DOI: 10.3969/j.issn.1007-5461.2024.01.012

基于半量子安全直接通信的量子拍卖协议

杨 涵[1*]， 冯 雁[1,2]， 谢四江[1,2]

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

摘 要: 针对现有量子密封拍卖协议中存在的报价隐私保护不够、恶意竞标者与第三方共谋等问题，提出了一种基于半量子安全直接通信的量子密封投标拍卖协议。该协议采用半量子安全直接通信，通信时拍卖方仅需拥有测量和反射粒子的能力；通过对投标方报价的保序加密，实现对报价的隐私保护；利用隐私比较，在无第三方参与的情况下，拍卖方也能比较保序加密后的报价信息。理论分析表明面对截获-重发、受控非门 (CNOT)、相位反转、共谋等攻击时，所提出协议仍具有较高的安全性，且与同类型量子拍卖协议相比，新协议通信效率不受投标人数的影响。

关 键 词: 量子信息; 量子拍卖; 量子密封投标拍卖; 半量子; 保序加密; 隐私比较

中 图 分 类 号 : TN918.1 **文 献 标 识 码 :** A **文章编号:** 1007-5461(2024)01-00125-10

Quantum auction protocol based on semi-quantum secure direct communication

YANG Han[1*], *FENG Yan*[1,2], *XIE Sijiang*[1,2]

(1 Cyberspace Security Department, Beijing Electronic Science and Technology Institute, Beijing 10070, China;
2 University of Science and Technology of China, Hefei 230026, China)

Abstract: To address the issues of insufficient privacy protection of quotations and collusion between malicious bidders and third parties in existing quantum sealed auction protocols, a quantum sealed-bid auction protocol based on semi-quantum secure direct communication is proposed. Firstly, the protocol adopts semi-quantum secure direct communication, in which the auctioneer only needs to measure and reflect particles during communication. Secondly, the bidder can achieve the privacy protection of quotations through order-preserving transformation. Thirdly, the auctioneer can achieve privacy comparison of the transformed bid information without the participation of a trusted third party. Theoretical analysis shows that the proposed protocol is highly secured even facing attacks such as intercept-resend attack, control-NOT (CNOT) attack, phase inversion, and collusion attack. In addition, compared with the existing similar quantum auction schemes, the communication efficiency of the new protocol is not affected by the number of bidders.

Key words: quantum information; quantum auction; quantum sealed-bid auction; semi-quantum; order preserving encryption; private comparison

基金项目: 安徽省量子通信与量子计算机重大项目引导性项目 (AHY180500), 广东省重点领域研发计划项目 (2020B03030100001)

作者简介: 杨 涵 (1998 -), 女, 研究生, 浙江温州人, 主要从事网络安全、量子密码方面的研究。E-mail: 3430127080@qq.com

导师简介: 谢四江 (1971 -), 湖北鄂州人, 硕士, 正高级工程师, 硕士生导师, 主要从事密码系统、量子保密通信网络安全体系等方面的研究。E-mail: xiesj@besti.edu.cn

收稿日期: 2022-03-30; **修改日期:** 2022-04-29

*通信作者。

0 引 言

电子拍卖作为现代化生活中特殊的商品交易方式, 使用户可以足不出户就能网上竞拍。传统电子拍卖协议的安全性主要依托于经典密码体制, 而量子计算的发展, 使得基于计算复杂性的经典加密机制在量子计算环境下不再安全, 由此一些研究者提出了量子拍卖。量子拍卖利用量子信息技术保障整个拍卖系统的安全性和高效性。量子密封拍卖作为量子拍卖的一种主要类型, 要求报价密封后不可更改、不可否认, 且量子具有不可克隆、不可测量等特性, 在保护报价隐私方面具有独特的优势。

