(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 116846535 A
(43)申请公布日 2023.10.03

(21)申请号 202310864942.3

(22)申请日 2023.07.13

(71)申请人 北京航空航天大学
地址 100191 北京市海淀区学院路37号

(72)发明人 关振宇 边松 潘豪文 金意儿 张舟

(74)专利代理机构 北京清亦华知识产权代理事务所(普通合伙) 11201
专利代理师 孙凯

(51)Int.Cl.
H04L 9/00(2022.01)
G06F 21/60(2013.01)
G06F 21/62(2013.01)

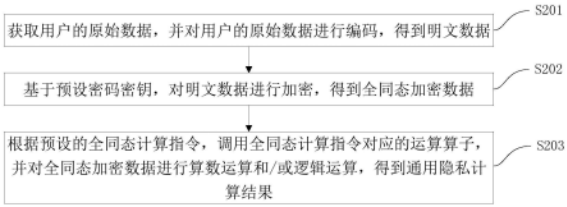
权利要求书2页 说明书9页 附图2页

(54)发明名称

基于全同态加密的通用隐私计算方法、装置、设备及介质

(57)摘要

本申请涉及一种基于全同态加密的通用隐私计算方法、装置、设备及介质，其中，方法包括：获取用户的原始数据，并对用户的原始数据进行编码，得到明文数据；基于预设密码密钥，对明文数据进行加密，得到全同态加密数据；根据预设的全同态计算指令，调用全同态计算指令对应的运算算子，并对全同态加密数据进行算术运算和/或逻辑运算，得到通用隐私计算结果。由此，解决了现有的基于全同态加密的隐私计算框架均与具体的加密方案相关，通用性较差，新的算法难以进行拓展，无法实现不同计算方式的融合等问题。



CN 116846535 A

1.一种基于全同态加密的通用隐私计算方法,其特征在于,包括以下步骤:

获取用户的原始数据,并对所述用户的原始数据进行编码,得到明文数据;

基于预设密码密钥,对所述明文数据进行加密,得到全同态加密数据;

根据预设的全同态计算指令,调用所述全同态计算指令对应的运算算子,并对所述全同态加密数据进行算术运算和/或逻辑运算,得到通用隐私计算结果。

2.根据权利要求1所述的方法,其特征在于,所述对所述用户的原始数据进行编码,得到明文数据,包括:

通过SISD编码、SIMD-Slot编码或SIMD-Coeff编码的方式对所述原始数据进行编码,得到满足预设代数结构的所述明文数据。

3.根据权利要求2所述的方法,其特征在于,所述基于预设密码密钥,对所述明文数据进行加密,得到全同态加密数据,包括:

基于预设明文/密文转换算子,通过LWE加密、RLWE加密、MLWE加密或RGSW加密的方法对所述明文数据进行加密,得到所述全同态加密数据。

4.根据权利要求1所述的方法,其特征在于,所述根据预设的全同态计算指令,调用所述全同态计算指令对应的运算算子,并对所述全同态加密数据进行算术运算和/或逻辑运算,得到通用隐私计算结果,包括:

基于预设全同态算术运算算子,对所述全同态加密数据进行算术运算;

基于预设全同态逻辑运算算子,对所述全同态加密数据进行逻辑运算。

5.根据权利要求1所述的方法,其特征在于,所述对所述全同态加密数据进行算术运算和/或逻辑运算,包括:

利用数学基础库对所述全同态加密数据进行算术运算和/或逻辑运算,其中,所述数学基础库包括整数代数结构、多项式代数结构、数论变换以及剩余数系统中的至少一项。

6.一种基于全同态加密的通用隐私计算装置,其特征在于,包括:

编码模块,用于获取用户的原始数据,并对所述用户的原始数据进行编码,得到明文数据;

加密模块,用于基于预设密码密钥,对所述明文数据进行加密,得到全同态加密数据;

计算模块,用于根据预设的全同态计算指令,调用所述全同态计算指令对应的运算算子,并对所述全同态加密数据进行算术运算和/或逻辑运算,得到通用隐私计算结果。

7.根据权利要求6所述的装置,其特征在于,所述编码模块具体用于,

通过SISD编码、SIMD-Slot编码或SIMD-Coeff编码的方式对所述原始数据进行编码,得到满足预设代数结构的所述明文数据。

8.根据权利要求7所述的装置,其特征在于,所述加密模块具体用于,

基于预设明文/密文转换算子,通过LWE加密、RLWE加密、MLWE加密或RGSW加密的方法对所述明文数据进行加密,得到所述全同态加密数据。

9.根据权利要求6所述的装置,其特征在于,所述计算模块包括:

第一运算单元,用于基于预设全同态算术运算算子,对所述全同态加密数据进行算术运算;

第二运算单元,用于基于预设全同态逻辑运算算子,对所述全同态加密数据进行逻辑运算。

10.根据权利要求6所述的装置,其特征在于,所述计算模块还包括:

