

PRIVACY COMPUTING SYSTEM, METHOD, APPARATUS, DEVICE AND MEDIUM

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims priority to Chinese Patent Application No. 202210837745.8, entitled “PRIVACY COMPUTING SYSTEM, METHOD, APPARATUS, DEVICE AND MEDIUM,” filed on July 15, 2022, the entire content of which is incorporated herein by reference.

FIELD OF THE DISCLOSURE

[0002] The disclosure generally relates to the field of data security technology and, more particularly, relates to a privacy computing system, method, apparatus, device and medium.

BACKGROUND

[0003] Privacy computing (or privacy compute) refers to a collection of technologies that realize data analysis and computation on the premise of protecting the data from being leaked to the outside world, to achieve the objective of “available but invisible data”, which then allows to achieve data value transformation and release on the premise of full data and privacy security protection.

[0004] With the increasing awareness of data protection in the relevant fields and the tightening of privacy regulatory policies, privacy computing has received widespread attention in the relevant fields due to its “available but invisible” feature. Many technology companies have launched their own privacy computing products with specific field-related features. A large variety of privacy computing products have enriched market choices and also brought new challenges. For example, privacy computing products launched by different technology

companies are usually designed and implemented based on different system platforms. When the privacy computing products of different system platforms are stored in different privacy computing devices, it is generally impossible to complete the interaction of information between privacy computing products of different system platforms, which then turns “data islands” into “computing islands”. In addition, even if the same privacy computing product is launched by the same technology company, when the same privacy computing product is stored in different privacy computing devices, the interaction of information between the same privacy computing product in different devices is usually impossible, which also turns a “data island” into a “computing island”.

[0005] Therefore, the problem of interconnection and interoperability between privacy algorithm products stored in different privacy computing devices has become an absolute pain point in the relevant fields. How to achieve interconnection and interoperability between privacy algorithm products stored in different privacy computing devices is a technical problem that needs to be urgently addressed currently.

SUMMARY

[0006] The disclosure provides a privacy computing system, method, apparatus, device and medium for realizing interconnection and interoperability between privacy algorithm products stored in different privacy computing devices.

[0007] In a first aspect, the disclosure provides a privacy computing system, which includes: a first privacy computing device and at least one second privacy computing device; where the first privacy computing device and each second privacy computing device collaborate on privacy computing tasks based on management plane interoperability, and execute the privacy computing tasks based on data plane interoperability, where the management plane

interoperability and the data planes interoperability are mutually independent; for each second privacy computing device, when the first privacy computing device and the second privacy computing device perform the management plane interoperability, the first privacy computing device is configured to send a first query request to the second privacy computing device, where the first query request carries first identification information of the first privacy computing device and second identification information of a to-be-queried sub-algorithm; the second privacy computing device is configured to receive the first query request, and when it is determined that the first identification information is located in stored identification information for compliance devices, send stored information for components included in the sub-algorithm with the second identification information to the first privacy computing device; the first privacy computing device is further configured to receive the information for components included in the sub-algorithm with the second identification information, and send, to the second privacy computing device, a loading request for loading the components included in the sub-algorithm with the second identification information; and the second privacy computing device is further configured to receive the loading request, load the components included in the sub-algorithm with the second identification information, and after the loading is successful, send a loading success message to the first privacy computing device.

[0008] In a second aspect, the disclosure provides a privacy computing method, which method is applied to a first privacy computing device, and the method includes: when performing management plane interoperability with a second privacy computing device, sending a first query request to the second privacy computing device, where the first query request carries first identification information of the first privacy computing device and second identification information of a to-be-queried sub-algorithm, and the first privacy computing device and the

second privacy computing device respectively collaborate on privacy computing tasks based on the management plane interoperability, and perform the privacy computing tasks based on data plane interoperability, where the management plane interoperability and the data plane interoperability are mutually independent; and when information for components included in the sub-algorithm with the second identification information sent by the second privacy computing device is received, sending to the second privacy computing device a loading request for loading the components included in the sub-algorithm with the second identification information.

[0009] In a third aspect, the disclosure provides a privacy computing method, which method is applied to any second privacy computing device, and the method includes: when performing management plane interoperability with a first privacy computing device, receiving a first query request sent by the first privacy computing device, where the first query request carries first identification information of the first privacy computing device and second identification information of a to-be-queried sub-algorithm, and the first privacy computing device and the second privacy computing device collaborate on privacy computing tasks based on the management plane interoperability and execute the privacy computing tasks based on data plane interoperability, where the management plane interoperability and the data plane interoperability are mutually independent; when it is determined that the first identification information is located in stored identification information for compliance devices, sending to the first privacy computing device stored information for components included `; and when a loading request sent by the first privacy computing device is received, loading the components included in the sub-algorithm with the second identification information, and after the loading is successful, sending a loading success message to the first privacy computing device.

[0010] In a fourth aspect, the disclosure provides a privacy computing device, which

includes: a first transmission module, configured to send a first query request to a second privacy computing device when performing management plane interoperability with the second privacy computing device, where the first query request carries first identification information of the first privacy computing device and second identification information of a to-be-queried sub-algorithm, and the first privacy computing device and the second privacy computing device collaborate on privacy computing tasks based on the management plane interoperability and perform the privacy computing tasks based on data plane interoperability, where the management plane interoperability and the data plane interoperability are mutually independent; and a second transmission module, configured to, when information for components included in the sub-algorithm with the second identification information sent by the second privacy computing device is received, send to the second privacy computing device a loading request for loading the components included in the sub-algorithm with the second identification information.

[0011] In a fifth aspect, the disclosure provides another privacy computing device, which includes: a first receiving module, configured to receive a first query request sent by a first privacy computing device when performing management plane interoperability with the first privacy computing device, where the first query request carries first identification information of the first privacy computing device and second identification information of a to-be-queried sub-algorithm, and the first privacy computing device and a second privacy computing device collaborate on privacy computing tasks based on the management plane interoperability and perform the privacy computing tasks based on data plane interoperability, where the management plane interoperability and the data plane interoperability are mutually independent; a third transmission module, configured to send stored information for components included in the sub-algorithm with the second identification information to the first privacy computing

device when it is determined that the first identification information is located in stored identification information for compliance devices; and a loading module, configured to load the components included in the sub-algorithm with the second identification information upon receiving a loading request sent by the first privacy computing device, and after the loading is successful, send a loading success message to the first privacy computing device.

[0012] In a sixth aspect, the disclosure provides an electronic device, which includes a processor and a memory, where the memory stores program code, and when the program code is executed by the processor, the processor is caused to execute the steps of the privacy computation methods described elsewhere herein.

[0013] In a seventh aspect, the disclosure provides a computer-readable storage medium, which includes program code. When the storage medium is run on an electronic device, the program code is configured to cause the electronic device to execute the steps of the privacy computation methods described elsewhere herein.

[0014] In an eighth aspect, the disclosure provides a computer program product. The computer program product includes: computer program code. When the computer program code is run on a computer, it causes the computer to execute the steps of the privacy computation methods described elsewhere herein.

[0015] Since the disclosure is directed to each second privacy computing device, when the first privacy computing device communicates with the second privacy computing device on the management plane, the first privacy computing device may send a first query request to the second privacy computing device. The query request carries the first identification information of the first privacy computing device and the second identification information of the to-be-queried sub-algorithm. The second privacy computing device may receive the first query request

and when it is determined that the first identification information is located in the stored identification information for compliance devices, stored information for components included in the sub-algorithm with the second identification information is sent to the first privacy computing device. The first privacy computing device receives the information for components included in the sub-algorithm with the second identification information, and sends to the second privacy computing device a loading request for loading the components included in the sub-algorithm with the second identification information. The second privacy computing device may receive the loading request, load the components included in the sub-algorithm with the second identification information, and after the loading is successful, send a loading success message to the first privacy computing device. Since the first privacy computing device and each second privacy computing device of the disclosure may respectively collaborate on privacy computing tasks based on management plane interoperability, and perform privacy computing tasks based on data plane interoperability, the management plane interoperability and the data plane interoperability are mutually independent. In this way, the purpose of interconnection and interoperability between privacy algorithm products stored in different privacy computing devices may be achieved.

BRIEF DESCRIPTION OF THE DRAWINGS

[0016] In order to more clearly explain the embodiments of the present disclosure or the implementation of related technologies, the following will briefly introduce the drawings that are essential for the understanding of the embodiments or related technologies. Apparently, the drawings in the following description are merely some of the present disclosure. For those of ordinary skill in the art, other drawings may also be obtained based on these drawings.

[0017] FIG. 1 shows a schematic structural diagram of a privacy computing system

according to some embodiments;

[0018] FIG. 2 shows a schematic diagram of a privacy algorithm interconnection and interoperability process according to some embodiments;

[0019] FIG. 3 shows a schematic diagram of another privacy algorithm interconnection and interoperability process according to some embodiments;

[0020] FIG. 4 shows a flowchart of a privacy computation method according to some embodiments;

[0021] FIG. 5 shows a schematic diagram of a privacy computing device according to some embodiments;

[0022] FIG. 6 shows a flowchart of another privacy computation method according to some embodiments;

[0023] FIG. 7 shows a schematic diagram of another privacy computing device according to some embodiments; and

[0024] FIG. 8 shows a schematic structural diagram of an electronic device according to some embodiments.

DETAILED DESCRIPTION

[0025] In order to realize interconnection and interoperability between different privacy computing products, the disclosure provides a privacy computing system, method, apparatus, device and medium.

[0026] In order to make the purpose and implementation of the disclosure clearer, the exemplary embodiments of the disclosure will be clearly and thoroughly described hereinafter in conjunction with the accompanying drawings in the exemplary embodiments of the disclosure. Apparently, the described exemplary embodiments are merely some embodiments, rather than all

of the embodiments of the disclosure.

[0027] The terms “first”, “second”, “third”, and the like in the description and claims of the disclosure and the drawings are used to distinguish same or similar objects or entities, and do not necessarily mean to limit specific sequences or sequential order unless otherwise noted. It is to be understood that the terms so used are interchangeable under appropriate circumstances.

[0028] The terms “comprise” and “include” and any variations thereof are intended to cover but not exclusively include, for example, a product or device that includes a list of components need not be limited to all components expressly listed, but may include any component not expressly listed, and other components listed separately or inherent to these products or devices.

[0029] Further, it should be noted that the above embodiments are merely used to illustrate the technical solution of the disclosure, but not to limit the disclosure. Although the disclosure has been described in detail with reference to the disclosed embodiments, those of ordinary skill in the art should understand that the technical solutions described in these embodiments may still be modified, or some or all of the technical features may be equivalently replaced. These modifications or substitutions do not deviate the essence of the corresponding technical solutions from the scope of the technical solution of the embodiments of the present disclosure.

