(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 115150084 A
(43)申请公布日 2022.10.04

(21)申请号 202211075407.1

(22)申请日 2022.09.05

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

(72)发明人 王震 李刚 张李军 杨超 张浩 黄芹健

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

(51)Int.Cl.
H04L 9/08(2006.01)
G06F 17/11(2006.01)
G06F 17/14(2006.01)

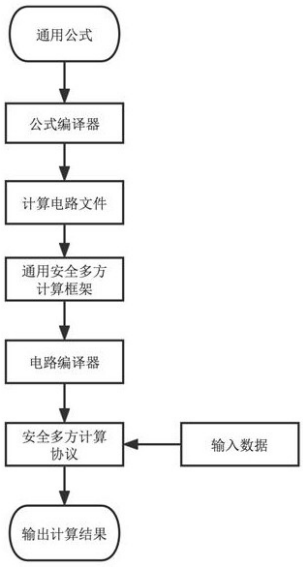
权利要求书3页 说明书12页 附图4页

(54)发明名称

一种安全多方计算方法、系统和计算机可读存储介质

(57)摘要

本发明提供一种安全多方计算方法、系统和计算机可读存储介质,通过设计一种基于后缀表达式的公式编译器,能自动将普通公式转化为通用安全多方计算框架可识别的计算公式,并转化生成特定的计算电路文件,然后通过电路编译器自动编译电路文件,生成二进制字节码,最后通过执行安全多方计算协议完成计算过程,输出结果。本发明能够自动生成并转化公式,提高安全多方计算产品的易用性,降低用户使用门槛,提高安全多方计算框架的使用灵活性。



CN 115150084 A

1.一种安全多方计算方法,其特征在于,所述方法包括:

根据安全多方计算需求确定通用公式,并将所述通用公式以字符串形式传入公式编译器;

由所述公式编译器解析所述通用公式,并将其转化为通用安全多方计算框架可支持的计算公式;

将所述计算公式写入电路中,生成特定格式的电路文件,并将电路文件输入通用安全多方计算框架;

使用通用安全多方计算框架的电路编译器编译电路文件,并进行编译优化,生成二进制字节码;

调用安全多方计算协议运行电路编译出的二进制字节码,并输入计算数据;

按照安全多方计算协议执行对输入计算数据的计算处理,并输出最终的计算结果。

2.根据权利要求1所述的一种安全多方计算方法,其特征在于,由所述公式编译器解析所述通用公式,并将其转化为通用安全多方计算框架可支持的计算公式;将所述计算公式写入电路中,生成特定格式的电路文件,具体包括:

由所述公式编译器接收所述通用公式,并将所述通用公式格式化,转化为符合标准格式的通用公式;

由公式编译器根据后缀逆波兰表达式规则,将所述公式进行解析,表示为后缀表达式向量;

将通用安全多方计算框架支持的计算类型与通用公式符号进行匹配,构造计算符号映射表;

由公式编译器根据计算符号映射表将后缀表达式向量一次映射为通用安全多方计算框架可识别的计算公式;

将转化后的计算公式增加输入参数及依赖信息后,写入电路,生成特定格式的电路文件。

3.根据权利要求1所述的一种安全多方计算方法,其特征在于,使用通用安全多方计算框架的电路编译器编译电路文件,并进行编译优化,生成二进制字节码,具体包括:

对电路文件中的电路语句进行分析,通过翻译程序将电路语句翻译为单独的基本语法块;

按照电路文件内传入参数数据设置特定参数,所述特定参数包括精度值、线程数、安全参数中的一种或多种;

在每个单独的基本语法块内,使用通用安全多方计算框架的电路解析模块对部分指令进行优化处理,生成包括安全多方计算指令的类汇编指令集;

将类汇编指令集转码生成二进制字节码并写入文件中,生成字节码文件。

4.根据权利要求3所述的一种安全多方计算方法,其特征在于,在使用通用安全多方计算框架的电路解析模块对部分指令进行优化处理之后,所述方法还包括:

使用通用安全多方计算框架的电路解析模块对部分指令进行优化处理,并记录本次优化方式;

通过评价模型对优化后的类汇编指令集进行评价处理,输出评价结果;

将部分指令、本次优化方式以及评价结果进行打包,形成一项样本数据;

汇集每次使用通用安全多方计算框架的电路解析模块对部分指令进行优化处理得到的样本数据，并形成样本数据库；

基于样本数据库中的每项样本数据对电路解析模块进行训练，使得电路解析模块基于每项样本数据进行深度学习，以得到所述电路解析模块的最佳优化参数；

将所述最佳优化参数置入所述电路解析模块中，得到更新后的电路解析模块；

使用更新后的电路解析模块对后续解析过程中的指令进行优化处理。

5.根据权利要求1所述的一种安全多方计算方法，其特征在于，调用安全多方计算协议运行电路编译出的二进制字节码，并输入计算数据；按照安全多方计算协议执行对输入计算数据的计算处理，并输出最终的计算结果，具体包括：

初始化安全多方计算协议参数，所述协议参数至少包括计算域大小、和安全参数大小；

进行预处理阶段，生成安全多方计算需要的预处理参数，包括全局密钥、随机数等

加载二进制字节码并解析成一组安全多方计算指令集；

按照解析出的安全多方计算指令集依次调用底层接口执行安全多方计算协议流程，完成计算任务，输出计算结果。

6.根据权利要求1所述的一种安全多方计算方法，其特征在于，根据安全多方计算需求确定通用公式，具体包括：

提供一个模板公式库，且所述模板公式库包括多个模板公式；

获取当前安全多方计算环境，并提取多项环境需求元素；

基于每一项环境需求元素，将每个模板公式逐一与其它模板公式进行适配性比对，如果前者模板公式与该项环境需求元素的适配性优于其它模板公式，则将前者模板公式在该项环境需求元素的得分加1，反之，则得分不变；

