(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
2016 年 10 月 6 日 (06.10.2016)

WIPO | PCT

(10) 国际公布号
WO 2016/155495 A1

(51) 国际专利分类号:
H04L 12/70 (2013.01)

(21) 国际申请号: PCT/CN2016/076413

(22) 国际申请日: 2016 年 3 月 15 日 (15.03.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201510155553.9 2015 年 4 月 2 日 (02.04.2015) CN

(71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 英属开曼群岛大开曼乔治城资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。

(72) 发明人; 及

(71) 申请人 (仅对美国): 代军 (DAI, Jun) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北京国昊天诚知识产权代理有限公司 (CO-HORIZON INTELLECTUAL PROPERTY INC.); 中国北京市朝阳区小关北里甲 2 号渔阳置业大厦 B 座 605, 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, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

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

[见续页]

(54) Title: DATA EXCHANGE METHOD, APPARATUS AND DEVICE

(54) 发明名称 : 数据交换方法、装置及设备

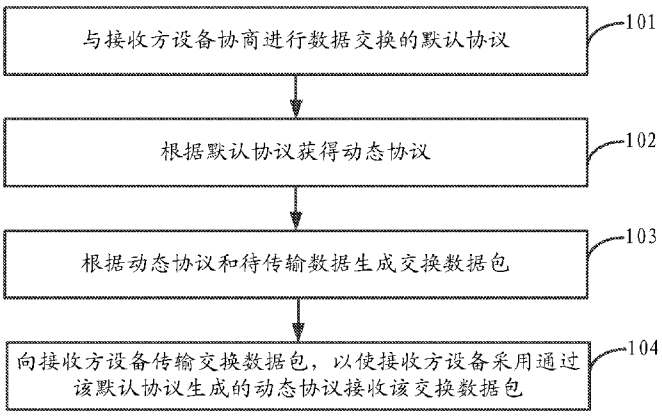

图 1

101 NEGOTIATING WITH A RECEIVER DEVICE FOR A DEFAULT PROTOCOL OF DATA EXCHANGE
102 OBTAINING A DYNAMIC PROTOCOL ACCORDING TO THE DEFAULT PROTOCOL
103 GENERATING AN EXCHANGE DATA PACKET ACCORDING TO THE DYNAMIC PROTOCOL AND DATA TO BE TRANSMITTED
104 TRANSMITTING THE EXCHANGE DATA PACKET TO THE RECEIVER DEVICE, SUCH THAT THE RECEIVER DEVICE RECEIVES THE EXCHANGE DATA PACKET USING THE DYNAMIC PROTOCOL GENERATED VIA THE DEFAULT PROTOCOL

(57) Abstract: Disclosed are a data exchange method, apparatus and device. The method is applied to a sender device exchanging data with a receiver device, and the method comprises: negotiating with a receiver device for a default protocol of data exchange; obtaining a dynamic protocol according to the default protocol; generating an exchange data packet according to the dynamic protocol and data to be transmitted; and transmitting the exchange data packet to the receiver device, such that the receiver device receives the exchange data packet using the dynamic protocol generated via the default protocol. By applying the embodiments of the present invention, a dynamic protocol is generated by means of a default protocol obtained by negotiation between a sender and a receiver, and data exchange is performed based on the dynamic protocol. Since the dynamic protocol can be dynamically generated when data exchange is required, a communication process of data exchange can be effectively prevented from being stolen by a malicious third party, such that the security of data exchange can be improved.

(57) 摘要: 本申请公开了数据交换方法、装置及设备，所述方法应用在与接收方设备进行数据交换的发送方设备上，所述方法包括：与所述接收方设备协商进行所述数据交换的默认协议；根据所述默认协议获得动态协议；根据所述动态协议和待传输数据生成交换数据包；向所述接收方设备传输所述交换数据包，以使所述接收方设备采用通过所述默认协议生成的动态协议接收所述交换数据包。应用本申请实施例，发送方和接收方之间通过协商的默认协议生成动态协议，并基于该动态协议进行数据交换，由于动态协议可以在有数据交换需求时动态生成，因此可以有效避免恶意第三方对数据交换的通信过程进行窃取，从而能够提高数据交换的安全性。

WO 2016/155495 A1

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

数据交换方法、装置及设备

技术领域

本申请涉及网络通信技术领域，尤其涉及数据交换方法、装置及设备。

背景技术

随着大数据时代的来临，在基于互联网开展各种业务时，可能会涉及不同领域，或者不同业务间的海量数据交换。现有技术中，对应不同业务的交换设备之间可以基于 FTP（File Transfer Protocol，文件传输协议）进行数据交换。在基于 FTP 进行数据交换时，通常由数据发送方设置账号和密码，并将账号和密码共享给数据接收方，当数据发送方将交换数据上传到 FTP 服务器后，数据接收方可以根据获得的账号和密码从 FTP 服务器上请求到交换数据。但是，由于数据发送方和数据接收方之间直接共享由其中一方设置的账号和密码，因此在使用该账号和密码时，容易被恶意第三方窃取，从而导致数据交换的安全性较差。

发明内容

本申请提供数据交换方法、装置及设备，以解决现有数据交换的安全性较差的问题。

根据本申请实施例的第一方面，提供一种数据交换方法，所述方法应用在与接收方设备进行数据交换的发送方设备上，所述方法包括：

与所述接收方设备协商进行所述数据交换的默认协议；

根据所述默认协议获得动态协议；

根据所述动态协议和待传输数据生成交换数据包；

向所述接收方设备传输所述交换数据包，以使所述接收方设备采用通过所述默认协议生成的动态协议接收所述交换数据包。

根据本申请实施例的第二方面，提供另一种数据交换方法，所述方法应用在与发送方设备进行数据交换的接收方设备上，所述方法包括：

与所述发送方设备协商进行所述数据交换的默认协议；

根据所述默认协议获得动态协议；

接收所述发送方设备传输的交换数据包，所述交换数据包为所述发送方设备采用通过所述默认协议生成的动态协议和待传输数据生成的数据包；

根据所述动态协议处理所述交换数据包。

根据本申请实施例的第三方面，提供一种数据交换装置，所述装置应用在与接收方设备进行数据交换的发送方设备上，所述装置包括：

协商单元，用于与所述接收方设备协商进行所述数据交换的默认协议；

获得单元，用于根据所述默认协议获得动态协议；

生成单元，用于根据所述动态协议和待传输数据生成交换数据包；

传输单元，用于向所述接收方设备传输所述交换数据包，以使所述接收方设备采用通过所述默认协议生成的动态协议接收所述交换数据包。

根据本申请实施例的第四方面，提供另一种数据交换装置，所述装置应用在与发送方设备进行数据交换的接收方设备上，所述装置包括：

协商单元，用于与所述发送方设备协商进行所述数据交换的默认协议；

获得单元，用于根据所述默认协议获得动态协议；

接收单元，用于接收所述发送方设备传输的交换数据包，所述交换数据包为所述发送方设备采用通过所述默认协议生成的动态协议和待传输数据生成的数据包；

处理单元，用于根据所述动态协议处理所述交换数据包。

根据本申请实施例的第五方面，提供一种数据交换设备，所述设备为与接收方设备进行数据交换的发送方设备，包括：处理器；用于存储所述处理器可执行指令的存储器；其中，所述处理器被配置为：

与所述接收方设备协商进行所述数据交换的默认协议；

根据所述默认协议获得动态协议；

根据所述动态协议和待传输数据生成交换数据包；

向所述接收方设备传输所述交换数据包，以使所述接收方设备采用通过所述默认协议生成的动态协议接收所述交换数据包。

根据本申请实施例的第六方面，提供另一种数据交换设备，所述设备为与发送方设备进行数据交换的接收方设备，包括：处理器；用于存储所述处理器可执行指令的存储器；其中，所述处理器被配置为：

与所述发送方设备协商进行所述数据交换的默认协议；

根据所述默认协议获得动态协议；

接收所述发送方设备传输的交换数据包，所述交换数据包为所述发送方设备采用通过所述默认协议生成的动态协议和待传输数据生成的数据包；

根据所述动态协议处理所述交换数据包。

本申请实施例进行数据交换时，发送方设备与接收方设备协商进行数据交换的默认协议后，根据该默认协议获得动态协议，发送方设备根据动态协议和待传输数据生成交换数据包，并将该交换数据包传输给接收方设备，接收方设备根据该动态协议处理交换数据包，从而完成数据交换。应用本申请实施例，发送方和接收方之间通过协商的默认协议生成动态协议，并基于该动态协议进行数据交换，由于动态协议可以在有数据交换需求时动态生成，因此可以有效避免恶意第三方对数据交换的通信过程进行窃取，从而能够提高数据交换的安全性。

应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本申请。

附图说明

此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本申请的实施例，并与说明书一起用于解释本申请的原理。

图 1 为本申请数据交换方法的一个实施例流程图；

图 2 为本申请数据交换方法的另一个实施例流程图；

图 3 为采用本申请实施例实现数据交换的应用场景示意图；

图 4A 为本申请数据交换方法的另一个实施例流程图；

图 4B 为图 4A 中一种根据默认协议生成动态协议的过程示意图；

图 4C 为图 4A 中一种交换数据包的包头格式示意图；

图 4D 为图 4A 中一种交换数据包的包体格式示意图；

图 5 为本申请数据交换装置所在设备的一种硬件结构图；

图 6 为本申请数据交换装置的一个实施例框图；

图 7 为本申请数据交换装置的另一个实施例框图。

具体实施方式

在本申请使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本申请。在本申请和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