调用单元,用于利用数学基础库对所述全同态加密数据进行算术运算和/或逻辑运算,其中,所述数学基础库包括整数代数结构、多项式代数结构、数论变换以及剩余数系统中的至少一项。

11.一种电子设备,其特征在于,包括:存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序,所述处理器执行所述程序,以实现如权利要求1-5任一项所述的基于全同态加密的通用隐私计算方法。

12.一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,该程序被处理器执行,以用于实现如权利要求1-5任一项所述的基于全同态加密的通用隐私计算方法。

基于全同态加密的通用隐私计算方法、装置、设备及介质

技术领域

[0001] 本申请涉及信息安全技术领域，特别涉及一种基于全同态加密的通用隐私计算方法、装置、设备及介质。

背景技术

[0002] 随着以区块链、5G、物联网、云计算、人工智能等为代表的新一代信息技术与国民日常生活的深度融合，大量的个人数据被采集、加工、处理、流转。针对数据隐私保护的旺盛需求，围绕隐私计算的相关研究以逐步形成，例如，在机器学习领域中的联邦学习技术、传统安全与密码学领域中的多方安全计算与同态加密技术、芯片设计领域中的可信执行环境等技术方案都被视为隐私计算技术。

[0003] 然而，由于不同种类的隐私计算技术各自拥有不同的安全定义、安全等级以及计算效率，且隐私计算领域本身仍处于高速发展、技术迭代的阶段，多种多样的隐私计算技术使得学术界、不同应用行业与政府标准化部门之间缺乏针对隐私保护技术方案的统一共识，导致单一隐私计算技术无法简单泛用至不同的隐私保护场景，形成该现象的主要原因则是拥有可证明安全性的隐私计算协议面临着极大的计算与通信带宽开销；例如，在最新的顶级会议成果中，基于传统多方安全计算的隐私神经网络推理协议需要9Gbytes以上的广域网通信带宽完成一轮推理计算(明文的本地推理计算不需要任何通信)；而基于全同态加密的隐私神经网络推理虽仅需极少通信带宽(数百Kbytes)，计算时间却比明文推理慢1000倍以上。

[0004] 综上，不同种类的隐私计算方案分别存在单一协议泛用性差、通信轮数多、带宽传输高、计算时间长等科学难题，造成使用者对隐私计算技术缺乏理解与信心，极大地阻碍了先进隐私计算方案在产业中的实际落地。

[0005] 因此，基于格的同态加密计算技术作为一种隐私计算方案快速发展。在全同态加密算法中，拥有隐私数据的数据所有方将数据加密后传输给计算方；计算方可在加密后的密文上直接执行任意图灵完备的计算机语言，且在这一过程中不需要与数据所有方进行任何交互，进而保护数据所有方的数据安全。

[0006] 随着全同态加密技术的快速发展，越来越多的算法在全同态加密方案上进行设计。然而，由于目前的基于全同态加密的隐私计算框架均与具体的加密方案相关，通用性较差，导致新的算法难以在原有方案上进行拓展，无法实现不同计算方式的融合，亟待解决。

发明内容

[0007] 本申请提供一种基于全同态加密的通用隐私计算方法、装置、设备及介质，以解决现有的基于全同态加密的隐私计算框架均与具体的加密方案相关，通用性较差，新的算法难以进行拓展，无法实现不同计算方式的融合等问题。

[0008] 本申请第一方面实施例提供一种基于全同态加密的通用隐私计算方法，包括以下步骤：获取用户的原始数据，并对所述用户的原始数据进行编码，得到明文数据；基于预设

密码密钥,对所述明文数据进行加密,得到全同态加密数据;根据预设的全同态计算指令,调用所述全同态计算指令对应的运算算子,并对所述全同态加密数据进行算术运算和/或逻辑运算,得到通用隐私计算结果。

[0009] 可选地,在本申请的一个实施例中,所述对所述用户的原始数据进行编码,得到明文数据,包括:通过SISD编码、SIMD-Slot编码或SIMD-Coeff编码的方式对所述原始数据进行编码,得到满足预设代数结构的所述明文数据。

[0010] 可选地,在本申请的一个实施例中,所述基于预设密码密钥,对所述明文数据进行加密,得到全同态加密数据,包括:基于预设明文/密文转换算子,通过LWE加密、RLWE加密、MLWE加密或RGSW加密的方法对所述明文数据进行加密,得到所述全同态加密数据。

[0011] 可选地,在本申请的一个实施例中,所述根据预设的全同态计算指令,调用所述全同态计算指令对应的运算算子,并对所述全同态加密数据进行算术运算和/或逻辑运算,得到通用隐私计算结果,包括:基于预设全同态算术运算算子,对所述全同态加密数据进行算术运算;基于预设全同态逻辑运算算子,对所述全同态加密数据进行逻辑运算。

[0012] 可选地,在本申请的一个实施例中,所述对所述全同态加密数据进行算术运算和/或逻辑运算,包括:利用数学基础库对所述全同态加密数据进行算术运算和/或逻辑运算,其中,所述数学基础库包括整数代数结构、多项式代数结构、数论变换以及剩余数系统中的至少一项。

