Enhancing Quantum Protocols with the Security of Decoherence-Free Subspaces and Subsystems

Elloá B. Guedes and Francisco M. de Assis

***Abstract*—In the attempt to overcome the negative effects of the noise on quantum channels and to provide secure communications, some quantum secure direct communication protocols and deterministic secure quantum communication protocols making use of decoherence-free subspaces and subsystems have been proposed in the literature. However, recent results regarding the use of decoherence-free subspaces and subsystems show that they can be used to convey classical information through quantum channels with unconditional security. In this work, we use these results to propose enhancements into four already existing protocols. As a result, in all cases considered, (i) the encoding was simplified, requiring less gates to be implemented; (ii) the number of qubit and bit exchange was reduced, reaching a four times reduction in one of the cases; (iii) no eavesdropping check nor redundancy are further required; and (iv) the rate of information transmission was increased in all protocols. Such enhancements favor the adoption of such modified protocols in practical scenarios.**

***Index Terms*—Collective Decoherence; Decoherence-Free Subspaces and Subsystems; Quantum Protocols.**

I. Introduction

THE principles of Quantum Mechanics provide novel ways for quantum information transmission and processing, such as Quantum Computation and Quantum Communication. Regarding Quantum Communication, in particular, some intrinsic properties of Quantum Mechanics enable features that do not have counterpart in Classical Communication, such as: (i) a qubit has not a definite value until the moment after it is read; (ii) every measurement in a qubit may disturb it; (iii) arbitrary states of qubits cannot be copied; (iv) qubits can be entangled; among others [1]. Thanks to these Quantum Mechanics principles, in certain scenarios unconditional security can be achieved in quantum information conveying through quantum channels.

The *Quantum Key Distribution* [2]–[5] is one of the most mature quantum information techniques nowadays. According QKD, two remote users can create a private key securely. These keys are then used to crypt the secret message into a ciphertext through a classical cryptographic scheme such as the one-time pad, and the ciphertexts are then sent from one user to another through a classical channel. However, in a practical transmission process, the channel noise cannot be avoided completely. Noise can increase not only the error rate of the sending message, but also the difficulty of finding an eavesdropper in the process of a security check.

Recently, the *quantum secure direct communication* (QSDC) protocols have been proposed as a new technique of communication. Its objective it to transmit classical messages directly, without the help of private keys nor classical communications. In this scheme, the QKD and the classical transmission of the chipertext are condensed into a single quantum communication. For this reason, QSDC is considered as a purely quantum mechanical technique [6].

In a similar way, in the *deterministic secure quantum communication* (DSQC) protocols, the message is deterministically sent through the quantum channel, but can only be deduced after a round of classical information transmission. In fact, this is the fundamental difference between QSDC and DSQC protocols [6].

So far, many QSDC and DSQC protocols have been proposed in the literature considering the use of different resources and methods, such as entanglement swapping [7], teleportation [8]–[10], quantum one-time pad [11], rearrangement of orders of particles [12], among others. The survey of Long et al. [6] contemplates the recent developments about both QSDC and DSQC.

In the attempt to avoid the negative effects of noise, some QSDC and DSQC protocols making use of *decoherence-free subspaces and subsystems* (DFS) have been proposed [13]–[15]. States belonging to these subspaces and subsystems exploit the dynamical symmetries existing in the quantum channel to keep their invariability against the noise [16].

However, recent results regarding codes built from states of a DFS show that they can achieve unconditional security [17], [18]. So, a question that arises is: are there any enhancements that can be made on these QSDC and DSQC protocols that use DFS aiming at simplification or at increase efficiency? This paper attempts at answering this question.

As a result, we propose changes into four already existing protocols, reducing significantly the number of qubits exchanged per communication and also avoiding redundancy and eavesdropping checking. In practical scenarios, the difficult to build completely closed systems [19] is a motivating factor for the use of such simplified protocols, specially considering the already existing results regarding the use of DFS in

Elloá B. Guedes and Francisco M. de Assis. IQuanta – Institute for Studies in Quantum Computation and Information, Federal University of Campina Grande, Av. Aprígio Veloso, 882 – 58429-140, Campina Grande – Paraíba – Brazil. E-mails: {elloaguedes,fmarassis}@gmail.com. This work was supported by the Brazilian funding agencies CAPES and CNPq.

communications [20]–[22], particularly in long-distance [23].

The rest of this paper is organized as follows. Section II introduces the concepts regarding DFS; Section III shows how codes built from DFS can achieve unconditional security; Sections IV, V, and VI, show the concepts of collective dephasing, rotation and amplitude damping quantum channels, respectively, as well as QSDC and DSQC protocols to them with the corresponding suggestions for improvement. Lastly, Section VII presents the final remarks and suggestions for future work.

II. Decoherence-Free Subspaces and Subsystems

Due to decoherence, a quantum system may lose energy into the environment and decay to a ground state, its relative phase may be erased and, thus, the information it carries becomes lost [24]. In this section, we will show how to avoid these undesired effects despite the existence of decoherence.

Let a closed quantum system be composed by the *system of interest* S defined on a Hilbert space $\mathcal{H}$ and by the *environment* E. The Hamiltonian that describes this system is defined as follows:

$$\mathbb{H} = \mathbb{H}_S \otimes \mathbb{1}_E + \mathbb{1}_S \otimes \mathbb{H}_E + \mathbb{H}_{SE} \tag{1}$$

where $\mathbb{1}$ is the identity operator; and $\mathbb{H}_S$, $\mathbb{H}_E$ and $\mathbb{H}_{SE}$ denote the Hamiltonians of system, environment and system-environment interaction, respectively.

