Secure quantum sealed-bid auction

Mosayeb Naseri *

Islamic Azad University, Kermanshah Branch, Kermanshah, Iran

Abstract

A new experimentally feasible and secure quantum sealed-bid auction protocol using quantum secure direct communication based on GHZ states is proposed. In this scheme all bidders Bob, Charlie, ..., and Zach use M groups n-particle GHZ states to represent their bids. Here, an auctioneer gives the auction outcome by performing a sequence of n-particle GHZ-basis measurements on the final quantum states. It has been shown that using this method guarantees the honesty of the protocol, and malicious bidders cannot collude with the auctioneers.

© 2009 Elsevier B.V. All rights reserved.

1. Introduction

Quantum key distribution (QKD) is an ingenious application of quantum mechanics in information field. It provides a novel way for two legitimate parties to establish a common key over a long distance. QKD has progressed quickly since the QKD protocol was first proposed by Bennett and Brassard in 1984 [1]. On the other hand, a novel concept, QSDC has been proposed and pursued attracted much attention [2–15]. Different from QKD whose goal is to generate a private key between two remote parties, the QSDC communicates the secret messages directly without generating a key in advance and then encrypting the secret messages. The QSDC protocol originally proposed by Beige et al. [2] is only a scheme for transmitting secret information which can be read out with an additional classical information for each qubit.

Bostrom and Felbinger put forward a ping-pong QSDC scheme following the idea of quantum dense coding [16] with Einstein–Podolsky–Rosen (EPR) pairs, which is just a quasi-secure direct communication protocol as it leaks some of the secret message in a noisy channel. Also general schemes for multi-party high-dimensional dense coding, explicit expressions for the measuring basis and the forms of the one-body unitary transformation operators have been constructed by Gao et al. [17]. Recently, a protocol for controlled quantum teleportation and secure direct communication using GHZ state has been designed [18]. Later, a three-party quantum secure direct communication (QSDC) protocol based on GHZ state has been proposed and generalized to the N multi-party case by Jin et al. [19].

Recent research on quantum computation and quantum information allowed to use it for describing financial market phenomena. Quantum information has extended the scope of game theory for the quantum world [20–23]. Also quantum game theory has been used for describing financial market phenomena [17,18]. An auction is one of the basic businesses in commerce. The protection of bidder privacy and the prevention of bidder default are the key problems needed to be urgently solved. There are few quantum auction protocols, where the applications of quantum game theory has been extended to quantum version of auctions [24,25].

An auction usually has three transactional types: traditional English auction, Dutch auction and sealed-bid auction [26–28]. Traditional English auction is also known as public bid auction, wherein each bidder casts his/her own bid, and the bid must be higher than the bottom price. The top price is adjusted upwards after a round. The auction goes on until there is only one bidder left who is willing to offer the price. Dutch auction is similar to traditional English auction, but it begins with the top price, and then the price goes down round after round until the first bidder decides to offer the price. Unlike the previous two kinds of auctions, all the customers who are willing to name their bids are gathered in a sealed-bid auction, where each bidder submit their own bids to the auctioneer. After the opening phase, the auctioneer makes all the bids public and determines the winner. In this article a new secure quantum sealed-bid auction protocol has been
presented. Here a quantum auction is considered as a communication process and it has been designed using a quantum secure direct communication based on GHZ states protocol [19]. This paper is organized as follows:

In the next section we discuss the brief description of multi-party quantum secure direct communication based on GHZ states protocol. Multi-party quantum sealed-bid auction is presented in Section 3. For convenience, as an example three-party quantum sealed-bid auction is described in Section 4. The security of the protocol is analyzed in Section 5. Finally, in the last section, the summary and conclusions are presented.

2. Multi-party quantum secure direct communication based on GHZ states

A multi-party quantum secure direct communication (QSDC) protocol based on GHZ state was proposed a by Jin et al. in Ref. [19]. In this section to demonstrate our viewpoint clearly, we review multi-party quantum secure direct communication based on GHZ states, in which, Alice, Bob, Charlie,...., and Zach can exchange their messages simultaneously.

