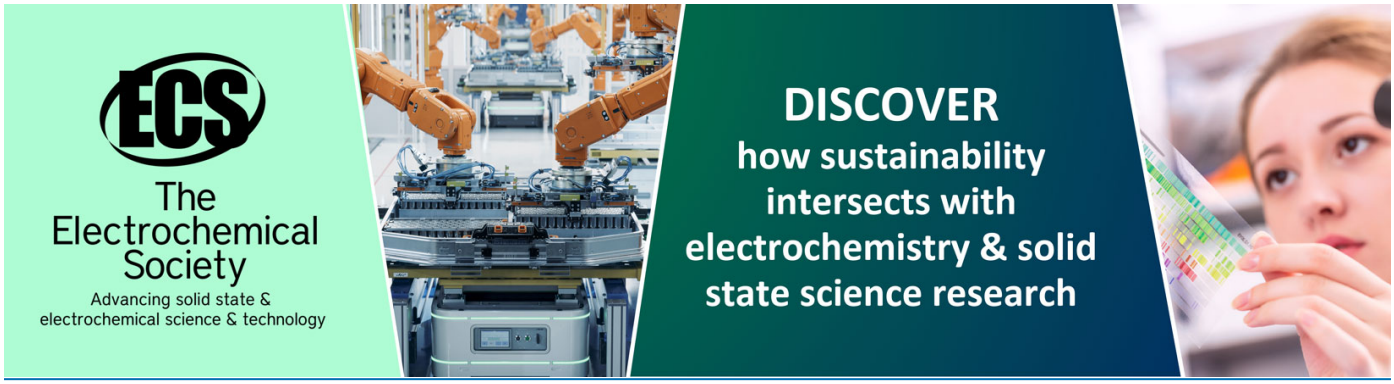
A two-party quantum private comparison of equality protocol with better performance in resisting outside attack



A two-party quantum private comparison of equality protocol with better performance in resisting outside attack

Xiao Feng[1,*], Zhe Zhang[2], Qing Wu[2], Changgui Huang[1], Jincheng Li[1], Ruyi Chen[1], Xiaoxiao Tang[3]

[1]State Grid Telecom Yili Technology Co., Ltd. ,Fuzhou, China
[2]State Grid Information and Communication Industry Group Co., Ltd. ,Beijing, China
[3]Beijing University of Posts and Telecommunications, Beijing, China

*Corresponding author e-mail: sxzyfx@163.com

Abstract. Private Comparison (PC) is an extension of Yao's millionaire problem: two millionaires want to know if their wealth is equal, but they don't want to reveal their specific wealth. In classical cryptography, this problem has been well studied. However, the security issues of these protocols are based on computational complexity assumptions, which means they cannot resist powerful quantum computing. In this paper, a quantum private comparison of equality with better performance in resisting outside attack is proposed based on two parties. Compared with the previous protocol, our protocol greatly reduce the total probability of obtaining the wrong result. And it also can compare successfully even if the two hash value string are short and close. Meanwhile, our protocol can be implemented easily without using entanglement, joint measurements and quantum memory and so on. Finally, we show that our protocol can be secure against the attacks from both the outside eavesdroppers and the inside participants.

1. Introduction

With the development of quantum mechanics, more and more people aim to understand the laws of motion in the microscopic world. Since 1984, Bennett and Brassard have proposed the first quantum cryptographic protocol(BB84)[1]. And then more and more quantum cryptography protocols have been proposed, such as quantum key distribution (QKD) [1–5], quantum secure multiparty computation(QSMC) [6–9], quantum secure direct communication (QSDC) [10–12], quantum signature(QS)[13–15] and so on.

As an important branch of secure multiparty computing(SMC), the private comparison of equality(PCE) because both millionaires want to know if they are equally rich without revealing their

respective wealth. This is an extension of Yao's millionaire question, in which the two millionaires want to know who is richer without revealing the exact amount of their wealth. QPCE is an important application in quantum mechanics. Its security depends on the laws of quantum mechanics and does not depend on the complexity of computation, such as Heisenberg uncertainty principle and quantum non-cloning theorem. However, As we all know that secure quantum two-party secure computation is impossible[17]. Therefore, additional assumptions are needed(e.g. a semi-honest third party).