2009 年, Naseri[1]提出了首个量子密封投标拍卖协议, 协议基于量子安全直接通信, 使用 GHZ 态作为信息传输的载体。同年, 针对文献[1]: Qin 等[2]指出其报价的密封性不强, 且无法抵御双 CNOT 攻击; Yang 等[3]指出其协议无法抵御假粒子纠缠; Liu 等[4]发现其协议无法及时发现截获-重发攻击, 且恶意投标者能够通过截获-重发非法赢得拍卖; Zheng 等[5]指出其协议无法抵御拍卖商和投标者共谋攻击。2010 年, Zhao 等[6]加入后确认机制, 以抵御共谋攻击, 但通信复杂度较高且无法预防大量竞标者串谋[7]。2011 年, Xu 等[8]针对文献[6]中恶意投标者可以猜到他人投标价的问题, 引入 Hash 函数, 但 Zhao 等[9]指出该协议存在碰撞的情况, 可以通过共谋猜测得到他人投标价。2012 年, He 等[7]改进了编码规则, 以解决文献[9]指出的投标者串谋问题。2013 年, Luo 等[10]指出文献[10]中一组恶意的投标者通过共谋猜测测量基, 有极高的概率获得投标价。2014 年, Wang 等[11]指出之前的协议中, 无法确定引入错误的是外部窃听者, 还是不诚实的拍卖商。2015 年, Wang 等[12]用置换原理改进后确认机制, 解决多个投标者共谋问题。上述协议中, 均采用 GHZ 态粒子实现投标, 有些研究学者考虑到降低资源制备难度, 使用其他粒子进行报价的传输。2010 年, Wang[13]使用 Bell 态实现量子密封投标拍卖。2014 年, Liu 等[14]指出文献[14]同样无法抵御 CNOT 攻击和共谋攻击。2016 年, liu 等[15]使用单光子完成投标, 但仍旧无法抵御共谋攻击[16] 。2018 年, Zhang 等[17]提出基于双模单光子的拍卖协议来提高粒子利用率。2019 年, Shi 等[18]提出用公告板机制代替后确认机制, 引入了公告板管理者; Liang 等[19]引入了可信第三方 TTP 对报价进行量子签名; Wang 等[20,21]引入半可信第三方进行报价的隐私比较, 并用秘密共享代替后确认机制。2020 年, Shi 等[22]提出用 Bell 态实现身份双向认证, 引入了身份管理者。2022 年, Shi[23]提出由两位拍卖师共同参与协议, 并设定二者互相监督不共谋。上述拍卖协议[18−22]虽然降低了后确认阶段复杂度, 但需引入半可信或可信第三方帮助完成拍卖, 且要求第三方不与参与者共谋。针对第三方不可信的问题, Shi 等在文献[24]中将报价区间转换成向量的形式完成比较, 在文献[25]中使用量子安全多方分离 (SMD) 完成比较, 但可能需进行多轮比较才能实现, 复杂度较高。而且, 目前几乎所有的量子拍卖协议的安全通信皆是建立在量子安全直接通信上, 对拍卖双方的量子能力均要求较高。

为了解决报价隐私保护问题及恶意投标者与第三方共谋问题, 本文受文献[26]启发, 将保序加密[27]与隐私比较[28]结合, 提出一种新的基于半量子安全直接通信的拍卖协议, 协议过程无需可信第三方参加, 且降低了对拍卖方量子能力的要求, 提高了安全性。

1 基础知识

1.1 Bell 态

本协议用到的 Bell 态粒子由四个两粒子纠缠态组成, 可表示为

$$\begin{cases} \left|\varphi^{+}\right\rangle = \frac{1}{\sqrt{2}}(\left|00\right\rangle + \left|11\right\rangle) \\ \left|\varphi^{-}\right\rangle = \frac{1}{\sqrt{2}}(\left|00\right\rangle - \left|11\right\rangle) \\ \left|\psi^{+}\right\rangle = \frac{1}{\sqrt{2}}(\left|01\right\rangle + \left|10\right\rangle) \\ \left|\psi^{-}\right\rangle = \frac{1}{\sqrt{2}}(\left|01\right\rangle - \left|10\right\rangle) \end{cases}. \tag{1}$$

1.2　半量子通信

半量子通信是指在通信过程中, 通信双方仅有一方即强量子方具有完整的量子操控能力, 比如量子态区分、投影测量、量子态制备等操作, 另一方即半量子方仅具有反射和测量量子操作的能力。其中, 反射操作是指半量子方对强量子方发来的粒子不做任何操作, 直接反射回去; 测量操作是指半量子方对强量子方发来的粒子进行Z基测量[26]。

1.3　半量子安全直接通信模型

半量子安全通信指强量子发送方能够安全直接地将信息传输给半量子接收方。Zheng 等[26]提出的半量子安全通信模型基于Bell态和半量子通信思想, 实现强量子方 Alice 向半量子方 Bob 发送长度为 n 的二进制位隐私信息, 简要步骤如下:

1) Alice 从 $\left|\varphi^{\pm}\right\rangle, \left|\psi^{\pm}\right\rangle$ 中随机制备 $N=4n(1+\delta)$ 个 Bell 态粒子, 并将所有第一位粒子称为序列 H 并保留, 将第二位粒子称为序列 T 并发送给 Bob。

2) Bob 收到后随机对每个粒子选择反射或测量操作, 选择反射则直接返回给 Alice, 选择测量则保留测量结果 M_B。

3) Alice 暂存 Bob 反射回的粒子并通知 Bob, 接着 Bob 公布反射粒子具体位置, Alice 将反射粒子与序列 H 相应粒子一起进行 Bell 基测量, 计算错误率, 若错误率大于阈值则通信停止, 反之信道建立成功。

