Quantum Information Processing (2024) 23:70
https://doi.org/10.1007/s11128-024-04268-2

Quantum sealed-bid auction protocol with post-confirmation based on blind signature

Qiuling Yue[1,2] · Chen Zhong[1] · Hong Lei[1,3]

Received: 12 July 2023 / Accepted: 12 January 2024

Abstract

Quantum sealed-bid auction protocol with post-confirmation is the one that ensures the fairness of the auction by verifying whether there is cheating after the winner is announced. To guarantee fairness, it is necessary to have both privacy and public verification simultaneously. In this paper, we make a first attempt to use the blind feature of the information in the blind signature to protect the bids' privacy and use two-state vector formalism to achieve public verification. Compared to previous quantum sealed-bid auction schemes, the utilization of these techniques gives our scheme a novel and distinctive quantum flavor. Through analysis and comparison, our scheme can resist malicious bidder attacks as well as collusive attacks. In addition, the efficiency of our scheme is also considerable. Participants only need to prepare EPR states, not complex multi-particle entangled states, and even the auctioneer can be purely classical.

Keywords Quantum sealed-bid auction · Post-confirmation · Quantum blind signature · Two-state vector formalism

✉ Hong Lei
leihong@hainanu.edu.cn

Qiuling Yue
yueqiuling@hainanu.edu.cn

Chen Zhong
zhongchen_@hainanu.edu.cn

[1] School of Cyberspace Security (School of Cryptology), Hainan University, Haikou 570228, China

[2] Key Laboratory of Internet Information Retrieval of Hainan Province, Haikou 570228, China

[3] SSC Holding Company Ltd., Chengmai 571924, China

Published online: 20 February 2024

1 Introduction

Since the first quantum protocol was proposed in 1984 [1], the development of quantum technology has achieved remarkable evolution and profound development. Initially, Bennett and Brassard proposed the quantum key distribution protocol, which theoretically enables uncrackable secure key transmission and addresses the potential threat of classical cryptography. This innovative idea leads the research direction of quantum cryptography and also triggers the extensive research of quantum information science. With the deepening of research, the research of quantum key distribution protocol has made great progress [2, 3]. In addition, quantum protocols with different characteristics and functions have emerged one after another, and have made rich theoretical results and experimental progress. For example, through quantum technology to achieve the direct transmission of information quantum direct secure communication protocol [4, 5], A quantum private query protocol that uses quantum technology to query information while protecting user privacy [6], quantum auction protocols to ensure fairness and transparency of bidding through quantum technology [7], as well as some other protocols related to the security of quantum communication [8–11]. The research of these quantum protocols will continue to lead the evolution of information science and communication technology.

This paper focuses on the design of quantum auction protocol to ensure the security of information transmission in the auction process by using quantum technology.

Auction is an ancient and still existing way of market transaction. According to different auction rules, there are many different auction methods. The British auction, for example, is also known as the rising auction, starting from the starting price, the bidder keeps increasing the bidding price until no one is willing to pay more [12, 13]. Another common type of auction is the sealed auction, which means that all bidders bid through sealed bids at the same time, no one knows the bids of others, and the highest bidder gets the lots [12, 14].

The concept of a quantum auction was introduced by Piotrowski et al. for the first time in 2008 [7]. In 2009, the quantum sealed-bid auction (QSA) protocol was based on the quantum secure direct communication protocol, which was first proposed by Naseri [14]. However, Naseri's protocol has many security vulnerabilities, such as Qin et al. 's discovery that a double CNOT attack can enable malicious bidders to obtain private bids from other bidders without being detected [15]. In addition, Yang et al. found that in this agreement, malicious bidders can obtain private bids from other bidders by sending fake entanglement resources [16]. Therefore, this protocol does not fairly accomplish the task of a sealed-bid auction. To defend against these attacks, A QSA with post-confirmation was proposed by Zhao et al. [17]. However, He et al. found that there was no resistance to collusive attacks by malicious bidders and dishonest auctioneers, which made it impossible to guarantee the fairness of auctions [18].

Since then, various new QSA protocols based on different models and other protocols have been proposed, (see Table 1, which is the classification of common QSA protocols based on different quantum protocol) further enriching the research work of quantum auction protocols. Such as QSA with secret order [19], in which bidders encode their bids by preparing their particles with a secret order. Quantum secret

Table 1 Classification of common QSA protocols based on different quantum protocol

Utilized quantum protocol	Schemes
Quantum secure direct communication	Scheme in [14, 15]
Quantum super dense coding	Scheme in [17]
Quantum secret order	Scheme in [19]
Quantum secret sharing	Scheme in [20, 21]
Quantum public key encryption	Scheme in [22]
Quantum key agreement	Scheme in [23]
Quantum algorithm	Scheme in [24]

sharing protocol is one of the more common ways to design QSA protocols, which distribute the bids as shared secret information to other bidders and after then verify the dishonest operation by restoring the secret later [20, 21]. Besides, other quantum cryptographic schemes, such as quantum public key encryption and quantum key agreement, have also been attempted use to implement QSA protocols [22, 23]. In addition, people are keen to study QSA protocols with various features and functions, which can better solve the corresponding problems in practice, such as QSA protocols with privacy-preserving [24, 25] [12, 26–29]. As a protocol with both security and application requirements, the cryptanalysis and improvement of the QSA protocol have also received much attention [30, 31].

In the process of studying QSA, especially QSA with post-confirmation, we noticed that there is a certain similarity between it and quantum blind signatures [32, 33]. That is, both schemes are needed to send secret information to others for their approval, but cannot let others know the real information. Therefore, we also focus on blind signatures. Chaum made the initial suggestion for a blind signature in [34], which is a special signature to prevent the signer to obtain the original information. After that, people used various ways to implement blind signatures(Since our goal is a quantum scheme, here we focus only on quantum blind signatures). For example, there are many blind signature protocols designed using different types of states, including EPR state [32, 35, 36], GHZ states [37, 38], χ-type entangled states [39], BB84-states [33].

In this paper, by extracting the commonalities between fairness requirements of QSA and blindness of blind signature, we put forward for the first time under this thought a QSA with post-confirmation protocol based on the blind signature.

