(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 115879552 B
(45)授权公告日 2024.06.14

(21)申请号 202111142483.5
(22)申请日 2021.09.28
(65)同一申请的已公布的文献号
申请公布号 CN 115879552 A
(43)申请公布日 2023.03.31
(73)专利权人 本源量子计算科技(合肥)股份有限公司
地址 230088 安徽省合肥市合肥市高新区创新大道2800号创新产业园二期E2楼六层
(72)发明人 窦猛汉 李叶 刘焱
(51)Int.Cl.
G06N 10/20(2022.01)
G06N 10/40(2022.01)
G06F 7/72(2006.01)

(56)对比文件
CN 104065478 A,2014.09.24
CN 112114776 A,2020.12.22

审查员 王青

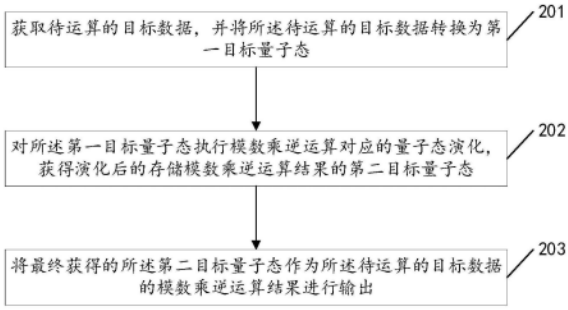
权利要求书3页 说明书16页 附图4页

(54)发明名称

量子模数乘逆运算方法、装置、电子装置及模数算术组件

(57)摘要

本发明公开了一种量子模数乘逆运算方法、装置、电子装置及模数算术组件,本发明通过获取待运算的目标数据,并将所述待运算的目标数据转换为第一目标量子态;对所述第一目标量子态执行模数乘逆运算对应的量子态演化,获得演化后的存储模数乘逆运算结果的第二目标量子态;将最终获得的所述第二目标量子态作为所述待运算的目标数据的模数乘逆运算结果进行输出,实现了量子线路中的模数乘逆运算操作,填补了相关技术空白。



CN 115879552 B

1.一种量子模数乘逆运算方法,其特征在于,所述方法包括:

获取待运算的目标数据,并将所述待运算的目标数据转换为第一目标量子态;

将第一个量子态转换模块的第一辅助输出项、第二个量子态转换项的第二辅助输出项作为乘逆输出模块的其中两个输入项;

将乘逆输出模块的第二个第三辅助输出项作为第三个量子态转换模块的输入项,以及将第三个第三辅助输出项作为第一CNOT门的其中一个输入项;将乘逆输出模块的第一个第三辅助输出项、第一待运算量子态输出项、第六个第三辅助输出项,第三个量子态转换模块的第五辅助输出项以及第一CNOT门的其中一个第四辅助输出项作为乘逆处理模块的五个输入项;

将乘逆处理模块的第二个第六辅助输出项作为第四个量子态转换模块的输入项;将乘逆处理模块的第一个第六辅助输出项、第三个第六辅助输出项和第四个第六辅助输出项,第四个量子态转换模块的第七辅助输出项,第一CNOT门的另外一个第四辅助输出项,乘逆输出模块的第一个第三辅助输出项和第一待运算量子态输出项作为逆乘逆输出模块的七个输入项;

将逆乘逆输出模块的第二个第八辅助输出项作为第五个所述量子态转换模块的输入项,将逆乘逆输出模块的第四个第八辅助输出项作为第六个量子态转换模块的输入项;

生成模数乘逆器对应的目标量子线路;

制备第一个所述量子态转换模块的输入项的第一辅助输入量子态、第二个所述量子态转换模块的输入项的第二辅助输入量子态、所述乘逆输出模块的四个第三辅助输入量子态和待运算量子态输入项、所述第一CNOT门的第四辅助输入量子态;

将所述第一目标量子态作为所述待运算量子态输入项的输入,得到制备初态后的所述目标量子线路;

运行制备初态后的所述目标量子线路,以及测量所述第四辅助输入项对应的量子比特,得到第二目标量子态;将最终获得的所述第二目标量子态作为所述待运算的目标数据的模数乘逆运算结果进行输出。

2.如权利要求1所述的方法,其特征在于,所述方法还包括:

获取量子态转换模块、乘逆输出模块、第一CNOT门、乘逆处理模块、逆乘逆输出模块,其中,组成所述乘逆输出模块的逻辑门与组成所述逆乘逆输出模块的逻辑门转置共轭。

3.如权利要求1所述的方法,其特征在于,

所述乘逆处理模块的五个输出项包括一个第二待运算量子态输出项和四个第六辅助输出项;

所述逆乘逆输出模块的七个输出项包括一个第三待运算量子态输出项和六个第八辅助输出项;

第五个所述量子态转换模块的输出项包括一个第九辅助输出项;第六个所述量子态转换模块的输出项包括一个第十辅助输出项。

4.如权利要求1所述的方法,其特征在于,第一个所述量子态转换模块用于将输入态转换为$|p\rangle$,第二个所述量子态转换模块和第四个所述量子态转换模块用于将输入态转换为$|1\rangle$,第三个所述量子态转换模块、第五个所述量子态转换模块和第六个所述量子态转换模

块用于将输入态转换为$|0\rangle$,其中,所述$|p\rangle$为模数p转换的量子态。

5.如权利要求1-4任一项所述的方法,其特征在于,所述方法还包括:

获取三个X门和2n个第一运算器模块,所述X门包括一个输入项和一个输出项,所述第一运算器模块包括八个输入项和八个输出项;

将2n所述个第一运算器模块进行级联,生成第二运算器模块;

将其中两个所述X门的输出项作为所述第二运算器模块的其中两个输入项,将所述第二运算器模块的其中一个输入项作为另外一个所述X门的输入项,将三个所述X门和所述第二运算器模块进行级联,生成所述乘逆处理模块。

6.如权利要求5所述的方法,其特征在于,所述方法还包括:

获取一个X门、两个第二CNOT门、一个普通加法器模块和一个Kaliski门,所述X门包括一个输入项和一个输出项,所述第二CNOT门包括两个输入项和两个输出项,所述普通加法器模块包括四个输入项和四个输出项,所述Kaliski门包括七个输入项和七个输出项;

将第一个所述第二CNOT门的其中一个输出项作为第二个所述第二CNOT门的其中一个输出项;

将第一个所述第二CNOT门的另外一个输出项和第二个所述第二CNOT门的其中一个输出项作为所述普通加法器的其中两个输入项;

将所述普通加法器的其中一个输出项作为第三个所述X门的输入项;

将所述普通加法器的其中两个输出项、第二个所述第二CNOT门的另外一个输出项以及第三个所述X门的输出项作为所述Kaliski门的其中四个输入项;

将所述一个X门、两个第二CNOT门、一个普通加法器模块和一个Kaliski门进行级联,生成所述第一运算器模块。

7.如权利要求1-4任一项所述的方法,其特征在于,所述方法还包括:

获取$l+1$个模数倍增器模块,以及将$l+1$个所述模数倍增器模块进行级联,生成所述乘逆处理模块。

8.一种量子模数乘逆运算装置,其特征在于,所述装置包括:

获取单元,用于获取待运算的目标数据,并将所述待运算的目标数据转换为第一目标量子态;

演化单元,用于将第一个量子态转换模块的第一辅助输出项、第二个量子态转换项的第二辅助输出项作为乘逆输出模块的其中两个输入项;将乘逆输出模块的第二个第三辅助输出项作为第三个量子态转换模块的输入项,以及将第三个第三辅助输出项作为第一CNOT门的其中一个输入项;将乘逆输出模块的第一个第三辅助输出项、第一待运算量子态输出项、第六个第三辅助输出项,第三个量子态转换模块的第五辅助输出项以及第一CNOT门的其中一个第四辅助输出项作为乘逆处理模块的五个输入项;将乘逆处理模块的第二个第六辅助输出项作为第四个量子态转换模块的输入项;将乘逆处理模块的第一个第六辅助输出项、第三个第六辅助输出项和第四个第六辅助输出项,第四个量子态转换模块的第七辅助输出项,第一CNOT门的另外一个第四辅助输出项,乘逆输出模块的第一个第三辅助输出项和第一待运算量子态输出项作为逆乘逆输出模块的七个输入项;将逆乘逆输出模块的第二个第八辅助输出项作为第五个所述量子态转换模块的输入项,将逆乘逆输出模块的第四个

第八辅助输出项作为第六个量子态转换模块的输入项;生成模数乘逆器对应的目标量子线路;制备第一个所述量子态转换模块的输入项的第一辅助输入量子态、第二个所述量子态转换模块的输入项的第二辅助输入量子态、所述乘逆输出模块的四个第三辅助输入量子态和待运算量子态输入项、所述第一CNOT门的第四辅助输入量子态;将所述第一目标量子态作为所述待运算量子态输入项的输入,得到制备初态后的所述目标量子线路;运行制备初态后的所述目标量子线路,以及测量所述第四辅助输入项对应的量子比特,得到第二目标量子态;

输出单元,用于将最终获得的所述第二目标量子态作为所述待运算的目标数据的模数乘逆运算结果进行输出。

9.一种存储介质,其特征在于,所述存储介质中存储有计算机程序,其中,所述计算机程序被设置为运行时执行所述权利要求1至7任一项中所述的方法。

10.一种电子装置,包括存储器和处理器,其特征在于,所述存储器中存储有计算机程序,所述处理器被设置为运行所述计算机程序以执行所述权利要求1至7任一项中所述的方法。

11.一种量子模数算术组件,其特征在于,包括根据权利要求1至7任一项中所述的方法确定的量子模数乘逆器。

量子模数乘逆运算方法、装置、电子装置及模数算术组件

技术领域

[0001] 本发明属于量子计算技术领域,特别是一种量子模数乘逆运算方法、装置、电子装置及模数算术组件。

背景技术

[0002] 量子计算机是一类遵循量子力学规律进行高速数学和逻辑运算、存储及处理量子信息的物理装置。当某个装置处理和计算的是量子信息,运行的是量子算法时,它就是量子计算机。量子计算机因其具有相对普通计算机更高效的处理数学问题的能力,例如,能将破解RSA密钥的时间从数百年加速到数小时,故成为一种正在研究中的关键技术。

