基于 d 级量子系统相互无偏基的量子安全多方求和及其应用

叶天语^{*}, 胡家莉

浙江工商大学信息与电子工程学院, 杭州 310018

^{*}联系人, E-mail: happyty@aliyun.com

收稿日期: 2020-07-09; 接受日期: 2020-08-18; 网络出版日期: 2020-12-11

国家自然科学基金(编号: 62071430)和浙江省自然科学基金(编号: LY18F020007)资助项目

摘要 本文提出一种新颖的基于 d 级量子系统相互无偏基的量子安全多方求和协议。 n 个秘密持有者通过变换操作将自己的秘密编码在相互无偏基量子态上, 以环形模式将其进行传输。安全性分析表明, 所提出的协议能抵抗外在攻击和参与者攻击。本文协议适用于 d 级量子系统, 采用整数加整数技术计算模 d 和, 相比于采用比特加比特计算的量子安全求和协议, 会具有更高的计算效率; 相比于求和模较小的量子安全求和协议, 会具有更广泛的应用。而且, 这个协议能被用于量子多方隐私比较和量子多方匿名投票。

关键词 量子安全多方求和, 相互无偏基, 量子多方隐私比较, 量子多方匿名投票

PACS: 03.67.Dd, 03.67.Hk, 03.67.Pp

1 引言

量子安全求和问题可被描述如下: n 个秘密持有者 $P_1, P_2, \dots, P_n$ 通过量子信号的传输在不泄露她们秘密信息 $a_1, a_2, \dots, a_n$ 的前提下计算一个求和函数 $\text{sum}(a_1, a_2, \dots, a_n)$, 其中 a_i 是 P_i 的秘密信息, $\text{sum}(\cdot)$ 是求和函数, $i = 1, 2, \dots, n$ 。量子安全求和的目标是在确保秘密持有者的秘密信息不被泄露的前提下得到正确的求和结果。量子安全求和是量子安全计算的一个基本问题, 其重要性不言而喻, 近年来越来越受到研究者的关注。2002年, Heinrich^[1]将量子求和应用到积分。2003年, Heinrich等人^[2]探讨最差平均情形下可重复的

量子布尔函数。2006年, Hillery等人^[3]设计一个基于两粒子 N 级纠缠态的量子多方求和协议, 在匿名投票过程中完成 N 个参与者输入信息的求和。2007年, Du等人^[4]设计一个基于非正交态的量子安全模 $n+1$ ($n \geq 2$)求和协议, 其中 n 是秘密持有者人数。2010年, Chen等人^[5]设计一种基于单光子和多粒子GHZ纠缠态的量子模2求和协议。2014年, Zhang等人^[6]提出一个基于具有极化和空模双自由度的单光子的量子模2求和协议。后来, Gu等人^[7]认为文献[6]的协议不能抵抗恶意参与者的截获-重发攻击并提出一个改进方案。2015年, Zhang等人^[8]设计一个基于六量子比特最大纠缠态纠缠相关性的三方量子模2求和协议。2016年, Shi等人^[9]利用离

引用格式: 叶天语, 胡家莉. 基于 d 级量子系统相互无偏基的量子安全多方求和及其应用. 中国科学: 物理学 力学 天文学, 2021, 51: 020301
Ye T-Y, Hu J-L. Quantum secure multiparty summation based on the mutually unbiased bases of d -level quantum systems and its application (in Chinese). Sci Sin-Phys Mech Astron, 2021, 51: 020301, doi: 10.1360/SSPMA-2020-0262

散量子傅里叶变换、控制非操作和离散量子傅里叶逆变换构建一个以整数加整数的方式计算求和的量子模 N 求和协议, 其中 $N=2^m$, m 是一个基态所代表的量子比特数. 2017年, Shi和Zhang^[10]提出一类特殊两方隐私求和问题的一种通用量子解决方法, 利用量子计数算法实现求和. 这个量子求和协议的特点是适用于 N 级量子系统, 采用比特加比特的计算方式以实现普通加法求和, 这里 N 是每个秘密持有者秘密的长度. 同年, Zhang等人^[11]利用单光子设计一个量子多方模2求和协议. 这个协议先利用单光子产生私钥对参与者的输入信息进行加密, 然后再对加密后的信息进行求和. 2018年, 我们提出一种基于量子傅里叶变换的量子安全多方求和协议^[12]. 2019年, Ji等人^[13]提出一种基于 d 级Cat态和 d 级Bell态纠缠交换的量子安全多方求和协议. 2020年, Duan^[14]提出一种基于量子底特移位操作的量子安全多方求和协议. 文献^[12–14]协议的特点是都适用于 d 级量子系统, 采用整数加整数的方式计算模 d 和.

不难发现, 文献^[5–8,11]协议的求和模过小, 导致更广泛的应用受到限制; 文献^[4–8,10,11]协议采用比特加比特的计算方式, 导致计算效率不高. 为了克服这些缺点, 本文利用 d 级量子系统 d 组相互无偏基提出一种新颖的量子安全多方求和协议, 其特点是适用于 d 级量子系统, 采用整数加整数的方式计算模 d 和. 安全性分析表明, 本文协议能抵抗外在攻击和参与者攻击. 另外, 本文还探讨所提出的协议在量子多方隐私比较和量子多方匿名投票的应用.