Embodiment 1:

[0030] FIG. 1 shows a schematic structural diagram of a privacy computing system according to some embodiments. The system includes a first privacy computing device 11 and at least one second privacy computing device 12. The first privacy computing device 11 and each second privacy computing device 12 collaborate on privacy computing tasks based on

management plane interoperability, and perform the privacy computing tasks based on data plane interoperability, where the management plane interoperability and the data plane interoperability are mutually independent.

[0031] For each second privacy computing device 12, when the first privacy computing device 11 and the second privacy computing device 12 perform management plane interoperability, the first privacy computing device 11 is configured to send a first query request to the second privacy computing device 12, which carries the first identification information of the first privacy computing device 11 and second identification information for a privacy algorithm to be queried.

[0032] The second privacy computing device 12 is configured to receive the first query request, and when it is determined that the first identification information is located in stored identification information for compliance devices, send to the first privacy computing device 11 stored information for components included in a sub-algorithm with the second identification information.

[0033] The first privacy computing device 11 is further configured to receive the information for components included in the sub-algorithm with the second identification information, and send to the second privacy computing device 12 a loading request for loading the components included in the sub-algorithm with the second identification information.

[0034] The second privacy computing device 12 is further configured to receive the loading request, load the components included in the sub-algorithm with the second identification information, and after the loading is successful, send a loading success message to the first privacy computing device 11.

[0035] In some embodiments, the first privacy computing device 11 and the

second privacy computing device 12 may be devices such as PCs, mobile terminals, servers, etc., which are not specifically limited in the disclosure. The first privacy computing device 11 and the second privacy computing device 12 may be two different devices.

[0036] In some embodiments, refer to FIG. 1, the first privacy computing device 11 and the second privacy computing device 12 each store a sub-algorithm of a privacy algorithm. For ease of description, the sub-algorithm stored in the first privacy computing device 11 is referred to as the first sub-algorithm, and the sub-algorithm stored in the second privacy computing device 12 is referred to as the second sub-algorithm. In some embodiments, the first sub-algorithm and the second sub-algorithm may respectively be part of the sub-algorithms included in a same privacy computing product launched by a same technology company. Optionally, the first sub-algorithm and the second sub-algorithm may also be different privacy computing products launched by different technology companies based on different system platforms, etc., which may be flexibly set according to needs and are not limited in the disclosure. For example, taking the first sub-algorithm and the second sub-algorithm as partial sub-algorithms included in the same privacy computing product (e.g., privacy algorithm) launched by the same technology company as an example, the first sub-algorithm stored in the first privacy computing device may be a sub-algorithm that includes a guest part (i.e., the party with label y which is the party for data consumption) in the privacy algorithm, and the second sub-algorithm stored in the second privacy computing device may be a sub-algorithm that includes a host part (i.e., the party without label y which is the party for data supply) in the privacy algorithm.

[0037] In some embodiments, the number of second privacy computing devices may be one or multiple. The disclosure does not specifically limit the number of second privacy computing devices, which may be flexibly set according to needs. Whether there is one or more

privacy computing devices, for each second privacy computing device, a privacy computing process between the privacy algorithm products stored in the first privacy computing device and in the second privacy computing device during the interconnection and interoperability can adopt the privacy computing process provided by the embodiments of the disclosure, which will not be specifically described here.

[0038] In some embodiments, the first sub-algorithm may be stored in the data plane of the first privacy computing device, and the second sub-algorithm may be stored in the data plane of the second privacy computing device. The first privacy computing device and each second privacy computing device respectively collaborate on privacy computing tasks based on management plane interoperability, and may perform the privacy computing tasks based on data plane interoperability, so that the first sub-algorithm stored in the first privacy computing device and the second sub-algorithm stored in the second privacy computing device may be interconnected and interoperated for joint computation. Optionally, management plane interoperability and data plane interoperability between privacy computing devices may be mutually independent. Exemplarily, refer to FIG. 2, which shows a schematic diagram of a privacy algorithm interconnection and interoperability process according to some embodiments. As shown in FIG. 2, in order to achieve interconnection and interoperability between privacy algorithm products stored in different privacy computing devices, in some embodiments, when the first privacy computing device and any second privacy computing device perform management plane interoperability, privacy algorithm developers and others may send to the second privacy computing device 12 offline in advance the Internet protocol (IP) address, identity document (ID) and other identification information (for ease of description, the identification information of the first privacy computing device 11 will be referred to as the first

identification information hereinafter) of the first privacy computing device 11. The second privacy computing device 12 may consider the first privacy computing device 11 corresponding to the first identification information as a secure compliance device, and save the first identification information in the identification information for its own compliance devices. At the same time, privacy algorithm developers and others may also send offline in advance the IP address, ID and other identification information of the second privacy computing device 12 (for ease of description, the identification information of the second privacy computing device 12 will be referred to as the second identification information hereinafter) to the first privacy computing device 11. The first privacy computing device 11 may consider the second privacy computing device 12 corresponding to the second identification information as a secure compliance device, and save the second identification information in the identification information for its own compliance devices. In other words, the first privacy computing device 11 and the second privacy computing device 12 may exchange identification information such as node IP and node ID and so on offline.

[0039] In some embodiments, in order to increase the flexibility and accuracy of privacy computations, a privacy algorithm such as the first sub-algorithm and the second sub-algorithm may be decoupled to include a scene algorithm and a security algorithm. Here, if a privacy algorithm does not include a security algorithm but just includes a scenario algorithm, a privacy computation may be considered to be a plaintext computation on the to-be-processed data without security encryption protection. If a privacy algorithm includes both a scenario algorithm and a security algorithm, the privacy computation may be considered to be a private computation on the to-be-processed data under secure encryption protection. The scenario algorithm and security algorithm included in a privacy algorithm may be flexibly selected according to needs,

which is not limited in the present disclosure.

[0040] In some embodiments, the first sub-algorithm may include a first scenario algorithm and a first security algorithm, and the second sub-algorithm may include a second scenario algorithm and a second security algorithm. In order to ensure the security of the interconnection and interoperability between privacy algorithm products stored in different privacy computing devices, in some embodiments, in addition to sending offline in advance the first identification information of the first privacy computing device 11 to the second privacy computing device 12, a security certificate of the first security algorithm included in the first sub-algorithm may also be sent offline in advance to the second privacy computing device 12. The second privacy computing device 12 may save the security certificate and a token of the first sub-algorithm carried by the security certificate (for ease of description, the token carried by the security certificate is referred to as the reference token). Similarly, in addition to sending the second identification information of the second privacy computing device 12 to the first privacy computing device 11 in advance, the security certificate of the second security algorithm included in the second sub-algorithm may also be sent offline in advance to the first privacy computing device 11. The first privacy computing device 11 may save the security certificate and the reference token of the second sub-algorithm carried by the security certificate. In other words, the first privacy computing device 11 and the second privacy computing device 12 may exchange security certificates and the like offline. The purpose of the reference tokens will be described later and will not be specifically described here.

[0041] In some embodiments, in order to achieve interconnection and interoperability between privacy algorithm products stored in different privacy computing devices, different privacy algorithm products, that is, sub-algorithms stored in different privacy computing devices,

may be configured as an algorithm with a container structure. The algorithm of the container structure may include several algorithm components. Optionally, in order to achieve interconnection and interoperability between privacy algorithm products stored in different privacy computing devices, a process of interoperating between algorithm components (i.e., sub-algorithms) included in different privacy computing products may be performed. Optionally, the process of interoperating between algorithm components may be as follows.

[0042] The first privacy computing device 11 may send to the second privacy computing device 12 a first query request for querying algorithm component information (for ease of description, the query request for querying algorithm component information is referred to as a first query request). The first query request may carry the first identification information of the first privacy computing device 11 and the second identification information of the to-be-queried sub-algorithm. If the second privacy computing device 12 receives the first query request, it may then determine whether the first identification information carried in the first query request is located in the pre-stored identification information for compliance devices. If the first identification information is located in the pre-stored identification information for compliance devices, the first privacy computing device 11 with the first identification information may be considered a secure compliance device. Stored information for components included in the sub-algorithm with the second identification information may be sent (or returned) to the first privacy computing device 11.

[0043] The first privacy computing device 11 may receive the information for components included in the sub-algorithm (i.e., second sub-algorithm) with the second identification information sent by the second privacy computing device 12 and save it. In some embodiments, before pre-running the first sub-algorithm and the second sub-algorithm, the

first privacy computing device 11 may send to the second privacy computing device 12 a loading request for loading components included in the algorithm with the second identification information (i.e., the second sub-algorithm). After receiving the loading request, the second privacy computing device 12 may load the components included in the sub-algorithm with the second identification information (i.e., second sub-algorithm), that is, the second privacy computing device 12 may load the components included in the second sub-algorithm. That is, the components included in the second sub-algorithm are synchronized online. Optionally, after the second privacy computing device 12 successfully loads the components included in the sub-algorithm with the second identification information (i.e., the algorithm components are completely online), a loading success message may be sent (or returned) to the first privacy computing device. This enables the first privacy computing device 11 to learn that the second sub-algorithm in the second privacy computing device 12 has been loaded successfully.

[0044] Since the disclosure is directed to each second privacy computing device 12, when the first privacy computing device 11 and each second privacy computing device 12 perform management plane interoperability, the first privacy computing device 11 may send a first query request to the second privacy computing device 12. The first query request carries the first identification information of the first privacy computing device 11 and the second identification information of the to-be-queried sub-algorithm. The second privacy computing device 12 may receive the first query request, and when it is determined that the first identification information is located in the stored identification information for compliance devices, stored information for components included in the sub-algorithm with the second identification information is sent to the first privacy computing device 11. The first privacy

computing device 11 receives the information for the components included in the sub-algorithm with the second identification information, and sends a loading request to the second privacy computing device 12 to load the components included in the sub-algorithm with the second identification information. The second privacy computing device 12 may receive the loading request, and load the components included in the sub-algorithm with the second identification information. After the loading is successful, a loading success message is sent to the first privacy computing device 11. In the disclosure, since the first privacy computing device 11 and each second privacy computing device 12 may respectively collaborate on the privacy computing tasks based on the management plane interoperability, and perform the privacy computing tasks based on the data plane interoperability, and the management plane interoperability and data plane interoperability are mutually independent, which then allows the realization of the purpose of interconnection and interoperability between privacy algorithm products stored in different privacy computing devices.

Embodiment 2:

[0045] In order to ensure the security of the interconnection and interoperability between the first sub-algorithm and the second sub-algorithm, on the basis of the above embodiments, in the embodiments disclosed herein, the first privacy computing device 11 is specifically configured to send the first query request to the second privacy computing device 12 based on a first application programming interface (API).

[0046] The second privacy computing device 12 is specifically configured to receive the first query request based on the first API; and based on the first API, send to the first privacy computing device 11 the store information for the components included in the sub-algorithm with the second identification information.

[0047] The first privacy computing device 11 is specifically configured to receive, based on the first API, the information for components included in the sub-algorithm with the second identification information; and send a loading request to the second privacy computing device 12 based on a configured second API.

