(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 115801327 A
(43)申请公布日 2023.03.14

(21)申请号 202211311956.4

(22)申请日 2022.10.25

(71)申请人 翼方健数(北京)信息科技有限公司
地址 100037 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 厦门翼方健数信息科技有限公司
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 北京华清迪源知识产权代理有限公司 11577
专利代理师 孙志一

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 9/32(2006.01)
H04L 9/20(2006.01)

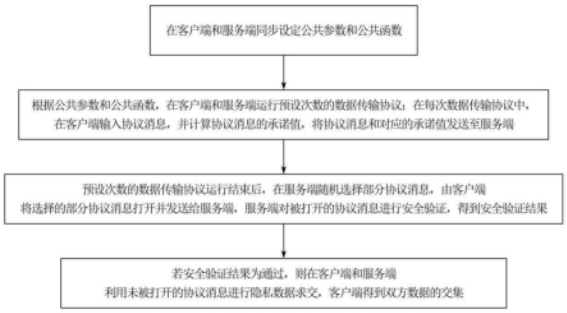
权利要求书4页 说明书13页 附图5页

(54)发明名称

一种安全的数据交互方法、系统、设备及存储介质

(57)摘要

本发明实施例公开了一种安全的数据交互方法、系统、设备及存储介质,首先在客户端和服务端同步设定公共参数并约定公共函数,然后在客户端和服务端运行预设次数的数据传输协议;在每次数据传输协议中,在客户端输入协议消息,并计算协议消息的承诺值,将协议消息和承诺值发送至服务端;协议运行结束后,在服务端随机选择部分协议消息,客户端将选择的部分协议消息打开并发送给服务端,服务端对被打开的协议消息进行安全验证,若安全验证通过,则在客户端和服务端进行隐私数据求交,客户端得到双方数据的交集。本发明实施例通过在数据传输协议阶段增加安全验证来保证服务端数据在恶意攻击下的安全性,从而避免客户端通过恶意攻击获取服务端数据。



CN 115801327 A

1.一种安全的数据交互方法,其特征在于,所述方法包括:

在客户端和服务端同步设定公共参数并约定公共函数;

根据所述公共参数和所述公共函数,在所述客户端和所述服务端运行预设次数的数据传输协议;在每次所述数据传输协议中,在所述客户端输入协议消息,并计算所述协议消息的承诺值,将所述协议消息和对应的所述承诺值发送至所述服务端;

预设次数的数据传输协议运行结束后,在所述服务端随机选择部分协议消息,由所述客户端将选择的部分协议消息打开并发送给所述服务端,所述服务端对被打开的协议消息进行安全验证,得到安全验证结果;

若所述安全验证结果为通过,则在所述客户端和所述服务端利用未被打开的协议消息进行隐私数据求交,所述客户端得到双方数据的交集。

2.如权利要求1所述的一种安全的数据交互方法,其特征在于,所述公共参数包括:密钥安全参数λ、第一协议参数m、第一协议参数ω、协议安全参数s、第一长度参数l_1和第二长度参数l_2,其中,s=2ω;所述公共函数包括:第一哈希函数H_1、第二哈希函数H_2、伪随机函数F和承诺函数Comm。

3.如权利要求2所述的一种安全的数据交互方法,其特征在于,在所述客户端和所述服务端运行预设次数的数据传输协议之前,包括:

在所述服务端根据所述协议安全参数s随机生成选择字符串cs。

4.如权利要求3所述的一种安全的数据交互方法,其特征在于,在所述客户端和所述服务端运行预设次数的数据传输协议之前,还包括:

在所述客户端根据所述第一协议参数m和所述协议安全参数s生成初始矩阵D,所述初始矩阵D为m行、s列的二进制矩阵,所述初始矩阵D中的所有元素均为1;

在所述客户端根据所述密钥安全参数λ随机采样生成二进制的密钥字符串k;

对于客户端本地数据中的每个元素y,利用所述第一哈希函数H_1、所述伪随机函数F以及所述密钥字符串k,计算得到加密结果v,所述加密结果v的计算公式为:

$$v=F_k(H_1(y))$$

其中,F_k表示基于所述密钥字符串k的伪随机函数F;

令所述初始矩阵D中的对应元素$D_i[v[i]]$为0,得到更新后的密文数据矩阵D′,其中,v[i]表示所述加密结果v中的第i个字符,$D_i[v[i]]$表示所述初始矩阵D的第i列、第v[i]行的元素,i为大于或等于0且小于或等于s的整数;

在所述客户端随机生成m行、s列的第一加密矩阵A;

利用所述第一加密矩阵A与所述客户端数据矩阵D′,计算得到第二加密矩阵B,所述第二加密矩阵B的计算公式为:

$$B = A \oplus D'$$

其中,$\oplus$表示矩阵的异或运算。

5.如权利要求4所述的一种安全的数据交互方法,其特征在于,根据所述公共参数和所述公共函数,在所述客户端和所述服务端运行预设次数的数据传输协议;在每次所述数据传输协议中,在所述客户端输入协议消息,并计算所述协议消息的承诺值,将所述协议消息和对应的所述承诺值发送至所述服务端,包括:

在所述服务端根据所述协议安全参数s随机生成第一承诺向量ra和第二承诺向量rb,

并发送至所述客户端；

在每次所述数据传输协议中，在所述客户端利用所述第一加密矩阵A和所述第二加密矩阵B得到待选择数据组$\{A_i,B_i\}$作为所述协议消息，其中，A_i表示所述第一加密矩阵A的第i列，B_i表示所述第二加密矩阵B的第i列；

所述客户端根据所述待选择数据组$\{A_i,B_i\}$、所述承诺函数Comm、所述第一承诺向量ra和所述第二承诺向量rb，计算得到第一承诺计算结果ca[i]和第二承诺计算结果cb[i]，所述第一承诺计算结果ca[i]的计算公式为：

$ca[i]=Comm(A_i,ra[i])$

其中，ra[i]表示所述第一承诺向量ra的第i个元素；

所述第二承诺计算结果cb[i]的计算公式为：

$cb[i]=Comm(B_i,rb[i])$

其中，rb[i]表示所述第二承诺向量rb的第i个元素；

所述客户端将所述待选择数据组$\{A_i,B_i\}$、所述第一承诺计算结果ca[i]和所述第二承诺计算结果cb[i]发送至所述服务端。

6.如权利要求5所述的一种安全的数据交互方法，其特征在于，在所述服务端随机选择部分协议消息，由所述客户端将选择的部分协议消息打开并发送给所述服务端，所述服务端对所述被打开的协议消息进行安全验证，得到安全验证结果，包括：

在所述服务端根据所述选择字符串cs对所述待选择数据组$\{A_i,B_i\}$进行选择；

若所述选择字符串cs的第i个字符cs[i]为0，则选择所述第一加密矩阵A的第i列A_i作为选择数据c_i；

若所述选择字符串cs的第i个字符cs[i]为1，则选择所述第二加密矩阵B的第i列B_i作为选择数据c_i；

利用各个所述选择数据c_i得到第三加密矩阵C；

在所述服务端根据所述第一协议参数ω随机生成验证向量ro，并将所述验证向量ro发送至所述客户端，其中，所述验证向量ro中的元素均为小于或等于s的正整数，并且所述验证向量ro中各个元素互不相同；

根据所述验证向量ro，在所述客户端从所述第一加密矩阵A和所述第二加密矩阵B中分别提取对应的第一验证数据$A_{ro[j]}$和第二验证数据$B_{ro[j]}$，将所述第一验证数据$A_{ro[j]}$和所述第二验证数据$B_{ro[j]}$返回至所述服务端，其中，ro[j]表示所述验证向量ro的第j个元素，$A_{ro[j]}$表示所述第一加密矩阵A的第ro[j]列，$B_{ro[j]}$表示所述第二加密矩阵B的第ro[j]列，j为大于或等于0且小于或等于ω的整数；

根据所述第一验证数据$A_{ro[j]}$、所述第二验证数据$B_{ro[j]}$、所述承诺函数Comm、所述第一承诺向量ra和所述第二承诺向量rb，在所述服务端计算得到第一承诺验证结果da和第二承诺验证结果db，所述第一承诺验证结果da的计算公式为：

$da=Comm(A_{ro[j]},ra[ro[j]])$

其中，ra[ro[j]]表示所述第一承诺向量ra的第ro[j]个元素；

所述第二承诺验证结果db的计算公式为：

$db=Comm(B_{ro[j]},rb[ro[j]])$

其中，rb[ro[j]]表示所述第二承诺向量rb的第ro[j]个元素；

根据所述第一承诺计算结果ca[i]、所述第二承诺计算结果cb[i]、所述第一承诺验证结果da、所述第二承诺验证结果db和所述第三加密矩阵C,在所述服务端对所述第一验证数据$A_{ro[j]}$和所述第二验证数据$B_{ro[j]}$进行安全验证;

判断是否同时满足第一条件、第二条件、第三条件;

所述第一条件为:所述第一验证数据$A_{ro[j]}$与所述第二验证数据$B_{ro[j]}$不相同;

所述第二条件为:所述验证向量ro的第j个元素对应的所述第一承诺计算结果ca[ro[j]]等于第一承诺验证结果da,并且所述验证向量ro的第j个元素对应的所述第二承诺计算结果cb[ro[j]]等于第二承诺验证结果db;

所述第三条件为:当所述选择字符串cs的第ro[j]个字符cs[ro[j]]为0时,所述第三加密矩阵C的第ro[j]列$C_{ro[j]}$等于所述第一验证数据$A_{ro[j]}$,并且当所述选择字符串cs的第ro[j]个字符cs[ro[j]]为1时,所述第三加密矩阵C的第ro[j]列$C_{ro[j]}$等于所述第二验证数据$B_{ro[j]}$;

