Using Multi-particle Entanglement in Secure Communication Scenarios

Mosayeb Naseri[*]

Islamic Azad University, Kermanshah Branch, Kermanshah, Iran
Sepehr1976@yahoo.com

Abstract. The Quantum Entanglement lies at the heart of the new field of quantum communication and computation. Recently, quantum information theory has shown the tremendous importance of quantum correlations for the formulation of new methods of information transfer and for algorithms exploiting the capabilities of quantum computers. This paper describes the application and the importance of the multi-particle entangled states in secure communication scenarios. We show how to make communication secure against eavesdropping using entanglement-based quantum communication, and how to apply this communication protocols in real life situations.

1 Introduction

Over the last 20 years quantum information theory and specially quantum communication has established itself as promising applications of quantum physics. In this way, one of the important scopes is to evaluate the practical applicability of quantum information science in real life. In real life every day people have to make important decisions that should remain secret. Protecting the privacy of those decisions, if their results are to be communicated, can be a challenging problem. Some examples of such decisions are voting and auction.

Recent research on quantum computation and quantum information allowed using it for describing real life communication scenarios. Financial market phenomena, has been considered in quantum information by researchers. Quantum information has extended the scope of game theory for the quantum world [1-4]. Also quantum game theory has been used for describing financial market phenomena [5, 6].

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 have been extended to quantum version of auctions [5, 6]. An auction usually has three transactional types: traditional English auction, Dutch auction and sealed-bid auction. 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 bottom 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

[*] Corresponding author.

A. Sergienko, S. Pascazio, and P. Villoresi (Eds.): QuantumCom 2009, LNICST 36, pp. 249–257, 2010.

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 submits their own bids to the auctioneer. After the opening phase, the auctioneer makes all the bids public and determines the winner. Recently we have presented a secure quantum sealed-bid auction protocol, in which, 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 [7].

On the other hand, a quantum telephone protocol including the dialing process and the talking one has proposed by Xiaojun Wen, Yun Liu, Nanrun Zhou in 2007 [8]. In this protocol in the dialing process, with their respective secret keys, the legitimate communicators Alice and Bob can pass the authentication by Charlie acting as a telephone company. In the talking process, Charlie provides the authenticated Alice and Bob with a quantum channel sequence, on which Alice and Bob can communicate with each other directly and privately by virtue of some encoding operations. Unfortunately, it has been shown that the quantum telephone protocol in its original form is not as secure as it claimed. In our recent work we have shown that the dishonest server can obtain full information of the communication with zero risk of being detected [9].

The aim of this work is to show how to use quantum information in designing a real life communication protocols.

2 Quantum Telecommunication

Quantum key distribution (QKD) is an ingenious application of quantum mechanics, in which two remote legitimate users (Alice and Bob) establish a shared secret key through the transmission of quantum signals and use this key to encrypt (decrypt) the secret messages. Since Bennett and Brassard presented the pioneering work in 1984 [10], a variety of QKD protocols have been proposed. Quantum key distribution has attracted much attention of the researchers. Quantum secure direct communication (QSDC) [11-22] is a branch of quantum cryptography, which allows that the sender transmits directly the secret (not a random key) to the receiver in a deterministic and secure manner. Quantum encryption algorithm has also been investigated [23, 24]. The goal of quantum encryption algorithm and classical encryption algorithm is consistent, i.e. to protect secret information or keep communications private. Quantum secret sharing (QSS) [25, 26] is another important application of quantum mechanics, which allows a secret to be shared among many participants in such a way that only the authorized groups can reconstruct it. Boström and Felbinger put forward a ping-pong QSDC scheme by using Einstein-Podolsky-Rosen (EPR) pairs [13]. Based on the idea of a ping-pong QSDC scheme, Nguyen proposed a quantum dialogue scheme (the quantum dialogue is actually two-way communication) by using EPR pairs [27]. However, an eavesdropper who adopts the intercept-and-resend attack strategy can steal the secret messages without being detected.