应当理解，尽管在本申请可能采用术语第一、第二、第三等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如，在不脱离本申请范围的情况下，第一信息也可以被称为第二信息，类似地，第二信息也可以被称为第一信息。取决于语境，如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

随着大数据时代的来临，互联网企业在开展各种业务时，其部署的业务服务器会产生海量业务数据，出于不同企业间业务的合作，这些企业部署的业务服务器之间可能会产生数据交换的需求，以便通过交换各自的业务数据，从而完善各自的业务。例如，企业 A 部署的业务服务器获得了大量的业务风险数据，企业 B 部署的业务服务器获得了大量的用户社交数据，则上述两个企业的业务服务器通过数据交换，企业 A 可以通过交换得到的用户社交数据

了解风险用户的传播方式，而企业 B 可以通过交换得到的业务风险数据在业务推广过程中避免风险用户。但是在现有技术中，业务服务器之间交换数据的安全性较差，因此本申请实施例中，数据交换的发送方和接收方之间通过协商的默认协议生成动态协议，并基于该动态协议进行数据交换，因此可以有效避免恶意第三方对数据交换的通信过程进行窃取，从而能够提高数据交换的安全性，下面结合具体实施例对本申请进行详细描述。

参见图 1，为本申请数据交换方法的一个实施例流程图，该实施例从与接收方设备进行数据交换的发送方设备侧进行描述，包括以下步骤：

步骤 101：与接收方设备协商进行数据交换的默认协议。

本实施例中，发送方设备在与接收方设备协商进行数据交换的默认协议时，可以同时协商进行该数据交换的密钥。

其中，发送方设备和接收方设备可以通过分别向可信服务器签到，获得上述默认协议和密钥，可信服务器由可信第三方设置，用于向进行数据交换的双方提供默认协议和密钥；当发送方设备获得默认协议和密钥后，可以将该默认协议和密钥通过串口写入 SIM（Subscriber Identity Module，客户识别模块）卡中。当与接收方设备协商默认协议和密钥时，发送方设备可以通过串口从 SIM 卡中读取从可信服务器获得的默认协议和密钥，然后与接收方设备之间通过握手协议，确定采用同样的默认协议和密钥进行数据交换。

步骤 102：根据默认协议获得动态协议。

本实施例中，发送方设备可以采用如下任一方式，通过与预先设置的动态协议生成器进行通信，从而获得动态协议。

在一个可选的实现方式中，动态协议在发送方设备侧生成：

发送方设备可以向动态协议生成器发送进行数据交换的注册请求，动态协议生成器根据该注册请求为该数据交换生成随机协议码，并将该随机协议码发送给发送方设备，发送方设备将该随机协议码与协商确定的默认协议按位进行二进制运算，得到动态协议。

在另一个可选的实现方式中，动态协议在动态协议生成器侧生成：

发送方设备可以向动态协议生成器发送进行数据交换的注册请求，该注册请求中可以携带协商确定的默认协议，动态协议生成器根据该注册请求为该数据交换生成随机协议码，将该随机协议码与注册请求中携带的默认协议按位进行二进制运算，得到动态协议，并将该动态协议发送至发送方设备。

步骤 103：根据动态协议和待传输数据生成交换数据包。

本实施例中，当发送方设备与接收方设备协商了密钥时，发送方设备可以通过该密钥对待传输数据进行加密，获得加密数据，然后根据获得的动态协议和该加密数据生成交换数据包。可选的，当待传输数据较大时，可以进一步对上述加密数据进行压缩，获得加密压缩数据后，根据获得的动态协议和该加密压缩数据生成交换数据包。

本实施例中，在生成交换数据包时，发送方设备可以调用预设的数据包格式，该数据包格式包括包头和包体，然后将获得的动态协议按照预设的包头格式写入交换数据包的包头，以及将待传输数据按照预设的包体格式写入交换数据包的包体。其中，当通过对待传输数据进行加密获得加密数据时，可以将上述加密数据按照预设的包体格式写入交换数据包的包体；当进一步对加密数据进行压缩得到加密压缩数据时，可以将上述加密压缩数据按照预设的包体格式写入交换数据包的包体。

其中，上述包头格式可以包括：动态协议的协议名，和待传输数据在该数据交换所要交换的所有数据中的顺序；

上述包体格式可以包括：将待传输数据分成的 N（N 为大于 1 的自然数）个数据子包，每个数据子包的子包格式包括子包长度和子包数据。其中，每个子包数据的数据格式可以包括位图索引和将子包数据分成的 M（M 为大于 1 的自然数）个子数据域，其中，该位图索引中包括 M 个子数据域中的每个子数据域的子数据域长度，和每个子数据域在其所属子包数据中的开始位置。

步骤 104：向接收方设备传输交换数据包，以使接收方设备采用通过该默认协议生成的动态协议接收该交换数据包。

由上述实施例可见，发送方和接收方之间通过协商的默认协议生成动态

协议，并基于该动态协议进行数据交换，由于动态协议可以在有数据交换需求时动态生成，因此可以有效避免恶意第三方对数据交换的通信过程进行窃取，从而能够提高数据交换的安全性。

参见图 2，为本申请数据交换方法的另一个实施例流程图，该实施例从与发送方设备进行数据交换的接收方设备侧进行描述，包括以下步骤：

步骤 201：与发送方设备协商进行数据交换的默认协议。

步骤 202：根据默认协议获得动态协议。

上述步骤 201 和步骤 202 描述的接收方设备侧协商默认协议，以及获得动态协议的过程与发送方设备侧一致，在此不再赘述。

步骤 203：接收发送方设备传输的交换数据包，该交换数据包为发送方设备采用通过该默认协议生成的动态协议和待传输数据生成的数据包。

步骤 204：根据该动态协议处理交换数据包。

本实施例中，接收方设备可以调用预设的数据包格式解析接收到的交换数据包，获取该交换数据包中携带的协议，接收方设备调用的预设的数据包格式与图 1 所示实施例中发送方设备调用的数据包格式一致，在此不再赘述。基于上述数据包格式，接收方设备可以从交换数据包的包头中获取协议，并可以判断交换数据包中携带的协议是否与获得的动态协议相同，如果相同，则可以从交换数据包的包体中获取待传输数据；其中，当包体中携带的是由发送方设备通过协商的密钥对待传输的数据进行加密得到的加密数据时，则接收方设备从包体中获取到加密数据后，可以通过协商的密钥对加密数据进行解密后，获得待传输数据；进一步，当包体中携带的是由发送方设备对加密数据进行压缩得到的加密压缩数据时，则接收方设备从包体中获取到加密压缩数据后，可以先对加密压缩数据进行解压后得到加密数据，然后再通过协商的密钥对加密数据进行解密后，获得待传输数据。

由上述实施例可见，发送方和接收方之间通过协商的默认协议生成动态协议，并基于该动态协议进行数据交换，由于动态协议可以在有数据交换需求时动态生成，因此可以有效避免恶意第三方对数据交换的通信过程进行窃

取，从而能够提高数据交换的安全性。

参见图 3，为采用本申请实施例实现数据交换的应用场景示意图：

图 3 所示的应用场景中包括：作为发送方设备的业务服务器 A，作为接收方设备的业务服务器 B，由可信第三方设置的用于提供默认协议和密钥的可信服务器，以及用于提供随机协议码的动态协议生成器。基于图 3 示出的应用场景，当业务服务器 A 和业务服务器 B 之间要进行数据交换时，业务服务器 A 和业务服务器 B 可以分别向可信服务器请求默认协议和密钥，可信服务器可以向进行数据交换的双方提供进行本次数据交换的默认协议和密钥，当业务服务器 A 和业务服务器 B 通过协商确定使用的默认协议和密钥后，各自通过与动态协议生成器进行通信，根据默认协议生成动态协议，并采用上述动态协议和密钥完成数据交换。

参见图 4A，为本申请数据交换方法的另一个实施例流程图，该实施例结合图 3 示出的应用场景，对业务服务器 A 和业务服务器 B 之间的数据交换过程进行了详细描述，包括以下步骤：

步骤 401：业务服务器 A 和业务服务器 B 分别通过向可信服务器签到，获得本次数据交换的默认协议和密钥。

业务服务器 A 和业务服务器 B 之间存在数据交换需求时，为了保证数据交换的安全性，可以分别向可信服务器进行签到，由可信服务器为业务服务器 A 和业务服务器 B 分配进行本次数据交换的默认协议和密钥。其中，业务服务器 A 和业务服务器可以在签到时提供进行本次数据交换的交换标识，以便可信服务器根据该交换标识，为进行本次数据交换业务服务器 A 和业务服务器 B 分配相同的默认协议和密钥。

步骤 402：业务服务器 A 和业务服务器 B 分别将获得的默认协议和密钥通过串口写入各自的 SIM 卡中。

本实施例中，业务服务器 A 和业务服务器 B 上分别设置有 SIM 卡，用于对默认协议和密钥进行保存，其中，默认协议和密钥可以通过串口，按照其信息的逐个字节写入 SIM 卡中，后续也可以从 SIM 卡中逐个字节读出信

息。

步骤 403：当业务服务器 A 和业务服务器 B 要进行数据交换时，各自通过串口从 SIM 卡中读取默认协议和密钥。

步骤 404：业务服务器 A 与业务服务器 B 之间通过握手协议，协商确定进行数据交换的默认协议和密钥。

本申请实施例中，如果业务服务器 A 和业务服务器 B 上仅保存了由可信服务器下发的一组默认协议和密钥，则业务服务器 A 和业务服务器 B 之间通过握手协议，协商确定使用该一组默认协议和密钥进行数据交换；如果业务服务器 A 和业务服务器 B 上保存了由可信服务器下发的多组默认协议和密钥，则业务服务器 A 和业务服务器 B 之间通过握手协议，可以从多组默认协议和密钥中协商确定一组默认协议和密钥进行数据交换。

