Universidade Federal de São Carlos
Departamento de Física

Análise de segurança de criptografia quântica baseada em teletransporte

Diogo Henrique Garcia Lima

Orientador: Prof. Dr. Gustavo Garcia Rigolin

São Carlos, fevereiro de 2021.

Universidade Federal de São Carlos
Departamento de Física

Análise de segurança de criptografia quântica baseada em teletransporte

Diogo Henrique Garcia Lima

Tese realizada sob a orientação do Prof. Dr. Gustavo Garcia Rigolin, apresentada ao Departamento de Física da Ufscar em preenchimento parcial dos requisitos para a obtenção do grau de Doutor em Física.

São Carlos, fevereiro de 2021.

Lima, Diogo Henrique Garcia

Análise de segurança de criptografia quântica baseada em teletransporte / Diogo Henrique Garcia Lima -- 2021.
98f.

Tese de Doutorado - Universidade Federal de São Carlos, campus São Carlos, São Carlos
Orientador (a): Prof. Dr. Gustavo Garcia Rigolin
Banca Examinadora: Prof. Dr. Gustavo Garcia Rigolin, Prof. Dr. Leonardo Kleber Castelano, Prof. Dr. Antonio Vidiella Barranco, Prof. Dr. Diogo de Oliveira Soares Pinto, Prof. Dr. Marcio Fernando Cornelio
Bibliografia

1. Criptografia quântica. 2. Teletransporte quântico. 3. Comunicação quântica. I. Lima, Diogo Henrique Garcia. II. Título.

Ficha catalográfica desenvolvida pela Secretaria Geral de Informática (SIn)

DADOS FORNECIDOS PELO AUTOR

Bibliotecário responsável: Ronildo Santos Prado - CRB/8 7325

UNIVERSIDADE FEDERAL DE SÃO CARLOS

Centro de Ciências Exatas e de Tecnologia
Programa de Pós-Graduação em Física

Folha de Aprovação

Defesa de Tese de Doutorado do candidato Diogo Henrique Garcia Lima, realizada em 04/02/2021.

Comissão Julgadora:

Prof. Dr. Gustavo Garcia Rigolin (UFSCar)

Prof. Dr. Leonardo Kleber Castelano (UFSCar)

Prof. Dr. Antonio Vidiella Barranco (IFI UNICAMP)

Prof. Dr. Diogo de Oliveira Soares Pinto (USP)

Prof. Dr. Marcio Fernando Cornelio (UFMT)

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.
O Relatório de Defesa assinado pelos membros da Comissão Julgadora encontra-se arquivado junto ao Programa de Pós-Graduação em Física.

It may be that you are not yourself luminous, but you are a conductor of light.
Sir Arthur Conan Doyle

Agradecimentos

Ao final desta etapa foi possível agregar muito a meu intelecto científico. E a isso devo agradecer a meu orientador Prof. Dr. Gustavo Garcia Rigolin pelas inúmeras e extensas discussões. Agradeço-o por me instruir no caminho ciêntifico, sobre o futuro da ciência, e por irmos muito além da física abordando conceitos econômicos e filosóficos. Registro aqui meu sincero agredecimento e respeito por todos esses anos de dedicação. Muito obrigado. Agradeço também a meu amigo Rafael Vieira pelas discussões e colaboração a elucidar temas na época ainda obscuros.

E fora da vida acadêmica, muito devo a minha esposa Hosana Ribeiro de Novaes e meus enteados Mateus, Maria Eduarda, Marcos, Marlon e Vitória por me acompanharem nessa jornada. Agradeço também a meus pais, Luiz e Maria, pelo apoio e incentivo. E a meus irmãos e cunhados Douglas, Stefani, Danny e Alan pela curiosidade e interesse no meu trabalho.

Por fim, agradeço a Capes e ao departamento de física da UFSCar pelo suporte financeiro e estrutural.

Resumo

Nesta Tese provamos que o protocolo de criptografia quântica GR10 [Opt. Commun. **283**, 184 (2010)], o qual por meio do teletransporte quântico utiliza somente estados ortogonais para codificar os bits clássicos da mensagem, é seguro assintoticamente contra todos tipos de ataques individuais e coletivos. Investigamos, então, modificações no protocolo GR10, as quais levaram a um aumento de sua eficiência e também a sua segurança contra ataques coerentes. Em outras palavras, mostramos a segurança incondicional de um protocolo de distribuição de chaves quânticas que não precisa de estados quânticos não ortogonais para codificar a chave secreta enviada de Alice a Bob. Conforme veremos, a razão para obtermos um protocolo seguro mesmo usando estados ortogonais tem sua origem no uso do teletransporte quântico para enviar os *qubits* que codificam a chave criptográfica de Alice para Bob. Revisitamos, também, a demonstração da segurança do BB84, explorando a decomposição de Schmidt expandida em diferentes bases ortonormais. Isto nos permitiu a elevar o limiar da taxa de erro, quando comparado à análise de segurança padrão, abaixo do qual o protocolo BB84 continua operando seguramente. Finalmente estudamos como os diferentes tipos de ruídos, normalmente presentes em situações realistas, afetam a segurança do protocolo BB84.

Abstract

We prove that the teleportation based quantum cryptography protocol presented in [Opt. Commun. **283**, 184 (2010)], which is built using only orthogonal states encoding the classical bits that are teleported from Alice to Bob, is asymptotically secure against all types of individual and collective attacks. We then investigate modifications to that protocol leading to greater secret-key rates and to security against coherent attacks. In other words, we show an unconditional secure quantum key distribution protocol that does not need non-orthogonal quantum states to encode the bits of the secret key sent from Alice to Bob. We also revisit the security proof of the BB84 protocol by exploring the non-uniqueness of the Schmidt decomposition of its entanglement-based representation. This allows us to arrive at a secure transmission of the key for a slightly greater quantum bit error rate (quantum communication channel's noise) when compared to its standard security analysis. After that, we investigate how different types of the noise usually present in realistic implementations of the BB84 protocolo affect its operation.

Notação e Convenção

Nesta Tese, utilizamos amplamente funções que dependem de estados quânticos, funções que dependem dos resultados das medidas associadas a um estado quântico e também funções que dependem dos estados quânticos e dos resultados das medidas dos estados quânticos. Sendo assim, para diferenciarmos estes três casos, estabelecemos o seguinte padrão de notação.

Seja o operador densidade ρ^A um estado quântico descrevendo o sistema A. Os resultados de qualquer medida efetuada no sistema A são dados pela variável aleatória A. Dessa forma, definimos:

$$\begin{aligned} f(A) &\equiv \text{função da variável aleatória } A, && (1)\\ f(\rho^A) &\equiv \text{função do estado quântico que descreve o sistema } A, && (2)\\ f(A:\rho^B) &\equiv \text{função da variável aleatória } A \text{ e do estado quântico que descreve} \\ &\quad \text{o sistema } B. && (3) \end{aligned}$$

Para simplificar a notação, consideramos que

$$\log(x) \equiv \log_2(x),$$
$$\ln(x) \equiv \log_{\mathrm{e}}(x).$$

Além disso, um estado do sistema A, $|a\rangle_A$, cujo adjunto é ${}_A\langle a|$, ao expressarmos na forma de um operador densidade consideramos que

$$|a\rangle_A \langle a| \equiv (|a\rangle_A)\,({}_A\langle a|)\,. \qquad (4)$$

As matrizes de Pauli são,

$$\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|, \tag{5}$$
$$\sigma_y = -\mathrm{i}\,|0\rangle\langle 1| + \mathrm{i}\,|1\rangle\langle 0|, \tag{6}$$
$$\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|, \tag{7}$$
$$\tag{8}$$

onde $|0\rangle$ e $|1\rangle$ são autoestados de σ_z. O operador $\mathbb{1}_A$ é o operador identidade com dimensão do espaço de Hilbert associado ao sistema A.

Por fim, em todos nossos cálculos, consideramos que os envolvidos na comunicação são Alice, Bob e Eva. Alice é a responsável por enviar a mensagem, Bob é responsável por recebê-la e a Eva é atribuída toda e qualquer interferência na comunicação entre Alice e Bob.

Sumário

Lista de Figuras

Capítulo 1

Introdução

No mundo de hoje, onde a quantidade de informação produzida, armazenada e transmitida aumentou para um nível sem precedentes, é de extrema importância a construção de maneiras para armazenar e transmitir informação seguramente, onde apenas as partes autorizadas podem acessar o conteúdo dos dados armazenados e transmitidos [1]. A criptografia é um campo de pesquisa interdisciplinar cujo objetivo principal é a construção de dispositivos e protocolos, de modo que a transmissão de informação possa ser feita de forma secreta, assim, impedindo que um espião (Eva) decifre a mensagem enviada de uma pessoa (Alice) para outra (Bob).

A solução padrão atualmente empregada por Alice para codificar uma mensagem, de modo que somente Bob possa decifrá-la, é baseada em protocolos de chave pública [2]. A segurança destes protocolos reside na suposição de que não existe um algoritmo eficiente para fatorar grandes números primos. Se esse algoritmo existisse, ele poderia ser adaptado para quebrar a segurança de todos os protocolos de criptografia de chave pública atuais. Apesar de não existir um algoritmo clássico conhecido que possa fatorar eficientemente números primos de qualquer tamanho, esse não é o caso quanticamente [3]. A prova de que um computador quântico pode fatorar eficientemente grandes números foi o principal fator que impulsionou o campo da criptografia quântica, que já havia oferecido uma solução alternativa para garantir a comunicação segura [4] cerca de dez anos antes do trabalho de Peter Shor [3].

O protocolo apresentado por Bennett e Brassard em 1984 [4], mais tarde chamado de protocolo BB84, foi a solução quântica para o principal problema associado à distribuição de chaves secretas. O principal problema da distribuição de chaves é basicamente a impossibilidade clássica de se ter 100% de certeza de que apenas duas pessoas, e mais ninguém,

concordam com uma sequência aleatória de bits que é enviada de uma pessoa para outra. A transmissão da chave de Alice para Bob por meios clássicos pode, em princípio, ser monitorada por uma Eva inteligente e poderosa o suficiente, que copie os bits aleatórios durante a transmissão sem nunca ser detectada por Alice e Bob. Este é o cenário ditado pela física clássica, na qual a cópia ou a clonagem de bits é sempre possível. No entanto, se usarmos estados quânticos não ortogonais para codificar os bits a serem transmitidos de Alice para Bob, pelas leis da mecânica quântica, nenhum monitoramento da transmissão pode adulterar a distribuição de chaves quânticas sem ser descoberto por Alice e Bob [4].

A solução quântica para o problema de distribuição de chaves criptográficas trouxe de volta à mesa os protocolos de criptografia clássicos de chave privada. São exemplos de protocolos clássicos de chave privada o protocolo de chaves de uso único (*one-time pad*) [1, 5] e o protocolo DES (*Data Encryption Standard*) [5] [1]. O protocolo one-time pad consiste em uma chave aleatória do tamanho da mensagem. Esta chave será utilizada somente uma vez e, após seu uso, ela é descartada. O *one-time pad* pode ser considerado incondicionalmente seguro se podemos garantir que a distribuição da chave criptográfica ocorreu de forma totalmente segura.

Agora, a distribuição da chave pode ser confirmada segura se ela ocorrer quanticamente usando o protocolo BB84 [2]. Além disso, uma vez que uma chave segura é estabelecida entre Alice e Bob, os protocolos de chave privada não se tornarão inseguros com o advento de um computador quântico. Esta é a principal razão que levou a expansão das pesquisas e desenvolvimento no campo da criptografia quântica nas últimas duas décadas [7–9], culminando com soluções de criptografia quântica comercialmente viáveis [10–12].

O conceito mais importante por trás de todos os esquemas usuais de distribuição de chaves quânticas é o uso de estados quânticos não ortogonais para codificar os bits clássicos 0 e 1 [13]. Esses bits são gerados aleatoriamente por Alice e codificados aleatoriamente em estados quânticos não ortogonais (qubits) que são enviados para Bob. Ao preparar e medir adequadamente esses *qubits*, Alice e Bob podem compartilhar uma sequência aleatória secreta de 0's e 1's. Ou seja, a chave secreta necessária à implementação de protocolos criptográficos de chave privada [3]. E como estados quânticos não ortogonais não podem ser clonados [14, 15], a transmissão de uma sequência aleatória de bits usando essa estratégia é segura de acordo com as leis da mecânica quântica.

[1] O protocolo DES apresentou vulnerabilidades limitando sua aplicação [6].

[2] Vale lembrar que classicamente a distribuição de chaves foi considerada insegura devido a impossibilidade de se detectar se um espião teve acesso a chave ou não.

[3] Alice e Bob também devem compartilhar um canal clássico autenticado, podendo ser totalmente inseguro, para realizar a distribuição de chaves.

O que acontece se os *qubits* que codificam os bits da chave secreta não são enviados fisicamente, mas teleportados de Alice para Bob [16]? Por um lado, podemos pensar nesse processo como uma substituição ao envio direto dos *qubits* de Alice para Bob através de um canal físico. Neste caso, o teletransporte de *qubits* é uma maneira alternativa de enviar para Bob as informações quânticas contidas nesses *qubits*, não desempenhando papel direto na geração da chave secreta. Além disso, nenhuma alteração qualitativa é feita nos protocolos de distribuição de chaves quânticas, seja quando usamos o protocolo de teletransporte quântico como um substituto para transmissão direta dos *qubits* ou quando usamos o teletransporte para aumentar a distância física entre Alice e Bob na qual eles ainda podem estabelecer uma chave secreta [17].

Por outro lado, podemos usar o protocolo de teletransporte quântico como ingrediente principal para a construção de um protocolo de distribuição de chaves quânticas, de modo que o protocolo de teletransporte desempenhe um papel *ativo* na geração da chave. Este papel ativo do protocolo de teletransporte na geração da chave é a principal característica da distribuição de chaves criptográficas quânticas do protocolo originalmente apresentado na Ref. [18], a partir de agora chamado de protocolo GR10. Além disso, o protocolo GR10 possui duas outras características interessantes. Primeiro, ele é seguro mesmo quando Alice e Bob usam estados parcialmente emaranhados para implementar o protocolo de teletransporte quântico [19–27]. Segundo, os bits clássicos da chave secreta podem ser codificados em dois estados *ortogonais* que são posteriormente teleportados de Alice para Bob. Este último recurso contrasta com o padrão usual de distribuição de chaves quânticas, onde o uso de estados quânticos não ortogonais para codificar os bits da chave são obrigatórios [4]. Há outros esquemas de distribuição de chaves criptográficas quânticas onde apenas estados ortogonais são utilizados em sua execução [30–32]. No entanto, nenhum deles se utiliza o teletransporte quântico.

Embora até o momento nenhuma falha de segurança tenha sido encontrada no protocolo GR10, uma análise rigorosa de sua segurança não foi feita. Um dos principais objetivos desta Tese é preencher essa lacuna, provando que o protocolo GR10 como originalmente concebido é seguro contra todos os tipos de ataques individuais e coletivos. Isso é mostrado no Cap. 7, onde também discutimos as principais razões qualitativas de sua segurança. Além disso, no Cap. 7 discutimos como o protocolo GR10 pode ser modificado para obtermos segurança incondicional assintótica, ou seja, segurança contra todos os tipos de ataques permitidos pelas leis da Física. Porém, antes de abordar a análise de segurança

[4] Também podemos usar estados maximamente emaranhados para criar uma chave secreta compartilhada por Alice e Bob sem enviar ou teletransportar *qubits* de Alice para Bob [28, 29].

do protocolo GR10, revisitamos detalhadamente a análise de segurança do protocolo BB84 no Cap. 4, apresentando as principais ferramentas necessárias para lidar com a análise de segurança do protocolo GR10. No Cap. 6 mostramos que, usando uma base diferente para a decomposição de Schmidt, podemos escrever a purificação do protocolo BB84 de tal maneira que seja possível provar sua segurança para taxas de erros (nivel de ruído) superiores às previstas pela análise de segurança usual, conforme descrita no o Cap. 4. No Cap. 7 modificamos o protocolo GR10 original, transformando-o em um protocolo determinístico. Com o intuito de manter esta Tese o mais autocontida possível, revisitamos no Cap. 3 o funcionamento dos protocolos de distribuição de chaves criptográficas aqui utilizados, isto é, os protocolos BB84 e GR10. E antes disso, no Cap. 2, apresentamos uma introdução à teoria da informação e as ferramentas matemáticas necessárias para realizarmos as análises de segurança nos capítulos seguintes. Mais adiante, no Cap. 8, analisamos como se comporta a transmissão segura de informação em determinados canais ruidosos. E no Cap. 9, apresentamos nossas observações finais. Ou seja, na Parte I desta Tese revisamos os conceitos, os protocolos e as técnicas de segurança apresentados na literatura relevantes ao nosso estudo. Posteriormente, na Parte II, apresentamos nossos resultados originais.

Parte I

Conceitos, protocolos e técnicas

Capítulo 2

Teoria da informação

Antes de prosseguirmos para os protocolos de criptografia quântica e suas respectivas análises de segurança, vamos introduzir os conceitos fundamentais para a obtenção desses resultados. O foco deste capítulo é realizar uma coletânea das ferramentas necessárias e dispersas em livros textos [33, 34] e artigos [8, 35, 36], colocando tudo em único lugar com uma notação padronizada para fácil compreensão e referência. Portanto, este capítulo tende a ser mais técnico, com várias definições fundamentais e demonstrações detalhadas de muitos teoremas. Com isso em mente, a primeira questão que podemos nos fazer é: o que é a teoria da informação?

Podemos dizer que a teoria da informação surgiu para trazer à luz problemas relacionados à teoria da comunicação. São eles: o quanto é possível comprimir os dados e qual a capacidade de um canal de comunicação [37]. O primeiro questiona o quanto é possível compactar, transmitir e recuperar uma mensagem, e a resposta para isso é a entropia de Shannon [38] discutida adiante. O segundo questiona a taxa de transmissão da informação de um canal, cuja resposta é a capacidade C do canal [37]. Não abordaremos nesta Tese esse segundo ponto.

Nas seções seguintes apresentaremos uma breve introdução da teoria da informação clássica. Nela, o principal conceito que vamos utilizar é a informação mútua, que pode ser escrita em função da entropia de Shannon e da entropia condicional. Posteriormente, adentraremos nos conceitos da teoria da informação quântica, pois a partir dela será possível calcularmos a segurança do protocolo de criptografia quântica GR10 utilizando a quantidade de Holevo.

2.1 Teoria da informação clásssica

Classicamente, a informação é quantificado pela entropia de Shannon $H(X)$ [38]:

$$H(X) \equiv -\sum_{x=1}^{d} p_X(x) \log[p_X(x)], \tag{2.1}$$

com $0 \cdot \log 0 = 0$. Esta última definição está de acordo com o fato que $\lim_{p\to 0} p \log p = 0$.

Na Eq. (2.1) X é uma variável aleatória e $p_X(x)$ é a probabilidade de se obter o resultado x para esta variável. A entropia de Shannon, também chamada como entropia clássica marginal, além de informar a quantidade mínima de bits necessários para enviar uma informação, ela mensura a *surpresa* proveniente de um evento ocorrer. Nada melhor que um exemplo para compreendermos o significado da surpresa no resultado da medida.

Considere o lançamento de uma moeda. Se para essa moeda temos a mesma probabilidade de se obter cara ou coroa, $P_X(\text{cara}) = P_X(\text{coroa}) = 1/2$, vemos que a entropia de Shannon é 1 pela Eq. (2.1). Agora, uma moeda cujo resultado é sempre *cara*, $P_X(\text{cara}) = 1$ e $P_X(\text{coroa}) = 0$, temos que o valor da entropia de Shannon é nulo. O que podemos compreender deste exemplo é que quando sabemos o resultado de um evento não ganhamos nenhuma informação ao observá-lo, logo a entropia de Shannon é zero. No outro caso, onde o resultado é inesperado, ganhamos 1 bit de informação ao descobrirmos o resultado. O fato de o evento ser inesperado nos permite obter mais informação do que possuíamos anteriormente. E quanto mais equiprováveis os eventos, maior será a quantidade de informação obtida. O exemplo citado possui somente dois elementos no espaço amostral, $P_X(\text{cara})$ e $P_X(\text{coroa})$. Considerando que a probabilidade de se obter cara é x, $P_X(\text{cara}) = x$, claramente $P_X(\text{coroa}) = 1 - x$. Portanto, a entropia de Shannon, Eq. (2.1), reduz-se a

$$h(x) = -x \log(x) - (1 - x) \log(1 - x). \tag{2.2}$$

A equação anterior é um resultado amplamente utilizado na teoria de informação, e ela é denominada entropia binária. Em outras palavras, a Eq. (2.2) é a entropia de Shannon quando recaímos em somente dois eventos prováveis.

Quando possuímos mais de uma variável aleatória envolvida no evento, por exemplo X e Y, temos outras definições de entropias [33, 37]. O primeiro caso é quando temos probabilidades conjuntas, $p_{X,Y}(x, y)$, isto é, a probabilidade de se obter o resultado x e y.

Neste cenário temos a entropia conjunta de X e Y, a qual é definida como se segue,

$$H(X,Y) \equiv -\sum_{x,y} p_{X,Y}(x,y) \log \left[p_{X,Y}(x,y)\right]. \tag{2.3}$$

Perceba que a entropia conjunta nada mais é do que a entropia de Shannon, Eq. (2.1), com as probabilidades $p_X(x)$ sendo $p_{X,Y}(x,y)$. A entropia conjunta $H(X,Y)$ mensura a quantidade de informação que se obtém nos eventos X e Y simultaneamente. Note, também, que $p_{X,Y}(x,y) = p_X(x)p_{Y|X}(y|x) = p_Y(y)p_{X|Y}(x|y)$ pela teoria das probabilidades [37]. A probabilidade condicional $p_{X|Y}(x|y)$ é a probabilidade de x ocorrer dado que y ocorreu e com isso podemos definir a entropia condicional

$$H(X|Y) \equiv -\sum_{x,y} p_{X|Y}(x|y) \log \left[p_{X|Y}(x|y)\right]. \tag{2.4}$$

A entropia condicional $H(X|Y)$ mensura a incerteza da variável aleatória X sendo que o resultado de Y é conhecido. Analogamente $H(Y|X)$ é a incerteza em Y dado o resultado de X evidente.

Por fim, o elemento mais importante que iremos utilizar da teoria da informação clássica é o quanto de informação dois eventos aleatórios compartilham entre si. Este valor é dado pela informação mútua e ela é definida como se segue,

$$I(X:Y) \equiv H(X) + H(Y) - H(X,Y). \tag{2.5}$$

Perceba que $I(X:Y) = I(Y:X)$, e podemos reescrevê-la como,

$$\begin{aligned} I(X:Y) &= H(X) - H(Y|X) && (2.6)\\ &= H(Y) - H(X|Y) && (2.7)\\ &= \sum_{x,y} p_{X,Y}(x,y) \log \left[\frac{p_{X,Y}(x,y)}{p_X(x)p_Y(y)}\right]. && (2.8) \end{aligned}$$

Demonstração. Para provar as Eqs. (2.6) e (2.7) iremos utilizar a seguinte propriedade da entropia conjunta, Eq. (2.3):

Lema 2.1. *A entropia conjunta pode ser escrita como a soma da entropia de Shannon*

com a entropia condicional,

$$H(X,Y) = H(X) + H(Y|X) \tag{2.9}$$
$$= H(Y) + H(X|Y). \tag{2.10}$$

Demonstração. A propriedade é validada utilizando que $p_{X,Y}(x,y) = p_X(x)p_{Y|X}(y|x)$ e que $\sum_x p_{X|Y}(x|y) = 1$ da teoria das probabilidades [37]. Assim, da definição de entropia conjunta, Eq. (2.3), temos

$$H(X,Y) = \sum_{x,y} p_{X,Y}(x,y) \log\left[p_X(x)p_{Y|X}(y|x)\right] \tag{2.11}$$
$$= \sum_{x,y} p_{X,Y}(x,y) \log\left[p_X(x)\right] + \sum_{x,y} p_{X,Y}(x,y) \log\left[p_{Y|X}(y|x)\right] \tag{2.12}$$
$$= \sum_{x} p_X(x) \left[\sum_{y} p_{Y|X}(y|x)\right] \log\left[p_X(x)\right] + \sum_{x,y} p_{X,Y}(x,y) \log\left[p_{Y|X}(y|x)\right] \tag{2.13}$$
$$= \sum_{x} p_X(x) \log\left[p_X(x)\right] + \sum_{x,y} p_{X,Y}(x,y) \log\left[p_{Y|X}(y|x)\right] \tag{2.14}$$
$$= H(X) + H(Y|X). \tag{2.15}$$

Confirmando assim a Eq. (2.9). Para provar a Eq. (2.10) basta refazer os cálculos acima com $p_{X,Y}(x,y) = p_Y(y)p_{X|Y}(x|y)$. □

Consequentemente, aplicando as Eq. (2.9) e (2.10) na definição de informação mútua, Eq. (2.5), obtemos as Eqs. (2.6) e (2.7). No entanto, para obtermos a informação mútua conforme a Eq.(2.8), usaremos que $\sum_y p_{Y|X}(y|x) = 1$. Com isso temos que a entropia de Shannon pode ser escrita como,

$$H(X) = -\sum_{x} p_X(x) \left[\sum_{y} p_{Y|X}(y|x)\right] \log\left[p_X(x)\right] \tag{2.16}$$
$$= -\sum_{x,y} p_X(x)p_{Y|X}(y|x) \log\left[p_X(x)\right] \tag{2.17}$$
$$= -\sum_{x,y} p_{X,Y}(x,y) \log\left[p_X(x)\right]. \tag{2.18}$$

Como $p_{Y,X}(y,x) = p_{X,Y}(x,y)$, refazendo os cálculos anteriores com $\sum_x p_{X|Y}(x|y) = 1$, obtemos

$$H(Y) = -\sum_{x,y} p_{X,Y}(x,y) \log\left[p_Y(y)\right]. \tag{2.19}$$

Substituindo as Eqs. (2.18) e (2.19) na Eq. (2.5) resulta em,

$$
\begin{aligned}
I(X:Y) &= -\sum_{x,y} p_{X,Y}(x,y)\log\left[p_X(x)\right] - \sum_{x,y} p_{X,Y}(x,y)\log\left[p_Y(y)\right] && (2.20)\\
&\quad + \sum_{x,y} p_{X,Y}(x,y)\log\left[p_{X,Y}(x,y)\right] && (2.21)\\
&= \sum_{x,y} p_{X,Y}(x,y)\left\{-\log\left[p_X(x)\right] - \log\left[p_Y(y)\right] + \log\left[p_{X,Y}(x,y)\right]\right\} && (2.22)\\
&= \sum_{x,y} p_{X,Y}(x,y)\log\left[\frac{p_{X,Y}(x,y)}{p_X(x)p_Y(y)}\right], && (2.23)
\end{aligned}
$$

provando a Eq. (2.8) □

A partir das Eqs. (2.6)-(2.8) podemos dizer que a informação mútua é a correlação entre os eventos X e Y. A relação das entropias envolvidas pode ser melhor compreendida analisando o diagrama de Venn, fig. 2.1, onde temos que a informação mútua é a intersecção dos conjuntos representando o quão relacionados dois eventos aleatórios X e Y estão.

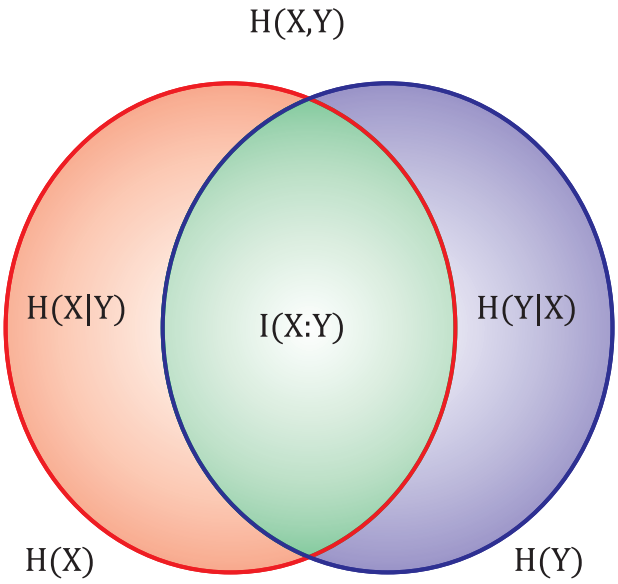

Figura 2.1: Diagrama de Venn relacionando entropia marginal ($H(X)$ e $H(Y)$), conjunta ($H(X,Y)$), condicional ($H(X|Y)$ e $H(Y|X)$) e também informação mútua ($I(X:Y)$). Note que a informação mútua é a intersecção entre as entropias marginais. Figura extraída de [37].

2.2 Teoria da informação quântica

Na mecânica quântica, os sistemas físicos podem ser descritos por um operador densidade, veja apêndice A para uma breve discussão sobre operadores quânticos. A quantidade de informação que pode ser extraída de um sistema físico é calculada através desses operadores. De modo análogo ao que ocorre na teoria da informação clássica, as entropias quânticas mensuram a quantidade de informação em sistemas quânticos. Para melhor compreendermos essas entropias quânticas e suas propriedades vamos apresentá-las separadamente. A análise que se segue é baseada nos livros textos [33] e [34]. Vale ressaltar que os conceitos apresentados nesta seção são fundamentais para que possamos realizar a análise de segurança de protocolos quânticos de distribuição de chaves criptográficas.

Em princípio, a máxima quantidade de informação que pode ser extraída de um sistema quântico é determinada pela entropia de von Neumann [40]. Esta entropia é uma função do operador densidade do sistema e é definida como se segue,

Definição 2.1. *Seja um sistema quântico A descrito pelo estado ρ^A. Sua entropia de von Neumann é*

$$S(\rho^A) \equiv -\mathrm{tr}\left\{\rho^A \log\left(\rho^A\right)\right\}. \tag{2.24}$$

Aqui $\mathrm{tr}\{\}$ denota o traço do operador, e algumas de suas propriedades são apresentadas no apêndice A. A entropia de von Neumann pode ser facilmente obtida através da decomposição espectral de ρ. Neste caso, $f(\rho)$ nada mais é que $\sum_i f(\lambda_i) |i\rangle \langle i|$, onde λ_i são os autovalores de ρ e $|i\rangle$ seus autoestados [34]. Assim, se $\rho^A = \sum_a \lambda_a |a\rangle \langle a|$, temos que $S(\rho^A) = -\sum_a \lambda_a \log \lambda_a$, que é a entropia de Shannon (2.1) para $p_A(a) = \lambda_a$. A entropia de von Neumann possui as seguintes propriedades:

Propriedade 2.1 (Positividade)**.** *A entropia quântica é sempre positiva, sendo nula quando a matriz densidade for um estado puro.*

$$S(\rho) \geq 0. \tag{2.25}$$

Demonstração. Considerando o operador densidade em sua decomposição espectral, $\rho = \sum_i \lambda_i |i\rangle \langle i|$, temos $S(\rho) = \sum_i \lambda_i \log \frac{1}{\lambda_i}$. Mas uma matriz densidade possui o traço unitário e seus autovalores positivos (veja apêndice A). Então que $\sum_i \lambda_i = 1$ com $0 \leq \lambda_i \leq 1$. Assim, $\log \frac{1}{\lambda_i} > 0$. Portanto, $S(\rho)$ é a soma de números positivos, provando o teorema. Considerando agora ρ um estado puro, $\lambda_i = 1$ e $\lambda_j = 0$ para todo $j \neq i$. Com isso,

$S(\rho) = -1\log 1 + (-0\log 0 - 0\log 0 - \cdots)$. Como $\log 1 = 0$ e $0\log 0 \equiv 0$ temos $S(\rho) = 0$ se ρ for estado puro. □

Propriedade 2.2 (Invariância sobre transformação unitária)**.** *A entropia de um operador densidade se conserva para uma transformação unitária* $\mathbf{U}$ *aplicada sobre ele,*

$$S(\rho) = S(\mathbf{U}\rho\mathbf{U}^\dagger) \tag{2.26}$$

Demonstração. A entropia de von Neumann é invariante, pois, podemos escrevê-la como a entropia de Shannon dos autovalores do operador densidade. Então, para provar a Eq. (2.26) basta provar que os autovalores são invariantes por transformações unitárias, consequentemente a entropia de von Neumann também o será.

Considere uma transformação unitária $\rho' = \mathbf{U}\rho\mathbf{U}^\dagger$. Os autovalores de ρ' são obtidos a partir da equação característica originada do determinante $\det[\rho' - \lambda I] = 0$, que pode ser reescrito como $\det[\mathbf{U}(\rho - \lambda I)\mathbf{U}^\dagger] = 0$. Sabendo que o determinante do produto é o produto dos determinantes, podemos reduzir a equação a $\det[\mathbf{U}]\det[\mathbf{U}^\dagger]\det[\rho - \lambda I] = 0$. Como podemos escrever $\det[\mathbf{U}]\det[\mathbf{U}^\dagger] = \det[\mathbf{U}\mathbf{U}^\dagger] = \det[I] = 1$, temos $\det[\rho - \lambda I] = 0$, a mesma equação para obter os autovalores de ρ antes de qualquer transformação unitária. Dessa forma, temos que a equação característica para obter os autovalores de um operador que sofreu uma transformação unitária é a mesma equação para obter os autovalores do operador sem nenhuma transformação. Isto resulta que os autovalores são os mesmos.

□

Antes de apresentarmos outras propriedades da entropia de von Neumann, vamos introduzir a definição da entropia relativa, $S(\rho||\sigma)$. Essa nova entropia e algumas de suas propriedades simplificarão as demonstrações das propriedades posteriores.

Definição 2.2. *Para duas matrizes densidades* ρ *e* σ *a entropia relativa entre ambas é*

$$S(\rho||\sigma) \equiv \operatorname{tr}\{\rho\log\rho\} - \operatorname{tr}\{\rho\log\sigma\}. \tag{2.27}$$

Perceba que $S(\rho||\sigma)$ pode ser infinita, não é limitada superiormente, quando temos o autovalor de σ nulo enquanto os autovalores de ρ diferentes de zero. A entropia relativa é também não negativa e este é um resultado conhecido como *Desigualdade de Klein*:

Propriedade 2.3 (Desigualdade de Klein)**.** *A entropia relativa é não negativa,*

$$S(\rho||\sigma) \geq 0, \tag{2.28}$$

com a igualdade verificada somente se $\rho = \sigma$.

Demonstração. Considere $\sum_i p_i \left|i\right\rangle \left\langle i\right|$ e $\sum_j q_j \left|u_j\right\rangle \left\langle u_j\right|$ a decomposição espectral de ρ e σ respectivamente. Como ρ e σ são operadores densidade temos que $\sum_i p_i = \sum_j q_j = 1$, com p_i e q_j positivos. Então, usando que $f(\rho) = \sum_i f(p_i) \left|i\right\rangle \left\langle i\right|$ e $f(\sigma) = \sum_j f(q_j) \left|u_j\right\rangle \left\langle u_j\right|$, ao tomarmos o traço na base em que ρ é diagonal temos

$$\begin{aligned} S(\rho||\sigma) &= \operatorname{tr}\{\rho \log \rho\} - \operatorname{tr}\{\rho \log \sigma\} \\ &= \sum_{i,k} p_i \log(p_i) \left\langle k|i\right\rangle \left\langle i|i\right\rangle \left\langle i|k\right\rangle - \sum_{i,j,k} p_i \log(q_j) \left\langle k|i\right\rangle \left\langle i|u_j\right\rangle \left\langle u_j|k\right\rangle \\ &= \sum_i p_i \log(p_i) - \sum_{i,j} p_i \log(q_j) \left|\left\langle i|u_j\right\rangle\right|^2. \end{aligned} \tag{2.29}$$

Chamando $\left|\left\langle i|u_j\right\rangle\right|^2 = P_{ij}$, e utilizando a concavidade do logaritmo, lema B.1 no apêndice B, podemos escrever a desigualdade $-\sum_j P_{ij} \log q_j \geq -\log\left(\sum_j P_{ij} q_j\right)$ pois de $P_{ij} \geq 0$ e $\sum_j P_{ij} = 1$. Desta forma, a Eq. (2.29) torna-se

$$\begin{aligned} S(\rho||\sigma) &= \sum_i p_i \left(\log p_i - \sum_j P_{ij} \log q_j\right), \\ &\geq \sum_i p_i \left[\log p_i - \log\left(\sum_j P_{ij} q_j\right)\right]. \end{aligned} \tag{2.30}$$

Por simplicidade, definimos agora $r_i = \sum_j P_{ij} q_j$ reduzindo a Eq. (2.30) a

$$\begin{aligned} S(\rho||\sigma) &\geq \sum_i p_i \left(\log p_i - \log r_i\right), \\ &= -\sum_i p_i \log\left(\frac{r_i}{p_i}\right), \end{aligned} \tag{2.31}$$

nos permitindo utilizar que $-\ln(x) \geq 1 - x$, resultado provado no lema B.6 no apêndice B. Aplicando este resultado na Eq. (2.31) obtemos que

$$\begin{aligned} S(\rho||\sigma) &\geq \frac{1}{\ln 2} \sum_i p_i \left(1 - \frac{r_i}{p_i}\right), \\ &= \frac{1}{\ln 2} \sum_{i,j} \left(p_i - P_{ij} q_j\right). \end{aligned} \tag{2.32}$$

Por fim, lembrando que $\sum_i P_{ij} = 1$, a Eq. (2.32) reduz-se a $\left(\sum_i p_i - \sum_j q_j\right) / \ln(2)$, que é

nulo pois $\sum_i p_i = \sum_j q_j = 1$, provando assim que a entropia relativa é não negativa. E mais, $S(\rho||\sigma) = 0$ ocorre somente quando temos $q_i = p_i$ e $\langle i|u_j\rangle = \delta_{i,j}$, conforme vemos analisando a Eq. (2.29). Ou seja, quando $\rho = \sigma$. □

Voltando agora as demais propriedades da entropia de von Neumann, Eq. (2.24), temos:

Propriedade 2.4 (Valor máximo)**.** *O máximo valor da entropia depende da dimensão do espaço de Hilbert da matriz densidade. Desse modo, se ρ um operador densidade que pertence ao espaço de Hilbert $\mathcal{H}$ com dimensão d temos*

$$S(\rho) \leq \log d. \tag{2.33}$$

Demonstração. O valor máximo da entropia pode ser obtido através da desigualdade de Klein, Eq. (2.28), e da definição da entropia relativa, Eq. (2.27):

$$\begin{aligned} S\left(\rho||\frac{I}{d}\right) &\geq 0, \\ \operatorname{tr}\{\rho\log\rho\} - \operatorname{tr}\left\{\rho\log\frac{I}{d}\right\} &\geq 0, \\ -S(\rho) - \operatorname{tr}\left\{\rho\log\frac{I}{d}\right\} &\geq 0, \\ S(\rho) &\leq \operatorname{tr}\{\rho\}\log d, \\ S(\rho) &\leq \log d. \end{aligned} \tag{2.34}$$

Note que a entropia de von Neumann é máxima quando temos um estado maximamente misto, isto é, $\rho = \frac{1}{d}I$. □

Propriedade 2.5 (Projeções aumentam a entropia)**.** *Considere um conjunto completo ortogonal de operadores de projeção P_i e um operador densidade ρ. Então, na entropia de von Neumann da nova matriz densidade $\rho' = \sum_i P_i\rho P_i$ verifica-se que*

$$S(\rho') \geq S(\rho). \tag{2.35}$$

Demonstração. Aplicando a desigualdade de Klein, Eq. (2.28), temos

$$
\begin{aligned}
S(\rho||\rho') &\geq 0, && (2.36)\\
-\mathrm{tr}\left\{\rho \log \rho'\right\} &\geq S(\rho), && (2.37)\\
-\sum_i \mathrm{tr}\left\{P_i P_i \rho \log \rho'\right\} &\geq S(\rho), && (2.38)\\
-\sum_i \mathrm{tr}\left\{P_i \rho \left(\log \rho'\right) P_i\right\} &\geq S(\rho), && (2.39)\\
-\sum_i \mathrm{tr}\left\{P_i \rho P_i \log \rho'\right\} &\geq S(\rho), && (2.40)\\
-\mathrm{tr}\left\{\rho' \log \rho'\right\} &\geq S(\rho), && (2.41)\\
S(\rho') &\geq S(\rho). && (2.42)
\end{aligned}
$$

Na terceira linha, Eq. (2.38), usamos que os projetores são um conjunto completo, $\sum_i P_i = 1$, e que também $P_i^2 = P_i$. Na linha seguinte, Eq. (2.39), aplicamos a invariância do traço perante permutações cíclicas. Por fim, como $\rho' P_i = P_i \rho'$ obtemos $(\log \rho')P_i = P_i(\log \rho')$ e com isso a Eq. (2.40). Para chegar à Eq. (2.41) usamos a definição de ρ' e com a definição da entropia de von Neumann chegamos à Eq. (2.42), finalizando o desenvolvimento da prova. □

Vale ressaltar que a Eq. (2.35) é válida para medidas projetivas.

2.2.1 Entropia Conjunta Quântica

Sabendo que há operadores densidade que descrevam mais de um sistema, temos que a quantidade de informação obtida desses operadores é dada pela entropia conjunta. Sem perda de generalidade, para uma matriz densidade ρ^{AB} a entropia conjunta $S(\rho^{AB})$ segue a mesma definição da entropia de von Neumann (2.24):

Definição 2.3 (Entropia Conjunta Quântica)**.** *Um sistema multipartido representado pelo operador densidade ρ^{AB} possui entropia conjunta como se segue,*

$$S(\rho^{AB}) = -\mathrm{tr}\left\{\rho^{AB} \log\left(\rho^{AB}\right)\right\}. \tag{2.43}$$

A intuição física para a entropia conjunta quântica é similar a interpretação da entropia quântica. Isto é, ela mensura a quantidade de informação contida no sistema como um todo. A entropia conjunta quântica $S(\rho^{AB})$ possui as mesmas propriedades apresentadas para a entropia marginal com a adição das seguintes propriedades:

Propriedade 2.6 (Subaditividade e desigualdade triangular)**.** *Considere um sistema quântico A e B com o operador densidade ρ^{AB}. Então a entropia conjunta obedece às desigualdades*

$$S(\rho^{AB}) \leq S(\rho^A) + S(\rho^B), \tag{2.44}$$
$$S(\rho^{AB}) \geq |S(\rho^A) - S(\rho^B)|. \tag{2.45}$$

A Eq. (2.44) é conhecida como sub-aditividade da entropia de von Neumann com a igualdade ocorrendo para sistemas não correlacionados, $\rho^{AB} = \rho^A \otimes \rho^B$. A outra, Eq. (2.45), é a desigualdade triangular da entropia, ou desigualdade de *Araki-Lieb*, com valor mínimo nulo ocorrendo quando ρ^{AB} for puro.

Demonstração. A prova da primeira parte é obtida aplicando-se a desigualdade de Klein, Eq.(2.28), considerando $\sigma = \rho^A \otimes \rho^B$. Pela Eq. (2.27), $S(\rho^{AB}||\sigma) \geq 0$ reduz-se a $S(\rho^{AB}) \leq -\mathrm{tr}\left\{\rho^{AB}\log(\sigma)\right\}$. Assim, calculando $-\mathrm{tr}\left\{\rho^{AB}\log(\sigma)\right\}$ para $\sigma = \rho^A \otimes \rho^B$:

$$\begin{aligned} -\mathrm{tr}\left\{\rho^{AB}\log\sigma\right\} &= -\mathrm{tr}\left\{\rho^{AB}\log\left(\rho^A\otimes\rho^B\right)\right\} \\ &= -\mathrm{tr}\left\{\rho^{AB}\left(\log\rho^A + \log\rho^B\right)\right\} \\ &= -\mathrm{tr}_A\left\{\rho^A\log\rho^A\right\} - \mathrm{tr}_B\left\{\rho^B\log\rho^B\right\} \\ &= S(\rho^A) + S(\rho^B). \end{aligned} \tag{2.46}$$

Na segunda linha usamos que os autovalores de um produto tensorial é o produto dos autovalores de cada sistema individual, $\sigma|A_iB_j\rangle = a_ib_j|A_iB_j\rangle$ (com $|A_iB_j\rangle$ autovetor de σ). Na terceira linha usamos que $\mathrm{tr}_{AB}\{\rho\} = \mathrm{tr}_A\{\mathrm{tr}_B\{\rho\}\}$, teorema A.3 do apêndice A, em conjunto com a definição da matriz reduzida, $\rho^A = \mathrm{tr}_B\{\rho\}$, teorema A.29. Assim,

$$\begin{aligned} -\mathrm{tr}\left\{\rho^{AB}\log\sigma\right\} &\geq S(\rho^{AB}), \\ S(\rho^A) + S(\rho^B) &\geq S(\rho^{AB}). \end{aligned} \tag{2.47}$$

A condição de igualdade, $S(\rho^{AB}) = S(\rho^A) + S(\rho^B)$, ocorre quando temos $\rho^{AB} = \rho^A \otimes \rho^B$. Para ver isso basta refazer o cálculo na Eq. (2.46) com $\rho^{AB} = \sigma = \rho^A \otimes \rho^B$. A condição de aditividade para produtos tensoriais nos permite obter a entropia em eventos que se repetem. Ou seja, $S(\rho^{\otimes n}) = nS(\rho)$. Neste caso, a entropia conjunta quântica é proporcional ao número de repetições do evento.

