

一种隐私计算系统、方法、装置、设备及介质

相关申请的交叉引用

本申请要求在2022年07月15日提交中国专利局、申请号为202210837745.8、
申请名称为“一种隐私计算系统、方法、装置、设备及介质”的中国专利申
5 请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及数据安全技术领域，尤其涉及一种隐私计算系统、方法、装
置、设备及介质。

10

背景技术

隐私计算 (Privacy compute 或 Privacy computing) 是指在保护数据本身不
对外泄露的前提下实现数据分析计算的技术集合，达到对数据“可用、不可见”
的目的，在充分保护数据和隐私安全的前提下，实现数据价值的转化和释放。

15 随着业界数据保护意识的增强以及隐私监管政策的趋严，隐私计算由于
其“可用、不可见”的特性受到了业界的广泛关注。众多技术厂商纷纷推出其具
有行业特色的隐私计算产品。众多的隐私计算产品在丰富了市场选择的同时，
也带来了新的挑战。例如不同技术厂商推出的隐私计算产品通常是基于不同
系统平台设计实现的，将不同系统平台的隐私计算产品分别保存在不同的隐
20 私计算设备中时，不同系统平台的隐私计算产品之间通常无法完成信息的交互，
将“数据孤岛”变成了“计算孤岛”。另外，即便是同一技术厂商推出的同一
隐私计算产品，将同一隐私计算产品分别保存在不同隐私计算设备中时，同
一隐私计算产品之间通常也无法完成信息的交互，同样将“数据孤岛”变成了
“计算孤岛”。

25 因此，不同隐私计算设备中保存的隐私算法产品之间的互联互通问题已
经成为业界的绝对痛点，如何实现不同隐私计算设备中保存的隐私算法产品

之间的互联互通是目前亟需解决的一个技术问题。

发明内容

本申请提供了一种隐私计算系统、方法、装置、设备及介质，用于实现
5 不同隐私计算设备中保存的隐私算法产品之间的互联互通。

第一方面，本申请提供了一种隐私计算系统，所述系统包括：第一隐私
计算设备和至少一个第二隐私计算设备；

所述第一隐私计算设备与每个第二隐私计算设备之间分别基于管理面互
通进行隐私计算任务的协同，基于数据面互通执行所述隐私计算任务，其中，
10 所述管理面互通与所述数据面互通相互独立；

针对每个第二隐私计算设备，所述第一隐私计算设备与该第二隐私计算
设备进行管理面互通时，所述第一隐私计算设备，用于向所述第二隐私计算
设备发送第一查询请求，所述第一查询请求中携带所述第一隐私计算设备的
第一标识信息以及待查询的子算法的第二标识信息；

15 所述第二隐私计算设备，用于接收所述第一查询请求，并在确定所述第
一标识信息位于保存的合规设备的标识信息中时，将保存的所述第二标识信
息的子算法包含的组件信息发送给所述第一隐私计算设备；

所述第一隐私计算设备，还用于接收所述第二标识信息的子算法包含的
组件信息，并向所述第二隐私计算设备发送加载所述第二标识信息的子算法
20 包含的组件的加载请求；

所述第二隐私计算设备，还用于接收所述加载请求，加载所述第二标识
信息的子算法包含的组件，并在加载成功后，将加载成功的信息发送给所述
第一隐私计算设备。

第二方面，本申请提供了一种隐私计算方法，所述方法应用于第一隐私
25 计算设备，所述方法包括：

与任一第二隐私计算设备进行管理面互通时，向第二隐私计算设备发送
第一查询请求，所述第一查询请求中携带所述第一隐私计算设备的第一标识

信息以及待查询的子算法的第二标识信息；其中，所述第一隐私计算设备与每个第二隐私计算设备之间分别基于管理面互通进行隐私计算任务的协同，基于数据面互通执行所述隐私计算任务，其中，所述管理面互通与所述数据面互通相互独立；

- 5 若接收到所述第二隐私计算设备发送的所述第二标识信息的子算法包含的组件信息，向所述第二隐私计算设备发送加载所述第二标识信息的子算法包含的组件的加载请求。

第三方面，本申请提供了一种隐私计算方法，所述方法应用于任一第二隐私计算设备，所述方法包括：

- 10 与第一隐私计算设备进行管理面互通时，接收所述第一隐私计算设备发送的第一查询请求，所述第一查询请求中携带所述第一隐私计算设备的第一标识信息以及待查询的子算法的第二标识信息；其中，所述第一隐私计算设备与每个第二隐私计算设备之间分别基于管理面互通进行隐私计算任务的协同，基于数据面互通执行所述隐私计算任务，其中，所述管理面互通与所述数据面互通相互独立；
- 15

在确定所述第一标识信息位于保存的合规设备的标识信息中时，将保存的所述第二标识信息的子算法包含的组件信息发送给所述第一隐私计算设备；

- 若接收到所述第一隐私计算设备发送的加载请求，加载所述第二标识信息的子算法包含的组件，在加载成功后，将加载成功的信息发送给所述第一隐私计算设备。
- 20

第四方面，本申请提供了一种隐私计算装置，所述装置包括：

- 第一发送模块，用于与任一第二隐私计算设备进行管理面互通时，向所述第二隐私计算设备发送第一查询请求，所述第一查询请求中携带所述第一隐私计算设备的第一标识信息以及待查询的子算法的第二标识信息；其中，
- 25 所述第一隐私计算设备与每个第二隐私计算设备之间分别基于管理面互通进行隐私计算任务的协同，基于数据面互通执行所述隐私计算任务，其中，所述管理面互通与所述数据面互通相互独立；

第二发送模块，用于若接收到所述第二隐私计算设备发送的所述第二标识信息的子算法包含的组件信息，向所述第二隐私计算设备发送加载所述第二标识信息的子算法包含的组件的加载请求。

第五方面，本申请提供了另一种隐私计算装置，所述装置包括：

5 第一接收模块，用于与第一隐私计算设备进行管理面互通时，接收所述第一隐私计算设备发送的第一查询请求，所述第一查询请求中携带所述第一隐私计算设备的第一标识信息以及待查询的子算法的第二标识信息；其中，所述第一隐私计算设备与每个第二隐私计算设备之间分别基于管理面互通进行隐私计算任务的协同，基于数据面互通执行所述隐私计算任务，其中，所述管理面互通与所述数据面互通相互独立；
10

第三发送模块，用于在确定所述第一标识信息位于保存的合规设备的标识信息中时，将保存的所述第二标识信息的子算法包含的组件信息发送给所述第一隐私计算设备；

加载模块，用于若接收到所述第一隐私计算设备发送的加载请求，加载
15 所述第二标识信息的子算法包含的组件，在加载成功后，将加载成功的信息发送给所述第一隐私计算设备。

第六方面，本申请提供了一种电子设备，其包括处理器和存储器，其中，所述存储器存储有程序代码，当所述程序代码被所述处理器执行时，使得所述处理器执行上述任一项所述隐私计算方法的步骤。

20 第七方面，本申请提供了一种计算机可读存储介质，其包括程序代码，当所述存储介质在电子设备上运行时，所述程序代码用于使所述电子设备执行上述任一项所述隐私计算方法的步骤。

第八方面，本申请提供了一种计算机程序产品，所述计算机程序产品包括：计算机程序代码，当所述计算机程序代码在计算机上运行时，使得计算机执行如上述任一所述隐私计算方法的步骤。
25

由于本申请针对每个第二隐私计算设备，第一隐私计算设备与该第二隐私计算设备进行管理面互通时，第一隐私计算设备可以向第二隐私计算设备

发送第一查询请求，第一查询请求中携带第一隐私计算设备的第一标识信息以及待查询的子算法的第二标识信息；第二隐私计算设备可以接收第一查询请求，并在确定第一标识信息位于保存的合规设备的标识信息中时，将保存的第二标识信息的子算法包含的组件信息发送给第一隐私计算设备；第一隐私计算设备接收第二标识信息的子算法包含的组件信息，并向第二隐私计算设备发送加载第二标识信息的子算法包含的组件的加载请求；第二隐私计算设备可以接收加载请求，加载第二标识信息的子算法包含的组件，并在加载成功后，将加载成功的信息发送给第一隐私计算设备，由于本申请第一隐私计算设备与每个第二隐私计算设备之间可以分别基于管理面互通进行隐私计算任务的协同，基于数据面互通执行隐私计算任务，管理面互通与数据面互通相互独立，基于此，可以实现不同隐私计算设备中保存的隐私算法产品之间可以互联互通的目的。

附图说明

为了更清楚地说明本申请实施例或相关技术中的实施方式，下面将对实施例或相关技术描述中所需要使用的附图作一简单地介绍，显而易见地，下面描述中的附图是本申请的一些实施例，对于本领域普通技术人员来讲，还可以根据这些附图获得其他的附图。

- 图 1 示出了一些实施例提供的一种隐私计算系统结构示意图；
- 图 2 示出了一些实施例提供的一种隐私算法互联互通过程示意图；
- 图 3 示出了一些实施例提供的另一种隐私算法互联互通过程示意图；
- 图 4 示出了一些实施例提供的一种隐私计算方法流程示意图；
- 图 5 示出了一些实施例提供的一种隐私计算装置示意图；
- 图 6 示出了一些实施例提供的另一种隐私计算方法流程示意图；
- 图 7 示出了一些实施例提供的另一种隐私计算装置示意图；
- 图 8 示出了一些实施例提供的一种电子设备结构示意图。

具体实施方式

为了实现不同隐私计算产品之间的互联互通，本申请提供了一种隐私计算系统、方法、装置、设备及介质。

5 为使本申请的目的和实施方式更加清楚，下面将结合本申请示例性实施例中的附图，对本申请示例性实施方式进行清楚、完整地描述，显然，描述的示例性实施例仅是本申请一部分实施例，而不是全部的实施例。

本申请中说明书和权利要求书及上述附图中的术语“第一”、“第二”、“第三”等是用于区别类似或同类的对象或实体，而不必然意味着限定特定的顺序或先后次序，除非另外注明。应该理解这样使用的用语在适当情况下可以互
10 换。

术语“包括”和“具有”以及他们的任何变形，意图在于覆盖但不排他的包含，例如，包含了一系列组件的产品或设备不必限于清楚地列出的所有组件，而是可包括没有清楚地列出的或对于这些产品或设备固有的其它组件。

最后应说明的是：以上各实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述各实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分或者全部技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案
15 的本质脱离本申请各实施例技术方案的范围。

实施例 1:

20 图 1 示出了一些实施例提供的一种隐私计算系统结构示意图，该系统包括：第一隐私计算设备 11 和至少一个第二隐私计算设备 12；其中，所述第一隐私计算设备 11 与每个第二隐私计算设备 12 之间分别基于管理面互通进行隐私计算任务的协同，基于数据面互通执行所述隐私计算任务，其中，所述管理面互通与所述数据面互通相互独立；

25 针对每个第二隐私计算设备 12，所述第一隐私计算设备 11 与该第二隐私计算设备 12 进行管理面互通时，所述第一隐私计算设备 11，用于向所述第二隐私计算设备 12 发送第一查询请求，所述第一查询请求中携带所述第一隐私

计算设备 11 的第一标识信息以及待查询的隐私算法的第二标识信息;