步骤 405：业务服务器 A 和业务服务器 B 分别向动态协议生成器发送进行本次数据交换的注册请求。

本实施例中，动态协议生成器用于为进行数据交换的双方生成随机协议码。当业务服务器 A 和业务服务器 B 协商确定了默认协议和密钥后，各自向动态协议生成器发送进行本次数据交换的注册请求，注册请求中可以包含本次数据交换的交换标识，以便动态协议生成器可以根据该交换标识为本次数据交换生成随机协议码，即为业务服务器 A 和业务服务器 B 生成相同的随机协议码。

步骤 406：动态协议生成器根据注册请求为本次数据交换生成随机协议码。

步骤 407：动态协议生成器将该随机协议码分别发送给业务服务器 A 和业务服务器 B。

步骤 408：业务服务器 A 和业务服务器 B 各自将随机协议码与协商的默认协议按位进行二进制运算，得到动态协议。

本步骤中，进行数据交换的业务服务器 A 和业务服务器 B 在获得了相同的随机协议码后，可以将该随机协议码与协商确定的默认协议按位进行二进

制运算，从而得到动态协议。其中，随机协议码的字节数与默认协议的字节数相同，在二者进行二进制运算后，可以得到字节数相同的动态协议。

参见图 4B，为图 4A 中一种根据默认协议生成动态协议的过程示意图：假设默认协议为七个字节的“ALIBABA”，随机协议码为七个字节的“1352847”，则将“ALIBABA”和“1352847”中的每个字节转换为八位的二进制值，然后将对称字节位的二进制值相加，将相加后的每个二进制值转换为组成动态协议的七个字节“BONDIFH”。

步骤 409：业务服务器 A 通过协商的密钥对待传输数据进行加密，获得加密数据。

本步骤中，密钥可以为采用对称加密方式加密数据的密钥，对称加密方式可以具体为 DEA（Data Encryption Algorithm，数据加密算法）加密方式，则可信服务器可以为业务服务器 A 和业务服务器 B 分配用于 DEA 加密的密钥，例如，该密钥可以为 8 个字节，其中最后一个字节为奇偶校验位，在采用 DEA 加密方式加密时，与现有技术中的描述一致，本申请实施例不再赘述。

步骤 410：业务服务器 A 对加密数据进行压缩，获得加密压缩数据。

本实施例中，业务服务器 A 和业务服务器 B 可以根据其支持平台的不同采用不同的压缩和解压方式，例如，WINDOWS 平台可以采用 ZIP 方式，LINUX 平台可以采用 GZIP 方式等，对此本申请实施例不进行限制。

步骤 411：业务服务器 A 根据得到的动态协议和加密压缩数据生成交换数据包。

本步骤中，当业务服务器 A 得到加密压缩数据包后，可以调用预设的数据包格式，该数据包格式包括包头和包体，然后将动态协议按照预设的包头格式写入交换数据包的包头，以及将待传输数据按照预设的包体格式写入交换数据包的包体。

参见图 4C，为图 4A 中一种交换数据包的包头格式示意图：

图 4C 中的包头格式可以包括：动态协议名字段，该字段中用于写入业

务服务器 A 上生成的动态协议的协议名；以及多包标记字段，该字段中用于写入待传输数据在本次数据交换所要交换的所有数据中的顺序，例如，本次数据交换需要传输一百个数据包，当前传输的是第五十个数据包，则可以在多包标记字段写入“50”。

参见图 4D，为图 4A 中一种交换数据包的包体格式示意图；

图 4D 中的包体格式可以包括：将加密压缩数据分成的 N（N 为大于 1 的自然数）个数据子包，每个数据子包的子包格式包括子包长度和子包数据，如图 4D 中，以第一个数据子包为例，其子包长度表示为“包 1 长度”，其子包数据为“压缩包 1”。其中，每个子包数据的数据格式包括位图索引和将子包数据分成的 N 个子数据域，其中，该位图索引中包括 N 个索引，每个索引对应一个子数据域，每个索引可以由两个字节组成，其中一个字节用于表示对应子数据域的长度，另一个字节用于表示对应子数据域在其所属子包数据中的开始位置。本实施例中，N 为大于 1 的自然数，例如，N 可以为 64 或 128。

步骤 412：业务服务器 A 向业务服务器 B 传输交换数据包。

步骤 413：业务服务器 B 根据得到的动态协议处理接收到的交换数据包，获得加密压缩数据包。

业务服务器接收到交换数据包后，可以调用预设的数据包格式解析该交换数据包，本步骤中预设的数据包格式与步骤 411 中所描述的业务服务器 A 生成交换数据包时调用的数据包格式一致。在业务服务器 B 解析完交换数据包后，可以从包头中获取交换数据包携带的协议，然后判断该协议是否与业务服务器 B 生成的动态协议相同，如果相同，则可以从包体中获取加密压缩数据。

步骤 414：业务服务器 B 对加密压缩数据进行解压获得加密数据。

步骤 415：业务服务器 B 通过协商的密钥对加密数据进行解密，获得待传输数据。

在业务服务器 A 和业务服务器 B 基于前述流程完成数据交换后，业务服

务器 A 和业务服务器 B 可以分别向动态协议生成器发送去注册请求，以便动态协议生成器可以删除为本次数据交换生成的随机协议码，从而完成自身的状态更新。

由上述实施例可见，发送方和接收方之间通过协商的默认协议生成动态协议，并基于该动态协议进行数据交换，由于动态协议可以在有数据交换需求时动态生成，因此可以有效避免恶意第三方对数据交换的通信过程进行窃取，从而能够提高数据交换的安全性；当待传输数据通过发送方和接收方协商的密钥进行加密传输时，可以进一步提高数据交换的安全性，并且，当对加密数据进行压缩传输，还可以节省数据交换时的传输资源。

与本申请数据交换方法的实施例相对应，本申请还提供了数据交换装置及设备的实施例。

本申请数据交换装置的实施例可以应用在用于进行数据交换的发送方设备或接收方设备上。装置实施例可以通过软件实现，也可以通过硬件或者软硬件结合的方式实现。以软件实现为例，作为一个逻辑意义上的装置，是通过其所在设备的处理器将非易失性存储器中对应的计算机程序指令读取到内存中运行形成的。从硬件层面而言，如图 5 所示，为本申请数据交换装置所在设备的一种硬件结构图，除了图 5 所示的处理器、内存、网络接口、以及非易失性存储器之外，实施例中装置所在的设备通常根据该设备的实际功能，还可以包括其他硬件，图 5 中不再一一示出。

参见图 6，为本申请数据交换装置的一个实施例框图，该装置可以应用在与接收方设备进行数据交换的发送方设备上，该装置包括：协商单元 610、获得单元 620、生成单元 630 和传输单元 640。

其中，协商单元 610，用于与所述接收方设备协商进行所述数据交换的默认协议；

获得单元 620，用于根据所述默认协议获得动态协议；

生成单元 630，用于根据所述动态协议和待传输数据生成交换数据包；

传输单元 640，用于向所述接收方设备传输所述交换数据包，以使所述

接收方设备采用通过所述默认协议生成的动态协议接收所述交换数据包。

在一个可选的实现方式中:

所述协商单元 610，还可以用于在与所述接收方设备协商进行所述数据交换的默认协议时，协商进行所述数据交换的密钥;

所述生成单元 630 可以包括（图 6 中未示出）:

数据加密子单元，用于通过所述密钥对所述待传输数据进行加密，获得加密数据;

数据包生成子单元，用于根据所述动态协议和所述加密数据生成交换数据包。

在另一个可选的实现方式中，所述生成单元 630 还可以包括（图 6 中未示出）:

数据压缩子单元，用于对所述加密数据进行压缩，获得加密压缩数据;

相应的，所述数据包生成子单元，可以具体用于根据所述动态协议和所述加密压缩数据生成交换数据包。

在另一个可选的实现方式中，所述装置还可以包括（图 6 中未示出）:

签到单元，用于所述协商单元与所述接收方设备协商进行所述数据交换的默认协议和密钥之前，当确定与所述接收方设备进行所述数据交换时，通过向可信服务器签到，获得所述默认协议和密钥;

写入单元，用于将所述默认协议和密钥通过串口写入客户识别模块 SIM 卡中;

所述协商单元 610 可以包括（图 6 中未示出）:

SIM 卡读取子单元，用于通过所述串口从所述 SIM 卡中读取所述默认协议和密钥;

握手协商子单元，用于与所述接收方设备之间通过握手协议，确定采用所述默认协议和密钥进行所述数据交换。

在另一个可选的实现方式中，所述获得单元 620 可以包括（图 6 中未示出）:

第一请求发送子单元，用于向动态协议生成器发送进行所述数据交换的注册请求；

随机协议码接收子单元，用于接收所述动态协议生成器根据所述注册请求为所述数据交换生成的随机协议码；

动态协议生成子单元，用于将所述随机协议码与所述默认协议按位进行二进制运算，得到动态协议。

在另一个可选的实现方式中，所述获得单元 620 也可以包括（图 6 中未示出）：

第二请求发送子单元，用于向动态协议生成器发送进行所述数据交换的注册请求，所述注册请求中携带所述默认协议，以使所述动态协议生成器将为所述数据交换生成的随机协议码与所述默认协议按位进行二进制运算，得到所述动态协议；

