(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 116055049 B
(45)授权公告日 2023.07.04

(21)申请号 202310339886.1

(22)申请日 2023.04.03

(65)同一申请的已公布的文献号
申请公布号 CN 116055049 A

(43)申请公布日 2023.05.02

(73)专利权人 富算科技(上海)有限公司
地址 200135 上海市浦东新区自由贸易试验区浦东大道1200号2层A区

(72)发明人 尤志强 卞阳 赵东

(74)专利代理机构 上海弼兴律师事务所 31283
专利代理师 李静 罗朗

(51)Int.Cl.
H04L 9/08(2006.01)

(56)对比文件
US 2022286294 A1,2022.09.08
WO 2019015541 A1,2019.01.24
CN 115765985 A,2023.03.07
王国华;刘志强;马红光;马猛.基于硬件加速的快速傅里叶变换.航空计算技术.2008,(05),全文.

审查员 王小龙

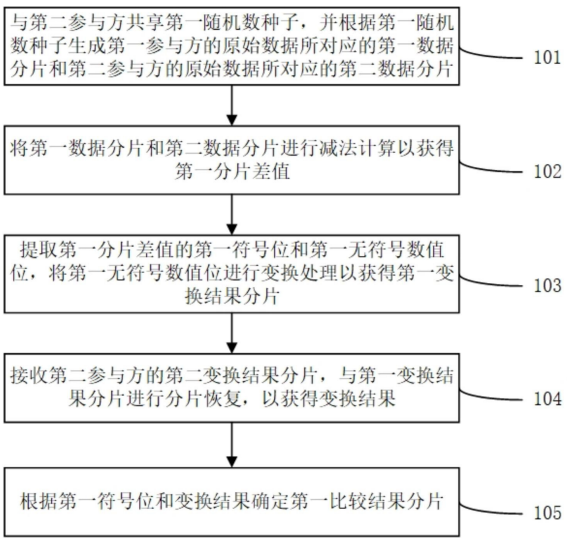
权利要求书4页 说明书15页 附图7页

(54)发明名称

多方安全计算方法、装置、系统、电子设备和存储介质

(57)摘要

本公开为一种多方安全计算方法、装置、系统、电子设备和存储介质，所述多方安全计算方法包括：第一参与方根据第一变换结果分片和第二变换结果分片确定变换结果；所述第一参与方根据第一符号位和所述变换结果确定第一比较结果分片；所述第二参与方根据所述第二符号位确定第二比较结果分片；所述第一比较结果分片和所述第二比较结果分片用于确定比较结果。本公开通过参与方之间共享随机数种子后，在不发生通信的条件下互相获取对方原始数据的数据分片，各自在本地进行计算，仅在执行多方安全计算乘法计算以及发送变换结果分片的时候发生通信。实现了整个计算过程中通信次数较少，运算量较少，且没有敏感信息在节点之间交互的效果。



CN 116055049 B

1.一种多方安全计算方法,其特征在于,所述多方安全计算方法应用于第一参与方,所述多方安全计算方法包括:

与第二参与方共享第一随机数种子,并根据所述第一随机数种子生成所述第一参与方的原始数据所对应的第一数据分片和所述第二参与方的原始数据所对应的第二数据分片;

将所述第一数据分片和所述第二数据分片进行减法计算以获得第一分片差值;

提取所述第一分片差值的第一符号位和第一无符号数值位,将所述第一无符号数值位进行变换处理以获得第一变换结果分片;

所述变换处理基于单调函数进行变换;

接收所述第二参与方的第二变换结果分片,与所述第一变换结果分片进行分片恢复,以获得变换结果;其中,所述第二变换结果分片由所述第二参与方根据所述第一随机数种子和所述第二参与方的原始数据生成;

根据所述第一符号位和所述变换结果确定第一比较结果分片,所述第一比较结果分片用于结合来自所述第二参与方的第二比较结果分片,以确定所述第一参与方的原始数据与所述第二参与方的原始数据的比较结果。

2.根据权利要求1所述的多方安全计算方法,其特征在于,所述将所述第一无符号数值位进行变换处理以获得第一变换结果分片,包括:

根据第二随机数种子生成所述第一参与方的第一无符号数值位所对应的第三数据分片和所述第二参与方的第二无符号数值位所对应的第四数据分片;

将所述第三数据分片和所述第四数据分片进行减法计算以获得第二分片差值;

将所述第二分片差值进行函数变换,以获得第一变换结果分片。

3.根据权利要求2所述的多方安全计算方法,其特征在于,所述将所述第二分片差值进行函数变换,包括:

与所述第二参与方协同生成变换函数参数,以生成第一变换函数参数分片;

将所述第一变换函数参数分片和第二分片差值代入变换函数进行求解。

4.根据权利要求3所述的多方安全计算方法,其特征在于,所述变换函数为单调递增函数或单调递减函数。

5.一种多方安全计算方法,其特征在于,所述多方安全计算方法应用于第二参与方,所述多方安全计算方法包括:

与第一参与方共享第一随机数种子,并根据所述第一随机数种子生成所述第一参与方的原始数据所对应的第五数据分片和所述第二参与方的原始数据所对应的第六数据分片;

将所述第五数据分片和所述第六数据分片进行减法计算以获得第三分片差值;

提取所述第三分片差值的第二符号位和第二无符号数值位,将所述第二无符号数值位进行变换处理以获得第二变换结果分片;

所述变换处理基于单调函数进行变换;

将所述第二变换结果分片发送给所述第一参与方,以由所述第一参与方根据所述第二变换结果分片和第一变换结果分片确定变换结果;所述第一变换结果分片由所述第一参与方根据所述第一随机数种子和所述第一参与方的原始数据生成;

根据所述第二符号位确定第二比较结果分片,发送所述第二比较结果分片至所述第一参与方,所述第二比较结果分片用于确定所述第一参与方的原始数据与所述第二参与方的

原始数据的比较结果。

6.一种多方安全计算方法,其特征在于,所述多方安全计算方法包括:

第一参与方与第二参与方共享第一随机数种子;

所述第一参与方根据所述第一随机数种子生成所述第一参与方的原始数据所对应的第一数据分片和所述第二参与方的原始数据所对应的第二数据分片;

所述第一参与方将所述第一数据分片和所述第二数据分片进行减法计算以获得第一分片差值;

所述第一参与方提取所述第一分片差值的第一符号位和第一无符号数值位,将所述第一无符号数值位进行变换处理以获得第一变换结果分片;

所述第二参与方根据所述第一随机数种子生成所述第一参与方的原始数据所对应的第五数据分片和所述第二参与方的原始数据所对应的第六数据分片;

所述第二参与方将所述第五数据分片和所述第六数据分片进行减法计算以获得第三分片差值;

所述第二参与方提取所述第三分片差值的第二符号位和第二无符号数值位,将所述第二无符号数值位进行变换处理以获得第二变换结果分片;

所述第二参与方将所述第二变换结果分片发送给所述第一参与方;

所述第一参与方对所述第二变换结果分片与所述第一变换结果分片进行分片恢复,以获得变换结果;

所述第一参与方根据所述第一符号位和所述变换结果确定第一比较结果分片;

所述第二参与方根据所述第二符号位确定第二比较结果分片;

所述第一比较结果分片和所述第二比较结果分片用于确定所述第一参与方的原始数据与所述第二参与方的原始数据的比较结果;

所述变换处理基于单调函数进行变换。

7.一种多方安全计算装置,其特征在于,所述多方安全计算装置应用于第一参与方,所述多方安全计算装置包括:

第一分片模块,用于与第二参与方共享第一随机数种子,并根据所述第一随机数种子生成所述第一参与方的原始数据所对应的第一数据分片和所述第二参与方的原始数据所对应的第二数据分片;

第一差值模块,用于将所述第一数据分片和所述第二数据分片进行减法计算以获得第一分片差值;

第一变换模块,用于提取所述第一分片差值的第一符号位和第一无符号数值位,将所述第一无符号数值位进行变换处理以获得第一变换结果分片;

所述变换处理基于单调函数进行变换;

分片接收模块,用于接收所述第二参与方的第二变换结果分片,与所述第一变换结果分片进行分片恢复,以获得变换结果;其中,所述第二变换结果分片由所述第二参与方根据所述第一随机数种子和所述第二参与方的原始数据生成;

第一结果确定模块,用于根据所述第一符号位和所述变换结果确定第一比较结果分片,所述第一比较结果分片用于结合来自所述第二参与方的第二比较结果分片,以确定所述第一参与方的原始数据与所述第二参与方的原始数据的比较结果。

8.一种多方安全计算装置,其特征在于,所述多方安全计算装置应用于第二参与方,所述多方安全计算装置包括:

第二分片模块,用于与第一参与方共享第一随机数种子,并根据所述第一随机数种子生成所述第一参与方的原始数据所对应的第五数据分片和所述第二参与方的原始数据所对应的第六数据分片;

第二差值模块,用于将所述第五数据分片和所述第六数据分片进行减法计算以获得第三分片差值;

第二变换模块,用于提取所述第三分片差值的第二符号位和第二无符号数值位,将所述第二无符号数值位进行变换处理以获得第二变换结果分片;

所述变换处理基于单调函数进行变换;

分片发送模块,用于将所述第二变换结果分片发送给所述第一参与方,以由所述第一参与方根据所述第二变换结果分片和第一变换结果分片确定变换结果;所述第一变换结果分片由所述第一参与方根据所述第一随机数种子和所述第一参与方的原始数据生成;

第二结果确定模块,用于根据所述第二符号位确定第二比较结果分片,发送所述第二比较结果分片至所述第一参与方,所述第二比较结果分片用于确定所述第一参与方的原始数据与所述第二参与方的原始数据的比较结果。

9.一种多方安全计算系统,其特征在于,所述多方安全计算系统包括:第一参与方与第二参与方;

所述第一参与方,用于与第二参与方共享第一随机数种子;

所述第一参与方,还用于根据所述第一随机数种子生成所述第一参与方的原始数据所对应的第一数据分片和所述第二参与方的原始数据所对应的第二数据分片;

所述第一参与方,还用于将所述第一数据分片和所述第二数据分片进行减法计算以获得第一分片差值;

所述第一参与方,还用于提取所述第一分片差值的第一符号位和第一无符号数值位,将所述第一无符号数值位进行变换处理以获得第一变换结果分片;

所述第二参与方,用于根据所述第一随机数种子生成所述第一参与方的原始数据所对应的第五数据分片和所述第二参与方的原始数据所对应的第六数据分片

所述第二参与方,还用于将所述第五数据分片和所述第六数据分片进行减法计算以获得第三分片差值;

所述第二参与方,还用于提取所述第三分片差值的第二符号位和第二无符号数值位,将所述第二无符号数值位进行变换处理以获得第二变换结果分片;

所述第二参与方,还用于将所述第二变换结果分片发送给所述第一参与方;

所述第一参与方,还用于对所述第二变换结果分片与所述第一变换结果分片进行分片恢复,以获得变换结果;

所述第一参与方,还用于根据所述第一符号位和所述变换结果确定第一比较结果分片;

