Utilização de Subespaços Livres de Descoerência em Comunicações Quânticas Incondicionalmente Seguras

Elloá B. Guedes e Francisco M. de Assis

***Resumo*— Neste trabalho será mostrado como subespaços livres de descoerência em canais quânticos com descoerência coletiva podem ser usados para transmitir informação clássica com sigilo absoluto. Além disso, também será mostrado que, se determinadas condições de simetrias forem garantidas, então a taxa máxima em que estas comunicações sigilosas acontecem iguala-se à capacidade ordinária do canal quântico para o envio de mensagens clássicas. Estes resultados caracterizam uma nova técnica para enviar mensagens clássicas via canais quânticos com segurança incondicional.**

***Palavras-Chave*— Subespaços Livres de Descoerência; Capacidade de Sigilo; Segurança Incondicional.**

***Abstract*— We show how to use decoherence-free subspaces over collective-noise quantum channels to convey classical information in perfect secrecy. We also show that if some symmetry conditions are guaranteed, the maximum rate on which such secret communications take place is equal to the ordinary capacity of a quantum channel to convey classical information. These results characterize a new technique to convey classical messages via quantum channels with unconditional security.**

***Keywords*— Decoherence-Free Subspaces; Secrecy Capacity; Unconditional Security.**

I. Introdução

A interação de um sistema quântico com o ambiente no qual ele está inserido e a subseqüente *descoerência* em função deste acoplamento é uma das principais causas de erros nestes sistemas. Em função da natureza frágil dos estados quânticos, a descoerência é considerada um dos maiores obstáculos para a transmissão de informação coerente [1].

Considerando um contexto criptográfico, a ocorrência de descoerência também causa o vazamento da informação para o ambiente. Se um espião passa a ter acesso ao estado do ambiente, pode vir a adquirir informações sobre uma dada mensagem secreta, por exemplo, o que é altamente indesejado neste cenário. Então, combater a descoerência é uma maneira de colaborar para o envio de informação secreta.

Em sistemas quânticos perfeitamente isolados, não há interação com o ambiente externo e, portanto, a descoerência não ocorre. Porém, construir sistemas desta natureza é uma tarefa altamente complexa e distante dos dias atuais [2]. Uma alternativa que resta é lidar com a descoerência e tentar prover meios de minimizá-la ou evitá-la. Neste sentido, diversas técnicas já vêm sendo propostas, a citar: códigos corretores de erros quânticos (QECC – *Quantum error-correcting codes*), desacoplamento dinâmico, subespaços livres de descoerência (DFS – *Decoherence-free subspaces*), dentre outros [3].

Em se tratando dos DFS, em particular, utilizam-se simetrias existentes nos operadores de erro para encontrar estados quânticos que são imunes aos efeitos da descoerência. Com isto, uma conseqüência que se tem é a preservação da coerência. Muitos trabalhos já exploram os DFS neste sentido [4]–[6], inclusive até com implementações experimentais [7]–[10].

Enquanto os trabalhos existentes na literatura focam na preservação da coerência, há um grande potencial no uso de DFS para Comunicações Quânticas. O presente trabalho se propõe a explorar esta perspectiva, tomando como objetivo verificar a adequação dos DFS para troca de mensagens com segurança incondicional.

Como resultado, foi verificado que é possível trocar mensagens clássicas via canais quânticos com segurança incondicional, desde que (i) o canal em uso possua algumas simetrias que possibilitem a existência de DFS; e que (ii) um espião da comunicação tenha acesso *apenas* ao ambiente. Foi possível constatar que a capacidade de enviar sigilo torna-se igual a capacidade de enviar informação clássica ordinária nesse cenário, ou seja, tem-se o caso particular em que a taxa de sigilo é maximal.

Uma das vantagens da estratégia proposta é a possibilidade de facilitar a construção de dispositivos para troca segura de mensagens quânticas. Ao invés de demandar um avanço tecnológico que combata completamente a descoerência, esta estratégia permite que dispositivos sejam construídos sem um total isolamento entre sistema de interesse e ambiente, mas ainda assim sendo capazes de prover comunicação com sigilo absoluto. Isto é bastante factível, especialmente já considerando resultados existentes sobre a utilização de DFS em comunicações [11]–[13], inclusive de longa distância [14].

