

## 一种数据传输方法、装置、存储介质及电子设备

### 技术领域

[01]本说明书涉及通信技术领域，尤其涉及一种数据传输方法、装置、存储介质及电子设备。

### 背景技术

[02]目前，客户端和服务端通过握手协议建立连接后，服务器可以创建一个会话 Session（即客户端服务器进行通讯的过程），当客户端与服务端的一段通讯结束后，服务器可以将创建的会话保存起来，以待该客户端再次访问时，服务器可以再次使用已经保存的会话，以与客户端继续进行通讯（即不用重新进行握手）。

[03]但是，服务器往往与大量的客户端并发进行通讯，这就导致服务器保存的与不同客户端之间的会话将会占用服务器的大量内存，这就需要对服务器的内存有着更加严格的要求，并且，如果出现内存占用过高的情况，可能导致服务器的运行出现异常，甚至是发生隐私数据泄露的情况。

### 发明内容

[04]本说明书提供一种数据传输方法、装置、存储介质及电子设备，以解决相关技术存在的服务器中保存的会话占用内容较高的问题。

[05]本说明书采用下述技术方案：本说明书提供了一种数据传输方法，所述方法应用于服务器，包括：响应于客户端发送的连接请求，判断所述连接请求中是否携带有会话状态信息，所述会话状态信息中包含所述服务器与所述客户端通过创建的会话进行数据传输所基于的参数，以及会话标识；若是，则根据所述连接请求中携带的会话状态信息，恢复与所述客户端之间的会话，并通过恢复的会话，与所述客户端进行数据传输；若否，则创建与所述客户端之间的会话，并将针对创建出的会话所生成的会话状态信息发送给所述客户端，以使所述客户端进行保存。

[06]可选地，将针对创建出的会话所生成的会话状态信息发送给所述客户端，具体包括：通过预先确定出的各加密密钥，对针对创建出的会话所生成的会话状态信息进行加密，得到加密后会话状态信息；将所述加密后会话状态信息发送给所述客户端。

[07]可选地，确定各加密密钥，具体包括：获取初始密钥以及N个密钥参数，N为正整数；根据得到的第N-1个加密密钥以及第N个密钥参数，生成第N个加密密钥，其中，第一个加密密钥是通过所述初始密钥和第一个密钥参数生成的。

[08]可选地，通过预先确定出的各加密密钥，对针对创建出的会话所生成的会话状态信息进行加密，得到加密后会话状态信息，具体包括：按照各加密密钥加密所述会话状态信息的先后顺序，依次使用各加密密钥对所述会话状态信息进行加密，得到加密后会话状态信息；其中，针对每个加密密钥，通过该加密密钥，对上一加密密钥加密后得到的会话状态信息进行加密，得到经过该加密密钥加密后的会话状态信息。

[09]可选地，通过该加密密钥，对上一加密密钥加密后得到的会话状态信息进行加密，得到经过该加密密钥加密后的会话状态信息，具体包括：通过该加密密钥，对上一加密密钥加密后得到的会话状态信息进行加密，得到基础加密会话状态信息；通过至少一种预设的置换方法，对所述基础加密会话状态信息进行置换，得到经过该加密密钥加密后的会话状态信息，所述置换方法包括：非线性置换、线性置换、反序置换中的至少一种。

[10]可选地，根据所述连接请求中携带的会话状态信息，恢复与所述客户端之间的会话，具体包括：根据预设的完整性校验算法，对所述连接请求中携带的会话状态信息进行完整性验证；若确定所述会话状态信息完整后，根据所述会话状态信息，恢复与所述客户端之间的会话。

[11]可选地，恢复与所述客户端之间的会话，具体包括：根据所述会话状态信息中携带的密钥标识，确定所述会话状态信息对应的各解密密钥；通过所述各解密密钥，对所述会话状态信息进行解密，得到解密后的会话状态信息；根据所述解密后的会话状态信息，恢复与所述客户端之间的会话。

[12]本说明书提供了一种数据传输方法，所述方法应用于客户端，包括：客户端确定目标服务器，所述目标服务器用于与所述客户端进行数据传输；判断所述客户端本地是否保存有与所述目标服务器进行会话所基于的会话状态信息；若是，将携带有所述会话状态信息的连接请求发送给所述目标服务器，以使所述目标服务器根据所述会话状态信息，恢复与所述客户端之间的会话，并通过恢复的会话，进行数据传输；若否，向所述目标服务器发送连接请求，以使所述目标服务器根据所述连接请求，创建与所述客户端之间的会话。

