Quantum Information and Computation, Vol. 0, No. 0 (2003) 000–000

Quantum Secure Multi-party Summation with Graph State

FIRST AUTHOR[a]
University Department, University Name, Address
City, State ZIP/Zone, Country[b]

SECOND AUTHOR
Group, Laboratory, Address
City, State ZIP/Zone, Country

Received (received date)
Revised (revised date)

这篇论文提出了基于量子图态的安全多方计算方法。与其他基于纠缠、基于门操作以及基于 QFT 的量子安全多方计算方法相比, 本文提供的方法基于量子图态本身的特殊性质，采用随机的量子图态结构和随机的加密门操作进一步提升计算的安全性。文章设计了两个加密协议，安全两方求和协议和安全多方求和协议，逐步说明如何应用量子图态技术实现安全多方计算。文章以模拟范例证明了两个协议的安全性和正确性，可以抵御来自内部和外部的攻击。又通过实验验证了协议是安全、有效、实用的。基于图态的量子安全多方计算方法为量子安全多方计算领域打开了一个新的思路，应用量子图态技术，更多的安全多方计算问题可以更安全高效的解决。

Keywords: 量子图态；安全多方计算；基于测量的量子计算

Communicated by: to be filled by the Editorial

1 Introduction

随着云计算、大数据时代的来临，数据安全与隐私保护问题日益突出。安全多方计算作为一种保护输入隐私的计算模式，在电子商务、医疗服务、金融交易等领域展现出广阔的应用前景，其核心目标是允许多个参与者在不泄露各自输入的情况下，共同完成一个计算任务。安全多方计算在经典计算领域已有深入的研究，主要依赖于数学困难问题的经典同态加密 (Homomorphic Encryption) 技术。但是，随着量子计算技术的发展，经典安全多方计算面临着来自量子计算的攻击，安全性无法得到保证。量子安全多方计算是一种利用量子力学的原理来设计安全多方计算协议的技术，它可以在完成多方计算的功能的同时，保证协议能够抵抗量子计算的攻击，并具有更优越的安全性能。当前量子安全多方计算多是应用量子纠缠态、量子门操作以及量子傅里叶变换实现同态加密，而量子图态作为一种描述多体量子系统复杂纠缠关系的量子态，具有可扩展性、测量友好以及误差容忍等优势，为量子安全多方计算提供了新的思路。

安全多方求和问题（Secure Multi-party Summation,SMS）是指多个参与方希望计算他们输入数据的总和，但又不愿意泄露自己的具体数据。设参与者为 $P_1, P_2, ..., P_n$, 私有

[a]Typeset names in 10 pt Times Roman, uppercase. Use the footnote to indicate the present or permanent address of the author.

[b]State completely without abbreviations, the affiliation and mailing address, including country. Typeset in 8 pt Times Italic.

数据分别为 $x_1, x_2, ..., x_n$, 目标是安全的计算:$f(x_1, x_2, ..., x_n) = x_1 + x_2 + ... + x_n$。安全多方求和问题在诸如数据挖掘和统计分析等领域有着广泛的应用。为解决此问题，研究者提出了众多基于不同密码学原语如加法秘密共享、Paillier 同态加密、Shamir 秘密共享等的协议。

量子计算的出现使经典协议面临安全威胁,Shor 算法的提出对经典领域基于数学困难问题的安全多方计算提出了挑战。Bennett 和 Brassard 在 1984 年提出 BB84 量子密钥分发方案 [1]，开启量子密码学研究。与经典计算相比，量子计算提供了新的机制和工具，如量子纠缠、量子门、量子傅里叶变换，这些工具为设计安全的计算协议提供了更多的可能性。Crepeau 等人于 2002 年提出了量子多方安全计算协议 [2]，证明了可以在不信任的环境中实现安全的数据交换。Liu 等人 2012 年提出了基于 GHZ 态和基于 χ-Type 的隐私比较协议 [3] [4]，为安全多方计算问题提供了新的量子解决方案。2016 年，Shi 等人基于 QFT 构造了一个安全求和协议 [5]。2019 年，Ji 等人基于 d 级量子系统的纠缠交换构造了安全多方求和协议。近年来，越来越多的量子安全多方计算协议被研究出来，但多是基于量子门电路模型。量子图态在量子力学本身安全性的基础上增加了结构化的安全性，为量子安全多方计算提供了新的思路。

量子图态可以通过一个图（Graph）来表示，其中的节点代表单个的量子比特，而边则表示量子比特之间的纠缠关系。这种纠缠关系可以是多体的，而不仅仅是两体的，这使得量子图态比其他传统的量子纠缠态更为复杂，为构建量子安全多方计算协议提供了丰富的可利用资源。Raussendorf 在 2001 年最早提出了量子 Cluster 态的概念 [6]。在此基础上，Hein 等人 2004 年提出了基于量子图态的多体纠缠 [7]。2016 年，梁等人提出了基于量子图态的量子秘密共享协议 [8]，将矩阵分割法与图态相结合的思想应用到量子领域中。2019 年，田等人提出基于冗余图态的多人协作量子计算协议 [9]，利用一种特殊的图态结构实现了多人协作计算。2020 年 Dou 等人提出了基于量子图态的隐私比较和多方安全求和等协议 [10]，应用图态的一些基本测量性质实现了安全多方计算。

本论文在前人研究的基础上提出一种基于图态的多方安全求和，利用图态的特殊性质，选用随机的图态的结构和随机的加密门操作进一步提升计算的安全性。随机的图态结构是指在图态的构建过程中，每个参与者都随机选择自己的图态结构，而不是事先约定好的。在确认半诚实第三方（TP）收到量子比特之后，再公布图态结构。TP 根据不同的图态结构选择不同的测量方式恢复数据比特，这样可以防止传输过程中被量子攻击者截获信息。随机的加密门操作是指在加密量子比特过程中，每个参与者都随机选择自己的加密门操作，这样可以防止 TP 获取参与者的输入信息，而 TP 可以在不知道何种加密门操作的情况实现同态加密。这些方法都是基于量子图态本身的特殊性质，文章将会通过具体案例详细介绍这些性质如何发挥作用。文章设计了两个加密协议，分别是安全两方求和协议、安全多方求和协议。其实，在公布求和信息的情况下，安全两方求和是不存在的，因为其中任何一方都可以通过求和信息和自己的输入信息计算出另一方的输入信息。但是，通过两个协议的介绍，可以逐步理解如何应用量子图态实现多方安全计算，为以后扩展其他多方安全计算问题打下基础。