[0013] 本申请第二方面实施例提供一种基于全同态加密的通用隐私计算装置,包括:编码模块,用于获取用户的原始数据,并对所述用户的原始数据进行编码,得到明文数据;加密模块,用于基于预设密码密钥,对所述明文数据进行加密,得到全同态加密数据;计算模块,用于根据预设的全同态计算指令,调用所述全同态计算指令对应的运算算子,并对所述全同态加密数据进行算术运算和/或逻辑运算,得到通用隐私计算结果。

[0014] 可选地,在本申请的一个实施例中,所述编码模块具体用于,通过SISD编码、SIMD-Slot编码或SIMD-Coeff编码的方式对所述原始数据进行编码,得到满足预设代数结构的所述明文数据。

[0015] 可选地,在本申请的一个实施例中,所述加密模块具体用于,基于预设明文/密文转换算子,通过LWE加密、RLWE加密、MLWE加密或RGSW加密的方法对所述明文数据进行加密,得到所述全同态加密数据。

[0016] 可选地,在本申请的一个实施例中,所述计算模块包括:第一运算单元,用于基于预设全同态算术运算算子,对所述全同态加密数据进行算术运算;第二运算单元,用于基于预设全同态逻辑运算算子,对所述全同态加密数据进行逻辑运算。

[0017] 可选地,在本申请的一个实施例中,所述计算模块还包括:调用单元,用于利用数学基础库对所述全同态加密数据进行算术运算和/或逻辑运算,其中,所述数学基础库包括整数代数结构、多项式代数结构、数论变换以及剩余数系统中的至少一项。

[0018] 本申请第三方面实施例提供一种电子设备,包括:存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序,所述处理器执行所述程序,以实现如上述实施例所述的基于全同态加密的通用隐私计算方法。

[0019] 本申请第四方面实施例提供一种计算机可读存储介质,所述计算机可读存储介质存储计算机程序,该程序被处理器执行时实现如上的基于全同态加密的通用隐私计算方

法。

[0020] 由此,本申请的实施例具有以下有益效果:

[0021] 本申请的实施例可通过获取用户的原始数据,并对用户的原始数据进行编码,得到明文数据;基于预设密码密钥,对明文数据进行加密,得到全同态加密数据;根据预设的全同态计算指令,调用全同态计算指令对应的运算算子,并对全同态加密数据进行算术运算和/或逻辑运算,得到通用隐私计算结果,从而消除了不同全同态加密方案间的壁垒,能够有效完成全同态加密中算术运算和逻辑运算混合的复杂计算任务,并且易于拓展新指令和实现硬件加速。由此,解决了现有的基于全同态加密的隐私计算框架均与具体的加密方案相关,通用性较差,新的算法难以进行拓展,无法实现不同计算方式的融合等问题。

[0022] 本申请附加的方面和优点将在下面的描述中部分给出,部分将从下面的描述中变得明显,或通过本申请的实践了解到。

附图说明

[0023] 本申请上述的和/或附加的方面和优点从下面结合附图对实施例的描述中将变得明显和容易理解,其中:

[0024] 图1为本申请的一种基于全同态加密的通用隐私计算方法的逻辑架构示意图;

[0025] 图2为根据本申请实施例提供的一种基于全同态加密的通用隐私计算方法的流程图;

[0026] 图3为本申请的一个实施例提供的一种密码运算库的计算过程示意图;

[0027] 图4为根据本申请实施例的基于全同态加密的通用隐私计算装置的示例图;

[0028] 图5为本申请实施例提供的电子设备的结构示意图。

[0029] 其中,10-基于全同态加密的通用隐私计算装置、100-编码模块、200-加密模块、300-计算模块、501-存储器、502-处理器、503-通信接口。

具体实施方式

[0030] 下面详细描述本申请的实施例,所述实施例的示例在附图中示出,其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的,旨在用于解释本申请,而不能理解为对本申请的限制。

[0031] 下面参考附图描述本申请实施例的基于全同态加密的通用隐私计算方法、装置、设备及介质。针对上述背景技术中提到的现有基于全同态加密的隐私计算框架存在的通用性较差等问题,本申请提供了一种基于全同态加密的通用隐私计算方法,在该方法中,通过获取用户的原始数据,并对用户的原始数据进行编码,得到明文数据;基于预设密码密钥,对明文数据进行加密,得到全同态加密数据;根据预设的全同态计算指令,调用全同态计算指令对应的运算算子,并对全同态加密数据进行算术运算和/或逻辑运算,得到通用隐私计算结果,从而消除了不同全同态加密方案间的壁垒,能够有效完成全同态加密中算术运算和逻辑运算混合的复杂计算任务,并且易于拓展新指令和实现硬件加速。由此,解决了现有的基于全同态加密的隐私计算框架均与具体的加密方案相关,通用性较差,新的算法难以进行拓展,无法实现不同计算方式的融合等问题。

