Robust variations of the Bennett-Brassard 1984 protocol against collective noise

Ying Sun,[1,2,*] Qiao-Yan Wen,[1] Fei Gao,[1] and Fu-Chen Zhu[3]
[1]*State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[2]*State Key Laboratory of Integrated Services Network, Xidian University, Xi'an 710071, China*
[3]*National Laboratory for Modern Communications, P.O. Box 810, Chengdu 610041, China*
(Received 23 May 2009; published 22 September 2009)

The security of the decoherence-free version of the Bennett-Brassard 1984 (BB84) protocol [A. Cabello, Phys. Rev. A **75**, 020301 (2007)] is analyzed and shown to be vulnerable under the intercept-resend attack. We propose two improved versions of this protocol. Both improvements remain the performance of robustness against collective noise and refuse the security flaw. Especially, the second improvement, which is called four-qubit decoherence-free (DF) BB84 protocol, not only remains all characteristics of the original protocol but also has a higher efficiency. We also give a detailed security proof of four-qubit DF BB84 protocol.

DOI: 10.1103/PhysRevA.80.032321 PACS number(s): 03.67.Dd

I. INTRODUCTION

Quantum mechanics allows the distribution of cryptographic keys whose security is based on the laws of physics instead of the difficulty of solving mathematical problems [1,2]. Since the pioneering work proposed by Bennett and Brassard [Bennett-Brassard 1984 protocol (BB84 protocol)] [2], quantum cryptography had attracted a great deal of attention [3–10]. So far, it has been one of the most promising applications of quantum information processing. However, qubit states are very fragile and tend to be destroyed by decoherence due to the unwanted coupling with the environment [11]. Such uncontrollable influences cause noise or errors in the communication and thus reduce the advantages of quantum cryptography protocols. For example, in quantum communication, the qubits carried by polarized photons which are successively sent via the optical fiber will experience the birefringence. If left untreated, this would result in an unacceptably high error rate and cut down the efficiency and security. It is well known that we can add redundancy when encoding quantum information in order to detect and correct the errors by many strategies such as quantum error correction [12–14], purification of noisy entanglement [15,16], and quantum error rejection [17–19]. However, they only work well when the interaction with the environment is weak enough and the qubits are affected with a low probability.

Fortunately, not all quantum states are equally fragile when interacting with the environment. When the photons are transmitted in some medium (e.g., the optical fiber), a particularly relevant symmetry arising when the environment couples with the qubits without distinguishing between them results in the so-called collective noise. The transformation of collective noise can be described by an unitary operator $U(t)$, where t denotes the time of transmission and means a temporal dependence. As mentioned in Ref. [20], if the time delay between the photons is small enough, the effect of collective noise on a N-qubit state can be modeled approximately as

$$\rho_N \Rightarrow [U(t)]^{\otimes N} \rho_N [U(t)^{\dagger}]^{\otimes N}, \tag{1}$$

where $[U(t)]^{\otimes N} = U(t) \otimes \cdots \otimes U(t)$ denotes the tensor product of N unitary transformations $U(t)$. In fact, there exist quantum states which are invariant under collective noise no matter how strong the interaction is. These states are called decoherence-free (DF) states and have been applied to the protection of quantum information in many researches [20–28]. The following equation shows the invariance property of DF states:

$$\rho_N = [U(t)]^{\otimes N} \rho_N [U(t)^{\dagger}]^{\otimes N}. \tag{2}$$

This immunity against $[U(t)]^{\otimes N}$ has been demonstrated in some experiences [29–31].

Recently, Boileau *et al.* proposed a quantum key distribution (QKD) protocol [26], which is in essence a DF version of Bennett 1992 protocol (B92) protocol [3], over the collective-noise channel using DF subspace and DF subsystem, respectively. Then, Cabello implemented a variation of BB84 protocol, which is robust against collective noise, in six-qubit DF subspaces [32]. Except for its robustness against collective noise, the DF version of BB84 protocol has two interesting properties which make it essentially different from the original scheme. (a) All four states used in this protocol can be obtained by permuting the qubits of a single DF state. (b) Two orthogonal states in either base can be distinguished reliably by an alternative fixed sequence of single-qubit measurements. These properties make the protocol easy to be implemented under current technologies.

However, an eavesdropper, Eve, can steal some information of the key distributed in this protocol by intercept-resend (IR) attack without being detected. In this paper, we will show that how the DF version of BB84 protocol proposed in Ref. [32] (hereinafter referred to as DF BB84 protocol) runs the risk of leaking information out to Eve and then give two improved versions which can distribute keys over the collective-noise channel in a secure and efficient manner.

*sunshiny2007@yahoo.cn

II. VULNERABILITY OF DF BB84 PROTOCOL UNDER IR ATTACK

In order to describe the attack strategy clearly, we review DF BB84 protocol first. In this protocol, two orthogonal bases are $\{|\hat{0}\rangle,|\hat{1}\rangle\}$ and $\{|\hat{\oplus}\rangle,|\hat{\ominus}\rangle\}$, respectively. These four states are in the forms of

$$|\hat{0}\rangle = |\psi^-\rangle_{12} \otimes \frac{1}{2\sqrt{3}}(2|0011\rangle - |0101\rangle - |0110\rangle - |1001\rangle - |1010\rangle + 2|1100\rangle)_{3456}, \tag{3a}$$

$$|\hat{1}\rangle = P_{1\leftrightarrow 3,2\leftrightarrow 4}|\hat{0}\rangle = |\psi^-\rangle_{34} \otimes \frac{1}{2\sqrt{3}}(2|0011\rangle - |0101\rangle - |0110\rangle - |1001\rangle - |1010\rangle + 2|1100\rangle)_{1256}, \tag{3b}$$

$$|\hat{\oplus}\rangle = P_{1\leftrightarrow 3}|\hat{0}\rangle = |\psi^-\rangle_{32} \otimes \frac{1}{2\sqrt{3}}(2|0011\rangle - |0101\rangle - |0110\rangle - |1001\rangle - |1010\rangle + 2|1100\rangle)_{1456}, \tag{3c}$$

$$|\hat{\ominus}\rangle = P_{2\leftrightarrow 4}|\hat{0}\rangle = |\psi^-\rangle_{14} \otimes \frac{1}{2\sqrt{3}}(2|0011\rangle - |0101\rangle - |0110\rangle - |1001\rangle - |1010\rangle + 2|1100\rangle)_{3256}, \tag{3d}$$

where $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ and $P_{i\leftrightarrow j}$ denotes permuting the ith qubit and the jth one in the quantum state. Because of the features shown above, it is obvious that only the state $|\hat{0}\rangle$ needs a setup which can be designed by combining the apparatuses in Ref. [27] and the other three states can be prepared by permuting the outputs of the setup for $|\hat{0}\rangle$ [33]. When the receiver Bob receives the six-qubit states randomly prepared by the sender Alice, he measures every received state in one of the measurement sequences $\{Z_1Z_2X_3X_4Z_5Z_6, X_1Z_2Z_3X_4Z_5Z_6\}$ at random. Either measurement sequence is formed by six single-qubit measurements, where $X_i(Z_i)(i=1,\ldots,6)$ denotes measuring the ith qubit in X basis (Z basis). Bob records his measurement results $\{|\hat{0}\rangle,|\hat{\oplus}\rangle\}$ and $\{|\hat{1}\rangle,|\hat{\ominus}\rangle\}$ as 0 and 1, respectively. At last, if and only if the measurement sequences chosen by Bob are coincident with Alice's preparations, the corresponding recorded bits can be kept for the raw key.

From the fixed sequences of single-qubit measurements used in DF BB84 protocol, $Z_1\mathbf{Z_2}X_3\mathbf{X_4Z_5Z_6}$ and $X_1\mathbf{Z_2}Z_3\mathbf{X_4Z_5Z_6}$, we can find that four single-qubit measurements, which are marked in bold, remain unaltered. So Eve can make use of this phenomenon to get some valuable information and escape from being detected. If she intercepts all the states sent from Alice and only measures the qubits with $Z_2X_4Z_5Z_6$ except for the first and the third ones in each state, neither of the communicators can discover her attacks.

TABLE I. All possible measurement results obtained by Eve with $Z_2X_4Z_5Z_6$ in her attack.

