Unconditionally Secure Quantum Communications via Decoherence-Free Subspaces

Elloá B. Guedes and Francisco M. de Assis

***Abstract*— We show how to use decoherence-free subspaces over collective-noise quantum channels to convey classical information in perfect secrecy. We argue that codes defined over decoherence-free subspaces are codes for quantum wiretap channels in which the gain of information by a non-authorized third part is zero. 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. As a consequence of these results, we show how some protocols for secure communication can be simplified, reducing significantly the number of communications performed.**

***Keywords*— Decoherence-free subspaces, Quantum wiretap channels, Unconditional Security.**

I. INTRODUÇÃO

PREVENIR erros na informação quântica é um dos principais objetivos da Teoria Quântica da Informação. Erros surgem do acoplamento entre um sistema de interesse o ambiente, em função da subsequente *descoerência* induzida por este acoplamento. Considerando a natureza frágil dos sistemas quânticos, a descoerência é tida como o principal obstáculo na transmissão de informação coerente [1].

No contexto das Comunicações Quânticas, a descoerência é responsável pelo *vazamento* da informação para o ambiente em um canal quântico ruidoso. Se mensagens secretas são transmitidas por este canal, pelo menos parte delas pode ser capturadas por um receptor não-autorizado, aqui chamado de *espião*. Esta situação é indesejada e, em um cenário criptográfico, deve ser evitada.

Cai et al. [2] e Devetak [3] modelaram este cenário por meio dos chamados *canais wiretap quânticos*. Eles também estabeleceram as condições para realizar a troca de informações clássicas por canais quânticos sem que o conteúdo das mensagens fosse descoberto por um espião. Nesta formulação, apenas são considerados adequados códigos que minimizem a probabilidade de erro de decodificação entre os participantes legítimos ao passo que maximizem a equivocação de um espião. Apesar disso, a taxa máxima em que estas comunicações secretas podem acontecer, a chamada *capacidade quântica de sigilo*, é usualmente menor que a capacidade ordinária para envio de informação clássica neste mesmo canal.

Para minimizar a descoerência, diversos métodos foram propostos, tais como códigos corretores de erros quânticos (QECC – *Quantum Error-Correcting Codes*), desacoplamento dinâmico, subespaços livres de descoerência (DFS – *Decoherence-Free Subspaces*), dentre outros [4]. Em se tratando dos DFS, em particular, se os operadores de erro que afetam os qubits possuírem algumas simetrias, então estes qubits irão sofrer o mesmo tipo de erro ao passarem pelo canal quântico. Em alguns casos, isto fará com que determinados estados sejam invariantes ao erro, significando que a descoerência não ocorre em determinados subespaços [5]. Desta maneira, verifica-se um potencial no uso destes subespaços para a construção de códigos que minimizem o vazamento da informação para o ambiente.

Nos dias atuais, alguns trabalhos na literatura já exploram o potencial dos DFS nas Comunicações Quânticas. Estes trabalhos consistem de protocolos contra certo tipo de ruído coletivo (a exemplo de rotação, defasamento, amortecimento de amplitude) e consideram o uso de DFS pequenos (com dois ou três qubits, por exemplo) [6]-[10]. Até mesmo realizações experimentais já foram construídas objetivando o processamento da informação quântica [11]-[14]. Na perspectiva destes trabalhos, a proteção da informação significa evitar a perda de coerência, mantendo a fidelidade dos estados quânticos.

Neste artigo, serão investigadas consequências mais gerais do uso de DFS em Comunicações Quânticas. Em particular, considerando a perspectiva da *troca segura de mensagens*. Para tanto, será apresentada uma definição formal de canais quânticos que satisfazem aos critérios de simetria para a existência de DFS, posteriormente serão definidos códigos sobre estes subespaços e, por fim, serão estabelecidas as condições para a realização de comunicações sigilosas.

A partir de uma análise formal realizada, foi possível concluir que os códigos definidos sobre os DFS também são códigos adequados para os canais *wiretap* quânticos. Isto significa que a utilização de DFS possibilita a realização de comunicações quânticas incondicionalmente seguras. Mais além, foi verificado que a capacidade de sigilo neste cenário iguala-se à capacidade para envio de informação clássica ordinária. Este é um caso particular em que a capacidade de sigilo é máxima.

Elloá B. Guedes - Escola Superior de Tecnologia, Universidade do Estado do Amazonas, Manaus, Amazonas Brasil, elloaguedes@gmail.com

Francisco M. de Assis - Centro de Engenharia Elétrica e Informática, Universidade Federal de Campina Grande, Campina Grande, Paraíba, Brasil, fmarassis@gmail.com

Após a apresentação destes resultados, serão exploradas algumas implicações resultantes em determinados protocolos para comunicação quântica segura direta e para comunicação quântica segura determinística. Alguns autores apresentaram estratégias para comunicações seguras sobre canais quânticos com ruído coletivo via DFS, mas o esforço requerido por alguns destes protocolos para checagem de espionagem aumenta significativamente o número de operações a serem implementadas, bem como o número de qubits trocados. Em face dos novos resultados sobre segurança incondicional e DFS, serão sugeridas simplificações nestes protocolos que diminuem a complexidade de implementá-los e também que reduzem substancialmente o número de comunicações realizadas.

O artigo está organizado como segue. As condições para privacidade quântica, estabelecidas por Schumacher e Westmoreland [15], serão apresentadas na Seção II. Os conceitos dos canais *wiretap* quânticos serão recapitulados na Seção III. Os fundamentos em DFS serão introduzidos na Seção IV. As contribuições sobre o uso de DFS para a realização de comunicações incondicionalmente seguras serão apresentadas na Seção V. Na seção VI, será mostrado um exemplo detalhado de como enviar informação secreta utilizando DFS. Os impactos dos resultados obtidos na simplificação de alguns protocolos existentes serão mostrados na Seção VII. Por fim, as considerações finais serão apresentadas na Seção VIII.

II. Privacidade Quântica

Suponha que um emissor (Alice) prepare um sistema quântico B em um estado inicial ρ. O objetivo de Alice é enviá-lo a um receptor (Bob) por meio de um canal quântico ruidoso, denotado pelo superoperador $\mathcal{E}^B$. Desta maneira, o estado recebido por Bob é $\rho_{\text{Bob}} = \mathcal{E}^B(\rho)$.

Devido à presença do ruído, para prover uma descrição unitária da evolução de ρ_{Bob} ao longo do canal, é necessário considerar a interação com o ambiente, que é assumido iniciar em um estado puro $|0_E\rangle$. Neste caso, o superoperador é dado por

$$\mathcal{E}^B(\rho) \quad = \quad Tr_E U^{BE} \left(\rho \otimes |0_{\text{E}}\rangle \langle 0_{\text{E}}|\right) U^{BE\dagger} \qquad (1)$$

em que U^{BE} representa a operação unitária de interação.

A *troca de entropia*, denotada por S_e, é definida como uma medida da informação trocada entre o sistema B e o ambiente E durante o período de interação. Considerando que o ambiente inicia em um estado puro, a troca de entropia é dada por $S_e = S(\rho_E)$, em que ρ_E é o estado final do ambiente. A troca de entropia é determinada inteiramente pelo estado inicial ρ de B e pela dinâmica do superoperador $\mathcal{E}^B$, isto significa que a troca de entropia é uma propriedade "intrínseca" ao sistema B e à sua dinâmica [15].

