 时初始化 TranscriptHash。

在一些实施例中，TranscriptHash 构造方法包括：

```
Transcript-Hash(M1,M2, ... Mn) = Hash(M1 ‖ M2 ‖ ... ‖ Mn)
```

其中，HelloRetryRequest 一般情况下是不需要使用的，这样整个交互过程就会省略 HelloRetryRequest 和第二个 ClientHello。

此时 TranscriptHash 组成包括：

```
Hash(ClientHello ‖ ServerHello ‖ ... Mn)
```

在一些实施例中，消息序号的代码包括：

```
struct {
    uint16 epoch;
    uint48 seq;
} RecordNumber;
```

其中，消息序号分为 epoch、seq 两部分，共 64 位。Client 与 Server 分开处理。epoch 为密钥代数。连接刚刚建立成功时，epoch 为 0。包括 epoch 0 在内，每发送和接收一条消息，seq 递增 1。

需要说明的是，在本申请实施例中，客户端可以作为第一端，相应地，服务端作为第二端；在另一些实施例中，客户端还可以作为第二端，服务端作为第一端。

图 18 示出了本申请实施例提供的客户端的一种可选结构示意图，将根据各个部分进行说明。

在一些实施例中，所述客户端 1100 包括：第一发送单元 1101，第一获取单元 1102 和第一确定单元 1103。

第一发送单元 1101，用于发送第一客户端问候消息，所述第一客户端问候消息包括第一信息，所述第一信息用于指示所述客户端能够支持的第一密钥协商模式；

第一获取单元 1102，用于获取服务端基于所述第一客户端问候消息发送的第一服务端反馈消息，所述第一反馈信息用于指示所述服务端确定的第二密钥协商模式，所述第一服务端反馈消息包括请求重发问候消息或服务端问候消息；

第一确定单元 1103，若所述第一密钥协商模式包括所述第二密钥协商模式，用于基于所述第二密钥协商模式确定第一客户端共享密钥，根据所述第一客户端共享密钥进行目标数据传输。

在一些实施例中，若所述第一密钥协商模式不包括所述第二密钥协商模式，则所述第一发送单元 1101，用于发送第二客户端问候消息，所述第二信息用于指示所述客户端能够支持的第三密钥协商模式；

所述第一获取单元 1102，用于获取所述服务端基于所述第二客户问候消息发送的第二服务端反馈消息，所述第二反馈信息用于指示所述服务端确定的第四密钥协商模式；

所述第一确定单元 1103，用于基于所述第四密钥协商模式确定第二客户端共享密钥，根据所述第二客户端共享密钥进行目标数据传输；

所述第一获取单元 1102，用于获取所述服务端基于所述第二客户端问候消息发送的第一警告消息，基于所述第一警告消息断开连接；或者，获取所述服务端基于所述第二客户端问候消息发送的第三服务端反馈消息，基于所述第三服务端反馈消息发送第二警告消息并断开连接。

在一些实施例中，所述第一客户端问候消息、第二客户端问候消息、第一服务端反馈消息、第二服务端反馈消息均包括预定义字段，所述预定义字段包括：协议版本字段、加密套件字段、加密曲线字段、第一公钥字段和第二公钥字段中的至少一种字段；所述协议版本字段用于指示所述客户端或所述服务端支持的部分或全部协议版本参数；所述加密套件字段用于指示所述客户端或所述服务端支持的部分或全部加密套件参数；所述加密曲线字段用于指示所述客户端或所述服务端支持的部分或全部加密曲线参数；所述第一公钥字段用于指示所述客户端或所述服务端的第一公钥；所述第二公钥字段用于指示所述客户端或所述服务端的第二公钥。

在一些实施例中，所述第一客户端问候消息包括所述协议版本字段、所述加密套件字段、所述第一公钥字段、所述加密曲线字段和所述第二公钥字段，其中，所述第一公钥字段包括所述客户端的第一公钥；所述第二公钥字段为空；和/或，当所述客户端和所述服务端适用第一密钥协商算法时，所述第二客户端问候消息包括所述协议版本字段、所述加密套件字段、所述第一公钥字段，所述第一公钥字段包括所述客户端的第二公钥；和/或，当所述客户端和所述服务端适用第二密钥协商算法，且所述客户端支持所述第二密钥协商模式时，所述第二客户端问候消息包括所述协议版本字段、所述加密套件字段、所述第二公钥字段，所述第二公钥字段包括所述客户端的第三公钥；和/或，当所述客户端和所述服务端适用第二密钥协商算法，且所述客户端不支持所述第二密钥协商模式时，所述第二客户端问候消息包括所述协议版本字段、所述加密套件字段、所述加密曲线字段。

在一些实施例中，所述第一密钥协商算法为 ECDH 算法，所述第二密钥协商算法为 ECJPAKE 算法。

在一些实施例中，所述若所述第一密钥协商模式包括所述第二密钥协商模式，包括：所述第一客户端问候消息的所述协议版本字段的协议版本参数包括所述第一服务端反馈消息的所述协议版本字段的协议版本参数；所述第一客户端问候消息的所述加密套件字段的加密套件参数包括所述第一服务端反馈消息的所述加密套件字段的加密套件参数；所述第一客户端问候消息的所述加密曲线字段的加密曲线参数包括所述第一服务端反馈消息的所述加密套件字段的加密套件参数；和/或，所述若所述第一密钥协商模式不包括所述第二密钥协商模

式，包括：所述第一客户端问候消息的所述协议版本字段的协议版本参数不包括所述第一服务端反馈消息的所述协议版本字段的协议版本参数；或者，所述第一客户端问候消息的所述加密套件字段的加密套件参数不包括所述第一服务端反馈消息的所述加密套件字段的加密套件参数；或者，所述第一客户端问候消息的所述加密曲线字段的加密曲线参数不包括所述第一服务端反馈消息的所述加密套件字段的加密套件参数。

在一些实施例中，若所述第一客户端共享密钥或所述第二客户端共享密钥使用预设次数或预设时间后，重新执行所述发送第一客户端问候消息的步骤。

图 19 示出了本申请实施例提供的数据传输装置的另一种可选结构示意图，将根据各个部分进行说明。

在一些实施例中，服务端 1200 包括：第二接收单元 1201 和第二确定单元 1202。

第二接收单元 1201，用于接收客户端发送的第一客户端问候消息，所述第一客户端问候消息用于指示所述客户端能够支持的第一密钥协商模式；

第二确定单元 1202，用于根据所述第一密钥协商模式确定所述服务端选择的第二密钥协商模式，并通过所述第一服务端反馈消息发送给所述客户端；或者，若所述第一密钥协商模式包括所述第二密钥协商模式，用于基于所述第二密钥协商模式确定第一服务端共享密钥，根据所述第一服务端共享密钥进行目标数据传输。

在一些实施例中，若所述第一密钥协商模式不包括所述第二密钥协商模式，所述第二接收单元 1201，用于接收所述客户端发送第二客户端问候消息，所述第二客户端问候消息用于指示所述客户端能够支持的第三密钥协商模式；

第二接收单元 1201，用于基于所述第二客户端问候消息发送第二服务端反馈消息，所述第二服务端反馈消息用于指示所述服务端确定的第四密钥协商模式；

所述第二确定单元 1202，用于基于所述第四密钥协商模式确定第二服务端共享密钥，根据所述第二客户端共享密钥进行目标数据传输；或者，基于所述第二客户端问候消息发送的第三服务端反馈消息并断开连接。

