Quantum Information Processing (2018) 17:316
https://doi.org/10.1007/s11128-018-2091-7

Improving the security of quantum key agreement protocols with single photon in both polarization and spatial-mode degrees of freedom

Hussein Abulkasim[1,2] · **Ahmed Farouk**[3] · **Hanan Alsuqaih**[4] · **Walaa Hamdan**[4,5] · **Safwat Hamad**[6] · **S. Ghose**[3,7]

Received: 9 July 2018 / Accepted: 3 October 2018 / Published online: 10 October 2018

Abstract
Recently, Wang and Ma (Quantum Inf Process 16(5):130, 2017) proposed two interesting quantum key agreement protocols with a single photon in both polarization and spatial-mode degrees of freedom. They claimed that the privacy of participants' secret keys in the multiparty case is protected against dishonest participants. However, in this paper, we prove that two dishonest participants can deduce the secret key of an honest one using a fake sequence of single photons, without being detected. Also, we propose an additional security detection process to avoid the security loophole in their protocol.

Keywords Quantum key agreement protocol · Single photons in both polarization and spatial-mode degrees of freedom · Collusive attack

1 Introduction

The rapid development and growing adoption of quantum cryptographic techniques have provided unconditional security for most of the conventional security issues. In

✉ Hussein Abulkasim
hussein@svu.edu.eg

1 Faculty of Science, New Valley University, El-Kharja, Egypt

2 Faculty of Science, South Valley University, Qena, Egypt

3 Department of Physics and Computer Science, Wilfrid Laurier University, Waterloo, Canada

4 Libraries, Documents and Information Department, Princess Nora Bint Abdulrahman University, Riyadh, Saudi Arabia

5 Libraries, Documents and Information Department, Assiut University, Assiut, Egypt

6 Faculty of Computer and Information Sciences, Ain Shams University, Cairo, Egypt

7 Perimeter Institute for Theoretical Physics, Waterloo, Canada

1984, Bennett and Brassard [1] published pioneering work in quantum cryptography. Since then, many quantum cryptographic schemes have been proposed, including quantum teleportation [2–7], quantum secure direct communication [8–11], quantum secret sharing [12–17], quantum private comparison [18–21], quantum anonymous voting [22], quantum anonymous ranking [23], quantum private query [24–27], and others. Compared to quantum key distribution (QKD) [1] in which one party generates a secret key, quantum key agreement (QKA) allows two or more parties to share equal roles in creating a secret key through public channels where any non-trivial subset of parties cannot deduce the generated key. In 2004, Zhou et al. [28] introduced the first QKA protocol by exploiting maximally entangled states and quantum teleportation. Unfortunately, Tsai and Hwang [29] found that their protocol is not fair, and the shared key can be determined by one party alone.

Subsequently, many two-party QKA protocols have been proposed [30–32]. Later, Shi and Zhong [33] suggested the first multiparty QKA protocol using entanglement swapping. Their multiparty protocol utilizes a Bell state as the quantum resource and the Bell measurement as the primary operation. Since then, many multiparty QKA protocols based on Shi and Zhong's [33] work have been presented [34–49]. Recently, Wang and Ma [50] presented two QKA protocols with single photons in both the polarization and the spatial-mode degrees of freedom. The first protocol enables three parties to generate a secret key using public channels, while the second protocol extends the three-party QKA case to the multiparty case. Their scheme improved the capacity of the transmitted information and introduced high-efficiency performance. Moreover, Wang and Ma claimed that their protocol could achieve privacy. However, we show that in the multiparty QKA case of Wang–Ma protocol, two dishonest parties may collude to eavesdrop on the private key of an honest party using a fake sequence of single photons. Moreover, this manuscript suggests a simple solution to address this defect and proposes a modified version of the Wang–Ma multiparty QKA protocol.

The rest of this paper is as follows. A review of the Wang–Ma multiparty QKA protocol is introduced in Sect. 2. Section 3 analyses the security of the Wang–Ma protocol. Section 4 introduces an improvement to Wang–Ma multiparty QKA protocol. Finally, Sect. 5 concludes this work.

2 Review of the Wang–Ma multiparty QKA protocol

Here, a brief review of Wang–Ma multiparty QKA protocol is presented (Fig. 1). In their protocol, a single-photon state $|\phi\rangle = |\phi\rangle_P \otimes |\phi\rangle_S$ in both polarization and spatial-mode degrees of freedom was used, where $|\phi\rangle_P$ denotes the single-photon states in the polarization degree of freedom and $|\phi\rangle_S$ denotes the single-photon states in the spatial-mode degree of freedom. In addition, two measuring bases are chosen in the polarization degree of freedom (i.e. $Z_P = \{|H\rangle, |V\rangle\}$ and $\mathrm{X}_P = \{|S\rangle_P, |A\rangle_P\}$) and two measuring bases are chosen in the spatial-mode degree of freedom (i.e. $Z_S = \{|b_1\rangle, |b_2\rangle\}$ and $\mathrm{X}_S = \{|s\rangle_S, |a\rangle_S\}$).$|H\rangle$ and $|V\rangle$ are the horizontal polarization and vertical polarization of particles, respectively. $|b_1\rangle$ and $|b_2\rangle$ represent the upper spatial mode and the lower spatial mode of particles, respectively, where

