(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2024 年 4 月 18 日 (18.04.2024)

WIPO | PCT

(10) 国际公布号
WO 2024/077948 A1

(51) 国际专利分类号:
G06F 21/62 (2013.01)

(21) 国际申请号: PCT/CN2023/094279

(22) 国际申请日: 2023 年 5 月 15 日 (15.05.2023)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202211252878.5 2022年10月13日 (13.10.2022) CN

(71) 申请人: 北京沃东天骏信息技术有限公司 (**BEIJING WODONG TIANJUN INFORMATION TECHNOLOGY CO., LTD.**) [CN/CN]; 中国北京市大兴区北京经济技术开发区科创十一街18号院2号楼4层A402室, Beijing 100176 (CN)。 北京京东世纪贸易有限公司(**BEIJING JINGDONG CENTURY TRADING CO., LTD.**) [CN/CN]; 中国北京市大兴区北京经济技术开发区科创十一街18号C座2层201室, Beijing 100176 (CN)。

(72) 发明人: 刘立伟(**LIU, Liwei**); 中国北京市大兴区北京经济技术开发区科创十一街18号院2号楼4层A402室, Beijing 100176 (CN)。 王新左(**WANG, Xinzuo**); 中国北京市大兴区北京经济技术开发区科创十一街18号院2号楼4层A402室, Beijing 100176 (CN)。 彭皓(**PENG, Hao**); 中国北京市大兴区北京经济技术开发区科创十一街18号院2号楼4层A402室, Beijing 100176 (CN)。 张泽华(**ZHANG, Zehua**); 中国北京市大兴区北京经济技术开发区科创十一街18号院2号楼4层A402室, Beijing 100176 (CN)。 何杰(**HE, Jie**); 中国北京市大兴区北京经济技术开发区科创十一街18号院2号楼4层A402室, Beijing 100176 (CN)。 林战刚(**LIN, Zhangang**); 中

(54) **Title:** PRIVATE QUERY METHOD, APPARATUS AND SYSTEM, AND STORAGE MEDIUM

(54) 发明名称: 匿踪查询方法、装置和系统及存储介质

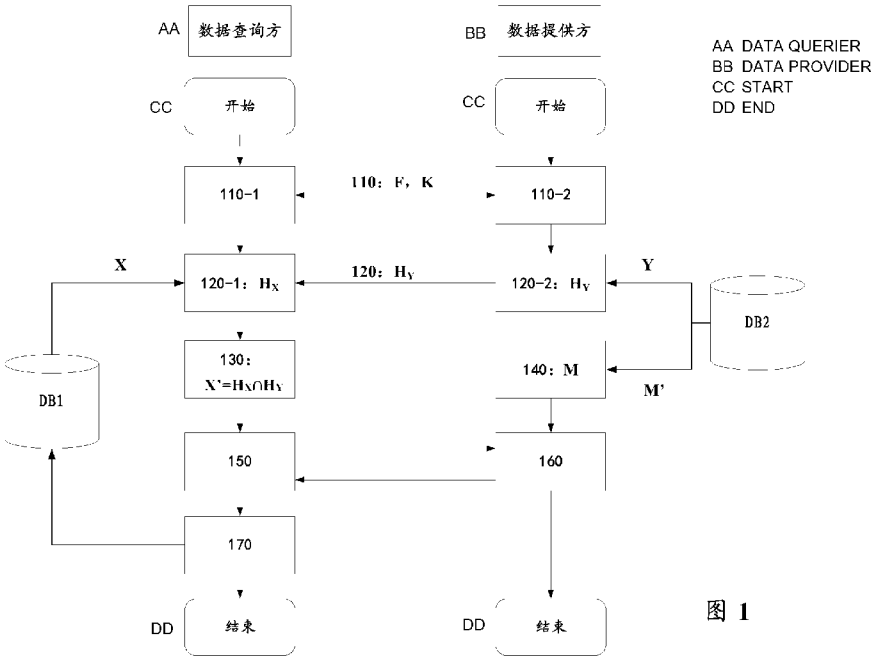

图 1

(57) **Abstract:** The present disclosure relates to the technical field of computers, and in particular to the field of privacy computation. Provided are a private query method, apparatus and system, and a storage medium. A private query solution provided in the embodiments of the present disclosure comprises: by means of finding the intersection of encrypted identifier data, determining the intersection of data records of a data provider and a data querier, without revealing the privacy of the two parties; if it is determined that a plurality of pieces of target label data corresponding to a plurality of target storage sequence numbers in the intersection are stored in the same

WO 2024/077948 A1

[见续页]

国北京市大兴区北京经济技术开发区科创十一街18号院2号楼4层A402室, Beijing 100176 (CN)。

(74) 代理人: 中国贸促会专利商标事务所有限公司 (CCPIT PATENT AND TRADEMARK LAW OFFICE); 中国北京市西城区复兴门内大街158号远洋大厦F10层, Beijing 100031 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:
— 包括国际检索报告(条约第21条(3))。

target plaintext, for such the plurality of target storage sequence numbers, using a ciphertext of index information of the target plaintext to initiate one ciphertext request to the data provider; and deciphering a ciphertext of the target plaintext in a ciphertext response, so that the plurality of pieces of target label data can be acquired from the target plaintext. Therefore, a plurality of pieces of target label data can be acquired at the same time by means of one ciphertext request and one ciphertext response, thereby reducing communication overhead and computation overhead, such that a private query solution can be run efficiently.

(57) 摘要: 本公开提出一种匿踪查询方法、装置和系统及存储介质，涉及计算机技术领域，尤其涉及隐私计算领域。本公开实施例的匿踪查询方案，通过加密标识数据求交集的方式，在不泄露双方隐私的情况下，确定数据提供方和数据查询方的数据记录的交集，如果判定交集中的多个目标存储序号相应的多个目标标签数据被存储在同一目标明文，针对这样的多个目标存储序号，利用目标明文的索引信息的密文向数据提供方发起一次密文请求，对密文响应中的目标明文的密文进行解密，从目标明文中可获取该多个目标标签数据。从而，通过一次密文请求和密文响应，可以同时获取多个目标标签数据，降低了通信开销和计算开销，进而使得匿踪查询方案能够高效运行。

匿踪查询方法、装置和系统及存储介质

相关申请的交叉引用

本申请是以 CN 申请号为 202211252878.5，申请日为 2022 年 10 月 13 日的申请为基础，并主张其优先权，该 CN 申请的公开内容在此作为整体引入本申请中。

技术领域

本公开涉及计算机技术领域，尤其涉及隐私计算领域，特别涉及一种匿踪查询方法、匿踪查询装置、匿踪查询系统及存储介质。

背景技术

匿踪查询，也称隐私信息检索 (Private Information Retrieval，PIR)，用来保护用户的查询隐私，也即，数据查询方向数据提供方提交数据查询请求时，在保证数据查询方的查询信息不被泄漏的条件下完成数据查询。

一种基于序号的匿踪查询方法，数据查询方针对数据提供方的每条数据记录的存储序号发起一次密文请求，通过密文响应获得该存储序号相应的数据记录的标签数据。

经研究发现，如果想要查询多个数据记录的标签数据，则数据查询方针对多个数据记录的多个存储序号，需要通过多次密文请求和密文响应，才能获得该多个数据记录的标签数据，导致通信开销和计算开销比较大。

发明内容

本公开一些实施例提出一种匿踪查询方法，包括：

确定第一加密标识数据集与第二加密标识数据集的交集，其中，所述第一加密标识数据集包括数据提供方的每条数据记录的加密标识数据和存储序号，所述第二加密标识数据集包括数据查询方的每条数据记录的加密标识数据，每条数据记录包括标识数据和标签数据，数据提供方的每多条数据记录的多个标签数据被存储在一个明文；

在根据所述交集中的多个目标存储序号判定相应多条目标数据记录的多个目标标签数据被存储在同一目标明文的情况下，针对所述多个目标存储序号，利用所述目标明文的索引信息的密文向数据提供方发起一次密文请求；

