Distribuição Quântica de Chaves em Canais Quânticos com Decaimento Coletivo de Amplitude

Elloá B. Guedes e Francisco M. de Assis

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

***Index Terms*—Quantum Key Distribution; Decoherence-Free Subspaces and Subsystems; Amplitude Damping.**

I. Introdução

Os princípios da Mecânica Quântica provêem novas maneiras para processamento e transmissão da informação quântica, a exemplo da Computação e da Comunicação Quânticas. Em se tratando da Comunicação Quântica, em particular, algumas propriedades intrínsecas da Mecânica Quântica possibilitam a existência de características que não possuem equivalente na Comunicação Clássica, a exemplo de: (i) um qubit[1] não possui valor definido até o momento posterior à sua medição; (ii) as medições em qubits podem perturbá-los, alterando os seus estados; (iii) estados quânticos arbitrários não podem ser copiados; (iv) qubits podem estar emaranhados, dentre outras [1]. Graças aos princípios da Mecânica Quântica, em certos cenários a segurança incondicional pode ser alcançada ao enviar informações por canais quânticos.

A *Distribuição Quântica de Chaves* (QKD – *Quantum Key Distribution*) [2]–[5] é uma das técnicas mais maduras da Comunicação Quântica nos dias atuais. De acordo com a QKD, duas entidades geograficamente separadas podem criar uma chave privada de maneira segura. Esta chave pode então ser usada para cifrar uma mensagem secreta por meio de algum esquema criptográfico clássico, tal como o *one-time pad*, e a cifra pode então ser enviada de uma entidade para a outra por meio de um canal clássico. Em cenários práticos de QKD, entretanto, o ruído do canal quântico pode não ser evitado por completo, o que causa não apenas o aumento da taxa de erros, como também dificulta o processo de encontrar espiões na comunicação em um processo de checagem de segurança.

Considera-se que o ruído em canais quânticos é causado por um fenômeno denominado *descoerência*, responsável por causar uma interação indesejada entre um sistema quântico de interesse e o ambiente, culminando na perda de informação [6]. Com o intuito de evitar os efeitos negativos deste fenômeno, alguns protocolos para QKD consideram o uso de canais quânticos que estão sujeitos à *descoerência coletiva* [7], [8]. Neste cenário, todos os qubits que sofrem descoerência são afetados exatamente da mesma maneira [9]. Considerando esta particularidade, em tais canais quânticos é possível encontrar algumas simetrias que protegem a informação do ruído. Em conseqüência, estes estados permanecem inalterados apesar da descoerência existente, compondo *Subespaços ou Subsistemas Livre de Descoerência* (DFSs – *Decoherence-Free Subspaces or Subsystems*) [10].

Boileau et al. [7] propuseram dois protocolos QKD utilizando para o canal quântico de rotação coletiva. O primeiro protocolo considera o uso de um subespaço, enquanto o segundo considera o uso de um subsistema, ambos livres de descoerência. Estes protocolos consideram o uso de *singlets*[2] e a codificação é baseada na paridade dos qubits. Graças a isto uma incerteza é inserida sobre o estado originalmente enviado, considerando a perspectiva do espião. Porém, isto não afeta as entidades legitimas, habilitando-as a criar uma chave privada que pode ser utilizada posteriormente para cifrar uma mensagem clássica. Considerando o cenário dos DFSs, o espião não é capaz de afetar os qubits trocados nem de capturar informações sobre a chave secreta. Baseando-se em idéias similares, Li e outros [8] propuseram dois protocolos QDK utilizando DFSs e considerando os canais quânticos de rotação e defasamento coletivos.

O *decaimento de amplitude* é um tipo de ruído que pode fazer um qubit ser perdido. Este tipo de erro também está sujeito à descoerência coletiva, caracterizando os *canais quânticos com decaimento coletivo de amplitude*. Embora estes canais possuam DFSs, nenhum protocolo para distribuição quântica de chaves foi proposto até então para este tipo de canal, segundo o que pôde ser apurado em revisões da literatura.

