**DOI:** 10.3969/j.issn.1007-5461. 2021.03.012

# 基于量子求和的安全多方量子排序协议

王蕊聪[1,2*]，冯 雁[1,3]

( 1 北京电子科技学院网络空间安全系， 北京 100070;
2 西安电子科技大学， 陕西 西安 710126;
3 中国科学技术大学， 安徽 合肥 230026 )

**摘 要:** 安全多方排序问题是保护用户隐私的安全多方计算中最为重要的核心问题之一。针对传统多方排序安全性低、易被窃取的问题, 提出了一种在半诚实模型下的安全多方量子排序协议, 该协议中各方基于量子傅立叶变换求和的方式参与计算, 在保密数值不被泄露的基础上获取排名。通过 IBM 提供的量子计算模拟器, 对协议的正确性进行了实验验证, 并对协议的安全性进行了理论分析。协议不仅为现有的量子排序提供了新思路, 而且很好地兼顾了公平性、有效性以及安全性。

**关 键 词:** 量子通信; 安全多方计算; 安全多方量子排序; 安全多方量子求和; 量子傅里叶变换

**中 图 分 类 号 :** TN918.1 **文 献 标 识 码 :** A **文章编号:** 1007-5461(2021)03-00354-11

# Secure multi-party quantum sorting protocol based on quantum summation

*WANG Ruicong*[1,2*]， *FENG Yan*[1,3]

( 1 Cyberspace Security Department, Beijing Electronic Science and Technology Institute, Beijing 100070, China;
2 Xidian University, Xian 710126, China;
3 University of Science and Technology of China, Hefei 230026, China )

Abstract: Secure multi-party sorting is one of the most important core issues in secure multi-party computing to protect user privacy. A secure multi-party quantum sorting protocol based on the semi-honest model is proposed to solve the problem of low security and eavesdropping of traditional multi-party sorting. In this protocol, each party participates in the calculation based on the sum of quantum Fourier transform and obtains the rank on the basis that the secret values are not leaked. Through the quantum computing simulator provided by IBM, correctness of the protocol is verified experimentally and security of the protocol is analyzed theoretically. The protocol not only provides a new idea for the existing quantum sorting, but also gives consideration to fairness, validity and security.

Key words: quantum cummunication; secure multi-party computation; secure multi-party quantum sorting; secure multi-party quantum summation; quantum Fourier transform

**基金项目:** Supported by National Key R & D Program of China (国家重点研发计划项目, 2018YFE0200600), Anhui Province Guidance Project of Quantum Communication and Quantum Computer Major Projects (安徽省量子通信与量子计算机重大项目引导性项目, AHY180500)

**作者简介:** 王蕊聪 ( 1995 - ), 女, 河南三门峡人, 主要从事网络安全, 量子密码方面的研究。 **E-mail:** 1193238657@qq.com

**收稿日期:** 2020–06–10; **修改日期:** 2020–10–19

*通信作者。

# 0　引　言

在安全多方计算执行的过程中, 计算可能发生在互不信任甚至互相竞争的多方中, 安全多方排序问题是信息保密的安全多方计算的核心问题之一, 其主要思想是: 假设有 $n$ 名参与者 $P_1$, $P_2$, $P_3$, $\cdots$, $P_n$, 每个参与者各自拥有一个秘密数值 $x_1$, $x_2$, $x_3$, $\cdots$, $x_n$, 他们希望在没有可信第三方的情况下, 能够设计出某种计算方式, 让所有参与者参与排序, 每个参与者可以安全获得自己秘密数值的排名, 且排名在各参与者之间也同样保密的一种安全方案。

目前, 国内外围绕安全多方排序开展了很多研究, 取得了不少研究成果。关于传统多方排序[1−3], 大多数采用了基于比较的排序思想, 即文献 [4] 中对百万富翁问题的自然推广, 人们针对这个问题, 利用传统的密码算法设计了各种能够提高排序效率的协议, 但却至少需要 $n\log n$ 次两方秘密比较, 计算开销大。文献 [5] 提出了随机化的安全希尔排序, 虽然以较高概率成功排序, 但该协议需要执行 $O(\log^2 n)$ 轮, 通信和计算开销较大。也有基于经典密码学的同态加密[6] 体制的保密排序方案, 以及基于大数分解 NP 问题的 RSA 密码体制[7] 设计的排序方案, 这些方案的安全性主要取决于计算机计算能力的强弱, 即随着攻击者计算能力的增强, 这些方案的安全性也会降低。与基于量子的安全多方排序相比, 传统多方排序方案都存着效率不高或安全性保障不强等问题。

量子密码与经典密码学对应的许多方面也得到了相应的研究, 如量子密钥分配协议[8−11]、量子秘密共享协议[12−14]、量子多方计算协议[15−18] 等。而关于量子化的排序问题, 文献 [19] 较早提出了利用形变量子化方法进行研究, 推导出排序相关分布函数的一般方法, 但只是从理论上分析了利用量子排序的可能性; 文献 [20] 设计了基于量子隐式模 $n+1$ 加法的保密排序协议, 但由于用到了特殊滤光器以避免不可见光子进入操作系统, 设备复杂度高, 实际应用实现难度大。

本文受到文献 [21] 中关于向量编码, 以及文献 [22] 中基于量子傅里叶变换的安全多方量子求和[23, 24] 的启示, 将向量编码与安全多方量子求和方法结合起来, 提出了一个新的安全多方量子排序协议, 该协议简单、安全且效率较高。

