(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2024 年 8 月 29 日 (29.08.2024)

WIPO | PCT

(10) 国际公布号
WO 2024/174596 A1

(51) 国际专利分类号:
H04L 9/40 (2022.01)

(21) 国际申请号: PCT/CN2023/131400

(22) 国际申请日: 2023 年 11 月 14 日 (14.11.2023)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202310201907.3 2023年2月23日 (23.02.2023) CN

(71) 申请人: 腾 讯 科 技 (深 圳) 有 限 公 司 **(TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED)** [CN/CN]; 中国广东省深圳市南山区高新区科技中一路腾讯大厦35层, Guangdong 518057 (CN)。

(72) 发明人: 吴 波 **(WU, Bo)**; 中国广东省深圳市南山区高新区科技中一路腾讯大厦35层, Guangdong 518057 (CN)。

(74) 代理人: 深圳市深佳知识产权代理事务所 (普通合伙) **(SHENPAT INTELLECTUAL PROPERTY AGENCY)**; 中国广东省深圳市罗湖区南湖街道春风路庐山大厦B座18C2、18D、18E、18E2, Guangdong 518001 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD,

(54) **Title:** DATA ENCRYPTION METHOD AND RELATED APPARATUS

(54) 发明名称: 一种数据加密方法和相关装置

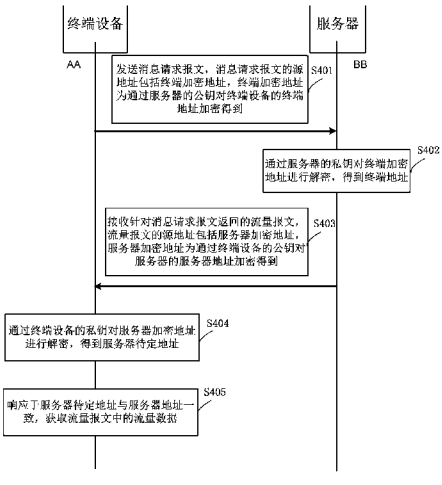

图 4

S401 Send a message request packet, a source address of the message request packet comprising a terminal encrypted address, and the terminal encrypted address being obtained by encrypting a terminal address of a terminal device by means of a public key of a server
S402 Decrypt the terminal encrypted address by means of a private key of the server, to obtain the terminal address
S403 Receive a traffic packet returned for the message request packet, a source address of the traffic packet comprising a server encrypted address, and the server encrypted address being obtained by encrypting a server address of the server by means of a public key of the terminal device
S404 Decrypt the server encrypted address by means of a private key of the terminal device, to obtain a server pending address
S405 Obtain traffic data in the traffic packet in response to the server pending address being consistent with the server address
AA Terminal device
BB Server

(57) Abstract: Embodiments of the present application disclose a data encryption method and a related apparatus. When a terminal device and a server perform network communication by means of an interaction packet, source addresses in a message request packet and a traffic packet for interaction between the terminal device and the server are encrypted by means of public keys of receiving ends, and real source addresses of the packets can be obtained only after decryption using private keys of the receiving ends. By encrypting the source addresses of the packets, even if an attacker acquires a packet, the attacker can only learn about a receiving end of a packet and cannot determine a sending end of the packet, so that the attacker can only obtain fragmented information and cannot concatenate the fragmented information, thereby reducing the possibility of leaking user privacy by means of the source address and destination address of the packet. Moreover, a terminal device acting as a data receiving end can also restore the real source address of the received packet using a private key of the terminal device, ensuring the security of the packet.

(57) 摘要: 本申请实施例公开了一种数据加密方法和相关装置，当终端设备和服务器通过交互报文进行网络通信时，之间交互的消息请求报文和流量报文中的源地址均被通过接收端的公钥进行加密，只有通过接收端的私钥解密后才能获得报文真实的源地址。通过加密报文的源地址，使得攻击者即使获取报文，也仅能知晓该报文的接收端，而无法确定报文的发送端，使得攻击者仅能得到碎片化的信息，无法将碎片化的信息进行拼接，从而降低了通过报文的源地址和目的地址泄露用户隐私的可能性。而且，作为数据接收端的终端设备也能通过自身私钥还原出所接收报文的真实源地址，保证了报文接收的安全性。

WO 2024/174596 A1

[见续页]

SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, 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))。

一种数据加密方法和相关装置

本申请要求于 2023 年 02 月 23 日提交中国专利局、申请号为 2023102019073、申请名称为“一种数据加密方法和相关装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及通信领域，特别涉及数据加密技术。

背景技术

网络通信的一种方式是基于目的地址的路由转发，其主要工作原理为：中间路由节点在从发送端或者其他中间路由节点收到报文后，从报文头部提取到对应的转发信息，例如对应的出端口等，中间路由节点将该报文通过该端口转发至下一跳的路由节点（例如中间路由节点或者目的端），直至目的端收到该报文。

网络通信的安全性是衡量互联网业务、客户端体验和运营商的重要条件，网络通信的安全性主要体现在通信安全和隐私保护等方面。相关技术中，为了提升网络通信的安全性，主要通过各类安全检测软硬件，对接收的报文进行安全检测，在一定概率上降低数据被篡改、流量被劫持、通信被非法获取的风险；如图 1 所示，当终端设备向数据存储服务器请求数据时，该服务器可以通过安全硬件平台对来自终端设备的请求报文或消息确认报文进行安全检测，并对检测出的恶意报文进行过滤，以进一步提升网络通信的安全性。

然而，相关技术对网络通信的安全性的检测维度并不全面，难以适应目前的隐私保护需求。

发明内容

为了解决上述技术问题，本申请提供了一种数据加密方法和相关装置，能够降低通过报文的源地址和目的地址泄露用户隐私的可能，满足目前的隐私保护需求。

本申请实施例公开了如下技术方案：

一方面，本申请实施例提供了一种数据加密方法，由终端设备执行，包括：

向服务器发送消息请求报文，消息请求报文的源地址包括终端加密地址，终端加密地址是通过服务器的公钥对终端设备的终端地址加密得到的；

接收服务器针对消息请求报文返回的流量报文，流量报文的源地址包括服务器加密地址，服务器加密地址是为通过终端设备的公钥对所述服务器的服务器地址加密得到的；

通过终端设备的私钥对服务器加密地址进行解密，得到服务器待定地址；

响应于服务器待定地址与服务器地址一致，获取流量报文中的流量数据。

另一方面，本申请实施例提供了一种数据加密方法，由服务器执行，包括：

接收终端设备发送的消息请求报文，消息请求报文的源地址包括终端加密地址，终端加密地址是通过服务器的公钥对终端设备的终端地址加密得到的；

通过服务器的私钥对终端加密地址进行解密，得到终端地址；

根据终端地址，向终端设备发送针对消息请求报文返回的流量报文，流量报文的源地址包括服务器加密地址，服务器加密地址是通过终端设备的公钥对服务器的服务器地址加密得到的。

另一方面，本申请实施例提供一种数据加密装置，包括发送单元，获取单元，解密单元和接收单元；

发送单元，用于向服务器发送用于消息请求报文，消息请求报文的源地址包括终端加密地址，终端加密地址是通过服务器的公钥对终端设备的终端地址加密得到的；

获取单元，用于接收服务器针对消息请求报文返回的流量报文，流量报文的源地址包括服务器加密地址，服务器加密地址是通过终端设备的公钥对服务器的服务器地址加密得到的；

解密单元，用于通过终端设备的私钥对服务器加密地址进行解密，得到服务器待定地址；

接收单元，用于响应于服务器待定地址与服务器地址一致，获取流量报文中的流量数据。

另一方面，本申请实施例提供了一种数据加密装置，包括获取单元，解密单元，发送单元；

获取单元，用于接收终端设备发送的消息请求报文，消息请求报文的源地址包括终端加密地址，终端加密地址是通过服务器的公钥对终端设备的终端地址加密得到的；

解密单元，用于通过服务器的私钥对终端加密地址进行解密，得到终端地址；

发送单元，用于根据终端地址，向终端设备发送针对消息请求报文返回的流量报文，流量报文的源地址包括服务器加密地址，服务器加密地址是通过终端设备的公钥对服务器的服务器地址加密得到的。

另一方面，本申请实施例提供了一种数据加密系统，数据加密系统包括终端设备和服务器，终端设备用于执行以上方面所述的方法，服务器用于执行以上方面所述的方法。

又一方面，本申请实施例提供了一种计算机设备，计算机设备包括处理器以及存储器：

存储器用于存储计算机程序，并将程序代码传输给处理器；

处理器用于根据计算机程序中的指令执行以上方面所述的方法。

又一方面，本申请实施例提供了一种计算机可读存储介质，计算机可读存储介质用于存储计算机程序，计算机程序用于执行以上方面所述的方法。

又一方面，本申请实施例提供了一种包括计算机程序的计算机程序产品，当其在计算机设备上运行时，使得计算机设备执行以上方面所述的方法。

由上述技术方案可以看出，终端设备通过交互报文和服务器进行网络通信时，之间交互的消息请求报文和流量报文中的源地址均被通过接收端的公钥进行了加密，只有通过接收端的私钥解密后才能获得报文真实的源地址。对源地址进行隐匿的原因在于，由于一个报文在网络通信中一般会携带源地址和目的地址，以便实现正确的转发，然而攻击者一旦截获报文，即可得到源地址和目的地址这一关系，相应地，可以确定终端设备的用户何时

上线并获取了哪些内容服务，从而推测出用户的隐私的信息。故通过加密报文的源地址，使得攻击者即使获取报文，也仅能知晓该报文的接收端，而无法确定报文的发送端，使得攻击者仅能得到碎片化的信息，而无法将碎片化的信息进行拼接，从而降低了通过报文的源地址和目的地址泄露用户隐私的可能性。而且，作为数据接收端的终端设备也能通过自身私钥还原出所接收报文的真实源地址，保证了报文接收的安全性。

附图说明

图 1 为一种基于安全硬件辅助的安全增强示意图；

图 2 为本申请实施例提供的一种数据加密场景的示意图；

图 3 为一种攻击者基于源地址和目的地址获取用户隐私的示意图；

图 4 为本申请实施例提供的一种数据加密方法的方法流程图；

图 5 为本申请实施例提供的一种消息请求报文示意图；

图 6 为本申请实施例提供的一种流量报文示意图；

图 7 为本申请实施例提供的一种流量确认报文示意图；

图 8 为本申请实施例提供的一种密钥创建报文示意图；

图 9 为本申请实施例提供的一种中间路由节点向密钥创建报文中添加中间共享密钥示意图；

图 10 为本申请实施例提供的一种密钥确认报文示意图；

图 11 为本申请实施例提供的一种加密源地址和目的地址的流量报文示意图；

图 12 为本申请实施例提供的一种数据加密方法的具体流程图；

图 13 为本申请实施例提供的一种数据加密方法的通信示意图；

图 14 为本申请实施例提供的一种数据加密装置的装置结构图；

图 15 为本申请实施例提供的另一种数据加密装置的装置结构图；

图 16 为本申请实施例提供的一种数据加密系统的系统结构图；

图 17 为本申请实施例提供的一种终端设备的结构图；

图 18 为本申请实施例提供的一种服务器的结构图。

具体实施方式

下面结合附图，对本申请的实施例进行描述。

相关技术中，可以通过各类安全检测软硬件对网络通信进行安全检测，如图 1 所示，可以通过安全检测硬件来对终端设备与数据存储服务器之间交互的各种报文进行安全检测，并对检测出的恶意报文进行过滤，在一定程度上提升了网络通信的安全性。此外，还可以从通信协议角度来提高网络通信的安全性，主要是通过加密方式来对报文中的数据进行加密，从而降低报文转发过程中数据被非法获取、篡改、重定向的风险，例如，在传输控制协议（TCP，Transport Control Protocol）基础上，通过安全套接字（SSL，Secure Sockets Layer）/传输层安全(TLS, Transport Layer Security)协议加密，或在用户数据报协议（UDP，User Datagram Protocol）基础上，提出快速 UDP 互联网连接（QUIC，Quick UDP Internet Connection）协议，实现对报文中的数据进行加密，从而使得恶意中间路由节点在缺乏解

密密钥的情况下无法获取报文中的数据内容。

然而，通过安全检测软硬件来对网络通信进行安全检测、以及从通信协议的角度来对数据进行加密，并不能在报文地址的维度上提升安全性，一旦被攻击者截获报文，攻击者能够得到该报文的源地址和目的地址，进而能够根据源地址和目的地址之间的关系推测出终端用户的隐私的信息，造成用户的隐私泄露。

为此，本申请实施例提供了一种数据加密方法和相关装置，对终端设备和服务器之间交互的报文中的源地址进行加密，降低攻击者通过报文的源地址和目的地址获取终端用户的隐私的信息的可能性，在报文地址的维度上提升了网络通信的安全性。

本申请实施例提供的数据加密方法可以通过计算机设备实施，该计算机设备可以是终端设备或服务器，其中，服务器可以是独立的物理服务器，也可以是多个物理服务器构成的服务器集群或者分布式系统，还可以是提供云计算服务的云服务器。终端可以是智能手机、平板电脑、笔记本电脑、台式计算机、智能音箱、智能手表、车载终端、智能电视等，但并不局限于此。终端以及服务器可以通过有线或无线通信方式进行直接或间接地连接，本申请在此不做限制。

本申请实施例提供的数据加密方法可基于云存储(cloud storage)实现，云存储是在云计算概念上延伸和发展出来的一个新的概念，分布式云存储系统（以下简称存储系统）是指通过集群应用、网格技术以及分布存储文件系统等功能，将网络中大量各种不同类型的存储设备（也称为存储节点）通过应用软件或应用接口集合起来协同工作，共同对外提供数据存储和业务访问功能的一个存储系统。

目前，存储系统的存储方法为：创建逻辑卷，在创建逻辑卷时，为每个逻辑卷分配物理存储空间，该物理存储空间可能由某个存储设备或者某几个存储设备的磁盘组成。客户端在某一逻辑卷上存储数据，也就是将数据存储在文件系统上，文件系统将数据分成许多部分，每一部分是一个对象，对象不仅包含数据而且还包含数据标识（ID，ID entity）等额外的信息，文件系统将每个对象分别写入该逻辑卷的物理存储空间，且文件系统会记录每个对象的存储位置信息，当客户端请求访问数据时，文件系统能够根据每个对象的存储位置信息让客户端对数据进行访问。

存储系统为逻辑卷分配物理存储空间的过程，具体为：按照对存储于逻辑卷的对象的容量估量（该估量往往相对于实际要存储的对象的容量有很大余量）和独立冗余磁盘阵列（RAID，Redundant Array of Independent Disk)的组别，预先将物理存储空间划分成分条，一个逻辑卷可以理解为一个分条，从而为逻辑卷分配了物理存储空间。

例如，在本申请实施例中的服务器可以是实现云存储的云服务器。

图 2 为本申请实施例提供的一种数据加密场景的示意图，其中，前述的计算机设备为终端设备和服务器，终端设备和服务器之间可以通过交互报文进行网络通信，该服务器可以是能实现云存储的云服务器，也可以是非云服务器，例如传统物理服务器等，该服务器可以是内容服务器，内容服务器是指能够实现内容分发网络（CDN，Content Delivery Network）的功能的服务器。

终端设备和服务器之间进行网络通信时，终端设备会发送消息请求报文，消息请求报

文是指终端设备向服务器发送的请求报文，例如，消息请求报文可以是终端设备向服务器发送的用于请求获取目标内容的请求报文，其中，消息请求报文的源地址并未被直接公开，如图 2 所示，而是采用接收端（服务器）的公钥对其进行了加密，只有在服务器接收该消息请求报文之后，通过服务器的私钥解密后才能获得该消息请求报文真实的源地址。

相应的，终端设备从服务器获取流量报文，流量报文是指服务器向终端设备发送的响应于消息请求报文的报文，例如，流量报文可以是服务器发送的用于使该终端设备获取目标内容的报文，其中，流量报文的源地址也并未被直接公开，如图 2 所示，也是采用接收端（终端设备）的公钥对其进行了加密，只有在终端设备获取该流量报文之后，通过终端设备的私钥解密后才能获得流量报文真实的源地址。

