An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement

2009 J. Phys. A: Math. Theor. 42 055305

(http://iopscience.iop.org/1751-8121/42/5/055305)

IOP PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND THEORETICAL

J. Phys. A: Math. Theor. **42** (2009) 055305 (9pp) doi:10.1088/1751-8113/42/5/055305

An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement

Yu-Guang Yang[1,2,3] **and Qiao-Yan Wen**[4]

[1] College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, People's Republic of China
[2] State Key Laboratory of Integrated Services Network, Xidian University, Xi'an 710071, People's Republic of China
[3] State Key Laboratory of Information Security (Graduate University of Chinese Academy of Sciences), Beijing 100049, People's Republic of China
[4] State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, People's Republic of China

E-mail: yangyang7357@bjut.edu.cn and wqy@bupt.edu.cn

Received 3 April 2008, in final form 28 November 2008
Published 6 January 2009
Online at stacks.iop.org/JPhysA/42/055305

Abstract

Following some ideas of the quantum secret sharing (QSS) protocol (2008, *Phys. Lett.* A **372**, 1957), we propose an efficient quantum private comparison (QPC) protocol for comparing information of equality with the help of a third party (TP). The protocol can ensure fairness, efficiency and security. The protocol is fair, which means that one party knows the sound result of the comparison if and only if the other one knows the result. The protocol is efficient with the help of the TP for calculating. However, the TP cannot learn any information about the players' respective private inputs and even about the comparison result and cannot collude with any player. The protocol is secure for the two players, that is, any information about their respective secret inputs will not leak except the final computation result. A precise proof of security of the protocol is presented. Applications of this protocol may include private bidding and auctions, secret ballot elections, commercial business, identification in a number of scenarios and so on.

PACS numbers: 03.67.Dd, 03.65.Ta, 89.70.+c

1. Introduction

Quantum information, an ingenious application of quantum mechanics within the field of information has attracted a lot of attentions [1–5]. In particular, almost all the branches

of quantum communication have been developed quickly since the original protocol was proposed by Bennett and Brassard [6] in 1984, such as quantum key distribution (QKD) [6–14], quantum secure direction communication (QSDC) [15–17], quantum teleportation [3, 4], quantum secret sharing (QSS) [18–20] and so on. QKD provides a secure way for creating a private key between two remote parties. To date, QKD has progressed quickly and becomes one of the most mature applications of quantum information.

Secret sharing and multiparty computation (also called 'secure function evaluation') are fundamental primitives in modern cryptography, allowing a group of mutually distrustful players to perform correct, distributed computations without leaking their respective secret inputs under the sole assumption that some of them will follow the protocol honestly. Secure multiparty computation can be applied extensively to many applications including private bidding and auctions, secret ballot elections, commercial business, identification in a number of scenarios and so on. At present, research on secure multi-party computation is of great interest in modern cryptography (see [21] for a survey). It should be acknowledged that if any function can be computed securely, then it results in a very powerful tool. In fact, all natural protocols are, or can be rephrased to be, special cases of the multi-party computation problems. Design and analysis of the special multi-party computation protocols is meaningful and has attracted much interest in this field.

In the traditional secure two-party computation scenario [22, 23], Alice has a secret input x, Bob has a secret input y, and both of them wish to compute $f(x, y)$ which is well known to the two parties; the usual example is that of two millionaires who wish to compare their wealth without disclosing how much they own [23]. Colbeck showed that unconditionally secure two-party classical computation is impossible for many classes of function by attacks [24]. However the story is changed when it was extended to the quantum setting by [25]. A secure quantum multiparty protocol allows n players $P_1, \ldots, P_n$ to compute an n input quantum circuit where each player P_i is responsible for providing one of the input states. The output of the circuit is broken into n components $H_1 \otimes H_2 \otimes \ldots \otimes H_n$. P_i receives the output H_i. Note that the inputs are arbitrary (possibly entangled) quantum states and each player simply has his input in his possession—he does not need to know its classical description. However we wish to achieve the same functionality if each player replaces his secret input quantum state with a special unitary operation and a TP measures the output quantum states. Many particular secure multiparty computation problems exist, such as secure multiparty summation, the private comparison of the size of two or more numbers and comparing information of equality. In fact, comparing information of equality is a very important problem in secure multiparty quantum computation, which is critical in quantum auction [26] and quantum voting [27, 28] and other special cases.

