(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
2023 年 3 月 16 日 (16.03.2023)

WIPO | PCT

(10) 国际公布号
WO 2023/036348 A1

(51) 国际专利分类号:
H04L 9/08 (2006.01) *H04L 61/103* (2022.01)

(21) 国际申请号: PCT/CN2022/130453

(22) 国际申请日: 2022 年 11 月 8 日 (08.11.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:

202111050009.X	2021年9月8日 (08.09.2021)	CN
202111051342.2	2021年9月8日 (08.09.2021)	CN
202111049948.2	2021年9月8日 (08.09.2021)	CN
202111051275.4	2021年9月8日 (08.09.2021)	CN

(71) 申请人: 北京世纪互联宽带数据中心有限公司 (**BEIJING VNET BROADBAND DATA CENTER CO., LTD.**) [CN/CN]; 中国北京市朝阳区酒仙桥东路10号冠捷办公楼, Beijing 100016 (CN)。

(72) 发明人: **陈升 (CHEN, Sheng)**; 中国北京市朝阳区酒仙桥东路10号冠捷办公楼, Beijing 100016 (CN)。 **李信满 (LI, Xinman)**; 中国北京市朝阳区酒仙桥东路10号冠捷办公楼, Beijing 100016 (CN)。 **蔡焜 (CAI, Kun)**; 中国北京市朝阳区酒仙桥东路10号冠捷办公楼, Beijing 100016 (CN)。 **佟磊 (TONG, Lei)**; 中国北京市朝阳区酒仙桥东路10号冠捷办公楼, Beijing 100016 (CN)。 **马炬 (MA, Ju)**; 中国北京市朝阳区酒仙桥东路10号冠捷办公楼, Beijing 100016 (CN)。

(74) 代理人: 北京同达信恒知识产权代理有限公司 (**TDIP & PARTNERS**); 中国北京市西城区裕民路18号北环中心A座2002, Beijing 100029 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI,

(54) **Title:** ENCRYPTED COMMUNICATION METHOD AND APPARATUS, DEVICE, AND STORAGE MEDIUM

(54) 发明名称: 一种加密通信方法、装置、设备及介质

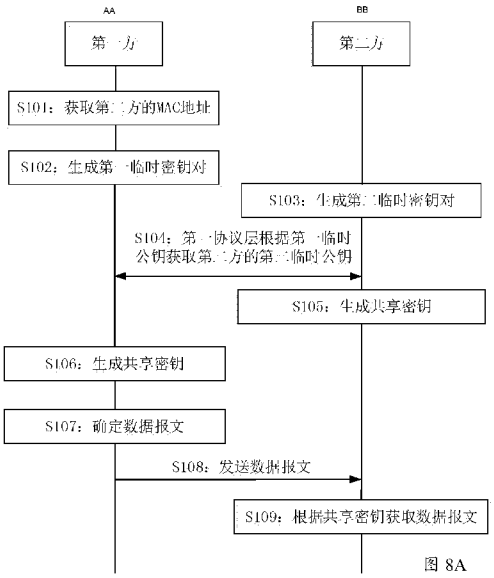

图 8A

S101 Obtain a MAC address of a second party
S102 Generate a first temporary key pair
S103 Generate a second temporary key pair
S104 The first protocol layer obtains a second temporary public key of the second party according to the first temporary public key
S105 Generate a shared key
S106 Generate a shared key
S107 Determine a data message
S108 Send the data message
S109 Obtain the data message according to the shared key
AA The first party
BB The second party

(57) **Abstract:** The present application provides an encrypted communication method and apparatus, a device, and a medium. The method comprises: a first protocol layer of a first party obtains a MAC address of a second party according to a data transmission request from an application layer, the data transmission request comprising an NLP address of the second party; the first protocol layer generates a first temporary key pair, the first temporary key pair comprising a first temporary public key and a first temporary private key; the first protocol layer obtains a second temporary public key of the second party according to the first temporary public key; the first protocol layer generates a shared key according to the second temporary public key and the first temporary private key; the first protocol layer determines a data message, the data message carrying encrypted data obtained by encrypting the shared key, and the receiver of the data message being the second party. The present method can prevent the shared key from being illegally stolen, and improve the communication security of both communication parties.

(57) **摘要**: 本申请提供一种加密通信方法、装置、设备及介质，其中，方法包括：第一方的第一协议层根据来自于应用层的数据传输请求获取第二方的MAC地址，数据传输请求中包括第二方的NLP地址；第一协议层生成第一临时密钥对，第一临时密钥对包括第一临时公钥以及第一临时私钥；第一协议层根据第一临时公钥获取第二方的第二临时公钥；第一协议层根据第二临时公钥和第一临时私钥生成共享密钥；第一协议层确定数据报文，数据报文中携带通过共享密钥加密获得的加密数据，数据报文的接收方为第二方。通过该方法，可以防止共享密钥被非法盗用，提高通信双方的通信安全。

WO 2023/036348 A1

[见续页]

GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, 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))。
— 在修改权利要求的期限届满之前进行，在收到该修改后将重新公布(细则48.2(h))。
— 包括关于请求恢复一项或多项优先权要求的信息(细则26之二.3和48.2(b)(vii))。

一种加密通信方法、装置、设备及介质

相关申请的交叉引用

本申请要求在2021年09月08日提交中国专利局、申请号为202111050009.X、申请名称为“一种加密通信方法、装置、设备及介质”的中国专利申请的优先权，其全部内容通过引用结合在本申请中；本申请要求在2021年09月08日提交中国专利局、申请号为202111051342.2、申请名称为“一种通信方法、装置、设备及介质”的中国专利申请的优先权，其全部内容通过引用结合在本申请中；本申请要求在2021年09月08日提交中国专利局、申请号为202111049948.2、申请名称为“一种源地址认证的方法、装置、电子设备及存储介质”的中国专利申请的优先权，其全部内容通过引用结合在本申请中；本申请要求在2021年09月08日提交中国专利局、申请号为202111051275.4、申请名称为“一种通信方法、装置、电子设备及存储介质”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本发明涉及网络通信技术领域，尤其涉及一种加密通信方法、装置、设备及介质。

背景技术

在互联网中，网络传输层协议通常使用的是传输控制协议（Transmission Control Protocol/Internet Protocol，TCP/IP），所有传输层如TCP、用户数据报协议（User Datagram Protocol，UDP）及其它传输层协议等的数据，都被直接封装为IP数据包进行传输。

在使用TCP/IP协议的网络层中传输数据时，攻击者可以通过IP地址欺骗目标主机，以便对目标主机进行拒绝服务攻击、伪造TCP连接、会话劫持、隐藏攻击主机地址等。对于只需接收方接收数据或信息（单边通信）的应用场景，当攻击者通过IP欺骗伪装为发送方向接收方发送攻击数据包时，由于接收方无法验证接收到的数据包的来源身份，使得接收方易被攻击。

在使用TCP/IP协议的网络中传输数据时，对于通信双方需要进行交互的场景而言，任一方被攻击都会造成双方不能进行正常通信。

鉴于此，如何实现通信过程中的数据安全，成为一个亟待解决的技术问题。

发明内容

本发明提供了一种加密通信方法、装置、设备及介质，用以解决现有技术中通信过程容易被攻击，数据传输存在风险的问题。

第一方面，本发明提供了一种加密通信方法，应用于第一方，所述第一方使用的是新链网协议（检测新链网）（new link protocol，NLP）协议栈，所述方法包括：

所述第一方的第一协议层根据来自于应用层的数据传输请求获取第二方的MAC地址，所述数据传输请求中包括所述第二方的NLP地址；所述第一协议层生成第一临时密钥对，

所述第一临时密钥对包括第一临时公钥以及第一临时私钥；所述第一协议层根据所述第一临时公钥获取所述第二方的第二临时公钥；所述第一协议层根据所述第二临时公钥和所述第一临时私钥生成共享密钥；所述第一协议层确定数据报文，所述数据报文中携带通过所述共享密钥加密获得的加密数据，所述数据报文的接收方为所述第二方。

基于该方法，可以对数据进行共享密钥加密，提高通信安全性。

在一种可能的设计中，所述第一方的第一协议层根据来自于应用层的数据传输请求获取第二方的MAC地址，所述数据传输请求中包括所述第二方的NLP地址，包括：所述第一协议层根据所述第二方的NLP地址以及第一对应关系，确定所述第二方的MAC地址，所述第一对应关系包括所述第二方的NLP地址与所述第二方的MAC地址之间的对应关系。

在一种可能的设计中，所述第一方的第一协议层根据来自于应用层的数据传输请求获取第二方的MAC地址，包括：所述第一协议层生成地址解析请求报文，所述地址解析请求报文的源地址为所述第一方的NLP地址，所述地址解析请求报文的目的地址为所述第二方的NLP地址，所述地址解析请求报文包括所述第一方的MAC地址和第一签名，所述第一签名是根据所述第一方的第一私钥生成的，所述第一方的NLP地址为所述第一私钥对应的公钥；所述第一协议层获取来自于所述第二方的第一响应报文，所述第一响应报文为所述地址解析请求报文的响应报文，所述第一响应报文的源地址为所述第二方的NLP地址，所述响应报文的目的地址为所述第一方的NLP地址，所述响应报文包括所述第二方的MAC地址和第二签名，所述第二签名是根据所述第二方的第二私钥生成的，所述第二方的NLP地址为所述第二私钥对应的公钥；所述第一协议层在根据所述第二方的NLP地址确定所述第二签名通过验证后，获得所述第二方的MAC地址。采用该设计，第一方能够获得第二方的MAC地址，使得攻击者不能通过伪造第二方的MAC地址来破坏通信安全，降低通信风险。

在一种可能的设计中，所述第一协议层根据所述第一临时公钥获取所述第二方的第二临时公钥，包括：所述第一协议层生成密钥协商请求报文，所述密钥协商请求报文包括第三签名以及所述第一临时公钥，所述密钥协商请求报文的源地址为所述第一方的NLP地址，所述密钥协商请求报文的目的地址为所述第二方的NLP地址，所述第三签名是根据所述第一方的第一私钥生成的，所述第一方的NLP地址为所述第一私钥对应的公钥；所述第一协议层获取第二响应报文，所述第二响应报文为所述密钥协商请求报文对应的响应报文，所述第二响应报文包括第四签名以及所述第二临时公钥，所述第二响应报文的源地址为所述第二方的NLP地址，所述第二响应报文的目的地址为所述第一方的NLP地址，所述第四签名是根据所述第二方的第二私钥生成的，所述第二方的NLP地址为所述第二私钥对应的公钥；所述第一协议层在根据所述第二方的NLP地址确定所述第四签名通过验证后，根据所述第一临时私钥和所述第二临时公钥确定所述共享密钥。采用该设计，利用密钥协商报文协商通信双方在通信的过程中使用的共享密钥，可以防止共享密钥被非法盗用，提高通信双方的通信安全。

第二方面，本申请还提供了一种加密通信方法，应用于第二方，所述第二方使用的是新链网NLP协议栈，所述方法包括：所述第二方的所述第二协议层获取第一方的第一临时公钥；所述第二协议层生成第二临时密钥对，所述第二临时密钥对包括第二临时公钥以及第二临时私钥；所述第二协议层根据所述第一临时公钥以及所述第二临时私钥生成共享密钥；所述第二协议层生成携带所述第二临时公钥的报文，所述报文的接收方为所述第一方，

所述第二临时公钥用于所述第一方生成所述共享密钥；所述第一协议层根据共享密钥解密数据报文中携带的加密数据，所述数据报文的发送方为所述第一方。

在一种可能的设计中，所述第二方的所述第二协议层获取第一方的第一临时公钥，包括：所述第二方的第二协议层获取来自于第一方的密钥协商请求报文，所述密钥协商请求报文包括第三签名以及所述第一临时公钥，所述密钥协商请求报文的源地址为所述第一方的 NLP 地址，所述密钥协商请求报文的目的地址为所述第二方的 NLP 地址，所述第三签名是根据所述第一方的第一私钥生成的，所述第一方的 NLP 地址为所述第一私钥对应的公钥。

在一种可能的设计中，所述第二协议层生成第二临时密钥对，包括：所述第二协议层在根据所述第一方的 NLP 地址确定所述第三签名通过验证后，生成所述第二临时密钥对。

在一种可能的设计中，所述第二协议层生成携带所述第二临时公钥的报文，包括：所述第二协议层生成第二响应报文，所述第二响应报文为所述密钥协商请求报文的响应报文，所述第二响应报文包括第四签名以及所述第二临时公钥，所述第二响应报文的源地址为所述第二方的 NLP 地址，所述第二响应报文的目的地址为所述第一方的 NLP 地址，所述第四签名是根据所述第二方的第二私钥生成的，所述第二方的 NLP 地址为所述第二私钥对应的公钥。

在一种可能的设计中，还包括：所述第二协议层接收来自于所述第一方的地址解析请求报文，所述地址解析请求报文的源地址为所述第一方的 NLP 地址，所述地址解析请求报文的目的地址为所述第二方的 NLP 地址，所述地址解析请求报文包括所述第一方的 MAC 地址和第一签名，所述第一签名是根据所述第一方的第一私钥生成的，所述第一方的 NLP 地址为所述第一私钥对应的公钥；所述第二协议层生成第一响应报文，所述第一响应报文为所述地址解析请求报文的响应报文，所述第一响应报文的源地址为所述第二方的 NLP 地址，所述响应报文的目的地址为所述第一方的 NLP 地址，所述响应报文包括所述第二方的 MAC 地址和第二签名，所述第二签名是根据所述第二方的第二私钥生成的，所述第二方的 NLP 地址为所述第二私钥对应的公钥。

第三方面，本发明提供了一种通信方法，应用于第一方，所述第一方使用的是新链网 NLP 协议栈，所述方法包括：所述第一方向第二方发送地址解析请求报文，所述地址解析请求报文的源地址为所述第一方的 NLP 地址，所述地址解析请求报文的目的地址为所述第二方的 NLP 地址，所述地址解析请求报文包括所述第一方的 MAC 地址和第一签名，所述第一签名是根据所述第一方的第一私钥生成的，所述第一方的 NLP 地址为所述第一私钥对应的公钥；所述第一方接收来自于所述第二方的第一响应报文，所述第一响应报文为所述地址解析请求报文的响应报文，所述第一响应报文的源地址为所述第二方的 NLP 地址，所述第一响应报文的目的地址为所述第一方的 NLP 地址，所述第一响应报文包括所述第二方的 MAC 地址和第二签名，所述第二签名是根据所述第二方的第二私钥生成的，所述第二方的 NLP 地址为所述第二私钥对应的公钥；所述第一方在根据所述第二方的 NLP 地址确定所述第二签名通过验证后，存储所述第二方的 NLP 地址与所述第二方的 MAC 地址之间的对应关系。

基于该方法，根据 NLP 地址/公钥实现通信双方的 MAC 地址的解析，能够应对 ARP 欺骗及其相关的中间人攻击和拒绝服务攻击，确保网络通信安全。

在一种可能的设计中，所述方法还包括：所述第一方随机生成所述第一私钥；所述第

一方根据所述第一私钥通过椭圆曲线算法生成所述第一私钥对应的公钥；所述第一方将所述第一私钥对应的公钥作为所述第一方的 NLP 地址。

采用该设计，可以为每个通信设备确定一个 NLP 地址，从而提高设备识别度。

在一种可能的设计中，所述地址解析请求报文为 VARP 报文，还包括：所述第一方根据所述第一私钥对所述地址解析请求报文中的待签名内容进行加密，获得所述第一签名。

采用该设计，可以为通信确定一个标签，使得接收侧设备能够根据该标签验证通信安全，提高通信的可靠性。

在一种可能的设计中，所述待签名内容包括时间戳，所述时间戳用于验证所述地址解析请求报文的时效性。

采用该设计，可以满足不同场景对数据时效性的需求。

在一种可能的设计中，所述第一方向第二方发送地址解析请求报文之前，还包括：

所述第一方确定邻居列表中未存储所述第二方的 MAC 地址，所述邻居列表用于存储与所述第一方进行通信的通信设备的 NLP 地址与 MAC 地址之间的对应关系。

采用该设计，可以查询已经存在的邻居列表并适当跳过一些不必要的通信环节，避免系统资源浪费。

第四方面，本发明提供了一种通信方法，应用于第二方，所述第二方使用的是新链网 NLP 协议栈，所述方法包括：所述第二方接收来自于第一方的地址解析请求报文，所述地址解析请求报文的源地址为所述第一方的 NLP 地址，所述地址解析请求报文的目的地址为所述第二方的 NLP 地址，所述地址解析请求报文包括所述第一方的 MAC 地址和第一签名，所述第一签名是根据所述第一方的第一私钥生成的，所述第一方的 NLP 地址为所述第一私钥对应的公钥；所述第二方根据所述第一方的 NLP 地址确定所述第一签名通过验证后，向所述第一方发送第一响应报文，所述第一响应报文为所述地址解析请求报文的响应报文，所述第一响应报文的源地址为所述第二方的 NLP 地址，所述第一响应报文的目的地址为所述第一方的 NLP 地址，所述第一响应报文包括所述第二方的 MAC 地址和第二签名，所述第二签名是根据所述第二方的第二私钥生成的，所述第二方的 NLP 地址为所述第二私钥对应的公钥。

在一种可能的设计中，所述方法还包括：所述第二方随机生成所述第二私钥；所述第二方根据所述第二私钥通过椭圆曲线算法生成所述第二私钥对应的公钥；所述第二方将所述第二私钥对应的公钥作为所述第二方的 NLP 地址。

在一种可能的设计中，所述第一响应报文为 VARP 报文，还包括：所述第二方根据所述第二私钥对所述第一响应报文中的待签名内容进行加密，获得所述第一签名。在一种可能的设计中，所述待签名内容包括时间戳，所述时间戳用于验证所述第一响应报文的时效性。

第五方面，本申请还提供一种源地址认证的方法，应用于发送方，所述发送方使用的是新链网 NLP 协议栈，包括：

根据数据传输请求，将发送方签名、NLP 源地址、待发送数据、防重放攻击的序列号以及 NLP 目的地址封装为一个 NLP 数据包；其中，所述发送方签名是通过所述发送方的发送方私钥生成的，所述 NLP 目的地址为所述接收方的接收方公钥，所述 NLP 源地址为所述发送方的发送方公钥，所述接收方使用的也是所述 NLP 协议栈；将所述 NLP 数据包发送给所述接收方，使所述接收方用所述 NLP 源地址验证所述发送方签名，并在验证成功

后记录所述序列号，以及获取所述待发送数据。

基于该方法，通过在发送方 NLP 数据包中携带能够验证其身份的 NLP 源地址和发送方签名、以及防重放攻击的序列号，使接收方能直接根据接收到的 NLP 数据包对其 NLP 源地址进行身份验证，这种源地址认证的方式具备去中心化自证与它证、发送方不可抵赖、杜绝 DDOS 攻击等特点；并验证其是否为重放攻击的数据包，在任一个验证不通过时，丢弃 NLP 数据包，从而能够在防止 IP 地址欺骗的同时有效地抵御直接复制报文的重放攻击，提高接收方的安全性，当应用在对时效性要求较高的单边通信中时，能够同时让接收高具有高时效性和高网络安全性。

在一种可能的设计中，所述将发送方签名、NLP 源地址、待发送数据、防重放攻击的序列号以及 NLP 目的地址封装为一个 NLP 数据包之前，还包括：随机生成所述发送方私钥；基于非对称加密算法和所述发送方私钥，生成所述发送方公钥。

在一种可能的设计中，将发送方签名、NLP 源地址、待发送数据、防重放攻击的序列号以及 NLP 目的地址封装为一个 NLP 数据包，包括：从所述数据传输请求中获取所述 NLP 目的地址和所述待发送数据；对所述 NLP 目的地址进行解析，获得所述接收方的接收方物理地址；用所述发送方私钥对所述 NLP 数据包中至少包含所述序列号及随机数的部分头部信息进行加密，获得所述发送方签名；将所述发送方签名、所述 NLP 源地址、所述发送方的发送方物理地址、所述 NLP 目的地址、所述接收方物理地址以及所述待发送数据封装为所述 NLP 数据包。

