SCIENTIFIC REPORTS
natureresearch

OPEN

Secure dynamic multiparty quantum private comparison

Hussein Abulkasim[1,2,3*], Ahmed Farouk[1,4*], Safwat Hamad[6], Atefeh Mashatan[1] & Shohini Ghose[4,5]

We propose a feasible and efficient dynamic multiparty quantum private comparison protocol that is fully secure against participant attacks. In the proposed scheme, two almost-dishonest third parties generate two random keys and send them to all participants. Every participant independently encrypts their private information with the encryption keys and sends it to the third parties. The third parties can analyze the equality of all or some participants' secrets without gaining access to the secret information. New participants can dynamically join the protocol without the need for any additional conditions in the protocol. We provide detailed correctness and security analysis of the proposed protocol. Our security analysis of the proposed protocol against both inside and outside attacks proves that attackers cannot extract any secret information.

The pioneering work of Bennett and Brassard[1] laid the groundwork for the rapidly growing field of quantum cryptography and quantum communication. Subsequently, various quantum protocols have been proposed including Shor's algorithm for factoring[2–4], quantum teleportation[5–9], superdense coding[10–13], quantum secure direct communication[14–16], quantum secret sharing[17–21], quantum dialogue[22,23] and quantum key agreement[24,25]. In 1982, the millionaires' problem was proposed as a possible application of secure multiparty computing[26], the goal is for two parties to compare their wealth and learn who is wealthier without revealing any extra data about the other's wealth. In 2001, an efficient and fair solution to the socialist millionaires' problem was proposed[27]. Furthermore, a solution for the socialist millionaires' problem based on homomorphic encryption in a semi-honest environment was discussed[28]. Lo[29] proved that the task of secure two-party computation is unachievable even with quantum cryptography[29]. Therefore, a quantum private comparison (QPC) protocol for comparing the equality of information with the help of a third party (TP) was proposed[30]. Furthermore, Hung *et al.*[31] proposed a secure QPC protocol with two almost-dishonest TPs. In general, there are four common levels of TP's trustworthiness[32,33]: (1) TP is fully honest. In this circumstance, the participants only send their encrypted secrets to the TP. The TP then compares the private information of the participants and announces the final result. This situation is surely ideal, but finding a fully honest TP in the real world could be challenging. (2) TP is dishonest such that all participants cannot trust the TP. This assumption is equivalent to the standard two-party QPC protocols without a TP, whose insecurity was proved by Lo[29]. (3) TP is semi-honest. Under this circumstance, the participants can partially trust the TP. The TP honestly executes the required processes and may eavesdrop on participants' private information using passive attacks[31]. (4) TP is almost-dishonest. This situation, which is more reasonable, assumes that the participants can partially trust the TP, and the TP may perform any active attack while executing the protocol, except conspiring with dishonest participants[31]. In general, QPC protocols can be used for novel and existing applications, including quantum voting[34,35], quantum bidding[36], and quantum auctions[37–39].

Chang *et al.* proposed the first multiparty quantum private comparison (MQPC) protocol for comparing the equality of secrets of any two parties among M participants[40]. The protocol used GHZ states as a quantum resource. Subsequently, a novel QPC protocol that included the support of a semi-honest TP and used d-dimensional entangled photons was proposed[41]. An MQPC protocol based on entanglement swapping of Bell states was subsequently presented[42]. This scheme used the one-way hash function to address information leakage issue and to encrypt secret information between the communicating parties. A pioneering M-participant QPC protocol that addressed the possibility of a dishonest TP collaborating with participants was discussed[43]. Furthermore, a novel MQPC protocol with a semi-honest TP that used entanglement swapping of d-level states

[1]Ted Rogers School of Information Technology Management, Ryerson University, Toronto, Canada. [2]Faculty of Science, The New Valley University, El-kharga, Egypt. [3]Faculty of Science, South Valley University, Qena, 83523, Egypt. [4]Department of Physics and Computer Science, Wilfrid Laurier University, Waterloo, Canada. [5]Perimeter Institute for Theoretical Physics, Waterloo, Canada. [6]Faculty of Computer and Information Sciences, Ain Shams University, Cairo, 11566, Egypt. *email: abulkasim@ryerson.ca; afarouk@wlu.ca

and a unitary operation to encrypt the participants' secrets was proposed[44]. Then, Hung *et al.*[31] presented a QPC protocol consisting of two third-parties in which one is malicious and the other is almost dishonest was presented. A multi-user QPC protocol that employs both scattered preparation operation and one-way convergent transmission operation of quantum states was also proposed[45], where two participants can compare their secrets with the support of the remaining participants using the polarization and spatial-mode degrees of freedom of photons to transmit information. Liu *et al.*[46] proposed a QPC protocol in which any participant can join dynamically to participate in the comparison of M participants.

These quantum private comparison protocols still suffer from low efficiency and an inadequate level of security. Therefore, this work proposes a feasible, efficient, and secure dynamic multiparty quantum private comparison protocol (DMQPC) that uses single-photons to encode and send encrypted information. Our proposed scheme has several important features. First, dishonest participants cannot individually or jointly attack the scheme to gain any private or secret information since every participant independently encrypts and transmits secret information to two TPs without the involvement or assistance of other participants. Second, our protocol is dynamic and flexible such that multiple participants can join or leave the protocol and the two TPs can successfully compare the encrypted information of any subset of M participants. Third, the participants only generate and transmit single photons, and the two TPs generate single photons and perform single-photon measurements. Hence, the cost of the deployed quantum devices and the employed quantum operations is reduced, and the efficiency of the proposed protocol is increased. Finally, the communication cost is significantly reduced since the proposed protocol can be executed in a variable number of rounds. We describe our scheme and provide proofs and illustrative examples in the following sections. Section 2 introduces the proposed DMQPC protocol. Section 3 verifies the correctness of the proposed scheme. The security analysis is presented in Section 4. Section 5 discussed the efficiency of the scheme and comparisons to some previous protocols. We show that our scheme is more feasible, efficient, secure and flexible compared to other protocols. Section 6 introduces comparisons to some existing QPC protocols. A summary and conclusion is presented in Section 7.

The Proposed DMQPC Protocol

Here, we will discuss the DMQPC protocol for three different scenarios, namely two-party QPC with two rounds, DMQPC with two rounds and DMQPC with B-block. Before the comparison of data, there are two main processes: (1) validation check process; (2) the initial preparation and encryption process. The two processes are similar in the three scenarios. So, they will be described in detail only for two-party QPC with two rounds.

Two-party QPC with two rounds. Suppose that Alice and Bob intend to compare the equality of their secrets X and Y, respectively, with the help of two almost-dishonest *TPs*. The binary representation of X in F_{2n} is $(x_0, x_1, ..., x_{n-1})$, and the binary representation of Y in F_{2n} is $(y_0, y_1, ..., y_{n-1})$ where $X_i, Y_i \in \{0, 1\}^n$ and $n \geq 2$ is the number of secret bits. In general, a protocol with two TPs has many advantages such as: (1) improving load balance performance since we can distribute the workload to two TPs (servers) instead of only one; (2) increasing availability that ensures continuity of communication; (3) ensuring security since one TP can monitor the performance of the other one[31]. The idea of adopting two TPs to execute the comparison task in QPC was first suggested by Hung *et al.*[31]. In our work, the advantage of using two TPs is that one can generate two independent random keys by two different TPs. More specifically, the first third-party (TP_1) computes the comparison result of the first round. The second third-party (TP_2) computes the comparison result of the second-round. Both TP_1 and TP_2 prepare a random secret key and send it to both Alice and Bob.

Validation check process. Firstly, X and Y must have the same length. Secondly, to correctly execute the proposed QPC protocol, secret data must be checked as follows; If the length of $X(Y)$ is odd, then Alice (Bob) must replace the last bit with two bits;

$$\begin{cases} 0 \rightarrow 00 \\ 1 \rightarrow 10 \end{cases} \tag{1}$$

Initial Preparation and Encryption Process. TP_1 and TP_2 prepare two random secret keys K_{rand}^{TP1} and K_{rand}^{TP2}, respectively, and send them through quantum channels to both Alice and Bob[16,47]. Alice and Bob compute $K_{rand} = \mathrm{K}_{rand}^{TP1} \oplus \mathrm{K}_{rand}^{TP2}$, where $|K_{rand}| = |\mathrm{K}_{rand}^{TP1}| = |\mathrm{K}_{rand}^{TP2}| = |X| = |Y|$. Then Alice and Bob split K_{rand} into two equal parts K_{rand}^1 and K_{rand}^2, where $K_{rand} \in \{0, 1\}^n$ and $K_{rand}^1, K_{rand}^2 \in \{0, 1\}^{\frac{n}{2}}$. To reduce the communication cost, Alice also divides X into two equal parts X_{part_1} and X_{part_2}. Alice then computes

$$X_1 = K_{rand}^1 \oplus X_{part\_1}, \tag{2}$$

$$X_2 = K_{rand}^2 \oplus X_{part\_2}. \tag{3}$$

The encrypted parts X_1 and X_2 can be represented as follows.

$$X_1 = \left\{ x_{1,0},\ x_{1,1},\ \ldots,\ x_{1,\left(\frac{n}{2}-1\right)} \right\}, \tag{4}$$

X_1		X_2		$X_{12}=X_1 \oplus X_2$		$X_1^{'}$		$X_{12}^{'}$	
$x_{1,0}$	0	$x_{2,\frac{n}{2}}$	0	$x_{\frac{n}{2}}$	0	$x_{1,0}^{'}$	1	$x_{\frac{n}{2}}^{'}$	1
$x_{1,1}$	0	$x_{2,\left(\frac{n}{2}+1\right)}$	1	$x_{\left(\frac{n}{2}+1\right)}$	1	$x_{1,1}^{'}$	0	$x_{\left(\frac{n}{2}+1\right)}^{'}$	1
$x_{1,2}$	1	$x_{2,\left(\frac{n}{2}+2\right)}$	0	$x_{\left(\frac{n}{2}+2\right)}$	1	$x_{1,2}^{'}$	0	$x_{\left(\frac{n}{2}+2\right)}^{'}$	0
…	…	…	…	…	…	…	…	…	…
$x_{1,\left(\frac{n}{2}-1\right)}$	1	$x_{2,(n-1)}$	1	$x_{(n-1)}$	0	$x_{1,\left(\frac{n}{2}-1\right)}^{'}$	1	$x_{(n-1)}^{'}$	0

Table 1. Illustration of the proposed technique for preparing $X_1^{'}$ and $X_{12}^{'}$.

$$X_2 = \left\{x_{2,\frac{n}{2}},\ x_{2,\left(\frac{n}{2}+1\right)},\ \ldots,\ x_{2,(n-1)}\right\}, \tag{5}$$

where X_1 and X_2 are the first and second parts of X encrypted with K_{rand}^1 and K_{rand}^2, respectively. Similarly, Bob computes Y_1 and Y_2 just as Alice does.

$$Y_1 = \left\{y_{1,0},\ y_{1,1},\ \ldots,\ y_{1,\left(\frac{n}{2}-1\right)}\right\}, \tag{6}$$

$$Y_2 = \left\{y_{2,\frac{n}{2}},\ y_{2,\left(\frac{n}{2}+1\right)},\ \ldots,\ y_{2,(n-1)}\right\}, \tag{7}$$

where Y_1 and Y_2 are the first and second parts of Y encrypted with K_{rand}^1 and K_{rand}^2, respectively. Also, we have $X_{12}=X_1 \oplus X_2$ and $Y_{12}=Y_1 \oplus Y_2$. Here, $\oplus$ is the exclusive-OR operation.

