Eur. Phys. J. Plus (2023) 138:31
https://doi.org/10.1140/epjp/s13360-023-03662-6

THE EUROPEAN PHYSICAL JOURNAL PLUS

Regular Article

Quantum sealed-bid auction using the phases of quantum entangled states as bids

Takashi Mihara[a]

Department of Information Sciences and Arts, Toyo University, 2100 Kujirai, Kawagoe 350-8585, Saitama, Japan

Received: 16 August 2022 / Accepted: 4 January 2023

Abstract Today, various processes are being carried out on the Internet. Therefore, we need to think about security on the Internet since various confidential information is also communicated. Quantum information such as quantum cryptography also plays an important role in the security. Moreover, many quantum applications are also proposed. In this paper, we focus on sealed-bid auction on the Internet and propose a quantum sealed-bid auction with entanglement. The advantage of our protocol is that it uses the phases of quantum entangled states as bid prices. Therefore, no one, including legitimate parties, can steal useful information such as bid prices unless all the states are obtained. As a result, any information is not leaked to any outside attacker, bidders cannot know each other's bid prices, and the auctioneer can only obtain the highest bid price.

1 Introduction

Many research results have been published on quantum information including quantum computers (see, e.g., [1]). Typical early results are Shor's prime factorization algorithm [2] and Grover's database search algorithm [3]. There are also many studies related to quantum security such as BB84 protocol and E91 protocol, i.e., such as quantum key exchange protocols [4, 5]. In addition, quantum steganography, derived from quantum security, is also studied [6–8].

Recently, there are also studies on collaboration between economics and quantum information. The auction in this paper is one of them. There are various types of auctions such as English auction, Dutch auction, and sealed-bid auction. English auction is an open-outcry ascending price auction, Dutch auction is a descending price auction or a uniform price auction, and sealed-bid auction is an auction in which all bidders simultaneously submit sealed bids to the auctioneer so that no bidder knows the bids of the other bidders. In particular, quantum versions of sealed-bid auction are being actively studied.

As an early study of sealed-bid auction, Naseri proposes a protocol using quantum secure direct communication to privately transmit the bids [9]. Later, some defects in this protocol have been pointed out and various improvements have also been proposed. However, we here omit about these contents because they are not related to the method of this paper in essence (see, e.g., [10] and references therein). Zhang et al. [11] propose a quantum protocol based on single photons in both the polarization and the spatial-mode degrees of freedom. Quantum protocols based on secret sharing are also proposed [12, 13]. In all the papers mentioned above, although each bidder cannot know the bid prices of all the other bidders, the auctioneer can know the bid prices of all the bidders, including the non-winning bidders. Shi and Zhang [14] propose a quantum protocol based on Grover's search algorithm. Their protocol can protect the privacy, i.e., the bid prices, of the non-winning bidders. However, there is the risk of information leakage because the state in which bid prices are input is sent to other bidders. Moreover, since their protocol uses Grover's algorithm, the number of different bid prices is limited to only the search area, i.e., the number of different states. Recently, a protocol with a condition different from traditional auctions including our protocol, i.e., a quantum protocol without an auctioneer, is also proposed [15].

In this paper, we propose a different type of quantum sealed-bid auction with entanglement. Our proposed protocol is executed in the following way. Legitimate parties share entanglement with each other, and operate the phases of the quantum entangled states in order to send their bid prices. The values of the phases mean the information of bid prices. No one can know the phases of the quantum entangled states unless a party knows all the states. Finally, the auctioneer can safely obtain the highest bid price with certainty, unlike protocols using probabilistic algorithms such as Grover's search algorithm. In addition, our protocol incorporates a mechanism that cannot know prices other than the highest bid price including the auctioneer, and does not need to limit the range of bid prices.

[a] e-mail: mihara@toyo.jp (corresponding author)

Published online: 16 January 2023

The rest of this paper is organized as follows. In Sect. 2, we construct basic quantum protocol used in our proposed auction. This protocol is our core protocol. In Sect. 3, we show our quantum sealed-bid auction protocol. In Sect. 4, we consider the security of our proposed protocol. Finally, in Sect. 5, we provide some concluding remarks.