In order to prevent errors, it would be ideal that $\mathbb{H}_{SE}$ were equal to zero, indicating that system and environment are decoupled and evolve independently and unitarily under their respective Hamiltonians $\mathbb{H}_S$ and $\mathbb{H}_E$ [16]. However, in practical scenarios, such an ideal situation is not possible since no system is noiseless. So, after isolating a system to the best of our ability, we should aim for the realistic goals of the identification and correction of errors when they occur and/or avoiding noises when possible and/or suppressing noise in the system [19].

If some symmetries exist in the interaction between the system and the environment, it is possible to find a "quiet corner" in the system Hilbert space not experiencing decoherence. Let $\{A_i(t)\}$ be a set of operators in the *operator-sum representation* (OSR) corresponding to the evolution of the system. We say that a system density matrix ρ_S is *invariant* under the OSR operators $\{A_i(t)\}$ if $\sum_i A_i(t)\rho_S A_i^\dagger(t) = \rho_S$. We are now able to define the *decoherence-free subspaces* whose states are invariant despite a non-trivial coupling between the system and the environment.

Definition 1. *(Decoherence-Free Subspace [25]) A subspace $\tilde{\mathcal{H}}$ of a Hilbert space $\mathcal{H}$ is called decoherence-free with respect to a system-environment coupling if every pure state from this subspace is invariant under the corresponding OSR evolution for any possible environment initial condition:*

$$\sum_i A_i(t)|\tilde{k}\rangle\langle\tilde{k}|A_i^\dagger(t) = |\tilde{k}\rangle\langle\tilde{k}|, \forall|\tilde{k}\rangle\langle\tilde{k}| \in \tilde{\mathcal{H}}, \forall\rho_E(0). \tag{2}$$

Let the Hamiltonian of the system-environment interaction be $\mathbb{H}_{SE} = \sum_j \mathbf{S}_j \otimes \mathbf{E}_j$, where $\mathbf{S}_j$ and $\mathbf{E}_j$ are the system and environment operators, respectively. We consider that the environment operators $\mathbf{E}_j$ are linearly independent. The symmetries required to define a decoherence-free subspace are described in the theorem below. For a detailed proof or different formulations see [16, Sec. 5].

Theorem 1. *(*DFS Conditions *[24]) A subspace $\tilde{\mathcal{H}}$ is a decoherence-free subspace iff the system operators $\mathbf{S}_j$ act proportional to identity on the subspace:*

$$\mathbf{S}_j|\tilde{k}\rangle = c_j|\tilde{k}\rangle \qquad \forall j, |\tilde{k}\rangle \in \tilde{\mathcal{H}}. \tag{3}$$

The notion of a subspace which remains decoherence-free throughout the evolution of a system is not, however, the most general method for providing decoherence-free encoding of information in a quantum system [16]. Knill et al. [26] discovered a method for decoherence-free encoding into subsystems instead of into subspaces which is presented below.

Definition 2. *(Decoherence-Free Subsystem) Consider a decomposition of the whole Hilbert space $\mathcal{H} = (\mathcal{H}^A \otimes \mathcal{H}^B) \oplus \mathcal{K}$, where $\dim(\mathcal{H}) = \dim(\mathcal{H}^A) \cdot \dim(\mathcal{H}^B) + \dim(\mathcal{K})$. A subspace $\mathcal{H}^B$ of the full Hilbert space is a decoherence-free subsystem if*

$$\forall\rho^A, \forall\rho^B, \exists\tau^A : \mathcal{E}(\rho^A \otimes \rho^B) = \tau^A \otimes \rho^B, \tag{4}$$

where $\rho^A, \tau^A \in \mathcal{B}(\mathcal{H}^A)$, and $\rho^B \in \mathcal{B}(\mathcal{H}^B)$.

In fact, B is said to encode a decoherence-free subsystem if (4) is satisfied. In particular, when $dim(\mathcal{H}^A) = 1$, B is a decoherence-free subspace.

To make explicit the difference between decoherence-free subspaces and subsystems, consider the encoding of a generic qubit $\alpha|0\rangle + \beta|1\rangle$ into $\alpha|01\rangle + \beta|10\rangle$. In this case, the information has been encoded into a *subspace* of the two qubit Hilbert space. Suppose now that the information is encoded only into the first qubit of the two qubits, i.e., $\alpha|0\rangle + \beta|1\rangle \mapsto (\alpha|0\rangle + \beta|1\rangle) \otimes |\psi\rangle$. Since this second encoding is a one-to-many mapping from the quantum information in one qubit to a two qubit Hilbert space, then it is said that the information has been encoded into a *subsystem* [25].

In practice, identifying a useful symmetry and taking advantage of it can be very difficult. One must (i) identify the symmetry, and (ii) find the states which are invariant to the interaction. Despite these difficulties, a method for obtaining DFS was already proposed in the literature [27].

Quantum codes constructed from states of a DFS are classified as *quantum error-avoiding codes* (QEAC) and the

tasks of perturbation and recovery on them are trivial. They can be contrasted with *quantum-error correcting codes* (QECC) in some aspects. While QECCs are devised to correct errors after their occurrence, QEACs do not have the ability to correct errors since they avoid them; QECCs devised in practical circumstances belong to the class of non-degenerate codes while QEACs are highly degenerate; QEACs usually require a lower number of physical qubits to encode one logical qubit than QECCs. In particular, if the degeneracy attains the maximum, a QECC reduces to a QEAC what illustrates a circumstance in which a type of code becomes equivalent to the other [28].