# 1　预备知识

## 1.1　安全性定义

安全多方计算一般只研究半诚实参与者模型下的保密计算问题。协议的计算过程要求参与者能够接触或观察到的内容只有输入和输出, 从而模拟协议的计算, 即参与者无法从中间数据中推导出任何有用的信息, 这样的协议过程可以认为是安全的。协议的安全性定义如图 1 所示, 假设有 $n$ 名参与者 $P_1$、$P_2$、$P_3$、$\cdots$、$P_n$, 每个参与者拥有秘密元素 $x_i \in \{x_1, x_2, x_3, \cdots, x_n\}$, 用 $f$ 表示一个 $n$ 元函数, 用 $f_i$ 表示函数 $f$ 的第 $i$ 个(其中 $i \in \{1, 2, \cdots, n\}$ ) 计算结果, 使用 $\pi$ 表示计算该函数的协议。每个参与者 $P_i$ 都会参与计算且想要在获得 $f_i$ 的同时不泄露自己的秘密数据 $x_i$。执行协议 $\pi$ 的时候 $P_i$ 得到的中间数据 $r_i$ 及所有信息可记为 $v_i^{\pi}$ 即 $(x_i, r_i, m_i^1, \cdots, m_i^t)$, 其中 $m_i^j$ 表示参与者 $P_i$ 第 $j$ 次所收到的信息。在执行完协议 $\pi$ 之后, 协议最终输出信息记为 $O^{\pi}$。根据文献 [25] 中的定义可知, 在半诚实参与者模型下, 计算函数 $f$ 的协议 $\pi$ 若存在概率多项式时间算法 $S$, 使得

$$\{S(x_i, f_i(x_1, x_2, \cdots, x_n)), f(x_1, x_2, \cdots, x_n)\} \overset{c}{\equiv} \{v_i^{\pi}(x_1, x_2, \cdots, x_n), O^{\pi}(x_1, x_2, \cdots, x_n)\} \tag{1}$$

成立, 其中 $\overset{c}{\equiv}$ 表示计算上不可区分, 则认为协议 $\pi$ 可以安全地计算函数 $f$。

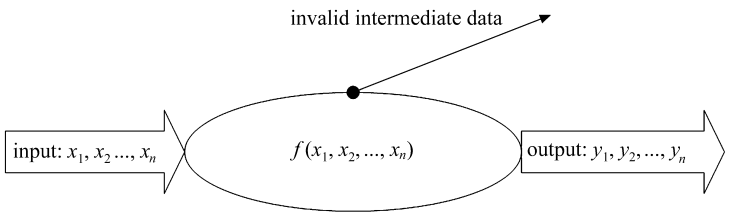


图 1 安全性定义图

Fig. 1 Diagram of security definition

### 1.2 安全多方量子求和

本方案用量子傅里叶变换方法进行多方安全求和, 以下为对该量子傅里叶变换的定义。对未知态 $|x\rangle$ 进行傅里叶变换, 定义为[22]

$$\mathrm{QFT}:\ |x\rangle \to \frac{1}{\sqrt{N}}\sum_{y=0}^{N-1}\exp\left(2\pi \mathrm{i}\frac{x}{N}y\right)|y\rangle\ , \tag{2}$$

对态 $|y\rangle$ 进行傅里叶逆变换, 定义为[22]

$$\mathrm{QFT}^{-1}:\ |y\rangle \to \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}\exp\left(-2\pi \mathrm{i}\frac{y}{N}x\right)|x\rangle\ , \tag{3}$$

且存在右边定义[22]

$$\sum_{y=0}^{N-1}\exp\left(2\pi \mathrm{i}\frac{x}{N}y\right)=\begin{cases}0 & \text{if } x\neq 0 \bmod N\\ N & \text{if } x=0 \bmod N\end{cases}\ . \tag{4}$$

基于态 $|y\rangle$ 进行傅里叶逆变换推导, 可得

$$\mathrm{QFT}^{-1}(\mathrm{QFT}\,|x\rangle)=|x\rangle\ . \tag{5}$$

在安全多方求和计算过程中每个参与者对自己收到的中间数据需要进行一个 $C_j$ 操作, $C_j$ 操作符定义为

$$C_j:|j\rangle_{\mathrm{t}}|x_i\rangle \to |j\rangle_{\mathrm{t}}U^j|x_i\rangle\ , \tag{6}$$

$$U|x_i\rangle=\exp\left(2\pi \mathrm{i}\frac{x_i}{N}\right)|x_i\rangle\ . \tag{7}$$

(6) 式中的下标 t 代表该粒子发送到量子信道中, $|j\rangle_{\mathrm{t}}$ 表示参与者从发起求和的发起者那里接受到的辅助量子态, 用以辅助求和计算。$|x\rangle_i$ 即为算符 $U$ 一个特征值为 $\exp(2\pi i x_i/N)$ 的特征向量。

根据量子傅里叶变换以及纠缠态纠缠交换的本质, 求和过程具体如下: 首先, 由多方量子求和的发起方对准备的随机态进行初始化傅里叶变换, 并将辅助态 $|j\rangle_{\mathrm{t}}$ 发送给第一个参与者, 由该参与者对 $|j\rangle_{\mathrm{t}}$ 进行 $C_j$ 操作, 随后将 $|j\rangle_{\mathrm{t}}$ 发送给下一个参与者, 每个参与者执行相同的过程, 最后一个参与者将 $|j\rangle_{\mathrm{t}}$ 返还给发起方, 由发起方执行傅里叶逆变换, 最终取得多方参与者和的取模结果 $\sum_{k=1}^{n}x_k \bmod N$, 其中 $N$ 为参与者参与计算的秘密数值的最大值。

## 2 安全多方量子排序协议

假设有 $N$ 个富翁 $P_1$、$P_2$、$P_3$、$\cdots$、$P_n$, 每个富翁 $P_i$ 的资产为 $s_i$ (其中 $s_1\neq s_2\neq s_3\cdots\neq s_n$), 每个富翁都想安全地知道自己的资产在所有富翁资产中的排名, 又不想向其他富翁泄漏自己的资产, 借鉴向量

编码和安全多方量子求和的思想, 将排序问题转化为求和问题, 所有参与者根据向量编码规则执行 $n$ 次多方求和协议, 从而确定各自的秘密在整个序列中的位置, 达到保密计算的效果。

所提出协议执行过程如下:

### 2.1 参与者准备阶段

1) 协议由 $n$ 个参与者 $P_1$、$P_2$、$P_3$、$\cdots$、$P_n$ (半诚实) 和一个第三方 $P_0$ (半诚实) 组成, 每个参与者拥有各自的秘密 $s_i$, 且 $s_i \in \{1,2,\cdots,n\}$。