所述第二参与方,还用于根据所述第二符号位确定第二比较结果分片;

所述第一比较结果分片和所述第二比较结果分片用于确定所述第一参与方的原始数据与所述第二参与方的原始数据的比较结果;

所述变换处理基于单调函数进行变换。

10.一种电子设备,包括存储器、处理器及存储在存储器上并用于在处理器上运行的计算机程序,其特征在于,所述处理器执行所述计算机程序时实现权利要求1至6中任一项所述的多方安全计算方法。

11.一种计算机可读存储介质,其上存储有计算机程序,其特征在于,所述计算机程序被处理器执行时实现权利要求1至6中任一项所述的多方安全计算方法。

多方安全计算方法、装置、系统、电子设备和存储介质

技术领域

[0001] 本公开涉及数据安全技术领域，尤其涉及一种多方安全计算方法、装置、系统、电子设备和存储介质。

背景技术

[0002] 多方安全计算主要是针对无可信第三方的情况下，如何安全地实现信息在多计算节点之间交互的过程中“可用，不可见”。

[0003] 相关技术中，安全多方计算在进行比较算子运算时，通常采用基于电路的技术、不经意传输技术或同态加密技术。

[0004] 然而，基于不经意传输的大小比较和相等测试方法，各个参与方之间的通信交互次数较多，通信开销大。基于同态加密技术的方法则计算复杂度较高，运算量巨大。上述方法除了运算及时间成本巨大，在节点交互过程中也会涉及敏感信息对信息安全构成威胁。

发明内容

[0005] 本公开要解决的问题是为了克服现有技术中运算及时间成本巨大，计算过程中涉及敏感信息的缺陷，提供一种多方安全计算方法、装置、系统、电子设备和存储介质。

[0006] 本公开是通过下述技术方案来解决上述技术问题：

[0007] 本公开提供一种多方安全计算方法，所述多方安全计算方法应用于第一参与方，所述多方安全计算方法包括：

[0008] 与第二参与方共享第一随机数种子，并根据所述第一随机数种子生成所述第一参与方的原始数据所对应的第一数据分片和所述第二参与方的原始数据所对应的第二数据分片；

[0009] 将所述第一数据分片和所述第二数据分片进行减法计算以获得第一分片差值；

[0010] 提取所述第一分片差值的第一符号位和第一无符号数值位，将所述第一无符号数值位进行变换处理以获得第一变换结果分片；

[0011] 接收所述第二参与方的第二变换结果分片，与所述第一变换结果分片进行分片恢复，以获得变换结果；其中，所述第二变换结果分片由所述第二参与方根据所述第一随机数种子和所述第二参与方的原始数据生成；

[0012] 根据所述第一符号位和所述变换结果确定第一比较结果分片，所述第一比较结果分片用于确定所述第一参与方的原始数据与所述第二参与方的原始数据的比较结果。

[0013] 较佳地，所述将所述第一无符号数值位进行变换处理以获得第一变换结果分片，包括：

[0014] 根据第二随机数种子生成所述第一参与方的第一无符号数值位所对应的第三数据分片和所述第二参与方的第二无符号数值位所对应的第四数据分片；

[0015] 将所述第三数据分片和所述第四数据分片进行减法计算以获得第二分片差值；

[0016] 将所述第二分片差值进行函数变换，以获得第一变换结果分片。

[0017] 较佳地，所述将所述第二分片差值进行函数变换，包括：

[0018] 与所述第二参与方协同生成变换函数参数，以生成第一变换函数参数分片；

[0019] 将所述第一变换函数参数分片和第二分片差值代入变换函数进行求解。

[0020] 较佳地，所述变换函数为单调递增函数或单调递减函数。

[0021] 本公开还提供一种多方安全计算方法，所述多方安全计算方法应用于第二参与方，所述多方安全计算方法包括：

[0022] 与第一参与方共享第一随机数种子，并根据所述第一随机数种子生成所述第一参与方的原始数据所对应的第五数据分片和所述第二参与方的原始数据所对应的第六数据分片；

[0023] 将所述第五数据分片和所述第六数据分片进行减法计算以获得第三分片差值；

[0024] 提取所述第三分片差值的第二符号位和第二无符号数值位，将所述第二无符号数值位进行变换处理以获得第二变换结果分片；

[0025] 将所述第二变换结果分片发送给所述第一参与方，以由所述第一参与方根据所述第二变换结果分片和第一变换结果分片确定变换结果；所述第一变换结果分片由所述第一参与方根据所述第一随机数种子和所述第一参与方的原始数据生成；

[0026] 根据所述第二符号位确定第二比较结果分片，所述第二比较结果分片用于确定所述第一参与方的原始数据与所述第二参与方的原始数据的比较结果。

[0027] 较佳地，所述将所述第二无符号数值位进行变换处理以获得第二变换结果分片，包括：

[0028] 根据第二随机数种子生成所述第一参与方的第一无符号数值位所对应的第七数据分片和所述第二参与方的第二无符号数值位所对应的第八数据分片；

[0029] 将所述第七数据分片和所述第八数据分片进行减法计算以获得第四分片差值；

[0030] 将所述第四分片差值进行函数变换，以获得第二变换结果分片。

[0031] 较佳地，所述将所述第四分片差值进行函数变换，包括：

[0032] 与所述第二参与方协同生成变换函数参数，以生成第二变换函数参数分片；

[0033] 将所述第二变换函数参数分片和第四分片差值代入变换函数进行求解。

[0034] 较佳地，所述变换函数为单调递增函数或单调递减函数。

[0035] 本公开还提供一种多方安全计算方法，所述多方安全计算方法包括：

[0036] 根据所述第二符号位确定第二比较结果分片第一参与方与第二参与方共享第一随机数种子；

[0037] 所述第一参与方根据所述第一随机数种子生成所述第一参与方的原始数据所对应的第一数据分片和所述第二参与方的原始数据所对应的第二数据分片；

[0038] 所述第一参与方将所述第一数据分片和所述第二数据分片进行减法计算以获得第一分片差值；

[0039] 所述第一参与方提取所述第一分片差值的第一符号位和第一无符号数值位，将所述第一无符号数值位进行变换处理以获得第一变换结果分片；

[0040] 所述第二参与方根据所述第一随机数种子生成所述第一参与方的原始数据所对应的第五数据分片和所述第二参与方的原始数据所对应的第六数据分片；

[0041] 所述第二参与方将所述第五数据分片和所述第六数据分片进行减法计算以获得

第三分片差值；

[0042] 所述第二参与方提取所述第三分片差值的第二符号位和第二无符号数值位，将所述第二无符号数值位进行变换处理以获得第二变换结果分片；

[0043] 所述第二参与方将所述第二变换结果分片发送给所述第一参与方；

[0044] 所述第一参与方对所述第二变换结果分片与所述第一变换结果分片进行分片恢复，以获得变换结果；

[0045] 所述第一参与方根据所述第一符号位和所述变换结果确定第一比较结果分片；

[0046] 所述第二参与方根据所述第二符号位确定第二比较结果分片；

[0047] 所述第一比较结果分片和所述第二比较结果分片用于确定所述第一参与方的原始数据与所述第二参与方的原始数据的比较结果。

[0048] 本公开还提供一种多方安全计算装置，所述多方安全计算装置应用于第一参与方，所述多方安全计算装置包括：

[0049] 第一分片模块，用于与第二参与方共享第一随机数种子，并根据所述第一随机数种子生成所述第一参与方的原始数据所对应的第一数据分片和所述第二参与方的原始数据所对应的第二数据分片；

[0050] 第一差值模块，用于将所述第一数据分片和所述第二数据分片进行减法计算以获得第一分片差值；

[0051] 第一变换模块，用于提取所述第一分片差值的第一符号位和第一无符号数值位，将所述第一无符号数值位进行变换处理以获得第一变换结果分片；

[0052] 分片接收模块，用于接收所述第二参与方的第二变换结果分片，与所述第一变换结果分片进行分片恢复，以获得变换结果；其中，所述第二变换结果分片由所述第二参与方根据所述第一随机数种子和所述第二参与方的原始数据生成；

[0053] 第一结果确定模块，用于根据所述第一符号位和所述变换结果确定第一比较结果分片，所述第一比较结果分片用于确定所述第一参与方的原始数据与所述第二参与方的原始数据的比较结果。

[0054] 较佳地，所述第一变换模块，包括：

[0055] 第一分片单元，用于根据第二随机数种子生成所述第一参与方的第一无符号数值位所对应的第三数据分片和所述第二参与方的第二无符号数值位所对应的第四数据分片；

[0056] 第一差值单元，用于将所述第三数据分片和所述第四数据分片进行减法计算以获得第二分片差值；

[0057] 第一变换单元，用于将所述第二分片差值进行函数变换，以获得第一变换结果分片。

[0058] 较佳地，所述第一变换单元，还用于与所述第二参与方协同生成变换函数参数，以生成第一变换函数参数分片；将所述第一变换函数参数分片和第二分片差值代入变换函数进行求解。

[0059] 较佳地，所述变换函数为单调递增函数或单调递减函数。

[0060] 本公开还提供一种多方安全计算装置，所述多方安全计算装置应用于第二参与方，所述多方安全计算装置包括：

[0061] 第二分片模块，用于与第一参与方共享第一随机数种子，并根据所述第一随机数

种子生成所述第一参与方的原始数据所对应的第五数据分片和所述第二参与方的原始数据所对应的第六数据分片；

[0062] 第二差值模块，用于将所述第五数据分片和所述第六数据分片进行减法计算以获得第三分片差值；

[0063] 第二变换模块，用于提取所述第三分片差值的第二符号位和第二无符号数值位，将所述第二无符号数值位进行变换处理以获得第二变换结果分片；

[0064] 分片发送模块，用于将所述第二变换结果分片发送给所述第一参与方，以由所述第一参与方根据所述第二变换结果分片和第一变换结果分片确定变换结果；所述第一变换结果分片由所述第一参与方根据所述第一随机数种子和所述第一参与方的原始数据生成；

[0065] 第二结果确定模块，用于根据所述第二符号位确定第二比较结果分片，所述第二比较结果分片用于确定所述第一参与方的原始数据与所述第二参与方的原始数据的比较结果。

[0066] 较佳地，所述第二变换模块，包括：

[0067] 第二分片单元，用于根据第二随机数种子生成所述第一参与方的第一无符号数值位所对应的第七数据分片和所述第二参与方的第二无符号数值位所对应的第八数据分片；

[0068] 第二差值单元，用于将所述第七数据分片和所述第八数据分片进行减法计算以获得第四分片差值；

[0069] 第二变换单元，用于将所述第四分片差值进行函数变换，以获得第二变换结果分片。

[0070] 较佳地，所述第二变换单元，还用于与所述第二参与方协同生成变换函数参数，以生成第二变换函数参数分片；将所述第二变换函数参数分片和第四分片差值代入变换函数进行求解。

