求解最小公倍数问题的量子安全多方计算协议

李子贤[1)] 刘文杰[1),2),3)]

[1)](南京信息工程大学软件学院 南京 210044)

[2)](江苏省大气环境与装备技术协同创新中心 南京 210044)

[3)](江苏省先进计算与智能服务工程研究中心 南京 210044)

摘 要 最小公倍数是解决很多数学问题的基础工具,在隐私保护的情况下如何对其进行多方协同计算具有一定的研究价值.部分经典安全多方计算协议虽然能够求解该问题,但计算复杂度为指数级.本文通过将最小公倍数问题转化为求多个周期函数的连接函数的周期,提出了一个基于量子周期查找算法的最小公倍数协议,将复杂度降为多项式级.在协议中,发起方对每个参与方发送一个粒子.每个参与方对粒子施加一个 Oracle 操作,其中 Oracle 函数的周期即各自的私有整数.然后,发起方通过运行量子周期查找算法来计算出连接函数的周期,即各自整数的最小公倍数.为了防御共谋和伪造攻击,采用星-环混合拓扑结构对粒子发送方进行诚实性检验.由于量子周期查找算法存在一定的失败概率,设计了一个量子匿名输出检验协议来检验最小公倍数结果的正确性.安全性分析表明了该协议在恶意模型下具有无条件安全性,且协议的计算复杂度和通信复杂度分别为 $O(n^3m^2\log(nm))$ 和 $O(n^2m\log(nm))$,均为多项式级.此外,该协议具有较好的扩展性,可应用于安全多方最大公约数计算、有理数求和、最值计算等问题.

关键词 量子计算;量子信息;安全多方计算;最小公倍数;量子周期查找算法;匿名输出检验;隐私计算

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2024.01393

Quantum Secure Multi-Party Computation Protocols for Solving Least Common Multiple Problem

LI Zi-Xian[1)] LIU Wen-Jie[1),2),3)]

[1)](*School of Software, Nanjing University of Information Science and Technology, Nanjing* 210044)

[2)](*Jiangsu Collaborative Innovation Center of Atmospheric Environment and Equipment Technology, Nanjing* 210044)

[3)](*Jiangsu Province Engineering Research Center of Advanced Computing and Intelligent Services, Nanjing* 210044)

Abstract Least common multiple (LCM) is a basic tool to solve many mathematical problems. It is worth to research how to calculate the LCM of multi parties collaboratively with privacy protection. Some classical secure multi-party computation protocols can solve this problem, but the computational complexity is exponential. In this paper, by transforming the LCM problem into finding the period of the connection of multiple periodic functions, an LCM protocol based on the quantum period-finding algorithm (QPA) is proposed, which reduces the complexity to polynomial level. In the protocol, the initiator sends a quantum register to each other participant. Each participant applies an Oracle operator on the register, where the Oracle function's period is the party's own private integer. Finally, the initiator runs QPA to obtain the period of the connection function, i.e., the LCM of all private integers. In order to defend collusion and forgery attacks,

收稿日期:2023-05-04;在线发布日期:2024-04-07.本课题得到国家自然科学基金(62071240)、科技创新 2030—"量子通信与量子计算机"重大项目(2021ZD0302901)、江苏省研究生科研创新计划项目(KYCX23_1370)、江苏省自然科学基金(BK20231142)资助.**李子贤**,硕士研究生,主要研究方向为量子密码通信、量子安全多方计算.E-mail:zixianli157@163.com.**刘文杰**(通信作者),博士,副教授,中国计算机学会(CCF)会员,主要研究方向为量子密码通信、量子安全多方计算、量子机器学习.E-mail:wenjiel@163.com.

we use a star-ring hybrid topology structure to test the honesty of the register sender. Since QPA has a certain failure probability, we design a quantum anonymous output validation protocol to validate the correctness of the LCM results. Security analysis shows that the proposed protocol is unconditionally secure under malicious model. Its computational complexity and communication complexity are $O(n^3m^2\log(nm))$ and $O(n^2m\log(nm))$, respectively, which are polynomial. In addition, the proposed protocol has good scalability, and can be applied to implement secure multi-party greatest common divisor computation, fraction summation, maximum (minimum) computation, etc.

Keywords quantum computation; quantum information; secure multi-party computation; least common multiple; quantum period-finding algorithm; anonymous output validation; privacy computing

1 引 言

安全多方计算(Secure Multi-party Computation, SMC)指两个或更多参与者利用各自的秘密信息作为输入,协同进行的保密计算,并且保证每一方仅获取自己的计算结果,无法通过计算过程中的交互数据推测出其他任意一方的秘密信息.自1982年Yao[1]提出安全多方计算的概念以来,安全多方计算迅速发展起来,并成为了现代密码学和网络安全领域不可或缺的一部分,保护了日益膨胀的网络数据的隐私安全.安全多方计算的主要问题包括安全科学计算[1-7]、安全几何计算[8-12]、安全集合计算[13-18]、安全数据挖掘[19,20]、安全统计分析[21,22]等等.

最小公倍数(Least Common Multiple, LCM)是初等数论、计算机科学、密码学等中重要的函数,其有着重要的应用,如有理数加法中通分需要求分母的最小公倍数.因此,研究LCM的安全多方计算具有一定的意义.2018年,杨晓艺等人[6]通过素因子分解将LCM的计算转化为求每个素因子的指数的最小值和最大值,从而应用安全多方最大值计算技术提出了相应的计算协议,这也是目前仅有的有关LCM的SMC计算思路.然而,杨晓艺等的方法虽然思路简洁,但并不高效,因为其复杂度依赖于素因子的选择.设涉及的整数最大为$N=2^m$,根据素数定理,小于N的素数数量为$\pi(N)\approx\frac{N}{\ln N}$,则为了完全覆盖所有可能的素因子,该方案起码要考虑$\frac{N}{\ln N}\geq\frac{N}{\sqrt{N}}=\sqrt{N}=2^{\frac{m}{2}}$个素因子的指数,从而复杂度达到了指数级.

实际上,对任意N以内的正整数x,y,存在公式$\mathrm{lcm}(x,y)=\frac{xy}{\gcd(x,y)}$,其中gcd表示最大公约数.如果不考虑安全性,那么,由于最大公约数的计算可以使用Euclidean算法在多项式时间内完成,因此LCM的计算只需要多项式复杂度.然而,该方法有几个缺陷:(1)对于$n>2$的多方计算,需要两两用该公式计算最小公倍数;(2)该公式仅适用于两个整数,无法简单地推广至$n>2$的多方计算;(3)计算两数乘积会直接泄露整数本身;(4)尚不存在安全的最大公约数计算方案.为了高效且安全地计算LCM,我们需要新的方法.

虽然尚未被严格证明,但量子计算机被认为具有超越经典计算机的计算能力.对于没有太多内部结构的问题,量子计算很难做到非凡的加速,比如对大小为$N=2^m$的无序数据库的搜索问题,Grover算法[23]只能降低复杂度到$O(2^{\frac{m}{2}})$.但对于特定问题,其可以达到指数级加速,比如Deutsch-Jozsa算法[24]能以$O(1)$复杂度区分单比特输出函数是常值的还是平衡的,Simon算法[25]能以$O(m)$复杂度得到m比特输入函数的异或周期,以及著名的Shor算法[26,27]能以$O(m^2\log^2 m)$复杂度分解m比特大数的素因子.Shor算法的核心是一个量子周期查找算法(Quantum Period-finding Algorithm, QPA)[28],可以在$O(\log m)$次Oracle操作内获得任意m比特函数的整数周期,这是已知的任何经典算法都做不到的.实际上,若将多个周期函数连接起来构成一个新的函数,则新函数也是周期函数,而且周期正好是各个周期的LCM.我们基于此原理提出了一种计算LCM的量子SMC(QSMC)协议.

基于环状拓扑结构的量子协议很难抵抗恶意攻击中的共谋攻击(Collusion attack),而基于星型拓

扑的协议很难抵抗伪造攻击(Forgery attack)，因此我们设计了一种星-环混合拓扑(Star-ring hybrid topology)结构来防御这种攻击. 当粒子的发送方满足非共谋条件时，该拓扑结构允许对任何一方提供的粒子进行验证，从而测试发送方的诚实性. 另一方面，由于 QPA 是概率性的算法，因此其应用到 SMC 中就要保证每个参与方都能检验计算出的结果，且仅在每个人都检验通过时才结束协议，并且不泄露每个人的检验结果，我们称这种过程为“匿名输出检验(Anonymous Output Validation，AOV)”. 该过程在数学上等价于逻辑乘(Logical AND，LA)问题和匿名否决(Anonymous Veto，AV)问题，其主要区别在于 AOV 问题必须在单次执行下具有确定性，而 LA 和 AV 问题没有这种要求. 2022 年，Shi 等人[29]基于相位匹配量子密钥分发提出了第一个量子多方 LA 协议，并基于该协议给出了一个多方交集基数计算协议. 然而，在该协议的预计算过程中，为了成功分发相同的密钥，需要多次对 n 个随机比特做相位匹配，直到全部相等为止，其耗费时间较大. 在匿名否决 AV 问题上，2015 年，Rahaman 等人[30]提出了第一个量子 AV(QAV)协议，然而其具有较多的安全性漏洞，并且需要多次迭代才能达到确定性. 2021 年，Wang 等人[31]通过引入半诚实第三方解决了前者的一些漏洞，然而其具有概率性，存在理论失败概率. 2022 年，Mishra 等人[32]在上述文献的基础上进行了深入探索，并给出了 7 个 QAV 协议，然而其中具有单次执行确定性的协议只有一个，并且有可能泄露否定票数. 为了实现一个符合 AOV 问题要求的协议，同时不泄露票数信息，我们使用安全多方求和来进行多方逻辑乘计算. Shi 等人[33]曾于 2016 年提出了一种量子安全多方加法协议(Secure Multi-party Quantum Summation，SMQS)，用于对多个整数进行安全求和，其通信复杂度和计算复杂度均是多项式级，而且是无条件安全的. 我们将 Shi 的 SMQS 协议改造为一个 AOV 协议，并引入一个非共谋的第三方，将其改造为星-环混合拓扑，从而允许协议的每个参与方保密地对计算出的结果进行正确性检验，并且不泄露总检验通过数，实现更高的安全性.

基于上述工作，我们给出了一个高效计算 LCM 的量子 SMC 协议. 主要工作内容如下：

(1) 提出了星-环混合拓扑结构，通过引入一个非共谋第三方，部分量子 SMC 协议在改造为该结构后可以同时对抗共谋攻击和伪造攻击；

(2) 提出了匿名输出检验问题，并设计了一个量子匿名输出检验协议. 该协议只在所有人都检验通过时才顺利通过，而且不泄露任何检验结果，甚至包括检验通过的数量；

(3) 利用上述两个工具构建了一个可行的求解 LCM 问题的量子 SMC 协议，在恶意模型下具有无条件安全性，并且具有较低的计算与通信复杂度；

(4) 提出了 LCM 协议的一些扩展应用，包括安全多方最大公约数计算、有理数求和、最值计算.

本文第 2 节介绍预备工作，包括约定一些符号、给出基本的定义，回顾经典 LCM 计算协议与已有量子 LA、AV 协议，并介绍 QPA 算法和 Shi 的 SMQS 协议；第 3 节首先提出星-环混合拓扑和一个匿名输出检验协议，然后基于此提出我们的 LCM 计算协议；第 4 节对提出的协议进行正确性、安全性和复杂度分析；第 5 节基于 LCM 协议提出了几个扩展应用；第 6 节总结全文.

2　预备工作

2.1　符号约定

本文中用到的一些符号的含义见表 1.

表 1　一些符号及其含义

符号	含义
n	协议参与人数
$[\![n]\!]$	集合 $\{1,2,\cdots,n\}$
$N=2^m$	输入整数的上限和比特数
$\log N$	$\log_2 N$
u,v	函数的输入和输出比特数
$[N]$	集合 $\{0,1,2,\cdots,N-1\}$
A°	集合 A 的奇数子集
$x\|y$	x 是 y 的因子
$x\equiv y(\bmod 2^m)$	$2^m\|(x-y)$
$D(X,Y),D(\rho,\sigma)$	随机变量 X,Y，量子态 ρ,σ 的迹距离
$X\overset{S}{\equiv}Y,\rho\overset{S}{\equiv}\sigma$	随机变量 X,Y，量子态 ρ,σ 统计不可区分
$\underset{i\in A}{\operatorname{lcm}}(x_i)$	$x_i,i\in A$ 的最小公倍数
$\|\Psi\rangle_h$	粒子 h 处于态 $\|\Psi\rangle$
$x\|\|y$	比特串 x,y 连接的新串
(h,t)	粒子 h,t 组成的复合系统
$\lfloor x\rfloor,\lceil x\rceil$	向下取整和向上取整
$\Pr[A]$	事件 A 发生的概率
$f^{-1}(y)(f:A\to B)$	解集 $\{x\|x\in A,f(x)=y\}$
$\mathbb{Z}$	整数集

此外，本文中用到的酉变换如下(用于描述的量子系统 h,t 均为 m 量子比特)：

(1) Hadamard 变换 $\mathrm{H}^{\otimes m}$：对每个比特施加 Hadamard 门：

$$\mathrm{H}^{\otimes m}:|x\rangle_h\rightarrow\frac{1}{\sqrt{2^m}}\sum_{j\in[2^m]}(-1)^{j\cdot x}|j\rangle_h,$$

其中 $j\cdot x=j_{m-1}x_{m-1}\oplus j_{m-2}x_{m-2}\oplus\cdots\oplus j_0x_0$ 表示 m 比特串 j,x 之间的内积;

(2)复制门 $\mathrm{CNOT}^{\otimes m}$:对于 $\forall i\in[n]$,以 h 的第 i 个比特为控制位,t 的第 i 个比特为目标施加受控非门:

$$\mathrm{CNOT}^{\otimes m}:|a\rangle_h|b\rangle_t\rightarrow|a\rangle_h|a\oplus b\rangle_t;$$

(3)量子傅里叶变换 QFT 和逆变换 $\mathrm{QFT}^\dagger$:

$$\mathrm{QFT}:|x\rangle_h\rightarrow\frac{1}{\sqrt{2^m}}\sum_{j\in[2^m]}e^{\frac{\sqrt{-1}2\pi xj}{2^m}}|j\rangle_h,$$

$$\mathrm{QFT}^\dagger:|x\rangle_h\rightarrow\frac{1}{\sqrt{2^m}}\sum_{j\in[2^m]}e^{-\frac{\sqrt{-1}2\pi xj}{2^m}}|j\rangle_h;$$

(4)相位门 U_+、指数门 C_j 和模乘法门 $\mathrm{U}_{\times q}$[33]:

$$\mathrm{U}_+:|x\rangle_h\rightarrow e^{\frac{\sqrt{-1}2\pi x}{2^m}}|x\rangle_h,$$

$$\mathrm{C}_j:|j\rangle_h|x\rangle_t\rightarrow|j\rangle_h\mathrm{U}_+^j|x\rangle_t=e^{\frac{\sqrt{-1}2\pi xj}{2^m}}|j\rangle_h|x\rangle_t,$$

$$\mathrm{U}_{\times q}:|j\rangle_h\rightarrow|jq\bmod 2^m\rangle_h,$$

其中 $q\in[2^m]^\circ$是奇数,因此模 2^m 乘法可逆.

2.2 基本定义

定义 1. 最大公约数与最小公倍数. 对于任意正整数 $x_1,x_2,\cdots,x_n$,最大公约数 $\gcd\limits_{i\in[n]}(x_i)$ 为满足 $\forall i\in[\![n]\!]$, $\gcd\limits_{i\in[n]}(x_i)\mid x_i$ 的最大正整数,最小公倍数 $\mathrm{lcm}\limits_{i\in[n]}(x_i)$ 为满足 $\forall i\in[\![n]\!], x_i\mid\mathrm{lcm}\limits_{i\in[n]}(x_i)$ 的最小正整数.

定义 2. 最小公倍数(LCM)问题. 设有 n 个参与方 $P_1,P_2,\cdots,P_n$,分别有私有整数 $x_1,x_2,\cdots,x_n$. LCM 问题定义如下:

(1)输入:$\forall i\in[\![n]\!]$,P_i 输入 x_i;

(2)输出:$y=\mathrm{lcm}\limits_{i\in[n]}(x_i)$;

(3)安全要求:每个 P_i 除得到 $\mathrm{lcm}\limits_{i\in[n]}(x_i)$ 外,不得到其他信息.

定义 3. 匿名输出检验(AOV)问题. 设一个有 n 方参与的 SMC 问题 P 具有如下性质:

(1)当输出结果不正确时,$P_1,P_2,\cdots,P_n$ 中至少存在一方可以察觉其不正确(或者当这种不正确很明显时,例如在 LCM 问题中,如果结果不是公倍数,很容易被发现,但如果是公倍数而并非最小,则无法被察觉).

(2)$P_1,P_2,\cdots,P_n$ 中如果有一方公开指出结果不正确,则它的私有信息会存在一定泄露(例如当 P_i 指出结果不是公倍数时,意味着他的输入整数里含有结果不包含的因子).

