SCIENTIFIC REPORTS
natureresearch

OPEN

Efficient travelling-mode quantum key agreement against participant's attacks

Wei-cong Huang, Yong-kai Yang, Dong Jiang* & Li-jun Chen*

Quantum key agreement (QKA) is to negotiate a final key among several participants fairly and securely. In this paper, we show that some existing travelling-mode multiparty QKA protocols are vulnerable to internal participant's attacks. Dishonest participants can exploit a favorable geographical location or collude with other participants to predetermine the final keys without being discovered. To resist such attacks, we propose a new travelling-mode multiparty QKA protocol based on non-orthogonal Bell states. Theoretical analysis shows that the proposed protocol is secure against both external and internal attacks, and can achieve higher efficiency compared with existing travelling-mode multiparty QKA protocols. Finally we design an optical platform for each participant, and show that our proposed protocol is feasible with current technologies.

In 1984, the first quantum cryptographic protocol, known as BB84 quantum key distribution protocol was proposed by Bennett and Brassard[1]. Since its unconditional security is guaranteed by the laws of quantum mechanics, quantum cryptography has become a heated topic, and various protocols including quantum key distribution (QKD)[1,2], quantum secure direct communication (QSDC)[3–9], quantum secret sharing (QSS)[10,11], etc., have been proposed. Recently, Quantum key agreement(QKA), a new branch of quantum cryptography, has attracted extensive attention.

Different from QKD, QKA can fairly and securely negotiate a final key among users. That is, the final key is equally determined by each participant and any non-trivial subset of the participants cannot absolutely predetermine the final key. In 2004, Zhou *et al.* proposed the first QKA protocol by utilizing the quantum teleportation technique[12]. In the same year, Hsueh and Chen proposed another QKA protocol by employing the entangled states[13]. Nevertheless, Tsai *et al.* pointed that neither of the two protocols is secure[14,15]. In 2010, Chong and Hwang devised a QKA protocol based on BB84[16]. However, the above protocols are all based on two-party. To extend QKA to the multi-party case, Shi and Zhong designed the first multiparty QKA (MQKA) protocol based on Bell states in 2013[17]. Since then, many MQKA protocols using single or entanglement quantum states have been proposed[18–34].

Liu[18] pointed out that existing MQKA protocols can be classified into three types according to the transmission topology of quantum photons: complete-graph-type[17,20], circle-type[19,21–34] (also known as travelling-mode) and tree-type[35]. In the first type, every participant sends each of other participants a sequence of photons which carries the information of his/her secret key. In the second type, each participant only sends out one sequence, which will be operated by each of other participants by turns and sent back to the one who prepares it. The third type is one participant generates a sequence of high dimensional photon states (e.g. GHZ states) and sends each of other participants one of its particles. Since the travelling-mode is more efficient than complete-graph-type and easier to satisfy the fairness property compared with the tree-type, it has attracted comprehensive study. In 2013, Sun *et al.* presented a MQKA protocol[19] in travelling-mode to improve the efficiency of Liu *et al*'s MQKA protocol[20]. In 2014, Shukla *et al.* proposed a travelling-mode MQKA protocol based on Bell state and Bell measurements[21]. In 2015, Zhu *et al.* put forward the attack strategy to defeat Shukla *et al*'s protocol and proposed an improved version[22]. In 2018, Abulkasim pointed out that Wang and Ma's protocol[23] is susceptible to participant's attacks and proposed an improved protocol[24]. Meanwhile, Cao and Ma proposed two MQKA protocols which were designed to be immune to the collusive attack[25]; they also presented a MQKA protocol based on non-orthogonal quantum entangled pairs[34]. Besides, some protocols based on higher-dimensional quantum states, such as five-qubit brown states[26], G-Like states[28], and four-qubit symmetric W state[29], were presented.

State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing, 210046, P. R. China. *email: jiangd@nju.edu.cn; chenlj@nju.edu.cn

In these travelling-mode MQKA protocols, we find that some protocols[25–30] cannot resist dishonest participant's attacks, which leads to the failure of fairness property[19]. The dishonest participant can take advantage of a favorable geographical location or collude with other participants to predetermine the final keys of honest participants without being discovered. Besides, we also find there exists the problem of information leakage in Cao-Ma MQKA protocol[34]. Following we take two Cao-Ma MQKA protocols[25,34] as examples to demonstrate the attacks in detail. To resist these attacks, We propose a new MQKA protocol based on non-orthogonal Bell states by utilizing Pauli and rotation operations. Our proposed protocol has three noticeable advantages: Firstly, owing to the use of non-orthogonal Bell states, the proposed protocol can resist attacks from both internal dishonest participants and external eavesdroppers. It also effectively solves the problem of information leakage in Cao-Ma protocol. Secondly, the frequency of eavesdropping detection has been greatly reduced. Hence, the qubit efficiency and measurement efficiency of our proposed protocol are higher than those of the existing secure ones[20,32–34]. Thirdly, since only Bell states and unitary operations are employed, the protocol is feasible with the current technology.

The rest of the paper is organized as follows. Next section first reviews and analyzes the security of Cao-Ma MQKA protocols, then introduces our improved travelling-mode MQKA protocol in detail, followed by the security analysis and efficiency comparisons with existing secure protocols. Furthermore, an optical setup is provided. Finally, a short conclusion of this paper is given in the final section.

Results

Review of Cao-Ma MQKA protocols. In this section we briefly describe the Cao-Ma MQKA protocol 1[25] without trust party and Cao-Ma MQKA protocol 2[34] based on non-orthogonal quantum entangled pairs respectively.

