Quantum Inf Process (2012) 11:113–122
DOI 10.1007/s11128-011-0236-z

Thwarting intercept-and-resend attack on Zhang's quantum secret sharing using collective rotation noises

Chun-Wei Yang · Chia-Wei Tsai · Tzonelih Hwang

Received: 31 July 2010 / Accepted: 25 February 2011 / Published online: 6 March 2011

Abstract This work deliberately introduces collective-rotation noise into quantum states to prevent an intercept-resend attack on Zhang's quantum secret sharing scheme over a collective-noise quantum channel (Zhang in Phys A 361:233–238, 2006). The noise recovering capability of the scheme remains intact. With this design, the quantum bit efficiency of the protocol is doubled when compared to Sun et al.'s improvement on Zhang's scheme (Sun et al. in Opt Commun 283:181–183, 2010).

Keywords Collective noise · Intercept-resend attack · Quantum secret sharing · Quantum cryptography

1 Introduction

Quantum cryptography has become one of the most important research topics in quantum information science. The security of quantum cryptographic protocols, such as quantum key distribution (QKD) and quantum secret sharing (QSS), is based on the laws of physics [1]. However, due to fluctuations of the birefringence of optical fiber [2], noises of transmission of photons in the optical fiber always exist. Since photons travel inside a time window which is shorter than the variation of noise [3],

C.-W. Yang · C.-W. Tsai · T. Hwang (✉)
Department of Computer Science and Information Engineering, National Cheng Kung University, No. 1, Ta-Hsueh Rd., Tainan, Taiwan, ROC
e-mail: hwangtl@ismail.csie.ncku.edu.tw

C.-W. Yang
e-mail: waywei.yang@gmail.com

C.-W. Tsai
e-mail: redbear676@gmail.com

these photons will be affected by the same noise, which is known as the collective noise.

Two types of collective noise are collective-dephasing noise and collective-rotation noise. The transformation results of these two collective noises are illustrated as follows. Equations (1) and (2) show the polarization photons $|0\rangle$ and $|1\rangle$undergoing the transformations of collective-dephasing noise and collective-rotation noise respectively, where $|0\rangle$ and $|1\rangle$ represent the horizontal and vertical polarization states respectively, and θ is the parameter of the noise fluctuating with time.

$$\begin{aligned} |0\rangle &\rightarrow \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle \\ |1\rangle &\rightarrow \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ e^{i\theta} \end{pmatrix} = e^{i\theta} |1\rangle \end{aligned} \tag{1}$$

$$\begin{aligned} |0\rangle &\rightarrow \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix} = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle \\ |1\rangle &\rightarrow \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -\sin\theta \\ \cos\theta \end{pmatrix} = -\sin\theta\,|0\rangle + \cos\theta\,|1\rangle \end{aligned} \tag{2}$$

It should be noted that Eqs. 1 and 2 show a single particle undergoing the transformation of a collective noise. If multiple photons travel inside a time window, then they will undergo the transformation of the same collective noise. For example, if the sender sends these particles $|0\rangle\,|0\rangle\,|1\rangle\,|1\rangle$ to the receiver in the same time window over a collective-dephasing noise channel (or a collective-rotation noise channel), then the transformation results of these particles $|0\rangle\,|0\rangle\,|1\rangle\,|1\rangle$ will change to the state in Eq. 3 (or Eq. 4).

$$|0\rangle\,|0\rangle\,|1\rangle\,|1\rangle \xrightarrow{\text{collective-dephasing noise channel}} |0\rangle\,|0\rangle\,e^{i\theta}\,|1\rangle\,e^{i\theta}\,|1\rangle$$

$$|0\rangle\,|0\rangle\,|1\rangle\,|1\rangle \xrightarrow{\text{collective-rotation noise channel}} \tag{3}$$