2) $P_1$、$P_2$、$P_3$、$\cdots$、$P_n$ 各自拥有秘密 $s_i \in \{1,2,\cdots,n\}$, 每个参与者将各自的秘密数值 $s_i$ 用一个长度为 $N$ 的向量表示为 $\boldsymbol{V}_i = (x_{i1}, x_{i2}, \cdots, x_{in})$, 其中向量的编码规则为如果 $1 \le j < s_i$, 则 $x_{ij} = 0$; 若 $j \ge s_i$, 则 $x_{ij} = 1$, 其中 $1 \le j \le n$, 例如 $s = 5$、$n = 7$, 则根据向量编码规则表示为 $V_i = (0,0,0,0,1,1,1)$, 如果 $s_i = 1$, 则该向量用 $\boldsymbol{V}_i = (1_{i1}, 1_{i2}, \cdots, 1_{in})$ 表示。

3) 首先发起人 $P_0$ 准备一个 $m$-bit 长的随机的基态 $|x_0\rangle_{\rm h}$, 其中 $m = \log_2 N$ (其中 $N$ 为上述的向量长度) 且 $|x_0\rangle_{\rm h}$ 是 $P_0$ 的私有态, 然后 $P_0$ 对 $|x_0\rangle_{\rm h}$ 应用量子傅里叶变换得到

$$|\phi_1\rangle = {\rm QFT}|x_0\rangle_{\rm h} = \frac{1}{N}\sum_{j=0}^{N-1}\exp\left(2\pi{\rm i}\frac{x_0}{N}j\right)|j\rangle_{\rm h}\,. \tag{8}$$

4) $P_0$ 再准备另外一个 $m$-bit 的辅助态 $|0\rangle_{\rm t}$, 并对 $|\phi_1\rangle|0\rangle_{\rm t}$ 执行 $m$ 个 CNOT 门, 得到

$$\begin{aligned}|\phi_2\rangle = {\rm CNOT}^{\otimes m}|\phi_1\rangle|0\rangle_{\rm t} = {\rm CNOT}(1,m+1)\otimes{\rm CNOT}(2,m+2)\cdots\otimes\\ {\rm CNOT}(m,2m)\left[\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}\exp\left(2\pi{\rm i}\frac{x_0}{N}j\right)|j\rangle_{\rm h}|0\rangle_{\rm t}\right] = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}\exp\left(2\pi{\rm i}\frac{x_0}{N}j\right)|j\rangle_{\rm h}|j\rangle_{\rm t}\,,\end{aligned} \tag{9}$$

很显然 $|\phi_2\rangle$ 是个纠缠态, 下标 h 代表着该粒子是用户保留, 而下标 t 代表该粒子发送到量子信道中。

5) 每个参与者 $P_i$ 都根据自己的向量准备 $n$ 个私有粒子态 $|x_1\rangle_i$, $|x_2\rangle_i$, $|x_3\rangle_i$, $\cdots$, $|x_n\rangle_i$。

### 2.2 协议操作阶段

1) $P_0$ 将计算得到的 $m$-bit 粒子 (辅助量子态 $|j\rangle_{\rm t}$) 通过默认量子信道发送给 $P_1$。

2) $P_1$ 接收到辅助量子态 $|j\rangle_{\rm t}$, 首先准备自己的私有粒子态 $|x_1\rangle_1$, 然后对 $|j\rangle_{\rm t}|x_1\rangle_1$ 应用一个操作符 $C_j$, 其中 $|x_1\rangle_1$ 即为 $U$ 的一个特征值为 $\exp(2\pi i x_1/N)$ 的特征向量, 随即对整个 $P_0$ 和 $P_1$ 的复合量子系统进行一个 $C_j$ 操作 [(6)、(7) 式], 得到

$$|\phi_3\rangle = C_j\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}\exp\left(2\pi{\rm i}\frac{x_0}{N}j\right)|j\rangle_{\rm h}|j\rangle_{\rm t}|x_1\rangle = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}\exp\left(2\pi{\rm i}\frac{x_0+x_1}{N}j\right)|j\rangle_{\rm h}|j\rangle_{\rm t}|x_1\rangle\,. \tag{10}$$

3) $P_1$ 通过量子信道传送辅助态 $|j\rangle_{\rm t}$ 给 $P_2$, 将手中的 $|x_1\rangle_1$ 保留。$P_2$ 执行与 $P_1$ 类似的过程, 操作完后同样通过量子信道传送辅助态 $|j\rangle_{\rm t}$ 给 $P_1$。之后的每个用户均执行该过程, 如果每位用户均诚实执行操作过程, 会得到

$$|\phi_4\rangle = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}\exp\left(2\pi{\rm i}\frac{\sum_{k=1}^{n}x_k}{N}j\right)|j\rangle_{\rm h}|j\rangle_{\rm t}|x_1\rangle\cdots|x_n\rangle\,. \tag{11}$$

4) 最后, $P_n$ 发送辅助量子态 $|j\rangle_{\rm t}$ 给 $P_0$, $P_0$ 对其应用 $m$ 重 CNOT 门, 得到结果

$$|\phi_5\rangle = \ \mathrm{CNOT}^{\otimes m}|\phi_4\rangle = \mathrm{CNOT}^{\otimes m}\left[\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}\exp\left(2\pi\mathrm{i}\frac{\sum\limits_{k=1}^{n}x_k}{N}j\right)|j\rangle_{\mathrm{h}}|j\rangle_{\mathrm{t}}|x_1\rangle\cdots|x_n\rangle\right]=$$

$$\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}\exp\left(2\pi\mathrm{i}\frac{\sum\limits_{k=1}^{n}x_k}{N}j\right)|j\rangle_{\mathrm{h}}|0\rangle_{\mathrm{t}}|x_1\rangle\cdots|x_n\rangle\ . \tag{12}$$