The original state	The possible results
$\|\hat{0}\rangle$	$\|0\rangle_2\|\pm\rangle_4\|0\rangle_5\|0\rangle_6$, $\|1\rangle_2\|\pm\rangle_4\|1\rangle_5\|1\rangle_6$, $\|0\rangle_2\|\pm\rangle_4\|1\rangle_5\|1\rangle_6$, $\|1\rangle_2\|\pm\rangle_4\|0\rangle_5\|0\rangle_6$, $\|0\rangle_2\|\pm\rangle_4\|0\rangle_5\|1\rangle_6$, $\|1\rangle_2\|\pm\rangle_4\|0\rangle_5\|1\rangle_6$, $\|0\rangle_2\|\pm\rangle_4\|1\rangle_5\|0\rangle_6$, $\|1\rangle_2\|\pm\rangle_4\|1\rangle_5\|0\rangle_6$.
$\|\hat{1}\rangle$	$\|0\rangle_2\|\pm\rangle_4\|1\rangle_5\|1\rangle_6$, $\|1\rangle_2\|\pm\rangle_4\|0\rangle_5\|0\rangle_6$, $\|0\rangle_2\|\pm\rangle_4\|0\rangle_5\|1\rangle_6$, $\|1\rangle_2\|\pm\rangle_4\|0\rangle_5\|1\rangle_6$, $\|0\rangle_2\|\pm\rangle_4\|1\rangle_5\|0\rangle_6$, $\|1\rangle_2\|\pm\rangle_4\|1\rangle_5\|0\rangle_6$.
$\|\hat{\oplus}\rangle$	$\|0\rangle_2\|\pm\rangle_4\|0\rangle_5\|0\rangle_6$, $\|1\rangle_2\|\pm\rangle_4\|1\rangle_5\|1\rangle_6$, $\|0\rangle_2\|\pm\rangle_4\|1\rangle_5\|1\rangle_6$, $\|1\rangle_2\|\pm\rangle_4\|0\rangle_5\|0\rangle_6$, $\|0\rangle_2\|\pm\rangle_4\|0\rangle_5\|1\rangle_6$, $\|1\rangle_2\|\pm\rangle_4\|0\rangle_5\|1\rangle_6$, $\|0\rangle_2\|\pm\rangle_4\|1\rangle_5\|0\rangle_6$, $\|1\rangle_2\|\pm\rangle_4\|1\rangle_5\|0\rangle_6$.
$\|\hat{\ominus}\rangle$	$\|0\rangle_2\|\pm\rangle_4\|1\rangle_5\|1\rangle_6$, $\|1\rangle_2\|\pm\rangle_4\|0\rangle_5\|0\rangle_6$, $\|0\rangle_2\|\pm\rangle_4\|0\rangle_5\|1\rangle_6$, $\|1\rangle_2\|\pm\rangle_4\|0\rangle_5\|1\rangle_6$, $\|0\rangle_2\|\pm\rangle_4\|1\rangle_5\|0\rangle_6$, $\|1\rangle_2\|\pm\rangle_4\|1\rangle_5\|0\rangle_6$.

All the possible measurement results obtained by Eve in this attack are shown in Table I. From Table I, we can see that when Alice sends $|\hat{0}\rangle$ and $|\hat{\oplus}\rangle$, Eve may obtain some results which will never appear in the cases $|\hat{1}\rangle$ and $|\hat{\ominus}\rangle$, i.e., $|0\rangle_2|\pm\rangle_4|0\rangle_5|0\rangle_6$ and $|1\rangle_2|\pm\rangle_4|1\rangle_5|1\rangle_6$. Consequently, we obtain the essential reason of information leakage

$$\rho^0_{2456} \neq \rho^1_{2456}, \quad \rho^{0'}_{2456} \neq \rho^{1'}_{2456}, \tag{4}$$

where ρ^0_{2456}, ρ^1_{2456}, $\rho^{0'}_{2456}$, and $\rho^{1'}_{2456}$ denote the reduced density matrices of quantum systems shown in Eqs. (3), respectively. If expressing $|\hat{0}\rangle$ and $|\hat{\oplus}\rangle$ in $Z_1Z_2X_3X_4Z_5Z_6$ or $X_1Z_2Z_3X_4Z_5Z_6$, we can find that $|0\rangle_2|\pm\rangle_4|0\rangle_5|0\rangle_6$ and $|1\rangle_2|\pm\rangle_4|1\rangle_5|1\rangle_6$ appear with a probability of 2/5 in either $|\hat{0}\rangle$ or $|\hat{\oplus}\rangle$. Thus, if Eve attains anyone of these four measurement results, she can make sure that Bob's record will be "0" in the case that he chooses the right base sequence. Since Alice sends $|\hat{0}\rangle$ and $|\hat{\oplus}\rangle$ with the probability of 1/2, Eve can gain the certain information with a probability of $\frac{1}{2}\times\frac{2}{5}=\frac{1}{5}$. Although Eve's attacking action disturbs the transmitted six-qubit DF states, they collapse to the tensor product states which are also the possible results Bob will obtain from his measurements no matter which sequence of single-qubit measurements he chooses.

III. FIRST IMPROVEMENT

Now we give an improved version of DF BB84 protocol. Considering the relationship among the states ($|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$) used in BB84 protocol, we keep $\{|\hat{0}\rangle,|\hat{1}\rangle\}$ unchanged and select another orthogonal basis $\{|\widehat{\varphi_0}\rangle,|\widehat{\varphi_1}\rangle\}$ [shown in Eqs. (5)] to replace $\{|\hat{\oplus}\rangle,|\hat{\ominus}\rangle\}$,

$$|\widehat{\varphi_0}\rangle = \frac{1}{\sqrt{2}}(|\hat{0}\rangle + |\hat{1}\rangle), \tag{5a}$$

$$|\widehat{\varphi_1}\rangle = \frac{1}{\sqrt{2}}(|\hat{0}\rangle - |\hat{1}\rangle). \tag{5b}$$

In order to reserve the virtues of DF BB84 protocol, we also want to use single-qubit measurements to distinguish the orthogonal states. But the states $|\widehat{\varphi_0}\rangle$ and $|\widehat{\varphi_1}\rangle$ are not distinguishable using a fixed sequence of single-qubit measurements. Fortunately, it has been proven that any two orthogonal states can be distinguished by single-qubit measurements assisted by local operation and classical communication (LOCC) [34]. It means that there are some conditioned sequences of single-qubit measurements which allow us to reliably distinguish between $|\widehat{\varphi_0}\rangle$ and $|\widehat{\varphi_1}\rangle$. In these sequences, what is measured on one qubit needs to depend on the result of a prior measurement on another qubit in the same state. We find these sequences of single-qubit measurements basing on the facts expressed in Eqs. (6) and then show them in Table II in detail.

$$\begin{aligned}|\widehat{\varphi_0}\rangle = \frac{1}{4\sqrt{3}}\{&|0\rangle|+\rangle|0\rangle[|+\rangle(2|11\rangle - |01\rangle - |10\rangle) + |-\rangle(|01\rangle \\ &+ |10\rangle)] + |0\rangle|-\rangle|0\rangle[|+\rangle(|01\rangle + |10\rangle) \\ &+ |-\rangle(-2|11\rangle - |01\rangle - |10\rangle)] + |1\rangle|+\rangle|1\rangle[|+\rangle(-2|11\rangle \\ &+ |01\rangle + |10\rangle) + |-\rangle(|01\rangle + |10\rangle)] + |1\rangle|-\rangle|1\rangle[|+\rangle(|01\rangle \\ &+ |10\rangle) + |-\rangle(2|11\rangle + |01\rangle + |10\rangle)] + |0\rangle|+\rangle|1\rangle[|+\rangle(|a_0\rangle \\ &\times|c_0\rangle + |a_1\rangle|d_1\rangle)] - |-\rangle(|+\rangle|+\rangle + |-\rangle|-\rangle)] + |0\rangle|-\rangle|1\rangle \\ &\times[-|+\rangle(|+\rangle|+\rangle + |-\rangle|-\rangle) + |-\rangle(|b_0\rangle|e_0\rangle + |b_1\rangle|f_1\rangle)] \\ &+ |1\rangle|+\rangle|0\rangle[|+\rangle(|+\rangle|-\rangle + |-\rangle|+\rangle) + |-\rangle(|a_0\rangle|e_0\rangle + |a_1\rangle \\ &\times|f_1\rangle)] + |1\rangle|-\rangle|0\rangle[|+\rangle(|b_0\rangle|c_0\rangle + |b_1\rangle|d_1\rangle) + |-\rangle(|+\rangle \\ &\times|-\rangle + |-\rangle|+\rangle)]\},\end{aligned} \tag{6a}$$