2 本文协议

2.1 协议描述

d 级量子系统 d 组相互无偏基为^[15]

$$|e_l^{(j)}\rangle = \frac{1}{\sqrt{d}} \sum_{r=0}^{d-1} \zeta^{r(l+jr)} |r\rangle, \quad (1)$$

其中 j 代表基的序号, l 代表在给定基下的量子态的序号, $j, l \in \{0, 1, \dots, d-1\}$, $\zeta = e^{2\pi i/d}$. 定义两个变换操作分别为^[15]

$$X_d = \sum_{u=0}^{d-1} \zeta^u |u\rangle \langle u| \quad (2)$$

和

$$Y_d = \sum_{u=0}^{d-1} \zeta^{u^2} |u\rangle \langle u|, \quad (3)$$

那么存在^[15]

$$\begin{aligned} X_d |e_l^{(j)}\rangle &= \frac{1}{\sqrt{d}} \left(\sum_{u=0}^{d-1} \zeta^u |u\rangle \langle u| \right) \left(\sum_{r=0}^{d-1} \zeta^{r(l+jr)} |r\rangle \right) \\ &= \frac{1}{\sqrt{d}} \sum_{r=0}^{d-1} \zeta^{r[(l+1)+jr]} |r\rangle \\ &= |e_{l \oplus 1}^{(j)}\rangle, \end{aligned} \quad (4)$$

$$\begin{aligned} Y_d |e_l^{(j)}\rangle &= \frac{1}{\sqrt{d}} \left(\sum_{u=0}^{d-1} \zeta^{u^2} |u\rangle \langle u| \right) \left(\sum_{r=0}^{d-1} \zeta^{r(l+jr)} |r\rangle \right) \\ &= \frac{1}{\sqrt{d}} \sum_{r=0}^{d-1} \zeta^{r[l+(j+1)r]} |r\rangle \\ &= |e_l^{(j \oplus 1)}\rangle, \end{aligned} \quad (5)$$

其中, $\oplus$ 是模 d 和. 进一步可得到^[15]

$$X_d^l Y_d^{j'} |e_l^{(j)}\rangle = |e_{l \oplus l'}^{(j \oplus j')} \rangle, \quad (6)$$

其中 $j', l' \in \{0, 1, \dots, d-1\}$. 式(6)表明, $|e_l^{(j)}\rangle$ 可通过 $X_d^l Y_d^{j'}$ 被映射到 $|e_{l \oplus l'}^{(j \oplus j')} \rangle$. 这就是式(1)所示的相互无偏基的循环性质.

存在 n 个秘密持有者 $P_1, P_2, \dots, P_n$, 其中第 i 个秘密持有者 P_i 拥有一个长度为 N 的秘密整数序列 $A_i = (a_i^1, a_i^2, \dots, a_i^N)$, $a_i^t \in \{0, 1, \dots, d-1\}$, $i = 1, 2, \dots, n$, $t = 1, 2, \dots, N$. $P_1, P_2, \dots, P_n$ 希望借助半忠诚第三方 P_0 在不泄露她们秘密整数序列 $A_1, A_2, \dots, A_n$ 的前提下得到 $A_1 \oplus A_2 \oplus \dots \oplus A_n$ 的正确求和结果. 这里, “半忠诚”意味着 P_0 在执行协议的同时会尽其所能去得到 A_i , 但不被允许与其他人合谋^[16].

步骤1: $P_1, P_2, \dots, P_n$ 事先通过安全的量子多方秘密共享协议^[17]共享密钥序列 $K_1, K_2, \dots, K_n$, 其中 $K_i = (k_i^1, k_i^2, \dots, k_i^N)$, $k_i^t \in \{0, 1, \dots, d-1\}$, $k_1^t \oplus k_2^t \oplus \dots \oplus k_n^t = 0$, $i = 1, 2, \dots, n$, $t = 1, 2, \dots, N$.

步骤2: P_0 制备一个由 N 个量子态 $|e_0^{(0)}\rangle$ 构成的量子态序列, 记为 $S = (|e_0^{(0)}\rangle, |e_0^{(0)}\rangle, \dots, |e_0^{(0)}\rangle)$. 为了检测窃听, P_0 制备 N 个诱骗光子^[18,19], 其中每个诱骗光子从集

合 $V_1 = \{|r\rangle\}$ 和 $V_2 = \{F|r\rangle\}$ 进行随机选择, $r \in \{0, 1, \dots, d-1\}$, F 为 d 阶离散量子傅里叶变换, 定义为 $F|r\rangle = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} \zeta^{lr} |l\rangle$. 然后, P_0 将所有诱骗光子随机插入 S 得到新序列 S_0 . 最后, P_0 将 S_0 以块传输的方式^[20] 发送给 P_1 . 值得提出的是, 块传输的方式在各种形式下的量子直接通信中得到广泛应用^[21-23].

步骤3: 对于 $i = 1, 2, 3, \dots, n$, 当 P_i 收到 S_{i-1} 后, P_i 与 P_{i-1} 一起检测 S_{i-1} 在传输过程是否被窃听. P_{i-1} 告诉 $P_i S_{i-1}$ 中诱骗光子的位置和制备基. 接着, P_i 利用 P_{i-1} 的制备基去测量 S_{i-1} 中的诱骗光子并将测量结果告诉 P_{i-1} . 然后, P_{i-1} 通过将 S_{i-1} 中亲自制备的诱骗光子的初态与 P_i 的测量结果相比较来判断 S_{i-1} 在传输过程是否被窃听. 如果量子信道是不安全的, 那么协议将被终止; 否则, 协议将被继续下去.