Este trabalho foi desenvolvido com o apoio da CAPES, CNPq, FAPEAM e QUANTA/RENASIC. Elloá B. Guedes é professora da Escola Superior de Tecnologia da Universidade do Estado do Amazonas, Manaus, AM, Brasil. (email: elloaguedes@gmail.com) Francisco M. de Assis é professor da Universidade Federal de Campina Grande, Campina Grande, PB, Brasil (email: fmarassis@gmail.com). Os autores são integrantes do Instituto de Estudos em Computação e Informação Quânticas (IQuanta).

[1] Qubit é o análogo quântico do bit clássico.

[2] *Singlets* são conjuntos de qubits emaranhados.

Assim, o principal objetivo deste trabalho é caracterizar um protocolo QKD para canais quânticos com decaimento coletivo de amplitude, viabilizando uma maneira segura de criar chaves privadas entre entidades geograficamente separadas, apesar da existência de ruído e de espionagem no canal quântico.

O trabalho está organizado como segue. O canal quântico de decaimento coletivo de amplitude e os DFSs existentes em sua estrutura são apresentados na Seção II. O modelo de comunicações considerado, o protocolo proposto e os passos para a checagem de espionagem são apresentados na Seção III. Uma análise da segurança do protocolo proposto é discutida na Seção IV. Por fim, considerações finais e sugestões de trabalhos futuros são apresentadas na Seção V.

Notação e Convenções: A *notação de Dirac* [11] será utilizada para denotar estados quânticos e operações sobre eles. Diz-se que um *estado puro* é um vetor unitário no espaço de Hilbert $\mathcal{H}$. A *operação de Hadamard*, implementada pela porta H, possui representação matricial dada por $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. O símbolo $\mathbb{1}$ denota a *matriz identidade*.

II. Canal Quântico com Decaimento Coletivo de Amplitude

O fenômeno de dissipação de energia ao enviar um estado quântico por um canal é modelado pelo *canal quântico com decaimento coletivo de amplitude*. Este canal possui a seguinte *Representação da Soma de Operadores* (OSR – *Operator-Sum Representation*)

$$\mathcal{E}(\rho) = A_0 \rho A_0^\dagger + A_1 \rho A_1^\dagger, \tag{1}$$

em que os operadores A_0 e A_1 são dados como segue

$$A_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix}, \qquad A_1 = \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix}, \tag{2}$$

em que γ é a taxa de decaimento, a qual pode ser pensada como a probabilidade de perder um qubit [1, p. 380].

Neste canal, graças ao cárater coletivo, todos os qubits que sofrem decaimento de amplitude estão sujeito à mesma taxa de decaimento. Graças à isto, é possível encontrar um DFS no espaço de Hilbert deste canal imune aos efeitos causados por este tipo de descoerência.

Neste canal existêm três DFSs diferentes, com dimensões 1, 2 e 3, respectivamente, como mostrados a seguir

$$\tilde{\mathcal{H}_1} = \{|1\rangle\}, \tag{3}$$

$$\tilde{\mathcal{H}_2} = \left\{ |00\rangle, \frac{|01\rangle - |10\rangle}{\sqrt{2}} \right\}, \tag{4}$$

$$\tilde{\mathcal{H}_3} = \left\{ \frac{1}{\sqrt{6}}(-2|001\rangle + |010\rangle + |100\rangle), \frac{1}{\sqrt{2}}(|011\rangle - |101\rangle), |000\rangle \right\}. \tag{5}$$

Em particular, o DFS $\tilde{\mathcal{H}_2}$ será utilizado no protocolo QKD que será proposto na seção a seguir.

III. Protocolo Proposto

O protocolo proposto considera o esquema de comunicações ilustrado na Figura 1. As entidades legítimas (Alice e Bob) estão conectadas por meio de um canal clássico e também por meio de um canal quântico com decaimento coletivo de amplitude. Ambos os canais são considerados inseguros. O objetivo de Alice e Bob é criar uma chave privada e realizar uma troca segura de mensagens clássicas.