[0071] 较佳地，所述变换函数为单调递增函数或单调递减函数。

[0072] 本公开还提供一种多方安全计算系统，所述多方安全计算系统包括：第一参与方与第二参与方；

[0073] 所述第一参与方，用于与第二参与方共享第一随机数种子；

[0074] 所述第一参与方，还用于根据所述第一随机数种子生成所述第一参与方的原始数据所对应的第一数据分片和所述第二参与方的原始数据所对应的第二数据分片；

[0075] 所述第一参与方，还用于将所述第一数据分片和所述第二数据分片进行减法计算以获得第一分片差值；

[0076] 所述第一参与方，还用于提取所述第一分片差值的第一符号位和第一无符号数值位，将所述第一无符号数值位进行变换处理以获得第一变换结果分片；

[0077] 所述第二参与方，用于根据所述第一随机数种子生成所述第一参与方的原始数据所对应的第五数据分片和所述第二参与方的原始数据所对应的第六数据分片；

[0078] 所述第二参与方，还用于将所述第五数据分片和所述第六数据分片进行减法计算以获得第三分片差值；

[0079] 所述第二参与方，还用于提取所述第三分片差值的第二符号位和第二无符号数值位，将所述第二无符号数值位进行变换处理以获得第二变换结果分片；

[0080] 所述第二参与方，还用于将所述第二变换结果分片发送给所述第一参与方；

[0081] 所述第一参与方，还用于对所述第二变换结果分片与所述第一变换结果分片进行分片恢复，以获得变换结果；

[0082] 所述第一参与方，还用于根据所述第一符号位和所述变换结果确定第一比较结果分片；

[0083] 所述第二参与方，还用于根据所述第二符号位确定第二比较结果分片；

[0084] 所述第一比较结果分片和所述第二比较结果分片用于确定所述第一参与方的原始数据与所述第二参与方的原始数据的比较结果。

[0085] 本公开还提供一种电子设备，包括存储器、处理器及存储在存储器上并用于在处理器上运行的计算机程序，所述处理器执行所述计算机程序时实现前述的多方安全计算方法。

[0086] 本公开还提供一种计算机可读存储介质，其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前述的多方安全计算方法。

[0087] 在符合本领域常识的基础上，上述各优选条件，可任意组合，即得本公开各较佳实例。

[0088] 本公开的积极进步效果在于：通过参与方之间共享随机数种子后，在不发生通信的条件下互相获取对方原始数据的数据分片，各自在本地进行计算，仅在执行多方安全计算乘法计算以及发送变换结果分片的时候发生通信。实现了整个计算过程中通信次数较少，运算量较少，且没有敏感信息在节点之间交互的效果。

附图说明

[0089] 图1为本公开一示例性实施例提供的一种多方安全计算方法的流程图；

[0090] 图2为本公开一示例性实施例提供的一种多方安全计算方法的数据交互过程的流程图；

[0091] 图3为本公开一示例性实施例提供的另一种多方安全计算方法的流程图；

[0092] 图4为本公开一示例性实施例提供的另一种多方安全计算方法的流程图；

[0093] 图5为本公开一示例性实施例提供的一种多方安全计算装置的模块示意图；

[0094] 图6为本公开一示例性实施例提供的另一种多方安全计算装置的模块示意图；

[0095] 图7为本公开一示例性实施例提供的一种多方安全计算系统的示意图；

[0096] 图8为本公开一示例性实施例提供的另一种多方安全计算系统的示意图；

[0097] 图9为本公开一示例性实施例提供的一种电子设备的结构示意图。

具体实施方式

[0098] 下面通过实施例的方式进一步说明本公开，但并不因此将本公开限制在所述的实施例范围之中。

[0099] 图1为本公开一示例性实施例提供的一种多方安全计算方法的流程图，图2为本公开一示例性实施例提供的一种多方安全计算方法的数据交互过程的流程图。该多方安全计算方法应用于第一参与方，参照图1和图2可知，多方安全计算方法包括：

[0100] 步骤101、与第二参与方共享第一随机数种子，并根据第一随机数种子生成第一参与方的原始数据所对应的第一数据分片和第二参与方的原始数据所对应的第二数据分片。

[0101] 在本步骤中，第一参与方和第二参与方共享第一随机数种子，该第一随机数种子用于随机数的生成，进而用于对原始数据进行数据分片。其中，第一随机数种子的共享，可选地，基于Diffie-Hellman密钥交换原理实现。

[0102] 例如，第一参与方与第二参与方分别持有原始数据X和Y，其中X为88，Y为12。第一参与方与第二参与方共享一对第一随机数种子$seed_{a1}$和$seed_{b1}$。第一参与方和第二参与方均基于$seed_{a1}$生成随机数R_x=1，以及基于$seed_{b1}$生成随机数R_y=-95。在对原始数据进行分片时，可选地，其规则为：随机数R_x为原始数据X所生成的两个分片的其中一个，随机数R_y为原始数据Y所生成的两个分片的其中一个，则原始数据X分为：1和87，原始数据Y分为：-95和107。

[0103] 第一参与方所持有的数据分片为：第一数据分片X_1和第二数据分片Y_1，其中，$X_1=X-R_x=88-1=87$，$Y_1=R_y=-95$；

[0104] 同理，第二参与方所持有的数据分片为：第五数据分片X_2和第六数据分片Y_2，其中，$X_2=R_x=1$，$Y_2=Y-R_y=12-(-95)=107$；

[0105] 可选地，在本步骤中的第一随机数种子在完成对原始数据进行数据分片之后，第一随机数种子需要进行更新，成为第二随机数种子，以用于下一次的数据分片，可选地，更新方法为：$seed_{a2}=seed_{a1}+1$和$seed_{b2}=seed_{b1}+1$。应该理解的是，该更新方法可根据实际需要调整，并不局限于上述更新方法，只要使得第二随机数种子区别于第一随机数种子即可。

[0106] 步骤102、将第一数据分片和第二数据分片进行减法计算以获得第一分片差值。

[0107] 在本步骤中，对在步骤101中所获取的第一数据分片和第二数据分片进行减法计算。例如，第一参与方所持有的第一数据分片X_1为87和第二数据分片Y_1为-95，则第一分片差值D_1为：$D_1=Y_1-X_1=-95-87=-182$。

[0108] 步骤103、提取第一分片差值的第一符号位和第一无符号数值位，将第一无符号数值位进行变换处理以获得第一变换结果分片。

[0109] 在本步骤中，对第一分片差值进行第一符号位提取，当第一分片差值为正数时，所提取的第一符号位为0，当第一分片差值为负数时，所提取的第一符号位为1。例如，当第一分片差值D_1为-182，则第一分片差值的第一符号位$sign_1$为1。

[0110] 对于第一无符号位数值的提取，当第一分片差值为正数时，则直接提取第一分片差值本身。可选地，当第一分片差值为负数时，既可以利用补码计算原理获得，也可以利用如下公式进行计算：

[0111] $D'_1=2^{L-1}+D_1$

[0112] 其中，D'_1为第一无符号数值位，L为限定的数值范围的二进制比特数。例如，当数值范围为32比特时L为32，当数值范围为64比特时L为64。

[0113] 其中，步骤103包括：

[0114] 步骤1031、根据第二随机数种子生成第一参与方的第一无符号数值位所对应的第三数据分片和第二参与方的第二无符号数值位所对应的第四数据分片；

[0115] 在本步骤中，由于第一参与方和第二参与方共享了第一随机数种子，并且第一随机数种子更新后生成了第二随机数种子，该第二随机数种子用于随机数的生成，进而用于对第一无符号数值位进行数据分片。

[0116] 步骤1032、将第三数据分片和第四数据分片进行减法计算以获得第二分片差值；

[0117] 步骤1033、将第二分片差值进行函数变换，以获得第一变换结果分片。

[0118] 其中，步骤1033包括：与第二参与方协同生成变换函数参数，以生成第一变换函数参数分片；将第一变换函数参数分片和第二分片差值代入变换函数进行求解。由于本步骤涉及MPC(多方安全计算)的计算工作，需要与第二参与方建立通信，以完成函数变换的计算。可选地，变换函数为单调递增函数或单调递减函数。

[0119] 在本步骤中，可选地，变换函数为线性函数，例如，d=a*D；可选地，变换函数也可为指数函数，例如，$d=a^D$。其中，a为变换函数参数，D是对第一无符号数值位和第二无符号数值位进行重分片的减法结果。其中，重分片的减法的过程为：

[0120] 根据第二随机数种子进行重分片，分别对第一无符号数值位e_1和第二无符号数值位e_2进行分片处理，第一无符号数值位分成第三数据分片G_1和第七数据分片G_2，第二无符号数值位分成第四数据分片H_1和第八数据分片H_2。

[0121] 因此，在第一参与方持有第三数据分片G_1和第四数据分片H_1，其中$G_1=e_1-R_{x2}$，$H_1=R_{y2}$；在第二参与方持有第七数据分片G_2和第八数据分片H_2，其中$G_2=R_{x2}$，$H_2=e_2-R_{y2}$。

[0122] 然后，执行分片的减法计算。在第一参与方计算第二分片差值为：$D_2=G_1-H_1$；在第二参与方计算第四分片差值为：$D_4=G_2-H_2$。步骤104、接收第二参与方的第二变换结果分片，与第一变换结果分片进行分片恢复，以获得变换结果；其中，第二变换结果分片由第二参与方根据第一随机数种子和第二参与方的原始数据生成。

[0123] 在本步骤中，变换结果根据第一变换结果分片与第二变换结果分片进行分片恢复后的数值确定。

[0124] 可选地，若变换函数为单调递增线性函数时，分片恢复后的数值若大于0，则变换结果输出为1，否则变换结果输出为0；其中，在执行分片的减法计算时，对于第一参与方计算第二分片差值为：$D_2=G_1-H_1$；对于第二参与方计算第四分片差值为：$D_4=G_2-H_2$。

[0125] 同理，若变换函数为单调递减线性函数时，分片恢复后的数值若大于0，则变换结果输出为1，否则变换结果输出为0；但是，在执行分片的减法计算时，对于第一参与方计算第二分片差值变为：$D_2=H_1-G_1$；对于第二参与方计算第四分片差值变为：$D_4=H_2-G_2$。

[0126] 可选地，若变换函数为单调递增指数函数时，分片恢复后的数值若大于1，则变换结果输出为1，否则变换结果输出为0。其中，在执行分片的减法计算时，对于第一参与方计算第二分片差值为：$D_2=G_1-H_1$；对于第二参与方计算第四分片差值为：$D_4=G_2-H_2$。

[0127] 同理，若变换函数为单调递减指数函数时，分片恢复后的数值若大于1，则变换结果输出为1，否则变换结果输出为0。但是，在执行分片的减法计算时，对于第一参与方计算第二分片差值变为：$D_2=H_1-G_1$；对于第二参与方计算第四分片差值变为：$D_4=H_2-G_2$。

[0128] 步骤105、根据第一符号位和变换结果确定第一比较结果分片，第一比较结果分片用于确定第一参与方的原始数据与第二参与方的原始数据的比较结果。

[0129] 在本步骤中，第一比较结果分片与第二比较结果分片用于判断比较结果。

[0130] 在本步骤中，比较结果分片的计算方法为：$ret_1=sign_1 \oplus carry$，其中，$ret_1$为第一参与方的比较结果分片，carry为变换结果，$sign_1$为第一分片差值的符号位。