Na demonstração da segunda parte, Eq. (2.45), vamos utilizar o seguinte lema

Lema 2.2. *Seja ρ^{AB} um sistema puro bipartido qualquer. As entropias quânticas são iguais, isto é,*

$$S(\rho^A) = S(\rho^B), \tag{2.48}$$

enquanto a entropia conjunta quântica se anula

$$S(\rho^{AB}) = 0. \tag{2.49}$$

Demonstração. A prova é feita por meio da decomposição de Schmidt, Eq. (C.1), a qual diz que qualquer estado puro bipartido $|\phi\rangle_{AB}$ admite a seguinte decomposição,

$$|\phi\rangle_{AB} = \sum_i \sqrt{\lambda_i}\, |i\rangle_A\, |i\rangle_B\,. \tag{2.50}$$

Aqui, $|i\rangle_A$ denota os autovetores ortonormais do sistema A e $|i\rangle_B$ os autovetores ortonormais do sistema B. Assim, tomando o traço parcial de cada sistema, onde $\rho^{AB} = |\phi\rangle_{AB}\langle\phi|$, encontramos

$$\begin{aligned} \rho^A &= \sum_i \lambda_i\, |i\rangle_A \langle i|\,, \\ \rho^B &= \sum_i \lambda_i\, |i\rangle_B \langle i|\,. \end{aligned} \tag{2.51}$$

Os sistemas A e B possuem os mesmos autovalores, consequentemente $S(\rho^A) = S(\rho^B)$. Por fim, para ρ^{AB} puro temos um único autovalor unitário. Portanto, $S(\rho^{AB}) = S(|\phi\rangle_{AB}\langle\phi|) = 1\log 1 = 0$ pela definição da entropia quântica, Eq. (2.24). □

Retornando à demonstração da desigualdade triangular, considere uma purificação do sistema ρ^{AB} resultando em um novo operador densidade puro ρ^{ABR}. Para $S(\rho^B) \geq S(\rho^A)$, aplicando o lema 2.2 temos que $S(\rho^{AR}) = S(\rho^B)$ e $S(\rho^R) = S(\rho^{AB})$. Essas igualdades aplicadas na equação de subaditividade para $S(\rho^{AR})$, Eq. (2.44), resulta em

$$\begin{aligned} S(\rho^{AR}) &\leq S(\rho^A) + S(\rho^R), \\ S(\rho^B) &\leq S(\rho^A) + S(\rho^{AB}), \\ S(\rho^{AB}) &\geq S(\rho^B) - S(\rho^A). \end{aligned} \tag{2.52}$$

No caso de $S(\rho^A) \geq S(\rho^B)$ aplicamos $S(\rho^{BR}) = S(\rho^A)$ e $S(\rho^R) = S(\rho^{AB})$ resultando em $S(\rho^{AB}) \geq S(\rho^A) - S(\rho^B)$. Provando, assim, a desigualdade triangular, Eq. (2.45).

□

Propriedade 2.7 (Concavidade)**.** *Sendo o operador densidade de um sistema qualquer* $\rho \equiv \sum_x p_X(x)\rho_x$*, temos que a entropia quântica relacionada a esse operador é côncava, isto é,*

$$S(\rho) \geq \sum_x p_X(x) S(\rho_x). \tag{2.53}$$

Demonstração. Seja o operador em questão a representação de um sistema total A. Para realizar a prova, consideraremos um sistema auxiliar B cujos estados são ortonormais na base $\{|x\rangle\}$ correspondente ao índice x do operador densidade ρ_x. Dessa forma, o operador do sistema A em conjunto com o sistema B é

$$\rho^{AB} = \sum_x p_X(x)\rho_x^A \otimes |x\rangle_B \langle x| . \tag{2.54}$$

Aplicando o traço parcial para obter os operadores densidade de cada sistema resulta em $\rho^A = \sum_x p_X(x)\rho_x^A$ e $\rho^B = \sum_x p_X(x) |x\rangle_B \langle x|$. Portanto,

$$\begin{aligned} S(\rho^A) &= S\left(\sum_x p_X(x)\rho_x^A\right), \\ S(\rho^B) &= S\left(\sum_x p_X(x) |x\rangle_B \langle x|\right) = H(X), \end{aligned} \tag{2.55}$$

com $H(X)$ a entropia clássica, Eq. (2.1), pois os estados $|x\rangle_B$ são os autovetores do sistema B. Além disso, definindo que a decomposição espectral de ρ_x^A seja $\sum_j \lambda_x^j |u_j\rangle_A \langle u_j|$ e calculando explicitamente a entropia conjunta quântica encontramos,

$$\begin{aligned} S(\rho^{AB}) &= -\mathrm{tr}\left\{\sum_x p_X(x)\rho_x^A \otimes |x\rangle_B \langle x| \log\left[\sum_y p_X(y)\rho_y^A \otimes |y\rangle_B \langle y|\right]\right\}, \\ &= -\mathrm{tr}\left\{\sum_{x,j} p_X(x)\lambda_x^j |u_j\rangle_A \langle u_j| \otimes |x\rangle_B \langle x| \log\left[\sum_{y,k} p_X(y)\lambda_y^k |u_k\rangle_A \langle u_k| \otimes |y\rangle_B \langle y|\right]\right\}, \\ &= -\mathrm{tr}\left\{\sum_{x,y,j,k} p_X(x)\lambda_x^j \log\left[p_X(y)\lambda_y^k\right] |u_j\rangle_A \langle u_j|u_k\rangle_A \langle u_k| \otimes |x\rangle_B \langle x|y\rangle_B \langle y|\right\}, \end{aligned} \tag{2.56}$$

onde usamos que $f(\rho^A) = \sum_a f(E_a) |a\rangle \langle a|$ se $\rho^A = \sum_a E_a |a\rangle \langle a|$. Em outras palavras, a função de um operador é a função de cada autovalor na base que diagonaliza o operador. Na última linha da Eq. (2.56) temos que $\langle u_j|u_k\rangle_A = \delta_{jk}$ e $\langle x|y\rangle_B = \delta_{x,y}$. Assim, usando

que o logaritmo do produto é a soma dos logaritmos, a Eq. (2.56) pode ser escrita como

$$\begin{aligned} S(\rho^{AB}) &= -\mathrm{tr}\left\{\sum_{x,j} p_X(x)\lambda_x^j \log\left[p_X(x)\lambda_x^j\right] |u_j\rangle_A \langle u_j| \otimes |x\rangle_B \langle x|\right\}, \\ &= -\mathrm{tr}\left\{\left\{\sum_{x,j} p_X(x)\lambda_x^j \log\left[p_X(x)\right] + \sum_{x,j} p_X(x)\lambda_x^j \log\left(\lambda_x^j\right)\right\} |u_j\rangle_A \langle u_j| \otimes |x\rangle_B \langle x|\right\}. \\ &= -\left\{\sum_x p_X(x) \sum_j \lambda_x^j \log\left[p_X(x)\right] + \sum_{x,j} p_X(x)\lambda_x^j \log\left(\lambda_x^j\right)\right\} \mathrm{tr}\left\{|u_j\rangle_A \langle u_j| \otimes |x\rangle_B \langle x|\right\}. \end{aligned} \tag{2.57}$$

O traço da última linha da Eq. (2.57) é unitário, reduzindo a entropia conjunta a

$$S(\rho^{AB}) = -\sum_x p_X(x) \sum_j \lambda_x^j \log\left[p_X(x)\right] - \sum_{x,j} p_X(x)\lambda_x^j \log\left(\lambda_x^j\right). \tag{2.58}$$

Por fim, aplicando que $\sum_j \lambda_x^j = 1$ devido aos operadores possuírem traço unitário resulta que

$$S(\rho^{AB}) = -\sum_x p_X(x) \log\left(p_X(x)\right) + \sum_x p_X(x) \left[-\sum_j \lambda_x^j \log\left(\lambda_x^j\right)\right]. \tag{2.59}$$

Reconhecendo que o primeiro termo Eq. (2.59) é a entropia de Shannon para variável aleatória X, $H(X)$, e o termo entre colchetes é a entropia quântica do operador ρ_x^A, $S(\rho_x^A)$, a entropia conjunta pode ser reescrita da seguinte forma

$$S(\rho^{AB}) = H(X) + \sum_x p_X(x) S(\rho_x^A) \tag{2.60}$$

Finalizando a demonstração, aplicamos as Eqs. (2.60) e (2.55) na fórmula da subaditividade, $S(\rho^A) + S(\rho^B) \geq S(\rho^{AB})$, verificando assim a concavidade da entropia:

$$\begin{aligned} S\left(\sum_x p_X(x)\rho_x^A\right) + H(X) &\geq H(X) + \sum_x p_X(x) S(\rho_x^A), \\ S\left(\sum_x p_X(x)\rho_x^A\right) &\geq \sum_x p_X(x) S\left(\rho_x^A\right). \end{aligned} \tag{2.61}$$

□

Propriedade 2.8. *Suponha um operador densidade $\rho = \sum_x p_X(x)\rho_x$, com $p_X(x)$ probabi-*

lidades e ρ_x operadores densidades. Então:

$$S(\rho) \leq H(X) + \sum_x p_X(x) S(\rho_x), \tag{2.62}$$

com $H(X)$ sendo a entropia clássica da variável aleatória X definida pelas probabilidades $p_x(x)$.

Demonstração. Inicialmente, vamos considerar $\rho_x = |\psi_x\rangle \langle\psi_x|$ um estado puro. Suponha que ρ_x seja um operador densidade do sistema A, e B um sistema auxiliar com uma base ortonormal $|x\rangle$ correspondente ao índice x da probabilidade $p_X(x)$. Assim, definimos

$$|\psi\rangle_{AB} = \sum_x \sqrt{p_X(x)}\, |\psi_x\rangle_A |x\rangle_B . \tag{2.63}$$

Como o estado $|\psi\rangle_{AB}$ é puro, nós temos pelo lema 2.2 que $S(\rho^{AB}) = 0$ e que

$$S(\rho^A) = S(\rho^B) = S\left(\sum_x p_X(x) |\psi_x\rangle_A \langle\psi_x|\right) = S(\rho). \tag{2.64}$$

Note que $\rho^B = \sum_{x,y} \left(\sqrt{p_X(x) p_X(y)}\, \langle\psi_y|\psi_x\rangle\right) |x\rangle_B \langle y|$, pois os $|\psi_x\rangle$ não necessariamente são ortogonais. Suponha que apliquemos uma medida projetiva no sistema B na base $|x\rangle$, originando o sistema o sistema descrito por B'

$$\rho^{B'} = \sum_x p_X(x) |x\rangle \langle x| , \tag{2.65}$$

um operador densidade diagonal. Portanto, $S(\rho^{B'}) = H(X)$, a entropia clássica de Shannon. Lembrando que uma medida projetiva não diminui a entropia, Eq. (2.35), então

$$S(\rho^A) = S(\rho^B) \leq S(\rho^{B'}) = -\sum_x p_X(x) \log [p_X(x)] = H(X). \tag{2.66}$$

Como $S(\rho_x^A) = 0$ por termos $\rho_x^A = |\psi_x\rangle \langle\psi_x|$ definido inicialmente como puro, podemos escrever a partir da Eq. (2.66)

$$S(\rho^A) \leq H(X) + \sum_x p_X(x) S(\rho_x^A). \tag{2.67}$$

Agora, se ρ_x^A não for puro, o operador densidade torna-se $\rho^A = \sum_{x,j} p_X(x) \lambda_j^x |e_j^x\rangle_A \langle e_j^x|$, sendo $\sum_j \lambda_j^x |e_j^x\rangle_A \langle e_j^x|$ a decomposição espectral de ρ_x^A. Então, aplicando o resultado (2.66)

com as probabilidades $p_X(x) \to p_X(x)\lambda_j^x$ e sabendo que $\sum_j \lambda_j^x = 1$ pois $\mathrm{tr}\left\{\rho_x^A\right\} = 1$, resulta que

$$\begin{aligned} S(\rho^A) &\leq -\sum_{x,j} p_X(x)\lambda_j^x \log\left[p_X(x)\lambda_j^x\right] \\ &= -\sum_x p_X(x)\log\left[p_X(x)\right]\left(\sum_j \lambda_j^x\right) - \sum_x p_X(x)\sum_j \left(\lambda_j^x \log \lambda_j^x\right). \end{aligned} \tag{2.68}$$

Reconhecendo que $\sum_j \lambda_j^x = 1$, $-\sum_x p_X(x)\log\left[p_X(x)\right] = H(X)$, e $-\sum_j \lambda_j^x \log \lambda_j^x = S(\rho_x^A)$ a Eq. (2.68) torna-se

$$S(\rho) \leq H(X) + \sum_x p_X(x) S(\rho_x), \tag{2.69}$$

onde usamos a Eq. (2.64) para identificar $S(\rho^A)$ com $S(\rho)$.

É importante ressaltar que a igualdade ocorre quando $B = B'$, isto é, quando temos $|\psi_x\rangle$ ortogonais. Assim para um operador densidade sendo $\rho = \sum_x p_X(x)\,|x\rangle\langle x| \otimes \rho_x$ a entropia conjunta é exatamente $S(\rho) = H(X) + \sum_x p_X(x) S(\rho_x)$. □

2.2.2 Entropia Condicional Quântica

A entropia condicional quântica $S(\rho^A|\rho^B)$ mensura a ignorância que Bob, portador do estado B, tem sobre o estado A que Alice possui, sendo que Bob já conhece o resultado de B. Do mesmo modo, $S(\rho^B|\rho^A)$ é a ignorância de Alice sobre os estados de Bob sendo que ela conhece o resultado de A. Em outras palavras, é a ignorância que se possui sobre uma parte do sistema conhecendo a informação sobre a outra. Sua definição é como se segue:

Definição 2.4. *A entropia condicional quântica $S(\rho^A|\rho^B)$ de um estado bipartido ρ^{AB} é a diferença entre a entropia conjunta quântica $S(\rho^{AB})$ e a entropia quântica $S(\rho^B)$:*

$$S(\rho^A|\rho^B) \equiv S(\rho^{AB}) - S(\rho^B). \tag{2.70}$$

A definição da entropia condicional abre a possibilidade de obtermos valores negativos. Este resultado puramente quântico nos diz que conhecemos mais sobre o sistema como um todo do que temos informação sobre as partes dele quando a entropia condicional é menor que zero. Isso ocorre porque a entropia conjunta quântica não necessariamente é maior que a entropia marginal de uma das partes. Um exemplo deste fato é quando temos um estado ρ^{AB} puro. Assim, a entropia conjunta quântica é nula enquanto a entropia quântica geralmente não o é.

A entropia condicional quântica nunca é maior que a entropia de von Neumann do sistema conjunto, $S(\rho^A|\rho^B) \leq S(\rho^{AB})$, e é limitada superior e inferiormente, como segue.

Propriedade 2.9 (Condicionar não aumenta a entropia)**.** *Para um estado bipartido ρ^{AB} temos que*

$$S(\rho^A) \geq S(\rho^A|\rho^B). \tag{2.71}$$

Demonstração. A prova deste teorema é uma simples aplicação da subaditividade, Eq. (2.44). Como $S(\rho^A)+S(\rho^B) \geq S(\rho^{AB})$ então $S(\rho^A) \geq S(\rho^{AB})-S(\rho^B)$ que é a entropia condicional quântica por definição. □

Propriedade 2.10 (Máximo e mínimo da entropia condicional quântica)**.** *Para um estado bipartido ρ^{AB}, tal que d_A seja a dimensão do espaço de Hilbert de ρ^A temos*

$$\left|S(\rho^A|\rho^B)\right| \leq \log d_A. \tag{2.72}$$

Demonstração. O limite superior é obtido diretamente da entropia condicional ser menor ou igual a entropia marginal, Eq. (2.71), em conjunto com o limite máximo da entropia marginal, Eq. (2.33): $S(\rho^A|\rho^B) \leq S(\rho^A) \leq \log d_A$.

Para obter o limite inferior é necessário o lema a seguir:

Lema 2.3. *Para um estado bipartido ρ^{AB} e o sistema $\rho^E = \mathrm{tr}_{AB}\left\{\rho^{ABE}\right\}$ com ρ^{ABE} puro, então vale as igualdades seguintes*

$$S(\rho^A|\rho^B) = S(\rho^E) - S(\rho^B) = -S(\rho^A|\rho^E). \tag{2.73}$$

Demonstração. Como ρ^{ABE} é puro, $S(\rho^{ABE}) = 0$ e pelo lema 2.2 temos que $S(\rho^{AB}) = S(\rho^E)$ e $S(\rho^B) = S(\rho^{AE})$. Usando a definição da entropia condicional, Eq. (2.70), temos

$$\begin{aligned} S(\rho^A|\rho^B) &= S(\rho^{AB}) - S(\rho^B) \\ &= S(\rho^E) - S(\rho^B) \\ &= S(\rho^E) - S(\rho^{AE}) \\ &= -S(\rho^A|\rho^E), \end{aligned} \tag{2.74}$$

provando o lema. □

Utilizando o lema representado pela Eq. (2.73), e aplicando as Eq.s (2.71) e (2.33), encontramos

$$S(\rho^A|\rho^B) = -S(\rho^A|\rho^E) \geq -S(\rho^A) \geq -\log d_A, \tag{2.75}$$

a desigualdade desejada. □

2.2.3 Entropia mútua quântica

Por fim, a última entropia de que vamos fazer uso é a entropia mútua quântica. No ambiente clássico a informação mútua representa o quanto duas variáveis aleatórias estão correlacionadas. Quanticamente essa entropia segue a mesma ideia. Assim, define-se entropia mútua como,

Definição 2.5 (Entropia Mútua Quântica)**.** *Para um estado bipartido ρ^{AB} qualquer, a entropia mútua quântica entre A e B é definida como se segue,*

$$\begin{aligned} S(\rho^A : \rho^B) &\equiv S(\rho^A) + S(\rho^B) - S(\rho^{AB}) \\ &= S(\rho^A) - S(\rho^A|\rho^B) \\ &= S(\rho^B) - S(\rho^B|\rho^A). \end{aligned} \tag{2.76}$$

As três formas acima equivalentes da entropia mútua decorrem da definição da entropia condicional, Eq. (2.70). Essa entropia é limitada superior e inferiormente da seguinte forma.

Propriedade 2.11 (Mínimo e máximo valor da entropia mútua)**.** *Para todo sistema bipartido ρ^{AB}, sendo o sistema A com espaço de Hilbert de dimensão d_A e o sistema B com dimensão d_B, temos*

$$0 \leq S(\rho^A : \rho^B) \leq 2\min\{\log d_A, \log d_B\}. \tag{2.77}$$

Demonstração. O limite inferior é uma implicação direta da Eq. (2.71), isto é, do fato de que $S(\rho^A) \geq S(\rho^A|\rho^B)$. Deste modo temos que a entropia mútua quântica é sempre não negativa. Alcançamos o limite superior aplicando a Eq. (2.72) em conjunto com a Eq. (2.71), de modo que $S(\rho^A : \rho^B) \leq 2S(\rho^A) \leq 2\log d_A$. Aqui usamos o limite máximo da entropia marginal, Eq. (2.33). Seguindo o mesmo raciocínio para $S(\rho^B)$ verificamos que $S(\rho^A : \rho^B) \leq 2\log d_B$. Além disso, pela primeira linha da Eq. (2.76), a entropia mútua quântica é máxima quando $S(\rho^{AB}) = 0$. Ou seja, quando ρ^{AB} é um estado puro. Logo, temos que a entropia mútua quântica é limitada por duas vezes o mínimo das dimensões envolvidas, $2\min\{\log d_A, \log d_B\}$, já que ρ^{AB} puro tem no máximo o número de autovalores não nulos associado ao espaço de Hilbert de menor dimensão. □

Terminado a apresentação das entropias quânticas, vamos dar continuidade com algumas propriedades extras que nos permitirá calcular a segurança da transmissão de informação em protocolos de criptografia quânticos.

2.2.4 Propriedades das Entropias quânticas

Propriedade 2.12 (Convexidade da entropia relativa)**.** *A entropia relativa é juntamente convexa em seus argumentos,*

$$S(\rho||\sigma) \leq \sum_x p_x(x) S(\rho_x||\sigma_x). \tag{2.78}$$

Demonstração. A prova dessa proposição é uma aplicação da monotonicidade da entropia relativa apresentada no lema B.5. Assim, definindo dois conjuntos de operadores com espaço de Hilbelt diferentes teremos a relação de monotonicidade, $S(\rho^B||\sigma^B) \leq S(\rho^{XB}||\sigma^{XB})$. Portanto, suponha os operadores densidade $\rho^{XB} = \sum_x p_X(x) \left|x\right\rangle_X \langle x| \otimes \rho_x^B$ e $\sigma^{XB} = \sum_x p_X(x) \left|x\right\rangle_X \langle x| \otimes \sigma_x^B$. Suponha também que o espectro de σ_x^B seja $\sum_j \lambda_x^j \left|j_x\right\rangle_B \langle j_x|$.

Para que possamos aplicar a definição da entropia relativa (2.27), temos que calcular $\mathrm{tr}\left\{\rho^{XB} \log\left(\sigma^{XB}\right)\right\}$ e $\mathrm{tr}\left\{\rho^{XB} \log\left(\rho^{XB}\right)\right\}$. Então, como a função de um operador é a função dos autovalores na base diagonal do operador temos

$$\begin{aligned}
\mathrm{tr}\left\{\rho^{XB} \log\left(\sigma^{XB}\right)\right\} &= \mathrm{tr}\left\{\rho^{XB} \sum_{x,j} \log\left[p_X(x)\lambda_x^j\right] \left|x\right\rangle_X \langle x| \otimes \left|j_x\right\rangle_B \langle j_x|\right\} \\
= \mathrm{tr}\left\{\rho^{XB} \sum_x \log\left[p_X(x)\right] \left|x\right\rangle_X \langle x| \otimes \sum_j \left|j_x\right\rangle_B \langle j_x|\right\} &+ \mathrm{tr}\left\{\rho^{XB} \sum_{x,j} \log\left(\lambda_x^j\right) \left|x\right\rangle_X \langle x| \otimes \left|j_x\right\rangle_B \langle j_x|\right\} \\
= \mathrm{tr}\left\{\rho^{XB} \sum_x \log\left[p_X(x)\right] \left|x\right\rangle_X \langle x| \otimes I^B\right\} &+ \mathrm{tr}\left\{\rho^{XB} \sum_x \left|x\right\rangle_X \langle x| \otimes \log\left(\sigma_x^B\right)\right\},
\end{aligned} \tag{2.79}$$

onde na última linha da Eq. (2.79) usamos que $\sum_j \left|j\right\rangle \left\langle j\right|^B$ é a indentidade I^B e que $\sum_j \log\left(\lambda_x^j\right) \left|j_x\right\rangle_B \langle j_x| = \log\left(\sigma_x^B\right)$. Assim, inserindo $\rho^{XB} = \sum_x p_X(y) \left|y\right\rangle_X \langle y| \otimes \rho_y^B$ e sabendo que $\langle x|y\rangle = \delta_{x,y}$ encontramos

$$\begin{aligned}
&\mathrm{tr}\left\{\rho^{XB} \log\left(\sigma^{XB}\right)\right\} \\
&= \mathrm{tr}\left\{\sum_{x,y} p_X(y) \log[p_X(x)] \left|x\right\rangle_X \langle x|y\rangle_X \langle y| \otimes \rho_y^B I^B\right\} + \mathrm{tr}\left\{\sum_{x,y} p_X(y) \left|y\right\rangle_X \langle y|x\rangle_X \langle x| \otimes \rho_x^B \log\left(\sigma_x^B\right)\right\} \\
&= \sum_x p_X(x) \log\left[p_X(x)\right] \mathrm{tr}_X\left\{\left|x\right\rangle_X \langle x|\right\} \mathrm{tr}_B\left\{\rho_x^B\right\} + \mathrm{tr}\left\{\sum_x p_X(x) \left|x\right\rangle_X \langle x| \otimes \rho_x^B \log\left(\sigma_x^B\right)\right\}.
\end{aligned} \tag{2.80}$$

Reconhecendo a somatória restante do primeiro traço como a entropia clássica de Shannon,

Eq. (2.1), e calculando o traço parcial em X do segundo termo, a seguinte relação é obtida,

$$\mathrm{tr}\left\{\rho^{XB}\log\left(\sigma^{XB}\right)\right\} = -H(X) + \sum_x p_X(x)\mathrm{tr}_B\left\{\rho_x^B\log\left(\sigma_x^B\right)\right\}. \tag{2.81}$$

Para calcular, por sua vez, $\mathrm{tr}\left\{\rho^{XB}\log\left(\rho^{XB}\right)\right\}$, basta substituir σ^{XB} por ρ^{XB} na Eq. (2.81). Assim, encontramos que esta expressão vale $-H(X)+\sum_x p_X(x)\mathrm{tr}_B\left\{\rho_x^B\log\left(\rho_x^B\right)\right\}$. Logo, podemos afirmar que

$$\begin{aligned}
S(\rho^{XB}||\sigma^{XB}) &= \mathrm{tr}\left\{\rho^{XB}\log\left(\rho^{XB}\right)\right\} - \mathrm{tr}\left\{\rho^{XB}\log\left(\sigma^{XB}\right)\right\} \\
&= -H(X) + \sum_x p_X(x)\mathrm{tr}_B\left\{\rho_x^B\log\left(\rho_x^B\right)\right\} - \left(-H(X) + \sum_x p_X(x)\mathrm{tr}_B\left\{\rho_x^B\log\left(\sigma_x^B\right)\right\}\right) \\
&= \sum_x p_X(x)\left[\mathrm{tr}_B\left\{\rho_x^B\log\left(\rho_x^B\right)\right\} - \mathrm{tr}_B\left\{\rho_x^B\log\left(\sigma_x^B\right)\right\}\right] \\
&= \sum_x p_X(x)S(\rho_x^B||\sigma_x^B).
\end{aligned} \tag{2.82}$$

Pelo lema B.5, $S(\rho^B||\sigma^B) \leq S(\rho^{XB}||\sigma^{XB}) = \sum_x p_X(x)S(\rho_x^B||\sigma_x^B)$, finalizando a prova.

□

Propriedade 2.13 (Concavidade da entropia condicional quântica)**.** *Seja AB um sistema composto. Então $S(\rho^A|\rho^B)$ é côncava no estado $\rho^{AB} = \sum_x p_X(x)\rho_x^{AB}$,*

$$S(\rho^A|\rho^B) \geq \sum_x p_X(x)S(\rho_x^A|\rho_x^B). \tag{2.83}$$

Demonstração. Pela definição da entropia relativa, Eq. (2.27), e da definição de entropia condicional, Eq. (2.70), temos que

$$\begin{aligned}
S\left(\rho^{AB}||\frac{I^A}{d}\otimes\rho^B\right) &= \mathrm{tr}\left\{\rho^{AB}\log\left(\rho^{AB}\right)\right\} - \mathrm{tr}\left\{\rho^{AB}\log\left(\frac{I^A}{d}\otimes\rho^B\right)\right\} \\
&= -S(\rho^{AB}) - \mathrm{tr}\left\{\rho^{AB}\left[\log\left(\frac{I^A}{d}\right) + \log\left(\rho^B\right)\right]\right\} \\
&= -S(\rho^{AB}) + \mathrm{tr}\left\{\rho^{AB}I^A\log\left(d\right)\right\} - \mathrm{tr}\left\{\rho^{AB}\log\left(\rho^B\right)\right\} \\
&= -S(\rho^{AB}) + \mathrm{tr}\left\{\rho^{AB}\right\}\log\left(d\right) - \mathrm{tr}_B\left\{\mathrm{tr}_A\left\{\rho^{AB}\right\}\log\left(\rho^B\right)\right\} \\
&= -S(\rho^{AB}) - \mathrm{tr}_B\left\{\rho^B\log\rho^B\right\} + \log d \\
&= -S(\rho^A|\rho^B) + \log(d).
\end{aligned} \tag{2.84}$$

Consequentemente, $S(\rho^A|\rho^B) - \log(d) = -S(\rho^{AB}||I/d \otimes \rho^B)$. E sabemos da monotonicidade da entropia relativa, Eq. (B.5), que $-S(\rho^{AB}||I^A/d \otimes \rho^B) \geq -S(\rho^{XAB}||I^A/d \otimes \rho^{XB})$. Para um $\rho^{XAB} = \sum_x p_X(x) \left|x\right\rangle_X \!\left\langle x\right| \otimes \rho_x^{AB}$ temos

$$S(\rho^A|\rho^B) - \log(d) \geq -S(\rho^{XAB}||I/d \otimes \rho^{XB}) = -\sum_x p_X(x) S(\rho_x^{AB}||I^A/d \otimes \rho_x^B). \tag{2.85}$$

A igualdade da equação anterior foi obtida substituindo ρ^{XB} por ρ^{XAB} e σ^{XB} por $I^A/d \otimes \rho^{XB}$ na Eq. (2.82). Refazendo as contas da Eq. (2.84) para $-S(\rho_x^{AB}||I^A/d \otimes \rho_x^B)$ encontramos que $S(\rho_x^{AB}||I^A/d \otimes \rho_x^B) = S(\rho_x^A|\rho_x^B) - \log(d)$. Juntando este resultado na Eq. (2.85) encontramos o resultado que buscávamos, Eq. (2.83),

$$\begin{aligned} S(\rho^A|\rho^B) - \log(d) &\geq \sum_x p_X(x) S(\rho_x^A|\rho_x^B) - \sum_x p_X(x) \log(d), \\ S(\rho^A|\rho^B)) &\geq \sum_x p_X(x) S(\rho_x^A|\rho_x^B). \end{aligned} \tag{2.86}$$

□

Propriedade 2.14 (Forte subaditividade)**.** *Para qualquer sistema tripartite A, B, C valem as inequações*

$$\begin{aligned} S(\rho^A) + S(\rho^B) &\leq S(\rho^{AC}) + S(\rho^{BC}), \\ S(\rho^{ABC}) + S(\rho^B) &\leq S(\rho^{AB}) + S(\rho^{BC}). \end{aligned} \tag{2.87}$$

Demonstração. Seja T o mapa que toma uma matriz densidade tripartite ρ^{ABC} como *input* e nos fornece como *output* o negativo da entropia condicional de C dado A mais a de C dado B. Aplicando a definição da entropia condicional, Eq. (2.70), T pode ser escrito da seguinte forma,

$$\begin{aligned} T(\rho^{ABC}) &= -S(\rho^C|\rho^A) - S(\rho^C|\rho^B) \\ &= S(\rho^A) - S(\rho^{AC}) + S(\rho^B) - S(\rho^{BC}). \end{aligned} \tag{2.88}$$

Agora, suponha que $\sum_x \lambda_x \rho_x^{ABC}$ seja a decomposição espectral de ρ^{ABC}, com ρ_x^{ABC} puro. Aplicando a concavidade da entropia condicional, Eq. (2.83), temos

$$\begin{aligned} T(\rho^{ABC}) &\leq -\sum_x \lambda_x \left(S(\rho_x^C|\rho_x^A) + S(\rho_x^C|\rho_x^B) \right) \\ &= \sum_x \lambda_x T(\rho_x^{ABC}). \end{aligned} \tag{2.89}$$

Mas, $T(\rho_x^{ABC})$ é um mapeamento de um estado puro e, aplicando o lema 2.2, que diz que

para todo estado puro bipartido as entropias das duas partes são iguais, temos $S(\rho_x^{AC}) = S(\rho_x^B)$ e $S(\rho_x^{BC}) = S(\rho_x^A)$. Disto, resulta que $T(\rho_x^{ABC}) = 0$ usando a segunda linha de (2.88) para ρ_x^A, ρ_x^{AC}, ρ_x^B e ρ_x^{BC}. Consequentemente provamos a primeira linha da subaditividade forte:

$$T(\rho^{ABC}) \leq 0 \Rightarrow S(\rho^A) + S(\rho^B) - S(\rho^{AC}) - S(\rho^{BC}) \leq 0. \tag{2.90}$$

A segunda desigualdade é obtida considerando uma purificação R [33] do estado ρ^{ABC}, resultando no operador densidade ρ^{ABCR} puro. Dessa forma, reaplicando o lema 2.2 temos que $S(\rho^{ABC}) = S(\rho^R)$ e $S(\rho^{RC}) = S(\rho^{AB})$. Usando a Eq. (2.90) com as devidas substituições finalizamos a prova,

$$\begin{aligned} S(\rho^R) + S(\rho^B) &\leq S(\rho^{RC}) + S(\rho^{BC}), \\ S(\rho^{ABC}) + S(\rho^B) &\leq S(\rho^{AB}) + S(\rho^{BC}). \end{aligned} \tag{2.91}$$

□

A subaditividade forte é um teorema que permite compreender o conteúdo informacional de sistema quânticos compostos. Três de suas maiores aplicações são os teoremas provados a seguir.

Propriedade 2.15 (Condicionar não aumenta a entropia condicional)**.** *Considere um sistema composto ABC, então*

$$S(\rho^A|\rho^{BC}) \leq S(\rho^A|\rho^B). \tag{2.92}$$

Demonstração. A prova do teorema é um simples rearranjo da subaditividade forte, Eq. (2.87), e do uso da definição de entropia condicional quântica, Eq. (2.70).

$$\begin{aligned} S(\rho^{ABC}) - S(\rho^{BC}) &\leq S(\rho^{AB}) - S(\rho^B), \\ S(\rho^A|\rho^{BC}) &\leq S(\rho^A|\rho^B). \end{aligned} \tag{2.93}$$

Esse teorema diz que ao adicionarmos um novo sistema C, podemos diminuir a ignorância sobre a informação presente em A.

□

Propriedade 2.16 (Descartar um sistema não aumenta a entropia mútua quântica)**.** *Considere um sistema composto ABC, então*

$$S(\rho^A : \rho^B) \leq S(\rho^A : \rho^{BC}). \tag{2.94}$$

E a condição de igualdade ocorre quando temos $\rho^{ABC} = \rho^{AB} \otimes \rho^{C}$.

Demonstração. Aplicando a definição de entropia mútua, Eq. (2.76), a Eq. (2.94) pode ser reescrita como

$$\begin{aligned} S(\rho^A) + S(\rho^B) - S(\rho^{AB}) \leq S(\rho^A) + S(\rho^{BC}) - S(\rho^{ABC}), \\ S(\rho^{ABC}) + S(\rho^B) \leq S(\rho^{AB}) + S(\rho^{BC}), \end{aligned} \tag{2.95}$$

que é a subaditividade forte, Eq. (2.87). A Eq. (2.94) indica que adicionando um sistema C podemos aumentar a quantidade de informação acessível do sistema A.

Suponha um operador densidade ρ^{AB} e um sistema auxiliar ρ^{C} tal que $\rho^{ABC} = \rho^{AB} \otimes \rho^{C}$. Aplicando a definição de entropia mútua, Eq. (2.76), e em seguida notando que o logaritmo de um produto tensorial, é a soma dos logaritmos, temos

$$\begin{aligned} S(\rho^A : \rho^{BC}) &= S(\rho^A) + S(\rho^{BC}) - S(\rho^{ABC}), \\ &= S(\rho^A) + S\left(\rho^B \otimes \rho^C\right) - S\left(\rho^{AB} \otimes \rho^C\right), \\ &= S(\rho^A) + S(\rho^B) + S(\rho^C) - S(\rho^{AB}) - S(\rho^C), \\ &= S(\rho^A : \rho^B), \end{aligned} \tag{2.96}$$

confirmando que a igualdade ocorre em $\rho^{ABC} = \rho^{AB} \otimes \rho^{C}$,

$$S(\rho^A : \rho^B) = S(\rho^A : \rho^{BC}). \tag{2.97}$$

Então, adicionar um sistema não correlacionado não altera a entropia mútua.

□

Propriedade 2.17 (Operações quânticas nunca aumentam a informação mútua)**.** *Considere um sistema composto* AB *e* $\mathcal{E}$ *uma operação quântica que preserva o traço atuando em* B*. Denotando* $S(\rho^A : \rho^B)$ *a entropia quântica mútua antes da atuação de* $\mathcal{E}$ *e* $S(\rho^{A'} : \rho^{B'})$ *a entropia mútua após a operação quântica, então*

$$S(\rho^{A'} : \rho^{B'}) \leq S(\rho^A : \rho^B). \tag{2.98}$$

Demonstração. Para provar o teorema precisamos da condição de igualdade da Eq. (2.95). Utilizamos também que, a ação de uma operação quântica $\mathcal{E}$ em ρ^B pode ser simulada por meio da introdução de um terceiro sistema quântico auxiliar inicialmente no estado puro, $|0\rangle\langle 0|$ [34]. Assim, a operação em B reduz-se a uma transformação unitária do sistema B

e C mais o traço parcial em C após a ação da transformação unitária **U**:

$$\mathcal{E}(\rho^B) = \mathrm{tr}_C \left\{ U \left(\rho^B \otimes |0\rangle \langle 0| \right) U^\dagger \right\}. \tag{2.99}$$

Como provado no lema da Eq. (2.95), a introdução do sistema puro não altera a entropia mútua. Então $S(\rho^A : \rho^B) = S(\rho^A : \rho^{BC})$. Temos também que a entropia é invariante perante transformações unitárias, Eq. (2.26). Assim, $S(\rho^A : \rho^{BC}) = S(\rho^{A'} : \rho^{B'C'})$. Por fim a Eq. (2.94) nos diz que $S(\rho^{A'} : \rho^{B'C'}) \geq S(\rho^{A'} : \rho^{B'})$. Logo, juntando todos estes fatos temos $S(\rho^A : \rho^B) \geq S(\rho^{A'} : \rho^{B'})$.

□

Aqui encerramos a revisão das ferramentas matemáticas necessárias para aferir a segurança da transmissão de uma chave secreta. E como usaremos esse conhecimento recém adquirido é apresentado na próxima seção.

2.3 Análise de segurança

Uma transmissão de chave criptográfica é considerada segura se o conhecimento que Bob, o receptor, possui sobre a chave enviada por Alice for maior que o conhecimento que Eva, a espiã, é capaz de obter dessa chave. Essa segurança de transmissão pode ser estimada comparando a informação compartilhada entre Alice e Bob, $I(A : B)$, com a quantidade máxima de informação que a espiã Eva pode obter, $I_{\max}(A : E)$. Aqui consideramos a informação máxima de Eva, pois queremos garantir que independentemente do que Eva faça, a chave codificará a mensagem entre Alice e Bob com segurança. E indo além, consideramos que Eva é somente limitada pelas leis da Física. Um limite genérico para quantificar a taxa de segurança de uma chave criptográfica quântica é o limite de Devetak e Winter [39]: $r = I(A : B) - \chi(A : \rho^E)$. A função $\chi(A : \rho^E)$ é o limite de Holevo [36].

A chave é dita segura para $r > 0$, ou seja, a comunicação é segura se Alice e Bob possuem mais informação sobre a chave do que Eva pode obter. O limite de Devetak Winter é válido para protocolos *one-time-pad*, ou seja, em chaves que serão utilizadas somente uma vez. O limite de Holevo previamente citado é o máximo de informação que pode ser obtido por um espião independentemente do tipo de ataque a segurança por ele perpetrado. Uma breve discussão sobre essa poderosa afirmação é feita a seguir.

2.3.1 A quantidade de Holevo

Vamos supor que um dos possíveis resultados a da variável aleatória A é associado ao estado quântico ρ_a^E. Podemos dizer que ρ_a^E é o estado quântico de Eva após uma medida projetiva de Alice no sistema dela por exemplo, no qual Alice obtém o estado $|a\rangle$. A probabilidade $p_A(a)$ de obter o valor a de A é a mesma de Alice obter o estado $|a\rangle$ em sua medida. Neste cenário, o operador densidade que descreve o sistema de Eva é

$$\rho^E = \sum_a p_A(a)\rho_a^E. \tag{2.100}$$

O estado ρ^E pode ser interpretado fisicamente como a descrição do sistema de Eva dado que ela não conheça o resultado obtido por Alice. Isto ocorre, por exemplo, quando Alice envia ou teleporta um *qubit* que codifica um dos bits da chave para Bob. Este é o caso dos protocolos BB84 e GR10 estudados nesta Tese, onde Eva não sabe os resultados das medidas obtidas por Alice quando esses protocolos são implementados na sua versão *entanglement-based*. (veja o capítulo 3). Nesses protocolos, nós temos apenas as bases das medidas reveladas publicamente, de modo que Eva não possui conhecimento sobre o estado $|a\rangle$ de Alice.

O estado ρ^E é obtido tomando o traço sobre Alice do sistema que descreve o estado conjunto de Alice e Eva antes de qualquer medida realizada por Alice,

$$\rho^E = \mathrm{Tr}_A(\rho^{AE}). \tag{2.101}$$

Usando ρ^{AE} e o postulado da medida da mecânica quântica se o estado de Alice é projetado em $|a\rangle\langle a|$ nós temos que

$$p_A(a) = \mathrm{tr}\left\{\rho^{AE}(|a\rangle_A\langle a| \otimes \mathbb{1}_E)\right\}, \tag{2.102}$$

onde nós tomamos o traço total e $\mathbb{1}_E$ é o operador identidade atuando no espaço de Hilbert do sistema de Eva. O postulado da medida diz que

$$\rho_a^E = \frac{1}{p_A(a)}(\langle a| \otimes \mathbb{1}_E)\rho^{AE}(|a\rangle \otimes \mathbb{1}_E). \tag{2.103}$$

O estado ρ^{AE}, por sua vez, é obtido a partir do traço parcial em relação a Bob do

estado ρ^{ABE}, o operador densidade que descreve o estado total de Alice, Bob e Eva,

$$\rho^{AE} = \mathrm{tr}_B \left\{ \rho^{ABE} \right\}. \tag{2.104}$$

Pela notação utilizada até o momento, a quantidade de Holevo é definida por

$$\chi(A : \rho^E) = S(\rho^E) - \sum_a p_A(a) S(\rho_a^E), \tag{2.105}$$

onde $S(\rho)$ é a entropia de von Neumann do estado quântico ρ, Eq. (2.24),

$$S(\rho) = -\mathrm{tr} \left\{ \rho \log \rho \right\}. \tag{2.106}$$

Nós podemos entender o significado da quantidade de Holevo $\chi(A : \rho^E)$ notando que ela limita a capacidade de comunicação de um canal quântico, onde a codificação do símbolo clássico a, cuja probabilidade de ocorrer é $p_A(a)$, é feita nos estados quânticos ρ_a^E [8,36,39]. Por causa desta propriedade a quantidade de Holevo é comumente considerada a extensão quântica da informação mútua. Perceba que diferentemente da entropia mútua quântica $S(\rho^A : \rho^E)$, a quantidade de Holevo $\chi(A : \rho^E)$ é construída somente após Alice realizar sua medida. Ou seja, ela depende da base utilizada por Alice.

A entropia quântica mútua $S(\rho^A : \rho^B)$ estabelece a correlação entre sistemas quânticos. Contudo, a quantidade de informação clássica que pode ser extraída depende do tipo de operação quântica a ser aplicada. A máxima informação mútua que pode ser extraída do sistema é denominada de informação acessível de um operador densidade. Em geral, encontrar a operação quântica que maximiza a informação pode ser trabalhoso. Entretanto, como dito anteriormente, a quantidade de Holevo [36] define um limite superior da quantidade de informação que pode ser extraída de um sistema quântico:

Definição 2.6 (Quantidade de Holevo)**.** *Suponha que Alice envie o estado ρ_x^B a Bob com probabilidades $p_A(x)$. Bob realiza uma medida descrita pelo elemento de POVM (positive-operator valued measure) $\{E_y\}$ no estado recebido de Alice com resultado B (veja apêndice A.1). O máximo de informação mútua $I(A : B)$ acessível a Bob é*

$$\begin{aligned} I(A : B) &\leq \chi(A : \rho^B) \\ &= S\left(\sum_x^n p_A(x) \rho_x^B \right) - \sum_x^n p_A(x) S(\rho_x^B). \end{aligned} \tag{2.107}$$

Aqui $\rho^B = \sum_x p_A(x) \rho_x^B$

Demonstração. A prova da quantidade de Holevo é simplesmente uma aplicação das propriedades da entropia mútua.

Seja um sistema tripartite A, B e M, onde A pode ser pensado como a preparação de Alice para enviar ρ_x^B a Bob (B) com probabilidade $p_A(x)$ e M o aparato utilizado por Bob para realizar a medida que retornará a probabilidade $p_B(y)$. O estado inicial do sistema é:

$$\rho^{ABM} = \sum_x p_A(x) \left|x\right\rangle_A \!\left\langle x\right| \otimes \rho_x^B \otimes \left|0\right\rangle_M \!\left\langle 0\right| . \tag{2.108}$$

A medida realizada por Bob pode ser descrita como uma operação quântica $\mathcal{E}$ que preserva o traço atuando em B e M, cujo resultado é armazenado no sistema M:

$$\mathcal{E}\left(\rho^B \otimes \left|0\right\rangle \left\langle 0\right|\right) \equiv \sum_y \sqrt{E_y}\rho^B\sqrt{E_y} \otimes \left|y\right\rangle_M \left\langle y\right| , \tag{2.109}$$

onde E_y é um operador positivo com $\sum_y E_y = \mathbb{1}$ (apêndice A.1).