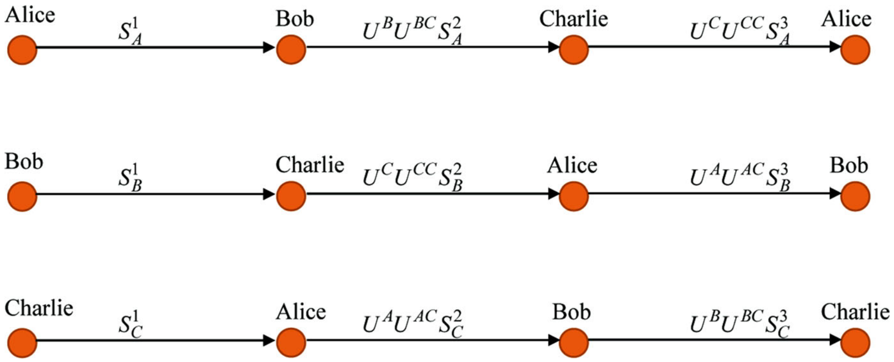

Fig. 1 Wang–Ma three-party QKA protocol [50]. The lines between every two parties represent the quantum channels. U^A,U^B, and U^C represent the collective unitary operation according to the sub-secret keys of Alice, Bob, and Charlie, respectively. U^{AC},U^{BC}, and U^{CC} represent another extra collective unitary operation applied to some single photons, those operated photons randomly selected by Alice, Bob, and Charlie, respectively

$$|S\rangle_P = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle), \quad |A\rangle_P = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$$
$$|s\rangle_S = \frac{1}{\sqrt{2}}(|b_1\rangle + |b_2\rangle), \quad |a\rangle_S = \frac{1}{\sqrt{2}}(|b_1\rangle - |b_2\rangle).$$

Two unitary operations are also used in each degree of freedom as follows:

$$I_P = |H\rangle\langle H| + |V\rangle\langle V|, \quad U_P = |V\rangle\langle H| - |H\rangle\langle V|,$$
$$I_S = |b_1\rangle\langle b_1| + |b_2\rangle\langle b_2|, \quad U_S = |b_2\rangle\langle b_1| - |b_1\rangle\langle b_2|.$$

Based on the above unitary operations we have

$$I_P|H\rangle = |H\rangle, \quad I_P|V\rangle = |V\rangle, \quad I_P|S\rangle_P = |S\rangle_P, \quad I_P|A\rangle_P = |A\rangle_P,$$
$$I_S|b_1\rangle = |b_1\rangle, \quad I_S|b_2\rangle = |b_2\rangle, \quad I_S|s\rangle_S = |S\rangle_S, \quad I_S|a\rangle_s = |a\rangle_s,$$
$$U_P|H\rangle = -|V\rangle, \quad U_P|V\rangle = |H\rangle, \quad U_P|S\rangle_P = |A\rangle_P, \quad U_P|A\rangle_P = -|S\rangle_P,$$
$$U_S|b_1\rangle = -|b_2\rangle, \quad U_S|b_2\rangle = |b_1\rangle, \quad U_S|s\rangle_S = |a\rangle_S, \quad U_S|a\rangle_S = -|s\rangle_S.$$

In the multiparty case of Wang–Ma protocol, M parties (e.g. $P_1, P_2, \ldots, P_M$) want to agree on a shared secure key. The steps of their protocol can be summarized as follows:

(1) *Initialization stage* Each party P_i ($i \in \{1, 2, \ldots, M\}$) prepares $2N$ classical bits string (K_i) as a sub-secret key, where $K_i = \{(r_{i1}, s_{i1})(r_{i2}, s_{i2}) \ldots (r_{iN}, s_{iN})\}$.
(2) *Preparation stage* Each party P_i generates a sequence (S_i) of ordered N single photons in both polarization and spatial-mode degrees of freedom. Each photon S_i is in the state $|\phi\rangle = |\phi\rangle_P \otimes |\phi\rangle_S$. P_i also generates kN_i decoy single photons and inserts them into S_i producing a new sequence S_i^i. Then P_i sends S_i^i to P_{i+1}.
(3) *Security detection stage* P_{i+1} uses the quantum filter and the photon number splitter device for avoiding a Trojan horse attack. Upon receiving S_i^i, P_i informs

P_{i+1} the positions and the corresponding measuring bases of all decoy particles. Hence, P_i and P_{i+1} can check the security of the transmission. If the transmission is not secure, they terminate the protocol. Otherwise, P_i and P_{i+1} continue to the encoding stage.

(4) *Encoding stage* P_{i+1} discards the decoy photons then he applies collective unitary operations to the remaining N photons according to K_{i+1}. That is, if the ith bit values of P_{i+1}'s sub-secret key are $(r_{(i+1,i)}, s_{(i+1,i)}) = 00\,(11)$, he will apply $I_P \oplus I_S(U_P \oplus U_S)$ to the ith photon. But, if the bit values are $(r_{(i+1,i)}, s_{(i+1,i)}) = 01\,(10)$, he will apply $I_P \oplus U_S(U_P \oplus I_S)$ to the ith photon.