[0048] The second privacy computing device 12 is specifically configured to receive the loading request based on the second API, and send the loading success message to the first privacy computing device 11 based on the second API.

[0049] In some embodiments, when the first privacy computing device 11 sends the first query request to the second privacy computing device 12, the first privacy computing device 11 may send the first query request to the second privacy computing device 12 based on the configured first API. Here, for ease of description, the API that sends the first query request is referred to as the first API. Optionally, the second privacy computing device 12 may also receive the first query request based on the first API, and when it is determined that the first identification information is located in the stored identification information for compliance devices, send to the first privacy computing device 11 the stored information for components included in the sub-algorithm with the second identification information (i.e., second sub-algorithm) based on the first API. The first privacy computing device 11 may receive, based on the first API, the information for components included in the sub-algorithm with the second identification information (i.e., second sub-algorithm) sent by the second privacy computing device 12.

[0050] In addition, when sending the loading request to the second privacy computing device 12, the first privacy computing device 11 may send the loading request to the second privacy computing device 12 based on a configured second API (for ease of description,

the API that sends the loading request is referred to as the second API). The second privacy computing device 12 may receive the loading request sent by the first privacy computing device 11 based on the second API, and may send a loading success message to the first privacy computing device 11 based on the second API after the loading is successful. Optionally, the first API and the second API may be representational state transfer (RESTful) API.

[0051] In the disclosure, since the first query request, information for components included in the sub-algorithm and other information can be sent based on the configured standard APIs, the security of the interconnection and interoperability between the sub-algorithms may be further improved.

Embodiment 3:

[0052] In order to improve the security of interconnection and interoperability between sub-algorithms, on the basis of the above embodiments, in the embodiments disclosed herein, the first privacy computing device 11 is further configured to send a cooperation request to the second privacy computing device 12 for sub-algorithm interoperability, where the cooperation request carries the first identification information of the first privacy computing device 11.

[0053] The second privacy computing device 12 is further configured to receive the cooperation request, and when it is determined that the first identification information is located in the stored identification information for compliance devices, send to the first privacy computing device 11 a first confirmation message for agreeing to cooperate.

[0054] In some embodiments, refer to FIG. 2 again, in order to improve the security of the interconnection and interoperability between sub-algorithms, before the first privacy computing device 11 sends the first query request to the second privacy computing device 12, a cooperation request (or cooperation application) for privacy algorithm interoperability (or

interconnection and interoperability) is sent to the second privacy computing device 12.

Optionally, the cooperation request may carry the first identification information of the first privacy computing device 11. When the second privacy computing device 12 receives the cooperation request, the second privacy computing device 12 may determine whether the first identification information carried in the cooperation request is located in the pre-stored identification information for compliance devices. If the second privacy computing device 12 determines that the first identification information carried in the cooperation request is located in the identification information for compliance devices stored by itself, the first privacy computing device 11 with the first identification information may be considered to be a secure compliance device. The second privacy computing device 12 may send (or return) the first confirmation message for agreeing to cooperate to the first privacy computing device 11 (for ease of description, the confirmation message for agreeing to cooperate is referred to as the first confirmation message). For ease of description, the subsequent processes in which the first privacy computing device 11 sends the cooperation request and the second privacy computing device 12 sends the first confirmation message for agreeing to cooperate are referred to as node interoperating.

[0055] In some embodiments, in order to ensure the security of the interconnection and interoperability between the first sub-algorithm and the second sub-algorithm, when the first privacy computing device 11 sends the cooperation request to the second privacy computing device 12, the first privacy computing device 11 may send the cooperation request to the second privacy computing device 12 based on a configured third API (for ease of description, the API that sends the cooperation request is referred to as the third API). The second privacy computing device 12 may receive the cooperation request sent by the first privacy computing

device 11 based on the third API, and may send the first confirmation message based on the third API when it is determined that the first identification information is located in the stored identification information for compliance devices. Optionally, the third API may be a RESTful API.

[0056] In the disclosure, since the cooperation request, first confirmation message and other information may be sent based on the configured standard APIs, the security of the interconnection and interoperability between sub-algorithms may be further improved.

Embodiment 4:

[0057] In order to improve the security of interconnection and interoperability between sub-algorithms, on the basis of the above embodiments, in the embodiments disclosed herein, the first privacy computing device 11 is further configured to send a second query request to the second privacy computing device 12, which carries the first identification information of the first privacy computing device 11 and third identification information of a to-be-queried data resource.

[0058] The second privacy computing device 12 is further configured to receive the second query request, and when it is determined that the first identification information is located in the stored identification information for compliance devices, send the stored information for the data resource with the third identification information to the first privacy computing device 11.

[0059] In some embodiments, optionally, refer to FIG. 2, in order to interconnect and interoperate privacy algorithm products (i.e., sub-algorithms) stored in different privacy computing devices, when performing management plane interoperability, one may perform a process of interoperating data resources corresponding to different sub-algorithms. Optionally,

the process of data resource interoperability may be as follows.

[0060] The first privacy computing device 11 may send a second query request for querying a data resource to the second privacy computing device 12 (for ease of description, the query request for querying a data resource is referred to as the second query request). The timing of sending the second query request is not specifically limited in the disclosure and may be flexibly set according to needs. For example, the first privacy computing device 11 may send a cooperation request to the second privacy computing device 12. After receiving a first confirmation message sent by the second privacy computing device 12 for agreeing to cooperate, the first privacy computing device 11 sends a second query request to the second privacy computing device 12. In some embodiments, the second query request may carry the first identification information of the first privacy computing device 11 and the third identification information of the to-be-queried data resource (for ease of description, the identification information for a to-be-queried data resource is referred to as third identification information).

[0061] After receiving the second query request, the second privacy computing device 12 may determine whether the first identification information carried in the second query request is located in the pre-stored identification information for compliance devices. If it is determined that the first identification information is located in its own stored identification information for compliance devices, the first privacy computing device 11 corresponding to the first identification information may be considered a secure compliance device. The stored information for the data resource with the third identification information may be sent (or returned) to the first privacy computing device 11. The first privacy computing device 11 may receive and save the information for the data resource with the third identification information, thereby realizing the interoperability of data resources corresponding to different sub-algorithms.

[0062] The disclosure may realize the interoperability of data resources corresponding to different sub-algorithms. In this way, the purpose of interconnection and interoperability of different privacy computing products may be achieved.

[0063] In addition, the disclosure does not specifically limit the order in which the data resources are interoperated and the algorithm components are interoperated. That is, the data resource interoperability steps may be performed first, or the algorithm component interoperability steps may be performed first, which may be flexibly selected according to needs.

[0064] In some embodiments, in order to ensure the security of the interconnection and interoperability between the first sub-algorithm and the second sub-algorithm, when sending the second query request to the second privacy computing device 12, the first privacy computing device 11 may send the second query request to the second privacy computing device 12 through a fourth API (for ease of description, the API that sends the second query request is referred to as the fourth API). The second privacy computing device 12 may receive the second query request sent by the first privacy computing device 11 based on the fourth API. The second privacy computing device 12 may determine that the first identification information is located in the stored identification information for compliance devices, and send the stored data resource information with the third identification information to the first privacy computing device 11 based on the fourth API. Optionally, the fourth API may be a RESTful API.

[0065] Since the disclosure may perform the data resource interoperability process based on the configured standard APIs, the security of interoperability between sub-algorithms may be further improved.

Embodiment 5:

[0066] In order to improve the security of interconnection and interoperability between

sub-algorithms, on the basis of the above embodiments, in the embodiments disclosed herein, the first privacy computing device 11 is further configured to send an authorization request to the second privacy computing device 12 for using the data resource with the third identification information, where the authorization request carries the first identification information of the first privacy computing device 11.

[0067] The second privacy computing device 12 is further configured to receive the authorization request, and when it is determined that the first identification information is located in the stored identification information for compliance devices, send to the first privacy computing device 11 a granted authorization message for using the data resource with the third identification information.

[0068] In some embodiments, in order to enable the first sub-algorithm to use the data resource of the second sub-algorithm and realize interconnection and interoperability between different sub-algorithms, when performing data resource interoperability, after receiving the information for the data resource with the third identification information sent by the second privacy computing device 12, the first privacy computing device 11 may send to the second privacy computing device 12 an authorization request for using the data resource with the third identification information. Optionally, the authorization request may carry the first identification information of the first privacy computing device 11.

[0069] After receiving the authorization request, the second privacy computing device 12 may determine whether the first identification information carried in the authorization request is located in the pre-stored identification information for compliance devices. If it is determined that the first identification information is located in the pre-stored identification information for compliance devices, the first privacy computing device 11 corresponding to the first

identification information may be considered a secure compliance device. A granted authorization message for authorized use of the data resource with the third identification information may be sent (or return) to the first privacy computing device 11. After receiving the granted authorization message, the first privacy computing device 11 may use the data resource with the third identification information to perform relevant computations. Optionally, the data resource with the third identification information may be metadata, etc.

[0070] In the disclosure, since the first privacy computing device 11 may use the data resource with the third identification information after receiving the granted authorization message sent by the second privacy computing device 12, the first sub-algorithm and the second sub-algorithm may be interconnected and interoperated. At the same time, it may also achieve refined control and data security protection of data flow in the privacy computing process.

[0071] In some embodiments, in order to ensure the security of the interconnection and interoperability between the first sub-algorithm and the second sub-algorithm, when sending the authorization request to the second privacy computing device 12, the first privacy computing device 11 may send the authorization request to the second privacy computing device 12 based on a configured fifth API (for ease of description, the API that sends the authorization request is referred to as the fifth API). The second privacy computing device 12 may receive the authorization request based on the fifth API, and when it is determined that the first identification information is located in the stored identification information for compliance devices, send a granted authorization message to the first privacy computing device 11 based on the fifth API. Optionally, the fifth API may be a RESTful API.

[0072] In the disclosure, since the authorization request, granted authorization message and other information may be sent based on the configured standard APIs, the security of the

interconnection and interoperability between sub-algorithms may be further improved.

Embodiment 6:

[0073] In order to improve the security of interconnection and interoperability between sub-algorithms, on the basis of the above embodiments, in the embodiments disclosed herein, the first privacy computing device 11 is further configured to send a project execution preparation request to the second privacy computing device 12, which carries the first identification information of the first privacy computing device 11, second identification information of the sub-algorithm required for a to-be-run project, and third identification information for a target data resource required for the to-be-run project.

[0074] The second privacy computing device 12 is further configured to receive the project execution preparation request, and when it is determined that the first identification information is located in the stored identification information for compliance devices, and when it is determined that the target data resource with the third identification information is saved, and when it is determined that the components included in the sub-algorithm with the second identification information are completely loaded, send a confirmation message confirming a readiness to the first privacy computing device 11.

