IEEE Transactions on Quantum Engineering

Received June 4, 2021; accepted January 31, 2022; date of publication February 7, 2022; date of current version March 2, 2022.

Digital Object Identifier 10.1109/TQE.2022.3148664

A Feasible Quantum Sealed-Bid Auction Scheme Without an Auctioneer

RUN-HUA SHI AND YI-FEI LI

School of Control and Computer Engineering, North China Electric Power University, Beijing 102206, China

Corresponding author: Run-Hua Shi (e-mail: rhshi@ncepu.edu.cn).

This work was supported by the National Natural Science Foundation of China under Grant 61772001.

ABSTRACT In this article, we first define a primitive problem of secure multiparty computations, i.e., secure multiparty disjunction (SMD), and present a novel quantum protocol for SMD that can ensure information-theoretical security, i.e., unconditional security. Furthermore, based on the quantum SMD protocol, we design a quantum sealed-bid auction (QSA) scheme without an auctioneer. In the proposed QSA scheme, all bidders can jointly find the winning bidder without the help of an auctioneer while it can perfectly protect the privacy of nonwinning bidders. The proposed quantum SMD protocol and quantum QSA scheme take Bell states as quantum resources and only perform single-particle Pauli operators and two-particle Bell measurements. Finally, we simulate the related quantum protocols in Qiskit and verify the correctness and the feasibility of the proposed protocols.

INDEX TERMS Privacy preserving, quantum computing, quantum sealed-bid auction (QSA), secure multiparty computation.

I. INTRODUCTION

With the rapid development of the Internet, there appear various secure electronic protocols, e.g., electronic voting, electronic auction, and electronic payment, which play essential roles in modern society. In this article, we focus on electronic auction [1], [2]. Generally, an auction can be mainly classified into three categories [3]: Dutch auction, English auction, and sealed-bid auction. The traditional English auction is a public bid auction. There are many round bids during the bidding phase, and all bids are public, where each round bid is higher than the previous bids. If there is no competing bidder to challenge the current highest bid within a given time frame, the candidate bidder of the highest bid will become the winner, and accordingly, the goods or services will be sold at a price equal to the highest bid. The Dutch auction is somewhat similar to the traditional English auction, but it starts at the highest price, and the price gradually decreases round after round until the first bidder is willing to pay the price. Unlike the first two auctions, only the winning bidder and the highest bid in the sealed-bid auction are revealed, whereas the losing (i.e., nonwinning) bids are kept private. Conventionally, the sealed-bid auction [4] asks for the help of a trusted third party, called the auctioneer. First, all bidders seal their respective bids by encrypting or concealing technologies so that others except for the auctioneer do not know their bids. Second, all sealed bids are submitted simultaneously to the auctioneer instead of one after another. Finally, the auctioneer selects the highest bid among all submitted bids and announces the corresponding winner. In addition, to meet higher security requirements, there are still other security properties of the sealed-bid auction [5], e.g., anonymity, fairness, verifiability, and privacy.

Generally speaking, English auction and Dutch auction have high efficiencies but lack privacy protection, whereas sealed-bid auction has relatively low efficiency due to protecting the bids' privacy.

In classical settings, there are many sealed-bid auction protocols based on classical cryptographic technologies [5]–[9]. As we all know, the security of classical cryptography mainly depends on difficult mathematical problems. However, with the development of quantum computing [10], [11], classical cryptography will face enormous challenges, because well-known cryptographic algorithms (e.g., RSA) are vulnerable to attacks from quantum computers or fast quantum algorithms [12]. On the other hand, in order to solve these challenges, there appears quantum cryptography [13]. Its security only depends on the fundamental laws of quantum mechanics so that it can guarantee unconditional security in theory.

In quantum settings, the first quantum sealed-bid auction (QSA) protocol was proposed by Naseri [14] in 2009, which adopted a multiparty quantum secure direct communication

protocol. However, Qin *et al.* [15] and Yang *et al.* [16] independently pointed out that a dishonest bidder in the protocol could obtain all the other bidders' private bids without being found by performing different attacks. Accordingly, they improved the original protocol by adding checking procedures, respectively. Furthermore, Liu *et al.* [17] and Zheng and Zhao [18] presented different strategies to prevent similar attacks. Subsequently, Zhao *et al.* [19] found that these previously proposed protocols did not resist the collusion attack of the dishonest auctioneer and the malicious bidders. Consequently, they designed a postconfirmation mechanism to resist the collusion attack [19]. However, Xu *et al.* [20] and He *et al.* [21] claimed that a group of dishonest bidders in [19] could collude to obtain the other bidders' private bids with a high probability, and they further proposed different prevention strategies. Later, there appeared many sealed-bid auction protocols. Particularly, Wang *et al.* [22] again found the potential loophole of He *et al.*'s protocol [21] and presented an improved protocol that can tactfully defeat the collusion attack. Wang [23] designed a QSA protocol with a set of ordered EPR pairs. In 2014, Liu *et al.* [24] proposed a new QSA protocol with a postconfirmation mechanism to resist internal bidders' attacks. In 2015, Wang *et al.* [25] proposed another sealed-bid auction protocol with a secret order in postconfirmation to improve Zhao's protocol [19]. In 2016, Liu *et al.* [26] proposed a multiparty quantum auction protocol using the single photons as the message carrier of bids to reduce the complexity of quantum resources. But Liu *et al.*'s protocol [26] still required EPR pairs in postconfirmation and needed quantum memory to long-timely store these EPR pairs. In 2017, Sharma *et al.* [27] presented a novel collusion attack-free QSA protocol by dividing all bidders into disjoint subgroups, in which each bidder sends his bid to the auctioneer in a circular manner but he also needs to share his bid with the remaining bidders to achieve honesty. In 2018, Zhang *et al.* [28] presented a feasible QSA protocol based on single photons in both the polarization and the spatial-mode degrees of freedom, in which the postconfirmation mechanism uses single photons instead of entangled EPR pairs, and it does not require quantum memory. In 2019, Shi *et al.* [3] proposed a secure QSA protocol based on Grover's search algorithm to protect the privacy of nonwinning bidders (i.e., losing bidders). Recently, we presented anonymous QSA by introducing two noncolluding auctioneers to ensure that they could supervise each other [29]. In addition, there also appeared quantum English auction [30], quantum combinatorial auction [31], and other quantum auctions [32]–[34]. Therefore, quantum auctions are becoming an increasingly popular research topic.

However, all previously proposed QSA protocols only consider the trusted auctioneer. But it is hard to find a fully trusted third party in the real world. Accordingly, a dishonest auctioneer might disclose the losing bids to anyone, including other bidders, since the real evaluation of the auction item is often considered a commercial secret. That is, each bid as a secret should be unknown to even the auctioneer. Therefore, these previously proposed QSA protocols do not meet the higher security requirements, because the nonwinning bidders lack privacy protection, which has been the focus of everyone's attention in modern society.

Furthermore, some existing QSA protocols are unfair, e.g., a malicious bidder could collude with the dishonest auctioneer to perform a collusion attack to win the auction unfairly. If we can remove the auctioneer from a sealed-bid auction scheme, the scheme will become more secure and robust. Of course, it seems challenging to design a sealed-bid auction scheme without an auctioneer, since there has always been no practical and feasible solution even in classical settings. Until recently, Bag *et al.* proposed the first auctioneer-free sealed-bid auction scheme [35], in which all bidders jointly compute the maximum bid bit-by-bit by using classical cryptographic technology, i.e., each bit applying the two-round classical anonymous veto protocol. Accordingly, it has a linear computation and communication complexity $O(c)$, c being the bit length of the bid price. It is equivalent to all bidders performing private comparisons in bit-by-bit ways. However, it is infeasible or impractical to implement $O(c)$ private multiparty comparisons when there are many bidders, i.e., the number of bidders is enormous. In addition, the proposed protocol in [27] can be modified and performed without an auctioneer theoretically. However, this protocol cannot protect the anonymity and the privacy of the bidders, because the bid of each bidder will be known to many other bidders. To our best knowledge, there is not a QSA protocol without an auctioneer but it can ensure the privacy of all other bids except the highest bid. In fact, to design secure protocols without any trusted third party is increasingly becoming the focus of research in fields of secure multiparty computations.

On the other hand, like quantum key distribution, the feasibility of QSA protocols is the focus of research. However, there are two intractable issues to implement many existing QSA protocols: one is that it is difficult to implement the complicated oracle operators and measurements in high-dimensional Hilbert space and the other is that it is hard to find a fully trusted third party in the real world. Based on these considerations, we first present a practical and feasible QSA scheme without any auctioneer in this article. The proposed scheme not only guarantees the correctness and fairness of the auction but also perfectly ensures the privacy of the nonwinning (i.e., losing) bidders. Compared with the current existing QSA, our proposed scheme can provide more robust privacy protections, which are just urgent requirements in the modern network society. Furthermore, it is feasible to implement this scheme with Bell states and Bell measurements.