(5) *Additional operation stage* The party P_{i+1} randomly selects the jth photon and randomly applies another extra collective unitary operation to it. Then, P_{i+1} prepares kN_{i+1} decoy single photons and inserts them into S_i producing a new sequence S_i^{i+1}. Then P_{i+1} sends S_i^{i+1} to P_{i+2}.

(6) *Particles exchange stage* The parties $P_{i+2}, \ldots, P_{i-1}$ execute steps (3), (4), and (5) in turn. That is, one by one, they check the security of transmission. If so, they encode their keys with S_i and apply another extra collective unitary operation to some selected single photons. Afterwards, they insert decoy particles randomly into the sequence S_i and send it to the next party.

(7) *Key extraction stage* Upon confirming that every party $(P_1, \cdots, P_i, \cdots, P_M)$ has executed the steps $(1) - (6)$, the parties $P_M, \cdots, P_{i-1}, \cdots, P_{M-1}$ send the sequences $S_0^M, \cdots, S_i^{i-1}, \cdots, S_M^{M-1}$ to $P_1, \cdots, P_i, \cdots, P_M$. They then check the security of the quantum channels as described in step (3). If the error rate is less than a preset threshold, every party publicly announces the information of extra collective unitary operations. P_i then applies same extra unitary operations to the corresponding single photons. Since P_i knows the initial states of all single photons in S_i, he can recover $K_i^{'}$ by measuring S_i. Hence, P_i can deduce the final shared key K, where $K = K_i \oplus K_i^{'}$.

3 Security analysis of the Wang–Ma multiparty QKA protocol

This section analyses the security of the Wang–Ma QKA protocol and introduces two cases. In Case 1, Wang and Ma claimed that the above multiparty QKA protocol could achieve privacy. However, Case 1 shows that Wang–Ma multiparty QKA protocol is not secure against a collusive attack performed by a group of two dishonest parties. Moreover, in Case 2, if two nested groups of dishonest parties or more try to adopt our suggested attack strategy, they will not succeed in stealing the private information of other parties as depicted in Fig. 2 and Table 2. Case 1 and Case 2 can be described in detail as follows.

3.1 Case 1: Wang–Ma protocol is not secure against our attack strategy

This collusive attack shows that two dishonest parties can eavesdrop on the sub-secret key of an honest party without being detected. For convenience, we assume that five parties P_0, P_1, P_2, P_3, and P_4 are wanting to agree upon a secure shared

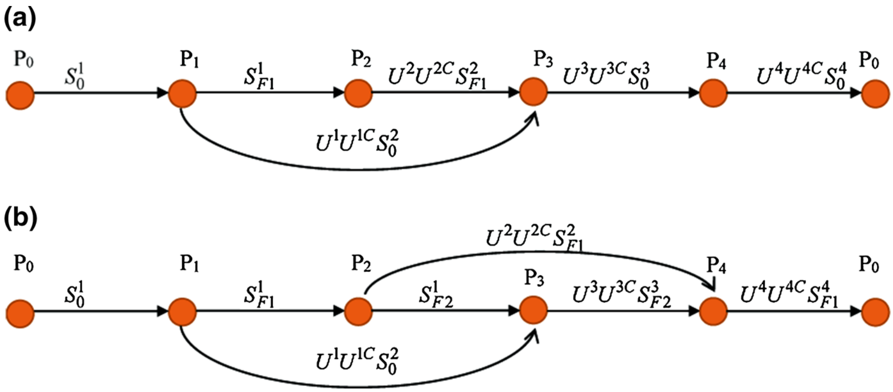

Fig. 2 Graphical representation of our suggested collusive attack strategy. In section **a**, the two dishonest parties P_1 and P_3 may collude to eavesdrop on the sub-secret key of the honest party P_3 according to our attack strategy. In section **b**, $\{P_1, P_3\}$ and $\{P_2, P_4\}$ are two groups of dishonest parties, where the two dishonest parties in each group try to eavesdrop on the private information of the honest ones; in that case, Wang–Ma protocol is secure against our attack strategy

key. According to the Wang–Ma protocol, the initiator $P_0(P_1/P_2/P_3/P_4)$ generates N single photons in both polarization and spatial-mode degrees of freedom and transmits them to $P_1(P_2/P_3/P_4/P_0)$. Then $P_1(P_2/P_3/P_4/P_0)$ applies joint unitary operations to the received photons based on his/her sub-secret key and sends the new states to $P_2(P_3/P_4/P_0/P_1)$. Also $P_2(P_3/P_4/P_0/P_1)$, $P_3(P_4/P_0/P_1/P_2)$, and $P_4(P_0/P_1/P_2/P_3)$ follow the same process of $P_1(P_2/P_3/P_4/P_0)$ and send the new states to $P_3(P_4/P_0/P_1/P_2)$, $P_4(P_0/P_1/P_2/P_3)$, and $P_0(P_1/P_2/P_3/P_4)$, respectively. Finally, according to the key extraction stage, $P_0(P_1/P_2/P_3/P_4)$ can obtain the final shared key.