[0131] 在本实施例中，第一参与方与第二参与方在获取第一随机数种子以后，仅在第一无符号数值位进行变换处理和获取第二变换结果分片时与第二参与方产生通信，其余的计算过程均在本地进行，且没有通信的产生，缩减通信次数以及计算成本。

[0132] 图3为本公开一示例性实施例提供的另一种多方安全计算方法的流程图，该多方安全计算方法应用于第二参与方，参见图2和图3可知，多方安全计算方法包括：

[0133] 步骤201、与第一参与方共享第一随机数种子，并根据第一随机数种子生成第一参与方的原始数据所对应的第五数据分片和第二参与方的原始数据所对应的第六数据分片。

[0134] 在本步骤中，第一参与方和第二参与方共享第一随机数种子，该第一随机数种子用于随机数的生成，进而用于对原始数据进行数据分片。其中，对原始数据进行数据分片的计算规则与步骤101相对应。

[0135] 例如，第一参与方与第二参与方分别持有原始数据X和Y，其中X为88，Y为12。第一参与方与第二参与方共享一对第一随机数种子$seed_{a1}$和$seed_{b1}$。第一参与方和第二参与方均基于$seed_{a1}$生成随机数R_x=1，以及基于$seed_{b1}$生成随机数R_y=-95。在对原始数据进行分片时，可选地，其规则为：随机数R_x为原始数据X所生成的两个分片的其中一个，随机数R_y为原始数据Y所生成的两个分片的其中一个，则原始数据X分为：1和87，原始数据Y分为：-95和107第一参与方所持有的数据分片为：

[0136] 第一数据分片X_1和第二数据分片Y_1，其中$X_1=X-R_x=88-1=87$，$Y_1=R_y=-95$；

[0137] 同理，第二参与方所持有的数据分片为：

[0138] 第五数据分片X_2和第六数据分片Y_2，其中$X_2=R_x=1$，$Y_2=Y-R_y=12-(-95)=107$；

[0139] 可选地，在本步骤中的第一随机数种子在完成对原始数据进行数据分片之后，第一随机数种子需要进行更新，成为第二随机数种子，以用于下一次的数据分片，更新方法可以为：$seed_{a2}=seed_{a1}+1$和$seed_{b2}=seed_{b1}+1$。应该理解的是，该更新方法可根据实际需要调整，并不局限于上述更新方法，只要使得第二随机数种子区别于第一随机数种子即可。

[0140] 步骤202、将第五数据分片和第六数据分片进行减法计算以获得第三分片差值。

[0141] 在本步骤中，对在步骤201中所获取的第五数据分片和第六数据分片进行减法计算。例如，第二参与方所持有的第五数据分片X_2为1和第六数据分片Y_2为107，则第三分片差值D_3为：$D_3=Y_2-X_2=107-1=106$。

[0142] 步骤203、提取第三分片差值的第二符号位和第二无符号数值位，将第二无符号数值位进行变换处理以获得第二变换结果分片。

[0143] 在本步骤中，对第三分片差值进行第二符号位提取，当第三分片差值为正数时，所提取的第二符号位为0，当第三分片差值为负数时，所提取的第二符号位为1。例如，当第三分片差值D_3为106，则第三分片差值的第二符号位$sign_2$为0。

[0144] 对于第二无符号位数值的提取，当第三分片差值为正数时，则直接提取第三分片差值本身。可选地，当第三分片差值为负数时，也可以利用如下公式进行计算：

[0145] $D'_3=2^{L-1}+D_3$

[0146] 其中，D'_3为第二无符号数值位，L为限定的数值范围的二进制比特数。例如，数值范围为32比特时L为32，数值范围为64比特时L为64。

[0147] 其中，步骤203包括：

[0148] 步骤2031、根据第二随机数种子生成第一参与方的第一无符号数值位所对应的第七数据分片和第二参与方的第二无符号数值位所对应的第八数据分片；

[0149] 在本步骤中，由于第一参与方和第二参与方共享了第一随机数种子，并且第一随机数种子更新后生成了第二随机数种子，该第二随机数种子用于随机数的生成，进而用于

对第三无符号数值位进行数据分片。

[0150] 步骤2032、将第七数据分片和第八数据分片进行减法计算以获得第四分片差值；

[0151] 步骤2033、将第四分片差值进行函数变换，以获得第二变换结果分片。

[0152] 其中，步骤2033包括：与第二参与方协同生成变换函数参数，以生成第二变换函数参数分片；将第二变换函数参数分片和第四分片差值代入变换函数进行求解，由于本步骤涉及MPC的计算工作，需要与第一参与方建立通信，以完成函数变换的计算。可选地，变换函数为单调递增函数或单调递减函数。

[0153] 在本步骤中，可选地，变换函数为线性函数，例如，d=a*D；可选地，变换函数也可为指数函数，例如，$d=a^D$。其中，a为变换函数参数，D是对第一无符号数值位和第二无符号数值位进行重分片的减法结果。其中，重分片的减法的过程为：

[0154] 根据第二随机数种子进行重分片，分别对第一无符号数值位e_1和第二无符号数值位e_2进行分片处理，第一无符号数值位分成第三数据分片G_1和第七数据分片G_2，第二无符号数值位分成第四数据分片H_1和第八数据分片H_2。

[0155] 因此，在第一参与方持有第三数据分片G_1和第四数据分片H_1，其中$G_1=e_1-R_{x2}$，$H_1=R_{y2}$；在第二参与方持有第七数据分片G_2和第八数据分片H_2，其中$G_2=R_{x2}$，$H_2=e_2-R_{y2}$。

[0156] 然后，执行分片的减法计算。在第一参与方计算第二分片差值为：$D_2=G_1-H_1$；在第二参与方计算第四分片差值为：$D_4=G_2-H_2$。

[0157] 步骤204、将第二变换结果分片发送给第一参与方，以由第一参与方根据第二变换结果分片和第一变换结果分片确定变换结果；第一变换结果分片由第一参与方根据第一随机数种子和第一参与方的原始数据生成；

[0158] 步骤205、根据第二符号位确定第二比较结果分片，第二比较结果分片用于确定第一参与方的原始数据与第二参与方的原始数据的比较结果。

[0159] 在本实施例中，第一参与方与第二参与方在获取第一随机数种子以后，仅在第二无符号数值位进行变换处理和发送第二变换结果分片时与第一参与方产生通信，其余的计算过程均在本地进行，且没有通信的产生，缩减通信次数以及计算成本。

[0160] 图4为本公开一示例性实施例提供的另一种多方安全计算方法的流程图，多方安全计算方法包括：

[0161] 步骤401、第一参与方与第二参与方共享第一随机数种子；

[0162] 步骤402、第一参与方根据第一随机数种子生成第一参与方的原始数据所对应的第一数据分片和第二参与方的原始数据所对应的第二数据分片；

[0163] 步骤403、第一参与方将第一数据分片和第二数据分片进行减法计算以获得第一分片差值；

[0164] 步骤404、第一参与方提取第一分片差值的第一符号位和第一无符号数值位，将第一无符号数值位进行变换处理以获得第一变换结果分片；

[0165] 步骤405、第二参与方根据第一随机数种子生成第一参与方的原始数据所对应的第五数据分片和第二参与方的原始数据所对应的第六数据分片；

[0166] 步骤406、第二参与方将第五数据分片和第六数据分片进行减法计算以获得第三分片差值；

[0167] 步骤407、第二参与方提取第三分片差值的第二符号位和第二无符号数值位，将第

二无符号数值位进行变换处理以获得第二变换结果分片；

[0168] 步骤408、第二参与方将第二变换结果分片发送给第一参与方；

[0169] 步骤409、第一参与方对第二变换结果分片与第一变换结果分片进行分片恢复，以获得变换结果；

[0170] 步骤410、第一参与方根据第一符号位和变换结果确定第一比较结果分片；

[0171] 步骤411、第二参与方根据第二符号位确定第二比较结果分片；

[0172] 第一比较结果分片和第二比较结果分片用于确定第一参与方的原始数据与第二参与方的原始数据的比较结果。

[0173] 步骤412、第一参与方根据第一比较结果分片和第二比较结果分片确定比较结果。

[0174] 在本步骤中，对于比较结果的确定可由第一参与方、第二参与方或者数据获取方执行，只要具备第一比较结果分片和第二比较结果分片就可确定比较结果。

[0175] 为对上述步骤进行说明，在此举一个具体示例，本示例包括：

[0176] 步骤501、第一参与方与第二参与方分别持有原始数据X和Y，其中X为88，Y为12。第一参与方与第二参与方共享一对第一随机数种子$seed_{a1}$和$seed_{b1}$。第一参与方和第二参与方均基于$seed_{a1}$生成随机数R_x=1，以及基于$seed_{b1}$生成随机数R_y=-95。在对原始数据进行分片时，可选地，其规则为：随机数R_x为原始数据X所生成的两个分片的其中一个，随机数R_y为原始数据Y所生成的两个分片的其中一个，则原始数据X分为：1和87，原始数据Y分为：-95和107。

[0177] 第一参与方所持有的数据分片为：

[0178] 第一数据分片X_1和第二数据分片Y_1，其中$X_1=X-R_x=88-1=87$，$Y_1=R_y=-95$；

[0179] 同理，第二参与方所持有的数据分片为：

[0180] 第五数据分片X_2和第六数据分片Y_2，其中$X_2=R_x=1$，$Y_2=Y-R_y=12-(-95)=107$；

[0181] 步骤502、第一参与方与第二参与方分别在本地进行减法计算，分别计算出第一分片差值和第三分片差值。

[0182] 在第一参与方第一分片差值D_1为：$D_1=Y_1-X_1=-95-87=-182$；

[0183] 在第二参与方第三分片差值D_3为：$D_3=Y_2-X_2=107-1=106$；

[0184] 步骤503、提取第一分片差值D_1的第一符号位和第三分片差值D_3的第二符号位。

[0185] 在本步骤中，第一分片差值D_1为-182，第一符号位$sign_1$为1。

[0186] 第三分片差值D_3为106，第二符号位$sign_2$为0。

[0187] 步骤504、提取第一分片差值D_1的第一无符号数值位D'_1和第三分片差值D_3的第二无符号数值位D'_3。

[0188] 在本步骤中，第一分片差值D_1为-182，获取第一无符号数值位D'_1的处理过程如下：-182的补码为32位数字“11111111111111111111111101001010”，其中左边第一位为第一符号位，当去掉第一符号位后变为31位数字“1111111111111111111111101001010”作为第一无符号数值位D'_1，将其转换成十进制后表示为2147483466。

[0189] 第三分片差值D_3为106，第二无符号数值位D'_3为106。

[0190] 步骤505、基于第一无符号数值位D'_1和第二无符号数值位D'_3进行变换获得第一变换数据e_1和第二变换数据e_2。变换规则可以为：第一参与方的第一变换数据e_1等于第一无符号数值位D'_1，第二参与方的第二无符号数值位D'_3根据如下公式进行转换：