接收数据提供方返回的密文响应，并对所述密文响应中的所述目标明文的密文

进行解密得到所述目标明文；

从所述目标明文中获取所述多个目标标签数据。

在一些实施例中，判定多条目标数据记录的多个目标标签数据被存储在同一目标明文包括：

根据多条目标数据记录的多个目标存储序号以及标签数据到明文的编码参数，确定每条目标数据记录的每个目标标签数据所存储的目标明文的索引信息；

在多条目标数据记录的多个目标标签数据所存储的目标明文的索引信息相同的情况下，判定多条目标数据记录的多个目标标签数据被存储在同一目标明文。

在一些实施例中，确定每条目标数据记录的每个目标标签数据所存储的目标明文的索引信息包括：

根据标签数据到明文的编码参数，确定每个明文所能存储的比特数量；

根据每个明文所能存储的比特数量以及每个标签数据占用的比特数量，确定每个明文所能存储的标签数据的数量；

通过每条目标数据记录的每个目标存储序号对每个明文所能存储的标签数据的数量的除法运算，确定出每条目标数据记录的每个目标标签数据所存储的目标明文的索引信息。

在一些实施例中，从所述目标明文中获取所述多个目标标签数据包括：

根据多条目标数据记录的多个目标存储序号以及标签数据到明文的编码参数，确定每条目标数据记录的每个目标标签数据在目标明文的存储位置；

根据每条目标数据记录的每个目标标签数据在目标明文的存储位置，从所述目标明文中获取各个目标标签数据。

在一些实施例中，确定每条目标数据记录的每个目标标签数据在目标明文的存储位置包括：

根据标签数据到明文的编码参数，确定每个明文所能存储的比特数量；

根据每个明文所能存储的比特数量以及每个标签数据占用的比特数量，确定每个明文所能存储的标签数据的数量；

通过每条目标数据记录的每个目标存储序号对每个明文所能存储的标签数据的数量的取模运算，确定出每条目标数据记录的每个目标标签数据在目标明文的存储位置。

在一些实施例中，还包括：通过提高每个明文所能存储的比特数量和降低每个标

签数据占用的比特数量，增加每个明文所能存储的标签数据的数量。

在一些实施例中，通过提高明文的多项式次数、明文的多项式系数取值范围中的至少一项，提高每个明文所能存储的比特数量。

在一些实施例中，通过压缩编码方式，降低每个标签数据占用的比特数量。

在一些实施例中，确定第一加密标识数据集与第二加密标识数据集的交集包括：

按照相同的排序方式，对所述第一加密标识数据集中的加密标识数据和所述第二加密标识数据集中的加密标识数据进行升序排列或降序排列；

确定具有相同加密标识数据的第一加密标识数据集与第二加密标识数据集的交集。

在一些实施例中，数据查询方与数据提供方采用协商一致的加密方法分别对自己数据记录的标识数据进行加密生成加密标识数据。

在一些实施例中，所述目标明文的索引信息包括：

所述目标明文的索引；或者，

所述目标明文在各明文组成的明文矩阵的位置。

在一些实施例中，向数据提供方发起一次密文请求包括：将所述交集中的目标存储序号划分为一个或多个批次，每个批次包括一个或多个组，每个组的目标存储序号对应同一目标明文，不同组的目标存储序号对应不同目标明文，针对每个批次向数据提供方发起一次密文请求，其中携带该批次的各个组对应的各个目标明文的索引信息的密文；

在接收数据提供方返回的密文响应之后，对所述密文响应中的各个目标明文的密文进行解密得到该批次的各个目标明文。

在一些实施例中，还包括：数据提供方对所述目标明文的索引信息的密文进行茫然传输扩展得到所述目标明文的索引信息的密文的目标向量，将各明文组成的明文矩阵与所述目标向量进行矩阵运算得到所述目标明文的密文。

本公开一些实施例提出一种匿踪查询装置，包括：

交集确定单元，被配置为确定第一加密标识数据集与第二加密标识数据集的交集，其中，所述第一加密标识数据集包括数据提供方的每条数据记录的加密标识数据和存储序号，所述第二加密标识数据集包括数据查询方的每条数据记录的加密标识数据，每条数据记录包括标识数据和标签数据，数据提供方的每多条数据记录的多个标签数据被存储在一个明文；

密文请求单元，被配置为在根据所述交集中的多个目标存储序号判定相应多条目标数据记录的多个目标标签数据被存储在同一目标明文的情况下，针对所述多个目标存储序号，利用所述目标明文的索引信息的密文向数据提供方发起一次密文请求；

密文响应单元，被配置为接收数据提供方返回的密文响应，并对所述密文响应中的所述目标明文的密文进行解密得到所述目标明文；

数据获取单元，被配置为从所述目标明文中获取所述多个目标标签数据。

在一些实施例中，所述密文请求单元，被配置为判定多条目标数据记录的多个目标标签数据被存储在同一目标明文包括：

根据多条目标数据记录的多个目标存储序号以及标签数据到明文的编码参数，确定每条目标数据记录的每个目标标签数据所存储的目标明文的索引信息；

在多条目标数据记录的多个目标标签数据所存储的目标明文的索引信息相同的情况下，判定多条目标数据记录的多个目标标签数据被存储在同一目标明文。

在一些实施例中，所述数据获取单元，被配置为

根据多条目标数据记录的多个目标存储序号以及标签数据到明文的编码参数，确定每条目标数据记录的每个目标标签数据在目标明文的存储位置；

根据每条目标数据记录的每个目标标签数据在目标明文的存储位置，从所述目标明文中获取各个目标标签数据。

本公开一些实施例提出一种匿踪查询装置，包括：

存储器；以及，

耦接至所述存储器的处理器，所述处理器被配置为基于存储在所述存储器中的指令，执行匿踪查询方法。

本公开一些实施例提出一种匿踪查询系统，包括：用于数据查询方的匿踪查询装置，以及，用于数据提供方的数据提供装置。

本公开一些实施例提出一种非瞬时性计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现匿踪查询方法的步骤。

附图说明

下面将对实施例或相关技术描述中所需要使用的附图作简单地介绍。根据下面参照附图的详细描述，可以更加清楚地理解本公开。

显而易见地，下面描述中的附图仅仅是本公开的一些实施例，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他的附图。

图 1 示出本公开一些实施例的匿踪查询方法的流程示意图。

图 2 示出本公开一些实施例的匿踪查询系统的示意图。

图 3 示出本公开一些实施例的匿踪查询装置的结构示意图。

图 4 示出本公开另一些实施例的匿踪查询装置的结构示意图。

具体实施方式

下面将结合本公开实施例中的附图，对本公开实施例中的技术方案进行清楚、完整地描述。

除非特别说明，否则，本公开中的“第一”“第二”等描述用来区分不同的对象，并不用来表示大小或时序等含义。

本公开实施例的匿踪查询方案，通过加密标识数据求交集的方式，在不泄露双方隐私的情况下，确定数据提供方和数据查询方的数据记录的交集，如果判定交集中的多个目标存储序号相应的多个目标标签数据被存储在同一目标明文，针对这样的多个目标存储序号，利用目标明文的索引信息的密文向数据提供方发起一次密文请求，对密文响应中的目标明文的密文进行解密，从目标明文中可获取该多个目标标签数据。从而，通过一次密文请求和密文响应，可以同时获取多个目标标签数据，降低了通信开销和计算开销，进而使得匿踪查询方案能够高效运行。

需要说明的是，本公开的技术方案中，所涉及的用户个人信息的采集、收集、更新、分析、处理、使用、传输、存储等方面，均符合相关法律法规的规定，被用于合法的用途，且不违背公序良俗。对用户个人信息采取必要措施，防止对用户个人信息数据的非法访问，维护用户个人信息安全、网络安全和国家安全。

图 1 示出本公开一些实施例的匿踪查询方法的流程示意图。

如图 1 所示，该实施例的匿踪查询方法包括：步骤 110-170。

在步骤 110，数据查询方与数据提供方协商加密方法，用于对自己数据记录的标识数据进行加密生成加密标识数据。步骤 110-1 和步骤 110-2 给出了一种示例。

在步骤 110-1，数据查询方按照协商的加密方法，构造不经意伪随机函数（Oblivious Pseudo-Random Function，OPRF），该函数（设为 F）的密钥（也称种子）为 K，该不经意伪随机函数及其密钥用于对自己数据记录的标识数据进行加密生成加密标识数据。

或者，数据查询方按照协商的加密方法，构造哈希函数，该哈希函数用于对自己数据记录的标识数据进行加密生成加密标识数据。

在步骤 110-2，数据提供方按照协商的加密方法，构造不经意伪随机函数，该函数的密钥为 K，该不经意伪随机函数及其密钥用于对自己数据记录的标识数据进行加密生成加密标识数据。