动态协议接收子单元，用于接收所述动态协议生成器生成的所述动态协议。

在另一个可选的实现方式中，所述生成单元 630 可以包括（图 6 中未示出）：

格式调用子单元，用于调用预设的数据包格式，所述数据包格式包括包头和包体；

数据写入子单元，用于将所述动态协议按照预设的包头格式写入所述交换数据包的包头，以及将所述待传输数据按照预设的包体格式写入所述交换数据包的包体。

其中，所述包头格式可以包括：

所述动态协议的协议名，和所述待传输数据在所述数据交换所要交换的所有数据中的顺序；

所述包体格式可以包括：

将所述待传输数据分成的 N 个数据子包，每个所述数据子包的子包格式包括子包长度和子包数据，所述 N 为大于 1 的自然数；其中，

每个所述子包数据的数据格式包括位图索引和将所述子包数据分成的M个子数据域，其中，所述位图索引中包括所述M个子数据域中的每个子数据域的子数据域长度，和每个子数据域在所述子包数据中的开始位置，所述M为大于1的自然数。

参见图 7，为本申请数据交换装置的另一个实施例框图，该装置可以应用在与发送方设备进行数据交换的接收方设备，该装置包括：协商单元710、获得单元720、接收单元730和处理单元740。

其中，协商单元 710，用于与所述发送方设备协商进行所述数据交换的默认协议；

获得单元720，用于根据所述默认协议获得动态协议；

接收单元 730，用于接收所述发送方设备传输的交换数据包，所述交换数据包为所述发送方设备采用通过所述默认协议生成的动态协议和待传输数据生成的数据包；

处理单元740，用于根据所述动态协议处理所述交换数据包。

在一个可选的实现方式中：

所述协商单元 710，还可以用于在与所述发送方设备协商进行所述数据交换的默认协议时，协商进行所述数据交换的密钥；

相应的，所述交换数据包可以具体为：根据所述动态协议和加密数据生成的交换数据包，所述加密数据为通过所述密钥对所述待传输数据进行加密后获得的数据。

在另一个可选的实现方式中，所述装置还可以包括（图 7 中未示出）：

签到单元，用于所述协商单元与所述发送方设备协商进行所述数据交换的默认协议和密钥之前，当确定与所述发送方设备进行所述数据交换时，通过向可信服务器签到，获得所述默认协议和密钥；

写入单元，用于将所述默认协议和密钥通过串口写入 SIM 卡中；

所述协商单元710可以包括（图 7 中未示出）：

SIM 卡读取子单元，用于通过所述串口从所述 SIM 卡中读取所述默认协

议和密钥;

握手协商子单元，用于与所述发送方设备之间通过握手协议，确定采用所述默认协议和密钥进行所述数据交换。

在另一个可选的实现方式中，所述获得单元 720 可以包括（图 7 中未示出）:

第一请求发送子单元，用于向动态协议生成器发送进行所述数据交换的注册请求;

随机协议码接收子单元，用于接收所述动态协议生成器根据所述注册请求为所述数据交换生成的随机协议码;

动态协议生成子单元，用于将所述随机协议码与所述默认协议按位进行二进制运算，得到动态协议。

在另一个可选的实现方式中，所述获得单元 720 也可以包括（图 7 中未示出）:

第二请求发送子单元，用于向动态协议生成器发送进行所述数据交换的注册请求，所述注册请求中携带所述默认协议，以使所述动态协议生成器将为所述数据交换生成的随机协议码与所述默认协议按位进行二进制运算，得到所述动态协议;

动态协议接收子单元，用于接收所述动态协议生成器生成的所述动态协议。

在另一个可选的实现方式中，所述处理单元 740 可以包括（图 7 中未示出）:

格式调用子单元，用于调用预设的数据包格式解析所述交换数据包，获取所述交换数据包中携带的协议;

协议判断子单元，用于判断所述交换数据包中携带的协议是否与所述动态协议相同;

数据获取子单元，用于如果所述交换数据包中携带的协议与所述动态协议相同，则从所述交换数据包中获取所述待传输数据。

所述预设的数据包格式可以包括包头和包体；其中，

所述包头的包头格式可以包括:

所述交换数据包中携带的协议的协议名，和所述待传输数据在所述数据交换所要交换的所有数据中的顺序;

所述包体的包体格式可以包括:

将所述待传输数据分成的 N 个数据子包，每个所述数据子包的子包格式包括子包长度和子包数据，所述 N 为大于 1 的自然数；其中，

每个所述子包数据的数据格式包括位图索引和将所述子包数据分成的 M 个子数据域，其中，所述位图索引中包括所述 M 个子数据域中的每个子数据域的子数据域长度，和每个子数据域在所述子包数据中的开始位置，所述 M 为大于 1 的自然数。

上述装置中各个单元的功能和作用的实现过程具体详见上述方法中对应步骤的实现过程，在此不再赘述。

对于装置实施例而言，由于其基本对应于方法实施例，所以相关之处参见方法实施例的部分说明即可。以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本申请方案的目的。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。

由上述实施例可见，发送方和接收方之间通过协商的默认协议生成动态协议，并基于该动态协议进行数据交换，由于动态协议可以在有数据交换需求时动态生成，因此可以有效避免恶意第三方对数据交换的通信过程进行窃取，从而能够提高数据交换的安全性。

本领域技术人员在考虑说明书及实践这里公开的发明后，将容易想到本申请的其它实施方案。本申请旨在涵盖本申请的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本申请的一般性原理并包括本申

请未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本申请的真正范围和精神由下面的权利要求指出。

应当理解的是，本申请并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本申请的范围仅由所附的权利要求来限制。

权 利 要 求 书

1、一种数据交换方法，其特征在于，所述方法应用在与接收方设备进行数据交换的发送方设备上，所述方法包括：

与所述接收方设备协商进行所述数据交换的默认协议；

根据所述默认协议获得动态协议；

根据所述动态协议和待传输数据生成交换数据包；

向所述接收方设备传输所述交换数据包，以使所述接收方设备采用通过所述默认协议生成的动态协议接收所述交换数据包。

2、根据权利要求 1 所述的方法，其特征在于，所述方法还包括：在与所述接收方设备协商进行所述数据交换的默认协议时，协商进行所述数据交换的密钥；

所述根据所述动态协议和待传输数据生成交换数据包，包括：

通过所述密钥对所述待传输数据进行加密，获得加密数据；

根据所述动态协议和所述加密数据生成交换数据包。

3、根据权利要求 2 所述的方法，其特征在于，所述根据所述动态协议和所述加密数据生成交换数据包之前，还包括：

对所述加密数据进行压缩，获得加密压缩数据；

所述根据所述动态协议和所述加密数据生成交换数据包，具体为：

根据所述动态协议和所述加密压缩数据生成交换数据包。

4、根据权利要求 2 所述的方法，其特征在于，与所述接收方设备协商进行所述数据交换的默认协议和密钥之前，所述方法还包括：

当确定与所述接收方设备进行所述数据交换时，通过向可信服务器签到，获得所述默认协议和密钥；

将所述默认协议和密钥通过串口写入客户识别模块 SIM 卡中；

所述与所述接收方设备协商进行所述数据交换的默认协议和密钥，包括：

通过所述串口从所述 SIM 卡中读取所述默认协议和密钥；

与所述接收方设备之间通过握手协议，确定采用所述默认协议和密钥进行所述数据交换。

5、根据权利要求 1 所述的方法，其特征在于，所述根据所述默认协议获得动态协议，包括:

向动态协议生成器发送进行所述数据交换的注册请求;

接收所述动态协议生成器根据所述注册请求为所述数据交换生成的随机协议码;

将所述随机协议码与所述默认协议按位进行二进制运算,得到动态协议。

6、根据权利要求 1 所述的方法，其特征在于，所述根据所述默认协议获得动态协议，包括:

向动态协议生成器发送进行所述数据交换的注册请求，所述注册请求中携带所述默认协议，以使所述动态协议生成器将为所述数据交换生成的随机协议码与所述默认协议按位进行二进制运算，得到所述动态协议;

接收所述动态协议生成器生成的所述动态协议。

7、根据权利要求 1 所述的方法，其特征在于，所述根据所述动态协议和待传输数据生成交换数据包，包括:

调用预设的数据包格式，所述数据包格式包括包头和包体;

将所述动态协议按照预设的包头格式写入所述交换数据包的包头，以及将所述待传输数据按照预设的包体格式写入所述交换数据包的包体。

8、根据权利要求 7 所述的方法，其特征在于，

所述包头格式包括:

所述动态协议的协议名，和所述待传输数据在所述数据交换所要交换的所有数据中的顺序;

所述包体格式包括:

将所述待传输数据分成的 N 个数据子包，每个所述数据子包的子包格式包括子包长度和子包数据，所述 N 为大于 1 的自然数; 其中，

每个所述子包数据的数据格式包括位图索引和将所述子包数据分成的 M

个子数据域，其中，所述位图索引中包括所述 M 个子数据域中的每个子数据域的子数据域长度，和每个子数据域在所述子包数据中的开始位置，所述 M 为大于 1 的自然数。