在终端设备和服务器之间进行网络通信的过程中，对所交互的消息请求报文和流量报文中的源地址进行隐匿的原因在于，为了实现网络通信中报文的正确转发，报文中一般会携带源地址和目的地址，然而，一旦攻击者截获该报文，即可得到该报文的源地址和目的地址这一关系，进而，可以根据源地址和目的地址之间的关系推测出终端设备的用户何时上线、获取了哪些内容服务等隐私的信息，如图 3 所示，位于终端设备和服务器之间的攻击者可以根据消息请求报文和流量报文的源地址和目的地址，得到“某个用户正在上网”这一信息，甚至产生该用户“是否在家”等推断，同时，攻击者如果获取到某个云服务提供商的服务器的地址集合，那么根据消息请求报文或流量报文中是否存在该地址集合中的地址，可以判断用户正在获取的内容服务，例如，某个云服务提供商用于为短视频平台提供服务的内容互连网协议（IP，Internet Protocol）地址有：IP1、IP2、IP3、…、IP100，那么如果攻击者截取的报文中源地址或目的地址有上述 IP 地址，就能够推断“该用户正在观看短视频”这一用户状态。

在本申请实施例中，通过加密报文的源地址，使得攻击者即使截取报文，也仅能知晓该报文的接收端，无法确定报文的发送端，使得攻击者仅能得到碎片化的信息，而无法对碎片化的信息进行拼接，从而降低了通过报文的源地址和目的地址泄露用户隐私的可能。

同时，作为流量报文的接收端的终端设备能够通过自身私钥还原出所接收的流量报文的真实源地址，降低了终端设备随意接收报文带来的危险，保证了报文接收的安全性。

图 4 为本申请实施例提供的一种数据加密方法的方法流程图，在本实施例中，以计算机设备为终端和服务器来进行说明，该方法包括：

S401、终端设备向服务器发送消息请求报文，消息请求报文的源地址包括终端加密地址，终端加密地址是通过服务器的公钥对终端设备的终端地址加密得到的。

终端设备可以和服务器通过交互报文的方式进行网络通信，在实际应用中，一个服务器可以向多个终端设备发送报文，一个终端也可以向多个服务器发送请求报文，本实施例中以一个终端设备和一个服务器进行网络通信为例进行说明。

终端设备和服务器之间网络通信的目的可以是让终端设备从服务器处获取目标内容，当终端设备通过交互报文来从服务器获取目标内容时，终端设备为数据请求端，服务器为数据发送端。目标内容为终端设备所需的数据内容，目标内容可以是各种形式的数据内容，例如文字、图片、视频、直播流等，由于不同的服务器可以提供不同的数据内容，故终端

设备在发送消息请求报文前，可以先根据目标内容确定对应的服务器，再向确定的服务器发送对应的消息请求报文。

消息请求报文是指终端设备向服务器发送的请求报文，为了避免消息请求报文被攻击者截获之后获得该报文中源地址和目的地址之间的关系，进而得到用户的隐私的信息，消息请求报文中的源地址在本实施例中被加密，即对消息报文中的源地址实现了隐匿，使得攻击者即使截获该报文，也仅能知晓该报文的目的地址，而无法确定该报文的源地址，即攻击者在截获了该报文之后，仅知道有设备向服务器发送了报文，但是不知道是哪个设备发送的，难以推断出用户的隐私的信息，也就是说，通过对消息请求报文的源地址进行加密，可以实现对消息请求报文中源地址的隐匿，降低了攻击者通过消息请求报文的源地址和目的地址推断出用户的隐私的信息的可能性。

需要说明的是，可以通过服务器的公钥对终端设备的终端地址进行加密，得到对应的终端加密地址，例如，可以通过下述公式得到终端加密地址：

$$IP_sec = Enc\{Key_pub_server, IP_i\}$$

其中，IP_sec 表示终端加密地址，Key_pub_server 表示服务器的公钥，IP_i 表示终端设备的终端地址，Enc{α,β}表示使用密钥 α 对数据 β 进行加密操作。

根据上述公式，可以通过服务器的公钥对真实的终端地址进行加密得到对应的终端加密地址，如图 5 所示，终端加密地址可以被携带在消息请求报文（Pkt_req）中，例如，可以被携带在消息请求报文的 payload 中，以便服务器能够在获取消息请求报文之后通过终端加密地址确定终端设备对应的终端地址，即让消息请求报文的接收端能够准确确定该消息请求报文的发送端，以便在后续步骤中该接收端能够准确生成目的地址为该发送端的流量报文，保证报文传播的安全性和准确性。

需要说明的是，为了保证消息请求报文能够被准确转发，本实施例中消息请求报文的目的地址并未被加密，即消息请求报文中包括明文的服务器的服务器地址，以便消息请求报文在网络通信中可以基于服务器地址被准确转发至服务器。

为了在攻击者截获消息请求报文之后进一步的混淆攻击者，进一步降低攻击者通过消息请求报文中真实的源地址和目的地址推断出用户的隐私的信息的可能性，在一种可能的实现方式中，消息请求报文的源地址还包括终端隐匿地址，终端隐匿地址与终端地址不同。

终端隐匿地址是指消息请求报文中的明文的虚拟源地址，其中，为了能够对消息请求报文真实的源地址进行隐匿，终端隐匿地址显然不同于发送消息请求报文的终端设备真实的终端地址，如图 5 所示，当终端设备的终端地址为 IP_i 时，消息请求报文中不仅包括终端加密地址 IP_sec，还包括终端隐匿地址 IP_j，例如，消息请求报文的头部可以携带终端隐匿地址，其中，IP_i 与 IP_j 并不相同。

在消息请求报文中加入终端隐匿地址，可以让攻击者在截获该消息请求报文之后，被消息请求报文中的终端隐匿地址混淆，诱使攻击者得到该消息请求报文的源地址为终端隐匿地址这一错误判断，进一步降低攻击者通过消息请求报文获得真实的源地址和目的地址，并据此推断出用户的隐私的信息的可能性。

此外，由于对消息请求报文的真实源地址进行了隐匿，会导致消息请求报文的报文格

式发生变化，而通过在消息请求报文的源地址中加入终端隐匿地址，可以保持加密了源地址的消息请求报文与未加密源地址的报文在格式上并无区别，使得在终端设备和服务器的网络通信中，用于转发的设备可以根据消息请求报文的格式成功理解消息请求报文的涵义，进而保证消息请求报文的成功转发。

S402、服务器通过服务器的私钥对终端加密地址进行解密，得到终端地址。

服务器接收终端设备发送的消息请求报文之后，需要确定消息请求报文的源地址，以便对消息请求报文做出准确响应，由于消息请求报文中的源地址被隐匿，故服务器无法直接得到消息请求报文的源地址，需要通过对消息请求报文中的终端加密地址进行解密才能得到对应的终端地址。

如 S401 所述，终端加密地址是通过服务器的公钥对终端设备的终端地址加密得到的，其中，服务器的公钥是指该服务器对应的公开的密钥，其他设备都可以用服务器的公钥来加密数据，而服务器的私钥是该服务器私有的密钥，只有服务器拥有这个密钥，即只有服务器可以通过服务器的私钥来解密被服务器的公钥加密的数据，故服务器可以通过服务器的私钥对终端加密地址进行解密得到终端地址，例如，可以通过下述公式得到终端地址：

$$IP_i = Dec\{Key_pri_server, IP_sec\}$$

其中，IP_i 表示终端设备的终端地址，Key_pri_server 表示服务器的私钥，IP_sec 表示终端加密地址，$Dec\{\alpha,\beta\}$表示使用密钥 α 对数据 β 进行解密操作。

根据上述公式，可以通过服务器的私钥对终端加密地址进行解密，得到终端地址，该终端地址就是消息请求报文真实的源地址，也就是说，服务器在获取到消息请求报文之后，通过解密其中的终端加密地址确定该消息请求报文真实的源地址，为后续步骤中服务器能够准确向该终端地址发送流量报文打下了基础。

S403、终端设备接收服务器针对消息请求报文返回的流量报文，流量报文的源地址包括服务器加密地址，服务器加密地址是通过终端设备的公钥对服务器的服务器地址加密得到的。

流量报文是指服务器向终端设备发送的响应于消息请求报文中的请求的报文，例如，当消息请求报文为终端设备向服务器请求获取目标内容的报文时，流量报文可以是服务器发送的用于让该终端设备获取目标内容的报文，若目标内容为终端设备所需的文字，流量报文会相应的包括该文字对应的数据，当目标内容为终端设备所需的文字和图片时，流量报文会相应的包括该文字和图片对应的数据。

为了避免流量报文被攻击者截获之后获得该报文中源地址和目的地址之间的关系，进而得到用户的隐私的信息，流量报文中的源地址在本实例中也被加密，使得攻击者即使截获该报文，也仅能知晓该报文的目的地址，而无法确定该报文的源地址，即攻击者在截获了该报文之后，仅知道有设备向终端设备发送了报文，但是不知道是哪个设备发送的，相应地，难以推断出用户的隐私的信息，也就是说，通过对流量报文的源地址进行加密实现对流量报文中源地址的隐匿，降低了攻击者通过消息请求报文的源地址和目的地址来推断出用户的隐私的信息的可能性。

需要说明的是，可以通过终端设备的公钥来对服务器的服务器地址进行加密得到对应

的服务器加密地址，例如，可以通过下述公式得到服务器加密地址：

$$IP_sec_server = Enc\{Key_pub_client, IP_m\}$$

其中，IP_sec_server 表示服务器加密地址，Key_pub_client 表示终端设备的公钥，IP_m 表示服务器地址，Enc{α,β}表示使用密钥 α 对数据 β 进行加密操作。

通过上述公式，可以通过终端设备的公钥来对真实的服务器地址进行加密得到对应的服务器加密地址，如图 6 所示，服务器加密地址可以被携带在流量报文（Pkt_traffic）中，以便终端设备在获取该流量报文之后，在该流量报文的源地址被隐匿的情况下，通过后续步骤依然能够确定该流量报文的源地址，为保证报文传播的安全性打下了基础。

需要说明的是，为了保证流量报文能够被准确转发，本实施例中流量报文的目的地址并未被加密，即流量报文中包括明文的终端设备的终端地址，以便流量报文在网络通信中可以基于终端地址被准确转发至发送消息请求报文的终端设备。

在一种可能的实现方式中，流量报文的源地址还包括服务器隐匿地址，服务器隐匿地址与服务器地址不同。

服务器隐匿地址是指流量报文中的明文的虚拟源地址，服务器隐匿地址不同于发送流量报文的服务器真实的服务器地址，如图 6 所示，当服务器地址为 IP_m 时，流量报文中不仅包括服务器加密地址 IP_sec_server，还包括终端隐匿地址 IP_n，其中，IP_n 与 IP_m 并不相同。

在流量报文中加入服务器隐匿地址，一方面可以让攻击者在截获该流量报文之后，被流量报文中的服务器隐匿地址混淆，进一步降低攻击者获取到流量报文真实的源地址和目的地址，并据此推断出用户的隐私的信息的可能性；另一方面可以保证流量报文的报文格式，进而保证流量报文的成功转发。

S404、终端设备通过终端设备的私钥对服务器加密地址进行解密，得到服务器待定地址。

为了保证报文传输的安全性，终端设备需要确定获取的报文的来源，以降低终端设备被恶意报文攻击的可能性，故终端设备从服务器获取到流量报文之后，需要确定流量报文的源地址，以便确定该流量报文的来源，由于流量报文的源地址被隐匿，故终端设备无法直接得到流量报文的源地址，需要通过对流量报文中的服务器加密地址进行解密来得到对应的服务器待定地址。

如 S403 所述，服务器加密地址是通过终端设备的公钥加密得到的，故终端设备可以通过终端设备的私钥对服务器加密地址进行解密，得到服务器待定地址，例如，可以通过下述公式得到服务器待定地址：

$$IP_m_l = Dec\{Key_pri_client, IP_sec_server\}$$

其中，IP_m_l 表示服务器待定地址，Key_pri_client 表示终端设备的私钥，IP_sec_server 表示服务器加密地址，Dec{α,β}表示使用密钥 α 对数据 β 进行解密操作。

根据上述公式，可以通过终端设备的私钥对服务器加密地址进行解密，得到服务器待定地址，该服务器待定地址就是流量报文真实的源地址，也就是说，终端设备在获取到隐匿了源地址的流量报文之后，通过对流量报文中的服务器加密地址进行解密，确定了该流

量报文真实的源地址。

需要说明的是，考虑到流量报文在传输过程中可能被非法截取并篡改，相应地，该流量报文中包括的服务器加密地址也可能被篡改，在该种情况下，终端设备对该服务器加密地址进行解密得到的服务器地址，可能并非真实的服务器地址，即并非服务器加密的自身的真实地址；当然，在流量报文正常传输的情况下，终端设备对该流量报文中的服务器加密地址进行解密得到的服务器地址，即为真实的服务器地址。鉴于终端设备对服务器加密地址进行解密得到的服务器地址，暂且无法确认其真实性，故先将其称为服务器待定地址。

S405、终端设备响应于服务器待定地址与服务器地址一致，获取流量报文中的流量数据。

终端设备获取了流量报文之后，通过 S404 确定了该流量报文真实的源地址为服务器待定地址，同时，终端设备发送的消息请求报文的目的地址为服务器的服务器地址。当服务器地址与服务器待定地址一致时，表示终端设备发送的消息请求报文的目的地址与终端设备获取的流量报文真实的源地址一致，表示该流量报文为终端设备所需的针对消息请求报文返回的报文，并不是其他服务器发送的恶意报文或者无关报文，终端设备可以接收该流量报文中的流量数据，从而使得终端设备能够获取流量报文中的数据内容。

由于网络通信过程中，数据的接收端并不一定能够完整获取数据的发送端发送的报文内容，故在终端设备和服务器的交互过程中，需要对终端设备是否成功获取了服务器发送的报文内容进行判断。

在一种可能的实现方式中，终端设备还可以确定针对流量报文的报文接收结果；向服务器发送包括报文接收结果的流量确认报文，流量确认报文的源地址包括终端加密地址。

报文接收结果用于在终端设备接收流量报文的流量数据之后表示该终端设备对流量报文的接收状态，即报文接收结果用于反映终端设备实际上是否成功接收到该流量报文。

需要注意的是，在终端设备和服务器的实际网络通信过程中，针对终端设备发送的消息请求报文，服务器经常会需要发送多条流量报文来响应消息请求报文中的请求，例如，当消息请求报文为向服务器请求获取视频内容时，服务器通常需要发送多条流量报文才能实现该视频内容的完整传输，此时，报文接收结果可以是在终端设备接收到多条流量报文之后分析得到的终端设备对该多条流量报文的接收状态，例如，可以根据终端设备实际接收到的(或未接收到的)报文编号范围，反映终端设备针对多条流量报文的报文接收结果。为了能够让服务器及时的获取终端设备对多条流量报文的接收状态，终端设备可以周期性的进行报文接收结果的确定，在每次确定出报文接收结果后生成对应的流量确认报文，并向服务器进行上报。

为了使服务器能够判断终端设备是否成功获取了服务器发送的数据内容，终端设备可以向服务器发送包括报文接收结果的流量确认报文，流量确认报文用于表示终端设备在接收流量报文的流量数据之后、向服务器反馈报文接收情况的报文。

为了避免流量确认报文被攻击者截获之后获得该报文中源地址和目的地址之间的关系，进而得到用户的隐私的信息，流量确认报文中的源地址也被隐匿，即流量确认报文中的源地址也不为终端地址，而是终端加密地址，进而降低了攻击者通过流量确认报文的源

地址和目的地址，并据此推断出用户的隐私的信息的可能性。

当流量确认报文的源地址被隐匿时，为了进一步混淆攻击者且保持报文格式，流量确认报文的源地址还可以包括终端隐匿地址。

如图 7 所示，由终端设备向服务器发送的流量确认报文（Pkt_ack）中可以包括终端隐匿地址 IP_j、终端加密地址 IP_sec 和当前接收到的报文编号范围 Pkt_num_range，其中，终端隐匿地址用于混淆攻击者和保持流量确认报文的报文格式，终端加密地址用于向服务器提供仅服务器可以解密的加密后的真实源地址，当前接收到的报文编号范围用于表示终端设备的报文接收结果。

需要说明的是，为了保证流量确认报文能够被准确转发，本实施例中流量确认报文的目的地址并未被加密，即流量确认报文包括明文的服务器的服务器地址。

终端设备在获取了流量报文的流量数据之后，可以向服务器发送包括报文接收结果的流量确认报文，以便服务器能够确定终端设备对流量报文的接收状态，从而验证流量报文是否成功传输，保证数据传输的完整性。

在一种可能的实现方式中，服务器接收终端设备发送的包括报文接收结果的流量确认报文，流量确认报文的源地址包括终端加密地址，报文接收结果用于标识终端设备对流量报文的接收状态；

