Quantum Key Distribution over Collective Amplitude Damping Quantum Channels

Elloá B. Guedes and Francisco M. de Assis
Institute for Studies in Quantum Computation and Information (IQuanta)
Post Graduation Programs in Electrical Engineering and Computer Science
Federal University of Campina Grande (UFCG)
Campina Grande – Paraíba – Brazil
Email: {elloaguedes, fmarassis}@gmail.com

***Abstract*—One of the most mature quantum information techniques nowadays is Quantum Key Distribution (QKD) in which two legitimate parties make use of a protocol to create a symmetric private key using a quantum channel. The quantum channel is not secure, since there may be an eavesdropper intercepting and re-sending the quantum states that are sent through it. One of the main problems in using QKD protocols is the existence of noise which can make difficult the task of eavesdropping checking. Considering these issues, this paper presents a QKD protocol over a collective amplitude damping quantum channel that makes use of decoherence-free subspaces and subsystems. The QKD protocol proposed is noiseless despite the errors existing in the quantum channel. Moreover, it makes the probability of the eavesdropper's retrieve the secret message negligible asymptotically. Besides, the probability of eavesdropper detection is stable during the whole communication which eases the eavesdropping checking procedures.**

***Keywords*—Quantum Key Distribution; One-Time Pad; Decoherence-Free Subspaces and Subsystems.**

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 a counterpart in Classical Communication, such as: (i) a qubit does not have 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 information conveying through quantum channels.

The *Quantum Key Distribution* (QKD) [2]–[5] is one of the most mature quantum information techniques nowadays. According to QKD, two remote users can create a private key securely. This key is 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.

In order to avoid the noise, some QKD protocols [6], [7] considered the use of quantum channels which are subject to *collective decoherence*. In this scenario, all qubits which suffer noise are affected exactly in the same way [8]. Considering this particularity, in such quantum channels it is possible to find some symmetries that protect the information from the noise. The states which remain unaffected by the decoherence compose a *decoherence-free subspace or subsystem* (DFS) [9].

Boileau et al. [6] proposed two QKD protocols using the DFS existing in the collective rotation quantum channel. The first protocol considers a subspace and the second a subsystem, both free of decoherence. Their protocol considers also the use of singlets and the encoding is based on the parity of qubits. Thanks to that, an uncertainty is inserted about the state originally sent from the perspective of the eavesdropper. However, it does not affect the legitimate parties of the protocol, enabling them to create a private key that can be later used to encrypt a classical message. It is important to emphasize that the eavesdropper is not able to affect the qubits exchanged, nor gather information about the key. Based on similar ideas, Li et al. [7] proposed two QKD protocols using DFS and considering the collective rotation and dephasing quantum channels.

The *amplitude damping* is a type of quantum noise which can make a qubit be lost. This type of error is also subject to collective decoherence, characterizing the *collective amplitude damping quantum channels*. Although these quantum channels have a DFS, no QKD protocols have been developed for them. Hence, the main objective of the present work is to characterize a QKD protocol over collective amplitude damping quantum channels, aiming at providing a secure way to create private keys between the legitimate parties despite the existence of an eavesdropper on the channel.

The present work is organized as follows. The decoherence-free subspaces and subsystems are characterized and exemplified in Section II. The collective amplitude damping quantum channels and the decoherence-free subspaces existing on their structure are shown in Section III. The model of communication considered as well as the steps that comprise the protocol proposed are shown in Section IV. An analysis of security is discussed in Section V. Lastly, final remarks and suggestions for future work are presented in Section VI.

Notations and Conventions – The Dirac notation [10] will be used to denote quantum states and operations over them throughout the paper. A quantum state is said to be pure if it can be represented by a unitary vector in the Hilbert space $\mathcal{H}$. The *Hadamard operation*, implemented by the gate H, has the following matricial representation $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. The symbol $\mathbb{1}$ denotes the *identity matrix*.

 ISBN: 978-1-61208-283-7

II. Decoherence-Free Subspaces and Subsystems

Due to decoherence, a quantum system may begin to lose energy into the environment and decay to a ground state, its relative phase may be erased and, thus, the information it carries may be lost [11]. In this section, we will show how to avoid these undesired effects despite the existence of decoherence.

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

$$\mathbb{H} = \mathbb{H}_S \otimes \mathbb{1}_E + \mathbb{1}_S \otimes \mathbb{H}_E + \mathbb{H}_{SE}, \quad (1)$$

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 $\mathbb{H}_E$ [9]. 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 [12].