However, for example, if P_1 and P_3 are dishonest parties, they can easily eavesdrop on the sub-secret key of the honest party P_2. That is, in step (4), the dishonest party P_1 encodes the received photons with collective unitary operations decided according to the bit values of his sub-secret key. He also applies some extra collective unitary operations according to step (5). Then P_1 sends the new photons (S_2) to the dishonest party P_3 instead of the honest party P_2 as illustrated in Fig. 2a. Also, P_1 generates a fake sequence (S_{F1}^1) of ordered N single photons in both polarization and spatial-mode degrees of freedom as in step (2). Afterwards, P_1 generates kN decoy photons and inserts them into the fake sequence S_{F1}^1 for security checking. Then, P_1 sends the sequence S_{F1}^1 to the honest party P_2. Upon receiving S_{F1}^1, P_2 executes the step (3) – (5) loyally because he does not know that the received sequence is fake. Hence, P_2 encodes the received photons with collective unitary operations decided according to the bit values of his sub-secret key, and he also applies some extra collective unitary operations. Then P_2 sends the new sequence (S_{F1}^2) to P_3. P_3 checks the security of the transmission with P_2 using the decoy photons (Fig. 2).

Since P_1 and P_3 know all the information about S_{F1}^1, P_1 and P_3 can easily recover P_2's unitary operations that are applied to S_{F1}^1 by comparing the measuring result of S_{F1}^2 and the original states as shown in Table 1. For clarity, for $N = 1$, assume that P_2's

Table 1 Evolved states of the dishonest party P_1 and the honest party P_2

P_0 to P_1	P_1 to P_3			P_1 to P_2	P_2 to P_3		
(S_0^1)	U^1	U^{1C}	$U^1U^{1C}S_0^2$	(S_{F1}^1)	U^2	U^{2C}	$U^2U^{2C}S_{F1}^2$
$\|H\rangle\|b_1\rangle$	$I_P\otimes I_S$	$I_P\otimes I_S$	$\|H\rangle\|b_1\rangle$	$\|V\rangle\|b_1\rangle$	$I_P\otimes I_S$	$I_P\otimes I_S$	$\|V\rangle\|b_1\rangle$
	$I_P\otimes I_S$	$I_P\otimes U_S$	$-\|H\rangle\|b_2\rangle$		$I_P\otimes I_S$	$I_P\otimes U_S$	$-\|V\rangle\|b_2\rangle$
	$I_P\otimes I_S$	$U_P\otimes I_S$	$-\|V\rangle\|b_1\rangle$		$I_P\otimes I_S$	$U_P\otimes I_S$	$\|H\rangle\|b_1\rangle$
	$I_P\otimes I_S$	$U_P\otimes U_S$	$\|V\rangle\|b_2\rangle$		$I_P\otimes I_S$	$U_P\otimes U_S$	$-\|H\rangle\|b_2\rangle$
	$I_P\otimes I_S$	N/A	$\|H\rangle\|b_1\rangle$		$I_P\otimes I_S$	N/A	$\|V\rangle\|b_1\rangle$
	$I_P\otimes U_S$	$I_P\otimes I_S$	$-\|H\rangle\|b_2\rangle$		$I_P\otimes U_S$	$I_P\otimes I_S$	$-\|V\rangle\|b_2\rangle$
	$I_P\otimes U_S$	$I_P\otimes U_S$	$-\|H\rangle\|b_1\rangle$		$I_P\otimes U_S$	$I_P\otimes U_S$	$-\|V\rangle\|b_1\rangle$
	$I_P\otimes U_S$	$U_P\otimes I_S$	$\|V\rangle\|b_2\rangle$		$I_P\otimes U_S$	$U_P\otimes I_S$	$-\|H\rangle\|b_2\rangle$
	$I_P\otimes U_S$	$U_P\otimes U_S$	$\|V\rangle\|b_1\rangle$		$I_P\otimes U_S$	$U_P\otimes U_S$	$-\|H\rangle\|b_1\rangle$
	$I_P\otimes U_S$	N/A	$-\|H\rangle\|b_2\rangle$		$I_P\otimes U_S$	N/A	$-\|V\rangle\|b_2\rangle$
	$U_P\otimes I_S$	$I_P\otimes I_S$	$-\|V\rangle\|b_1\rangle$		$U_P\otimes I_S$	$I_P\otimes I_S$	$\|H\rangle\|b_1\rangle$
	$U_P\otimes I_S$	$I_P\otimes U_S$	$\|V\rangle\|b_2\rangle$		$U_P\otimes I_S$	$I_P\otimes U_S$	$-\|H\rangle\|b_2\rangle$
	$U_P\otimes I_S$	$U_P\otimes I_S$	$-\|H\rangle\|b_1\rangle$		$U_P\otimes I_S$	$U_P\otimes I_S$	$-\|V\rangle\|b_1\rangle$
	$U_P\otimes I_S$	$U_P\otimes U_S$	$\|H\rangle\|b_2\rangle$		$U_P\otimes I_S$	$U_P\otimes U_S$	$\|V\rangle\|b_2\rangle$
	$U_P\otimes I_S$	N/A	$-\|V\rangle\|b_1\rangle$		$U_P\otimes I_S$	N/A	$\|H\rangle\|b_1\rangle$
	$U_P\otimes U_S$	$I_P\otimes I_S$	$\|V\rangle\|b_2\rangle$		$U_P\otimes U_S$	$I_P\otimes I_S$	$-\|H\rangle\|b_2\rangle$
	$U_P\otimes U_S$	$I_P\otimes U_S$	$\|V\rangle\|b_1\rangle$		$U_P\otimes U_S$	$I_P\otimes U_S$	$-\|H\rangle\|b_1\rangle$
	$U_P\otimes U_S$	$U_P\otimes I_S$	$\|H\rangle\|b_2\rangle$		$U_P\otimes U_S$	$U_P\otimes I_S$	$\|V\rangle\|b_2\rangle$
	$U_P\otimes U_S$	$U_P\otimes U_S$	$\|H\rangle\|b_1\rangle$		$U_P\otimes U_S$	$U_P\otimes U_S$	$\|V\rangle\|b_1\rangle$
	$U_P\otimes U_S$	N/A	$\|V\rangle\|b_2\rangle$		$U_P\otimes U_S$	N/A	$-\|H\rangle\|b_2\rangle$