[13]本说明书提供了一种数据传输装置，包括：判断模块，用于响应于客户端发送的连

接请求，判断所述连接请求中是否携带有会话状态信息，所述会话状态信息中包含所述服务器与所述客户端通过创建的会话进行数据传输所基于的参数，以及会话标识；恢复模块，用于在确定所述连接请求中携带有会话状态信息时，根据所述连接请求中携带的会话状态信息，恢复与所述客户端之间的会话，并通过恢复的会话，与所述客户端进行数据传输；创建模块，用于在确定所述连接请求中未携带有会话状态信息时，创建与所述客户端之间的会话，并将针对创建出的会话所生成的会话状态信息发送给所述客户端，以使所述客户端进行保存。

[14]本说明书提供了一种数据传输装置，包括：确定模块，用于确定目标服务器，所述目标服务器用于与所述客户端进行数据传输；判断并执行模块，用于判断所述客户端本地是否保存有与所述目标服务器进行会话所基于的会话状态信息；若是，将携带有所述会话状态信息的连接请求发送给所述目标服务器，以使所述目标服务器根据所述会话状态信息，恢复与所述客户端之间的会话，并通过恢复的会话，进行数据传输；若否，向所述目标服务器发送连接请求，以使所述目标服务器根据所述连接请求，创建与所述客户端之间的会话。

[15]本说明书提供了一种计算机可读存储介质，所述存储介质存储有计算机程序，所述计算机程序被处理器执行时实现上述数据传输方法。

[16]本说明书提供了一种电子设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时实现上述数据传输方法。

[17]本说明书采用的上述至少一个技术方案能够达到以下有益效果：在本说明书提供的数据传输方法，响应于客户端发送的连接请求，判断连接请求中是否携带有会话状态信息，会话状态信息中包含服务器与客户端通过创建的会话进行数据传输所基于的参数，以及会话标识，若是，则根据连接请求中携带的会话状态信息，恢复与客户端之间的会话，并通过恢复的会话，与客户端进行数据传输，若否，则创建与客户端之间的会话，并将针对创建出的会话所生成的会话状态信息发送给客户端，以使客户端进行保存。

[18]从上述方法中可以看出，服务器可以将与客户端的会话的会话状态信息，发送给客户端保存，以使在客户端需要再次使用该会话时，可以将会话状态信息携带在连接请求中发送给服务器，服务器可以根据客户端发送的携带有会话状态信息的连接请求，恢复与客户端之间的会话，从而降低了服务器保存的与各个客户端的会话对服务器内存的占用。

## 附图说明

[19]此处所说明的附图用来提供对本说明书的进一步理解，构成本说明书的一部分，本说明书的示意性实施例及其说明用于解释本说明书，并不构成对本说明书的不当限定。在附图中：

[20]图 1 为本说明书中提供的一种数据传输方法的流程示意图；

[21]图 2 为本说明书中提供的另一种数据传输方法的流程示意图；

[22]图 3 为本说明书提供的一种数据传输装置的示意图；

[23]图 4 为本说明书提供的另一种数据传输装置的示意图；

[24]图 5 为本说明书提供的一种对应于图 1 的电子设备的示意图。

## 具体实施方式

[25]为使本说明书的目的、技术方案和优点更加清楚，下面将结合本说明书具体实施例及相应的附图对本说明书技术方案进行清楚、完整地描述。显然，所描述的实施例仅是本说明书一部分实施例，而不是全部的实施例。基于本说明书中的实施例，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他实施例，都属于本说明书保护的范围。

[26]目前，当客户端与服务器通过握手协议建立连接后，服务器会创建一个与客户端的会话 Session，并将会话的唯一标识信息 Session ID 发送给客户端，进而可以通过会话与客户端进行数据传输，当客户端结束本次会话后，服务器可以将与客户端的会话状态保存下来，以便于客户端在下次需要进行数据传输时，可以不用再重新通过握手协议建立连接，而是可以根据客户端中保存的 Session ID 直接恢复会话，并进行数据传输。

[27]但是，由于服务器往往需要同时与大量的客户端并发进行数据传输，这就使得服务器需要保存大量的与不同客户端的会话，从而导致服务器的内存被大量占用。除此之外，在分布式服务器集群（即，单个服务器在使用的过程中，往往由于自身的硬件资源以及其他条件限制，而导致单个服务器的性能不能无限增加，因此，为了对服务器的性能进行进一步地的拓展，就可以使用多个服务器共同提供服务，也就是服务器集群的方式来提供服务）中，客户端每次访问的服务器可能并不是同一个，这就导致新的服务器并不能根据客户端中保存的 Session ID 恢复客户端与上一个服务器之间的会话，从而就导致