$$\begin{aligned}|\widehat{\varphi_1}\rangle = \frac{1}{4\sqrt{3}}\{&2|0\rangle|+\rangle|0\rangle|-\rangle|11\rangle - 2|0\rangle|-\rangle|0\rangle|+\rangle|11\rangle + 2|1\rangle|+\rangle \\ &\times|1\rangle|-\rangle|00\rangle - 2|1\rangle|-\rangle|1\rangle|+\rangle|00\rangle + |0\rangle|+\rangle|1\rangle[|+\rangle(|a_0\rangle \\ &\times|c_1\rangle + |a_1\rangle|d_0\rangle) - |-\rangle|+\rangle|-\rangle] + |0\rangle|-\rangle|1\rangle[-|+\rangle|-\rangle \\ &\times|+\rangle + |-\rangle(|b_0\rangle|e_1\rangle + |b_1\rangle|f_0\rangle)] + |1\rangle|+\rangle|0\rangle[-|+\rangle|-\rangle \\ &\times|-\rangle + |-\rangle(|a_0\rangle|e_1\rangle + |a_1\rangle|f_0\rangle)] + |1\rangle|-\rangle|0\rangle[|+\rangle \\ &\times(|b_0\rangle|c_1\rangle + |b_1\rangle|d_0\rangle) - |-\rangle|+\rangle|+\rangle]\},\end{aligned} \tag{6b}$$

where

$$|a_0\rangle = \frac{p}{p^2+q^2}|0\rangle + \frac{q}{p^2+q^2}|1\rangle,$$

$$|a_1\rangle = \frac{q}{p^2+q^2}|0\rangle - \frac{p}{p^2+q^2}|1\rangle,$$

TABLE II. The conditioned sequences of single-qubit measurements used to distinguish $|\widehat{\varphi_0}\rangle$ and $|\widehat{\varphi_1}\rangle$. B, R, and C are used to denote basis, result, and conclusion for short, respectively.

B	R	B	R	C
Z_5Z_6	$\|0\rangle\|+\rangle\|0\rangle\|+\rangle$ $\|0\rangle\|-\rangle\|0\rangle\|-\rangle$		$\|11\rangle,\|01\rangle,\|10\rangle$	
	$\|1\rangle\|+\rangle\|1\rangle\|+\rangle$ $\|1\rangle\|-\rangle\|1\rangle\|-\rangle$		$\|00\rangle,\|01\rangle,\|10\rangle$	$\|\widehat{\varphi_0}\rangle$
	$\|0\rangle\|+\rangle\|0\rangle\|-\rangle$		$\|01\rangle,\|10\rangle$	
	$\|0\rangle\|-\rangle\|0\rangle\|+\rangle$		$\|11\rangle$	$\|\widehat{\varphi_1}\rangle$
	$\|1\rangle\|+\rangle\|1\rangle\|-\rangle$		$\|00\rangle$	
X_5X_6	$\|1\rangle\|-\rangle\|1\rangle\|+\rangle$		$\|01\rangle,\|10\rangle$	$\|\widehat{\varphi_0}\rangle$
	$\|0\rangle\|+\rangle\|1\rangle\|-\rangle$		$\|++\rangle,\|--\rangle$	
			$\|+-\rangle$	$\|\widehat{\varphi_1}\rangle$
	$\|0\rangle\|-\rangle\|1\rangle\|+\rangle$		$\|-+\rangle$	
			$\|++\rangle,\|--\rangle$	$\|\widehat{\varphi_0}\rangle$
	$\|1\rangle\|+\rangle\|0\rangle\|+\rangle$		$\|+-\rangle,\|-+\rangle$	
			$\|--\rangle$	$\|\widehat{\varphi_1}\rangle$
	$\|1\rangle\|-\rangle\|0\rangle\|-\rangle$		$\|++\rangle$	
			$\|--\rangle$	$\|\widehat{\varphi_0}\rangle$

$Z_1X_2Z_3X_4$	R	B	R	B	R	C
	$\|0\rangle\|+\rangle\|1\rangle\|-\rangle$	A_5	$\|a_0\rangle$	C_6	$\|c_0\rangle$ $\|c_1\rangle$	$\|\widehat{\varphi_0}\rangle$ $\|\widehat{\varphi_1}\rangle$
			$\|a_1\rangle$	D_6	$\|d_0\rangle$ $\|d_1\rangle$	$\|\widehat{\varphi_0}\rangle$
	$\|0\rangle\|-\rangle\|1\rangle\|-\rangle$	B_5	$\|b_0\rangle$	E_6	$\|e_0\rangle$ $\|e_1\rangle$	$\|\widehat{\varphi_1}\rangle$
			$\|b_1\rangle$	F_6	$\|f_0\rangle$ $\|f_1\rangle$	$\|\widehat{\varphi_0}\rangle$
	$\|1\rangle\|+\rangle\|0\rangle\|-\rangle$	A_5	$\|a_0\rangle$	E_6	$\|e_0\rangle$ $\|e_1\rangle$	$\|\widehat{\varphi_1}\rangle$
			$\|a_1\rangle$	F_6	$\|f_0\rangle$ $\|f_1\rangle$	$\|\widehat{\varphi_0}\rangle$
	$\|0\rangle\|+\rangle\|1\rangle\|-\rangle$	B_5	$\|b_0\rangle$	C_6	$\|c_0\rangle$ $\|c_1\rangle$	$\|\widehat{\varphi_1}\rangle$
			$\|b_1\rangle$	D_6	$\|d_0\rangle$ $\|d_1\rangle$	$\|\widehat{\varphi_0}\rangle$

$$|b_0\rangle = -\frac{p}{p^2+q^2}|0\rangle + \frac{q}{p^2+q^2}|1\rangle,$$

$$|b_1\rangle = \frac{q}{p^2+q^2}|0\rangle + \frac{p}{p^2+q^2}|1\rangle,$$

$$|c_0\rangle = p|0\rangle - q|1\rangle, |c_1\rangle = (p-q)|0\rangle - (p+q)|1\rangle,$$

$$|d_0\rangle = (p+q)|0\rangle + (q-p)|1\rangle, |d_1\rangle = q|0\rangle + p|1\rangle,$$

$$|e_0\rangle = -p|0\rangle - q|1\rangle, |e_1\rangle = (q-p)|0\rangle + (p+q)|1\rangle,$$

$$|f_0\rangle = (p+q)|0\rangle + (p-q)|1\rangle, |f_1\rangle = q|0\rangle - p|1\rangle,$$

where

$$p = \frac{\sqrt{2+\sqrt{2}}}{2}, q = \frac{\sqrt{2-\sqrt{2}}}{2}.$$

However, in this improved version, some good features of the original DF BB84 protocol have not been kept such as the qubit-permutation character. So we consider to give an improvement which have all virtues of the original DF BB84 protocol. We also try to achieve our goal with orthogonal bases in lower-dimensional DF subspaces. It means that this version has more excellent efficiency than the original one.

