(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 115795514 A
(43)申请公布日 2023.03.14

(21)申请号 202211652351.1

(22)申请日 2022.12.21

(71)申请人 绿盟科技集团股份有限公司
地址 100089 北京市海淀区北洼路4号益泰大厦5层
申请人 北京神州绿盟科技有限公司

(72)发明人 王真 汤旭 陈磊 李德全 高翔 刘文懋

(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
专利代理师 刘源

(51)Int.Cl.
G06F 21/60(2013.01)
G06F 21/62(2019.01)
G06F 16/245(2013.01)

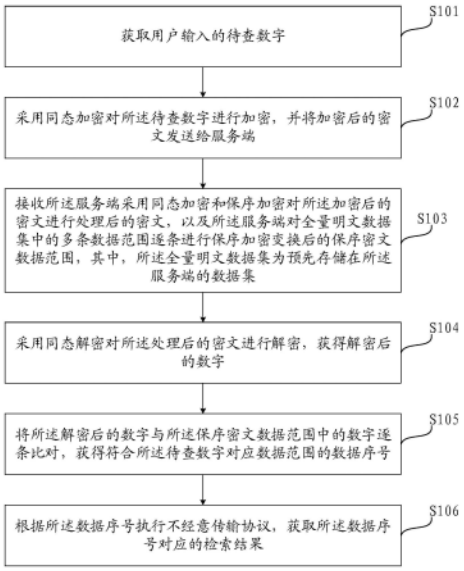
权利要求书3页 说明书12页 附图7页

(54)发明名称

一种隐私信息检索方法、装置及系统

(57)摘要

本发明提供了一种隐私信息检索方法、装置及系统，其中，该隐私信息检索方法，应用于客户端，包括：获取用户输入的待查数字；采用同态加密对所述待查数字进行加密，并将加密后的密文发送给服务端；接收所述服务端采用同态加密和保序加密对所述加密后的密文进行处理后的密文，以及所述服务端对全量明文数据集中的多条数据范围逐条进行保序加密变换后的保序密文数据范围；采用同态解密对所述处理后的密文进行解密，获得解密后的数字；将所述解密后的数字与所述保序密文数据范围中的数字逐条比对，获得符合所述待查数字对应数据范围的数据序号；根据所述数据序号执行不经意传输协议，获取所述数据序号对应的检索结果。



CN 115795514 A

1.一种隐私信息检索方法,应用于客户端,其特征在于,包括:

获取用户输入的待查数字;

采用同态加密对所述待查数字进行加密,并将加密后的密文发送给服务端;

接收所述服务端采用同态加密和保序加密对所述加密后的密文进行处理后的密文,以及所述服务端对全量明文数据集中的多条数据范围逐条进行保序加密变换后的保序密文数据范围,其中,所述全量明文数据集为预先存储在所述服务端的数据集;

采用同态解密对所述处理后的密文进行解密,获得解密后的数字;

将所述解密后的数字与所述保序密文数据范围中的数字逐条比对,获得符合所述待查数字对应数据范围的数据序号;

根据所述数据序号执行不经意传输协议,获取所述数据序号对应的检索结果。

2.如权利要求1所述的方法,其特征在于,所述采用同态加密对所述待查数字进行加密,并将加密后的密文发送给服务端,包括:

生成用于同态加密的公钥和私钥;

利用所述公钥加密隐藏所述待查数字,获取加密后的密文;

将所述加密后的密文以及所述公钥发送给服务端,并存储所述私钥。

3.如权利要求2所述的方法,其特征在于,所述接收所述服务端采用同态加密和保序加密对所述加密后的密文进行处理后的密文,以及所述服务端对全量明文数据集中的多条数据范围逐条进行保序加密变换后的保序密文数据范围,包括:

接收所述服务端用所述公钥分别对随机生成的两个数字进行加密所得的第一密文和第二密文,以及所述第一密文和所述第二密文对所述加密后的密文进行同态乘法运算和同态加法运算所得的处理后的密文,其中,所述两个数字为用于保序加密的密钥;

接收所述服务端利用所述两个数字对全量明文数据集中的多条数据范围逐条进行保序加密变换后的保序密文数据范围。

4.如权利要求3所述的方法,其特征在于,所述采用同态解密对所述处理后的密文进行解密,获得解密后的数字,包括:

利用所述私钥对所述处理后的密文进行解密,获得经所述服务端利用所述两个数字进行保序加密后的数字,并将所述保序加密后的数字作为解密后的数字。

5.一种隐私信息检索方法,应用于服务端,其特征在于,包括:

接收来自客户端的加密后的密文,所述加密后的密文为所述客户端采用同态加密对用户输入的待查数字进行加密的密文;

采用同态加密和保序加密对所述加密后的密文进行处理,获得处理后的密文;

对全量明文数据集中的多条数据范围逐条进行保序加密变换,获得保序密文数据范围,其中,所述全量明文数据集为预先存储在所述服务端的数据集;

将所述处理后的密文和所述保序密文数据范围发送给所述客户端,以使所述客户端将采用同态解密对所述处理后的密文进行解密所获得的解密后的数字,与所述保序密文数据范围中的数字逐条比对,并获得符合所述待查数字对应数据范围的数据序号。

6.如权利要求5所述的方法,其特征在于,所述采用同态加密和保序加密对所述加密后的密文进行处理,获得处理后的密文,包括:

随机生成用于保序加密的两个数字;

接收所述客户端发送的用于同态加密的公钥，并通过所述公钥对所述两个数字进行加密，分别获得第一密文和第二密文；

采用所述第一密文和所述第二密文对所述加密后的密文进行同态乘法运算和同态加法运算，获得处理后的密文。

7.一种隐私信息检索装置，应用于客户端，其特征在于，包括：

第一获取单元，用于获取用户输入的待查数字；

加密单元，用于采用同态加密对所述待查数字进行加密，并将加密后的密文发送给服务端；

第一接收单元，用于接收所述服务端采用同态加密和保序加密对所述加密后的密文进行处理后的密文，以及所述服务端对全量明文数据集中的多条数据范围逐条进行保序加密变换后的保序密文数据范围，其中，所述全量明文数据集为预先存储在所述服务端的数据集；

解密单元，用于采用同态解密对所述处理后的密文进行解密，获得解密后的数字；

第一获得单元，用于将所述解密后的数字与所述保序密文数据范围中的数字逐条比对，获得符合所述待查数字对应数据范围的数据序号；

第二获取单元，用于根据所述数据序号执行不经意传输协议，获取所述数据序号对应的检索结果。

8.一种隐私信息检索装置，应用于服务端，其特征在于，包括：

第二接收单元，用于接收来自客户端的加密后的密文，所述加密后的密文为所述客户端采用同态加密对用户输入的待查数字进行加密的密文；

处理单元，用于采用同态加密和保序加密对所述加密后的密文进行处理，获得处理后的密文；

第二获得单元，用于对全量明文数据集中的多条数据范围逐条进行保序加密变换，获得保序密文数据范围，其中，所述全量明文数据集为预先存储在所述服务端的数据集；

发送单元，用于将所述处理后的密文和所述保序密文数据范围发送给所述客户端，以使所述客户端将采用同态解密对所述处理后的密文进行解密所获得的解密后的数字，与所述保序密文数据范围中的数字逐条比对，并获得符合所述待查数字对应数据范围的数据序号。

9.一种隐私信息检索系统，其特征在于，包括：

客户端以及与所述客户端连接的服务端；其中：所述客户端被配置为：

获取用户输入的待查数字；

采用同态加密对所述待查数字进行加密，并将加密后的密文发送给所述服务端；

接收所述服务端采用同态加密和保序加密对所述加密后的密文进行处理后的密文，以及所述服务端对全量明文数据集中的多条数据范围逐条进行保序加密变换后的保序密文数据范围，其中，所述全量明文数据集为预先存储在所述服务端的数据集；

采用同态解密对所述处理后的密文进行解密，获得解密后的数字；

将所述解密后的数字与所述保序密文数据范围中的数字逐条比对，获得符合所述待查数字对应数据范围的数据序号；

根据所述数据序号执行不经意传输协议，获取所述数据序号对应的检索结果。

10.一种隐私信息检索装置,其特征在于,所述检索装置包括处理器,所述处理器用于执行存储器中存储的计算机程序时实现如权利要求1-6任一项所述的隐私信息检索方法的步骤。

一种隐私信息检索方法、装置及系统

技术领域

[0001] 本发明涉及信息技术领域，尤其涉及一种隐私信息检索方法、装置及系统。

背景技术

[0002] 隐私信息检索协议可以实现服务端不知道用户检索条件和检索结果的前提下，实现用户的检索任务。

[0003] 在隐私信息检索领域，现有隐私信息检索方法仅实现了基于关键字检索的方法，尚无法做到支持数据范围检索。以如下场景为例，安全企业C掌握了软件D的漏洞信息，形成知识库，该知识库的存储样例为：{漏洞1，影响版本范围(1.2～3.7)}，……，{漏洞n，影响版本范围(3.9～7.8)}。某用户U(比如，金融、工控等安全要求较高领域的客户)恰好使用了该软件D，假设所用的版本是4.7，用户U希望在不暴露自己所用版本号的前提下，让安全企业C给出该软件D在4.7特定版本下的漏洞信息，由于涉及到数据范围的检索，目前无法用基于关键字的隐私信息检索方法实现。

