

(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
2023 年 2 月 9 日 (09.02.2023)



(10) 国际公布号
WO 2023/010273 A1

(51) 国际专利分类号:
G06F 16/2455 (2019.01) **G06F 16/23** (2019.01)
G06F 21/62 (2013.01)

(21) 国际申请号: PCT/CN2021/110269

(22) 国际申请日: 2021 年 8 月 3 日 (03.08.2021)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: 浙江大学(ZHEJIANG UNIVERSITY) [CN/CN]; 中国浙江省杭州市西湖区余杭塘路 866 号, Zhejiang 310058 (CN)。

(72) 发明人: 刘健(LIU, Jian); 中国浙江省杭州市西湖区余杭塘路 866 号, Zhejiang 310058 (CN)。 曹新乐(CAO, Xin Le); 中国浙江省杭州市西湖区余杭塘路 866 号, Zhejiang 310058 (CN)。 芦浩(LU, Hao); 中国浙江省杭州市西湖区余杭塘路 866 号, Zhejiang 310058 (CN)。 任奎(REN, Kui); 中国浙江省杭州市西湖区余杭塘路 866 号, Zhejiang 310058 (CN)。

(74) 代理人: 杭州求是专利事务所有限公司(HANGZHOU QIUSHI PATENT OFFICE CO., LTD.); 中国浙江省杭州市西湖区古墩路 701 号绿城紫金广场 C 座 1506 室邱启旺, Zhejiang 310014 (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, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, 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, GH, GM, KE, LR, LS, MW, MZ, NA, RW, 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, 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))。

(54) Title: DATABASE ENCRYPTION METHOD THAT SUPPORTS COMBINABLE SQL QUERY

(54) 发明名称: 一种支持可组合 SQL 查询的加密数据库方法

(57) Abstract: Disclosed in the present invention is a database encryption method that supports combinable SQL query. The solution mainly comprises the following steps: (1) on the basis of an encryption method provided in the present invention, a user encrypting and pre-processing data, and uploading an encryption result and the pre-processed data to a service provider; (2) setting and uploading an SQL query instruction; and the user uploading the query instruction to the service provider according to an actual requirement, and simultaneously uploading auxiliary parameters used for the query instruction; and (3) performing data query, involving: the service provider performing SQL query according to the query instruction and the auxiliary parameters that are received from the user, storing a computation result, updating the data and returning a query result to the user. The present invention may be applied to data encrypted storage and encrypted data query in real life and commerce, and has the advantages of strong universality, security and high efficiency, privacy protection, simple use, high efficiency, low memory and time consumption, etc.

(57) 摘要: 本发明公开了一种支持可组合 SQL 查询的加密数据库方法, 该方案主要包括如下步骤: (1) 基于本发明提出的加密方法, 用户对数据进行加密和预处理, 并将加密结果和预处理数据上传给服务商; (2) 设定并上传 SQL 查询指令: 用户根据实际需求上传查询指令给服务商, 并同时上传用于查询指令的辅助参数; (3) 数据查询: 服务商根据收到的来自用户的查询指令和辅助参数进行 SQL 查询, 保存计算结果、更新数据并返回给用户查询结果。本发明可在实际生活和商业中应用于数据加密存储和加密数据查询, 具有通用性强、安全高效、保护隐私、使用简便、效率高、内存和时间消耗少等优点。

WO 2023/010273 A1

一种支持可组合 SQL 查询的加密数据库方法

技术领域

本发明涉及离散对数问题、乘法加密、加密数据库和密文搜索技术领域，尤其涉及一种支持可组合 SQL 查询的加密数据库方法。

背景技术

离散对数问题是指在一个可计算的有限循环群中求对数的问题，这个问题由迪菲(W.Diffie)和赫尔曼(E.Hellman)发表于 1976 年。至今为止，离散对数问题仍被认为是难以求解的问题，因此被广泛应用于加密。

乘法加密被广泛应用于密码学，包括 ElGamal 和 RSA 等知名加密方案。乘法加密能够实现“perfect security”，且能保证密文下的乘同态，即对密文的乘法操作也是对明文的乘法操作。因此，乘法加密实现了良好的安全性和可操作性。2014 年，Sigmod 会议上提出一个方案利用乘法加密方案实现加密数据库，但该方案并不安全且和本发明相差较大。

加密数据库技术最早在 2011 年被提出。第一个加密数据库模型为 CryptDB，它巧妙地结合了多种技术实现了加密数据库的多种查询操作。然而，从 2015 年开始，出现了一系列的工作攻击 CryptDB。这些工作证明，CryptDB 的安全性极差，尽管 CryptDB 已经落地，但其不应被用于商业活动。2014 年，Sigmod 上提出一个方案用于加密数据库，这个方案被称为 SDB。它提出了一种新颖的加密方案，实现了大部分的多种查询操作。然而，这个方案依然被证明是不安全的，难以运用到商业活动中。

密文搜索技术已经发展了几十年，至今出现了多种用于密文搜索的技术，包括 DET(Deterministic Encryption), OPE(Order-Preserving Encryption)。然而，至今为止，这些技术被证明或是不安全，或是太过复杂，难以被用于真实场景。此外，尽管可组合 SQL 查询是加密数据库的主流需求，但是目前没有任何数据库支持安全的组合 SQL 查询。

随着 Internet 的飞速发展，用户（包括个人和公司）对于存储大规模数据（GB 以上）的需求越来越大。目前，用户将数据存储于提供存储服务的服务商处，即广泛意义下的云端，成为了主流趋势。然而，将数据存储于服务商处，面临着两个问题：如果将数据不加密存储于服务商处，则用户的隐私将被暴露给服务商；如果将数据加密存储于服务商处，则用户不能对加密数据进行安全高效的的操作，尤其是可组合 SQL 查询。

因此，如何支持对用户隐私数据的操作特别是组合 SQL 查询包括更新、加和、搜索指定

关键字和查询指定范围仍然是一个有待解决的问题。

发明内容

本发明的目的针对现有技术不足，提供了一种支持可组合 SQL 查询的加密数据库方法。

本发明的目的是通过以下技术方案来实现的：一种支持可组合 SQL 查询的加密数据库方法，包括以下步骤：

(1) 加密存储数据：用户对自己的存储数据进行加密和预处理，并将加密结果和预处理数据上传给服务商，所述服务商提供用于运行数据库的软件、装置、电子设备或存储介质存储用户上传的数据；所述步骤 (1) 具体包括以下子步骤：

(1.1) 用户针对自己的数据，生成随机数集合作为数据的行密钥和列密钥；基于乘法加密，用户用行密钥和列密钥来加密数据，输出加密后的数据库；

(1.2) 用户将加密后的数据库上传到服务商处，用户选择任意一种加密方式将步骤 (1.1) 生成的行密钥加密上传到服务商实现对行密钥的加密存储，同时根据需求选择将列密钥不加密地存储在本地或加密上传至服务商处；

(1.3) 用户针对指令进行预处理，生成运行指令所需的辅助数据；用户将辅助数据上传至服务商，所述服务商不能从该辅助数据中获取任何关于数据库的隐私信息；所述指令包括更新、插入、删除、加和、搜索指定关键字和查询指定范围操作；

(1.4) 服务商根据实际情况选择存储形式，所述存储形式包括数据库软件、装置、电子设备或存储介质，并基于该存储形式进行存储加密数据和辅助数据，并进行后续指令执行。

(2) 设定组合 SQL 查询指令，用户根据实际需求上传组合 SQL 查询指令给服务商，并上传用于查询指令的辅助参数；

(3) 运行步骤 (2) 设定的组合 SQL 查询指令：服务商根据收到的来自用户的组合 SQL 查询指令和辅助参数运行查询指令，保存指令运行后的计算结果、更新数据并返回给用户查询结果。

进一步地，所述步骤 (1.1) 具体为：

用户随机生成两个大质数 p 和 q ，得到大整数 $N = p \cdot q$ ；用户将此大整数 N 作为生成元 g 的阶数，并在有限域 Z_{N^2} 上找到生成元 g ；用户将生成随机数作为行密钥和列密钥，利用该行密钥和列密钥来加密数据库，第 i 行的行密钥为 $(r_i, t_i) \in Z_N^2$ ；第 j 列的列密钥为 (m_j, x_j) ，其中 $m_j \in Z_{N^2}, x_j \in Z_N$ ；行密钥和列密钥应保证对于任意的 i, j ，都存在整数 $M_{(i,j)} \in Z_{N^2}$ 使得 $m_j g^{r_i x_j} \cdot M_{(i,j)} \bmod N^2 = 1$ ，把该整数 $M_{(i,j)}$ 称为 $m_j g^{r_i x_j}$ 相对于 N^2 的逆，记为 $(m_j g^{r_i x_j})^{-1}$ ；最后数据库第 i 行第 j 列的元素 $v_{(i,j)}$ 被加密如下：

$$c_{(i,j)} = (N+1)^{t_i v(i,j)} \cdot (m_j g^{r_i x_j})^{-1} \mod N^2$$

进一步地, 所述步骤 (1.3) 具体为:

对于删除和加和指令, 用户无需生成辅助数据 D;

对于更新和插入指令, 用户每更新或插入一行数据, 则需提前生成一个行密钥加密存放至服务商处, 更新和插入时, 用户从服务商处下载提前生成的行密钥, 从服务商或本地获取列密钥, 实现对更新的数据进行解密更新并重新加密上传至服务商处或直接将插入的数据进行加密上传至服务商处;

对于搜索指定关键字指令, 用户可以选择两列之间查询每一行是否为同一关键字或对某一列所有行查询是否为某一指定关键字, 若用户对两列之间查询相同行是否为同一关键字, 则用户每进行一次查询需要生成一列加密的随机数 $\alpha_i (i = 1, 2, \dots, n)$, 对应的列密钥为 (m_α, x_α) , 加密方式为 $E(\alpha_i) = (m_\alpha \cdot g^{r_i x_\alpha})^{-1} \cdot (N+1)^{t_i \alpha} \mod N^2$; 每一行加密的元素都是 1, 统称这列为 S 列, 所述 S 列对应的列密钥为 (m_s, x_s) , 第 i 行元素 1 被加密为 $E(1)_i = (m_s \cdot g^{r_i x_s})^{-1} \cdot 1 \mod N^2$, 其中, m_s 存在对于 N^2 的逆 $m_s^{-1} \in Z_{N^2}$, 即 $m_s \cdot m_s^{-1} \mod N^2 = 1$; x_s 存在对于 N 的逆 $x_s^{-1} \in Z_N$, 即 $x_s \cdot x_s^{-1} \mod N = 1$; 一列随机数 $h_i^{e_i} (i = 1, 2, \dots, n)$, 其中 h_i 为 Z_{N_1} 上的 N_2 阶生成元, N_1 为两个或多个随机大质数的积, N_2 为其中任意一个大质数, 即 N_2 整除 N_1 , e_i 是 Z_{N_2} 上的随机整数; 一列数 $h^{e_i \cdot (t_i \cdot \alpha_i \mod N) \mod N_2} (i = 1, 2, \dots, N)$; 若用户对某一列所有行查询是否为某一指定关键字, 则用户每进行一次查询除需要上述两列之间比较每一行是否为同一关键字所需的辅助数据外还需要额外生成一列加密的 γ , 即每一行加密的元素都是 γ , 对应的列密钥为 (m_γ, x_γ) , 第 i 行元素被加密为 $E(\gamma)_i = (m_\gamma \cdot g^{r_i x_\gamma})^{-1} \cdot (N+1)^{t_i \gamma}$, 其中, γ 为 Z_N 上的随机数, γ 应保证存在相对于 N 的逆 $\gamma^{-1} \in Z_N$, 即 $\gamma \cdot \gamma^{-1} \mod N = 1$;