那么,对于问题 P 的匿名输出检验问题 AOV(P)的定义为:

(1)输入:$P_1,P_2,\cdots,P_n$ 分别具有私有布尔值 $c_1,c_2,\cdots,c_n\in\{0,1\}$,其中,若 P_i 检验到 P 的输出不正确,则 $c_i=0$,否则令 $c_i=1$;

(2)输出:$y=\prod\limits_{i\in[\![n]\!]}c_i$;

(3)安全要求:每个 P_i 除了得到 $\prod\limits_{i\in[\![n]\!]}c_i$ 外,不得到其他信息. 注意,在与其类似的匿名否决(AV)问题中,只要求保护每个人的输入,但对于总否定票数没有要求,从而可能不满足该要求.

(4)其他要求:在 AOV(P)的单次执行中,若参与方均正确执行协议,则应以 100% 概率获得正确结果.

在上述定义中,(2)是因为在 AOV 问题中所有人必须全部检验通过才认为结果正确,而有任何人发现不正确就不行. 显然,其在数学上等价于多方逻辑乘(LA)问题和匿名否决(AV)问题,即只有输入全部为 1 时结果才是 1,否则是 0;(4)是因为作为一个输出检验程序,其本身的正确性不应存在争议(即理论上不应具有失败概率),并且无法多次重复(防止被篡改),因此应当具有单次执行的完全确定性.

2.3 经典最小公倍数协议回顾

2018 年,杨晓艺等人[6]提出了一个基于门限解密的最大值计算协议,n 个参与方可以通过该协议保密地计算出他们各自私有整数的最大值,而不泄露各自的整数. 他们基于该协议,进一步提出了一个多方最小公倍数计算协议,基本过程如下:

(1)基于算术基本定理,每个参与方 P_i 将私有整数 x_i 分解为素因子的乘积:

$$x_i=2^{x_{i1}}\cdot3^{x_{i2}}\cdot\cdots\cdot q_t^{x_{it}},$$

其中 t 是这些整数允许存在的素因子数量,q_k 是第 $1\leq k\leq t$ 个素因子,x_{ik} 是其对应的指数;

(2)通过提出的最大值计算协议,分别对每个 $1\leq k\leq t$,计算出 x_{ik} 的最大值 $Y_k=\max\limits_{i\in[\![n]\!]}(x_{ik})$;

(3)最小公倍数结果为 $\mathrm{lcm}\limits_{i\in[n]}(x_i)=2^{Y_1}\cdot3^{Y_2}\cdot\cdots\cdot q_t^{Y_t}$.

上述过程需要对每个 $1\leq k\leq t$ 施加一次最值计算. 设涉及的整数最大不超过 $N=2^m$,根据素数定理,小于 N 的素数数量为

$$\pi(N)\approx\frac{N}{\ln N}\geq\frac{N}{\sqrt{N}}=\sqrt{N}=2^{\frac{m}{2}}.$$

因此,为了保证素因子的完全覆盖,杨晓艺的 LCM 协议需要考虑 $t=O(2^{\frac{m}{2}})$ 个素因子. 设执行一次最大值计算的复杂度为 K,则该 LCM 协议的复

杂度为 $O(tK)=O(2^{\frac{m}{2}}K)$，达到了指数级. 具体来说，执行一次基于门限解密的最大值计算的计算复杂度为 $l(3n+1)=O(nl)$，其中 l 为整数取值范围的长度；通信复杂度为 $(2n-1)=O(n)$. 对于最小的素因子 2，指数 x_{i1} 的取值范围为 $0,1,\cdots,m-1$，故计算复杂度为 $O(nm)$. 因此，计算和通信复杂度分别为 $O(2^{\frac{m}{2}}nm)$ 和 $O(2^{\frac{m}{2}}n)$.

2.4　量子逻辑乘协议与匿名否决投票协议回顾

2021 年，Shi 等人[29]提出了第一个量子多方逻辑乘(LA)协议，其基本思路是使用 n 次量子 Toffoli 门进行逻辑乘计算，具有单次执行下的确定性，并且不泄露输入 0 的个数. 然而，为了加密每个人的 Toffoli 操作，在预计算阶段需要匹配每个人随机生成的一个比特，直到这些比特完全相等，其概率为 $\frac{2}{2^n}=\frac{1}{2^{n-1}}$，因此成功所需的平均时间复杂度为 $O(2^n)$，属于指数级复杂度. 在匿名否决方面，已有的量子 AV(QAV)协议都具有多项式复杂度，其中 Rahaman 等人[30]的协议在单次执行中只需分享一个 n 比特 GHZ 态和执行单比特操作即可，但是需要迭代 $O(\log n)$ 次以获得确定性结果，而且迭代性协议具有泄露否定票数的可能性，因为迭代终止条件为票数是奇数；Wang 等人[31]的协议将 l 次迭代执行改为同时执行，但是具有理论失败概率 2^{-l}；Mishra 等人[32]提出了 7 个 QAV 协议，其中，协议 1～4 属于概率性协议，基本思路相同，都需要每两个人之间进行量子密钥分发或分享纠缠态，并同时准备 l 个备份；协议 5 是协议 2 的迭代版本；协议 6 与 Rahaman 等人的协议类似，属于迭代性协议；协议 7 为确定性协议，使用随机分发的不相交泡利子群进行超密编码，具有最高的效率和成功率. 因此，符合匿名输出检验问题要求(单次执行确定性)的协议只有一个，即 Mishra 等人的协议 7. 其基本过程如下：

(1) 每个参与方 P_i 随机获得一个泡利子群

$$g_i=\{\mathrm{I},\mathrm{O}_i\}\subset G_{2^{m_l}}=\{\mathrm{I},\mathrm{X},\sqrt{-1}\mathrm{Y},\mathrm{Z}\}^{\otimes\lceil\log m_l\rceil},$$

其中任意两个 g_i、g_j 满足 $g_i\cap g_j=\{\mathrm{I}\}$，且 $\prod_{i=1}^{n}\mathrm{O}_i=\mathrm{I}$.

(2) TP 制备一个 $m_l\geq n-1$ 比特的纠缠态，将其中 l 比特发送出去，在每个参与方之间传递，直到回归 TP. 其中，每个 P_i 若投否定票 $c_i=0$，则将自己的操作 O_i 施加到手中的粒子上；

(3) TP 测量纠缠态，若其与一开始一致，则发现没有否定票，输出 $y=1$；否则，将得到否定票 $y=0$.

为了隐藏每个人具体的操作，每个人的泡利子群是随机分配的. 然而，我们可以证明其仍然会泄露否定票数. 以 $n=4$，TP 制备 3 比特的 GHZ 态 $|\Psi\rangle=\frac{|000\rangle+|111\rangle}{\sqrt{2}}$ 为例，其对应的子群为[32]

$$(\mathrm{O}_1,\mathrm{O}_2,\mathrm{O}_3,\mathrm{O}_4)=(\mathrm{X}\otimes\mathrm{I},\mathrm{X}\otimes\mathrm{X},\mathrm{Y}\otimes\mathrm{X},\mathrm{Y}\otimes\mathrm{I}),$$

其中为了简洁省略系数 $\sqrt{-1}$. 显然，若否定票数为 3，则根据 $\prod_{i=1}^{4}\mathrm{O}_i=\mathrm{I}$，以及泡利算子之间的对易关系有 $\prod_{i=1}^{3}\mathrm{O}_{k_i}=\mathrm{O}_{k_4}$，其中 k_1、k_2、k_3、k_4 为 1、2、3、4 的任意全排列，即最终结果将仍为上述 4 种算子. 然而，若总票数为 2，例如 $\mathrm{O}_1\mathrm{O}_2=\mathrm{I}\otimes\mathrm{X}$，则得到了不在上述集合内的算子. 我们将证明，TP 很容易区分上述情况，因为：

(1) 若票数为奇数，则 $|\Psi\rangle$ 将变为 $\frac{|100\rangle\pm|011\rangle}{\sqrt{2}}$ 或 $\frac{|110\rangle\pm|001\rangle}{\sqrt{2}}$(省略全局相位)；

(2) 若票数为 0，则 $|\Psi\rangle$ 不变；

(3) 若票数为 2，例如 P_1，P_2 施加了 $\mathrm{O}_1\mathrm{O}_2=\mathrm{I}\otimes\mathrm{X}$，则 $|\Psi\rangle$ 变为 $\frac{|010\rangle+|101\rangle}{\sqrt{2}}$.

那么，若票数为 2，则 TP 只要进行 GHZ 基测量，就能轻易发现这一点. 因此，目前与匿名输出验证问题类似的量子协议要么计算效率偏低，要么不具有确定性，要么会泄露票数信息.

2.5　恶意模型下的安全性定义

当考虑量子计算时，有些用在经典 SMC 中的方法可能会失去其安全性，因此在量子安全多方计算中需要考虑更高的安全性. 在本文中，我们在恶意攻击模型下分析协议的安全性，且尽可能不依赖于计算复杂性假设. 由于量子 SMC 相对于经典 SMC 具有一定的特殊性，例如，其无条件安全性往往建立在对窃听或作弊的敏感性上，且一旦任何一方施加非法的测量行为就可能导致量子态坍缩，使结果不正确，故很难直接套用经典 SMC 的理想-现实范式[34]来同时定义正确性和安全性. 然而，如果只考虑安全性，仍可以如下类似地定义：

定义 4.　恶意攻击模型. 在恶意模型中，对手可能采取一切可能的攻击手段，以尽可能获得其他人的信息. 原则上，在恶意模型中除了以下三种行为：(1) 拒绝参加协议，(2) 不完成协议，(3) 伪造输入以外，一切对私有信息的攻击都应被防御或被发现[34]. 与之对应的是半诚实模型，即参与方只被动地分析所获得的信息，而不进行主动攻击. 此外，为

了研究方便起见,进行如下假设:

(1)由于量子态的脆弱性,我们不抵抗也无法抵抗对于量子协议的纯粹破坏性攻击,例如拒绝服务攻击(DoS)等;

(2)假设存在一个满足非共谋条件的第三方平台 TP,即不与其他人共谋.注意,其并不一定是半诚实的,而可能是恶意的;

(3)考虑到接下来的 AOV 协议和 LCM 协议的特殊性,如果某一方发动攻击,则其不会输入有效信息.注意,在这两个协议中,这等价于输入 1,实际上是协议允许的.

定义 5. 迹距离.设两个随机变量 X,Y 分别具有概率分布 $p(x),q(x)$,其迹距离(或称 Kolmogorov 距离)为 $D(X,Y)=\frac{1}{2}\sum_x|p(x)-q(x)|$;对于两个量子态 ρ,σ,其迹距离为 $D(\rho,\sigma)=\frac{1}{2}\mathrm{Tr}(|\rho-\sigma|)$[28].

定义 6. 统计不可区分.对于一个函数 $\mu(m)$:$\mathbb{R}\to[0,1]$,若不存在任何正多项式 $poly(m)$ 使得 $\mu(m)\geqslant\frac{1}{poly(m)}$,则称为可忽略函数.若两个随机变量 X,Y(或两个量子态 ρ,σ)的迹距离可忽略,则称为统计不可区分,记作 $X\overset{S}{\equiv}Y$($\rho\overset{S}{\equiv}\sigma$).该概念意味着在协议的多项式次执行下攻击方无法获得不可忽略的有效信息.

定义 7. 恶意模型下的无条件安全性.设有协议 Π,其中 n 个参与方 $I=(P_1,P_2,\cdots,P_n)$ 分别具有输入 $x_I=(x_1,x_2,\cdots,x_n)$,并且想要计算目标函数 $F(x_I)=(F_1(x_I),F_2(x_I),\cdots,F_n(x_I))$.若在协议中任意允许的攻击策略 B 下,至少满足以下条件之一:(1)存在一个概率模拟算法 SI,使得攻击方所在集合 I_1 获得的所有经典和量子信息的总视图满足 $VIEW_{I_1}(x_I)\overset{S}{\equiv}SI(x_{I_1},F_{I_1})$;(2)该攻击不被非攻击方 I_1 发现的概率可忽略,则称该协议满足恶意模型下的无条件安全性.

2.6 量子周期查找算法

Shor 量子周期查找算法[28]的主要过程如下.

算法 1. 量子周期查找算法(QPA).

输入:函数 $f:[2^u]\to[2^v]$.其存在正整数周期 $1\leqslant T<2^v$,对于每对不同的 $j,j'\in[2^u]$,$f(j)=f(j')$ 当且仅当 $j\equiv j'(\mathrm{mod}\,T)$

输出:周期 T

成功概率:$O\left(\frac{1}{\log\log T}\right)\geqslant O\left(\frac{1}{\log\log 2^v}\right)=O\left(\frac{1}{\log v}\right)$

1.准备两个量子寄存器 h,t,分别为 u,v 量子比特,并初始化为初态 $|0\rangle_h|0\rangle_t$;

2.对 h 施加 $\mathrm{H}^{\otimes u}$:

$$|0\rangle_h|0\rangle_t\xrightarrow{\mathrm{H}^{\otimes u}}\frac{1}{\sqrt{2^u}}\sum_{j\in[2^u]}|j\rangle_h|0\rangle_t;$$

3.对 h,t 施加 Oracle 操作 $\mathrm{U}_f:|j\rangle_h|0\rangle_t\to|j\rangle_h|f(j)\rangle_t$:

$$\frac{1}{\sqrt{2^u}}\sum_{j\in[2^u]}|j\rangle_h|0\rangle_t\xrightarrow{\mathrm{U}_f}\frac{1}{\sqrt{2^u}}\sum_{j\in[2^u]}|j\rangle_h|f(j)\rangle_t$$

$$\approx\frac{1}{\sqrt{T2^u}}\sum_{l\in[T]}\sum_{j\in[2^u]}e^{\frac{\sqrt{-1}2\pi}{T}jl}|j\rangle_h|\hat{f}(l)\rangle_t,$$

其中 $|\hat{f}(l)\rangle=\frac{1}{\sqrt{T}}\sum_{k\in[T]}e^{-\frac{\sqrt{-1}2\pi}{T}lk}|f(k)\rangle$ 是 $|f(j)\rangle$ 的傅里叶逆变换[28];

4.对 h 施加 $\mathrm{QFT}^\dagger$:

$$\frac{1}{\sqrt{T}}\sum_{l\in[T]}\frac{1}{\sqrt{2^u}}\sum_{j\in[2^u]}e^{\frac{\sqrt{-1}2\pi}{T}jl}|j\rangle_h|\hat{f}(l)\rangle_t$$

$$\xrightarrow{\mathrm{QFT}^\dagger}\frac{1}{\sqrt{T}}\sum_{l\in[T]}\left|\frac{l}{T}2^u\right\rangle_h|\hat{f}(l)\rangle_t;$$

5.测量 h:

$$\frac{1}{\sqrt{T}}\sum_{l\in[T]}\left|\frac{l}{T}2^u\right\rangle_h|\hat{f}(l)\rangle_t\xrightarrow{Measure}\left|\frac{l}{T}2^u\right\rangle_h|\hat{f}(l)\rangle_t,$$

以 $\frac{1}{T}$ 概率得到任意 $\varphi\approx\frac{l}{T}$,$l\in[T]$;其中 $\gcd(l,T)=1$ 的概率为 $O\left(\frac{1}{\log\log T}\right)$[26];

6.用连分式展开算法计算 φ 的连分式展开 P_1,得到 $\frac{l'}{T'}\approx\frac{l}{T}$.如果 T' 是正确的周期(计算 $f(T')=f(0)$ 是否成立),则算法结束;否则,重复上述步骤.

之所以函数要满足 $f(j)=f(j')$ 当且仅当 $j\equiv j'(\mathrm{mod}\,T)$ 的要求,是因为在 QPA 的推导过程中,如果存在非周期 T 的碰撞,则无法保证得到正确周期.此外,在步骤 6 中,如 Shor 所述,我们应该让 $2^u\geqslant2\cdot2^v+1$,即 $u\geqslant2v+1$,以确保连分数展开 φ 可以找到 $\frac{l}{T}$.另一方面,如果 $\gcd(l,T)=1$(概率为 $O\left(\frac{1}{\log\log T}\right)$),那么我们得到 $T'=T$;否则 $T'<T$,则算法失败.因此,我们应该重复算法 $O(\log\log T)\leqslant O(\log\log 2^v)=O(\log v)$ 次,以确保能遇到正确的 T.

2.7 量子安全多方加法协议

Shi 等人[33]提出了一个量子安全多方加法协议,其主要过程如下.

协议 1. 量子安全多方加法(SMQS).