As shown in Table 1, Alice generates new encoded parts $X_1^{'}$ and $X_{12}^{'}$ from X_1, X_2, and X_{12} according to the following rule: If the bit value of $X_1=X_{12}=0(X_1=X_{12}=1)$ then $X_1^{'} = X_{12}^{'} = 1$ $(X_1^{'} = X_{12}^{'} = 0)$. Otherwise, $X_1^{'} = X_1$ and $X_{12}^{'} = X_{12}$, where $X_1^{'}$ and $X_{12}^{'}$ are updated parts of X_1 and X_{12}. The purpose of this process is to relate the secret message parts to each other so that we can reduce the communication cost. That is to say, it is possible to only compare one part of the secret messages in some situations to get the final result.

From Table 1, we can get the sequences $X_1^{'}$, X_{12}, and $X_{12}^{'}$, with length $\frac{n}{2}$:

$$X_1^{'} = \left\{x_{1,0}^{'},\ x_{1,1}^{'},\ \ldots,\ x_{1,\left(\frac{n}{2}-1\right)}^{'}\right\} \tag{8}$$

$$X_{12} = \left\{x_{\frac{n}{2}},\ x_{\left(\frac{n}{2}+1\right)},\ \ldots,\ x_{(n-1)}\right\}, \tag{9}$$

$$X_{12}^{'} = \left\{x_{\frac{n}{2}}^{'},\ x_{\left(\frac{n}{2}+1\right)}^{'},\ \ldots,\ x_{(n-1)}^{'}\right\}. \tag{10}$$

Alice uses the XOR function to encrypt X_1 with $X_1^{'}$ getting C_{a1},

$$C_{a1} = X_1 \oplus X_1^{'} = \{(x_{1,0} \oplus x_{1,0}^{'}),\ (x_{1,1} \oplus x_{1,1}^{'}),\ \ldots,\ \left\{x_{1,\left(\frac{n}{2}-1\right)} \oplus x_{1,\left(\frac{n}{2}-1\right)}^{'}\right\}\}, \tag{11}$$

Similarly, Bob performs the same processes as Alice does,

$$C_{b1} = Y_1 \oplus Y_1^{'}, \tag{12}$$

Alice computes $X_{12}=X_1 \oplus X_2$:

$$X_{12} = \left\{\left(x_{1,0} \oplus x_{2,\frac{n}{2}}\right),\ \left(x_{1,1} \oplus x_{2,\left(\frac{n}{2}+1\right)}\right),\ \ldots,\ \left(x_{1,\left(\frac{n}{2}-1\right)} \oplus x_{2,(n-1)}\right)\right\}. \tag{13}$$

Bob also computes $Y_{12}=Y_1 \oplus Y_2$:

$$Y_{12} = \left\{\left(y_{1,0} \oplus y_{2,\frac{n}{2}}\right),\ \left(y_{1,1} \oplus y_{2,\left(\frac{n}{2}+1\right)}\right),\ \ldots,\ \left(y_{1,\left(\frac{n}{2}-1\right)} \oplus y_{2,(n-1)}\right)\right\}. \tag{14}$$

In our protocol, we have three options to compute and announce the comparison result. The first option would be for TP_1 to compute and announce (in the first and second rounds) the comparison result. The second option would be for TP_2 to compute and announce the comparison result. These two options can be used when

<table>
<tr><th colspan="2">The private information</th><th>$X = \{001100110010\}$</th><th>$Y = \{011100110010\}$</th></tr>
<tr><td colspan="2" rowspan="2">Random keys</td><td colspan="2">$\mathrm{K}_{rand}^{TP1} = \{010110010110\}, \mathrm{K}_{rand}^{TP2} = \{111111010010\}$</td></tr>
<tr><td colspan="2">$K_{rand} = \mathrm{K}_{rand}^{TP1} \oplus \mathrm{K}_{rand}^{TP2} = \{101001000100\}, K_{rand}^{1} = \{101001\}, K_{rand}^{2} = \{000100\}$</td></tr>
<tr><td rowspan="2">Validity check</td><td>Length check for equality</td><td colspan="2">$X\_length = Y\_length = 12$</td></tr>
<tr><td>Length check for 2 blocks</td><td colspan="2">$\frac{12}{2} = 6$</td></tr>
<tr><td colspan="2">Initial preparation</td><td>$X_{part\_1} = \{001100\}, X_{part\_2} = \{110010\}, K_{rand}^{1} = \{101001\}, K_{rand}^{2} = \{000100\}$.</td><td>$Y_{part\_1} = \{011100\}, Y_{part\_2} = \{110010\}, K_{rand}^{1} = \{101001\}, K_{rand}^{2} = \{000100\}$.</td></tr>
<tr><td colspan="2">Encryption</td><td>$X_1 = K_{rand}^{1} \oplus X_{part\_1}, X_2 = K_{rand}^{2} \oplus X_{part\_2}$,
$X_1 = \{100101\}, X_2 = \{110110\}$</td><td>$Y_1 = K_{rand}^{1} \oplus Y_{part\_1}, Y_2 = K_{rand}^{2} \oplus Y_{part\_2}$,
$Y_1 = \{110101\}, Y_2 = \{110110\}$.</td></tr>
<tr><td colspan="2" rowspan="2">Encoding
If $X_1 = X_{12} = 0$ $(X_1 = X_{12} = 1)$ then $X_1^{'} = X_{12}^{'} = 1$ $(X_1^{'} = X_{12}^{'} = 0)$. Else, $X_1^{'} = X_1$ &amp; $X_{12}^{'} = X_{12}$
The same process for Y</td><td><table><tr><th>X_1</th><th>X_2</th><th>X_{12}</th><th>X_1'</th><th>X_{12}'</th></tr><tr><td>1</td><td>1</td><td>0</td><td>1</td><td>0</td></tr><tr><td>0</td><td>1</td><td>1</td><td>0</td><td>1</td></tr><tr><td>0</td><td>0</td><td>0</td><td>1</td><td>1</td></tr><tr><td>1</td><td>1</td><td>0</td><td>1</td><td>0</td></tr><tr><td>0</td><td>1</td><td>1</td><td>0</td><td>1</td></tr><tr><td>1</td><td>0</td><td>1</td><td>0</td><td>0</td></tr></table></td><td><table><tr><th>Y_1</th><th>Y_2</th><th>Y_{12}</th><th>Y_1'</th><th>Y_{12}'</th></tr><tr><td>1</td><td>1</td><td>0</td><td>1</td><td>0</td></tr><tr><td>1</td><td>1</td><td>0</td><td>1</td><td>0</td></tr><tr><td>0</td><td>0</td><td>0</td><td>1</td><td>1</td></tr><tr><td>1</td><td>1</td><td>0</td><td>1</td><td>0</td></tr><tr><td>0</td><td>1</td><td>1</td><td>0</td><td>1</td></tr><tr><td>1</td><td>0</td><td>1</td><td>0</td><td>0</td></tr></table></td></tr>
<tr><td>$X_1 = 100101, X_1^{'} = 101100, X_{12} = 010011$.</td><td>$Y_1 = 110101, Y_1^{'} = 111100, Y_{12} = 000011$.</td></tr>
<tr><td colspan="2">Compute $C_{a1} = X_1 \oplus X_1^{'}, X_{12} = X_1 \oplus X_2$, &amp; $C_{b1} = Y_1 \oplus Y_1^{'}, Y_{12} = Y_1 \oplus Y_2$.</td><td>$C_{a1} = \{001001\}, X_{12} = \{010011\}$.</td><td>$C_{b1} = \{001001\}, Y_{12} = \{000011\}$.</td></tr>
</table>

Table 2. Illustration of preparation of encrypted secrets for two participants.

availability of at least one *TP* is the most important requirement. The third option would be for the two *TPs* to collaborate to compute and announce the final result. The steps for executing the two rounds to compare the equality of parties' secrets are similar in the three options. The choice of which of the three options to use depends on whether the priority is availability, workload or security. The two rounds are described as follows.

The first-round. ***Step 1***. TP_1 asks Alice and Bob to prepare $\mathrm{C}_{a1} = \mathrm{X}_1 \oplus \mathrm{X}_1^{'}$ and $\mathrm{C}_{b1} = \mathrm{Y}_1 \oplus \mathrm{Y}_1^{'}$, respectively.

Step 2. Alice prepares a sequence of $\frac{n}{2}$ single photons, called S_{a1}, corresponding to C_{a1} in the Z-basis $\{|0\rangle, |1\rangle\}$ or the X-basis $\left\{| + \rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), | - \rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right\}$.

Step 3. For the eavesdropping check, Alice randomly prepares a sequence of decoy photons l_{a1} in one of the states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. At random positions, she inserts l_{a1} into S_{a1} producing a new sequence $S_{a1}^{'}$. Then, Alice transmits $S_{a1}^{'}$ to the TP_1.

Step 4. Alice announces the random positions and the measurement bases of l_{a1} to TP_1 for performing single photon measurements. TP_1 then reveals the measurement outcomes. Hence, TP_1 and Alice analyze the error rate. If the rate is higher than a predetermined threshold, then they terminate the protocol and restart the process again. Otherwise, TP_1 discards l_{a1} from $S_{a1}^{'}$ and extracts S_{a1}. Then TP_1 can restore C_{a1}, where S_{a1} represents C_{a1}.

Step 5. Bob and TP_1 perform the same *Steps 2–4* as Alice and TP_1 to send C_{b1} to TP_1.

Step 6. TP_1 performs a comparison between the first part of Alice's and Bob's secrets by computing $R_1 = C_{a1} \oplus C_{b1}$. If $R_1 = 0$, this indicates that X and Y may be equal. In this case, they move to the next round to check whether Alice's and Bob's secrets are equal or not. Otherwise, X and Y are not equal, so there is no need to continue to the second-round to check the equality of the second parts.

The second-round. ***Step 7***. TP_1 informs TP_2 that the first-round comparison result may be equal. Then TP_2 asks Alice and Bob to prepare X_{12} and Y_{12}, respectively.

Step 8. Alice and Bob perform the same processes described in *Steps 2–4* to send X_{12} and Y_{12} to TP_2.

Step 9. TP_2 computes $R_2 = X_{12} \oplus Y_{12}$. If $R = R_1 + R_2 = 0$ then X and Y are equal. Otherwise, X and Y are not equal. A detailed example to check the equality of $X = \{001100110010\}$ and $Y = \{011100110010\}$ is shown in Tables 2 and 3.

Adding new participants. One of the main features of this protocol is the ease of joining of one or more participants. Without loss of generality, suppose a new participant called Charlie want to joint the old participants (Alice and Bob). The steps for adding a new participant are described as follows.

The first-round. ***Step 1***. Charlie asks TP_1 and TP_2 to join the protocol.

Step 2. TP_1 asks Charlie to prepare $\mathrm{C}_{c1} = \mathrm{Z}_1 \oplus \mathrm{Z}_1^{'}$ using the same protocol as Alice and Bob to prepare C_{a1} and C_{b1}, respectively.

Step 3. Charlie prepares a sequence of $\frac{n}{2}$ single photons, called S_{c1}, corresponding to C_{c1} in the Z-basis $\{|0\rangle, |1\rangle\}$ or the X-basis $\left\{|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right\}$.

Round 1	***Alice***	***TP_1***	***Bob***
Step 1: Preparation $\langle Alice \rangle$	Prepares $C_{a1} = \{001001\}$ in Z-basis or X-basis		
Steps 2&4: Eavesdropping check $\langle Alice, TP_1 \rangle$	*error rate* $<$ *specified Threshold*, TP_1 obtains C_{a1}. Else, the communication process is terminated.		
Step 5: Preparation $\langle Bob \rangle$			Prepares $C_{b1} = \{001001\}$, in Z-basis or X-basis
Step 5: Eavesdropping check $\langle Bob, TP_1 \rangle$		*error rate* $<$ *specified Threshold*, TP_1 obtains C_{b1}. Else, the communication process is terminated.	
Step 6: Check the equality		If $R_1 = C_{a1} \oplus C_{b1} \neq 0$; $X_1 \neq Y_1$, $X \neq Y$. The protocol will terminate and no need for a second-round. Otherwise, they continue to *Round 2*.	
Round 2	***Alice***	*TP_2*	***Bob***
Step 7: Preparation $\langle Alice \rangle$	Prepares $X_{12} = \{010011\}$ in Z-basis or X-basis		
Step 8: Eavesdropping check $\langle Alice, TP_2 \rangle$	*error rate* $<$ *specified Threshold*, TP_2 obtains X_{12}. Otherwise, the communication process is terminated.		
Step 7: Preparation $\langle Bob \rangle$			Prepares $Y_{12} = \{000011\}$ in Z-basis or X-basis
Step 8: Eavesdropping check $\langle Bob, TP_2 \rangle$		*error rate* $<$ *specified Threshold*, TP_2 obtains Y_{12}. Otherwise, the communication process is terminated.	
Step 9: Check the equality		If $R_2 = X_{12} \oplus Y_{12} = 0$; $X = Y$. Otherwise, $X \neq Y$.	