在一些实施例中，所述第一客户端问候消息、第二客户端问候消息、第一服务端反馈消息、第二服务端反馈消息均包括预定义字段，所述预定义字段包括：协议版本字段、加密套件字段、加密曲线字段、第一公钥字段和第二公钥字段中的至少一种字段；所述协议版本字段用于指示所述客户端或所述服务端支持的部分或全部协议版本参数；所述加密套件字段用于指示所述客户端或所述服务端支持的部分或全部加密套件参数；所述加密曲线字段用于指示所述客户端或所述服务端支持的部分或全部加密曲线参数；所述第一公钥字段用于指示所述客户端或所述服务端的第一公钥；所述第二公钥字段用于指示所述客户端或所述服务端的第二公钥。

在一些实施例中，所述客户端和所述服务端能够适用第一密钥协商算法和/或第二密钥协商算法；所述第一服务端反馈消息包括请求重发问候消息或服务端问候消息。

在一些实施例中，所述请求重发问候消息为第一请求重发问候消息、第二请求重发问候消息、第三请求重发问候消息、第四请求重发消息中的任一种，所述服务端问候消息为第一服务端问候消息、第二服务端问候消息中的任一种，其中，所述第一请求重发问候消息用于在所述服务端适用所述第一密钥协商算法且不支持所述第一密钥协商模式的情况下发送的；和/或，所述第二请求重发问候消息用于在所述服务端适用所述第二密钥协商算法且支持所述第一密钥协商模式的情况下发送的；和/或，所述第三请求重发问候消息用于在所述服务端适用所述第二密钥协商算法且不支持所述第一密钥协商模式的情况下发送的；和/或，所述第四请求重发问候消息用于在所述服务适用所述第一密钥协商算法且支持第一密钥协商模式，但不支持所述第一公钥的情况下发送的；所述第一服务端问候消息用于在所述服务端适用所述第二密钥协商算法且支持所述第一密钥协商模式的情况下发送；和/或，所述第二服务端问候消息用于在所述服务端适用所述第一密钥协商算法且支持所述第一密钥协商模式的情况下发送的。

在一些实施例中，所述第一密钥协商算法为 ECDH 算法，所述第二密钥协商算法为 ECJPAKE 算法。

图 20 示出了本申请实施例提供的数据传输装置的一种可选结构示意图，将根据各个部分进行说明。

在一些实施例中，数据传输装置 1400，包括：协商单元 1401 和应用数据单元 1402。

协商单元 1401，用于通过握手消息与第二端协商密钥；

应用数据单元 1402，用于通过内容消息与所述第二端传输应用数据，所述内容消息通过使用所述共享密钥进行加密和解密；

其中，所述握手消息和所述内容消息具有相同的消息格式，所述消息格式包括：消息序号和消息载荷；所述消息序号包括密钥代数标识和消息计数标识，其中，所述密钥代数标识通过小于第一位数的比特信息进行表征，所述消息计数标识通过小于第二位数的比特信息进行表征。

在一些实施例中，所述消息载荷包括实际数据和消息类型，所述消息类型包括填充类型、应用数据类型、警告类型和握手类型。

在一些实施例中，所述数据传输装置 1400 还包括：加密单元 1403；

所述加密单元 1403，用于通过所述共享密钥对所述内容消息中的消息载荷进行加密。

在一些实施例中，所述数据传输装置 1400 还包括：校验单元 1404；

所述校验单元 1404，用于在协商共享密钥过程中，对所述握手消息进行校验得到校验值。

在一些实施例中，所述握手消息包括握手完成消息，用于指示完成所述共享密钥的协商流程，其中，所述握手完成消息携带所述校验值。

在一些实施例中，所述握手消息包括以下至少一项：握手问候消息、握手应答消息、重发请求消息、认证数据消息、握手完成消息。

在一些实施例中，所述握手问候消息、握手应答消息、重发请求消息的消息载荷中至少包括以下字段中的一种或多种：协议版本字段、加密套件字段、共享密钥字段、加密曲线字段。

在一些实施例中，所述第一端通过所述握手问候消息、所述握手应答消息或所述重发请求消息与所述第二

端协商共享密钥时，所述密钥代数标识为 a；所述第一端通过所述认证数据消息或所述握手完成消息与所述第二端协商共享密钥时，所述密钥代数标识为 a+1；所述第一端通过所述内容消息与所述第二端传输应用数据时，所述密钥代数标识为 a+2 至 a+N；其中，a 为整数，N 为大于或等于 2 的整数。

在一些实施例中，所述握手问候消息或所述握手应答消息的消息载荷中包括公钥列表字段，所述公钥列表字段的值为空（NULL），所述空值用于确定所述第二端是否支持目标加密套件。

在一些实施例中，所述第二端基于所述握手问候消息返回所述重发请求消息，其中，所述重发请求消息中的加密套件字段配置为所述目标加密套件。

在一些实施例中，所述第一端为客户端，所述第二端为服务端；或者，所述第一端为服务端，所述第二端为客户端。

图 21 是本申请实施例的电子设备的硬件组成结构示意图，电子设备 1300 包括：至少一个处理器 1301、存储器 1302 和至少一个网络接口 1304。客户端或服务端 1300 中的各个组件通过总线系统 1305 耦合在一起。可理解，总线系统 1305 用于实现这些组件之间的连接通信。总线系统 1305 除包括数据总线之外，还包括电源总线、控制总线和状态信号总线。但是为了清楚说明起见，在图 15 中将各种总线都标为总线系统 1305。

在一些实施例中，所述电子设备可以是客户端或服务器对应的硬件结构。

可以理解，存储器 1302 可以是易失性存储器或非易失性存储器，也可包括易失性和非易失性存储器两者。其中，非易失性存储器可以是 ROM、可编程只读存储器（PROM，Programmable Read-Only Memory）、可擦除可编程只读存储器（EPROM，Erasable Programmable Read-Only Memory）、电可擦除可编程只读存储器（EEPROM，Electrically Erasable Programmable Read-Only Memory）、磁性随机存取存储器（FRAM，ferromagnetic random access memory）、快闪存储器（Flash Memory）、磁表面存储器、光盘、或只读光盘（CD-ROM，Compact Disc Read-Only Memory）；磁表面存储器可以是磁盘存储器或磁带存储器。易失性存储器可以是随机存取存储器（RAM，Random Access Memory），其用作外部高速缓存。通过示例性但不是限制性说明，许多形式的 RAM 可用，例如静态随机存取存储器（SRAM，Static Random Access Memory）、同步静态随机存取存储器（SSRAM，Synchronous Static Random Access Memory）、动态随机存取存储器（DRAM，Dynamic Random Access Memory）、同步动态随机存取存储器（SDRAM，Synchronous Dynamic Random Access Memory）、双倍数据速率同步动态随机存取存储器（DDRSDRAM，Double Data Rate Synchronous Dynamic Random Access Memory）、增强型同步动态随机存取存储器（ESDRAM，Enhanced Synchronous Dynamic Random Access Memory）、同步连接动态随机存取存储器（SLDRAM，SyncLink Dynamic Random Access Memory）、直接内存总线随机存取存储器（DRRAM，Direct Rambus Random Access Memory）。本申请实施例描述的存储器 1302 旨在包括但不限于这些和任意其它适合类型的存储器。

本申请实施例中的存储器 1302 用于存储各种类型的数据以支持客户端或服务端 1300 的操作。这些数据的示例包括：用于在客户端或服务端 1300 上操作的任何计算机程序，如应用程序 1322。实现本申请实施例方法的程序可以包含在应用程序 1322 中。