在一种可能的设计中，所述发送方连续发送给所述接收方的多个数据包中的多个序列号是按升序设置的。

在一种可能的设计中，所述序列号包括时间戳。

第六方面，本申请还提供一种源地址认证的方法，应用于接收方，所述接收方使用的是新链网 NLP 协议栈，包括：接收发送方发送的 NLP 数据包；其中，所述 NLP 数据包是由发送方签名、NLP 源地址、待发送数据、防重放攻击的序列号以及 NLP 目的地址封装成的，所述发送方签名是通过所述发送方的发送方私钥生成的，所述 NLP 目的地址为所述接收方的接收方公钥，所述 NLP 源地址为所述发送方的发送方公钥，所述发送方使用的也是所述 NLP 协议栈；从所述 NLP 数据包中获取所述 NLP 源地址、所述发送方签名及所述序列号；通过所述 NLP 源地址、所述发送方签名及所述序列号验证所述 NLP 数据包来源的真实性和非重复性，若都验证通过则存储所述序列号并获取所述待发送数据，否则丢弃所述 NLP 数据包。

在一种可能的设计中，通过所述 NLP 源地址、所述发送方签名及所述序列号验证所述 NLP 数据包来源的真实性和非重复性，包括：用所述 NLP 源地址验证所述发送方签名，若验证成功则确定所述 NLP 数据包的来源为所述发送方；判断所述序列号是否大于从所述发送方接收到的上一个 NLP 数据包中的序列号，若为是，则确定所述 NLP 数据包是非重复的。

第七方面，本发明提供了一种通信方法，应用于第一方，所述第一方使用的是新链网 NLP 协议栈，所述方法包括：

根据数据传输请求，生成包含第一签名、第一 NLP 地址、及第一临时公钥的密钥协商报文；其中，所述密钥协商报文用于所述第一方与所述第二方进行身份认证和密钥交换，所述第一签名是通过所述第一方的第一私钥生成的，所述第一 NLP 地址为所述第一方的第

一公钥；将所述密钥协商报文发送给所述第二方，使所述第二方用所述第一签名和所述第一 NLP 地址验证所述第一方的身份，并在验证成功后存储所述第一临时公钥，及生成包含第二签名、第二 NLP 地址及第二临时公钥的响应报文；其中，所述第二签名是通过所述第二方的第二私钥生成的，所述第二 NLP 地址为所述第二方的第二公钥，所述第二方使用的也是所述 NLP 协议栈；接收所述响应报文，并用所述第二签名和所述第二 NLP 地址验证所述第二方的身份，在验证成功后，根据椭圆曲线迪菲-赫尔曼秘钥交换 ECDH，对与所述第一临时公钥对应的第一临时私钥及所述第二临时公钥进行计算，得到共享密钥；在与所述第二方进行数据交互时，用所述共享密钥进行数据的加密传输。

基于该方法，根据所述新链网 NLP 协议栈，可以提高通信安全。

在一种可能的设计中，生成包含第一签名、第一 NLP 地址以及第一临时公钥的密钥协商报文之前，还包括：根据所述 ECDH 生成第一临时密钥对；将所述第一临时密钥对中的公钥作为所述第一临时公钥；将所述第一临时密钥对中的私钥作为所述第一临时私钥。

在一种可能的设计中，生成包含第一签名、第一 NLP 地址以及第一临时公钥的密钥协商报文之前，还包括：随机生成所述第一私钥；采用非对称加密算法和所述第一私钥生成所述第一公钥。

在一种可能的设计中，生成包含第一签名、第一 NLP 地址以及第一临时公钥的密钥协商报文，包括：从所述数据传输请求中获取所述第二 NLP 地址；对所述第二 NLP 地址进行解析，获得所述第二方的第二物理地址；用所述第一私钥对所述密钥协商报文中至少包含所述第一临时公钥和时间戳的部分头部信息进行加密，获得所述第一签名；其中，所述时间戳用于验证所述密钥协商报文的时效性；将所述第一签名、所述第一 NLP 地址、所述第一方的第一物理地址、所述第二 NLP 地址、所述第二物理地址以及所述第一临时公钥封装为所述密钥协商报文。

在一种可能的设计中，所述部分头部信息，包括：所述密钥协商报文的 NLP 基本头部和 NLP 扩展头部；或，所述 NLP 基本头部中的部分头部和所述 NLP 扩展头部。

在一种可能的设计中，用所述第二签名和所述第二 NLP 地址验证所述第二方的身份，包括：用所述第二 NLP 地址验证所述第二签名；若验证成功，则确定所述第二方的身份验证成功；若用所述第二 NLP 地址验证所述第二签名失败，则确定所述第二方的身份验证失败，并丢弃所述响应报文。

在一种可能的设计中，在与所述第二方进行数据交互时，用所述共享密钥进行数据的加密传输，包括：当向所述第二方发送待传输数据时，从所述数据传输请求中获取所述待传输数据；并用具有关联数据的认证加密 AEAD 性质的对称加密算法及所述共享密钥加密所述待传输数据，获得加密后的待传输数据；其中，所述待传输数据为得到所述第一方的 NLP 协议栈中网络层之上的多层数据；将所述加密后的待传输数据封装在第一 NLPSec 报文中，并发送给所述第二方；当接收到所述第二方发送的第二 NLPSec 报文后，用所述对称加密算法和所述共享密钥，对所述第二 NLPSec 报文中的加密数据进行解密及完整性校验，在校验成功后将解密后的数据传输给所述第一方的 NLP 协议栈中的传输层进行处理。

第八方面，本申请还提供了一种通信装置，用于实现第一方面及其任一可能的设计中的方法。

在一种可能的实现方式中，该装置包括：MAC 地址获取模块，所述获取模块用于根据来自于应用层的数据传输请求获取第二方的 MAC 地址，所述数据传输请求中包括所述

第二方的 NLP 地址。

在一种可能的实现方式中，该装置包括：密钥生成模块，所述密钥生成模块用于生成第一临时密钥对，所述第一临时密钥对包括第一临时公钥以及第一临时私钥。

在一种可能的实现方式中，所述密钥生成模块，还用于根据所述第一临时公钥获取所述第二方的第二临时公钥，并根据所述第二临时公钥和所述第一临时私钥生成共享密钥。

在一种可能的实现方式中，该装置包括：确定模块，所述确定模块用于确定数据报文，所述数据报文中携带所述第二方的 MAC 地址和通过所述共享密钥加密获得的加密数据，所述数据报文的接收方为所述第二方。

第九方面，本申请还提供了一种通信装置，用于实现第二方面及其任一可能的设计中的方法。

在一种可能的实现方式中，该装置可包括：获取模块，所述获取模块用于获取第一方的第一临时公钥。

在一种可能的实现方式中，该装置包括：密钥生成模块，所述密钥生成模块用于生成第二临时密钥对，所述第二临时密钥对包括第二临时公钥以及第二临时私钥。

在一种可能的实现方式中，所述密钥生成模块还用于根据所述第一临时公钥以及所述第二临时私钥生成共享密钥。

在一种可能的实现方式中，该装置包括：报文生成模块，所述报文生成模块用于生成携带所述第二临时公钥的报文，所述报文的接收方为所述第一方，所述第二临时公钥用于所述第一方生成所述共享密钥。

在一种可能的实现方式中，该装置包括：解密模块，所述解密模块用于根据共享密钥解密数据报文中携带的加密数据，所述数据报文的发送方为所述第一方，所述数据报文还携带所述第二方的 MAC 地址。

第十方面，本申请还提供了一种通信装置，应用于第一方，所述第一方使用的是新链网 NLP 协议栈。

在一种可能的实现方式中，该装置包括：报文发送模块，用于发送地址解析请求报文，所述地址解析请求报文的源地址为所述第一方的 NLP 地址，所述地址解析请求报文的目的地址为所述第二方的 NLP 地址，所述地址解析请求报文包括所述第一方的 MAC 地址和第一签名，所述第一签名是根据所述第一方的第一私钥生成的，所述第一方的 NLP 地址为所述第一私钥对应的公钥。

在一种可能的实现方式中，该装置包括：报文接收模块，用于接收来自于所述第二方的第一响应报文，所述第一响应报文为所述地址解析请求报文的响应报文，所述第一响应报文的源地址为所述第二方的 NLP 地址，所述第一响应报文的目的地址为所述第一方的 NLP 地址，所述第一响应报文包括所述第二方的 MAC 地址和第二签名，所述第二签名是根据所述第二方的第二私钥生成的，所述第二方的 NLP 地址为所述第二私钥对应的公钥。

在一种可能的实现方式中，该装置包括：存储模块，用于在根据所述第二方的 NLP 地址确定所述第二签名通过验证后，存储所述第二方的 NLP 地址与所述第二方的 MAC 地址之间的对应关系。

第十一方面，本申请还提供了一种通信装置，应用于第二方，所述第二方使用的是新链网 NLP 协议栈。

在一种可能的实现方式中，该装置包括：报文接收模块，用于接收来自于第一方的地

址解析请求报文，所述地址解析请求报文的源地址为所述第一方的NLP地址，所述地址解析请求报文的目的地址为所述第二方的NLP地址，所述地址解析请求报文包括所述第一方的MAC地址和第一签名，所述第一签名是根据所述第一方的第一私钥生成的，所述第一方的NLP地址为所述第一私钥对应的公钥。

在一种可能的实现方式中，该装置包括：报文发送模块，用于根据所述第一方的NLP地址确定所述第一签名通过验证后，向所述第一方发送第一响应报文，所述第一响应报文为所述地址解析请求报文的响应报文，所述第一响应报文的源地址为所述第二方的NLP地址，所述第一响应报文的目的地址为所述第一方的NLP地址，所述第一响应报文包括所述第二方的MAC地址和第二签名，所述第二签名是根据所述第二方的第二私钥生成的，所述第二方的NLP地址为所述第二私钥对应的公钥。

第十二方面，本申请还提供了一种通信装置，用于实现第三方面及其任一可能的设计中的方法。

在一种可能的实现方式中，该装置包括：报文发送模块，用于发送地址解析请求报文，所述地址解析请求报文的源地址为所述第一方的NLP地址，所述地址解析请求报文的目的地址为所述第二方的NLP地址，所述地址解析请求报文包括所述第一方的MAC地址和第一签名，所述第一签名是根据所述第一方的第一私钥生成的，所述第一方的NLP地址为所述第一私钥对应的公钥。

在一种可能的实现方式中，该装置包括：报文接收模块，用于接收来自于所述第二方的第一响应报文，所述第一响应报文为所述地址解析请求报文的响应报文，所述第一响应报文的源地址为所述第二方的NLP地址，所述第一响应报文的目的地址为所述第一方的NLP地址，所述第一响应报文包括所述第二方的MAC地址和第二签名，所述第二签名是根据所述第二方的第二私钥生成的，所述第二方的NLP地址为所述第二私钥对应的公钥；

在一种可能的实现方式中，该装置包括：存储模块，用于在根据所述第二方的NLP地址确定所述第二签名通过验证后，存储所述第二方的NLP地址与所述第二方的MAC地址之间的对应关系。

第十三方面，本申请还提供了一种通信装置，用于实现第四方面及其任一可能的设计中的方法。

在一种可能的实现方式中，该装置包括：报文接收模块，用于接收来自于第一方的地址解析请求报文，所述地址解析请求报文的源地址为所述第一方的NLP地址，所述地址解析请求报文的目的地址为所述第二方的NLP地址，所述地址解析请求报文包括所述第一方的MAC地址和第一签名，所述第一签名是根据所述第一方的第一私钥生成的，所述第一方的NLP地址为所述第一私钥对应的公钥。

在一种可能的实现方式中，该装置包括：报文发送模块，用于根据所述第一方的NLP地址确定所述第一签名通过验证后，向所述第一方发送第一响应报文，所述第一响应报文为所述地址解析请求报文的响应报文，所述第一响应报文的源地址为所述第二方的NLP地址，所述第一响应报文的目的地址为所述第一方的NLP地址，所述第一响应报文包括所述第二方的MAC地址和第二签名，所述第二签名是根据所述第二方的第二私钥生成的，所述第二方的NLP地址为所述第二私钥对应的公钥。

第十四方面，本申请还提供一种源地址认证的装置，用于实现第五方面及其任一可能的设计中的方法。

在一种可能的实现方式中，该装置包括：封装单元，用于根据数据传输请求，将发送方签名、NLP 源地址、待发送数据、防重放攻击的序列号以及 NLP 目的地址封装为一个 NLP 数据包；其中，所述发送方签名是通过所述发送方的发送方私钥生成的，所述 NLP 目的地址为所述接收方的接收方公钥，所述 NLP 源地址为所述发送方的发送方公钥，所述接收方使用的也是新链网 NLP 协议栈。

在一种可能的实现方式中，该装置包括：发送单元，用于将所述 NLP 数据包发送给所述接收方，使所述接收方用所述 NLP 源地址验证所述发送方签名，并在验证成功后记录所述序列号，以及获取所述待发送数据。

一种可能的实施方式，该装置还包括：生成单元，用于随机生成所述发送方私钥；基于非对称加密算法和所述发送方私钥，生成所述发送方公钥。

一种可能的实施方式，所述封装单元还用于：从所述数据传输请求中获取所述 NLP 目的地址和所述待发送数据；对所述 NLP 目的地址进行解析，获得所述接收方的接收方物理地址；用所述发送方私钥对所述 NLP 数据包中至少包含所述序列号及随机数的部分头部信息进行加密，获得所述发送方签名；将所述发送方签名、所述 NLP 源地址、所述发送方的发送方物理地址、所述 NLP 目的地址、所述接收方物理地址以及所述待发送数据封装为所述 NLP 数据包。

一种可能的实施方式，所述发送方连续发送给所述接收方的多个数据包中的多个序列号是按升序设置的。

一种可能的实施方式，所述序列号包括时间戳。

第十五方面，本申请还提供一种源地址认证的装置，用于实现第六方面及其任一可能的设计中的方法。

在一种可能的实现方式中，该装置包括：接收单元，用于接收发送方发送的 NLP 数据包；其中，所述 NLP 数据包是由发送方签名、NLP 源地址、待发送数据、防重放攻击的序列号以及 NLP 目的地址封装成的，所述发送方签名是通过所述发送方的发送方私钥生成的，所述 NLP 目的地址为所述接收方的接收方公钥，所述 NLP 源地址为所述发送方的发送方公钥，所述发送方使用的也是新链网 NLP 协议栈。

在一种可能的实现方式中，该装置包括：获取单元，用于从所述 NLP 数据包中获取所述 NLP 源地址、所述发送方签名及所述序列号。

在一种可能的实现方式中，该装置包括：验证单元，用于通过所述 NLP 源地址、所述发送方签名及所述序列号验证所述 NLP 数据包来源的真实性和非重复性，若都验证通过则存储所述序列号并获取所述待发送数据，否则丢弃所述 NLP 数据包。

一种可能的实施方式，所述验证单元还用于：用所述 NLP 源地址验证所述发送方签名，若验证成功则确定所述 NLP 数据包的来源为所述发送方；判断所述序列号是否大于从所述发送方接收到的上一个 NLP 数据包中的序列号，若为是，则确定所述 NLP 数据包是非重复的。

第十六方面，本申请还提供一种通信装置，应用于第一方。

在一种可能的实现方式中，该装置包括：生成单元，用于根据数据传输请求，生成包含第一签名、第一 NLP 地址、及第一临时公钥的密钥协商报文；其中，所述密钥协商报文用于所述第一方与所述第二方进行身份认证和密钥交换，所述第一签名是通过所述第一方的第一私钥生成的，所述第一 NLP 地址为所述第一方的第一公钥。

在一种可能的实现方式中，该装置包括：验证单元，用于将所述密钥协商报文发送给所述第二方，使所述第二方用所述第一签名和所述第一 NLP 地址验证所述第一方的身份，并在验证成功后存储所述第一临时公钥，及生成包含第二签名、第二 NLP 地址及第二临时公钥的响应报文；其中，所述第二签名是通过所述第二方的第二私钥生成的，所述第二 NLP 地址为所述第二方的第二公钥，所述第二方使用的也是所述 NLP 协议栈；

在一种可能的实现方式中，该装置包括：传输单元，用于接收所述响应报文，并用所述第二签名和所述第二 NLP 地址验证所述第二方的身份，在验证成功后，根据椭圆曲线迪菲-赫尔曼秘钥交换 ECDH，对与所述第一临时公钥对应的第一临时私钥及所述第二临时公钥进行计算，得到共享密钥；在与所述第二方进行数据交互时，用所述共享密钥进行数据的加密传输。

第十七方面，提供一种计算机可读存储介质，该计算机可读存储介质中存储有计算机程序或指令，当所述计算机程序或指令在计算机上运行时，使得所述计算机实现前述第一方面至第七方面及其任意可能的实现方式中的方法。

第十八方面，提供一种芯片，该芯片包括处理器，还可以包括存储器，所述处理器与存储器耦合，用于执行所述存储器中存储的计算机程序或指令，使得芯片实现前述第一方面或第七方面及其任意可能的实现方式中的方法。

附图说明

为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简要介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域的普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

图1为本申请实施例提供的一种NLP数据包的封装结构示意图；

图2为本申请实施例提供的一种NLP数据包中NLP基本头部的结构示意图；

图3为本申请实施例提供的一种NLPKey扩展头部的结构示意图；

图4为本申请实施例提供的一种NLPSec扩展头部的结构示意图；

图5为本申请实施例提供的一种VARP包结构的结构示意图；

图6为本申请实施例提供的一种密钥协商报文的结构示意图；

图7为本申请实施例提供的一种NLPSec包封装的结构示意图；

图8A为本申请实施例提供的一种通信方法的过程示意图；

图8B为本申请实施例提供的另一种通信方法的过程示意图；

图8C为本申请实施例提供的一种通信装置（或设备）的模块化结构示意图；

图8D为本申请实施例提供的一种通信方法的通信装置（或设备）结构示意图；

图8E为本申请实施例提供的另一种通信方法的通信装置（或设备）结构示意图；

图8F为本申请实施例提供的另一种通信方法的通信装置（或设备）结构示意图；

图8G为本申请实施例提供的另一种通信方法的通信装置（或设备）结构示意图；

图9A为本申请实施例提供的另一种通信装置（或设备）的模块化结构示意图；

图9B为本申请实施例提供的另一种通信装置（或设备）的模块化结构示意图；

图9C为本申请实施例提供的另一种通信装置（或设备）的模块化结构示意图；

图10为本申请实施例提供的另一种通信方法的通信装置（或设备）结构示意图；

图11为本申请实施例提供的另一种通信装置（或设备）的模块化结构示意图。

具体实施方式

为了使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明作进一步地详细描述，显然，所描述的实施例仅仅是本发申请一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其它实施例，都属于本发明保护的范围。

为了提高通信安全，降低数据传输的风险，本发明实施例提供了一种加密通信方法、装置、设备及介质。

为了使本领域的技术人员能充分理解本发明，现对 NLP 协议栈做一个简单的介绍。

请参见表 1 为本发明实施例提供的 NLP 协议栈的结构示意图。

层标识	层名称	需要遵循的通信协议	
LAYER5	应用层	如，超文本传输协议（Hyper Text Transfer Protocol，HTTP）	
NLP 通信接口（NLP Socket API）			
LAYER4	传输层	TCP	传输层协议（Transmission Protocol，TP）
LAYER3	网络层	NLP	公钥地址解析协议（VNET Address Resolution Protocol，VARP）
LAYER2	数据链路层	以太网（ethernet，ETH）协议	
PHY	物理层		

表 1

NLP 协议栈相当于将传统 IP 协议栈中的网络层使用的 IP 协议改为 NLP 协议。在 NLP 协议栈通信双方使用的网络地址为 NLP 地址，该 NLP 地址为本地生成的 32 字节的公钥。

通过 NLP 协议栈生成的数据包被称之为 NLP 数据包，通过 NLP 协议栈生成的报文称之为 NLP 协议报文。

VARP 是对 ARP 协议的扩展，用于解析 NLP 地址和 MAC 地址的映射关系。本申请中将基于 NLP 地址的请求和应答 ARP 包称之为 VARP 包。为了实现安全，防止 ARP 欺骗，VARP 头部之后增加签名，签名内容可以为 VARP 头前 88 字节，用于身份认证。其中，签名可以用私钥加密生成。

请参见图 1 为本发明实施例提供的一种 NLP 数据包的封装结构示意图。

NLP 数据包包括以太头（占用 14 字节）、NLP 基本头部（占用 72 字节）、NLP 扩展头部（可有、可无，即可选）、传输层头部（占用字节长度可以跟实际需要设置，即不定长）、数据（不定长）。

