Chapter 6
Zero-Error Secrecy Capacity

Quantum key distribution is one of the most settled techniques nowadays to perform secure communications over quantum channels [42, p. 586]. Even though its security proofs are well established [37], in practical scenarios many of these protocols are not adequate due to noise in the quantum channel. The noise does not only increase the error rate in the transmission, but can also hinder eavesdropping detection in a process of security control [34].

Considering the practical difficulties to perform secure communications in noisy quantum channels, this chapter introduces some recent results regarding the *zero-error secrecy capacity* (ZESC), the higher transmission rate that can be achieved in certain noisy quantum channels that allows information to be sent without errors and in an unconditionally secure way. This capacity unifies concepts from quantum zero-error information theory, from quantum secrecy capacity of quantum channels, and also from decoherence-free subspaces and subsystems.

To present such developments, this chapter is organized as follows. Some background concepts of decoherence-free subspaces and subsystems are presented in Sect. 6.1. Section 6.2 discusses the quantum secrecy capacity. The model of communications and the formalism of concepts and proofs regarding ZESC are shown in Sect. 6.3. The relation between ZESC and graph theory is elucidated in Sect. 6.4. After that, the security level that this approach provides is presented in Sect. 6.5. Detailed examples considering different scenarios for the ZESC are illustrated in Sect. 6.6. Recent works in literature that have intersections with the ZESC, and that may point to further work are introduced in Sect. 6.7. Lastly, further reading is suggested in Sect. 6.8.

E.B. Guedes et al., *Quantum Zero-Error Information Theory*,
DOI 10.1007/978-3-319-42794-2_6

6.1 Decoherence-Free Subspaces and Subsystems

Suppose a closed quantum system composed by a system of interest, denoted by S and defined in a Hilbert space $\mathcal{H}$, and by the environment, denoted by E. This system has the following Hamiltonian:

$$\mathbb{H} = \mathbb{H}_S \otimes \mathbb{1}_E + \mathbb{1}_S \otimes \mathbb{H}_E + \mathbb{H}_{SE}, \tag{6.1}$$

where $\mathbb{1}$ is the identity operator, $\mathbb{H}_S$ denotes the operator of the system of interest, $\mathbb{H}_E$ denotes the operator of the environment, and $\mathbb{H}_{SE}$ denotes the operator of the interaction between system and environment [34].

To a complete absence of errors, the ideal scenario happens when $\mathbb{H}_{SE}$ is zero, indicating that system and environment are completely decoupled and evolved unitary according to their own Hamiltonians $\mathbb{H}_S$ and $\mathbb{H}_E$, respectively [34]. However, in realistic situations, this ideal scenario does not occur since no system can be completely free of errors. So, after isolating a system as better as possible, we must adopt at least one of the following strategies: identify and correct errors when they occur; avoid error as much as possible; suppress the error of the system [5].

If some symmetries exist in the interaction between system and environment, it is possible to find a "safe place" in the Hilbert space that is not subject to the negative effects of decoherence. Let $\{A_i(t)\}$ be a set of operators in the operator-sum representation (OSR) describing the evolution of a system. We say that a density matrix ρ_S is invariant under the operators $\{A_i(t)\}$ if $\sum_i A_i(t)\rho_S A_i^\dagger(t) = \rho_S$. Taking this into account, we can define the *decoherence-free subspaces and subsystems* (DFS) whose states are invariant despite a non-trivial coupling between system and environment.

Definition 6.1 (Decoherence-Free Subspaces and Subsystems [1]). A subspace $\tilde{\mathcal{H}}$ from a Hilbert space $\mathcal{H}$ is said to be decoherence-free regarding the coupling between system and environment if every pure state in this subspace is invariant under the OSR evolution, despite any environment initial condition, i.e.,

$$\sum_i A_i(t)|\tilde{k}\rangle\langle\tilde{k}|A_i^\dagger(t) = |\tilde{k}\rangle\langle\tilde{k}|, \forall |\tilde{k}\rangle\langle\tilde{k}| \in \tilde{\mathcal{H}}, \forall \rho_E(0). \tag{6.2}$$

Let the Hamiltonian of the interaction between system and environment be $\mathbb{H}_{SE} = \sum_j S_j \otimes E_j$, where S_j and E_j are the operators of the system and the environment, respectively. We consider that the environment operators E_j are linearly independent. The symmetries required to the existence of a DFS are described as follows, whose proof is shown in [34, Sect. 5].

Theorem 6.1 (Conditions for the Existence of Decoherence-Free Subspaces). *A subspace $\tilde{\mathcal{H}}$ is decoherence-free if and only if the system operators S_j act proportionally to the identity in this subspace, i.e.,*

$$S_j|\tilde{k}\rangle = c_j|\tilde{k}\rangle \qquad \forall j, |\tilde{k}\rangle \in \tilde{\mathcal{H}}. \tag{6.3}$$

The notion of a subspace that remains decoherence-free during the system evolution is not, however, the most general way to decoherence-free encoding in quantum systems [34]. Knill et al. [32] developed a method to encoding into subsystems instead of subspaces.

Definition 6.2 (Decoherence-Free Subsystems). Let $\mathcal{E} : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$ be a positive trace-preserving superoperator in a Hilbert space $\mathcal{H}$. Suppose $\mathcal{H} = (\mathcal{H}^A \otimes \mathcal{H}^B) \oplus \mathcal{K}$. We say that $\mathcal{H}^B$ ($\dim(\mathcal{H}^B) \geq 1$) is a *decoherence-free subsystem* if, $\forall \sigma^A \in B(\mathcal{H}^A)$ and $\forall \sigma^B \in B(\mathcal{H}^B)$, there is $\tau^A \in B(\mathcal{H}^A)$ such that

$$\mathcal{E}(\sigma^A \otimes \sigma^B) = \tau^A \otimes \sigma^B. \tag{6.4}$$

We can also write this definition using the partial trace:

$$\mathrm{Tr}_A\left[\mathcal{E}(\sigma)\right] = \mathrm{Tr}_A(\sigma) \qquad \forall \sigma = \sigma^A \otimes \sigma^B. \tag{6.5}$$

When $\dim(\mathcal{H}^A) = 1$, we say that $\mathcal{H}^B$ is a decoherence-free subspace for $\mathcal{E}$.

It is possible to build codes from states of a DFS which are known as *quantum error-avoiding codes* (QEAC). Information encoded into DFS is not affected by the channel's noise. Therefore, no error-correcting procedure is necessary. Error-avoiding codes can be contrasted with *quantum error-correcting codes* (QECC) regarding some aspects: QECCs are designed to correct errors after they occur, while QEACs do not have abilities to correct errors, because they avoid it; the most adopted QECCs are non-degenerated, while QEACs are highly degenerated codes; QEACs usually require less physical qubits to represent a logical qubit when compared to QECCs. In particular, if the degenerescence of a QECC reaches the maximum, then this code is reduced to a QEAC, showing a situation where one kind of code becomes equivalent to the other [14].

Even though DFS is a way to avoid errors, not all situations attain symmetry requirements to the existence of such subspaces. Zanardi and Rasetti [58] state that such conditions occur only if there is *collective decoherence* which occurs when several qubits couple in an identical way with the environment while undergoing both dephasing and dissipation.

Example 6.1 (Collective Dephasing Quantum Channel). Dephasing is a phenomenon in which the relative phase of a qubit is lost. Quantum channels with collective dephasing act on the input state in the following way:

$$|0\rangle \to |0\rangle\,,$$
$$|1\rangle \to e^{\imath\phi}\,|1\rangle\,,$$

where ϕ is the collective dephasing parameter that varies with time. A logic qubit composed by two physical qubits with anti-parallel parity is immune to collective dephasing, i.e.,

$$|0_L\rangle = |01\rangle\,,$$
$$|1_L\rangle = |10\rangle\,.$$

A qubit can be, thus, encoded as $|\psi_L\rangle = \alpha\,|0_L\rangle + \beta\,|1_L\rangle$. As expected, $|\psi_L\rangle$ does not suffer from the collective decoherence due to this channel:

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

since the global phase factor $e^{\imath\phi}$ acquired during this process has no physical significance [7]. It means that the states $|01\rangle$ and $|10\rangle$ belong to $\tilde{\mathcal{H}}$, a decoherence-free subspace from $\mathcal{H}$ in a quantum channel with collective dephasing.

Some practical results already reported in the literature consider the identification, implementation, and adoption of several DFS in quantum computation and communication [2, 17, 29, 31, 33, 35, 41, 51, 57, 59]. For quantum communications, in particular, DFS are useful for building quantum repeaters. Such devices are used for quantum key distribution, quantum teleportation schemes and also for quantum computer networks [13]. The work of Xue [56] shows the characterization of quantum repeaters with DFS for long distance quantum communications.

6.1.1 *Method for Obtaining Decoherence-Free Subspaces and Subsystem*

Despite the ability to preserve the fidelity of quantum states, one of the limitations regarding the use of DFS relies on the difficulty to identify them [5]. In order to circumvent this problem, Choi and Kribs [9] proposed a method to identify DFS when the error model of the quantum channel is known. The main goal of this section is the characterization of this method that is mainly algebraic.

Let $\mathcal{E} : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$ be a quantum operation. The error model can be specified, for example by the operation elements $\{E_a\}$ of an OSR, $\mathcal{E} \equiv \{E_a\}$. The *noise commutator* $\mathcal{A}'$ for $\mathcal{E}$ is the set of all operators $\mathcal{B}(\mathcal{H})$ which commute with the operators E_a and $E_a^\dagger$. When considering unital channels (which satisfy $\mathcal{E}(\mathbb{1}) = \mathbb{1}$), we have that all $\sigma \in \mathcal{A}'$ satisfy $\mathcal{E}(\sigma) = \sigma$. As a consequence, $\mathcal{A}$ is a †-algebra[1] generated by E_a that is called *interaction algebra* associated with $\mathcal{E}$.

[1]The formalism of †-algebras, also known as C^*-algebras, was developed for its use on quantum mechanics of observables. A †-algebra is a Banach $*$-algebra with an additional condition for the norm: $||A^* \cdot A|| = ||A^2||$ for all $A \in \mathcal{U}$, where $\mathcal{U}$ is an algebra with complex norm. A complete tutorial on †-algebras can be found on Davidson [10].