在文章结构上，第二章介绍了量子图态的基本性质；第三章介绍了三种量子安全多方计算协议的具体内容；第四章用一些具体的例子证明协议的正确的性和安全性；第五章用实验验证协议的有效性和实用性；第六章是总结与展望。

2 量子图态的基本性质

本文主要介绍量子图态的基本概念及其特殊的性质。量子计算和量子算法相关内容可以参考 Portugal 等人撰写的综述文章 [11]，近期量子计算相关技术可以参考 Huang 等

人撰写的综述文章 [12]。

2.1 量子门操作和量子测量

本文用到的量子门主要有以下几个：

- Hadamard 门：$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
- X 门：$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
- Y 门：$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
- Z 门：$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
- CZ 门：$CZ = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
- S 门：$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
- CNOT 门：$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

本文用到的测量基主要有以下几个：

- X 基：$\{|+\rangle, |-\rangle\}$
- Y 基：$\{|+i\rangle, |-i\rangle\}$
- Z 基：$\{|0\rangle, |1\rangle\}$

对于当前的量子计算机来说，Z 基测量相当于直接应用投影测量，测量结果为 0 或 1；X 基测量可以先应用 H 门再进行测量，即从 X 基变为 Z 基，Y 基测量可先应用 S 门和 H 门再进行测量。

2.2 量子图态的制备和稳定子

量子图态是由一堆顶点和边组成。顶点代表量子比特，边代表量子比特之间的纠缠关系。G=(V,E) 表示一个图，其中 V 表示顶点集合，E 表示边集合。对于任意一个顶点 $a \in V$，与其相邻的顶点 $b \in V$，有 $\{a,b\} \in E$。制备过程为：

1. 对所有的顶点，应用 H 门，成为 $|+\rangle$ 态；

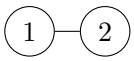
2. 对所有的边，应用 CZ 门，如 CZ_{ab}，使基成为纠缠态。

这样图态 $|G\rangle$ 就制备完成了。

$$|G\rangle = \left(\prod_{\{a,b\} \in E} CZ_{ab} \right) |+\rangle^{\otimes V}$$

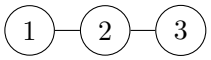
接下来我们介绍图态的稳定子表示法。稳定子对于理解图态非常有帮助，因为稳定子不仅可以用来描述图态的结构，还能揭示图态的一些性质。对于每一个顶点 $a \in V$, 设与之相连的顶点为 N(a)。顶点 a 对自身应用 X 门，对与之相连的结点 N(a) 应用 Z 门，则构成了顶点 a 的一个稳定子。有多少个顶点就有多少个稳定子，所有稳定子可以固定一个图态。对于图 G，其稳定子表示为 $S(G) = \{S_a | a \in V\}$，其中 $S_a = X_a \prod_{b \in N(a)} Z_b$。

对一个图态应用稳定子后，图态不变，即：$S_a |G\rangle = |G\rangle$。Dou 等人 [10] 根据稳定子的特性，让两个参与者分别选择 X 门和 Z 门加密数据，实现了两个数据的模 2 加法。下面举几个图态和稳定子的例子。形如：



这是最简单的图态，制备过程为对 $|00\rangle$ 应用 H 门和 CZ 门。$H_1 H_2 |00\rangle = |{+}{+}\rangle$. $CZ_{12} |{+}{+}\rangle = \frac{1}{\sqrt{2}}(|0\rangle |+\rangle + |1\rangle |-\rangle)$，基本的图态就制作完成了。从该表达式可以看出，对其应用 $X_1 Z_2$，结果为：$\frac{1}{\sqrt{2}}(|1\rangle |-\rangle + |0\rangle |+\rangle)$，显然与原式相等，所以其稳定子为 $X_1 Z_2$。同理，原式也可以展开为 $\frac{1}{\sqrt{2}}(|+\rangle |0\rangle + |-\rangle |1\rangle)$。显然，$Z_1 X_2$ 也是其稳定子。对式子进一步展开，最终结果为 $\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)$。这其中用到了量子门的基本原理，$X |0\rangle = |1\rangle, X |1\rangle = |0\rangle, Z |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + Z |1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle, Z |-\rangle = |+\rangle$。

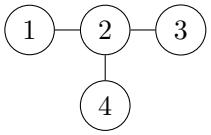
形如：



制备过程为 $H_1 H_2 H_3 CZ_{12} CZ_{23}$, 结果为：$\frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + |010\rangle - |011\rangle + |100\rangle + |101\rangle - |110\rangle + |111\rangle)$。稳定子为：

$$\begin{bmatrix} 1 & X_1 Z_2 I \\ 2 & Z_1 X_2 Z_3 \\ 3 & I Z_2 X_3 \end{bmatrix}$$

形如：



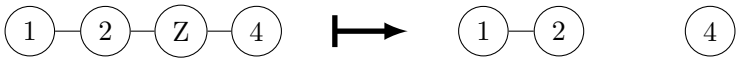
制备过程为 $H_1H_2H_3H_4CZ_{12}CZ_{23}CZ_{24}$, 结果为：$\frac{1}{4}(|0000\rangle+|0001\rangle+|0010\rangle+|0011\rangle+|0100\rangle-|0101\rangle-|0110\rangle+|0111\rangle+|1000\rangle+|1001\rangle+|1010\rangle+|1011\rangle-|1100\rangle+|1101\rangle+|1110\rangle-|1111\rangle)$。稳定子为：

$$\begin{bmatrix} 1 & X_1Z_2II \\ 2 & Z_1X_2Z_3Z_4 \\ 3 & IZ_2X_3I \\ 4 & IZ_2IX4 \end{bmatrix}$$

其他形式的图态类似。

2.3 量子图态的测量性质

下面介绍图态在 Z 基、X 基、Y 基下的测量性质。首先是基于 Z 基的测量，对于量子开发环境来说，直接在 $|0\rangle$、$|1\rangle$ 上进行测量。其性质如下：