当服务器根据报文接收结果确定终端设备未接收到目标流量报文时，服务器向终端设备发送作为流量重传报文的目标流量报文，流量重传报文的源地址包括服务器加密地址。

在终端设备向服务器发送流量确认报文之后，服务器可以接收终端设备发送的流量确认报文，流量确认报文中包括报文接收结果，服务器可以根据报文接收结果确定终端设备对目标流量报文的接收情况。

当服务器根据报文接收结果确定终端设备已接收到目标流量报文时，服务器可以确定目标流量报文传输成功，无需再对目标流量报文进行重传处理。

当服务器根据报文接收结果确定终端设备未接收到目标流量报文时，服务器可以向终端设备发送作为流量重传报文的目标流量报文，流量重传报文是指报文接收结果标识的终端设备未接收到的流量报文，流量重传报文用于对终端设备未接收到的流量报文进行重传。也就是说，当存在终端设备未接收到的流量报文时，服务器可以将上述未接收到的流量报文作为流量重传报文进行重传，以便终端设备能够获取未接收到的流量报文。通过让服务器发送流量重传报文，可以让终端设备获取未接收到的目标流量报文，以保证终端设备和服务器之间的报文传输的可靠性。

为了避免流量重传报文重传时被攻击者截获之后获得该报文中源地址和目的地址之间的关系，流量重传报文中的源地址也被隐匿，即流量重传报文中的源地址也不为服务器地址，而是服务器加密地址，进而降低了攻击者通过流量重传报文的源地址和目的地址，并据此推断出用户的隐私的信息的可能性。

当流量重传报文的源地址被隐匿时，为了进一步混淆攻击者且保持报文格式，流量重传报文的源地址还可以包括服务器隐匿地址。

需要说明的是，为了保证流量重传报文能够被准确转发，本实施例中流量重传报文的

目的地址并未被加密，即流量重传报文包括明文的服务器的服务器地址。

服务器在接收到终端设备发送的流量确认报文之后，可以根据流量确认报文确定终端设备对流量报文的接收情况，在终端设备并未接收到目标流量报文的情况下，即在终端设备并未完整接收到服务器返回的流量报文的情况下，生成表示该终端设备并未成功接收到针对消息请求报文返回的目标流量报文的报文接收结果，并将其添加至流量确认报文中，服务器可以响应该流量确认报文向终端设备发送流量重传报文，以便实现丢包重传，降低由于终端设备所接收的报文发生丢包的可能性。

在一种可能的实现方式中，终端设备接收服务器获取响应流量确认报文返回的流量重传报文，流量重传报文是报文接收结果标识的终端设备未接收到的流量报文，流量重传报文的源地址包括服务器加密地址。

当服务器根据流量确认报文确定终端设备存在未接收到的流量报文时，终端设备可以从服务器获取响应流量确认报文返回的流量重传报文，流量重传报文是指终端设备未接收到的需要重传的报文，终端设备通过获取流量重传报文可以实现对未接收到的流量报文的接收，其中，为了避免终端设备获取流量重传报文时，流量重传报文被攻击者截获之后获得该报文中源地址和目的地址之间的关系，流量重传报文中的源地址也被隐匿，当流量重传报文的源地址被隐匿时，为了进一步混淆攻击者且保持报文格式，流量重传报文的源地址还可以包括服务器隐匿地址。

终端设备获取响应流量确认报文返回的流量重传报文，以实现对未接收到的流量报文的再次接收，从而保证终端设备和服务器之间的报文传输的可靠性。

由此可见，终端设备通过交互报文来和服务器网络通信时，之间交互的消息请求报文和流量报文中的源地址均被通过接收端的公钥进行了加密，只有通过接收端的私钥解密后才能获得报文真实的源地址。对源地址进行隐匿的原因在于，由于报文在网络通信中一般会携带源地址和目的地址，以便实现正确的转发，然而一旦报文被攻击者截获，攻击者将得到源地址和目的地址这一关系，进而确定终端设备的用户何时上线并获取了哪些内容服务，从而推测出用户的隐私的信息。故通过加密报文的源地址，使得攻击者即使获取报文，也仅能知晓该报文的接收端，而无法确定报文的发送端，使得攻击者仅能得到碎片化的信息，而无法将碎片化的信息拼接，从而降低了通过报文的源地址和目的地址泄露用户隐私的可能。而且，作为数据接收端的终端设备也能通过自身私钥还原出所接收的报文的真实源地址，保证了报文接收的安全性。

在前述实施例中，会对终端设备和服务器之间的报文的源地址进行加密，从而降低通过报文的源地址和目的地址泄露用户隐私的可能。由于相关技术中网络通信主要是基于目的地址来进行转发的，如果擅自修改报文的目的地址，则会造成报文无法被正确转发，进而造成用户体验质量（QoE，Quality of Experience）和服务质量（QoS，Quality of Services）的下滑，故报文中仍然会有明文的目的地址，从而让该报文可以基于该目的地址被准确转发，保证终端设备和服务器之间的报文交互的可靠实现。

虽然终端设备和服务器之间的报文的源地址被加密可以在一定程度上降低通过报文的源地址和目的地址泄露用户隐私的可能，但是由于该报文中的目的地址并未被加密，还

是会存在用户隐私泄露的风险，故可以对终端设备和服务器之间网络通信过程中数量最多的流量报文的目的地址也进行加密，使得攻击者在获取流量报文时，不仅无法获取流量报文的发送端，也无法获取流量报文的接收端，从而进一步降低攻击者通过真实的源地址和目的地址推断出用户的隐私的信息的可能性。

在一种可能的实现方式中，S403 中终端设备接收针对消息请求报文返回的流量报文，相应的，即服务器可以根据终端地址，向终端设备发送针对消息请求报文返回的流量报文，而在服务器根据终端地址向终端设备发送针对消息请求报文返回的流量报文方面，数据加密方法具体包括：

S11、服务器根据终端地址，确定从服务器到终端设备的流量链路，流量链路包括 N 个中间路由节点，N 为大于等于 1 的整数；

S12、服务器通过流量链路中的 N 个中间路由节点，向终端设备发送针对消息请求报文返回的流量报文。

流量链路是指服务器和终端设备之间用于传输流量报文的链路，在服务器和终端设备的报文交互的实际过程中，由于服务器通常会向终端设备发送多条流量报文，为了能够得到稳定的链路来对流量报文进行可靠转发，可以由服务器根据终端地址确定从服务器到终端设备用于传输流量报文的流量链路，其中，流量链路包括 N 个中间路由节点。

中间路由节点是指流量链路包括的用于转发流量报文的路由节点，在服务器根据流量链路向终端设备发送流量报文的过程中，中间路由节点用于对流量报文进行转发，直至终端设备的上一跳路由节点将该流量报文顺利转发至终端设备。

为了能够让流量报文从服务器成功发送至终端设备，服务器可以先根据终端地址确定服务器到终端设备的流量链路，再通过该流量链路中的 N 个中间路由节点实现流量报文由服务器至终端设备的准确转发。

在服务器可以根据终端地址确定用于转发流量报文的流量链路的基础上，服务器可以先基于该流量链路向终端设备发送密钥创建报文，以获取该流量链路的中间路由节点的相关信息，即在一种可能的实现方式中，数据加密方法还包括：

S21、服务器根据终端地址和服务器地址，生成针对流量链路的流标识和共享密钥；

S22、服务器通过终端设备的公钥加密共享密钥，得到密钥加密数据；

S23、服务器通过流量链路，向终端设备发送包括密钥加密数据和流标识的密钥创建报文，密钥创建报文的源地址包括服务器加密地址，密钥创建报文用于指示 N 个中间路由节点根据流标识生成中间共享密钥，通过终端设备的公钥加密中间共享密钥，并将加密结果添加到密钥加密数据中。

如前所述，流量链路是指服务器和终端设备之间用于传输流量报文的链路，由于服务器和终端设备之间可以存在多条链路，故可以根据流标识来准确标识流量链路，即流标识是唯一标识流量链路的标识数据，例如，可以根据下述公式来确定流量链路的流标识：

$$FlowID = Hash(IP_m||IP_i||Port_server||Port_client||Protocol)$$

其中，FlowID 表示流标识，IP_m 表示服务器的服务器地址，IP_i 表示终端设备的终端地址，Port_server 表示服务器的服务器端口、Port_client 表示终端设备的终端端口，

Protocol 表示服务器和终端设备之间的通信协议，Hash()表示哈希操作，||表示拼接操作。

根据上述公式可以确定服务器和终端设备之间用于传输流量报文的流量链路对应的流标识。

针对该流量链路的共享密钥是指服务器根据流标识计算的、与终端设备共享的密钥信息，共享密钥会在加密后由服务器发送给终端设备，在后续步骤中用于给终端设备向服务器发送的数据进行加密，也就是说，共享密钥虽然是服务器生成的，但是并不是服务器私有的，而是可以与终端设备共享的密钥信息。例如，可以根据下述公式计算针对该流量链路的共享密钥：

$$Key_share = Hash(info_server||FlowID)$$

其中，Key_share 表示共享密钥，info_server 表示服务器的自身私有信息，FlowID 表示流标识，Hash()表示哈希操作，||表示拼接操作。

根据上述公式可以让服务器根据自身私有信息和流标识计算得到与终端设备共享的共享密钥。

在服务器根据流标识生成与终端设备共享的共享密钥之后，为了只让终端设备获取该共享密钥，可以根据终端设备的公钥对共享密钥进行加密，得到对应的密钥加密数据，例如，可以通过下述公式得到共享密钥对应的密钥加密数据：

$$Enc_share = Enc\{Key_pub_client, Key_share\}$$

其中，Enc_share 表示密钥加密数据，Key_pub_client 表示终端设备的公钥，Key_share 表示共享密钥，Enc{α,β}表示使用密钥 α 对数据 β 进行加密操作。

根据上述公式可以让服务器通过终端设备的公钥对共享密钥进行加密，得到仅有终端设备可以解密的密钥加密数据。

在服务器获取了针对流量链路的流标识和密钥加密数据之后，服务器可以通过密钥创建报文向终端设备发送流标识和密钥加密数据，其中，为了避免密钥创建报文在转发时被攻击者截获之后获得该报文中源地址和目的地址之间的关系，密钥创建报文中的源地址也被隐匿，即密钥创建报文中的源地址也不为服务器地址，而是服务器加密地址，进而降低了攻击者通过密钥创建报文的源地址和目的地址来推断出用户的隐私的信息的可能性。当密钥创建报文的源地址被隐匿时，为了进一步混淆攻击者且保持报文格式，密钥创建报文的源地址还可以包括服务器隐匿地址，如图 8 所示，密钥创建报文（Pkt_key）中包括服务器隐匿地址 IP_n、流标识 FlowID、服务器加密地址 IP_sec_server 和密钥加密数据 Enc_share。

需要说明的是，为了保证密钥创建报文能够被准确转发，本实施例中，密钥创建报文的目的地址并未被加密，即密钥创建报文中包括明文的终端设备的终端地址，以便密钥创建报文在网络通信中可以基于终端地址被准确转发至终端设备。

密钥创建报文通过流量链路中的中间路由节点可以由服务器转发至终端设备，在转发过程中，为了能够获取中间路由节点和服务器以及终端设备共享的中间共享密钥，中间共享密钥是指中间路由节点根据流标识计算的、与终端设备以及服务器共享的密钥信息，中间共享密钥会在加密后被添加到密钥创建报文中的密钥加密数据中，以便发送给终端设备，

并且在后续步骤中可以再由终端设备发送给服务器，以便服务器可以根据中间共享密钥对流量报文的目的地址进行加密，也就是说，中间共享密钥虽然是由中间路由节点生成的，但是并不是中间路由节点私有的，而是可以与终端设备以及服务器共享的密钥信息。例如，可以根据下述公式计算针对该流量链路的中间共享密钥：

$$Key_share_i = Hash(Info_i||FlowID)$$

其中，Key_share_i 表示第 i 个中间路由节点的中间共享密钥，info_i 表示第 i 个中间路由节点的自身私有信息，FlowID 表示流标识，Hash()表示哈希操作，||表示拼接操作。

根据上述公式可以让流量链路中的每个中间路由节点根据自身私有信息和流标识，计算得到与终端设备以及服务器共享的中间共享密钥。

在中间路由节点根据流标识生成与终端设备和服务器共享的中间共享密钥之后，为了只让终端设备能够根据密钥确认报文获取该中间共享密钥，可以根据终端设备的公钥对中间共享密钥进行加密，得到对应的加密结果，例如，可以通过下述公式得到中间共享密钥对应的加密结果：

$$Enc_share_i = Enc\{Key_pub_client, Key_share_i||IP_router_i\}$$

其中，Enc_share_i 表示第 i 个中间路由节点的中间共享密钥对应的加密结果，Key_pub_client 表示终端设备的公钥，Key_share_i 表示第 i 个中间路由节点的中间共享密钥，IP_router_i 表示第 i 个中间路由节点的 IP 地址，Enc{α,β}表示使用密钥 α 对数据 β 进行加密操作，||表示拼接操作。

根据上述公式，可以让流量链路中每个中间路由节点在生成中间共享密钥之后，通过终端设备的公钥对中间共享密钥得到对应的加密结果，加密结果中每个中间路由节点的中间共享密钥与其 IP 地址一一对应。

在中间路由节点得到中间共享密钥对应的加密结果之后，为了能够让终端设备根据密钥创建报文获取该加密结果，如图 9 所示，图 9 中示例性的将流量链路中的中间路由节点确定为 3 个，以 R1、R2 和 R3 表示，其中，可以将流量链路中每个中间路由节点对应的加密结果（Enc_share_i）都添加到密钥创建报文（Pkt_key）中，图 9 中的“+=”符号表示在密钥创建报文中嵌入中间共享密钥的加密结果，该加密结果可以嵌入至密钥创建报文的头部的“扩展”部分。也可以嵌入至 payload 中，在此不做限定。将该加密结果添加到密钥创建报文中可以让终端设备通过密钥创建报文不仅可以获取共享密钥，还可以获取中间共享密钥。

也就是说，服务器在生成针对流量链路的流标识和共享密钥之后，通过流量链路可以向终端设备发送包括密钥加密数据（包括加密后的共享密钥）和流标识的密钥创建报文，在通过流量链路中的中间路由节点将该密钥创建报文向终端设备转发的过程中，密钥创建报文可以指示中间路由节点根据流标识生成中间共享密钥，并把加密后的中间共享密钥添加至该密钥加密数据中，以便后续步骤中终端设备在获取密钥创建报文之后，可以通过密钥创建报文中的密钥加密数据，获取流量链路中每个中间路由节点对应的中间共享密钥，为后续步骤中服务器根据中间共享密钥来加密流量报文中的目的地址这一步骤打下了基础，提高了报文传输的可靠性和安全性。

在一种可能的实现方式中，在S23中服务器通过流量链路向终端设备发送包括密钥加密数据和流标识的密钥创建报文之后，数据加密方法还包括：

S31、终端设备通过与服务器间的流量链路，接收服务器针对消息请求报文返回的密钥创建报文，密钥创建报文的源地址包括服务器加密地址，密钥创建报文包括通过终端设备的公钥加密得到的密钥加密数据；

S32、终端设备通过终端设备的私钥对密钥加密数据进行解密，得到终端设备与服务器间的共享密钥，以及N个中间共享密钥，这N个中间共享密钥与流量链路中的N个中间路由节点一一对应，N为大于等于1的整数；

S33、终端设备通过共享密钥对N个中间共享密钥进行加密，得到中间密钥加密数据；

S34、终端设备向服务器发送包括中间密钥加密数据的密钥确认报文，密钥确认报文的源地址包括终端加密地址。

终端设备可以通过流量链路，接收服务器发送的密钥创建报文，在获取密钥创建报文之后，需要确定密钥创建报文的源地址，以便对密钥创建报文做出准确响应，由于密钥创建报文中的源地址被隐匿，故可以通过对密钥创建报文中的服务器加密地址进行解密得到服务器的服务器地址。

如前所述，密钥创建报文包括密钥加密数据，密钥加密数据中不仅包括加密后的服务器与终端设备共享的共享密钥，还包括加密后的、流量链路中每个中间路由节点与终端设备以及服务器共享的中间共享密钥。

由于密钥加密数据是通过终端设备的公钥进行加密的，故可以通过终端设备的私钥对该密钥加密数据进行解密，得到终端设备和服务器之间共享的共享密钥，以及与流量链路中每个中间路由节点对应的中间共享密钥，例如，可以通过下述公式得到共享密钥：

$$Key_share = Dec\{Key_pri_client, Enc_share\}$$

其中，Key_share表示共享密钥，Key_pri_client表示终端设备的私钥，Enc_share表示共享密钥对应的密钥加密数据，Dec{α,β}表示使用密钥α对数据β进行解密操作。