However, quantum channels are generally non-unital and hence we must explore a more general formalism. Any operator σ that belongs to the noise commutator $\mathcal{A}^{'}$ satisfies $\mathcal{E}(\sigma) = \sigma\mathcal{E}(\mathbb{1}) = \mathcal{E}(\mathbb{1})\sigma$. Given a projector P in $\mathcal{B}(\mathcal{H})$, the objective is to find a subalgebra $P\mathcal{B}(\mathcal{H})P$ of $\mathcal{B}(\mathcal{H})$ with algebra $\mathcal{B}(P\mathcal{H})$. To do so, we have the following theorem.

Theorem 6.2 (Choi and Kribs [9]). *Let $\mathcal{E} = \{E_a\}$ be a quantum operation on $\mathcal{B}(\mathcal{H})$. Suppose that P is a projection onto $\mathcal{H}$ that satisfies*

$$\mathcal{E}(P) = P\mathcal{E}(P)P. \tag{6.6}$$

Then, $E_aP = PE_aP$, $\forall a$. Define

$$\mathcal{A}_P^{'} \equiv \left\{\sigma \in \mathcal{B}(P\mathcal{H}) : [\sigma, PE_aP] = 0 = \left[\sigma, PE_a^{\dagger}P\right]\right\} \tag{6.7}$$

and

$$\begin{aligned}\mathrm{Fix}_P(\mathcal{E}) \equiv \{&\sigma \in \mathcal{B}(P\mathcal{H}) : \mathcal{E}(\sigma) = \sigma\mathcal{E}(P) = \mathcal{E}(P)\sigma,\\ &\mathcal{E}(\sigma^{\dagger}\sigma) = \sigma^{\dagger}\mathcal{E}(P)\sigma, \mathcal{E}(\sigma, \sigma^{\dagger}) = \sigma\mathcal{E}(P)\sigma^{\dagger}\}\,.\end{aligned} \tag{6.8}$$

Therefore, $\mathrm{Fix}_P(\mathcal{E})$ *is a †-algebra inside $\mathcal{B}(P\mathcal{H})$ that coincides with $\mathcal{A}_P^{'}$, i.e.,*

$$\mathrm{Fix}_P(\mathcal{E}) = \mathcal{A}_P^{'}. \tag{6.9}$$

The proof of this theorem will not be fully discussed; we just highlight some of the most important aspects. If P satisfies (6.6), then

$$0 \leq P^{\perp}E_aPE_a^{\dagger}P^{\perp} \leq P^{\perp}\mathcal{E}(P)P^{\perp} = 0 \qquad \forall a. \tag{6.10}$$

To whatever operators $A, B \in \mathcal{B}(\mathcal{H}), A \leq B \Rightarrow \langle\psi|\, B - A\,|\psi\rangle \geq 0, \forall\, |\psi\rangle \in \mathcal{H}$. This way, $P^{\perp}E_aP = 0$ or, equivalently, $E_aP = PE_aP$, $\forall a$. When considering $\sigma \in \mathcal{A}_P^{'}$, then

$$\begin{aligned}\mathcal{E}(\sigma) &= \sum_a E_aP\sigma PE_a^{\dagger}\\ &= \sigma\sum_a E_aPE_a^{\dagger} = \sum_a E_aPE_a^{\dagger}\sigma\\ &= \sigma\mathcal{E}(P) = \mathcal{E}(P)\sigma.\end{aligned} \tag{6.11}$$

Projectors P satisfying (6.6) have some properties. For instance, a quantum channel $\mathcal{E} \equiv \{E_a\}$ acts on a quantum state $\sigma \in \mathcal{A}_P^{'}$ projecting it into another state σ' in the subspace defined by P. To support this statement, we have that

$$\begin{aligned}\sigma' &= \mathcal{E}(\sigma) \\ &= \sigma\mathcal{E}(P) \\ &= (P\sigma P)(P\mathcal{E}(P)P) \\ &= P[\sigma P\mathcal{E}(P)]P \in \mathcal{B}(P\mathcal{H}). \end{aligned} \tag{6.12}$$

In this particular case, $\mathcal{E}(\sigma) = \sigma$ only if $\mathcal{E}(P) = \mathbb{1}$.

The next step is to show how projectors with such characterization can capture the DFS of a quantum operation $\mathcal{E}$.

Theorem 6.3 (Method for Obtaining DFS [9]). *Let $\mathcal{E}$ be a quantum operation in $\mathcal{B}(\mathcal{H})$. Let P be a projector that satisfies (6.6), and let $P\mathcal{H} = \oplus_k(\mathcal{H}^{A_k} \otimes \mathcal{H}^{B_k})$ be the decomposition of $P\mathcal{H}$ induced by the structure of the $\dagger$-algebra $\mathcal{A}_P^{'} = \mathrm{Fix}_P(\mathcal{E})$. Then, the subsystems $\mathcal{H}^{B_k}$, with $\dim(\mathcal{H}^{B_k}) > 1$, are decoherence-free for $\mathcal{E}$.*

We can say that the essence of this method relies on the identification of all projectors P satisfying (6.6). Thenceforth, the structure of $\mathcal{A}_P^{'} = \mathrm{Fix}_P(\mathcal{E})$ is used to determine what are the states that belong to the DFS.

One important aspect is the *optimality* of the proposed method. It means that it can capture all projectors satisfying (6.6) [9, Theorem 3]. Despite the characterization of such method, the authors state that no computational procedures were developed to this purpose yet.

Example 6.2 (Identifying a DFS in a Quantum Channel). Suppose that the quantum channel $\mathcal{E} \equiv \{E_0, E_1, E_2\}$ acts on a bidimensional space state with the following Kraus operators:

$$\begin{aligned} E_0 &= \alpha(|00\rangle\langle 00| + |11\rangle\langle 11|) + |01\rangle\langle 01| + |10\rangle\langle 10|, \\ E_1 &= \beta(|00\rangle\langle 00| + |11\rangle\langle 11| + |01\rangle\langle 01| + |10\rangle\langle 10|), \\ E_2 &= \beta(|00\rangle\langle 00| + |11\rangle\langle 11| - |01\rangle\langle 01| - |10\rangle\langle 10|), \end{aligned}$$

where q is a scalar, $0 < q < 1$; $\alpha = \sqrt{1-2q}$; $\beta = \sqrt{q/2}$. It is possible to notice that $\mathcal{E}(\mathbb{1}) = \sum_{a=0}^{2} E_a E_a^{\dagger} \neq \mathbb{1}$ and, therefore, this channel is not unital.

In this channel model, there is only one state ρ such that $\mathcal{E}(\rho) = \rho$. However, such invariance does not come from the action of $\mathcal{E}$, but from a fixed point. Despite that, there is a DFS with such dimension when we consider the projector $P = |01\rangle\langle 01| + |10\rangle\langle 10|$, i.e., all operators supported by P are invariant under $\mathcal{E}$. It means that $\mathcal{E}(\sigma') = \sigma'$ for all $\sigma' = P\sigma P$.

To exemplify this statement, let the density operator of the state $|\psi\rangle$ be

$$|\psi\rangle\langle\psi| = \frac{|01\rangle\langle 01| + |01\rangle\langle 00| + |00\rangle\langle 01| + |00\rangle\langle 00|}{2}.$$

Applying the projector P onto $|\psi\rangle$ results

$$\begin{aligned}
\left|\psi'\right\rangle\left\langle\psi'\right| &= P\left|\psi\right\rangle\left\langle\psi\right|P \\
&= \left(\left|01\right\rangle\left\langle 01\right| + \left|10\right\rangle\left\langle 10\right|\right)\left(\frac{\left|01\right\rangle\left\langle 01\right| + \left|01\right\rangle\left\langle 00\right| + \left|00\right\rangle\left\langle 01\right| + \left|00\right\rangle\left\langle 00\right|}{2}\right)P \\
&= \left(\frac{\left|01\right\rangle\left\langle 01\right| + \left|01\right\rangle\left\langle 00\right|}{2}\right)\left(\left|01\right\rangle\left\langle 01\right| + \left|10\right\rangle\left\langle 10\right|\right) \\
&= \frac{\left|01\right\rangle\left\langle 01\right|}{2}.
\end{aligned}$$

Note that $\left|\psi'\right\rangle\left\langle\psi'\right|$ does not vary after passing the channel $\mathcal{E}$, despite it does not belong to the noise commutator $\mathcal{A}'$ for $\mathcal{E}$:

$$\begin{aligned}
\mathcal{E}(\left|\psi'\right\rangle\left\langle\psi'\right|) &= \sum_{a=0}^{2} E_a \left|\psi'\right\rangle\left\langle\psi'\right| E_a^\dagger \\
&= \frac{\left|01\right\rangle\left\langle 01\right|}{2} + \beta \cdot \frac{\left|01\right\rangle\left\langle 01\right|}{2} - \beta \cdot \frac{\left|01\right\rangle\left\langle 01\right|}{2} \\
&= \frac{\left|01\right\rangle\left\langle 01\right|}{2}.
\end{aligned}$$

6.1.2 *Relation with the Zero-Error Capacity of Quantum Channels*

The work of Medeiros et al. [39] explores the relation between DFS and zero-error capacity of quantum channels. This relation is established from the method for obtaining DFS of Choi and Kribs [9], showed in the previous section. The purpose of this section is to show this relation.

We know that a quantum channel has zero-error capacity if and only if there are at least two non-adjacent states at the channel input. Considering an optimum pair $(\mathcal{S}, \mathcal{M})$ according to Definition 5.3, it is possible to derive a pair $(\mathcal{S}', \mathcal{M}')$, where $\mathcal{S}' \subset \mathcal{S}$, $\mathcal{M}' = \{M_1, \ldots, M_k, M_{k+1}\} \subset \mathcal{M}$, and $M_{k+1} = \mathbb{1} - \sum_{i=1}^{k} M_i$. The projectors $M_i \in \mathcal{M}'$, with $1 \leq i \leq k$, satisfy

$$\mathcal{E}(M_i) = M_i \mathcal{E}(M_i) M_i \tag{6.13}$$

and

$$M_i M_j = \delta_{ij} M_i M_j, \tag{6.14}$$

where δ denotes the Kronecker's delta. When choosing projectors with such restrictions, we notice that the elements of $\mathcal{S}'$ can define a DFS, as established in the method for obtaining DFS explored in Sect. 6.1.1.

As a consequence, we have that the set $(\mathcal{S}', \mathcal{M}')$ is optimum and the zero-error capacity $C^{(')}(\mathcal{E})$ defined for this set can be bigger than the zero-error capacity $C^{(0)}(\mathcal{E})$ defined for $(\mathcal{S}, \mathcal{P})$, it means that $C^{(')}(\mathcal{E}) \geq C^{(0)}(\mathcal{E})$. The proofs of such consequences make use of graph theory and mappings properties [39].