U^1 and U^2 are the unitary operation of P_1 and P_2, U^{1C} and U^{2C} are the extra unitary operation of P_1 and P_2, $U^1U^{1C}S_0^2$ and $U^2U^{2C}S_{F1}^2$ are the evolved states of P_1 and P_2, S_0^1 and S_{F1}^1 are the initial states of P_0 and P_1, respectively

(the honest party) sub-secret key is "10". According to Table 1, without considering the security check process, assume that the initiator P_0 sends S_0^1 (e.g. $|H\rangle|b_1\rangle$) to the dishonest party P_1. P_1 applies $U^1 =$ (e.g. $\{U_P\otimes I_S\}$) and $U^{1C} =$ (e.g. $\{U_P\otimes U_S\}$) to the state $|H\rangle|b_1\rangle$, where U^1 represents unitary operation corresponding to the private information of P_1 and U^{1C} represents an additional unitary operation to be applied to some particles. So, the evolved state is $|H\rangle|b_2\rangle$. Also, P_1 sends a fake state S_{F1}^1(e.g. $|V\rangle|b_1\rangle$) to the honest party P_2. P_2 applies $U^2 = \{U_P\otimes I_S\}$ (where U^2 represents his private information (i.e. 10)) and $U^{2C} =$ (e.g. $\{U_P\otimes U_S\}$) to the fake state $|V\rangle|b_1\rangle$. P_2 then sends the evolved state to the dishonest P_3. Subsequently, P_3 measures P_2's states getting the state $|V\rangle|b_2\rangle$. P_1 and P_3 compare the initial fake state (i.e. $|V\rangle|b_1\rangle$) with the measuring result (i.e. $|V\rangle|b_2\rangle$), which means that P_2 applied the overall unitary operation $I_P\otimes U_S$ to $|V\rangle|b_1\rangle$.

However, the goal of P_1 and P_3 is not to know the overall unitary operation but to recover U^2 that represents the private information of P_2. Thus, P_1 and P_3 register the previous information and wait for step (7), where every party publicly announces the information of extra collective unitary operation (i.e. $U^{2C} = \{U_P\otimes U_S\}$). Finally, P_1

Table 2 Unitary operations that can be applied to the fake initial state ($|V\rangle|b_1\rangle$) when the evolved state is $\pm|V\rangle|b_2\rangle$

P_1 to P_2	P_2 to P_3		
(S^1_{F1})	U^2	U^{2C}	$U^2U^{2C}S^2_{F1}$
$\|V\rangle\|b_1\rangle$	$I_P \otimes I_S$	$I_P \otimes U_S$	$-\|V\rangle\|b_2\rangle$
	$I_P \otimes U_S$	$I_P \otimes I_S$	$-\|V\rangle\|b_2\rangle$
	$I_P \otimes U_S$	N/A	$-\|V\rangle\|b_2\rangle$
	$U_P \otimes I_S$	$U_P \otimes U_S$	$\|V\rangle\|b_2\rangle$
	$U_P \otimes U_S$	$U_P \otimes I_S$	$\|V\rangle\|b_2\rangle$

and P_3 can easily recover U^2(i.e. $\{U_P \otimes I_S\}$) with the help of Table 2 and $U^{2C} = \{U_P \otimes U_S\}$.

3.2 Case 2: Wang–Ma protocol is secure against our attack strategy

Figure 2b shows that Wang–Ma protocol can resist our suggested attack strategy. For clarity, according to Fig. 2b, assume that there are two nested groups of dishonest parties $\{P_1, P_3\}$ and $\{P_2, P_4\}$, each group would like to steal the private information of the middle party. At the beginning, the initiator P_0 sends the initial states S^1_0 to P_1. P_1 applies her unitary operations to S^1_0 and sends the evolved states to P_3. Also P_1 prepares a fake sequence (S^1_{F1}) and sends it to P_2. Because $\{P_2, P_4\}$ is another group of dishonest parties, they will not perform the process of the protocol honestly. So, P_2 sends another fake sequence (S^1_{F2}) to P_3. Now, P_2 and P_3 encode their information with two fake sequences producing two evolved fake sequences $U^2U^{2C}S^2_{F1}$ and $U^3U^{3C}S^3_{F2}$, respectively. Accordingly, P_4 sends fake evolved sequence (i.e. $U^3U^{3C}S^3_{F2}$) to P_0. Finally, in step (7), P_0 checks the security of transmission, and she will find that the error rate is greater than the preset threshold, because the received operated sequence is not real. As a result, P_0 ends the protocol and announces that the transmission is not secure. So, we can say that the Wang–Ma protocol is secure against our attack strategy in that case.