At first Alice, Bob, Charlie,...., and Zach agree on Alice can perform the four unitary operations $I$, $i$, $r$, $y$, to encode two bits classical information $00$, $01$, $10$, $11$, where:

$$l = |0\rangle \langle 0| + |1\rangle \langle 1|, \sigma_y = |0\rangle \langle 1| - |1\rangle \langle 0|, \sigma_z = |0\rangle \langle 0| - |1\rangle \langle 1|.$$  (1)

And also they agree on Bob, Charlie,...., and Zach can only perform the two unitary operations $l$, $i$, to encode classical bits information $0$, $1$, where:

$$l = |0\rangle \langle 0| + |1\rangle \langle 1|, \sigma_y = |0\rangle \langle 1| - |1\rangle \langle 0|.$$  (2)

The n-party (an auctioneer and n-1 bidders) simultaneous (QSDC) scheme can be achieved as follows:

Step I: Alice prepares a set of M groups n-particle GHZ states randomly in one of the $2^n$ n-particle GHZ states $(|\psi_{ijk...y}\rangle_{abc...z}, i,j,k,...,y = 0,1)$. Then she sends M groups b particles to Bob, c particles to Charlie,...., $z$ particles to Zach. Here, since Bob, Charlie,...., and Zach can not distinguish the particles a, b, c,...., and z, Alice must let them know which particles they have received.

Step II: Once Bob, Charlie,...., and Zach receive all the b particles, c particles,...., and z particles respectively, they inform Alice that they have received all the particles. Afterwards anyone of them, we say Bob, selects randomly a sufficiently large subset of particles from the M groups b particles, which we call the T groups b particles, and measures each of them using one of the two measuring bases $(|0\rangle \langle 1|)$ or $(|+\rangle \langle -|)$ randomly, and he tells Alice, Charlie,...., and Zach the position, the measuring basis and the result of his measurement for each of the T groups b particles via a classical channel. Then Charlie,...., and Zach measure T groups c particles,...., z particles using the same measuring bases, respectively. Afterwards they tell Alice their result for each of the particles. Also Alice measure T groups a particles. According to the measurement results of Bob, Charlie,...., and Zach herself, Alice can determine whether there is any eavesdropping or not. If there is an error, Alice concludes that the channel is not secure and halts the communication. Otherwise, Alice, Bob, Charlie,...., and Zach proceed to the next step.

Step III: The particles leftover are called the I groups particles $(I = M - T)$ after the security checking of the quantum channel. In this step, Alice, Bob, Charlie,...., Zach have particle sequences $(a_1,a_2,...,a_I), (b_1,b_2,...,b_T), (c_1,c_2,...,c_I),...., and (z_1,z_2,...,z_I)$ in their hands. So Bob, Charlie,...., and Zach encode each of the subgroups b particles, c particles,...., $z$ particles with one of the two unitary operations $l$ and $i\sigma_y$, respectively, according to their secret messages. Then they return the I groups b particles c particles,...., and $z$ particles to Alice. After receiving the I groups b particles c particles,...., and $z$ particles, Alice encodes each of the I groups a particles with one of the four unitary operations $l$, $i\sigma_y$, $i\sigma_z$, and $y$, according to her secret message. Then she performs a n-particle GHZ-basis measurement on I groups a, b, c,...., and $z$ particles and publicly publishes the results of her measurement and initial n-particle GHZ states. According to her results, initial n-particle GHZ states and the unitary operations performed by herself, Alice can read out the secret messages of Bob, Charlie,...., and Zach. Also, Bob (Charlie,...., Zach) can read out the secret messages of the others. So the n-party simultaneous QSDC has been successfully completed.