Seja A', B' e M' o sistema após a operação quântica. Antes da medida tem-se que $S(\rho^A : \rho^B) = S(\rho^A : \rho^{BM})$, pois a adição de sistema puro não altera a entropia mútua (veja a condição de igualdade no lema associado à Eq. (2.95)). Após Bob realizar sua medida, temos que $S(\rho^{A'} : \rho^{B'M'}) \leq S(\rho^A : \rho^{BM}) = S(\rho^A : \rho^B)$, pela propriedade de que operações quânticas não aumentam a entropia mútua, Eq. (2.98). Por fim, descartando-se B' tem-se que $S(\rho^{A'} : \rho^{M'}) \leq S(\rho^{A'} : \rho^{B'M'})$, uma vez que descartando um sistema não aumenta a entropia mútua, Eq. (2.94). Portanto, podemos afirmar que

$$S(\rho^{A'} : \rho^{M'}) \leq S(\rho^A : \rho^B). \tag{2.110}$$

Cálculos direto da Eq. (2.108) nos dão $S(\rho^A) = H(A)$ e $S(\rho^{AB}) = H(A) + \sum_x p_A(x) S(\rho_x^B)$, onde $H(A)$ é a entropia clássica de se obter a variável aleatória A, isto é, a entropia de Shannon sobre o conjunto de probabilidades de Alice enviar um determinado estado a Bob, Eq. (2.1). Portanto, aplicando a definição da entropia mútua, $S(\rho^A : \rho^B) = S(\rho^A) + S(\rho^B) - S(\rho^{AB})$, obtemos

$$S(\rho^A : \rho^B) = S(\rho^B) - \sum_x p_A(x) S(\rho_x^B) = \chi(A : \rho^B). \tag{2.111}$$

Ou seja, exatamente a quantidade de Holevo.

Após a medida de Bob, o estado $\rho^{A'B'M'}$ é

$$\rho^{A'B'M'} = \sum_{x,y} p_A(x) \left|x\right\rangle_A\!\langle x| \otimes \sqrt{E_y}\rho_x^B\sqrt{E_y} \otimes \left|y\right\rangle \langle y| \,. \tag{2.112}$$

Sabendo que $\rho^{A'M'} = \mathrm{tr}_{B'}\left\{\rho^{A'B'M'}\right\}$ e que $\mathrm{tr}_{B'}\left\{\sqrt{E_y}\rho_x^B\sqrt{E_y}\right\} = \mathrm{tr}_{B'}\left\{E_y\rho_x^B\right\} = p_{B|A}(y|x)$, então

$$\begin{aligned}\rho^{A'M'} &= \sum_{x,y} p_A(x)p_{B|A}(y|x) \left|x\right\rangle_A\!\langle x| \otimes \left|y\right\rangle_M\!\langle y| \\ &= \sum_{x,y} p_{A,B}(x,y) \left|x\right\rangle_A\!\langle x| \otimes \left|y\right\rangle_M\!\langle y| \,.\end{aligned} \tag{2.113}$$

Tomando o traço parcial ora no sistema M' e ora no sistema A', a Eq. (2.113) dá

$$\rho^{A'} = \sum_x p_A(x) \left|x\right\rangle_A\!\langle x| \,, \tag{2.114}$$

$$\rho^{M'} = \sum_y p_B(y) \left|y\right\rangle_M\!\langle y| \,. \tag{2.115}$$

Dessa forma, calculando a entropia quântica diretamente pela definição, Eq. (2.24), temos para os operadores densidades (2.114), (2.115) e (2.113) que $S(\rho^{A'}) = H(A)$, $S(\rho^{M'}) = H(B)$ e $S(\rho^{A'M'}) = H(A,B)$. Note que $H(A,B)$ é entropia clássica conjunta de Alice e Bob, Eq. (2.3). Utilizando esses valores nós temos que

$$S(\rho^{A'} : \rho^{M'}) = H(A) + H(B) - H(A,B) = I(A:B), \tag{2.116}$$

a informação mútua dada pela Eq. (2.6). Logo, substituindo as Eqs. (2.111) e (2.116) na Eq. (2.110) leva a

$$I(A:B) \leq \chi(A:\rho^B). \tag{2.117}$$

□

2.3.2 Consequências da descoberta de Holevo

Além de estabelecer um limite máximo para a informação mútua, a quantidade de Holevo permite determinar a informação máxima que pode ser transmitida entre Alice e Bob por um canal. Considere que Alice envie o operador densidade ρ_x^B com $p_A(x)$ de probabilidade. Desse modo, reescrevendo a Eq. (2.62) em função da quantidade de Holevo

encontramos

$$S(\rho) \leq H(A) + \sum_x p_A(x) S(\rho_x^B) \tag{2.118}$$

$$\chi(A:\rho) \leq H(A). \tag{2.119}$$

Note que $H(A)$ é a entropia clássica interpretada como a quantidade de informação que Alice possui (veja a Sec. 2.1). Além disso, a quantidade de Holevo é o máximo valor da informação mútua, Eq. (2.6). Consequentemente, a Eq. (2.119) mostra não ser possível obter mais informação além do transmitido por Alice. Este resultado é conhecido como o limite de Holevo. Em outras palavras, $I(A:B) \leq \chi(A:\rho)$ e isto dá, usando as Eqs. (2.117) e (2.119), que $I(A:B) \leq H(A)$. Ou seja, a informação compartilhada entre Alice e Bob ($I(A:B)$) nunca será maior que a informação originalmente com Alice ($H(A)$).

Podemos compreender mais sobre a máxima informação obtida através do operador densidade $\rho^{AB} = \sum_x p_A(x) \left|x\right\rangle_A \langle x| \otimes \rho_x^B$. A Eq. (2.60) mostra que a entropia conjunta quântica para esse tipo de operador vale

$$S(\rho^{AB}) = H(A) + \sum_x p_A(x) S(\rho_x^B). \tag{2.120}$$

O estado $\rho^A = \sum_x p_A(x) \left|x\right\rangle_A \langle x|$ pode ser interpretado como um estado auxiliar para Alice enviar apropriadamente o estado ρ_x^B a Bob, ou mesmo uma operação quântica local realizada por Alice em um operador ρ^{AB} compartilhado entre eles resultando no estado $\left|x\right\rangle_A \langle x|$ com probabilidade $p_A(x)$.

Aplicando a definição de entropia mútua e substituindo $S(\rho^{AB})$ pela Eq. (2.120) temos

$$\begin{aligned} S(\rho^A:\rho^B) &= S(\rho^A) + S(\rho^B) - S(\rho^{AB}) \\ &= H(A) + S(\rho^B) - H(A) - \sum_x p_A(x) S(\rho_x^B) \\ &= S(\rho^B) - \sum_x p_A(x) S(\rho_x^B) \\ &= \chi(A:\rho^B). \end{aligned} \tag{2.121}$$

Logo, a entropia mútua quântica $S(\rho^A : \rho^B)$ é máxima e equivalente a informação mútua somente se ρ_x^B for puro. Neste caso $S(\rho_x^B) = 0$, e a penúltima linha da Eq. (2.121) implica que $S(\rho^A : \rho^B) = S(\rho^B)$. E quando ρ_x^B for puro também temos que $S(\rho^B) = S(\rho^A) = H(A)$, o que pode ser obtido usando ρ^{AB} supondo ρ_x^B puro. Dessa forma, como por Eq. (2.121) temos que $S(\rho^A : \rho^B) = \chi(A : \rho^B)$ obtemos $\chi(A : \rho^B) = H(A)$, o que

satura a desigualdade (2.119). Então, como por (2.117) temos $I(A:B) \leq \chi(A:\rho^B)$, chegamos a $I(A:B) \leq H(A)$. Isso mostra que $H(A)$ é o máximo de informação mútua permitida.

2.3.3 Segurança e criptografia

Um dos principais problemas da criptografia, tanto clássica quanto quântica, é obter de forma rigorosa a segurança incondicional de um protocolo que almeja transmitir informação de forma segura. Os protocolos de criptografia clássicos não possuem essa segurança incondicional provadas matematicamente. Eles são considerados seguros devido a dificuldade computacional para decriptar a mensagem sem conhecer a chave criptográfica que permite facilmente recuperar a mensagem cifrada. Um bom exemplo para ilustrar esse ponto é o protocolo clássico RSA [1].

O protocolo RSA é um protocolo de criptografia de chave assimétrica. Isto é, a chave que codifica a mensagem é diferente da que decodifica a mensagem cifrada. O elemento necessário para criptografar a mensagem é o resultado da multiplicação de dois números primos. Para decriptar a mensagem precisa-se conhecer exatamente quais são esses números primos. No entanto, é bem conhecido classicamente que fatorar números grandes em seus fatores primos não é uma tarefa simples, sendo necessário anos de processamento com computadores clássicos. A descrição passo a passo do protocolo RSA pode ser acompanhada no apêndice D.

Outra desvantagem da criptografia clássica é não ser possível descobrir se a chave foi descoberta ou se ela ainda permanece segura. Por outro lado, nos protocolos de criptografia quântica essa desvantagem não existe. Quando Eva monitora a transmissão da chave criptográfica quântica, ela introduz erros no sistema devido a não ser possível clonar estados quânticos arbitrários não-ortogonais [14,15]. Logo, para se obter a segurança incondicional precisamos calcular um limite máximo de erro tolerado, abaixo do qual o esquema de distribuição da chave seja seguro. Mas antes de calcularmos a confiabilidade da chave, precisamos compreender quais são os tipos de ataques que Eva pode realizar em seus *qubits* auxiliares (*ancillas*) nos *qubits* enviados de Alice para Bob [7–9]:

Ataques individuais ou incoerente: A primeira classe de ataque é a menos poderosa dos três tipos de ataques considerados. Eva ataca cada um dos *qubits* enviados independentemente dos outros *qubits* e sempre usando a mesma estratégia de ataque. Supõe-se também que Eva implementa todas as suas medidas que ela usou para

interagir com os *qubits* enviados por Alice, antes de Alice e Bob iniciarem o pós-processamento clássico dos dados (correção de erros e amplificação de privacidade).

Ataques coletivos: O segundo tipo de ataque amplia as possibilidades de Eva no sentido de que ela agora pode fazer tudo o que é permitido por ataques individuais e, além disso, pode decidir adiar as medições em suas *ancillas* até o momento no qual ela considerar mais conveniente. Ou seja, ela tem à sua disposição uma memória quântica para armazenar os estados quânticos antes de qualquer medição por exemplo. Além disso, Eva também pode realizar medidas conjuntas (medidas coletivas), onde ela mede mais de uma *ancilla* simultaneamente.

Ataques coerente: Este é o ataque mais poderoso possível realizado por Eva. Ela pode fazer tudo o que é permitido pelas outras duas classes de ataques, bem como implementar qualquer tipo de interação (operação unitária) envolvendo qualquer número de *ancillas* com qualquer número de *qubits* enviados de Alice para Bob. Eva também pode implementar qualquer tipo de medida que ela queira e no momento mais conveniente para ela. Em resumo, Eva tem total liberdade para manipular os *qubits* enviados, sendo restrita somente pelas leis da mecânica quântica.

Com o intuito de evitar técnicas clássicas de decriptação, a chave criada será utilizada apenas uma vez (*one-time pad*) e também nos restringiremos ao pós processamento unidirecional (*one-way postprocessing*) da chave bruta [1] . *One-way postprocessing* é idealmente dividido em uma primeira etapa de correção de erros (reconciliação de informações) e depois em uma etapa de amplificação de privacidade [8]. Estes são protocolos de processamento clássicos aplicados à chave bruta e eles são chamados de mão única sempre que apenas uma parte envia informações clássicas durante a implementação do protocolo. A outra parte, quem recebeu a informação (receptor), age de acordo com regras previamente estabelecidas, mas nunca envia qualquer *feedback* para a parte comunicante. Além disso, se a parte comunicante envia estados quânticos, nós temos o que é conhecido por pós-processamento por reconciliação direta (*direct reconciliation*). Usando nossa terminologia, Alice é a parte que se comunica classicamente com Bob durante a fase de pós-processamento e ele é quem age em seus dados sem se comunicar com Alice. Se N *qubits* são enviados para formar a chave criptográfica quântica, no final da etapa de reconciliação (correção de erros), a chave criptográfica possuíra um tamanho (número de bits) R. O valor R é conhecido como chave

[1] A chave bruta é composta por todos os bits enviados de Alice a Bob antes de realizar qualquer etapa de descarte ou pós-processamento.

crua ou bruta (*raw key*). E mais, apenas uma fração r dessa chave crua original será segura e perfeitamente correlacionada. Em outras palavras, o tamanho da chave secreta compartilhada é $K = rR$. Essa nova redução do tamanho da chave decorre da implementação dos protocolos clássicos de amplificação de privacidade, que visam aumentar a segurança dos dados compartilhados entre Alice e Bob.

Uma ferramenta importante na análise da segurança de um esquema de distribuição de chaves quânticas sob ataques coletivos, com pós-processamento clássico unidirecional e reconciliação direta, é o limite Devetak-Winter [39]:

$$r = I(A:B) - \max_{\text{Eva}} \chi(A:\rho^E). \tag{2.122}$$

Aqui r é a fração ou taxa da chave secreta (*secret-key fraction*), conforme definida anteriormente e entendida no caso assintótico, isto é, estamos lidando com chaves brutas infinitamente longas ($N \to \infty$) [8]. O primeiro termo no lado direito da Eq. (2.122), $I(A:B)$, é a informação mútua entre os dados clássicos de Alice e Bob, Eq. (2.5), ou seja, a correlação entre a sequência de bits de Alice com a sequência de bits com Bob após a etapa de peneiramento (*sifting*). Veja a Sec. 2.1. Em um cenário ideal, sem ruído e sem Eva, $r = I(A:B) = 1$. Isso significa que cada bit da sequência de bits de Alice é idêntico ao correspondente da sequência de bits de Bob, ou seja, a chave bruta é a chave compartilhada secreta ($K = R$). O segundo termo no lado direito, $\chi(A:\rho^E)$, é a quantidade de Holevo [36] apresentado na Sec. 2.3.1 e discutido na Sec. 2.3.2. Ele pode ser visto como uma generalização quântica da informação mútua, quantificando a informação de Eva sobre a chave bruta. Maximizando-o em todos os possíveis ataques coletivos, isto é o que a notação $\max_{\text{Eva}}$ está nos dizendo para fazer, podemos obter a taxa da chave secreta de um protocolo de distribuição de chaves quânticas subtraindo a máxima informação de Eva da informação mútua de Alice e Bob. Assim, se $r > 0$ o protocolo é seguro e se $r \leq 0$ ele é inseguro [39].

Um outro fato que permitiu avançar na análise de segurança de protocolos quânticos de criptografia foi o entendimento subsequente de que um protocolo de distribuição de chaves quânticas tipo BB84 possui uma representação baseada em emaranhamento (*entanglement-based-representation*) [7–9, 29, 43]. Esta representação baseada em emaranhamento levou a métodos práticos para calcular a fração da chave secreta fornecida pela Eq. (2.122). Trabalhando diretamente com a versão baseada em emaranhamento de um protocolo de distribuição de chaves quânticas, podemos escrever o estado quântico compartilhado por Alice, Bob e Eva após a interferência de Eva como um estado puro (purificação do estado

com Alice e Bob). E este é o melhor cenário possível para Eva [39] e, usando a purificação, podemos estimar um limite inferior para a fração da chave secreta r dependente das taxas de erro do protocolo [8, 39]. Observe que o mapeamento de um protocolo de prepare-e-meça (*prepare-and-measure*), como o BB84 e GR10, para sua representação baseada em emaranhamento não implica que esta última seja fácil implementação prática. Esse mapeamento apenas nos informa que a prova de segurança obtida para o protocolo baseado em emaranhamento é tão boa quanto se tivéssemos trabalhado diretamente com o protocolo original [7–9].

A próxima inovação na análise de segurança dos protocolos de distribuição de chaves criptográficas quânticas, generalizando as idéias dadas nas refs. [44, 45], foi a prova de que a análise de segurança incondicional pode ser realizada no regime assintótico estudando-se apenas a segurança de um determinado protocolo no nível de ataque coletivo [46,47]. Com a ajuda do teorema de de Finetti quântico, Renner [46] provou para protocolos com variáveis discretas, e Renner e Cirac [47] para variáveis contínuas, que a análise de segurança de ataques coletivos e de ataques coerentes são equivalentes.

Capítulo 3

Protocolos de distribuição de chaves criptográficas quânticas

Para que possamos criar uma representação baseada em emaranhamento dos protocolos de criptografia quântica, precisamos compreender em todos os detalhes o protocolo em questão. Neste capítulo apresentamos o protocolo de distribuição de chaves criptográficas quânticas BB84 [4] e também o protocolo GR10 [18]. O primeiro já possui sua segurança amplamente testada na literatura e servirá de base para que possamos expandir a análise de segurança dele para o segundo. Lembramos que o protocolo GR10, criado em 2010 por Gordon e Rigolin, não possui sua segurança incondicional provada na literatura. Alcançar tal prova é um dos objetivos centrais desta Tese.

3.1 Protocolo BB84

O uso da mecânica quântica para o desenvolvimento de protocolos seguros de transmissão e armazamento de informação tem suas raízes nos anos 1960 quando Stephen Wiesner propôs o "dinheiro quântico" [1]. Contudo, as dificuldades técnicas da época e também atuais impedem aplicação desta moeda. Foi em 1984 que Bennett e Brassard desenvolveram um protocolo funcional que usa as leis da mecânica quântica para estabelecer uma comunicação segura. Este trabalho pioneiro, conhecido como protocolo de distribuição de chaves criptográficas quânticas BB84 [4], almeja distribuir uma chave secreta entre duas partes (pessoas). Esta chave permite criptografar e decriptar a mensagem a ser enviada. Esse tipo de chave é conhecida como chave simétrica. Entretanto, o conceito de chave criptográfica simétrica não é novo, mas devido às complicações da distribuição da chave em

larga escala e/ou em grande distâncias, sem contar a impossibilidade clássica de confirmar que a chave é segura, implicou na substituição dela por chaves assimétricas. Atualmente, é difundindo o uso de protocolos assimétricos de segurança, isto é, a chave codificadora é diferente da chave decriptadora da informação. Veja apêndice D para um exemplo deste tipo de chave. No entanto, o protocolo BB84 eliminou o problema da insegurança da transmissão da chave, onde pelas características intrínsecas da mecânica quântica temos como verificar se a chave foi acessada por uma terceira parte (pessoa). A seguir, nós damos uma descrição curta de como o protocolo BB84 funciona:

(i) Primeiramente, Alice e Bob concordam de antemão que a codificação dos bits clássicos enviados de Alice para Bob é aleatoriamente feita utilizando duas bases com estados quânticos não-ortogonais para cada bit. Por exemplo, o bit 0 é codificado pelos *qubits* $|0\rangle$ ou $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ e o bit 1 pelos *qubits* $|1\rangle$ ou $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$.

(ii) Em seguida, Alice aleatoriamente prepara seu *qubit* em um dos quatro estados descritos anteriomente e o envia a Bob. Após receber o *qubit* de Alice, Bob o mede utilizando aleatoriamente a base z, expandida pelos estados $\{|0\rangle, |1\rangle\}$, ou a base x dados pelos estados $\{|+\rangle, |-\rangle\}$. Caso Bob obtenha o resultado $|0\rangle$ ou $|+\rangle$, ele supõe que Alice enviou o bit 0, caso o resultado de sua medida seja $|1\rangle$ ou $|-\rangle$, ele associa o bit 1. Este passo é repetido N vezes.

(iii) Após Bob finalizar todas as medidas dos N *qubits*, Alice e Bob se comunicam em um canal público clássico e autenticado. O canal pode ser passível de monitoramento. Aqui, Alice revela a base utilizada no preparo dos seus *qubits*. Eles descartam os casos onde diferentes bases foram usadas e mantém os resultados cujas bases foram iguais. Pode se dizer que na média $N/2$ *qubits* foram descartados e $N/2$ foram mantidos. Esses *qubits* restantes são comumente chamados de chave crua, e este processo de selecionar quais *qubits* são úteis e quais não são é conhecido por *sifting* (peneiramento). Note que esse é um passo crucial. Pois, de acordo com as leis da mecânica quântica, e se não houver monitoramento externo na transmissão, Alice e Bob sempre concordarão sobre os valores dos *qubits* quando ele realiza sua medida na mesma base em que ela preparou o *qubit* enviado. Se eles mantivessem os *qubits* descartados eles obteriam o resultado errado em 50% dos casos.

(iv) Alice ou Bob revela uma parte dos bits da chave crua (aqueles que não foram descartados). Eles escolhem aleatoriamente para esta tarefa uma parte dos bits que

formam a chave crua. Estes bits são usados para checar a presença de monitoramento na transmissão e geralmente consiste em metade dos bits restantes, isto é, $N/4$ [4]. Se Alice e Bob concordam sobre os valores dos bits revelados (os bits de Alice são os mesmos de Bob), então eles supõem que não ocorreu monitoramento na distribuição da chave e usam os $N/4$ bits restantes (aqueles que não foram revelados) para formar a chave criptográfica. Se, como geralmente ocorre na prática, alguns dos bits revelados por Alice e Bob não são os mesmos, eles usam essa informação para calcular a taxa de erro do canal quântico de comunicação. Supões-se que a taxa de erro do canal é sempre causada pela ação de Eva. Desta forma, consideramos que toda informação perdida (mesmo devido a imperfeição do canal) é uma informação que beneficiará Eva. E, *se a taxa de erro for abaixo de um certo limite estipulado*, Alice e Bob realizam protocolos clássicos de correção de erro e amplificação de privacidade na chave secreta. No final, eles compartilham uma sequência reduzida de bits que pode ser considerada segura e idêntica. Note que esse limite de erro tolerado é definido pela taxa de segurança r do limite de Devetak Winter, Eq. (2.122).

Na seção seguinte, iremos apresentar o protocolo que é o foco do estudo desta Tese.

3.2 Protocolo GR10

O protocolo de distribuição de chave criptográfica quântica GR10 [18], desenvolvido em 2010 por Gordon e Rigolin, utiliza o teletransporte quântico para a transmissão dos *qubits* que formarão a chave secreta. Diferentemente do protocolo de teletransporte determinístico [16], o GR10 utiliza uma base *não maximamente emaranhada* para conectar Alice com Bob gerando assim um teletransporte probabilístico [1]. Antes de explicarmos o protocolo GR10, introduziremos o protocolo de teletransporte probabilístico:

(i) Alice quer teletransportar para Bob o estado

$$|\phi\rangle_A = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{3.1}$$

com $|\alpha|^2 + |\beta|^2 = 1$. Para isso, ela vai utilizar um canal quântico que será enviado por Bob.

[1] Nem sempre o estado teleportado por Alice chega a Bob com fidelidade um.

(ii) Bob prepara o estado de Bell generalizado

$$|\Phi_1^n\rangle_{AB} = \frac{|00\rangle_{AB} + n\,|11\rangle_{AB}}{\sqrt{1+n^2}}, \tag{3.2}$$

com $0 \leq n \leq 1$. Perceba que o estado na Eq. (3.2) é maximamente emaranhado somente se $n = 1$. Além disso, a Eq. (3.2) forma uma base completa e ortonormal no espaço de Hilbert com dois *qubits* juntamente com os outros estados de Bell generalizados [19–21]

$$|\Phi_2^n\rangle = \frac{n|00\rangle - |11\rangle}{\sqrt{1+n^2}}, \tag{3.3}$$

$$|\Phi_3^n\rangle = \frac{|01\rangle + n|10\rangle}{\sqrt{1+n^2}}, \tag{3.4}$$

$$|\Phi_4^n\rangle = \frac{n|01\rangle - |10\rangle}{\sqrt{1+n^2}}. \tag{3.5}$$

(iii) Bob envia um os *qubits* do seu canal quântico emaranhado, Eq. (3.2), para Alice, mantendo o outro consigo.

(iv) Alice recebe o *qubit* enviado por Bob e juntamente com o *qubit* que ela quer teleportar para Bob, Eq. (3.1), ela os projeta em um estado generalizado de Bell $|\Phi_j^k\rangle$, onde a princípio assumimos que $k \neq n$.

A probabilidade de Alice medir um estado generalizado de Bell particular $|\Phi_j^k\rangle$ é

$$p_1 = [f_1(\alpha,\beta)]^2, \quad p_2 = [f_2(\alpha,\beta)]^2, \tag{3.6}$$

$$p_3 = [f_2(\beta,\alpha)]^2, \quad p_4 = [f_1(\beta,\alpha)]^2, \tag{3.7}$$

com

$$f_1(\alpha,\beta) = \sqrt{\frac{|\alpha|^2 + k^2n^2|\beta|^2}{(1+k^2)(1+n^2)}}, \tag{3.8}$$

$$f_2(\alpha,\beta) = \sqrt{\frac{k^2|\alpha|^2 + n^2|\beta|^2}{(1+k^2)(1+n^2)}}. \tag{3.9}$$

(v) Após implementar sua medida, Alice comunica à Bob por um canal clássico o resultado que ela obteve. Note que ao Alice obter o resultado $|\Phi_j^k\rangle$, o estado de Bob

colapsa para o estado $U_j^\dagger |\phi_j\rangle_B$, com $|\phi_j\rangle_B$ dado pelas Eqs. (3.10)-(3.13).

(vi) Bob usa a informação revelada por Alice sobre o resultado de sua medida e aplica uma transformação unitária U_j no seu *qubit*. As transformações correspondentes a cada resultado da medida de Alice que Bob aplica são: $U_1 = \mathbb{1}$ a matriz identidade, $U_2 = \sigma_z$, $U_3 = \sigma_x$ ou $U_4 = \sigma_z\sigma_x$, com σ_i sendo as matrizes de Pauli. Logo, após Bob aplicar U_j no seu *qubit*. ele torna-se um dos quatro estados seguintes,

$$|\phi_1\rangle_B = \frac{\alpha|0\rangle_B + kn\beta|1\rangle_B}{\sqrt{|\alpha|^2 + k^2n^2|\beta|^2}}, \tag{3.10}$$

$$|\phi_2\rangle_B = \frac{k\alpha|0\rangle_B + n\beta|1\rangle_B}{\sqrt{k^2|\alpha|^2 + n^2|\beta|^2}}, \tag{3.11}$$

$$|\phi_3\rangle_B = \frac{n\alpha|0\rangle_B + k\beta|1\rangle_B}{\sqrt{n^2|\alpha|^2 + k^2|\beta|^2}}, \tag{3.12}$$

$$|\phi_4\rangle_B = \frac{kn\alpha|0\rangle_B + \beta|1\rangle_B}{\sqrt{k^2n^2|\alpha|^2 + |\beta|^2}}. \tag{3.13}$$

Em outras palavras, se Alice obtém o estado $|\Phi_j^k\rangle$ após medir seus dois *qubits* em um estado de Bell generalizado, o *qubit* de Bob ao final do protocolo de teletransporte é um estado correspondente $|\phi_j\rangle_B$. Vale mencionar que se $k = n = 1$ recuperamos o protocolo de teletransporte original [16], que possui $p_j = 1/4$ e $|\phi_j\rangle_B = \alpha|0\rangle_B + \beta|1\rangle_B$ para qualquer j.

Pelas Eqs. (3.10)-(3.13), percebemos que Bob obterá uma réplica exata do estado que Alice teleportou se ela escolheu $k = n$. Isso somente ocorre em dois dos quatro possíveis resultados medidos por Alice. Ou seja, Alice obtém $|\Phi_2^k\rangle$ ou $|\Phi_3^k\rangle$ quando $k = n$ (mesmo emaranhamento do canal). Esta condição para os valores k e n é conhecida por condição de *matching* [18, 20, 21, 24, 25]. No cenário que Alice usou o mesmo emaranhamento do canal de Bob e obteve $|\Phi_2^k\rangle$ ou $|\Phi_3^k\rangle$, os estados $|\phi_2\rangle_B$ e $|\phi_3\rangle_B$ são dados por $\alpha|0\rangle_B + \beta|1\rangle_B$ e, portanto, o protocolo de teletransporte foi bem sucedido. A probabilidade de um evento bem sucedido é

$$p_{suc}(n) = p_2 + p_3 = \frac{2n^2}{(1+n^2)^2}. \tag{3.14}$$

Chamamos a probabilidade anterior de probabilidade de sucesso. A Fig. 3.1 mostra a representação esquemática do protocolo de teletransporte.

Compreendido o protocolo de teletransporte, vamos agora explicar o protocolo de dis-

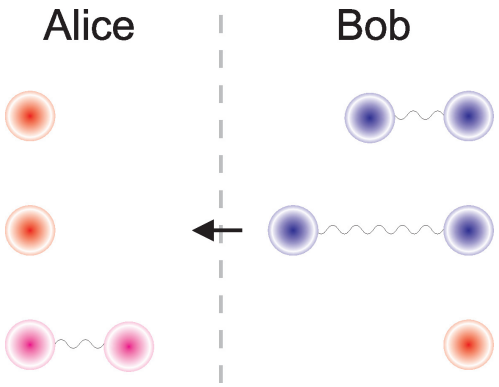

Figura 3.1: Representação esquemática do teletransporte probabilístico. Bob envia um *qubit* para Alice. Ela, por sua vez, realiza uma medida conjunta em seu *qubit* e o *qubit* recebido de Bob. Dependendo do resultado de Alice, o *qubit* de Bob pode pode se tornar uma réplica perfeita do *qubit* de Alice.

tribuição de chaves criptográficas quânticas GR10, originalmente proposto na Ref. [18]:

(i) Alice e Bob concordam de antemão sobre qual base ortogonal será usada para codificar os bits clássicos 0 e 1. A única restrição é que os vetores que geraram a base escolhida sejam não-ortogonais aos vetores usados para expressar o estado de Bell parcialmente emaranhado usado no teletransporte quântico probabilístico. Por exemplo, se o canal quântico preparado por Bob é dado por $|\Phi_1^n\rangle_{AB} = (|00\rangle_{AB} + n|11\rangle_{AB})/\sqrt{1+n^2}$, eles concordam que $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ codifica bit 0 e $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ o bit 1. Isto é, eles usam a base x para codificar os bits e a base z para escrever o estado de Bell generalizado. [2] Alice e Bob também concordam entre os possíveis valores de n. Na versão original do protocolo GR10 apenas dois valores são usados, n_1 e n_2.

(ii) Alice aleatoriamente prepara um *qubit* em um dos estados descritos anteriormente, $|+\rangle$ ou $|-\rangle$. Bob, por sua vez, cria um dos estados de Bell generalizados, $|\Phi_1^{n_1}\rangle_{AB}$ ou $|\Phi_1^{n_2}\rangle_{AB}$, enviando um dos *qubits* para Alice e mantendo o outro consigo.

(iii) Recebendo o *qubit* de Bob, Alice inicia o protocolo de teletransporte probabilístico previamente descrito. Especificamente, ela projeta seu *qubit* que codifica o bit clássico e o *qubit* enviado por Bob em um estado de Bell generalizado $|\Phi_j^k\rangle_{AA}$, com k

[2] Podemos sempre usar mais que uma base ortogonal para codificar o mesmo bit clássico, com estados não ortogonais codificando o mesmo bit. Se nós utilizarmos duas bases por exemplo, temos um protocolo de distribuição de chave secreta tipo BB84, onde o protocolo de teletransporte probabilístico funciona como uma camada extra de segurança ao protocolo BB84. Mas o ponto aqui é mostrar claramente que o protocolo GR10 é seguro mesmo utilizando somente *uma base ortogonal* para codificar os bits clássicos, como veremos na análise de segurança apresentada em capítulos posteriores.

aleatoriamente escolhido como n_1 ou n_2. Nesta parte do protocolo, *nem Bob avisa Alice do valor de n* escolhido para preparar o estado emaranhado, *nem Alice conta a Bob o valor de k* que ela escolheu para projetar seus *qubits*. Alice comunica a Bob somente qual estado de Bell parcialmente emaranhado $|\Phi_j^k\rangle_{AA}$ ela obteve, $j = 1, \ldots, 4$, mas não o valor de k.

(iv) Após descobrir qual foi o resultado da medida de Bell efetuada por Alice (o valor j do estado $|\Phi_j^k\rangle$, mas não o k), Bob implementa a transformação unitária correspondente para corrigir seu *qubit* como descrito anteriormente no protocolo de teletransporte. O *qubit* que Bob possui em mãos é um dos quatro possíveis estados listados nas Eqs. (3.10)-(3.13), onde $\alpha = |\beta| = 1/\sqrt{2}$. Ele então projeta seu *qubit* na base x. Se o resultado da medida é o estado $|+\rangle$, ele supõe que Alice teletransportou o bit 0, caso seja $|-\rangle$, ele associa ao bit o valor 1.

(v) Os passos (i) a (iv) são repetidos N vezes.

(vi) *Após Bob finalizar todas as medidas* nos N *qubits*, Alice e Bob revelam por meio de um canal clássico autenticado as informações sobre os emaranhamentos utilizados. Bob revela para quais casos ele usou o emaranhamento n_1 e para quais casos usou n_2 para preparar o canal quântico $|\phi_1^n\rangle$. Alice, por sua vez, conta a Bob se ela usou o mesmo emaranhamento de Bob ($k = n$) em cada medida, ou se ela usou um diferente. Eles descartam os casos em que ocorreu divergências ($k \neq n$), mantendo apenas os casos de *matching* ($k = n$). Ao final, cerca $N/2$ bits são mantidos e $N/2$ são descartados.

(vii) Nos $N/2$ bits restantes, Alice e Bob implementam uma nova fase de descarte. Esta nova fase é inerente ao protocolo de teletransporte probabilístico, já que Bob só pode *afirmar* que possui uma réplica do *qubit* de Alice se $k = n$ e se ela mediu os estados $|\Phi_2^n\rangle$ ou $|\Phi_3^n\rangle$. Portanto, eles descartam todos os casos em que ela obteve $|\Phi_1^n\rangle$ or $|\Phi_4^n\rangle$. Dessa forma, Bob pode afirmar que seus *qubits* restantes são os mesmos que Alice teleportou. Após essa nova seleção (*sifting*), os bits remanescentes formam a chave crua, a qual, a partir da Eq. (3.14), é dada por [18]

$$R = \left(\frac{p_{suc}(n_1)}{2} + \frac{p_{suc}(n_2)}{2} \right) \frac{N}{2}. \tag{3.15}$$

(viii) Por fim, Alice e Bob expõe parte da chave crua com o intuito de detectar a presença de monitoramento. Essa informação é aplicada para estimar a taxa de erro na execução

do protocolo no canal de comunicação quântico. Com esta informação, eles podem aumentar a segurança da chave clássica compartilhada através de protocolos clássicos de amplificação de privacidade e de reconciliação de informação.

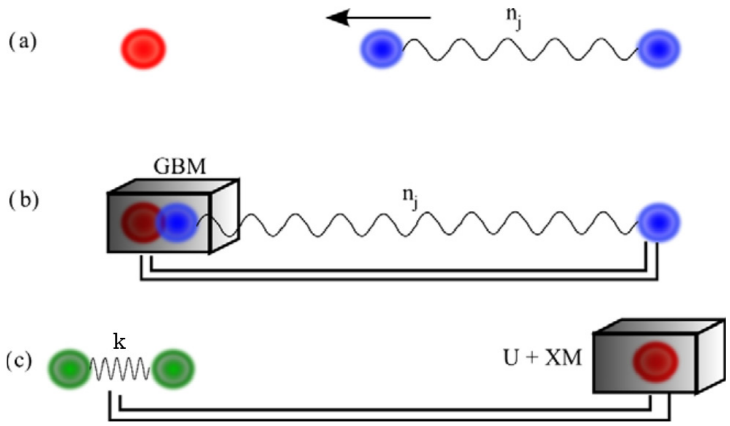

Figura 3.2: Representação esquemática do protocolo de criptografia GR10. Alice e Bob executam o protocolo de teletransporte probabilístico, onde Bob prepara um canal com emaranhamento n_j. Ao receber um dos *qubits* do canal de Bob, Alice realiza uma medida de Bell generalizada com emaranhamento k, o qual pode ser igual ou não a n_j. Dependendo do resultado de Alice, Bob aplica uma transformação unitária em seu *qubit*, obtendo uma cópia exata do bit teleportado. Figura extraída de [18].

É importante ter em mente que Alice não possui controle sobre o resultado da medida de Bell generalizada efetuada em seu *qubit* em conjunto com o recebido de Bob. Esse fato, característico do protocolo de teletransporte, é o ponto-chave que garante a segurança do protocolo GR10, conforme detalharemos nas análises de segurança adiante.

Capítulo 4

Análise de segurança do protocolo BB84

A análise de segurança apresentada aqui é baseada no artigo de revisão [8] que, por sua vez, se baseia nas técnicas de [44] e [45]. Diferentemente de [8, 44, 45], utilizaremos a decomposição de Schmidt para definir o estado final de Alice e Bob após Eva interferir na transmissão. A decomposição de Schmidt está implícita nas análise de segurança [8, 44, 45, 52], já que os autores consideram que o estado de Eva seja uma purificação do estado total após a intromissão da espiã Eva. O que faremos aqui é tirar a decomposição de Schmidt do plano de fundo e deixá-la em evidência desde o princípio no cálculo da segurança.

Na análise de segurança do BB84, consideramos que a chave será extraída somente da base z e que as outras bases de medidas são utilizadas para estimar o quanto de informação Eva possui sobre a base z. E como comentado na Sec. 2.3.3, consideramos todos os erros experimentais obtidos devido ao monitoramento de Eva no sistema, e que ela é somente limitada pelas leis da Física. Consideramos também que a chave seja utilizada apenas uma vez com amplificação de privacidade e correções de erros perfeitas. A amplificação de privacidade e correções de erros são protocolos clássicos que aumentam a correlação entre Alice e Bob, garantindo que os bits enviados por Alice sejam os mesmos aferidos por Bob. Por fim, utilizamos uma representação baseada em emaranhamento (*entanglement-based representation* - EBR) [8], para extrairmos a segurança.

Não necessariamente a representação baseada em emaranhamento (EBR) é uma descrição real do protocolo de envio, mas ela deve reproduzir fielmente os resultados do protocolo, isto é, toda a sua estatística. Portanto, a EBR é um estado emaranhado que representará matematicamente os resultados do protocolo original de transmissão de chave [8]. No caso

do BB84 na base z temos sua EBR dada por

$$|\phi_1\rangle = |\phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right). \tag{4.1}$$

Este é um dos quatro estados de Bell e como podemos ver, ele reproduz exatamente as estatísticas que Alice e Bob obtém no esquema original de preparação e medida do BB84 [4]. De fato, se Alice medir seus *qubits* na base z, eles obterão chances iguais de medirem o *qubit* $|0\rangle$ ou $|1\rangle$. Notando que o estado $|\phi^+\rangle$ representado na base x é $|\phi^+\rangle = \left(|{+}{+}\rangle + |{-}{-}\rangle\right)\sqrt{2}$, temos também uma perfeita correlação na base x, como ocorre no protocolo BB84 quando Alice prepara seu *qubit* na base x e Bob mede também nesta base. O estado de Bell $|\phi^+\rangle$ juntamente com os outros três,

$$|\phi_2\rangle = |\phi^-\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right), \tag{4.2}$$

$$|\phi_3\rangle = |\psi^+\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right), \tag{4.3}$$

$$|\phi_4\rangle = |\psi^-\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right), \tag{4.4}$$

formam uma base completa e ortonormal que pode ser usada para expandir qualquer estado puro de dois *qubits*.

No cenário perfeito, depois de cada envio da versão baseada em emaranhamento do protocolo BB84, Alice e Bob compartilham o estado $|\phi^+\rangle$. Após repetir N vezes o envio dos *qubits*, eles compartilham o estado $|\phi^+\rangle^{\otimes N}$. Contudo, na presença de Eva e no nível de ataques coletivos, Eva perturba cada *qubit* enviado para Bob usando a mesma estratégia [1]. Com isso temos que após Eva monitorar a transmissão, o estado compartilhado por Alice, Bob e agora Eva, após N envios, pode ser escrito como

$$|\Psi\rangle_{ABE}^{\otimes N} = |\Psi\rangle_{ABE} \otimes \cdots \otimes |\Psi\rangle_{ABE}, \tag{4.5}$$

onde

$$|\Psi\rangle_{ABE} = \sum_{j=1}^{4} \sqrt{\lambda_j}|\Phi_j\rangle_{AB}|\epsilon_j\rangle_E. \tag{4.6}$$

A Eq. (4.6) é uma purificação do estado que descreve Alice, Bob, e Eva, e nós sempre pode-

[1] Mesmo lidando com ataques coletivos, a análise realizada permanece válida para o caso de ataques coerentes devido aos resultados das Refs. [44–47]. E se Eva usar estratégias distintas, Alice e Bob podem detectar a espionagem analisando diferentes amostras (*sub-ensembles*) da chave bruta. Isso resultará em taxas de erros distintas, fazendo com que Alice e Bob descubram que estão sendo espionados.

mos usar este estado global após a interferência de Eva devido ao teorema da decomposição de Schmidt [34] (veja a demonstração deste teorema no apêndice C). Quando temos um espaço de Hilbert descrevendo os estados de Eva grande o suficiente, nós sempre podemos escrever $|\Psi\rangle_{ABE}$ como dado anteriomente, com todos os λ_j não negativos, $\sum_j \lambda_j = 1$ e $|\epsilon_j\rangle$ formando uma base ortonormal.

Após N envios o estado global compartilhado por todas as partes é $|\Psi\rangle_{ABE}^{\otimes N}$. Isto é, nós temos um *ensemble* de N réplicas do estado $|\Psi\rangle_{ABE}$. Então, todas as correlações entre AB (Alice e Bob) e E (Eva) podem ser analisadas diretamente de $|\Psi\rangle_{ABE}$. Note que sem a interferência de Eva ou ruídos, nós temos que $\lambda_1 = 1$ e $\lambda_j = 0$, $j = 2, 3, 4$. No entanto, quando Eva está presente, nós temos em geral $\lambda_j \neq 0$, para todos os j.

Usando a Eq. (4.6), nós conseguimos determinar como a presença de Eva afeta o protocolo BB84 ou, equivalentemente, podemos estudar como a presença de ruído muda as estatísticas no protocolo BB84 quando comparadas às do caso sem ruído. Quando Eva está presente e Alice e Bob usam a mesma base para preparar e enviar seus *qubits*, a probabilidade de eles concordarem no resultado não é mais um.

Considerando as amostras na qual Alice e Bob utilizaram a base z, a probabilidade de concordarem sobre o valor do bit enviado é $1 - \varepsilon_z = p_A(0)p_{B|A}(0|0) + p_A(1)p_{B|A}(1|1)$, enquanto a probabilidade de discordarem (erro) é $\varepsilon_z = p_A(0)p_{B|A}(1|0) + p_A(1)p_{B|A}(0|1)$. Contudo, um resultado padrão da teoria de probabilidades diz que $p_{AB}(a, b) = p_A(a)p_{B|A}(b|a)$, onde $p_{AB}(a, b)$ é a probabilidade conjunta de Alice e Bob obterem simultaneamente os valores a e b respectivamente. Isto leva a

$$\varepsilon_z = p_{AB}(0, 1) + p_{AB}(1, 0) \tag{4.7}$$

e uma expressão similar para $1 - \varepsilon_z$.

Aplicando o postulado da medida da mecânica quântica, temos que

$$p_{AB}(a, b) = \mathrm{tr}\left\{ \left(|a\rangle_A\langle a| \otimes |b\rangle_B\langle b| \otimes \mathbb{1}_E\right) \rho^{ABE} \right\}, \tag{4.8}$$

onde

$$\rho^{ABE} = |\Psi\rangle_{ABE}\langle\Psi|, \tag{4.9}$$

com $|\Psi\rangle_{ABE}$ dado pela Eq. (4.6).

Inserindo a Eq. (4.9) na (4.8) obtemos

$$p_{AB}(0,1) = p_{AB}(1,0) = \frac{\lambda_3 + \lambda_4}{2} \tag{4.10}$$

e consequentemente

$$\varepsilon_z = \lambda_3 + \lambda_4. \tag{4.11}$$

Se nós considerarmos os casos onde Alice e Bob utilizam na base x, um cálculo similar leva à seguinte probabilidade de Bob cometer um erro no valor do bit enviado por Alice,

$$\varepsilon_x = \lambda_2 + \lambda_4. \tag{4.12}$$

Estamos prontos agora para calcular as duas quantidades necessárias para obter a fração da chave secreta do protocolo BB84, Eq. (2.122). Nós começaremos calculando a informação mútua e, em seguida calcularemos a quantidade de Holevo.

4.1 A informação mútua do protocolo BB84

Para determinar a informação mútua entre Alice e Bob, nós consideramos o caso no qual eles usaram a base z para preparar e medir seus *qubits*. O caso em que ambos usaram a base x será empregada apenas para estimar o erro ε_x necessários para a computação da quantidade de Holevo [8].

Devido a simetria do estado $\rho^{AB} = \mathrm{tr}_E \left\{\rho^{ABE}\right\}$ sobre permutação dos *qubits* de Alice com os de Bob, nós temos que $p_A(a) = p_B(a)$. Como

$$p_A(a) = \mathrm{tr}\left\{\left(|a\rangle_A\langle a| \otimes \mathbb{1}_{BE}\right)\rho^{ABE}\right\} \tag{4.13}$$

obtemos

$$p_A(0) = p_A(1) = p_B(0) = p_B(1) = 1/2. \tag{4.14}$$

Usando a Eq. (4.14), não é difícil ver que a Eq. (2.1), $H(X) = \sum_x\{-p_X(x)\log[p_X(x)]\}$, dá

$$H(A) = H(B) = 1. \tag{4.15}$$

Agora, usando que $p_{AB}(a,b) = p_A(a)p_{B|A}(b|a)$ e que $\sum_b p_{AB}(a,b) = p_A(a)$, é possível

calcular a entropia condicional, Eq. (2.4),

$$H(B|A) = -\sum_{a,b} p_{A,B}(a,b)\log[p_{B|A}(b|a)]. \tag{4.16}$$

Com o auxílio das Eqs. (4.10) e (4.14) temos

$$H(B|A) = h(\varepsilon_z), \tag{4.17}$$

onde $h(x) = -x\log x-(1-x)\log(1-x)$, é a entropia binária. Para obtermos este resultado, usamos que $p_{AB}(0,0) = p_{AB}(1,1) = (\lambda_1+\lambda_2)/2 = (1-\lambda_3-\lambda_4)/2$ em conjunto com a Eq. (4.11) para escrevermos a Eq. (4.17) como apresentada acima.