4) Alice 用 Z 基测量剩余 H 序列, 并得到结果 M_A, 从 M_A 随机选择 n 位粒子编码秘密消息 M_e, 编码规则为: 若消息为 0 则 Alice 不做操作, 若为 1 则相应位置相位取反, 剩余 n 位粒子称 M_c 用于安全性检测。Alice 组合 M_e 和 M_c, 得到 M_A' 并发送给 Bob。

5) Bob 收到后对 M_A' 进行 Z 基测量, Alice 公布 M_c 和 M_e 的位置和初次测量结果, Bob 计算 M_c 测量结果的错误率, 若错误率低于阈值, 协议继续, 反之停止。

6) Alice 公布序列的初始 Bell 态, Bob 根据 M_e 的测量结果结合保留的 M_B, 可知 Alice 发送的信息。具体转换规则为: 当初始 Bell 态为 $\left|\varphi^{\pm}\right\rangle$ 时, 若 M_B 为 0, 则 Alice 发送的信息与 M_e 一致; 若 M_B 为 1, 则信息与 M_e 相反。初始 Bell 态为 $\left|\psi^{\pm}\right\rangle$ 时, 若 M_B 为 0, 则信息与 M_e 相反; 若 M_B 为 1, 则信息与 M_e 一致。

2　拍卖协议

假设拍卖协议的参与方由拍卖商 A 及 n 位投标者 $B_i\,(i=1,2,\cdots,n)$ 组成, 投标者 $B_i\,(i=1,2,\cdots,n)$ 分别持有私人投标价 $x_i\,(i=1,2,\cdots,n)$。协议规定拍卖商 A 为半量子方, 只能完成反射和 Z 基测量操作。投标者 B_i $(i=1,2,\cdots,n)$ 作为强量子方, 拥有全部的量子操控能力。

拍卖协议分为准备、加密、投标及公布四个阶段。准备阶段主要是参与双方约定公共参数等信息; 加密阶段主要是 B_i 加密报价 x_i 不改变报价顺序的关系下, 实现报价的隐私性, 并承诺自己报价的真实性及不可

更改性; 投标阶段主要是B_i通过半量子安全直接通信发送处理后的加密报价给A; 公布阶段是A通过对比加密后的报价找到并公布中标者及中标价, 各方可以验证中标价的真实性。

2.1 准备阶段

步骤1: 拍卖商A和投标者$B_i(i=1,2,\cdots,n)$之间通过量子密钥分发 (QKD) 协议共享一组密钥K_{ABi} ($K_{ABi}=\{K_{AB1},K_{AB2},\cdots,K_{ABn}|K_{ABi}\in\{00,01,10,11\}\}$)。同时A和$B_i(i=1,2,\cdots,n)$约定以下信息: 安全参数a ($a>1$且$\forall x_i>a,a\in N^*$), 一个抗碰撞的Hash函数H: $\{0,1\}^*\to\{0,1\}^d$ (d为Hash函数的输出长度), 及一组由非零自然数组成的非等差递增序列$\left\{k_1,k_2,\cdots,k_n,\ (\forall i>j,k_i>k_j)\right\}$, $k_i\in N^*$。

2.2 加密阶段

步骤2: 投标者B_i根据参数a对自己的报价$x_i(i=1,2,\cdots,n)$进行预处理, 得到m_i和s_i。具体处理方式可表示为

$$x_i\xrightarrow{a}\begin{cases}m_i=\lfloor\log_a x_i\rfloor,\text{"}\lfloor\ \rfloor\text{"表示向下取整}\\ s_i=x_i\cdot a^{-m_i}\end{cases}\Rightarrow x_i=a^{m_i}\cdot s_i\quad . \tag{2}$$

由 (2) 式和$a(a>1$且$\forall x_i>a,a\in N^*)$可知m_i和s_i的数据范围及数据类型, 由$x_i>a,m_i=\lfloor\log_a x_i\rfloor$可得$m_i\geq 1$且为整数; 由$a^{m_i}\leq x_i<a^{m_i+1}\xrightarrow{\cdot a^{-m_i}}1\leq s_i<a$, 可知$1\leq s_i<a$且$s_i$不一定为整数。通过比较$m_i+\frac{s_i}{a}$的顺序, 拍卖商能够得到对应$x_i$的顺序关系。