对于查询指定范围指令, 用户选择两列之间互相比对或某一列与同一个常数进行比较用于查询指定范围, 若用户对两列之间互相比对, 则每一次比较操作都需要生成一列加密的随机数 $\alpha_i (i = 1, 2, \dots, n)$, 对应的列密钥为 (m_α, x_α) , 加密方式为 $E(\alpha_i) = (m_\alpha \cdot g^{r_i x_\alpha})^{-1} \cdot (N+1)^{t_i \alpha} \mod N^2$; 每一行加密的元素都是 1, 统称这列为 S 列, 所述 S 列对应的列密钥为 (m_s, x_s) , 第 i 行元素 1 被加密为 $E(1)_i = (m_s \cdot g^{r_i x_s})^{-1} \cdot 1 \mod N^2$, 其中, m_s 存在对于 N^2 的逆 $m_s^{-1} \in Z_{N^2}$, 即 $m_s \cdot m_s^{-1} \mod N^2 = 1$; x_s 存在对于 N 的逆 $x_s^{-1} \in Z_N$, 即 $x_s \cdot x_s^{-1} \mod N = 1$; 一列 $\beta_i \cdot t_i^{-1} (i = 1, 2, \dots, n)$, 一列 $u_i - \beta_i \cdot \alpha_i$, 其中 $t_i^{-1} \in Z_N$ 为 t_i 相对于 N 的逆, 即 $t_i^{-1} \cdot t_i \mod N = 1$, β_i, u_i 为 Z_N 上的随机数且满足 $0 \ll u_i \ll \beta_i \ll \frac{N}{2}$; 若用户对某一列与同一个常数进行比较, 则用户每进行一次比较操作除需要上述两列之间相互比较需要的辅助数据外还

需要额外生成一列加密的 γ ，即每一行加密的元素都是 γ ，对应的列密钥为 (m_γ, x_γ) ，第 i 行元素被加密为 $E(\gamma)_i = (m_\gamma \cdot g^{r_i x_\gamma})^{-1} \cdot (N+1)^{t_i \gamma}$ ，其中， γ 为 Z_N 上的随机数， γ 应保证存在相对于 N 的逆 $\gamma^{-1} \in Z_N$ ，即 $\gamma \cdot \gamma^{-1} \bmod N = 1$ 。

进一步地，所述步骤（2）具体包括以下子步骤：

（2.1）用户根据其实际的商业需求上传运行指令至服务商；所述运行指令包括更新、加和、搜索指定关键字和查询指定范围；

（2.2）用户根据其上传的指令计算辅助参数，并将该辅助参数随指令或在接收到服务商请求后上传至服务商：

所述步骤（2.2）具体为，对于更新、插入和删除操作，用户无需进行任何辅助参数的计算；对于加和操作，若对 A 列和 B 列进行加和，对应的列密钥为 (m_A, x_A) 和 (m_B, x_B) ，则新生成列 $C = A + B$ 的列密钥被用户进行计算并存储，相应计算方式为 $(m_C = m_A \cdot m_B \bmod N^2, x_C = x_A + x_B \bmod N)$ ，用户选择本地不加密地存储该密钥或加密上传至服务商处进行存储；对于搜索指定关键字指令，用户选择两列之间查询每一行是否为同一关键字或对某一列所有行查询是否为某一指定关键字，若用户对两列如 A 列和 B 列之间查询每一行是否为同一关键字，对应的列密钥为 (m_A, x_A) 和 (m_B, x_B) ，则用户需计算：

（I）列 $A' = A - B + \alpha$ 的列密钥 $(m_{A'} = m_A \cdot m_B^{-1} \cdot m_\alpha \bmod N^2, x_{A'} = x_A - x_B + x_\alpha \bmod N)$ ；

（II）计算辅助参数 $\zeta = -x_S^{-1} x_{A'} \bmod N, \eta = m_{A'} m_S^\zeta \bmod N^2$ ，得到最后用户上传的辅助参数为 (ζ, η) ；

若用户对某一列如 A 列所有行查询是否为某一指定关键字如 v ，则用户需计算：

（I） $v \cdot \gamma^{-1}$ ，其中 γ 为步骤（1.3）所述辅助数据；

（II）列 $\gamma' = E(\gamma)^{v \cdot \gamma^{-1}}$ 的列密钥 $(m_{\gamma'} = m_\gamma^{v \cdot \gamma^{-1}} \bmod N^2, x_{\gamma'} = v \cdot \gamma^{-1} \cdot x_\gamma \bmod N)$ ，其中，列 γ' 为服务商通过列 γ 计算出的新列，列 γ' 的第 i 行元素 $E(\gamma')_i$ 通过列 γ 的第 i 行元素 $E(\gamma)_i$ 计算： $E(\gamma')_i = E(\gamma)_i^{v \cdot \gamma^{-1}} \bmod N^2$ ；

（III）列 $A' = A - \gamma' + \alpha$ 的列密钥 $(m_{A'} = m_A \cdot (m_{\gamma'})^{-1} \cdot m_\alpha \bmod N^2, x_{A'} = x_A - x_{\gamma'} + x_\alpha \bmod N)$ ；

（IV）计算辅助参数 P ： $\zeta = -x_S^{-1} x_{A'} \bmod N, \eta = m_{A'} m_S^\zeta \bmod N^2$ ；得到最后用户上传的辅助参数为 $(v \cdot \gamma^{-1}, \zeta, \eta)$ 。

对于查询指定范围指令, 用户选择两列之间互相比大小或某一列与同一个常数进行比较大用于查询指定范围, 若用户在两列如A列和B列相同行之间进行比较大, 两列对应的列密钥为 (m_A, x_A) 和 (m_B, x_B) , 则用户需计算:

(I) 列 $A' = A - B + \alpha$ 的 列 密 钥 $(m_{A'} = m_A \cdot m_B^{-1} \cdot m_\alpha \bmod N^2, x_{A'} = x_A - x_B + x_\alpha \bmod N)$; (2) $\zeta = -x_S^{-1} x_{A'} \bmod N, \eta = m_{A'} m_S^\zeta \bmod N^2$; 得到最后用户上传的辅助参数为 (ζ, η) ;

若用户对某一列如A列所有行与同一个常数如 v 进行比较大, 则用户需计算

(I) $v \cdot \gamma^{-1}$, 其中 γ 为步骤 (1.3) 所述辅助数据;

(II) 计算列 γ' 的列密钥 $(m_{\gamma'} = m_\gamma^{v \cdot \gamma^{-1}} \bmod N^2, x_{\gamma'} = v \cdot \gamma^{-1} \cdot x_\gamma \bmod N)$, 其中, 列 γ' 为服务商通过列 γ 计算出的新列, 列 γ' 的第 i 行元素 $E(\gamma')_i$ 通过列 γ 的第 i 行元素 $E(\gamma)_i$ 计算:
 $E(\gamma')_i = E(\gamma)_i^{v \cdot \gamma^{-1}} \bmod N^2$;

(III) 计算列 $A' = A - \gamma' + \alpha$ 的 列 密 钥 $(m_{A'} = m_A \cdot (m_{\gamma'})^{-1} \cdot m_\alpha \bmod N^2, x_{A'} = x_A - x_{\gamma'} + x_\alpha \bmod N)$;

(IV) 计算辅助参数 $\zeta = -x_S^{-1} x_{A'} \bmod N, \eta = m_{A'} m_S^\zeta \bmod N^2$; 得到最后用户上传的辅助参数为 $(v \cdot \gamma^{-1}, \zeta, \eta)$ 。

进一步地, 所述步骤 (3) 具体包括以下子步骤:

(3.1) 服务商在收到用户的组合 SQL 查询指令后进行相应的计算和操作, 根据其计算中的需求向用户提出对辅助参数的请求或从用户随指令上传的辅助参数中选取所需参数;

(3.2) 服务商收到辅助参数后, 根据指令进行计算, 保存指令运行后的计算结果、更新数据并返回给用户查询结果。

进一步地, 所述步骤 (3.1) 具体为: 对于删除指令, 服务商只需进行正常的删除操作并更新数据库; 对于插入和更新操作, 若用户将行密钥与列密钥加密存储在服务商处, 则服务商只需返回用户索取的行密钥和列密钥, 接收用户上传的新数据进行正常的插入和更新即可; 对于加和操作, 若对A列和B列进行加和得到C列, 则服务商计算C列的第 i 行元素 C_i 如下:
 $C_i = A_i \times B_i (i = 1, 2, 3, \dots, n)$, 其中 A_i, B_i 分别表示A列和B列的第 i 行元素。在上述指令运行中, 服务商不需要用户提供任何辅助参数;

对于搜索指定关键字操作, 用户选择两列之间查询每一行是否为同一关键字或对某一列所有行查询是否为某一指定关键字, 若用户对两列如A列和B列之间查询每一行是否为同一关键字, 对应的列密钥为 (m_A, x_A) 和 (m_B, x_B) , 则服务商进行以下计算:

(I) 计算列 B' , 计算如下: 列 B' 的第 i 行元素 $B'_i = B_i^{N-1} \bmod N^2$, 其中, B_i 为 B 列的第 i 行元素;

(II) 计算列 A' , 计算如下: 列 A' 的第 i 行元素 $A'_i = A_i \times B'_i \times E(\alpha)_i \bmod N^2$, 其中, A_i 为 A 列的第 i 行元素, $E(\alpha)_i$ 为步骤(1.3)所述辅助数据 α 列的第 i 行元素;

(III) 服务商向用户提出对辅助参数 P 的请求或从用户随指令上传的辅助参数中选取所需参数;

若用户对某一列如 A 列所有行查询是否为某一外部关键字如 v , 则服务商直接向用户提出对辅助参数的请求或从用户随指令上传的辅助参数中选取所需参数;

对于查询指定范围指令, 用户可以选择两列之间互比较大小或某一列与同一个常数进行比较大小用于查询指定范围, 若用户在两列如 A 列和 B 列相同行之间进行比较大小, 两列对应的列密钥为 (m_A, x_A) 和 (m_B, x_B) , 则服务商进行以下计算:

(I) 计算列 B' , 计算如下: 列 B' 的第 i 行元素 $B'_i = B_i^{N-1} \bmod N^2$, 其中, B_i 为 B 列的第 i 行元素;