若不满足所述第一条件或所述第二条件或所述第三条件,则安全验证结果为不通过,终止所述客户端和所述服务端的数据交互过程;

若同时满足所述第一条件、所述第二条件和所述第三条件,则安全验证结果为通过。

7.如权利要求6所述的一种安全的数据交互方法,其特征在于,在所述客户端和所述服务端利用未被打开的协议消息进行隐私数据求交,所述客户端得到双方数据的交集,包括:

在所述客户端将所述第一验证数据$A_{ro[j]}$从所述第一加密矩阵A中删除,得到m行、ω列的第四加密矩阵E,并将所述密钥字符串k发送至所述服务端;

在所述服务端将所述第三加密矩阵C的第ro[j]列$C_{ro[j]}$从所述第三加密矩阵C中删除,得到m行、ω列的第五加密矩阵G;

在所述服务端,对于所述服务端本地数据中的每个元素x,利用所述第一哈希函数H_1、所述伪随机函数F以及所述字符串密钥k,计算得到第一加密向量p,所述第一加密向量p的计算公式为:

$$p=F_k(H_1(x))$$

在所述服务端将所述第一加密向量p中的p[ro[j]删除,得到第二加密向量p′,其中,p[ro[j]]表示所述第一加密向量p的第ro[j]个字符;

在所述服务端利用所述第二加密向量p′、所述第五加密矩阵G和所述第二哈希函数H_2,计算得到第一加密密文φ_1,所述第一加密密文φ_1的计算公式为:

$$\varphi_1 = H_2(G_1[p'[1]] \| \ldots \| G_\omega[p'[\omega]])$$

其中,p′[ω]表示所述第二加密向量p′的第ω个字符,G_ω[p′[ω]]表示所述第五加密矩阵G的第ω列、第p′[ω]行的元素;

在所述服务端将所有所述第一加密密文φ_1发送至所述客户端;

在所述客户端,对于所述客户端本地数据中的每个元素y,利用所述第一哈希函数H_1、所述伪随机函数F以及所述字符串密钥k,计算得到第三加密向量q,所述第三加密向量q的计算公式为:

$$q=F_k(H_1(y))$$

在所述客户端将所述第三加密向量q中的q[ro[j]]删除,得到第四加密向量q′,其中,q

[ro[j]]表示所述第三加密向量q的第ro[j]个字符；

在所述客户端利用所述第四加密向量q′、所述第四加密矩阵E和所述第二哈希函数H_2，计算第二加密密文φ_2，所述第二加密密文φ_2的计算公式为：

$$\varphi_2 = H_2(E_1\left[q'[1]\right] \| \ldots \| E_\omega\left[q'[\omega]\right])$$

其中，q′[ω]表示所述第四加密向量q′的第ro[j]个字符，E_ω[q′[ω]]表示所述第四加密矩阵E的第ω列、第q′[ω]行的元素；

在所述客户端将所述第二加密密文φ_2和接收到的所述第一加密密文φ_1进行对比，所述客户端得到所述服务端本地数据与所述客户端本地数据的交集。

8.一种安全的数据交互系统，其特征在于，所述系统包括客户端和服务端，具体用于：

在客户端和服务端同步设定公共参数并约定公共函数；

根据所述公共参数和所述公共函数，在所述客户端和所述服务端运行预设次数的数据传输协议；在每次所述数据传输协议中，在所述客户端输入协议消息，并计算所述协议消息的承诺值，将所述协议消息和对应的所述承诺值发送至所述服务端；

预设次数的数据传输协议运行结束后，在所述服务端随机选择部分协议消息，由所述客户端将选择的部分协议消息打开并发送给所述服务端，所述服务端对被打开的协议消息进行安全验证，得到安全验证结果；

若所述安全验证结果为通过，则在所述客户端和所述服务端利用未被打开的协议消息进行隐私数据求交，所述客户端得到双方数据的交集。

9.一种安全的数据交互设备，其特征在于，所述设备包括：处理器和存储器；

所述存储器用于存储一个或多个程序指令；

所述处理器，用于运行一个或多个程序指令，用以执行如权利要求1至7中任一项所述的一种安全的数据交互方法的步骤。

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上存储有计算机程序，所述计算机程序被处理器执行时实现如权利要求1至7中任一项所述的一种安全的数据交互方法的步骤。

一种安全的数据交互方法、系统、设备及存储介质

技术领域

[0001] 本发明实施例涉及加密通信技术领域，具体涉及一种安全的数据交互方法、系统、设备及存储介质。

背景技术

[0002] 隐匿求交(Private Set Intersection)简称PSI协议，能够允许持有各自数据集合的两方执行双方数据集合的交集运算。PSI协议结束之后，一方或两方能够得到交集结果，但是双方都无法获知交集以外的对方集合数据的任何信息，PSI协议广泛应用于纵向联邦学习等场景中。

[0003] 现有的基于OPRF的PSI算法对于服务端来说不满足恶意攻击下的安全性要求，其主要原因是在不经意传输协议过程中，如果客户端违反协议进行恶意攻击，例如客户端在不经意传输协议中输入相同的协议消息，客户端即可破解服务端的加密矩阵，从而获取服务端的全部数据，所以上述算法不满足服务端数据在恶意攻击下的安全性要求。

发明内容

[0004] 为此，本发明实施例提供一种安全的数据交互方法、系统、设备及存储介质，以解决现有的基于OPRF的PSI算法在数据传输阶段无法进行安全验证的问题。

[0005] 为了实现上述目的，本发明实施例提供如下技术方案：

[0006] 根据本发明实施例的第一方面，提供了一种安全的数据交互方法，所述方法包括：

[0007] 在客户端和服务端同步设定公共参数并约定公共函数；

[0008] 根据所述公共参数和所述公共函数，在所述客户端和所述服务端运行预设次数的数据传输协议；在每次所述数据传输协议中，在所述客户端输入协议消息，并计算所述协议消息的承诺值，将所述协议消息和对应的所述承诺值发送至所述服务端；

[0009] 预设次数的数据传输协议运行结束后，在所述服务端随机选择部分协议消息，由所述客户端将选择的部分协议消息打开并发送给所述服务端，所述服务端对所述被打开的协议消息进行安全验证，得到安全验证结果；

[0010] 若所述安全验证结果为通过，则在所述客户端和所述服务端利用未被打开的协议消息进行隐私数据求交，所述客户端得到双方数据的交集。

[0011] 进一步地，所述公共参数包括：密钥安全参数λ、第一协议参数m、第一协议参数ω、协议安全参数s、第一长度参数l_1和第二长度参数l_2，其中，$s=2\omega$；所述公共函数包括：第一哈希函数H_1、第二哈希函数H_2、伪随机函数F和承诺函数Comm。

[0012] 进一步地，在所述客户端和所述服务端运行预设次数的数据传输协议之前，包括：

[0013] 在所述服务端根据所述协议安全参数s随机生成选择字符串cs。

[0014] 进一步地，在所述客户端和所述服务端运行预设次数的数据传输协议之前，还包括：

[0015] 在所述客户端根据所述第一协议参数m和所述协议安全参数s生成初始矩阵D，所

述初始矩阵D为m行、s列的二进制矩阵，所述初始矩阵D中的所有元素均为1；

[0016] 在所述客户端根据所述密钥安全参数λ随机采样生成二进制的密钥字符串k；

[0017] 对于客户端本地数据中的每个元素y，利用所述第一哈希函数H_1、所述伪随机函数F以及所述密钥字符串k，计算得到加密结果v，所述加密结果v的计算公式为：

[0018] $v=F_k(H_1(y))$

[0019] 其中，F_k表示基于所述密钥字符串k的伪随机函数F；

[0020] 令所述初始矩阵D中的对应元素$D_i[v[i]]$为0，得到更新后的密文数据矩阵D'，其中，v[i]表示所述加密结果v中的第u个字符，$D_i[v[i]]$表示所述初始矩阵D的第i列、第v[i]行的元素，i为大于或等于0且小于或等于s的整数；

[0021] 在所述客户端随机生成m行、s列的第一加密矩阵A；

[0022] 利用所述第一加密矩阵A与所述客户端数据矩阵D'，计算得到所述第二加密矩阵B，所述第二加密矩阵B的计算公式为：

[0023] $$B = A \oplus D'$$

[0024] 其中，$\oplus$表示矩阵的异或运算。

[0025] 进一步地，根据所述公共参数和所述公共函数，在所述客户端和所述服务端运行预设次数的数据传输协议；在每次所述数据传输协议中，在所述客户端输入协议消息，并计算所述协议消息的承诺值，将所述协议消息和对应的所述承诺值发送至所述服务端，包括：

[0026] 在所述服务端根据所述协议安全参数s随机生成第一承诺向量ra和第二承诺向量rb，并发送至所述客户端；

[0027] 在每次所述数据传输协议中，在所述客户端利用所述第一加密矩阵A和所述第二加密矩阵B得到待选择数据组$\{A_i,B_i\}$作为所述协议消息，其中，A_i表示所述第一加密矩阵A的第i列，B_i表示所述第二加密矩阵B的第i列；

[0028] 所述客户端根据所述待选择数据组$\{A_i,B_i\}$、所述承诺函数Comm、所述第一承诺向量ra和所述第二承诺向量rb，计算得到第一承诺计算结果ca[i]和第二承诺计算结果cb[i]，所述第一承诺计算结果ca[i]的计算公式为：

[0029] $ca[i]=Comm(A_i,ra[i])$

[0030] 其中，ra[i]表示所述第一承诺向量ra的第i个元素；

[0031] 所述第二承诺计算结果cb[i]的计算公式为：

[0032] $Cb[i]=Comm(B_i,rb[i])$

[0033] 其中，rb[i]表示所述第二承诺向量rb的第i个元素；

[0034] 所述客户端将所述待选择数据组$\{A_i,B_i\}$、所述第一承诺计算结果ca[i]和所述第二承诺计算结果cb[i]发送至所述服务端。

[0035] 进一步地，在所述服务端随机选择部分协议消息，由所述客户端将选择的部分协议消息打开并发送给所述服务端，所述服务端对所述被打开的协议消息进行安全验证，得到安全验证结果，包括：