Our contributions in this article are summarized as follows.

1) We define a primitive problem of secure multiparty computations, i.e., secure multiparty disjunction (SMD), and present a novel quantum protocol for

IEEE Transactions on Quantum Engineering

SMD, which can ensure the information-theoretical security, i.e., the unconditional security.

2) We design a QSA scheme without an auctioneer. In the proposed QSA scheme, all bidders can jointly find the winning bidder without the help of an auctioneer while it can perfectly protect the privacy of nonwinning bidders, i.e., it cannot reveal any private information about the private bids of nonwinning bidders.
3) Proposed quantum SMD protocol and quantum QSA scheme take Bell states as quantum resources, and only perform single-particle Pauli operators and two-particle Bell measurements. So, it is feasible to implement them with present quantum processing technologies.
4) Finally, we simulate the related quantum protocols in Qiskit and verify the correctness and the feasibility of the proposed protocols.

II. PRELIMINARIES

Entanglement is an essential resource for quantum computation and quantum communication. Bell state is the most widely used among various entangled states, which is a maximally entangled two-particle state in two-dimensional Hilbert space as follows [36]:

$$|\phi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{1}$$

$$|\phi_{01}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{2}$$

$$|\phi_{10}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \tag{3}$$

$$|\phi_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \tag{4}$$

From (1)–(4), we can see that any Bell state $|\phi_{ij}\rangle$ can be described as the following general form:

$$|\phi_{ij}\rangle = \frac{1}{\sqrt{2}}(|0i\rangle + (-1)^j|1\bar{i}\rangle) \tag{5}$$

where $i, j \in \{0, 1\}$ and $\bar{i} = 1 \oplus i$ (i.e., a logical NOT). Furthermore, four Pauli operators can be written as follows:

$$U_{00} = I = |0\rangle\langle 0| + |1\rangle\langle 1| \tag{6}$$

$$U_{01} = \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1| \tag{7}$$

$$U_{10} = \sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0| \tag{8}$$

$$U_{11} = i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|. \tag{9}$$

In the following sections, $|\phi_{ij}\rangle_{12}$ denotes the Bell state of two particles 1 and 2, i.e., the subscripts 1 and 2 denote two particles. Accordingly, the subscript ij has four possible combinations corresponding to four different Bell states, which can be regarded as the feature of the Bell state $|\phi_{ij}\rangle_{12}$. Similarly, pq is also regarded as the feature of the Pauli operator U_{pq}, where $p, q \in \{0, 1\}$.

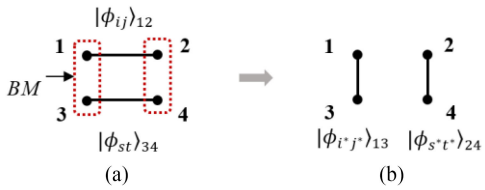


FIGURE 1. Entanglement swapping of Bell states. The solid line denotes the entanglement between the two particles. The red dashed box denotes Bell measurement. (a) Before measuring. (b) After measuring.

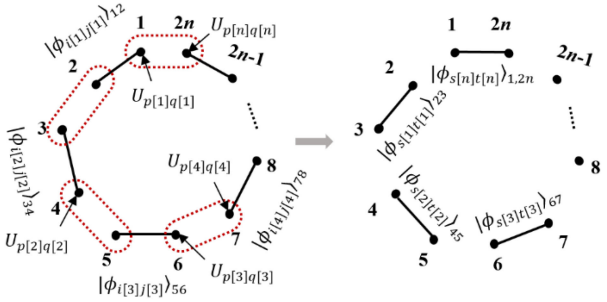


FIGURE 2. Entanglement swapping of *n* Bell states.

Theorem 1 (See [36]): For any two Bell states $|\phi_{ij}\rangle_{12}$ and $|\phi_{st}\rangle_{34}$, after performing Bell basis measurements on the particles 1 and 3, and the particles 2 and 4, respectively (see Fig. 1), the possible measured results $|\phi_{i^*j^*}\rangle_{13}$ and $|\phi_{s^*t^*}\rangle_{24}$ always satisfy the following property:

$$i^*j^* \oplus s^*t^* = ij \oplus st \tag{10}$$

where $\oplus$ denotes bitwise XOR. That is, the parity of the features of Bell states does not change after entanglement swapping.

Theorem 2 (See [36]): After applying any Pauli operator U_{pq} (i.e., $p, q \in_R \{0, 1\}$) to any particle of arbitrary Bell state $|\phi_{ij}\rangle_{12}$, the transformed state $|\phi_{i^*j^*}\rangle_{12}$ of the particles 1 and 2 always satisfies the following property:

$$i^*j^* = pq \oplus ij. \tag{11}$$

From Theorems 1 and 2, it can easily generalize the following Theorem 3.

Theorem 3 (See [36]): For any n EPR pairs $(1, 2)$, $(3, 4)$, …, $(2x - 1, 2x)$, …, $(2n - 1, 2n)$, which are initially in Bell states $|\phi_{i[1]j[1]}\rangle_{12}$, $|\phi_{i[2]j[2]}\rangle_{34}$, …, $|\phi_{i[x]j[x]}\rangle_{2x-1,2x}$, …, $|\phi_{i[n]j[n]}\rangle_{2n-1,2n}$, respectively, if we apply any Pauli operator $U_{p[x]q[x]}$ to any particle (i.e., $2x - 1$ or $2x$) of the xth EPR pair $(2x - 1, 2x)$ for x=1, 2, …, n and further measure the particle pair $(2x, 2x + 1)$ in Bell basis for x=1, 2, …, n (see Fig. 2), then the possible measured results $(|\phi_{s[x]t[x]}\rangle_{2x,2x+1}$ for $x = 1, 2, \ldots, n)$ should meet the following equation:

$$\begin{aligned} &s[1]t[1] \oplus s[2]t[2] \oplus \ldots s[n]t[n] \\ &= \{i[1]j[1] \oplus i[2]j[2] \oplus \ldots i[n]j[n]\} \\ &\quad \oplus \{p[1]q[1] \oplus p[2]q[2] \oplus \ldots p[n]q[n]\} \end{aligned}$$

$$\oplus_{x=1}^{n} s[x]\,t[x] = \{\oplus_{x=1}^{n} i[x]\,j[x]\} \oplus \left\{\oplus_{x=1}^{n} p[x]\,q[x]\right\}. \tag{12}$$

More generally, for any n Bell states, if we perform an arbitrary number of Pauli operators on any particles of these Bell states and randomly measure any two particles, then the parity of the features of the finally measured Bell states is entirely determined by that of all initial Bell states and all performed Pauli operators, i.e., satisfying a XOR equation similar to (12).

III. QUANTUM PROTOCOL FOR SMD

In this section, we first define a primitive problem of secure multiparty computations, called SMD, and present a novel quantum protocol for SMD, which will be utilized later in the QSA scheme.

Definition 1 (SMD): Suppose that there are n parties: $P_1, P_2, \ldots, P_n$, each of which has a private input $x_i \in \{0, 1\}$ $(i = 1, 2, \ldots, n)$. After executing the SMD protocol, it outputs $x_1 \vee x_2 \vee \ldots \vee x_n$. Here, "$\vee$" denotes a logical OR, also called disjunction, i.e., $0 \vee 0 = 0$, $0 \vee 1 = 1$, $1 \vee 0 = 1$, and $1 \vee 1 = 1$. Furthermore, SMD should satisfy the following security requirements.

1) *Correctness*: If all parties honestly execute this protocol, then the final output is $x_1 \vee x_2 \vee \ldots \vee x_n$, i.e., the output is correct.
2) *Fairness*: Under no circumstances, one party should have an advantage over another or other parties. In other words, all parties are equivalent entities, and they can get the final output $x_1 \vee x_2 \vee \ldots \vee x_n$ with equal opportunities.
3) *Privacy*: Any other party except for the party P_i learns no information about x_i except the final output $x_1 \vee \ldots x_i \ldots \vee x_n$.

In the aforementioned SMD protocol, the core idea is to repeatedly compute $\oplus_{i=1}^{n} p[i]q[i]$ until it finds $\oplus_{i=1}^{n} p[i]q[i] \neq 00$ but it repeats at most k times, where $p[i]$ or $q[i]$ is random each time but $p[i] \vee q[i] = x_i$. Furthermore, $\oplus_{i=1}^{n} p[i]q[i] \neq 00$ implies $x_1 \vee \ldots x_i \ldots \vee x_n = 1$.