In this paper, following some ideas of the QSS protocol [29], we propose an efficient protocol for comparing information of equality using decoy photons and two-photon entangled states. Suppose there are a third party TP, and two players Bob and Charlie. The secret inputs of Bob and Charlie are x and y, respectively. The protocol can ensure

(i) *Fairness:* the protocol is fair, which means that one player knows the sound result of $x = y$ if and only if the other one knows the result and that one player knows the sound result of $x \neq y$ if and only if the other one knows the result.

(ii) *Security:* although the protocol is implemented with the help of a TP for calculating, the TP cannot learn any information about the players' private inputs and even about the comparison result. One player cannot deduce the other's secret input from the comparison result of $x \neq y$ and even the size relation of x and y. The protocol is secure for the two players, that is, any information about their secret inputs will not leak including the final comparison result.

(iii) *Efficiency:* the protocol is implemented with the help of the TP for calculating, which improves the efficiency of the protocol. Here, the term 'efficiency' means the involvement of the TP will improve the efficiency of the protocol in contrast to the case without the TP. That is, if the protocol involves only the two players, it maybe consumes more quantum and classical resources.

2. Comparing information of equality between two parties

Similar to [29, 19], let us first define the four Bell states as

$$\begin{aligned}|\phi^{\pm}\rangle &= \tfrac{1}{\sqrt{2}}(|+z\rangle_B|+z\rangle_C \pm |-z\rangle_B|-z\rangle_C),\\ &= \tfrac{1}{\sqrt{2}}(|+x\rangle_B|\pm x\rangle_C + |-x\rangle_B|\mp x\rangle_C),\\ |\psi^{\pm}\rangle &= \tfrac{1}{\sqrt{2}}(|+z\rangle_{\mathrm{B}}|-z\rangle_{\mathrm{C}} \pm |-z\rangle_{\mathrm{B}}|+z\rangle_{\mathrm{C}}),\\ &= \tfrac{1}{\sqrt{2}}(|\pm x\rangle_B|+x\rangle_C - |\mp x\rangle_B|-x\rangle_C),\end{aligned} \tag{1}$$

where $|+z\rangle \equiv |0\rangle$ and $|-z\rangle \equiv |1\rangle$ are the spin eigenstates along the z-direction. $|+x\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-x\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ are the spin eigenstates along the x-direction. The subscripts B and C denote the two particles in a Bell state. The four unitary operations $U_i (i = 00, 01, 10, 11)$ can transform one of the Bell states into another, i.e., $I \otimes U_{00}|\psi^{\pm}\rangle = |\psi^{\pm}\rangle$, $I \otimes U_{00}|\phi^{\pm}\rangle = |\phi^{\pm}\rangle$, $I \otimes U_{01}|\psi^{\pm}\rangle = -|\psi^{\mp}\rangle$, $I \otimes U_{01}|\phi^{\pm}\rangle = |\phi^{\mp}\rangle$, $I \otimes U_{10}|\psi^{\pm}\rangle = |\phi^{\pm}\rangle$, $I \otimes U_{10}|\phi^{\pm}\rangle = |\psi^{\pm}\rangle$, $I \otimes U_{11}|\psi^{\pm}\rangle = |\phi^{\mp}\rangle$, $I \otimes U_{11}|\phi^{\pm}\rangle = -|\psi^{\mp}\rangle$.

Here

$$\begin{aligned}U_{00} &= I = |0\rangle\langle 0| + |1\rangle\langle 1|,\\ U_{01} &= \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|,\\ U_{10} &= \sigma_x = |1\rangle\langle 0| + |0\rangle\langle 1|,\\ U_{11} &= i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|.\end{aligned} \tag{2}$$

For simplicity, we consider the case with two distrustful players who want to compare whether their secrets are equal with a help of the TP. Suppose that the two players, say, Bob and Charlie have secrets x and y, respectively.

Let

$$X = (x_{N-1}, x_{N-2}, \ldots, x_0) \tag{3}$$

and

$$Y = (y_{N-1}, y_{N-2}, \ldots, y_0) \tag{4}$$

be the binary representations of x and y in F_{2^N}, respectively, where $x = \sum_{i=0}^{N-1} x_i 2^i$, $y = \sum_{i=0}^{N-1} y_i 2^i$, with $x_i, y_i \in \{0, 1\}$, $2^{N-1} \leqslant \max\{x, y\} < 2^N$. For other $i \geqslant N$ and $i < 0$, $x_i = y_i = 0$.

