SCIENTIFIC REPORTS

OPEN

Privacy-preserving Quantum Sealed-bid Auction Based on Grover's Search Algorithm

Received: 3 February 2019
Accepted: 27 April 2019
Published online: 20 May 2019

Run-hua Shi[1,2] & Mingwu Zhang[1]

Sealed-bid auction is an important tool in modern economic especially concerned with networks. However, the bidders still lack the privacy protection in previously proposed sealed-bid auction schemes. In this paper, we focus on how to further protect the privacy of the bidders, especially the non-winning bidders. We first give a new privacy-preserving model of sealed-bid auction and then present a quantum sealed-bid auction scheme with stronger privacy protection. Our proposed scheme takes a general state in N-dimensional Hilbert space as the message carrier, in which each bidder privately marks his bid in an anonymous way, and further utilizes Grover's search algorithm to find the current highest bid. By $O(ln)$ iterations, it can get the highest bid finally. Compared with any classical scheme in theory, our proposed quantum scheme gets the lower communication complexity.

Nowadays, quantum computations and quantum communications[1] have received extensive attention and gained lots of promising achievements, e.g., quantum cryptography[2], quantum teleportation[3] and quantum artificial intelligence[4,5].

Early 70s in the last century, Stephen Wiesner first presented the idea of quantum cryptography (e.g., quantum money). However, unfortunately, his innovative idea could not be immediately accepted at that time. Until 1984, C. H. Bennett and G. Brassard[6] revived the research of quantum cryptography by presenting famous quantum key distribution (QKD) protocol, later called BB84 protocol.

The security of quantum cryptography is guaranteed by the physical principles of quantum mechanics, so it can provide unconditional security in theory. Since Bennett and Brassard presented the first quantum key distribution (i.e., BB84 QKD) protocol, quantum cryptography has been widely studied and rapidly developed. Nowadays, many results have been reported, such as quantum secret sharing[7], quantum secure direct communication[8–10], quantum encryption[11], quantum signature[12–14], quantum authentication[15,16], and blind quantum computation[17,18].

In addition, there are also many well-known issues involving the protection of privacy in classical setting such as electronic voting, electronic auction, electronic payment, and so on. Furthermore, these issues have also been studied extensively in quantum setting, and accordingly there have appeared the corresponding quantum protocols, such as quantum voting[19], quantum auction[20], quantum e-payment[21], and so on.

In this paper, we focus on quantum auction, especially a specific type of quantum auction, i.e., quantum sealed-bid auction (QSA). In currently existing QSA schemes, there is only one winning bidder, who will win the auction finally, but the auctioneer needs to know all bids of all bidders, including the non-winning bidders. That is, even if the non-winning bidder cannot win the auction, he still needs to privately send his bid to the auctioneer. In certain settings, these QSA schemes do not meet the higher secure requirements, because the non-winning bidders lack the privacy protection, which has been the focus of everyone's attention in modern society. In this paper, we mainly consider how to further protect the privacy of the non-winning bidders in QSA.

Related Works

Electronic auction plays an important role in modern economy especially concerned with networks. Generally, electronic auction can be mainly classified into three categories: English auction, Dutch auction and Sealed-bid auction. The traditional English auction is a public ascending price auction. In this auction, the auctioneer first gives a base price, and then some bidder bids a higher price than the base price. Furthermore, the next bidder

[1]School of Computer Science, Hubei University of Technology, Wuhan City, 430068, China. [2]School of Control and Computer Engineering, North China Electric Power University, Beijing City, 102206, China. Correspondence and requests for materials should be addressed to R.-h.S. (email: rhshi@ncepu.edu.cn) or M.Z. (email: mzhang@hbut.edu.cn)

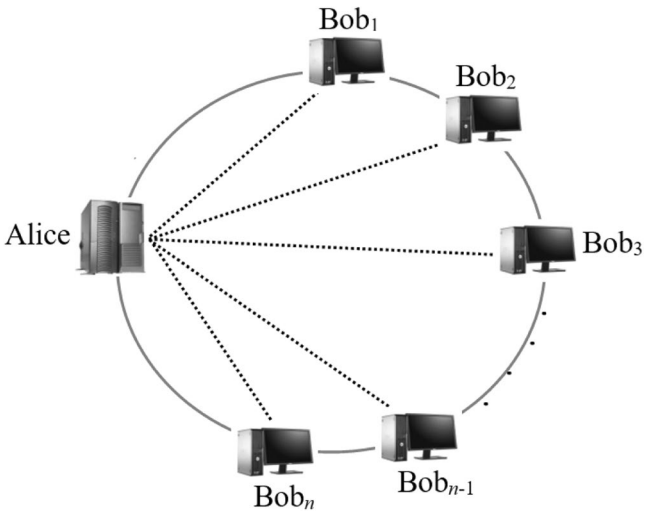

Figure 1. A system model of QAS.

outbids the last bidder, and the process continues until no one else bids a higher price. Finally, the item is sold to the highest bidder at the highest bid. On the contrary, the Dutch auction is a public descending price auction. The auctioneer in Dutch auction begins with a high asking price which is lowered until some bidder is willing to accept the auctioneer's price. Difference from the former two auctions, the sealed-bid auction needs to protect the privacy of the bids and ensure the fairness among the bidders. That is, any eavesdropper cannot get any private information about the bids, and the auctioneer cannot help any bidder to win the auction unfairly. During traditional sealed-bid auction, the bidder does not know the bids of others. After all bids are transmitted privately to the auctioneer, the auctioneer selects out the highest bid and announces it and the corresponding winner.

The first quantum sealed-bid auction protocol was proposed by Naseri in 2009[20]. The auction protocol introduced a multi-party quantum secure direct communication protocol to privately transmit the bids. However, Qin *et al.*[22] and Yang *et al.*[23] independently pointed out that there was a secure flaw in Naseri' protocol, i.e., a malicious bidder could obtain all private bids without being found by performing double Controlled NOT attack or using fake entangled particles. Then they improved Naseri's original protocol by inserting some decoy particles into the transmitted particles. In addition to the detecting strategy of the decoy particles, there still appeared other defense strategies[24,25] to prevent these attacks. Furthermore, Zhao *et al.*[26] found that these previously proposed protocols were unfair, i.e., a malicious bidder could collude the dishonest auctioneer to perform a collusion attack to win the auction unfairly. Accordingly, they presented a security protocol for QSA with post-confirmation[26]. Subsequently, in order to enhance the security of QSA or ensure the feasibility of QSA, many quantum protocols with post-confirmation were proposed[27–33]. In 2017, we presented an economic and feasible quantum sealed-bid auction protocol based on single photons in both the polarization and the spatial-mode degrees of freedom[34]. In our protocol, the post-confirmation mechanism uses single photons instead of entangled EPR pairs, and it does not require quantum memory. Therefore, our protocol is a practical and feasible quantum sealed-bid auction.