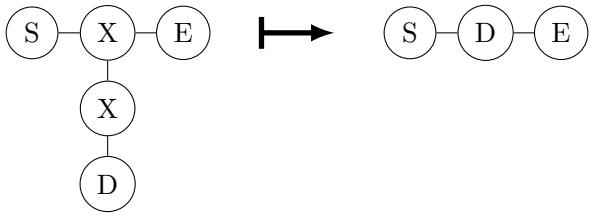


即对于某一个顶点应用 Z 基测量相当于断掉这个顶点所有的边。注意，如果测量结果为 0，则可以直接断掉边，变成新的图态，如果测量结果为 1，需要对与该顶点相连的顶点应用 Z 门，才能达到目标状态。形如上图的图态，其状态表示为：$\frac{1}{4}(|0000\rangle+|0001\rangle+|0010\rangle-|0011\rangle+|0100\rangle+|0101\rangle-|0110\rangle+|0111\rangle+|1000\rangle+|1001\rangle+|1010\rangle-|1011\rangle-|1100\rangle-|1101\rangle+|1110\rangle-|1111\rangle)$。当我们对 Z 基进行测量且结果为 0 时，容易发现，原状态坍缩为 $\frac{1}{2\sqrt{2}}(|0000\rangle+|0001\rangle+|0100\rangle+|0101\rangle+|1000\rangle+|1001\rangle-|1100\rangle-|1101\rangle)$，容易发现其与上图右边所示的图态一致。当测量结果为 1 时，原状态坍缩为 $\frac{1}{2\sqrt{2}}(|0010\rangle-|0011\rangle-|0110\rangle+|0111\rangle+|1010\rangle-|1011\rangle+|1110\rangle-|1111\rangle)$。对与之相连的 2、4 顶点比特应用 Z 门，变为 $\frac{1}{2\sqrt{2}}(|0010\rangle+|0011\rangle+|0110\rangle+|0111\rangle+|1010\rangle+|1011\rangle-|1110\rangle-|1111\rangle)$，与上图右边所示的图态一致。

其次，考虑图态在 X 基测量，对于量子开发环境来说，相当于先应用 H 门，再在 Z 基上进行测量。其性质如下：

即对于相连的两个顶点应用 X 基测量，相当于把与这两个顶点相连的其他顶点连接起来。注意，当两个顶点的测量结果均为 0 时，直接变成上图右边的图态。如果测量结果有 1 的情况需要应用一些门操作来修正以达到上图右边的状态。上图左边图态为 $\frac{1}{4}(|0000\rangle+|0001\rangle+|0010\rangle-|0011\rangle+|0100\rangle+|0101\rangle-|0110\rangle+|0111\rangle+|1000\rangle+|1001\rangle+|1010\rangle-|1011\rangle-|1100\rangle-|1101\rangle+|1110\rangle-|1111\rangle)$。对中间两个结点应用 H 门之后变为 $\frac{1}{4}(|0000\rangle+|0001\rangle+|0010\rangle+|0011\rangle+|0100\rangle-|0101\rangle-|0110\rangle+|0111\rangle+|1000\rangle-|1001\rangle-|1010\rangle+|1011\rangle+|1100\rangle+|1101\rangle+|1110\rangle+|1111\rangle)$。当两个顶点的测量结果均为 0 时，原状态坍缩为 $\frac{1}{2}(|0000\rangle+|0001\rangle+|1000\rangle-|1001\rangle)$，容易发现其与上图右边所示的图态一致。当两个顶点测量结果为 01 时，原状态坍缩为 $\frac{1}{2}(|0010\rangle+|0011\rangle-|1010\rangle+|1011\rangle)$，对第 1 个结点应用 Z 门，状态变为 $\frac{1}{2}(|0010\rangle+|0011\rangle+|1010\rangle-|1011\rangle)$，与上图右边所示的图态一致。当两个顶点测量结果为 10 时，原状态坍缩为 $\frac{1}{4}(|0100\rangle-|0101\rangle+|1100\rangle+|1101\rangle)$，对第 4 个结点应用 Z 门，则与上图右边所示图态一致。当两个顶点测量结果为 11 时，原

状态坍缩为 $\frac{1}{4}(-|0110\rangle+|0111\rangle+|1110\rangle+|1111\rangle)$，对第 1 个结点和第 4 个结点应用 X 门，则与上图右边所示图态一致。这样就用两个 X 基测量实现了图态的转换。下面考虑另一种图态的 X 基测量：



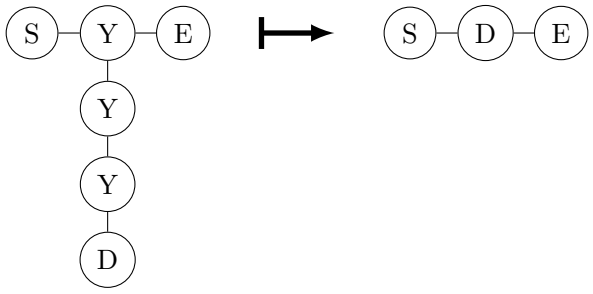
其证明方法与上一个图态类似，容易发现，当两个 X 基测量结果均为 0 时，直接变成上图右边的图态。当两个顶点测量结果为 01 时，需要对 S、E 应用 Z 门；当两个顶点测量结果为 10 时，需要对 D 应用 Z 门；当两个顶点测量结果为 11 时，需要对 E、D 应用 X 门。

再次，考虑图态在 Y 基上进行测量，对于量子开发环境来说，相当于先应用 Y 门和 H 门，再在 Z 基上进行测量。其性质如下：

容易推导，当三个 Y 基测量结果全部为 0 时，直接变成上图右边的图态；当第一个 Y 基测量结果为 1 时，需要对第 1 个顶点应用 X 门；当第二个 Y 基测量结果为 1 时，需要对第 1 个顶点和第 5 个顶点应用 X 门；当第三个 Y 基测量结果为 1 时，需要对第 5 个顶点应用 X 门。通过上述操作即可得到上图右边的图态。真值表如下：

$$\begin{bmatrix} I & 000 & 111 \\ X_1 & 100 & 011 \\ X_5 & 001 & 110 \\ X_1X_5 & 010 & 101 \end{bmatrix}$$

同样，我们考虑另一种图态的 Y 基测量：

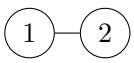


容易推导，当三个 Y 基测量结果全部为 0 时，直接变成上图右边的图态；当第一个 Y 基测量结果为 1 时，需要对顶点 S 应用 X 门；当第二个 Y 基测量结果为 1 时，需要对顶点 S 和顶点 D 应用 X 门；当第三个 Y 基测量结果为 1 时，需要对顶点 D 应用 X 门。通过上述操作即可得到上图右边的图态。真值表如下：

$$\begin{bmatrix} I & 000 & 111 \\ X_S & 100 & 011 \\ X_D & 001 & 110 \\ X_S X_D & 010 & 101 \end{bmatrix}$$