[0036] 在所述服务端根据所述选择字符串cs对所述待选择数据组$\{A_i,B_i\}$进行选择；

[0037] 若所述选择字符串cs的第i个字符cs[i]为0，则选择所述第一加密矩阵A的第i列A_i作为选择数据c_i；

[0038] 若所述选择字符串cs的第i个字符cs[i]为1,则选择所述第二加密矩阵B的第i列B_i作为选择数据c_i;

[0039] 利用各个所述选择数据c_i得到所述第三加密矩阵C;

[0040] 在所述服务端根据所述第一协议参数ω随机生成验证向量ro,并将所述验证向量ro发送至所述客户端,其中,所述验证向量ro中的元素均为小于或等于s的正整数,并且所述验证向量ro中各个元素互不相同;

[0041] 根据所述验证向量ro,在所述客户端从所述第一加密矩阵A和所述第二加密矩阵B中分别提取对应的第一验证数据$A_{ro[j]}$和第二验证数据$B_{ro[j]}$,将所述第一验证数据$A_{ro[j]}$和所述第二验证数据$B_{ro[j]}$返回至所述服务端,其中,ro[j]表示所述验证向量ro的第j个元素,$A_{ro[j]}$表示所述第一加密矩阵A的第ro[j]列,$B_{ro[j]}$表示所述第二加密矩阵B的第rp[j]列,j为大于或等于0且小于或等于ω的整数;

[0042] 根据所述第一验证数据$A_{ro[j]}$、所述第二验证数据$B_{ro[j]}$、所述承诺函数Comm、所述第一承诺向量ra和所述第二承诺向量rb,在所述服务端计算得到第一承诺验证结果da和第二承诺验证结果db,所述第一承诺验证结果da的计算公式为:

[0043] $da=Comm(A_{ro[j]},r0[ro[j]])$

[0044] 其中,ra[ro[j]]表示所述第一承诺向量ra的第ro[j]个元素;

[0045] 所述第二承诺验证结果db的计算公式为:

[0046] $db=Comm(B_{ro[j]},rb[ro[j]])$

[0047] 其中,rb[ro[j]]表示所述第二承诺向量rb的第ro[j]个元素;

[0048] 根据所述第一承诺计算结果ca[i]、所述第二承诺计算结果cb[i]、所述第一承诺验证结果da、所述第二承诺验证结果db和所述第三加密矩阵C,在所述服务端对所述第一验证数据$A_{ro[j]}$和所述第二验证数据$B_{ro[j]}$进行安全验证;

[0049] 判断是否同时满足第一条件、第二条件、第三条件;

[0050] 所述第一条件为:所述第一验证数据$A_{ro[j]}$与所述第二验证数据$B_{ro[j]}$不相同;

[0051] 所述第二条件为:所述验证向量ro的第j个元素对应的所述第一承诺计算结果ca[ro[j]]等于第一承诺验证结果da,并且所述验证向量ro的第j个元素对应的所述第二承诺计算结果cb[ro[j]]等于第二承诺验证结果db;

[0052] 所述第三条件为:当所述选择字符串cs的第ro[j]个字符cs[ro[j]]为0时,所述第三加密矩阵C的第ro[j]列$C_{ro[j]}$等于所述第一验证数据$A_{ro[j]}$,并且当所述选择字符串cs的第ro[j]个字符cs[ro[j]]为1时,所述第三加密矩阵C的第ro[j]列$C_{ro[j]}$等于所述第二验证数据$B_{ro[j]}$;

[0053] 若不满足所述第一条件或所述第二条件或所述第三条件,则安全验证结果为不通过,终止所述客户端和所述服务端的数据交互过程;

[0054] 若同时满足所述第一条件、所述第二条件和所述第三条件,则安全验证结果为通过。

[0055] 进一步地,在所述客户端和所述服务端利用未被打开的协议消息进行隐私数据求交,所述客户端得到双方数据的交集,包括:

[0056] 在所述客户端将所述第一验证数据$A_{ro[j]}$从所述第一加密矩阵A中删除,得到m行、ω列的第四加密矩阵E,并将所述密钥字符串k发送至所述服务端;

[0057] 在所述服务端将所述第三加密矩阵C的第ro[j]列$C_{ro[j]}$从所述第三加密矩阵C中删除，得到m行、ω列第五加密矩阵G；

[0058] 在所述服务端，对于所述服务端本地数据中的每个元素x，利用所述第一哈希函数H_1、所述伪随机函数F以及所述字符串密钥k，计算得到第一加密向量p，所述第一加密向量p的计算公式为：

[0059] $p=F_k(H_i(x))$

[0060] 在所述服务端将所述第一加密向量p中的p[ro[j]]删除，得到第二加密向量p'，其中，p[ro[j]]表示所述第一加密向量p的第ro[j]个字符；

[0061] 在所述服务端利用所述第二加密向量p'、所述第五加密矩阵G和所述第二哈希函数H_2，计算得到第一加密密文φ_1，所述第一加密密文φ_1的计算公式为：

[0062] $$\varphi_1 = H_2(G_1[p'[1]] \| \ldots \| G_\omega[p'[\omega]])$$

[0063] 其中，p'[ω]表示所述第二加密向量p'的第ω个字符，G_ω[p'[ω]]表示所述第五加密矩阵G的第ω列、第p'[ω]行的元素；

[0064] 在所述服务端将所有所述第一加密密文φ_1发送至所述客户端；

[0065] 在所述客户端，对于所述客户端本地数据中的每个元素y，利用所述第一哈希函数H_1、所述伪随机函数F以及所述字符串密钥k，计算得到第三加密向量q，所述第三加密向量q的计算公式为：

[0066] $q=F_k(H_1(y))$

[0067] 在所述客户端将所述第三加密向量q中的q[ro[j]]删除，得到第四加密向量q'，其中，q[ro[j]]表示所述第三加密向量q的第ro[j]个字符；

[0068] 在所述客户端利用所述第四加密向量q'、所述第四加密矩阵E和所述第二哈希函数H_2，计算第二加密密文φ_2，所述第二加密密文φ_2的计算公式为：

[0069] $$\varphi_2 = H_2(E_1[q'[1]] \| \ldots \| E_\omega[q'[\omega]])$$

[0070] 其中，q'[ω]表示所述第四加密向量q'的第ro[j]个字符，E_ω[q'[ω]]表示所述第四加密矩阵E的第ω列、第q'[ω]行的元素；

[0071] 在所述客户端将所述第二加密密文φ_2和接收到的所述第一加密密文φ_1进行对比，所述客户端得到所述服务端本地数据与所述客户端本地数据的交集。

[0072] 根据本发明实施例的第二方面，提供了一种安全的数据交互系统，所述系统包括客户端和服务端，具体用于：

[0073] 在客户端和服务端同步设定公共参数并约定公共函数；

[0074] 根据所述公共参数和所述公共函数，在所述客户端和所述服务端运行预设次数的数据传输协议；在每次所述数据传输协议中，在所述客户端输入协议消息，并计算所述协议消息的承诺值，将所述协议消息和对应的所述承诺值发送至所述服务端；

[0075] 预设次数的数据传输协议运行结束后，在所述服务端随机选择部分协议消息，由所述客户端将选择的部分协议消息打开并发送给所述服务端，所述服务端对所述被打开的协议消息进行安全验证，得到安全验证结果；

[0076] 若所述安全验证结果为通过，则在所述客户端和所述服务端利用未被打开的协议消息进行隐私数据求交，所述客户端得到双方数据的交集。

[0077] 进一步地，所述公共参数包括：密钥安全参数λ、第一协议参数m、第一协议参数ω、协议安全参数s、第一长度参数l_1和第二长度参数l_2，其中，s＝2ω；所述公共函数包括：第一哈希函数H_1、第二哈希函数H_2、伪随机函数F和承诺函数Comm。

[0078] 进一步地，在所述客户端和所述服务端运行预设次数的数据传输协议之前，包括：

[0079] 在所述服务端根据所述协议安全参数s随机生成选择字符串cs。

[0080] 进一步地，在所述客户端和所述服务端运行预设次数的数据传输协议之前，还包括：

[0081] 在所述客户端根据所述第一协议参数m和所述协议安全参数s生成初始矩阵D，所述初始矩阵D为m行、s列的二进制矩阵，所述初始矩阵D中的所有元素均为1；

[0082] 在所述客户端根据所述密钥安全参数λ随机采样生成二进制的密钥字符串k；

[0083] 对于客户端本地数据中的每个元素y，利用所述第一哈希函数H_1、所述伪随机函数F以及所述密钥字符串k，计算得到加密结果v，所述加密结果v的计算公式为：

[0084] $v=F_k(H_i(y))$

[0085] 其中，F_k表示基于所述密钥字符串k的伪随机函数F；

[0086] 令所述初始矩阵D中的对应元素$D_i[v[i]]$为0，得到更新后的密文数据矩阵D'，其中，v[i]表示所述加密结果v中的第i个字符，$D_i[v[i]]$表示所述初始矩阵D的第i列、第v[i]行的元素，i为大于或等于0且小于或等于s的整数；

[0087] 在所述客户端随机生成m行、s列的第一加密矩阵A；

[0088] 利用所述第一加密矩阵A与所述客户端数据矩阵D'，计算得到所述第二加密矩阵B，所述第二加密矩阵B的计算公式为：

[0089] $$B = A \oplus D'$$

[0090] 其中，$\oplus$表示矩阵的异或运算。

[0091] 进一步地，根据所述公共参数和所述公共函数，在所述客户端和所述服务端运行预设次数的数据传输协议；在每次所述数据传输协议中，在所述客户端输入协议消息，并计算所述协议消息的承诺值，将所述协议消息和对应的所述承诺值发送至所述服务端，包括：