Cao-Ma MQKA protocol 1. The main process of Cao-Ma MQKA protocol without trust party can be divided into two stages. The first stage is initialization and encoding stage. Each participant $P_i(i=0, 1, \ldots, N-1)$ possesses a n-bit 0–1 sequence $\widetilde{K}_i$ and TS_i as his secret key and additional random sequence, and calculates $K_i = \widetilde{K}_i \oplus TS_i$. Then he prepares a sequence of Bell states randomly selected from four Bell states, wherein the states of the photon sequence can be expressed as W_i. Each participant keeps the first photon sequence in his hand and sends the second photon sequence which is inserted into decoy photons to next participant P_{i+1}. P_i and P_{i+1} perform eavesdropping checking. If the communication is secure, P_{i+1} performs one of the four Pauli operations on the received photon sequence according to K_{i+1}. Next, P_{i+1} inserts decoy photons into the photon sequence and sends it to next participant P_{i+2}. This process continues until P_i gets the sequence which he generated. The second stage is final key negotiation stage. After each participant gets the sequence he generates, he performs Bell measurements on corresponding photon pairs. The measurement results of the sequence can be expressed as V_i. Then each participant P_i publishes his random sequence TS_i and calculates $\mathrm{TS} = TS_0 \oplus TS_1 \oplus \ldots \oplus TS_{N-1}$. Finally, each participant can obtain the final common key K_c, where $K_c = TS \oplus W_i \oplus V_i \oplus \widetilde{K}_i$.

Cao-Ma MQKA protocol 2. This protocol is based on non-orthogonal quantum pairs and adopts the idea of Pauli and Hadamard operations mixed encoding. The process is as follows. Firstly, there are eight photon pairs which are in $BS=\{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$ and $DBS=\{H|\phi^-\rangle, H|\phi^+\rangle, H|\psi^-\rangle, H|\psi^+\rangle\}$, and four unitary operations in $U=\{U_{00}, U_{11}, U_{01}, U_{10}\}=\{I, iY, H, iYH\}$, wherein H is Hadamard operation. Each participant $P_i(i=0, 1, \ldots, N-1)$ generates a sequence of classical bits K_i as his private key, wherein $K_i \in \{00, 11, 01, 10\}$. Moreover, P_i also generates a sequence C_i, where C_i is 0 if $K_i \in \{00, 11\}$ and C_i is 1 if $K_i \in \{01, 10\}$. Then each participant P_i prepares a random quantum pair sequence from BS or DBS and transmitted the second photon sequence to the next participant P_{i+1}. After receiving the sequence, P_{i+1} executes the eavesdropping checking and performs unitary operations on the received quantum sequence according to his private key. Until each participant has encoded his private key on the photon sequences of others and receives the sequence he generates, he publishes a classical sequence C_i to reveal the measurement basis and calculates $C=C_1 \oplus C_2 \oplus \ldots \oplus C_N$. Each participant performs BS or DBS measurements on the photon pairs according to C. If C is 0, the measurement basis is the same as the initial state; otherwise, the measurement basis is the dual basis of the initial states. Finally, all participants can extract the common key by comparing the initial states and measurement results.

Security analysis of the Cao-Ma MQKA protocols. In this section, we first show that the dishonest participant in Cao-Ma MQKA protocol 1 can take advantage of a favorable geographical location or collude with other participants to predetermine the final key without being discovered, leading to the failure of fairness property. Next we reveal the problem of information leakage in Cao-Ma MQKA protocol 2.

Fairness analysis. In travelling-mode MQKA protocols, participants encode their secret keys on photons by performing the unitary operations. Besides, they usually perform additional random operations on photons in case to divulge the secret keys. Therefore, once the additional operation is obtained, the participant will deduce the final key directly. Following we take the tripartite (Alice, Bob and Charlie) example to introduce the attack strategy. Suppose Bob is a dishonest participant, his detailed attack process is as follows.

(1) Before Alice and Bob publish the random sequence TS_A and TS_C, Bob selects an advantageous geographical position aside Alice and Charlie so that he can get TS_A and TS_C earlier than expected.
(2) Once Bob gets the sequence, he calculates the final key $K = TS_A \oplus TS_C \oplus \widetilde{K}_B \oplus W_B \oplus V_B$ and $M=K \oplus K'$, where K' is the final key he excepts.
(3) Then Bob informs Alice and Charlie of $TS'_B=M \oplus TS_B$. Thus, Alice and Charlie will get the illegal final keys $K_A=\widetilde{K}_A \oplus TS'_B \oplus TS_C \oplus W_A \oplus V_A=K'$ and $K_C=\widetilde{K}_C \oplus TS'_B \oplus TS_A \oplus W_C \oplus V_C=K'$ as Bob anticipates.

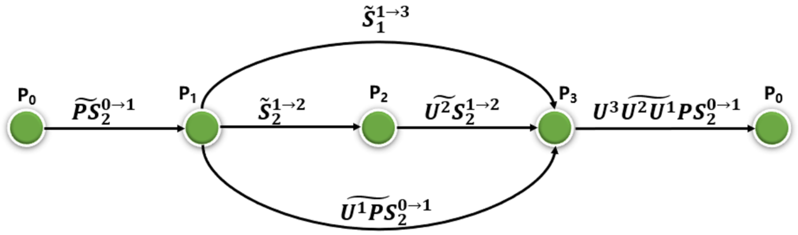
$\tilde{S}_1^{1\to3}$
P_0
$\widetilde{PS}_2^{0\to1}$
P_1
$\tilde{S}_2^{1\to2}$
P_2
$\widetilde{U^2S}_2^{1\to2}$
P_3
$U^3\widetilde{U^2U^1PS}_2^{0\to1}$
P_0
$\widetilde{U^1PS}_2^{0\to1}$

Figure 1. Dishonest participants' collusive attack strategy. P_1 and P_3 collude to eavesdrop on the honest participant P_2's secret key.