至此, 协议参与者进行的操作阶段已经完成。

### 2.3 测量公布结果阶段

1) $P_0$ 在适当测量基上测量第二个 $m$-bit 位的粒子 ($|0\rangle_{\mathrm{t}}$), 如果测量的结果均为 $|0\rangle$, 则继续下一步, 否则认为可能存在第三方攻击者窃取并修改了中间数据, 立即结束本次交互。

2) $P_0$ 将傅里叶逆变换应用于第一个 $m$-bit 粒子, 得到 $|\omega\rangle$, 且 $|\omega\rangle = \sum\limits_{k=1}^{n}x_k \bmod N$。最后一步逆变换计算可表示为

$$\mathrm{QFT}^{-1}\left[\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}\exp\left(2\pi\mathrm{i}\frac{\sum\limits_{k=1}^{n}x_k}{N}j\right)|j\rangle_{\mathrm{h}}\right]=$$

$$\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}\exp\left(2\pi\mathrm{i}\frac{\sum\limits_{k=1}^{n}x_k}{N}j\right)\left[\frac{1}{\sqrt{N}}\sum_{l=0}^{N-1}\exp\left(-2\pi\mathrm{i}\frac{j}{N}j\right)|l\rangle_{\mathrm{h}}\right]=$$

$$\frac{1}{N}\sum_{j=0}^{N-1}\sum_{l=0}^{N-1}\exp\left(2\pi\mathrm{i}\frac{(\sum\limits_{k=1}^{n}x_k)-l}{N}j\right)|l\rangle_{\mathrm{h}}=$$

$$\frac{1}{N}\sum_{j=0}^{N-1}\left|\sum_{k=0}^{n}x_k \bmod N\right\rangle_{\mathrm{h}}+\frac{1}{N}\sum_{j=0\wedge l\neq\sum\limits_{k=1}^{n}x_k \bmod N}^{N-1}\left[\sum_{j=0}^{N-1}\exp\left(2\pi\mathrm{i}\frac{(\sum\limits_{k=1}^{n}x_k)-l}{N}j\right)\right]|l\rangle_{\mathrm{h}}=$$

$$\left|\sum_{k=0}^{n}x_k \bmod N\right\rangle_{\mathrm{h}}+\frac{1}{N}\sum_{j=0\wedge l\neq\sum\limits_{k=1}^{n}x_k \bmod N}^{N-1}0\cdot|l\rangle_{\mathrm{h}}=$$

$$\left|\sum_{k=0}^{n}x_k \bmod N\right\rangle_{\mathrm{h}}=|\omega\rangle_{\mathrm{h}}\ . \tag{13}$$

因此, 当参与者诚实地执行该协议, $P_0$ 将会正确地得到多方参与者的和的取模结果 $\sum\limits_{k=1}^{n}x_k \bmod N$。

3) $P_0$ 针对 $P_1$、$P_2$、$P_3$、$\cdots$、$P_n$ 各自拥有的向量 $\boldsymbol{V}=(x_{i1},x_{i2},\cdots,x_{in})$ 按列重新调用协议操作阶段 2.2 和协议测量公布阶段 2.3, 即除去协议准备阶段外重新执行一遍协议。则 $P_0$ 最终可获得一段数字序列: $\sum\limits_{i=1}^{n}x_{i1} \bmod N$, $\sum\limits_{i=1}^{n}x_{i2} \bmod N$, $\sum\limits_{i=1}^{n}x_{i3} \bmod N$, $\sum\limits_{i=1}^{n}x_{i4} \bmod N$ $\cdots$。虽然上述量子多方加法做的是取模运算, 但由于参与者取 $x_i$ 向量之后的单列向量之和一定小于 $N$, 所以对 $N$ 的取模运算可以得到 $n$ 个参与者单列的和。

4) $P_0$ 将该数字序列公布, 该序列即为 $s_i$ 的由小至大的升序排序序列, 各参与者寻找与 $s_i$ 相等的序列号, 该序列号对应的数值即为各参与者的排名。

理论上, 该方案适用于整数 $N$ 确定后, 任意不大于 $N$ 的参与者, 均可使用该方案获得参与者秘密数据在所有参与者数据中的排名。

## 3　实验验证

使用量子计算云平台 IBM Q Experience 上的模拟器对本协议核心量子求和部分的正确性进行验证, 即将量子计算过程转化为量子可逆逻辑电路[26,27], 在模拟器上设计出实验电路图, 根据实验结果确定本协议执行的正确性。

### 3.1　实验量子电路图

基于文献 [28], 验证重点是关于量子傅里叶变换理论计算到逻辑电路的实现, 量子傅里叶变换即作用在空间 $C^{2^n}$ 上的离散傅里叶变换, 其把一组标准正交基 $\{|x\rangle\}$ 用另一组标准正交基 $\{|y\rangle\}$ 表示: $Y = UX$。此处 $\boldsymbol{U}$ 即为量子傅里叶变换的核心操作, 即作用在 Hilbert 空间中任意矢量上的变换矩阵 $\boldsymbol{U}_{\mathrm{QFT}}$, 该矩阵可拆分为一系列逻辑门。一个量子比特的量子傅里叶变换就是单个 H 门操作, 多量子位态空间上的傅里叶变换就是对 H 门的推广。将任意量子态制备成叠加态, 从而进行酉变换完成指数级加速。根据方案中的量子多方求和方法设计量子电路, 完成关于安全多方量子排序的验证。

验证: 当参与者数目 $m = 4$, 参与者拥有私密数据 $1 \le n < 8$, 即 $N = 7$, 假设有参与者 $P_1$、$P_2$、$P_3$、$P_4$, $P_1$ 所拥有秘密数值是 6, $P_2$ 是5, $P_3$ 是3, $P_4$ 是7。实验电路如图 2~4 所示, 其中 $q$[6]、$q$[7]、$q$[10]、$q$[11] 分别表示参与者 $P_1$、$P_2$、$P_3$、$P_4$, $q$[3]、$q$[4]、$q$[5] 则为辅助量子比特, 第三方测量位 $P_0$ 用 $q$[0]、$q$[1]、$q$[2] 表示。