[0003] 在破密量子算法的实现过程中,通常需要借助各种量子逻辑门构建量子算法,但是,仅依靠各种量子逻辑门构建量子算法时,并没有对应经典模数运算例如模数加法、模数乘法、模数平方、模数乘逆的模数基本算术运算操作的量子逻辑门。因此,急需提供一种能够实现量子线路中的模数基本算术运算操作的技术,以填补相关技术空白。

发明内容

[0004] 本发明的目的是提供一种量子模数乘逆运算方法、装置、电子装置及模数算术组件,旨在实现量子线路中的模数乘逆运算操作,以填补相关技术空白。

[0005] 本申请的一个实施例提供了一种量子模数乘逆运算方法,所述方法包括:

[0006] 获取待运算的目标数据,并将所述待运算的目标数据转换为第一目标量子态;

[0007] 对所述第一目标量子态执行模数乘逆运算对应的量子态演化,获得演化后的存储模数乘逆运算结果的第二目标量子态;

[0008] 将最终获得的所述第二目标量子态作为所述待运算的目标数据的模数乘逆运算结果进行输出。

[0009] 可选的,在所述对所述第一目标量子态执行模数乘逆运算对应的量子态演化,获得演化后的存储模数乘逆运算结果的第二目标量子态方面,包括:

[0010] 获取量子态转换模块、乘逆输出模块、第一CNOT门、乘逆处理模块、逆乘逆输出模块,其中,组成所述乘逆输出模块的逻辑门与组成所述逆乘逆输出模块的逻辑门转置共轭;

[0011] 将所述量子态转换模块、所述乘逆输出模块、所述第一CNOT门、所述乘逆处理模块和所述逆乘逆输出模块进行级联,生成模数乘逆器对应的目标量子线路;

[0012] 通过所述目标量子线路对所述第一目标量子态的各量子比特进行模数乘逆运算,生成第二目标量子态。

[0013] 可选的,所述量子态转换模块的数量为六,所述量子态转换模块包括一个输入项和一个输出项,所述乘逆输出模块包括七个输入项和七个输出项,所述第一CNOT门包括两个输入项和两个输出项;所述乘逆处理模块包括五个输入项和五个输出项;所述逆乘逆处理模块包括七个输入项和七个输出项;

[0014] 在所述将所述量子态转换模块、所述乘逆输出模块、所述第一CNOT门、所述乘逆处

理模块和所述逆乘逆输出模块进行级联,生成模数乘逆器对应的目标量子线路方面,包括:

[0015] 将第一个所述量子态转换模块的输出项、第二个所述量子态转换项的输出项作为所述乘逆输出模块的其中两个输入项;

[0016] 将所述乘逆输出模块的第二个输出项作为第三个所述量子态转换模块的输入项,第四个输出项作为所述第一CNOT门的其中一个输入项;将所述乘逆输出模块的第一个输出项、第三个输出项、第七个输出项,第三个所述量子态转换模块的输出项以及所述第一CNOT门的其中一个输出项作为所述乘逆处理模块的五个输入项;

[0017] 将所述乘逆处理模块的第二个输出项作为第四个所述量子态转换模块的输入项;将所述乘逆处理模块的第一个输出项、第三个输出项和第四个输出项,第四个所述量子态转换模块的输出项,所述第一CNOT门的另外一个输出项,所述乘逆输出模块的第五个输出项和第六个输出项作为所述逆乘逆输出模块的七个输入项;

[0018] 将所述逆乘逆输出模块的第二个输出项作为第五个所述量子态转换模块的输入项,将所述逆乘逆输出模块的第五个输出项作为第六个所述量子态转换模块的输入项;

[0019] 将所述量子态转换模块、所述乘逆输出模块、所述第一CNOT门、所述乘逆处理模块和所述逆乘逆输出模块进行级联,生成模数乘逆器对应的目标量子线路。

[0020] 可选的,第一个所述量子态转换模块的输入项包括一个第一辅助输入项,第一个所述量子态转换模块的输出项包括一个第一辅助输出项;第二个所述量子态转换模块的输入项包括一个第二辅助输入项,第二个所述量子态转换模块的输出项包括一个第二辅助输出项;

[0021] 所述乘逆输出模块的七个输入项包括一个待运算量子态输入项、一个所述第一辅助输出项、一个所述第二辅助输出项和四个第三辅助输入项;所述乘逆输出模块的七个输出项包括一个第一待运算量子态输出项和六个第三辅助输出项;

[0022] 所述第一CNOT门的两个输入项包括一个所述第三辅助输出项和一个第四辅助输入项,所述第一CNOT门的两个输出项包括两个第四辅助输出项;第三个所述量子态转换模块的输入项包括一个所述第三辅助输出项,第三个所述量子态转换模块的输出项包括一个第五辅助输出项;

[0023] 所述乘逆处理模块的五个输入项包括两个所述第三辅助输出项、一个所述第五辅助输出项、一个所述第一待运算量子态输出项和其中一个所述第四辅助输出项;所述乘逆处理模块的五个输出项包括一个第二待运算量子态输出项和四个第六辅助输出项;

[0024] 第四个所述量子态转换项的输入项包括一个所述第六辅助输出项,第四个所述量子态转换项的输出项包括一个第七辅助输出项;

[0025] 所述逆乘逆输出模块的七个输入项包括两个所述第六辅助输出项、一个所述辅助第七输出项、一个所述第二待运算量子态输出项、另外一个所述第四辅助输出项、两个所述第三辅助输出项,所述逆乘逆输出模块的七个输出项包括一个第三待运算量子态输出项和六个第八辅助输出项;

[0026] 第五个所述量子态转换模块的输入项包括一个所述第八辅助输出项,第五个所述量子态转换模块的输出项包括一个第九辅助输出项;第六个所述量子态转换模块的输入项包括一个所述第八辅助输出项,第六个所述量子态转换模块的输出项包括一个第十辅助输出项。

[0027] 可选的,第一个所述量子态转换模块用于将输入态转换为|p>,第二个所述量子态转换模块和第四个所述量子态转换模块用于将输入态转换为|1>,第三个所述量子态转换模块、第五个所述量子态转换模块和第六个所述量子态转换模块用于将输入态转换为|0>,其中,所述|p>为模数p转换的量子态。

[0028] 可选的,所述方法还包括:

[0029] 获取三个X门和2n个第一运算器模块,所述X门包括一个输入项和一个输出项,所述第一运算器模块包括八个输入项和八个输出项;

[0030] 将2n所述个第一运算器模块进行级联,生成第二运算器模块;

[0031] 将其中两个所述X门的输出项作为所述第二运算器模块的其中两个输入项,将所述第二运算器模块的其中一个输入项作为另外一个所述X门的输入项,将三个所述X门和所述第二运算器模块进行级联,生成所述乘逆处理模块。

[0032] 可选的,所述方法还包括:

[0033] 获取一个X门、两个第二CNOT门、一个普通加法器模块和一个Kaliski门,所述X门包括一个输入项和一个输出项,所述第二CNOT门包括两个输入项和两个输出项,所述普通加法器模块包括四个输入项和四个输出项,所述Kaliski门包括七个输入项和七个输出项;

[0034] 将第一个所述第二CNOT门的其中一个输出项作为第二个所述第二CNOT门的其中一个输出项;

[0035] 将第一个所述第二CNOT门的另外一个输出项和第二个所述第二CNOT门的其中一个输出项作为所述普通加法器的其中两个输入项;

[0036] 将所述普通加法器的其中一个输出项作为第三个所述X门的输入项;

[0037] 将所述普通加法器的其中两个输出项、第二个所述第二CNOT门的另外一个输出项以及第三个所述X门的输出项作为所述Kaliski门的其中四个输入项;

[0038] 将所述一个X门、两个第二CNOT门、一个普通加法器模块和一个Kaliski门进行级联,生成所述第一运算器模块。

[0039] 可选的,所述方法还包括:

[0040] 获取l+1个模数倍增器模块,以及将l+1个所述模数倍增器模块进行级联,生成所述乘逆处理模块。

[0041] 可选的,在所述通过所述目标量子线路对所述第一目标量子态的各量子比特进行模数乘逆运算,生成第二目标量子态方面,包括:

[0042] 制备第一辅助输入量子态、第二辅助输入量子态、第三辅助输入量子态和第四辅助输入量子态;

[0043] 将所述第一辅助输入量子态作为所述第一辅助输入项的输入,将所述第二辅助输入量子态作为所述第二辅助输入项的输入,将所述第三辅助输入量子态作为所述第三辅助输入项的输入,将所述第四辅助输入量子态作为所述第四辅助输入项的输入,将所述第一目标量子态作为所述待运算量子态输入项的输入,得到制备初态后的所述目标量子线路;

[0044] 运行制备初态后的所述目标量子线路,以及测量所述第四辅助输入项对应的量子比特,得到第二目标量子态。

[0045] 本申请的又一实施例提供了一种量子模数乘逆运算装置,所述装置包括:

[0046] 获取单元,用于获取待运算的目标数据,并将所述待运算的目标数据转换为第一

目标量子态；

[0047] 演化单元，用于对所述第一目标量子态执行模数乘逆运算对应的量子态演化，获得演化后的存储模数乘逆运算结果的第二目标量子态；

[0048] 输出单元，用于将最终获得的所述第二目标量子态作为所述待运算的目标数据的模数乘逆运算结果进行输出。

[0049] 可选的，在所述对所述第一目标量子态执行模数乘逆运算对应的量子态演化，获得演化后的存储模数乘逆运算结果的第二目标量子态方面，所述演化单元具体用于：

[0050] 获取量子态转换模块、乘逆输出模块、第一CNOT门、乘逆处理模块、逆乘逆输出模块，其中，组成所述乘逆输出模块的逻辑门与组成所述逆乘逆输出模块的逻辑门转置共轭；