IV. SECOND IMPROVEMENT

As is known, the maximum number of bits encoded in quantum states depends on the dimension of the space spanned by these quantum states. So encoding 1 bit classical information in DF states requires a two-dimensional DF subspace at least. Thus, in our different scheme, we need to use two orthogonal bases in two-dimensional DF subspaces for optimal efficiency. A natural choice of orthogonal base in the two-dimensional DF subspace is as follows [23], which has been generated experimentally by Bourennane *et al.* [27] using parametric down-converted polarization-entangled photons:

$$|\phi_0\rangle = \frac{1}{2}(|0101\rangle_{1234} - |0110\rangle_{1234} - |1001\rangle_{1234} + |1010\rangle_{1234}) = |\psi^-\rangle_{12} \otimes |\psi^-\rangle_{34}, \tag{7a}$$

$$|\phi_1\rangle = \frac{1}{2\sqrt{3}}(2|0011\rangle_{1234} - |0101\rangle_{1234} - |0110\rangle_{1234} - |1001\rangle_{1234} - |1010\rangle_{1234} + 2|1100\rangle_{1234}) = \frac{1}{\sqrt{3}}(|\phi^+\rangle_{12} \otimes |\phi^+\rangle_{34} - |\phi^-\rangle_{12} \otimes |\phi^-\rangle_{34} - |\psi^+\rangle_{12} \otimes |\psi^+\rangle_{34}). \tag{7b}$$

If permuting the qubits 1 and 4 in above states, we can obtain the other orthogonal base needed in our scheme:

$$|\phi_0'\rangle = P_{1\leftrightarrow 4}|\phi_0\rangle = |\psi^-\rangle_{42} \otimes |\psi^-\rangle_{31}, \tag{8a}$$

$$|\phi_1'\rangle = P_{1\leftrightarrow 4}|\phi_1\rangle = \frac{1}{\sqrt{3}}(|\phi^+\rangle_{42} \otimes |\phi^+\rangle_{31} - |\phi^-\rangle_{42} \otimes |\phi^-\rangle_{31} - |\psi^+\rangle_{42} \otimes |\psi^+\rangle_{31}). \tag{8b}$$

In Ref. [27], it is proven that $|\phi_0\rangle$ and $|\phi_1\rangle$ are distinguishable using the outcomes of single-qubit measurements, $Z_1Z_2X_3X_4$, on these four qubits. Therefore, the sequences of single-qubit measurements, $Z_1Z_2X_3X_4$ and $X_1Z_2X_3Z_4$, can be used as the bases which will be randomly chosen by Bob in the scheme. Obviously, Z_2X_3 are kept unaltered in two alternative bases $Z_1Z_2X_3X_4$ and $X_1Z_2X_3Z_4$. The detailed steps of the four-qubit DF variation of BB84 (FQDF BB84) protocol are similar with the original BB84 protocol. Thus we omit these redundant descriptions here. Naturally, the most predominance of the new variation over BB84 protocol is that it can distribute secure keys in the collective-noise channel.

TABLE III. The possible outcomes which will be obtained by measuring the four states, $|\phi_0\rangle$, $|\phi_1\rangle$, $|\phi_0'\rangle$ and $|\phi_1'\rangle$, in the bases $Z_1Z_2X_3X_4$ and $X_1Z_2X_3Z_4$, respectively.

State	$Z_1Z_2X_3X_4$ basis	$X_1Z_2X_3Z_4$ basis
$\|\phi_0\rangle$	$\|0\rangle\|1\rangle\|+\rangle\|-\rangle$, $\|0\rangle\|1\rangle\|-\rangle\|+\rangle$, $\|1\rangle\|0\rangle\|+\rangle\|-\rangle$, $\|1\rangle\|0\rangle\|-\rangle\|+\rangle$.	$\|\pm\rangle\|1\rangle\|\pm\rangle\|0\rangle$, $\|\pm\rangle\|1\rangle\|\pm\rangle\|1\rangle$, $\|\pm\rangle\|0\rangle\|\pm\rangle\|0\rangle$, $\|\pm\rangle\|0\rangle\|\pm\rangle\|1\rangle$.
$\|\phi_1\rangle$	$\|0\rangle\|0\rangle\|\pm\rangle\|\pm\rangle$, $\|1\rangle\|1\rangle\|\pm\rangle\|\pm\rangle$, $\|0\rangle\|1\rangle\|+\rangle\|+\rangle$, $\|0\rangle\|1\rangle\|-\rangle\|-\rangle$, $\|1\rangle\|0\rangle\|+\rangle\|+\rangle$, $\|1\rangle\|0\rangle\|-\rangle\|-\rangle$.	$\|+\rangle\|0\rangle\|+\rangle\|0\rangle$, $\|-\rangle\|1\rangle\|-\rangle\|1\rangle$, $\|\pm\rangle\|0\rangle\|\pm\rangle\|1\rangle$, $\|-\rangle\|0\rangle\|-\rangle\|0\rangle$, $\|\pm\rangle\|1\rangle\|\pm\rangle\|0\rangle$, $\|+\rangle\|1\rangle\|+\rangle\|1\rangle$.
$\|\phi_0'\rangle$	$\|0\rangle\|1\rangle\|\pm\rangle\|\pm\rangle$, $\|1\rangle\|1\rangle\|\pm\rangle\|\pm\rangle$, $\|0\rangle\|0\rangle\|\pm\rangle\|\pm\rangle$, $\|1\rangle\|0\rangle\|\pm\rangle\|\pm\rangle$.	$\|-\rangle\|1\rangle\|+\rangle\|0\rangle$, $\|+\rangle\|1\rangle\|-\rangle\|0\rangle$, $\|-\rangle\|0\rangle\|+\rangle\|1\rangle$, $\|+\rangle\|0\rangle\|-\rangle\|1\rangle$.
$\|\phi_1'\rangle$	$\|0\rangle\|0\rangle\|+\rangle\|+\rangle$, $\|1\rangle\|1\rangle\|-\rangle\|-\rangle$, $\|1\rangle\|0\rangle\|\pm\rangle\|\pm\rangle$, $\|0\rangle\|0\rangle\|-\rangle\|-\rangle$, $\|0\rangle\|1\rangle\|\pm\rangle\|\pm\rangle$, $\|1\rangle\|1\rangle\|+\rangle\|+\rangle$.	$\|\pm\rangle\|0\rangle\|\pm\rangle\|0\rangle$, $\|\pm\rangle\|1\rangle\|\pm\rangle\|1\rangle$, $\|+\rangle\|1\rangle\|+\rangle\|0\rangle$, $\|-\rangle\|1\rangle\|-\rangle\|0\rangle$, $\|+\rangle\|0\rangle\|+\rangle\|1\rangle$, $\|-\rangle\|0\rangle\|-\rangle\|1\rangle$.

Compared to the original DF BB84 protocol, our improved version has more excellent performances. On the one hand, the key generation rate can reach 12.5% in FQDF BB84 protocol while 8.33% in the original one. On the other hand, although FQDF BB84 protocol has some good features similar to the original one, it does not share the insecurity flaw. We can derive from Eqs. (7) and (8) that, for qubits measured in Z_2X_3,

$$\rho_{23}^{\phi_0} = \rho_{23}^{\phi_1} = \rho_{23}^{\phi_0'} = \rho_{23}^{\phi_1'}, \tag{9}$$

where $\rho_{23}^{\phi_0}$, $\rho_{23}^{\phi_1}$, $\rho_{23}^{\phi_0'}$, and $\rho_{23}^{\phi_1'}$ are reduced density matrices of systems shown in Eqs. (7) and (8). Thus, $|\phi_0\rangle, |\phi_1\rangle, |\phi_0'\rangle$ and $|\phi_1'\rangle$ cannot be distinguished by measuring the second and the third qubits in Z_2X_3. This conclusion can also be gained from Table III intuitively.

Then we will give a more strict proof to prove the security of FQDF BB84 protocol. Obviously, the security of FQDF BB84 protocol is based on the security of qubits transmission. According to Stingspring dilation theorem [35], as Eve is limited to eavesdropping on the quantum line between Alice and Bob, her eavesdropping can be realized by a unitary operation, $\hat{U}$, on a larger Hilbert space, $H_B \otimes H_E$. Since the second and the third single-qubit measurement bases in two basis sequences, $Z_1Z_2X_3X_4$ and $X_1Z_2X_3Z_4$, are kept invariable, the optimal attack on the second and the third qubits of each DF state is measuring them in the basis Z_2X_3 directly. Thus, in every transmitted four-qubit DF state, only the first and the fourth qubit should be considered. The effect of Eve's eavesdropping on the first and fourth qubits of $|\phi_0\rangle$,