1) $P_1$、$P_2$、$P_3$、$P_4$ 各个用户将各自的秘密用一个长度为 $N$ 的向量表示, 其生成的二维向量分别为: $\boldsymbol{V}_1 = (0,0,0,0,0,1,1)$、$\boldsymbol{V}_2 = (0,0,0,0,1,1,1)$、$\boldsymbol{V}_3 = (0,0,1,1,1,1,1)$、$\boldsymbol{V}_4 = (0,0,0,0,0,0,1)$。由此可知, 需要进行 7 次求和计算, 并公布计算结果, 方可得出 4 个参与者的排名。

2) $P_0$ 开始初始化, 进行傅里叶变换并用 CNOT 门添加辅助量子进行辅助检测, 电路图如图 2 所示。

3) 参与者依次通过 $C_j$ (这里使用 CNOT 门和 Toffoli 门分割量子态)向下复合, 并将结果传回给 $P_0$。此处以参与者输入手中拥有的数字 1、1、1、0 为例, 电路图如图 3 所示。

4) $P_0$ 通过执行 CNOT 门变换及傅里叶逆变换, 并最终对 $q$[0]、$q$[1]、$q$[2] 进行测量并收集结果, 电路图如图 4 所示。

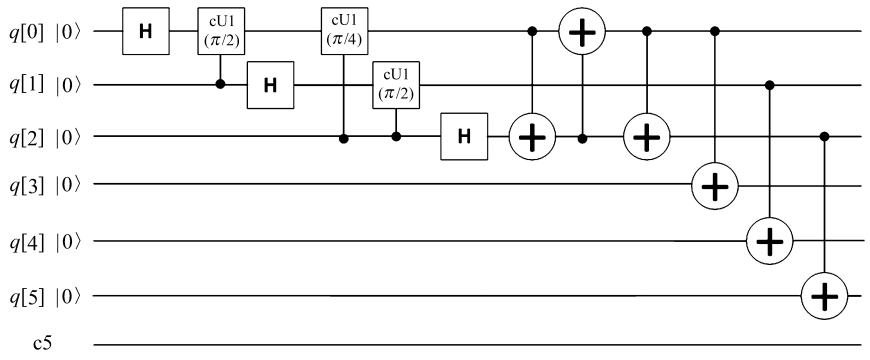


图 2　量子傅里叶变换和 CNOT 门初始化

Fig. 2　Quantum Fourier transform and initialization of CNOT gate circuit

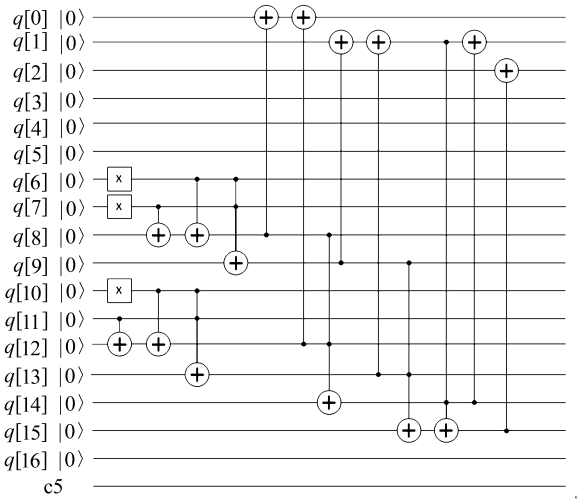


图 3 实验电路图

Fig. 3 Diagram of experimental circuit

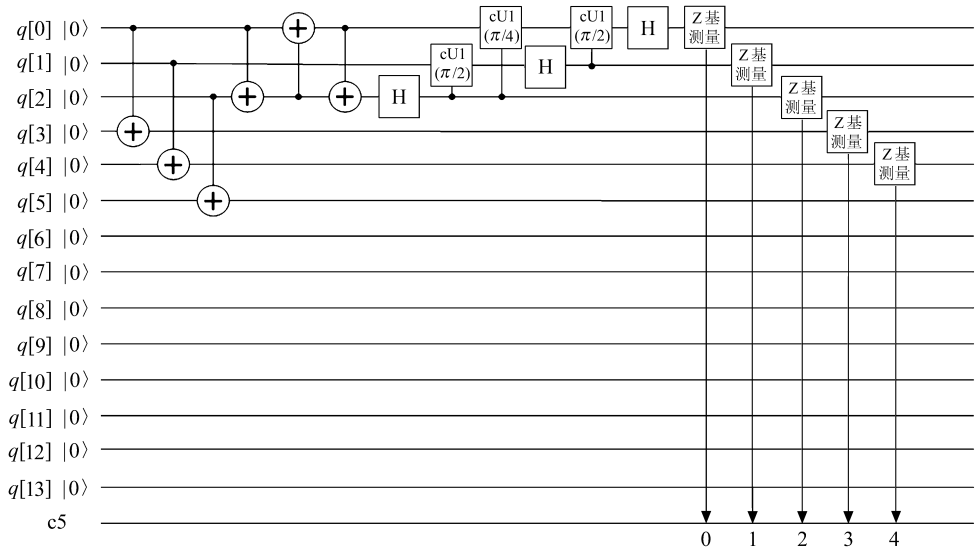


图 4 傅里叶逆变换和测量电路

Fig. 4 Inverse Fourier transform and measurement circuit

参与者输入手中拥有的数字 1、1、1、0 的理论计算结果: $S = \sum_{i=1}^{4} y_i \bmod 8 = (1 + 1 + 1 + 0) \bmod 8 = 3$, 电路实验结果如图 5 所示 (该图由实验平台对电路图运行结果所得)。其中纵坐标代表得到横坐标对应

