(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 114969128 A
(43)申请公布日 2022.08.30

(21)申请号 202210895387.6

(22)申请日 2022.07.28

(71)申请人 翼方健数(北京)信息科技有限公司
地址 100000 北京市海淀区阜成路73号A座五层507,508,509,510,511,512号
申请人 翼健(上海)信息科技有限公司

(72)发明人 潘光明

(74)专利代理机构 北京沃杰永益知识产权代理事务所(普通合伙) 11905
专利代理师 杨杰

(51)Int.Cl.
G06F 16/2455(2019.01)
G06F 21/60(2013.01)
G06F 21/62(2013.01)
H04L 9/40(2022.01)

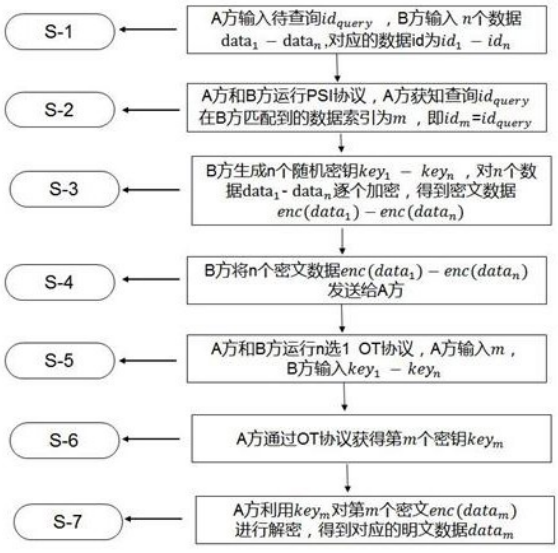
权利要求书2页 说明书11页 附图1页

(54)发明名称

一种基于安全多方计算技术的隐匿查询方法、系统和存储介质

(57)摘要

本申请提供了一种基于安全多方计算技术的隐匿查询方法、系统和存储介质。本申请通过PSI协议搜寻数据方中与查询id信息相匹配的索引结果,根据索引结果通过OT协议获取与索引结果相对应的加密密钥信息,再根据获取得到的加密密钥信息对数据方相对应的加密明文数据进行解密,生成索引结果的明文数据并反馈至查询方。本申请采用MPC加密技术和对称加密技术实现隐匿查询,在满足查询结果正确的情况下,查询方的查询条件不会被泄漏给数据方,数据方除符合查询条件之外的数据也不会泄露给查询方,可以实现对查询方和数据方的双方数据隐私保护;另外在机密性上优于传统明文查询方案,安全性方面优于TEE技术,查询性能方面优于FHE查询技术。



CN 114969128 A

1.一种基于安全多方计算技术的隐匿查询方法,其特征在于,包括如下步骤:

接收来自查询方的查询id信息,通过PSI协议搜寻数据方中与查询id信息相匹配的索引结果;

接收来自数据方的加密明文数据,根据索引结果通过OT协议获取与索引结果相对应的加密密钥信息;

根据获取得到的加密密钥信息对数据方相对应的加密明文数据进行解密,生成索引结果的明文数据并反馈至查询方。

2.根据权利要求1所述的基于安全多方计算技术的隐匿查询方法,其特征在于,还包括:

将来自数据方的加密明文数据发送至查询方,在接收到的加密明文数据中搜寻与查询id信息相匹配的索引结果;

查询方根据索引结果通过OT协议获取与索引结果相对应的加密密钥信息。

3.根据权利要求1所述的基于安全多方计算技术的隐匿查询方法,其特征在于,通过PSI协议搜寻数据方中与查询id信息相匹配的索引结果具体为:

对数据方的所有资源数据设置数据标识,生成每一个数据对应的数据id信息;

分别对查询id信息和数据id信息采用相同的加密算法进行加密设置生成模拟id信息;

通过比对模拟查询id信息和模拟数据id信息的特征值筛选符合要求的模拟数据id信息作为索引结果反馈至查询方。

4.根据权利要求1所述的基于安全多方计算技术的隐匿查询方法,其特征在于,通过PSI协议搜寻数据方中与查询id信息相匹配的索引结果具体为:

根据查询id信息的字符组合和排列方式引入特征标签;

利用特征标签对数据id信息的识别作用调取数据方中的部分资源数据所对应的数据id信息;

采用同类别的转换规则分别对查询id信息和数据id信息进行数据归一化处理并利用设定阈值搜寻符合要求的数据id信息。

5.根据权利要求1所述的基于安全多方计算技术的隐匿查询方法,其特征在于,所述加密明文数据具体为:

对数据方的每个资源数据进行编号,利用生成随机数的方式生成每个对应编号的加密密钥;