[0004] 如此一来，如何实现基于数据范围的隐私信息检索成为急需解决的技术问题。

发明内容

[0005] 本发明实施例提供了一种隐私信息检索方法、装置及系统，用于实现基于数据范围的隐私信息检索，保证用户的信息安全。

[0006] 第一方面，本发明实施例提供了一种隐私信息检索方法，应用于客户端，包括：

[0007] 获取用户输入的待查数字；

[0008] 采用同态加密对所述待查数字进行加密，并将加密后的密文发送给服务端；

[0009] 接收所述服务端采用同态加密和保序加密对所述加密后的密文进行处理后的密文，以及所述服务端对全量明文数据集中的多条数据范围逐条进行保序加密变换后的保序密文数据范围，其中，所述全量明文数据集为预先存储在所述服务端的数据集；

[0010] 采用同态解密对所述处理后的密文进行解密，获得解密后的数字；

[0011] 将所述解密后的数字与所述保序密文数据范围中的数字逐条比对，获得符合所述待查数字对应数据范围的数据序号；

[0012] 根据所述数据序号执行不经意传输协议，获取所述数据序号对应的检索结果。

[0013] 在其中一种可能的实现方式中，所述采用同态加密对所述待查数字进行加密，并将加密后的密文发送给服务端，包括：

[0014] 生成用于同态加密的公钥和私钥；

[0015] 利用所述公钥加密隐藏所述待查数字，获取加密后的密文；

[0016] 将所述加密后的密文以及所述公钥发送给服务端，并存储所述私钥。

[0017] 在其中一种可能的实现方式中，所述接收所述服务端采用同态加密和保序加密对所述加密后的密文进行处理后的密文，以及所述服务端对全量明文数据集中的多条数据范围逐条进行保序加密变换后的保序密文数据范围，包括：

[0018] 接收所述服务端用所述公钥分别对随机生成的两个数字进行加密所得的第一密文和第二密文，以及所述第一密文和所述第二密文对所述加密后的密文进行同态乘法运算和同态加法运算所得的处理后的密文，其中，所述两个数字为用于保序加密的密钥；

[0019] 接收所述服务端利用所述两个数字对全量明文数据集中的多条数据范围逐条进行保序加密变换后的保序密文数据范围。

[0020] 在其中一种可能的实现方式中，所述采用同态解密对所述处理后的密文进行解密，获得解密后的数字，包括：

[0021] 利用所述私钥对所述处理后的密文进行解密，获得经所述服务端利用所述两个数字进行保序加密后的数字，并将所述保序加密后的数字作为解密后的数字。

[0022] 第二方面，本发明实施例还提供了一种隐私信息检索方法，应用于服务端，包括：

[0023] 接收来自客户端的加密后的密文，所述加密后的密文为所述客户端采用同态加密对用户输入的待查数字进行加密的密文；

[0024] 采用同态加密和保序加密对所述加密后的密文进行处理，获得处理后的密文；

[0025] 对全量明文数据集中的多条数据范围逐条进行保序加密变换，获得保序密文数据范围，其中，所述全量明文数据集为预先存储在所述服务端的数据集；

[0026] 将所述处理后的密文和所述保序密文数据范围发送给所述客户端，以使所述客户端将采用同态解密对所述处理后的密文进行解密所获得的解密后的数字，与所述保序密文数据范围中的数字逐条比对，并获得符合所述待查数字对应数据范围的数据序号。

[0027] 在其中一种可能的实现方式中，所述采用同态加密和保序加密对所述加密后的密文进行处理，获得处理后的密文，包括：

[0028] 随机生成用于保序加密的两个数字；

[0029] 接收所述客户端发送的用于同态加密的公钥，并通过所述公钥对所述两个数字进行加密，分别获得第一密文和第二密文；

[0030] 采用所述第一密文和所述第二密文对所述加密后的密文进行同态乘法运算和同态加法运算，获得处理后的密文。

[0031] 第三方面，本发明实施例还提供了一种隐私信息检索装置，应用于客户端，包括：

[0032] 第一获取单元，用于获取用户输入的待查数字；

[0033] 加密单元，用于采用同态加密对所述待查数字进行加密，并将加密后的密文发送给服务端；

[0034] 第一接收单元，用于接收所述服务端采用同态加密和保序加密对所述加密后的密文进行处理后的密文，以及所述服务端对全量明文数据集中的多条数据范围逐条进行保序加密变换后的保序密文数据范围，其中，所述全量明文数据集为预先存储在所述服务端的数据集；

[0035] 解密单元，用于采用同态解密对所述处理后的密文进行解密，获得解密后的数字；

[0036] 第一获得单元，用于将所述解密后的数字与所述保序密文数据范围中的数字逐条比对，获得符合所述待查数字对应数据范围的数据序号；

[0037] 第二获取单元，用于根据所述数据序号执行不经意传输协议，获取所述数据序号对应的检索结果。

[0038] 第四方面，本发明实施例还提供了一种隐私信息检索装置，应用于服务端，包括：

[0039] 第二接收单元，用于接收来自客户端的加密后的密文，所述加密后的密文为所述客户端采用同态加密对用户输入的待查数字进行加密的密文；

[0040] 处理单元，用于采用同态加密和保序加密对所述加密后的密文进行处理，获得处理后的密文；

[0041] 第二获得单元，用于对全量明文数据集中的多条数据范围逐条进行保序加密变换，获得保序密文数据范围，其中，所述全量明文数据集为预先存储在所述服务端的数据集；

[0042] 发送单元，用于将所述处理后的密文和所述保序密文数据范围发送给所述客户端，以使所述客户端将采用同态解密对所述处理后的密文进行解密所获得的解密后的数字，与所述保序密文数据范围中的数字逐条比对，并获得符合所述待查数字对应数据范围的数据序号。

[0043] 第五方面，本发明实施例还提供了一种隐私信息检索系统，包括：

[0044] 客户端以及与所述客户端连接的服务端；其中：所述客户端被配置为：

[0045] 获取用户输入的待查数字；

[0046] 采用同态加密对所述待查数字进行加密，并将加密后的密文发送给所述服务端；

[0047] 接收所述服务端采用同态加密和保序加密对所述加密后的密文进行处理后的密文，以及所述服务端对全量明文数据集中的多条数据范围逐条进行保序加密变换后的保序密文数据范围，其中，所述全量明文数据集为预先存储在所述服务端的数据集；

[0048] 采用同态解密对所述处理后的密文进行解密，获得解密后的数字；

[0049] 将所述解密后的数字与所述保序密文数据范围中的数字逐条比对，获得符合所述待查数字对应数据范围的数据序号；

[0050] 根据所述数据序号执行不经意传输协议，获取所述数据序号对应的检索结果。

[0051] 第六方面，本发明实施例还提供了一种隐私信息检索装置，所述检索装置包括处理器，所述处理器用于执行存储器中存储的计算机程序时实现如第一方面和/或第二方面所述的隐私信息检索方法的步骤。

[0052] 第七方面，本发明实施例还提供了一种可读存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时实现如第一方面和/或第二方面所述的隐私信息检索方法的步骤。

[0053] 本发明的有益效果如下：

[0054] 本发明实施例提供了一种隐私信息检索方法、装置及系统，其中，首先，获取用户输入的待查数字，然后，采用同态加密对待查数字进行加密，并将加密后的密文发送给服务端；该服务端采用同态加密和保序加密对该加密后的密文进行处理，并对预先存储在服务端的全量明文数据集中的多条数据范围逐条进行保序加密变换，获得保序密文数据范围，然后，将处理后的密文和保序密文数据范围发送给客户端；然后，客户端采取同态解密对该处理后的密文进行解密，获得解密后的数字；然后，将该解密后的数字与保序密文数据范围中的数字逐条比对，获得符合待查数字对应数据范围的数据序号；然后，根据该数据序号执行不经意传输协议，获得该数据序号对应的检索结果。

[0055] 如此一来，通过同态加密和保序加密，可以实现对服务端数据的保护，以及客户端对服务端数据的密文范围检索。从而保证了服务端范围数据以保序密文的形式呈现给用

户，这样的话，用户在不知道保序密钥的情况下，无法反解密服务端的原始数据范围明文；同时，保序密文保证了客户端可以对服务端数据进行依次保序密文范围检索；从而实现了支持数据范围的隐私信息检索，保证了用户的信息安全。