或者，数据提供方按照协商的加密方法，构造哈希函数，该哈希函数用于对自己数据记录的标识数据进行加密生成加密标识数据。

其中，每条数据记录包括标识数据和标签数据。标识数据用来唯一标识一条数据记录，不同数据记录的标识数据也不同。标识数据例如包括但不限于用户标识、设备标识等能够起到标识作用的数据。标签数据是指数据记录的业务数据，业务数据是业务相关的数据，不同业务对应的业务数据也不同，本公开实施例并不限定业务数据的具体类型。

序号	身份号	人名	年龄
1	0001	人名 1	30
2	0002	人名 2	10
3	0003	人名 3	20

例如，上表有 3 条数据记录，身份号可以作为标识数据，人名和年龄可以作为标签数据。

数据记录的存储序号能够表征该数据记录存储在数据库的哪一行。在数据库更新之前，数据记录在数据库中的存储序号是固定不变的，利用存储序号可实现匿踪查询。

数据查询方的数据记录可以存储在数据查询方的数据库（DB1）。数据提供方的数据记录可以存储在数据提供方的数据库（DB2）。

在步骤 120，数据查询方和数据提供方采用协商一致的加密方法分别对自己数据记录的标识数据进行加密生成加密标识数据，并形成各自的加密标识数据集，数据提供方还将自己的加密标识数据集发送给数据查询方。步骤 120-1 和步骤 120-2 给出了一种示例。

在步骤 120-1，数据查询方按照协商的加密方法，例如利用不经意伪随机函数及其密钥或者利用哈希函数，对自己数据记录的标识数据（即，第二标识数据集 X）进行加密生成加密标识数据，形成第二加密标识数据集 H_X，所述第二加密标识数据集包括数据查询方的每条数据记录的加密标识数据。

在步骤 120-2，数据提供方按照协商的加密方法，例如利用不经意伪随机函数及其密钥或者利用哈希函数，对自己数据记录的标识数据（即，第一标识数据集 Y）进行加密生成加密标识数据，形成第一加密标识数据集 H_Y，并将第一加密标识数据集发送给数据查询方，所述第一加密标识数据集包括数据提供方的每条数据记录的加密标识数据和存储序号。

如果标识数据相同，则数据查询方和数据提供方针对该相同的标识数据会生成相同的加密标识数据，以便确定两方数据记录的交集。

在步骤 130，数据查询方确定第一加密标识数据集与第二加密标识数据集的交集 $X'=H_X \cap H_Y$，也即将第一加密标识数据集中与第二加密标识数据集具有相同加密标识数据的部分确定为第一加密标识数据集与第二加密标识数据集的交集。

在一些实施例中，确定第一加密标识数据集与第二加密标识数据集的交集包括：按照相同的排序方式，对所述第一加密标识数据集中的加密标识数据和所述第二加密标识数据集中的加密标识数据进行升序排列或降序排列；然后，确定具有相同加密标识数据的第一加密标识数据集与第二加密标识数据集的交集。从而，利用排序后的加密标识数据能更快地确定交集。

在步骤 140，数据提供方对自己的标签数据集 M’进行预处理得到明文数据 M，其中，数据提供方的每多条数据记录的多个标签数据被存储在一个明文。

其中，步骤 140 可以在数据提供方响应数据查询方的查询之前的任意步骤执行，也可以预先执行。

明文空间是一个剩余类多项式环$\mathbf{R_t = Z_t[x]/(x^n + 1)}$，它是一个 n 次多项式，系数是$\mathbf{0, 1, 2, \ldots, t-1}$ 等整数，系数的二进制表示时对应$\mathbf{logt}$比特，一个明文多项式可以储存$\mathbf{nlogt}$比特的数据。假设每个标签数据占用 S 比特，按存储序号排列的标签数据$\mathbf{y_1, y_2, \ldots, y_p}$，将它们长度对齐后，将所有标签数据共$\mathbf{P \times S}$个比特，按顺序每$\mathbf{nlogt}$比特放进一个明文多项式(即明文)中，一共得到$\mathbf{N = P \times S/(nlogt)}$个明文，从而完成标签数据到明文的编码。也即，对于某个标签数据来说，它会被存储在某个明文多项式（即明文）的若干个连续系数上。

其中，$\mathbf{nlogt/S}$表示一个明文多项式（即明文）所能存储的标签数据的数量，其为大于 1 的数值。通过提高每个明文所能存储的比特数量$\mathbf{nlogt}$和降低每个标签数据占用的比特数量 S，增加每个明文所能存储的标签数据的数量$\mathbf{nlogt/S}$。从而，进一步提高一次密文请求/响应所能获得的标签数据的数量，进一步降低了通信开销和计

算开销。其中，通过提高明文的多项式次数 n、明文的多项式系数取值范围 t 中的至少一项，提高每个明文所能存储的比特数量$\mathbf{nlogt}$。通过压缩编码方式，降低每个标签数据占用的比特数量 S。

假设：多项式取值空间为剩余类环$\mathbf{R_q = Z_q[x]/(x^n + 1)}$，它是一个 n 次多项式，系数是$\mathbf{0, 1, 2, \dots, q - 1}$ 等整数，明文多项式取值自$\mathbf{R_t = Z_t[x]/(x^n + 1)}$，它是一个 n 次多项式，系数是$\mathbf{0, 1, 2, \dots, t - 1}$ 等整数，$\boldsymbol{q \geq t}$。在全同态加密算法（如 BFV 算法）中，密态计算操作（如明密文相乘、密文旋转等）会增加噪声，消耗噪声预算，初始的噪声预算为$\mathbf{2logq/logt}$，因此明文系数范围 t 越大，初始预算越小，当增加的噪声累计超过初始噪声预算时，解密会失败，导致匿踪查询失败。因此，应当在不超过噪声预算的前提下选择尽量大的$\mathbf{logt}$。例如，每个标签占用 S=41 比特，n=2048 时，$\mathbf{logt}$最大可以取 16，超过 16 会导致匿踪查询失败。

在步骤 150，数据查询方在根据所述交集中的多个目标存储序号判定相应多条目标数据记录的多个目标标签数据被存储在同一目标明文的情况下，针对所述多个目标存储序号，利用所述目标明文的索引信息的密文向数据提供方发起一次密文请求。

数据查询方知晓数据提供方的数据标签到明文的编码方式，因此，数据查询方根据数据记录在数据提供方的存储序号，以及数据标签到明文的编码参数，可以确定该数据记录的标签数据被存储到哪个明文。

其中，判定多条目标数据记录的多个目标标签数据被存储在同一目标明文包括：根据多条目标数据记录的多个目标存储序号以及标签数据到明文的编码参数，确定每条目标数据记录的每个目标标签数据所存储的目标明文的索引信息；在多条目标数据记录的多个目标标签数据所存储的目标明文的索引信息相同的情况下，判定多条目标数据记录的多个目标标签数据被存储在同一目标明文。

其中，确定每条目标数据记录的每个目标标签数据所存储的目标明文的索引信息包括：根据标签数据到明文的编码参数，确定每个明文所能存储的比特数量；根据每个明文所能存储的比特数量以及每个标签数据占用的比特数量，确定每个明文所能存储的标签数据的数量；通过每条目标数据记录的每个目标存储序号对每个明文所能存储的标签数据的数量的除法运算，确定出每条目标数据记录的每个目标标签数据所存储的目标明文的索引信息。

其中，确定目标明文的索引信息可用以下公式表示：

$$\mathbf{index = \lfloor id/(nlogt/S) \rfloor},$$

其中，index 表示目标明文的索引，id 表示目标数据记录的目标存储序号，$\mathbf{nlogt}$ 表示根据编码参数（多项式次数 n、明文的多项式系数取值范围 t）确定的每个明文所能存储的比特数量，S 表示每个标签数据占用的比特数量，$\mathbf{nlogt/S}$表示每个明文所能存储的标签数据的数量，$\lfloor\ \ \rfloor$表示向下取整。

从 index 的公式可以看出，连续的$\mathbf{nlogt/S}$个存储序号相应的标签数据对应一个明文；相应的，针对连续的$\mathbf{nlogt/S}$个存储序号中的任意一个或多个存储序号，利用这些存储序号对应的同一明文的索引信息，可以向数据提供方发起一次密文请求。