所述本申请实施例揭示的方法可以应用于处理器 1301 中，或者由处理器 1301 实现。处理器 1301 可能是一种集成电路芯片，具有信号的处理能力。在实现过程中，所述方法的各步骤可以通过处理器 1301 中的硬件的集成逻辑电路或者软件形式的指令完成。所述的处理器 1301 可以是通用处理器、数字信号处理器（DSP，Digital Signal Processor），或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。处理器 1301 可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者任何常规的处理器等。结合本申请实施例所公开的方法的步骤，可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于存储介质中，该存储介质位于存储器 1302，处理器 1301 读取存储器 1302 中的信息，结合其硬件完成前述方法的步骤。

在示例性实施例中，客户端或服务端 1300 可以被一个或多个应用专用集成电路（ASIC，Application Specific Integrated Circuit）、DSP、可编程逻辑器件（PLD，Programmable Logic Device）、复杂可编程逻辑器件（CPLD，Complex Programmable Logic Device）、FPGA、通用处理器、控制器、MCU、MPU、或其他电子元件实现，用于执行前述方法。

本申请实施例还提供了一种存储介质，用于存储计算机程序。

可选的，该存储介质可应用于本申请实施例中的第一客户端，并且该计算机程序使得计算机执行本申请实施例的各个方法中的相应流程，为了简洁，在此不再赘述。

本申请是参照根据本申请实施例的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

以上所述，仅为本申请的较佳实施例而已，并非用于限定本申请的保护范围，凡在本申请的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本申请的保护范围之内。

权利要求书

1、一种数据传输方法，所述方法包括：

第一端通过握手消息与第二端协商共享密钥；

所述第一端通过内容消息与所述第二端传输应用数据，所述内容消息通过使用所述共享密钥进行加密和解密；

其中，所述握手消息和所述内容消息具有相同的消息格式，所述消息格式包括：消息序号和消息载荷；

所述消息序号包括密钥代数标识和消息计数标识，其中，所述密钥代数标识通过小于第一位数的比特信息进行表征，所述消息计数标识通过小于第二位数的比特信息进行表征。

2、根据权利要求 1 所述的数据传输方法，其中，所述消息载荷包括实际数据和消息类型，所述消息类型包括填充类型、应用数据类型、警告类型和握手类型。

3、根据权利要求 1 所述的数据传输方法，其中，所述内容消息通过使用所述共享密钥进行加密，包括：

使用所述共享密钥对所述内容消息中的消息载荷进行加密。

4、根据权利要求 1 所述的数据传输方法，其中，所述方法还包括：

在协商共享密钥过程中，所述第一端对所述握手消息进行校验得到校验值。

5、根据权利要求 4 所述的数据传输方法，其中，所述握手消息包括握手完成消息，用于指示完成所述共享密钥的协商流程，其中，所述握手完成消息携带所述校验值。

6、根据权利要求 1 所述的数据传输方法，其中，所述握手消息包括以下至少一项：握手问候消息、握手应答消息、重发请求消息、认证数据消息、握手完成消息。

7、根据权利要求 6 所述的数据传输方法，其中，所述握手问候消息、握手应答消息、以及重发请求消息的消息载荷中至少包括以下字段中的一种或多种：协议版本字段、加密套件字段、共享密钥字段、加密曲线字段。

8、根据权利要求 6 所述的数据传输方法，其中，

所述第一端通过所述握手问候消息、所述握手应答消息或所述重发请求消息与所述第二端协商共享密钥时，所述密钥代数标识为 a；

所述第一端通过所述认证数据消息或所述握手完成消息与所述第二端协商共享密钥时，所述密钥代数标识为 a+1；

所述第一端通过所述内容消息与所述第二端传输应用数据时，所述密钥代数标识为 a+2 至 a+N；其中，a 为整数，N 为大于或等于 2 的整数。

9、根据权利要求 7 所述的数据传输方法，其中，所述握手问候消息或所述握手应答消息的消息载荷中包括公钥列表字段，所述公钥列表字段的值为空值，所述空值用于确定所述第二端是否支持目标加密套件。

10、根据权利要求 9 所述的数据传输方法，其中，所述重发请求消息是所述第二端基于所述握手问候消息返回的，其中，所述重发请求消息中的加密套件字段配置为所述目标加密套件。

11、根据权利要求 1 所述的数据传输方法，其中，

所述第一端为客户端，所述第二端为服务端；

或者，

所述第一端为服务端，所述第二端为客户端。

12、一种数据传输装置，包括：

协商单元，用于通过握手消息与第二端协商共享密钥；

应用数据单元，用于通过内容消息与所述第二端传输应用数据，所述内容消息通过使用所述共享密钥进行加密和解密；

其中，所述握手消息和所述内容消息具有相同的消息格式，所述消息格式包括：消息序号和消息载荷；

所述消息序号包括密钥代数标识和消息计数标识，其中，所述密钥代数标识通过小于第一位数的比特信息进行表征，所述消息计数标识通过小于第二位数的比特信息进行表征。

13、根据权利要求 12 所述的数据传输装置，其中，所述消息载荷包括实际数据和消息类型，所述消息类型包括填充类型、应用数据类型、警告类型和握手类型。

14、根据权利要求 12 所述的数据传输装置，其中，还包括加密单元，用于通过使用所述共享密钥对所述内容消息中的消息载荷进行加密。

15、根据权利要求 12 所述的数据传输装置，其中，还包括校验单元，用于在协商共享密钥过程中，对所述握手消息进行校验得到校验值。

16、根据权利要求 15 所述的数据传输装置，其中，所述握手消息包括握手完成消息，用于指示完成所述共享密钥的协商流程，其中，所述握手完成消息携带所述校验值。

17、根据权利要求 12 所述的数据传输装置，其中，所述握手消息包括以下至少一项：握手问候消息、握手应答消息、重发请求消息、认证数据消息、握手完成消息。

18、根据权利要求 17 所述的数据传输装置，其中，所述握手问候消息、握手应答消息、重发请求消息的消息载荷中至少包括以下字段中的一种或多种：协议版本字段、加密套件字段、共享密钥字段、加密曲线字段。

19、一种存储介质，存储有可执行程序，所述可执行程序被处理器执行时，实现权利要求 1 至 11 任一项所述的数据传输方法的步骤。

20、一种电子设备，包括存储器、处理器及存储在存储器上并能够由所述处理器运行的可执行程序，所述处理器运行所述可执行程序时执行如权利要求 1 至 11 任一项所述的数据传输方法的步骤。

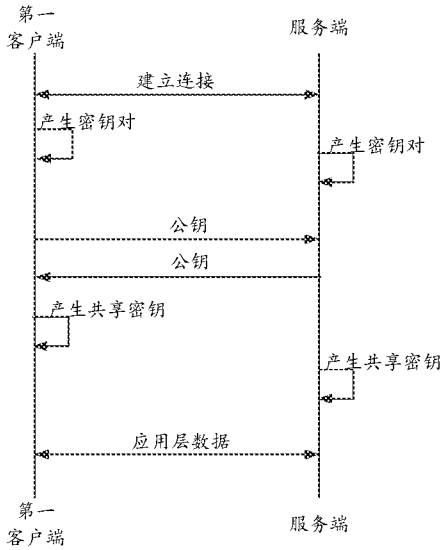
第一
客户端
服务端
建立连接
产生密钥对
产生密钥对
公钥
公钥
产生共享密钥
产生共享密钥
应用层数据
第一
客户端
服务端