With the assistant of a third party, Yang[18] proposed the first efficient protocol for QPC based on decoy photons and two-photon entanglement. Much research focus on QPCE and many related agreements have been proposed[19– 21]. Nearly all the former QPCE protocols need a third party, and Yang[22] also improved third-party assumptions. Recently, He[23] proposed a QPCE protocol without using a third party. Although it is not an ideal protocol and has a certain probability of getting wrong, the probability of getting wrong is very small. He found that his protocol can complete the task that leak very little bit information to the dishonest party.

However, if there is an eavesdropper in the quantum channel, the result of comparison will be changed. Because the quantum state will collapse after Eve's measurements. Eve can also intercept the quantum state from Alice and resend a quantum state. Inspired by previous work[23], we propose a QPCE protocol without a third party which can resist the outside attack. And we reduce the total probability of obtaining the wrong result by increasing the number of hash functions. Compared with the protocol in Ref.[23], we reduced the total probability of obtaining the wrong result to 0.07% when n = 5 which is the same order of magnitude compared to n = 32 in Ref.[23].

The rest of this paper is organized as follows: In section 2, we will introduce our QPCE protocol. Then we have the correctness and security analysis of the protocol in section 3 and section 4, respectively. The conclusion is presented in section.

2. Our Protocol

Let A be a n-bit string of Alice and Bob's n-bit string is B where A ≡ A1A2 . . . An and B ≡ B1B2 . . . Bn, respectively. Hi(x) is a series of classical hash functions, each of them is a one-to-one mapping between two n-bit strings(H :{0, 1}n → {0, 1}n). In our protocol, we denote two orthogonal quantum states . $|0\rangle_0 = |0\rangle, |1\rangle_0 = |1\rangle, |0\rangle_1 = |+\rangle, |1\rangle_1 = |-\rangle$

Different subscripts represent different groups of measurement. Different numbers stand for different states in the same basis.

The QPCE Protocol:

(1) Alice calculates the n-bit hash value string $a_1^1 a_1^2 ... a_1^n$ by using the hash function $H_1(x)$,

Then using the hash function $H_2(x)$, Alice can get string $a_2^1 a_2^2 ... a_2^{n1}$. Finally, Alice can get a n-bit string $a_n^1 a_n^2 ... a_n^n$. Then Alice stitches the n strings together in order and obtains a n2-bit string $H(A) \equiv h_1^A h_2^A ... h_{n^2}^A$. Bob does the same operation as Alice, he can get the string $H(B) \equiv h_1^B h_2^B ... h_{n^2}^B$.

(2) A and B compare H(A) and H(B) bit-by-bit from j = 1 to n^2 (each of them has n^2 bits):

Before comparing the two strings bit-by-bit, Alice divides the string into several parts randomly and inserts a 2-bit detection bit between each substring. And then she tells Bob the location of the detection bits, Bob inserts a 2-bit detection bit in the same location.

If *j* is odd, then:

1.Alice chooses a bit $\alpha \in 0, 1$ randomly, then she sends a quantum state $\left|\alpha_j\right\rangle_{h_j^A}$ to Bob.

2.After receiving this quantum state, Bob measure this state in the basis and gets the measurement result $\left|\beta_j\right\rangle_{h_j^B}$.

3. Bob announces β_j and maintains secrecy h_j^B .

4. Alice announces α_j .

When the comparison proceeds to the detection bit, Alice chooses a quantum state from {|0⟩, |1⟩, |+⟩, |−⟩} randomly. She sends it to Bob. After receiving the quantum state, Bob measures it using {|0⟩, |1⟩}, {|+⟩, |−⟩} randomly.

if j is even, then:

1. Bob chooses a bit $\beta \in 0, 1$ randomly, then he sends a quantum state $\left|\beta_j\right\rangle_{h_j^B}$ to Alice.