Bob and Charlie share a secret hash function H beforehand. Here the hash function is defined as

$$H : \{0, 1\}^N \to \{0, 1\}^M, \tag{5}$$

where N and M denote the length of the secret inputs and the length of the hash values of the secret inputs, respectively. The hash values of X and Y are

$$H(X) = (x'_{M-1}, x'_{M-2}, \ldots, x'_0) \tag{6}$$

and

$$H(Y) = (y'_{M-1}, y'_{M-2}, \ldots, y'_0), \tag{7}$$

respectively.

If M is even, $H(X)$ and $H(Y)$ are divided into groups $\{(x'_{M-1}, x'_{M-2}), (x'_{M-3}, x'_{M-4}), \ldots, (x'_1, x'_0)\}$ and $\{(y'_{M-1}, y'_{M-2}), (y'_{M-3}, y'_{M-4}), \ldots, (y'_1, y'_0)\}$, respectively. Otherwise, $H(X)$ and $H(Y)$ are divided into groups $\{(x'_{M-1}, x'_{M-2}), (x'_{M-3}, x'_{M-4}), \ldots, (x'_0, x'_{-1})\}$ and $\{(y'_{M-1}, y'_{M-2}), (y'_{M-3}, y'_{M-4}), \ldots, (y'_0, y'_{-1})\}$, respectively.

2.1. Our scheme

Now, let us describe the principle of our QPC scheme in detail as follows.

Step 1. The TP, Bob and Charlie agree that the four unitary operations $U_i (i = 00, 01, 10, 11)$ represent two-bit information 00,01,10 and 11, respectively.

Step 2. The TP prepares a sequence of $n(n > M/2)$ ordered EPR pairs T each randomly in one of the four Bell states only known to him. We denote the n ordered EPR pairs in the sequence T with $\{(t_B^1, t_C^1), (t_B^2, t_C^2), \ldots, (t_B^n, t_C^n)\}$, where the superscripts $1, 2, \ldots, n$ indicate the order of each EPR pair in the sequence T, and the subscripts B and C represent the different photons in each EPR pair. Subsequently, the TP takes the photon B from each EPR pair in the sequence T to form an ordered photon sequence $\{t_B^1, t_B^2, \ldots, t_B^n\}$, called the sequence T_B. The remaining partner photons compose of another ordered photon sequence $\{t_C^1, t_C^2, \ldots, t_C^n\}$, called the sequence T_C. He sends the sequence T_B to Bob via the TP–Bob quantum channel and T_C to Charlie via the TP–Charlie quantum channel. For preventing the dishonest player from eavesdropping, similar to [29], the TP adopts the decoy photon technique by inserting decoy photons each randomly in one of the four nonorthogonal states $\{|0\rangle, |1\rangle, |+x\rangle, |-x\rangle\}$ into the sequences T_B and T_C at random positions with the probability p_d, respectively.

Step 3. After Bob and Charlie publicly confirm that they have received all particles, to guarantee the security of the transmission from the TP to the two players, the TP, Bob and Charlie should check whether the particles are eavesdropped during the transmission. The checking procedure is (i) the TP informs Bob and Charlie of the positions and the measuring bases (MBs) of the decoy photons sent to them, respectively. (ii) Bob and Charlie perform the same MBs as the TP published and publish their measurement outcomes, respectively. The TP analyses the error rate. If the error rate is higher than the threshold ε_1, then he aborts the protocol. Otherwise, they proceed to step 4.

Step 4. Before Bob and Charlie encode their secrets, they still have to check whether the TP is honest. That is, they need to check whether the remaining photons held by them are in a genuine Bell state by using the correlation property of EPR pairs. The checking procedure is (i) Bob and Charlie choose some photons randomly in the sequences T_B and T_C with the probability p_c and require the TP to publish the states of the randomly chosen EPR pairs. (ii) For each chosen EPR pair, Bob and Charlie measure the corresponding sampling photons with the two MBs, Z or X randomly and announce their measurement outcomes and MBs in the order randomly determined as either ((1) Bob's outcome, (2) Charlie's outcome, (3) Charlie's MB, (4) Bob's MB) or ((1) Charlie's outcome, (2) Bob's outcome, (3) Bob's MB, (4) Charlie's MB). If Bob and Charlie find the error rate is higher than the threshold ε_2, then they abort the protocol. Otherwise they proceed to step 5.