输入:$P_1,P_2,\cdots,P_n$ 各自有其私有整数 $x_1,x_2,\cdots,x_n\in[2^m]$

输出:$y=\sum_{i\in[n]}x_i\bmod 2^m$

1.P_1 准备两个粒子 h,t,均为 m 量子比特,并初始化为初态 $|x_1\rangle_h|0\rangle_t$;

对 h 施加 QFT：

$$|x_1\rangle_h|0\rangle_t \xrightarrow{\text{QFT}} \frac{1}{\sqrt{2^m}}\sum_{j\in[2^m]} e^{\frac{\sqrt{-1}2\pi x_1}{2^m}j}|j\rangle_h|0\rangle_t;$$

以 h 为控制，t 为目标施加 $\text{CNOT}^{\otimes m}$：

$$\frac{1}{\sqrt{2^m}}\sum_{j\in[2^m]} e^{\frac{\sqrt{-1}2\pi x_1}{2^m}j}|j\rangle_h|0\rangle_t$$

$$\xrightarrow{\text{CNOT}^{\otimes m}} \frac{1}{\sqrt{2^m}}\sum_{j\in[2^m]} e^{\frac{\sqrt{-1}2\pi x_1}{2^m}j}|j\rangle_h|j\rangle_t;$$

最后将 t 发送给 P_2；

2. P_i，$i=2,3,\cdots,n$ 的操作如下：

对 t 施加 C_j：

$$\frac{1}{\sqrt{2^m}}\sum_{j\in[2^m]} e^{\frac{\sqrt{-1}2\pi\sum\limits_{k\in[i-1]}x_k}{2^m}j}|j\rangle_h|j\rangle_t|x_i\rangle$$

$$\xrightarrow{\text{C}_j} \frac{1}{\sqrt{2^m}}\sum_{j\in[2^m]} e^{\frac{\sqrt{-1}2\pi\sum\limits_{k\in[i]}x_k}{2^m}j}|j\rangle_h|j\rangle_t|x_i\rangle;$$

将 t 发送给 P_{i+1}. 如果是 P_n 就发给 P_1；

3. P_1 以 h 为控制，t 为目标再次施加 $\text{CNOT}^{\otimes m}$：

$$\frac{1}{\sqrt{2^m}}\sum_{j\in[2^m]} e^{\frac{\sqrt{-1}2\pi\sum\limits_{k\in[n]}x_k}{2^m}j}|j\rangle_h|j\rangle_t$$

$$\xrightarrow{\text{CNOT}^{\otimes m}} \frac{1}{\sqrt{2^m}}\sum_{j\in[2^m]} e^{\frac{\sqrt{-1}2\pi\sum\limits_{k\in[n]}x_k}{2^m}j}|j\rangle_h|0\rangle_t;$$

测量 t，如果不为 $|0\rangle$ 态则认为有人作弊；他对 h 施加 $\text{QFT}^\dagger$：

$$\frac{1}{\sqrt{2^m}}\sum_{j\in[2^m]} e^{\frac{\sqrt{-1}2\pi\sum\limits_{k\in[n]}x_k}{2^m}j}|j\rangle_h \xrightarrow{\text{QFT}^\dagger} \left|\sum_{i\in[n]}x_i \bmod 2^m\right\rangle_h,$$

并测量 h，得到 $y=\sum\limits_{i\in[n]}x_i \bmod 2^m$，然后将其广播给其他参与方.

在该协议中，为了进一步加强安全性，Shi 等人提到粒子发送的顺序可以不预先指定，而是每个人随机选择发送对象.

3　求解最小公倍数问题的量子安全多方计算协议

本节中我们基于量子周期查找算法，提出一个求解最小公倍数问题的量子安全多方计算协议. 首先我们描述共谋攻击，并设计星-环混合拓扑结构以抵御共谋攻击和伪造攻击，然后设计了一个量子匿名输出检验协议来进行计算结果的验证，最后提出了一个量子最小公倍数协议.

3.1　用于诚实性验证的星-环混合拓扑

Shi 等人的 SMQS 协议结构属于环状拓扑，即从 P_1 起始传递一些计算粒子，历经 $P_2,\cdots,P_n$，直到返回 P_1，然后提取出最终结果. 基于环状拓扑的量子协议无法防御共谋的伪造攻击. 例如，设有两个参与方 P_{k-1} 和 P_{k+1+l} 串通，P_{k-1} 制备一个伪造粒子，伪装成真正的协议粒子，将其传递下去. 由于传递中途不对粒子进行测量，得到该伪造粒子的参与方 $P_k,P_{k+1},\cdots,P_{k+l}$ 无法察觉攻击的发生，诚实地将私有信息施加在伪造粒子上，最终传递到 P_{k+1+l} 手上，被其读取出来. Shi 等人提到每个参与方可以随机选择其要传递的下一个目标，从而扰乱这种攻击. 因为在随机选择传递顺序的情况下，攻击者将不能确定攻击目标及其数量，从而得不到预期的信息. 然而，如果攻击者无差别地随机攻击，那么他仍然可能获得一定的有效信息，例如在求和协议中，获得一部分参与方的局部求和结果；此外，当恶意攻击者的共谋数量占大多数时，这种方法也无法防御.

我们注意到，该结构容易被共谋攻击的原因是每个参与方唯一能得到的只有前一个参与方传来的粒子，即问题来自于环状拓扑结构. 然而，若将结构改为星型拓扑，即由一个处于中心的制备方对每个参与者发送一份粒子，然后收回，则虽然共谋攻击不再奏效，但是制备方本人可以施加伪造攻击，即发送互相没有真正纠缠的粒子，从而轻易获取每个参与方的信息. 为了真正解决上述问题，我们提出了星-环混合拓扑. 其思想是，假如协议中粒子的制备方满足非共谋条件，即不与任何其他参与者共谋，那么他在计算开始前首先向每个参与方单独发送一个用于验证的粒子（该粒子的态来自于计算用的粒子，可令计算粒子为控制，施加 $\text{CNOT}^{\otimes m}$ 得到，见协议 1 第 1 步），该过程属于星型拓扑；然后发送用于计算的粒子，而计算过程仍然属于环状拓扑；这样，当 P_k 得到 P_{k-1} 发来的粒子时，他首先将该粒子与制备方发来的验证粒子进行纠缠验证（如施加 $\text{CNOT}^{\otimes m}$ 解纠缠，并测量目标粒子是否处于态 $|0\rangle$，见协议 1 第 3 步），一旦发现两个粒子的态并不纠缠，则其中存在伪造粒子，说明制备方和他之前的参与方中至少有一个不诚实，从而申请协议终止. 此外，若存在参与方进行了拦截-再发送攻击，即，获得计算粒子后将其保留，并伪造了另一份与其不纠缠的粒子返回，以试图获取信息，那么他将失败，因为其仍然是共谋攻击的变体. 图 1 对比了环状拓扑和星-环混合拓扑的执行过程.

如下定理 1 给出了在非共谋制备方假设下星-

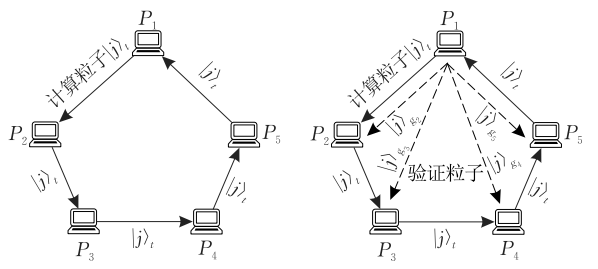

图 1 环状拓扑(a)与星-环混合拓扑(b)(其中 $n=5$,计算粒子用 t 表示,其传输为黑色箭头;验证粒子用 g_i 表示,其传输为虚线箭头)

环混合拓扑抵抗伪造、共谋攻击或拦截-再发送攻击的能力,证明见附录.

定理 1. 设有一个满足星-环混合拓扑结构的协议,并设粒子的制备方满足非共谋条件.那么,如果任何一方施加了伪造攻击、共谋攻击或拦截-再发送攻击,则其不被发现的概率为$\frac{1}{2^m}$,其中 m 是每一个粒子的量子比特数.

值得注意的是,星-环混合拓扑有效的必要条件是用于计算的粒子的量子态最多只能发生相位的改变,而不能改变基态.比如在接下来的协议 2 中,计算粒子的量子态一开始为$|j\rangle_t|j\rangle_{g_i}$,此时,粒子 t,g_i 之间可以用 $\mathrm{CNOT}^{\otimes m}$ 门精确相消;而在协议进行到 P_i 时,量子态为$|j\rangle_t|j\rangle_{g_i}$,粒子 t 始终保持为$|j\rangle_t$,因此此时仍可以相消.但是,如果在协议中发生了任何比特位上的改变$|j\rangle_t\to|\varepsilon(j)\rangle_t$,那么 $\mathrm{CNOT}^{\otimes m}$ 将无法用于相消,该方法将会失败.另一个弊端是当制备方可以与其他参与方共谋时,则若恶意方占绝大多数时仍然无法防止信息被窃取,因此非共谋假设是必要的.

3.2 用于结果验证的匿名输出检验协议

基于协议 1 和星-环混合拓扑,我们设计了一个量子匿名输出检验协议,作为最小公倍数协议的子协议.在协议 1 的基础上,通过加入一个随机奇数,并引入一个非共谋的第三方(Third Party,TP),他不与任何参与者共谋,使得其能够隐藏每个人的检验结果,且不泄露总的检验通过数量,其安全性依赖于一个参数 M 的选定.

协议 2. 量子匿名输出检验(Quantum Anonymous Output Validation,QAOV).

输入:$P_1,P_2,\cdots,P_n$ 各自有其私有布尔值 $c_1,c_2,\cdots,c_n\in[2]$

输出:$y=\prod_{i\in[\![n]\!]}c_i$

1. 选定一个大整数$M=4K\geq1$,例如取 $K=100$ 或以上.对每个 P_i,如果 $c_i=0$,则随机选择一个正整数 $x_i\in[\![M]\!]$;如果 $c_i=1$,则令 $x_i=0$;取整数 m 满足 $2^{m-1}\leq nM<2^m$,即 $m=\lfloor\log_2(nM)\rfloor+1=O(\log n)$;

2. $P_1,P_2,\cdots,P_n$ 通过量子会议密钥分发[35-37]分享一个随机的 $m-1$ 比特数 $\bar{q}\in[2^{m-1}]$,其对于 TP 保密;然后增加一个末位比特 1,得到随机奇数 $q\in[2^m]$°;

3. TP 准备两个 m 量子比特粒子$|0\rangle_h|0\rangle_t$,并与协议 1 一样施加 QFT 与 $\mathrm{CNOT}^{\otimes m}$,然后准备 n 个 m 量子比特的粒子 $g_1,\cdots,g_n$,初态均为$|0\rangle$,用 $\mathrm{CNOT}^{\otimes m}$ 将 $g_1,\cdots,g_n$ 复制为$|j\rangle$:

$$\frac{1}{\sqrt{2^m}}\sum_{j\in[2^m]}|j\rangle_h|j\rangle_t|0\rangle_{g_1}\cdots|0\rangle_{g_n}$$
$$\xrightarrow{\mathrm{CNOT}^{\otimes m}}\frac{1}{\sqrt{2^m}}\sum_{j\in[2^m]}|j\rangle_h|j\rangle_t|j\rangle_{g_1}\cdots|j\rangle_{g_n},$$

再将 $g_1,\cdots,g_n$ 发送给对应的 $P_1,\cdots,P_n$,最后再将 t 发送给 P_1;

4. P_1 收到 t 后,以 t 为控制,g_1 为目标施加 $\mathrm{CNOT}^{\otimes m}$:

$$\frac{1}{\sqrt{2^m}}\sum_{j\in[2^m]}|j\rangle_h|j\rangle_t|j\rangle_{g_1}|j\rangle_{g_2}\cdots|j\rangle_{g_n}$$
$$\xrightarrow{\mathrm{CNOT}^{\otimes m}}\frac{1}{\sqrt{2^m}}\sum_{j\in[2^m]}|j\rangle_h|j\rangle_t|0\rangle_{g_1}|j\rangle_{g_2}\cdots|j\rangle_{g_n},$$

并测量 g_1,如果不为$|0\rangle$态则认为有人作弊;

5. 若没有发现作弊行为,则 P_1 对粒子 t 施加 C_j 操作:

$$\frac{1}{\sqrt{2^m}}\sum_{j\in[2^m]}|j\rangle_h|j\rangle_t|j\rangle_{g_2}\cdots|j\rangle_{g_n}|qx_1\rangle$$
$$\xrightarrow{\mathrm{C}_j}\frac{1}{\sqrt{2^m}}\sum_{j\in[2^m]}e^{\frac{\sqrt{-1}2\pi qx_1}{2^m}j}|j\rangle_h|j\rangle_t|j\rangle_{g_2}\cdots|j\rangle_{g_n}|qx_1\rangle;$$

然后将 t 发送给 P_2;

6. $P_i,i\in2,\cdots,n$ 收到 t 后,以 t 为控制,g_i 为目标施加 $\mathrm{CNOT}^{\otimes m}$:

$$\frac{1}{\sqrt{2^m}}\sum_{j\in[2^m]}e^{\frac{\sqrt{-1}2\pi q\sum_{k\in[\![i-1]\!]}x_k}{2^m}j}|j\rangle_h|j\rangle_t|j\rangle_{g_i}|j\rangle_{g_{i+1}}\cdots|j\rangle_{g_n}$$
$$\xrightarrow{\mathrm{CNOT}^{\otimes m}}\frac{1}{\sqrt{2^m}}\sum_{j\in[2^m]}e^{\frac{\sqrt{-1}2\pi q\sum_{k\in[\![i-1]\!]}x_k}{2^m}j}|j\rangle_h|j\rangle_t|0\rangle_{g_i}|j\rangle_{g_{i+1}}\cdots|j\rangle_{g_n},$$

并测量 g_i,如果不为$|0\rangle$态则认为有人作弊.否则,对粒子 t 施加 C_j 操作:

$$\frac{1}{\sqrt{2^m}}\sum_{j\in[2^m]}e^{\frac{\sqrt{-1}2\pi q\sum_{k\in[\![i-1]\!]}x_k}{2^m}j}|j\rangle_h|j\rangle_t|j\rangle_{g_{i+1}}\cdots|j\rangle_{g_n}|qx_i\rangle$$
$$\xrightarrow{\mathrm{C}_j}\frac{1}{\sqrt{2^m}}\sum_{j\in[2^m]}e^{\frac{\sqrt{-1}2\pi q\sum_{k\in[\![i]\!]}x_k}{2^m}j}|j\rangle_h|j\rangle_t|j\rangle_{g_{i+1}}\cdots|j\rangle_{g_n}|qx_i\rangle,$$

最后将 t 发送给 P_{i+1},如果是 P_n 则发给 TP;

7. TP 收到 t 后,再次以 h 为控制,t 为目标施加 $\mathrm{CNOT}^{\otimes m}$,并测量 t 以验证.如果通过,则对 h 施加 $\mathrm{QFT}^\dagger$:

$$\frac{1}{\sqrt{2^m}}\sum_{j\in[2^m]}e^{\frac{\sqrt{-1}2\pi q\sum_{k\in[\![n]\!]}x_k}{2^m}j}|j\rangle_h\xrightarrow{\mathrm{QFT}^\dagger}\left|q\sum_{k\in[\![n]\!]}x_k\right\rangle_h,$$

并测量得到 $z=q\sum_{i\in[\![n]\!]}x_i \bmod 2^m$；

8. 若 $z>0$，则 TP 公布 $y=\prod_{i\in[\![n]\!]}c_i=0$；若 $z=0$，则 $y=\prod_{i\in[\![n]\!]}c_i=1$.

3.3 最小公倍数计算协议

基于 QPA 算法，我们提出了最小公倍数计算协议. 在协议中，每个参与方将定义一个整数周期函数，其周期就是各自的私有整数. 一个非共谋的第三方将对每个人分发一份粒子，这些粒子全部纠缠起来，而每个人对这个粒子施加与由自己的函数定义的 Oracle 操作. 在这个分发过程中，星-环混合拓扑将作为验证机制，防止出现伪造或共谋攻击. 当所有人都施加了 Oracle 操作后，其等价于施加了一个由这些函数连接成的大周期函数的 Oracle 操作，其周期正好是这些小周期的最小公倍数. 随后，第三方运行 QPA，得到这个大周期，并将其广播给其他人. 由于 QPA 存在一定的失败概率，此时运行协议 2，每个人检验这个大周期是否是自己的整数的倍数，从而检验其是否是正确的最小公倍数. 协议的具体过程如下.

协议 3.　量子安全多方最小公倍数计算(Secure Multiparty Quantum Least Common Multiple, SMQLCM).