2. After receiving this quantum state, Alice measure this state in the basis and gets the measurement result $\left|\alpha_j\right\rangle_{h_j^A}$. h_j^A

3. Alice announces α_j and maintains secrecy h_j^A.

4. Bob announces β_j .

When the comparison proceeds to the detection bit, Bob chooses a quantum state from {|0 ⟩, |1 ⟩, |+ ⟩, |− ⟩} randomly. He sends it to Alice. After receiving the quantum state, Alice measures it using {|0 ⟩, |1 ⟩}, {|+ ⟩, |− ⟩} randomly.

(3) Compare α_j with β_j : If $\alpha_j \neq \beta_j$, Alice and Bob stop running the protocol immediately, then they obtain the conclusion that A = B. They do not need to compare the rest bits of H(A) and H(B). If there is eavesdropping exist (i.e.this protocol does not pass the eavesdropping test), The result of the comparison is not accurate. If $\alpha_j = \beta_j$ for all j = 1, . . . , n^2, then they obtain the conclusion that A = B.

3. Correctness

According to our protocol, we know that the quantum state $\left|a_j\right\rangle_{h_j^A}$ is send to Bob. If $h_j^B = h_j^A$, Bob will get the correct result with a probability of 1.But if $h_j^B \neq h_j^A$ that is Bob uses the different basis $\bar{h}_j^B$, the result $\beta_j = \alpha_j$ $\beta_j = \alpha_j$ will occur with a probability of 1/2. In another word, if A's secret data is equal to Bob's secret data, they will always obtain the correct comparison result $\alpha_j = \beta_j$ for all j = 1, . . . , n^2. Then they have the conclusion that A = B. However, if $A \neq B$, the hash string H(A) and H(B) must be different. The probability that H(A) and H(B) have k different bits is

$$p_k = \frac{C_{n^2}^k}{(2^{n^2}-1)} \tag{1}$$

So in each of k bit, the quantum state is measured using the different basis.Alice and Bob will obtain the correct result with a probability of 1/2. Then they stop running the rest of the protocol, output the result $A \neq B$. However, there is still a probability of 1/2 obtaining the wrong result. This is because all the k bits still obtain $\beta_j = \alpha_j$ even if Bob used a different basis. The total probability for obtaining a wrong result is

$$p = \sum_{k=1}^{n^2} p_k (1/2)^k = \sum_{k=1}^{n^2} \frac{c_{n^2}^k}{(2^{n^2}-1)2^k} \tag{2}$$

Compared with the previous protocol, our protocol is still not an ideal QPCE protocol. But our protocol can compare a smaller n-bit string than Ref.[23]. For example, the previous protocol comparing two 32-bit strings, the total probability for obtaining a wrong result is p $\simeq$ 0.01%. According to our protocol, Alice and Bob can compare two 5-bit strings(n = 5) with the total probability p $\simeq$ 0.07%. When n increase to 8, the total probability for obtaining a wrong result is p $\simeq$ 5 $\times$ 10− 7% only.Moreover, the previous protocol[23] needs to verify the result A = B because the protocol will be wrong with the probability p. In ref., Alice and Bob replace.

A and B with A $\oplus$S and B $\oplus$S. They run the entire protocol again from the beginning. It is useful when the hash value of Alice and Bob are close, because the hash value of A $\oplus$S and B $\oplus$S are still close with a probability of 1/2. So the probability p for obtaining a wrong comparison result will be further decreased.However, Alice and Bob do not need to consider this situation. In the beginning of our protocol, they calculated several hash values by using different hash functions $H_i(x)$. This method can play the same role as the method mentioned above. There is a disadvantage that Alice and

Bob need to compare too much bits through quantum channel. So they just need 3 different hash functions(n = 3) in practical applications.