也可以通过下述公式得到中间共享密钥：

$$Key_share_i,IP_router_i = Dec\{Key_pri_client, Enc_share_i\}$$

其中，Key_share_i表示第i个中间路由节点的中间共享密钥，IP_router_i表示第i个中间路由节点的IP地址，Key_pri_client表示终端设备的私钥，Enc_share_i表示第i个中间路由节点的中间共享密钥对应的加密结果，Dec{α,β}表示使用密钥α对数据β进行解密操作。

在终端设备获取到流量链路中每个中间路由节点对应的中间共享密钥之后，需要向服务器发送该中间共享密钥，为了仅让服务器可以获取该中间共享密钥，可以通过终端设备和服务器之间的共享密钥，对该N个中间共享密钥进行加密，得到中间密钥加密数据。例如，可以根据下述公式计算中间密钥加密数据：

$$Enc_share_server_i = Enc\{Key_share, Key_share_i||IP_router_i\}$$

其中，Enc_share_server_i表示第i个中间路由节点的中间密钥加密数据，Key_share表示共享密钥，Key_share_i表示第i个中间路由节点的中间共享密钥，IP_router_i表示第

i个中间路由节点的IP地址，Enc{α,β}表示使用密钥α对数据β进行加密操作，||表示拼接操作。

根据上述公式，可以通过共享密钥对中间共享密钥进行加密，得到对应的中间密钥加密数据，中间密钥加密数据中每个中间路由节点的中间共享密钥与其IP地址一一对应。

终端设备可以通过向服务器发送包括中间密钥加密数据的密钥确认报文，让服务器通过获取密钥确认报文，来获取流量链路中每个中间路由节点对应的中间共享密钥，为后续步骤中根据中间共享密钥来对流量报文的目的地址的加密打下了基础。

为了避免密钥确认报文在转发时被攻击者截获之后获得该报文中源地址和目的地址之间的关系，密钥确认报文中的源地址也被隐匿，即密钥确认报文中的源地址也不为终端地址，而是终端加密地址，进而降低了攻击者通过密钥确认报文的源地址和目的地址来推断出用户的隐私的信息的可能性。当密钥确认报文的源地址被隐匿时，为了进一步混淆攻击者且保持报文格式，密钥确认报文的源地址还可以包括终端隐匿地址，如图10所示，密钥确认报文（Pkt_key_ack）中包括终端隐匿地址IP_j、终端加密地址IP_sec和中间密钥加密数据Enc_share_server_i。

需要说明的是，为了保证密钥确认报文能够被准确转发，本实施例中，密钥确认报文的目的地址并未被加密，即密钥确认报文中包括明文的服务器的服务器地址，以便密钥确认报文在网络通信中可以基于服务器地址被准确转发至服务器。

此外，如图10所示，密钥确认报文并不需要基于上述流量链路从终端设备转发至服务器，也就是说，密钥确认报文只需基于服务器地址从终端设备成功转发至服务器即可，并不需要一定根据流量链路中的中间路由节点进行转发。

终端设备在获取了密钥创建报文之后，可以通过密钥创建报文中的密钥加密数据，确定用于传输流量报文的流量链路中的每个中间路由节点对应的中间共享密钥，并通过向服务器发送包括中间密钥加密数据（根据共享密钥加密后的中间共享密钥）的密钥确认报文，使服务器可以获取中间路由节点对应的中间共享密钥，为后续步骤中服务器可以根据中间共享密钥来加密流量报文的目的地址打下了基础，提高了报文传输的可靠性和安全性。

在一种可能的实现方式中，在S34中终端设备向服务器发送包括中间密钥加密数据的密钥确认报文之后，数据加密方法还包括：

S41、服务器接收终端设备响应密钥创建报文返回的密钥确认报文，密钥确认报文的源地址包括终端加密地址，密钥确认报文包括中间密钥加密数据，中间密钥加密数据为通过共享密钥对N个中间共享密钥加密得到的，N个中间共享密钥与N个中间路由节点一一对应；

S42、服务器通过共享密钥对中间密钥加密数据进行解密，得到N个中间共享密钥；

S43、服务器根据N个中间共享密钥和N个中间路由节点的路由地址，得到N个中间路由节点各自对应的加密路由信息，针对N个中间路由节点中的第i个中间路由节点，其对应的加密路由信息是通过第i个中间路由节点对应的中间共享密钥对第i个中间路由节点的路由信息、以及第i个中间路由节点的下一跳节点的路由信息加密得到的；

S44、服务器将加密路由信息添加到流量报文中，流量报文的的目的地址是通过目标

中间共享密钥对终端地址加密得到的，目标中间共享密钥为流量链路中终端设备的上一跳中间路由节点的中间共享密钥。

服务器可以接收终端设备返回的密钥确认报文，服务器在接收密钥确认报文之后，需要确定密钥确认报文的源地址，以便能够确定终端设备已成功获取了密钥创建报文且返回了对应的密钥确认报文，由于密钥确认报文中的源地址被隐匿，故可以通过对密钥确认报文中的终端加密地址进行解密，确定密钥确认报文的真实源地址为终端设备的终端地址。

由于密钥确认报文中包括中间密钥加密数据，如前所述，中间密钥加密数据为终端设备通过共享密钥对流量链路中每个中间路由节点对应的的中间共享密钥进行加密得到的，且共享密钥是终端设备和服务器之间共享的密钥信息，故服务器可以根据共享密钥对中间密钥加密数据进行解密，得到流量链路中每个中间路由节点对应的中间共享密钥，例如，可以通过下述公式得到中间共享密钥：

$$Key_share_i, IP_router_i = Dec\{Key_share, Enc_share_server_i\}$$

其中，Key_share_i 表示第 i 个中间路由节点的中间共享密钥，IP_router_i 表示第 i 个中间路由节点的 IP 地址，Key_share 表示共享密钥，Enc_share_server_i 表示第 i 个中间路由节点的中间密钥加密数据，Dec{α,β}表示使用密钥 α 对数据 β 进行解密操作。

通过上述公式，服务器可以根据共享密钥对中间密钥加密数据进行解密，得到流量链路中每个中间路由节点对应的中间共享密钥。

在服务器获取了流量链路中每个中间路由节点对应的中间共享密钥之后，可以对中间共享密钥进行保存，以便后续在生成基于流量链路传输的流量报文时，可以直接获取已保存的中间共享密钥来对流量链路中的每个中间路由节点进行加密。

服务器在获取了流量链路中每个中间路由节点对应的中间共享密钥之后，为了能够对基于流量链路传输的流量报文的目的地址进行加密，可以基于流量链路中每个中间路由节点的路由信息、下一跳节点的路由信息和对应的中间共享密钥，来为每个中间路由节点确定用于指示其下一跳节点的加密路由信息，从而对流量链路中每个中间路由节点进行加密，其中，终端地址则作为流量链路中终端设备的上一跳中间路由节点的下一跳节点的路由信息，也被对应的目标中间共享密钥进行了加密，目标中间共享密钥是指终端设备的上一跳中间路由节点对应的中间共享密钥。中间路由节点的加密路由信息是指被对应的中间共享密钥加密的、用于指示其下一跳节点的信息数据，例如，可以通过下述公式得到流量链路中每个中间路由节点对应的加密路由信息：

$$Enc_routing_i = Enc\{Key_share_i, IP_router_i||IP_router_i+1\}$$

其中，Enc_routing_i 表示第 i 个中间路由节点的加密路由信息，Key_share_i 表示第 i 个中间路由节点的中间共享密钥，IP_router_i 表示第 i 个中间路由节点的 IP 地址，，IP_router_i+1 表示第 i 个中间路由节点的下一跳节点的 IP 地址，Enc{α,β}表示使用密钥 α 对数据 β 进行加密操作，||表示拼接操作。

根据上述公式，可以通过第 i 个中间路由节点对应的中间共享密钥对第 i 个中间路由节点的下一跳节点的路由信息进行加密，得到对应的加密路由信息。通过加密路由信息可以使得流量链路中的中间路由节点仅能获取下一跳节点的路由信息，减少了攻击者通过劫

持中间路由节点来获取流量报文的目的地址的风险。

当服务器将加密路由信息添加至流量报文中时，流量链路中每个中间路由节点在收到该流量报文后，就可以根据该中间路由节点对应的中间共享密钥对加密路由信息进行解密，得到该中间路由节点的路由信息和对应的下一跳节点的路由信息，例如，可以通过下述公式得到解密后的路由信息：

$$IP_router_i, IP_router_i+1 = Dec\{Key_share_i, Enc_routing_i\}$$

其中，IP_router_i 表示第 i 个中间路由节点的 IP 地址，，IP_router_i+1 表示第 i 个中间路由节点的下一跳节点的 IP 地址，Key_share_i 表示第 i 个中间路由节点的中间共享密钥，Enc_routing_i 表示第 i 个中间路由节点的加密路由信息，Dec{α,β}表示使用密钥 α 对数据 β 进行解密操作。

通过上述公式，可以根据第 i 个中间路由节点的中间共享密钥对加密路由信息进行解密，得到第 i 个中间路由节点的 IP 地址和下一跳节点的 IP 地址。若第 i 个中间路由节点的 IP 地址和自身 IP 地址相符，就可以将流量报文转发至下一跳节点的 IP 地址；若第 i 个中间路由节点的 IP 地址和自身 IP 地址不相符，则可以将该流量报文直接丢弃。也就是说，当中间路由节点根据其对应的中间共享密钥对加密路由信息进行解密之后，会得到某个中间路由节点的路由信息和对应的下一跳节点的路由信息，若该某个中间路由节点的路由信息与该中间路由节点的自身路由信息一致，则该中间路由节点就可以将该流量报文转发至下一跳节点，即通过加密路由信息可以完成流量报文在流量链路上的依次转发。

服务器可以将加密路由信息添加到流量报文中，进而使得该流量报文可以不包括明文的目的地址，而是让流量链路中每个中间路由节点根据其对应的加密路由信息将该流量报文依次转发至下一跳节点处，直至该流量报文被成功转发至终端设备，其中，终端地址就被流量链路中该终端设备的上一跳中间路由节点对应的目标中间共享密钥实现了加密，具体的，终端地址作为终端设备的上一跳中间路由节点的下一跳节点的路由信息，可以通过目标中间共享密钥被加密在该上一跳中间路由节点的加密路由信息中，从而实现了对流量报文中的目的地址的加密。

此外，流量报文中的源地址依然被隐匿，即流量报文中的源地址不为服务器地址，而是服务器加密地址。当流量报文的源地址和目的地址都被隐匿时，为了进一步混淆攻击者且保持报文格式，流量报文的源地址还可以包括服务器隐匿地址，相应的，流量报文的目的地址还可以包括终端隐匿地址，如图 11 所示，流量报文（Pkt_traffic）中可以包括服务器隐匿地址 IP_n、终端隐匿地址 IP_j、服务器加密地址 IP_sec_server 和加密路由信息 Enc_routing_i。

服务器在根据密钥确认报文获取流量链路中每个中间路由节点对应的中间共享密钥之后，可以根据该中间共享密钥，加密流量链路中每个中间路由节点的下一跳路由信息，从而让流量报文在不包括明文的目的地址的情况下，根据加密路由信息被准确转发至终端设备。也就是说，流量报文在对源地址实现了加密的基础上，可以通过加密路由信息对目的地址也实现了加密，使得攻击者在截取了流量报文时，不仅无法获取流量报文的发送端，也无法获取流量报文的接收端，从而进一步降低了流量报文中源地址和目的地址被攻击者

推测出的可能，提高了报文传输的安全性。

相应的，在一种可能的实现方式中，在 S403 中终端设备接收针对消息请求报文返回的流量报文中，数据加密方法具体包括：

终端设备通过流量链路，接收服务器针对消息请求报文返回的流量报文，流量报文的目的地址是通过目标中间共享密钥对终端地址加密得到的，目标中间共享密钥为流量链路中终端设备的上一跳中间路由节点的中间共享密钥。

当服务器将加密路由信息添加至流量报文时，流量链路中的中间路由节点可以对加密路由信息进行解密，从而让流量报文通过流量链路中的中间路由节点依次转发至终端设备。此时，流量报文中并不包括明文的终端地址，而是通过流量链路中目标中间共享密钥（终端设备的上一跳中间路由节点对应的中间共享密钥）对终端地址进行了加密，使得该流量报文的源地址和目的地址均通过被加密在报文中实现了隐匿。

在流量报文的源地址被加密的基础上，还可以通过目标中间共享密钥对目的地址进行加密，此时，流量报文可以根据流量链路中的中间路由节点被依次转发至终端设备，也就是说，流量报文可以在源地址和目的地址均被加密的情况下，实现由服务器至终端设备的成功转发，从而进一步降低了流量报文中的源地址和目的地址被攻击者推测出的可能，提高了报文传输的安全性。

服务器在获取了终端设备发送的密钥确认报文之后，需要根据共享密钥来对密钥确认报文中的中间密钥加密数据进行解密，如果服务器为此一直维护与终端设备共享的共享密钥，这无疑会加大服务器的负担，故在一种可能的实现方式中，在 S42 中根据共享密钥对中间密钥加密数据进行解密之前，服务器可以通过如下方式获取共享密钥：

服务器通过服务器的私钥对终端加密地址进行解密，得到终端地址；

服务器根据终端地址和服务器地址，生成针对流量链路的流标识；

服务器通过终端地址和流标识生成共享密钥。

由于密钥确认报文中包括终端加密地址，故可以根据服务器的私钥对终端加密地址进行解密，得到终端地址。服务器可以根据终端地址和服务器地址，再次生成针对流量链路的流标识，例如，可以根据下述公式来确定流量链路的流标识：

$$FlowID = Hash(IP_m||IP_i||Port_server||Port_client||Protocol)$$

其中，FlowID 表示流标识，IP_m 表示服务器的服务器地址，IP_i 表示终端设备的终端地址，Port_server 表示服务器的服务器端口、Port_client 表示终端设备的终端端口，Protocol 表示服务器和终端设备之间的通信协议，Hash()表示哈希操作，||表示拼接操作。

服务器在确定了流量链路的流标识的基础上，可以根据终端地址和流标识再次确定和终端设备对应的共享密钥，例如，可以根据下述公式计算针对该流量链路的共享密钥：

$$Key_share = Hash(info_server||FlowID)$$

其中，Key_share 表示共享密钥，info_server 表示服务器的自身私有信息，FlowID 表示流标识，Hash()表示哈希操作，||表示拼接操作。

服务器无需一直维护与终端设备共享的共享密钥，当需要根据共享密钥对密钥确认报文中的中间密钥加密数据进行解密时，服务器可以根据终端地址和服务器地址再次生成流

量链路对应的流标识和共享密钥，并通过直接生成的共享密钥，对中间密钥加密数据进行解密，从而降低服务器用于维护共享密钥的成本。

同理，为了避免中间路由节点用于维护中间共享密钥的成本，在一种可能的实现方式中，流量报文还包括流标识，流标识用于指示中间路由节点根据流标识生成对应的中间共享密钥，并通过中间共享密钥对加密路由信息进行解密，得到下一跳节点的路由信息。

当流量报文包括加密路由信息时，中间路由节点需要基于对应的中间共享密钥来对加密路由信息进行解密，以得到下一跳节点的路由信息，而中间路由节点如果为此一直维护中间共享密钥显然会造成一定的成本，故让流量报文中还可以包括流标识，如图 11 所示，流量报文（Pkt_traffic）中还可以包括流标识 FlowID，以便中间路由节点可以根据流标识直接生成对应的中间共享密钥，例如，可以根据下述公式计算中间共享密钥：

$$Key_share_i = Hash(Info_i||FlowID)$$

其中，Key_share_i 表示第 i 个中间路由节点的中间共享密钥，info_i 表示对应的第 i 个中间路由节点的自身私有信息，FlowID 表示流标识，Hash()表示哈希操作，||表示拼接操作。

中间路由节点无需一直维护与终端设备和服务器共享的中间共享密钥，当需要根据中间共享密钥对流量报文中的加密路由信息进行解密时，中间路由节点可以根据流标识再次生成对应的中间共享密钥，以便降低中间路由节点用于维护中间共享密钥的成本。

下面通过一个方法实施例，对本申请中的数据加密方法在实际情况中的具体流程进行说明，如图 12 所示，该数据加密方法的具体流程包括：

S1201、终端设备发送携带终端隐匿地址和终端加密地址的消息请求报文。

终端设备向服务器发送消息请求报文，该消息请求报文可以用于向服务器请求获取目标内容，其中，消息请求报文中不包括明文的终端地址，而是将终端加密地址携带于消息请求报文中，以便通过源地址加密的方式实现对于消息请求报文中源地址的隐匿，并为了进一步混淆攻击者和保持报文格式，消息请求报文还携带有终端隐匿地址。