所述第二隐私计算设备 12, 用于接收所述第一查询请求, 并在确定所述第一标识信息位于保存的合规设备的标识信息中时, 将保存的所述第二标识信息的子算法包含的组件信息发送给所述第一隐私计算设备 11;

5 所述第一隐私计算设备 11, 还用于接收所述第二标识信息的子算法包含的组件信息, 并向所述第二隐私计算设备 12 发送加载所述第二标识信息的子算法包含的组件的加载请求;

所述第二隐私计算设备 12, 还用于接收所述加载请求, 加载所述第二标识信息的子算法包含的组件, 并在加载成功后, 将加载成功的信息发送给所述
10 所述第一隐私计算设备 11。

在一种可能的实施方式中, 第一隐私计算设备 11 和第二隐私计算设备 12 可以是 PC、移动终端等设备, 也可以是服务器等设备, 本申请对此不作具体限定。第一隐私计算设备 11 与第二隐私计算设备 12 可以是两台不同的设备。

在一种可能的实施方式中, 请再次参阅图 1, 第一隐私计算设备 11 和
15 第二隐私计算设备 12 中均分别保存有任意隐私算法的子算法, 为方便描述, 将第一隐私计算设备 11 中保存的子算法称为第一子算法, 将第二隐私计算设备 12 中保存的子算法称为第二子算法。在一种可能的实施方式中, 第一子算法和第二子算法可以分别为同一技术厂商推出的同一隐私计算产品中包含的部分子算法, 可选的, 第一子算法和第二子算法也可以分别为不同技术厂商基
20 于不同系统平台推出的不同隐私计算产品等, 可以根据需求灵活设置, 本申请对此不作具体限定。示例性的, 以第一子算法和第二子算法分别为同一技术厂商推出的同一隐私计算产品(隐私算法)中包含的部分子算法为例, 第一隐私计算设备中保存的第一子算法可以为隐私算法中包含 guest (有标签 y 的一方, 数据的应用方) 部分的子算法, 第二隐私计算设备中保存的第二子
25 算法可以为隐私算法中包含 host 部分(没有标签 y 的一方, 数据的提供方)的子算法。

在一种可能的实施方式中, 第二隐私计算设备的数量可以为一个也可以

为多个，本申请对第二隐私计算设备的数量不作具体限定，可以根据需求灵活设置，其中，无论第二隐私计算设备的数量是一个还是多个，针对每个第二隐私计算设备，第一隐私计算设备与该第二隐私计算设备中保存的隐私算法产品之间进行互联互通时的隐私计算过程均可以采用本申请实施例提供的

5 隐私计算过程，在此不再赘述。

在一种可能的实施方式中，第一子算法可以保存在第一隐私计算设备的数据面中，第二子算法可以保存在第二隐私计算设备的数据面中，第一隐私计算设备与每个第二隐私计算设备之间分别基于管理面互通进行隐私计算任务的协同，并可以基于数据面互通执行该隐私计算任务，使得第一隐私计算

10 设备中保存的第一子算法与第二隐私计算设备中保存的第二子算法之间可以互联互通进行联合计算。可选的，隐私计算设备之间的管理面互通与数据面互通可以是相互独立的。示例性的，参阅图 2，图 2 示出了一些实施例提供的一种隐私算法互联互通过程示意图，如图 2 所示，为了实现不同隐私计算设备中保存的隐私算法产品之间的互联互通，在一种可能的实施方式中，第一

15 隐私计算设备与任一第二隐私计算设备在进行管理面互通时，隐私算法开发人员等可以预先线下将第一隐私计算设备 11 的网际互连协议（Internet Protocol, IP）地址、唯一编码（Identity document, ID）等标识信息（为方便描述，后续将第一隐私计算设备 11 的标识信息称为第一标识信息）发送给第二隐私计算设备 12，第二隐私计算设备 12 可以将第一标识信息对应的第一隐

20 私计算设备 11 作为安全的合规设备，将第一标识信息保存在自身的合规设备的标识信息中。同时，隐私算法开发人员等也可以预先线下将第二隐私计算设备 12 的 IP 地址、ID 等标识信息（为方便描述，后续将第二隐私计算设备 12 的标识信息称为第二标识信息）发送给第一隐私计算设备 11，第一隐私计算设备 11 可以将第二标识信息对应的第二隐私计算设备 12 作为安全的合规

25 设备，将第二标识信息保存在自身的合规设备的标识信息中。也就是说，第一隐私计算设备 11 和第二隐私计算设备 12 可以线下交换节点 IP、节点 ID 等标识信息。

在一种可能的实施方式中，为了增加隐私计算的灵活性和准确性，可以将第一子算法和第二子算法等隐私算法解耦为包含场景算法和安全算法。其中，如果隐私算法中不包含安全算法，只包含场景算法的话，可以认为是在没有安全加密保护的情况下对待处理数据进行明文计算；如果隐私算法中包含场景算法以及安全算法的话，可以认为是在安全加密保护的情况下对待处理数据进行隐私计算。隐私算法中包含的场景算法及安全算法均可以根据需求灵活选择，本申请对此不作具体限定。

在一种可能的实施方式中，第一子算法中可以包含第一场景算法和第一安全算法，第二子算法可以包含第二场景算法和第二安全算法。为了保证不同隐私计算设备中保存的隐私算法产品之间的互联互通时的安全性，在一种可能的实施方式中，除了可以预先线下将第一隐私计算设备 11 的第一标识信息发送给第二隐私计算设备 12 之外，还可以预先线下将第一子算法包含的第一安全算法的安全证书发送给第二隐私计算设备 12，第二隐私计算设备 12 可以保存该安全证书及该安全证书携带的第一子算法的令牌（为方便描述，将安全证书携带的令牌称为参考令牌）。同样的，除了可以预先线下将第二隐私计算设备 12 的第二标识信息发送给第一隐私计算设备 11 之外，还可以预先线下将第二子算法包含的第二安全算法的安全证书发送给第一隐私计算设备 11，第一隐私计算设备 11 可以保存该安全证书及该安全证书携带的第二子算法的参考令牌。也就是说，第一隐私计算设备 11 和第二隐私计算设备 12 可以线下交换安全证书等。其中，关于参考令牌的用途在后文进行描述，在此不再赘述。

在一种可能的实施方式中，为了实现不同隐私计算设备中保存的隐私算法产品之间的互联互通，可以将不同隐私算法产品，即不同隐私计算设备中保存的子算法均配置为容器结构的算法，容器结构的算法中可以包含若干个算法组件。可选的，为了实现不同隐私计算设备中保存的隐私算法产品之间的互联互通，可以进行将不同隐私计算产品（子算法）包含的算法组件互通的过程。可选的，算法组件互通的过程可以如下：

第一隐私计算设备 11 可以向第二隐私计算设备 12 发送查询算法组件信息的第一查询请求（为方便描述，将查询算法组件信息的查询请求称为第一查询请求），该第一查询请求中可以携带第一隐私计算设备 11 的第一标识信息以及待查询的子算法的第二标识信息。第二隐私计算设备 12 若接收到该第一查询请求，可以继而判断第一查询请求中携带的第一标识信息是否位于预先保存的合规设备的标识信息中，若第一标识信息位于预先保存的合规设备的标识信息中，可以认为第一标识信息的第一隐私计算设备 11 为安全的合规设备，则可以将保存的第二标识信息的子算法包含的组件信息发送（返回）给第一隐私计算设备 11。

第一隐私计算设备 11 可以接收第二隐私计算设备 12 发送的第二标识信息的子算法（第二子算法）包含的组件信息，并保存。在一种可能的实施方式中，在预运行第一子算法和第二子算法之前，第一隐私计算设备 11 可以向第二隐私计算设备 12 发送加载第二标识信息的子算法（第二子算法）包含的组件的加载请求，第二隐私计算设备 12 接收到该加载请求后，可以加载第二标识信息的子算法（第二子算法）包含的组件，即可以将第二子算法包含的组件同步上线，可选的，第二隐私计算设备 12 将第二标识信息的子算法包含的组件加载成功（算法组件上线完成）后，可以将加载成功的信息发送（返回）给第一隐私计算设备 11，使第一隐私计算设备 11 可以获知第二隐私计算设备 12 中的第二子算法已经加载成功。

由于本申请针对每个第二隐私计算设备 12，第一隐私计算设备 11 与该第二隐私计算设备 12 进行管理面互通时，第一隐私计算设备 11 可以向第二隐私计算设备 12 发送第一查询请求，第一查询请求中携带第一隐私计算设备 11 的第一标识信息以及待查询的子算法的第二标识信息；第二隐私计算设备 12 可以接收第一查询请求，并在确定第一标识信息位于保存的合规设备的标识信息中时，将保存的第二标识信息的子算法包含的组件信息发送给第一隐私计算设备 11；第一隐私计算设备 11 接收第二标识信息的子算法包含的组件信息，并向第二隐私计算设备 12 发送加载第二标识信息的子算法包含的组件的

加载请求；第二隐私计算设备 12 可以接收加载请求，加载第二标识信息的子算法包含的组件，并在加载成功后，将加载成功的信息发送给第一隐私计算设备 11，由于本申请第一隐私计算设备 11 与每个第二隐私计算设备 12 之间可以分别基于管理面互通进行隐私计算任务的协同，基于数据面互通执行隐私计算任务，管理面互通与数据面互通相互独立，基于此，可以实现不同隐私计算设备中保存的隐私算法产品之间可以互联互通的目的。

实施例 2:

为了保证第一子算法和第二子算法互联互通的安全性，在上述实施例的基础上，在本申请实施例中，所述第一隐私计算设备 11，具体用于基于设定的第一应用程序编程接口 API，向所述第二隐私计算设备 12 发送所述第一查询请求；

所述第二隐私计算设备 12，具体用于基于所述第一 API，接收所述第一查询请求；并基于所述第一 API，将保存的所述第二标识信息的子算法包含的组件信息发送给所述第一隐私计算设备 11；

所述第一隐私计算设备 11，具体用于基于所述第一 API，接收所述第二标识信息的子算法包含的组件信息；基于设定的第二 API，向所述第二隐私计算设备 12 发送所述加载请求；

所述第二隐私计算设备 12，具体用于基于所述第二 API，接收所述加载请求，并基于所述第二 API，将所述加载成功的信息发送给所述第一隐私计算设备 11。

在一种可能的实施方式中，第一隐私计算设备 11 在向第二隐私计算设备 12 发送第一查询请求时，可以基于设定的第一应用程序编程接口（Application Programming Interface，API）向第二隐私计算设备 12 发送第一查询请求，其中，为方便描述，将发送第一查询请求的 API 称为第一 API。可选的，第二隐私计算设备 12 也可以基于该第一 API 接收第一查询请求，并可以在确定第一标识信息位于保存的合规设备的标识信息中时，基于该第一 API，将保存的第二标识信息的子算法（第二子算法）包含的组件信息发送给第一隐私计算

设备 11。第一隐私计算设备 11 可以基于该第一 API，接收第二隐私计算设备 12 发送的第二标识信息的子算法（第二子算法）包含的组件信息。

另外，第一隐私计算设备 11 在向第二隐私计算设备 12 发送加载请求时，可以基于设定的第二 API（为方便描述，将发送加载请求的 API 称为第二 API），
5 向第二隐私计算设备 12 发送加载请求。第二隐私计算设备 12 可以基于第二 API 接收第一隐私计算设备 11 发送的加载请求，并可以在加载成功后，基于该第二 API，将加载成功的信息发送给第一隐私计算设备 11。可选的，第一 API 和第二 API 可以为 Representational State Transfer（RESTful）API。