3. Multi-party quantum sealed-bid auction

Now let us turn to our protocol of quantum sealed-bid auction. In our scheme, the auction model consists of one buyer agent Alice, who is the auctioneer, who needs particular L items (service or product) and a fixed number of n-1 seller agents, Bob, Charlie,...., and Zach, who are the bidders. The scheme can be explained as follows:

(1) At the beginning of the auction, the buyer, Alice announces her request items (which consists of the items desired characteristics and the auction protocol) by a classical channel. In this step all parties agree that Alice can perform the four unitary operations $l$, $i\sigma_y$, $i\sigma_z$, and $y$, to encode two bits classical information $00$, $01$, $10$, $11$, where $l$, $i\sigma_y$, $i\sigma_z$, and $y$ are defined in Eq. (1).

(2) Auctioneer, Alice, prepares a set of M groups n-particle GHZ states randomly in one of the $2^n$ n-particle GHZ states $(|\psi_{ijk...y}\rangle_{abc...z}, i,j,k,...,y = 0,1)$, and she sends M groups b particles to Bob, M groups c particles to Charlie,...., and M groups $z$ particles to Zach. Here, since Bob, Charlie,...., and Zach can not distinguish the particles a, b, c,...., and z, the auctioneer must let them know which particles they have received.

(3) Bob, Charlie,...., and Zach let Alice know that they have received all the b particles, c particles,...., and $z$ particles respectively. Afterwards, Bob (anyone of the n-1 bidders Bob, Charlie,...., Zach, we say Bob) selects randomly a sufficiently large subset of particles from the M groups b particles, which we call the T groups b particles, and measures each of these particles using one of the two measuring bases $(|0\rangle \langle 1|)$ or $(|+\rangle \langle -|)$ randomly. Then he tells All other bidders the position, the measuring basis and the measurement results for each of the T groups b particles via a classical channel and asks them to measure T groups c particles,...., $z$ particles using the same measuring bases, respectively. Then all of the bidders tell Alice their measurement results for each of the particles. Also Alice measures T groups a particles. According to the results of Bob's, Charlie's,...., Zach's measurement and the unitary operations performed by herself and the results of her measurements, Alice can determine whether there is any eavesdropping or not. If there is an error, Alice concludes that the channel is not secure, and halts the auction. Otherwise, Alice, Bob, Charlie,...., and Zach continue the next step.

(4) The particles leftover are called the I groups $(I = M - T)$ after checking eavesdropping. So after the security checking of the quantum channel, Bob has particle sequence $(b_1, b_2,...,b_T)$, Charlie has particle sequence $(c_1,c_2,...,c_I)$, and Zach has particle sequence $(z_1,z_2,...,z_I)$ in his hands; also Alice's left-
over particle sequence is \((a_1, a_2, \ldots, a_t)\). Then according to \(L\) auctioned items, Alice and all bidders divide \(L\) groups \(a\) particles, \(b\) particles, \(c\) particles, \(\ldots\), \(z\) particles on \(L\) subgroups \(p\)-particles \((LP = I)\) as follows:

\[
\begin{align*}
&\{(b_1, b_2, \ldots, b_p), (b_{p+1}, b_{p+2}, \ldots, b_{2p}), \ldots, (b_{L-1p+1}, b_{L-1p+2}, \ldots, b_{Lp})\}, \\
&\{(c_1, c_2, \ldots, c_p), (c_{p+1}, c_{p+2}, \ldots, c_{2p}), \ldots, (c_{L-1p+1}, c_{L-1p+2}, \ldots, c_{Lp})\}, \\
&\quad \vdots \\
&\{(z_1, z_2, \ldots, z_p), (z_{p+1}, z_{p+2}, \ldots, z_{2p}), \ldots, (z_{L-1p+1}, z_{L-1p+2}, \ldots, z_{Lp})\}.
\end{align*}
\]

Then all bidders encode each of the \(L\) subgroups \(b\) particles, \(c\) particles, \(\ldots\), \(z\) particles with one of the two unitary operations \(I\) and \(i\sigma_y\), according to their secret bids, and return the encoded particles to Alice.