[0051] 将所述量子态转换模块、所述乘逆输出模块、所述第一CNOT门、所述乘逆处理模块和所述逆乘逆输出模块进行级联，生成模数乘逆器对应的目标量子线路；

[0052] 通过所述目标量子线路对所述第一目标量子态的各量子比特进行模数乘逆运算，生成第二目标量子态。

[0053] 可选的，所述量子态转换模块的数量为六，所述量子态转换模块包括一个输入项和一个输出项，所述乘逆输出模块包括七个输入项和七个输出项，所述第一CNOT门包括两个输入项和两个输出项；所述乘逆处理模块包括五个输入项和五个输出项；所述逆乘逆处理模块包括七个输入项和七个输出项；

[0054] 在所述将所述量子态转换模块、所述乘逆输出模块、所述第一CNOT门、所述乘逆处理模块和所述逆乘逆输出模块进行级联，生成模数乘逆器对应的目标量子线路方面，所述演化单元具体用于：

[0055] 将第一个所述量子态转换模块的输出项、第二个所述量子态转换项的输出项作为所述乘逆输出模块的其中两个输入项；

[0056] 将所述乘逆输出模块的第二个输出项作为第三个所述量子态转换模块的输入项，第四个输出项作为所述第一CNOT门的其中一个输入项；将所述乘逆输出模块的第一个输出项、第三个输出项、第七个输出项，第三个所述量子态转换模块的输出项以及所述第一CNOT门的其中一个输出项作为所述乘逆处理模块的五个输入项；

[0057] 将所述乘逆处理模块的第二个输出项作为第四个所述量子态转换模块的输入项；将所述乘逆处理模块的第一个输出项、第三个输出项和第四个输出项，第四个所述量子态转换模块的输出项，所述第一CNOT门的另外一个输出项，所述乘逆输出模块的第五个输出项和第六个输出项作为所述逆乘逆输出模块的七个输入项；

[0058] 将所述逆乘逆输出模块的第二个输出项作为第五个所述量子态转换模块的输入项，将所述逆乘逆输出模块的第五个输出项作为第六个所述量子态转换模块的输入项；

[0059] 将所述量子态转换模块、所述乘逆输出模块、所述第一CNOT门、所述乘逆处理模块和所述逆乘逆输出模块进行级联，生成模数乘逆器对应的目标量子线路。

[0060] 可选的，第一个所述量子态转换模块的输入项包括一个第一辅助输入项，第一个所述量子态转换模块的输出项包括一个第一辅助输出项；第二个所述量子态转换模块的输入项包括一个第二辅助输入项，第二个所述量子态转换模块的输出项包括一个第二辅助输出项；

[0061] 所述乘逆输出模块的七个输入项包括一个待运算量子态输入项、一个所述第一辅

助输出项、一个所述第二辅助输出项和四个第三辅助输入项;所述乘逆输出模块的七个输出项包括一个第一待运算量子态输出项和六个第三辅助输出项;

[0062] 所述第一CNOT门的两个输入项包括一个所述第三辅助输出项和一个第四辅助输入项,所述第一CNOT门的两个输出项包括两个第四辅助输出项;第三个所述量子态转换模块的输入项包括一个所述第三辅助输出项,第三个所述量子态转换模块的输出项包括一个第五辅助输出项;

[0063] 所述乘逆处理模块的五个输入项包括两个所述第三辅助输出项、一个所述第五辅助输出项、一个所述第一待运算量子态输出项和其中一个所述第四辅助输出项;所述乘逆处理模块的五个输出项包括一个第二待运算量子态输出项和四个第六辅助输出项;

[0064] 第四个所述量子态转换项的输入项包括一个所述第六辅助输出项,第四个所述量子态转换项的输出项包括一个第七辅助输出项;

[0065] 所述逆乘逆输出模块的七个输入项包括两个所述第六辅助输出项、一个所述辅助第七输出项、一个所述第二待运算量子态输出项、另外一个所述第四辅助输出项、两个所述第三辅助输出项,所述逆乘逆输出模块的七个输出项包括一个第三待运算量子态输出项和六个第八辅助输出项;

[0066] 第五个所述量子态转换模块的输入项包括一个所述第八辅助输出项,第五个所述量子态转换模块的输出项包括一个第九辅助输出项;第六个所述量子态转换模块的输入项包括一个所述第八辅助输出项,第六个所述量子态转换模块的输出项包括一个第十辅助输出项。

[0067] 可选的,第一个所述量子态转换模块用于将输入态转换为|p>,第二个所述量子态转换模块和第四个所述量子态转换模块用于将输入态转换为|1>,第三个所述量子态转换模块、第五个所述量子态转换模块和第六个所述量子态转换模块用于将输入态转换为|0>,其中,所述|p>为模数p转换的量子态。

[0068] 可选的,所述演化单元还用于:

[0069] 获取三个X门和2n个第一运算器模块,所述X门包括一个输入项和一个输出项,所述第一运算器模块包括八个输入项和八个输出项;

[0070] 将2n所述个第一运算器模块进行级联,生成第二运算器模块;

[0071] 将其中两个所述X门的输出项作为所述第二运算器模块的其中两个输入项,将所述第二运算器模块的其中一个输入项作为另外一个所述X门的输入项,将三个所述X门和所述第二运算器模块进行级联,生成所述乘逆处理模块。

[0072] 可选的,所述演化单元还用于:

[0073] 获取一个X门、两个第二CNOT门、一个普通加法器模块和一个Kaliski门,所述X门包括一个输入项和一个输出项,所述第二CNOT门包括两个输入项和两个输出项,所述普通加法器模块包括四个输入项和四个输出项,所述Kaliski门包括七个输入项和七个输出项;

[0074] 将第一个所述第二CNOT门的其中一个输出项作为第二个所述第二CNOT门的其中一个输出项;

[0075] 将第一个所述第二CNOT门的另外一个输出项和第二个所述第二CNOT门的其中一个输出项作为所述普通加法器的其中两个输入项;

[0076] 将所述普通加法器的其中一个输出项作为第三个所述X门的输入项;

[0077] 将所述普通加法器的其中两个输出项、第二个所述第二CNOT门的另外一个输出项以及第三个所述X门的输出项作为所述Kaliski门的其中四个输入项;

[0078] 将所述一个X门、两个第二CNOT门、一个普通加法器模块和一个Kaliski门进行级联,生成所述第一运算器模块。

[0079] 可选的,所述演化单元还用于:

[0080] 获取l+1个模数倍增器模块,以及将l+1个所述模数倍增器模块进行级联,生成所述乘逆处理模块。

[0081] 可选的,在所述通过所述目标量子线路对所述第一目标量子态的各量子比特进行模数乘逆运算,生成第二目标量子态方面,所述演化单元具体用于:

[0082] 制备第一辅助输入量子态、第二辅助输入量子态、第三辅助输入量子态和第四辅助输入量子态;

[0083] 将所述第一辅助输入量子态作为所述第一辅助输入项的输入,将所述第二辅助输入量子态作为所述第二辅助输入项的输入,将所述第三辅助输入量子态作为所述第三辅助输入项的输入,将所述第四辅助输入量子态作为所述第四辅助输入项的输入,将所述第一目标量子态作为所述待运算量子态输入项的输入,得到制备初态后的所述目标量子线路;

[0084] 运行制备初态后的所述目标量子线路,以及测量所述第四辅助输入项对应的量子比特,得到第二目标量子态。

[0085] 本申请的又一实施例提供了一种存储介质,所述存储介质中存储有计算机程序,其中,所述计算机程序被设置为运行时执行上述任一项中所述的方法。

[0086] 本申请的又一实施例提供了一种电子装置,包括存储器和处理器,所述存储器中存储有计算机程序,所述处理器被设置为运行所述计算机程序以执行上述任一项中所述的方法。

[0087] 与现有技术相比,本发明提供的一种量子模数乘逆运算方法,通过获取待运算的目标数据,并将所述待运算的目标数据转换为第一目标量子态;对所述第一目标量子态执行模数乘逆运算对应的量子态演化,获得演化后的存储模数乘逆运算结果的第二目标量子态;将最终获得的所述第二目标量子态作为所述待运算的目标数据的模数乘逆运算结果进行输出,实现了量子线路中的模数乘逆运算操作,填补了相关技术空白。

附图说明

[0088] 图1为本发明实施例提供的一种量子模数乘逆运算方法的计算机终端的硬件结构框图;

[0089] 图2为本发明实施例提供的一种量子模数乘逆运算方法的流程示意图;

[0090] 图3为本发明实施例提供的一种模数乘逆器的对应的目标量子线路图;

[0091] 图4为本发明实施例提供的一种乘逆输出模块的量子线路图;

[0092] 图5为本发明实施例提供的一种Kaliski门的对应的量子线路图;

[0093] 图6为本发明实施例提供的一种乘逆处理模块的量子线路图;

[0094] 图7为本发明实施例提供的一种量子模数乘逆运算装置的结构示意图。

具体实施方式

[0095] 下面通过参考附图描述的实施例是示例性的,仅用于解释本发明,而不能解释为对本发明的限制。

[0096] 本发明实施例首先提供了一种量子模数乘逆运算方法,该方法可以应用于电子设备,如计算机终端,具体如普通电脑、量子计算机等。

[0097] 下面以运行在计算机终端上为例对其进行详细说明。图1为本发明实施例提供的一种量子模数乘逆运算方法的计算机终端的硬件结构框图。如图1所示,计算机终端可以包括一个或多个(图1中仅示出一个)处理器102(处理器102可以包括但不限于微处理器MCU或可编程逻辑器件FPGA等的处理装置)和用于存储基于量子线路的量子模数乘逆运算方法的存储器104,可选地,上述计算机终端还可以包括用于通信功能的传输装置106以及输入输出设备108。本领域普通技术人员可以理解,图1所示的结构仅为示意,其并不对上述计算机终端的结构造成限定。例如,计算机终端还可包括比图1中所示更多或者更少的组件,或者具有与图1所示不同的配置。