利用加密密钥信息通过对称加密算法对每个相应编号的资源数据进行加密生成加密明文数据。

6.根据权利要求1所述的基于安全多方计算技术的隐匿查询方法,其特征在于,根据索引结果通过OT协议获取与索引结果相对应的加密密钥信息具体为:

将加密密钥信息进行编码并建立密钥编码集合发送至查询方;

获取索引结果所在密钥编码集合中的所处位置,根据所处位置获取相应的加密密钥信息。

7.根据权利要求6所述的基于安全多方计算技术的隐匿查询方法,其特征在于,还包括:

根据数据类型和数据值对资源数据的所属编号进行分区,对每个分区内的资源数据设

置不同的随机方案生成加密密钥；

对索引结果的数据类型和数据值进行分析，根据分析结果设置阈值对加密密钥进行预选后再对选中的加密密钥信息建立密钥编码集合。

8.根据权利要求1所述的基于安全多方计算技术的隐匿查询方法，其特征在于，根据索引结果通过OT协议获取与索引结果相对应的加密密钥信息具体为：

将加密密钥信息按编码次序排列上传至中转站；

采集索引结果的核心字符串并根据核心字符信息对中转站中的加密密钥信息进行过滤；

将过滤后的加密密钥信息发送至查询方。

9.一种基于安全多方计算技术的隐匿查询系统，其特征在于，包括存储器和处理器，所述存储器中包括基于安全多方计算技术的隐匿查询程序，所述基于安全多方计算技术的隐匿查询程序被所述处理器执行时，实现如权利要求1~8任一项所述基于安全多方计算技术的隐匿查询方法的步骤。

10.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质中包括基于安全多方计算技术的隐匿查询程序，所述基于安全多方计算技术的隐匿查询程序被处理器执行时，实现如权利要求1~8任一项所述基于安全多方计算技术的隐匿查询方法的步骤。

一种基于安全多方计算技术的隐匿查询方法、系统和存储介质

技术领域

[0001] 本申请属于大数据安全技术领域，更具体的，涉及一种基于安全多方计算技术的隐匿查询方法、系统和存储介质。

背景技术

[0002] 在传统数据库查询应用中，查询方提交明文查询条件到数据库(数据方)，数据方能够获知查询方的查询条件，查询方无法隐藏自己的查询条件，无法保护查询方的查询条件隐私，存在用户数据泄露等安全问题。而在隐匿查询中，数据方无法获知查询方的查询条件，与此同时不影响查询方查询到符合查询条件的数据。目前，隐匿查询算法应用范围较广，可用于保护查询方隐私的数据库查询场景中。

[0003] 同态加密FHE作为一种隐私保护技术，能够实现密文数据计算和比较，但是该技术对计算资源要求较高，在一般IT环境中，基于FHE技术的隐匿查询算法运行时间远远大于明文算法运行时间，计算性能较低。可信执行环境TEE作为一种可信执行环境的隐私保护技术，允许在安全环境下进行数据明文计算，明文数据对安全环境之外的其他任何攻击者都不可见，因此可以保证数据隐私安全。但是，基于TEE技术的隐私计算程序需要运行在支持TEE技术的CPU上，因此需要对CPU生产商绝对信任，这也导致TEE技术的安全模型需要依赖于CPU生产商。

发明内容

[0004] 有鉴于此，本申请提供了一种基于安全多方计算技术的隐匿查询方法、系统和存储介质，查询方和数据方之间可保证数据安全传递的同时，无需依赖固定的处理器，能够改善隐匿查询计算性能。

[0005] 本申请的具体技术方案如下：

本申请第一方面提供一种基于安全多方计算技术的隐匿查询方法，包括如下步骤：

接收来自查询方的查询id信息，通过PSI协议搜寻数据方中与查询id信息相匹配的索引结果；

接收来自数据方的加密明文数据，根据索引结果通过OT协议获取与索引结果相对应的加密密钥信息；

根据获取得到的加密密钥信息对数据方相对应的加密明文数据进行解密，生成索引结果的明文数据并反馈至查询方。

[0006] 优选地，还包括：

将来自数据方的加密明文数据发送至查询方，在接收到的加密明文数据中搜寻与查询id信息相匹配的索引结果；

查询方根据索引结果通过OT协议获取与索引结果相对应的加密密钥信息。

[0007] 优选地,通过PSI协议搜寻数据方中与查询id信息相匹配的索引结果具体为:

对数据方的所有资源数据设置数据标识,生成每一个数据对应的数据id信息;

分别对查询id信息和数据id信息采用相同的加密算法进行加密设置生成模拟id信息;

通过比对模拟查询id信息和模拟数据id信息的特征值筛选符合要求的模拟数据id信息作为索引结果反馈至查询方。

[0008] 优选地,通过PSI协议搜寻数据方中与查询id信息相匹配的索引结果具体为:

根据查询id信息的字符组合和排列方式引入特征标签;

利用特征标签对数据id信息的识别作用调取数据方中的部分资源数据所对应的数据id信息;

采用同类别的转换规则分别对查询id信息和数据id信息进行数据归一化处理并利用设定阈值搜寻符合要求的数据id信息。

[0009] 优选地,所述加密明文数据具体为:

对数据方的每个资源数据进行编号,利用生成随机数的方式生成每个对应编号的加密密钥;

利用加密密钥信息通过对称加密算法对每个相应编号的资源数据进行加密生成加密明文数据。

[0010] 优选地,根据索引结果通过OT协议获取与索引结果相对应的加密密钥信息具体为:

将加密密钥信息进行编码并建立密钥编码集合发送至查询方;

获取索引结果所在密钥编码集合中的所处位置,根据所处位置获取相应的加密密钥信息。

[0011] 优选地,还包括:

根据数据类型和数据值对资源数据的所属编号进行分区,对每个分区内的资源数据设置不同的随机方案生成加密密钥;

对索引结果的数据类型和数据值进行分析,根据分析结果设置阈值对加密密钥进行预选后再对选中的加密密钥信息建立密钥编码集合。

[0012] 优选地,根据索引结果通过OT协议获取与索引结果相对应的加密密钥信息具体为:

将加密密钥信息按编码次序排列上传至中转站;

采集索引结果的核心字符串并根据核心字符信息对中转站中的加密密钥信息进行过滤;

将过滤后的加密密钥信息发送至查询方。

[0013] 本申请第二方面提供一种基于安全多方计算技术的隐匿查询系统,包括存储器和处理器,所述存储器中包括基于安全多方计算技术的隐匿查询程序,所述基于安全多方计算技术的隐匿查询程序被所述处理器执行时,实现如下步骤:

接收来自查询方的查询id信息,通过PSI协议搜寻数据方中与查询id信息相匹配的索引结果;

接收来自数据方的加密明文数据,根据索引结果通过OT协议获取与索引结果相对

应的加密密钥信息；

根据获取得到的加密密钥信息对数据方相对应的加密明文数据进行解密，生成索引结果的明文数据并反馈至查询方。

[0014] 优选地，还包括：

将来自数据方的加密明文数据发送至查询方，在接收到的加密明文数据中搜寻与查询id信息相匹配的索引结果；

查询方根据索引结果通过OT协议获取与索引结果相对应的加密密钥信息。

[0015] 优选地，通过PSI协议搜寻数据方中与查询id信息相匹配的索引结果具体为：

对数据方的所有资源数据设置数据标识，生成每一个数据对应的数据id信息；

分别对查询id信息和数据id信息采用相同的加密算法进行加密设置生成模拟id信息；

通过比对模拟查询id信息和模拟数据id信息的特征值筛选符合要求的模拟数据id信息作为索引结果反馈至查询方。

[0016] 优选地，通过PSI协议搜寻数据方中与查询id信息相匹配的索引结果具体为：

根据查询id信息的字符组合和排列方式引入特征标签；

利用特征标签对数据id信息的识别作用调取数据方中的部分资源数据所对应的数据id信息；

采用同类别的转换规则分别对查询id信息和数据id信息进行数据归一化处理并利用设定阈值搜寻符合要求的数据id信息。

[0017] 优选地，所述加密明文数据具体为：

对数据方的每个资源数据进行编号，利用生成随机数的方式生成每个对应编号的加密密钥；

利用加密密钥信息通过对称加密算法对每个相应编号的资源数据进行加密生成加密明文数据。

[0018] 优选地，根据索引结果通过OT协议获取与索引结果相对应的加密密钥信息具体为：

将加密密钥信息进行编码并建立密钥编码集合发送至查询方；

获取索引结果所在密钥编码集合中的所处位置，根据所处位置获取相应的加密密钥信息。

[0019] 优选地，还包括：

根据数据类型和数据值对资源数据的所属编号进行分区，对每个分区内的资源数据设置不同的随机方案生成加密密钥；

对索引结果的数据类型和数据值进行分析，根据分析结果设置阈值对加密密钥进行预选后再对选中的加密密钥信息建立密钥编码集合。

[0020] 优选地，根据索引结果通过OT协议获取与索引结果相对应的加密密钥信息具体为：

将加密密钥信息按编码次序排列上传至中转站；

采集索引结果的核心字符串并根据核心字符信息对中转站中的加密密钥信息进行过滤；

将过滤后的加密密钥信息发送至查询方。

[0021] 本申请第三方面提供一种计算机可读存储介质，所述计算机可读存储介质中包括基于安全多方计算技术的隐匿查询程序，所述基于安全多方计算技术的隐匿查询程序被处理器执行时，实现所述基于安全多方计算技术的隐匿查询方法的步骤。

