(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 108737334 A
(43)申请公布日 2018.11.02

(21)申请号 201710250601.1

(22)申请日 2017.04.17

(71)申请人 中国科学院微电子研究所
地址 100029 北京市朝阳区北土城西路3号 中国科学院微电子研究所

(72)发明人 李国君 陈岚

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 王宝筠

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)
A61B 5/00(2006.01)

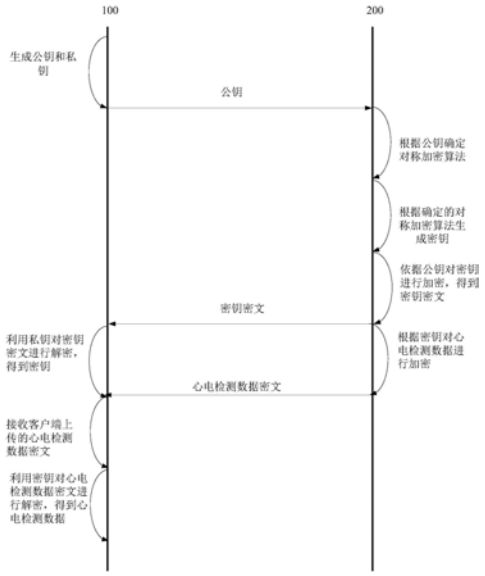
权利要求书3页 说明书10页 附图12页

(54)发明名称

一种心电检测数据上传系统及方法

(57)摘要

本申请公开了一种心电检测数据上传系统及方法，其中，所述心电检测数据上传系统利用非对称加密算法产生公钥和私钥，并将公钥下发给客户端以供客户端确定对称加密算法并生成密钥，由于私钥不在服务器和客户端中进行传输，即使根据公钥对密钥进行加密得到的密文在传输过程中被第三方截获，由于第三方不具有私钥，无法对密文进行解密，从而无法得到密钥，也就无法解密使用密钥加密的心电检测数据，这就提升了心电检测数据传输过程的保密程度；并且在该系统中，仅利用非对称加密算法产生公钥和私钥，而不直接利用非对称加密算法对心电检测数据进行加密，提升了心电检测数据的加密效率。



CN 108737334 A

1.一种心电检测数据上传系统,其特征在于,包括:服务器和至少一个客户端,其中,

所述服务器,用于生成公钥和私钥,并将所述公钥下发给客户端,以及接收所述客户端发送的密钥密文,并利用所述私钥对所述密钥密文进行解密,得到密钥,以及接收所述客户端上传的心电检测数据密文,并利用所述密钥对所述心电检测数据密文进行解密,得到心电检测数据;

所述客户端,用于接收服务器下发的所述公钥,并根据所述公钥确定对称加密算法,以及根据确定的对称加密算法生成密钥,以及依据所述公钥对所述密钥进行加密,得到密钥密文,并将所述密钥密文发送至所述服务器,以及根据所述密钥对心电检测数据进行加密,得到心电检测数据密文,并将所述心电检测数据密文上传至所述服务器。

2.根据权利要求1所述的系统,其特征在于,所述服务器,还用于:

接收所述客户端发送的上传请求密文,并利用所述密钥对所述上传请求密文进行解密,得到客户端身份验证信息,以及判断所述客户端身份验证信息是否满足预设验证条件,以及若是,则执行所述接收所述客户端上传的心电检测数据密文,这一步骤;

所述客户端,还用于当检测到客户端身份验证信息时,生成包含有所述客户端身份验证信息的心电检测数据上传请求,以及根据所述密钥对所述心电检测数据上传请求进行加密,得到上传请求密文,并将所述上传请求密文发送至所述服务器。

3.根据权利要求1所述的系统,其特征在于,所述客户端根据所述公钥确定对称加密算法,具体用于:

将所述公钥的MD5值的各位数求和,并将求和结果与对称加密算法的个数取余,根据取余结果确定选取的对称加密算法种类。

4.根据权利要求1所述的系统,其特征在于,所述将所述心电检测数据密文上传至所述服务器,具体用于:

判断所述心电检测数据密文的大小是否大于预设大小;如果是,则利用第一预设模式将所述心电检测数据密文上传至所述服务器;如果否,则利用第二预设模式将所述心电检测数据密文上传至所述服务器。

5.根据权利要求4所述的系统,其特征在于,所述利用第一预设模式将所述心电检测数据密文上传至所述服务器,具体用于:

根据当前系统状态对所述心电检测数据密文进行分块,获得多块心电检测数据密文,并通过socket连接的方式与所述服务器建立连接,上传所述多块心电检测数据密文至所述服务器。

6.根据权利要求5所述的系统,其特征在于,在所述第一预设模式中,所述服务器还用于:

根据所有所述客户端请求上传的心电检测数据密文及其客户端网络状态确定各个所述客户端的任务优先级,并根据所述客户端的任务优先级确定所述客户端的上传顺序。

7.根据权利要求4所述的系统,其特征在于,所述利用第二预设模式将所述心电检测数据密文上传至所述服务器,具体用于:

利用Web Service接口与所述服务器建立连接,并将所述心电检测数据密文上传至所述服务器。

8.一种心电检测数据上传方法,其特征在于,应用于服务器,所述心电检测数据上传方

法包括：

生成公钥和私钥，并将所述公钥下发给客户端；

接收所述客户端发送的密钥密文，并利用所述私钥对所述密钥密文进行解密，得到密钥；

接收所述客户端上传的心电检测数据密文，并利用所述密钥对心电检测数据密文进行解密，得到心电检测数据。

9.根据权利要求8所述的方法，其特征在于，在所述接收所述客户端上传的心电检测数据密文，之前，还包括：

接收所述客户端发送的上传请求密文，并利用所述密钥对所述上传请求密文进行解密，得到客户端身份验证信息；

判断所述客户端身份验证信息是否满足预设验证条件；

若是，则执行所述接收所述客户端上传的心电检测数据密文，这一步骤。

10.根据权利要求8所述的方法，其特征在于，当所述客户端处于第一预设模式时，还包括：

根据所有所述客户端请求上传的心电检测数据密文及其客户端网络状态确定各个所述客户端的任务优先级，并根据所述客户端的任务优先级确定所述客户端的上传顺序。

11.一种心电检测数据上传方法，其特征在于，应用于客户端，所述心电检测数据上传方法包括：

接收服务器下发的公钥，并根据所述公钥确定对称加密算法；

根据确定的对称加密算法生成密钥；

依据所述公钥对所述密钥进行加密，得到密钥密文，并将所述密钥密文发送至所述服务器；

根据所述密钥对心电检测数据进行加密，得到心电检测数据密文，并将所述心电检测数据密文上传至所述服务器。

12.根据权利要求11所述的方法，其特征在于，所述根据所述密钥对心电检测数据进行加密，之前，还包括：

当检测到客户端身份验证信息时，生成包含有所述客户端身份验证信息的心电检测数据上传请求；

根据所述密钥对所述心电检测数据上传请求进行加密，得到上传请求密文，并将所述上传请求密文发送至所述服务器。

13.根据权利要求11所述的方法，其特征在于，所述根据所述公钥确定对称加密算法，包括：

将所述公钥的MD5值的各位数求和，并将求和结果与对称加密算法的个数取余，根据取余结果确定选取的对称加密算法种类。

14.根据权利要求11所述的方法，其特征在于，所述将所述心电检测数据密文上传至所述服务器，包括：

判断所述心电检测数据密文的大小是否大于预设大小；

如果是，则利用第一预设模式将所述心电检测数据密文上传至所述服务器；

如果否，则利用第二预设模式将所述心电检测数据密文上传至所述服务器。

15.根据权利要求14所述的方法,其特征在于,所述利用第一预设模式将所述心电检测数据密文上传至所述服务器,包括:

根据当前系统状态对所述心电检测数据密文进行分块,获得多块心电检测数据密文,并通过socket连接的方式与所述服务器建立连接,上传所述多块心电检测数据密文至所述服务器。

16.根据权利要求14所述的方法,其特征在于,所述利用第二预设模式将所述心电检测数据密文上传至所述服务器,包括:

利用Web Service接口与所述服务器建立连接,并将所述心电检测数据密文上传至所述服务器。

一种心电检测数据上传系统及方法

技术领域

[0001] 本申请涉及通信技术领域，更具体地说，涉及一种心电检测数据上传系统及方法。

背景技术

[0002] 心电检测数据是反映人体心脏健康的重要数据，心电检查也是临床心血管疾病诊断经常使用的重要方法，心电检查产生的心电检测数据的保存和管理对于用户而言具有重要意义。

[0003] 发明人在将心电检测数据通过网络进行传输并保存在服务器的尝试过程中发现，如果单纯对心电检测数据利用对称加密算法进行加密，很可能导致密钥在传输过程中被截获，从而使得加密传输的心电检测数据一旦被截获，就可以利用被截获的密钥解密心电传输数据，进而导致心电检测数据的泄漏，而心电检测数据作为用户健康状态的重要数据，其重要性和隐私性不言而喻，因此对称加密算法难以满足心电检测数据传输过程中的保密要求；

[0004] 而由于心电检测数据的数据量一般较大，如果利用非对称加密算法对心电检测数据进行加密，则又会导致加密效率低下的问题。

发明内容

[0005] 为解决上述技术问题，本发明提供了一种心电检测数据上传系统及方法，以实现在提升心电检测数据的传输过程中的保密性的基础上，提升对心电检测数据加密效率的目的。

[0006] 为实现上述技术目的，本发明实施例提供了如下技术方案：

[0007] 一种心电检测数据上传系统，包括：服务器和至少一个客户端，其中，

[0008] 所述服务器，用于生成公钥和私钥，并将所述公钥下发给客户端，以及接收所述客户端发送的密钥密文，并利用所述私钥对所述密钥密文进行解密，得到密钥，以及接收所述客户端上传的心电检测数据密文，并利用所述密钥对所述心电检测数据密文进行解密，得到心电检测数据；

[0009] 所述客户端，用于接收服务器下发的所述公钥，并根据所述公钥确定对称加密算法，以及根据确定的对称加密算法生成密钥，以及依据所述公钥对所述密钥进行加密，得到密钥密文，并将所述密钥密文发送至所述服务器，以及根据所述密钥对心电检测数据进行加密，得到心电检测数据密文，并将所述心电检测数据密文上传至所述服务器。

[0010] 优选的，所述服务器，还用于：

[0011] 接收所述客户端发送的上传请求密文，并利用所述密钥对所述上传请求密文进行解密，得到客户端身份验证信息，以及判断所述客户端身份验证信息是否满足预设验证条件，以及若是，则执行所述接收所述客户端上传的心电检测数据密文，这一步骤；

[0012] 所述客户端，还用于当检测到客户端身份验证信息时，生成包含有所述客户端身份验证信息的心电检测数据上传请求，以及根据所述密钥对所述心电检测数据上传请求进

行加密，得到上传请求密文，并将所述上传请求密文发送至所述服务器。

[0013] 优选的，所述客户端根据所述公钥确定对称加密算法，具体用于：

[0014] 将所述公钥的MD5值的各位数求和，并将求和结果与对称加密算法的个数取余，根据取余结果确定选取的对称加密算法种类。

[0015] 优选的，所述将所述心电检测数据密文上传至所述服务器，具体用于：

[0016] 判断所述心电检测数据密文的大小是否大于预设大小；如果是，则利用第一预设模式将所述心电检测数据密文上传至所述服务器；如果否，则利用第二预设模式将所述心电检测数据密文上传至所述服务器。