Suponha que Alice esteja usando o canal quântico para enviar informações clássicas para Bob. Alice então prepara o ρ_k

p_k

sistema quântico B em um dos possíveis estados com probabilidades *a priori* . O estado ρ enviado por Alice pode ser denotado por uma média

$$\rho = \sum_k p_k \rho_k \qquad (2)$$

Bob obtém o k-ésimo estado como sendo $\rho_{\text{Bob},k} = \mathcal{E}^B(\rho_k)$. Uma vez que $\mathcal{E}^B$ é linear, a média do estado recebido por Bob é

$$\rho_{\text{Bob}} \quad = \quad \sum_k p_k \cdot \mathcal{E}^B(\rho_k) \qquad (3)$$

$$= \quad \mathcal{E}^B(\rho) \qquad (4)$$

Para decodificar a mensagem recebida, Bob realiza uma medição utilizando algum *observável de decodificação*. A quantidade de informação clássica transmitida de Alice para Bob, denotada por $\mathbf{H}_{\text{Bob}}$, é governada pela quantidade de Holevo χ^{Bob}, definida como

$$\chi^{\text{Bob}} = S(\rho_{\text{Bob}}) - \sum_k p_k S\left(\rho_{\text{Bob},k}\right) \qquad (5)$$

Algumas considerações sobre a quantidade de Holevo neste cenário devem ser mencionadas: (*i*) $\mathbf{H}_{\text{Bob}} \leq \chi^{\text{Bob}}$ independente do observável de decodificação escolhido; e (*ii*) $\mathbf{H}_{\text{Bob}}$ pode ser arbitrariamente próxima de χ^{Bob} por meio de uma escolha adequada de um código e de um observável de decodificação. Neste caso, χ^{Bob} representa um limitante superior para a informação clássica transmitida de Alice para Bob.

Ao considerar os fins criptográficos do canal, então é estabelecido que uma espiã (Eve) deve ter acesso a alguma parte ou a todo o ambiente E com o qual B interage. O superoperador de evolução $\mathcal{E}^B$ descreve todos os efeitos da espiã no canal ou, em outras palavras, todos os esforços para a espionagem de Alice e Bob estão contidos no operador de interação U^{BE}. Desta maneira, a informação acessível à Eve, denotada por $\mathbf{H}_{\text{Eve}}$, será limitada por

$$\chi^{\text{Eve}} = S(\rho_{\text{Eve}}) + \sum_k p_k S(\rho_{\text{Eve},k}) \qquad (6)$$

A desigualdade $\mathbf{H}_{\text{Eve}} \leq \chi^{\text{Eve}}$ é verdadeira quer Eve tenha acesso total ou não ao ambiente.

A *privacidade quântica* é definida como

$$P = \mathbf{H}_{\text{Bob}} - \mathbf{H}_{\text{Eve}} \qquad (7)$$

Alice e Bob desejam maximizar P ao máximo possível. Mas, eles também devem assumir que a espiã está adquirindo o máximo de informação disponível. A *privacidade garantida*, $P_G = \inf P$, é o ínfimo sobre todas as possíveis estratégias adoptadas por Eve. Uma vez que $\mathbf{H}_{\text{Eve}} \leq \chi^{\text{Eve}}$, então $P_G \geq \mathbf{H}_{\text{Bob}} - \chi^{\text{Eve}}$. Por outro lado, Alice e Bob desejam usar

o canal de modo que tornem a privacidade garantida P_G tão grande quanto o possível. Seja $\mathcal{P} = \sup P_G$. O melhor esquema que Alice e Bob podem utilizar aproxima $\mathbf{H}_{\text{Bob}}$ de χ^{Bob}. Desta maneira, é possível denotar $\mathcal{P}$ como

$$\mathcal{P} = \chi^{\text{Bob}} - \chi^{\text{Eve}} \tag{8}$$

Apesar da caracterização da privacidade quântica, é necessário estabelecer esquemas que descrevam como Alice e Bob devem proceder para estabelecer as propriedades necessárias para a realização de comunicações seguras mesmo na presença da espiã. Estes aspectos serão discutidos na próxima seção.

III. CANAIS *WIRETAP* QUÂNTICOS

Na tentativa de prover uma descrição das propriedades do canal para estabelecer comunicações secretas sem possibilitar a descoberta de informações por um espião, Cai et al. [2] e Devetak [3] simultaneamente definiram os *canais wiretap quânticos*, cuja formalização é apresentada a seguir.

Definição 1. *Um canal wiretap quântico sem memória é descrito por um par de superoperadores $\mathcal{E}^B$ e $\mathcal{E}^E$ de um espaço de Hilbert complexo $\mathcal{H}$. Quando Alice envia um estado quântico ω de $\mathcal{H}^{\otimes n}$, Bob re$\mathcal{E}^{\otimes n,B}(\omega)$ e Eve $\mathcal{E}^{\otimes n,E}(\omega)$ recebe , em que n é a dimensão do espaço de Hilbert de entrada.*

Os códigos utilizados pelos participantes legítimos da comunicação são caracterizados na Definição 2.

Definição 2. *Um conjunto de palavras código de comprimento n $(n = dim(\mathcal{H}))$ para um conjunto $\mathcal{U}$ de mensagens clássicas é um conjunto de estados de entrada rotulados por mensagens em $\mathcal{U}$, $\Omega(\mathcal{U}) = \{\omega(u) : u \in \mathcal{U}\}$, e uma decodificação de medição de comprimento n com saída em $\mathcal{U}$, i.e., um conjunto de operadores $\mathcal{D}_u$, $u \in \mathcal{U}$ com $\sum_{u\in\mathcal{U}} \mathcal{D}_u \leq \mathbb{1}$. O par $(\Omega(\mathcal{U}), \{\mathcal{D}_u : u \in \mathcal{U}\})$ é chamado de um código de comprimento n para o conjunto de mensagens $\mathcal{U}$. A taxa deste código é $\frac{1}{n}\log|\mathcal{U}|$.*

De acordo com ambas as definições apresentadas, a Figura 1 ilustra os procedimentos requeridos para o cenário quântico. Alice deve criar um estado $\omega(u)$ quando desejar enviar uma mensagem $u \in \mathcal{U}$ para Bob. Devido ao ruído, Bob recebe $\mathcal{E}^{\otimes n,B}(\omega(u)) = Tr_E\left[\mathcal{E}^{\otimes n}(\rho \otimes |0_E\rangle\langle 0_E|\right]$ e realiza a decodificação da mensagem original utilizando um POVM (*Positive Operator-Value Measurement*) $\{\mathcal{D}_u : u \in \mathcal{U}\}$, que resulta em uma estimativa u' para u. A espiã Eve, por sua vez, recebe o estado $\mathcal{E}^{\otimes n,E}(\omega(u)) = Tr_B\left[\mathcal{E}^{\otimes n}(\rho \otimes |0_E\rangle\langle 0_E|\right]$ e irá tentar obter o máximo possível de informação sobre a mensagem originalmente enviada por Alice. Para tanto, ela irá tentar construir um POVM baseando-se na tipicalidade dos estados que recebe do canal, seguindo uma estratégia apresentada em [2, Sec. 4].