[0022] 综上所述，本申请提供了一种基于安全多方计算技术的隐匿查询方法、系统和存储介质。本申请通过PSI协议搜寻数据方中与查询id信息相匹配的索引结果，根据索引结果通过OT协议获取与索引结果相对应的加密密钥信息，再根据获取得到的加密密钥信息对数据方相对应的加密明文数据进行解密，生成索引结果的明文数据并反馈至查询方。本申请采用MPC加密技术和对称加密技术实现隐匿查询，在满足查询结果正确的情况下，查询方的查询条件不会被泄漏给数据方，数据方除符合查询条件之外的数据也不会泄露给查询方，可以实现对查询方和数据方的双方数据隐私保护；另外在机密性上优于传统明文查询方案，安全性和查询性能方面优于TEE、FHE查询技术。

附图说明

[0023] 为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其它的附图。

[0024] 图1为本申请一种基于安全多方计算技术的隐匿查询方法的流程图；

图2为本申请一种基于安全多方计算技术的隐匿查询系统的框图。

具体实施方式

[0025] 为使得本申请的目的、特征、优点能够更加的明显和易懂，对本申请实施例中的技术方案进行清楚、完整地描述，显然，下面所描述的实施例仅仅是本申请一部分实施例，而非全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其它实施例，都属于本申请保护的范围。

[0026] 本申请实施例第一方面提供一种基于安全多方计算技术的隐匿查询方法，包括如下步骤：

接收来自查询方的查询id信息，通过PSI(Private Set Intersection)协议搜寻数据方中与查询id信息相匹配的索引结果；

接收来自数据方的加密明文数据，根据索引结果通过OT(Oblivious Transfer)协议获取与索引结果相对应的加密密钥信息；

根据获取得到的加密密钥信息对数据方相对应的加密明文数据进行解密，生成索引结果的明文数据并反馈至查询方。

[0027] 需要说明的是，查询id是指对查询信息进行数字标识，便于索引、提取等数据处理。索引结果是指数据方提供的查询结果相应的数据id信息。加密明文数据的加密解密过程可采用本领域常规的对称加密算法实现。其中，在接收来自数据方的加密明文数据时，还可以提取其中的加密密钥信息，具体根据本领域技术人员的实际需要而定。

[0028] 根据本申请实施例，还包括：

将来自数据方的加密明文数据发送至查询方，在接收到的加密明文数据中搜寻与查询id信息相匹配的索引结果；

查询方根据索引结果通过OT协议获取与索引结果相对应的加密密钥信息。

[0029] 需要说明的是，数据方的加密明文数据可直接发送查询方，查询和筛选过程可全部由查询方完成，无需依赖固定的处理介质，在查询方的查询信息量较大的情况下还可简化后续再次查询的数据管理流程。

[0030] 根据本申请实施例，通过PSI协议搜寻数据方中与查询id信息相匹配的索引结果具体为：

对数据方的所有资源数据设置数据标识，生成每一个数据对应的数据id信息；

分别对查询id信息和数据id信息采用相同的加密算法进行加密设置生成模拟id信息；

通过比对模拟查询id信息和模拟数据id信息的特征值筛选符合要求的模拟数据id信息作为索引结果反馈至查询方。

[0031] 需要说明的是，查询方输入待查询数据id信息可表示为 $\mathrm{id}_{\mathrm{query}}$，数据方输入 n 个数据 $data_1 - data_n$，n个数据对应的数据id为 $id_1 - id_n$。查询方和数据方运行隐私求交算法PSI，查询方获知 id_{query} 在数据方匹配到的数据索引结果为 m，即 $id_{query}=id_m$。隐私求交算法可以保证只有查询方知道 m 值，数据方无法获知 m 值。

[0032] 根据本申请实施例，通过PSI协议搜寻数据方中与查询id信息相匹配的索引结果具体为：

根据查询id信息的字符组合和排列方式引入特征标签；

利用特征标签对数据id信息的识别作用调取数据方中的部分资源数据所对应的数据id信息；

采用同类别的转换规则分别对查询id信息和数据id信息进行数据归一化处理并利用设定阈值搜寻符合要求的数据id信息。

[0033] 需要说明的是，利用特征标签对数据方的数据id信息进行分区预筛选，再利用数据归一化的方式统一数据处理口径，通过阈值筛选查询方需要的索引结果，可以减少数据运算量、缩短数据传输耗时。