S1202、服务器发送密钥创建报文。

服务器在获取了消息请求报文之后，为了获取用于传输流量报文的流量链路包括的中间路由节点对应的中间共享密钥，服务器会发送密钥创建报文，其中，密钥创建报文中也不包括明文的服务器地址，而是将服务器加密地址携带于密钥创建报文中，以便通过对源地址加密的方式实现对于密钥创建报文的源地址的隐匿，并为了进一步混淆攻击者和保持报文格式，密钥创建报文还携带有服务器隐匿地址。

同时，密钥创建报文中还携带有服务器和终端设备之间共享的共享密钥和流量链路对应的流标识。

S1203、中间路由节点计算中间共享密钥，并加密后嵌入至密钥创建报文中

中间路由节点在转发密钥创建报文时，会通过自身信息和流标识信息计算得到对应的中间共享密钥，并将计算的中间共享密钥通过目的地址（终端设备）对应的公钥加密后嵌入至密钥创建报文中，以便终端设备可以通过密钥创建报文获取中间共享密钥。

S1204、终端设备解密得到中间共享密钥，并加密后通过密钥确认报文回传至服务器。

终端设备在获取密钥创建报文之后，可以根据自身私钥解密该密钥创建报文中携带的加密后的中间共享密钥信息，并将得到的中间共享密钥通过和服务器共享的共享密钥加密后嵌入至密钥确认报文中，以便将加密后的中间共享密钥可以通过密钥确认报文回传至服务器，其中，密钥确认报文中也不包括明文的终端地址，而是将终端加密地址携带于密钥确认报文中，以便通过对源地址加密的方式实现对于密钥确认报文中源地址的隐匿，并为了进一步混淆攻击者和保持报文格式，密钥确认报文还携带有终端隐匿地址。

S1205、服务器解密得到中间共享密钥，并使用中间共享密钥加密流量链路的路由信息。

服务器在收到密钥确认报文之后，通过与终端设备共享的共享密钥可以解密密钥确认报文中携带的加密后的中间共享密钥信息，获得与流量链路的中间路由节点共享的中间共享密钥，并通过中间共享密钥加密流量链路中的中间路由节点的路由信息，得到对应的加密路由信息，将该加密路由信息添加至流量报文中可以使得流量报文在不包括明文的目的地址的情况下，通过该流量报文携带的加密后中间路由节点每一跳对应的路由信息来完成流量报文的转发，也就是说，流量报文可以通过中间共享密钥实现目的地址的加密，在此基础上，流量报文依然能够对源地址也进行加密，从而对流量报文中源地址和目的地址均实现隐匿。

S1206、中间路由节点计算中间共享密钥，并验证流量报文中的加密路由信息。

中间路由节点在收到流量报文之后，中间路由节点可以根据流标识再次计算中间共享密钥，并使用中间共享密钥来对流量报文中的携带的加密路由信息进行解密，以获取解密后的路由信息和对应的下一跳节点的路由信息。

S1207、中间路由节点验证中间路由节点的自身路由信息与解密后的路由信息是否一致。

中间路由节点在对流量报文携带的加密路由信息进行解密之后，需要验证中间路由节点的自身路由信息与解密后的路由信息是否一致。

S1208a、若中间路由节点的自身路由信息与解密后的路由信息一致，则可以将该流量报文转发至下一跳节点，以实现流量报文在流量链路的依次转发。

S1208b、若中间路由节点的自身路由信息与解密后的路由信息不一致，中间路由节点则可以丢弃该报文。

S1209、终端设备发送流量确认报文至服务器，以便丢包重传。

终端设备在收到流量报文之后，可以向服务器发送流量确认报文，流量确认报文用于让服务器可以获知终端设备的丢包信息，并在终端设备丢包时可以通过再次发送流量报文的方式来对丢包数据进行重传，流量确认报文也不包括明文的终端地址，而是将终端加密地址携带至流量确认报文中，以便通过对源地址加密的方式实现对于流量确认报文中源地址的隐匿，并为了进一步混淆攻击者和保持报文格式，流量确认报文还携带有终端隐匿地址。

如图 13 所示，采用上述数据加密方法，以服务器和终端设备 B 的网络通信为例，可以对服务器和终端设备之间的网络通信进行说明，本申请可以通过加密了源地址的消息请

求报文、加密了源地址的密钥创建报文、加密了源地址的密钥确认报文、加密了源地址和目的地址的流量报文和加密了源地址的流量确认报文，来实现终端设备B和服务器之间的网络通信，并在报文交互过程中，服务器和终端设备之间交互的报文源地址和目的地址之间至少有一个被加密，并且对数量最多的流量报文中的源地址和目的地址均实现了加密，从而降低了攻击者通过源地址和目的地址来获取用户隐私的可能，增强了报文交互的安全性。

在前述图1-13所对应的实施例的基础上，图14为本申请实施例提供的一种数据加密装置的装置结构图，数据加密装置1400包括发送单元1401、获取单元1402、解密单元1403和接收单元1404：

发送单元1401，用于向服务器发送消息请求报文，消息请求报文的源地址包括终端加密地址，终端加密地址是通过服务器的公钥对终端设备的终端地址加密得到的；

获取单元1402，用于接收服务器针对消息请求报文返回的流量报文，流量报文的源地址包括服务器加密地址，服务器加密地址是通过终端设备的公钥对服务器的服务器地址加密得到的；

解密单元1403，用于通过终端设备的私钥对服务器加密地址进行解密，得到服务器待定地址；

接收单元1404，用于响应于服务器待定地址与服务器地址一致，获取流量报文中的流量数据。

在一种可能的实现方式中，消息请求报文的源地址还包括终端隐匿地址，终端隐匿地址为与终端地址不同的虚拟终端地址；流量报文的源地址还包括服务器隐匿地址，服务器隐匿地址为与服务器地址不同的虚拟服务器地址。

在一种可能的实现方式中，发送单元1401还用于：

通过与服务器间的流量链路，接收服务器针对消息请求报文返回的密钥创建报文，密钥创建报文的源地址包括服务器加密地址，密钥创建报文包括通过终端设备的公钥加密得到的密钥加密数据；

通过终端设备的私钥对密钥加密数据进行解密，得到终端设备与服务器间的共享密钥、以及N个中间共享密钥，N个中间共享密钥与流量链路中的N个中间路由节点一一对应，N为大于等于1的整数；

通过共享密钥对N个中间共享密钥进行加密，得到中间密钥加密数据；

向所述服务器发送包括中间密钥加密数据的密钥确认报文，密钥确认报文的源地址包括终端加密地址。

在一种可能的实现方式中，获取单元1402用于通过流量链路，接收服务器针对消息请求报文返回的的流量报文，流量报文的目的地址是通过目标中间共享密钥对终端地址加密得到的，目标中间共享密钥为流量链路中终端设备的上一跳中间路由节点的中间共享密钥。

在一种可能的实现方式中，发送单元1401还用于：

确定针对流量报文的报文接收结果；

向服务器发送包括报文接收结果的流量确认报文，流量确认报文的源地址包括终端加密地址。

在一种可能的实现方式中，获取单元 1402 还用于：

接收服务器获取响应流量确认报文返回的流量重传报文，流量重传报文是根据报文接收结果标识的终端设备未接收到的流量报文，流量重传报文的源地址包括服务器加密地址。

在前述图 1-13 所对应的实施例的基础上，图 15 为本申请实施例提供的另一种数据加密装置的装置结构图，数据加密装置 1500 包括获取单元 1501，解密单元 1502，发送单元 1503；

获取单元 1501，用于接收终端设备发送的消息请求报文，消息请求报文的源地址包括终端加密地址，终端加密地址是通过服务器的公钥对终端设备的终端地址加密得到的；

解密单元 1502，用于通过服务器的私钥对终端加密地址进行解密，得到终端地址；

发送单元 1503，用于根据终端地址，向终端设备发送针对消息请求报文返回的流量报文，流量报文的源地址包括服务器加密地址，服务器加密地址是通过终端设备的公钥对服务器的服务器地址加密得到的。

在一种可能的实现方式中，发送单元 1503 用于：

根据终端地址，确定从服务器到终端设备的流量链路，流量链路包括 N 个中间路由节点，N 为大于等于 1 的整数；

通过流量链路中的 N 个中间路由节点，向所终端设备发送针对消息请求报文返回的流量报文。

在一种可能的实现方式中，发送单元 1503 还用于：

根据终端地址和服务器地址，生成针对流量链路的流标识和共享密钥；

通过终端设备的公钥加密共享密钥，得到密钥加密数据；

通过流量链路，向终端设备发送包括密钥加密数据和流标识的密钥创建报文，密钥创建报文的源地址包括服务器加密地址，密钥创建报文用于指示 N 个中间路由节点根据流标识生成中间共享密钥，通过终端设备的公钥加密中间共享密钥，并将加密结果添加到密钥加密数据中。

在一种可能的实现方式中，获取单元 1501 还用于：

接收终端设备响应密钥创建报文返回的密钥确认报文，密钥确认报文的源地址包括终端加密地址，密钥确认报文包括中间密钥加密数据，中间密钥加密数据为通过共享密钥对 N 个中间共享密钥加密得到的，N 个中间共享密钥与 N 个中间路由节点一一对应；

通过共享密钥对中间密钥加密数据进行解密，得到 N 个中间共享密钥；

根据 N 个中间共享密钥和 N 个中间路由节点的路由地址，得到 N 个中间路由节点各自对应的加密路由信息，针对 N 个中间路由节点中的第 i 个中间路由节点，其对应的加密路由信息是通过第 i 个中间路由节点对应的中间共享密钥对第 i 个中间路由节点的路由信息、以及第 i 个中间路由节点的下一跳节点的路由信息加密得到的；

将加密路由信息添加到流量报文中，流量报文的目的地址是通过目标中间共享密钥对终端地址加密得到的，目标中间共享密钥为流量链路中终端设备的上一跳中间路由节点的

中间共享密钥。

在一种可能的实现方式中，获取单元 1501 还用于：

通过服务器的私钥对终端加密地址进行解密，得到终端地址；

根据终端地址和服务器地址，生成针对流量链路的流标识；

通过终端地址和流标识生成共享密钥。

在一种可能的实现方式中，流量报文还包括流标识，流标识用于指示中间路由节点根据流标识生成对应的中间共享密钥，并通过中间共享密钥对加密路由信息进行解密，得到下一跳节点的路由信息。

在一种可能的实现方式中，发送单元 1503 还用于：接收终端设备发送的包括报文接收结果的流量确认报文，流量确认报文的源地址包括终端加密地址，报文接收结果用于标识终端设备对流量报文的接收状态；

当根据报文接收结果确定终端设备未接收到目标流量报文时，向终端设备发送作为流量重传报文的目标流量报文，流量重传报文的源地址包括服务器加密地址。

在前述图 1-13 所对应的实施例的基础上，图 16 为本申请实施例提供的一种数据加密系统的系统结构图，数据加密系统 1600 包括终端设备 1601 和服务器 1602，终端设备 1601 用于执行前述方法实施例的方法，服务器 1602 用于执行前述方法实施例的方法。

私的信本申请实施例还提供了一种计算机设备，该计算机设备为前述介绍的计算机设备，可以包括终端设备或服务器，前述的数据加密装置可以配置在该计算机设备中。下面结合附图对该计算机设备进行介绍。

若该计算机设备为终端设备，请参见图 17 所示，本申请实施例提供了一种终端设备，以终端设备为手机为例：

图 17 示出的是与本申请实施例提供的终端设备相关的手机的部分结构的框图。参考图 17，手机包括：射频（Radio Frequency，简称 RF）电路 1410、存储器 1420、输入单元 1430、显示单元 1440、传感器 1450、音频电路 1460、无线保真（简称 WiFi）模块 1470、处理器 1480、以及电源 1490 等部件。本领域技术人员可以理解，图 17 中示出的手机结构并不构成对手机的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。

下面结合图 17 对手机的各个构成部件进行具体的介绍：

RF 电路 1410 可用于收发信息或通话过程中，信号的接收和发送，特别地，将基站的下行信息接收后，给处理器 1480 处理；另外，将设计上行的数据发送给基站。

存储器 1420 可用于存储软件程序以及模块，处理器 1480 通过运行存储在存储器 1420 的软件程序以及模块，从而执行手机的各种功能应用以及数据处理。存储器 1420 可主要包括存储程序区和存储数据区，其中，存储程序区可存储操作系统、至少一个功能所需的应用程序（比如声音播放功能、图像播放功能等）等；存储数据区可存储根据手机的使用所创建的数据（比如音频数据、电话本等）等。此外，存储器 1420 可以包括高速随机存取存储器，还可以包括非易失性存储器，例如至少一个磁盘存储器件、闪存器件、或其他易失性固态存储器件。

输入单元 1430 可用于接收输入的数字或字符信息，以及产生与手机的用户设置以及功能控制有关的键信号输入。具体地，输入单元 1430 可包括触控面板 1431 以及其他输入设备 1432。

显示单元 1440 可用于显示由用户输入的信息或提供给用户的信息以及手机的各种菜单。显示单元 1440 可包括显示面板 1441。

手机还可包括至少一种传感器 1450，比如光传感器、运动传感器以及其他传感器。

音频电路 1460、扬声器 1461，传声器 1462 可提供用户与手机之间的音频接口。

WiFi 属于短距离无线传输技术，手机通过 WiFi 模块 1470 可以帮助用户收发电子邮件、浏览网页和访问流式媒体等，它为用户提供了无线的宽带互联网访问。

处理器 1480 是手机的控制中心，利用各种接口和线路连接整个手机的各个部分，通过运行或执行存储在存储器 1420 内的软件程序和/或模块，以及调用存储在存储器 1420 内的数据，执行手机的各种功能和处理数据。

手机还包括给各个部件供电的电源 1490（比如电池）。

在本实施例中，该终端设备所包括的处理器 1480 还用于执行本申请实施例提供的终端设备侧的数据加密方法。

若计算机设备为服务器，本申请实施例还提供一种服务器，请参见图 18 所示，图 18 为本申请实施例提供的服务器 1500 的结构图，服务器 1500 可因配置或性能不同而产生比较大的差异，可以包括一个或一个以上中央处理器（Central Processing Units，简称 CPU）1522（例如，一个或一个以上处理器）和存储器 1532，一个或一个以上存储应用程序 1542 或数据 1544 的存储介质 1530（例如一个或一个以上海量存储设备）。其中，存储器 1532 和存储介质 1530 可以是短暂存储或持久存储。存储在存储介质 1530 的程序可以包括一个或一个以上模块（图示没标出），每个模块可以包括对服务器中的一系列指令操作。更进一步地，中央处理器 1522 可以设置为与存储介质 1530 通信，在服务器 1500 上执行存储介质 1530 中的一系列指令操作。

服务器 1500 还可以包括一个或一个以上电源 1526，一个或一个以上有线或无线网络接口 1550，一个或一个以上输入输出接口 1558，和/或，一个或一个以上操作系统 1541，例如 Windows Server™，Mac OS X™，Unix™, Linux™，FreeBSD™ 等等。

上述实施例中由服务器所执行的步骤可以基于图 18 所示的服务器结构。

另外，本申请实施例还提供了一种存储介质，所述存储介质用于存储计算机程序，所述计算机程序用于执行上述实施例提供的方法。

本申请实施例还提供了一种包括指令的计算机程序产品，当其在计算机上运行时，使得计算机执行上述实施例提供的方法。

本领域普通技术人员可以理解：实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成，前述程序可以存储于一计算机可读取存储介质中，该程序在执行时，执行包括上述方法实施例的步骤；而前述的存储介质可以是下述介质中的至少一种：只读存储器（英文：Read-only Memory，缩写：ROM）、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

需要说明的是，本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于设备及系统实施例而言，由于其基本相似于方法实施例，所以描述得比较简单，相关之处参见方法实施例的部分说明即可。以上所描述的设备及系统实施例仅仅是示意性的，其中作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

以上所述，仅为本申请的一种具体实施方式，但本申请的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本申请揭露的技术范围内，可轻易想到的变化或替换，都应涵盖在本申请的保护范围之内。而且本申请在上述各方面提供的实现方式的基础上，还可以进行进一步组合以提供更多实现方式。因此，本申请的保护范围应该以权利要求的保护范围为准。