2 Basic protocol used in our proposed auction

2.1 Proposed protocol

We propose a quantum sealed-bid auction using the phases of quantum entangled states as bid prices. In this section, first, we construct a basic protocol used as a subroutine in the next section. This protocol can announce bidders' several information to the auctioneer (and all the bidders) keeping secret who bid. In this paper, we assume that legitimate parties can share entanglement securely since many methods are proposed in order to share entanglement securely (see, e.g., [16, 17]).

Let Alice be an auctioneer, and B_1, B_2, ..., and B_m be m bidders. Moreover, let L be the number of different bid values. In this paper, L means either the maximum expected number of digits in bid price or 10 for decimal number (i.e., 10 different numbers $(0, 1, \ldots, 9)$), and $\mathbf{L}(|\mathbf{L}| = L)$ is the set of values corresponding to digits mentioned above. For example, if Alice expects the highest bid price to be less than 300,000, $\mathbf{L} = \{1, 2, 3, 4, 5, 6\}$, each element of which corresponds to each digit(i.e., $6(= L)$ digits). In addition, let $\mathbf{S}_i$ be the set of suffixes of bidders that bid i for $i \in \mathbf{L}$. Namely, the suffix $3 \in \mathbf{S}_5$ if a bidder B_3 bids $5 \in \mathbf{L}$. Note that $\mathbf{S}_i \cap \mathbf{S}_{i'} = \emptyset$ for any $i \neq i'$. This means that bidders are classified according to each element in $\mathbf{L}$. However, these sets are merely symbols necessary to describe the following protocol and the protocol does not actually execute classification processing. Our protocol is to find the maximum element in $\mathbf{L}$ satisfying $\mathbf{S}_i \neq \emptyset$. Then, we can construct a basic quantum auction protocol as follows and we call this protocol *B-QSBP*:

Step 1 Alice, B_1, ..., and B_m share entanglement

$$\bigotimes_{i=1}^{L} \sum_{x_i=0}^{2^{n_i}-1} \frac{1}{\sqrt{2^{n_i}}} |x_i\rangle_A |x_i\rangle_{B_1} \otimes \cdots \otimes |x_i\rangle_{B_m} \tag{1}$$

beforehand, where n_i is the length of qubits state $|x_i\rangle$. Here, let 2^{n_i} be sufficiently large value compared to m, the number of bidders. Moreover, Alice has $|x_i\rangle_A$ and B_k has $|x_i\rangle_{B_k}$ for $k \in \{1, 2, \ldots, m\}$.

Step 2 Each bidder executes some of the following procedures according to his/her bid price.

Step 2-1 Every bidder $B_k \in \{B_1, B_2, \ldots, B_m\}$ applies the following operation to his/her bidding state $|x_j\rangle_{B_k}$ for any $j \in \{1, 2, \ldots, L\}$:

$$|x_j\rangle_{B_k} \to |x_j \oplus b_{jk}\rangle_{B_k}, \tag{2}$$

where b_{jk} is a random constant n_j-bit value determined by B_k.

Step 2-2 Each bidder $B_k (k \in \mathbf{S}_i)$ applies the phase shift operation for any $j \in \{1, 2, \ldots, i\}$:

$$|x_j\rangle_{B_k} \to e^{i2\pi a_{jk} x_j / 2^{n_j}} |x_j\rangle_{B_k}, \tag{3}$$

where a_{jk} is a random constant value determined by B_k satisfying $0 < a_{jk} < \lfloor 2^{n_j}/m \rfloor$.

Step 2-3 Each bidder $B_k (k \in \mathbf{S}_i)$ applies the following operation for any $j \in \{1, 2, \ldots, i-1\}$:

$$|x_j\rangle_{B_k} \to |f_{jk}(x_j \oplus b_{jk})\rangle_{B_k}, \tag{4}$$

where $f_{jk} : \{0,1\}^{n_j} \to \{0,1\}^{n_j}$ is a random one-to-one function determined by B_k.

After Step 2, the state can be classified into the following three cases, and the entanglement becomes the combination of these states. Here, let $I = \max\{i \mid \mathbf{S}_i \neq \emptyset\}$.

Case 1 ($j > I$): The state becomes

$$\sum_{x_j=0}^{2^{n_j}-1} \frac{1}{\sqrt{2^{n_j}}} |x_j\rangle_A |x_j \oplus b_{j1}\rangle_{B_1} \otimes \cdots \otimes |x_j \oplus b_{jm}\rangle_{B_m}. \tag{5}$$

In this case, only Step 2-1 is executed.