附图说明

[0056] 图1为本发明实施例提供的一种隐私信息检索方法的其中一种方法流程图；

[0057] 图2为图1中步骤S102的其中一种方法流程图；

[0058] 图3为图1中步骤S103的其中一种方法流程图；

[0059] 图4为本发明实施例提供的一种隐私信息检索方法中基于同态加密和保序加密确定数据序号的其中一种方法示意图；

[0060] 图5为本发明实施例提供的一种隐私信息检索方法中支持范围查询的隐私信息检索方案的具体实现过程的方法示意图；

[0061] 图6为本发明实施例提供的一种隐私信息检索方法中隐私查询阶段所采用的多选1的不经意传输协议的其中一种方法示意图；

[0062] 图7为本发明实施例提供的一种隐私信息检索方法的另外一种方法流程图；

[0063] 图8为图7中步骤S402的其中一种方法流程图；

[0064] 图9为本发明实施例提供的一种隐私信息检索装置的其中一种结构框图；

[0065] 图10为本发明实施例提供的一种隐私信息检索装置的另外一种结构框图；

[0066] 图11为本发明实施例提供的一种隐私信息检索系统的其中一种结构框图。

具体实施方式

[0067] 为使本发明实施例的目的、技术方案和优点更加清楚，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作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] 本发明的说明书和权利要求书及上述附图中的“第一”、“第二”等是用于区别不同对象，而不是用于描述特定顺序。此外，术语“包括”以及它们的任何变形，意图在于覆盖不排他的包含。例如包含了一系列步骤或单元的过程、方法、系统、产品或设备没有限定于已列出的步骤或单元，而是可选地还包括没有列出的步骤或单元，或可选地还包括对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0069] 在本文中提及“实施例”意味着，结合实施例描述的特定特征、结构或特性可以包含在本发明的至少一个实施例中。在说明书中的各个位置出现该短语并不一定均是指相同的实施例，也不是与其它实施例互斥的独立的或备选的实施例。本领域技术人员显式地和隐式地理解的是，本文所描述的实施例可以与其它实施例相结合。

[0070] 本发明实施例中术语“和/或”，描述关联对象的关联关系，表示可以存在三种关系，例如，A和/或B，可以表示：单独存在A，同时存在A和B，单独存在B这三种情况。字符“/”一般表示前后关联对象是一种“或”的关系。

[0071] 本发明实施例描述的应用场景是为了更加清楚的说明本发明实施例的技术方案，并不构成对于本发明实施例提供的技术方案的限定，本领域普通技术人员可知，随着新应

用场景的出现，本发明实施例提供的技术方案对于类似的技术问题，同样适用。其中，在本发明的描述中，除非另有说明，“多个”的含义是两个或两个以上。

[0072] 在相关技术中，现有隐私信息检索方法仅实现了基于关键字检索的方法，尚无法做到支持数据范围检索。

[0073] 鉴于此，本发明实施例提供了一种隐私信息检索方法、装置及系统，用于实现基于数据范围的隐私信息检索，保证用户的信息安全。

[0074] 在介绍本发明所提及的隐私信息检索方法、装置及系统之前，对所涉及到的相关术语进行简单的介绍。

[0075] 隐私信息检索(Private Information Retrieval,PIR)，又称匿踪查询，通过PIR可以保证查询用户向服务端上的数据库提交查询请求时，在用户查询隐私信息不被泄漏的条件下完成查询，也就是说，在用户查询过程中，服务端不知道用户具体查询信息以及检索出的数据项。

[0076] 保序加密(Order Preserving Encryption,OPE)，指的是明文的顺序和密文的顺序是匹配的，比如，如果明文a和b满足a＜b，那么经过加密后的密文k(a)和k(b)也满足k(a)＜k(b)。

[0077] 对于不经意传输协议(Oblivious Transfer,OT)，在隐私信息查询阶段，客户端利用已知数据项(index)，服务端利用已知数据集E，双方共同执行多选一的OT协议，客户端可以获得最终的检索结果，服务端仅能猜测到客户端检索结果是数据集E中的某一项，但并不能确定具体是哪一项。举个具体的例子来说，张三拥有n条消息$\{m_1,\cdots\cdots,m_n\}$，李四想知道其中一条消息m_i；通过执行OT协议，李四可以正确获得想要知道的消息m_i，无法获得n条消息里其它(n-1)条消息，而张三无法知道李四获得的是哪条消息。

[0078] 如图1所示，本发明实施例提供了一种隐私信息检索方法，应用于客户端，包括：

[0079] S101：获取用户输入的待查数字；

[0080] S102：采用同态加密对所述待查数字进行加密，并将加密后的密文发送给服务端；

[0081] S103：接收所述服务端采用同态加密和保序加密对所述加密后的密文进行处理后的密文，以及所述服务端对全量明文数据集中的多条数据范围逐条进行保序加密变换后的保序密文数据范围，其中，所述全量明文数据集为预先存储在所述服务端的数据集；

[0082] S104：采用同态解密对所述处理后的密文进行解密，获得解密后的数字；

[0083] S105：将所述解密后的数字与所述保序密文数据范围中的数字逐条比对，获得符合所述待查数字对应数据范围的数据序号；

[0084] S106：根据所述数据序号执行不经意传输协议，获取所述数据序号对应的检索结果。

[0085] 在具体实施过程中，对步骤S101至步骤S106的具体实现过程解释如下：

[0086] 首先，获取用户输入的待查数字，比如，a；然后，采用同态加密对该待查数字进行加密，并将该加密后的密文发送给服务端；在其中一种示例性实施例中，客户端可以是根据产生的同态加密所用的公钥对该待查数字进行加密；客户端将加密后的密文发送给服务端之后，接收服务端采用同态加密和保序加密对该加密后的密文进行处理后的密文，以及该服务端对全量明文数据集中多条数据范围逐条进行保序加密变换后的保序密文数据范围。

[0087] 然后，采用同态解密对处理后的密文进行解密，获得解密后的数字。在其中一种示

例性实施例中，可以是利用客户端产生的与同态加密所用的公钥相对应的私钥，对处理后的密文进行解密，获得解密后的数字；然后，将该解密后的数字与保序密文数据范围中的数字逐条比对，获得符合待查数字对应数据范围的数据序号；然后，根据该数据序号执行不经意传输协议，获取该数据序号对应的检索结果。如此一来，通过同态加密和保序加密，可以实现对服务端数据的保护，以及客户端对服务端数据的密文范围检索。从而保证了服务端范围数据以保序密文的形式呈现给用户，这样的话，用户在不知道保序密钥的情况下，无法反解密服务端的原始数据范围明文；同时，保序密文保证了客户端可以对服务端数据进行依次保序密文范围检索；从而实现了支持数据范围的隐私信息检索，保证了用户的信息安全。

[0088] 在本发明实施例中，如图2所示，步骤S102：采用同态加密对所述待查数字进行加密，并将加密后的密文发送给服务端，包括：

[0089] S201：生成用于同态加密的公钥和私钥；

[0090] S202：利用所述公钥加密隐藏所述待查数字，获取加密后的密文；

[0091] S203：将所述加密后的密文以及所述公钥发送给服务端，并存储所述私钥。

[0092] 在具体实施过程中，步骤S201至步骤S203的具体实现过程如下：

[0093] 首先，客户端产生同态加密所用的公私钥对，该公私钥对包括公钥和私钥；然后，利用该公钥加密隐藏用户输入的待查数字，获得加密后的密文；然后，将该加密后的密文和公钥发送给服务端，同时，客户端存储私钥。

[0094] 在本发明实施例中，如图3所示，步骤S103：接收所述服务端采用同态加密和保序加密对所述加密后的密文进行处理后的密文，以及所述服务端对全量明文数据集中的多条数据范围逐条进行保序加密变换后的保序密文数据范围，包括：

[0095] S301：接收所述服务端用所述公钥分别对随机生成的两个数字进行加密所得的第一密文和第二密文，以及所述第一密文和所述第二密文对所述加密后的密文进行同态乘法运算和同态加法运算所得的处理后的密文，其中，所述两个数字为用于保序加密的密钥；

[0096] S302：接收所述服务端利用所述两个数字对全量明文数据集中的多条数据范围逐条进行保序加密变换后的保序密文数据范围。

[0097] 在具体实施过程中，步骤S301至步骤S302的具体实现过程如下：

[0098] 首先，在客户端将加密后的密文以及公钥发送给服务端之后，服务端利用公钥分别对随机生成的两个数字进行加密，获得第一密文和第二密文；在其中一种示例性实施例中，客户端生成的公私钥对为(pk，sk)，其中，pk表示公钥，sk表示私钥；客户端用公钥pk对用户输入的待查数字a加密后，获得加密后的密文为En_a＝E(pk，a)；服务端随机生成的两个数字分别为x和y，这两个数字可以用做保序加密中的密钥；服务端利用公钥pk加密x，获得第一密文En_x＝E(pk，x)，利用公钥pk加密y，获得第二密文En_y＝E(pk，y)；然后，服务端对加密后的密文En_a进行同态乘法运算和同态加法运算，得到的处理后的密文$En_En_a = En_a \odot En_x \oplus En_y$，其中，⊙表示密文同态相乘，⊕表示密文同态相加。然后，服务端利用保序加密密钥x和y对全量明文数据集中的多条数据范围逐条进行保序加密变换，生成保序密文数据范围。然后，服务端将该保序密文数据范围发送给客户端，以使客户端根据所接收到第一密文和第二密文对加密后的密文进行同态乘法运算和同态加法运算所得的处理后的密文，以及保序密文数据范围确定待查数字对应数据范围的数据序号。