$|\phi_1\rangle$, $|\phi_0'\rangle$, and $|\phi_1'\rangle$ can be described by the following equations:

$$\hat{U}|0+\rangle|\varepsilon\rangle = |0+\rangle|\varepsilon_{00}^1\rangle + |0-\rangle|\varepsilon_{01}^1\rangle + |1+\rangle|\varepsilon_{10}^1\rangle + |1-\rangle|\varepsilon_{11}^1\rangle,$$

$$\hat{U}|0-\rangle|\varepsilon\rangle = |0+\rangle|\varepsilon_{00}^2\rangle + |0-\rangle|\varepsilon_{01}^2\rangle + |1+\rangle|\varepsilon_{10}^2\rangle + |1-\rangle|\varepsilon_{11}^2\rangle,$$

$$\hat{U}|1+\rangle|\varepsilon\rangle = |0+\rangle|\varepsilon_{00}^3\rangle + |0-\rangle|\varepsilon_{01}^3\rangle + |1+\rangle|\varepsilon_{10}^3\rangle + |1-\rangle|\varepsilon_{11}^3\rangle,$$

$$\hat{U}|1-\rangle|\varepsilon\rangle = |0+\rangle|\varepsilon_{00}^4\rangle + |0-\rangle|\varepsilon_{01}^4\rangle + |1+\rangle|\varepsilon_{10}^4\rangle + |1-\rangle|\varepsilon_{11}^4\rangle,$$

$$\hat{U}|+0\rangle|\varepsilon\rangle = \frac{1}{4}(|+0\rangle_{14}|\xi_{0000}\rangle + |+1\rangle_{14}|\xi_{0001}\rangle + |-0\rangle_{14}|\xi_{0010}\rangle + |-1\rangle_{14}|\xi_{0011}\rangle),$$

$$\hat{U}|+1\rangle|\varepsilon\rangle = \frac{1}{4}(|+0\rangle_{14}|\xi_{0100}\rangle + |+1\rangle_{14}|\xi_{0101}\rangle + |-0\rangle_{14}|\xi_{0110}\rangle + |-1\rangle_{14}|\xi_{0111}\rangle),$$

$$\hat{U}|-0\rangle|\varepsilon\rangle = \frac{1}{4}(|+0\rangle_{14}|\xi_{1000}\rangle + |+1\rangle_{14}|\xi_{1001}\rangle + |-0\rangle_{14}|\xi_{1010}\rangle + |-1\rangle_{14}|\xi_{1011}\rangle),$$

$$\hat{U}|-1\rangle|\varepsilon\rangle = \frac{1}{4}(|+0\rangle_{14}|\xi_{1100}\rangle + |+1\rangle_{14}|\xi_{1101}\rangle + |-0\rangle_{14}|\xi_{1110}\rangle + |-1\rangle_{14}|\xi_{1111}\rangle),$$

where $|\varepsilon\rangle$ is the initial state of Eve's ancilla, which is appended to the first and the fourth qubits of each DF state, $|\varepsilon_{ij}^k\rangle$ $(i,j \in \{0,1\}, k=1,2,3,4)$ are the pure ancilla's states determined uniquely by the unitary operation $\hat{U}$, and

$$|\xi_{0000}\rangle = |\varepsilon_{00}^1\rangle + |\varepsilon_{00}^2\rangle + |\varepsilon_{00}^3\rangle + |\varepsilon_{00}^4\rangle + |\varepsilon_{01}^1\rangle + |\varepsilon_{01}^2\rangle + |\varepsilon_{01}^3\rangle + |\varepsilon_{01}^4\rangle + |\varepsilon_{10}^1\rangle + |\varepsilon_{10}^2\rangle + |\varepsilon_{10}^3\rangle + |\varepsilon_{10}^4\rangle + |\varepsilon_{11}^1\rangle + |\varepsilon_{11}^2\rangle + |\varepsilon_{11}^3\rangle + |\varepsilon_{11}^4\rangle,$$

$$|\xi_{0001}\rangle = |\varepsilon_{00}^1\rangle + |\varepsilon_{00}^2\rangle + |\varepsilon_{00}^3\rangle + |\varepsilon_{00}^4\rangle - |\varepsilon_{01}^1\rangle - |\varepsilon_{01}^2\rangle - |\varepsilon_{01}^3\rangle - |\varepsilon_{01}^4\rangle + |\varepsilon_{10}^1\rangle + |\varepsilon_{10}^2\rangle + |\varepsilon_{10}^3\rangle + |\varepsilon_{10}^4\rangle - |\varepsilon_{11}^1\rangle - |\varepsilon_{11}^2\rangle - |\varepsilon_{11}^3\rangle - |\varepsilon_{11}^4\rangle,$$

$$|\xi_{0010}\rangle = |\varepsilon_{00}^1\rangle + |\varepsilon_{00}^2\rangle + |\varepsilon_{00}^3\rangle + |\varepsilon_{00}^4\rangle + |\varepsilon_{01}^1\rangle + |\varepsilon_{01}^2\rangle + |\varepsilon_{01}^3\rangle + |\varepsilon_{01}^4\rangle) - |\varepsilon_{10}^1\rangle - |\varepsilon_{10}^2\rangle - |\varepsilon_{10}^3\rangle - |\varepsilon_{10}^4\rangle - |\varepsilon_{11}^1\rangle - |\varepsilon_{11}^2\rangle - |\varepsilon_{11}^3\rangle - |\varepsilon_{11}^4\rangle,$$

$$|\xi_{0011}\rangle = |\varepsilon_{00}^1\rangle + |\varepsilon_{00}^2\rangle + |\varepsilon_{00}^3\rangle + |\varepsilon_{00}^4\rangle - |\varepsilon_{01}^1\rangle - |\varepsilon_{01}^2\rangle - |\varepsilon_{01}^3\rangle - |\varepsilon_{01}^4\rangle - |\varepsilon_{10}^1\rangle - |\varepsilon_{10}^2\rangle - |\varepsilon_{10}^3\rangle - |\varepsilon_{10}^4\rangle + |\varepsilon_{11}^1\rangle + |\varepsilon_{11}^2\rangle + |\varepsilon_{11}^3\rangle + |\varepsilon_{11}^4\rangle,$$

$$|\xi_{0100}\rangle = |\varepsilon_{00}^1\rangle - |\varepsilon_{00}^2\rangle + |\varepsilon_{00}^3\rangle - |\varepsilon_{00}^4\rangle + |\varepsilon_{01}^1\rangle - |\varepsilon_{01}^2\rangle + |\varepsilon_{01}^3\rangle - |\varepsilon_{01}^4\rangle + |\varepsilon_{10}^1\rangle - |\varepsilon_{10}^2\rangle + |\varepsilon_{10}^3\rangle - |\varepsilon_{10}^4\rangle + |\varepsilon_{11}^1\rangle - |\varepsilon_{11}^2\rangle + |\varepsilon_{11}^3\rangle - |\varepsilon_{11}^4\rangle,$$

$$|\xi_{0101}\rangle = |\varepsilon_{00}^1\rangle - |\varepsilon_{00}^2\rangle + |\varepsilon_{00}^3\rangle - |\varepsilon_{00}^4\rangle - |\varepsilon_{01}^1\rangle + |\varepsilon_{01}^2\rangle - |\varepsilon_{01}^3\rangle + |\varepsilon_{01}^4\rangle + |\varepsilon_{10}^1\rangle - |\varepsilon_{10}^2\rangle + |\varepsilon_{10}^3\rangle - |\varepsilon_{10}^4\rangle - |\varepsilon_{11}^1\rangle + |\varepsilon_{11}^2\rangle - |\varepsilon_{11}^3\rangle + |\varepsilon_{11}^4\rangle,$$

$$|\xi_{0110}\rangle = |\varepsilon_{00}^1\rangle - |\varepsilon_{00}^2\rangle + |\varepsilon_{00}^3\rangle - |\varepsilon_{00}^4\rangle + |\varepsilon_{01}^1\rangle - |\varepsilon_{01}^2\rangle + |\varepsilon_{01}^3\rangle - |\varepsilon_{01}^4\rangle - |\varepsilon_{10}^1\rangle + |\varepsilon_{10}^2\rangle - |\varepsilon_{10}^3\rangle + |\varepsilon_{10}^4\rangle - |\varepsilon_{11}^1\rangle + |\varepsilon_{11}^2\rangle - |\varepsilon_{11}^3\rangle + |\varepsilon_{11}^4\rangle,$$

$$|\xi_{0111}\rangle = |\varepsilon_{00}^1\rangle - |\varepsilon_{00}^2\rangle + |\varepsilon_{00}^3\rangle - |\varepsilon_{00}^4\rangle - |\varepsilon_{01}^1\rangle + |\varepsilon_{01}^2\rangle - |\varepsilon_{01}^3\rangle + |\varepsilon_{01}^4\rangle - |\varepsilon_{10}^1\rangle + |\varepsilon_{10}^2\rangle - |\varepsilon_{10}^3\rangle + |\varepsilon_{10}^4\rangle + |\varepsilon_{11}^1\rangle - |\varepsilon_{11}^2\rangle + |\varepsilon_{11}^3\rangle - |\varepsilon_{11}^4\rangle,$$