[0075] In some embodiments, before preparing to run the first sub-algorithm and the second sub-algorithm, the first privacy computing device 11 may also send a project execution preparation request to the second privacy computing device 12. In order to make the second privacy computing device 12 learn which sub-algorithm(s) and data resource(s) need to be prepared for the to-be-run project, in addition to the first identification information of the first privacy computing device 11, the project execution preparation request may also carry the second identification information for the sub-algorithm required for the to-be-run project and the

third identification information for the target data resource required for the to-be-run project. Here, the sub-algorithm and target data resource carried in the project execution preparation request may be flexibly set according to needs, which is not limited in the present disclosure.

[0076] After receiving the project execution preparation request, the second privacy computing device 12 may determine whether the first identification information carried in the project execution preparation request is located in the pre-stored identification information for compliance devices. If it is determined that the first identification information is located in the pre-stored identification information for compliance devices stored by itself, the first privacy computing device 11 corresponding to the first identification information may be considered a secure compliance device. The second privacy computing device 12 may then check whether it currently stores the target data resource with the third identification information and whether the components included in the sub-algorithm with the second identification information are completely loaded. When it is determined that the target data resource with the third identification information is stored and that the components included in the sub-algorithm with the second identification information are completely loaded, the second privacy computing device 12 may send a confirmation message for readiness (for ease of description, it is referred to as the second confirmation message) to the first privacy computing device 11. For ease of description, the process in which the first privacy computing device 11 sends a project execution preparation request to the second privacy computing device 12 and the second privacy computing device 12 sends the second confirmation message confirming a readiness to the first privacy computing device 11 is referred to as a project and task interoperating processes.

[0077] In the disclosure, before the project is run, the first privacy computing device 11 may send a project execution preparation request to the second privacy computing device 12, so

that the second privacy computing device 12 verifies whether the sub-algorithm and the data resource required to run the project are currently saved, to ensure the smooth execution of the interconnection and interoperability projects between sub-algorithms.

[0078] In some embodiments, in order to ensure the security of the interoperability between the first sub-algorithm and the second sub-algorithm, the first privacy computing device 11 may send to the second privacy computing device 12 the project execution preparation request based on a configured sixth API (for ease of description, the API for sending the project execution preparation request is referred to as the sixth API). The second privacy computing device 12 may receive the project execution preparation request based on the sixth API. When it is determined that the first identification information is located in the stored identification information for compliance devices, that the target data source with third identification information is stored, and that the components included in the sub-algorithm with the second identification information are completely loaded, the second privacy computing device 12 may send a second confirmation message to the first privacy computing device 11 based on the sixth API. Optionally, the sixth API may be a RESTful API.

[0079] In some embodiments, during the project and task interoperating process, when it is determined that the target data resource with the third identification information is stored, and that the components included in the sub-algorithm with the second identification information are completely loaded, the second privacy computing device 12 may send the second confirmation message confirming a readiness to the first privacy computing device 11. Optionally, the first privacy computing device 11 may receive the second confirmation message, and after receiving the second confirmation message, may perform a process of data plane interoperability with the second privacy computing device 12. In some embodiments, when the first privacy

computing device 11 performs data plane interoperability with any second privacy computing device 12, the first privacy computing device 11 may send a startup request for stating a computing task to the second privacy computing device 12. The second privacy computing device 12 may receive the startup request. After receiving the startup request, the second privacy computing device 12 may run the second sub-algorithm according to the privacy algorithm protocol. Optionally, the second privacy computing device 12 may run the sub-algorithm with the second identification information stored in its data plane based on the target data resource with the third identification information. That is, the second privacy computing device 12 runs the second sub-algorithm. It may be understood that when the first privacy computing device 11 sends a startup request to the second privacy computing device 12 so that the second privacy computing device 12 runs the second sub-algorithm, the first privacy computing device 11 may also run the first sub-algorithm stored in its data plane. That is, the first sub-algorithm and the second sub-algorithm may be run at the same time to perform an interconnected and interoperability computation process. In addition, after the execution of the computing task is completed, the first privacy computing device 11 and the second privacy computing device 12 may respectively obtain corresponding algorithm execution reports.

[0080] If the node interoperability, data resource interoperability, algorithm component interoperability, project and task process interoperability, and so on provided in the above embodiments are referred to as management plane interoperability, the interconnection and interoperability-based computing process that the first sub-algorithm and the second sub-algorithm start to execute is referred to as data plane interoperability. For example, after the management plane interoperability is completed, the first sub-algorithm and the second sub-algorithm may be run at the same time. When performing the interoperability computation

process (data plane interoperability), it is assumed that, when the second privacy computing device 12 where the second sub-algorithm is located sends computing data to the first privacy computing device 11 where the first sub-algorithm is located, a processing instruction to process the computing data based on the first sub-algorithm may be sent at the same time. The processing instruction may carry the token of the second sub-algorithm (for ease of description, a token carried in the processing instruction is referred to as a target token). After the first privacy computing device 11 receives the processing instruction, the gateway of the first privacy computing device 11 may determine the target token carried in the processing instruction. Is the token consistent with the pre-stored reference token of the second sub-algorithm? If consistent, the second computing data may be considered to be sent by a secure compliance device, and it may be considered that the second computing data needs to be recomputed based on the first sub-algorithm stored in the first privacy computing device 11. The first privacy computing device 11 may perform a process of recomputing the second computing data based on the first sub-algorithm. If the target token is inconsistent with the pre-stored reference token of the second sub-algorithm, it may be considered that the second computing data is not sent by a safe and compliance device, and it may be considered that there is no need to compute the second computing data based on the first sub-algorithm. This ensures the security of different sub-algorithms when interconnected and interoperated.

[0081] To facilitate understanding, the following is an example of the interconnection and interoperability process between the first sub-algorithm and the second sub-algorithm provided in the disclosure through a specific embodiment. FIG. 3 shows a schematic diagram of another sub-algorithm interconnection and interoperability process according to some embodiments. Optionally, task collaboration and data control may be performed between the

management plane and the data plane through a policy module. In some embodiments, the first privacy computing device 11 and the second privacy computing device 12 may each include a privacy computing framework base. It may be understood that the structure and principles of running sub-algorithms in the first privacy computing device 11 and the second privacy computing device 12 may be the same. For ease of description, the first privacy computing device 11 is taken as an example for illustration. The policy module of the first privacy computing device 11 may store, the information about the node (also called station) interoperability in the management plane, in the node management module in the privacy computing framework base of the first privacy computing device 11, and may also store, the information about the data resource interoperability in the management plane, in the resource management module in the privacy computing framework base. Information about algorithm component interoperability in the management plane may also be stored in the algorithm management module in the privacy computing framework base. Information about project and task process interoperability in the management plane may also be stored in the project management and process orchestration module in the privacy computing framework base.

[0082] The first privacy computing device 11 may implement the management plane interoperability such as node interoperability, data resource interoperability, algorithm component interoperability, and project and task process interoperability in the above embodiments based on the privacy computing engine of the first sub-algorithm. After the management plane interoperability is completed, the first sub-algorithm and the second sub-algorithm may run at the same time. When performing the interoperability computation process (i.e., data plane interoperability), the first privacy computing device 11 may input authorized data into an algorithm container of the first sub-algorithm, and the second privacy computing

device 12 may input authorized data into the stored algorithm container of the second sub-algorithm. For example, if the first privacy computing device 11 performs corresponding computation on the to-be-processed data based on the first sub-algorithm and obtains the first computing data, and determines that the first computing data needs to be recomputed based on the second sub-algorithm stored in the second privacy computation device 12, the first privacy computing device 11 may determine a proxy interface corresponding to the first sub-algorithm and a proxy interface corresponding to the second sub-algorithm based on the pre-stored correspondence between sub-algorithms and standard proxy interfaces. The communication module in the first privacy computing device 11 may send the first computing data to the proxy interface of the second privacy computing device 12 (i.e., the proxy interface corresponding to the second sub-algorithm) through the proxy interface corresponding to the first sub-algorithm. The communication module in the second privacy computing device 12 may receive the first computing data based on the proxy interface corresponding to the second sub-algorithm. When it is determined that the first computing data needs to be recomputed based on the second sub-algorithm, the second privacy computing device 12 may perform corresponding computation on the first computing data based on the second sub-algorithm, to realize interconnection and interoperability between the first sub-algorithm and the second sub-algorithm.

[0083] Since the disclosure may achieve low coupling between management plane interoperability and data plane interoperability, management plane interoperability and data plane interoperability may be mutually independent, thereby simplifying the implementation of interconnection and interoperability between different privacy computing products (i.e., sub-algorithms). The overall design is conducive to the realization of interconnection and interoperability between privacy algorithm products stored in different privacy computing

devices. In addition, the sub-algorithms in the disclosure may be configured as a container structure, so that the sub-algorithm interconnection and interoperability method provided by the disclosure has good compatibility and operability, and may be accepted by most mainstream privacy computing products.

Embodiment 7:

[0084] Based on similar technical concept, the disclosure provides a privacy computing method, which is applied to the first privacy computing device. FIG. 4 shows a flowchart of a privacy computing method according to some embodiments. As shown in FIG. 4, the method includes the following steps.

[0085] S401: When performing management plane interoperability with any second privacy computing device, send a first query request to the second privacy computing device, where the first query request carries first identification information of the first privacy computing device and second identification information of a to-be-queried sub-algorithm, and the first privacy computing device and each second privacy computing device collaborate on privacy computing tasks based on the management plane interoperability and execute the privacy computing tasks based on data plane interoperability, where the management plane interoperability and the data plane interoperability are mutually independent.

[0086] S402: If information for components included in the sub-algorithm with the second identification information sent by the second privacy computing device is received, send to the second privacy computing device a loading request for loading the components included in the sub-algorithm with the second identification information.

[0087] In some embodiments, sending the first query request to the second privacy computing device includes: sending the first query request to the second privacy computing

device based on a configured first API, and sending the loading request to the second privacy computing device for loading the components included in the sub-algorithm with the second identification information includes: sending the loading request to the second privacy computing device based on a configured second API.

[0088] In some embodiments, before sending the first query request to the second privacy computing device, the method further includes: sending a cooperation request for sub-algorithm interoperability to the second privacy computing device, where the cooperation request carries the first identification information of the first privacy computing device.

[0089] In some embodiments, sending the cooperation request for sub-algorithm interoperability to the second privacy computing device includes: sending the cooperation request for sub-algorithm interoperability to the second privacy computing device based on a configured third API.

[0090] In some embodiments, the method further includes: sending a second query request to the second privacy computing device, where the second query request carries the first identification information of the first privacy computing device and third identification information for a to-be-queried data resource.

[0091] In some embodiments, sending the second query request to the second privacy computing device includes: sending the second query request to the second privacy computing device based on a configured fourth API.

[0092] In some embodiments, after sending the second query request to the second privacy computing device, the method further includes: sending an authorization request for using the data resource with the third identification information to the second privacy computing device, where the authorization request carries the first identification information of the first

privacy computing device.