请参见图 2 为本发明实施例提供的一种 NLP 数据包中 NLP 基本头部的结构示意图。

NLP 基本头部可包括以下字段:

版本（占用 1 字节），表示使用的 NLP 协议版本。

服务（占用 1 字节），表示提供的服务类型，类似 IP 中的 ToS 字段。

流标签（占用 2 字节），标记报文的数据流类型，可用于质量服务。

包长度（占用 2 字节），包含 NLP 基本头部的长度，NLP 扩展头部的长度和数据的长

度。

下个头（占用 1 字节），用于指示下一个扩展头或者上层协议类型。

跳数（占用 1 字节），用于指示限制 NLP 数据包被转发的次数。

NLP 源地址（占用 32 字节），用于指示发送方的 NLP 地址。

NLP 目的地址（占用 32 字节），用于指示接收方的 NLP 地址。

上述 NLP 数据包中的 NLP 扩展头部可包括 NLPKey 扩展头部和 NLPSec 扩展头部等。

请参见图 3 为本发明实施例提供的一种 NLPKey 扩展头部的结构示意图。

NLPKey 扩展头部包括以下字段:

下个头（占用 1 字节），表示下一个扩展头或者上层协议类型。

类型（占用 1 字节），表示 NLP 数据包是属于请求的类型，还是属于回复的类型，如主动连接方（发送方）发送的是请求，被动连接方（接收方）返回的是响应。

保留（占用 2 字节），预留的位置，用于后续有需要时使用。

时间戳（占用 4 字节），用于确认 NLP 数据包的时效性。

临时公钥（占用 32 字节），在通信双方交互时临时生成的，用于与对端交换公钥，以计算共享密钥。其中，协议栈生成的临时密钥对包含临时公钥。其中，临时密钥对和共享密钥与对端绑定。

数字签名（占用 64 字节），通常对扩展头部前 40 个字节进行加密签名，以认证身份，同时也可以保证扩展头内容的完整性。

请参见图 4 为本发明实施例提供的一种 NLPSec 扩展头部的结构示意图。

NLPSec 扩展头部包括:

下个头（占用 1 字节），表示下一个扩展头或者上层协议类型。

保留（占用 1 字节），预留的位置，用于后续有需要时使用。

加密数据长度（占用 2 字节），被加密的数据的长度。

序列号（占用 4 字节），保证了即使是完全相同的原始数据传输(如重传)，因为序列号的不同，而使得密文（加密数据）也不相同。

请参见图 5 为本发明实施例提供的一种 VARP 包结构的结构示意图。

VARP 包结构可包括硬件类型（占用 2 字节）、协议（占用 2 字节）、硬件地址大小（占用 1 字节）、地址大小（占用 1 字节）、请求类型（占用 2 字节）和时间戳+签名（占用 4+64 字节）等字段。

此外，VARP 包结构还可包括:

源 MAC 地址（占用 6 字节），用于指示发送方的 MAC 地址。

NLP 源地址（占用 32 字节），用于指示发送方的 NLP 地址。

目的 MAC 地址（占用 6 字节），用于指示接收方的 MAC 地址。

NLP 目的地址（占用 32 字节），用于指示接收方的 NLP 地址。

参见图 6 为本发明实施例提供的一种密钥协商报文的结构示意图。

密钥协商报文可包括以太头部、NLP 基本头部和 NLPKey 扩展头部，NLPKey 扩展头部占用 104 字节。

请参见图 7 为本发明实施例提供的一种 NLPSec 包封装的结构示意图。

NLPSec 数据包即为 NLP 数据包中 NLP 扩展头部为 NLPSec 扩展头部，NLPSec 扩展头部占用 8 字节，且不包含传输层头部，而是将传输层头部的数据作为数据的一部分，一

起进行加密，得到加密数据，加密数据是对 NLP 协议栈中三层（layer3）以上的数据进行加密。

NLPSec 包封装可包括以太头（占用 2 字节）、NLP 基本头部（占用 2 字节）、NLPSec 扩展头（占用 2 字节）和加密数据（占用 2 字节）等字段。

下面将结合方法实施例对本申请提供的通信过程进行介绍。

图 8A 为本发明实施例提供的一种通信方法的过程示意图，该过程可由第一方和第二方执行。其中，第一方可以是加密数据的发送方，第二方可以是加密数据的接收方。

该过程包括以下步骤:

S101: 第一方的第一协议层根据来自于应用层的数据传输请求获取第二方的 MAC 地址，数据传输请求中包括第二方的 NLP 地址。

具体的，应用层调用第一方的第一协议层或其他传输层协议的 API 接口，在该接口上接收上层协议或者应用的数据传输请求，该数据传输请求可用于请求向第二方发送数据。其中，数据传输请求包括第二方的 NLP 地址以及数据内容。该 API 接口可以是类 Socket 接口，是基于 NLP 地址而不是 IP 地址进行通信的接口。

在一种可能的实现方式中，获取第二方的 MAC 地址的方式例如: 第一方的第一协议层根据该数据传输请求确定第二方的 MAC 地址。第一方的第一协议层判断第一方与第二方的数据传输连接是否存在，若存在，则执行 S107。若不存在，则继续执行下一步骤。

本申请中，数据传输连接（简称为连接）是指获得用于加密数据的共享密钥之后，第一方与第二方之间建立的加密通信连接，该连接用于第一方与第二方之间参数加密数据。在第一方与第二方之间的加密通信过程中，如果第一方和第二方中的发送方确定该连接存在，则可使用共享密钥进行通信，无需重新获取共享密钥，相应地，第一方和第二方中的接收方可使用共享密钥进行数据的解密。可选的，连接可能因为建立时间超时等原因而断开。

在另一种可能的实现方式中，第一协议层可以根据第二方的 NLP 地址以及第一对应关系，确定第二方的 MAC 地址。第一对应关系包括多个设备的 NLP 地址与 MAC 地址之间的对应关系，多个设备包括但不限于第一方和/或第二方。其中，第一对应关系可以由第一协议层根据历史通信记录获得，比如，第一方每与一个设备进行通信，则记录对方设备的 NLP 地址与 MAC 地址的对应关系，存储至第一对应关系中，则在下一次进行通信时，第一协议层可从第一对应关系中查询对方设备。

本申请中第一对应关系可以通过邻居列表的形式存储。如果第一协议层查询邻居列表能够确定第二方的 MAC 地址，则可根据第二方的 MAC 地址获取共享密钥，获取共享密钥的过程可参照本申请中的说明。

可选的，本申请中，第一方和第二方都具备 NLP 地址。其中，NLP 地址的确定可以是先随机生成私钥（32 字节），再通过椭圆曲线算法 ED25519 生成公钥（32 字节）。生成的公钥即为 NLP 地址。

可选的，第一协议层可以是第一方的网络层，也可以是其他的协议层。

可选的，第一协议层生成地址解析请求报文，地址解析请求报文的源地址为第一方的 NLP 地址，地址解析请求报文的目的地址为第二方的 NLP 地址，地址解析请求报文包括第一方的 MAC 地址和第一签名，第一签名是根据第一方的第一私钥生成的，第一方的 NLP

地址为第一私钥对应的公钥。第一协议层获取来自于第二方的第一响应报文，第一响应报文为地址解析请求报文的响应报文，第一响应报文的源地址为第二方的NLP地址，第一响应报文的目的地址为第一方的NLP地址，第一响应报文包括第二方的MAC地址和第二签名，第二签名是根据第二方的第二私钥生成的，第二方的NLP地址为第二私钥对应的公钥。第一协议层在根据第二方的NLP地址确定第二签名通过验证后，获得第二方的MAC地址。

具体的，地址解析请求报文可以是VARP报文，第一响应报文可以是VARP响应报文。此时第一方的第一协议层可构造VARP请求报文，并将该报文发送给第二方，报文格式按照上述VARP包结构。其中，VARP请求报文包含第一方的NLP地址、第二方的NLP地址、第一方的MAC地址（作为源地址）、广播MAC地址（作为目的地址）、序列号和第一签名。第二方的第二协议层收到VARP请求报文，用第一方的NLP地址作为公钥验证第一签名，若验证成功，则保存第一方的第一对应关系，即保存第一方的NLP地址与第一方的MAC地址之间的对应关系。若验证失败，则丢弃该报文，结束本流程。第二协议层构造并发送VARP响应报文，报文格式按照上述VARP包结构。其中，VARP响应报文包含第二方的NLP地址、第一方的NLP地址、第二方的MAC地址（作为源地址）、第一方的MAC地址（作为目的地址）、序列号和第二签名。第一协议层收到VARP响应报文，用第二方的NLP地址作为公钥验证第二签名。若验证成功，保存第二方的第一对应关系，即保存第二方的NLP地址与MAC地址之间的对应关系。若验证失败，则丢弃该报文，结束本流程。至此，地址解析完成。

可选的，第二协议层可以是第二方的网络层，也可以是其他的协议层。

可选的，以第一协议层生成第一签名为例，第一签名根据第一方的私钥和待签名内容生成，第一签名占用64字节。其中，待签名内容可包括图5所示的硬件类型、协议、硬件地址大小、地址大小、请求类型、源MAC地址、NLP源地址、目的MAC地址、NLP目的地址以及时间戳在内的88个字节。

可选的，第一协议层和第二协议层可以通过将各自生成的临时密钥对和共享密钥绑定，结合设置的时间戳，为共享密钥设置失效机制，例如，当到达时间戳对应的失效时间时，强制双方重新协商生成新的共享密钥进行数据传输。例如，时间戳设置为30分钟，则密钥协商报文生成的共享密钥的有效时间为30分钟。另外，根据不同密钥协商报文中的时间戳也可以识别用于承载最新的临时密钥对的密钥协商报文。

可选的，S101之前，第一协议层可以判断第一方与第二方之间的连接是否存在（或者说，判断第一方是否存储由第一方和第二方使用的共享密钥，该共享密钥可参照本申请中的介绍生成），如果存在就可以根据该共享密钥进行加密传输，即跳过S101执行S107。如果不存在该连接，则第一协议层可以根据第二方的NLP地址进一步查询邻居列表判断是否存储有第二方的MAC地址，如果存储有第二方的MAC地址，可以执行重新获取共享密钥，即跳过S101执行S102。如果既不存在该连接，也不存在第二方的MAC地址，则第一协议层可以需要获取第二方的MAC地址，即执行S101。

S102：第一协议层生成第一临时密钥对，第一临时密钥对包括第一临时公钥以及第一临时私钥。

其中，第一临时密钥对是随机生成的。

可选的，可以使用椭圆曲线X25519生成第一临时密钥对。

可选的，S102可以在S101之前执行。

S103：第二方的第二协议层生成第二临时密钥对，第二临时密钥对包括第二临时公钥以及第二临时私钥。

其中，第二临时密钥对是随机生成的。

第二协议层生成第二临时密钥对的方式可参照第一方的第一协议层生成第一临时密钥对的方式。可选的，第二协议层可以根据第二方的 MAC 地址使用椭圆曲线 X25519 生成第二临时密钥对。

可选的，第二协议层可以是第二方的传输层协议，也可以是其他的协议层。

S103 也可以在 S101 或 S102 之前执行，本申请不具体限定。

S104：第一协议层根据第一临时公钥获取第二方的第二临时公钥。

相应的，第二协议层获取来自于第一协议层的第一临时公钥。比如，第二协议层在获取来自于第一方的第一临时公钥后，生成并通过第二方的物理层发送第二临时公钥。此外，第二协议层也可以在获取第一临时公钥之前生成第二临时公钥。

可选的，第一协议层根据第一临时公钥获取第二方的第二临时公钥的方式可以是第一协议层向第二协议层发送密钥协商请求报文，并接收携带第二临时公钥的密钥协商请求报文的响应报文，以获得第二临时公钥，该密钥协商请求报文和该响应报文可以是 NLPKey 请求报文。其中，密钥协商请求报文中可携带第一临时公钥，第二协议层可获得第一临时公钥。

具体的，第一协议层可构造并通过第一方的物理层发送 NLPKey 请求报文，NLPKey 请求报文的格式按照图 6 所示密钥协商报文格式封装，该 NLPKey 请求报文可携带第二方的 NLP 地址、第二方的 MAC 地址、第一方的 NLP 地址、第一方的 MAC 地址、第一临时公钥、第三签名和时间戳。第二协议层可通过第二方的物理层接收 NLPKey 请求报文，并发送 NLPKey 响应报文，NLPKey 响应报文格式可按照图 6 所示密钥协商报文格式封装，该 NLPKey 响应报文可携带第一方的 NLP 地址、第一方的 MAC 地址、第二方的 NLP 地址、第二方的 MAC 地址、第二临时公钥、第四签名和时间戳。第一协议层接收 NLPKey 响应报文，获得第二临时公钥。通过上述步骤，可以使第一方与第二方实现第一临时公钥和第二临时公钥的交换。

S105：第二协议层根据第一临时公钥以及第二临时私钥生成共享密钥。

具体的，第二协议层在收到 S104 中的 NLPKey 请求报文后，可以用该报文中第一方的 NLP 地址作为公钥验证签名。若验证成功，则第二协议层根据第二临时私钥和第一临时公钥确定共享密钥。

可选的，基于 S104 和 S105，包含 NLPKey 扩展头部的报文在共享密钥的生成过程中至少会被使用两次，以进一步提高安全性。

可选的，可以设定超时失效机制，强制更新密钥，以避免临时密钥对和共享密钥与对端绑定带来的信息滞后。例如，在共享密钥生成达到一定时长后，可认为共享密钥失效，此后第一方和第二方在进行加密传输的过程中可按照上述流程重新生成共享密钥。

可选的，第二协议层可以根据椭圆曲线迪菲-赫尔曼密钥交换（Elliptic Curve Diffie–Hellman key Exchange，ECDH）原理确定共享密钥。

S106：第一协议层根据第二临时公钥和第一临时私钥生成共享密钥。

具体的，第一协议层在收到 S104 中的 NLPKey 响应报文后，可以用该报文中的第二方的 NLP 地址作为公钥验证签名。若验证成功，则第一协议层根据第一临时私钥和第二临

时公钥确定共享密钥。

可选的，第一协议层可以根据 ECDH 原理确定共享密钥。

因此，第一协议层和第二协议层均可根据 ECDH 原理生成共享密钥，也就是说，第一协议层生成的共享密钥和第二协议层生成的共享密钥是相等的。

可选的，本申请不具体限定 S105 和 S106 之间的执行顺序。

S107: 第一协议层确定数据报文，数据报文中携带通过共享密钥加密获得的加密数据，数据报文的接收方为第二方。

可选的，加密数据可以是三层以上的数据，例如，传输层头也被封装在加密数据中。具体的，第一协议层用共享密钥加密待传输数据，并封装为第一 NLPSec 报文。格式按照 NLPSec 包封装，所述 NLP 数据包包含以太头、NLP 基本头部、NLPSec 扩展头、加密数据。

应理解，在第一协议层和第二协议层分别获得共享密钥后，第一方与第二方之间的数据交互过程可由第一协议层和第二协议层分别根据共享密钥进行数据的加密/解密。

可选的，加密数据可以通过 chacha20-poly1305 算法获得，该算法是关联数据的认证加密（Authenticated Encryption with Associated Data，AEAD）算法，具备保密性和完整性的加密形式。

S108: 第一协议层发送该数据报文，数据报文的接收方为第二方。

具体的，第一协议层发送所构造的 NLPSec 报文给第二方。

S109: 第二协议层根据共享密钥解密数据报文中携带的加密数据。

具体的，第二协议层收到 NLPSec 报文，使用共享密钥解密数据和完整性校验，若完整性校验成功，解密后数据交于上层传输层协议处理。

在互联网中，网络传输层协议通常使用的是传输控制协议（Transmission Control Protocol/Internet Protocol，TCP/IP），所有传输层如 TCP、用户数据报协议（User Datagram Protocol，UDP）及其它传输层协议等的数据，都被直接封装为 IP 数据包进行传输。在使用 TCP/IP 协议的链路层中传输数据时，需要使用地址解析协议（Address Resolution Protocol，ARP）进行地址解析。然而，攻击者可以向某一主机发送伪 ARP 应答报文，使其发送的信息无法到达预期的主机或到达错误的主机，这就构成了一个 ARP 欺骗（ARP spoofing）。因此，本发明实施例还提供另一种通信方法，用以防止 ARP 欺骗，提高网络通信的安全性。

图 8B 为本发明实施例提供的另一种通信方法的过程示意图，该过程可由图 8B 所示的第一方和由第二方执行。所述由图 8B 所示的第一方和第二方使用的是新链网协议（检测新链网）（new link protocol，NLP）协议栈。其中，第一方可以是加密数据的发送方，第二方可以是加密数据的接收方。例如，第一方在发送加密数据之前，可根据该通信方法获取第二方的 MAC 地址，用于根据第二方的 MAC 地址发送加密数据。

可选的，所述由图 8B 所示的第一方和第二方采用 NLP 协议栈进行通信，该过程包括以下步骤:

S201: 第一方发送地址解析请求报文，该地址解析请求报文的接收方为第二方。其中，地址解析请求报文的源地址为第一方的 NLP 地址，地址解析请求报文的目的地址为第二方的 NLP 地址，地址解析请求报文包括第一方的 MAC 地址和第一签名，第一签名是根据第一方的第一私钥生成的，第一方的 NLP 地址为第一私钥对应的公钥。

在一种可能的实现方式中，地址解析请求报文使用公钥地址解析协议（VNET Address Resolution Protocol，VARP）封装，也就是说地址解析请求报文可以是 VARP 报文。第一方可以根据第一私钥对地址解析请求报文中的待签名内容进行加密，获得第一签名。其中，VARP 是对地址解析协议（Address Resolution Protocol，ARP）协议的扩展，用于解析 NLP 地址和 MAC 地址的映射关系，VARP 头部之后增加签名，用于身份认证。

图 5 所示为本发明实施例提供的一种 VARP 报文的结构示意图。

示例性的，结合图 5，第一签名可根据第一方的第一私钥和待签名内容生成，第一签名占用 64 字节。例如，待签名内容可以是包括图 5 所示的硬件类型、协议、硬件地址大小、地址大小、请求类型、源 MAC 地址、NLP 源地址、目的 MAC 地址、NLP 目的地址以及时间戳在内的 88 个字节。

可选的，由图 8B 所示的第一方可以对完整的 VARP 报文头进行签名，还可以对报文中的任意字段组合进行签名。

在一种可能的实现方式中，待签名内容包括时间戳，时间戳用于验证地址解析请求报文的时效性。

具体的，由图 8B 所示的第一方可以为地址解析请求报文设置的时间戳，也就是说可以为该通信设置失效机制，例如，当到达时间戳对应的失效时间时，强制第一方重新构建地址解析请求报文。例如，时间戳设置为 30 分钟，则地址解析请求报文的有效时间为 30 分钟。另外，根据不同地址解析请求报文中的时间戳也可以识别用于承载最新的数据信息的地址解析请求报文。

可选的，VARP 报文中的时间戳可以替换成单调递增的任意形式和不同字节数的序列号，用以杜绝重放攻击。

可选的，由图 8B 所示的第一方向第二方发送地址解析请求报文之前，第一方可以根据第二方的 NLP 地址以及第一对应关系，确定第一对应关系中不包括第二方的 MAC 地址。第一对应关系包括多个设备的 NLP 地址与 MAC 地址之间的对应关系，多个设备包括但不限于第一方和/或第二方。其中，第一对应关系可以由第一方根据历史通信记录获得，比如，第一方每与一个设备进行通信，则记录对方设备的 NLP 地址与 MAC 地址的对应关系，存储至第一对应关系中，则在下一次进行通信时，第一方可从第一对应关系中查询对方设备。

本申请中第一对应关系可以通过邻居列表的形式存储。如果第一方查询邻居列表能够确定第二方的 MAC 地址，则不需要再执行 S201。

相应地，第二方接收来自第一方的地址解析请求报文。

其中，地址解析请求报文的源地址为第一方的 NLP 地址，地址解析请求报文的目的地址为第二方的 NLP 地址，地址解析请求报文包括第一方的 MAC 地址和第一签名，第一签名是根据第一方的第一私钥生成的，第一方的 NLP 地址为第一私钥对应的公钥。