The absence of decoherence in DFS has been shown as of major importance for implementations of quantum memory and quantum algorithms. Other applications of it cover encoding information in quantum dots, collective dissipation, noise reduction, among others [16], [19].

III. Unconditional Security in Decoherence-Free Subspaces and Subsystems

Until nowadays, many works in the literature already explored the potential of DFS in Quantum Communications. All of them consist of protocols against certain types of collective noise (such as rotation, dephasing, amplitude damping, among others) and consider the use of small DFS (with two or three qubits, for instance) [13]–[15], [29], [30]. Even experimental realizations were already implemented aiming at quantum information processing [31]–[34]. In the perspective of these works, the protection of information means avoiding the loss of coherence, maintaining the fidelity of the quantum states.

The work of Guedes and de Assis [17], [18] attempted to investigate the potential of DFS in terms of *secure message exchange*. To do so, they considered the following scenario: a sender (Alice) wants to convey secret classical messages through a quantum channel to a legitimate receiver (Bob). These messages must be protected from a wiretapper (Eve) that has full access to the environment.

To exchange the messages without being deceived by Eve, Alice and Bob use a QEAC build from the states of a DFS according to the following definition.

Definition 3. *Let $\tilde{\mathcal{H}}$ be a DFS spanned by a set of eigenvectors $\{|\tilde{k}\rangle\}$, i.e., $\tilde{\mathcal{H}} = Span[\{|\tilde{k}\rangle\}]$. A set of codewords of length n ($n = dim(\tilde{\mathcal{H}})$) for a set $\mathcal{U}$ of classical messages is a set of input states labeled by messages in $\mathcal{U}$, $\tilde{K}(\mathcal{U}) = \{\tilde{k}(u) : u \in \mathcal{U}\} \subseteq \tilde{\mathcal{H}}$, and a decoding measurement composed of a set of positive operators $\tilde{\mathcal{D}}_u$, $u \in \mathcal{U}$ with $\sum_{u\in\mathcal{U}} \tilde{\mathcal{D}}_u \leq \mathbb{1}$. The pair $(\tilde{K}(\mathcal{U}), \{\tilde{\mathcal{D}}_u : u \in \mathcal{U}\})$ is called a QEAC of length n for the set $\mathcal{U}$ of messages. The rate of this code is $\frac{1}{n}\log|\mathcal{U}|$.*

Using the code defined, if Alice wants to send a classical message u over a quantum channel $\mathcal{E}$, now she encodes it the QEAC defined over $\tilde{\mathcal{H}}$, obtaining $\tilde{k}(u)$. When she sends it through the communication channel, the message interacts with the environment (which is assumed to start in a pure state $|0_E\rangle$). This scenario is depicted in Figure 1. Bob then receives $\rho_{\text{Bob}}(\tilde{k}(u))$ and Eve receives $\rho_{\text{Eve}}(\tilde{k}(u))$ which are given by:

$$\rho_{\text{Bob}}(\tilde{k}(u)) = \text{Tr}_{\text{E}}\left[\mathcal{E}^{\otimes n}(\tilde{k}(u)\otimes|0_E\rangle\langle 0_E|)\right], \quad (5)$$

$$\rho_{\text{Eve}}(\tilde{k}(u)) = \text{Tr}_{\text{B}}\left[\mathcal{E}^{\otimes n}(\tilde{k}(u)\otimes|0_E\rangle\langle 0_E|)\right]. \quad (6)$$

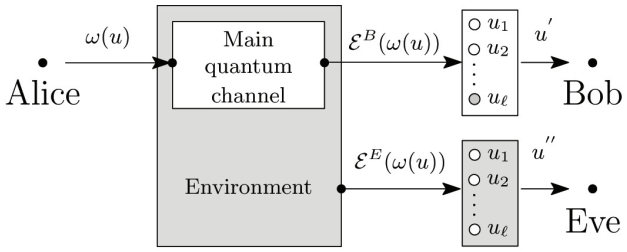

Fig. 1: General idea of the scenario described.

To analyze the security of such message exchange, Guedes and de Assis [17], [18] considered (i) the use of a QEAC; (ii) the interaction Hamiltonian of (1); (iii) the fact that Eve is restricted only to the environment; (iv) the accessible information by Bob and Eve; and (v) the theory of quantum wiretap channels [35], [36]. They established a proof that, in this scenario, the Holevo quantity of Eve is $\chi^{\text{Eve}} = 0$. Recalling that the Holevo quantity is an upper bound for the accessible information, it means that Eve does not gather anything from the secret message exchanged between Alice and Bob. It means that the criterion for *unconditional security* is achieved in this scenario.

On the other hand, the maximum accessible information by Bob is equal to $\max_{\{P\}}\chi^{\text{Bob}}$ where the maximum is taken over all probability distributions P over $\mathcal{U}$. This coincides with the classical capacity of a quantum channel according to the Holevo-Schumacher-Westmoreland theorem [37], [38]. It means that the ability of such quantum channel to send secret information can be made as large as its capacity to send ordinary classical information.

However, not all quantum channels exhibit such properties – only those which are subject to collective noise do. In collective noise quantum channels several qubits couple identically to the same environment, while undergoing both dephasing and dissipation [16].

In the next sections, some QSDC and DSQC protocol that consider the use of collective noise quantum channels will be examined taking into account the security results regarding DFS. The main objective is to point out some simplifications or modifications that aim at their enhancement.