(II) 计算列 A' , 计算如下: 列 A' 的第 i 行元素 $A'_i = A_i \times B'_i \times E(\alpha)_i \bmod N^2$, 其中, A_i 为 A 列的第 i 行元素, $E(\alpha)_i$ 为步骤(1.3)所述辅助数据 α 列的第 i 行元素;

(III) 服务商向用户提出对辅助参数的请求或从用户随指令上传的辅助参数中选取所需参数;

若用户对某一列如 A 列所有行与同一个常数如 v 进行比较大小, 则服务商直接向用户提出对辅助参数的请求或从用户随指令上传的辅助参数中选取所需参数。

进一步地, 所述步骤(3.2)具体为: 对于搜索指定关键字操作, 用户选择两列之间查询每一行是否为同一关键字或对某一列所有行查询是否为某一指定关键字, 若用户对两列如 A 列和 B 列之间查询每一行是否为同一关键字, 对应的列密钥为 (m_A, x_A) 和 (m_B, x_B) , 则服务商收到用户步骤(2)计算并上传的辅助参数 (ζ, η) , 进行以下计算:

(I) 计算列 a , 计算列 a 的第 i 行元素 a_i 如下: $a_i = A'_i \times \eta \times E(1)_i^{\zeta} \bmod N^2$, 其中, A'_i 为步骤(3.1)所述列 A' 的第 i 行元素, $E(1)_i$ 为步骤(1.3)所述辅助数据 S 列的第 i 行元素;

(II) 计算列 H , 计算列 H 的第 i 行元素 H_i 如下: $H_i = (h_i^{e_i})^{a_i} \bmod N_1$, 其中, $h_i^{e_i}$ 为步骤(1.3)所述辅助数据 h 列的第 i 行元素, N_1 是步骤(1.3)所述 N_1 ; (III) 比较 $(h^{e_i \cdot (t_i \cdot \alpha_i \bmod N)} \bmod N_2, H_i)$, 其中, $h^{e_i \cdot (t_i \cdot \alpha_i \bmod N)} \bmod N_2$ 为步骤(1.3)所述辅助数据 h' 列的第 i 行元素, 若两者相等, 则 A 列和 B 列第 i 行的元素相等; 若不相等, 则 A 列和 B 列第 i 行的元素不相等;

若用户对某一列如A列所有行查询是否为某一外部关键字如 v ，则服务商收到用户上传的辅助参数 $(v \cdot \gamma^{-1}, \zeta, \eta)$ 进行以下计算：

(I) 计算列 γ' ，列 γ' 为服务商根据步骤(1.3)所述辅助数据列 γ 和用户上传计算出的辅助参数 P 计算出的新列，列 γ' 的第 i 行元素 $E(\gamma')_i$ 通过列 γ 的第 i 行元素 $E(\gamma)_i$ 计算：

$$E(\gamma')_i = E(\gamma)_i^{v \cdot \gamma^{-1}} \bmod N^2$$

(II) 计算列 A' ，计算如下：列 A' 的第 i 行元素 $A'_i = A_i \times E(\gamma')_i^{N-1} \times E(\alpha)_i \bmod N^2$ ，其中， A_i 为A列的第 i 行元素， $E(\alpha)_i$ 为步骤(1.3)所述辅助数据 α 列的第 i 行元素；

(III) 计算列 a ，计算列 a 的第 i 行元素 a_i 如下： $a_i = A'_i \times \eta \times E(1)_i^{\zeta} \bmod N^2$ ，其中， A'_i 为步骤(3.1)所述列 A' 的第 i 行元素， $E(1)_i$ 为步骤(1.3)所述辅助数据S列的第 i 行元素；

(IV) 计算列 H ，计算列 H 的第 i 行元素 H_i 如下： $H_i = (h_i^{e_i})^{a_i} \bmod N_1$ ，其中， $h_i^{e_i}$ 为步骤(1.3)所述辅助数据 h 列的第 i 行元素， N_1 是步骤(1.3)所述 N_1 ；

(V) 比较 $(h^{e_i \cdot (t_i \cdot \alpha_i \bmod N) \bmod N_2}, H_i)$ ，其中， $h^{e_i \cdot (t_i \cdot \alpha_i \bmod N) \bmod N_2}$ 为步骤(1.3)所述辅助数据 h' 列的第 i 行元素，若两者相等，则A列第 i 行的元素与 v 相等；若不相等，则A列第 i 行的元素与 v 不相等；

对于查询指定范围指令，用户选择两列之间互相比大小或某一列与同一个常数进行比较大小用于查询指定范围，若用户在两列如A列和B列相同行之间进行比较大小，两列对应的列密钥为 (m_A, x_A) 和 (m_B, x_B) ，服务商收到用户上传的辅助参数 $P: (\zeta, \eta)$ 进行以下计算：

(I) 计算列 a ，计算列 a 的第 i 行元素 a_i 如下： $a_i = A'_i \times \eta \times E(1)_i^{\zeta} \bmod N^2$ ，其中， A'_i 为步骤(3.1)所述列 A' 的第 i 行元素， $E(1)_i$ 为步骤(1.3)所述辅助数据S列的第 i 行元素；

(II) 计算列 a' ，计算列 a' 的第 i 行元素 a'_i 如下： $a'_i = a_i \times (\beta_i \cdot t_i^{-1}) + u_i - \beta_i \alpha_i \bmod N$ ，其中， $\beta_i t_i^{-1}$ 为步骤(1.3)所述辅助数据 β 列的第 i 行元素， $u_i - \beta_i \alpha_i$ 是步骤(1.3)所述 u 列的第 i 行元素；

(III) 比较 a'_i 与 $\frac{N}{2}$ ，若 $a'_i > \frac{N}{2}$ ，则A列第 i 行的元素较小；不然，则B列第 i 行的元素不大于A列第 i 行的元素；

若用户对某一列如A列所有行与同一个常数如 v 进行比较大小，则服务商收到用户上传的辅助参数 $(v \cdot \gamma^{-1}, \zeta, \eta)$ ，进行以下计算：

(I) 计算列 γ' ，列 γ' 为服务商根据步骤(1.3)所述辅助数据列 γ 和用户上传计算出的辅助参数 P 计算出的新列，列 γ' 的第 i 行元素 $E(\gamma')_i$ 通过列 γ 的第 i 行元素 $E(\gamma)_i$ 计算：

$$E(\gamma')_i = E(\gamma)_i^{v \cdot \gamma^{-1}} \bmod N^2$$

(II) 计算列 A' , 计算如下: 列 A' 的第 i 行元素 $A'_i = A_i \times E(\gamma')_i^{N-1} \times E(\alpha)_i \mod N^2 (i = 1, 2, \dots, n)$, 其中, A_i 为 A 列的第 i 行元素, $E(\alpha)_i$ 为步骤(1.3)所述辅助数据 α 列的第 i 行元素;

(III) 计算列 a , 计算列 a 的第 i 行元素 a_i 如下: $a_i = A'_i \times \eta \times E(1)_i^{\zeta} \mod N^2$, 其中, A'_i 为步骤(3.1)所述列 A' 的第 i 行元素, $E(1)_i$ 为步骤(1.3)所述辅助数据 S 列的第 i 行元素;

(IV) 计算列 a' , 计算列 a' 的第 i 行元素 a'_i 如下: $a'_i = a_i \times (\beta_i \cdot t_i^{-1}) + u_i - \beta_i \alpha_i \mod N$, 其中, $\beta_i t_i^{-1}$ 为步骤(1.3)所述辅助数据 β 列的第 i 行元素, $u_i - \beta_i \alpha_i$ 是步骤(1.3)所述 u 列的第 i 行元素;

(V) 比较 a'_i 与 $\frac{N}{2}$, 若 $a'_i < \frac{N}{2}$, 则 A 列第 i 行的元素不小于 v ; 不然, 则 A 列第 i 行的元素小于 v 。

根据以上技术方案, 本发明的有益效果如下:

1. 本发明基于离散对数问题, 实现了对用户数据的加密保护、减少了用户隐私信息的泄露, 从而为实际商业活动中用户数据的云端存储提供了安全完整的保护方案;
2. 本发明实现了在加密数据上安全高效地执行可组合 SQL 查询指令, 指令包括更新、插入、删除、加和、搜索指定关键字和查询指定范围, 满足了实际商业活动中用户对云端存储数据远程操作和查询的需求。
3. 本发明具有通用性强、安全高效、保护隐私、使用简便、效率高、内存和时间消耗少等优点。

具体实施方式

为使本申请的目的、技术方案和优点更加清楚, 下面将结合本申请具体实施例及相应的附图对本申请技术方案进行清楚、完整地描述。显然, 所描述的实施例仅是本申请一部分实施例, 而不是全部的实施例。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他实施例, 都属于本申请保护的范围。

实施例 1:

假设售货公司用户甲将自己的数据集 M 存储于某服务商乙处, 并要求服务商乙不能获取任何关于 M 的信息。此外, 用户甲要求能够对数据集 M 进行不泄露隐私的操作 (操作包括但不限于更新、插入、删除、加和、搜索指定关键字和查询指定范围, 如返回交易额大于 5000 的订单)。为了解决这种情况, 利用本发明一种支持可组合 SQL 查询的加密数据库方法, 来满足用户甲的要求, 具体包括以下步骤:

步骤(1) 加密存储数据: 用户甲对数据 M 进行加密和预处理, 并将加密结果和预处理数据上传给服务商乙, 所述服务商乙提供用于运行数据库的软件、装置、电子设备或存储介质

用于存储用户上传的数据；

具体地，步骤(1.1)用户甲生成随机数集合 R 和 C 分别作为数据库 M 的行密钥和列密钥。基于乘法加密，用户甲用密钥 R 和 C 来加密数据，输出加密后的数据库；

具体来说，用户甲随机生成两个大质数 p 和 q ，得到大整数 $N = p \cdot q$ ；此外，用户甲将此大整数 N 作为生成元的阶数在有限域 Z_{N^2} 上找到生成元 g ；用户甲生成随机数作为行密钥和列密钥来加密数据库 M ，第 i 行的行密钥为 $(r_i, t_i) \in Z_N^2$ ；第 j 列的列密钥为 (m_j, x_j) ，其中 $m_j \in Z_{N^2}, x_j \in Z_N$ ；行密钥和列密钥应保证对于任意的 i, j ，都存在整数 $M_{(i,j)} \in Z_{N^2}$ 使得 $m_j g^{r_i x_j} \cdot M_{(i,j)} \bmod N^2 = 1$ ，把该整数 $M_{(i,j)}$ 称为 $m_j g^{r_i x_j}$ 相对于 N^2 的逆，记为 $(m_j g^{r_i x_j})^{-1}$ 。最后数据库 M 第 i 行第 j 列的元素 $v_{(i,j)}$ 被加密如下：

$$c_{(i,j)} = (N + 1)^{t_i v_{(i,j)}} \cdot (m_j g^{r_i x_j})^{-1} \bmod N^2$$

步骤 (1.2) 用户甲将加密后的数据库 M 上传到服务商乙处；此外，用户甲选择任意一种安全的加密方式加密随机数集合 R 并将加密后的随机数集合 R 上传至服务商乙处，用户甲也可根据自己的需求选择将随机数集合 C 不加密地存储在本地或加密上传至服务商乙处；

