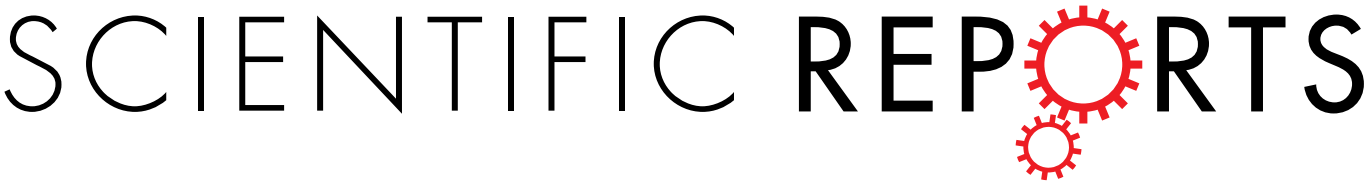

OPEN

Efficient multiparty quantum key agreement with collective detection

Received: 25 August 2017
Accepted: 23 October 2017
Published online: 10 November 2017

Wei Huang[1], Qi Su[2], Bin Liu[3], Yuan-Hang He[1], Fan Fan[1] & Bing-Jie Xu[1]

As a burgeoning branch of quantum cryptography, quantum key agreement is a kind of key establishing processes where the security and fairness of the established common key should be guaranteed simultaneously. However, the difficulty on designing a qualified quantum key agreement protocol increases significantly with the increase of the number of the involved participants. Thus far, only few of the existing multiparty quantum key agreement (MQKA) protocols can really achieve security and fairness. Nevertheless, these qualified MQKA protocols are either too inefficient or too impractical. In this paper, an MQKA protocol is proposed with single photons in travelling mode. Since only one eavesdropping detection is needed in the proposed protocol, the qubit efficiency and measurement efficiency of it are higher than those of the existing ones in theory. Compared with the protocols which make use of the entangled states or multi-particle measurements, the proposed protocol is more feasible with the current technologies. Security and fairness analysis shows that the proposed protocol is not only immune to the attacks from external eavesdroppers, but also free from the attacks from internal betrayers.

Since the pioneer work published by Bennett and Brassard in 1984[1], the principles of quantum mechanics was introduced to protect information security, which opened the new research area of cryptography, quantum cryptography[1–45]. Thus far, many branches of quantum cryptography have been presented to offer various security properties, including quantum key distribution (QKD)[1–12], quantum secure direct communication (QSDC)[13–20], quantum secret sharing (QSS)[21–26], quantum secure multiparty computation(QSMC)[27–41], etc. Recently, a new branch of quantum cryptography, quantum key agreement (QKA), has received more and more attention. Different from QKD, in which a participant generates the secret key and then distributes it to the others, each of the participants in the QKA protocol should contribute his/her influence to the final common key. In other words, aside from having the ability of resisting the external attackers from stealing the key as QKD protocols, QKA protocols should also have the ability of being immune to the participant attack, i.e., a non-trivial subset of the participants tries to predetermine the final common key alone.

As the earliest and the maturest branch of quantum cryptography, QKD has been developed theoretically and experimentally to be one of the most promising technologies in quantum cryptography. However, as a new branch of quantum cryptography, QKA is still in its infancy. In 2004, the first QKA protocol was proposed by Zhou *et al*. with the maximally entangled states and the technique of quantum teleportation[46]. Almost simultaneously, Hsueh and Chen proposed another QKA protocol by employing the maximally entangled states[47]. However, Tsai *et al*. demonstrated that neither of the two protocols could qualify as a QKA protocol[48,49], i.e., neither of them can simultaneously achieve the fairness property or security property. In 2010, by utilizing the ideas of the famous BB84 protocol, Chong *et al*. proposed a QKA protocol based on the technique of delayed measurement[50]. In 2011, in order to close the flaws pointed out by Tsai *et al*.[49], Chong *et al*.[51] presented a modified version of the QKA protocol proposed in ref.[47]. In 2014, Huang *et al*. presented two QKA protocols which can be immune to the collective noises[52,53], In 2016, He *et al*. put forward a QKA protocol by utilizing four-particle entangled states[49]. Nevertheless, all of the protocols mentioned above are limited to the two-party case[46–54].

To extend the research of QKA to the multiparty case, researchers begin to focus on MQKA, where more than two participants cooperate to share a common key securely and fairly. In 2013, by utilizing EPR pairs and the technique of entanglement swapping, Shi *et al*.[55] tried to propose the first MQKA protocol. However, Liu *et al*.[56]

[1]Science and Technology on Communication Security Laboratory, Chengdu, 610041, China. [2]State Key Laboratory of Cryptology, Beijing, 100878, China. [3]College of Computer Science, Chongqing University, Chongqing, 400044, China. Correspondence and requests for materials should be addressed to W.H. (email: huangwei096505@aliyun.com)

pointed out that this protocol failed to achieve the fairness property, and further put forward a distributed-mode MQKA protocol with single photons. In 2013, Sun *et al.*[57] made the attempt to improve the efficiency of Liu *et al.*'s MQKA protocol and propose a MQKA protocol in travelling mode. Unfortunately, this protocol has also been demonstrated to be unfairness[58]. In 2014, a distributed-mode MQKA protocol is proposed with GHZ states by Xu *et al.*[59]. In the same year, two travelling-mode MQKA protocols were presented with cluster states and six-qubit states, respectively by Sun *et al.*[60,61]. Meanwhile, Shukla *et al.* put forward a travelling-mode MQKA protocol by employing Bell state and Bell measurements[62]. Nevertheless, Zhu *et al.* found out that there exist some loopholes in Shukla *et al.*'s protocol and further proposed an improved version of this protocol[63]. In 2016, Sun *et al.* presented an MQKA protocol based on commutative encryption[64]. However, these travelling-mode MQKA protocols[60,61,63,64] are unfair under the collusion attack from internal betrayers[65,66]. In other words, a non-trivial subset of the involved participants can conspire to predetermine the final common key without being noticed by others. In 2016, Huang *et al.* proposed a travelling-mode MQKA protocol with single photons and unitary operations[67]. Recently, Cao *et al.* also presented a travelling-mode MQKA protocol based on quantum search algorithm[68].

In a travelling-mode MQKA protocol, every quantum information carrier sequence, which is used for encoding secret information, will sequentially be processed by all the involved participants of the protocol. That is to say, in an n-party QKA protocol, each quantum information carrier sequence will be transmitted n times. If the eavesdropping is checked after every transmission, a lot of quantum states (usually referred to the decoy qubits) need consuming, and hence the qubit efficiency and measurement efficiency will drop substantially. To our best knowledge, all of the existing travelling-mode MQKA protocols have fallen into this category[57,60–64,67], i.e., eavesdropping check is needed in each transmission of the quantum information carriers sequence. To improve the qubit efficiency of travelling-mode MQKA, we devote ourselves to designing a travelling-mode MQKA protocol where the eavesdropping check is not required in each transmission of the quantum information carrier sequence. In this paper, we propose an efficient travelling-mode MQKA with single photons, inspired by the results of refs[11,12,64,67]. By employing the ideas of collective eavesdropping detection strategy[11,12] which was first proposed by Shih *et al.*[11], the number of eavesdropping checks needed in this protocol has been significantly reduced. Hence, the qubit efficiency and measurement efficiency of the proposed protocol are higher than those of the existing ones (including both the protocols in travelling mode and the ones in distributed mode) in theory. In addition, compared with the protocols which utilize the entangled states or multi-particle measurements, the proposed protocol is more feasible with the current technologies due to the utilization of single photons and single-particle measurements.