[0034] 根据本申请实施例，所述加密明文数据具体为：

对数据方的每个资源数据进行编号，利用生成随机数的方式生成每个对应编号的加密密钥；

利用加密密钥信息通过对称加密算法对每个相应编号的资源数据进行加密生成加密明文数据。

[0035] 需要说明的是，数据方随机生成 n 个密钥 $key_1 - key_n$，然后通过对称加密算法对 n 个数据 $data_1 - data_n$ 进行加密，得到 n 个密文数据 $enc(data_1) - enc(data_n)$。具体来说第 i 个密钥 key_i 对第 i 个数 $data_i$ 进行加密得到密文数据 $enc(data_i)$。数据方需要对 n 个密钥 $key_1 - key_n$ 进行保密。数据方将 n 个密文数据 $enc(data_1) - enc(data_n)$

发送给查询方。对称加密算法安全性保证了查询方在不知道密钥的情况下无法获取数据方的数据明文。

[0036] 根据本申请实施例，根据索引结果通过OT协议获取与索引结果相对应的加密密钥信息具体为：

将加密密钥信息进行编码并建立密钥编码集合发送至查询方；

获取索引结果所在密钥编码集合中的所处位置，根据所处位置获取相应的加密密钥信息。

[0037] 需要说明的是，本申请实施例中查询方和数据方运行n选1 OT协议。双方通过多轮协议交互，数据方提供n个消息$d_1 - d_n$，查询方根据输$b \in [n]$选择接受d_b。OT协议可以保证数据方无法获知查询方的b值，查询方无法获知d_b以外的内容。查询方输入值为m，数据方输入$key_1 - key_n$。查询方通过n选1 OT协议获取到数据方的随机密钥key_m，OT协议安全性保证了查询方无法获取数据方key_m之外的其他密钥。最后，查询方通过对称加密算法使用key_m对密文数据$enc(data_m)$进行解密，得到明文数据$data_m$。

[0038] 根据本申请实施例，还包括：

根据数据类型和数据值对资源数据的所属编号进行分区，对每个分区内的资源数据设置不同的随机方案生成加密密钥；

对索引结果的数据类型和数据值进行分析，根据分析结果设置阈值对加密密钥进行预选后再对选中的加密密钥信息建立密钥编码集合。

[0039] 需要说明的是，对数据方的资源数据按照不同场景或功能性质分区，并建立每个分区特定的加密算法，使得索引结果在匹配加密密钥信息时可通过数据解析快速筛选信息，提高数据运算效率。

[0040] 根据本申请实施例，根据索引结果通过OT协议获取与索引结果相对应的加密密钥信息具体为:

将加密密钥信息按编码次序排列上传至中转站；

采集索引结果的核心字符串并根据核心字符信息对中转站中的加密密钥信息进行过滤；

将过滤后的加密密钥信息发送至查询方。

[0041] 需要说明的是，加密密钥信息还可以放置在中转站，经过核心字符筛选后再发送至查询方，核心字符串可以是通过数字编排、数据类型解析等方式实现，索引结果和加密密钥信息中的数据类型均可与核心字符串相关联。

[0042] 请参照图1，图1为本申请一种基于安全多方计算技术的隐匿查询方法的流程图。其中，A方为查询方，B方为数据方。经过S1~S7的运行，首先通过PSI协议搜寻数据方中与查询id信息相匹配的索引结果，根据索引结果通过OT协议获取与索引结果相对应的加密密钥信息，再根据获取得到的加密密钥信息对数据方相对应的加密明文数据进行解密，最后生成索引结果的明文数据并反馈至查询方。

[0043] 在本申请另一实施例中，通过PSI协议搜寻数据方中与查询id信息相匹配的索引

结果具体为：

获取来自数据方的所有资源数据进行hash值加密设置并发送至查询方；

对查询id信息进行hash值加密设置，通过比对查询id信息与资源数据的hash值筛选符合要求的资源数据；

对资源数据数据hash值采用预设的算法解析生成索引结果并反馈至查询方。

[0044] 需要说明的是，本申请实施例采用基于hash加密实现隐私求交算法。数据方将n个数据都加密为hash值，得到n个hash密文数据$hash_1 - hash_n$然后将$hash_1 - hash_n$发送给查询方。根据hash函数特性，hash值无法反推出对应数据明文，因此数据方的明文数据是安全的，查询方无法获知。查询方将查询id_{query}加密为hash值$hash_{query}$，然后将$hash_{query}$与$hash_1 - hash_n$逐个比对得到匹配的数据索引结果m。

[0045] 在本申请另一实施例中，还包括：

对加密明文数据中的加密密钥进行时间周期设置，对每个小范围时间周期采用动态随机数的方式生成相应的加密密钥；

对超过预设时间周期的加密明文数据进行清除。

[0046] 需要说明的是，由于数据方的所有明文数据均被暂存于查询方，会产生大量数据缓存影响使用流畅感，需要通过时间周期设置定期清理，在保证查询性能的同时也提升数据安全性。