具体为，在整个过程中假设该数据库有 n 行 m 列元素，则除加密的数据库密文外，用户甲将 n 个加密行密钥同时上传到服务商乙处，将 m 个列密钥不加密存储于本地或加密上传至服务商乙处，行密钥和列密钥的加密方式可采取任意一种安全的加密方式，如 AES 加密。将加密数据库和加密的行密钥统称为加密结果，加密结果被用户甲上传至服务商乙处进行存储。服务商乙不能从加密结果中获取任何关于用户甲的数据库 M 的敏感信息。若用户甲需还原数据库元素明文，则需从服务商乙处同时下载加密元素及加密元素对应行密钥。若列密钥被加密上传至服务商乙处，则用户甲需要下载加密元素对应列密钥；若列密钥被不加密存储于用户甲本地，则甲只需在本地找到加密元素相应列密钥。若用户甲需对数据库的某一列进行查询指令的操作，则甲需要此列的列密钥，若列密钥被加密上传至服务商乙处，则用户甲需从服务商乙处下载此列的列密钥；若列密钥被不加密存储于用户甲本地，则甲只需在本地找到此列的列密钥。

步骤 (1.3)，用户甲针对指令进行预处理，生成执行指令所需要的辅助数据 D ；用户甲将辅助数据 D 上传至服务商乙处，服务商乙不能从该辅助数据 D 中获取任何关于数据库 M 的隐私信息；所述服务商乙必须得到用户甲计算的辅助参数 P 才可以进行指定操作；所述指令包括但不限于更新、插入、删除、加和、搜索指定关键字和查询指定范围等操作；

具体地, 对于删除和加和指令, 用户甲无需生成辅助数据 D ; 对于更新和插入指令, 用户甲每更新或插入一行数据, 则需提前生成一个行密钥加密存放至服务商乙处, 更新和插入时, 用户甲从服务商乙处下载提前生成的行密钥, 从服务商乙或本地获取列密钥, 因此可以对更新的数据进行解密更新并重新加密上传至服务商乙处或直接对插入的数据进行加密上传至服务商乙处; 对于搜索指定关键字指令, 用户甲可以选择两列之间查询每一行是否为同一关键字或对某一列所有行查询是否为某一指定关键字, 若用户甲对两列之间查询相同行是否为同一关键字, 则用户甲每进行一次查询需要生成一列加密的随机数 $\alpha_i (i = 1, 2, \dots, n)$ (统称为 α 列), 对应的列密钥为 (m_α, x_α) , 加密方式为 $E(\alpha_i) = (m_\alpha \cdot g^{r_i x_\alpha})^{-1} \cdot (N+1)^{t_i \alpha} \bmod N^2$; 每一行加密的元素都是 1, 统称这列为 S 列, 所述 S 列对应的列密钥为 (m_s, x_s) , 第 i 行元素 1 被加密为 $E(1)_i = (m_s \cdot g^{r_i x_s})^{-1} \cdot 1 \bmod N^2$, 其中, m_s 存在对于 N^2 的逆 $m_s^{-1} \in Z_{N^2}$, 即 $m_s \cdot m_s^{-1} \bmod N^2 = 1$; x_s 存在对于 N 的逆 $x_s^{-1} \in Z_N$, 即 $x_s \cdot x_s^{-1} \bmod N = 1$; 一列随机数 $h_i^{e_i} (i = 1, 2, \dots, n)$ (统称为 h 列), 其中 h_i 为 Z_{N_1} 上的 N_2 阶生成元, N_1 为两个或多个随机大质数的积, N_2 为其中任意一个大质数, 即 N_2 整除 N_1 , e_i 是 Z_{N_2} 上的随机整数; 一列数 $h^{e_i(t_i \cdot \alpha_i \bmod N) \bmod N_2} (i = 1, 2, \dots, N)$ (统称为 h' 列); 若用户甲对某一列所有行查询是否为某一指定关键字, 则用户甲每进行一次查询除需要上述两列之间比较每一行是否为同一关键字所需的辅助数据外还需要额外生成一列加密的 γ (即每一行加密的元素都是 γ , 统称此列为 γ 列), 对应的列密钥为 (m_γ, x_γ) , 第 i 行元素被加密为 $E(\gamma)_i = (m_\gamma \cdot g^{r_i x_\gamma})^{-1} \cdot (N+1)^{t_i \gamma}$, 其中, γ 为 Z_N 上的随机数, γ 应保证存在相对于 N 的逆 $\gamma^{-1} \in Z_N$, 即 $\gamma \cdot \gamma^{-1} \bmod N = 1$; 对于查询指定范围指令, 用户甲可以选择两列之间互相比对或某一列与同一个常数进行比较用于查询指定范围, 若用户甲对两列之间互相比对, 则每一次比较操作都需要生成一列加密的随机数 $\alpha_i (i = 1, 2, \dots, n)$ (统称为 α 列), 对应的列密钥为 (m_α, x_α) , 加密方式为 $E(\alpha_i) = (m_\alpha \cdot g^{r_i x_\alpha})^{-1} \cdot (N+1)^{t_i \alpha} \bmod N^2$; 每一行加密的元素都是 1, 统称这列为 S 列, 所述 S 列对应的列密钥为 (m_s, x_s) , 第 i 行元素 1 被加密为 $E(1)_i = (m_s \cdot g^{r_i x_s})^{-1} \cdot 1 \bmod N^2$, 其中, m_s 存在对于 N^2 的逆 $m_s^{-1} \in Z_{N^2}$, 即 $m_s \cdot m_s^{-1} \bmod N^2 = 1$; x_s 存在对于 N 的逆 $x_s^{-1} \in Z_N$, 即 $x_s \cdot x_s^{-1} \bmod N = 1$; 一列 $\beta_i \cdot t_i^{-1} (i = 1, 2, \dots, n)$ (统称为 β 列), 一列 $u_i - \beta_i \cdot \alpha_i$ (统称为 u 列), 其中 $t_i^{-1} \in Z_N$ 为 t_i 相对于 N 的逆, 即 $t_i^{-1} \cdot t_i \bmod N = 1$, β_i, u_i 为 Z_N 上的随机数且满足 $0 \ll u_i \ll \beta_i \ll \frac{N}{2}$; 若用户甲对某一列与同一个常数进行比较, 则用户甲每进行一次比较操作除需要上述两列之间相互比较需要的辅助数据外还需要额外生成一列加密的 γ (即每一行加密的元素都是 γ , 统称此列为 γ 列), 对应的列密钥为 (m_γ, x_γ) , 第 i 行元素被加密为 $E(\gamma)_i = (m_\gamma \cdot g^{r_i x_\gamma})^{-1} \cdot (N+1)^{t_i \gamma}$, 其中,

γ 为 Z_N 上的随机数, γ 应保证存在相对于 N 的逆 $\gamma^{-1} \in Z_N$, 即 $\gamma \cdot \gamma^{-1} \bmod N = 1$ 。

上述辅助数据 α 列、 S 列和 γ 列既可用于搜索指定关键字指令, 也可用于查询指定范围指令。上述所有辅助数据都应在查询指令上传以前被上传至服务商乙处, 服务商乙借助辅助数据完成查询指令, 大大提升查询指令的执行效率。

步骤(1.4) 服务商乙根据实际情况选择数据库软件、装置、电子设备或存储介质存储加密的 M 、随机数集合 R 和辅助数据 D 并基于该方式进行后续指令执行。

步骤(2) 设定组合 SQL 查询指令, 用户甲根据实际需求上传指令给服务商乙, 并计算上传用于执行指令的辅助参数 P 。

具体地, 步骤(2.1) 用户甲根据其实际的商业需求上传运行指令 Q 至服务商乙处; 所述指令包括更新、加和、搜索指定关键字和查询指定范围;

步骤(2.2) 用户甲根据其上传的指令 Q 计算辅助参数 P , 并将该辅助参数 P 随指令或在接收到服务商乙请求后上传至服务商乙处。

具体来说, 对于更新、插入和删除操作, 用户甲无需进行任何辅助参数 P 的计算; 对于加和操作, 若对 A 列和 B 列进行加和, 对应的列密钥为 (m_A, x_A) 和 (m_B, x_B) , 则新生成列 $C = A + B$ 的列密钥被用户甲进行计算并存储, 相应计算方式为 $(m_C = m_A \cdot m_B \bmod N^2, x_C = x_A + x_B \bmod N)$, 用户甲可以选择本地不加密地存储该密钥, 或加密上传至服务商乙处进行存储。

对于搜索指定关键字指令, 用户甲可以选择两列之间查询每一行是否为同一关键字或对某一列所有行查询是否为某一指定关键字, 若用户甲对两列如 A 列和 B 列之间查询每一行是否为同一关键字, 对应的列密钥为 (m_A, x_A) 和 (m_B, x_B) , 则用户甲需计算:

(I) 列 $A' = A - B + \alpha$ 的列密钥 $(m_{A'} = m_A \cdot m_B^{-1} \cdot m_\alpha \bmod N^2, x_{A'} = x_A - x_B + x_\alpha \bmod N)$;

(II) 计算辅助参数 P : $\zeta = -x_S^{-1} x_{A'} \bmod N, \eta = m_A \cdot m_S^\zeta \bmod N^2$, 得到最后用户甲上传的辅助参数 P 为 (ζ, η) ;

若用户甲对某一列如 A 列所有行查询是否为某一指定关键字如 v , 则用户甲需计算:

(I) $v \cdot \gamma^{-1}$, 其中 γ 为步骤(1.3)所述辅助数据;

(II) 列 $\gamma' = E(\gamma)^{v \cdot \gamma^{-1}}$ 的列密钥 $(m_{\gamma'} = m_\gamma^{v \cdot \gamma^{-1}} \bmod N^2, x_{\gamma'} = v \cdot \gamma^{-1} \cdot x_\gamma \bmod N)$, 其中, 列 γ' 为服务商乙通过列 γ 计算出的新列, 列 γ' 的第 i 行元素 $E(\gamma')_i$ 通过列 γ 的第 i 行元素 $E(\gamma)_i$ 计算: $E(\gamma')_i = E(\gamma)_i^{v \cdot \gamma^{-1}} \bmod N^2$;

(III) 列 $A' = A - \gamma' + \alpha$ 的列密钥 $(m_{A'} = m_A \cdot (m_{\gamma'})^{-1} \cdot m_{\alpha} \bmod N^2, x_{A'} = x_A - x_{\gamma'} + x_{\alpha} \bmod N)$;

(IV) 计算辅助参数 P : $\zeta = -x_S^{-1} x_{A'} \bmod N, \eta = m_{A'} m_S^{\zeta} \bmod N^2$; 得到最后用户甲上传的辅助参数为 $(v \cdot \gamma^{-1}, \zeta, \eta)$ 。