Table 3. Illustration of the equality check of X and Y.

Step 4. For eavesdropping check, Charlie randomly prepares a sequence of decoy photons l_{c1} in one of the states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. At random positions, he inserts l_{c1} into S_{c1} producing a new sequence $S_{c1}^{'}$. Then, Charlie transmits $S_{c1}^{'}$ to the TP_1.

Step 5. Upon receiving $S_{c1}^{'}$, Charlie announces the random positions and the measurement bases of l_{c1} to TP_1 for performing single photon measurements. TP_1 then reveals the measurement outcomes. Hence, TP_1 and Charlie analyze the error rate. If the rate is higher than a predetermined threshold, then they terminate the protocol and restart the process again. Otherwise, TP_1 discards l_{c1} from $S_{c1}^{'}$ and extracts S_{c1}. Then TP_1 can restore C_{c1}.

Step 6. TP_1 performs a comparison between the first part of Alice's, Bob's, and Charlie's secrets by computing $R_1 = (C_{a1} \oplus C_{b1}) + (C_{b1} \oplus C_{c1})$. If $R_1 = 0$, this indicates that X, Y, and Z may be equal. In this case, they move to the next round to check whether Alice's, Bob's, and Charlie's secrets are equal or not. Otherwise, X, Y, and Z are not equal, so there is no need to continue to the second-round to check the equality of the second parts.

The second-round. ***Step 7***. TP_1 informs TP_2 that the first-round comparison result may be equal. Then TP_2 asks Charlie to prepare Z_{12} using the same protocol as Alice and Bob to prepare X_{12} and Y_{12}, respectively.

Step 8. Charlie performs the same processes described in *Steps 3–4* to send Z_{12} to TP_2.

Step 9. TP_2 computes $R_2 = (X_{12} \oplus Y_{12}) + (Y_{12} \oplus Z_{12})$. If $R = R_1 + R_2 = 0$, TP_2 announces to Alice, Bob, and Charlie that X, Y, and Z are equal. Otherwise, X, Y, and Z are not equal.

Deleting old participants. Without loss of generality, suppose we have three participants Alice, Bob, and Charlie. TP_1 and TP_2 are allowed to delete one or more participants (e.g., Charlie) for several reasons. For example, they may want to compare just Bob's and Alice's private information. The detailed steps for deleting Charlie are as follows.

The first-round. ***Step 1***. TP_1 and TP_2 agree to delete Charlie. TP_1 then discards C_{c1}.

Step 2. TP_1 updates the comparison process, to be only between Alice and Bob, TP_1 then recomputes R_1. In that case, TP_1 computes and considers the result of $R_1 = C_{a1} \oplus C_{b1}$ instead of $R_1 = (C_{a1} \oplus C_{b1}) + (C_{b1} \oplus C_{c1})$. If the result of $R_1 = 0$, this indicates that X and Y may be equal. In this case, they move to the next round to check whether Alice's and Bob's secrets are equal or not. Otherwise, X and Y are not equal and the final result is announced.

The second-round. ***Step 3***. TP_1 informs TP_2 that the first-round comparison result of Alice's and Bob's secrets may be equal.***Step 4***. TP_2 discards the encrypted information of Charlie (Z_{12}) and only considers the private information of Alice and Bob, that is, X_{12} and Y_{12}, respectively.

Step 5. TP_2 computes and considers $R_2 = X_{12} \oplus Y_{12}$ instead of $R_2 = (X_{12} \oplus Y_{12}) + (Y_{12} \oplus Z_{12})$. If $R = R_1 + R_2 = 0$ then X and Y are equal. Otherwise, X and Y are not equal.

Multi-party QPC with two rounds. The proposed two-party QPC protocol is easy to extend to M participants (see Fig. 1). In this scenario, there are M participants P_i ($i = 1, 2, \ldots, M$), and each of them has secret information X_i^* with length n. Firstly, participants check the validity of their secrets according to the validation check

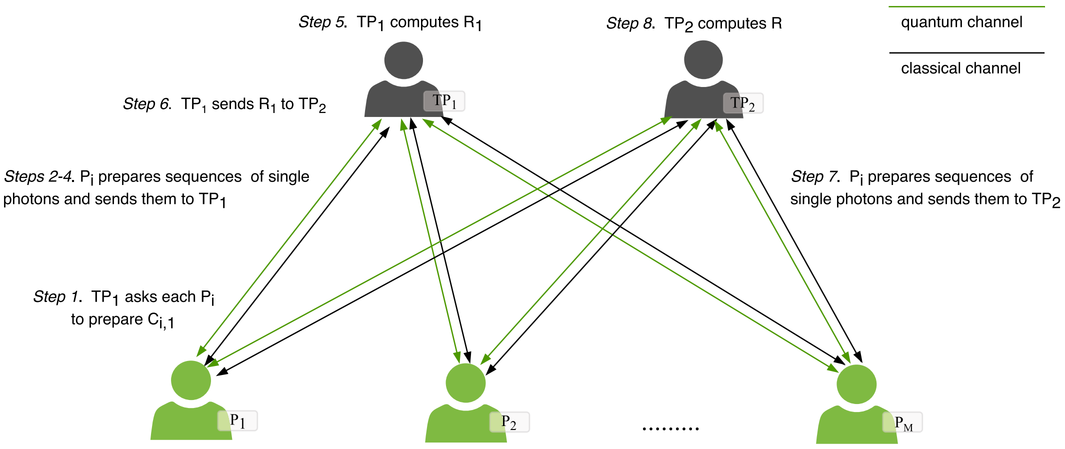
Step 5. TP$_1$ computes R$_1$
Step 8. TP$_2$ computes R
quantum channel
classical channel
Step 6. TP$_1$ sends R$_1$ to TP$_2$
TP$_1$
TP$_2$
Steps 2-4. P$_i$ prepares sequences of single photons and sends them to TP$_1$
Step 7. P$_i$ prepares sequences of single photons and sends them to TP$_2$
Step 1. TP$_1$ asks each P$_i$ to prepare C$_{i,1}$
P$_1$
P$_2$
....
P$_M$

Figure 1. The proposed DMQPC protocol for M participants.

process. After they make sure that their secrets are valid for applying the proposed protocol, TP_1 and TP_2 send two random secret keys (K_{rand}^{TP1} and K_{rand}^{TP2}) with length n to all participants. P_i then perform the initial preparation and encryption process as shown in Eqs. (2–5) for producing $X_{i,1}^*$ and $X_{i,2}^*$. From Table 1, each participant gets the sequences $X_{i,1}^*$ and $X_{i,2}^*$, with length $\frac{n}{2}$ for each sequence. Also, each participant computes $C_{i,1}=X_{i,1}^*\oplus X_{i,1}$. Now each participant has completed preparing encrypted secrets, and they are ready for checking the equality of their secrets using the QPC protocol.

The first-round. ***Step 1***. TP_1 asks each participant to prepare $C_{i,1}$.

Step 2. P_i prepares a quantum sequence containing $\frac{n}{2}$ single photons corresponding to $C_{i,1}$ (i.e. $S_{i,1}$) in the Z-basis $\{|0\rangle, |1\rangle\}$ or X-basis $\left\{|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right\}$.

Step 3. For the eavesdropping check, P_i randomly prepares a sequence of decoy photons $l_{i,1}$ in one of the states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. At random positions, P_i inserts $l_{i,1}$ into $S_{i,1}$ producing a new sequence $S_{i,1}^{'}$. Then, P_i sends $S_{i,1}^{'}$ to the TP_1.

Step 4. Upon receiving $S_{i,1}^{'}$, P_i announces the random positions and the measurement bases of $l_{i,1}$ to TP_1 for performing single photon measurements. TP_1 then announces the measurement outcomes. TP_1 and P_i analyze the error rate. If the rate is higher than a predetermined threshold, they terminate the communication and restart the process again. Otherwise, TP_1 discards $l_{i,1}$ from $S_{i,1}^{'}$ and extracts $S_{i,1}$. Then the TP_1 can restore $C_{i,1}$, where $S_{i,1}$ represents $C_{i,1}$.

Step 5. TP_1 performs a comparison of the first part of P_i's secret, where for $M=3$

$$R_1 = (C_{1,1} \oplus C_{2,1}) + (C_{2,1} \oplus C_{3,1}), \tag{15}$$

For $M > 3$

$$R_1 = (C_{1,1} \oplus C_{2,1}) + (C_{2,1} \oplus C_{3,1}) + \cdots + (C_{M-1,1} \oplus C_{M,1}). \tag{16}$$

If $R_1=0$, $X_1^*,\ X_2^*,\ \ldots,\ X_M^*$ may be equal. Hence, they move to the next round to compute the comparison check of $X_{i,12}$. Otherwise, $X_1^*, X_2^*,\ \ldots,\ X_M^*$ are not equal. Then it is not necessary to execute the second-round to check the equality of $X_{i,12}$.

The second-round. ***Step 6***. TP_1 informs TP_2 that the first-round comparison result may be equal. Then TP_2 asks P_i to prepare $X_{i,12}$.

Step 7. P_i performs the same processes as in Steps 2–4 to send $X_{i,12}$ to TP_2.

Step 8. TP_2 computes the comparison check of $X_{i,12}$,
where for $M=3$

$$R_2 = (X_{1,12} \oplus X_{2,12}) + (X_{2,12} \oplus X_{3,12}), \tag{17}$$

for $M > 3$

$$R_2 = (X_{1,12} \oplus X_{2,12}) + (X_{2,12} \oplus X_{3,12}) + \cdots + (X_{M-1,12} \oplus X_{M,12}), \tag{18}$$

Now, TP_2 can compute $R=R_1+R_2$ to determine whether $X_1^*, X_2^*,\ \ldots,\ X_M^*$ are equal or not. If $X_1^*, X_2^*,\ \ldots,\ X_M^*$ are equal. Otherwise, $X_1^*, X_2^*,\ \ldots,\ X_M^*$ are not equal. Obviously, it is easy to add or remove any subset of participants to the protocol, where participants independently perform the required processes to prepare their secret for the final step of the protocol. Moreover, TP_1 and TP_2 can easily compare the equality of the secrets of any subset of M participants without any additional conditions.