图 1

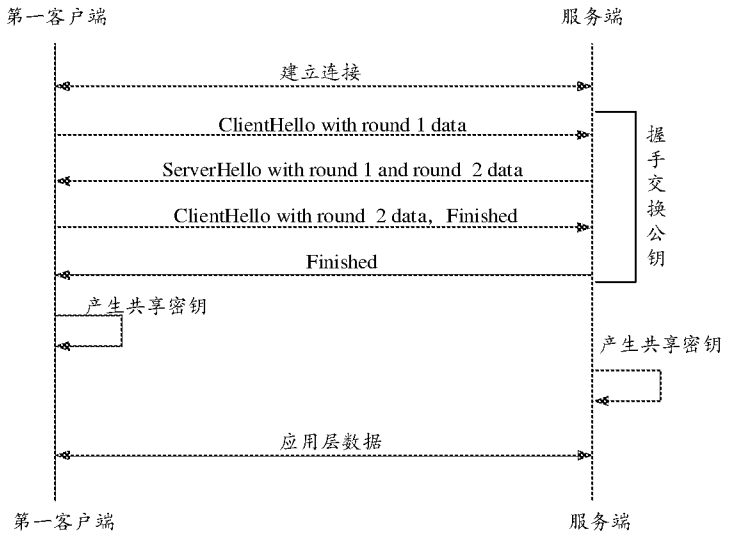
第一客户端
服务端
建立连接
ClientHello with round 1 data
ServerHello with round 1 and round 2 data
ClientHello with round 2 data, Finished
Finished
握手交换公钥
产生共享密钥
产生共享密钥
应用层数据
第一客户端
服务端

图 2

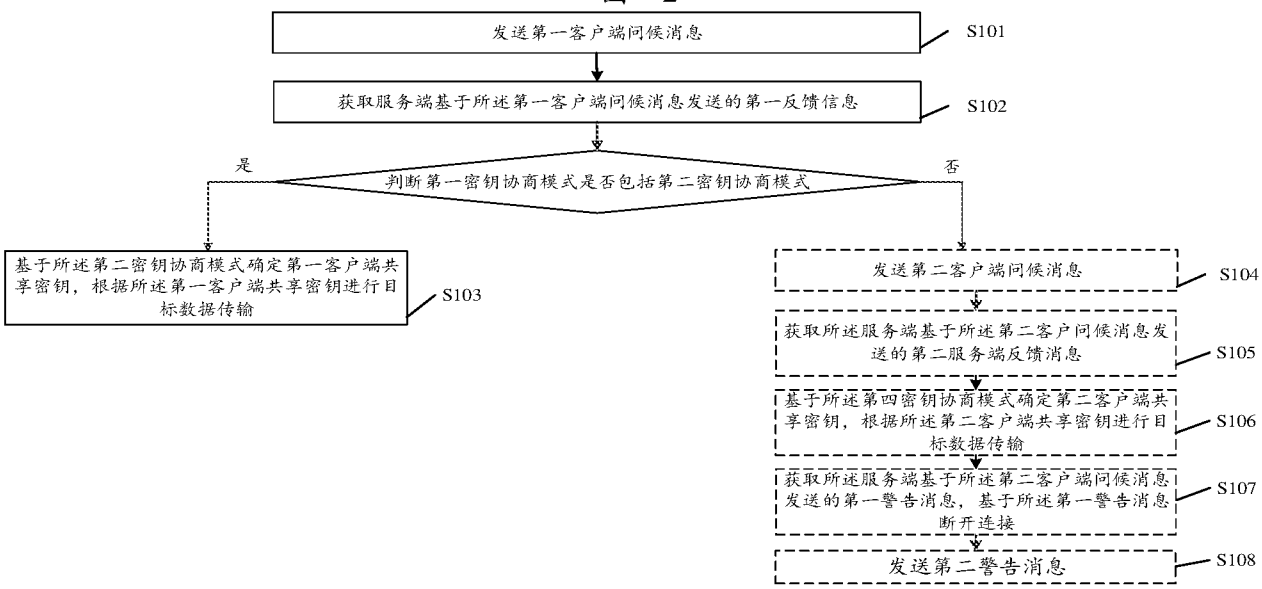
发送第一客户端问候消息
S101
获取服务端基于所述第一客户端问候消息发送的第一反馈信息
S102
是
判断第一密钥协商模式是否包括第二密钥协商模式
否
基于所述第二密钥协商模式确定第一客户端共享密钥，根据所述第一客户端共享密钥进行目标数据传输
S103
发送第二客户端问候消息
S104
获取所述服务端基于所述第二客户问候消息发送的第二服务端反馈消息
S105
基于所述第四密钥协商模式确定第二客户端共享密钥，根据所述第二客户端共享密钥进行目标数据传输
S106
获取所述服务端基于所述第二客户端问候消息发送的第一警告消息，基于所述第一警告消息断开连接
S107
发送第二警告消息
S108

图 3

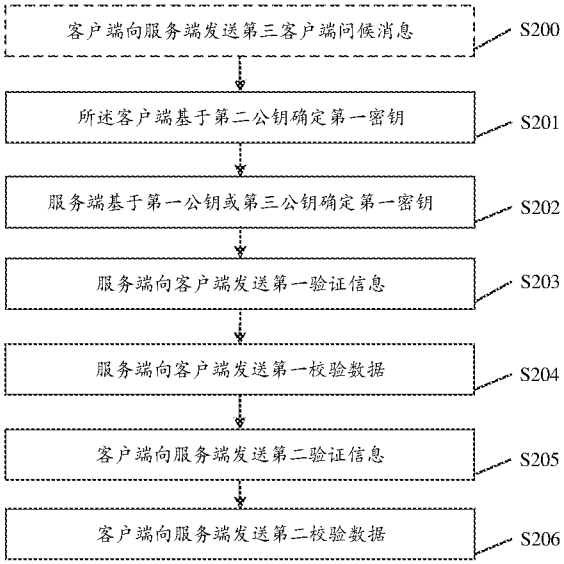
客户端向服务端发送第三客户端问候消息
S200
所述客户端基于第二公钥确定第一密钥
S201
服务端基于第一公钥或第三公钥确定第一密钥
S202
服务端向客户端发送第一验证信息
S203
服务端向客户端发送第一校验数据
S204
客户端向服务端发送第二验证信息
S205
客户端向服务端发送第二校验数据
S206

图 4

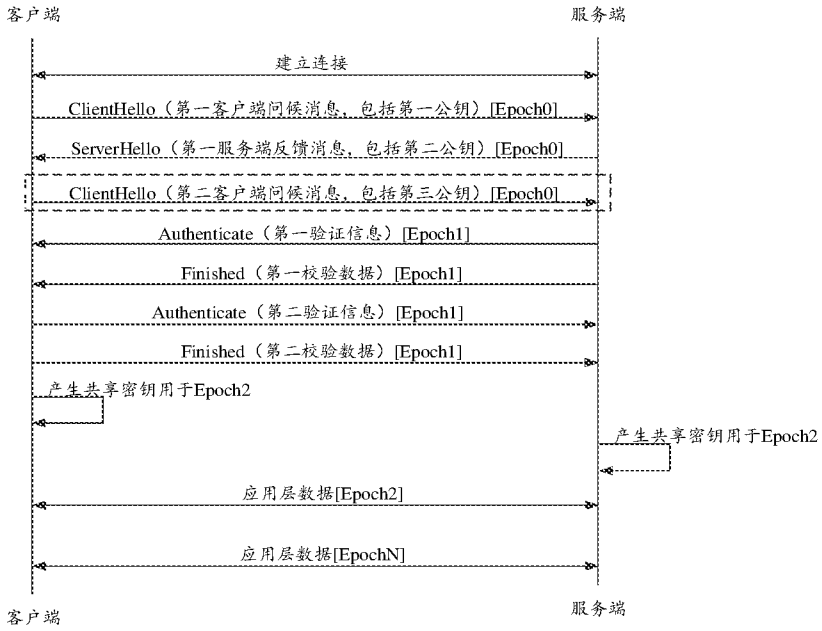
客户端
服务端
建立连接
ClientHello（第一客户端问候消息，包括第一公钥）[Epoch0]
ServerHello（第一服务端反馈消息，包括第二公钥）[Epoch0]
ClientHello（第二客户端问候消息，包括第三公钥）[Epoch0]
Authenticate（第一验证信息）[Epoch1]
Finished（第一校验数据）[Epoch1]
Authenticate（第二验证信息）[Epoch1]
Finished（第二校验数据）[Epoch1]
产生共享密钥用于Epoch2
产生共享密钥用于Epoch2
应用层数据[Epoch2]
应用层数据[EpochN]
客户端
服务端