由于本申请可以基于设定的标准 API 发送第一查询请求、子算法包含的
10 组件信息等信息，可以进一步提高子算法之间互联互通的安全性。

实施例 3:

为了提高子算法之间互联互通的安全性，在上述各实施例的基础上，在本申请实施例中，所述第一隐私计算设备 11，还用于向所述第二隐私计算设备 12 发送子算法互通的合作请求，所述合作请求中携带所述第一隐私计算设备 11 的第一标识信息；
15

所述第二隐私计算设备 12，还用于接收所述合作请求，并在确定所述第一标识信息位于保存的合规设备的标识信息中时，向所述第一隐私计算设备 11 发送同意合作的第一确认信息。

在一种可能的实施方式中，请再次参阅图 2，为了提高子算法之间互联互通的安全性，第一隐私计算设备 11 在向第二隐私计算设备 12 发送第一查询请求之前，可以先向第二隐私计算设备 12 发送隐私算法互通（互联互通）的合作请求（合作申请），可选的，该合作请求中可以携带第一隐私计算设备 11 的第一标识信息。第二隐私计算设备 12 接收到该合作请求时，可以判断合作请求中携带的第一标识信息是否位于预先保存的合规设备的标识信息中，如
20 果第二隐私计算设备 12 确定合作请求中携带的第一标识信息位于自身保存的合规设备的标识信息中时，可以认为第一隐私计算设备 11 是安全的合规设备，可以向第一隐私计算设备 11 发送（返回）同意合作的第一确认信息（为方便
25

描述, 将同意合作的确认信息称为第一确认信息)。为方便描述, 后续将第一隐私计算设备 11 发送合作请求, 第二隐私计算设备 12 发送同意合作的第一确认信息的过程称为节点互通。

在一种可能的实施方式中, 为了保证第一子算法和第二子算法互联互通的安全性, 第一隐私计算设备 11 在向第二隐私计算设备 12 发送合作请求时, 可以基于设定的第三 API(为方便描述, 将发送合作请求的 API 称为第三 API) 向第二隐私计算设备 12 发送合作请求。隐私计算设备可以基于第三 API, 接收第一隐私计算设备 11 发送的合作请求, 并可以在确定第一标识信息位于保存的合规设备的标识信息中时, 基于第三 API, 发送第一确认信息。可选的, 第三 API 可以为 RESTful API。

由于本申请可以基于设定的标准 API 发送合作请求、第一确认信息等信息, 可以进一步提高子算法之间互联互通的安全性。

实施例 4:

为了提高子算法之间互联互通的安全性, 在上述各实施例的基础上, 在本申请实施例中, 所述第一隐私计算设备 11, 还用于向所述第二隐私计算设备 12 发送第二查询请求, 所述第二查询请求中携带所述第一隐私计算设备 11 的第一标识信息以及待查询的数据资源的第三标识信息;

所述第二隐私计算设备 12, 还用于接收所述第二查询请求, 并在确定所述第一标识信息位于保存的合规设备的标识信息中时, 将保存的所述第三标识信息的数据资源的信息发送给所述第一隐私计算设备 11。

在一种可能的实施方式中, 可选的, 请再次参阅图 2, 为了不同隐私计算设备中保存的隐私算法产品(子算法)之间的互联互通, 在进行管理面互通时, 可以进行将不同子算法各自对应的数据资源互通的过程。可选的, 数据资源互通的过程可以如下:

第一隐私计算设备 11 可以向第二隐私计算设备 12 发送查询数据资源的第二查询请求(为方便描述, 将查询数据资源的查询请求称为第二查询请求)。其中, 本申请对发送第二查询请求的时机不作具体限定, 可以根据需求灵活

设置，示例性的，第一隐私计算设备 11 可以在向第二隐私计算设备 12 发送合作请求，并接收到第二隐私计算设备 12 发送的同意合作的第一确认信息之后，向第二隐私计算设备 12 发送第二查询请求。在一种可能的实施方式中，第二查询请求中可以携带第一隐私计算设备 11 的第一标识信息以及待查询的数据资源的第三标识信息（为方便描述，将待查询的数据资源的标识信息称为第三标识信息）。

第二隐私计算设备 12 在接收到第二查询请求之后，可以判断第二查询请求中携带的第一标识信息是否位于预先保存的合规设备的标识信息中，如果确定第一标识信息位于自身保存的合规设备的标识信息中时，可以认为第一标识信息对应的第一隐私计算设备 11 为安全的合规设备，可以将保存的第三标识信息的数据资源的信息发送（返回）给第一隐私计算设备 11，第一隐私计算设备 11 可以接收该第三标识信息的数据资源的信息并保存，从而实现将不同子算法各自对应的数据资源互通。

由于本申请可以实现将不同子算法各自对应的数据资源互通，基于此，可以实现不同隐私计算产品互联互通的目的。

另外，本申请对进行数据资源互通和算法组件互通的先后顺序不作具体限定，即可以先进行数据资源互通的步骤，也可以先进行算法组件互通的步骤，可以根据需求灵活选择。

在一种可能的实施方式中，为了保证第一子算法和第二子算法互联互通的安全性，第一隐私计算设备 11 在向第二隐私计算设备 12 发送第二查询请求时，可以基于设定的第四 API（为方便描述，将发送第二查询请求的 API 称为第四 API）向第二隐私计算设备 12 发送第二查询请求。第二隐私计算设备 12 可以基于第四 API，接收第一隐私计算设备 11 发送的第二查询请求，第二隐私计算设备 12 可以在确定第一标识信息位于保存的合规设备的标识信息中时，基于第四 API，将保存的第三标识信息的数据资源的信息发送给第一隐私计算设备 11。可选的，第四 API 可以为 RESTful API。

由于本申请可以基于设定的标准 API 进行数据资源互通的过程，可以进

一步提高子算法之间互联互通的安全性。

实施例 5:

为了提高子算法之间互联互通的安全性，在上述各实施例的基础上，在本申请实施例中，所述第一隐私计算设备 11，还用于向所述第二隐私计算设备 12 发送使用所述第三标识信息的数据资源的授权请求，所述授权请求中携带所述第一隐私计算设备 11 的第一标识信息；

所述第二隐私计算设备 12，还用于接收所述授权请求，并在确定所述第一标识信息位于保存的合规设备的标识信息中时，向所述第一隐私计算设备 11 发送授权使用所述第三标识信息的数据资源的授权通过信息。

10 在一种可能的实施方式中，为了使得第一子算法可以使用第二子算法的数据资源，实现不同子算法之间的互联互通，在进行数据资源互通时，第一隐私计算设备 11 在接收到第二隐私计算设备 12 发送的第三标识信息的数据资源的信息之后，还可以向第二隐私计算设备 12 发送使用第三标识信息的数据资源的授权请求，可选的，授权请求中可以携带第一隐私计算设备 11 的第一标识信息。

第二隐私计算设备 12 接收到授权请求后，可以判断授权请求中携带的第一标识信息是否位于预先保存的合规设备的标识信息中，如果确定第一标识信息位于自身保存的合规设备的标识信息中时，可以认为第一标识信息对应的第一隐私计算设备 11 为安全的合规设备，可以向第一隐私计算设备 11 发送（返回）授权使用第三标识信息的数据资源的授权通过信息。第一隐私计算设备 11 接收到授权通过信息后，可以使用第三标识信息的数据资源进行相关计算。可选的，第三标识信息的数据资源可以为元数据等。

25 由于本申请第一隐私计算设备 11 在接收到第二隐私计算设备 12 发送的授权通过信息后，方可以使用第三标识信息的数据资源，可以使得第一子算法和第二子算法可以互联互通的同时，还可以实现对隐私计算过程中数据流动的精细化管控与数据安全防护。

在一种可能的实施方式中，为了保证第一子算法和第二子算法互联互通

的安全性,第一隐私计算设备 11 在向第二隐私计算设备 12 发送授权请求时,可以基于设定的第五 API(为方便描述,将发送授权请求的 API 称为第五 API)向第二隐私计算设备 12 发送授权请求。第二隐私计算设备 12 可以基于第五 API,接收授权请求,并在确定第一标识信息位于保存的合规设备的标识信息中时,基于第五 API,向第一隐私计算设备 11 发送授权通过信息。可选的,第五 API 可以为 RESTful API。

由于本申请可以基于设定的标准 API 发送授权请求、授权通过信息等信
息,可以进一步提高子算法之间互联互通的安全性。

实施例 6:

10 为了提高子算法之间互联互通的安全性,在上述各实施例的基础上,在本申请实施例中,所述第一隐私计算设备 11,还用于向所述第二隐私计算设备 12 发送项目运行准备请求,所述项目运行准备请求中携带所述第一隐私计算设备 11 的第一标识信息、待运行项目所需的子算法的第二标识信息以及待运行项目所需的目标数据资源的第三标识信息;

15 所述第二隐私计算设备 12,还用于接收所述项目运行准备请求,并在确定所述第一标识信息位于保存的合规设备的标识信息中时,并在确定保存有所述第三标识信息的目标数据资源,以及所述第二标识信息的子算法包含的组件加载完成时,向所述第一隐私计算设备 11 发送准确就绪的第二确认信息。

在一种可能的实施方式中,在准备运行第一子算法及第二子算法之前,
20 第一隐私计算设备 11 还可以向第二隐私计算设备 12 发送项目运行准备请求,为了使第二隐私计算设备 12 获知需要为待运行的项目准备哪个或哪些子算法以及数据资源,该项目运行准备请求中除了可以携带第一隐私计算设备 11 的第一标识信息之外,还可以携带待运行项目所需的子算法的第二标识信息以及待运行项目所需的目标数据资源的第三标识信息。其中,项目运行准备请
25 求中携带的子算法和目标数据资源等可以根据需求灵活设置,本申请对此不作具体限定。

第二隐私计算设备 12 接收到项目运行准备请求之后,可以判断项目运行

准备请求中携带的第一标识信息是否位于预先保存的合规设备的标识信息中，如果确定第一标识信息位于自身保存的合规设备的标识信息中时，可以认为第一标识信息对应的第一隐私计算设备 11 为安全的合规设备，可以核查一下自身当前是否保存第三标识信息的目标数据资源，以及第二标识信息的子算法包含的组件是否加载完成。第二隐私计算设备 12 可以在确定保存有第三标识信息的目标数据资源，以及第二标识信息的子算法包含的组件加载完成时，向第一隐私计算设备 11 发送准确就绪的确认信息（为方便描述，称为第二确认信息）。为方便描述，将第一隐私计算设备 11 向第二隐私计算设备 12 发送项目运行准备请求，第二隐私计算设备 12 向第一隐私计算设备 11 发送准备就绪的第二确认信息的过程称为项目与任务流程互通。

由于本申请在项目运行之前，第一隐私计算设备 11 可以向第二隐私计算设备 12 发送项目运行准备请求，使得第二隐私计算设备 12 核实当前是否保存有运行该项目所需的子算法及数据资源，从而可以确保子算法之间互联互通项目的顺利运行。