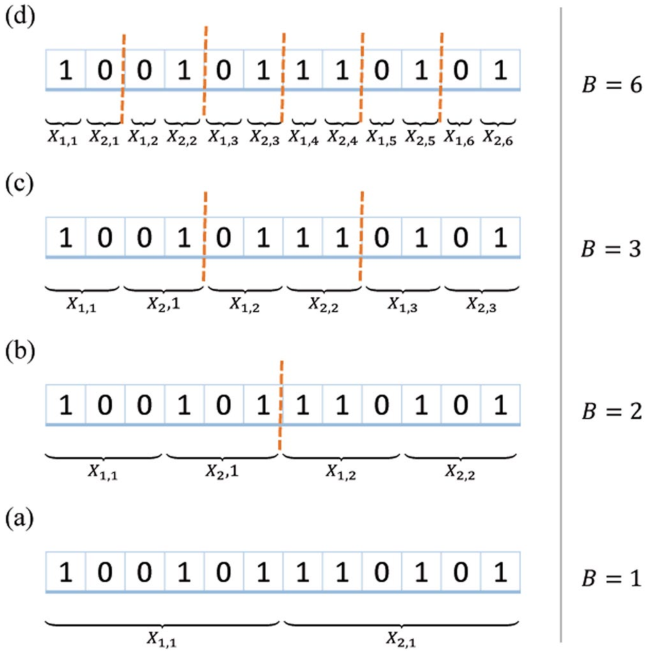
(d)
1 0 0 1 0 1 1 1 0 1 0 1
$X_{1,1}$ $X_{2,1}$ $X_{1,2}$ $X_{2,2}$ $X_{1,3}$ $X_{2,3}$ $X_{1,4}$ $X_{2,4}$ $X_{1,5}$ $X_{2,5}$ $X_{1,6}$ $X_{2,6}$
$B = 6$
(c)
1 0 0 1 0 1 1 1 0 1 0 1
$X_{1,1}$ $X_2,1$ $X_{1,2}$ $X_{2,2}$ $X_{1,3}$ $X_{2,3}$
$B = 3$
(b)
1 0 0 1 0 1 1 1 0 1 0 1
$X_{1,1}$ $X_2,1$ $X_{1,2}$ $X_{2,2}$
$B = 2$
(a)
1 0 0 1 0 1 1 1 0 1 0 1
$X_{1,1}$ $X_{2,1}$
$B = 1$

Figure 2. A secret of length 12 can be divided into: (**a**) 1 block divided into two parts and executed in two rounds; (**b**) 2 blocks; (**c**) 3 blocks; (**d**) 6 blocks with two rounds for each block.

Multi-Party QPC with B blocks. The secret data can be divided into several blocks (B), which could be useful in comparing the equality of big data. Each block contains $\frac{n}{B}$ bits and is executed in two rounds, where $\frac{n}{B}$ is an even number such that,

$$2 \le \frac{n}{B} \le n \left\{ \begin{array}{c} B\ is\ even \\ B\ is\ odd,\ \ and\ \ \dfrac{n}{B}\ is\ even \end{array} \right. . \tag{19}$$

Suppose there are M participants P_i ($i = 1, 2, ..., M$). Each of them has secret information X_i with a length of n, and they would like to check the equality of their secrets. Firstly, all participants check the validity of their secrets according to the previously described validation check. After they make sure that their secrets are valid for applying the proposed protocol, TP_1 and TP_2 send two random secret keys (K_{rand}^{TP1} and K_{rand}^{TP2}) with length n to all participants. Based on the length of the secret data (n), TP_1 and TP_2 agree with participants on the value of B (see Fig. 2). P_i computes $K_{rand} = K_{rand}^{TP1} \oplus K_{rand}^{TP2}$ and divides K_{rand} into B blocks. Each block contains two sub-keys $K_{rand}^{1,j}$ and $K_{rand}^{2,j}$, where $j = 1,2, \ldots, B$.

Subsequently, P_i performs the initial preparations as previously indicated in Eq. (2) and Eq. (3) for generating $X_{i,j}^1$ and $X_{i,j}^2$, where $i = 1, 2, \ldots, M$. At this point, using Table 1, participants can easily prepare their encrypted secret information producing $C_{i,j}$ and $X_{12}^{i,j}$, and are ready to check the equality of their secrets using the following steps.

The first-round. ***Step 1***. TP_1 asks each participant to prepare $C_{i,j}$.

Step 2. P_i prepares a sequence of $\frac{n}{2B}$ single photons for each block, called $S_{i,j}$, corresponding to $C_{i,j}$, in the Z-basis {|0,⟩ |1⟩} or X-basis $\left\{|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right\}$.

Step 3. To prevent eavesdropping, P_i randomly prepares a sequence of decoy photons $l_{i,j}$ in one of the states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. At random positions, P_i inserts $l_{i,j}$ into $S_{i,j}$ producing a new sequence $S_{i,1}^{'}$. P_i then sends $S_{i,1}^{'}(S_{i,2}^{'}, \ldots, S_{i,B}^{'})$ to TP_1.

Step 4. Upon receiving $S_{i,j}^{'}$, P_i announces the random positions and the measurement bases of $l_{i,j}$ to TP_1 for performing single photon measurements. TP_1 then announces the measurement outcomes. TP_1 and P_i analyze the error rate. For any error rate above a predetermined threshold, they cancel the communication and restart all over again. Otherwise, TP_1 discards $l_{i,j}$ from $S_{i,j}^{'}$ and extracts $S_{i,j}$. TP_1 then can construct $C_{i,j}$, where $S_{i,j}$ represents $C_{i,j}$.

Step 5. TP_1 computes the comparison check of $C_{i,j}$, where for $M = 3$

$$\begin{aligned} R_1^1 &= (C_{1,1} \oplus C_{2,1}) + (C_{2,1} \oplus C_{3,1})(R_1^2 = (C_{1,2} \oplus C_{2,2}) + (C_{2,2} \oplus C_{3,2}), \ \ldots, \ R_1^B \\ &= (C_{1,B} \oplus C_{2,B}) + (C_{2,B} \oplus C_{3,B})). \end{aligned} \tag{20}$$

For $M > 3$

					To be sent to TP_1	To be sent to TP_2
X_1	X_2	X_{12}	$X_1^{'}$	$X_{12}^{'}$	$C_{a1} = X_1 \oplus X_1^{'}$	X_{12}
0	0	0	1	1	1	0
0	1	1	0	1	0	1
1	0	1	0	0	1	1
1	1	0	1	0	0	0

Table 4. All possible encrypted data from two bits according to the initial preparation and encryption method, where $X_1 = K_{rand}^1 \oplus X_{part\_1}, X_2 = K_{rand}^2 \oplus X_{part\_2}$.

$$\begin{aligned} R_1^1 \; = \; & (C_{1,1} \oplus C_{2,1}) + (C_{2,1} \oplus C_{3,1}) + \ldots + (C_{M-1,1} \oplus C_{M,1})(R_1^2 = (C_{1,2} \oplus C_{2,2}) \\ & + (C_{2,2} \oplus C_{3,2}) + \ldots + (C_{M-1,2} \oplus C_{M,2}), \;\; \ldots, \;\; R_1^B = (C_{1,B} \oplus C_{2,B}) \\ & + (C_{2,B} \oplus C_{3,B}) + \ldots + (C_{M-1,B} \oplus C_{M,B})). \end{aligned} \tag{21}$$

If $R_1^1 = 0$ $(R_1^2 = 0, \ldots, R_1^B = 0)$, $X_1, X_2, \ldots, X_M$ may be equal, where $R_1^B$is the comparison result of the first round of block number B for all participants. Hence, they move to the next round to compute the comparison check of $X_{12}^{i,1}$ $X_{12}^{i,2}, \;\ldots, \;X_{12}^{i,B}$. Otherwise, their secrets are not equal.

The second-round. ***Step 6***. TP_1 informs TP_2 that the first-round comparison result of the $1st-block$ $(2\,nd-block, \ldots,$ $Bth-block)$ may be equal. Then TP_2 asks P_i to prepare $X_{12}^{i,1}$ $(X_{12}^{i,2}, \;\ldots, \;X_{12}^{i,B})$.

Step 7. P_i performs the same processes as in *Steps 2–4* to send $X_{12}^{i,1}(X_{12}^{i,2}, \;\ldots, \;X_{12}^{i,B})$ to TP_2.

Step 8. TP_2 computes the comparison check of $X_{12}^{i,1}(X_{12}^{i,2}, \;\ldots, \;X_{12}^{i,B})$, where for $M = 3$

$$\begin{aligned} R_2^1 \; = \; & (X_{12}^{1,1} \oplus X_{12}^{2,1}) + (X_{12}^{2,1} \oplus \; X_{12}^{3,1})(R_2^2 = (X_{12}^{1,2} \oplus X_{12}^{2,2}) \\ & + (X_{12}^{2,2} \oplus X_{12}^{3,2}), \;\; \ldots, \;\; R_2^B = (X_{12}^{1,B} \oplus X_{12}^{2,B}) + (X_{12}^{2,B} \oplus X_{12}^{3,B})), \end{aligned} \tag{22}$$

for $M > 3$

$$\begin{aligned} R_2^1 \; = \; & (X_{12}^{1,1} \oplus X_{12}^{2,1}) + (X_{12}^{2,1} \oplus X_{12}^{3,1}) + \ldots + (X_{12}^{M-1,1} \oplus X_{12}^{M,1})(R_2^2 = (X_{12}^{1,2} \oplus X_{12}^{2,2}) \\ & + (X_{12}^{2,2} \oplus X_{12}^{3,2}) + \ldots + (X_{12}^{M-1,2} \oplus X_{12}^{M,2}), \;\; \ldots, \;\; R_2^B = (X_{12}^{1,B} \oplus X_{12}^{2,B}) \\ & + (X_{12}^{2,B} \oplus X_{12}^{3,B}) + \ldots + (X_{12}^{M-1,B} \oplus X_{12}^{M,B})). \end{aligned} \tag{23}$$

If $R = R_1^1 + R_2^1 = R_1^2 + R_2^2 = \ldots = R_1^B + R_2^B = 0$, this means that $X_1, X_2, \ldots, X_M$ are equal. Otherwise, $X_1, X_2, \ldots,$ X_M are not equal. Note, participants check the result of the first block (R_2^1) and if $R_2^1 = 0$ they continue to check the next block and so on until they reach the last block; otherwise, TP_2 announces that the secrets are not equal.

Correctness

From Table 4, according to our initial preparation and encryption method, for every two bits we get two different encrypted bits, that is to say, we get $C_{a1} = 1$ and $X_{12} = 0$ only when $X_1 = 0$ and $X_2 = 0$. So, the bit values of C_{a1} and X_{12} together are decisive in determining the bit values of X_1 and X_2. Assume we have two participants Alice and Bob, and each participant has two bits $X = 00$ and $Y = 10$, respectively, and $K_{rand} = 00$. Alice computes $C_{a1} = X_1 \oplus X_1^{'} = K_{rand}^1 \oplus X_{part_1} \oplus X_1^{'}$ getting 1, and sends it to TP_1. Bob also computes $C_{b1} = Y_1 \oplus Y_1^{'} = K_{rand}^1 \;\oplus Y_{part\_1} \oplus Y_1^{'}$ getting 1, and sends it to TP_1. When TP_1 computes $R_1 = C_{a1} \oplus C_{b1}$ he gets $R_1 = 0$, which means that the secrets of Alice and Bob may be equal or unequal (note if $R_1 = 1$, TP_1 announces that the secrets of Alice and Bob are not equal). So, they should move to the second-round to compare X_{12} and Y_{12}.

In the second-round, Alice and Bob send $X_{12} = X_1 \oplus X_2 = K_{rand}^1 \;\oplus X_{part\_1} \;\oplus K_{rand}^2 \;\oplus X_{part\_2}$ and $Y_{12} = Y_1 \oplus Y_2 = K_{rand}^1 \;\oplus Y_{part\_1} \;\oplus K_{rand}^2 \;\oplus Y_{part\_2}$ to TP_2, respectively. TP_2 computes $R_2 = X_{12} \oplus Y_{12} = 0 \oplus 1$ getting $R_2 = 1$. TP_1 then computes $R = R_1 + R_2$ getting $R = 1$, which means that X and Y are not equal. Thus, X and Y are equal if and only if $R = R_1 = R_2 = 0$. For example, suppose we have $X = 0000$ and $K_{rand} = 0000$. Then $X_1 = 00$ and $X_2 = 00$. As shown in Table 5, we must get $C_{a1} = X_1 \oplus X_1^{'} = 11$ and $X_{12} = 00$ only when $X_1 = 00$ and $X_2 = 00$. Also, if we have $Y = 0000$ and $K_{rand} = 0000$, then $Y_1 = 00$ and $Y_2 = 00$. Hence, we get $C_{b1} = Y_1 \oplus Y_1^{'} = 11$ and $Y_{12} = 00$. Now the two TPs can announce that the two inputs are equal by computing $R = (C_{a1} \oplus C_{b1}) +$ $(X_{12} \oplus Y_{12}) = 0$, which proves the correctness of this protocol. Note that if we proposed that $C_{a1} = X_2 \oplus X_2^{'}$ and $C_{b1} = Y_2 \oplus Y_2^{'}$ instead of $C_{a1} = X_1 \oplus X_1^{'}$ and $C_{b1} = Y_1 \oplus Y_1^{'}$ respectively, we also get the same correct comparison result.