The remainder of this paper is organized as follows. Next section first presents our travelling-mode MQKA protocol with single photons in detail. Then the security and fairness of the proposed protocol is analyzed. Finally, a discussion as well as a brief conclusion is given in the "Discussion section".

Results

The proposed travelling-mode MQKA protocol. Herein we propose a new travelling-mode MQKA protocol by employing single photons, where n participants, $P_1, P_2, \ldots, P_n$ cooperate to establish a common key securely and fairly. For each of the involved participant P_i, $1 \le i \le n$, we suppose that he/she has an $(l+kl)$-bit private random key K_i and $n-1(l+kl)$-bit random controlling strings $C_{i(i+1)}, C_{i(i+2)}, \ldots, C_{i(i-1)}$, where $C_{i(j+n)} = C_{ij}$, and k is the detection rate. Similar to the existing QKA protocols[46–67], the classical communication channels are assumed to be authenticated in this protocol. Moreover, the technique of "block transmission"[13–16] where the quantum information carriers are ordered and transmitted in blocks, is utilized to ensure the security of the photon transmission in this protocol. The detailed steps of the proposed MQKA protocol can be described as follows.

(1) Each of the n participants P_i ($i = 1, 2, \ldots, n$) prepares an ordered sequence (denoted as S_i) of $l+kl$ single photons, each of which is randomly in one of the four states in $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Here,

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{1}$$

Then P_i sends S_i to P_{i+1}, for $i = 1, 2, 3, \ldots, n$, where $P_{n+i} = P_i$.

(2) After the reception of S_i, P_{i+1} announces the fact. Then he/she encodes his private key and the corresponding controlling binary string, K_{i+1} and $C_{(i+1)i}$, onto S_i. Specifically, if the j-th bits of K_{i+1} and $C_{(i+1)i}$, i.e., $K_{i+1}^j C_{(i+1)i}^j$, are 00/10/01/11, P_{i+1} performs the unitary operation $I/F/W\left(\frac{p\pi}{n}\right)/FW\left(\frac{p\pi}{n}\right)$ on the j-th photon of S_i (i.e., S_i^j), for $j = 1, 2, 3, \ldots, l+kl$, where

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad F = -iY = -i\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$
$$W\left(\frac{p\pi}{n}\right) = e^{\frac{-p\pi Y}{2n}} = \cos\left(\frac{p\pi}{2n}\right)I - i\sin\left(\frac{p\pi}{n}\right)Y = \begin{pmatrix} \cos\left(\frac{p\pi}{2n}\right) & -\sin\left(\frac{p\pi}{2n}\right) \\ \sin\left(\frac{p\pi}{2n}\right) & \cos\left(\frac{p\pi}{2n}\right) \end{pmatrix}, \tag{2}$$

where p is a prime number, and $p < n$. The effect of F and $W\left(\frac{p\pi}{n}\right)$ on the four polarized photons, $|0\rangle, |1\rangle, |+\rangle$ and $|-\rangle$, can be respectively described as

$$
\begin{aligned}
F|0\rangle = |1\rangle, \quad F|1\rangle = -|0\rangle, \quad F|+\rangle = -|-\rangle, \quad F|-\rangle = |+\rangle,\\
W\left(\frac{p\pi}{n}\right)|0\rangle = \cos\left(\frac{p\pi}{2n}\right)|0\rangle + \sin\left(\frac{p\pi}{2n}\right)|1\rangle,\\
W\left(\frac{p\pi}{n}\right)|1\rangle = \cos\left(\frac{p\pi}{2n}\right)|1\rangle - \sin\left(\frac{p\pi}{2n}\right)|0\rangle,\\
W\left(\frac{p\pi}{n}\right)|+\rangle = \cos\left(\frac{p\pi}{2n}\right)|+\rangle - \sin\left(\frac{p\pi}{2n}\right)|-\rangle,\\
W\left(\frac{p\pi}{n}\right)|-\rangle = \cos\left(\frac{p\pi}{2n}\right)|-\rangle + \sin\left(\frac{p\pi}{2n}\right)|+\rangle.
\end{aligned} \tag{3}
$$

After finishing performing the unitary operations, P_{i+1} sends the new sequence (denoted as $S_{i(i+1)}$) to P_{i+2}. Meanwhile, each of the other $n-1$ participants processes his/her received sequence just in the same way and sends the obtained new sequence to next participant. That is, P_{i+1} sends $S_{i(i+1)}$ to P_{i+2}, for $i = 1, 2, 3, \ldots, n$. Here, we denote what the n participants have done in this step as the first round of encoding (denoted as Round 1).

(3) The n participants execute another $n-2$ rounds of encoding similar to the process of Round 1. That is, just in the same way as P_{i+1} dose in steps (2), the n participants repeatedly execute information encoding phase until P_i receives $S_{i(i+1)\ldots(i-1)}$ from P_{i-1}, for $i = 1, 2, 3, \ldots, n$. In other words, for each participant P_i, $i = 1, 2, 3, \ldots, n$, when he/she receives the photon sequence from P_{i-1} in Round v, $v \in \{2, \ldots, n-1\}$, he/she encodes K_i and $C_{i(i+n-v)}$ $(=C_{i(i-v)})$ onto the received sequence. Afterwards, he/she sends the processed sequence $S_{(i-v)(i-v+1)\ldots i}$ to P_{i+1}. This procedure is repeated until P_i receives $S_{i(i+1)\ldots(i-1)}$ from P_{i-1}.

(4) Upon receiving $S_{i(i+1)\ldots(i-1)}$ from P_{i-1}, P_i announces the fact. Once conforming that every participant has received the photon sequence prepared by himself/herself, all the n participants cooperate to randomly choose kl positions (from $l+kl$ positions), at which the quantum information carriers will be used to check eavesdropping hereafter. Concretely, P_1 randomly chooses $\left\lfloor \frac{kl}{n} \right\rfloor$ positions, and publishes the information of each chosen position, where $\lfloor x \rfloor$ represents the largest one of the integers which are smaller than x. Then P_2 chooses another $\left\lfloor \frac{kl}{n} \right\rfloor$ positions from the remaining $kl - \left\lfloor \frac{kl}{n} \right\rfloor$ positions and announces the position information. Just in the same way, P_i ($i = 3, 4, \ldots, n-1$) randomly chooses $\left\lfloor \frac{kl}{n} \right\rfloor$ from the remaining $l-(i-1)\left\lfloor \frac{kl}{n} \right\rfloor$ positions and publishes the position information. It should be noted that P_n should choose $kl-(n-1)\left\lfloor \frac{kl}{n} \right\rfloor$ positions for this check in order to make sure that the total number of the positions chosen by them is kl.