[0032] 为了便于本领域技术人员对本申请的一种基于全同态加密的通用隐私计算方法

的理解，下述对本申请的逻辑架构进行简要说明。

[0033] 本申请的基于全同态加密的通用隐私计算方法的逻辑框架主要包括：数学基础库、数据类型库、密码运算库以及计算指令库四个部分，如图1所示。其中数学基础库为整个计算架构提供底层数学结构和数学运算支持；数据类型库定义了计算过程中涉及的不同数据类型，包括原始数据、明文数据、密码密钥、密文数据和运算密钥；密码运算库定义了各类全同态密码基础算法和算子，为计算指令模块中的各类运算指令提供支持；计算指令库则实现了多种同态指令运算算子，通过调用密码运算库和数据类型库的相应元素，完成对应计算指令。

[0034] 具体而言，图2为本申请实施例所提供的一种基于全同态加密的通用隐私计算方法的流程图。

[0035] 如图2所示，该基于全同态加密的通用隐私计算方法包括以下步骤：

[0036] 在步骤S201中，获取用户的原始数据，并对用户的原始数据进行编码，得到明文数据。

[0037] 在本申请的实施例中，首先可获取预设数据类型库中用户的原始数据，例如32比特整数、浮点数向量或矩阵等，并通过计算指令库从密码运算库调用编码运算的密码运算方式对该原始数据进行编码，以得到用户原始数据对应的明文数据。其中，数据类型库定义了计算过程中涉及的不同数据类型，为编译器和其他库提供了相应的数据类型支持，能够根据编译器和其他库的需要提供相应的数据类型，使得计算过程更加灵活；原始数据即为实际应用中产生的未经加密的真实数据类型；明文数据为同态加密方案中已进行加密未经加密的数据，在基于LWE的同态方案中，明文数据是整数，而在基于RLWE的同态方案中，明文数据是一个多项式。

[0038] 本领域技术人员可以理解的是，编码在全同态加密方案中具备重要地位，编码方式可以很大程度上决定全同态加密方案的形式，不同的全同态加密方案(例如CKKS和BFV)的关键区别即为其编码方式不同，对于不同的原始数据类型，密码运算库可将原始数据编码为不同的明文数据类型。

[0039] 可选地，在本申请的一个实施例中，对用户的原始数据进行编码，得到明文数据，包括：通过SISD编码、SIMD-Slot编码或SIMD-Coeff编码的方式对原始数据进行编码，得到满足预设代数结构的明文数据。

[0040] 需要说明的是，本申请的实施例可通过SISD编码、SIMD-Slot编码或SIMD-Coeff编码等方式对原始数据进行编码，以得到满足一定的代数结构的明文数据，例如得到的整数明文数据需要在某一个剩余类中，而向量明文数据则需在某一环中。

[0041] 由此，本申请的实施例通过获取明文数据，从而为后续密文数据的获取提供可靠的数据支撑。

[0042] 在步骤S202中，基于预设密码密钥，对明文数据进行加密，得到全同态加密数据。

[0043] 在获取明文数据后，进一步地，本申请的实施例还可通过计算指令库从密码运算库调用加密运算的密码运算方式，利用数据类型库中的密码密钥对所获取的明文数据进行加密处理，从而得到数据类型库中密文数据。

[0044] 其中，密码密钥即为将明文数据加密为密文数据的密钥，包括对称密码密钥和非对称密码密钥；密文数据为同态加密方案中加密后的数据，在基于LWE的同态方案中，密文

数据是整数向量，而在基于RLWE的同态方案中，密文数据是一个多项式向量或多项式矩阵；密码运算库作为全同态加密的核心模块，其定义了各类全同态密码基础算法和算子，提供了编码和加密两个重要功能，其计算过程如图3所示，密码运算库可将不同的原始数据编码为不同的明文数据类型，进而将明文数据加密为不同的密文类型，从而为计算指令库中的各类运算指令提供支持。

[0045] 可选地，在本申请的一个实施例中，基于预设密码密钥，对明文数据进行加密，得到全同态加密数据，包括：基于预设明文/密文转换算子，通过LWE加密、RLWE加密、MLWE加密或RGSW加密的方法对明文数据进行加密，得到全同态加密数据。

[0046] 需要说明的是，本申请的实施例可通过密码运算库通过LWE加密、RLWE加密、MLWE加密或RGSW加密的方法，利用密码密钥，即预设的明文/密文转换算子对不同的明文数据进行对称加密或非对称加密，得到全同态加密数据。

[0047] 由此，本申请的实施例通过对明文数据进行加密，获取全同态加密数据，从而为后续的全同态计算指令提供数据支持。

[0048] 在步骤S203中，根据预设的全同态计算指令，调用全同态计算指令对应的运算算子，并对全同态加密数据进行算术运算和/或逻辑运算，得到通用隐私计算结果。

[0049] 在实际计算过程中，针对不同的全同态计算任务，本申请实施例可利用编译器调用数据类型库中对应的数据类型和计算指令模块中的计算指令，计算指令库则会从密码运算库调用加密、编码等密码运算方式，进而通过数学基础库完成对应的密码运算，计算过程和全同态加密方案无关，可以完成具备同态算术运算和同态逻辑运算的复杂任务，具备通用性和高效性。