4 Improvement to Wang–Ma multiparty QKA protocol

In Wang–Ma multiparty QKA protocol, the security of the transmission between every two parties is checked by the parties themselves. Thus, this strategy enables the dishonest parties to deceive the honest ones and steal their sub-secret keys. Following some previous works [15, 46, 51] for solving such kinds of collusive attacks, we present here modifications to the steps 2, 3, and 7 of Wang–Ma multiparty QKA protocol to solve this defect (see also Fig. 3). The modifications are:

(2*) *Preparation stage* The initiator P_i generates a sequence S_i of ordered N single photons in both polarization and spatial-mode degrees of freedom. And each photon in S_i in the state $|\phi\rangle = |\phi\rangle_P \otimes |\phi\rangle_S$. P_i generates kN_i decoy single photons, where each photon is randomly in one of the states $\{|H\rangle, |V\rangle, |A\rangle_P, |S\rangle_P\}$ for checking the

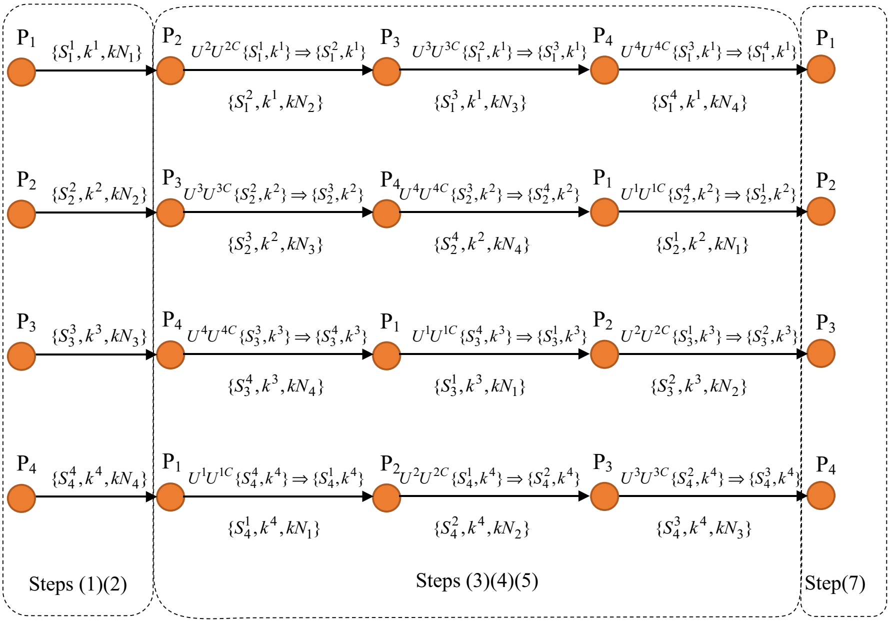

Fig. 3 Graphical representation of our improvement to Wang–Ma multiparty QKA protocol for $M = 4$

quantum channel between P_i and P_{i+1}, and inserts them into S_i. Also, P_i generates k^i decoy single photons and inserts them into S_i producing a new sequence S_i^i. Then P_i sends S_i^i to P_{i+1}. Here, k^i is the decoy photon subsequence used for checking the security of the overall transmission, by the initiators P_i.

(3*) *Security detection stage* P_{i+1} uses the quantum filter and the photon number splitter device for avoiding a Trojan horse attack. Upon receiving S_i^i, P_i informs P_{i+1} the positions and the corresponding measuring bases of kN_i. Hence, P_i and P_{i+1} can check the security of the transmission. If the transmission is not secure, they terminate the protocol. Otherwise, P_i and P_{i+1} continue to the encoding stage.

(7*) *Key extraction stage* Upon confirming that $P_1, \ldots, P_i, \ldots, P_M$ have finished the step $(1)-(6)$, the parties $P_M, \ldots, P_{i-1}, \ldots, P_1$ send $S_0^1, \ldots, S_i^{i-1}, \ldots, S_M^{M-1}$ to $P_1, \ldots, P_i, \ldots, P_M$, respectively. Afterwards, P_M and $P_1,\ldots, P_{i-1}$ and $P_i,\ldots, P_{M-1}$ and P_M check the security of the quantum channel using the decoy photons technique. If the transmission is not safe, they terminate the protocol. Otherwise, they move to the sub-step (7.1*).

(7.1*) *Additional security detection stage* Firstly, every party announces the information of the extra collective unitary operations. Secondly, P_i announces the positions of k^i and asks every party to announce the information of the collective unitary operations that were applied to it. P_i then applies the same unitary operations to k^i and measures each photon in k^i with the corresponding basis. Hence, P_i can judge whether the final transmission is secure or not. If not, P_i ends the protocol and announces that there is a collusive attack. Otherwise, P_i measures each photon in S_i with the corresponding basis. Finally, since P_i knows the initial states of all single photons in S_i,

$K_i^{'}$ can be recovered by measuring S_i. Hence, P_i can deduce the final shared key K, where $K = K_i \oplus K_i^{'}$.