步骤3: 投标者B_i对m_i进行保序加密得到对应的密文m_i^*, 加密规则可表示为

$$m_i^*=\begin{cases}k_1\cdot m_i, & m_i<k_1\\ k_j\cdot m_i, & k_j\leq m_i<k_{j+1}\quad (j=1,2,\cdots,n-1)\\ k_n\cdot m_i, & k_n\leq m_i\end{cases}\quad . \tag{3}$$

由于$1\leq s_i<a\Rightarrow 0<\frac{s_i}{a}<1$, 对$m_i$的加密不会改变对应$m_i^*+\frac{s_i}{a}$的顺序关系, 仍能够反映出$x_i$的顺序关系。该方法实现了对报价的非线性加密, 且将报价拆分成两个数据, 必须同时拥有两种数据才能实现比较, 报价的安全性和隐私性得到了更好的保护。

步骤4: 投标者B_i将密文m_i^*转换成长度为l_1的二进制数, 将$\frac{s_i}{a}$转换成长度为l_2的二进制数, 并将二者按如下规则拼接

$$str_i=\begin{cases}str(m_i^*)+str(\frac{s_i}{a}),K_{ABi}\in\{00,01\}\\ str(\frac{s_i}{a})+str(m_i^*),K_{ABi}\in\{10,11\}\end{cases}\quad , \tag{4}$$

式中$str(m)$表示将m转换成二进制字符串。

步骤5: 投标者B_i随机选取一个长度为$l=l_1+l_2$的二进制序列随机数$r_i\in\{0,1\}^l$, 并根据共享的强碰撞hash函数, 计算h_i并公告

$$h_i=H(r_i\oplus H(r_i\oplus str_i))\quad , \tag{5}$$

除B_i外的人在r_i未知的情况下, 无法通过h_i得知str_i的值。

2.3　投标阶段

步骤 6: 每位投标者 $B_i(i=1,2,\cdots,n)$ 随机从四组 Bell 态 $|\varphi^{\pm}\rangle,|\psi^{\pm}\rangle$ 中选择, 制备 $N=4l(1+\delta)$ 个 Bell 态粒子, 其中 l 为秘密消息的长度, δ 为固定参数。称 B_i 制备的 Bell 态粒子中, 所有的第一位粒子为 C_i 序列, 所有的第二位粒子为 D_i 序列。B_i 保留序列 C_i, 将序列 D_i 发送给拍卖商 A。

步骤 7: 拍卖商 A 收到 B_i 发送的 D_i 序列后, 随机对每个粒子执行测量或反射操作, 执行测量操作时, A 对粒子 Z 基测量, 并将测量结果保存为 M_{B_i}, $M_{B_i}\in\{0,1\}$; 执行反射操作时, A 直接将粒子发回给 B_i, 不做任何其他操作。当 N 足够大时, A 选择测量和反射的粒子总数相同, 均为 $2l$, 以下假设 N 为足够大的情况。

步骤 8: 投标者 B_i 暂存 A 反射回来的粒子序列, 并告知 A 接收完成。接着, A 告知 B_i 反射粒子在 D_i 序列中的位置信息。然后, B_i 根据 A 公布的信息找到 C_i 序列中对应位置的粒子, 与接收的反射粒子一起执行 Bell 基测量, 进行窃听检测操作, 即 B_i 将测量结果与初始状态进行对比, 计算错误率, 若错误率低于约定的阈值, 则认为量子信道成功建立, B_i 丢掉所有反射粒子并进行下一步; 否则, 协议结束。

步骤 9: 投标者 B_i 选择 Z 基对剩余的序列 C_i 粒子进行测量, 得到测量结果 M_{A_i}, $M_{A_i}\in\{0,1\}$。B_i 从中随机挑选 l 个粒子将密文 str_i 按照编码规则, 组成编码序列, 记为 M_{e_i}。具体编码规则为: 当前位置的秘密消息为 0 时, B_i 不做任何操作, 当前位置秘密消息为 1 时, B_i 将对应位置的粒子相位取反, 即 $|0\rangle\leftrightarrow|1\rangle$, 得到编码序列。$B_i$ 从剩余粒子中随机挑选 l 个粒子组成窃听检测粒子序列 M_{c_i}。然后, B_i 按照一定规则组合 M_{A_i}', 组合规则为

$$M_{A_i}'=\begin{cases}M_{e_i}+M_{c_i}, K_{ABi}\in\{00,10\}\\ M_{c_i}+M_{e_i}, K_{ABi}\in\{01,11\}\end{cases},\tag{6}$$