[0047] 在本申请另一实施例中，还包括：

获取加密密钥的生成时间信息；

将所述加密密钥的生成时间与加密密钥进行关联连接；

判断所述加密密钥的生成时间是否大于第二预设阈值，若是，则得到所述加密密钥失效信息。

[0048] 需要说明的是，明文数据的加密密钥具有时效性，当加密密钥生成时，所述加密密钥被印上生成时间戳，查询方需要及时输入所述加密密钥，当所述加密密钥的存储时间超过第二预设阈值时，所述加密密钥无效，例如，加密密钥的生成时间为当天9点整，第二预设阈值为30分钟，则当时间到当天9点30分钟后，所述加密密钥失效。

[0049] 在本申请另一实施例中，还包括：

获取加密密钥的使用次数信息；

判断所述加密密钥的使用次数是否大于第三预设阈值，若是，则得到所述加密密钥无效信息。

[0050] 需要说明的是，明文数据的加密密钥具有输入次数有限性，查询方在失误操作下关闭查询页面后，可以重新输入加密密钥继续进行查看明文数据，不需要重新申请获取加密密钥，节省了时间，同时，加密密钥在使用次数达到第三预设阈值后，所述加密密钥失去效果，例如，第三预设阈值设为3，则所述加密密钥在规定的时间内可以重复使用三次，当同一加密密钥使用第4次时，则显示所述加密密钥无效。

[0051] 在本申请另一实施例中，还包括：

获取查询方IP地址信息；

判断所述查询方在多次使用同一加密密钥时的IP地址是否一致，若是，则同意访问，若否，则所述加密密钥无效。

[0052] 需要说明的是，一个加密密钥只对一个用户且同一个IP地址有效，当同一个查询方通过不同IP地址访问同一个id信息时，需要获取对应的加密密钥信息，以防止查询方被盗等安全事故发生。

[0053] 在本申请另一实施例中，还包括：

获取历史查询id信息；

将所述历史查询id按照时间先后顺序进行存储。

[0054] 需要说明的是，当查询方每次输入查询id信息时，后台服务器将所述查询id进行存储，所述历史查询id存储只是将所述查询id的链接进行存储，所述查询id所包含的明文数据并未存储，当查询方输入查询id部分名称时，服务器将有关联的历史查询id进行显示，查询方可以根据显示的历史查询id进行访问，以节省查询方的时间。

[0055] 请参照图2，图2为本申请一种基于安全多方计算技术的隐匿查询系统的框图。

[0056] 本申请实施例第二方面提供一种基于安全多方计算技术的隐匿查询系统，包括存储器21和处理器22，所述存储器21中包括基于安全多方计算技术的隐匿查询程序，所述基于安全多方计算技术的隐匿查询程序被所述处理器22执行时，实现如下步骤：

接收来自查询方的查询id信息，通过PSI协议搜寻数据方中与查询id信息相匹配的索引结果；

接收来自数据方的加密明文数据，根据索引结果通过OT协议获取与索引结果相对应的加密密钥信息；

根据获取得到的加密密钥信息对数据方相对应的加密明文数据进行解密，生成索引结果的明文数据并反馈至查询方。

[0057] 根据本申请实施例，通过PSI协议搜寻数据方中与查询id信息相匹配的索引结果具体为：

获取来自数据方的所有资源数据进行hash值加密设置并发送至查询方；

对查询id信息进行hash值加密设置，通过比对查询id信息与资源数据的hash值筛选符合要求的资源数据；

对资源数据数据hash值采用预设的算法解析生成索引结果并反馈至查询方。

[0058] 根据本申请实施例，还包括：

将来自数据方的加密明文数据发送至查询方，在接收到的加密明文数据中搜寻与查询id信息相匹配的索引结果；

查询方根据索引结果通过OT协议获取与索引结果相对应的加密密钥信息。

[0059] 根据本申请实施例，通过PSI协议搜寻数据方中与查询id信息相匹配的索引结果具体为：

根据查询id信息的字符组合和排列方式引入特征标签；

利用特征标签对数据id信息的识别作用调取数据方中的部分资源数据所对应的数据id信息；

采用同类别的转换规则分别对查询id信息和数据id信息进行数据归一化处理并

利用设定阈值搜寻符合要求的数据id信息。

[0060] 根据本申请实施例,所述加密明文数据具体为:

对数据方的每个资源数据进行编号,利用生成随机数的方式生成每个对应编号的加密密钥;

利用加密密钥信息通过对称加密算法对每个相应编号的资源数据进行加密生成加密明文数据。

[0061] 根据本申请实施例,根据索引结果通过OT协议获取与索引结果相对应的加密密钥信息具体为:

将加密密钥信息进行编码并建立密钥编码集合发送至查询方;

获取索引结果所在密钥编码集合中的所处位置,根据所处位置获取相应的加密密钥信息。

[0062] 根据本申请实施例,还包括:

根据数据类型和数据值对资源数据的所属编号进行分区,对每个分区内的资源数据设置不同的随机方案生成加密密钥;

对索引结果的数据类型和数据值进行分析,根据分析结果设置阈值对加密密钥进行预选后再对选中的加密密钥信息建立密钥编码集合。

[0063] 根据本申请实施例,根据索引结果通过OT协议获取与索引结果相对应的加密密钥信息具体为:

将加密密钥信息按编码次序排列上传至中转站;

采集索引结果的核心字符串并根据核心字符信息对中转站中的加密密钥信息进行过滤;

将过滤后的加密密钥信息发送至查询方。

[0064] 在本申请另一实施例中,通过PSI协议搜寻数据方中与查询id信息相匹配的索引结果具体为:

获取来自数据方的所有资源数据进行hash值加密设置并发送至查询方;

对查询id信息进行hash值加密设置,通过比对查询id信息与资源数据的hash值筛选符合要求的资源数据;

对资源数据数据hash值采用预设的算法解析生成索引结果并反馈至查询方。

[0065] 在本申请另一实施例中,还包括:

对加密明文数据中的加密密钥进行时间周期设置,对每个小范围时间周期采用动态随机数的方式生成相应的加密密钥;

对超过预设时间周期的加密明文数据进行清除。

[0066] 在本申请另一实施例中,还包括:

获取加密密钥的生成时间信息;

将所述加密密钥的生成时间与加密密钥进行关联连接;

判断所述加密密钥的生成时间是否大于第二预设阈值,若是,则得到所述加密密钥失效信息。

[0067] 需要说明的是,明文数据的加密密钥具有时效性,当加密密钥生成时,所述加密密钥被印上生成时间戳,查询方需要及时输入所述加密密钥,当所述加密密钥的存储时间超

过第二预设阈值时，所述加密密钥无效，例如，加密密钥的生成时间为当天9点整，第二预设阈值为30分钟，则当时间到当天9点30分钟后，所述加密密钥失效。

[0068] 在本申请另一实施例中，还包括：

获取加密密钥的使用次数信息；

判断所述加密密钥的使用次数是否大于第三预设阈值，若是，则得到所述加密密钥无效信息。

[0069] 需要说明的是，明文数据的加密密钥具有输入次数有限性，查询方在失误操作下关闭查询页面后，可以重新输入加密密钥继续进行查看明文数据，不需要重新申请获取加密密钥，节省了时间，同时，加密密钥在使用次数达到第三预设阈值后，所述加密密钥失去效果，例如，第三预设阈值设为3，则所述加密密钥在规定的时间内可以重复使用三次，当同一加密密钥使用第4次时，则显示所述加密密钥无效。

[0070] 在本申请另一实施例中，还包括：

获取查询方IP地址信息；

判断所述查询方在多次使用同一加密密钥时的IP地址是否一致，若是，则同意访问，若否，则所述加密密钥无效。

[0071] 需要说明的是，一个加密密钥只对一个用户且同一个IP地址有效，当同一个查询方通过不同IP地址访问同一个id信息时，需要获取对应的加密密钥信息，以防止查询方被盗等安全事故发生。

[0072] 在本申请另一实施例中，还包括：

获取历史查询id信息；

将所述历史查询id按照时间先后顺序进行存储。

[0073] 需要说明的是，当查询方每次输入查询id信息时，后台服务器将所述查询id进行存储，所述历史查询id存储只是将所述查询id的链接进行存储，所述查询id所包含的明文数据并未存储，当查询方输入查询id部分名称时，服务器将有关联的历史查询id进行显示，查询方可以根据显示的历史查询id进行访问，以节省查询方的时间。

[0074] 本申请实施例第三方面提供一种计算机可读存储介质，所述计算机可读存储介质中包括基于安全多方计算技术的隐匿查询程序，所述基于安全多方计算技术的隐匿查询程序被处理器执行时，实现所述基于安全多方计算技术的隐匿查询方法的步骤，具体参见图1对方法步骤的描述，在此不再赘述。

[0075] 在本申请所提供的几个实施例中，应该理解到，所揭露的设备和方法，可以通过其它的方式实现。以上所描述的设备实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，如：多个单元或组件可以结合，或可以集成到另一个系统，或一些特征可以忽略，或不执行。另外，所显示或讨论的各组成部分相互之间的耦合、或直接耦合、或通信连接可以是通过一些接口，设备或单元的间接耦合或通信连接，可以是电性的、机械的或其它形式的。