图 5

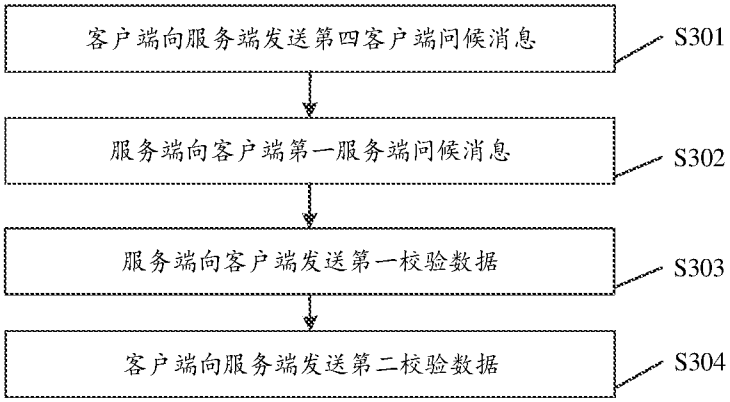
客户端向服务端发送第四客户端问候消息
S301
服务端向客户端第一服务端问候消息
S302
服务端向客户端发送第一校验数据
S303
客户端向服务端发送第二校验数据
S304

图 6

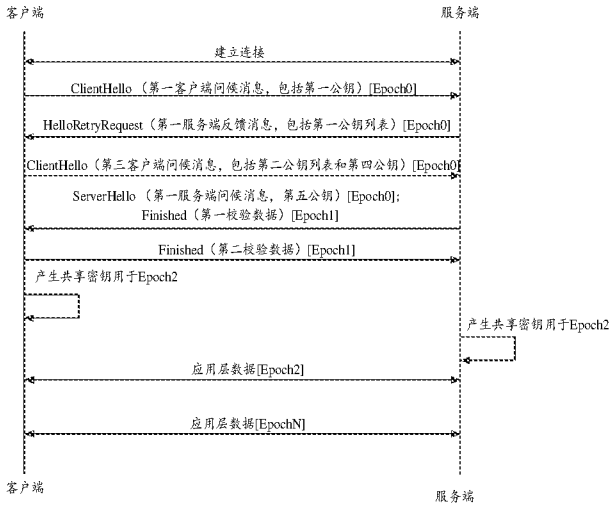
客户端
服务端
建立连接
ClientHello（第一客户端问候消息，包括第一公钥）[Epoch0]
HelloRetryRequest（第一服务端反馈消息，包括第一公钥列表）[Epoch0]
ClientHello（第三客户端问候消息，包括第二公钥列表和第四公钥）[Epoch0]
ServerHello（第一服务端问候消息，第五公钥）[Epoch0];
Finished（第一校验数据）[Epoch1]
Finished（第二校验数据）[Epoch1]
产生共享密钥用于Epoch2
产生共享密钥用于Epoch2
应用层数据[Epoch2]
应用层数据[EpochN]
客户端
服务端

图 7

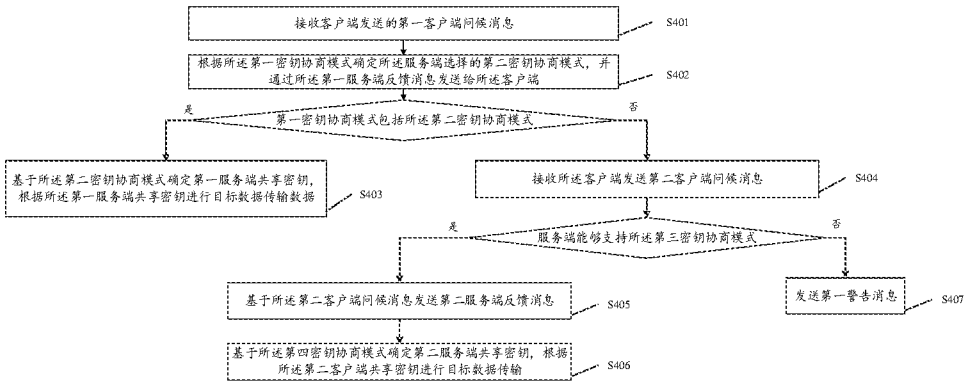
接收客户端发送的第一客户端问候消息
S401
根据所述第一密钥协商模式确定所述服务端选择的第二密钥协商模式，并通过所述第一服务端反馈消息发送给所述客户端
S402
是
否
第一密钥协商模式包括所述第二密钥协商模式
基于所述第二密钥协商模式确定第一服务端共享密钥，根据所述第一服务端共享密钥进行目标数据传输数据
S403
接收所述客户端发送第二客户端问候消息
S404
是
否
服务端能够支持所述第三密钥协商模式
基于所述第二客户端问候消息发送第二服务端反馈消息
S405
发送第一警告消息
S407
基于所述第四密钥协商模式确定第二服务端共享密钥，根据所述第二客户端共享密钥进行目标数据传输
S406

图 8

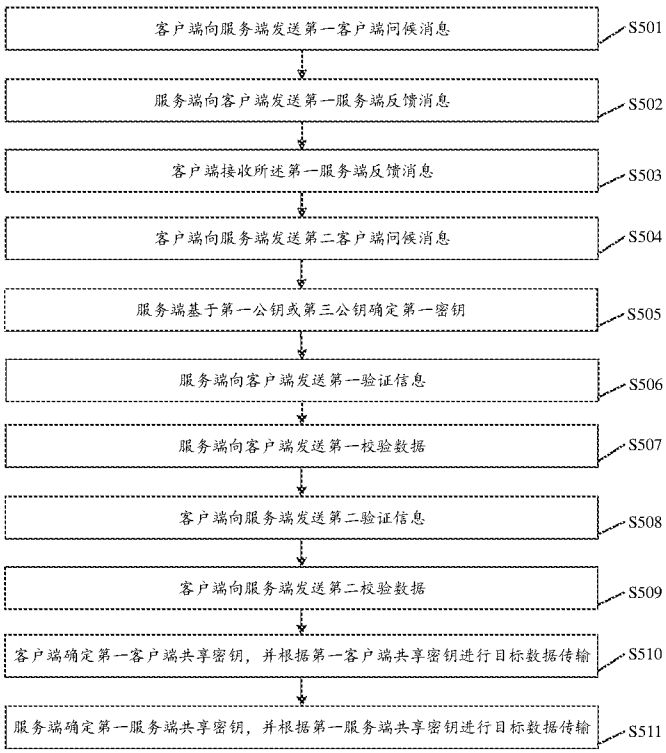
客户端向服务端发送第一客户端问候消息
S501
服务端向客户端发送第一服务端反馈消息
S502
客户端接收所述第一服务端反馈消息
S503
客户端向服务端发送第二客户端问候消息
S504
服务端基于第一公钥或第三公钥确定第一密钥
S505
服务端向客户端发送第一验证信息
S506
服务端向客户端发送第一校验数据
S507
客户端向服务端发送第二验证信息
S508
客户端向服务端发送第二校验数据
S509
客户端确定第一客户端共享密钥，并根据第一客户端共享密钥进行目标数据传输
S510
服务端确定第一服务端共享密钥，并根据第一服务端共享密钥进行目标数据传输
S511