在服务器集群中并不能很好的根据 Session ID 实现会话复用。

[28]以下结合附图，详细说明本说明书各实施例提供的技术方案。

[29]图 1 为本说明书中提供的一种软件管理方法的流程示意图，包括以下步骤 S100 至 S104。

[30]S100: 响应于客户端发送的连接请求，判断所述连接请求中是否携带有会话状态信息，所述会话状态信息中包含所述服务器与所述客户端通过创建的会话进行数据传输所基于的参数，以及会话标识，若是，则执行步骤 S102，若否，则执行步骤 S104。

[31]在本说明书中，服务器在接收到客户端发送的连接请求后，可以响应于客户端发送的连接请求，判断接收到的连接请求中是否携带有会话状态信息，若是，则根据会话状态信息，恢复与客户端之间的会话，并通过恢复的会话，与客户端进行数据传输，若否，则创建与客户端之间的会话，并通过创建的会话，与客户端进行数据传输，其中，会话状态信息中包含服务器与客户端通过会话进行数据传输所基于的参数，例如：客户端和服务器协商的加密协议的版本 version、客户端和服务器协商的进行数据通讯时使用的密码套件 cipher、客户端和服务器协商的进行数据通讯时使用的密钥 master\_key、会话状态信息可以被复用的时间 timestamp 等，以及所述会话的会话标识 Session ID。

[32]S102: 根据所述连接请求中携带的会话状态信息，恢复与所述客户端之间的会话，并通过恢复的会话，与所述客户端进行数据传输。

[33]服务器若确定客户端发送的连接请求中携带有会话状态信息，则可以根据客户端发送的连接请求中携带的会话状态信息，恢复服务器与客户端之间的会话，并通过恢复的会话，与客户端进行数据传输。

[34]具体地，为了防止加密后的会话状态信息在客户端保存期间被篡改，服务器在将会话状态信息发送给客户端保存之前，可以通过预设的完整性校验算法对加密后的会话状态信息进行完整性加密，其中，预设的完整性校验算法可以是诸如：哈希运算消息认证码（Keyed-Hash Message Authentication Code，HMAC）、消息摘要算法（SM3）等，对应的，在服务器需要根据客户端中携带的会话状态信息，恢复与客户端之间的会话之前，需要先对会话状态信息进行完整性校验，以下以 HMAC 算法为例，对服务器对会话状态信息进行完整性校验的过程进行详细说明。

[35]服务器在获取到客户端发送的连接请求中携带的会话状态信息后，可以根据会话状态信息的标识，从预设的配置文件中，确定出与该会话状态信息对应的 HMAC 密钥，

并通过 HMAC 密钥计算出会话状态信息中的密钥标识 key-name, 初始化向量 iv, 以及加密后的会话状态信息对应的 HMAC 值, 并将计算出的密钥标识 key-name, 初始化向量 iv, 以及加密后的会话状态信息对应的 HMAC 值与会话状态信息中携带的 MAC 值进行比对, 若一致, 则可以确定出会话状态信息完整。

[36]上述内容中的密钥标识 key-name 是对会话状态信息进行加密时所使用的的一套密钥对应的标识, 初始化向量 iv 是用于在对会话状态数据进行进一步加密时使用的初始化向量, 即服务器在会话状态信息进行加密后, 可以将加密过程中所使用的密钥对应的密钥标识, 以及在加密过程中使用的初始化向量保存到会话状态信息中 (需要说明的是, 这里的加密是指对上述内容中的包含有客户端和服务端协商的加密协议的版本 version、客户端和服务端协商的进行数据通讯时使用的密码套件 cipher、客户端和服务端协商的进行数据通讯时使用的密钥 master\_key、会话状态信息可以被复用的时间 timestamp 等, 以及所述会话的会话标识 Session ID 等信息的会话状态信息进行加密, 服务器在确定上述的密钥标识 key-name, 初始化向量 iv, 以及加密后的会话状态信息的完整性之后, 可以根据上述的密钥标识 key-name, 初始化向量 iv 对加密后的会话状态信息进行解密)。

[37]进一步地, 在服务器对客户端再次发送的连接请求中携带的会话状态信息进行完整性验证后, 可以根据会话状态信息中携带的密钥标识, 确定会话状态信息对应的各解密密钥, 并通过各解密密钥, 对会话状态信息进行解密, 得到解密后的会话状态信息, 根据解密后的会话状态信息, 恢复与客户端之间的会话。