In summary, the conclusion of those authors regarding the relation of DFS and zero-error capacity is that if a zero-error quantum channel has a DFS, then the zero-error capacity must be obtained from the DFS by using projectors that attain certain properties.

6.2 Quantum Secrecy Capacity

The privacy in quantum systems was initially considered by Schumacher and Westmoreland [45]. These researchers conceived a model that allows two legitimate parties, Alice and Bob, to exchange classical messages through a noisy quantum channel. An eavesdropper (Eve) has total access to the environment of the quantum channel from which she is able to capture information of the legitimate parties.

Alice sends messages from a set of integers $\mathcal{U} = \{1, 2, \ldots, |\mathcal{U}|\}$ mapped on an ensemble of quantum states $\{\rho(u), p_u : u \in \mathcal{U}\}$. The states of the ensemble are called *quantum codewords*, composed by tensor products of quantum states:

$$\rho(u) = \rho_1(u) \otimes \rho_2(u) \otimes \ldots \otimes \rho_n(u) \qquad u \in \mathcal{U}, \rho_i(u) \in \mathcal{H}, i = 1, 2, \ldots, n. \tag{6.15}$$

The mapping characterizes a quantum block code with block length n and rate $R = \frac{1}{n} \log |\mathcal{U}|$. A decoding scheme for this quantum code is a decoding function that associates univocally an output quantum state with a set of integers, i.e., $g : \mathcal{H} \to \mathcal{U}$, $\hat{u} = g(\mathcal{E}(\rho(u))) \in \mathcal{U}$. An error occurs when $g(\mathcal{E}(\rho(u))) \neq u$.

The quantum privacy between Alice and Bob is limited by the *coherent information* among them. The coherent information is an information measure that quantifies the difference between the von Neumann entropies of two systems: the system of interest and the environment [45]. When considering this formulation, Cai et al. [6] and Devetak [11] notice some similarities with classical wiretap channels proposed by Wyner [54]. Then, they proposed a quantum version of such channels, presented in Definition 6.3 and illustrated in Fig. 6.1.

Definition 6.3 (Quantum Wiretap Channel). A quantum memoryless wiretap channel is described by a superoperator $\mathcal{E}$ in a complex Hilbert space $\mathcal{H} = \mathcal{H}_{\text{Bob}} \otimes \mathcal{H}_{\text{Eve}}$. When Alice sends a quantum state $\rho \in \mathcal{H}^{\otimes n}$, Bob receives $\rho_{\text{Bob}} = \text{Tr}_{\text{Eve}}[\mathcal{E}^{\otimes n}(\rho)]$ and Eve receives $\rho_{\text{Eve}} = \text{Tr}_{\text{Bob}}[\mathcal{E}^{\otimes n}(\rho)]$, where n is the dimension of input Hilbert space.

When communicating over a quantum wiretap channel, security can be achieved by using a particular type of quantum block code: the *quantum wiretap codes*. Two additional parameters are necessary: λ, which represents an upper bound for the error-probability; and μ, which represents an upper bound for the maximum

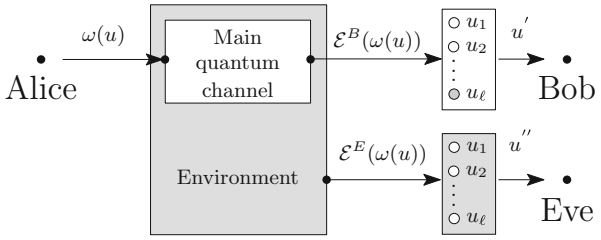

Fig. 6.1 General model of a quantum wiretap channel

accessible information by the eavesdropper Eve. A quantum wiretap code is referred to as a 4-tuple $(n, |\mathcal{U}|, \lambda, \mu)$. A formal characterization of such codes is given below.

Definition 6.4 (Quantum Wiretap Block Codes). Consider a quantum block code of length n and rate $R = \frac{1}{n}\log|\mathcal{U}|$, where $\mathcal{U} = \{1, 2, \ldots, |\mathcal{U}|\}$ is a set of classical messages. The set of codewords labeled by the index of the messages is given as follows:

$$\Omega(\mathcal{U}) = \{\rho(u) : u \in \mathcal{U}\}. \tag{6.16}$$

We assume that the decoding function is given by the POVM $\{\mathcal{D}_u : u \in \mathcal{U}\}$, where $\sum_u \mathcal{D}_u \leq \mathbb{1}$.

This code is said to be a quantum wiretap block code with parameters $(n, |\mathcal{U}|, \lambda, \mu)$, or quantum wiretap code for short, if two conditions are attained:

$$P_e = 1 - \frac{1}{|\mathcal{U}|}\sum_{u\in\mathcal{U}} \mathrm{Tr}_{\mathrm{Eve}}[\mathcal{E}(\rho(u))\mathcal{D}_u] \leq \lambda, \tag{6.17}$$

and

$$\frac{1}{n}\left\{S\left(\sum_{u\in\mathcal{U}} \mathrm{Tr}_{\mathrm{Bob}}[\mathcal{E}^{\otimes n}(\rho(u))]\right) - \sum_{u\in\mathcal{U}} \frac{1}{|\mathcal{U}|} S(\mathrm{Tr}_{\mathrm{Bob}}[\mathcal{E}^{\otimes n}(\rho(u))])\right\} \leq \mu. \tag{6.18}$$

In the definition of a quantum wiretap code with parameters $(n, |\mathcal{U}|, \lambda, \mu)$, (6.17) ensures an average probability of decoding errors for Bob lower than λ, and (6.18) limits the information accessible to the eavesdropper, which captures almost nothing from the message sent by Alice [6].

Lastly, the *secrecy capacity of a quantum channel* is defined as follows.

Definition 6.5 (Quantum Secrecy Capacity). The secrecy capacity of a quantum channel $\mathcal{E}$ is the largest real number $C_S(\mathcal{E})$, such that for all $\epsilon, \lambda, \mu > 0$ and n large enough, there is a quantum wiretap code with parameters $(n, |\mathcal{U}|, \lambda, \mu)$ such that

$$C_S(\mathcal{E}) < \frac{1}{n}\log|\mathcal{U}| + \epsilon. \tag{6.19}$$

Only uniformly distributed messages were considered in the previous definitions, but the following theorem is a more general result for the quantum secrecy capacity [6, Sect. 5].

Theorem 6.4 (Quantum Secrecy Capacity). *Let $\mathcal{E}$ be a quantum wiretap channel as characterized in Definition 6.3. The quantum secrecy capacity of $\mathcal{E}$ satisfies*

$$C_S(\mathcal{E}) \geq \max_{\{P\}} \left[\chi^{Bob} - \chi^{Eve}\right], \tag{6.20}$$

where the maximum is taken over all probability distributions over $\mathcal{U}$; and χ^{Bob} and χ^{Eve} are Holevo quantities defined as

$$\chi^{Bob} = S(\rho_{Bob}) - \sum_i p_i S(\rho_{Bob}(i)), \tag{6.21}$$

$$\chi^{Eve} = S(\rho_{Eve}) - \sum_i p_i S(\rho_{Eve}(i)), \tag{6.22}$$

where ρ_{Bob} is the state received by Bob after a partial trace over the environment; and ρ_{Eve} is Eve's final state.

The proof of this theorem makes use of the *random coding proof* technique to ensure that the information gathered by Eve is negligible. When the information transmission rate through the channel is smaller than the quantum secrecy capacity, the protocol guarantees *unconditional security* [6]. This capacity is equivalent to the definition of privacy presented by Schumacher and Westmoreland [45].

The quantum secrecy capacity (6.20) is the quantum counterpart of the classical secrecy capacity proposed by Wyner [54]. We can, therefore, notice some similarities between both definitions: they limit the decoding error probability and the information accessible to the wiretapper.

A particular characteristic of the quantum secrecy capacity is that it does not have single letter characterization, i.e., the capacity cannot be directly calculated because the maximum is taken over all possible input states as well as all possible probability distributions [6, 11].

Some codes for quantum wiretap channels can be found in the literature. Hamada [25, 26] proposed classes of codes for both classical and quantum wiretap channels. In the quantum case, they are based on concatenated conjugate codes that are equivalent to the Calderbank-Shor-Steane (CSS) codes [42, Sect. 10.4.2]. Another characteristic of the proposed code is the polynomial-time complexity for encoding and decoding in terms of channel usage.

Another class of codes for quantum wiretap channels was proposed by Wilde and Guha [53]. This construction is based on polar codes for degraded wiretap channels that reach the symmetric secrecy capacity for a quantum wiretap channel with a classical eavesdropper. Although this class of codes also has a polynomial-time complexity for encoding and decoding, examples of such codes are strongly dependent on numerical simulations [16]. Nonetheless, the authors showed that such codes perform well when used to carry information through amplitude damping, dephasing, erasure, and cloning quantum channels [16, 53].

6.3 Zero-Error Secrecy Capacity

Consider a scenario where two legitimate parties, Alice and Bob, want to exchange classical messages through a quantum channel $\mathcal{E}$ in a secret and error-free way. These messages must be protected from an eavesdropper (Eve), which has complete and non-restricted access to the environment. This communication model is similar to the scenario already considered in Fig. 6.1.

The communication model where the eavesdropper has complete access to the environment follows the formalism proposed by Cai et al. [6] and of Devetak [11] for the characterization of quantum wiretap channels. In practical scenarios, it is more common to consider a direct action of the eavesdropper on the main quantum channel and its implications in the communication and in the non-authorized information gathering, e.g., in quantum key distribution protocols. The scenario described in Fig. 6.1, although different from this approach, can also be physically implemented and is already consolidated in the literature for quantum privacy purposes [45]. In particular, the channel $\mathcal{E}$ has Kraus operators $\{E_a\}$ and positive zero-error capacity. The following characterization presents the quantum channel under consideration.