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 $\{E_i(t)\}$ 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 $\{E_i(t)\}$ if $\sum_i E_i(t)\rho_S E_i^\dagger(t) = \rho_S$. 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)**.** *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:*

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

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 [9, Section 5].

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

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

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 [9]. Knill et al. discovered a method for decoherence-free encoding into subsystems instead of into subspaces, which is presented below [13].

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, for a quantum channel $\mathcal{E}$:*

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

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

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

A. Example

The *collective rotation quantum channel* acts on the input as follows:

$$|0\rangle \mapsto \cos\theta|0\rangle + \sin\theta|1\rangle, \quad (5)$$
$$|1\rangle \mapsto -\sin\theta|0\rangle + \cos\theta|1\rangle, \quad (6)$$

where θ is the collective rotation parameter which fluctuates over time t. Two states that are immune to the decoherence caused by this quantum noisy channel are the following Bell states

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad (7)$$
$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \quad (8)$$

Despite being entangled, these states are distinguishable and can be properly obtained at the channel's end using Bell measurements.

If one encodes a generic quantum state $|\psi\rangle = a|0\rangle + b|1\rangle$ using the mentioned Bell states as logic qubits, i.e., $|\psi_L\rangle = a|\beta_{00}\rangle + b|\beta_{11}\rangle$, we have that the resulting encoded state is protected from decoherence since the logic states are immune to the decoherence caused by the collective rotation quantum channel $\mathcal{E}$ as follows:

 ISBN: 978-1-61208-283-7

$$\mathcal{E}(|\beta_{00}\rangle) = \frac{1}{\sqrt{2}}\left[(\cos\theta|0\rangle + \sin\theta|1\rangle) \otimes (\cos\theta|0\rangle + \sin\theta|1\rangle) + (-\sin\theta|0\rangle + \cos\theta|1\rangle) \otimes (-\sin\theta|0\rangle + \cos\theta|1\rangle)\right] \quad (9)$$

$$= |\beta_{00}\rangle, \quad (10)$$

and

$$\mathcal{E}(|\beta_{11}\rangle) = \frac{1}{\sqrt{2}}\left[(\cos\theta|0\rangle + \sin\theta|1\rangle) \otimes (-\sin\theta|0\rangle + \cos\theta|1\rangle) + (-\sin\theta|0\rangle + \cos\theta|1\rangle) \otimes (\cos\theta|0\rangle + \sin\theta|1\rangle)\right] \quad (11)$$

$$= |\beta_{11}\rangle. \quad (12)$$

Besides the collective rotation quantum channel, the collective amplitude damping and the collective dephasing quantum channels are also examples of noisy quantum channels that have subspaces and subsystems that are immune to the existing decoherence.

III. Collective Amplitude Damping Quantum Channel

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

$$\mathcal{E}(\rho) = A_0\rho A_0^\dagger + A_1\rho A_1^\dagger, \quad (13)$$

where the operation elements A_0 and A_1 are as follows:

$$A_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix}, \qquad A_1 = \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix}, \quad (14)$$

where γ is the damping rate which can be thought of as the probability of losing a photon [1, p. 380].

In this channel, due to its collectiveness behaviour, all qubits which suffer amplitude damping are subject to the same damping rate. Thanks to that, it is possible to find a "quiet corner" in the Hilbert space of this channel whose states do not suffer from the effects caused by this type of decoherence. Such states are said to belong to a DFS $\tilde{\mathcal{H}}$ of the input Hilbert space $\mathcal{H}$ of this quantum channel [9]. If a state $\rho \in \tilde{\mathcal{H}}$, where $\tilde{\mathcal{H}} \subset \mathcal{H}$, then it is not affected by the existing decoherence on the collective amplitude damping quantum channel $\mathcal{E}$, i.e., $\mathcal{E}(\rho) = \rho$.

In this quantum channel, there are three different DFS, with dimensions 1, 2 and 3, respectively, as shown below:

$$\tilde{\mathcal{H}}_1 = \{|1\rangle\}, \quad (15)$$

$$\tilde{\mathcal{H}}_2 = \left\{|00\rangle, \frac{|01\rangle - |10\rangle}{\sqrt{2}}\right\}, \quad (16)$$

$$\tilde{\mathcal{H}}_3 = \left\{\frac{1}{\sqrt{6}}(-2|001\rangle + |010\rangle + |100\rangle), \frac{1}{\sqrt{2}}(|011\rangle - |101\rangle), |000\rangle\right\}. \quad (17)$$

In particular, the DFS $\tilde{\mathcal{H}}_2$ will be used in the quantum key distribution protocol that will be described in the next section.