[0050] 当需加入新的计算指令或新的数据类型时，可仅在计算指令库定义新的计算指令，在数据类型库增加新的数据类型，无需对整个计算架构进行修改，具备良好的可拓展性；若要对计算架构进行硬件加速，则可以在数学基础库提供加速接口，直接加速底层数学运算，易于硬件加速。

[0051] 可选地，在本申请的一个实施例中，根据预设的全同态计算指令，调用全同态计算指令对应的运算算子，并对全同态加密数据进行算术运算和/或逻辑运算，得到通用隐私计算结果，包括：基于预设全同态算术运算算子，对全同态加密数据进行算术运算；基于预设全同态逻辑运算算子，对全同态加密数据进行逻辑运算。

[0052] 需要说明的是，本申请的实施例中的计算指令库是整个计算架构的最上层模块，其可实现多种同态指令运算算子通过调用密码运算模块和数据类型模块的相应元素，完成对应计算指令。计算指令库定义并实现了一系列全同态算术运算算子、全同态逻辑运算算子以及明文/密文转换算子等，为同态算术运算和同态逻辑运算提供了多种全同态计算指令。

[0053] 其中，全同态算术运算算子包括加法、减法、同态矩阵乘法、同态卷积，旋转、线性化、层级加法及层级乘法等运算；全同态逻辑运算算子包括同态与非门、密文转换、密钥轮换、盲旋转、功能自举、选择器及模数轮换等；明文/密文转换算子则用于在明文和密文之间进行转换。计算指令库中的指令和加密方案无关，不同加密方案对应的密文类型可以使用同一指令进行计算。

[0054] 由此，本申请的实施例可通过不同类型的密文转换方案，计算同时包含同态算术

运算和同态逻辑运算的复杂任务,并可利用已有计算指令构建更加复杂的同态计算指令,以根据编译器的需求提供各类指令,实现各种复杂的计算操作。

[0055] 可选地,在本申请的一个实施例中,对全同态加密数据进行算术运算和/或逻辑运算,包括:利用数学基础库对全同态加密数据进行算术运算和/或逻辑运算,其中,数学基础库包括整数代数结构、多项式代数结构、数论变换以及剩余数系统中的至少一项。

[0056] 在本申请的实施例中,数学基础库作为整个隐私计算框架的基础,提供底层的数学结构和数学运算支持,对全同态加密数据利用运算密钥进行算术运算和/或逻辑运算,该运算密钥由一系列密文组成,大部分运算密钥是公开的,可用于同态逻辑电路的计算。

[0057] 上述该数学基础库包括四种基本数学结构和运算,即整数代数结构、多项式代数结构、数论变换和剩余数系统。其中,整数代数结构是全同态加密中最基本的数学结构,多项式代数结构则用于支持全同态多项式密文运算,数论变换用于支持全同态密文上的乘法操作,剩余数系统则用于支持大密文的全同态运算。上述数学结构和运算被广泛应用于全同态加密中,能够支持各种计算操作,例如加法、减法、乘法等运算,为其他库提供了可靠的数学结构和数学运算基础。

[0058] 根据本申请实施例提出的基于全同态加密的通用隐私计算方法,通过获取用户的原始数据,并对用户的原始数据进行编码,得到明文数据;基于预设密码密钥,对明文数据进行加密,得到全同态加密数据;根据预设的全同态计算指令,调用全同态计算指令对应的运算算子,并对全同态加密数据进行算术运算和/或逻辑运算,得到通用隐私计算结果,从而消除了不同全同态加密方案间的壁垒,能够有效完成全同态加密中算术运算和逻辑运算混合的复杂计算任务,并且易于拓展新指令和实现硬件加速。

[0059] 其次,参照附图描述根据本申请实施例提出的基于全同态加密的通用隐私计算装置。

[0060] 图4是本申请实施例的基于全同态加密的通用隐私计算装置的方框示意图。

[0061] 如图4所示,该基于全同态加密的通用隐私计算装置10包括:编码模块100、加密模块200以及计算模块300。

[0062] 其中,编码模块100,用于获取用户的原始数据,并对用户的原始数据进行编码,得到明文数据。

[0063] 加密模块200,用于基于预设密码密钥,对明文数据进行加密,得到全同态加密数据。

[0064] 计算模块300,用于根据预设的全同态计算指令,调用全同态计算指令对应的运算算子,并对全同态加密数据进行算术运算和/或逻辑运算,得到通用隐私计算结果。

[0065] 可选地,在本申请的一个实施例中,编码模块100具体用于,通过SISD编码、SIMD-Slot编码或SIMD-Coeff编码的方式对原始数据进行编码,得到满足预设代数结构的明文数据。