In all previously proposed quantum sealed-bid auction (QSA) protocols, it requires all bidders to send their real bids to the auctioneer. Even if the bidder can not win the auction, the auctioneer also knows his or her real bid. However, in practical settings, the bidders who will not be able to win the auction don't want to reveal their real bids. That is, the non-winning bidders lack the privacy protection in current QSA schemes. In this paper, we present a strong privacy-preserving QSA model. In our model, anyone cannot get the real bid of other bidders, even for the auctioneer. So the privacy of the bidders can be better protected in our model. In addition, the bids of the bidders are anonymous, i.e., no one can discern who these bids belong to. Furthermore, we design a novel privacy-preserving QSA scheme based on Grover's search algorithm. The proposed scheme not only guarantees the correctness and fairness of the auction, but also ensures the privacy and anonymity of the bidders, even for the auctioneer. Compared with the current existing quantum sealed-bid auction, our proposed scheme can provide stronger privacy protections, which are urgently requirements in modern network society.

Results and Discussion

Privacy-preserving quantum sealed-bid auction. *System model.* Here we first present our system model for privacy-preserving quantum sealed-bid auction (PQSA), in which there are two kinds of participants, i.e., an auctioneer (Alice) who wants to sell an item at the highest possible price and n bidders (Bob_1, Bob_2, …, Bob_n) who want to buy the item alone at the lowest possible price. In our PQAS model, suppose that there is a circle quantum channel among the auctioneer and all bidders (see the solid line in Fig. 1) and there is a classical channel between any two participants (see the dashed line in Fig. 1).

Initially, Alice has a valuation price (x) of the item, and each bidder (Bob_i) has a private bid (x_i) for the item. Furthermore, we assume that the valuation price and all bids are not changed during the whole auction. Finally, Alice can select out the highest bid. If the highest bid is greater than or equal to her initial valuation price, then she will announce the winner and the highest bid. Otherwise, she will declare the failure to all bidders. In addition, our PQSA should meet the following secure and privacy requirements:

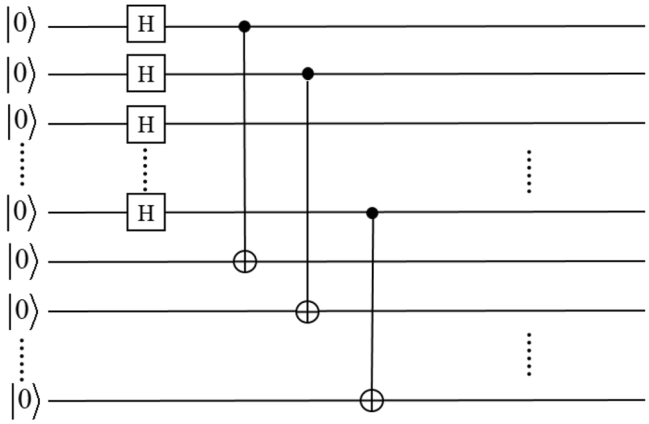

Figure 2. Quantum circuit for the preparation of the initial state.

The auctioneer's privacy: All bidders can not get any private information about the auctioneer's initial valuation price (x) before announcing the winner or the failure of the auction.

The bidder's privacy: No one can get the private bid of the bidder without risking the auctioneer's detection.

Anonymity: The bidder's bid is anonymous for all participants, including the auctioneer. That is, even if a dishonest participant or an outsider attacker gets a bid, he or she cannot identify whose bid it is.

Public verifiability: When the winner is announced, anyone can verify the authenticity of the winning bid. This attribute can defend the collusion attack between the malicious bidder and the dishonest auctioneer.

Fairness: The auctioneer cannot help a malicious bidder to win the auction illegally without being found by other bidders.

Proposed scheme. In the following scheme, we mainly consider the honest-but-curious model, which is similar to the semi-honesty model in the classical setting. That is, the parties honestly execute the protocol, but they try to find out as much as possible about the other inputs despite following the protocol. Furthermore, suppose that the initial valuation price and all bids lie in $Z_N = \{0, 1, 2, \ldots, N-1\}$. For simplicity, we assume that all bids are distinct. In addition, we assume that there is a public hash $H(\cdot)$.

Step 1. Each bidder Bob_j $(j = 1, 2, \ldots, n)$ randomly selects an integer $r_j \in Z_N$ and computes $b_j = H(r_j \oplus H(r_j \oplus x_j))$. Then the bidder Bob_j sends b_j to all other participants by the classical channel. That is, the bidder Bob_j commits x_j to all other participants, but no participant can get x_j only from b_j without r_j. In addition, the auctioneer Alice also needs to commit x to all bidders, i.e., she selects a random number $r \in Z_N$, computes $b = H(r \oplus H(r \oplus x))$ and sends b to all bidders by the classical channel.

Step 2. Repeat the following procedures $p + q$ times, including the normal procedure (to find the highest bid) p times and the test procedure (to detect the dishonesty or attacks) q times, where $p = \ln n$, and q is a secure parameter, e.g., $q = p$. That is, Alice randomly selects to execute the following normal procedure with the probability of $\frac{p}{p+q}$ or the following test procedure with the probability of $\frac{q}{p+q}$.

The normal procedure: (1.1) Alice first prepares a general state $|\psi\rangle_h = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle_h$ and a basis state $|0\rangle_t$, which are both log$N$ qubits. Furthermore, Alice performs log$N$ CNOT gate operators[35] on the product state $|\psi\rangle_h|0\rangle_t$, where each qubit of the first log$N$ qubits is the control qubit and the corresponding qubit of the second log$N$ qubits is the target qubit (see Fig. 2). Here we call the resultant state $|\psi_0\rangle$, which is written as

$$\begin{aligned} |\psi_0\rangle &= CNOT^{\otimes \log N}|\psi\rangle_h|0\rangle_t \\ &= CNOT(1,\ \log N + 1) \otimes CNOT(2,\ \log N + 2)\ldots \\ &\quad \otimes CNOT(\log N,\ 2\log N)\left(\frac{1}{\sqrt{N}}\sum_{i+0}^{N-1}|i\rangle_h|0\rangle_t\right) \\ &= \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle_h|i\rangle_t. \end{aligned} \tag{1}$$

Clearly, $|\psi_0\rangle$ is an entangled state. Here, the subscript h and t denote two registers, where the register h will stay at home and the register t will be transmitted through the quantum channel. Then Alice sends the register t to the first bidder Bob_1 through the quantum channel.