Initial State	$\widetilde{K}_2 \oplus$ TS	Final State
$\|\phi^+\rangle$	$00 \oplus 00$	$\|\phi^+\rangle$
	$11 \oplus 11$	
	$01 \oplus 01$	
	$10 \oplus 10$	
$\|\phi^+\rangle$	$00 \oplus 11$	$\|\phi^-\rangle$
	$11 \oplus 00$	
	$01 \oplus 10$	
	$10 \oplus 01$	
$\|\phi^+\rangle$	$00 \oplus 01$	$\|\psi^+\rangle$
	$11 \oplus 10$	
	$01 \oplus 00$	
	$10 \oplus 11$	
$\|\phi^+\rangle$	$00 \oplus 10$	$\|\psi^-\rangle$
	$11 \oplus 01$	
	$01 \oplus 11$	
	$10 \oplus 00$	

Table 1. Relationship between P_1's photon states, P_2's operations and P_3's measurement results.

Through the above operations, Bob can determine the final keys of Alice and Charlie. Following, we will analyze the collusion attack in detail. For clarity, we assume that four participants P_0, P_1, P_2 and P_3 want to generate the final key. P_1 and P_3 are dishonest and want to steal P_2's secret key. The detailed attack process is as follows:

(1) P_0 prepares a sequence of Bell states $|PS_1{}^0PS_2{}^0\rangle$, then he transmits the second photon sequence $|PS_2{}^0\rangle$ with decoy photons $|\widetilde{PS}_2{}^{0\to1}\rangle s$ to P_1.
(2) P_1 performs unitary operations on the received photons according to his secret key and sends the sequence $|\widetilde{U^1PS}_2{}^{0\to1}\rangle$ to P_3 instead of P_2 as illustrated in Fig. 1. Meanwhile, P_1 prepares a fake sequence of Bell states $|S_1{}^1S_2{}^1\rangle$ and sends the first photon sequence $|\tilde{S}_1{}^{1\to3}\rangle$ to P_3 and the second photon sequence $|\tilde{S}_2{}^{1\to2}\rangle$ to P_2.
(3) After security checking, as P_2 does not know the received photon sequence is fake, he encodes the sequence by performing unitary operations according to TS_2 and sends the sequence $|\widetilde{U^2S}_2{}^{1\to2}\rangle$ to P_3.
(4) After confirming P_3 has received the sequence $|\widetilde{U^2S}_2{}^{1\to2}\rangle$, P_2 and P_3 execute eavesdropping checking. If the communication is secure, P_1 and P_3 will perform Bell measurement on $|S_1{}^{1\to3}\rangle$ and $|U^2S_2{}^{1\to2}\rangle$. Then they can get P_2's unitary operations, i.e., $\widetilde{K}_2 \oplus TS$, by comparing the measurement results and initial states.
(5) P_3 encodes photon sequence $|U^1PS_2{}^{0\to1}\rangle$ with P_2's unitary operations and his unitary operations. P_3 also generates some decoy photons and inserts them in to $|U^3U^2U^1PS_2{}^{0\to1}\rangle$ randomly. Then he sends the sequence to P_0.
(6) P_1 and P_3 wait for the common key negotiation stage, where every participant publishes his TS_i. By comparing P_2's unitary operations and TS_2, P_1 and P_3 can effortlessly recover $\widetilde{K}_2$. For example, suppose the fake photon pairs prepared by P_1 is $|\phi^+\rangle$, and the result of Bell measurement by P_1 and P_3 is $|\phi^+\rangle$ after P_2's encoding, they can deduce the operation performed by P_2 is U_{00}. Assume the TS_2 published by P_2 is 01, P_1 and P_3 can definitely deduce the P_2's secret key is 01 according to Table 1. Then P_1 and P_3 can determine P_2's final key by announcing fake TS_1 and TS_3.

In addition to the Cao-Ma protocol 1, these agreements[26–30] are also vulnerable to dishonest participants' collusion attack, where indicates the protocols cannot satisfy the fairness property.

State	$\|BS_{00}\rangle$	$\|BS_{01}\rangle$	$\|BS_{10}\rangle$	$\|BS_{11}\rangle$
Operation				
I	$\|BS_{00}\rangle$	$\|BS_{01}\rangle$	$\|BS_{10}\rangle$	$\|BS_{11}\rangle$
Z	$\|BS_{01}\rangle$	$\|BS_{00}\rangle$	$\|BS_{11}\rangle$	$\|BS_{10}\rangle$
R_zI	$\|DBS_{00}\rangle$	$\|DBS_{01}\rangle$	$\|DBS_{10}\rangle$	$\|DBS_{11}\rangle$
R_zZ	$\|DBS_{01}\rangle$	$\|DBS_{00}\rangle$	$\|DBS_{11}\rangle$	$\|DBS_{10}\rangle$

Table 2. Effects of unitary operations $\{I, Z, R_zI, R_zZ\}$ on the second particles of Bell states $|\mathrm{BS}\rangle$.

Information leakage analysis. Information leakage is that Eve can extract some information about secret key without any active attack[36]. In Cao-Ma MQKA protocol 2, each participant P_i needs to publish a classical sequence C_i after he receives the sequence he generates. However, C_i and K_i are closely related. If C_i is 0, Eve can draw a conclusion that the secret key of P_i must be 00 or 11; otherwise, the K_i is 01 or 10, which contains $-2 \times \frac{1}{2}\, log_2 \frac{1}{2} = 1$ bit of information. Thus, one bit of the secret information is leaked to Eve unconsciously.

The improved travelling-mode MQKA protocol.