Para apresentar os resultados mencionados, o presente artigo está organizado como segue. Os conceitos de DFS serão apresentados na Seção II. Após isto, a caracterização e os resultados da aplicação do mesmo em comunicações quânticas incondicionalmente seguras serão apresentados na Seção III. Um exemplo detalhado ilustrando um canal quântico com descoerência coletiva será apresentado na Seção IV. Por fim, as considerações finais serão apresentadas na Seção V.

II. Subespaços Livres de Descoerência

A *descoerência* emerge como resultado de um acoplamento inevitável entre um sistema quântico e o ambiente no qual

Elloá B. Guedes e Francisco M. de Assis, Instituto de Estudos em Computação e Informação Quânticas (IQuanta), Universidade Federal de Campina Grande, Rua Aprígio Veloso, 882 – Campina Grande-PB – Brasil, E-mails: elloaguedes@gmail.com, fmarcos@dee.ufcg.edu.br. Este trabalho foi parcialmente financiado com recursos do CNPq.

ele está inserido. Em função deste acoplamento indesejado, o sistema pode, por exemplo, começar a perder energia para o ambiente, decaindo para um estado de baixa energia e tendo sua fase relativa apagada, o que culmina com a perda da informação [15].

Seja um sistema quântico fechado composto pelo sistema de interesse S definido sob um espaço de Hilbert $\mathcal{H}$ e pelo ambiente E. O hamiltoniano que descreve este sistema é definido como segue:

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

em que $\mathbb{1}$ é o operador identidade; e $\mathbb{H}_S$, $\mathbb{H}_E$ e $\mathbb{H}_{SE}$ denotam os hamiltonianos do sistema, ambiente e interação sistema-ambiente, respectivamente.

Para prevenir erros, seria ideal fazer $\mathbb{H}_{SE}$ igual a zero, indicando que sistema e ambiente estão desacoplados e evoluem independentemente e unitariamente de acordo com seus respectivos hamiltonianos $\mathbb{H}_S$ e $\mathbb{H}_E$ [2]. Porém, em cenários práticos, tal situação ideal não é possível visto que nenhum sistema é totalmente imune a erros. Então, após isolar o sistema de interesse da melhor maneira possível, deve-se buscar meios realísticos para identificação e correção de erros quando eles ocorram, para prevenção de erros quando possível, ou para supressão de erros no sistema [3].

Se algumas simetrias existem na interação entre sistema e ambiente, é possível encontrar "locais seguros" no espaço de Hilbert que não experienciam a descoerência. Seja $\{A_i(t)\}$ um conjunto de operadores segundo a *representação operator-sum* (OSR), correspondendo à evolução do sistema. Diz-se que a matriz densidade ρ_S é *invariante* perante os operadores $\{A_i(t)\}$ se $\sum_i A_i(t)\rho_S A_i^\dagger(t) = \rho_S$. Levando isto em consideração, agora é possível definir os DFS, cujos estados são invariantes apesar de existir um acoplamento não-trivial entre sistema e ambiente:

Definição 1. *(Subespaço Livre de Descoerência [16]) Um subespaço $\tilde{\mathcal{H}}$ de um espaço de Hilbert $\mathcal{H}$ é chamado* livre de descoerência *com respeito ao acoplamento entre sistema e ambiente se cada estado puro*[1] *deste subespaço é invariante perante a evolução OSR para quaisquer condição inicial possível do ambiente:*

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

Sistemas quânticos definidos sobre DFS são totalmente desacoplados do ambiente e, por esta razão, completamente imunes aos efeitos da descoerência. Códigos quânticos construídos a partir de estados de um DFS são classificados como *códigos quânticos de prevenção de erros* (QEAC – *Quantum Error-Avoiding Codes*), nos quais as tarefas de perturbação e recuperação são triviais [17].

O próximo passo na caracterização dos DFS é especificar as condições onde eles ocorrem. Seja o hamiltoniano da interação entre sistema e ambiente dado por: $\mathbb{H}_{SE} = \sum_j \mathbf{S}_j \otimes \mathbf{E}_j$, em que $\mathbf{S}_j$ e $\mathbf{E}_j$ são os operadores do sistema e ambiente, respectivamente. Considera-se que os operadores $\mathbf{E}_j$ são linearmente independentes. As simetrias requeridas para a existência de um DFS são apresentadas no teorema a seguir. Para uma prova detalhada ou diferentes formulação, ver [2, Sec. 5].