Step 5. Bob and Charlie encode their secrets' hash values $H(X)$ and $H(Y)$ on the remaining photons held by them with the four unitary operations, respectively. If M is even, Bob (Charlie) performs a unitary operation $U_{x'_{2k}x'_{2k+1}}$ ($U_{y'_{2k}y'_{2k+1}}$) on the $(k+1)$th photon in the photon sequence according to his secret bits $x'_{2k}x'_{2k+1}(y'_{2k}y'_{2k+1})$, $k = 0, 1, \ldots, \left|\frac{M-2}{2}\right|$. Otherwise, Bob

(Charlie) performs a unitary operation $U_{x'_{2k-1}x'_{2k}}$ ($U_{y'_{2k-1}y'_{2k}}$) on the $(k+1)$th photon in the photon sequence according to his secret bits $x'_{2k-1}x'_{2k}(y'_{2k-1}y'_{2k})$, $k = 0, 1, \ldots, \left|\frac{M-2}{2}\right|$. To check whether the TP will cheat in the following announcement of his measurement outcomes, Bob and Charlie secretly generate a random number l by using the QKD method. Bob (Charlie) inserts the remaining intact EPR photons into the encoded photon sequence at the positions determined by the value of l. And Bob and Charlie require the TP to publish the states of the remaining EPR pairs beforehand. For checking eavesdropping in the Bob–TP and Charlie–TP quantum channels, each player also inserts decoy photons each randomly in one of the four nonorthogonal states $\{|0\rangle, |1\rangle, |+x\rangle, |-x\rangle\}$ into the EPR photon sequence at random positions with the probability p_e, respectively. And then they send the sequences back to the TP.

Step 6. After the TP publicly confirms that he has received all particles, the TP, Bob and Charlie should first check whether the dishonest player eavesdrops during the transmission by using the checking procedure similar to step 3. If they confirm no eavesdropping, then the TP takes a Bell-basis measurement on each two correlated photons received from Bob and Charlie with the two-photon entanglement basis $\{|\phi^{\pm}\rangle, |\psi^{\pm}\rangle\}$, records these measurement outcomes and publish his initial states of EPR pairs except for eavesdropping check. These measurement outcomes are divided into two sets: the set of the sampling EPR pairs' measurement outcomes, C and that of the encoding EPR pairs' measurement outcomes, M. The TP cannot know the information about which set each measurement outcome of EPR pair belongs to. Bob and Charlie choose a subset of the positions from one of the two sets randomly and ask the TP to publish the measurement outcomes at these chosen positions. For the positions chosen from the set C, if the inconsistency rate between the measurement outcomes and the TP's beforehand announcements is higher than the threshold ε_3, Bob and Charlie can find that the TP is cheating and abort the protocol. Otherwise, they continue to choose a position subset randomly from one of the two sets and ask the TP to publish the measurement outcomes. For the positions chosen from the set M, Bob and charlie can distill the outcomes of the combination of the unitary operations performed by them from the TP' measurement outcomes and their initial states with error correction and privacy amplification [7] and deduce the comparison result.

According to the TP's measurement outcomes of the encoded EPR pairs, Bob and Charlie can obtain whether x is equal to y, but they cannot deduce each other's secret in terms of the one-way property of the hash function. If all the error rates are lower than the threshold $\varepsilon_{\text{th}} = \min\{\varepsilon_1, \varepsilon_2, \varepsilon_3\} = \min\{p_d/4, p_c/4, p_e/4\}$, our QPC protocol can realize the function of comparing whether their secrets are equal, our QPC protocol can realize the function of comparing whether their secrets are equal between two parties without disclosing any knowledge about their respective secrets with the help of the TP. From this QPC protocol, one can easily see that no TP in a QPC protocol is impossible. In the QPC protocol, the TP plays a very important role in preparing the quantum sources and measuring them, which provides a fair comparison environment.