P_i 丢弃 S_{i-1} 中的诱骗光子重新得到 S . 然后, P_i 对 S 中的粒子编码其秘密整数序列 A_i . 具体地, P_i 对第 t 个量子态施加 $X_d^{a_i^t \oplus k_i^t} Y_d^{y_i^t}$, 其中 y_i^t 为 P_i 随机选择的整数, 且 $y_i^t \in \{0, 1, \dots, d-1\}$, $t = 1, 2, \dots, N$. 当 P_i 操作完后, S 的粒子变为

$$\left| e^{\left(\begin{matrix} y_1^1 \oplus y_2^1 \oplus \dots \oplus y_n^1 \\ a_1^1 \oplus a_2^1 \oplus \dots \oplus a_n^1 \oplus k_1^1 \oplus k_2^1 \oplus \dots \oplus k_n^1 \end{matrix} \right)} \right\rangle, \left| e^{\left(\begin{matrix} y_1^2 \oplus y_2^2 \oplus \dots \oplus y_n^2 \\ a_1^2 \oplus a_2^2 \oplus \dots \oplus a_n^2 \oplus k_1^2 \oplus k_2^2 \oplus \dots \oplus k_n^2 \end{matrix} \right)} \right\rangle, \dots, \left| e^{\left(\begin{matrix} y_1^N \oplus y_2^N \oplus \dots \oplus y_n^N \\ a_1^N \oplus a_2^N \oplus \dots \oplus a_n^N \oplus k_1^N \oplus k_2^N \oplus \dots \oplus k_n^N \end{matrix} \right)} \right\rangle.$$

为了检测窃听, P_i 制备 N 个诱骗光子, 其中每个诱骗光子从集合 V_1 和 V_2 进行随机选择. 然后, P_i 将所有诱骗光子随机插入 S 得到新序列 S_i . 最后, P_i 将 S_i 以块传输的方式发送给 P_{i+1} .

特别指出的是, P_n 最终将 S_n 以块传输的方式发送给 P_0 .

步骤4: 当 P_0 收到 S_n 后, P_0 与 P_n 一起检测 S_n 在传输过程是否被窃听. P_n 告诉 $P_0 S_n$ 中诱骗光子的位置和制备基. 接着, P_0 利用 P_n 的制备基去测量 S_n 中的诱骗光子并将测量结果告诉 P_n . 然后, P_n 通过将 S_n 中亲自制备的诱骗光子的初态与 P_0 的测量结果相比较来判断 S_n 在传输

过程是否被窃听. 如果量子信道是不安全的, 那么协议将被终止; 否则, 协议被继续下去.

步骤5: P_0 丢弃 S_n 中的诱骗光子重新得到 S . 此时, S 的粒子为

$$\left| e^{\left(\begin{matrix} y_1^1 \oplus y_2^1 \oplus \dots \oplus y_n^1 \\ a_1^1 \oplus a_2^1 \oplus \dots \oplus a_n^1 \oplus k_1^1 \oplus k_2^1 \oplus \dots \oplus k_n^1 \end{matrix} \right)} \right\rangle, \left| e^{\left(\begin{matrix} y_1^2 \oplus y_2^2 \oplus \dots \oplus y_n^2 \\ a_1^2 \oplus a_2^2 \oplus \dots \oplus a_n^2 \oplus k_1^2 \oplus k_2^2 \oplus \dots \oplus k_n^2 \end{matrix} \right)} \right\rangle, \dots, \left| e^{\left(\begin{matrix} y_1^N \oplus y_2^N \oplus \dots \oplus y_n^N \\ a_1^N \oplus a_2^N \oplus \dots \oplus a_n^N \oplus k_1^N \oplus k_2^N \oplus \dots \oplus k_n^N \end{matrix} \right)} \right\rangle.$$

P_i 通过经典安全信道(比如基于 QKD 的保密通信)将 y_i^t 告诉 P_0 . 然后 P_0 计算 $J_t = y_1^t \oplus y_2^t \oplus \dots \oplus y_n^t$, 其中 $i=1, 2, \dots, n$, $t=1, 2, \dots, N$. P_0 选择第 J_t 组相互无偏基测量 S 的第 t 个粒子 $\left| e^{\left(\begin{matrix} y_1^t \oplus y_2^t \oplus \dots \oplus y_n^t \\ a_1^t \oplus a_2^t \oplus \dots \oplus a_n^t \oplus k_1^t \oplus k_2^t \oplus \dots \oplus k_n^t \end{matrix} \right)} \right\rangle$, 得到测量结果 $a_1^t \oplus a_2^t \oplus \dots \oplus a_n^t \oplus k_1^t \oplus k_2^t \oplus \dots \oplus k_n^t$, 也就是得到 $\text{sum}_t = a_1^t \oplus a_2^t \oplus \dots \oplus a_n^t$. P_0 向 $P_1, P_2, \dots, P_n$ 公布求和结果 sum_t .

2.2 安全性分析

(1) 外在攻击

本文协议是以环形方式传输量子态序列, 即 P_0 将 S_0 发送给 P_1 , P_1 将 S_1 发送给 P_2 , 如此继续下去, 直到 P_n 将 S_n 发送回 P_0 . 每次量子态序列的传送都采用随机选自两组非正交基 V_1 和 V_2 的诱骗光子来确保其安全性. 诱骗光子技术^[18,19] 可被视为 BB84 QKD 协议^[24] 的窃听检测方法的一个变种, 后者的无条件安全性在文献^[25] 已被证实. 因此, 外在攻击对于本文协议是无效的.