$$|\xi_{1000}\rangle = |\varepsilon_{00}^1\rangle + |\varepsilon_{00}^2\rangle - |\varepsilon_{00}^3\rangle - |\varepsilon_{00}^4\rangle + |\varepsilon_{01}^1\rangle + |\varepsilon_{01}^2\rangle - |\varepsilon_{01}^3\rangle - |\varepsilon_{01}^4\rangle + |\varepsilon_{10}^1\rangle + |\varepsilon_{10}^2\rangle - |\varepsilon_{10}^3\rangle - |\varepsilon_{10}^4\rangle + |\varepsilon_{11}^1\rangle + |\varepsilon_{11}^2\rangle - |\varepsilon_{11}^3\rangle - |\varepsilon_{11}^4\rangle,$$

$$|\xi_{1001}\rangle = |\varepsilon_{00}^1\rangle + |\varepsilon_{00}^2\rangle - |\varepsilon_{00}^3\rangle - |\varepsilon_{00}^4\rangle - |\varepsilon_{01}^1\rangle - |\varepsilon_{01}^2\rangle + |\varepsilon_{01}^3\rangle + |\varepsilon_{01}^4\rangle + |\varepsilon_{10}^1\rangle + |\varepsilon_{10}^2\rangle - |\varepsilon_{10}^3\rangle - |\varepsilon_{10}^4\rangle - |\varepsilon_{11}^1\rangle - |\varepsilon_{11}^2\rangle + |\varepsilon_{11}^3\rangle + |\varepsilon_{11}^4\rangle,$$

$$|\xi_{1010}\rangle = |\varepsilon_{00}^1\rangle + |\varepsilon_{00}^2\rangle - |\varepsilon_{00}^3\rangle - |\varepsilon_{00}^4\rangle + |\varepsilon_{01}^1\rangle + |\varepsilon_{01}^2\rangle - |\varepsilon_{01}^3\rangle - |\varepsilon_{01}^4\rangle - |\varepsilon_{10}^1\rangle - |\varepsilon_{10}^2\rangle + |\varepsilon_{10}^3\rangle + |\varepsilon_{10}^4\rangle - |\varepsilon_{11}^1\rangle - |\varepsilon_{11}^2\rangle + |\varepsilon_{11}^3\rangle + |\varepsilon_{11}^4\rangle,$$

$$|\xi_{1011}\rangle = |\varepsilon_{00}^1\rangle + |\varepsilon_{00}^2\rangle - |\varepsilon_{00}^3\rangle - |\varepsilon_{00}^4\rangle - |\varepsilon_{01}^1\rangle - |\varepsilon_{01}^2\rangle + |\varepsilon_{01}^3\rangle + |\varepsilon_{01}^4\rangle - |\varepsilon_{10}^1\rangle - |\varepsilon_{10}^2\rangle + |\varepsilon_{10}^3\rangle + |\varepsilon_{10}^4\rangle + |\varepsilon_{11}^1\rangle + |\varepsilon_{11}^2\rangle - |\varepsilon_{11}^3\rangle - |\varepsilon_{11}^4\rangle,$$

$$|\xi_{1100}\rangle = |\varepsilon_{00}^1\rangle - |\varepsilon_{00}^2\rangle - |\varepsilon_{00}^3\rangle + |\varepsilon_{00}^4\rangle + |\varepsilon_{01}^1\rangle - |\varepsilon_{01}^2\rangle - |\varepsilon_{01}^3\rangle + |\varepsilon_{01}^4\rangle + |\varepsilon_{10}^1\rangle - |\varepsilon_{10}^2\rangle - |\varepsilon_{10}^3\rangle + |\varepsilon_{10}^4\rangle + |\varepsilon_{11}^1\rangle - |\varepsilon_{11}^2\rangle - |\varepsilon_{11}^3\rangle + |\varepsilon_{11}^4\rangle,$$

$$|\xi_{1101}\rangle = |\varepsilon_{00}^1\rangle - |\varepsilon_{00}^2\rangle - |\varepsilon_{00}^3\rangle + |\varepsilon_{00}^4\rangle - |\varepsilon_{01}^1\rangle + |\varepsilon_{01}^2\rangle + |\varepsilon_{01}^3\rangle - |\varepsilon_{01}^4\rangle + |\varepsilon_{10}^1\rangle - |\varepsilon_{10}^2\rangle - |\varepsilon_{10}^3\rangle + |\varepsilon_{10}^4\rangle - |\varepsilon_{11}^1\rangle + |\varepsilon_{11}^2\rangle + |\varepsilon_{11}^3\rangle - |\varepsilon_{11}^4\rangle,$$

$$|\xi_{1110}\rangle = |\varepsilon_{00}^1\rangle - |\varepsilon_{00}^2\rangle - |\varepsilon_{00}^3\rangle + |\varepsilon_{00}^4\rangle + |\varepsilon_{01}^1\rangle - |\varepsilon_{01}^2\rangle - |\varepsilon_{01}^3\rangle + |\varepsilon_{01}^4\rangle - |\varepsilon_{10}^1\rangle + |\varepsilon_{10}^2\rangle + |\varepsilon_{10}^3\rangle - |\varepsilon_{10}^4\rangle - |\varepsilon_{11}^1\rangle + |\varepsilon_{11}^2\rangle + |\varepsilon_{11}^3\rangle - |\varepsilon_{11}^4\rangle,$$

$$|\xi_{1111}\rangle = |\varepsilon_{00}^1\rangle - |\varepsilon_{00}^2\rangle - |\varepsilon_{00}^3\rangle + |\varepsilon_{00}^4\rangle - |\varepsilon_{01}^1\rangle + |\varepsilon_{01}^2\rangle + |\varepsilon_{01}^3\rangle - |\varepsilon_{01}^4\rangle - |\varepsilon_{10}^1\rangle + |\varepsilon_{10}^2\rangle + |\varepsilon_{10}^3\rangle - |\varepsilon_{10}^4\rangle + |\varepsilon_{11}^1\rangle - |\varepsilon_{11}^2\rangle - |\varepsilon_{11}^3\rangle + |\varepsilon_{11}^4\rangle.$$

Obviously, $|\varepsilon_{ij}^k\rangle (i,j \in \{0,1\}, k=1,2,3,4)$ must satisfy the relationship $\hat{U}^\dagger \hat{U} = I$, i.e.,

$$\sum_{k=1}^{4} \langle \varepsilon_{ij}^k | \varepsilon_{ij}^k \rangle = 1, \quad \text{where} \quad i,j \in \{0,1\},$$

$$\sum_{k=0}^{4} \langle \varepsilon_{ij}^k | \varepsilon_{mn}^k \rangle - \sum_{l=1}^{4} \langle \varepsilon_{ij}^l | \varepsilon_{ij}^l \rangle = 0, \quad \text{where} \quad i,j,m,n \in \{0,1\}.$$

The quantum systems shown in Eqs. (7) and (8) can be rewritten with the effect of Eve's eavesdropping as follows, respectively:

$$\begin{aligned}\hat{U}|\phi_0\rangle|\varepsilon\rangle = \frac{1}{2}[&|1-\rangle_{23}(|0+\rangle_{14}|\varepsilon_{00}^1\rangle + |0-\rangle_{14}|\varepsilon_{01}^1\rangle + |1+\rangle_{14}|\varepsilon_{10}^1\rangle \\ &+ |1-\rangle_{14}|\varepsilon_{11}^1\rangle) - |1+\rangle_{23}(|0+\rangle_{14}|\varepsilon_{00}^2\rangle + |0-\rangle_{14}|\varepsilon_{01}^2\rangle \\ &+ |1+\rangle_{14}|\varepsilon_{10}^2\rangle + |1-\rangle_{14}|\varepsilon_{11}^2\rangle) - |0-\rangle_{23}(|0+\rangle_{14}|\varepsilon_{00}^3\rangle \\ &+ |0-\rangle_{14}|\varepsilon_{01}^3\rangle + |1+\rangle_{14}|\varepsilon_{10}^3\rangle + |1-\rangle_{14}|\varepsilon_{11}^3\rangle) \\ &+ |0+\rangle_{23}(|0+\rangle_{14}|\varepsilon_{00}^4\rangle + |0-\rangle_{14}|\varepsilon_{01}^4\rangle + |1+\rangle_{14}|\varepsilon_{10}^4\rangle \\ &+ |1-\rangle_{14}|\varepsilon_{11}^4\rangle)], \end{aligned} \tag{10a}$$