Characterization 6.1 (Quantum Channel with Positive Zero-Error Capacity). *Let $\mathcal{E}$ be a trace-preserving quantum map with Kraus operators $\{E_a\}$, which represents a noisy quantum channel $\mathcal{E}$. We consider that $\mathcal{E}$ has a strictly positive zero-error capacity, $C^{(0)}(\mathcal{E}) > 0$, reached by an optimum pair $(\mathcal{S}, \mathcal{M})$.*

If there exists a POVM $\mathcal{M}' = \{M_1, \ldots, M_k\}$ that satisfies (6.13) and (6.14), then

$$\mathcal{E}(M_i) = M_i \mathcal{E}(M_i) M_i, \tag{6.23}$$

$$M_i M_j = \delta_{i,j} M_i M_j, \tag{6.24}$$

for all $i, j \leq k$. Furthermore, if we define

$$\mathcal{S}' = \left\{ \rho_i = |s_i\rangle \langle s_i|_{i=1}^{k}, \rho_i \in M_i \mathcal{H} \text{ and } [\rho_i, M_i E_a M_i] = 0 = \left[\rho_i, M_i E_a^{\dagger} M_i\right] \right\}, \tag{6.25}$$

then the pair $(\mathcal{S}', \mathcal{M}')$ is also optimum. Since $(\mathcal{S}', \mathcal{M}')$ has been obtained according to the method described in Sect. 6.1.1, the quantum states $\rho_i \in \mathcal{S}'$ characterize an orthonormal basis set for the decoherence-free subspace $\tilde{\mathcal{H}}$. For the sake of simplicity, from now on we will use the notation $\tilde{\mathcal{H}}$ in a reference for the basis states of this decoherence-free subspace. Therefore, states in $\mathcal{S}'$ can be used to encode information that will be immune to an eavesdropper, as shown in the following lemmas.

Lemma 6.1 (Optimum Pair $(\mathcal{S}', \mathcal{M}')$ Defines a QEAC). *The optimum pair $(\mathcal{S}', \mathcal{M}')$ is a quantum error avoiding code (vide Sect. 6.2).*

Proof. In order to prove this lemma, we must show that the pair $(\mathcal{S}', \mathcal{M}')$ has all the elements of a QEAC.

Let $\mathcal{U} = \{u_1, \ldots, u_k\}$ be a set of classical messages; each message in $\mathcal{U}$ is associated with a state in $\mathcal{S}'$ through a bijection. The set $\mathcal{S}'$ defines a codebook $\tilde{P}(\mathcal{U}) = \{\tilde{\rho}(u_i) = \rho_i\} \equiv \mathcal{S}'$ with codewords of length n. The decoding is performed by a set of positive operators $M_i \in \mathcal{M}'$, $i \in 1, \ldots, |\mathcal{U}|$, with $\sum_{i=1}^{|\mathcal{U}|} M_i \leq \mathbb{1}$. Indeed, there is a bijective correspondence between the set of POVM operators $\mathcal{M}'_i$ and the set of messages $\mathcal{U}$. Therefore, the pair $(\tilde{\mathcal{P}}(\mathcal{U}), \mathcal{M}')$, which is equivalent to $(\mathcal{S}', \mathcal{M}')$, defines a quantum error-avoiding code of length n and rate $\frac{1}{n} \log |\mathcal{U}|$.

It is straightforward to see that for each DFS we can construct a quantum error-avoiding code to the corresponding quantum channel. The channel $\mathcal{E}$ is subject to collective decoherence, being governed by the Hamiltonian (6.1). Thanks to symmetries existing in collective decoherence, states in the DFS do not suffer the action of $\mathbb{H}_{SE}$, the Hamiltonian component representing the interaction between system and environment.

When Alice wants to send a message u to Bob using a quantum error-avoiding code, she encodes u into a quantum codeword $\tilde{\rho}(u)$ and sends the corresponding state through the channel $\mathcal{E}$. We assume that the environment starts in a pure state $|0_E\rangle \langle 0_E|$. Due to the decoherence, Bob and Eve will receive the following states, respectively,

$$\rho_{\text{Bob}}(\tilde{\rho}(u)) = \text{Tr}_{\text{Eve}} \left[\mathcal{E}(\tilde{\rho}(u) \otimes |0_{\text{E}}\rangle \langle 0_{\text{E}}|)\right], \tag{6.26}$$

$$\rho_{\text{Eve}}(\tilde{\rho}(u)) = \text{Tr}_{\text{Bob}} \left[\mathcal{E}(\tilde{\rho}(u) \otimes |0_{\text{E}}\rangle \langle 0_{\text{E}}|)\right]. \tag{6.27}$$

Since Alice uses a QEAC, dynamic symmetries protect the quantum codeword from interacting with the environment. Therefore, the joint evolution between system and environment happens in a decoupled way. Thus, the state $\rho_{\text{Bob}}(\tilde{\rho}(u))$ is given by

$$\begin{aligned} \rho_{\text{Bob}}(\tilde{\rho}(u)) &= \text{Tr}_{\text{Eve}} \left[\mathcal{E}(\tilde{\rho}(u) \otimes |0_E\rangle \langle 0_E|)\right] && (6.28) \\ &= \text{Tr}_{\text{Eve}} \left[\sum_a E_a \left(\tilde{\rho}(u) \otimes |0_E\rangle \langle 0_E|\right) E_a^\dagger\right] \\ &= \text{Tr}_{\text{Eve}} \left[\tilde{\rho}(u) \otimes \rho_E\right] && (6.29) \\ &= \tilde{\rho}(u), && (6.30) \end{aligned}$$

where (6.29) is due to the invariance of a state from a DFS under the OSR operators.

Taking into account the Hamiltonian (6.1) of the quantum system and considering the fact that system of interest and environment have not interacted, then it is possible to ensure that the environment suffered only the action of $\mathbb{H}_E$, which indicates a unitary evolution restricted to the environment. It means that $\rho_{\text{Eve}}(\tilde{\rho}(u)) = \rho_{\text{E}}$ (6.27) is a *pure state*.

Proceeding with the development, it is possible to state and prove the following lemma.

Lemma 6.2 (Optimum Pair $(\mathcal{S}', \mathcal{M}')$ Defines a Wiretap Code). *The pair $(\mathcal{S}', \mathcal{M}')$ defines a quantum wiretap code with parameters $(n, |\mathcal{U}|, 0, 0)$.*

Proof. In Definition 6.4 of a wiretap code as proposed by Cai et al. [6], two conditions must be satisfied in order to achieve secrecy: (1) the average error decoding probability must be small; and (2) the accessible information to the eavesdropper must be arbitrarily small. As we show below, these two requirements are actually satisfied.

For the first condition, note that the pair $(\mathcal{S}', \mathcal{M}')$ is optimal, i.e., the set $\mathcal{S}'$ attains the zero-error capacity. If quantum codewords are composed of tensor products of states in $\mathcal{S}'$, then the communication is accomplished without decoding errors. Therefore, $\lambda = 0$ and the first condition is attained.

In order to verify the second condition, we need to check the accessible information by Eve, which is given as

$$S\left(\sum_{u\in\mathcal{U}} \frac{1}{|\mathcal{U}|} \operatorname{Tr}_{\text{Bob}} \mathcal{E}(\tilde{\rho}(u))\right) - \sum_{u\in\mathcal{U}} \frac{1}{|\mathcal{U}|} S\left(\operatorname{Tr}_{\text{Bob}} \mathcal{E}(\tilde{\rho}(u))\right) \leq \mu, \tag{6.31}$$

where μ is arbitrarily small. Instead of calculating the left side of (6.31), we make use of an upper bound for the accessible information, the Holevo quantity, defined by

$$\chi^{\text{Eve}} = S(\rho_{\text{Eve}}(\tilde{\rho}(u))) - \sum_u p_u S(\rho_{\text{Eve},u}\tilde{\rho}(u)). \tag{6.32}$$

Because quantum codewords are composed by states in $\mathcal{S}'$ that belongs to a DFS, there are no interactions between the system and the environment. Therefore, the initial environment state, $|0_E\rangle$, evolves only under the Hamiltonian $\mathbb{H}_E$, indicating a unitary evolution restricted to the environment. It means that the final environment state is pure. This way:

$$\begin{aligned}
\chi^{\text{Eve}} &= S(\rho_{\text{Eve}}(\tilde{\rho}(u))) - \sum_u p_u S(\rho_{\text{Eve},u}\tilde{\rho}(u)) \\
&= S(\rho_E) - \sum_u p_u S(\rho_{\text{Eve},u}\tilde{\rho}(u)) \\
&= 0 - \sum_u p_u S(\rho_{\text{Eve},u}\tilde{\rho}(u)).
\end{aligned} \tag{6.33}$$

Because $\chi^{\text{Eve}} \geq 0$, $S(\rho) \geq 0$ for any ρ, and that $p_u \geq 0$ for all u, then the sum at the right side of (6.33) is zero. Therefore, $\chi^{\text{Eve}} = 0$. Since the Holevo quantity is an upper bound for accessible information, the left side of (6.31) is zero, i.e., $\mu = 0$.

Lemmas 6.1 and 6.2 guarantee that unconditionally secure communication can be performed by using codewords composed by quantum states belonging to a DFS for corresponding quantum channel [23].

Even though an optimum $(\mathcal{S}', \mathcal{M}')$ defines a wiretap code with parameters $(n, |\mathcal{U}|,0,0)$, it is not always possible to extract $(\mathcal{S}', \mathcal{M}')$ from an optimum pair $(\mathcal{S}, \mathcal{M})$. According to Lemma 6.1, the quantum states in $\mathcal{S}'$ belongs to $\tilde{\mathcal{H}}$ for the channel $\mathcal{E}$.

However, considering practical scenarios, a DFS may exist in such conditions, even with smaller cardinality than the set of messages, i.e., with $dim(\tilde{\mathcal{H}}) < |\mathcal{U}|$. For such situations, we use a wiretap code with parameters $(n, \dim(\tilde{\mathcal{H}}), 0, 0)$, which allows a communication free of errors and without information leakage. Despite that, in this second situation the communication occurs with a lower rate than when considered the code obtained according to the conditions previously mentioned. Taking this into account and also both lemmas proved, we can characterize a new kind of capacity for quantum channels, whose definition is given as follows.

Definition 6.6 (Zero-Error Secrecy Capacity). Let $\mathcal{E}$ be a quantum channel according to Characterization 6.1. We define the zero-error secrecy capacity of $\mathcal{E}$ as the largest real number $C_S^{(0)}(\mathcal{E})$ such that, for every $\epsilon > 0$ and sufficiently large n, there is a quantum wiretap code $(n, |\mathcal{U}|, 0, 0)$ which satisfies

$$C_S^{(0)}(\mathcal{E}) \leq \frac{1}{n} \log |\mathcal{U}| + \epsilon. \tag{6.34}$$

Two main features of this capacity are the absence of decoding errors and of information leakage to the eavesdropper. It is in contrast with the secrecy capacity of quantum channels, in which decoding errors among the legitimate parties can occur.