在一种可能的实施方式中，为了保证第一子算法和第二子算法互联互通的安全性，第一隐私计算设备 11 可以基于设定的第六 API（为方便描述，将发送项目运行准备请求的 API 称为第六 API），向第二隐私计算设备 12 发送项目运行准备请求。第二隐私计算设备 12 可以基于第六 API，接收项目运行准备请求，并可以在确定第一标识信息位于保存的合规设备的标识信息中时，并在确定保存有第三标识信息的目标数据资源，以及第二标识信息的子算法包含的组件加载完成时，基于第六 API，向第一隐私计算设备 11 发送第二确认信息。可选的，第六 API 可以为 RESTful API。

在一种可能的实施方式中，在项目与任务流程互通环节中，第二隐私计算设备 12 确定保存有第三标识信息的目标数据资源，以及第二标识信息的子算法包含的组件加载完成时，可以向第一隐私计算设备 11 发送准确就绪的第二确认信息，可选的，第一隐私计算设备 11 可以接收该第二确认信息，并可以在接收到第二确认信息之后，可以进行与第二隐私计算设备 12 进行数据面

互通的过程。在一种可能的实施方式中，第一隐私计算设备 11 与任一第二隐私计算设备 12 进行数据面互通时，第一隐私计算设备 11 可以向第二隐私计算设备 12 发送启动计算任务的启动请求。第二隐私计算设备 12 可以接收该启动请求，并可以在接收到启动请求之后，按照隐私算法协议运行第二子算法，可选的，第二隐私计算设备 12 可以基于第三标识信息的目标数据资源，运行保存在其数据面中的第二标识信息的子算法，即运行第二子算法。可以理解的，第一隐私计算设备 11 在向第二隐私计算设备 12 发送启动请求，使得第二隐私计算设备 12 运行第二子算法时，第一隐私计算设备 11 也可以运行保存在其数据面中的第一子算法，即第一子算法和第二子算法可以同时运行，以进行互联互通的计算过程。另外，在计算任务执行完毕后，第一隐私计算设备 11 和第二隐私计算设备 12 可以分别获取相应的算法执行报告。

如果将上述实施例提供的节点互通、数据资源互通、算法组件互通、项目与任务流程互通等称为管理面的互通（管理面互通），可以将第一子算法和第二子算法开始启动运行、进行互联互通的计算过程称为数据面的互通（数据面互通）。例如，在管理面的互通均完成后，第一子算法和第二子算法可以同时运行，进行互联互通的计算过程（数据面互通）时，假设第二子算法所在的第二隐私计算设备 12 向第一子算法所在的第一隐私计算设备 11 发送计算数据时，可以同时发送需基于第一子算法对该计算数据进行处理的处理指令，该处理指令中可以携带第二子算法的令牌（为方便描述，将处理指令中携带的令牌称为目标令牌），第一隐私计算设备 11 接收到处理指令后，第一隐私计算设备 11 的网关等可以判断该处理指令中携带的目标令牌与预先保存的第二子算法的参考令牌是否一致，如果一致，则可以认为第二计算数据为安全的合规设备发送的，可以认为需基于第一隐私计算设备 11 保存的第一子算法对该第二计算数据进行再计算，第一隐私计算设备 11 则可以执行基于第一子算法对该第二计算数据进行再计算的过程。而如果目标令牌与预先保存的第二子算法的参考令牌不一致，则可以认为该第二计算数据不是安全的合规设备发送的，则可以认为无需基于第一子算法对该第二计算数据进行再计

算，从而可以保证不同子算法互联互通时的安全性。

为方便理解，下面通过一个具体实施例对本申请提供的第一子算法和第二子算法互联互通的过程进行举例说明。参阅图 3，图 3 示出了一些实施例提供的另一种子算法互联互通过程示意图，可选的，管理面与数据面之间可以通过策略模块进行任务的协同与数据的控制。在一种可能的实施方式中，第一隐私计算设备 11 和第二隐私计算设备 12 中可以分别包含一个隐私计算框架底座，可以理解的，第一隐私计算设备 11 和第二隐私计算设备 12 的结构以及运行子算法的原理是相同的，为方便描述，以第一隐私计算设备 11 为例进行举例说明。第一隐私计算设备 11 的策略模块可以将管理面中节点（也可称为站点）互通的信息保存在第一隐私计算设备 11 的隐私计算框架底座中的节点管理模块中，还可以将管理面中数据资源互通的信息保存在隐私计算框架底座中的资源管理模块中，还可以将管理面中算法组件互通的信息保存在隐私计算框架底座中的算法管理模块中，还可以将管理面中项目与任务流程互通的信息保存在隐私计算框架底座中的项目管理和流程编排模块中。

第一隐私计算设备 11 可以基于第一子算法的隐私计算引擎实现上述实施例中的节点互通、数据资源互通、算法组件互通、项目与任务流程互通等管理面的互通。在管理面的互通均完成后，第一子算法和第二子算法可以同时运行，进行互联互通的计算过程（数据面互通）时，第一隐私计算设备 11 可以将经过授权的数据输入至第一子算法的算法容器中，第二隐私计算设备 12 可以将经过授权的数据输入至保存的第二子算法的算法容器中。示例性的，若第一隐私计算设备 11 基于第一子算法对待处理数据进行相应计算后得到第一计算数据，且确定该第一计算数据需基于保存在第二隐私计算设备 12 中的第二子算法进行再计算时，第一隐私计算设备 11 可以根据预先保存的各子算法与标准代理接口的对应关系，确定第一子算法对应的代理接口，以及第二子算法对应的代理接口，第一隐私计算设备 11 中的通信模块可以通过第一子算法对应的代理接口，将第一计算数据发送给第二隐私计算设备 12 的代理接口（第二子算法对应的代理接口），第二隐私计算设备 12 中的通信模块可以

基于第二子算法对应的代理接口接收到第一计算数据，并可以在确定第一计算数据需基于第二子算法进行再计算时，第二隐私计算设备 12 可以基于第二子算法对第一计算数据进行相应计算，实现第一子算法和第二子算法之间的互联互通。

- 5 由于本申请可以实现管理面互通和数据面互通之间的低耦合，管理面互通和数据面互通之间可以是相互独立，从而可以简化实现不同隐私计算产品（子算法）之间互联互通时的整体设计，有利于不同隐私计算设备中保存的隐私算法产品之间的互联互通的实现。另外，本申请中可以将子算法配置为容器（Container）结构，从而可以使得本申请提供的子算法互联互通方式具有
- 10 有良好的兼容性和可操作性，能够被目前大多数主流的隐私计算产品所接受。

实施例 7:

基于相同的技术构思，本申请提供了一种隐私计算方法，该方法应用于第一隐私计算设备，图 4 示出了一些实施例提供的一种隐私计算方法流程示意图，如图 4 所示，该方法包括：

- 15 S401：与任一第二隐私计算设备进行管理面互通时，向第二隐私计算设备发送第一查询请求，所述第一查询请求中携带所述第一隐私计算设备的第一标识信息以及待查询的子算法的第二标识信息；其中，所述第一隐私计算设备与每个第二隐私计算设备之间分别基于管理面互通进行隐私计算任务的协同，基于数据面互通执行所述隐私计算任务，其中，所述管理面互通与所
- 20 述数据面互通相互独立。

S402：若接收到所述第二隐私计算设备发送的所述第二标识信息的子算法包含的组件信息，向所述第二隐私计算设备发送加载所述第二标识信息的子算法包含的组件的加载请求。

- 在一种可能的实施方式中，所述向第二隐私计算设备发送第一查询请求
- 25 包括：

 基于设定的第一应用程序编程接口 API，向所述第二隐私计算设备发送所述第一查询请求；

所述向所述第二隐私计算设备发送加载所述第二标识信息的子算法包含的组件的加载请求包括:

基于设定的第二 API, 向所述第二隐私计算设备发送所述加载请求。

5 在一种可能的实施方式中, 所述向第二隐私计算设备发送第一查询请求之前, 所述方法还包括:

向所述第二隐私计算设备发送子算法互通的合作请求, 所述合作请求中携带所述第一隐私计算设备的第一标识信息。

在一种可能的实施方式中, 所述向所述第二隐私计算设备发送子算法互通的合作请求包括:

10 基于设定的第三 API, 向所述第二隐私计算设备发送子算法互通的合作请求。

在一种可能的实施方式中, 所述方法还包括:

15 向所述第二隐私计算设备发送第二查询请求, 所述第二查询请求中携带所述第一隐私计算设备的第一标识信息以及待查询的数据资源的第三标识信息。

在一种可能的实施方式中, 所述向所述第二隐私计算设备发送第二查询请求包括:

基于设定的第四 API, 向所述第二隐私计算设备发送所述第二查询请求。

20 在一种可能的实施方式中, 所述向所述第二隐私计算设备发送第二查询请求之后, 所述方法还包括:

向所述第二隐私计算设备发送使用所述第三标识信息的数据资源的授权请求, 所述授权请求中携带所述第一隐私计算设备的第一标识信息。

在一种可能的实施方式中, 所述向所述第二隐私计算设备发送使用所述第三标识信息的数据资源的授权请求包括:

25 基于设定的第五 API, 向所述第二隐私计算设备发送所述授权请求。

在一种可能的实施方式中, 所述方法还包括:

向所述第二隐私计算设备发送项目运行准备请求, 所述项目运行准备请

求中携带所述第一隐私计算设备的第一标识信息、待运行项目所需的子算法的第二标识信息以及待运行项目所需的目标数据资源的第三标识信息。

在一种可能的实施方式中，所述向所述第二隐私计算设备发送项目运行准备请求包括：

- 5 基于设定的第六 API, 向所述第二隐私计算设备发送所述项目运行准备请求。

在一种可能的实施方式中，所述方法还包括：

- 与任一第二隐私计算设备进行数据面互通时，所述第一隐私计算设备接收所述第二隐私计算设备发送的第二确认信息，向所述第二隐私计算设备发送启动计算任务的启动请求。
- 10

基于相同的技术构思，本申请提供了一种隐私计算装置，应用于第一隐私计算装置，图 5 示出了一些实施例提供的一种隐私计算装置示意图，该装置包括：

- 第一发送模块 501，用于与任一第二隐私计算设备进行管理面互通时，向所述第二隐私计算设备发送第一查询请求，所述第一查询请求中携带所述第一隐私计算设备的第一标识信息以及待查询的子算法的第二标识信息；其中，所述第一隐私计算设备与每个第二隐私计算设备之间分别基于管理面互通进行隐私计算任务的协同，基于数据面互通执行所述隐私计算任务，其中，所述管理面互通与所述数据面互通相互独立；
- 15

- 第二发送模块 502，用于若接收到所述第二隐私计算设备发送的所述第二标识信息的子算法包含的组件信息，向所述第二隐私计算设备发送加载所述第二标识信息的子算法包含的组件的加载请求。
- 20