IV. QSA WITHOUT AN AUCTIONEER

Definition 2 (Sealed-Bid Auction Without an Auctioneer): Suppose that there are n bidders to compete a good or service. During the bidding phase, each bidder commits (i.e., submits) a private bid. After that, all bidders jointly select the winning bidder with the highest bid. In addition, it should satisfy the following security requirements.

1) *Correctness*: If all parties honestly execute this protocol, then the final output is the winning bidder with the highest bid, i.e., the output is correct.
2) *Fairness:* Under no circumstances, one party should have an advantage over another or other parties.
3) *Privacy*: Any nonwinning bidder's bid is privacy, i.e., anyone else learns no information about the bid of any nonwinning bidder except himself.

Quantum SMD protocol

Input: Each party P_i privately inputs x_i for $i = 1, 2, \ldots, n$, where $x_i \in \{0, 1\}$.
Output: $x_1 \vee \ldots x_i \ldots \vee x_n$.

{**Step 1**. All parties agree on a small integer k, e.g., $k = 5$, which is related to the probability of successfully outputting $x_1 \vee \ldots x_i \ldots \vee x_n$, i.e., $1 - \frac{1}{\delta^k}$ (see Theorem 4);

Step 2. All parties execute the following procedures:

{For $j = 1$ *to* k do {

(1) Each party P_i $(i = 1, 2, \ldots, n)$ privately prepares a Bell state $|\phi_{s[i]t[i]}\rangle_{2i-1,2i}$, where $s[i], t[i] \in_R \{0, 1\}$.

(2) Each party P_i $(i = 1, 2, \ldots, n)$ sends the particle $2i$ to the next party P_{i+1} through the authenticated quantum channel (Note $P_{n+1} = P_1$), while he keeps the particle $2i - 1$ in hands.

(3) Each party P_i $(i = 1, 2, \ldots, n)$ selects any one of two particles $2(i - 1)$, $2i - 1$ owned by himself and performs the Pauli operator $U_{p[i]q[i]}$ on the selected particle, where $p[i] \vee q[i] = x_i$. That is, if $x_i = 0$, then $p[i] = q[i] = 0$; if $x_i = 1$, then "$p[i] = 1$ and $q[i] = 0$", or "$p[i] = 0$ and $q[i] = 1$", or "$p[i] = 1$ and $q[i] = 1$".

(4) Each party P_i $(i = 1, 2, \ldots, n)$ measures the particle pair $(2(i - 1), 2i - 1)$ in Bell basis. Suppose that the measured result is $|\phi_{\bar{s}[i]\bar{t}[i]}\rangle_{2(i-1),2i-1}$.

(5) Each party P_i $(i = 1, 2, \ldots, n)$ calculates $y[i] = s[i]t[i] \oplus \bar{s}[i]\bar{t}[i]$ and opens $y[i]$.

(6) Each party P_i $(i = 1, 2, \ldots, n)$ calculates $y = y[1] \oplus y[2] \oplus \ldots y[n]$ by the public information.

(7) If $y \neq 00$, then Return 1 (i.e., $x_1 \vee \ldots x_i \ldots \vee x_n = 1$) and end the procedures of Step 2.}//end For

Return 0, i.e., $x_1 \vee \ldots x_i \ldots \vee x_n = 0$.
}
}

4) *Verifiability*: All bidders must approve the winning bidder as the true winner with the highest bid through verification protocols.

In the following QSA scheme, suppose that there are n bidders: $Bob_1, Bob_2, \ldots, Bob_n$, where each bidder Bob_i has a private bid b_i $(i = 1, 2, \ldots, n)$ and all bids lie in $Z_N = \{0, 1, 2, \ldots, N - 1\}$. In addition, we assume that there is a public collision-resistant hash $H(\cdot)$. The proposed scheme consists of three phases: Commitment phase (i.e., bidding phase), finding the highest bid phase, and verification phase, which are described in detail as follows.

A. COMMITMENT PHASE

Each bidder Bob_i $(i = 1, 2, \ldots, n)$ randomly selects an integer $r_i \in Z_N$ and computes $c_i = H(r_i \oplus H(r_i \oplus b_i))$, where b_i is his private bid. Then the bidder Bob_i announces c_i to all other bidders by the classical channels. That is, the bidder Bob_i commits b_i to all other bidders, but no bidder can get b_i only from c_i without r_i.

B. FINDING THE HIGHEST BID PHASE

Step 1: All bidders Bob_1, Bob_2, …, Bob_n agree on two parameters d and Δ, such that $d = \frac{N}{\Delta}$. Accordingly, Z_N is partitioned into d intervals: $[0, \Delta)$, $[\Delta, 2\Delta)$, …, $[N - 2\Delta, N - \Delta)$, $[N - \Delta, N)$.

Step 2: Each bidder Bob_i $(i = 1, 2, \ldots, n)$ encodes his private bid b_i as a 0/1 vector of the length d (i.e., d components) by the interval, at which his bid is located. That is, if $b_i \in [N - (k + 1)\Delta, N - k\Delta)$, then the $(k + 1)th$ component of the vector is 1 and all other remaining components are 0. Here, the vector encoded by the bidder Bob_i is denoted as $\boldsymbol{v}_i$. For example, if $b_i \in [0, \Delta)$, then $\boldsymbol{v}_i = (0, \ldots, 0, 1)$; if $b_i \in [N - 2\Delta, N - \Delta)$, then $\boldsymbol{v}_i = (0, 1, 0, \ldots, 0, 0)$. Note that the far left of $\boldsymbol{v}_i$ is the most significant bit.

Step 3: All bidders execute the following procedures (from left to right to compute the disjunction of the components of all private vectors by quantum SMD protocols, i.e., from high to low to find the highest bid's located interval):

{ For $j = 1$ *to* d do {// starting from the most significant bit

1) All bidders Bob_1, Bob_2, …, Bob_n jointly execute a quantum SMD protocol, where the bidder Bob_i $(i = 1, 2, \ldots, n)$ takes the jth component of his private vector $\boldsymbol{v}_i$ as his private input.
2) If the quantum SMD protocol outputs 1, then it can determine that the highest bid is located at the interval $[N - j\Delta, N - (j - 1)\Delta)$. Otherwise, let $j++$. Note that if the highest bid's interval is determined, then it will exit and go to Step 4.

}

Step 4: Suppose that the highest bid is located at the interval $[N - k\Delta, N - (k - 1)\Delta)$. Note that if Δ is relatively large, it can further subdivide the interval $[N - k\Delta, N - (k - 1)\Delta)$. That is, all bidders agree on two smaller parameters d^* and Δ^* again, such that $d^* = \frac{\Delta}{\Delta^*}$. Furthermore, all bidders repartition the interval $[N - k\Delta, N - (k - 1)\Delta)$ into d^* smaller intervals, encode new private vectors of the length d^*, and execute the similar procedures in Step 3. Otherwise, go to Step 5. That is, the highest bid's located interval is relatively small and acceptable.

Step 5: Without loss of generality, we assume that the highest bid is finely determined at the interval $[a, b)$. All bidders call a synchronization algorithm [37] to correct and synchronize their respective times. At the same time, all bidders set $b - a$ clock cycles corresponding to $b - a$ integers from $b - 1$ down to a, where each clock cycle includes a fixed time frame. During the ith clock cycle $(i = 1, \ldots, b - a)$, i.e., within a given time frame, if there is a bid that is just right equal to $b - i$, then the corresponding bidder with the bid $b - i$ will claim that his bid is the highest, i.e., the highest bid is $b - i$. Once there appears the highest bid, the bidders with the nonhighest bids cannot open their bids again, to protect their respective privacy. Therefore, if there is the candidate bidder who claims the highest bid, then this phase ends.

Note that the authors in [37] present a multiparty quantum time synchronization protocol, where each clock cycle consists of three stages: Initialization, interrogation, and feedback. In Initialization, each party (i.e., each node) as a center prepares and distributes a multiqubit GHZ entangled state by sharing EPR pair and performing quantum teleportation among distant nodes. In interrogation, all parties perform a phase operator on their respective qubits by their local times and then measure their respective qubits in the x-basis. In feedback, the center provides feedback information to other parties, which can help other parties to correct their respective local times. As a result, after a few cycles, the local times corresponding to each individual party achieve accuracy and stability. In practical applications, we can implement time synchronization by precomputing this protocol. Furthermore, for simplicity, we can also ask for the help of a public bulletin board or public blockchain to synchronize the time, because we do not need to achieve precision with the atomic-level error.

The previous idea mainly includes two processes: the first is to locate the highest bid's interval roughly by subtly encoding private bids and jointly computing SMD, and the second is to further find it precisely by publicly claiming, which borrows the public query way of Dutch auction round after round, but there is no auctioneer. Note that the difference between two rounds in the publicly claiming phase (i.e., Step 5) may be far greater than 1, e.g., 100, which depends on the actual auction.