然后将 M_{A_i}' 发送给 A。

步骤 10: 拍卖商 A 收到 M_{A_i}' 后, 对 M_{A_i}' 进行 Z 基测量。A 根据 K_{ABi} 可以恢复 M_{e_i} 和 M_{c_i} 正确位置顺序。B_i 公布 M_{e_i} 和 M_{c_i} 初始 Bell 态粒子状态。然后, A 对收到的序列进行测量操作, 得到 M_{e_i} 和 M_{c_i} 的值, 对应 B_i 公布的初始 Bell 态可以进行安全窃听检测: 若 B_i 制备的 Bell 态粒子为 $|\varphi^{\pm}\rangle(|\psi^{\pm}\rangle)$, A 测量 M_{B_i} 和 M_{c_i} 的结果若不是 00 或 11 (10 或 01), 则说明发生窃听或其他错误, 若错误率低于约定的阈值, 则协议继续; 否则, 协议结束。

步骤 11: 拍卖商 A 根据编码序列 M_{e_i} 的测量值、M_{B_i} 的测量值, 及 B_i 公布的初始 Bell 态信息约定的编码规则, 可以得到 B_i 想要发送的 str_i。具体转换规则如表 1 所示。

表 1　获取秘密信息 str_i 的过程

Table 1　The process of obtaining secret information str_i

The original Bell state	M_{B_i}	M_{e_i}	str_i	The original Bell state	M_{B_i}	M_{e_i}	str_i
$\|\varphi^{\pm}\rangle$	0	0	0	$\|\psi^{\pm}\rangle$	0	1	0
	0	1	1		0	0	1
	1	1	0		1	0	0
	1	0	1		1	1	1

2.4　公布阶段

步骤 12: 拍卖商 A 根据 str_i 和 K_{ABi}, 得到 m_i^* 和 $\frac{s_i}{a}$, 后计算并比较 $m_i^*+\frac{s_i}{a}$, 选出最大值假定为 $m_{e\max}^*+\frac{s_{e\max}}{a}$, 投标者 B_e 即为中标者。A 能够通过 $m_{e\max}^*+(s_{e\max}/a)$ 还原对应的 x_e, 若仅有 B_e 认领, 则中标者 B_e 公布 r_e, 所有人能够根据 B_e 公布的 h_e 验证其真实性, 若其他投标者没有提出异议, 拍卖成功。

3 安全分析

拍卖协议的安全主要指投标方报价数据的隐私保密性, 以及所有参与计算的参与者传输数据信息过程的机密性、防窃听性。本节重点分析计算过程中外部攻击者进行攻击, 以及恶意参与者进行共谋攻击时, 协议是否可以检测到攻击以保证拍卖过程的安全。

3.1 外部攻击

假设存在一个A和B_i以外的外部攻击者Eve想要获取或是改变B_i发送给A的秘密信息, 但不希望被A和B_i发现, 那么他将攻击步骤6、9中的粒子序列传输过程, 能够获得的有效信息一是步骤6中B_i将D_i序列的粒子发送给A, 二是步骤9中A完成窃听检测后, B_i将编码后的M_{A_i}'序列发给A。

3.1.1 截获-重发攻击

步骤6中, B_i将D_i序列的粒子发送给A, Eve进行截获-重发攻击, 即截获传输的粒子序列D_i并测量, 根据得到的测量结果重新发送恰当的粒子给A。协议通过对A反射回的粒子进行窃听检测来避免截获-重发攻击, 由于传送的粒子是Bell态粒子的一部分, Eve截获测量的行为将导致Bell态粒子的坍缩, 引入错误量, 当Eve造成的错误率超过阈值, 信道将不被信任, 协议结束。

步骤9中, B_i将编码后的M_{A_i}'序列发给A, Eve进行截获-重发攻击, 即截获传输粒子序列M_{A_i}'并测量。协议利用密钥K_{ABi}保护投标者传输信息的正确顺序, 同时对获取到的M_{A_i}'进行安全性检测, Eve截获的行为也将导致Bell态粒子的坍缩, 引入错误量, 当错误率超过阈值时, 协议结束。

因此, 本协议可以抵御截获重发攻击。

3.1.2 CNOT攻击

步骤6中, B_i将D_i序列的粒子发送给A, Eve进行CNOT攻击, 即制备虚假粒子$|0\rangle_e$作为目标比特, 将截获到的粒子序列D_i作为控制比特进行CNOT操作后, 再发送给A, 根据虚假粒子的变换, 可以得到发送粒子的相位。协议通过窃听检测A反射的粒子, Eve进行CNOT攻击将可能导致粒子序列的粒子也发生相位变换, 具体变换如表2所示, 且由于C_i序列和D_i序列是一对纠缠粒子, 其中一方粒子变换, 另一方粒子随之改变, 这就引入了错误量, 而错误率超过阈值, 则协议结束。