Steps (1*), (4*), (5*), and (6*) will remain the same as steps (1), (4), (5), and (6) in Sect. 2. According to the above improvement, if the dishonest parties try to eavesdrop on the honest one by adopting the collusive attack strategy mentioned in Sect. 3.1, they will be detected in Step (7*) by the initiator P_i. Thus, the privacy problem mentioned in Case 1 can be addressed.

5 Conclusion

This paper shows the security flaw of the Wang–Ma multiparty QKA protocol. In their protocol, the quantum channels among participants are checked using the decoy photon technique. However, we proved that two dishonest participants could deduce the secret key of an honest participant using a fake sequence of single photons without being detected. Moreover, an additional security detection process is suggested to avoid the security loophole in Wang–Ma's protocol.

References

1. Bennet, C.H., Brassard, G.: Quantum cryptography: public-key distribution and coin tossing. In: IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, pp. 175–179 (1984)
2. Bouwmeester, D., Pan, J.-W., Mattle, K., Eibl, M., Weinfurter, H., Zeilinger, A.: Experimental quantum teleportation. Nature **390**(6660), 575 (1997)
3. Bennett, C.H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., Wootters, W.K.: Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels. Phys. Rev. Lett. **70**(13), 1895 (1993)
4. Zhao, N., Li, M., Chen, N., Zhu, C.-H., Pei, C.-X.: Quantum teleportation of eight-qubit state via six-qubit cluster state. Int. J. Theor. Phys. **57**(2), 516–522 (2018)
5. Muralidharan, S., Panigrahi, P.K.: Perfect teleportation, quantum-state sharing, and superdense coding through a genuinely entangled five-qubit state. Phys. Rev. A **77**(3), 032321 (2008)
6. Choudhury, S., Muralidharan, S., Panigrahi, P.K.: Quantum teleportation and state sharing using a genuinely entangled six-qubit state. J. Phys. A Math. Theor. **42**(11), 115303 (2009)
7. Sarvaghad-Moghaddam, M., Farouk, A., Abulkasim, H.: Bidirectional Quantum Controlled Teleportation by Using Five-qubit Entangled State as a Quantum Channel (2018). arXiv preprint arXiv:1806.07061
8. Boström, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. **89**(18), 187902 (2002)
9. Farouk, A., Zakaria, M., Megahed, A., Omara, F.A.: A generalized architecture of quantum secure direct communication for N disjointed users with authentication. Sci. Rep. **5**, 16080 (2015)
10. Jain, S., Muralidharan, S., Panigrahi, P.K.: Secure quantum conversation through non-destructive discrimination of highly entangled multipartite states. EPL (Europhys. Lett.) **87**(6), 60008 (2009)
11. Wei, H., Qiao-Yan, W., Heng-Yue, J., Su-Juan, Q., Fei, G.: Fault tolerant quantum secure direct communication with quantum encryption against collective noise. Chin. Phys. B **21**(10), 100308 (2012)
12. Hillery, M., Bužek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**(3), 1829 (1999)
13. Abulkasim, H., Hamad, S., Khalifa, A., El Bahnasy, K.: Quantum secret sharing with identity authentication based on Bell states. Int. J. Quantum Information **15**(04), 1750023 (2017)
14. Abulkasim, H., Hamad, S., El Bahnasy, K., Rida, S.Z.: Authenticated quantum secret sharing with quantum dialogue based on Bell states. Phys. Scr. **91**(8), 085101 (2016)