(1.2) After receiving the register t, the bidder Bob_1 prepares a basis state $|0\rangle$ in an auxiliary register, and applies an oracle operator U_{Bob_1} to the register t and the auxiliary register, where the oracle operator U_{Bob_1} is defined by

$$U_{Bob_1}: \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle_t \otimes |0\rangle \rightarrow \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle_t|0 \oplus f(i, x_1)\rangle, \tag{2}$$

with

$$f(i, x_1) = \begin{cases} 1 & if\ i = x_1 \\ 0 & else \end{cases}. \tag{3}$$

Let $|\psi_1\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle_h|i\rangle_t|f(i, x_1)\rangle$ (i.e., the state of the whole quantum system). Obviously, $|\psi_1\rangle = \frac{1}{\sqrt{N}}[|x_1\rangle_h|x_1\rangle_t|1\rangle + \sum_{i\neq x_1}|i\rangle_h|i\rangle_t|0\rangle]$. That is, the oracle operator U_{Bob_1} is utilized to mark the item x_1.

(1.3) Furthermore, the bidder Bob_1 sends the two registers (i.e., $\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle_t|f(i, x_1)\rangle$) to the second bidder Bob_2 through the quantum channel.

(1.4) After receiving $\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle_t|f(i, x_1)\rangle$, similarly, the bidder Bob_2 applies an oracle operator U_{Bob_2} to $\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle_t|f(i, x_1)\rangle$, where the oracle operator U_{Bob_2} is defined by his bid x_2 as follows:

$$U_{Bob_2}: \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle_t|f(i, x_1)\rangle \rightarrow \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle_t|f(i, x_1) \oplus f(i, x_2)\rangle, \tag{4}$$

with

$$f(i, x_2) = \begin{cases} 1 & if\ i = x_2 \\ 0 & else \end{cases}. \tag{5}$$

Let $|\psi_2\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle_h|i\rangle_t|f(i, x_1) \oplus f(i, x_2)\rangle$. Furthermore, the bidder Bob_2 sends two transmitted registers (i.e., $\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle_t|f(i, x_1) \oplus f(i, x_2)\rangle$) to the next bidder Bob_3 though the quantum channel. Afterward, the bidder Bob_3 executes the similar process of the bidder Bob_2, and so on. This process is repeated n times in total, so that every bidder has marked his bid by an oracle operator. Then, the final quantum state will be in

$$\begin{aligned} |\psi_n\rangle &= \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle_h|i\rangle_t|f(i, x_1) \oplus f(i, x_2) \oplus \cdots \oplus f(i, x_n)\rangle \\ &= \frac{1}{\sqrt{N}}\Big[\sum_{i\notin\{x_1,x_2,\ldots x_n\}}|i\rangle_h|i\rangle_t|0\rangle + \sum_{j\in\{x_1,x_2,\ldots x_n\}}|j\rangle_h|j\rangle_t|1\rangle\Big] \end{aligned}. \tag{6}$$

(1.5) Finally, the bidder Bob_n sends all remaining qubits of the marked state $|\psi_n\rangle$ back to the auctioneer Alice through the quantum channel.

(1.6) After receiving the whole state $|\psi_n\rangle$, Alice again applies $\mathrm{CNOT}^{\otimes \log N}$ on two registers h and t, i.e., the first $2\log N$ qubits of $|\psi_n\rangle$, where each qubit of the first $\log N$ qubits is the control qubit and the corresponding qubit of the second $\log N$ qubits is the target qubit. Call the resultant state $|\widetilde{\psi}\rangle_n$. That is,

$$\begin{aligned} |\widetilde{\psi}\rangle_n &= CNOT^{\otimes \log N}|\psi_n\rangle \\ &= CNOT^{\otimes \log N}[\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle_h|i\rangle_t|f(i, x_1) \oplus f(i, x_2) \oplus \cdots \oplus f(i, x_n)\rangle] \\ &= \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle_h|0\rangle_t|f(i, x_1) \oplus f(i, x_2) \oplus \cdots \oplus f(i, x_n)\rangle. \end{aligned} \tag{7}$$

(1.7) Furthermore, Alice measures the second register t, i.e., the second $\log N$ qubits of the whole quantum system, in the computational basis. If the measured result is $|0\rangle$, then she will continue to execute the next step; Otherwise she will believe that there is at least one dishonest bidder or outsider attacker and end this auction.

(1.8) Let $|\phi_n\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle_h|f(i, x_1) \oplus f(i, x_2) \oplus \cdots \oplus f(i, x_n)\rangle$. Alice prepares another auxiliary state $|0\rangle$, and then applies an oracle operator U_{Alice} to $|\phi\rangle_n \otimes |0\rangle$, where the oracle operator U_{Alice} is defined by

$$f_1(i, x_1, \ldots, x_n) = f(i, x_1) \oplus f(i, x_2) \oplus \cdots \oplus f(i, x_n), \tag{8}$$

$$U_{Alice}: \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle_h|f_1(i, x_1, \ldots, x_n)\rangle \otimes |0\rangle \rightarrow \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle_h|f_1(i, x_1, \ldots, x_n)\rangle|0 \oplus f_2(i, x)\rangle, \tag{9}$$

with

$$f_2(i, x) = \begin{cases} 1 & if\ f_1(i, x_1, \ldots, x_n) = 1\ and\ i \geq x \\ 0 & else \end{cases}. \tag{10}$$

Let $|\phi_A\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle|f_1(i, x_1, \ldots, x_n)\rangle|f_2(i, x)\rangle$. Please note that the subscript h is omitted in $|\phi_A\rangle$, because all qubits are held by Alice at this moment. Clearly,

$$\begin{aligned} |\phi_A\rangle &= \frac{1}{\sqrt{N}}\Big[\sum_{i\notin\{x_1,x_2,\ldots x_n\}}|i\rangle|0\rangle|0\rangle + \sum_{j\in\{x_1,x_2,\ldots x_n\}\wedge j<x}|j\rangle|1\rangle|0\rangle \\ &\quad + \sum_{j\in\{x_1,x_2,\ldots x_n\}\wedge j\geq x}|j\rangle|1\rangle|1\rangle\Big] \end{aligned}. \tag{11}$$

(1.9) Alice applies the Grover's search algorithm[36] to $|\phi_A\rangle$ for finding a marked state $|j\rangle|1\rangle|1\rangle$, which implies $j \in \{x_1, x_2 \ldots, x_n\}$ and $j \geq x$ (i.e., finding a bid x_i greater than or equal to x). Alice makes a measurement on the first register. Let the result of the measurement be y. If $y > x$ and satisfy $|y\rangle|1\rangle|1\rangle$), then replace x with y.