[38]进一步地, 当服务器得到解密后的会话状态信息之后, 可以确定解密后的会话状态信息中携带的会话状态信息可以被复用的时间 timestamp, 并判断与客户端进行上次会话的时间, 与客户端再次发送连接请求的时间之间的时间间隔, 是否超过会话状态信息可以被复用的时间 timestamp, 若否, 则恢复与客户端之间的会话, 若是, 则服务器需要重新通过预设的握手协议与客户端进行连接。

[39]S104: 创建与所述客户端之间的会话, 并将针对创建出的会话所生成的会话状态信息发送给所述客户端, 以使所述客户端进行保存。

[40]服务器若确定客户端发送的连接请求中未携带有会话状态信息, 则可以接收客户端发送的连接请求, 并响应于接收到的连接请求, 按照预设的握手协议, 与客户端互相进行身份验证, 并与客户端协商确定在数据传输过程中使用的加密协议的版本 version, 与客户端协商确定数据传输所使用的密码套件 cipher、以及密钥 master\_key 等信息后, 创建与客户端之间的会话。

[41]服务器在创建与客户端之间的会话后，可以针对创建出的会话生成会话状态信息，将会话状态信息发送给客户端，以使客户端在当前会话结束后需要再次发起会话时使用。

[42]进一步地，当服务器需要将会话状态信息发送给客户端时，服务器可以通过预设的加密方法对会话状态信息进行加密，并将加密后的会话状态信息发送给客户端。

[43]上述内容中，服务器对会话状态信息进行加密的方法可以通过预先确定出的各加密密钥，对会话状态信息进行加密，得到加密后会话状态信息，并将加密后会话状态信息发送给客户端。

[44]具体地，服务器可以按照预先确定出的各加密密钥加密会话状态信息的先后顺序，依次使用各加密密钥对会话状态信息进行加密，得到加密后会话状态信息，其中，针对每个加密密钥，通过该加密密钥，对上一加密密钥加密后得到的会话状态信息进行加密，得到经过该加密密钥加密后的会话状态信息。

[45]其中，服务器通过该加密密钥对上一加密密钥加密后得到的会话状态信息进行加密的方法可以是，服务器可以按照预设的运算方式，确定该加密密钥与上一加密密钥加密后的会话状态信息的运算值，这里的运算方式可以是诸如：异或运算、与运算、求和运算等，相应的若服务器使用的运算方式为异或运算时，上述的运算值即为异或运算值。

[46]进一步地，服务器可以将确定出的该加密密钥与上一加密密钥加密后的会话状态信息的运算值，作为基础加密会话状态，进而可以通过至少一种预设的置换方法，对该基础加密会话状态信息进行置换，得到最终输出的经过该加密密钥加密后的会话状态信息，这里的置换方法包括：非线性置换（例如：对照 S 盒 Sbox 进行置换）、线性置换（例如：通过左移运算进行置换）、反序置换（即，将基础加密会话状态信息中的每个值的顺序进行调整，例如：假设反序置换前的值为：（a1、a2、a3、a4），则进行反序置换后的值就为（a4、a3、a2、a1）中的至少一种。

[47]上述内容中，每轮加密所使用的各加密密钥的确定方法可以是获取初始密钥以及 N 个密钥参数，这里的 N 为正整数，根据得到的第 N-1 个加密密钥以及第 N 个密钥参数，生成第 N 个加密密钥，其中，第一个加密密钥是通过初始密钥和第一个密钥参数生成的，这里的密钥参数是预设的一组固定的参数。

[48]具体地，根据得到的第 N-1 个密钥以及第 N 个密钥参数，生成第 N 个密钥的方法可以是服务器可以按照预设的运算方式，确定第 N-1 个加密密钥以及第 N 个密钥参数的运算值，这里的运算方式可以是诸如：异或运算、与运算、求和运算等，进一步地，通过

预设的置换算法，对确定出的第 N-1 个加密密钥以及第 N 个密钥参数的运算值进行置换，从而得到第 N 个加密密钥。

[49]除此之外，服务器还可以将需要加密的会话状态信息进行分组（例如：将会话状态信息中的每 128 位为一组，也就是每 16 个字节为一组），然后分别针对每组会话状态信息，通过上述的方法进行加密，得到每组会话状态信息加密后的结果，进而可以针对每组的加密后的会话状态信息，将该组的加密后的会话状态信息与前一组的加密后的会话状态信息按照预设的算法进行运算（例如：进行异或运算），得到该组加密后的会话状态信息，经过进一步加密后的会话状态信息，其中，第一组加密后的会话状态信息可以与预设的初始值 iv 进行预算，以得到第一种加密后的会话状态信息，经过进一步加密后的会话状态信息。