Our scheme can provide a new way to design QSA with post-confirmation, which is different from the previous methods, and we hope it can provide inspiration for more researchers to design more abundant QSA schemes. In addition, our work will further promote the integration of different protocols. In the meantime, another noteworthy feature of our scheme is the adoption of two-state vector formalism (see Appendix for more details), which we think is a suitable tool to implement a post-confirmation mechanism to ensure the fairness of the QSA protocol [40–42]. For two-state vector formalism is utilized to sketch the complete description of a system between two measurements. This property of the two-state vector form is consistent with the case of the two measurements used in our scheme, the first being that bidders encode their bids into quantum states by measurement, and the second being confirmed by measurement after bid opening. Therefore, we can deduce whether there is cheating behavior according to the probability of the results of two measurements.

The rest of the paper is organized as follows. The general blind signature model is shown in Sect. 2. In Sect. 3, we propose a new QSA protocol with post-confirmation based on a quantum blind signature, which uses two states vector formalism. In Sect. 4, we give a security analysis of the new QSA protocol and three enhanced schemes. Three enhanced versions are presented in Sect. 5, which can detect if a malicious bidder is dishonestly executing the agreement and make our scheme resistant to Trojan attacks. Efficiency and other properties are discussed in Sect. 6. Finally, we make a conclusion in Sect. 7.

2 Blind signature

Blind signature is a way for signers to sign without knowing the specific content, which is widely used in electronic payment systems, electronic election voting, and other situations that need to protect the privacy of messages [32, 34]. Here, we describe an abstract blind signature model, regardless of whether it is a quantum version or a classical one.

(1) Initialization phase. In this stage, the signature applicant, signer, and verifier prepare for signature, including identity authentication, key preparation, or challenge sending.
(2) Message blinding phase. In this stage, the signer secretly selects a blinding factor to blind the real message to be signed and then sends the blinded message to the signer.
(3) Signature phase. The signer signs the received message and sends the signature and signed message together to the signature applicant. Note that the signer cannot see the real message.
(4) Blindness phase. The signature applicant will de-blind the signature received and get the real information and its legitimate signature.
(5) Verification phase. The signature verifier verifies the validity of the signature.

3 QSA protocol with post-confirmation based on SHWL blind signature

There are some common characteristics of quantum sealed-bid auction and quantum blind signature, so we exploited SHWL blind signature [32] to build a novel quantum sealed-bid auction protocol. SHWL protocol not only satisfies the characteristics of blind signature that the information is not known to others but more importantly, it adopts TSVF mechanism, which well matches the post-confirmation of our QSA protocol design.

The characters in our scheme are defined as follows:

(1) Alice: Alice is the auctioneer.

(2) Bob$_i$: Bob$_i$ is the $i-th$ bidder. Suppose there are $t+1$ bidders in this auction protocol in total.

Note that in our scheme, the channel between the two bidders is authenticated by default, and the classical information is sent via broadcast.

The scheme has five steps as follows:

3.1 Initialization phase

After bidders have signed up, the initialization phase begins.

(1) Share secret key: Alice shares secret key K_i with each bidder Bob$_i$ through quantum key distribution.

(2) State preparation: Each bidder Bob$_i$ prepares t copies EPR pairs $|\Phi_i\rangle = |\Phi_i^1\rangle, \ldots, |\Phi_i^t\rangle$, where every pair is in the same state as

$$|\Phi_i^j\rangle = \frac{1}{\sqrt{2}}(|0_{X_{i_j}} 0_{Y_{i_j}}\rangle + |1_{X_{i_j}} 1_{Y_{i_j}}\rangle), \tag{1}$$

where i is the index of the bidder (i.e., corresponding to Bob$_i$), $j=1,\ldots,t$, X_{i_j} is the subscript which stands for the first particle in $|\Phi_i^j\rangle$ and Y_{i_j} is the subscript which stands for the second particle in $|\Phi_i^j\rangle$.

(3) State distribution: For each EPR state $|\Phi_i^j\rangle$, Bob$_i$ keeps the second particle Y_{i_j} and transmits the first particle X_{i_j} to other bidders Bob$_j$ in sequence separately, where $j=1,\ldots,t$.

3.2 Tender preparation phase

In the next stage of the introduction, we will change the protagonist of the story description from the role of the sender of the quantum states to the role of the receiver of the quantum states, although they are the same one. Hence, for convenience and clarity, we choose another subscript k to represent either bidder who received the particles.

(1) After receiving t particles, Bob_k randomly picks $t-n$ particles to form a new set O_k (Without loss of generality, we assume that $n<t$). The remaining ones form another set B_k.

(2) Bob_k does nothing to particles in O_k and measures the particles in B_k according to his bid $m_k = \{m_{k-1}, \ldots, m_{k-n}\}$. Concretely, Bob_k performs the following operations

$$\begin{cases} \text{measurement of } \sigma_Z, \ \text{if } m_{k_j} = 0, \ \text{ and } \ 1 \le j \le n \\ \text{measurement of } \sigma_X, \ \text{if } m_{k_j} = 1, \ \text{ and } \ 1 \le j \le n \end{cases} \tag{2}$$

(3) Bob_k records the measurement result $R_k = \{r_{k_1}, \ldots, r_{k_n}\}$, and obtain a new sequence

$$M_k = \{m_{k_1} \| r_{k_1}, \ldots, m_{k_n} \| r_{k_n}\}. \tag{3}$$

3.3 Tender delivery phase

(1) Bob_k encrypts M_k with K_k as following and send M'_k to the auctioneer.

$$M'_k = \{K_{k_1} \oplus m_{k_1} \| K_{k_2} \oplus r_{k_1}, \ldots, K_{k_{2n-1}} \oplus m_{k_n} \| K_{k_{2n}} \oplus r_{k_n}\}. \tag{4}$$

(2) Bob_k returns the measured particles by original route to whose sender separately. Consequently, every bidder holds t pairs of particles $|\phi_k\rangle$ again. Note that $|\phi_k\rangle$ is diffrent from $|\Phi_k\rangle$.

3.4 Bid opening phase

The auctioneer decrypts M'_k, where $j = 1, \ldots, t+1$ and obtains $t+1$ bids. Then the winner Bob^* and M^* will be announced.