The test procedure: (2.1) Alice first prepares a quantum state $|\psi\rangle_h = \frac{|0\rangle_h + |i\rangle_h}{\sqrt{2}}$, where $i \notin \{x_1, x_2 \ldots, x_n\}$ (Note. i may be selected by Alice's experience and the valuation price, e.g., i could be a large enough number in Z_N^*), and another quantum basis state $|0\rangle_t$. Similarly, Alice further performs log$N$ CNOT gate operators on the product state $|\psi\rangle_h|0\rangle_t$ to generate an entangled state $|\psi_0\rangle = \frac{|0\rangle_h|0\rangle_t + |i\rangle_h|i\rangle_t}{\sqrt{2}}$. Here the subscript h and t denote two registers, where the register h will stay at home and the register t will be transmitted through the quantum channel. Then Alice sends the register t to the first bidder Bob_1 through the quantum channel.

(2.2) All bidders cannot distinguish the quantum states from the normal procedure and the test procedure, so they continue to execute the same oracle operators as the normal procedure (i.e., (1.2–1.5)) to mark their respective bids in the transmitted quantum state $|\psi_i\rangle$. However, $i \notin \{x_1, x_2 \ldots, x_n\}$, so $|\psi_n\rangle = \frac{|0\rangle_h|0\rangle_t + |i\rangle_h|i\rangle_t}{\sqrt{2}}|0\rangle$. Finally, the bidder Bob_n sends all remaining qubits of the state $|\psi_n\rangle$ back to the auctioneer Alice through the quantum channel.

(2.3) After receiving the state $|\psi_n\rangle$, Alice again applies $\mathrm{CNOT}^{\otimes \log N}$ on two registers h and t, i.e., the first 2log$N$ qubits of $|\psi_n\rangle$, where each qubit of the first log$N$ qubits is the control qubit and the corresponding qubit of the second log$N$ qubits is the target qubit. Then Alice should get $|\psi_n^*\rangle = \frac{|0\rangle_h + |i\rangle_h}{\sqrt{2}}|0\rangle_t|0\rangle$.

(2.4) Furthermore, Alice measures the first register by a von Neumann measurement $\{P_{+i}, P_{-i}\}$, where P_{+i} and P_{-i} are defined by[37],

$$P_{+i} = \frac{1}{2}(|0\rangle\langle 0| + |0\rangle\langle i| + |i\rangle\langle 0| + |i\rangle\langle i|), \tag{12}$$

$$P_{-i} = \frac{1}{2}(|0\rangle\langle 0| - |0\rangle\langle i| - |i\rangle\langle 0| + |i\rangle\langle i|). \tag{13}$$

Obviously, $P_{+i} + P_{-i} = I$ and $P_{+i}P_{-i} = 0$. If the measurement result is in $\frac{|0\rangle_h + |i\rangle_h}{\sqrt{2}}$, then she will further measure the latter two registers in computational basis. If three measurement results are in $\frac{|0\rangle_h + |i\rangle_h}{\sqrt{2}}$, $|0\rangle_t$ and $|0\rangle$, respectively, then she will continue to execute the next step. Otherwise Alice will believe that there is at least one dishonest bidder or outsider attacker and end this auction.

Step 3. After executing the procedures of Step 2 $(p + q)$ times, including the normal procedure p times and the test procedure q times, if the return result y is greater than or equal to her initial valuation price, Alice will announce y, i.e., the current highest bid ($y \in \{x_1, x_2, \ldots, x_n\}$). Otherwise Alice will open her commitment x (i.e., the initial valuation price) by opening the random number r simultaneously, declare the failure of the auction and terminate this auction. That is, there is not a bid greater than or equal to her initial valuation price, so this auction is fail. Of course, all participants may verify its truth by comparing $H(r \oplus H(r \oplus x))$ with the corresponding value b committed in Step 1.

Step 4. If there is a bid x_j greater than the current highest bid y, the bidder Bob_j will broadcast a complaint about the incorrectness of the current highest bid. Furthermore, if there is a complaint, Alice will ask for the bid of the complainer, and then she will update the current highest bid with it. But if there are two or more complaints, Alice will think there are dishonest bidders or outsider attackers and accordingly terminate this auction.

Step 5. Furthermore, if each bidder does not further receive any complaint, then he will believe that the current highest bid is highest. Suppose $y = x_k$, i.e., the bidder Bob_k should be the winner of the auction. Finally, in order to win the auction successfully, the bidder Bob_k must publish his random number r_k and his bid x_k, i.e., open his commitment. All participants will compute $H(r_k \oplus H(r_k \oplus x_k))$ and verify its authenticity by comparing it with the corresponding value b_k committed in Step 1. In addition, Alice also needs to open her commitment x and accepts the verification of all bidders. If there is no error, the auctioneer Alice and all bidders will believe the auction is fair.

Analysis. *Correctness*. Our PQSA scheme is based on Grover's search algorithm, which can find a solution with a high probability[1,36]. Assume the failure probability of Grover's search algorithm is $\frac{1}{\delta}$, where $\delta \geq e$ (Note. e is the Euler's constant, which is the base of natural logarithms (approximately 2.7183)). Let $E(N, t)$ be the expectation value of the number of iterations (i.e., the number of repeating Grover's search algorithm in Step 2) for finding the highest bid of N items in which t items are marked[38]. Then we write a recurrence equation for $E(N, t)$ as:

$$E(N, t) = \frac{1}{t}[E(N, t-1) + \ldots + E(N, 1)] + 1. \tag{14}$$

So we get

$$tE(N, t) = \sum_{i=1}^{t-1} E(N, i) + t, \tag{15}$$

$$(t-1)E(N, t-1) = \sum_{i=1}^{t-2} E(N, i) + (t-1). \tag{16}$$

Subtracting Eqs (16) from (15) and rearranging, we get

$$E(N, t) = E(N, t-1) + \frac{1}{t}. \tag{17}$$

Writing the same equation for $(t-1), \ldots, 2$ and adding all of them, we get,

$$E(N, t) = E(N, 1) + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{t}. \tag{18}$$

Obviously, $E(N, 1) = 1$. That is, there is only one marked item in the general state of N items, so it only needs to execute Grover's search algorithm once to get the highest bid with the high probability of $1 - \frac{1}{\delta}$. Furthermore, it will give,

$$E(N, t) = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{t}. \tag{19}$$

From Eq. (19) we can get,

$$E(N, t) \leq \int_1^t \frac{1}{t} dt = \ln t. \tag{20}$$

In our PQSA scheme, there are at most n marked item, i.e., all bids are greater than the initial valuation price. So an upper bound is achieved for $t = n$, when we get,

$$E(N, n) \leq lnn. \tag{21}$$

Therefore, we can repeat Grover's search algorithm to obtain the highest bid with a probability of $1 - \left(\frac{1}{\delta}\right)^{\ln n}$ after $\ln n$ repetitions of this algorithm. That is, the failure probability ε of Step 2 to obtain the highest bid is $\left(\frac{1}{\delta}\right)^{\ln n}$. When $\delta \geq e$, we can get

$$\varepsilon = \left(\frac{1}{\delta}\right)^{\ln n} \leq \left(\frac{1}{e}\right)^{\ln n} \leq \frac{1}{n}. \tag{22}$$

The failure probability of $\frac{1}{n}$ is very small, so we only tolerate a complaint in Step 4. Therefore, if all participants honestly execute the procedures, our PQSA scheme is correct.