A espiã Eva possui acesso ao canal quântico existente entre Alice e Bob. Ela utiliza um dispositivo que mede o estado quântico enviado pelo canal e armazena a base utilizada para medição e também o resultado obtido. Após esta medição, o dispositivo envia o estado quântico resultante pelo canal. O tipo de ataque realizado por Eva é, portanto, do tipo "intercepta e re-envia".

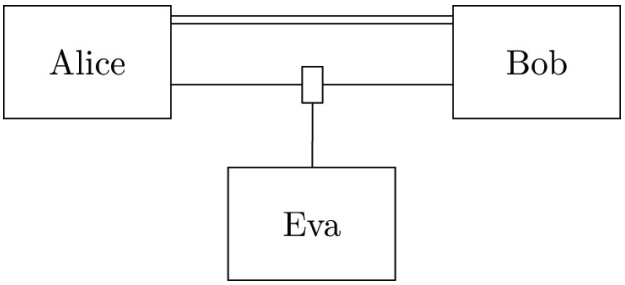

Figura 1. Modelo de comunicações considerado. A linha única representa o canal quântico, enquanto a linha dupla representa o canal utilizado para comunicações clássicas.

A idéia do protocolo proposto é bastante similar ao protocolo QKD BB84 [2], mas com a vantagem da prevenção ao ruído devido ao DFS existente. A descrição do protocolo será feita nas seções a seguir.

A. Descrição do Protocolo

As entidades legítimas Alice e Bob fazem uso do seguintes estados quânticos

$$|{\rightarrow}\rangle = |00\rangle, \tag{6}$$

$$|{\uparrow}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}, \tag{7}$$

$$|{\nearrow}\rangle = |{+}{+}\rangle, \tag{8}$$

$$|{\searrow}\rangle = \frac{|{+}{-}\rangle - |{-}{+}\rangle}{\sqrt{2}}, \tag{9}$$

em que $|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ e $|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$.

Os estados quânticos $|{\nearrow}\rangle$ e $|{\searrow}\rangle$ são obtidos a partir dos estados $|{\rightarrow}\rangle$ e $|{\uparrow}\rangle$ por meio da aplicação de uma operação de Hadamard. Graças às propriedades dos DFSs, nenhum dos estados quânticos apresentados nas Eqs. (6)-(9) é afetado pelo decaimento de amplitude. Os circuitos quânticos ilustrados na Figura 2 mostra como obter tais estados.

Alice inicia o protocolo enviando estados aleatoriamente escolhidos para Bob a partir do conjunto $\{|{\rightarrow}\rangle, |{\uparrow}\rangle, |{\nearrow}\rangle, |{\searrow}\rangle\}$.

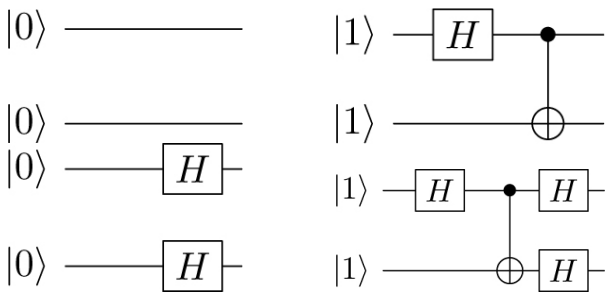

Figura 2. Circuitos quânticos que implementam os estados $|\rightarrow\rangle$, $|\uparrow\rangle$, $|\nearrow\rangle$, e $|\searrow\rangle$, respectivamente.

Bob e Eva medem os estados utilizando as bases horizontal-vertical $+ = \{|\rightarrow\rangle\langle\rightarrow|, |\uparrow\rangle\langle\uparrow|\}$ ou diagonal $\times = \{|\nearrow\rangle\langle\nearrow|, |\searrow\rangle\langle\searrow|\}$, também escolhidas de maneira aleatória.