输入：$P_1,P_2,\cdots,P_n$ 各自有其私有整数 $x_1,x_2,\cdots,x_n\in[2^m]-\{0\}$

输出：$y=\operatorname{lcm}_{i\in[\![n]\!]}(x_i)$

成功概率：$O\left(\frac{1}{\log(nm)}\right)$

1. 首先令 $u=O(nm)$. 对 $\forall i\in[\![n]\!]$，P_i 各自定义函数 f_i：$[2^u]\to[2^m]$ 为：$f_i(j)=j \bmod x_i$；如果 $x_i=1$，则 $f_i(j)=j \bmod 1=0$；

2. 非共谋第三方 TP 准备粒子 $h,t,g_1,g_2,\cdots,g_n$，均为 u 量子比特，并全部初始化为 $|0\rangle$；

对 h 施加 $\mathrm{H}^{\otimes u}$：

$$|0\rangle_h|0\rangle_t|0\rangle_{g_1}\cdots|0\rangle_{g_n}$$

$$\xrightarrow{\mathrm{H}^{\otimes u}}\frac{1}{\sqrt{2^u}}\sum_{j\in[2^u]}|j\rangle_h|0\rangle_t|0\rangle_{g_1}\cdots|0\rangle_{g_n};$$

以 h 为控制，$t,g_1,\cdots,g_n$ 为目标施加 $\mathrm{CNOT}^{\otimes u}$：

$$\frac{1}{\sqrt{2^u}}\sum_{j\in[2^u]}|j\rangle_h|0\rangle_t|0\rangle_{g_1}\cdots|0\rangle_{g_n}$$

$$\xrightarrow{\mathrm{CNOT}^{\otimes u}}\frac{1}{\sqrt{2^u}}\sum_{j\in[2^u]}|j\rangle_h|j\rangle_t|j\rangle_{g_1}\cdots|j\rangle_{g_n};$$

随机将 $g_1,\cdots,g_n$ 发送给对应的 $P_1,\cdots,P_n$，

最后再将 t 发送给 P_1；

3. P_1 得到 t 后，首先以 t 为控制，g_i 为目标施加 $\mathrm{CNOT}^{\otimes u}$：

$$\frac{1}{\sqrt{2^u}}\sum_{j\in[2^u]}|j\rangle_h|j\rangle_t|j\rangle_{g_1}|j\rangle_{g_2}\cdots|j\rangle_{g_n}$$

$$\xrightarrow{\mathrm{CNOT}^{\otimes u}}\frac{1}{\sqrt{2^u}}\sum_{j\in[2^u]}|j\rangle_h|j\rangle_t|0\rangle_{g_1}|j\rangle_{g_2}\cdots|j\rangle_{g_n},$$

并测量 g_1，如果不为 $|0\rangle$ 态则认为 TP 作弊；他随后准备一个 m 量子比特粒子 e_1，并对 t,e_1 施加 Oracle 操作 $\mathrm{U}_1:|j\rangle_t|0\rangle_{e_1}\to|j\rangle_t|f_1(j)\rangle_{e_1}$：

$$\frac{1}{\sqrt{2^u}}\sum_{j\in[2^u]}|j\rangle_h|j\rangle_t|j\rangle_{g_2}\cdots|j\rangle_{g_n}|0\rangle_{e_1}$$

$$\xrightarrow{\mathrm{U}_1}\frac{1}{\sqrt{2^u}}\sum_{j\in[2^u]}|j\rangle_h|j\rangle_t|j\rangle_{g_2}\cdots|j\rangle_{g_n}|f_1(j)\rangle_{e_1},$$

然后将 t 发送给 P_2；

4. $P_i,i=2,3,\cdots,n$ 的操作如下：

得到 t 后，首先以 t 为控制，g_i 为目标施加 $\mathrm{CNOT}^{\otimes u}$：

$$\frac{1}{\sqrt{2^u}}\sum_{j\in[2^u]}|j\rangle_h|j\rangle_t|j\rangle_{g_i}\cdots|j\rangle_{g_n}|f_1(j)\rangle_{e_1}\cdots|f_{i-1}(j)\rangle_{e_{i-1}}$$

$$\xrightarrow{\mathrm{CNOT}^{\otimes u}}\frac{1}{\sqrt{2^u}}\sum_{j\in[2^u]}|j\rangle_h|j\rangle_t|0\rangle_{g_i}\cdots|j\rangle_{g_n}|f_1(j)\rangle_{e_1}\cdots|f_{i-1}(j)\rangle_{e_{i-1}},$$

并测量 g_i，如果不为 $|0\rangle$ 态则认为有人作弊；然后他准备 m 量子比特粒子 e_i，对 t,e_i 施加 Oracle 操作 $\mathrm{U}_i:|j\rangle_t|0\rangle_{e_i}\to|j\rangle_t|f_i(j)\rangle_{e_i}$：

$$\frac{1}{\sqrt{2^u}}\sum_{j\in[2^u]}|j\rangle_h|j\rangle_t|j\rangle_{g_{i+1}}\cdots|j\rangle_{g_n}|f_1(j)\rangle_{e_1}\cdots|f_{i-1}(j)\rangle_{e_{i-1}}|0\rangle_{e_i}$$

$$\xrightarrow{\mathrm{U}_i}\frac{1}{\sqrt{2^u}}\sum_{j\in[2^u]}|j\rangle_h|j\rangle_t|j\rangle_{g_{i+1}}\cdots|j\rangle_{g_n}|f_1(j)\rangle_{e_1}\cdots|f_i(j)\rangle_{e_i};$$

将 t 发送给 P_{i+1}. 如果是 P_n，则发给 TP；

5. TP 以 h 为控制，t 为目标再次施加 $\mathrm{CNOT}^{\otimes u}$：

$$\frac{1}{\sqrt{2^u}}\sum_{j\in[2^u]}|j\rangle_h|j\rangle_t|f_1(j)\rangle_{e_1}\cdots|f_n(j)\rangle_{e_n}$$

$$\xrightarrow{\mathrm{CNOT}^{\otimes u}}\frac{1}{\sqrt{2^u}}\sum_{j\in[2^u]}|j\rangle_h|0\rangle_t|f_1(j)\rangle_{e_1}\cdots|f_n(j)\rangle_{e_n};$$

测量粒子 t，如果不为 $|0\rangle$ 态则认为有人作弊；令粒子 $e=(e_1,\cdots,e_n)$，函数 $f(j)=f_1(j)\,\|\cdots\|\,f_n(j)$，对粒子 h 施加 $\mathrm{QFT}^\dagger$：

$$\frac{1}{\sqrt{2^u}}\sum_{j\in[2^u]}|j\rangle_h|f(j)\rangle_e\xrightarrow{\mathrm{QFT}^\dagger}\frac{1}{\sqrt{y}}\sum_{l\in[y]}\left|\frac{l}{y}2^u\right\rangle_h|\hat{f}(l)\rangle_e,$$

其中 $y=\operatorname{lcm}_{i\in[\![n]\!]}(x_i)$；

7. 测量 h：

$$\frac{1}{\sqrt{y}}\sum_{l\in[y]}\left|\frac{l}{y}2^u\right\rangle_h|\hat{f}(l)\rangle_e\xrightarrow{Measure}\left|\frac{l}{y}2^u\right\rangle_h|\hat{f}(l)\rangle_e,$$

以 $\frac{1}{y}$ 概率得到任意 $\varphi\approx\frac{l}{y}$，$l\in[y]$；

用连分式展开算法计算 φ 的连分式展开，得到 l',y'，其满足 $\frac{l'}{y'}=\frac{l}{y}$，是约分后的最简分数；

8. 所有人开始对自己的 e_i 进行测量，并根据测量结果将其恢复为 $|0\rangle$ 态，以准备进行接下来的操作. 当所有人都完成后，进行下一步；

9. 广播 y'，然后调用协议 2，对每个 P_i，如果 $x_i\,|\,y'$，则

$c_i=1$,否则 $c_i=0$. 如果检验的结果为 $\prod_{i\in[\![n]\!]}c_i=1$,广播目前的结果;否则,再进行一次完整的本协议.

同样,为了得到的结果是最小的公倍数,需令 $u\geq 2nm+1=O(nm)$,且要重复 $O(\log(nm))$ 次算法以得到最小公倍数.

Oracle 算子 $U_i:|j\rangle_t|0\rangle_{e_i}\rightarrow|j\rangle_t|f_i(j)\rangle_{e_i}$ 可以由整数除法实现. 首先使用 $CNOT^{\otimes u}:|j\rangle_t|0\rangle_{e_i}\rightarrow|j\rangle_t|j\rangle_{e_i}$. 引入一个额外的寄存器 $|0\rangle_a$,通过量子酉电路依次实现:

(1) 整数除法[38]

$$|j\rangle_t|0\rangle_a\rightarrow|j\rangle_t|\lfloor j/x_i\rfloor\rangle_a;$$

(2) 整数模乘法[27]

$|\lfloor j/x_i\rfloor\rangle_a|0\rangle_{e_i}\rightarrow|\lfloor j/x_i\rfloor\rangle_a|(2^u-x_i)\lfloor j/x_i\rfloor\rangle_{e_i}$,其中乘数为 $(2^u-x_i)\equiv -x_i(\mathrm{mod}\,2^u)$;

(3) 整数模加法[39]

$|-x_i\lfloor j/x_i\rfloor\rangle_b|j\rangle_{e_i}\rightarrow|-x_i\lfloor j/x_i\rfloor\rangle_b|j-x_i\lfloor j/x_i\rfloor\rangle_{e_i}=|-x_i\lfloor j/x_i\rfloor\rangle_b|j\bmod x_i\rangle_{e_i}=|-x_i\lfloor j/x_i\rfloor\rangle_b|f_i(j)\rangle_{e_i}$.

最后施加除法和模乘法的逆电路以使 a,b 恢复为 $|0\rangle$,则完成了取模函数的计算.

4 协议分析

4.1 正确性分析

协议 2 的正确性. 由于协议的核心过程依然是相位上的加法,因此最终获得的结果必将是 $z=q\sum_{i\in[\![n]\!]}x_i\bmod 2^m$,正确性与协议 1 一致. 至于协议总体正确性,假设 $c_1=c_2=\cdots=c_n=1$,则第 1 步中 $x_1=x_2=\cdots=x_n=0$,因此求和得到的结果也满足 $z=q\sum_{i\in[\![n]\!]}x_i\bmod 2^m=0$,从而 $y=1=\prod_{i\in[\![n]\!]}c_i$;如果 $c_1,c_2,\cdots,c_n$ 中至少有一个 $c_i=0$,则其对应的 $x_i>0$,求和后的 $\sum_{i\in[\![n]\!]}x_i\bmod 2^m>0$($2^m>nM$,加法不溢出),则由 q 是奇数,有 $z=q\sum_{i\in[\![n]\!]}x_i\bmod 2^m\neq 0$,因此 $y=0=\prod_{i\in[\![n]\!]}c_i$,从而协议 2 正确地给出了布尔值的逻辑乘,即完成了输出检验.

协议 3 的正确性. 现在我们分析协议 3 主体的正确性. 如下的定理 2 说明最后计算出的函数 $f(j)$ 的周期确实是小周期 $x_1,x_2,\cdots,x_n$ 的最小公倍数,从而 QPA 算法将正确地输出结果,其证明见附录.

定理 2. 设函数 $f_1,f_2,\cdots,f_n:[2^u]\rightarrow[2^v]$,其最小正周期分别为正整数 $x_1,x_2,\cdots,x_n$,且满足对所有 $i\in[\![n]\!]$,$f_i(j)=f_i(j')$ 当且仅当 $j\equiv j'(\mathrm{mod}\,x_i)$. 定义函数 $f(j)=f_1(j)\|f_2(j)\|\cdots\|f_n(j)$,则其最小正周期为 $y=\mathrm{lcm}_{i\in[\![n]\!]}(x_i)$,且对所有 $i\in[\![n]\!]$,$f(j)=f(j')$ 当且仅当 $j\equiv j'(\mathrm{mod}\,y)$.

因此,协议 3 正确地输出所有人的最小公倍数.

4.2 安全性分析

不失一般性,我们假设恶意方达到最大攻击能力,即,除了 P_1 外的参与方集合 $I_1=\{P_2,\cdots,P_n\}$ 全部共谋,并且第三方 TP 也是独立的恶意攻击者,而只有 P_1 为半诚实方. 只要证明了在这种情况下 P_1 的隐私得到保护,则在其他情况下的隐私泄露不会比这更大,即协议的恶意安全性得到了证明. 根据定理 1,在星-环混合拓扑下,伪造攻击、共谋攻击和拦截-再发送攻击的成功率均为 $\frac{1}{2^m}$(在协议 3 中,粒子的量子比特数为 $u\geq 2nm+1$,即概率为 $\frac{1}{2^u}$),可忽略,因此我们不必考虑这三种攻击策略.

协议 2 的安全性. 在协议 2 中允许存在的恶意攻击策略有:

(1) 测量攻击:不进行额外操作,只分析得到的经典和量子信息;

(2) 非法密钥分发:在第 2 步时,参与方 I_1 在量子密钥分发过程中作弊;

(3) 非法制备:在第 3 步时,TP 在制备叠加态时没有制备正确的平衡叠加态,但是正常纠缠所有粒子;

(4) 非法输入:得到粒子后参与方 I_1 不施加正确的 C_j 门;

(5) 纠缠-测量攻击:得到粒子 a(包含所有获得的粒子)后,参与方 I_1 准备一个辅助粒子 b,然后纠缠 a,b. 设 a 的某个基态为 $|\varphi\rangle$,则纠缠门的一般定义为

$$|\varphi\rangle_a|0\rangle_b\rightarrow\sqrt{\eta}|\varphi\rangle_a|\varepsilon(\varphi)\rangle_b+\sqrt{1-\eta}|\delta(\varphi)\rangle_{(a,b)},$$

其中 $0\leq\eta\leq 1$ 是不改变 a 所处基态的概率. I_1 随后将粒子 a 发送给下一个参与方,并保留 b. 等到合适的时机,就分析 b 上的量子信息.

(6) 非法输出:最后一步时,TP 不输出正确的检验结果.

而只要在上述攻击策略下恶意方的视图都可模拟,或攻击被非恶意方高概率发现,则协议的安全性就得到了证明. 于是,我们有如下定理,其详细证明见附录.

定理 3. 协议 2 满足恶意模型下的无条件安全性,即在上述攻击策略下,恶意方要么无法获得信

息，要么攻击被发现.

该定理的证明依赖于一个核心原理，即当只拥有整个量子傅里叶纠缠态[40]中的部分粒子，而不是全部粒子时，就不可能提取出存在于相位上的任何信息. 也即，除非计算完成，否则无论有效信息的取值是多少，攻击者所拥有的量子信息都是统计不可区分的. 在这个基础上，诸如测量攻击、纠缠-测量攻击等量子态分析手段都是无效的. 因此，只需证明半诚实安全性，即当安全参数 M 足够大时，c_i 的不同取值对应的 z 对于 TP 是统计不可区分的，即无法从 $z=q\sum_{i\in[n]}x_i \bmod 2^m$ 反推出 c_i 的取值，就能证明协议 2 的安全性.

至于(3)、(4)、(5)、(6)这些剩余的手段，其只具有纯粹的破坏性，而没有造成信息泄露问题，因此不影响协议的安全性. 另一方面，通过使用量子相等比较[41-44]等方法，参与方之间可以检验各方获得的密钥 q 是否相同，从而以高概率发现密钥分发过程中的作弊. 此外，由于匿名输出检验本身的特性，如果某个人检验未通过，但最后广播的结果却是检验正确的，那么此人将立刻发现存在不诚实情况；而如果所有人都检验通过，但广播的结果是不通过，那么这在原则上是不可察觉的，因为要想检验结果正确性，就必须公开所有人的检验结果，因此我们不考虑其处理方法.

协议 3 的安全性. 上述分析表明协议 3 中最后一步的 AOV 过程是安全的，并且同样抵抗伪造攻击、共谋攻击和拦截-再发送攻击，因此与协议 2 类似，仍然允许存在的恶意攻击策略有：

(1) 测量攻击：不进行额外操作，只分析得到的经典和量子信息；

(2) 非法制备：在第 3 步时，TP 在制备叠加态时没有制备正确的平衡叠加态，但是正常纠缠所有粒子；

(3) 非法输入：得到粒子后参与方 I_1 不施加正确的 Oracle 操作 U_i；

(4) 纠缠-测量攻击：得到粒子 a 后，参与方 I_1 准备一个辅助粒子 b，然后纠缠 a,b，随后将粒子 a 发送给下一个参与方，并保留 b. 等到合适的时机，就分析 b 上的量子信息.

(5) 非法输出：最后一步时，TP 不输出正确的最小公倍数结果.

相应地，我们给出如下定理 4，其描述了协议 3 在上述攻击下的安全性，其证明见附录. 由于协议 3 的整体结构逻辑与协议 2 类似，故分析方法也是类似的.

定理 4.　协议 3 满足恶意模型下的无条件安全性，即在上述攻击策略下，恶意方要么无法获得信息，要么攻击被发现.

值得注意的是，在测量攻击下的安全性本身也是我们在协议第 8 步要求所有人测量来破坏量子态的合理性所在，因为这一步等价于测量攻击，从而是安全的，而破坏掉量子态后可以将恢复初态的量子比特回收利用，从而节省资源消耗. 此外，量子匿名输出检验本身也是一重保险，因为一旦有人破坏协议，那么协议的输出始终保持错误，继而由于协议 2 执行的次数过多，协议的执行异常将会被发现. 此外，如果 TP 最后广播的结果并不是所有整数的公倍数，那么将至少被一个其他参与方发现. 或者，虽然他必须广播公倍数，但可以私自在最小公倍数上乘以一个因子. 与协议 2 中的否定票类似，如果不允许公开每个人的输入，则原理上无法防御这种攻击，但是其没有对 TP 揭示任何有效信息，故不影响安全性.