2.2. *Security analysis*

As pointed out in [30–32], a participant generally has more advantages in an attack than an outsider eavesdropper in the QSS protocols. If a QSS protocol is secure for a dishonest participant, it is secure for any eavesdropper. So the participant attack should be paid more attention to in the security analysis of a QSS protocol. The security analysis of a QPC protocol is, however, different from and even more complex than that of a QSS protocol as the attack from the compromised TP except the player has to be considered in the design of QPC protocols. To see this in a sufficient way, we will consider three possible cases: (1) the

honest TP and Charlie, and a dishonest one Bob. Because the role of Bob is same as that of Charlie. Without loss of generality, we assume Bob is the dishonest one; (2) a compromised TP and two honest players Bob and Charlie. (3) the TP colludes with a dishonest player, say Bob.

Case 1. The honest TP and Charlie, and a dishonest one Bob.

If Bob is dishonest, the purpose of his attack is to try to obtain the other party's secret by cheating. In fact he cannot attain this goal. The reasons are as follows. Similar to [29], the process of eavesdropping check with decoy photons between the TP and Charlie does not require Bob to participate in it, which will forbid Bob to eavesdrop the quantum channel from the TP to Charlie with an opaque attack strategy [33], especially when the transmission efficiencies are lower than 50%. Similar to [29, 34], the TP exploits the refined error analysis technique [34] for checking eavesdropping of the process of the transmission from the TP to the two players Bob and Charlie. That is, the TP only picks up the decoy photons to check eavesdropping. This eavesdropping check in step 3 will find out Bob monitoring the quantum channel from the TP to Charlie as any eavesdropping will leave a trace in the outcomes of the decoy sampling photons. Hence, the use of the decoy photons can prevent the dishonest player from eavesdropping freely. Last, if Bob tries to take a disturbance attack, no cryptography is possible at all. Also, the parties can complete a faithful qubit transmission against collective noise with the technique in [35], which will improve the practical efficiency in this QPC protocol.

As for the delay-photon Trojan horse attack and the invisible photon eavesdropping (IPE) Trojan horse attack [36, 37], the player can insert a filter in front of his devices to filter out the photon signal with an illegitimate wavelength, and the eavesdropper obtains no information by performing IPE Trojan horse attack strategies.

As for the photon-number-splitting (PNS) attack [31, 37, 38], the player can insert a filter in front of his devices to filter out the photon signal with an illegitimate wavelength and use some beam splitters to split the sampling signals chosen for eavesdropping check before they measure the signals with the MB Z or X.

Case 2. A compromised TP, and two honest parties Bob and Charlie.

To check whether the TP is honest, Bob and Charlie need to check whether the remaining photons held by them are in a genuine Bell state. It is known that when a qubit of an entangled pair travels in a noisy quantum channel, the initial entanglement might be lost. Hence, a security problem for this protocol in a noisy channel seems to arise. Incidentally, the quantum purification and distillation or quantum repeater techniques should be adopted if the quantum channel noise or decoherence is taken into account [3, 39–43]. Once the two players have shared an entangled qubit pair, then the TP's attack can be detected by adopting the strategy suggested in [15, 44], that is, using the two-set-measuring-bases method to check the qubit distribution security. In this case, if there exists a compromised TP, any eavesdropping attack will inevitably introduce some detectable errors [15, 44]. This indicates that any attack of the TP's can be found. The TP cannot learn any information about the players' respective private inputs and even about the comparison result in that the TP cannot discriminate between the encoded EPR pairs and the sampling ones because Bob and Charlie insert the sampling ones into the encoded EPR particle sequences at the positions determined by the random number l only known to Bob and Charlie. And with a negligible probability that the TP can discriminate between the encoded EPR pairs and the sampling ones, he can obtain only the correlation information about the hash values of the secrets of Bob and Charlie and cannot deduce the players' respective private inputs.

Case 3. The TP colludes with a dishonest player, say Bob.

If the TP tries to collude with Bob to obtain Charlie's secret, they cannot achieve this goal. In terms of the one-way property of the hash function, $x \to f(x)$ is easy, but the reverse, i.e., $f(x) \to x$ is difficult computationally. Hence, even if the TP colludes with Bob, they obtain only the information about the hash value of Charlie's secret not Charlie's secret itself because of the one-way property of the hash function.