(5) After the participants finishing choosing the positions used for checking eavesdropping, each participant announces his/her $n-1$ controlling strings. Namely, P_i announces C_{ij}, for $i = 1, 2, 3, \ldots, n$, and $j = i+1, i+2, \ldots, i-1$. With the announced information, each of the participants deduces a $(l+kl)$-bit string as follows. P_i ($i = 1, 2, \ldots, n$) first offsets the effect of the controlling operations (operations determined by the bits of controlling strings) that have been performed on the photons of $S_{i(i+1)\ldots(i-1)}$. Concretely, to offset the controlling operations performed on the photons of $S_{i(i+1)\ldots(i-1)}$, P_i performs $W\left(\frac{-\widetilde{C}_i^j p\pi}{n}\right)$ on the j-th photon of $S_{i(i+1)\ldots(i-1)}$ (i.e., $S^j_{i(i+1)\ldots(i-1)}$), for $j = 1, 2, 3, \ldots, l+kl$, where $\widetilde{C}_i^{\,j} = C^j_{(i+1)i} + C^j_{(i+2)i} + \ldots + C^j_{(i-1)i}$. After that, he/she measures each of the $l+kl$ processed photons in the original basis as he/she prepares it. That is, if the original state of the processed photon is in basis $\{|0\rangle, |1\rangle\}/\{|+\rangle, |-\rangle\}$, he measures it in basis $\{|0\rangle, |1\rangle\}/\{|+\rangle, |-\rangle\}$. In ideal condition, P_i can obtain an $(l+kl)$-bit string $\overline{K}_i = K_{i+1} \oplus K_{i+2} \oplus \ldots \oplus K_{i-1}$ according to the $l+kl$ measurement results. To be specific, if the measurement result of the j-th photon is the same as (opposite to) its original state, $\overline{K}_i^{\,j} = 0$ (1). Once getting $\overline{K}_i$, P_i is able to deduce a $(l+kl)$-bit string $\hat{K}_i = K_i \oplus \overline{K}_i = K_1 \oplus K_2 \oplus \ldots \oplus K_n$. Just in the same manner, each participant gets his/her corresponding $(l+kl)$-bit string, i.e., P_i gets $\hat{K}_i$ for $i = 1, 2, 3, \ldots, n$. Obviously, in ideal condition, these n binary strings should be identical if there exists no eavesdropping.

(6) The n participants check eavesdropping with the kl positions chosen in step (4) and the $(l+kl)$-bit strings obtained in step (5). Specifically, each of the n participants publishes the values of the kl positions of his/her obtained string, i.e., P_i publishes the corresponding kl bits of $\hat{K}_i$ for $i = 1, 2, 3, \ldots, n$. Then each participants compares his/her announced kl-bit string with the ones published by the other participants. With the comparison results of the kl positions, they can judge whether the procedure is secure. If there exists no eavesdropping, each participant P_i drops the bits used for checking eavesdropping and getting an l-bit binary string with the remaining bits, i.e., $\hat{K}'_i$, $i = 1, 2, 3, \ldots, n$; otherwise, they abort the protocol. In ideal condition, by utilizing steps (1)-(5), the n established random strings should be identical, i.e., $\hat{K}'_1 = \hat{K}'_2 = \ldots = \hat{K}'_n$. To check consistency of the n binary strings, each participant P_i calculates the hash value $h(\lambda \| \hat{K}'_i)$. Here, h: $\{0,1\}^* \rightarrow \{0,1\}^s$ is a one-way hash function previously chosen by the n participants, and $\lambda = f(\lambda_1, \lambda_2, \ldots, \lambda_n)$ (e.g., $\lambda = f(\lambda_1 \oplus \lambda_2 \oplus \ldots \oplus \lambda_n)$, where λ_i is a random bit generated and announced by P_i after deducing $\hat{K}'_i$, $i = 1, 2, \ldots, n$. If all the n hash values are identical, the n participants have established a common key $K = \hat{K}'_1 = \hat{K}'_2 = \ldots = \hat{K}'_n$; otherwise, they abort the results and restart the protocol.

Thus far, we have presented a new efficient travelling-mode MQKA protocol. In practical situation, there may exist a certain number of errors, which are caused by the noise, in $\hat{K}'_i$, $i = 1, 2, \ldots, n$. And this may lead the protocol fails in step (6) with a high probability. To circumvent this problem, several existing methods, such as

quantum error correction codes (QECC)[69] and quantum error avoiding codes (QEAC)[70] could be utilized. Moreover, as the proposed MQKA protocol contains two-way quantum communication, the participants involved in the protocol should also make use of a filter and a beam splitter to prevent the Trojan horse attack and the invisible-photon attack in practical implementation[71,72].

Security and fairness analysis. Herein we analyze the security and fairness of the proposed MQKA protocol. We first demonstrate that the protocol can achieve security property, i.e., be secure against the attacks from the external eavesdropper. Then we show its fairness property, i.e., be immune to the attacks from dishonest participants.

Security analysis. To analyze the security of the proposed protocol, we first suppose that Eve is an evil attacker who wants to eavesdrop the final common key without being noticed by the legal participants. Based on the principles of the proposed MQKA protocol, if Eve wants to achieve this goal, she should be capable of obtaining the private key of each participant without being found. To get a participant's private key, Eve can make use of different kinds of attacks. For instance, she could intercept and substitute the travelling photons, which are sent to the legal receiver, with the ones prepared by herself, or she could entangle the travelling photons with some additional states, with which she may be able to extract some valuable information about the encoded private key. However, in the proposed protocol, the private keys and controlling strings of the participants are encoded on the transmitted photons by performing certain unitary operations. Hence, whatever kind of attack Eve utilizes, the action to eavesdrop a participant's private key is equivalent to discriminate the operations that he/she has performed on the transmitted photon sequences. For example, when P_i receives the photon sequence from P_{i-1} in Round v, $v\in\{1, 2, 3, \ldots, n-1\}$, he/she encodes K_i^j and $C_{i(i+n-v)}^j(=C_{i(i-v)}^j)$ onto the j-th photon of the received sequence $S_{(i-v)(i-v+1)\ldots(i-1)}$. Obviously, if Eve wants to get K_i^j, she should know which one of the operations, I, F, $W\left(\frac{p\pi}{n}\right)$ and $FW\left(\frac{p\pi}{n}\right)$, P_i has performed on the corresponding photon. Since the controlling bit $C_{i(i-v)}^j$ will be encoded only once, Eve should be capable of discriminating the four unitary operations with a single use. In fact, these four unitary operations, I, F, $W\left(\frac{p\pi}{n}\right)$ and $FW\left(\frac{p\pi}{n}\right)$, utilized our protocol cannot be unambiguously discriminated with a single use. To demonstrate this conclusion, we first introduce a theory on quantum operation discrimination.