Herein we design a new travelling-mode MQKA protocol based on non-orthogonal Bell states, where n participants negotiate a final key fairly and securely. The detailed process of our protocol is as follows:

Initialization phase. Each participant P_i first generates a $(l+kl)$-bit 0–1 secret key sequence $K_i=\{K_{i,1}, K_{i,2}, \ldots, K_{i,m}\}$, $m \in \{1, 2, \ldots, l+kl\}$. Besides he also generates a random $(l+kl)$-bit 0–1 controlling string RH_i^j, where k is the detection rate, i, j $\in \{1, 2, \ldots, n\}$ and i $\neq$ j. Then P_i prepares a sequence $BS_i=\{|BS_{wi,1\;wi,2}{}^{i}\rangle, |BS_{wi,3\;wi,4}{}^{i}\rangle, \ldots, |BS_{wi,2(l+kl)-1\;wi,2(l+kl)}{}^{i}\rangle\}$ of $l+kl$ Bell states, where $|BS_{wi,2m-1\;wi,2m}{}^{i}\rangle \in \{|BS_{00}\rangle, |BS_{01}\rangle, |BS_{10}\rangle, |BS_{11}\rangle\}$ and $W_i=(w_{i,1}, w_{i,2}, \ldots, w_{i,2(l+kl)-1}, w_{i,2(l+kl)})$ is a random $2(l+kl)$-bit 0–1 sequence.

$$
\begin{aligned}
|BS_{00}\rangle &= |\phi^{+}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |BS_{01}\rangle = |\phi^{-}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle),\\
|BS_{10}\rangle &= |\psi^{+}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad |BS_{11}\rangle = |\psi^{-}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).
\end{aligned}
\tag{1}
$$

Sending photons. P_i divides BS_i into two single photon sequence: the first photon sequence $|BS_1{}^{i\to i}\rangle$ and the second photon sequence $|BS_2{}^{i\to i+1}\rangle$ (symbol '+' in $i+1$ denotes the additional mod n). Then P_i keeps the first photon sequence in home and transmits the second photon sequence to the next participant P_{i+1}.

Encoding phase. After P_{i+1} receives the photon sequence, he performs unitary operation I or Z on $|BS_2{}^{i\to i+1}\rangle$ according to his private key sequence, where $I=|0\rangle\langle 0|+|1\rangle\langle 1|$ and $Z=|0\rangle\langle 0|-|1\rangle\langle 1|$.

Controlling operations. Depending on whether the sequence $RH_{i+1}{}^{i}$ is 1 or 0, P_{i+1} performs rotation operation $R_z\left(\frac{\pi}{2}\right)$ on the sequence $|BS_2{}^{i\to i+1}\rangle$ or does nothing, where $R_z\left(\frac{\pi}{2}\right)$ is the rotation operator of the z axis and the definition is as follows:

$$
R_z\left(\frac{\pi}{2}\right) = \frac{\sqrt{2}}{2}I - \frac{\sqrt{2}}{2}iZ = \begin{bmatrix} \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i & 0 \\ 0 & \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \end{bmatrix}
\tag{2}
$$

The rotation operator can change the state of the $|BS\rangle$ to $|DBS\rangle=\{|DBS_{00}\rangle, |DBS_{01}\rangle, |DBS_{10}\rangle, |DBS_{11}\rangle\}$, where $|DBS\rangle$ are defined as follows. Table 2 shows the relationship of the unitary operations and the transformed Bell states.

$$
\begin{aligned}
|DBS_{00}\rangle &= R_z\left(\frac{\pi}{2}\right)|\phi^{+}\rangle = \frac{1}{\sqrt{2}}(|\phi^{+}\rangle - i|\phi^{-}\rangle),\\
|DBS_{01}\rangle &= R_z\left(\frac{\pi}{2}\right)|\phi^{-}\rangle = \frac{1}{\sqrt{2}}(|\phi^{-}\rangle - i|\phi^{+}\rangle),\\
|DBS_{10}\rangle &= R_z\left(\frac{\pi}{2}\right)|\psi^{+}\rangle = \frac{1}{\sqrt{2}}(|\psi^{+}\rangle + i|\psi^{-}\rangle),\\
|DBS_{11}\rangle &= R_z\left(\frac{\pi}{2}\right)|\psi^{-}\rangle = \frac{1}{\sqrt{2}}(|\psi^{-}\rangle + i|\psi^{+}\rangle).
\end{aligned}
\tag{3}
$$

After performing the extra unitary operation, P_{i+1} sends the sequence $|BS_2{}^{i\to i+2}\rangle$ to the next participant P_{i+2}. Meanwhile, each of the other $n-1$ participants processes his received sequence just in the same way and sends the obtained new sequence to next participant. This process continues until P_i receives the sequence which he generated from P_{i-1}.

Security checking. Once receiving his own sequence, each participant P_i announces the fact, confirms other participants have received their sequences and informs participant *j* of his controlling sequence RH_i^j. Then all participants cooperate to choose *kl* positions from $l+kl$ Bell states for security checking, and the remaining *l* Bell states are used to form the final key, i.e., K_i', i = 1, 2, 3, …, n. Specifically, P_i randomly selects $\frac{kl}{n}$ positions from the remaining $(l+kl)-(i-1)\frac{kl}{n}$ positions and announces the positional information. After finishing selection, each participant publishes the secret key sequence at the *kl* positions. Then they calculate the *XOR* results of other participants' secret keys, offset the extra controlling operations according to RH_j^i (the detailed process is shown in the next step) and perform Bell measurements on the photon pairs at their chosen $\frac{kl}{n}$ positions. If the measurements are consistent with the calculations, they drop the *kl* bits used for security checking and continue; otherwise they terminate the protocol.