目标明文的索引 index 还可以转换为目标明文 M[i,j]在各明文组成的明文矩阵 M 的位置[i,j]，其中，$\mathbf{i = index/T}$，$\mathbf{j = index\ mod\ T}$，T 表示矩阵 M 的维数，假设对标签数据编码共得到 N 个明文，则$\mathbf{T = \sqrt{N}}$。

综上所述，本实施例中的目标明文的索引信息有两种形式，第一种是目标明文的索引 index，第二种是目标明文在各明文组成的明文矩阵的位置[i,j]。第二种的矩阵形式的明文查询定位方式相对于第一种的向量形式的明文查询定位方式，由于矩阵可以从行/列两个维度同时定位、且矩阵单一维度的长度远小于一维向量的长度，因此，利用第二种方式可以更快地查询定位目标明文，提高查询效率。

数据查询方在根据所述交集中的多个目标存储序号判定相应多条目标数据记录的多个目标标签数据被存储在同一目标明文的情况下，针对所述多个目标存储序号，利用所述目标明文的索引信息的密文向数据提供方发起一次密文请求。

假设交集中的多个目标存储序号（例如 id2、id4）的目标标签数据被存储在同一目标明文，利用前述公式$\mathbf{index = \lfloor id/(nlogt/S) \rfloor}$可以确定目标明文的索引$\mathbf{index}$，还可以利用前述公式$\mathbf{i = index/T}$，$\mathbf{j = index\ mod\ T}$，根据需要确定目标明文 M[i,j]在各明文组成的明文矩阵 M 的位置[i,j]。

如果采用向量形式的明文查询定位方式，则数据查询方利用自身公钥进行同态加密（如 BFV 加密）得到$\mathbf{Enc}\left(\mathbf{x}^{\mathbf{index}}\right)$一条密文，作为密文请求，序列化后发送给数据提供方。

如果采用矩阵形式的明文查询定位方式，则数据查询方利用自身公钥进行同态加密（如 BFV 加密）得到$\mathbf{Enc}(\mathbf{x}^{\mathbf{i}}), \mathbf{Enc}(\mathbf{x}^{\mathbf{j}})$两条密文，作为密文请求，序列化后发送给数据提供方。

其中，步骤 150 中的加密用的公钥与步骤 170 中解密用的私钥为数据查询方的同态加密的密钥对。同态加密能够基于密文进行加法、数乘、乘法和旋转等操作。例

如，$Enc(a+b)=Enc(a)+Enc(b);k\times Enc(a)=Enc(k\times a)$，其中，$Enc$表示同态加密操作。

在步骤 160，数据提供方对所述目标明文的索引信息的密文进行茫然传输扩展得到所述目标明文的索引信息的密文的目标向量，将各明文组成的明文矩阵与所述目标向量进行矩阵运算得到所述目标明文的密文，并通过密文响应返回给数据查询方。

如果采用矩阵形式的明文查询定位方式，数据提供方反序列化接收到的数据查询方的数据，利用数据查询方提供的 Galois 密钥，对接收到的两条密文$\mathbf{Enc(x^i),Enc(x^j)}$进行“茫然传输扩展”得到两条维数为 T 的列向量，形式如$\mathbf{\left(Enc(0),\dots,Enc(1),\dots,Enc(0)\right)}$，由 0 的密文和 1 的密文组成，其中 1 的密文仅出现一次：对于$\mathbf{Enc(x^i)}$而言，1 的密文出现在第$\mathbf{i}$个位置上，对于$\mathbf{Enc(x^j)}$而言，1 的密文出现在第$\mathbf{j}$个位置上，由于同态加密的语义安全性，对于数据提供方来说，无法判断 1 的密文位置，从而无法得知数据查询方想要查询的$\mathbf{i,j}$。

然后，数据提供方将明文矩阵 M 和以上两条密文向量进行矩阵-向量乘，即同态加密的明文密文相乘操作，假设得到 R 条密文$\mathbf{C_1,C_2,\dots,C_R}$，R 是密文膨胀系数，作为目标明文 M[i,j]的密文响应，序列化后发送给数据查询方。

如果采用向量形式的明文查询定位方式，数据提供方反序列化接收到的数据查询方的数据，利用数据查询方提供的 Galois 密钥，对接收到的一条密文$\mathbf{Enc\left(x^{index}\right)}$进行“茫然传输扩展”得到一条维数为 N 的列向量，形式如$\mathbf{\left(Enc(0),\dots,Enc(1),\dots,Enc(0)\right)}$，由 0 的密文和 1 的密文组成，其中 1 的密文仅出现一次，对于$\mathbf{Enc\left(x^{index}\right)}$而言，1 的密文出现在第$\mathbf{index}$个位置上，由于同态加密的语义安全性，对于数据提供方来说，无法判断 1 的密文位置，从而无法得知数据查询方想要查询的$\mathbf{index}$。

然后，数据提供方将各明文组成的明文向量和以上一条密文向量进行向量-向量乘，即同态加密的明文密文相乘操作，假设得到$\mathbf{R'}$条密文$\mathbf{C_1,C_2,\dots,C_{R'}}$，$\mathbf{R'}$是密文膨胀系数，作为目标明文 M[i,j]的密文响应，序列化后发送给数据查询方。

在步骤 170，数据查询方接收数据提供方返回的密文响应，并对所述密文响应中的所述目标明文的密文进行解密得到所述目标明文，并从所述目标明文中获取所述多个目标标签数据，可以将获取的目标标签数据存储到数据库 DB1。从而，数据查询方可以利用自己的标签数据和数据提供方的标签数据开展业务。

数据查询方反序列化接收到的密文响应，利用自身的私钥，对 R 条密文进行组合

并解密，或者，对$\mathbf{R'}$条密文进行组合并解密，均可以得到目标明文M[i,j]，然后，根据标签数据到明文的编码方式，对目标明文M[i,j]进行解码，即可得到多个目标存储序号的多个标签数据。

其中，通过解码，从所述目标明文中获取所述多个目标标签数据包括：根据多条目标数据记录的多个目标存储序号以及标签数据到明文的编码参数，确定每条目标数据记录的每个目标标签数据在目标明文的存储位置；根据每条目标数据记录的每个目标标签数据在目标明文的存储位置，从所述目标明文中获取各个目标标签数据。

其中，确定每条目标数据记录的每个目标标签数据在目标明文的存储位置包括：根据标签数据到明文的编码参数，确定每个明文所能存储的比特数量；根据每个明文所能存储的比特数量以及每个标签数据占用的比特数量，确定每个明文所能存储的标签数据的数量；通过每条目标数据记录的每个目标存储序号对每个明文所能存储的标签数据的数量的取模运算，确定出每条目标数据记录的每个目标标签数据在目标明文的存储位置。

其中，确定目标标签数据在目标明文的存储位置可以用以下公式表示：

$$\mathbf{offset = id \bmod (nlogt/S)},$$

其中，偏置$\mathbf{offset}$表示目标标签数据在目标明文的起始存储位置，id表示目标数据记录的目标存储序号，$\mathbf{nlogt}$表示根据编码参数（多项式次数n、明文的多项式系数取值范围t）确定的每个明文所能存储的比特数量，S表示每个标签数据占用的比特数量，$\mathbf{nlogt/S}$表示每个明文所能存储的标签数据的数量，$\mathbf{mod}$表示取模运算。

在知晓目标标签数据在目标明文的起始存储位置$\mathbf{offset}$、以及每个标签数据占用的比特数量S的情况下，就可以从目标明文中提取出相应的目标标签数据。

在一些实施例中，数据查询方可以针对交集中每个批次的存储序号发起一次密文请求。具体来说，数据查询方将所述交集中的目标存储序号划分为一个或多个批次，每个批次包括一个或多个组，每个组的目标存储序号对应同一目标明文，不同组的目标存储序号对应不同目标明文，针对每个批次向数据提供方发起一次密文请求，其中携带该批次的各个组对应的各个目标明文的索引信息的密文。相应的，后续数据查询方在接收数据提供方返回的密文响应之后，对所述密文响应中的各个目标明文的密文进行解密得到该批次的各个目标明文，然后从每个目标明文中分别获取相应的目标标签数据。在一个批次对应多个目标明文的情况下，可进一步降低通信开销。其中，批次尺寸参数（batchsize，即每个批次的组的数量）可以灵活设置。此外，数据查询方