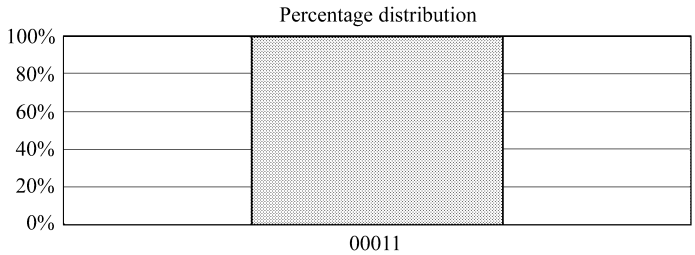


图 5 实验结果

Fig. 5 Experimental results

数字的概率, 此处为 100%, 得到 00011; 横坐标表示的二进制数, 其中前两位表示辅助测量位 (如果辅助测量位均为 0 则表示实验电路没有受到参与者重复操作攻击), 后三位都表示结果位, 按照二进制进行解读, 其中 011, 转化成十进制即代表 3, 与理论计算结果相等, 所以实验结果正确。

### 3.2　实验结果分析

分别改变参与者输入为 0、0、0、0, 0、0、1、0, 0、1、1、0, 1、1、1、0 以及 1、1、1、1 得到计算结果, 并绘制结果如图 6, 其中横坐标代表的二进制编码表示的是依次按列调用排序协议得到的统计结果, 将二进制编码转化成十进制即为排名信息分布, 纵坐标代表计算的每一列, 例如纵坐标 5 表示第 5 列计算结果对应 010 (十进制数为 2)。

至此 $P_0$ 只需将该数据公布, 各参与者把自己的数字当做编号, 对照查看自己的排名 (由小至大)。例如参与者 $P_1$ 秘密数字为 6, 查看纵坐标 6 对应横坐标排名为 3, 所以根据参与者 $P_1$、$P_2$、$P_3$、$P_4$ 的秘密数字为 6、5、3、7, 其所得到的排名分别为 3、2、1、4。

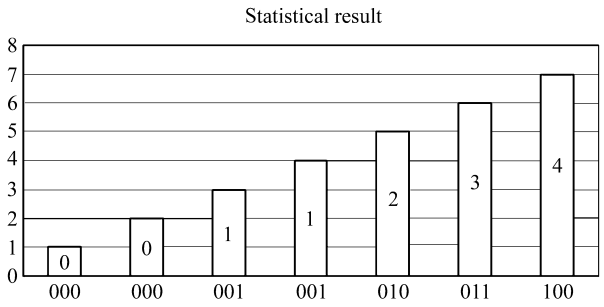


图 6　计算结果分布

Fig. 6　Distribution of calculation results

## 4　安全性分析

### 4.1　内部参与者攻击

由协议可知, $P_1$ 无法得到关于 $P_0$ 私有秘密 $s_1$ 的任何信息, 因为 $P_0$ 只向 $P_1$ 发送了辅助量子比特 $|j\rangle_{\rm t}$, 其中没有任何有用信息, 现在对 $P_1$ 和 $P_2$ 进行分析, 分两种情况: 一种是参与者对第三方发送过程的中间数据进行攻击, 一种是参与者对其他参与者进行攻击。

1) $P_1$ 测量辅助量子比特 $|j\rangle_{\rm t}$, 显然他可以以相同概率 $1/N$ 得到 $|j\rangle$ ($j\in\{0,1,\cdots,N-1\}$) , 然而测量结果 $j$ 与 $P_0$ 手中的纠缠态没有关系, 也无法推导出更多数据, 因此这样的攻击无效。

2) 在将 $U$ 操作算子应用于辅助比特 $|j\rangle_{\rm t}$ 后, $P_2$ 再次测量它。$P_2$ 知道 $P_1$ 的秘密状态 $|x_1\rangle$ 已经进化成与 $|j\rangle_{\rm t}$ 相同的状态。基于量子傅里叶变换的辅助态 $|j\rangle_{\rm t}$, 他可以在辅助态 $|j\rangle_{\rm t}$ 上执行量子傅里叶逆变换, 期望提取 $|x_1\rangle$。其攻击描述可表示为

$$\begin{aligned}{\rm QFT}^{-1}\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}\exp\left(2\pi{\rm i}\frac{x_1}{N}j\right)|j\rangle_{\rm h}|j\rangle_{\rm t}=\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}\exp\left(2\pi{\rm i}\frac{x_1}{N}j\right)|j\rangle_{\rm h}{\rm QFT}^{-1}|j\rangle_{\rm t}=\\ \frac{1}{N}\sum_{l=0}^{N-1}\sum_{j=0}^{N-1}\exp\left(2\pi{\rm i}\frac{x_1-l}{N}j\right)|j\rangle_{\rm h}|l\rangle_{\rm t}\,.\end{aligned}\tag{14}$$

通过上述推导, 如果 $P_2$ 测量辅助状态, 他会以等概率 $1/N$ 得到 $|l\rangle_{\rm t}$ ($l\in\{0,1,\cdots,N-1\}$)。这意味着 $P_2$ 无法获得任何关于 $P_1$ 的秘密信息, 因为他不能从具有下标 h 和 t 的纠缠量子系统的部分量子位中提取全局

相位信息。事实上, 任何局部酉算子都是如此 (除非直接测量), 否则部分量子位不能完全分离复合系统的纠缠。因此, 即使 $P_2$ 执行这种攻击, 他仍然无法得到任何关于 $P_1$ 的私密信息 $|x_1\rangle$。

### 4.2 截取-重发攻击

协议采用对协议 2.2 中步骤 3)、4) 和协议 2.3 中步骤 1) 中的辅助量子比特进行检测, 来避免截取-重发攻击。在协议中, 参与者事实上并没有将自己的私有数据通过量子信道传送, 而是将自己的私有态通过 $U$ 操作与初始量子系统进行复合得到纠缠态, 再根据适当的傅里叶逆变换操作来得到求和结果。假设有攻击者通过量子信道获取 $P_0$ 所发送的中间数据 $|j\rangle_t$, 攻击者得到的中间数据只有 $|j\rangle_t$, 攻击者一旦对其进行测量, 由于该复合系统是纠缠的, 就会对 $P_0$ 手中拥有的量子态进行塌缩, 在协议 2.3 步骤 1) 中 $P_0$ 对复合系统进行 CNOT 门还原, 再对 $|j\rangle_t$ 进行测量, 理论上, 如果没有攻击者攻击, 可以测得 $|j\rangle_t$ 为 $|0\rangle_t$, 但是由于攻击者攻击, 使之前的数据塌缩, $P_0$ 可以正确获得 $|j\rangle_t$ 刚好为 $|0\rangle_t$ 的概率为 $1/2^N$, 所以 $P_0$ 会发现信息被窃取, 可以立即停止当前协议, 废除数据, 重新开始协议进行计算。同理, 攻击者对 $P_1$ 及其它参与者采取这样的攻击都适用上述分析, 因此, 理论上协议可以抵御截取-重发攻击。