$$\begin{aligned} &\cos^4\alpha\,|0\rangle\,|0\rangle\,|1\rangle\,|1\rangle - \cos^3\alpha\sin\alpha\,(|0\rangle\,|0\rangle\,|0\rangle\,|1\rangle + |0\rangle\,|0\rangle\,|1\rangle\,|0\rangle \\ &\quad - |0\rangle\,|1\rangle\,|1\rangle\,|1\rangle - |1\rangle\,|0\rangle\,|1\rangle\,|1\rangle) + \sin^4\alpha\,|1\rangle\,|1\rangle\,|0\rangle\,|0\rangle \\ &\quad + \cos\alpha\sin^3\alpha\,(|0\rangle\,|1\rangle\,|0\rangle\,|0\rangle + |1\rangle\,|0\rangle\,|0\rangle\,|0\rangle - |1\rangle\,|1\rangle\,|0\rangle\,|1\rangle - |1\rangle\,|1\rangle\,|1\rangle\,|0\rangle) \\ &\quad + \cos^2\alpha\sin^2\alpha\,(|0\rangle\,|0\rangle\,|0\rangle\,|0\rangle - |0\rangle\,|1\rangle\,|0\rangle\,|1\rangle - |0\rangle\,|1\rangle\,|1\rangle\,|0\rangle \\ &\quad - |1\rangle\,|0\rangle\,|0\rangle\,|1\rangle - |1\rangle\,|0\rangle\,|1\rangle\,|0\rangle + |1\rangle\,|1\rangle\,|1\rangle\,|1\rangle) \end{aligned} \tag{4}$$

With the existence of collective noise, an eavesdropper can disguise his/her attack as noise in order to avoid being detected in eavesdropping check process [3,4]. How to design secure quantum protocols which can also resist collective noise is becoming an important research issue.

Decoherence-free (DF) states, which are invariant under collective noise, are frequently used to solve this problem [5–8]. For instance, the singlet state $\psi^- = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ is unchanged by these collective noise channels [11,15]. Hence, it can form a noiseless subspace (i.e., a DF subspace).

Several methods [2–4,9–18] have been developed to remove the effects of noise in quantum key distribution and quantum secret sharing. In 2004, Boileau et al. proposed a robust photon-polarization-based quantum key distribution protocol over two collective-noise channels using a DF subspace [11]. In 2006, based on Boileau et al.'s protocol, Zhang developed a multiparty quantum secret sharing of key over two collective-noise channels [15]. Recently, Sun et al. presented an insider attack [18] to capture the key without being detected on Zhang's QSS. Their scheme used a special state (i.e., $|0011\rangle_{1234}$) to obtain an agent's permutations without being detected through perfect channels. The attacker (the last agent) could also obtain the key of Alice (a boss) without needing the help of the others. However, if the special state $|0011\rangle_{1234}$ is contaminated by collective-rotation noise, then the attacker cannot infer the agent's permutations because $|0011\rangle_{1234}$ is not a DF state. Based on this observation, this paper deliberately introduces collective-rotation noise to the received quanta to upset the attacker's state (i.e., $|0011\rangle_{1234}$). Compared to Sun et al.'s improvement on Zhang's QSS, our approach has two advantages. Firstly, it eliminates an extra public discussion. Secondly, it ensures higher qubit efficiency.

The rest of this paper is organized as follows. In Sect. 2, Zhang's QSS protocol and Sun et al.'s method are introduced respectively. Section 3 details the improved QSS scheme and Sect. 4 analyzes its performance and security. Section 5 concludes this paper.

2 Related works

This section reviews Zhang's QSS protocol and Sun et al.'s intercept-resend attack. Moreover, the improved scheme proposed by Sun et al. will also be described in this section.

2.1 Review of Zhang's QSS

In Zhang's QSS protocol, the following three normalized states of the product state of two singlets ψ^- are employed initially:

$$\begin{aligned} w_x &= \psi_{12}^- \psi_{34}^- = \frac{1}{\sqrt{2}}(|a\rangle - |b\rangle), \\ w_y &= \psi_{13}^- \psi_{24}^- = \frac{1}{\sqrt{2}}(|c\rangle - |b\rangle), \\ w_z &= \psi_{14}^- \psi_{23}^- = \frac{1}{\sqrt{2}}(|a\rangle - |c\rangle), \end{aligned} \tag{5}$$

where

$$\begin{aligned} |a\rangle &= \frac{1}{\sqrt{2}}(|0101\rangle + |1010\rangle), \\ |b\rangle &= \frac{1}{\sqrt{2}}(|0110\rangle + |1001\rangle), \end{aligned} \tag{6}$$

$$|c\rangle = \frac{1}{\sqrt{2}}(|0011\rangle + |1100\rangle).$$

In the protocol, Alice, a boss, wants to send a secret key to two agents, Bob and Charlie, but the secret key can be deduced only when the two agents work collaboratively. Zhang's QSS scheme includes the following six steps.