[0066] 可选地,在本申请的一个实施例中,加密模块200具体用于,基于预设明文/密文转换算子,通过LWE加密、RLWE加密、MLWE加密或RGSW加密的方法对明文数据进行加密,得到全同态加密数据。

[0067] 可选地,在本申请的一个实施例中,计算模块300包括:第一运算单元和第二运算单元。

[0068] 其中,第一运算单元,用于基于预设全同态算术运算算子,对全同态加密数据进行算术运算。

[0069] 第二运算单元,用于基于预设全同态逻辑运算算子,对全同态加密数据进行逻辑运算。

[0070] 可选地,在本申请的一个实施例中,计算模块300还包括:调用单元,用于利用数学基础库对全同态加密数据进行算术运算和/或逻辑运算,其中,数学基础库包括整数代数结构、多项式代数结构、数论变换以及剩余数系统中的至少一项。

[0071] 需要说明的是,前述对基于全同态加密的通用隐私计算方法实施例的解释说明也适用于该实施例的基于全同态加密的通用隐私计算装置,此处不再赘述。

[0072] 根据本申请实施例提出的基于全同态加密的通用隐私计算装置,通过获取用户的原始数据,并对用户的原始数据进行编码,得到明文数据;基于预设密码密钥,对明文数据进行加密,得到全同态加密数据;根据预设的全同态计算指令,调用全同态计算指令对应的运算算子,并对全同态加密数据进行算术运算和/或逻辑运算,得到通用隐私计算结果,从而消除了不同全同态加密方案间的壁垒,能够有效完成全同态加密中算术运算和逻辑运算混合的复杂计算任务,并且易于拓展新指令和实现硬件加速。

[0073] 图5为本申请实施例提供的电子设备的结构示意图。该电子设备可以包括:

[0074] 存储器501、处理器502及存储在存储器501上并可在处理器502上运行的计算机程序。

[0075] 处理器502执行程序时实现上述实施例中提供的基于全同态加密的通用隐私计算方法。

[0076] 进一步地,电子设备还包括:

[0077] 通信接口503,用于存储器501和处理器502之间的通信。

[0078] 存储器501,用于存放可在处理器502上运行的计算机程序。

[0079] 存储器501可能包含高速RAM存储器,也可能还包括非易失性存储器(non-volatile memory),例如至少一个磁盘存储器。

[0080] 如果存储器501、处理器502和通信接口503独立实现,则通信接口503、存储器501和处理器502可以通过总线相互连接并完成相互间的通信。总线可以是工业标准体系结构(Industry Standard Architecture,简称为ISA)总线、外部设备互连(Peripheral Component,简称为PCI)总线或扩展工业标准体系结构(Extended Industry Standard Architecture,简称为EISA)总线等。总线可以分为地址总线、数据总线、控制总线等。为便于表示,图5中仅用一条粗线表示,但并不表示仅有一根总线或一种类型的总线。

[0081] 可选地,在具体实现上,如果存储器501、处理器502及通信接口503,集成在一块芯片上实现,则存储器501、处理器502及通信接口503可以通过内部接口完成相互间的通信。

[0082] 处理器502可能是一个中央处理器(Central Processing Unit,简称为CPU),或者是特定集成电路(Application Specific Integrated Circuit,简称为ASIC),或者是被配置成实施本申请实施例的一个或多个集成电路。

[0083] 本申请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,该程序被处理器执行时实现如上的基于全同态加密的通用隐私计算方法。

[0084] 在本说明书的描述中,参考术语“一个实施例”、“一些实施例”、“示例”、“具体示

例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本申请的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不必须针对的是相同的实施例或示例。而且，描述的具体特征、结构、材料或者特点可以在任一个或N个实施例或示例中以合适的方式结合。此外，在不相互矛盾的情况下，本领域的技术人员可以将本说明书中描述的不同实施例或示例以及不同实施例或示例的特征进行结合和组合。

[0085] 此外，术语“第一”、“第二”仅用于描述目的，而不能理解为指示或暗示相对重要性或者隐含指明所指示的技术特征的数量。由此，限定有“第一”、“第二”的特征可以明示或者隐含地包括至少一个该特征。在本申请的描述中，“N个”的含义是至少两个，例如两个，三个等，除非另有明确具体的限定。

[0086] 流程图中或在此以其他方式描述的任何过程或方法描述可以被理解为，表示包括一个或N个用于实现定制逻辑功能或过程的步骤的可执行指令的代码的模块、片段或部分，并且本申请的优选实施方式的范围包括另外的实现，其中可以不按所示出或讨论的顺序，包括根据所涉及的功能按基本同时的方式或按相反的顺序，来执行功能，这应被本申请的实施例所属技术领域的技术人员所理解。