图 9

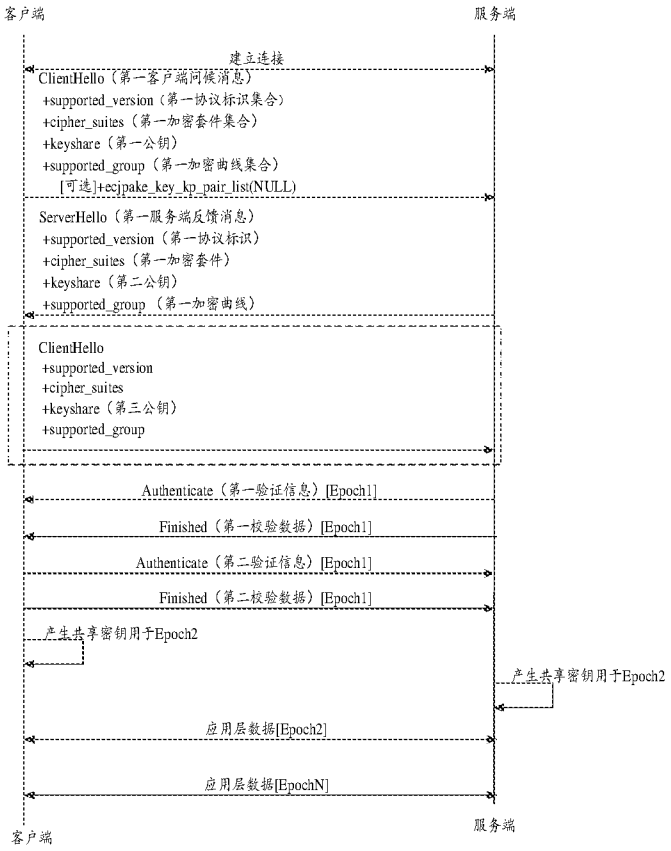
客户端
服务端
建立连接
ClientHello（第一客户端问候消息）
+supported_version（第一协议标识集合）
+cipher_suites（第一加密套件集合）
+keyshare（第一公钥）
+supported_group（第一加密曲线集合）
[可选]+ecjpake_key_kp_pair_list(NULL)
ServerHello（第一服务端反馈消息）
+supported_version（第一协议标识）
+cipher_suites（第一加密套件）
+keyshare（第二公钥）
+supported_group （第一加密曲线）
ClientHello
+supported_version
+cipher_suites
+keyshare（第三公钥）
+supported_group
Authenticate（第一验证信息）[Epoch1]
Finished（第一校验数据）[Epoch1]
Authenticate（第二验证信息）[Epoch1]
Finished（第二校验数据）[Epoch1]
产生共享密钥用于Epoch2
产生共享密钥用于Epoch2
应用层数据[Epoch2]
应用层数据[EpochN]
客户端
服务端

图 10

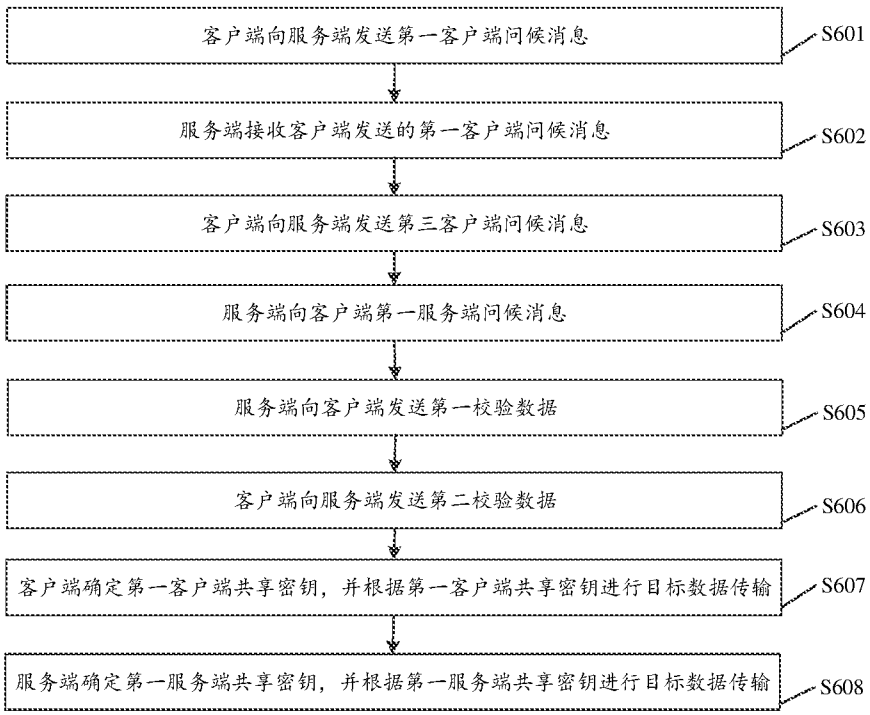
客户端向服务端发送第一客户端问候消息
S601
服务端接收客户端发送的第一客户端问候消息
S602
客户端向服务端发送第三客户端问候消息
S603
服务端向客户端第一服务端问候消息
S604
服务端向客户端发送第一校验数据
S605
客户端向服务端发送第二校验数据
S606
客户端确定第一客户端共享密钥，并根据第一客户端共享密钥进行目标数据传输
S607
服务端确定第一服务端共享密钥，并根据第一服务端共享密钥进行目标数据传输
S608

图 11

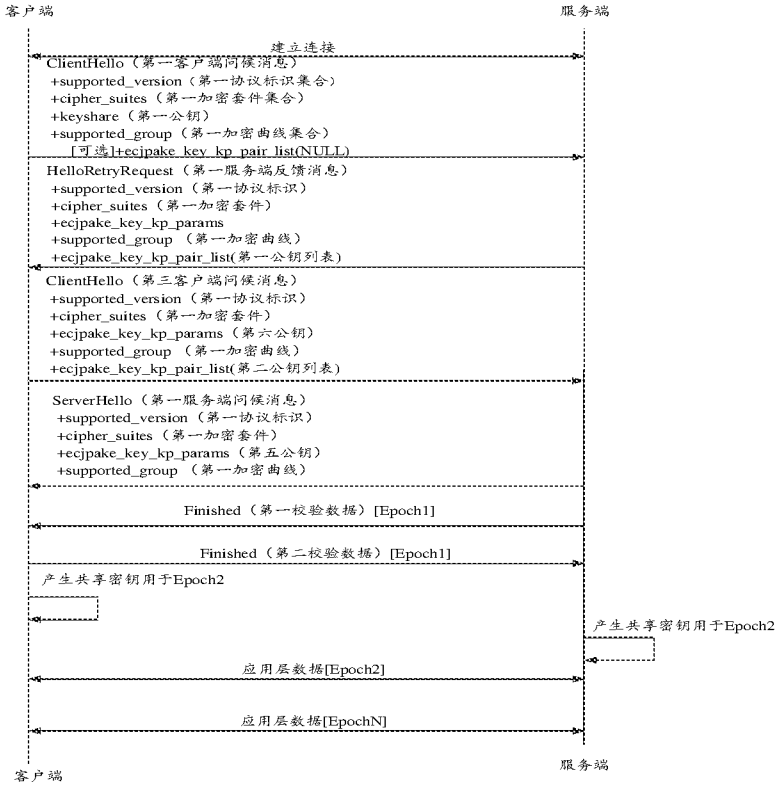
客户端
服务端
建立连接
ClientHello（第一客户端问候消息）
+supported_version（第一协议标识集合）
+cipher_suites（第一加密套件集合）
+keyshare（第一公钥）
+supported_group（第一加密曲线集合）
[可选]+ecjpake_key_kp_pair_list(NULL)
HelloRetryRequest（第一服务端反馈消息）
+supported_version（第一协议标识）
+cipher_suites（第一加密套件）
+ecjpake_key_kp_params
+supported_group（第一加密曲线）
+ecjpake_key_kp_pair_list(第一公钥列表)
ClientHello（第三客户端问候消息）
+supported_version（第一协议标识）
+cipher_suites（第一加密套件）
+ecjpake_key_kp_params（第六公钥）
+supported_group（第一加密曲线）
+ecjpake_key_kp_pair_list(第二公钥列表)
ServerHello（第一服务端问候消息）
+supported_version（第一协议标识）
+cipher_suites（第一加密套件）
+ecjpake_key_kp_params（第五公钥）
+supported_group（第一加密曲线）
Finished（第一校验数据）[Epoch1]
Finished（第二校验数据）[Epoch1]
产生共享密钥用于Epoch2
产生共享密钥用于Epoch2
应用层数据[Epoch2]
应用层数据[EpochN]
客户端
服务端