另外, 尽管外在窃听者可能听到 P_0 在步骤 5 向 $P_1, P_2, \dots, P_n$ 公布的求和结果 $a_1^t \oplus a_2^t \oplus \dots \oplus a_n^t$, 但仍然无法从 $a_1^t \oplus a_2^t \oplus \dots \oplus a_n^t$ 解密出 a_i^t , 这里, $i=1, 2, \dots, n$, $t=1, 2, \dots, N$.

(2) 参与者攻击

不忠诚参与者的攻击往往能量更大, 在协议设计时应当引起特别重视^[26]. 这里考虑以下三种情形的参与者攻击.

1) 来自单个不忠诚秘密持有者的攻击

在本文协议中, 每个秘密持有者都执行三个动作, 即与前一个参与者进行窃听检测、编码自己的秘密整

数序列以及与后一个参与者进行窃听检测. 因此, 每个秘密持有者的角色是类似的. 假设 $P_j (j \in \{1, 2, \dots, n\})$ 是不忠诚的秘密持有者, 她可能尝试以下两种攻击.

① $P_j (j \in \{1, 2, \dots, n\})$ 对量子态序列 $S_v (v \in \{0, 1, \dots, n\})$ 且 $v \neq j-1, j$ 的粒子发起主动攻击. 由于不知道 S_v 中诱骗光子的位置, 她将不可避免地在诱骗光子上留下痕迹, 从而被当成外在窃听者检测到. ② $P_j (j \in \{2, 3, \dots, n\})$ 制备假的量子态序列 $S_f = (|e_0^{(0)}\rangle, |e_0^{(0)}\rangle, \dots, |e_0^{(0)}\rangle)$ 发送给 P_{j-1} , 然后 P_{j-1} 对 S_f 的第 $t (t = 1, 2, \dots, N)$ 个粒子施加 $X_d^{a_{j-1}^t \oplus k_{j-1}^t} Y_d^{y_{j-1}^t}$ 来编码她的秘密整数 a_{j-1}^t 并将编码后的量子态序列发送给 P_j . 在与 P_{j-1} 进行窃听检测后, P_j 丢弃诱骗光子得到编码了 A_{j-1} 的假的量子态序列

$$S_f' = \left[\left| e_{a_{j-1}^1 \oplus k_{j-1}^1}^{(y_{j-1}^1)} \right\rangle, \left| e_{a_{j-1}^2 \oplus k_{j-1}^2}^{(y_{j-1}^2)} \right\rangle, \dots, \left| e_{a_{j-1}^N \oplus k_{j-1}^N}^{(y_{j-1}^N)} \right\rangle \right].$$

由于不知道 y_{j-1}^t 的值, P_j 将无法选择正确的测量基去测量 S_f' 中的第 t 个粒子, 从而无法解密出 a_{j-1}^t . 另一方面, 在步骤 5 中 P_j 从 P_0 收到求和结果 $a_1^t \oplus a_2^t \oplus \dots \oplus a_n^t$, 但仍然无法从 $a_1^t \oplus a_2^t \oplus \dots \oplus a_n^t$ 解密出 a_l^t , 这里, $l=1, 2, \dots, n$ 且 $l \neq j$.

2) 来自两个或多个不忠诚秘密持有者的共谋攻击

本文协议无法抵抗来自 $n-1$ 个秘密持有者的共谋攻击, 因为她们共谋在一起就能轻易从求和结果中解密出剩余一个秘密持有者的秘密整数序列.

为分析本文协议能否抵抗来自 $n-2$ 个秘密持有者的共谋攻击, 不失一般性, 假设不忠诚的 $P_1, \dots, P_{j-1}, P_{j+1}, \dots, P_{n-1} (j \in \{2, 3, \dots, n-2\})$ 试图共谋得到 P_j 和 P_n 的秘密整数序列. ① $P_1, \dots, P_{j-1}, P_{j+1}, \dots, P_{n-1}$ 制备假的量子态序列 $S_f = (|e_0^{(0)}\rangle, |e_0^{(0)}\rangle, \dots, |e_0^{(0)}\rangle)$ 发送给 P_j , 然后 P_j 对 S_f 的第 $t (t = 1, 2, \dots, N)$ 个粒子施加 $X_d^{a_j^t \oplus k_j^t} Y_d^{y_j^t}$ 来编码她的秘密整数 a_j^t 并将编码后的量子态序列发送给 P_{j+1} . 在与 P_j 进行窃听检测后, $P_1, \dots, P_{j-1}, P_{j+1}, \dots, P_{n-1}$ 丢弃诱骗光子得到编码了 A_j 的假的量子态序列

$$S_f'' = \left[\left| e_{a_j^1 \oplus k_j^1}^{(y_j^1)} \right\rangle, \left| e_{a_j^2 \oplus k_j^2}^{(y_j^2)} \right\rangle, \dots, \left| e_{a_j^N \oplus k_j^N}^{(y_j^N)} \right\rangle \right].$$