Theorem 1 The quantum operations $\zeta_1, \ldots, \zeta_n$ can be unambiguously discriminated by a single use if and only if for any $i=1, 2, \ldots, n$, $\mathrm{supp}(\zeta_i) \nsubseteq \mathrm{supp}(M_i)$, where $\mathrm{supp}(\zeta)$ denotes the support of a quantum operation ζ and $M_i = \{\zeta_j: j \neq i\}$[73].

It is easy to find that the unitary operations, I, F, $W\left(\frac{p\pi}{n}\right)$ and $FW\left(\frac{p\pi}{n}\right)$, satisfy the following relationship,

$$W\left(\frac{p\pi}{n}\right) = \cos\left(\frac{p\pi}{2n}\right)\cdot I + \sin\left(\frac{p\pi}{2n}\right)\cdot F + 0\cdot FW\left(\frac{p\pi}{n}\right), \tag{4}$$

which indicates that $\mathrm{supp}(W\left(\frac{p\pi}{n}\right)) \subseteq \mathrm{supp}(I, F, FW\left(\frac{p\pi}{n}\right))$. Hence according to according to Theorem 1, these four operations cannot be unambiguously discriminated by a single use. Namely, when these four unitary operations are respectively performed on a single qubit or one qubit of any entangled state, they cannot be unambiguously discriminated.

Moreover, in practical implementation, the participants involved in this protocol will make use of the methods given in refs[71,72] to resist the Trojan horse attack and invisible photon attack in each transmission of the every photon sequence. Therefore, the protocol is also immune to these two attacks.

Fairness analysis. It is well known that, for a multiparty quantum cryptographic protocol, the participant attacks[74] (i.e., the attacks from dishonest participants) are always more threatening than external attacks (i.e., the attacks from external eavesdroppers). In the executing process of a multiparty protocol, a dishonest participant has more opportunities to attack the protocol. First, he/she is able to replace the legal photon sequences, which are prepared or received by himself/herself, with whatever he/she wants. Second, in order to avoid introducing errors into the eavesdropping check, he/she could tell lies in the phase of classical information exchange. More important, in order to occupy a greater advantage, some dishonest participants can collaborate to cheat in the executing process of the protocol. Now, we make an analysis on the fairness of the proposed protocol to show its immunity to the participant attacks.

In the participant attack on the proposed protocol, one or more dishonest participants try to predetermine the final common key without being found by the honest participant. To show the immunity of the proposed protocol to such kind of attack, we consider the worst case, where the number of the honest participants is 1. In other words, n-1 dishonest participants collaborate to determine the final common key. Obviously, if the proposed protocol is immune to the participant attack under this assumption, it can also resist the participant attacks where the number of the dishonest participants is less than $n-1$.

Herein we show the immunity of the proposed protocol to the worst case. Without loss of generality, we suppose that P_i is the only participant who is honest, $i\in\{1, 2, \ldots, n\}$. According to the principles of the proposed protocol, we can find out that the final key gotten by P_i (i.e., $\hat{K}'_i$) is part of the $(l+kl)$-bit string $\hat{K}_i$, $i\in\{1, 2, \ldots, n\}$. Hence, if the $n-1$ dishonest participants could predetermine $\hat{K}_i$, they will have significant advantage in determining $\hat{K}'_i$. Apparently, the key point for the $n-1$ dishonest participants to predetermine $\hat{K}_i$ is to eavesdrop P_i's private key K_i before $S_{i(i+1)\ldots(i-1)}$ is sent back to P_i. For example, if the $n-1$ dishonest participants have obtained K_i and want $\hat{K}_i$ to be K^*, they can attack as follows. When P_{i+j} receives the sequence generated by P_i, i.e., $S_{i(i+1)..(i+j-1)}$, for $j=1, 2, \ldots, n$-2, he/she only encodes his/her corresponding controlling string $C_{(i+j)i}$ onto $S_{i(i+1)..(i+j-1)}$. This is

equivalent to the case that K_{i+j} is a zero vector. After receiving $S_{i(i+1)..(i-2)}$ from P_{i-2}, P_{i-1} encodes $K_i \oplus K^*$ and $C_{(i-1)i}$ onto $S_{i(i+1)..(i-2)}$. Then he/she sends the sequence $S_{i(i+1)..(i-1)}$ to P_i. Obviously, if there exists no external eavesdropping and the $n-1$ dishonest participants honestly announces their controlling strings in step (5). The $(l+kl)$-bit string obtained by P_i is K^*, i.e., $\hat{K}_i = K^* \oplus K_i \oplus K_i = K^*$.

As we analyzed in security analysis, the bits of K_i and the corresponding controlling string are encoded onto the received photon sequence with the four unitary operations, I, F, $W\left(\frac{p\pi}{n}\right)$ and $FW\left(\frac{p\pi}{n}\right)$. In other words, no matter what kind of attacking strategy the dishonest participants utilize, if they want to get K_i before being aware of P_i's controlling strings, they should be capable of unambiguously discriminating the four unitary operations with a single use. Nevertheless, according to the conclusion given above, the dishonest participants can never have this ability since these four unitary operations cannot be unambiguously discriminated with a single use. For instance, according to the principles of the proposed protocol, if the j-th photon of a sequence sent from P_{i-1}, i.e., S^j_{i-1}, is in basis $\{|0\rangle, |1\rangle\}(\{|+\rangle, |-\rangle\})$, after P_i's processing, the j-th photon of the sequence $S_{(i-1)i}$, i.e., $S^j_{(i-1)i}$, will randomly be one of the state in $\{|0\rangle, |1\rangle, |\overline{0}\rangle, |\overline{1}\rangle\}$ $(\{|+\rangle, |-\rangle, |\overline{+}\rangle, |=\rangle\})$, where

$$\begin{aligned}
|\overline{0}\rangle &= \cos\left(\frac{p\pi}{2n}\right)|0\rangle + \sin\left(\frac{p\pi}{2n}\right)|1\rangle,\\
|\overline{1}\rangle &= \cos\left(\frac{p\pi}{2n}\right)|1\rangle - \sin\left(\frac{p\pi}{2n}\right)|0\rangle,\\
|\overline{+}\rangle &= \cos\left(\frac{p\pi}{2n}\right)|+\rangle - \sin\left(\frac{p\pi}{2n}\right)|-\rangle,\\
|=\rangle &= \cos\left(\frac{p\pi}{2n}\right)|-\rangle + \sin\left(\frac{p\pi}{2n}\right)|+\rangle.
\end{aligned} \tag{5}$$

Obviously, without the controlling bit $C^j_{i(i-1)}$, P_{i+1} is unable to correctly deduce K_i^j since he/she does not know which basis he can utilize to measure $S^j_{(i-1)i}$. In fact, according the the conclusion drawn above, no matter what kind of state $S^j_{(i-1)}$ is in, P_{i+1} cannot deduce K_i^j correctly.