The following theorem gives a way of quantifying the zero-error secrecy capacity.

Theorem 6.5 (Zero-Error Secrecy Capacity). *Let $\mathcal{E}$ be a quantum channel according to Characterization 6.1. The zero-error secrecy capacity of $\mathcal{E}$ is given by*

$$C_S^{(0)}(\mathcal{E}) \equiv \min \left\{ C^{(0)}(\mathcal{E}), C_S(\mathcal{E}) \right\} \tag{6.35}$$

$$\equiv \min \left\{ \sup_{\tilde{\mathcal{H}}} \sup_n \frac{1}{n} \log \dim(\tilde{\mathcal{H}})^n, \max_{\{P\}} \chi^{Bob} \right\}, \tag{6.36}$$

where n is the length of the code; the maximum is taken over all probability distributions P over $\mathcal{U}$, and χ^{Bob} denotes an upper bound for the accessible information of the receiver (Bob):

$$\chi^{Bob} = S\left(\sum_u p_u \rho_{Bob}(\tilde{\rho}(u)) \right) - \sum_u p_u S\left(\rho_{Bob}(\tilde{\rho}(u)) \right), \tag{6.37}$$

where p_u is the a priori probability of the symbol $u \in \mathcal{U}$.

Proof. This proof considers some facts about the capacities of a quantum channel $\mathcal{E}$. Let $C_{1,\infty}(\mathcal{E})$ be the ordinary classical capacity of $\mathcal{E}$ defined according to the Holevo-Schumacher-Westmoreland theorem [28, 44]. Let $C_S(\mathcal{E})$ be the secrecy capacity of $\mathcal{E}$ [6, 11]. And, lastly, let $C^{(0)}(\mathcal{E})$ be the classical zero-error capacity of a quantum channel $\mathcal{E}$ [38]. We have that $C_S(\mathcal{E}) \leq C_{1,\infty}(\mathcal{E})$, and that $C^{(0)}(\mathcal{E}) \leq C_{1,\infty}(\mathcal{E})$.

Considering that $|\mathcal{U}| = \dim(\tilde{\mathcal{H}})$, a code with parameters $(n, |\mathcal{U}|, 0, 0)$ is simultaneously an error-free code and also a wiretap code. By definition, we know that the zero-error capacity is related to the maximum amount of messages that are distinguishable at the channel output. Since each word in the alphabet was associated with a state of a DFS, according to Lemma 6.1, we have

$$C^{(0)}(\mathcal{E}) = \sup_{\tilde{\mathcal{H}}} \sup_{n} \frac{1}{n} \log \dim(\tilde{\mathcal{H}})^n, \tag{6.38}$$

where n is the length of the code. Since this is a wiretap code having input symbols belonging to $\tilde{\mathcal{H}}$, $C_S(\mathcal{E}) = \chi^{\text{Bob}} - \chi^{\text{Eva}}$. As a consequence of Lemma 6.2,

$$\begin{aligned} C_S^{(0)}(\mathcal{E}) &\geq \max_{\{P\}} \left[\chi^{\text{Bob}} - \chi^{\text{Eva}}\right] \\ &\geq \max_{\{P\}} \left[\chi^{\text{Bob}} - 0\right] \\ &= \max_{\{P\}} \chi^{\text{Bob}}, \end{aligned} \tag{6.39}$$

where the maximum is taken over all a priori probability distributions P of the symbols $u \in \mathcal{U}$. The equality follows from the HSW theorem. We have to consider two situations:

1. There exists an optimum pair $(\mathcal{S}', \mathcal{M}')$ derived from $(\mathcal{S}, \mathcal{M})$ according to (6.23) and (6.24). In this case, $|\mathcal{U}| = \dim(\tilde{\mathcal{H}})$ and $C_S^{(0)}(\mathcal{E}) = C_S(\mathcal{E}) = C^{(0)}(\mathcal{E})$.
2. There exists a DFS $\tilde{\mathcal{H}}$ for the channel that is not directly obtained from the error-free code. In this situation, $C_S(\mathcal{E}) < C^{(0)}(\mathcal{E})$, i.e., error-free and leakage-free communication is only possible if $C_S^{(0)}(\mathcal{E}) = \min\left\{C^{(0)}(\mathcal{E}), C_S(\mathcal{E})\right\}$.

This way, the final expression for the zero-error secrecy capacity can be described in terms of the relation between the zero-error capacity and the secrecy capacity:

$$C_S^{(0)}(\mathcal{E}) = \min\left\{C^{(0)}(\mathcal{E}), C_S(\mathcal{E})\right\}, \tag{6.40}$$

where $C^{(0)}(\mathcal{E})$ and $C_S(\mathcal{E})$ are the zero-error capacity and the secrecy capacity of $\mathcal{E}$, respectively.

When a quantum channel $\mathcal{E}$ has $C_S^{(0)}(\mathcal{E}) = \sup_{\tilde{\mathcal{H}}} \sup_n \frac{1}{n} \log \dim(\tilde{\mathcal{H}})^n$, then the zero-error secrecy capacity is straightforwardly obtained from the dimension of the largest existing DFS for the channel.

According to Medeiros et al. [40], the zero-error capacity can be achieved using tensor product of pure states at the channel input. We can see that the same holds for the zero-error secrecy capacity $C_S^{(0)}(\mathcal{E})$.

The zero-error secrecy capacity communication protocol has the same level of security of the protocol established by Schumacher and Westmoreland [45]. According to the authors, the ability of a quantum channel to send private information is at least as great as its ability to send coherent information. In the zero-error secrecy capacity scenario, the information can be retrieved completely free of errors at the channel output. Therefore, the ability to communicate private information is maximized.

When considering the difficulties to implement quantum channels that enable communications completely free of errors [34], the zero-error secrecy capacity allows error-free and secure communications to be performed since the quantum channel attains some conditions. This is the case of quantum channels with collective decoherence [13, 30, 55], and the quantum channels with positive zero-error capacity discussed in [24]. In the latter example, the quantum channel proposed by Xue [56] can be used for long-distance zero-error quantum communications.

Although the zero-error secrecy capacity was adequately defined, it is zero for many kinds of quantum channels. We can say, indeed, that this capacity is different from zero only for quantum channels with positive zero-error capacity and for channels under the effect of collective-decoherence, allowing the existence of decoherence-free subspaces. Nevertheless, the definition of the zero-error secrecy capacity can improve our knowledge regarding the "abilities" of quantum channels, allowing a more adequate use in certain situations.

6.4 Representation in Graphs

In this section the relation between the ZESC and the graph theory will be depicted. Unfortunately, this relation is not so general as for the zero-error capacity of quantum channels, as presented previously in Sect. 5.2. The relation is only useful to describe quantum channels satisfying the first situation described in the proof of Theorem 6.5.

If there is a non-empty subset $\mathcal{M}'$ obtained from $\mathcal{M}$ according to (6.23) and (6.24), then it follows from the method of Choi and Kribs shown previously in Sect. 6.1.1 that $(\mathcal{S}', \mathcal{M}')$ characterizes a DFS $\tilde{\mathcal{H}}$, which is a subspace of the input Hilbert space $\mathcal{H}$. Supposing the existence of a set $\mathcal{S}'$, it is possible to build a characteristic graph for quantum channels with positive zero-error secrecy capacity. This construction is similar to that made for the zero-error capacity, as presented in Definition 5.5. However, there are some differences between the two vertex sets in each case.

Let $\mathcal{E}$ be a quantum channel with positive zero-error secrecy capacity attaining the first situation of the Theorem 6.5. The characteristic graph of $\mathcal{E}$, denoted by $\tilde{\mathcal{G}} = \langle V, E \rangle$, is built as follows.

1. The vertex set V is composed by the elements $\tilde{\mathcal{H}}$, which are referred by the indexes of the corresponding messages, i.e., $V = \{1, 2, \ldots, \dim(\tilde{\mathcal{H}})\}$.
2. The set of edges E connects two vertices if they are non-adjacent at the channel's end (see Definition 5.4).

The n-th Shannon product of $\tilde{\mathcal{G}}$, denoted by $\tilde{\mathcal{G}}^n$, has the vertex set V^n, each vertex corresponding to an n-tensor product of state belonging to $\mathcal{S}'^{\otimes n}$. Two vertices in V^n are connected if the two corresponding n-tensor product states are adjacent.

Taking under consideration such graph, since the elements of a DFS $\tilde{\mathcal{H}}$ are pairwise distinguishable at the channel's end, then the resulting graph is *complete*. Thus, the largest number of messages that can be transmitted without error by the quantum channel $\mathcal{E}$ is given by the clique number $\tilde{\mathcal{G}}^n$.

This way, the zero-error secrecy capacity of a quantum channel $\mathcal{E}$ that attends the situation 1 of Theorem 6.5 is

$$C_S^{(0)} = \sup_{\tilde{\mathcal{H}}} \sup_n \frac{1}{n} \log \omega(\tilde{\mathcal{G}}^n). \tag{6.41}$$

Given a certain integer and a graph, finding a clique in the graph with size equal to the integer given is an $\mathcal{NP}$-Complete problem. However, some characteristics of the zero-error and of DFS can be taken into account to obtain $C_S^{(0)}(\mathcal{E})$. If the graph built from $\tilde{\mathcal{H}}$ is complete, then the clique number $\tilde{\mathcal{G}}$ is equal to $\dim(\tilde{\mathcal{H}})$, which takes us to the known expression (6.38). Such relation between the clique number and the cardinality of the corresponding set of vertices does not arise in ordinary quantum zero-error channels. This particularity arises thanks to the DFS.

6.5 Security Analysis

To analyze the security of the proposed scheme, we have to consider that there are three types of secrecy.

1. **Strong Secrecy**. It requires that the total amount of information transferred to the eavesdropper goes to zero in the asymptotic limit of the number of communications;
2. **Weak Secrecy**. It requires that the information per symbol transferred to the eavesdropper go to zero in the asymptotic limit of the number of communications [50];
3. **Perfect Secrecy**. It requires that no information is transferred to the eavesdropper [48].