4.3　复杂度分析

协议 2 的复杂度. 首先，协议第 2 步共享密钥需要在 n 方之间共享 $m-1$ 比特密钥 $\bar{q}$，其总复杂度一般为 $O(nm)$；量子傅里叶变换的单量子门复杂度为 $O(m^2)$；在模加法中的相位操作 U_+^j 可以分解为 $\mathrm{U}_+^{\sum_{i\in[m]}j_i2^i}=\prod_{i\in[m]}(\mathrm{U}_+^{2^i})^{j_i}$，其中算子 $\mathrm{U}_+^{2^i}$：$|x\rangle\to e^{\frac{\sqrt{-1}2\pi x2^i}{2^m}}|x\rangle$ 可以进一步分解为

$$e^{\frac{\sqrt{-1}2\pi x}{2^{m-i}}}|x\rangle=e^{\frac{\sqrt{-1}2\pi\sum_{k\in[m]}x_k2^k}{2^{m-i}}}\bigotimes_{k\in[m]}|x_k\rangle=\bigotimes_{k\in[m]}e^{\frac{\sqrt{-1}2\pi x_k2^k}{2^{m-i}}}|x_k\rangle$$

$$=\bigotimes_{k\in[m]}e^{\frac{\sqrt{-1}2\pi x_k}{2^{m-i-k}}}|x_k\rangle=\bigotimes_{k\in[m]}\boldsymbol{R}_{m-i-k}|x_k\rangle,$$

其中相位旋转矩阵 $\boldsymbol{R}_{m-i-k}=\begin{pmatrix}1 & 0\\ 0 & e^{\frac{\sqrt{-1}2\pi}{2^{m-i-k}}}\end{pmatrix}$，因此有 $\mathrm{U}_+^{2^i}=\bigotimes_{k\in[m]}\boldsymbol{R}_{m-i-k}$，从而 $\mathrm{U}_+^{2^i}$ 的计算复杂度(基本量子门数)为 $O(m)$，U_+^j 的复杂度为 $O(m^2)$. 因此协议的计算复杂度为 $O(nm^2)$，通信复杂度为 $O(nm)$. 因为比特数参数 $m=O(m_M+\log n)$，其中安全参数 m_M 可视为常数，故总计算复杂度和通信复杂度分别为 $O(n\log^2 n)$ 和 $O(n\log n)$.

协议 3 的复杂度. U_i：$|j\rangle|0\rangle\to|j\rangle|j \bmod x_i\rangle$ 的取余操作可以视为两个 $O(nm)$ 比特整数的整数除法，则计算复杂度为 $O(n^2m^2)$[28]；量子傅里叶逆变换

需要 $O(n^2m^2)$的复杂度;量子匿名输出检验的计算复杂度为 $O(n\log^2 n)$,通信复杂度为 $O(n\log n)$;因此,执行一次协议 3 全过程的总计算复杂度为 $O(n^3m^2+n\log^2 n)=O(n^3m^2)$,总通信复杂度为 $O(n^2m+n\log n)=O(n^2m)$;由于总协议需要重复 $O(\log(nm))$次保证结果正确,故完整的计算和通信复杂度分别为 $O(n^3m^2\log(nm))$和 $O(n^2m\log(nm))$.

4.4 协议对比

根据上述分析与第 2.4 节中的回顾分析,我们将协议 2 与 Shi 等人[29]的量子 LA 协议和已有的量子 AV 协议[30-32]做了简单对比,如表 2 所示. 显然,在具有确定性成功率的协议中,我们的协议效率仅次于 Mishra 等人[32]的协议 7. 而正如第 2.4 节所述,协议 7 与迭代性 QAV 协议都具有泄露否定票数的可能性,但是我们的协议不会泄露否定票数. 最后,我们的协议还考虑了一个可能进行主动攻击的第三方,而非半诚实第三方,而其他协议都没有考虑这一点. 因此,我们的协议在保持了高效的同时,实现了安全性的进一步提升.

表 2 协议 2 与类似量子协议比较

协议	类型	单次计算复杂度	单次通信复杂度	迭代次数	失败率	保护票数
[29]	LA	$O(2^n)$	$O(n^2)$	1	0	√
[30]	AV	$O(n)$	$O(n)$	$O(\log n)$	0	×
[31]	AV	$O(nl)$	$O(nl)$	1	2^{-l}	√
[32] QAV1~4	AV	$O(n^2l)$	$O(n^2l)$	1	2^{-l}	√
[32] QAV5	AV	$O(n^2)$	$O(n^2)$	$O(\log n)$	2^{-l}	×
[32] QAV6	AV	$O(n)$	$O(n)$	$O(\log n)$	0	×
[32] QAV7	AV	$O(n\log n)$	$O(n\log n)$	1	0	×
协议 2	AOV	$O(n\log^2 n)$	$O(n\log n)$	1	0	√

对于已有的最小公倍数协议[6],我们给出了协议 3 与其的比较结果,如表 3 所示. 显然,我们的协议相比经典同类协议实现了指数加速,并且实现了恶意模型下的无条件安全性.

表 3 协议 3 与经典最小公倍数协议比较

协议	计算复杂度	通信复杂度
协议 3	$O(n^3m^2\log(nm))$	$O(n^2m\log(nm))$
[6]	$O(2^{\frac{m}{2}}nm)$	$O(2^{\frac{m}{2}}n)$

5 基于最小公倍数协议的扩展应用

本节中,我们基于 LCM 协议提出了一些扩展应用,包括安全多方的最大公约数计算、分数求和、最大值计算等. 由于这些应用的正确性和安全性都建立在 LCM 协议上,故我们只说明这些问题均可以规约到 LCM 问题上,从而都可用 LCM 协议解决.

5.1 最大公约数计算

定义 8. 最大公约数问题. 设 n 个参与方 $P_1,P_2,\cdots,P_n$分别有私有整数 $x_1,x_2,\cdots,x_n$,这些人进行安全多方计算,每个 P_i除得到 $\gcd\limits_{i\in[\![n]\!]}(x_i)$外,不得到他人的其他信息.

我们解决该问题的思想见如定理 5,其表明了 LCM 和 GCD 之间的数学关系,证明见附录.

定理 5. 令 $\omega_i=\dfrac{\operatorname{lcm}\limits_{j\in[\![n]\!]}(x_j)}{x_i}$,则有

$$\gcd_{i\in[\![n]\!]}(x_i)=\frac{\operatorname{lcm}\limits_{j\in[\![n]\!]}(x_j)}{\operatorname{lcm}\limits_{k\in[\![n]\!]}(\omega_k)}.$$

我们首先计算各自输入方的私有整数的最小公倍数,然后将结果除以各自的整数得到商,从而将求最大公约数转化为求这些商的最小公倍数. 值得注意的是,该过程需要知道最小公倍数,在人数很低时可能会泄露信息. 协议的主要过程如下.

协议 4. 量子安全多方最大公约数计算.

输入:$P_1,P_2,\cdots,P_n$各自有其私有整数$x_1,x_2,\cdots,x_n\in[2^m]$

输出:$y=\gcd\limits_{i\in[\![n]\!]}(x_i)$和 $z=\operatorname{lcm}\limits_{i\in[\![n]\!]}(x_i)$

1. 调用协议 3(参数$m_1=m$),计算后TP得到$z=\operatorname{lcm}\limits_{j\in[\![n]\!]}(x_j)$,并广播给其他人;

2. 对每个 P_i,计算出 $\omega_i=\dfrac{z}{x_i}$;

3. 调用协议 3(参数 $m_2=nm$),计算后 TP 将得到输出 $\lambda=\operatorname{lcm}\limits_{k\in[\![n]\!]}(\omega_k)$;

4. TP 计算出 $y=\dfrac{z}{\lambda}$,并广播给其他人.

5.2 有理数求和

定义 9. 有理数求和问题. 设 n 个参与方 $P_1,P_2,\cdots,P_n$ 分别有私有有理数$\dfrac{a_1}{b_1},\dfrac{a_2}{b_2},\cdots,\dfrac{a_n}{b_n}$,其中 $\forall i\in[\![n]\!],\gcd(a_i,b_i)=1$. 这些人进行安全多方计算,每个 P_i除得到$\dfrac{x}{y}=\dfrac{a_1}{b_1}+\dfrac{a_2}{b_2}+\cdots+\dfrac{a_n}{b_n}$外,不得到他人的其他信息.

我们首先计算各自输入方的分母的最小公倍数,然后各方根据最小公倍数将自己的分数进行通分,最后使用协议 1 对通分后的分子进行求和(可增添星-环混合拓扑). 协议的主要过程如下.

协议 5.　量子安全多方有理数求和.

输入：$P_1,P_2,\cdots,P_n$ 各自有其私有整数 $\frac{a_1}{b_1},\frac{a_2}{b_2},\cdots,\frac{a_n}{b_n}$，其中 $\forall i\in[\![n]\!],a_i,b_i\in[2^m]$

输出：$\frac{x}{y}=\frac{a_1}{b_1}+\frac{a_2}{b_2}+\cdots+\frac{a_n}{b_n}$

1. 调用协议 3(参数 $m_1=m$)，计算后 TP 得到 $z=\underset{j\in[\![n]\!]}{\mathrm{lcm}}(b_j)$，并广播给其他人；

2. 对每个 P_i，计算出 $\omega_i=\frac{z}{b_i}a_i$；

3. 调用协议 1(参数 $m_2=m$)，计算后 TP 得到 $\lambda=\sum_{k\in[\![n]\!]}\omega_k$；

4. TP 计算出 $x/y=\frac{\lambda}{z}$，并广播给其他人.

5.3　最值计算

定义 10.　最值计算问题. 设 n 个参与方 $P_1,P_2,\cdots,P_n$ 分别有私有整数 $x_1,x_2,\cdots,x_n$. 这些人进行安全多方计算，每个参与方 P_i 除了能得到最值 $y=\max(x_1,x_2,\cdots,x_n)$(或 $y=\min(x_1,x_2,\cdots,x_n)$)外，不得到他人的其他信息.

作为例子，我们只描述如何计算最大值. 假设所有的输入整数 $x_1,x_2,\cdots,x_n$ 都属于一个已知偏序集 $U=\{u_0,u_1,\cdots,u_{L-1}\}$，且 $u_0<u_1<\cdots<u_{L-1}$. 那么，对每个 x_i 都存在一个 $k_i\in[L]$，使得 $x_i=u_{k_i}$. 设最大值 $y=u_z$，则由偏序集的性质有 $z=\max(k_1,k_2,\cdots,k_n)$. 此时，每个 P_i 取正整数 $\omega_i=2^{k_i}$，则根据最小公倍数的性质有 $\underset{j\in[\![n]\!]}{\mathrm{lcm}}(\omega_j)=\underset{j\in[\![n]\!]}{\mathrm{lcm}}(2^{k_j})=2^{\max\limits_{j\in[\![n]\!]}(k_j)}=2^z$. 这样，就将多方最大值计算转化为最小公倍数计算. 此外，由于存储所有正整数 $\omega_i=2^{k_i}$ 所需的比特数均为 $O(\log 2^L)=O(L)$，故计算复杂度和通信复杂度均为关于 L,n 的多项式级. 协议的主要过程如下.

协议 6.　量子安全多方最大值计算.

输入：设已知偏序集 $U=\{u_0,u_1,\cdots,u_{L-1}\}$，$u_0<u_1<\cdots<u_{L-1}$，$P_1,P_2,\cdots,P_n$ 各自有其私有整数 $x_1,x_2,\cdots,x_n$，其中 $\forall i\in[\![n]\!],x_i=u_{k_i}\in U$

输出：$y=\max(x_1,x_2,\cdots,x_n)$

1. 对每个 P_i，计算出正整数 $\omega_i=2^{k_i}$；

2. 调用协议 3(参数 $m_1=L$)，计算后 TP 得到 $\lambda=\underset{j\in[\![n]\!]}{\mathrm{lcm}}(\omega_j)$；

3. TP 计算 $z=\log_2\lambda$，则 $y=u_z$，并广播给其他人.

6　结　论

本文中，我们提出了求解最小公倍数问题的量子安全多方计算协议. 首先提出了星-环混合拓扑，其可以高概率防御共谋攻击和伪造攻击；然后设计了一个量子匿名输出检验协议，其不泄露每个人的结果检验信息；随后，我们基于周期函数的连接的周期是各周期的最小公倍数这一性质，提出了一个基于量子周期查找算法的最小公倍数计算协议，其以多项式时间完成计算，并且在恶意模型下是无条件安全的；最后，基于最小公倍数协议，提出一些扩展应用.

我们工作的意义在于：(1) 提出的计算协议将计算最小公倍数的复杂度从指数级降低至多项式级；(2) 通过星-环混合拓扑实现了在共谋攻击下的无条件安全性；(3) 通过设计一个匿名输出检验协议，解决了最小公倍数协议成功概率不高的问题；(4) 我们的协议可以应用于一些具体的 SMC 问题上. 虽然我们的协议可以有效解决最小公倍数问题，但仍存在一些有待进一步改进或探索的地方：(1) 提出的协议是概率性的，必须要重复进行多次，并配合匿名输出检验才能计算出正确结果，是否能找到某种确定性的协议是我们未来研究工作之一；(2) 如何去除非共谋第三方假设，建立恶意参与方之间的制衡机制；(3) 如何改造该协议，使其能够更有效地应用于如集合计算与几何计算问题等应用更广的 SMC 问题.

致　谢　作者感谢所有在本文撰写、审查、修改过程中给予帮助者！

参　考　文　献

[1] Yao A C. Protocols for secure computations//Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science. Piscataway, USA, 1982: 160-164

[2] Fagin R, Naor M, Winkler P. Comparing information without leaking it. Communications of the ACM, 1996, 39(5): 77-85

[3] Du W, Atallah J M. Privacy-preserving cooperative scientific computations//Proceedings of the 14th IEEE Computer Security Foundations Workshop. Nova Scotia, Canada, 2001: 273-282

[4] Xiong L Z, Zhou W H, Xia Z H, et al. Efficient privacy-preserving computation based on additive secret sharing. arXiv preprint arXiv:2009.05356, 2009

[5] Tang Chun-Ming, Shi Gui-Hua, Yao Zheng-An. Secure multi-party computation protocol for sequencing problem. Scientia Sinica Informationis, 2011, 41(7): 789-797(in Chinese)
(唐春明，石桂花，姚正安. 排序问题的安全多方计算协议. 中国科学：信息科学，2011，41(7)：789-797)

[6] Yang Xiao-Yi, Li Shun-Dong, Kang Jia. Private substitution and its applications in private scientific computation. Chinese Journal of Computers, 2018, 41(5): 1132-1142(in Chinese)

(杨晓艺，李顺东，亢佳. 保密替换及其在保密科学计算中的应用. 计算机学报，2018，41(5)：1132-1142)

[7] Kim E Y，Lee H S，Park J. Towards round-optimal secure multiparty computations：Multikey FHE without a CRS. International Journal of Foundations of Computer Science，2020，31(2)：157-174

[8] Atallah M J，Du W. Secure multi-party computational geometry //Proceedings of the Algorithms and Data Structures. Berlin，Heidelberg，2001：165-179

[9] Luo Yong-Long，Huang Liu-Sheng，Xu Wei-Jiang，Jing Wei-Wei. A protocol for privacy-preserving intersect-determination of two polygons. Acta Electronica Sinica，2007，35(4)：685-691(in Chinese)
(罗永龙，黄刘生，徐维江，荆巍巍. 一个保护私有信息的多边形相交判定协议. 电子学报，2007，35(4)：685-691)

[10] Li S D，Wu C Y，Wang D S，Dai Y Q. Secure multiparty computation of solid geometric problems and their applications. Information Sciences，2014，282(1)：401-413

[11] Chen Zhen-Hua，Li Shun-Dong，Chen Li-Chao，et al. Fully privacy-preserving determination of point-range relationship. Scientia Sinica Informationis，2018，48(2)：187-204(in Chinese)
(陈振华，李顺东，陈立朝等. 点和区间关系的全隐私保密判定. 中国科学：信息科学，2018，48(2)：187-204)

[12] Chen Zhen-Hua，Huang Lu-Qi，Shi Xiao-Nan，Nie Jing-Jing. Three basic information-theoretic secure protocols for outsourcing computing and privacy-preserving determination of spatial location-relation. Journal of Xi'an University of Science and Technology，2019，39(6)：1049-1056(in Chinese)
(陈振华，黄路琪，史晓楠，聂靖靖. 信息论安全的 3 个基础外包计算协议及空间位置关系保密判定. 西安科技大学学报，2019，39(6)：1049-1056)

[13] Freedman M J，Hazay C，Nissim K，Pinkas B. Efficient set intersection with simulation-based security. Journal of Cryptology，2016，29(1)：115-155

[14] Dou Jia-Wei，Liu Xu-Hong，Zhou Su-Fang，Li Shun-Dong. Efficient secure multiparty set operations protocols and their application. Chinese Journal of Computers，2018，41(8)：1844-1860(in Chinese)
(窦家维，刘旭红，周素芳，李顺东. 高效的集合安全多方计算协议及应用. 计算机学报，2018，41(8)：1844-1860)

[15] Zhou Su-Fang，Li Shun-Dong，Guo Yi-Min，et al. Efficient secure set intersection problem computation. Chinese Journal of Computers，2018，41(2)：464-480(in Chinese)
(周素芳，李顺东，郭奕旻等. 保密集合相交问题的高效计算. 计算机学报，2018，41(2)：464-480)

[16] Song Xiang-Fu，Gai Min，Zhao Sheng-Nan，Jiang Han. Privacy-preserving statistics protocol for set-based computation. Journal of Computer Research and Development，2020，57(10)：2221-2231(in Chinese)
(宋祥福，盖敏，赵圣楠，蒋瀚. 面向集合计算的隐私保护统计协议. 计算机研究与发展，2020，57(10)：2221-2231)