[0092] 在所述服务端根据所述协议安全参数s随机生成第一承诺向量ra和第二承诺向量rb，并发送至所述客户端；

[0093] 在每次所述数据传输协议中，在所述客户端利用所述第一加密矩阵A和所述第二加密矩阵B得到待选择数据组$\{A_i,B_i\}$作为所述协议消息，其中，A_i表示所述第一加密矩阵A的第i列，B_i表示所述第二加密矩阵B的第i列；

[0094] 所述客户端根据所述待选择数据组$\{A_i,B_i\}$、所述承诺函数Comm、所述第一承诺向量ra和所述第二承诺向量rb，计算得到第一承诺计算结果ca[i]和第二承诺计算结果cb[i]，所述第一承诺计算结果ca[i]的计算公式为：

[0095] $ca[i]=Comm(A_i,ra[i])$

[0096] 其中，ra[i]表示所述第一承诺向量ra的第i个元素；

[0097] 所述第二承诺计算结果cb[i]的计算公式为：

[0098] $cb[i]=Comm(B_i,rb[i])$

[0099] 其中，rb[i]表示所述第二承诺向量rb的第i个元素；

[0100] 所述客户端将所述待选择数据组$\{A_i,B_i\}$、所述第一承诺计算结果ca[i]和所述第二承诺计算结果cb[i]发送至所述服务端。

[0101] 进一步地，在所述服务端随机选择部分协议消息，由所述客户端将选择的部分协议消息打开并发送给所述服务端，所述服务端对所述被打开的协议消息进行安全验证，得到安全验证结果，包括：

[0102] 在所述服务端根据所述选择字符串cs对所述待选择数据组$\{A_i,B_i\}$进行选择；

[0103] 若所述选择字符串cs的第i个字符cs[i]为0，则选择所述第一加密矩阵A的第i列A_i作为选择数据c_i；

[0104] 若所述选择字符串cs的第i个字符cs[i]为1，则选择所述第二加密矩阵B的第i列B_i作为选择数据c_i；

[0105] 利用各个所述选择数据c_i得到所述第三加密矩阵C；

[0106] 在所述服务端根据所述第一协议参数ω随机生成验证向量ro，并将所述验证向量ro发送至所述客户端，其中，所述验证向量ro中的元素均为小于或等于s的正整数，并且所述验证向量ro中各个元素互不相同；

[0107] 根据所述验证向量ro，在所述客户端从所述第一加密矩阵A和所述第二加密矩阵B中分别提取对应的第一验证数据$A_{ro[j]}$和第二验证数据$B_{ro[j]}$，将所述第一验证数据$A_{ro[j]}$和所述第二验证数据$B_{ro[j]}$返回至所述服务端，其中，ro[j]表示所述验证向量ro的第j个元素，$A_{ro[j]}$表示所述第一加密矩阵A的第ro[j]列，$B_{ro[j]}$表示所述第二加密矩阵B的第ro[j]列，j为大于或等于0且小于或等于ω的整数；

[0108] 根据所述第一验证数据$A_{ro[j]}$、所述第二验证数据$B_{ro[j]}$、所述承诺函数Comm、所述第一承诺向量ra和所述第二承诺向量rb，在所述服务端计算得到第一承诺验证结果da和第二承诺验证结果db，所述第一承诺验证结果da的计算公式为：

[0109] $da=Comm(A_{ro[j]},ra[ro[j]])$

[0110] 其中，ra[ro[j]]表示所述第一承诺向量ra的第ro[j]个元素；

[0111] 所述第二承诺验证结果db的计算公式为：

[0112] $db=Comm(B_{ro[j]},rb[ro[j]])$

[0113] 其中，rb[ro[j]]表示所述第二承诺向量rb的第ro[j]个元素；

[0114] 根据所述第一承诺计算结果ca[i]、所述第二承诺计算结果cb[i]、所述第一承诺验证结果da、所述第二承诺验证结果db和所述第三加密矩阵C，在所述服务端对所述第一验证数据$A_{ro[j]}$和所述第二验证数据$B_{ro[j]}$进行安全验证；

[0115] 判断是否同时满足第一条件、第二条件、第三条件；

[0116] 所述第一条件为：所述第一验证数据$A_{ro[j]}$与所述第二验证数据$B_{ro[j]}$不相同；

[0117] 所述第二条件为：所述验证向量ro的第j个元素对应的所述第一承诺计算结果ca[ro[j]]等于第一承诺验证结果da，并且所述验证向量ro的第j个元素对应的所述第二承诺计算结果cb[ro[j]]等于第二承诺验证结果db；

[0118] 所述第三条件为：当所述选择字符串cs的第ro[j]个字符cs[ro[j]]为0时，所述第三加密矩阵C的第ro[j]列$C_{ro[j]}$等于所述第一验证数据$A_{ro[j]}$，并且当所述选择字符串cs的

第ro[j]个字符cs[ro[j]]为1时，所述第三加密矩阵C的第ro[j]列$C_{ro[j]}$等于所述第二验证数据$B_{ro[j]}$；

[0119] 若不满足所述第一条件或所述第二条件或所述第三条件，则安全验证结果为不通过，终止所述客户端和所述服务端的数据交互过程；

[0120] 若同时满足所述第一条件、所述第二条件和所述第三条件，则安全验证结果为通过。

[0121] 进一步地，在所述客户端和所述服务端利用未被打开的协议消息进行隐私数据求交，所述客户端得到双方数据的交集，包括：

[0122] 在所述客户端将所述第一验证数据$A_{ro[j]}$从所述第一加密矩阵A中删除，得到m行、ω列的第四加密矩阵E，并将所述密钥字符串k发送至所述服务端；

[0123] 在所述服务端将所述第三加密矩阵C的第ro[j]列$C_{ro[j]}$从所述第三加密矩阵C中删除，得到m行、ω列第五加密矩阵G；

[0124] 在所述服务端，对于所述服务端本地数据中的每个元素x，利用所述第一哈希函数H_1、所述伪随机函数F以及所述字符串密钥k，计算得到第一加密向量p，所述第一加密向量p的计算公式为：

[0125] $p=F_k(H_1(x))$

[0126] 在所述服务端将所述第一加密向量p中的p[ro[j]]删除，得到第二加密向量p'，其中，p[ro[j]]表示所述第一加密向量p的第ro[j]个字符；

[0127] 在所述服务端利用所述第二加密向量p'、所述第五加密矩阵G和所述第二哈希函数H_2，计算得到第一加密密文φ_1，所述第一加密密文φ_1的计算公式为：

[0128] $$\varphi_1 = H_2(G_1\left[p'[1]\right] \| \ldots \| G_\omega\left[p'[\omega]\right])$$

[0129] 其中，p'[ω]表示所述第二加密向量p'的第ω个字符，G_ω[p'[ω]]表示所述第五加密矩阵G的第ω列、第p'[ω]行的元素；

[0130] 在所述服务端将所有所述第一加密密文φ_1发送至所述客户端；

[0131] 在所述客户端，对于所述客户端本地数据中的每个元素y，利用所述第一哈希函数H_1、所述伪随机函数F以及所述字符串密钥k，计算得到第三加密向量q，所述第三加密向量q的计算公式为：

[0132] $q=F_k(H_1(y))$

[0133] 在所述客户端将所述第三加密向量q中的q[ro[j]]删除，得到第四加密向量q'，其中，q[ro[j]]表示所述第三加密向量q的第ro[j]个字符；

[0134] 在所述客户端利用所述第四加密向量q'、所述第四加密矩阵E和所述第二哈希函数H_2，计算第二加密密文φ_2，所述第二加密密文φ_2的计算公式为：

[0135] $$\varphi_2 = H_2(E_1\left[q'[1]\right] \| \ldots \| E_\omega\left[q'[\omega]\right])$$

[0136] 其中，q'[ω]表示所述第四加密向量q'的第ro[j]个字符，E_ω[q'[ω]]表示所述第四加密矩阵E的第ω列、第q'[ω]行的元素；

[0137] 在所述客户端将所述第二加密密文φ_2和接收到的所述第一加密密文φ_1进行对

比，所述客户端得到所述服务端本地数据与所述客户端本地数据的交集。

[0138] 根据本发明实施例的第三方面，提供了一种安全的数据交互设备，所述设备包括：处理器和存储器；

[0139] 所述存储器用于存储一个或多个程序指令；

[0140] 所述处理器，用于运行一个或多个程序指令，用以执行如上任一项所述的一种安全的数据交互方法的步骤。

[0141] 根据本发明实施例的第四方面，提供了一种计算机可读存储介质，所述计算机可读存储介质上存储有计算机程序，所述计算机程序被处理器执行时实现如上任一项所述一种安全的数据交互方法的步骤。

[0142] 本发明实施例具有如下优点：

[0143] 本发明实施例公开了一种安全的数据交互方法、系统、设备及存储介质，首先在客户端和服务端同步设定公共参数并约定公共函数，然后在客户端和服务端运行预设次数的数据传输协议；在每次数据传输协议中，在客户端输入协议消息，并计算协议消息的承诺值，将协议消息和承诺值发送至服务端；协议运行结束后，在服务端随机选择部分协议消息，客户端将选择的部分协议消息打开并发送给服务端，服务端对被打开的协议消息进行安全验证，若安全验证通过，则在客户端和服务端进行隐私数据求交，客户端得到双方数据的交集。本发明实施例通过在数据传输协议阶段增加安全验证来保证服务端数据在恶意攻击下的安全性，从而避免客户端通过恶意攻击获取服务端数据。

附图说明

[0144] 为了更清楚地说明本发明的实施方式或现有技术中的技术方案，下面将对实施方式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示例性的，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据提供的附图引伸获得其它的实施附图。