步骤9中, B_i将编码后的M_{A_i}'序列发给A, Eve进行CNOT攻击, 即制备虚假粒子$|0\rangle_e$作为目标比特, 将截获到的粒子序列M_{A_i}'作为控制比特进行CNOT操作后, 再发送给A。协议也将对传输的粒子序列M_{A_i}'进行窃听检测, Eve的攻击行为将以同样的理由被发现导致协议结束。表2展示了粒子被攻击前后的状态。

表2 执行CNOT操作前后粒子状态

Table 2 Particle state before and after CNOT operation

Intercepting particles	Attacking particle	System mixed state after attack
$\|0\rangle_t$	$\|0\rangle_e$	$\|\phi_{\text{CNOT}}\rangle = \|0\rangle_t\|0\rangle_e$
$\|1\rangle_t$		$\|\phi_{\text{CNOT}}\rangle = \|1\rangle_t\|1\rangle_e$
$\|+\rangle_t$		$\|\phi_{\text{CNOT}}\rangle = \frac{\|0\rangle_t\|0\rangle_e + \|1\rangle_t\|1\rangle_e}{\sqrt{2}}$
$\|-\rangle_t$		$\|\phi_{\text{CNOT}}\rangle = \frac{\|0\rangle_t\|0\rangle_e - \|1\rangle_t\|1\rangle_e}{\sqrt{2}}$

因此, 本协议可以抵御CNOT攻击。

3.1.3 相位反转攻击

步骤6中, B_i将D_i序列的粒子发送给A, 攻击者Eve执行相位翻转攻击, 即将截获的粒子序列D_i进行相

位反转后再发送给A。协议仍能通过窃听检测发现C_i序列部分粒子的变换是由A测量引起的还是由攻击者Eve造成的, 若变换的粒子不在A告知反射粒子具体位置的情况过多, 意味着错误率超过阈值, 协议结束。

步骤9中, B_i将编码后的M_{A_i}'序列发给A, Eve 执行相位翻转攻击, 将截获的粒子序列M_{A_i}'进行相位反转后发送给A。协议在发送序列M_{A_i}'时, 由密钥K_{ABi}对报价数据进行重排, 即便Eve猜中正确顺序, Eve的攻击也会导致窃听检测的错误率超过阈值, 此时协议结束。

因此, 本协议可以抵御相位反转攻击。

3.2　共谋攻击

除以上提到外部攻击, 协议还将面临来自内部的攻击, 如共谋攻击, 由于本研究协议中除拍卖商A与投标者B_i无第三方参与者, 那么就意味着本研究协议仅需考虑恶意投标者与拍卖商之间的共谋。

假设拍卖商与恶意投标者共谋, 公布虚假的获胜价为$x_{e\max}$, 中标者为B_e, 而B_e的真实报价为x_e。此时, 其他投标者可以根据B_e公开的随机数r_e、密钥K_{ABe}和A宣布的$x_{e\max}$计算出$h_{e\max}$。由于Hash函数抗碰撞的特性, 难以找到$x_{e\max}\neq x_e$时$h_{e\max}=h_e$, 此时其他投标者通过计算将会发现$h_{e\max}\neq h_e$, 此时共谋攻击会被发现。

因此, 本协议可以抵御共谋攻击。

3.3　隐私性分析

在量子拍卖协议研究领域, 投标阶段主要通过纠缠态或单光子作为信息载体将报价信息发送给拍卖商, 拍卖商将得到投标者的真实报价, 投标者的报价并没有得到很强的隐私保护。本协议中, 包含拍卖商在内的所有参与者均不能获得其他投标者的真实报价。

本协议采用的加密方式仅保持报价顺序关系, 加密后的报价信息不呈线性关系, 对报价的隐私保护能力更强, 且通过纠缠态粒子传输信息, 一旦信息被测量或造成相位改变, 均将造成坍缩, 对报价的保护更高。表3展示了几个典型拍卖协议的隐私性比较。

表3 量子密封投标拍卖协议间的隐私性比较

Table 3 Privacy comparison between quantum sealed auction protocols

Item	Information carrier	Quantum carrying information	Quotation encryption mode	Privacy	Literature
1	Bell state	Real quotation	None	Low	Reference [4]
2	GHZ state	Real quotation	None	Low	Reference [6]
3	Single particle	Encryption quotation	Linear encryption	Normal	Reference [20]
4	Bell state	Encryption quotation	Nonlinear encryption	High	This research