To summarize, by the detailed security analysis of the QPC protocol, we can see that our QPC protocol is secure against eavesdropping.

3. Discussion and summary

In this paper, following some ideas of the QSS protocol [29], we propose a QPC protocol based on two-photon entanglement. The protocol in [29] is in fact the improved version of the protocol in [19] with quantum dense coding and decoy photons, which increases its intrinsic efficiency, the source capacity and the security largely. Our present QPC scheme retains these advantages of high intrinsic efficiency and security. Almost all the instances $((1-p_d)(1-p_e)M/2n)$ (for M is even) or $((1-p_d)(1-p_e)(M+1)/2n)$ (for M is odd) are useful for encoding the secret bits except for those chosen for eavesdropping check and each of the two-photon entangled quantum system can carry two bits of information. Moreover, the classical information exchanged is reduced largely as the two players need not publish their MBs when they encode their secret's hash value with the four unitary operations. And the efficiency for qubits η_q is defined as $\eta_q \equiv \frac{q_u}{q_t}$. Then the efficiency for qubits $\eta_q = ((1-p_d)(1-p_c)(1-p_e)M/2n)$ (for M is even) or $((1-p_d)(1-p_c)(1-p_e)(M+1)/2n)$ (for M is odd) approaches 1 when p_d, p_c and p_e are very small and $n \to M/2$. The total efficiency η_t is defined as $\eta_t = \frac{b_s}{q_t+b_t}$, where b_s, q_t and b_t are the number of secret bits, the qubits transmitted and the total classical bits exchanged between the parties in the quantum communication, respectively. Then the total efficiency

$$\eta_t = \frac{(1-p_d)(1-p_c)(1-p_e)M/2n}{2+2p_d+2p_c+2p_e} \qquad \text{(for } M \text{ is even)}$$

or

$$\frac{(1-p_d)(1-p_c)(1-p_e)(M+1)/2n}{2+2p_d+2p_c+2p_e} \qquad \text{(for } M \text{ is odd)}$$

approaches 50% when p_d, p_c and p_e are very small and $nM/2$. From the formulae of the efficiency for qubits η_q and the total efficiency η_t, one can easily see that the efficiency of the present protocol directly depends on the values of p_d, p_c and p_e. Hence it is necessary to analyze how they scale. However, the values of p_d, p_c and p_e are subject to several factors including the type of the eavesdropper's attack and the quantum channel noise. For example, if the eavesdropper performs an intercept-resend attack in an ideal quantum channel, the probability of his attack being detected in the three security checks is 1/2, 1/8 and 1/2, respectively. In a practical quantum noisy channel, the quantum channel noise may affect the particles through the quantum channel and consequently induce the quantum bit error. Hence the players cannot tell affirmatively how many outcomes are changed by the quantum channel noise. Therefore, the quantum bit error rate (QBER) induced by the present intercept-resend eavesdropping practically ranges from $1/2 \times 1/2 = 1/4$ to 1/2, $1/2 \times 1/l8 \approx 6.25\%$ to 12.5% and $1/2 \times 1/2 = 1/4$ to 1/2, respectively. For other types of attacks and the different types of the noisy quantum channel, the QBER may be different. However, the value of the QBER directly determines the probability of the players' choosing the sampling photons from the photon sequence, i.e., the values of p_d, p_c and p_e. The detailed analysis of how the different

attacks and the type of the noisy channel have effect on the QBER is outside the scope of our paper. In addition, our QPC protocol has a disadvantage, that is, it cannot prevent the dishonest player from providing a false secret.

Our two-party QPC protocol can be simply generalized to the case with more parties. If the generalization is done, it solves the problem only on whether the secret values among more parties are equal, but not on the sort order of the secret values, i.e., our protocol cannot solve the problem on which the secret value is the largest, which secret value is the second largest, which secret value is the smallest and so on. This needs us to study further.

Acknowledgments

This work is supported by the National Basic Research Program of China (973 Program) (Grant No. 2007CB311100); the National Natural Science Foundation of China (Grant No. 60873191); the National High Technology Research and Development Program of China (Grant No. 2006AA01Z419); the Major Research plan of the National Natural Science Foundation of China (Grant No. 90604023); the Scientific Research Common Program of Beijing Municipal Commission of Education (Grant No. KM200810005004); the Natural Science Foundation of Beijing (Grant No. 1093015); the ISN open foundation.