此外，对于数据序号确定的具体实现过程可以参照下述相关部分的描述，在此不做详述。

[0099] 在本发明实施例中，步骤S104：采用同态解密对所述处理后的密文进行解密，获得解密后的数字，包括：

[0100] 利用所述私钥对所述处理后的密文进行解密，获得经所述服务端利用所述两个数字进行保序加密后的数字，并将所述保序加密后的数字作为解密后的数字。

[0101] 在具体实施过程中，在客户端接收到服务端采用同态加密和保序加密对加密后的密文进行处理后的密文之后，客户端可以利用私钥对处理后的密文进行解密；仍以上述示例性实施例为例，客户端可以采用同态加密私钥sk对处理后的密文En_En_a进行解密，从而得到经服务端利用保序加密密钥x和y保序加密后的数字A，且A＝(a*x+y)。

[0102] 下面结合图4所示对基于同态加密和保序加密确定数据序号的具体实现过程进行详细的解释说明。

[0103] 在其中一种示例性实施例中，服务端有n条数据范围{(a_1,b_1)，……，(a_n,b_n)}，这n条数据范围属于全量明文数据范围，其中的第i条数据范围满足$a_i<b_i$，i为1至n中的任意正整数，用户输入为a。为了确定用户的检索条件所能够匹配到的服务端的数据序号，就需要找到数据序号t，且满足$a_t<a<b_t$。对数据序号t的具体确定过程如下：

[0104] 首先，用户端产生同态加密所用公私密钥对(pk，sk)，pk为公钥，sk为私钥；然后，利用公钥pk加密隐藏用户输入的a，加密结果为En_a＝E(pk，a)；然后，将密文En_a和公钥pk传递给服务端。

[0105] 对于服务端，服务端随机生成两个数字x和y，用做保序加密中的密钥；然后，可以通过服务端中的第一计算模块，利用公钥，加密x和y，得到En_x＝E(pk，x)，En_y＝E(pk，y)；然后对密文En_a进行同态乘法运算和同态加法运算，得到密文$En_En_a=En_a\odot En_x\oplus En_y$，其中，⊙表示密文同态相乘，⊕表示密文同态相加；密文En_En_a展开后实际上等同于利用公钥pk对原始明文(a*x+y)进行加密后的结果；

[0106] 可以通过服务端中的第二计算模块，利用保序加密密钥x和y，对数据范围{(a_1,b_1)，……，(a_n,b_n)}中的n条数据逐条进行保序加密变换，生成保序密文数据范围En_db＝{$(A_1,B_{1)}$，……，(A_n,B_n)}，其中，$(A_1,B_1)=(a_1*x+y,b_1*x+y)$，$(A_n,B_n)=(a_n*x+y,b_n*x+y)$，对于$(A_i,B_i)=(a_i*x+y,b_i*x+y)$，$1\leqslant i\leqslant n$。

[0107] 然后，服务端中的第一计算模块和第二计算模块，分别将保序密文数据范围En_db和同态加密密文En_En_a发送给客户端。

[0108] 然后，客户端利用同态加密私钥sk对密文En_En_a进行解密，得到经服务端利用保序加密密钥x和y保序加密后的数字A，A＝D(sk，En_En_a)＝a*x+y。由于A和En_db是利用同样的保序加密密钥x和y加密而来，因此满足保序关系，所以，“找到数据序号t，满足$a_t<a<b_t$”的任务，也就变成了“找到数据序号t，满足$A_t<A<B_t$”。

[0109] 在客户端找到满足关系的数据序号t之后，即可执行不经意传输协议，获取检索结果。如此一来，便实现了基于同态加密和保序加密确定数据序号，能够实现支持范围查询的隐私信息检索。

[0110] 下面结合图5所示对本发明实施例中支持范围查询的隐私信息检索方案的具体实现过程进行详细的解释说明，其中，User表示客户端，Server表示服务端。

[0111] 在图5所示的示例性例中，预先存储在服务端的全量明文数据集(也称为原始明文

数据集)db为{[(range1_left,range1_right),plaintext1],…,[(rangen_left,rangen_right),plaintextn]},其内包括n条数据,其中,rangei_left,rangei_right)表示n条数据中的第i条数据对应的某个属性的范围区间,plaintexti表示n条数据中的第i条数据对应的某个属性的具体值。若用户在客户端输入的待查数字为a,相应地,需要服务端给出满足rangei_left＜a＜rangei_right的数据范围中的plaintexti。

[0112] 在图5所示的示例性实施例中支持范围查询的隐私信息检索方案,该检索方案包括公钥生成阶段、保序加密阶段、确定索引阶段和隐私信息查询阶段。

[0113] 在公钥生成阶段,客户端执行如下数据预处理:

[0114] 1、输入待查数字a;

[0115] 2、产生同态加密所用公私钥对(pk,sk),pk为公钥,sk为私钥;

[0116] 3、利用公钥pk加密隐藏用户的输入a,加密结果为En_a,加密公式为En_a＝E(pk,a),E()表示同态加密。然后,将密文En_a和公钥pk传递给服务端。

[0117] 在保序加密阶段,服务端在获取到公钥pk和密文En_a后,执行如下操作:

[0118] 4、随机生成两个符合一定要求的数字x和y,将x和y用作本次保序加密算法的密钥;在其中一种示例性实施例中,x和y可以是整数,在实际应用中,并不仅限于此。

[0119] 5、对En_a做计算:$En\_En\_a = En\_a \odot En\_x \oplus En\_y$,其中,⊙表示密文同态相乘,⊕表示密文同态相加;

[0120] 6、利用x和y,以及数据集db,生成保序加密的密文范围集En_list,En_list＝{(range1_left*x+y,range1_right*x+y),……,(rangen_left*x+y,rangen_right*x+y)};然后,将密文范围集En_list和变换后的密文数据En_En_a返回给客户端。

[0121] 在确定索引阶段,客户端在收到密文范围集En_list和变换后的密文数据En_En_a后,执行以下操作:

[0122] 7、利用同态加密私钥sk对密文数据En_En_a进行解密,得到A＝D(sk,En_En_a)＝a*x+y;

[0123] 8、利用A和En_list,找到满足范围的数据项,该数据项(index)即为待查数字的索引index。

[0124] 在隐私信息查询阶段,客户端利用已知index,服务端利用已知数据集db,双方共同执行n选1的不经意传输协议,客户端获得最终的检索结果;服务端仅能猜测到客户端检索结果是数据集db中的某一项,但并不能确定具体是哪一项。也就是说,客户端和服务端分别执行PIR,从而实现了支持数据范围的隐私信息检索。

[0125] 在图5所示的示例性实施例中,步骤3、5和7利用同态加密和保序加密算法,对客户端数据进行保序加密变换。从而确保了保序加密算法密钥对客户端的隐藏,同时可以保证服务端在不知道客户端原始数据情况下,对客户端数据进行保序加密变换。步骤2～8利用同态加密和保序加密算法,实现了服务端数据的保护和客户端对服务端数据的密文范围检索。从而确保了服务端范围数据以保序密文的形式呈现给用户,用户在不知道保序密钥的情况下无法反解密服务端原始数据范围明文;同时,保序密文保证了客户端可以对服务端数据进行一次保序密文范围检索。

[0126] 对于隐私信息查询阶段所采用的多选1的不经意传输协议,可以采用如图6所示的其中一种示例性实施例,来实现经典多选1不经意传输协议,其中,用户端也称为客户端。在

该示例性实施例中，可以利用RSA公钥加密和高级加密标准(Advanced Encryption Standard，AES)对称加密来实现多选1不经意传输协议执行过程。对于具体的实现过程可以参照相关技术中的技术实现，在此不做详述。

[0127] 基于同一发明构思，如图7所示，本发明实施例还提供了一种隐私信息检索方法，应用于服务端，包括：

[0128] S401：接收来自客户端的加密后的密文，所述加密后的密文为所述客户端采用同态加密对用户输入的待查数字进行加密的密文；

[0129] S402：采用同态加密和保序加密对所述加密后的密文进行处理，获得处理后的密文；

[0130] S403：对全量明文数据集中的多条数据范围逐条进行保序加密变换，获得保序密文数据范围，其中，所述全量明文数据集为预先存储在所述服务端的数据集；

[0131] S404：将所述处理后的密文和所述保序密文数据范围发送给所述客户端，以使所述客户端将采用同态解密对所述处理后的密文进行解密所获得的解密后的数字，与所述保序密文数据范围中的数字逐条比对，并获得符合所述待查数字对应数据范围的数据序号。

[0132] 对于步骤S401至步骤S404的具体实现过程，可以参照前述相关部分的描述，在此不做赘述。

[0133] 在本发明实施例中，如图8所示，步骤S402：采用同态加密和保序加密对所述加密后的密文进行处理，获得处理后的密文，包括：

[0134] S501：随机生成用于保序加密的两个数字；

[0135] S502：接收所述客户端发送的用于同态加密的公钥，并通过所述公钥对所述两个数字进行加密，分别获得第一密文和第二密文；

[0136] S503：采用所述第一密文和所述第二密文对所述加密后的密文进行同态乘法运算和同态加法运算，获得处理后的密文。

[0137] 对于步骤S501至步骤S503的具体实现过程，可以参照前述相关部分的描述，在此不做赘述。

[0138] 此外，本发明实施例所提供的应用于服务端的隐私信息检索方法，与前述应用于客户端的隐私信息检索方法，二者所要解决的技术问题相同，相关部分的技术实现可以参照前述对应部分的具体描述，在此不做赘述。