[0145] 本说明书所绘示的结构、比例、大小等，均仅用以配合说明书所揭示的内容，以供熟悉此技术的人士了解与阅读，并非用以限定本发明可实施的限定条件，故不具技术上的实质意义，任何结构的修饰、比例关系的改变或大小的调整，在不影响本发明所能产生的功效及所能达成的目的下，均应仍落在本发明所揭示的技术内容得能涵盖的范围内。

[0146] 图1为本发明实施例提供的一种安全的数据交互系统的结构示意图；

[0147] 图2为本发明实施例提供的一种安全的数据交互方法的流程示意图；

[0148] 图3为本发明实施例提供的数据预处理的流程示意图；

[0149] 图4为本发明实施例提供的数据传输协议的流程示意图；

[0150] 图5为本发明实施例提供的安全验证的流程示意图；

[0151] 图6为本发明实施例提供的隐私数据求交的流程示意图。

具体实施方式

[0152] 以下由特定的具体实施例说明本发明的实施方式，熟悉此技术的人士可由本说明书所揭露的内容轻易地了解本发明的其他优点及功效，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，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，都属于本发明保护的范围。

[0153] 参考图1，本发明实施例提供了一种安全的数据交互系统，上述系统包括客户端和服务端。

[0154] 进一步地，上述系统具体用于在客户端和服务端同步设定公共参数并约定公共函数；根据公共参数和公共函数，在客户端和服务端运行预设次数的数据传输协议；在每次数据传输协议中，在客户端输入协议消息，并计算协议消息的承诺值，将协议消息和对应的承诺值发送至服务端；在服务端随机选择部分协议消息，由客户端将选择的部分协议消息打开并发送给服务端，服务端对被打开的协议消息进行安全验证，得到安全验证结果；在客户端和服务端利用未被打开的协议消息进行隐私数据求交，客户端得到双方数据的交集。

[0155] 本发明实施例公开了一种安全的数据交互系统，首先在客户端和服务端同步设定公共参数并约定公共函数，然后在客户端和服务端运行预设次数的数据传输协议；在每次数据传输协议中，在客户端输入协议消息，并计算协议消息的承诺值，将协议消息和承诺值发送至服务端；协议运行结束后，在服务端随机选择部分协议消息，客户端将选择的部分协议消息打开并发送给服务端，服务端对被打开的协议消息进行安全验证，若安全验证通过，则在客户端和服务端进行隐私数据求交，客户端得到双方数据的交集。本发明实施例通过在数据传输协议阶段增加安全验证来保证服务端数据在恶意攻击下的安全性，从而避免客户端通过恶意攻击获取服务端数据。

[0156] 与上述公开的一种安全的数据交互系统相对应，本发明实施例还公开了一种安全的数据交互方法。以下结合上述描述的一种安全的数据交互系统详细介绍本发明实施例中公开的一种安全的数据交互方法。

[0157] 参考图2，以下对本发明实施例提供的一种安全的数据交互方法的具体步骤进行描述。

[0158] 在客户端和服务端同步设定公共参数并约定公共函数。

[0159] 上述步骤具体包括：根据客户端和服务端双方的数据量，同步设定公共参数并约定公共函数。上述公共参数包括：密钥安全参数λ、第一协议参数m、第一协议参数ω、协议安全参数s、第一长度参数l_1和第二长度参数l_2，其中，s＝2ω，例如：客户端和服务端双方数据的元素数量最大值为1000万，则同步设置第一协议参数$m=2^{20}$，第二协议参数$\omega=2^{10}$，协议安全参数$s=2^{21}$，第一长度参数$l_1=256$，第二长度参数$l_2=128$。

[0160] 上述公共函数包括第一哈希函数H_1、第二哈希函数H_2和伪随机函数F，上述第一哈希函数H_1的函数式为：

[0161] $$H_1: \{0,1\}^* \rightarrow \{0,1\}^{l_1}$$

[0162] 其中，$\{0,1\}^* \rightarrow \{0,1\}^{l_1}$表示将$\{0,1\}^*$转化为$\{0,1\}^{l_1}$，$\{0,1\}^*$表示任意长度的二进制字符串，$\{0,1\}^{l_1}$表示长度为$l_1$的二进制字符串；

[0163] 上述第二哈希函数H_2的函数式为：

[0164] $$H_2: \{0,1\}^{\omega} \rightarrow \{0,1\}^{l_2}$$

[0165] 其中，$\{0,1\}^{\omega} \rightarrow \{0,1\}^{l_2}$表示将长度为ω的二进制字符串转化为长度为$l_2$的二进制字符串；

[0166] 上述伪随机函数F的函数式为：

[0167] $$F:\ \{0,1\}^{\lambda}\times\{0,1\}^{l_1}\rightarrow[m]^{s}$$

[0168] 其中，$\{0,1\}^{\lambda}\times\{0,1\}^{l_1}\rightarrow[m]^{s}$表示将长度为λ的二进制字符串和长度为$l_1$的二进制字符串转化为由s个小于m的整数组成的字符串；

[0169] 上述承诺函数Comm的函数式为：

[0170] t＝Comm(n,r)

[0171] 其中，n为由客户端提供的协议消息，r为由服务端提供的随机数，该承诺函数的具体构造有多种方式，例如：可以以Hash摘要函数作为承诺函数，即Comm(n,r)＝SHA256(n||r)，其中，n||r表示n和r的串联拼接。

[0172] 参考图3，在客户端和服务端运行预设次数的数据传输协议之前，在服务端和客户端进行数据预处理。

[0173] 上述步骤具体包括：在服务端根据协议安全参数s随机生成选择字符串cs，选择字符串cs是长度为s的随机二进制字符串；在客户端根据第一协议参数m和协议安全参数s生成初始矩阵D，初始矩阵D为m行s列的二进制矩阵，并且初始矩阵D中的所有元素均为1；在客户端根据密钥安全参数λ随机采样生成二进制的密钥字符串k；对于客户端本地数据中的每个元素y，利用第一哈希函数H_1、伪随机函数F以及密钥字符串k，计算得到加密结果v，加密结果v的计算公式为：

[0174] $v=F_k(H_i(y))$

[0175] 其中，F_k表示基于密钥字符串k的伪随机函数F，上述加密结果v由s个小于m的整数组成的字符串；

[0176] 令初始矩阵D中的对应元素$D_i[v[i]]$为0，待利用客户端本地数据的每个元素y对初始矩阵D进行更新，得到更新后的密文数据矩阵D'，其中，v[i]表示加密结果v中的第i个字符，$D_i[v[i]]$表示初始矩阵D的第i列第v[i]行的元素，i为大于或等于0且小于或等于s的整数；在客户端随机生成m行s列的第一加密矩阵A；利用第一加密矩阵A与客户端数据矩阵D'，计算得到第二加密矩阵B，第二加密矩阵B的计算公式为：

[0177] $$B=A\oplus D'$$

[0178] 其中，$\oplus$表示矩阵的异或运算。

[0179] 根据公共参数和公共函数，在客户端和服务端运行s次的数据传输协议；在每次数据传输协议中，在客户端输入协议消息，并计算协议消息的承诺值，将协议消息和对应的承诺值发送至服务端。

[0180] 参考图4，上述步骤具体包括：在服务端根据协议安全参数s随机生成第一承诺向量ra和第二承诺向量rb，并发送至客户端，其中，第一承诺向量ra和第二承诺向量rb均由s个随机数组成；在每次数据传输协议中，在客户端利用第一加密矩阵A和第二加密矩阵B得到待选择数据组$\{A_i,B_i\}$作为协议消息，其中，A_i表示第一加密矩阵A的第i列，B_i表示第二加密矩阵B的第i列；客户端根据待选择数据组$\{A_i,B_i\}$、承诺函数Comm、第一承诺向量ra和第二承诺向量rb，计算得到第一承诺计算结果ca[i]和第二承诺计算结果cb[i]，上述第一承诺计算结果ca[i]的计算公式为：

[0181] $ca[i]=Comm(A_i,ra[i])$

[0182] 其中，ra[i]表示第一承诺向量ra的第i个元素；

[0183] 上述第二承诺计算结果cb[i]的计算公式为：

[0184] $cb[i]=Comm(B_i,rb[i])$

[0185] 其中，rb[i]表示第二承诺向量rb的第i个元素；

[0186] 在客户端将待选择数据组$\{A_i,B_i\}$、第一承诺计算结果ca[i]和第二承诺计算结果cb[i]发送至服务端。

[0187] 在s次的数据传输协议运行结束后，在服务端随机选择部分协议消息，由客户端将选择的部分协议消息打开并发送给服务端，服务端对被打开的协议消息进行安全验证，得到安全验证结果。

[0188] 参考图5，上述步骤具体包括：在服务端根据选择字符串cs对接收到的待选择数据组$\{A_i,B_i\}$进行选择；若选择字符串cs的第i个字符cs[i]为0，则选择第一加密矩阵A的第i列A_i作为选择数据c_i；若选择字符串cs的第i个字符cs[i]为1，则选择第二加密矩阵B的第i列B_i作为选择数据c_i；利用各个选择数据c_i得到第三加密矩阵C。

[0189] 在服务端根据第一协议参数ω随机生成验证向量ro，并将验证向量ro发送至客户端，其中，验证向量ro中的元素均为小于或等于s的正整数，并且验证向量ro中各个元素互不相同；在客户端根据验证向量ro，从第一加密矩阵A中提取对应的第一验证数据$A_{ro[j]}$，从第二加密矩阵B中提取对应的第二验证数据$B_{ro[j]}$，将第一验证数据$A_{ro[j]}$和第二验证数据$B_{ro[j]}$返回至服务端，其中，ro[j]表示验证向量ro的第j个元素，$A_{ro[j]}$表示第一加密矩阵A的第ro[j]列，$B_{ro[j]}$表示第二加密矩阵B的第ro[j]列，j为大于或等于0且小于或等于ω的整数；