3.5 Verify phase

(1) Each bidder Bob_i selects the corresponding state $|\phi_i^*\rangle$ from the sequence of particles in his hand.
(2) The winner Bob^* announces where the particles in the set O^* come from.
(3) According to O^*, Bob_i measures with different measurement basis.

(i) If $|\phi_i^*\rangle$ does not belong to the set O^*, Bob_i measures the observable D, which has four nondegenerate eigenstates as following

$$\begin{aligned}
|\Psi_1\rangle &= \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{2}(e^{i\frac{\pi}{4}}|01\rangle + e^{-i\frac{\pi}{4}}|10\rangle),\\
|\Psi_2\rangle &= \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{2}(e^{i\frac{\pi}{4}}|01\rangle + e^{-i\frac{\pi}{4}}|10\rangle),\\
|\Psi_3\rangle &= \frac{1}{\sqrt{2}}|11\rangle + \frac{1}{2}(e^{i\frac{\pi}{4}}|10\rangle + e^{-i\frac{\pi}{4}}|01\rangle),\\
|\Psi_4\rangle &= \frac{1}{\sqrt{2}}|11\rangle - \frac{1}{2}(e^{i\frac{\pi}{4}}|10\rangle + e^{-i\frac{\pi}{4}}|01\rangle),
\end{aligned} \tag{5}$$

Bob_i verifies based on the matching relationship between M^* and the measurement result. If the following table is met, the verification passes. Otherwise, verification fails (Table 2).

Table 2 The correspondence between M^* and measurement results

Measurement	M^*1
$\|\Psi_1\rangle$ or $\|\Psi_2\rangle$	00
$\|\Psi_3\rangle$ or $\|\Psi_4\rangle$	01
$\|\Psi_1\rangle$ or $\|\Psi_3\rangle$	10
$\|\Psi_2\rangle$ or $\|\Psi_4\rangle$	11

The first bit of M^* is the corresponding bit of bid, and the second one is the measurement

(ii) If $|\phi_i^*\rangle$ belongs to the set O^*, that is winner did not encode bid on his particle, Bob_i performs Bell measurement, which has four eigenstates as follows

$$\begin{aligned}
|\Psi_1\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),\\
|\Psi_2\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle),\\
|\Psi_3\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle),\\
|\Psi_4\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle),
\end{aligned} \tag{6}$$

Bob_i verifies based on the measurement result. If the measurement result is $|\Psi_1\rangle$, the verification passes. Otherwise, verification fails.

To more clearly express our solution, we give a concrete example to visualize the protocol in Fig. 1. In our example, we chose a situation where there were three bidders. Alice is the auctioneer and Bob_i is the bidder. Figure 1 shows the five important stages of our protocol, in which (a) shows each bidder prepares 2 EPR pairs in the initial stage; (b) shows each bidder distributes X particles to other participants in the initial stage; (c) describes each bidder measures the received particles in accordance with the protocol at the tender preparation stage and tender delivery stage and then sends the bid price to the auctioneer Alice secretly. (d) describes that each bidder receives his or her distributed particles and the auctioneer announces the winning information for the tender delivery stage and bid opening stage.

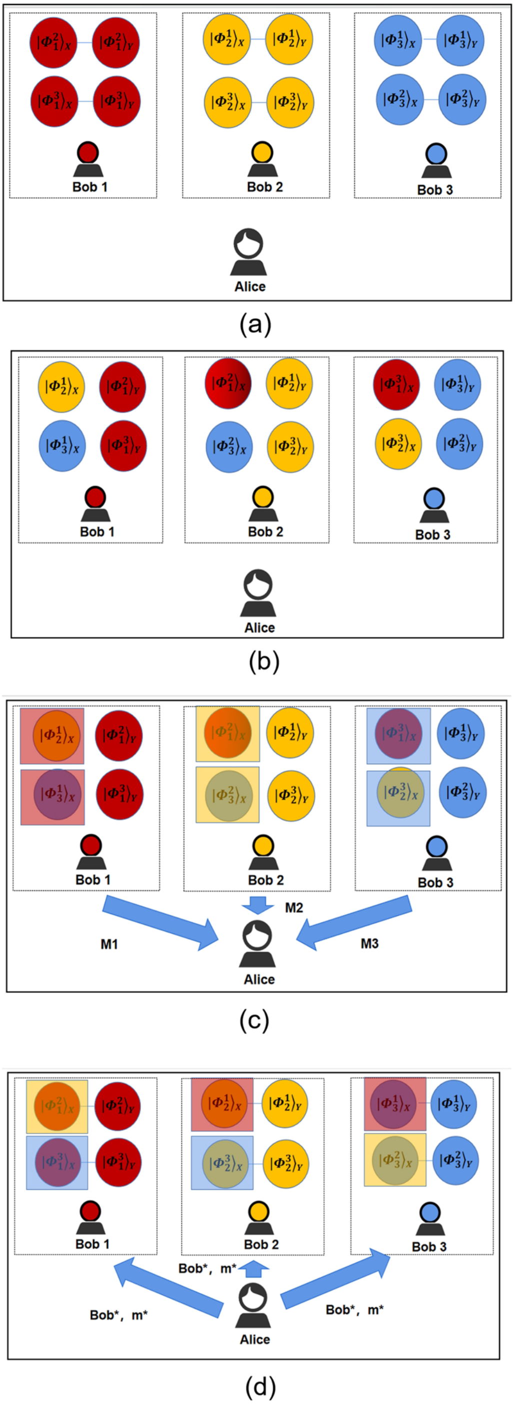
4 Analysis

A good sealed-bid auction protocol needs to meet not only the application requirements but also the security requirements. Next, we analyze the security of the above protocol.