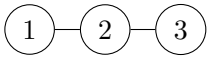
2.4 图态的编码

最后，我们来讨论一下，应用 X 门或者 Z 门来编码数据时，图态的变化。首先，我们来看一下，对于两个顶点的图态，应用 X 门或者 Z 门时，图态的变化。对于图态：



当我们对顶点 1 应用 X 门编码数据，对顶点 2 应用 Z 门加密数据时，容易发现，当数据为 00 时，即不做任何操作，图态不变，为 $\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)$，如果我们实施图态的逆操作，即先应用 CZ 门，再应用 H 门，结果为 $|00\rangle$。当数据为 10 时，对顶点 1 应用 X 门，图态变为：$\frac{1}{2}(|10\rangle + |11\rangle + |00\rangle - |01\rangle)$，对图态实施逆操作，先应用 CZ 门，结果为 $\frac{1}{2}(|10\rangle - |11\rangle + |00\rangle - |01\rangle)$，再应用 H 门，结果为 $|01\rangle$。当数据为 01 时，对顶点 2 应用 Z 门，图态变为：$\frac{1}{2}(|00\rangle - |01\rangle + |10\rangle + |11\rangle)$，对图态实施逆操作，结果为 $|01\rangle$。当数据为 11 时，对顶点 1 应用 X 门，对顶点 2 应用 Z 门，由图态的稳定子表示法可知，应用 $X_1 Z_2$ 之后，图态不变，结果为 $|00\rangle$。由此可知，对于这种编码方法，测量结果的模 2 加法与原数据的模 2 加法相同。用同样的方法可我们可以推导出来，对两个顶点采用 ZX 门、XX 门、ZZ 门编码数据均可以得到相同的结论。也就是说，对于两个顶点的图态，随机选择 X 门或者 Z 门来编码数据时，图态的测量结果与原数据的模 2 加法相同。这为两个参与者的隐私比较和安全求和提供了思路。

接下来推广到更一般的图态情况，我们来看一下，对于多个顶点的图态（以 3 个为例），应用 Z 门或应用 X 门会产生何种测量结果。对于图态：



当我们对顶点 2 应用 Z 门编码数据时，原图态变为：$\frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle - |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle - |111\rangle)$。应用图态的逆操作，图态变为：$|010\rangle$。测量结果与编码数据一致。当我们对顶点 2 应用 X 门编码数据时，原图态变为：$\frac{1}{2\sqrt{2}}(|010\rangle + |011\rangle + |000\rangle - |001\rangle + |110\rangle + |111\rangle - |100\rangle + |101\rangle)$。应用图态的逆操作，图态变为：$|101\rangle$, 即在原编码数据的基础上，进行了三个比特的位翻转，对于测量结果解码，可以通过三个比特的位翻转获得。对于 $|101\rangle$, 以第 2 个比特为中心，实现 123 比特的位翻转，即可获得原始数据于 $|010\rangle$。容易推导，对于多个量子比特，随机采用 X 门或者 Z 门编码数据的情况，Z 比特加密部分不用解码，对 X 比特加密部分应用比特位翻转，即可获得原始数据。随机的加密门操作，进一步提升了数据的安全性。

同样容易发现，这种加密、解密操作是模 2 加法同态的，即对于多条随机门操作加密的数据，其测量结果的模 2 加法经过解密后，与原始数据的模 2 加法相同。这为多个参与者的安全多方求和提供了思路。下面看一个简单的例子，对于数据 011010，采用 IXXIZI 编码，对于 001000，采用 IIXIII 编码，对于 011100，采用 IZXXII 编码。三个原始数据的模 2 加法为：011010+001000+011100=001110。第 1 个数据编码后，测量结

果为：111110，第 2 个数据编码后，测量结果为：010100，第三个数据编码后，测量结果为：001110。测量结果的模 2 加法运算为：111110+010100+001110=100100。对 100100 进行解码，首先第 1 个参与者进行解码，对于编码 IXXIZI，先对 123 比特应用位翻转，得到：011100，再对第 234 个比特应用位翻转，得到：000000。第 2 个参与者根据编码 IIXIII，对 234 比特应用位翻转，得到 011100。第 3 个参与者根据编码 IZXXII，对 234 比特应用位翻转，得到：000000，再对 345 比特应用位翻转，得到：001110，与原始数据的模 2 加法相同。这样就实现了三个参与者的安全多方求和。但直接应用这种方法，给 TP 提供了破解的可能，因为 TP 可以通过分析测量结果反推每个人的数据。实现真正的安全多方计算需要与其他加密解密方法结合起来，具体的方案将在下一节介绍。

3 基于图态的安全多方求和协议

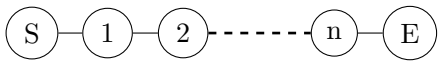
本节主要介绍基于图态的安全两方求和以及安全多方求和协议。两个协议均应用了图态的特殊性质实现同态加密，通过图态结构的复杂性、随机性，加密门操作的随机性进一步提升信息的安全性。

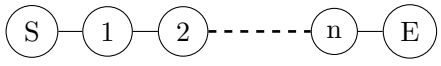
3.1 安全两方求和协议

协议描述：在 TP 的帮助下，Alice 和 Bob 对数据进行加密求和。TP 只知道最终的求和结果，但不知道 Alice 和 Bob 的具体数值。需要注意的是，TP 如果公布求和的结果，Alice 和 Bob 可以将求和结果与自己的数据进行减法，从而推断出另一方的数据。因此说，不存在安全的两方求和协议。本协议主要为理解安全多方求和协议作准备。当然我们也可以要求 TP 不公布求和结果，在某种应用场景下，实现两方的安全求和。例如某个工程项目由 TP 发标，因项目体量比较大，该领域任何一家单一企业无法独立完成，需要至少两家企业联合承包。如 Alice 和 Bob 考虑联合承包该项目，他们各自的目的是尽量使自己的数额较大以获取更多的利润，他们同时也希望联合的投标价格较低，以打败其他竞争者。在公布评标结果前，TP 知道 Alice 和 Bob 出价的总和以便和其他联合体进行比较，但三方均不知道其他方的数值。