可以利用 unordered_map 的数据结构，将目标明文的索引信息（index 或[i, j]）作为键，将目标标签数据在目标明文的起始存储位置（即偏置**offset**）作为值，进行存储，方便查找。

本公开实施例的匿踪查询方案，通过加密标识数据求交集的方式，在不泄露双方隐私的情况下，确定数据提供方和数据查询方的数据记录的交集，如果判定交集中的多个目标存储序号相应的多个目标标签数据被存储在同一目标明文，针对这样的多个目标存储序号，利用目标明文的索引信息的密文向数据提供方发起一次密文请求，对密文响应中的目标明文的密文进行解密，从目标明文中可获取该多个目标标签数据。从而，通过一次密文请求和密文响应，可以同时获取多个目标标签数据，降低了通信开销和计算开销。

下面对通信开销和计算开销进行对比分析。假设采用矩阵形式的明文查询定位方式，请求需要传输 2 个密文，响应需要传输 R 个密文，每个密文大小假设为 c，如果查询 P 个数据记录。

按照相关技术的方案，数据查询方和数据提供方的密文通信开销为$(\mathbf{R}+\mathbf{2})\times\mathbf{P}\times\mathbf{C}$。按照本公开实施例的方案，假设平均下来 s 个数据记录在同一个密文请求中查询，则数据查询方和数据提供方的密文通信开销为$(\mathbf{R}+\mathbf{2})\times\mathbf{P}\times\mathbf{C}/\mathbf{s}$。可见，本公开实施例的方案极大地减少了密文通信开销。

对于对应同一明文的多个数据记录，本公开实施例的方案需要一次密态计算，而相关技术的方案需要多次密态计算，因此，本公开实施例的方案极大地减少了计算开销。

图 2 示出本公开一些实施例的匿踪查询系统的示意图。

如图 2 所示，该实施例的匿踪查询系统 200 包括：用于数据查询方的匿踪查询装置 210，以及，用于数据提供方的数据提供装置 220。

匿踪查询装置 210，被配置为确定第一加密标识数据集与第二加密标识数据集的交集，其中，所述第一加密标识数据集包括数据提供方的每条数据记录的加密标识数据和存储序号，所述第二加密标识数据集包括数据查询方的每条数据记录的加密标识数据，每条数据记录包括标识数据和标签数据，数据提供方的每多条数据记录的多个标签数据被存储在一个明文；

在根据所述交集中的多个目标存储序号判定相应多条目标数据记录的多个目标标签数据被存储在同一目标明文的情况下，针对所述多个目标存储序号，利用所述目

标明文的索引信息的密文向数据提供方发起一次密文请求；

接收数据提供方返回的密文响应，并对所述密文响应中的所述目标明文的密文进行解密得到所述目标明文；

从所述目标明文中获取所述多个目标标签数据。

匿踪查询装置 210，被配置为判定多条目标数据记录的多个目标标签数据被存储在同一目标明文包括：

根据多条目标数据记录的多个目标存储序号以及标签数据到明文的编码参数，确定每条目标数据记录的每个目标标签数据所存储的目标明文的索引信息；

在多条目标数据记录的多个目标标签数据所存储的目标明文的索引信息相同的情况下，判定多条目标数据记录的多个目标标签数据被存储在同一目标明文。

匿踪查询装置 210，被配置为确定每条目标数据记录的每个目标标签数据所存储的目标明文的索引信息包括：

根据标签数据到明文的编码参数，确定每个明文所能存储的比特数量；

根据每个明文所能存储的比特数量以及每个标签数据占用的比特数量，确定每个明文所能存储的标签数据的数量；

通过每条目标数据记录的每个目标存储序号对每个明文所能存储的标签数据的数量的除法运算，确定出每条目标数据记录的每个目标标签数据所存储的目标明文的索引信息。

匿踪查询装置 210，被配置为从所述目标明文中获取所述多个目标标签数据包括：

根据多条目标数据记录的多个目标存储序号以及标签数据到明文的编码参数，确定每条目标数据记录的每个目标标签数据在目标明文的存储位置；

根据每条目标数据记录的每个目标标签数据在目标明文的存储位置，从所述目标明文中获取各个目标标签数据。

匿踪查询装置 210，被配置为确定每条目标数据记录的每个目标标签数据在目标明文的存储位置包括：

根据标签数据到明文的编码参数，确定每个明文所能存储的比特数量；

根据每个明文所能存储的比特数量以及每个标签数据占用的比特数量，确定每个明文所能存储的标签数据的数量；

通过每条目标数据记录的每个目标存储序号对每个明文所能存储的标签数据的数量的取模运算，确定出每条目标数据记录的每个目标标签数据在目标明文的存储位

置。

匿踪查询装置 210，被配置为通过提高每个明文所能存储的比特数量和降低每个标签数据占用的比特数量，增加每个明文所能存储的标签数据的数量。

匿踪查询装置 210，被配置为通过提高明文的多项式次数、明文的多项式系数取值范围中的至少一项，提高每个明文所能存储的比特数量；或者，通过压缩编码方式，降低每个标签数据占用的比特数量。

匿踪查询装置 210，被配置为确定第一加密标识数据集与第二加密标识数据集的交集包括：

按照相同的排序方式，对所述第一加密标识数据集中的加密标识数据和所述第二加密标识数据集中的加密标识数据进行升序排列或降序排列；

确定具有相同加密标识数据的第一加密标识数据集与第二加密标识数据集的交集。

数据查询方与数据提供方采用协商一致的加密方法分别对自己数据记录的标识数据进行加密生成加密标识数据。

所述目标明文的索引信息包括：所述目标明文的索引；或者，所述目标明文在各明文组成的明文矩阵的位置。

匿踪查询装置 210，被配置为向数据提供方发起一次密文请求包括：将所述交集中的目标存储序号划分为一个或多个批次，每个批次包括一个或多个组，每个组的目标存储序号对应同一目标明文，不同组的目标存储序号对应不同目标明文，针对每个批次向数据提供方发起一次密文请求，其中携带该批次的各个组对应的各个目标明文的索引信息的密文；在接收数据提供方返回的密文响应之后，对所述密文响应中的各个目标明文的密文进行解密得到该批次的各个目标明文。

数据提供装置 220，被配置为：对所述目标明文的索引信息的密文进行茫然传输扩展得到所述目标明文的索引信息的密文的目标向量，将各明文组成的明文矩阵与所述目标向量进行矩阵运算得到所述目标明文的密文。

图 3 示出本公开一些实施例的匿踪查询装置的结构示意图。

如图 3 所示，该实施例的匿踪查询装置 210 包括：单元 310-340。

交集确定单元 310，被配置为确定第一加密标识数据集与第二加密标识数据集的交集，其中，所述第一加密标识数据集包括数据提供方的每条数据记录的加密标识数据和存储序号，所述第二加密标识数据集包括数据查询方的每条数据记录的加密标识

数据，每条数据记录包括标识数据和标签数据，数据提供方的每多条数据记录的多个标签数据被存储在一个明文；

密文请求单元 320，被配置为在根据所述交集中的多个目标存储序号判定相应多条目标数据记录的多个目标标签数据被存储在同一目标明文的情况下，针对所述多个目标存储序号，利用所述目标明文的索引信息的密文向数据提供方发起一次密文请求；