(Z_1) Alice generates a random $4n$ bit string X and a random $4n$ trit string Y.
(Z_2) Based on the values of X and Y, Alice generates a sequence of product states $\{w_x, w_y, w_z\}$. If $Y = 0$, then the set $\{w_x, w_y\}$ is chosen; if $Y = 1$, then $\{w_y, w_z\}$ is chosen; and if $Y = 2$, $\{w_z, w_x\}$ is chosen. Then, based on the value of X, Alice generates the corresponding w_x, w_y, w_z. For example, if $Y = 1$ and $X = 0$ then w_y, the first element in $\{w_y, w_z\}$, is generated; if $Y = 1$ and $X = 1$ then the second element w_z in the same set is generated. Finally, Alice sends the $4n$ states ($4 \times 4n$ photons) to Bob after she has generated these states.
(Z_3) After receiving these $4n$ states, Bob performs a permutation on two arbitrary photons in each state. Then, he sends the permuted $4n$ states to Charlie.
(Z_4) When Charlie receives the permuted states, he randomly selects either the Z-basis or X-basis to measure these states and also records the measurement results, where $Z = \{|0\rangle, |1\rangle\}$ and $X = \{|+\rangle, |-\rangle\}$.
(Z_5) Alice randomly chooses half of these $4n$ states for the eavesdropping check. For these chosen states, Bob and Charlie have to announce the corresponding permutation and the measurement result respectively. If the error rate exceeds a predetermined threshold, then communication is aborted. Otherwise, Alice announces Y.
(Z_6) After obtaining Y, Bob and Charlie can cooperatively recover n-bit shared key.

2.2 Sun et al.'s intercept-resend attack and modification

In this section, Sun et al.'s intercept-resend attack on Zhang's scheme is reviewed and their improvement is also given.

2.2.1 Intercept-resend attack

Sun et al. assume that Charlie is an inside attacker with the ability to generate perfect channels, and he attempts to obtain the secret key without Bob's assistance. At first, Charlie intercepts the photons generated by Alice in Step (Z_2) in Zhang's QSS and then forges $|0011\rangle_{1234}$ and sends it to Bob through a perfect channel. In Step (Z_4), Charlie receives the permuted photons, and measures them in the Z-basis to reveal Bob's permutations. Accordingly, Charlie performs the same permutations on the intercepted photons and measures them. He then can obtain the secret key without Bob's assistance.

2.2.2 Sun et al.'s improved scheme

To avoid the intercept-resend attack, Sun et al. improved Zhang's QSS scheme as follows:

- (S_1) Alice generates a random $4n + m$ bit string X and a random $4n + m$ trit string Y, where m is the number of bits for the eavesdropping check.
- (S_2) Alice generates states according to Step (Z_2) in Zhang's protocol. Then, Alice sends the $4n + m$ states to Bob after she has encoded these photons.
- (S_3) After receiving the $4n + m$ states, Bob replies "OK" to Alice. Alice randomly chooses m states for the eavesdropping check. Bob randomly uses the Z-basis or X-basis to measure them and then replies with the measurement results. If the error rate of the measurement exceeds a threshold, the communication will be aborted. Otherwise, they continue the next step (S_4).

The remaining steps (S_4)–(S_7) of Sun et al.'s scheme are the same as (Z_3)–(Z_6) in Zhang's QSS scheme. Although the modified QSS protocol can avoid the intercept-resend attack, $4m$ photons are transmitted and 4 classical transmissions are added in the eavesdropping check to guarantee the security of the photons transmission between Alice and Bob. The qubit efficiency of Sun et al.'s QSS protocol is decreased from $\frac{1}{16}$ to $\frac{1}{32}$ in the Sun et al.'s modification to avoid the intercept-resend attack.