Primeiramente será considerado que Eva não afeta a comunicação entre Alice e Bob. A Tabela I mostra exemplo dos resultados obtidos por Alice e Bob ao criarem uma chave privada simétrica. Se Alice envia $|\rightarrow\rangle$ e $|\uparrow\rangle$ e Bob mede com a base $+$, ele irá obter os bits 0 e 1, respectivamente, com 100% de certeza. O mesmo ocorre quando Alice envia $|\nearrow\rangle$ e $|\searrow\rangle$ e Bob mede com a base $\times$. Porém, por exemplo, se Alice envia $|\rightarrow\rangle$ e Bob mede utilizando a base $\times$, então há uma probabilidade de $0,5$ dele receber o bit 0 e de $0,5$ de receber o bit 1.

Tabela I
RESULTADOS OBTIDOS POR BOB APÓS MEDIR OS ESTADOS QUÂNTICOS ENVIADOS POR ALICE, COM SUAS RESPECTIVAS PROBABILIDADES.

Alice envia	$\|\rightarrow\rangle$	$\|\uparrow\rangle$	$\|\nearrow\rangle$	$\|\searrow\rangle$
Base de Bob	$+$	$+$	$\times$	$\times$
Bit obtido	0	1	0	1
Probabilidade	1	1	1	1

Alice envia	$\|\rightarrow\rangle$	$\|\searrow\rangle$	$\|\nearrow\rangle$	$\|\uparrow\rangle$
Base de Bob	$\times$	$+$	$+$	$\times$
Bit obtido	0 ou 1	0 ou 1	0 ou 1	0 ou 1
Probabilidade	0,5	0,5	0,5	$0,5$

Com o intuito de evitar incertezas em relação aos bits obtidos por Bob, ele irá comunicar-se com Alice com o intuito de informá-la as bases que foram utilizadas para medir os qubits que ela enviou. Alice irá retornar a Bob uma string de bits, em que 0 indica que a respectiva medição deve ser descartada por conduzir a uma incerteza. Após este processo, mesmo sem comunicarem o resultado das medições, Alice e Bob possuem a mesma seqüência de bits. Estes bits irão compor a chave privada simétrica que será utilizada na cifragem da mensagem via *one-time pad* que será enviada pelo canal clássico.

Para ilustrar o protocolo proposto, supõe-se que Alice envia para Bob a seguinte seqüência de qubits: $|\nearrow\rangle, |\uparrow\rangle, |\uparrow\rangle, |\rightarrow\rangle, |\nearrow\rangle, |\searrow\rangle, |\uparrow\rangle$. Bob utiliza a seqüência de bases $+, +, \times, +, \times, +, +$ e obtém uma seqüência de bits dada por 0100011. Bob envia as bases que ele utilizou pelo canal clássico e Alice retorna para ele a seqüência 0011101. Esta seqüência de bits enviada por Alice indica que o primeiro, segundo e sexto bits devem ser descartados por Bob. Assim, a chave privada simétrica entre Alice e Bob possui comprimento igual a 5 e será igual a 00001. Com esta chave, Alice pode enviar para Bob uma mensagem secreta utilizando o esquema *one-time pad*.

A cifragem via *one-time pad* requer que a mensagem e a chave sejam de mesmo tamanho. Seja m a mensagem e k a chave, ambas com n bits. A versão cifrada da mensagem e é obtida por $e_i = m_i \oplus k_i$, for $i = 1, \ldots, n$, em que $\oplus$ denota a soma módulo 2. Se a chave é utilizada uma única vez e mantida em segredo, então as condições para o *sigilo absoluto* nesta comunicação são garantidos [12].

No exemplo em questão, supõe-se que Alice deseja enviar a mensagem $m = 10101$ para Bob. Ela irá seguir os passos da cifragem *one-time pad*, considerando a chave $k = 00001$, obtendo a mensagem cifrada $e = 10100$ que será enviada pelo canal clássico para Bob. Ao receber e, Bob irá utilizar sua chave k e irá obter a mensagem original enviada por Alice utilizando a operação soma módulo 2, a qual resultará em $m' = m = 10101$. Desta maneira, o protocolo de distribuição quântica de chaves e o envio da mensagem secreta foram concluídos com sucesso.