[0098] 存储器104可用于存储应用软件的软件程序以及模块,如本申请实施例中的量子模数乘逆运算方法对应的程序指令/模块,处理器102通过运行存储在存储器104内的软件程序以及模块,从而执行各种功能应用以及数据处理,即实现上述的方法。存储器104可包括高速随机存储器,还可包括非易失性存储器,如一个或者多个磁性存储装置、闪存、或者其他非易失性固态存储器。在一些实例中,存储器104可进一步包括相对于处理器102远程设置的存储器,这些远程存储器可以通过网络连接至计算机终端。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

[0099] 传输装置106用于经由一个网络接收或者发送数据。上述的网络具体实例可包括计算机终端的通信供应商提供的无线网络。在一个实例中,传输装置106包括一个网络适配器(Network Interface Controller,NIC),其可通过基站与其他网络设备相连从而可与互联网进行通讯。在一个实例中,传输装置106可以为射频(Radio Frequency,RF)模块,其用于通过无线方式与互联网进行通讯。

[0100] 需要说明的是,真正的量子计算机是混合结构的,它包含两大部分:一部分是经典计算机,负责执行经典计算与控制;另一部分是量子设备,负责运行量子程序进而实现量子计算。而量子程序是由量子语言如QRunes语言编写的一串能够在量子计算机上运行的指令序列,实现了对量子逻辑门操作的支持,并最终实现量子计算。具体的说,量子程序就是一系列按照一定时序操作量子逻辑门的指令序列。

[0101] 在实际应用中,因受限于量子设备硬件的发展,通常需要进行量子计算模拟以验证量子算法、量子应用等等。量子计算模拟即借助普通计算机的资源搭建的虚拟架构(即量子虚拟机)实现特定问题对应的量子程序的模拟运行的过程。通常,需要构建特定问题对应的量子程序。本发明实施例所指量子程序,即是经典语言编写的表征量子比特及其演化的程序,其中与量子计算相关的量子比特、量子逻辑门等等均有相应的经典代码表示。

[0102] 量子线路作为量子程序的一种体现方式,也称量子逻辑电路,是最常用的通用量子计算模型,表示在抽象概念下对于量子比特进行操作的线路,其组成包括量子比特、线路(时间线)、以及各种量子逻辑门,最后常需要通过量子测量操作将结果读取出来。

[0103] 不同于传统电路是用金属线所连接以传递电压信号或电流信号,在量子线路中,

线路可看成是由时间所连接,亦即量子比特的状态随着时间自然演化,在这过程中按照哈密顿运算符的指示,一直到遇上逻辑门而被操作。

[0104] 一个量子程序整体上对应有一条总的量子线路,本发明所述量子程序即指该条总的量子线路,其中,该总的量子线路中的量子比特总数与量子程序的量子比特总数相同。可以理解为:一个量子程序可以由量子线路、针对量子线路中量子比特的测量操作、保存测量结果的寄存器及控制流节点(跳转指令)组成,一条量子线路可以包含几十上百个甚至成千上万个量子逻辑门操作。量子程序的执行过程,就是对所有的量子逻辑门按照一定时序执行的过程。需要说明的是,时序即单个量子逻辑门被执行的时间顺序。

[0105] 需要说明的是,经典计算中,最基本的单元是比特,而最基本的控制模式是逻辑门,可以通过逻辑门的组合来达到控制电路的目的。类似地,处理量子比特的方式就是量子逻辑门。使用量子逻辑门,能够使量子态发生演化,量子逻辑门是构成量子线路的基础,量子逻辑门包括单比特量子逻辑门,如Hadamard门(H门,阿达马门)、泡利-X门(X门)、泡利-Y门(Y门)、泡利-Z门(Z门)、RX门、RY门、RZ门等等;多比特量子逻辑门,如CNOT门、CR门、iSWAP门、Toffoli门等等。量子逻辑门一般使用酉矩阵表示,而酉矩阵不仅是矩阵形式,也是一种操作和变换。一般量子逻辑门在量子态上的作用是通过酉矩阵左乘以量子态右矢对应的矩阵进行计算。

[0106] 数论中,把一个计量单位称之为模或者模数,例如时钟是以12进制进行计数循环的,即以12为模。模运算在数论和程序设计中都有着广泛的应用,奇偶数的判别到素数的判别,从模幂运算到最大公约数的求法,从孙子问题到凯撒密码问题,无不充斥着模运算的身影。模数乘逆运算是指任意一个数据的逆求模的运算,例如任何对1/10的模数乘逆运算,$(1/10)^{-1}\bmod 10=0$。在量子计算领域中,急需提供一种能够实现量子线路中的模数乘逆运算操作的技术,以填补相关技术空白。

[0107] 参见图2,图2为本发明实施例提供的一种量子模数乘逆运算方法的流程示意图。

[0108] 本实施例提供一种量子模数乘逆运算方法,所述方法包括:

[0109] 步骤201:获取待运算的目标数据,并将所述待运算的目标数据转换为第一目标量子态;

[0110] 具体地,在所述获取待运算的目标数据,并将所述待运算的目标数据转换为第一目标量子态方面,可以是利用现有的振幅编码方式,将待运算的十进制数据转换为二进制的量子态表示。例如,一个目标数据为7,带符号的二进制表示0111;另一个目标数据为4,带符号的二进制表示011;其中,最高位为0表示正数,1表示负数。其中,目标量子态为两个目标量子比特对应的本征态,量子比特位对应的所有本征态表征的数量是2的量子比特位的个数次方。例如:例如一组量子比特为q_0、q_1、q_2,表示第0位、第1位、第2位量子比特,从高位到低位排序为$q_2q_1q_0$,则该组量子比特位对应的本征态(即量子态)总共有8个,分别为:|000>、|001>、|010>、|011>、|100>、|101>、|110>、|111>,该8个本征态之间的叠加态。该组量子比特位的个数可以根据实际运算需要进行设置。

[0111] 步骤202:对所述第一目标量子态执行模数乘逆运算对应的量子态演化,获得演化后的存储模数乘逆运算结果的第二目标量子态;

[0112] 本实施例用于介绍如何在量子计算机中实现乘逆运算的逻辑电路,并结合预先开发软件QPanda对每个模块进行说明。任何经典逻辑电路,也可以通过量子线路来表示。经典

电路和量子线路一一对应,量子逻辑门/量子线路的输入与输出均是量子比特,且输入与输出的量子比特数量相等。量子线路允许量子态以叠加的方式输入,输出的状态即可以相同的方式叠加输出。可逆计算是量子计算的基本,即任何可逆线路存在逆线路,也就是说,将每个原有的输出作为输入,正好可以映射到原来的输入上。可逆线路意味着对于每一种输出,都正好有一种输入与之对应,这种映射是一一映射。例如非门是一个典型的可逆逻辑门,它的逆线路就是它自身。典型的不可逆逻辑门就是与门、或门。例如与门的输入是0,0;0,1;1,0的时候均输出0,这说明不存在从输出到输入的唯一映射。可逆计算意味着信息在计算过程中没有丢失,经过逆变换之后可以恢复原来的状态。不可逆计算意味着信息丢失了。例如从与门的输出,无法推知输入的状态。对于可逆计算来说,是可以推知的。任何连续执行的可逆逻辑门,合起来是一个可逆操作。量子逻辑门全部是可逆逻辑门,所以量子线路是可逆线路。但是量子测量不是可逆计算。

[0113] 具体地,在所述对所述第一目标量子态执行模数乘逆运算对应的量子态演化,获得演化后的存储模数乘逆运算结果的第二目标量子态方面,包括:

[0114] 获取量子态转换模块、乘逆输出模块、第一CNOT门、乘逆处理模块、逆乘逆输出模块,其中,组成所述乘逆输出模块的逻辑门与组成所述逆乘逆输出模块的逻辑门转置共轭;

[0115] 将所述量子态转换模块、所述乘逆输出模块、所述第一CNOT门、所述乘逆处理模块和所述逆乘逆输出模块进行级联,生成模数乘逆器对应的目标量子线路;

[0116] 通过所述目标量子线路对所述第一目标量子态的各量子比特进行模数乘逆运算,生成第二目标量子态。

[0117] 其中,CNOT门的矩阵形式如下:

[0118] $$\begin{bmatrix}1 & 0 & 0 & 0\\0 & 1 & 0 & 0\\0 & 0 & 0 & 1\\0 & 0 & 1 & 0\end{bmatrix}$$

[0119] CNOT门的控制位为|0>时,被控制位不变;CNOT门的控制位为|1>时,被控制位取反。

[0120] 其中,量子态转换模块用于将一个已知的量子态转换为另外一个待确定的量子态,其可以通过X门实现。X门的矩阵形式如下:

[0121] $$\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$$

[0122] 其用于将|0>和|1>互变。

[0123] 其中,转置共轭指的是矩阵的一种数学变换,具体操作方法是先将矩阵A中的每个元素取共轭,将新得到的元素组成新的矩阵B,然后再对矩阵B作转置变换。各模块由多个逻辑门组成,逻辑门可以写成矩阵形式,模块的转置共轭即组成该模块的逻辑门的转置共轭。

[0124] 进一步地,所述量子态转换模块的数量为六,所述量子态转换模块包括一个输入项和一个输出项,所述乘逆输出模块包括七个输入项和七个输出项,所述第一CNOT门包括两个输入项和两个输出项;所述乘逆处理模块包括五个输入项和五个输出项;所述逆乘逆处理模块包括七个输入项和七个输出项;

[0125] 所述将所述量子态转换模块、所述乘逆输出模块、所述第一CNOT门、所述乘逆处理

模块和所述逆乘逆输出模块进行级联,生成模数乘逆器对应的目标量子线路,包括:

[0126] 将第一个所述量子态转换模块的输出项、第二个所述量子态转换项的输出项作为所述乘逆输出模块的其中两个输入项;

[0127] 将所述乘逆输出模块的第二个输出项作为第三个所述量子态转换模块的输入项,第四个输出项作为所述第一CNOT门的其中一个输入项;将所述乘逆输出模块的第一个输出项、第三个输出项、第七个输出项,第三个所述量子态转换模块的输出项以及所述第一CNOT门的其中一个输出项作为所述乘逆处理模块的五个输入项;