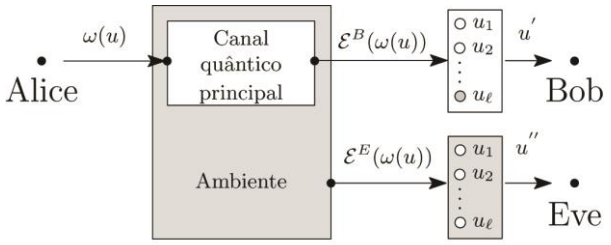

Figura 1. Idéia geral do canal *wiretap* quântico.

Entretanto, embora a estratégia de comunicação tenha sido detalhada, os argumentos de segurança sobre a troca de mensagens ainda não foram definidos. É necessário garantir uma baixa probabilidade de erro na decodificação entre os Alice e Bob, ao passo que Eve não aprende praticamente nada a respeito da mensagem secreta que passou pelo canal. A formalização destes dois requisitos é satisfeita pelos códigos da Definição 3.

Definição 3. *(Código Wiretap) Um código $(\Omega(\mathcal{U}), \{\mathcal{D}_u : u \in \mathcal{U}\})$ de comprimento n é chamado um código wiretap com parâmetros $(n, |\mathcal{U}|, \lambda, \mu)$ se, para $\lambda, \mu > 0$*

$$P_e = 1 - \frac{1}{|\mathcal{U}|}\sum_{u\in\mathcal{U}} Tr_E\left[\mathcal{E}^{\otimes n,B}(\omega(u))\mathcal{D}_u\right] \leq \lambda \tag{9}$$

e

$$\frac{1}{n}\left[S\left(\sum_{u\in\mathcal{U}}\frac{1}{|\mathcal{U}|}\mathcal{E}^{\otimes n,E}(\omega(u))\right) - \sum_{u\in\mathcal{U}}\frac{1}{|\mathcal{U}|}S\left(\mathcal{E}^{\otimes n,E}(\omega(u))\right)\right] < \mu \tag{10}$$

em que $\frac{1}{n}\log|\mathcal{U}|$ é a taxa deste código.

Na definição de um código com parâmetros $(n, |\mathcal{U}|, \lambda, \mu)$, a Eq. (9) garante que a probabilidade média de erro na decodificação por Bob é menor que um parâmetro λ, e a Eq. (10) limita a informação media acessível por Eve, de tal maneira que esta não captura praticamente nada a respeito da mensagem secreta enviada por Alice.

Por fim, a *capacidade quântica de sigilo* é definida.

Definição 4. *(Capacidade Quântica de Sigilo [2]) A capacidade de sigilo de um canal quântico é o maior número real C_S tal que para todo $\epsilon, \lambda, \mu > 0$ e n suficientemente grande, existe um código $(n, |\mathcal{U}|, \lambda, \mu)$ com*

$$C_S < \frac{1}{n}\log|\mathcal{U}| + \epsilon \tag{11}$$

Apesar das definições anteriores assumirem mensagens uniformemente distribuídas, o seguinte teorema de [2, Sec. 5] sobre a capacidade quântica de sigilo é um resultado mais geral.

Teorema 1. *Para um canal wiretap quântico $\mathcal{E}$ como caracterizado na Definição 1, a capacidade quântica de sigilo satisfaz*

$$C_S(\mathcal{E}) \geq \max_{\{P\}} \left[\chi^{\text{Bob}} - \chi^{\text{Eve}}\right] \quad (12)$$

em que o máximo é tomado sobre todas as distribuições de probabilidade sobre $\mathcal{U}$; e χ^{Bob} e χ^{Eve} são as quantidades de Holevo dadas nas Eqs. (5) e (6), respectivamente.

A capacidade quântica de sigilo pode ser compreendida como a capacidade de um canal quântico para enviar informação clássica em sigilo absoluto. Esta capacidade é equivalente ao supremo da privacidade garantida definida na Eq. (8).

A capacidade de sigilo definida na Eq. (12) é o análogo quântico da capacidade de sigilo clássica proposta por Wyner [16]. É possível verificar algumas similaridades entre ambas as definições: as duas limitam a probabilidade de erro na decodificação e também a informação que deve ser acessível por um espião. Entretanto, o caso quântico utiliza-se de medidas de informação próprias deste domínio, tais como a entropia de von Neumann e a quantidade de Holevo. Uma característica particular da capacidade quântica de sigilo é que esta não possui uma caracterização de letra isolada, significando que a mesma não é computável por considerar todos os possíveis estados de entrada e todas as possíveis distribuições sobre eles [2], [3].

IV. Subespaços Livres de Descoerência

Devido à descoerência, um sistema quântico decai para um estado de baixa energia em função das perdas sofridas para o ambiente, tem sua fase desvanecida e, por fim, a informação que armazenava é perdida [17].

Seja um sistema quântico fechado composto por um *sistema de interesse* S e pelo *ambiente* E. O hamiltoniano que descreve este sistema é definido como segue

$$\mathbb{H} = \mathbb{H}_S \otimes \mathbb{1}_E + \mathbb{1}_S \otimes \mathbb{H}_E + \mathbb{H}_{SE} \quad (13)$$

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

Para prevenir erros, seria ideal que $\mathbb{H}_{SE}$ fosse igual a zero, indicando que o sistema e o ambiente estão desacoplados e evoluem independentemente e unitariamente de acordo com seus respectivos hamiltonianos $\mathbb{H}_S$ e $\mathbb{H}_E$ [5]. Porém, em cenários práticos, esta situação ideal não é possível, uma vez que limitações tecnológicas impedem a construção de um sistema completamente livre de ruído. Assim, após isolar o sistema da melhor maneira possível, o adequado é vislumbrar objetivos realísticos para identificar e corrigir erros quando eles ocorrerem, evitar o ruído quando possível, ou então até mesmo tentar suprimir o ruído do sistema [4].

Se algumas simetrias existirem na interação entre sistema e ambiente, então é possível encontrar "locais seguros" no espaço de Hilbert do sistema que não sofrem os efeitos da descoerência. Seja $\{A_i(t)\}$ um conjunto de operadores na representação da soma de operadores (OSR – *Operator-Sum Representation*) correspondendo à evolução do sistema. Diz-se que a matriz densidade ρ_S é *invariante* perante os operadores OSR $\{A_i(t)\}$ se $A_i(t)\rho_S A_i^\dagger(t) = \rho_S$. Levando isto em consideração, é possível definir os subespaços livres de descoerência, cujos estados são invariantes apesar da existência de um acoplamento não-trivial entre sistema de interesse e ambiente.

Definição 5. *(Subespaço Livre de Descoerência [16]) Um subespaço $\tilde{\mathcal{H}}$ de um espaço de Hilbert $\mathcal{H}$ é chamado DFS em relação ao acoplamento entre sistema e ambiente se cada estado puro deste subespaço é invariante perante a correspondente evolução OSR para qualquer condição inicial do ambiente, isto é*

$$\sum_i A_i(t)|\tilde{k}\rangle\langle\tilde{k}|A_i^\dagger(t) = |\tilde{k}\rangle\langle\tilde{k}|, \forall|\tilde{k}\rangle\langle\tilde{k}| \in \tilde{\mathcal{H}}, \forall\rho_E(0) \quad (14)$$

Apesar da definição de DFS apresentada ter sido feita em termos de estados puros, um estado emaranhado que tenha suporte apenas em estados puros de um DFS também será invariante e, portanto, protegido da descoerência [18].