$$\begin{aligned}\hat{U}|\phi_1\rangle|\varepsilon\rangle = \frac{1}{2\sqrt{3}}[&(|0+\rangle - |0-\rangle - |1+\rangle)_{23}(|0+\rangle_{14}|\varepsilon_{00}^1\rangle \\ &+ |0-\rangle_{14}|\varepsilon_{01}^1\rangle + |1+\rangle_{14}|\varepsilon_{10}^1\rangle + |1-\rangle_{14}|\varepsilon_{11}^1\rangle) \\ &+ (|0-\rangle - |0+\rangle + |1-\rangle)_{23}(|0-\rangle_{14}|\varepsilon_{01}^2\rangle + |1+\rangle_{14}|\varepsilon_{10}^2\rangle \\ &+ |1-\rangle_{14}|\varepsilon_{11}^2\rangle + |0+\rangle_{14}|\varepsilon_{00}^2\rangle) + (|1+\rangle + |1-\rangle - |0+\rangle)_{23} \\ &\times(|1+\rangle_{14}|\varepsilon_{10}^3\rangle + |1-\rangle_{14}|\varepsilon_{11}^3\rangle + |0+\rangle_{14}|\varepsilon_{00}^3\rangle \\ &+ |0-\rangle_{14}|\varepsilon_{01}^3\rangle) + (|0-\rangle + |1+\rangle + |1-\rangle)_{23}(|1-\rangle_{14}|\varepsilon_{11}^4\rangle \\ &+ |0+\rangle_{14}|\varepsilon_{00}^4\rangle + |0-\rangle_{14}|\varepsilon_{01}^4\rangle + |1+\rangle_{14}|\varepsilon_{10}^4\rangle)], \end{aligned} \tag{10b}$$

$$\begin{aligned}\hat{U}|\phi_0'\rangle|\varepsilon\rangle = \frac{1}{8}[&|1-\rangle_{23}(|+0\rangle_{14}|\xi_{0000}\rangle + |+1\rangle_{14}|\xi_{0001}\rangle \\ &+ |-0\rangle_{14}|\xi_{0010}\rangle + |-1\rangle_{14}|\xi_{0011}\rangle) \\ &- |1+\rangle_{23}(|+0\rangle_{14}|\xi_{0100}\rangle + |+1\rangle_{14}|\xi_{0101}\rangle \\ &+ |-0\rangle_{14}|\xi_{0110}\rangle + |-1\rangle_{14}|\xi_{0111}\rangle) - |0-\rangle_{23} \\ &\times(|+0\rangle_{14}|\xi_{1000}\rangle + |+1\rangle_{14}|\xi_{1001}\rangle + |-0\rangle_{14}|\xi_{1010}\rangle \\ &+ |-1\rangle_{14}|\xi_{1011}\rangle) + |0+\rangle_{23}(|+0\rangle_{14}|\xi_{1100}\rangle \\ &+ |+1\rangle_{14}|\xi_{1101}\rangle + |-0\rangle_{14}|\xi_{1110}\rangle \\ &+ |-1\rangle_{14}|\xi_{1111}\rangle)], \end{aligned} \tag{10c}$$

$$\begin{aligned}\hat{U}|\phi_1'\rangle|\varepsilon\rangle = \frac{1}{8\sqrt{3}}[&(|0+\rangle - |0-\rangle - |1+\rangle)_{23}(|+0\rangle_{14}|\xi_{0000}\rangle \\ &+ |+1\rangle_{14}|\xi_{0001}\rangle + |-0\rangle_{14}|\xi_{0010}\rangle + |-1\rangle_{14}|\xi_{0011}\rangle) \\ &+ (|0-\rangle - |0+\rangle + |1-\rangle)_{23}(|+0\rangle_{14}|\xi_{0100}\rangle \\ &+ |+1\rangle_{14}|\xi_{0101}\rangle + |-0\rangle_{14}|\xi_{0110}\rangle + |-1\rangle_{14}|\xi_{0111}\rangle) \\ &+ (|1+\rangle + |1-\rangle - |0+\rangle)_{23}(|+0\rangle_{14}|\xi_{1000}\rangle \\ &+ |+1\rangle_{14}|\xi_{1001}\rangle + |-0\rangle_{14}|\xi_{1010}\rangle + |-1\rangle_{14}|\xi_{1011}\rangle) \\ &+ (|0-\rangle + |1+\rangle + |1-\rangle)_{23}(|+0\rangle_{14}|\xi_{1100}\rangle \\ &+ |+1\rangle_{14}|\xi_{1101}\rangle + |-0\rangle_{14}|\xi_{1110}\rangle + |-1\rangle_{14}|\xi_{1111}\rangle)]. \end{aligned} \tag{10d}$$

For every transmitted four-qubit DF state, the action of Eve's eavesdropping will introduce an error rate

$$P_e^{\phi_0} = 1 - \frac{1}{4}(\langle \varepsilon_{00}^1 | \varepsilon_{00}^1 \rangle + \langle \varepsilon_{01}^2 | \varepsilon_{01}^2 \rangle + \langle \varepsilon_{10}^3 | \varepsilon_{10}^3 \rangle + \langle \varepsilon_{11}^4 | \varepsilon_{11}^4 \rangle), \tag{11a}$$

$$\begin{aligned}P_e^{\phi_1} = \frac{1}{12}(&\langle \varepsilon_{11}^1 | \varepsilon_{11}^1 \rangle + \langle \varepsilon_{11}^2 | \varepsilon_{11}^2 \rangle + \langle \varepsilon_{11}^3 | \varepsilon_{11}^3 \rangle - 2\langle \varepsilon_{11}^1 | \varepsilon_{11}^2 \rangle \\ &- \langle \varepsilon_{11}^1 | \varepsilon_{11}^3 \rangle + 2\langle \varepsilon_{11}^2 | \varepsilon_{11}^3 \rangle + \langle \varepsilon_{10}^1 | \varepsilon_{10}^1 \rangle + \langle \varepsilon_{10}^2 | \varepsilon_{10}^2 \rangle \\ &+ \langle \varepsilon_{10}^4 | \varepsilon_{10}^4 \rangle - 2\langle \varepsilon_{10}^1 | \varepsilon_{10}^2 \rangle - 2\langle \varepsilon_{10}^1 | \varepsilon_{10}^4 \rangle + 2\langle \varepsilon_{10}^2 | \varepsilon_{10}^4 \rangle \\ &+ \langle \varepsilon_{01}^1 | \varepsilon_{01}^1 \rangle + \langle \varepsilon_{01}^3 | \varepsilon_{01}^3 \rangle + \langle \varepsilon_{01}^4 | \varepsilon_{01}^4 \rangle - 2\langle \varepsilon_{01}^1 | \varepsilon_{01}^3 \rangle \\ &- 2\langle \varepsilon_{01}^1 | \varepsilon_{01}^4 \rangle + 2\langle \varepsilon_{01}^3 | \varepsilon_{01}^4 \rangle + \langle \varepsilon_{00}^2 | \varepsilon_{00}^2 \rangle + \langle \varepsilon_{00}^3 | \varepsilon_{00}^3 \rangle \\ &+ \langle \varepsilon_{00}^4 | \varepsilon_{00}^4 \rangle + 2\langle \varepsilon_{00}^2 | \varepsilon_{00}^3 \rangle + 2\langle \varepsilon_{00}^2 | \varepsilon_{00}^4 \rangle + 2\langle \varepsilon_{00}^3 | \varepsilon_{00}^4 \rangle), \end{aligned} \tag{11b}$$

$$\begin{aligned}P_e^{\phi_0'} = 1 - \frac{1}{64}(&\langle \xi_{0000} | \xi_{0000} \rangle + \langle \xi_{0101} | \xi_{0101} \rangle + \langle \xi_{1010} | \xi_{1010} \rangle \\ &+ \langle \xi_{1111} | \xi_{1111} \rangle), \end{aligned} \tag{11c}$$