4.1 Resist collusion attacks

Before analyzing the security of the scheme, let's clarify some assumptions of the protocol again for the convenience of subsequent analysis. Here, we assume that

Fig. 1 This is an example demonstration of the main steps of QSA with post confirmation based on SHWL blind signature **a** the second step in the initial phase; **b** The third step in the initial phase; **c** the tender preparation phase and tender delivery phase; **d** the tender delivery phase and bid opening phase


$|\Phi_1^2\rangle_X$ $|\Phi_1^2\rangle_Y$ $|\Phi_1^3\rangle_X$ $|\Phi_1^3\rangle_Y$
Bob 1
$|\Phi_2^1\rangle_X$ $|\Phi_2^1\rangle_Y$ $|\Phi_2^3\rangle_X$ $|\Phi_2^3\rangle_Y$
Bob 2
$|\Phi_3^1\rangle_X$ $|\Phi_3^1\rangle_Y$ $|\Phi_3^2\rangle_X$ $|\Phi_3^2\rangle_Y$
Bob 3
Alice
(a)
$|\Phi_2^1\rangle_X$ $|\Phi_1^2\rangle_Y$ $|\Phi_3^1\rangle_X$ $|\Phi_1^3\rangle_Y$
Bob 1
$|\Phi_1^2\rangle_X$ $|\Phi_2^1\rangle_Y$ $|\Phi_3^2\rangle_X$ $|\Phi_2^3\rangle_Y$
Bob 2
$|\Phi_1^3\rangle_X$ $|\Phi_3^1\rangle_Y$ $|\Phi_2^3\rangle_X$ $|\Phi_3^2\rangle_Y$
Bob 3
Alice
(b)
$|\Phi_2^1\rangle_X$ $|\Phi_1^2\rangle_Y$ $|\Phi_3^1\rangle_X$ $|\Phi_1^3\rangle_Y$
Bob 1
$|\Phi_1^2\rangle_X$ $|\Phi_2^1\rangle_Y$ $|\Phi_3^2\rangle_X$ $|\Phi_2^3\rangle_Y$
Bob 2
$|\Phi_1^3\rangle_X$ $|\Phi_3^1\rangle_Y$ $|\Phi_2^3\rangle_X$ $|\Phi_3^2\rangle_Y$
Bob 3
M2
M1
M3
Alice
(c)
$|\Phi_1^2\rangle_X$ $|\Phi_1^2\rangle_Y$ $|\Phi_1^3\rangle_X$ $|\Phi_1^3\rangle_Y$
Bob 1
$|\Phi_2^1\rangle_X$ $|\Phi_2^1\rangle_Y$ $|\Phi_2^3\rangle_X$ $|\Phi_2^3\rangle_Y$
Bob 2
$|\Phi_3^1\rangle_X$ $|\Phi_3^1\rangle_Y$ $|\Phi_3^2\rangle_X$ $|\Phi_3^2\rangle_Y$
Bob 3
Bob*, m*
Bob*, m*
Bob*, m*
Alice
(d)

all bidders send information to each other over an authenticated channel (whether sending quantum information or classical information). Moreover, we assume that the auctioneer is usually honest. Therefore, in the following security analysis, we mainly consider two cases, the first is that the auctioneer is absolutely honest, that is, the auctioneer will not collude with any bidder during the whole process. The second is that the auctioneer will only be absolutely honest until the tender closes. In the following, we will analyze the security of the scheme under two different honesty supposes.

(i) Case 1: The auctioneer is absolutely honest. Under this assumption, people are usually more concerned about whether two or more malicious bidders can collude to know a bidder's bid in advance, and then the malicious bidder can adjust his bid in time, and finally win with a rather small price advantage. Thus, in this case, any u bidders can conspire to obtain the bid information of someone else (let's say Bob_k). Since there is no way for bidders to know which measurement bases Bob_k selected, there is no additional attack advantage if the malicious auctioneer chooses to send a single particle or uses another entangled state instead of $\frac{1}{\sqrt{2}}|00\rangle + |11\rangle$. Because the case of only one malicious bidder is a special case of case 1. It is not more aggressive than case 1. So we ignore the case of only one malicious bidder.

(ii) Case 2: The auctioneer will only be absolutely honest until the tender is closed. That is, after the bidding is finished, a dishonest bidder may immediately find the auctioneer to launch a conspiracy to cheat and want the auctioneer to declare his own victory. In order to prevent such attacks, our scheme adopts a post-confirmation approach to ensure the fairness of the auction agreement. After the winner and bid are announced by the auctioneer, the winner Bob^* will publicly announce O^*. If O^* is fake, then it can be detected by Bell measurements. If m^* is tampered with, then other bidders can detect it based on their measurements of D. Besides, the quantum states used to encode the bid are prepared jointly by all bidders, and $|\Phi_i\rangle$ always has a particle in Bob_i's hand throughout the execution of the protocol.

4.2 Privacy

Our program supports the confidentiality of bidding information for non-winning bidders. That is, any bid of a non-winning bidder is completely confidential, that is, no one except himself and the auctioneer knows any bid information of a non-winning bidder. Because each bidder in 3.2 (1) randomly selected particles by themselves as the encoded carrier of the bid information. If the bidder does not win, he will not disclose how he selected the particle. Since it is not known which particles are the chosen coding particles, it is impossible to get his bid even if other bidders launch a collusive attack. What we need to note here is that in this case, we assume that the auctioneer is honest, that is, the auctioneer will not voluntarily disclose the bid price of other non-winning bidders.

5 The enhanced schemes

In this part, we give three enhanced versions of QSA protocols in Sect. 3, which is to further protect against malicious bidder attacks. To avoid repetition, we only give the different steps here, and the other steps that are not described are the same as the original scheme in Sect. 3.

5.1 The first enhanced version

This version is designed to defeat Trojan Horse attacks and fake photon attacks without using any additional hardware similar to [43].

5.1.1 Initialization phase

(2′) State preparation: Each bidder Bob$_i$ prepares $2t$ copies EPR pairs $|\Phi_i\rangle = |\Phi_i^1\rangle, \ldots, |\Phi_i^t\rangle$, where every pair is in the same state as

$$|\Phi_i^j\rangle = \frac{1}{\sqrt{2}}(|0_{X_{i_j}} 0_{Y_{i_j}}\rangle + |1_{X_{i_j}} 1_{Y_{i_j}}\rangle), \tag{7}$$

where i is the index of the bidder (i.e., corresponding to Bob$_i$), $j = 1, \ldots, 2t$, X_{i_j} is the subscript which stands for the first particle in $|\Phi_i^j\rangle$ and Y_{i_j} is the subscript which stands for the second particle in $|\Phi_i^j\rangle$.

(3’) State distribution: For each EPR state $|\Phi_i^j\rangle$, Bob$_i$ keeps the second particle Y_{i_j} and transmits particles X_{i_k} and $X_{i_{t+k}}$ to other bidders Bob$_k$ in sequence separately, where $k = 1, \ldots, t$.