[0191] $e_2=2^{L-1}-1-D'_3$

[0192] 其中，数值长度为32比特时L为32，所以，在本步骤中第一变换数据e_1为2147483466，第二变换数据e_2为2147483541。

[0193] 步骤506、对第一变换数据e_1和第二变换数据e_2进行数据分片处理。第一参与方和第二参与方均基于第二随机数种子$seed_{a2}$和$seed_{b2}$生成随机数R_{x2}=42378，以及基于$seed_{b1}$生成随机数R_{y2}=893425。在对原始数据进行分片时，可选地，其规则为：随机数R_{x2}为原始数据e_1的分片，随机数R_{y2}为原始数据e_2的分片，则原始数据X分为：2147441088和42378，原始数据Y分为：893425和2146590116。

[0194] 第一参与方所持有的数据分片为：

[0195] 第三数据分片G_1和第四数据分片H_1，其中$G_1=e_1-R_{x2}$=2147483466-42378=2147441088，$H_1=R_{y2}$=893425；

[0196] 同理，第二参与方所持有的数据分片为：

[0197] 第七数据分片G_2和第八数据分片H_2，其中$G_2=R_{x2}$=42378，$H_2=e_2-R_{y2}$=2147483541-893425=2146590116。

[0198] 步骤507、分别在第一参与节点和第二参与节点进行减法计算，计算出第二分片差值和第四分片差值：

[0199] 对于第一参与方计算第二分片差值为：$D_2=G_1-H_1$=2147441088-893425=2146547663；

[0200] 对于第二参与方计算第四分片差值为：$D_4=G_2-H_2$=42378-2146590116=-2146547738。

[0201] 步骤508、第一参与方和第二参与方分别协同生成第一变换函数参数分片a_1和第二变换函数参数分片a_2。

[0202] 步骤509、第一参与方和第二参与方分别进行MPC乘法计算。

[0203] 在本步骤中，MPC乘法计算是基于乘法三元组实现的，经过MPC乘法计算后，在第一参与方计算第一变换结果分片为d_1，在第二参与方计算第二变换结果分片为d_2。

[0204] 步骤510、第二参与方将第二变换结果分片发送给第一参与方，在第一参与方将第一变换结果分片和第二变换结果分片进行分片恢复，生成分片恢复结果d，其中$d=d_1+d_2$=-1875。

[0205] 步骤511、根据分片恢复结果d的数值计算变换结果carry的值，当d大于0时则变换结果carry为1，当d不大于0时则变换结果carry为0。由于d为负数，所以变换结果carry为0。

[0206] 步骤512、分别在第一参与方和第二参与方计算第一比较结果分片和第二比较结果分片。

[0207] 其中，第一比较结果分片为：$ret_1=sign_1 \oplus carry=1$；

[0208] 第二比较结果分片为：$ret_2=sign_2=0$。

[0209] 步骤513、计算比较结果，若比较结果为1则表示True，即表示第一参与方的原始数据大于第二参与方的原始数据。在本步骤中，比较结果计算为：$ret=ret_1 \oplus ret_2=1 \oplus 0=1$，则表明表示第一参与方的原始数据88大于第二参与方的原始数据12。若比较结果为0则表示False，即表示第一参与方的原始数据不大于第二参与方的原始数据。

[0210] 另外，对于判断第一参与方的原始数据与第二参与方的原始数据是否相等的情

况，判断方法为：首先，对原始数据之间进行两次比较计算，得到比较结果。然后，再对比较结果进行取反计算，将取反后的比较结果进行与运算，若运算结果为1则表示相等，若运算结果为0则表示不相等。在此举两个示例进行说明：

[0211] 示例1：当第一参与方的原始数据为x=2，第二参与方的原始数据为y=2时，先比较x是否大于y，比较结果为0；再比较y是否大于x，比较结果为0。对两次比较结果取反后进行与运算为：1&1=1，则表明x与y相等。

[0212] 示例2：当第一参与方的原始数据为x=2，第二参与方的原始数据为y=3时，先比较x是否大于y，比较结果为0；再比较y是否大于x，比较结果为1。对两次比较结果取反后进行与运算为：1&0=0，则表明x与y不相等。

[0213] 在本步骤中，在确定比较结果的时候，可选地，在第一参与方进行和/或在第二参与方进行。或者，如图8所示，在第一参与方和第二参与方之外设置结果获取方，第一参与方和第二参与方分别将第一比较结果分片和第二比较结果分片发送给结果获取方，在结果获取方确定比较结果。

[0214] 在本实施例中，第一参与方与第二参与方在获取第一随机数种子以后，仅在函数变换的过程中以及第二变换结果从第二参与方发送至第一参与方时发生通信，其余的计算过程均在本地进行，且没有通信的产生，缩减通信次数以及计算成本。

[0215] 图5为本公开一示例性实施例提供的一种多方安全计算装置的模块示意图，该多方安全计算装置对应于上述多方安全计算方法，多方安全计算装置应用于第一参与方，多方安全计算装置包括：

[0216] 第一分片模块51，用于与第二参与方共享第一随机数种子，并根据第一随机数种子生成第一参与方的原始数据所对应的第一数据分片和第二参与方的原始数据所对应的第二数据分片；

[0217] 第一差值模块52，用于将第一数据分片和第二数据分片进行减法计算以获得第一分片差值；

[0218] 第一变换模块53，用于提取第一分片差值的第一符号位和第一无符号数值位，将第一无符号数值位进行变换处理以获得第一变换结果分片；

[0219] 分片接收模块54，用于接收第二参与方的第二变换结果分片，与第一变换结果分片进行分片恢复，以获得变换结果；其中，第二变换结果分片由第二参与方根据第一随机数种子和第二参与方的原始数据生成；

[0220] 第一结果确定模块55，用于根据第一符号位和变换结果确定第一比较结果分片，第一比较结果分片用于确定第一参与方的原始数据与第二参与方的原始数据的比较结果。

[0221] 在本实施例中，第一参与方与第二参与方在获取第一随机数种子以后，仅在第一无符号数值位进行变换处理和获取第二变换结果分片时与第二参与方产生通信，其余的计算过程均在本地进行，且没有通信的产生，缩减通信次数以及计算成本。

[0222] 可选地，第一变换模块53，包括：

[0223] 第一分片单元，用于根据第二随机数种子生成第一参与方的第一无符号数值位所对应的第三数据分片和第二参与方的第二无符号数值位所对应的第四数据分片；

[0224] 第一差值单元，用于将第三数据分片和第四数据分片进行减法计算以获得第二分片差值；

[0225] 第一变换单元，用于将第二分片差值进行函数变换，以获得第一变换结果分片。

[0226] 可选地，第一变换单元，还用于与第二参与方协同生成变换函数参数，以生成第一变换函数参数分片；将第一变换函数参数分片和第二分片差值代入变换函数进行求解。

[0227] 可选地，变换函数为单调递增函数或单调递减函数。

[0228] 图6为本公开一示例性实施例提供的另一种多方安全计算装置的模块示意图，该多方安全计算装置对应于上述多方安全计算方法，多方安全计算装置应用于第二参与方，多方安全计算装置包括：

[0229] 第二分片模块61，用于与第一参与方共享第一随机数种子，并根据第一随机数种子生成第一参与方的原始数据所对应的第五数据分片和第二参与方的原始数据所对应的第六数据分片；

[0230] 第二差值模块62，用于将第五数据分片和第六数据分片进行减法计算以获得第三分片差值；

[0231] 第二变换模块63，用于提取第三分片差值的第二符号位和第二无符号数值位，将第二无符号数值位进行变换处理以获得第二变换结果分片；

[0232] 分片发送模块64，用于将第二变换结果分片发送给第一参与方，以由第一参与方根据第二变换结果分片和第一变换结果分片确定变换结果；第一变换结果分片由第一参与方根据第一随机数种子和第一参与方的原始数据生成；

[0233] 第二结果确定模块65，用于根据第二符号位确定第二比较结果分片，第二比较结果分片用于确定第一参与方的原始数据与第二参与方的原始数据的比较结果。

[0234] 可选地，第二变换模块63，包括：

[0235] 第二分片单元，用于根据第二随机数种子生成第一参与方的第一无符号数值位所对应的第七数据分片和第二参与方的第二无符号数值位所对应的第八数据分片；

[0236] 第二差值单元，用于将第七数据分片和第八数据分片进行减法计算以获得第四分片差值；

[0237] 第二变换单元，用于将第四分片差值进行函数变换，以获得第二变换结果分片。

[0238] 可选地，第二变换单元，还用于与第二参与方协同生成变换函数参数，以生成第二变换函数参数分片；将第二变换函数参数分片和第四分片差值代入变换函数进行求解。

[0239] 可选地，变换函数为单调递增函数或单调递减函数。

[0240] 在本实施例中，第一参与方与第二参与方在获取第一随机数种子以后，仅在第二无符号数值位进行变换处理和发送第二变换结果分片时与第一参与方产生通信，其余的计算过程均在本地进行，且没有通信的产生，缩减通信次数以及计算成本。

[0241] 图7为本公开一示例性实施例提供的另一种多方安全计算系统的示意图，该多方安全计算系统对应于上述多方安全计算方法，该多方安全计算系统包括：第一参与方与第二参与方；

[0242] 第一参与方，用于与第二参与方共享第一随机数种子；

[0243] 第一参与方，用于根据第一随机数种子生成第一参与方的原始数据所对应的第一数据分片和第二参与方的原始数据所对应的第二数据分片；

[0244] 第一参与方，还用于将第一数据分片和第二数据分片进行减法计算以获得第一分片差值；

[0245] 第一参与方，还用于提取第一分片差值的第一符号位和第一无符号数值位，将第一无符号数值位进行变换处理以获得第一变换结果分片；

[0246] 第二参与方，用于根据第一随机数种子生成第一参与方的原始数据所对应的第五数据分片和第二参与方的原始数据所对应的第六数据分片；

[0247] 第二参与方，还用于将第五数据分片和第六数据分片进行减法计算以获得第三分片差值；

[0248] 第二参与方，还用于提取第三分片差值的第二符号位和第二无符号数值位，将第二无符号数值位进行变换处理以获得第二变换结果分片；

[0249] 第二参与方，还用于将第二变换结果分片发送给第一参与方；

[0250] 第一参与方，还用于对第二变换结果分片与第一变换结果分片进行分片恢复，以获得变换结果；

[0251] 第一参与方，还用于根据第一符号位和变换结果确定第一比较结果分片；

[0252] 第二参与方，还用于根据第二符号位确定第二比较结果分片；

[0253] 第一比较结果分片和第二比较结果分片用于确定第一参与方的原始数据与第二参与方的原始数据的比较结果。

[0254] 其中，第一比较结果分片和第二比较结果分片用于确定比较结果。在确定比较结果的时候，可选地，在第一参与方进行和/或在第二参与方进行。或者，如图8所示，在第一参与方和第二参与方之外设置结果获取方，第一参与方和第二参与方分别将第一比较结果分片和第二比较结果分片发送给结果获取方，在结果获取方确定比较结果。