[0139] 基于同一发明构思，如图9所示，本发明实施例还提供了一种隐私信息检索装置，应用于客户端，包括：

[0140] 第一获取单元10，用于获取用户输入的待查数字；

[0141] 加密单元20，用于采用同态加密对所述待查数字进行加密，并将加密后的密文发送给服务端；

[0142] 第一接收单元30，用于接收所述服务端采用同态加密和保序加密对所述加密后的密文进行处理后的密文，以及所述服务端对全量明文数据集中的多条数据范围逐条进行保序加密变换后的保序密文数据范围，其中，所述全量明文数据集为预先存储在所述服务端的数据集；

[0143] 解密单元40，用于采用同态解密对所述处理后的密文进行解密，获得解密后的数字；

[0144] 第一获得单元50，用于将所述解密后的数字与所述保序密文数据范围中的数字逐条比对，获得符合所述待查数字对应数据范围的数据序号；

[0145] 第二获取单元60，用于根据所述数据序号执行不经意传输协议，获取所述数据序号对应的检索结果。

[0146] 在本发明实施例中，所述加密单元20用于：

[0147] 生成用于同态加密的公钥和私钥；

[0148] 利用所述公钥加密隐藏所述待查数字，获取加密后的密文；

[0149] 将所述加密后的密文以及所述公钥发送给服务端，并存储所述私钥。

[0150] 在本发明实施例中，第一接收单元30用于：

[0151] 接收所述服务端用所述公钥分别对随机生成的两个数字进行加密所得的第一密文和第二密文，以及所述第一密文和所述第二密文对所述加密后的密文进行同态乘法运算和同态加法运算所得的处理后的密文，其中，所述两个数字为用于保序加密的密钥；

[0152] 接收所述服务端利用所述两个数字对全量明文数据集中的多条数据范围逐条进行保序加密变换后的保序密文数据范围。

[0153] 在本发明实施例中，解密单元40用于：

[0154] 利用所述私钥对所述处理后的密文进行解密，获得经所述服务端利用所述两个数字进行保序加密后的数字，并将所述保序加密后的数字作为解密后的数字。

[0155] 基于同一发明构思，如图10所示，本发明实施例还提供了一种隐私信息检索装置，应用于服务端，包括：

[0156] 第二接收单元70，用于接收来自客户端的加密后的密文，所述加密后的密文为所述客户端采用同态加密对用户输入的待查数字进行加密的密文；

[0157] 处理单元80，用于采用同态加密和保序加密对所述加密后的密文进行处理，获得处理后的密文；

[0158] 第二获得单元90，用于对全量明文数据集中的多条数据范围逐条进行保序加密变换，获得保序密文数据范围，其中，所述全量明文数据集为预先存储在所述服务端的数据集；

[0159] 发送单元100，用于将所述处理后的密文和所述保序密文数据范围发送给所述客户端，以使所述客户端将采用同态解密对所述处理后的密文进行解密所获得的解密后的数字，与所述保序密文数据范围中的数字逐条比对，并获得符合所述待查数字对应数据范围的数据序号。

[0160] 在本发明实施例中，所述处理单元80包括：

[0161] 随机生成用于保序加密的两个数字；

[0162] 接收所述客户端发送的用于同态加密的公钥，并通过所述公钥对所述两个数字进行加密，分别获得第一密文和第二密文；

[0163] 采用所述第一密文和所述第二密文对所述加密后的密文进行同态乘法运算和同态加法运算，获得处理后的密文。

[0164] 基于同一发明构思，如图11所示，本发明实施例还提供了一种隐私信息检索系统，包括：

[0165] 客户端110以及与所述客户端110连接的服务端120；其中：所述客户端110被配置

为：

[0166] 获取用户输入的待查数字；

[0167] 采用同态加密对所述待查数字进行加密，并将加密后的密文发送给所述服务端120；

[0168] 接收所述服务端120采用同态加密和保序加密对所述加密后的密文进行处理后的密文，以及所述服务端120对全量明文数据集中的多条数据范围逐条进行保序加密变换后的保序密文数据范围，其中，所述全量明文数据集为预先存储在所述服务端120的数据集；

[0169] 采用同态解密对所述处理后的密文进行解密，获得解密后的数字；

[0170] 将所述解密后的数字与所述保序密文数据范围中的数字逐条比对，获得符合所述待查数字对应数据范围的数据序号；

[0171] 根据所述数据序号执行不经意传输协议，获取所述数据序号对应的检索结果。

[0172] 基于同一发明构思，本发明实施例还提供了一种隐私信息检索装置，所述检索装置包括处理器，所述处理器用于执行存储器中存储的计算机程序时实现如前面所述的隐私信息检索方法的步骤。

[0173] 基于同一发明构思，本发明实施例还提供了一种可读存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时实现如前面所述的隐私信息检索方法的步骤。

[0174] 本发明实施例提供了一种隐私信息检索方法、装置及系统，其中，首先，获取用户输入的待查数字，然后，采用同态加密对待查数字进行加密，并将加密后的密文发送给服务端；该服务端采用同态加密和保序加密对该加密后的密文进行处理，并对预先存储在服务端的全量明文数据集中的多条数据范围逐条进行保序加密变换，获得保序密文数据范围，然后，将处理后的密文和保序密文数据范围发送给客户端；然后，客户端采取同态解密对该处理后的密文进行解密，获得解密后的数字；然后，将该解密后的数字与保序密文数据范围中的数字逐条比对，获得符合待查数字对应数据范围的数据序号；然后，根据该数据序号执行不经意传输协议，获得该数据序号对应的检索结果。

[0175] 如此一来，通过同态加密和保序加密，可以实现对服务端数据的保护，以及客户端对服务端数据的密文范围检索。从而保证了服务端范围数据以保序密文的形式呈现给用户，这样的话，用户在不知道保序密钥的情况下，无法反解密服务端的原始数据范围明文；同时，保序密文保证了客户端可以对服务端数据进行依次保序密文范围检索；从而实现了支持数据范围的隐私信息检索，保证了用户的信息安全。

[0176] 本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0177] 本申请是参照根据本申请的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流

程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0178] 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。

[0179] 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。

[0180] 显然，本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的精神和范围。这样，倘若本申请的这些修改和变型属于本申请权利要求及其等同技术的范围之内，则本申请也意图包含这些改动和变型在内。