Based on the above analysis, we have shown that the dishonest participants are unable to get K_i before P_i receives $S_{i(i+1)...(i-1)}$. More precisely, the dishonest participants are unable to get K_i before P_i publishes his/her controlling strings. Under this circumstance, to eavesdrop K_i, each of the dishonest participants has to process the photon sequence, which is generated by P_i, strictly following the principles of the proposed protocol. It is not hard to find that, by utilizing this strategy, the dishonest participants could deduce K_i with the photon sequences prepared by themselves and the controlling strings announced by P_i. After obtaining K_i, the dishonest participants can deduce $\hat{K}_i^{'}$, which will be obtained by P_i in step (6), before announcing their controlling own strings. However, once the protocol proceed to this step, the only method that they can use to modify $\hat{K}_i^{'}$, is to announce fake controlling strings. Concretely, if the dishonest participants want to modify the j-th bit of $\hat{K}_i^{'}$, i.e., $\hat{K}_i^{'j}$, they should change the values of their corresponding controlling bits, $C^j_{(i+1)i}, \ldots, C^j_{(i-1)i}$, to make P_i perform an additional operation F on $S^j_{i(i+1)...(i-1)}$. However, whatever strategy they employ to modify the controlling bits that will be announced, the additional unitary operation, which they can make P_i perform on $S^j_{i(i+1)...(i-1)}$, will ineluctably belong to $\overline{W} = \left\{W\left(\frac{-p\pi}{n}\right), W\left(\frac{-2p\pi}{n}\right), \ldots, W\left(\frac{-(n-1)p\pi}{n}\right)\right\}$. It is easy to verify that, no matter what operation in $\overline{T}$ is performed on $S^j_{i(i+1)...(i-1)}$, the final state of $S^j_{i(i+1)...(i-1)}$ (i.e., the state of $S^j_{i(i+1)...(i-1)}$ after being performed $W\left(\frac{-\widetilde{C}_i^j p\pi}{n}\right)$ on it) will be transformed to a superposition state of $|0\rangle$ and $|1\rangle$ ($|+\rangle$ and $|-\rangle$), which indicates that the $n-1$ dishonest participants are unable to deterministically determine the value of $\hat{K}_i^{'j}$. Till now, we have shown that the proposed protocol is immune to the participant attack.

Discussion

Thus far, an efficient travelling-mode MQKA protocol has been proposed. In order to illustrate the advantages of this protocol, a discussion, where the proposed protocol is compared with the existing MQKA protocols, is made first in this section. After that, we end this paper with a short conclusion.

Key indicators of the proposed protocol. Before comparing the proposed protocol with the existing MQKA protocols, we first focus on some key indicators of the proposed protocol, i.e., qubit efficiency, measurement efficiency and the unitary operation efficiency.

Firstly, to check eavesdropping, the proposed protocol only need the n participants cooperate to perform one eavesdropping detection, i.e, the detection in step (6). In other words, in the process of the photon sequence transmitting, i.e., in steps (1)–(5), a participant need not perform any eavesdropping detection when they received a photon sequence from his/her previous participant. Obviously, this is the main merit of the proposed protocol since it can greatly reduce the number of the photons used for checking eavesdropping, and hence make the proposed efficient, i.e., has a high qubit efficiency. The qubit efficiency here is defined as $\eta = n_c/n_q$, where n_c is the length of the final common key established in this protocol, and n_q is the total number of the photons used for establishing the corresponding final common key. Concretely, to establish an l-bit final common key in ideal condition, each of the involved participants should prepare a sequence of $l+kl$ photons. In the only one eavesdropping detection, each participant will use kl photons in his/her sequences for checking eavesdropping. Since

n-party protocols	η_q	η_m	η_u
SZ13 protocol[55]	$\frac{1}{(2+kn)n}$; $\frac{1}{[70]}$	$\frac{2}{(2+k)n^2}$; $\frac{1}{[125]}$	0
LGHW13 protocol[56]	$\frac{1}{(n-1)(1+k)n}$; $\left[\frac{1}{135}\right]$	$\frac{1}{(n-1)(1+k)n}$; $\left[\frac{1}{135}\right]$	0
SZWLL13[57]	$\frac{1}{(1+kn)n}$; $\left[\frac{1}{60}\right]$	$\frac{1}{(1+kn)n}$; $\left[\frac{1}{60}\right]$	$\frac{1}{n^2}$; $\left[\frac{1}{100}\right]$
SYW16 protocol[60]	$\frac{2}{(4+kn)n}$; $\left[\frac{1}{45}\right]$	$\frac{2}{(kn+1)n}$; $\left[\frac{1}{30}\right]$	$\frac{2}{(n-1)n}$; $\left[\frac{1}{45}\right]$
SZWYZL16 protocol[61]	$\frac{1}{(3+2kn)n}$; $\left[\frac{1}{130}\right]$	$\frac{2}{(3+4kn)n}$; $\left[\frac{1}{115}\right]$	$\frac{2}{(2n-1)n}$; $\left[\frac{1}{95}\right]$
SHW15 protocol[64]	$\frac{1}{(1+kn)n}$; $\left[\frac{1}{60}\right]$	$\frac{1}{(1+kn)n}$; $\left[\frac{1}{60}\right]$	$\frac{1}{(1+n)n}$; $\left[\frac{1}{110}\right]$
HSXLFJY16 protocol[67]	$\frac{1}{(1+kn)n}$; $\left[\frac{1}{60}\right]$	$\frac{1}{(1+kn)n}$; $\left[\frac{1}{60}\right]$	$\frac{1}{n^2}$; $\left[\frac{1}{100}\right]$
CM17 protocol[68]	$\frac{1}{(1+kn)n}$; $\left[\frac{1}{60}\right]$	$\frac{1}{(1+kn)n}$; $\left[\frac{1}{60}\right]$	$\frac{2}{(n+1)n}$; $\left[\frac{1}{55}\right]$
Our protocol	$\frac{1}{n(1+k)}$; $\left[\frac{1}{15}\right]$	$\frac{1}{n(1+k)}$; $\left[\frac{1}{15}\right]$	$\frac{1}{(1+k)n^2}$; $\left[\frac{1}{150}\right]$

Table 1. Comparison of the efficiencies. In this table, η_q, η_m and η_u are qubit efficiency, measurement efficiency and unitary operation efficiency, respectively. The number in [] represents the concrete value of the efficiency when $n = 10$ and $k = 0.5$.