S202：第二方根据第一方的 NLP 地址验证地址解析请求中的第一签名。

S202 中，若第二方对于第一签名的验证成功，则执行图 8B 所示的 S204，若验证失败，则丢弃该报文，结束本流程。

可选的，若第一签名验证成功，第二方可以存储第二对应关系之后再执行 S204。其中，第二对应关系可以包括第一方的 NLP 地址与第一方的 MAC 地址之间的对应关系。

S203：第二方发送第一响应报文，该第一响应报文的接收方为第一方。其中，第一响应报文为上述地址解析请求报文的响应报文，第一响应报文的源地址为第二方的 NLP 地址，

第一响应报文的目的地址为第一方的NLP地址，第一响应报文包括第二方的MAC地址和第二签名，第二签名是根据第二方的第二私钥生成的，第二方的NLP地址为第二私钥对应的公钥。

示例性的，本申请中的第一响应报文可以使用如图5所示的VARP结构。其中，第一响应报文的源地址为第二方的NLP地址，第一响应报文的目的地址为第一方的NLP地址。

在一种可能的实现方式中，第二私钥的长度为32字节，第二方可以随机生成第二私钥。该第二私钥对应的公钥的长度为占用32字节，该公钥可以根据第二私钥和椭圆曲线算法ED25519确定。第二方可以将第二私钥对应的公钥作为第二方的NLP地址。

在一种可能的实现方式中，地址解析请求报文使用VARP地址解析协议报文，第二方可以根据第二私钥对第一响应报文中的待签名内容进行加密，获得第二签名。

示例性的，结合图5，第二签名根据第二方的第二私钥和待签名内容生成，第二签名占用64字节。例如，待签名内容可以是包括图5所示的硬件类型、协议、硬件地址大小、地址大小、请求类型、源MAC地址、NLP源地址、目的MAC地址、NLP目的地址以及时间戳在内的88个字节。

可选的，第二方可以对完整的VARP报文头进行签名，还可以对报文中的任意字段组合进行签名。

在一种可能的实现方式中，待签名内容包括时间戳，时间戳用于验证地址解析请求报文的时效性。

具体的，第二方可以为第一响应报文设置的时间戳，也就是说可以为该通信设置失效机制，例如，当到达时间戳对应的失效时间时，强制第二方重新构建第一响应报文。例如，时间戳设置为30分钟，则第一响应报文的有效时间为30分钟。另外，根据不同第一响应报文中的时间戳也可以识别用于承载最新的数据信息的第一响应报文。

可选的，VARP报文中的时间戳可以替换成单调递增的任意形式和不同字节数的序列号，用以杜绝重放攻击。

相应地，第一方接收来自第二方的第一响应报文。其中，第一响应报文为地址解析请求报文的响应报文，第一响应报文的源地址为第二方的NLP地址，第一响应报文的目的地址为第一方的NLP地址，第一响应报文包括第二方的MAC地址和第二签名，第二签名是根据第二方的第二私钥生成的，第二方的NLP地址为第二私钥对应的公钥。

S204：第一方根据第二方的NLP地址验证第二签名，若验证成功，则存储第二方的NLP地址和第二方的MAC地址之间的对应关系。

此外，若第二签名的验证失败，则第一方丢弃该报文，结束本流程。其中，第二方的NLP地址和第二方的MAC地址之间的对应关系可以存储至第一对应关系中。

基于以上方法，第一方在获取第二方的MAC地址的过程中，需要第一方和第二方分别验证对方的签名，能够防止ARP欺骗等攻击，以提高通信安全。

可选的，以上S201至S204中第一方的动作可由第一方的第一协议层实现，和/或，以上S201至S204中第二方的动作可由第二方的第二协议层实现。第一协议层实现可以是第一方的网络层，也可以是其他的协议层。第二协议层实现可以是第二方的网络层，也可以是其他的协议层。网络层在NLP协议栈中遵循NLP协议。

结合表1所示，NLP协议栈相当于将传统IP协议栈中的网络层使用的IP协议改为NLP协议。在NLP协议栈通信双方使用的网络地址为NLP地址，该NLP地址为本地生成的32

字节的公钥。

可选的，以上 S201 的具体实施中，第一协议层可生成地址解析请求报文，地址解析请求报文的源地址为第一方的 NLP 地址，地址解析请求报文的目的地址为第二方的 NLP 地址，地址解析请求报文包括第一方的 MAC 地址和第一签名，第一签名是根据第一方的第一私钥生成的，第一方的 NLP 地址为第一私钥对应的公钥。在 S203 中，第一协议层可获取来自于第二方的第一响应报文，第一响应报文为地址解析请求报文的响应报文，第一响应报文的源地址为第二方的 NLP 地址，第一响应报文的目的地址为第一方的 NLP 地址，第一响应报文包括第二方的 MAC 地址和第二签名，第二签名是根据第二方的第二私钥生成的，第二方的 NLP 地址为第二私钥对应的公钥。第一协议层在根据第二方的 NLP 地址确定第二签名通过验证后，获得第二方的 MAC 地址。

具体的，地址解析请求报文可以是 VARP 报文，第一响应报文可以是 VARP 响应报文。此时第一方的第一协议层可构造 VARP 请求报文，并将该报文发送给第二方，报文格式按照上述 VARP 包结构。其中，VARP 请求报文包含第一方的 NLP 地址、第二方的 NLP 地址、第一方的 MAC 地址（作为源地址）、广播 MAC 地址（作为目的地址）、序列号和第一签名。第二协议层收到 VARP 请求报文，用第一方的 NLP 地址作为公钥验证第一签名，若验证成功，则保存第一方的第一对应关系，即保存第一方的 NLP 地址与第一方的 MAC 地址之间的对应关系。若验证失败，则丢弃该报文，结束本流程。第二协议层构造并发送 VARP 响应报文，报文格式按照上述 VARP 包结构。其中，VARP 响应报文包含第二方的 NLP 地址、第一方的 NLP 地址、第二方的 MAC 地址（作为源地址）、第一方的 MAC 地址（作为目的地址）、序列号和第二签名。第一协议层收到 VARP 响应报文，用第二方的 NLP 地址作为公钥验证第二签名。若验证成功，保存第二方的第一对应关系，即保存第二方的 NLP 地址与 MAC 地址之间的对应关系。若验证失败，则丢弃该报文，结束本流程。至此，地址解析完成。

在使用 TCP/IP 协议的网络中传输数据时，攻击者可以通过 IP 地址欺骗目标主机，以便对目标主机进行拒绝服务攻击、伪造 TCP 连接、会话劫持、隐藏攻击主机地址等。对于只需接收方接收数据或信息（单边通信）的应用场景，当攻击者通过 IP 欺骗伪装为发送方向接收方发送攻击数据包时，由于接收方无法验证接收到的数据包的来源身份，使得接收方易被攻击。因此，本申请还提供一种源地址认证的方法，用以提高网络通信的安全性。

示例性的，本申请提供的一种源地址认证的方法、装置，其中，本申请中的通信双方（发送方、接收方）都使用了发明人设计的新链网（New Link Protocol，NLP）协议栈，使通信双方可以使用公钥作为 NLP 地址进行网络通信。

如图 8C 所示，本发明实施例提供一种源地址认证的方法，应用于发送方，发送方使用的是 NLP 协议栈，该方法的处理过程如下：

S301：根据数据传输请求，将发送方签名、NLP 源地址、待发送数据、防重放攻击的序列号以及 NLP 目的地址封装为一个 NLP 数据包；其中，发送方签名是通过发送方的发送方私钥生成的，NLP 目的地址为接收方的接收方公钥，NLP 源地址为发送方的发送方公钥，接收方使用的也是 NLP 协议栈；

S302：将 NLP 数据包发送给接收方，使接收方用 NLP 源地址验证发送方签名，并在验证成功后记录序列号，以及获取待发送数据。

在 S301 中，数据传输请求可以使基于发送方中的上层应用生成的，在数据传输请求中可以包括待发送数据、接收方的 NLP 地址。

NLP 数据包中的 NLP 扩展头部使用的是 NLPSig 扩展头，NLP 数据包按图 1 的 NLP 数据包的封装结构进行封装的。

S301 中，将发送方签名、NLP 源地址、待发送数据、防重放攻击的序列号以及 NLP 目的地址封装为一个NLP数据包之前，若发送方已生成NLP源地址，则可以直接执行S301。

若发送方并未生成 NLP 源地址，则还需要先生成 NLP 源地址，具体通过下列方式实现:

随机生成发送方私钥；基于非对称加密算法和发送方私钥生成发送方公钥。

非对称加密算法，例如可以是椭圆曲线算法 ED25519。

例如，发送方为一台服务器，在此服务器中使用的是 NLP 协议栈，当前服务器中的一个应用需要向接收方（假设为一台电脑）发送某个电影的视频流时，会将此电影分成多个待发送数据依次发送给接收方，服务器在发送其中任一个待发送数据时，会生成对应的数据传输请求，在该数据传输请求中包括待发送数据和接收方的 NLP 目的地址。

但由于此服务器为新接入的服务器，其还没有设置 NLP 地址，因此需要先随机生成 32 字节的发送方私钥，再用非对称加密算法（如椭圆曲线算法 ED25519）和发送方私钥，生成发送方公钥，并将发送方公钥作为服务器的 NLP 地址。之后，服务器便可将发送方签名、NLP 源地址、待发送数据、防重放攻击的序列号以及 NLP 目的地址封装为一个 NLP 数据包，并发送给电脑。

一种可能的实施方式，将发送方签名、NLP 源地址、待发送数据、防重放攻击的序列号以及 NLP 目的地址封装为一个 NLP 数据包，可以通过下列方式实现:

从数据传输请求中获取 NLP 目的地址和待发送数据；对 NLP 目的地址进行解析，获得接收方的接收方物理地址；用发送方私钥对 NLP 数据包中至少包含序列号及随机数的部分头部信息进行加密，获得发送方签名；将发送方签名、NLP 源地址、发送方的发送方物理地址、NLP 目的地址、接收方物理地址以及待发送数据封装为数据包。

例如，老师通过设备 A（即发送方）进行在线视频教学，观看教学视频的学生通过设备 B（及接收方）接收视频内容，设备 A 从数据传输请求中获取设备 B 的 NLP 目的地址及待发送数据，然后对 NLP 目的地址进行解析，得到对于的接收方物理地址，同时还用设备 A 的发送方私钥对 NLP 数据包中至少包含序列号及随机数的部分头部进行加密，得到此 NLP 数据包对应的发送方签名，将其作为 NLP 扩展头部中的数字签名。最后，将发送方签名、NLP 源地址、发送方的发送方物理地址、NLP 目的地址、接收方物理地址以及待发送数据封装为 NLP 数据包，并发送给设备 B，使设备 B 可以用 NLP 源地址验证发送方签名，进而验证发送方的身份，在验证成功后记录当前接收到的 NLP 数据包的序列号，以便验证下一个 NLP 数据包是否是重复的，并获取待发送数据。

需要理解的是，在依次生成上述教学视频的多个待发送数据后，相应的会为每个待发送数据分配对应的序列号，多个待发送数据对应的多个序列号的值是按时间顺序递增的，如最先生成的第一个待发送数据对应的序列号为 1，第二待发送数据的序列号为 2，...，第 n 个待发送数据的序列号为 n。

一种可能的实施方式，发送方连续发送给接收方的多个数据包中的多个序列号是按升序设置的。

一种可能的实施方式，序列号包括时间戳。及可以将时间戳作为序列号。

例如，上述教学视频的多个待发送数据中第一个待发送数据的生成时间（即时间戳）为 8:31，则对应的序列号可以设置为 831，第二待发送数据的生成时间为 8:32，则对应的序列号可以设置为 832，其他可依次类推，不再一一赘述。

在介绍完源地址认证的方法中发送方所在侧的实施例后，下面将从接收方所在侧进行介绍。

请参见图 8D，本发明一实施例中提供一种源地址认证的方法，应用于接收方，接收方使用的是新链网 NLP 协议栈，该方法包括:

S401：接收发送方发送的 NLP 数据包；其中，NLP 数据包是由发送方签名、NLP 源地址、待发送数据、防重放攻击的序列号以及 NLP 目的地址封装成的，发送方签名是通过发送方的发送方私钥生成的，NLP 目的地址为接收方的接收方公钥，NLP 源地址为发送方的发送方公钥，发送方使用的也是 NLP 协议栈;

S402：从 NLP 数据包中获取 NLP 源地址、发送方签名及序列号;

S403：通过 NLP 源地址、发送方签名及序列号验证 NLP 数据包来源的真实性和非重复性，若都验证通过则存储序列号并获取待发送数据，否则丢弃 NLP 数据包。

通过 NLP 源地址、发送方签名及序列号验证 NLP 数据包来源的真实性和非重复性，可以通过下列方式实现:

用 NLP 源地址验证发送方签名，若验证成功则确定 NLP 数据包的来源为发送方；判断序列号是否大于从发送方接收到的上一个 NLP 数据包中的序列号，若为是，则确定 NLP 数据包是非重复的。

例如，接收方本地存储了发送方发送的上一个 NLP 数据包的序列号为 n，当前接收方接收到 NLP 数据包 1 和 NLP 数据包 2，从 NLP 数据包 1 获取其中携带的 NLP 源地址 1 和发送方签名 1，并用发送 NLP 地址 1 验证发送方签名 1，验证结果是失败，接收方确定 NLP 数据包 1 的来源存疑，验证不通过，将 NLP 数据包 1 丢弃。

接收方从 NLP 数据包 2 获取其中携带的 NLP 源地址 2 和发送方签名 2，并用发送 NLP 地址 2 验证发送方签名 2，验证结果是通过，确定 NLP 数据包 2 的来源正常，然后进一步判断 NLP 数据包 2 中携带的序列号 2 是否大于 n（上一个 NLP 数据包的序列号），若为是确定 NLP 数据包 2 是非重复的，之后可以从 NLP 数据包 2 中获取待发送数据，并传输给上层协议处理，以便传输给上层应用。若序列号 2 小于等于 n，则确定 NLP 数据包 2 无效，丢弃 NLP 数据包 2。

为了是本领域的技术人员能充分理解上述技术方案，下面提供一个详细的例子进行说明:

请参见图 8E 为本发明实施例提供的源地址认证方法的流程图。

假设发送方为网络电视提供端，接收方为客户端，网络电视提供端将电视节目分为多个待发送数据发送给客户端，网络电视提供端针对每个待发送数据生成对应的数据传输请求，在该数据传输请求中包含客户端的 NLP 目的地址和待发送数据。

S501：网络电视提供端根据数据传输请求，生成对应的 NLP 数据包。

具体生成 NLP 数据包的方法可以参见发送方中实施例部分的描述，在此不再赘述。

S502：网络电视提供端发送 NLP 数据包给客户端。

S503: 客户端根据 NLP 数据包中携带的 NLP 源地址和发送方签名，验证发送方身份，

若发送方的身份验证成功则进一步验证NLP数据包是否是非重复的，若为是则记录此NLP数据包中的序列号并获取其中的待发送数据，若不成功则丢弃NLP数据包。

在本发明提供的实施例中，通过在发送方NLP数据包中携带能够验证其身份的NLP源地址和发送方签名、以及防重放攻击的序列号，使接收方能直接根据接收到的NLP数据包对其NLP源地址进行身份验证，这种源地址认证的方式具备去中心化自证与它证、发送方不可抵赖、杜绝DDOS攻击等特点；并验证其是否为重放攻击的数据包，在任一个验证不通过时，丢弃NLP数据包，从而能够在防止IP地址欺骗的同时有效地抵御直接复制报文的重放攻击，提高接收方的安全性，当应用在对时效性要求较高的单边通信中时，能够同时让接收高具有高时效性和高网络安全性。

在使用TCP/IP协议的网络中传输数据时，对于通信双方需要进行交互的场景而言，任一方被攻击都会造成双方不能进行正常通信。因此，本申请还提供一种通信方法，用以提高网络通信的安全性。

示例性的，如图8F所示，本申请实施例提供一种通信方法，应用于第一方，第一方使用的是NLP协议栈，该通信方法的处理过程如下：

S601：根据数据传输请求，生成包含第一签名、第一NLP地址、及第一临时公钥的密钥协商报文；其中，密钥协商报文用于第一方与第二方进行身份认证和密钥交换，第一签名是通过第一方的第一私钥生成的，第一NLP地址为第一方的第一公钥。

在S601中，数据传输请求可以使基于第一方中的上层应用生成的，在数据传输请求中可以包括待发送数据、第一方的第一NLP地址。

在本发明提供的实施例中，第一方可以是主动发起连接的一方，也可以是被动连接的一方；当主动发起连接的一方向被动连接的一方发送数据时，主动发起连接的一方为第一方，被动连接的一方为第二方；当被动连接的一方向主动发起连接的一方返回数据时，被动连接的一方为第一方，主动发起连接的一方为第二方。

若第一方还已经生成第一临时公钥，则可以直接使用；若第一方还没有生成第一临时公钥，则在生成包含第一签名、第一NLP地址以及第一临时公钥的密钥协商报文之前，还需要先生成第一临时公钥，具体可以通过下列方式实现：

根据椭圆曲线迪菲-赫尔曼秘钥交换（Elliptic Curve Diffie–Hellman key Exchange，ECDH）生成第一临时密钥对；将第一临时密钥对中的公钥作为第一临时公钥；将第一临时密钥对中的私钥作为第一临时私钥。

在本申请提供的实施例中，通过根据ECDH生成第一临时密钥对，可以使第一方、第二方基于对方的临时公钥和己方的临时私钥生成相同的共享密钥，以确保通信双方使用相同的共享密钥基于对称加密算法对待传输数据进行加密传输，使通信双方能利用共享密钥解密接收到的加密数据（及加密后的待传输数据）。

在本申请提供的实施例中，密钥协商报文采用的是密钥协商数据包的结构进行封装的。

若第一方已经生成第一NLP地址，则可以直接执行在本步骤；若第一方没有生成第一NLP地址，则在生成包含第一签名、第一NLP地址以及第一临时公钥的密钥协商报文之前，还需要先生成第一NLP地址，具体采用下列方式实现：

随机生成第一私钥；采用非对称加密算法和第一私钥生成第一公钥。

一种可能的实施方式，生成包含第一签名、第一NLP地址以及第一临时公钥的密钥协

商报文，包括：

从数据传输请求中获取第二 NLP 地址；对第二 NLP 地址进行解析，获得第二方的第二物理地址；用第一私钥对密钥协商报文中至少包含第一临时公钥和时间戳的部分头部信息进行加密，获得第一签名；其中，时间戳用于验证密钥协商报文的时效性；将第一签名、第一 NLP 地址、第一方的第一物理地址、第二 NLP 地址、第二物理地址以及第一临时公钥封装为密钥协商报文。

其中，部分头部信息包括密钥协商报文的 NLP 基本头部和 NLP 扩展头部；或，NLP 基本头部中的部分头部和 NLP 扩展头部。NLP 扩展头部为 NLPKey 扩展头部。

例如，第一方在获得第二 NLP 地址和第二物理地址后，时间戳设置为 30 分钟，部分头部信息为 NLPKey 扩展头部和部分 NLP 基本头部，用第一私钥对部分头部信息进行计算，得到第一签名；之后，按密钥协商数据包的结构对第一签名、第一 NLP 地址、第一方的第一物理地址、第二 NLP 地址、第二物理地址以及第一临时公钥进行封装，得到密钥协商报文，通过该密钥协商报文生成的共享密钥的有效时间为 30 分钟。

在本发明提供的实施例中，利用密钥协商报文协商通信双方在通信的过程中使用的共享密钥，使得通过在密钥协商报文中设置通信双方生成的共享密钥的有效时间，可以防止共享密钥被非法盗用，提高通信双方的通信安全。第一方和第二方可以通过将各自生成的临时密钥对和共享秘钥绑定，结合设置的时间戳，为共享秘钥设置失效机制，当到达时间戳对应的失效时间时，强制双方重新协商生成新的共享秘钥进行数据传输。

在第一方生成密钥协商报文后，便可执行 S602。

S602：将密钥协商报文发送给第二方，使第二方用第一签名和第一 NLP 地址验证第一方的身份，并在验证成功后存储第一临时公钥，及生成包含第二签名、第二 NLP 地址及第二临时公钥的响应报文；其中，第二签名是通过第二方的第二私钥生成的，第二 NLP 地址为第二方的第二公钥，第二方使用的也是 NLP 协议栈。