(5) After receiving the \(L\) subgroups \(b\) particles, \(L\) subgroups \(c\) particles, \(\ldots\), and \(L\) subgroups \(z\) particles, Alice encodes each of the \(L\) subgroups \(a\) particles with one of the four unitary operations \(I, \sigma_x, i\sigma_y\), and \(i\sigma_z\) according to her secret message (auction ending announcement, \(\ldots\)). Then Alice performs \(n\)-particle GHZ-basis measurements on \((I = Lp)\) groups \(a, b, c, \ldots, z\) particles and publicly publishes the results of her measurements and initial \(n\)-particle GHZ states. According to the results of her measurements, initial \(n\)-particle GHZ states and the unitary operations performed by herself, Alice can read out the secret bids of \(b\), \(c\), \(\ldots\), and \(z\). Also, Bob (\(c\), \(\ldots\), and \(z\)) can see the other’s bids. So the winner of the auction will be revealed publicly and the \(n\)-party QSBA (quantum sealed-bid auction) will be successfully completed.

4. An example: Three-party quantum sealed-bid auction

For the sake of clarity, as an example let us describe a three-party quantum sealed-bid auction protocol. Suppose auctioneer, Alice needs particular \(L\)-items (services or products) and there are two seller agents, Bob and Charlie, who are the bidders.

Our three-party protocol of quantum sealed-bid auction (an auctioneer and two bidders) can be achieved in following steps:

**Step I:** At first, Alice prepares a set of \(M\) groups three-particle GHZ states randomly in one of the eight \((2^3 = 8)\) three-particle GHZ states \(|\psi_{000}\rangle_{abc}, |\psi_{001}\rangle_{abc}, |\psi_{010}\rangle_{abc}, |\psi_{100}\rangle_{abc}, |\psi_{011}\rangle_{abc}, |\psi_{101}\rangle_{abc}, |\psi_{110}\rangle_{abc}, |\psi_{111}\rangle_{abc}\), where:

\[
\begin{align*}
|\psi_{000}\rangle_{abc} &= \frac{1}{\sqrt{2}} \left( |000\rangle + |111\rangle \right)_{abc}, \\
|\psi_{001}\rangle_{abc} &= \frac{1}{\sqrt{2}} \left( |000\rangle - |111\rangle \right)_{abc}, \\
|\psi_{010}\rangle_{abc} &= \frac{1}{\sqrt{2}} \left( |100\rangle + |011\rangle \right)_{abc}, \\
|\psi_{011}\rangle_{abc} &= \frac{1}{\sqrt{2}} \left( |100\rangle - |011\rangle \right)_{abc}, \\
|\psi_{100}\rangle_{abc} &= \frac{1}{\sqrt{2}} \left( |100\rangle + |011\rangle \right)_{abc}, \\
|\psi_{101}\rangle_{abc} &= \frac{1}{\sqrt{2}} \left( |100\rangle - |011\rangle \right)_{abc}, \\
|\psi_{110}\rangle_{abc} &= \frac{1}{\sqrt{2}} \left( |110\rangle + |001\rangle \right)_{abc}, \\
|\psi_{111}\rangle_{abc} &= \frac{1}{\sqrt{2}} \left( |110\rangle - |001\rangle \right)_{abc}.
\end{align*}
\]

Then Alice sends \(M\) groups \(b\) particles to Bob and \(M\) groups \(c\) particles to Charlie, respectively. Here, since Bob and Charlie cannot distinguish the particles \(a, b\), and \(c\), Alice must let them know which one they have received.