设 Alice 持有的数据为 A=$\{a_i; i = 1, 2, \ldots\ldots, n; a_i \in \{0, 1\}\}$,B 持有的数据为 B=$\{b_i; i = 1, 2, \ldots\ldots, n; b_i \in \{0, 1\}\}$，目标为 TP 在不知道 A、B 具体数值的情况下得到 $f(A, B) = A \oplus B$。下面是协议的具体步骤：

step1: 制备和分发图态。TP 制备两组图态，每组图态包含 n+2 个量子比特，包括 S（start）比特和 E（end）比特，具体形式为：

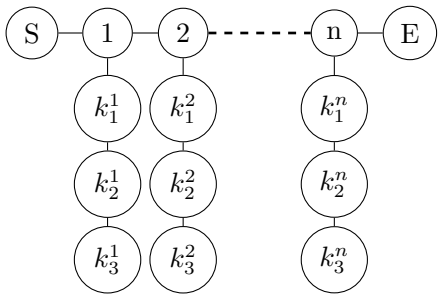




TP，将两组量子比特分别发送给 Alice 和 Bob，S 和 E 不发送。在发送时，TP 通过在其中添加诱饵比特、公布位置、测量并与阈值比较的方式保证量子信道的安全性。

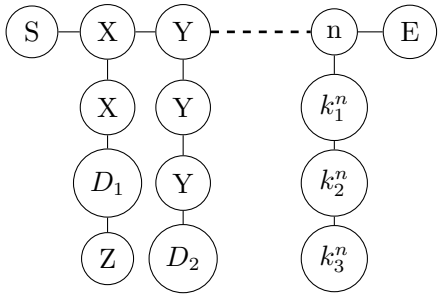
step2: 加密数据并编码图态。Alice 准备两组私钥分别为 $X_A = \{x_i; i = 1, 2, \ldots\ldots, n; x_i \in \{0, 1\}\}$，$Y_A = \{y_i; i = 1, 2, \ldots\ldots, n; y_i \in \{0, 1\}\}$。Bob 准备两组私钥，分别为 $X_B = \{x_i; i = 1, 2, \ldots\ldots, n; x_i \in \{0, 1\}\}$，$Y_B = \{y_i; i = 1, 2, \ldots\ldots, n; y_i \in \{0, 1\}\}$。Alice 和 Bob 先用 X 对数

据进行加密，得到秘密串 $S_A = A \oplus X_A; S_B = B \oplus X_B$。下面先考虑 Alice 的情况，Bob 与 Alice 类似。Alice 根据收到的量子比特制备自己的图态，结构如下：

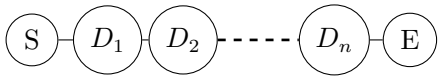


Alice 根据 Y 的值确定将数据加密到哪一个比特上，对于 $y_i = 0$，将数据加密到 k_2^i 上；对于 $y_i = 1$，将数据加密到 k_3^i 上。加密方法为：对于 $S_A^i = 0$，不做任何操作；对于 $S_A^i = 1$，对需要加密的比特随机应用 X 门或 Z 门。Alice 记录自己的加密方式，即记录一组 I、X、Z 的序列（共 n 个）。I 为 $S_A^i = 0$，X 或 Z 为 $S_A^i = 1$。Bob 用同样的方法加密数据并编码图态。Alice 和 Bob 将编码好的图态通过量子信道发送给 TP，期间通过加入诱饵比特的方式确保信道安全。

step3: 同态求和。TP 在确认收到所有比特后，Alice 和 Bob 公布 Y 的值，TP 根据 Y 的值对图态进行解码。对于 $y_i = 0$，TP 对 i、k_1^i 应用 X 基测量，对 k_3^i 应用 Z 基测量，保留 k_2^i 为 D（data）。对于 $y_i = 1$，TP 对 i、k_1^i、k_2^i 应用 Y 基测量，保留 k_3^i 为 D。形如下图的图态：



解码后，变成新的图态为：



具体的 X、Y、Z 基测量方法和对图态进行修正的方法请参考本文第二章节。得到新的图态后，TP 对 Alice 和 Bob 的图态进行逆操作、测量并对结果进行模 2 加法, 得到秘密串 $D = D_A \oplus D_B$。

step4: 解密。Alice 和 Bob 根据自己记录的加密序列（由 I、X、Y 组成的 n 个门操作）和 X_A、X_B 制作解密码。具体方法为，每出现一个 X 门，对 X_A、X_B 中相邻的 3 个比特应用位翻转。如 Alice 对第 i 个比特应用了 X 门，则对 $\{X_A^{i-1}$、X_A^i、$X_A^{i+1}\}$ 进行位翻

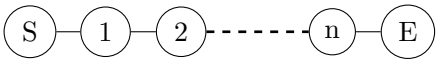
转，得到解密密钥 X'_A。Bob 根据自己的加密序列和 X_B 制作解密密钥 X'_B。最终的解密密钥通过 X'_A、X'_B 进行模 2 加法得到。即 $X' = X'_A \oplus X'_B$。如何计算 X' 可以有三种考虑，一是由 Alice 将 X_A 发送给 Bob，由 Bob 制作 X' 发送给 TP；二是 Alice 和 Bob 将 X'_A、X'_B 发送给半诚实的第三方 TP'，TP' 将计算好的 X' 发送给 TP。三是由 TP 将一组图态中的两个顶点分别发送给 Alice 和 Bob，Alice 和 Bob 根据自己的数据随机选用 X 门或 Z 门进行编码，TP 计算 Alice 和 Bob 解密密钥模 2 的和。

总之，TP 得到 X' 之后，可以对求和数据 D 进行解密，最终 $f(A,B) = D \oplus X'$。协议结束。

3.2 安全多方求和协议

协议描述：在 TP 的帮助下，对 n 个参与者 $P = \{P_k; k = 1, 2, \ldots\ldots, n\}$ 的数据进行加密求和。TP 和每个参与者只知道最终的求和结果，但不知道每个参与者的具体数据。本协议是在安全两方求和协议的基础上发展而来，在当前云计算、大数据的技术背景下，有广泛的应用场景。设 P_k 持有的数据为 $T^k = \{t_i^k; i = 1, 2, \ldots\ldots, n; t_i^k \in \{0,1\}\}$, 协议的目标是在不泄漏 T^k 的情况下得到 $f(T^1, T^2, \ldots\ldots T^n) = \overset{n}{\underset{k=1}{\oplus}} T_k$。下面是协议的具体步骤：

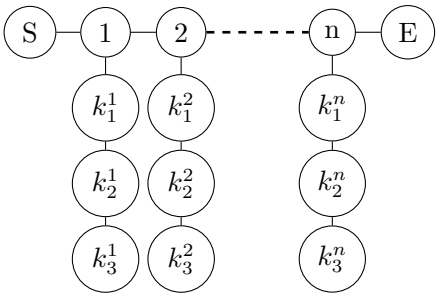
step1: 制备和分发图态。TP 制备 n 组图态，每组图态包含 n+2 个量子比特，包括 S（start）比特和 E（end）比特，具体形式为：