IV. Proposed Protocol

Our protocol considers the scheme of communications showed in Figure 1. The legitimate parties (Alice and Bob) are connected through a classical channel and also through a collective amplitude damping quantum channel. Both channels are considered insecure. Despite of that, the objective of Alice and Bob is to create a private key to perform a secure classical message exchange.

The eavesdropper Eve has access to the quantum channel between Alice and Bob. She makes use of a device, which measures the quantum states sent through the channel and stores the basis used for measurement as well as the classical result obtained.

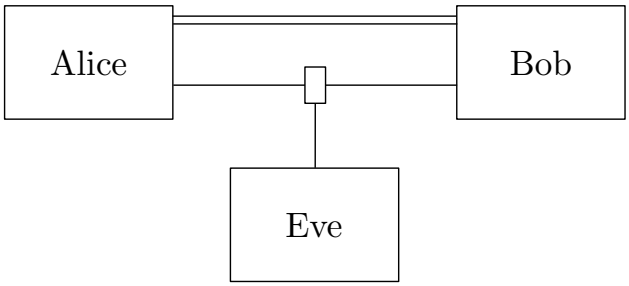

Fig. 1. Communication model considered. The single line wire represented is used for quantum communications while the double line wire is used for classical communications.

The idea of this protocol is very similar to the BB84 QKD protocol [2], but with the advantage of the noise avoidance due to the use of the DFS existing. The description of the protocol will be presented in the sections below.

A. Protocol Description

The legitimate parties Alice and Bob makes use of the following quantum states:

$$|\rightarrow\rangle = |00\rangle, \quad (18)$$

$$|\uparrow\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}, \quad (19)$$

$$|\nearrow\rangle = |{+}{+}\rangle, \quad (20)$$

$$|\searrow\rangle = \frac{|{+}{-}\rangle - |{-}{+}\rangle}{\sqrt{2}}, \quad (21)$$

where $|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ and $|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$. Notice that the quantum states $|\nearrow\rangle$ and $|\searrow\rangle$ are obtained from $|\rightarrow\rangle$ and $|\uparrow\rangle$ by a Hadamard operation. Thanks to the DFS properties, none of the quantum states presented in Eqs. (18)-(21) are affected by the collective amplitude damping. The quantum circuits illustrated on Figure 2 show how to obtain such quantum states.

 ISBN: 978-1-61208-283-7

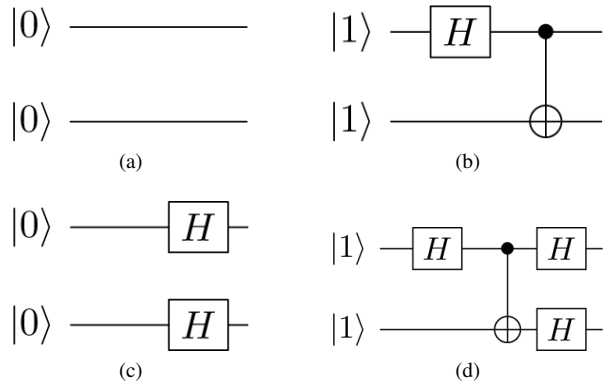

Fig. 2. Quantum circuits that implement the states $|\rightarrow\rangle$, $|\uparrow\rangle$, $|\nearrow\rangle$, and $|\searrow\rangle$, respectively.

Alice starts the protocol sending states randomly chosen from the set $\{|\rightarrow\rangle, |\uparrow\rangle, |\nearrow\rangle, |\searrow\rangle\}$. Bob and Eve measure the states received using the bases horizontal-vertical $+ = \{|\rightarrow\rangle, |\uparrow\rangle\}$ or diagonal $\times = \{|\nearrow\rangle, |\searrow\rangle\}$ also randomly chosen.