在一种可能的实施方式中，所述第一发送模块 501，具体用于基于设定的第一应用程序编程接口 API, 向所述第二隐私计算设备发送所述第一查询请求；

- 所述第二发送模块 502，具体用于基于设定的第二 API, 向所述第二隐私计算设备发送所述加载请求。
- 25

在一种可能的实施方式中，所述第一发送模块 501，还用于向所述第二隐

私计算设备发送子算法互通的合作请求，所述合作请求中携带所述第一隐私计算设备的第一标识信息。

在一种可能的实施方式中，所述第一发送模块 501，具体用于基于设定的第三 API，向所述第二隐私计算设备发送子算法互通的合作请求。

5 在一种可能的实施方式中，所述第一发送模块 501，还用于向所述第二隐私计算设备发送第二查询请求，所述第二查询请求中携带所述第一隐私计算设备的第一标识信息以及待查询的数据资源的第三标识信息。

在一种可能的实施方式中，所述第一发送模块 501，具体用于基于设定的第四 API，向所述第二隐私计算设备发送所述第二查询请求。

10 在一种可能的实施方式中，所述第一发送模块 501，还用于向所述第二隐私计算设备发送使用所述第三标识信息的数据资源的授权请求，所述授权请求中携带所述第一隐私计算设备的第一标识信息。

在一种可能的实施方式中，所述第一发送模块 501，具体用于基于设定的第五 API，向所述第二隐私计算设备发送所述授权请求。

15 在一种可能的实施方式中，所述第一发送模块 501，还用于向所述第二隐私计算设备发送项目运行准备请求，所述项目运行准备请求中携带所述第一隐私计算设备的第一标识信息、待运行项目所需的子算法的第二标识信息以及待运行项目所需的目标数据资源的第三标识信息。

20 在一种可能的实施方式中，所述第一发送模块 501，具体用于基于设定的第六 API，向所述第二隐私计算设备发送所述项目运行准备请求。

在一种可能的实施方式中，所述第一发送模块 501，还用于与任一第二隐私计算设备进行数据面互通时，所述第一隐私计算设备接收所述第二隐私计算设备发送的第二确认信息，向所述第二隐私计算设备发送启动计算任务的启动请求。

25 实施例 8:

基于相同的技术构思，本申请提供了一种隐私计算方法，该方法应用于任一第二隐私计算设备，图 6 示出了一些实施例提供的另一种隐私计算方法

流程示意图，如图 6 所示，该方法包括：

5 S601：与第一隐私计算设备进行管理面互通时，接收所述第一隐私计算设备发送的第一查询请求，所述第一查询请求中携带所述第一隐私计算设备的第一标识信息以及待查询的子算法的第二标识信息；其中，所述第一隐私计算设备与每个第二隐私计算设备之间分别基于管理面互通进行隐私计算任务的协同，基于数据面互通执行所述隐私计算任务，其中，所述管理面互通与所述数据面互通相互独立。

10 S602：在确定所述第一标识信息位于保存的合规设备的标识信息中时，将保存的所述第二标识信息的子算法包含的组件信息发送给所述第一隐私计算设备。

S603：若接收到所述第一隐私计算设备发送的加载请求，加载所述第二标识信息的子算法包含的组件，在加载成功后，将加载成功的信息发送给所述第一隐私计算设备。

15 在一种可能的实施方式中，所述接收第一隐私计算设备发送的第一查询请求包括：

基于第一 API，接收所述第一查询请求；

所述将保存的所述第二标识信息的子算法包含的组件信息发送给所述第一隐私计算设备包括：

20 基于所述第一 API，将保存的所述第二标识信息的子算法包含的组件信息发送给所述第一隐私计算设备；

接收所述第一隐私计算设备发送的加载请求包括：

基于第二 API，接收所述加载请求；

所述将加载成功的信息发送给所述第一隐私计算设备包括：

基于所述第二 API，将加载成功的信息发送给所述第一隐私计算设备。

25 在一种可能的实施方式中，所述接收第一隐私计算设备发送的第一查询请求之前，所述方法还包括：

接收所述第一隐私计算设备发送的合作请求，所述合作请求中携带所述

第一隐私计算设备的第一标识信息;

在确定所述第一标识信息位于保存的合规设备的标识信息中时, 向所述第一隐私计算设备发送同意合作的第一确认信息。

5 在一种可能的实施方式中, 所述接收所述第一隐私计算设备发送的合作请求包括:

基于第三 API, 接收所述合作请求;

所述向所述第一隐私计算设备发送同意合作的第一确认信息包括:

基于所述第三 API, 发送所述第一确认信息。

在一种可能的实施方式中, 所述方法还包括:

10 接收所述第一隐私计算设备发送的第二查询请求, 所述第二查询请求中携带所述第一隐私计算设备的第一标识信息以及待查询的数据资源的第三标识信息;

在确定所述第一标识信息位于保存的合规设备的标识信息中时, 将保存的所述第三标识信息的数据资源的信息发送给所述第一隐私计算设备。

15 在一种可能的实施方式中, 所述接收所述第一隐私计算设备发送的第二查询请求包括:

基于第四 API, 接收所述第二查询请求;

所述将保存的所述第三标识信息的数据资源的信息发送给所述第一隐私计算设备包括:

20 基于所述第四 API, 将所述第三标识信息的数据资源的信息发送给所述第一隐私计算设备。

在一种可能的实施方式中, 所述接收所述第一隐私计算设备发送的第二查询请求之后, 所述方法还包括:

25 接收所述第一隐私计算设备发送的授权请求, 所述授权请求中携带所述第一隐私计算设备的第一标识信息;

在确定所述第一标识信息位于保存的合规设备的标识信息中时, 向所述第一隐私计算设备发送授权使用所述第三标识信息的数据资源的授权通过信

息。

在一种可能的实施方式中，所述接收所述第一隐私计算设备发送的授权请求包括：

基于第五 API，接收所述授权请求；

5 所述向所述第一隐私计算设备发送授权使用所述第三标识信息的数据资源的授权通过信息包括：

基于所述第五 API，向所述第一隐私计算设备发送所述授权通过信息。

在一种可能的实施方式中，所述方法还包括：

接收所述第一隐私计算设备发送的项目运行准备请求，所述项目运行准备请求中携带所述第一隐私计算设备的第一标识信息、待运行项目所需的子
10 算法的第二标识信息以及待运行项目所需的目标数据资源的第三标识信息；

在确定所述第一标识信息位于保存的合规设备的标识信息中时，并在确定保存有所述第三标识信息的目标数据资源，以及所述第二标识信息的子算法包含的组件加载完成时，向所述第一隐私计算设备发送准确就绪的第二确
15 认信息。

在一种可能的实施方式中，所述接收所述第一隐私计算设备发送的项目运行准备请求包括：

基于第六 API，接收所述项目运行准备请求；

所述向所述第一隐私计算设备发送准确就绪的第二确认信息包括：

20 基于所述第六 API，所述第一隐私计算设备发送所述第二确认信息。

在一种可能的实施方式中，所述方法还包括：

与所述第一隐私计算设备进行数据面互通时，接收所述第一隐私计算设备发送的启动请求，并基于所述第三标识信息的目标数据资源，运行所述第二标识信息的子算法。

25 基于相同的技术构思，本申请提供了一种隐私计算装置，应用于第二隐私计算装置，图 7 示出了一些实施例提供的另一种隐私计算装置示意图，该装置包括：

第一接收模块 701, 用于与第一隐私计算设备进行管理面互通时, 接收所述第一隐私计算设备发送的第一查询请求, 所述第一查询请求中携带所述第一隐私计算设备的第一标识信息以及待查询的子算法的第二标识信息; 其中, 所述第一隐私计算设备与每个第二隐私计算设备之间分别基于管理面互通进行隐私计算任务的协同, 基于数据面互通执行所述隐私计算任务, 其中, 所述管理面互通与所述数据面互通相互独立;

第三发送模块 702, 用于在确定所述第一标识信息位于保存的合规设备的标识信息中时, 将保存的所述第二标识信息的子算法包含的组件信息发送给所述第一隐私计算设备;

10 加载模块 703, 用于若接收到所述第一隐私计算设备发送的加载请求, 加载所述第二标识信息的子算法包含的组件, 在加载成功后, 将加载成功的信息发送给所述第一隐私计算设备。

在一种可能的实施方式中, 所述第一接收模块 701, 具体用于基于第一 API, 接收所述第一查询请求;

15 所述第三发送模块 702, 具体用于基于所述第一 API, 将保存的所述第二标识信息的子算法包含的组件信息发送给所述第一隐私计算设备;

所述加载模块 703, 具体用于基于第二 API, 接收所述加载请求; 并基于所述第二 API, 将加载成功的信息发送给所述第一隐私计算设备。

在一种可能的实施方式中, 所述第一接收模块 701, 还用于接收所述第一隐私计算设备发送的合作请求, 所述合作请求中携带所述第一隐私计算设备的第一标识信息; 在确定所述第一标识信息位于保存的合规设备的标识信息中时, 向所述第一隐私计算设备发送同意合作的第一确认信息。

在一种可能的实施方式中, 所述第一接收模块 701, 具体用于基于第三 API, 接收所述合作请求;

25 基于所述第三 API, 发送所述第一确认信息。

在一种可能的实施方式中, 所述第一接收模块 701, 还用于接收所述第一隐私计算设备发送的第二查询请求, 所述第二查询请求中携带所述第一隐私

计算设备的第一标识信息以及待查询的数据资源的第三标识信息；在确定所述第一标识信息位于保存的合规设备的标识信息中时，将保存的所述第三标识信息的数据资源的信息发送给所述第一隐私计算设备。

5 在一种可能的实施方式中，所述第一接收模块 701，具体用于基于第四 API，接收所述第二查询请求；

基于所述第四 API，将所述第三标识信息的数据资源的信息发送给所述第一隐私计算设备。

10 在一种可能的实施方式中，所述第一接收模块 701，还用于接收所述第一隐私计算设备发送的授权请求，所述授权请求中携带所述第一隐私计算设备的第一标识信息；在确定所述第一标识信息位于保存的合规设备的标识信息中时，向所述第一隐私计算设备发送授权使用所述第三标识信息的数据资源的授权通过信息。

所述第一接收模块 701，具体用于基于第五 API，接收所述授权请求；

基于所述第五 API，向所述第一隐私计算设备发送所述授权通过信息。

15 在一种可能的实施方式中，所述第一接收模块 701，还用于接收所述第一隐私计算设备发送的项目运行准备请求，所述项目运行准备请求中携带所述第一隐私计算设备的第一标识信息、待运行项目所需的子算法的第二标识信息以及待运行项目所需的目标数据资源的第三标识信息；

20 在确定所述第一标识信息位于保存的合规设备的标识信息中时，并在确定保存有所述第三标识信息的目标数据资源，以及所述第二标识信息的子算法包含的组件加载完成时，向所述第一隐私计算设备发送准确就绪的第二确认信息。

在一种可能的实施方式中，所述第一接收模块 701，具体用于基于第六 API，接收所述项目运行准备请求；

25 基于所述第六 API，所述第一隐私计算设备发送所述第二确认信息。

在一种可能的实施方式中，所述第一接收模块 701，还用于与所述第一隐私计算设备进行数据面互通时，接收所述第一隐私计算设备发送的启动请求，

并基于所述第三标识信息的目标数据资源，运行所述第二标识信息的子算法。

实施例 9:

基于相同的技术构思，本申请还提供了一种电子设备，图 8 示出了一些
实施例提供的一种电子设备结构示意图，如图 8 所示，包括：处理器 81、通
5 信接口 82、存储器 83 和通信总线 84，其中，处理器 81，通信接口 82，存储
器 83 通过通信总线 84 完成相互间的通信；