there are n participants involved in the proposed protocol, the total number of the photons, which will be used in establishing an l-bit final common key, is $n(l + kl)$. Therefore, the qubit efficiency of the proposed protocol is

$$\frac{l}{n(l+kl)} = \frac{1}{n(1+k)}. \tag{6}$$

Secondly, as the proposed protocol only need one eavesdropping detection, the number of the measurements required in this protocol is relatively small. Specifically, to establish an l-bit final common key, each of the participants need perform $l + kl$ measurements in theory. Namely, $(l + kl)n$ measurements are needed in this whole procedure of the protocol. Hence, the measurement efficiency (the ratio of the length of final common key to the number of the performed measurements) of the protocol is

$$\frac{l}{(l+kl)n} = \frac{1}{n(1+k)}. \tag{7}$$

Thirdly, since the security of the protocol is mainly based on the unitary operations performed on the transmitted photons. Here we calculate the unitary operation efficiency (the ratio of the length of final common key to the number of the performed unitary operations) of the protocol. Concretely, to establish an l-bit final common key, each of the participants need perform $n(l + kl)$ unitary operations in theory. That is to say, $(l + kl)n^2$ unitary operations are needed in total. Thus, the unitary operation efficiency of the proposed protocol is

$$\frac{l}{(l+kl)n^2} = \frac{1}{(1+k)n^2}. \tag{8}$$

Moreover, in the existing MQKA protocols, after the participants confirm that there exists no eavesdropping in the executing procedure of the protocol, each participant directly makes use of the measurements results of the remaining quantum information carriers to deduce a binary string as his/her final key. However, they do not check whether the keys in their hands are identical. In order to solve this problem, we have added a step, i.e., step (6), in this proposed to check the consistency of the final keys in the participants' hands.

Comparison. Herein we compare the proposed protocols with seven existing MQKA protocols in the following five aspects: qubit efficiency, measurement efficiency, unitary operation efficiency, security against participant attack and key consistency check. The seven existing protocols are SZ13 protocol[55], LGHW13 protocol[56], SZWLL13 protocol[57], SYW16 protocol[60], SZWYZL16 protocol[61], SHW15 protocol[64], HSXLFJY16 protocol[67] and HM17 protocol[68]. The indicators of these existing MQKA protocols are calculated below, and the specific comparison results are shown in Table 1 and Table 2.

SZ13 protocol. This protocol make use of entanglement to establish the final common key, and utilize the technique of decoy particles to assure its security. The qubit efficiency of this protocol is $\frac{1}{(2+kn)n}$. The measurement efficiency of this protocol is $\frac{2}{(2+k)n^2}$. It should be pointed out that the measurements performed in this protocol

n-party protocols	key consistency check	security against participant attack	needing entanglement?
SZ13 protocol[55]	No	insecure	Yes
LGHW13 protocol[56]	No	secure	No
SZWLL13[57]	No	insecure	No
SYW16 protocol[60]	No	insecure	Yes
SZWYZL16 protocol[61]	No	insecure	Yes
SHW15 protocol[64]	No	insecure	No
HSXLFJY16 protocol[67]	No	secure	No
CM17 protocol[68]	No	secure	Yes
Our protocol	Yes	secure	No

Table 2. Comparison of the other indicators.

includes both single-particle measurements and multi-particle measurements (i.e., Bell measurements). More important, this protocols is vulnerable to the participant attack[55,56].

LGHW13 protocol. The protocol is immune to the participant attack, and it does not need utilize entanglement to establish the final key[56]. However, this protocol is quite inefficient due to a low qubit efficiency $\left(\frac{1}{(n-1)(1+k)n}\right)$ and a low measurement efficiency $\left(\frac{1}{(n-1)(1+k)n}\right)$.

SZWLL13. This protocol attempts to establish a final common key efficiently with single photons and unitary operations. The qubit efficiency, measurement efficiency and unitary efficiency of this protocol are $\frac{1}{(1+kn)n}$, $\frac{1}{(1+kn)n}$ and $\frac{1}{n^2}$, respectively. However, it cannot stand against the participant attack[57,58].

SYW16 protocol. The protocol tries to achieve the purpose of MQKA with four-qubit entangled cluster states. Its qubit efficiency, measurement efficiency and unitary efficiency are $\frac{2}{(4+kn)n}$, $\frac{2}{(kn+1)n}$ and $\frac{2}{(n-1)n}$, respectively. It should be noticed that the cluster basis measurements performed in this protocol is more difficult to implement than single-particle measurements under the current techniques. Moreover, this protocol is susceptible to the participant attack[60,65].

SZWYZL16 protocol. Due to the utilizing six-qubit entangled states, this protocol is not very efficient. Concretely, the qubit efficiency, measurement efficiency and unitary operation efficiency are $\frac{1}{(3+2kn)n}$, $\frac{2}{(3+4kn)n}$ and $\frac{2}{(2n-1)n}$, respectively. Moreover, this protocol is also insecure against participant attack[61,65].

SHW15 protocol. This protocol aims to achieve an efficient MQKA with single photons and unitary operations. In fact, the qubit efficiency, measurement efficiency and unitary operation efficiency of this protocol are $\frac{1}{(1+kn)n}$, $\frac{1}{(1+kn)n}$ and $\frac{1}{(1+n)n}$, respectively. However, this protocol still cannot be immune to the participant attack[64,65].

HSXLFJY16 protocol. This protocol is presented with single photons, single-particle measurements and unitary operations[67]. Since the eavesdropping detection is needed is each step of the sequence transmission, The qubit efficiency, measurement efficiency and unitary operation efficiency are respectively $\frac{1}{(1+kn)n}$, $\frac{1}{(1+kn)n}$ and $\frac{1}{n^2}$.

CM17 protocol. This protocol is proposed with quantum search algorithm, where entanglement and unitary operations are needed[68]. The qubit efficiency, measurement efficiency and unitary operation efficiency are $\frac{1}{(1+kn)n}$, $\frac{1}{(1+kn)n}$ and $\frac{2}{(n+1)n}$.

Conclusion

In this paper, we focus on improving the efficiency of the travelling-mode MQKA protocol and propose an efficient MQKA protocol with single photons. Security and fairness analysis shows that the proposed protocol is immune to both the external attack and participant attack. By utilizing the ideas of collective eavesdropping, the qubit efficiency and measurement efficiency of this protocol are higher than those of the existing protocols, especially the ones which are also secure and fair. In addition, due to the utilization of single photons and single-particle measurement, the proposed protocol is more feasible with the current technologies than the ones which employ entanglement or multi-particle measurements.

Finally, we should point out that, to design a really practical QKA protocol, one should not only consider the fairness in the quantum exchange process (i.e., the process to generate raw keys), but also propose qualified information reconciliation process and privacy amplification process which can be utilized in QKA protocols for negotiating the final key fairly. How to design a qualified classical postprocessing processes for QKA/MQKA, still remains an open problem, which we would like to research in future.