[0017] 优选的，所述利用第一预设模式将所述心电检测数据密文上传至所述服务器，具体用于：

[0018] 根据当前系统状态对所述心电检测数据密文进行分块，获得多块心电检测数据密文，并通过socket连接的方式与所述服务器建立连接，上传所述多块心电检测数据密文至所述服务器。

[0019] 优选的，在所述第一预设模式中，所述服务器还用于：

[0020] 根据所有所述客户端请求上传的心电检测数据密文及其客户端网络状态确定各个所述客户端的任务优先级，并根据所述客户端的任务优先级确定所述客户端的上传顺序。

[0021] 优选的，所述利用第二预设模式将所述心电检测数据密文上传至所述服务器，具体用于：

[0022] 利用Web Service接口与所述服务器建立连接，并将所述心电检测数据密文上传至所述服务器。

[0023] 一种心电检测数据上传方法，应用于服务器，所述心电检测数据上传方法包括：

[0024] 生成公钥和私钥，并将所述公钥下发给客户端；

[0025] 接收所述客户端发送的密钥密文，并利用所述私钥对所述密钥密文进行解密，得到密钥；

[0026] 接收所述客户端上传的心电检测数据密文，并利用所述密钥对心电检测数据密文进行解密，得到心电检测数据。

[0027] 优选的，在所述接收所述客户端上传的心电检测数据密文，之前，还包括：

[0028] 接收所述客户端发送的上传请求密文，并利用所述密钥对所述上传请求密文进行解密，得到客户端身份验证信息；

[0029] 判断所述客户端身份验证信息是否满足预设验证条件；

[0030] 若是，则执行所述接收所述客户端上传的心电检测数据密文，这一步骤。

[0031] 优选的，当所述客户端处于第一预设模式时，还包括：

[0032] 根据所有所述客户端请求上传的心电检测数据密文及其客户端网络状态确定各个所述客户端的任务优先级，并根据所述客户端的任务优先级确定所述客户端的上传顺序。

[0033] 一种心电检测数据上传方法，应用于客户端，所述心电检测数据上传方法包括：

[0034] 接收服务器下发的公钥，并根据所述公钥确定对称加密算法；

[0035] 根据确定的对称加密算法生成密钥；

[0036] 依据所述公钥对所述密钥进行加密，得到密钥密文，并将所述密钥密文发送至所述服务器；

[0037] 根据所述密钥对心电检测数据进行加密，得到心电检测数据密文，并将所述心电检测数据密文上传至所述服务器。

[0038] 优选的，所述根据所述密钥对心电检测数据进行加密，之前，还包括：

[0039] 当检测到客户端身份验证信息时，生成包含有所述客户端身份验证信息的心电检测数据上传请求；

[0040] 根据所述密钥对所述心电检测数据上传请求进行加密，得到上传请求密文，并将所述上传请求密文发送至所述服务器。

[0041] 优选的，所述根据所述公钥确定对称加密算法，包括：

[0042] 将所述公钥的MD5值的各位数求和，并将求和结果与对称加密算法的个数取余，根据取余结果确定选取的对称加密算法种类。

[0043] 优选的，所述将所述心电检测数据密文上传至所述服务器，包括：

[0044] 判断所述心电检测数据密文的大小是否大于预设大小；

[0045] 如果是，则利用第一预设模式将所述心电检测数据密文上传至所述服务器；

[0046] 如果否，则利用第二预设模式将所述心电检测数据密文上传至所述服务器。

[0047] 优选的，所述利用第一预设模式将所述心电检测数据密文上传至所述服务器，包括：

[0048] 根据当前系统状态对所述心电检测数据密文进行分块，获得多块心电检测数据密文，并通过socket连接的方式与所述服务器建立连接，上传所述多块心电检测数据密文至所述服务器。

[0049] 优选的，所述利用第二预设模式将所述心电检测数据密文上传至所述服务器，包括：

[0050] 利用Web Service接口与所述服务器建立连接，并将所述心电检测数据密文上传至所述服务器。

[0051] 从上述技术方案可以看出，本发明实施例提供了一种心电检测数据上传系统及方法，其中，所述心电检测数据上传系统利用非对称加密算法产生公钥和私钥，并将公钥下发给客户端以供客户端确定对称加密算法并生成密钥，由于私钥不在服务器和客户端中进行传输，即使根据公钥对密钥进行加密得到的密文在传输过程中被第三方截获，由于第三方不具有私钥，无法对密文进行解密，从而无法得到密钥，也就无法解密使用密钥加密的心电检测数据，这就提升了心电检测数据传输过程的保密程度；并且在该系统中，仅利用非对称加密算法产生公钥和私钥，而不直接利用非对称加密算法对心电检测数据进行加密，提升了心电检测数据的加密效率。

附图说明

[0052] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据提供的附图获得其他的附图。

[0053] 图1为本申请的一个实施例提供的一种心电检测数据上传系统的处理流程示意图；

[0054] 图2为本申请的一个实施例提供的一种心电检测数据上传系统的结构示意图；

[0055] 图3为本申请的另一个实施例提供的一种心电检测数据上传系统的处理流程示意图；

[0056] 图4为本申请的又一个实施例提供的一种心电检测数据上传系统的处理流程示意图；

[0057] 图5为本申请的再一个实施例提供的一种心电检测数据上传系统的处理流程示意图；

[0058] 图6为本申请的一个实施例提供的一种心电检测数据上传方法的流程示意图；

[0059] 图7为本申请的另一个实施例提供的一种心电检测数据上传方法的流程示意图；

[0060] 图8为本申请的又一个实施例提供的一种心电检测数据上传方法的流程示意图；

[0061] 图9为本申请的再一个实施例提供的一种心电检测数据上传方法的流程示意图；

[0062] 图10为本申请的一个优选实施例提供的一种心电检测数据上传方法的流程示意图；

[0063] 图11为本申请的另一个优选实施例提供的一种心电检测数据上传方法的流程示意图；

[0064] 图12为本申请的又一个优选实施例提供的一种心电检测数据上传方法的流程示意图；

[0065] 图13为本申请的再一个优选实施例提供的一种心电检测数据上传方法的流程示意图；

[0066] 图14为本申请的再一个优选实施例提供的一种心电检测数据上传方法的流程示意图。

具体实施方式

[0067] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0068] 本申请实施例提供了一种心电检测数据上传系统，如图1和图2所示，包括：服务器和至少一个客户端，其中，

[0069] 服务器，用于生成公钥和私钥，并将公钥下发给客户端，以及接收客户端发送的密钥密文，并利用私钥对密钥密文进行解密，得到密钥，以及接收客户端上传的心电检测数据密文，并利用密钥对心电检测数据密文进行解密，得到心电检测数据；

[0070] 客户端，用于接收服务器下发的公钥，并根据公钥确定对称加密算法，以及根据确定的对称加密算法生成密钥，以及依据公钥对密钥进行加密，得到密钥密文，并将密钥密文发送至服务器，以及根据密钥对心电检测数据进行加密，得到心电检测数据密文，并将心电检测数据密文上传至所述服务器。

[0071] 图1为所述心电检测数据上传系统的服务器和客户端的通信过程示意图，图2为所

述心电检测数据上传系统的结构示意图；

[0072] 心脏疾病是一种不定期触发性疾病，需要长期观测患者的身体状况，记录其心电参数，便携式的心电数据监测设备不但能够为医生提供准确的数据信息，还能为患者争取宝贵的治疗时间，对于心血管类疾病的诊断和预防具有重要的实际意义。便携式心电监测设备会产生大量的数据，心电数据是个人健康核心数据之一，如果不进行加密，被截取、攻击后会造成无法估量的后果。心电数据量大，采用非对称加密较慢，而采用对称加密密钥容易被截取，安全性不能得到保证。本申请实施例提出了配合使用对称加密和非对称加密的方法对心电数据进行加密，既可以保证心电数据的传输安全又可以解决资源消耗过多的问题。

[0073] 具体地，所述心电检测数据上传系统利用非对称加密算法产生公钥和私钥，并将所述公钥下发给客户端以供客户端确定对称加密算法并生成密钥，由于私钥不在服务器和客户端中进行传输，即使根据公钥对密钥进行加密得到的密文在传输过程中被第三方截获，由于第三方不具有私钥，无法对密文进行解密，从而无法得到密钥，也就无法解密使用密钥加密的心电检测数据，这就提升了心电检测数据传输过程的保密程度；并且在该系统中，仅利用非对称加密算法产生公钥和私钥，而不直接利用非对称加密算法对心电检测数据进行加密，提升了心电检测数据的加密效率。

[0074] 在上述实施例的基础上，在本申请的又一个实施例中，如图3所示，服务器，还用于：

[0075] 接收客户端发送的上传请求密文，并利用密钥对上传请求密文进行解密，得到客户端身份验证信息，以及判断客户端身份验证信息是否满足预设验证条件，以及若是，则执行接收客户端上传的心电检测数据密文，这一步骤；

[0076] 客户端，还用于当检测到客户端身份验证信息时，生成包含有客户端身份验证信息的心电检测数据上传请求，以及根据密钥对所述心电检测数据上传请求进行加密，得到上传请求密文，并将上传请求密文发送至服务器。

[0077] 需要说明的是，当服务器判定客户端身份验证信息不满足预设验证条件，或者说当服务器检测到身份验证信息为伪造身份验证信息或者失效身份验证信息时，可以认为正在使用的密钥已被截获，存在一定的风险，因此重新生成公钥和私钥，以进行密钥的更新，进而使得客户端重新对心电检测数据上传请求进行加密；

[0078] 为进一步提高上传请求发送至服务器过程的保密性，客户端在生成包含有客户端身份验证信息的心电检测数据上传请求的同时，记录当前系统时间，可采用对称加密算法对客户端身份验证信息以及当前系统时间进行加密，并根据密钥对心电检测数据上传请求进行加密，得到上传请求密文；由于该上传请求密文与当前系统时间相关，因此对于伪造身份验证信息或者失效身份验证信息，由于时间异常可迅速被服务器识别；同样，由于客户端身份验证信息存在使用时效，这个时效可以是一天，也可以是12小时，本申请对客户端身份验证信息的使用时效的具体长度并不做限定，具体视实际情况而定。

[0079] 在上述实施例的基础上，在本申请的另一个实施例中，如图4所示，所述客户端根据公钥确定对称加密算法，具体用于：

[0080] 将公钥的MD5值的各位数求和，并将求和结果与对称加密算法的个数取余，根据取余结果确定选取的对称加密算法种类。

[0081] 需要说明的是,本实施例提供了一种具体地根据所述公钥确定对称加密算法的具体过程,其中,所述对称加密算法的个数是指系统中备用的对称加密算法的数量;例如,某一次产生的公钥的MD5(Message Digest,信息摘要)值的各位数之和为1000002,系统中备用的对称加密算法的个数为5个,分别A、B、C、D、E,对称加密算法的个数为5,公钥的MD5值的各位数之和与对称加密算法的个数取余后的结果为2,则最后确定的对称加密算法为B。

[0082] 在本申请的其他实施例中,还可以通过其他的方式确定对称加密算法,例如,可以通过将公钥和服务器下发的种子产生的随机数作逻辑运算(与、或、非及其组合)后,再对逻辑运算的结果进行哈希算法的运算,最后根据哈希运算的结果和系统中备用的对称加密算法确定选用的对称加密算法。本申请对根据所述公钥确定对称加密算法的具体过程并不做限定,具体视实际情况而定。

[0083] 在上述实施例的基础上,在本申请的又一个实施例中,如图5所示,所述客户端将心电检测数据密文上传至服务器,具体用于:

[0084] 判断心电检测数据密文的大小是否大于预设大小;如果是,则利用第一预设模式将心电检测数据密文上传至服务器;如果否,则利用第二预设模式将心电检测数据密文上传至服务器。

[0085] 需要说明的是,所述预设大小一般为一次心电检测过程中产生的心电检测数据的大小,这个大小根据所使用的心电检测设备的不同而有所不同,一般情况下,所述预设大小的大小在数兆(M)范围内,本申请对所述预设大小的具体取值并不做限定,具体视实际情况而定。

[0086] 具体地,所述客户端利用第一预设模式将心电检测数据密文上传至服务器,具体用于:

[0087] 根据当前系统状态对心电检测数据密文进行分块,获得多块心电检测数据密文,并通过socket连接的方式与服务器建立连接,上传多块心电检测数据密文至服务器。

[0088] 需要说明的是,在具体使用过程中,客户端将分块的心电检测数据密文上传成功后,客户端向服务器进行查询是否成功,如果成功则完成此次上传,如果没成功,则根据服务器下发的job_id重新申请服务器开启socket上传。直到所有分块的心电检测数据密文全部上传成功,最终实现整个上传任务成功。客户端通过Web Service向服务器发送所有的job_id,并通知服务器每个分块文件都已经上传成功,服务器检查后将所有分块心电数据密文进行合并,然后用密钥进行解密后保存。

[0089] 在第一预设模式中,服务器还用于:

[0090] 根据所有客户端请求上传的心电检测数据密文及其客户端网络状态确定各个客户端的任务优先级,并根据客户端的任务优先级确定客户端的上传顺序。

[0091] 具体地,在系统中,服务器建立固定数量的socket池与客户端进行连接,定期检查服务器硬件升级情况以及扩展情况对socket池初始化数量进行更新。如果服务器socket池已经没有空闲时还有客户端申请大文件上传,这时也会生成相应的job_id并进行保存,并将任务存储在优先级队列中,从而达到均衡的效果。根据心电检测数据密文的心电检测数据大小以及心电检测数据任务等级决定优先级队列中的优先级。如果socket池正在处理的任务都是低优先级的任务,那么当前任务优先级较高,可通过传输速度、优先级、所需时间等参数来决策将正在处理的少量socket提前终止,并调整被终止任务的优先级,被结束掉

的任务会将优先级提高一些，然后将这些任务加入到优先级队列中。大文件分块后上传速度很快，如果优先级较高，高优先级的任务将更早的进行上传处理。

[0092] 在上述实施例的基础上，在本申请的再一个实施例中，所述客户端利用第二预设模式将心电检测数据密文上传至服务器，具体用于：

[0093] 利用Web Service接口与服务器建立连接，并将心电检测数据密文上传至服务器。

[0094] 需要说明的是，当客户端需要进行上传的心电检测数据密文小于预设大小时，利用Web Service进行上传具有较大的性能优势，而当需要上传的心电检测数据密文较大时，长连接的Socket则具有较大的性能优势。

[0095] 在本申请的其他实施例中，客户端结合心电检测数据密文大小文件并存的特点，采用不同传输策略，对于小文件的心电检测数据密文通过Web Service接口进进行传输，而对于大文件的心电检测数据密文则通过socket连接的方式进行传输，相比于Web Service的传输方式，socket的传输方式数据传输效率以及稳定性会更高，因此，这也就提高了系统传输效率和稳定性。

[0096] 相应的，本申请实施例还提供了一种心电检测数据上传方法，如图6所示，应用于服务器，所述心电检测数据上传方法包括：

[0097] S101:生成公钥和私钥，并将公钥下发给客户端；

[0098] S102:接收客户端发送的密钥密文，并利用私钥对密钥密文进行解密，得到密钥；

[0099] S103，接收客户端上传的心电检测数据密文，并利用密钥对心电检测数据密文进行解密，得到心电检测数据。

[0100] 心脏疾病是一种不定期触发性疾病，需要长期观测患者的身体状况，记录其心电参数，便携式的心电数据监测设备不但能够为医生提供准确的数据信息，还能为患者争取宝贵的治疗时间，对于心血管类疾病的诊断和预防具有重要的实际意义。便携式心电监测设备会产生大量的数据，心电数据是个人健康核心数据之一，如果不进行加密，被截取、攻击后会造成无法估量的后果。心电数据量大，采用非对称加密较慢，而采用对称加密密钥容易被截取，安全性不能得到保证。本申请实施例提出了配合使用对称加密和非对称加密的方法对心电数据进行加密，既可以保证心电数据的传输安全又可以解决资源消耗过多的问题。

[0101] 具体地，所述心电检测数据上传系统利用非对称加密算法产生公钥和私钥，并将公钥下发给客户端以供客户端确定对称加密算法并生成密钥，由于私钥不在服务器和客户端中进行传输，即使根据公钥对密钥进行加密得到的密文在传输过程中被第三方截获，由于第三方不具有私钥，无法对密文进行解密，从而无法得到密钥，也就无法解密使用密钥加密的心电检测数据，这就提升了心电检测数据传输过程的保密程度；并且在该系统中，仅利用非对称加密算法产生公钥和私钥，而不直接利用非对称加密算法对心电检测数据进行加密，提升了心电检测数据的加密效率。

[0102] 在上述实施例的基础上，在本申请的又一个实施例中，如图7所示，在步骤S103，之前，还可包括：

[0103] S201，接收客户端发送的上传请求密文，并利用密钥对上传请求密文进行解密，得到客户端身份验证信息；

[0104] S202，判断客户端身份验证信息是否满足预设验证条件；若是，则执行步骤S103。

[0105] 需要说明的是，当服务器判定客户端身份验证信息不满足预设验证条件，也就是当服务器检测到身份验证信息为伪造身份验证信息或者失效身份验证信息时，可以认为正在使用的密钥已被截获，存在一定的风险，因此重新生成公钥和私钥，以进行密钥的更新，进而使得客户端重新对心电检测数据上传请求进行加密；

[0106] 为进一步提高上传请求发送至服务器过程的保密性，客户端在生成包含有客户端身份验证信息的心电检测数据上传请求的同时，记录当前系统时间，可采用对称加密算法对客户端身份验证信息以及当前系统时间进行加密，并根据密钥对心电检测数据上传请求进行加密，得到上传请求密文；由于该上传请求密文与当前系统时间相关，因此对于伪造身份验证信息或者失效身份验证信息，由于时间异常可迅速被服务器识别；同样，由于客户端身份验证信息存在使用时效，这个时效可以是一天，也可以是12小时，本申请对客户端身份验证信息的使用时效的具体长度并不做限定，具体视实际情况而定。

[0107] 在上述实施例的基础上，在本申请的又一个实施例中，如图8所示，当所述客户端处于第一预设模式时，还包括：

[0108] S301：根据所有客户端请求上传的心电检测数据密文及其客户端网络状态确定各个客户端的任务优先级，并根据客户端的任务优先级确定客户端的上传顺序。

[0109] 具体地，在系统中，服务器建立固定数量的socket池与客户端进行连接，定期检查服务器硬件升级情况以及扩展情况对socket池初始化数量进行更新。如果服务器socket池已经没有空闲时还有客户端申请大文件上传，这时也会生成相应的job_id并进行保存，并将任务存储在优先级队列中，从而达到均衡的效果。根据心电检测数据密文的心电检测数据大小以及心电检测数据任务等级决定优先级队列中的优先级。如果socket池正在处理的任务都是低优先级的任务，那么当前任务优先级较高，可通过传输速度、优先级、所需时间等参数来决策将正在处理的少量socket提前终止，并调整被终止任务的优先级，被结束掉的任务会将优先级提高一些，然后将这些任务加入到优先级队列中。大文件分块后上传速度很快，如果优先级较高，高优先级的任务将更早的进行上传处理。

[0110] 相应的，本申请实施例还提供了一种心电检测数据上传方法，如图9所示，应用于客户端，所述心电检测数据上传方法包括：

[0111] S401：接收服务器下发的公钥，并根据公钥确定对称加密算法；

[0112] S402：根据确定的对称加密算法生成密钥；

[0113] S403：依据公钥对密钥进行加密，得到密钥密文，并将密钥密文发送至服务器；

[0114] S404，根据密钥对心电检测数据进行加密，得到心电检测数据密文，并将心电检测数据密文上传至服务器。

[0115] 具体地，在本申请的一个实施例中，如图10所示，步骤S401中根据公钥确定对称加密算法的具体执行过程，包括：

[0116] S4011：将公钥的MD5值的各位数求和，并将求和结果与对称加密算法的个数取余，根据取余结果确定选取的对称加密算法种类。

[0117] 需要说明的是，本实施例提供了一种具体地根据所述公钥确定对称加密算法的具体过程，其中，所述对称加密算法的个数是指系统中备用的对称加密算法的数量；例如，某一次产生的公钥的MD5(Message Digest，信息摘要)值的各位数之和为1000002，系统中备用的对称加密算法的个数为5个，分别A、B、C、D、E，对称加密算法的个数为5，公钥的MD5值的

各位数之和与对称加密算法的个数取余后的结果为2,则最后确定的对称加密算法为B。

[0118] 在本申请的其他实施例中,还可以通过其他的方式确定对称加密算法,例如,可以通过将公钥和服务器下发的种子产生的随机数作逻辑运算(与、或、非及其组合)后,再对逻辑运算的结果进行哈希算法的运算,最后根据哈希运算的结果和系统中备用的对称加密算法确定选用的对称加密算法。本申请对根据所述公钥确定对称加密算法的具体过程并不做限定,具体视实际情况而定。

[0119] 在上述实施例的基础上,在本申请的另一个实施例中,如图11所示,步骤S404中将心电检测数据密文上传至服务器的具体执行过程,如图11所示,包括:

[0120] S4041:判断心电检测数据密文的大小是否大于预设大小;如果是,则执行步骤S4042;若否,则执行步骤S4043;

[0121] S4042,利用第一预设模式将心电检测数据密文上传至服务器;

[0122] S4043,利用第二预设模式将心电检测数据密文上传至服务器。

[0123] 需要说明的是,所述预设大小一般为一次心电检测过程中产生的心电检测数据的大小,这个大小根据所使用的心电检测设备的不同而有所不同,一般情况下,所述预设大小的大小在数兆(M)范围内,本申请对所述预设大小的具体取值并不做限定,具体视实际情况而定。

[0124] 具体地,如图12所示,步骤S4042中利用第一预设模式将心电检测数据密文上传至服务器的具体执行过程,包括:

[0125] 根据当前系统状态对心电检测数据密文进行分块,获得多块心电检测数据密文,并通过socket连接的方式与服务器建立连接,上传多块心电检测数据密文至服务器。

[0126] 需要说明的是,在具体使用过程中,客户端将分块的心电检测数据密文上传成功后,客户端向服务器进行查询是否成功,如果成功则完成此次上传,如果没成功,则根据服务器下发的job_id重新申请服务器开启socket上传。直到所有分块的心电检测数据密文全部上传成功,最终实现整个上传任务成功。客户端通过Web Service向服务器发送所有的job_id,并通知服务器每个分块文件都已经上传成功,服务器检查后将所有分块心电数据密文进行合并,然后用密钥进行解密后保存。

[0127] 具体地,如图13所示,步骤S4043中用第二预设模式将心电检测数据密文上传至服务器的具体执行过程,包括:

[0128] 利用Web Service接口与所述服务器建立连接,并将心电检测数据密文上传至服务器。

[0129] 需要说明的是,当客户端需要进行上传的心电检测数据密文小于预设大小时,利用Web Service进行上传具有较大的性能优势,而当需要上传的心电检测数据密文较大时,长连接的Socket则具有较大的性能优势。

[0130] 在上述实施例的基础上,在本申请的又一个实施例中,如图14所示,步骤S403之前,还包括如下步骤:

[0131] S501,当检测到客户端身份验证信息时,生成包含有客户端身份验证信息的心电检测数据上传请求;

[0132] S502,根据密钥对心电检测数据上传请求进行加密,得到上传请求密文,并将上传请求密文发送至服务器。

[0133] 综上所述，本申请实施例提供了一种心电检测数据上传系统及方法，其中，所述心电检测数据上传系统利用非对称加密算法产生公钥和私钥，并将公钥下发给客户端以供客户端确定对称加密算法并生成密钥，由于私钥不在服务器和客户端中进行传输，即使根据公钥对密钥进行加密得到的密文在传输过程中被第三方截获，由于第三方不具有私钥，无法对密文进行解密，从而无法得到密钥，也就无法解密使用密钥加密的心电检测数据，这就提升了心电检测数据传输过程的保密程度；并且在该系统中，仅利用非对称加密算法产生公钥和私钥，而不直接利用非对称加密算法对心电检测数据进行加密，提升了心电检测数据的加密效率。

[0134] 本说明书中各个实施例采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似部分互相参见即可。

[0135] 对所公开的实施例的上述说明，使本领域专业技术人员能够实现或使用本发明。对这些实施例的多种修改对本领域的专业技术人员来说将是显而易见的，本文中所定义的一般原理可以在不脱离本发明的精神或范围的情况下，在其它实施例中实现。因此，本发明将不会被限制于本文所示的这些实施例，而是要符合与本文所公开的原理和新颖特点相一致的最宽的范围。

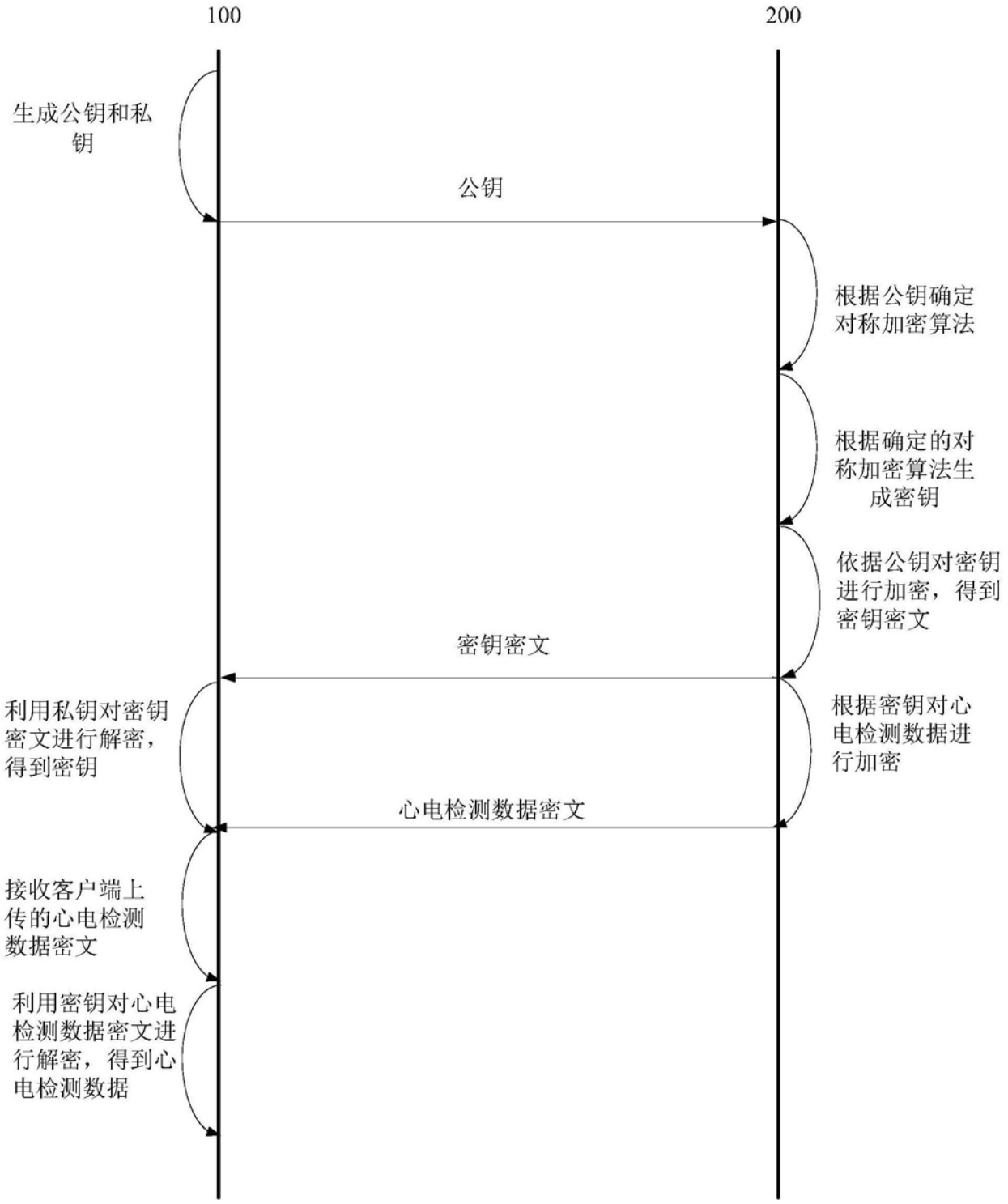

100
200
生成公钥和私钥
公钥
根据公钥确定对称加密算法
根据确定的对称加密算法生成密钥
依据公钥对密钥进行加密，得到密钥密文
密钥密文
利用私钥对密钥密文进行解密，得到密钥
根据密钥对心电检测数据进行加密
心电检测数据密文
接收客户端上传的心电检测数据密文
利用密钥对心电检测数据密文进行解密，得到心电检测数据