## 5 结 论

将多方排序问题转化为求和问题, 基于量子傅里叶变换求和设计出一种安全多方量子排序协议, 以求取一组秘密数据的排序序列, 参与者可获得自己对应的排名, 且该排名不会被其他参与者知晓。相较于其他量子排序协议, 所提出协议只需要执行 $O(n)$ 轮次就能够得到排名, 一定程度上降低了通信和计算开销。通过在 IBM Q 平台上对协议进行验证, 可知此协议执行正确有效。同时, 此协议还能够抵御恶意攻击者的截取-重发攻击, 以及 $n-2$ 名以下参与者的联合攻击。

**参考文献:**


[1] Cheng C, Luo Y L, Chen C X, *et al*. Research on secure multi-party ranking problem and secure selection problem [C]. *International Conference on International Conference on Web Information Systems and Mining*, 2010: 79-84.

[2] Wang N, Gu H M, Zheng T. A practical and efficient secure multi-party sort protocol [J]. *Computer Applications and Software*, 2018, 35(10): 305-311.
王 宁, 顾昊旻, 郑 彤. 一种实用高效的安全多方排序协议[J]. 计算机应用与软件, 2018, 35(10): 305-311.

[3] Li S D, Zhang X P. Secure multi-party computation protocol for sorting problem [J]. *Journal of Xi'an Jiaotong University*, 2008, 42(2): 231-233, 255.
李顺东, 张选平. 排序问题的多方保密计算协议[J]. 西安交通大学学报, 2008, 42(2): 231-233, 255.

[4] Yao A C. Protocols for secure computations [C]. *Annual Symposium on Foundations of Computer Science*, 1982, 54: 160-164.

[5] Goodrich M T. Zig-zag sort: A simple deterministic data-oblivious sorting algorithm running in O(nlogn) time [C]. *Proceedings of the Annual ACM Symposium on Theory of Computing*, 2014, 46: 684-693.

[6] Xiao Q, Luo S S, Chen P, *et al*. Research on secure multi party scheduling problem under semi honest model [J]. *Acta Electronica Sinica*, 2008, 36(4): 709-714.
肖 倩, 罗守山, 陈 萍, 等. 半诚实模型下安全多方排序问题的研究[J]. 电子学报, 2008, 36(4): 709-714.

[7] Qiu M, Luo S S, Liu W, *et al*. Using RSA cryptosystem to solve secure multi party multi data sorting problem [J]. *Acta Electronica Sinica*, 2009, 37(5): 1119-1123.
邱 梅, 罗守山, 刘 文. 利用 RSA 密码体制解决安全多方多数据排序问题[J]. 电子学报, 2009, 37(5): 1119-1123.

[8] Shi B S, Jiang Y K, Guo G C. Manipulating the frequency-entangled states by an acoustic-optical modulator [J]. *Physical Review A*, 2000, 61(6): 064102.

[9] Xue P, Li C F, Guo G C. Addendum to efficient quantum-key-distribution scheme with nonmaximally entangled states [J]. *Physical Review A*, 2002, 65(3): 034302.

[10] Yang Y G, Wen Q Y, Zhu F C. Optimal inclusive teleportation of a *d*-dimensional two particle unknown quantum state [J]. *Chinese Physics B (English Version)*, 2006, 15(5): 907-911.

[11] YangY G, Wen Q Y, Zhu F C. An efficient two step quantum key distribution protocol with orthogonal product states [J]. *Chinese Physics B (English Version)*, 2007, 16(4): 910-914.

[12] Cleve R, Gottesman D, Lo H K. How to share a quantum secret [J]. *Physical Review Letters*, 1999, 83(3): 648-651.

[13] Lu H, Zhang Z, Chen L K, *et al*. Secret sharing of a quantum state [J]. *Physical Review Letters*, 2016, 117(3): 030501.

[14] Ain N U. A novel approach for secure multi-party secret sharing scheme via quantum cryptography [C]. *2017 International Conference on Communication, Computing and Digital Systems (C-CODE). IEEE*, 2017: 112-116.

[15] Shi R H. *Research on Quantum Secret Sharing and Other Multi-Party Quantum Cryptography Protocols* [D]. Hefei: University of Science and Technology of China, 2011.
石润华. 量子秘密共享及其它多方量子密码协议研究[D]. 合肥: 中国科学技术大学, 2011.

[16] Majumder A, Mohapatra S, Kumar A. Experimental realization of secure multiparty quantum summation using five-qubit IBM quantum computer on cloud [J]. *2017, arXiv*: 1707. 07460.

[17] Zhong H, Huang L S, Luo Y L. Multi candidate electronic election scheme based on secure multi-party summation [J]. *Computer Research and Development*, 2006, 43(8): 1405-1410.
仲 红, 黄刘生, 罗永龙. 基于安全多方求和的多候选人电子选举方案[J]. 计算机研究与发展, 2006, 43(8): 1405-1410.

[18] Zhang Y H. *Research on the Choice of Protecting Private Information* [D]. Anhui: Anhui University, 2014.
张永华. 保护私有信息的选择问题研究[D]. 安徽: 安徽大学, 2014.

[19] Zhang H X, Lu Z C. The ordering problem of quantization [J]. *Journal of Hangzhou University (Natural Science Edition)*, 1997, 24(3): 226-229.
张洪宪, 陆志成. 量子化的排序问题[J]. 杭州大学学报(自然科学版), 1997, 24(3): 226-229.

[20] Liu W, Wang Y B. Research on secure multiparty quantum scheduling problem [J]. *Acta Physica Sinica*, 2011, 60(7): 53-60.
刘 文, 王永滨. 保密多方量子排序问题的研究[J]. 物理学报, 2011, 60(7): 53-60.