[0093] In some embodiments, sending the authorization request for using the data resource with the third identification information to the second privacy computing device includes: sending the authorization request to the second privacy computing device based on a configured fifth API.

[0094] In some embodiments, the method further includes: sending a project execution preparation request to the second privacy computing device, where the project execution preparation request carries the first identification information of the first privacy computing device, second identification information of a sub-algorithm required for a to-be-run project, and third identification information for a target data resource required for the to-be-run project.

[0095] In some embodiments, sending the project execution preparation request to the second privacy computing device includes: sending the project execution preparation request to the second privacy computing device based on a configured sixth API.

[0096] In some embodiments, the method further includes: when performing data plane interoperability with any second privacy computing device, the first privacy computing device receives a second confirmation message sent by the second privacy computing device, and sends a startup request for starting a computing task to the second privacy computing device.

[0097] Based on similar technical concept, the disclosure provides a privacy computing device, which is applied to the first privacy computing device. FIG. 5 shows a schematic diagram of a privacy computing device according to some embodiments. The device includes: a first transmission module 501, configured to send a first query request to a second privacy computing device when performing management plane interoperability with any second privacy computing device, where the first query request carries the first identification information of the first

privacy computing device and the second identification information of a to-be-queried sub-algorithm, the first privacy computing device and each second privacy computing device collaborate on privacy computing tasks based on the management plane interoperability and perform the privacy computing tasks based on data plane interoperability, where the management plane interoperability and the data plane interoperability are mutually independent; and a second transmission module 502, configured to, upon receiving information for components included in the sub-algorithm with the second identification information sent by the second privacy computing device, send a loading request for loading components included in the sub-algorithm with the second identification information to the second privacy computing device.

[0098] In some embodiments, the first transmission module 501 is specifically configured to send the first query request to the second privacy computing device based on a configured first API. The second transmission module 502 is specifically configured to send the loading request to the second privacy computing device based on a configured second API.

[0099] In some embodiments, the first transmission module 501 is further configured to send a cooperation request for sub-algorithm interoperability to the second privacy computing device, where the cooperation request carries the first identification information of the first privacy computing device.

[00100] In some embodiments, the first transmission module 501 is specifically configured to send the cooperation request for sub-algorithm interoperability to the second privacy computing device based on a configured third API.

[00101] In some embodiments, the first transmission module 501 is further configured to send a second query request to the second privacy computing device, where the second query

request carries the first identification information of the first privacy computing device and third identification information for a to-be-queried data resource.

[00102] In some embodiments, the first transmission module 501 is specifically configured to send the second query request to the second privacy computing device based on a configured fourth API.

[00103] In some embodiments, the first transmission module 501 is further configured to send an authorization request for using the data resource with the third identification information to the second privacy computing device, where the authorization request carries the first identification information of the first privacy computing device.

[00104] In some embodiments, the first transmission module 501 is specifically configured to send the authorization request to the second privacy computing device based on a configured fifth API.

[00105] In some embodiments, the first transmission module 501 is further configured to send a project execution preparation request to the second privacy computing device, where the project execution preparation request carries the first identification information of the first privacy computing device, second identification information of a sub-algorithm required for a to-be-run project, and third identification information of a target data resource required for the to-be-run project.

[00106] In some embodiments, the first transmission module 501 is specifically configured to send the project execution preparation request to the second privacy computing device based on a configured sixth API.

[00107] In some embodiments, the first transmission module 501 is further configured to, when performing the data plane interoperability with any second privacy computing device, and

when the first privacy computing device receives a second confirmation message sent by the second privacy computing device, send a startup request to start a computing task to the second privacy computing device.

Embodiment 8:

[00108] Based on similar technical concept, the disclosure provides a privacy computing method, which is applied to any second privacy computing device. FIG. 6 shows a flowchart of another privacy computing method according to some embodiments. As shown in FIG. 6, the method includes the following steps.

[00109] S601: When performing management plane interoperability with a first privacy computing device, receive a first query request sent by the first privacy computing device, where the first query request carries first identification information of the first privacy computing device and second identification information of a to-be-queried sub-algorithm, and the first privacy computing device and each second privacy computing device collaborate on privacy computing tasks based on the management plane interoperability and perform the privacy computing tasks based on data plane interoperability, where the management plane interoperability and the data plane interoperability are mutually independent.

[00110] S602: When it is determined that the first identification information is located in stored identification information for compliance devices, send stored information for components included in the sub-algorithm with the second identification information to the first privacy computing device.

[00111] S603: When a loading request sent by the first privacy computing device is received, load the components included in the sub-algorithm with the second identification information, and after the loading is successful, send a loading success message to the first

privacy computing device.

[00112] In some embodiments, receiving the first query request sent by the first privacy computing device includes: receiving the first query request based on a first API; sending stored information for components included in the sub-algorithm with the second identification information to the first privacy computing device includes: sending the stored information for components included in the sub-algorithm with the second identification information to the first privacy computing device based on the first API; receiving the loading request sent by the first privacy computing device includes: receive the loading request based on a second API; and sending a loading success message to the first privacy computing device includes: sending the loading success message to the first privacy computing device based on the second API.

[00113] In some embodiments, before receiving the first query request sent by the first privacy computing device, the method further includes: receiving a cooperation request sent by the first privacy computing device, where the cooperation request carries the first identification information of the first privacy computing device; and when it is determined that the first identification information is located in the stored identification information for compliance devices, send a first confirmation message for agreeing to cooperate to the first privacy computing device.

[00114] In some embodiments, receiving the cooperation request sent by the first privacy computing device includes: receiving the cooperation request based on a third API; and sending the first confirmation message for agreeing to cooperate to the first privacy computing device includes: sending the first confirmation message based on the third API.

[00115] In some embodiments, the method further includes: receiving a second query request sent by the first privacy computing device, where the second query request carries the

first identification information of the first privacy computing device and third identification information of a to-be-queried data resource; and when it is determined that the first identification information is located in the stored identification information for compliance devices, send stored information for the data resource with the third identification information to the first privacy computing device.

[00116] In some embodiments, receiving the second query request sent by the first privacy computing device includes: receiving the second query request based on a fourth API; and sending the stored information for the data resource with the third identification information to the first privacy computing device includes: sending the information for the data resource with the third identification information to the first privacy computing device based on the fourth API.

[00117] In some embodiments, after receiving the second query request sent by the first privacy computing device, the method further includes: receiving an authorization request sent by the first privacy computing device, where the authorization request carries the first identification information of the first privacy computing device; and when it is determined that the first identification information is located in the stored identification information for compliance devices, send to the first privacy computing device a granted authorization message for authorized use of the data resource with the third identification information.

[00118] In some embodiments, receiving the authorization request sent by the first privacy computing device includes: receiving the authorization request based on a fifth API; and sending to the first privacy computing device the granted authorization message for authorized use of the data resource with the third identification information includes: sending the granted authorization message to the first privacy computing device based on the fifth API.

[00119] In some embodiments, the method further includes: receiving a project execution

preparation request sent by the first privacy computing device, where the project execution preparation request carries the first identification information of the first privacy computing device, second identification information of a sub-algorithm required for a to-be-run project, and third identification information of a target data resource required for the to-be-run project; and when it is determined that the first identification information is located in the stored identification information for compliance devices, and when it is determined that the target data resource with the third identification information is saved, and that the components included in the sub-algorithm with the second identification information are completely loaded, sending a second confirmation message confirming a readiness to the first privacy computing device.

[00120] In some embodiments, receiving the project execution preparation request sent by the first privacy computing device includes: receiving the project execution preparation request based on a sixth API; and sending the second confirmation message confirming a readiness to the first privacy computing device includes: sending the second confirmation message to the first privacy computing device based on the sixth API.

[00121] In some embodiments, the method further includes: when performing the data plane interoperability with the first privacy computing device, receiving a startup request sent by the first privacy computing device, and running the sub-algorithm with the second identification information based on the target data resource with the third identification information.

[00122] Based on similar technical concept, the disclosure provides a privacy computing device, which is applied to a second privacy computing device. FIG. 7 shows a schematic diagram of another privacy computing device according to some embodiments. The device includes: a first receiving module 701, configured to receive a first query request sent by a first privacy computing device when performing management plane interoperability with the first

privacy computing device, where the first query request carries the first identification information of the first privacy computing device and second identification information of a to-be-queried sub-algorithm, and the first privacy computing device and each second privacy computing device collaborate on privacy computing tasks based on the management plane interoperability and perform the privacy computing tasks based on data plane interoperability, where the management plane interoperability and the data plane interoperability are mutually independent; and a third transmission module 702, configured to send stored information for components included in the sub-algorithm with the second identification information to the first privacy computing device when it is determined that the first identification information is located in the stored identification information for compliance devices; and a loading module 703, configured to load the components included in the sub-algorithm with the second identification information upon receiving a loading request sent by the first privacy computing device, and after the loading is successful, send a loading success message to the first privacy computing device.

[00123] In some embodiments, the first receiving module 701 is specifically configured to receive the first query request based on a first API; the third transmission module 702 is specifically configured to send to the first privacy computing device the stored information for components included in the sub-algorithm with the second identification information based on the first API; and the loading module 703 is specifically configured to receive the loading request based on a second API, and send the loading success message to the first privacy computing device based on the second API.

[00124] In some embodiments, the first receiving module 701 is further configured to receive a cooperation request sent by the first privacy computing device, where the cooperation

request carries the first identification information of the first privacy computing device, and when it is determined that the first identification information is located in the stored identification information for compliance devices, send a first confirmation message for agreeing to cooperate to the first privacy computing device.

[00125] In some embodiments, the first receiving module 701 is specifically configured to receive the cooperation request based on a third API, and send the first confirmation message based on the third API.

[00126] In some embodiments, the first receiving module 701 is further configured to receive a second query request sent by the first privacy computing device, where the second query request carries the first identification information of the first privacy computing device and third identification information of a to-be-queried data resource; when it is determined that the first identification information is located in the stored identification information for compliance devices, send stored information for the data resource with the third identification information to the first privacy computing device.

[00127] In some embodiments, the first receiving module 701 is specifically configured to receive the second query request based on a fourth API, and send the information for the data resource with the third identification information to the first privacy computing device based on the fourth API.

[00128] In some embodiments, the first receiving module 701 is further configured to receive an authorization request sent by the first privacy computing device, where the authorization request carries the first identification information of the first privacy computing device; and when it is determined that the first identification information is located in the stored identification information for compliance devices, send a granted authorization message for

authorized use of the data resource with the third identification information to the first privacy computing device.

[00129] In some embodiments, the first receiving module 701 is specifically configured to receive the authorization request based on a fifth API, and send the granted authorization message to the first privacy computing device based on the fifth API.