4. Security analysis

Our work is dedicated to ensuring that our QPCE protocol is secure against external attacks and participant attacks.

5. Outside attack

Assuming Eve was an outside attacker, she wanted to eavesdrop on Alice and Bob's secrets without being noticed. Eve is capable to intercept the quantum state from a party and send to the other party which she wants to instead, and she is capable to entangle the quantum states with her additional particles. For example: suppose A = B, according to our protocol step(2).1, Alice sends a quantum state to Bob. But Eve intercept and measure it. It is known to us that Eve does not know what the quantum state is. So she has to guess the state and chooses a measurement basis from {|0⟩, |1⟩}, {|+⟩, |−⟩}, then she sends the measured state to Bob. This quantum state will change with a probability of 1/2, then Bob will obtain the wrong conclusion.

In order to detect eavesdropping by outsider attacker, we insert the detection eavesdropping position at the beginning of the step(2). When detecting eavesdropping, Alice randomly chooses one of the decoy states, then sends to Bob and tells him the basis of measurement {|0⟩, |1⟩} or {|+⟩, |−⟩}. Bob measures the state using the basis that Alice told him, then he announces the result. Alice compare the decoy state she chose with the result from Bob. Bob uses the same method to detect eavesdropping. If these two quantum state are different, it is as an error. Once the eavesdropping is found (the error rate is too high), the communication is terminated and the protocol is aborted. The outsider attacker tries to confuse comparison results. So a eavesdropping detection is necessary. Otherwise, Alice and Bob will never compare with each other successfully.

6. Participant attack

As we all know, some participants in quantum cryptography are not trusted. A untruthful participant is more capable of attacking the plan than an external eavesdropper. The participant attack means that Alice and Bob have at least one dishonesty. Suppose Alice is dishonest, when A = B, both Alice and Bob know each other's secrets from the comparison results. So we want to learn how much information Alice can obtain, when $A \neq B$. In our protocol, if it is aborted after comparing l bits in step(2), the rest bits will no longer be compared. That is, Alice will never obtain the information of these bits. If Alice wants to obtain more information of Bob, she must ensure that the protocol should run as much round as possible. Therefore, in each odd round of step(2), she must announce $\alpha_j = \beta_j$ even though $\alpha_j \neq \beta_j$. In each even round of step(2), Alice must try her best to guess β_j of the quantum state $\left|\beta_j\right\rangle_{h_j^B}$, before Bob announces his result. Therefore, Alice needs to distinguish

$$\frac{|0\rangle\langle 0|+|+\rangle\langle 0|}{2}, \frac{|1\rangle\langle 1|+|-\rangle\langle 1|}{2} \tag{3}$$

The maximal probability for distinguishing above two states is

$$p_{\max} = \cos^2(\pi/8) \sim 0.8536 \tag{4}$$

That is, Alice will control the protocol in each of these l rounds with probability of pmax. In summary, the probability for the protocol is aborted at l round is

$$p^l = p_{\max}^{l-1}(1-p_{\max}) = \cos^{2(l-1)}(\frac{\pi}{8})\sin^2(\frac{\pi}{8}) \tag{5}$$

We can see that this abort probability is equal to abort probability in [23]. The method we used to resist outside attack by calculating a series of different hash functions has no impact on participant attacks. In Ref.[23], the author analyzed the situation of the participant attacks in detail and gives the upper bounds of the information that each participant can reveal.

7. Conclusion

In this paper, we proposed a QPCE protocol which can resist the outside attack without a third party. Our protocol have the following merits. First, we do not need a third party. Second, the proposed protocol has a better performance in resisting outside attack. Third, compared with the protocol in Ref.[23], our protocol have greatly reduced the total probability of obtaining wrong result. Finally, further verifying the result A = B is not needed even if $H(A)^n$ and $H(B)^n$ are very close. In terms of experimental implementation, Alice and Bob send a single qubit in each round of step(2), then they can measure it at once without storing the quantum state. We didn't use entanglement state or joint measurement either. It can be practically applied in quantum information processing.