IV. Collective Dephasing

Dephasing is a phenomenon in which the relative phase of a qubit is lost. Collective dephasing quantum channels act as follows on input qubits

$$|0\rangle \rightarrow |0\rangle, \tag{7}$$
$$|1\rangle \rightarrow e^{\imath\phi}|1\rangle. \tag{8}$$

where ϕ is the parameter of a collective-dephasing which fluctuates with time t. A logical qubit composed of two physical qubits with an antiparallel parity is immune to the collective dephasing, i.e.

$$|0_L\rangle = |01\rangle, \tag{9}$$
$$|1_L\rangle = |10\rangle. \tag{10}$$

A qubit can, thus, be codified as $|\psi_L\rangle = \alpha|0_L\rangle + \beta|1_L\rangle$. It is interesting to see that $|\psi_L\rangle$ does not suffer from the effects of decoherence

$$\begin{aligned}
\mathcal{E}(|\psi_L\rangle) &= \mathcal{E}\left(\alpha|0_L\rangle + \beta|1_L\rangle\right) && (11)\\
&= \alpha e^{\imath\phi}|01\rangle + \beta e^{\imath\phi}|10\rangle && (12)\\
&= e^{\imath\phi}\left(\alpha|01\rangle + \beta|10\rangle\right) && (13)\\
&= e^{\imath\phi}|\psi_L\rangle && (14)\\
&= |\psi_L\rangle, && (15)
\end{aligned}$$

because the overall phase factor $e^{\imath\phi}$ acquired due to the dephasing process has no physical significance. It means that both states $|01\rangle$ and $|10\rangle$ belong to $\tilde{\mathcal{H}}$, a decoherence-free subspace of the Hilbert space $\mathcal{H}$ in the collective dephasing quantum channel.

Gu et al. [13] proposed a DSQC over a collective dephasing quantum channel which is described as follows:

1) Alice prepares a sequence of quantum states in a three-photon entangled state
$$|\psi^+\rangle = \frac{1}{\sqrt{2}}\left(|0_A\rangle|0_{B1}1_{B_2}\rangle + |1_A\rangle|1_{B_1}0_{B_2}\rangle\right). \tag{16}$$
Notice that the two qubits B_1 and B_2 are entangled with the qubit A of Alice. Alice divides the quantum systems into two sequences S_A and S_B, where S_A is composed of the qubits A, and S_B is composed of qubits B_1 and B_2, respectively. Alice keeps S_A and sends S_B to Bob;
2) Bob picks up some samples for eavesdropping check after he receives S_B. He measures the two qubits with one of the two measuring bases $Z_{B_1}\otimes Z_{B_2}$ or $X_{B_1}\otimes X_{B_2}$, randomly. The state $|\psi^+\rangle$ can be written as follows
$$\begin{aligned}
|\psi^+\rangle = \frac{1}{2}\big[&|+_A\rangle\left(|+_{B_1}+_{B_2}\rangle - |-_{B_1}-_{B_2}\rangle\right)\\
&- |-_A\rangle\left(|+_{B_1}-_{B_2}\rangle - |-_{B_1}+_{B_2}\rangle\right)\big]. \qquad (17)
\end{aligned}$$
The outcomes obtained by Alice and Bob are correlated if they choose two corresponding measuring basis;
3) Bob tells Alice which qubits are chosen for eavesdropping check and the states obtained for the samples;
4) If Bob chooses $Z_{B_1}\otimes Z_{B_2}$, Alice chooses Z_A to measure her qubit; otherwise she chooses X_A;
5) Alice and Bob use the correlation between their samples to analyze the error rate for eavesdropping check. They code the outcomes $|0_A\rangle, |+_A\rangle, |0_{B_1}1_{B_2}\rangle, |+_{B_1}+_{B_2}\rangle$, and $|-_{B_1}-_{B_2}\rangle$ as the classical bit 0; and the outcomes $|1_A\rangle, |-_A\rangle, |1_{B_1}0_{B_2}\rangle, |+_{B_1}-_{B_2}\rangle$, and $|-_{B_1}+_{B_2}\rangle$ as the classical bit 1. The error rate must be below a threshold;
6) Alice tells Bob $C_A = O_A \oplus M_A$ where O_A is the outcome of the measurements performed by Alice; M_A is the secret classical message; and $\oplus$ denotes a sum modulo 2;
7) Bob reads the message directly with his outcome O_B, i.e., $M_A = O_B \oplus C_A$.

To analyze this protocol, we will estimate its Communication Complexity. The communication complexity is a measure of how many communications are necessary until two distribute parties become able to accomplish some task using as little communication as possible [39]. We will use the *hybrid variant* which takes into account the number of qubits and bits exchanged between the parties.

Let's suppose that the message M_A has m bits. First of all, Alice and Bob need to create a key with at least m bits by using the correlation between their outcomes to encode the message, that will be sent classically in the penultimate step of the protocol. If they use e qubits to eavesdropping check, the communication complexity of this protocol will be lower bounded by $Q^*(2\cdot m + e)$.

Considering the results shown in Section III, the use of states of a DFS enable unconditional security. So, if Alice uses the encoding $0 \equiv |01\rangle$ and $1 \equiv |10\rangle$, Bob can distinguish both states and decode the secret message sent by Alice. It results in a communication complexity of $Q^*(m)$ and a rate of 1 bit per channel use, considering that the bits 0 and 1 are equally probable. In comparison with the protocol proposed by Gu et al. [13], this scheme requires less than the half of the amount of bits and qubits exchanged.