In above analysis, we assume that Grover's search algorithm has some probability of failure, i.e., the probability of finding the marked item is not exactly 1. Furthermore, Long[39] presented a modified version of Grover's search algorithm that searches a marked state with full successful rate. So, if we use Long's algorithm in our proposed protocol, it can get the better result theoretically.

Security. First, we analysis the proposed scheme can resist all kinds of outsider attacks. For an outsider attacker, he can intercept the transmitted messages, including classical messages and quantum messages. If the outsider attacker wants to get x_i from $H(r_i \oplus H(r_i \oplus x_i))$ without r_i, it is equivalent to break Hash function. At present, there is still not efficient method to break secure Hash function (e.g., SHA-1, SHA-2) by quantum computers or quantum algorithms. So, in the following we main analysis the possible attack to the transmitted quantum messages.

Firstly, the outsider attacker may perform an intercept-and-resend attack, i.e., he can intercept the transmitted quantum messages, and resend a fake quantum messages back to Alice. For example, the attacker intercepts the partial qubits of the state $|\psi_n\rangle = \frac{1}{\sqrt{N}}\left[\sum_{i \notin \{x_1, x_2, \ldots x_n\}} |i\rangle_h |i\rangle_t |0\rangle + \sum_{j \in \{x_1, x_2, \ldots x_n\}} |j\rangle_h |j\rangle_t |1\rangle\right]$ in the normal model. Clearly, the state $|\psi_n\rangle$ held by Alice and the attacker is an entangled state, where the reduced density matrixes of the subsystem held by them are $\frac{1}{N}\sum_{i=0}^{N-1} |i\rangle\langle i|$ and $\frac{1}{N}\left[\sum_{i \notin \{x_1, x_2, \ldots x_n\}} |i, 0\rangle\langle i, 0| + \sum_{j \in \{x_1, x_2, \ldots x_n\}} |j, 1\rangle\langle j, 1|\right]$, respectively. Though the reduced density matrix held by the attacker hides all private bids, the attacker cannot extract all by the principle of quantum mechanics. That is, even if the attacker measures his intercepted subsystem, he cannot get all private bids (i.e., all marked items). In fact, he can get at most one bid (i.e., one marked item) with a low probability because $n \ll N$, and the bid does not reveal any identity of the bidder. However, if the attacker intercepts the partial qubits of the state $|\psi_n\rangle = \frac{|0\rangle_h |0\rangle_t + |i\rangle_h |i\rangle_t}{\sqrt{2}} |0\rangle$ in the test model, then the reduced density matrix of the subsystem held by himself is $\frac{|0, 0\rangle\langle 0, 0| + |i, 0\rangle\langle i, 0|}{2}$, which is independent of all bids. That is, the intercepted subsystem cannot contain any private information about any private bid.

However, the attacker cannot distinguish the transmitted quantum states from the normal model and the test model. So, if the attacker measures his intercepted subsystem to get a bid, then he will be found later by Alice with great risk. For example, if the attacker measures the state $|\psi_n\rangle = \frac{|0\rangle_h |0\rangle_t + |i\rangle_h |i\rangle_t}{\sqrt{2}} |0\rangle$ of the test model in the computation basis, the state $|\psi_n\rangle$ will be collapsed into $|0\rangle_h |0\rangle_t |0\rangle$ or $|i\rangle_h |i\rangle_t |0\rangle$ with the probability of $\frac{1}{2}$, respectively. Later, Alice performs the test procedure in (2.4) of Step 2, so she can easily find this attack.

Of course, if the attacker sends a fake quantum system back to Alice, instead of the true subsystem intercepted by him, it will be easily found by Alice in (1.7) or (2.4) of Step 2. Therefore, our scheme can resist the intercept-and-resend attack.

Secondly, we analyze a more complicated attack, that is, the outsider attacker performs an entangle-and-measure attack that he first prepares an ancillary quantum system and further entangles his ancillary quantum system and the

intercepted subsystem by a local unitary operator, and afterward he can measure the ancillary quantum system to get the partial information about the private bids. The attacker's dishonest action can be described by a local unitary operator $\widetilde{U}$, which is simply defined by,

$$\widetilde{U}|j\rangle|0\rangle = \sqrt{\eta_j}|j\rangle|\xi(j)\rangle + \sqrt{1-\eta_j}|V(j)\rangle, \tag{23}$$

where $|V(j)\rangle$ is a vector orthogonal to $|j\rangle|\xi(j)\rangle$, i.e.,

$$\langle j|\langle\xi(j)|V(j)\rangle = 0 \tag{24}$$

In order to completely pass the honest test (see (1.7) or (2.4) of Step 2), it can easily deduce that $\eta_j = 1$. That is, the whole quantum system sent back to Alice in the normal model should be in the following state after performing the operator $\widetilde{U}$:

$$\begin{aligned}\widetilde{U}|\psi_n\rangle|0\rangle &= \widetilde{U}\frac{1}{\sqrt{N}}\left[\sum_{i\notin\{x_1,x_2,\ldots x_n\}}|i\rangle_h|i\rangle_t|0\rangle + \sum_{j\in\{x_1,x_2,\ldots x_n\}}|j\rangle_h|j\rangle_t|1\rangle\right]|0\rangle \\ &= \frac{1}{\sqrt{N}}\left[\sum_{i\notin\{x_1,x_2,\ldots x_n\}}|i\rangle_h|i\rangle_t|0\rangle|\xi(i,0)\rangle + \sum_{j\in\{x_1,x_2,\ldots x_n\}}|j\rangle_h|j\rangle_t|1\rangle|\xi(j,1)\rangle\right].\end{aligned} \tag{25}$$

After successfully passing the honest test, the state of the whole quantum system is in,

$$\frac{1}{\sqrt{N}}\left[\sum_{i\notin\{x_1,x_2,\ldots x_n\}}|i\rangle_h|0\rangle|\xi(i,0)\rangle + \sum_{j\in\{x_1,x_2,\ldots x_n\}}|j\rangle_h|1\rangle|\xi(j,1)\rangle\right]. \tag{26}$$

After performing U_{Alice} in (1.8) of Step 2, the state of the quantum system becomes,

$$\frac{1}{\sqrt{N}}\left[\sum_{i\notin\{x_1,x_2,\ldots x_n\}}|i\rangle_h|0\rangle|0\rangle|\xi(i,0)\rangle + \sum_{j\in\{x_1,x_2,\ldots x_n\}}|j\rangle_h|1\rangle|f_2(j,x)|\xi(j,1)\rangle\right]. \tag{27}$$

At this moment, if the attacker measures his ancillary quantum system, then he will get $\xi(i, 0)$ with a higher probability or $\xi(j, 1)$ with a lower probability, because $n \ll N$ actually, where the latter includes a bid. However, if Alice further executes Grover's search algorithm to find a marked state $|j\rangle|1\rangle|1\rangle|\xi(j, 1)\rangle$, then the attacker will get $\xi(j, 1)$ with a high probability. Now, he can get a bid, but he cannot distinguish his identity.