第二方接收到密钥协商报文后，用第一 NLP 地址验证第一签名，以验证源地址（即第一 NLP 地址）的身份，在验证失败后，确定接收到的密钥协商报文是非法的，直接丢弃；若用第一 NLP 地址验证第一签名成功，则从密钥协商报文中获取并存储第一临时公钥，并根据 ECDH 对第一临时公钥和第二方生成的第二临时私钥进行计算，获得并存储共享密钥，以待后续进行数据传输时使用。

同时，还会将第二方的第二临时公钥发送给第一方，以完成密钥协商（即生成相同的共享密钥），具体采用的方式为：

将第二签名、第二 NLP 地址及第二临时公钥，按密钥协商数据包进行封装，生成密钥协商报文的响应报文，发送给第一方。

需要说明的是，第二方生成第二临时密钥对（包含第二临时公钥、第二临时私钥）的方式与第一方生成第一临时密钥对的方式相同，故不再赘述。

在第二方发送响应报文给第一方后，便可执行步骤 603。

S603：接收响应报文，并用第二签名和第二 NLP 地址验证第二方的身份，在验证成功后，根据椭圆曲线迪菲-赫尔曼秘钥交换 ECDH，对与第一临时公钥对应的第一临时私钥及第二临时公钥进行计算，得到共享密钥；在与第二方进行数据交互时，用共享密钥进行数据的加密传输。

第二方接收到响应报文后，需要用响应报文中携带的第二 NLP 地址验证第二签名，以

验证第二方的身份，具体通过下列方式实现：

用第二 NLP 地址验证第二签名；若验证成功，则确定第二方的身份验证成功；若用第二 NLP 地址验证第二签名失败，则确定第二方的身份验证失败，并丢弃响应报文。

在第二 NLP 地址验证第二签名成功后，从响应报文中获取第二临时公钥，完成第一方与第二方的密钥交换；同时，根据 ECDH 对第一临时私钥及第二临时公钥进行计算，得到并存储共享密钥，完成第一方与第二方的密钥协商，之后，第一方和第二方便可利用双方协商好的共享密钥进行数据的加密传输。

需要理解的是，由于第一方和第二方生成的共享密钥相同，因此在本发明提供的实施例中，并没有严格区分第一方生成的共享密钥和第二方生成的共享密钥。

在本发明提供的实施例中，第一方与第二方完成密钥协商后，便可用协商得到的共享密钥进行数据交互，具体通过下列方式实现：

当向第二方发送待传输数据时，从数据传输请求中获取待传输数据；并用具有关联数据的认证加密 AEAD 性质的对称加密算法及共享密钥加密待传输数据，获得加密后的待传输数据；其中，待传输数据为得到第一方的 NLP 协议栈中网络层之上的多层数据；

将加密后的待传输数据封装在第一 NLPSec 报文中，并发送给第二方；

当接收到第二方发送的第二 NLPSec 报文后，用对称加密算法和共享密钥，对第二 NLPSec 报文中的加密数据进行解密及完整性校验，在校验成功后将解密后的数据传输给第一方的 NLP 协议栈中的传输层进行处理。

例如，继续以第一方为用户 1 使用的电脑 1，向第二方（用户 2 使用的电脑 2）发送邮件为例，在电脑 1（第一方）通秘钥协商报文与电脑 2（第二方）完成秘钥交换，并各自生成相同的共享秘钥后，电脑 1 便可利用生成的共享秘钥向电脑 2 发送邮件内容。

电脑 1 从数据传输请求中获取邮件内容，并用具有 AEAD 性质的对称加密算法（如 chacha20-poly1305 算法）及共享秘钥加密本地 NLP 协议栈中网络层之上的多层数据（邮件内容包含在其中），获得加密后的待传输数据，并按照 NLPSec 数据包进行封装，生成第一 NLPSec 报文，将第一 NLPSec 报文发送给电脑 2。

电脑 2 接收到第一 NLPSec 报文后，在通过第一 NLP 地址验证其中携带的数字签名，并验证成功后，从第一 NLPSec 报文中获取加密后的待传输数据，用本地的共享秘钥解密加密后的待传输数据，得到待传输数据，从待传输数据中得到邮件内容。并且，电脑 2 向电脑 1 发送成功接收邮件内容的响应报文(即第二 NLPSec 报文)，该响应报文是按 NLPSec 数据包封装的。

电脑 1 接收到第二 NLPSec 报文（邮件内容的响应报文）后，用其中携带的第二 NLP 地址验证第二 NLPSec 报文中携带的数字签名成功后，获取其中携带的确认电脑 2 成功接收到邮件内容的确认信息，至此完成电脑 1 与电脑 2 的双边交互过程。

在本发明提供的实施例中，在进行数据传输时，通过使用具有 AEAD 性质的对称加密算法和双方协商出的共享秘钥对待传输数据进行加密，可以同时保障待传输数据的机密性和 NLPSec 数据包的完整性，同时实现了安全认证从上层应用中解耦。

请参见图 8G 为本发明实施例提供的第一方与第二方交互的流程图。

S701：第一方生成携带第一临时公钥的秘钥协商报文。

第一方需要远程登录第二方的数据库，于是第二方的上层应用生成了包含数据传输请求登录数据库所需的用户名和密码以及第二方的第二 NLP 地址。并生成包含第一签名、第

一 NLP 地址、及第一临时公钥的密钥协商报文。

S702: 第一方发送秘钥协商报文给第二方。

S703: 第二方在成功验证秘钥协商报文的来源后，生成包含第二临时公钥的响应报文，以及基于第一临时公钥和第二临时私钥生成并存储共享秘钥。

第二方验证秘钥协商报文的来源，即用秘钥协商报文中携带的第一 NLP 地址验证第一签名。

S704: 第二方将响应报文发送给第一方。

S705: 第一方在成功验证响应报文的来源后，基于第一临时私钥和第二临时公钥生成共享秘钥。

至此，第一方和第二方均获得了对方的临时公钥，完成秘钥交换，生成相同的共享秘钥。

S705: 第一方用共享秘钥加密待传输数据，并封装我第一 NLPSec 报文。

待传输数据中包含登录数据库所需的用户名和密码，第一方用具有 AEAD 性质的对称加密算法和共享秘钥加密待传输数据。

S706: 第一方将第一 NLPSec 报文发送给第二方。

S707: 第二方在成功验证第一 NLPSec 报文的来源后，从第一 NLPSec 报文中获取用户名和密码，在确定用户名和密码正确后生成授权访问数据库的信息，并封装在第二 NLPSec 报文中。

S709: 第二方将第二 NLPSec 报文发送给第一方。

S710: 第一方在成功验证第二 NLPSec 报文的来源后，获取授权访问数据库的信息，以访问第二方的数据库。

图 9A 所示为本申请实施例提供的一种通信装置（或设备）的模块化结构示意图。其中，处理模块 901 可用于执行处理动作，收发模块 902 可用于实现通信动作。例如，在通过该结构实现以上方法实施例介绍的第一 VPN 设备时，处理模块 901 可用于执行 S101、S102、S106 和/或 S107，收发模块 902 可用于执行 S104 和/或 S108。在通过该结构实现以上方法实施例介绍的第二 VPN 设备时，收发模块 902 可用于 S104，并由处理模块 901 执行 S103、S105 和/或 S109。具体执行的动作和功能这里不再具体展开，可参照前述方法实施例部分的说明。

示例性的，在通过图 9A 所示结构实现图 8A 所示的第一方时，处理模块 901 可用于实现由第一方的第一协议层实现的处理动作。例如，处理模块 901 可用于获取第二方的 MAC 地址，并生成第一临时密钥对。收发模块 902 可用于实现由第一方实现的通信动作。例如，收发模块 902 可用于第一方向第二方进行发送，或用于接收来自于第二方的信息、数据或信号等，如用于发送前述第一临时密钥对中的第一临时公钥。

示例性的，处理模块 901 具体可包括 MAC 地址获取模块、密钥生成模块和确定模块。在实现第一方的第一协议层实现的处理动作时，MAC 地址获取模块可用于第一方的第一协议层根据来自于应用层的数据传输请求获取第二方的 MAC 地址。密钥生成模块可用于根据所述第一临时公钥获取所述第二方的第二临时公钥，并根据所述第二临时公钥和所述第一临时私钥生成共享密钥。确定模块可用于确定数据报文，数据报文中携带所述第二方的 MAC 地址和通过所述共享密钥加密获得的加密数据。

处理模块 901 具体还可用于生成共享密钥。

处理模块 901 还可根据待发送数据和前述共享密钥确定数据报文。

同理，在通过图 9A 所示结构实现图 8A 所示的第二方时，处理模块 901 可用于实现由第二方的第二协议层实现的处理动作。例如，处理模块 901 可用于生成第二临时密钥对。收发模块 902 可用于实现由第二方实现的通信动作。例如，收发模块 902 可用于第二方向第一方进行发送，或用于接收来自于第一方的信息、数据或信号等，如用于发送用于承载第二临时公钥的报文。

示例性的，处理模块 901 具体可包括获取模块、密钥生成模块、报文生成模块和解密模块。在实现第二方的第二协议层实现的处理动作时，获取模块可用于获取第一方的第一临时公钥。密钥生成模块可用于生成第二临时密钥对，并根据第一临时公钥以及第二临时私钥生成共享密钥。报文生成模块可用于生成携带第二临时公钥的报文。解密模块可用于根据共享密钥解密数据报文中携带的加密数据。

处理模块 901 具体还可用于生成共享密钥。

处理模块 901 还可获取来自第一方的数据报文。该数据报文可由收发模块 902 接收。

以上装置实施例部分设计的概念和定义可以参见方法实施例部分的说明。

示例性的，在通过图 9A 所示结构实现图 8B 所示的第一方时，处理模块 901 可用于执行处理动作，收发模块 902 可用于实现通信动作。例如，在通过该结构实现以上方法实施例介绍的第一方时，收发模块 902 可用于执行 S201 向第二方发送地址解析请求报文的动作和/或执行 S203 中接收来自第二方的第一响应报文的动作，处理模块 901 可用于执行 S204。示例性的，此时收发模块 902 可包括报文发送模块和报文接收模块，报文发送模块可用于发送地址解析请求报文，报文接收模块可用于接收来自于所述第二方的第一响应报文。处理模块 901 可包括存储模块，用于在根据所述第二方的 NLP 地址确定所述第二签名通过验证后，存储所述第二方的 NLP 地址与所述第二方的 MAC 地址之间的对应关系。

示例性的，在通过该结构实现以上方法实施例介绍的图 8B 所示的第二方时，收发模块 902 可用于 S201 接收来自第一方的地址解析请求报文的动作，并由处理模块 901 执行 S203 验证第一签名的动作，收发模块 902 还可用于执行 S203 向第一方发送第一响应报文的动作。具体执行的动作和功能这里不再具体展开，可参照前述方法实施例部分的说明。示例性的，此时收发模块 902 可包括报文发送模块和报文接收模块，报文接收模块可用于接收来自于第一方的地址解析请求报文，报文发送模块可用于根据第一方的 NLP 地址确定第一签名通过验证后，向第一方发送第一响应报文。

示例性的，如图 9B 所示，基于同一发明构思，本发明一实施例中提供一种源地址认证的装置，应用于图 8E 中的发送方，该装置的源地址认证方法的具体实施方式可参见发送方侧方法实施例部分的描述，重复之处不再赘述，该装置包括：

封装单元 1001，用于根据数据传输请求，将发送方签名、NLP 源地址、待发送数据、防重放攻击的序列号以及 NLP 目的地址封装为一个 NLP 数据包；其中，所述发送方签名是通过所述发送方的发送方私钥生成的，所述 NLP 目的地址为所述接收方的接收方公钥，所述 NLP 源地址为所述发送方的发送方公钥，所述接收方使用的也是新链网 NLP 协议栈；

发送单元 1002，用于将所述 NLP 数据包发送给所述接收方，使所述接收方用所述 NLP 源地址验证所述发送方签名，并在验证成功后记录所述序列号，以及获取所述待发送数据。

一种可能的实施方式，所述装置还包括生成单元 1003，所述生成单元 1003 用于：随

机生成所述发送方私钥；基于非对称加密算法和所述发送方私钥，生成所述发送方公钥。

一种可能的实施方式，所述封装单元 1001 还用于：从所述数据传输请求中获取所述 NLP 目的地址和所述待发送数据；对所述 NLP 目的地址进行解析，获得所述接收方的接收方物理地址；用所述发送方私钥对所述 NLP 数据包中至少包含所述序列号及随机数的部分头部信息进行加密，获得所述发送方签名；将所述发送方签名、所述 NLP 源地址、所述发送方的发送方物理地址、所述 NLP 目的地址、所述接收方物理地址以及所述待发送数据封装为所述 NLP 数据包。

一种可能的实施方式，所述发送方连续发送给所述接收方的多个数据包中的多个序列号是按升序设置的。

一种可能的实施方式，所述序列号包括时间戳。

基于同一发明构思，本发明一实施例中提供一种源地址认证的装置，应用于接收方，该装置的源地址认证方法的具体实施方式可参见接收方侧方法实施例部分的描述，重复之处不再赘述，请参见图 9C，该装置包括：

接收单元 1101，用于接收发送方发送的 NLP 数据包；其中，所述 NLP 数据包是由发送方签名、NLP 源地址、待发送数据、防重放攻击的序列号以及 NLP 目的地址封装成的，所述发送方签名是通过所述发送方的发送方私钥生成的，所述 NLP 目的地址为所述接收方的接收方公钥，所述 NLP 源地址为所述发送方的发送方公钥，所述发送方使用的也是新链网 NLP 协议栈；

获取单元 1102，用于从所述 NLP 数据包中获取所述 NLP 源地址、所述发送方签名及所述序列号；

验证单元 1103，用于通过所述 NLP 源地址、所述发送方签名及所述序列号验证所述 NLP 数据包来源的真实性和非重复性，若都验证通过则存储所述序列号并获取所述待发送数据，否则丢弃所述 NLP 数据包。

一种可能的实施方式，所述验证单元 803 还用于：用所述 NLP 源地址验证所述发送方签名，若验证成功则确定所述 NLP 数据包的来源为所述发送方；判断所述序列号是否大于从所述发送方接收到的上一个 NLP 数据包中的序列号，若为是，则确定所述 NLP 数据包是非重复的。

图 10 示出了本申请实施例提供的一种通信方法的通信装置（或设备）结构示意图。

本申请实施例中的电子设备可包括处理器 1201。处理器 1201 是该装置的控制中心，可以利用各种接口和线路连接该装置的各个部分，通过运行或执行存储在存储器 1202 内的指令以及调用存储在存储器 1202 内的数据。可选的，处理器 1201 可包括一个或多个处理单元，处理器 1201 可集成应用处理器和调制解调处理器，其中，应用处理器主要处理操作系统和应用程序等，调制解调处理器主要处理无线通信。可以理解的是，上述调制解调处理器也可以不集成到处理器 1201 中。在一些实施例中，处理器 1201 和存储器 1202 可以在同一芯片上实现，在一些实施例中，它们也可以在独立的芯片上分别实现。

处理器 1201 可以是通用处理器，例如中央处理器（CPU）、数字信号处理器、专用集成电路、现场可编程门阵列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，可以实现或者执行本申请实施例中公开的各方法、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风险评估系统台所执行的步骤可以直接由硬件处理器执行完成，或者用处理器中的硬件及软件模块组合执

行完成。

在本申请实施例中，存储器 1202 存储有可被至少一个处理器 1201 执行的指令，至少一个处理器 1201 通过执行存储器 1202 存储的指令，可以用于执行前述由第一方（或第一协议层）和/或第二方（或第二协议层）执行的通信过程。

存储器 1202 作为一种非易失性计算机可读存储介质，可用于存储非易失性软件程序、非易失性计算机可执行程序以及模块。存储器 1202 可以包括至少一种类型的存储介质，例如可以包括闪存、硬盘、多媒体卡、卡型存储器、随机访问存储器（Random Access Memory，RAM）、静态随机访问存储器（Static Random Access Memory，SRAM）、可编程只读存储器（Programmable Read Only Memory，PROM）、只读存储器（Read Only Memory，ROM）、带电可擦除可编程只读存储器（Electrically Erasable Programmable Read-Only Memory，EEPROM）、磁性存储器、磁盘、光盘等等。存储器 1202 是能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质，但不限于此。本申请实施例中的存储器 1202 还可以是电路或者其它任意能够实现存储功能的装置，用于存储程序指令和/或数据。

本申请实施例中，该装置还可以包括通信接口 1203，电子设备可以通过该通信接口 1203 传输数据。例如电子设备为第一方，通信接口 1203 可用于向第二方发放报文。

可选的，可由图 10 所示处理器 1201（或处理器 1201 和存储器 1202）实现图 9A 所示的处理模块 901，和/或，由通信接口 1203 实现图 9A 所示的收发模块 902。

基于同一发明构思，本申请实施例还提供一种通信装置，该通信装置的通信方法的具体实施方式可参见方法实施例部分的描述，重复之处不再赘述，请参见图 11，该通信装置包括：生成单元 1301，用于根据数据传输请求，生成包含第一签名、第一 NLP 地址、及第一临时公钥的密钥协商报文；其中，所述密钥协商报文用于所述第一方与所述第二方进行身份认证和密钥交换，所述第一签名是通过所述第一方的第一私钥生成的，所述第一 NLP 地址为所述第一方的第一公钥；验证单元 1302，用于将所述密钥协商报文发送给所述第二方，使所述第二方用所述第一签名和所述第一 NLP 地址验证所述第一方的身份，并在验证成功后存储所述第一临时公钥，及生成包含第二签名、第二 NLP 地址及第二临时公钥的响应报文；其中，所述第二签名是通过所述第二方的第二私钥生成的，所述第二 NLP 地址为所述第二方的第二公钥，所述第二方使用的也是所述 NLP 协议栈；传输单元 1303，用于接收所述响应报文，并用所述第二签名和所述第二 NLP 地址验证所述第二方的身份，在验证成功后，根据椭圆曲线迪菲-赫尔曼秘钥交换 ECDH，对与所述第一临时公钥对应的第一临时私钥及所述第二临时公钥进行计算，得到共享密钥；在与所述第二方进行数据交互时，用所述共享密钥进行数据的加密传输。

一种可能的实施方式，所述生成单元 1301 还用于：根据所述 ECDH 生成第一临时密钥对；将所述第一临时密钥对中的公钥作为所述第一临时公钥；将所述第一临时密钥对中的私钥作为所述第一临时私钥。

一种可能的实施方式，所述生成单元 1301 还用于：随机生成所述第一私钥；采用非对称加密算法和所述第一私钥生成所述第一公钥。

一种可能的实施方式，所述生成单元 1301 还用于：从所述数据传输请求中获取所述第二 NLP 地址；对所述第二 NLP 地址进行解析，获得所述第二方的第二物理地址；用所述第一私钥对所述密钥协商报文中至少包含所述第一临时公钥和时间戳的部分头部信息

进行加密，获得所述第一签名；其中，所述时间戳用于验证所述密钥协商报文的时效性；将所述第一签名、所述第一 NLP 地址、所述第一方的第一物理地址、所述第二 NLP 地址、所述第二物理地址以及所述第一临时公钥封装为所述密钥协商报文。

一种可能的实施方式，所述部分头部信息，包括：所述密钥协商报文的 NLP 基本头部和 NLP 扩展头部；或，所述 NLP 基本头部中的部分头部和所述 NLP 扩展头部。

一种可能的实施方式，所述验证单元 1302 还用于：用所述第二 NLP 地址验证所述第二签名；若验证成功，则确定所述第二方的身份验证成功；若用所述第二 NLP 地址验证所述第二签名失败，则确定所述第二方的身份验证失败，并丢弃所述响应报文。

一种可能的实施方式，所述传输单元 1303 具体用于：当向所述第二方发送待传输数据时，从所述数据传输请求中获取所述待传输数据；并用具有关联数据的认证加密 AEAD 性质的对称加密算法及所述共享密钥加密所述待传输数据，获得加密后的待传输数据；其中，所述待传输数据为得到所述第一方的 NLP 协议栈中网络层之上的多层数据；将所述加密后的待传输数据封装在第一 NLPSec 报文中，并发送给所述第二方；当接收到所述第二方发送的第二 NLPSec 报文后，用所述对称加密算法和所述共享密钥，对所述第二 NLPSec 报文中的加密数据进行解密及完整性校验，在校验成功后将解密后的数据传输给所述第一方的 NLP 协议栈中的传输层进行处理。