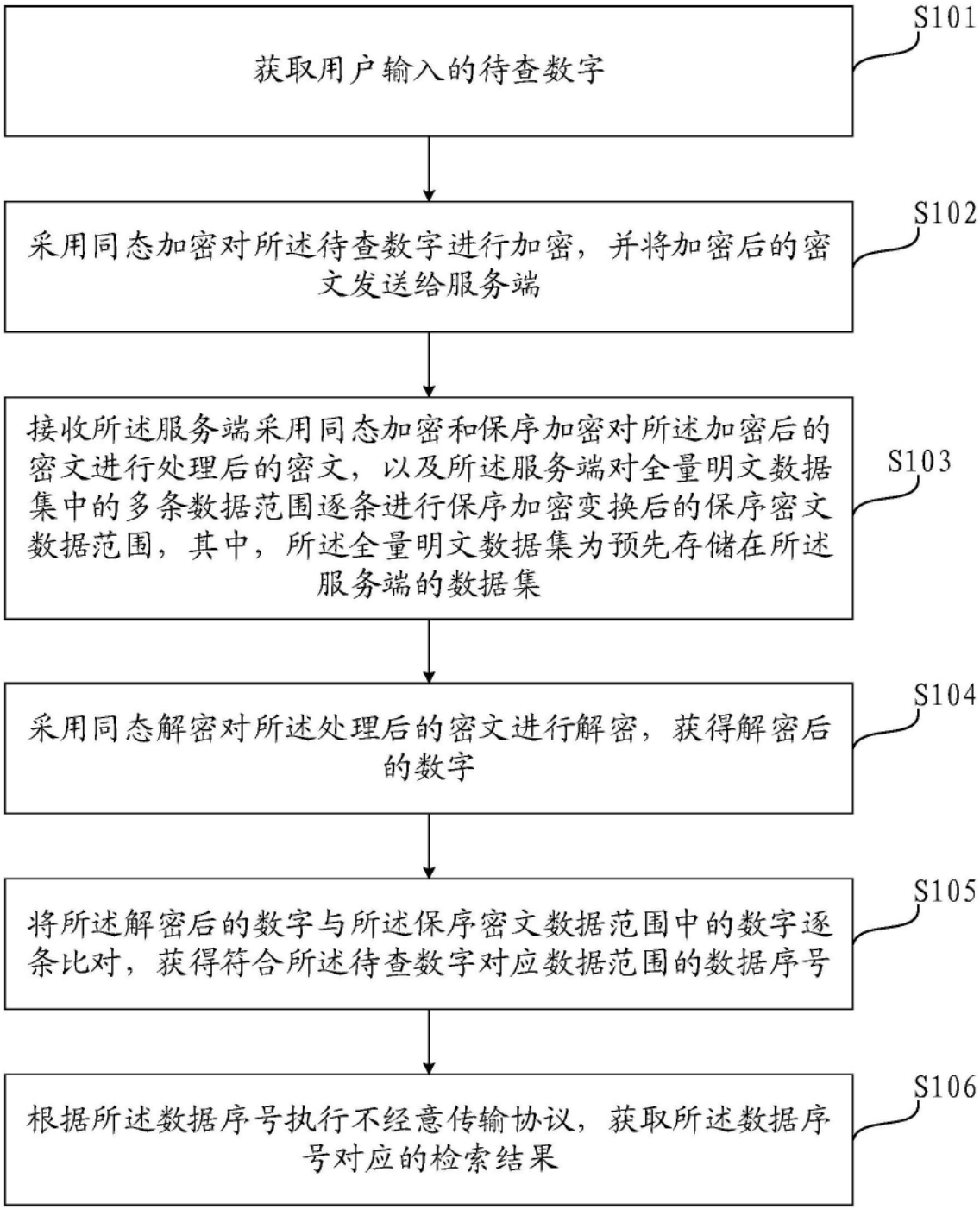

S101
获取用户输入的待查数字
S102
采用同态加密对所述待查数字进行加密，并将加密后的密文发送给服务端
S103
接收所述服务端采用同态加密和保序加密对所述加密后的密文进行处理后的密文，以及所述服务端对全量明文数据集中的多条数据范围逐条进行保序加密变换后的保序密文数据范围，其中，所述全量明文数据集为预先存储在所述服务端的数据集
S104
采用同态解密对所述处理后的密文进行解密，获得解密后的数字
S105
将所述解密后的数字与所述保序密文数据范围中的数字逐条比对，获得符合所述待查数字对应数据范围的数据序号
S106
根据所述数据序号执行不经意传输协议，获取所述数据序号对应的检索结果

图1

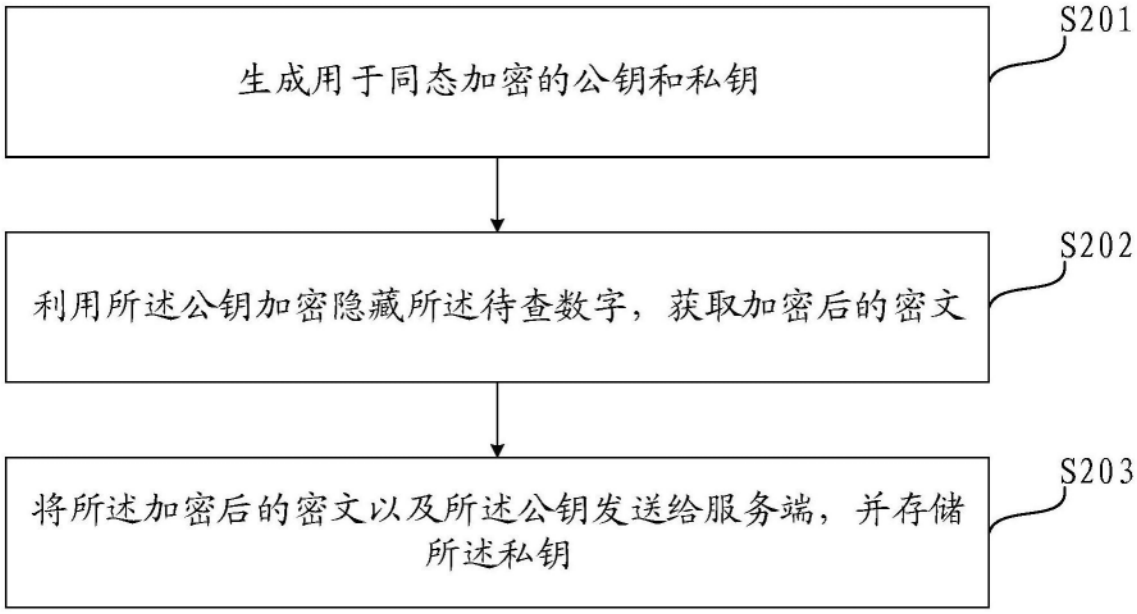

生成用于同态加密的公钥和私钥
S201
利用所述公钥加密隐藏所述待查数字，获取加密后的密文
S202
将所述加密后的密文以及所述公钥发送给服务端，并存储所述私钥
S203

图2

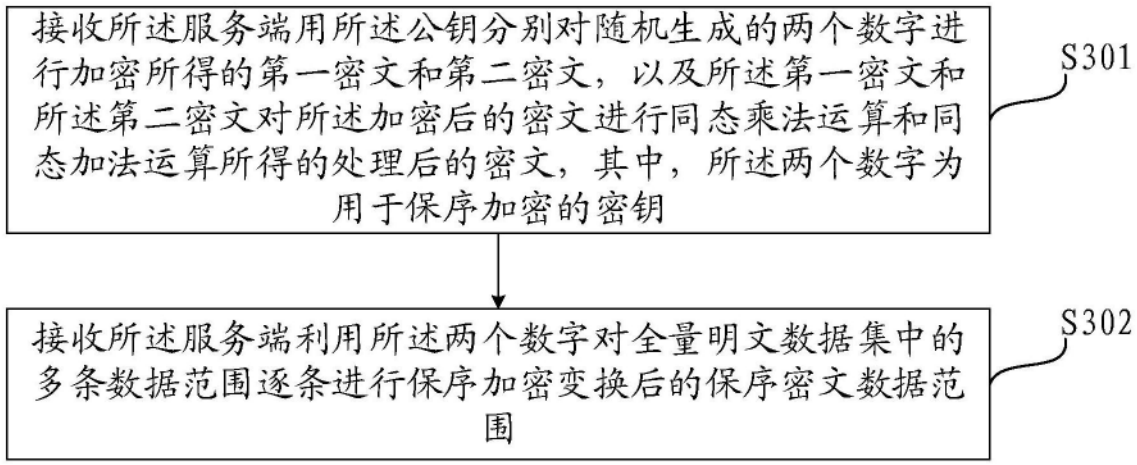

接收所述服务端用所述公钥分别对随机生成的两个数字进行加密所得的第一密文和第二密文，以及所述第一密文和所述第二密文对所述加密后的密文进行同态乘法运算和同态加法运算所得的处理后的密文，其中，所述两个数字为用于保序加密的密钥
S301
接收所述服务端利用所述两个数字对全量明文数据集中的多条数据范围逐条进行保序加密变换后的保序密文数据范围
S302

图3

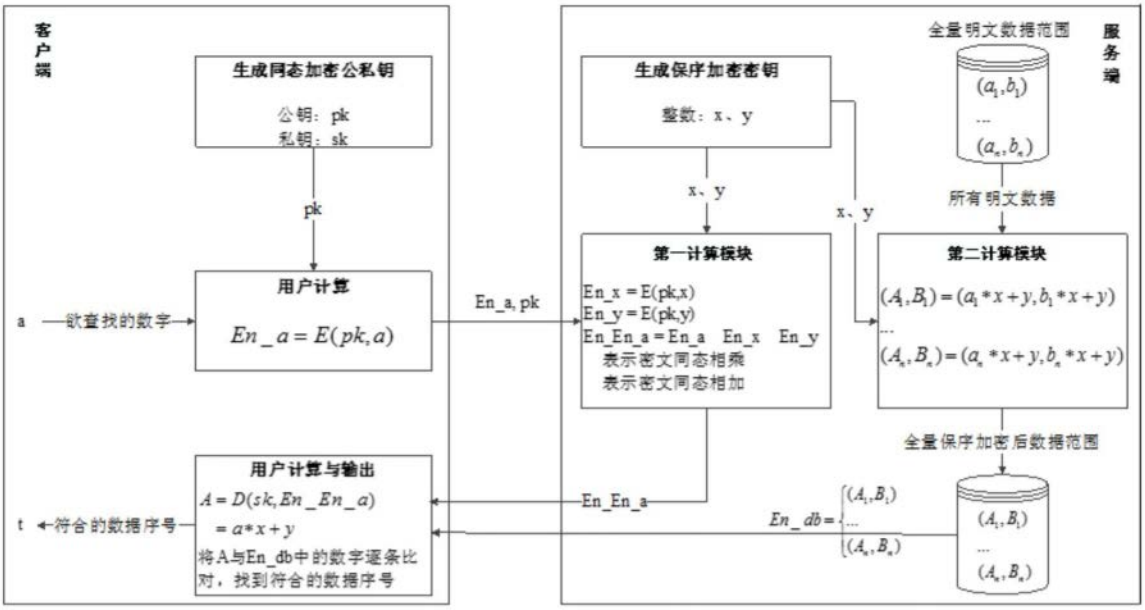

客户端
生成同态加密公私钥
公钥：pk
私钥：sk
pk
用户计算
$En\_a = E(pk,a)$
a
欲查找的数字
En_a, pk
用户计算与输出
$A = D(sk, En\_En\_a)$
$= a*x+y$
将A与En_db中的数字逐条比对，找到符合的数据序号
t
符合的数据序号
En_En_a
服务端
生成保序加密密钥
整数：x、y
x、y
x、y
全量明文数据范围
(a_1,b_1)
...
(a_n,b_n)
所有明文数据
第一计算模块
En_x = E(pk,x)
En_y = E(pk,y)
En_En_a = En_a En_x En_y
表示密文同态相乘
表示密文同态相加
第二计算模块
$(A_1,B_1) = (a_1*x+y, b_1*x+y)$
...
$(A_n,B_n) = (a_n*x+y, b_n*x+y)$
全量保序加密后数据范围
$En\_db = \{(A_1,B_1), ..., (A_n,B_n)\}$
(A_1,B_1)
...
(A_n,B_n)