2.1 Quantum Dialogue

To get information from Alice, Bob prepares two qubits $|\phi_{kl}\rangle_{ht}$ in one among the four mutually orthogonal Bell states,

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

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

$$|\phi_{10}\rangle_{ht} = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle),$$

$$|\phi_{11}\rangle_{ht} = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle),$$

where, h and t stand for "home" and "travel" qubits, respectively. Then he sends qubit “t” to Alice while stores qubit “h” with himself. Alice decides to use qubit “t” as the message mode (MM) or the control mode (CM) randomly. In the MM, Alice encodes her information by performing a unitary operation I or σ_z on qubit “t” corresponding to her message bit 0 or 1, then he pongs it back to Bob, who can obtain Alice’s information by a Bell measurement. In the CM, Alice performs a measurement in the basis, $B_z = |0\rangle, |1\rangle$ and sends the result to Bob via a public classical channel. Bob then also switches to the CM and performs a measurement in the same basis B_z. Comparing his own result with that of Alice, Bob can detect the presence of Eve [27] .

2.2 Quantum Telephone

A quantum telephone protocol including the dialing process and the talking one has proposed by Xiaojun Wen , Yun Liu , Nanrun Zhou in 2007 [8]. In this protocol in the dialing process, with their respective secret keys, the legitimate communicators Alice and Bob can pass the authentication by Charlie acting as a telephone company. In the talking process, Charlie provides the authenticated Alice and Bob with a quantum channel sequence, on which Alice and Bob can communicate with each other directly and privately by virtue of some encoding operations. Unfortunately, it has been shown that the quantum telephone protocol in its original form is not as secure as it claimed .i.e., recently Y. Sun et al. in [28] have shown that an attacker could eavesdrop on the communicator's conversation without introducing any error by an attack with fake particles and local operations. At the same time, very recently, we have realized that a dishonest server, an eavesdropper, can gain full information of the communication with zero risk of being detected by using fake entangled particles [29]. Then the authors of the both papers [28, 29] have presented a modification procedure to avoid the vulnerability of the protocol against the possible presented attacks.

It is apparently that the modifications presented in [28, 29], improve the original protocol against the eavesdropping of the secure information, but I think the main theoretical source of insecurity of the protocol still remains! Since I see here the main source of theoretical insecurity, let me spend some more words on the theoretical condition for the security. As a matter of fact, each and every secure quantum communication protocol, in fact, the efficiency of transportation was bounded by Holevo quantity [30], which shows that n qubits cannot be used to transmit more than n bits of classical information in a 2-level system. Obviously, in secure quantum telephone protocol, Alice and Bob can transmit 4 bits secret message (two for Alice and two for Bob) via per EPR pair in the above communication. Whereas, Gao et al. [28] pointed out that among the 4-bit information only 2 bits are transmitted securely. Due to Bob's declaration, everyone (of course the Eve) can infer that there would be four possibilities for operations performed by Bob and Alice. Assuming four possibilities having equal probability, the channel contains only two bits of secret information for Eve.

$$-\sum_i p_i \log\ p_i = -4(\frac{1}{4}) \log_2 \frac{1}{4} = 2.$$

In other words, 2-bits secret has been leaked to Eve. Since, this capacity has been exceeded in secure quantum telephone protocol, it is undoubtedly insecure. However, it seems that this theoretical limitation has been tacitly mentioned by the authors of reference [28] (Ref. [28] page 2280 second column second paragraph).

3 Quantum Finance (Quantum Auction)

Recent research on quantum computation and quantum information allowed using it for describing financial market phenomena. Quantum information has extended the scope of game theory for the quantum world [1-3]. Also quantum game theory has been used for describing financial market phenomena [5,6]. 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 have been extended to quantum version of auctions [31]. An auction usually has three transactional types: traditional English auction, Dutch auction and sealed-bid auction, 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 bottom 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 submits his/her own bids to the auctioneer. After the opening phase, the auctioneer makes all the bids public and determines the winner.

The crucial issue of any auction protocol is its security. Each secure auction protocol includes an auctioneer, a third party or an auction host and many bidders (sometimes an auctioneer plays the role of third party in auction protocols). Essentially the most important requirements of secure auction can be summarized as follows [32]:

(1) Anonymity: all bidders can keep anonymity in an auction, even if the bid is opened, i.e., no one can gain access to other bidder's information, except the auction host. In addition, only the auction host stores the bidder's information, there- fore, it can maintain anonymity in the auction, even after the bid is opened.

(2) Public verifiability: all the bidding prices and the winning prices can be verified by anyone, i.e., everybody should be able to see all the bids and verify that the auctioneer chosen the biggest one to prevent the dishonest auction host or auctioneer cheating bidders and performing a conspiracy with a malicious bidder.