[0190] 根据第一验证数据$A_{ro[j]}$、第二验证数据$B_{ro[j]}$、承诺函数Comm、第一承诺向量ra和第二承诺向量rb，在服务端计算得到第一承诺验证结果da和第二承诺验证结果db，上述第一承诺验证结果da的计算公式为：

[0191] $da=Comm(A_{ro[j]},r0[r0[j]])$

[0192] 其中，ra[ro[j]]表示第一承诺向量ra的第ro[j]个元素；

[0193] 上述第二承诺验证结果db的计算公式为：

[0194] $db=Comm(B_{ro[j]},rb[ro[j]])$

[0195] 其中，rb[ro[j]]表示第二承诺向量rb的第ro[j]个元素；

[0196] 在服务端根据第一承诺计算结果ca[i]、第二承诺计算结果cb[i]、第一承诺验证结果da、第二承诺验证结果db和第三加密矩阵C，对第一验证数据$A_{ro[j]}$和第二验证数据$B_{ro[j]}$进行安全验证；判断是否同时满足第一条件、第二条件、第三条件；第一条件为：第一验证数据$A_{ro[j]}$与第二验证数据$B_{ro[j]}$不相同；第二条件为：验证向量ro的第j个元素对应的第一承诺计算结果ca[ro[j]]等于第一承诺验证结果da，并且验证向量ro的第j个元素对应的第二承诺计算结果cb[ro[j]]等于第二承诺验证结果db；第三条件为：当选择字符串cs的第ro[j]个字符cs[ro[j]]为0时，第三加密矩阵C的第ro[j]列$C_{ro[j]}$等于第一验证数据$A_{ro[j]}$，并且当选择字符串cs的第ro[j]个字符cs[ro[j]]为1时，第三加密矩阵C的第ro[j]列$C_{ro[j]}$等于第二验证数据$B_{ro[j]}$；若不满足第一条件或第二条件或第三条件，则安全验证结果为不通过，终止客户端和服务端之间的数据交互过程；若同时满足第一条件、第二条件和第三条

件，则安全验证结果为通过。

[0197] 在客户端和服务端利用未被打开的协议消息进行隐私数据求交，客户端得到双方数据的交集。

[0198] 参考图6，上述步骤具体包括：在客户端将第一验证数据$A_{ro[j]}$从第一加密矩阵A中删除，得到m行ω列的第四加密矩阵E，并将密钥字符串k发送至服务端；在服务端将第三加密矩阵C的第ro[j]列$C_{ro[j]}$从第三加密矩阵C中删除，得到m行ω列第五加密矩阵G；在服务端，对于服务端本地数据中的每个元素x，利用第一哈希函数H_1、伪随机函数F以及字符串密钥k，计算得到第一加密向量p，第一加密向量p的计算公式为：

[0199] $p=F_k(H_1(x))$

[0200] 在服务端将第一加密向量p中的p[ro[j]]删除，得到第二加密向量p'，其中，p[ro[j]]表示第一加密向量p的第ro[j]个字符；在服务端利用第二加密向量p'、第五加密矩阵G和第二哈希函数H_2，计算得到第一加密密文φ_1，第一加密密文φ_1的计算公式为：

[0201] $$\varphi_1 = H_2(G_1[p'[1]] \| \ldots \| G_\omega[p'[\omega]])$$

[0202] 其中，p'[ω]表示第二加密向量p'的第ω个字符，G_ω[p'[ω]]表示第五加密矩阵G的第ω列第p'[ω]行的元素；服务端将所有第一加密密文φ_1发送至客户端；

[0203] 在客户端，对于客户端本地数据中的每个元素y，利用第一哈希函数H_1、伪随机函数F以及字符串密钥k，计算得到第三加密向量q，第三加密向量q的计算公式为：

[0204] $q=F_k(H_1(y))$

[0205] 在客户端将第三加密向量q中的q[ro[j]]删除，得到第四加密向量q'，其中，q[ro[j]]表示第三加密向量q的第Aro[j]个字符；在客户端利用第四加密向量q'、第四加密矩阵E和第二哈希函数H_2，计算第二加密密文φ_2，第二加密密文φ_2的计算公式为：

[0206] $$\varphi_2 = H_2(E_1[q'[1]] \| \ldots \| E_\omega[q'[\omega]])$$

[0207] 其中，q'[ω]表示第四加密向量q'的第ro[j]个字符，E_ω[q'[ω]]表示第四加密矩阵E的第ω列第q'[ω]行的元素；

[0208] 在客户端将第二加密密文φ_2和接收到的第一加密密文φ_1进行逐一对比，客户端得到服务端本地数据与客户端本地数据的交集。

[0209] 本发明实施例公开了一种安全的数据交互方法，首先在客户端和服务端同步设定公共参数并约定公共函数，然后在客户端和服务端运行预设次数的数据传输协议；在每次数据传输协议中，在客户端输入协议消息，并计算协议消息的承诺值，将协议消息和承诺值发送至服务端；协议运行结束后，在服务端随机选择部分协议消息，客户端将选择的部分协议消息打开并发送给服务端，服务端对被打开的协议消息进行安全验证，若安全验证通过，则在客户端和服务端进行隐私数据求交，客户端得到双方数据的交集。本发明实施例通过在数据传输协议阶段增加安全验证来保证服务端数据在恶意攻击下的安全性，从而避免客户端通过恶意攻击获取服务端数据。

[0210] 另外，本发明实施例还提供了一种安全的数据交互设备，所述设备包括：处理器和存储器；所述存储器用于存储一个或多个程序指令；所述处理器，用于运行一个或多个程序指令，用以执行如上任一项所述的一种安全的数据交互方法的步骤。

[0211] 另外,本发明实施例还提供了一种计算机可读存储介质,所述计算机可读存储介质上存储有计算机程序,所述计算机程序被处理器执行时实现如上任一项所述一种安全的数据交互方法的步骤。

[0212] 在本发明实施例中,处理器可以是一种集成电路芯片,具有信号的处理能力。处理器可以是通用处理器、数字信号处理器(Digital Signal Processor,简称DSP)、专用集成电路(Application Specific Integrated Circuit,简称ASIC)、现场可编程门阵列(Field Programmable Gate Array,简称FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。

[0213] 可以实现或者执行本发明实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本发明实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成,或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器,闪存、只读存储器,可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。处理器读取存储介质中的信息,结合其硬件完成上述方法的步骤。

[0214] 存储介质可以是存储器,例如可以是易失性存储器或非易失性存储器,或可包括易失性和非易失性存储器两者。

[0215] 其中,非易失性存储器可以是只读存储器(Read-Only Memory,简称ROM)、可编程只读存储器(Programmable ROM,简称PROM)、可擦除可编程只读存储器(Erasable PROM,简称EPROM)、电可擦除可编程只读存储器(Electrically EPROM,简称EEPROM)或闪存。

[0216] 易失性存储器可以是随机存取存储器(Random Access Memory,简称RAM),其用作外部高速缓存。通过示例性但不是限制性说明,许多形式的RAM可用,例如静态随机存取存储器(Static RAM,简称SRAM)、动态随机存取存储器(Dynamic RAM,简称DRAM)、同步动态随机存取存储器(Synchronous DRAM,简称SDRAM)、双倍数据速率同步动态随机存取存储器(Double Data Rate SDRAM,简称DDRSDRAM)、增强型同步动态随机存取存储器(Enhanced SDRAM,简称ESDRAM)、同步连接动态随机存取存储器(Synchlink DRAM,简称SLDRAM)和直接内存总线随机存取存储器(Direct Rambus RAM,简称DRRAM)。

[0217] 本发明实施例描述的存储介质旨在包括但不限于这些和任意其它适合类型的存储器。

[0218] 本领域技术人员应该可以意识到,在上述一个或多个示例中,本发明所描述的功能可以用硬件与软件组合来实现。当应用软件时,可以将相应功能存储在计算机可读介质中或者作为计算机可读介质上的一个或多个指令或代码进行传输。计算机可读介质包括计算机存储介质和通信介质,其中通信介质包括便于从一个地方向另一个地方传送计算机程序的任何介质。存储介质可以是通用或专用计算机能够存取的任何可用介质。

[0219] 虽然,上文中已经用一般性说明及具体实施例对本发明作了详尽的描述,但在本发明基础上,可以对之作一些修改或改进,这对本领域技术人员而言是显而易见的。因此,在不偏离本发明精神的基础上所做的这些修改或改进,均属于本发明要求保护的范围。