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*) e as tarefas de perturbação e recuperação nestes códigos são triviais [19].

Seja o hamiltoniano da interação sistema-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 do ambiente, respectivamente. Considera-se que os operadores do ambiente $\mathbf{E}_j$ são linearmente independentes. As simetrias requeridas para a existência de DFS são descritas no teorema a seguir. Para um prova detalhada ou diferentes formulações ver [5, Sec. 5].

Teorema 2. *(Condições para DFS) Um subespaço $\tilde{\mathcal{H}}$ é um DFS se, e somente se, os operadores do sistema $\mathbf{S}_j$ atuarem proporcionalmente à identidade neste subespaço*

$$\mathbf{S}_j|\tilde{k}\rangle = c_j|\tilde{k}\rangle \quad \forall j, |\tilde{k}\rangle \in \tilde{\mathcal{H}} \quad (15)$$

Na prática, identificar uma simetria útil e tirar proveito dela pode ser uma tarefa bastante difícil. Isto acontece porque é necessário (*i*) identificar a simetria; (*ii*) encontrar estados que sejam invariantes a interação e, por fim, (*iii*) construir, se possível, operações no sistema que preservem as simetrias necessárias. Apesar destas dificuldades, quando comparados aos QECCs, por exemplo, os DFS possuem algumas vantagens, a exemplo de frequentemente requererem menos qubits físicos para representar um qubit lógico e também de

não demandarem uma repetida identificação e correção de erros [4].

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 após a sua ocorrência, QEACs não possuem a habilidade de corrigir erros, uma vez que os previnem; QECCs adotados em cenários práticos pertencem a classe dos códigos não-degenerados, enquanto QEACs são códigos altamente degenerados; QEACs possuem distância infinita, enquanto os QECCs não-degenerados possuem distância infinita. Em particular, se a degenerescência atinge o máximo, um QECC se reduz a um QEAC, o que ilustra a circunstância em que um tipo de código torna-se equivalente ao outro [19].

A ausência de descoerência em DFS têm se mostrado de grande importância para implementações de memórias quânticas e algoritmos quânticos. Outras aplicações incluem codificação da informação em pontos quânticos, dissipação coletiva, redução de ruído, dentre outros [4], [5].

V. DFS em Comunicações Seguras

A partir de agora serão consideradas as aplicações dos DFS nas Comunicações Quânticas. Será considerado como referência o modelo de *canais quânticos com ruído coletivo*, i.e., um modelo de canal no qual os qubits se acoplam identicamente ao mesmo ambiente, ao passo que sofrem defasamento e dissipação [20]. Apesar de não ser um modelo abrangente, este caso especial traz à tona algumas consequências particulares do uso de DFS em comunicações quânticas. O foco a ser considerado, em particular, será nos aspectos da *troca segura de mensagens*.

Considera-se o caso em que Alice quer enviar mensagens clássicas secretas para Bob por um canal quântico. Estas mensagens devem ser protegidas da espiã Eve, que tem acesso total ao ambiente. O canal entre Alice e Bob possui um subespaço livre de descoerência que será utilizado para codificar as mensagens secretas. A definição a seguir caracteriza este canal quântico.

Definição 6. *(Canal Wiretap Quântico com Ruído Coletivo) Um canal wiretap quântico com ruído coletivo $\mathcal{E}$ é um canal como na Definição 1, mas cuja decomposição de Kraus $\{A_i\}$ satisfaz o Teorema 2.*

Nesta definição, uma vez que $\{A_i\}$ satisfaz ao Teorema 2, então o canal $\mathcal{E}$ possui um DFS $\tilde{\mathcal{H}}$. Quando Alice deseja enviar um estado para Bob, ela o faz pelo canal quântico e este estado interage com o ambiente. Bob recebe o estado resultante do traço parcial sobre o ambiente. A espiã Eve, por sua vez, captura o que vazou para o ambiente.

Sem perda de generalidade, será considerado aqui que o ambiente inicia em um estado puro $|0_E\rangle\langle 0_E|$. Esta é uma hipótese plausível, pois sempre é possível imaginar que um ambiente "local" em um estado misto é apenas parte de um sistema maior em um estado puro emaranhado [15].

O passo seguinte é definir o QEAC sobre $\tilde{\mathcal{H}}$ para codificar as mensagens entre Alice e Bob.

Definição 7. *Seja $\tilde{\mathcal{H}}$ um DFS gerado por um conjunto de autovetores $\{|\tilde{k}\rangle\}$, i.e., $\tilde{\mathcal{H}} = Span[\{|\tilde{k}\rangle\}]$. Um conjunto de palavras código de comprimento n $(n = dim(\tilde{\mathcal{H}}))$ para um conjunto $\mathcal{U}$ de mensagens clássicas 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 medição trivial composto por um conjunto POVM $\tilde{\mathcal{D}}_u$, $u \in \mathcal{U}$ com a restrição $\sum_{u\in\mathcal{U}} \tilde{\mathcal{D}}_u \leq \mathbb{1}$. 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 $\frac{1}{n}\log|\mathcal{U}|$.*

Utilizando o código definido, se Alice deseja enviar a mensagem u para Bob, ela deve codifica-la no QEAC definido sobre $\tilde{\mathcal{H}}$, $\tilde{k}(u)$ndo . Quando ela envia o estado resultante pelo canal, este interage com o ambiente. Bob então recebe $\rho_{\text{Bob}}(\tilde{k}(u))$ e Eve recebe $\rho_{\text{Eve}}(\tilde{k}(u))$, os quais são dados por

$$\rho_{\text{Bob}}(\tilde{k}(u)) = \text{Tr}_{\text{E}}\left[\mathcal{E}^{\otimes n}(\tilde{k}(u)\otimes|0_E\rangle\langle 0_E|)\right] \quad (16)$$

$$\rho_{\text{Eve}}(\tilde{k}(u)) = \text{Tr}_{\text{B}}\left[\mathcal{E}^{\otimes n}(\tilde{k}(u)\otimes|0_E\rangle\langle 0_E|)\right] \quad (17)$$

Uma vez que Alice utilizou um QEAC como na Definição 7, então a simetria dinâmica existente protegeu a informação quântica 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

$$\rho_{\text{Bob}}(\tilde{k}(u)) = \text{Tr}_{\text{E}}\left[\mathcal{E}^{\otimes n}(\tilde{k}(u)\otimes|0_E\rangle\langle 0_E|)\right] \quad (18)$$

$$= \text{Tr}_{\text{E}}\left[\sum_i A_i\left(\tilde{k}(u)\otimes|0_E\rangle\langle 0_E|\right)A_i^\dagger\right] \quad (19)$$

$$= \text{Tr}_{\text{E}}\left[\tilde{k}(u)\otimes\rho_E\right] \quad (20)$$

$$= \tilde{k}(u) \quad (21)$$

em que a Eq. (20) deve-se à invariância dos estados do DFS perante os operadores OSR. Levando em consideração o hamiltoniano dado na Eq. (13) e o fato do sistema de interesse e do ambiente não terem interagido, este é o caso em que o ambiente sofreu apenas a ação de $\mathbb{H}_E$, indicando uma evolução unitária restrita ao ambiente. Isto significa que $\rho_{\text{Eve}}(\tilde{k}(u)) = \rho_E$ é um estado puro.