由于不知道 y_j^t 的值, $P_1, \dots, P_{j-1}, P_{j+1}, \dots, P_{n-1}$ 将无法选择正确的测量基去测量 S_f'' 中的第 t 个粒子, 从而无法解密出 a_j^t . 这里, y_j^t 实质上起到对 a_j^t 进行加密的作用. ② $P_1, \dots, P_{j-1}, P_{j+1}, \dots, P_{n-1}$ 制备假的量子态序列

$$S_f = (|e_0^{(0)}\rangle, |e_0^{(0)}\rangle, \dots, |e_0^{(0)}\rangle)$$

发送给 P_n , 然后 P_n 对 S_f 的第 t 个粒子施加 $X_d^{a_n^t \oplus k_n^t} Y_d^{y_n^t}$ 来编码她的秘密整数 a_n^t 并将编码后的量子态序列

$$S_f''' = \left[\left| e_{a_n^1 \oplus k_n^1}^{(y_n^1)} \right\rangle, \left| e_{a_n^2 \oplus k_n^2}^{(y_n^2)} \right\rangle, \dots, \left| e_{a_n^N \oplus k_n^N}^{(y_n^N)} \right\rangle \right] \text{ 发送给 } P_0.$$

$P_1, \dots, P_{j-1}, P_{j+1}, \dots, P_{n-1}$ 截获编码后的量子态序列 S_f''' 并测量后重发给 P_0 . 由于不知道 y_n^t 的值, $P_1, \dots, P_{j-1}, P_{j+1}, \dots, P_{n-1}$ 将无法选择正确的测量基去测量 S_f''' 中的第 t 个粒子, 从而无法解密出 a_n^t . 这里, y_n^t 实质上起到对 a_n^t 进行加密的作用. 与此同时, 由于不知道诱骗光子的真实位置, $P_1, \dots, P_{j-1}, P_{j+1}, \dots, P_{n-1}$ 的攻击行为将不可避免地被 P_0 检测到. ③ $P_1, \dots, P_{j-1}, P_{j+1}, \dots, P_{n-1}$ 制备 N 个 d 级 Bell 态, 并将所有 Bell 态的第一个粒子发送给 P_j , 然后 P_j 对收到的第 $t (t = 1, 2, \dots, N)$ 个粒子施加 $X_d^{a_j^t \oplus k_j^t} Y_d^{y_j^t}$ 来编码她的秘密整数 a_j^t 并将编码后的粒子序列发送给 P_{j+1} . 在与 P_j 进行窃听检测后, $P_1, \dots, P_{j-1}, P_{j+1}, \dots, P_{n-1}$ 丢弃诱骗光子得到编码了 A_j 的 N 个两粒子量子纠缠态. 根据

$$X_d^{a_j^t \oplus k_j^t} Y_d^{y_j^t} |\Psi(u, v)\rangle = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} \zeta^{l(u+a_j^t+k_j^t)+y_j^t l^2} |l\rangle |l+v\rangle, \quad (7)$$

其中 $|\Psi(u, v)\rangle = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} \zeta^{lu} |l\rangle |l+v\rangle$ 为 d 级 Bell 态, $u, v \in \{0, 1, \dots, d-1\}$. 由于不知道 y_j^t 的值, $P_1, \dots, P_{j-1}, P_{j+1}, \dots, P_{n-1}$ 无法从第 t 个两粒子量子纠缠态解密出 a_j^t . 这里, y_j^t 实质上起到对 a_j^t 进行加密的作用. ④ 在步骤 5 中 $P_1, \dots, P_{j-1}, P_{j+1}, \dots, P_{n-1}$ 可以从 P_0 知道求和结果 $a_1^t \oplus a_2^t \oplus \dots \oplus a_n^t$. 然而, $P_1, \dots, P_{j-1}, P_{j+1}, \dots, P_{n-1}$ 仍然只能从 $a_1^t \oplus a_2^t \oplus \dots \oplus a_n^t$ 得到 $a_j^t \oplus a_n^t$, 而无法解密出 a_j^t 和 a_n^t .

3) 来自第三方 P_0 的攻击

半忠诚第三方 P_0 试图发起以下三种攻击来得到秘密持有者的秘密整数序列. ① P_0 截获 S_1 并测量后重发给 P_2 . 然而, 由于不知道 S_1 中诱骗光子的真实位置, P_0 的攻击行为将不可避免地被 P_2 检测到. ② P_0 截获 S_{j-1} ($j \in \{2, 3, \dots, n-1\}$) 并将制备的假的量子态序列 $S_f = (|e_0^{(0)}\rangle, |e_0^{(0)}\rangle, \dots, |e_0^{(0)}\rangle)$ 发送给 P_j , 然后 P_j 对 S_f 的第 t ($t = 1, 2, \dots, N$) 个粒子施加 $X_d^{a'_t \oplus k'_t} Y_d^{y'_t}$ 来编码她的秘密整数 a'_t 并将编码后的量子态序列 S_f'' 发送给 P_{j+1} . P_0 截获 S_f'' 并测量后重发给 P_{j+1} . 然而, 由于不知道诱骗光子的真实位置, P_0 的攻击行为将不可避免地被 P_{j+1} 检测到. ③ P_0 截获 S_{n-1} 并将制备的假的量子态序列 $S_f = (|e_0^{(0)}\rangle, |e_0^{(0)}\rangle, \dots, |e_0^{(0)}\rangle)$ 发送给 P_n , 然后 P_n 对 S_f 的第 t 个粒子施加 $X_d^{a'_t \oplus k'_t} Y_d^{y'_t}$ 来编码她的秘密整数 a'_t 并将编码后的量子态序列 S_f'' 发送给 P_0 . 在与 P_n 进行窃听检测后, P_0 丢弃诱骗光子得到编码了 A_n 的假的量子态序列 S_f'' . 即使在步骤5可以知道 y_n^t 的值而选择正确的测量基去测量 S_f'' 中的第 t 个粒子得到 $a_n^t \oplus k_n^t$, 但由于不知道 k_n^t , P_0 仍然无法解密出 a_n^t .