密文响应单元 330，被配置为接收数据提供方返回的密文响应，并对所述密文响应中的所述目标明文的密文进行解密得到所述目标明文；

数据获取单元 340，被配置为从所述目标明文中获取所述多个目标标签数据。

其中，所述密文请求单元 320，被配置为判定多条目标数据记录的多个目标标签数据被存储在同一目标明文包括：

根据多条目标数据记录的多个目标存储序号以及标签数据到明文的编码参数，确定每条目标数据记录的每个目标标签数据所存储的目标明文的索引信息；

在多条目标数据记录的多个目标标签数据所存储的目标明文的索引信息相同的情况下，判定多条目标数据记录的多个目标标签数据被存储在同一目标明文。

其中，所述密文请求单元 320，被配置为确定每条目标数据记录的每个目标标签数据所存储的目标明文的索引信息包括：

根据标签数据到明文的编码参数，确定每个明文所能存储的比特数量；

根据每个明文所能存储的比特数量以及每个标签数据占用的比特数量，确定每个明文所能存储的标签数据的数量；

通过每条目标数据记录的每个目标存储序号对每个明文所能存储的标签数据的数量的除法运算，确定出每条目标数据记录的每个目标标签数据所存储的目标明文的索引信息。

其中，所述数据获取单元 340，被配置为：

根据多条目标数据记录的多个目标存储序号以及标签数据到明文的编码参数，确定每条目标数据记录的每个目标标签数据在目标明文的存储位置；

根据每条目标数据记录的每个目标标签数据在目标明文的存储位置，从所述目标明文中获取各个目标标签数据。

其中，所述数据获取单元 340，被配置为：确定每条目标数据记录的每个目标标签数据在目标明文的存储位置包括：

根据标签数据到明文的编码参数，确定每个明文所能存储的比特数量；

根据每个明文所能存储的比特数量以及每个标签数据占用的比特数量，确定每个明文所能存储的标签数据的数量；

通过每条目标数据记录的每个目标存储序号对每个明文所能存储的标签数据的数量的取模运算，确定出每条目标数据记录的每个目标标签数据在目标明文的存储位置。

通过提高每个明文所能存储的比特数量和降低每个标签数据占用的比特数量，增加每个明文所能存储的标签数据的数量。通过提高明文的多项式次数、明文的多项式系数取值范围中的至少一项，提高每个明文所能存储的比特数量。通过压缩编码方式，降低每个标签数据占用的比特数量。

交集确定单元 310，被配置为按照相同的排序方式，对所述第一加密标识数据集中的加密标识数据和所述第二加密标识数据集中的加密标识数据进行升序排列或降序排列；确定具有相同加密标识数据的第一加密标识数据集与第二加密标识数据集的交集。

密文请求单元 320，被配置为向数据提供方发起一次密文请求包括：将所述交集中的目标存储序号划分为一个或多个批次，每个批次包括一个或多个组，每个组的目标存储序号对应同一目标明文，不同组的目标存储序号对应不同目标明文，针对每个批次向数据提供方发起一次密文请求，其中携带该批次的各个组对应的各个目标明文的索引信息的密文；密文响应单元 330，被配置为在接收数据提供方返回的密文响应之后，对所述密文响应中的各个目标明文的密文进行解密得到该批次的各个目标明文。

图 4 示出本公开另一些实施例的匿踪查询装置的结构示意图。

如图 4 所示，该实施例的匿踪查询装置 210 包括：存储器 410 以及耦接至该存储器 410 的处理器 420，处理器 420 被配置为基于存储在存储器 410 中的指令，执行前述任意一些实施例中的匿踪查询方法。

匿踪查询装置 210 还可以包括输入输出接口 430、网络接口 440、存储接口 450 等。这些接口 430，440，450 以及存储器 410 和处理器 420 之间例如可以通过总线 460 连接。

其中，存储器 410 例如可以包括系统存储器、固定非易失性存储介质等。系统存储器例如存储有操作系统、应用程序、引导装载程序（Boot Loader）以及其他程序等。

其中，处理器 420 可以用通用处理器、数字信号处理器（Digital Signal Processor，DSP）、应用专用集成电路（Application Specific Integrated Circuit，ASIC）、现场可

编程门阵列（Field Programmable Gate Array ，FPGA）或其它可编程逻辑设备、分立门或晶体管等分立硬件组件方式来实现。

其中，输入输出接口 430 为显示器、鼠标、键盘、触摸屏等输入输出设备提供连接接口。网络接口 440 为各种联网设备提供连接接口。存储接口 450 为 SD 卡、U 盘等外置存储设备提供连接接口。总线 460 可以使用多种总线结构中的任意总线结构。例如，总线结构包括但不限于工业标准体系结构（Industry Standard Architecture，ISA）总线、微通道体系结构（Micro Channel Architecture，MCA）总线、外围组件互连（Peripheral Component Interconnect，PCI）总线。

需要说明的是，本公开的技术方案中，所涉及的用户个人信息的获取、存储和应用等，均符合相关法律法规的规定，且不违背公序良俗。

本领域内的技术人员应当明白，本公开的实施例可提供为方法、系统、或计算机程序产品。因此，本公开可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本公开可采用在一个或多个其中包含有计算机程序代码的非瞬时性计算机可读存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

本公开是参照根据本公开实施例的方法、设备（系统）、和计算机程序产品的流程图和 / 或方框图来描述的。应理解为可由计算机程序指令实现流程图和 / 或方框图中的每一流程和 / 或方框、以及流程图和 / 或方框图中的流程和 / 或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的步骤。

以上所述仅为本公开的较佳实施例，并不用以限制本公开，凡在本公开的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本公开的保护范围之内。

权 利 要 求

1. 一种匿踪查询方法，包括：

确定第一加密标识数据集与第二加密标识数据集的交集，其中，所述第一加密标识数据集包括数据提供方的每条数据记录的加密标识数据和存储序号，所述第二加密标识数据集包括数据查询方的每条数据记录的加密标识数据，每条数据记录包括标识数据和标签数据，数据提供方的每多条数据记录的多个标签数据被存储在一个明文；

在根据所述交集中的多个目标存储序号判定相应多条目标数据记录的多个目标标签数据被存储在同一目标明文的情况下，针对所述多个目标存储序号，利用所述目标明文的索引信息的密文向数据提供方发起一次密文请求；

接收数据提供方返回的密文响应，并对所述密文响应中的所述目标明文的密文进行解密得到所述目标明文；

从所述目标明文中获取所述多个目标标签数据。

2. 根据权利要求 1 所述的匿踪查询方法，其中，判定相应多条目标数据记录的多个目标标签数据被存储在同一目标明文包括：

根据多条目标数据记录的多个目标存储序号以及标签数据到明文的编码参数，确定每条目标数据记录的每个目标标签数据所存储的目标明文的索引信息；

在多条目标数据记录的多个目标标签数据所存储的目标明文的索引信息相同的情况下，判定多条目标数据记录的多个目标标签数据被存储在同一目标明文。

3. 根据权利要求 2 所述的匿踪查询方法，其中，确定每条目标数据记录的每个目标标签数据所存储的目标明文的索引信息包括：

根据标签数据到明文的编码参数，确定每个明文所能存储的比特数量；

根据每个明文所能存储的比特数量以及每个标签数据占用的比特数量，确定每个明文所能存储的标签数据的数量；

通过每条目标数据记录的每个目标存储序号对每个明文所能存储的标签数据的数量的除法运算，确定出每条目标数据记录的每个目标标签数据所存储的目标明文的索引信息。

4. 根据权利要求 1-3 任一项所述的匿踪查询方法，其中，从所述目标明文中获取所述多个目标标签数据包括：

根据多条目标数据记录的多个目标存储序号以及标签数据到明文的编码参数，确定每条目标数据记录的每个目标标签数据在目标明文的存储位置；

根据每条目标数据记录的每个目标标签数据在目标明文的存储位置，从所述目标明文中获取各个目标标签数据。

5. 根据权利要求 4 所述的匿踪查询方法，其中，确定每条目标数据记录的每个目标标签数据在目标明文的存储位置包括：

根据标签数据到明文的编码参数，确定每个明文所能存储的比特数量；

根据每个明文所能存储的比特数量以及每个标签数据占用的比特数量，确定每个明文所能存储的标签数据的数量；

通过每条目标数据记录的每个目标存储序号对每个明文所能存储的标签数据的数量的取模运算，确定出每条目标数据记录的每个目标标签数据在目标明文的存储位置。

6. 根据权利要求 3 或 5 所述的匿踪查询方法，还包括：

通过提高每个明文所能存储的比特数量和降低每个标签数据占用的比特数量，增加每个明文所能存储的标签数据的数量。

7. 根据权利要求 6 所述的匿踪查询方法，其中，

通过提高明文的多项式次数、明文的多项式系数取值范围中的至少一项，提高每个明文所能存储的比特数量；或者，

通过压缩编码方式，降低每个标签数据占用的比特数量。

8. 根据权利要求 1-7 任一项所述的匿踪查询方法，其中，确定第一加密标识数据集与第二加密标识数据集的交集包括：

按照相同的排序方式，对所述第一加密标识数据集中的加密标识数据和所述第二加密标识数据集中的加密标识数据进行升序排列或降序排列；

将第一加密标识数据集中与第二加密标识数据集具有相同加密标识数据的部分

确定为第一加密标识数据集与第二加密标识数据集的交集。

9. 根据权利要求 1-8 任一项所述的匿踪查询方法，其中，数据查询方与数据提供方采用协商一致的加密方法分别对自己数据记录的标识数据进行加密生成加密标识数据。

10. 根据权利要求 1-9 任一项所述的匿踪查询方法，其中，所述目标明文的索引信息包括：

所述目标明文的索引；或者，

所述目标明文在各明文组成的明文矩阵的位置。

11. 根据权利要求 1-10 任一项所述的匿踪查询方法，其中，向数据提供方发起一次密文请求包括：将所述交集中的目标存储序号划分为一个或多个批次，每个批次包括一个或多个组，每个组的目标存储序号对应同一目标明文，不同组的目标存储序号对应不同目标明文，针对每个批次向数据提供方发起一次密文请求，其中携带该批次的各个组对应的各个目标明文的索引信息的密文；