5.1.2 Tender preparation phase

(1′) After receiving X_{i_k} and $X_{i_{t+k}}$ from Bob_i, Bob_k randomly flip a coin to generate a random bit b. If $b = 0$, Bob_k chooses X_{i_k} as the encoded state to encode his bid and $X_{i_{t+k}}$ as decoy state to check. If $b = 1$, Bob_k chooses $X_{i_{t+k}}$ as the encoded state to encode his bid and X_{i_k} as decoy state to check.

(2’) Bob_k randomly measure the decoy particle with X basis or Z basis and record his choices. Then Bob_k announces the location of the decoy state and measurement basis he chooses. The tested bidder uses the same basis to measure the other particle of the corresponding EPR pair in his hand and informs Bob_k of the measurement results.

If the measurement result is the same as Bob_k’s, Bob_k believes that the other bidders did honestly prepare the EPR pairs as required by the protocol. If the result is different, Bob stops the protocol.

5.2 The second enhanced version

This version is designed to prevent malicious bidders from stealing others’ bidding information before bids are opened.

5.2.1 Initialization phase

(2″) State preparation: Each bidder Bob$_i$ prepares $2t$ copies EPR pairs $|\Phi_i\rangle = |\Phi_i^1\rangle, \ldots, |\Phi_i^t\rangle$, where every pair is in the same state as

$$|\Phi_i^j\rangle = \frac{1}{\sqrt{2}}(|0_{X_{i_j}} 0_{Y_{i_j}}\rangle + |1_{X_{i_j}} 1_{Y_{i_j}}\rangle), \tag{8}$$

where i is the index of the bidder (i.e., corresponding to Bob$_i$), $j = 1, \cdots, 2t$, X_{i_j} is the subscript which stands for the first particle in $|\Phi_i^j\rangle$ and Y_{i_j} is the subscript which stands for the second particle in $|\Phi_i^j\rangle$.

(3″) State distribution: For each EPR state $|\Phi_i^j\rangle$, Bob$_i$ keeps the second particle Y_{i_j} and transmits particles X_{i_k} and $X_{i_{t+k}}$ to other bidders Bob$_k$ in sequence separately, where $k = 1, \cdots, t$.

5.2.2 Tender preparation phase

(1″) After receiving X_{i_k} and $X_{i_{t+k}}$ from Bob_i, Bob_k randomly flip a coin to generate a random bit b. If $b = 0$, Bob_k chooses X_{i_k} as the encoded state to encode his bid and $X_{i_{t+k}}$ as decoy state to check. If $b = 1$, Bob_k chooses $X_{i_{t+k}}$ as the encoded state to encode his bid and X_{i_k} as decoy state to check.

(2″) Bob_k randomly does one of these four operations X, Z, $X \otimes Z$ and I on decoy particles and record his choices. For the encoded particles, B_k measures them in according to his bid $m_k = \{m_{k-1}, \cdots, m_{k-n}\}$. Concretely, Bob_k performs the following operations

$$\begin{cases} \text{measurement of } \sigma_Z, & \text{if } m_{k_j} = 0, \text{ and } 1 \le j \le n \\ \text{measurement of } \sigma_X, & \text{if } m_{k_j} = 1, \text{ and } 1 \le j \le n \end{cases} \tag{9}$$

5.2.3 Verify phase

(1″) The winner $Bob*$ announces which states are decoys and where the particles in the set $O*$ originate.

(4″) Each bidder Bob_i can announce the location of some decoy states for random testing. The chosen bidder performs Bell measurement on the corresponding particles and then informs Bob_i of the measurement results. Bob_i compares the result of the measurement with the operation he took earlier. If the corresponding relationship in the following Table 3 is fulfilled, the detection is passed; if it is not met, the bidder maliciously stole the information prior to the bid opening.

5.3 The third enhanced version

This version is a combination of the above two enhancement ones, which can detect whether bidders are transmitting EPR pairs honestly or through measuring to steal bidding information before opening bids.

Table 3 The relationship between Bell measurement results and selection operations

Selection operations	Measurement
I	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$
X	$\frac{1}{\sqrt{2}}(\|01\rangle + \|10\rangle)$
Z	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$
$X \otimes Z$	$\frac{1}{\sqrt{2}}(\|01\rangle - \|10\rangle)$

5.3.1 Initialization phase

Due to the content of this part as the same as Sect. 5.1.1, it will not be repeated here.

5.3.2 Tender preparation phase

(1$''$) After receiving X_{i_k} and $X_{i_{t+k}}$ from Bob_i, Bob_k randomly generates a random bit b. If $b = 0$, Bob_k chooses X_{i_k} as the encoded state to encode his bid and $X_{i_{t+k}}$ as decoy state to check. If $b = 1$, Bob_k chooses $X_{i_{t+k}}$ as the encoded state to encode his bid and X_{i_k} as decoy state to check.

(2$'''$) Bob_k randomly measures the decoy particle with X basis or Z basis. If X basis was chosen, Bob_k randomly does Z or I; If Z basis was chosen, Bob_k randomly does X or I and record his choices. For the encoded particles, B_k measures them in according to his bid $m_k = \{m_{k-1}, \cdots, m_{k-n}\}$. Concretely, Bob_k performs the following operations

$$\begin{cases} \text{measurement of } \sigma_Z, & \text{if } \ m_{k_j} = 0, \ \text{ and } \ 1 \leq j \leq n \\ \text{measurement of } \sigma_X, & \text{if } \ m_{k_j} = 1, \ \text{ and } \ 1 \leq j \leq n \end{cases} \tag{10}$$

5.3.3 Verify phase

(1$''$) The winner Bob^* announces which are decoy states and where the particles in the set O^* come from.

(4$''$) Each bidder Bob_i can announce the location of some decoy states for random testing and measurement basis. The selected bidder performs the corresponding measurement on the corresponding particles and then reports the results to Bob_i. Bob_i compares the result of the measurement with the operation he took earlier. If the corresponding relationship in the following Table 4 is met, the detection is passed; if it is not met, it indicates that the bidder maliciously stole the information before the bid opening.