图1

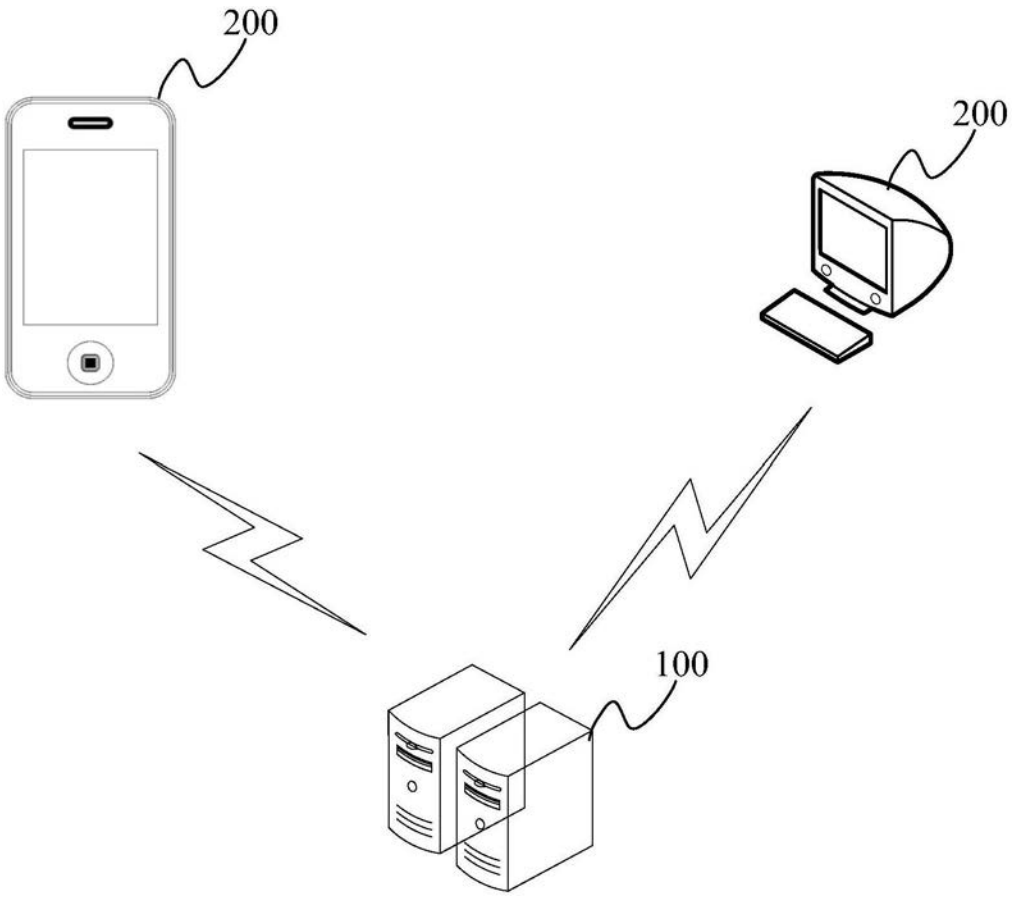


图2

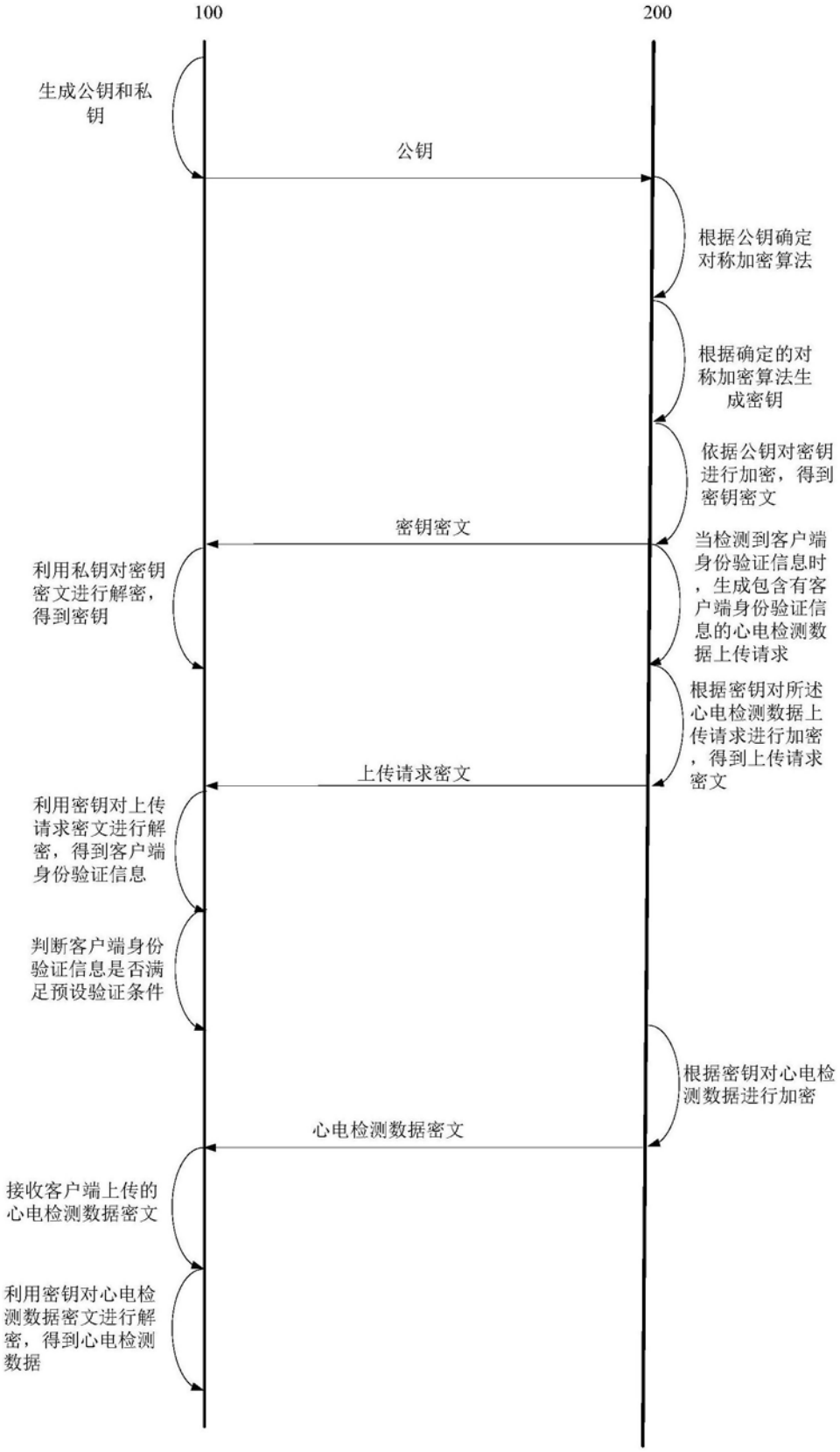

100
200
生成公钥和私钥
公钥
根据公钥确定对称加密算法
根据确定的对称加密算法生成密钥
依据公钥对密钥进行加密，得到密钥密文
密钥密文
当检测到客户端身份验证信息时，生成包含有客户端身份验证信息的心电检测数据上传请求
利用私钥对密钥密文进行解密，得到密钥
根据密钥对所述心电检测数据上传请求进行加密，得到上传请求密文
上传请求密文
利用密钥对上传请求密文进行解密，得到客户端身份验证信息
判断客户端身份验证信息是否满足预设验证条件
根据密钥对心电检测数据进行加密
心电检测数据密文
接收客户端上传的心电检测数据密文
利用密钥对心电检测数据密文进行解密，得到心电检测数据

图3

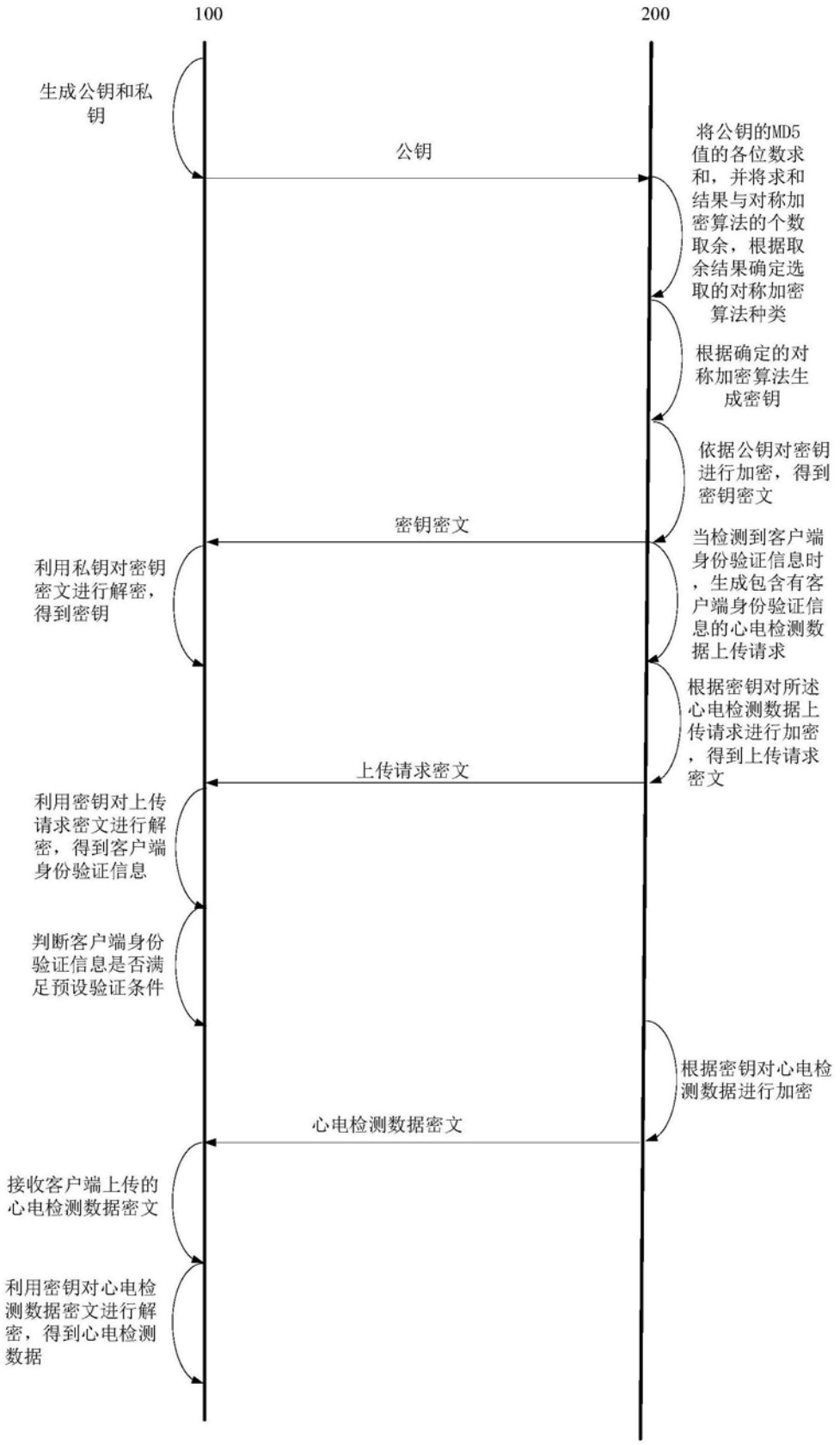

100
200
生成公钥和私钥
公钥
将公钥的MD5值的各位数求和，并将求和结果与对称加密算法的个数取余，根据取余结果确定选取的对称加密算法种类
根据确定的对称加密算法生成密钥
依据公钥对密钥进行加密，得到密钥密文
密钥密文
当检测到客户端身份验证信息时，生成包含有客户端身份验证信息的心电检测数据上传请求
利用私钥对密钥密文进行解密，得到密钥
根据密钥对所述心电检测数据上传请求进行加密，得到上传请求密文
上传请求密文
利用密钥对上传请求密文进行解密，得到客户端身份验证信息
判断客户端身份验证信息是否满足预设验证条件
根据密钥对心电检测数据进行加密
心电检测数据密文
接收客户端上传的心电检测数据密文
利用密钥对心电检测数据密文进行解密，得到心电检测数据

图4

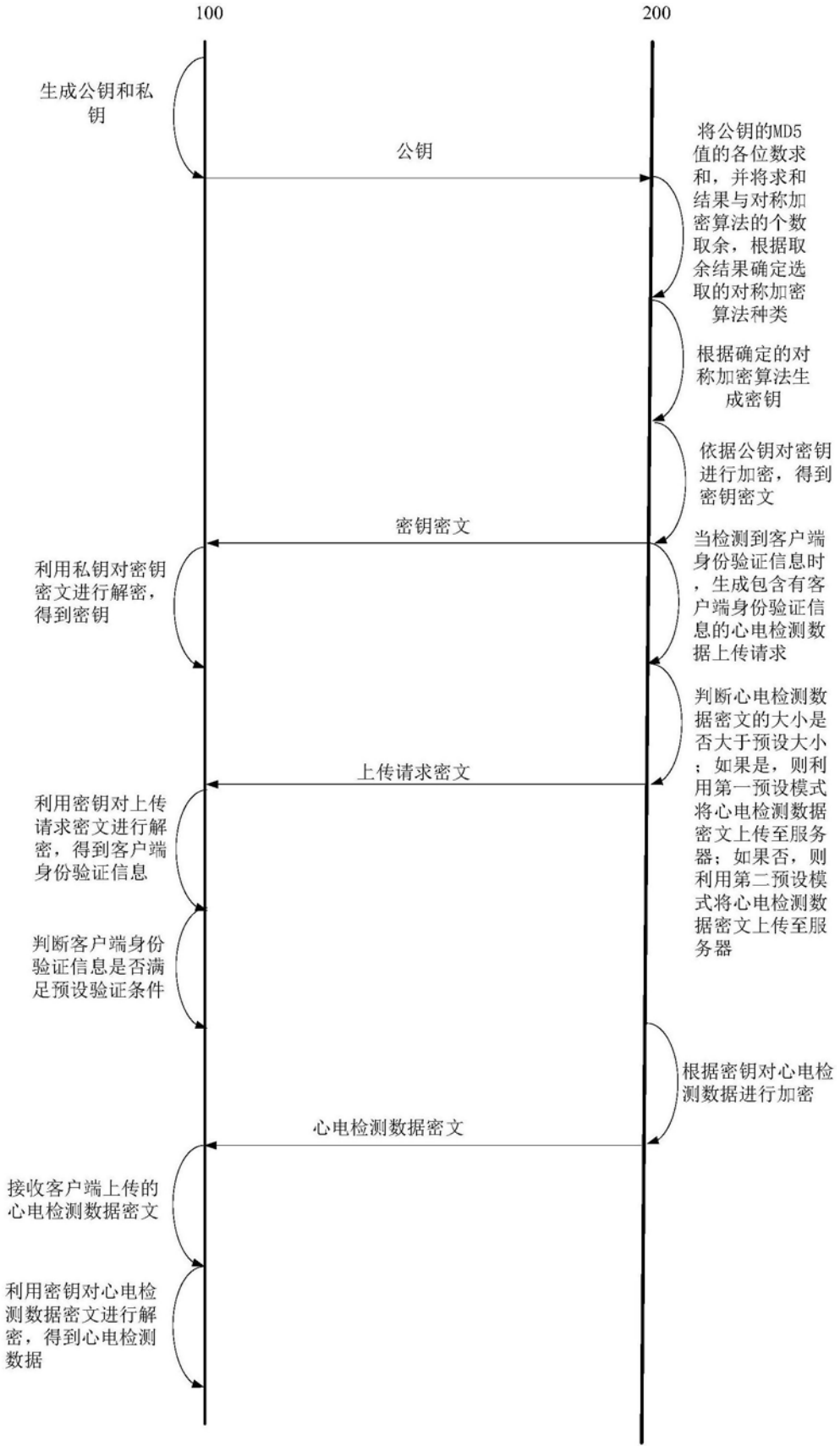

100
200
生成公钥和私钥
公钥
将公钥的MD5值的各位数求和，并将求和结果与对称加密算法的个数取余，根据取余结果确定选取的对称加密算法种类
根据确定的对称加密算法生成密钥
依据公钥对密钥进行加密，得到密钥密文
密钥密文
利用私钥对密钥密文进行解密，得到密钥
当检测到客户端身份验证信息时，生成包含有客户端身份验证信息的心电检测数据上传请求
判断心电检测数据密文的大小是否大于预设大小；如果是，则利用第一预设模式将心电检测数据密文上传至服务器；如果否，则利用第二预设模式将心电检测数据密文上传至服务器
上传请求密文
利用密钥对上传请求密文进行解密，得到客户端身份验证信息
判断客户端身份验证信息是否满足预设验证条件
根据密钥对心电检测数据进行加密
心电检测数据密文
接收客户端上传的心电检测数据密文
利用密钥对心电检测数据密文进行解密，得到心电检测数据