9、一种数据交换方法，其特征在于，所述方法应用在与发送方设备进行数据交换的接收方设备上，所述方法包括：

与所述发送方设备协商进行所述数据交换的默认协议；

根据所述默认协议获得动态协议；

接收所述发送方设备传输的交换数据包，所述交换数据包为所述发送方设备采用通过所述默认协议生成的动态协议和待传输数据生成的数据包；

根据所述动态协议处理所述交换数据包。

10、根据权利要求 9 所述的方法，其特征在于，所述方法还包括：在与所述发送方设备协商进行所述数据交换的默认协议时，协商进行所述数据交换的密钥；

所述交换数据包具体为：根据所述动态协议和加密数据生成的交换数据包，所述加密数据为通过所述密钥对所述待传输数据进行加密后获得的数据。

11、根据权利要求 10 所述的方法，其特征在于，在与所述发送方设备协商进行所述数据交换的默认协议和密钥之前，所述方法还包括：

当确定与所述发送方设备进行所述数据交换时，通过向可信服务器签到，获得所述默认协议和密钥；

将所述默认协议和密钥通过串口写入 SIM 卡中；

所述与所述发送方设备协商进行所述数据交换的默认协议和密钥，包括：

通过所述串口从所述 SIM 卡中读取所述默认协议和密钥；

与所述发送方设备之间通过握手协议，确定采用所述默认协议和密钥进行所述数据交换。

12、根据权利要求 9 所述的方法，其特征在于，所述根据所述默认协议获得动态协议，包括：

向动态协议生成器发送进行所述数据交换的注册请求；

接收所述动态协议生成器根据所述注册请求为所述数据交换生成的随机协议码;

将所述随机协议码与所述默认协议按位进行二进制运算,得到动态协议。

13、根据权利要求 9 所述的方法，其特征在于，所述根据所述默认协议获得动态协议，包括:

向动态协议生成器发送进行所述数据交换的注册请求，所述注册请求中携带所述默认协议，以使所述动态协议生成器将为所述数据交换生成的随机协议码与所述默认协议按位进行二进制运算，得到所述动态协议;

接收所述动态协议生成器生成的所述动态协议。

14、根据权利要求 9 所述的方法，其特征在于，所述根据所述动态协议处理所述交换数据包，包括:

调用预设的数据包格式解析所述交换数据包，获取所述交换数据包中携带的协议;

判断所述交换数据包中携带的协议是否与所述动态协议相同;

如果相同，则从所述交换数据包中获取所述待传输数据。

15、根据权利要求 14 所述的方法，其特征在于，所述预设的数据包格式包括包头和包体; 其中，

所述包头的包头格式包括:

所述交换数据包中携带的协议的协议名，和所述待传输数据在所述数据交换所要交换的所有数据中的顺序;

所述包体的包体格式包括:

将所述待传输数据分成的 N 个数据子包，每个所述数据子包的子包格式包括子包长度和子包数据，所述 N 为大于 1 的自然数; 其中，

每个所述子包数据的数据格式包括位图索引和将所述子包数据分成的 M 个子数据域，其中，所述位图索引中包括所述 M 个子数据域中的每个子数据域的子数据域长度，和每个子数据域在所述子包数据中的开始位置，所述 M 为大于 1 的自然数。

16、一种数据交换装置，其特征在于，所述装置应用在与接收方设备进行数据交换的发送方设备上，所述装置包括:

协商单元，用于与所述接收方设备协商进行所述数据交换的默认协议;

获得单元，用于根据所述默认协议获得动态协议;

生成单元，用于根据所述动态协议和待传输数据生成交换数据包;

传输单元，用于向所述接收方设备传输所述交换数据包，以使所述接收方设备采用通过所述默认协议生成的动态协议接收所述交换数据包。

17、根据权利要求 16 所述的装置，其特征在于，所述协商单元，还用于在与所述接收方设备协商进行所述数据交换的默认协议时，协商进行所述数据交换的密钥;

所述生成单元包括:

数据加密子单元，用于通过所述密钥对所述待传输数据进行加密，获得加密数据;

数据包生成子单元，用于根据所述动态协议和所述加密数据生成交换数据包。

18、根据权利要求 17 所述的装置，其特征在于，所述生成单元还包括:

数据压缩子单元，用于对所述加密数据进行压缩，获得加密压缩数据;

所述数据包生成子单元，具体用于根据所述动态协议和所述加密压缩数据生成交换数据包。

19、根据权利要求 17 所述的装置，其特征在于，所述装置还包括:

签到单元，用于所述协商单元与所述接收方设备协商进行所述数据交换的默认协议和密钥之前，当确定与所述接收方设备进行所述数据交换时，通过向可信服务器签到，获得所述默认协议和密钥;

写入单元，用于将所述默认协议和密钥通过串口写入客户识别模块 SIM 卡中;

所述协商单元包括:

SIM 卡读取子单元，用于通过所述串口从所述 SIM 卡中读取所述默认协

议和密钥;

握手协商子单元，用于与所述接收方设备之间通过握手协议，确定采用所述默认协议和密钥进行所述数据交换。

20、根据权利要求 16 所述的装置，其特征在于，所述获得单元包括:

第一请求发送子单元，用于向动态协议生成器发送进行所述数据交换的注册请求;

随机协议码接收子单元，用于接收所述动态协议生成器根据所述注册请求为所述数据交换生成的随机协议码;

动态协议生成子单元，用于将所述随机协议码与所述默认协议按位进行二进制运算，得到动态协议。

21、根据权利要求 16 所述的装置，其特征在于，所述获得单元包括:

第二请求发送子单元，用于向动态协议生成器发送进行所述数据交换的注册请求，所述注册请求中携带所述默认协议，以使所述动态协议生成器将为所述数据交换生成的随机协议码与所述默认协议按位进行二进制运算，得到所述动态协议;

动态协议接收子单元，用于接收所述动态协议生成器生成的所述动态协议。

22、根据权利要求 16 所述的装置，其特征在于，所述生成单元包括:

格式调用子单元，用于调用预设的数据包格式，所述数据包格式包括包头和包体;

数据写入子单元，用于将所述动态协议按照预设的包头格式写入所述交换数据包的包头，以及将所述待传输数据按照预设的包体格式写入所述交换数据包的包体。

23、根据权利要求 22 所述的装置，其特征在于，

所述包头格式包括:

所述动态协议的协议名，和所述待传输数据在所述数据交换所要交换的所有数据中的顺序;

所述包体格式包括:

将所述待传输数据分成的 N 个数据子包，每个所述数据子包的子包格式包括子包长度和子包数据，所述 N 为大于 1 的自然数；其中，

每个所述子包数据的数据格式包括位图索引和将所述子包数据分成的 M 个子数据域，其中，所述位图索引中包括所述 M 个子数据域中的每个子数据域的子数据域长度，和每个子数据域在所述子包数据中的开始位置，所述 M 为大于 1 的自然数。

24、一种数据交换装置，其特征在于，所述装置应用在与发送方设备进行数据交换的接收方设备上，所述装置包括:

协商单元，用于与所述发送方设备协商进行所述数据交换的默认协议;

获得单元，用于根据所述默认协议获得动态协议;

接收单元，用于接收所述发送方设备传输的交换数据包，所述交换数据包为所述发送方设备采用通过所述默认协议生成的动态协议和待传输数据生成的数据包;

处理单元，用于根据所述动态协议处理所述交换数据包。

25、根据权利要求 24 所述的装置，其特征在于，所述协商单元，还用于在与所述发送方设备协商进行所述数据交换的默认协议时，协商进行所述数据交换的密钥;

所述交换数据包具体为：根据所述动态协议和加密数据生成的交换数据包,所述加密数据为通过所述密钥对所述待传输数据进行加密后获得的数据。

26、根据权利要求 25 所述的装置，其特征在于，所述装置还包括:

签到单元，用于所述协商单元与所述发送方设备协商进行所述数据交换的默认协议和密钥之前，当确定与所述发送方设备进行所述数据交换时，通过向可信服务器签到，获得所述默认协议和密钥;

写入单元，用于将所述默认协议和密钥通过串口写入 SIM 卡中;

所述协商单元包括:

SIM 卡读取子单元，用于通过所述串口从所述 SIM 卡中读取所述默认协

议和密钥;

握手协商子单元，用于与所述发送方设备之间通过握手协议，确定采用所述默认协议和密钥进行所述数据交换。

27、根据权利要求 24 所述的装置，其特征在于，所述获得单元包括:

第一请求发送子单元，用于向动态协议生成器发送进行所述数据交换的注册请求;

随机协议码接收子单元，用于接收所述动态协议生成器根据所述注册请求为所述数据交换生成的随机协议码;

动态协议生成子单元，用于将所述随机协议码与所述默认协议按位进行二进制运算，得到动态协议。

28、根据权利要求 24 所述的装置，其特征在于，所述获得单元包括:

第二请求发送子单元，用于向动态协议生成器发送进行所述数据交换的注册请求，所述注册请求中携带所述默认协议，以使所述动态协议生成器将为所述数据交换生成的随机协议码与所述默认协议按位进行二进制运算，得到所述动态协议;

动态协议接收子单元，用于接收所述动态协议生成器生成的所述动态协议。

29、根据权利要求 24 所述的装置，其特征在于，所述处理单元包括:

格式调用子单元，用于调用预设的数据包格式解析所述交换数据包，获取所述交换数据包中携带的协议;

协议判断子单元，用于判断所述交换数据包中携带的协议是否与所述动态协议相同;

数据获取子单元，用于如果所述交换数据包中携带的协议与所述动态协议相同，则从所述交换数据包中获取所述待传输数据。

30、根据权利要求 29 所述的装置，其特征在于，所述预设的数据包格式包括包头和包体; 其中，

所述包头的包头格式包括:

所述交换数据包中携带的协议的协议名，和所述待传输数据在所述数据交换所要交换的所有数据中的顺序；

所述包体的包体格式包括：

将所述待传输数据分成的 N 个数据子包，每个所述数据子包的子包格式包括子包长度和子包数据，所述 N 为大于 1 的自然数；其中，

每个所述子包数据的数据格式包括位图索引和将所述子包数据分成的 M 个子数据域，其中，所述位图索引中包括所述 M 个子数据域中的每个子数据域的子数据域长度，和每个子数据域在所述子包数据中的开始位置，所述 M 为大于 1 的自然数。

31、一种数据交换设备，其特征在于，所述设备为与接收方设备进行数据交换的发送方设备，包括：处理器；用于存储所述处理器可执行指令的存储器；其中，所述处理器被配置为：

与所述接收方设备协商进行所述数据交换的默认协议；

根据所述默认协议获得动态协议；

根据所述动态协议和待传输数据生成交换数据包；

向所述接收方设备传输所述交换数据包，以使所述接收方设备采用通过所述默认协议生成的动态协议接收所述交换数据包。

32、一种数据交换设备，其特征在于，所述设备为与发送方设备进行数据交换的接收方设备，包括：处理器；用于存储所述处理器可执行指令的存储器；其中，所述处理器被配置为：

与所述发送方设备协商进行所述数据交换的默认协议；

根据所述默认协议获得动态协议；

接收所述发送方设备传输的交换数据包，所述交换数据包为所述发送方设备采用通过所述默认协议生成的动态协议和待传输数据生成的数据包；

根据所述动态协议处理所述交换数据包。

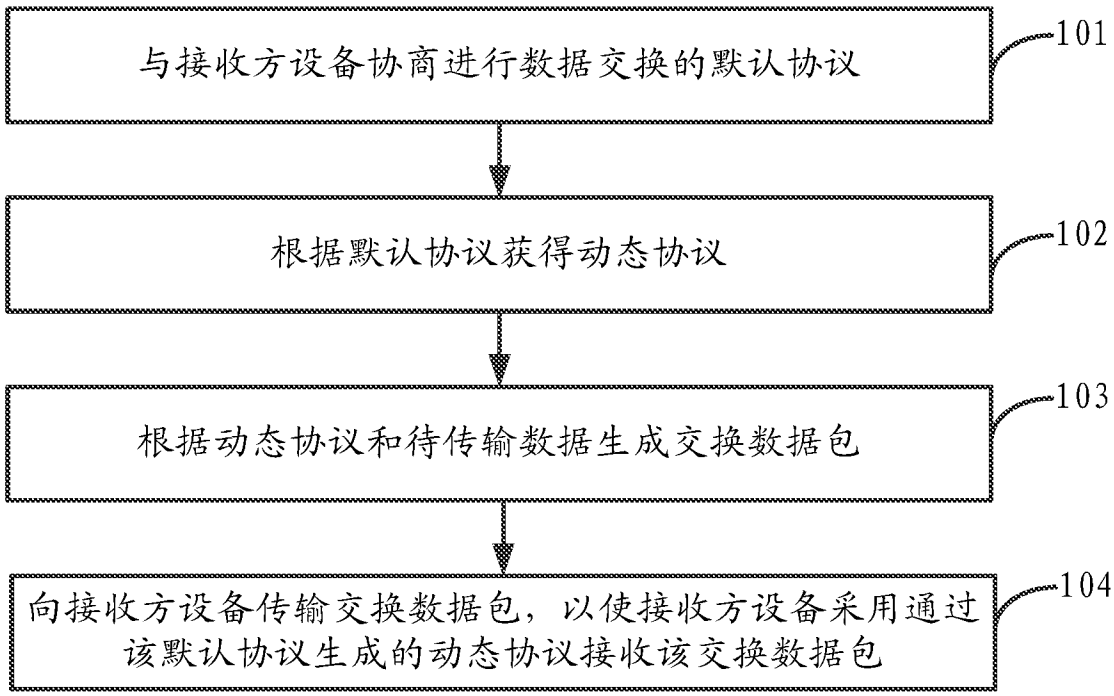
与接收方设备协商进行数据交换的默认协议
101
根据默认协议获得动态协议
102
根据动态协议和待传输数据生成交换数据包
103
向接收方设备传输交换数据包，以使接收方设备采用通过该默认协议生成的动态协议接收该交换数据包
104

图 1

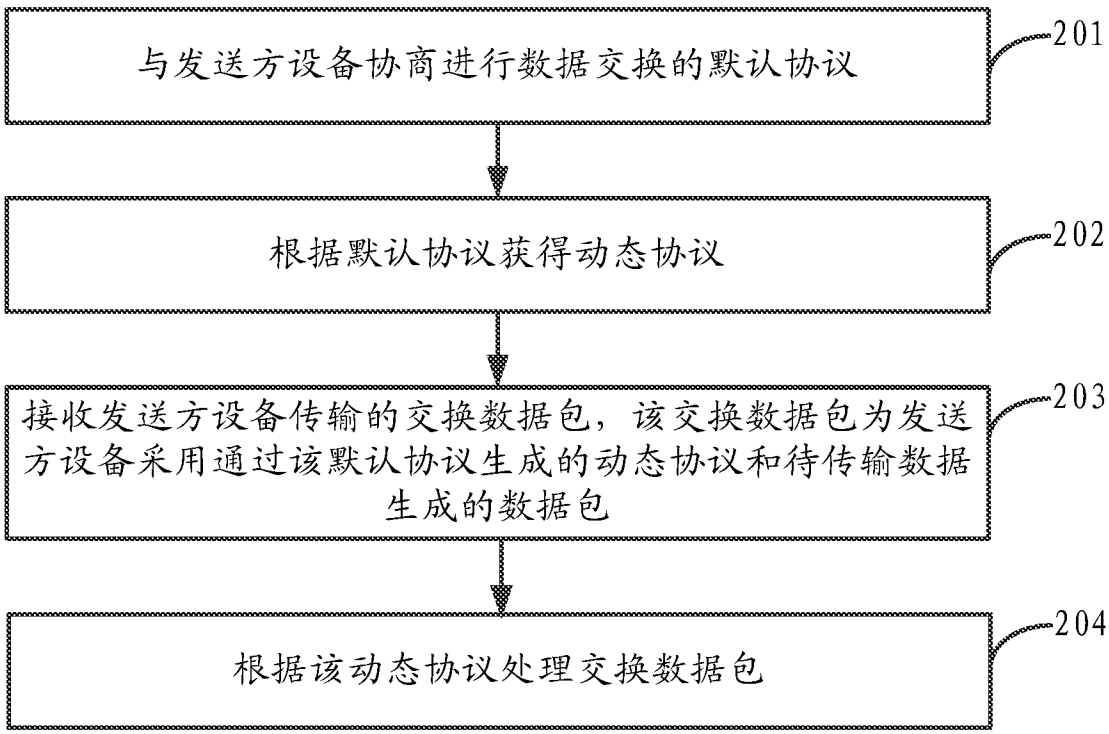
与发送方设备协商进行数据交换的默认协议
201
根据默认协议获得动态协议
202
接收发送方设备传输的交换数据包，该交换数据包为发送方设备采用通过该默认协议生成的动态协议和待传输数据生成的数据包
203
根据该动态协议处理交换数据包
204

图 2

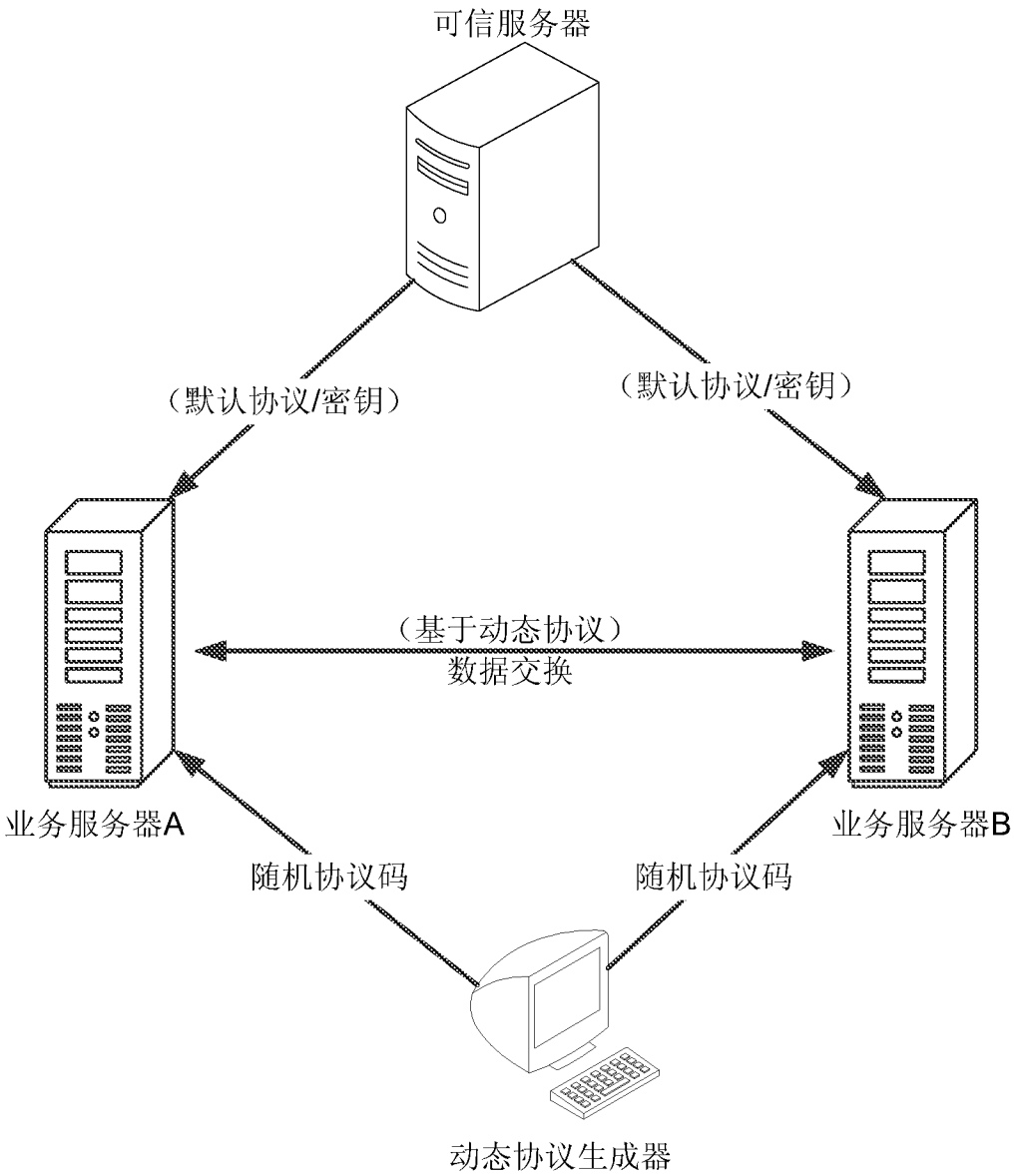
可信服务器
（默认协议/密钥）
（默认协议/密钥）
（基于动态协议）
数据交换
业务服务器A
业务服务器B
随机协议码
随机协议码
动态协议生成器