Here, we provide the necessary equations to verify the equality check by TP_1 and TP_2 for the various suggested protocols.

Two-party QPC with two rounds.

From Eqs. (11) and (12), TP_1 computes

					To be sent to TP_1	To be sent to TP_2
$\boldsymbol{X_1}$	$\boldsymbol{X_2}$	$\boldsymbol{X_{12}}$	$X_1^{'}$	$X_{12}^{'}$	$\boldsymbol{C_{a1} = X_1 \oplus X_1^{'}}$	$\boldsymbol{X_{12}}$
0	0	0	1	1	1	0
0	0	0	1	1	1	0
0	0	0	1	1	1	0
1	1	0	1	0	0	0
1	1	0	1	0	0	0
0	0	0	1	1	1	0
1	1	0	1	0	0	0
1	1	0	1	0	0	0
0	0	0	1	1	1	0
1	0	1	0	0	1	1
0	0	0	1	1	1	0
0	1	1	0	1	0	1
1	1	0	1	0	0	0
1	0	1	0	0	1	1
1	1	0	1	0	0	0
0	1	1	0	1	0	1
1	0	1	0	0	1	1
0	0	0	1	1	1	0
1	0	1	0	0	1	1
1	1	0	1	0	0	0
0	1	1	0	0	0	1
0	0	0	1	1	1	0
0	1	1	0	1	0	1
1	1	0	1	0	0	0
1	0	1	0	0	1	1
1	0	1	0	0	1	1
1	0	1	0	0	1	1
0	1	1	0	1	0	1
0	1	1	0	1	0	1
0	0	1	1	1	1	1
0	1	1	0	1	0	1
0	1	1	0	1	0	1

Table 5. All possible encrypted data when X contains four bits, and both X_1 and X_2 include two bits, where $X_1 = K_{rand}^{1} \oplus X_{part\_1}$, $X_2 = K_{rand}^{2} \oplus X_{part\_2}$.

$$\begin{aligned} R_1 &= C_{a1} \oplus C_{b1}, \\ &= X_1 \oplus X_1^{'} \oplus Y_1 \oplus Y_1^{'}, \\ &= K_{rand}^{1} \oplus X_{part\_1} \oplus X_1^{'} \oplus K_{rand}^{1} \oplus Y_{part\_1} \oplus Y_1^{'} \\ &= X_{part\_1} \oplus X_1^{'} \oplus Y_{part\_1} \oplus Y_1^{'}. \end{aligned}$$

From Eqs. (13) and (14), TP_2 computes

$$\begin{aligned} R_2 &= X_{12} \oplus Y_{12}, \\ &= X_1 \oplus X_2 \oplus Y_1 \oplus Y_2, \\ &= K_{rand}^{1} \oplus X_{part\_1} \oplus K_{rand}^{2} \oplus X_{part\_2} \oplus K_{rand}^{1} \oplus Y_{part\_1} \oplus K_{rand}^{2} \oplus Y_{part\_2}. \\ &= X_{part\_1} \oplus X_{part\_2} \oplus Y_{part\_1} \oplus Y_{part\_2}. \end{aligned}$$

In the proposed protocol, computing only R_2 is not sufficient for getting the comparison result. For example, if we have $X_1 = X_2 = 0$, $Y_1 = Y_2 = 1$, and $K_{rand}^{1} = K_{rand}^{2} = 0$. Then $R_2 = 0 \oplus 0 \oplus 1 \oplus 1 = 0$. This means that X and Y are equal in contrast to the correct comparison result ($R = R_1 + R_2 = 1 + 0 = 1$). In such a case, R_1 guarantees the correctness of the final result.

MDQPC with two rounds. From Eq. (15), for $M = 3$, TP_1 computes

$$\begin{aligned} R_1 &= (C_{1,1} \oplus C_{2,1}) + (C_{2,1} \oplus C_{3,1}). \\ R_1 &= (X_{1,1} \oplus X'_{1,1} \oplus X_{2,1} \oplus X'_{2,1}) + (X_{2,1} \oplus X'_{2,1} \oplus X_{3,1} \oplus X'_{3,1}). \\ R_1 &= (K^1_{rand} \oplus X_{1,\ part\_1} \oplus X'_{1,1} \oplus K^1_{rand} \oplus X_{2,\ part\_1} \oplus X'_{2,1}) \\ &\quad + (K^1_{rand} \oplus X_{2,\ part\_1} \oplus X'_{2,1} \oplus K^1_{rand} \oplus X_{3,\ part\_1} \oplus X'_{3,1}). \end{aligned}$$

From Eq. (16), for $M > 3$, TP_1 computes

$$\begin{aligned} R_1 &= (C_{1,1} \oplus C_{2,1}) + (C_{2,1} \oplus C_{3,1}) + \cdots + (C_{M-1,1} \oplus C_{M,1}), \\ R_1 &= (X_{1,1} \oplus X'_{1,1} \oplus X_{2,1} \oplus X'_{2,1}) + (X_{2,1} \oplus X'_{2,1} \oplus X_{3,1} \oplus X'_{3,1}) + \cdots \\ &\quad + (X_{M-1,1} \oplus X'_{M-1,1} \oplus X_{M,1} \oplus X'_{M,1}), \\ R_1 &= (K^1_{rand} \oplus X_{1,part\_1} \oplus X'_{1,1} \oplus K^1_{rand} \oplus X_{2,part\_1} \oplus X'_{2,1}) \\ &\quad + (K^1_{rand} \oplus X_{2,part\_1} \oplus X'_{2,1} \oplus K^1_{rand} \oplus X_{3,part\_1} \oplus X'_{3,1}) \\ &\quad + \cdots + (K^1_{rand} \oplus X_{M-1,part\_1} \oplus X'_{M-1,1} \oplus K^1_{rand} \oplus X_{M,part\_1} \oplus X'_{M,1}). \end{aligned}$$

In addition, from Eq. (17), for $M = 3$, TP_2 computes

$$\begin{aligned} R_2 &= (X_{1,12} \oplus X_{2,12}) + (X_{2,12} \oplus X_{3,12}), \\ R_2 &= (X_{1,1} \oplus X_{1,2} \oplus X_{2,1} \oplus X_{2,2}) + (X_{2,1} \oplus X_{2,2} \oplus X_{3,1} \oplus X_{3,2}), \\ R_2 &= (K^1_{rand} \oplus X_{1,part_1} \oplus K^2_{rand} \oplus X_{1,part_2} \oplus K^1_{rand} \oplus X_{2,part_1} \oplus K^2_{rand} \oplus X_{2,\ part_2}) \\ &\quad + (K^1_{rand} \oplus X_{2,part_1} \oplus K^2_{rand} \oplus X_{2,part_2} \oplus K^1_{rand} \oplus X_{3,part_1} \oplus K^2_{rand} \oplus X_{3,part_2}), \end{aligned}$$

where K^1_{rand} and K^2_{rand} represent the random encryption keys for the first and second parts of the private information. $X_{i,part\_1}$ and $X_{i,part\_2}$ represent the first part and second part of the private information of P_i.

From Eq. (18), for $M > 3$, TP_2 computes

$$\begin{aligned} R_2 &= (X_{1,12} \oplus X_{2,12}) + (X_{2,12} \oplus X_{3,12}) + \cdots + (X_{M-1,12} \oplus X_{M,12}). \\ R_2 &= (X_{1,1} \oplus X_{1,2} \oplus X_{2,1} \oplus X_{2,2}) + (X_{2,1} \oplus X_{2,2} \oplus X_{3,1} \oplus X_{3,2}) \\ &\quad + \cdots + (X_{M-1,1} \oplus X_{M-1,2} \oplus X_{M,1} \oplus X_{M,2}), \\ R_2 &= (K^1_{rand} \oplus X_{1,part\_1} \oplus K^2_{rand} \oplus X_{1,part\_2} \oplus K^1_{rand} \oplus X_{2,part\_1} \oplus K^2_{rand} \oplus X_{2,part\_2}) \\ &\quad + (K^1_{rand} \oplus X_{2,part\_1} \oplus K^2_{rand} \oplus X_{2,part\_2} \oplus K^1_{rand} \oplus X_{3,part\_1} \oplus K^2_{rand} \oplus X_{3,part\_2}) \\ &\quad + \cdots + (K^1_{rand} \oplus X_{M-1,part\_1} \oplus K^2_{rand} \oplus X_{M-1,part\_2} \oplus K^1_{rand} \oplus X_{M,part\_1} \oplus K^2_{rand} \oplus X_{M,part\_2}). \end{aligned}$$

Thus, if $R_1 = 0$ and $R_2 = 0$, $R = R_1 + R_2 = 0$, hence $X_1, X_2, ..., X_M$ are equal. Otherwise, $X_1, X_2, ..., X_M$ are not equal.

MDQPC with B-block.

From Eq. (20), for $M = 3$, TP_1 computes

$$\begin{aligned} R^1_1 &= (C_{1,1} \oplus C_{2,1}) + (C_{2,1} \oplus C_{3,1})(R^2_1 = (C_{1,2} \oplus C_{2,2}) \\ &\quad + (C_{2,2} \oplus C_{3,2}),\ \ldots,\ R^B_1 = (C_{1,B} \oplus C_{2,B}) + (C_{2,B} \oplus C_{3,B})), \end{aligned}$$

So,

$$\begin{aligned} R^1_1 &= (X_{1,1} \oplus X'_{1,1} \oplus X_{2,1} \oplus X'_{2,1}) + (X_{2,1} \oplus X'_{2,1} \oplus X_{3,1} \oplus X'_{3,1}) \\ &\quad \times (R^2_1 = (X_{1,2} \oplus X'_{1,2} \oplus X_{2,2} \oplus X'_{2,2}) + (X_{2,2} \oplus X'_{2,2} \oplus X_{3,2} \oplus X'_{3,2}),\ \ldots, \\ &\quad R^B_1 = (X_{1,B} \oplus X'_{1,B} \oplus X_{2,B} \oplus X'_{2,B}) + (X_{2,B} \oplus X'_{2,B} \oplus X_{3,B} \oplus X'_{3,B})), \\ R^1_1 &= (K^1_{rand} \oplus X_{1,part\_1} \oplus X'_{1,1} \oplus K^1_{rand} \oplus X_{2,part\_1} \oplus X'_{2,1}) \\ &\quad + (K^1_{rand} \oplus X_{2,part\_1} \oplus X'_{2,1} \oplus K^1_{rand} \oplus X_{3,part\_1} \oplus X'_{3,1}) \\ &\quad \times (R^2_1 = (K^{1,,2}_{rand} \oplus X_{1,part\_2} \oplus X'_{1,2} \oplus K^{1,2}_{rand} \oplus X_{2,part\_2} \oplus X'_{2,2}) \\ &\quad + (K^{1,2}_{rand} \oplus X_{2,part\_2} \oplus X'_{2,2} \oplus K^{1,2}_{rand} \oplus X_{3,part\_2} \oplus X'_{3,2}),\ \ldots, \\ &\quad R^B_1 = (K^{1,B}_{rand} \oplus X_{1,part\_B} \oplus X'_{1,B} \oplus K^{1,B}_{rand} \oplus X_{2,part\_B} \oplus X'_{2,B}) \\ &\quad + (K^{1,B}_{rand} \oplus X_{2,part\_B} \oplus X'_{2,B} \oplus K^{1,B}_{rand} \oplus X_{3,part\_B} \oplus X'_{3,B})). \end{aligned}$$