Teorema 1. *(*Condições para DFS *[18]) Um subespaço $\tilde{\mathcal{H}}$ é um DFS se, e somente se, os operadores do sistema $\mathbf{S}_j$ atuam proporcionalmente à identidade neste subespaço:*

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

Na prática, identificar uma simetria útil e tirar proveito dela pode ser difícil, pois deve-se: (i) identificar a simetria; e (ii) encontrar os estados imunes à interação. Para facilitar esta tarefa, um método proposto por Choi e Kribs [19] visa encontrar os estados pertencentes a um DFS dado o modelo de erros que atua sobre o sistema quântico de interesse.

Em se tratando dos DFS como QEACs, eles podem ser contrastados com os QECCs em alguns aspectos. Enquanto os QECCs são projetados para corrigir erros apenas após a sua ocorrência, QEACs não possuem habilidades de corrigir erros, uma vez que eles atuam prevenindo-os; QECCs em cenários práticos pertencem à classe dos códigos não-degenerados, ao passo que os QEACs são altamente degenerados; QEACs possuem distância infinita, enquanto os QECCs não-degenerados possuem distância finita; QEACs costumam demandar menos qubits físicos para representar um qubit lógico que os QECCs. Em particular, se a degenerescência atinge o máximo, um QECC se reduz a um QEAC, o que ilustra uma circunstância em que um tipo de código torna-se equivalente ao outro [17].

A ausência de descoerência nos DFS tem se mostrado de grande utilidade em implementações de memórias e algoritmos quânticos. Outras aplicações dos DFS incluem codificação em pontos quânticos, dissipação coletiva, redução de ruído, dentre outras [2], [3].

III. DFS em Comunicações Quânticas Incondicionalmente Seguras

A partir de agora serão consideradas as aplicações do DFS em Comunicações Quânticas. Para tanto, será considerado o uso de *canais quânticos com ruído coletivo*, i.e., um modelo de canais quânticos no qual diversos qubits se acoplam identicamente ao mesmo ambiente, ao passo que sofrem defasamento e dissipação [20]. O foco a ser considerado nesta análise, em particular, será nos aspectos da troca de mensagens seguras.

Para caracterizar a troca segura de mensagens, é necessário caracterizar o modelo de comunicações e a estratégia utilizada pelo espião. Neste trabalho será utilizado um modelo análogo ao proposto Wyner [21], no qual os participantes legítimos (Alice e Bob) utilizam um canal, denominado *canal principal*, e o espião (Eva) utiliza um canal *wiretap*, uma versão degradada do canal principal. A depender do código utilizado pelos participantes legítimos, pode haver sigilo absoluto. Para tanto, a taxa do código utilizado por Alice e Bob deve ficar abaixo da chamada *capacidade de sigilo clássica*, dada por

$$C_S = \max_{\{P\}} \{I(A;B) - I(A;E)\}, \quad (4)$$

em que o máximo é tomado sobre todas as distribuições de probabilidade sobre o símbolos de entrada; I denota a

[1] Um estado puro é um vetor unitário no espaço de Hilbert $\mathcal{H}$.

informação mútua; e, A, B e E são variáveis aleatórias, representando a entrada do canal principal provida por Alice, a saída do canal principal recebida por Bob, e a saída do canal *wiretap* recebida por Eva, respectivamente.

Mais especificamente, o modelo a ser utilizado neste trabalho consiste na versão quântica do modelo proposto por Wyner [21], adaptada por Cai et al. [22] e por Devetak [23]. Neste modelo, Alice e Bob utilizam um sistema quântico, chamado de *canal quântico principal*, para trocar mensagens, enquanto a espiã Eva tem acesso total ao ambiente no qual este sistema quântico está inserido, conforme ilustrado Figura 1. Há sigilo sempre que a taxa do código quântico utilizado estiver abaixo da *capacidade quântica de sigilo*, denotada por

$$C_S \geq \max_{\{P\}} \left\{ \chi^{\text{Bob}} - \chi^{\text{Eva}} \right\} \tag{5}$$

em que o máximo é tomado sobre todas as distribuições de probabilidade sobre a entrada, e χ^{Bob} e χ^{Eva} representam as quantidades de Holevo de Bob e Eva, respectivamente.

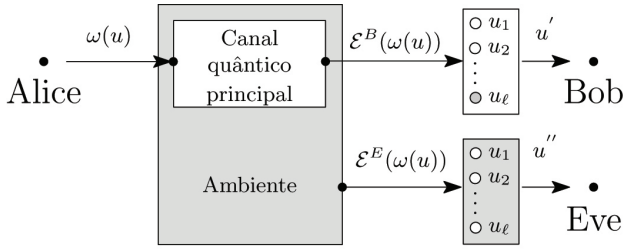

Fig. 1. Idéia geral do canal *wiretap* quântico.