**Step II:** Bob and Charlie confirm Alice that they have received all the \(b\) particles and \(c\) particles. Afterwards to checking the security of the quantum channel, Bob or Charlie, we say Bob, selects randomly a sufficiently large subset of particles from the \(M\) groups \(b\) particles, which we call the \(T\) groups \(b\) particles, and he measures each of them using one of the two measuring bases \((|0\rangle, |1\rangle)\) or \((|+\rangle, |−\rangle)\) randomly and he tells Charlie and Alice the position, the measuring basis and the results of his measurements for each of the \(T\) groups \(b\) particles via a classical channel. Then Alice and Charlie measure their particles on the corresponding \(T\) groups \(b\) and \(c\) particles by same measuring bases, respectively. Afterwards Charlie tells Alice the results of his measurements for each of the \(T\) groups \(c\) particles. According to the results of Bob’s and Charlie’s measurements and her results, Alice can determine, whether there is any eavesdropping in the channel. If there is an error, Alice concludes that the channel is not secure and decides to stop the communication. Otherwise, Alice, Bob, and Charlie proceed to the next step.

**Step III:** After insuring the security of quantum channel, Alice’s, Bob’s and Charlie’s particles leftover sequences are \((a_1, a_2, \ldots, a_t), (b_1, b_2, \ldots, b_t)\), and \((c_1, c_2, \ldots, c_t)\), where \(t = M - T\). According to \(L\) auctioned items Alice, Bob and Charlie divide up their particles, a particle, \(b\) particles and \(c\) particles on \(L\) subsequence \(p\)-particles \((LP = I)\). Afterwards according to their bids, the bidders (Bob and Charlie) encode their offers on \(L\) groups \(b\) particles and \(L\) groups \(c\) particles with one of the two unitary operations \(I, \sigma_x, i\sigma_y\), respectively, and they return the \(L\) groups \(b\) particles and \(L\) groups \(c\) particles to Alice.

**Step IV:** Once Alice receives all particles, she encodes her final message on \(L\) groups a particles with one of the four unitary operations \(I, \sigma_x, i\sigma_y\), and \(i\sigma_z\) according to her message. Then she performs three particle GHZ-basis measurements on \(L\) groups \(a, b\), and \(c\) particles and publicly announces the results of her measurements and initial three-particle GHZ states. According to her results, initial three-particle GHZ states and the unitary operations performed by herself, Alice can read out the secret bids of Bob and Charlie. Also, Bob (or Charlie) can read out the Alice’s final message and Charlie’s bids (or Bob’s bids). So the auction winner can be determined simply.

The relationship between the results of Alice’s measurements, the initial GHZ states, Alice’s, Bob’s and Charlie’s encoding operations is shown in Table 1.
Table 1

The relationship between the results of Alice's measurements, the initial GHZ states, Alice's, Bob's and Charlie's encoding operation.