[17] Cheng Nan，Zhao Yun-Lei. Efficient approach regarding two-party privacy-preserving set union/intersection cardinality. Journal of Cryptologic Research，2021，8(2)：352-364(in Chinese)
(程楠，赵运磊. 一种高效的关于两方集合并/交集基数的隐私计算方法. 密码学报，2021，8(2)：352-364)

[18] Zhao Xue-Ling，Jia Zhu-Liang，Li Shun-Dong. A secure multiparty intersection computation. Journal of Cryptologic Research，2022，9(2)：294-307(in Chinese)
(赵雪玲，家珠亮，李顺东. 集合交集问题的安全计算. 密码学报，2022，9(2)：294-307)

[19] Liu J，Tian Y，Zhou Y，et al. Privacy preserving distributed data mining based on secure multi-party computation. Computer Communications，2020，153(1)：208-216

[20] Sin G T，Cao J N，Lee C S. DAG：A general model for privacy-preserving data mining. IEEE Transactions on Knowledge and Data Engineering，2020，32(1)：40-53

[21] Du W L，Atallah M J. Privacy-preserving cooperative statistical analysis//Proceedings of the Annual Computer Security Applications Conference. New Orleans，USA，2001：102-110

[22] Vaidya J. Privacy-preserving statistics. IEEE Computer，2018，51(9)：8-9

[23] Grover L K. Quantum mechanics helps in searching for a needle in a haystack. Physical Review Letters，1997，79(2)：325-328

[24] Deutsch D，Jozsa R. Rapid solution of problems by quantum computation. Proceedings of the Royal Society of London. Series A，1992，439(1907)：553-558

[25] Simon D R. On the power of quantum computing. SIAM Journal of Computing，1997，26(5)：1474-1483

[26] Shor P W. Algorithms for quantum computation：Discrete logarithms and factoring//Proceedings of the 35th Annual Symposium on Foundations of Computer Science. Los Alamitos，USA，1994：124-134

[27] Shor P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing，1997，26(5)：1484-1509

[28] Nielsen M A，Chuang I L. Quantum Computation and Quantum Information. Cambridge，UK：Cambridge University Press，2000

[29] Shi R H，Li Y F. Quantum protocol for secure multiparty logical AND with application to multiparty private set intersection cardinality. IEEE Transactions on Circuits and Systems I：Regular Papers，2022，69(12)：5206-5218

[30] Rahaman R，Kar G. GHZ correlation provides secure anonymous veto protocol. arXiv preprint arXiv：1507.00592，2015

[31] Wang Q，Li Y，Yu C，et al. Quantum-based anonymity and secure veto. Quantum Information Processing，2021，20(3)：85

[32] Mishra S，Thapliyal K，Parakh A，Pathak A. Quantum anonymous veto：A set of new protocols. EPJ Quantum Technology，2022，9(1)：14

[33] Shi R H, Mu Y, Zhong H, et al. Secure multiparty quantum computation for summation and multiplication. Scientific Reports, 2016, 6(1): 19655

[34] Goldreich O. Foundations of Cryptography. Cambridge, UK: Cambridge University Press, 2004

[35] Murta G, Grasselli F, Kampermann H, Bruß D. Quantum conference key agreement: A review. Advanced Quantum Technologies, 2020, 3(11): 2000025

[36] Cao X Y, Lu Y S, Li Z, et al. High key rate quantum conference key agreement with unconditional security. IEEE Access, 2021, 9(1): 128870-128876

[37] Yi H-M, Zhou R-G, Xu R-Q. Anonymous quantum conference key agreement using the W state. Quantum Information Processing, 2023, 22(8): 306

[38] Thapliyal H, MuÑoz-Coreas E, Varun T S S, Humble T S. Quantum circuit designs of integer division optimizing T-count and T-depth. IEEE Transactions on Emerging Topics in Computing, 2021, 9(2): 1045-1056

[39] Draper T G. Addition on a quantum computer. arXiv preprint arXiv: quant-ph/0008033, 2000

[40] Liu W J, Li Z X. Secure and efficient two-party quantum scalar product protocol with application to privacy-preserving matrix multiplication. IEEE Transactions on Circuits and Systems I: Regular Papers, 2023, 70(11): 4456-4469

[41] Li Z, Liu T, Zhu H. Private comparison protocol for multiple semi-quantum users based on bell states. International Journal of Theoretical Physics, 2022, 61(6): 177

[42] Kou T-Y, Che B-C, Dou Z, et al. Efficient quantum private comparison protocol utilizing single photons and rotational encryption. Chinese Physics B, 2022, 31(6): 060307

[43] Joseph J, Ali S T. Multiparty quantum private comparison based on quantum walks. Quantum Information Processing, 2022, 22(1): 17

[44] Lian J-Y, Li X, Ye T-Y. Multi-party semiquantum private comparison of size relationship with d-dimensional bell states. EPJ Quantum Technology, 2023, 10(1): 10

附录 1.　用于证明的引理.

引理 1.　设有如下的二系统傅里叶纠缠态：

$$|\Psi(x)\rangle_{(A,B)}=\frac{1}{\sqrt{2^m}}\sum_{j\in[2^m]}e^{\frac{\sqrt{-1}2\pi V_1(x)}{2^m}j}|V_2(j,x)\rangle_A|\varphi(j)\rangle_B,$$

其中$\langle V_2(j',x)|V_2(j,x)\rangle_A=\delta_{jj'}$，$V_1$，$V_2$都是隐私信息 x 的函数，则当只拥有系统 B 时，在 x 的任意两个不同取值之间，其对应的量子态都统计不可区分.

证明.　总态的密度算子为

$$\rho_{AB}(x)=|\Psi(x)\rangle\langle\Psi(x)|=$$

$$\frac{1}{2^m}\sum_{j,j'\in[2^m]}e^{\frac{\sqrt{-1}2\pi V_1(x)}{2^m}(j-j')}|V_2(j,x)\rangle\langle V_2(j',x)|_A|\varphi(j)\rangle\langle\varphi(j')|_B,$$

则系统 B 的约化密度算子为

$$\rho_B(x)=\mathrm{Tr}_A(\rho_{AB}(x))$$

$$=\frac{1}{2^m}\sum_{j,j'\in[2^m]}e^{\frac{\sqrt{-1}2\pi V_1(x)}{2^m}(j-j')}\mathrm{Tr}(|V_2(j,x)\rangle\langle V_2(j',x)|_A)|\varphi(j)\rangle\langle\varphi(j')|_B$$

$$=\frac{1}{2^m}\sum_{j,j'\in[2^m]}e^{\frac{\sqrt{-1}2\pi V_1(x)}{2^m}(j-j')}\langle V_2(j',x)|V_2(j,x)\rangle_A|\varphi(j)\rangle\langle\varphi(j')|_B$$

$$=\frac{1}{2^m}\sum_{j,j'\in[2^m]}e^{\frac{\sqrt{-1}2\pi V_1(x)}{2^m}(j-j')}\delta_{jj'}|\varphi(j)\rangle\langle\varphi(j')|_B$$

$$=\frac{1}{2^m}\sum_{j\in[2^m]}|\varphi(j)\rangle\langle\varphi(j)|_B,$$

即若 $x_1\neq x_2$，必有 $\rho_B(x_1)=\rho_B(x_2)$，从而统计不可区分.

证毕.

引理 2.　对于任意正整数 Q，若 $M\geq Q^2$ 成立，$x_i\in[\![M]\!]$ 均匀选取，则 $\Pr\left[Q\middle|\sum_{i\in[\![n_0]\!]}x_i\right]\approx\frac{1}{Q}$，其中 n_0 是投否定票的人数.

证明.　首先证若 $M\geq Q^2$，则对于任意 $a\in[Q]$，有 $\Pr[x_i\equiv a(\mathrm{mod}\,Q)]\approx\frac{1}{Q}$. 其等价于 $x_i=a+kQ$，则根据 $1\leq x_i\leq M$ 有 $1\leq a+kQ\leq M$，即 $\left\lceil\frac{1-a}{Q}\right\rceil\leq k\leq\left\lfloor\frac{M-a}{Q}\right\rfloor$，故 k 共对应 $\left\lfloor\frac{M-a}{Q}\right\rfloor-\left\lceil\frac{1-a}{Q}\right\rceil+1$ 种可能性，且

$$\left\lfloor\frac{M-a}{Q}\right\rfloor-\left\lceil\frac{1-a}{Q}\right\rceil+1\leq\frac{M-a}{Q}-\frac{1-a}{Q}+1+1=\frac{M}{Q}+2-\frac{1}{Q},$$

$$\left\lfloor\frac{M-a}{Q}\right\rfloor-\left\lceil\frac{1-a}{Q}\right\rceil+1\geq\frac{M-a}{Q}-1-\frac{1-a}{Q}+1=\frac{M}{Q}-\frac{1}{Q},$$

即 $\Pr[x_i\equiv a(\mathrm{mod}\,Q)]\in\frac{1}{Q}+\left[-\frac{1}{QM},\frac{2}{M}-\frac{1}{QM}\right]$. 而当成立 $M=KQ^2\geq Q^2$ 时，有 $\frac{2}{M}-\frac{1}{QM}=\frac{2}{KQ^2}-\frac{1}{KQ^3}<\frac{1}{KQ}\ll\frac{1}{Q}$，$\frac{1}{QM}=\frac{1}{KQ^3}<\frac{1}{KQ}\ll\frac{1}{Q}$，从而 $\Pr[x_i\equiv a(\mathrm{mod}\,Q)]\approx\frac{1}{Q}$.

现在证明 $\Pr\left[Q\middle|\sum_{i\in[\![n_0]\!]}x_i\right]\approx\frac{1}{Q}$. 以下计算省略“mod Q”.

$$\Pr\left[Q\middle|\sum_{i\in[\![n_0]\!]}x_i\right]=\Pr\left[\sum_{i\in[\![n_0]\!]}x_i\equiv 0\right]$$

$$=\sum_{a_1\in[Q]}\Pr\left[\sum_{i\in[\![n_0]\!]-[\![1]\!]}x_i\equiv a_1\right]\Pr[x_1\equiv -a_1]$$

$$\approx\frac{1}{Q}\sum_{a_1\in[Q]}\Pr\left[\sum_{i\in[\![n_0]\!]-[\![1]\!]}x_i\equiv a_1\right],$$

$$\Pr\left[\sum_{i\in[\![n_0]\!]-[\![1]\!]}x_i\equiv a_1\right]=\sum_{a_2\in[Q]}\Pr\left[\sum_{i\in[\![n_0]\!]-[\![2]\!]}x_i\equiv a_2\right]\Pr[x_2\equiv a_1-a_2]$$

$$\approx\frac{1}{Q}\sum_{a_2\in[Q]}\Pr\left[\sum_{i\in[\![n_0]\!]-[\![2]\!]}x_i\equiv a_2\right],$$

$$\cdots$$

$$\Pr[x_{n_0}\equiv a_{n_0-1}]\approx\frac{1}{Q},$$

故有

$$\Pr\Big[Q\Big|\sum_{i\in[\![n_0]\!]}x_i\Big]=\frac{1}{Q}\sum_{a_1\in[Q]}\Pr\Big[\sum_{i\in[\![n_0]\!]-[\![1]\!]}x_i\equiv a_1\Big]$$

$$=\frac{1}{Q^2}\sum_{a_1,a_2\in[Q]}\Pr\Big[\sum_{i\in[\![n_0]\!]-[\![2]\!]}x_i\equiv a_2\Big]=\cdots$$

$$=\frac{1}{Q^{n_0-1}}\sum_{a_1,a_2,\cdots,a_{n_0-1}\in[Q]}\Pr[x_{n_0}\equiv a_{n_0-1}]$$

$$=\frac{1}{Q^{n_0}}\sum_{a_1,a_2,\cdots,a_{n_0-1}\in[Q]}1=\frac{1}{Q^{n_0}}Q^{n_0-1}=\frac{1}{Q}.$$

证毕.

引理 3. 令 $M=4K\geq 4$,例如取倍数 $K=100$ 或以上,$m=\lfloor\log(nM)\rfloor+1$,则以下两个随机变量统计不可区分:.

(1) $z=q\sum_{i\in[\![n_0]\!]}x_i \bmod 2^m$,其中 $x_i\in[\![M]\!]$ 和 $q\in[2^m]^\circ$ 均为均匀选取,$1\leq n_0\leq n$;

(2) $\hat{z}=\hat{q}\hat{x}_1 \bmod 2^m$,其中 $\hat{x}_1\in[\![M]\!]$ 和 $\hat{q}\in[2^m]^\circ$ 均为均匀选取.

证明. 注意到两个随机变量都不可能取 0,故设取值为 $z'=s2^{m_1}\in[2^m]$,其中 $s\in[2^{m-m_1}]^\circ$ 是其奇数因子,$2^0\leq 2^{m_1}<2^m$ 是其偶数因子. 那么,其迹距离为

$$D(\hat{z},z)=\frac{1}{2}\sum_{z'}|\Pr[\hat{z}=z']-\Pr[z=z']|$$

$$=\frac{1}{2}\sum_{\substack{m_1\in[m],\\ s\in[2^{m-m_1}]^\circ}}|\Pr[\hat{z}=s2^{m_1}]-\Pr[z=s2^{m_1}]|.$$

我们首先计算各自的概率值. 对于 $\hat{z}$,有

$$\Pr[\hat{z}=s2^{m_1}]=\Pr[\hat{x}_1\hat{q}\equiv s2^{m_1}\pmod{2^m}]$$

$$=\sum_{q'\in[2^m]^\circ}\Pr[\hat{q}=q']\Pr[\hat{x}_1q'=s2^{m_1}\pmod{2^m}]$$

$$=\sum_{q'\in[2^m]^\circ}\frac{1}{2^{m-1}}\Pr\Big[\hat{x}_1=sq'^{-1}2^{m_1} \bmod 2^m\in[\![M]\!]\Big]$$

$$=\frac{1}{2^{m-1}}\sum_{\substack{q'\in[2^m]^\circ,\\ sq'^{-1}2^{m_1}\bmod 2^m\in[\![M]\!]}}\Pr[\hat{x}_1=sq'^{-1}2^{m_1} \bmod 2^m].$$

其中,对于每一个满足 $a\in[2^m]^\circ$,$a2^{m_1}\in[\![M]\!]$ 的 a 取值,易知 $sq'^{-1}2^{m_1}\equiv a2^{m_1}\pmod{2^m}$ 等价于 $q'\equiv a^{-1}s\pmod{2^{m-m_1}}$,即 $q'=\overline{a^{-1}}s+k2^{m-m_1}$,其中 $\overline{a^{-1}}s\in[2^{m-m_1}]^\circ$,$k\in[2^{m_1}]$,故

$$\Pr[\hat{z}=s2^{m_1}]=\frac{1}{2^{m-1}}\sum_{\substack{a2^{m_1}\in[\![M]\!]\\ a\in[2^m]^\circ}}\sum_{\substack{q'\in[2^m]^\circ,\\ sq'^{-1}2^{m_1}\equiv a2^{m_1}\pmod{2^m}}}\Pr[\hat{x}_1=a2^{m_1}]$$

$$=\frac{2^{m_1}}{2^{m-1}}\sum_{\substack{a2^{m_1}\in[\![M]\!]\\ a\in[2^m]^\circ}}\Pr[\hat{x}_1=a2^{m_1}]=\frac{2^{m_1}}{2^{m-1}}\Pr[2^{m_1}\mid\hat{x}_1,2^{m_1}\nmid\hat{x}_1],$$

这是因为 $\sum_{\substack{a2^{m_1}\in[\![M]\!]\\ a\in[2^m]^\circ}}\Pr[\hat{x}_1=a2^{m_1}]$ 恰好是 $\hat{x}_1$ 取 2^{m_1} 的任何奇数倍的概率. 而根据引理 2,当 $M\geq(2^{m_1+1})^2$ 时,在集合 $[\![M]\!]$ 中近似有 $\frac{M}{2^{m_1+1}}$ 个 2^{m_1} 的奇数倍,即

$$\Pr[\hat{z}=s2^{m_1}]\approx\frac{2^{m_1}}{2^{m-1}}\frac{1}{2^{m_1+1}}=\frac{1}{2^m}.$$

现在考虑 z 的概率分布. 类似地,

$$\Pr[z=s2^{m_1}]=\Pr\Big[q\sum_{i\in[\![n_0]\!]}x_i\equiv s2^{m_1}\pmod{2^m}\Big]$$

$$=\sum_{q\in[2^m]^\circ}\Pr[q=q']\Pr\Big[q'\sum_{i\in[\![n_0]\!]}x_i\equiv s2^{m_1}\pmod{2^m}\Big]$$

$$=\sum_{q\in[2^m]^\circ}\frac{1}{2^{m-1}}\Pr\Big[\sum_{i\in[\![n_0]\!]}x_i=sq'^{-1}2^{m_1} \bmod 2^m\in[\![n_0M]\!]\Big]$$

$$=\frac{1}{2^{m-1}}\sum_{\substack{q'\in[2^m]^\circ,\\ sq'^{-1}2^{m_1}\bmod 2^m\in[\![n_0M]\!]}}\Pr\Big[\sum_{i\in[\![n_0]\!]}x_i=sq'^{-1}2^{m_1} \bmod 2^m\Big].$$