TP 随机确定参与者的顺序，将 n 组量子比特按顺序发送给每个参与者 P_k，S 和 E 不发送。在发送时，TP 通过在其中添加诱饵比特、公布位置、测量并与阈值比较的方式保证量子信道的安全性。

step2: 加密数据并编码图态。每个参与者 P_k 准备两组随机私钥分别为 $X_k = \{x_i^k; i = 1, 2, \ldots\ldots, n; x_i^k \in \{0,1\}\}$，$Y_k = \{y_i^k; i = 1, 2, \ldots\ldots, n; y_i^k \in \{0,1\}\}$。$P_k$ 用 X 对数据进行加密，得到秘密串 $S_k = T_k \oplus X_k$。根据 S_k 的值，P_k 准备第 3 组随机私钥 $Z_k = \{z_i^k; i = 1, 2, \ldots\ldots, n; z_i^k \in \{I, X, Z\}\}$，规则为：当 $S_i^k = 0$ 时，$z_i^k = I$；当 $S_i^k = 1$ 时，$z_i^k = \{X, Z\}$, 即为随机选择 X 门或 Z 门。以上三组私钥的功能为：X_k 用于对原始数据进行加密，防止 TP 在测量后通过推理获取原始数据；Y_k 用于随机选取图态结构，防止量子信道的窃听者获取数据；Z_k 用图态本身的性质加密数据，防止在经典信道窃听到解密密钥后盗取数据。接下来利用图态进行加密编码：

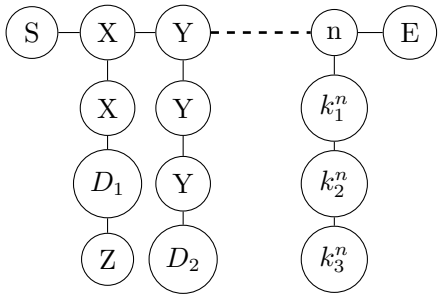
P_k 根据收到的量子比特制备自己的图态，结构如下：



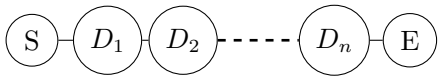
P_k 根据 Y 的值确定将数据编码到哪一个比特上，对于 $y_i = 0$，将数据编码到 k_2^i 上；

对于 $y_i = 1$，将数据编码到 k_3^i 上。加密方法为根据 z_i^k 的值 {I,X,Z} 对要编码的比特应用相应的门操作。P_k 将编码好的图态通过量子信道发送给 TP，期间通过加入诱饵比特的方式确保信道安全。

step3: 同态求和。TP 在确认收到所有比特后，所有参与者 P 公布 Y 的值，TP 根据 Y 的值对图态进行解码。对于 $y_i = 0$，TP 对 i、k_1^i 应用 X 基测量，对 k_3^i 应用 Z 基测量，保留 k_2^i 为 D_i（data）。对于 $y_i = 1$，TP 对 i、k_1^i、k_2^i 应用 Y 基测量，保留 k_3^i 为 D_i。形如下图的图态：



解码后，变成新的图态为：



具体的 X、Y、Z 基测量方法和对图态进行修正的方法请参考本文第二章节。得到新的图态后，TP 对每个参与者的图态进行逆操作，测量并对结果应用模 2 加法, 得到秘密串 $D = \overset{n}{\underset{k=1}{\oplus}} D^k$。

step4: 解密。P_k 根据 X_k 和 Z_k 制作解密码。具体方法为，如果 $z_i^k = X$, 对 X_k 中相邻的 3 个比特 $\{X_{i-1}^k、X_i^k、X_{i+1}^k\}$ 应用位翻转；如果 $z_i^k = Z$ 或 I，则不做任何操作，得到解密密钥 X_k'。n 个参与者 P 联合计算解密密钥 $X' = \overset{n}{\underset{k=1}{\oplus}} X_k'$。TP 将秘密串 D 通过经典信道随机传送给一个参与者 P_k，由参与者 P_k 对数据 D 进行解密 $D^1 = D \oplus X_k'$，然后将 D^1 传送给下一个参与者 P_{k+1}，由 P_{k+1} 对 D^1 进行解密 $D^2 = D^1 \oplus X_{k+1}'$，直到最后一个参与者 P_{k-1}，P_{k-1} 对 D^{n-1} 进行解密 $D^n = D^{n-1} \oplus X_{k-1}'$，最终得到 $D^n = D \oplus X'$。

TP 得到 X' 之后，可以对求和数据 D 进行解密，最终 $f(T^1, T^2, \ldots\ldots T^n) = D \oplus X'$。协议结束。

4 协议分析

接下来，我们对提供的协议进行分析，包括正确性分析和安全性分析，正确性分析通过理论推导和举例说明的方式分别分析；安全性分析主要介绍了协议如何抵御外部攻击和内部攻击。

4.1 正确性分析

安全两方求和是安全多方求和的一个特例，故本章节主要针对安全多方求和正确性进行分析。

4.1.1 理论分析

在安全多方求和协议中，我们最终得到的求和结果为 $f(T^1, T^2, \ldots\ldots T^n) = D \oplus X'$，我们需要验证 $D \oplus X' = \overset{n}{\underset{k=1}{\oplus}} T_k$。下面进行理论推导。我们定义一个操作 $\{U(H, J); H_i \in \{I, X, Z\}; J_i \in \{0, 1\}\}$, 其功能为根据 H_i 的信息，对 J_i 进行操作，当 $H_i = X$ 时，对 J_{i-1}、J_i、J_{i+1} 三个比特进行位翻转，容易发现 $U^2 = I$。

每个参与者原始数据为 T_k, 在 step2 中，首先应用 X 进行加密，$S_k = T_k \oplus X_k$。根据 Y 对图态结构的加密在 TP 解密后转化为同一结构，在正确性分析中可以不予考虑。根据 S_k, 参与者随机生成了 Z_k，随后通过编码图态传输给 TP，TP 又通过图态的逆操作及测量还原了数据。由第二章图态的性质可知，该过程实际上是应用了 $U(Z_k, S_k)$，由 U 的操作性质可知，$U(Z_k, S_k) = U(Z_k, T_k \oplus X_k) = T_k \oplus U(Z_k, X_k)$。因为对某个比特 Q 实施位翻转的过程，实际上是 $Q \oplus 1$ 的过程，也就是说实施 $U(Z_k, S_k)$ 实际上相当于某个 0、1 组成的字符串与 S_k 进行模 2 加法，即 $U(Z_k, S_k) = U(Z_k, \{0, 0, \ldots\ldots, 0\}) \oplus S_k$，故 $U(Z_k, S_k) = U(Z_k, T_k \oplus X_k) = T_k \oplus U(Z_k, X_k)$。