Case 2 ($j = I$): The state becomes

$$\sum_{x_I=0}^{2^{n_I}-1} \frac{1}{\sqrt{2^{n_I}}} e^{i2\pi \sum_{k \in \mathbf{S}_I} a_{Ik} x_I / 2^{n_I}} |x_I\rangle_A \otimes |x_I \oplus b_{I1}\rangle_{B_1} \otimes \cdots \otimes |x_I \oplus b_{Im}\rangle_{B_m}. \tag{6}$$

In this case, Step 2-1 and Step 2-2 are executed.

Case 3 ($j < I$): The state becomes

$$\sum_{x_j=0}^{2^{n_j}-1} \frac{1}{\sqrt{2^{n_j}}} e^{i2\pi \sum_{k\in\cup_{j'=j}^{I}\mathbf{S}_{j'}} a_{jk}x_j/2^{n_j}} |x_j\rangle_A \bigotimes_{k'\in\cup_{i\le j}\mathbf{S}_i} |x_j \oplus b_{jk'}\rangle_{B_{k'}} \bigotimes_{k'\in\cup_{j<i\le I}\mathbf{S}_i} |f_{jk'}(x_j \oplus b_{jk'})\rangle_{B_{k'}}. \tag{7}$$

Note that $\bigcup_{I<i} \mathbf{S}_i = \emptyset$, and $\sum_{k\in\mathbf{S}_j} a_{jk} = 0$ if $\mathbf{S}_j = \emptyset$.

Step 3 Each bidder $B_k \in \{B_1, B_2, \ldots, B_m\}$ sends his/her states to Alice.

Step 4 Alice applies the exclusive-or operation between her state and each bidder's state. Then, the state becomes as follows according to each case of Step 2:

Case 1 ($j > I$):

$$\sum_{x_j=0}^{2^{n_j}-1} \frac{1}{\sqrt{2^{n_j}}} |x_j\rangle_A |b_{j1}\rangle_{B_1} \otimes \cdots \otimes |b_{jm}\rangle_{B_m}. \tag{8}$$

Case 2 ($j = I$):

$$\sum_{x_I=0}^{2^{n_I}-1} \frac{1}{\sqrt{2^{n_I}}} e^{i2\pi \sum_{k\in\mathbf{S}_I} a_{Ik}x_I/2^{n_I}} |x_I\rangle_A \otimes |b_{I1}\rangle_{B_1} \otimes \cdots \otimes |b_{Im}\rangle_{B_m}. \tag{9}$$

Case 3 ($j < I$):

$$\sum_{x_j=0}^{2^{n_j}-1} \frac{1}{\sqrt{2^{n_j}}} e^{i2\pi \sum_{k\in\cup_{j'=j}^{I}\mathbf{S}_{j'}} a_{jk}x_j/2^{n_j}} |x_j\rangle_A \bigotimes_{k'\in\cup_{i\le j}\mathbf{S}_i} |b_{jk'}\rangle_{B_{k'}} \bigotimes_{k'\in\cup_{j<i\le I}\mathbf{S}_i} |f_{jk'}(x_j \oplus b_{jk'}) \oplus x_j\rangle_{B_{k'}}. \tag{10}$$

Step 5 Alice also applies the inverse quantum Fourier transform ($|x_i\rangle \to \sum_{y_i=0}^{2^{n_i}-1} \frac{1}{\sqrt{2^{n_i}}} e^{-i2\pi x_i y_i/2^{n_i}} |y_i\rangle$) [2] to her states. Then, the state becomes as follows according to each case of Step 4:

Case 1 ($j > I$):

$$|0\rangle_A |b_{j1}\rangle_{B_1} \otimes \cdots \otimes |b_{jm}\rangle_{B_m}. \tag{11}$$

Case 2 ($j = I$):

$$\left| \sum_{k\in\mathbf{S}_I} a_{Ik} \right\rangle_A |b_{I1}\rangle_{B_1} \otimes \cdots \otimes |b_{Im}\rangle_{B_m}. \tag{12}$$