[0087] 在流程图中表示或在此以其他方式描述的逻辑和/或步骤，例如，可以被认为是用于实现逻辑功能的可执行指令的定序列表，可以具体实现在任何计算机可读介质中，以供指令执行系统、装置或设备(如基于计算机的系统、包括处理器的系统或其他可以从指令执行系统、装置或设备取指令并执行指令的系统)使用，或结合这些指令执行系统、装置或设备而使用。就本说明书而言，"计算机可读介质"可以是任何可以包含、存储、通信、传播或传输程序以供指令执行系统、装置或设备或结合这些指令执行系统、装置或设备而使用的装置。计算机可读介质的更具体的示例(非穷尽性列表)包括以下：具有一个或N个布线的电连接部(电子装置)，便携式计算机盘盒(磁装置)，随机存取存储器(RAM)，只读存储器(ROM)，可擦除可编辑只读存储器(EPROM或闪速存储器)，光纤装置，以及便携式光盘只读存储器(CDROM)。另外，计算机可读介质甚至可以是可在其上打印所述程序的纸或其他合适的介质，因为可以通过对纸或其他介质进行光学扫描，接着进行编辑、解译或必要时以其他合适方式进行处理来以电子方式获得所述程序，然后将其存储在计算机存储器中。

[0088] 应当理解，本申请的各部分可以用硬件、软件、固件或它们的组合来实现。在上述实施方式中，N个步骤或方法可以用存储在存储器中且由合适的指令执行系统执行的软件或固件来实现。如果用硬件来实现和在另一实施方式中一样，可用本领域公知的下列技术中的任一项或他们的组合来实现：具有用于对数据信号实现逻辑功能的逻辑门电路的离散逻辑电路，具有合适的组合逻辑门电路的专用集成电路，可编程门阵列(PGA)，现场可编程门阵列(FPGA)等。

[0089] 本技术领域的普通技术人员可以理解实现上述实施例方法携带的全部或部分步骤是可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，该程序在执行时，包括方法实施例的步骤之一或其组合。

[0090] 此外，在本申请各个实施例中的各功能单元可以集成在一个处理模块中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。所述集成的模块如

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。

[0091] 上述提到的存储介质可以是只读存储器，磁盘或光盘等。尽管上面已经示出和描述了本申请的实施例，可以理解的是，上述实施例是示例性的，不能理解为对本申请的限制，本领域的普通技术人员在本申请的范围内可以对上述实施例进行变化、修改、替换和变型。


编译器
数据类型
运算密钥
旋转/自举…/密钥
密文数据
向量/多项式向量
密码密钥
加/解密密钥
明文数据
整数/多项式
原始数据
整数/向量/矩阵
计算指令
矩阵乘法
卷积
密文转换
盲旋转
功能自举
旋转
线性化
NAND
选择器
层级加/乘
密钥轮换
模数轮换
密码运算
加密
LWE
RLWE
MLWE
RGSW
编码
SISD
SIMD-Slot
SIMD-Coeff
大/小端
数学基础
整数代数结构
多项式代数结构
数论变换
剩余数字系统

图1

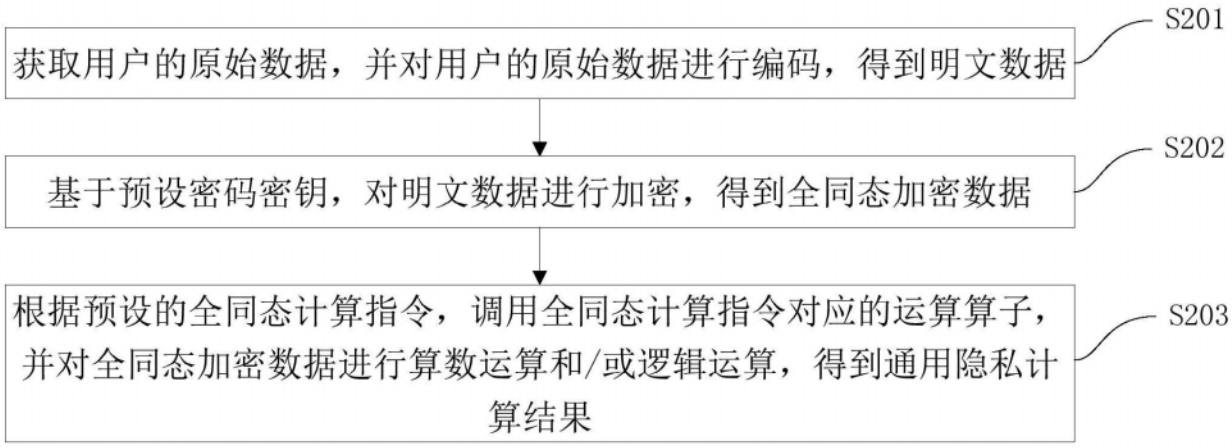

S201
获取用户的原始数据，并对用户的原始数据进行编码，得到明文数据
S202
基于预设密码密钥，对明文数据进行加密，得到全同态加密数据
S203
根据预设的全同态计算指令，调用全同态计算指令对应的运算算子，并对全同态加密数据进行算数运算和/或逻辑运算，得到通用隐私计算结果