According to the communication scheme proposed, when Alice encodes a message using a quantum wiretap code with parameters $(n, |\mathcal{U}|, 0, 0)$ and sends it to Bob, we have that the set of input states belong to a DFS. Thanks to the DFS, the input states do not interact with the environment. The eavesdropper, in turn, has access only to the environment whose state is pure along the interaction. As a consequence, the information accessible to Eve is zero, obtained from $\chi^{\text{Eva}} = 0$ as shown in the proof of Lemma 6.2. Eve's uncertainty regarding the secret messages does not have changes, even if she observed the state of the environment completely. We can conclude, therefore, that the scheme under consideration has perfect secrecy.

6.6 Examples

We will now show some examples regarding the zero-error secrecy capacity.

Example 6.3 (Strictly Positive ZESC). Initially, we assume that a quantum channel $\mathcal{E}_1$ has positive quantum zero-error capacity reached by an optimum pair $(\mathcal{S}_1, \mathcal{M}_1)$, as shown in Fig. 6.2a. By following the procedures described in Sect. 6.3, a pair $(\mathcal{S}_1^{'}, \mathcal{M}_1^{'})$ is obtained, as shown in Fig. 6.2b.

Characteristic graphs for $\mathcal{E}_1$ with inputs $(\mathcal{S}_1, \mathcal{M}_1)$ and $(\mathcal{S}_1^{'}, \mathcal{M}_1^{'})$ can be found in Fig. 6.3a, b, respectively.

As can be seen, the largest clique has size 2 and is obtained by the pair $(0, 1)$ in both cases. It leads to a quantum zero-error capacity equal to

$$\begin{aligned} C^{(0)}(\mathcal{E}_1) &= \sup_{\tilde{\mathcal{H}}_1} \sup_{n} \frac{1}{n} \log \dim(\tilde{\mathcal{H}}_1)^n \\ &= \log 2 \\ &= 1 \text{ bit per symbol per channel use.} \end{aligned} \tag{6.42}$$

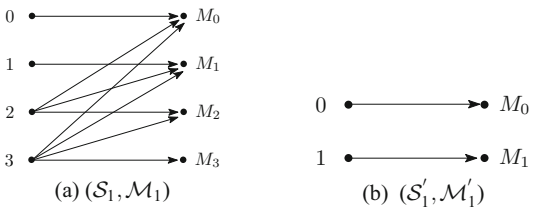

Fig. 6.2 Representation of the transitions performed in the quantum channel $\mathcal{E}_1$ for input states from optimum pairs (**a**) $(\mathcal{S}_1, \mathcal{M}_1)$ and (**b**) $(\mathcal{S}_1^{'}, \mathcal{M}_1^{'})$

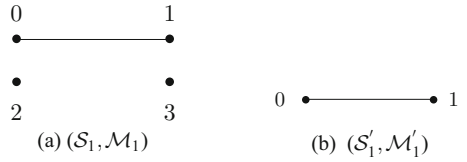

Fig. 6.3 Characteristic graphs for (**a**) $(\mathcal{S}_1, \mathcal{M}_1)$ and (**b**) $(\mathcal{S}_1^{'}, \mathcal{M}_1^{'})$

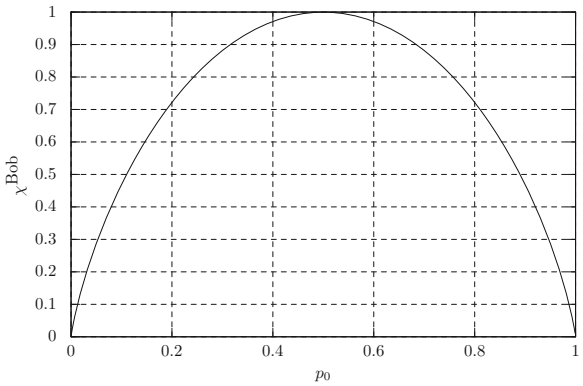

Fig. 6.4 Results obtained in the attempt to maximize (6.43) over the pairs (p_0, p_1)

The quantum states in the DFS $\tilde{\mathcal{H}}_1$ are those from $\mathcal{S}_1^{'}$. To obtain the secrecy capacity of this channel, the software Mathematica® was adopted in the attempt to obtain a maximum value for χ^{Bob}:

$$\begin{aligned} C_S(\mathcal{E}_1) &= \chi^{\text{Bob}} \\ &= \max_{\{P\}} S\left(p_0 \cdot \rho_0 + p_1 \cdot \rho_1\right). \end{aligned} \tag{6.43}$$

To reach this objective, we used an exhaustive search among 30,000 pairs of (p_0, p_1) respecting the restriction that $p_0 + p_1 = 1$. The graphic shown in Fig. 6.4 is a result of such search. As it can be seen, the maximum value for Bob's Holevo quantity is 1. This result was already expected since equal probabilities maximize the von Neumann entropy (6.43).

This way, for the channel $\mathcal{E}_1$, the zero-error secrecy capacity is

$$\begin{aligned} C_S^{(0)}(\mathcal{E}_1) &= \min\left\{C^{(0)}(\mathcal{E}_1), C_S(\mathcal{E}_1)\right\} \\ &= \min\{1, 1\} \\ &= 1 \text{ bits per symbol per channel use.} \end{aligned}$$

It is possible to conclude, from this first example, that there are quantum channels $\mathcal{E}$ whose zero-error secrecy capacity is strictly positive, i.e. , $C_S^{(0)}(\mathcal{E}) > 0$.

Example 6.4 (Non-Trivial ZESC). In this second example, the quantum channel $\mathcal{E}_2$ has positive zero-error capacity reached by an optimum pair $(\mathcal{S}_2, \mathcal{M}_2)$ where $\mathcal{S}_2 = \{\rho_1, \ldots, \rho_6\}$ and $\mathcal{M}_2 = \{M_i = |\rho_i\rangle\langle\rho_i|\}_{i=1}^{6}$. The model of errors for the channel is shown in Fig. 6.5a. Since we are interested in the adjacency relations, the probabilities were omitted.

From the pair $(\mathcal{S}_2, \mathcal{M}_2)$ we obtained the pair $(\mathcal{S}_2^{'}, \mathcal{M}_2^{'})$ were $\mathcal{S}_2^{'} = \{\rho_2, \rho_3, \rho_5\}$ and $\mathcal{M}_2^{'} = \{M_2, M_3, M_5\}$. The relation between input and output states is depicted in Fig. 6.5b.

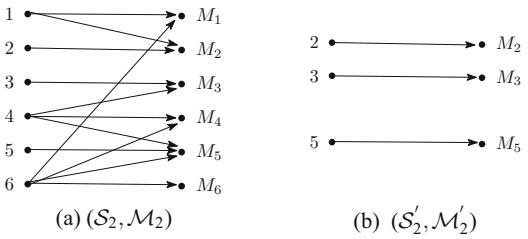

Fig. 6.5 Transitions performed by the quantum channel $\mathcal{E}_2$ over inputs from the optimum pairs (**a**) $(\mathcal{S}_2, \mathcal{M}_2)$ and (**b**) $(\mathcal{S}_2', \mathcal{M}_2')$

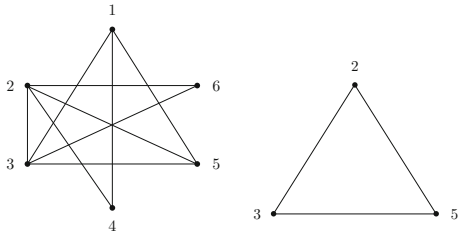

Fig. 6.6 Characteristic graphs of (**a**) $(\mathcal{S}_2, \mathcal{M}_2)$ and (**b**) $(\mathcal{S}_2', \mathcal{M}_2')$

Characteristic graphs for $\mathcal{E}_2$ with inputs $(\mathcal{S}_2, \mathcal{M}_2)$ and $(\mathcal{S}_2', \mathcal{M}_2')$ can be found in Fig. 6.6a, b, respectively. The clique number $\omega(\tilde{\mathcal{G}}(\mathcal{E}_2))$ is equal to 3 and can be obtained from the vertices $(2, 3, 5)$, $(1, 3, 5)$, or also $(2, 3, 6)$ considering the graph in Fig. 6.6a. On the other hand, the clique of the graph in Fig. 6.6b is also equal to 3, but obtained directly from the vertices $(2, 3, 5)$.

The quantum zero-error capacity of $\mathcal{E}_2$ considering the pair $(\mathcal{S}_2', \mathcal{M}_2')$ is

$$\begin{aligned} C^{(0)}(\mathcal{E}_2) &= \sup_{\tilde{\mathcal{H}}_2} \sup_{n} \frac{1}{n} \log \dim(\tilde{\mathcal{H}}_2)^n \\ &= \log 3 \\ &\approx 1,5849 \text{ bits per symbol per channel use.} \end{aligned} \tag{6.44}$$

Aiming at quantifying $C_S(\mathcal{E}_2)$, Bob's Holevo quantity (6.45) was obtained with the software Mathematica® in the attempt to maximize it over the triple (p_1, p_2, p_3) under the restriction $p_1 + p_2 + p_3 = 1$.

$$C_S(\mathcal{E}_2) = \chi^{\text{Bob}} = \max_{\{P\}} S\left(p_1 \cdot \rho_2 + p_2 \cdot \rho_3 + p_3 \cdot \rho_5\right). \tag{6.45}$$

The exhaustive search considered 20,000 valid triples. The results obtained are presented in Fig. 6.7, which shows the graphic obtained in two different perspectives. According to the results observed, the highest value observed for χ^{Bob} was 1.5849 bits per symbol per channel use.

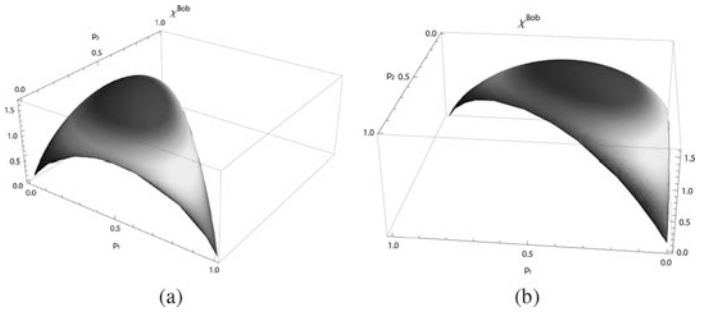

Fig. 6.7 Two different perspectives for the graph of Holevo quantity (6.45) with exhaustive search over the pairs (p_1, p_2, p_3). (**a**) Perspective 1 (**b**) Perspective 2

With these results, we have that the zero-error secrecy capacity of $\mathcal{E}_2$ is

$$\begin{aligned} C_S^{(0)}(\mathcal{E}_2) &\geq \min\left\{C^{(0)}(\mathcal{E}_2), C_S(\mathcal{E}_2)\right\} \\ &\geq \min\{1.5849, 1.5849\} \\ &\geq 1.5849 \text{ bits per symbol per channel use.} \end{aligned}$$

From this example, we can conclude that there are quantum channels $\mathcal{E}$ whose zero-error secrecy capacity is non-trivial, i.e., $C_S^{(0)}(\mathcal{E}) > 1$. We cannot guarantee that the ZESC of $\mathcal{E}_2$ is 1.5849 because we considered the case for $n = 1$. We do not have knowledge if there exists other DFS with higher dimensions for different values of n.