[0255] 在本实施例中，第一参与方与第二参与方在获取第一随机数种子以后，仅在函数变换的过程中以及第二变换结果从第二参与方发送至第一参与方时发生通信，其余的计算过程均在本地进行，且没有通信的产生，缩减通信次数以及计算成本。

[0256] 图9为本实施例提供的一种电子设备的结构示意图。所述电子设备包括存储器、处理器及存储在存储器上并用于在处理器上运行的计算机程序，所述处理器执行所述程序时实现上述任一实施例提供的多方安全计算方法。图9显示的电子设备300仅仅是一个示例，不应对本公开实施例的功能和使用范围带来任何限制。

[0257] 参照图9，电子设备300可以以通用计算设备的形式表现，例如其可以为服务器设备。电子设备300的组件可以包括但不限于：上述至少一个处理器301、上述至少一个存储器302、连接不同系统组件(包括存储器302和处理器301)的总线303。

[0258] 总线303包括数据总线、地址总线和控制总线。

[0259] 存储器302可以包括易失性存储器，例如随机存取存储器(RAM)321和/或高速缓存存储器322，还可以进一步包括只读存储器(ROM)323。

[0260] 存储器302还可以包括具有一组(至少一个)程序模块324的程序/实用工具325，这样的程序模块324包括但不限于：操作系统、一个或者多个应用程序、其它程序模块以及程序数据，这些示例中的每一个或某种组合中可能包括网络环境的实现。

[0261] 处理器301通过运行存储在存储器302中的计算机程序，从而执行各种功能应用以及数据处理，例如本公开实施例中的多方安全计算方法。

[0262] 电子设备300也可以与一个或多个外部设备304(例如键盘、指向设备等)通信。这种通信可以通过输入/输出(I/O)接口305进行。并且，模型生成的设备300还可以通过网络

适配器306与一个或者多个网络(例如局域网(LAN),广域网(WAN)和/或公共网络,例如因特网)通信。如图所示,网络适配器306通过总线303与模型生成的设备300的其它模块通信。应当明白,尽管图中未示出,可以结合模型生成的设备300使用其它硬件和/或软件模块,包括但不限于:微代码、设备驱动器、冗余处理器、外部磁盘驱动阵列、RAID(磁盘阵列)系统、磁带驱动器以及数据备份存储系统等。

[0263] 应当注意,尽管在上文详细描述中提及了电子设备的若干单元/模块或子单元/模块,但是这种划分仅仅是示例性的并非强制性的。实际上,根据本公开的实施方式,上文描述的两个或更多单元/模块的特征和功能可以在一个单元/模块中具体化。反之,上文描述的一个单元/模块的特征和功能可以进一步划分为由多个单元/模块来具体化。

[0264] 本实施例还提供一种计算机可读存储介质,其上存储有计算机程序,所述程序被处理器执行时实现上述任一实施例提供的多方安全计算方法。

[0265] 其中,可读存储介质可以采用的更具体可以包括但不限于:便携式盘、硬盘、随机存取存储器、只读存储器、可擦拭可编程只读存储器、光存储器件、磁存储器件或上述的任意合适的组合。

[0266] 在可能的实施方式中,本公开还可以实现为一种程序产品的形式,其包括程序代码,当所述程序产品在终端设备上运行时,所述程序代码用于使所述终端设备执行实现上述任一实施例提供的多方安全计算方法。

[0267] 其中,可以以一种或多种程序设计语言的任意组合来编写用于执行本公开的程序代码,所述程序代码可以完全地在用户设备上执行、部分地在用户设备上执行、作为一个独立的软件包执行、部分在用户设备上部分在远程设备上执行或完全在远程设备上执行。

[0268] 虽然以上描述了本公开的具体实施方式,但是本领域的技术人员应当理解,这仅是举例说明,本公开的保护范围是由所附权利要求书限定的。本领域的技术人员在不背离本公开的原理和实质的前提下,可以对这些实施方式做出多种变更或修改,但这些变更和修改均落入本公开的保护范围。

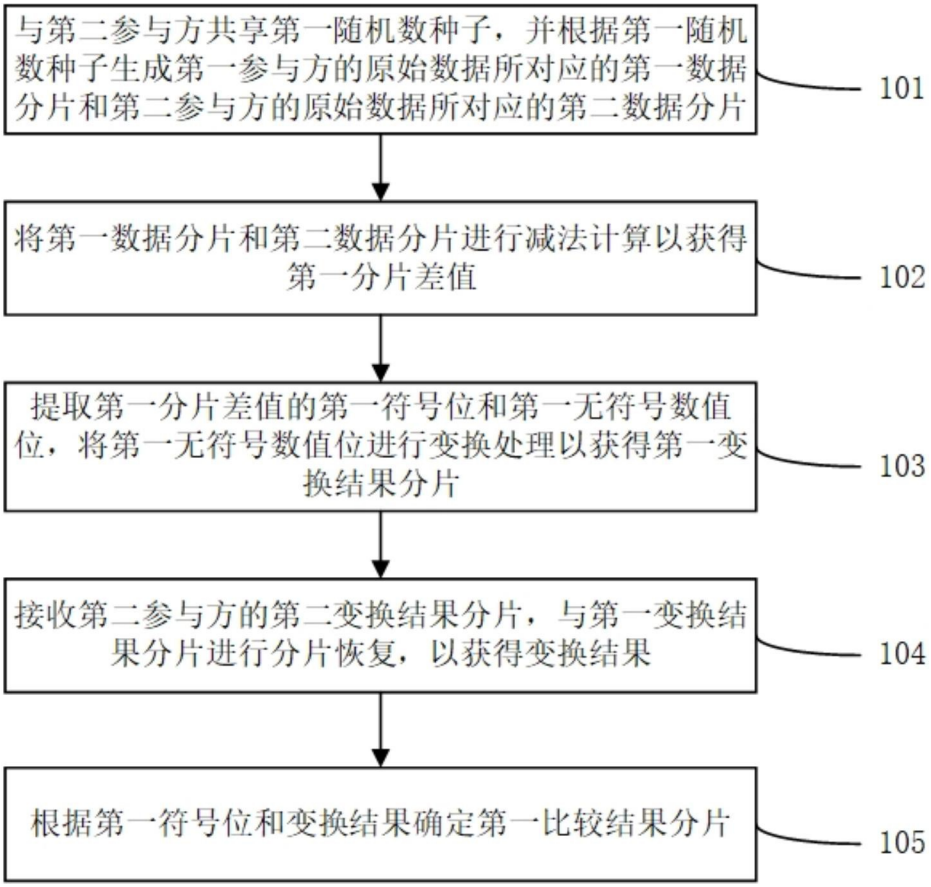

与第二参与方共享第一随机数种子，并根据第一随机数种子生成第一参与方的原始数据所对应的第一数据分片和第二参与方的原始数据所对应的第二数据分片
101
将第一数据分片和第二数据分片进行减法计算以获得第一分片差值
102
提取第一分片差值的第一符号位和第一无符号数值位，将第一无符号数值位进行变换处理以获得第一变换结果分片
103
接收第二参与方的第二变换结果分片，与第一变换结果分片进行分片恢复，以获得变换结果
104
根据第一符号位和变换结果确定第一比较结果分片
105

图1

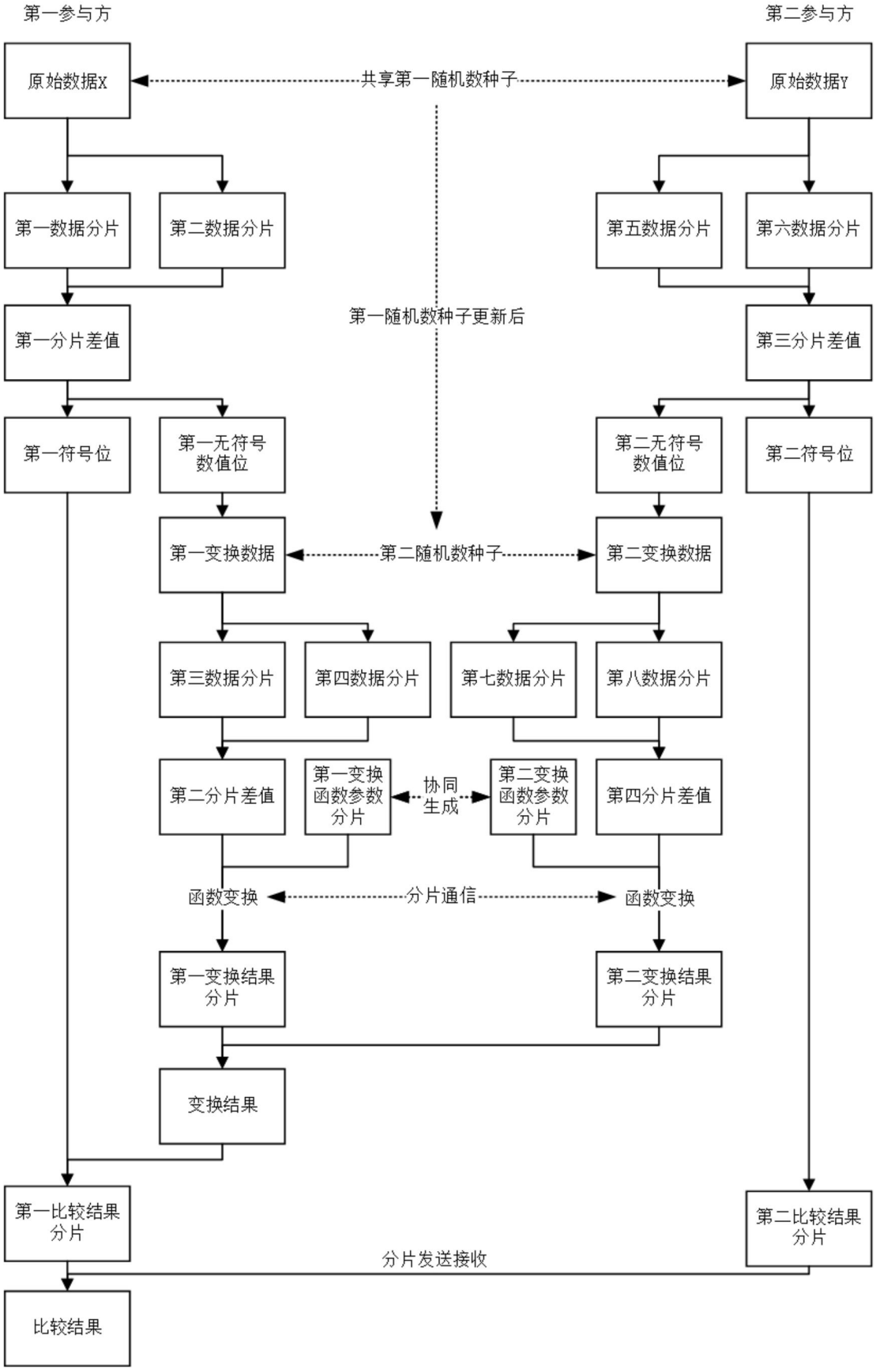

第一参与方
第二参与方
原始数据X
共享第一随机数种子
原始数据Y
第一数据分片
第二数据分片
第五数据分片
第六数据分片
第一随机数种子更新后
第一分片差值
第三分片差值
第一符号位
第一无符号数值位
第二无符号数值位
第二符号位
第一变换数据
第二随机数种子
第二变换数据
第三数据分片
第四数据分片
第七数据分片
第八数据分片
第二分片差值
第一变换函数参数分片
协同生成
第二变换函数参数分片
第四分片差值
函数变换
分片通信
函数变换
第一变换结果分片
第二变换结果分片
变换结果
第一比较结果分片
第二比较结果分片
分片发送接收
比较结果