C. VERIFICATION PHASE

Step 1: Suppose that the highest bid belongs to Bob_k. As the candidate, the bidder Bob_k first declares that he is the winning bidder and then opens the highest bid b_k and the corresponding secret r_k.

Step 2: By the public information (b_k, r_k), each bidder calculates $H(r_k \oplus H(r_k \oplus b_k))$ and verifies whether $c_k = H(r_k \oplus H(r_k \oplus b_k))$. If $c_k = H(r_k \oplus H(r_k \oplus b_k))$, it will successfully pass the public verification. Otherwise, the verification fails.

Step 3: If there is a bid x_j greater than the candidate bid x_k, the bidder Bob_j will broadcast a complaint about the incorrectness of the current highest bid and request all bidders to go to arbitration. Finally, if each bidder does not receive any complaint, then he will believe that the candidate bid b_k is the highest indeed and accordingly the bidder Bob_k is the winning bidder.

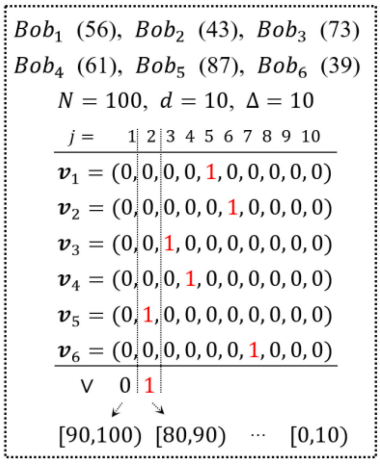


FIGURE 3. Finding the highest bid's interval.

V. ANALYSIS

A. CORRECTNESS

First, we illustrate the correctness of the proposed QSA scheme, including three phases: Commitment phase, finding the highest bid phase, and verification phase. Clearly, commitment and verification phases ensure that the bidder cannot change his bid during the whole scheme, and otherwise, he will run the risk of being detected. Therefore, the correctness of the proposed QSA scheme is fully guaranteed by that of finding the highest bid in the second phase. Furthermore, we give a simple example to illustrate how to find the highest bid, as shown in Fig. 3.

In the aforementioned example, suppose that $N = 100$, and there are six bidders: Bob_1 (56), Bob_2 (43), Bob_3 (73), Bob_4 (61), Bob_5 (87), and Bob_6 (39), where the integers in parentheses are their respective private bids. Furthermore, we assume that $d = 10$ and $\Delta = 10$, which are negotiated and determined by all bidders in Step 1. Accordingly, $\boldsymbol{v}_1 = (0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$, $\boldsymbol{v}_2 = (0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$, $\boldsymbol{v}_3 = (0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$, $\boldsymbol{v}_4 = (0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$, $\boldsymbol{v}_5 = (0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$, and $\boldsymbol{v}_6 = (0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$. When $j = 1$, $\boldsymbol{v}_1(j) \vee \boldsymbol{v}_2(j) \vee \boldsymbol{v}_3(j) \vee \boldsymbol{v}_4(j) \vee \boldsymbol{v}_5(j) \vee \boldsymbol{v}_1(j) = 0$, i.e., no bid is located at the interval [90, 100), where $\boldsymbol{v}_i(j)$ denotes the jth component of the bidder Bob_i's private vector $\boldsymbol{v}_i$. When $j = 2$, $\boldsymbol{v}_1(j) \vee \boldsymbol{v}_2(j) \vee \boldsymbol{v}_3(j) \vee \boldsymbol{v}_4(j) \vee \boldsymbol{v}_5(j) \vee \boldsymbol{v}_1(j) = 1$, i.e., there is a bid located at the interval [80, 90). By the proposed scheme, six bidders only need to call two quantum SMD protocols, where the first returns 0 and the second returns 1. Accordingly, all bidders can know that the highest bid is located at the interval [80, 90). Furthermore, during the first and second clock cycles corresponding to 89 and 88, it is evident that there is no claiming bidder, because there is no bid equal to 89 or 88. However, during the third clock cycle, the bidder Bob_5 first claims that he is the winning bidder because of the basic facts that 87 is the highest processing integer currently and there is still no claiming bidder before, and accordingly, he opens his bid 87. That is, it finds the highest bid successfully.

Furthermore, the aforementioned analysis shows that the QSA scheme's correctness still depends on the quantum SMD protocol. So, we further analyze the correctness of the quantum SMD protocol as the following theorem.

Theorem 4: In the proposed quantum SMD protocol, the probability of successfully outputting $x_1 \vee \ldots x_i \ldots \vee x_n$ is $1 - \delta^k$, where $\delta = \frac{\sum_{i=1}^{m-1}(-1)^{m-1-i}.3^i}{3^m}$. Here, m is the number of ones in all x_i's and k is the parameter publicly determined by all bidders. Note that δ is the probability to wrongly get $x_1 \vee \ldots x_i \ldots \vee x_n$ by the value of $\oplus_{i=1}^n p[i]q[i]$ in each round of the For loop, i.e., the error probability that $x_1 \vee \ldots x_i \ldots \vee x_n = 1$ but $\oplus_{i=1}^n p[i]q[i] = 00$. Clearly, $\delta \ll \frac{1}{2}$, so $1 - \delta^k \approx 1$.

Proof: The proposed quantum SMD protocol includes two steps: The first step is to agree on the parameter k; The second step is to compute $x_1 \vee \ldots x_i \ldots \vee x_n$ by repeatedly computing $\oplus_{i=1}^n p[i]q[i]$ at most k times, where $p[i] \vee q[i] = x_i$ for $i = 1$ to n.

First, we prove that the procedure to compute $\oplus_{i=1}^n p[i]q[i]$ is correct. By the proposed procedure, each party P_i $(i = 1, 2, \ldots, n)$ calculates $y = y[1] \oplus y[2] \oplus \ldots y[n]$, where $y[i] = s[i]t[i] \oplus \bar{s}[i]\bar{t}[i]$. Furthermore, we can get

$$\begin{aligned} y &= y[1] \oplus y[2] \oplus \ldots y[n] \\ y &= s[1]t[1] \oplus \bar{s}[1]\bar{t}[1] \oplus s[2]t[2] \oplus \bar{s}[2]\bar{t}[2] \\ &\quad \oplus \ldots \oplus s[n]t[n] \oplus \bar{s}[n]\bar{t}[n] \\ y &= (\oplus_{i=1}^n s[i]t[i]) \oplus (\oplus_{i=1}^n \bar{s}[i]\bar{t}[i]) \text{ (by Theorem 3)} \\ y &= \oplus_{i=1}^n p[i]q[i]. \end{aligned} \tag{13}$$

Second, we analyze the error probability to determine $x_1 \vee \ldots x_i \ldots \vee x_n$ by the value of $\oplus_{i=1}^n p[i]q[i]$. Specifically, we consider the following different cases that n inputs $x_1, \ldots x_i, \ldots, x_n$ have m ones (i.e., m is the number of 1's in all x_i's).

In the case of $m = 0$ (i.e., all x_i's are equal to 0):

If $x_i = 0$, then both $p[i]$ and $q[i]$ are equal to 0. Accordingly, if $x_i = 0$, then $x_1 \vee \ldots \vee x_i \vee \ldots \vee x_n = x_1 \vee \ldots x_{i-1} \vee x_{i+1} \ldots \vee x_n$. At the same time, $\oplus_{j=1}^n p[j]q[j] = \oplus_{j=1}^{i-1} p[j]q[j] \oplus \oplus_{j=i+1}^n p[j]q[j]$ because $p[i]q[i] = 00$. Furthermore, if all x_i's are equal to 0 for $i = 1, 2, \ldots, n$, then $\oplus_{i=1}^n p[i]q[i] = 00$. It finally outputs 0 by the proposed procedures. So, $\delta = 0$ in this case. That is, it is correct.

In the case of $m = 1$:

If only one of all x_i's is equal to 1, then all the other $p[i]q[i]$s are equal to 00 except the corresponding $p[j]q[j] \neq 00$ (i.e., $x_j = 1$). It finally outputs 1 by the proposed procedures. So, $\delta = 0$ in this case. That is, it is correct.