3 The enhanced scheme

This section proposes an improvement on Zhang's QSS by deliberately introducing collective-rotation noise to the received photons in order to avoid the intercept-resend attack. As described earlier, $|0011\rangle_{1234}$ is not a DF state. Thus the state will be changed under the interference of collective-rotation noise. Once it is distorted by the noise, the attacker cannot exactly obtain Bob's permutations. Based on this observation, our proposed enhancement deliberately introduces collective-rotation noise into the received quantum states to prevent intercept-resend attack on Zhang's QSS. Consequently, as compared to Sun et al.'s improvement on Zhang's QSS, the efficiency in our QSS protocol is enhanced. The improvement is performed on Step (Z_3) in Zhang's QSS. The other steps are the same as in the original protocol.

(Z_3) $\rightarrow$ (Z_3') When Bob receives the $4n$ states, he introduces random collective-rotation noise by performing the operation U_r on each state, where $U_r = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$, and α is a random parameter $\left(0 \leq \alpha \leq \frac{\pi}{2}\right)$. After Bob deliberately introduces collective-rotation noise to the received photons, he performs a permutation on two arbitrary photons in each state and then sends the permuted $4n$ states to Charlie.

In Step (Z_3'), the deliberately introduced collective-rotation noise does not affect the initial state of the photons because they are in a DF subspace [5–8]. However, the forged state $|0011\rangle_{1234}$, not a DF state, will change to the state in Eq. 7 below under the interference of the deliberately introduced collective-rotation noise. The attacker

may not be able to infer Bob's permutations by using the Z-basis to measure these states (an attack described in Sect. 2.2.1) because he cannot determine whether the measurement results are correct or not. A more detailed security analysis is available in Sect. 4.2.

$$\begin{aligned}&\cos^4\alpha\,|0011\rangle_{1234} - \cos^3\alpha\sin\alpha\,(|0001\rangle + |0010\rangle - |0111\rangle - |1011\rangle)_{1234}\\&+\sin^4\alpha\,|1100\rangle_{1234} + \cos\alpha\sin^3\alpha\,(|0100\rangle + |1000\rangle - |1101\rangle - |1110\rangle)_{1234}\\&+\cos^2\alpha\sin^2\alpha\,(|0000\rangle - |0101\rangle - |0110\rangle - |1001\rangle - |1010\rangle + |1111\rangle)_{1234}\end{aligned} \tag{7}$$

4 Performance analyses

In this section, we analyze the efficiency and security of our improved QSS.

4.1 Efficiency analysis

Table 1 compares the cost and efficiency of Zhang's and Sun et al.'s QSS [15,18] with our QSS. In the public discussion step in the protocols, let us assume here that half of the transmitted states are used for detecting the presence of eavesdroppers.

In Zhang's QSS [15], Alice has to generate $4n$product states (i.e., $16n$ qubits), and each state can carry one information bit. Since the measurement results are inconclusive in the protocol (i.e., a product state can be correctly decoded with probability 50%), and also half of these states are used for eavesdropper checking, the qubit efficiency of Zhang's QSS is $\frac{4n}{4n\times 4}\times\frac{1}{2}\times\frac{1}{2}=\frac{1}{16}$.

In Sun et al.'s protocol [18], Alice has to prepare $8n$ states, and each state can carry one information bit. Two rounds of public discussion are used in Sun et al.'s QSS. Thus, the qubit efficiency of Sun et al.'s protocol is $\frac{8n}{8n\times 4}\times\frac{1}{2}\times\frac{1}{2}\times\frac{1}{2}=\frac{1}{32}$.

By deliberately introducing collective-rotation noise to the received quanta, our modified QSS improves the qubit efficiency of Sun et al.'s QSS protocol from $\frac{1}{32}$ to $\frac{1}{16}$.

4.2 Security analysis

This section analyzes the security of the enhanced scheme in detail. The security analysis of our protocol is divided into two parts. The first part deals with the security

Table 1 Comparison of QSS protocols

	Zhang's protocol	Sun et al.'s protocol	Proposed protocol
Intercept-resend attack	Yes	No	No
Number of qubits	$4(4n)$	$4(4n+m)=4(8n)$	$4(4n)$
Qubit efficiency	$\frac{1}{16}$	$\frac{1}{32}$	$\frac{1}{16}$
Public discussion	1	2	1

analysis against ordinary eavesdropping as described in Zhang's QSS. The second part considers the special intercept-resend attack proposed by Sun et al. using the state $|0011\rangle_{1234}$.