Uma particularidade a ser considerada neste trabalho diz respeito à existência de um DFS no canal quântico principal utilizado por Alice e Bob, cujos estados serão empregados na codificação da mensagem secreta. A formalização do canal em questão é dada a seguir.

Definição 2. *(Canal* Wiretap *Quântico com Ruído Coletivo) Um canal* wiretap *quântico com superoperador $\mathcal{E}$ em um espaço de Hilbert complexo $\mathcal{H}$ é um canal* wiretap *quântico como definido por [22, Sec. 3, Def. 1], mas com a particularidade dos operadores de erro $\{A_i\}$ respeitarem às condições do Teorema 1, dando origem a um DFS $\tilde{\mathcal{H}} \subset \mathcal{H}$.*

Embora o canal já esteja caracterizado, é necessário definir um código para Alice e Bob se comunicarem. Este código será um QEAC definido sobre $\tilde{\mathcal{H}}$, cuja formalização se dá como segue.

Definição 3. *Seja $\tilde{\mathcal{H}}$ um DFS gerado pelo conjunto de autovetores $\{\tilde{k}\}$, i.e., $\tilde{\mathcal{H}} = Span[\{\tilde{k}\}]$. Um conjunto de palavras código de comprimento n para um conjunto de mensagens clássicas $\mathcal{U}$ é um conjunto de estados de entrada rotulados por mensagens em $\mathcal{U}$, $\tilde{K}(\mathcal{U}) = \{\tilde{k}(u) : u \in \mathcal{U}\} \subseteq \tilde{\mathcal{H}}$, e um processo de decodificação trivial composto por operadores positivos $\tilde{\mathcal{D}}_u$, $u \in \mathcal{U}$ com $\sum_{u\in\mathcal{U}} \tilde{\mathcal{D}}_u \leq \mathbb{1}$. O par $(\tilde{K}(\mathcal{U}), \{\tilde{\mathcal{D}}_u : u \in \mathcal{U}\})$ é chamado um QEAC de comprimento n para o conjunto de mensagens $\mathcal{U}$. A taxa deste código é igual a $R = \frac{1}{n}\log|\mathcal{U}|$.*

Usando o código definido, se Alice quer enviar uma mensagem u, ela irá codificá-la utilizando o QEAC definido sobre $\tilde{\mathcal{H}}$, obtendo $\tilde{k}(u)$. Quando ela envia o estado $\tilde{k}(u)$ pelo canal, este irá interagir com o ambiente, que é assumido iniciar no estado $|0_E\rangle\langle 0_E|$. Bob então recebe $\rho_{\text{Bob}}(\tilde{k}(u))$ e Eva recebe $\rho_{\text{Eva}}(\tilde{k}(u))$, os quais serão dados por:

$$\rho_{\text{Bob}}(\tilde{k}(u)) = \text{Tr}_{\text{E}}\left[\mathcal{E}^{\otimes n}(\tilde{k}(u)\otimes|0_{\text{E}}\rangle\langle 0_{\text{E}}|)\right], \tag{6}$$

$$\rho_{\text{Eva}}(\tilde{k}(u)) = \text{Tr}_{\text{B}}\left[\mathcal{E}^{\otimes n}(\tilde{k}(u)\otimes|0_{\text{E}}\rangle\langle 0_{\text{E}}|)\right]. \tag{7}$$

Uma vez que Alice utilizou um QEAC como na Definição 3, então a simetria dinâmica existente protegeu a informação da interação com o ambiente. Isto significa que a evolução conjunta entre sistema e ambiente aconteceu de maneira desacoplada. Assim, o estado $\rho_{\text{Bob}}(\tilde{k}(u))$ é dado por:

$$\rho_{\text{Bob}}(\tilde{k}(u)) = \text{Tr}_{\text{E}}\left[\mathcal{E}^{\otimes n}(\tilde{k}(u)\otimes|0_E\rangle\langle 0_E|)\right] \tag{8}$$

$$= \text{Tr}_{\text{E}}\left[\sum_i A_i\left(\tilde{k}(u)\otimes|0_E\rangle\langle 0_E|\right)A_i^\dagger\right] \tag{9}$$

$$= \text{Tr}_{\text{E}}\left[\tilde{k}(u)\otimes\rho_E\right] \tag{10}$$

$$= \tilde{k}(u), \tag{11}$$

em que (10) acontece devido à invariância de um estado do DFS perante os operadores OSR. Levando em conta o hamiltoniano do sistema quântico dado em (1) e o fato do sistema de interesse e o ambiente não terem interagido, então é possível garantir que o ambiente sofreu apenas a ação de $\mathbb{H}_E$, o qual indica uma evolução unitária restrita ao ambiente. Isto significa que $\rho_{\text{Eva}}(\tilde{k}(u)) = \rho_{\text{E}}$ em (7) é um estado puro.