In the case of $m = 2$:

Suppose that $x_{i_1} = 1$, $x_{i_2} = 1$, and all the other x_i's are equal to 0. Accordingly, $p[i_1] \vee q[i_1] = 1$, $p[i_2] \vee q[i_2] = 1$,

TABLE 1. Possible values of $p[i_1]$, $q[i_1]$, $p[i_2]$, and $q[i_2]$

$p[i_1]$	$q[i_1]$	$p[i_1] \vee q[i_1]$	$p[i_2]$	$q[i_2]$	$p[i_2] \vee q[i_2]$
0	1	1	0	1	1
1	0	1	1	0	1
1	1	1	1	1	1

TABLE 2. More Cases of Different *m*s

m	The number of possible combinations	The error number	δ	$1-\delta^4$	$1-\delta^5$	$1-\delta^6$
0	1	0	0	0	0	0
1	3	0	0	0	0	0
2	9	3	0.333	0.988	0.996	0.999
3	27	6	0.222	0.998	0.9995	0.9999
4	81	21	0.259	0.996	0.9988	0.9997
5	243	60	0.247	0.996	0.9991	0.9998
6	729	183	0.251	0.996	0.999	0.9998

and $\oplus_{i=1(i\neq i_1,i_2)}^{n} p[i]q[i] = 00$. Furthermore, possible $p[i_1]$, $q[i_1]$, $p[i_2]$, and $q[i_2]$ are listed in Table 1.

From Table 1, we can see that there are nine possible combinations for $p[i_1]$, $q[i_1]$, $p[i_2]$, and $q[i_2]$, including three combinations of $p[i_1]q[i_1] \oplus p[i_2]q[i_2] = 00$ and six combinations of $p[i_1]q[i_1] \oplus p[i_2]q[i_2] \neq 00$. However, $x_1 \vee \ldots x_i \ldots \vee x_n = 1$, so the error probability is $\frac{1}{3}$ in one round, i.e., $\delta = \frac{1}{3}$.

Furthermore, we list more cases in Table 2. In Table 2, we only consider the number of possible combinations of $p[i]$ and $q[i]$ satisfying $x_i = 1$, where the error combination is corresponding to the case that both the number of $p[i]$ satisfying $p[i] = 1$ and the number of $q[i]$ satisfying $q[i] = 1$ are even, i.e., the XOR result of all $p[i]$s and that of all $q[i]$s are equal to 0 (but $x_1 \vee \ldots x_i \ldots \vee x_n = 1$). In fact, we can deduce ($m \geq 2$)

$$\delta = \frac{\sum_{i=1}^{m-1} (-1)^{m-1-i} \cdot 3^i}{3^m}. \tag{14}$$

For example, if $m = 6$, then $\delta = \frac{3^5-3^4+3^3-3^2+3^1}{3^6} = \frac{183}{729} \approx 0.251$; if $m = 7$, then $\delta = \frac{3^6-3^5+3^4-3^3+3^2-3^1}{3^7} = \frac{729-183}{729\times 3} = \frac{546}{2187} \approx 0.250$. Clearly, we can see that $\delta \neq 0$ but $\delta \ll \frac{1}{2}$ for any m (≥ 2). So, $1-\delta^k \approx 1$, where k is a constant, e.g., $k = 5$. That is, it can ensure to output the right result with a very high probability.

Therefore, the proposed quantum SMD protocol is correct.

B. SECURITY

Theorem 5: The proposed quantum SMD protocol can perfectly ensure the privacy of each party. That is, any other party except for the party P_i learns no information about x_i except the final output $x_1 \vee \ldots x_i \ldots \vee x_n$.

Proof: The proposed quantum SMD protocol is to compute $x_1 \vee \ldots x_i \ldots \vee x_n$ by repeatedly computing $\oplus_{i=1}^{n} p[i]q[i]$ at most k times. Furthermore, we focus on the amount of revealed information about private x_i of the party P_i in computing $\oplus_{i=1}^{n} p[i]q[i]$ once (i.e., a For loop). Compared with any outsider or insider, obviously, the party P_{i+1} is most likely to steal party P_i's private information, because only he can get one particle $2i$ sent by the party P_i, which is entangled with the other particle $2i-1$ kept by the party P_i. When executing a For loop, the party P_i first prepares Bell state $|\phi_{s[i]t[i]}\rangle_{2i-1,2i}$.

On the one hand, the state of $|\phi_{s[i]t[i]}\rangle_{2i-1,2i}$ is unknown to anyone else except for the party P_i, where

$$|\phi_{s[i]t[i]}\rangle_{2i-1,2i} = \frac{1}{\sqrt{2}}\left(|0\mathrm{s}\,[i]\rangle + (-1)^{t[i]}|\,0\overline{\mathrm{s}\,[i]}\rangle\right)_{2i-1,2i}. \tag{15}$$

Accordingly, we can get the reduced density matrix of the particle $2i$ sent to the party P_{i+1} through the authenticated quantum channel as follows:

$$\begin{aligned}
\rho_{2i} &= {}_{2i+1}\langle 0|\phi_{s[i]t[i]}\rangle_{2i-1,2i}\langle\phi_{s[i]t[i]}|0\rangle_{2i+1} \\
&\quad + {}_{2i+1}\langle 1|\phi_{s[i]t[i]}\rangle_{2i-1,2i}\langle\phi_{s[i]t[i]}|1\rangle_{2i+1} \\
\rho_{2i} &= \frac{|0\rangle_{2i}\langle 0| + |1\rangle_{2i}\langle 1|}{2} \\
\rho_{2i} &= \frac{I}{2}.
\end{aligned} \tag{16}$$

Given from (16), we can see that the reduced density matrix is the totally mixed state (i.e., maximally mixed state), so the party P_{i+1} cannot learn any private information about $s[i]$ and $t[i]$ of the party P_i. Furthermore, after the party P_i performs a Pauli operator $U_{p[i]q[i]}$ on the particle $2i$ or $2i-1$, $|\phi_{s[i]t[i]}\rangle_{2i-1,2i}$ will be changed as another Bell state by Theorem 2. However, the reduced density matrix of the particle $2i$ owned by the party P_{i+1} remains unchanged, i.e., it is still the totally mixed state as the same of (16). So, the party P_{i+1} cannot yet get any private information of the party P_i, e.g., $s[i]t[i]$ and $p[i]q[i]$.

On the other hand, the party P_i opens the classical information $y[i]$, where $y[i] = s[i]t[i] \oplus \bar{s}[i]\bar{t}[i]$. It is obvious that the party P_{i+1} cannot get any private information about $p[i]q[i]$ only from $y[i]$, because $s[i]t[i]$ is selected randomly and privately by the party P_i and $\bar{s}[i]\bar{t}[i]$ is subject to the uniform distribution (i.e., random) by the property of quantum measurements, and accordingly they are unknown to anyone else except for the party P_i.

Therefore, anyone including the party P_{i+1} cannot get any private information of the party P_i, though all parties can successfully compute $y = \oplus_{i=1}^{n} p[i]q[i]$. That is, the proposed quantum SMD protocol is perfect security, i.e., information-theoretical security.

Theorem 6: The proposed QSA scheme can perfectly protect the privacy of nonwinning bidders. That is, it is information-theoretical security to protect the privacy of nonwinning bidders.

Proof: On the one hand, in the commitment phase, each bidder Bob_i, including the nonwinning bidder computes $c_i = H(r_i \oplus H(r_i \oplus b_i))$ and announces the commitment value c_i

TABLE 3. Performance Comparisons

Schemes	Quantum Resources	Transmitted Qubits	Quantum Operators	Quantum Measurements	Post-Confirmation
Naseri's [14]	n-qubit GHZ states	$O(2n\log N)$	Pauli operators	n-qubit GHZ-basis measurements	-
R.D.Sharma's [27]	(r-1)-qubit entangled states	$O(n^2)$	Pauli operators	(r-1)-qubit-entangled-state measurements	-
Zhao's [19]	n-qubit GHZ states	$O(2n\log N)$	Pauli operators	n-qubit GHZ-basis measurements	$O(n^2\log N)$ Single Particles
Wang's [25]	n-qubit GHZ states	$O(2n\log N)$	Pauli operators	n-qubit GHZ-basis measurements	$O(2n^2\log N)$ Single Particles
Liu's [26]	Single particles	$O(2n\log N)$	Pauli operators	Single-particle measurements	$O(n^2\log N)$ EPR pairs
Zhang's [28]	Single photons	$O(n\log N)$	Single-photon unitary operations	Single-photon measurements	$O(n^2k)$ Single photons
Shi's [3]	3-qubit entangled states	$O(3n\log N\ln N)$	*CNOT*s, Oracle operator, Grover's Search Algorithm	*CMN*s	Classical hash
Ours	Bell states	$O(nkd)$	Pauli operators	Bell-state measurements	Classical hash

Note: CMNs denote computational basis measurements in N-dimensional Hilbert space. Furthermore, n is the number of the bidders and N is the space of private bids.

to all other bidders. Obviously, r_i is random and private for anyone except for the bidder Bob_i, so no one can get any private information about the bid b_i without r_i. That is, the proposed commitment protocol has the perfect concealing.