Na caracterização do protocolo apresentada, a espiã Eva não efetuou nenhuma ação durante o processo da criação da chave secreta. Esta situação, porém, é altamente não-realística e as ações da mesma no canal quântico devem ser consideradas. A próxima seção mostra como Eva pode tentar capturar informações a respeito da chave secreta criada por Alice e Bob e como estes podem utilizar estratégias para detectar a espionagem realizada, evitando que esta última seja bem sucedida.

B. Checagem de Espionagem

De acordo com o modelo de comunicações considerado, Eva pode realizar medições no estado enviado por Alice, obter um bit a partir disto, e re-enviar o estado resultante para Bob. Durante este processo, Eva pode não apenas capturar bits da chave privada, mas também alterar o estado quântico enviado originalmente por Alice para Bob.

Eva realiza medições nos estados enviados por Alice utilizando as bases $+$ e $\times$ escolhidas aleatoriamente, i.e., utilizando a mesma estratégia que Bob. Para tanto, ela utiliza um dispositivo que captura a estado no canal quântico, o mede, e re-envia o estado quântico resultante para Bob. Os efeitos das medições realizadas por ela podem degradar a informação recebida por Bob. A Tabela II sintetiza os efeitos de Eva no canal quântico.

Se em umas das escolhas aleatórias da base de medição Eva, por coincidência, utilizar a mesma base que Alice utilizou para preparar um determinado estado quântico, como mostrado na

Tabela II
ESTADOS ENVIADOS POR ALICE E MEDIDOS PELA ESPIÃ EVA.

Alice envia	$\|\rightarrow\rangle$	$\|\uparrow\rangle$	$\|\nearrow\rangle$	$\|\searrow\rangle$
Base de Eva	$+$	$+$	$\times$	$\times$
Bit resultante de Eva	0	1	0	1
Probabilidade	1	1	1	1
Estado recebido por Bob	$\|\rightarrow\rangle$	$\|\uparrow\rangle$	$\|\nearrow\rangle$	$\|\searrow\rangle$

Alice envia	$\|\rightarrow\rangle$	$\|\uparrow\rangle$
Base de Eva	$\times$	$\times$
Bit resultante de Eva	0 ou 1	0 ou 1
Probabilidade	$0,5$	$0,5$
Estado recebido por Bob	$\|\nearrow\rangle$ ou $\|\searrow\rangle$	$\|\nearrow\rangle$ ou $\|\searrow\rangle$

Alice envia	$\|\nearrow\rangle$	$\|\searrow\rangle$
Base de Eva	$+$	$+$
Bit resultante de Eva	0 ou 1	0 ou 1
Probabilidade	$0,5$	$0,5$
Estado recebido por Bob	$\|\rightarrow\rangle$ ou $\|\uparrow\rangle$	$\|\rightarrow\rangle$ ou $\|\uparrow\rangle$

primeira parte da Tabela II, ela irá obter o mesmo bit que Bob e não irá causar nenhuma perturbação no sistema. Porém, se ela medir os estados utilizando a base incorreta, como mostrado na segunda e terceira parte da Tabela II, ela não irá ter certeza sobre o estado enviado por Alice e também irá modificar o estado originalmente enviado. Quando esta segunda situação acontece, Alice e Bob podem executar um procedimento para detecção de espionagem.

Para realizar a detecção de espionagem, além de revelar as bases utilizadas, Bob irá também enviar para Alice alguns bits que ele obteve após a medição. Estes bits serão importantes para detectar a presença de um espião, mas devem ser descartados para não comprometer a segurança da chave privada. Para ilustrar esta situação, suponha que Alice enviou para Bob o estado $|\nearrow\rangle$, o qual Eva mediu com a base $+$ e obteve o bit 1. Bob, por sua vez, efetuou a medição bom a base $\times$ e recebeu o bit 1. Ao repassar para Alice a informação que ele usou a base $\times$ e recebeu o bit 1, Alice percebe que há algo errado e conclui que existe um espião no canal quântico, visto que o cenário considerado é livre de ruído.