References

[1] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[2] Long G L and Xiao L 2004 *Phys. Rev.* A **69** 052303
[3] Bennett C H, Brassard G, Crépeau C, Jozsa R, Peres A and Wootters W K 1993 *Phys. Rev. Lett.* **70** 1895
[4] Bouwmeester D, Pan J W, Mattle K, Eibl M, Weinfurter H and Zeilinger A 1997 *Nature* **390** 575
[5] Bennett C H and Wiesner S J 1992 *Phys. Rev. Lett.* **69** 2881
[6] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing (Bangalore, India, IEEE press, New York)* pp 175–9
[7] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[8] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[9] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
[10] Mayers D 2001 *J. Assoc. Comp. Mach.* **48** 351
[11] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[12] LÄutkenhaus N 1996 *Phys. Rev.* A **54** 97
[13] Gottesman D and Lo H K 2003 *IEEE Trans. Inform. Theory* **49** 457
[14] Scarani V, Pasquinucci H B, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2008 arXiv:0802.4155
[15] Deng F G, Long G L and Liu X S 2003 *Phys. Rev.* A **68** 042317
[16] Deng F G and Long G L 2004 *Phys. Rev.* A **69** 052319
[17] Wang C *et al.* 2005 *Phys. Rev.* A **71** 044305
[18] Hillery M, Bužek V and Berthiaume A 1999 *Phys. Rev.* A **59** 1829
[19] Karlsson A, Koashi M and Imoto N 1999 *Phys. Rev.* A **59** 162
[20] Deng F G, Zhou H Y and Long G L 2005 *Phys. Lett.* A **337** 329
[21] Goldwasser S 1997 *PODC '97* p 1
[22] Abadi M and Feigenbaum J 1990 *J. Cryptol.* **2** 1
[23] Yao A C 1986 *Proc. 27th Ann. Symp. on Foundations of Computer Science (IEEE Computer Society Press)* p 162
[24] Colbeck R 2007 *Phys. Rev.* A **76** 062308
[25] Crépeau C, Gottesman D and Smith A 2002 *STOC'02* pp 643–52
[26] Hogg T, Harsha P and Chen K Y 2007 arXiv:0704.0800v1
[27] Vaccaro J A, Spring J and Chefles A 2007 *Phys. Rev.* A **75** 012333
[28] Hillery M, Ziman M, Bužek V and Bieliková M 2006 *Phys. Lett.* A **349** 75
[29] Deng F G, Li X H and Zhou H Y 2008 *Phys. Lett.* A **372** 1957
[30] Qin S J, Gao F, Wen Q Y and Zhu F C 2006 *Phys. Lett.* A **357** 101

[31] Deng F G, Li X H, Zhou H Y and Zhang Z J 2005 *Phys. Rev.* A **72** 044302
[32] Gao F, Qin S J, Wen Q Y and Zhu F C 2007 *Quantum Inf. Comput.* **7** 329
[33] Deng F G, Li X H and Zhou H Y 2007 arXiv:0705.0279
[34] Lo H K, Chau H F and Ardehali M 2005 *J. Cryptol.* **18** 133
[35] Li X H, Deng F G and Zhou H Y 2007 *Appl. Phys. Lett.* **91** 144101
[36] Cai Q Y 2006 *Phys. Lett* A **351** 2325
[37] Li X H, Deng F G and Zhou H Y 2006 *Phys. Rev.* A **74** 054302
[38] Gisin N *et al* 2006 *Phys. Rev.* A **73** 022320
[39] Bennett C H, DiVincenzo D P, Smolin J A and Wootters W K 1996 *Phys. Rev.* A **54** 3824
[40] Briegel H J, Dur W, Cirac J I and Zoller P 1998 *Phys. Rev. Lett.* **81** 5932
[41] Dur W, Briegel H J, Cirac J I and Zoller P 1998 *Phys. Rev.* A **59** 169
[42] Lo H K and Chau H F 1999 *Science* **283** 2050
[43] van Enk S J, Cirac J I and Zoller P 1997 *Phys. Rev. Lett.* **78** 4293
[44] Yang C P and Guo G C 1999 *Phys. Rev.* A **59** 4217