权利要求

1、一种数据加密方法，所述方法由终端设备执行，所述方法包括：

向服务器发送消息请求报文，所述消息请求报文的源地址包括终端加密地址，所述终端加密地址是通过所述服务器的公钥对所述终端设备的终端地址加密得到的；

接收所述服务器针对所述消息请求报文返回的流量报文，所述流量报文的源地址包括服务器加密地址，所述服务器加密地址是通过所述终端设备的公钥对所述服务器的服务器地址加密得到的；

通过所述终端设备的私钥对所述服务器加密地址进行解密，得到服务器待定地址；

响应于所述服务器待定地址与所述服务器地址一致，获取所述流量报文中的流量数据。

2、根据权利要求 1 所述的方法，所述消息请求报文的源地址还包括终端隐匿地址，所述终端隐匿地址为与所述终端地址不同的虚拟终端地址；所述流量报文的源地址还包括服务器隐匿地址，所述服务器隐匿地址为与所述服务器地址不同的虚拟服务器地址。

3、根据权利要求 1 或 2 所述的方法，所述方法还包括：

通过与所述服务器间的流量链路，接收所述服务器针对所述消息请求报文返回的密钥创建报文，所述密钥创建报文的源地址包括所述服务器加密地址，所述密钥创建报文包括通过所述终端设备的公钥加密得到的密钥加密数据；

通过所述终端设备的私钥对所述密钥加密数据进行解密，得到所述终端设备与所述服务器间的共享密钥以及 N 个中间共享密钥，所述 N 个中间共享密钥与所述流量链路中的 N 个中间路由节点一一对应，所述 N 为大于等于 1 的整数；

通过所述共享密钥对所述 N 个中间共享密钥进行加密，得到中间密钥加密数据；

向所述服务器发送包括所述中间密钥加密数据的密钥确认报文，所述密钥确认报文的源地址包括所述终端加密地址。

4、根据权利要求 3 所述的方法，所述接收所述服务器针对所述消息请求报文返回的流量报文，包括：

通过所述流量链路，接收所述服务器针对所述消息请求报文返回的所述流量报文，所述流量报文的目的地址是通过目标中间共享密钥对所述终端地址加密得到的，所述目标中间共享密钥为所述流量链路中所述终端设备的上一跳中间路由节点对应的中间共享密钥。

5、根据权利要求 1 至 4 任一项所述的方法，所述方法还包括：

确定针对所述流量报文的报文接收结果；

向所述服务器发送包括所述报文接收结果的流量确认报文，所述流量确认报文的源地址包括所述终端加密地址。

6、根据权利要求 5 所述的方法，所述方法还包括：

接收所述服务器获取响应所述流量确认报文返回的流量重传报文，所述流量重传报文是所述报文接收结果标识的所述终端设备未接收到的流量报文，所述流量重传报文的源地址包括所述服务器加密地址。

7、一种数据加密方法，所述方法由服务器执行，所述方法包括：

接收终端设备发送的消息请求报文，所述消息请求报文的源地址包括终端加密地址，

所述终端加密地址是通过所述服务器的公钥对所述终端设备的终端地址加密得到的；

通过所述服务器的私钥对所述终端加密地址进行解密，得到所述终端地址；

根据所述终端地址，向所述终端设备发送针对所述消息请求报文返回的流量报文，所述流量报文的源地址包括服务器加密地址，所述服务器加密地址是通过所述终端设备的公钥对所述服务器的服务器地址加密得到的。

8、根据权利要求 7 所述的方法，所述根据所述终端地址，向所述终端设备发送针对所述消息请求报文返回的流量报文，包括：

根据所述终端地址，确定从所述服务器到所述终端设备的流量链路，所述流量链路包括 N 个中间路由节点，所述 N 为大于等于 1 的整数；

通过所述流量链路中的所述 N 个中间路由节点，向所述终端设备发送所述流量报文。

9、根据权利要求 8 所述的方法，所述方法还包括：

根据所述终端地址和所述服务器地址，生成针对所述流量链路的流标识和共享密钥；

通过所述终端设备的公钥加密所述共享密钥，得到密钥加密数据；

通过所述流量链路，向所述终端设备发送包括所述密钥加密数据和所述流标识的密钥创建报文，所述密钥创建报文的源地址包括所述服务器加密地址，所述密钥创建报文用于指示所述 N 个中间路由节点根据所述流标识生成中间共享密钥，并通过所述终端设备的公钥加密所述中间共享密钥，并将加密结果添加到所述密钥加密数据中。

10、根据权利要求 9 所述的方法，所述方法还包括：

接收所述终端设备响应所述密钥创建报文返回的密钥确认报文，所述密钥确认报文的源地址包括所述终端加密地址，所述密钥确认报文包括中间密钥加密数据，所述中间密钥加密数据为通过所述共享密钥对 N 个中间共享密钥加密得到的，所述 N 个中间共享密钥与所述 N 个中间路由节点一一对应；

通过所述共享密钥对所述中间密钥加密数据进行解密，得到所述 N 个中间共享密钥；

根据所述 N 个中间共享密钥和所述 N 个中间路由节点的路由地址，得到所述 N 个中间路由节点各自对应的加密路由信息，针对所述 N 个中间路由节点中的第 i 个中间路由节点，其对应的加密路由信息是通过所述第 i 个中间路由节点对应的中间共享密钥，对所述第 i 个中间路由节点的路由信息、以及第 i 个中间路由节点的下一跳节点的路由信息加密得到的；

将所述加密路由信息添加到所述流量报文中，所述流量报文的目的地址是通过目标中间共享密钥对所述终端地址加密得到的，所述目标中间共享密钥为所述流量链路中所述终端设备的上一跳中间路由节点的中间共享密钥。

11、根据权利要求 10 所述的方法，在所述通过所述共享密钥对所述中间密钥加密数据进行解密，得到所述 N 个中间共享密钥之前，所述方法还包括：

通过所述服务器的私钥对所述终端加密地址进行解密，得到所述终端地址；

根据所述终端地址和所述服务器地址，生成针对所述流量链路的流标识；

通过所述终端地址和所述流标识生成所述共享密钥。

12、根据权利要求 9 至 11 任一项所述的方法，所述流量报文还包括流标识，所述流

标识用于指示所述中间路由节点根据所述流标识生成对应的中间共享密钥，并通过所述中间共享密钥对所述加密路由信息进行解密，得到下一跳节点的路由信息。

13、根据权利要求 7 至 12 任一项所述的方法，所述方法还包括：

接收所述终端设备发送的包括报文接收结果的流量确认报文，所述流量确认报文的源地址包括所述终端加密地址，所述报文接收结果用于标识所述终端设备对所述流量报文的接收状态；

当根据所述报文接收结果确定所述终端设备未接收到目标流量报文时，向所述终端设备发送作为流量重传报文的所述目标流量报文，所述流量重传报文的源地址包括所述服务器加密地址。

14、一种数据加密装置，所述装置包括发送单元，获取单元，解密单元和接收单元；

所述发送单元，用于向服务器发送消息请求报文，所述消息请求报文的源地址包括终端加密地址，所述终端加密地址是通过所述服务器的公钥对所述终端设备的终端地址加密得到的；

所述获取单元，用于接收所述服务器针对所述消息请求报文返回的流量报文，所述流量报文的源地址包括服务器加密地址，所述服务器加密地址是通过所述终端设备的公钥对所述服务器的服务器地址加密得到的；

所述解密单元，用于通过所述终端设备的私钥对所述服务器加密地址进行解密，得到服务器待定地址；

所述接收单元，用于响应于所述服务器待定地址与所述服务器地址一致，获取所述流量报文中的流量数据。

15、一种数据加密装置，所述装置包括获取单元，解密单元，发送单元；

所述获取单元，用于接收终端设备发送的消息请求报文，所述消息请求报文的源地址包括终端加密地址，所述终端加密地址是通过所述服务器的公钥对所述终端设备的终端地址加密得到的；

所述解密单元，用于通过所述服务器的私钥对所述终端加密地址进行解密，得到所述终端地址；

所述发送单元，用于根据所述终端地址，向所述终端设备发送针对所述消息请求报文返回的流量报文，所述流量报文的源地址包括服务器加密地址，所述服务器加密地址是通过所述终端设备的公钥对所述服务器的服务器地址加密得到的。

16、一种数据加密系统，所述系统包括终端设备和服务器，所述终端设备用于执行权利要求 1-6 中任意一项所述的方法，所述服务器用于执行权利要求 7-13 中任意一项所述的方法。

17、一种计算机设备，所述计算机设备包括处理器以及存储器：

所述存储器用于存储计算机程序，并将所述程序代码传输给所述处理器；

所述处理器用于根据所述计算机程序中的指令执行权利要求 1-6 中任意一项所述的方法，或者，执行权利要求 7-13 中任意一项所述的方法。

18、一种计算机可读存储介质，所述计算机可读存储介质用于存储计算机程序，所述

计算机程序用于执行权利要求 1-6 中任意一项所述的方法，或者，执行权利要求 7-13 中任意一项所述的方法。

19、一种包括计算机程序的计算机程序产品，当其在计算机设备上运行时，使得所述计算机设备执行权利要求 1-6 中任意一项所述的方法，或者，执行权利要求 7-13 中任意一项所述的方法。

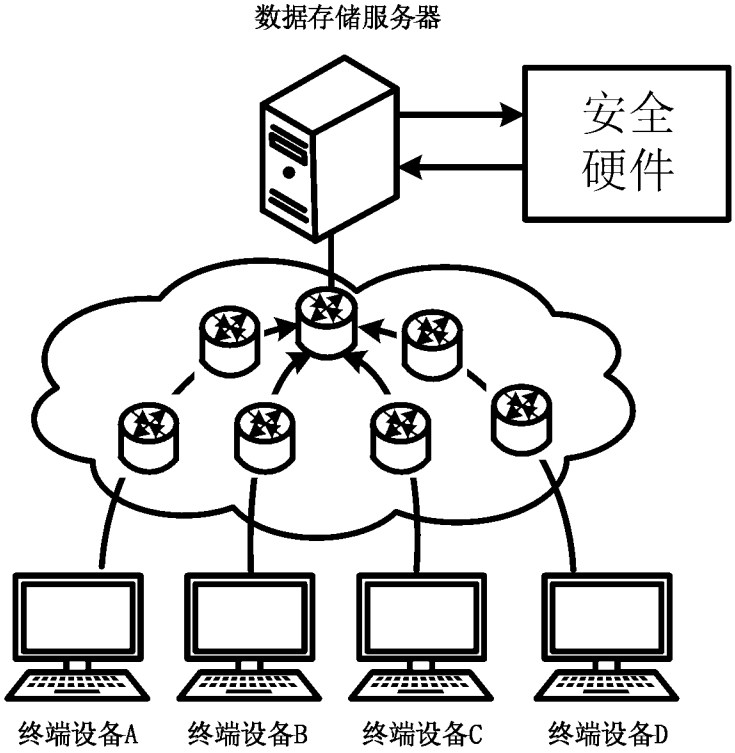
数据存储服务器
安全
硬件
终端设备A
终端设备B
终端设备C
终端设备D

图 1

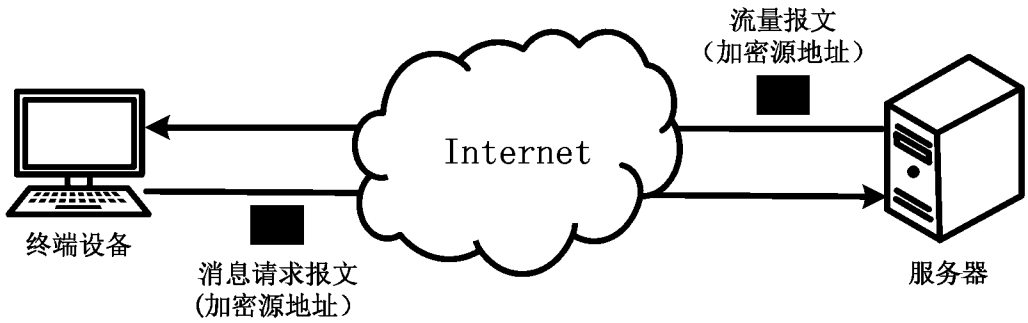
流量报文
（加密源地址）
Internet
终端设备
消息请求报文
（加密源地址）
服务器

图 2

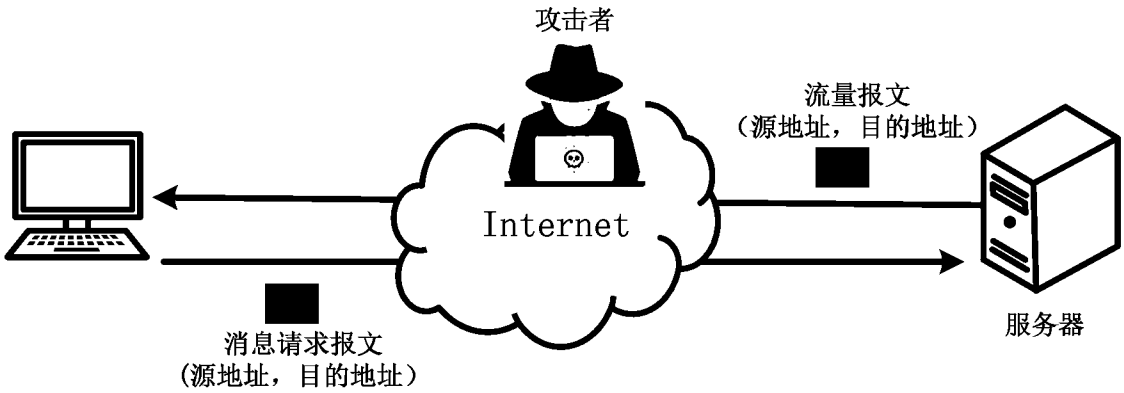

图 3

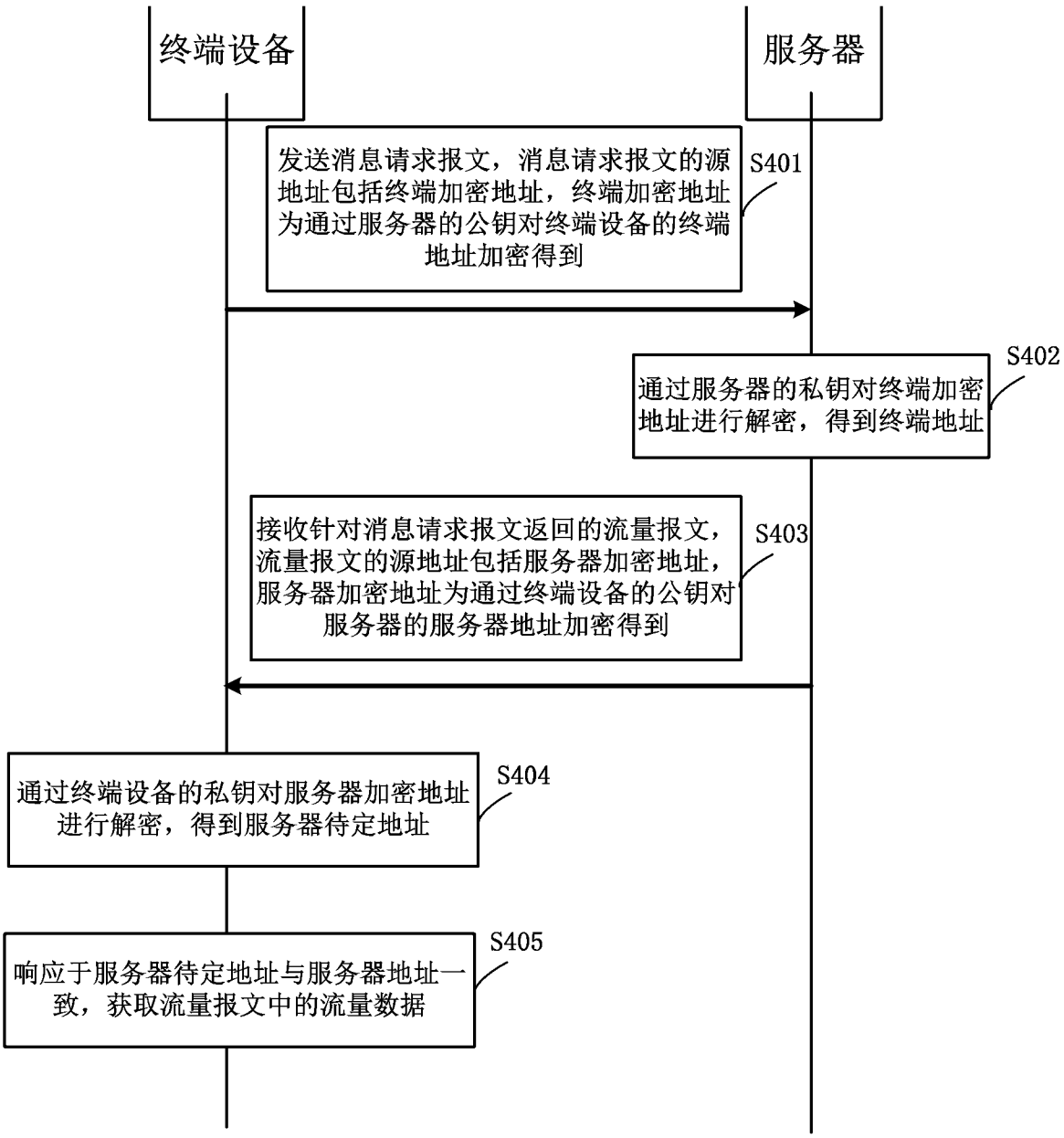
终端设备
服务器
发送消息请求报文，消息请求报文的源地址包括终端加密地址，终端加密地址为通过服务器的公钥对终端设备的终端地址加密得到
S401
通过服务器的私钥对终端加密地址进行解密，得到终端地址
S402
接收针对消息请求报文返回的流量报文，流量报文的源地址包括服务器加密地址，服务器加密地址为通过终端设备的公钥对服务器的服务器地址加密得到
S403
通过终端设备的私钥对服务器加密地址进行解密，得到服务器待定地址
S404
响应于服务器待定地址与服务器地址一致，获取流量报文中的流量数据
S405