| Quantum channel | | | | | | | | |
|-----------------|---------|---------|---------|---------|---------|---------|---------|
| $\lvert 000\rangle_{abc}$ | $\lvert 001\rangle_{abc}$ | $\lvert 010\rangle_{abc}$ | $\lvert 011\rangle_{abc}$ | $\lvert 100\rangle_{abc}$ | $\lvert 101\rangle_{abc}$ | $\lvert 110\rangle_{abc}$ | $\lvert 111\rangle_{abc}$ |
| $ \lvert 0\rangle \otimes \lvert 0\rangle \otimes \lvert 0\rangle $ | $ \lvert 0\rangle \otimes \lvert 0\rangle \otimes \lvert 1\rangle $ | $ \lvert 0\rangle \otimes \lvert 1\rangle \otimes \lvert 0\rangle $ | $ \lvert 0\rangle \otimes \lvert 1\rangle \otimes \lvert 1\rangle $ | $ \lvert 1\rangle \otimes \lvert 0\rangle \otimes \lvert 0\rangle $ | $ \lvert 1\rangle \otimes \lvert 0\rangle \otimes \lvert 1\rangle $ | $ \lvert 1\rangle \otimes \lvert 1\rangle \otimes \lvert 0\rangle $ | $ \lvert 1\rangle \otimes \lvert 1\rangle \otimes \lvert 1\rangle $ |
| $ \lvert 0\rangle \otimes \lvert 1\rangle \otimes \lvert 0\rangle $ | $ \lvert 0\rangle \otimes \lvert 1\rangle \otimes \lvert 1\rangle $ | $ \lvert 1\rangle \otimes \lvert 0\rangle \otimes \lvert 0\rangle $ | $ \lvert 1\rangle \otimes \lvert 0\rangle \otimes \lvert 1\rangle $ | $ \lvert 1\rangle \otimes \lvert 1\rangle \otimes \lvert 0\rangle $ | $ \lvert 1\rangle \otimes \lvert 1\rangle \otimes \lvert 1\rangle $ | $ \lvert 1\rangle \otimes \lvert 0\rangle \otimes \lvert 1\rangle $ | $ \lvert 1\rangle \otimes \lvert 1\rangle \otimes \lvert 1\rangle $ |
| $ \lvert 0\rangle \otimes \lvert 0\rangle \otimes \lvert 1\rangle $ | $ \lvert 0\rangle \otimes \lvert 0\rangle \otimes \lvert 1\rangle $ | $ \lvert 1\rangle \otimes \lvert 0\rangle \otimes \lvert 1\rangle $ | $ \lvert 1\rangle \otimes \lvert 1\rangle \otimes \lvert 1\rangle $ | $ \lvert 0\rangle \otimes \lvert 0\rangle \otimes \lvert 1\rangle $ | $ \lvert 0\rangle \otimes \lvert 0\rangle \otimes \lvert 1\rangle $ | $ \lvert 1\rangle \otimes \lvert 0\rangle \otimes \lvert 1\rangle $ | $ \lvert 1\rangle \otimes \lvert 1\rangle \otimes \lvert 1\rangle $ |

For more convenience, consider a simple case, where Alice needs a particular service or product ($L = 1$). Suppose that Alice, Bob and Charlie after checking the security have particles leftover $(a_1, b_2, b_3, c_2, c_3, c_4)$. From the initial quantum states $(\lvert 0\rangle_{000}, \lvert 0\rangle_{000}, \lvert 0\rangle_{000}, \lvert 0\rangle_{000}, \lvert 0\rangle_{000}, \lvert 0\rangle_{000})$, i.e. $(I = 4)$. Also suppose that Bob’s and Charlie’s secret bids are 1101 and 1100 and Alice’s final message is 00100111.

To offer their bids, Bob and Charlie must perform a sequence of unitary operations $(i_1, i_2, i_3, i_4)$ on particles $(b_1, b_2, b_3, b_4)$ and $(c_1, c_2, c_3, c_4)$, respectively, according to their bids. The initial quantum states become $(\lvert 0\rangle_{000}, \lvert 0\rangle_{000}, \lvert 0\rangle_{000}, \lvert 0\rangle_{000}, \lvert 0\rangle_{000}, \lvert 0\rangle_{000})$.

Once Alice receives encoded particles from Bob and Charlie, she encodes her final message 00100111 by performing a sequence of unitary operations $(i_1, i_2, i_3, i_4)$ on particles $(a_1, b_2, b_3, b_4)$, respectively. Then she performs three particle GHZ measurements on four groups three particles $(a_1, b_2, b_3, b_4)$, with the results $(\lvert 0\rangle_{000}, \lvert 0\rangle_{000}, \lvert 0\rangle_{000}, \lvert 0\rangle_{000}, \lvert 0\rangle_{000}, \lvert 0\rangle_{000})$. Afterwards she publishes the results of her measurements and the initial three-particle GHZ states. According to her results, the initial three-particle GHZ states and the unitary operations performed by herself, Alice can read out Bob’s and Charlie’s secret messages 1101 and 1100, respectively. Similarly, Bob (or Charlie) can also read out Alice’s secret messages 00100111 and Charlie’s (or Bob’s) secret bids 1101 (or 1100), respectively. So the auction winner can be determined by the bidders.