References

1. Bennett, C. H. & Brassard, G. In: Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India, IEEE Press, New York, pp. 175–179 (1984).
2. Song, T. T., Qin, S. J., Wen, Q. Y., Wang, Y. K. & Jia, H. Y. Finite-key security analyses on passive decoy-state QKD protocols with different unstable sources. *Scientific Reports* **5**, 15276 (2015).
3. Li, H. W. *et al*. Randomness determines practical security of BB84 quantum key distribution. *Scientific Reports* **5**, 16200 (2015).
4. Deng, F. G. & Long, G. L. Controlled order rearrangement encryption for quantum key distribution. *Phys. Rev. A* **68**, 042315 (2003).
5. Song, T. T., Wen, Q. Y., Guo, F. Z. & Tan, X. Q. Finite-key analysis for measurement-device-independent quantum key distribution. *Phys. Rev. A* **86**, 022332 (2012).
6. Sun, Y., Wen, Q. Y., Gao, F. & Zhu, F. C. Robust variations of the Bennett-Brassard 1984 protocol against collective noise. *Phys. Rev. A* **80**, 032321 (2009).
7. Lin, S. & Guo, G. D. Quantum key distribution: defeating collective noise without reducing efficiency. *Quantum. Inf. Comput.* **14**, 845–856 (2014).
8. Gao, F., Qin, S. J., Guo, F. Z. & Wen, Q. Y. Dense-coding attack on three-party quantum key distribution protocols. *IEEE J. Quant. Electron.* **47**, 630–635 (2011).
9. Tan, Y. G. & Cai, Q. Y. Practical decoy state quantum key distribution with finite resource. *European Physical Journal D* **56**, 449–455 (2010).
10. Guo, F. Z., Liu, L., Qin, S. J. & Wen, Q. Y. Round-robin differential-phase-shift quantum key distribution with a passive decoy state method. *Scientific Reports* **7**, 42261 (2017).
11. Shih, H. C., Lee, K. C. & Hwang, T. New efficient three-party quantum key distribution protocols. *IEEE Journal of Selected Topics in Quantum Electronics* **15**, 1602–1606 (2009).
12. Liu, B., Gao, F. & Wen, Q. Y. Single-photon multiparty quantum cryptographic protocols with collective detection. *IEEE J Quant. Electron.* **47**, 1383–1390 (2011).
13. Long, G. L. & Liu, X. S. Theoretically efficient high-capacity quantum-key-distribution scheme. *Phys. Rev. A* **65**, 032302 (2002).
14. 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).
15. Deng, F. G. & Long, G. L. Secure direct communication with a quantum one-time pad. *Phys. Rev. A* **69**, 052319 (2004).
16. 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).
17. Hu, J. Y. *et al*. Experimental quantum secure direct communication with single photons. *Light-Science & Applications* **5**, 16144 (2015).
18. Huang, W., Wen, Q. Y., Jia, H. Y., Qin, S. J. & Gao, F. Fault tolerant quantum secure direct communication with quantum encryption against collective noise. *Chin. Phys. B* **21**, 100308 (2012).
19. Yan, F. L. & Zhang, X. Q. A scheme for secure direct communication using EPR pairs and teleportation. *European Physical Journal B* **41**, 75–78 (2004).
20. Lin, S., Wen, Q. Y. & Zhu, F. C. Quantum secure direct communication with χ-type entangled states. *Phys. Rev. A* **78**, 064304 (2008).
21. Hillery, M., Buzěk, V. & Berthiaume, A. Quantum secret sharing. *Phys. Rev. A* **59**, 1829–1834 (1999).
22. Wang, T. Y., Liu, Y. Z., Wei, C. Y., Cai, X. Q. & Ma, J. F. Security of a kind of quantum secret sharing with entangled states. *Scientific Reports* **7**, 2485 (2017).
23. Yang, Y. H. *et al*. Quantum secret sharing via local operations and classical communication. *Scientific Reports* **5**, 16967 (2015).
24. Yang, Y. G., Teng, Y. W., Chai, H. P. & Wen, Q. Y. Fault-tolerant quantum secret sharing against collective noise. *Phys. Scr.* **83**, 025003 (2011).
25. Song, X. L., Liu, Y. B., Deng, H. Y. & Xiao, Y. G. (t, n) Threshold d-Level Quantum Secret Sharing. *Scientific Reports* **7**, 6366 (2017).
26. Zhang, Z. J., Li, Y. & Man, Z. X. Multiparty quantum secret sharing. *Phys. Rev. A* **71**, 044301 (2005).
27. Gao, F., Liu, B., Wen, Q. Y. & Chen, H. Flexible quantum private queries based on quantum key distribution. *Opt. Express* **20**, 17411 (2012).
28. Gao, F., Liu, B., Huang, W. & Wen, Q. Y. Postprocessing of the Oblivious Key in Quantum Private Query. *IEEE Journal of Selected Topics in Quantum Electronics* **21**, 98–108 (2014).
29. Wei, C. Y., Gao, F., Wen, Q. Y. & Wang, T. Y. Practical quantum private query of blocks based on unbalanced-state Bennett-Brassard-1984 quantum-key-distribution protocol. *Scientific Reports* **4**, 7537 (2014).
30. Liu, B. *et al*. Efficient quantum private comparison employing single photons and collective detection. *Quantum Inf Process* **12**, 887–897 (2012).
31. Shi, R. H., Mu, Y., Zhong, H., Cui, J. & Zhou, S. Two Quantum Protocols for Oblivious Set-member Decision Problem. *Scientific Reports* **5**, 15914 (2015).
32. Tseng, H. Y., Lin, j & Hwang, T. New quantum private comparison protocol using EPR pairs. *Quantum Inf. Process.* **11**, 373–384 (2012).
33. Li, Y. B. *et al*. Information leak in Liu *et al*.'s quantum private comparison and a new protocol. *Eur. Phys. J. D* **66**, 110 (2012).
34. Huang, W. *et al*. Quantum anonymous ranking. *Phys. Rev. A* **89**, 032325 (2014).
35. Wen, X. J. An E-payment system based on quantum group signature. *Phys. Scr.* **82**, 065403–065407 (2010).
36. Yang, Y. G., Xu, P., Yang, R., Zhou, Y. H. & Shi, W. M. Quantum Hash function and its application to privacy amplification in quantum key distribution, pseudo-random number generation and image encryption. *Scientific Reports* **6**, 19788 (2016).
37. Chen, X. B. *et al*. An efficient protocol for the private comparison of equal information based on the triplet entangled state and single-particle measurement. *Opt. Commun.* **283**, 1161–1165 (2009).
38. Wang, Q. L., Zhang, W. W. & Su, Q. Revisiting "The loophole of the improved secure quantum sealed-bid auction with post-confirmation and solution". *Int. J. Theor. Phys.* **53**, 3147–3153 (2014).
39. Wei, C. Y., Gao, F., Wen, Q. Y. & Yue, Q. L. Practical quantum private query of blocks based on unbalanced-state Bennett-Brassard-1984 quantum-key-distribution protocol. *Scientific Reports* **4**, 4537 (2014).
40. Zhou, N. R., Hua, T. X., Wu, G. T., He, C. S. & Zhang, Y. Single-Photon Secure Quantum Dialogue Protocol Without Information Leakage. *Int. J. Theor. Phys.* **53**, 3829–3837 (2014).
41. Wang, Q. L., Yu, C. H., Gao, F., Qi, H. Y. & Wen, Q. Y. Self-tallying Quantum Anonymous Voting. *Phys. Rev. A* **94**, 022333 (2016).
42. Imre, S. & Gyongyosi, L. Advanced Quantum Communications¡ªAn Engineering Approach (Wiley-IEEE Press, Hoboken, New Jersey, 2012).
43. Hanzo, L. *et al*. 2012 Wireless myths, realities, and futures: from 3G/4G to optical and quantum wireless. Proceedings of IEEE **100**, Special Centennial Issue, 1853ÍC1888 (2012).
44. Gyongyosi, L. & Imre, S. SPIE Photonics West OPTO 2014, Advances in Photonics of Quantum Computing, Memory, and Communication VII 8997 89970C (2014).
45. Mraz, A., Imre, S. & Gyongyosi, L. IEEE Signal Processing Conference Proceedings, 2016 24th European Signal Processing Conference (EUSIPCO 2016), section on Quantum Communications Budapest, 29 August-2 September, https://doi.org/10.1109/EUSIPCO.2016.7760298 (2016).
46. Zhou, N., Zeng, G. & Xiong, J. Quantum key agreement protocol. *Electron. Lett.* **40**, 1149 (2004).