On the other hand, in finding the highest bid phase, all bidders, including nonbidders, agree on the public parameters (d and Δ) in Step 1 and further encode their respective private vectors in Step 2. Clearly, all bidders cannot exchange any private information in the two steps, and accordingly, it cannot reveal any private information of each bidder in these steps.

Furthermore, all bidders execute the quantum SMD protocol in Step 3 or Step 4, which is information-theoretical security proved above by Theorem 5. In Step 5, only the winning bidder with the highest bid opens his bid while all nonwinning bidders do not open their bids.

In the verification phase, it only needs the winning bidder Bob_k to open the secrets b_k and r_k. All nonwinning bidders cannot reveal any private information.

Therefore, no private information of nonwinning bidders has been revealed in our QSA scheme. That is, the proposed QSA scheme can perfectly protect the privacy of nonwinning bidders.

Theorem 7: Any bidder, including the winning bidder, cannot change his bid once commit is finished in the commitment phase.

Proof: In the commitment phase, each bidder Bob_i (including the winning bidder) computes $c_i = H(r_i \oplus H(r_i \oplus b_i))$ and announces the commitment value c_i to all other bidders. Later, if a dishonest bidder, e.g., Bob_k, wants to change his bid b_k, i.e., change the commitment value b_k to b_k^*, he must find another r_k^*, such that $H(r_k \oplus H(r_k \oplus b_k)) = H(r_k^* \oplus H(r_k^* \oplus b_k^*))$, to successfully pass the verification. It is equivalent to find y_1 and y_2, such that $H(y_1) = H(y_2)$, where $y_1 = r_k \oplus H(r_k \oplus b_k)$ and $y_2 = r_k^* \oplus H(r_k^* \oplus b_k^*)$. However, it is impossible to decipher the hash function with strong collision-resistant even for quantum computers [12]. Meanwhile, it is also impossible for quantum computers to find r_k^* only by $H(r_k^* \oplus b_k^*) = r_k^* \oplus r_k \oplus H(r_k \oplus b_k)$ (i.e., solving the inverse of the hash). So, the dishonest bidder Bob_k cannot change the commitment value b_k to be revealed in the verification phase (i.e., open phase), once the commit is finished. That is, our proposed commitment protocol based on a strong collision-resistant hash is secure, which can resist the attack of quantum computers.

In a word, there is no auctioneer in our QSA scheme, so the bidders do not need to submit the private bids to anyone. Moreover, all bidders are peer, i.e., completely equivalent entities. There is not a bidder who can get more private information with a higher probability. Therefore, our proposed QSA scheme can also ensure anonymity and fairness.

Finally, like most existing secure multiparty quantum computations, our proposed QSA scheme needs authenticated quantum channels, which can ensure the authenticity of quantum resources and participant identities. In principle, we may combine quantum authentication technologies with classical authentication technologies to implement various authentications in quantum channels [36], [38].

C. PERFORMANCE

The proposed quantum SMD protocol takes Bell states as quantum resources and only performs single-particle Pauli operators and two-particle Bell measurements. Especially, each bidder executes the same procedures to jointly compute $\oplus_{i=1}^{n} p[i]q[i]$ in each round, i.e., preparing a Bell state, sending one particle of the Bell state to the next bidder, applying a Pauli operator, and finally performing a Bell-basis measurement. In total, each bidder prepares at most k Bell states, transmits at most k particles, and performs at most

IEEE Transactions on Quantum Engineering

TABLE 4. Security Comparisons

Schemes	Verifiability	Anonymity	Fairness	Privacy	Trusted Auctioneer
Naseri's [14]	No	No	No	No	Yes
R.D.Sharma's [27]	Yes	No	Yes	No	Yes
Zhao's [19]	Public	Weak	No	No	Yes
Wang's [25]	Public	Weak	Yes	No	Yes
Liu's [26]	Public	Weak	Yes	No	Yes
Zhang's [28]	Public	Weak	Yes	No	Yes
Shi's [3]	Public	Strong	Yes	Partial	Yes
Ours	Public	Strong	Yes	Perfect	No

Note: Weak anonymity means that it is anonymous for other bidders except the auctioneer, whereas strong anonymity means that it is anonymous for any one, including the auctioneer. Privacy means the privacy of nonwinning bidders.

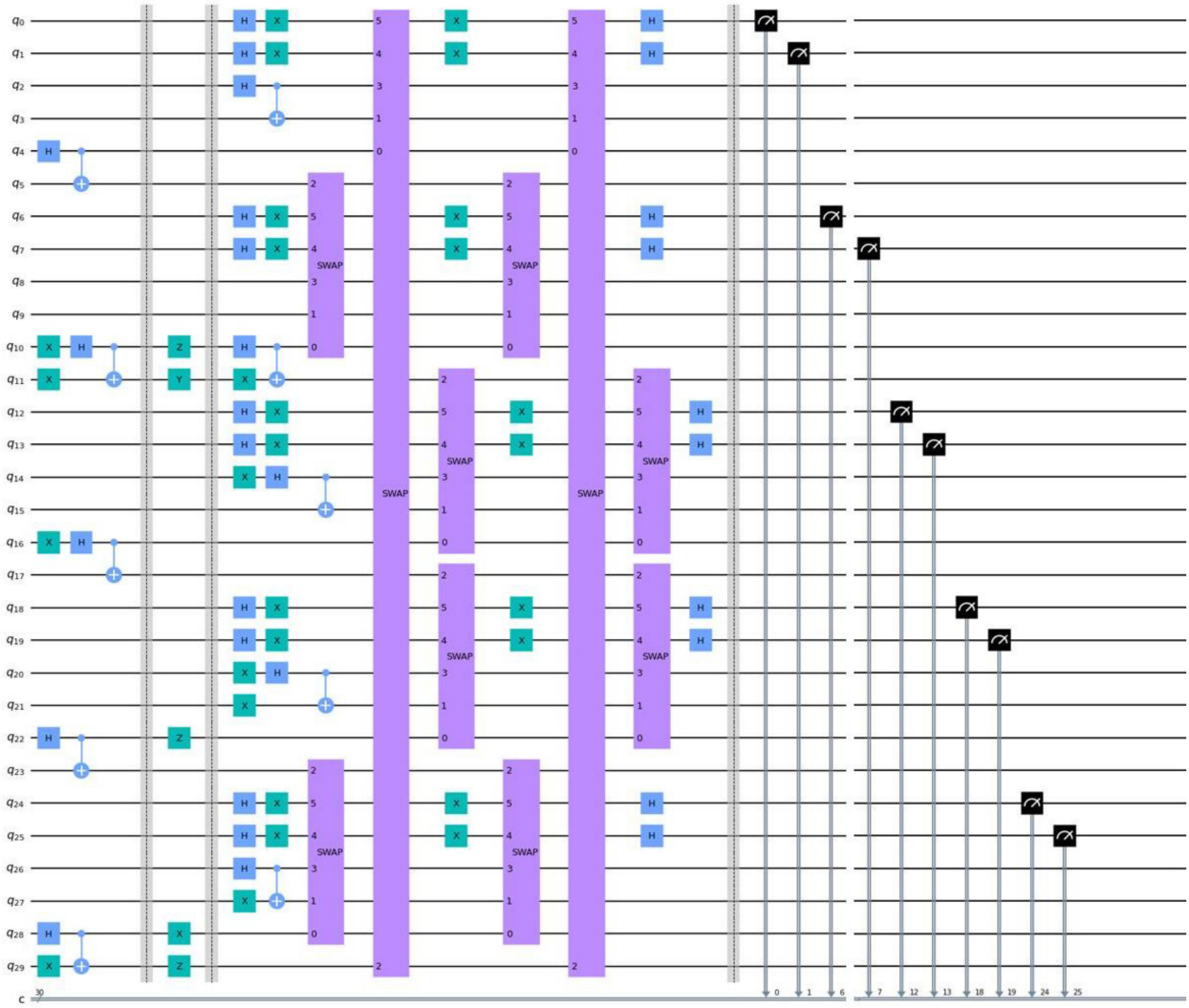


FIGURE 4. Quantum circuit of the proposed quantum SMD protocol.

k Pauli operators and at most k Bell-basis measurements. Accordingly, both the total computational complexity and the total communicational complexity are $O(kn)$, where n is the number of all bidders and k is a constant.

Furthermore, the proposed QSA scheme first encodes the bidders' private vectors by public information, which is lightweight and negligible, and further computes the disjunction of the components of all private vectors from high down to low. Accordingly, the main cost of the proposed QSA scheme is to execute multiple quantum SMD protocols, where the number of executing the quantum SMD protocols is $O(d)$.