O lema a seguir formaliza como o QEAC protege a informação transmitida pelo canal da atuação de um espião.

Lema 1. *Um QEAC como na Definição 7 sobre um canal wiretap quântico com ruído coletivo, como na Definição 6, é um código wiretap com parâmetros $(n, |\mathcal{U}|, \lambda, \mu)$.*

Prova. A prova é feita de maneira direta, mostrando como o QEAC satisfaz aos critérios das Eqs. (9) e (10).

Primeiro será analisada a probabilidade de erro na decodificação. Uma vez que $\tilde{k}(u)$ pertence a $\tilde{\mathcal{H}}$, sabe-se que este estado não interagiu com o ambiente. Então, $\rho_{\text{Bob}} = \tilde{k}(u)$ como mostrado nas Eqs. (18)-(21). Verifica-se que o processo de decodificação é trivial e que a mensagem enviada por Alice pode ser perfeitamente recuperada, visto que há um operador de decodificação $\tilde{\mathcal{D}}_u$ para cada $u \in \mathcal{U}$. É possível concluir, portanto, que há uma probabilidade desprezível de erro na decodificação por Bob. Logo, o critério da Eq. (9) é satisfeito.

Prossegue-se para a análise do critério da Eq. (10). É interessante verificar que esta equação representa a média da informação acessível por Eve, a qual é limitada pela quantidade de Holevo definida na Eq. (6). A quantidade de Holevo será obtida primeiramente.

Apesar do estado final do ambiente ρ_E (vide Eq. (20)) não ser conhecido, o fato de Alice e Bob terem utilizado apenas estados de um DFS garantiu que o hamiltoniano de interação $\mathbb{H}_{SE}$ não governou a evolução conjunta entre sistema de interesse e ambiente. Ao contrário, é possível garantir que cada sistema evoluiu de maneira completamente unitária de acordo com seu próprio hamiltoniano, o que implica que o ambiente apenas sofreu a atuação de $\mathbb{H}_E$. No contexto em questão, isto significa que o ambiente terminou em um estado puro. Utilizando este resultado para calcular a quantidade de Holevo, tem-se

$$\chi^{\text{Eve}} = S(\rho_{\text{Eve}}(\tilde{k}(u))) - \sum_k p_k S(\rho_{\text{Eve},k}\tilde{k}(u)) \quad (22)$$

$$= S(\rho_E) - \sum_k p_k S(\rho_{\text{Eve},k}\tilde{k}(u)) \quad (23)$$

$$= 0 - \sum_k p_k S(\rho_{\text{Eve},k}\tilde{k}(u)) \quad (24)$$

Um fato conhecido sobre a quantidade de Holevo é que $\chi^{\text{Eve}} \geq 0$. Uma vez que $S(\rho) \geq 0$ para qualquer ρ, e que $p_k \geq 0$ para todo k, então este é o caso que o termo remanescente é igual a zero. Portanto, $\chi^{\text{Eve}} = 0$.

Dado que a quantidade de Holevo é um limitante superior para a informação acessível, este é o caso em que a Eq. (10) também é igual a zero. Este resultado significa que a quantidade de informação capturada por Eve não pôde reduzir a incerteza sobre a mensagem secreta u enviada de Alice para Bob – implicando em *sigilo absoluto*, um requisito essencial para códigos *wiretap*. Isto conclui a prova. ■

Outra medida de informação que enfatiza a ausência de interação entre sistema e ambiente é a troca de entropia, cuja medida é determinada inteiramente pelo estado inicial de B e pela dinâmica do canal [15]. Neste caso, esta medida é igual a $S_e = S(\rho_{\text{Eve}}(\tilde{k}(u))) = S(\rho_E) = 0$, uma vez que ρ_E é um estado puro. Assim é possível reforçar a conclusão que sistema e ambiente evoluíram de maneira completamente desacoplada.

Por fim, parte-se para a caracterização da capacidade de sigilo de um canal *wiretap* quântico com ruído coletivo.

Teorema 3. *A capacidade de sigilo de uma canal wiretap quântico com ruído coletivo $\mathcal{E}$, caracterizado na Definição 6, satisfaz*

$$C_{S,\text{DFS}}(\mathcal{E}) = \max_{\{P\}} \left[\chi^{\text{Bob}}\right] \quad (25)$$

em que o máximo é tomado sobre todas as distribuições de probabilidade P sobre $\mathcal{U}$; e χ^{Bob} é a quantidade de Holevo dada na Eq. (5).

Prova. Seja um QEAC $(\tilde{K}(\mathcal{U}), \{\tilde{\mathcal{D}}_u : u \in \mathcal{U}\})$ utilizado no canal $\mathcal{E}$. Como visto no Lema 1, este é um código *wiretap*. Um fato verificado na prova deste lema foi que a quantidade de Holevo de Eve $\chi^{\text{Eve}} = 0$. Primeiro substitui-se este resultado na Eq. (12). A igualdade final é advinda como consequência do Teorema de Holevo-Schumacher-Westmoreland [21], que afirma que a taxa de um código deve ser limitada pela quantidade de Holevo. ■

Pode-se concluir, então, que é possível realizar comunicações quânticas com sigilo absoluto em canais quânticos espionados desde que os operadores de erro satisfaçam algumas simetrias. O critério de segurança incondicional é satisfeito, uma vez que $\chi^{\text{Eve}} = 0$.

A expressão resultante da capacidade de sigilo de um DFS possui relação com resultados apresentados por Schumacher e Westmoreland [15]. Estes autores argumentam que a habilidade de um canal quântico de enviar informação privada é pelo menos tão grande quanto a habilidade de enviar informação coerente. Uma vez que a informação codificada em um DFS não perde coerência, então a capacidade de enviar informação privada é maximizada, particularmente quando comparada a outros tipos de canais quânticos.

VI. Exemplo – Defasamento Coletivo

Para ilustrar os resultados descritos neste artigo, nesta seção será mostrado um exemplo detalhado do envio sigiloso de informação clássica por um canal quântico com defasamento coletivo $\mathcal{E}$. Neste modelo de canal, os qubits se acoplam ao ambiente de maneira simétrica ao passo que sofrem defasamento, definido como:

$$|0\rangle \rightarrow |0\rangle \quad (26)$$

$$|1\rangle \rightarrow e^{\imath\phi}|1\rangle \quad (27)$$

Alice deseja enviar mensagens clássicas secretas para Bob, porém Eve espiona o canal com acesso total ao ambiente. Se há descoerência, então é possível que Eve adquira alguma

informação acerca da mensagem secreta trocada entre Alice e Bob.