2.3 与现有量子安全求和协议的对比

本文协议与现有量子安全求和协议在适用量子系统、加法类型和计算方式三个方面的对比结果列于表1中. 显然, 本文协议的求和模大于文献[5–8, 11]的协议, 会有更广泛的应用; 本文协议采用整数加整数的计算方式, 比文献[4–8, 10, 11]的协议会有更高的计算效率.

本文协议与文献[5, 9, 11–14]的协议在忽略安全检测过程后的对比结果列于表2中. 根据表2, 在量子资源上, 本文协议只采用 d 级量子系统 d 组相互无偏基量子态, 文献[5, 12, 13]的协议需采用量子纠缠态, 所以本文协议在量子资源上优于文献[5, 12, 13]的协议; 在量子操作上, 不同于文献[9, 12, 13]的协议, 本文协议不需要采用离散量子傅里叶变换或量子态纠缠交换; 在量子测量上, 本文协议只需要 d 级量子系统相互无偏基测量, 不需要量子纠缠态测量, 而文献[5, 13]的协议需要

量子纠缠态测量, 所以本文协议在量子测量上优于文献[5, 13]的协议.

另外, 文献[14]的协议只能实现对随机整数序列进行模 d 和, 无法实现对特定整数序列进行模 d 和, 所以其实际应用范围会有一定的局限性. 而本文协议对特定整数序列能实现模 d 和. 因此, 在实际应用范围上, 本文协议优于文献[14]的协议. 在安全性上, 文献[14]的协议不是一个真正安全的量子多方求和协议, 因为它无法抵抗量子态制备者 P_1 发起的一种特定攻击. 这种攻击描述如下: 量子态制备者 P_1 制备量子态序列 $S = (|r_1\rangle, |r_2\rangle, \dots, |r_{N+\delta}\rangle)$ 和足够多的诱骗光子并将它们一起发送给 P_i ($i = 2, 3, \dots, n$); P_i 对收到的每个粒子施加随机次数的 U_X , 对它们进行置乱后发送给下一个参与者; P_1 截获这些粒子; P_i 公布对这些粒子的置乱顺序; P_1 将这些粒子恢复成原始顺序, 然后对编码后的 S 序列的粒子进行 V_1 基测量, 从而解密出 P_i 的编码操作而不被发现. 因此, 在安全性上, 本文协议优于文献[14]的协议.

3 本文协议的应用

这里讨论本文协议在量子安全多方计算上的应用.

(1) 应用到量子多方隐私比较

量子多方隐私比较^[27]判断来自 n 个秘密持有者的秘密整数 $A_1, A_2, \dots, A_n$ 是否全都相等. 将所有秘密持有者的秘密整数分解成对应的二进制序列, 然后分别对所有整数的每个相同位置的二进制比特进行相等性比较. 即首先计算出 $\text{sum}_t = a_1^t \oplus a_2^t \oplus \dots \oplus a_n^t$, 然后根据 sum_t 的值来判断 n 个二进制比特数 $a_1^t, a_2^t, \dots, a_n^t$ 是否全都相等. 这里, $\oplus$ 表示模 n 和, $a_i^t \in \{0, 1\}$ 为 A_i 的第 t 个二进制比特, $t = 1, 2, \dots, N$, N 为 A_i 的二进制长度. 若 $\text{sum}_t = 0$, 则 $a_1^t = a_2^t = \dots = a_n^t = 0$ 或 $a_1^t = a_2^t = \dots = a_n^t = 1$, 即 $a_1^t, a_2^t, \dots, a_n^t$ 全都相等; 否则, $a_1^t, a_2^t, \dots, a_n^t$ 不全都相等. 如果 $\text{sum}_t = 0$ 对于所有 $t = 1, 2, \dots, N$ 都成立, 那么认为 n 个整数 $A_1, A_2, \dots, A_n$ 全都相等.

只要做到以下两点, 就可以将本文协议应用到量子多方隐私比较:

表 1 现有量子安全求和协议在适用量子系统、加法类型和计算方式的对比结果^[12]
Table 1 Comparison results of present quantum secure summation protocols on the aspects of applicative quantum system, summation type and calculation way [12]

比较项目	文献[4]	文献[5]	文献[6,7]	文献[8]	文献[9]	文献[10]	文献[11]	文献[12]	文献[13]	文献[14]	本文
量子系统	$n+1$ 级量子系统	2级量子系统	2级量子系统	2级量子系统	N 级量子系统	N 级量子系统	2级量子系统	d 级量子系统	d 级量子系统	d 级量子系统	d 级量子系统
加法类型	模 $n+1$ 和	模2和	模2和	模2和	模 N 和	和	模2和	模 d 和	模 d 和	模 d 和	模 d 和
计算方式	比特加比特	比特加比特	比特加比特	比特加比特	整数加整数	比特加比特	比特加比特	整数加整数	整数加整数	整数加整数	整数加整数

表 2 现有量子安全多方求和协议的详细对比结果

Table 2 Detailed comparison results of present quantum secure multiparty summation protocols