3.4　效率分析

本协议基于半量子安全直接通信实现粒子的安全传输, 协议的通信效率取决于半量子安全直接通信的效率, 计算公式为

$$\eta=\frac{c}{q+b}\times 100\% \quad , \tag{7}$$

式中: c表示传输信息的粒子数, q表示传输过程中使用的量子粒子数, b表示经典交互信息数。本协议通信过程不需要交互经典信息, 即$b=0$。假设协议需要传输的粒子数$c=l$, 则传输过程中使用的量子粒子数q由步骤6中B_i制备的$8l$位粒子、步骤7中A进行反射操作返回的$2l$位粒子、步骤9中B_i发送加密报价的$2l$位

粒子以及步骤10中A返回用于窃听检测的l位粒子组成, 即$q=13l$。可见, 本协议的通信效率为$\eta=l/(13l+0)\times 100\%=7.69\%$。

本协议采用的半量子安全直接通信的通信效率与文献[29]提出的两种半量子安全直接通信协议相比, 通信效率较高, 如表4所示[26]。

表4 半量子安全直接通信的通信效率对比

Table 4 Communication efficiency comparison of semi-quantum secure direct communication

Item	c	q	b	Efficiency η	Protocol
1	l	$21l$	$2l$	4.35%	SQKD1 in reference [29]
2	l	$14l$	$2l$	6.25%	SQKD2 in reference [29]
3	l	$13l$	0	7.69%	Protocol proposed by this research

对比一些已有的量子拍卖协议, 由于对比的协议中用于窃听检测的粒子数量相对用于投标及后确认的粒子数较少, 因此在下表中忽略对比协议中窃听检测的粒子数。不难发现当参与投标的人数较少时, 本协议的通信效率是低于其他拍卖协议的, 但随着参与投标人数上升, 本协议的通信效率能够超过部分量子拍卖协议, 虽然仍旧低于部分协议, 但本协议降低了对拍卖商的量子能力要求, 使操作更为简化, 具体如表5所示。

表5 几种量子拍卖协议的通信效率对比

Table 5 Communication efficiency comparison of several quantum auction protocols

Item	Bidder's Quantum ability	Auctioneer's Quantum ability	Efficiency η (n: the number of bidders)	Literature
1	All	All	$\eta=1/n$ (ignore decoy particles)	Reference [6]
2	All	All	$\eta=1/(n+1)$ (ignore decoy particles)	Reference [10]
3	All	All	$\eta=20\%$ (ignore decoy particles)	Reference [19]
4	All	Measure and reflect	$\eta=7.69\%$	This research

4 结 论

本协议结合保序加密, 对报价加密后再传输给拍卖商进行隐私比较, 进一步加强了报价的隐私保护; 且协议无第三方参与, 让协议的安全性得到了进一步提升。另外, 本协议基于半量子安全直接通信模型, 在降低对拍卖方量子能力要求的同时, 使得操作简单化, 通信效率较其他半量子安全直接通信协议也有所提升, 当投标人数足够多时, 通信效率也能超过部分量子拍卖协议。通过理论分析可以证明本协议在同类型的量子拍卖协议中, 安全性有所提升, 对量子的能力要求降低, 但通信效率方面还有提升的空间。

参考文献:

[1] Naseri M. Secure quantum sealed-bid auction [J]. *Optics Communications*, 2009, 282(9): 1939-1943.

[2] Qin S J, Gao F, Wen Q Y, *et al*. Cryptanalysis and improvement of a secure quantum sealed-bid auction [J]. *Optics Communications*, 2009, 282(19): 4014-4016.

[3] Yang Y G, Naseri M, Wen Q Y. Improved secure quantum sealed-bid auction [J]. *Optics Communications*, 2009, 282(20): 4167-4170.

[4] Liu Y M, Wang D, Liu X S, *et al*. Revisiting Naseri's secure quantum sealed-bid auction [J]. *International Journal of Quantum Information*, 2009, 7(6): 1295-1301.

[5] Zheng Y Q, Zhao Z W. Comment on: "Secure quantum sealed-bid auction" [Opt. Comm. 282 (2009) 1939] [J]. *Optics Communications*, 2009, 282(20): 4182.

[6] Zhao Z W, Naseri M, Zheng Y Q. Secure quantum sealed-bid auction with post-confirmation [J]. *Optics Communications*, 2010, 283(16): 3194-3197.

[7] He L B, Huang L S, Yang W, *et al*. Cryptanalysis and melioration of secure quantum sealed-bid auction with post-confirmation [J]. *Quantum Information Processing*, 2012, 11(6): 1359-1369.

[8] Xu G A, Zhao Z W, Chen X B, *et al*. Cryptanalysis and improvement of the secure quantum sealed-bid auction with postconfirmation [J]. *International Journal of Quantum Information*, 2011, 9(6): 1383-1392.