Combinando as Eqs. (4.15) e (4.17) finalmente obtemos a informação mútua entre Alice e Bob, Eq. (2.6),

$$I(A:B) = 1 - h(\varepsilon_z). \tag{4.18}$$

Observe que se $\varepsilon_z = 0$, $I(A:B) = 1$. Isto é, os bits de Bob estão perfeitamente correlacionados com os bits de Alice. Por outro lado, se $\varepsilon_z = 1/2$, temos que $h(1/2) = 1$ reduzindo a informação mútua a zero.

4.2 A quantidade de Holevo do protocolo BB84

Analisando a quantidade de Holevo, Eq. (2.105), que diz que, $\chi(A:\rho^E) = S(\rho^E) - \sum_a p_A(a)S(\rho_a^E)$, vemos que para computá-la precisamos de $\rho^E = \mathrm{tr}_{AB}\left\{\rho^{ABE}\right\}$, estado quântico de Eva após ela interagir com os *qubits* enviados por Alice, e ρ_a^E, a descrição do sistema físico de Eva se ela souber que Alice projetou seu *qubit* no estado $|a\rangle$.

Tomando o traço sobre Alice e Bob em ρ^{ABE}, Eq. (4.9), obtemos

$$\rho^E = \sum_{j=1}^{4} \lambda_j |\epsilon_j\rangle_E\langle\epsilon_j|. \tag{4.19}$$

Com isso obtemos a entropia de von Neumman, Eq. (2.24), vale

$$S(\rho^E) = -\sum_{j=1}^{4} \lambda_j \log\lambda_j. \tag{4.20}$$

Agora, a partir do postulado da medida, Eqs. (2.103) e (2.104), e utilizando as Eqs. (4.9)

e (4.14), obtemos

$$\begin{aligned}\rho_0^E &= \sum_{j=1}^{4}\lambda_j \left|\epsilon_j\right\rangle_E\langle\epsilon_j| + \sqrt{\lambda_1\lambda_2}\left(\left|\epsilon_1\right\rangle_E\langle\epsilon_2| + h.c.\right) \\ &\quad +\sqrt{\lambda_3\lambda_4}\left(\left|\epsilon_3\right\rangle_E\langle\epsilon_4| + h.c.\right), \qquad (4.21)\\ \rho_1^E &= \sum_{j=1}^{4}\lambda_j \left|\epsilon_j\right\rangle_E\langle\epsilon_j| - \sqrt{\lambda_1\lambda_2}\left(\left|\epsilon_1\right\rangle_E\langle\epsilon_2| + h.c.\right) \\ &\quad -\sqrt{\lambda_3\lambda_4}\left(\left|\epsilon_3\right\rangle_E\langle\epsilon_4| + h.c.\right), \qquad (4.22)\end{aligned}$$

onde $h.c.$ denota o Hermitiano conjugado do operador que aparece antes do símbolo $h.c.$. Os autovalores de ambos operadores ρ_0^E e ρ_1^E são $0, 0, \lambda_1+\lambda_2$, e $\lambda_3+\lambda_4$. Consequentemente a entropia de von Neumann, Eq. (2.24), para esses estados torna-se

$$S(\rho_0^E) = S(\rho_1^E) = h(\varepsilon_z), \qquad (4.23)$$

onde usamos a Eq. (4.11) para eliminar os λ's em favor da taxa de erro ε_z.

As Eqs. (4.20) e (4.23) quando inseridas na definição da quantidade de Holevo, Eq. (2.105), dá

$$\chi(A:\rho^E) = -\sum_{j=1}^{4}\lambda_j\log\lambda_j - h(\varepsilon_z), \qquad (4.24)$$

onde usamos que $p_A(a) = 1/2$ para obter a expressão acima.

4.3 A fração da chave secreta do protocolo BB84

Se nós inserirmos as Eqs. (4.18) e (4.24) no limite de Devetak-Winter (2.122), obtemos a seguinte expressão para a fração da chave secreta do protocolo BB84,

$$\begin{aligned}r &= 1 - h(\varepsilon_z) - \max_{\text{Eve}}\left\{-\sum_{j=1}^{4}\lambda_j\log\lambda_j - h(\varepsilon_z)\right\} \\ &= 1 - h(\varepsilon_z) + h(\varepsilon_z) - \max_{\text{Eve}}\left\{-\sum_{j=1}^{4}\lambda_j\log\lambda_j\right\} \\ &= 1 + \min_{\text{Eve}}\left\{\sum_{j=1}^{4}\lambda_j\log\lambda_j\right\}. \qquad (4.25)\end{aligned}$$

Perceba que para chegar na última igualdade usamos que $-\max_x[f(x)] = \min_x[-f(x)]$, i.e., o negativo do máximo valor da função f sobre seu domínio é igual ao mínimo de $-f$ no mesmo domínio.

Para o protocolo BB84 original, temos que (veja as Eqs. (4.11), (4.12))

$$\lambda_3 + \lambda_4 = \varepsilon_z, \tag{4.26}$$

$$\lambda_2 + \lambda_4 = \varepsilon_x, \tag{4.27}$$

$$\sum_{i=1}^{4} \lambda_i = 1. \tag{4.28}$$

Note que a última é a condição de normalização de ρ^{ABE}. Como temos quatro λ's, não podemos expressá-los unicamente em termos das taxas de erros experimentalmente determinadas ε_z e ε_x. Isto significa que precisamos minimizar a expressão dentro das chaves na Eq. (4.25) para obter um limite inferior da fração da chave secreta em função das taxas de erros.

Usando a Eq. (4.26) vemos que $\lambda_4 = \varepsilon_z - \lambda_3$. Assim, $0 \leq \lambda_3 \leq \varepsilon_z$ pois nenhum λ_j pode ser negativo. Isto implica que nós podemos escrever

$$\lambda_3 = v\varepsilon_z, \tag{4.29}$$

$$\lambda_4 = (1-v)\varepsilon_z, \tag{4.30}$$

onde $v \in [0, 1]$.

Agora, a Eq. (4.28) pode ser reescrita como $\lambda_2 = 1 - \lambda_1 - \lambda_3 - \lambda_4 = (1 - \varepsilon_z) - \lambda_1$, onde usamos a Eq. (4.26) para obtermos a última igualdade. Como λ_2 é não negativo, $0 \leq \lambda_1 \leq 1 - \varepsilon_z$ e, como antes, podemos escrever

$$\lambda_1 = u(1-\varepsilon_z), \tag{4.31}$$

$$\lambda_2 = (1-u)(1-\varepsilon_z), \tag{4.32}$$

com $u \in [0, 1]$.

Os parâmetros u e v não são independentes como podemos ver pela Eq. (4.27), isto implica que $(1-u)(1-\varepsilon_z) + (1-v)\varepsilon_z = \varepsilon_x$. Resolvendo para u chegamos a

$$u = \frac{1 - \varepsilon_x - v\varepsilon_z}{1 - \varepsilon_z}. \tag{4.33}$$

Agora temos apenas v como parâmetro livre. Inserindo a Eq. (4.33) nas Eqs. (4.31) e (4.32) e usando as Eqs. (4.29)-(4.32), podemos escrever a fração da chave-secreta do protocolo BB84, Eq. (4.25), como

$$r = 1 + \min_{\text{Eve}} \left\{ \theta\left(1 - \varepsilon_x - \varepsilon_z v\right) + \theta\left(\varepsilon_x - \varepsilon_z(1-v)\right) + \theta(\varepsilon_z - \varepsilon_z v) + \theta(\varepsilon_z v) \right\}, \tag{4.34}$$

onde

$$\theta(x) = x \log x. \tag{4.35}$$

Minimizando r em função de v, i.e., resolvendo $dr/dv = 0$ nos dá

$$v = 1 - \varepsilon_x, \tag{4.36}$$

que de fato é um ponto de mínimo para r pois um cálculo direto leva a $d^2r/dv^2 > 0$ quando temos $v = 1 - \varepsilon_x$.

Utilizando as Eqs. (4.33) e (4.36), podemos expressar os λ's que dão um limite inferior para a fração da chave-secreta como

$$\lambda_1 = (1 - \varepsilon_x)(1 - \varepsilon_z), \tag{4.37}$$

$$\lambda_2 = \varepsilon_x(1 - \varepsilon_z), \tag{4.38}$$

$$\lambda_3 = \varepsilon_z(1 - \varepsilon_x), \tag{4.39}$$

$$\lambda_4 = \varepsilon_z \varepsilon_x. \tag{4.40}$$

Inserindo as Eqs.(4.37)-(4.40) em (4.25), obtemos o limite inferior da fração da chave-secreta do protocolo BB84 em termos das quantidades mensuráveis ε_z e ε_x,

$$r = 1 - h(\varepsilon_x) - h(\varepsilon_z). \tag{4.41}$$

As quantidades ε_x e ε_z são as probabilidades de Bob obter um resultado equivocado (taxa de erro) para o valor do bit enviado por Alice quando ambos utilizam a mesma base (base x ou base z) para preparar e medir o *qubit* que codifica aquele bit.

Supondo que os erros são simétricos, isto é, $\varepsilon_x = \varepsilon_z = \varepsilon$, a fração da chave secreta pode ser reescrita como

$$r = 1 - 2h(\varepsilon), \tag{4.42}$$

onde não é difícil de se ver que $r > 0$ quando temos

$$\varepsilon \lesssim 11\%. \tag{4.43}$$

Em outras palavras, para taxas simétricas de erros abaixo de 11% o protocolo BB84 pode ser considerado seguro [8].

Capítulo 5

Protocolo BB84 com uma base adicional

Antes de explorarmos um novo método para calcular a fração da chave secreta do protocolo BB84, vamos ver o que acontece quando Alice e Bob alteram o protocolo BB84 original. A mudança que estamos sugerindo é considerar que ao invés de Alice e Bob utilizarem a base x e a base z, eles realizam a preparação e a medida também considerando a base y. Esta alteração é conhecida como protocolo BB84 seis-estados [8, 42, 48–50]. Ou seja, ele utiliza dois estados a mais que o protocolo BB84 original. O motivo de empregarem essa mudança é a falta de informação que Alice e Bob possuem para determinar unicamente os valores dos λ's da purificação do estado que descreve o sistema de Alice, Bob e Eva dado pela Eq. (4.6), $|\Psi\rangle_{ABE} = \sum_j \sqrt{\lambda_j}\,|\Phi_j\rangle_{AB}\,|\epsilon_j\rangle_E$. No capítulo anterior vimos que eles contavam com apenas três equações para estimarem os valores dos λ's,

$$\begin{aligned} \lambda_3 + \lambda_4 &= \varepsilon_z, \\ \lambda_2 + \lambda_4 &= \varepsilon_x, \\ \sum_{i=1}^{4} \lambda_i &= 1. \end{aligned}$$

Portanto, ao utilizarem uma nova base, Alice e Bob terão dados suficientes para definir todos os λ's.

Contudo, podemos ver que a representação baseada em emaranhamento, Eq. (4.1), do

protocolo BB84 é anti-correlacionada quando escrita na base y,

$$|\phi_1\rangle = \frac{1}{\sqrt{2}} \left(|y_0 y_1\rangle + |y_1 y_0\rangle \right), \tag{5.1}$$

onde $|y_0\rangle = (|0\rangle + \mathrm{i}\,|1\rangle)\sqrt{2}$ e $|y_1\rangle = (|0\rangle - \mathrm{i}\,|1\rangle)\sqrt{2}$. Então, para melhor compreendermos as implicações desta anti-correlação e como corrigi-la, faremos a análise que segue.

5.1 Observações sobre a representação baseada em emaranhamento

A representação baseada em emaranhamento, como dito anteriormente, é um estado quântico que representa a execução do protocolo criptográfico original [8]. Consequentemente, se a segurança é constatada para as estatísticas da representação baseada em emaranhamento (EBR), e temos que o protocolo, por conter essas mesmas estatísticas, também é seguro. É comum os protocolos de segurança quânticos utilizarem mais de uma base para a codificação dos bits. E vimos no BB84 que a EBR pode coincidir. Isto é, a representação baseada em emaranhamento da base z, Eq. (4.1), é a mesma que a da base x, pois este estado de Bell é invariante perante essa transformação,

$$|\phi_1\rangle_{AB} = \frac{1}{\sqrt{2}} \left(|00\rangle_{AB} + |11\rangle_{AB} \right) = \frac{1}{\sqrt{2}} \left(|{+}{+}\rangle_{AB} + |{-}{-}\rangle_{AB} \right). \tag{5.2}$$

No entanto, pode ocorrer que a representação baseada em emaranhamento seja diferente ao usarmos uma outra base, como ocorre se usássemos para o protocolo BB84 a base y, Eq. (5.1). Neste caso

$$|\phi_1\rangle_{AB} \neq \frac{1}{\sqrt{2}} \left(|y_0 y_0\rangle_{AB} + |y_1 y_1\rangle_{AB} \right). \tag{5.3}$$

Entretanto, existe ao menos uma transformação local que relaciona o estado (5.1) com $\left(|y_0 y_0\rangle_{AB} + |y_1 y_1\rangle_{AB} \right)/\sqrt{2}$. Esta transformação consiste em aplicar $\mathbb{1}_A \otimes \sigma_{zB}$ no estado $|\phi_1\rangle_{AB}$. Em outras palavras, implementamos um *bit flip* no *qubit* que pertencerá a Bob. Ao utilizarmos esse artifício surge uma questão que deve ser respondida: Se uma transformação unitária é aplicada no estado, a mesma decomposição de Schmidt após a interferência de Eva é válida para as diferentes bases?

Primeiramente, a representação baseada em emaranhamento de Alice, Bob e Eva em

uma base qualquer antes intromissão de Eva é

$$|\psi_0\rangle_{ABE} = |\psi\rangle_{AB} \otimes |\epsilon\rangle_E \,. \tag{5.4}$$

Então, após Alice enviar o *qubit* a Bob, Eva aplica um mapa $\mathcal{E}$ neste estado para extrair alguma informação sobre o *qubit* enviado. Este mapa pode ser representado por uma transformação unitária se considerarmos, sem perda de generalidade, o espaço de Hilbert de Eva grande o suficiente [34],

$$|\psi_f\rangle_{ABE} = U_{ABE} \, |\psi\rangle_{AB} \otimes |\tilde{\epsilon}\rangle_E \,, \tag{5.5}$$

onde o estado $|\tilde{\epsilon}\rangle_E$ pertence a Eva. Pela decomposição de Schmidt,

$$|\psi_f\rangle_{ABE} = \sum_i \sqrt{a_i} \, |\psi_i\rangle_{AB} \otimes |\tilde{\epsilon}_i\rangle_E \,. \tag{5.6}$$

Considere, agora, que a representação baseada em emaranhamento da segunda base $|\varphi_0\rangle_{ABE}$ está relacionada com a primeira por uma transformação unitária $|\varphi_0\rangle_{ABE} = V_{AB} \otimes \mathbb{1}_E \, |\psi_0\rangle_{ABE}$. Então, Alice pode aplicar V_{AB} para que a representação baseada em emaranhamento da base anterior reproduza as mesmas estatísticas na nova base.

Se Alice aplicar V_{AB} *antes* dela enviar o *qubit* para Bob, certamente não poderemos utilizar que o estado de Alice, Bob e Eva para essa segunda base é a transformação unitária $V_{AB} \otimes \mathbb{1}_E$ da decomposição de Schmidt (5.6), isto é,

$$|\varphi_f\rangle_{ABE} = (V_{AB} \otimes \mathbb{1}_E) \, |\psi_f\rangle_{ABE} \tag{5.7}$$

pois o estado final da segunda base é

$$|\tilde{\varphi}_f\rangle_{ABE} = U_{ABE} \cdot (V_{AB} \otimes \mathbb{1}_E) \, |\psi\rangle_{AB} \otimes |\tilde{\epsilon}\rangle_E \,. \tag{5.8}$$

Consequentemente, nós não podemos garantir que a Eq. (5.8) é igual a Eq. (5.7), pois em geral U_{ABE} não comuta com $V_{AB} \otimes \mathbb{1}_E$. [1]

No entanto, se a transformação unitária for aplicada *após* ela enviar o *qubit* para Bob, então poderemos utilizar a mesma decomposição de Schmidt para extrair as estatísticas

[1] Lembramos que Eva não tem conhecimento se Alice aplicou ou não a transformação, portanto ela não tem motivo para utilizar uma estratégia diferente, já que ela pode ser descoberta ao aplicar esta nova estratégia de ataque de segurança.

em ambas as bases. Em outras palavras, se $V_{AB} = V_A \otimes V_B$ forem operações locais, então

$$\begin{aligned} |\varphi_f\rangle_{ABE} &= (V_{AB} \otimes \mathbb{1}_E) |\psi_f\rangle_{ABE} && (5.9) \\ &= \sum_i \sqrt{a_i} (V_A \otimes V_B) |\psi_i\rangle_{AB} \otimes |\tilde{\epsilon}_i\rangle_E . && (5.10) \end{aligned}$$

Deste modo, as estatísticas de ambas as bases contribuem para determinar os valores dos coeficientes a_i do estado dado pela Eq. (5.6). Em outras palavras, se V_{AB} for aplicada localmente após o envio, temos que a representação baseada em emaranhamento da primeira base, Eq. (5.4), é válida para ambas as bases. [2]

Considerando a análise aqui, se existir um $V_A \otimes V_B$ unitário tal que a Eq. (4.1) torne-se a representação baseada em emaranhamento na base y do protocolo BB84 seis-estados, então podemos usar a Eq. (4.6) como decomposição de Schmidt para obter as estatísticas nessa base. E essa transformação existe pois,

$$\frac{1}{\sqrt{2}} (|y_0 y_0\rangle + |y_1 y_1\rangle) = (\mathbb{1}_A \otimes \sigma_{zB}) |\phi_1\rangle , \tag{5.11}$$

com σ_z a matriz de Pauli escrita na base z. Vamos verificar uma aplicação direta deste raciocínio na seção a seguir.

5.2 Protocolo BB84 seis-estados

Retornando ao protocolo BB84 seis-estados, consideramos que Bob aplica um *bit flip* σ_z quando Alice e ele utilizam a base y, de modo que os resultados estatísticos previstos serão coerentes aos resultados reais. Logo, poderemos utilizar a representação baseada em emaranhamento dada pela Eq. (4.6) para gerar as estatísticas das bases x e z e também da base y. Assim como foi feito para os envios nas bases x e y, definiremos a taxa de erro da base y como

$$\varepsilon_y = p_{A,B}(y_0, y_1) + p_{A,B}(y_1, y_0). \tag{5.12}$$

Então, aplicando o postulado da medida da mecânica quântica, juntamente com a alteração necessária de Bob, as probabilidades serão obtidas da seguinte maneira

$$p_{AB}(a,b) = \mathrm{tr} \left\{ (|a\rangle_A \langle a| \otimes |b\rangle_B \langle b| \otimes \mathbb{1}_E) \cdot \left[(\mathbb{1}_{AE} \otimes \sigma_{zB}) \rho^{ABE} (\mathbb{1}_{AE} \otimes \sigma_{zB}) \right] \right\}, \tag{5.13}$$

[2] Vale ressaltar que a representação baseada em emaranhamento (5.4), no sentido de aplicar transformações para obter as estatísticas corretas, funciona similarmente a um canal quântico de comunicação.

onde ρ^{ABE} é a Eq. (4.9). Calculando a equação acima para a base y obtemos

$$p_{A,B}(y_0, y_1) = p_{A,B}(y_1, y_0) = \frac{\lambda_2 + \lambda_3}{2} \tag{5.14}$$

e consequentemente

$$\varepsilon_y = \lambda_2 + \lambda_3. \tag{5.15}$$

Acrescentando a Eq. (5.15) às Eqs. (4.26)-(4.28), obtemos o seguinte conjunto de equações:

$$\begin{aligned} \lambda_3 + \lambda_4 &= \varepsilon_z, \\ \lambda_2 + \lambda_4 &= \varepsilon_x, \\ \lambda_2 + \lambda_3 &= \varepsilon_y, \\ \sum_{i=1}^{4} \lambda_i &= 1. \end{aligned} \tag{5.16}$$

Como temos quatro equações e quatro incógnitas, o sistema linear possui uma única solução possível e determinada para os valores dos λ's em função das taxas de erros:

$$\lambda_1 = 1 - \frac{\varepsilon_x + \varepsilon_y + \varepsilon_z}{2}, \tag{5.17}$$

$$\lambda_2 = \frac{\varepsilon_x + \varepsilon_y - \varepsilon_z}{2}, \tag{5.18}$$

$$\lambda_3 = \frac{-\varepsilon_x + \varepsilon_y + \varepsilon_z}{2}, \tag{5.19}$$

$$\lambda_4 = \frac{\varepsilon_x - \varepsilon_y + \varepsilon_z}{2}. \tag{5.20}$$

Substituindo as Eqs. (5.17)-(5.20) na função da fração da chave secreta r, Eq. (4.25), encontramos o limite de segurança do BB84 seis-estados dependendo somente dos dados experimentais, ε_x, ε_y e ε_z:

$$\begin{aligned} r = {} & 1 + \theta\left(1 - \frac{\varepsilon_x + \varepsilon_y + \varepsilon_z}{2}\right) + \theta\left(\frac{\varepsilon_x + \varepsilon_y - \varepsilon_z}{2}\right) \\ & + \theta\left(\frac{-\varepsilon_x + \varepsilon_y + \varepsilon_z}{2}\right) + \theta\left(\frac{\varepsilon_x - \varepsilon_y + \varepsilon_z}{2}\right), \end{aligned} \tag{5.21}$$

com θ dado pela Eq. (4.35). Este resultado, diferentemente do obtido para o BB84 original, Eq. (4.41), não é uma minimização da fração da chave secreta r, Eq. (4.34), mas sim o valor *exato* da fração da chave secreta pois possuímos estatísticas suficientes para determinar

todos os λ's inequivocamente.

E para taxas de erros simétricos, $\varepsilon_x = \varepsilon_y = \varepsilon_z = \varepsilon$, a fração da chave secreta (5.21) vale

$$r = 1 + \left(1 - \frac{3\varepsilon}{2}\right) \log \left(1 - \frac{3\varepsilon}{2}\right) + 3 \left(\frac{\varepsilon}{2}\right) \log \left(\frac{\varepsilon}{2}\right). \tag{5.22}$$

Consequentemente, r é zero quando $\varepsilon \approx 12,61\%$. Isto quer dizer que, se Alice e Bob determinam uma taxa de erro maior que $12,61\%$ eles devem descartar a chave gerada pois ela foi comprometida. Em outras palavras, Eva tem maior conhecimento sobre a chave que Alice e Bob compartilham.

Como podemos ver aqui, a taxa máxima de erro simétrico permitida para que a chave criada possa ser considerada segura é menor que $12,61\%$, valor maior do obtido com o protocolo BB84 original, 11%. O que faremos a seguir é explorar um teorema da mecânica quântica para mostrar que podemos obter $12,61\%$ para a taxa de erro mesmo utilizando somente o protocolo BB84 original. Essa ferramenta a ser explorada é a escolha da base para expandir os estados de Alice e Bob na decomposição de Schmidt.

Parte II

Resultados originais

Capítulo 6

Revisitando o protocolo BB84

O protocolo BB84 original aparenta não possuir estatísticas suficientes para obtermos um valor exato da fração da chave secreta r. Levando em conta este fato, implementar uma base a mais para executar o protocolo BB84 sanou essa aparente lacuna. Como visto no Cap. 5, a informação extra da aplicação de uma base adicional resultou em dados experimentais suficientes para determinarmos os λ's unicamente em função das taxas de erros das bases utilizadas, Eqs. (5.17)-(5.20). Consequentemente, foi possível determinar o valor exato da fração da chave secreta para o protocolo BB84 seis-estados, não sendo necessário realizar uma minimização para estimar o limite inferior de segurança como feito no protocolo BB84 original, Cap. 4.

Embora o uso da base adicional resolveu o problema da minimização, ela não veio sem custo. No protocolo BB84, quando Alice e Bob utilizam bases diferentes para envio e medida eles devem descartar esse *qubit*, pois o *qubit* obtido na medida feita por Bob não está correlacionado ao *qubit* enviado por Alice. Em outras palavras, Bob não teria certeza de que o bit originado da decodificação do *qubit* que ele mediu é o mesmo que Alice codificou. Então, ao adicionarmos uma base a mais no protocolo BB84 aumentamos o número de *qubits* descartados.

De fato, no protocolo BB84 original, a probabilidade de Alice e Bob utilizarem a mesma base é 1/2. Já no protocolo BB84 seis-estados, a probabilidade deles usarem a mesma base reduz-se a 1/3. Implicando que 2/3 dos *qubits* serão descartados durante a execução do protocolo. Isso indica que ao usarem a base adicional, Alice e Bob, na média, terão que descartar aproximadamente 33% a mais de *qubits* do que eles descartariam usando o protocolo BB84 originalmente proposto.

No entanto, a aparente falta de estatística no protocolo BB84 original é devido a de-

composição de Schmidt utilizada. Neste capítulo vamos mostrar que não há necessidade de usarmos uma base adicional para obtermos o mesmo limite inferior de segurança do protocolo BB84 seis-estados. E para obtermos esse resultado vamos explorar que a purificação de um operador densidade não é única.

6.1 A decomposição de Schmidt e a segurança do protocolo BB84

Após a intromissão de Eva, ela perturba o estado compartilhado entre Alice e Bob adicionando erros. O estado final compartilhado por Alice, Bob e Eva pode ser representado por uma decomposição de Schmidt, apêndice C. No entanto, podemos escolher diferentes bases ortonormais para representarmos os estados de Alice e Bob. Vale notar que a base escolhida para expandirmos os estados de Alice e Bob deve satisfazer os dados experimentais originados da execução do protocolo. Sendo assim, ao invés da Eq. (4.6), uma perfeita e legítima decomposição de Schmidt representando o estado de Alice, Bob e Eva é

$$|\tilde{\Psi}\rangle_{ABE} = \sum_{j=1}^{4} \sqrt{\tilde{\lambda}_j} |\tilde{\Phi}_j\rangle_{AB} |\tilde{\epsilon}_j\rangle_E, \tag{6.1}$$

onde

$$|\tilde{\Phi}_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \tag{6.2}$$

$$|\tilde{\Phi}_2\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \tag{6.3}$$

$$|\tilde{\Phi}_3\rangle = |01\rangle, \tag{6.4}$$

$$|\tilde{\Phi}_4\rangle = |10\rangle, \tag{6.5}$$

abrangem uma base ortonormal completa que pode ser usada para descrever qualquer estado puro de dois *qubits*. Note que $|\tilde{\Phi}_1\rangle = |\phi_1\rangle$ e $|\tilde{\Phi}_2\rangle = |\phi_2\rangle$, onde $|\phi_1\rangle$ e $|\phi_2\rangle$ são dados pelas Eqs. (4.1) e (4.2). Quando Eva não está presente $\tilde{\lambda}_1 = 1$, com os outros $\tilde{\lambda}$'s sendo zero, recuperamos a representação baseada em emaranhamento do protocolo BB84 no cenário perfeito, Eq. (4.1).

A Eq. (6.1) é uma outra purificação descrevendo o estado de Alice, Bob e Eva após a última acoplar seus *ancillas* com o *qubit* enviado de Alice a Bob. O mesmo argumento que nos levou a escrever a Eq. (4.6) implica $0 \leq \tilde{\lambda}_j \leq 1$, $\sum_j \tilde{\lambda}_j = 1$, e $|\tilde{\epsilon}_j\rangle$, $j = 1, \ldots, 4$, formam

uma base ortonormal.

As purificações (4.6) e (6.1) são conectadas pela seguinte relação

$$|\tilde{\Psi}\rangle_{ABE} = (U_{AB} \otimes U_E)|\Psi\rangle_{ABE}, \tag{6.6}$$

onde

$$U_{AB} = \sum_{j=1}^{2} |\phi_j\rangle_{AB}\langle\phi_j| + |01\rangle_{AB}\langle\phi_3| + |10\rangle_{AB}\langle\phi_4|, \tag{6.7}$$

$$U_E = \sum_{j=1}^{4} |\tilde{\epsilon}_j\rangle_E\langle\epsilon_j| \,. \tag{6.8}$$

Vale mencionar que a transformação unitária conectando as duas purificações são locais em relação as partes AB e E. Já que operação unitária é local com respeito a Eva, nós podemos alternativamente ir de (4.6) para (6.1) identificando $|\tilde{\epsilon}_j\rangle$ com $|\epsilon_j\rangle$, $\tilde{\lambda}_j$ com λ_j, e simplesmente aplicando a seguinte operação unitária,

$$U_{AB} \otimes \mathbb{1}_E, \tag{6.9}$$

onde $\mathbb{1}_E$ é o operador identidade atuando no espaço de Hilbert de Eva. Desde que a operação unitária de Eva é dada por um operador identidade, claramente este não muda os estados descrevendo seu sistema. Além disso, pensando em $|\tilde{\Psi}\rangle_{ABE}$ dado por $U_{AB} \otimes U_E|\Psi\rangle_{ABE}$ ou por $U_{AB} \otimes \mathbb{1}_E|\Psi\rangle_{ABE}$, nós obteremos o mesmo limite inferior para a fração da chave secreta já que devemos calcular a quantidade de Holevo maximizando sobre todas as possíveis estratégias que Eva possa empregar. Sendo assim, e para simplificar notação, escreveremos $|\epsilon_j\rangle$ e λ_j ao invés de $|\tilde{\epsilon}_j\rangle$ e $\tilde{\lambda}_j$.

A purificação (6.1) não é, entretanto, equivalente a (4.6) no seguinte sentido. Conforme mostraremos abaixo, a forma na qual escrevemos a purificação (6.1) nos força a introduzir um outro vínculo entre os λ's que não aparece em (4.6). Isto nos permitirá obter um limite inferior mais preciso (neste caso será exato) para a fração da chave secreta, que culminará no aumento da taxa de erro na qual o protocolo BB84 continuará a operar com segurança.

Vamos apresentar este vínculo extra. Se repetirmos os passos que levaram à Eq. (4.14) usando a Eq. (6.1) ao invés de (4.6) obtemos,

$$p_A(0) = (\lambda_1 + \lambda_2)/2 + \lambda_3, \tag{6.10}$$

$$p_A(1) = (\lambda_1 + \lambda_2)/2 + \lambda_4. \tag{6.11}$$

Independentemente da interferência de Eva, o protocolo BB84 é construído a sempre termos

$$p_A(0) = p_A(1) = \frac{1}{2}, \tag{6.12}$$

já que Alice aleatoriamente escolhe com iguais probabilidades se ela enviará a Bob o bit 0 ou 1. Impondo nas Eqs. (6.10) e (6.11) a condição (6.12), verificamos que

$$\lambda_3 = \lambda_4 = \lambda. \tag{6.13}$$

Usando o vínculo (6.13), um cálculo direto, similar ao feito na Sec. 4.1, nos leva a

$$p_A(0) = p_A(1) = p_B(0) = p_B(1) = \frac{1}{2} \tag{6.14}$$

e

$$p_{AB}(0,0) = p_{AB}(1,1) = \frac{\lambda_1 + \lambda_2}{2}, \tag{6.15}$$

$$p_{AB}(0,1) = p_{AB}(1,0) = \lambda. \tag{6.16}$$

Considerando a base x nós temos

$$p_{AB}(+,-) = p_{AB}(-,+) = \frac{\lambda_2 + \lambda}{2}. \tag{6.17}$$

Das Eqs. (6.14)-(6.16), nós obtemos a informação mútua entre Alice e Bob usando a Eq. (2.6) pode ser reescrita como:

$$I(A:B) = \sum_{a,b} \left\{ -p_B(b) \log \left[p_B(b) \right] + p_{A,B}(a,b) \log \left[\frac{p_{A,B}(a,b)}{p_A(a)} \right] \right\}. \tag{6.18}$$

Assim,

$$I(A:B) = 1 - h(\varepsilon_z), \tag{6.19}$$

onde

$$\varepsilon_z = 2\lambda, \tag{6.20}$$

$$\varepsilon_x = \lambda_2 + \lambda, \tag{6.21}$$

pelas Eqs. (6.16) e (6.17).

Agora calcularemos a quantidade de Holevo, Eq. (2.105), usando a nova purificação, isto é, a Eq. (6.1). Usando a Eq. (6.1) e o vínculo (6.13) obtemos

$$\begin{aligned}\rho^E &= \mathrm{Tr}_{AB}(\rho^{ABE}) \\ &= \sum_{j=1}^{2} \lambda_j |\epsilon_j\rangle_E\langle\epsilon_j| + \lambda(|\epsilon_3\rangle_E\langle\epsilon_3| + |\epsilon_4\rangle_E\langle\epsilon_4|)\end{aligned}$$

e consequentemente

$$S(\rho^E) = -\lambda_1 \log \lambda_1 - \lambda_2 \log \lambda_2 - 2\lambda \log \lambda. \tag{6.22}$$

Usando a Eq. (6.1) ao invés de (4.6), o postulado da medida nos dá

$$\rho_a^E = \frac{1}{p_A(a)} \mathrm{tr}_{AE} \left\{ (|a\rangle_A \langle a| \otimes \mathbb{1}_{BE}) \, |\tilde{\Psi}\rangle_{ABE} \langle\tilde{\Psi}| \, (|a\rangle_A \langle a| \otimes \mathbb{1}_{BE}) \right\}, \tag{6.23}$$

onde

$$\rho_0^E = \lambda_1 |\epsilon_1\rangle_E\langle\epsilon_1| + \lambda_2 |\epsilon_2\rangle_E\langle\epsilon_2| + 2\lambda |\epsilon_3\rangle_E\langle\epsilon_3| + \sqrt{\lambda_1\lambda_2} \, (|\epsilon_1\rangle_E\langle\epsilon_2| + h.c.), \tag{6.24}$$

$$\rho_1^E = \lambda_1 |\epsilon_1\rangle_E\langle\epsilon_1| + \lambda_2 |\epsilon_2\rangle_E\langle\epsilon_2| + 2\lambda |\epsilon_4\rangle_E\langle\epsilon_4| - \sqrt{\lambda_1\lambda_2} \, (|\epsilon_1\rangle_E\langle\epsilon_2| + h.c.). \tag{6.25}$$

Os autovalores de ambos operadores, ρ_0^E e ρ_1^E, são $0, 0, \lambda_1 + \lambda_2$, e 2λ, levando à seguinte entropia de von Neumann,

$$S(\rho_0^E) = S(\rho_1^E) = h(\varepsilon_z), \tag{6.26}$$

após usarmos a Eq. (6.20).

A quantidade de Holevo obtida quando inserimos as Eqs. (6.14), (6.22) e (6.26) em (2.105) é

$$\chi(A:E) = -\lambda_1 \log \lambda_1 - \lambda_2 \log \lambda_2 - 2\lambda \log \lambda - h(\varepsilon_z). \tag{6.27}$$

Finalmente, a fração da chave secreta, Eq. (2.122), dada pela diferença da Eq. (6.19) com (6.27) resulta em

$$r = 1 + \lambda_1 \log \lambda_1 + \lambda_2 \log \lambda_2 + 2\lambda \log \lambda. \tag{6.28}$$

Vale mencionar que não será necessário minimizar r sobre todas as estratégias que Eva possa empregar pois todas as quantidades já estão determinadas pelos dados experimentais, i.e., tudo que precisamos para calcular r é ε_x and ε_z. Isto é devido ao vínculo extra,

Eq. (6.13), o qual nos permitiu determinar unicamente os λ's como função das taxas de erros ε_x e ε_z. Usando as Eqs. (6.20), (6.21), e a condição de normalização dos λ's, i.e., $\lambda_1 + \lambda_2 + 2\lambda = 1$, temos

$$\lambda_1 = 1 - \varepsilon_x - \varepsilon_z/2, \tag{6.29}$$

$$\lambda_2 = \varepsilon_x - \varepsilon_z/2, \tag{6.30}$$

$$\lambda = \varepsilon_z/2. \tag{6.31}$$

A fração da chave secreta é obtida inserindo as Eqs. (6.29)-(6.31) na (6.28), a qual após algumas simples manipulações matemática pode ser reescrita como se segue,

$$r = \varepsilon_z \log \varepsilon_z + (1 - \varepsilon_x - \varepsilon_z/2) \log(2 - 2\varepsilon_x - \varepsilon_z) + (\varepsilon_x - \varepsilon_z/2) \log(2\varepsilon_x - \varepsilon_z). \tag{6.32}$$

Assumindo que lidamos com um canal depolarizante ($\varepsilon_x = \varepsilon_z = \varepsilon$), como feito anteriormente, a fração da chave secreta torna-se

$$r = (3\varepsilon/2) \log \varepsilon + (1 - 3\varepsilon/2) \log(2 - 3\varepsilon), \tag{6.33}$$

mesma equação para o BB84 seis-estados com erros simétricos, Eq. (5.22). Procurando por um máximo ε de tal forma que ainda temos $r > 0$ encontramos

$$\varepsilon \lesssim 12.61\%. \tag{6.34}$$

A taxa de erro acima é o limiar obtido trabalhando com o protocolo BB84 seis-estados apresentado no início deste capítulo e presente nas Refs. [8, 42, 48–50], onde, além da base z e da base x, a base y também é usada na codificação da chave criptográfica. Isto significa que tanto o protocolo BB84 original quanto o protocolo BB84 seis-estados são seguros perante o mesmo nível de ruído. Vale a pena relembrar que só foi possível atingir esse limiar para o protocolo BB84 original devido a podermos representar os estados de Alice e Bob em outras bases ortonormais na decomposição de Schmidt que descreve o estado de Alice, Bob e Eva.

Nós também realizamos a análise de segurança para o protocolo BB84 utilizando a decomposição de Schmidt (6.1) sem impor o vínculo (6.13). Neste caso somos obrigados a realizar a minimização de r sobre todas as possíveis estratégias de Eva porque ainda temos um λ livre na expressão para r (veja o apêndice E.1). Ao final do processo de minimização

encontramos que o vínculo (6.13) emerge naturalmente como o cenário mais vantajoso para Eva. Uma vez que o vínculo (6.13) é relacionado ao fato de $p_A(0) = p_A(1) = 1/2$, é possível que um protocolo de envio assimétrico, $p_A(0) \neq p_A(1)$, possa levar ao aumento da tolerância do nível de ruído abaixo do qual o protocolo operará seguramente.

6.2 Considerações finais sobre o protocolo BB84

Na seção anterior vimos que ao utilizarmos uma nova decomposição de Schmidt conseguimos aumentar o limiar de segurança do protocolo BB84 para o mesmo nível do protocolo BB84 seis-estados. Note que esse resultado foi obtido considerando erros simétricos ($\varepsilon_x = \varepsilon_y = \varepsilon_x$). Neste regime, mostramos que o uso de uma base adicional não aumentará a fração da chave secreta r. Esta conclusão pode ser melhor visualizada na Fig. 6.1, onde temos uma comparação dos três resultados da fração da chave secreta do BB84. Isto é, a taxa de segurança dada pela Eq. (4.42) para a solução original do BB84, pela Eq. (5.22) do BB84 seis-estados e pela Eq. (6.33) obtida pela alteração da decomposição de Schmidt do protocolo BB84 original.

Ainda na Fig. 6.1, vemos claramente que a fração da chave secreta do BB84 seis-estados é exatamente igual a do BB84 com a nova decomposição de Schimdt. Com isso podemos dizer que adicionar uma nova base no protocolo BB84 não traz benefício algum em relação a fração da chave secreta. Na verdade, adicionar uma nova base pode ser considerado até desvantajoso pois diminui o tamanho da chave crua R após o peneiramento (*sifting*). Com duas bases na média $R = N/2$ bits e com três bases (protocolo BB84 seis-estados) $R = N/3$ bits.

No entanto, nem sempre temos que as taxas de erros são simétricas. A Fig. 6.2 apresenta a comparação entre a fração da chave secreta para o BB84 original, Eq. (4.41), e a do BB84 com a nova decomposição de Schmidt, Eq. (6.32), em função de ε_x e ε_z. Como era esperado, vemos que o cálculo original de r limita inferiormente o valor de r quando usamos a nova decomposição de Schmidt.

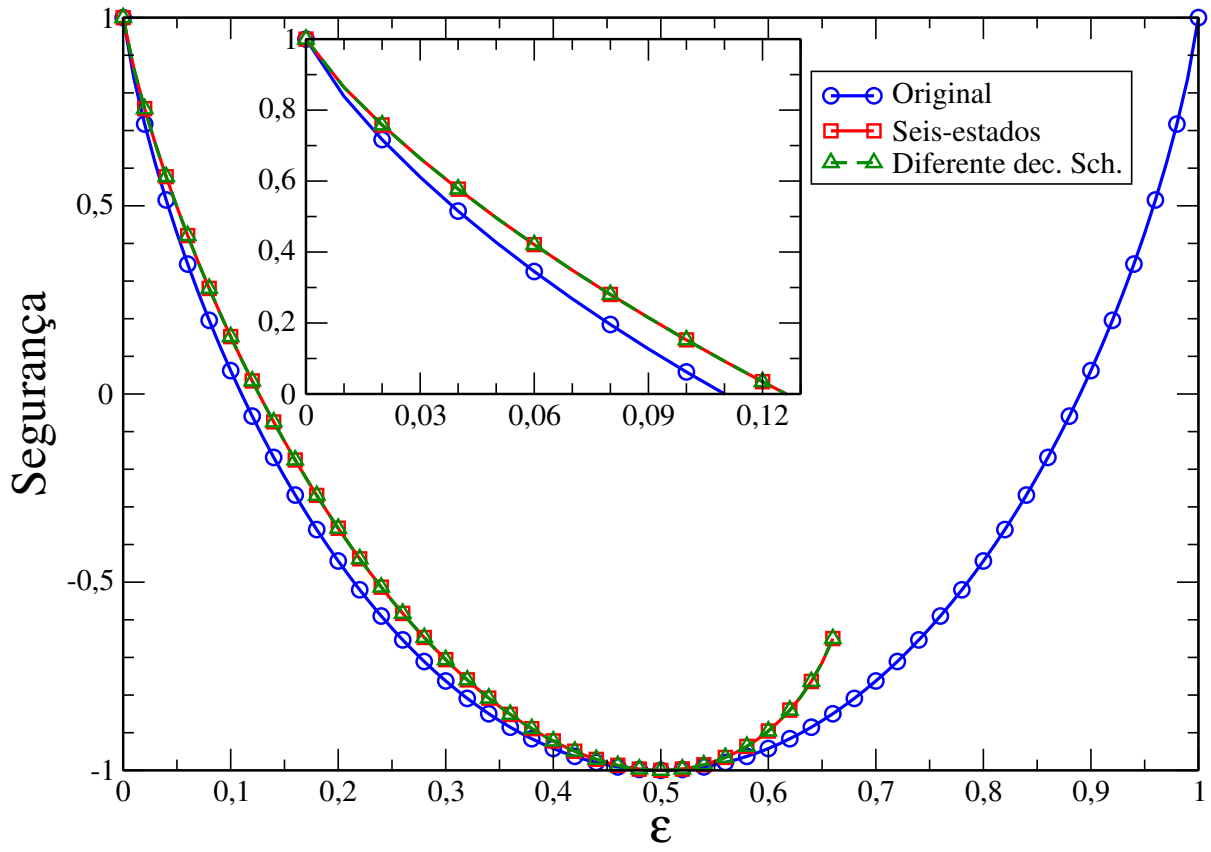

Figura 6.1: Comparação entre a segurança do protocolo BB84 original (4.42), curva azul com círculos, com a do protocolo BB84 seis-estados (5.22), curva vermelha com quadrados, e a fração da chave secreta do protocolo BB84 usando uma diferente decomposição de Schmidt (6.33), curva verde com triângulos. Para plotar os gráficos consideramos as taxas de erros simétricas, $\varepsilon_x = \varepsilon_y = \varepsilon_z = \varepsilon$. Aqui visualizamos que utilizando uma decomposição de Schmidt diferente obtemos exatamente a mesma taxa de segurança do BB84 seis-estados. Este resultado é superior ao cálculo original do BB84. No detalhe do gráfico visualizamos a faixa em que o protocolo é considerado seguro, ou seja, quando $r > 0$.