$$\begin{aligned}P_e^{\phi_1'} = \frac{1}{192}(&\langle \xi_{0011} | \xi_{0011} \rangle + \langle \xi_{0100} | \xi_{0100} \rangle + \langle \xi_{10141} | \xi_{1011} \rangle \\ &- 2\langle \xi_{0011} | \xi_{0110} \rangle - 2\langle \xi_{0011} | \xi_{1011} \rangle + 2\langle \xi_{0110} | \xi_{1011} \rangle \\ &+ \langle \xi_{0010} | \xi_{0010} \rangle + \langle \xi_{0110} | \xi_{0110} \rangle + \langle \xi_{1110} | \xi_{1110} \rangle \\ &- 2\langle \xi_{0010} | \xi_{0110} \rangle - 2\langle \xi_{0010} | \xi_{1110} \rangle + 2\langle \xi_{0110} | \xi_{1110} \rangle \\ &+ \langle \xi_{0001}^1 | \xi_{0001} \rangle + \langle \xi_{1001} | \xi_{1001} \rangle + \langle \xi_{1101} | \xi_{1101} \rangle \\ &- 2\langle \xi_{0001} | \xi_{1001} \rangle - 2\langle \xi_{0001} | \xi_{1101} \rangle + 2\langle \xi_{1001} | \xi_{1101} \rangle \\ &+ \langle \xi_{0100} | \xi_{0100} \rangle + \langle \xi_{1000} | \xi_{1000} \rangle + \langle \xi_{1100} | \xi_{1100} \rangle \\ &+ 2\langle \xi_{0100} | \xi_{1000} \rangle + 2\langle \xi_{0100} | \xi_{1100} \rangle + 2\langle \xi_{1000} | \xi_{1100} \rangle). \end{aligned} \tag{11d}$$

Eve is supposed to be clever enough to prevent Alice and Bob from detecting her eavesdropping by finding the discrepancy in the error rates of quantum states, i.e.,

$$P_e^{\phi_0} = P_e^{\phi_1} = P_e^{\phi_0'} = P_e^{\phi_1'}. \tag{12}$$

If Eve tries to achieve the eavesdropping without being detected, the error rates $P_e^{\phi_0}$, $P_e^{\phi_1}$, $P_e^{\phi_0'}$, and $P_e^{\phi_1'}$ have to be equal to 0 in the ideal collective-noise environment. Then Eqs. (13) follows:

$$|\varepsilon_{00}^1\rangle = |\varepsilon_{01}^2\rangle = |\varepsilon_{10}^3\rangle = |\varepsilon_{11}^4\rangle, \tag{13a}$$

$$|\varepsilon_{00}^2\rangle = |\varepsilon_{00}^3\rangle = |\varepsilon_{00}^4\rangle = 0, \tag{13b}$$

$$|\varepsilon_{01}^1\rangle = |\varepsilon_{01}^3\rangle = |\varepsilon_{01}^4\rangle = 0, \tag{13c}$$

$$|\varepsilon_{10}^1\rangle = |\varepsilon_{10}^2\rangle = |\varepsilon_{10}^4\rangle = 0, \tag{13d}$$

$$|\varepsilon_{11}^1\rangle = |\varepsilon_{11}^2\rangle = |\varepsilon_{11}^3\rangle = 0. \tag{13e}$$

Thus, the quantum systems shown in Eqs. (10) can be rewritten as a tensor product of Eve's ancilla $|\varepsilon_{00}^1\rangle$ and the initial quantum systems ($|\phi_0\rangle$, $|\phi_1\rangle$, $|\phi_0'\rangle$, and $|\phi_1'\rangle$) because of the relationship shown in Eqs. (13). It implies that Eve's eavesdropping will have no effect on the whole system used to construct keys if she wants to eavesdrop without being detected. That is to say, all Eve's attacks can be detected. So it suffices to conclude that FQDF BB84 protocol is secure for Eve's eavesdropping under an collective-noise environment.

V. CONCLUSION

To summarize, in this paper, we showed that an eavesdropper can elicit a certain amount of information from the transmitted qubits in the original DF BB84 protocol. The essence of information leakage can be concluded that, for qubits measured in the unchanged bases, not all reduced density matrices of the involved systems are equal. We presented two schemes which are also robust against collective noise to improve the security of DF BB84 protocol. Especially, FQDF BB84 protocol has a more excellent efficiency except keeping the original properties of DF BB84 protocol.

ACKNOWLEDGMENTS

This work is supported by NSFC (Grants No. 60873191 and No. 60821001), SRFDP (Grant No. 200800131016), Beijing Nova Program (Grant No. 2008B51), Key Project of Chinese Ministry of Education (Grant No. 109014), Beijing Natural Science Foundation (Grant No. 4072020), National Laboratory for Modern Communications Science Foundation of China (Grant No. 9140C1101010601), China Postdoctoral Foundation (Grant No. 20090450018) and ISN Open Foundation.

[1] S. Wiesner, SIGACT News **15**, 78 (1983).
[2] C. H. Bennett and G. Brassard, Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India (IEEE, New York, 1984), pp. 175–179.
[3] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[4] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
[5] A. Beige, B. –G. Englert, Ch. Kurtsiefer, and H. Weinfurter, Acta Phys. Pol. A **101**, 357 (2002).
[6] K. Boström and T. Felbinger, Phys. Rev. Lett. **89**, 187902 (2002).
[7] F. G. Deng and G. L. Long, Phys. Rev. A **69**, 052319 (2004).
[8] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Zukowski, and H. Weinfurter, Phys. Rev. Lett. **95**, 230505 (2005).
[9] M. Boyer, D. Kenigsberg, and T. Mor, Phys. Rev. Lett. **99**, 140501 (2007).
[10] F. G. Deng, X. H. Li, and H. Y. Zhou, Phys. Lett. A **372**, 1957 (2008).
[11] W. H. Zurek, Phys. Today **44**(10), 36 (1991).
[12] P. W. Shor, Phys. Rev. A **52**, R2493 (1995).
[13] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, Phys. Rev. Lett. **77**, 198 (1996).
[14] A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996).
[15] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).
[16] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).
[17] X. B. Wang, Phys. Rev. Lett. **92**, 077902 (2004).
[18] X. B. Wang, Phys. Rev. A **69**, 022320 (2004).
[19] Y. A. Chen, A. N. Zhang, Z. Zhao, X. Q. Zhou, and J. W. Pan, Phys. Rev. Lett. **96**, 220504 (2006).
[20] P. Zanardi and M. Rasetti, Phys. Rev. Lett. **79**, 3306 (1997).
[21] D. A. Lidar, I. L. Chuang, and K. B. Whaley, Phys. Rev. Lett. **81**, 2594 (1998).
[22] D. A. Lidar, D. Bacon, J. Kempe, and K. B. Whaley, Phys. Rev. A **61**, 052307 (2000).
[23] J. Kempe, D. Bacon, D. A. Lidar, and K. B. Whaley, Phys. Rev. A **63**, 042307 (2001).
[24] A. Cabello, Phys. Rev. Lett. **89**, 100402 (2002).
[25] A. Cabello, Phys. Rev. Lett. **91**, 230403 (2003).
[26] J. C. Boileau, D. Gottesman, R. Laflamme, D. Poulin, and R. W. Spekkens, Phys. Rev. Lett. **92**, 017901 (2004).
[27] M. Bourennane, M. Eibl, S. Gaertner, C. Kurtsiefer, A. Cabello, and H. Weinfurter, Phys. Rev. Lett. **92**, 107901 (2004).
[28] T. Y. Chen, J. Zhang, J. C. Boileau, X. M. Jin, B. Yang, Q. Zhang, T. Yang, R. Laflamme, and J. W. Pan, Phys. Rev. Lett. **96**, 150504 (2006).
[29] P. G. Kwiat, A. J. Berglund, J. B. Altepeter, and A. G. White, Science **290**, 498 (2000).
[30] D. Kielpinski, V. Meyer, M. A. Rowe, C. A. Sackett, W. M. Itano, C. Monroe, and D. J. Wineland, Science **291**, 1013 (2001).
[31] J. E. Ollerenshaw, D. A. Lidar, and L. E. Kay, Phys. Rev. Lett. **91**, 217904 (2003).
[32] A. Cabello, Phys. Rev. A **75**, 020301 (2007).
[33] C.-H. Ji, Y. Yee, J. Choi, S.-H. Kim, and J.-U. Bu, IEEE J. Sel. Top. Quantum Electron. **10**, 545 (2004).
[34] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, Phys. Rev. Lett. **85**, 4972 (2000).
[35] W. F. Stinespring, Proc. Am. Math. Soc. **6**, 211 (1955).