在一种可能的实施方式中，所述存储器 83 中存储有计算机程序，当所述
程序被所述处理器 81 执行时，使得所述处理器 81 执行如下步骤：

与任一第二隐私计算设备进行管理面互通时，向第二隐私计算设备发送
10 第一查询请求，所述第一查询请求中携带所述第一隐私计算设备的第一标识
信息以及待查询的子算法的第二标识信息；其中，所述第一隐私计算设备与
每个第二隐私计算设备之间分别基于管理面互通进行隐私计算任务的协同，
基于数据面互通执行所述隐私计算任务，其中，所述管理面互通与所述数据
面互通相互独立；

15 若接收到所述第二隐私计算设备发送的所述第二标识信息的子算法包含
的组件信息，向所述第二隐私计算设备发送加载所述第二标识信息的子算法
包含的组件的加载请求。

在一种可能的实施方式中，所述处理器 81，具体用于基于设定的第一应
用程序编程接口 API，向所述第二隐私计算设备发送所述第一查询请求；

20 所述向所述第二隐私计算设备发送加载所述第二标识信息的子算法包含
的组件的加载请求包括：

基于设定的第二 API，向所述第二隐私计算设备发送所述加载请求。

在一种可能的实施方式中，所述处理器 81，还用于所述向第二隐私计算
设备发送第一查询请求之前，向所述第二隐私计算设备发送子算法互通的合
25 作请求，所述合作请求中携带所述第一隐私计算设备的第一标识信息。

在一种可能的实施方式中，所述处理器 81，具体用于基于设定的第三 API，
向所述第二隐私计算设备发送子算法互通的合作请求。

在一种可能的实施方式中,所述处理器 81,还用于向所述第二隐私计算设备发送第二查询请求,所述第二查询请求中携带所述第一隐私计算设备的第一标识信息以及待查询的数据资源的第三标识信息。

在一种可能的实施方式中,所述处理器 81,具体用于基于设定的第四 API,向所述第二隐私计算设备发送所述第二查询请求。

在一种可能的实施方式中,所述处理器 81,还用于所述向所述第二隐私计算设备发送第二查询请求之后,向所述第二隐私计算设备发送使用所述第三标识信息的数据资源的授权请求,所述授权请求中携带所述第一隐私计算设备的第一标识信息。

在一种可能的实施方式中,所述处理器 81,具体用于基于设定的第五 API,向所述第二隐私计算设备发送所述授权请求。

在一种可能的实施方式中,所述处理器 81,还用于向所述第二隐私计算设备发送项目运行准备请求,所述项目运行准备请求中携带所述第一隐私计算设备的第一标识信息、待运行项目所需的子算法的第二标识信息以及待运行项目所需的目标数据资源的第三标识信息。

在一种可能的实施方式中,所述处理器 81,具体用于基于设定的第六 API,向所述第二隐私计算设备发送所述项目运行准备请求。

在一种可能的实施方式中,所述处理器 81,还用于与任一第二隐私计算设备进行数据面互通时,所述第一隐私计算设备接收所述第二隐私计算设备发送的第二确认信息,向所述第二隐私计算设备发送启动计算任务的启动请求。

另外,在一种可能的实施方式中,所述存储器 83 中存储有计算机程序,当所述程序被所述处理器 81 执行时,使得所述处理器 81 执行如下步骤:

与第一隐私计算设备进行管理面互通时,接收所述第一隐私计算设备发送的第一查询请求,所述第一查询请求中携带所述第一隐私计算设备的第一标识信息以及待查询的子算法的第二标识信息;其中,所述第一隐私计算设备与每个第二隐私计算设备之间分别基于管理面互通进行隐私计算任务的协

同，基于数据面互通执行所述隐私计算任务，其中，所述管理面互通与所述数据面互通相互独立；

在确定所述第一标识信息位于保存的合规设备的标识信息中时，将保存的所述第二标识信息的子算法包含的组件信息发送给所述第一隐私计算设备；

- 5 若接收到所述第一隐私计算设备发送的加载请求，加载所述第二标识信息的子算法包含的组件，在加载成功后，将加载成功的信息发送给所述第一隐私计算设备。

在一种可能的实施方式中，所述处理器 81，具体用于基于第一 API，接收所述第一查询请求；

- 10 基于所述第一 API，将保存的所述第二标识信息的子算法包含的组件信息发送给所述第一隐私计算设备；

基于第二 API，接收所述加载请求；

基于所述第二 API，将加载成功的信息发送给所述第一隐私计算设备。

- 15 在一种可能的实施方式中，所述处理器 81，还用于所述接收第一隐私计算设备发送的第一查询请求之前，接收所述第一隐私计算设备发送的合作请求，所述合作请求中携带所述第一隐私计算设备的第一标识信息；

在确定所述第一标识信息位于保存的合规设备的标识信息中时，向所述第一隐私计算设备发送同意合作的第一确认信息。

- 20 在一种可能的实施方式中，所述处理器 81，具体用于基于第三 API，接收所述合作请求；

基于所述第三 API，发送所述第一确认信息。

在一种可能的实施方式中，所述处理器 81，还用于接收所述第一隐私计算设备发送的第二查询请求，所述第二查询请求中携带所述第一隐私计算设备的第一标识信息以及待查询的数据资源的第三标识信息；

- 25 在确定所述第一标识信息位于保存的合规设备的标识信息中时，将保存的所述第三标识信息的数据资源的信息发送给所述第一隐私计算设备。

在一种可能的实施方式中，所述处理器 81，具体用于基于第四 API，接

收所述第二查询请求;

所述将保存的所述第三标识信息的数据资源的信息发送给所述第一隐私计算设备包括:

5 基于所述第四 API, 将所述第三标识信息的数据资源的信息发送给所述第一隐私计算设备。

在一种可能的实施方式中, 所述处理器 81, 还用于所述接收所述第一隐私计算设备发送的第二查询请求之后, 接收所述第一隐私计算设备发送的授权请求, 所述授权请求中携带所述第一隐私计算设备的第一标识信息;

10 在确定所述第一标识信息位于保存的合规设备的标识信息中时, 向所述第一隐私计算设备发送授权使用所述第三标识信息的数据资源的授权通过信息。

在一种可能的实施方式中, 所述处理器 81, 具体用于基于第五 API, 接收所述授权请求;

基于所述第五 API, 向所述第一隐私计算设备发送所述授权通过信息。

15 在一种可能的实施方式中, 所述处理器 81, 还用于接收所述第一隐私计算设备发送的项目运行准备请求, 所述项目运行准备请求中携带所述第一隐私计算设备的第一标识信息、待运行项目所需的子算法的第二标识信息以及待运行项目所需的目标数据资源的第三标识信息;

20 在确定所述第一标识信息位于保存的合规设备的标识信息中时, 并在确定保存有所述第三标识信息的目标数据资源, 以及所述第二标识信息的子算法包含的组件加载完成时, 向所述第一隐私计算设备发送准确就绪的第二确认信息。

在一种可能的实施方式中, 所述处理器 81, 具体用于基于第六 API, 接收所述项目运行准备请求;

25 基于所述第六 API, 所述第一隐私计算设备发送所述第二确认信息。

在一种可能的实施方式中, 所述处理器 81, 还用于与所述第一隐私计算设备进行数据面互通时, 接收所述第一隐私计算设备发送的启动请求, 并基

于所述第三标识信息的目标数据资源，运行所述第二标识信息的子算法。

由于上述电子设备解决问题的原理与隐私计算方法相似，因此上述电子设备的实施可以参见方法的实施，重复之处不再赘述。

上述电子设备提到的通信总线可以是外设部件互连标准（Peripheral Component Interconnect, PCI）总线或扩展工业标准结构（Extended Industry Standard Architecture, EISA）总线等。该通信总线可以分为地址总线、数据总线、控制总线等。为便于表示，图中仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。

通信接口 82 用于上述电子设备与其他设备之间的通信。

存储器可以包括随机存取存储器（Random Access Memory, RAM），也可以包括非易失性存储器（Non-Volatile Memory, NVM），例如至少一个磁盘存储器。可选地，存储器还可以是至少一个位于远离前述处理器的存储装置。

上述处理器可以是通用处理器，包括中央处理器、网络处理器（Network Processor, NP）等；还可以是数字指令处理器（Digital Signal Processing, DSP）、专用集成电路、现场可编程门阵列或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。

基于相同的技术构思，本申请实施例提供了一种计算机可读存储介质，所述计算机可读存储介质内存储有可由电子设备执行的计算机程序，当所述程序在所述电子设备上运行时，使得所述电子设备执行时实现如下步骤：

与任一第二隐私计算设备进行管理面互通时，向第二隐私计算设备发送第一查询请求，所述第一查询请求中携带所述第一隐私计算设备的第一标识信息以及待查询的子算法的第二标识信息；其中，所述第一隐私计算设备与每个第二隐私计算设备之间分别基于管理面互通进行隐私计算任务的协同，基于数据面互通执行所述隐私计算任务，其中，所述管理面互通与所述数据面互通相互独立；

若接收到所述第二隐私计算设备发送的所述第二标识信息的子算法包含的组件信息，向所述第二隐私计算设备发送加载所述第二标识信息的子算法

包含的组件的加载请求。

在一种可能的实施方式中，所述向第二隐私计算设备发送第一查询请求包括：

5 基于设定的第一应用程序编程接口 API，向所述第二隐私计算设备发送所述第一查询请求；

所述向所述第二隐私计算设备发送加载所述第二标识信息的子算法包含的组件的加载请求包括：

基于设定的第二 API，向所述第二隐私计算设备发送所述加载请求。

10 在一种可能的实施方式中，所述向第二隐私计算设备发送第一查询请求之前，所述方法还包括：

向所述第二隐私计算设备发送子算法互通的合作请求，所述合作请求中携带所述第一隐私计算设备的第一标识信息。

在一种可能的实施方式中，所述向所述第二隐私计算设备发送子算法互通的合作请求包括：

15 基于设定的第三 API，向所述第二隐私计算设备发送子算法互通的合作请求。

在一种可能的实施方式中，所述方法还包括：

20 向所述第二隐私计算设备发送第二查询请求，所述第二查询请求中携带所述第一隐私计算设备的第一标识信息以及待查询的数据资源的第三标识信息。

在一种可能的实施方式中，所述向所述第二隐私计算设备发送第二查询请求包括：

基于设定的第四 API，向所述第二隐私计算设备发送所述第二查询请求。

25 在一种可能的实施方式中，所述向所述第二隐私计算设备发送第二查询请求之后，所述方法还包括：

向所述第二隐私计算设备发送使用所述第三标识信息的数据资源的授权请求，所述授权请求中携带所述第一隐私计算设备的第一标识信息。

在一种可能的实施方式中，所述向所述第二隐私计算设备发送使用所述第三标识信息的数据资源的授权请求包括：

基于设定的第五 API，向所述第二隐私计算设备发送所述授权请求。

在一种可能的实施方式中，所述方法还包括：

- 5 向所述第二隐私计算设备发送项目运行准备请求，所述项目运行准备请求中携带所述第一隐私计算设备的第一标识信息、待运行项目所需的子算法的第二标识信息以及待运行项目所需的目标数据资源的第三标识信息。