5.4 Comparison of different protocols

There are four schemes in the paper, among which the first scheme is QSA based on SHWL Blind signature, which aims at the situation that bidders have honestly

Table 4 The relationship between measurement basis, operations, and the measurement result

Measurement basis	Selection operations	Measurement of Bob_k	Measurement of Bob_i
X	I	$\|+\rangle$	$\|+\rangle$
X	I	$\|-\rangle$	$\|-\rangle$
X	Z	$\|+\rangle$	$\|-\rangle$
X	Z	$\|-\rangle$	$\|+\rangle$
Z	I	$\|0\rangle$	$\|0\rangle$
Z	I	$\|1\rangle$	$\|1\rangle$
Z	X	$\|1\rangle$	$\|0\rangle$
Z	X	$\|0\rangle$	$\|1\rangle$

prepared and sent EPR pairs, and a total of t EPR pairs are used in the entire agreement. Compared to the latter three enhanced versions of the protocol, there are no additional measurements and operations, so it is the one that uses the least quantum resources of the four protocols.

The first enhanced version is for the enemy may launch Trojan attacks and false photon attacks. the scheme uses 2t EPR pairs. The receiver can randomly select t particles as the decoy state, and then randomly make a single-particle measurement of the decoy state particles in their hands, after informing the sender of the selected measurement basis, Then let the sender publish the measurement results of the particles left in the hands of the sender, and detect whether there is Trojan attack and false photon attack by comparing whether the measurement results are consistent. Compared to QSA, which is based on SHWL Blind signature, this protocol increases the security to some extent, but doubles the use of EPR pairs and requires additional single-particle measurements.

The second enhanced version deals with cases where other bidders secretly steal information about other bidders before the auction is announced. The scheme uses $2t$ EPR pairs. The bidder also randomly selects t particles as the decoy state, and then randomly performs a single-particle operation on the decoy state particles in his hand, and then sends the particles to the other party, so that the sender can do Bell measurement so according to the measurement results, it can determine whether other bidders have stolen bidding information by measuring in advance. Compared with QSA based on SHWL Blind signature, this protocol also increases the security to a certain extent like the above protocol, using $2t$ EPR pairs. The difference is that it requires the sender to use Bell measurement instead of single-particle measurement.

The third enhanced version, which is a synthesis of the two scenarios above, addresses whether other bidders are honestly sending EPR pairs, or are secretly stealing bids from other bidders before the auction is announced. The scheme uses $2t$ EPR pairs. The bidder also randomly selects t particles as the decoy state, and then randomly performs single-particle measurement on the decoy state particles in his hand, and then performs single-particle operation according to the selected measurement basis. After informing the sender of the selected measurement basis, the sender then asks the sender to publish the measurement results of the particles left in the

Table 5 Security comparison of different protocols

Schemes	Post-confirmation for validity	Defeat Trojan Horse and fake photon attacks	Prevent stealing bid information
QSA in Sect. 3	✓	×	×
The first enhanced version	✓	✓	×
The second enhanced version	✓	×	✓
The third enhanced version	✓	✓	✓

Table 6 Quantum resource consumption comparison of different protocols

Schemes	Number of EPR pairs	Extra single particle measure	Extra Bell measure	Extra quantum operation
QSA in Sect. 3	t	–	–	–
The first enhanced version	$2t$	✓	–	–
The second enhanced version	$2t$	–	✓	✓
The third enhanced version	$2t$	✓	–	✓

corresponding position in the sender's hand. Finally, by comparing the measurement results, we can judge whether other bidders have dishonest behavior. This protocol is the most secure of the four protocols, but it also consumes more resources, and it requires additional single-particle operations and single-particle measurements by the bidder, as well as single-particle measurements by the sender.

The security indicators of these four different protocols are compared in Table 5, and the required quantum resources are compared in Table 6.

6 Discussion

The auctioneer in the above protocol is classical and does not necessarily have the ability to prepare or measure or manipulate quantum states. It is noted that the auctioneer in the above protocol can also be the quantum version, that is, Bob_k could send encrypted states to the auctioneer. For example, Bob_k prepares single particles according to the shared key K_k and his bid m_k. If the $K_{k_j} = 0$, $m_{k_j} = 0$, Bob_k prepare $|0\rangle$. If the $K_{k_j} = 0$, $m_{k_j} = 1$, Bob_k prepare $|1\rangle$. If the $K_{k_j} = 1$, $m_{k_j} = 0$, Bob_k prepare $|+\rangle$. If the $K_{k_j} = 1$, $m_{k_j} = 1$, Bob_k prepare $|-\rangle$. Bob_k, of course, also can use entangled states, like Bell states, GHZ states, and so on. In addition, Bob_k could choose other ways to send his bid either, such as the quantum secure direct communication protocol.

Compared with other protocols, this one is more efficient. Regardless of the shared key K_i through QKD between Bob_i and the auctioneer, the entire protocol requires a total of $t(t+1)$ EPR pairs. In addition, instead of a multi-bidders collaboration for global measurements, each bidder only takes local measurements. In our protocol, the utilization of particles is very high, no matter which base Bob_k chooses, every particle contributes for verification.

It should be noted that the protocol proposed in Sect. 3 is considered in an ideal situation, that is, there are no problems such as multi-photon and quantum detector defect. In practical applications, we can achieve the ideal state of safety by using additional components, such as a wavelength filter and a photon number splitter. The usual practice is to add a wavelength filter and a photon number splitter in front of the device before measurement, and then make measurements to defeat IPE attacks and delay photon attacks [44, 45]. Wavelength filters can be used to filter out non-specific wavelengths of photons, limiting the attacker's measurement at a specific wavelength, photon number splitters are used to segment photons into different output channels to achieve the separation of single-photon states and multi-photon states, thereby improving the security of the system. If it is not convenient to use the device to protect against these attacks, we also present three different enhanced protocols in Sect. 5.

7 Conclusion

In this paper, we have made a first attempt to design a quantum sealed-bid protocol with post-confirmation based on a quantum blind signature scheme, which uses two-state vector formalism. The discovery that TSVF is yet another useful tool for implementing post confirmation of the QSA protocol is another interesting aspect of this paper. After analysis, our protocol is efficient and secure, which is publicly verifiable by other bidders, and resistant to malicious attacks and collusion attacks. Moreover, we consider three different enhancement versions to further guard against the dishonest behavior of malicious bidders.