待每个模板公式在所有项环境需求元素均完成与其它模板公式的比对后，统计每个模板公式在每项环境需求元素的总得分；

预设每项环境需求元素对模板公式选定的影响权重不同，将每个模板公式在每项环境需求元素的总得分分别乘以对应影响权重，并对乘积进行累加，得到每个模板公式的选取得分；

基于每个模板公式的选取得分进行模板公式库排序，并将选取得分最高的模板公式作为所述通用公式。

7.一种安全多方计算系统，其特征在于，包括存储器和处理器，所述存储器中包括一种安全多方计算方法程序，所述安全多方计算方法程序被所述处理器执行时实现如下步骤：

根据安全多方计算需求确定通用公式，并将所述通用公式以字符串形式传入公式编译器；

由所述公式编译器解析所述通用公式，并将其转化为通用安全多方计算框架可支持的计算公式；

将所述计算公式写入电路中，生成特定格式的电路文件，并将电路文件输入通用安全多方计算框架；

使用通用安全多方计算框架的电路编译器编译电路文件，并进行编译优化，生成二进制字节码；

调用安全多方计算协议运行电路编译出的二进制字节码，并输入计算数据；

按照安全多方计算协议执行对输入计算数据的计算处理，并输出最终的计算结果。

8.根据权利要求7所述的一种安全多方计算系统，其特征在于，由所述公式编译器解析所述通用公式，并将其转化为通用安全多方计算框架可支持的计算公式；将所述计算公式写入电路中，生成特定格式的电路文件，具体包括：

由所述公式编译器接收所述通用公式，并将所述通用公式格式化，转化为符合标准格式的通用公式；

由公式编译器根据后缀逆波兰表达式规则，将所述公式进行解析，表示为后缀表达式向量；

将通用安全多方计算框架支持的计算类型与通用公式符号进行匹配，构造计算符号映射表；

由公式编译器根据计算符号映射表将后缀表达式向量一次映射为通用安全多方计算框架可识别的计算公式；

将转化后的计算公式增加输入参数及依赖信息后，写入电路，生成特定格式的电路文件。

9.根据权利要求7所述的一种安全多方计算系统，其特征在于，使用通用安全多方计算框架的电路编译器编译电路文件，并进行编译优化，生成二进制字节码，具体包括：

对电路文件中的电路语句进行分析，通过翻译程序将电路语句翻译为单独的基本语法块；

按照电路文件内传入参数数据设置特定参数，所述特定参数包括精度值、线程数、安全参数中的一种或多种；

在每个单独的基本语法块内，使用通用安全多方计算框架的电路解析模块对部分指令进行优化处理，生成包括安全多方计算指令的类汇编指令集；

将类汇编指令集转码生成二进制字节码并写入文件中，生成字节码文件。

10.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质中包括一种安全多方计算方法程序，所述安全多方计算方法程序被处理器执行时，实现如权利要求1至6中任一项所述的一种安全多方计算方法的步骤。

一种安全多方计算方法、系统和计算机可读存储介质

技术领域

[0001] 本发明涉及数据处理技术领域，尤其涉及一种安全多方计算方法、系统和计算机可读存储介质。

背景技术

[0002] 安全多方计算旨在解决数据流通中的安全隐私问题，目前可大量应用于医疗、政务等场景，能够使各方在原始数据不泄漏的情况下，完成数据的协同计算，从而充分利用数据价值，支撑数据的安全流通和数据价值释放。

[0003] 安全多方计算源于姚期智提出的百万富翁问题，即两个百万富翁在不泄漏自己财富值的情况下比较谁更富有的问题，百万富翁问题或安全多方计算核心问题在于参与方都不想泄漏自己原始数据，也不信任任何第三方的情况下，安全地计算数据的结果。

[0004] 自姚期智提出安全多方计算问题以来，目前安全多方计算已发展超过40年时间，经历了理论研究阶段、实验研究阶段、应用探索阶段和规模化发展阶段。在2000年以前这20年左右时间主要是理论研究阶段，从2000到2009年，有一些项目使用安全多方计算技术在实际中应用，从2010年到2017年，国外的行业巨头开始尝试使用基于通用的安全多方计算技术在实际中解决隐私数据的计算问题。从2018年开始，国内相关行业也开始关注和尝试采用安全多方计算技术。

[0005] 安全多方计算虽然具有广泛的应用场景，但现阶段技术发展仍存在种种挑战，如性能瓶颈、易用性等，因此需要不断改进完善安全多方计算技术和应用。

[0006] 安全多方计算目前主要有两种主流方案，基于秘密共享和基于混淆电路的安全多方计算技术，基于秘密共享的安全多方计算主要采用线性秘密共享的方式实现安全多方计算，而基于基于混淆电路的安全多方计算技术，则采用混淆电路和不经意传输等密码技术。

[0007] 基于秘密共享的安全多方计算主要方式为使用线性秘密共享方案如Shamir秘密共享方案等对用户输入值进行分割，由多个参与方共同持有输入值的份额，并且在中间计算过程中，计算值都使用秘密份额参与计算，由于线性计算性质，使用各参与方计算值可恢复出最终计算结果，因此可以保护原始输入数据的安全性。

[0008] 基于混淆电路的安全多方计算主要适用于2方计算，发送方首先混淆电路将计算转化为布尔电路，并将每个门电路输入、输出结果进行加密，将加密结果发送给接收方，然后使用不经意传输技术传输对应的解密密钥，最终由接收方解密电路计算结果。混淆电路技术和不经意传输技术可保证发送方、接收方原始数据不泄漏。

[0009] 此外，还存在针对特性问题的安全多方计算技术，主要有隐私集合求交集，隐私信息检索，安全多方统计，保护隐私的数据挖掘等，但该方案不适合应用于一般场景，不属于通用解决方案。

[0010] 目前多数安全多方技术框架基于以上方案实现，主流两方安全多方计算框架包括EMP-toolkit，Obliv-C，ObliVM，TinyGarble，ABY等，主流三方及多方安全多方计算框架包括MP-SPDZ 、ABY3、SCALE-MAMBA、Sharemind MPC、Wysteria等框架。

[0011] 现有技术的通用安全多方计算框架通常存在以下问题：

(1)部分安全多方计算框架只支持两方或三方，不支持多方计算；

(2)目前各通用安全多方计算框架流程复杂，使用门槛较高，用户使用体验不友好；

(3)使用安全多方计算框架前，用户需要自主编写电路文件，对用户专业性要求高，使用方式不灵活。

发明内容

[0012] 为了解决上述至少一个技术问题，本发明提出了一种安全多方计算方法、系统和计算机可读存储介质，能够自动生成并转化公式，提高安全多方计算产品的易用性，降低用户使用门槛，提高安全多方计算框架的使用灵活性。