[0076] 上述作为分离部件说明的单元可以是、或也可以不是物理上分开的，作为单元显示的部件可以是、或也可以不是物理单元；既可以位于一个地方，也可以分布到多个网络单元上；可以根据实际的需要选择其中的部分或全部单元来实现本实施例方案的目的。

[0077] 另外，在本发明各实施例中的各功能单元可以全部集成在一个处理单元中，也可

以是各单元分别单独作为一个单元，也可以两个或两个以上单元集成在一个单元中；上述集成的单元既可以采用硬件的形式实现，也可以采用硬件加软件功能单元的形式实现。

[0078] 本领域普通技术人员可以理解：实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成，前述的程序可以存储于计算机可读取存储介质中，该程序在执行时，执行包括上述方法实施例的步骤；而前述的存储介质包括：移动存储设备、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0079] 或者，本发明上述集成的单元如果以软件功能模块的形式实现并作为独立的产品销售或使用时，也可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明实施例的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备(可以是个人计算机、服务器、或者网络设备等)执行本发明各个实施例所述方法的全部或部分。而前述的存储介质包括：移动存储设备、ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0080] 以上所述，以上实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本申请各实施例技术方案的精神和范围。

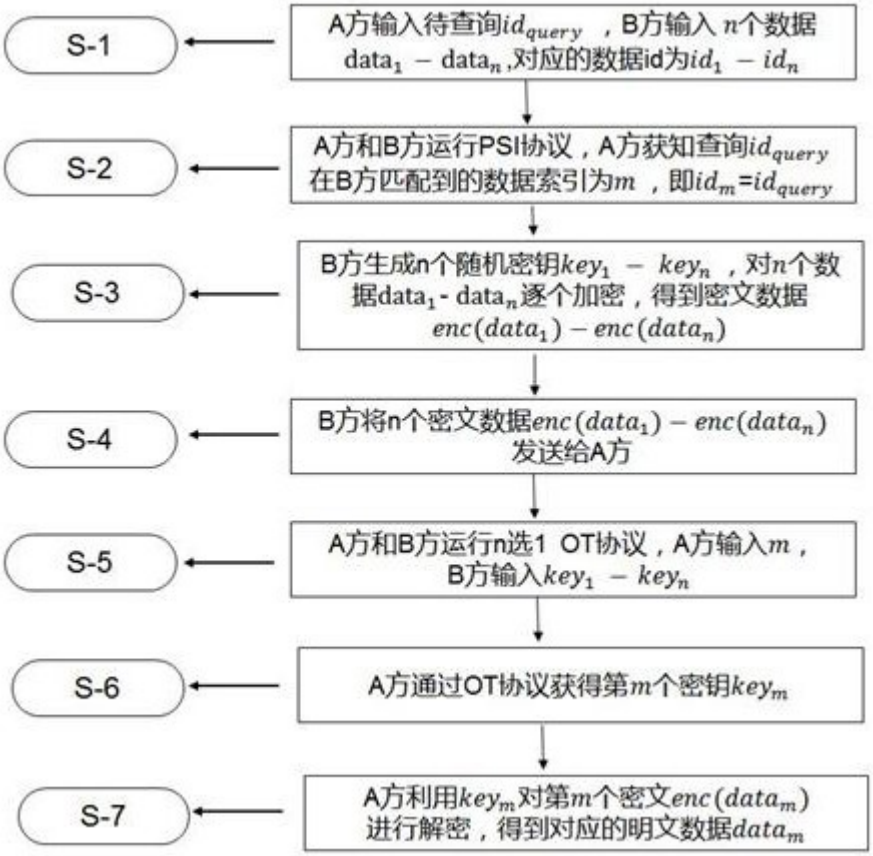

S-1
A方输入待查询id_{query} ，B方输入 n个数据 $data_1 - data_n$,对应的数据id为$id_1 - id_n$
S-2
A方和B方运行PSI协议，A方获知查询id_{query}在B方匹配到的数据索引为m ，即id_m=id_{query}
S-3
B方生成n个随机密钥$key_1 - key_n$ ，对n个数据$data_1$- $data_n$逐个加密，得到密文数据 $enc(data_1) - enc(data_n)$
S-4
B方将n个密文数据$enc(data_1) - enc(data_n)$发送给A方
S-5
A方和B方运行n选1 OT协议，A方输入m，B方输入$key_1 - key_n$
S-6
A方通过OT协议获得第m个密钥key_m
S-7
A方利用key_m对第m个密文$enc(data_m)$进行解密，得到对应的明文数据$data_m$

图1


存储器21
处理器22
基于安全多方计算技术的隐匿查询系统

图2