For $M > 3$,

$$\begin{aligned} R_1^1 \;=\; & (C_{1,1} \oplus C_{2,1}) + (C_{2,1} \oplus C_{3,1}) + \ldots + (C_{M-1,1} \oplus C_{M,1})(R_1^2 = (C_{1,2} \oplus C_{2,2}) \\ & + (C_{2,2} \oplus C_{3,2}) + \ldots + (C_{M-1,2} \oplus C_{M,2}),\ \ldots,\ R_M^B = (C_{1,B} \oplus C_{2,B}) \\ & + (C_{2,B} \oplus C_{3,B}) + \ldots + (C_{M-1,B-1} \oplus C_{M,B})), \end{aligned}$$

So,

$$\begin{aligned} R_1^1 \;=\; & (X_{1,1} \oplus X_{1,1}^{'} \oplus X_{2,1} \oplus X_{2,1}^{'}) + (X_{2,1} \oplus X_{2,1}^{'} \oplus X_{3,1} \oplus X_{3,1}^{'}) \\ & + \ldots + (X_{M-1,1} \oplus X_{M-1,1}^{'} \oplus X_{M,1} \oplus X_{M,1}^{'}) \\ & \times(R_1^2 =\ (X_{1,2} \oplus X_{1,2}^{'} \oplus X_{2,2} \oplus X_{2,2}^{'}) + (X_{2,2} \oplus X_{2,2}^{'} \oplus X_{3,2} \oplus X_{3,2}^{'}) + \ldots \\ & + (X_{M-1,2} \oplus X_{M-1,2}^{'} \oplus X_{M,2} \oplus X_{M,2}^{'}),\ \ldots,\ R_M^B = (X_{1,B} \oplus X_{1,B}^{'} \oplus X_{2,B} \oplus X_{2,B}^{'}) \\ & + (X_{2,B} \oplus X_{2,B}^{'} \oplus X_{3,B} \oplus X_{3,B}^{'}) + \ldots + (X_{M-1,B} \oplus X_{M-1,B}^{'} \oplus X_{M,B} \oplus X_{M,B}^{'})), \\ R_1^1 \;=\; & (K_{rand}^{1,1} \oplus X_{1,part\_1} \oplus X_{1,1}^{'} \oplus K_{rand}^{1,1} \oplus X_{2,part\_1} \oplus X_{2,1}^{'}) \\ & + (K_{rand}^{1,1} \oplus X_{2,part\_1} \oplus X_{2,1}^{'} \oplus K_{rand}^{1,1} \oplus X_{3,part\_1} \oplus X_{3,1}^{'}) + \ldots \\ & + (K_{rand}^{1,1} \ \oplus X_{M-1,part\_1} \oplus X_{M-1,1}^{'} \oplus K_{rand}^{1,1} \oplus X_{M,part\_1} \oplus X_{M,1}^{'}) \\ & \times(R_1^2 = (K_{rand}^{1,2} \oplus X_{1,part\_2} \oplus X_{1,2}^{'} \oplus K_{rand}^{1,2} \oplus X_{2,part\_2} \oplus X_{2,2}^{'}) \\ & + (K_{rand}^{1,2} \oplus X_{2,part\_1} \oplus X_{2,2}^{'} \oplus K_{rand}^{1,2} \oplus X_{3,part\_2} \oplus X_{3,2}^{'}) + \ldots \\ & + (K_{rand}^{1,2} \ \oplus X_{M-1,part\_2} \oplus X_{M-1,2}^{'} \oplus K_{rand}^{1,2} \ \oplus X_{M,part\_2} \oplus X_{M,2}^{'}),\ \ldots, \\ & R_M^B = (K_{rand}^{1,B} \oplus X_{1,part\_\mathrm{B}} \oplus X_{1,B}^{'} \oplus K_{rand}^{1,B} \oplus X_{2,part\_\mathrm{B}} \oplus X_{2,B}^{'}) \\ & + (K_{rand}^{1,B} \oplus X_{2,part\_\mathrm{B}} \oplus X_{2,B}^{'} \oplus K_{rand}^{1,B} \oplus X_{3,part\_\mathrm{B}} \oplus X_{3,B}^{'}) + \ldots \\ & + (K_{rand}^{1,B} \oplus X_{M\_1,part\_\mathrm{B}} \oplus X_{M-1,B}^{'} \oplus K_{rand}^{1,B} \oplus X_{M,part\_\mathrm{B}} \oplus X_{M,B}^{'})), \end{aligned}$$

In addition, from Eq. (22), for $M = 3$, TP_2 computes

$$\begin{aligned} R_2^1 \;=\; & (X_{12}^{1,1} \oplus X_{12}^{2,1}) + (X_{12}^{2,1} \oplus X_{12}^{3,1})(R_2^2 = (X_{12}^{1,2} \oplus X_{12}^{2,2}) \\ & + (X_{12}^{2,2} \oplus X_{12}^{3,2}),\ \ldots,\ R_2^B = (X_{12}^{1,B} \oplus X_{12}^{2,B}) + (X_{12}^{2,B} \oplus X_{12}^{3,B})), \\ R_2^1 \;=\; & (X_1^{1,1} \oplus X_2^{1,1} \oplus X_1^{2,1} \oplus X_2^{2,1}) +\ (X_1^{2,1} \oplus X_2^{2,1} \oplus\ X_1^{3,1} \oplus\ X_2^{3,1}) \\ & \times(R_2^2 = (X_1^{1,2} \oplus X_2^{1,2} \oplus X_1^{2,2} \oplus X_2^{2,2}) + (X_1^{2,2} \oplus X_2^{2,2} \oplus X_1^{3,2} \oplus X_2^{3,2}),\ \ldots, \\ R_2^B \;=\; & (X_1^{1,B} \oplus X_2^{1,B} \oplus X_1^{2,B} \oplus X_2^{2,B}) + (X_1^{2,B} \oplus X_2^{2,B} \oplus X_1^{3,B} \oplus X_2^{3,B})), \end{aligned}$$

$$\begin{aligned} R_2^1 \;=\; & (K_{rand}^{1,1} \oplus X_{part\_1}^{1,1} \oplus K_{rand}^{2,1} \oplus X_{part\_2}^{1,1} \oplus K_{rand}^{1,1} \oplus X_{part\_1}^{2,1} \oplus K_{rand}^{2,1} \oplus X_{part\_2}^{2,1}) \\ & + (K_{rand}^{1,1} \oplus X_{part\_1}^{2,1} \oplus K_{rand}^{2,1} \oplus X_{part\_2}^{2,1} \oplus\ K_{rand}^{1,1} \oplus X_{part\_1}^{3,1} \oplus K_{rand}^{2,1} \oplus X_{part\_2}^{3,1}) \\ & \times(R_2^2 = (K_{rand}^{1,2} \oplus X_{part\_1}^{1,2} \oplus K_{rand}^{2,2} \oplus X_{part\_2}^{2,2} \oplus K_{rand}^{1,2} \oplus X_{part\_1}^{2,2} \oplus K_{rand}^{2,2} \oplus X_{part\_2}^{2,2}) \\ & + (K_{rand}^{1,2} \oplus X_{part\_1}^{2,2} \oplus K_{rand}^{2,2} \oplus X_{part\_2}^{2,2} \oplus K_{rand}^{1,3} \oplus X_{part\_1}^{3,2} \oplus K_{rand}^{2,3} \oplus X_{part\_2}^{3,2}),\ \ldots, \\ & R_2^B = (K_{rand}^{1,\mathrm{B}} \oplus X_{part\_1}^{1,B} \oplus K_{rand}^{2,\mathrm{B}} \oplus X_{part\_2}^{1,B} \oplus K_{rand}^{1,\mathrm{B}} \oplus X_{part\_1}^{2,B} \oplus K_{rand}^{2,\mathrm{B}} \oplus X_{part\_2}^{2,B}) \\ & + (K_{rand}^{1,\mathrm{B}} \oplus X_{part\_1}^{2,B} \oplus K_{rand}^{2,\mathrm{B}} \oplus X_{part\_2}^{2,B} \oplus K_{rand}^{1,\mathrm{B}} \oplus X_{part\_1}^{3,B} \oplus K_{rand}^{2,\mathrm{B}} \oplus X_{part\_2}^{3,B})), \end{aligned}$$

where $\mathrm{K}_{rand}^{1,j}$ and $\mathrm{K}_{rand}^{2,j}$ are random subkeys for encrypting the first and second part of the *jth* block, $j = 1, 2, \ldots, B$.

From Eq. (23) for $M > 3$, TP_2 computes

$$\begin{aligned} R_2^1 \;=\; & (X_{12}^{1,1} \oplus X_{12}^{2,1}) + (X_{12}^{2,1} \oplus X_{12}^{3,1}) + \ldots + (X_{12}^{M-1,1} \oplus X_{12}^{M,1})(\ldots, \\ & R_2^B = (X_{12}^{1,B} \oplus X_{12}^{2,B}) + (X_{12}^{2,B} \oplus X_{12}^{3,B}) + \ldots + (X_{12}^{M-1,B} \oplus X_{12}^{M,B})), \end{aligned}$$

So, we can get

$$\begin{aligned} R_2^1 \;=\; & (X_1^{1,1} \oplus X_2^{1,1} \oplus X_1^{2,1} \oplus X_2^{2,1}) + (X_1^{2,1} \oplus X_2^{2,1} \oplus X_1^{3,1} \oplus X_2^{3,1}) + \ldots \\ & + (X_1^{M-1,1} \oplus X_2^{M-1,1} \oplus X_1^{M,1} \oplus X_2^{M,1})(\ldots,\ R_2^B = (X_1^{1,B} \oplus X_2^{1,B} \oplus X_1^{2,B} \oplus X_2^{2,B}) \\ & + (X_1^{2,B} \oplus X_2^{2,B} \oplus X_1^{3,B} \oplus X_2^{3,B}) + \ldots + (X_1^{M-1,B} \oplus X_2^{M-1,B} \oplus X_1^{M,B} \oplus X_2^{M,B})), \end{aligned}$$

$$\begin{aligned} R_2^1 \;=\;& (K_{rand}^{1,1} \oplus X_{part\_1}^{1,1} \oplus K_{rand}^{2,1} \oplus X_{part\_2}^{1,1} \oplus K_{rand}^{1,1} \oplus X_{part\_1}^{2,1} \oplus K_{rand}^{2,1} \oplus X_{part\_2}^{2,1})\\ &+ (K_{rand}^{1,1} \oplus X_{part\_1}^{2,1} \oplus K_{rand}^{2,1} \oplus X_{part\_2}^{2,1} \oplus K_{rand}^{1,1} \oplus X_{part\_1}^{3,1} \oplus K_{rand}^{2,1} \oplus X_{part\_2}^{3,1})\\ &+ \ldots + (K_{rand}^{1,1} \oplus X_{part\_1}^{M-1,1} \oplus K_{rand}^{2,1} \oplus X_{part\_2}^{M-1,1} \oplus K_{rand}^{1,1} \oplus X_{part\_1}^{M,1} \oplus K_{rand}^{2,1} \oplus X_{part\_2}^{M,1})\\ &\times (\ldots,\;\; R_2^B = (K_{rand}^{1,B} \oplus X_{part\_1}^{1,B} \oplus K_{rand}^{2,B} \oplus X_{part\_2}^{1,B} \oplus K_{rand}^{1,B} \oplus X_{part\_1}^{2,B} \oplus K_{rand}^{2,B} \oplus X_{part\_2}^{2,B})\\ &+ (K_{rand}^{1,B} \oplus X_{part\_1}^{2,B} \oplus K_{rand}^{2,B} \oplus X_{part\_2}^{2,B} \oplus K_{rand}^{1,B} \oplus X_{part\_1}^{3,B} \oplus K_{rand}^{2,B} \oplus X_{part\_2}^{3,B}) + \ldots\\ &+ (K_{rand}^{1,B} \oplus X_{part\_11}^{M-1,B} \oplus K_{rand}^{2,B} \oplus X_{part\_2}^{M-1,B} \oplus K_{rand}^{1,B} \oplus X_{part\_1}^{M,B} \oplus K_{rand}^{2,B} \oplus X_{part\_2}^{M,B})). \end{aligned}$$

Thus, if $R_2^1 = R_2^2 = \cdots = R_2^B = 0, X_1, X_2, \ldots, X_M$ are equal. Otherwise, $X_1, X_2, \ldots, X_M$ are not equal.