[0013] 本发明第一方面提出了一种安全多方计算方法，所述方法包括：

根据安全多方计算需求确定通用公式，并将所述通用公式以字符串形式传入公式编译器；

由所述公式编译器解析所述通用公式，并将其转化为通用安全多方计算框架可支持的计算公式；

将所述计算公式写入电路中，生成特定格式的电路文件，并将电路文件输入通用安全多方计算框架；

使用通用安全多方计算框架的电路编译器编译电路文件，并进行编译优化，生成二进制字节码；

调用安全多方计算协议运行电路编译出的二进制字节码，并输入计算数据；

按照安全多方计算协议执行对输入计算数据的计算处理，并输出最终的计算结果。

[0014] 本方案中，由所述公式编译器解析所述通用公式，并将其转化为通用安全多方计算框架可支持的计算公式；将所述计算公式写入电路中，生成特定格式的电路文件，具体包括：

由所述公式编译器接收所述通用公式，并将所述通用公式格式化，转化为符合标准格式的通用公式；

由公式编译器根据后缀逆波兰表达式规则，将所述公式进行解析，表示为后缀表达式向量；

将通用安全多方计算框架支持的计算类型与通用公式符号进行匹配，构造计算符号映射表；

由公式编译器根据计算符号映射表将后缀表达式向量一次映射为通用安全多方计算框架可识别的计算公式；

将转化后的计算公式增加输入参数及依赖信息后，写入电路，生成特定格式的电路文件。

[0015] 本方案中，使用通用安全多方计算框架的电路编译器编译电路文件，并进行编译优化，生成二进制字节码，具体包括：

对电路文件中的电路语句进行分析，通过翻译程序将电路语句翻译为单独的基本

语法块；

按照电路文件内传入参数数据设置特定参数，所述特定参数包括精度值、线程数、安全参数中的一种或多种；

在每个单独的基本语法块内，使用通用安全多方计算框架的电路解析模块对部分指令进行优化处理，生成包括安全多方计算指令的类汇编指令集；

将类汇编指令集转码生成二进制字节码并写入文件中，生成字节码文件。

[0016] 本方案中，在使用通用安全多方计算框架的电路解析模块对部分指令进行优化处理之后，所述方法还包括：

使用通用安全多方计算框架的电路解析模块对部分指令进行优化处理，并记录本次优化方式；

通过评价模型对优化后的类汇编指令集进行评价处理，输出评价结果；

将部分指令、本次优化方式以及评价结果进行打包，形成一项样本数据；

汇集每次使用通用安全多方计算框架的电路解析模块对部分指令进行优化处理得到的样本数据，并形成样本数据库；

基于样本数据库中的每项样本数据对电路解析模块进行训练，使得电路解析模块基于每项样本数据进行深度学习，以得到所述电路解析模块的最佳优化参数；

将所述最佳优化参数置入所述电路解析模块中，得到更新后的电路解析模块；

使用更新后的电路解析模块对后续解析过程中的指令进行优化处理。

[0017] 本方案中，调用安全多方计算协议运行电路编译出的二进制字节码，并输入计算数据；按照安全多方计算协议执行对输入计算数据的计算处理，并输出最终的计算结果，具体包括：

初始化安全多方计算协议参数，所述协议参数至少包括计算域大小、和安全参数大小；

进行预处理阶段，生成安全多方计算需要的预处理参数，包括全局密钥、随机数等

加载二进制字节码并解析成一组安全多方计算指令集；

按照解析出的安全多方计算指令集依次调用底层接口执行安全多方计算协议流程，完成计算任务，输出计算结果。

[0018] 本方案中，根据安全多方计算需求确定通用公式，具体包括：

提供一个模板公式库，且所述模板公式库包括多个模板公式；

获取当前安全多方计算环境，并提取多项环境需求元素；

基于每一项环境需求元素，将每个模板公式逐一与其它模板公式进行适配性比对，如果前者模板公式与该项环境需求元素的适配性优于其它模板公式，则将前者模板公式在该项环境需求元素的得分加1，反之，则得分不变；

待每个模板公式在所有项环境需求元素均完成与其它模板公式的比对后，统计每个模板公式在每项环境需求元素的总得分；

预设每项环境需求元素对模板公式选定的影响权重不同，将每个模板公式在每项环境需求元素的总得分分别乘以对应影响权重，并对乘积进行累加，得到每个模板公式的选取得分；

基于每个模板公式的选取得分进行模板公式库排序，并将选取得分最高的模板公

式作为所述通用公式。

[0019] 本发明第二方面还提出一种安全多方计算系统，包括存储器和处理器，所述存储器中包括一种安全多方计算方法程序，所述安全多方计算方法程序被所述处理器执行时实现如下步骤：

根据安全多方计算需求确定通用公式，并将所述通用公式以字符串形式传入公式编译器；

由所述公式编译器解析所述通用公式，并将其转化为通用安全多方计算框架可支持的计算公式；

将所述计算公式写入电路中，生成特定格式的电路文件，并将电路文件输入通用安全多方计算框架；

使用通用安全多方计算框架的电路编译器编译电路文件，并进行编译优化，生成二进制字节码；

调用安全多方计算协议运行电路编译出的二进制字节码，并输入计算数据；

按照安全多方计算协议执行对输入计算数据的计算处理，并输出最终的计算结果。

[0020] 本方案中，由所述公式编译器解析所述通用公式，并将其转化为通用安全多方计算框架可支持的计算公式；将所述计算公式写入电路中，生成特定格式的电路文件，具体包括：