Let's first consider that Eve is not affecting the communication between Alice and Bob. Table I shows some examples of the results obtained by Alice and Bob in order to create their private symmetric key. If Alice sends $|\rightarrow\rangle$ or $|\uparrow\rangle$ and Bob measures with $+$, he will obtain bits 0 and 1, respectively, with 100% of certainty. The same is true when Alice sends $|\nearrow\rangle$ and $|\searrow\rangle$ and Bob measures with $\times$. However, for instance, if Alice sends $|\rightarrow\rangle$ and Bob measures with $\times$, then there is a probability of 0.5 that he will receive the bit 0 and of 0.5 regarding the bit 1.

TABLE I. RESULTS OBTAINED BY BOB AFTER MEASURING THE QUANTUM STATES SENT BY ALICE WITH THEIR RESPECTIVE PROBABILITY.

Alice sends	$\|\rightarrow\rangle$	$\|\uparrow\rangle$	$\|\nearrow\rangle$	$\|\searrow\rangle$
Bob measurement	$+$	$+$	$\times$	$\times$
Bit obtained	0	1	0	1
Probability	1	1	1	1

Alice sends	$\|\rightarrow\rangle$	$\|\searrow\rangle$	$\|\nearrow\rangle$	$\|\uparrow\rangle$
Bob measurement	$\times$	$+$	$+$	$\times$
Bit obtained	0 or 1	0 or 1	0 or 1	0 or 1
Probability	0.5	0.5	0.5	0.5

In order to avoid uncertainties regarding the bits obtained by Bob, he will communicate to Alice the sequence of bases he used to measure the qubits that she sent. Alice will return to Bob a string of 0's and 1's, where 0 indicates that the respective measurement must be discarded because it leads to uncertainty. After this process, even without communicating the results of the measurements, Alice and Bob agree on the results obtained after the measurement. The bits resultant will compose the private symmetric key that they will use in an one-time pad encryption of the secret classical message sent through the classical channel.

To illustrate the protocol proposed, let's suppose that Alice sends to Bob the following sequence of qubits: $|\nearrow\rangle, |\uparrow\rangle, |\uparrow\rangle, |\rightarrow\rangle, |\nearrow\rangle, |\searrow\rangle, |\uparrow\rangle$. Bob uses the sequence of bases $+, +, \times, +, \times, +, +$ and obtains the sequence of bits given by 0100011. Bob sends the sequence of bases he used through the classical channel and Alice returns him the sequence 0011101. The sequence of bits sent by Alice indicates that the first, second and sixth bits obtained by Bob must be discarded. So, the private symmetric key between Alice and Bob will have length 5 and will be equal to 00001. With this key, Alice can send Bob a classical message in secrecy by using the one-time pad scheme.

The *one-time pad* encryption scheme requires that the message and the secret key must be of equal length. Let m be the message and k be the key, both with n bits. The encrypted version of the message e is obtained by $e_i = m_i \oplus k_i$, for $i = 1, \ldots, n$, where $\oplus$ denotes the addition modulo 2. If the key is used only a single time and if it is kept in secret, then the conditions for *perfect secrecy* in the communication are guaranteed [14].

In the considered example, let's suppose that Alice wants to send a message $m = 10101$ to Bob. She will follow the one-time pad steps, considering the key $k = 00001$, and will obtain $e = 10100$ that will be sent through the classical channel to Bob. Upon receiving $e = 10100$, Bob will use the key $k = 00001$, and will retrieve the message sent by Alice by also using the $\oplus$ operation, which results in $m = 10101$. This way, the quantum key distribution protocol and the secret classical message exchange conclude successfully.

In the characterization of the protocol presented, the eavesdropper Eve makes no action during the key creation process. However, it is very unrealistic and her action on the quantum channel must be considered. The next section shows how she can gather information from the private key created by Alice and Bob and how they can use strategies in order to detect her presence and to avoid her success.

B. Eavesdropping Checking

According to the model of communications considered, Eve can perform measurements in the state sent by Alice, recover a bit from it, and resend the resulting state to Bob. During this process, Eve can not only recover bits from the private key, but also change the quantum state originally sent to Bob.

Eve performs measurements in the state send by Alice using the bases $+$ and $\times$ randomly chosen, i.e, using the same strategy than Bob. To do so, she uses a device which gets the input on the quantum channel, measures it, and resend the resulting quantum state to the channel's output. The effects on the measurements performed by her may degrade the information received by Bob. Table II synthesizes the effects of Eve on the quantum channel.