在一种可能的实施方式中，所述向所述第二隐私计算设备发送项目运行准备请求包括：

- 10 基于设定的第六 API，向所述第二隐私计算设备发送所述项目运行准备请求。

在一种可能的实施方式中，所述方法还包括：

- 与任一第二隐私计算设备进行数据面互通时，所述第一隐私计算设备接收所述第二隐私计算设备发送的第二确认信息，向所述第二隐私计算设备发
15 送启动计算任务的启动请求。

另外，当所述程序在所述电子设备上运行时，还可以使得所述电子设备执行时实现如下步骤：

- 与第一隐私计算设备进行管理面互通时，接收所述第一隐私计算设备发送的第一查询请求，所述第一查询请求中携带所述第一隐私计算设备的第一
20 标识信息以及待查询的子算法的第二标识信息；其中，所述第一隐私计算设备与每个第二隐私计算设备之间分别基于管理面互通进行隐私计算任务的协
同，基于数据面互通执行所述隐私计算任务，其中，所述管理面互通与所述数据面互通相互独立；

- 在确定所述第一标识信息位于保存的合规设备的标识信息中时，将保存
25 的所述第二标识信息的子算法包含的组件信息发送给所述第一隐私计算设备；

若接收到所述第一隐私计算设备发送的加载请求，加载所述第二标识信息的子算法包含的组件，在加载成功后，将加载成功的信息发送给所述第一

隐私计算设备。

在一种可能的实施方式中，所述接收第一隐私计算设备发送的第一查询请求包括：

基于第一 API，接收所述第一查询请求；

5 所述将保存的所述第二标识信息的子算法包含的组件信息发送给所述第一隐私计算设备包括：

基于所述第一 API，将保存的所述第二标识信息的子算法包含的组件信息发送给所述第一隐私计算设备；

接收所述第一隐私计算设备发送的加载请求包括：

10 基于第二 API，接收所述加载请求；

所述将加载成功的信息发送给所述第一隐私计算设备包括：

基于所述第二 API，将加载成功的信息发送给所述第一隐私计算设备。

在一种可能的实施方式中，所述接收第一隐私计算设备发送的第一查询请求之前，所述方法还包括：

15 接收所述第一隐私计算设备发送的合作请求，所述合作请求中携带所述第一隐私计算设备的第一标识信息；

在确定所述第一标识信息位于保存的合规设备的标识信息中时，向所述第一隐私计算设备发送同意合作的第一确认信息。

20 在一种可能的实施方式中，所述接收所述第一隐私计算设备发送的合作请求包括：

基于第三 API，接收所述合作请求；

所述向所述第一隐私计算设备发送同意合作的第一确认信息包括：

基于所述第三 API，发送所述第一确认信息。

在一种可能的实施方式中，所述方法还包括：

25 接收所述第一隐私计算设备发送的第二查询请求，所述第二查询请求中携带所述第一隐私计算设备的第一标识信息以及待查询的数据资源的第三标识信息；

在确定所述第一标识信息位于保存的合规设备的标识信息中时，将保存的所述第三标识信息的数据资源的信息发送给所述第一隐私计算设备。

在一种可能的实施方式中，所述接收所述第一隐私计算设备发送的第二查询请求包括：

- 5 基于第四 API，接收所述第二查询请求；

所述将保存的所述第三标识信息的数据资源的信息发送给所述第一隐私计算设备包括：

基于所述第四 API，将所述第三标识信息的数据资源的信息发送给所述第一隐私计算设备。

- 10 在一种可能的实施方式中，所述接收所述第一隐私计算设备发送的第二查询请求之后，所述方法还包括：

接收所述第一隐私计算设备发送的授权请求，所述授权请求中携带所述第一隐私计算设备的第一标识信息；

- 15 在确定所述第一标识信息位于保存的合规设备的标识信息中时，向所述第一隐私计算设备发送授权使用所述第三标识信息的数据资源的授权通过信息。

在一种可能的实施方式中，所述接收所述第一隐私计算设备发送的授权请求包括：

基于第五 API，接收所述授权请求；

- 20 所述向所述第一隐私计算设备发送授权使用所述第三标识信息的数据资源的授权通过信息包括：

基于所述第五 API，向所述第一隐私计算设备发送所述授权通过信息。

在一种可能的实施方式中，所述方法还包括：

- 25 接收所述第一隐私计算设备发送的项目运行准备请求，所述项目运行准备请求中携带所述第一隐私计算设备的第一标识信息、待运行项目所需的子算法的第二标识信息以及待运行项目所需的目标数据资源的第三标识信息；

在确定所述第一标识信息位于保存的合规设备的标识信息中时，并在确

定保存有所述第三标识信息的目标数据资源，以及所述第二标识信息的子算法包含的组件加载完成时，向所述第一隐私计算设备发送准确就绪的第二确认信息。

5 在一种可能的实施方式中，所述接收所述第一隐私计算设备发送的项目运行准备请求包括：

基于第六 API，接收所述项目运行准备请求；

所述向所述第一隐私计算设备发送准确就绪的第二确认信息包括：

基于所述第六 API，所述第一隐私计算设备发送所述第二确认信息。

在一种可能的实施方式中，所述方法还包括：

10 与所述第一隐私计算设备进行数据面互通时，接收所述第一隐私计算设备发送的启动请求，并基于所述第三标识信息的目标数据资源，运行所述第二标识信息的子算法。

由于上述计算机可读存储介质解决问题的原理与隐私计算方法相似，因此上述计算机可读存储介质的实施可以参见方法的实施，重复之处不再赘述。

15 上述计算机可读存储介质可以是电子设备中的处理器能够存取的任何可用介质或数据存储设备，包括但不限于磁性存储器如软盘、硬盘、磁带、磁盘（MO）等、光学存储器如 CD、DVD、BD、HVD 等、以及半导体存储器如 ROM、EPROM、EEPROM、非易失性存储器（NAND FLASH）、固态硬盘（SSD）等。

20 基于相同的技术构思，在上述各实施例的基础上，本申请提供了一种计算机程序产品，所述计算机程序产品包括：计算机程序代码，当所述计算机程序代码在计算机上运行时，使得计算机执行如上述任一所述隐私计算方法的步骤。

25 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。

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。

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。

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。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。

权 利 要 求

1、一种隐私计算系统，所述系统包括：第一隐私计算设备和至少一个第二隐私计算设备；

5 所述第一隐私计算设备与每个第二隐私计算设备之间分别基于管理面互通进行隐私计算任务的协同，基于数据面互通执行所述隐私计算任务，其中，所述管理面互通与所述数据面互通相互独立；

针对每个第二隐私计算设备，所述第一隐私计算设备与该第二隐私计算设备进行管理面互通时，所述第一隐私计算设备，用于向所述第二隐私计算设备发送第一查询请求，所述第一查询请求中携带所述第一隐私计算设备的第一标识信息以及待查询的子算法的第二标识信息；

所述第二隐私计算设备，用于接收所述第一查询请求，并在确定所述第一标识信息位于保存的合规设备的标识信息中时，将保存的所述第二标识信息的子算法包含的组件信息发送给所述第一隐私计算设备；

15 所述第一隐私计算设备，还用于接收所述第二标识信息的子算法包含的组件信息，并向所述第二隐私计算设备发送加载所述第二标识信息的子算法包含的组件的加载请求；

所述第二隐私计算设备，还用于接收所述加载请求，加载所述第二标识信息的子算法包含的组件，并在加载成功后，将加载成功的信息发送给所述第一隐私计算设备。

20 2、根据权利要求 1 所述的系统，其中，所述第一隐私计算设备，具体用于基于设定的第一应用程序编程接口 API，向所述第二隐私计算设备发送所述第一查询请求；

所述第二隐私计算设备，具体用于基于所述第一 API，接收所述第一查询请求；并基于所述第一 API，将保存的所述第二标识信息的子算法包含的组件信息发送给所述第一隐私计算设备；

所述第一隐私计算设备，具体用于基于所述第一 API，接收所述第二标识

信息的子算法包含的组件信息；基于设定的第二 API，向所述第二隐私计算设备发送所述加载请求；

所述第二隐私计算设备，具体用于基于所述第二 API，接收所述加载请求，并基于所述第二 API，将所述加载成功的信息发送给所述第一隐私计算设备。

- 5 3、根据权利要求 1 所述的系统，所述第一隐私计算设备，还用于向所述第二隐私计算设备发送隐私算法互通的合作请求，所述合作请求中携带所述第一隐私计算设备的第一标识信息；

所述第二隐私计算设备，还用于接收所述合作请求，并在确定所述第一标识信息位于保存的合规设备的标识信息中时，向所述第一隐私计算设备发送同意合作的第一确认信息。

10

4、根据权利要求 3 所述的系统，其中，所述第一隐私计算设备，具体用于基于设定的第三 API，向所述第二隐私计算设备发送隐私算法互通的合作请求；

所述第二隐私计算设备，具体用于基于所述第三 API，接收所述合作请求，并发送所述第一确认信息。

15

5、根据权利要求 1-4 任一所述的系统，所述第一隐私计算设备，还用于向所述第二隐私计算设备发送第二查询请求，所述第二查询请求中携带所述第一隐私计算设备的第一标识信息以及待查询的数据资源的第三标识信息；

所述第二隐私计算设备，还用于接收所述第二查询请求，并在确定所述第一标识信息位于保存的合规设备的标识信息中时，将保存的所述第三标识信息的数据资源的信息发送给所述第一隐私计算设备。

20

6、根据权利要求 5 所述的系统，其中，所述第一隐私计算设备，具体用于基于设定的第四 API，向所述第二隐私计算设备发送所述第二查询请求；

所述第二隐私计算设备，具体用于基于所述第四 API，接收所述第二查询请求，并发送所述第三标识信息的数据资源的信息。

25

7、根据权利要求 5 所述的系统，所述第一隐私计算设备，还用于向所述第二隐私计算设备发送使用所述第三标识信息的数据资源的授权请求，所述

授权请求中携带所述第一隐私计算设备的第一标识信息；

所述第二隐私计算设备，还用于接收所述授权请求，并在确定所述第一标识信息位于保存的合规设备的标识信息中时，向所述第一隐私计算设备发送授权使用所述第三标识信息的数据资源的授权通过信息。

- 5 8、根据权利要求7所述的系统，其中，所述第一隐私计算设备，具体用于基于设定的第五API，向所述第二隐私计算设备发送所述授权请求；

所述第二隐私计算设备，具体用于基于所述第五API，接收所述授权请求，并发送所述授权通过信息。

- 9、根据权利要求5所述的系统，其中，所述第一隐私计算设备，还用于
10 向所述第二隐私计算设备发送项目运行准备请求，所述项目运行准备请求中携带所述第一隐私计算设备的第一标识信息、待运行项目所需的子算法的第二标识信息以及待运行项目所需的目标数据资源的第三标识信息；

所述第二隐私计算设备，还用于接收所述项目运行准备请求，并在确定所述第一标识信息位于保存的合规设备的标识信息中时，并在确定保存有所
15 述第三标识信息的目标数据资源，以及所述第二标识信息的子算法包含的组件加载完成时，向所述第一隐私计算设备发送准确就绪的第二确认信息。