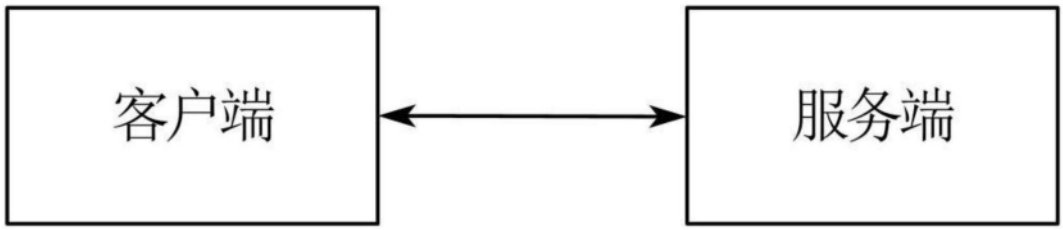

客户端
服务端

图1

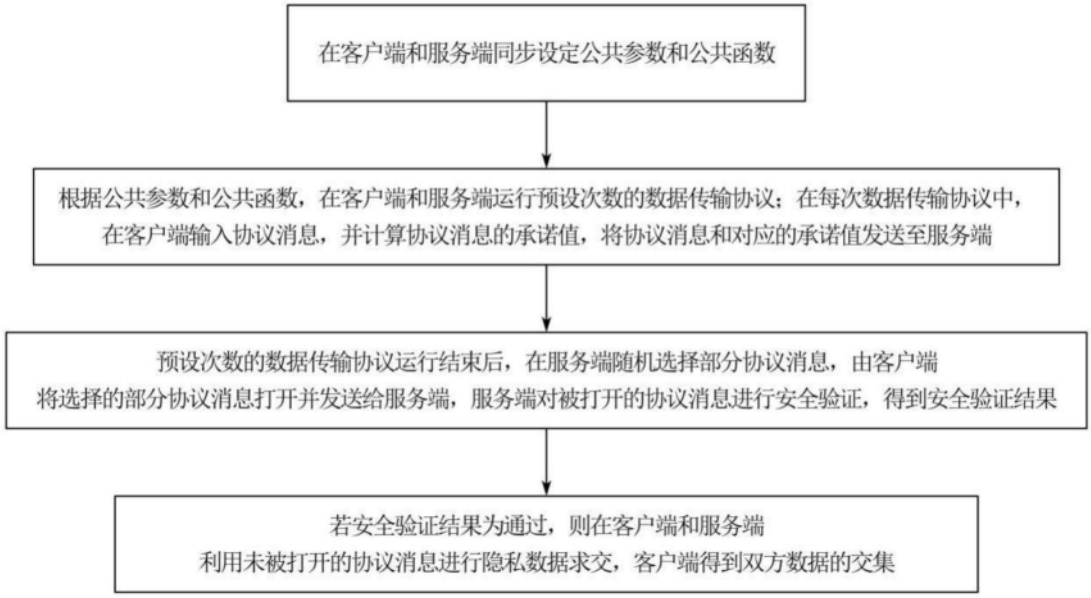

在客户端和服务端同步设定公共参数和公共函数
根据公共参数和公共函数，在客户端和服务端运行预设次数的数据传输协议；在每次数据传输协议中，
在客户端输入协议消息，并计算协议消息的承诺值，将协议消息和对应的承诺值发送至服务端
预设次数的数据传输协议运行结束后，在服务端随机选择部分协议消息，由客户端
将选择的部分协议消息打开并发送给服务端，服务端对被打开的协议消息进行安全验证，得到安全验证结果
若安全验证结果为通过，则在客户端和服务端
利用未被打开的协议消息进行隐私数据求交，客户端得到双方数据的交集

图2

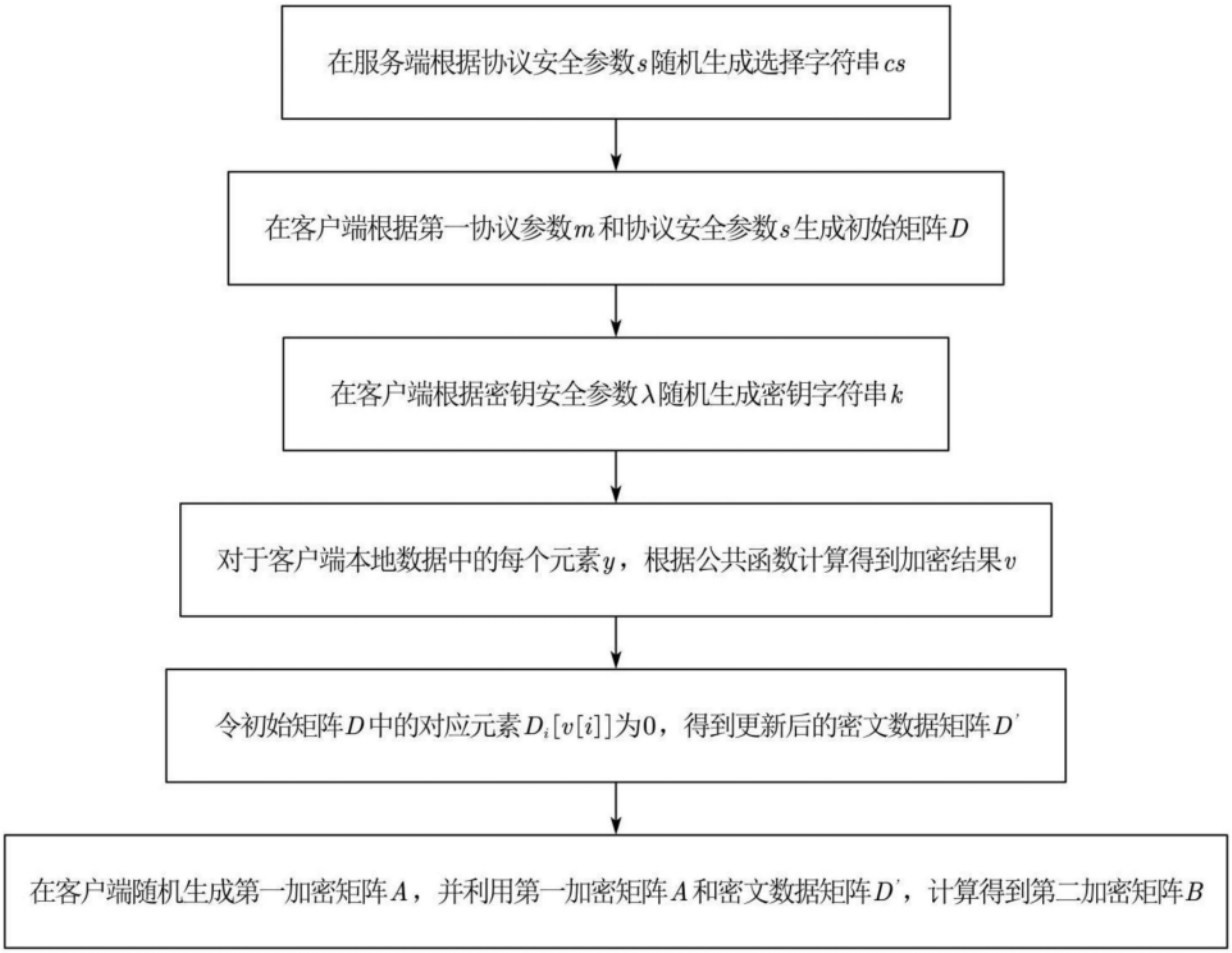

在服务端根据协议安全参数s随机生成选择字符串cs
在客户端根据第一协议参数m和协议安全参数s生成初始矩阵D
在客户端根据密钥安全参数λ随机生成密钥字符串k
对于客户端本地数据中的每个元素y，根据公共函数计算得到加密结果v
令初始矩阵D中的对应元素$D_i[v[i]]$为0，得到更新后的密文数据矩阵D'
在客户端随机生成第一加密矩阵A，并利用第一加密矩阵A和密文数据矩阵D'，计算得到第二加密矩阵B

图3

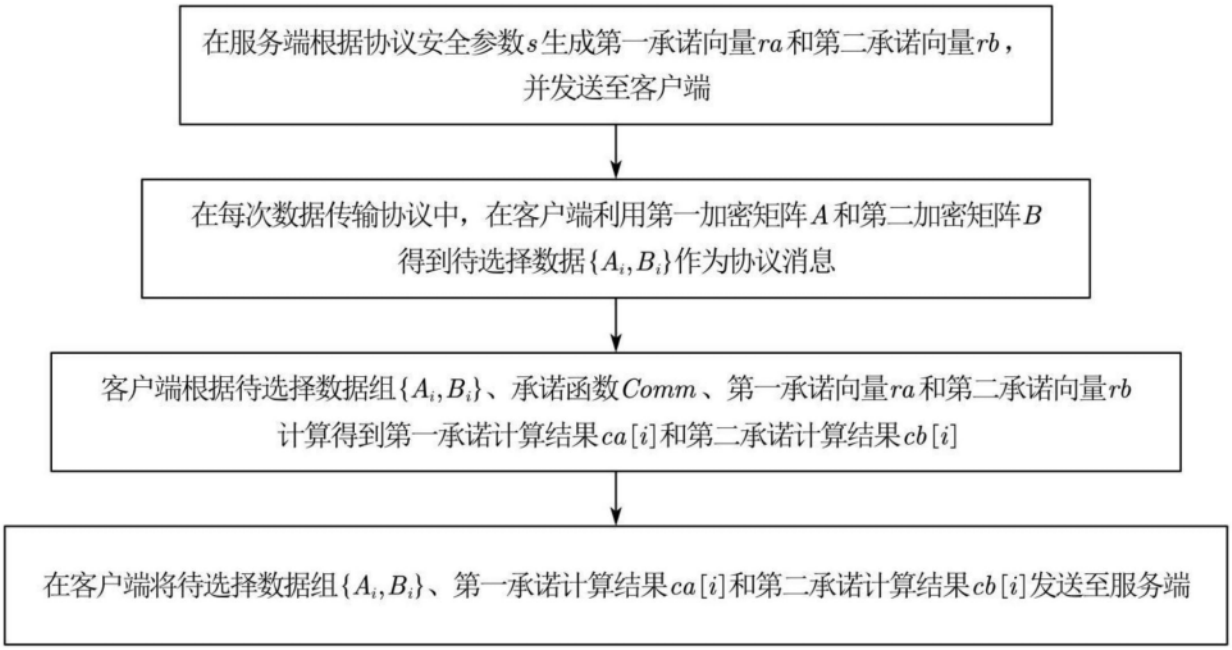

在服务端根据协议安全参数s生成第一承诺向量ra和第二承诺向量rb，并发送至客户端
在每次数据传输协议中，在客户端利用第一加密矩阵A和第二加密矩阵B得到待选择数据$\{A_i,B_i\}$作为协议消息
客户端根据待选择数据组$\{A_i,B_i\}$、承诺函数$Comm$、第一承诺向量ra和第二承诺向量rb计算得到第一承诺计算结果$ca[i]$和第二承诺计算结果$cb[i]$
在客户端将待选择数据组$\{A_i,B_i\}$、第一承诺计算结果$ca[i]$和第二承诺计算结果$cb[i]$发送至服务端