(1) Security against ordinary eavesdropping

As described in [15], Zhang's protocol, based on the quantum states in DF space, is not only immune to collective noise, but also secure against ordinary eavesdropping. Our enhancement is based on the deliberate introduction of collective-rotation noise into the noise immune quantum states. Thus, the enhanced protocol is also secure against the ordinary eavesdropping.

(2) Security against the intercept-resend attack by using the special state $|0011\rangle_{1234}$

In order to reveal Bob's permutation, Charlie, an inside attacker, upon intercepting the photons from Alice to Bob, sends $|0011\rangle_{1234}$ to Bob. Bob implements the operations, U_r and P_{ij} where $i \neq j$, $1 \leqq i, j \leqq 4$, on photons in the Step (Z'$_3$), where U_r represents the introduction of collective-rotation noise to the photons and P_{ij} denotes the permutation on photons i and j. There are six permutations for Bob to choose (i.e., $C_2^4 = 6$). As described in [18], these six permutations can be classified into three groups since $P_{12} = P_{34}$, $P_{13} = P_{24}$ and $P_{14} = P_{23}$ (see also Eqs. 5 and 6). Therefore, the security analysis considers only the permutations: P_{12}, P_{23} and P_{24}.

Let us first compute the average probability for each state to be measured by Charlie. Given that $0 \leq \alpha \leq \frac{\pi}{2}$, based on Eq. 7, the average probability for Charlie to get the measurement result $|0011\rangle_{1234}$ (or $|1100\rangle_{1234}$) is $\frac{35}{128}$, as shown in Eq. 8. Similarly, that for $|0001\rangle$, $|0010\rangle$, $|0111\rangle$, $|1011\rangle$, $|0100\rangle$, $|1000\rangle$, $|1101\rangle$ or $|1110\rangle$ is $\frac{5}{128}$, and with the probability of $\frac{3}{128}$, Charlie's measurement result could be one of the following: $|0000\rangle$, $|0101\rangle$, $|0110\rangle$, $|1001\rangle$, $|1010\rangle$ or $|1111\rangle$.

$$\frac{\int_0^{\frac{\pi}{2}} \left(\cos^4\alpha\right)^2 d\alpha}{\frac{\pi}{2}} = \frac{\int_0^{\frac{\pi}{2}} \left(\sin^4\alpha\right)^2 d\alpha}{\frac{\pi}{2}} = \frac{35}{128} \tag{8}$$

Table 2 shows the relationship between Bob's permutations and Charlie's measurement results. We would like to analyze the strategy for Charlie to determine Bob's permutation in performing the special attack. If Bob performs the permutation P_{12}, then the measurement results, $|0011\rangle_{1234}$ and $|1100\rangle_{1234}$, have the higher probability $\left(\frac{35}{128}\right)$ than the other states. Similarly, if Bob implements the permutation P_{23}(or P_{24}), then the measurement results $\{|0101\rangle_{1234}$ and $|1010\rangle_{1234}\}$ (or $\{|0110\rangle_{1234}$ and $|1001\rangle_{1234}\}$) have the higher probability (see also Table 2). Therefore, if the measurement result of Charlie is $|0011\rangle_{1234}$ or $|1100\rangle_{1234}$, then Charlie will treat Bob's permutation as P_{12}. Similarly, if Charlie's measurement result is $\{|0101\rangle_{1234}$, $|1010\rangle_{1234}\}$ or $\{|0110\rangle_{1234}$, $|1001\rangle_{1234}\}$, then Charlie decides that Bob's permutation is P_{23} or P_{24} respectively. On the other hand, if the measurement result of Charlie is one of the remaining states, then Charlie could only guess Bob's permutation randomly because the permutations, P_{12}, $P_{23}$and P_{24}, appear equally likely (see also Table 3).

Table 3 shows the possible decision for Charlie to choose the permutation of Bob based on his measurement results. Thus, if Bob introduces the collective-rotation

Table 2 The relationship between Bob's permutations and Charlie's measurement results