In essence, three-party quantum secure direct communication (QSDC) protocol based on GHZ state and it’s generalized version and subsequently the secure quantum sealed-bid auction scheme can be considered as a direct application of the multi-party superdense coding scheme to the sealed-bid auction problem. Actually, each bit in the sealed bids is communicated using a multi-party superdense coding scheme that has been experimentally demonstrated. An experimental realization of quantum superdense coding (QSDC) between three parties using nuclear magnetic resonance (NMR) has been reported by Wei et al. [29]. So our presented protocol is experimentally feasible.

5. Security analysis

As our presented scheme is based on quantum secure direct communication based on GHZ states protocol introduced in [19], it resists the intercept-and-resend attack and disturbance attack. Here we discuss this two possible types of attack. We suppose that malicious bidder, say Charlie, prepares a sequence of single particle B in the state $(\lvert 0\rangle_{111})$ or $(\lvert +\rangle_{111})$ randomly. When Alice sends particles b and c to Bob and Charlie, he takes the particles b and keeps them with him, and sends the particles B to Bob, so Bob will take B particles for b particles and encodes his secret messages on B particles and sends them back to Alice, so Charlie can take these particles perform single particle measurements on them. Since the particles B is prepared by Charlie, he can obtain Bob’s encoding bids according to the original states of particles B and the results of his measurement. Then he can encode the same messages on the particles b and also he can encode the better bid on particle c and sends them back to Alice, so he can win the auction. This is the intercept-and-resend attack. However, the method described in Step II can resist the attack, namely, Alice, Bob and Charlie collaborate to select randomly a sufficiently large subset of particles from the M groups to check whether there is any eavesdropping in the channel through analyzing the error rate. If there are no attacks, the measurement result of Alice, Bob and Charlie should have deterministic correlation [19].

The other type of attack is disturbance attack, where malicious bidder can intercept the particles b when the particles are transmitted from Bob to Alice. malicious bidder, say Charlie, may either measure on the particles b or perform one of the unitary operations $I$ and $i_5$ on them. By doing so, the entanglement between each three particles b, c and a is destroyed or the phase of the entanglement is changed. In this case, Charlie can only remain undetected and he can not gain the information encoded by Bob. To resist the disturbance attack, Alice asks Bob and Charlie to announce publicly the positions of their particles and a part of their secret messages to her to check whether the particles travelling from Bob’s and Charlie’s sites to Alice’s site have been attacked. However, if the particles are attacked, the malicious bidder, Charlie cannot get any useful information but he can interrupt the transmissions [19].

6. Summary

In summary, we have presented a new experimentally feasible and secure quantum sealed-bid auction protocol using a Multi-party quantum secure direct communication based on GHZ entangled state. This protocol is a direct application of the multi-party superdense coding scheme to the sealed-bid auction problem. It has been seen that in the presented scheme by using M groups n-particle GHZ states multi-party bidders Bob, Charlie, ..., and Zach can offer their bids. and measuring the final quantum GHZ states by auctioneer gives the auction outcome. Actually in the pre-
sented scheme each bit in the sealed-bid is communicated using a multi-party superdense coding. Here it has been shown that scheme is secure not only against the intercept-and-resend attack but also against disturbance attack. Also it has been seen that using this method guarantees the honesty of the protocol, and malicious bidders can not collude with auctioneers.

Acknowledgements

It is a pleasure to thank the reviewers and the editor for their many fruitful discussions about the topic and of Alimorad Ahmadi for his helpful comments and the final edition of the paper. Also the author would like to thank Soheila Gholipour and Yasna Naseri for their interests in this work. This work is supported by Islamic Azad University, Kermanshah Branch, Kermanshah, Iran.

References