[9] Zhao Z J, Wang W J. Comment on "Cryptanalysis and improvement of the secure quantum sealed-bid auction with post confirmation" [J]. *International Journal of Quantum Information*, 2014, 12(6): 1475001.

[10] Luo Y, Zhao Z W, Zhao Z J, *et al*. The loophole of the improved secure quantum sealed-bid auction with post-confirmation and solution [J]. *Quantum Information Processing*, 2013, 12(1): 295-302.

[11] Wang Q L, Zhang W W, Su Q. Revisiting "the loophole of the improved secure quantum sealed-bid auction with post-confirmation and solution" [J]. *International Journal of Theoretical Physics*, 2014, 53(9): 3147-3153.

[12] Wang J T, Chen X B, Xu G, *et al*. A new quantum sealed-bid auction protocol with secret order in post-confirmation [J]. *Quantum Information Processing*, 2015, 14(10): 3899-3911.

[13] Wang Z Y. Quantum secure direct communication and quantum sealed-bid auction with EPR pairs [J]. *Communications in Theoretical Physics*, 2010, 54(6): 997-1002.

[14] Liu W J, Wang F, Ji S, *et al*. Attacks and improvement of quantum sealed-bid auction with EPR pairs [J]. *Communications in Theoretical Physics*, 2014, 61(6): 686-690.

[15] Liu W J, Wang H B, Yuan G L, *et al*. Multiparty quantum sealed-bid auction using single photons as message carrier [J]. *Quantum Information Processing*, 2016, 15(2): 869-879.

[16] Zhang K J, Kwek L C, Ma C G, *et al*. Security analysis with improved design of post-confirmation mechanism for quantum sealed-bid auction with single photons [J]. *Quantum Information Processing*, 2018, 17(2): 38.

[17] Zhang R, Shi R H, Qin J Q, *et al*. An economic and feasible quantum sealed-bid auction protocol [J]. *Quantum Information Processing*, 2018, 17(2): 35.

[18] Shi R H, Liang F Y, Wang Q, *et al*. An effective quantum sealed-bid auction protocol [J]. *Netinfo Security*, 2019(8): 44-50.
石润华, 梁风雨, 王 晴, 等. 一种有效的量子密封投标拍卖协议 [J]. 信息网络安全, 2019(8): 44-50.

[19] Liang F Y. *Design of Verifiable Quantum Sealed Bidding Auction Protocol* [D]. Hefei: Anhui University, 2020.
梁风雨. 可验证的量子密封投标拍卖协议设计 [D]. 合肥: 安徽大学, 2020.

[20] Wang Q. *Research on Privacy Protection and Post-confirmation Mechanism of Quantum Sealed Bidding Auction* [D]. Hefei: Anhui University, 2020.
王 晴. 量子密封投标拍卖的隐私保护与后确认机制研究 [D]. 合肥: 安徽大学, 2020.

[21] Wang Q, Shi R H, Chen Z K, *et al*. A quantum sealed auction protocol based on secret sharing [J]. *International Journal of Theoretical Physics*, 2019, 58(4): 1128-1137.

[22] Shi R H, Zhang R, Liu B, *et al*. Cryptanalysis and improvement of quantum sealed-bid auction [J]. *International Journal of Theoretical Physics*, 2020, 59(6): 1917-1926.

[23] Shi R H. Anonymous quantum sealed-bid auction [J]. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2022, 69 (2): 414-418.

[24] Shi R H. Quantum sealed-bid auction without a trusted third party [J]. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2021, 68(10): 4221-4231.

[25] Shi R H, Li Y F. A feasible quantum sealed-bid auction scheme without an auctioneer [J]. *IEEE Transactions on Quantum Engineering*, 2022, 3: 1-12.

[26] Zheng T, Zhang S B, Sun Y H, *et al*. Semi-quantum secure direct communication protocol based on Bell state [J]. *Application Research of Computers*, 2020, 37(7): 2144-2147.
郑 涛, 张仕斌, 孙裕华, 等. 基于贝尔态的半量子安全直接通信协议 [J]. 计算机应用研究, 2020, 37(7): 2144-2147.

[27] Ahmed S, Annisa, Zaman A, *et al*. Semi-order preserving encryption technique for numeric data to enhance privacy [C]. *Fifth International Symposium on Computing and Networking,* Aomori, Japan, IEEE, 2017.

[28] Ji Z X, Zhang H G, Wang H Z. Quantum private comparison protocols with a number of multi-particle entangled states [J]. *IEEE Access*, 2019, 7: 44613-44621.

[29] Shukla C, Thapliyal K, Pathak A. Semi-quantum communication: Protocols for key agreement, controlled secure direct communication and dialogue [J]. *Quantum Information Processing*, 2017, 16(12): 295.