图4

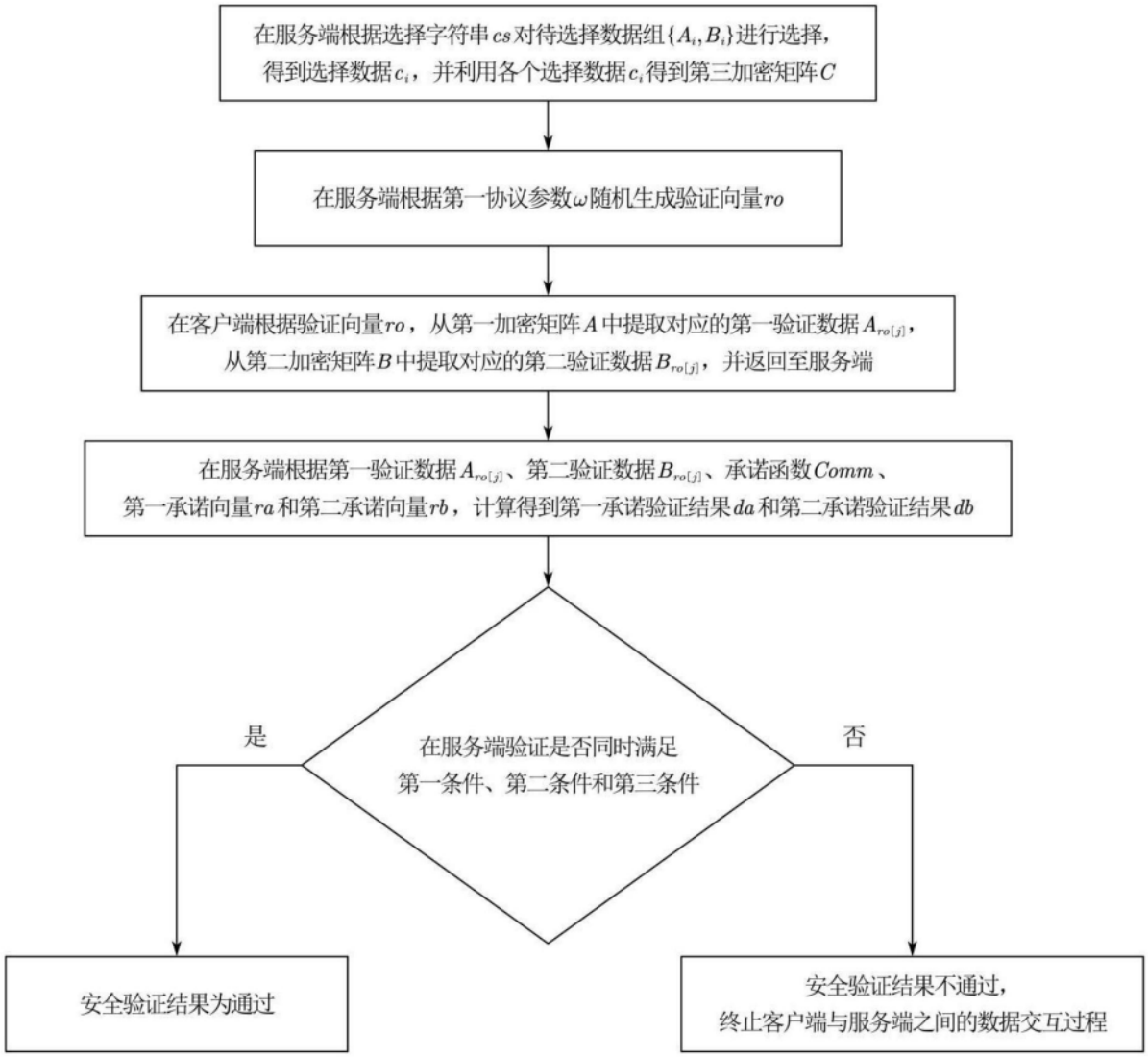

在服务端根据选择字符串cs对待选择数据组$\{A_i,B_i\}$进行选择，得到选择数据c_i，并利用各个选择数据c_i得到第三加密矩阵C
在服务端根据第一协议参数ω随机生成验证向量ro
在客户端根据验证向量ro，从第一加密矩阵A中提取对应的第一验证数据$A_{ro[j]}$，从第二加密矩阵B中提取对应的第二验证数据$B_{ro[j]}$，并返回至服务端
在服务端根据第一验证数据$A_{ro[j]}$、第二验证数据$B_{ro[j]}$、承诺函数$Comm$、第一承诺向量ra和第二承诺向量rb，计算得到第一承诺验证结果da和第二承诺验证结果db
在服务端验证是否同时满足第一条件、第二条件和第三条件
是
否
安全验证结果为通过
安全验证结果不通过，终止客户端与服务端之间的数据交互过程

图5

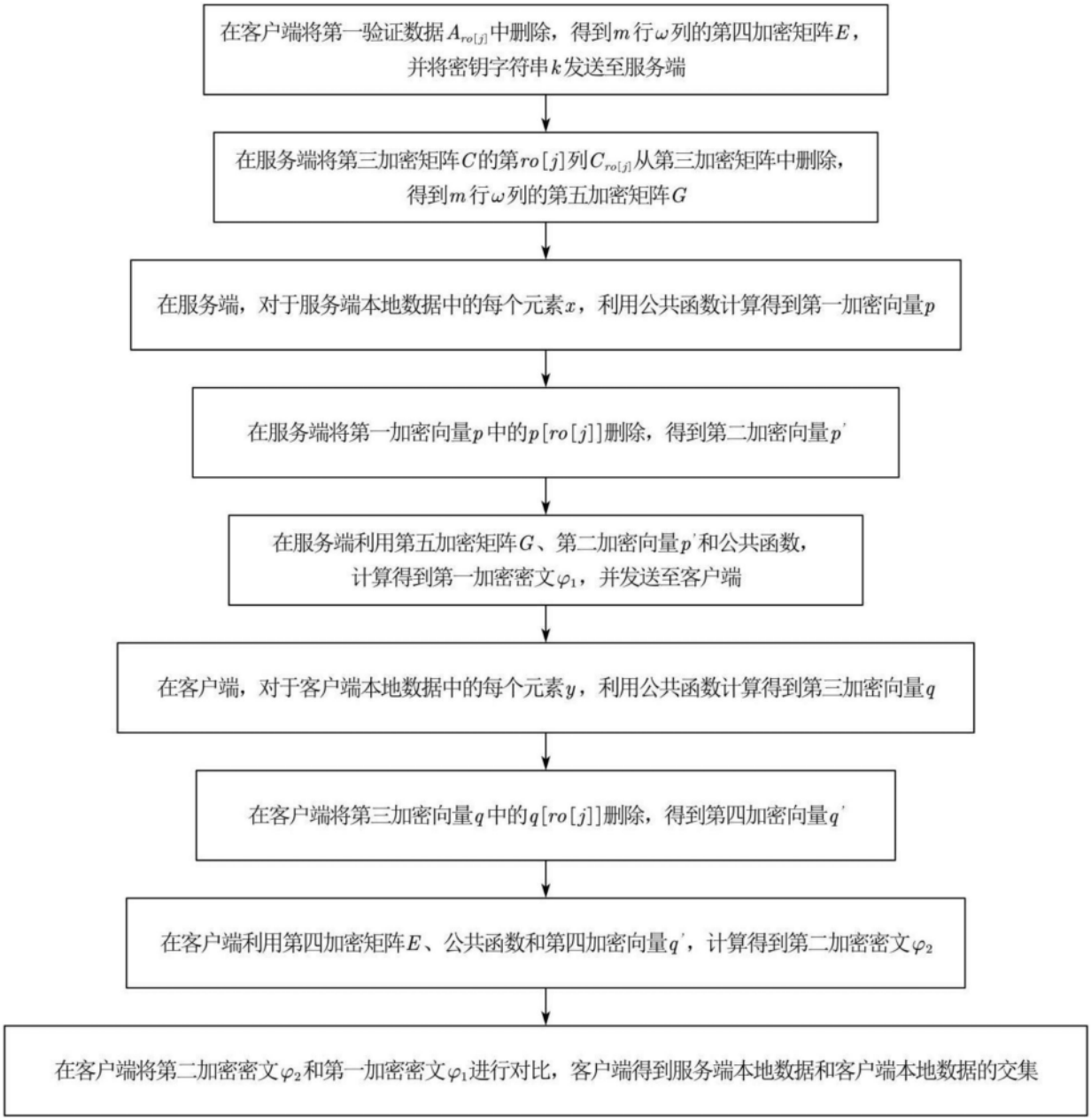

在客户端将第一验证数据$A_{ro[j]}$中删除，得到m行ω列的第四加密矩阵E，并将密钥字符串k发送至服务端
在服务端将第三加密矩阵C的第$ro[j]$列$C_{ro[j]}$从第三加密矩阵中删除，得到m行ω列的第五加密矩阵G
在服务端，对于服务端本地数据中的每个元素x，利用公共函数计算得到第一加密向量p
在服务端将第一加密向量p中的$p[ro[j]]$删除，得到第二加密向量p'
在服务端利用第五加密矩阵G、第二加密向量p'和公共函数，计算得到第一加密密文φ_1，并发送至客户端
在客户端，对于客户端本地数据中的每个元素y，利用公共函数计算得到第三加密向量q
在客户端将第三加密向量q中的$q[ro[j]]$删除，得到第四加密向量q'
在客户端利用第四加密矩阵E、公共函数和第四加密向量q'，计算得到第二加密密文φ_2
在客户端将第二加密密文φ_2和第一加密密文φ_1进行对比，客户端得到服务端本地数据和客户端本地数据的交集

图6