(3) Accountability of bidder: the auction cannot be interrupted by any malicious bidders with a dishonest bid without being detected. That is to say, the auction host can verify each bid when the bidder casts a bid.

(4) Fairness: all sealed-bids are opened at the same time, and the third party or the auctioneer cannot collude with a malicious bidder to cheat the other bidders.

(5) Non-repudiation: the property of non-repudiation is that both the bidder cannot deny having cast his/her bid and the auction host cannot deny that he has received the bid from the bidder.

(6) Traceability: the winning bidder can be identified when the auction is finished.

There are few quantum auction protocols, where the applications of quantum game theory have been extended to quantum version of auctions. Recently, we proposed a quantum sealed-bid auction protocol using quantum secure direct communication based on GHZ states [7]. Here, the protocol of quantum sealed-bid auction protocol is reviewed.

3.1 Quantum Sealed-Bid Auction

The auction model consists of one buyer agent Alice, who is the auctioneer that needs a particular L items (service or product) and a fixed number of n seller agents Bob, Charlie . . . and Zach, who are the bidders. The scheme can be explained as follows:

- At the beginning of the auction, the buyer, Alice announces her request items (which consist of the items desired characteristics and the auction protocol) by classical channel. In this step all parties agree on that Auctioneer, Alice can perform the four unitary operations I; σ_x; i σ_y; σ_z to encode two bits classical information 00, 01, 10, 11. Also they agree on that all bidders can only perform the two unitary operations I; σ_x to encode classical bits information 0, 1, where I; σ_x; i σ_y and σ_z are Pauli matrixes [7].
- The auctioneer Alice generates M groups N-partite GHZ states. For example, suppose that the i-th GHZ state is in the form of

$$\left|\phi\right\rangle^{i}{}_{abc\ ,\dots\ z}=\frac{1}{\sqrt{2}}\left(\left|0\,s^{i}{}_{1}s^{i}{}_{2}\dots s^{i}{}_{N-1}\right\rangle+\left|1\,\overline{s}^{i}{}_{1}\,\overline{s}^{i}{}_{2}\dots\overline{s}^{i}{}_{N-1}\right\rangle\right)_{abc\ ,\dots\ z}.$$

  Where $s^{i}{}_{j}=0$ or 1, $\overline{s}^{i}{}_{j}=s^{i}{}_{j}+1$ modulo 2, and the subscripts a; b; c; . . . ; z represent the particles belonging to Alice, Bob, Charlie . . . and Zach, respectively. Then Alice sends b particles to Bob, c particles to Charlie . . . z particles to Zach.
- Bob, Charlie . . . and Zach confirm Alice that they have received all the particles b, particles c . . . and particles z, 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 $|0\rangle, |1\rangle$ or $|+\rangle, |-\rangle$ randomly and tells all other bidders the position, the measuring basis and the measurement result for each of the T groups b particles via classical channel and ask 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 measure T groups a particles. According to the measurement results of Bob, Charlie. . . Zach and herself, Alice can determine whether there is any eavesdropping. 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.

- If no error happens, the N- 1 bidders Bob, Charlie . . . and Zach encode their secret bids by applying operators I; iσ_y on their leftover particles and return their particles to Alice.
- After receiving all the particles from the N- 1 bidders, for each GHZ state, Alice encodes her final message with one of the four unitary operations I; σ_x; i σ_y and σ_z on her particle. Then she performs N-particle GHZ-basis measurements on the remaining groups a; b; c; . . . ; z and publicly announces the initial states and the measurement results of the GHZ states leftover. According to the initial states and the measurement results of the GHZ states leftover, Alice can read out the secret bids of Bob, Charlie . . . and Zach. Also every bidder can deduce the secret bids encoded by the other bidders. Concluding the auction winner can be determined simply.

Very recently, the Quantum Sealed-Bid Auction has been considered by different research groups and it has been shown that be shown that a dishonest bidder can obtain all the other one's secret bids by double CNOT attack or using fake entangled particles attack and according to these secret bids values he can encode the better bids on his particles and win the auction [33-33].