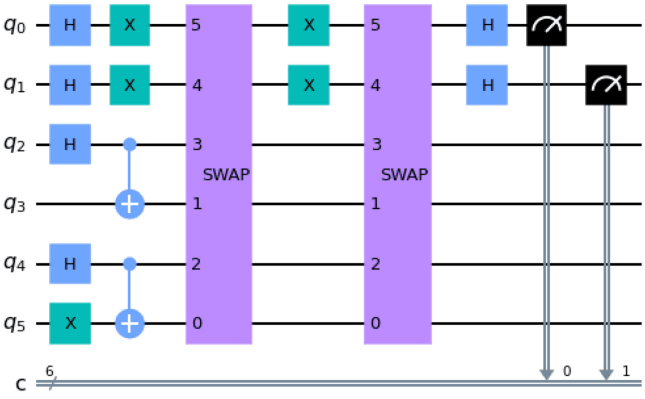


FIGURE 5. Quantum circuit of identifying Bell state.

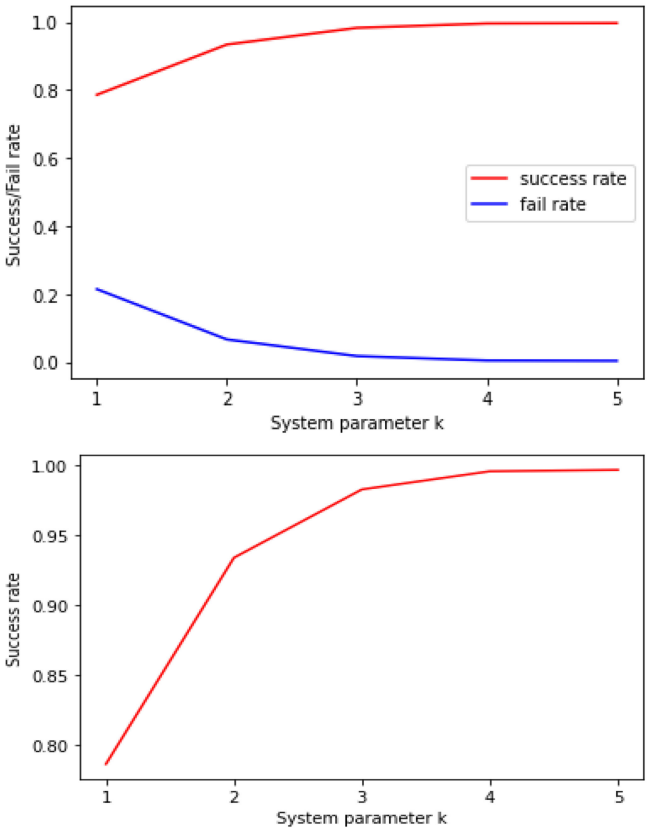


FIGURE 6. Average results 10 000 times with 5 bidders.

In the following section, we give detailed comparisons of our proposed QSA scheme and other related QSA schemes from quantum resources, transmitted qubits, necessary quantum operators and quantum measurements, post-confirmation, and security properties, as listed in Tables 2 and 4.

From Table 3, we can see that most QSA schemes take multiqubit entangled states as quantum resources and need the corresponding measurements in high-dimensional Hilbert space. But it is still difficult to prepare these quantum states and implement the corresponding operators and measurements on these quantum states.

Furthermore, in Table 4, only our proposed QSA protocol meets all security properties, i.e., public verifiability, strong anonymity, fairness, perfect privacy, and no auctioneer.

In addition, as a primitive protocol of secure multiparty computations, our proposed quantum SMD protocol can be utilized to implement the anonymous veto [39], where the inputs 0 and 1 mean "approval" and "disapproval" on one proposal, respectively. Once existing at least one "disapproval," the proposal is rejected. Like most multiparty quantum protocols, currently existing anonymous veto protocols ask for the help of a trusted third party. On the contrary, no trusted third party is just our most advantage.

Finally, we simulate the proposed SMD protocol in Qiskit of IBM (Qiskit-0.23.2; Python-3.8.6; OS-Linux). In our simulation experiments, suppose that there are five bidders and they jointly compute the SMD protocol 10 000 times in total, where each input is random each time. The detailed circuits are shown in Fig. 4. In the first phase in Fig. 4, five bidders prepare five Bell states as inputs, e.g., $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{q_4q_5}$, $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{q_{10}q_{11}}$, $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{q_{16}q_{17}}$, $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{q_{22}q_{23}}$, and $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{q_{28}q_{29}}$, whereas all the rest are ancillary qubits. In the second phase in Fig. 4, the bidders randomly perform Pauli operators, e.g., Z, Y ,Z, X , and Z on the qubits q_{10}, q_{11}, q_{22}, q_{28} , and q_{29}, respectively. The last phase denotes the measurements.

Here, we borrow the idea of probabilistically identifying Bell states by adopting the circuit of Fig. 5 instead of directly measuring Bell states [40]. Fig. 5 shows quantum swapping circuits for determining the inner product of two-qubit states. If the projection measurement is performed on the ancillary qubits (q_0, q_1) in Fig. 5, the probability that it is in the state $|00\rangle$ is $\frac{1}{2}(1 + |\langle_{q_4q_5}\psi|\psi_{q_2q_3}\rangle|^2)$. In turn, the inner product of $|\psi_{q_2q_3}\rangle$ and $|\psi_{q_4q_5}\rangle$ can be calculated as $\langle_{q_4q_5}\psi|\psi_{q_2q_3}\rangle = \sqrt{2P(|00\rangle) - 1}$, where $P(|00\rangle)$ is the probability that the ancillary qubits are in state $|00\rangle$. Accordingly, we can verify the XOR equation by setting ancillary Bell states reasonably.

The average results are shown in Fig. 6. By Fig. 6, we can see that the success rate is approximately equal to 1 when $k = 5$. Clearly, it verifies the results of Theorem 4.

In short, the simulation experiments show that the proposed SMD protocol is correct and prove that it is feasible to implement it with the present quantum technologies.

VI. CONCLUSION

In this article, we presented a novel QSA scheme without an auctioneer, in which all bidders jointly find the highest bid by using proposed quantum SMD protocols. On the one hand, the proposed quantum primitive protocol perfectly protects the privacy of nonwinning bidders, i.e., it is information-theoretically secure for nonwinning (losing) bidders. On the

other hand, tactfully combining the private encoding with the public query achieves high efficiency instead of bit-by-bit comparisons.

The proposed QSA scheme takes Bell states as quantum resources and performs single-particle Pauli operators and Bell-basis measurements. Furthermore, the simulation experiments verify that it is feasible to implement this scheme with the present quantum processing technologies. Due to perfect privacy protection, high efficiency, and feasibility, we believe the proposed scheme had wider popularization and application prospects.

REFERENCES

[1] A. Jin, W. Song, and W. Zhuang, "Auction-based resource allocation for sharing cloudlets in mobile cloud computing," *IEEE Trans. Emerg. Top. Comput.*, vol. 6, no. 1, pp. 45–57, Jan.–Mar. 2018, doi: 10.1109/TETC.2015.2487865.

[2] Y. Chen, X. Tian, Q. Wang, J. Jiang, M. Li, and Q. Zhang, "SAFE: A general secure and fair auction framework for wireless markets with privacy preservation," *IEEE Trans. Dependable Secure Comput.*, to be published, doi: 10.1109/TDSC.2020.3045449.

[3] R. H. Shi and M. Zhang, "Privacy-preserving quantum sealed-bid auction based on Grover's search algorithm," *Sci. Rep.*, vol. 9, May 2019, Art. no. 7626, doi: 10.1038/s4159-019-44030-8.

[4] R. H. Shi, R. Zhang, B. Liu, and M. Zhang, "Cryptanalysis and improvement of quantum sealed-bid auction," *Int. J. Theor. Phys.*, vol. 59, no. 6, pp. 1917–1926, Apr. 2020, doi: 10.1007/s10773-020-04463-8.

[5] R. Alvarez and M. Nojoumian, "Comprehensive survey on privacy-preserving protocols for sealed-bid auctions," *Comput. Secur.*, vol. 88, Jan. 2020, Art. no. 101502, doi: 10.1016/j.cose.2019.03.023.

[6] M. K. Franklin and M. K. Reiter, "The design and implementation of a secure auction service," *IEEE Trans. Softw. Eng.*, vol. 22, no. 5, pp. 302–312, May 1996, doi: 10.1109/32.502223.

[7] M. Naor, B. Pinkas, and R. Sumner, "Privacy preserving auctions and mechanism design," in *Proc. 1st ACM Conf. Electron. Commerce*, Nov. 1999, pp. 129–139, doi: 10.1145/336992.337028.

[8] K. Sako, "An auction protocol which hides bids of losers," in *Proc. Int. Workshop Public Key Cryptogr.*, Jan. 2000, vol. 1751, pp. 422–432, doi: 10.1007/978-3-540-46588-1_28.