[21] Qian X Q. *Research on Secure Multiparty Ordering* [D]. Anhui: Anhui University, 2013.
钱小强. 安全多方排序的研究[D]. 安徽: 安徽大学, 2013.

[22] Shi R H, Mu Y, Zhong H, *et al*. Secure multiparty quantum computation for summation and multiplication [J]. *Scientific Reports*, 2016, 6(1): 28-34.

[23] Yang H Y, Ye T Y. Secure multi-party quantum summation based on quantum Fourier transform [J]. *Quantum Information Processing*, 2018, 17(6): 1-17.

[24] Du J Z, Chen X B, Wen Q Y, *et al*. Secure multiparty quantum summation [J]. *Acta Physica Sinica*, 2007, 56(11): 6214-6219.
杜建忠, 陈秀波, 温巧燕, 等. 保密多方量子求和[J]. 物理学报, 2007, 56(11): 6214-6219.

[25] Overill R E. Review: Foundations of cryptography, volume II: Basic applications [J]. *Journal of Logic and Computation*, 2005, 15(3): 218-229.

[26] Shen M Y, Cheng X Y, Guan Z J, *et al*. Realization method of two-dimensional nearest neighbor for quantum circuits [J]. *Chinese Journal of Quantum Electronics*, 2019, 36(4): 476-482.
沈鸣燕, 程学云, 管致锦, 等. 一种量子线路二维近邻实现方法[J]. 量子电子学报, 2019, 36(4): 476-482.

[27] Dai J, Li Z Q, Pan S H, *et al*. Deutsch-Jozsa algorithm realization based on IBM Q [J]. *Chinese Journal of Quantum Electronics*, 2020, 37(2): 202-209.
戴 娟, 李志强, 潘苏含, 等. 基于 IBM Q 的 Deutsch-Jozsa 算法实现[J]. 量子电子学报, 2020, 37(2): 202-209.

[28] Wei J, Ni M, Zhou M, *et al*. Research of quantum algorithm based on IBM Q platform [J]. *Computer Engineering*, 2018, 44(12): 6-12.
卫 佳, 倪 明, 周 明, 等. 基于 IBM Q 平台的量子算法研究[J]. 计算机工程, 2018, 44(12): 6-12.

# “轨道角动量: 从经典光学到量子信息” 专辑征稿

自 1992 年 Allen 等理论确认了光子轨道角动量的物理存在以来, 轨道角动量的制备、调控及应用已成为国际光学前沿研究的一门新兴学科。从经典光学领域的新型光通信体制、光学微操控、新颖光学成像, 到量子光学领域的高维量子信息编码、新型的量子信息协议、量子精密测量等, 轨道角动量都展示出独特的魅力和诱人的应用前景。

为促进光轨道角动量领域相关专家学者以及研究人员的学术交流, 反映该领域的最新研究进展与前沿动态, 并从专业的视角对该领域所面临的未来挑战及发展趋势进行客观、全面的展望, 在主编郭光灿院士的倡议下, 《量子电子学报》拟于 2022 年第 1 期出版 “轨道角动量: 从经典光学到量子信息” 专辑, 现面向全国征集相关领域的综述、评论与原创研究论文, 欢迎赐稿!

**特邀专栏主编**:

史保森, 中国科学技术大学物理学院二级教授, 中国光学学会光量子科学与技术专委会委员。曾入选教育部 “新世纪优秀人才支持计划”, 获得国家基金委杰出青年基金支持。从事量子信息、非线性光学、集成光学及量子光学的理论和实验研究, 近年来在Nat.Photon.、Nat. Commun.、PRL/X等著名学术刊物以第一/通信作者发表论文 100 余篇。获中国光学学会光学科技奖一等奖 (排名第一) 和安徽省自然科学一等奖 (排名第一) 及 2014、2016 和2018 年中科院优秀导师奖。

贾晓军, 山西大学光电研究所、量子光学与光量子器件国家重点实验室教授, 博士生导师。国家杰出青年基金获得者。主要从事各种波长非经典光场的产生及应用、量子纠缠操控等方面的研究。先后在 Sci. Adv.、Nat. Common.、Phys. Rev. Lett. 等物理学重要学术刊物上发表论文 80 余篇。主持国家杰出青年科学基金项目、国家优秀青年科学基金项目、国家重点研发课题、国家自然科学基金项目等。获山西省自然科学奖一等奖 2 项。

陈理想, 厦门大学教授、博士生导师, 物理科学与技术学院副院长, 教育部 “国家级人才计划” 青年学者。主要从事光场调控及应用研究, 已以通讯作者/第一作者在 Phys. Rev. Lett.、Light Sci. Appl.、Optica 等发表系列论文, 研究工作被美国物理学会 Physics 网站和英国物理学会 Physics World 网站等亮点报道。曾获中国光学学会 “饶毓泰基础光学奖”(二等奖)、中国激光杂志社 “中国光学重要成果”、中国物理学会 “萨本栋应用物理奖”, 主持基金委重点项目等。

**征稿范围**:

1. 光轨道角动量制备的方法、技术与器件; 2. 轨道角动量光波的传播规律及测量方法; 3. 基于轨道角动量的傅里叶光学与光信息处理; 4. 基于超颖材料的轨道角动量光场调控; 5. 轨道角动量调控与非线性光学效应; 6. 轨道角动量光量子调控与高维量子信息协议; 7. 轨道角动量光量子调控与量子成像技术; 8. 轨道角动量光量子调控与精密测量方法

**截稿日期**: 2021 年 9 月 30 日

**投稿方式**:

登录网址http://lk.hfcas.ac.cn，点击 “作者投稿查稿系统” 进入, 按要求填写相关信息并上传稿件 (稿件题目中标注 “轨道角动量: 从经典光学到量子信息” 专题投稿)。投稿模板及其他材料请见期刊首页 “相关下载”。

**联系方式**:

Tel: 0551-65591564; E-mail: lk@aiofm.ac.cn