在 step3 中,TP 通过测量得到了秘密串 $D = \overset{n}{\underset{k=1}{\oplus}} D^k = \overset{n}{\underset{k=1}{\oplus}} U(Z_k, S_k) = \overset{n}{\underset{k=1}{\oplus}} U(Z_k, T_k \oplus X_k) = \overset{n}{\underset{k=1}{\oplus}} T_k \oplus U(Z_k, X_k)$ 。在 step4 中，每个参与者制作了解密密钥 $U(Z_k, X_k)$，n 个参与者联合制作了最终的解密密钥 $X' = \overset{n}{\underset{k=1}{\oplus}} U(Z_k, X_k)$。TP 实施解密 $f(T^1, T^2, \ldots\ldots T^n) = D \oplus X' = \left(\overset{n}{\underset{k=1}{\oplus}} (T_k \oplus U(Z_k, X_k))\right) \oplus \left(\overset{n}{\underset{k=1}{\oplus}} U(Z_k, X_k)\right) = \left(\overset{n}{\underset{k=1}{\oplus}} T_k\right) \oplus \left(\overset{n}{\underset{k=1}{\oplus}} U^2(Z_k, X_k)\right) = \overset{n}{\underset{k=1}{\oplus}} T_k$。

4.1.2 举例分析

设有三个参与者，P_1 持有的数据为 0101010,P_2 持有的数据为 0011010,P_3 持有的数据为 0110100，期望的求和结果 $f(T^1, T^2, T^3) = 0101010 \oplus 0011010 \oplus 01101000 = 0000100$。在 step2 中，3 个参与者分别随机生成私钥 $X_1 = 0100100$、$X_2 = 0101110$、$X_3 = 0010010$，3 个参与者对原始数据进行加密，$S_1 = T_1 \oplus X_1 = 0101010 \oplus 0100100 = 0001110$，$S_2 = T_2 \oplus X_2 = 0011010 \oplus 0101110 = 0110100$，$S_3 = T_3 \oplus X_3 = 0110100 \oplus 0010010 = 0100110$。根据 S 的值，三个参与者 P 制作密钥 Z，$Z_1 = IIIXXZI$、$Z_2 = IXXIZII$、$Z_3 = IXIIZXI$。在 step3，TP 获取测量结果，$D_1 = 0011100$、$D_2 = 1111100$、$D_3 = 1010001$，$D = D_1 \oplus D_2 \oplus D_3 = 0110001$。在 step4, 三个参与者分别计算解密密钥，$X_1' = 0110110$、$X_2' = 1100110$、$X_3' = 1100101$。三个参与者联合计算解密密钥 $X' = X_1' \oplus X_2' \oplus X_3' = 0110101$。TP 计算最终的求和结果，$f(T^1, T^2, \ldots\ldots T^n) = D \oplus X' = 0110001 \oplus 0110101 = 0000100$，与期望的求和结果一致。

4.2 安全性分析

基于图态的安全计算协议安全性保证主要基于图态结构的随机性和加密门操作的随机性。另外，由于图态的稳定子性质，一定程度的信道噪声可以通过稳定子予以修正。下面我们将分别对外部攻击和内部攻击进行分析。

4.2.1 外部攻击

外部攻击主要指的是窃听者对量子信道的攻击，窃听者可以通过纠缠测量、拦截重发、测量重发进行攻击。我们首先讨论协议 2，协议 1 是协议 2 的特例。在协议 2 中，主要通过四种方式保证信道安全，一是在量子数据传输前后加入了诱饵比特，Eve 的窃听行为会被发现，而数据的编码和解码工作是在确保量子信道安全之后才进行的，一旦发

现了 Eve，协议直接终止。二是在 step2，参与者根据 Y 的值采用随机的图态结构进行编码，即使窃听者 Eve 获取了所有比特，其无法知道哪些比特是相邻的，哪些比特是不相邻的，也不知道数据被加密到哪一个量子比特上，无法恢复原始图态结构。三是在 step2，参与者采用随机的 X 门和 Z 门编码数据，即使窃听者通过其他渠道（比如与 TP 合谋）获取了图态结构，也无法知道哪些应用了 X 门，哪些应用了 Z 门。四是在 step2，参与者 P 根据 X 的值对原始数据进行了加密，如果 Eve 通过其他渠道（比如与 TP 和部分参与者合谋）推断出哪些应用了 X 门，哪些应用了 Z 门，但不知道 X 的值也无法获取原始数据。通过上述四个手段，我们可以保证在协议 3 中即使窃听者 Eve 获取了所有比特，也无法获取原始数据。协议 1 的抵御外部攻击的方式与协议 2 类似。

4.2.2 内部攻击

对于协议 3，首先考虑一个参与者进行内部攻击，如果他直接窃听量子信道，他会被认为是外部攻击而被发现，外部攻击的四种情况同样适用他。考虑两个及以上参与者合谋，他们无法同时获取其他参与者的测量信息和解密密钥，因为测量信息是 TP 完成的，而解密密钥是由所有参与者联合计算的，故他们无法获取其他参与者的原始数据。考虑 TP 进行内部攻击，他可以获取所有参与者的测量信息和最终的解密密钥，但他无法获取某个参与者的解密密钥，所以他无法还原某个参与者的原始数据。对于协议 1，因为协议是安全两方的，如果 TP 与其中一个参与者合谋，将没有秘密可言。而两个参与者存在竞争关系，协议设计的基础就是两个参与者不能进行合谋。考虑其中一个参与者想要获取另一个参与者的信息或者求和信息，对于协议 1，因为他无法获取另一个参与者随机选择的图态结构和随机选择的编码门操作，所以他无法获取另一个参与者的信息。

5 实验验证

6 总结与展望

本文提出了一种新的基于图态的量子安全多计算协议，利用图态的特殊性质保证了数据的安全性。文章设计了两个加密协议，均是为了解决安全多方计算领域的经典问题。协议基于随机的图态结构、随机的门操作和随机的加密密钥，为数据安全提供了三重保护。文章提供了理论验证、举例验证、安全性分析和实验验证，充分证实了协议的正确性、安全性、实用性。在未来研究方面，可以考虑利用当前图态的基本性质解决其他安全多方计算的问题；可以进一步研究图态稳定子的性质，在存在噪声的信道中应用协议；可以考虑进一步拓展其他图态结构、研究其他图态性质，应用到量子安全多方计算中来；可以进一步研究图态和经典加密方式的结合，图态和基于纠缠的、基于门操作和基于 QFT 等其他量子安全多方计算方法的结合，进一步提高协议的安全性。

6.1 Lists of items

Lists may be laid out with each item marked by a dot:

- item one,
- item two.