图 4

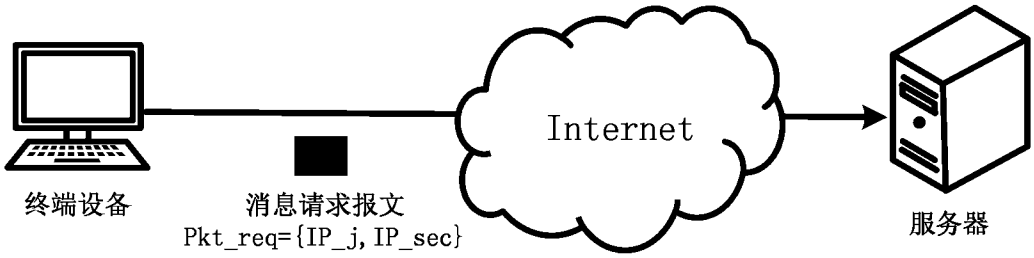
Internet
终端设备
消息请求报文
Pkt_req={IP_j, IP_sec}
服务器

图 5

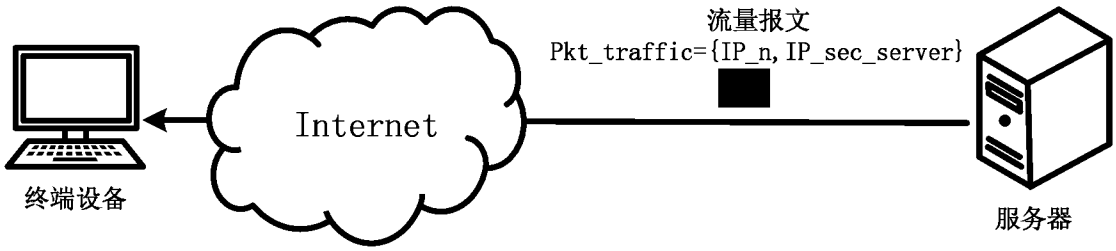
流量报文
Pkt_traffic={IP_n, IP_sec_server}
Internet
终端设备
服务器

图 6

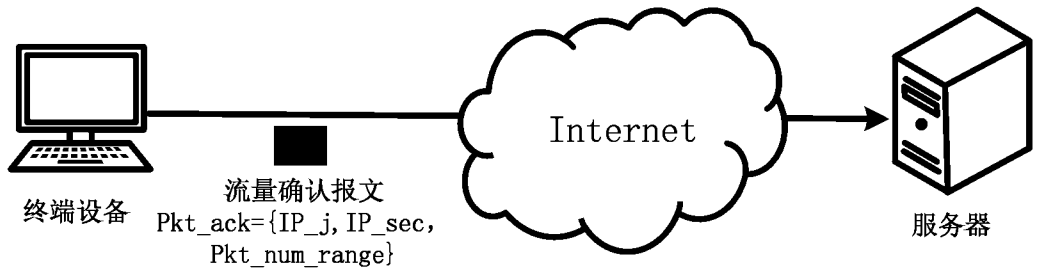
Internet
终端设备
流量确认报文
Pkt_ack={IP_j, IP_sec,
Pkt_num_range}
服务器

图 7

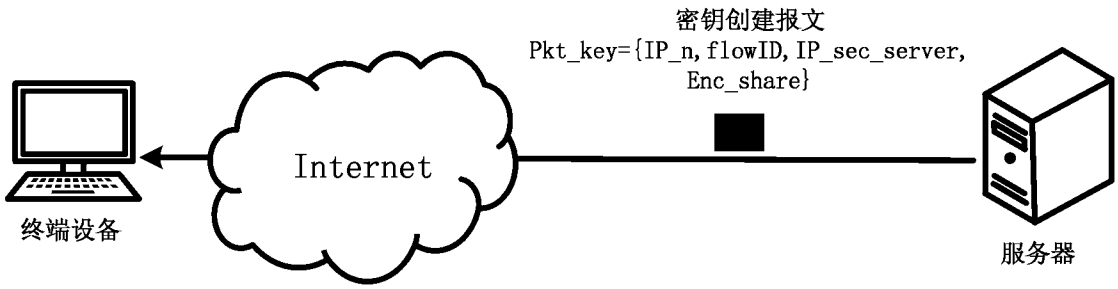
密钥创建报文
Pkt_key={IP_n, flowID, IP_sec_server,
Enc_share}
Internet
终端设备
服务器

图 8

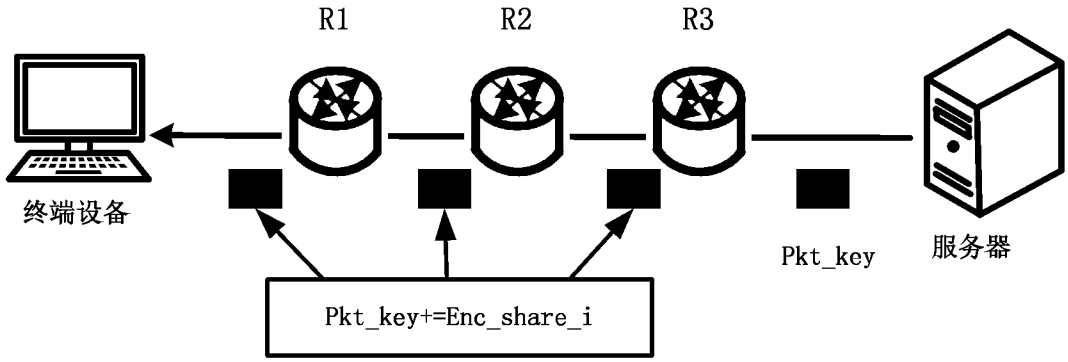
R1
R2
R3
终端设备
Pkt_key
服务器
Pkt_key+=Enc_share_i

图 9

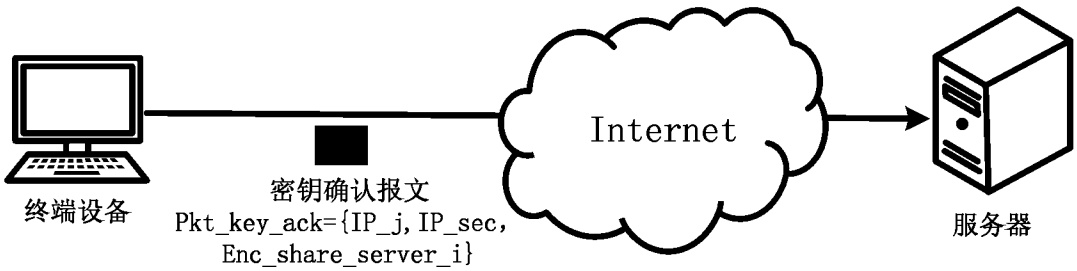
Internet
终端设备
密钥确认报文
Pkt_key_ack={IP_j, IP_sec,
Enc_share_server_i}
服务器

图 10

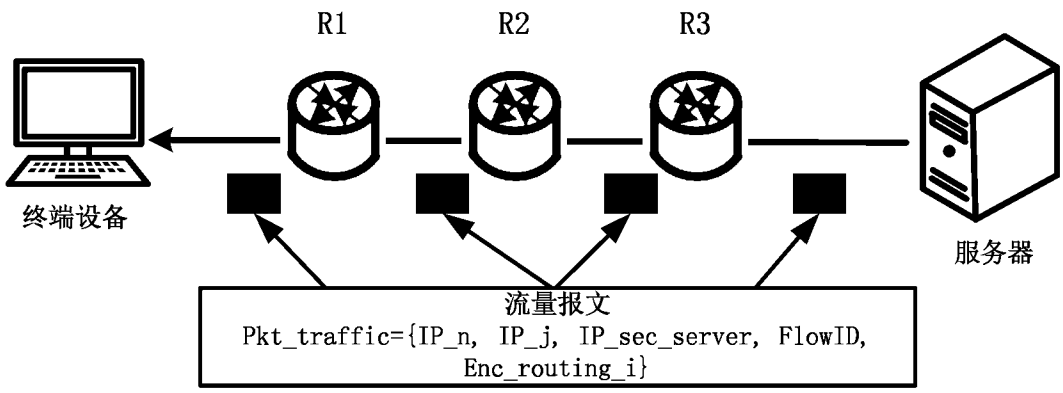
R1
R2
R3
终端设备
服务器
流量报文
Pkt_traffic={IP_n, IP_j, IP_sec_server, FlowID,
Enc_routing_i}

图 11

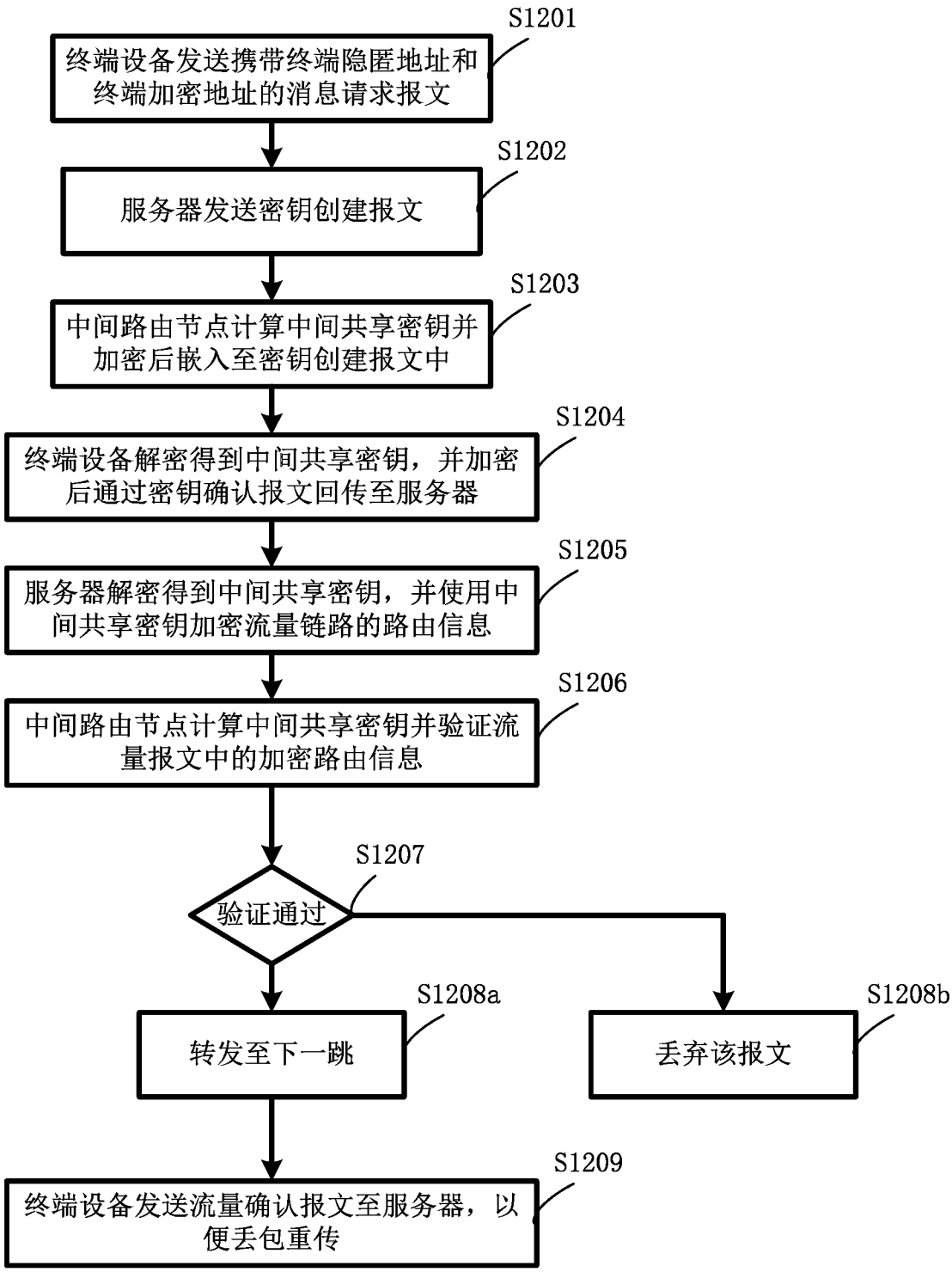
S1201
终端设备发送携带终端隐匿地址和终端加密地址的消息请求报文
S1202
服务器发送密钥创建报文
S1203
中间路由节点计算中间共享密钥并加密后嵌入至密钥创建报文中
S1204
终端设备解密得到中间共享密钥，并加密后通过密钥确认报文回传至服务器
S1205
服务器解密得到中间共享密钥，并使用中间共享密钥加密流量链路的路由信息
S1206
中间路由节点计算中间共享密钥并验证流量报文中的加密路由信息
S1207
验证通过
S1208a
转发至下一跳
S1208b
丢弃该报文
S1209
终端设备发送流量确认报文至服务器，以便丢包重传

图 12

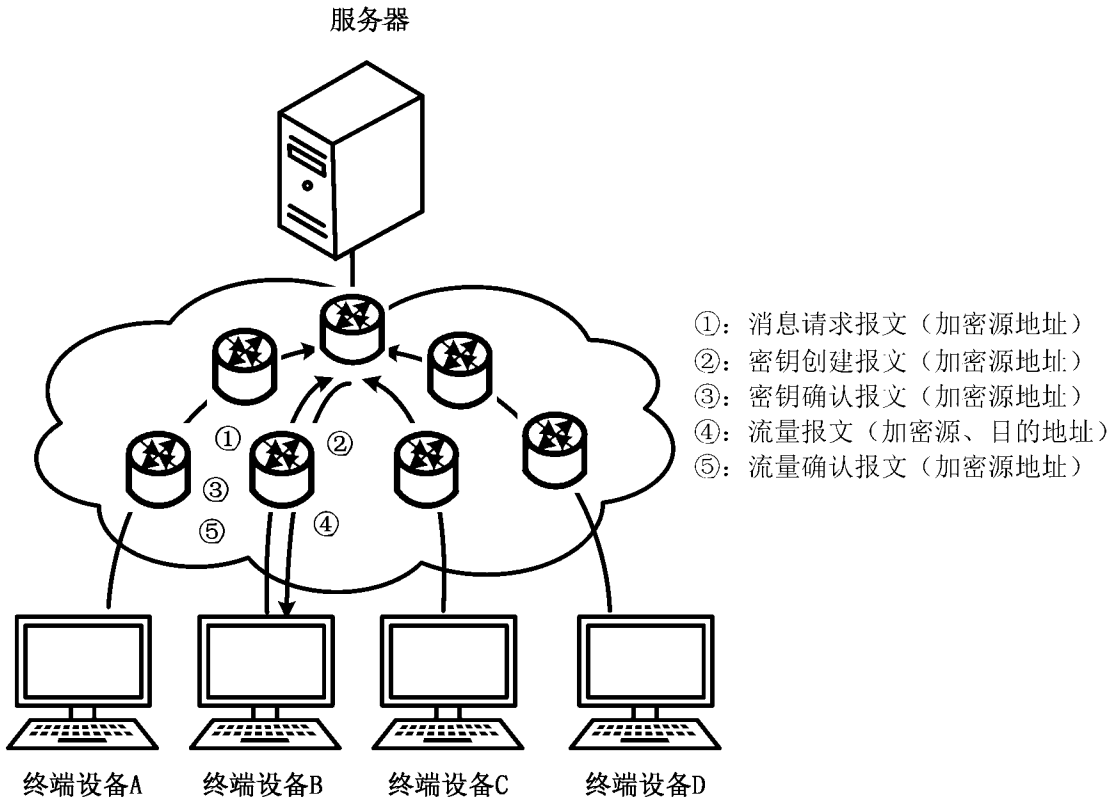
服务器
①：消息请求报文（加密源地址）
②：密钥创建报文（加密源地址）
③：密钥确认报文（加密源地址）
④：流量报文（加密源、目的地址）
⑤：流量确认报文（加密源地址）
①
②
③
④
⑤
终端设备A
终端设备B
终端设备C
终端设备D