图2

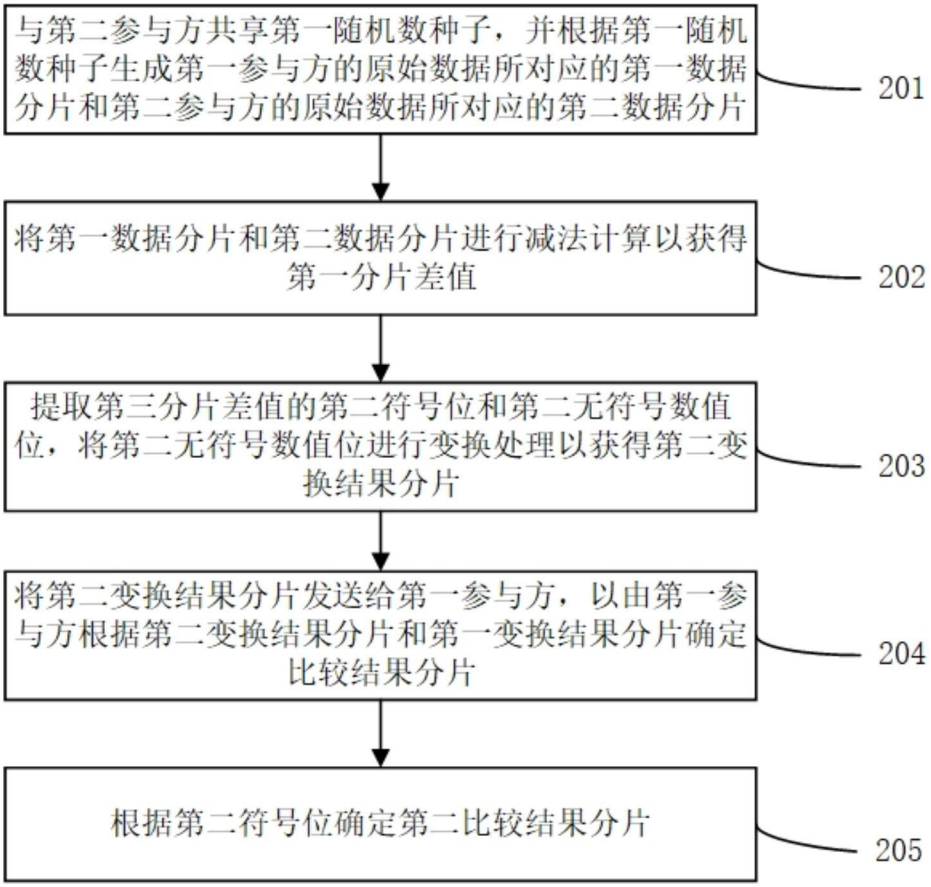

与第二参与方共享第一随机数种子，并根据第一随机数种子生成第一参与方的原始数据所对应的第一数据分片和第二参与方的原始数据所对应的第二数据分片
201
将第一数据分片和第二数据分片进行减法计算以获得第一分片差值
202
提取第三分片差值的第二符号位和第二无符号数值位，将第二无符号数值位进行变换处理以获得第二变换结果分片
203
将第二变换结果分片发送给第一参与方，以由第一参与方根据第二变换结果分片和第一变换结果分片确定比较结果分片
204
根据第二符号位确定第二比较结果分片
205

图3

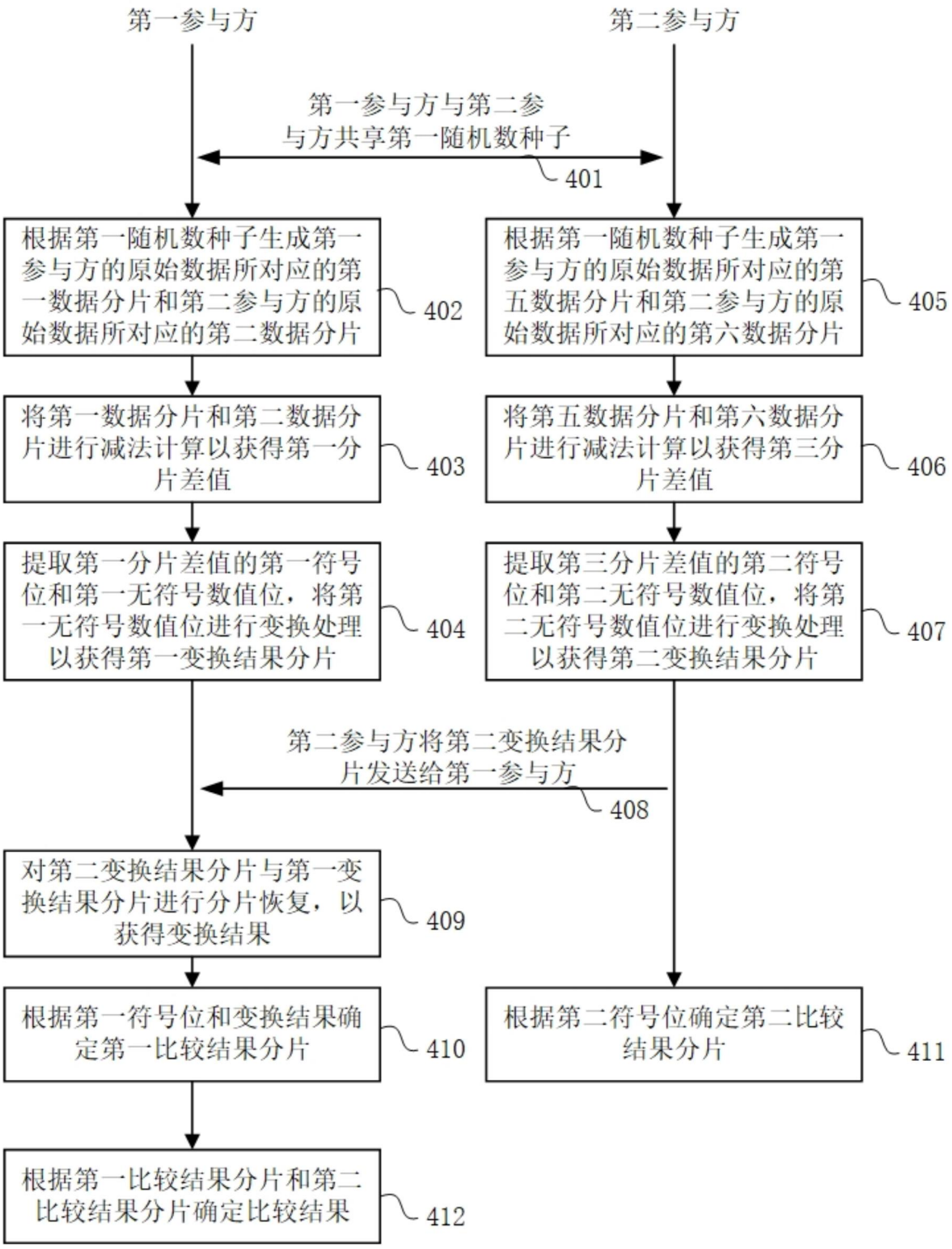

第一参与方
第二参与方
第一参与方与第二参与方共享第一随机数种子
401
根据第一随机数种子生成第一参与方的原始数据所对应的第一数据分片和第二参与方的原始数据所对应的第二数据分片
402
根据第一随机数种子生成第一参与方的原始数据所对应的第五数据分片和第二参与方的原始数据所对应的第六数据分片
405
将第一数据分片和第二数据分片进行减法计算以获得第一分片差值
403
将第五数据分片和第六数据分片进行减法计算以获得第三分片差值
406
提取第一分片差值的第一符号位和第一无符号数值位，将第一无符号数值位进行变换处理以获得第一变换结果分片
404
提取第三分片差值的第二符号位和第二无符号数值位，将第二无符号数值位进行变换处理以获得第二变换结果分片
407
第二参与方将第二变换结果分片发送给第一参与方
408
对第二变换结果分片与第一变换结果分片进行分片恢复，以获得变换结果
409
根据第一符号位和变换结果确定第一比较结果分片
410
根据第二符号位确定第二比较结果分片
411
根据第一比较结果分片和第二比较结果分片确定比较结果
412