在接收数据提供方返回的密文响应之后，对所述密文响应中的各个目标明文的密文进行解密得到该批次的各个目标明文。

12. 根据权利要求 1-11 任一项所述的匿踪查询方法，还包括：

数据提供方对所述目标明文的索引信息的密文进行茫然传输扩展得到所述目标明文的索引信息的密文的目标向量，将各明文组成的明文矩阵与所述目标向量进行矩阵运算得到所述目标明文的密文。

13. 根据权利要求 1-12 任一项所述的匿踪查询方法，其中：

所述目标明文的索引信息的密文是利用同态加密的密钥对中的公钥对所述目标明文的索引信息进行加密得到的，

所述目标明文是利用同态加密的密钥对中的私钥对所述目标明文的密文进行解密得到的。

14. 一种匿踪查询装置，包括：

交集确定单元，被配置为确定第一加密标识数据集与第二加密标识数据集的交集，其中，所述第一加密标识数据集包括数据提供方的每条数据记录的加密标识数据和存储序号，所述第二加密标识数据集包括数据查询方的每条数据记录的加密标识数据，每条数据记录包括标识数据和标签数据，数据提供方的每多条数据记录的多个标签数据被存储在一个明文；

密文请求单元，被配置为在根据所述交集中的多个目标存储序号判定相应多条目标数据记录的多个目标标签数据被存储在同一目标明文的情况下，针对所述多个目标存储序号，利用所述目标明文的索引信息的密文向数据提供方发起一次密文请求；

密文响应单元，被配置为接收数据提供方返回的密文响应，并对所述密文响应中的所述目标明文的密文进行解密得到所述目标明文；

数据获取单元，被配置为从所述目标明文中获取所述多个目标标签数据。

15. 根据权利要求 14 所述的匿踪查询装置，其中，所述密文请求单元，被配置为判定相应多条目标数据记录的多个目标标签数据被存储在同一目标明文包括：

根据多条目标数据记录的多个目标存储序号以及标签数据到明文的编码参数，确定每条目标数据记录的每个目标标签数据所存储的目标明文的索引信息；

在多条目标数据记录的多个目标标签数据所存储的目标明文的索引信息相同的情况下，判定多条目标数据记录的多个目标标签数据被存储在同一目标明文。

16. 根据权利要求 14 所述的匿踪查询装置，其中，所述数据获取单元，被配置为

根据多条目标数据记录的多个目标存储序号以及标签数据到明文的编码参数，确定每条目标数据记录的每个目标标签数据在目标明文的存储位置；

根据每条目标数据记录的每个目标标签数据在目标明文的存储位置，从所述目标明文中获取各个目标标签数据。

17. 一种匿踪查询装置，包括：

存储器；以及，

耦接至所述存储器的处理器，所述处理器被配置为基于存储在所述存储器中的指

令，执行权利要求 1-11、13 中任一项所述的匿踪查询方法。

18. 一种匿踪查询系统，包括：

用于数据查询方的匿踪查询装置，被配置为执行权利要求 1-11 中任一项所述的匿踪查询方法；以及，

用于数据提供方的数据提供装置，被配置为执行权利要求 12 所述的匿踪查询方法。

19. 一种非瞬时性计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现权利要求 1-13 中任一项所述的匿踪查询方法的步骤。

20. 一种计算机程序，包括：

指令，所述指令由处理器执行时使所述处理器执行根据权利要求 1-13 中任一项所述的匿踪查询方法。

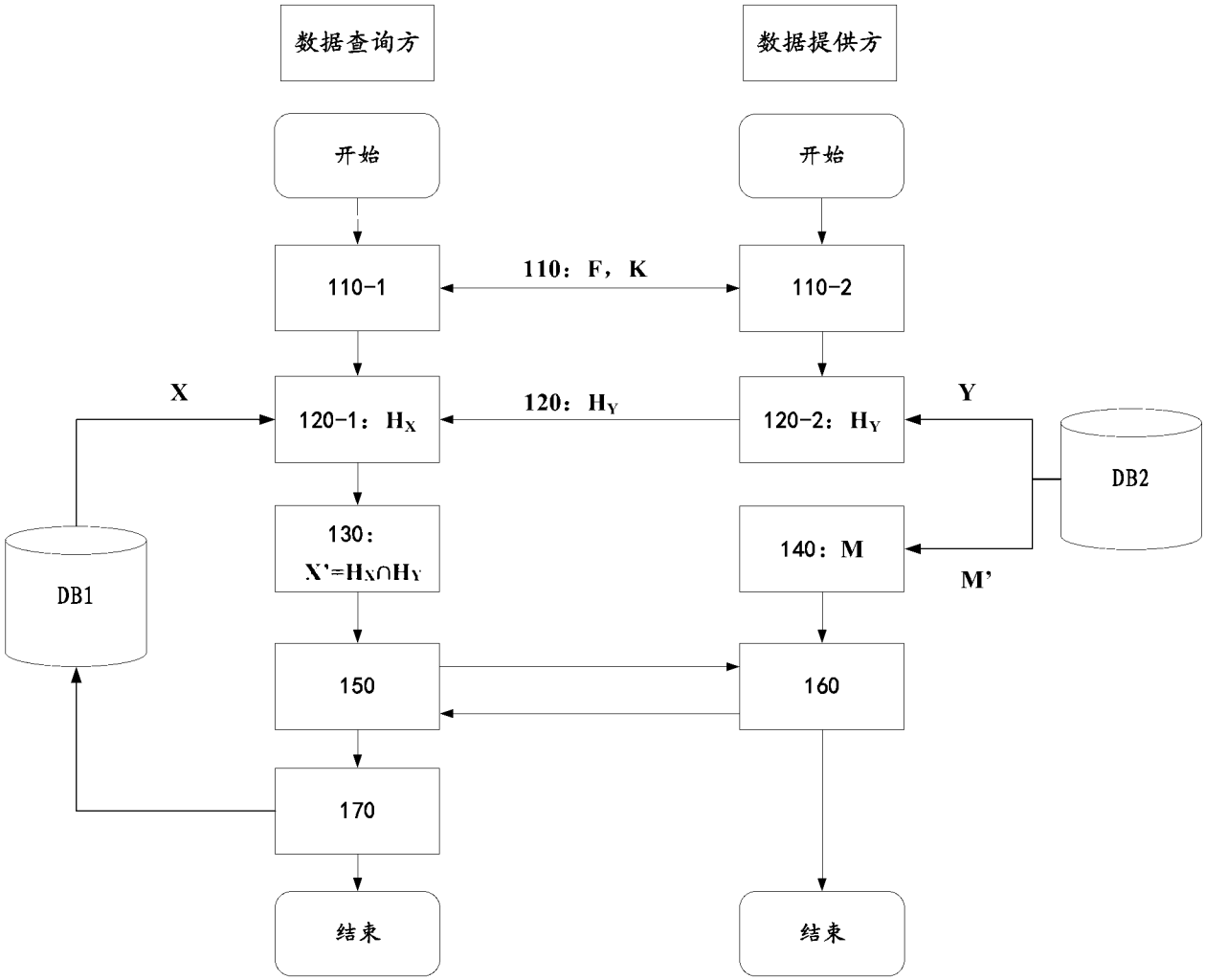
数据查询方
数据提供方
开始
开始
110-1
110：F，K
110-2
X
120-1：H_X
120：H_Y
120-2：H_Y
Y
DB2
130：
$X'=H_X \cap H_Y$
140：M
M'
DB1
150
160
170
结束
结束