The collective amplitude damping quantum channel [1] has ZESC equal to the one of $\mathcal{E}_2$, characterizing a practical example of the non-triviality of this capacity.

The equality between the zero-error and secrecy capacities verified in the results of the quantum channel $\mathcal{E}_2$ is not a surprise. It happens because it is possible to derive an optimum pair $(\mathcal{S}_2', \mathcal{M}_2')$ from $(\mathcal{S}_2, \mathcal{M}_2)$. This example illustrates a quantum channel which is in the first situation of Theorem 6.5.

Example 6.5 (Situation 2 of Theorem 6.5). In the examples shown previously, we have that $C^{(0)}(\mathcal{E}) = C_S(\mathcal{E})$, emphasizing occurrences of the first situation in the proof of Theorem 6.5. The third example illustrates the second situation described.

Let $\mathcal{E}_3$ be a quantum channel whose model of errors is composed by four elements: $E_0 = |0\rangle\langle 0|, E_1 = |1\rangle\langle 1|, E_2 = \frac{1}{2}|2\rangle\langle 2| + \frac{1}{2}|3\rangle\langle 2|$, and $E_3 = \frac{1}{2}|3\rangle\langle 3| + \frac{1}{2}|2\rangle\langle 3|$, i.e., $\mathcal{E}_3 \equiv \{E_i\}_{i=0}^3$. We have that $\mathcal{S}_3 = \{\rho_i = |i\rangle\langle i|, i = 0, \ldots, 3\}$. The mappings of the channel $\mathcal{E}_3$ over the inputs from $(\mathcal{S}_3, \mathcal{M}_3)$ are shown in Fig. 6.8a.

Upon considering the channel $\mathcal{E}_3$, we can see that its quantum zero-error capacity is equal to $C^{(0)}(\mathcal{E}_3) = \log 3$ bits per symbol per channel use, considering three classical messages associated with the input states in the following way: $0 \mapsto \rho_0$, $1 \mapsto \rho_1$, $2 \mapsto \rho_2$, and $2 \mapsto \rho_3$. However, in the attempt to obtain the quantum secrecy capacity of $\mathcal{E}_3$, it is not possible to obtain a pair $(\mathcal{S}_3', \mathcal{M}_3')$ which is also

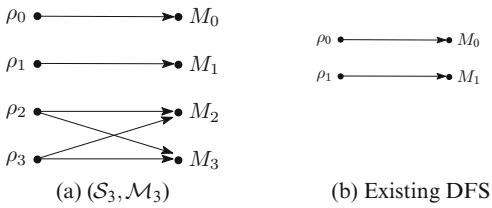

Fig. 6.8 Representation of the mappings of $\mathcal{E}_3$ into the inputs of the optimum pair (**a**) $(\mathcal{S}_3, \mathcal{M}_3)$ and of the (**b**) existing DFS

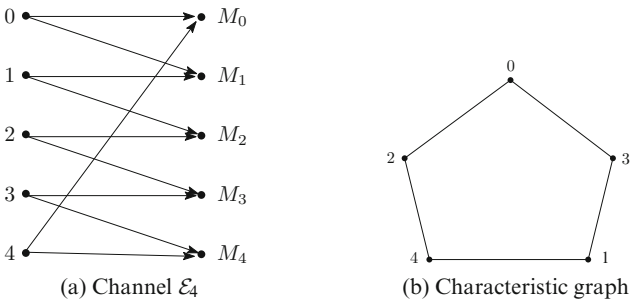

Fig. 6.9 Quantum (**a**) channel $\mathcal{E}_4$ and its (**b**) characteristic graph

optimum, because the transitions that cause $\mathcal{E}_3(\rho_2) = \rho_3$ and $\mathcal{E}_3(\rho_3) = \rho_2$ result in an interaction with the environment. Such interaction causes information leakage which is not adequate for a quantum secrecy scenario. However, this channel has a DFS with 2 states, ρ_0 and ρ_1, shown in Fig. 6.8b.

This way, the ZESC of $\mathcal{E}_3$ is

$$\begin{aligned} C_S^{(0)}(\mathcal{E}_3) &= \min\left\{C^{(0)}(\mathcal{E}_3), C_S(\mathcal{E}_3)\right\} \\ &= \min\{\log 3, \log 2\} \\ &= 1 \text{ bits per symbol per channel use.} \end{aligned}$$

Example 6.6 (Quantum Channel With No Zero-Error Secrecy Capacity). In the previous examples we saw that $C_S^{(0)}(\mathcal{E}) \neq 0$, but it is important to show that it is not always true. For the quantum channel $\mathcal{E}_4$ in Fig. 6.9a, whose characteristic graph is shown in Fig. 6.9b, we have that $C^{(0)}(\mathcal{E})$ is reached by an optimum pair $(\mathcal{S}_4, \mathcal{M}_4)$, with $\mathcal{S}_4 = \{|00\rangle, |12\rangle, |24\rangle, |31\rangle, |43\rangle\}$ and $\mathcal{M}_4 = \{M_{0,0}, M_{1,2}, M_{2,4}, M_{3,1}, M_{4,3}\}$, where $\sum_{M\in\mathcal{M}_4}^{4} M \leq \mathbb{1}$.

Finding the zero-error capacity of the classical channel corresponding to $\mathcal{E}_4$ was a problem proposed by Shannon [49] whose solution was presented 20 years later by Lovász [36]. In the quantum case, the quantum zero-error capacity is reached after two or more uses of the channel, as shown by Medeiros [38, p. 70]. Such result was previously shown in Example 5.4.

The channel $\mathcal{E}_4$ is not unital and there is no $M_i \in \mathcal{M}$ that satisfies the condition $\mathcal{E}(M_i) = M_i \mathcal{E} M_i$. This way, there is no DFS in the inner structure of the error-free code associated with the channel. It means that every input performs a transition which causes an undesired interaction with the environment which can lead to an information leakage. This way, we have that the quantum secrecy capacity of $\mathcal{E}_4$ is

$$\begin{aligned} C_S^{(0)} &= \min\left\{C^{(0)}(\mathcal{E}), C_S(\mathcal{E})\right\} \\ &= \min\left\{\frac{1}{2}\log 5, 0\right\} \\ &= 0. \end{aligned}$$

This example illustrates that despite some channels have positive and non-trivial quantum zero-error capacity obtained from two or more uses of the channel, the nonexistence of a DFS causes $\mathcal{M}' = \varnothing$. It results that no pair $(\mathcal{S}', \mathcal{M}')$ can be used to encode messages without decoding errors and with secrecy. In other words, $C_S^{(0)}(\mathcal{E}_4) = 0$.

6.7 Related Literature

Until the first articles describing the results presented in Sect. 6.3 [20–23], many works in the literature explored the use of DFS in communication, but not considering their capability to send unconditionally secure messages. Among some works it was possible to see applications of DFS in protocols for quantum secure direct communication and for quantum deterministic secure communication [3, 12, 43]. In such protocols there is redundancy and eavesdropping check which increases significantly the number of messages exchanged in order to perform the communication with security. By using results previously discussed [23], all these protocols could be simplified with less message exchanges but with the same security, as can be seen in more detail in [19].

Regarding quantum wiretap channels, a few codes for this purpose were found, as presented previously in Sect. 6.2. The codes proposed by Hamada [25, 26] are based on CSS codes and, according to the author, can be easily used for practical implementation since they do not demand resources as entanglement. However, the rate of these codes is below the quantum secrecy capacity of the channel. The work of Wilde, Guha, and Dutton [16, 53] shows a code for quantum wiretap channels based on polar codes. The authors discuss that these codes can be restricted to certain quantum channels. Regarding the proposition of wiretap codes from DFS and quantum error-avoiding codes, as shown in Sect. 6.3, no similar strategies were found so far.

Braunstein et al. [4] enlighten the relation between DFS and zero-error subspaces, showing how the last is an instance of the former. Besides, the authors also

proposed a method to find DFS in zero-error subspaces which has similarities with the method of Medeiros et al. [39]. In the characterization of the zero-error secrecy capacity we opted out to use the method of Medeiros et al. because it is guaranteed optimum and because it helped in showing a more intuitive approach to find a DFS in a quantum channel with positive zero-error capacity. It is important to emphasize that the work of Braunstein et al. [4] has other results, such as lower and upper bounds for the dimension of such subspaces.

Starting from confusability graphs for quantum channels, the work of Chiribella and Yang [8] aims at searching for connected components to identify, among others, decoherence-free subspaces. The work of these authors, however, focus on quantum covariant channels and they did not explore the quantum zero-error capacity of such channels nor the relation with the confusability graphs considered by Duan et al. [15].

Regarding capacity, Watanabe [52] characterizes a class of *quantum channels more capable than the environment*. In these channels, the quantum capacity and the secrecy capacity are equal. However, the author shows that the conditions that make a channel of such kind are, in general, hard to verify.

6.8 Further Reading

This chapter aimed at showing the zero-error secrecy capacity, the highest rate according to which it is possible to exchange messages through certain noisy and wiretapped quantum channels without decoding errors nor information leakage. This capacity puts together concepts of quantum zero-error information theory, of quantum secrecy capacity, and of decoherence-free subspaces and subsystems. The results, when possible, were also shown in terms of graph theory and the security analysis was discussed. Detailed examples illustrated the concepts introduced. Relations with other works in literature were also presented.

The articles that introduce the concepts to build up the zero-error secrecy capacity can be found in [20–23]. The thesis in which the concept was fully characterized was published only in Portuguese [18].