图4

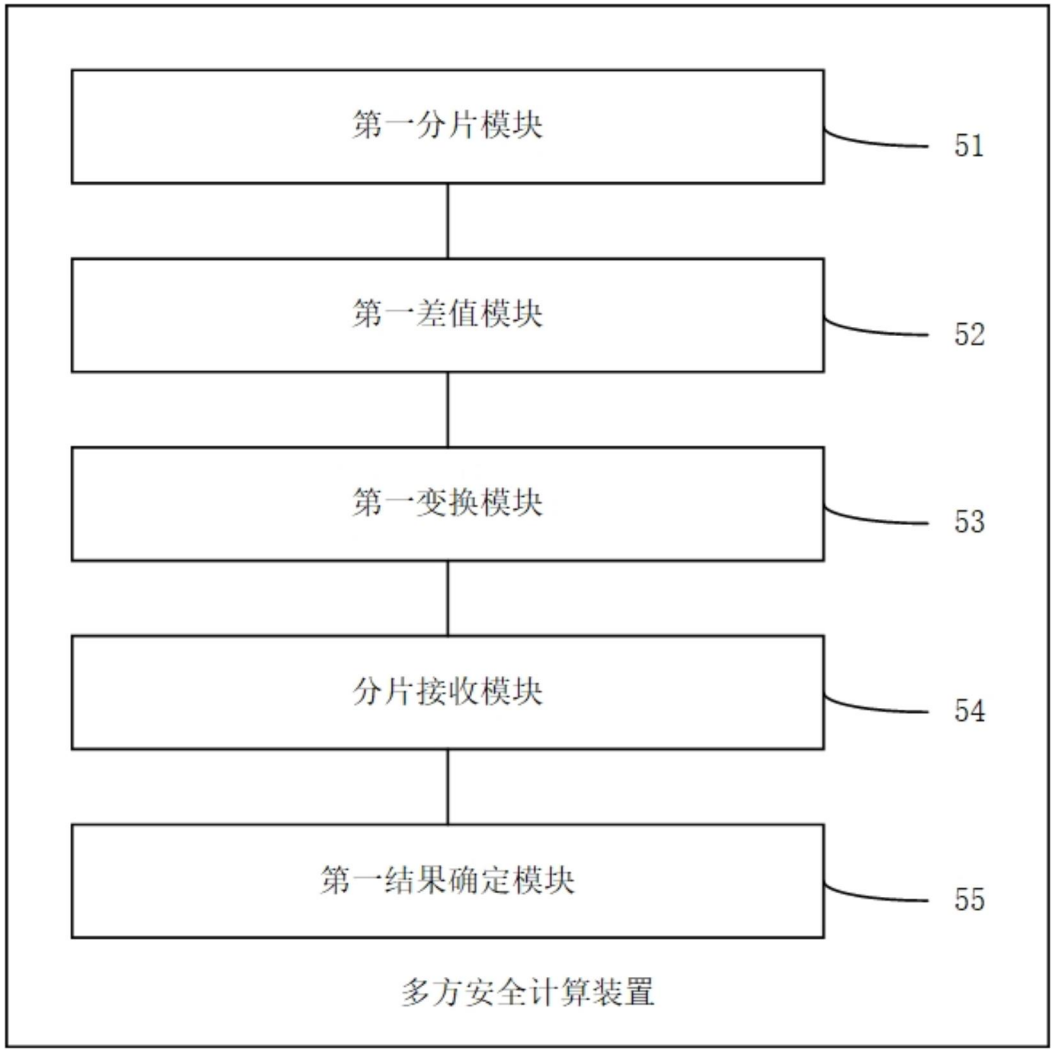

第一分片模块
51
第一差值模块
52
第一变换模块
53
分片接收模块
54
第一结果确定模块
55
多方安全计算装置

图5

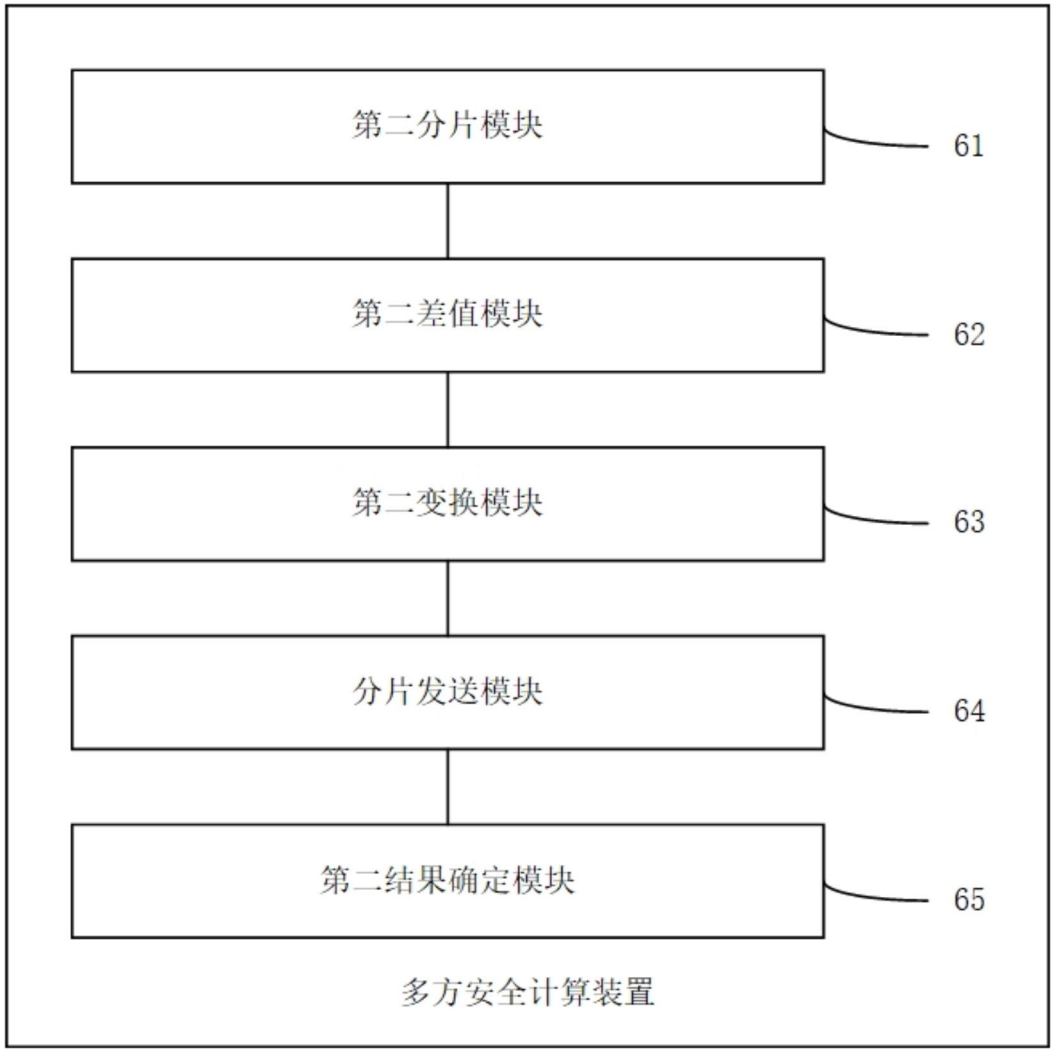

第二分片模块
61
第二差值模块
62
第二变换模块
63
分片发送模块
64
第二结果确定模块
65
多方安全计算装置

图6

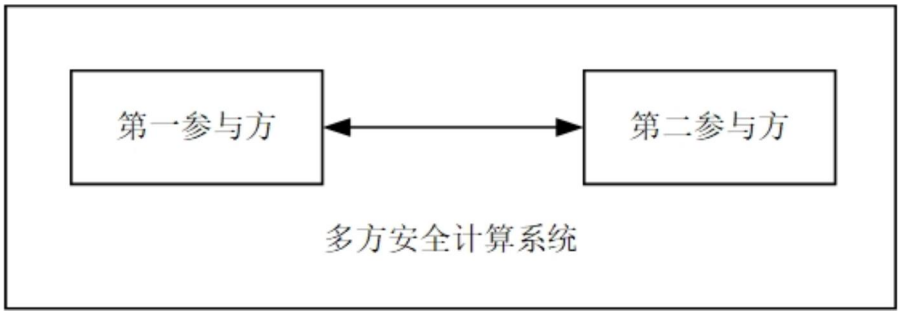

第一参与方
第二参与方
多方安全计算系统

图7

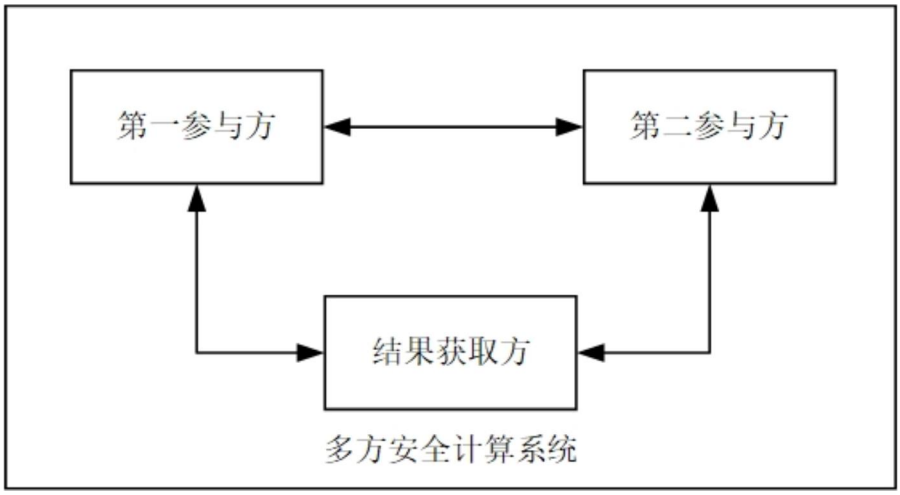

第一参与方
第二参与方
结果获取方
多方安全计算系统

图8

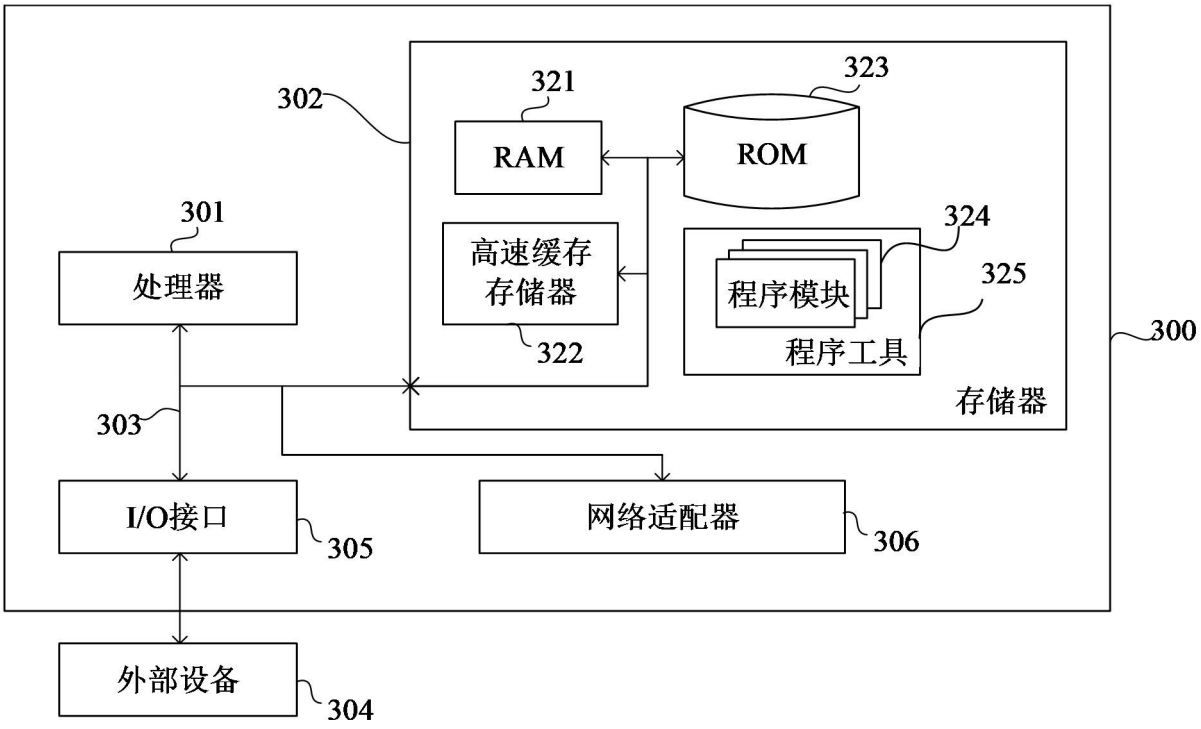

302
321
323
RAM
ROM
301
处理器
高速缓存
存储器
322
324
325
程序模块
程序工具
300
存储器
303
I/O接口
305
网络适配器
306
外部设备
304

图9