However, it is apparently that with the presented improvement, the original protocol does complete the task of a sealed-bid auction fairly. But I think one of the main sources of insecurity of the original protocol still remains!, in fact, in any secure auction protocol the possibility of collusion of the bidders with the auctioneer should be mentioned and the protocol should contains a security method which is guarantees that if one of the bidders or a group of the bidders decide to collude with the auctioneers, they would not succeed. It is clear, the original article, does not present such a method to bind the collusion of the bidders with the auctioneer. It is noticeable that every secure communication protocol, whether quantum or classical, needs an authenticated channel. User authentication (also called user identification) makes it possible for a communicator to prove his/her identity, often as the first step to log into a system. If there is no authenticated channel, then a man-in-the-middle attack is always possible, resulting in a complete loss of security. In fact, the perfect security of a quantum communication protocol stands and falls with the integrity of the public channel. Usually the classical channel is tacitly assumed to be as the one and only trusted channel of the protocol. Since in the original protocol it is not mentioned how the public communication is realized, the reader must assume that it is not necessarily the auction host or the auctioneer who act as the public channel throughout the entire protocol. Concluding, it is possible to use the auction host or auctioneer as the one and only trusted channel of the protocol, doing so would make the protocol more straightforward, because it is in fact the auction host who establishes the quantum channels between the bidders in the auction, and thus actively performs an authentication of the legitimate parties (not of himself, though). Also, engaging the auction host as the authenticated channel would avoid the vulnerability of the protocol against the collusion of the dishonest auction host or auctioneer with the bidders.

4 Quantum Voting

Recent research on quantum computation and quantum information makes it possible to using it for voting protocols [35, 36]. The advantage of quantum voting protocols is that security that is based on the laws of quantum mechanics rather than assumptions about computational complexity.

Reliable voting protocols should satisfy a number of conditions [37], three of which are: (i) security, (ii) verifiability, and (iii) privacy. The security condition guarantees that all users can influence the result only by casting a *single* valid vote. That is, each voter can vote just once (non-reusability), only legitimate users can vote (eligibility) and no one can learn any intermediate result (fairness). The strongest version of the verifiability requirement is that each voter can verify the correctness of the result; however none of the voters is able to prove how he or she voted. This prevents vote buying. A voting scheme satisfying all properties except the privacy condition is easy to implement. Privacy is related to the secrecy of the ballots, or equivalently to the anonymity of the voters. Ideally, no one should be able to tell how any of the voters voted.

In 2006 Mark Hillery et al., proposed quantum protocols that guarantee the anonymity of participants in voting procedures and can be used in several complex communication tasks. The advantage of quantum voting protocols is that security that is based on the laws of quantum mechanics rather than assumptions about computational complexity [35]. In this protocol quantum voting is based on voters applying local operations to an entangled state, in which a method of preventing voters from cheating is presented.

On the other hands, quantum protocols for ensuring the anonymous voting in a number of different scenarios have been presented by J. A. Vaccaro et al. [36].

5 Conclusion

Quantum computing and communications are novel ways of engineering quantum systems and are proving to dramatically change the way we think about computation, complexity, information, and communication. We have presented some applications of multi-particle entanglement quantum communication, in real life scenarios. Undoubtedly, quantum technologies will play a very important role in the future, and already to date, several companies are commercializing quantum communication systems.

Acknowledgement

It is a pleasure to thank Soheila Gholipour and Yasna Naseri for their interests in the present work. This work is supported by Islamic Azad University, Kermanshah Branch, Kermanshah, IRAN.