Desta maneira, para criar a chave privada em sigilo, Alice e Bob devem comunicar não apenas as bases utilizadas para medição, mas também alguns dos resultados obtidos. Isto é essencial para garantir a segurança do protocolo proposto, como será mostrado na próxima seção.

IV. ANÁLISE DE SEGURANÇA

O objetivo de uma distribuição de chaves é permitir que as entidades legítimas, as quais inicialmente não compartilham nenhuma informação, possam criar uma chave secreta (uma string de bits) ao final do processo, ao passo que o espião não é capaz de obter nenhuma informação a respeito desta chave. Além disto, o que quer que o espião faça, a chave criada entre as entidades legítimas deve ser idêntica. Assume-se que as informações que trafegam tanto no canal quântico quanto no clássico estão sujeitas à espionagem [5].

Não é possível obter sucesso em um protocolo QKD se o espião puder representar o papel de uma das entidades legítimas da comunicação. Se as entidades legítimas puderem ter alguma comunicação prévia, existem técnicas de autenticação as quais podem ser utilizadas para alcançar a segurança incondicional [13].

Diferentemente da comunicação clássica, cuja segurança se baseia na hipótese de intratabilidade computacional de determinados problemas, a segurança das comunicações quânticas é baseada nas leis da Física. O espião é capaz de realizar diversas ações, limitando-se apenas àquelas que são fisicamente impossíveis. A impossibilidade de clonar um estado quântico arbitrário devido ao *Teorema da Não-Clonagem* [14], por exemplo, impede que o espião capture estados quânticos sem perturbá-los, o que deixará evidências de sua presença para as entidades legítimas [8]. Tais fatos serão utilizados na caracterização da segurança do protocolo proposto.

A estratégia utilizada pelo espião que será considerada na análise de segurança será o ataque do tipo "intercepta e reenvia" [15], no qual o espião mede o estado quântico originalmente enviado, obtém um bit, e re-envia o estado resultado pelo canal. Este tipo de ataque e suas conseqüências já foram detalhados na Seção III, mas a probabilidade de sucesso do espião será descrita de agora em diante. Vale salientar que, uma vez que este protocolo é baseado no protocolo QKD BB84 [2], as mesmas provas de segurança que se aplicam à este protocolo são adequadas para proposição feita no escopo deste artigo. O trabalho de Mayers [5] é sugerido como uma fonte de informação para obtenção de tais provas formais.

Se Alice envia um bit b para Bob, ela pode codificá-lo de quatro maneiras diferentes, utilizando dois modos de preparo para isto. Eva, ao interceptar este bit, possui duas opções de bases de medição. A chance de Eva acertar qual o bit enviado é de 50%. Mas, se Eva utilizar uma base incorreta, isto pode levar Bob a receber um bit diferente do que foi originalmente enviado por Alice, com uma chance de detecção de espionagem de 50% a cada bit enviado.

Supõe-se que Alice e Bob desejam criar uma chave privada de tamanho k. Dado que Eva pode realizar ataques, Alice e Bob irão utilizar estratégias para detecção de espionagem utilizando k bits adicionais. A probabilidade de Eva medir corretamente os $2 \cdot k$ bits trocados entre as entidades legítimas sem afetá-los é de $p(2 \cdot k) = 0.5^{2 \cdot k}$, a qual decresce exponencialmente à medida que o tamanho da chave aumenta, como mostrado na linha azul do gráfico ilustrado na Figura 3.