The simplification proposed consists in a very simplified encoding-decoding scheme since it does not require entanglement between the parties nor eavesdropping check. Given that the states used belong to a DFS, no error threshold is necessary to be imposed, because such states are immune to errors. The process of encoding-decoding is also very trivial and can be constructed using only the well-known Pauli X gates as shown in Figure 2, where Figures 2a and 2b show the encoding for $|01\rangle$ and $|10\rangle$, respectively.

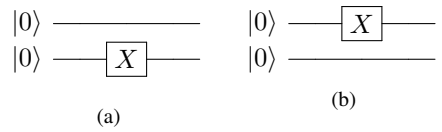

Fig. 2: Circuit for encoding the simplification suggested to the protocol of Gu et al. [13].

V. Collective Amplitude Damping

The phenomenon of energy dissipation when conveying a quantum state is modeled by the *collective amplitude damping channel*. This channel has the following OSR

$$\mathcal{E}(\rho) = A_0 \rho A_0^\dagger + A_1 \rho A_1^\dagger, \tag{18}$$

where the operation elements A_0 and A_1 are as follows

$$A_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix}, \qquad A_1 = \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix}, \tag{19}$$

where γ is the damping rate which can be thought of as the probability of losing a photon [40, p. 380].

A QSDC protocol over collective amplitude damping channels was proposed by Qin et al. [14]. This protocol makes use of two states from a DFS defined over this channel ($|0_L\rangle$ and $|1_L\rangle$) and also of other two states based on them ($|+_L\rangle$ and $|-_L\rangle$). These quantum states are

$$|0_L\rangle = |00\rangle, \tag{20}$$
$$|1_L\rangle = \frac{|10\rangle - |01\rangle}{\sqrt{2}}, \tag{21}$$
$$|+_L\rangle = \frac{|0_L\rangle + |1_L\rangle}{\sqrt{2}}, \tag{22}$$
$$|-_L\rangle = \frac{|0_L\rangle - |1_L\rangle}{\sqrt{2}}. \tag{23}$$

The protocol of Qin et al. [14] works as follows:

1) Alice generates a random sequence of the following states $\{|0_L\rangle, |1_L\rangle, |+_L\rangle, |-_L\rangle\}$ and sends to Bob;
2) Bob chooses a set of qubits to check eavesdropping. He measures them in one of the two bases randomly chosen ($\{|0_L\rangle, |1_L\rangle\}$ or $\{|+_L\rangle, |-_L\rangle\}$) and publish his outputs. Alice checks the outcomes in order judge whether there are eavesdroppers online. Bob performs certain operations on the remaining qubits, inserts some random bits, and sends back the encoded qubits to Alice;
3) Alice measures the received qubits in the same bases that she originally prepared. According to the relationship between her outcomes and the initial states, Alice can deterministically decode Bob's message;
4) Bob declares the position and values of the random bits. Alice judges the security and retrieves the message sent.

In this protocol, the number of communications required in the attempt to detect eavesdropping, besides the secret message, includes redundancy, random bits and also classical communications to publish measurement outcomes. If the message has m bits, then the communication complexity of this protocol is upper bounded by $Q^*(4 \cdot m + e)$. Besides that, even using a 2-qubit state, the rate achieved by this protocol is less than 0.25 bits per channel use.

A simplification in this protocol than can be suggested considers the use of a QEAC ($\tilde{K}(\{0,1\} = \{\tilde{k}(0) = |0_L\rangle, \tilde{k}(1) = |1_L\rangle\}, \{\tilde{D}_0 = |0_L\rangle\langle 0_L|, \tilde{D}_1 = |1_L\rangle\langle 1_L|\}$) to perform quantum secure direct communications. So, the secret message can be conveyed directly through the quantum channel without requiring random bits nor classical communications. The rate achieved is equal to 1 bit per symbol per channel use and the encoding-decoding procedures are less complex, which reduces the number of quantum gates required to implement this scheme.

Moreover, another suggestion to such scenario is to use the four states $|0_L\rangle$, $|1_L\rangle$, $|+_L\rangle$ and $|-_L\rangle$ from Eqs. (20)-(23) to perform QKD with the BB84 protocol [2] over a collective amplitude damping channel.

VI. Collective Rotation

A collective rotation noise can be written as

$$|0\rangle \rightarrow \cos\theta|0\rangle + \sin\theta|1\rangle, \tag{24}$$
$$|1\rangle \rightarrow -\sin\theta|0\rangle + \cos\theta|1\rangle. \tag{25}$$

where θ is the parameter of a collective-rotation noise which fluctuates with time t. Two states immune to the effects of this channels are the Bell states

$$\left|\phi^+\right\rangle = \frac{1}{\sqrt{2}}(|0_1 0_2\rangle + |1_1 1_2\rangle), \tag{26}$$
$$\left|\psi^-\right\rangle = \frac{1}{\sqrt{2}}(|0_1 1_2\rangle - |0_1 1_2\rangle). \tag{27}$$

Recently, Gu et al. [13] proposed a DSQC which makes use of the existing DFS on the collective rotation quantum channel. According to these authors, the creation of a key in this protocol is made as follows:

1) Alice prepares a three-photon entangled state

$$\left|\Phi^+\right\rangle_{AB_1B_2} = \frac{1}{\sqrt{2}}\left(|0_A\rangle\left|\phi^+_{B_1B_2}\right\rangle + |1_A\rangle\left|\psi^-_{B_1B_2}\right\rangle\right). \tag{28}$$