图5

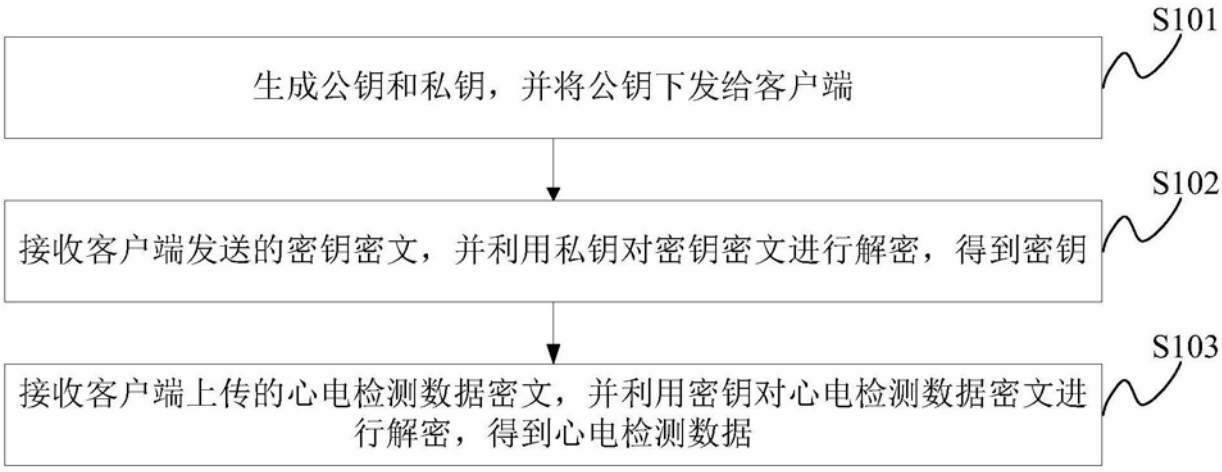

S101
生成公钥和私钥，并将公钥下发给客户端
S102
接收客户端发送的密钥密文，并利用私钥对密钥密文进行解密，得到密钥
S103
接收客户端上传的心电检测数据密文，并利用密钥对心电检测数据密文进行解密，得到心电检测数据

图6

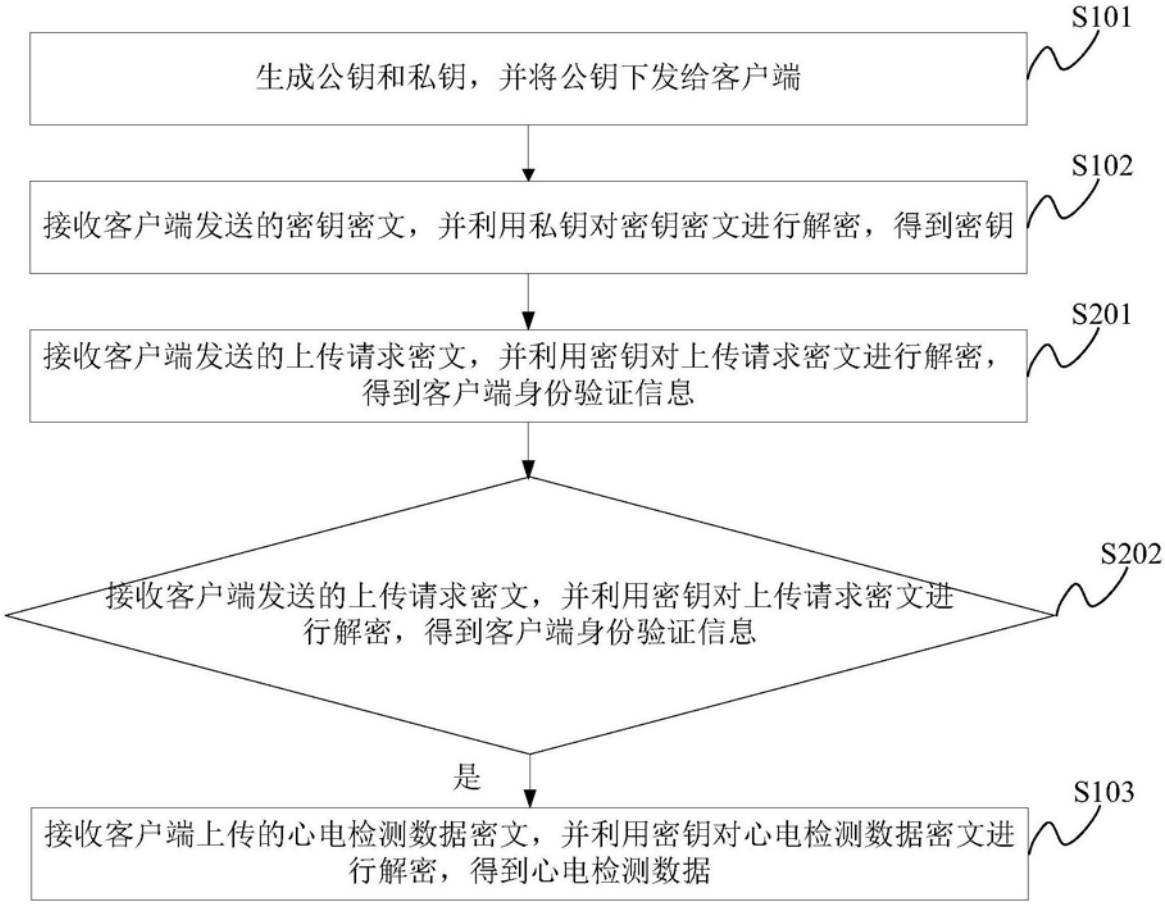

S101
生成公钥和私钥，并将公钥下发给客户端
S102
接收客户端发送的密钥密文，并利用私钥对密钥密文进行解密，得到密钥
S201
接收客户端发送的上传请求密文，并利用密钥对上传请求密文进行解密，得到客户端身份验证信息
S202
接收客户端发送的上传请求密文，并利用密钥对上传请求密文进行解密，得到客户端身份验证信息
是
S103
接收客户端上传的心电检测数据密文，并利用密钥对心电检测数据密文进行解密，得到心电检测数据

图7

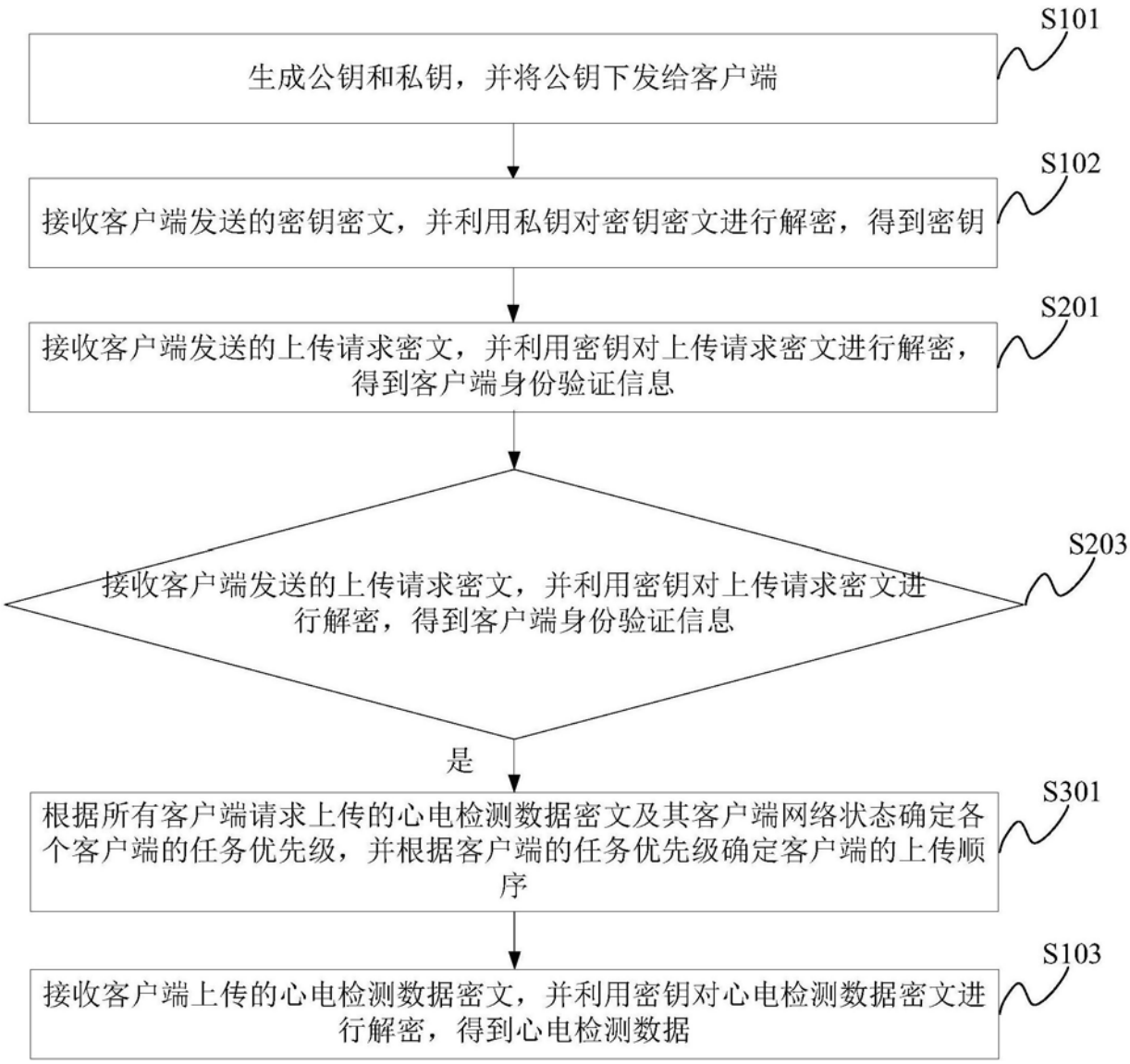

S101
生成公钥和私钥，并将公钥下发给客户端
S102
接收客户端发送的密钥密文，并利用私钥对密钥密文进行解密，得到密钥
S201
接收客户端发送的上传请求密文，并利用密钥对上传请求密文进行解密，得到客户端身份验证信息
S203
接收客户端发送的上传请求密文，并利用密钥对上传请求密文进行解密，得到客户端身份验证信息
是
S301
根据所有客户端请求上传的心电检测数据密文及其客户端网络状态确定各个客户端的任务优先级，并根据客户端的任务优先级确定客户端的上传顺序
S103
接收客户端上传的心电检测数据密文，并利用密钥对心电检测数据密文进行解密，得到心电检测数据