由所述公式编译器接收所述通用公式，并将所述通用公式格式化，转化为符合标准格式的通用公式；

由公式编译器根据后缀逆波兰表达式规则，将所述公式进行解析，表示为后缀表达式向量；

将通用安全多方计算框架支持的计算类型与通用公式符号进行匹配，构造计算符号映射表；

由公式编译器根据计算符号映射表将后缀表达式向量一次映射为通用安全多方计算框架可识别的计算公式；

将转化后的计算公式增加输入参数及依赖信息后，写入电路，生成特定格式的电路文件。

[0021] 本方案中，使用通用安全多方计算框架的电路编译器编译电路文件，并进行编译优化，生成二进制字节码，具体包括：

对电路文件中的电路语句进行分析，通过翻译程序将电路语句翻译为单独的基本语法块；

按照电路文件内传入参数数据设置特定参数，所述特定参数包括精度值、线程数、安全参数中的一种或多种；

在每个单独的基本语法块内，使用通用安全多方计算框架的电路解析模块对部分指令进行优化处理，生成包括安全多方计算指令的类汇编指令集；

将类汇编指令集转码生成二进制字节码并写入文件中，生成字节码文件。

[0022] 本发明第三方面还提出一种计算机可读存储介质，所述计算机可读存储介质中包括一种安全多方计算方法程序，所述安全多方计算方法程序被处理器执行时，实现如上述

的一种安全多方计算方法的步骤。

[0023] 本发明提出的一种安全多方计算方法、系统和计算机可读存储介质，增加了公式编译器的环节，可以根据用户输入的通用公式，自动生成并转化为通用安全多方计算能够识别的计算公式，能够有效降低相关技术产品的使用难度和使用门槛；本发明能够通过自动化的脚本完成电路编译过程和执行过程，使用户对中间过程无感知，提高用户使用体验；本发明可以根据用户需求灵活实现计算公式的转化，具有通用性，使用更加灵活。

[0024] 本发明的附加方面和优点将在下面的描述部分中给出，部分将从下面的描述中变得明显，或通过本发明的实践了解到。

附图说明

[0025] 图1示出了本发明一种安全多方计算的整体方法流程图；

图2示出了本发明的公式编译流程图；

图3示出了本发明的电路编译流程图；

图4示出了本发明的安全多方计算流程图；

图5示出了本发明一种安全多方计算系统的框图。

具体实施方式

[0026] 为了能够更清楚地理解本发明的上述目的、特征和优点，下面结合附图和具体实施方式对本发明进行进一步的详细描述。需要说明的是，在不冲突的情况下，本申请的实施例及实施例中的特征可以相互组合。

[0027] 在下面的描述中阐述了很多具体细节以便于充分理解本发明，但是，本发明还可以采用其他不同于在此描述的其他方式来实施，因此，本发明的保护范围并不受下面公开的具体实施例的限制。

[0028] 图1示出了本发明一种安全多方计算方法的流程图。

[0029] 如图1所示，本发明第一方面提出一种安全多方计算方法，所述方法包括：

根据安全多方计算需求确定通用公式，并将所述通用公式以字符串形式传入公式编译器；

由所述公式编译器解析所述通用公式，并将其转化为通用安全多方计算框架可支持的计算公式；

将所述计算公式写入电路中，生成特定格式的电路文件，并将电路文件输入通用安全多方计算框架；

使用通用安全多方计算框架的电路编译器编译电路文件，并进行编译优化，生成二进制字节码；

调用安全多方计算协议运行电路编译出的二进制字节码，并输入计算数据；

按照安全多方计算协议执行对输入计算数据的计算处理，并输出最终的计算结果。

[0030] 可以理解，在使用通用安全多方计算框架的电路编译器编译电路文件时，所有参与方在编译过程中需要保证电路文件相同并且编译方式也需要保持一致。以确保多方计算的结果相同或相适配。所述安全多方计算协议为计算机可执行程序。

[0031] 优选的，上述通用安全多方计算框架可以为MP-SPDZ，但不限于此。

[0032] 根据本发明的具体实施例，根据安全多方计算需求确定通用公式，具体包括：

由用户根据安全多方计算需求直接输入或从模板公式库中选取的通用公式。

[0033] 本发明提出的安全多方计算方法，增加了公式编译器的环节，可以根据用户输入的通用公式，自动生成并转化为通用安全多方计算能够识别的计算公式，能够有效降低相关技术产品的使用难度和使用门槛；本发明能够通过自动化的脚本完成电路编译过程和执行过程，使用户对中间过程无感知，提高用户使用体验；本发明可以根据用户需求灵活实现计算公式的转化，具有通用性，使用更加灵活。

[0034] 根据本发明的实施例，由所述公式编译器解析所述通用公式，并将其转化为通用安全多方计算框架可支持的计算公式；将所述计算公式写入电路中，生成特定格式的电路文件，具体包括：

由所述公式编译器接收所述通用公式，并将所述通用公式格式化，转化为符合标准格式的通用公式；

由公式编译器根据后缀逆波兰表达式规则，将所述公式进行解析，表示为后缀表达式向量；

将通用安全多方计算框架支持的计算类型与通用公式符号进行匹配，构造计算符号映射表；

由公式编译器根据计算符号映射表将后缀表达式向量一次映射为通用安全多方计算框架可识别的计算公式；

将转化后的计算公式增加输入参数及依赖信息后，写入电路，生成特定格式的电路文件。

[0035] 为了进一步说明公式编译过程，下面以具体公式进行举例说明。

[0036] 公式编译过程主要通过公式编译器实现，公式编译器负责将用户输入的通用公式转化为通用安全多方计算框架能够识别的计算公式，并且生成特定格式的电路文件，具体过程如下：

(1)用户根据安全多方计算需求确定计算公式，并以字符串形式输入公式编译器中，假设需求场景为2方计算，计算公式为 $I_{0,1}+\sqrt{I_{1,1}}*2^{3.12}$，其中 $I_{0,1}$ 表示第一个计算方的第一个输入，$I_{1,1}$ 表示第二个计算方的第一个输入；

(2)公式编译器首先将上述公式格式化，转化为符合标准格式的通用公式，形如 $I0\_1+I1\_1\text{^}0.5*2\text{^}3.12$；

(3)公式编译器根据后缀表达式(逆波兰式)规则，将公式进行解析，表示为后缀表达式向量，形如 $\{I0\_1, I1\_1, 0.5, \text{^}, 2, 3.12, \text{^}, *, +\}$；

(4)将通用安全多方计算框架支持的计算类型(加、减、乘、除、指数运算等)与通用公式符号(+、-、*、/、^等)进行匹配，构造计算符号映射表，如下表1所示；

表1：

计算类型	通用公式符号
加法	+
减法	-
乘法	*
除法	/
指数运算	^
大于	>
小于	<
等于	==
大于等于	>=
小于等于	<=
逻辑与运算	&&

(5)公式编译器根据计算符号映射表将后缀表达式向量一次映射为通用安全多方计算框架可识别的计算公式,如对于MP-SPDZ安全多方计算框架,转化后计算公式为:

(I0_1+mpc_math.pow_fx(I1_1,sfix(0.5))*mpc_math.pow_fx(sfix(2),sfix(3.12)));

(6)将转化后的计算公式增加输入(如输入数据类型、精度、安全参数、线程数等)及依赖信息(如计算函数库等)后,写入电路,生成特定格式的电路文件,如对于MP-SPDZ安全多方计算框架,生成电路文件内容为:

```
from Compiler import mpc_math
program.use_edabit(True)
sfix.set_precision(16, 64)
loop = 1
n_threads = 1
@for_range_multithread(n_threads, None, loop)
def _(i):
    I0_0 = sfix.get_input_from(0)
    I1_0 = sfix.get_input_from(1)
    rlt = (I0_1+mpc_math.pow_fx(I1_1,sfix(0.5))*mpc_math.pow_fx(sfix(2),sfix(3.12)))
    print_ln("%s",rlt.reveal())。
```

[0037] 根据本发明的实施例,使用通用安全多方计算框架的电路编译器编译电路文件,并进行编译优化,生成二进制字节码,具体包括:

对电路文件中的电路语句进行分析,通过翻译程序将电路语句翻译为单独的基本语法块;

按照电路文件内传入参数数据设置特定参数,所述特定参数包括精度值、线程数、安全参数中的一种或多种;

在每个单独的基本语法块内,使用通用安全多方计算框架的电路解析模块对部分

指令进行优化处理，生成包括安全多方计算指令的类汇编指令集；

将类汇编指令集转码生成二进制字节码并写入文件中，生成字节码文件。

[0038] 优选的，上述优化处理方式包括减少循环次数，使用多线程、并行计算指令、以及多个指令的合并等。

[0039] 优选的，所述电路翻译程序可以开源框架MP-SPDZ电路翻译程序，但不限于此。

[0040] 根据本发明的实施例，在使用通用安全多方计算框架的电路解析模块对部分指令进行优化处理之后，所述方法还包括：

使用通用安全多方计算框架的电路解析模块对部分指令进行优化处理，并记录本次优化方式；

通过评价模型对优化后的类汇编指令集进行评价处理，输出评价结果；

将部分指令、本次优化方式以及评价结果进行打包，形成一项样本数据；

汇集每次使用通用安全多方计算框架的电路解析模块对部分指令进行优化处理得到的样本数据，并形成样本数据库；

基于样本数据库中的每项样本数据对电路解析模块进行训练，使得电路解析模块基于每项样本数据进行深度学习，以得到所述电路解析模块的最佳优化参数；

将所述最佳优化参数置入所述电路解析模块中，得到更新后的电路解析模块；

使用更新后的电路解析模块对后续解析过程中的指令进行优化处理。

[0041] 需要说明的是，电路解析模块可以对单独的基本语法块内的部分指令进行优化，具体优化方式如减少循环次数，使用多线程、并行计算指令、以及多个指令的合并等。然而，根据部分指令的多样性，需要选择恰当的优化方式，一旦选择不恰当的优化方式，则容易导致优化结果不佳，进而不利于后续安全多方计算，降低了安全多方计算的效率。本发明通过采用评价模型对每次优化结果进行评价，并基于评价结果对电路解析模块的优化参数进行更新，以此得到最佳优化参数，基于最佳优化参数进一步更新电路解析模块，从而使得更新后的电路解析模块实现对指令合理优化，提升了指令优化效果，提高了安全多方计算的效率。

[0042] 根据本发明的具体实施例，基于样本数据库中的每项样本数据对电路解析模块进行训练，使得电路解析模块基于每项样本数据进行深度学习，以得到所述电路解析模块的最佳优化参数，具体包括：

如果评价结果较好，则表示本次优化方式合理，则基于对应的样本数据进行正向深度学习，如果评价效果不好，则表示本次优化方式不合理，则基于对应的样本数据进行反向深度学习。

[0043] 可以理解，所谓的正向深度学习是吸取本次好的优化经验，所谓的反向深度学习是吸取本次不好的优化经验。

[0044] 根据本发明的具体实施例，通过评价模型对优化后的类汇编指令集进行评价处理，输出评价结果，具体包括：

获取对应的安全多方计算效率和计算冗余度；

由所述评价模型基于计算效率和计算冗余度，并采用预设评价算法对优化后的类汇编指令集进行评价。

[0045] 根据本发明的具体实施例，采用预设评价算法对优化后的类汇编指令集进行评

价,具体包括:

预设计算效率等级转置表和计算冗余度等级转置表,将计算效率和计算冗余度分别通过计算效率等级转置表和计算冗余度等级转置表进行转置,得到对应的计算效率等级和计算冗余度等级;

预设计算效率对评价结果的影响权重A和计算冗余度对评价结果的影响权重B;

将计算效率等级乘以影响权重A,计算冗余度等级乘以影响权重B,并对乘积进行累加,得到评价值;

基于所述评价值,并通过查询评价表获取对应的评价结果。

[0046] 根据本发明的实施例,调用安全多方计算协议运行电路编译出的二进制字节码,并输入计算数据;按照安全多方计算协议执行对输入计算数据的计算处理,并输出最终的计算结果,具体包括:

初始化安全多方计算协议参数,所述协议参数至少包括计算域大小、和安全参数大小;

进行预处理阶段,生成安全多方计算需要的预处理参数,包括全局密钥、随机数等

加载二进制字节码并解析成一组安全多方计算指令集;

按照解析出的安全多方计算指令集依次调用底层接口执行安全多方计算协议流程,完成计算任务,输出计算结果。

[0047] 优选的,计算域大小为128bit,安全参数为40bit。但不限于此。

[0048] 根据本发明的实施例,根据安全多方计算需求确定通用公式,具体包括:

提供一个模板公式库,且所述模板公式库包括多个模板公式;

获取当前安全多方计算环境,并提取多项环境需求元素;

基于每一项环境需求元素,将每个模板公式逐一与其它模板公式进行适配性比对,如果前者模板公式与该项环境需求元素的适配性优于其它模板公式,则将前者模板公式在该项环境需求元素的得分加1,反之,则得分不变;