[50]进一步地，服务器可以确定上述内容中所使用的各加密密钥对应的一个密钥标识 key-name（可以通过随机数生成器等方法确定密钥标识，也可以从配置文件中获取的），并通过预先确定的 HMAC 密钥（可以是随机数生成器生成的，也可以是从配置文件中获取的）确定该密钥标识、上述内容中使用的初始值 iv、最终得到的加密后的会话状态信息的 HMAC 值，以及与该密钥标识、上述内容中使用的初始值 iv、最终得到的加密后的会话状态信息的 HMAC 值对应的消息验证码 MAC 值，并将该密钥标识、上述内容中使用的初始值 iv、以及最终得到的加密后的会话状态信息的 HMAC 值，以及上述的 MAC 值发送给客户端以使客户端进行保存，其中，消息验证码 MAC 用于校验会话状态信息的完整性。

[51]需要说明的是，服务器使用的对会话状态信息进行加密的加密密钥，可以通过上述方法生成的，也可以是从预先设置的配置文件（这里的配置文件中保存有由开发人员设置的多套加密密钥，其中，每套加密密钥对应着一个密钥标识，且一个服务器集群中的若干各服务器可以使用同一套配置文件）中获取的各加密密钥，若服务器使用的各加密密钥是从配置文件中获取的，则与该服务器处于同一集群的其他服务器也可以根据客户端发送的连接请求中携带的会话状态信息中的密钥标识，从配置文件中确定出相应的解密密钥，从而通过解密密钥，对会话状态信息进行解密，并恢复与客户端之间的会话，进而可以实现客户端与服务器集群中的任意一个服务器之间会话，在该服务器集群的不同服务器上的复用。

[52]从上述内容中可以看出，服务器可以在创建与客户端之间的会话后，会话的会话状态信息通过预设的加密算法进行加密，并将加密后的会话状态信息发送给客户端中保存，在客户端需要复用会话时，可以将客户端中保存的会话状态信息携带在连接请求中发送

给服务器，以使服务器能够根据会话状态信息恢复会话，从而减少了服务器保存的与各个客户端的会话对服务器内存的占用，以及能够实现在服务器集群中进行会话的复用。

[53]为了对上述内容进行进一步地的详细说明，本说明书中还提供了一种数据传输的方法，如图 2 所示。

[54]图 2 为本说明书中提供的另一种数据传输的方法的流程示意图，包括以下步骤 S200 至 S206。

[55]S200: 客户端确定目标服务器，所述目标服务器用于与所述客户端进行数据传输。

[56]S202: 判断所述客户端本地是否保存有与所述目标服务器进行会话所基于的会话状态信息，若是，则执行步骤 S204，若否，则执行步骤 S206。

[57]S204: 将携带有所述会话状态信息的连接请求发送给所述目标服务器，以使所述目标服务器根据所述会话状态信息，恢复与所述客户端之间的会话，并通过恢复的会话，进行数据传输。

[58]S206: 向所述目标服务器发送连接请求，以使所述目标服务器根据所述连接请求，创建与所述客户端之间的会话。

[59]客户端可以在需要向服务器发送连接请求之前，可以先确定接收连接请求的服务器，作为目标服务器，进而可以判断客户端本地中是否保存有与目标服务器进行会话所基于的会话状态信息，若确定没有，则可以向服务器发送连接请求，并按照预设的握手协议与服务器进行身份验证，以及与服务器协商确定在数据传输过程中使用的加密协议的版本 version，与客户端协商确定数据传输所使用的密码套件 cipher、以及密钥 master\_key 等信息后，响应于服务器创建的与客户端之间的会话，与服务器进行数据传输，并接收服务器发送的会话状态信息并保存。

[60]若客户端确定本地保存有与目标服务器进行会话所基于的会话状态信息时，客户端可以从本地获取会话状态信息，然后向服务器发送携带有会话状态信息的连接请求，以使服务器根据携带有所述会话状态信息的连接请求，恢复与客户端之间的会话，并通过服务器恢复的与客户端之间的会话，与服务器进行数据传输。

[61]需要说明的是，由于保存在客户端中的会话状态信息是经过服务器加密的，因此，客户端只能保存该会话状态信息，而并不能读取到会话状态信息中的具体内容，也不能对会话状态信息进行修改。

[62]从上述内容中可以看出，客户端可以将服务器发送的加密后的会话状态信息保存起来，并在再次向服务器发送连接请求时，将会话状态信息携带在连接请求中发送给服务器，从而实现了会话的复用，进而减少了服务器保存的与各个客户端的会话对服务器内