基于相同的发明构思，本申请实施例还提供一种计算机可读存储介质，其中可存储有指令，当该指令在计算机上运行时，使得计算机执行上述方法实施例中图 9A 所述提供的操作步骤。该计算机可读存储介质可以是图 10 所示的存储器 1202。

基于同一发明构思，本发明实施例中提供了一种源地址认证的电子设备，当该电子设备在运行时，能够执行上述方法实施例中图 9B 和图 9C 所述提供的操作步骤。包括：至少一个处理器，以及与所述至少一个处理器连接的存储器；

其中，所述存储器存储有可被所述至少一个处理器执行的指令，所述至少一个处理器通过执行所述存储器存储的指令，执行如上所述的发送方侧或接收方策的源地址认证方法。

基于同一发明构思，本发明实施例还提一种可读存储介质，包括：

存储器，所述存储器用于存储指令，当所述指令被处理器执行时，使得包括所述可读存储介质的装置完成如上所述的发送方侧或接收方策的源地址认证方法。

本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

本申请是参照根据本申请的方法、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。

显然，本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的精神和范围。这样，倘若本申请的这些修改和变型属于本申请权利要求及其等同技术的范围之内，则本申请也意图包含这些改动和变型在内。

权 利 要 求

1、一种加密通信方法，应用于第一方，所述第一方使用的是新链网 NLP 协议栈，其特征在于，所述方法包括:

所述第一方的第一协议层根据来自于应用层的数据传输请求获取第二方的 MAC 地址，所述数据传输请求中包括所述第二方的 NLP 地址;

所述第一协议层生成第一临时密钥对，所述第一临时密钥对包括第一临时公钥以及第一临时私钥;

所述第一协议层根据所述第一临时公钥获取所述第二方的第二临时公钥;

所述第一协议层根据所述第二临时公钥和所述第一临时私钥生成共享密钥;

所述第一协议层确定数据报文，所述数据报文中携带所述第二方的 MAC 地址和通过所述共享密钥加密获得的加密数据，所述数据报文的接收方为所述第二方。

2、如权利要求 1 所述的方法，其特征在于，所述第一方的第一协议层根据来自于应用层的数据传输请求获取第二方的 MAC 地址，所述数据传输请求中包括所述第二方的 NLP 地址，包括:

所述第一协议层根据所述第二方的 NLP 地址以及第一对应关系，确定所述第二方的 MAC 地址，所述第一对应关系包括所述第二方的 NLP 地址与所述第二方的 MAC 地址之间的对应关系。

3、如权利要求 1 所述的方法，其特征在于，所述第一方的第一协议层根据来自于应用层的数据传输请求获取第二方的 MAC 地址，包括:

所述第一协议层生成地址解析请求报文，所述地址解析请求报文的源地址为所述第一方的 NLP 地址，所述地址解析请求报文的目的地址为所述第二方的 NLP 地址，所述地址解析请求报文包括所述第一方的 MAC 地址和第一签名，所述第一签名是根据所述第一方的第一私钥生成的，所述第一方的 NLP 地址为所述第一私钥对应的公钥;

所述第一协议层获取来自于所述第二方的第一响应报文，所述第一响应报文为所述地址解析请求报文的响应报文，所述第一响应报文的源地址为所述第二方的 NLP 地址，所述响应报文的目的地址为所述第一方的 NLP 地址，所述响应报文包括所述第二方的 MAC 地址和第二签名，所述第二签名是根据所述第二方的第二私钥生成的，所述第二方的 NLP 地址为所述第二私钥对应的公钥;

所述第一协议层在根据所述第二方的 NLP 地址确定所述第二签名通过验证后，获得所述第二方的 MAC 地址。

4、如权利要求 1 中任一所述的方法，其特征在于，所述第一协议层根据所述第一临时公钥获取所述第二方的第二临时公钥，包括:

所述第一协议层生成密钥协商请求报文，所述密钥协商请求报文包括第三签名以及所述第一临时公钥，所述密钥协商请求报文的源地址为所述第一方的 NLP 地址，所述密钥协商请求报文的目的地址为所述第二方的 NLP 地址，所述第三签名是根据所述第一方的第一私钥生成的，所述第一方的 NLP 地址为所述第一私钥对应的公钥;

所述第一协议层获取第二响应报文，所述第二响应报文为所述密钥协商请求报文对应的响应报文，所述第二响应报文包括第四签名以及所述第二临时公钥，所述第二响应报文的源地址为所述第二方的 NLP 地址，所述第二响应报文的目的地址为所述第一方的 NLP 地址，所述第四签名是根据所述第二方的第二私钥生成的，所述第二方的 NLP 地址为所述第二私钥对应的公钥；

所述第一协议层在根据所述第二方的 NLP 地址确定所述第四签名通过验证后，根据所述第一临时私钥和所述第二临时公钥确定所述共享密钥。

5、如权利要求 4 中任一所述的方法，其特征在于，所述方法还包括：

所述第一方随机生成所述第一私钥；

所述第一方根据所述第一私钥通过椭圆曲线算法生成所述第一私钥对应的公钥；

所述第一方将所述第一私钥对应的公钥作为所述第一方的 NLP 地址。

6、如权利要求 4 所述的方法，其特征在于，所述地址解析请求报文为 VARP 报文，还包括：

所述第一方根据所述第一私钥对所述地址解析请求报文中的待签名内容进行加密，获得所述第一签名。

7、如权利要求 4 所述的方法，其特征在于，所述待签名内容包括时间戳，所述时间戳用于验证所述地址解析请求报文的时效性。

8、如权利要求 4-7 中任一所述的方法，其特征在于，所述第一方向第二方发送地址解析请求报文之前，还包括：

所述第一方确定邻居列表中未存储所述第二方的 MAC 地址，所述邻居列表用于存储与所述第一方进行通信的通信设备的 NLP 地址与 MAC 地址之间的对应关系。

9、一种加密通信方法，应用于第二方，所述第二方使用的是新链网 NLP 协议栈，其特征在于，所述方法包括：

所述第二方的所述第二协议层获取第一方的第一临时公钥；

所述第二协议层生成第二临时密钥对，所述第二临时密钥对包括第二临时公钥以及第二临时私钥；

所述第二协议层根据所述第一临时公钥以及所述第二临时私钥生成共享密钥；

所述第二协议层生成携带所述第二临时公钥的报文，所述报文的接收方为所述第一方，所述第二临时公钥用于所述第一方生成所述共享密钥；

所述第一协议层根据共享密钥解密数据报文中携带的加密数据，所述数据报文的发送方为所述第一方，所述数据报文还携带所述第二方的 MAC 地址。

10、如权利要求 9 所述的方法，其特征在于，所述第二方的所述第二协议层获取第一方的第一临时公钥，包括：

所述第二方的第二协议层获取来自于第一方的密钥协商请求报文，所述密钥协商请求

报文包括第三签名以及所述第一临时公钥，所述密钥协商请求报文的源地址为所述第一方的 NLP 地址，所述密钥协商请求报文的目的地址为所述第二方的 NLP 地址，所述第三签名是根据所述第一方的第一私钥生成的，所述第一方的 NLP 地址为所述第一私钥对应的公钥。

11、如权利要求 10 所述的方法，其特征在于，所述第二协议层生成第二临时密钥对，包括:

所述第二协议层在根据所述第一方的 NLP 地址确定所述第三签名通过验证后，生成所述第二临时密钥对。

12、如权利要求 11 所述的方法，其特征在于，所述第二协议层生成携带所述第二临时公钥的报文，包括:

所述第二协议层生成第二响应报文，所述第二响应报文为所述密钥协商请求报文的响应报文，所述第二响应报文包括第四签名以及所述第二临时公钥，所述第二响应报文的源地址为所述第二方的 NLP 地址，所述第二响应报文的目的地址为所述第一方的 NLP 地址，所述第四签名是根据所述第二方的第二私钥生成的，所述第二方的 NLP 地址为所述第二私钥对应的公钥。

13、如权利要求 9 所述的方法，其特征在于，还包括:

所述第二协议层接收来自于所述第一方的地址解析请求报文，所述地址解析请求报文的源地址为所述第一方的 NLP 地址，所述地址解析请求报文的目的地址为所述第二方的 NLP 地址，所述地址解析请求报文包括所述第一方的 MAC 地址和第一签名，所述第一签名是根据所述第一方的第一私钥生成的，所述第一方的 NLP 地址为所述第一私钥对应的公钥;

所述第二协议层生成第一响应报文，所述第一响应报文为所述地址解析请求报文的响应报文，所述第一响应报文的源地址为所述第二方的 NLP 地址，所述响应报文的目的地址为所述第一方的 NLP 地址，所述响应报文包括所述第二方的 MAC 地址和第二签名，所述第二签名是根据所述第二方的第二私钥生成的，所述第二方的 NLP 地址为所述第二私钥对应的公钥。

14、如权利要求 13 所述的方法，其特征在于，还包括:

所述第二方随机生成所述第二私钥;

所述第二方根据所述第二私钥通过椭圆曲线算法生成所述第二私钥对应的公钥;

所述第二方将所述第二私钥对应的公钥作为所述第二方的 NLP 地址。

15、如权利要求 13 所述的方法，其特征在于，所述第一响应报文为 VARP 报文，还包括:

所述第二方根据所述第二私钥对所述第一响应报文中的待签名内容进行加密，获得所述第一签名。

16、如权利要求 13 所述的方法，其特征在于，所述待签名内容包括时间戳，所述时间戳用于验证所述第一响应报文的时效性。

17、一种源地址认证的方法，应用于接收方，所述接收方使用的是新链网 NLP 协议栈，其特征在于，包括：

接收发送方发送的 NLP 数据包；其中，所述 NLP 数据包是由发送方签名、NLP 源地址、待发送数据、防重放攻击的序列号以及 NLP 目的地址封装成的，所述发送方签名是通过所述发送方的发送方私钥生成的，所述 NLP 目的地址为所述接收方的接收方公钥，所述 NLP 源地址为所述发送方的发送方公钥，所述发送方使用的也是所述 NLP 协议栈；

从所述 NLP 数据包中获取所述 NLP 源地址、所述发送方签名及所述序列号；

通过所述 NLP 源地址、所述发送方签名及所述序列号验证所述 NLP 数据包来源的真实性和非重复性，若都验证通过则存储所述序列号并获取所述待发送数据，否则丢弃所述 NLP 数据包。

18、如权利要求 17 所述的方法，其特征在于，通过所述 NLP 源地址、所述发送方签名及所述序列号验证所述 NLP 数据包来源的真实性和非重复性，包括：

用所述 NLP 源地址验证所述发送方签名，若验证成功则确定所述 NLP 数据包的来源为所述发送方；

判断所述序列号是否大于从所述发送方接收到的上一个 NLP 数据包中的序列号，若为是，则确定所述 NLP 数据包是非重复的。

19、一种加密通信装置，应用于第一方，所述第一方使用的是新链网 NLP 协议栈，其特征在于，所述装置包括：

MAC 地址获取模块，所述获取模块用于根据来自于应用层的数据传输请求获取第二方的 MAC 地址，所述数据传输请求中包括所述第二方的 NLP 地址；

密钥生成模块，所述密钥生成模块用于生成第一临时密钥对，所述第一临时密钥对包括第一临时公钥以及第一临时私钥；

所述密钥生成模块，还用于根据所述第一临时公钥获取所述第二方的第二临时公钥，并根据所述第二临时公钥和所述第一临时私钥生成共享密钥；

确定模块，所述确定模块用于确定数据报文，所述数据报文中携带所述第二方的 MAC 地址和通过所述共享密钥加密获得的加密数据，所述数据报文的接收方为所述第二方。

20、一种加密通信装置，应用于第二方，所述第二方使用的是新链网 NLP 协议栈，其特征在于，所述装置包括：

获取模块，所述获取模块用于获取第一方的第一临时公钥；

密钥生成模块，所述密钥生成模块用于生成第二临时密钥对，所述第二临时密钥对包括第二临时公钥以及第二临时私钥；

所述密钥生成模块还用于根据所述第一临时公钥以及所述第二临时私钥生成共享密钥；

报文生成模块，所述报文生成模块用于生成携带所述第二临时公钥的报文，所述报文

的接收方为所述第一方，所述第二临时公钥用于所述第一方生成所述共享密钥；

解密模块，所述解密模块用于根据共享密钥解密数据报文中携带的加密数据，所述数据报文的发送方为所述第一方，所述数据报文还携带所述第二方的 MAC 地址。

21、一种通信装置，应用于第一方，所述第一方使用的是新链网 NLP 协议栈，其特征在于，所述装置包括：

报文发送模块，用于发送地址解析请求报文，所述地址解析请求报文的源地址为所述第一方的 NLP 地址，所述地址解析请求报文的目的地址为所述第二方的 NLP 地址，所述地址解析请求报文包括所述第一方的 MAC 地址和第一签名，所述第一签名是根据所述第一方的第一私钥生成的，所述第一方的 NLP 地址为所述第一私钥对应的公钥；

报文接收模块，用于接收来自于所述第二方的第一响应报文，所述第一响应报文为所述地址解析请求报文的响应报文，所述第一响应报文的源地址为所述第二方的 NLP 地址，所述第一响应报文的目的地址为所述第一方的 NLP 地址，所述第一响应报文包括所述第二方的 MAC 地址和第二签名，所述第二签名是根据所述第二方的第二私钥生成的，所述第二方的 NLP 地址为所述第二私钥对应的公钥；

存储模块，用于在根据所述第二方的 NLP 地址确定所述第二签名通过验证后，存储所述第二方的 NLP 地址与所述第二方的 MAC 地址之间的对应关系。

22、一种通信装置，应用于第二方，所述第二方使用的是新链网 NLP 协议栈，其特征在于，所述装置包括：

报文接收模块，用于接收来自于第一方的地址解析请求报文，所述地址解析请求报文的源地址为所述第一方的 NLP 地址，所述地址解析请求报文的目的地址为所述第二方的 NLP 地址，所述地址解析请求报文包括所述第一方的 MAC 地址和第一签名，所述第一签名是根据所述第一方的第一私钥生成的，所述第一方的 NLP 地址为所述第一私钥对应的公钥；

报文发送模块，用于根据所述第一方的 NLP 地址确定所述第一签名通过验证后，向所述第一方发送第一响应报文，所述第一响应报文为所述地址解析请求报文的响应报文，所述第一响应报文的源地址为所述第二方的 NLP 地址，所述第一响应报文的目的地址为所述第一方的 NLP 地址，所述第一响应报文包括所述第二方的 MAC 地址和第二签名，所述第二签名是根据所述第二方的第二私钥生成的，所述第二方的 NLP 地址为所述第二私钥对应的公钥。

23、一种源地址认证的装置，应用于发送方，其特征在于，包括：

封装单元，用于根据数据传输请求，将发送方签名、NLP 源地址、待发送数据、防重放攻击的序列号以及 NLP 目的地址封装为一个 NLP 数据包；其中，所述发送方签名是通过所述发送方的发送方私钥生成的，所述 NLP 目的地址为所述接收方的接收方公钥，所述 NLP 源地址为所述发送方的发送方公钥，所述接收方使用的也是新链网 NLP 协议栈；

发送单元，用于将所述 NLP 数据包发送给所述接收方，使所述接收方用所述 NLP 源地址验证所述发送方签名，并在验证成功后记录所述序列号，以及获取所述待发送数据。

24、一种源地址认证的装置，应用于接收方，其特征在于，包括:

接收单元，用于接收发送方发送的 NLP 数据包；其中，所述 NLP 数据包是由发送方签名、NLP 源地址、待发送数据、防重放攻击的序列号以及 NLP 目的地址封装成的，所述发送方签名是通过所述发送方的发送方私钥生成的，所述 NLP 目的地址为所述接收方的接收方公钥，所述 NLP 源地址为所述发送方的发送方公钥，所述发送方使用的也是新链网 NLP 协议栈;

获取单元，用于从所述 NLP 数据包中获取所述 NLP 源地址、所述发送方签名及所述序列号;

验证单元，用于通过所述 NLP 源地址、所述发送方签名及所述序列号验证所述 NLP 数据包来源的真实性和非重复性，若都验证通过则存储所述序列号并获取所述待发送数据，否则丢弃所述 NLP 数据包。

25、一种电子设备，其特征在于，所述电子设备包括处理器，所述处理器用于执行存储器中存储的计算机程序时实现如权利要求 1 至 8、9 至 16、17 至 18 中任一所述方法的步骤。

26、一种计算机可读存储介质，其特征在于，其存储有计算机程序，所述计算机程序被处理器执行时实现如权利要求 1 至 8、9 至 16、17 至 18 中任一所述方法的步骤。

14字节	72字节	可选	不定长	不定长
以太头	NLP基本头部	NLP扩展头部	传输层头部	数据

图 1

2字节	2字节	2字节	2字节	1字节	1字节
版本	服务	流标签	包长度	下个头	跳数
NLP源地址（32字节）					
NLP目的地址（32字节）					

图 2

下个头（1字节）	类型（1字节）	保留（2字节）
时间戳（4字节）		
临时公钥（32字节）		
数字签名（64字节）		

图 3

下个头（1字节）	类型（1字节）	加密数据长度（2字节）
序列号（时间戳 4字节）		

图 4

硬件类型（2字节）	协议（2字节）	硬件地址大小（2字节）	地址大小（2字节）	请求类型（2字节）
源MAC地址（6字节）				
NLP源地址（32字节）				
目的MAC地址（6字节）				
NLP目的地址（32字节）				
时间戳+签名（4+64字节）				

图 5

14字节	72字节	104字节
以太头	NLP基本头部	NLPKey扩展头部

图 6

14字节	72字节	8字节	不定长
以太头	NLP基本头部	NLPSec扩展头部	加密数据

图 7

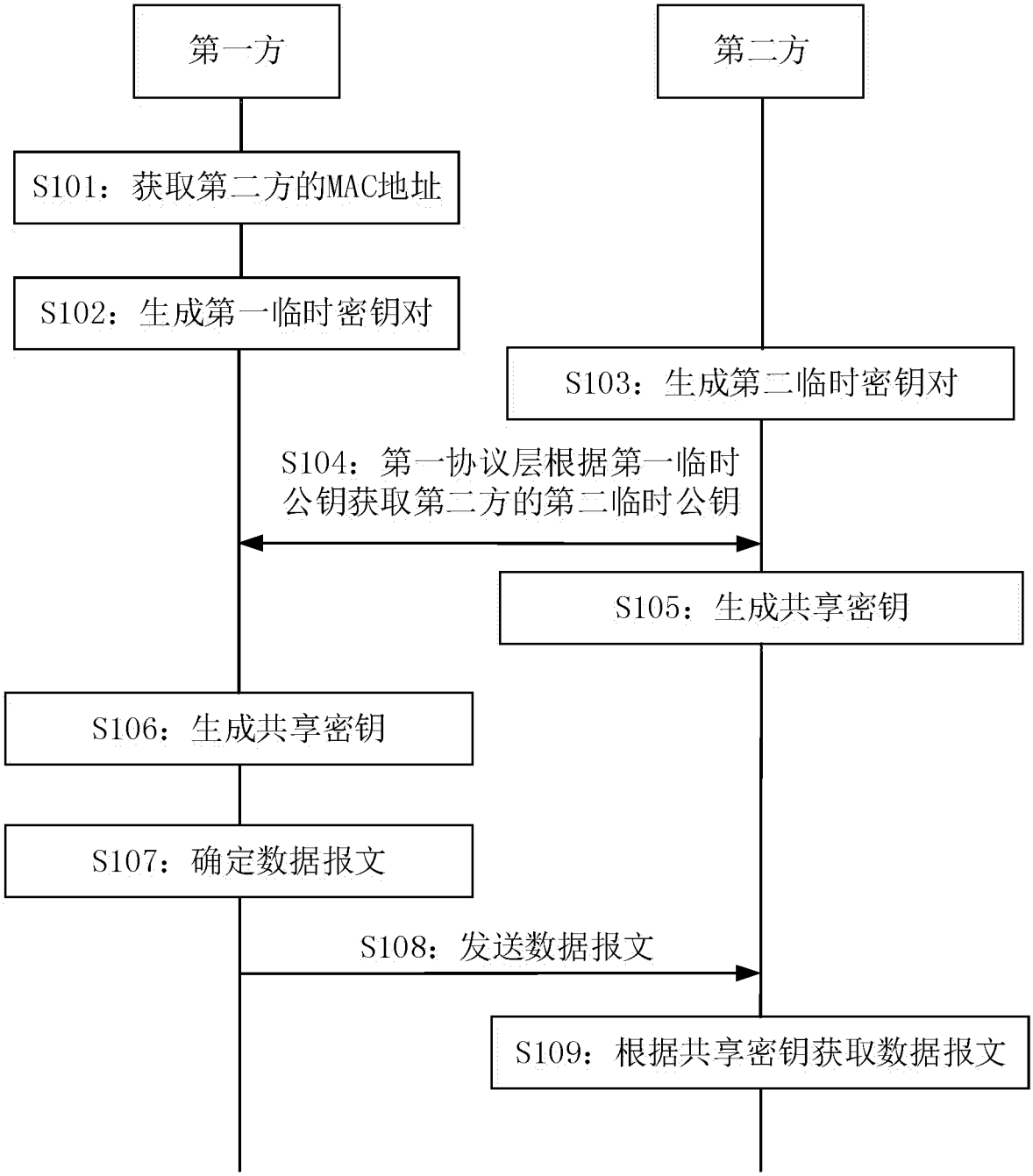
第一方
第二方
S101：获取第二方的MAC地址
S102：生成第一临时密钥对
S103：生成第二临时密钥对
S104：第一协议层根据第一临时公钥获取第二方的第二临时公钥
S105：生成共享密钥
S106：生成共享密钥
S107：确定数据报文
S108：发送数据报文
S109：根据共享密钥获取数据报文