This work broadens the way we think about designing QSA with post confirmation protocols. It also provides an interesting example of how different protocols can be used to implement each other's functions. Hopefully, our approach will inspire more research. Of course, there are still many aspects worth paying attention to, such as how to further improve efficiency, including optimizing the use of decoy states. Besides, the issue of reducing bidders' quantum requirements is also worth considering so that more bidders can participate in the auction without too many hardware constraints.

Acknowledgements This work was supported in part by the National Key R&D Program of China (No. 2021YFB2700600); in part by Hainan Province Science and Technology Special Fund (No. GHYF2022010); in part by the Finance Science and Technology Project of Hainan Province (No. ZDKJ2020009); in part by the National Natural Science Foundation of China (No. 62163011); in part by the Research Startup Fund of Hainan University under Grant KYQD(ZR)-22098 and KYQD(ZR)-21071.

Data availability All data generated or analyzed during this study are included in this article.

Declarations

Conflict of interest We declare that we have no conflict of interest.

Appendix A: Two-state vector formalism

Two-state vector formalism (TSVF) presented by [40] which is used to completely describe the state of now system at time t. That is, there needs two complete measurements, one before time t and one after time t. More details on this section can be found in Reference [40, 41]. The following is a brief description of the main content extracted from the above literature, so as to better understand the QSA scheme with post-confirmation proposed by us later. Specifically, at the time $t_1 < t$, if we measure the observable A_1 of the system and get the measurement result $A_1 = a$, produces a corresponding quantum state $|a\rangle$. Then, at time t, a system in the current state $|\psi_{t_1}\rangle$, which is called a forward-evolving state, can be obtained by Hamiltonian evolution H from $|a\rangle$, i.e

$$|\psi_{t_1}\rangle = U(t, t_1)|a\rangle = e^{-i\int_{t_1}^{t} Hdt}|a\rangle. \tag{A1}$$

Similarly, after that at time $t_2 > t$, if we measure the observable A_2 of the system and get the measurement result $A_2 = b$, produces a corresponding quantum state $|b\rangle$. Then, the desired state is reached by the backward time evolution from t_2 to t, which is called a backward-evolving state

$$|\psi_{t_2}\rangle = U(t, t_2)|b\rangle = e^{-i\int_{t_2}^{t} Hdt}|b\rangle. \tag{A2}$$

For the time t, where $t_1 < t < t_2$, we can describe the state of the system by two states vector formalism $\langle\psi_{t_2}||\psi_{t_1}\rangle$. Concretely, we can use the TSVF to predict the probability of each measurement between time t_1 and time t_2. The probability of measurements c_n by measuring the system by observable A_3 is

$$p(c_n) = \frac{|\langle\psi_{t_2}|P_{A_3=c_n}|\psi_{t_1}\rangle|^2}{\sum_j |\langle\psi_{t_2}|P_{A_3=c_j}|\psi_{t_1}\rangle|^2}, \tag{A3}$$

where $P_{A_3=c_j}$ is the projection operator corresponding to c_j.

References

1. Ch, H.B., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: International Conference on Computers, Systems and Signal Processing, Bangalore, India, vol. 175 (1984)
2. Zeng, P., Zhou, H., Wu, W., Ma, X.: Mode-pairing quantum key distribution. Nat. Commun. **13**(1), 3903 (2022)
3. Xie, Y.-M., Lu, Y.-S., Weng, C.-X., Cao, X.-Y., Jia, Z.-Y., Bao, Y., Wang, Y., Fu, Y., Yin, H.-L., Chen, Z.-B.: Breaking the rate-loss bound of quantum key distribution with asynchronous two-photon interference. PRX Quantum **3**(2), 020315 (2022)
4. Sheng, Y.-B., Zhou, L., Long, G.-L.: One-step quantum secure direct communication. Sci. Bull. **67**(4), 367–374 (2022)
5. Zhou, L., Xu, B.-W., Zhong, W., Sheng, Y.-B.: Device-independent quantum secure direct communication with single-photon sources. Phys. Rev. Appl. **19**(1), 014036 (2023)
6. Liu, B., Xia, S., Xiao, D., Huang, W., Xu, B., Li, Y.: Decoy-state method for quantum-key-distribution-based quantum private query. Sci. China Phys. Mech. Astron. **65**(4), 240312 (2022)