存的占用。

[63]以上为本说明书的一个或多个实施例提供的数据传输方法，基于同样的思路，本说明书还提供了相应的数据传输装置，如图 3、图 4 所示。

[64]图 3 为本说明书提供的一种数据传输装置的示意图，包括：判断模块 301，用于响应于客户端发送的连接请求，判断所述连接请求中是否携带有会话状态信息，所述会话状态信息中包含所述服务器与所述客户端通过创建的会话进行数据传输所基于的参数，以及会话标识；恢复模块 302，用于在确定所述连接请求中携带有会话状态信息时，根据所述连接请求中携带的会话状态信息，恢复与所述客户端之间的会话，并通过恢复的会话，与所述客户端进行数据传输；创建模块 303，用于在确定所述连接请求中未携带有会话状态信息时，创建与所述客户端之间的会话，并将针对创建出的会话所生成的会话状态信息发送给所述客户端，以使所述客户端进行保存。

[65]可选地，所述创建模块 303 具体用于，通过预先确定出的各加密密钥，对针对创建出的会话所生成的会话状态信息进行加密，得到加密后会话状态信息；将所述加密后会话状态信息发送给所述客户端。

[66]可选地，所述创建模块 303 具体用于，获取初始密钥以及 N 个密钥参数，N 为正整数；根据得到的第 N-1 个加密密钥以及第 N 个密钥参数，生成第 N 个加密密钥，其中，第一个加密密钥是通过所述初始密钥和第一个密钥参数生成的。

[67]可选地，所述创建模块 303 具体用于，按照各加密密钥加密所述会话状态信息的先后顺序，依次使用各加密密钥对所述会话状态信息进行加密，得到加密后会话状态信息；其中针对每个加密密钥，通过该加密密钥，对上一加密密钥加密后得到的会话状态信息进行加密，得到经过该加密密钥加密后的会话状态信息。

[68]可选地，所述创建模块 303 具体用于，通过该加密密钥，对上一加密密钥加密后得到的会话状态信息进行加密，得到基础加密会话状态信息；通过至少一种预设的置换方法，对所述基础加密会话状态信息进行置换，得到经过该加密密钥加密后的会话状态信息，所述置换方法包括：非线性置换、线性置换、反序置换中的至少一种。

[69]可选地，所述恢复模块 302 具体用于，根据预设的完整性校验算法，对所述连接请求中携带的会话状态信息进行完整性验证；若确定所述会话状态信息完整后，根据所述会话状态信息，恢复与所述客户端之间的会话。

[70]可选地，所述恢复模块 302 具体用于，根据所述会话状态信息中携带的密钥标识，确定所述会话状态信息对应的各解密密钥；通过所述各解密密钥，对所述会话状态信息进行解密，得到解密后的会话状态信息；根据所述解密后的会话状态信息，恢复与所述

客户端之间的会话。

[71]图 4 为本说明书提供的另一种数据传输装置的示意图，包括：确定模块 401，用于确定目标服务器，所述目标服务器用于与所述客户端进行数据传输；判断并执行模块 402，用于判断所述客户端本地是否保存有与所述目标服务器进行会话所基于的会话状态信息；若是，将携带有所述会话状态信息的连接请求发送给所述目标服务器，以使所述目标服务器根据所述会话状态信息，恢复与所述客户端之间的会话，并通过恢复的会话，进行数据传输；若否，向所述目标服务器发送连接请求，以使所述目标服务器根据所述连接请求，创建与所述客户端之间的会话。

[72]本说明书还提供了一种计算机可读存储介质，该存储介质存储有计算机程序，计算机程序可用于执行上述图 1 提供的一种数据传输方法。

[73]本说明书还提供了图 5 所示的一种对应于图 1 的电子设备的示意结构图。如图 5，在硬件层面，该电子设备包括处理器、内部总线、网络接口、内存以及非易失性存储器，当然还可能包括其他业务所需要的硬件。处理器从非易失性存储器中读取对应的计算机程序到内存中然后运行，以实现上述图 1 的数据传输方法。当然，除了软件实现方式之外，本说明书并不排除其他实现方式，比如逻辑器件抑或软硬件结合的方式等等，也就是说以下处理流程的执行主体并不限于各个逻辑单元，也可以是硬件或逻辑器件。