Case 3 ($j < I$):

$$\sum_{y_j=0}^{2^{n_j}-1} \sum_{x_j=0}^{2^{n_j}-1} \frac{1}{2^{n_j}} e^{i2\pi \left(\sum_{k\in\cup_{j'=j}^{I}\mathbf{S}_{j'}} a_{jk}k - y_j\right) x_j/2^{n_j}} |y_j\rangle_A \bigotimes_{k'\in\cup_{i\le j}\mathbf{S}_i} |b_{jk'}\rangle_{B_{k'}} \bigotimes_{k'\in\cup_{j<i\le I}\mathbf{S}_i} |f_{jk'}(x_j \oplus b_{jk'}) \oplus x_j\rangle_{B_{k'}}. \tag{13}$$

Step 6 When she observes her states, Alice can obtain a value with certainty in Case 1 or in Case 2, i.e., she can obtain 0 for Case 1 and $\sum_{k\in\mathbf{S}_I} a_{Ik}$ for Case 2. However, she cannot obtain a value with certainty in Case 3 because some bidders' states corresponding to $B_{k'}(k' \in \cup_{j<i\le I}\mathbf{S}_i)$ disturb. In the case of Case 3, therefore, it is also unknown whether or not the bid was made. Therefore, Alice can know the maximum suffix I corresponding to the non-zero observation values, i.e., the maximum value.

In this protocol, Alice requires all the L states shared by each bidder in Step 3 and after simultaneously. If it is sequentially sent to Alice from the highest value L to the lowest value 1 and is executed in each case, the protocol can be completed when the maximum suffix I is obtained. Therefore, she can obtain it with a simpler protocol. However, each bidder must send his/her state up to L times to Alice if $I = L$.

2.2 An example

Let's consider finding the maximum number of digits in bidders' bid prices in order to understand the procedure of B-QSBP. Now, assume that an auctioneer Alice expects L to be 5 or less, and three bidders B_1, B_2, and B_3 consider bidding at prices of \$115, \$202, and \$98, respectively. This example means that $\mathbf{L} = \{1, 2, 3, 4, 5\}$, $\mathbf{S}_5 = \mathbf{S}_4 = \mathbf{S}_1 = \emptyset$, $\mathbf{S}_3 = \{1, 2\}$, and $\mathbf{S}_2 = \{3\}$. Moreover, let $n_i = 10$ for any i.

In Step 1, first, Alice and three bidders share entanglement

$$\bigotimes_{i=1}^{5} \sum_{x_i=0}^{2^{10}-1} \frac{1}{\sqrt{2^{10}}} |x_i\rangle_A |x_i\rangle_{B_1} |x_i\rangle_{B_2} |x_i\rangle_{B_3} \tag{14}$$

beforehand.

Next, Step 2 is executed in order to give the information on the number of the digits. After Step 2, the state becomes

$$\begin{aligned}
&\sum_{x_1=0}^{2^{10}-1} \frac{1}{\sqrt{2^{10}}} |x_1\rangle_A e^{i2\pi 33x_1/2^{10}} |f_{11}(x_1 \oplus b_{11})\rangle_{B_1} \\
&\otimes e^{i2\pi 13x_1/2^{10}} |f_{12}(x_1 \oplus b_{12})\rangle_{B_2} e^{i2\pi 7x_1/2^{10}} |f_{13}(x_1 \oplus b_{13})\rangle_{B_3} \\
&\otimes \sum_{x_2=0}^{2^{10}-1} \frac{1}{\sqrt{2^{10}}} |x_2\rangle_A e^{i2\pi 79x_2/2^{10}} |f_{21}(x_2 \oplus b_{21})\rangle_{B_1} \\
&\otimes e^{i2\pi 4x_2/2^{10}} |f_{22}(x_2 \oplus b_{22})\rangle_{B_2} e^{i2\pi 23x_2/2^{10}} |x_2 \oplus b_{23}\rangle_{B_3} \\
&\otimes \sum_{x_3=0}^{2^{10}-1} \frac{1}{\sqrt{2^{10}}} |x_3\rangle_A e^{i2\pi 14x_3/2^{10}} |x_3 \oplus b_{31}\rangle_{B_1} \\
&\otimes e^{i2\pi 6x_3/2^{10}} |x_3 \oplus b_{32}\rangle_{B_2} |x_3 \oplus b_{33}\rangle_{B_3} \\
&\otimes \sum_{x_4=0}^{2^{10}-1} \frac{1}{\sqrt{2^{10}}} |x_4\rangle_A |x_4 \oplus b_{41}\rangle_{B_1} |x_4 \oplus b_{42}\rangle_{B_2} |x_4 \oplus b_{43}\rangle_{B_3} \\
&\otimes \sum_{x_5=0}^{2^{10}-1} \frac{1}{\sqrt{2^{10}}} |x_5\rangle_A |x_5 \oplus b_{51}\rangle_{B_1} |x_5 \oplus b_{52}\rangle_{B_2} |x_2 \oplus b_{53}\rangle_{B_3},
\end{aligned} \tag{15}$$