图 12

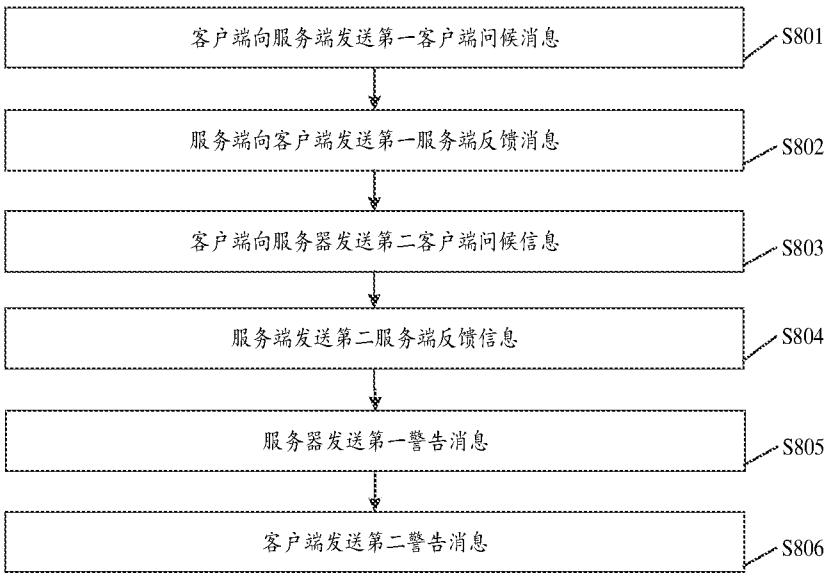
客户端向服务端发送第一客户端问候消息
S801
服务端向客户端发送第一服务端反馈消息
S802
客户端向服务器发送第二客户端问候信息
S803
服务端发送第二服务端反馈信息
S804
服务器发送第一警告消息
S805
客户端发送第二警告消息
S806

图 13

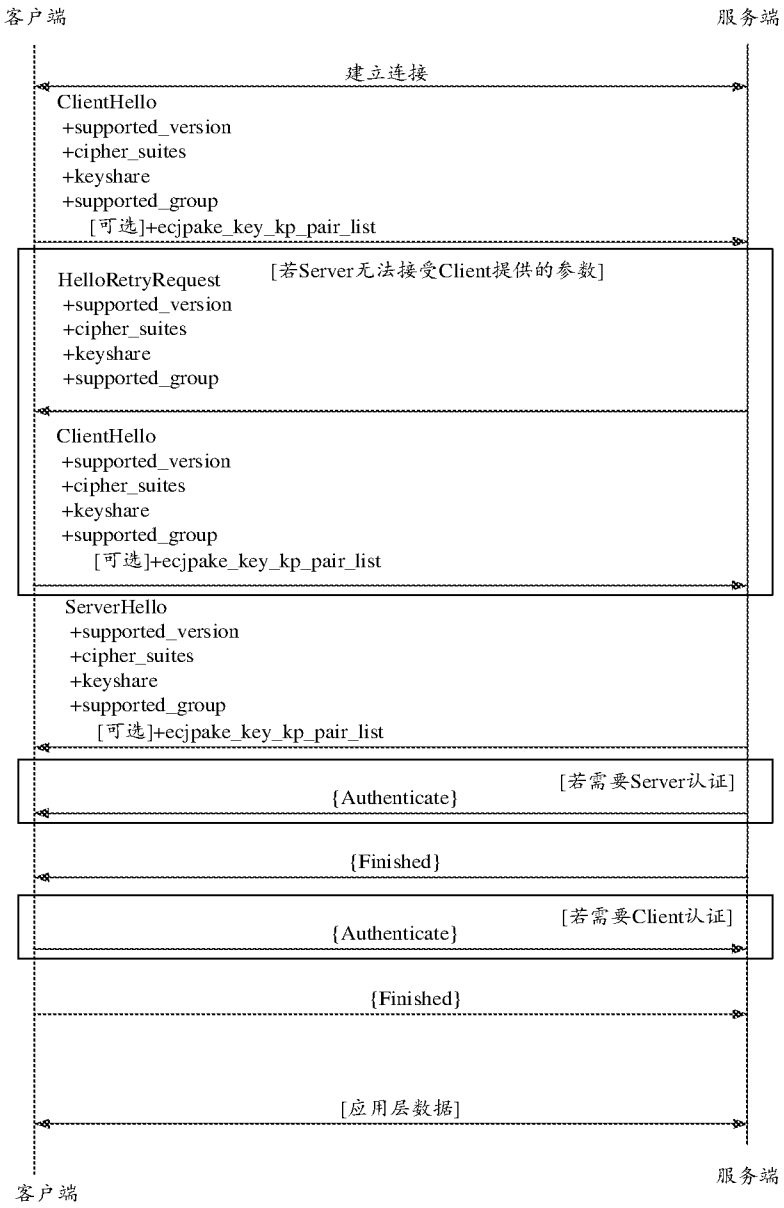
客户端
服务端
建立连接
ClientHello
+supported_version
+cipher_suites
+keyshare
+supported_group
[可选]+ecjpake_key_kp_pair_list
[若Server无法接受Client提供的参数]
HelloRetryRequest
+supported_version
+cipher_suites
+keyshare
+supported_group
ClientHello
+supported_version
+cipher_suites
+keyshare
+supported_group
[可选]+ecjpake_key_kp_pair_list
ServerHello
+supported_version
+cipher_suites
+keyshare
+supported_group
[可选]+ecjpake_key_kp_pair_list
[若需要Server认证]
{Authenticate}
{Finished}
[若需要Client认证]
{Authenticate}
{Finished}
[应用层数据]
客户端
服务端

图 14

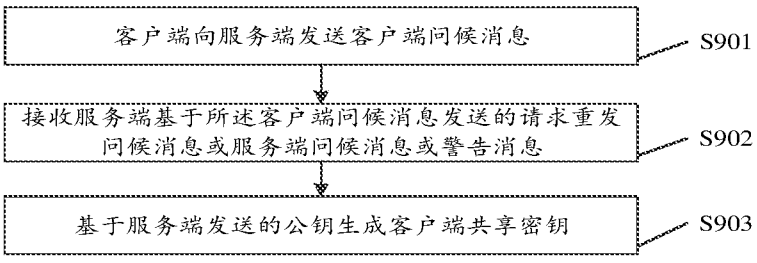
客户端向服务端发送客户端问候消息
S901
接收服务端基于所述客户端问候消息发送的请求重发问候消息或服务端问候消息或警告消息
S902
基于服务端发送的公钥生成客户端共享密钥
S903