However, our scheme still has another model, i.e., the test model. If the attacker performs the entangle-and-measure attack in the test model, the whole quantum system sent back to Alice should be in the following state after performing the operator $\widetilde{U}$:

$$\begin{aligned}\widetilde{U}|\psi_n\rangle &= \widetilde{U}\frac{|0\rangle_h|0\rangle_t|0\rangle + |i\rangle_h|i\rangle_t|0\rangle}{\sqrt{2}}|0\rangle \\ &= \frac{|0\rangle_h|0\rangle_t|0\rangle|\xi(0,0)\rangle + |i\rangle_h|i\rangle_t|0\rangle|\xi(i,0)\rangle}{\sqrt{2}}.\end{aligned} \tag{28}$$

After Alice executes the procedure of (2.3) in Step 2, the quantum system will become $|\psi_n^*\rangle = \frac{|0\rangle_h|0\rangle_t|0\rangle \mid \xi(0,0)\rangle + |i\rangle_h|0\rangle_t|0\rangle \mid \xi(i,0)\rangle}{\sqrt{2}}$. At this moment, if Alice continues to execute the test procedure of (2.4), i.e., she performs a von Neumann measurement $\{P_{+i}, P_{-i}\}$ on the first register, then she will get the following results,

$$p_{+i} = \langle\psi_n^*|P_{+i}\otimes I\otimes I\otimes I|\psi_n^*\rangle = \frac{1}{2}, \tag{29}$$

$$p_{-i} = \langle\psi_n^*|P_{-i}\otimes I\otimes I\otimes I|\psi_n^*\rangle = \frac{1}{2}, \tag{30}$$

$$\frac{P_{+i}\otimes I\otimes I\otimes I|\psi_n^*\rangle}{\sqrt{p_{+i}}} = \frac{|0\rangle_h + |i\rangle_h}{\sqrt{2}}\otimes|0\rangle_t\otimes|0\rangle\otimes\frac{|\xi(0,0)\rangle + |\xi(i,0)\rangle}{\sqrt{2}}, \tag{31}$$

$$\frac{P_{-i}\otimes I\otimes I\otimes I|\psi_n^*\rangle}{\sqrt{p_{-i}}} = \frac{|0\rangle_h - |i\rangle_h}{\sqrt{2}}\otimes|0\rangle_t\otimes|0\rangle\otimes\frac{|\xi(0,0)\rangle - |\xi(i,0)\rangle}{\sqrt{2}}. \tag{32}$$

That is, she will get $\frac{|0\rangle_h + |i\rangle_h}{\sqrt{2}}$ or $\frac{|0\rangle_h - |i\rangle_h}{\sqrt{2}}$ with the probability of $\frac{1}{2}$, respectively. Obviously, Alice will detect the attack with the probability of $\frac{1}{2}$.

Finally, we consider that the attacker tries to add some false marked items in the returned state $|\psi_n\rangle$ by the oracle operators to manipulate the auction. On the one hand, if the false marked items are smaller than the highest bid, it will not affect the correctness of the auction; On the other hand, if a certain false marked item is greater

than the highest bid, it will be easily found because no bidder claims the false bid. Even if a collusion bidder claims the false bid, obviously he will not successfully pass the public verification.

In a word, no matter which attack the outsider attacker performs, he cannot get any private information without risking Alice's detection, and cannot manipulate the auction yet. That is, our scheme can resist the outsider attacks.

In addition, by the system model defined in the section of 3.1, PQSA should meets five secure and privacy requirements. In the following section, we will prove that our proposed PQSA scheme can meet all these secure and privacy requirements.

(1) **The auctioneer's privacy**: From the scheme proposed above, we can easily see that the transmitted quantum messages do not include any information about Alice's initial valuation price x. In addition, among all quantum oracle operators utilized by our proposed scheme, it is only the oracle operator U_{Alice} concerning x. However, U_{Alice} only is performed in Alice's registers, and these quantum states transferred by the operator U_{Alice} will be measured timely by Alice. So, if a dishonest bidder (or an outsider attacker) wants to steal Alice's private information, he can only perform the entangle-and-measure attack. However, we have analyzed the infeasibility of this attack above, because he cannot yet discern the normal model and the test model. If he performs the entangle-and-measure attack in the test model, his dishonesty will be found by Alice with the probability of $\frac{1}{2}$.

(2) **The bidder's privacy**: As we have analyzed above, any outsider attacker cannot get any private bid without risking the auctioneer's detection. In fact, for a bidder, he cannot get more information from the transmitted quantum messages than the outsider. If a dishonest bidder performs an attack, no matter concerned with measurement or entanglement, similarly, he will risk to be found later by the auctioneer. In short, no one can get the private bid of the bidder without risking the auctioneer's detection.

(3) **Anonymity**: By the proposed scheme, each bidder marks his bid in the transmitted quantum state $|\psi_i\rangle$. However, each bidder marks his bid in an anonymous way, i.e., the marked item in $|\psi_i\rangle$ does not leave any identity.

For a dishonest bidder, e.g., Bob_2, if he wants to get the specific bid of Bob_1 when receiving $|\psi_1\rangle$, he can perform Grover's search algorithm to find $|x_1\rangle_t|1\rangle$ because Bob_2 knows that there is only one marked item (i.e., x_1) in $|\psi_1\rangle$. However, if Alice selects the test model in Step 2, she can easily find this dishonesty because the final measurement result will be $|0\rangle_h$ or $|i\rangle_h$, instead of $\frac{|0\rangle_h + |i\rangle_h}{\sqrt{2}}$. That is, the dishonest bidder Bob_2 cannot get the bid of the first bidder Bob_1 without risking Alice's detection. In addition, after performing Grover's search algorithm, if Bob_2 directly sends a fake state to the next bidder, not $|x_1\rangle_t|1\rangle$, obviously it will be easily found by Alice in (1.7) or (2.4) of Step 2.