图 8A

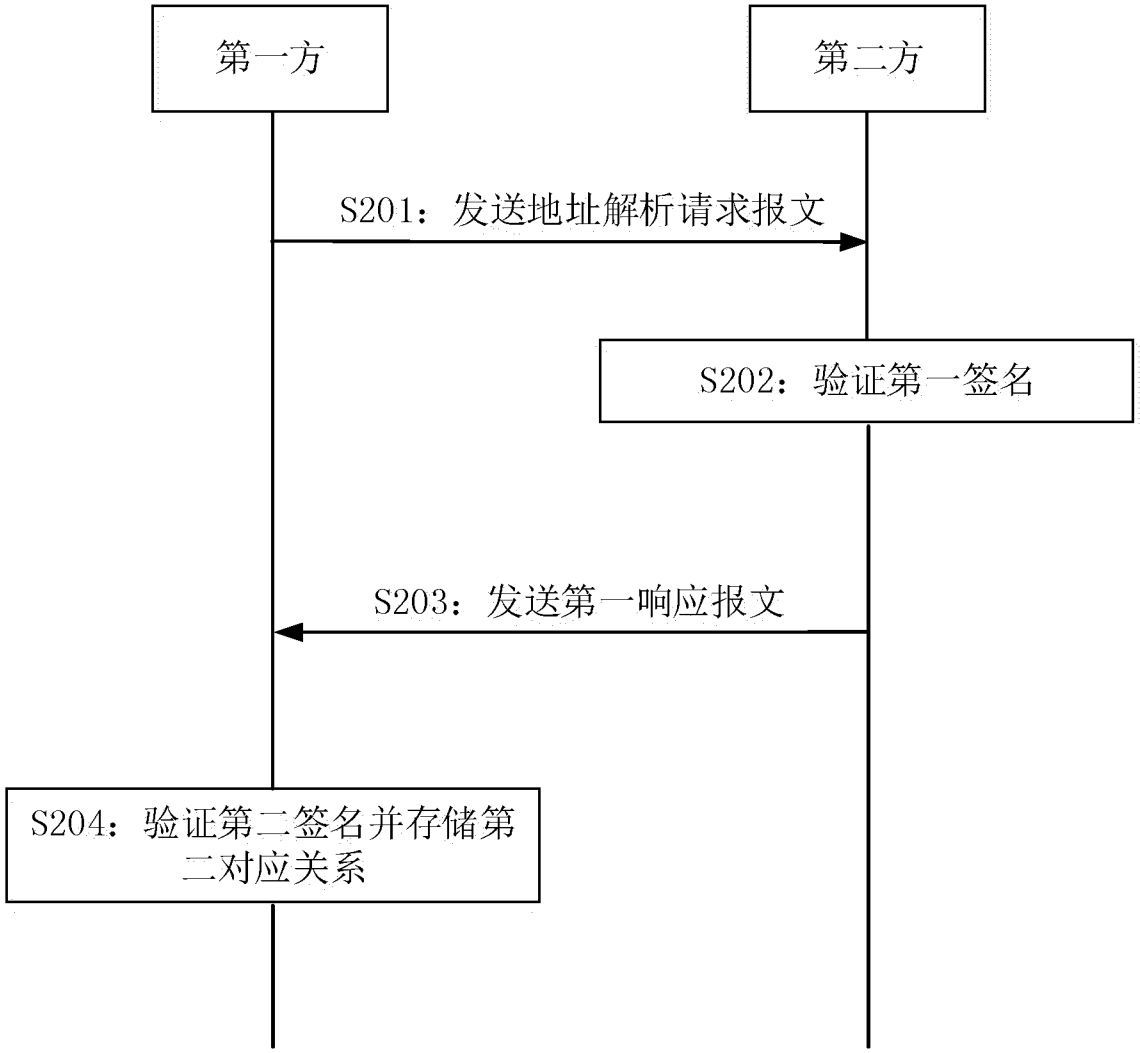
第一方
第二方
S201：发送地址解析请求报文
S202：验证第一签名
S203：发送第一响应报文
S204：验证第二签名并存储第二对应关系

图 8B

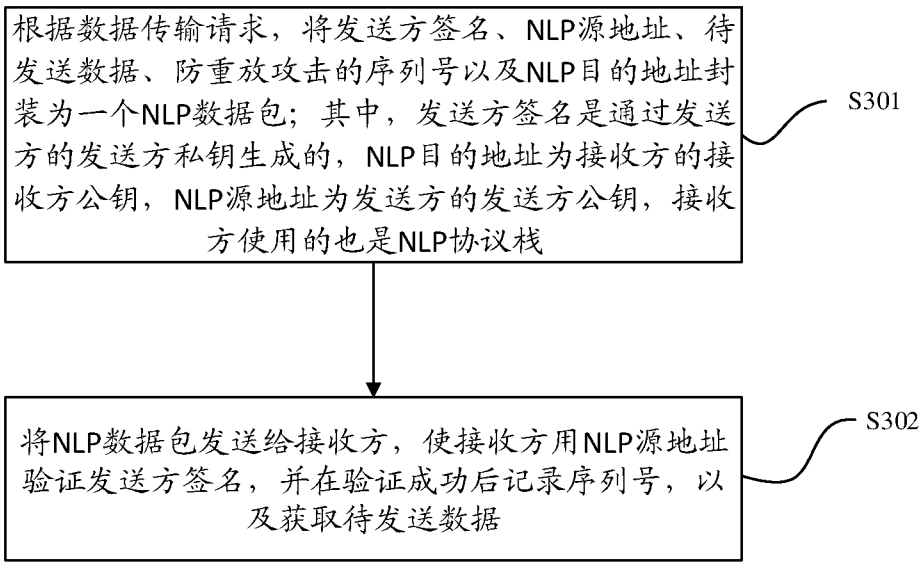
根据数据传输请求，将发送方签名、NLP源地址、待发送数据、防重放攻击的序列号以及NLP目的地址封装为一个NLP数据包；其中，发送方签名是通过发送方的发送方私钥生成的，NLP目的地址为接收方的接收方公钥，NLP源地址为发送方的发送方公钥，接收方使用的也是NLP协议栈
S301
将NLP数据包发送给接收方，使接收方用NLP源地址验证发送方签名，并在验证成功后记录序列号，以及获取待发送数据
S302

图 8C

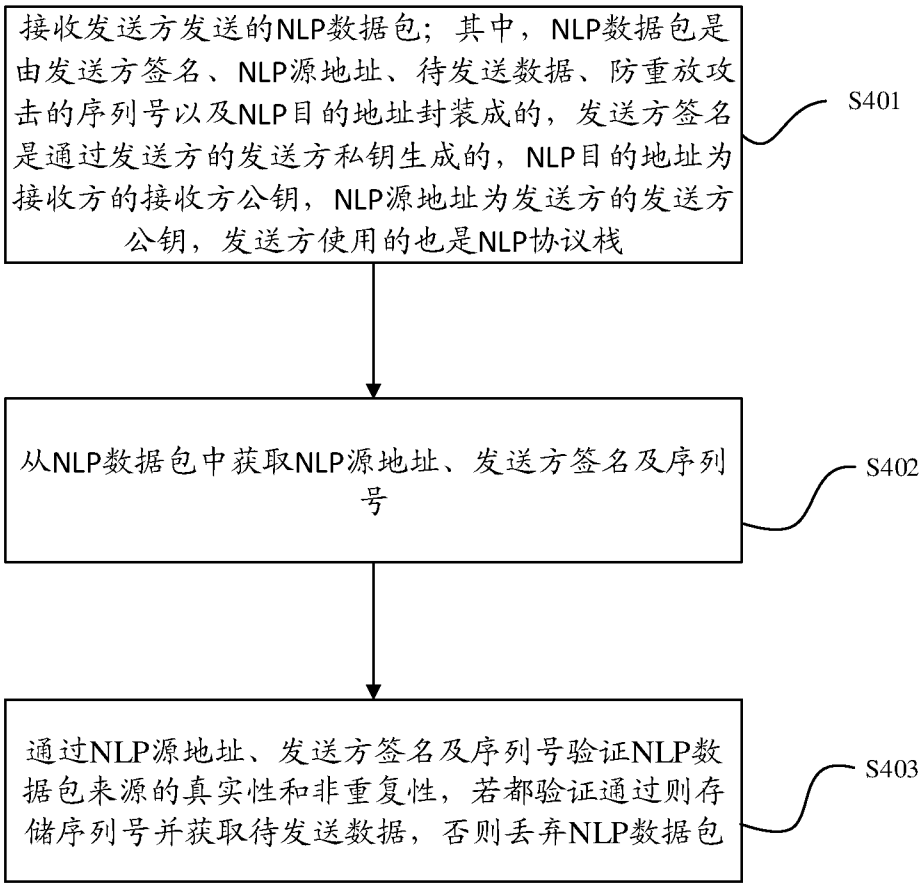
接收发送方发送的NLP数据包；其中，NLP数据包是由发送方签名、NLP源地址、待发送数据、防重放攻击的序列号以及NLP目的地址封装成的，发送方签名是通过发送方的发送方私钥生成的，NLP目的地址为接收方的接收方公钥，NLP源地址为发送方的发送方公钥，发送方使用的也是NLP协议栈
S401
从NLP数据包中获取NLP源地址、发送方签名及序列号
S402
通过NLP源地址、发送方签名及序列号验证NLP数据包来源的真实性和非重复性，若都验证通过则存储序列号并获取待发送数据，否则丢弃NLP数据包
S403

图 8D

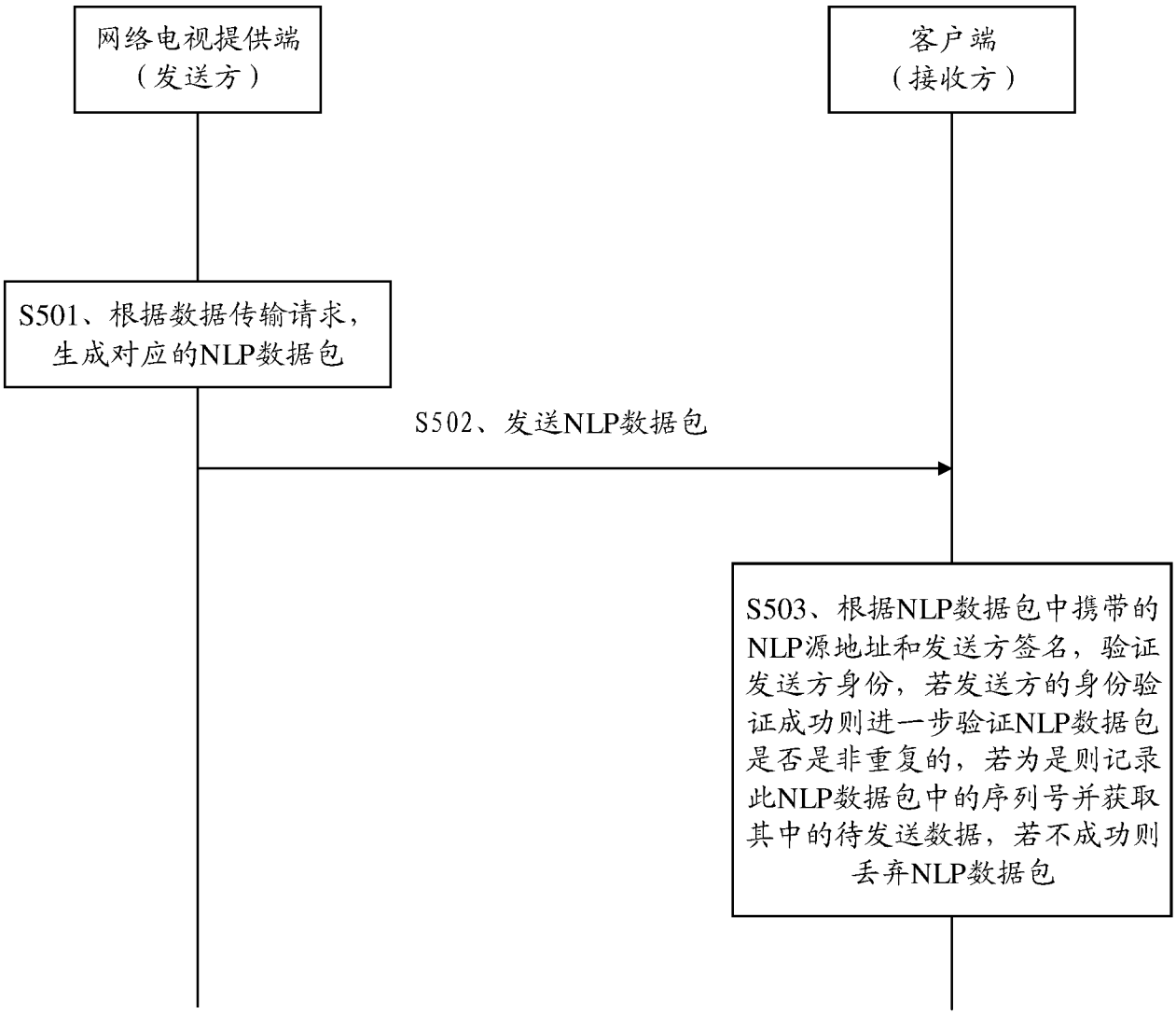
网络电视提供端
（发送方）
客户端
（接收方）
S501、根据数据传输请求，
生成对应的NLP数据包
S502、发送NLP数据包
S503、根据NLP数据包中携带的NLP源地址和发送方签名，验证发送方身份，若发送方的身份验证成功则进一步验证NLP数据包是否是非重复的，若为是则记录此NLP数据包中的序列号并获取其中的待发送数据，若不成功则丢弃NLP数据包

图 8E

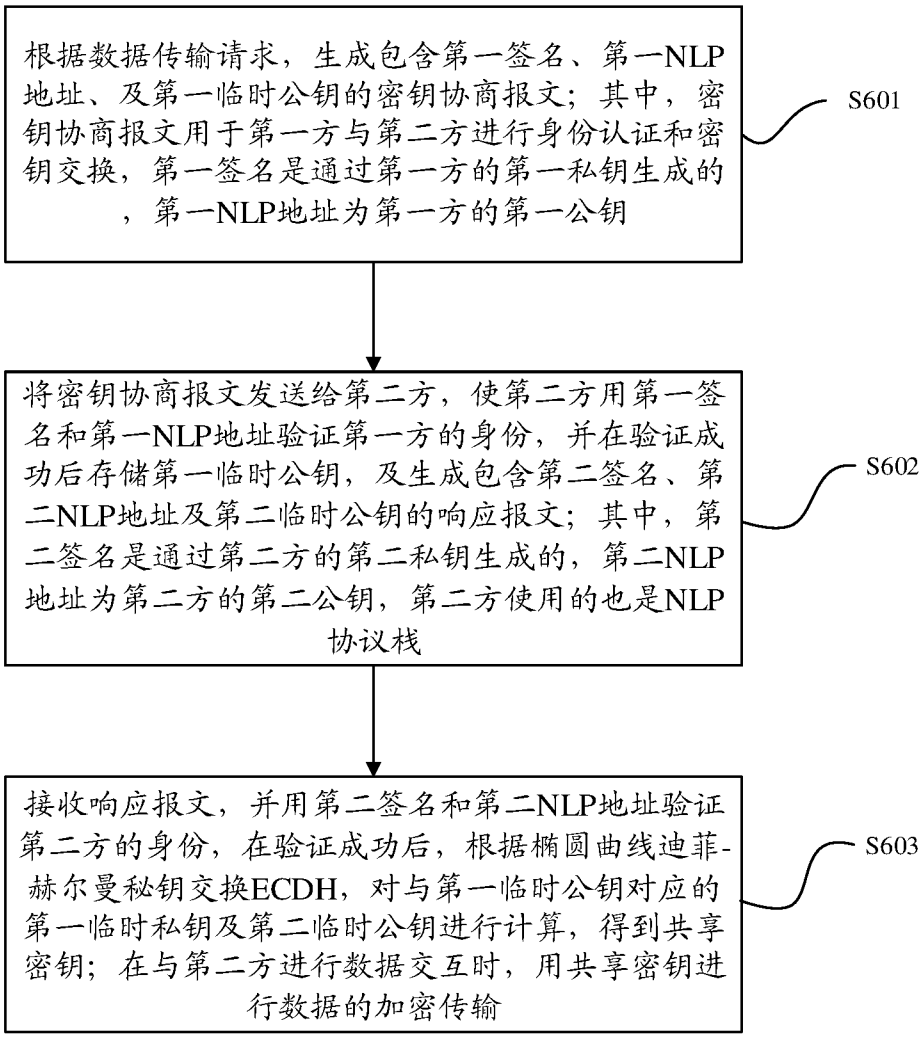
根据数据传输请求，生成包含第一签名、第一NLP地址、及第一临时公钥的密钥协商报文；其中，密钥协商报文用于第一方与第二方进行身份认证和密钥交换，第一签名是通过第一方的第一私钥生成的，第一NLP地址为第一方的第一公钥
S601
将密钥协商报文发送给第二方，使第二方用第一签名和第一NLP地址验证第一方的身份，并在验证成功后存储第一临时公钥，及生成包含第二签名、第二NLP地址及第二临时公钥的响应报文；其中，第二签名是通过第二方的第二私钥生成的，第二NLP地址为第二方的第二公钥，第二方使用的也是NLP协议栈
S602
接收响应报文，并用第二签名和第二NLP地址验证第二方的身份，在验证成功后，根据椭圆曲线迪菲-赫尔曼秘钥交换ECDH，对与第一临时公钥对应的第一临时私钥及第二临时公钥进行计算，得到共享密钥；在与第二方进行数据交互时，用共享密钥进行数据的加密传输
S603