[9] H. S. Galal and A. M. Youssef, "Verifiable sealed-bid auction on the Ethereum blockchain," in *Proc. Financial Cryptogr. Data Secur.*, Mar. 2018, pp. 265–278, doi: 10.1007/978-3-662-58820-8_18.

[10] D. J. Egger *et al.*, "Quantum computing for finance: State-of-the-art and future prospects," *IEEE Trans. Quantum Eng.*, vol. 1, Oct. 2020, Art. no. 3101724, doi: 10.1109/TQE.2020.3030314.

[11] J. Kusyk, S. M. Saeed, and M. U. Uyar, "Survey on quantum circuit compilation for noisy intermediate-scale quantum computers: Artificial intelligence to heuristics," *IEEE Trans. Quantum Eng.*, vol. 26, Mar. 2021, Art. no. 2501616, doi: 10.1109/TQE.2021.3068355.

[12] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[13] R. H. Shi, "Quantum bloom filter and its applications," *IEEE Trans. Quantum Eng.*, vol. 2, Art. no. 2100411, Jan. 2021, doi: 10.1109/TQE.2021.3054623.

[14] M. Naseri, "Secure quantum sealed-bid auction," *Opt. Commun.*, vol. 282, no. 9, pp. 1939–1943, Sep. 2009, doi: 10.1016/j.optcom.2009.01.026.

[15] S. J. Qin *et al.*, "Cryptanalysis and improvement of a secure quantum sealed-bid auction," *Opt. Commun.*, vol. 282, no. 19, pp. 4014–4016, Oct. 2009, doi: 10.1016/j.optcom.2009.06.070.

[16] Y. G. Yang, M. Naseri, and Q. Y. Wen, "Improved secure quantum sealed-bid auction," *Opt. Commun.*, vol. 282, no. 20, pp. 4167–4170, Oct. 2009, doi: 10.1016/j.optcom.2009.07.010.

[17] Y. M. Liu *et al.*, "Revisiting Naseri's secure quantum sealed-bid auction," *Int. J. Quantum Inf.*, vol. 7, no. 6, pp. 1295–1301, Jun. 2009, doi: 10.1142/S0219749909005808.

[18] Y. Zheng and Z. Zhao, "Comment on: 'Secure quantum sealed-bid auction' [Opt. Comm. 282 (2009) 1939]," *Opt. Commun.*, vol. 282, no. 20, Oct. 2009, Art. no. 4182, doi: 0.1016/j.optcom.2009.07.013.

[19] Z. Zhao, M. Naseri, and Y. Zheng, "Secure quantum sealed-bid auction with post-confirmation," *Opt. Commun.*, vol. 283, no. 16, pp. 3194–3197, Aug. 2010, doi: 10.1016/j.optcom.2010.04.019.

[20] G. A. Xu *et al.*, "Cryptanalysis and improvement of the secure quantum sealed-bid auction with postconfirmation," *Int. J. Quantum Inf.*, vol. 9, no. 6, pp. 1383–1392, Jun. 2011, doi: 10.1142/S0219749911008076.

[21] L. B. He *et al.*, "Cryptanalysis and melioration of secure quantum sealed-bid auction with post-confirmation," *Quantum Inf. Process*, vol. 11, no. 12, pp. 1359–1369, Dec. 2012, doi: 10.1007/s11128-011-0275-5.

[22] Q. L. Wang, W. W. Zhang, and Q. Su, "Revisiting 'The loophole of the improved secure quantum sealed-bid auction with post-confirmation and solution'," *Int. J. Theor. Phys.*, vol. 53, no. 9, pp. 3147–3153, Sep. 2014, doi: 10.1007/s10773-014-2112-y.

[23] Y. Z. Wang, "Quantum secure direct communication and quantum sealed-bid auction with EPR pairs," *Commun. Theor. Phys.*, vol. 54, no. 6, pp. 997–1002, Dec. 2010, doi: 10.1088/0253-6102/54/6/08.

[24] W. J. Liu *et al.*, "Attacks and improvement of quantum sealed-bid auction with EPR pairs," *Commun. Theor. Phys.*, vol. 61, no. 6, Jun. 2014, Art. no. 686, doi: 10.1088/0253-6102/61/6/05.

[25] J. T. Wang *et al.*, "A new quantum sealed-bid auction protocol with secret order in post-confirmation," *Quantum Inf. Process.*, vol. 14, no. 10, pp. 3899–3911, Oct. 2015, doi: 10.1007/s11128-015-1076-z.

[26] W. J. Liu *et al.*, "Multiparty quantum sealed-bid auction using single photons as message carrier," *Quantum Inf. Process.*, vol. 15, no. 2, pp. 869–879, Feb. 2016, doi: 10.1007/s11128-015-1202-y.

[27] R. D. Sharma, K. Thapliyal, and A. Pathak, "Quantum sealed-bid auction using a modified scheme for multiparty circular quantum key agreement," *Quantum Inf. Process.*, vol. 16, May 2017, Art. no. 169, doi: 10.1007/s11128-017-1620-0.

[28] R. Zhang *et al.*, "An economic and feasible quantum sealed-bid auction protocol," *Quantum Inf. Process.*, vol. 17, no. 2, Jan. 2018, Art. no. 35, doi: 10.1007/s11128-017-1805-6.

[29] R. H. Shi, "Anonymous quantum sealed-bid auction," *IEEE Trans. Circuits II*, vol. 69, no. 2, pp. 414–418, Feb. 2022, doi: 10.1109/TCSII.2021.3098755.

[30] E. W. Piotrowski and J. S∤adkowski, "Quantum English auctions," *Physica A*, vol. 318, no. 3/4, pp. 505–515, Feb. 2003, doi: 10.1016/s0378-4371(02)01533-9.

[31] D. Wang and N. Wang, "Quantum computation based bunding optimization for combinatorial auction in freight service procurements," *Comput. Ind. Eng.*, vol. 89, pp. 186–193, Nov. 2015, doi: 10.1016/j.cie.2014.11.014.

[32] T. Hogg, P. Harsha, and K.Y. Chen, "Quantum auctions," *Int. J. Quantum Inf.*, vol. 5, no. 5, pp. 751–780, Oct. 2007, doi: 10.1142/S0219749907003183.

[33] E. W. Piotrowski and J. S∤adkowski, "Quantum auctions: Facts and myths," *Physica A*, vol. 387, no. 15, pp. 3949–3953, Jun. 2008, doi: 10.1016/j.physa.2008.02.07.

[34] K. Y. Chen and T. Hogg, "Experiments with probabilistic quantum auctions," *Quantum Inf. Process.*, vol. 7, pp. 139–152, Aug. 2008, doi: 10.1007/s11128-008-0079-4.

[35] S. Bag, F. Hao, S. F. Shahandashti, and I. G. Gay, "SEAL: Sealed-bid auction without auctioneers," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 2042–2052, Nov. 2019, doi: 10.1109/TIFS.2019.2955793.

[36] R. H. Shi, "Useful equations about bell states and their applications to quantum secret sharing," *IEEE Commun. Lett.*, vol. 24, no. 2, pp. 386–390, Nov. 2019, doi: 10.1109/lcomm.2019.2954134.

[37] P. Komar *et al.*, "A quantum network of clocks," *Nature Phys.*, vol. 10, no. 8, pp. 582–587, Aug. 2014, doi: 10.1038/nphys3000.

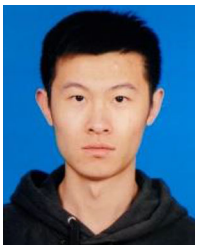
[38] R. H. Shi *et al.*, "Two quantum protocols for oblivious set-member decision problem," *Sci. Rep.*, vol. 5, Oct. 2015, Art. no. 15914, doi: 10.1038/srep15914.

[39] Q. Wang *et al.*, "Quantum-based anonymity and secure veto," *Quantum Inf. Process.*, vol. 20, Mar. 2021, Art. no. 85, doi: 10.1007/s11128-021-03022-2.

[40] A. Gupta, B. K. Behera, and P. K. Panigrahi, "Measurement-device-independent QSDC protocol using Bell and GHZ states on quantum simulator," Jul. 2020, *arXiv:2007.01122*.

Run-Hua Shi received the Ph.D. degree in information security from the University of Science and Technology of China, Hefei, China, in 2011.

He is currently a Professor with North China Electric Power University, Beijing, China. His current research interest includes classical/quantum cryptographic algorithms/protocols and their applications.



Yi-Fei Li received the bachelor's degree in information security in 2019 from North China Electric Power University, Beijing, China, where he is currently working toward the master's degre in computer science and technology.

His main research interests include quantum computing and quantum circuits.