[00130] In some embodiments, the first receiving module 701 is further configured to receive a project execution preparation request sent by the first privacy computing device, where the project execution preparation request carries the first identification information of the first privacy computing device, second identification information of a sub-algorithm required for a to-be-run project, and third identification information of a target data resource required for the to-be-run project; and when it is determined that the first identification information is located in the stored identification information for compliance devices, and when it is determined that the target data resource with the third identification information is saved, and that the components included in the sub-algorithm with the second identification information are completely loaded, send a second confirmation message confirming a readiness to the first privacy computing device.

[00131] In some embodiments, the first receiving module 701 is specifically configured to receive the project execution preparation request based on a sixth API, and send the second confirmation message to the first privacy computing device based on the sixth API.

[00132] In some embodiments, the first receiving module 701 is further configured to receive a startup request sent by the first privacy computing device when performing the data plane interoperability with the first privacy computing device, and run the sub-algorithm with the second identification information based on the target data resource with the third identification

information.

Embodiment 9:

[00133] Based on similar technical concept, the disclosure also provides an electronic device. FIG. 8 shows a schematic structural diagram of an electronic device according to some embodiments. As shown in FIG. 8, the electronic device includes: a processor 81, a communication interface 82, a memory 83, and a communication bus 84, where the processor 81, communication interface 82, and memory 83 complete communication with each other through the communication bus 84.

[00134] In some embodiments, the memory 83 stores a computer program. When the program is executed by the processor 81, the processor 81 performs the following steps.

[00135] When performing management plane interoperability with any second privacy computing device, send a first query request to the second privacy computing device, where the first query request carries first identification information of a first privacy computing device and second identification information for a to-be-queried sub-algorithm, and the first privacy computing device and each second privacy computing device collaborate on privacy computing tasks based on the management plane interoperability and perform the privacy computing tasks based on data plane interoperability, where the management plane interoperability and the data plane interoperability are mutually independent.

[00136] If information for components included in the sub-algorithm with the second identification information sent by the second privacy computing device is received, send a load request for loading components included in the sub-algorithm with the second identification information to the second privacy computing device.

[00137] In some embodiments, the processor 81 is specifically configured to send the first

query request to the second privacy computing device based on a configured first API, where sending a loading request to the second privacy computing device for loading the components included in the sub-algorithm with the second identification information includes: sending the loading request to the second privacy computing device based on a configured second API.

[00138] In some embodiments, the processor 81 is further configured to send a cooperation request for sub-algorithm interoperability to the second privacy computing device before sending the first query request to the second privacy computing device, where the cooperation request carries the first identification information of the first privacy computing device.

[00139] In some embodiments, the processor 81 is specifically configured to send the cooperation request for sub-algorithm interoperability to the second privacy computing device based on a configured third API.

[00140] In some embodiments, the processor 81 is further configured to send a second query request to the second privacy computing device, where the second query request carries the first identification information of the first privacy computing device and third identification information of a to-be-queried data resource.

[00141] In some embodiments, the processor 81 is specifically configured to send the second query request to the second privacy computing device based on a configured fourth API.

[00142] In some embodiments, the processor 81 is further configured to, after sending the second query request to the second privacy computing device, send an authorization request for using a data resource with third identification information to the second privacy computing device, where the authorization request carries the first identification information of the first privacy computing device.

[00143] In some embodiments, the processor 81 is specifically configured to send the authorization request to the second privacy computing device based on a configured fifth API.

[00144] In some embodiments, the processor 81 is further configured to send a project execution preparation request to the second privacy computing device, where the project execution preparation request carries the first identification information of the first privacy computing device, second identification information of a sub-algorithm required for a to-be-run project, and third identification information of a target data resource required for the to-be-run project.

[00145] In some embodiments, the processor 81 is specifically configured to send the project execution preparation request to the second privacy computing device based on a configured sixth API.

[00146] In some embodiments, the processor 81 is further configured to: when performing the data plane interoperability with any second privacy computing device, and when the first privacy computing device receives a second confirmation message sent by the second privacy computing device, send a startup request to start a computing task to the second privacy computing device.

[00147] In addition, in some embodiments, the memory 83 stores a computer program. When the program is executed by the processor 81, the processor 81 performs the following processes.

[00148] When performing management plane interoperability with a first privacy computing device, receive a first query request sent by the first privacy computing device, where the first query request carries first identification information of the first privacy computing device and second identification information for a to-be-queried sub-algorithm, and the first

privacy computing device and each second privacy computing device collaborate on privacy computing tasks based on the management plane interoperability and execute the privacy computing tasks based on data plane interoperability, where the management plane interoperability and the data plane interoperability are mutually independent.

[00149] When it is determined that the first identification information is located in the stored identification information for compliance devices, send stored information for components included in the sub-algorithm with the second identification information to the first privacy computing device.

[00150] If a loading request sent by the first privacy computing device is received, the components included in the sub-algorithm with the second identification information are completely loaded, and after the loading is successful, send a loading success message to the first privacy computing device.

[00151] In some embodiments, the processor 81 is specifically configured to receive the first query request based on a first API, send stored information for components included in the sub-algorithm with the second identification information to the first privacy computing device based on the first API; receive the loading request based on a second API, and send the loading success message to the first privacy computing device based on the second API.

[00152] In some embodiments, the processor 81 is further configured to receive a cooperation request sent by the first privacy computing device before receiving the first query request sent by the first privacy computing device, where the cooperation request carries the first identification information of the first privacy computing device. When it is determined that the first identification information is located in the stored identification information for compliance devices, send a first confirmation message for agreeing to cooperate to the first privacy

computing device.

[00153] In some embodiments, the processor 81 is specifically configured to receive the cooperation request based on a third API; and send the first confirmation message based on the third API.

[00154] In some embodiments, the processor 81 is further configured to receive a second query request sent by the first privacy computing device, where the second query request carries the first identification information of the first privacy computing device and third identification information of a to-be-queried data resource. When it is determined that the first identification information is located in the stored identification information for compliance devices, send stored information for the data resource with the third identification information to the first privacy computing device.

[00155] In some embodiments, the processor 81 is specifically configured to receive the second query request based on a fourth API, where sending the stored information for the data resource with the third identification information to the first privacy computing device includes: sending the information for the data resource with the third identification information to the first privacy computing device based on the fourth API.

[00156] In some embodiments, the processor 81 is further configured to receive an authorization request sent by the first privacy computing device after receiving the second query request sent by the first privacy computing device, where the authorization request carries the first identification information of the first privacy computing device. When it is determined that the first identification information is located in the stored identification information for compliance devices, send to the first privacy computing device a granted authorization message for authorized use of the data resource with the third identification information.

[00157] In some embodiments, the processor 81 is specifically configured to receive the authorization request based on a fifth API; and send the granted authorization message to the first privacy computing device based on the fifth API.

[00158] In some embodiments, the processor 81 is further configured to receive a project execution preparation request sent by the first privacy computing device, where the project execution preparation request carries the first identification information of the first privacy computing device, second identification information of a sub-algorithm required for a to-be-run project, and third identification information of a target data resource required for the to-be-run project. When it is determined that the first identification information is located in the stored identification information for compliance devices, and when it is determined that the target data resource with the third identification information is saved, and that the components included in the sub-algorithm with the second identification information are completely loaded, send a second confirmation message confirming a readiness to the first privacy computing device.

[00159] In some embodiments, the processor 81 is specifically configured to receive the project execution preparation request based on a sixth API; and send the second confirmation message to the first privacy computing device based on the sixth API.

[00160] In some embodiments, the processor 81 is further configured to receive a startup request sent by the first privacy computing device when performing the data plane interoperability with the first privacy computing device, and run the sub-algorithm with the second identification information based on the target data resource with the third identification information.

[00161] Since the problem-solving principle of the above electronic device is similar to that of the privacy computing method, the implementation of the electronic device may refer to

the implementation of the privacy computing method, details of which will not be repeated here.

[00162] The communication bus mentioned in the electronic device may be a peripheral component interconnect (PCI) bus or an extended industry standard architecture (EISA) bus, etc. The communication bus may be divided into address bus, data bus, control bus, etc. For ease of presentation, just one thick line is used in the figure, but it does not mean that there is just one bus or one type of bus.

[00163] The communication interface 82 is used for communication between the electronic device and other devices.

[00164] The memory may include random access memory (RAM) or non-volatile memory (NVM), such as at least one disk memory. Optionally, the memory may also be at least one storage device located remotely from the processor.

[00165] The processor may be a general-purpose processor, including a central processing unit, a network processor (NP), etc. The processor may also be a digital instruction processor (DSP), an application-specific integrated circuit, a field programmable gate array, or other programmable logic devices, discrete gate or transistor logic devices, discrete hardware components, etc.

[00166] Based on similar technical concept, embodiments of the disclosure provide a computer-readable storage medium. The computer-readable storage medium stores a computer program that may be executed by an electronic device. When the program is run on the electronic device, the electronic device is caused to execute the following processes.

[00167] When performing management plane interoperability with any second privacy computing device, send a first query request to the second privacy computing device, where the first query request carries first identification information of the first privacy computing device

and second identification information for a to-be-queried sub-algorithm, and the first privacy computing device and each second privacy computing device collaborate on privacy computing tasks based on the management plane interoperability and perform the privacy computing tasks based on data plane interoperability, where the management plane interoperability and the data plane interoperability are mutually independent.

[00168] If information for components included in the sub-algorithm with the second identification information sent by the second privacy computing device is received, send to the second privacy computing device a load request for loading components included in the sub-algorithm with the second identification information.

[00169] In some embodiments, sending the first query request to the second privacy computing device includes: sending the first query request to the second privacy computing device based on a configured first API; and sending the loading request to the second privacy computing device for loading the components included in the sub-algorithm with the second identification information includes: sending the loading request to the second privacy computing device based on a configured second API.

[00170] In some embodiments, before sending the first query request to the second privacy computing device, the method further includes: sending a cooperation request for sub-algorithm interoperability to the second privacy computing device, where the cooperation request carries the first identification information of the first privacy computing device.

[00171] In some embodiments, sending the cooperation request for sub-algorithm interoperability to the second privacy computing device includes: sending the cooperation request for sub-algorithm interoperability to the second privacy computing device based on a configured third API.

[00172] In some embodiments, the method further includes: sending a second query request to the second privacy computing device, where the second query request carries the first identification information of the first privacy computing device and the third identification information of a to-be-queried data resource.

[00173] In some embodiments, sending the second query request to the second privacy computing device includes: sending the second query request to the second privacy computing device based on a configured fourth API.

[00174] In some embodiments, after sending the second query request to the second privacy computing device, the method further includes: sending an authorization request for using the data resource with the third identification information to the second privacy computing device, where the authorization request carries the first identification information of the first privacy computing device.

[00175] In some embodiments, sending the authorization request for using the data resource with the third identification information to the second privacy computing device includes: sending the authorization request to the second privacy computing device based on a configured fifth API.