Secret extraction. Each participant P_i offsets the controlling operations for the remaining *l* positions according to RH_j^i. Concretely, since $R_z\left(\frac{\pi}{2}\right)$ commutes with each of the encoding operations {*I*, *Z*}, we can deduce that $R_z\left(\frac{\pi}{2}\right)I = IR_z\left(\frac{\pi}{2}\right)$ and $R_z\left(\frac{\pi}{2}\right)Z = ZR_z\left(\frac{\pi}{2}\right)$. Therefore, each participant P_i can offset all controlling operations $R_z\left(\frac{\pi}{2}\right)$ by repeating C_i^j operations $R_z\left(\frac{\pi}{2}\right)^{\dagger}$ (i.e., by performing once operation $R_z\left(\frac{-C_i^j\pi}{2}\right)$) on the j-th pair of photons in sequence BS_i after all the participants have completed their encoding operations *E* and controlling operations *C* in turn: $CECECE = CCCEEE$, where C_i^j is the j-th bit of the sequence C_i ($C_i = RH_{i+1}{}^i + RH_{i+2}{}^i + \ldots + RH_{i-1}{}^i$), $R_z\left(\frac{\pi}{2}\right)^{\dagger} = \left(R_z\left(\frac{\pi}{2}\right)^T\right)^*$ and $R_z\left(\frac{\pi}{2}\right)^{\dagger}R_z\left(\frac{\pi}{2}\right) = I$. After that, each participant performs Bell measurements on the *l* processed photon pairs and obtains $\overline{K'_i} = K'_{i+1} \oplus K'_{i+2} \oplus \ldots \oplus K'_{i-1}$. Finally P_i can get the final key $K = K'_i \oplus \overline{K'_i}$.

So far, we have demonstrated our proposed travelling-mode MQKA protocol. In the real scenario, the raw keys may have very few mistakes which are caused by the channel noise. We can use the multiparty cascade error-correcting protocols for information reconciliation[37,38] and utilize the universal hashing to realize privacy amplification process[39].

Security analysis.

Herein we give a detailed security analysis for both outside and participant's attacks. It is proved that the proposed protocol can satisfy the fairness property effectively. We also show the problem of information leakage does not exist in our protocol.

Outside Attacks. Suppose Eve wants to eavesdrop the final key, he should obtain each participant's private key first. Here are three mainstream attack methods he may take.

Firstly, let us discuss the intercept-resend attack[25,35]. In intercept-resend attack, Eve intercepts and stores the photon sequences sent from participant P_i to P_{i+1}. Then he sends the second photon sequence of the fake Bell states which he prepared in advance to P_{i+1}. After step (3) and (4), P_{i+1} finishes performing his unitary operations and extra controlling operations on the photon sequence and sends to P_{i+2}. At this time Eve will intercept the photon sequence again and sends the original photon sequence to P_{i+2}. Since Eve does not know whether P_{i+1} performs the controlling operation $R_z\left(\frac{\pi}{2}\right)$ on the photons or not, he won't perform Bell measurements on his photon sequence until each participant publishes the random controlling sequence. Therefore he cannot deduce P_{i+1}'s operations and encode correct information on the original sequence. Eve will be detected with the probability $1-\left(\frac{1}{2}\right)^{kl} \approx 1$ (*kl* is big enough) when all participants perform security checking in step (5). Hence the proposed protocol can resist the intercept-resend attack.

Secondly, let us discuss the entangle-measure attack[35,40]. In entangle-measure attack, Eve wants to steal P_{i+1}'s secret key by intercepting the traveling photon sequence $|BS_2{}^{i\rightarrow i+1}\rangle$ and $|BS_2{}^{i\rightarrow i+2}\rangle$, and executing Controlled-not operation on it and his auxiliary photon $|0\rangle_e$, where intercepted photon is a control bit and photon $|0\rangle_e$ is a target bit. For instance, the Bell state prepared by P_i is $|\Psi_1\rangle_{pq} = \frac{1}{\sqrt{2}}|00\rangle + |11\rangle s$. After Eve's operation on *q* and *e*, the entangled state will transform to $|\Psi_2\rangle_{pqe} = \frac{1}{\sqrt{2}}|000\rangle + |111\rangle$, which is composed of three entangled particles. Then Eve sends the particle *q* to P_{i+1}. After P_{i+1} performs unitary operations on the sequence and sends to P_{i+2}, Eve intercepts the particle *q*, performs Controlled-not operation on *q* and *e* again and sends *q* to P_{i+2}. After all participants have received their sequences, they start to announce the controlling sequence RH_i^j and offset the extra controlling operations on the checking photons. The states can be defined as follows:

$$\begin{aligned} U_{CNOT}(q\otimes e)I_q|\Psi_2\rangle_{pqe} &= |\phi^+\rangle_{pq}|0\rangle_e, \\ U_{CNOT}(q\otimes e)Z_q|\Psi_2\rangle_{pqe} &= |\phi^-\rangle_{pq}|0\rangle_e, \\ R_q^{\dagger}U_{CNOT}(q\otimes e)R_qI_q|\Psi_2\rangle_{pqe} &= |\phi^+\rangle_{pq}|0\rangle_e, \\ R_q^{\dagger}U_{CNOT}(q\otimes e)R_qZ_q|\Psi_2\rangle_{pqe} &= |\phi^-\rangle_{pq}|0\rangle_e. \end{aligned} \tag{4}$$

According to the Eq. (4), the state of auxiliary photon *e* is always $|0\rangle_e$ whether P_{i+1}'s operation is *I*, *Z*, R_zI or R_zZ. Therefore Eve cannot obtain P_{i+1}'s secret key even if the photon *e* is entangled with transmitted photons sequence. We can consider that the Entangle-Measure attack is inefficient.

Thirdly, let us discuss the trojan horse attack. The trojan horse attack is another common attack in travelling-mode MQKA protocols which have been discussed in Li *et al*'s protocol[41]. To prevent this type of attack, participant can install some special quantum optical devices to detect the attack, such as the wavelength

Protocol	η_q	η_m	η_u	Quantum resource	Category
LGHW13	$\frac{1}{n(n-1)(1+k)}$	$\frac{1}{n(n-1)(1+k)}$	0	Single photons	Complete-graph
HSXL16	$\frac{1}{n(1+kn)}$	$\frac{1}{n(1+kn)}$	$\frac{1}{n^2}$	Single photons	Circle
CM17	$\frac{1}{n(1+kn)}$	$\frac{1}{n(1+kn)}$	$\frac{2}{n(n+1)}$	Two particles	Circle
*HSL*17	$\frac{1}{n(1+k)}$	$\frac{1}{n(1+k)}$	$\frac{1}{n^2(1+k)}$	Single photons	Circle
Ours	$\frac{1}{n(1+k)}$	$\frac{1}{n\left(1+\frac{k}{n}\right)}$	$\frac{1}{n^2(1+k)}$	Bell states	Circle

Table 3. Comparison between existing security protocols. η_q, η_m and η_u are qubit efficiency, measurement efficiency and unitary operation efficiency, respectively.

quantum filter to filter invisible photons and the photon number splitter(PNS) to discover the delay photons. If the multi-photon rate is unreasonable high, then such attack can be detected.