Besides the quantum zero-error information theory, the other building blocks of ZESC which are the decoherence-free subspaces and quantum wiretap channels, covered in the sections of this chapter, are very interesting with many applications and with perspective for many developments. As a suggestion regarding DFS, we recommend the work of Lidar and Whaley [34] and the thesis of Bacon [1]. Regarding quantum wiretap channels, we recommend the seminal papers of Cai et al. [6] and Devetak [11]. The book of Hayashi [27, Sect. 9.5] contains a section regarding this subject in the context of discussing quantum communications over eavesdropped channels.

Regarding future work with ZESC, Shabani et al. [46, 47] discuss the existence of "more relaxed" conditions for the existence of DFS. Taking this into account, could such conditions be considered and implemented in practical scenarios to

favor the positivity of the zero-error secrecy capacity in a more wide number of noisy quantum channels? Such answer could favor more practical implementations of quantum communications which are simultaneously error-free and secure.

References

1. Bacon DM (2001) Decoherence, control, and symmetry in quantum computers. Ph.D Thesis, University of California at Berkeley, USA
2. Beige A, Braun D, Tregenna B, Knight PL (2000) Quantum computing using dissipation to remain in a decoherence-free subspace. Phys Rev Lett 85:1762, doi:10.1103/PhysRevLett.85.1762
3. Bin G, ShiXin P, Biao S, Kun Z (2009) Deterministic secure quantum communication over a collective-noise channel. Science in China Series G: Sci China Ser G Phys Mech Astron 52(12):1913–1918. doi:10.1007/s11433-009-0303-y
4. Braunstein SL, Kribs DW, Patra MK (2011) Zero-error subspaces of quantum channels. In: IEEE international symposium on information theory, Russia, pp 104–108
5. Byrd MS, Wu LA, Lidar DA (2004) Overview of quantum error prevention and leakage elimination. J Mod Opt 51(16–18):2449–2460. doi:10.1080/09500340408231803
6. Cai N, Winter A, Yeung RW (2004) Quantum privacy and quantum wiretap channels. Probl Inf Transm 40:318–336
7. Casati GBG, Strini G (2007) Principles of quantum computation and information. In: Basic tools and special topics, vol II. World Scientific, Singapore
8. Chiribella G, Yang Y (2013) Confusability graphs for symmetric sets of quantum states. In: XXIX international colloquium on group-theoretical methods in physics, World Scientific, Tianjin, China, pp 251–256
9. Choi MD, Kribs DW (2006) A method to find quantum noiseless subsystems. Phys Rev Lett 96:501–506
10. Davidson K (1996) C^*-algebras by example. Fields institute monographs. American Mathematical Society, Rhode Island
11. Devetak I (2005) The private classical capacity and quantum capacity of a quantum channel. IEEE Trans Inf Theory 51(1):44–55
12. Dong HK, Dong L, Xiu XM, Gao YJ (2010) A deterministic secure quantum communication protocol through a collective rotation noise channel. Int J Quantum Inf 8(8):1389–1395
13. Dorner U, Klein A, Jaksch D (2008) A quantum repeater based on decoherence free subspaces. Quantum Inf Comput 8:468
14. Duan LM, Guo GC (1999) Quantum error avoiding codes versus quantum error correcting codes. Phys Lett A 255:209–212. doi:10.1016/S0375-9601(99)00183-8
15. Duan R, Severini S, Winter A (2013) Zero-error communication via quantum channels, noncommutative graphs and a quantum Lovasz ϑ function. IEEE Trans Inf Theory 59(2):1164–1174
16. Dutton Z, Guha S, Wilde MM (2012) Performance of polar codes for quantum and private classical communication. In: 50th annual allerton conference on communication, control, and computing, Illinois, pp 1–8
17. Feng M (2001) Quantum computing and communication with decoherence-free atomic states. http://arxiv.org/abs/quant-ph/0111041. Accessed 2 Dec 2012
18. Guedes EB (2013) Capacidade quântica de sigilo erro-zero e informação acessível erro-zero de fontes quânticas. Ph.D Thesis, Universidade Federal de Campina Grande, Brazil
19. Guedes EB, de Assis FM (2012) Enhancing quantum protocols with the security of decoherence-free subspaces and subsystems. In: IV workshop school of quantum computation and information, Fortaleza, Brazil, pp 1–8

20. Guedes EB, de Assis FM (2012) Quantum zero-error secrecy capacity. In: IV workshop school of quantum computation and information, Fortaleza, Brazil, pp 1–8
21. Guedes EB, de Assis FM (2012) Unconditional security with decoherence-free subspaces. http://arxiv.org/abs/1204.3000. Accessed 30 Mar 2012
22. Guedes EB, de Assis FM (2012) Utilização de subespaços livres de descoerência em comunicações quânticas incondicionalmente seguras. In: Simpósio Brasileiro de Telecomunicações – SBrT'12, Brasília, Brazil, pp 1–5
23. Guedes EB, de Assis FM (2013) On the security of decoherence-free subspaces and subsystems for classical information conveying through quantum channels. Int J Quantum Inf 11(2):1350022-1–1350022-14
24. Gyongyosi L, Imre S (2012) Long-distance quantum communications with superactivated gaussian optical quantum channels. Opt Eng 51(1):1–16
25. Hamada M (2008) Algebraic and quantum theoretical approach to coding on wiretap channels. In: International symposium on communications, control and signal processing, Malta, pp 1–6
26. Hamada M (2008) Constructive codes for classical and quantum wiretap channels. Nova Science Publishers, New York, pp 1–48
27. Hayashi M (2006) Quantum Information – An Introduction. Springer, Japan
28. Holevo AS (1998) The capacity of the quantum channel with general signal states. IEEE Trans Inform Theory 4(1):269–273
29. Ivanov PA, Poschinger UG, Singer K, Schmidt-Kaler F (2010) Quantum gate in the decoherence-free subspace of trapped-ion qubits. Europhysics Letters 92(3):30006
30. Jaeger G, Sergienko A (2008) Constructing four-photon states for quantum communication and information processing. Int J Theoret Phys 47:2120
31. Kielpinski D (2001) A decoherence-free quantum memory using trapped ions. Science 291:1013
32. Knill E, Laflamme R, Viola L (2000) Theory of quantum error correction for general noise. Phys Rev Lett 84:2525
33. Kwiat PG, Berglund AJ, Altepeter JB, White AG (2000) Experimental verification of decoherence-free subspaces. Science 290:498–501
34. Lidar DA, Whaley KB (2003) Decoherence-Free Subspaces and Subsystems, Springer Lecture Notes in Physics, Berlin, pp 83–120
35. Lidar DA, Chuang IL, Whaley KB (1998) Decoherence-free subspaces for quantum computation. Phys Rev Lett 81:2594–2597
36. Lovász L (1979) On the Shannon capacity of a graph. IEEE Trans Inform Theory 25(1):1–7
37. Mayers D (2001) Unconditional security in quantum cryptography. J ACM 48(3):351–406
38. Medeiros RAC (2008) Zero-error capacity of quantum channels. PhD thesis, Universidade Federal de Campina Grande – TELECOM Paris Tech
39. Medeiros RA, Alleaume R, Cohen G, de Assis FM (2006) Zero-error capacity of quantum channels and noiseless subsystems. In: IEEE International Telecommunications Symposium, Fortaleza, Brazil, pp 900–905, 3–6 Sept 2006
40. Medeiros RAC, Alleaume R, Cohen G, de Assis FM (2006) Quantum states characterization for the zero-error capacity. http://arxiv.org/abs/quant-ph/0611042, accessed 25 Oct. 2013
41. Mohseni M, Lundeen JS, Resch KJ, Steinberg AM (2003) Experimental application of decoherence-free subspaces in an optical quantum-computing algorithm. Phys Rev Lett 91:187903
42. Nielsen MA, Chuang IL (2010) Quantum Computation and Quantum Information. Cambridge University Press, Cambridge, England
43. Qin S, Wen Q, Meng L, Zhu F (2009) Quantum secure direct communication over the collective amplitude damping channel. Science in China Series G: Physics, Mechanics and Astronomy 52(8):1208–1212, DOI 10.1007/s11433-009-0140-z
44. Schumacher B, Westmoreland MD (1997) Sending classical information via noisy quantum channels. Phys Rev A 56:131–138, doi: 10.1103/PhysRevA.56.131
45. Schumacher B, Westmoreland M (1998) Quantum privacy and quantum coherence. Phys Rev Lett 80(25):5695–5697

46. Shabani A (2009) Open quantum systems and error correction. Ph.D Thesis, University of Southern California
47. Shabani A, Lidar DA (2005) Theory of initialization-free decoherence-free subspaces and subsystems. Phys Rev A 72:042303. doi:10.1103/PhysRevA.72.042303
48. Shannon CE (1949) Communication theory of secrecy systems. Bell Syst Tech J 28(4): 656–715
49. Shannon CE (1956) The zero error capacity of a noisy channel. IRE Trans Inf Theory 2(3):8–19
50. Subramaniany A, Suresh AT, Raj S, Thangaraj A, Blochy M, McLaughliny S (2010) Strong and weak secrecy in wiretap channels. In: International symposium on turbo codes and iterative information processing, Brest, France, pp 30–34
51. Viola L, Fortunato EM, Pravia MA, Knill E, Laflamme R, Cory DG (2001) Experimental realization of noiseless subsystems for quantum information processing. Science 293:2059–2063. doi:10.1103/PhysRevA.85.012326
52. Watanabe S (2012) Private and quantum capacities of more capable and less noisy quantum channels. Phys Rev A 85:012326. doi:10.1103/PhysRevA.85.012326
53. Wilde MM, Guha S (2011) Polar codes for degradable quantum channels. http://arxiv.org/abs/1109.5346. Accessed 13 Feb 2016
54. Wyner AD (1975) The wire-tap channel. Bell Syst Tech J 54(8):1355–1387
55. Xia Y, Song J, Yang ZB, Zheng SB (2010) Generation of four-photon polarization-entangled decoherence-free states within a network. Appl Phys B 99:651–656
56. Xue P (2008) Long-distance quantum communication in a decoherence-free subspace. Phys Lett A 372:6859–6866
57. Xue P, Xiao YF (2006) Universal quantum computation in decoherence-free subspace with neutral atoms. Phys Rev Lett 97:140501
58. Zanardi P, Rasetti M (1997) Noiseless quantum codes. Phys Rev Lett 79:3306. doi:10.1103/PhysRevLett.79.3306
59. Zhang XD, Zhang Q, Wang ZD (2006) Physical implementation of holonomic quantum computation in decoherence-free subspaces with trapped ions. Phys Rev A 74:034302