同样,任选一个满足 $a\in[2^m]^\circ$,$a2^{m_1}\in[\![n_0M]\!]$ 的 a 取值,则 $sq'^{-1}2^{m_1}\equiv a2^{m_1}\pmod{2^m}$ 等价于 $q'=\overline{a^{-1}}s+k2^{m-m_1}$,其中 $\overline{a^{-1}}s\in[2^{m-m_1}]^\circ$,$k\in[2^{m_1}]$,故

$$\Pr[z=s2^{m_1}]=\frac{1}{2^{m-1}}\sum_{\substack{a2^{m_1}\in[\![n_0M]\!]\\ a\in[2^m]^\circ}}\sum_{\substack{q'\in[2^m]^\circ\\ sq'^{-1}2^{m_1}\equiv a2^{m_1}\pmod{2^m}}}\Pr\Big[\sum_{i\in[\![n_0]\!]}x_i=a2^{m_1}\Big]$$

$$=\frac{1}{2^{m-1}}\sum_{\substack{a2^{m_1}\in[\![n_0M]\!]\\ a\in[2^m]^\circ}}\sum_{k\in[2^{m_1}]}\Pr\Big[\sum_{i\in[\![n_0]\!]}x_i=a2^{m_1}\Big]$$

$$=\frac{2^{m_1}}{2^{m-1}}\sum_{\substack{a2^{m_1}\in[\![n_0M]\!]\\ a\in[2^m]^\circ}}\Pr\Big[\sum_{i\in[\![n_0]\!]}x_i=a2^{m_1}\Big]$$

$$=\frac{2^{m_1}}{2^{m-1}}\Pr\Big[2^{m_1}\Big|\sum_{i\in[\![n_0]\!]}x_i,2^{m_1}\nmid\sum_{i\in[\![n_0]\!]}x_i\Big]$$

$$\approx\frac{2^{m_1}}{2^{m-1}}\frac{1}{M}\frac{M}{2^{m_1+1}}=\frac{1}{2^m}.$$

类似地,根据引理 2,当 $M\geq(2^{m_1+1})^2$ 时,有

$$\Pr\Big[2^{m_1}\Big|\sum_{i\in[\![n_0]\!]}x_i,2^{m_1+1}\nmid\sum_{i\in[\![n_0]\!]}x_i\Big]$$

$$=\Pr\Big[2^{m_1}\Big|\sum_{i\in[\![n_0]\!]}x_i\Big]-\Pr\Big[2^{m_1+1}\Big|\sum_{i\in[\![n_0]\!]}x_i\Big]$$

$$\approx\frac{1}{2^{m_1}}-\frac{1}{2^{m_1+1}}=\frac{1}{2^{m_1+1}}.$$

为了满足 $M\geq(2^{m_1+1})^2$ 的要求,设 $M=2^{m_M}=K(2^{m_1+1})^2$,其中 $K=2^{m_K}$,则 $2m_1+2+m_K\leq m_M$,$m_1\leq\frac{m_M-m_K}{2}-1$. 因此,想要至少存在一个 m_1,需要 $\frac{m_M-m_K}{2}\geq 1$,即 $m_M\geq m_K+2$,$m_M=4K$. 在此条件下,有

$$D(\hat{z},z)=\frac{1}{2}\sum_{\substack{m_1\in[m],\\ s\in[2^{m-m_1}]^\circ}}|\Pr[\hat{z}=s2^{m_1}]-\Pr[z=s2^{m_1}]|$$

$$=\frac{1}{2}\sum_{\substack{m_1\leq\frac{m_M-m_K}{2}-1\\ s\in[2^{m-m_1}]^\circ}}|\Pr[\hat{z}=s2^{m_1}]-\Pr[z=s2^{m_1}]|+$$

$$\frac{1}{2}\sum_{\substack{m_1>\frac{m_M-m_K}{2}-1\\ s\in[2^{m-m_1}]^\circ}}|\Pr[\hat{z}=s2^{m_1}]-\Pr[z=s2^{m_1}]|$$

$$\approx\frac{1}{2}\sum_{\substack{m_1>\frac{m_M-m_K}{2}-1\\ s\in[2^{m-m_1}]^\circ}}|\Pr[\hat{z}=s2^{m_1}]-\Pr[z=s2^{m_1}]|$$

$$\leq\frac{1}{2}\sum_{\substack{m_1>\frac{m_M-m_K}{2}-1\\ s\in[2^{m-m_1}]^\circ}}\Pr[\hat{z}=s2^{m_1}]+\frac{1}{2}\sum_{\substack{m_1>\frac{m_M-m_K}{2}-1\\ s\in[2^{m-m_1}]^\circ}}\Pr[z=s2^{m_1}].$$

而

$$\sum_{\substack{m_1>\frac{m_M-m_K}{2}-1\\ s\in[2^{m-m_1}]^*}}\Pr[\hat{z}=s2^{m_1}]=1-\sum_{m_1=0}^{\frac{m_M-m_K}{2}-1}\sum_{s\in[2^{m-m_1}]^*}\Pr[\hat{z}=s2^{m_1}]$$

$$\approx 1-\sum_{m_1=0}^{\frac{m_M-m_K}{2}-1}\frac{2^{m-m_1}}{2^m}\approx 1-\frac{\frac{1}{2}-\frac{1}{2^{\frac{m_M-m_K}{2}-1+1}}\frac{1}{2}}{1-\frac{1}{2}}=\frac{1}{2^{\frac{m_M-m_K}{2}}},$$

同理可得 $\sum_{m_1>\frac{m_M-m_K}{2}-1,s\in[2^{m-m_1}]^*}\Pr[z=s2^{m_1}]\approx\frac{1}{2^{\frac{m_M-m_K}{2}}}$，从而

$$D(\hat{z},z)\leq\frac{1}{2^{\frac{m_M-m_K}{2}}}=2^{\frac{m_K}{2}}\times\frac{1}{2^{\frac{m_M}{2}}}=O\left(\frac{1}{2^{\frac{m_M}{2}}}\right).$$

该式成立只需 $m_M\geq m_K+2$ 即可，从而是可忽略的.

证毕.

引理 4.　设 Alice 制备了一个叠加态 $\sum_j\alpha_j e^{\sqrt{-1}\theta_j}|j\rangle_t$，其中 $\sum_j\alpha_j^2=1$ 都是实数(注意，这里她没有制备粒子 h，因为当她是攻击者时无必要). 她将 t 发给 Bob，而后者会使用如下量子门中的一个：

(1) C：$|j\rangle_t|x\rangle_e\to e^{\frac{\sqrt{-1}2\pi V(x)}{2^m}j}|j\rangle_t|x\rangle_e$，其中 $V(x)$ 是 x 的函数；

(2) U：$|j\rangle_t|0\rangle_e\to|j\rangle_t|f(j)\rangle_e$，其中 $f(j)$ 具有周期 x；

然后会将粒子 t 送回. 那么，Alice 能获得的信息最多分别为 $V(x)$ 和 x，而无法获得任何其他信息.

证明.　首先，在上述操作下 Alice 分别获得的量子信息为：

(1) $|\varphi_1(x)\rangle_{(t,e)}=\sum_j\alpha_j e^{\sqrt{-1}\theta_j}e^{\frac{\sqrt{-1}2\pi V(x)}{2^m}j}|j\rangle_t|x\rangle_e$，

由于粒子 t,e 之间不存在纠缠，故可直接拆分为

$$|\varphi_1(x)\rangle_t=\sum_j\alpha_j e^{\sqrt{-1}\theta_j}e^{\frac{\sqrt{-1}2\pi V(x)}{2^m}j}|j\rangle_t.$$

即只要 $V(x)$ 不变，则 $|\varphi_1(x)\rangle_t$ 也不变，因此 Alice 不可能获得其他信息；

(2) $|\varphi_2(f)\rangle_{(t,e)}=\sum_j\alpha_j e^{\sqrt{-1}\theta_j}|j\rangle_t|f(j)\rangle_e$，

取偏迹可得

$$\begin{aligned}\rho_2(f)&=\mathrm{Tr}_e(|\varphi_2(f)\rangle\langle\varphi_2(f)|_{(t,e)})\\&=\sum_{j,j'}\alpha_{j'}e^{\sqrt{-1}\theta_{j'}}\alpha_j e^{-\sqrt{-1}\theta_j}|j'\rangle\langle j|_t\mathrm{Tr}(|f(j')\rangle\langle f(j)|_e)\\&=\sum_{j,j'}\alpha_{j'}e^{\sqrt{-1}\theta_{j'}}\alpha_j e^{-\sqrt{-1}\theta_j}|j'\rangle\langle j|_t\langle f(j)|f(j')\rangle_e\\&=\sum_j\alpha_j e^{\sqrt{-1}\theta_j}\sum_{j'\equiv j(\mathrm{mod}x)}\alpha_{j'}e^{-\sqrt{-1}\theta_{j'}}|j'\rangle\langle j|_t\end{aligned}$$

即只要 x 不变，则 $\rho_2(f)$ 不变，因此不可能获得其他信息.

证毕.

附录 2.　定理的证明.

定理 1 的证明.　首先我们证明假如计算粒子 t 和验证粒子 g 并不纠缠，例如处于态 $\frac{1}{\sqrt{2^m}}\sum_{j\in[2^m]}|j\rangle_t$ 和 $\frac{1}{\sqrt{2^m}}\sum_{j'\in[2^m]}|j'\rangle_g$，则当施加 $\mathrm{CNOT}^{\otimes m}$ 时，得到

$$\begin{aligned}&\frac{1}{\sqrt{2^m}}\sum_{j\in[2^m]}|j\rangle_t\frac{1}{\sqrt{2^m}}\sum_{j'\in[2^m]}|j'\oplus j\rangle_g\\&=\frac{1}{\sqrt{2^m}}\sum_{j\in[2^m]}|j\rangle_t\frac{1}{\sqrt{2^m}}\sum_{j''-j\in[2^m]}|j''\rangle_g\\&=\frac{1}{\sqrt{2^m}}\sum_{j\in[2^m]}|j\rangle_t\frac{1}{\sqrt{2^m}}\sum_{j'\in[2^m]}|j'\rangle_g,\end{aligned}$$

从而当测量 g 时，其为 $|0\rangle$ 的概率为 $\frac{1}{2^m}$，从而不被发现的概率也是 $\frac{1}{2^m}$. 现在我们分析三种攻击策略：

(1) 伪造攻击：设制备方单独进行了伪造攻击，那么至少有两个参与方 P_k 和 P_l，其对应的验证粒子一个与 t 纠缠，另一个没有，那么其将以概率 $1-\frac{1}{2^m}$ 被发现.

(2) 共谋攻击：同样，若除了制备方以外的一个参与方团体 I_1 进行了伪造攻击，则由于他们伪造的粒子与来自制备方的验证粒子 g 不纠缠，也无法通过上述验证.

(3) 拦截-再发送攻击：设存在参与方进行了拦截-再发送攻击，即获得计算粒子后将其保留，并伪造了另一份与其不纠缠的粒子返回，以试图获取信息，那么他将失败，因为若他之后的参与方中有人与他不共谋，则很容易被后者发现. 由于至少制备方本人不与他共谋，故制备方可以通过 $\mathrm{CNOT}^{\otimes m}$ 验证来发现攻击.

总之，在制备方非共谋假设下，伪造攻击、共谋攻击和拦截-再发送攻击的成功概率均为 $\frac{1}{2^m}$.

证毕.

定理 2 的证明.　设 $f(j)=f(j')$，则有 $f_1(j)\|f_2(j)\|\cdots\|f_n(j)=f_1(j')\|f_2(j')\|\cdots\|f_n(j')$，即对所有 $i\in[\![n]\!]$ 有 $f_i(j)=f_i(j')$，因此 $j\equiv j'(\mathrm{mod}x_i)$，也即 $j-j'=k_ix_i$，其中 k_i 是整数，因此 $j-j'$ 必然是 x_i 的公倍数，从而 $j\equiv j'(\mathrm{mod}y)$；另一方面，设 $j\equiv j'(\mathrm{mod}y)$，即 $j-j'=ky$，则 $j\equiv j'(\mathrm{mod}x_i)$ 成立，则 $f_i(j)=f_i(j')$，从而 $f(j)=f(j')$. 也就是说，$f(j)=f(j')$ 当且仅当 $j\equiv j'(\mathrm{mod}y)$，从而最小公倍数 y 是 $f(j)$ 的最小正周期.

证毕.

定理 3 的证明.　正如我们分析的，我们只需考虑在以下攻击下的安全性：

(1) 测量攻击：不进行额外操作，只分析得到的经典和量子信息. 假设攻击方收集了所有其能收集的经典和量子信息. 在协议 2 中，攻击方 $I_1=(P_2,\cdots,P_n)$ 获得的信息最大只有 $VIEW_{I_1}(c_I)=(c_{I_1},y,x_{I_1},q,\rho_{I_1})$，其中 ρ_{I_1} 是系统 $B=(g_2,g_3,\cdots,g_n,t)$ 所处的态. 于是可构造模拟算法 $SI_{I_1}(c_{I_1},y)=(c_{I_1},y,\hat{x}_{I_1},\hat{q},\hat{\rho}_{I_1})$ 为：

① 按原协议相同的 x_{I_1} 选取方法来选取 $\hat{x}_{I_1}$；随机选取被攻击方 I_2 的输入值 $\hat{x}_{I_2}$.

② 随机选取一个奇数 $\hat{q}\in[2^m]^*$；

③ 攻击方内部模拟协议 2，其中输入参数值分别为 $\hat{x}_{I_1}$，

$\hat{x}_{I_2}$ 和 $\hat{q}$，直到模拟协议与实际上攻击的时间点重合，然后丢弃除了系统 $B=(g_2,g_3,\cdots,g_n,t)$ 外的所有系统 $A=(g_1,h)$，剩下的量子态为 $\hat{\rho}_{I_1}$.

显然，$\hat{x}_{I_1}$ 和 $\hat{q}$ 都和实际视图完全相同，而对于模拟量子态 $\hat{\rho}_{I_1}$，根据引理 1，其与实际协议执行的对应量子态 ρ_{I_1} 是统计不可区分的，因为攻击方只拥有纠缠态的一部分粒子，而不是全部. 因此，$SI_{I_1}(c_{I_1},y)\overset{S}{\equiv}VIEW_{I_1}(c_I)$，即 I_1 没有获得有效信息.

现在考虑 TP. 在协议 2 中 TP 所能获得的信息仅有 $VIEW_{TP}(c_I)=(y,z,\rho_{TP1},\rho_{TP2})$，其中 $z=q\sum_{i\in[\![n]\!]}x_i \bmod 2^m$，$\rho_{TP1}$ 是所有粒子未返回时他所拥有粒子的状态，ρ_{TP2} 是粒子完全返回后他所拥有系统的状态. 为了模拟该视图，我们构建如下模拟算法 $SI_{TP}(y)=(y,\hat{z},\hat{\rho}_{TP1},\hat{\rho}_{TP2})$：

① 若 $y=1$，则 $\hat{z}=0$；

② 若 $y=0$，则计算随机选择一个正整数 $\hat{x}_1\in[\![M]\!]$，随机选择 $\hat{q}\in[2^m]^\circ$，令 $\hat{z}=\hat{q}\hat{x}_1 \bmod 2^m$；

③ 随机选取其他参与方 I 的输入值 $\hat{x}_I$，只要存在否定票，然后自己模拟协议 2，输入参数分别为 $\hat{x}_I$ 和 $\hat{q}$，直到模拟协议与实际上攻击的时间点重合，然后丢弃除了粒子 h 外的所有粒子，剩下的量子态为 $\hat{\rho}_{TP1}$.

④ 制备态 $|\hat{z}\rangle_h|0\rangle_t$，然后对其施加 QFT 和 $\mathrm{CNOT}^{\otimes m}$ 以得到 $\hat{\rho}_{TP2}$.

为了证明确实有 $SI_{TP}(y)\overset{S}{\equiv}VIEW_{TP}(c_I)$，首先当 $y=1$ 时，显然 $\hat{z}=z$；当 $y=0$ 时，由引理 3，可知无论否定票人数 $1\leq n_0\leq n$ 为多少，都有 $\hat{z}\overset{S}{\equiv}z$. 与模拟器 SI_{I_1} 类似，由引理 1，无论他输入什么值 $\hat{x}_I$ 和 $\hat{q}$，能得到的量子态都无法区分，故 $\hat{\rho}_{TP1}\overset{S}{\equiv}\rho_{TP1}$；而当协议正常运行时，他对最后到手的粒子的所有操作都是可逆的，故只需用模拟的 $\hat{z}$ 反推即可模拟出量子态 $\hat{\rho}_{TP2}$. 综上，有 $SI_{TP}(y)\overset{S}{\equiv}VIEW_{TP}(c_I)$，从而 TP 也没有获得信息.