References

[1] Bennett, C.H. and G. Brassard, Quantum cryptography: public-key distribution and coin tossing, in IEEE International Conference on Computers, Systems and Signal Processing, IEEE, New York: Bangalore, India. p. 175-179(1984).
[2] Ekert A K. Quantum cryptography based on Bells theorem. Phys. Rev. Lett, 67:661C663 (1991).
[3] Wen K, Long G L. Modified Bennett-Brassard 1984 quantum key distribution protocol with two-way classical communications. Phys Rev A, 72: 022336 (2005).
[4] Gao F, Wen Q Y, Qin S J, et al. Quantum asymmetric cryptography with symmetrickeys. Sci China Ser G-Phys Mech Astron, 52: 1925C1931 (2009).
[5] Huang W, Guo F Z, Huang Z, et al. Three-particle QKD protocol against a collective noise. Opt Commun, 284: 536C540 (2011).
[6] Cleve R, Gottesman D, Lo H K. How to share a quantum secret. Phys. Rev. Lett, 83: 648C651 (1999).
[7] Yang Y G, Chai H P, Wang Y, et al. Fault tolerant quantum secret sharing against collective-amplitude-damping noise. Sci China-Phys Mech Astron, 54: 1619C1624 (2011).
[8] Jia H Y, Wen Q Y, Song T T, et al. Quantum protocol for millionaire problem. Opt Commun, 284: 545C549 (2011).
[9] Huang W, Wen Q Y, Liu B, et al. Robust and efficient quantum private comparison of equality with collective detection over collective-noise channels. Science China Physics, Mechanics and Astronomy, 56(9): 1670-1678 (2013).

[10] Long G L, Liu X. Theoretically high-capacity quantum-keydistribution scheme. Phys. Rev. A, 65: 032302 (2002). Title Suppressed Due to Excessive Length 7
[11] Bostrom K, Felbinger T. Deterministic secure direct communication using entanglement. Phys Rev Lett, 89: 187902 (2002).
[12] Long G L, Deng F G, Wang C, et al. Quantum secure direct communication and deterministic secure quantum communication. Front Phys. China, 2: 251C27(2007).
[13] Zhang L, Sun H W, Zhang K J, et al. The Security Problems in Some Novel Arbitrated Quantum Signature Protocols. International Journal of Theoretical Physics, pp. 1-12 (2017).
[14] Zhang L, Zhang H Y, Zhang K J, et al. The Security Analysis and Improvement of Some Novel Quantum Proxy Signature Schemes. International Journal of Theoretical Physics, pp. 1-12 (2017).
[15] Sun H W, Zhang L, Zuo H J, Zhang K J, Ma C G. Offline arbitrated quantum blind dual-signature protocol with better performance in resisting existential forgery attack. International Journal of Theoretical Physics, Vol. 57(9), pp. 2695-2708 (2018).
[16] Yao A. Protocols for secure computations. In: Proceedings of 23rd IEEE Symposium on Foundations of Computer Science (FOCS 82). Washington: (1982)
[17] Lo H K. Insecurity of quantum secure computations. Physical Review A, 56(2):1154 (1997).
[18] Yang Y G, Wen Q Y. An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. Journal of Physics A: Mathematical and Theoretical, 42(5): 055305 (2009).
[19] Liu B, Gao F, Jia H Y, et al. Ecient quantum private comparison employing single photons and collective detection. Quantum Inf Process, 12: 887C897 (2012).
[20] Chen X B, Xu G, Niu X X, et al. An client protocol for the private comparison of equal information based on the triplet entangled state and single-particle measurement. Opt Commun, 283: 1161C 1165 (2009).
[21] Yang, Y G, Xia J, Jia X, et al. Comment on quantum private comparison protocols with a semi-honest third party. Quantum Inf Process, 12: 877C885(2013).
[22] He G P. Quantum private comparison protocol without a third party. International Journal of Quantum Information, 15(02): 1750014 (2017).