图 3

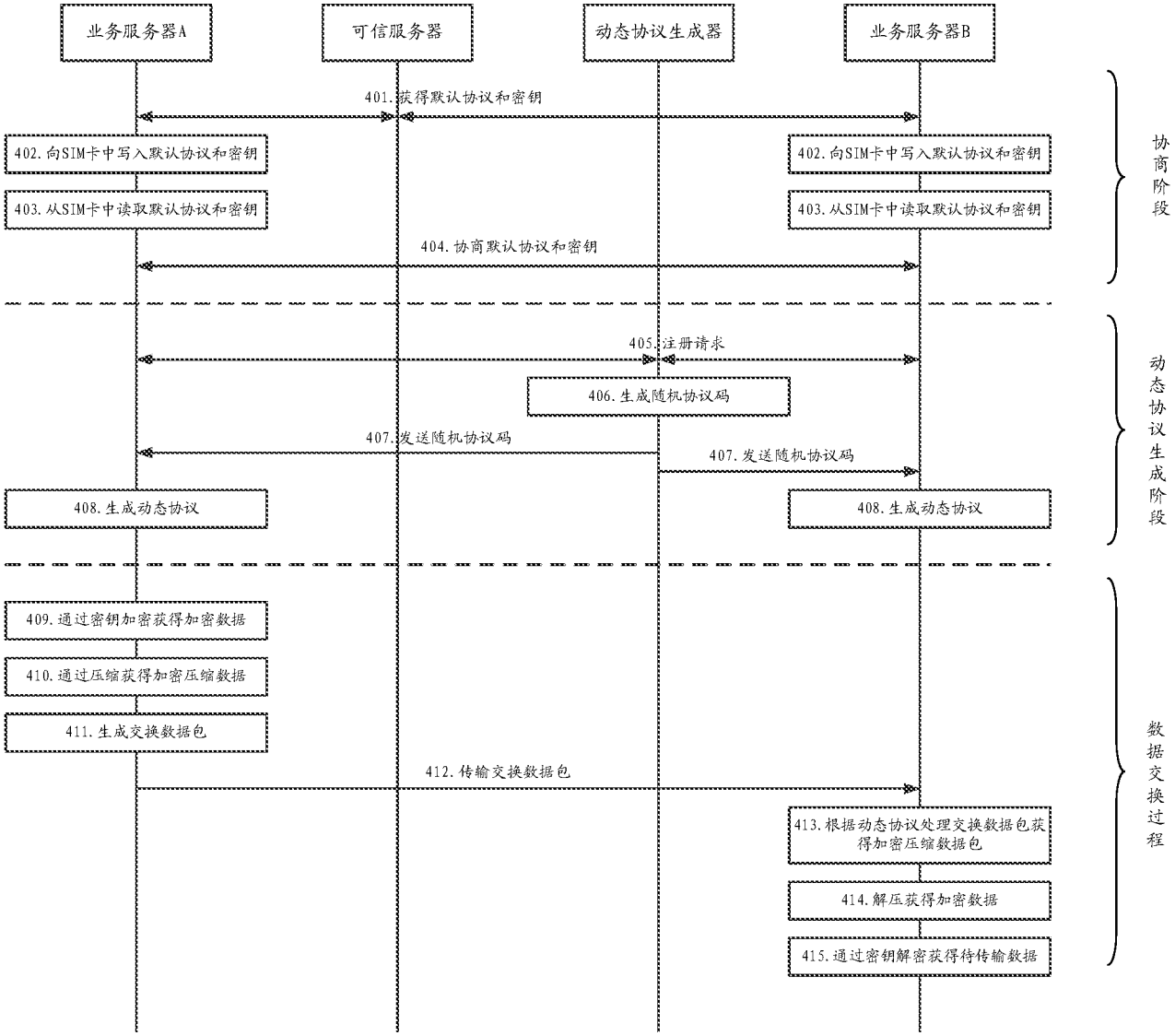
业务服务器A
可信服务器
动态协议生成器
业务服务器B
401.获得默认协议和密钥
402.向SIM卡中写入默认协议和密钥
402.向SIM卡中写入默认协议和密钥
403.从SIM卡中读取默认协议和密钥
403.从SIM卡中读取默认协议和密钥
404.协商默认协议和密钥
协商阶段
405.注册请求
406.生成随机协议码
407.发送随机协议码
407.发送随机协议码
408.生成动态协议
408.生成动态协议
动态协议生成阶段
409.通过密钥加密获得加密数据
410.通过压缩获得加密压缩数据
411.生成交换数据包
412.传输交换数据包
413.根据动态协议处理交换数据包获得加密压缩数据包
414.解压获得加密数据
415.通过密钥解密获得待传输数据
数据交换过程

图 4A

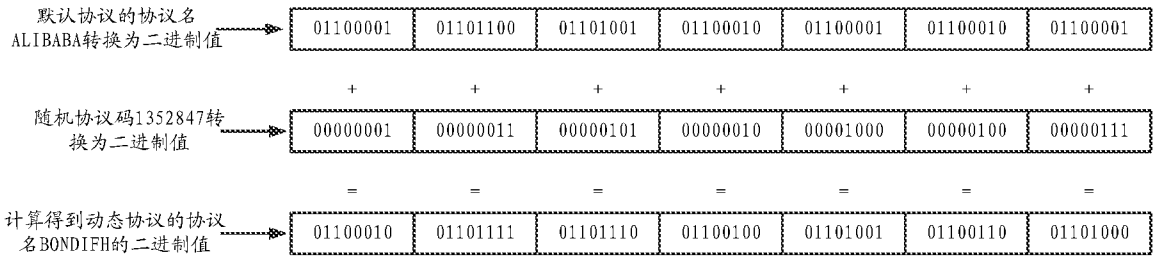
默认协议的协议名ALIBABA转换为二进制值
01100001 01101100 01101001 01100010 01100001 01100010 01100001
+ + + + + + +
随机协议码1352847转换为二进制值
00000001 00000011 00000101 00000010 00001000 00000100 00000111
= = = = = = =
计算得到动态协议的协议名BONDIFH的二进制值
01100010 01101111 01101110 01100100 01101001 01100110 01101000