Para mostrar que a informação enviada pelo canal, utilizando o código apresentado, é protegida de Eva, o seguinte lema é apresentado.

Lema 1. *Um QEAC como na Definição 3 sobre um canal* wiretap *com ruído coletivo como na Definição 2 é um código para* wiretap *quântico com parâmetros $(n, |\mathcal{U}|, \lambda, \mu)$ sobre este mesmo canal.*

Demonstração. Um código para *wiretap* quântico é definido por Cai et al. [22, Sec. 3]. De acordo com estes autores, para que haja sigilo duas condições precisam ser satisfeitas: (i) deve haver uma baixa probabilidade média de erro na decodificação e (ii) a informação acessível média do espião deve ser arbitrariamente pequena.[2] A prova de que o QEAC é equivalente a um código *wiretap* quântico é feita de maneira direta, mostrando pontualmente como cada um destes requisitos são satisfeitos.

Primeiro a probabilidade média de erro na decodificação será analisada. Uma vez que $\tilde{k}(u)$ pertence a $\tilde{\mathcal{H}}$, então é possível garantir que não houve interação com o ambiente. Então, $\rho_{\text{Bob}} = \tilde{k}(u)$, como mostrado em (8)-(10). Por conseqüência, tem-se que o processo de decodificação é trivial e que a mensagem enviada por Alice pode ser perfeitamente recuperada por Bob, visto que há um operador $\tilde{\mathcal{D}}_u$ para cada

[2] A formulação matemática de tais requisitos é apresentada em (9) e (10) no trabalho de Cai et al. [22].

$u \in \mathcal{U}$. É possível constatar, portanto, que a probabilidade de erro média na decodificação é desprezível.

O segundo passo consiste em analisar a informação média acessível por Eva, que é dada da seguinte forma, em que S é a entropia de von Neumann:

$$S\left(\sum_{u\in\mathcal{U}} \frac{1}{|\mathcal{U}|} \operatorname{Tr}_{\mathrm{B}} \mathcal{E}^{\otimes n}(\tilde{k}(u))\right) - \sum_{u\in\mathcal{U}} \frac{1}{|\mathcal{U}|} S\left(\operatorname{Tr}_{\mathrm{B}} \mathcal{E}^{\otimes n}(\tilde{k}(u))\right) \leq \mu \tag{12}$$

em que μ é um número arbitrariamente pequeno. Para provar este requisito, ao invés de calcular a informação acessível média diretamente, será utilizado um limitante para esta medida, denominado *quantidade de Holevo*, cuja definição é apresentada a seguir:

$$\chi^{\text{Eve}} = S(\rho_{\text{Eve}}(\tilde{k}(u))) - \sum_k p_k S(\rho_{\text{Eve},k}\tilde{k}(u)) \tag{13}$$

Em virtude da utilização de estados de um DFS para codificação, é possível afirmar que não houve interação entre sistema e ambiente. Nesse caso, a evolução do ambiente foi governada apenas pelo hamiltoniano $\mathbb{H}_E$, o que indica uma evolução unitária dentro do ambiente. Isto significa que o estado final do ambiente é puro. Portanto:

$$\begin{aligned}
\chi^{\text{Eve}} &= S(\rho_{\text{Eve}}(\tilde{k}(u))) - \sum_k p_k S(\rho_{\text{Eve},k}\tilde{k}(u)) && (14)\\
&= S(\rho_E) - \sum_k p_k S(\rho_{\text{Eve},k}\tilde{k}(u)) && (15)\\
&= 0 - \sum_k p_k S(\rho_{\text{Eve},k}\tilde{k}(u)). && (16)
\end{aligned}$$

Sabe-se que $\chi^{\text{Eve}} \geq 0$, $S(\rho) \geq 0$ para qualquer ρ, e que $p_k \geq 0$. Então, para assegurar a positividade, este é o caso em que o termo remanescente é igual a zero, implicando em $\chi^{\text{Eve}} = 0$. Dado que a quantidade de Holevo é um limitante superior para a informação acessível, tem-se que (12) é igual a zero. Isto conclui a prova. □

Outra medida de informação que enfatiza a ausência de interação entre sistema e ambiente é a *troca de entropia*, a qual é determinada inteiramente pelo estado inicial do sistema de interesse e pela dinâmica do canal [24]. Neste caso, esta medida é igual a $S_e = S(\rho_{\text{Eve}}(\tilde{k}(u))) = S(\rho_E) = 0$ porque ρ_E é um estado puro. É possível concluir, então, que sistema e ambiente estão completamente desacoplados.