Porém, se Eva errar na medição de um único bit em uma seqüência de $2 \cdot k$ bits (em que a probabilidade de erro é igual a $p_{\text{erro}} = 0,5$ por bit), isto pode resultar em um erro de bit entre Alice e Bob (em que a probabilidade de detecção deste erro é dada por $p_{\text{detecção}} = 0,5$ por bit). Considerando estas probabilidades, a chance de detectar Eva no n-ésimo bit

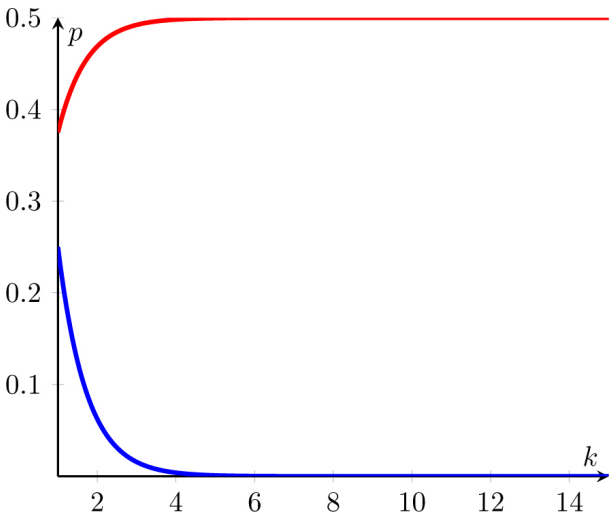

Figura 3. Gráfico mostrando o decréscimo exponencial na probabilidade de sucesso de Eva ao tentar capturar todos os bits da chave privada (linha azul) e a probabilidade de Alice e Bob detectarem Eva a cada bit trocado para criação da chave (linha vermelha).

trocado entre Alice e Bob converge assintoticamente para $0,5$, como mostrado na linha vermelha do gráfico da Figura 3, ou seja, tende a depender apenas da probabilidade de detecção do erro. Diferentemente da probabilidade de sucesso de Eva, a probabilidade de detecção de espionagem é independente a cada bit trocado. Uma vez que existe a possibilidade de Eva alterar o estado de um qubit e esta alteração não ser detectada, como mostrado anteriormente nas Tabelas I e II, existe sempre a possibilidade de não conseguir detectar o espião na comunicação.

Como pode ser visto, enquanto o sucesso de Eva depende do acerto de todos os bits sem perturbar a comunicação entre Alice e Bob, a detecção de espionagem depende apenas de um único erro de Eva que provoca uma perturbação no estado quântico e da detecção desta no processo de espionagem. Com isto, pode-se concluir que a probabilidade de detecção de espionagem neste protocolo é alta, garantindo segurança suficiente para cenários práticos de seu uso. Conclui-se, então, a análise de segurança do protocolo de distribuição quântica de chaves proposto.

V. Considerações Finais

A primeira demonstração prática de um protocolo QKD foi feita nos anos 90 utilizando fótons em uma distância de 30 cm pelo ar. Trabalhos posteriores conseguiram implementar este tipo de protocolo pela atmosfera garantindo a criação de chaves via troca de estados quânticos em uma distância de 2 km. Posteriormente, com o avanço da tecnologia, protocolos QKD puderam ser implementados em distâncias em torno de 250 km [16]. Atualmente, existem dispositivos comercializados livremente para realizar a distribuição quântica de chaves via fibra óptica [17].

Embora no quesito distância os protocolos QKD tenham evoluído bastante, um dos principais problemas práticos que ainda persistem é o ruído, o qual pode não somente afetar a comunicação entre as entidades legítimas, como também favorecer um espião existente no canal. Na tentativa de minimizar tais problemas, este trabalho apresentou um protocolo QKD para canais quânticos com decaimento coletivo de amplitude em que os estados quânticos são imunes ao ruído.

O protocolo proposto é inspirado no protocolo QKD BB84 [2], mas uma vez que considera a existência de DFSs no canal quântico, a comunicação ocorre livre de ruídos. Na caracterização deste protocolo é considerada a existência de um espião que almeja descobrir a chave privada por meio da interceptação das informações trocadas entre as entidades legítimas. Com o intuito de evitar que isto aconteça, bits extras, aleatoriedade e determinados procedimentos são realizados para consolidar uma checagem de espionagem. Como mostrado na Seção IV, isto culmina em uma probabilidade desprezível de sucesso do espião.