Para contornar os efeitos da descoerência, Alice e Bob podem tirar proveito de uma simetria existente no canal. Se eles codificarem as mensagens utilizando estados imunes à descoerência, então Eve não irá capturar nada a respeito das mensagens secretas. Para tanto, Alice e Bob utilizarão o seguinte esquema de codificação

$$|0_L\rangle = |01\rangle \quad (28)$$
$$|1_L\rangle = |10\rangle \quad (29)$$

Um qubit pode, portanto, ser codificado como $|\psi_L\rangle = \alpha|0_L\rangle + \beta|1_L\rangle$. É possível constatar que $|\psi_L\rangle$ não sofre os efeitos da descoerência ao passar pelo canal

$$\begin{aligned}\mathcal{E}(|\psi_L\rangle) &= \mathcal{E}(\alpha|0_L\rangle + \beta|1_L\rangle) && (30)\\ &= \alpha e^{\imath\phi}|01\rangle + \beta e^{\imath\phi}|10\rangle && (31)\\ &= e^{\imath\phi}(\alpha|01\rangle + \beta|10\rangle) && (32)\\ &= e^{\imath\phi}|\psi_L\rangle && (33)\\ &= |\psi_L\rangle && (34)\end{aligned}$$

porque o fator de fase global $e^{\imath\phi}$ adquirido durante o processo de defasamento não possui significância física. Isto significa que ambos os estados $|01\rangle$ e $|10\rangle$ pertencem a $\tilde{\mathcal{H}}$, um DFS do espaço de Hilbert $\mathcal{H}$ no canal quântico de defasamento coletivo.

Neste exemplo, as mensagens enviadas por Alice são binárias, logo $\tilde{K}(\mathcal{U}) = \{|01\rangle, |10\rangle\}$. Fazendo uso deste código, para enviar a mensagem u, Alice a codifica no estado correspondente $\tilde{k}(u)$, o qual será enviado pelo canal. Assume-se aqui que os bits 0 e 1 são equiprováveis e que o ambiente inicia no estado puro $|0_E\rangle\langle 0_E|$.

Dado que Alice utilizou estados do DFS para codificar mensagens para Bob, o sistema de interesse e o ambiente não interagiram. Como já provado anteriormente, Eve não captura qualquer informação a respeito da mensagem secreta.

Em relação a Bob, de acordo com o esquema caracterizado, o estado recebido $\rho_{\text{Bob}}(\tilde{k}(u))$ é dado por

$$\begin{aligned}\rho_{\text{Bob}}(\tilde{k}(u)) &= \text{Tr}_{\text{E}}\left[\mathcal{E}^{\otimes n}(\tilde{k}(u)\otimes|0_E\rangle\langle 0_E|)\right] && (35)\\ &= \tilde{k}(u) && (36)\end{aligned}$$

Para decodificar a mensagem recebida, Bob deve seguir as instruções do QEAC na Definição 7, devendo construir os projetores POVM $\tilde{\mathcal{D}}_0 = |01\rangle\langle 01|$ e $\tilde{\mathcal{D}}_1 = |10\rangle\langle 10|$.

A quantidade de Holevo de Bob, como definida na Eq. (5), assume o seguinte valor neste cenário:

$$\begin{aligned}\chi^{\text{Bob}} &= S\left(\rho_{\text{Bob}}\tilde{k}(u)\right) - \sum_u p_u S\left(\rho_{\text{Bob},u}\right) && (37)\\ &= S\left(\frac{1}{2}|01\rangle\langle 01| + \frac{1}{2}|10\rangle\langle 10|\right) - \frac{1}{2}S\left(\tilde{k}(0)\right) && (38)\\ &\quad -\frac{1}{2}S\left(\tilde{k}(1)\right) && (39)\\ &= 1-0-0 && (40)\\ &= 1 && (41)\end{aligned}$$

Utilizando este resultado na Eq. (25), é possível concluir que a capacidade quântica de sigilo para este cenário é igual a $C_{S,DFS}(\mathcal{E}) = 1$ bit por uso do canal. Este é um exemplo de como enviar mensagens secretas a uma taxa positiva utilizando DFS em um canal quântico ruidoso utilizando um procedimento de codificação-decodificação bastante simplificado.

VII. Impactos em Protocolos QSDC e DSQC

A Mecânica Quântica provê novas maneiras para realização de transmissão e processamento da informação. Em um contexto criptográfico, a *distribuição quântica de chaves* (QKD – *Quantum Key Distribution*) é uma das técnicas mais maduras atualmente, a qual possibilita a criação de chaves privadas clássicas com o intuito de permitir que duas partes realizem comunicações de forma segura [22, p. 586]. Estas chaves podem ser usadas para cifrar mensagens em esquemas de criptografias clássicos, tais como o *one-time pad*. Deste modo, percebe-se que há pelo menos duas transmissões em um protocolo QKD: a primeira delas via um canal quântico com o intuito de criar uma chave segura entre as partes; e a segunda, na qual a mensagem cifrada é transmitida. Muitos protocolos para QKD já foram propostos, inclusive com suas provas de segurança adequadamente estabelecidas [23].

Porém, em transmissões práticas, o ruído do canal não pode ser evitado completamente. Este ruído não apenas aumenta a taxa de erro no envio da mensagem, mas também pode dificultar a detecção de um espião num processo de checagem de segurança [10].

Recentemente, a *comunicação quântica segura direta* (QSDC – *Quantum Secure Direct Communication*) foi proposta como uma nova técnica de comunicação. Ela tem por objetivo transmitir mensagens secretas diretamente, sem o auxílio de chaves privadas nem de comunicações clássicas. Neste esquema, tem-se que a QKD e a transmissão clássica da mensagem cifrada são condensadas em uma única comunicação quântica. Por esta razão, considera-se que o QSDC como uma técnica completamente baseada na Mecânica Quântica [24].

Outra técnica que permite a comunicação quântica segura é intitulada *comunicação quântica determinística segura* (DSQC – *Deterministic Secure Quantum Communication*). Nesta técnica, a mensagem é enviada deterministicamente pelo canal quântico, mas pode ser deduzida apenas após uma transmissão de informação clássica [25]. De fato, a diferença

fundamental entre QSDC e DSQC é esta necessidade de mais um envio de comunicação clássica [24].

Até os dias atuais, muitos protocolos para QSDC e DSQC já foram propostos na literatura, considerando o uso de diferentes recursos e métodos, tais como troca de emaranhamento [26], teleportação [25], [27], [28], *one-time pad* quântico [29], rearranjo da ordem de partículas [30], dentre outros. O *survey* de Long et al. [24] contempla desenvolvimentos recentes tanto sobre QSDC quanto DSQC.

O uso de canais com ruído coletivo também foi considerado na proposição de alguns protocolos de QSDC e DSQC em uma tentativa de prevenir o ruído. Tais protocolos exploram as simetrias existentes no DFS para transmitir informação. Decaimento de amplitude [9], rotação [6], [10] e defasamento [6] são modelos de canais com ruído coletivo que já foram considerados por estes protocolos. Porém, como provado na Seção V, codificar informação em um DFS habilita comunicação quântica incondicionalmente segura. Deste modo, uma questão que emerge é: existem modificações que podem ser feitas nestes protocolos visando uma simplificação ou aumento de eficiência? As subseções a seguir irão caracterizar estes protocolos de acordo com o tipo de canal e irão apresentar algumas sugestões nesta direção.

A. Canal de Decaimento de Amplitude Coletivo

O fenômeno de dissipação de energia ao transmitir um estado quântico é modelado pelo *canal de decaimento de amplitude coletivo*. Este canal possui a seguinte representação OSR

$$\mathcal{E}(\rho) = A_0 \rho A_0^\dagger + A_1 \rho A_1^\dagger \tag{42}$$

em que os operadores A_0 e A_1 possuem a seguinte definição

$$A_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix} \qquad A_1 = \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix} \tag{43}$$

em que γ denota a taxa de decaimento, que pode ser pensada como a probabilidade de perda de um fóton [22, p. 380].