Fairness Analysis. The dishonest participants pose a greater threat to the security of the protocol than outside eavesdroppers. As we mentioned above, the dishonest participant can take the advantage position or collaborate with others to predetermine the final key. Following we conduct a fairness analysis to show that our protocol can resist participant's attacks.

Let's discuss the first attack strategy. For the sake of convenience, we suppose there are only three participants Alice, Bob and Charlie, wherein Bob is dishonest. In step (5), Bob selects an advantageous geographical position aside Alice and Charlie so he can obtain Alice's and Charlie's controlling sequence RH_i^j earlier than expected. According to the controlling sequences, Bob can perform the operations $R_z\left(\frac{-C_i^j\pi}{2}\right)$ to remove the additional controlling operations and perform Bell measurements to obtain the final key in advance. Then Bob wants to predetermine the final keys of Alice and Charlie by announcing incorrect controlling sequences to them. However, we request that each participant first announces the controlling sequence before they cooperate to choose photons for security checking, so this ineluctably leads to the photon pairs for security checking in DBS basis being measured in BS basis and collapsing randomly into one of the four Bell states. Suppose the number of final keys which Bob wants to change is m, there is a $\frac{kl}{l+kl}$ probability that the selected photons are for security checking since bob cannot unambiguously distinguish the photons for security checking and for final keys. The probability that Bob will successfully pass the security checking is $\left(\frac{1}{2}\right)^{\frac{klm}{l+kl}}=\left(\frac{1}{2}\right)^{\frac{km}{1+k}}\approx 0$ and predetermine the final key is $\left(\frac{1}{2}\right)^{\frac{lm}{l+kl}}=\left(\frac{1}{2}\right)^{\frac{m}{1+k}}\approx 0$ according to Table 2 (if the number m is large enough). So the dishonest participant cannot predetermine the final keys of honest participants and the protocol can achieve fairness property.

Following we analyze the collusive attack. The worst case is that only one participant is honest and all others are dishonest. Let's take three participants P_1, P_2 and P_3 for example, where P_1 and P_3 are dishonest. They want to predetermine P_2's final key. The detailed attack strategies are as follows. P_1 prepares Bell states and sends the photon sequence $|BS_2{}^{1\to 2}\rangle$ to P_2. After P_2 completes his operations on the photon sequence $|BS_2{}^{1\to 2}\rangle$ and sends the sequence $|BS_2{}^{1\to 3}\rangle$ to P_3, P_1 and P_3 won't measure the Bell states until step (5) where each participant publishes their additional controlling sequences. After obtaining P_2's controlling sequence $RH_2{}^1$, P_1 and P_3 can deduce P_2's secret key K_2. However, the only method for P_1 and P_3 to determine the final key of P_2 is to announce fake controlling sequences to him. Based on the analysis of the first participant's attack strategy, we can conclude the probability they will successfully pass the security checking and predetermine P_2's final key is close to 0. Therefore $n-1$ dishonest participants cannot determine the final key. In summary, our proposed protocol can resist participant's attacks.

Information leakage analysis. In addition to the above attacks, information leakage should also be considered. In our protocol, only the controlling string RH_i^j needs to be published in stage (5). Since RH_i^j has nothing to do with the secret key, Eve can only guess that the operation performed by each participant is either I or Z, which contains $-2\times\frac{1}{2}\log_2\frac{1}{2}=1$ bit of uncertain information for Eve. As a result, Eve cannot obtain any information of secret key without taking any active attacks. The problem of information leakage does not exist in our agreement.

Efficiency analysis. Following we compare the proposed MQKA protocol with the existing four secure protocols, i.e., LGHW13 protocol[20], HSXL16 protocol[33], CM17 protocol[34] and HSL17 protocol[32], in five aspects: qubit efficiency η_q, measurement efficiency η_m, unitary operation efficiency η_u, quantum resource and category of the protocol. The definitions are as follows: qubit efficiency $\eta_q=\frac{l}{q}$, measurement efficiency $\eta_m=\frac{l}{m}$, and unitary operation efficiency $\eta_u=\frac{l}{u}$, where l denotes the length of the final common key, q is the number of the transmitted qubits on the quantum channel, m is the number of quantum measurements, and u is the number of unitary operations. Table 3 shows the detailed comparison results between these four MQKA protocols and ours. The efficiency analysis is given as follows.

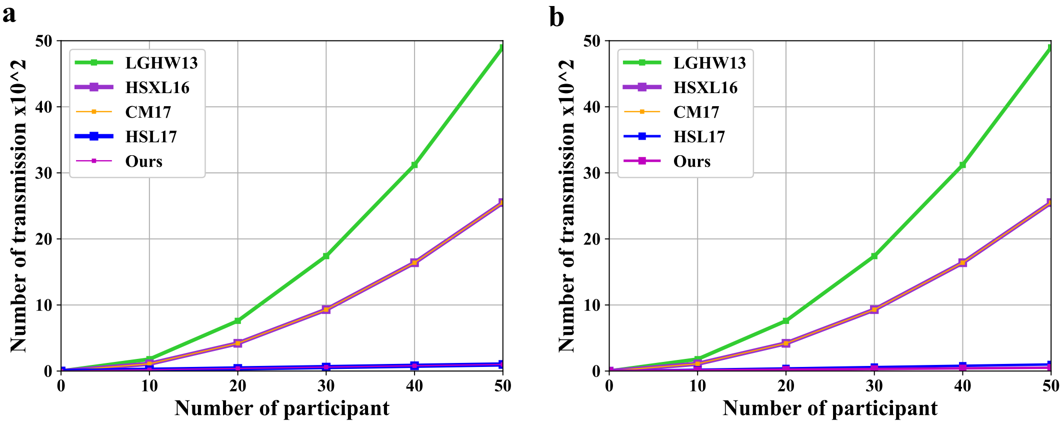

Figure 2. The comparisons of the number of transmissions and measurements, where k = 1.