If by random choice Eve chooses the same basis that Alice used to prepare the quantum states, as shown in the first part of Table II, she will measure the same bit than Bob and will cause no disturbance on the system. However, if she measure the states using the wrong basis, as shown in the second part of Table II, she will have no certainty about the state sent by Alice and will also modify the state received by Bob. When this second situation happens, Alice and Bob can perform successfully the eavesdropper detection.

To perform the eavesdrop detection, besides the bases exchange between Bob and Alice, Bob will also reveal to Alice some bits that he obtained after the measurement. Those bits revealed are important to detect the eavesdropper but they must be discarded after that in order to not compromise the security

 ISBN: 978-1-61208-283-7

TABLE II. STATES SENT BY ALICE AND MEASURED BY THE EAVESDROPPER EVE.

Alice sends	$\|\rightarrow\rangle$	$\|\uparrow\rangle$	$\|\nearrow\rangle$	$\|\searrow\rangle$
Eve measurement	$+$	$+$	$\times$	$\times$
Eve's resulting bit	0	1	0	1
Probability	1	1	1	1
Bob received state	$\|\rightarrow\rangle$	$\|\uparrow\rangle$	$\|\nearrow\rangle$	$\|\searrow\rangle$

Alice sends	$\|\rightarrow\rangle$	$\|\uparrow\rangle$	$\|\nearrow\rangle$	$\|\searrow\rangle$
Eve measurement	$\times$	$\times$	$+$	$+$
Eve's resulting bit	0 or 1	0 or 1	0 or 1	0 or 1
Probability	0.5	0.5	0.5	0.5
Bob received state	$\|\nearrow\rangle$ or $\|\searrow\rangle$	$\|\nearrow\rangle$ or $\|\searrow\rangle$	$\|\rightarrow\rangle$ or $\|\uparrow\rangle$	$\|\rightarrow\rangle$ or $\|\uparrow\rangle$

of private key. To illustrate such situation, let's suppose that Alice sent Bob the state $|\nearrow\rangle$, Eve measured it with the basis $+$ and obtained the bit 1, and Bob measured with the basis $\times$ and received the bit 1. When Bob tells Alice that he used the basis $\times$ and obtained the bit 1, she can notice that something is wrong and can conclude that there exists an eavesdropper in the quantum channel, because the scenario considered is noiseless.

So, in order to create a private key in secrecy, they must communicate not only the bases used for measurement, but also some of the results obtained. It is essential to ensure the security in the protocol proposed as it is going to be shown in the next section.

V. SECURITY ANALYSIS

The goal of an ideal key distribution is to allow Alice and Bob, who share no information initially, to share a secret key (a string of bits) at the end. Eve, the eavesdropper, should not obtain information about the key. Also, whatever Eve does, Alice's and Bob's key should be identical. It is assumed that all quantum and communication between Alice and Bob passes through Eve, and similarly for classical communication [5].

No quantum key distribution protocol can succeed if Eve has the power to impersonate Alice while communicating with Bob and to impersonate Bob while communicating with Alice. If Alice and Bob meet previously, there are authentication techniques which can be used to ensure unconditional security [15]. However, in a scenario where Alice and Bob have never exchanged a secret key before, one must assume that Alice and Bob have access to a faithful (classical) public channel so a third part cannot accomplish the impersonation attack without being detected.

Different from classic communication, the security of quantum communication is based on the laws of physics rather than the difficulty of computation. The eavesdropper Eve is so powerful that her ability is only limited by the principles in quantum mechanics. However, the *No-Cloning Theorem* [16] forbids Eve to eavesdrop the quantum signals freely and fully as her action will inevitably disturb the unknown states and leave a trace in the outcomes obtained by the two legitimate users [7]. These facts will help us in the characterization of the security in the proposed protocol.

The eavesdropping strategy that we will consider in the security analysis of the proposed protocol is the *intercept and resend attack* [17] in which Eve measures the quantum state sent by Alice, obtains a bit, and re-sends the resulting quantum