[00176] In some embodiments, the method further includes: sending a project execution preparation request to the second privacy computing device, where the project execution preparation request carries the first identification information of the first privacy computing device, second identification information for a sub-algorithm required for a to-be-run project, and third identification information for a target data resource required for the to-be-run project.

[00177] In some embodiments, sending the project execution preparation request to the second privacy computing device includes: sending the project execution preparation request to

the second privacy computing device based on a configured sixth API.

[00178] In some embodiments, the method further includes: when performing the data plane interoperability with any second privacy computing device, the first privacy computing device receives the second confirmation message sent by the second privacy computing device, and sends a startup request for starting a computing task to the second privacy computing device.

[00179] In addition, when the program is run on an electronic device, the electronic device is caused to execute the following processes.

[00180] When performing management plane interoperability with a first privacy computing device, receive a first query request sent by the first privacy computing device, where the first query request carries first identification information of the first privacy computing device and second identification information for a to-be-queried sub-algorithm, and the first privacy computing device and each second privacy computing device collaborate on privacy computing tasks based on the management plane interoperability and execute the privacy computing tasks based on data plane interoperability, where the management plane interoperability and the data plane interoperability are mutually independent.

[00181] When it is determined that the first identification information is located in the stored identification information for compliance devices, send stored information for components included in the sub-algorithm with the second identification information to the first privacy computing device.

[00182] If a loading request sent by the first privacy computing device is received, the components included in the sub-algorithm with the second identification information are completely loaded, and after the loading is successful, send a loading success message to the first privacy computing device.

[00183] In some embodiments, receiving the first query request sent by the first privacy computing device includes: receiving the first query request based on a first API; sending the stored information for components included in the sub-algorithm with the second identification information to the first privacy computing device includes: sending the stored information for components included in the sub-algorithm with the second identification information to the first privacy computing device based on the first API; receiving the loading request sent by the first privacy computing device includes: receiving the loading request based on a second API; and sending a loading success message to the first privacy computing device includes: sending the loading success message to the first privacy computing device based on the second API.

[00184] In some embodiments, before receiving the first query request sent by the first privacy computing device, the method further includes: receiving a cooperation request sent by the first privacy computing device, where the cooperation request carries first identification information of the first privacy computing device; and when it is determined that the first identification information is located in the stored identification information for compliance devices, sending a first confirmation message for agreeing to cooperate to the first privacy computing device.

[00185] In some embodiments, receiving the cooperation request sent by the first privacy computing device includes: receiving the cooperation request based on a third API; and sending to the first privacy computing device the first confirmation message for agreeing to cooperate includes: sending the first confirmation message based on the third API.

[00186] In some embodiments, the method further includes: receiving a second query request sent by the first privacy computing device, where the second query request carries the first identification information of the first privacy computing device and third identification

information of a to-be-queried data resource; and when it is determined that the first identification information is located in the stored identification information for compliance devices, sending stored information for the data resource with the third identification information to the first privacy computing device.

[00187] In some embodiments, receiving the second query request sent by the first privacy computing device includes: receiving the second query request based on a fourth API; and sending to the first privacy computing device the stored information for the data resource information with the third identification information includes: sending to the first privacy computing device the stored information for the data resource information with the third identification information based on the fourth API.

[00188] In some embodiments, after receiving the second query request sent by the first privacy computing device, the method further includes: receiving an authorization request sent by the first privacy computing device, where the authorization request carries the first identification information of the first privacy computing device; and when it is determined that the first identification information is located in the stored identification information for compliance devices, sending a granted authorization message for authorized use of the data resource with the third identification information to the first privacy computing device.

[00189] In some embodiments, receiving the authorization request sent by the first privacy computing device includes: receiving the authorization request based on a fifth API; and sending to the first privacy computing device the granted authorization message for authorized use of the data resource with the third identification information includes: sending the granted authorization message to the first privacy computing device based on the fifth API.

[00190] In some embodiments, the method further includes: receiving a project execution

preparation request sent by the first privacy computing device, where the project execution preparation request carries the first identification information of the first privacy computing device, second identification information of a sub-algorithm required for a to-be-run project, and third identification information of a target data resource required for the to-be-run project; and when it is determined that the first identification information is located in the stored identification information for compliance devices, and when it is determined that the target data resource with the third identification information is saved, and that the components included in the sub-algorithm with the second identification information are completely loaded, send a second confirmation message confirming a readiness to the first privacy computing device.

[00191] In some embodiments, receiving the project execution preparation request sent by the first privacy computing device includes: receiving the project execution preparation request based on a sixth API; and sending the second confirmation message confirming a readiness to the first privacy computing device includes: sending the second confirmation message to the first privacy computing device based on the sixth API.

[00192] In some embodiments, the method further includes: when performing data plane interoperability with the first privacy computing device, receiving a startup request sent by the first privacy computing device, and run the sub-algorithm with the second identification information based on the target data resource with the third identification information.

[00193] Since the problem-solving principle of the above computer-readable storage medium is similar to the privacy computing method, the implementation of the computer-readable storage medium may refer to the implementation of the privacy computing method, details of which will not be repeated here.

[00194] The aforementioned computer-readable storage media may be any available

media or data storage devices that may be accessed by the processor in the electronic device, including but not limited to magnetic memories such as floppy disks, hard disks, magnetic tapes, magneto-optical (MO) disks, etc., and optical memories such as CD, DVD, blue-ray disc (BD), holographic versatile disc (HVD), etc., as well as semiconductor memories such as ROM, EPROM, EEPROM, non-volatile memory (NAND FLASH), solid state drive (SSD), etc.

[00195] Based on similar technical concept and on the basis of the above embodiments, the disclosure provides a computer program product. The computer program product includes: computer program code. When the computer program code is run on a computer, the computer perform the steps of the privacy computation method as described elsewhere herein.

[00196] Those skilled in the art will understand that embodiments of the disclosure may be provided as methods, systems, or computer program products. Accordingly, the disclosure may take the form of an entirely hardware embodiment, an entirely software embodiment, or an embodiment that combines software and hardware aspects. Furthermore, the disclosure may take the form of a computer program product embodied on one or more computer-usable storage media (including, but not limited to, disk memory, CD-ROM, optical storage, etc.) having computer-usable program code embodied therein.

[00197] The disclosure is described with reference to flowchart illustrations and/or block diagrams of methods, apparatus (systems), and computer program products according to the disclosure. It will be understood that each process and/or block in the flowchart illustrations and/or block diagrams, and combinations of processes and/or blocks in the flowchart illustrations and/or block diagrams, may be implemented by computer program instructions. These computer program instructions may be provided to a processor of a general purpose computer, special purpose computer, embedded processor, or another programmable data processing device to

produce a machine, such that the instructions executed by the processor of the computer or other programmable data processing device produce a device for realizing the functions specified in one process or multiple processes of the flowchart and/or one block or multiple blocks of the block diagram.

[00198] These computer program instructions may also be stored in a computer-readable memory that causes a computer or other programmable data processing apparatus to operate in a particular manner, such that the instructions stored in the computer-readable memory produce an article of manufacture including the instruction means, where the instructions means implements the functions specified in a process or processes of the flowchart and/or a block or blocks of the block diagram.

[00199] These computer program instructions may also be loaded onto a computer or other programmable data processing device, causing a series of operating steps to be performed on the computer or other programmable device to produce computer-implemented processing, thereby executing on the computer or other programmable device. Instructions provide steps for implementing the functions specified in a process or processes of a flowchart diagram and/or a block or blocks of a block diagram. Apparently, those skilled in the art may make various changes and modifications to the present disclosure without departing from the spirit and scope of the present disclosure. Accordingly, if these modifications and variations of the present disclosure fall within the scope of the claims of the present disclosure and equivalent technologies, the present disclosure is also intended to include these modifications and variations.

What is claimed is:

1. A privacy computing system, comprising: a first privacy computing device and at least one second privacy computing device, wherein:

the first privacy computing device and a second privacy computing device collaborate on privacy computing tasks based on management plane interoperability and execute the privacy computing tasks based on data plane interoperability, wherein the management plane interoperability and the data plane interoperability are mutually independent;

for the second privacy computing device, when the first privacy computing device and the second privacy computing device perform the management plane interoperability, the first privacy computing device is configured to send a first query request to the second privacy computing device, wherein the first query request carries first identification information of the first privacy computing device and second identification information of a to-be-queried sub-algorithm;

the second privacy computing device is configured to receive the first query request, and when it is determined that the first identification information is located in stored identification information for compliance devices, send stored information for components included in the sub-algorithm with the second identification information to the first privacy computing device;

the first privacy computing device is further configured to receive the information for components included in the sub-algorithm with the second identification information, and send, to the second privacy computing device, a loading request for loading the components included in the sub-algorithm with the second identification information; and

the second privacy computing device is further configured to receive the loading request, load the components included in the sub-algorithm with the second identification information,

and after the loading is successful, send a loading success message to the first privacy computing device.

2. The system according to claim 1, wherein:

the first privacy computing device is further configured to send the first query request to the second privacy computing device based on a configured first application programming interface (API);

the second privacy computing device is further configured to receive the first query request based on the first API, and send the stored information for components included in the sub-algorithm with the second identification information to the first privacy computing device based on the first API;

the first privacy computing device is further configured to receive, based on the first API, the information for components included in the sub-algorithm with the second identification information, and send the loading request to the second privacy computing device based on a configured second API; and

the second privacy computing device is further configured to receive the loading request based on the second API, and send the loading success message to the first privacy computing device based on the second API.

3. The system according to claim 1, wherein:

the first privacy computing device is further configured to send a cooperation request for privacy algorithm interoperability to the second privacy computing device, wherein the

cooperation request carries the first identification information of the first privacy computing device; and

the second privacy computing device is further configured to receive the cooperation request, and when it is determined that the first identification information is located in the stored identification information for compliance devices, send to the first privacy computing device a first confirmation message for agreeing to cooperate.

4. The system according to claim 3, wherein:

the first privacy computing device is further configured to send the cooperation request for privacy algorithm interoperability to the second privacy computing device based on a configured third API; and

the second privacy computing device is further configured to receive the cooperation request and send the first confirmation message based on the third API.

5. The system according to any one of claims 1-4, wherein:

the first privacy computing device is further configured to send a second query request to the second privacy computing device, wherein the second query request carries the first identification information of the first privacy computing device and third identification information of a to-be-queried data resource; and

the second privacy computing device is further configured to receive the second query request, and when it is determined that the first identification information is located in the stored identification information for compliance devices, send to the first privacy computing device stored information for the data source with the third identification information.

6. The system according to claim 5, wherein:

the first privacy computing device is further configured to send the second query request to the second privacy computing device based on a configured fourth API; and

the second privacy computing device is further configured to receive the second query request and send the information for the data resource with the third identification information based on the fourth API.