待每个模板公式在所有项环境需求元素均完成与其它模板公式的比对后,统计每个模板公式在每项环境需求元素的总得分;

预设每项环境需求元素对模板公式选定的影响权重不同,将每个模板公式在每项环境需求元素的总得分分别乘以对应影响权重,并对乘积进行累加,得到每个模板公式的选取得分;

基于每个模板公式的选取得分进行模板公式库排序,并将选取得分最高的模板公式作为所述通用公式。

[0049] 可以理解,所述环境需求元素可以包括安全级别、参与方数量等。例如有的多方计算环境需要的安全级别较高,则适配的公式复杂程度也将提高。有点多方计算环境的参与方数量较多,则适配的公式变量也将增多。

[0050] 本发明通过提供模板公式库,并结合当前环境需求选定适配的模板公式作为通用公式,无需用户自己编写公式,大大降低用户使用门槛,提高安全多方计算框架的使用灵活性。

[0051] 根据本发明的具体实施例,所述方法还包括:

在通用安全多方计算框架的电路上设置电压预警模块;

由电压预警模块实时监测电压值，当电压预警模块感测到电压值高于预设阈值时，则记录处理节点的中间数据，以对各个处理节点的中间数据进行掉电保护。

[0052] 可以理解，在进行安全多方计算过程中，一旦出现掉电等突发状况，则可能导致中间部分数据丢失，当上电后，则将会重新进行计算，从而影响计算效率，本发明通过电压预警模块进行实时监测电压值，一旦发现异常，则进行报各个处理节点保存中间数据，便于后续上电后继续基于保护的中间数据进行处理，避免数据丢失的可能性，提高了安全多方计算效率。

[0053] 根据本发明的具体实施例，由电压预警模块实时监测电压值，具体包括：

预设检测时间窗的初始长度和扩大步长，并将初始的检测时间窗左边缘与开始安全多方计算的时刻对齐；

对检测时间窗内的电压数据进行极大重叠离散小波变换处理，得到离散小波变换系数曲线，并基于离散小波变换系数曲线获取所述检测时间窗内各个采样点的离散小波变换系数值；

分别计算所述检测时间窗内相邻两个采样点之间的离散小波变换系数差值的绝对值；

通过对比多个离散小波变换系数差值的绝对值，找出最大的离散小波变换系数差值的绝对值；

以最大的离散小波变换系数差值的绝对值为基准分别选择周围预设数量的其它离散小波变换系数差值的绝对值，并计算最大的离散小波变换系数差值的绝对值与其它离散小波变换系数差值的绝对值的平均值，然后将所述平均值作为预设阈值；

将所述检测时间窗内相邻两个采样点之间的离散小波变换系数差值的绝对值逐个与所述预设阈值进行比较，判断是否超过所述预设阈值；

如果超过，则记录当前的时间节点，如果未超过，则将所述检测时间窗按照预设的扩大步长进行扩充，并基于扩充后的检测时间窗重新计算最大的离散小波变换系数差值的绝对值以及对应的平均值。

[0054] 图5示出了本发明一种安全多方计算系统的框图。

[0055] 如图5所示，本发明第二方面还提出一种安全多方计算系统5，包括存储器51和处理器52，所述存储器中包括一种安全多方计算方法程序，所述安全多方计算方法程序被所述处理器执行时实现如下步骤：

根据安全多方计算需求确定通用公式，并将所述通用公式以字符串形式传入公式编译器；

由所述公式编译器解析所述通用公式，并将其转化为通用安全多方计算框架可支持的计算公式；

将所述计算公式写入电路中，生成特定格式的电路文件，并将电路文件输入通用安全多方计算框架；

使用通用安全多方计算框架的电路编译器编译电路文件，并进行编译优化，生成二进制字节码；

调用安全多方计算协议运行电路编译出的二进制字节码，并输入计算数据；

按照安全多方计算协议执行对输入计算数据的计算处理，并输出最终的计算结

果。

[0056] 根据本发明的实施例，由所述公式编译器解析所述通用公式，并将其转化为通用安全多方计算框架可支持的计算公式；将所述计算公式写入电路中，生成特定格式的电路文件，具体包括：

由所述公式编译器接收所述通用公式，并将所述通用公式格式化，转化为符合标准格式的通用公式；

由公式编译器根据后缀逆波兰表达式规则，将所述公式进行解析，表示为后缀表达式向量；

将通用安全多方计算框架支持的计算类型与通用公式符号进行匹配，构造计算符号映射表；

由公式编译器根据计算符号映射表将后缀表达式向量一次映射为通用安全多方计算框架可识别的计算公式；

将转化后的计算公式增加输入参数及依赖信息后，写入电路，生成特定格式的电路文件。

[0057] 根据本发明的实施例，使用通用安全多方计算框架的电路编译器编译电路文件，并进行编译优化，生成二进制字节码，具体包括：

对电路文件中的电路语句进行分析，通过翻译程序将电路语句翻译为单独的基本语法块；

按照电路文件内传入参数数据设置特定参数，所述特定参数包括精度值、线程数、安全参数中的一种或多种；

在每个单独的基本语法块内，使用通用安全多方计算框架的电路解析模块对部分指令进行优化处理，生成包括安全多方计算指令的类汇编指令集；

将类汇编指令集转码生成二进制字节码并写入文件中，生成字节码文件。

[0058] 本发明第三方面还提出一种计算机可读存储介质，所述计算机可读存储介质中包括一种安全多方计算方法程序，所述安全多方计算方法程序被处理器执行时，实现如上述的一种安全多方计算方法的步骤。

[0059] 本发明提出的一种安全多方计算方法、系统和计算机可读存储介质，通过设计一种基于后缀表达式的公式编译器，能自动将普通公式转化为通用安全多方计算框架可识别的计算公式，并转化生成特定的计算电路文件，然后通过电路编译器自动编译电路文件，生成二进制字节码，最后通过执行安全多方计算协议完成计算过程，输出结果。

[0060] 与现有安全多方计算方案相比，本发明增加了公式编译器的环节，可以根据用户输入的通用公式，自动生成并转化为通用安全多方计算能够识别的计算公式，能够有效降低相关技术产品的使用难度和使用门槛；本发明能够通过自动化的脚本完成电路编译过程和执行过程，使用户对中间过程无感知，提高用户使用体验；本发明可以根据用户需求灵活实现计算公式的转化，具有通用性，使用更加灵活。