7. Piotrowski, E.W., Sładkowski, J.: Quantum auctions: facts and myths. Physica A **387**(15), 3949–3953 (2008)
8. Yin, H.-L., Fu, Y., Li, C.-L., Weng, C.-X., Li, B.-H., Gu, J., Lu, Y.-S., Huang, S., Chen, Z.-B.: Experimental quantum secure network with digital signatures and encryption. Natl. Sci. Rev. **10**(4), 228 (2023)
9. Li, C.-L., Fu, Y., Liu, W.-B., Xie, Y.-M., Li, B.-H., Zhou, M.-G., Yin, H.-L., Chen, Z.-B.: Breaking universal limitations on quantum conference key agreement without quantum memory. Commun. Phys. **6**(1), 122 (2023)
10. Shen, A., Cao, X.-Y., Wang, Y., Fu, Y., Gu, J., Liu, W.-B., Weng, C.-X., Yin, H.-L., Chen, Z.-B.: Experimental quantum secret sharing based on phase encoding of coherent states. Sci. China Phys. Mech. Astron. **66**(6), 260311 (2023)
11. Zhou, L., Lin, J., Xie, Y.-M., Lu, Y.-S., Jing, Y., Yin, H.-L., Yuan, Z.: Experimental quantum communication overcomes the rate-loss limit without global phase tracking. Phys. Rev. Lett. **130**(25), 250801 (2023)
12. Shi, R.-H.: Quantum sealed-bid auction without a trusted third party. IEEE Trans. Circuits Syst. I Regul. Pap. **68**(10), 4221–4231 (2021)
13. Krishna, V.: Auction Theory. Academic Press, London (2009)
14. Naseri, M.: Secure quantum sealed-bid auction. Opt. Commun. **282**(9), 1939–1943 (2009)
15. Qin, S.-J., Gao, F., Wen, Q.-Y., Meng, L.-M., Zhu, F.-C.: Cryptanalysis and improvement of a secure quantum sealed-bid auction. Opt. Commun. **282**(19), 4014–4016 (2009)
16. Yang, Y.-G., Naseri, M., Wen, Q.-Y.: Improved secure quantum sealed-bid auction. Opt. Commun. **282**(20), 4167–4170 (2009)
17. Zhao, Z., Naseri, M., Zheng, Y.: Secure quantum sealed-bid auction with post-confirmation. Opt. Commun. **283**(16), 3194–3197 (2010)
18. He, L.-B., Huang, L.-S., Yang, W., Xu, R., Han, D.-Q.: Cryptanalysis and melioration of secure quantum sealed-bid auction with post-confirmation. Quantum Inf. Process. **11**, 1359–1369 (2012)
19. Wang, J.-T., Chen, X.-B., Xu, G., Meng, X.-H., Yang, Y.-X.: A new quantum sealed-bid auction protocol with secret order in post-confirmation. Quantum Inf. Process. **14**, 3899–3911 (2015)
20. Wang, Q., Shi, R.-H., Chen, Z.-K., Wang, S.-L.: A quantum sealed auction protocol based on secret sharing. Int. J. Theor. Phys. **58**, 1128–1137 (2019)
21. Wang, J.-T., Pan, Y., Liu, W., Li, Z.-Z.: Quantum sealed-bid auction protocol based on quantum secret sharing. Quantum Inf. Process. **21**(8), 278 (2022)
22. Wu, M., Shi, R.-H., Gao, W., Li, K.: A secure quantum sealed-bid auction protocol based on quantum public key encryption. Quantum Inf. Process. **21**(2), 77 (2022)
23. Sharma, R.D., Thapliyal, K., Pathak, A.: Quantum sealed-bid auction using a modified scheme for multiparty circular quantum key agreement. Quantum Inf. Process. **16**, 1–16 (2017)
24. Shi, R.-H., Zhang, M.: Privacy-preserving quantum sealed-bid auction based on Grover's search algorithm. Sci. Rep. **9**(1), 7626 (2019)
25. Gao, W., Shi, R.-H., Wu, M.: A privacy-preserving quantum sealed-bid auction protocol with epr pairs. Quantum Inf. Process. **21**, 1–15 (2022)
26. Shi, R.-H., Li, Y.-F.: A feasible quantum sealed-bid auction scheme without an auctioneer. IEEE Trans. Quantum Eng. **3**, 1–12 (2022)
27. Asagodu, P., Thapliyal, K., Pathak, A.: Quantum and semi-quantum sealed-bid auction: vulnerabilities and advantages. Quantum Inf. Process. **21**(5), 185 (2022)
28. Xu, Y., Li, Z., Wang, C., Zhu, H.: Quantum sealed-bid auction protocol for simultaneous ascending auction with ghz states. Quantum Inf. Process. **20**, 1–14 (2021)
29. Li, Z., Chen, L., Zhu, H.: Quantum sealed-bid Vickrey auction protocol with semi-quantum bidders. Int. J. Theor. Phys. **60**, 3760–3770 (2021)
30. Zhang, K.-J., Kwek, L.-C., Ma, C.-G., Zhang, L., Sun, H.-W.: Security analysis with improved design of post-confirmation mechanism for quantum sealed-bid auction with single photons. Quantum Inf. Process. **17**, 1–14 (2018)
31. Shi, R.-H., Zhang, R., Liu, B., Zhang, M.: Cryptanalysis and improvement of quantum sealed-bid auction. Int. J. Theor. Phys. **59**, 1917–1926 (2020)
32. Qi, S., Zheng, H., Qiaoyan, W., Wenmin, L.: Quantum blind signature based on two-state vector formalism. Opt. Commun. **283**(21), 4408–4410 (2010)
33. Chen, F.-L., Wang, Z.-H., Hu, Y.-M.: A new quantum blind signature scheme with bb84-state. Entropy **21**(4), 336 (2019)

34. Chaum, D.: Blind signatures for untraceable payments. In: Advances in Cryptology: Proceedings of Crypto, vol. 82, pp. 199–203. Springer (1983)
35. Wen, X., Niu, X., Ji, L., Tian, Y.: A weak blind signature scheme based on quantum cryptography. Opt. Commun. **282**(4), 666–669 (2009)
36. Khodambashi, S., Zakerolhosseini, A.: A sessional blind signature based on quantum cryptography. Quantum Inf. Process. **13**, 121–130 (2014)
37. Wang, M., Chen, X., Yang, Y.: A blind quantum signature protocol using the ghz states. Sci. China Phys. Mech. Astron. **56**, 1636–1641 (2013)
38. Xia, C., Li, H., Hu, J.: A semi-quantum blind signature protocol based on five-particle ghz state. Eur. Phys. J. Plus **136**(6), 633 (2021)
39. Yin, X.-R., Ma, W.-P., Liu, W.-Y.: A blind quantum signature scheme with χ-type entangled states. Int. J. Theor. Phys. **51**, 455–461 (2012)
40. Aharonov, Y., Vaidman, L.: The two-state vector formalism of quantum mechanics. In: Time in Quantum Mechanics, pp. 369–412 (2002)
41. Aharonov, Y., Vaidman, L.: The two-state vector formalism: an updated review. Time in quantum mechanics, pp. 399–447 (2008)
42. Bub, J.: Secure key distribution via pre-and postselected quantum states. Phys. Rev. A **63**(3), 032309 (2001)
43. Yang, C.-W., Hwang, T., Luo, Y.-P.: Enhancement on "quantum blind signature based on two-state vector formalism". Quantum Inf. Process. **12**, 109–117 (2013)
44. Deng, F.-G., Li, X.-H., Zhou, H.-Y., Zhang, Z.: Improving the security of multiparty quantum secret sharing against trojan horse attack. Phys. Rev. A **72**(4), 044302 (2005)
45. Deng, F.-G., Li, X.-H., Zhou, H.-Y., Zhang, Z.: Erratum: Improving the security of multiparty quantum secret sharing against trojan horse attack [phys. rev. a 72, 044302 (2005)]. Phys. Rev. A **73**(4), 049901 (2006)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.