47. Hsueh, C. C. & Chen, C. Y. Quantum key agreement protocol with maximally entangled states. In: Proceedings of the 14th Information Security Conference, National Taiwan University of Science and Technology, Taipei, pp. 236–242 (2004).
48. Tsai, C. W. & Hwang, T. On quantum key agreement protocol. Technical Report C-S-I-E, NCKU, Taiwan (2009).
49. Tsai, C. W., Chong, S. K. & Hwang, T. Comment on quantum key agreement protocol with maximally entangled states. In: Proc. IEEE Int. Conf. on the 20th Cryptology and Information Security Conference (2010).
50. Chong, S. K. & Hwang, T. Quantum key agreement protocol based on BB84. *Opt. Commun.* **283**, 1192–1195 (2010).
51. Chong, S. K., Tsai, C. W. & Hwang, T. Improvement on Quantum Key Agreement Protocol with Maximally Entangled States. *Int. J. Theor. Phys.* **50**, 1793–1802 (2011).
52. Huang, W., Wen, Q. Y., Liu, B., Gao, F. & Sun, Y. Quantum key agreement with EPR pairs and single-particle measurements. *Quantum Inf. Process.* **13**, 649–663 (2014).
53. Huang, W., Su, Q., Wu, X., Li, Y. B. & Sun, Y. Quantum key agreement against collective decoherence. *Int. J. Theor. Phys.* **53**, 2891–2901 (2014).
54. He, Y. F. & Ma, W. P. Two-party quantum key agreement protocol with four-particle entangled states. *Modern Physics Letters B* **30**, 1650332 (2016).
55. Shi, R. H. & Zhong, H. Multi-party quantum key agreement with bell states and bell measurements. *Quantum Inf. Process.* **12**, 921–932 (2013).
56. Liu, B., Gao, F., Huang, W. & Wen, Q. Y. Multiparty quantum key agreement with single particles. *Quantum Inf. Process.* **12**, 1797–1805 (2013).
57. Sun, Z. W., Zhang, C., Wang, B. H., Li, Q. & Long, D. Y. Improvements on "multiparty quantum key agreement with single particles". *Quantum Inf. Process.* **12**, 3411–3420 (2013).
58. Huang, W., Wen, Q. Y., Liu, B., Su, Q. & Gao, F. Cryptanalysis of a multi-party quantum key agreement protocol with single particles. *Quantum Inf. Process.* **13**, 1651–1657 (2014).
59. Xu, G. B., Wen, Q. Y., Gao, F. & Qin, S. J. Novel multiparty quantum key agreement protocol with GHZ states. *Quantum Inf. Process.* **13**, 2587 (2014).
60. Sun, Z. W., Yu, J. P. & Wang, P. Efficient multi-party quantum key agreement by cluster states. *Quantum Inf. Process.* **15**, 373–384 (2016).
61. Sun, Z. W. *et al*. Multi-party quantum key agreement by an entangled six-qubit state. *Int. J. Theor. Phys.* **55**, 1920–1929 (2016).
62. Shukla, C., Alam, N. & Pathak, A. Protocols of quantum key agreement solely using Bell states and Bell measurement. *Quantum Inf. Process.* **13**, 2391–2405 (2014).
63. Zhu, Z. C., Hu, A. Q. & Fu, A. M. Improving the security of protocols of quantum key agreement solely using Bell states and Bell measurement. *Quantum Inf. Process.* **14**, 4245–4254 (2015).
64. Sun, Z. W., Huang, J. & Wang, P. Efficient multiparty quantum key agreement protocol based on commutative encryption. *Quantum Inf. Process.* **15**, 2101–2111 (2015).
65. Liu, B., Xiao, D. & Jia, H. Y. Collusive attacks to "circle-type" multi-party quantum key agreement protocols. *Quantum Inf. Process.* **15**, 2113–2124 (2016).
66. Mohajer, R. & Eslami Z. Cryptanalysis of a multiparty quantum key agreement protocol based on commutative encryption. Quantum Inf. Process. https://doi.org/10.1007/s11128-017-1647-2 (2017).
67. Huang, W. *et al*. Improved multiparty quantum key agreement in travelling mode. *Sci. China-Phys. Mech. Astron.* **59**, 120311 (2016).
68. Cao, H. & Ma, W. P. Multiparty Quantum Key Agreement Based on Quantum Search Algorithm. *Scientific Reports.* **7**, 45046 (2017).
69. Laflamme, R. *et al*. Perfect Quantum Error Correcting Code. *Phys. Rew. Lett.* **77**, 198–201 (1996).
70. Zanardi, P. & Rasetti, M. Noiseless Quantum Codes. *Phys. Rew. Lett.* **79**, 3306–3309 (1997).
71. Cai, Q. Y. Eavesdropping on the two-way quantum communication protocols with invisible photons. *Phys. Lett. A* **351**, 23 (2006).
72. Li, X. H., Deng, F. G. & Zhou, H. Y. Improving the security of secure direct communication based on the secret transmitting order of particles. *Phys. Rev. A* **74**, 054302 (2006).
73. Wang, G. M. & Ying, M. S. Unambiguous discrimination among quantum operations. *Phys. Rew. A* **73**, 042301 (2006).
74. Gao, F., Qin, S. J., Wen, Q. Y. & Zhu, F. C. A simple participant attack on the brádler-dušek protocol. *Quant. Inf. Comput.* **7**, 329–334 (2007).

Acknowledgements

This work is supported by National Natural Science Foundation of China (Grant Nos 61771439, 61501414, 61702469, 61602045, 61702061, 11504024, 61502041), National Cryptography Development Fund (Grant No. MMJJ20170120), Sichuan Youth Science and Technology Foundation(Grant No. 2017JQ0045), Foundation of Science and Technology on Communication Security Laboratory (Grant No. 6142103040105).

Author Contributions

W.H. and B.L. designed the protocol and wrote the manuscript. Q.S., Y.-H.H. and B.-J.X. did the analysis and discussion of the proposed protocol. All authors reviewed the manuscript.

Additional Information

Competing Interests: The authors declare that they have no competing interests.

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