[0061] 在本申请所提供的几个实施例中，应该理解到，所揭露的设备和方法，可以通过其它的方式实现。以上所描述的设备实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，如：多个单元或组件可以结合，或可以集成到另一个系统，或一些特征可以忽略，或不执行。另外，所显示或讨论的各组成部

分相互之间的耦合、或直接耦合、或通信连接可以是通过一些接口，设备或单元的间接耦合或通信连接，可以是电性的、机械的或其它形式的。

[0062] 上述作为分离部件说明的单元可以是、或也可以不是物理上分开的，作为单元显示的部件可以是、或也可以不是物理单元；既可以位于一个地方，也可以分布到多个网络单元上；可以根据实际的需要选择其中的部分或全部单元来实现本实施例方案的目的。

[0063] 另外，在本发明各实施例中的各功能单元可以全部集成在一个处理单元中，也可以是各单元分别单独作为一个单元，也可以两个或两个以上单元集成在一个单元中；上述集成的单元既可以采用硬件的形式实现，也可以采用硬件加软件功能单元的形式实现。

[0064] 本领域普通技术人员可以理解：实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成，前述的程序可以存储于计算机可读取存储介质中，该程序在执行时，执行包括上述方法实施例的步骤；而前述的存储介质包括：移动存储设备、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0065] 或者，本发明上述集成的单元如果以软件功能模块的形式实现并作为独立的产品销售或使用时，也可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明实施例的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备(可以是个人计算机、服务器、或者网络设备等)执行本发明各个实施例所述方法的全部或部分。而前述的存储介质包括：移动存储设备、ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0066] 以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应以所述权利要求的保护范围为准。

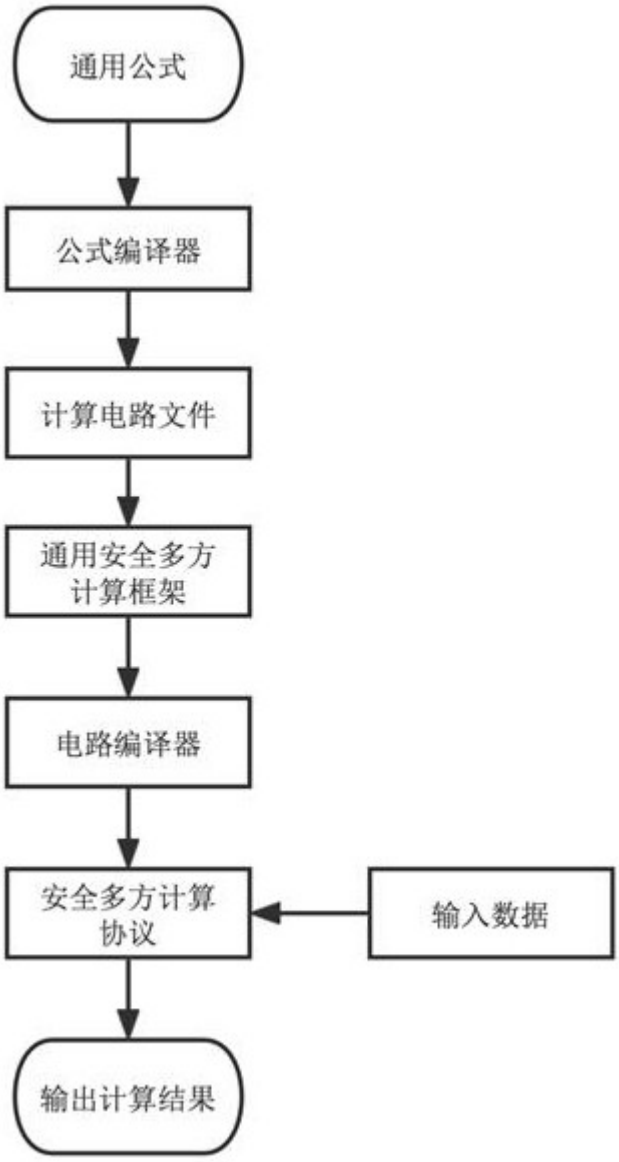


图1

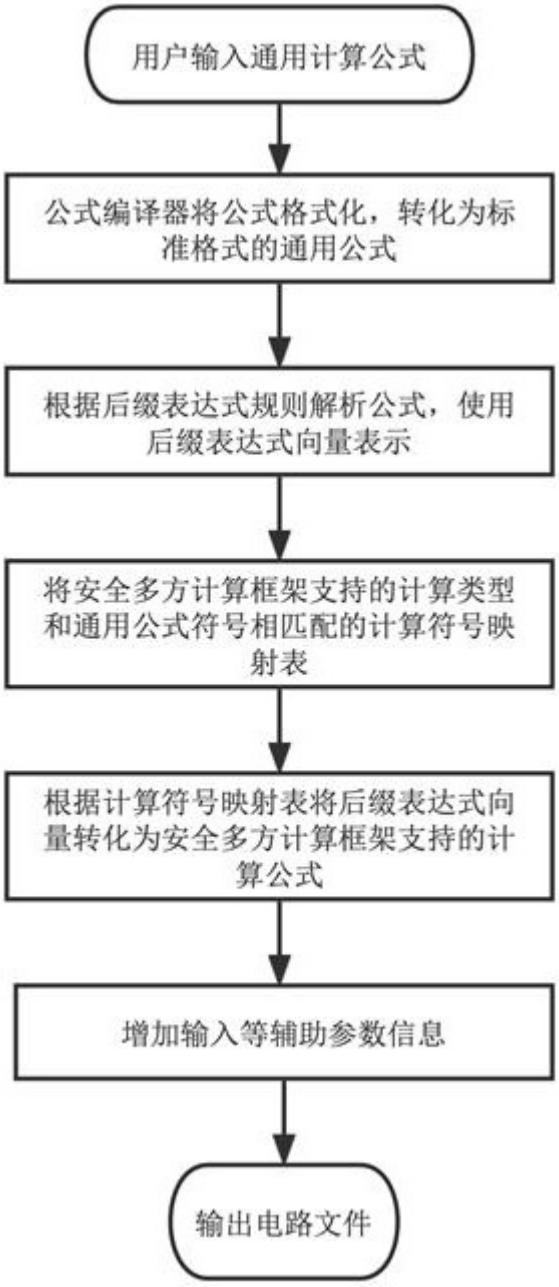

用户输入通用计算公式
公式编译器将公式格式化，转化为标准格式的通用公式
根据后缀表达式规则解析公式，使用后缀表达式向量表示
将安全多方计算框架支持的计算类型和通用公式符号相匹配的计算符号映射表
根据计算符号映射表将后缀表达式向量转化为安全多方计算框架支持的计算公式
增加输入等辅助参数信息
输出电路文件