图4

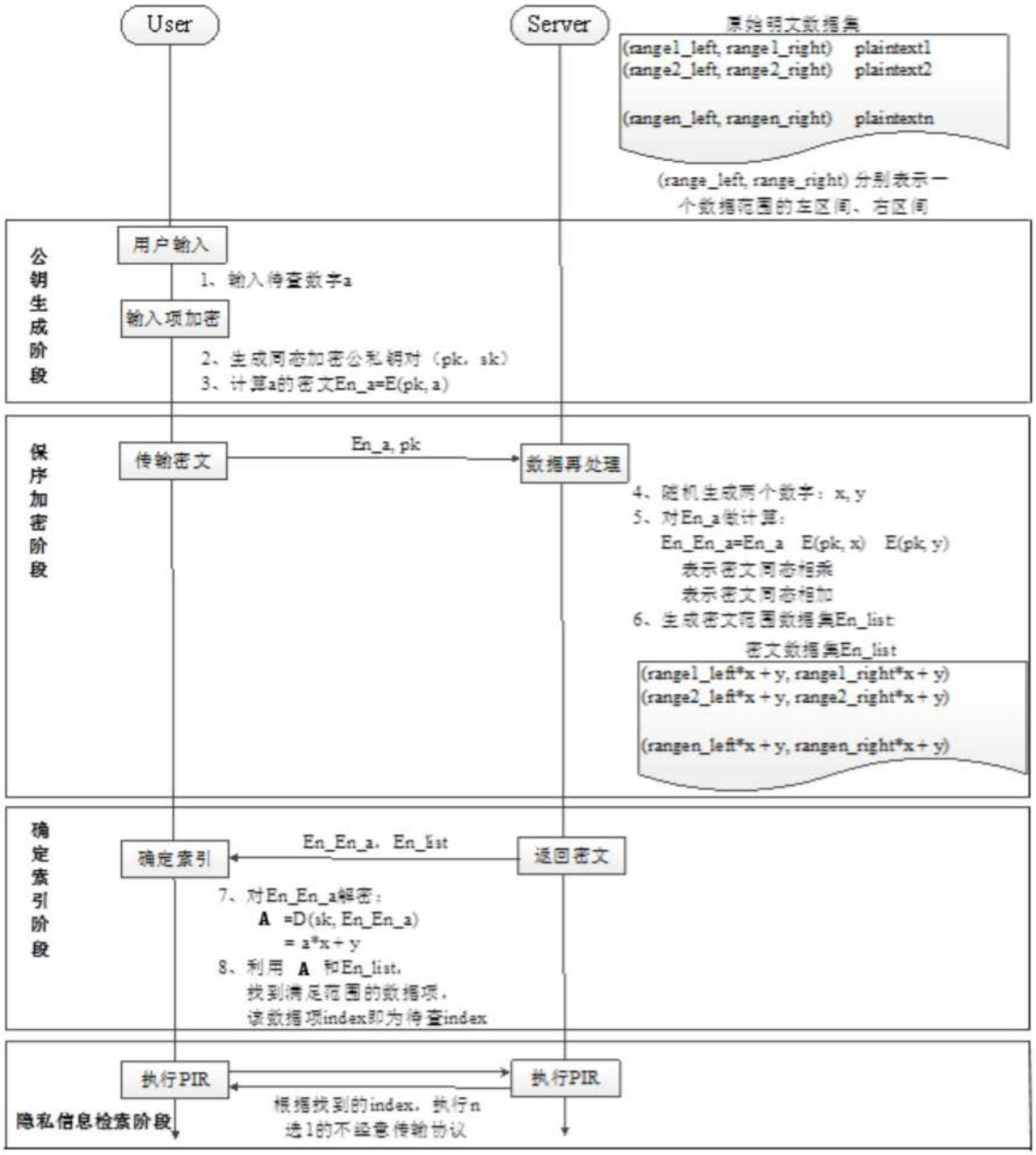

User
Server
原始明文数据集
(range1_left, range1_right) plaintext1
(range2_left, range2_right) plaintext2
(rangen_left, rangen_right) plaintextn
(range_left, range_right) 分别表示一个数据范围的左区间、右区间
公钥生成阶段
用户输入
1、输入待查数字a
输入项加密
2、生成同态加密公私钥对（pk，sk）
3、计算a的密文En_a=E(pk, a)
保序加密阶段
传输密文
En_a, pk
数据再处理
4、随机生成两个数字：x, y
5、对En_a做计算：
En_En_a=En_a E(pk, x) E(pk, y)
表示密文同态相乘
表示密文同态相加
6、生成密文范围数据集En_list
密文数据集En_list
(range1_left*x + y, range1_right*x + y)
(range2_left*x + y, range2_right*x + y)
(rangen_left*x + y, rangen_right*x + y)
确定索引阶段
确定索引
En_En_a，En_list
返回密文
7、对En_En_a解密：
A =D(sk, En_En_a)
= a*x + y
8、利用 A 和En_list，
找到满足范围的数据项，
该数据项index即为待查index
执行PIR
执行PIR
根据找到的index，执行n选1的不经意传输协议
隐私信息检索阶段

图5

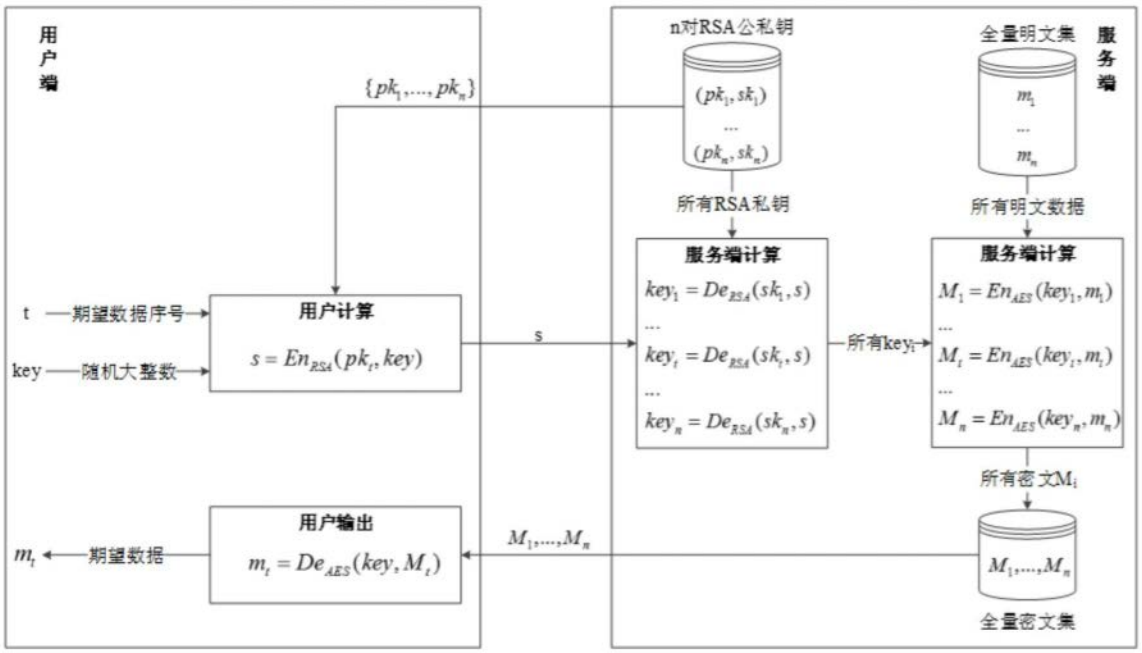

用户端
服务端
n对RSA公私钥
全量明文集
$\{pk_1,\ldots,pk_n\}$
(pk_1,sk_1)
...
(pk_n,sk_n)
m_1
...
m_n
所有RSA私钥
所有明文数据
t
期望数据序号
key
随机大整数
用户计算
$s=En_{RSA}(pk_t,key)$
s
服务端计算
$key_1=De_{RSA}(sk_1,s)$
...
$key_t=De_{RSA}(sk_t,s)$
...
$key_n=De_{RSA}(sk_n,s)$
所有key
服务端计算
$M_1=En_{AES}(key_1,m_1)$
...
$M_t=En_{AES}(key_t,m_t)$
...
$M_n=En_{AES}(key_n,m_n)$
所有密文M_i
m_t
期望数据
用户输出
$m_t=De_{AES}(key,M_t)$
$M_1,\ldots,M_n$
$M_1,\ldots,M_n$
全量密文集