where let $a_{11} = 33$, $a_{21} = 79$, $a_{31} = 14$, $a_{12} = 13$, $a_{22} = 4$, $a_{32} = 6$, $a_{13} = 7$, and $a_{23} = 23$. Each value is randomly selected by each bidder.

Here, all the bidders' states are sent to Alice in Step 3, and unnecessary entanglement is removed in Step 4. After Step 4, the state becomes

$$\begin{aligned}
&\sum_{x_1=0}^{2^{10}-1} \frac{1}{\sqrt{2^{10}}} e^{i2\pi 53x_1/2^{10}} |x_1\rangle_A |f_{11}(x_1 \oplus b_{11}) \oplus x_1\rangle_{B_1} \\
&\otimes |f_{12}(x_1 \oplus b_{12}) \oplus x_1\rangle_{B_2} |f_{13}(x_1 \oplus b_{13}) \oplus x_1\rangle_{B_3} \\
&\otimes \sum_{x_2=0}^{2^{10}-1} \frac{1}{\sqrt{2^{10}}} e^{i2\pi 106x_2/2^{10}} |x_2\rangle_A |f_{21}(x_2 \oplus b_{21}) \oplus x_2\rangle_{B_1} \\
&\otimes |f_{22}(x_2 \oplus b_{22}) \oplus x_1\rangle_{B_2} |b_{23}\rangle_{B_3} \\
&\otimes \sum_{x_3=0}^{2^{10}-1} \frac{1}{\sqrt{2^{10}}} e^{i2\pi 20x_3/2^{10}} |x_3\rangle_A |b_{31}\rangle_{B_1} |b_{32}\rangle_{B_2} |b_{33}\rangle_{B_3} \\
&\otimes \sum_{x_4=0}^{2^{10}-1} \frac{1}{\sqrt{2^{10}}} |x_4\rangle_A |b_{41}\rangle_{B_1} |b_{42}\rangle_{B_2} |b_{43}\rangle_{B_3} \\
&\otimes \sum_{x_5=0}^{2^{10}-1} \frac{1}{\sqrt{2^{10}}} |x_5\rangle_A |b_{51}\rangle_{B_1} |b_{52}\rangle_{B_2} |b_{53}\rangle_{B_3}.
\end{aligned} \tag{16}$$

Finally, a quantum Fourier transform is executed in order to obtain the information of the maximum number of digits in Step 5. After Step 5, the state becomes

$$\begin{aligned}
&\sum_{y_1=0}^{2^{10}-1}\sum_{x_1=0}^{2^{10}-1}\frac{1}{2^{10}}e^{i2\pi(53-y_1)x_1/2^{10}}|y_1\rangle_A|f_{11}(x_1\oplus b_{11})\oplus x_1\rangle_{B_1}\\
&\quad\otimes|f_{12}(x_1\oplus b_{12})\oplus x_1\rangle_{B_2}|f_{13}(x_1\oplus b_{13})\oplus x_1\rangle_{B_3}\\
&\quad\otimes\sum_{y_2=0}^{2^{10}-1}\sum_{x_2=0}^{2^{10}-1}\frac{1}{2^{10}}e^{i2\pi(106-y_2)x_2/2^{10}}|y_2\rangle_A|f_{21}(x_2\oplus b_{21})\oplus x_2\rangle_{B_1}\\
&\quad\otimes|f_{22}(x_2\oplus b_{22})\oplus x_1\rangle_{B_2}|b_{23}\rangle_{B_3}\\
&\quad\otimes|20\rangle_A|b_{31}\rangle_{B_1}|b_{32}\rangle_{B_2}|b_{33}\rangle_{B_3}\\
&\quad\otimes|0\rangle_A|b_{41}\rangle_{B_1}|b_{42}\rangle_{B_2}|b_{43}\rangle_{B_3}\\
&\quad\otimes|0\rangle_A|b_{51}\rangle_{B_1}|b_{52}\rangle_{B_2}|b_{53}\rangle_{B_3}.
\end{aligned}\tag{17}$$

Then, the auctioneer Alice can know that the bidders' maximum number of digits is 3 by observing her states in Step 6 because the maximum suffix I corresponding to the non-zero observation values is 3. In addition, she cannot obtain any useful information of the states smaller than I.