对于查询指定范围指令, 用户甲可以选择两列之间互比较大小或某一列与同一个常数进行比较大小用于查询指定范围, 若用户甲在两列如 A 列和 B 列相同行之间进行比较大小, 两列对应的列密钥为 (m_A, x_A) 和 (m_B, x_B) , 则用户甲需计算:

(I) 列 $A' = A - B + \alpha$ 的列密钥 $(m_{A'} = m_A \cdot m_B^{-1} \cdot m_{\alpha} \bmod N^2, x_{A'} = x_A - x_B + x_{\alpha} \bmod N)$; (2) $\zeta = -x_S^{-1} x_{A'} \bmod N, \eta = m_{A'} m_S^{\zeta} \bmod N^2$; 得到最后用户甲上传的辅助参数 P 为 (ζ, η) ;

若用户甲对某一列如 A 列所有行与同一个常数如 v 进行比较大小, 则用户甲需计算

(I) $v \cdot \gamma^{-1}$, 其中 γ 为步骤 (1.3) 所述辅助数据;

(II) 计算列 γ' 的列密钥 $(m_{\gamma'} = m_{\gamma}^{v \cdot \gamma^{-1}} \bmod N^2, x_{\gamma'} = v \cdot \gamma^{-1} \cdot x_{\gamma} \bmod N)$, 其中, 列 γ' 为服务商乙通过列 γ 计算出的新列, 列 γ' 的第 i 行元素 $E(\gamma')_i$ 通过列 γ 的第 i 行元素 $E(\gamma)_i$ 计算:
 $E(\gamma')_i = E(\gamma)_i^{v \cdot \gamma^{-1}} \bmod N^2$;

;

(III) 计算列 $A' = A - \gamma' + \alpha$ 的列密钥 $(m_{A'} = m_A \cdot (m_{\gamma'})^{-1} \cdot m_{\alpha} \bmod N^2, x_{A'} = x_A - x_{\gamma'} + x_{\alpha} \bmod N)$;

(IV) 计算辅助参数 P : $\zeta = -x_S^{-1} x_{A'} \bmod N, \eta = m_{A'} m_S^{\zeta} \bmod N^2$; 得到最后用户甲上传的辅助参数为 $(v \cdot \gamma^{-1}, \zeta, \eta)$ 。

步骤 (3) 运行步骤 (2) 设定的组合 SQL 查询指令: 服务商乙根据收到的来自用户甲的指令和步骤 (2) 计算得到的辅助参数 P 运行该指令, 保存该指令运行后的计算结果、更新数据并返回给用户甲查询结果 U ; 包括以下子步骤:

步骤 (3.1), 服务商乙在收到用户甲设定的组合 SQL 查询指令后进行相应的计算和操作, 根据其计算中的需求向用户甲提出对辅助参数 P 的请求或从用户甲随指令上传的辅助参数 P 中选取所需参数;

具体来说, 对于删除指令, 服务商乙只需进行正常的删除操作并更新数据库; 对于插入和更新操作, 若用户甲将行密钥与列密钥加密存储在服务商乙处, 则服务商乙只需返回用户

甲索取的行密钥和列密钥，接收用户甲上传的新数据进行正常的插入和更新即可；对于加和操作，若对A列和B列进行加和得到C列，则服务商乙计算C列的第i行元素 C_i 如下： $C_i = A_i \times B_i (i = 1, 2, 3, \dots, n)$ ，其中 A_i, B_i 分别表示A列和B列的第i行元素。在上述指令运行中，服务商乙不需要用户甲提供任何辅助参数。

对于搜索指定关键字操作，用户甲可以选择两列之间查询每一行是否为同一关键字或对某一列所有行查询是否为某一指定关键字，若用户甲对两列如A列和B列之间查询每一行是否为同一关键字，对应的列密钥为 (m_A, x_A) 和 (m_B, x_B) ，则服务商乙进行以下计算：

(I) 计算列 B' ，计算如下：列 B' 的第i行元素 $B'_i = B_i^{N-1} \bmod N^2 (i = 1, 2, \dots, n)$ ，其中， B_i 为B列的第i行元素；

(II) 计算列 A' ，计算如下：列 A' 的第i行元素 $A'_i = A_i \times B'_i \times E(\alpha)_i \bmod N^2 (i = 1, 2, \dots, n)$ ，其中， A_i 为A列的第i行元素， $E(\alpha)_i$ 为步骤(1.3)所述辅助数据 α 列的第i行元素；

(III) 服务商乙向用户甲提出对辅助参数P的请求或从用户甲随指令上传的辅助参数P中选取所需参数；

若用户甲对某一列如A列所有行查询是否为某一外部关键字如 v ，则服务商乙直接向用户甲提出对辅助参数P的请求或从用户甲随指令上传的辅助参数P中选取所需参数；

对于查询指定范围指令，用户甲可以选择两列之间互比较大小或某一列与同一个常数进行比较大小用于查询指定范围，若用户甲在两列如A列和B列相同行之间进行比较大小，两列对应的列密钥为 (m_A, x_A) 和 (m_B, x_B) ，则服务商乙进行以下计算：

(I) 计算列 B' ，计算如下：列 B' 的第i行元素 $B'_i = B_i^{N-1} \bmod N^2 (i = 1, 2, \dots, n)$ ，其中， B_i 为B列的第i行元素；

(II) 计算列 A' ，计算如下：列 A' 的第i行元素 $A'_i = A_i \times B'_i \times E(\alpha)_i \bmod N^2 (i = 1, 2, \dots, n)$ ，其中， A_i 为A列的第i行元素， $E(\alpha)_i$ 为步骤(1.3)所述辅助数据 α 列的第i行元素；

(III) 服务商乙向用户甲提出对辅助参数P的请求或从用户甲随指令上传的辅助参数P中选取所需参数；

若用户甲对某一列如A列所有行与同一个常数如 v 进行比较大小，则服务商乙直接向用户甲提出对辅助参数P的请求或从用户甲随指令上传的辅助参数P中选取所需参数。

步骤(3.2) 服务商乙收到辅助参数P后，根据指令进行计算，保存指令运行后的计算结果、更新数据并返回给用户甲查询结果U。

具体来说，对于搜索指定关键字操作，用户可以选择两列之间查询每一行是否为同一关键字或对某一列所有行查询是否为某一指定关键字，若用户对两列如A列和B列之间查询每一行是否为同一关键字，对应的列密钥为 (m_A, x_A) 和 (m_B, x_B) ，则服务商乙收到用户甲步骤(2)

计算并上传的辅助参数 $P: (\zeta, \eta)$ ，进行以下计算：

(I) 计算列 a ，计算列 a 的第 i 行元素 a_i 如下： $a_i = A'_i \times \eta \times E(1)_i^\zeta \bmod N^2$ ，其中， A'_i 为步骤(3.1)所述列 A' 的第 i 行元素， $E(1)_i$ 为步骤(1.3)所述辅助数据 S 列的第 i 行元素；

(II) 计算列 H ，计算列 H 的第 i 行元素 H_i 如下： $H_i = (h_i^{e_i})^{a_i} \bmod N_1$ ，其中， $h_i^{e_i}$ 为步骤(1.3)所述辅助数据 h 列的第 i 行元素， N_1 是步骤(1.3)所述 N_1 ；(III) 比较 $(h^{e_i \cdot (t_i \cdot a_i \bmod N)} \bmod N_2, H_i)$ ，其中， $h^{e_i \cdot (t_i \cdot a_i \bmod N)} \bmod N_2$ 为步骤(1.3)所述辅助数据 h' 列的第 i 行元素，若两者相等，则 A 列和 B 列第 i 行的元素相等；若不相等，则 A 列和 B 列第 i 行的元素不相等；

若用户甲对某一列如 A 列所有行查询是否为某一外部关键字如 v ，则服务商乙收到用户甲上传的辅助参数 $P: (v \cdot \gamma^{-1}, \zeta, \eta)$ 进行以下计算：

(I) 计算列 γ' ，列 γ' 为服务商乙根据步骤(1.3)所述辅助数据列 γ 和用户甲上传计算出的辅助参数 P 计算出的新列，列 γ' 的第 i 行元素 $E(\gamma')_i$ 通过列 γ 的第 i 行元素 $E(\gamma)_i$ 计算：

$$E(\gamma')_i = E(\gamma)_i^{v \cdot \gamma^{-1}} \bmod N^2$$

(II) 计算列 A' ，计算如下：列 A' 的第 i 行元素 $A'_i = A_i \times E(\gamma')_i^{N-1} \times E(\alpha)_i \bmod N^2 (i = 1, 2, \dots, n)$ ，其中， A_i 为 A 列的第 i 行元素， $E(\alpha)_i$ 为步骤(1.3)所述辅助数据 α 列的第 i 行元素；

(III) 计算列 a ，计算列 a 的第 i 行元素 a_i 如下： $a_i = A'_i \times \eta \times E(1)_i^\zeta \bmod N^2$ ，其中， A'_i 为步骤(3.1)所述列 A' 的第 i 行元素， $E(1)_i$ 为步骤(1.3)所述辅助数据 S 列的第 i 行元素；

(IV) 计算列 H ，计算列 H 的第 i 行元素 H_i 如下： $H_i = (h_i^{e_i})^{a_i} \bmod N_1$ ，其中， $h_i^{e_i}$ 为步骤(1.3)所述辅助数据 h 列的第 i 行元素， N_1 是步骤(1.3)所述 N_1 ；

(V) 比较 $(h^{e_i \cdot (t_i \cdot a_i \bmod N)} \bmod N_2, H_i)$ ，其中， $h^{e_i \cdot (t_i \cdot a_i \bmod N)} \bmod N_2$ 为步骤(1.3)所述辅助数据 h' 列的第 i 行元素，若两者相等，则 A 列第 i 行的元素与 v 相等；若不相等，则 A 列第 i 行的元素与 v 不相等；

对于查询指定范围指令，用户甲可以选择两列之间互比较大小或某一列与同一个常数进行比较大小用于查询指定范围，若用户甲在两列如 A 列和 B 列相同行之间进行比较大小，两列对应的列密钥为 (m_A, x_A) 和 (m_B, x_B) ，服务商乙收到用户甲上传的辅助参数 $P: (\zeta, \eta)$ 进行以下计算：

(I) 计算列 a ，计算列 a 的第 i 行元素 a_i 如下： $a_i = A'_i \times \eta \times E(1)_i^\zeta \bmod N^2$ ，其中， A'_i 为步骤(3.1)所述列 A' 的第 i 行元素， $E(1)_i$ 为步骤(1.3)所述辅助数据 S 列的第 i 行元素；

(II) 计算列 a' , 计算列 a' 的第 i 行元素 a'_i 如下: $a'_i = a_i \times (\beta_i \cdot t_i^{-1}) + u_i - \beta_i \alpha_i \bmod N$, 其中, $\beta_i t_i^{-1}$ 为步骤(1.3)所述辅助数据 β 列的第 i 行元素, $u_i - \beta_i \alpha_i$ 是步骤(1.3)所述 u 列的第 i 行元素;