比较项目	量子资源	量子操作	量子测量	编码秘密的位置	粒子传输模式	求和类型	计算方式
文献[5]	n 粒子GHZ态和单光子	Pauli算子 I 和 Z	Bell态测量和单光子测量	单光子	树型	模2和	比特加比特
文献[9]	d 级基态	离散量子傅里叶变换, 控制非操作, oracle操作 C_p , 离散量子傅里叶逆变换	V_1 基测量	全局相位	环形	模 N 和	整数加整数
文献[11]	单光子	控制非操作, Hadamard操作	单光子测量	经典一次一密	树型	模2和	比特加比特
文献[12]	d 级 n 粒子纠缠态	离散量子傅里叶变换, 变换操作 U_k	V_1 基测量	d 级 n 粒子纠缠态	树型	模 d 和	整数加整数
文献[13]	d 级 $n+1$ 粒子Cat态和 d 级两粒子Bell态	量子态纠缠交换, 变换操作 $U(u,v)$	d 级 $n+1$ 粒子Cat态测量和 d 级两粒子Bell态测量	d 级两粒子Bell态	树型	模 d 和	整数加整数
文献[14]	d 级基态	变换操作 U_X	V_1 基测量	d 级基态	环形	模 d 和	整数加整数
本文	d 组相互无偏基量子态	变换操作 X_d 和 Y_d	相互无偏基测量	d 组相互无偏基量子态	环形	模 d 和	整数加整数

1) 本文协议将 $(a_i^1, a_i^2, \dots, a_i^N)$ 看成是 A_i 的二进制比特序列, 其中 $a_i^t \in \{0, 1\}$, $i=1, 2, \dots, n$, $t=1, 2, \dots, N$, 并令 $d=n$;

2) 在本文协议的步骤5, P_0 得到 $\text{sum}_t = a_1^t \oplus a_2^t \oplus \dots \oplus a_n^t$ 后, 如果 $\text{sum}_t = 0$ 对于所有 $t=1, 2, \dots, N$ 都成立, 那么 P_0 向 $P_1, P_2, \dots, P_n$ 公布 $A_1, A_2, \dots, A_n$ 全都相等; 否则, P_0 向 $P_1, P_2, \dots, P_n$ 公布 $A_1, A_2, \dots, A_n$ 不全相等。

(2) 应用到量子多方匿名投票

量子多方匿名投票问题^[3]描述如下: 假设要求 n 个投票者 $P_1, P_2, \dots, P_n$ 对 N 个被投票对象 $C_1, C_2, \dots, C_N$ 进行匿名投票, 每个投票者只能对一个被投票对象投“赞成”票, 对其他被投票对象只能投“反对”票, 而且每个投票者的投票行为要被严格保密, 不能被其他任何人知道。用1和0分别代表“赞成”票和“反对”票。用 a_i^t 表示 P_i 对 C_t

的投票, 其中 $a_i^t \in \{0, 1\}$, $i=1, 2, \dots, n$, $t=1, 2, \dots, N$, 而且 $a_i^1 + a_i^2 + \dots + a_i^N = 1$ 。计票人对第 t 个被投票对象得到的票数进行统计, 统计结果为 $\sum_{i=1}^n a_i^t$ 。

只要做到以下三点, 就可以将本文协议应用到量子多方匿名投票:

1) 在本文协议, 令 $n < d$;

2) 在本文协议的步骤2, 将 P_0 制备的 N 个量子态

$|e_0^{(0)}\rangle_1, |e_0^{(0)}\rangle_2, \dots, |e_0^{(0)}\rangle_N$ 视为 N 个被投票对象;

3) 在本文协议的步骤3, P_i 通过对 N 个量子态 $|e_0^{(0)}\rangle_1, |e_0^{(0)}\rangle_2, \dots, |e_0^{(0)}\rangle_N$ 进行编码来实现对 N 个被投票对象进行投票, 即 P_i 对第 t 个被投票对象投“赞成”票时令 $a_i^t = 1$, 投“反对”票时令 $a_i^t = 0$, 而且满足 $a_i^1 +$

$a_i^2 + \dots + a_i^N = 1$, 其中 $i=1, 2, \dots, n$, $t=1, 2, \dots, N$.

4 结论

本文利用 d 级量子系统相互无偏基提出一种新颖的采用整数加整数方式计算模 d 的环形量子安全多方求和协议, 并且详细验证了其对外在攻击和参与者攻击的有效性. 相比于采用比特加比特计算方式的量子安全求和协议, 本文协议会有更高的计算效率; 相

比于求和模较小的量子安全求和协议, 会有更广泛的应用. 本文还探讨了所提出的协议在量子多方隐私比较和量子多方匿名投票的应用. 由于量子安全计算内涵丰富, 本文协议在量子多方密钥协商、量子多方匿名排序、量子多方距离计算等量子安全计算上的应用值得进一步研究. 本文只设计了一个 d 级量子系统量子安全多方求和的理论方案, 其物理实现有待进一步研究. 另外, 本文关注的高维量子协议是一个研究热点^[28], 有待进一步被深入研究.