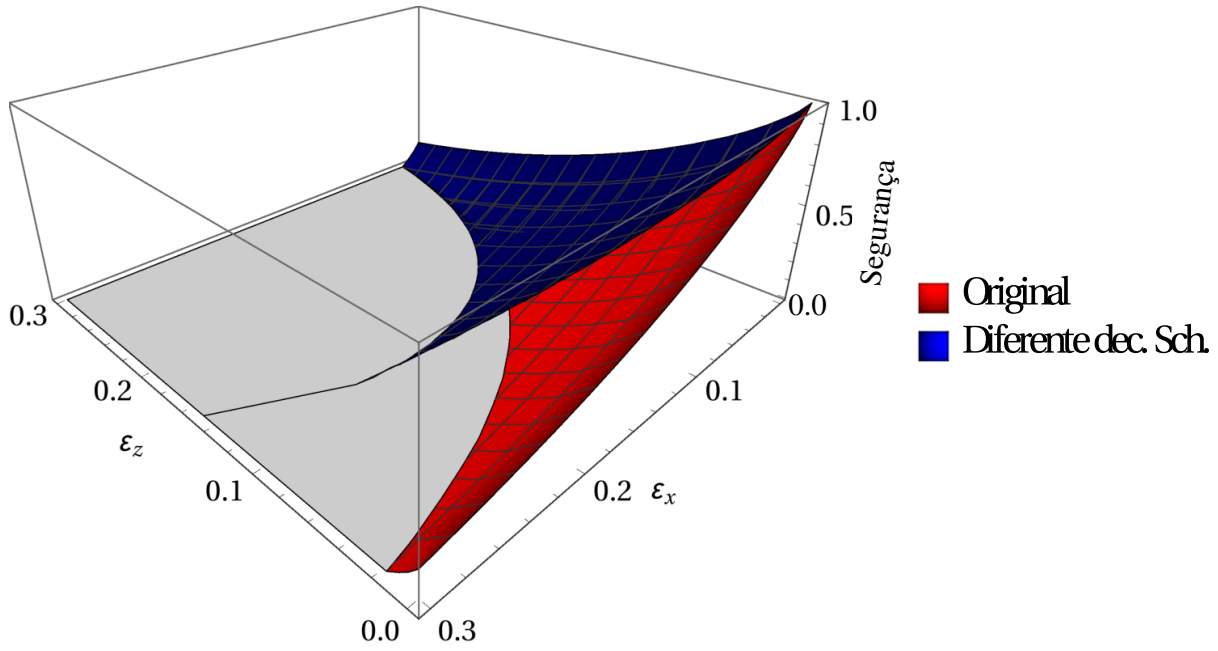

Figura 6.2: Gráfico comparativo entre a fração da chave secreta r do BB84 original (4.41) obtido através da decomposição de Schmidt (4.6), superfície vermelha, com a Eq. (6.32) obtida pela nova decomposição de Schmidt, Eq. (6.1), superfície azul. Nele podemos ver que ao utilizarmos uma decomposição de Schmidt diferente somos capazes de obter uma taxa de segurança maior.

Capítulo 7

A segurança do protocolo GR10

Este é o principal capítulo desta Tese [53]. Nele nós mostraremos em detalhes como foi feita a análise de segurança do protocolo GR10. Inicialmente veremos como obter a fração da chave secreta para o protocolo GR10 em sua versão original. Depois apresentaremos modificações na construção do GR10.

Estas modificações consistem na mudança do *ensemble* utilizado para se gerar a chave bruta. Como visto na Sec. 3.2, não são todos os *qubits* enviados que compõem a chave bruta compartilhada entre Alice e Bob na construção original do protocolo GR10. Somente os casos em que Alice obtém em sua medida generalizada de Bell os estados $|\phi_2\rangle$ ou $|\phi_3\rangle$, e com o mesmo emaranhamento do canal de Bob, são utilizados. A outra sugestão de alteração é considerar mais estados para codificar os bits 0 e 1. Ou seja, além dos estados $|+\rangle$ e $|-\rangle$, consideramos os estados da base y, $|y_0\rangle$ e $|y_1\rangle$. Basicamente isto consiste na junção do protocolo BB84 com o GR10.

7.1 Análise de segurança do protocolo GR10

A forma mais simples de compreender qualitativamente a segurança do protocolo GR10 [18] é comparar sua execução com a do protocolo BB84 [4]. Para isto, no protocolo GR10 Alice e Bob descartam todos os casos em que as medidas de Bell de Alice, Eqs. (3.2)-(3.5), resultaram em $|\Phi_1^n\rangle$ e $|\Phi_4^n\rangle$. Das duas possibilidades restantes, quatro casos diferentes emergem. Alice pode ter teletransportado o estado $|+\rangle$ e obtido $|\Phi_2^n\rangle$ para sua medida de Bell ou teletransportou $|+\rangle$ e obtido $|\Phi_3^n\rangle$. Similarmente, ela pode ter escolhido teletransportar o estado $|-\rangle$ e obteve $|\Phi_2^n\rangle$ ou $|\Phi_3^n\rangle$ após implementar a medida generalizada de Bell. O estado quântico que descreve o *qubit* de Bob é dado pelas Eqs. (3.11) e (3.12) (apresentadas

novamente abaixo) provenientes do protocolo de teletransporte probabilístico, Sec. 3.2:

$$|\phi_2\rangle_B = \frac{k\alpha|0\rangle_B + n\beta|1\rangle_B}{\sqrt{k^2|\alpha|^2 + n^2|\beta|^2}},$$
$$|\phi_3\rangle_B = \frac{n\alpha|0\rangle_B + k\beta|1\rangle_B}{\sqrt{n^2|\alpha|^2 + k^2|\beta|^2}}.$$

Quando Alice teletransportou o estado $|+\rangle$, isto é, $\alpha = 1/\sqrt{2}$ e $\beta = 1/\sqrt{2}$ nas Eqs. (3.11) e (3.12), e obteve $|\Phi_2^k\rangle$ ou $|\Phi_3^k\rangle$, os estados possíveis de Bob são, respectivamente,

$$|\widetilde{0}\rangle_B = \frac{k\,|0\rangle_B + n\,|1\rangle_B}{\sqrt{n^2+k^2}} = \frac{(k+n)\,|+\rangle_B + (k-n)\,|-\rangle_B}{\sqrt{2(n^2+k^2)}}, \tag{7.1}$$
$$|\widetilde{+}\rangle_B = \frac{n\,|0\rangle_B + k\,|1\rangle_B}{\sqrt{n^2+k^2}} = \frac{(k+n)\,|+\rangle_B + (n-k)\,|-\rangle_B}{\sqrt{2(n^2+k^2)}}. \tag{7.2}$$

Analogamente, se ela teleportou $|-\rangle$ ($\alpha = 1/\sqrt{2}$ e $\beta = -1/\sqrt{2}$), ele por sua vez teria em mãos respectivamente

$$|\widetilde{-}\rangle_B = \frac{k\,|0\rangle_B - n\,|1\rangle_B}{\sqrt{n^2+k^2}} = \frac{(k-n)\,|+\rangle_B + (k+n)\,|-\rangle_B}{\sqrt{2(n^2+k^2)}}, \tag{7.3}$$
$$|\widetilde{1}\rangle_B = \frac{n\,|0\rangle_B - k\,|1\rangle_B}{\sqrt{n^2+k^2}} = \frac{(n-k)\,|+\rangle_B + (k+n)\,|-\rangle_B}{\sqrt{2(n^2+k^2)}}, \tag{7.4}$$

para os resultados $|\Phi_2^k\rangle$ ou $|\Phi_3^k\rangle$ da medida generalizada de Bell feita por Alice. Não é difícil de se ver que o conjunto $\{|\widetilde{0}\rangle_B, |\widetilde{1}\rangle_B\}$ define uma base ortonormal, assim como o conjunto $\{|\widetilde{+}\rangle_B, |\widetilde{-}\rangle_B\}$. Vamos chamá-los respectivamente por base $\tilde{z}$ e base $\tilde{x}$.

A analogia com o protocolo BB84 está agora evidente. Sempre que Alice teletransporta o estado $|+\rangle$, Bob aleatoriamente obtém o estado $|\widetilde{0}\rangle$ ou $|\widetilde{+}\rangle$, dependendo da medida de Bell que ela obteve. Se a condição de *mathcing* é satisfeita ($n = k$), nós temos que $|\widetilde{0}\rangle = |\widetilde{+}\rangle = |+\rangle$ e Bob supõe corretamente que o bit possui o valor 0 após medir seu *qubit* na base x. Similarmente, se Alice teletransporta o estado $|-\rangle$, o *qubit* de Bob será $|\widetilde{1}\rangle$ ou $|\widetilde{-}\rangle$. Quando $n = k$ nós temos $|\widetilde{1}\rangle = |\widetilde{-}\rangle = |-\rangle$ e Bob associará corretamente o bit 1 após finalizar sua medida na base x.

Por outro lado, se a condição de *matching* não é satisfeita ($n \neq k$), a probabilidade de Bob obter um resultado diferente do envido por Alice é não nulo, e é dado por $(k-n)^2/(2(n^2+k^2))$. Além disso, o fato de que $k \neq n$ quebra a degenerescência dos possíveis

estados de Bob após o teletransporte, isto é, $|\widetilde{0}\rangle \neq |\widetilde{+}\rangle$ e $|\widetilde{1}\rangle \neq |\widetilde{-}\rangle$. Isto induz a uma codificação em estados não ortogonais para os bits enviados por Alice, exatamente como ocorre no BB84. De fato, neste cenário o bit de valor 0 é ora associado ao estado $|\widetilde{0}\rangle$ e ora ao estado $|\widetilde{+}\rangle$, onde $\langle\widetilde{0}|\widetilde{+}\rangle = 2nk/(n^2+k^2)$, e o bit de valor 1 é identificado por $|\widetilde{1}\rangle$ ou $|\widetilde{-}\rangle$, onde novamente temos $\langle\widetilde{1}|\widetilde{-}\rangle = \langle\widetilde{0}|\widetilde{+}\rangle$.

Ou seja, apesar de no protocolo GR10 utilizarmos somente um conjunto de estados ortonormais para codificar a chave, o fato da sua operação ser baseada no teletransporte probabilístico leva a uma codificação não-ortogonal efetiva para todo $n \neq k$. E, uma vez que Eva não sabe com certeza valor dos k e n em sua espionagem *antes* de Alice e Bob finalizarem todas suas medidas, ela necessariamente será pega manipulando a execução do protocolo GR10.

Passemos, agora, à analise quantitativa da segurança do protocolo GR10. De acordo com a discussão do parágrafo anterior, sempre que a condição de *matching* é satisfeita ($k = n$) Bob obtém uma réplica exata do estado teletransportado. Desta forma, a representação baseada em emaranhamento dos casos pós-selecionados de sucesso do protocolo GR10 é:

$$|\tilde{\Phi}_1\rangle = \frac{1}{\sqrt{2}}(|{+}{+}\rangle + |{-}{-}\rangle). \tag{7.5}$$

A Eq. (7.5) é o estado de Bell (4.1) escrito na base x.

Após Eva interferir na transmissão, uma possível purificação representando o estado de Alice, Bob e Eva é

$$|\Psi\rangle_{ABE} = \sum_{j=1}^{4} \sqrt{\lambda_j}|\tilde{\Phi}_j\rangle_{AB}|\epsilon_j\rangle_E, \tag{7.6}$$

onde $|\tilde{\Phi}_1\rangle$ foi definido acima e

$$|\tilde{\Phi}_2\rangle = \frac{1}{\sqrt{2}}(|+-\rangle + |-+\rangle), \tag{7.7}$$

$$|\tilde{\Phi}_3\rangle = |01\rangle\,, \tag{7.8}$$

$$|\tilde{\Phi}_4\rangle = |10\rangle\,. \tag{7.9}$$

A Eq. (7.7) é o estado de Bell usual (4.2) reescrito na base x.

A representação baseada em emaranhamento (7.6) é a mesma que foi aplicada quando nós revisitamos a análise de segurança do protocolo BB84 usando uma purificação diferente, Eq. (6.1). Aqui, contudo, nós trabalhamos apenas com a base x, enquanto na Sec. 6.1 tinhamos as bases x e z à disposição de Alice e Bob para a preparação e medida dos *qubits*.

Devido a não termos conhecimento agora sobre ε_z, um dos λ's na expressão da taxa de segurança r ficará indeterminado. Isto nos levará a maximizar a informação acessível de Eva sobre todas as possíveis estratégias que ela possa empregar. Quando compararmos com os cálculos da Sec. 6.1, isto levará a um valor inferior para a taxa de erro ε_x abaixo da qual temos uma fração da chave secreta positiva e portanto segura.

O estado teletransportado por Alice é $|+\rangle$ ou $|-\rangle$. Como eles são equiprováveis, o *ensemble* de *qubits* de Alice é dado por $(|+\rangle\langle+| + |-\rangle\langle-|)/2$ ou, equivalentemente, por $(|0\rangle\langle 0| + |1\rangle\langle 1|)/2$. Novamente, como na Sec. 6.1, Eva não tem acesso aos *qubits* de Alice. Portanto, nós devemos ter com ou sem Eva

$$p_A(0) = p_A(1) = 1/2. \tag{7.10}$$

Calculando $p_A(a) = \mathrm{tr}\left\{(|a\rangle_A\langle a| \otimes \mathbb{1}_{BE})\,|\Psi\rangle_{ABE}\langle\Psi|\right\}$ com $|\Psi\rangle_{ABE}$ dado pela Eq. (7.6) temos,

$$p_A(0) = \frac{\lambda_1 + \lambda_2}{2} + \lambda_3, \tag{7.11}$$

$$p_A(1) = \frac{\lambda_1 + \lambda_2}{2} + \lambda_4, \tag{7.12}$$

onde a igualdade entre as probabilidades $p_A(0)$ e $p_A(1)$ só é satisfeita se tivermos o vínculo (6.13),

$$\lambda_3 = \lambda_4 = \lambda. \tag{7.13}$$

Note que $p_A(+) = p_A(-) = 1/2$ já é automaticamente satisfeito pela purificação (7.6).

Procedendo analogamente ao que fizemos na Sec. 4.1, temos que a taxa de erro é dada por

$$\varepsilon_x = p_{AB}(+,-) + p_{AB}(-,+), \tag{7.14}$$

onde

$$p_{AB}(a,b) = \mathrm{tr}\left\{(|a\rangle_A|a\rangle \otimes |b\rangle_B|b\rangle \otimes \mathbb{1}_E)\rho^{ABE}\right\}. \tag{7.15}$$

Assim, para $\rho^{ABE} = |\Psi\rangle_{ABE}\langle\Psi|$, onde $|\Psi\rangle_{ABE}$ é dado pela Eq. (7.6), temos

$$p_{AB}(+,+) = p_{AB}(-,-) = \frac{1 - \lambda_2 - \lambda}{2}, \tag{7.16}$$

$$p_{AB}(+,-) = p_{AB}(-,+) = \frac{\lambda_2 + \lambda}{2}, \tag{7.17}$$

já aplicado o vínculo (6.13). Com isso, a taxa de erro, Eq. (7.14), torna-se

$$\varepsilon_x = \lambda_2 + \lambda = \frac{1}{2}(1 + \lambda_2 - \lambda_1), \tag{7.18}$$

onde usamos a condição de normalização

$$\lambda_1 + \lambda_2 + 2\lambda = 1 \tag{7.19}$$

para obter a igualdade anterior.

Calculando $p_B(b) = \mathrm{tr}\left\{(|b\rangle_b\langle b| \otimes \mathbb{1}_{AE})\,|\Psi\rangle_{ABE}\langle\Psi|\right\}$, obtemos $p_B(+) = p_B(-) = 1/2$. Consequentemente, a entropia de Shannon $H(B) = -\sum_b p_B(b)\log[p_B(b)]$, Eq. (2.1), vale

$$H(B) = 1. \tag{7.20}$$

Para calcular a entropia condicional clássica, Eq. (2.4),

$$H(B|A) = -\sum_{a,b} p_A(a) p_{B|A}(b|a) \log\left[p_{B|A}(b|a)\right],$$

vamos usar novamente o resultado $p_{B|A}(b|a) = p_{AB}(a,b)/p_A(a)$ da teoria das probabilidades. Usando que $p_A(+) = p_A(-) = 1/2$, juntamente com as Eqs. (7.16) e (7.17), temos

$$p_{B|A}(+|+) = p_{B|A}(-|-) = 1 - \lambda_2 - \lambda, \tag{7.21}$$

$$p_{B|A}(+|-) = p_{B|A}(-|+) = \lambda_2 + \lambda. \tag{7.22}$$

Assim, pela Eq. (7.18) podemos escrever a entropia condicional como

$$H(B|A) = h(\lambda_2 + \lambda) = h(\varepsilon_x), \tag{7.23}$$

com $h(x) = -x\log(x) - (1-x)\log(1-x)$ sendo a entropia binária (2.2).

Juntando as Eqs. (7.20) e (7.23) nós obtemos a seguinte expressão para a informação mútua entre Alice e Bob,

$$I(A:B) = 1 - h(\varepsilon_x). \tag{7.24}$$

Agora, tomando o traço parcial sobre AB de $|\Psi\rangle_{ABE}\langle\Psi|$, Eq. (7.6), resulta

$$\rho^E = \sum_i \lambda_i\,|\epsilon_i\rangle_E\langle\epsilon_i|\,. \tag{7.25}$$

Com isso, usando a definição da entropia de von Neumann, Eq. (2.24), a entropia quântica do sistema E é

$$S(\rho^E) = -\lambda_1 \log \lambda_1 - \lambda_2 \log \lambda_2 - 2\lambda \log \lambda. \tag{7.26}$$

A partir do postulado da medida, Eq. (2.103), que também pode ser reescrito da seguinte forma,

$$\rho_a^E = \frac{1}{p_A(a)} \mathrm{tr}_{AB} \left\{ \left(|a\rangle_A \langle a| \otimes \mathbb{1}_{BE} \right) \rho^{ABE} \left(|a\rangle_A \langle a| \otimes \mathbb{1}_{BE} \right) \right\},$$

e sabendo que $p_A(+) = p_A(-) = 1/2$ e que $\rho^{ABE} = |\Psi\rangle_{ABE}\langle\Psi|$, Eq. (7.6), obtemos

$$\begin{aligned} \rho_+^E &= \sum_{j=1}^{4} \lambda_j |\epsilon_j\rangle_E \langle\epsilon_j| \\ &\quad + \sqrt{\lambda_1\lambda_3/2} \left(|\epsilon_1\rangle_E \langle\epsilon_3| + h.c. \right) + \sqrt{\lambda_1\lambda_4/2} \left(|\epsilon_1\rangle_E \langle\epsilon_4| + h.c. \right) \\ &\quad - \sqrt{\lambda_2\lambda_3/2} \left(|\epsilon_2\rangle_E \langle\epsilon_3| + h.c. \right) + \sqrt{\lambda_2\lambda_4/2} \left(|\epsilon_2\rangle_E \langle\epsilon_4| + h.c. \right), \end{aligned} \tag{7.27}$$

$$\begin{aligned} \rho_-^E &= \sum_{j=1}^{4} \lambda_j |\epsilon_j\rangle_E \langle\epsilon_j| \\ &\quad - \sqrt{\lambda_1\lambda_3/2} \left(|\epsilon_1\rangle_E \langle\epsilon_3| + h.c. \right) - \sqrt{\lambda_1\lambda_4/2} \left(|\epsilon_1\rangle_E \langle\epsilon_4| + h.c. \right) \\ &\quad + \sqrt{\lambda_2\lambda_3/2} \left(|\epsilon_2\rangle_E \langle\epsilon_3| + h.c. \right) - \sqrt{\lambda_2\lambda_4/2} \left(|\epsilon_2\rangle_E \langle\epsilon_4| + h.c. \right). \end{aligned} \tag{7.28}$$

Os dois autovalores não-nulos, tanto de ρ_+^E quanto de ρ_-^E, são $(1 + \lambda_1 - \lambda_2)/2 = 1 - \varepsilon_x$ e $(1 + \lambda_2 - \lambda_1)/2 = \varepsilon_x$, onde usamos que $\lambda_3 = \lambda_4 = \lambda$, Eq. (6.13), e a Eq. (7.18) para reescrevê-los como apresentados. Assim, para os operadores acima, aplicando a definição da entropia quântica, $S(\rho) = -\mathrm{tr}\{\rho \log \rho\}$, encontramos

$$S(\rho_+^E) = S(\rho_-^E) = h(\varepsilon_x), \tag{7.29}$$

sendo h a entropia binária (2.2). Dessa forma, com o auxílio da Eq. (7.26) escrevemos a quantidade de Holevo como se segue,

$$\chi(A : \rho^E) = -\lambda_1 \log \lambda_1 - \lambda_2 \log \lambda_2 - 2\lambda \log \lambda - h(\varepsilon_x). \tag{7.30}$$

Finalmente, a fração da chave secreta (2.122) torna-se

$$\begin{aligned} r &= 1 + \min_{\text{Eve}} \{\lambda_1 \log \lambda_1 + \lambda_2 \log \lambda_2 + 2\lambda \log \lambda\} \\ &= 1 + \min_{\lambda} \{(1 - \varepsilon_x - \lambda) \log(1 - \varepsilon_x - \lambda) + (\varepsilon_x - \lambda) \log(\varepsilon_x - \lambda) + 2\lambda \log \lambda\} . \end{aligned} \tag{7.31}$$

Para obter a última igualdade usamos as Eqs. (7.18) e (7.19) expressando λ_1 e λ_2 em função de ε_x e λ,

$$\lambda_1 = 1 - \varepsilon_x - \lambda, \tag{7.32}$$

$$\lambda_2 = \varepsilon_x - \lambda. \tag{7.33}$$

Resolvendo para λ a condição de minimização,

$$\frac{dr}{d\lambda} = 0, \tag{7.34}$$

obtemos

$$\lambda_{min} = \varepsilon_x(1 - \varepsilon_x), \tag{7.35}$$

onde para esse valor de λ_{min} temos

$$\frac{d^2 r(\lambda_{min})}{d\lambda^2} > 0, \tag{7.36}$$

provando que realmente encontramos um mínimo para $r(\lambda)$.

Inserindo a Eq. (7.35) na (7.31) obtemos o seguinte limite inferior de segurança para a fração da chave secreta do protocolo GR10,

$$r = 1 - 2h(\varepsilon_x). \tag{7.37}$$

Procurando a raiz da Eq. (7.37) obtemos que $r > 0$ se

$$\varepsilon_x \lesssim 11\%. \tag{7.38}$$

Em outras palavras, para taxas de erros menores que 11% o protocolo GR10 opera seguramente. Na Fig. 7.1 mostramos a Eq. (7.37) como função de ε_x.

Assim como fizemos para o protocolo BB84 revisitado, nós estimamos a segurança do protocolo GR10 sem a imposição do vínculo (6.13). Novamente, nós obtivemos a Eq. (6.13)

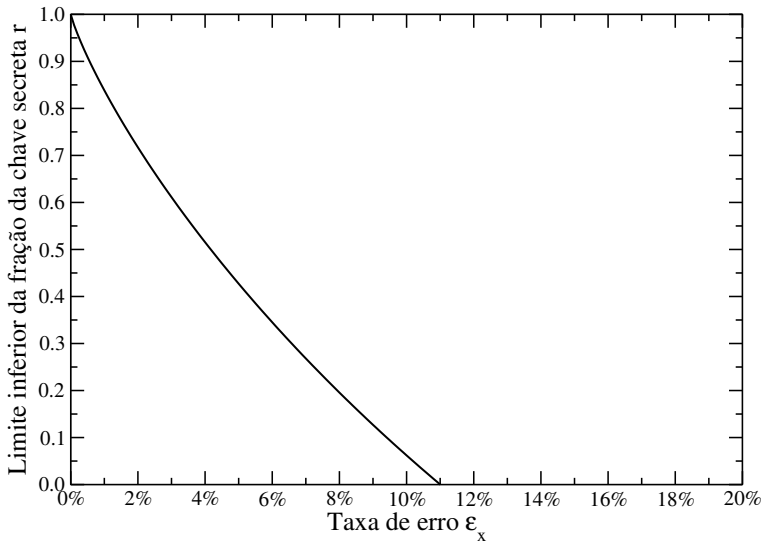

Figura 7.1: Limite inferior da fração da chave secreta r em função do ε_x para o protocolo GR10, Eq. (7.37). A outra quantidade ε_x é a taxa de erro das medidas feitas por Bob na base x. Aqui, e em todos os gráficos, todas as grandezas são adimensionais.

ao fim do processo de minimização como cenário mais promissor para Eva. O cálculo para a segurança sem o uso do vínculo pode ser visto no apêndice E.

Note que, a purificação (7.6) é crucial para obter um limite inferior da fração da chave secreta r mais próximo do valor exato. Se tivéssemos usado a purificação (4.6), como comumente feita na análise de segurança do protocolo BB84, obteríamos um limite inferior muito baixo, um que levaria a $r < 0$ para qualquer valor de $\varepsilon_x > 0$.

Finalmente, é importante notar que as análises de segurança apresentadas aqui e nas próximas seções podem ser diretamente estendidas para ataques coerentes, implicando em uma segurança incondicional do protocolo GR10 e sua versão modificada dada na Sec. 7.2. Esta afirmação decorre do trabalho de Renner [46] e Renner e Cirac [47], que generalizam os resultados das Refs. [44, 45]. O resultado chave da Ref. [46] foi provar que no limite assintótico, segurança contra ataques coletivos é essencialmente equivalente à segurança contra ataques coerentes. Isto é, se o protocolo é seguro no nível de ataques coletivos temos que ele também possui segurança para ataques coerentes. E o limiar da taxa de erro da qual temos segurança é o mesmo do resultado obtido para ataques coletivos.

7.2 Modificações no protocolo GR10

Nós, agora, modificaremos a operação do protocolo GR10 original no seguinte sentido. Originalmente, pela Ref. [18], todos os casos em que as medidas de Bell de Alice davam $|\Phi_1^k\rangle$ e $|\Phi_4^k\rangle$ eram descartados, bem como os casos em que não haviam a condição de *matching* ($k \neq n$). Agora, nós consideraremos todos os casos como válidos. Neste cenário, aumentamos o tamanho da chave crua R ao custo de reduzir o valor da fração da chave secreta r.

O tamanho da chave secreta $K = rR$ será maior em uma ou em outra forma de implementar o protocolo GR10 conforme veremos. K dependerá do valor da taxa de erro e dos valores de n_1 e n_2 escolhidos em sua operação.

Quando consideramos todos os possíveis resultados da medida de Alice, estão incluídos, como dissemos, tanto os casos nos quais $n = m$ e também os casos em que a condição de *matching* não é satisfeita. Dessa forma, Bob inevitavelmente falhará algumas vezes na identificação correta do valor do bit teleportado por Alice, mesmo no caso sem ruído. Portanto, a representação baseada em emaranhamento do protocolo GR10 modificado herdará essa propriedade e é descrita por

$$\begin{aligned} |\xi_1\rangle \;=\; & \sqrt{p_{AB}(+,+)}|++\rangle + \sqrt{p_{AB}(-,-)}|--\rangle \\ & + \sqrt{p_{AB}(+,-)}|+-\rangle + \sqrt{p_{AB}(-,+)}|-+\rangle. \end{aligned} \tag{7.39}$$

Aqui, $p_{AB}(+,+) + p_{AB}(-,-)$ é a probabilidade de Alice e Bob obterem uma perfeita correlação entre os valores dos seus bits e $p_{AB}(+,-) + p_{AB}(-,+)$ é a probabilidade deles diferirem sobre esses valores.

7.2.1 Calculando os coeficientes da representação baseada em emaranhamento

Para calcular os coeficientes da Eq. (7.39), primeiramente vamos recapitular o funcionamento do protocolo GR10. O protocolo GR10, descrito na Sec. 3.2, pode ser posto matematicamente da seguinte forma.

O estado inicial conjunto de Alice e Bob quando ela deseja teleportar o estado $|+\rangle$ e

após Bob ter enviado um *qubit* do canal quântico $|\Phi_1^n\rangle$, é

$$\varrho_+^{AB} = |+\rangle_A\langle+| \otimes |\Phi_1^n\rangle_{AB}\langle\Phi_1^n|\,, \tag{7.40}$$

e, se Alice teleportar o estado $|-\rangle$, o estado conjunto será

$$\varrho_-^{AB} = |-\rangle_A\langle-| \otimes |\Phi_1^n\rangle_{AB}\langle\Phi_1^n|\,. \tag{7.41}$$

Note que os estados dados pelas Eqs. (7.40) e (7.41) ainda não sofreram nenhuma operação quântica (medida ou transformação unitária). Podemos pensá-los como sendo os possíveis estados iniciais para cada rodada de execução do protocolo (transmissão de um bit de Alice para Bob) .

Alice, agora, realiza uma medida projetiva nos dois primeiros *qubits* do operador (7.40) ou (7.41). Dependendo de qual estado de Bell generalizado Alice obtém na sua medida, $|\Phi_1^k\rangle$, $|\Phi_2^k\rangle$, $|\Phi_3^k\rangle$ ou $|\Phi_4^k\rangle$, Bob aplica uma transformação unitária em seu *qubit*. Se Alice obteve $|\Phi_1^k\rangle$, Bob não faz nada; se obteve $|\Phi_2^k\rangle$ Bob aplica σ_z; se obteve $|\Phi_3^k\rangle$ Bob aplica σ_x; e, por fim, se Alice obteve $|\Phi_4^k\rangle$ Bob aplica $\sigma_z\sigma_x$. Sendo assim, as probabilidades condicionais de Bob, dado que Alice obteve um estado de Bell já com as transformações necessárias aplicadas são

$$\begin{aligned}
p_{B|A}(b|\Phi_1^k a) &= \mathrm{tr}\left\{\varrho_a^{AB}\left(|\Phi_1^k\rangle_A\langle\Phi_1^k| \otimes |b\rangle_B\langle b|\right)\right\},\\
p_{B|A}(b|\Phi_2^k a) &= \mathrm{tr}\left\{(\mathbb{1}_A \otimes \sigma_{zB})\,\varrho_a^{AB}\,(\mathbb{1}_A \otimes \sigma_{zB})\left(|\Phi_2^k\rangle_A\langle\Phi_2^k| \otimes |b\rangle_B\langle b|\right)\right\},\\
p_{B|A}(b|\Phi_3^k a) &= \mathrm{tr}\left\{(\mathbb{1}_A \otimes \sigma_{xB})\,\varrho_a^{AB}\,(\mathbb{1}_A \otimes \sigma_{xB})\left(|\Phi_3^k\rangle_A\langle\Phi_3^k| \otimes |b\rangle_B\langle b|\right)\right\},\\
p_{B|A}(b|\Phi_4^k a) &= \mathrm{tr}\left\{[\mathbb{1}_A \otimes (\sigma_z\sigma_x)_B]\,\varrho_a^{AB}\,[\mathbb{1}_A \otimes (\sigma_x\sigma_z)_B]\left(|\Phi_4^k\rangle_A\langle\Phi_4^k| \otimes |b\rangle_B\langle b|\right)\right\}.
\end{aligned} \tag{7.42}$$

Aqui $p_{B|A}(b|\Phi_j^k a)$ denota a chance de Bob medir o estado $|b\rangle$ dado que Alice mediu $|\Phi_j^k\rangle$ e teleportou o estado $|a\rangle$ e ϱ_a^{AB} é dado pelas Eqs. (7.40) ou (7.41), dependo do *qubit* teletransportado por Alice. Se Alice quis teleportar $|+\rangle$ (o bit 0), a probabilidade de Bob obter o resultado correto (estado $|+\rangle$) para cada possível estado de Bell obtido por Alice é

$$p_{B|A}(+|\Phi_1^k+) = \frac{(1+kn)^2}{4(1+k^2)(1+n^2)}, \tag{7.43}$$

$$p_{B|A}(+|\Phi_2^k+) = \frac{(k+n)^2}{4(1+k^2)(1+n^2)}, \tag{7.44}$$

$$p_{B|A}(+|\Phi_3^k+) = \frac{(k+n)^2}{4(1+k^2)(1+n^2)}, \tag{7.45}$$

$$p_{B|A}(+|\Phi_4^k+) = \frac{(1+kn)^2}{4(1+k^2)(1+n^2)}. \tag{7.46}$$

Perceba que as probabilidades (7.43)-(7.46) dependem do emaranhamento usado por Alice na medida de Bell (valor de k) e do emaranhamento do canal escolhido por Bob (valor de n). Alice tem 50% de chance de escolher se ela vai teleportar $|+\rangle$ ou $|-\rangle$ ($p_A(+) = p_A(-) = 1/2$). Portanto, a probabilidade de Bob ver $|+\rangle$ se Alice teletransportou $|+\rangle$ é

$$p_{A,B}(+,+) = p_A(+)\sum_{i=1}^{4} p_{B|A}(+|\Phi_i^k+) = \frac{1}{2}\sum_{i=1}^{4} p_{B|A}(+|\Phi_i^k+). \tag{7.47}$$

Substituindo as Eqs. (7.43)-(7.46) em (7.47) obtemos

$$p_{A,B}(+,+)\Big|_{k,n} = \frac{1}{4} + \frac{kn}{(1+k^2)(1+n^2)}. \tag{7.48}$$

Já a probabilidade de Bob obter o valor errado da codificação do bit de Alice dependendo, do resultado da medida de Bell de Alice, de acordo com (7.42),

$$\begin{aligned} p_{B|A}(-|\Phi_1^k+) = p_{B|A}(-|\Phi_4^k+) &= \frac{(1-kn)^2}{4(1+k^2)(1+n^2)}, \\ p_{B|A}(-|\phi_2^k+) = p_{B|A}(-|\phi_3^k+) &= \frac{(k-n)^2}{4(1+k^2)(1+n^2)}. \end{aligned} \tag{7.49}$$

Consequentemente, a probabilidade total de Bob associar um valor errado para o bit é

$$p_{A,B}(+,-)\Big|_{k,n} = \frac{1}{4} - \frac{kn}{(1+k^2)(1+n^2)}. \tag{7.50}$$

Realizando os mesmos cálculos com Alice teletransportando $|-\rangle$ encontramos que a probabilidade $p_{A,B}(-,-)|_{k,n}$ é a mesma que a probabilidade de Alice enviar $|+\rangle$ e Bob ver $|+\rangle$, Eq. (7.48). Portanto, devemos também ter $p_{A,B}(-,+)|_{k,n} = p_{A,B}(+,-)|_{k,n}$.

As contas acima foram feitas para valores k e n arbitrários. No protocolo GR10 como originalmente proposto, há quatro combinações possíveis para o par (k, n). Podemos ter os casos em que Alice e Bob usaram os mesmos valores para k e n, i.e., $(k,n) = (n_1,n_1)$ e $(k,n) = (n_2,n_2)$. Além desses, há os dois casos nos quais eles discordam dos valores de k e n, ou seja, $(k,n) = (n_1,n_2)$ e $(k,n) = (n_2,n_1)$. Dessa forma, sendo $p_A(n_i)$ e $p_B(n_i)$ as

probabilidades de Alice e Bob usarem o valor de n_i, a probabilidade conjunta de Alice e Bob enviar o bit a e Bob obter o bit b é

$$\begin{aligned} p_{A,B}(a,b) =& p_A(n_1)p_B(n_1)p_{A,B}(a,b)\Big|_{\substack{k=n_1\\n=n_1}} + p_A(n_1)p_B(n_2)p_{A,B}(a,b)\Big|_{\substack{k=n_1\\n=n_2}} \\ &+ p_A(n_2)p_B(n_1)p_{A,B}(a,b)\Big|_{\substack{k=n_2\\n=n_1}} + p_A(n_2)p_B(n_2)p_{A,B}(a,b)\Big|_{\substack{k=n_2\\n=n_2}}. \end{aligned} \tag{7.51}$$

Mas no protocolo GR10 temos $p_A(n_i) = p_B(n_j) = 1/2$ para quaisquer $i, j = 1, 2$. Esse fato mais as Eqs. (7.48) e (7.50) nos permite escrever a Eq. (7.51) da seguinte forma:

$$p_{A,B}(+,+) = p_{A,B}(-,-) = p, \tag{7.52}$$

$$p_{A,B}(+,-) = p_{A,B}(-,+) = 1/2 - p, \tag{7.53}$$

onde

$$p = \frac{1}{4} + \frac{(n_1+n_2)^2(1+n_1n_2)^2}{4(1+n_1^2)^2(1+n_2^2)^2}. \tag{7.54}$$

É importante notar que p é simétrico se trocarmos o valor de n_1 com o de n_2 e que p é uma função crescente nos valores de n_1 ou n_2, sendo sempre maior que $1/4$ se $n_1 \neq 0$ ou $n_2 \neq 0$. Agora, se $n_1 = n_2 = 1$ temos $p = 1/2$. Uma vez que sempre deve haver algum emaranhamento compartilhado entre Alice e Bob na execução do protocolo GR10, temos $1/4 < p \leq 1/2$. [1]

[1] Vale a pena mencionar que se no protocolo BB84 nós aceitássemos todos os casos como um resultado válido, mesmo quando Alice e Bob usaram diferentes bases de preparação e medida, obteríamos uma taxa de erro de 25% no cenário ideal (sem Eva ou ruídos). Quando a condição de *matching* não é satisfeita, os resultados de Bob são completamente aleatórios. Por outro lado, a taxa de erro ideal no protocolo GR10 modificado, $1 - 2p$, depende do emaranhamento dos estados quânticos compartilhados entre Alice e Bob (os valores de n_1 e n_2, conforme a Eq. (7.54)). Por isso, para o protocolo GR10 modificado nós podemos controlar como quisermos a taxa de erro e, para todo $p \geq 3/8 \approx 0.375$, a taxa de $1 - 2p$ será inferior a 25%, aproximando-se do zero conforme n_1 e n_2 tendem a um. E mais, como o protocolo GR10 é baseado no teletransporte quântico, os resultados medidos por Bob não são completamente independentes dos *qubits* teleportados por Alice, incluindo os casos para os quais Alice e Bob associaram diferentes valores de emaranhamento ($n_1 \neq n_2$). É essa onipresente correlação, dependente do emaranhamento, que permite o protocolo GR10 modificado operar seguramente para níveis de emaranhamento suficiente altos.

7.2.2 Análise de segurança do protocolo GR10 modificado

Usando as Eqs. (7.52) e (7.53), a representação baseada em emaranhamento (7.39) torna-se

$$\begin{aligned} |\xi_1\rangle &= \sqrt{p}(|+,+\rangle + |--\rangle) + \sqrt{1/2-p}(|+-\rangle + |-+\rangle) \\ &= \sqrt{2p}|\phi_1\rangle + \sqrt{1-2p}|\phi_2\rangle, \end{aligned} \tag{7.55}$$

onde $|\phi_1\rangle$ e $|\phi_2\rangle$ são os estados de Bell (4.1) and (4.2). Note que suprimimos por simplicidade os subíndices AB quando escrevemos os kets acima.

O estado descrevendo Alice, Bob, e Eva depois que Eva interferiu na transmissão da chave, pode ser representado pela purificação

$$|\Psi\rangle_{ABE} = \sum_{j=1}^{4} \sqrt{\lambda_j}|\xi_j\rangle_{AB}|\epsilon_j\rangle_E. \tag{7.56}$$

Aqui $|\xi_1\rangle$ é dado pela Eq. (7.55) e

$$|\xi_2\rangle = \sqrt{2p}|\phi_2\rangle - \sqrt{1-2p}|\phi_1\rangle, \tag{7.57}$$

$$|\xi_3\rangle = |\phi_3\rangle\,, \tag{7.58}$$

$$|\xi_4\rangle = |\phi_4\rangle\,, \tag{7.59}$$

onde $|\phi_3\rangle$ e $|\phi_4\rangle$ são os estados de Bell (4.3) e (4.4).

Assim como antes, esta maneira específica de se escrever a purificação é crucial em nossa busca por um limite inferior para a fração da chave secreta r. Isto ocorre pois nós iremos obter um vínculo adicional nos possíveis valores dos λ's ao usarmos (7.56) para representar o protocolo GR10 modificado. Este vínculo é obtido notando que Alice sempre teleporta com iguais probabilidades os estados $|+\rangle$ ou $|-\rangle$ e, portanto, o *ensemble* que descreve os estados de Alice são tais que

$$p_A(0) = p_A(1) = 1/2. \tag{7.60}$$

Note que $p_A(+) = p_A(-) = 1/2$ é trivialmente satisfeito.

Um cálculo direto $p_A(a) = \mathrm{tr}\left\{(|a\rangle_A\langle a| \otimes \mathbb{1}_{BE})\,|\Psi\rangle_{ABE}\langle\Psi|\right\}$, e a Eq. (7.56), dá

$$p_A(0) = 1/2 + (\lambda_1 - \lambda_2)\sqrt{2p(1-2p)}, \tag{7.61}$$

$$p_A(1) = 1/2 - (\lambda_1 - \lambda_2)\sqrt{2p(1-2p)}. \tag{7.62}$$

Dessa forma, a Eq. (7.60) é satisfeita para $p \neq 1/2$ se, e apenas se,

$$\lambda_1 = \lambda_2 = \lambda. \tag{7.63}$$

Para $p = 1/2$ esta restrição não é necessária pois nós automaticamente temos $p_A(0) = p_A(1) = 1/2$. Contudo, aplicando argumentos de continuidade para o valor da fração da chave secreta como função de p nós podemos impor $\lambda_1 = \lambda_2$ para todo valor de p sem incorrer em alguma inconsistência física ou matemática. [2]

Antes de prosseguirmos, é importante definir, no contexto atual, o que nós queremos dizer com o *erro* cometido por Bob quando ele mediu seus *qubits* na presença de Eva. Como agora, mesmo sem a interferência de Eva, é possível que Bob obtenha o valor errado do bit enviado por Alice, precisamos de uma definição mais sofisticada "do erro cometido" por Bob que leve em conta este fato.

Com isso em mente, é mais apropriado falar sobre o *desvio* do resultado esperado do caso ideal (sem Eva). Dessa forma, definimos o desvio δ_x como segue,

$$\delta_x = p_{A,B}(+,-) + p_{A,B}(-,+) - p^0_{A,B}(+,-) - p^0_{A,B}(-,+), \tag{7.64}$$

onde $p^0_{A,B}(a,b)$ é a probabilidade conjunta de Alice e Bob obterem, respectivamente, os valores a e b quando Eva não interfere. Note que $p^0_{A,B}(+,-)+p^0_{A,B}(-,+)$ é a probabilidade de Alice e Bob discordarem sobre o valor dos bits na ausência de Eva enquanto $p_{A,B}(+,-)+p_{A,B}(-,+)$ é a probabilidade de eles discordarem quando Eva está presente.

Definimos, também, o desvio relativo em relação à chance de Alice e Bob concordarem com os valores dos bits,

$$\begin{aligned}
\Delta_x &= \frac{p^0_{A,B}(+,+) + p^0_{A,B}(-,-) - p_{A,B}(+,+) - p_{AB}(-,-)}{p^0_{A,B}(+,+) + p^0_{A,B}(-,-)} \\
&= \frac{\left[1 - p^0_{A,B}(+,-) - p^0_{A,B}(-,+)\right] - \left[1 - p_{A,B}(+,-) - p_{A,B}(-,+)\right]}{p^0_{A,B}(+,+) + p^0_{A,B}(-,-)} \\
&= \frac{\delta_x}{p^0_{A,B}(+,+) + p^0_{A,B}(-,-)},
\end{aligned} \tag{7.65}$$

onde a última igualdade origina-se da Eq. (7.64) e do fato de que $\sum_{a,b} p_{A,B}(a,b) = 1$. Perceba que $\delta_x = \Delta_x = \varepsilon_x$ quando a probabilidade de cometer um erro no cenário ideal é

[2] A fração da chave secreta para $p = 1/2$ é a mesma do protocolo GR10 originalmente protosto, veja Sec. 7.1.

zero, como ocorre no protocolo BB84 e no protocolo GR10 original.