(III) 比较 a'_i 与 $\frac{N}{2}$, 若 $a'_i > \frac{N}{2}$, 则 A 列第 i 行的元素较小; 不然, 则 B 列第 i 行的元素不大于 A 列第 i 行的元素;

若用户甲对某一列如 A 列所有行与同一个常数如 v 进行比较大小, 则服务商乙收到用户甲上传的辅助参数 $P: (v \cdot \gamma^{-1}, \zeta, \eta)$, 进行以下计算:

(I) 计算列 γ' , 列 γ' 为服务商乙根据步骤(1.3)所述辅助数据列 γ 和用户甲上传计算出的辅助参数 P 计算出的新列, 列 γ' 的第 i 行元素 $E(\gamma')_i$ 通过列 γ 的第 i 行元素 $E(\gamma)_i$ 计算:

$$E(\gamma')_i = E(\gamma)_i^{v \cdot \gamma^{-1}} \bmod N^2$$

(II) 计算列 A' , 计算如下: 列 A' 的第 i 行元素 $A'_i = A_i \times E(\gamma')_i^{N-1} \times E(\alpha)_i \bmod N^2 (i = 1, 2, \dots, n)$, 其中, A_i 为 A 列的第 i 行元素, $E(\alpha)_i$ 为步骤(1.3)所述辅助数据 α 列的第 i 行元素;

(III) 计算列 a , 计算列 a 的第 i 行元素 a_i 如下: $a_i = A'_i \times \eta \times E(1)_i^{\zeta} \bmod N^2$, 其中, A'_i 为步骤(3.1)所述列 A' 的第 i 行元素, $E(1)_i$ 为步骤(1.3)所述辅助数据 S 列的第 i 行元素;

(IV) 计算列 a' , 计算列 a' 的第 i 行元素 a'_i 如下: $a'_i = a_i \times (\beta_i \cdot t_i^{-1}) + u_i - \beta_i \alpha_i \bmod N$, 其中, $\beta_i t_i^{-1}$ 为步骤(1.3)所述辅助数据 β 列的第 i 行元素, $u_i - \beta_i \alpha_i$ 是步骤(1.3)所述 u 列的第 i 行元素;

(V) 比较 a'_i 与 $\frac{N}{2}$, 若 $a'_i < \frac{N}{2}$, 则 A 列第 i 行的元素不小于 v ; 不然, 则 A 列第 i 行的元素小于 v 。

实施例 2

本发明公开了一种支持可组合 SQL 查询的加密数据库系统, 可以执行任意本发明任意实施例所提供的安全存储用户数据并对用户数据支持更新、插入、删除、加和、搜索指定关键字和查询指定范围的功能。所述支持可组合 SQL 查询的加密数据库系统包括用户装置模块和服务商模块; 所述用户装置模块对用户数据进行加密和预处理, 并将加密结果和预处理数据上传给服务商模块; 所述用户模块执行数据操作指令, 根据实际需求上传运行指令给服务商模块, 所述运行指令包括更新、插入、删除、加和、搜索指定关键字和查询指定范围, 并上传辅助参数运行指令到服务商模块, 所述辅助参数运行指令包括更新、插入、删除、加和、搜索指定关键字和查询指定范围; 所述服务商模块根据收到的运行指令和辅助参数运行指令保存指令运行后的计算结果、更新数据并返回给用户模块查询结果。

实施例 3

在数据库领域，某企业运行数据库测试国际标准 TPC-C 进行交易，即某一个货物仓库同时接受多个用户的订单，该仓库同时与这些用户发生多笔交易。为了节省内存和提高性能，仓库将交易数据加密存储到云端，根据实时交易的需求，仓库不断向云端的加密数据提交 SQL 指令（指令包括更新、插入、删除、加和、搜索指定关键字和查询指定范围），根据指令对于实际交易的意义，指令被分为五个集合：

- 1.新订单（New-Order）：客户输入一笔新的订货交易。
- 2.支付操作（Payment）：更新客户账户余额以及反映其支付状况。
- 3.发货（Delivery）：发货（模拟批处理交易）。
- 4.订单状态查询（Order-Status）：查询客户最近交易的状态。
- 5.库存状态查询（Stock-Level）：查询仓库库存状态，以便能够及时补货。

本实施例用一台装有两个 2.5GHz Intel Xeon Gold 6248 处理器，配有 256GB 内存的服务器模拟该云端服务商，使用本发明方法对五个集合的指令分别进行执行，所花费的时间如表 1。

表 1

交易事务	运行1次耗时/ms	运行2次耗时/ms	运行3次耗时/ms
New-Order	192023	411606	614116
Payment	136020	275803	417246
Delivery	422247	843313	1266638
Order-Status	346161	690062	1051611
Stock-Level	101926	204299	293828

如上表 1 所示，本发明支持对 TPC-C 五种事务的执行，完成一次 TPC-C 五种事务时，本发明所用的最短时间为 101 秒，而最长时间也仅为 422 秒（Delivery 事务），由于 TPC-C 的每种事务由数十条 SQL 查询指令组成，可见本发明在实际商业活动中，即使考虑了传输的延迟，仍然能在 10 秒左右完成一条 SQL 查询指令，且在此过程中，能始终保证用户的数据隐私。此外，随着执行次数的增加，本发明所用时间始终保持稳定，因此能在实际商业活动中保持着稳定的性能。因此，使用本发明方法，数据库运行速度较快，时间消耗少，运行稳定。综上，本发明基于离散对数问题，实现了对用户数据的加密保护、减少了用户隐私信息的泄露，从而为实际商业活动中用户数据的云端存储提供了安全完整的保护方案；本发明实现了在加密数据上安全高效地执行可组合 SQL 查询指令，指令包括更新、插入、删除、加和、搜索指定关键字和查询指定范围，满足了实际商业活动中用户对云端存储数据远程操作和查询的需求；本发明具有通用性强、安全高效、保护隐私、使用简便、效率高、内存和时间消耗少等优点。

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

权 利 要 求 书

1、一种支持可组合 SQL 查询的加密数据库方法，其特征在于，包括以下步骤：

(1) 加密存储数据：用户对自己的存储数据进行加密和预处理，并将加密结果和预处理数据上传给服务商，所述服务商提供用于运行数据库的软件、装置、电子设备或存储介质存储用户上传的数据；所述步骤 (1) 具体包括以下子步骤：

(1.1) 用户针对自己的数据，生成随机数集合作为数据的行密钥和列密钥；基于乘法加密，用户用行密钥和列密钥来加密数据，输出加密后的数据库；

(1.2) 用户将加密后的数据库上传到服务商处，用户选择任意一种加密方式将步骤 (1.1) 生成的行密钥加密上传到服务商实现对行密钥的加密存储，同时根据需求选择将列密钥不加密地存储在本地或加密上传至服务商处；

(1.3) 用户针对指令进行预处理，生成运行指令所需的辅助数据；用户将辅助数据上传至服务商，所述服务商不能从该辅助数据中获取任何关于数据库的隐私信息；所述指令包括更新、插入、删除、加和、搜索指定关键字和查询指定范围操作；

(1.4) 服务商根据实际情况选择存储形式，所述存储形式包括数据库软件、装置、电子设备或存储介质，并基于该存储形式进行存储加密数据和辅助数据，并进行后续指令执行。

(2) 设定组合 SQL 查询指令，用户根据实际需求上传组合 SQL 查询指令给服务商，并上传用于查询指令的辅助参数；

(3) 运行步骤 (2) 设定的组合 SQL 查询指令：服务商根据收到的来自用户的组合 SQL 查询指令和辅助参数运行查询指令，保存指令运行后的计算结果、更新数据并返回给用户查询结果。

2、根据权利要求 1 所述的支持可组合 SQL 查询的加密数据库方法，其特征在于，所述步骤 (1.1) 具体为：

用户随机生成两个大质数 p 和 q ，得到大整数 $N = p \cdot q$ ；用户将此大整数 N 作为生成元 g 的阶数，并在有限域 Z_{N^2} 上找到生成元 g ；用户将生成随机数作为行密钥和列密钥，利用该行密钥和列密钥来加密数据库，第 i 行的行密钥为 $(r_i, t_i) \in Z_N^2$ ；第 j 列的列密钥为 (m_j, x_j) ，其中 $m_j \in Z_{N^2}, x_j \in Z_N$ ；行密钥和列密钥应保证对于任意的 i, j ，都存在整数 $M_{(i,j)} \in Z_{N^2}$ 使得 $m_j g^{r_i x_j} \cdot M_{(i,j)} \bmod N^2 = 1$ ，把该整数 $M_{(i,j)}$ 称为 $m_j g^{r_i x_j}$ 相对于 N^2 的逆，记为 $(m_j g^{r_i x_j})^{-1}$ ；最后数据库第 i 行第 j 列的元素 $v_{(i,j)}$ 被加密如下：

$$c_{(i,j)} = (N + 1)^{t_i v_{(i,j)}} \cdot (m_j g^{r_i x_j})^{-1} \mod N^2$$

3、根据权利要求 1 所述的支持可组合 SQL 查询的加密数据库方法，其特征在于，所述步骤（1.3）具体为：

对于删除和加和指令，用户无需生成辅助数据 D；

对于更新和插入指令，用户每更新或插入一行数据，则需提前生成一个行密钥加密存放至服务商处，更新和插入时，用户从服务商处下载提前生成的行密钥，从服务商或本地获取列密钥，实现对更新的数据进行解密更新并重新加密上传至服务商处或直接将插入的数据进行加密上传至服务商处；

对于搜索指定关键字指令，用户可以选择两列之间查询每一行是否为同一关键字或对某一列所有行查询是否为某一指定关键字，若用户对两列之间查询相同行是否为同一关键字，则用户每进行一次查询需要生成一列加密的随机数 $\alpha_i (i = 1, 2, \dots, n)$ ，对应的列密钥为 (m_α, x_α) ，加密方式为 $E(\alpha_i) = (m_\alpha \cdot g^{r_i x_\alpha})^{-1} \cdot (N + 1)^{t_i \alpha} \mod N^2$ ；每一行加密的元素都是 1，统称这列为 S 列，所述 S 列对应的列密钥为 (m_s, x_s) ，第 i 行元素 1 被加密为 $E(1)_i = (m_s \cdot g^{r_i x_s})^{-1} \cdot 1 \mod N^2$ ，其中， m_s 存在对于 N^2 的逆 $m_s^{-1} \in Z_{N^2}$ ，即 $m_s \cdot m_s^{-1} \mod N^2 = 1$ ； x_s 存在对于 N 的逆 $x_s^{-1} \in Z_N$ ，即 $x_s \cdot x_s^{-1} \mod N = 1$ ；一列随机数 $h_i^{e_i} (i = 1, 2, \dots, n)$ ，其中 h_i 为 Z_{N_1} 上的 N_2 阶生成元， N_1 为两个或多个随机大质数的积， N_2 为其中任意一个大质数，即 N_2 整除 N_1 ， e_i 是 Z_{N_2} 上的随机整数；一列数 $h^{e_i \cdot (t_i \cdot \alpha_i \mod N) \mod N_2} (i = 1, 2, \dots, N)$ ；若用户对某一列所有行查询是否为某一指定关键字，则用户每进行一次查询除需要上述两列之间比较每一行是否为同一关键字所需的辅助数据外还需要额外生成一列加密的 γ ，即每一行加密的元素都是 γ ，对应的列密钥为 (m_γ, x_γ) ，第 i 行元素被加密为 $E(\gamma)_i = (m_\gamma \cdot g^{r_i x_\gamma})^{-1} \cdot (N + 1)^{t_i \gamma}$ ，其中， γ 为 Z_N 上的随机数， γ 应保证存在相对于 N 的逆 $\gamma^{-1} \in Z_N$ ，即 $\gamma \cdot \gamma^{-1} \mod N = 1$ ；