Bob's permutations	Average probability	Charlie's measurement results
P_{12}	$\frac{35}{128}$	$\|0011\rangle$ or $\|1100\rangle$
	$\frac{5}{128}$	$\|0001\rangle, \|0010\rangle, \|1000\rangle, \|0100\rangle, \|1011\rangle, \|0111\rangle, \|1101\rangle$ or $\|1110\rangle$
	$\frac{3}{128}$	$\|0000\rangle, \|1111\rangle, \|1001\rangle, \|0110\rangle, \|1010\rangle$ or $\|0101\rangle$
P_{23}	$\frac{35}{128}$	$\|0101\rangle$ or $\|1010\rangle$
	$\frac{5}{128}$	$\|0001\rangle, \|0010\rangle, \|1000\rangle, \|0100\rangle, \|1011\rangle, \|0111\rangle, \|1101\rangle$ or $\|1110\rangle$
	$\frac{3}{128}$	$\|0000\rangle, \|1111\rangle, \|0011\rangle, \|1100\rangle, \|0110\rangle$ or $\|1001\rangle$
P_{24}	$\frac{35}{128}$	$\|0110\rangle$ or $\|1001\rangle$
	$\frac{5}{128}$	$\|0001\rangle, \|0010\rangle, \|1000\rangle, \|0100\rangle, \|1011\rangle, \|0111\rangle, \|1101\rangle$ or $\|1110\rangle$
	$\frac{3}{128}$	$\|0000\rangle, \|1111\rangle, \|0101\rangle, \|1010\rangle, \|0011\rangle$ or $\|1100\rangle$

Table 3 The possible decision for Charlie to choose the permutation of Bob based on his measurement results

	P_{12}	P_{23}	P_{24}
$\|0000\rangle$	1/3	1/3	1/3
$\|0001\rangle$	1/3	1/3	1/3
$\|0010\rangle$	1/3	1/3	1/3
$\|0011\rangle$	1	0	0
$\|0100\rangle$	1/3	1/3	1/3
$\|0101\rangle$	0	1	0
$\|0110\rangle$	0	0	1
$\|0111\rangle$	1/3	1/3	1/3
$\|1000\rangle$	1/3	1/3	1/3
$\|1001\rangle$	0	0	1
$\|1010\rangle$	0	1	0
$\|1011\rangle$	1/3	1/3	1/3
$\|1100\rangle$	1	0	0
$\|1101\rangle$	1/3	1/3	1/3
$\|1110\rangle$	1/3	1/3	1/3
$\|1111\rangle$	1/3	1/3	1/3

noise to $|0011\rangle_{1234}$ and then performs a permutation on two arbitrary photons, then the probability for Charlie to obtain Bob's permutation can be computed in the following (refer also to Tables 2, 3). If the measurement result of Charlie is $\{|0011\rangle_{1234}$ and $|1100\rangle_{1234}\}$, $\{|0101\rangle_{1234}$ and $|1010\rangle_{1234}\}$ or $\{|0110\rangle_{1234}$ and $|1001\rangle_{1234}\}$, then Charlie can correctly obtain Bob's permutation with probability $\frac{35}{128} \times 2 = \frac{35}{64}$. On the other hand, if the measurement result is one of the remaining states, then Charlie guesses Bob's permutation randomly. Charlie derives the correct permutation with probability $\left(\frac{3}{128} \times 2 + \frac{5}{128} \times 8\right) \times \frac{1}{3} = \frac{23}{192}$. Therefore, the probability for Charlie to correctly obtain the permutation of Bob is $\frac{23}{192} + \frac{35}{64} = \frac{2}{3}$.

Based on the above observation, we further analyze the probability for Charlie to pass the eavesdropping check in the public discussion as follows. Charlie can always pass the eavesdropping check if he can correctly obtain Bob's permutation. Thus, the probability for this situation is $\frac{2}{3} \times 1 = \frac{2}{3}$. On the other hand, if Charlie incorrectly derives Bob's permutation, then he still can pass the eavesdropping check with probability $\left(1 - \frac{2}{3}\right) \times \frac{1}{2} = \frac{1}{6}$. Because any two of $\{w_x, w_y, w_z\}$ are nonorthogonal, the measurement results in any two states of $\{w_x, w_y, w_z\}$ are the same with the probability of $\frac{1}{2}$ (see also Eq. 5). In other words, though Charlie incorrectly permutes these intercepted photons, still he obtains the correct measurement result with the probability of $\frac{1}{2}$.

To summarize, the probability for Charlie to pass the eavesdropping check is $\frac{2}{3} + \frac{1}{6} = \frac{5}{6}$. Therefore, for $2n$ states, Charlie can be detected in the public discussion with probability $1 - \left(\frac{5}{6}\right)^{2n}$. When n is large enough, the probability for Charlie to be detected in the public discussion converges to 1. Thus, the enhanced scheme is secure under the special intercept-resend attack proposed by Sun et al.