Notando que $p^0_{A,B}(a,b)$, para $a,b = +,-$, são dados pelas Eqs. (7.52) e (7.53) e que $p_{A,B}(A,B)$ é obtido refazendo os cálculos da Sec. 7.2.1 utilizando a Eq (7.56) ao invés da (7.39), temos que as Eqs. (7.64) e (7.65) valem

$$\begin{aligned} \delta_x &= \lambda + \lambda_4 - 1 + 2p, && (7.66)\\ \Delta_x &= \delta_x/(2p). && (7.67) \end{aligned}$$

Usando as Eqs. (7.63) e (7.66), junto com a condição de normalização $\sum_{j=1}^{4}\lambda_j = 1$, nós podemos expressar os quatro λ's como se segue,

$$\begin{aligned} \lambda_1 &= \lambda_2 = \lambda, && (7.68)\\ \lambda_3 &= 2p - \delta_x - \lambda = \lambda_+ - \lambda, && (7.69)\\ \lambda_4 &= 1 - 2p + \delta_x - \lambda = \lambda_- - \lambda, && (7.70) \end{aligned}$$

onde

$$\begin{aligned} \lambda_+ &= 2p - \delta_x, && (7.71)\\ \lambda_- &= 1 - 2p + \delta_x, && (7.72) \end{aligned}$$

Como $p_B(+) = p_B(-) = 1/2$ de acordo com a Eq. (7.56), obtemos $H(B) = 1$. Além disso, $p_{B|A}(-|+) = p_{B|A}(+|-) = \lambda_1 + \lambda_4 - 2p(\lambda_1 - \lambda_2)$ e $p_{B|A}(+|+) = p_{B|A}(-|-) = \lambda_2 + \lambda_3 + 2p(\lambda_1 - \lambda_2)$. Consequentemente,

$$H(B|A) = h\left[\lambda_1 + \lambda_4 - 2p(\lambda_1 - \lambda_2)\right] \tag{7.73}$$

pela definição de entropia condicional, Eq. (2.4), com h sendo a entropia binária, Eq. (2.2). Substituindo as Eqs. (7.68)-(7.70) na Eq. (7.73), notando que $H(B) = 1$, a informação mútua entre Alice e Bob vale

$$I(A:B) = 1 - h(2p - \delta_x). \tag{7.74}$$

As quantidades relevantes necessárias para o cálculo da quantidade de Holevo são obtidas da mesma forma que explicamos para os protocolos BB84 e GR10 original:

$$S(\rho^E) = -2\lambda\log\lambda - \lambda_3\log\lambda_3 - \lambda_4\log\lambda_4, \tag{7.75}$$

$$\begin{aligned}\rho_+^E &= \sum_{j=1}^{4} \lambda_j \left|\epsilon_j\right\rangle_E \langle\epsilon_j| \\ &+\sqrt{2p\lambda_1\lambda_3}\left(\left|\epsilon_1\right\rangle_E\langle\epsilon_3| + h.c.\right) - \sqrt{2p\lambda_2\lambda_4}\left(\left|\epsilon_2\right\rangle_E\langle\epsilon_4| + h.c.\right) \\ &-\sqrt{(1-2p)\lambda_1\lambda_4}\left(\left|\epsilon_1\right\rangle_E\langle\epsilon_4| + h.c.\right) - \sqrt{(1-2p)\lambda_2\lambda_3}\left(\left|\epsilon_2\right\rangle_E\langle\epsilon_3| + h.c.\right),\end{aligned} \tag{7.76}$$

$$\begin{aligned}\rho_-^E &= \sum_{j=1}^{4} \lambda_j \left|\epsilon_j\right\rangle_E \langle\epsilon_j| \\ &-\sqrt{2p\lambda_1\lambda_3}\left(\left|\epsilon_1\right\rangle_E\langle\epsilon_3| + h.c.\right) + \sqrt{2p\lambda_2\lambda_4}\left(\left|\epsilon_2\right\rangle_E\langle\epsilon_4| + h.c.\right) \\ &+\sqrt{(1-2p)\lambda_1\lambda_4}\left(\left|\epsilon_1\right\rangle_E\langle\epsilon_4| + h.c.\right) + \sqrt{(1-2p)\lambda_2\lambda_3}\left(\left|\epsilon_2\right\rangle_E\langle\epsilon_3| + h.c.\right).\end{aligned} \tag{7.77}$$

Os autovalores de ρ_+^E and ρ_-^E são os mesmos. Os autovalores não nulos, se usarmos as Eqs. (7.68)-(7.70), podem ser escritos como λ_+ e λ_-, Eqs. (7.71) e (7.72). Isto nos permite escrever

$$S(\rho_+^E) = S(\rho_-^E) = h(\lambda_+) = h(2p - \delta_x). \tag{7.78}$$

A quantidade de Holevo torna-se

$$\chi(A:E) = -2\lambda\log\lambda - (\lambda_+ - \lambda)\log(\lambda_+ - \lambda) - (\lambda_- - \lambda)\log(\lambda_- - \lambda) - h(\lambda_+), \tag{7.79}$$

levando à seguinte fração da chave secreta

$$r = 1 + \min_{\text{Eva}}\left\{2\lambda\log\lambda + (\lambda_+ - \lambda)\log\left(\lambda_+ - \lambda\right) + (\lambda_- - \lambda)\log\left(\lambda_- - \lambda\right).\right\} \tag{7.80}$$

Lembrando que λ_- é dado pela Eq. (7.72) e λ_+ pela Eq. (7.71), nós podemos resolver

$$\frac{dr}{d\lambda} = 0 \tag{7.81}$$

para λ e obter

$$\lambda_{min} = \lambda_+\lambda_- = (2p - \delta_x)(1 - 2p + \delta_x). \tag{7.82}$$

E por um cálculo direto verificamos que

$$\frac{d^2 r(\lambda_{min})}{d\lambda^2} > 0, \tag{7.83}$$

provando que obtemos o valor mínimo de $r(\lambda)$.

Dessa forma, usando as Eqs. (7.71), (7.72) e (7.82), podemos escrever o limite inferior (*lower bound*) para a fração da chave secreta (7.80) como se segue,

$$r = 1 - 2h(\lambda_+) = 1 - 2h(2p - \delta_x) = 1 - 2h[2p(1 - \Delta_x)], \tag{7.84}$$

onde a última igualdade é obtida usando a Eq. (7.67).

No painel principal da Fig. 7.2 nós apresentamos r como função do Δ_x para vários valores de p. Vemos que quanto maior o valor de p maior r e, portanto, maior a fração da chave secreta para um dado valor de Δ_x. Para valores de p próximos ao valor máximo $1/2$, nós garantimos a segurança do protocolo GR10 modificado para uma taxa de desvio relativo no nível de 11%. Conforme diminuímos o valor de p, o qual é relacionado a um menor emaranhamento compartilhado por Alice e Bob, nós não temos mais $r > 0$ para todo $p \lesssim 0.45$. Em outras palavras, contanto que o nível de emaranhamento tal que $p < 0.45$, nós podemos gerar uma chave secreta segura apenas se usarmos o protocolo GR10 original, o qual funciona para qualquer valor de $p > 1/4$ ($n_1 \neq 0$ e $n_2 \neq 0$). Contudo, o preço a ser pago ao se reduzir p no protocolo original corresponde a redução do tamanho da chave bruta R.

No detalhe da Fig. 7.2 nós mostramos como o limite inferior da fração da chave secreta responde aos protocolos de reconciliação de erro cuja eficiência não seja máxima. Os protocolos de reconciliação não-ideal possuem uma redução efetiva na informação mútua compartilhada por Alice e Bob na expressão de r [7–9]. Neste cenário, r altera-se para

$$r = \beta I(A : B) - \max_{\text{Eve}} \chi(A : E), \tag{7.85}$$

onde $0 \leq \beta \leq 1$. Repetindo todos os passos dos cálculos anteriores quando tivemos $\beta = 1$, nós encontramos para o limite inferior da fração da chave secreta,

$$r = \beta[1 - h(\lambda_+)] - h(\lambda_+). \tag{7.86}$$

Para esquemas de distribuição de chaves quânticas com variáveis discretas, os protocolos de reconciliação possuem $\beta \approx 1$. Em todo caso, nós testamos como o protocolo GR10 modificado responde ao protocolo de reconciliação com $\beta = 0.8$, um valor muito conservador. Como podemos ver no detalhe da Fig. 7.2, o protocolo GR10 ainda opera seguramente para $p \geq 0.46$ quando nós temos taxas de desvios Δ_x menores ou iguais a 1% enquanto para $p = 0.49$ nós encontramos segurança sempre que$\Delta_x \lesssim 7\%$.

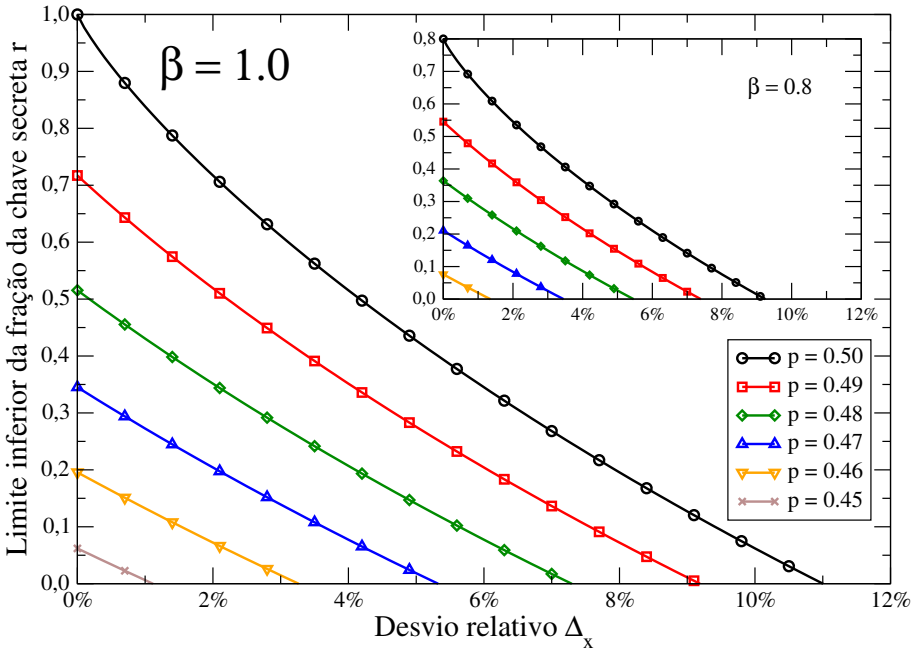

Figura 7.2: Painel principal: Limite inferior (*lower bound*) de r, a fração da chave secreta para o protocolo GR10 modificado como dado pela Eq. (7.84), em função de Δ_x, o desvio relativo do valor esperado da probabilidade de Alice e Bob obter o mesmo valor do bit com e sem a presença de Eva. Detalhe: O mesmo que o painel principal mas supondo uma eficiência para o protocolo de reconciliação de $\beta = 0.8$.

Vale mencionar que o limite inferior para a fração da chave secreta computada acima implica que o protocolo GR10 modificado funciona mesmo para $n_1 = n_2$ e, em particular, para $n_1 = n_2 = 1$. O último caso corresponde ao uso do protocolo de teletransporte quântico padrão e determinístico para estabelecer uma chave secreta entre Alice e Bob, onde Alice teletransporta apenas os estados $|+\rangle$ e $|-\rangle$. Em outras palavras, isto significa que ao usarmos o protocolo de teletransporte como originalmente apresentado [16], nós podemos estabelecer uma comunicação segura entre as partes empregando apenas estados ortogonais para codificar os valores dos bits teleportados de Alice para Bob. Não há a necessidade de usar estados não-ortogonais como nos protocolos BB84 e B92 [4, 13].

Este comportamento *contraintuitivo* pode ser compreendido notando que o protocolo de teletransporte possui um aspecto probabilístico que não pode ser evitado por nenhum espião. De fato, pelas leis da mecânica quântica, ninguém, nem mesmo Eva, tem controle sobre qual estado de Bell irá emergir da medida realizada por Alice. Este aspecto probabilístico intrínseco do protocolo de teletransporte quântico impede Eva de interferir no protocolo de teletransporte quântico sem ser detectada por Alice e Bob. Isto ocorre

precisamente por causa das transformações unitárias que Bob necessita realizar em seus *qubits* ao final do protocolo as quais dependem do resultado da medida de Bell de Alice e do emaranhamento compartilhado entre eles. Desta maneira, se Eva interferir no protocolo de teletransporte tentando descobrir o estado teleportado a Bob, ela irá causar mudanças no estado de Bell compartilhado entre Alice e Bob. Portanto, a operação unitária correta que Bob deve implementar para corrigir seu *qubit* mudará também. Bob, sem saber desta interferência, implementará o operação unitária associada ao estado de Bell original que compartilhou com Alice. Mas o uso de uma operação unitária errada fará com que Bob associe um valor errado para o bit teletransportado de Alice. E este erro levará Alice e Bob a detectar a presença de Eva quando eles compararem os valores dos seus bits. Matematicamente, este fato intuitivo irá eventualmente se refletir em uma taxa de chave secreta r positiva, mesmo quando $n_1 = n_2$.

Finalizamos esta seção considerando duas outras maneiras de se modificar o protocolo GR10. A primeira é baseada no fato de que quanto maior p maior a taxa de desvio tolerada e ainda assim a chave ser considerada segura (Fig. 7.2). A segunda corresponde a aumentar o número de estados quânticos utilizados para codificar os bits teletransportados de Alice para Bob. Nós podemos, como no protocolo BB84, usar os estados $|y_0\rangle$ e $|y_1\rangle$ (base y) juntamente com os estados $|+\rangle$ e $|-\rangle$ para codificar os valores dos bits. Neste caso nós estaremos usando estados não ortogonais para codificar os bits e podemos pensar que o protocolo GR10 é uma camada extra de segurança para o protocolo BB84.

Essas duas modificações serão investigadas a seguir.

7.2.3 Explorando os possíveis valores da probabilidade p

Na Sec. 7.2.1 calculamos o valor de p, Eq. (7.54), para a representação baseada em emaranhamento $|\xi_1\rangle$, Eq. (7.55),

$$|\xi_1\rangle = \sqrt{2p}|\phi_1\rangle + \sqrt{1-2p}|\phi_2\rangle.$$

Descobrimos, ao final da seção, que quanto maior o valor de p maior a taxa de erro tolerada pelo sistema para que a transmissão da chave seja considerada segura. Com isso em mente, podemos elaborar novos *ensembles* para definir outros coeficientes p. Isto é, pós-selecionando determinados eventos nós podemos aumentar p.

Previamente, p foi calculado considerando todos os casos. Isto é, Bob usou o canal com emaranhamento n_1 e Alice mediu com emaranhamento n_1; Bob usou o canal n_1 e Alice

mediu com n_2; Bob usou o canal n_2 e Alice mediu com n_1; Bob usou o canal n_2 e Alice mediu com n_2. Incluímos, também, todos os resultados das medidas realizadas por Alice. Resumindo, nada foi descartado. Esse *ensemble* nos levou à Eq. (7.54),

$$p = \frac{1}{4} + \frac{(n_1+n_2)^2(1+n_1n_2)^2}{4(1+n_1^2)^2(1+n_2^2)^2}.$$

Este resultado foi obtido através das Eqs. (7.48) e (7.50) reescritas abaixo,

$$p_{A,B}(+,+)\Big|_{k,n} = p_{A,B}(-,-)\Big|_{k,n} = \frac{1}{4} + \frac{kn}{(1+k^2)(1+n^2)}.$$

$$p_{A,B}(+,-)\Big|_{k,n} = p_{A,B}(-,+)\Big|_{k,n} = \frac{1}{4} - \frac{kn}{(1+k^2)(1+n^2)}.$$

No novo *ensemble* consideramos somente os casos para os quais a condição de *matching* foi satisfeita. Portanto, descartaremos todos os casos em que o emaranhamento k escolhido por Alice para realizar a medida de Bell generalizada seja diferente do emaranhamento n do canal escolhido por Bob.

Podemos ver pelas equações anteriores que a probabilidade de Bob associar o valor correto do bit de Alice é o mesmo se ela teleportou $|+\rangle$ ou $|-\rangle$. Portanto, definiremos o coeficiente deste *ensemble* como p_M (p do *matching*), o qual é dado por

$$p_M = \frac{1}{\mathcal{N}}\left(p_{A,B}(+,+)\Big|_{\substack{k=n_1\\n=n_1}} + p_{A,B}(+,+)\Big|_{\substack{k=n_2\\n=n_2}}\right). \tag{7.87}$$

Aqui, $1/\mathcal{N}$ é a constante de normalização, i.e., a somatória de todos os eventos possíveis em que ocorre o *matching*.

$$\begin{aligned}\mathcal{N} =& p_{A,B}(+,+)\Big|_{\substack{k=n_1\\n=n_1}} + p_{A,B}(+,+)\Big|_{\substack{k=n_2\\n=n_2}} + p_{A,B}(-,-)\Big|_{\substack{k=n_1\\n=n_1}} + p_{A,B}(-,-)\Big|_{\substack{k=n_2\\n=n_2}} \\ &+ p_{A,B}(+,-)\Big|_{\substack{k=n_1\\n=n_1}} + p_{A,B}(+,-)\Big|_{\substack{k=n_2\\n=n_2}} + p_{A,B}(-,+)\Big|_{\substack{k=n_1\\n=n_1}} + p_{A,B}(-,+)\Big|_{\substack{k=n_2\\n=n_2}}.\end{aligned} \tag{7.88}$$

Aplicando as Eqs. (7.48) e (7.50) nas Eqs. (7.87) e (7.88) encontramos que

$$p_M = \frac{1}{4} + \frac{n_1^2}{2\left(1+n_1^2\right)^2} + \frac{n_2^2}{2\left(1+n_2^2\right)^2}. \tag{7.89}$$

Perceba que, assim como p, p_M não muda se trocarmos n_1 por n_2 e seu comportamento é

monotonicamente crescente com n_1 e n_2, sendo o mínimo 1/4 ocorrendo para $n_1 = n_2 = 0$ e o valor máximo 1/2 quando temos $n_1 = n_2 = 1$.

Outro *ensemble* que podemos usar ocorre quando Bob mantém seu canal fixo, n_1 por exemplo, e Alice escolhe n_1 ou n_2 para realizar a medida. Neste conjunto os casos descartados são todos aqueles em que Bob utilizou o canal n_2. Definiremos este coeficiente como p_{P_1} (p parcial com n_1):

$$\begin{aligned} p_{P_1} =& p_A(n_1)p_{A,B}(+,+)\Big|_{\substack{k=n_1\\n=n_1}} + p_A(n_2)p_{A,B}(+,+)\Big|_{\substack{k=n_2\\n=n_1}}, \\ =& \frac{1}{2}\left(p_{A,B}(+,+)\Big|_{\substack{k=n_1\\n=n_1}} + p_{A,B}(+,+)\Big|_{\substack{k=n_2\\n=n_1}} \right). \end{aligned} \tag{7.90}$$

Substituindo a Eq. (7.48) na Eq. (7.90) encontramos

$$p_{P_1} = \frac{1}{4} + \frac{n_1(n_1+n_2)(1+n_1n_2)}{2\left(1+n_1^2\right)^2\left(1+n_2^2\right)^2}. \tag{7.91}$$

Considerando agora que Bob manteve fixo o canal n_2 encontramos

$$p_{P_2} = \frac{1}{4} + \frac{n_2(n_1+n_2)(1+n_1n_2)}{2\left(1+n_1^2\right)^2\left(1+n_2^2\right)^2}. \tag{7.92}$$

Note que os valores p_{P_1} e p_{P_2}, Eqs. (7.91) e (7.92), não são simétricos quando reindexamos $n_1 \leftrightarrow n_2$. Contudo, o comportamento estritamente crescente ainda está presente. Os limites inferior e superior são os mesmos dos outros coeficientes calculados. Isto é, $1/4 \leq p_{P_i} \leq 1/2$.

Até o presente momento definimos quatro diferentes *ensembles* cujas representações baseadas em emaranhamento são dadas por $|\xi_1\rangle$ com p dado pelas Eqs. (7.54), (7.89), (7.91) e (7.92) [3]. Das Eqs. (7.54) e (7.89) podemos dizer que $p_M \geq p$ se somente se

$$(n_1 - n_2)^2(1 - n_1n_2)^2 \geq 0, \tag{7.93}$$

o que é verdade para todo n_1 e n_2 reais. Verificamos também que $p_{P1} \geq p_M$, pelas

[3] Se levarmos em consideração o protocolo GR10 original, teremos um mais um *ensemble*. O protocolo GR10 original nada mais é que o *ensemble* onde os casos considerados são provenientes de quando a condição de *matching* é satisfeita e Alice obtém $|\Phi_2^k\rangle$ ou $|\Phi_3^k\rangle$ na medida generalizada de Bell. O conjunto citado leva a um coeficiente independente dos emaranhamentos n_1 e n_2, isto é, o coeficiente p é constante e igual a1/2.

Eqs. (7.89) e (7.91), se somente se

$$(n_1 - n_2)(1 - n_1 n_2)n_2 \geq 0. \tag{7.94}$$

Essa afirmação é verdadeira para $n_1 \geq n_2$ devido a n_1 e n_2 pertencerem ao intervalo $[0, 1]$.

Levando em consideração os resultados (7.93) e (7.94), e também os limites inferior e superior dos p's, podemos afirmar que

$$\frac{1}{2} \geq p_{P1} \geq p_M \geq p \geq \frac{1}{4} \qquad \text{para } n_1 \geq n_2. \tag{7.95}$$

Definindo que n_1 sempre será maior que n_2 temos que a relação acima sempre se verificará para o protocolo GR10. Na Fig. 7.3 podemos ver este comportamento. Nela plotamos dois gráficos da probabilidade em função do emaranhamento n_1. No primeiro consideramos $n_2 = 0.25$ e no segundo $n_2 = 0.8$. Podemos ver que as probabilidades referentes aos *ensembles* parciais p_{P_1} e p_{P_2}, Eqs. (7.91) e (7.92), alternam entre a maior e a menor probabilidade. Vale ressaltar que a probabilidade p_{P_i} ocorre quando descartamos o canal enviado por Bob com emaranhamento diferente de n_i. Para o *ensemble* em que consideramos somente os casos que satisfazem a condição de *matching*, p_M (veja Eq. (7.89), é maior do que p (veja Eq. (7.54))quando consideramos todos os casos como válido.

7.2.4 Protocolo GR10 com estados não ortogonais

Na seção anterior vimos que é possível aumentar o valor de p dependo do *ensemble* escolhido. Agora, nós nos propomos a aumentar o número de estados quânticos que codificam os bits. Ou seja, ao invés de Alice teletransportar os *qubits* somente na base x, ela irá teletransportá-los também na base de y. Ao implementar o protocolo GR10 utilizando duas bases, tudo se passa como se realizássemos o protocolo BB84 usando teletransporte quântico. Adicionamos, assim, uma camada extra de segurança ao protocolo BB84. Além disso, utilizamos a base y para a codificação dos bits em detrimento da base z (como proposto originalmente no protocolo BB84), por ser mais simples relacionarmos a representação baseada em emaranhamento da base x com a da base y. Com essa escolha para as bases precisamos apenas de uma transformação local entre Alice e Bob para conectá-las. Se usássemos a base z, o emaranhamento entre Alice e Bob seria diferente do emaranhamento da base x. Logo, seria preciso realizar uma transformação global entre Alice e Bob para relacionarmos as duas representações baseadas no emaranhamento. Uma explicação mais

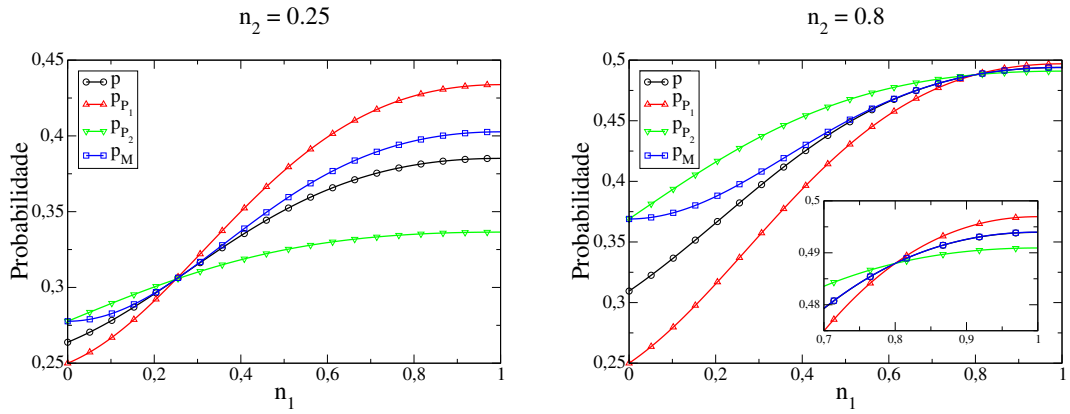

Figura 7.3: Gráfico comparativo entre os diferentes *ensembles* utilizados para construir o protocolo GR10 modificado. A ordenada é a probabilidade de Alice e Bob concordarem com os valores dos bits em função do emaranhamento n_1 para n_2 fixo. No painel 7.3a fixamos $n_2 = 0.25$ e no painel 7.3b temos $n_2 = 0.8$. Em ambos os gráficos temos p, Eq. (7.54), curva preta com círculos; p_{P_1} e p_{P_2}, Eqs. (7.91) e (7.92), curvas vermelha com triângulos para cima e verde com triângulos invertidos, respectivamente; e por fim, p_M, a Eq. (7.89), representado pela curva azul com quadrados. Nos gráficos percebemos que a maior fração da chave secreta é obtida pelo *ensemble* representado pelo coeficiente p_{P_1} quando $n_1 > n_2$ (p_{P_2} se $n_2 > n_1$) e o segundo melhor resultado é dado por p_M.

detalhada disso será dada adiante.

Considerando que agora temos duas bases para codificar os bits, a decomposição de Schmidt mais vantajosa para se trabalhar nessas condições é

$$|\Psi\rangle_{ABE} = \sum_{j=1}^{4} \sqrt{\lambda_j} |\Xi_j\rangle_{AB} |\epsilon_j\rangle_E . \tag{7.96}$$

onde

$$\begin{aligned} |\Xi_1\rangle &= \sqrt{2p}\,|\phi_1\rangle + \sqrt{1-2p}\,|\phi_2\rangle\,, \\ |\Xi_2\rangle &= \sqrt{2p}\,|\phi_2\rangle - \sqrt{1-2p}\,|\phi_1\rangle\,, \\ |\Xi_3\rangle &= \sqrt{2p}\,|\phi_3\rangle + \sqrt{1-2p}\,|\phi_4\rangle\,, \\ |\Xi_4\rangle &= \sqrt{2p}\,|\phi_4\rangle - \sqrt{1-2p}\,|\phi_3\rangle\,. \end{aligned} \tag{7.97}$$

Aqui os $|\phi_i\rangle$ são os estados de Bell, Eqs. (4.1)-(4.4), e p representa qualquer uma das probabilidades de Alice e Bob possuírem o mesmo *qubit* após o envio da chave secreta calculados nas seções anteriores. Isto é, p pode assumir valores dados pelas Eqs. (7.54), (7.89), (7.91) e $p = 1/2$ quando usamos protocolo GR10 original, Sec. 7.1. Desta forma, escrevendo a

decomposição de Schmidt a partir dos resultados dados pela Eq. (7.97) englobamos todos os protocolos GR10 estudados até o momento. Como nós possuímos uma nova representação para o estado $|\Psi\rangle_{ABE}$, Eq. (7.96), devemos recalcular a fração da chave secreta r, Eq. (2.122) para esta purificação.

A informação mútua entre Alice e Bob, cuja definição é $I(A:B) = H(B) - H(B|A)$, pode ser obtida facilmente considerando o operador densidade $\varrho^{AB} = \mathrm{tr}_E \{|\Psi\rangle_{ABE}\langle\Psi|\}$ da Eq. (7.96). Calculando os elementos necessários para se obter a entropia de Shannon de Bob $H(B)$, a partir de

$$p_B(b) = \mathrm{tr}\left\{\varrho^{AB}(\mathbb{1}_A \otimes |b\rangle_B\langle b|)\right\}, \tag{7.98}$$

resultando em

$$p_B(+) = p_B(-) = \frac{1}{2}. \tag{7.99}$$

Aplicando diretamente essas probabilidades na definição de entropia, Eq. (2.1), temos

$$H(B) = 1. \tag{7.100}$$

Para $H(B|A)$, a parte condicional da informação mútua, devemos calcular as probabilidades de Alice e as probabilidades condicionais de Bob utilizando

$$p_A(a) = \mathrm{tr}\left\{\varrho^{AB}(|a\rangle_A\langle a|) \otimes \mathbb{1}_B\right\} \tag{7.101}$$

e

$$p_{B|A}(b|a) = \mathrm{tr}\left\{\left(\frac{(|a\rangle_A\langle a| \otimes \mathbb{1}_B)\,\varrho^{AB}\,(|a\rangle_A\langle a| \otimes \mathbb{1}_B)}{\mathrm{tr}\left\{\varrho^{AB}\,(|a\rangle_A\langle a| \otimes \mathbb{1}_B)\right\}}\right)(\mathbb{1}_A \otimes |b\rangle_B\langle b|)\right\}. \tag{7.102}$$

Disso resulta que

$$p_A(+) = p_A(-) = \frac{1}{2} \tag{7.103}$$

e

$$\begin{aligned} p_{B|A}(+|+) = p_{B|A}(-|-) &= 2p + (1-4p)(\lambda_2+\lambda_4), \\ p_{B|A}(+|-) = p_{B|A}(-|+) &= 1 - 2p - (1-4p)(\lambda_2+\lambda_4). \end{aligned} \tag{7.104}$$

O resultado anterior é obtido utilizando a normalização dos λ's, $\sum_i^4 \lambda_i = 1$. Consequentemente, usando as probabilidades (7.103) e (7.104) encontramos a entropia condicional de Bob em relação a Alice (veja Eq. (2.4)),

$$H(B|A) = h\Big[2p + (1-4p)(\lambda_2+\lambda_4)\Big], \tag{7.105}$$

onde $h(x) = -x\log(x) - (1-x)\log(1-x)$ é a entropia binária (2.2).

Portanto, juntando as Eqs. (7.100) e (7.105) temos a seguinte expressão para a informação mútua (Eq. (2.6))

$$I(A:B) = 1 - h\Big[2p + (1-4p)(\lambda_2 + \lambda_4)\Big], \tag{7.106}$$

onde h é a Eq. (2.2) e os coeficientes λ_2 e λ_4 serão determinados mais à frente.

A quantidade de Holevo entre Alice e Eva, Eq. (2.105), dado por $\chi(A:\varrho^E) = S(\varrho^E) - \sum p_A(a)S(\varrho_a^E)$, já possuí um de seus fatores calculados. Este fator é a entropia quântica de Eva que é igual a entropia quântica conjunta de Alice e Bob , $S(\varrho^E) = S(\varrho^{AB})$, lema associado a Eq. (2.48). Pela definição da entropia quântica, Eq. (2.24), a entropia quântica de um operador é a entropia de Shannon dos autovalores desse operador e como ϱ^{AB} é diagonal, a entropia quântica de Eva é

$$S(\varrho^E) = -\sum_{i=1}^{4} \lambda_i \log(\lambda_i), \tag{7.107}$$

Para calcular ϱ_0^E e ϱ_1^E usamos o postulado da medida cuja aplicação é dada pela Eq. (2.103),

$$\varrho_a^E = \mathrm{tr}_{AB}\left\{\frac{(|a\rangle_A\langle a| \otimes \mathbb{1}_{BE})\varrho^{ABE}(|a\rangle_A\langle a| \otimes \mathbb{1}_{BE})}{\mathrm{tr}\left\{\varrho^{ABE}(|a\rangle_A\langle a| \otimes \mathbb{1}_{BE})\right\}}\right\},$$

com $\varrho^{ABE} = |\Psi\rangle_{ABE}\langle\Psi|$ dado pela Eq. (7.96). Assim, com $|a\rangle = |+\rangle$ e $|a\rangle = |-\rangle$, obtemos as matrizes densidade de Eva caso ela conhecesse o estado medido por Alice,

$$\begin{aligned}\varrho_0^E =& \sum_{i=1}^{4} \lambda_i |\epsilon_i\rangle_E\langle\epsilon_i| \\ &- (1-4p)\sqrt{\lambda_1\lambda_3}\left(|\epsilon_1\rangle_E\langle\epsilon_3| + h.c.\right) - 2\sqrt{2p(1-2p)\lambda_1\lambda_4}\left(|\epsilon_1\rangle_E\langle\epsilon_4| + h.c.\right) \\ &- 2\sqrt{2p(1-2p)\lambda_2\lambda_3}\left(|\epsilon_2\rangle_E\langle\epsilon_3| + h.c.\right) + (1-4p)\sqrt{\lambda_2\lambda_4}\left(|\epsilon_2\rangle_E\langle\epsilon_4| + h.c.\right),\end{aligned} \tag{7.108}$$

$$\begin{aligned}\varrho_1^E =& \sum_{i=1}^{4} \lambda_i |\epsilon_i\rangle_E\langle\epsilon_i| \\ &+ (1-4p)\sqrt{\lambda_1\lambda_3}\left(|\epsilon_1\rangle_E\langle\epsilon_3| + h.c.\right) + 2\sqrt{2p(1-2p)\lambda_1\lambda_4}\left(|\epsilon_1\rangle_E\langle\epsilon_4| + h.c.\right) \\ &+ 2\sqrt{2p(1-2p)\lambda_2\lambda_3}\left(|\epsilon_2\rangle_E\langle\epsilon_3| + h.c.\right) - (1-4p)\sqrt{\lambda_2\lambda_4}\left(|\epsilon_2\rangle_E\langle\epsilon_4| + h.c.\right).\end{aligned} \tag{7.109}$$

Os autovalores de ϱ_0^E e ϱ_1^E são idênticos e valem

$$\begin{aligned}&\Big\{0, 0, \frac{1}{2}\left[1-\sqrt{(\lambda_1-\lambda_2+\lambda_3-\lambda_4)^2-32p(1-2p)(\lambda_1-\lambda_2)(\lambda_3-\lambda_4)}\right],\\ &\frac{1}{2}\left[1+\sqrt{(\lambda_1-\lambda_2+\lambda_3-\lambda_4)^2-32p(1-2p)(\lambda_1-\lambda_2)(\lambda_3-\lambda_4)}\right]\Big\}.\end{aligned} \tag{7.110}$$

Consequentemente, pela definição de entropia quântica,

$$S(\varrho_0^E)=S(\varrho_1^E)=h\left[\frac{1}{2}-\frac{1}{2}\sqrt{(\lambda_1-\lambda_2+\lambda_3-\lambda_4)^2-32p(1-2p)(\lambda_1-\lambda_2)(\lambda_3-\lambda_4)}\right], \tag{7.111}$$

com h sendo a entropia binária (2.2).

Juntando as Eqs. (7.111) e (7.107), podemos calcular a quantidade de Holevo (2.105),

$$\begin{aligned}\chi(A:\varrho^E)=&-\lambda_1\log(\lambda_1)-\lambda_2\log(\lambda_2)-\lambda_3\log(\lambda_3)-\lambda_4\log(\lambda_4)\\ &-h\left[\frac{1}{2}-\frac{1}{2}\sqrt{(\lambda_1-\lambda_2+\lambda_3-\lambda_4)^2-32p(1-2p)(\lambda_1-\lambda_2)(\lambda_3-\lambda_4)}\right].\end{aligned} \tag{7.112}$$

Por fim, a fração da chave secreta (2.122), definida como $r=I(A:B)-\max\{\chi(A:\varrho^E)\}$ é obtida utilizando a Eq. (7.106) para a informação mútua e Eq. (7.112) para a quantidade de Holevo. Disso resulta em

$$\begin{aligned}r=&1-h\Big[2p+(1-4p)(\lambda_2+\lambda_4)\Big]\\ &+\min\Bigg\{\lambda_1\log(\lambda_1)+\lambda_2\log(\lambda_2)+\lambda_3\log(\lambda_3)+\lambda_4\log(\lambda_4)\\ &+h\left[\frac{1}{2}-\frac{1}{2}\sqrt{(\lambda_1-\lambda_2+\lambda_3-\lambda_4)^2-32p(1-2p)(\lambda_1-\lambda_2)(\lambda_3-\lambda_4)}\right]\Bigg\}.\end{aligned} \tag{7.113}$$

Se a Eq. (7.113) for positiva temos uma chave criptográfica transmitida de forma segura. De fato, se $r>0$ Alice e Bob conhecem mais sobre a chave do que Eva. Vale lembrar que, os autovalores λ's estão associados a dados experimentais (taxas de erro). Temos, então, que verificar como as taxas de erro estão relacionadas com os λ's. E como feito para o BB84 nos capítulos 4 e 6, a base x foi usada para escrever a fração da chave secreta, enquanto a base y é utilizada para verificarmos quanta informação Eva é capaz de extrair dos *qubits* enviados e codificados pela base x.

Se o canal fosse perfeito e não monitorado por Eva, a representação baseada em emaranhamento (7.96) possuiria todos os λ's nulos exceto λ_1, cujo valor seria um. Sendo assim,

o estado $|\Xi_1\rangle$, Eq. (7.97), é a representação baseada em emaranhamento quando Alice e Bob utilizam a base x para codificar os bits. Escrevendo explicitamente $|\Xi_1\rangle$ na base x temos

$$|\Xi_1\rangle_{AB} = \sqrt{p}\,(|{+}{+}\rangle_{AB} + |{-}{-}\rangle_{AB}) + \sqrt{\frac{1}{2} - p}\,(|{+}{-}\rangle_{AB} + |{-}{+}\rangle_{AB})\,. \tag{7.114}$$

Por outro lado, se representarmos $|\Xi_1\rangle = \sqrt{2p}\,|\phi_1\rangle + \sqrt{1-2p}\,|\phi_2\rangle$ na base y encontramos

$$|\Xi_1\rangle_{AB} = \sqrt{p}\,(|y_0y_1\rangle_{AB} + |y_1y_0\rangle_{AB}) + \sqrt{\frac{1}{2} - p}\,(|y_0y_0\rangle_{AB} + |y_1y_1\rangle_{AB})\,. \tag{7.115}$$

Note que a Eq. (7.115) não é uma representação fidedigna da execução do protocolo quando Alice e Bob utilizam a base y. Isto ocorre pois, a probabilidade de Bob associar o valor correto do bit enviado por Alice deveria ser p e não $1/2 - p$ [4]. Portanto, para que uma mesma representação baseada em emaranhamento reproduza as estastísticas corretas para ambas as bases, Bob deve aplicar um *bit flip* em seus *qubits* quando ele e Alice estão usando a base y (veja Sec. 5.1) [5]. Sendo assim, nós temos que a representação baseada em emaranhamento para a base y é

$$|\Psi_y\rangle_{ABE} \;=\; (\mathbb{1}_{AE} \otimes \sigma_{zB})\,|\Psi\rangle_{ABE}\,. \tag{7.116}$$

Se ao invés de considerarmos a base y tivéssemos considerado a base z, a representação baseada em emaranhamento na base z seria dada por $|\phi_1\rangle$ (veja apêndice F). Portanto, não seria possível associar o estado inicial de Alice e Bob na base x, $|\Xi_1\rangle = \sqrt{2p}\,|\phi_1\rangle + \sqrt{1-2p}\,|\phi_2\rangle$ com o estado inicial da base z por uma transformação unitária local. Isso ocorre do fato que a quantidade de emaranhamento dos ambos dois estados é diferente. Dessa forma, seria necessária uma transformação global em Alice e Bob para conectar os dois estados.

Como no nosso caso Bob aplica localmente a transformação unitária $\mathbb{1}_A \otimes \sigma_{zB}$, podemos

[4] Essa probabilidade é obtida seguindo os passos da Sec. 7.2.1 substituindo $|+\rangle$ por $|y_0\rangle$ e $|-\rangle$ por $|y_1\rangle$. Ao final dos cálculos encontraríamos que a representação baseada em emaranhamento quando Alice e Bob utilizam a base y é $\sqrt{2p}\,|\phi_2\rangle + \sqrt{1-2p}\,|\phi_1\rangle$. Ou seja, o $|\Xi_2\rangle$. Estes cálculos podem ser visualizados no apêndice F

[5] Note que esse *bit flip* somente ocorre no nível da representação baseada em emaranhamento. Durante a execução real do protocolo, Bob somente aplica as transformações em seus *qubits* baseados nas medidas de Bell obtidas por Alice.

usar uma única representação baseada em emaranhamento, $|\Psi\rangle_{ABE}$ dado pela Eq. (7.96), para extrair as informações da base y (veja mais detalhes na Sec. 5.1).

Com isso em mente, após Eva interferir temos o estado (7.96),

$$|\Psi\rangle_{ABE} = \sum_{i=1}^{4} \sqrt{\lambda_i}\, |\Xi_i\rangle_{AB}\, |\epsilon_i\rangle_E \,,$$

onde $|\Xi_i\rangle$ são os estados de Alice e Bob dados pela Eq. (7.97) e $|\epsilon_i\rangle$ os estados de Eva que Alice e Bob não possuem conhecimento. Tomando o traço sobre Eva, obtemos o estado de Alice e Bob quando eles usam a base x,

$$\varrho^{AB} = \lambda_1 |\Xi_1\rangle_{AB}\langle\Xi_1| + \lambda_2 |\Xi_2\rangle_{AB}\langle\Xi_2| + \lambda_3 |\Xi_3\rangle_{AB}\langle\Xi_3| + \lambda_4 |\Xi_4\rangle_{AB}\langle\Xi_4| \,. \tag{7.117}$$

Por outro lado, pela Eq. (7.116), quando Alice e Bob utilizam a base y, o operador densidade compartilhado por ambos é

$$\varrho_y^{AB} \;=\; (\mathbb{1}_A \otimes \sigma_{zB})\, \varrho^{AB}\, (\mathbb{1}_A \otimes \sigma_{zB})^\dagger \,. \tag{7.118}$$

Antes do monitoramento de Eva as probabilidades de concordância sobre os valores dos bits são

$$p^0_{A,B}(+,+) = p^0_{A,B}(-,-) \;=\; p, \tag{7.119}$$

$$p^0_{A,B}(+,-) = p^0_{A,B}(-,+) \;=\; \left(\frac{1}{2} - p\right). \tag{7.120}$$

Com Eva ou ruído, as probabilidades de Alice e Bob na base x são calculadas a partir de

$$p_{A,B}(a,b) = \mathrm{tr}\left\{\varrho^{AB}(|a\rangle_A\langle a| \otimes |b\rangle_B\langle b|)\right\}, \qquad a,b = +,-, \tag{7.121}$$

onde ϱ^{AB} é a Eq. (7.117). Após os cálculos temos que

$$p_{A,B}(+,+) = p_{A,B}(-,-) \;=\; p(\lambda_1 + \lambda_3) + \left(\frac{1}{2} - p\right)(\lambda_2 + \lambda_4), \tag{7.122}$$

$$p_{A,B}(+,-) = p_{A,B}(+,-) \;=\; \left(\frac{1}{2} - p\right)(\lambda_1 + \lambda_3) + p(\lambda_2 + \lambda_4). \tag{7.123}$$

Como discutido anteriormente, não faz sentido falarmos aqui em erro da medida, já que o protocolo GR10 permite que Bob obtenha um resultado diferente do teletransportado

por Alice dependendo do valor de p utilizado. Sendo assim, vamos definir

$$\delta_x \equiv p_{A,B}(+,-) + p_{A,B}(-,+) - p^0_{A,B}(+,-) - p^0_{A,B}(-,+), \tag{7.124}$$

com $p^0_{A,B}$ sendo as probabilidades na ausência de Eva e $p_{A,B}$ as probabilidades após Eva interferir (as probabilidades reais obtidas). Aplicando as Eqs. (7.123) e (7.120) na Eq. (7.124), e usando que $\sum_i^4 \lambda_i = 1$, encontramos para a base x,

$$\delta_x = (4p-1)(\lambda_2 + \lambda_4). \tag{7.125}$$

Perceba que δ_x é não negativo e pode ser no máximo $(4p-1)$ já que $(\lambda_2+\lambda_4) \leq 1$ e $1/4 < p \leq 1/2$. Note também que o valor de p deve ser diferente de $1/4$ para que δ_x não seja nulo para todo λ.

Considerando agora que Alice teletransportou os *qubits* na base y, as probabilidades na ausência de Eva são

$$p^0_{A,B}(y_0,y_0) = p^0_{A,B}(y_1,y_1) = p, \tag{7.126}$$

$$p^0_{A,B}(y_0,y_1) = p^0_{A,B}(y_1,y_0) = \frac{1}{2} - p. \tag{7.127}$$

Após a intromissão de Eva, utilizando ϱ^{AB}_y, Eq. (7.118), temos

$$p_{A,B}(y_i,y_j) = \mathrm{tr}\left\{(\mathbb{1}_A \otimes \sigma_{zB})\,\varrho^{AB}\,(\mathbb{1}_A \otimes \sigma_{zB})^\dagger\,(|y_i\rangle_A\langle y_i| \otimes |y_j\rangle_B\langle y_j|)\right\}, \qquad i,j = 0,1, \tag{7.128}$$

e portanto

$$p_{A,B}(y_0,y_0) = p_{A,B}(y_1,y_1) = p(\lambda_1+\lambda_4) + \left(\frac{1}{2}-p\right)(\lambda_2+\lambda_4), \tag{7.129}$$

$$p_{A,B}(y_0,y_1) = p_{A,B}(y_1,y_0) = \left(\frac{1}{2}-p\right)(\lambda_1+\lambda_4) + p(\lambda_2+\lambda_3). \tag{7.130}$$

Substituindo (7.130) e (7.127) na Eq. (7.124) e se valendo da normalização dos λ's obtemos

$$\delta_y = (4p-1)(\lambda_2+\lambda_3), \tag{7.131}$$

também com valores pertencentes ao intervalo 0 e $(4p-1)$.

Para obter os valores dos λ's em função dos dados experimentais, devemos resolver o sistema linear composto pelas Eqs. (7.125), (7.131), juntamente com a condição de

normalização:

$$\begin{aligned}
\frac{\delta_x}{4p-1} &= \lambda_2 + \lambda_4, \\
\frac{\delta_y}{4p-1} &= \lambda_2 + \lambda_3, \\
\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 &= 1.
\end{aligned}$$

Apesar de termos somente três equações e quatro incógnitas (λ_1, λ_2, λ_3 e λ_4), podemos utilizar o mesmo esquema realizado no estudo do protocolo BB84, Sec. 4, e definir os λ's como

$$\begin{aligned}
\lambda_1 &= \left(1 - \frac{\delta_x}{4p-1}\right)(1-\tilde{v}), \\
\lambda_2 &= \frac{\delta_x}{4p-1}(1-\tilde{u}), \\
\lambda_3 &= \left(1 - \frac{\delta_x}{4p-1}\right)\tilde{v}, \\
\lambda_4 &= \frac{\delta_x}{4p-1}\tilde{u},
\end{aligned} \tag{7.132}$$

com $\tilde{u}, \tilde{v}$ pertencendo ao intervalo $[0,1]$. Substituindo os λ's dados pela Eq. (7.132) na Eq. (7.131) obtemos

$$\delta_y = (4p-1)\left[\frac{\delta_x}{4p-1}(1-\tilde{u}) + \left(1 - \frac{\delta_x}{4p-1}\right)\tilde{v}\right]. \tag{7.133}$$

Isolando $\tilde{v}$,

$$\tilde{v} = \frac{\delta_y - \delta_x(1-\tilde{u})}{4p-1-\delta_x}. \tag{7.134}$$

Inserindo a Eq. (7.134) em (7.132), podemos expressar os autovalores por meio de um único parâmetro livre:

$$\begin{aligned}
\lambda_1 &= 1 - \frac{\tilde{u}\delta_x + \delta_y}{4p-1}, \\
\lambda_2 &= \frac{\delta_x}{4p-1}(1-\tilde{u}), \\
\lambda_3 &= \frac{\delta_y - (1-\tilde{u})\delta_x}{4p-1}, \\
\lambda_4 &= \frac{\delta_x}{4p-1}(\tilde{u}).
\end{aligned} \tag{7.135}$$

Para calcular a fração da chave secreta é imprescindível realizar uma maximização da quantidade de Holevo, o que nos leva a um *lower bound* para r. Olhando com cuidado para

a fórmula da segurança (7.113), vemos que é suficiente maximizar a entropia quântica de Eva, representada pela Eq. (7.112), pois os outros termos, ao substituirmos os λ's pela Eq. (7.135), não dependerão de $\tilde{u}$. Portanto, inserindo a Eq. (7.135) na entropia quântica de Eva, Eq. (7.107), temos

$$s(\varrho^E) = \theta\left(\frac{\delta_x}{4p-1}(1-\tilde{u})\right) + \theta\left(\frac{\delta_x}{4p-1}(\tilde{u})\right) + \theta\left(1 - \frac{\tilde{u}\delta_x + \delta_y}{4p-1}\right) + \theta\left(\frac{\delta_y - (1-\tilde{u})\delta_x}{4p-1}\right), \tag{7.136}$$

com $\theta(x) = x\log x$. Resolvendo $\frac{\mathrm{d}S(\varrho^E)}{\mathrm{d}\tilde{u}} = 0$ encontramos,

$$\log\left(1 - \frac{\delta_y + \tilde{u}\delta_x}{4p-1}\right) - \log\left(\frac{\delta_y - \delta_x(1-\tilde{u})}{4p-1}\right) - \log\left(\frac{\delta_x\tilde{u}}{4p-1}\right) + \log\left(\frac{\delta_x(1-\tilde{u})}{4p-1}\right) = 0. \tag{7.137}$$

Para $\delta_x \neq 0$ e $p \neq 1/4$, a Eq. (7.137) é nula somente se

$$\tilde{u} = 1 - \frac{\delta_y}{4p-1}. \tag{7.138}$$

Tomando a derivada segunda da Eq. (7.136) e substituindo (7.138) encontramos

$$-\frac{(1-4p)^2\delta_x}{\delta_y \log(2)(4p-1-\delta_x)(4p-1-\delta_y)}. \tag{7.139}$$

A expressão acima é negativo devida a δ_x e δ_y serem menores que o valor positivo $4p-1$, garantindo assim que $\tilde{u}$ é ponto de máximo.