对于查询指定范围指令，用户选择两列之间互相比对或某一列与同一个常数进行比较用于查询指定范围，若用户对两列之间互相比对，则每一次比较操作都需要生成一列加密的随机数 $\alpha_i (i = 1, 2, \dots, n)$ ，对应的列密钥为 (m_α, x_α) ，加密方式为 $E(\alpha_i) = (m_\alpha \cdot g^{r_i x_\alpha})^{-1} \cdot (N + 1)^{t_i \alpha} \mod N^2$ ；每一行加密的元素都是 1，统称这列为 S 列，所述 S 列对应的列密钥为 (m_s, x_s) ，第 i 行元素 1 被加密为 $E(1)_i = (m_s \cdot g^{r_i x_s})^{-1} \cdot 1 \mod N^2$ ，其中， m_s 存在对于 N^2 的逆 $m_s^{-1} \in Z_{N^2}$ ，即 $m_s \cdot m_s^{-1} \mod N^2 = 1$ ； x_s 存在对于 N 的逆 $x_s^{-1} \in Z_N$ ，即 $x_s \cdot x_s^{-1} \mod N = 1$ ；一列 $\beta_i \cdot t_i^{-1} (i = 1, 2, \dots, n)$ ，一列 $u_i - \beta_i \cdot \alpha_i$ ，其中 $t_i^{-1} \in Z_N$ 为 t_i 相对于 N 的逆，即 $t_i^{-1} \cdot t_i \mod N = 1$ ， β_i, u_i 为 Z_N 上的随机数且满足 $0 \ll u_i \ll \beta_i \ll \frac{N}{2}$ ；若用户对某一列与同一个常

数进行比较, 则用户每进行一次比较操作除需要上述两列之间相互比较需要的辅助数据外还需要额外生成一列加密的 γ , 即每一行加密的元素都是 γ , 对应的列密钥为 (m_γ, x_γ) , 第 i 行元素被加密为 $E(\gamma)_i = (m_\gamma \cdot g^{r_i x_\gamma})^{-1} \cdot (N+1)^{t_i \gamma}$, 其中, γ 为 Z_N 上的随机数, γ 应保证存在相对于 N 的逆 $\gamma^{-1} \in Z_N$, 即 $\gamma \cdot \gamma^{-1} \bmod N = 1$ 。

4、根据权利要求1所述的支持可组合SQL查询的加密数据库方法, 其特征在于, 所述步骤(2)具体包括以下子步骤:

(2.1) 用户根据其实际的商业需求上传运行指令至服务商; 所述运行指令包括更新、加和、搜索指定关键字和查询指定范围;

(2.2) 用户根据其上传的指令计算辅助参数, 并将该辅助参数随指令或在接收到服务商请求后上传至服务商:

所述步骤(2.2)具体为, 对于更新、插入和删除操作, 用户无需进行任何辅助参数的计算; 对于加和操作, 若对 A 列和 B 列进行加和, 对应的列密钥为 (m_A, x_A) 和 (m_B, x_B) , 则新生成列 $C = A + B$ 的列密钥被用户进行计算并存储, 相应计算方式为 $(m_C = m_A \cdot m_B \bmod N^2, x_C = x_A + x_B \bmod N)$, 用户选择本地不加密地存储该密钥或加密上传至服务商处进行存储; 对于搜索指定关键字指令, 用户选择两列之间查询每一行是否为同一关键字或对某一列所有行查询是否为某一指定关键字, 若用户对两列如 A 列和 B 列之间查询每一行是否为同一关键字, 对应的列密钥为 (m_A, x_A) 和 (m_B, x_B) , 则用户需计算:

(I) 列 $A' = A - B + \alpha$ 的列密钥 $(m_{A'} = m_A \cdot m_B^{-1} \cdot m_\alpha \bmod N^2, x_{A'} = x_A - x_B + x_\alpha \bmod N)$;

(II) 计算辅助参数 $\zeta = -x_S^{-1} x_{A'} \bmod N, \eta = m_{A'} m_S^\zeta \bmod N^2$, 得到最后用户上传的辅助参数为 (ζ, η) ;

若用户对某一列如 A 列所有行查询是否为某一指定关键字如 v , 则用户需计算:

(I) $v \cdot \gamma^{-1}$, 其中 γ 为步骤(1.3)所述辅助数据;

(II) 列 $\gamma' = E(\gamma)^{v \cdot \gamma^{-1}}$ 的列密钥 $(m_{\gamma'} = m_\gamma^{v \cdot \gamma^{-1}} \bmod N^2, x_{\gamma'} = v \cdot \gamma^{-1} \cdot x_\gamma \bmod N)$, 其中, 列 γ' 为服务商通过列 γ 计算出的新列, 列 γ' 的第 i 行元素 $E(\gamma')_i$ 通过列 γ 的第 i 行元素 $E(\gamma)_i$ 计算:
 $E(\gamma')_i = E(\gamma)_i^{v \cdot \gamma^{-1}} \bmod N^2$;

(III) 列 $A' = A - \gamma' + \alpha$ 的列密钥 $(m_{A'} = m_A \cdot (m_{\gamma'})^{-1} \cdot m_\alpha \bmod N^2, x_{A'} = x_A - x_{\gamma'} + x_\alpha \bmod N)$;

(IV) 计算辅助参数 P : $\zeta = -x_S^{-1}x_{A'} \bmod N, \eta = m_{A'}m_S^\zeta \bmod N^2$; 得到最后用户上传的辅助参数为 $(v \cdot \gamma^{-1}, \zeta, \eta)$ 。

对于查询指定范围指令, 用户选择两列之间互相比大小或某一列与同一个常数进行比较大用于查询指定范围, 若用户在两列如 A 列和 B 列相同行之间进行比较大, 两列对应的列密钥为 (m_A, x_A) 和 (m_B, x_B) , 则用户需计算:

(I) 列 $A' = A - B + \alpha$ 的列密钥 $(m_{A'} = m_A \cdot m_B^{-1} \cdot m_\alpha \bmod N^2, x_{A'} = x_A - x_B + x_\alpha \bmod N)$; (2) $\zeta = -x_S^{-1}x_{A'} \bmod N, \eta = m_{A'}m_S^\zeta \bmod N^2$; 得到最后用户上传的辅助参数为 (ζ, η) ;

若用户对某一列如 A 列所有行与同一个常数如 v 进行比较大, 则用户需计算

(I) $v \cdot \gamma^{-1}$, 其中 γ 为步骤 (1.3) 所述辅助数据;

(II) 计算列 γ' 的列密钥 $(m_{\gamma'} = m_\gamma^{v \cdot \gamma^{-1}} \bmod N^2, x_{\gamma'} = v \cdot \gamma^{-1} \cdot x_\gamma \bmod N)$, 其中, 列 γ' 为服务商通过列 γ 计算出的新列, 列 γ' 的第 i 行元素 $E(\gamma')_i$ 通过列 γ 的第 i 行元素 $E(\gamma)_i$ 计算:
 $E(\gamma')_i = E(\gamma)_i^{v \cdot \gamma^{-1}} \bmod N^2$;

(III) 计算列 $A' = A - \gamma' + \alpha$ 的列密钥 $(m_{A'} = m_A \cdot (m_{\gamma'})^{-1} \cdot m_\alpha \bmod N^2, x_{A'} = x_A - x_{\gamma'} + x_\alpha \bmod N)$;

(IV) 计算辅助参数 $\zeta = -x_S^{-1}x_{A'} \bmod N, \eta = m_{A'}m_S^\zeta \bmod N^2$; 得到最后用户上传的辅助参数为 $(v \cdot \gamma^{-1}, \zeta, \eta)$ 。

5、根据权利要求 1 所述的支持可组合 SQL 查询的加密数据库方法, 其特征在于, 所述步骤 (3) 具体包括以下子步骤:

(3.1) 服务商在收到用户的组合 SQL 查询指令后进行相应的计算和操作, 根据其计算中的需求向用户提出对辅助参数的请求或从用户随指令上传的辅助参数中选取所需参数;

(3.2) 服务商收到辅助参数后, 根据指令进行计算, 保存指令运行后的计算结果、更新数据并返回给用户查询结果。

6、根据权利要求 5 所述的支持可组合 SQL 查询的加密数据库方法, 其特征在于, 所述步骤 (3.1) 具体为: 对于删除指令, 服务商只需进行正常的删除操作并更新数据库; 对于插入和更新操作, 若用户将行密钥与列密钥加密存储在服务商处, 则服务商只需返回用户索取的行密钥和列密钥, 接收用户上传的新数据进行正常的插入和更新即可; 对于加和操作, 若对 A 列和 B 列进行加和得到 C 列, 则服务商计算 C 列的第 i 行元素 C_i 如下: $C_i = A_i \times B_i (i = 1, 2, 3, \dots, n)$,

其中 A_i , B_i 分别表示 A 列和 B 列的第 i 行元素。在上述指令运行中, 服务商不需要用户提供任何辅助参数;

对于搜索指定关键字操作, 用户选择两列之间查询每一行是否为同一关键字或对某一列所有行查询是否为某一指定关键字, 若用户对两列如 A 列和 B 列之间查询每一行是否为同一关键字, 对应的列密钥为 (m_A, x_A) 和 (m_B, x_B) , 则服务商进行以下计算:

(I) 计算列 B' , 计算如下: 列 B' 的第 i 行元素 $B'_i = B_i^{N-1} \bmod N^2$, 其中, B_i 为 B 列的第 i 行元素;

(II) 计算列 A' , 计算如下: 列 A' 的第 i 行元素 $A'_i = A_i \times B'_i \times E(\alpha)_i \bmod N^2$, 其中, A_i 为 A 列的第 i 行元素, $E(\alpha)_i$ 为步骤(1.3)所述辅助数据 α 列的第 i 行元素;

(III) 服务商向用户提出对辅助参数 P 的请求或从用户随指令上传的辅助参数中选取所需参数;

若用户对某一列如 A 列所有行查询是否为某一外部关键字如 v , 则服务商直接向用户提出对辅助参数的请求或从用户随指令上传的辅助参数中选取所需参数;

对于查询指定范围指令, 用户可以选择两列之间互比较大小或某一列与同一个常数进行比较大小用于查询指定范围, 若用户在两列如 A 列和 B 列相同行之间进行比较大小, 两列对应的列密钥为 (m_A, x_A) 和 (m_B, x_B) , 则服务商进行以下计算:

(I) 计算列 B' , 计算如下: 列 B' 的第 i 行元素 $B'_i = B_i^{N-1} \bmod N^2$, 其中, B_i 为 B 列的第 i 行元素;

(II) 计算列 A' , 计算如下: 列 A' 的第 i 行元素 $A'_i = A_i \times B'_i \times E(\alpha)_i \bmod N^2$, 其中, A_i 为 A 列的第 i 行元素, $E(\alpha)_i$ 为步骤(1.3)所述辅助数据 α 列的第 i 行元素;

(III) 服务商向用户提出对辅助参数的请求或从用户随指令上传的辅助参数中选取所需参数;

若用户对某一列如 A 列所有行与同一个常数如 v 进行比较大小, 则服务商直接向用户提出对辅助参数的请求或从用户随指令上传的辅助参数中选取所需参数。

7、根据权利要求5所述的支持可组合 SQL 查询的加密数据库方法, 其特征在于, 所述步骤(3.2)具体为: 对于搜索指定关键字操作, 用户选择两列之间查询每一行是否为同一关键字或对某一列所有行查询是否为某一指定关键字, 若用户对两列如 A 列和 B 列之间查询每一行是否为同一关键字, 对应的列密钥为 (m_A, x_A) 和 (m_B, x_B) , 则服务商收到用户步骤(2)计算并上传的辅助参数 (ζ, η) , 进行以下计算:

(I) 计算列 a , 计算列 a 的第 i 行元素 a_i 如下: $a_i = A'_i \times \eta \times E(1)_i^\zeta \bmod N^2$, 其中, A'_i 为

步骤 (3.1) 所述列A'的第i行元素, $E(1)_i$ 为步骤 (1.3) 所述辅助数据S列的第i行元素;

(II) 计算列H, 计算列H的第i行元素 H_i 如下: $H_i = (h_i^{e_i})^{a_i} \bmod N_1$, 其中, $h_i^{e_i}$ 为步骤 (1.3) 所述辅助数据h列的第i行元素, N_1 是步骤 (1.3) 所述 N_1 ; (III) 比较 $(h^{e_i \cdot (t_i \cdot \alpha_i \bmod N)} \bmod N_2, H_i)$, 其中, $h^{e_i \cdot (t_i \cdot \alpha_i \bmod N)} \bmod N_2$ 为步骤 (1.3) 所述辅助数据h'列的第i行元素, 若两者相等, 则A列和B列第i行的元素相等; 若不相等, 则A列和B列第i行的元素不相等;

若用户对某一列如A列所有行查询是否为某一外部关键字如v, 则服务商收到用户上传的辅助参数 $(v \cdot \gamma^{-1}, \zeta, \eta)$ 进行以下计算:

(I) 计算列 γ' , 列 γ' 为服务商根据步骤 (1.3) 所述辅助数据列 γ 和用户上传计算出的辅助参数 P 计算出的新列, 列 γ' 的第i行元素 $E(\gamma')_i$ 通过列 γ 的第i行元素 $E(\gamma)_i$ 计算:

$$E(\gamma')_i = E(\gamma)_i^{v \cdot \gamma^{-1}} \bmod N^2$$

(II) 计算列A', 计算如下: 列A'的第i行元素 $A'_i = A_i \times E(\gamma')_i^{N-1} \times E(\alpha)_i \bmod N^2$, 其中, A_i 为A列的第i行元素, $E(\alpha)_i$ 为步骤 (1.3) 所述辅助数据 α 列的第i行元素;

(III) 计算列a, 计算列a的第i行元素 a_i 如下: $a_i = A'_i \times \eta \times E(1)_i^{\zeta} \bmod N^2$, 其中, A'_i 为步骤 (3.1) 所述列A'的第i行元素, $E(1)_i$ 为步骤 (1.3) 所述辅助数据S列的第i行元素;

(IV) 计算列H, 计算列H的第i行元素 H_i 如下: $H_i = (h_i^{e_i})^{a_i} \bmod N_1$, 其中, $h_i^{e_i}$ 为步骤 (1.3) 所述辅助数据h列的第i行元素, N_1 是步骤 (1.3) 所述 N_1 ;

(V) 比较 $(h^{e_i \cdot (t_i \cdot \alpha_i \bmod N)} \bmod N_2, H_i)$, 其中, $h^{e_i \cdot (t_i \cdot \alpha_i \bmod N)} \bmod N_2$ 为步骤 (1.3) 所述辅助数据h'列的第i行元素, 若两者相等, 则A列第i行的元素与v相等; 若不相等, 则A列第i行的元素与v不相等;

对于查询指定范围指令, 用户选择两列之间互比较大小或某一列与同一个常数进行比较大小用于查询指定范围, 若用户在两列如A列和B列相同行之间进行比较大小, 两列对应的列密钥为 (m_A, x_A) 和 (m_B, x_B) , 服务商收到用户上传的辅助参数 P: (ζ, η) 进行以下计算:

(I) 计算列a, 计算列a的第i行元素 a_i 如下: $a_i = A'_i \times \eta \times E(1)_i^{\zeta} \bmod N^2$, 其中, A'_i 为步骤 (3.1) 所述列A'的第i行元素, $E(1)_i$ 为步骤 (1.3) 所述辅助数据S列的第i行元素;

(II) 计算列a', 计算列a'的第i行元素 a'_i 如下: $a'_i = a_i \times (\beta_i \cdot t_i^{-1}) + u_i - \beta_i \alpha_i \bmod N$, 其中, $\beta_i t_i^{-1}$ 为步骤 (1.3) 所述辅助数据 β 列的第i行元素, $u_i - \beta_i \alpha_i$ 是步骤 (1.3) 所述u列的第i行元素;

(III) 比较 a'_i 与 $\frac{N}{2}$, 若 $a'_i > \frac{N}{2}$, 则A列第*i*行的元素较小; 不然, 则B列第*i*行的元素不大于A列第*i*行的元素;

若用户对某一列如A列所有行与同一个常数如 v 进行比较大小, 则服务商收到用户上传的辅助参数 $(v \cdot \gamma^{-1}, \zeta, \eta)$, 进行以下计算:

(I) 计算列 γ' , 列 γ' 为服务商根据步骤(1.3)所述辅助数据列 γ 和用户上传计算出的辅助参数 P 计算出的新列, 列 γ' 的第 i 行元素 $E(\gamma')_i$ 通过列 γ 的第 i 行元素 $E(\gamma)_i$ 计算:

$$E(\gamma')_i = E(\gamma)_i^{v \cdot \gamma^{-1}} \bmod N^2$$

(II) 计算列 A' , 计算如下: 列 A' 的第 i 行元素 $A'_i = A_i \times E(\gamma')_i^{N-1} \times E(\alpha)_i \bmod N^2 (i = 1, 2, \dots, n)$, 其中, A_i 为A列的第 i 行元素, $E(\alpha)_i$ 为步骤(1.3)所述辅助数据 α 列的第 i 行元素;

(III) 计算列 a , 计算列 a 的第 i 行元素 a_i 如下: $a_i = A'_i \times \eta \times E(1)_i^{\zeta} \bmod N^2$, 其中, A'_i 为步骤(3.1)所述列 A' 的第 i 行元素, $E(1)_i$ 为步骤(1.3)所述辅助数据 S 列的第 i 行元素;

(IV) 计算列 a' , 计算列 a' 的第 i 行元素 a'_i 如下: $a'_i = a_i \times (\beta_i \cdot t_i^{-1}) + u_i - \beta_i \alpha_i \bmod N$, 其中, $\beta_i t_i^{-1}$ 为步骤(1.3)所述辅助数据 β 列的第 i 行元素, $u_i - \beta_i \alpha_i$ 是步骤(1.3)所述 u 列的第 i 行元素;

(V) 比较 a'_i 与 $\frac{N}{2}$, 若 $a'_i < \frac{N}{2}$, 则A列第*i*行的元素不小于 v ; 不然, 则A列第*i*行的元素小于 v 。

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2021/110269

A. CLASSIFICATION OF SUBJECT MATTER

G06F 16/2455(2019.01)i; G06F 21/62(2013.01)i; G06F 16/23(2019.01)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)

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; CNKI; SIPOABS; DWPI; USTXT; WOTXT; EPTXT: 查询, 语句, 重写, 重构, 组合, 改写, 转换, 加密, 乘法, 同态, 行密钥, 列密钥, 隐私, 泄露, SQL, refactor, rewrite, multiplication, encryption, key, homomorphic, privacy

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 112800088 A (NORTHEASTERN UNIVERSITY) 14 May 2021 (2021-05-14) description, paragraphs [0035]-[0064]	1-7
A	CN 110750797 A (NANJING UNIVERSITY) 04 February 2020 (2020-02-04) entire document	1-7
A	CN 111859426 A (XIDIAN UNIVERSITY) 30 October 2020 (2020-10-30) entire document	1-7
A	US 2013191650 A1 (BALAKRISHNAN, H. et al.) 25 July 2013 (2013-07-25) entire document	1-7



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

“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

16 April 2022

Date of mailing of the international search report

27 April 2022

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing
100088, China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2021/110269

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	112800088	A	14 May 2021	None			
CN	110750797	A	04 February 2020	None			
CN	111859426	A	30 October 2020	None			
US	2013191650	A1	25 July 2013	US	9087212	B2	21 July 2015

国际检索报告

国际申请号

PCT/CN2021/110269

A. 主题的分类

G06F 16/2455(2019.01)i; G06F 21/62(2013.01)i; G06F 16/23(2019.01)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)

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;CNKI;SIPOABS;DWPI;USTXT;WOTXT;EPTXT: 查询, 语句, 重写, 重构, 组合, 改写, 转换, 加密, 乘法, 同态, 行密钥, 列密钥, 隐私, 泄露, SQL, refactor, rewrite, multiplication, encryption, key, homomorphic, privacy

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
A	CN 112800088 A (东北大学) 2021年5月14日 (2021 - 05 - 14) 说明书第[0035]-[0064]段	1-7
A	CN 110750797 A (南京大学) 2020年2月4日 (2020 - 02 - 04) 全文	1-7
A	CN 111859426 A (西安电子科技大学) 2020年10月30日 (2020 - 10 - 30) 全文	1-7
A	US 2013191650 A1 (BALAKRISHNAN HARI等) 2013年7月25日 (2013 - 07 - 25) 全文	1-7

☐ 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

“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

2022年4月16日

国际检索报告邮寄日期

2022年4月27日

ISA/CN的名称和邮寄地址

中国国家知识产权局(ISA/CN)

中国北京市海淀区蓟门桥西土城路6号 100088

传真号 (86-10)62019451

授权官员

张琳

电话号码 (86-512) 88996292

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2021/110269

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	112800088	A	2021年5月14日	无			
CN	110750797	A	2020年2月4日	无			
CN	111859426	A	2020年10月30日	无			
US	2013191650	A1	2013年7月25日	US	9087212	B2	2015年7月21日