[74]在 20 世纪 90 年代，对于一个技术的改进可以很明显地区分是硬件上的改进（例如，对二极管、晶体管、开关等电路结构的改进）还是软件上的改进（对于方法流程的改进）。然而，随着技术的发展，当今的很多方法流程的改进已经可以视为硬件电路结构的直接改进。设计人员几乎都通过将改进的方法流程编程到硬件电路中来得到相应的硬件电路结构。因此，不能说一个方法流程的改进就不能用硬件实体模块来实现。例如，可编程逻辑器件（Programmable Logic Device, PLD）（例如现场可编程门阵列（Field Programmable Gate Array, FPGA））就是这样一种集成电路，其逻辑功能由用户对器件编程来确定。由设计人员自行编程来把一个数字系统“集成”在一片 PLD 上，而不需要请芯片制造厂商来设计和制作专用的集成电路芯片。而且，如今，取代手工地制作集成电路芯片，这种编程也多半改用“逻辑编译器（logic compiler）”软件来实现，它与程序开发撰写时所用的软件编译器相类似，而要编译之前的原始代码也得用特定的编程语言来撰写，此称之为硬件描述语言（Hardware Description Language, HDL），而 HDL 也并非仅有一种，而是有许多种，如 ABEL（Advanced Boolean Expression Language）、AHDL（Altera Hardware Description Language）、Confluence、CUPL（Cornell University Programming Language）、HDCal、JHDL（Java Hardware Description Language）、Lava、

Lola、MyHDL、PALASM、RHDL（Ruby Hardware Description Language）等，目前最普遍使用的是 VHDL（Very-High-Speed Integrated Circuit Hardware Description Language）与 Verilog。本领域技术人员也应该清楚，只需要将方法流程用上述几种硬件描述语言稍作逻辑编程并编程到集成电路中，就可以很容易得到实现该逻辑方法流程的硬件电路。

[75]控制器可以按任何适当的方式实现，例如，控制器可以采取例如微处理器或处理器以及存储可由该（微）处理器执行的计算机可读程序代码（例如软件或固件）的计算机可读介质、逻辑门、开关、专用集成电路（Application Specific Integrated Circuit, ASIC）、可编程逻辑控制器和嵌入微控制器的形式，控制器的例子包括但不限于以下微控制器：ARC 625D、Atmel AT91SAM、Microchip PIC18F26K20 以及 Silicone Labs C8051F320，存储器控制器还可以被实现为存储器的控制逻辑的一部分。本领域技术人员也知道，除了以纯计算机可读程序代码方式实现控制器以外，完全可以通过将方法步骤进行逻辑编程来使得控制器以逻辑门、开关、专用集成电路、可编程逻辑控制器和嵌入微控制器等的形式来实现相同功能。因此这种控制器可以被认为是一种硬件部件，而对其内包括的用于实现各种功能的装置也可以视为硬件部件内的结构。或者甚至，可以将用于实现各种功能的装置视为既可以是实现方法的软件模块又可以是硬件部件内的结构。

[76]上述实施例阐明的系统、装置、模块或单元，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机。具体的，计算机例如可以为个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任何设备的组合。

[77]为了描述的方便，描述以上装置时以功能分为各种单元分别描述。当然，在实施本说明书时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

[78]本领域内的技术人员应明白，本说明书的实施例可提供为方法、系统、或计算机程序产品。因此，本说明书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，本说明书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。

[79]本说明书是参照根据本说明书实施例的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理

设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[80]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。

[81]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。

[82]在一个典型的配置中，计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[83]内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。

[84]计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体(transitory media)，如调制的数据信号和载波。

[85]还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括要素的过程、方法、商品或者设备中还存在另外的相同要素。

[86]本领域技术人员应明白，本说明书的实施例可提供为方法、系统或计算机程序产品。

因此，本说明书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，本说明书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。

[87]本说明书可以在由计算机执行的计算机可执行指令的一般上下文中描述，例如程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计算环境中实践本说明书，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

[88]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，对于系统实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[89]以上仅为本说明书的实施例而已，并不用于限制本说明书。对于本领域技术人员来说，本说明书可以有各种更改和变化。凡在本说明书的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本说明书的权利要求范围之内。

### 权利要求书

1、一种数据传输方法，所述方法应用于服务器，包括：

响应于客户端发送的连接请求，判断所述连接请求中是否携带有会话状态信息，所述会话状态信息中包含所述服务器与所述客户端通过创建的会话进行数据传输所基于的参数，以及会话标识；