图6

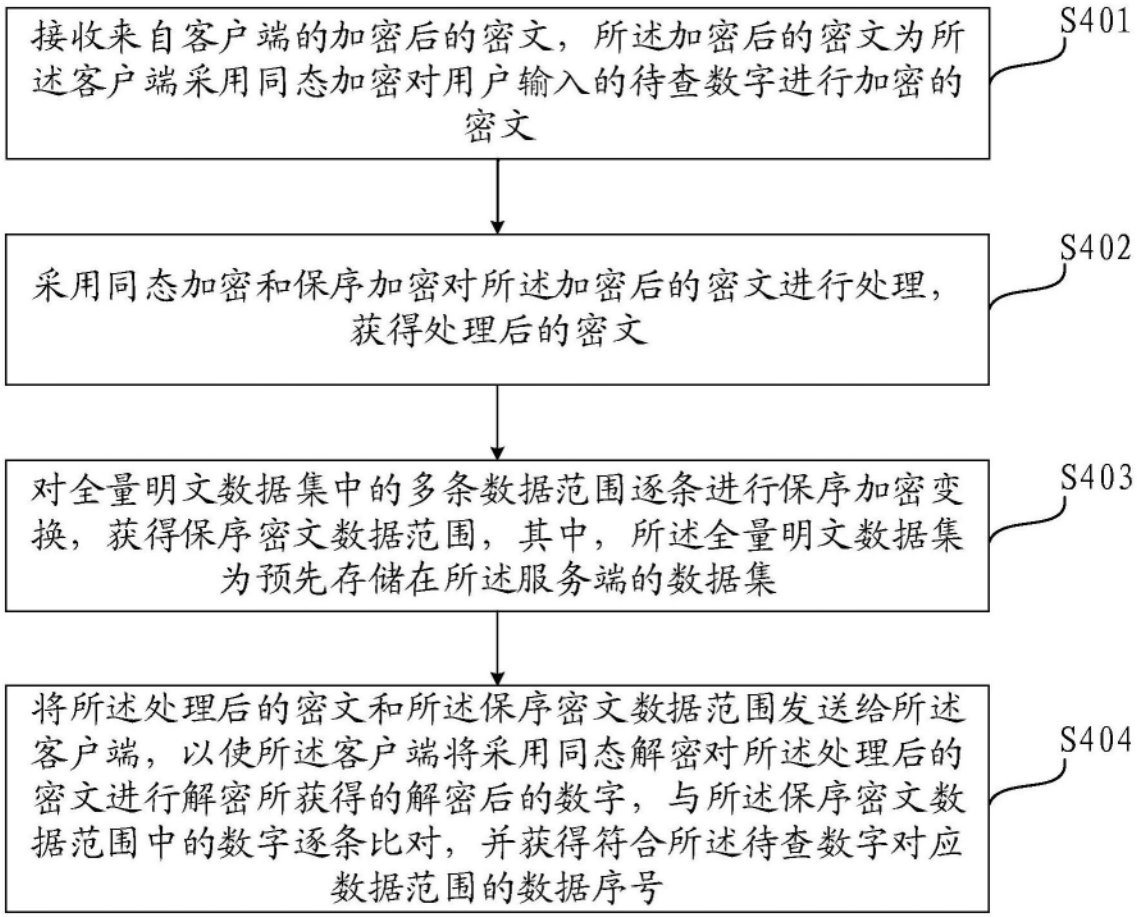

接收来自客户端的加密后的密文，所述加密后的密文为所述客户端采用同态加密对用户输入的待查数字进行加密的密文
S401
采用同态加密和保序加密对所述加密后的密文进行处理，获得处理后的密文
S402
对全量明文数据集中的多条数据范围逐条进行保序加密变换，获得保序密文数据范围，其中，所述全量明文数据集为预先存储在所述服务端的数据集
S403
将所述处理后的密文和所述保序密文数据范围发送给所述客户端，以使所述客户端将采用同态解密对所述处理后的密文进行解密所获得的解密后的数字，与所述保序密文数据范围中的数字逐条比对，并获得符合所述待查数字对应数据范围的数据序号
S404

图7

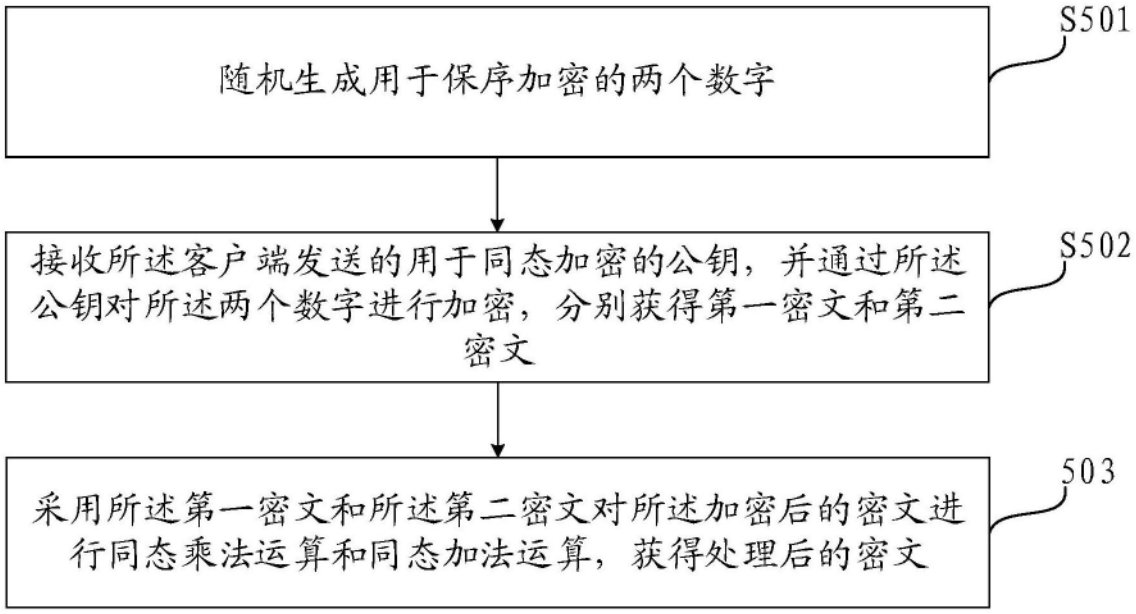

随机生成用于保序加密的两个数字
S501
接收所述客户端发送的用于同态加密的公钥，并通过所述公钥对所述两个数字进行加密，分别获得第一密文和第二密文
S502
采用所述第一密文和所述第二密文对所述加密后的密文进行同态乘法运算和同态加法运算，获得处理后的密文
503

图8

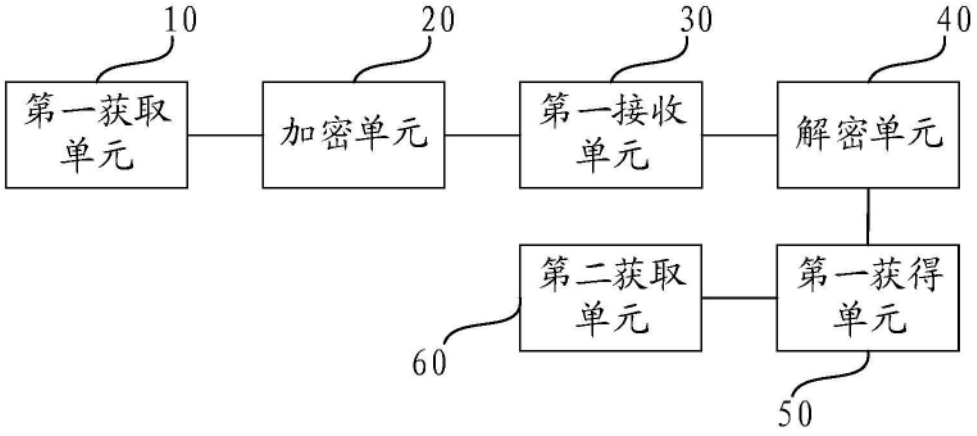

10
第一获取单元
20
加密单元
30
第一接收单元
40
解密单元
第二获取单元
60
第一获得单元
50

图9

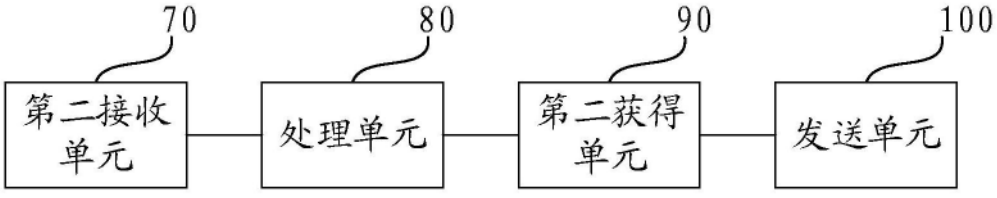

70
第二接收单元
80
处理单元
90
第二获得单元
100
发送单元

图10

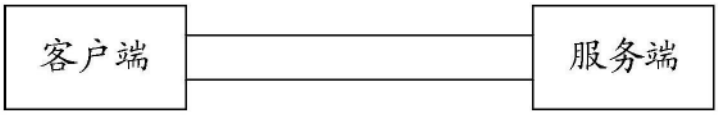


图11