15. Abulkasim, H., Hamad, S., Elhadad, A.: Reply to Comment on 'Authenticated quantum secret sharing with quantum dialogue based on Bell states'. Phys. Scr. **93**(2), 027001 (2018)
16. Joy, D., Behera, B.K., Panigrahi, P.K.: In principle demonstration of quantum secret sharing in the IBM quantum computer (2018). arXiv preprint arXiv:1807.03219
17. 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**(4), 042317 (2003)
18. Yang, Y.-G., Wen, Q.-Y.: An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. J. Phys. A: Math. Theor. **42**(5), 055305 (2009)
19. Hung, S.-M., Hwang, S.-L., Hwang, T., Kao, S.-H.: Multiparty quantum private comparison with almost dishonest third parties for strangers. Quantum Inf. Process. **16**(2), 36 (2017)
20. Zhou, M.-K.: Improvements of quantum private comparison protocol based on cluster states. Int. J. Theor. Phys. **57**(1), 42–47 (2018)
21. Huang, W., Wen, Q., Liu, B., Gao, F., Sun, Y.: Robust and efficient quantum private comparison of equality with collective detection over collective-noise channels. Sci. China Phys. Mech. Astron. **56**(9), 1670–1678 (2013)
22. Vaccaro, J.A., Spring, J., Chefles, A.: Quantum protocols for anonymous voting and surveying. Phys. Rev. A **75**(1), 012333 (2007)
23. Huang, W., Wen, Q.-Y., Liu, B., Su, Q., Qin, S.-J., Gao, F.: Quantum anonymous ranking. Phys. Rev. A **89**(3), 032325 (2014)
24. Jakobi, M., Simon, C., Gisin, N., Bancal, J.-D., Branciard, C., Walenta, N., Zbinden, H.: Practical private database queries based on a quantum-key-distribution protocol. Phys. Rev. A **83**(2), 022301 (2011)
25. Wei, C.-Y., Wang, T.-Y., Gao, F.: Practical quantum private query with better performance in resisting joint-measurement attack. Phys. Rev. A **93**(4), 042318 (2016)
26. Gao, F., Liu, B., Huang, W., Wen, Q.-Y.: Postprocessing of the oblivious key in quantum private query. IEEE J. Sel. Top. Quantum Electron. **21**(3), 98–108 (2015)
27. Wei, C.-Y., Cai, X.-Q., Liu, B., Wang, T., Gao, F.: A generic construction of quantum-oblivious-key-transfer-based private query with ideal database security and zero failure. IEEE Trans. Comput. **67**, 2–8 (2017)
28. Zhou, N., Zeng, G., Xiong, J.: Quantum key agreement protocol. Electron. Lett. **40**(18), 1149–1150 (2004)
29. Tsai, C., Hwang, T.: On quantum key agreement protocol. Technical Report C-S-I-E, NCKU, Taiwan (2009)
30. He, Y.-F., Ma, W.-P.: Two-party quantum key agreement based on four-particle GHZ states. Int. J. Quantum Inf. **14**(01), 1650007 (2016)
31. 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**(3), 649–663 (2014)
32. He, Y.-F., Ma, W.-P.: Two-party quantum key agreement against collective noise. Quantum Inf. Process. **15**(12), 5023–5035 (2016)
33. Shi, R.-H., Zhong, H.: Multi-party quantum key agreement with bell states and bell measurements. Quantum Inf. Process. **12**(2), 921–932 (2013)
34. Cai, B., Guo, G., Lin, S.: Multi-party quantum key agreement with teleportation. Mod. Phys. Lett. B **31**(10), 1750102 (2017)
35. Cai, B.-B., Guo, G.-D., Lin, S.: Multi-party quantum key agreement without entanglement. Int. J. Theor. Phys. **56**(4), 1039–1051 (2017)
36. Cao, H., Ma, W.: Multiparty quantum key agreement based on quantum search algorithm. Sci. Rep. **7**, 45046 (2017)
37. Huang, W., Su, Q., Liu, B., He, Y.-H., Fan, F., Xu, B.-J.: Efficient multiparty quantum key agreement with collective detection. Sci. Rep. **7**(1), 15264 (2017)
38. Huang, W., Su, Q., Xu, B., Liu, B., Fan, F., Jia, H., Yang, Y.: Improved multiparty quantum key agreement in travelling mode. Sci. CHINA Phys. Mech. Astron. **59**(12), 120311 (2016)
39. 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**(5), 2113–2124 (2016)
40. Liu, W.-J., Chen, Z.-Y., Ji, S., Wang, H.-B., Zhang, J.: Multi-party semi-quantum key agreement with delegating quantum computation. Int. J. Theor. Phys. **56**(10), 3164–3174 (2017)
41. Luo, Q.-B., Yang, G.-W., She, K., Niu, W.-N., Wang, Y.-Q.: Multi-party quantum private comparison protocol based on d-dimensional entangled states. Quantum Inf. Process. **13**(10), 2343–2352 (2014)

42. Sun, Z., Huang, J., Wang, P.: Efficient multiparty quantum key agreement protocol based on commutative encryption. Quantum Inf. Process. **15**(5), 2101–2111 (2016)
43. Sun, Z., Yu, J., Wang, P.: Efficient multi-party quantum key agreement by cluster states. Quantum Inf. Process. **15**(1), 373–384 (2016)
44. Sun, Z., Zhang, C., Wang, B., Li, Q., Long, D.: Improvements on "multiparty quantum key agreement with single particles". Quantum Inf. Process. **12**(11), 3411–3420 (2013)
45. Sun, Z., Zhang, C., Wang, P., Yu, J., Zhang, Y., Long, D.: Multi-party quantum key agreement by an entangled six-qubit state. Int. J. Theor. Phys. **55**(3), 1920–1929 (2016)
46. Wang, P., Sun, Z., Sun, X.: Multi-party quantum key agreement protocol secure against collusion attacks. Quantum Inf. Process. **16**(7), 170 (2017)
47. Xu, G.-B., Wen, Q.-Y., Gao, F., Qin, S.-J.: Novel multiparty quantum key agreement protocol with GHZ states. Quantum Inf. Process. **13**(12), 2587–2594 (2014)
48. 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**(7), 1651–1657 (2014)
49. Liu, B., Gao, F., Huang, W., Wen, Q.-Y.: Multiparty quantum key agreement with single particles. Quantum Inf. Process. **12**(4), 1797–1805 (2013)
50. Wang, L., Ma, W.: Quantum key agreement protocols with single photon in both polarization and spatial-mode degrees of freedom. Quantum Inf. Process. **16**(5), 130 (2017)
51. 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. Sci. Rep. **7**(1), 2485 (2017)