7. The system according to claim 5, wherein:

the first privacy computing device is further configured to send to the second privacy computing device an authorization request for using the data resource with the third identification information, wherein the authorization request carries the first identification information of the first privacy computing device; and

the second privacy computing device is further configured to receive the authorization request, and when it is determined that the first identification information is located in the stored identification information for compliance devices, send to the first privacy computing device a granted authorization message for authorized use of the data resource with the third identification information.

8. The system according to claim 7, wherein:

the first privacy computing device is further configured to send the authorization request to the second privacy computing device based on a configured fifth API; and

the second privacy computing device is further configured to receive the authorization request and send the granted authorization message based on the fifth API.

9. The system according to claim 5, wherein:

the first privacy computing device is further configured to send a project execution preparation request to the second privacy computing device, wherein the project execution preparation request carries the first identification information of the first privacy computing device, second identification information of a sub-algorithm required for a to-be-run project, and third identification information of a target data resource required for the to-be-run project; and

the second privacy computing device is further configured to receive the project execution preparation request, and when it is determined that the first identification information is located in the stored identification information for compliance devices, and when it is determined that the target data resource of the third identification information is stored, and when it is determined that the components included in the sub-algorithm with the second identification information are completely loaded, sent to the first privacy computing device a second confirmation message confirming a readiness.

10. The system according to claim 9, wherein:

for the second privacy computing device, when the first privacy computing device and the second privacy computing device perform the data plane interoperability, the first privacy computing device is further configured to receive the second confirmation message, and send to the second privacy computing device a startup request to start a computing task; and

the second privacy computing device is further configured to receive the startup request, and run the sub-algorithm with the second identification information based on the target data resource with the third identification information.

11. The system according to claim 9, wherein:

the first privacy computing device is further configured to send the project execution preparation request to the second privacy computing device based on a configured sixth API; and

the second privacy computing device is further configured to receive the project execution preparation request and send the second confirmation message to the first privacy computing device based on the sixth API.

12. The system according to claim 1, wherein the sub-algorithm is an algorithm with a container structure.

13. A privacy computing method, applied to a first privacy computing device, the method comprising:

when performing management plane interoperability with a second privacy computing device, sending a first query request to the second privacy computing device, wherein the first query request carries first identification information of the first privacy computing device and second identification information of a to-be-queried sub-algorithm, and the first privacy computing device and the second privacy computing device respectively collaborate on privacy computing tasks based on the management plane interoperability and perform the privacy

computing tasks based on data plane interoperability, wherein the management plane interoperability and the data plane interoperability are mutually independent; and

when information for components included in the sub-algorithm with the second identification information sent by the second privacy computing device is received, sending to the second privacy computing device a loading request for loading the components included in the sub-algorithm with the second identification information.

14. The method according to claim 13, wherein:

sending the first query request to the second privacy computing device includes sending the first query request to the second privacy computing device based on a configured first API; and

sending the loading request to the second privacy computing device for loading the components included in the sub-algorithm with the second identification information includes sending the loading request to the second privacy computing device based on a configured second API.

15. The method according to claim 13, wherein, before sending the first query request to the second privacy computing device, the method further comprises:

sending a cooperation request for privacy algorithm interoperability to the second privacy computing device, wherein the cooperation request carries the first identification information of the first privacy computing device.

16. The method according to claim 15, wherein sending the cooperation request for privacy algorithm interoperability to the second privacy computing device comprises:

sending the cooperation request for privacy algorithm interoperability to the second privacy computing device based on a configured third API.

17. The method according to any one of claims 13-16, further comprising:

sending a second query request to the second privacy computing device, wherein the second query request carries the first identification information of the first privacy computing device and third identification information of a to-be-queried data resource.

18. The method according to claim 17, wherein sending the second query request to the second privacy computing device comprises:

sending the second query request to the second privacy computing device based on a configured fourth API.

19. The method according to claim 17, wherein, after sending the second query request to the second privacy computing device, the method further comprises:

sending to the second privacy computing device an authorization request for using the data resource with the third identification information, wherein the authorization request carries the first identification information of the first privacy computing device.

20. The method according to claim 19, wherein sending to the second privacy computing device the authorization request for using the data resource with the third identification information comprises:

 sending the authorization request to the second privacy computing device based on a configured fifth API.

21. The method according to claim 17, further comprising:

 sending a project execution preparation request to the second privacy computing device, wherein the project execution preparation request carries the first identification information of the first privacy computing device, second identification information of a sub-algorithm required for a to-be-run project, and third identification information of a target data resource required for the to-be-run project.

22. The method according to claim 21, wherein sending the project execution preparation request to the second privacy computing device comprises:

 sending the project execution preparation request to the second privacy computing device based on a configured sixth API.

23. The method according to claim 21, further comprising:

 when performing the data plane interoperability with the second privacy computing device, the first privacy computing device receiving a second confirmation message sent by the second privacy computing device, and sending to the second privacy computing device a startup request to start a computing task.

24. A privacy computing method, applied to a second privacy computing device, the method comprising:

when performing management plane interoperability with a first privacy computing device, receiving a first query request sent by the first privacy computing device, wherein the first query request carries first identification information of the first privacy computing device and second identification information of a to-be-queried sub-algorithm, and the first privacy computing device and the second privacy computing device collaborate on privacy computing tasks based on the management plane interoperability and execute the privacy computing tasks based on data plane interoperability, wherein the management plane interoperability and the data plane interoperability are mutually independent;

when it is determined that the first identification information is located in stored identification information for compliance devices, sending to the first privacy computing device stored information for components included in the sub-algorithm with the second identification information; and

when a loading request sent by the first privacy computing device is received, loading the components included in the sub-algorithm with the second identification information, and after the loading is successful, sending a loading success message to the first privacy computing device.

25. The method according to claim 24, wherein:

receiving the first query request sent by the first privacy computing device includes receiving the first query request based on a first API;

sending stored information for components included in the sub-algorithm with the second identification information to the first privacy computing device includes sending the stored information for components included in the sub-algorithm with the second identification information to the first privacy computing device based on the first API;

receiving the loading request sent by the first privacy computing device includes receiving the loading request based on a second API; and

sending a loading success message to the first privacy computing device includes sending the loading success message to the first privacy computing device based on the second API.

26. The method according to claim 24, wherein, before receiving the first query request sent by the first privacy computing device, the method further comprises:

receiving a cooperation request sent by the first privacy computing device, wherein the cooperation request carries the first identification information of the first privacy computing device; and

when it is determined that the first identification information is located in the stored identification information for compliance devices, sending to the first privacy computing device a first confirmation message for agreeing to cooperate.

27. The method according to claim 26, wherein:

receiving the cooperation request sent by the first privacy computing device includes receiving the cooperation request based on a third API; and

sending the first confirmation message for agreeing to cooperate to the first privacy computing device includes sending the first confirmation message based on the third API.

28. The method according to any one of claims 24-27, further comprising:
receiving a second query request sent by the first privacy computing device, wherein the second query request carries the first identification information of the first privacy computing device and third identification information of a to-be-queried data resource; and
when it is determined that the first identification information is located in the stored identification information for compliance devices, sending to the first privacy computing device stored information for the data resource with the third identification information.

29. The method according to claim 28, wherein:
receiving the second query request sent by the first privacy computing device includes receiving the second query request based on a fourth API; and
sending to the first privacy computing device the stored information for the data resource information with the third identification information to the first privacy computing device includes sending the information for the data resource with the third identification information based on the fourth API.

30. The method according to claim 28, wherein, after receiving the second query request sent by the first privacy computing device, the method further comprises:
receiving an authorization request sent by the first privacy computing device, wherein the authorization request carries the first identification information of the first privacy computing device; and

when it is determined that the first identification information is located in the stored identification information for compliance devices, sending to the first privacy computing device a granted authorization message for authorized use of the data resource with the third identification information.

31. The method according to claim 30, wherein:
receiving the authorization request sent by the first privacy computing device includes receiving the authorization request based on a fifth API; and
sending to the first privacy computing device the granted authorization message for authorized use of the data resource with the third identification information includes sending to the first privacy computing device the granted authorization message based on the fifth API.

32. The method according to claim 28, further comprising:
receiving a project execution preparation request sent by the first privacy computing device, wherein the project execution preparation request carries the first identification information of the first privacy computing device, second identification information of a sub-algorithm required for a to-be-run project, and third identification information of a target data resource required for the to-be-run project; and

when it is determined that the first identification information is located in the stored identification information for compliance devices, when it is determined that the target data resource of the third identification information is stored, and when it is determined that the components included in the sub-algorithm with the second identification information are

completely loaded, sending to the first privacy computing device a second confirmation message confirming a readiness.

33. The method according to claim 32, wherein:

receiving the project execution preparation request sent by the first privacy computing device includes receiving the project execution preparation request based on a sixth API; and
sending to the first privacy computing device the second confirmation message confirming a readiness includes sending to the first privacy computing device the second confirmation message based on the sixth API.

34. The method according to claim 32, further comprising:

when performing the data plane interoperability with the first privacy computing device, receiving a startup request sent by the first privacy computing device, and running the sub-algorithm with the second identification information based on the target data resource with the third identification information.

35. A privacy computing device, comprising:

a first transmission module, configured to send a first query request to a second privacy computing device when performing management plane interoperability with the second privacy computing device, wherein the first query request carries first identification information of the first privacy computing device and second identification information of a to-be-queried sub-algorithm, and the first privacy computing device and the second privacy computing device collaborate on privacy computing tasks based on the management plane interoperability and

perform the privacy computing tasks based on data plane interoperability, wherein the management plane interoperability and the data plane interoperability are mutually independent; and

a second transmission module, configured to, when information for components included in the sub-algorithm with the second identification information sent by the second privacy computing device is received, send to the second privacy computing device a loading request for loading the components included in the sub-algorithm with the second identification information.

36. A privacy computing device, comprising:

a first receiving module, configured to receive a first query request sent by a first privacy computing device when performing management plane interoperability with the first privacy computing device, wherein the first query request carries first identification information of the first privacy computing device and second identification information of a to-be-queried sub-algorithm, and the first privacy computing device and a second privacy computing device collaborate on privacy computing tasks based on the management plane interoperability and perform the privacy computing tasks based on data plane interoperability, wherein the management plane interoperability and the data plane interoperability are mutually independent;

a third transmission module, configured to send stored information for components included in the sub-algorithm with the second identification information to the first privacy computing device when it is determined that the first identification information is located in stored identification information for compliance devices; and

a loading module, configured to load the components included in the sub-algorithm with the second identification information upon receiving a loading request sent by the first privacy

computing device, and after the loading is successful, send a loading success message to the first privacy computing device.

37. An electronic device, comprising a processor and a memory, wherein the memory stores program code, when the program code is executed by the processor, the program code causes the processor to execute the privacy computing method according to any one of claims 13 to 34.

38. A computer-readable storage medium, storing program code, wherein, when the storage medium is run on an electronic device, the program code is configured to cause the electronic device to execute the privacy computing method according to any one of claims 13 to 34.