Um protocolo QSDC sobre o canal de decaimento de amplitude coletivo foi proposto por Qin et al. [9]. Este protocolo faz uso de dois estados de um DFS definidos sobre este canal ($|0_L\rangle$ e $|1_L\rangle$) e também de dois outros estados baseados numa superposição deles ($|+_L\rangle$ e $|-_L\rangle$). Estes estados quânticos são

$$|0_L\rangle = |00\rangle \tag{44}$$
$$|1_L\rangle = \frac{|10\rangle - |01\rangle}{\sqrt{2}} \tag{45}$$
$$|+_L\rangle = \frac{|0_L\rangle + |1_L\rangle}{\sqrt{2}} \tag{46}$$
$$|-_L\rangle = \frac{|0_L\rangle - |1_L\rangle}{\sqrt{2}} \tag{47}$$

O protocolo de Qin et al. é definido como segue:

1) Alice gera uma seqüência aleatória dos seguintes estados $\{|0_L\rangle, |1_L\rangle, |+_L\rangle, |-_L\rangle\}$ e os envia para Bob;
2) Bob escolhe alguns qubits para realizar uma checagem de espionagem. Ele os mede em uma das duas bases possíveis aleatoriamente escolhidas ($\{|0_L\rangle, |1_L\rangle\}$ ou $\{|+_L\rangle, |-_L\rangle\}$) e publica os resultados obtidos. Alice checa as saídas e julga quando existem espiões no canal. Bob realiza algumas operações nos qubits remanescentes, introduz alguns bits aleatórios, e os envia de volta para Alice;
3) Alice mede os qubits recebidos na mesma base que ela originalmente os preparou. A depender da relação entre as saídas obtidas e os estados originalmente preparados, Alice pode deterministicamente decodificar a mensagem enviada por Bob;
4) Bob declara a posição e os valores dos bits aleatórios. Alice julga a segurança e recupera a mensagem enviada.

Neste protocolo, o número de comunicações requerido para a troca da mensagem e também para a checagem de espionagem inclui redundância, bits aleatórios e também comunicações clássicas para divulgar a saída de determinadas medições. Vale mencionar também que a taxa deste protocolo é de 1 bit de informação por uso do canal, uma vez que um estado de dois qubits é utilizado.

Os estados $|0_L\rangle$ e $|1_L\rangle$ do DFS existente no canal também possibilitam o envio de 1 bit de informação por uso do canal, mas com a vantagem de que não é necessário realizar checagem de espionagem, pois os DFS habilitam segurança incondicional. Formalizando, Alice e Bob podem usar um OEAC $(\tilde{K}(\{0,1\} = \{\tilde{k}(0) = |0_L\rangle, \tilde{k}(1) = |1_L\rangle\}, \{\tilde{D}_0 = |0_L\rangle\langle 0_L|, \tilde{D}_1 = |1_L\rangle\langle 1_L|\})$ para realizar a troca de mensagens de forma segura.

Apesar da taxa resultante ser a mesma, o uso do QEAC sugerido provê uma redução significativa na Complexidade Comunicacional Quântica[1] deste protocolo. Na proposição original, se a mensagem possui tamanho m, então é evidente que mais de m bits e qubits precisam ser trocados para realizar a comunicação. Utilizando a simplificação apresentada, este número iguala-se exatamente a m, com a vantagem adicional de não ser necessário utilizar um canal clássico. Além disso, o processo de codificação-decodificação se torna menos complexo, o que reduz o número de portas quânticas requeridas para implementar este esquema.

B. Canal Quântico de Rotação Coletiva

Um canal quântico de rotação coletiva pode ser denotado como

$$|0\rangle \rightarrow \cos\theta\,|0\rangle + \sin\theta\,|1\rangle \tag{48}$$
$$|1\rangle \rightarrow -\sin\theta\,|0\rangle + \cos\theta\,|1\rangle \tag{49}$$

em que θ denota o parâmetro de rotação o qual flutua com o tempo t. Dois estados imunes aos efeitos deste canal são estados de Bell

[1] A complexidade comunicacional é uma medida de quantas comunicações são necessárias para que duas partes possam concluir uma tarefa distribuída utilizando o mínimo de comunicações possível [31].

$$\left|\phi^+\right\rangle = \frac{1}{\sqrt{2}}(|0_1 0_2\rangle + |1_1 1_2\rangle) \quad (50)$$

$$\left|\psi^-\right\rangle = \frac{1}{\sqrt{2}}(|0_1 1_2\rangle - |0_1 1_2\rangle) \quad (51)$$

Recentemente, Gu et al. [6] propuseram um DSQC o qual faz uso do DFS existente neste canal. De acordo com estes autores, a comunicação sigilosa pode ser feita da seguinte forma:

1) Alice prepara um estado emaranhado de três fótons

$$\left|\Phi^+\right\rangle_{AB_1B_2} = \frac{1}{\sqrt{2}}\left(|0_A\rangle\left|\phi^+_{B_1B_2}\right\rangle + |1_A\rangle\left|\psi^-_{B_1B_2}\right\rangle\right) \quad (52)$$

   Ela mantém o qubit A e envia os qubits B_1 e B_2 para Bob;
2) Após receber a seqüência de Alice, Bob escolhe algumas amostras para checar a existência de espionagem. Para tanto, ele mede alguns qubits utilizando as bases $Z_{B_1} \otimes Z_{B_2}$, $Z_{B_1} \otimes X_{B_2}$ e $X_{B_1} \otimes Z_{B_2}$ escolhidas de maneira aleatória;
3) Bob divulga para Alice quais os qubits escolhidos para checagem de espionagem e o resultado obtido da medição de tais amostras;
4) Se Bob escolheu medir com a base $Z_{B_1} \otimes Z_{B_2}$, então Alice escolhe a base Z_A para medir seu fóton correspondente; em caso contrário, ela o mede utilizando X_A;
5) Alice e Bob utilizam a correlação existente entre as suas amostras para analisar a taxa de erro. Se o erro é maior que um limiar, eles repetem o protocolo desde o início. Em caso contrário, irão codificar as saídas $|0_A\rangle$, $|00_{B_1B_2}\rangle$, $|11_{B_1B_2}\rangle$, $|+_A\rangle$, $|0+_{B_1B_2}\rangle$, $|1-_{B_1B_2}\rangle$, $|-0_{B_1B_2}\rangle$ e $|+1_{B_1B_2}\rangle$ como correspondendo ao bit clássico 0, enquanto as saídas $|1_A\rangle$, $|01_{B_1B_2}\rangle$, $|10_{B_1B_2}\rangle$, $|-_A\rangle$, $|0-_{B_1B_2}\rangle$, $|1+_{B_1B_2}\rangle$, $|+0_{B_1B_2}\rangle$ e como correspondendo ao bit clássico 1;
6) Alice divulga para Bob a saída $C_A = O_A \oplus M_A$ em que O_A é o resultado das medições que ela obteve no fóton A e M_A é a mensagem secreta que ela deseja mandar para Bob de maneira privada;
7) Bob lê a mensagem secreta diretamente, i.e., $M_A = C_A \oplus O_B$, em que O_B é o resultado das medições que Bob efetuou nos fótons B_1 e B_2.