She keeps the qubit A and sends the qubits B_1 and B_2 to Bob;
2) After receiving the sequence sent by Alice, Bob picks up some samples for eavesdropping check. To do so, he measure some samples in three measuring bases $Z_{B_1} \otimes Z_{B_2}$, $Z_{B_1} \otimes X_{B_2}$ and $X_{B_1} \otimes Z_{B_2}$ randomly chosen;

3) Bob tells Alice which qubits are chosen for eavesdropping check and the outcomes of measurements on the samples;
4) If Bob chooses the measuring basis $Z_{B_1} \otimes Z_{B_2}$, then Alice chooses Z_A to measure her corresponding photon; otherwise, she chooses X_A;
5) Alice and Bob use the correlation between their samples to analyze the error rate. If the error rate is higher than the threshold, they repeat the protocol from the beginning. They code the outcomes $|0_A\rangle$, $|0_{B1}0_{B_2}\rangle$, $|1_{B_1}1_{B_2}\rangle$, $|+_A\rangle$, $|0_{B_1}+_{B_2}\rangle$, $|1_{B1}-_{B_2}\rangle$, $|-_{B_1}0_{B_2}\rangle$, and $|+_{B_1}1_{B_2}\rangle$ as the classical bit 0; while the outcomes $|1_A\rangle$, $|0_{B_1}1_{B_2}\rangle$, $|1_{B_1}0_{B_2}\rangle$, $|-_A\rangle$, $|0_{B_1}-_{B_2}\rangle$, $|1_{B_1}+_{B_2}\rangle$, $|+_{B_1}0_{B_2}\rangle$, and $|-_{B_1}1_{B_2}\rangle$ correspond to the classical bit 1;
6) Alice tells Bob the outcome $C_A = O_A \oplus M_A$ where O_A is the outcome of her measurement on photon A and M_A is the secret message that she wants to send Bob privately;
7) Bob reads out the secret message directly, i.e., $M_A = C_A \oplus O_B$ where O_B is the outcome of his measurements on the photons B_1 and B_2.

Before start the analysis of this protocol, we first make some considerations about it. The states of the DFS are Bell states; the existing correlation between the samples of Alice and Bob enable eavesdropping checking; and, lastly, an one-time pad encryption is made before the message is sent. This protocol is very similar to the one presented in Section IV, but considering the collective rotation scenario.

In face of the existence of a DFS, some simplifications can be applied in this protocol. If Alice and Bob want to send the message directly through the quantum channel, an appropriate encoding using only the states $|\phi^+\rangle$ and $|\psi^-\rangle$ can be made to send 1 bit of information per channel use. Two strategies can be used to simplify this protocol: the first one is to send the classical information directly via the quantum channel using an appropriate encoding, such as $0 \equiv |\phi^+\rangle$ and $1 \equiv |\psi^-\rangle$, and Bell measurements for decoding; the second strategy uses the quantum channel to create a private classical key and the message is sent through a classical channel, using a one-time pad encryption scheme, according to the last two steps of the protocol presented.

In both suggestions, the unconditional secrecy provided by the DFS is the key ingredient to increase the simplicity of the protocols. As can also be observed, in both cases no eavesdropping checking is required – it reduces significantly the number of communications performed. In the original protocol, the communication complexity is lower bounded by $Q^*(4 \cdot m)$ where m is the number of bits of the secret classical message to be exchanged. In contrast, the first simplification suggested has communication complexity equal to $Q^*(m)$, and the second is $Q^*(2 \cdot m)$ because and additional communication must be made to send the ciphertext through the classical channel. It is important to emphasize that, even in the second suggestion of simplification in which the number of communication is higher, there is a reduction of at least half of the number of communications performed when compared to the original protocol.

A second protocol found in the literature to collective rotation quantum channels is a DSQC proposed by Dong et al. [15] as is characterized as follows

1) Alice prepares a $4 \cdot m$ two-photons sequence randomly in the state $\{|0_L\rangle, |1_L\rangle, |+_L\rangle, |-_L\rangle\}$ where

$$|0_L\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{29}$$

$$|1_L\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \tag{30}$$

$$\begin{aligned} |+_L\rangle &= \frac{1}{\sqrt{2}}(|0_L\rangle + |1_L\rangle) \\ &= \frac{1}{\sqrt{2}}(|+\rangle|1\rangle + |-\rangle|0\rangle) \end{aligned} \tag{31}$$

$$\begin{aligned} |-_L\rangle &= \frac{1}{\sqrt{2}}(|0_L\rangle - |1_L\rangle) \\ &= \frac{1}{\sqrt{2}}(|-\rangle|1\rangle + |+\rangle|0\rangle) \end{aligned} \tag{32}$$

where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Alice sends it to Bob;
2) Bob measures the first qubit of each pair randomly in the Z or X basis, the second one in the Z basis, and records the measurement outcomes where $\{|0\rangle, |1\rangle\}$ are two bases of Z measurement, and $\{|+\rangle, |-\rangle\}$ are two bases of X measurement;
3) Alice and Bob check the security of the channel. Bob publicizes the measurements in sequence. Then they abandon the records in two situations: (i) when the state prepared by Alice is $|+_L\rangle$ or $|-_L\rangle$ and the measurement basis of the first qubit performed by Bob is the Z basis; and (ii) when the state prepared by Alice is $|0_L\rangle$ and $|1_L\rangle$ and Bob's measurement basis of the first qubit is in the X basis. After this step, about $2 \cdot m$ qubits remain. They then use m qubits for eavesdropping check;
4) If the quantum channel is safe, they use the leftover m measurements records to communicate. Alice and Bob agree on the following encoding: $0 \equiv |0_L\rangle, |+_L\rangle$ and $1 \equiv |1_L\rangle, |-_L\rangle$. Alice sends 0 through the classical channel if the secret message is the same as the encoding message. Otherwise 1 is sent.