Security analysis. Here, we will show the robustness of the proposed QPC protocol against insider and outsider attacks. If the length of the secrets is odd, it should be modified. This process not only contributes to correctly executing the proposed protocol but also assists in enhancing the security of the protocol by altering the original secret bits without affecting the final comparison result. Moreover, two random keys are generated and distributed between TPs and participants to encrypt the private information of parties. As discussed in[30,48], for improving the efficiency of the proposed DMQPC protocol, the private information of parties can be divided into several blocks of data. If the comparison result of a particular block is not equal, TP_1 announces that the outcome of the comparison is not similar; hence there is no need to execute the remaining rounds. The three protocols in subsections 2.1, 2.4, and 2.5 are similar. Also, in the two-party QPC with two rounds, the quantum channel in the first-round is similar to the quantum channel in the second-round, so here we only analyze the quantum communication in the first-round between the participants and TP_1.

Outside attack. In the two-party situation, Alice (Bob) sends $S_a^{'}$ ($S_b^{'}$) to TP_1, protected by single decoy photons l_{a1} (l_{b1}). Alice (Bob) then announces the measurement bases and the positions of all inserted decoy particles. Subsequently, the TP_1 announces the measurement results of all embedded decoy particles. Alice (Bob) then checks the security of the communication by checking whether the measurement results of the decoy particles are correct. Since the outside attacker does not learn the measurement bases of the decoy particles and their positions ahead of time, the well-known attacks such as entangle-resend attacks[32], correlation-elicitation attacks[49], and intercept-resend attacks[50] can be detected with nonzero probability[51]. For instance, if the eavesdropper, Eve, attempts to measure the decoy photons $|0\rangle$ or $|1\rangle$ in $S_a^{'}$ ($S_b^{'}$) with the correct basis (e.g., Z-basis), she successfully passes the public eavesdropping check. But, If Eve attempts to measure the decoy photons $|0\rangle$ or $|1\rangle$ in $S_a^{'}$ ($S_b^{'}$) with an incorrect basis (e.g., X-basis), she will be detected with a probability of 50%. The probability of choosing the wrong measuring basis is 50%. Thus, the rate of detecting Eve for each single decoy photon is 25% (i.e., 50% × 50%). Hence, the rate of detecting Eve for l single decoy photon is $1-(3/4)^l$, where $|l| = |l_{a1}| = |l_{b1}|$. This rate approaches 1 when l is large enough. Furthermore, a Trojan-horse attack[52] is prevented since photons are transmitted only once from participants to the TP_1. So, our two-party QPC protocol is fully secure against outsider attacks. Since the proposed DMQPC protocol uses the same strategy as the two-party process, it is also secure against outsider attacks.

Participant's attack. A significant advantage of our three different scenarios is that participant attacks such as collusion attack and cheating attack are not possible for the proposed protocols. Each participant receives two random keys from TP_1 and TP_2 for encrypting her/his secret without the participation or assistance of other parties. Therefore, there is no exchange of information or even communication among participants, and each participant sends the private information directly to the TP_1 and TP_2 through quantum channels. Thus, to steal confidential information, dishonest participants must adopt Eve's attack strategies because they act as outside attackers. As discussed above, the protocol is secure against outside attacks.

TP's attack. TP's attack is another type of participant's attack which could threaten the security of the protocol. Here we prove that our scheme is secure against dishonest or malicious TPs. Firstly, with the assumption that the two TPs are not allowed to collude together or with participants, our protocol is secure since the encrypted data is distributed to two independent TPs for computing the final comparison result. To clarify, assume we have a secret a and an encryption key b and $c = a \oplus b$. The probability of an attacker to know a is $\frac{1}{2^n}$, where n is the length of the secret a[53]. In the proposed protocol, from TP_2's point of view, as shown in Table 4, $X_{12} = X_1 \oplus X_2$. From Eqs. (2) and (3), $X_1 = K_{rand}^1 \oplus X_{part\_1}$ and $X_2 = K_{rand}^2 \oplus X_{part\_2}$ where X_{part_1} is the first part of the secret message (X) and X_{part_2} is the second part of X. The probability of TP_2 to know X is $\frac{1}{2^{\frac{n}{2}}}$, where n is the length of the secret X, and $\frac{n}{2}$ is the length of X_{12}. When n is large enough, the probability of getting the secret data is negligible. In addition, according to Table 4, TP_2 can obtain $X_{12} = 1 \oplus X_1^{'}$. Hence, if $X_{12} = 0$ then TP_2 can learn that $X_1^{'} = 1$, otherwise $X_1^{'} = 0$. However, the private information of Alice is still secure against TP_2's attack for two reasons: (1) TP_2 cannot learn any private information of Alice using $X_1^{'}$; (2) the private information of Alice (X_{part_1} and X_{part_2}) is protected by two random keys (K_{rand}^1 and K_{rand}^2).

From TP_1's point of view, Alice sends her encrypted secret (i.e., $C_{a1} = X_1 \oplus X_1^{'}$ ($C_{a2} = X_2 \oplus X_2^{'}$)) to TP_1. TP_1 cannot reveal any useful information without knowing X_1 or $X_1^{'}$ (X_2 or $X_2^{'}$). The probability of knowing the original secret is $\frac{1}{2^{\frac{n}{2}}}$, where n is the length of the secret X, and $\frac{n}{2}$ is the length of $C_{a1}(C_{a2})$. When n is large enough, the probability of TP_1 to know the original secret is negligible. Also, when participants' secret data is divided into B

Parameters	Liu-Wang protocol[46]	Our protocol
Quantum resource	Single photon states	Single photon states
Number of TPs	One	Two
Secure against participant attack	No	Yes
Quantum measurement (TP)	Single photon measurements	Single photon measurements
Quantum measurement (parties)	Single photon measurements	Single photon measurements
Preparing single photons (TP)	Yes	Yes
Preparing single photons (parties)	Yes	Yes
Dynamic	Yes	Yes
The Flexibility of comparing the private information of parties	TP can compare the secret information of any two parties of M ($M \geq 4$) parties with the assistance of other $M-2$ parties	TPs can compare the secret information of any subset of M parties without any assistance of other parties
Joining and leaving the comparison protocol	Any subset of M parties can join in the protocol before the quantum states are measured	Any subset of M parties can join in or leave the protocol at any time without any extra conditions
The cost of transmission	All private information of parties should be transmitted among parties for deducing the final result of the comparison	In case of executing the protocol in one round, only the first part of the secret bits is transmitted to TP_1 for deducing the final result of the comparison

Table 6. Comparison to Liu-Wang protocol[46].

Features	Ref. [58]	Ref. [40]	Ref. [41]	Ref. [42]	Ref. [43]	Ref. [44]	Ref. [31]	Ref. [45]	Ref. [46]	Our
Multiparty	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dynamic	No	No	No	No	No	No	No	No	Yes	Yes
Secure against participant attack	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	Yes
Secure against the malicious TP	No	No	No	No	No	No	No	No	No	Yes
Work in strangers' environment[31]	No	No	No	No	No	No	Yes	No	Yes	Yes

Table 7. Comparison to some existing QPC protocols.

blocks, the probability of $TP_1(TP_2)$ to identify the original secret is $\left(\frac{1}{2^{\left(\left(\frac{n}{B}\right)/2\right)}}\right)^B$, where B is the number of blocks. In addition, according to Table 4, TP_1 can obtain $C_{a1} = 1 \oplus X_2$ and $X_2 = 1 \oplus C_{a1}$. Hence, if $C_{a1} = 0$; then TP_1 can learn that $X_2 = 1$, otherwise $X_2 = 0$. However, the private information of Alice (X_{part_1} and X_{part_2}) is still secure against TP_1's attack, since $X_{part\_1} = X_1 \oplus K_{rand}^1$ and $X_{part\_2} = X_2 \oplus K_{rand}^2$.

Efficiency Analysis

The used qubit efficiency is defined as $\eta = \frac{C}{q}$ [54–56], where C refers to all classical bits that can be transmitted, and q refers to the total number of used photons. In the two-party case, the proposed protocol is executed in one or two rounds depending on the first-round result. If the proposed protocol is executed in one round, both Alice and Bob prepare $\frac{n}{2}$ single photons. The protocol is completed in one round when the comparison result of the first parts of Alice's secret and Bob's secret are not equal. Thus, the qubit efficiency is $\frac{n}{\frac{n}{2}+\frac{n}{2}}$ (i.e., 100%). However, if the first parts of Alice's secret and Bob's secret are equal, the proposed protocol is executed in two rounds. Hence, the qubit efficiency is $\frac{n}{2\left(\frac{n}{2}+\frac{n}{2}\right)}$ (i.e. 50%). In the multi-party protocol with two rounds, the qubit efficiency of one round is $\frac{n}{M\frac{n}{2}}$, and the qubit efficiency for the two rounds is $\frac{n}{Mn}$. In the multi-party protocol with B blocks, the proposed protocol is executed in one or more blocks depending on the previous block result. Thus, the qubit efficiency is ranging from $\frac{n}{Mr_n}$ to $\frac{n}{Mn}$, where $r_n = \frac{n}{2B}$ is the number of bits in each round and B is the number of determined blocks. For example, consider four participants ($M = 4$) who would like to compare their secrets of length 12 bits ($n = 12$). In this case, they can divide the secret into 2, 3, or 6 blocks, each part containing 6 bits, 4 bits, or 2 bits, respectively. Assume that they choose to divide the secrets into 2 blocks (i.e., $B = 2$) and each block contains 6 bits (i.e., $\frac{n}{B} = 6$); hence the $r_n = \frac{12}{4} = 3$. Then the qubit efficiency ranges from 25% to 100%. It should be noted that the qubit efficiency increases or decreases depending on the number of participants and selected blocks. For comparison, in Liu and Wang's protocol[46], the qubit efficiency is $\frac{n}{M\left(\frac{n}{2}+\frac{n}{2}\right)}$, and for $n = 12$ and $M = 4$, the qubit efficiency is equal to 40%.

Comparison

Here we compare the performance of our DMQPC proposed scheme with previous MQPC schemes. We first compare our DMQPC protocol with Liu and Wang's protocol[46] (see Table 6). We then compare our DMQPC protocol with previous MQPC protocols.

Abulkasim *et al.*[57] showed that the Liu-Wang protocol suffers from participant attack. In our proposed protocol, participant attack is not possible. Thus, our protocol is safe not only against well-known participant attacks but also against potential participant attacks. Both the Liu-Wang protocol and our protocol use single photon states as a quantum resource and perform single photon measurements. The Liu-Wang protocol uses one TP who performs single photon measurements. In our protocol, two TPs are adopted and they also perform single photon preparation and measurements.

Like the Liu-Wang protocol, in our scheme, both the TP and the participants prepare single photons for deducing the comparison result. Like the Liu-Wang protocol, our protocol is dynamic so that any new subset of *M* parties can join or leave the protocol at any time. However, in the Liu-Wang protocol, new participants have to participate in the protocol before the quantum states are measured. Unlike the Liu-Wang protocol, in our scheme, the TPs can compare the private information of any subset of M parties without any assistance from other parties. In contrary to the Liu-Wang protocol, our scheme reduces the cost of communication by half, in some situations, where the protocol can be executed in one round to get the final comparison result.

From Table 7, like the protocols in refs. [31,40,42–45,58], our protocol is secure against participant attack. In contrast with the proposed protocols in refs. [31,40–46], which suppose that there is a semi-honest TP who executes the QPC protocol loyally, our proposed protocol allows for almost-dishonest TPs. Unlike the protocols in refs. [31,40–46,58], our protocol is secure against a malicious $TP_1(TP_2)$. Like the protocols in refs. [31,46], our protocol works in an environment where participants and TPs could be strangers, where there is no need for authenticated channels to prevent secret information from leaking. Compared to previous work, our main contribution is that participant attack is not possible in this work, since there is no exchange of information or even communication among participants. In addition, our scheme reduces the cost of communication.