References

1. Meyer, D.A.: Quantum Strategies. Phys. Rev. Lett. 82, 1052 (1999)
2. Eisert, J., Wilkens, M., Lewenstein, M.: Quantum Games and Quantum Strategies. Phys. Rev. Lett. 83, 3077 (1999)
3. Piotrowski, E.W., Sladkowski, J.: Quantum Game Theory. In: Mathematical Physics Frontiers. Nova Science Publishers, Inc., Berlin (2004)
4. Piotrowski, E.W., Sladkowski, J.: An invitation to quantum game theory. Int. J. Theor. Phys. 42, 1089 (2003)
5. Piotrowskia, E.W., Sladkowski, J.: Quantum English Auctions. Physica A 318, 505 (2003)
6. Piotrowskia, E.W., Sladkowski, J.: Quantum Auctions: Facts and Myths. Physica A 387, 3949 (2008)
7. Naseri, M.: Secure quantum sealed-bid auction. Opt. Commun. 282, 1939 (2009)
8. Wen, X., et al.: Secure Quantum Telephone. Optics Communications 275, 278–282 (2007)
9. Naseri, M.: Eavesdropping on secure quantum telephone protocol with dishonest server. Opt. Commun. (2009), doi:10.1016/j.optcom.2009.05.012
10. Bennett, C.H., Brassard, G.: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processings, Bangalore, India, p. 175. IEEE, New York (1984)
11. Beige, A., Engler, B.G., Kurtsiefer, C., Weinfurter, H.: Secure communication with a publicly known key. Acta Phys. Pol. A 101, 357 (2002)
12. Long, G.L., Liu, X.S.: Theoretically efficient high-capacity quantum-key-distribution scheme. Phys. Rev. A 65, 32302 (2002)
13. Bostrom, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. 89, 187902 (2002)
14. 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)
15. Deng, F.G., Long, G.L., Li, X.H., Wen, K., Wang, W.Y.: Improving the security of secure direct communication based on the secret transmitting order of particles. Front. Phys. China 2(3), 251 (2007)
16. Zhang, Z.J., Man, Z.X., Li, Y.: Improving Wójcik's eavesdropping attack on the ping–pong protocol. Phys. Lett. A 333, 46 (2004)
17. Deng, F.G., Long, G.L.: Secure direct communication with a quantum one-time pad. Phys. Rev. A 69, 052319 (2004)
18. Zhang, Z.J., Li, Y., Man, Z.X.: Improved Wójcik's eavesdropping attack on ping-pong protocol without eavesdropping-induced channel loss. Phys. Lett. A 341, 385 (2005)
19. Wang, C., Deng, F.G., Long, G.L.: Multi-step quantum secure direct communication using multi-particle Green–Horne–Zeilinger state. Opt. Commun. 253, 15 (2005)
20. Zhang, Z.J., Man, Z.X., Li, Y.: The Improved Bostrom–Felbinger Protocol Against Attacks Without Eavesdropping. Int. J. Quantum Inform. 2, 521 (2005)
21. Man, Z.X., Zhang, Z.J., Li, Y.: Quantum Dialogue Revisited. Chin. Phys. Lett. 22, 18 (2005)

22. Deng, F.G., Long, G.L.: Secure direct communication with a quantum one-time pad. Phys. Rev. A 69, 052319 (2004)
23. Wojcik, A.: Eavesdropping on the "Ping-Pong" Quantum Communication Protocol. Phys. Rev. Lett. 90, 157901 (2003)
24. Zeng, G.H., Keitel, C.H.: Arbitrated quantum-signature scheme. Phys. Rev. A 65, 042312 (2002)
25. Boykin, P.O., Roychowdhury, V.: Optimal encryption of quantum bits. Phys. Rev. A 67, 042317 (2003)
26. Hillery, M., Buzek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A 59, 1829 (1999)
27. Karlsson, A., Koashi, M., Imoto, N.: Quantum entanglement for secret sharing and secret splitting. Phys. Rev. A 59, 162 (1999)
28. Nguyen, B.A.: Quantum Dialogue. Phys. Lett. A 328, 6 (2004)
29. Sun, Y., et al.: Improving the security of secure quantum telephone against an attack with fake particles and local operations. Opt. Commun. 282, 2278 (2009)
30. Naseri, M.: Eavesdropping on secure quantum telephone protocol with dishonest server. Optics Commun. 282, 3375–3378 (2009)
31. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000)
32. Liu, X.S., et al.: General scheme for superdense coding between multiparties. Phys. Rev. A 65, 022304 (2002)
33. Subramanian, S.: Design and verification of a secure electronic auction protocol. In: Proc. IEEE 17th Symposium on Reliable Distributed Systems, Washington DC, USA, pp. 204–210 (1998)
34. Yang, Y.G., et al.: Improved Secure Quantum Sealed-Bid Auction. Optics Communications 282, 4167–4170 (2009)
35. Qin, S.-J., et al.: Cryptanalysis and improvement of a secure quantum sealed-bid auction. Optics Communications 282, 4014–4016 (2009)
36. Hillery, M., et al.: Towards quantum-based privacy and voting. Physics Letters A 349, 75–81 (2006)
37. Vaccaro, J.A., et al.: Quantum protocols for anonymous voting and surveying. Physical Review A 75, 012333 (2007)
38. Schneier, B.: Applied Cryptography, p. 125. Wiley, New York (1996)