[0128] 将所述乘逆处理模块的第二个输出项作为第四个所述量子态转换模块的输入项;将所述乘逆处理模块的第一个输出项、第三个输出项和第四个输出项,第四个所述量子态转换模块的输出项,所述第一CNOT门的另外一个输出项,所述乘逆输出模块的第五个输出项和第六个输出项作为所述逆乘逆输出模块的七个输入项;

[0129] 将所述逆乘逆输出模块的第二个输出项作为第五个所述量子态转换模块的输入项,将所述逆乘逆输出模块的第五个输出项作为第六个所述量子态转换模块的输入项;

[0130] 将所述量子态转换模块、所述乘逆输出模块、所述第一CNOT门、所述乘逆处理模块和所述逆乘逆输出模块进行级联,生成模数乘逆器对应的目标量子线路。

[0131] 其中,第一个所述量子态转换模块的输入项包括一个第一辅助输入项,第一个所述量子态转换模块的输出项包括一个第一辅助输出项;第二个所述量子态转换模块的输入项包括一个第二辅助输入项,第二个所述量子态转换模块的输出项包括一个第二辅助输出项;

[0132] 所述乘逆输出模块的七个输入项包括一个待运算量子态输入项、一个所述第一辅助输出项、一个所述第二辅助输出项和四个第三辅助输入项;所述乘逆输出模块的七个输出项包括一个第一待运算量子态输出项和六个第三辅助输出项;

[0133] 所述第一CNOT门的两个输入项包括一个所述第三辅助输出项和一个第四辅助输入项,所述第一CNOT门的两个输出项包括两个第四辅助输出项;第三个所述量子态转换模块的输入项包括一个所述第三辅助输出项,第三个所述量子态转换模块的输出项包括一个第五辅助输出项;

[0134] 所述乘逆处理模块的五个输入项包括两个所述第三辅助输出项、一个所述第五辅助输出项、一个所述第一待运算量子态输出项和其中一个所述第四辅助输出项;所述乘逆处理模块的五个输出项包括一个第二待运算量子态输出项和四个第六辅助输出项;

[0135] 第四个所述量子态转换项的输入项包括一个所述第六辅助输出项,第四个所述量子态转换项的输出项包括一个第七辅助输出项;

[0136] 所述逆乘逆输出模块的七个输入项包括两个所述第六辅助输出项、一个所述辅助第七输出项、一个所述第二待运算量子态输出项、另外一个所述第四辅助输出项、两个所述第三辅助输出项,所述逆乘逆输出模块的七个输出项包括一个第三待运算量子态输出项和六个第八辅助输出项;

[0137] 第五个所述量子态转换模块的输入项包括一个所述第八辅助输出项,第五个所述量子态转换模块的输出项包括一个第九辅助输出项;第六个所述量子态转换模块的输入项包括一个所述第八辅助输出项,第六个所述量子态转换模块的输出项包括一个第十辅助输出项。

[0138] 其中,第一个所述量子态转换模块用于将输入态转换为|p>,第二个所述量子态转换模块和第四个所述量子态转换模块用于将输入态转换为|1>,第三个所述量子态转换模块、第五个所述量子态转换模块和第六个所述量子态转换模块用于将输入态转换为|0>,其中,所述|p>为模数p转换的量子态。

[0139] 具体地,在所述通过所述目标量子线路对所述第一目标量子态的各量子比特进行模数乘逆运算,生成第二目标量子态方面,包括:

[0140] 制备第一辅助输入量子态、第二辅助输入量子态、第三辅助输入量子态和第四辅助输入量子态;

[0141] 将所述第一辅助输入量子态作为所述第一辅助输入项的输入,将所述第二辅助输入量子态作为所述第二辅助输入项的输入,将所述第三辅助输入量子态作为所述第三辅助输入项的输入,将所述第四辅助输入量子态作为所述第四辅助输入项的输入,将所述第一目标量子态作为所述待运算量子态输入项的输入,得到制备初态后的所述目标量子线路;

[0142] 运行制备初态后的所述目标量子线路,以及测量所述第四辅助输入项对应的量子比特,得到第二目标量子态。

[0143] 如图3所示,图3为本发明实施例提供的一种模数乘逆器的对应的目标量子线路图。第一个所述量子态转换模块的输入项包括一个第一辅助输入项,其对应n个量子比特(图3中的第二条线),这n个量子比特的初始量子态即第一辅助输入量子态制备为|0>;第二个所述量子态转换模块的输入项包括一个第二辅助输入项,其对应n+1个量子比特(图3中的第五条线),这n+1个量子比特的初始量子态即第二辅助输入量子态制备为|0>。

[0144] 乘逆输出模块的一个待运算量子态输入项对应n个量子比特(图3中的第三条线),这n个量子比特的初始量子态即第一目标量子态制备为|x>;第一个第三辅助输入项对应4个量子比特(图3中的第一条线),这4个量子比特的初始量子态即第三辅助输入量子态制备为|0>,其用于作为乘逆输出模块的控制位;第二个第三辅助输入项对应n+1个量子比特(图3中的第四条线),这n+1个量子比特的初始量子态即第三辅助输入量子态制备为|0>;第三个第三辅助输入项对应2n个量子比特(图3中的第六条线),这2n个量子比特的初始量子态即第三辅助输入量子态制备为|0>;第四个第三辅助输入项对应1个量子比特(图3中的第七条线),这1个量子比特的初始量子态即第三辅助输入量子态制备为|0>,其中l=logn。

[0145] 所述第一CNOT门的第四辅助输入项对应n个量子比特(图3中的第八条线),这n个量子比特的初始量子态即第四辅助输入量子态制备为|0>。

[0146] 待运算量子态输入项对应n个量子比特的末态为|x>,第一辅助输入项对应的n个量子比特的末态为|0>,第二辅助输入项对应的n+1个量子比特的末态为|0>,四个第三辅助输入项对应的量子比特的末态为|0>,这些量子比特可以用于后续的运算操作。第四辅助输入项对应的量子比特的末态为$|x^{-1}\bmod p>$,用于存储模数乘逆运算结果。

[0147] 步骤203:将最终获得的所述第二目标量子态作为所述待运算的目标数据的模数乘逆运算结果进行输出。

[0148] 本实施例中,通过将待运算的目标数据转换后的第一目标量子态,输入量子模数乘逆器(即所述目标量子线路)中,得到对应的二进制表示模数乘逆结果的第二目标量子态。然后将二进制表示的表示模数乘逆结果的第二目标量子态直接输出,完成目标数据的模数乘逆运算。

[0149] 与现有技术相比,本发明提供的一种量子模数乘逆运算方法,通过获取待运算的目标数据,并将所述待运算的目标数据转换为第一目标量子态;对所述第一目标量子态执行模数乘逆运算对应的量子态演化,获得演化后的存储模数乘逆运算结果的第二目标量子态;将最终获得的所述第二目标量子态作为所述待运算的目标数据的模数乘逆运算结果进行输出,实现了量子线路中的模数乘逆运算操作,填补了相关技术空白。

[0150] 在本发明的一具体实施例中,所述方法还包括:

[0151] 获取三个X门和2n个第一运算器模块,所述X门包括一个输入项和一个输出项,所述第一运算器模块包括八个输入项和八个输出项;

[0152] 将2n所述个第一运算器模块进行级联,生成第二运算器模块;

[0153] 将其中两个所述X门的输出项作为所述第二运算器模块的其中两个输入项,将所述第二运算器模块的其中一个输入项作为另外一个所述X门的输入项,将三个所述X门和所述第二运算器模块进行级联,生成所述乘逆处理模块。

[0154] 进一步地,所述方法还包括:

[0155] 获取一个X门、两个第二CNOT门、一个普通加法器模块和一个Kaliski门,所述X门包括一个输入项和一个输出项,所述第二CNOT门包括两个输入项和两个输出项,所述普通加法器模块包括四个输入项和四个输出项,所述Kaliski门包括七个输入项和七个输出项;

[0156] 将第一个所述第二CNOT门的其中一个输出项作为第二个所述第二CNOT门的其中一个输出项;

[0157] 将第一个所述第二CNOT门的另外一个输出项和第二个所述第二CNOT门的其中一个输出项作为所述普通加法器的其中两个输入项;

[0158] 将所述普通加法器的其中一个输出项作为第三个所述X门的输入项;

[0159] 将所述普通加法器的其中两个输出项、第二个所述第二CNOT门的另外一个输出项以及第三个所述X门的输出项作为所述Kaliski门的其中四个输入项;

[0160] 将所述一个X门、两个第二CNOT门、一个普通加法器模块和一个Kaliski门进行级联,生成所述第一运算器模块。

[0161] 参见图4,图4为本发明实施例提供的一种乘逆输出模块的量子线路图,其中,空白圆形十字图案表示X门,由直线连接的空白圆形十字和实心黑点组成的图案表示CNOT门,实心黑点表示该CNOT门为1控CNOT门,中间的第一运算器模块被重复执行2n次。在图3中,第一个第三辅助输入项对应4个量子比特(图3中的第一条线),在图4中将其分为了两部分:普通加法器的其中一个输入项对应的3个量子比特和一个X门的输入项对应的一个量子比特。图4中其余的输入项与图3中输入项的关系可以根据图3和图4得出,在此不作详细阐述。

[0162] 这里需要说明的是,该模块用于将$|p\rangle|x\rangle|0\rangle|1\rangle$通过执行少于2n次Kaliski门转化为$|1\rangle|0\rangle|x^{-1}(-2^{2n-k}) \bmod p\rangle|p\rangle$,但是具体执行多少次Kalishi门并不确定,因此需要控制量子线路在转化成功后停止执行Kaliski门,并且记录Kaliski门的执行次数(2n-k)。用2n个量子比特编码的$|recoder\rangle$,其第i个量子比特编码的量子态记录了第i轮重复线路执行的信息,以保证信息的可逆性。

[0163] 从图4中可以看出,每个第一运算器模块只能运行普通加法器和Kaliski门中的一个。当图4中的第三条线路的输入量子态为$|0\rangle$时,普通加法器会被激活从而执行,Kaliski门未被激活不执行;输入量子态为$|1\rangle$时,相反。