As for the other bidder Bob_i, even if he performs the similar attack to get $|x_1\rangle_t|1\rangle$ by Grover's search algorithm, he still cannot get the specific identity of x_j because of $j \in \{1, 2, \ldots, i-1\}$. Even if multiple bidders collude to perform this attack, it will be found later by Alice with the probability of $\frac{q}{p+q}$. In addition, this attack also brings a risk of the failure of the auction, because our proposed scheme only permits at most one complaint when announcing the highest bid.

At present, we only assume that there is a circle quantum channel among the auctioneer and all bidders in our PQAS model. For the current technical conditions, obviously this model is more feasible. In fact, if there is a quantum channel between any two parties, the quantum messages can be transmitted in a random order, i.e., from Bob_i to random Bob_j, not Bob_{i+1}, such that it can provide the perfect anonymity of the bids.

For the auctioneer Alice, she can receive the returned state $|\psi_n\rangle$, in which all bids have be marked in an anonymous way. Furthermore, she can get a marked item $|y\rangle|1\rangle|1\rangle$ by Grover's search algorithm, but she cannot know y belongs to who because of $y \in \{1, 2, \ldots, n\}$.

Therefore, our proposed scheme can ensure that the bidder's bid is anonymous for all participants, including the auctioneer.

(4) **Public verifiability**: On the one hand, when the highest bid x_k is announced publicly, it needs to accept the comparisons of all other bidders to decide whether it is greater than their respective bids. On the other hand, to further win the auction successfully, the highest bidder Bob_k requires to open his commitment x_k to accept the verifications of the authenticity of the bid x_k. As you know, there is not a perfect secure quantum bit commitment based on the No-Go Theorem[40–42]. So we utilizes a practical and efficient classical bit string commitment, in which it can not get x_k only from $H(r_k \oplus H(r_k \oplus x_k))$ without r_k, unless cracking the secure hash function, e.g., SHA-1, SHA-2. By the opening information r_k, anyone can verify the authenticity of the winning bid x_k. Even if the auctioneer wants to help a malicious bidder Bob_j to win this auction, but they cannot revise the hash value $H(r_j \oplus H(r_j \oplus x_j))$, which was published in advance, so the fake bid r_j^* (implying $r_j^* > r_k$) cannot pass the verification finally. That is, this attribute can defend the collusion attack between the malicious bidder and the dishonest auctioneer. In fact, bit string commitments ensures that the initial valuation price and all bids can not changed during the whole auction, otherwise the cheating will be found easily.

(5) **Fairness**: Since all bidders and the auctioneer need to commit their bids and the valuation price at the beginning of the auction, and the successfully winning bid needs to be verified publicly by all participants finally, no one can manipulate the auction, even for the auctioneer. That is, the auctioneer cannot help a malicious bidder to win the auction illegally without being found by other bidders. Therefore, our proposed scheme can guarantee the fairness of the auction.

We have analyzed the security of proposed scheme in ideal settings. However, in practical settings, there may be some faults (e.g., noise and error) in the quantum channels and quantum measurements. In order to ensure its security in practical settings, one can use the fault tolerant technologies, such as decoherence-free states and error-correcting code. In addition, we can use classical authenticated channels and quantum authenticated channels to ensure the correctness of distributing messages.

Performance. The proposed scheme is mainly based on Grover's search algorithm. By the previous analysis, the number of iterations (i.e., the number of repeating Grover's search algorithm in Step 2) for finding the highest bid is less than or equal to ln$n$, which is its upper bound, so both the computational complexity and the communicational complexity are $O(\ln n)$, i.e., to execute $O(\ln n)$ Grover's search algorithms and to distribute $O(\ln n)$ quantum messages. To complete the task, any classical scheme needs to distribute $O(n)$ messages in theory, where each message gets a bid in an anonymous way, and then finds the highest bid by comparing $O(n)$ times. Obviously, our proposed quantum scheme gets the lower communicational complexity than any classical scheme.

In addition, to make our scheme work, the key step is to construct the efficient circuits implementing the oracle operators. In our scheme, we define two kinds of oracle operators to mark items in a general state. Similarly, using the techniques of reversible computation[1], we can construct a classical reversible circuit which takes (x, y) - representing an input register initially set to x and a one bit output register initially set to y - to $(x, y \oplus f(x))$, by modifying the usual (irreversible) classical circuit for doing the classical function $f(x)$.

At present, Grover's search algorithm and its variants have been implemented by the newest reports[43–45], especially in IBM quantum cloud[46]. So, with the rapid development of quantum computing and quantum information processing, we believe that our proposed PQSA scheme is feasible in the near future.

Conclusions

In this paper, we define a new privacy-preserving quantum sealed-bid auction model, and further present a novel privacy-preserving quantum sealed-bid auction scheme based on Grover's search algorithm. The proposed scheme not only guarantees the correctness and fairness of the auction, but also ensures the privacy and anonymity of the bidders, even for the auctioneer. Compared with the current existing quantum sealed-bid auction, our proposed scheme can provide stronger privacy protections, which are urgently requirements in modern network society. So the proposed scheme has wider popularization and application prospects.

In addition, we actually give an efficient quantum approach to privately find the optimal solution under the constraint conditions among multiple distributed participants, which can also be generalized into other secure applications, e.g., an election satisfying more than half of votes.

Data Availability

Data sharing is not applicable as no datasets were used during the current study.