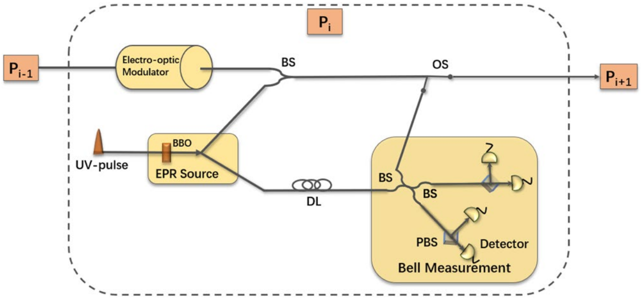

Figure 3. Experimental setup of participants. BBO: beta barium borate. BS: beam splitter. OS: optical switch. DL: delay line. PBS: polarization beam splitter. Each participant can generate and measure the polarization-entangled photon pairs, encode the received photon sequence and send the photon sequence to next participant.

In our protocol, each participant will prepare $l + kl$ photon pairs to establish l-bit final key, wherein kl bits are used for security detection. As there are only half photon sequence transmitted in the quantum channel and n participants involved in our protocol, the total number of transmitted photons on the quantum channel is $n(l + kl)$. Hence, the qubit efficiency is

$$\frac{l}{n(l+kl)} = \frac{1}{n(1+k)}. \tag{5}$$

Since only one eavesdropping detection for each participant, the number of measurements required in this protocol is greatly reduced. To establish an l-bit final key, each participant needs to perform $l + \frac{kl}{n}$ measurements. Therefore, the measurement efficiency of our protocol is

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

The security of our protocol is mainly based on the controlling operations of each participant on the photon sequences. To establish an l-bit final key, each participant needs perform $n(l + kl)$ unitary operations. Thus, the unitary operation efficiency of the proposed protocol is

$$\frac{l}{n^2(l+kl)} = \frac{1}{n^2(1+k)}. \tag{7}$$

The specific comparison results are shown in Fig. 2. As shown in the two subgraphs (a) and (b), the qubit efficiency of the improved protocol is no less than that of the existing security protocols, and it has higher measurement efficiency. Although we increase the number of unitary operations in exchange for higher qubit efficiency and measurement efficiency, the unitary operations can be easily realized with the rapid development of quantum technology. Therefore our protocol is efficient and feasible.

Optical setup. As shown in Fig. 3, we design an optical setup for each participant. In the experiment, ultraviolet (UV) laser pulses pass through a BBO crystal to produce polarization-entangled photon pairs[42]. One of the photon pairs can be first stored in P_ic delay line and the other is sent to P_{i+1}. P_i encodes his secret key and controlling information on other participant's photon sequence by utilizing electro-optic modulator[43] and sends the photon sequence to next participant P_{i+1}. This process continues until P_i receives the sequence which he generates. After offsetting the extra controlling operations on his second photon sequence by utilizing electro-optic modulator, P_i fetches the first photon sequence from the delay line and performs Bell measurement[42] on the photon pairs. According to the measurement results and initial states, all participants can obtain the consistent final key.

Conclusion

In this paper, we find that some existing travelling-mode MQKA protocols are generally vulnerable to the internal dishonest participants. Besides, we also find the problem of information leakage in Cao-Ma MQKA protocol. Then We take Cao-Ma MQKA protocols as examples to illustrate these attacks in detail. To resist the attacks, we propose a robust travelling-mode MQKA protocol based on non-orthogonal Bell states. The analyses show that our protocol can resist the both outside and participant's attacks and achieve higher efficiency. Finally, We design an optical platform for each participant, and show that our proposed protocol can be realized with feasible technologies.