若是，则根据所述连接请求中携带的会话状态信息，恢复与所述客户端之间的会话，并通过恢复的会话，与所述客户端进行数据传输；

若否，则创建与所述客户端之间的会话，并将针对创建出的会话所生成的会话状态信息发送给所述客户端，以使所述客户端进行保存。

2、如权利要求 1 所述的方法，将针对创建出的会话所生成的会话状态信息发送给所述客户端，包括：

通过预先确定出的各加密密钥，对针对创建出的会话所生成的会话状态信息进行加密，得到加密后会话状态信息；

将所述加密后会话状态信息发送给所述客户端。

3、如权利要求 2 所述的方法，确定各加密密钥，包括：

获取初始密钥以及 N 个密钥参数，N 为正整数；

根据得到的第 N-1 个加密密钥以及第 N 个密钥参数，生成第 N 个加密密钥，其中，第一个加密密钥是通过所述初始密钥和第一个密钥参数生成的。

4、如权利要求 2 所述的方法，通过预先确定出的各加密密钥，对针对创建出的会话所生成的会话状态信息进行加密，得到加密后会话状态信息，包括：

按照各加密密钥加密所述会话状态信息的先后顺序，依次使用各加密密钥对所述会话状态信息进行加密，得到加密后会话状态信息；其中

针对每个加密密钥，通过该加密密钥，对上一加密密钥加密后得到的会话状态信息进行加密，得到经过该加密密钥加密后的会话状态信息。

5、如权利要求 4 所述的方法，通过该加密密钥，对上一加密密钥加密后得到的会话状态信息进行加密，得到经过该加密密钥加密后的会话状态信息，包括：

通过该加密密钥，对上一加密密钥加密后得到的会话状态信息进行加密，得到基础加密会话状态信息；

通过至少一种预设的置换方法，对所述基础加密会话状态信息进行置换，得到经过该加密密钥加密后的会话状态信息，所述置换方法包括：非线性置换、线性置换、反序置换中的至少一种。

6、如权利要求 1 所述的方法，根据所述连接请求中携带的会话状态信息，恢复与  
所述客户端之间的会话，包括：

根据预设的完整性校验算法，对所述连接请求中携带的会话状态信息进行完整性验证；

若确定所述会话状态信息完整后，根据所述会话状态信息，恢复与所述客户端之间的会话。

7、如权利要求 2 所述的方法，恢复与所述客户端之间的会话，包括：

根据所述会话状态信息中携带的密钥标识，确定所述会话状态信息对应的各解密密钥；

通过所述各解密密钥，对所述会话状态信息进行解密，得到解密后的会话状态信息；  
根据所述解密后的会话状态信息，恢复与所述客户端之间的会话。

8、一种数据传输方法，所述方法应用于客户端，包括：

客户端确定目标服务器，所述目标服务器用于与所述客户端进行数据传输；

判断所述客户端本地是否保存有与所述目标服务器进行会话所基于的会话状态信息；

若是，将携带有所述会话状态信息的连接请求发送给所述目标服务器，以使所述目标服务器根据所述会话状态信息，恢复与所述客户端之间的会话，并通过恢复的会话，进行数据传输；

若否，向所述目标服务器发送连接请求，以使所述目标服务器根据所述连接请求，创建与所述客户端之间的会话。

9、一种数据传输装置，包括：

判断模块，用于响应于客户端发送的连接请求，判断所述连接请求中是否携带有会话状态信息，所述会话状态信息中包含服务器与所述客户端通过创建的会话进行数据传输所基于的参数，以及会话标识；

恢复模块，用于在确定所述连接请求中携带有会话状态信息时，根据所述连接请求中携带的会话状态信息，恢复与所述客户端之间的会话，并通过恢复的会话，与所述客户端进行数据传输；

创建模块，用于在确定所述连接请求中未携带有会话状态信息时，创建与所述客户端之间的会话，并将针对创建出的会话所生成的会话状态信息发送给所述客户端，以使所述客户端进行保存。

10、一种数据传输装置，包括：

确定模块，用于确定目标服务器，所述目标服务器用于与客户端进行数据传输；

判断并执行模块，用于判断所述客户端本地是否保存有与所述目标服务器进行会话所基于的会话状态信息；若是，将携带有所述会话状态信息的连接请求发送给所述目标服务器，以使所述目标服务器根据所述会话状态信息，恢复与所述客户端之间的会话，并通过恢复的会话，进行数据传输；若否，向所述目标服务器发送连接请求，以使所述目标服务器根据所述连接请求，创建与所述客户端之间的会话。

11、一种计算机可读存储介质，所述存储介质存储有计算机程序，所述计算机程序被处理器执行时实现上述权利要求 1~8 任一项所述的方法。

12、一种电子设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时实现上述权利要求 1~8 任一项所述的方法。