5 Conclusion

In order to avoid a special intercept-resend attack, Sun et al.'s modification on Zhang's QSS scheme performs an extra eavesdropping check to guarantee the security of the photons transmission between Alice and Bob. As a result, the quantum efficiency as well as the protocol efficiency is reduced. The contribution of this paper is to deliberately introduce collective-rotation noise to a noise-immune DF state to prevent the attack. The newly enhanced Zhang's QSS protocol not only avoids Sun et al.'s special intercept-resend attack but also doubles the quantum efficiency. The security analysis shows that the insider attacker (Charlie) can be detected in the public discussion with a very high probability.

Acknowledgments The authors would like to thank the anonymous reviewers' valuable comments and suggestions on the improvement of this article. This article is financially supported by the National Science Council of Republic of China, under Contract No. NSC 98-2221-E-006-097-MY3.

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, pp. 175–179 (1984)
2. Dong, L., Xiu, X.M., Gao, Y.J., Chi, F.: Deterministic secure quantum communication against collective-dephasing noise by using EPR pairs and auxiliary photons. Opt. Commun. **282**, 1688–1690 (2009)
3. Li, X.H., Deng, F.G., Zhou, H.Y.: Efficient quantum key distribution over a collective noise channel. Phys. Rev. A **78**, 022321 (2008)
4. Xiu, X.M., Dong, L., Gao, Y.J., Chi, F.: Quantum key distribution protocols with six-photon states against collective noise. Opt. Commun. **282**, 4171–4174 (2009)
5. Zanardi, P., Rasstti, M.: Noiseless quantum codes. Phys. Rev. Lett. **79**, 3306–3309 (1997)
6. Knill, E., Laflamme, R., Viola, L.: Theory of quantum error correction for general noise. Phys. Rev. Lett. **84**, 2525–2528 (2000)

7. Kempe, J., Bacon, D., Lidar, D.A., Whaley, K.B.: Theory of decoherence-free fault-tolerant universal quantum computation. Phys. Rev. A **63**, 042307 (2001)
8. Lidar, D.A., Chuang, I.L., Whaley, K.B.: Decoherence-free subspaces for quantum computation. Phys. Rev. Lett. **81**, 2594–2597 (1998)
9. Lidar, D.A., Bacon, D., Kempe, J., Whaley, K.B.: Protecting quantum information encoded in decoherence-free states against exchange errors. Phys. Rev. A **61**, 052307 (2000)
10. Walton, Z.D., Abouraddy, A.F., Sergienko, A.V., Saleh, B.E.A., Teich, M.C.: Decoherence-free subspaces in quantum key distribution. Phys. Rev. Lett. **91**, 087901 (2003)
11. Boileau, J.C., Gottesman, D., Laflamme, R., Poulin, D., Spekkens, R.W.: Robust polarization-based quantum key distribution over a collective-noise channel. Phys. Rev. Lett. **92**, 017901 (2004)
12. Bourennane, M., Eibl, M., Gaertner, S., Kurtsiefer, C.: Decoherence-free quantum information processing with four-photon entangled states. Phys. Rev. Lett. **92**, 107901 (2004)
13. Yamamoto, T., Shimamura, J., Ozdemir, S.K., Koashi, M., Imoto, N.: Faithful qubit distribution assisted by one additional qubit against collective noise. Phys. Rev. Lett. **95**, 040503 (2005)
14. Wang, X.B.: Fault tolerant quantum key distribution protocol with collective random unitary noise. Phys. Rev. A **72**, 050304(R) (2005)
15. Zhang, Z.J.: Robust multiparty quantum secret key sharing over two collective-noise channels. Phys. A **361**, 233–238 (2006)
16. Li, X.H., Deng, F.G., Zhou, H.Y.: Faithful qubit transmission against collective noise without ancillary qubits. Appl. Phys. Lett. **91**, 144101 (2007)
17. 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)
18. Sun, Y., Wen, Q.Y., Zhu, F.C.: Improving the multiparty quantum secret sharing over two collective-noise channels against insider attack. Opt. Commun. **283**, 181–183 (2010)