Substituindo a Eq. (7.138) na Eq. (7.135), descobrimos que os λ's em função dos desvios δ_x e δ_y são,

$$\begin{aligned}
\lambda_1 &= \frac{(4p-1-\delta_x)(4p-1-\delta_y)}{(4p-1)^2}, \\
\lambda_2 &= \frac{\delta_x\delta_y}{(4p-1)^2}, \\
\lambda_3 &= \frac{(4p-1-\delta_x)\delta_y}{(4p-1)^2}, \\
\lambda_4 &= \frac{\delta_x(4p-1-\delta_y)}{(4p-1)^2}.
\end{aligned} \tag{7.140}$$

Nós temos também que os desvios relativos dados por

$$\Delta_i \equiv \frac{p^0_{A,B}(i_0,i_0) + p^0_{A,B}(i_1,i_1) - p_{A,B}(i_0,i_0) - p_{A,B}(i_1,i_1))}{p^0 A,B(i_0,i_0) + p^0_{A,B}(i_1,i_1)}, \quad i = x,y, \tag{7.141}$$

podem ser escritos como $\Delta_i = \delta_i/(p^0 A, B(i_0, i_0) + p^0_{A,B}(i_1, i_1))$. Consequentemente,

$$\Delta_x = \frac{\delta_x}{2p}, \tag{7.142}$$

e

$$\Delta_y = \frac{\delta_y}{2p}, \tag{7.143}$$

após usarmos as Eqs. (7.119) e (7.126), respectivamente.

Substituindo os desvios δ's pelos desvios relativos Δ's, Eqs (7.142) e (7.143), na Eq. (7.140) resulta,

$$\begin{aligned}
\lambda_1 &= \frac{[2p(2-\Delta_x)-1][2p(2-\Delta_y)-1]}{(4p-1)^2}, \\
\lambda_2 &= \frac{4p^2\Delta_x\Delta_y}{(4p-1)^2}, \\
\lambda_3 &= \frac{2p\Delta_y[2p(2-\Delta_x)-1]}{(4p-1)^2}, \\
\lambda_4 &= \frac{2p\Delta_x[2p(2-\Delta_y)-1]}{(4p-1)^2}.
\end{aligned} \tag{7.144}$$

Por fim, usando a Eq. (7.144) na fração da chave secreta (7.113) obtemos

$$\begin{aligned}
r = 1 - h[2p(1-\Delta_x)] - h\left(1 - \frac{2p\Delta_x}{4p-1}\right) - h\left(1 - \frac{2p\Delta_x}{4p-1}\right) \\
+ h\left[\frac{1}{2} + \frac{1}{2}\sqrt{1 + 8p\left[(1-4p)\Delta_x\left(1 + \frac{2p\Delta_x}{1-4p}\right) + (1-2p)\frac{8p\Delta_y}{1-4p}\left(1 + \frac{2p\Delta_y}{1-4p}\right)\right]}\right],
\end{aligned} \tag{7.145}$$

onde a função h é a entropia binária (2.2).

7.2.5 Considerações finais sobre o protocolo GR10

Plotando a Eq. (7.145) em função dos desvios relativos Δ_x e Δ_y com o valor de p fixo, Fig. 7.4, podemos perceber que quanto maior o valor do p escolhido maior é a fração da chave secreta que obtemos. Vale ressaltar que a forma funcional de p depende do *ensemble* escolhido bem como dos valores de n_1 e n_2 [Eqs. (7.54), (7.91), (7.89) ou $\frac{1}{2}$ (protocolo GR10 original)]. A Fig. 7.4 também mostra que podemos ter segurança mesmo com um

desvio relativo em uma base maior que 30%, desde de que a outra base possua desvio relativo muito pequeno.

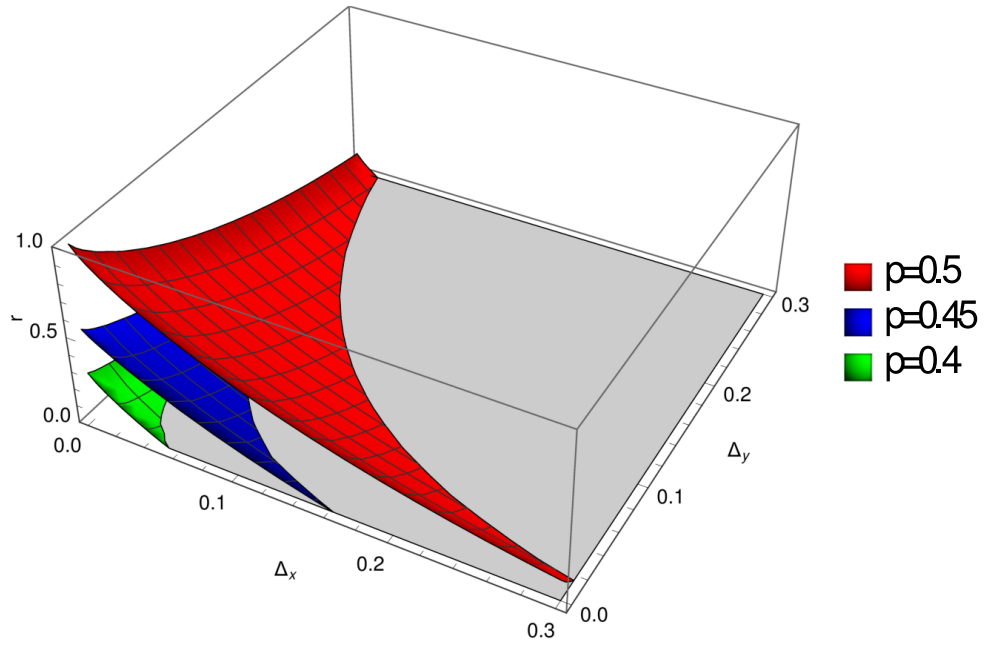

Figura 7.4: Limite inferior de r, a fração da chave secreta para o protocolo GR10 utilizando estados não ortogonais (estados na base x e na base y para codificar 0 e 1). A fração da chave secreta é dada pela Eq. (7.145) em função de Δ_x e Δ_y, o desvio relativo do valor esperado da probabilidade de Alice e Bob obter o mesmo valor do bit sem a presença de Eva. No gráfico temos três superfícies, sendo respectivamente de cima para baixo, $p = 0.5$, $p = 0.45$ e $p = 0.4$.

Por outro lado, podemos considerar o cenário de desvios simétricos, $\Delta_x = \Delta_y = \Delta$, e ver o comportamento da Eq. (7.145) em função dos emaranhamentos escolhidos (valores de n_1 e n_2). Este cenário é mostrado na Fig. 7.5. Nela, escolhemos o *ensemble* em que a condição de *mathcing* é satisfeita, isto é, p_M, veja Eq. (7.89). Na Fig. 7.5 podemos ver que quanto maior o desvio relativo, mais próximos de 1 n_1 e n_2 devem se encontrar para termos uma chave segura.. Ou seja, para 11% temos segurança somente se $p \approx 1/2$.

Na Fig. 7.6 comparamos a fração da chave secreta do protocolo GR10 com estados não ortogonais, Eq. (7.145), com o protocolo GR10 modificado, Eq. (7.37), no regime de desvios simétricos. A partir da Fig. 7.6 podemos afirmar que para $p < 1/2$ o protocolo GR10 com estados não ortogonais apresenta maior taxa de segurança que o modificado. Contudo, quando temos $p = 1/2$ a fração da chave secreta é a mesma. Vale ressaltar que obtemos $p = 1/2$ quando temos $n_1 = n_2 = 1$ ou também quando utilizamos a execução do

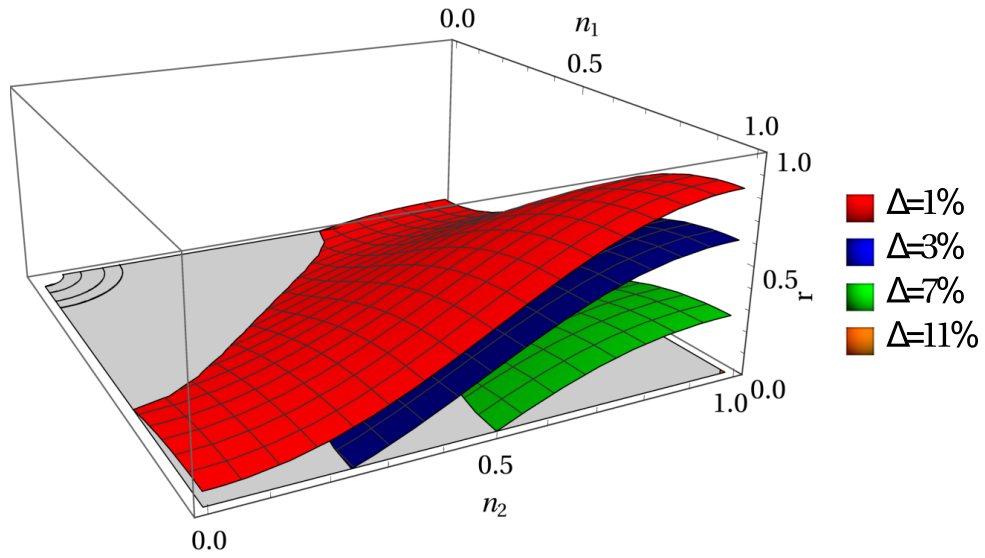

Figura 7.5: Fração da chave secreta r do protocolo GR10 com estados não ortogonais, Eq. (7.145), utilizando p_M, Eq. (7.89), e $\Delta_x = \Delta_y = \Delta$. A superfície vermelha mostra que com um desvio relativo $\Delta = 1\%$ a segurança ocorrerá se o protocolo for realizado com um dos n_i's maior que 0.7. Já na superfície azul, desvio relativo $\Delta = 3\%$, é possível ter segurança desde de que n_1 e n_2 sejam maiores que 0.5. A superfície verde mostra que para n_1 e n_2 maiores que 0.7 é possível ter segurança mesmo com um desvio relativo $\Delta = 7\%$. E a última superfície, a marrom, mostra que só é possível ter fração da chave secreta positiva para um desvio relativo $\Delta = 11\%$ desde que o protocolo tenha sido realizado considerando $n_1 = n_2 = 1$.

protocolo GR10 originalmente proposto.

A diferença prática entre os protocolos se dá no tamanho da chave efetiva $K = rR$ disponível ao término da execução dos protocolos. Aqui r é a fração da chave secreta e R o número de bits da chave crua. Na execução do GR10 original, o tamanho da chave crua é dado pela Eq. (3.15), isto é, $R = \sum_{i=1}^{2}(n_i/1 + n_i^2)^2(N/2)$, com N sendo a quantidade de *qubits* teletransportados. Quando temos o protocolo GR10 modificado $R = N$ pois consideramos todos os casos. Em contrapartida, quando temos os *ensembles* da condição de *matching* e quando Bob usa somente um canal, $R = N/2$. Esses valores são para o GR10 ortogonal, isto é, somente usando a base x. Se considerarmos o GR10 com estados não ortogonais os valores de R são reduzidos pela metade pois a probabilidade de Bob e Alice utilizarem a mesma base é de 50%. A Fig. 7.7 representa a razão do tamanho da chave em relação ao número de *qubits* teletransportados para as diversas versões do protocolo GR10 que fazem uso apenas de estados ortogonais para codificar os bits. Perceba que, mesmo que a fração da chave secreta r para certas versões do GR10 sejam menor do que a do

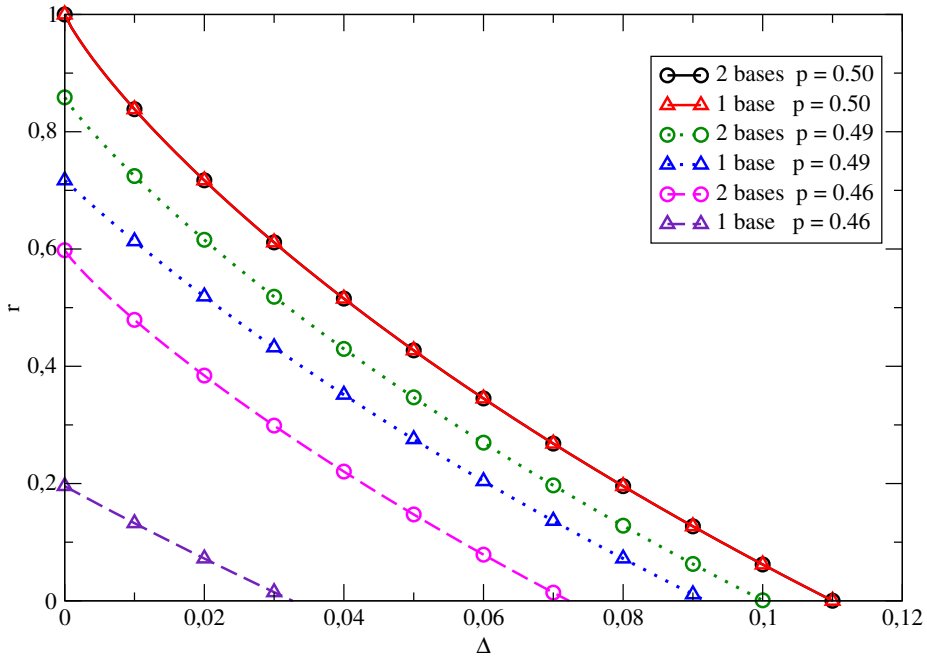

Figura 7.6: Limite inferior de r, a fração da chave secreta, para o protocolo GR10 utilizando a base x e base y como dado pela Eq. (7.145) e $\Delta_x = \Delta_y = \Delta$ (curvas com círculos), e para o protocolo GR10 modificado dado pela Eq. (7.37) em função de $\Delta_x = \Delta$ (curvas com triângulos). Para a linha contínua supomos $p = 0.5$, a pontilhada $p = 0.49$, enquanto para a tracejada temos $p = 0.46$. A partir do gráfico podemos ver que utilizar uma base extra aumenta o limite máximo da taxa de erro abaixo do qual temos transmissão segura ($r > 0$). Quando temos $p = 0.5$ a fração da chave secreta é equivalente para ambos os casos.

protocolo original, há um ganho em relação ao tamanho efetivo da chave K/N.

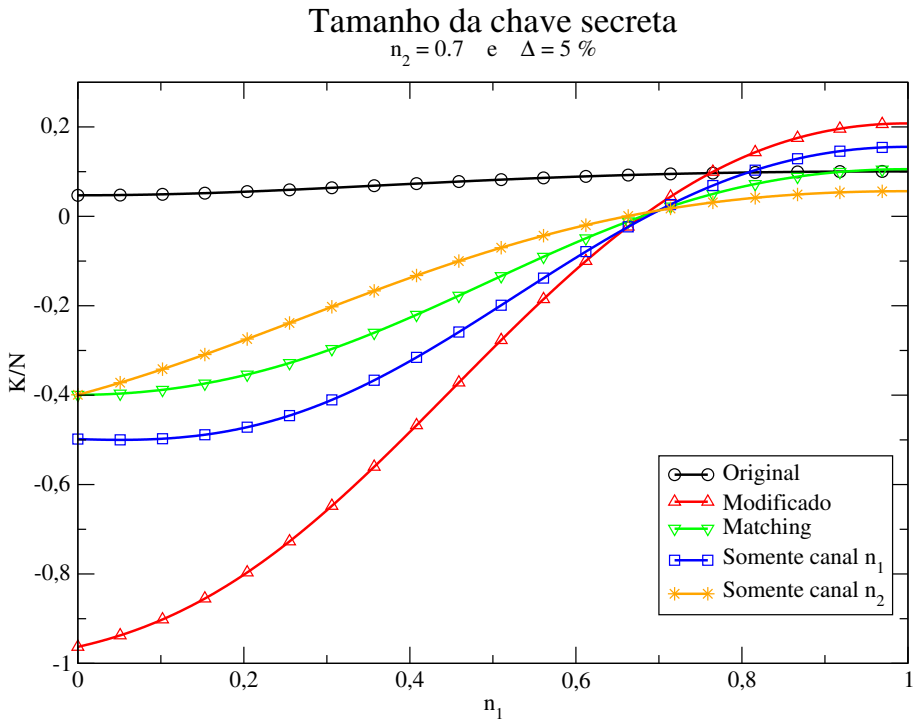

Figura 7.7: Razão $K/N = rR/N$ para as diversas versões do protocolo GR10 que usam estados ortogonais. Supondo $n_2 = 0.7$ e $\Delta = 5\%$ fixos. A curva preta com círculos refere-se ao protocolo GR10 original com r dado pela Eq. (7.37) e R pela Eq (3.15). As demais curvas são variações do protocolo com r sendo dado pela Eq. (7.84). A curva vermelha com triângulos para cima é a fração da chave secreta com probabilidade p dado pela Eq. (7.54), e $R/N = 1$. A curva verde com triângulos invertidos considera o *ensemble* que satisfaz a condição de *matching* p_M, a Eq. (7.89), e $R/N = 1/2$. A curva azul com quadrados considera que o canal n_2 foi descartado e com isso $p = p_{P_1}$, Eq. (7.91), e $R/N = 1/2$. Na curva laranja com estrela o canal n_1 foi descartado, assim a probabilidade é dada por p_{P_2}, Eq. (7.92), e $R/N = 1/2$. Pelo gráfico podemos perceber que apesar do protocolo GR10 original e do GR10 modificado com probabilidade p_M possuírem maior fração da chave secreta r que o GR10 modificado com p dado pela Eq. (7.54) (triângulos), este último apresenta maior tamanho efetivo de chave segura para altos valores de n_1. Isto é devido a ele não ter fase de descartes durante sua execução.

Capítulo 8

A segurança sob a ótica do ruído para o protocolo BB84

Nos capítulos anteriores, calculamos a fração da chave secreta r considerando de forma genérica os erros que ocorrem durante o envio da chave. Isto é, não foi levado em consideração o tipo de ruído (interferência) que a transmissão da chave secreta sofreu. Nas análises anteriores consideramos o ruído que leva ao pior cenário possível para Alice e Bob (pólos envolvidos na comunicação segura). Por outro lado, é importante averiguar como um determinado ruído específico influência a segurança da distribuição da chave criptográfica quântica.

8.1 Modelando o ruído

A interação do *qubit* transmitido com o ambiente ruidoso é descrita por um mapa $\mathcal{E}$. Assim, o sistema ρ que sofreu a ação do ruído se transforma no estado $\mathcal{E}(\rho)$ [34]. Geralmente o mapa $\mathcal{E}$ não é descrito por transformações unitárias. No entanto, aumentando suficientemente a dimensão do espaço de Hilbert do ambiente, podemos escrever qualquer interação por uma transformação unitária [34].

Supondo que o estado que descreve o *qubit* mais o ambiente seja dado por $\rho \otimes \rho_{amb}$ e modelando a ação do ruído por transformações unitárias temos [34]:

$$\mathcal{E}(\rho) = \mathrm{tr}_{amb}\left\{U\left(\rho \otimes \rho_{amb}\right)U^{\dagger}\right\}. \tag{8.1}$$

Supondo que $\rho_{amb} = |\epsilon_0\rangle\langle\epsilon_0|$, obtemos

$$\begin{aligned} \mathcal{E}(\rho) &= \mathrm{tr}_{amb}\left\{U\left(\rho \otimes |\epsilon_0\rangle_{amb}\langle\epsilon_0|\right)U^\dagger\right\}, & (8.2)\\ &= \sum_k \langle\epsilon_k|\left[U\left(\rho \otimes |\epsilon_0\rangle_{amb}\langle\epsilon_0|\right)U^\dagger\right]|\epsilon_k\rangle. & (8.3)\end{aligned}$$

Definindo a operação $\langle\epsilon_k| U |\epsilon_0\rangle = E_k$, a Eq. (8.3) torna-se

$$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger. \tag{8.4}$$

Perceba que como o $\mathrm{tr}\{\mathcal{E}(\rho)\} = 1$, já que $\mathcal{E}(\rho)$ é um operador densidade, temos que $\sum_k E_k E_k^\dagger = \mathbb{1}$.

Os operadores E_k são conhecidos por operadores de Kraus. Uma breve descrição dos ruídos mais comuns [34] e seus respectivos operadores de Kraus são dados abaixo utilizando a notação de [26].

Bit flip: O ruído conhecido por *bit flip* descreve o ruído que faz o *qubit* $|0\rangle$ tornar-se $|1\rangle$ ou o *qubit* $|1\rangle$ virar $|0\rangle$. Se a probabilidade de isso ocorrer é q, os operadores de Kraus deste ruído são

$$\begin{aligned} E_{b_0} &= \sqrt{1-q}\,\mathbb{1}, & (8.5)\\ E_{b_1} &= \sqrt{q}\,\sigma_x. & (8.6)\end{aligned}$$

Phase flip: O ruído *phase flip* altera a fase do *qubit* $|1\rangle$ para $-|1\rangle$ com probabilidade q. Seus operadores de Kraus são descritos por,

$$\begin{aligned} E_{p_0} &= \sqrt{1-q}\,\mathbb{1}, & (8.7)\\ E_{p_1} &= \sqrt{q}\,\sigma_z. & (8.8)\end{aligned}$$

Depolarizing noise: Este ruído transforma com probabilidade q o *qubit* em um estado

misto sem polarização definida. Seus quatro operadores de Kraus são

$$E_{d_0} = \sqrt{1-\frac{3q}{4}}\,\mathbb{1}, \tag{8.9}$$

$$E_{d_1} = \sqrt{\frac{q}{4}}\,\sigma_x, \tag{8.10}$$

$$E_{d_2} = \sqrt{\frac{q}{4}}\,\sigma_y, \tag{8.11}$$

$$E_{d_3} = \sqrt{\frac{q}{4}}\,\sigma_z. \tag{8.12}$$

Amplitude damping: O último tipo de ruído que estudaremos modela o decaimento do *qubit* $|1\rangle$ para o estado $|0\rangle$ como probabilidade q disso ocorrer. Seus operadores de Kraus são

$$E_{a_0} = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-q} \end{bmatrix}, \tag{8.13}$$

$$E_{a_1} = \begin{bmatrix} 0 & \sqrt{q} \\ 0 & 0 \end{bmatrix}. \tag{8.14}$$

8.2 O protocolo BB84 sob ação dos ruídos

Na Sec. 4 calculamos a fração da chave secreta para o protocolo BB84, Eq. (4.25),

$$r = 1 + \min_{\text{Eve}} \left\{ \sum_{j=1}^{4} \lambda_j \log \lambda_j \right\}. \tag{8.15}$$

Este resultado foi obtido a partir da representação baseada em emaranhamento

$$|\phi_1\rangle = \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle \right) \tag{8.16}$$

que, após a interferência de Eva, resultou no seguinte operador densidade para Alice e Bob,

$$\rho_f^{AB} = \begin{bmatrix} \frac{\lambda_1+\lambda_2}{2} & 0 & 0 & \frac{\lambda_1-\lambda_2}{2} \\ 0 & \frac{\lambda_3+\lambda_4}{2} & \frac{\lambda_3-\lambda_4}{2} & 0 \\ 0 & \frac{\lambda_3-\lambda_4}{2} & \frac{\lambda_3+\lambda_4}{2} & 0 \\ \frac{\lambda_1-\lambda_2}{2} & 0 & 0 & \frac{\lambda_1+\lambda_2}{2} \end{bmatrix}. \tag{8.17}$$

O operador ρ_f^{AB} foi escrito na base $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. A matriz dada pela Eq. (8.17) foi obtida da decomposição de Schmidt (Eq. (4.6)),

$$|\Psi\rangle_{ABE} = \sum_{j=1}^{4} \sqrt{\lambda_j} |\Phi_j\rangle_{AB} |\epsilon_j\rangle_E.$$

Comparando o estado dado pela Eq. (8.17) com o estado de Alice e Bob este após ser submetido a um determinado tipo de ruído conforme apresentado na seção anterior, podemos obter os λ's em função dos parâmetros que descrevem o ruído. Nos casos em que a comparação direta não é possível, consideramos que Eva possui uma purificação do estado obtida após o ruído e calculamos novamente a taxa de segurança considerando esse estado purificado de Alice, Bob e Eva.

O estado inicial de Alice e Bob é o estado de Bell $|\phi_1\rangle$, Eq. (4.1), portanto o operador densidade é

$$\rho^{AB} = |\phi_1\rangle_{AB} \langle\phi_1| . \tag{8.18}$$

Após a atuação do ruído, Alice e Bob compartilharão o estado

$$\rho_j^{AB} = \sum_{k=0}^{n} (\mathbb{1}_A \otimes E_{j_k B}) \rho^{AB} (\mathbb{1} \otimes E_{j_k B})^\dagger, \tag{8.19}$$

com j sendo os tipos de ruídos possíveis atuando no *qubit* de Bob. [1]

Considerando que o ruído presente no envio do *qubit* de Alice a Bob seja o *phase flip*, as Eqs. (8.7), (8.8) e (8.19) dão

$$\rho_p^{AB} = \begin{bmatrix} \frac{1}{2} & 0 & 0 & \frac{1}{2} - q \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \frac{1}{2} - q & 0 & 0 & \frac{1}{2} \end{bmatrix}. \tag{8.20}$$

Comparando o operador densidade (8.17) com a matriz (8.20) encontramos que os valores dos λ's são

$$\lambda_1 = 1 - q, \qquad \lambda_2 = q, \qquad \lambda_3 = 0, \qquad \lambda_4 = 0. \tag{8.21}$$

[1] Consideramos aqui que o *qubit* que sofre o ruído é o que percorre o canal de comunicação. Portanto, o ruído atua somente no *qubit* de Bob pois este *qubit* é que viaja de Alice a Bob enquanto o *qubit* de Alice permanece sempre com ela.

Substituindo esses valores de λ na fração da chave secreta dada pela Eq. (8.15) encontramos para o *phase flip*,

$$r_p = 1 - h(q), \tag{8.22}$$

com h sendo a entropia binária (2.2).

Supondo, agora, que os operadores E_{j_k} da Eq. (8.19) são dados pelas Eqs. (8.5) e (8.6), ou seja, temos o ruído *bit flip*, o estado de Bob vale

$$\rho_b^{AB} = \begin{bmatrix} \frac{1-q}{2} & 0 & 0 & \frac{1-q}{2} \\ 0 & \frac{q}{2} & \frac{q}{2} & 0 \\ 0 & \frac{q}{2} & \frac{q}{2} & 0 \\ \frac{1-q}{2} & 0 & 0 & \frac{1-q}{2} \end{bmatrix}. \tag{8.23}$$

Comparando com a Eq. (8.17) obtemos

$$\lambda_1 = 1 - q, \qquad \lambda_2 = 0, \qquad \lambda_3 = q, \qquad \lambda_4 = 0 \tag{8.24}$$

e usando a Eq. (8.15) encontramos

$$r_b = 1 - h(q). \tag{8.25}$$

Perceba que a fração da chave secreta para o ruído *bit flip*, Eq. (8.25), é igual a obtida para o ruído *phase flip*, Eq. (8.22).

No caso do *depolarizing noise* temos os quatro operadores de Kraus dados pelas Eqs. (8.9)-(8.12). Aplicando esses operadores na Eq. (8.19) resulta

$$\rho_d^{AB} = \begin{bmatrix} \frac{2-q}{4} & 0 & 0 & \frac{1-q}{2} \\ 0 & \frac{q}{4} & 0 & 0 \\ 0 & 0 & \frac{q}{4} & 0 \\ \frac{1-q}{2} & 0 & 0 & \frac{2-q}{4} \end{bmatrix}. \tag{8.26}$$

Comparando a Eq. (8.26) com a Eq. (8.17) encontramos que

$$\lambda_1 = 1 - \frac{3q}{4}, \qquad \lambda_2 = \frac{q}{4}, \qquad \lambda_3 = \frac{q}{4}, \qquad \lambda_4 = \frac{q}{4} \tag{8.27}$$

e consequentemente

$$r_d = 1 + \left(1 - \frac{3q}{4}\right) \log\left(1 - \frac{3q}{4}\right) + 3\left(\frac{q}{4}\right) \log\left(\frac{q}{4}\right). \tag{8.28}$$

A fração da chave secreta acima é a mesma encontrada quando temos taxas de erros simétricos para o BB84 seis-estados, Eq. (5.22), ou para o protocolo BB84 original utilizando a nova decomposição de Schmidt, Eq. (6.33). Em ambos os casos temos que $\varepsilon_x = \varepsilon_y = \varepsilon_z = q/2$ (lembre-se que ε_y não existe no BB84 original).

Para o último tipo de ruído, o *amplitude damping*, não é possível obter uma comparação direta com o operador densidade (8.17). Para este ruído, usando E_{j_k} dado pelas Eq. (8.13) e (8.14) temos

$$\rho_a^{AB} = \begin{bmatrix} \frac{1}{2} & 0 & 0 & \frac{\sqrt{1-q}}{2} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{q}{2} & 0 \\ \frac{\sqrt{1-q}}{2} & 0 & 0 & \frac{1-q}{2} \end{bmatrix}. \tag{8.29}$$

Comparando com a Eq. (8.17) vemos que $(\lambda_3 + \lambda_4)/2 = 0 = q/2$. Isto é, a identificação só é válida quando temos a probabilidade do ruído ocorrer sendo zero.

Para obtermos a fração da chave secreta neste caso, devemos refazer a análise de segurança desde o início, usando uma decomposição de Schmidt compatível com o tipo de ruído que estamos lidando. Para isso, consideramos que o ruído é devido a presença de Eva. Sendo assim, consideramos que Eva possui uma purificação do operador densidade (8.29).

Os autovetores da Eq. (8.29) são

$$|w_1\rangle = \frac{1}{\sqrt{2-q}} \left(-\sqrt{1-q}\,|00\rangle + |11\rangle\right), \tag{8.30}$$

$$|w_2\rangle = |01\rangle, \tag{8.31}$$

$$|w_3\rangle = \frac{1}{\sqrt{2-q}} \left(1\,|00\rangle + \sqrt{1-q}\,|11\rangle\right), \tag{8.32}$$

$$|w_4\rangle = |10\rangle. \tag{8.33}$$

Os autovalores associados a estes autovetores são, respectivamente,

$$\{0, 0, 1 - q/2, q/2\}. \tag{8.34}$$

Como os autovalores associados aos autoestados $|w_1\rangle$ e $|w_2\rangle$ são nulos, a purificação é

$$|\psi\rangle_{ABE} = \sqrt{1-\frac{q}{2}}\,|w_3\rangle_{AB}\,|\epsilon_3\rangle_E + \sqrt{\frac{q}{2}}\,|w_4\rangle_{AB}\,|\epsilon_4\rangle_E\,. \tag{8.35}$$

Perceba que tomando o traço sobre Eva no operador densidade $|\psi\rangle_{ABE}\langle\psi|$ recuperamos, como esperado, a Eq. (8.29).

Precisamos, agora, calcular a informação mútua $I(A:B)$ e quantidade de Holevo $\chi(A:\rho^E)$.

Utilizando o operador densidade (8.29), temos que

$$p_B(0) = \frac{1+q}{2}, \tag{8.36}$$

$$p_B(1) = \frac{1-q}{2}, \tag{8.37}$$

$$p_A(0) = p_A(1) = \frac{1}{2}. \tag{8.38}$$

Com isso a Eq. (2.6) dá

$$H(B) = h\left(\frac{1+q}{2}\right), \tag{8.39}$$

com $h(x) = -(1-x)\log(1-x) - x\log(x)$.

As probabilidades condicionais de Bob são

$$p_{B|A}(0|0) = 1, \tag{8.40}$$

$$p_{B|A}(0|0) = 0, \tag{8.41}$$

$$p_{B|A}(1|1) = 1-q, \tag{8.42}$$

$$p_{B|A}(0|1) = q, \tag{8.43}$$

$$\tag{8.44}$$

resultando na entropia condicional (veja a Eq. (2.4)) abaixo

$$H(B|A) = \frac{1}{2}h(1-q). \tag{8.45}$$

Por fim, juntando as Eq. (8.39) e (8.45) temos a informação mútua, Eq. (2.6),

$$I(A:B) = h\left(\frac{1+q}{2}\right) - \frac{1}{2}h(1-q). \tag{8.46}$$

No cálculo da quantidade de Holevo entre Alice e Eva, precisamos da entropia quântica de Eva,

$$S(\rho^E) = h(q/2). \tag{8.47}$$

A expressão acima é obtida por meio dos autovalores de ρ_a^{AB}, representados na Eq. (8.34), e por meio do lema 2.2.

Pelo postulado da medida, se Alice enviou o bit 0, o estado final de Alice e Eva é

$$\rho_{a_0}^{AE} = |0\rangle_A \langle 0| \otimes |\epsilon_3\rangle_E \langle \epsilon_3| . \tag{8.48}$$

Se enviou o bit 1 temos

$$\rho_{a_1}^{AE} = |1\rangle_A \langle 1| \otimes [(1-q) |\epsilon_3\rangle_E \langle \epsilon_3| + q |\epsilon_4\rangle_E \langle \epsilon_4|] . \tag{8.49}$$

Tomando o traço sobre o sistema de Alice, e pela definição da entropia quântica, temos que

$$S(\rho_0^E) = 0, \tag{8.50}$$

e

$$S(\rho_1^E) = h(q). \tag{8.51}$$

A partir das Eqs. (8.50), (8.51) e (8.38) temos

$$\sum_{a=0}^{1} p_A(a) S(\rho_a^E) = \frac{h(q)}{2}. \tag{8.52}$$

Juntando as Eqs. (8.47) e (8.52), a Eq. (2.105) dá

$$\chi(A : \rho^E) = h\left(\frac{q}{2}\right) - \frac{h(q)}{2}. \tag{8.53}$$

Finalmente, substituindo as Eqs. (8.46) e (8.53) na Eq. (2.122) obtemos a taxa da chave secreta para a atuação do ruído *amplitude damping*,

$$r_a = h\left(\frac{1+q}{2}\right) - h\left(\frac{q}{2}\right), \tag{8.54}$$

com h sendo a Eq. (2.2).

Na Fig. 8.1 temos a taxa de segurança para os quatro tipos de ruído em função da probabilidade p do ruído atuar. Nela podemos ver que o ruído *bit flip*, Eq. (8.25), e *phase*

flip, Eq. (8.22), possuem a mesma fração da chave secreta. Além disso, para esses dois tipos de ruído sempre temos segurança pois $r \geq 0$ para todo q, com o mínimo $r = 0$ ocorrendo para $p = 1/2$. Em contrapartida, quando a transmissão é suscetível ao ruído *depolarizing*, Eq. (8.28), e ao *amplitude damping*, Eq. (8.54), temos que a transmissão não é mais segura para $q \lesssim 25.2\%$ e $q < 50\%$ respectivamente.

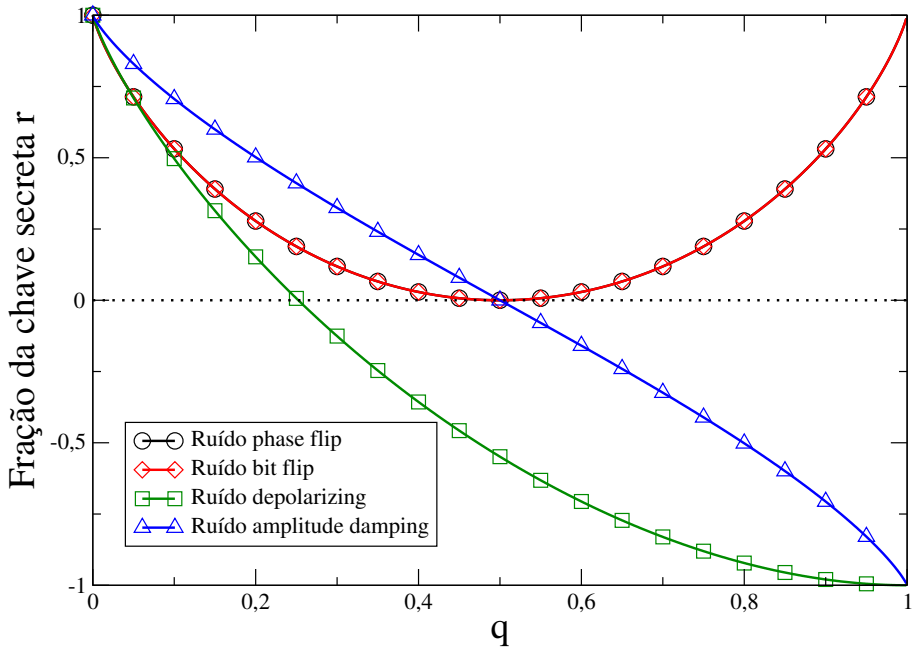

Figura 8.1: Fração da chave secreta para uma transmissão com ruídos *phase flip*, *bit flip*, *depolarizing* e *amplitude damping*, Eqs. (8.22), (8.25), (8.28) e (8.54), respectivamente. O gráfico está em função da probabilidade q do ruído ocorrer e nele podemos perceber que o ruído *depolarizing* é o mais agressivo dos ruídos. Para o *depolarizing noise* a partir de $q \approx 0.25$ a transmissão torna-se insegura.

Capítulo 9

Conclusão

A criptografia quântica, um ramo da teoria de informação, ganhou notoriedade após se perceber que os protocolos clássicos de criptografia teriam seus dias contados com o advento da computação quântica. De fato, a existência de um computador quântico culminaria em poder de processamento capaz de "quebrar" os protocolos de criptografia atuais por força bruta (testando todas as possibilidades de chaves criptográficas em frações de segundo). No entanto, a engenhosa proposição de Bennet e Brassard em 1984 [4] proporcionou uma nova esperança para comunicações seguras mesmo com o advento do computador quântico.

O protocolo BB84, pioneiro e amplamente utilizado atualmente, teve sua segurança rigorosamente analisada e testada. Originalmente como foi proposto, foi encontrado o limiar de aproximadamente 11% no erro máximo tolerado para que o protocolo fosse considerado seguro (considerando que o erro da base x seja o mesmo da base z) [8]. Por esse protocolo ter sido bem aceito e sua segurança inquestionável, esmiuçamos as sutilezas técnicas de sua análise de segurança para podermos aplicá-las no protocolo GR10. Ao tomarmos este caminho, descobrimos que a escolha da base que descreve o estado quântico de Alice, Bob e Eva na decomposição de Schmidt desempenha um papel central na análise de segurança. Explorando essa não unicidade, encontramos uma nova representação da purificação que resultou em um máximo de erro tolerado maior (12% aproximadamente). Mesmo resultado obtido para a modificação do BB84 conhecida como BB84 seis-estados. Ou seja, aumentar uma nova base no BB84 não melhora a fração da secreta da chave. Mais ainda, ao usarmos uma base extra no BB84 diminuímos a fração da chave efetiva K, que é proporcional ao tamanho da chave crua R. Isto é, R é cerca de $N/2$ para o protocolo BB84 original e $N/3$ para o protocolo BB84 seis estados. Esse incremento na taxa de erro máximo tolerado ocorreu devido ao cálculo original ser uma minimização da fração da chave secreta, isto é,

na Ref. [8] os autores obtiveram um *lower bound* para a chave secreta. No nosso caso, ao utilizarmos uma nova purificação encontramos vínculos extras que nos permitiram calcular o valor exato da taxa da chave secreta.

Posteriormente, apresentamos uma prova de segurança rigorosa para o protocolo de distribuição de chaves quântica GR10, cuja operação é baseada no protocolo de teletransporte probabilístico e no uso de apenas estados quânticos ortogonais para codificar os bits da chave secreta [18]. Para ser mais específico, realizamos a análise de segurança assintótica do protocolo GR10 contra todos os tipos de ataques individuais e coletivos, determinando as taxas de erro abaixo das quais garantimos uma operação segura do esquema de distribuição de chaves. Nesta análise, provamos que o protocolo GR10 originalmente proposto é seguro contra ataques coletivos. Além disso, aplicando os resultados das Refs. [44–47], argumentamos que a presente análise de segurança é facilmente estendida a ataques coerentes, levando à segurança incondicional do protocolo GR10. Vimos, também, que o limiar de erro tolerável para o protocolo GR10 ser considerado seguro é o mesmo do protocolo BB84 original. Além disso, vimos que a taxa de segurança r não depende do grau de emaranhamento escolhido por Alice e Bob para o teletransporte da chave. No entanto, a chave efetiva $K = rR$ depende, disso, pois quanto menor o emaranhamento menor o tamanho da chave bruta R.

Após constatarmos que o protocolo GR10 é seguro, propomos alterações em sua execução. Essas alterações consistiram em alterar o *ensemble* utilizado para gerar as estatísticas para estimar a segurança do protocolo. Conforme originalmente proposto, o protocolo GR10 considera somente os resultados da medida generalizada de Bell $|\Phi_2\rangle$ e $|\Phi_3\rangle$ com Bob e Alice utilizando o mesmo emaranhamento no canal e na medida ($n = k$). As modificações do protocolo GR10 apresentaram fração da chave secreta r inferior ao original, especialmente quando o grau de emaranhamento compartilhado entre Alice e Bob é pequeno. As diversas representações para a decomposição de Schmidt foi o ingrediente principal do nosso estudo, nos permitindo obter regimes de segurança com taxas de erro mais elevadas. Se por um lado as modificações levaram a uma menor fração da chave secreta r, por outro lado aumentaram a taxa da chave $K = rR$ como visto na Fig. 7.7. Consequentemente, o preço a pagar ao se passar do protocolo probabilístico (GR10 original) para o determinístico (GR10 modificado) é uma redução do valor da fração de chave secreta r com consequente aumento da chave bruta R. Além disso, os protocolos GR10 modificados levaram a uma fração da chave secreta dependente dos emaranhamentos n_1 e n_2. A partir deste resultado descobrimos que o protocolo é seguro mesmo quando $n_1 = n_2$.

O protocolo GR10 é seguro mesmo quando apenas um único canal é utilizado na execução do protocolo ($n_1 = n_2$). Isto é possível devido as características intrínsecas do protocolo de teletransporte pois, nem mesmo Eva é capaz de prever o resultado da medida generalizada de Bell feita por Alice.

Analisamos, também, a segurança do protocolo BB84 considerando que os ataques de Evas simulassem os tipos de ruídos mais comuns encontrados durante a transmissão de estados quânticos. Essa empreitada mostrou que o ruído que mais afeta a segurança do protocolo BB84 é o *depolarizing noise*.

Por fim, concluímos que o protocolo GR10 é seguro incondicionalmente e que, ao explorarmos outras representações da decomposição de Schmidt, foi possível estabelecer mais precisamente a segurança incondicional do protocolo BB84. Uma vez que, obtemos um valor exato para r e não apenas um limite inferior. Além disso, gostaríamos de apontar duas possíveis extensões das idéias aqui apresentadas que acreditamos serem dignas de investigação. Primeiro, seria interessante estudar como criar um protocolo semelhante ao GR10 que opera com *qudits* ao invés de *qubits*. A principal busca aqui é obter um cenário em que o uso de *qudits* leve a um aumento da taxa de erro abaixo da qual o protocolo é seguro. A segunda extensão é um pouco mais difícil e consiste em como remodelar o protocolo GR10 para fazê-lo funcionar com sistemas de variáveis contínuas.

Apêndice A

Operações quânticas

Neste apêndice daremos uma breve explanação sobre algumas propriedades associadas às operações quânticas mais utilizadas [33, 34]. E a origem destas propriedades está intimamente ligada com a definição do traço de um operador:

$$\mathrm{tr}\left\{A\right\} \equiv \sum_i \langle i| A |i\rangle . \tag{A.1}$$

Em outras palavras, o traço de A é a soma dos elementos diagonais de A.