Para finalizar a caracterização do uso de QEACs em comunicações incondicionalmente seguras, o último passo consiste em caracterizar a capacidade de sigilo no canal.

Teorema 2. *A capacidade de sigilo de um canal* wiretap *quântico com ruído coletivo $\mathcal{E}$, caracterizado como na Definição 2, satisfaz:*

$$C_{S,DFS}(\mathcal{E}) = \max_{\{P\}} \left[\chi^{Bob}\right], \tag{17}$$

em que o máximo é tomado sobre todas as distribuições de probabilidade P sobre $\mathcal{U}$; e χ^{Bob} é a quantidade de Holevo de Bob.

Demonstração. A capacidade de sigilo de um canal quântico arbitrário é dada por (5). Como visto no Lema 1, tem-se que $\chi^{\text{Eva}} = 0$. Este resultado é substituído na referida equação. A igualdade é advinda do Teorema de Holevo-Schumacher-Westmoreland [25], [26]. □

Assim, pode-se concluir que é possível realizar comunicações quânticas seguras por meio de canais wiretap quânticos com ruído coletivo quando os operadores de erro satisfazem alguns critérios de simetria. O critério de segurança incondicional é satisfeito, uma vez que $\chi^{\text{Eve}} = 0$, significando que nenhuma informação foi capturada por Eva e que, portanto, a comunicação foi realizada em *sigilo absoluto*.

A expressão resultante da capacidade de sigilo para os DFS possui relação com os resultados apresentados por Schumacher e Westmoreland [24]. Estes autores mostram que a habilidade de um canal quântico de enviar informação privada pode ser feita tão grande quanto a habilidade de enviar informação coerente. Uma vez que a informação codificada em um DFS não perde coerência, então a sua probabilidade de enviar informação privada é máxima.

IV. Exemplo – Defasamento Coletivo

Para ilustrar os conceitos e resultados apresentados neste artigo, será apresentado um exemplo detalhado de como enviar informações clássicas através de um canal quântico com defasamento coletivo $\mathcal{E}$. Neste canal, os qubits se acoplam ao ambiente de maneira simétrica ao passo que sofrem um processo de defasamento, definido por

$$|0\rangle \to |0\rangle, \qquad |1\rangle \to e^{\imath\phi}|1\rangle. \tag{18}$$

Alice quer enviar mensagens clássicas para Bob por meio deste canal. Porém, Eva o espiona, com acesso total ao ambiente. Se ocorre descoerência, então Eva captura informação sobre a mensagem secreta trocada entre eles.

Para minimizar os efeitos da descoerência, Alice e Bob podem tirar vantagem de uma simetria existente no canal. Se eles codificarem as mensagens utilizando estados imunes à descoerência, Eva não é capaz de descobrir nada a respeito da mensagem trocada. Para tirarem proveito desta simetria, Alice e Bob utilizarão o seguinte esquema de codificação:

$$|0_L\rangle = |01\rangle, \qquad |1_L\rangle = |10\rangle. \tag{19}$$

Um qubit pode, portanto, ser codificado como $|\psi_L\rangle = \alpha|0_L\rangle + \beta|1_L\rangle$. É interessante comprovar que $|\psi_L\rangle$ não sofre os efeitos da descoerência

$$\begin{aligned}
\mathcal{E}(|\psi_L\rangle) &= \mathcal{E}(\alpha|0_L\rangle + \beta|1_L\rangle) && (20)\\
&= \alpha e^{\imath\phi}|01\rangle + \beta e^{\imath\phi}|10\rangle && (21)\\
&= e^{\imath\phi}(\alpha|01\rangle + \beta|10\rangle) && (22)\\
&= e^{\imath\phi}|\psi_L\rangle && (23)\\
&= |\psi_L\rangle. && (24)
\end{aligned}$$

Este resultado é alcançado pois o fator de fase global $e^{\imath\phi}$, adquirido durante o defasamento, não possui significância física. Isto significa que ambos os estados $|01\rangle$ e $|10\rangle$ estão

em $\tilde{\mathcal{H}}$, um DFS do espaço de Hilbert $\mathcal{H}$ no canal quântico com defasamento coletivo.