图 4B

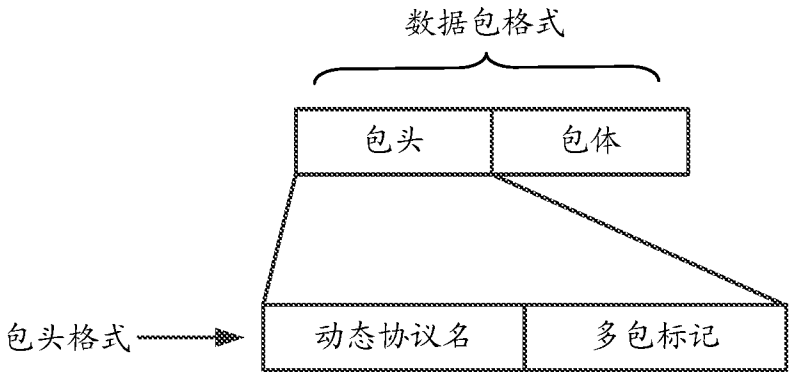
数据包格式
包头
包体
包头格式
动态协议名
多包标记

图 4C

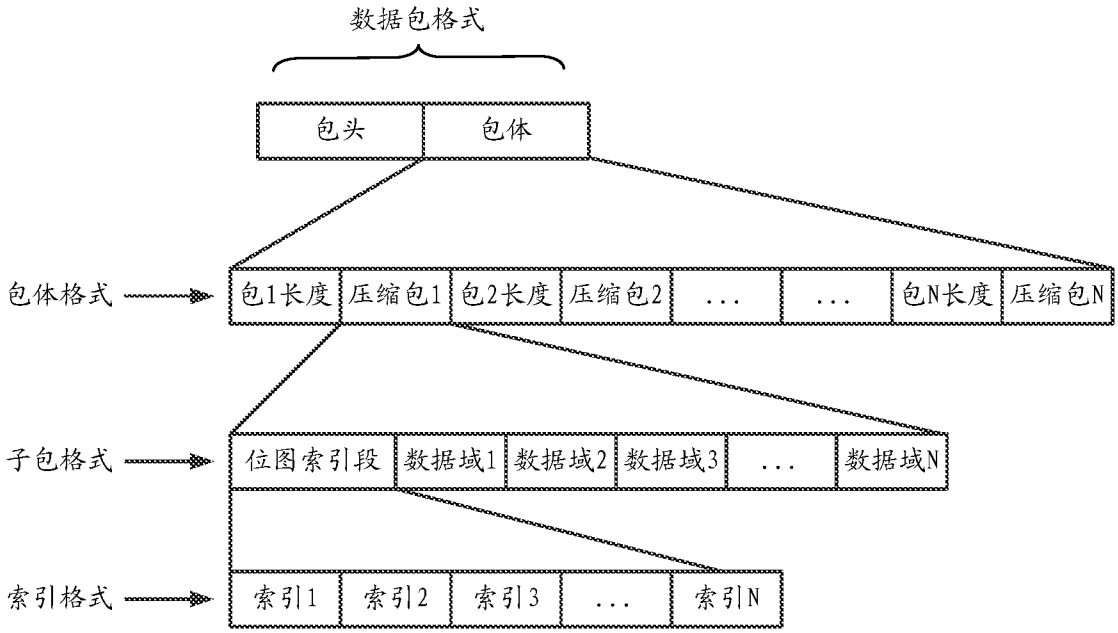
数据包格式
包头
包体
包体格式
包1长度
压缩包1
包2长度
压缩包2
...
...
包N长度
压缩包N
子包格式
位图索引段
数据域1
数据域2
数据域3
...
数据域N
索引格式
索引1
索引2
索引3
...
索引N

图 4D

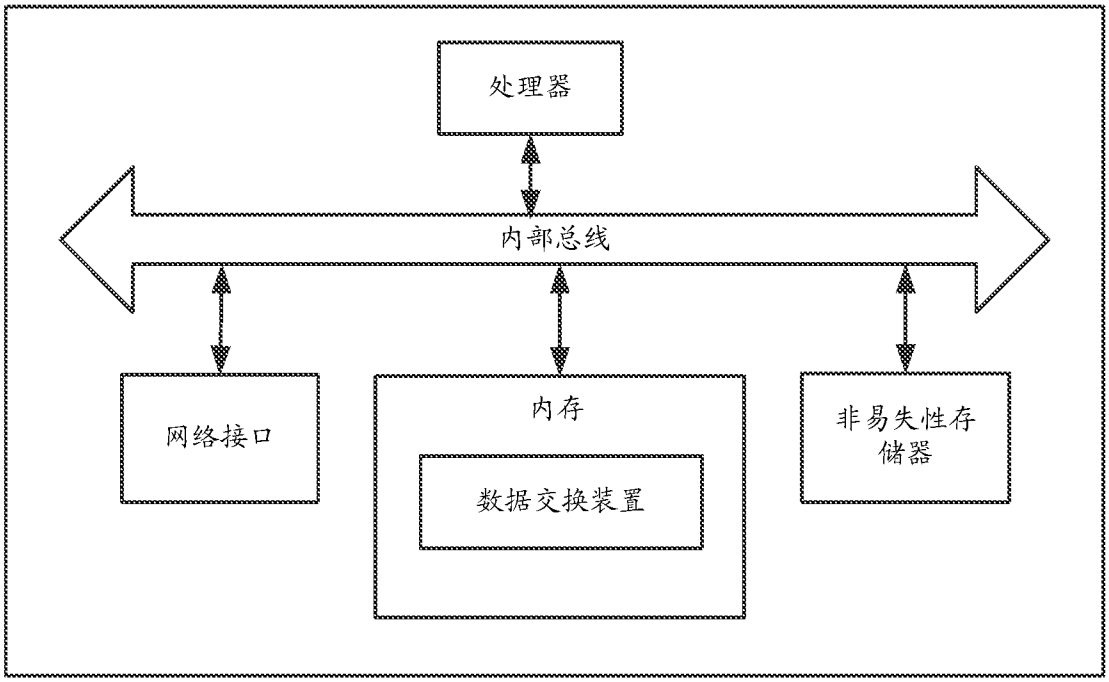
处理器
内部总线
网络接口
内存
数据交换装置
非易失性存储器

图 5

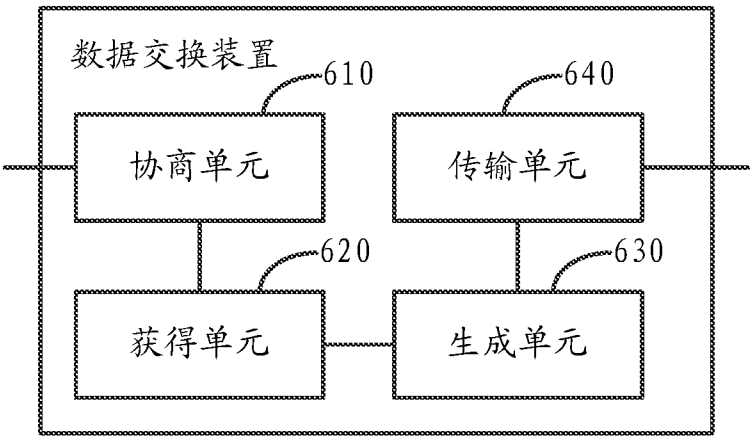
数据交换装置
610
640
协商单元
传输单元
620
630
获得单元
生成单元

图 6

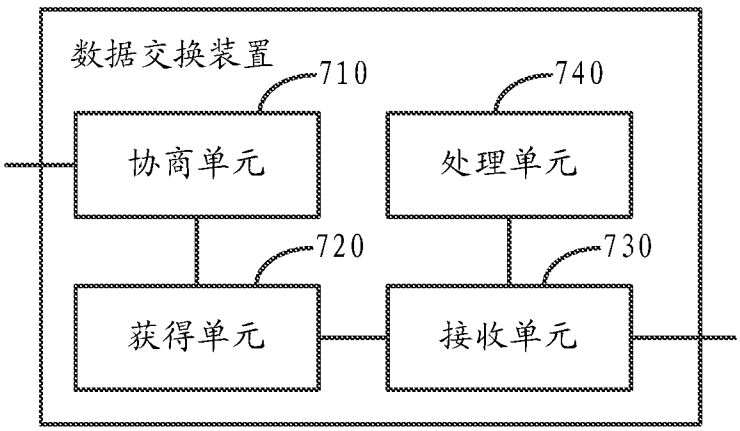
数据交换装置
710
740
协商单元
处理单元
720
730
获得单元
接收单元

图 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/076413

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/70 (2013.01) 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; H04W; H04Q

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

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

CNPAT, WPI, EPODOC: sender, receiver, protocol, default, dynamic, encrypt+, key, produce, create, make

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 103858389 A (HUAWEI TECHNOLOGIES CO., LTD.), 11 June 2014 (11.06.2014), description, paragraphs [0064]-[0073], and figures 1-2	1-32
A	CN 102420740 A (ZTE CORP.), 18 April 2012 (18.04.2012), the whole document	1-32
A	CN 101163145 A (HUAWEI TECHNOLOGIES CO., LTD.), 16 April 2008 (16.04.2008), the whole document	1-32
A	US 2008288576 A1 (INTERNATIONAL BUSINESS MACHINES C0RPORAION), 20 November 2008 (20.11.2008), the whole document	1-32

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

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 May 2016 (19.05.2016)	**12 June 2016 (12.06.2016)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **ZHANG, Nan** Telephone No.: (86-10) **010-62413413**

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/076413

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103858389 A	11 June 2014	None	
CN 102420740 A	18 April 2012	WO 2012040971 A1	05 April 2012
CN 101163145 A	16 April 2008	None	
US 2008288576 A1	20 November 2008	CN 1787530 A	14 June 2006
		US 2006126812 A1	15 June 2006

国际检索报告

国际申请号
PCT/CN2016/076413

A. 主题的分类

H04L 12/70(2013.01)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; H04W; H04Q

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNPAT,WPI,EPODOC:发送方，接收方，协议，默认，动态，密钥，加密，生成，产生，sender，receiver，protocol，default，dynamic，encrypt+，key，produce，create，make

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
A	CN 103858389 A (华为技术有限公司) 2014年 6月 11日 (2014-06-11) 说明书第[0064]-[0073]段，附图1-2	1-32
A	CN 102420740 A (中兴通讯股份有限公司) 2012年 4月 18日 (2012-04-18) 全文	1-32
A	CN 101163145 A (华为技术有限公司) 2008年 4月 16日 (2008-04-16) 全文	1-32
A	US 2008288576 A1 (INTERNATIONAL BUSINESS MACHINES CORPORAION) 2008年 11月 20日 (2008-11-20) 全文	1-32

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

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

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

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

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

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

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2016年 5月 19日	2016年 6月 12日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	张楠
传真号 (86-10)62019451	电话号码 (86-10)010-62413413

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/076413

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	103858389	A	2014年 6月 11日		无		
CN	102420740	A	2012年 4月 18日	WO	2012040971	A1	2012年 4月 5日
CN	101163145	A	2008年 4月 16日		无		
US	2008288576	A1	2008年 11月 20日	CN	1787530	A	2006年 6月 14日
				US	2006126812	A1	2006年 6月 15日