[0164] 其中,Kaliski门的具体量子线路参见图5。如图5所示,Kaliski门由十个个控制门(由直线连接的空白十字和实心点或空心点图案表示)、两个比较器、四个SAWP门、一个普通加法器、一个普通减法器、一个常数倍减器和一个常数倍增器级联而成。控制门还分为一控一(一个控制位,一个被控位),一控多(一个控制位,多个被控位),多控一(多个控制位,一个被控位),多控多(多个控制位,多个被控位),其中控制位用实心点(1控)或空心点(0控)表示,被控位用中间有十字的圆表示。若为1控,控制位为|0〉时,被控制位不变;控制位为|1〉时,被控制位取反;若为0控,控制位为|1〉时,被控制位不变;控制位为|0〉时,被控制位取反。常数倍增器用于将目标数据增大至其两倍,常数倍减器用于将目标数据减小至其1/2。

[0165] 在图4中,乘逆输出模块的第一个输入项(图4中的第一条线)对应3个量子比特,在图5中将其分为了三个输入项,图5中其余的输入项与图4中输入项的关系可以根据图3和图4得出,在此不作详细阐述。各逻辑门的连接关系可以根据图5得出,也不进行赘述。$|u_i\rangle$、$|v_i\rangle$、$|r_i\rangle$、$|s_i\rangle$分别为第一运算器第i+1次被执行时的输入,$|u_{i+1}\rangle$、$|v_{i+1}\rangle$、$|r_{i+1}\rangle$、$|s_{i+1}\rangle$分别为第一运算器第i+1次被执行时的输出。

[0166] 在本发明的一具体实施例中,所述方法还包括:

[0167] 获取l+1个模数倍增器模块,以及将l+1个所述模数倍增器模块进行级联,生成所述乘逆处理模块。

[0168] 如图6所示,图6为本发明实施例提供的一种乘逆处理模块的量子线路图。前l个模数倍增器模块均包括5个输入项和5个输出项,最后一个模数倍增器模块包括4个输入项和4个输出项。前一个模数倍增器模块的输出项作为后一个模数倍增器模块的输入项,l+1个模数倍增器模块级联。其中,5个输入项中有一个输入项对应的量子态为模数倍增器模块的控制位,控制是否执行模数倍增器模块,若量子态为|1>则执行,若量子态为|0>则不执行。最后一个模数倍增器模块无控制位。

[0169] 本发明的另一实施例提供了一种量子模数乘逆运算运算装置,如图7所示,所述装置包括:

[0170] 获取单元701,用于获取待运算的目标数据,并将所述待运算的目标数据转换为第一目标量子态;

[0171] 演化单元702,用于对所述第一目标量子态执行模数乘逆运算对应的量子态演化,获得演化后的存储模数乘逆运算结果的第二目标量子态;

[0172] 输出单元703,用于将最终获得的所述第二目标量子态作为所述待运算的目标数据的模数乘逆运算结果进行输出。

[0173] 可选的,在所述对所述第一目标量子态执行模数乘逆运算对应的量子态演化,获得演化后的存储模数乘逆运算结果的第二目标量子态方面,所述演化单元702具体用于:

[0174] 获取量子态转换模块、乘逆输出模块、第一CNOT门、乘逆处理模块、逆乘逆输出模块,其中,组成所述乘逆输出模块的逻辑门与组成所述逆乘逆输出模块的逻辑门转置共轭;

[0175] 将所述量子态转换模块、所述乘逆输出模块、所述第一CNOT门、所述乘逆处理模块和所述逆乘逆输出模块进行级联,生成模数乘逆器对应的目标量子线路;

[0176] 通过所述目标量子线路对所述第一目标量子态的各量子比特进行模数乘逆运算,生成第二目标量子态。

[0177] 可选的,所述量子态转换模块的数量为六,所述量子态转换模块包括一个输入项

和一个输出项,所述乘逆输出模块包括七个输入项和七个输出项,所述第一CNOT门包括两个输入项和两个输出项;所述乘逆处理模块包括五个输入项和五个输出项;所述逆乘逆处理模块包括七个输入项和七个输出项;

[0178] 在所述将所述量子态转换模块、所述乘逆输出模块、所述第一CNOT门、所述乘逆处理模块和所述逆乘逆输出模块进行级联,生成模数乘逆器对应的目标量子线路方面,所述演化单元702具体用于:

[0179] 将第一个所述量子态转换模块的输出项、第二个所述量子态转换项的输出项作为所述乘逆输出模块的其中两个输入项;

[0180] 将所述乘逆输出模块的第二个输出项作为第三个所述量子态转换模块的输入项,第四个输出项作为所述第一CNOT门的其中一个输入项;将所述乘逆输出模块的第一个输出项、第三个输出项、第七个输出项,第三个所述量子态转换模块的输出项以及所述第一CNOT门的其中一个输出项作为所述乘逆处理模块的五个输入项;

[0181] 将所述乘逆处理模块的第二个输出项作为第四个所述量子态转换模块的输入项;将所述乘逆处理模块的第一个输出项、第三个输出项和第四个输出项,第四个所述量子态转换模块的输出项,所述第一CNOT门的另外一个输出项,所述乘逆输出模块的第五个输出项和第六个输出项作为所述逆乘逆输出模块的七个输入项;

[0182] 将所述逆乘逆输出模块的第二个输出项作为第五个所述量子态转换模块的输入项,将所述逆乘逆输出模块的第五个输出项作为第六个所述量子态转换模块的输入项;

[0183] 将所述量子态转换模块、所述乘逆输出模块、所述第一CNOT门、所述乘逆处理模块和所述逆乘逆输出模块进行级联,生成模数乘逆器对应的目标量子线路。

[0184] 可选的,第一个所述量子态转换模块的输入项包括一个第一辅助输入项,第一个所述量子态转换模块的输出项包括一个第一辅助输出项;第二个所述量子态转换模块的输入项包括一个第二辅助输入项,第二个所述量子态转换模块的输出项包括一个第二辅助输出项;

[0185] 所述乘逆输出模块的七个输入项包括一个待运算量子态输入项、一个所述第一辅助输出项、一个所述第二辅助输出项和四个第三辅助输入项;所述乘逆输出模块的七个输出项包括一个第一待运算量子态输出项和六个第三辅助输出项;

[0186] 所述第一CNOT门的两个输入项包括一个所述第三辅助输出项和一个第四辅助输入项,所述第一CNOT门的两个输出项包括两个第四辅助输出项;第三个所述量子态转换模块的输入项包括一个所述第三辅助输出项,第三个所述量子态转换模块的输出项包括一个第五辅助输出项;

[0187] 所述乘逆处理模块的五个输入项包括两个所述第三辅助输出项、一个所述第五辅助输出项、一个所述第一待运算量子态输出项和其中一个所述第四辅助输出项;所述乘逆处理模块的五个输出项包括一个第二待运算量子态输出项和四个第六辅助输出项;

[0188] 第四个所述量子态转换项的输入项包括一个所述第六辅助输出项,第四个所述量子态转换项的输出项包括一个第七辅助输出项;

[0189] 所述逆乘逆输出模块的七个输入项包括两个所述第六辅助输出项、一个所述辅助第七输出项、一个所述第二待运算量子态输出项、另外一个所述第四辅助输出项、两个所述第三辅助输出项,所述逆乘逆输出模块的七个输出项包括一个第三待运算量子态输出项和

六个第八辅助输出项；

[0190] 第五个所述量子态转换模块的输入项包括一个所述第八辅助输出项，第五个所述量子态转换模块的输出项包括一个第九辅助输出项；第六个所述量子态转换模块的输入项包括一个所述第八辅助输出项，第六个所述量子态转换模块的输出项包括一个第十辅助输出项。

[0191] 可选的，第一个所述量子态转换模块用于将输入态转换为|p>，第二个所述量子态转换模块和第四个所述量子态转换模块用于将输入态转换为|1>，第三个所述量子态转换模块、第五个所述量子态转换模块和第六个所述量子态转换模块用于将输入态转换为|0>，其中，所述|p>为模数p转换的量子态。

[0192] 可选的，所述演化单元还用于：

[0193] 获取三个X门和2n个第一运算器模块，所述X门包括一个输入项和一个输出项，所述第一运算器模块包括八个输入项和八个输出项；

[0194] 将2n所述个第一运算器模块进行级联，生成第二运算器模块；

[0195] 将其中两个所述X门的输出项作为所述第二运算器模块的其中两个输入项，将所述第二运算器模块的其中一个输入项作为另外一个所述X门的输入项，将三个所述X门和所述第二运算器模块进行级联，生成所述乘逆处理模块。

[0196] 可选的，所述演化单元702还用于：

[0197] 获取一个X门、两个第二CNOT门、一个普通加法器模块和一个Kaliski门，所述X门包括一个输入项和一个输出项，所述第二CNOT门包括两个输入项和两个输出项，所述普通加法器模块包括四个输入项和四个输出项，所述Kaliski门包括七个输入项和七个输出项；

[0198] 将第一个所述第二CNOT门的其中一个输出项作为第二个所述第二CNOT门的其中一个输出项；

[0199] 将第一个所述第二CNOT门的另外一个输出项和第二个所述第二CNOT门的其中一个输出项作为所述普通加法器的其中两个输入项；

[0200] 将所述普通加法器的其中一个输出项作为第三个所述X门的输入项；

[0201] 将所述普通加法器的其中两个输出项、第二个所述第二CNOT门的另外一个输出项以及第三个所述X门的输出项作为所述Kaliski门的其中四个输入项；

[0202] 将所述一个X门、两个第二CNOT门、一个普通加法器模块和一个Kaliski门进行级联，生成所述第一运算器模块。

[0203] 可选的，所述演化单元702还用于：

[0204] 获取l+1个模数倍增器模块，以及将l+1个所述模数倍增器模块进行级联，生成所述乘逆处理模块。

[0205] 可选的，在所述通过所述目标量子线路对所述第一目标量子态的各量子比特进行模数乘逆运算，生成第二目标量子态方面，所述演化单元702具体用于：

[0206] 制备第一辅助输入量子态、第二辅助输入量子态、第三辅助输入量子态和第四辅助输入量子态；

[0207] 将所述第一辅助输入量子态作为所述第一辅助输入项的输入，将所述第二辅助输入量子态作为所述第二辅助输入项的输入，将所述第三辅助输入量子态作为所述第三辅助输入项的输入，将所述第四辅助输入量子态作为所述第四辅助输入项的输入，将所述第一