图8

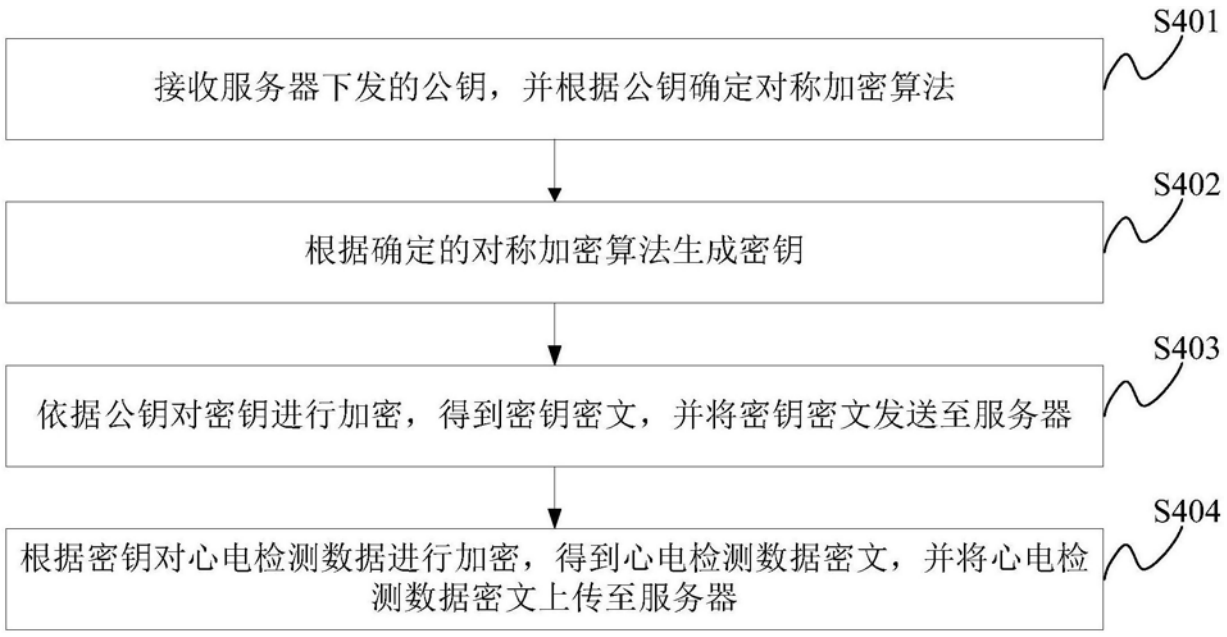

S401
接收服务器下发的公钥，并根据公钥确定对称加密算法
S402
根据确定的对称加密算法生成密钥
S403
依据公钥对密钥进行加密，得到密钥密文，并将密钥密文发送至服务器
S404
根据密钥对心电检测数据进行加密，得到心电检测数据密文，并将心电检测数据密文上传至服务器

图9

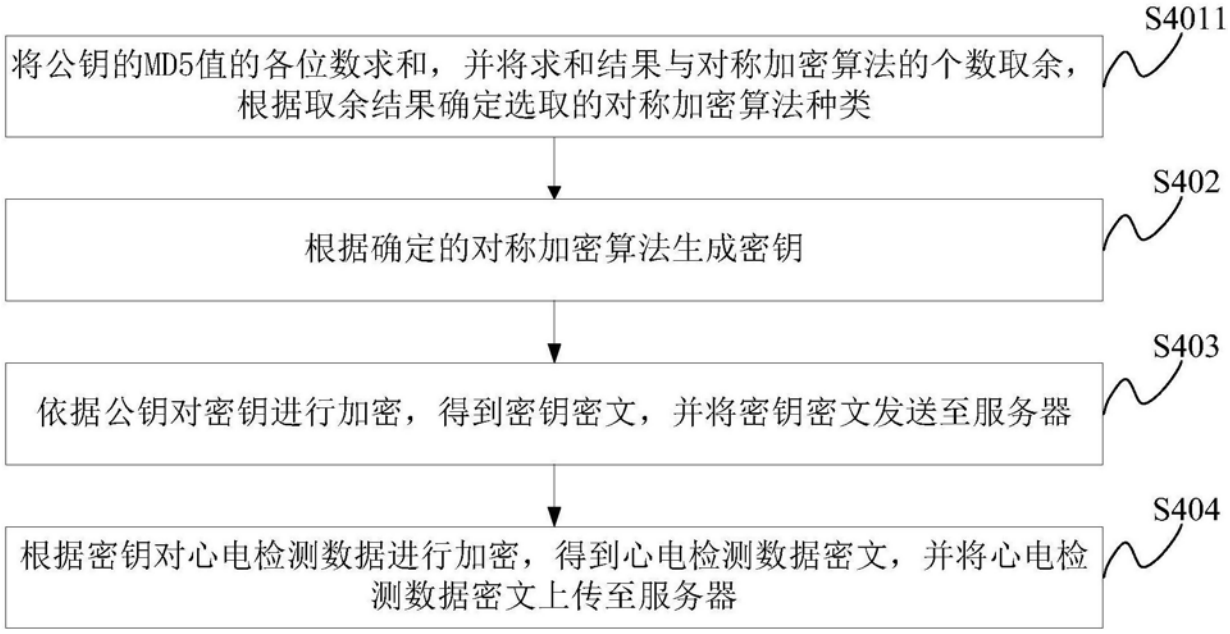

S4011
将公钥的MD5值的各位数求和，并将求和结果与对称加密算法的个数取余，根据取余结果确定选取的对称加密算法种类
S402
根据确定的对称加密算法生成密钥
S403
依据公钥对密钥进行加密，得到密钥密文，并将密钥密文发送至服务器
S404
根据密钥对心电检测数据进行加密，得到心电检测数据密文，并将心电检测数据密文上传至服务器

图10

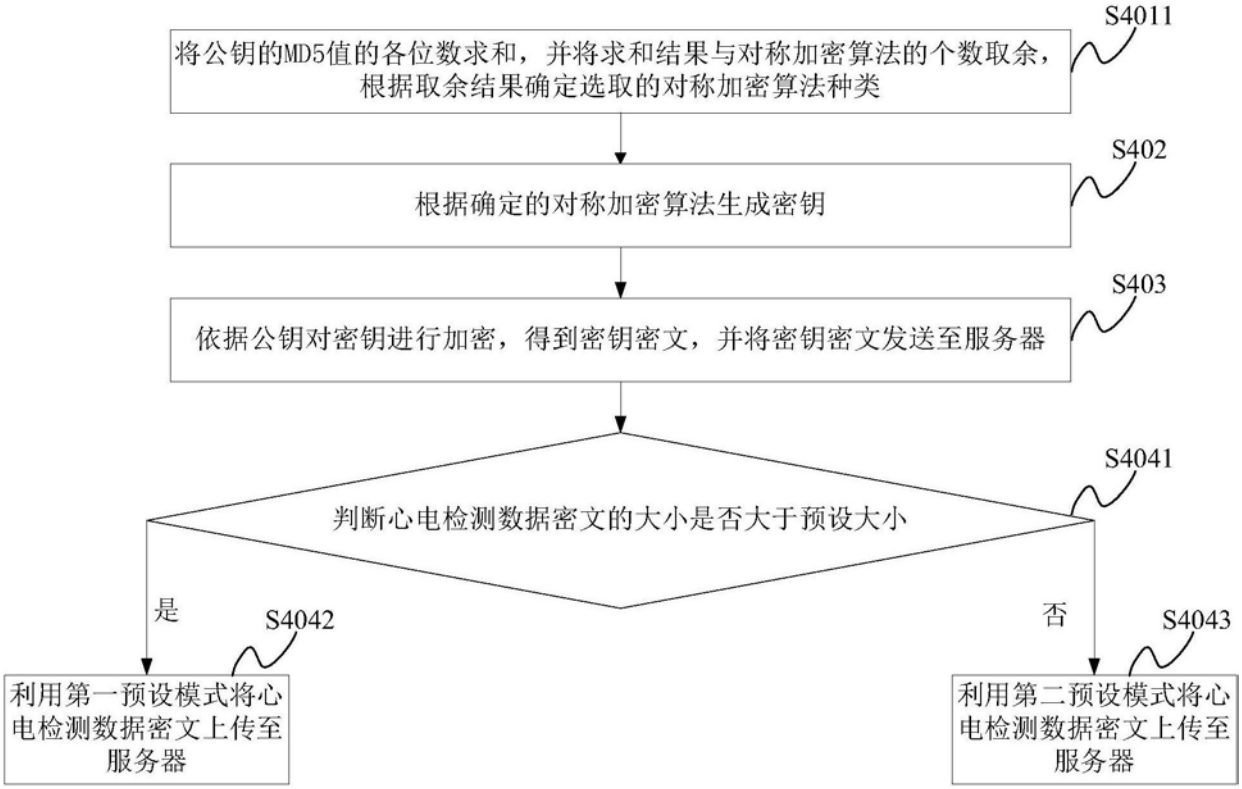

S4011
将公钥的MD5值的各位数求和，并将求和结果与对称加密算法的个数取余，根据取余结果确定选取的对称加密算法种类
S402
根据确定的对称加密算法生成密钥
S403
依据公钥对密钥进行加密，得到密钥密文，并将密钥密文发送至服务器
S4041
判断心电检测数据密文的大小是否大于预设大小
是
S4042
利用第一预设模式将心电检测数据密文上传至服务器
否
S4043
利用第二预设模式将心电检测数据密文上传至服务器

图11

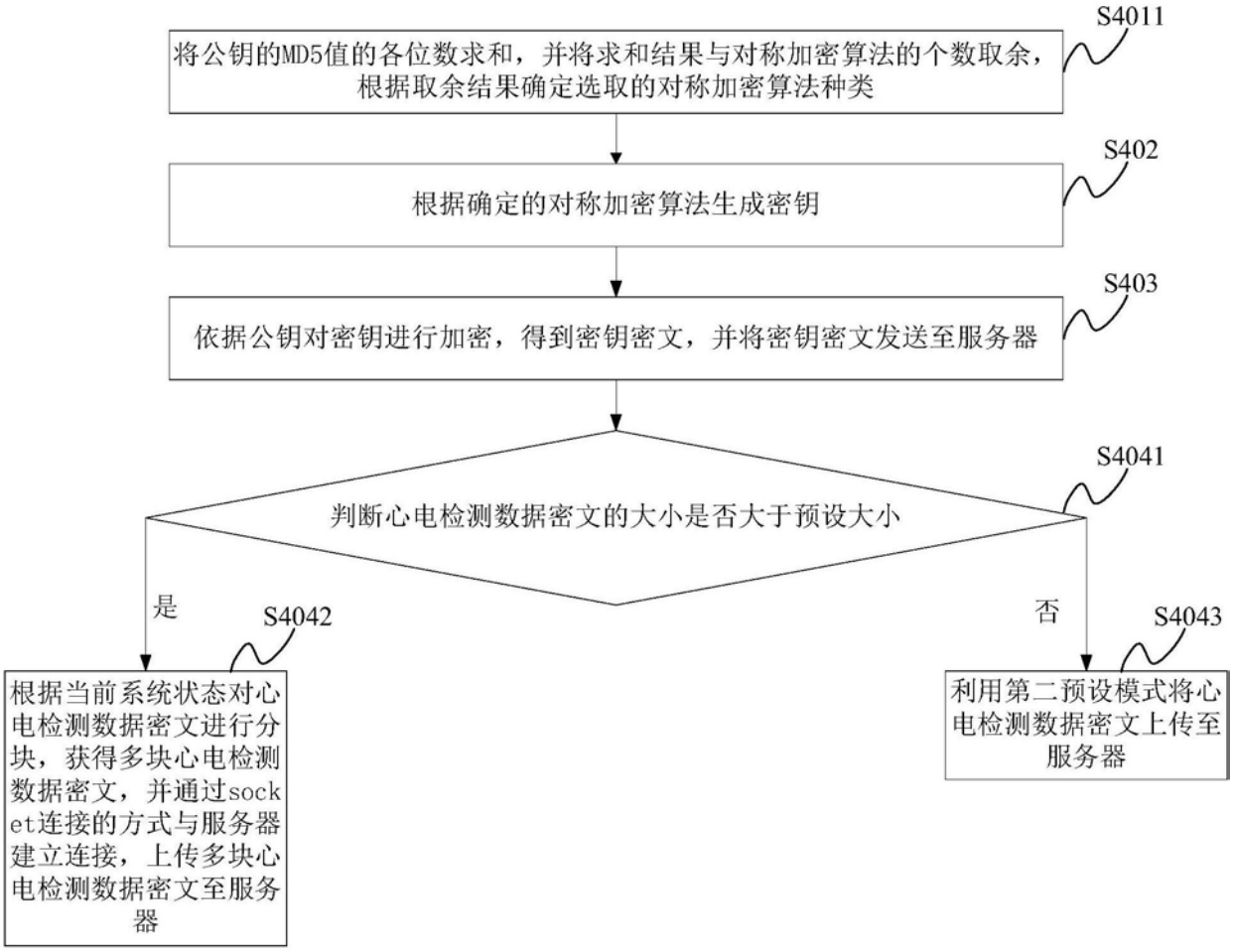

S4011
将公钥的MD5值的各位数求和，并将求和结果与对称加密算法的个数取余，根据取余结果确定选取的对称加密算法种类
S402
根据确定的对称加密算法生成密钥
S403
依据公钥对密钥进行加密，得到密钥密文，并将密钥密文发送至服务器
S4041
判断心电检测数据密文的大小是否大于预设大小
是
S4042
根据当前系统状态对心电检测数据密文进行分块，获得多块心电检测数据密文，并通过socket连接的方式与服务器建立连接，上传多块心电检测数据密文至服务器
否
S4043
利用第二预设模式将心电检测数据密文上传至服务器