图 1

200


匿踪查询装置
210
数据提供装置
220

图 2

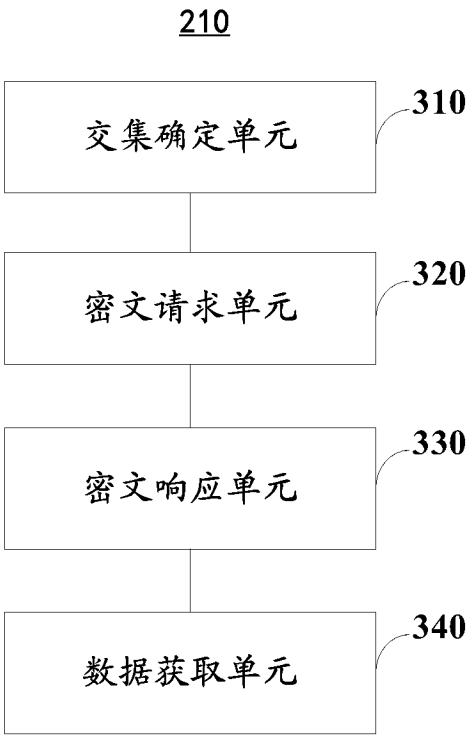
210
交集确定单元
310
密文请求单元
320
密文响应单元
330
数据获取单元
340

图 3

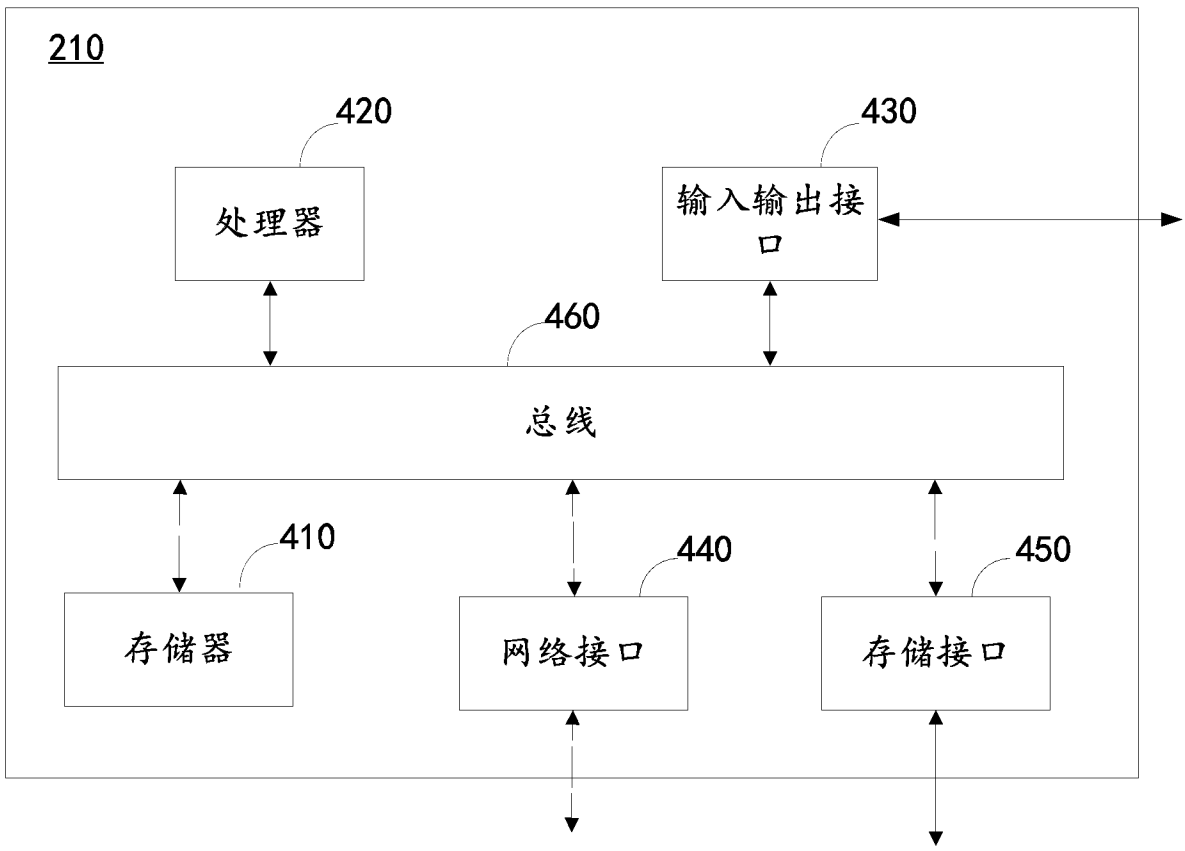
210
420
处理器
430
输入输出接口
460
总线
410
存储器
440
网络接口
450
存储接口

图 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2023/094279

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/62(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC:G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS; CNTXT; VEN; DWPI; USTXT; WOTXT; EPTXT; CNKI: 隐匿, 索引, 明文, 加密, 交集, 解密, 多项式, privacy, index, plain, encrypt, intersection, decrypt, polynomial

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 115688167 A (BEIJING WODONG TIANJUN INFORMATION TECHNOLOGY CO., LTD. et al.) 03 February 2023 (2023-02-03) description, paragraphs 62-179, and figures 1-4	1-20
A	CN 114065271 A (ALIBABA HEALTH INFORMATION TECHNOLOGY LTD.) 18 February 2022 (2022-02-18) description, paragraphs 29-123, and figures 1-8	1-20
A	CN 112699384 A (SHANDONG UNIVERSITY) 23 April 2021 (2021-04-23) description, paragraphs 42-127, and figures 1-7	1-20
A	CN 114722049 A (HUAKONG TSINGJIAO INFORMATION SCIENCE (BEIJING) CO., LTD.) 08 July 2022 (2022-07-08) entire document	1-20
A	US 2015172258 A1 (KABUSHIKI KAISHA TOSHIBA) 18 June 2015 (2015-06-18) entire document	1-20

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"D" document cited by the applicant in the international application
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 July 2023	**14 August 2023**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **China No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2023/094279

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 115688167 A	03 February 2023	None	
CN 114065271 A	18 February 2022	None	
CN 112699384 A	23 April 2021	None	
CN 114722049 A	08 July 2022	CN 114722049 B	12 August 2022
US 2015172258 A1	18 June 2015	US 9413729 B2	09 August 2016
		JP 2015114629 A	22 June 2015
		JP 6173904 B2	02 August 2017

国际检索报告

国际申请号
PCT/CN2023/094279

A. 主题的分类

G06F 21/62(2013.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC:G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNABS;CNTXT;VEN;DWPI;USTXT;WOTXT;EPTXT;CNKI:隐匿，索引，明文，加密，交集，解密，多项式，privacy，index，plain，encrypt，intersection，decrypt，polynomial

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 115688167 A (北京沃东天骏信息技术有限 等) 2023年2月3日 (2023 - 02 - 03) 说明书第62-179段，图1-4	1-20
A	CN 114065271 A (阿里健康信息技术有限公司) 2022年2月18日 (2022 - 02 - 18) 说明书第29-123段，图1-8	1-20
A	CN 112699384 A (山东大学) 2021年4月23日 (2021 - 04 - 23) 说明书第42-127段，图1-7	1-20
A	CN 114722049 A (华控清交信息科技（北京）有限公司) 2022年7月8日 (2022 - 07 - 08) 全文	1-20
A	US 2015172258 A1 (KABUSHIKI KAISHA TOSHIBA) 2015年6月18日 (2015 - 06 - 18) 全文	1-20

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“D” 申请人在国际申请中引证的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2023年7月25日	2023年8月14日
ISA/CN的名称和邮寄地址 中国国家知识产权局 中国北京市海淀区蓟门桥西土城路6号 100088	受权官员 赵畅 电话号码 (+86) 020-28958965

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2023/094279

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	115688167	A	2023年2月3日	无			
CN	114065271	A	2022年2月18日	无			
CN	112699384	A	2021年4月23日	无			
CN	114722049	A	2022年7月8日	CN	114722049	B	2022年8月12日
US	2015172258	A1	2015年6月18日	US	9413729	B2	2016年8月9日
				JP	2015114629	A	2015年6月22日
				JP	6173904	B2	2017年8月2日