图 13

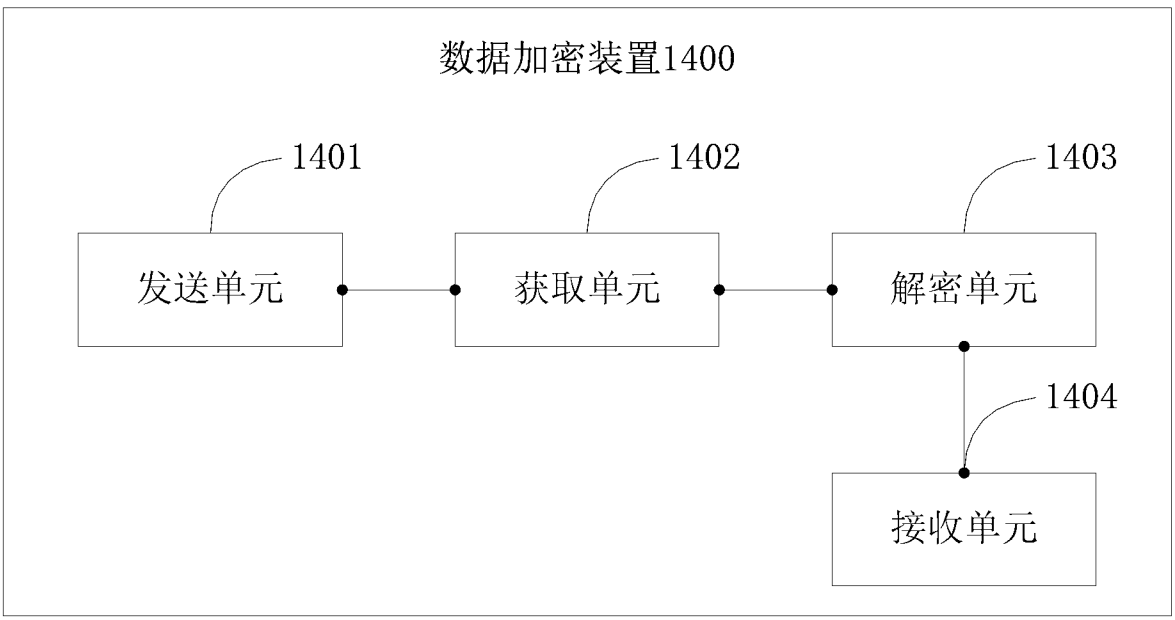
数据加密装置1400
1401
1402
1403
发送单元
获取单元
解密单元
1404
接收单元

图 14

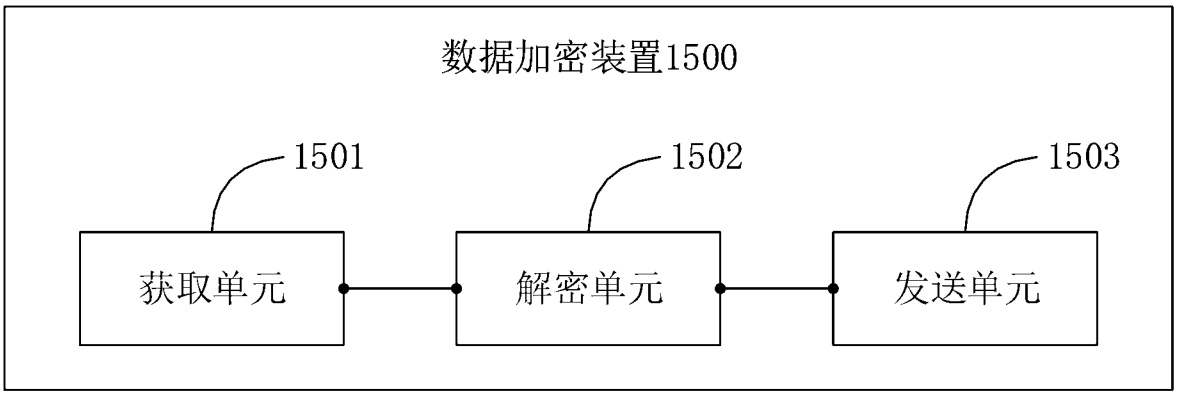
数据加密装置1500
1501
1502
1503
获取单元
解密单元
发送单元

图 15

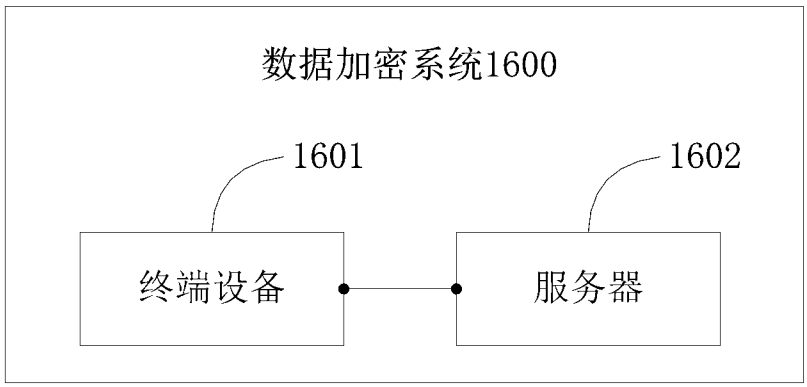
数据加密系统1600
1601
1602
终端设备
服务器

图 16

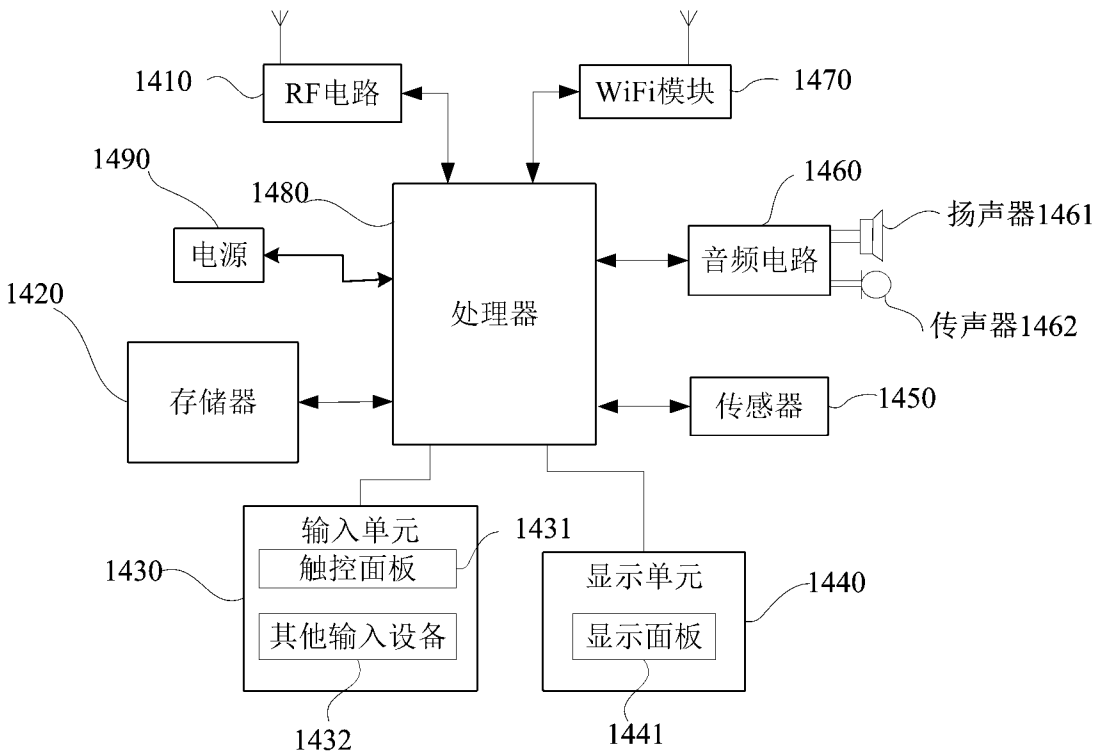
1410
RF电路
WiFi模块
1470
1490
1480
1460
扬声器1461
电源
音频电路
1420
处理器
传声器1462
存储器
传感器
1450
输入单元
1431
1430
触控面板
显示单元
1440
其他输入设备
显示面板
1432
1441

图 17

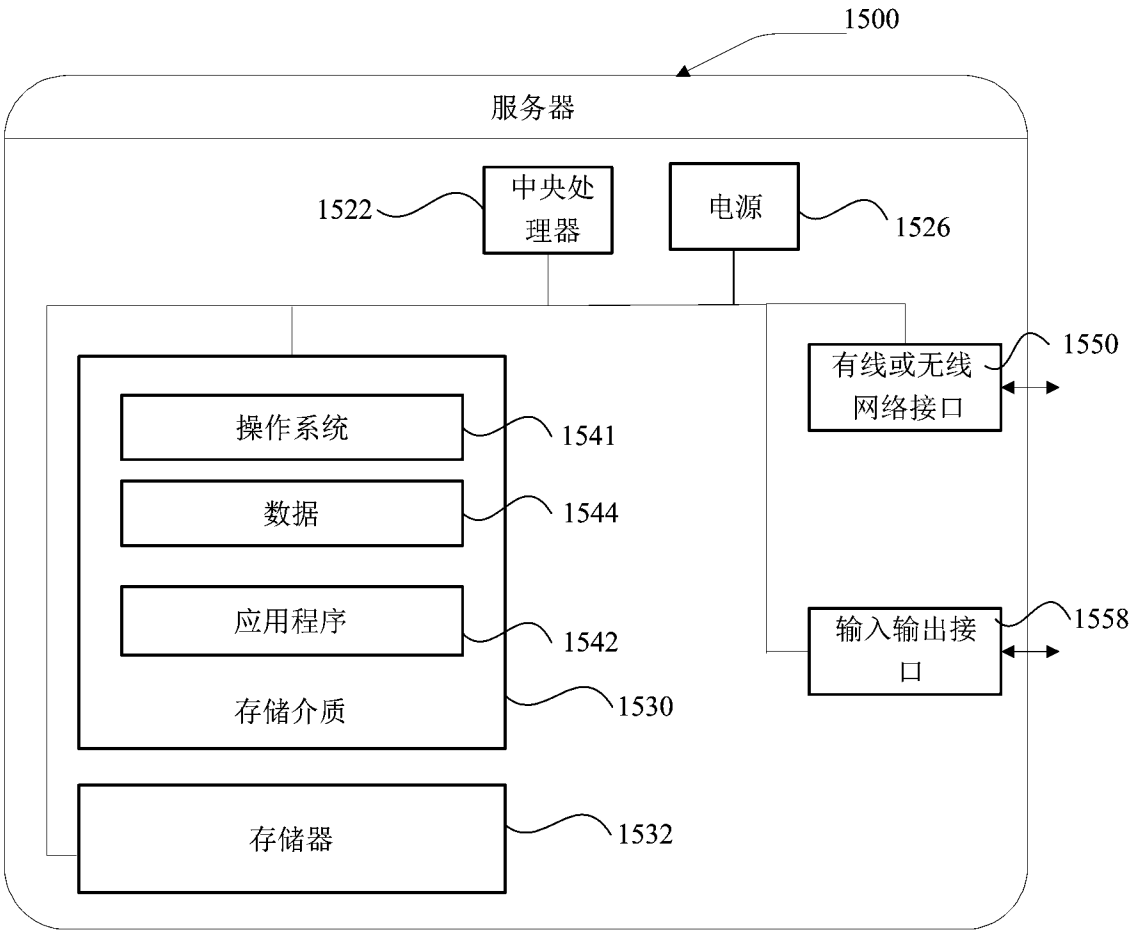
1500
服务器
1522
中央处理器
电源
1526
有线或无线网络接口
1550
操作系统
1541
数据
1544
应用程序
1542
存储介质
1530
输入输出接口
1558
存储器
1532

图 18

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2023/131400

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/40(2022.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L

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

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

3GPP, CNTXT, ENTXT, ENTXTC, WPABS, DWPI, VCN, CNKI: 加密, 报文, 地址, 源, 目的, 隐藏, 隐匿, 伪装, 公钥, 私钥, 共享, 中间, 路由, encryption, packet, address, source, destination, hide, public key, private key, shared, intermediate, route

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 110493367 A (TSINGHUA UNIVERSITY) 22 November 2019 (2019-11-22) description, paragraphs 30-55	1-2, 5-8, 13-19
X	CN 114915583 A (ZTE CORP.) 16 August 2022 (2022-08-16) description, paragraphs 50-69	1-2, 5-8, 13-19
A	CN 105978798 A (ZICT TECHNOLOGY CO., LTD.) 28 September 2016 (2016-09-28) entire document	1-19
A	CN 109462594 A (VISIONVERA INFORMATION TECHNOLOGY CO., LTD.) 12 March 2019 (2019-03-12) entire document	1-19
A	US 2011264908 A1 (CHENGDU HUAWEI SYMANTEC TECHNOLOGIES CO., LTD.) 27 October 2011 (2011-10-27) entire document	1-19

☐ 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
19 January 2024	**24 January 2024**

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

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2023/131400

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 110493367 A	22 November 2019	None	
CN 114915583 A	16 August 2022	WO 2022166979 A1	11 August 2022
CN 105978798 A	28 September 2016	None	
CN 109462594 A	12 March 2019	None	
US 2011264908 A1	27 October 2011	US 8499146 B2	30 July 2013
		EP 2346205 A1	20 July 2011
		EP 2346205 A4	21 March 2012
		EP 2346205 B1	12 June 2013
		WO 2010048865 A1	06 May 2010
		CN 101404579 A	08 April 2009

国际检索报告

国际申请号
PCT/CN2023/131400

A. 主题的分类

H04L 9/40(2022.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC: H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

3GPP, CNTXT, ENTXT, ENTXTC, WPABS, DWPI, VCN, CNKI: 加密，报文，地址，源，目的，隐藏，隐匿，伪装，公钥，私钥，共享，中间，路由，encryption, packet, address, source, destination, hide, public key, private key, shared, intermediate, route

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 110493367 A (清华大学) 2019年11月22日 (2019 - 11 - 22) 说明书第30−55段	1−2、5−8、13−19
X	CN 114915583 A (中兴通讯股份有限公司) 2022年8月16日 (2022 - 08 - 16) 说明书第50−69段	1−2、5−8、13−19
A	CN 105978798 A (深圳中兴网信科技有限公司) 2016年9月28日 (2016 - 09 - 28) 全文	1−19
A	CN 109462594 A (视联动力信息技术股份有限公司) 2019年3月12日 (2019 - 03 - 12) 全文	1−19
A	US 2011264908 A1 (CHENGDU HUAWEI SYMANTEC TECHNOLOGIES CO., LTD.) 2011年10月27日 (2011 - 10 - 27) 全文	1−19

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“D” 申请人在国际申请中引证的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

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

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

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

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

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

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2024年1月19日	2024年1月24日
ISA/CN的名称和邮寄地址 中国国家知识产权局 中国北京市海淀区蓟门桥西土城路6号 100088	受权官员 张德珍 电话号码 (+86) 010−53961658

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2023/131400

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	110493367	A	2019年11月22日	无			
CN	114915583	A	2022年8月16日	WO	2022166979	A1	2022年8月11日
CN	105978798	A	2016年9月28日	无			
CN	109462594	A	2019年3月12日	无			
US	2011264908	A1	2011年10月27日	US	8499146	B2	2013年7月30日
				EP	2346205	A1	2011年7月20日
				EP	2346205	A4	2012年3月21日
				EP	2346205	B1	2013年6月12日
				WO	2010048865	A1	2010年5月6日
				CN	101404579	A	2009年4月8日