Received: 27 June 2019; Accepted: 27 September 2019;
Published online: 11 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. Lo, H. K., Ma, X. F. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).
3. Long, G. L. & Liu, X. S. Theoretically efficient high-capacity quantum-key-distribution scheme. *Phys. Rev. A* **65**, 032302 (2002).
4. 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).
5. Deng, F. G. & Long, G. L. Secure direct communication with a quantum one-time pad. *Phys. Rev. A* **69**, 052319 (2004).
6. Zhang, W. *et al.* Quantum secure direct communication with quantum memory. *Phys. Rev. Lett.* **118**, 220501 (2017).
7. Zhu, F., Zhang, W., Sheng, Y. B. & Huang, Y. Experimental long-distance quantum secure direct communication. *Sci. Bull.* **62**, 1519–1524 (2017).
8. Chen, S. S., Zhou, L., Zhong, W. & Sheng, Y. B. Three-step three-party quantum secure direct communication. *Sci. China Physics, Mech. & Astron.* **61**, 90312 (2018).
9. Wu, F. *et al.* High-capacity quantum secure direct communication with two-photon six-qubit hyperentangled states. *Sci. China Physics, Mech. & Astron.* **60**, 120313 (2017).
10. Hillery, M., Bužek, V. & Berthiaume, A. Quantum secret sharing. *Phys. Rev. A* **59**, 1829 (1999).
11. Zhang, Z., Li, Y. & Man, Z. Multiparty quantum secret sharing. *Phys. Rev. A* **71**, 044301 (2005).
12. Zhou, N., Zeng, G. & Xiong, J. Quantum key agreement protocol. *Electron. Lett.* **40**, 1149–1150 (2004).
13. Hsueh, C. & Chen, C. Quantum key agreement protocol with maximally entangled states. In *Proceedings of the 14th Information Security Conference (ISC 2004)*, 236–242 (2004).
14. Tsai, C. W. & Hwang, T. On quantum key agreement protocol. *Tech. Rep*. (2009).
15. Tsai, C. W., Chong, S. K. & Hwang, T. Comment on "quantum key agreement protocol with maximally entangled states". In *Proceedings of the 20th Cryptology and Information Security*, 47–49 (2010).
16. Chong, S. K. & Hwang, T. Quantum key agreement protocol based on bb84. *Opt. Commun.* **283**, 1192–1195 (2010).
17. Shi, R. H. & Zhong, H. Multi-party quantum key agreement with bell states and bell measurements. *Quantum Inf. Process.* **12**, 921–932 (2013).
18. Liu, B., Xiao, D., Jia, H. Y. & Liu, R. Z. Collusive attacks to circle-type multi-party quantum key agreement protocols. *Quantum Inf. Process.* **15**, 2113–2124 (2016).
19. Sun, Z., Zhang, C., Wang, B., Li, Q. & Long, D. Improvements on multiparty quantum key agreement with single particles. *Quantum Inf. Process.* **12**, 3411–3420 (2013).
20. Liu, B., Gao, F., Huang, W. & Wen, Q. Y. Multiparty quantum key agreement with single particles. *Quantum Inf. Process.* **12**, 1797–1805 (2013).
21. 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).
22. 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).
23. Wang, L. & Ma, W. Quantum key agreement protocols with single photon in both polarization and spatial-mode degrees of freedom. *Quantum Inf. Process.* **16**, 130 (2017).
24. Abulkasim, H. *et al.* Improving the security of quantum key agreement protocols with single photon in both polarization and spatial-mode degrees of freedom. *Quantum Inf. Process.* **17**, 316 (2018).
25. Cao, H. & Ma, W. Multi-party traveling-mode quantum key agreement protocols immune to collusive attack. *Quantum Inf. Process.* **17**, 219 (2018).
26. Cai, T., Jiang, M. & Cao, G. Multi-party quantum key agreement with five-qubit brown states. *Quantum Inf. Process.* **17**, 103 (2018).
27. Cao, H. & Ma, W. Efficient multi-party quantum key agreement protocol based on nonorthogonal quantum entangled pairs. *Laser Phys. Lett.* **15**, 095201 (2018).
28. Min, S. Q., Chen, H. Y. & Gong, L. H. Novel multi-party quantum key agreement protocol with g-like states and bell states. *Int. J. Theor. Phys.* **57**, 1811–1822 (2018).
29. Wang, S. S., Xu, G. B., Liang, X. Q. & Wu, Y. L. Multiparty quantum key agreement with four-qubit symmetric w state. *Int. J. Theor. Phys.* **57**, 3716–3726 (2018).
30. Yin, X. R. & Ma, W. P. Multiparty quantum key agreement based on three-photon entanglement with unidirectional qubit transmission. *Int. J. Theor. Phys.* **58**, 631–638 (2019).
31. Zhao, X. Q., Zhou, N. R., Chen, H. Y. & Gong, L. H. Multiparty quantum key agreement protocol with entanglement swapping. *Int. J. Theor. Phys.* **58**, 436–450 (2019).
32. Huang, W. *et al.* Efficient multiparty quantum key agreement with collective detection. *Sci. reports* **7**, 15264 (2017).

33. Huang, W. *et al*. Improved multiparty quantum key agreement in travelling mode. *Sci. China Physics, Mech. & Astron.* **59**, 120311 (2016).
34. Cao, H. & Ma, W. Multiparty quantum key agreement based on quantum search algorithm. *Sci. reports* **7**, 45046 (2017).
35. Gu, J. & Hwang, T. Improvement of novel multiparty quantum key agreement protocol with ghz states. *Int. J. Theor. Phys.* **56**, 3108–3116 (2017).
36. Gao, F., Guo, F., Wen, Q. & Zhu, F. Revisiting the security of quantum dialogue and bidirectional quantum secure direct communication. *Sci. China Ser. G: Physics, Mech. Astron.* **51**, 559–566 (2008).
37. Chen, R. K., Zhang, Y. Y., Shi, J. H. & Li, F. G. A multiparty error-correcting method for quantum secret sharing. *Quantum Inf. Process.* **13**, 21–31 (2014).
38. Laflamme, R., Miquel, C., Paz, J. P. & Zurek, W. H. Perfect quantum error correcting code. *Phys. Rev. Lett.* **77**, 198 (1996).
39. Deutsch, D. *et al*. Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Phys. Rev. Lett.* **77**, 2818 (1996).
40. Nguyen, B. A. Quantum exam. *Phys. Lett. A* **350**, 174–178 (2006).
41. 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).
42. Mattle, K., Weinfurter, H., Kwiat, P. G. & Zeilinger, A. Dense coding in experimental quantum communication. *Phys. Rev. Lett.* **76**, 4656 (1996).
43. Weihs, G., Jennewein, T., Simon, C., Weinfurter, H. & Zeilinger, A. Violation of bell's inequality under strict Einstein locality conditions. *Phys. Rev. Lett.* **81**, 5039 (1998).

Acknowledgements

This research is financially supported by the National Key Research and Development Program of China (NO. 2017YFA0303700), the Major Program of National Natural Science Foundation of China (No. 11690030, 11690032), the National Natural Science Foundation of China (No. 61771236), and the Excellence Research Program of Nanjing University.

Author contributions

W. Huang designed the scheme and wrote the manuscript under the guidance of D. Jiang and L. Chen. W. Huang, Y. Yang and D. Jiang carried out the theoretical analysis. All authors reviewed the manuscript.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to D.J. or L.-j.C.

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.