Antes de iniciar a análise deste protocolo, primeiramente algumas considerações serão feitas sobre ele. Os estados do DFS são estados de Bell, a correlação existente entre as amostras de Alice e Bob permite uma checagem de espionagem e, por último, uma cifragem do tipo *one-time pad* é efetuada antes de a mensagem ser enviada.

Em face do DFS existente, algumas simplificações são passíveis de aplicação nesse protocolo. Se Alice e Bob desejam enviar a mensagem diretamente pelo canal quântico, uma codificação apropriada utilizando apenas os estados $|\phi^+\rangle$ e $|\psi^-\rangle$ pode ser feita alcançando a taxa de um bit de informação por uso do canal. Estes bits podem ser utilizados para criar uma chave secreta privada para codificar as mensagens utilizando *one-time pad*, de acordo com os dois últimos passos do protocolo de Gu et al. [6]. Outra sugestão que pode ser explorada tira proveito da correlação existente entre os estados de Alice e Bob para criar esta chave.

Em ambas as sugestões, a segurança incondicional provida pelo DFS é um ingrediente chave para as simplificações realizadas. Como pode ser observado, em nenhum dos casos a checagem de espionagem é requerida, o que reduz substancialmente o número de comunicações realizadas.

Estas sugestões podem ser aplicadas de maneira similar no DSQC proposto por Dong et al. [10] que é bastante similar ao protocolo de Gu et al [6] mostrado nesta seção. A principal diferença entre eles consiste no uso do canal clássico: enquanto o protocolo de Gu et al. utiliza este canal para enviar uma versão cifrada da mensagem, o protocolo de Dong et al. o utiliza para converter os resultados das medições nos bits apropriados da mensagem secreta. Neste protocolo, enviar uma mensagem de m bits requer que Alice e Bob troquem pelo menos $4 \cdot m$ bits e qubits. Seguindo a primeira sugestão de modificação, este número de comunicações seria reduzido a m qubits.

C. Canal Quântico de Defasamento Coletivo

O canal quântico de defasamento coletivo já foi caracterizado anteriormente na Seção VI. Um protocolo que faz uso deste DFS foi proposto por Gu et al [6], o qual é bastante similar ao QSDC proposto por estes mesmos autores para o canal de rotação coletiva, discutido previamente na seção VII-B.

Também foi mostrado na Seção VI como enviar 1 bit de informação por uso do canal sem a necessidade de checagem de espionagem. A mesma idéia pode ser utilizada aqui para simplificar significativamente o protocolo em questão.

VIII. Considerações Finais

A partir da análise realizada, é possível concluir que se um canal quântico é caracterizado como na Definição 6, então a existência de certas simetrias pode ser explorada para enviar informação clássica com segurança incondicional. A codificação da informação em um DFS pode ser vista como uma instância de um código *wiretap*, com a particularidade de que nenhuma informação é capturada por um espião.

A expressão da capacidade de sigilo destes canais, mostrada na Eq. (25) é igual à capacidade de um canal quântico para o envio de mensagens clássicas [21]. Este é um caso particular em que a habilidade de um canal quântico para enviar informação secreta é tão grande quando a sua habilidade de enviar informação clássica ordinária.

Em se tratando da capacidade quântica de sigilo, Cai et al. [2] argumentam que esta não possui letra isolada e, em virtude disso, obter uma versão computável da mesma torna-se ainda mais difícil que obter uma versão computável para a

capacidade clássica de um canal quântico. O caso particular para canais quânticos com ruído coletivo apresentado neste trabalho mostra que esta capacidade de sigilo é igual à capacidade clássica de um canal quântico, o que indica uma menor complexidade na obtenção desta capacidade.

Apesar das dificuldades existentes atualmente para construir sistemas quânticos completamente fechados [8], os resultados mostrados aqui podem ser aplicados para construir dispositivos que realizam a troca de mensagens com segurança incondicional mesmo na presença da descoerência. Isto é bastante promissor para implementações práticas, especialmente considerando os resultados já existentes sobre o uso de DFS em comunicações [32]-[34], incluindo de longa distância [35].

Uma primeira conseqüência dos resultados deste trabalho foi mostrar uma simplificação substancial em protocolos de QSDC e DSQC existentes na literatura. O número de comunicações realizadas e de operações pôde ser significativamente reduzido em função dos novos resultados sobre segurança incondicional e DFS. Isto reforça a viabilidade prática do uso de DFS em comunicações.

É importante enfatizar que os resultados apresentados não podem ser generalizados para todos os tipos de canais quânticos, pois nem todos eles satisfazem às condições para existência de DFS. Zanardi e Rasetti [20] argumentam que só existem DFS em cenários onde há descoerência coletiva. Apesar de ser um caso especial, as vantagens alcançadas em termos de segurança e taxa são significativas.

Em trabalhos futuros, sugere-se a investigação de condições mais gerais para a existência de sigilo absoluto em comunicações quânticas.

AGRADECIMENTOS

Os autores agradecem o apoio provido pelas agências de fomento brasileiras CAPES e CNPq e pelo projeto QUANTA/RENASIC/FINEP.

REFERÊNCIAS

[1] M. Schlosshauer, Decoherence and the Quantum-to-Classical Transition, Springer, Ed. Springer, 2007.

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

[3] 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.

[4] 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.

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

[6] 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.

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

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

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

[10] 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.

[11] 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.

[12] 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.

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

[14] 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.

[15] B. Schumacher and M. Westmoreland, "Quantum privacy and quantum coherence," Phys. Rev. Lett., vol. 80, no. 25, pp. 5695–5697, 1998.

[16] A. D. Wyner, "The wire-tap channel," The Bell System Technical Journal, vol. 1, pp. 1355–1387, 1975.

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

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

[19] 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.

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

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

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

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

[24] G. Lu Long, F. Guo Deng, C. W. X. Han Lo, K. Wen, and W. Ying Wang, "Quantum secure direct communication and deterministic secure quantum communication," Front. Phys. China, vol. 2, no. 3, pp. 251–272, 2007.

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

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

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

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

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

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

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

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

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

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

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

Elloá B. Guedes é doutora em Ciência da Computação pela Universidade Federal de Campina Grande, pesquisadora do Instituto de Estudos em Computação e Informação Quânticas (IQuanta) e docente da Escola Superior de Tecnologia da Universidade do Estado do Amazonas (UEA). A autora já desenvolveu outros trabalhos nas áreas de Computação e Informação Quânticas, especialmente ligados à predição de geradores pseudoaleatórios criptograficamente seguros. Atualmente trabalha com simulação de algoritmos quânticos em computadores clássicos e também com comunicações seguras por canais quânticos ruidosos.

Francisco M. de Assis é professor titular da Universidade Federal de Campina Grande com pós-doutorado na Universidade de Toronto, Canadá. Os principais interesses de pesquisa do autor são Teoria da Informação Clássica e Quântica, Sistemas de Telecomunicação, Algoritmos e Complexidade Computacional. Atualmente é presidente do Instituto de Estudos em Computação e Informação Quânticas (IQuanta) e também coordenador do Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Campina Grande.