图 8F

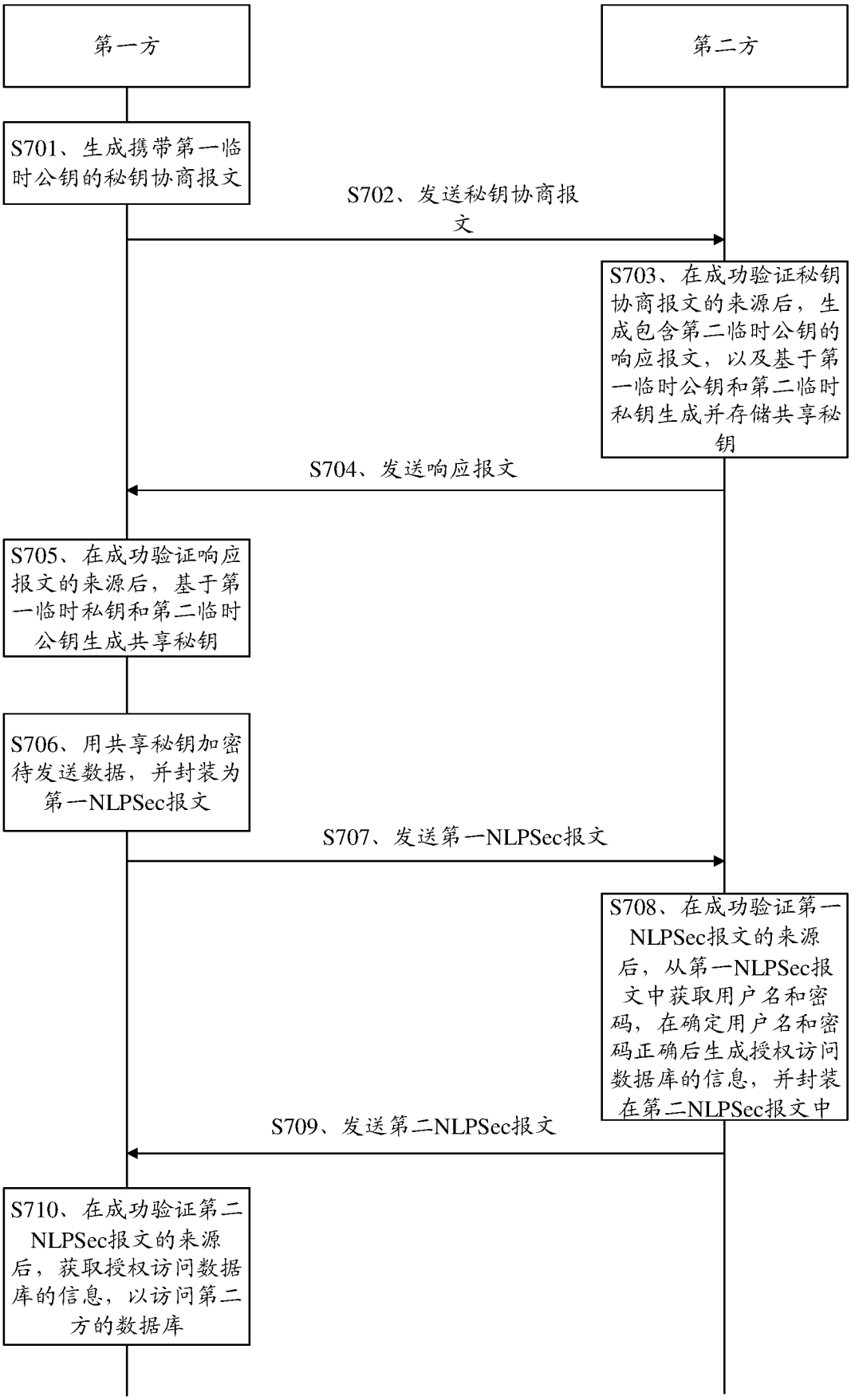
第一方
第二方
S701、生成携带第一临时公钥的秘钥协商报文
S702、发送秘钥协商报文
S703、在成功验证秘钥协商报文的来源后，生成包含第二临时公钥的响应报文，以及基于第一临时公钥和第二临时私钥生成并存储共享秘钥
S704、发送响应报文
S705、在成功验证响应报文的来源后，基于第一临时私钥和第二临时公钥生成共享秘钥
S706、用共享秘钥加密待发送数据，并封装为第一NLPSec报文
S707、发送第一NLPSec报文
S708、在成功验证第一NLPSec报文的来源后，从第一NLPSec报文中获取用户名和密码，在确定用户名和密码正确后生成授权访问数据库的信息，并封装在第二NLPSec报文中
S709、发送第二NLPSec报文
S710、在成功验证第二NLPSec报文的来源后，获取授权访问数据库的信息，以访问第二方的数据库

图 8G

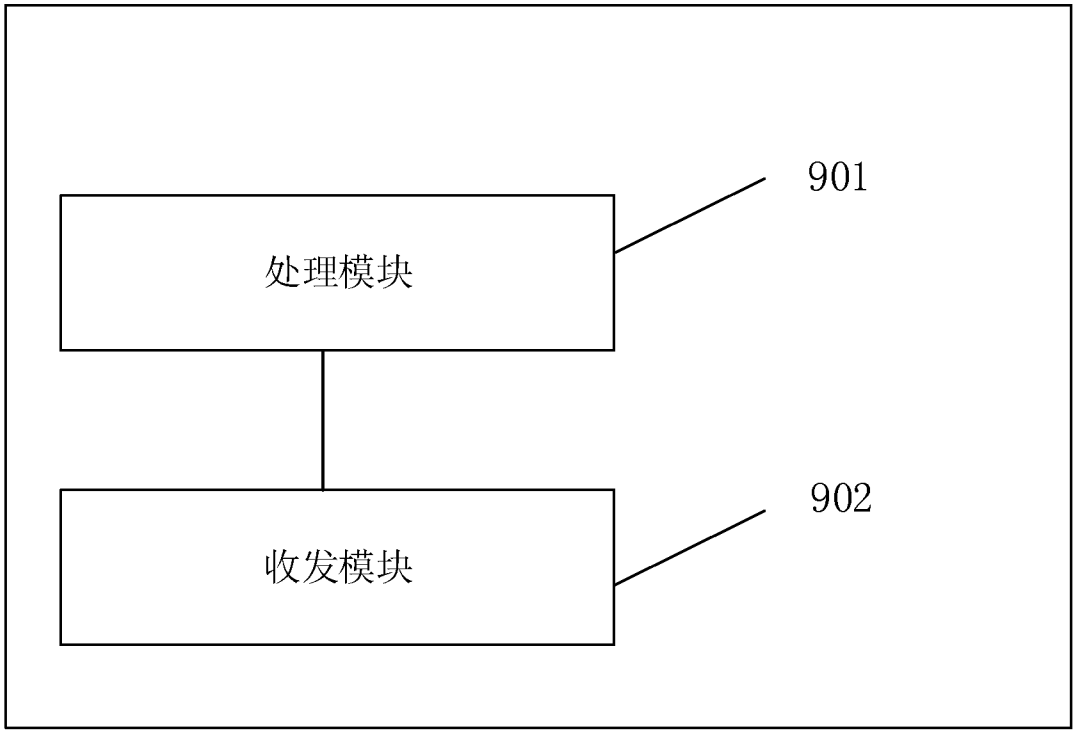

图 9A

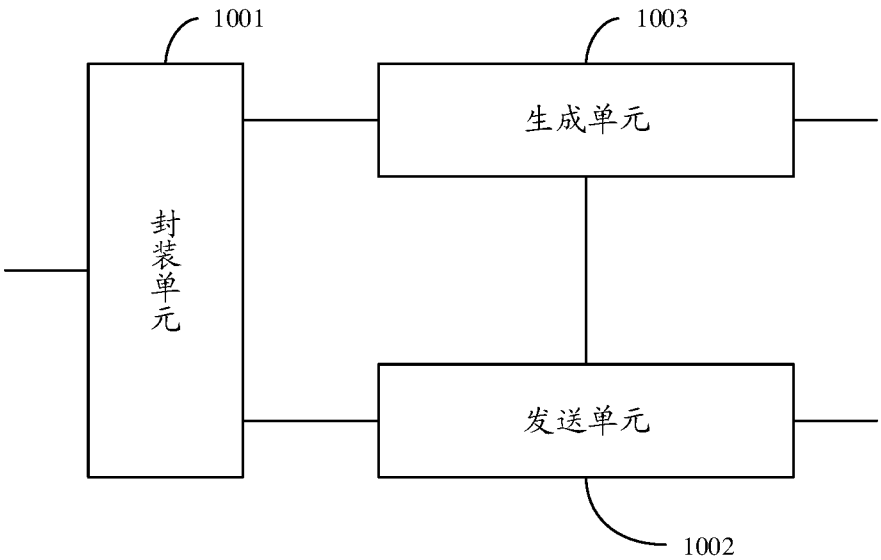

图 9B

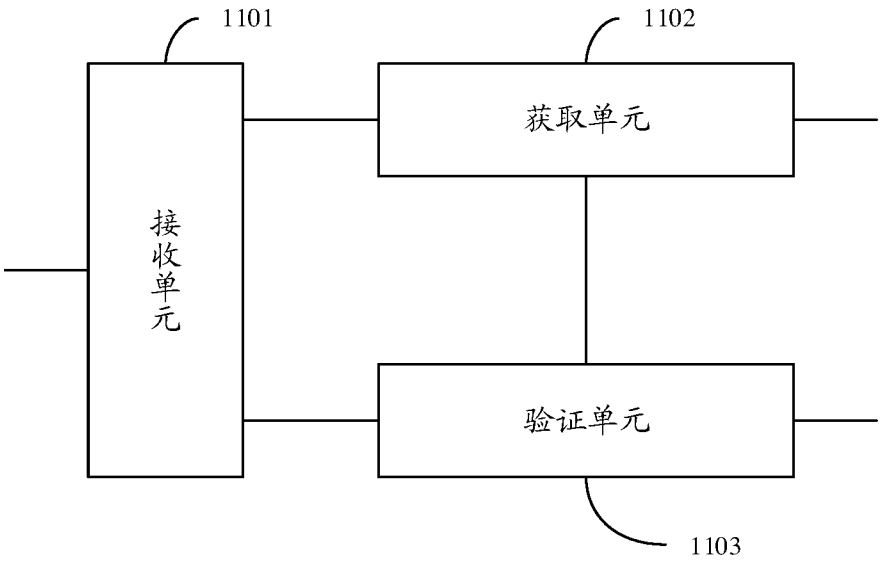

图 9C

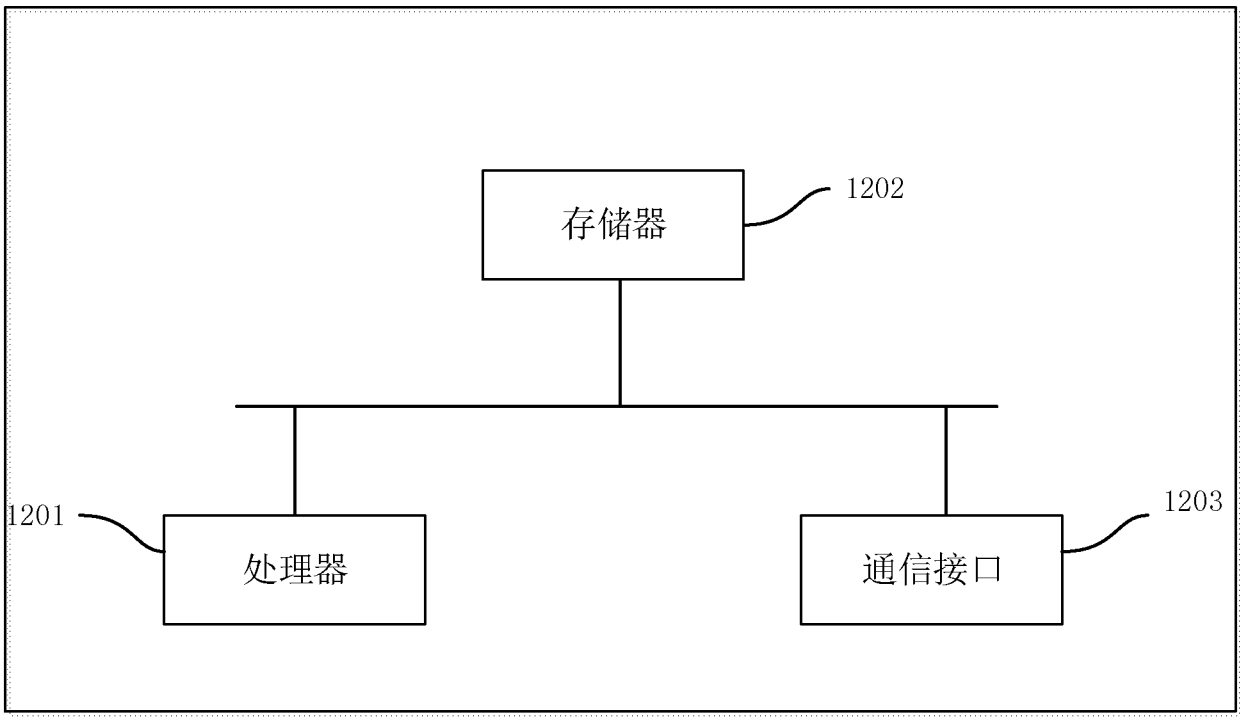

图 10

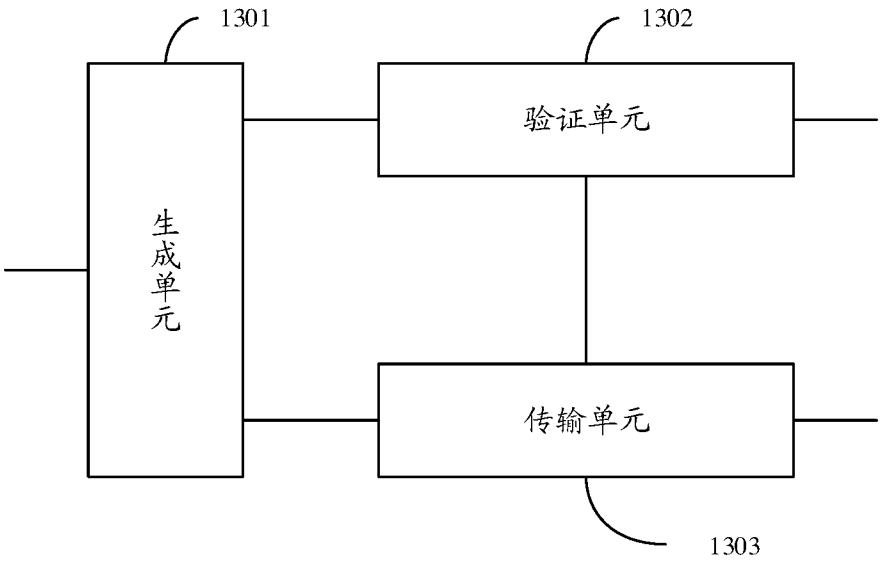

图 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2022/130453

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/08(2006.01)i;H04L 61/103(2022.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 9/-; H04L 61/-; H04W 12/-; H04L 12/-

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)

CNABS; CNTXT; CNKI; 万方, WANFANG; 百度学术, BAIDU SCHOLAR: MAC地址, 公钥, 私钥, 密钥, 秘钥, 欺骗, 欺诈, 虚假, 仿冒, 伪造, 诈骗, 仿造, 伪装, 恶意, 非法, 假冒, 攻击, 认证, 鉴权, 校验, 检验, 检测, 合法, 鉴定, 签名, 源, 源地址, 序号, 序列, 重放, 重复; VEN; WOTXT; USTXT; EPTXT; IEEE; 3GPP: MAC address, public key, private key, secret key, spoof, fraud, false, counterfeit, disguise, malicious, illegal, attack, authenticat+, verificat+, detect+, source address, serial number, sequence, replay, repeat+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 113904766 A (BEIJING CENTURY INTERNET BROADBAND DATA CENTER CO., LTD.) 07 January 2022 (2022-01-07) description, paragraphs [0007]-[0042]	1-16, 19-22, 25-26
PX	CN 113905012 A (BEIJING CENTURY INTERNET BROADBAND DATA CENTER CO., LTD.) 07 January 2022 (2022-01-07) claims 10 and 11	21-22
PX	CN 113904807 A (BEIJING CENTURY INTERNET BROADBAND DATA CENTER CO., LTD.) 07 January 2022 (2022-01-07) description, paragraphs [0005]-[0052]	17-18, 23-26
X	US 2019306705 A1 (BROTHER KOGYO KABUSHIKI KAISHA) 03 October 2019 (2019-10-03) description, paragraphs [0062]-[0067]	1-16, 19-22, 25-26

☑ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"D" document cited by the applicant in the international application
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
02 February 2023	**08 February 2023**

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101640631 A (CHENGDU HUAWEI SYMANTEC TECHNOLOGIES CO., LTD.) 03 February 2010 (2010-02-03) page 1, lines 3-7, page 5, line 19-page 9, line 21	17-18, 23-26
A	CN 101304407 A (HUAWEI TECHNOLOGIES CO., LTD.) 12 November 2008 (2008-11-12) entire document	1-26
A	CN 112235608 A (VISIONVERA INFORMATION TECHNOLOGY CO., LTD.) 15 January 2021 (2021-01-15) entire document	1-26

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2022/130453

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 113904766 A	07 January 2022	None	
CN 113905012 A	07 January 2022	None	
CN 113904807 A	07 January 2022	None	
US 2019306705 A1	03 October 2019	US 11064362 B2	13 July 2021
		US 2021306860 A1	30 September 2021
		JP 2019180037 A	17 October 2019
		JP 7052496 B2	12 April 2022
CN 101640631 A	03 February 2010	US 2011119534 A1	19 May 2011
		WO 2010012171 A1	04 February 2010
		EP 2309686 A1	13 April 2011
		EP 2309686 A4	14 December 2011
		EP 2309686 B1	18 June 2014
		CN 101640631 B	16 November 2011
CN 101304407 A	12 November 2008	None	
CN 112235608 A	15 January 2021	None	

国际检索报告

国际申请号
PCT/CN2022/130453

A. 主题的分类

H04L 9/08(2006.01)i;H04L 61/103(2022.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L 9/-; H04L 61/-; H04W 12/-; H04L 12/-

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））

CNABS;CNTXT;CNKI;万方;百度学术: MAC地址，公钥，私钥，密钥，秘钥，欺骗,欺诈,虚假,仿冒,伪造,诈骗,仿造,伪装,恶意,非法,假冒,攻击，认证,鉴权,校验,检验,检测,合法,鉴定,签名,源,源地址，序号,序列,重放,重复 VEN;WOTXT;USTXT;EPTXT;IEEE;3GPP: MAC address, public key, private key, secret key, spoof, fraud, false, counterfeit, disguise, malicious, illegal, attack, authenticat+, verificat+, detect+, source address, serial number, sequence, replay, repeat+

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
PX	CN 113904766 A (北京世纪互联宽带数据中心有限公司) 2022年1月7日 (2022-01-07) 说明书[0007]-[0042]段	1-16,19-22,25-26
PX	CN 113905012 A (北京世纪互联宽带数据中心有限公司) 2022年1月7日 (2022-01-07) 权利要求10,11	21-22
PX	CN 113904807 A (北京世纪互联宽带数据中心有限公司) 2022年1月7日 (2022-01-07) 说明书[0005]-[0052]段	17-18,23-26
X	US 2019306705 A1 (BROTHER KOGYO KABUSHIKI KAISHA) 2019年10月3日 (2019-10-03) 说明书[0062]-[0067]段	1-16,19-22,25-26

☑ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"D" 申请人在国际申请中引证的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2023年2月2日	2023年2月8日
ISA/CN的名称和邮寄地址 中国国家知识产权局 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 潘丽娜 电话号码 (+86) 028-62969259

国际检索报告

国际申请号
PCT/CN2022/130453

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 101640631 A（成都市华为赛门铁克科技有限公司）2010年2月3日（2010-02-03） 第1页第3-7行,第5页19行-第9页21行	17-18,23-26
A	CN 101304407 A（华为技术有限公司）2008年11月12日（2008-11-12） 全文	1-26
A	CN 112235608 A（视联动力信息技术股份有限公司）2021年1月15日（2021-01-15） 全文	1-26

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2022/130453

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	113904766	A	2022年1月7日	无			
CN	113905012	A	2022年1月7日	无			
CN	113904807	A	2022年1月7日	无			
US	2019306705	A1	2019年10月3日	US	11064362	B2	2021年7月13日
				US	2021306860	A1	2021年9月30日
				JP	2019180037	A	2019年10月17日
				JP	7052496	B2	2022年4月12日
CN	101640631	A	2010年2月3日	US	2011119534	A1	2011年5月19日
				WO	2010012171	A1	2010年2月4日
				EP	2309686	A1	2011年4月13日
				EP	2309686	A4	2011年12月14日
				EP	2309686	B1	2014年6月18日
				CN	101640631	B	2011年11月16日
CN	101304407	A	2008年11月12日	无			
CN	112235608	A	2021年1月15日	无			