Este trabalho contribui para o uso de DFSs em comunicações seguras. Se o espião é passivo, o modelo de canais *wiretap* quânticos [18], [19] pode ser utilizado para consolidar segurança incondicional nas comunicações [20], [21]. Este cenário, entretanto, nem sempre ocorre e é essencial considerar outros protocolos e técnicas. Uma vez que os DFSs surgem onde há descoerência coletiva [22], outros trabalhos na literatura já propuseram protocolos QKD para canais quânticos com defasamento e rotação coletivos [7], [8]. Apesar do canal de decaimento coletivo de amplitude possuir DFS, não havia registro de protocolo QKD na literatura para este canal.

Em cenários práticos, alguns trabalhos já reportam implementações de canais quânticos com DFSs [23]–[25], inclusive para uso em longas distâncias [26]. Com estas tecnologias já existentes, o protocolo proposto pode ser adotado em cenários realísticos para promover a realização de comunicações seguras.

Em trabalhos futuros, almeja-se a proposição de outros protocolos e técnicas para comunicações seguras em canais quânticos espionados e ruidosos.

Referências

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

[2] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," in *Int. Conf. Computers, Systems & Signal Processing, Bangalore, India*.

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

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

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

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

[7] J.-C. Boileau, D. Gottesman, R. Laflamme, D. Poulin, and R. W. Spekkens, "Robust Polarization-Based Quantum Key Distribution over a Collective-Noise Channel," *Phys. Rev. Lett.*, vol. 92, p. 017901, 2004.

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

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

[10] D. A. Lidar and K. B. Whaley, "Decoherence-Free Subspaces and Subsystems," arXiv:quant-ph/0301032v1, pp. 83–120, 2003.
[11] P. Dirac, *The principles of Quantum Mechanics*, 4th ed., O. U. Press, Ed. Oxford UK, 1982, iSBN 0198520115.
[12] C. Paar and J. Pelzl, *Understanding Cryptography*, Springer, Ed. Springer, 2010.
[13] M. N. Wegman and J. L. Carter, "New Hash Function and their Use in Authentication and Set Equality," *J. Comput. Syst. Sci.*, vol. 22, pp. 265–279, 1981.
[14] W. K. Wootters and W. H. Zurek, "A Single Quantum Cannot be Cloned," *J. Comput. Syst. Sci.*, vol. 299, pp. 802–803, 1982.
[15] D. Kalamidas, "Single-Photon Quantum Error Rejection and Correction With Linear Optics," *Phys. Lett. A*, vol. 343, pp. 331–335, 2005.
[16] J. Mullins, "Making Unbreakable Code," *IEEE Spectrum*, vol. May, pp. 40–45, 2002.
[17] ID Quantique, "Quantum key distribution," http://www.idquantique.com/network-encryption/products/network-encryption-overview.html, 2014.
[18] N. Cai, A. Winter, and R. W. Yeung, "Quantum privacy and quantum wiretap channels," *Problems of Information Transmission*, vol. 40, pp. 318–336, 2004.
[19] 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.
[20] E. B. Guedes and F. M. de Assis, "Utilização de subespaços livres de descoerência em comunicações quânticas incondicionalmente seguras," Brasília, 2012, in Simpósio Brasileiro de Telecomunicações – SBrT'12.
[21] ——, "Unconditional security with decoherence-free subspaces," arXiv:quant-ph/1204.3000, pp. 1–6, 2012.
[22] P. Zanardi and M. Rasetti, "Noiseless quantum codes," *Phys. Rev. Lett.*, vol. 79, p. 3306, 1997.
[23] G. Jaeger and A. Sergienko, "Constructing four-photon states for quantum communication and information processing," *Int. J. Theor. Phys.*, vol. 47, p. 2120, 2008.
[24] U. Dorner, A. Klein, and D. Jaksch, "A quantum repeater based on decoherence free subspaces," *Quant. Inf. Comp.*, vol. 8, p. 468, 2008.
[25] 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.
[26] P. Xue, "Long-distance quantum communication in a decoherence-free subspace," *Phys. Lett. A*, vol. 372, pp. 6859–6866, 2008.