目标量子态作为所述待运算量子态输入项的输入,得到制备初态后的所述目标量子线路;

[0208] 运行制备初态后的所述目标量子线路,以及测量所述第四辅助输入项对应的量子比特,得到第二目标量子态。

[0209] 本发明的再一实施例提供了一种存储介质,所述存储介质中存储有计算机程序,其中,所述计算机程序被设置为运行时执行上述任一项中方法实施例中的步骤。

[0210] 具体的,在本实施例中,上述存储介质可以被设置为存储用于执行以下步骤的计算机程序:

[0211] 获取待运算的目标数据,并将所述待运算的目标数据转换为第一目标量子态;

[0212] 对所述第一目标量子态执行模数乘逆运算对应的量子态演化,获得演化后的存储模数乘逆运算结果的第二目标量子态;

[0213] 将最终获得的所述第二目标量子态作为所述待运算的目标数据的模数乘逆运算结果进行输出。

[0214] 具体的,在本实施例中,上述存储介质可以包括但不限于:U盘、只读存储器(Read-Only Memory,简称为ROM)、随机存取存储器(Random Access Memory,简称为RAM)、移动硬盘、磁碟或者光盘等各种可以存储计算机程序的介质。

[0215] 本发明的再一实施例还提供了一种电子装置,包括存储器和处理器,所述存储器中存储有计算机程序,所述处理器被设置为运行所述计算机程序以执行上述任一项中方法实施例中的步骤。

[0216] 具体的,上述电子装置还可以包括传输设备以及输入输出设备,其中,该传输设备和上述处理器连接,该输入输出设备和上述处理器连接。

[0217] 具体的,在本实施例中,上述处理器可以被设置为通过计算机程序执行以下步骤:

[0218] 获取待运算的目标数据,并将所述待运算的目标数据转换为第一目标量子态;

[0219] 对所述第一目标量子态执行模数乘逆运算对应的量子态演化,获得演化后的存储模数乘逆运算结果的第二目标量子态;

[0220] 将最终获得的所述第二目标量子态作为所述待运算的目标数据的模数乘逆运算结果进行输出。

[0221] 本申请的又一实施例提供了一种量子模数算术组件,包括根据上述任一项中所述的方法确定的量子模数乘逆器。

[0222] 以上依据图式所示的实施例详细说明了本发明的构造、特征及作用效果,以上所述仅为本发明的较佳实施例,但本发明不以图面所示限定实施范围,凡是依照本发明的构想所作的改变,或修改为等同变化的等效实施例,仍未超出说明书与图示所涵盖的精神时,均应在本发明的保护范围内。

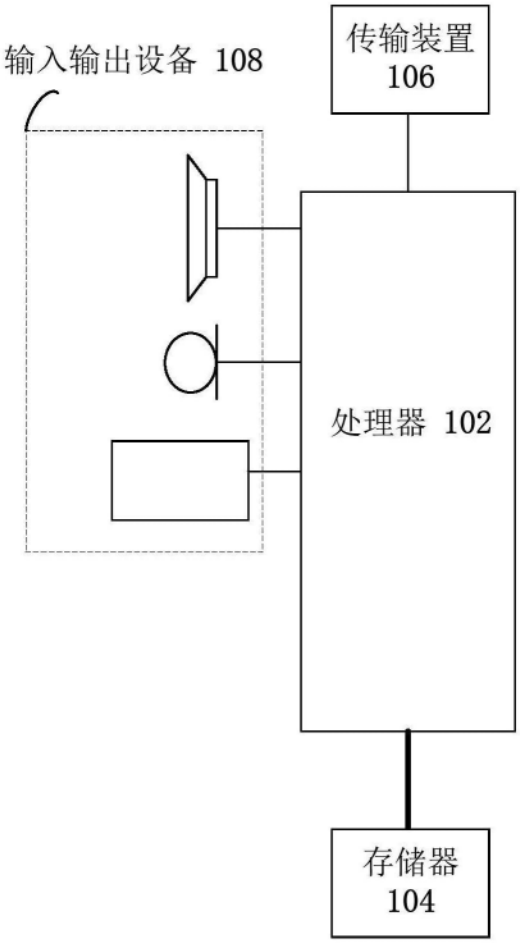

输入输出设备 108
传输装置
106
处理器 102
存储器
104

图1

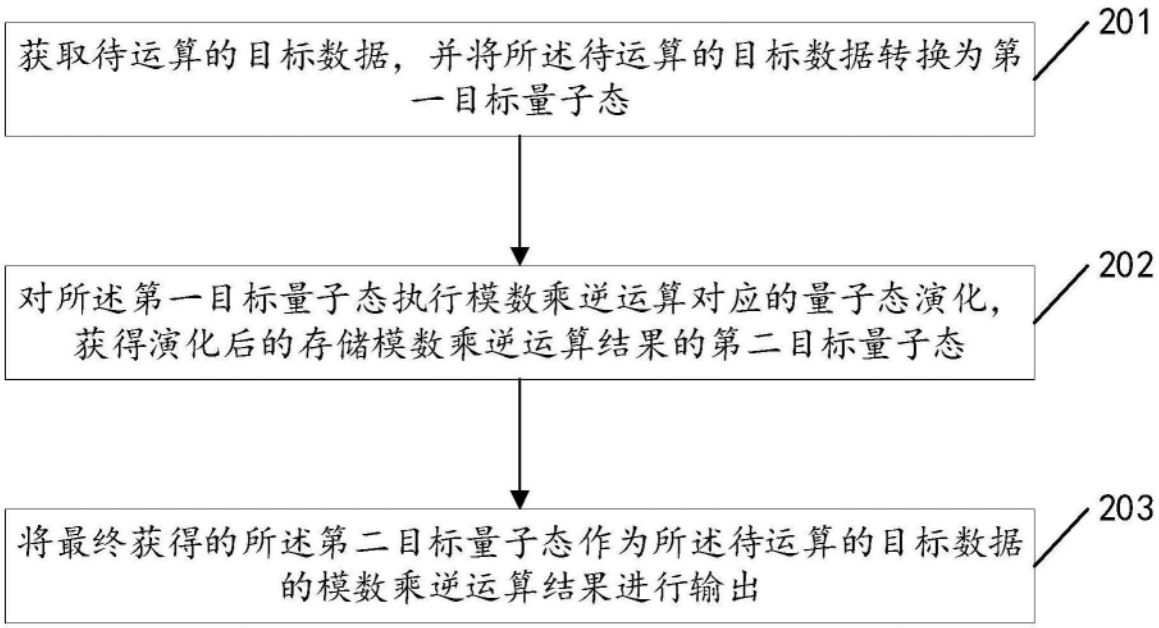

获取待运算的目标数据，并将所述待运算的目标数据转换为第一目标量子态
201
对所述第一目标量子态执行模数乘逆运算对应的量子态演化，获得演化后的存储模数乘逆运算结果的第二目标量子态
202
将最终获得的所述第二目标量子态作为所述待运算的目标数据的模数乘逆运算结果进行输出
203

图2

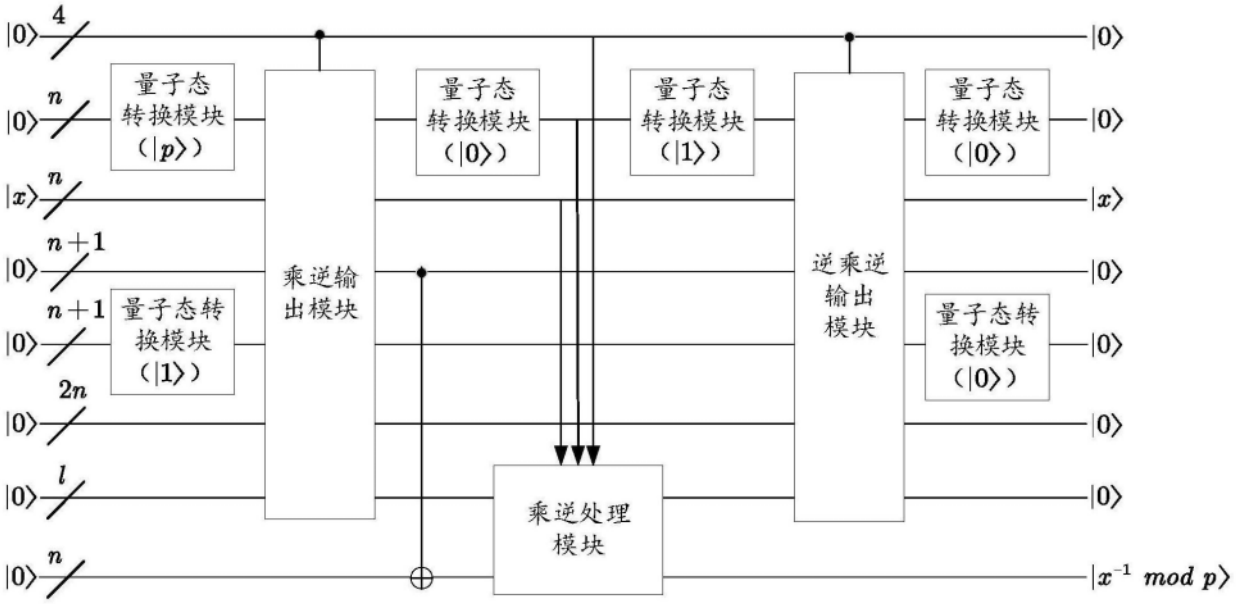

量子态转换模块（|p⟩）
乘逆输出模块
量子态转换模块（|0⟩）
量子态转换模块（|1⟩）
逆乘逆输出模块
量子态转换模块（|0⟩）
量子态转换模块（|1⟩）
量子态转换模块（|0⟩）
乘逆处理模块