The protocol of Dong et al. [15] requires $Q^*(5 \cdot m)$ bits and qubits exchanges to be performed. Most of these communications are spent in eavesdropping check and also in making Alice learn Bob's outcomes by the publication of the basis he used. This last step is essencial for the protocol execution because it makes both of them agree on the bits to

be used without communicate them directly.

When compared to the protocol of Gu et al. [13] which has communication complexity of $Q^*(4 \cdot m)$, we can conclude that the protocol of Dong et al. [15] is more expensive. However, it does not require entanglement between the parties as the former does. The two suggestions for simplification presented for the protocol of Gu et al. [13] can similarly be applied in this scenario, simplifying significantly the protocol, reducing the number of communications, and also providing unconditional security.

VII. Final Remarks

In this work, we proposed modifications into four already existing QSDC and DSQC protocols that make use of DFS aiming at simplification or at increase efficiency. Such modifications were motivated by a recent result of Guedes and de Assis [17], [18] that codes built with states from a DFS can achieve unconditional security. The simplifications proposed were compared with their original versions taking into account the communication complexity, a measure of how many communications a protocol performs.

In the collective dephasing quantum channel, the protocol of Gu et al. [13] was considered, which has communication complexity lower bounded by $Q^*(2 \cdot m + e)$. The simplification suggested does not require eavesdropping check and has communication complexity equal to $Q^*(m)$. Furthermore, the process of encoding-decoding becomes very trivial and can be constructed using only the well-known Pauli X gates.

To the collective amplitude damping scenario, the protocol of Qin et al. [14] was considered. The simplification proposed to it was the use of a QEAC with rate of 1 bit per channel use. The original version has communication complexity of $Q^*(4 \cdot m + e)$ in contrast with $Q^*(m)$ of the simplification suggested. Furthermore, we suggested how the four states of the existing DFS can be used to perform the BB84 over the collective amplitude damping quantum channel. Regarding the QKD using DFS in the collective amplitude damping quantum channel, no similar propositions were found in literature. It is in contrast with the collective rotation and dephasing quantum channels to which QKD protocols were already proposed [41], [42]

In the case of the collective rotation quantum channels, two protocols were considered: one proposed by Gu et al. [13] and another proposed by Dong et al. [15]. Two suggestions were made and are applicable to both protocols. In the best case observed, the number of communications performed was reduced in four times.

The use of DFS and its ability to send information with unconditional security can be exploited in practical scenarios of implementation of quantum channels. Since it is difficult to build completely closed systems [19], some results already consolidated considering the use of DFS in practical quantum communications [20]–[23] favors the implementation of such simplifications suggested. They can be considered well-suited for such scenarios for requiring (i) a small number of resources (absence of entanglement between the parties, for instance); (ii) a small amount of information exchange; and (iii) simple quantum gates that are already widely use in encoding-decoding processes.

In future works, we suggest the investigation of more general conditions to the existence of perfect secrecy in quantum systems.

Acknowledgments

The authors thanks Gilson O. Santos for his valuable suggestions.

References

[1] C. P. Williams, *Explorations in Quantum Computing*, 2nd ed., Springer, Ed. Springer, 2011.

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *Int. Conf. Computers, Systems & Signal Processing, Bangalore, India*.

[3] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Phys. Rev. Lett.*, vol. 67, pp. 661–663, 1991.

[4] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.*, vol. 68, p. 3121, 1992.

[5] D. Mayers, "Unconditional security in quantum cryptography," *Journal of the ACM*, vol. 48, no. 3, pp. 351–406, 2001.

[6] G. lu Long, F. guo Deng, C. W. X. han Lo, K. Wen, and W. ying Wang, "Quantum secure direct communication and deterministic secure quantum communication," *Front. Phys. China*, vol. 2, no. 3, pp. 251–272, 2007.

[7] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, ""event-ready-detectors" bell experiment via entanglement swapping," *Phys. Rev. Lett.*, vol. 71, p. 4287, 1993.

[8] T. Gao, "Controlled and secure direct communication using ghz state and teleportation," *Z. Naturforsch*, vol. 59, p. 597, 2004.

[9] T. Gao, F.-L. Yan, and Z.-X. Wang, "Controlled quantum teleportation and secure direct communication," *Chinese Phys.*, vol. 14, p. 893, 2005.

[10] F. L. Yan, , and X. Q. Zhang, "A scheme for secure direct communication using EPR pairs and teleportation," *Eur. Phys. J. B*, vol. 41, pp. 75–78, 2004.

[11] F. G. Deng and G. L. Long, "Secure direct communication with a quantum one-time pad," *Phys. Rev. A*, vol. 69, p. 052319, 2004.

[12] A. D. Zhu, Y. Xia, Q. B. Fan, and S. Zhang, "Secure direct communication based on secret transmitting order of particles," *Phys. Rev. A*, vol. 73, p. 022338, 2006.

[13] G. Bin, P. ShiXin, S. Biao, and Z. Kun, "Deterministic secure quantum communication over a collective-noise channel," *Science in China Series G: Physics, Mechanics and Astronomy*, vol. 52, no. 12, pp. 1913–1918, 2009.