(2) 非法密钥分发：在第 2 步时，参与方 I_1 在量子密钥分发过程中作弊. 无论作弊的策略如何，这个操作都不会带来信息泄露，因为密钥分发的结果与各方的输入信息无关，其唯一会影响的就是 TP 获得的结果，而参与方是无法获得信息的；另一方面，通过使用量子相等比较等方法，参与方之间可以检验各方获得的密钥 q 是否相同，从而以高概率发现这种攻击. 由于攻击者和 TP 是非共谋的，故 TP 不知道攻击者的作弊策略，也就无法从这种攻击中获得额外信息. 非共谋是必要条件，因为若 TP 与攻击者不满足非共谋条件，那么最简单的攻击就是将密钥 q 泄露给 TP，从而获得输入信息.

(3) 非法制备：在第 3 步时，TP 在制备叠加态时没有制备正确的平衡叠加态，但是正常纠缠所有粒子. 根据引理 4 可知，即使他进行了伪造，也无法获得协议 2 理应获得的 z 以外的信息，因此与(1)测量攻击一致，他获得的视图可模拟.

(4) 非法输入：得到粒子后参与方 I_1 不施加正确的 C_j 门. 注意，若他们只篡改自己的经典输入，这种情况是恶意模型所允许的，并且没有办法防御，因此我们只考虑他们甚至不进行正确的量子操作的情况. 显然，在这种情况下根本没有任何信息收益，仅有的可能后果是 TP 得到错误的输出，但由于 TP 不与 I_1 串通，故 TP 也不会获得额外信息. 因此该行为是纯粹的破坏，可以不考虑.

(5) 纠缠-测量攻击：得到粒子 a(包含所有获得的粒子)后，参与方 I_1 准备一个辅助粒子 b，然后纠缠 a,b. 设 a 的某个基态为 $|\varphi\rangle$，则纠缠门的一般定义为

$$|\varphi\rangle_a|0\rangle_b\rightarrow\sqrt{\eta}|\varphi\rangle_a|\varepsilon(\varphi)\rangle_b+\sqrt{1-\eta}|\delta(\varphi)\rangle_{(a,b)},$$

其中 $0\leq\eta\leq1$ 是不改变 a 所处基态的概率. I_1 随后将粒子 a 发送给下一个参与方，并保留 b，等到合适的时机，就分析 b 上的量子信息. 为了通过星环-混合拓扑的验证，上述操作必须不改变 a 所处基态，即 $\eta=1$；而为了区分信息，$|\varepsilon(\varphi)\rangle$ 与 $|\varphi\rangle$ 应一一对应且保持正交，即存在酉变换 $|j\rangle\rightarrow|\varepsilon(j)\rangle$. 注意到只有当所有粒子返回 TP 时，TP 的 $\mathrm{QFT}^\dagger$ 操作才有可能改变傅里叶纠缠态的实质，从而突破引理 1 的限制，故我们只考虑这个时间点. 显然，当 I_1 有 $n-1$ 人参与时，a 中将包含除了 h,t,g_1 以外的所有粒子，而这些粒子等价于只有一个 $|j\rangle_a$，因为更多粒子可以从 $|0\rangle$ 态通过复制门得到；同理，a 以外的有关粒子也等价于只有一个 $|j\rangle_h$. 于是，当施加了纠缠门，并返回粒子 a 后，量子态为 $\frac{1}{\sqrt{2^m}}\sum_{j\in[2^m]}e^{\frac{\sqrt{-1}2\pi z}{2^m}j}|j\rangle_h|\varepsilon(j)\rangle_b$，其中 z 是求和信息. 此时，TP 对其施加 $\mathrm{QFT}^\dagger$，得到

$$\begin{aligned}&\frac{1}{\sqrt{2^m}}\sum_{j\in[2^m]}e^{\frac{\sqrt{-1}2\pi z}{2^m}j}|j\rangle_h|\varepsilon(j)\rangle_b\\&\xrightarrow{\mathrm{QFT}^\dagger}\frac{1}{2^m}\sum_{j\in[2^m]}e^{\frac{\sqrt{-1}2\pi z}{2^m}j}\sum_{k\in[2^m]}e^{-\frac{\sqrt{-1}2\pi k}{2^m}j}|k\rangle_h|\varepsilon(j)\rangle_b\\&=\frac{1}{2^m}\sum_{k\in[2^m]}|k\rangle_h\Big(\sum_{j\in[2^m]}e^{\frac{\sqrt{-1}2\pi(z-k)}{2^m}j}|\varepsilon(j)\rangle_b\Big),\end{aligned}$$

从而 TP 通过测量获得了随机数 k. 显然，此时对于 TP 而言，他获得的量子信息等价于施加 $\mathrm{QFT}^\dagger$ 之前的信息，因为两者可以通过酉算子 $\mathrm{QFT}^\dagger$ 进行可逆变换. 因此 I_1 虽然施加了纠缠门，但是总系统仍处于引理 1 中的广义傅里叶叠加态，因此 TP 此时的视图 $VIEW_{TP}(c_I)=(\rho_{TP})$ 不含任何有关 z，从而 c_I 的信息，从而很容易模拟他的视图，模拟器构造方法与前文类似，只需随机输入然后自己模拟整个协议即可.

另一方面，由于 TP 不会公布自己测量得到的 k，因此，对于 I_1 而言，等价于 TP 没有进行测量，从而上述论述对于 I_1 也成立，即总态仍然是傅里叶纠缠态，从而 I_1 此时的视图 $VIEW_{I_1}(c_I)=(c_{I_1},x_{I_1},\rho_{I_1})$ 也可被模拟，即没有从纠缠-测量攻击中获得信息. 就本质而言，这是因为 TP 和 I_1 没有共谋，测量结果 k 没有互通，导致了没有信息收益的结果.

(6) 非法输出：最后一步时，TP 不输出正确的检验结果. 该行为同样只具有纯粹破坏性，而不会造成信息泄露，因此不影响安全性.

因此，在上述攻击策略下恶意方的视图都可模拟，或攻击被非恶意方高概率发现，于是协议是恶意安全的.

证毕.

定理 4 的证明.　如正文讨论的结果，我们只需分析如下攻击策略.

(1) 测量攻击：不进行额外操作，只分析得到的经典和量子信息. 与协议 2 的分析类似，根据引理 1，由于协议 3 仍然是在傅里叶纠缠态下的计算，故所有粒子没有返回 TP 时，无论是恶意参与方 I_1 还是 TP 都无法获得任何有效信息，从而视图可模拟；而对于 TP，根据引理 4，当粒子收回后他获得的量子信息只包含他本应获得的经典信息，即最小公倍数结果，从而也可模拟. 唯一与协议 2 不同的是，当 TP 完成测量操作后，在参与方 I_1 手中仍然残留着一个粒子 e_{I_1}，而在第 7 步之后，总态为

$$|\Psi(x_I)\rangle=\frac{1}{\sqrt{y}}\sum_{l\in[y]}\left|\frac{l}{y}2^u\right\rangle_h|\hat{f}(l)\rangle_{e_I},$$

其中 $l\in[y]$ 随机选择且对于 I_1 不可见，因此可以视为没有测量，而 $|\hat{f}(l)\rangle=\frac{1}{\sqrt{y}}\sum_{k\in[y]}e^{-\frac{\sqrt{-1}2\pi}{y}lk}|f(k)\rangle$ 是 $|f(j)\rangle$ 的傅里叶逆变换. 于是

$$|\hat{f}(l)\rangle_{e_I}=\frac{1}{\sqrt{y}}\sum_{k\in[y]}e^{-\frac{\sqrt{-1}2\pi}{y}lk}|f_{I_1}(k)\rangle_{e_{I_1}}|f_{I_2}(k)\rangle_{e_{I_2}}.$$

则 I_1 的视图为 $VIEW_{I_1}(x_I)=(x_{I_1},y,\rho_{I_1})$，其中

$$\begin{aligned}\rho_{I_1}(x_I)&=\mathrm{Tr}_{e_{I_1}}(|\Psi(x_I)\rangle\langle\Psi(x_I)|)\\&=\frac{1}{y^2}\sum_{l,l'\in[y]}\sum_{k,k'\in[y]}e^{\frac{\sqrt{-1}2\pi}{y}(l'k'-lk)}|f_{I_1}(k)\rangle\langle f_{I_1}(k')|_{e_{I_1}}\\&\quad\left\langle\frac{l'}{y}2^u\middle|\frac{l}{y}2^u\right\rangle_h\langle f_{I_2}(k')|f_{I_2}(k)\rangle_{e_{I_2}}\\&=\frac{1}{y^2}\sum_{l,l'\in[y]}\sum_{k,k'\in[y]}e^{\frac{\sqrt{-1}2\pi}{y}(l'k'-lk)}\delta_{ll'}\delta_{kk'}|f_{I_1}(k)\rangle\langle f_{I_1}(k')|_{e_{I_1}}\\&=\frac{1}{y^2}\sum_{l\in[y]}\sum_{k\in[y]}|f_{I_1}(k)\rangle\langle f_{I_1}(k')|_{e_{I_1}}\\&=\frac{1}{y^2}\sum_{k\in[y]}|f_{I_1}(k)\rangle\langle f_{I_1}(k')|_{e_{I_1}},\end{aligned}$$

其中 $y,f_{I_1}(k)$ 都是已知量. 即无论其他人的输入 x_I 如何，对应的视图 $\rho_{I_1}(x_I)$ 都不可区分，因此存在一个模拟的量子算法 $SI_{I_1}(x_{I_1},y)=(x_{I_1},y,\hat{\rho}_{I_1})$ 来模拟出 I_1 的视图，具体构造方法参照定理 3 的证明. 于是，协议 3 在测量攻击下也是安全的.

(2) 非法制备：在第 3 步时，TP 在制备叠加态时没有制备正确的平衡叠加态，但是正常纠缠所有粒子. 与协议 2 类似，根据引理 4，TP 无论如何伪造，都最多只能获取他本应获得的最小公倍数结果，因此仍是可模拟的.

(3) 非法输入：得到粒子后参与方 I_1 不施加正确的操作 U_i. 与协议 2 类似，如果 I_1 仅仅不输入正确值，这是恶意模型所允许的；而若其还不执行正确的量子操作，则其唯一结果是输出错误，并且仍然无法获得信息.

(4) 纠缠-测量攻击：得到粒子 a 后，参与方 I_1 准备一个辅助粒子 b，然后纠缠 a,b，随后将粒子 a 发送给下一个参与方，并保留 b. 等到合适的时机，就分析 b 上的量子信息. 与协议 2 类似，为了通过星环拓扑的检验，需要令 $\eta=1$；而为了区分信息，$|\varepsilon(\varphi)\rangle$ 与 $|\varphi\rangle$ 应一一对应且保持正交. 同样，只有当所有粒子返回 TP 时，TP 的 $\mathrm{QFT}^\dagger$ 操作才会改变傅里叶纠缠态的实质，故我们只考虑这个时间点. 与定理 3 的证明(5)类似，当施加了纠缠门并返回粒子 a 后，总的量子态为 $\frac{1}{\sqrt{2^u}}\sum_{j\in[2^u]}|j\rangle_h|f_{I_2}(j)\rangle_{e_{I_2}}|f_{I_1}(j)\rangle_{e_{I_1}}|\varepsilon(j)\rangle_b$，其中设 $f_{I_2}(j)$ 的周期是最小公倍数 y_1. 此时，$f_{I_2}(j)\|f_{I_1}(j)\|\varepsilon(j)$ 本身构成了一个函数 $f_\varepsilon(j)$，而当 $\varepsilon(j)$ 具有周期时，$f_\varepsilon(j)$ 的周期将是原本的最小公倍数的倍数，而这没有带来比最小公倍数更多的信息；当 $\varepsilon(j)$ 不具有周期时，TP 将得到错误的结果，并且与定理 3 的证明(5)类似，TP 和 I_1 各自也没有得到额外信息. 同样，就本质而言，这是因为他们没有共谋，从而无法通过经典通信改变傅里叶纠缠态的实质.

(5) 非法输出：最后一步时，TP 不输出正确的最小公倍数结果. 该行为只具有纯粹破坏性，而不会造成信息泄露，因此不影响安全性.

因此，在上述攻击策略下恶意方的视图都可模拟，或攻击被非恶意方高概率发现，于是协议是恶意安全的.

证毕.

定理 5 的证明.　令 $\mathrm{lcm}_{k\in[n]}(\omega_k)=\omega_i r_i$. 假如 $\gcd_{i\in[n]}(r_i)\neq1$，则 $\frac{\mathrm{lcm}_{k\in[n]}(\omega_k)}{\gcd_{i\in[n]}(r_i)}<\mathrm{lcm}_{k\in[n]}(\omega_k)$ 也是 ω_i 的公倍数，从而发生矛盾，因此 $\gcd_{i\in[n]}(r_i)=1$. 已知 $\mathrm{lcm}_{k\in[n]}(\omega_k)=\omega_k r_i=r_i\frac{\mathrm{lcm}_{j\in[n]}(x_j)}{x_i}$，即

$$x_i\,\mathrm{lcm}_{k\in[n]}(\omega_k)=r_i\,\mathrm{lcm}_{j\in[n]}(x_j),$$

对等式左边取 GCD，有

$$\gcd_{i\in[n]}\left(x_i\,\mathrm{lcm}_{k\in[n]}(\omega_k)\right)=\mathrm{lcm}_{k\in[n]}(\omega_k)\gcd_{i\in[n]}(x_i);$$

对右边也取 GCD：注意到 $\left(\mathrm{lcm}_{j\in[n]}(x_j)\gcd_{i\in[n]}(r_i)\right)\mid\left(r_i\,\mathrm{lcm}_{j\in[n]}(x_j)\right)$ 显然成立，而假设存在正整数 $s>1$ 满足

$$\left(s\,\mathrm{lcm}_{j\in[n]}(x_j)\gcd_{i\in[n]}(r_i)\right)\mid\left(r_i\,\mathrm{lcm}_{j\in[n]}(x_j)\right),$$

那么 $\left(s\gcd_{i\in[n]}(r_i)\right)\mid r_i$，即 $s\gcd_{i\in[n]}(r_i)$ 是比 $\gcd_{i\in[n]}(r_i)$ 更大的 r_i 的公约数，从而矛盾，因此有

$$\gcd_{i\in[n]}\left(r_i\,\mathrm{lcm}_{j\in[n]}(x_j)\right)=\mathrm{lcm}_{j\in[n]}(x_j)\gcd_{i\in[n]}(r_i)=\mathrm{lcm}_{j\in[n]}(x_j).$$

则有

$$\mathrm{lcm}_{k\in[n]}(\omega_k)\gcd_{i\in[n]}(x_i)=\mathrm{lcm}_{j\in[n]}(x_j),$$

从而

$$\gcd_{i\in[n]}(x_i)=\frac{\mathrm{lcm}_{j\in[n]}(x_j)}{\mathrm{lcm}_{k\in[n]}(\omega_k)}.$$

证毕.

LI Zi-Xian, M. S. candidate. His main research interests include quantum cryptographic communication and quantum secure multiparty computation.

LIU Wen-Jie, Ph. D., associate professor. His main research interests include quantum cryptographic communication, quantum secure multiparty computation and quantum machine learning.

Background

In this paper, we mainly study the secure multiparty computation (SMC) of least common multiple (LCM), as an important number theoretic function. In 2018, Yang et al proposed a LCM protocol based on private maximum (minimum) computation, but the complexity depends on the choice of prime factors, which can reach exponential level in the worst case. As far as we know, there is no more efficient LCM protocol.

In this paper, we use quantum computing with higher potential to realize the SMC of LCM. Shor's quantum period-finding algorithm (QPA) can find the period of multi-bit function in polynomial time, but it has a certain failure probability. We propose an efficient LCM protocol based on QPA by using the following property of periodic functions: the connection of multiple periodic functions is also a periodic function, and its period is exactly the LCM of these small periods. We use a star-ring hybrid topology structure to defend against collusion attacks, and a quantum anonymous output validation (AOV) protocol to validate the LCM results. The proposed LCM protocol has polynomial computational and communication complexity, which is the lowest among the known protocols of the same kind, and has unconditional security under known malicious attacks. In addition, we also propose some extended applications based on the LCM protocol, including secure multi-party greatest common divisor computation, fraction summation, maximum (minimum) computation.

Our work is supported by the following projects:

(1) National Natural Science Foundation of China, "Verifiable Multi-Client Blind Quantum Computation and Its Application to Complex Secure Multi-party Computation Problems" (No. 62071240), which studies the verifiable multi-client blind quantum computation model and explore its application in several kinds of complex SMC problems. This paper belongs to the category of secure multiparty computation in this project.

(2) The Innovation Program for Quantum Science and Technology (No. 2021ZD0302901), which studies the theory of the design and analysis of quantum algorithms, develops polynomial-accelerated quantum algorithms, and develops post-quantum cryptographic protocols based on quantum algorithms and hardware technologies. This paper belongs to the category of secure multiparty computation in this project.

(3) Postgraduate Research & Practice Innovation Program of Jiangsu Province (No. KYCX23_1370), which studies the application of exponentially accelerating quantum algorithms in quantum SMC, and study the formal verification of quantum SMC protocols. This paper belongs to the category of secure multiparty computation in this project.

(4) The Natural Science Foundation of Jiangsu Province (No. BK20231142), which studies the quantum optimal detection of multi-dimensional signals, and based on this, studies the key technologies of quantum multi user detection suitable for optical frequency communication. This paper belongs to the category of quantum communication in this project.