Conclusion

This work proposes a novel dynamic multiparty quantum private comparison protocol that does not allow participant attack. The proposed protocol divides the private information into equal parts, and every participant independently encrypts her/his secrets using two random keys before sending them to two third parties using quantum channels. The protocol is executed in one or more rounds depending on the result of the previous round. The private information can also be divided into a number of blocks, with each block containing two equal parts of the secret. The dynamic nature of the proposed protocol enables the two TPs to compare the private information of any subset of *M* parties without any assistance from other parties. Any subset of *M* parties can join in or leave the protocol at any time without any extra conditions. Our analysis proves that the proposed protocol is correct and fully secure against outside attack. Furthermore, the scheme is not open to participant attacks. Compared to existing schemes, our protocol is more efficient, more secure and more feasible. Thus, our scheme is an ideal choice for comparing private information of *M* parties.

Received: 31 December 2018; Accepted: 5 November 2019;
Published online: 28 November 2019

References

1. Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **560**, 7–11 (2014).
2. Shor, P. W. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A* **52**, R2493 (1995).
3. Martin-Lopez, E. *et al.* Experimental realization of Shor's quantum factoring algorithm using qubit recycling. *Nat. Photo.* **6**, 773 (2012).
4. Politi, A., Matthews, J. C. & O'brien, J. L. Shor's quantum factoring algorithm on a photonic chip. *Science* **325**, 1221–1221 (2009).
5. Jin, X.-M. *et al.* Experimental free-space quantum teleportation. *Nat. photo.* **4**, 376 (2010).
6. Yin, J. *et al.* Quantum teleportation and entanglement distribution over 100-kilometre free-space channels. *Nature* **488**, 185 (2012).
7. Zhang, Q. *et al.* Experimental quantum teleportation of a two-qubit composite system. *Nat. Phys.* **2**, 678 (2006).
8. Huang, Y.-F., Ren, X.-F., Zhang, Y.-S., Duan, L.-M. & Guo, G.-C. Experimental teleportation of a quantum controlled-NOT gate. *Phys Rev Lett* **93**, 240501 (2004).
9. Ren, J.-G. *et al.* Ground-to-satellite quantum teleportation. *Nature* **549**, 70 (2017).
10. Bennett, C. H. & Wiesner, S. J. Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states. *Phys Rev Lett* **69**, 2881 (1992).
11. Mattle, K., Weinfurter, H., Kwiat, P. G. & Zeilinger, A. Dense coding in experimental quantum communication. *Phys Rev Lett* **76**, 4656 (1996).
12. Wang, C., Deng, F.-G., Li, Y.-S., Liu, X.-S. & Long, G. L. Quantum secure direct communication with high-dimension quantum superdense coding. *Phys. Rev. A* **71**, 044305 (2005).
13. Hu, X.-M. *et al.* Beating the channel capacity limit for superdense coding with entangled ququarts. *Sci. advances* **4**, eaat9304 (2018).
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. Chen, X.-B., Wang, T.-Y., Du, J.-Z., Wen, Q.-Y. & Zhu, F.-C. Controlled quantum secure direct communication with quantum encryption. *Int. J. Quantum Inf* **6**, 543–551 (2008).
16. Farouk, A., Zakaria, M., Megahed, A. & Omara, F. A. A generalized architecture of quantum secure direct communication for N disjointed users with authentication. *Sci. reports* **5**, 16080 (2015).
17. Hillery, M., Bužek, V. & Berthiaume, A. Quantum secret sharing. *Phys. Rev. A* **59**, 1829 (1999).
18. Abulkasim, H., Hamad, S., El Bahnasy, K. & Rida, S. Z. Authenticated quantum secret sharing with quantum dialogue based on Bell states. *Phys. Scr.* **91**, 085101 (2016).
19. Abulkasim, H., Hamad, S., Khalifa, A. & El Bahnasy, K. Quantum secret sharing with identity authentication based on Bell states. *Int. J. Quantum Inf* **15**, 1750023 (2017).
20. Qin, H., Tang, W. K. & Tso, R. Rational quantum secret sharing. *Sci. reports* **8**, 11115 (2018).
21. Abulkasim, H., Hamad, S. & Elhadad, A. Reply to Comment on 'Authenticated quantum secret sharing with quantum dialogue based on Bell states'. *Phys. Scr.* **93**, 027001 (2018).
22. Nguyen, B. A. Quantum dialogue. *Phys. Lett. A* **328**, 6–10 (2004).

23. Zhou, N.-R., Li, J.-F., Yu, Z.-B., Gong, L.-H. & Farouk, A. New quantum dialogue protocol based on continuous-variable two-mode squeezed vacuum states. *Quantum Inf Process* **16**, 4 (2017).
24. Zhou, N., Zeng, G. & Xiong, J. Quantum key agreement protocol. *Electron. Lett.* **40**, 1149–1150 (2004).
25. Cao, H. & Ma, W. Multi-party traveling-mode quantum key agreement protocols immune to collusive attack. *Quantum Inf Process* **17**, 219 (2018).
26. Yao, A. C. In *Foundations of Computer Science*, 1982. *SFCS'08. 23rd Annual Symposium on*. 160–164 (IEEE).
27. Boudot, F., Schoenmakers, B. & Traore, J. A fair and efficient solution to the socialist millionaires' problem. *Discrete Appl. Math.* **111**, 23–36 (2001).
28. Lin, H.-Y. & Tzeng, W.-G. In *International Conference on Applied Cryptography and Network Security*. 456–466 (Springer).
29. Lo, H.-K. Insecurity of quantum secure computations. *Phys. Rev. A* **56**, 1154 (1997).
30. Yang, Y.-G. & Wen, Q.-Y. An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. *J Phys A-Math Theor* **42**, 055305 (2009).
31. Hung, S.-M., Hwang, S.-L., Hwang, T. & Kao, S.-H. Multiparty quantum private comparison with almost dishonest third parties for strangers. *Quantum Inf Process* **16**, 36 (2017).
32. Gao, F., Qin, S.-J., Wen, Q.-Y. & Zhu, F.-C. A simple participant attack on the brádler-dušek protocol. *Quantum. Inf. Comput.* **7**, 329–334 (2007).
33. Zhang, W.-W. & Zhang, K.-J. Cryptanalysis and improvement of the quantum private comparison protocol with semi-honest third party. *Quantum Inf Process* **12**, 1981–1990 (2013).
34. Jiang, L., He, G., Nie, D., Xiong, J. & Zeng, G. Quantum anonymous voting for continuous variables. *Phys. Rev. A* **85**, 042309 (2012).
35. Xue, P. & Zhang, X. A simple quantum voting scheme with multi-qubit entanglement. *Sci. reports* **7**, 7586 (2017).
36. Muhammad, S. *et al*. Quantum bidding in Bridge. *Phys. Rev. X* **4**, 021047 (2014).
37. Hogg, T., Harsha, P. & Chen, K.-Y. Quantum auctions. *Int. J. Quantum Inf* **5**, 751–780 (2007).
38. Zhang, R., Shi, R.-h, Qin, J.-q & Peng, Z.-w An economic and feasible Quantum Sealed-bid Auction protocol. *Quantum Inf Process* **17**, 35 (2018).
39. Zhao, Z., Naseri, M. & Zheng, Y. Secure quantum sealed-bid auction with post-confirmation. *Opt Commun* **283**, 3194–3197 (2010).
40. Chang, Y.-J., Tsai, C.-W. & Hwang, T. Multi-user private comparison protocol using GHZ class states. *Quantum Inf Process* **12**, 1077–1088 (2013).
41. Luo, Q.-b, Yang, G.-w, She, K., Niu, W.-n & Wang, Y.-q Multi-party quantum private comparison protocol based on d-dimensional entangled states. *Quantum Inf Process* **13**, 2343–2352 (2014).
42. Ye, T.-Y. Multi-party quantum private comparison protocol based on entanglement swapping of Bell entangled states. *Commun. Theor. Phys.* **66**, 280 (2016).
43. Huang, S.-L., Hwang, T. & Gope, P. Multi-party quantum private comparison protocol with an almost-dishonest third party using GHZ states. *Int. J. Theor. Phys.* **55**, 2969–2976 (2016).
44. Zhao-Xu, J. & Tian-Yu, Y. Multi-party quantum private comparison based on the entanglement swapping of d-level cat states and d-level Bell states. *Quantum Inf Process* **16**, 177 (2017).
45. Ye, T. & Ji, Z. Multi-user quantum private comparison with scattered preparation and one-way convergent transmission of quantum states. *Sci. China Phys. Mech. Astron.* **60**, 090312 (2017).
46. Liu, W. & Wang, Y.-B. Dynamic multi-party quantum private comparison protocol with single photons in both polarization and spatial-mode degrees of freedom. *Int. J. Theor. Phys.* **55**, 5307–5317 (2016).
47. Hu, J.-Y. *et al*. Experimental quantum secure direct communication with single photons. *Light Sci. Appl.* **5**, e16144 (2016).
48. Li, J., Jia, L., Zhou, H.-F. & Zhang, T.-T. Secure quantum private comparison protocol based on the entanglement swapping between three-particle W-class state and bell state. *Int. J. Theor. Phys.* **55**, 1710–1718 (2016).
49. Fei, G., Song, L., Qiao-Yan, W. & Fu-Chen, Z. A special eavesdropping on one-sender versus N-receiver QSDC protocol. *Chinese Phys. Lett.* **25**, 1561 (2008).
50. Lin, J., Tseng, H.-Y. & Hwang, T. Intercept–resend attacks on Chen *et al*.'s quantum private comparison protocol and the improvements. *Opt Commun* **284**, 2412–2414 (2011).
51. Cai, Q.-Y. Eavesdropping on the two-way quantum communication protocols with invisible photons. *Phys. Lett. A* **351**, 23–25 (2006).
52. Gisin, N., Fasel, S., Kraus, B., Zbinden, H. & Ribordy, G. Trojan-horse attacks on quantum-key-distribution systems. *Phys. Rev. A* **73**, 022320 (2006).
53. Sun, Z., Yu, J., Wang, P., Xu, L. & Wu, C. Quantum private comparison with a malicious third party. *Quantum Inf Process* **14**, 2125–2133 (2015).
54. Chen, J.-H., Lee, K.-C. & Hwang, T. The enhancement of Zhou *et al*.'s quantum secret sharing protocol. *Int. J. Mod. Phy. C* **20**, 1531–1535 (2009).
55. Ting, X. & Tian-Yu, Y. Cryptanalysis and Improvement for the Quantum Private Comparison Protocol Based on Triplet Entangled State and Single-Particle Measurement. *Int. J. Theor. Phys.* **56**, 771–780 (2017).
56. Hwang, T. & Lee, K.-C. EPR quantum key distribution protocols with potential 100% qubit efficiency. *IET Inf. Secur.* **1**, 43–45 (2007).
57. Abulkasim, H. *et al*. Improved Dynamic Multi-Party Quantum Private Comparison for Next-Generation Mobile Network. *IEEE Access* **7**, 17917–17926 (2019).
58. Zhou, Y.-H., Shi, W.-M. & Yang, Y.-G. Comment on "Efficient and feasible quantum private comparison of equality against the collective amplitude damping noise". *Quantum Inf Process* **13**, 573–585 (2014).

Author contributions

Abulkasim, H. designed the scheme. Abulkasim, H., Farouk, A., Hamad, S., Mashatan, A. and Ghose, S. did security analysis and comparisons. Abulkasim, H. and Farouk, A. prepared all tables and figures. All authors contributed to the writing and discussion of the paper.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to H.A. or A.F.

Reprints and permissions information is available at www.nature.com/reprints.

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