- 10、根据权利要求9所述的系统，针对每个第二隐私计算设备，所述第一隐私计算设备与该第二隐私计算设备进行数据面互通时，所述第一隐私计算设备，还用于接收所述第二确认信息，并向所述第二隐私计算设备发送启动计算任务的启动请求；
20

所述第二隐私计算设备，还用于接收所述启动请求，并基于所述第三标识信息的目标数据资源，运行所述第二标识信息的子算法。

- 11、根据权利要求9所述的系统，其中，所述第一隐私计算设备，具体用于基于设定的第六API，向所述第二隐私计算设备发送所述项目运行准备请求；
25

所述第二隐私计算设备，具体用于基于所述第六API，接收所述项目运行准备请求，并基于所述第六API，向所述第一隐私计算设备发送所述第二确认

信息。

12、根据权利要求 1 所述的系统，其中，所述子算法为容器结构的算法。

13、一种隐私计算方法，所述方法应用于第一隐私计算设备，所述方法包括：

5 与任一第二隐私计算设备进行管理面互通时，向第二隐私计算设备发送第一查询请求，所述第一查询请求中携带所述第一隐私计算设备的第一标识信息以及待查询的子算法的第二标识信息；其中，所述第一隐私计算设备与每个第二隐私计算设备之间分别基于管理面互通进行隐私计算任务的协同，基于数据面互通执行所述隐私计算任务，其中，所述管理面互通与所述数据面互通相互独立；
10

 若接收到所述第二隐私计算设备发送的所述第二标识信息的子算法包含的组件信息，向所述第二隐私计算设备发送加载所述第二标识信息的子算法包含的组件的加载请求。

14、根据权利要求 13 所述的方法，其中，所述向第二隐私计算设备发送第一查询请求包括：
15

 基于设定的第一应用程序编程接口 API，向所述第二隐私计算设备发送所述第一查询请求；

 所述向所述第二隐私计算设备发送加载所述第二标识信息的子算法包含的组件的加载请求包括：

20 基于设定的第二 API，向所述第二隐私计算设备发送所述加载请求。

15、根据权利要求 13 所述的方法，所述向第二隐私计算设备发送第一查询请求之前，所述方法还包括：

 向所述第二隐私计算设备发送隐私算法互通的合作请求，所述合作请求中携带所述第一隐私计算设备的第一标识信息。

25 16、根据权利要求 15 所述的方法，其中，所述向所述第二隐私计算设备发送隐私算法互通的合作请求包括：

 基于设定的第三 API，向所述第二隐私计算设备发送隐私算法互通的合作

请求。

17、根据权利要求 13-16 任一所述的方法，所述方法还包括：

向所述第二隐私计算设备发送第二查询请求，所述第二查询请求中携带所述第一隐私计算设备的第一标识信息以及待查询的数据资源的第三标识信息。

5

18、根据权利要求 17 所述的方法，其中，所述向所述第二隐私计算设备发送第二查询请求包括：

基于设定的第四 API，向所述第二隐私计算设备发送所述第二查询请求。

19、根据权利要求 17 所述的方法，所述向所述第二隐私计算设备发送第二查询请求之后，所述方法还包括：

10

向所述第二隐私计算设备发送使用所述第三标识信息的数据资源的授权请求，所述授权请求中携带所述第一隐私计算设备的第一标识信息。

20、根据权利要求 19 所述的方法，其中，所述向所述第二隐私计算设备发送使用所述第三标识信息的数据资源的授权请求包括：

15

基于设定的第五 API，向所述第二隐私计算设备发送所述授权请求。

21、根据权利要求 17 所述的方法，所述方法还包括：

向所述第二隐私计算设备发送项目运行准备请求，所述项目运行准备请求中携带所述第一隐私计算设备的第一标识信息、待运行项目所需的子算法的第二标识信息以及待运行项目所需的目标数据资源的第三标识信息。

20

22、根据权利要求 21 所述的方法，其中，所述向所述第二隐私计算设备发送项目运行准备请求包括：

基于设定的第六 API，向所述第二隐私计算设备发送所述项目运行准备请求。

23、根据权利要求 21 所述的方法，所述方法还包括：

与任一第二隐私计算设备进行数据面互通时，所述第一隐私计算设备接收所述第二隐私计算设备发送的第二确认信息，向所述第二隐私计算设备发送启动计算任务的启动请求。

25

24、一种隐私计算方法，所述方法应用于任一第二隐私计算设备，所述方法包括：

与第一隐私计算设备进行管理面互通时，接收所述第一隐私计算设备发送的第一查询请求，所述第一查询请求中携带所述第一隐私计算设备的第一标识信息以及待查询的子算法的第二标识信息；其中，所述第一隐私计算设备与每个第二隐私计算设备之间分别基于管理面互通进行隐私计算任务的协同，基于数据面互通执行所述隐私计算任务，其中，所述管理面互通与所述数据面互通相互独立；

在确定所述第一标识信息位于保存的合规设备的标识信息中时，将保存的所述第二标识信息的子算法包含的组件信息发送给所述第一隐私计算设备；

若接收到所述第一隐私计算设备发送的加载请求，加载所述第二标识信息的子算法包含的组件，在加载成功后，将加载成功的信息发送给所述第一隐私计算设备。

25、根据权利要求 24 所述的方法，其中，所述接收所述第一隐私计算设备发送的第一查询请求包括：

基于第一 API，接收所述第一查询请求；

所述将保存的所述第二标识信息的子算法包含的组件信息发送给所述第一隐私计算设备包括：

基于所述第一 API，将保存的所述第二标识信息的子算法包含的组件信息发送给所述第一隐私计算设备；

接收所述第一隐私计算设备发送的加载请求包括：

基于第二 API，接收所述加载请求；

所述将加载成功的信息发送给所述第一隐私计算设备包括：

基于所述第二 API，将加载成功的信息发送给所述第一隐私计算设备。

26、根据权利要求 24 所述的方法，所述接收第一隐私计算设备发送的第一查询请求之前，所述方法还包括：

接收所述第一隐私计算设备发送的合作请求，所述合作请求中携带所述

第一隐私计算设备的第一标识信息;

在确定所述第一标识信息位于保存的合规设备的标识信息中时, 向所述第一隐私计算设备发送同意合作的第一确认信息。

27、根据权利要求 26 所述的方法, 其中, 所述接收所述第一隐私计算设备发送的合作请求包括:

基于第三 API, 接收所述合作请求;

所述向所述第一隐私计算设备发送同意合作的第一确认信息包括:

基于所述第三 API, 发送所述第一确认信息。

28、根据权利要求 24-27 任一所述的方法, 所述方法还包括:

10 接收所述第一隐私计算设备发送的第二查询请求, 所述第二查询请求中携带所述第一隐私计算设备的第一标识信息以及待查询的数据资源的第三标识信息;

在确定所述第一标识信息位于保存的合规设备的标识信息中时, 将保存的所述第三标识信息的数据资源的信息发送给所述第一隐私计算设备。

15 29、根据权利要求 28 所述的方法, 其中, 所述接收所述第一隐私计算设备发送的第二查询请求包括:

基于第四 API, 接收所述第二查询请求;

所述将保存的所述第三标识信息的数据资源的信息发送给所述第一隐私计算设备包括:

20 基于所述第四 API, 将所述第三标识信息的数据资源的信息发送给所述第一隐私计算设备。

30、根据权利要求 28 所述的方法, 所述接收所述第一隐私计算设备发送的第二查询请求之后, 所述方法还包括:

25 接收所述第一隐私计算设备发送的授权请求, 所述授权请求中携带所述第一隐私计算设备的第一标识信息;

在确定所述第一标识信息位于保存的合规设备的标识信息中时, 向所述第一隐私计算设备发送授权使用所述第三标识信息的数据资源的授权通过信

息。

31、根据权利要求 30 所述的方法，其中，所述接收所述第一隐私计算设备发送的授权请求包括：

基于第五 API，接收所述授权请求；

5 所述向所述第一隐私计算设备发送授权使用所述第三标识信息的数据资源的授权通过信息包括：

基于所述第五 API，向所述第一隐私计算设备发送所述授权通过信息。

32、根据权利要求 28 所述的方法，所述方法还包括：

接收所述第一隐私计算设备发送的项目运行准备请求，所述项目运行准备请求中携带所述第一隐私计算设备的第一标识信息、待运行项目所需的子
10 算法的第二标识信息以及待运行项目所需的目标数据资源的第三标识信息；

在确定所述第一标识信息位于保存的合规设备的标识信息中时，并在确定保存有所述第三标识信息的目标数据资源，以及所述第二标识信息的子算法包含的组件加载完成时，向所述第一隐私计算设备发送准确就绪的第二确
15 认信息。

33、根据权利要求 32 所述的方法，其中，所述接收所述第一隐私计算设备发送的项目运行准备请求包括：

基于第六 API，接收所述项目运行准备请求；

所述向所述第一隐私计算设备发送准确就绪的第二确认信息包括：

20 基于所述第六 API，所述第一隐私计算设备发送所述第二确认信息。

34、根据权利要求 32 所述的方法，所述方法还包括：

与所述第一隐私计算设备进行数据面互通时，接收所述第一隐私计算设备发送的启动请求，并基于所述第三标识信息的目标数据资源，运行所述第二标识信息的子算法。

25 35、一种隐私计算装置，所述装置包括：

第一发送模块，用于与任一第二隐私计算设备进行数据面互通时，向所述第二隐私计算设备发送第一查询请求，所述第一查询请求中携带所述第一

隐私计算设备的第一标识信息以及待查询的子算法的第二标识信息；其中，所述第一隐私计算设备与每个第二隐私计算设备之间分别基于管理面互通进行隐私计算任务的协同，基于数据面互通执行所述隐私计算任务，其中，所述管理面互通与所述数据面互通相互独立；

- 5 第二发送模块，用于若接收到所述第二隐私计算设备发送的所述第二标识信息的子算法包含的组件信息，向所述第二隐私计算设备发送加载所述第二标识信息的子算法包含的组件的加载请求。

36、一种隐私计算装置，所述装置包括：

- 10 第一接收模块，用于与第一隐私计算设备进行管理面互通时，接收所述第一隐私计算设备发送的第一查询请求，所述第一查询请求中携带所述第一隐私计算设备的第一标识信息以及待查询的子算法的第二标识信息；其中，所述第一隐私计算设备与每个第二隐私计算设备之间分别基于管理面互通进行隐私计算任务的协同，基于数据面互通执行所述隐私计算任务，其中，所述管理面互通与所述数据面互通相互独立；

- 15 第三发送模块，用于在确定所述第一标识信息位于保存的合规设备的标识信息中时，将保存的所述第二标识信息的子算法包含的组件信息发送给所述第一隐私计算设备；

- 20 加载模块，用于若接收到所述第一隐私计算设备发送的加载请求，加载所述第二标识信息的子算法包含的组件，在加载成功后，将加载成功的信息发送给所述第一隐私计算设备。

37、一种电子设备，其包括处理器和存储器，其中，所述存储器存储有程序代码，当所述程序代码被所述处理器执行时，使得所述处理器执行权利要求 13 至 34 任一项所述隐私计算方法的步骤。

- 25 38、一种计算机可读存储介质，其包括程序代码，当所述存储介质在电子设备上运行时，所述程序代码用于使所述电子设备执行权利要求 13 至 34 任一项所述隐私计算方法的步骤。