图2

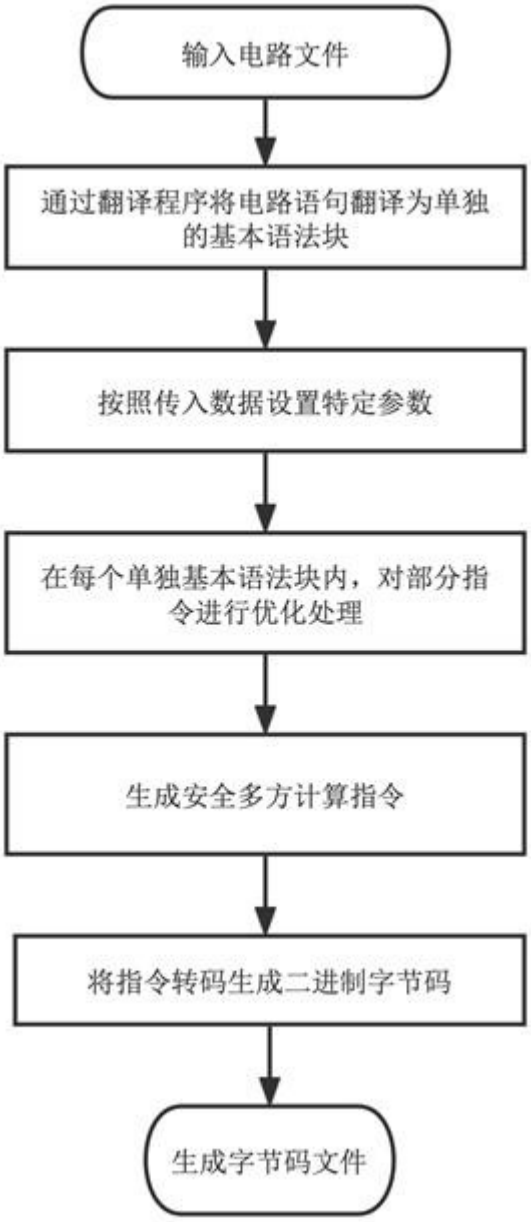

输入电路文件
通过翻译程序将电路语句翻译为单独的基本语法块
按照传入数据设置特定参数
在每个单独基本语法块内，对部分指令进行优化处理
生成安全多方计算指令
将指令转码生成二进制字节码
生成字节码文件

图3

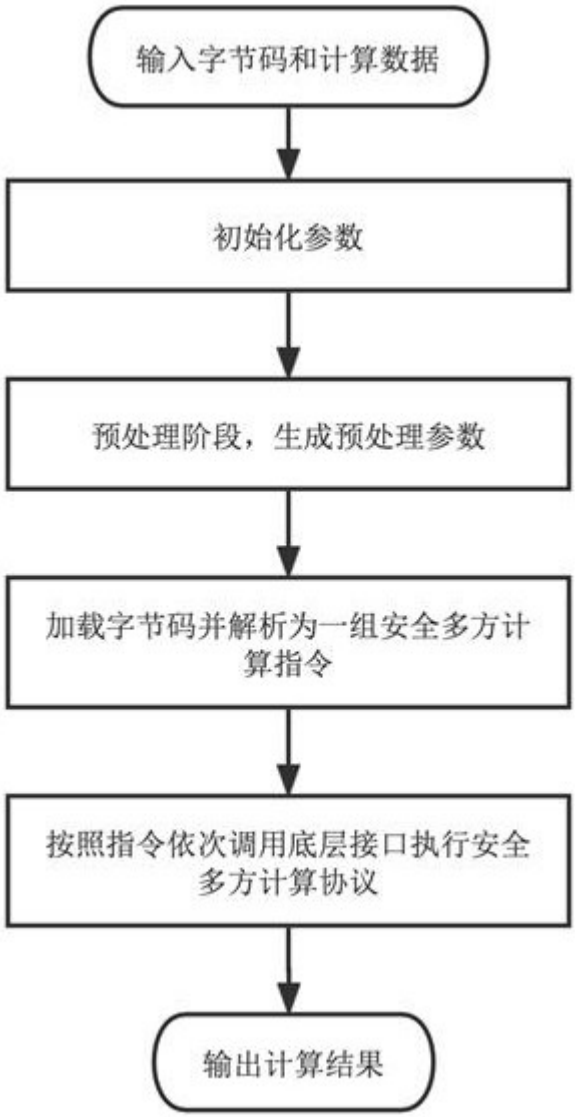

输入字节码和计算数据
初始化参数
预处理阶段，生成预处理参数
加载字节码并解析为一组安全多方计算指令
按照指令依次调用底层接口执行安全多方计算协议
输出计算结果

图4

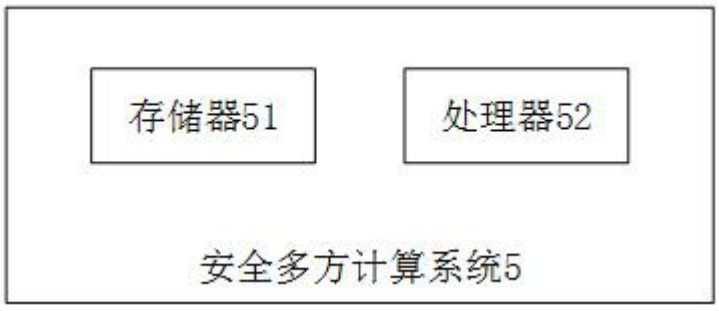

存储器51
处理器52
安全多方计算系统5

图5