参考文献

- 1 Heinrich S. Quantum summation with an application to integration. *J Complexity*, 2002, 18: 1–50
- 2 Heinrich S, Kwas M, Wozniakowski H. Quantum boolean summation with repetitions in the worst-average setting. arXiv: [quant-ph/0311036](#)
- 3 Hillery M, Ziman M, Bužek V, et al. Towards quantum-based privacy and voting. *Phys Lett A*, 2006, 349: 75–81, arXiv: [quant-ph/0505041](#)
- 4 Du J Z, Chen X B, Wen Q Y, et al. Secure multiparty quantum summation. *Acta Phys Sin*, 2007, 56: 6214–6219
- 5 Chen X B, Xu G, Yang Y X, et al. An efficient protocol for the secure multi-party quantum summation. *Int J Theor Phys*, 2010, 49: 2793–2804
- 6 Zhang C, Sun Z W, Huang Y, et al. High-capacity quantum summation with single photons in both polarization and spatial-mode degrees of freedom. *Int J Theor Phys*, 2014, 53: 933–941
- 7 Gu J, Hwang T, Tsai C W. Improving the security of high-capacity quantum summation with single photons in both polarization and spatial-mode degrees of freedom. *Int J Theor Phys*, 2019, 58: 2213–2217
- 8 Zhang C, Sun Z W, Huang X, et al. Three-party quantum summation without a trusted third party. *Int J Quantum Inform*, 2015, 13: 1550011
- 9 Shi R H, Mu Y, Zhong H, et al. Secure multiparty quantum computation for summation and multiplication. *Sci Rep*, 2016, 6: 19655
- 10 Shi R H, Zhang S. Quantum solution to a class of two-party private summation problems. *Quantum Inf Process*, 2017, 16: 225
- 11 Zhang C, Situ H, Huang Q, et al. Multi-party quantum summation without a trusted third party based on single particles. *Int J Quantum Inform*, 2017, 15: 1750010
- 12 Yang H Y, Ye T Y. Secure multi-party quantum summation based on quantum Fourier transform. *Quantum Inf Process*, 2018, 17: 129
- 13 Ji Z X, Zhang H G, Wang H Z, et al. Quantum protocols for secure multi-party summation. *Quantum Inf Process*, 2019, 18: 168
- 14 Duan M Y. Multi-party quantum summation within a d -level quantum system. *Int J Theor Phys*, 2020, 59: 1638–1643
- 15 Tavakoli A, Herbauts I, Żukowski M, et al. Secret sharing with a single d -level quantum system. *Phys Rev A*, 2015, 92: 030302, arXiv: [1501.05582](#)
- 16 Yang Y G, Xia J, Jia X, et al. Comment on quantum private comparison protocols with a semi-honest third party. *Quantum Inf Process*, 2013, 12: 877–885
- 17 Chen X B, Tang X, Xu G, et al. Cryptanalysis of secret sharing with a single d -level quantum system. *Quantum Inf Process*, 2018, 17: 225
- 18 Li C Y, Zhou H Y, Wang Y, et al. Secure quantum key distribution network with Bell states and local unitary operations. *Chin Phys Lett*, 2005, 22: 1049–1052, arXiv: [0705.1746](#)
- 19 Li C Y, Li X H, Deng F G, et al. Efficient quantum cryptography network without entanglement and quantum memory. *Chin Phys Lett*, 2006, 23: 2896–2899, arXiv: [0705.1748](#)
- 20 Long G L, Liu X S. Theoretically efficient high-capacity quantum-key-distribution scheme. *Phys Rev A*, 2002, 65: 032302, arXiv: [quant-ph/0012056](#)
- 21 Zhou Z R, Sheng Y B, Niu P H, et al. Measurement-device-independent quantum secure direct communication. *Sci China-Phys Mech Astron*, 2020, 63: 230362, arXiv: [1805.07228](#)
- 22 Niu P H, Zhou Z R, Lin Z S, et al. Measurement-device-independent quantum communication without encryption. *Sci Bull*, 2018, 63: 1345–1350
- 23 Wu J W, Lin Z S, Yin L G, et al. Security of quantum secure direct communication based on Wyner's wiretap channel theory. *Quantum Eng*,

2019, 1: e26

- 24 Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing. Bangalore, 1984. 175–179
- 25 Shor P W, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys Rev Lett*, 2000, 85: 441–444, arXiv: [quant-ph/0003004](https://arxiv.org/abs/quant-ph/0003004)
- 26 Gao F, Qin S J, Wen Q Y, et al. A simple participant attack on the Bradler-Dusek protocol. *Quantum Inf Comput*, 2007, 7: 329
- 27 Chang Y J, Tsai C W, Hwang T. Multi-user private comparison protocol using GHZ class states. *Quantum Inf Process*, 2013, 12: 1077–1088
- 28 Romero J. Shaping up high-dimensional quantum information. *AAPPS Bull*, 2019, 29: 2–4

Quantum secure multiparty summation based on the mutually unbiased bases of d -level quantum systems and its application

YE Tian-Yu^{*} & HU Jia-Li

College of Information & Electronic Engineering, Zhejiang Gongshang University, Hangzhou 310018, China

In this paper, a novel quantum secure multiparty summation protocol is proposed based on the mutually unbiased bases of d -level quantum systems. The quantum states of mutually unbiased bases, which are transmitted in a circular pattern, are imposed with the transformation operations of n secrecy owners to encode their secrecies. Security analysis reveals that the proposed protocol can resist outside attacks as well as participant attacks. The proposed protocol is suitable for d -level quantum systems and can calculate the modulo d addition using the integer-by-integer technique. Compared with the quantum secure summation protocols with bit-by-bit calculations, the proposed protocol has a higher calculation efficiency and has more extensive applications compared with the protocols with smaller modulo. Moreover, this protocol can be successfully used for quantum multiparty private comparison and quantum multiparty anonymous voting.

quantum secure multiparty summation, mutually unbiased bases, quantum multiparty private comparison, quantum multiparty anonymous voting

PACS: 03.67.Dd, 03.67.Hk, 03.67.Pp

doi: [10.1360/SSPMA-2020-0262](https://doi.org/10.1360/SSPMA-2020-0262)