图 15

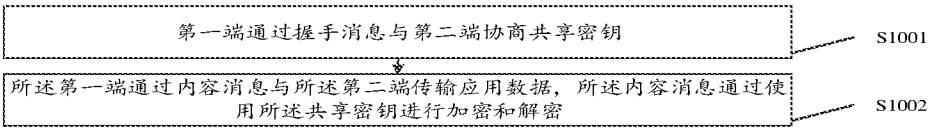
第一端通过握手消息与第二端协商共享密钥
S1001
所述第一端通过内容消息与所述第二端传输应用数据，所述内容消息通过使用所述共享密钥进行加密和解密
S1002

图 16

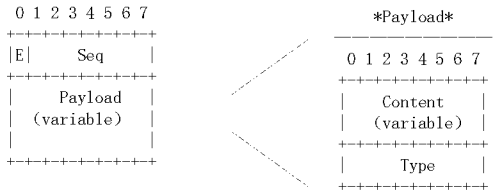

图 17

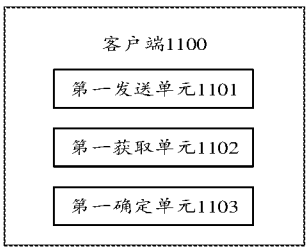

图 18

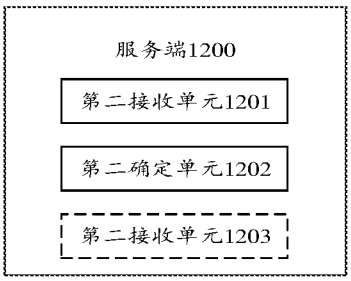

图 19

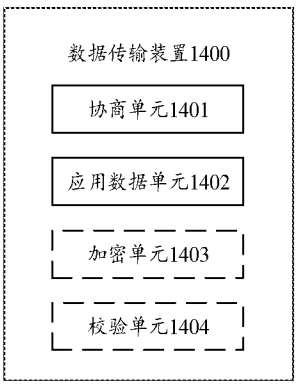

图 20

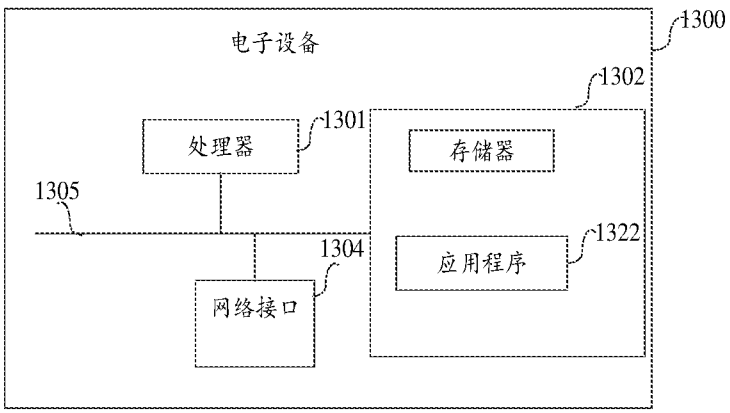

图 21

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2021/107277

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, EPODOC, WPI: 握手, 消息, 协议, 协商, 共享, 密钥, 格式, 序号, 载荷, 标识, 校验, 类型, 套件, 客户端, 服务器; handshake, message, protocol, negotiation, shared, key, format, serial, load, identification, verification, type, socket, client, server

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 109309570 A (BEIJING TOPSEC NETWORK SECURITY TECHNOLOGY CO., LTD. et al.) 05 February 2019 (2019-02-05) description paragraphs 0047-0070	1-20
A	CN 103581167 A (HUAWEI TECHNOLOGIES CO., LTD.) 12 February 2014 (2014-02-12) entire document	1-20
A	CN 104394164 A (JIN, Hu) 04 March 2015 (2015-03-04) entire document	1-20
A	CN 106453233 A (ZTEWELINK CORPORATION) 22 February 2017 (2017-02-22) entire document	1-20
A	CN 110519050 A (NO. 30 INSTITUTE OF CHINA ELECTRONIC TECHNOLOGY GROUP CORPORATION) 29 November 2019 (2019-11-29) entire document	1-20
A	WO 2012081968 A1 (MIMOS BERHAD) 21 June 2012 (2012-06-21) entire document	1-20
A	US 2019058579 A1 (7TUNNELS, INC.) 21 February 2019 (2019-02-21) entire document	1-20

☐ 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
13 October 2021	**21 October 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/CN2021/107277

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 109309570 A	05 February 2019	None	
CN 103581167 A	12 February 2014	None	
CN 104394164 A	04 March 2015	None	
CN 106453233 A	22 February 2017	None	
CN 110519050 A	29 November 2019	None	
WO 2012081968 A1	21 June 2012	MY 157055 A	29 April 2016
US 2019058579 A1	21 February 2019	EP 3286870 A2	28 February 2018
		HK 1249682 A1	02 November 2018
		CA 2983436 A1	19 January 2017
		US 2020295918 A1	17 September 2020
		AU 2016294131 A1	16 November 2017
		CN 107787568 A	09 March 2018
		WO 2017011046 A2	19 January 2017
		US 2016315763 A1	27 October 2016
		IL 255135 A	28 February 2021

国际检索报告

国际申请号
PCT/CN2021/107277

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, EPODOC, WPI：握手，消息，协议，协商，共享，密钥，格式，序号，载荷，标识，校验，类型，套件，客户端，服务器；handshake，message，protocol，negotiation，shared，key，format，serial，load，identification，verification，type，socket，client，server

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
A	CN 109309570 A (北京天融信网络安全技术有限公司 等) 2019年 2月 5日 (2019-02-05) 说明书第0047-0070段	1-20
A	CN 103581167 A (华为技术有限公司) 2014年 2月 12日 (2014-02-12) 全文	1-20
A	CN 104394164 A (金琥) 2015年 3月 4日 (2015-03-04) 全文	1-20
A	CN 106453233 A (深圳市中兴物联科技股份有限公司) 2017年 2月 22日 (2017-02-22) 全文	1-20
A	CN 110519050 A (中国电子科技集团公司第三十研究所) 2019年 11月 29日 (2019-11-29) 全文	1-20
A	WO 2012081968 A1 (MIMOS BERHAD) 2012年 6月 21日 (2012-06-21) 全文	1-20

☑ 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 10月 13日	2021年 10月 21日
ISA/CN的名称和邮寄地址 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 传真号 (86-10)62019451	受权官员 彭亮 电话号码 86-10-53961652

国际检索报告

国际申请号
PCT/CN2021/107277

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
A	US 2019058579 A1 (7TUNNELS, INC.) 2019年 2月 21日 (2019-02-21) 全文	1-20

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2021/107277

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	109309570	A	2019年 2月 5日	无			
CN	103581167	A	2014年 2月 12日	无			
CN	104394164	A	2015年 3月 4日	无			
CN	106453233	A	2017年 2月 22日	无			
CN	110519050	A	2019年 11月 29日	无			
WO	2012081968	A1	2012年 6月 21日	MY	157055	A	2016年 4月 29日
US	2019058579	A1	2019年 2月 21日	EP	3286870	A2	2018年 2月 28日
				HK	1249682	A1	2018年 11月 2日
				CA	2983436	A1	2017年 1月 19日
				US	2020295918	A1	2020年 9月 17日
				AU	2016294131	A1	2017年 11月 16日
				CN	107787568	A	2018年 3月 9日
				WO	2017011046	A2	2017年 1月 19日
				US	2016315763	A1	2016年 10月 27日
				IL	255135	A	2021年 2月 28日