Supondo, neste exemplo, que as mensagens enviadas por Alice sejam binárias, então $\mathcal{U} = \{0, 1\}$, e a codificação se dará da seguinte forma: $\tilde{k}(0) = |01\rangle$ and $\tilde{k}(1) = |10\rangle$. Logo, $\tilde{K}(\mathcal{U}) = \{|01\rangle, |10\rangle\}$. Assume-se que os bits 0 e 1 são equiprováveis. Assim, Alice escolhe uma mensagem u, a codifica como $\tilde{k}(u)$ e a envia pelo canal.

Uma vez que Alice usou estados do DFS para codificar as mensagens destinadas a Bob, o sistema e o ambiente não interagiram. De acordo com o Lema 1, tem-se que Eva não capturou informação alguma, visto que $\chi^{\text{Eva}} = 0$.

Levando em consideração o estado recebido por Bob, $\rho_{\text{Bob}}(\tilde{k}(u)) = \tilde{k}(u)$, tem-se que a decodificação é trivial e usa os seguintes POVM: $\tilde{\mathcal{D}}_0 = |01\rangle\langle 01|$ e $\tilde{\mathcal{D}}_1 = |10\rangle\langle 10|$.

A quantidade de informação acessível a Bob é limitada pela quantidade de Holevo, dada da seguinte forma:

$$\chi^{\text{Bob}} = S\left(\rho_{\text{Bob}}\tilde{k}(u)\right) - \sum_{u\in\{0,1\}} p_u S\left(\rho_{\text{Bob},u}\right) \quad (25)$$

$$= S\left(\frac{1}{2}|01\rangle\langle 01| + \frac{1}{2}|10\rangle\langle 10|\right) - \frac{1}{2}\cdot 0 - \frac{1}{2}\cdot 0 \quad (26)$$

$$= 1. \quad (27)$$

Utilizando este resultado em (17), é possível concluir que a taxe de sigilo para este cenário é igual a $C_{S,DFS}(\mathcal{E}) = 1$ bit por símbolo por uso do canal. Este exemplo ilustra o envio de informação sigilosa codificada em um DFS via um canal quântico ruidoso com taxa de sigilo positiva utilizando um esquema simples de codificação-decodificação.

V. Considerações Finais

A partir da análise realizada, é possível concluir que existem certas simetrias nos operadores de erro de um canal quântico que podem ser exploradas para enviar informação clássica com segurança incondicional via canais quânticos. Para tanto, é necessário que (i) estes canais sejam caracterizados como na Definição 2; (ii) o espião tenha acesso apenas ao ambiente; e (iii) a codificação entre as partes legítimas seja feita segundo a Definição 3. Com isto, a informação é codificada em um DFS, o que pode ser visto, conforme Lema 1, como uma instância de um código *wiretap* quântico com a particularidade de que nenhuma informação é capturada pelo adversário.

A capacidade de sigilo de tais canais, mostrada em (17), é igual a capacidade clássica de um canal quântico [25], [26]. Este é um caso particular em que a habilidade de um canal quântico para enviar informação secreta pode ser tão grande quanto a capacidade de enviar informação clássica ordinária.

Apesar das vantagens, os resultados apresentados nesse trabalho não podem ser generalizados para todos os canais quânticos devido ao fato de nem todos eles satisfazerem às condições de um DFS. Zanardi e Rasetti [20] afirmam que as condições para um DFS são satisfeitas apenas em cenários onde há descoerência coletiva. Apesar disso, enquanto processos de codificação propostos para *wiretap* favorecem a generalidade, eles não capturam as características particulares e conseqüências que foram observadas neste trabalho para um tipo específico de canal.

Agradecimentos

Os autores agradecem o auxílio financeiro do CNPq e as sugestões dadas por Gilson O. Santos.