Similarly, she can also obtain the highest value for each digit of all the bidders' bid prices by applying B-QSBP for $L = 10$ (i.e., $\mathbf{L} = \{0, 1, 2, \ldots, 9\}$). For example, for the third digit, $\mathbf{S}_2 = \{2\}$, $\mathbf{S}_1 = \{1\}$, $\mathbf{S}_0 = \{3\}$, and all the remaining sets are empty sets because three bidders B_1, B_2, and B_3 consider bidding at prices of \$115, \$202, and \$98, respectively. Then, the protocol B-QSBP is executed in the same manner as described above, except that new b_{ik}, a_{jk} and f_{ik} are generated from a security point of view.

3 Proposed quantum sealed-bid auction protocol

The procedure of sealed-bid auction is executed in the following way. First, each bidder bids a price without revealing his/her price to other bidders. In addition, this is executed anonymously. And then, the auctioneer chooses the bidder bidding the highest bid price as the winning bidder. In this section, we construct a quantum sealed-bid auction protocol with entanglement. Bidders' bid prices are embedded in the phases of quantum entangled states and are sent to Alice.

Step 1 Each bidder $B_k \in \{B_1, B_2, \ldots, B_m\}$ sends his/her bid information BID_k to Alice (and/or to other bidders if needed), where the content of BID_k includes B_k's bid price, B_k's signature, and so on. In addition, BID_k is encrypted and/or is shared among the other legitimate parties by using secret sharing.

Step 2 Find the maximum number of digits for all the bid prices:

Step 2-1 Alice, $B_1, \ldots,$ and B_m share entanglement

$$\bigotimes_{i=1}^{L}\sum_{x_i=0}^{2^{n_i}-1}\frac{1}{\sqrt{2^{n_i}}}|x_i\rangle_A|x_i\rangle_{B_1}\otimes\cdots\otimes|x_i\rangle_{B_m}\tag{18}$$

beforehand, where L is the maximum expected number of digits for all the bid prices.

Step 2-2 The legitimate parties execute the protocol B-QSBP in order to obtain the maximum number of digits for all the bid prices. When Alice does not know the maximum expected number of digits at the start, by interpreted as having the number of digits larger than L if a positive value is obtained in the procedure corresponding to the state $|x_L\rangle$, the legitimate parties repeat the procedure with a larger value for L, and obtain the maximum number of digits.

Step 3 Repeat the following two steps from the highest digit to the lowest digit in order to find the highest bid price:

Step 3-1 The legitimate parties share entanglement

$$\bigotimes_{i=0}^{9}\sum_{x_i=0}^{2^{n_i}-1}\frac{1}{\sqrt{2^{n_i}}}|x_i\rangle_A|x_i\rangle_{B_1}\otimes\cdots\otimes|x_i\rangle_{B_m}\tag{19}$$

beforehand.

Step 3-2 The legitimate parties execute the protocol B-QSBP for each bid digit from the highest digit to the lowest digit in order to find the highest value for each digit. As Alice discloses the value for each procedure, every bidder can know the highest bid price sequentially from the highest digit.

In this repetition, each bidder executes only Step 2-1 in Step 2 of B-QSBP from the time when he/she knows that his/her bid price is lower than the bid price of other bidders.

Step 4 Alice formally announces the highest bid price to the bidders although the bidders already know it at this point. The winner $B_w(w \in \{1, 2, \ldots, m\})$ discloses his/her BID_w, and Alice (and the other bidders) confirms whether it is correct.

This proposed protocol can be used when the bid price range is unknown, or when the number of possible bid prices is large. If there are only N different bid prices for small N, the legitimate parties can just execute the following procedure.