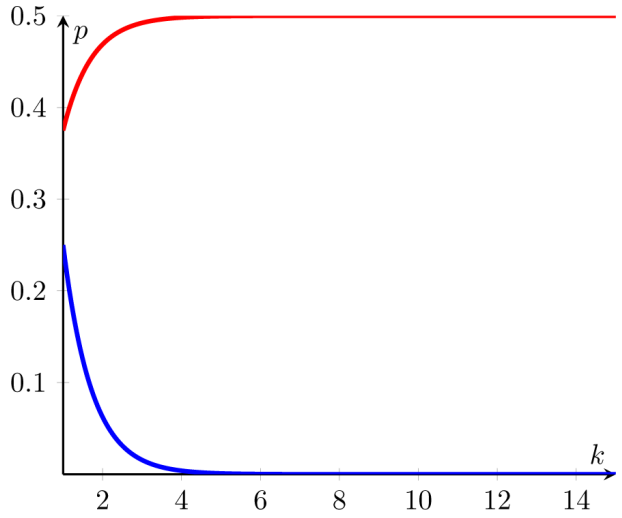

Fig. 3. Graphic showing the exponential decrease in Eve's success probability in recovering all key bits (blue line) and the probability of Alice and Bob detecting the eavesdropper per bit exchanged to create the secret key (red line).

state to Bob. This kind of attack was already depicted in Section IV, but the probability of eavesdropping detection and of Eve's success is going to be described from now on. It is important to emphasize that since this protocol is based on the BB84 QKD protocol [2], the same proofs of security are adequate to our proposition. We strongly suggest the work of Mayers [5] as a source of a more formal approach to these proofs.

If Alice wants to send a bit b to Bob, she can encode it in two different ways. Eve, upon intercepting it, can also use two options of measurement bases. Her chance of guessing the correct bit is equal to 50%. But if she uses an incorrect basis and it leads to Bob receiving a different bit than was originally sent by Alice, the chance of eavesdropping detection is also of 50% per bit sent.

Let us suppose that Alice and Bob want to create a private key of size k. Given that Eve may perform intercept and resend attacks, they will reinforce the eavesdropping checking procedure by using k additional bits. The probability of Eve measuring correctly the $2 \cdot k$ bits exchanged between the legitimate parties is of $p(2 \cdot k) = 0.5^{2 \cdot k}$ which decreases exponentially as the size of the key increases as shown in the blue line in Figure 3.

However, if Eve mistakes a single bit in a $2 \cdot k$ bits sequences (probability equal to $p_{\text{error}}(1) = 0.5$ per bit), it may result in a bit error detection by Bob and Alice (probability equal to $p_{\text{detection}}(1) = 0.5$ per bit missed by Eve). Considering these probabilities, the chance of detecting Eve at the n-th bit goes asymptotically to 0.5, as shown in the red line of the graphic in Figure 3, i.e., it is strongly related with the probability of error detection. Differently from the probability of Eve success, the probability of eavesdropping detection is independent per bit exchanged. Since Eve can change a qubit and this alteration may not be detected, as reported in Tables I and II, there always a probability of not detecting the eavesdropper in the communication.

As it can be seen, while the success of Eve depends on guessing all bits without disturbing the communication between Alice and Bob, her detection depends on one mistake

 ISBN: 978-1-61208-283-7

on her measurements which disturbs the bit received by Bob used in the eavesdrop checking process. Thus, we can conclude that the ability of the protocol to detect eavesdropping is high, ensuring enough security for practical scenarios of its use. This concludes the analysis of security of the quantum key distribution protocol proposed.

VI. Conclusion

The first practical demonstration of a QKD protocol took place in the early 1990s using photons over a distance of 30 cm through air. After that, the next implementation over the atmosphere guaranteed a secure communication with quantum bits over a distance of 2 km. After that, QKD protocols could be implemented in distances up to 250 km [18]. Nowadays, even commercial devices are being developed and sold to perform secure quantum key distribution [19].

However, one of the main problems in practical QKD is the noise, which can not only affect the communication between the legitimate parties, but can also favor an existing eavesdropper. In the attempt to minimize such problems, we proposed a QKD protocol over a collective amplitude damping quantum channel where an eavesdropper performs intercept and resend attacks.

This protocol is mainly based on BB84 QKD protocol [2], but since it considers the existing DFS on the quantum channel taken into account, the communication is noiseless. However, we consider the existence of an eavesdropper which aims at discovering the private key in the attempt to make a breach of security in the message exchange between Alice and Bob. In order to avoid it, the legitimate parties must use extra bits, randomness and also certain procedures for eavesdropping checking. As shown in Section V, it causes a very low probability of Eve's success while the probability of eavesdropping detection is high.