图2

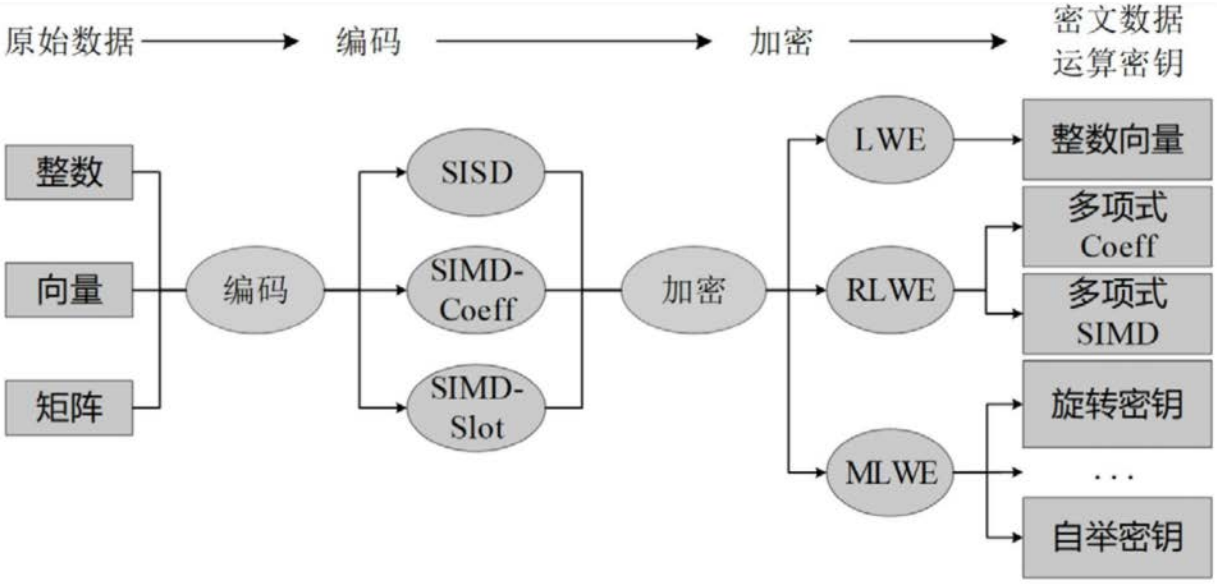

原始数据
编码
加密
密文数据
运算密钥
整数
向量
矩阵
编码
SISD
SIMD-Coeff
SIMD-Slot
加密
LWE
RLWE
MLWE
整数向量
多项式Coeff
多项式SIMD
旋转密钥
...
自举密钥

图3

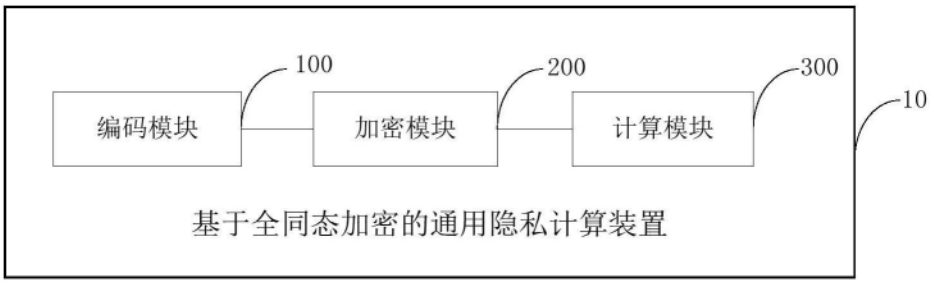

100
200
300
10
编码模块
加密模块
计算模块
基于全同态加密的通用隐私计算装置

图4

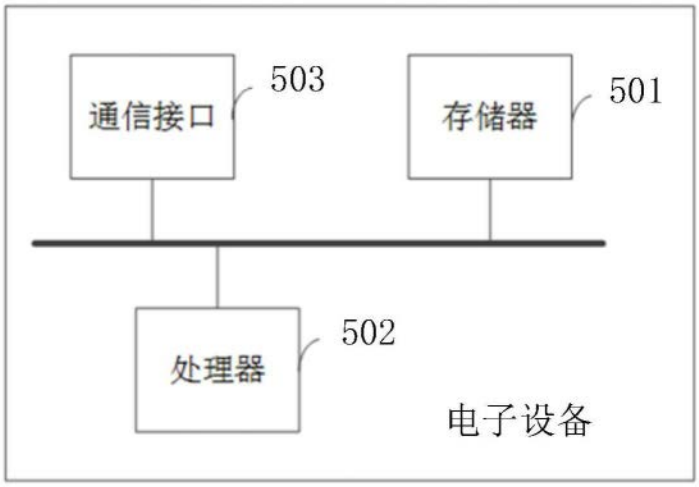

通信接口
503
存储器
501
处理器
502
电子设备

图5