图12

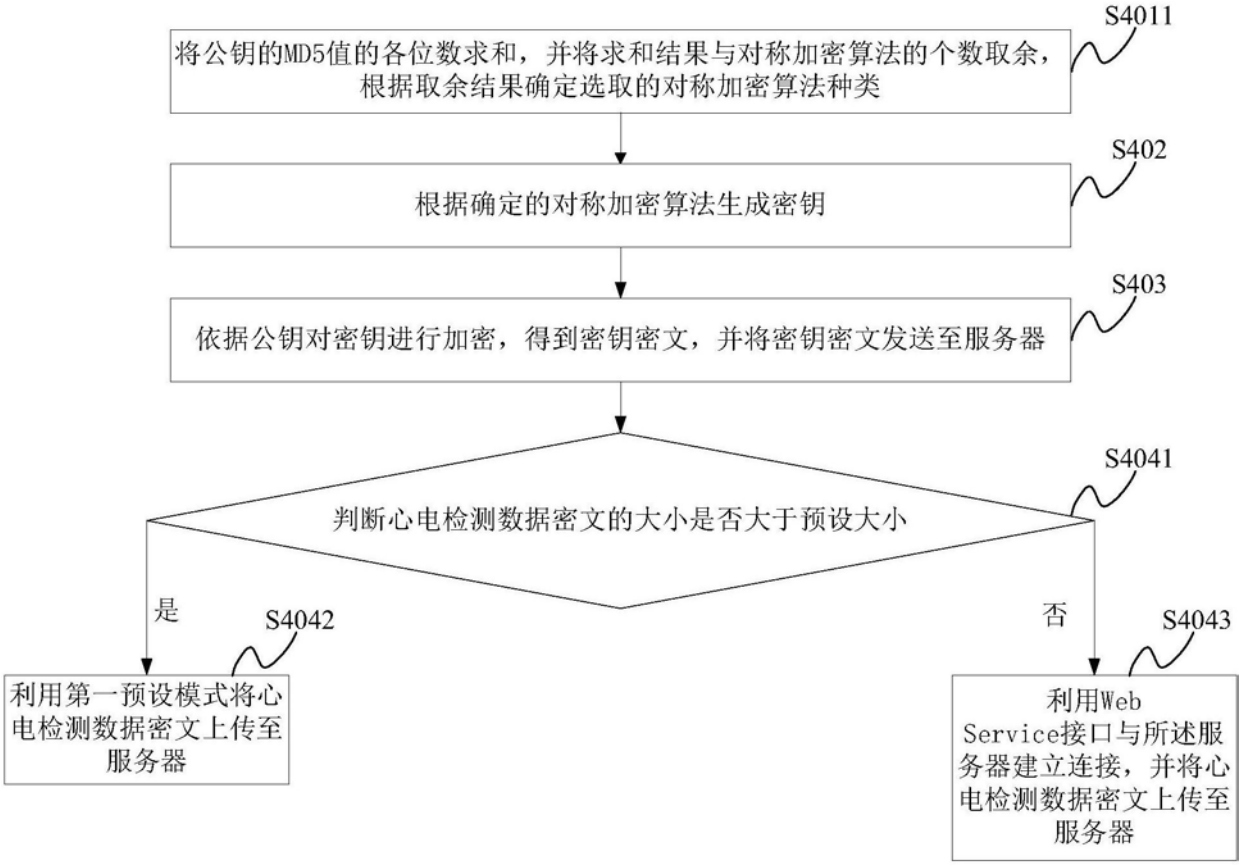

S4011
将公钥的MD5值的各位数求和，并将求和结果与对称加密算法的个数取余，根据取余结果确定选取的对称加密算法种类
S402
根据确定的对称加密算法生成密钥
S403
依据公钥对密钥进行加密，得到密钥密文，并将密钥密文发送至服务器
S4041
判断心电检测数据密文的大小是否大于预设大小
是
S4042
利用第一预设模式将心电检测数据密文上传至服务器
否
S4043
利用Web Service接口与所述服务器建立连接，并将心电检测数据密文上传至服务器

图13

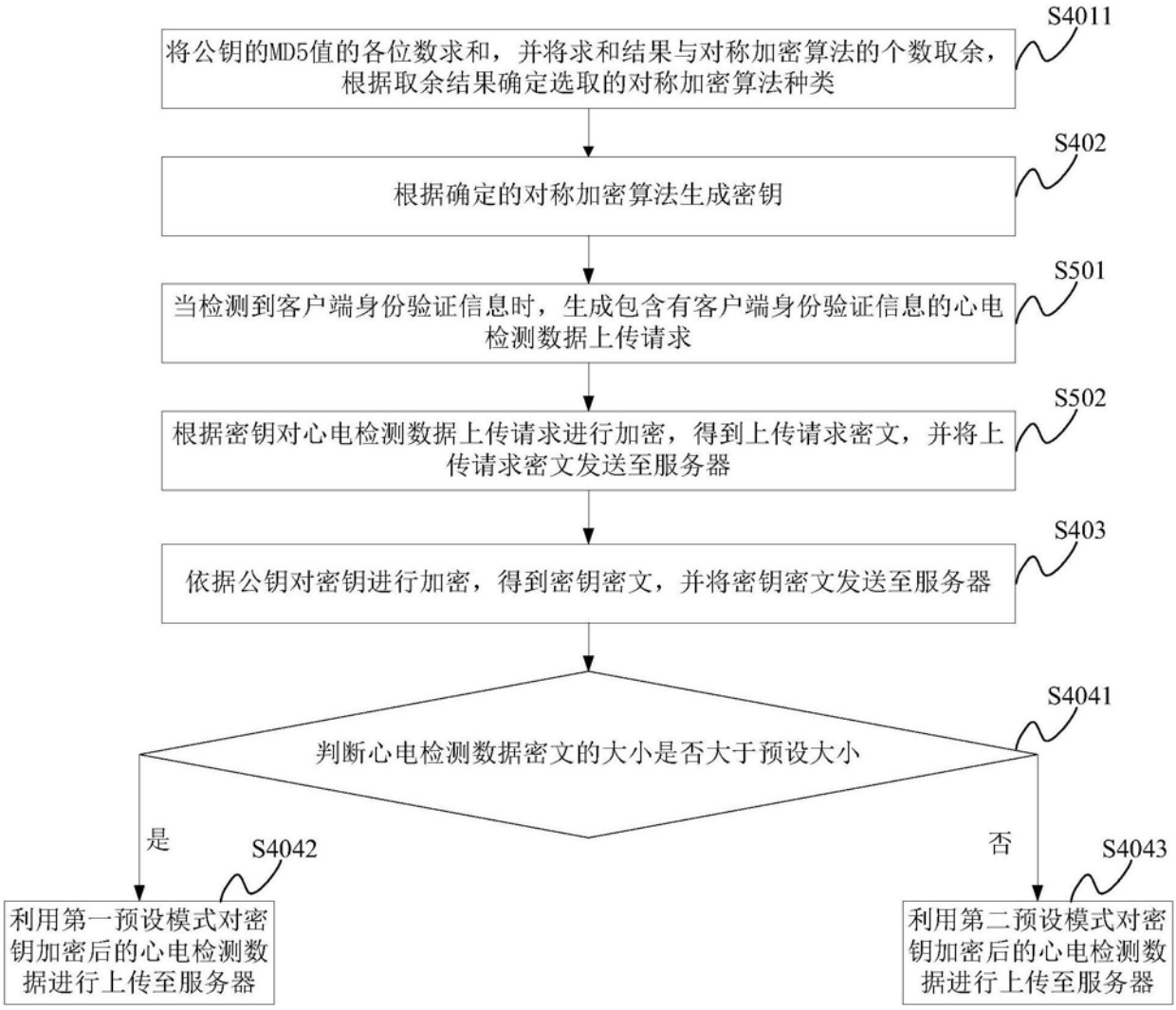

S4011
将公钥的MD5值的各位数求和，并将求和结果与对称加密算法的个数取余，根据取余结果确定选取的对称加密算法种类
S402
根据确定的对称加密算法生成密钥
S501
当检测到客户端身份验证信息时，生成包含有客户端身份验证信息的心电检测数据上传请求
S502
根据密钥对心电检测数据上传请求进行加密，得到上传请求密文，并将上传请求密文发送至服务器
S403
依据公钥对密钥进行加密，得到密钥密文，并将密钥密文发送至服务器
S4041
判断心电检测数据密文的大小是否大于预设大小
是
S4042
利用第一预设模式对密钥加密后的心电检测数据进行上传至服务器
否
S4043
利用第二预设模式对密钥加密后的心电检测数据进行上传至服务器

图14

专利名称(译)	一种心电检测数据上传系统及方法		
公开(公告)号	CN108737334A	公开(公告)日	2018-11-02
申请号	CN201710250601.1	申请日	2017-04-17
[标]申请(专利权)人(译)	中国科学院微电子研究所		
申请(专利权)人(译)	中国科学院微电子研究所		
当前申请(专利权)人(译)	中国科学院微电子研究所		
[标]发明人	李国君 陈岚		
发明人	李国君 陈岚		
IPC分类号	H04L29/06 H04L29/08 A61B5/00		
CPC分类号	A61B5/0006 H04L63/045 H04L63/08 H04L67/02		
外部链接	Espacenet SIPO		

摘要(译)

本申请公开了一种心电检测数据上传系统及方法，其中，所述心电检测数据上传系统利用非对称加密算法产生公钥和私钥，并将公钥下发给客户端以供客户端确定对称加密算法并生成密钥，由于私钥不在服务器和客户端中进行传输，即使根据公钥对密钥进行加密得到的密文在传输过程中被第三方截获，由于第三方不具有私钥，无法对密文进行解密，从而无法得到密钥，也就无法解密使用密钥加密的心电检测数据，这就提升了心电检测数据传输过程的保密程度；并且在该系统中，仅利用非对称加密算法产生公钥和私钥，而不直接利用非对称加密算法对心电检测数据进行加密，提升了心电检测数据的加密效率。