First, the state in Step 2 is

$$\bigotimes_{i=1}^{N} \sum_{x_i=0}^{2^{n_i}-1} \frac{1}{\sqrt{2^{n_i}}} |x_i\rangle_A |x_i\rangle_{B_1} \otimes \cdots \otimes |x_i\rangle_{B_m}. \tag{20}$$

This state is the same state as the state in Step 2. However, since N has a different meaning from L, we rewrite again. In this case, $|x_i\rangle (i \in \{1, 2, \ldots, N\})$ is the state corresponding to the ith bid price (The larger the number, the higher the price). Here, each bidder B_k executes Step 2 of B-QSBP as $a_{jk} = 1$ for $k \in \mathbf{S}_j$ and a random $a_{j'k}$ for $j' \in \{1, 2, \ldots, j-1\}$. Then, the observed value corresponding to I in Step 6 of B-QSBP becomes the number of bidders bidding the highest bid price.

Moreover, we consider executing this protocol for $N = 1$. The auctioneer announces a bid price and each bidder uses this protocol in order to bid at the price, i.e., each bidder represents willingness to bid for that price. Furthermore, they repeat the protocol up to the highest price. Therefore, we will be also able to use this restricted protocol as English auction and Dutch auction.

4 Security of our proposed protocol

If all the legitimate parties are honest, this protocol can be obviously executed correctly. If the winning bidder does not give his/her name to the auctioneer in Step 4 of Sect. 3, this auction becomes the failure. Any information is not leaked to an outside attacker even if the auctioneer and the attacker collude because quantum entangled states are securely shared and the information that the auctioneer can obtain is only the information disclosed to bidders, i.e., the highest value in each step is only disclosed.

Here, we consider the following properties.

- Anonymity: No one can obtain the private bid price of each bidder except the winning bid.
- Public Verifiability: When the winner is announced, anyone can verifies the information of winner's bid.
- Fairness: The auctioneer cannot help a malicious bidder to win the auction illegally without being found by other bidders.
- Traceability: The winning bidder and the highest bid price can be verified even the auction has finished.

(1) Anonymity

First, if each legitimate party does not know all the others' random values a_{jk}, it is impossible to determine whether there exist bid prices corresponding to the suffixes except I because the observed phase values are random values. Therefore, bid price information cannot be obtained by the auctioneer Alice alone or by each bidder alone. In addition, any outside attacker cannot also obtain any information of random values a_{jk} in alone or in collusion with Alice because of entanglement.

Next, we consider that some legitimate bidders collude. Alice discloses only the highest bid price in each protocol, Therefore, each bidder cannot obtain any other information even if all the bidders collude because Alice does not disclose the observed phase values in each protocol.

Finally, we consider that Alice and some legitimate bidders collude. As an attack method, first, Alice discloses each observed phase value to the the malicious bidders, and each malicious bidder subtracts his/her own random value from the value by using secure computation. The final value is the sum of honest bidders' random values. If there are multiple honest bidders, it is unknown who bid at that corresponding suffix. In addition, even if there is only one honest bidder, only a part of information will be leaked because he/she executes only Step 2-1 in Step 2 of B-QSBP from the time when he/she knows that his/her bid price is lower than the bid price of other bidders. In the first place, however, having only one honest bidder would not be a legitimate auction. Moreover, as mentioned at the end of Sect. 2.1, if it is sequentially sent to Alice from the highest value L to the lowest value 1 and is executed in each case, only the phase corresponding to the subscript I is obtained, and this attack can be avoided.

(2) Public verifiability

The bid price of each bidder B_k is sent to Alice (and/or to other bidders if needed) as BID_k beforehand. Therefore, legitimate parties can verify whether it is the winning bid.

(3) Fairness

Let's consider that the auctioneer and/or some malicious bidders cheat. If some bidders do not execute the correct procedure in Step 2 or Step 3 of Sect. 3, the incorrect bid price may become the highest bid price. However, the bidder bidding the highest bid price can make a complaint by using BID_k together with public verifiability.

(4) Traceability
The procedure is open to the public, and legitimate parties give also BID_k in this case. Therefore, the information of winning bidder can be verified even the auction has finished.