图3

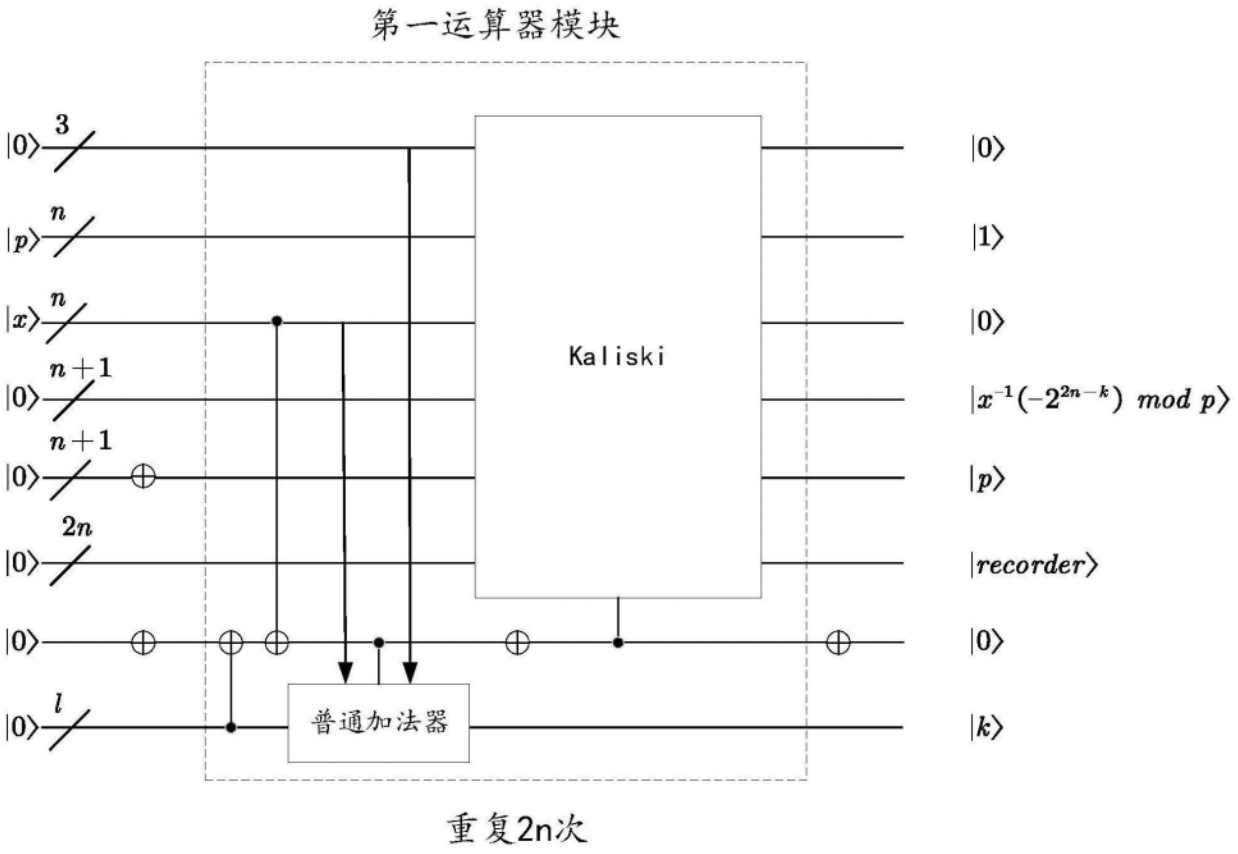

第一运算器模块
Kaliski
普通加法器
重复2n次

图4

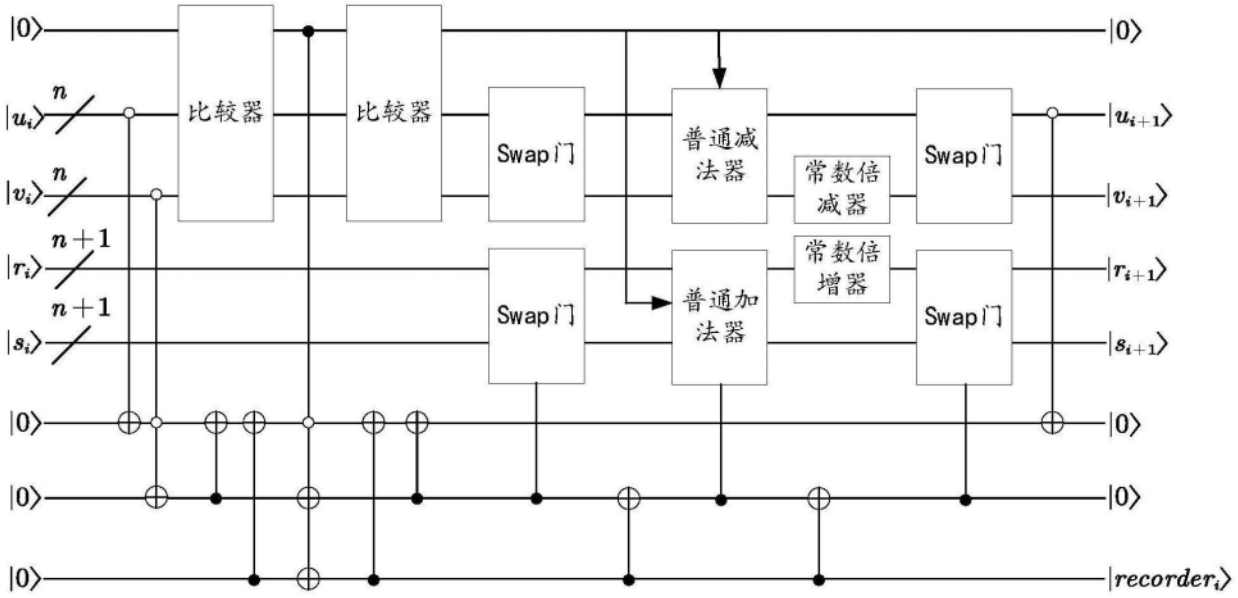

|0⟩
|u_i⟩
n
|v_i⟩
n
|r_i⟩
n+1
|s_i⟩
n+1
|0⟩
|0⟩
|0⟩
比较器
比较器
Swap门
Swap门
普通减法器
普通加法器
常数倍减器
常数倍增器
Swap门
Swap门
|0⟩
|u_{i+1}⟩
|v_{i+1}⟩
|r_{i+1}⟩
|s_{i+1}⟩
|0⟩
|0⟩
|recorder_i⟩

图5

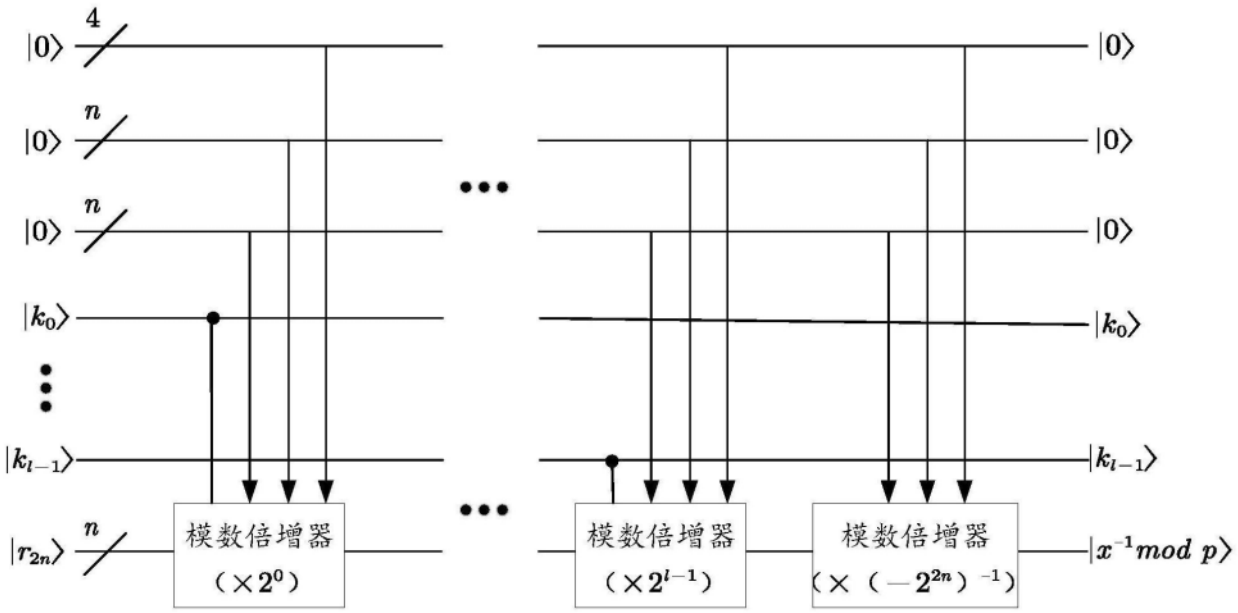

|0⟩
4
|0⟩
n
|0⟩
n
|k_0⟩
|k_{l-1}⟩
|r_{2n}⟩
n
模数倍增器
（×2^0）
模数倍增器
（×2^{l-1}）
模数倍增器
（×（−2^{2n}）^{-1}）
|0⟩
|0⟩
|0⟩
|k_0⟩
|k_{l-1}⟩
|x^{-1} mod p⟩

图6

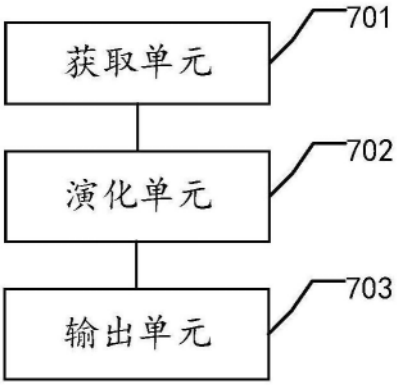


图7