Referências

[1] M. Schlosshauer, *Decoherence and the Quantum-to-Classical Transition*, Springer, Ed. Springer, 2007.
[2] D. A. Lidar and K. B. Whaley, "Decoherence-free subspaces and subsystems," arxiv: quantum-ph/0301032v1, 2003.
[3] M. S. Byrd, L.-A. Wu, and D. A. Lidar, "Overview of quantum error prevention and leakage elimination," *Journal of Modern Optics*, vol. 51, no. 16-18, pp. 2449–2460, 2004.
[4] G. Bin, P. ShiXin, S. Biao, and Z. Kun, "Deterministic secure quantum communication over a collective-noise channel," *Science in China Series G: Physics, Mechanics and Astronomy*, vol. 52, no. 12, pp. 1913–1918, 2009.
[5] Q. SuJuan, W. QiaoYan, M. LuoMing, and Z. FuChen, "Quantum secure direct communication over the collective amplitude damping channel," *Science in China Series G: Physics, Mechanics and Astronomy*, vol. 52, no. 8, pp. 1208–1212, 2009.
[6] H.-K. Dong, L. Dong, X.-M. Xiu, and Y.-J. Gao, "A deterministic secure quantum communication protocol through a collective rotation noise channel," *Int. J. of Quantum Inf.*, vol. 8, no. 8, pp. 1389–1395, 2010.
[7] L. Viola, E. M. Fortunato, M. A. Pravia, E. Knill, R. Laflamme, and D. G. Cory, "Experimental realization of noiseless subsystems for quantum information processing," *Science*, vol. 293, pp. 2059–2063, 2001.
[8] A. Beige, D. Braun, B. Tregenna, and P. Knight, "Quantum computing using dissipation to remain in a decoherence-free subspace," *Phys. Rev. Lett.*, vol. 85, p. 1762, 2000.
[9] D. Kielpinski, "A decoherence-free quantum memory using trapped ions," *Science*, vol. 291, p. 1013, 2001.
[10] P. G. Kwiat, A. J. Berglund, J. B. Altepeter, and A. G. White, "Experimental verification of decoherence-free subspaces," *Science*, vol. 290, pp. 498–501, 2000.
[11] U. Dorner, A. Klein, and D. Jaksch, "A quantum repeater based on decoherence free subspaces," *Quant. Inf. Comp.*, vol. 8, p. 468, 2008.
[12] G. Jaeger and A. Sergienko, "Constructing four-photon states for quantum communication and information processing," *Int. J. Theor. Phys.*, vol. 47, p. 2120, 2008.
[13] Y. Xia, J. Song, Z.-B. Yang, and S.-B. Zheng, "Generation of four-photon polarization-entangled decoherence-free states within a network," *Appl. Phys. B*, vol. 99, pp. 651–656, 2010.
[14] P. Xue, "Long-distance quantum communication in a decoherence-free subspace," *Phys. Lett. A*, vol. 372, pp. 6859–6866, 2008.
[15] A. S. Barzegar, "Open quantum systems and error correction," Ph.D. dissertation, University of Southern California, 2009.
[16] D. M. Bacon, "Decoherence, control, and symmetry in quantum computers," Ph.D. dissertation, University of California at Berkeley, 2001.
[17] L.-M. Duan and G.-C. Guo, "Quantum error avoiding codes versus quantum error correcting codes," *Phys. Lett. A*, vol. 255, pp. 209–212, 1999.
[18] A. Shabani and D. Lidar., "Theory of initialization-free decoherence-free subspaces and subsystems," *Phys. Rev. A*, vol. 72, p. 042303, 2005.
[19] M.-D. Choi and D. W. Kribs, "A method to find quantum noiseless subsystems," *Phys. Rev. Lett.*, vol. 96, p. 050501, 2006.
[20] P. Zanardi and M. Rasetti, "Noiseless quantum codes," *Phys. Rev. Lett.*, vol. 79, p. 3306, 1997.
[21] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 1, pp. 1355–1387, 1975.
[22] N. Cai, A. Winter, and R. W. Yeung, "Quantum privacy and quantum wiretap channels," *Problems of Information Transmission*, vol. 40, pp. 318–336, 2004.
[23] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," *IEEE Transactions on Information Theory*, vol. 51, no. 1, pp. 44 –55, 2005.
[24] B. Schumacher and M. Westmoreland, "Quantum privacy and quantum coherence," *Phys. Rev. Lett.*, vol. 80, no. 25, pp. 5695–5697, 1998.
[25] B. Schumacher and M. D. Westmoreland, "Sending classical information via noisy quantum channels," *Phys. Rev. A*, vol. 56, pp. 131–138, 1997.
[26] A. S. Holevo, "The capacity of the quantum channel with general signal states," *IEEE Trans. Info. Theory*, vol. 4, no. 1, pp. 269–273, 1998.