Items may also be numbered in lowercase roman numerals:

(i) item one
(ii) item two

(a) Lists within lists can be numbered with lowercase roman letters,
(b) second item.

7 Equations

Displayed equations should be numbered consecutively in each section, with the number set flush right and enclosed in parentheses.

$$\mu(n,t) = \frac{\sum_{i=1}^{\infty} 1(d_i < t, N(d_i) = n)}{\int_{\sigma=0}^{t} 1(N(\sigma) = n) d\sigma} \,. \tag{1}$$

Equations should be referred to in abbreviated form, e.g. "Eq. (1)" or "(2)". In multiple-line equations, the number should be given on the last line.

Displayed equations are to be centered on the page width. Standard English letters like x are to appear as x (italicized) in the text if they are used as mathematical symbols. Punctuation marks are used at the end of equations as if they appeared directly in the text.

Theorem 1: Theorems, lemmas, etc. are to be numbered consecutively in the paper. Use double spacing before and after theorems, lemmas, etc.

Proof: Proofs should end with □.

8 Illustrations and Photographs

Figures are to be inserted in the text nearest their first reference. The postscript files of figures can be imported by using the commends used in the examples here.

Figures are to be sequentially numbered in Arabic numerals. The caption must be placed below the figure. Typeset in 8 pt Times Roman with baselineskip of 10 pt. Use double spacing between a caption and the text that follows immediately.

Previously published material must be accompanied by written permission from the author and publisher.

9 Tables

Tables should be inserted in the text as close to the point of reference as possible. Some space should be left above and below the table.

Tables should be numbered sequentially in the text in Arabic numerals. Captions are to be centralized above the tables. Typeset tables and captions in 8 pt Times Roman with baselineskip of 10 pt.

Table 1. Number of tests for WFF triple NA = 5, or NA = 8.

		NP			
		3	4	8	10
NC	3	1200	2000	2500	3000
	5	2000	2200	2700	3400
	8	2500	2700	16000	22000
	10	3000	3400	22000	28000

If tables need to extend over to a second page, the continuation of the table should be preceded by a caption, e.g. "(*Table 2. Continued*)."

10 References Cross-citation

References cross-cited in the text are to be numbered consecutively in Arabic numerals, in the order of first appearance. They are to be typed in brackets such as.

11 Sections Cross-citation

Sections and subsctions can be cross-cited in the text by using the latex command shown here. In Section 11, we discuss ....

12 Footnotes

Footnotes should be numbered sequentially in superscript lowercase Roman letters.[a]

Acknowledgements

We would thank ...

References

References are to be listed in the order cited in the text. For each cited work, include all the authors' names, year of the work, title, place where the work appears. Use the style shown in the following examples. For journal names, use the standard abbreviations. Typeset references in 9 pt Times Roman.

[a]Footnotes should be typeset in 8 pt Times Roman at the bottom of the page.

1. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, pp. 7–11, Dec. 2014.
2. C. Crepeau, D. Gottesman, and A. Smith, "Secure Multi-party Quantum Computing," June 2002. arXiv:quant-ph/0206138 titleTranslation: 安全多方量子计算.
3. W. Liu, Y.-B. Wang, Z.-T. Jiang, Y.-Z. Cao, and W. Cui, "New Quantum Private Comparison Protocol Using X-Type State," *International Journal of Theoretical Physics*, vol. 51, pp. 1953–1960, June 2012. titleTranslation: 使用 X -型态的新的量子私有比较协议.
4. W. Liu and Y.-B. Wang, "Quantum Private Comparison Based on GHZ Entangled States," *International Journal of Theoretical Physics*, vol. 51, pp. 3596–3604, Nov. 2012. titleTranslation: 基于 Ghz 纠缠态的量子保密比较.
5. R.-h. Shi, Y. Mu, H. Zhong, J. Cui, and S. Zhang, "Secure Multiparty Quantum Computation for Summation and Multiplication," *Scientific Reports*, vol. 6, p. 19655, Jan. 2016. Number: 1 Publisher: Nature Publishing Group.
6. R. Raussendorf and H. J. Briegel, "A One-Way Quantum Computer," *Physical Review Letters*, vol. 86, pp. 5188–5191, May 2001. Publisher: American Physical Society.
7. M. Hein, J. Eisert, and H. J. Briegel, "Multiparty entanglement in graph states," *Physical Review A*, vol. 69, p. 062311, June 2004. Publisher: American Physical Society.
8. 梁建武, 程资, 石金晶, and 郭迎, "基于量子图态的量子秘密共享," *物理学报*, vol. 65, pp. 160301–160301, Aug. 2016. Publisher: 物理学报.
9. 田宇玲, 冯田峰, and 周晓祺, "基于冗余图态的多人协作量子计算," *物理学报*, vol. 68, pp. 110302–7, June 2019. Publisher: 物理学报.
10. Z. Dou, X.-B. Chen, G. Xu, W. Liu, Y.-X. Yang, and Y. Yang, "An attempt at universal quantum secure multi-party computation with graph state," *Physica Scripta*, vol. 95, p. 055106, Mar. 2020. Publisher: IOP Publishing titleTranslation: 对具有图态的通用量子安全多方计算的尝试.
11. R. Portugal, "Basic Quantum Algorithms," Apr. 2023. arXiv:2201.10574 [quant-ph].
12. H.-L. Huang, X.-Y. Xu, C. Guo, G. Tian, S.-J. Wei, X. Sun, W.-S. Bao, and G.-L. Long, "Near-term quantum computing techniques: Variational quantum algorithms, error mitigation, circuit compilation, benchmarking and classical simulation," *Science China Physics, Mechanics & Astronomy*, vol. 66, p. 250302, May 2023. titleTranslation: 近期量子计算技术：变分量子算法、误差抑制、电路编译、基准测试和经典模拟.

Appendix A

Appendices should be used only when absolutely necessary. They should come after the References. If there is more than one appendix, number them alphabetically. Number displayed equations occurring in the Appendix in this way, e.g. (A.1), (A.2), etc.

$$\langle \hat{O} \rangle = \int \psi^*(x) O(x) \psi(x) d^3x \ . \tag{A.1}$$