5 Conclusions

In this electronic society, it is important to realize various processes on the Internet. In addition, the security on the Internet for commercial transactions is also important. Recently, various quantum protocols for sealed-bid auction are also proposed. In this paper, we proposed a different type of quantum sealed-bid auction using the phases of quantum entangled states as bids. An auctioneer and bidders share entanglement with each other beforehand. Each bidder can send his/her bid prices safely by converting his/her bid prices to phases of quantum entangled states. No one can know the values of the phases unless a bidder knows all the quantum entangled states. Thus, we constructed a secure quantum protocol taking advantage of this property, and then the auctioneer can retrieve only the highest bid price.

Our proposed protocol uses a huge amount of entanglement. In fact, our protocol needs entanglement shown in Eq. (1). Namely, each step of our protocol requires L entangled states among the legitimate parties, where L is either the maximum expected number of digits in bid price or 10 for decimal number. Currently, it is difficult to control entanglement, so our protocol may not be practical at present. However, since nobody knows what future technological progress will be, we believe that theoretically proposing secure protocols is also an important part of our research. For more details on quantum entanglement research including the construction of multipartite entanglement, see, e.g., a review paper [18] and references therein. However, if certain restrictions such as the range of bid prices or the number of legitimate parties are placed on an auction in advance, it might be possible to construct quantum entanglement more efficiently according to them.

We use B-QSBP, the protocol in Sect. 2, as a tool of finding the highest bid price. However, we may be able to modify this protocol to a protocol to find some values that meet a certain condition, or to a protocol to count the number of each information according to the conditions such as election candidate. Thus, we hope that this protocol can be used as a basic technology for sending information anonymously.

Funding The author did not receive support from any organization for the submitted work.

Data Availibility Statement No Data associated in the manuscript.

Declarations

Conflict of interest The author has no relevant financial or non-financial interests to disclose.

References

1. M.A. Nielsen, I.L. Chuang, *Quantum Computation and Quantum Information* (Cambridge Univ. Press, Cambridge, 2000)
2. P.W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. **26**, 1484 (1997)
3. L.K. Grover, A fast quantum mechanical algorithm for database search, in *Proc. of the 28th ACM Symposium on Theory of Computing*, vol. 212 (ACM Press, New York, 1996)
4. C.H. Bennett, G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proc. of IEEE Int. Conf. on Computers, Systems and Signal Processing*, Bangalore, India, vol. 175 (1984)
5. G. Ekert, Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. **67**, 661 (1991)
6. B.A. Shaw, T.A. Brun, Quantum steganography with noisy quantum channels. Phys. Rev. A **83**, 022310 (2011)
7. T. Mihara, Quantum steganography using prior entanglement. Phys. Lett. A **379**, 952 (2015)
8. T. Mihara, Multi-party quantum steganography. Int. J. Theor. Phys. **56**, 576 (2017)
9. M. Naseri, Secure quantum sealed-bid auction. Opt. Commun. **282**, 1939 (2009)
10. P. Asagodu, K. Thapliyal, A. Pathak, Quantum and semi-quantum sealed-bid auction: vulnerabilities and advantages. Quantum Inf. Process. **21**, 185 (2022)
11. R. Zhang, R.-H. Shi, J.-Q. Qin, Z.-W. Peng, An economic and feasible quantum sealed-bid auction protocol. Quantum Inf. Process. **17**, 35 (2018)
12. Q. Wang, R.-H. Shi, Z.-K. Chen, S.-L. Wang, A quantum sealed auction protocol based on secret sharing. Int. J. Theor. Phys. **58**, 1128 (2019)
13. J.-T. Wang, Y. Pan, W. Liu, Z.-Z. Li, Quantum sealed-bid auction protocol based on quantum secret sharing. Quantum Inf. Process. **21**, 278 (2022)
14. R.-H. Shi, M. Zhang, Privacy-preserving quantum sealed-bid auction based on Grover's search algorithm. Sci. Rep. **9**, 1 (2019)
15. R.-H. Shi, Y.-F. Li, A feasible quantum sealed-bid auction scheme without an auctioneer. IEEE Trans. Quantum Eng. **3**, 2100212 (2022)
16. H.-K. Lo, H.F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances. Science **283**, 2050 (1999)
17. C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, W.K. Wootters, Mixed-State entanglement and quantum error correction. Phys. Rev. A **54**, 3824 (1996)
18. N. Friis, G. Vitagliano, M. Malik, M. Huber, Entanglement certification from theory to experiment. Nat. Rev. Phys. **1**, 72 (2019)