[14] S. Qin, Q. Wen, L. Meng, and F. Zhu, "Quantum secure direct communication over the collective amplitude damping channel," *Science in China Series G: Physics, Mechanics and Astronomy*, vol. 52, no. 8, pp. 1208–1212, 2009.

[15] H.-K. Dong, L. Dong, X.-M. Xiu, and Y.-J. Gao, "A deterministic secure quantum communication protocol through a collective rotation noise channel," *Int. J. of Quantum Inf.*, vol. 8, no. 8, pp. 1389–1395, 2010.

[16] D. A. Lidar and K. B. Whaley, "Decoherence-free subspaces and subsystems," arXiv:quant-ph/0301032v1, pp. 83–120, 2003.

[17] E. B. Guedes and F. M. de Assis, "Unconditional security with decoherence-free subspaces," arXiv:quant-ph/1204.3000, pp. 1–6, 2012.

[18] ——, "Utilização de subespaços livres de descoerência em comunicações quânticas incondicionalmente seguras," in *XXX Simpósio Brasileiro de Telecomunicações – SBrT'12*, 2012.

[19] M. S. Byrd, L.-A. Wu, and D. A. Lidar, "Overview of quantum error prevention and leakage elimination," *Journal of Modern Optics*, vol. 51, no. 16-18, pp. 2449–2460, 2004.

[20] U. Dorner, A. Klein, and D. Jaksch, "A quantum repeater based on decoherence free subspaces," *Quant. Inf. Comp.*, vol. 8, p. 468, 2008.

[21] G. Jaeger and A. Sergienko, "Constructing four-photon states for quantum communication and information processing," *Int. J. Theor. Phys.*, vol. 47, p. 2120, 2008.

[22] Y. Xia, J. Song, Z.-B. Yang, and S.-B. Zheng, "Generation of four-photon polarization-entangled decoherence-free states within a network," *Appl. Phys. B*, vol. 99, pp. 651–656, 2010.

[23] P. Xue, "Long-distance quantum communication in a decoherence-free subspace," *Phys. Lett. A*, vol. 372, pp. 6859–6866, 2008.

[24] A. Shabani and D. Lidar., "Theory of initialization-free decoherence-free subspaces and subsystems," *Phys. Rev. A*, vol. 72, p. 042303, 2005.

[25] D. M. Bacon, "Decoherence, control, and symmetry in quantum computers," Ph.D. dissertation, University of California at Berkeley, 2001.

[26] E. Knill, R. Laflamme, and L. Viola, "Theory of quantum error correction for general noise," *Phys. Rev. Lett.*, vol. 84, p. 2525, 2000.

[27] M.-D. Choi and D. W. Kribs, "A method to find quantum noiseless subsystems," *Phys. Rev. Lett.*, vol. 96, p. 050501, 2006.

[28] L.-M. Duan and G.-C. Guo, "Quantum error avoiding codes versus quantum error correcting codes," *Phys. Lett. A*, vol. 255, pp. 209–212, 1999.

[29] K. Majgier, H. Maassen, and K. Zÿczkowski, "Protected subspaces in quantum information," *Quantum Inf. Process*, vol. 9, pp. 343–367, 2010.

[30] M. S. Byrd, D. A. Lidar, L.-A. Wu, and P. Zanardi, "Universal leakage elimination," *Phys. Rev. A*, vol. 71, p. 052301, 2005.

[31] L. Viola, E. M. Fortunato, M. A. Pravia, E. Knill, R. Laflamme, and D. G. Cory, "Experimental realization of noiseless subsystems for quantum information processing," *Science*, vol. 293, pp. 2059–2063, 2001.

[32] A. Beige, D. Braun, B. Tregenna, and P. L. Knight, "Quantum computing using dissipation to remain in a decoherence-free subspace," *Phys. Rev. Lett.*, vol. 85, p. 1762, 2000.

[33] D. Kielpinski, "A decoherence-free quantum memory using trapped ions," *Science*, vol. 291, p. 1013, 2001.

[34] P. G. Kwiat, A. J. Berglund, J. B. Altepeter, and A. G. White, "Experimental verification of decoherence-free subspaces," *Science*, vol. 290, pp. 498–501, 2000.

[35] N. Cai, A. Winter, and R. W. Yeung, "Quantum privacy and quantum wiretap channels," *Problems of Information Transmission*, vol. 40, pp. 318–336, 2004.

[36] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," *IEEE Trans. Inf. Th.*, vol. 51, no. 1, pp. 44 –55, 2005.

[37] A. S. Holevo, "The capacity of the quantum channel with general signal states," *IEEE Trans. Info. Theory*, vol. 4, no. 1, pp. 269–273, 1998.

[38] B. Schumacher and M. D. Westmoreland, "Sending classical information via noisy quantum channels," *Phys. Rev. A*, vol. 56, pp. 131–138, 1997.

[39] R. de Wolf, "Quantum communication and complexity," *Theoretical Computer Science*, vol. 287, no. 1, pp. 337–353, 2002.

[40] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, C. U. Press, Ed. Bookman, 2010.

[41] J.-C. Boileau, D. Gottesman, R. Laflamme, D. Poulin, and R. W. Spekkens, "Robust polarization-based quantum key distribution over a collective-noise channel," *Phys. Rev. Lett.*, vol. 92, p. 017901, 2004.

[42] X.-H. Li, F.-G. Deng, and H.-Y. Zhou, "Efficient quantum key distribution over a collective noise channel," *Phys. Rev. A*, vol. 78, p. 022321, 2008.