References

1. Nielsen, M. A. & Chuang, I. L. Quantum Computation and Quantum Information: 10th Anniversary Edition, (Cambridge University Press, Cambridge, 2011).
2. Long, G. L. & Liu, X. S. Theoretically efficient high-capacity quantum key distribution scheme. *Phys. Rev. A* **65**, 032302 (2002).
3. Bennett, C. H. *et al*. Teleporting an Unknown Quantum State via Dual Classical and EPR Channels. *Phys. Rev. Lett.* **70**, 1895–1899 (1993).
4. Cai, X. D. *et al*. Entanglement-based machine learning on a quantum computer. *Phys. Rev. Lett.* **114**, 110504 (2015).
5. Sheng, Y. B. & Zhou, L. Distributed secure quantum machine learning. *Sci. Bull.* **62**, 1025 (2017).
6. Bennett, C. H. & Brassard, G. Quantum Cryptography: Public Key Distribution and Coin Tossing. In: *Proc. IEEE International Conference on Computers, Systems, and Signal Processing*, pp.175–179 (1984).
7. Hillery, M., Bužek, V. & Berthiaume, A. Quantum Secret Sharing. *Phys. Rev. A* **59**, 1829 (1999).
8. Deng, F. G., Long, G. L. & Liu, X. S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. *Phys. Rev. A* **68**, 042317 (2003).
9. Zhang, W. *et al*. Quantum Secure Direct Communication with Quantum Memory. *Phys. Rev. Lett.* **118**, 220501 (2017).
10. Chen, S. S., Zhou, L., Zhong, W. & Sheng, Y. B. Three-step three-party quantum secure direct. *Sci. China-Phys. Mech. Astron.* **61**, 090312 (2017).
11. Boykin, P. O. & Roychowdhury, V. Optimal encryption of quantum bits. *Phys. Rev. A* **67**, 042317 (2003).
12. Zeng, G. & Keitel, C. H. Arbitrated quantum-signature scheme. *Phys. Rev. A* **65**, 042312 (2002).
13. Wang, T. Y. *et al*. Security of quantum digital signatures for classical messages. *Sci. Rep.* **5**, 9231 (2015).
14. Wang, T. Y., Ma, J. F. & Cai, X. Q. The postprocessing of quantum digital signatures. *Quantum Inf. Process.* **16**, 19 (2017).
15. Shi, R. H. *et al*. Quantum private set intersection cardinality and its application to anonymous authentication. *Inf. Sci.* **370–371**, 147–158 (2016).
16. Wang, T. Y., Wen, Q. Y. & Zhu, F. C. Secure authentication of classical messages with decoherence-free states. *Opt. Commun.* **282**, 3382–3385 (2009).
17. Fitzsimons, J. F. Private quantum computation: an introduction to blind quantum computing and related protocols. *NPJ Quantum Inf.* **3**, 23 (2017).
18. Sheng, Y. B. & Zhou, L. Blind quantum computation with a noise channel. *Phys. Rev. A* **98**, 052343 (2018).
19. Hillery, M. Quantum voting and privacy protection: first steps. *Int. Soc. Opt. Eng.* https://doi.org/10.1117/2.1200610.0419 (2006).
20. Naseri, M. Secure quantum sealed-bid auction. *Opt. Commun.* **282**(9), 1939–1943 (2009).
21. Zhang, J. Z., Yang, Y. Y. & Xie, S. C. A Third-Party E-Payment Protocol Based on Quantum Group Blind Signature. *Int J Theor Phys* **56**, 2981–2989 (2017).
22. Qin, S. J. *et al*. Cryptanalysis and improvement of a secure quantum sealed-bid auction. *Opt. Commun.* **282**, 4014–4016 (2009).
23. Yang, Y. G., Naseri, M. & Wen, Q. Y. Improved secure quantum sealed-bid auction. *Opt. Commun.* **282**, 4167–4170 (2009).
24. Liu, Y. M. *et al*. Revisiting Naseri's secure quantum sealed-bid auction. *Int. J. Quantum Inf.* **7**, 1295–1301 (2009).
25. Zheng, Y. & Zhao, Z. Comment on: "Secure quantum sealed-bid auction". *Opt. Commun.* **282**, 4182 (2009).
26. Zhao, Z., Naseri, M. & Zheng, Y. Secure quantum sealed-bid auction with post-confirmation. *Opt. Commun.* **283**, 3194–3197 (2010).
27. Xu, G. A. *et al*. Cryptanalysis and improvement of the secure quantum sealed-bid auction with postconfirmation. *Int. J. Quantum Inf.* **9**, 1383–1392 (2011).
28. He, L. B. *et al*. Cryptanalysis and melioration of secure quantum sealed-bid auction with post-confirmation. *Quantum Inf. Process.* **11**, 1359–1369 (2012).
29. Wang, Q. L., Zhang, W. W. & Su, Q. Revisiting "The loophole of the improved secure quantum sealed-bid auction with post-confirmation and solution". *Int. J. Theor. Phys.* **53**, 3147–3153 (2014).
30. Zhang, Y. W. Quantum secure direct communication and quantum sealed-bid auction with EPR pairs. *Commun. Theor. Phys.* **54**, 997 (2010).
31. Wen, J. L. *et al*. Attacks and improvement of quantum sealed-bid auction with EPR pairs. *Commun. Theor. Phys.* **61**, 686 (2014).

32. Wang, J. T. *et al*. A new quantum sealed-bid auction protocol with secret order in post-confirmation. *Quantum Inf. Process.* **14**, 3899–3911 (2015).
33. Liu, W. J. *et al*. Multiparty quantum sealed-bid auction using single photons as message carrier. *Quantum Inf. Process.* **15**, 869–879 (2016).
34. Zhang, R. *et al*. An economic and feasible Quantum Sealed-bid Auction protocol. *Quantum Inf. Process.* **17**, 35 (2018).
35. Shi, R. H. *et al*. Secure Multiparty Quantum Computation for Summation and Multiplication. *Sci. Rep.* **6**, 19655 (2016).
36. Grover, L. K. A fast quantum mechanical algorithm for database search. In: *Proc. 28th Annual ACM Symposium on Theory of Computing, ACM*, pp.212–219 (1996).
37. Shi, R. H. *et al*. Comment on "Secure quantum private information retrieval using phase-encoded queries". *Phys. Rev. A* **94**, 066301 (2016).
38. Ahuja, A. & Kapoor, S. A Quantum Algorithm for finding the Maximum. arXiv:quant-ph/9911082v1.
39. Long, G. L. Grover algorithm with zero theoretical failure rate. *Phys. Rev. A* **64**, 022307 (2001).
40. Lo, H. K. Insecurity of quantum secure computations. *Phys. Rev. A* **56**, 1154–1162 (1997).
41. Colbeck, R. The impossibility of secure two-party classical computation. *Phys. Rev. A* **76**, 062308 (2007).
42. Buhrman, H., Christandl, M. & Schaffner, C. Complete Insecurity of Quantum Protocols for Classical Two-Party Computation. *Phys. Rev. Lett.* **109**, 160501 (2012).
43. Chuang, I. L., Gershenfeld, N. & Kubinec, M. Experimental implementation of fast quantum searching. *Phys. Rev. Lett.* **80**, 3408–3411 (1998).
44. Brickman, K.-A. *et al*. Implementation of Grover's quantum search algorithm in a scalable system. *Phys. Rev. A* **72**, 050306(R) (2005).
45. Figgatt, C. *et al*. Complete 3-Qubit Grover search on a programmable quantum computer. *Nat. Commun.* **8**, 1918 (2017).
46. Majumder, A., Mohapatra, S. & Kumar, A. Experimental Realization of Secure Multiparty Quantum Summation Using Five-Qubit IBM Quantum Computer on Cloud. arXiv:1707.07460v3 (2017).

Acknowledgements

This work was supported by National Natural Science Foundation of China (Nos 61772001 and 61672010).

Author Contributions

Two authors equally contributed to the work. Study conception, design, and writing of the manuscript: Shi R.H. and Zhang M.; Analysis and discussion: Shi R.H. and Zhang M.; All authors reviewed the manuscript.

Additional Information

Competing Interests: The authors declare no competing interests.

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