This work contributes to the use of the DFS in secure communications. If the eavesdropper is passive, following the model of quantum wiretap channels [20], [21], it is possible to reach unconditional security in the communications [22], [23]. This scenario not always occurs, so it is essential to consider other protocols and techniques. Since DFS arise where collective decoherence takes place [24], other works developing QKD protocols for collective dephasing and rotation quantum channels were already considered [6], [7]. However, so far, no protocol for QKD on collective amplitude damping quantum channels were known.

In practical scenarios, some works already report the implementation of quantum channels with DFS [25]–[27] even in long distance [28]. With this already existing technology, the proposed protocol can be adopted in realistic scenarios to provide secure communications.

In future work, we aim at proposing other protocols and techniques for secure communications over eavesdropped quantum noisy channels.

Acknowledgements

The authors acknowledge the financial support rendered by the Brazilian funding agencies CAPES and CNPq, by the Post Graduation Program in Electrical Engineering at the Federal University of Campina Grande, and by the project QUANTA/RENASIC/FINEP.

References

[1] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information, 2nd ed., Bookman: Cambridge University Press, 2010.

[2] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," ICCSSP Press, 1984, pp. 175-179.

[3] A. K. Ekert, "Quantum Cryptography Based on Bell's Theorem," Phys. Rev. Lett., vol. 67, 1991, pp. 661-663.

[4] C. H. Bennett, "Quantum Cryptography Using any Two Nonorthogonal States," Phys. Rev. Lett., vol. 68, 1992, pp. 3121-3124.

[5] D. Mayers, "Unconditional Security in Quantum Cryptography," Journal of the ACM, vol. 48, 2001, pp. 351-406.

[6] 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, 2004, pp. 017901.

[7] X.-H. Li, F.-G. Deng and H.-Y. Zhou, "Efficient Quantum Key Distribution Over a Collective Noise Channel," Phys. Rev. A, vol. 78, 2008, pp. 022321.

[8] J. Stolze and D. Suter, Quantum Computing – A short course from theory to experiment, Wiley: VCH Verlag, 2004.

[9] D. A. Lidar and K. B. Whaley, "Decoherence-Free Subspaces and Subsystems", arxiv: quantum-ph/0301032v1, 2003. (Retrieved: May, 2013).

[10] P. Dirac, The principles of Quantum Mechanics, 4th ed., Oxford UniversityPress: Oxford, 1982.

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

[12] M. S. Byrd, L.-A. Wu and D. A. Lidar, "Overview of quantum error prevention and leakage elimination," Journal of Modern Optics, vol. 51, 2004, pp. 2449-2460.

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

[14] C. Paar and J. Pelzl, Understanding Cryptography, Springer: Springer, 2010.

[15] M. N. Wegman and J. L. Carter, "New Hash Function and their Use in Authentication and Set Equality," J. Comput. Syst. Sci., vol. 22, 1981, pp. 265-279.

[16] W. K. Wootters and W. H. Zurek, "A Single Quantum Cannot be Cloned," J. Comput. Syst. Sci., vol. 299, 1982, pp. 802-803.

[17] D. Kalamidas, "Single-Photon Quantum Error Rejection and Correction With Linear Optics," Phys. Lett. A, vol. 343, 2005, pp. 331-335.

[18] J. Mullins, "Making Unbreakable Code," IEEE Spectrum, vol. May, 2002, pp. 40-45.

[19] ID Quantique, "Quantum Key Distribution", http://www.idquantique.com, 2013. (Retrieved: May, 2013).

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

[21] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," IEEE Transactions on Information Theory, vol. 51, 2005, pp. 44 -55.

[22] E. B. Guedes and F. M. Assis, "Utilização de Subespaços Livres de Descoerência em Comunicações Quânticas Incondicionalmente Seguras," Proc. Simpósio Brasileiro de Telecomunicações (SBrT'12), SBrT Press, 2012, pp. 1-5.

[23] E. B. Guedes and F. M. Assis, "Unconditional Security with Decoherence-Free Subspaces", arXiv:quant-ph/1204.3000, 2012, pp. 1-6. (Retrieved: May, 2013).

[24] P. Zanardi and M. Rasetti, "Noiseless quantum codes," Phys. Rev. Lett., vol. 79, 1997, pp. 3306.

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

[26] U. Dorner, A. Klein and D. Jaksch, "A quantum repeater based on decoherence free subspaces," Quant. Inf. Comp., vol. 8, 2008, pp. 468-490.

[27] 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, 2010, pp. 651-656.

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

 ISBN: 978-1-61208-283-7