Seja Π_j um elemento de medida projetiva tal que $\sum_j \Pi_j = \mathbb{1}$, e $|\psi\rangle$ um estado quântico qualquer. Pelo postulado da medida nós temos que

$$p_J(j) \equiv \langle\psi| \Pi_j |\psi\rangle , \tag{A.2}$$

a probabilidade de obter o resultado j para o estado $|\psi\rangle$. Indo além, podemos supor que o estado $|\psi\rangle$ seja expandido nos estados $|\psi_x\rangle$ com x sendo uma variável aleatória do conjunto X. Usando novamente o postulado da medida temos a probabilidade condicional

$$p_{J|X}(j|x) = \langle\psi_x| \Pi_j |\psi_x\rangle . \tag{A.3}$$

Além disso, após a medida o estado do sistema torna-se

$$\frac{\Pi_j |\psi_x\rangle}{\sqrt{p_{J|X}(j|x)}}. \tag{A.4}$$

Sabendo que a identidade $\mathbb{1}$ pode ser representada em qualquer base, ou seja, $\mathbb{1} =$

$\sum_i |i\rangle\langle i|$, nós temos que

$$\begin{aligned}\langle\psi_x|\,\Pi_j\,|\psi_x\rangle &= \langle\psi_x|\left(\sum_i |i\rangle\langle i|\right)\Pi_j\,|\psi_x\rangle &\text{(A.5)}\\ &= \sum_i \langle\psi_x|i\rangle\langle i|\,\Pi_j\,|\psi_x\rangle &\text{(A.6)}\\ &= \sum_i \langle i|\left(\Pi_j\,|\psi_x\rangle\langle\psi_x|\right)|i\rangle\,. &\text{(A.7)}\end{aligned}$$

A Eq. (A.7) nada mais é que a definição da função traço (A.1) com $A = (\Pi_j\,|\psi_x\rangle\langle\psi_x|)$. Portanto,

$$p_{J|X}(j|x) = \langle\psi_x|\,\Pi_j\,|\psi_x\rangle = \mathrm{tr}\left\{\Pi_j\,|\psi_x\rangle\langle\psi_x|\right\}. \tag{A.8}$$

Utilizando a lei de probabilidades, as Eq. (A.2) e (A.3) são relacionadas por

$$\begin{aligned}p_J(j) &= \sum_x p_X(x)p_{J|X}(j|x) &\text{(A.9)}\\ &= \sum_x p_X(x)\mathrm{tr}\left\{\Pi_j\,|\psi_x\rangle\langle\psi_x|\right\} &\text{(A.10)}\\ &= \mathrm{tr}\left\{\Pi_j\left(\sum_x p_X(x)\,|\psi_x\rangle\langle\psi_x|\right)\right\}. &\text{(A.11)}\end{aligned}$$

A última linha foi obtida valendo-se da definição do traço (A.1). Ou seja, escrevemos o traço como somatória e deslocamos os elementos para dentro dela. Mais ainda, a Eq. (A.11) pode ser reescrita como

$$p_J(j) = \mathrm{tr}\left\{\Pi_j\rho\right\}, \tag{A.12}$$

onde definimos ρ o operador densidade,

$$\rho = \sum_x p_X(x)\,|\psi_x\rangle\langle\psi_x|\,. \tag{A.13}$$

O operador densidade recebeu esse nome por ser o análogo quântico da distribuição de probabilidades. Como a distribuição de densidade é normalizada, o operador densidade satisfaz a seguinte propriedade:

$$\begin{aligned}\mathrm{tr}\left\{\rho\right\} &= \sum_x p_X(x)\sum_i \langle i|\psi_x\rangle\langle\psi_x|i\rangle &\text{(A.14)}\\ &= \sum_x p_X(x)\,\langle\psi_x|\psi_x\rangle &\text{(A.15)}\\ &= 1. &\text{(A.16)}\end{aligned}$$

Por fim, é interessante analisar algumas propriedades do traço.

Propriedade A.1. *O traço de A pode ser representado em qualquer base. Ou seja,*

$$\mathrm{tr}\left\{A\right\} = \sum_i \langle i| A |i\rangle = \sum_x \langle u_x| A |u_x\rangle . \tag{A.17}$$

Demonstração. Definindo $A = \sum_{m,n} a_{m,n} |m\rangle \langle n|$, onde os $|m\rangle$ formam uma base ortogonal, e aplicando a definição de traço encontramos

$$\begin{aligned} \mathrm{tr}\left\{A\right\} &= \sum_i \langle i| \left(\sum_{m,n} a_{m,n} |m\rangle \langle n| \right) |i\rangle & \text{(A.18)} \\ &= \sum_i a_{i,i}. & \text{(A.19)} \end{aligned}$$

pois $\langle i|j\rangle = \delta_{i,j}$. Considerando que $|u_x\rangle$ forma uma base completa ortogonal, temos que

$$\begin{aligned} \sum_x \langle u_x| \left(\sum_{m,n} a_{m,n} |m\rangle \langle n| \right) |u_x\rangle &= \sum_{m,n} a_{m,n} \sum_x \langle u_x|m\rangle \langle n|u_x\rangle , & \text{(A.20)} \\ &= \sum_{m,n} a_{m,n} \langle n| \left(\sum_x |u_x\rangle \langle u_x| \right) |m\rangle , & \text{(A.21)} \\ &= \sum_{m,n} a_{m,n} \delta_{m,n}, & \text{(A.22)} \\ &= \sum_n a_{n,n}, & \text{(A.23)} \\ &= \mathrm{tr}\left\{A\right\} . & \text{(A.24)} \end{aligned}$$

Finalizando assim a prova. □

Além disso, se A sofre uma transformação unitária U o valor do traço de A não se altera:

Propriedade A.2. *O traço é invariante sobre transformações unitárias, isto é*

$$\mathrm{tr}\left\{UAU^\dagger\right\} = \mathrm{tr}\left\{A\right\} . \tag{A.25}$$

Demonstração. Vamos supor que $U^\dagger |i\rangle = |u_i\rangle$. Assim,

$$\begin{aligned} \mathrm{tr}\left\{UAU^\dagger\right\} &= \sum_i \langle i| UAU^\dagger |i\rangle , & \text{(A.26)} \\ &= \sum_i \langle u_i| A |u_i\rangle . & \text{(A.27)} \end{aligned}$$

Pela propriedade A.1, $\sum_i \langle u_i| A |u_i\rangle = \mathrm{tr}\{A\}$. □

Como naturalmente um estado pode representar mais de um sistema, o mesmo ocorre para o operador densidade. E corriqueiramente é interessante conhecer o operador densidade localmente. Para isso, vamos definir o conceito de traço parcial. Considerando um sistema bipartido ρ^{AB}, temos que o traço parcial em B é dado por

$$\mathrm{tr}_B\left\{\rho^{AB}\right\} \equiv \sum_i (\mathbb{1}_A \otimes_B \langle i|)\rho^{AB}(\mathbb{1}_A \otimes |i\rangle_B). \tag{A.28}$$

Claramente o resultado da equação anterior é um operador: o operador densidade do sistema A.

Teorema A.1. *Seja um sistema físico AB cujo operador densidade é ρ^{AB}. O operador densidade do sistema A é definido como*

$$\rho^A = \mathrm{tr}_B\left\{\rho^{AB}\right\}. \tag{A.29}$$

Demonstração. Considere um operador densidade ρ^{AB}, cuja decomposição espectral é dada por $\sum_{a,b} p_{A,B}(a,b)\,|a\rangle_A\langle a| \otimes |b\rangle_B\langle b|$. Então, tomando o traço parcial em um dos subsistemas, por exemplo o subsistema B, temos

$$\begin{aligned}
\mathrm{tr}_B\left\{\rho^{AB}\right\} &= \sum_i \sum_{a,b} p_{A,B}(a,b)\,|a\rangle_A\langle a| \otimes_B \langle i|b\rangle_B \langle b|i\rangle_B && \text{(A.30)}\\
&= \sum_{a,b,i} \delta_{i,b} p_{A,B}(a,b)\,|a\rangle_A\langle a| && \text{(A.31)}\\
&= \sum_a \left[\sum_b p_{A,B}(a,b)\right] |a\rangle_A\langle a|\,. && \text{(A.32)}
\end{aligned}$$

Da teoria das probabilidades temos que $\sum_b p_{A,B}(a,b) = p_A(a)$. Assim,

$$\mathrm{tr}_B\left\{\rho^{AB}\right\} = \sum_a p_A(a)\,|a\rangle_A\langle a| = \rho^A. \tag{A.33}$$

□

Para se computar o traço total é indiferente a ordem do sistema em que se toma o traço parcial, isto é

Propriedade A.3. *O traço para um sistema multipartido é*

$$\mathrm{tr}\left\{\rho^{AB}\right\} = \mathrm{tr}_A\left\{\mathrm{tr}_B\left\{\rho^{AB}\right\}\right\} = \mathrm{tr}_B\left\{\mathrm{tr}_A\left\{\rho^{AB}\right\}\right\}. \tag{A.34}$$

Demonstração. Seja $\rho^{AB} = \sum_{i,j,k,l} b_{i,j,k,l} \left|ij\right\rangle_{AB} \left|kl\right\rangle$, um sistema bipartido geral. Assim, pela definição de traço

$$\begin{aligned}
\mathrm{tr}\left\{\rho^{AB}\right\} &= \sum_{m,n} {}_{AB}\left\langle mn\right| \left(\sum_{i,j,k,l} b_{i,j,k,l} \left|ij\right\rangle_{AB}\!\left\langle kl\right|\right) \left|mn\right\rangle_{AB} && \text{(A.35)}\\
&= \sum_{m} {}_{A}\left\langle m\right| \left[\sum_{n} {}_{B}\!\left\langle n\right| \left(\sum_{i,j,k,l} b_{i,j,k,l} \left|ij\right\rangle_{AB}\!\left\langle kl\right|\right) \left|n\right\rangle_{B}\right] \left|m\right\rangle_{A} && \text{(A.36)}\\
&= \sum_{m} {}_{A}\left\langle m\right| \left[\mathrm{tr}_B\left\{\rho^{AB}\right\}\right] \left|m\right\rangle_{A} && \text{(A.37)}\\
&= \mathrm{tr}_A\left\{\mathrm{tr}_B\left\{\rho^{AB}\right\}\right\}. && \text{(A.38)}
\end{aligned}$$

Para se obter $\mathrm{tr}_B\left\{\mathrm{tr}_A\left\{\rho^{AB}\right\}\right\}$ no lugar da Eq. (A.38), basta calcular primeiro o traço sobre o sistema A na Eq. (A.36),

$$\begin{aligned}
\mathrm{tr}\left\{\rho^{AB}\right\} &= \sum_{m,n} {}_{AB}\left\langle mn\right| \left(\sum_{i,j,k,l} b_{i,j,k,l} \left|ij\right\rangle_{AB}\!\left\langle kl\right|\right) \left|mn\right\rangle_{AB} && \text{(A.39)}\\
&= \sum_{n} {}_{B}\left\langle n\right| \left[\sum_{m} {}_{A}\!\left\langle m\right| \left(\sum_{i,j,k,l} b_{i,j,k,l} \left|ij\right\rangle_{AB}\!\left\langle kl\right|\right) \left|m\right\rangle_{A}\right] \left|n\right\rangle_{B} && \text{(A.40)}\\
&= \sum_{n} {}_{B}\left\langle n\right| \left[\mathrm{tr}_A\left\{\rho^{AB}\right\}\right] \left|n\right\rangle_{B} && \text{(A.41)}\\
&= \mathrm{tr}_B\left\{\mathrm{tr}_A\left\{\rho^{AB}\right\}\right\}. && \text{(A.42)}
\end{aligned}$$

Concluindo assim a prova. □

A.1 Medidas POVM

Em algumas situações, o estado quântico após a medida não é relevante. Nestes casos, o importante são as probabilidades dos resultados. Sendo assim, o formalismo POVM (*positive-operator valued measure*) simplifica as análises destes tipos de medidas.

Para compreender o POVM, suponha que a medida M_m aplicada no estado quântico

$|\Psi\rangle$. Pelo postulado da medida temos que a probabilidade do resultado m é

$$p(m) = \langle\Psi| M_m^\dagger M_m |\Psi\rangle . \tag{A.43}$$

Definindo

$$E_m = M_m^\dagger M_m, \tag{A.44}$$

temos que

$$p(m) = \langle\Psi| E_m |\Psi\rangle = \mathrm{tr}\left\{E_m |\Psi\rangle \langle\Psi|\right\}, \tag{A.45}$$

usando o formalismo do traço visto na seção anterior.

O conjunto dos elementos $\{E_m\}$ são conhecidos como POVM. E eles devem ser completos ($\sum_m E_m = \mathbb{1}$) e positivos pelo postulado da medida. Note que $E_m^\dagger = E_m$, pois

$$(M_m^\dagger M_m)^\dagger = (M_m)^\dagger (M_m^\dagger)^\dagger = M_m^\dagger M_m. \tag{A.46}$$

Portanto, E_m é um operador autoadjunto. Consequentemente, um operador positivo. A condição de ser completo origina-se a partir da soma da probabilidade total ser 1, ou melhor, $\sum_m M_m^\dagger M_m = \mathbb{1}$. Assim,

$$\sum_m E_m \;=\; \sum_m M_m^\dagger M_m = \mathbb{1}. \tag{A.47}$$

Um exemplo de POVM são as medidas projetivas, onde P_m são os projetores tal que $\sum_m P_m = \mathbb{1}$. Neste caso, $E_m = P_m^\dagger P_m = P_m$.

Por fim, suponha, agora, que o $\{E_m\}$ é um conjunto de operadores positivos tal que $\sum_m E_m = \mathbb{1}$. Definindo $M_m = \sqrt{E_m}$ nós temos que $\{M_m\}$ é o conjunto que descreve a medida com o POVM $\{E_m\}$. Lembrando que $E_m = E_m^\dagger$ e positivo, note que $\sum_m M_m^\dagger M_m = \mathbb{1}$, pois

$$\begin{aligned}
\sum_m M_m^\dagger M_m &= \sum_m \left[\left(\sqrt{E_m}\right)^\dagger \sqrt{E_m}\right] && \text{(A.48)}\\
&= \sum_m \left(\sqrt{E_m^\dagger E_m}\right) && \text{(A.49)}\\
&= \sum_m \sqrt{E_m^2} && \text{(A.50)}\\
&= \sum_m E_m && \text{(A.51)}\\
&= \mathbb{1}. && \text{(A.52)}
\end{aligned}$$

Apêndice B

Monotonicidade da entropia relativa

Neste apêndice vamos provar a monotonicidade da entropia relativa conforme feito na Ref. [35]. Mas antes de alcançar esse objetivo precisamos dos seguintes lemas.

Lema B.1. *Se f é uma função convexa então $\frac{\mathrm{d}^2 f(x)}{\mathrm{d}x^2} \geq 0$ para qualquer x. Isso implica que*

$$f(tx + (1-t)y) \geq tf(x) + (1-t)f(y), \tag{B.1}$$

para todo $t \in [0,1]$.

Demonstração. A prova dar-se-á expandindo a função aplicando o teorema de Taylor [54, 55] em torno do ponto a,

$$f(z) = f(a) + (z-a)f'(a) + \frac{1}{2}(z-a)^2 f''(\xi). \tag{B.2}$$

onde ξ é qualquer valor entre a e z.

Por hipótese, $f''(\xi) \geq 0$, pois f é uma função convexa. Portanto, o último termo escrito é essencialmente não negativo. Assim

$$f(z) \geq f(a) + f'(a)(z-a). \tag{B.3}$$

Chamando $z = x$ e $z = tx + (1-t)y$ e depois considerando que $z = y$ mantendo $a = tx + (1-t)y$ na Eq. (B.3) encontramos as seguintes desigualdades

$$f(x) \geq f(tx + (1-t)y) + (1-t)(x-y)f'(tx + (1-t)y), \tag{B.4}$$

$$f(y) \geq f(tx + (1-t)y) - t(x-y)f'(tx + (1-t)y). \tag{B.5}$$

Multiplicando a Eq. (B.4) por t, a Eq. (B.5) por $(1-t)$ e somando as duas equações recobramos a equação (B.1).

$$f(tx + (1-t)y) \geq tf(x) + (1-t)f(y).$$

□

Lema B.2. *Seja x um número real, verifica-se a seguinte desigualdade:*

$$\ln x \leq x - 1. \tag{B.6}$$

Demonstração. Para provar esse lema vamos considerar uma função que seja a diferença entre os dois lados da desigualdade,

$$f(x) = (x-1) - \ln(x). \tag{B.7}$$

Derivando duas vezes a Eq. (B.7) em relação a x obtemos

$$f'(x) = 1 - \frac{1}{x}, \tag{B.8}$$

$$f''(x) = \frac{1}{x^2}. \tag{B.9}$$

Como a derivada segunda é sempre positiva para x real, Eq. (B.9), e a Eq. (B.8) é nula somente para $x = 1$, temos que esse valor de x é um ponto de mínimo. Portanto, o menor valor da função é $f(1) = 0$. Consequente $f(x)$ é uma função estritamente positiva ou nula. Em outras palavras,

$$(x-1) - \ln(x) \geq 0 \Rightarrow \ln(x) \leq x - 1. \tag{B.10}$$

□

Lema B.3. *Seja X um operador quântico. Então, a função $f(X) = -\ln(X)$ é um operador convexo.*

Demonstração. Antes de tudo, é importante ver que se um operador $Y - X$ é um operador positivo, então temos que $X \leq Y$ por definição. Mais ainda, se $X \leq Y$ então $ZXZ^\dagger \leq ZYZ^\dagger$ para qualquer $ZZ^\dagger = \mathbb{1}$. Esta conclusão é obtida considerando o seguinte. Se $Y - X$ é um operador positivo podemos escrever $Y - X = \sum_i \alpha_i |u_i\rangle \langle u_i|$, com α_i positivo (definição de operadores positivos). Considere agora um Z qualquer, tal que $Z|u_i\rangle = |z_i\rangle$. Sendo

assim

$$Y - X = \sum_i \alpha_i \left|u_i\right\rangle \left\langle u_i\right|, \tag{B.11}$$

$$Z(Y-X)Z^\dagger = \sum_i \alpha_i \left(Z\left|u_i\right\rangle \left\langle u_i\right| Z^\dagger\right) \tag{B.12}$$

$$= \sum_i \alpha_i \left|z_i\right\rangle \left\langle z_i\right|. \tag{B.13}$$

Como $\left|z_i\right\rangle \left\langle z_i\right|$ é um estado puro então $Z(Y-X)Z^\dagger$ é uma matriz positiva implicando que $ZXZ^\dagger \leq ZYZ^\dagger$.

A prova do lema B.3 consiste em provar que

$$-\ln[pZ + (1-p)W] \leq -p\ln(Z) - (1-p)\ln(W), \tag{B.14}$$

com Z e W operadores e p variando de 0 a 1. Para chegarmos à Eq. (B.14) vamos usar que $-\ln(x) = \int_0^\infty \mathrm{d}t \left(\frac{1}{x+t} - \frac{1}{1+t}\right)$ cuja adptação para operadores positivos é

$$-\ln(X) = \int_0^\infty \mathrm{d}t \left\{[X + t\mathbb{1}]^{-1} - [\mathbb{1} + t\mathbb{1}]^{-1}\right\}. \tag{B.15}$$

Portanto, se provarmos que $f(X) = X^{-1}$ é um operador convexo chegaremos à relação dada pela Eq. (B.14) a partir da Eq. (B.15). E do mesmo modo, se $f(X) = X^{-1}$ é um operador convexo, então $[pZ + (1-p)W]^{-1} \leq pZ^{-1} + (1-p)W^{-1}$.

Primeiramente, vamos considerar que $Z = \mathbb{1}$ e $W = Y$, dois operadores que comutam entre si. Consequentemente, se $f(X) = X^{-1}$ é um operador convexo temos que $f(p\mathbb{1} + (1-p)Y) \leq pf(\mathbb{1}) + (1-p)f(Y)$, isto é,

$$[p\mathbb{1} + (1-p)Y]^{-1} \leq p\mathbb{1}^{-1} + (1-p)Y^{-1}. \tag{B.16}$$

Por $\mathbb{1}$ e Y, comutarem eles possuem uma base em comum. Portanto, $\mathbb{1} = \sum_i \left|y_i\right\rangle \left\langle y_i\right|$ e $Y = \sum_i y_i \left|y_i\right\rangle \left\langle y_i\right|$. Assim,

$$\left\{\sum_i [p + (1-p)y_i] \left|y_i\right\rangle \left\langle y_i\right|\right\}^{-1} \leq p\left(\sum_i \left|y_i\right\rangle \left\langle y_i\right|\right)^{-1} + (1-p)\left(\sum_i y_i \left|y_i\right\rangle \left\langle y_i\right|\right)^{-1}, \tag{B.17}$$

$$\sum_i \frac{1}{[p + (1-p)y_i]} \left|y_i\right\rangle \left\langle y_i\right| \leq p\sum_i 1^{-1} \left|y_i\right\rangle \left\langle y_i\right| + (1-p)\sum_i y_i^{-1} \left|y_i\right\rangle \left\langle y_i\right|, \tag{B.18}$$

$$0 \leq \sum_i \left\{\left[\frac{p}{1} + \frac{(1-p)}{y_i}\right] - \frac{1}{[p+(1-p)y_i]}\right\} \left|y_i\right\rangle \left\langle y_i\right|. \tag{B.19}$$

A Eq. (B.19) é verdadeira, pois pelo lema B.1 $f(x) = 1/x$ possui derivada segunda positiva implicando que a relação se verifica. Da Eq. (B.17) para a Eq. (B.18) usamos que a função de um operador é a função dos autovalores na base diagonal.

Para a expansão do caso geral, basta considerarmos que $Y = Z^{-\frac{1}{2}} W Z^{-\frac{1}{2}}$. Assim, pela Eq. (B.17) ser verdade temos que

$$\begin{aligned}
[p\mathbb{1} + (1-p)Y]^{-1} &\leq p\mathbb{1}^{-1} + (1-p)Y^{-1}, && \text{(B.20)}\\
\left[p\mathbb{1} + (1-p)\left(Z^{-\frac{1}{2}} W Z^{-\frac{1}{2}}\right)\right]^{-1} &\leq p\mathbb{1}^{-1} + (1-p)\left(Z^{-\frac{1}{2}} W Z^{-\frac{1}{2}}\right)^{-1}, && \text{(B.21)}\\
\left\{Z^{-\frac{1}{2}}\left[pZ + (1-p)W\right] Z^{-\frac{1}{2}}\right\}^{-1} &\leq p\mathbb{1}^{-1} + (1-p)\left(Z^{-\frac{1}{2}} W Z^{-\frac{1}{2}}\right)^{-1}, && \text{(B.22)}\\
Z^{\frac{1}{2}}\left[pZ + (1-p)W\right]^{-1} Z^{\frac{1}{2}} &\leq pZ^{\frac{1}{2}} Z^{-1} Z^{\frac{1}{2}} + (1-p)Z^{\frac{1}{2}} (W)^{-1} Z^{\frac{1}{2}}, && \text{(B.23)}\\
[pZ + (1-p)W]^{-1} &\leq pZ^{-1} + (1-p)W^{-1}, && \text{(B.24)}
\end{aligned}$$

provando que $f(X) = X^{-1}$ é convexa para todo operador.

Por fim, basta agora provarmos que $\ln(X)$ é convexa usando a Eq. (B.15),

$$\begin{aligned}
-\ln[pZ + (1-p)W] &\leq -p\ln(Z) - (1-p)\ln(W), && \text{(B.25)}\\
\int_0^\infty \mathrm{d}t \left\{[pZ+(1-p)W+t\mathbb{1}]^{-1} - [\mathbb{1}+t\mathbb{1}]^{-1}\right\} &\leq \int_0^\infty \mathrm{d}t \left\{p\left[Z + t\mathbb{1}\right]^{-1} + (1-p)\left[W + t\mathbb{1}\right]^{-1}\right\}\\
&\quad - \int_0^\infty \mathrm{d}t \left(\mathbb{1} + t\mathbb{1}\right)^{-1}, && \text{(B.26)}\\
\int_0^\infty \mathrm{d}t \left\{[pZ + (1-p)W + t\mathbb{1}]^{-1}\right\} &\leq \int_0^\infty \mathrm{d}t \left\{p\left[Z + t\mathbb{1}\right]^{-1} + (1-p)\left[W + t\mathbb{1}\right]^{-1}\right\},\\
\int_0^\infty \mathrm{d}t \left\{[p(Z + t\mathbb{1}) + (1-p)(W + t\mathbb{1}) +]^{-1}\right\} &\leq \int_0^\infty \mathrm{d}t \left\{p\left[Z + t\mathbb{1}\right]^{-1} + (1-p)\left[W + t\mathbb{1}\right]^{-1}\right\}. && \text{(B.27)}
\end{aligned}$$

A partir da Eq. (B.24) vemos que a linha (B.27) é verdadeira, finalizando a prova do lema. □

Antes de prosseguirmos para o próximo lema, é importante ter em mente que um operador isométrico é uma transformação que preserva a distância [51]. Em outras palavras, se a, b pertence a um espaço métrico $\mathcal{H}_1$ e A um operador isométrico com domínio $\mathcal{H}_1$ e imagem em $\mathcal{H}_2$, então

$$\langle Aa, Ab\rangle_2 = \langle a, b\rangle_1,$$

com $\langle\cdot,\cdot\rangle_1$ e $\langle\cdot,\cdot\rangle_2$ o produto interno atuando no espaço $\mathcal{H}_1$ e $\mathcal{H}_2$ respectivamente. Quando

$\mathcal{H}_1 = \mathcal{H}_2$ temos um tipo especial de isomeria muito conhecida. Este tipo especial de isomeria é chamada de transformação unitária.

Lema B.4. *Se f é um operador convexo, e $T : V \to W$ uma isometria tal que a* $\dim(V) \leq \dim(W)$*, então $f(T^\dagger XT) \leq T^\dagger f(X)T$ para todo X.*

Demonstração. Considere uma transformação $T : V \to W$, e que a imagem W' desta transformação T é um subespaço de W. Seja P um projetor no espaço W' sendo Q seu projetor ortonormal, isto é, Q é uma projeção no espaço $W - W'$. Seja também f uma função convexa. Por fim, introduzimos a notação f_V, f_W e $f_{W'}$. Onde, f_V pega entradas do espaço V e produz resultados também no espaço V, o mesmo vale para f_W e $f_{W'}$ que agem em seus respectivos espaços.

Perceba que $PT = T$ já que P projeta na imagem de T. Assim, para uma matriz X que pertence ao espaço V temos que

$$f_V(T^\dagger XT) = f_V(T^\dagger PXPT) = f_V(T^\dagger PPXPPT), \tag{B.28}$$

onde usamos $P = P^2$ por ser um projetor. Note que PXP pertence ao espaço W', assim PT atuando em PXP é uma isomeria que leva W' em W'. Portanto, uma transformação unitária, e por $T^\dagger P$ ser uma transformação unitária em PXP, sabemos que a igualdade deste lema se verifica, pois os autovalores não se alteram após transformações unitárias. Assim,

$$\begin{aligned} f_V(T^\dagger XT) &= T^\dagger P f_V(PXP)PT \\ &= T^\dagger PP f_V(PXP)PPT \\ &= T^\dagger P f_{W'}(PXP)PT. \end{aligned} \tag{B.29}$$

Considere agora, uma matriz Y qualquer pertencente a W. A decomposição espectral de Y é $\sum_i y_i |i\rangle \langle i|$. Se reordenarmos os índices de forma que $i \leq n$ pertença ao subespaço W' e o restante ao complementar de W' temos que $Y = PYP + QYQ$ e também que

$$f_W(Y) = \sum_i f_W(y_i) |i\rangle \langle i| \tag{B.30}$$

$$= \sum_i^n f_W(y_i) |i\rangle \langle i| + \sum_{i=n+1} f_W(y_i) |i\rangle \langle i| \tag{B.31}$$

$$= \sum_i^n f_W(y_i) P |i\rangle \langle i| P + \sum_{i=n+1} f_W(y_i) Q |i\rangle \langle i| Q \tag{B.32}$$

$$f_W(PYP + QYQ) = f_W(PYP) + f_W(QYQ). \tag{B.33}$$

A função da Eq. (B.29), $f_{W'}(PXP)$, nada mais é que $Pf_W(PXP)P = Pf_W(PXP + QXQ)P$ (lembre-se que P projeta em W'). Esta igualdade é obtida considerando as Eqs. (B.32) e (B.33), pois o termo $Pf_W(QXQ)P = P\sum_{i=n+1} f_W(y_i)Q\,|i\rangle\langle i|\,QP$ dá um valor nulo. Utilizando esta informação e substituindo na Eq. (B.29), temos

$$f_V(T^\dagger XT) = T^\dagger P f_W(PXP + QXQ)PT. \tag{B.34}$$

Definindo $S = P - Q$ e lembrando que a identidade é $\mathbb{1} = P + Q$ obtemos

$$\begin{aligned}\frac{1}{2}(X + SXS) &= \frac{1}{2}\left[(P+Q)X(P+Q) + (P-Q)X(P-Q)\right] \\ &= \frac{1}{2}\left[PXP + PXQ + QXP + QXQ + PXP - PXQ - QXP + QXQ\right] \\ &= (PXP + QXQ)\,.\end{aligned} \tag{B.35}$$

Dessa forma, utilizando o lema B.3, a Eq. (B.34) possui o seguinte desenvolvimento

$$\begin{aligned}f_V(T^\dagger XT) &= T^\dagger P f_W\left(\frac{1}{2}X + \frac{1}{2}SXS\right)PT \\ &\leq T^\dagger P\left[\frac{1}{2}f_W(X) + \frac{1}{2}f_W(SXS)\right]PT.\end{aligned} \tag{B.36}$$

Como S é uma transformação unitária no espaço W, pois $SS^\dagger = P + Q = \mathbb{1}$, temos que $f_W(SXS) = Sf_W(X)S$. Então,

$$\begin{aligned}f_V(T^\dagger XT) &\leq T^\dagger P\left[\frac{1}{2}f_W(X) + \frac{1}{2}Sf_W(X)S\right]PT, \\ &= T^\dagger\left[\frac{1}{2}Pf_W(X)P + \frac{1}{2}(PP - PQ)f_W(X)(PP - QP)\right]T, \\ &= T^\dagger P f_W(X)PT,\end{aligned} \tag{B.37}$$

já que $PQ = QP = 0$. No entanto, $PT = T$, e consequentemente obtemos

$$f_V(T^\dagger XT) \leq T^\dagger f_W(X)T. \tag{B.38}$$

□

Lema B.5 (Monotonicidade da entropia relativa)**.** *A entropia relativa entre dois estados ρ^{AB} e σ^{AB} pode apenas decrescer se for aplicada uma redução do sistema [35].*

$$S(\rho^A||\sigma^A) \leq S(\rho^{AB}||\sigma^{AB}). \tag{B.39}$$

Demonstração. Definimos que $\mathcal{L}(X) \equiv \sigma X$ e $\mathcal{R}(X) \equiv X\rho^{-1}$, onde σ e ρ são operadores densidades positivos e que possuem inversa. Definimos. também, outro mapa linear que é a aplicação sucessiva dos mapas anteriores, $\Delta = \mathcal{L}\mathcal{R}$. Perceba que $\mathcal{L}\mathcal{R} = \mathcal{R}\mathcal{L}$.

Nosso próximo passo é definir que para um mapa linear $\mathcal{E} = \sum_j \lambda_j \mathcal{E}_j$ temos que $\ln(\mathcal{E}) = \sum_j \ln(\lambda_j)\mathcal{E}_j$. Então, considerando que a decomposição espectral de σ é $\sum_i s_i \left|s_i\right\rangle \left\langle s_i\right|$, logo $\ln(\mathcal{L})X = \sum_i \ln(s_i)\mathcal{L}_j(X)$, onde o mapa $\mathcal{L}_j$ significa multiplicar pela esquerda pelo operador $\left|s_i\right\rangle \left\langle s_i\right|$. Assim, $\ln(\mathcal{L})X = \sum_i X \ln(s_i) \left|s_i\right\rangle \left\langle s_i\right|$. Devido a $\ln(s_i) \left|s_i\right\rangle \left\langle s_i\right| = \ln(\sigma)$ temos que $\ln(\mathcal{L})X = \ln(\sigma)X$. Aplicando o mesmo raciocínio encontramos que $\ln(\mathcal{R})X = -X\ln(\rho)$. Ainda mais, como $\mathcal{L}$ e $\mathcal{R}$ comutam, temos que $\ln(\Delta) = \ln(\mathcal{L}) + \ln(\mathcal{R})$.

Por fim temos que o produto interno de Hilbert-Schimdt é definido por

$$\langle X, Y\rangle \equiv \mathrm{tr}\left\{X^\dagger Y\right\}. \tag{B.40}$$

Com todas as informações necessárias inseridas, vamos provar agora que o produto interno de Hilbert-Schmidt de $\langle \rho^{\frac{1}{2}}, -\ln(\Delta)(\rho^{\frac{1}{2}})\rangle$ nada mais que a entropia relativa $S\left(\rho||\sigma\right)$ dada pela Eq. (2.27),

$$\begin{aligned}
\langle \rho^{\frac{1}{2}}, -\ln(\Delta)(\rho^{\frac{1}{2}})\rangle &= \mathrm{tr}\left\{\left(\rho^{\frac{1}{2}}\right)^\dagger \left[-\ln(\Delta)(\rho^{\frac{1}{2}})\right]\right\} && \text{(B.41)}\\
&= \mathrm{tr}\left\{\left(\rho^{\frac{1}{2}}\right)^\dagger \left[-\ln(\mathcal{L})(\rho^{\frac{1}{2}}) - \ln(\mathcal{R})(\rho^{\frac{1}{2}})\right]\right\} && \text{(B.42)}\\
&= \mathrm{tr}\left\{\left(\rho^{\frac{1}{2}}\right)^\dagger \left[-\ln(\sigma)\rho^{\frac{1}{2}} + \rho^{\frac{1}{2}}\ln(\rho)\right]\right\} && \text{(B.43)}\\
&= -\mathrm{tr}\left\{\left(\rho^{\frac{1}{2}}\right)^\dagger \ln(\sigma)\rho^{\frac{1}{2}}\right\} + \mathrm{tr}\left\{\left(\rho^{\frac{1}{2}}\right)^\dagger \rho^{\frac{1}{2}}\ln(\rho)\right\} && \text{(B.44)}\\
&= -\mathrm{tr}\left\{\rho^{\frac{1}{2}}\left(\rho^{\frac{1}{2}}\right)^\dagger \ln(\sigma)\right\} + \mathrm{tr}\left\{\left(\rho^{\frac{1}{2}}\right)^\dagger \rho^{\frac{1}{2}}\ln(\rho)\right\} && \text{(B.45)}\\
&= -\mathrm{tr}\left\{\left(\rho\rho^\dagger\right)^{\frac{1}{2}}\ln(\sigma)\right\} + \mathrm{tr}\left\{\left(\rho^\dagger\rho\right)^{\frac{1}{2}}\ln(\rho)\right\} && \text{(B.46)}\\
&= -\mathrm{tr}\left\{\rho\ln(\sigma)\right\} + \mathrm{tr}\left\{\rho\ln(\rho)\right\}, && \text{(B.47)}\\
&= S\left(\rho||\sigma\right). && \text{(B.48)}
\end{aligned}$$

Vamos fixar a seguinte notação

$$\Delta^{AB}(X) \equiv \sigma^{AB} X \left(\rho^{AB}\right)^{-1}, \tag{B.49}$$

$$\Delta^{A}(X) \equiv \sigma^{A} X \left(\rho^{A}\right)^{-1}, \tag{B.50}$$

para aplicarmos na demonstração do lema da Eq. B.39. Isto é, queremos mostrar que $S\left(\rho^A||\sigma^A\right) \leq \left(\rho^{AB}||\sigma^{AB}\right)$ e, para isto, utilizamos a Eq. (B.48), reduzindo o lema a

$$\langle\sqrt{\rho^A}, -\ln(\Delta^A)(\sqrt{\rho^A})\rangle \leq \langle\sqrt{\rho^{AB}}, -\ln(\Delta^{AB})(\sqrt{\rho^{AB}})\rangle. \tag{B.51}$$

Vamos supor que exista um mapa linear $T : M(A) \to M(AB)$ tal que

$$\begin{aligned} &\text{i)} \quad T^\dagger \Delta^{AB} T = \Delta^A, \\ &\text{ii)} \quad T\sqrt{\rho^A} = \sqrt{\rho^{AB}}, \\ &\text{iii)} \quad \text{Que o mapa seja uma isomeria de } M(A) \text{ para } M(AB). \end{aligned} \tag{B.52}$$

Se T fosse uma transformação unitária (um caso especial de isomeria onde $\mathcal{H}_A = \mathcal{H}_{AB}$) obteríamos diretamente que

$$-\ln\left(\Delta^A\right) = -\ln\left(T^\dagger \Delta^{AB} T\right) \tag{B.53}$$

$$= -T^\dagger \ln\left(\Delta^{AB}\right) T. \tag{B.54}$$

Mas como podemos ter que $\mathcal{H}_A \neq \mathcal{H}_{AB}$, usamos o lema B.4 para obtermos a relação para um operador convexo

$$-\ln\left(\Delta^A\right) \leq -T^\dagger \ln\left(\Delta^{AB}\right) T. \tag{B.55}$$

Assim, pelo item i) da Eq. (B.52) temos,

$$\left\langle \sqrt{\rho^A}, -\ln\left(\Delta^A\right)\left(\sqrt{\rho^A}\right)\right\rangle = \left\langle \sqrt{\rho^A}, -\ln\left(T^\dagger \Delta_{AB} T\right)\left(\sqrt{\rho^A}\right)\right\rangle, \tag{B.56}$$

e pela Eq. (B.55) segue o seguinte raciocínio,

$$\begin{aligned}
\left\langle \sqrt{\rho^A}, -\ln\left(\Delta^A\right)\left(\sqrt{\rho^A}\right)\right\rangle &\leq \left\langle \sqrt{\rho^A}, -T^\dagger \ln\left(\Delta^{AB}\right) T\left(\sqrt{\rho^A}\right)\right\rangle && \text{(B.57)}\\
&= -\mathrm{tr}\left\{\sqrt{\rho^A}^\dagger T^\dagger \ln\left(\Delta^{AB}\right) T\left(\sqrt{\rho^A}\right)\right\} && \text{(B.58)}\\
&= -\mathrm{tr}\left\{\left(T\sqrt{\rho^A}\right)^\dagger \ln\left(\Delta^{AB}\right)\left(T\sqrt{\rho^A}\right)\right\} && \text{(B.59)}\\
&= \left\langle T\sqrt{\rho^A}, -\ln\left(\Delta^{AB}\right)\left(T\sqrt{\rho^A}\right)\right\rangle. && \text{(B.60)}
\end{aligned}$$

Pelo item ii) da Eq. (B.52) temos que $T\sqrt{\rho^A} = \sqrt{\rho^{AB}}$. Portanto,

$$\begin{aligned}
\left\langle \sqrt{\rho^A}, -\ln\left(\Delta^A\right)\left(\sqrt{\rho^A}\right)\right\rangle &\leq \left\langle \sqrt{\rho^{AB}}, -\ln\left(\Delta^{AB}\right)\left(\sqrt{\rho^{AB}}\right)\right\rangle, && \text{(B.61)}\\
S(\rho_A||\sigma_A) &\leq S(\rho_{AB}||\sigma_{AB}), && \text{(B.62)}
\end{aligned}$$

que é o resultado desejado. Para finalizarmos a prova, temos que mostrar que a isometria T existe. De fato, se a transformação for

$$T(X_A) = \left[X_A\left(\sqrt{\rho^A}\right)^{-1} \otimes \mathbb{1}_B\right]\sqrt{\rho^{AB}}, \tag{B.63}$$

resolvemos este problema.

Para encontrar $T^\dagger$ vamos usar a definição de uma isomeria. Isto é, vamos resolver

$$\langle Y_{AB}, X_{AB}\rangle = \langle Y_A, X_A\rangle. \tag{B.64}$$

Sabendo que $T(X_A) = (X_{AB})$, e que o adjunto de $T^\dagger(Y_{AB}) = Y_A$, a equação anterior torna-se,

$$\langle Y_{AB}, T(X_A)\rangle = \langle T^\dagger(Y_{AB}), X_A\rangle. \tag{B.65}$$

Aplicando a definição do produto interno de Hilbert-Schimdt para a Eq. (B.65) encon-

tramos o seguinte resultado,

$$\begin{aligned}
\left\langle T^{\dagger}\left(Y_{AB}\right), X_A\right\rangle &= \left\langle Y_{AB}, T\left(X_A\right)\right\rangle, && \text{(B.66)}\\
\operatorname{tr}\left\{\left[T^{\dagger}\left(Y_{AB}\right)\right]^{\dagger} X_A\right\} &= \operatorname{tr}\left\{Y_{AB}^{\dagger}\, T\left(X_A\right)\right\} && \text{(B.67)}\\
&= \operatorname{tr}\left\{Y_{AB}^{\dagger}\left[X_A\left(\rho^A\right)^{-\frac{1}{2}}\otimes \mathbb{1}_B\right]\left(\rho^{AB}\right)^{\frac{1}{2}}\right\} && \text{(B.68)}\\
&= \operatorname{tr}\left\{\left[X_A\left(\rho^A\right)^{-\frac{1}{2}}\otimes \mathbb{1}_B\right]\left(\rho^{AB}\right)^{\frac{1}{2}} Y_{AB}^{\dagger}\right\} && \text{(B.69)}\\
&= \operatorname{tr}\left\{\left(X_A\otimes \mathbb{1}_B\right)\left[\left(\rho^A\right)^{-\frac{1}{2}}\otimes \mathbb{1}_B\right]\left(\rho^{AB}\right)^{\frac{1}{2}} Y_{AB}^{\dagger}\right\} && \text{(B.70)}\\
&= \operatorname{tr}\left\{\left[\left(\rho^A\right)^{-\frac{1}{2}}\otimes \mathbb{1}_B\right]\left(\rho^{AB}\right)^{\frac{1}{2}} Y_{AB}^{\dagger}\left(X_A\otimes \mathbb{1}_B\right)\right\} && \text{(B.71)}\\
&= \operatorname{tr}\left\{\left\{Y_{AB}\left(\rho^{AB}\right)^{\frac{1}{2}}\left[\left(\rho^A\right)^{-\frac{1}{2}}\otimes \mathbb{1}_B\right]\right\}^{\dagger}\left(X_A\otimes \mathbb{1}_B\right)\right\} && \text{(B.72)}\\
&= \operatorname{tr}_A\left\{\left[\operatorname{tr}_B\left\{Y_{AB}\left(\rho^{AB}\right)^{\frac{1}{2}}\left[\left(\rho^A\right)^{-\frac{1}{2}}\otimes \mathbb{1}_B\right]\right\}\right]^{\dagger}\left(X_A\right)\right\}. && \text{(B.73)}
\end{aligned}$$

Consequentemente, por comparação direta o adjunto de T é dado por,

$$T^{\dagger}\left(Y_{AB}\right) = \operatorname{tr}_B\left\{Y_{AB}\left(\rho^{AB}\right)^{\frac{1}{2}}\left[\left(\rho^A\right)^{-\frac{1}{2}}\otimes \mathbb{1}_B\right]\right\}. \qquad \text{(B.74)}$$

O último elemento para verificar é se $T^{\dagger}\Delta_{AB}T\left(X_A\right) = \Delta_A\left(X_A\right)$. Aplicando a Eq. (B.63) para explicitar $T\left(X_A\right)$ resulta em

$$\begin{aligned}
T^{\dagger}\Delta_{AB}T\left(X_A\right) &= T^{\dagger}\Delta_{AB}\left\{\left[X_A\left(\rho^A\right)^{-\frac{1}{2}}\otimes \mathbb{1}_B\right]\left(\rho^{AB}\right)^{\frac{1}{2}}\right\} && \text{(B.75)}\\
&= T^{\dagger}\left\{\sigma^{AB}\left[X_A\left(\rho^A\right)^{-\frac{1}{2}}\otimes \mathbb{1}_B\right]\left(\rho^{AB}\right)^{\frac{1}{2}}\left(\rho^{AB}\right)^{-1}\right\} && \text{(B.76)}\\
&= T^{\dagger}\left\{\sigma^{AB}\left[X_A\left(\rho^A\right)^{-\frac{1}{2}}\otimes \mathbb{1}_B\right]\left(\rho^{AB}\right)^{-\frac{1}{2}}\right\}. && \text{(B.77)}
\end{aligned}$$

Evidenciando o adjunto de T encontrado na Eq. (B.74) na última equação obtemos

$$T^{\dagger}\Delta_{AB}T\left(X_A\right) = \mathrm{tr}_B\left\{\left\{\sigma^{AB}\left[X_A\left(\rho^A\right)^{-\frac{1}{2}}\otimes \mathbb{1}_B\right]\left(\rho^{AB}\right)^{-\frac{1}{2}}\right\}\left(\rho^{AB}\right)^{\frac{1}{2}}\left[\left(\rho^A\right)^{-\frac{1}{2}}\otimes \mathbb{1}_B\right]\right\} \tag{B.78}$$

$$= \mathrm{tr}_B\left\{\sigma^{AB}\left[X_A\ \left(\rho^A\right)^{-\frac{1}{2}}\otimes \mathbb{1}_B\right]\ \left[\left(\rho^A\right)^{-\frac{1}{2}}\otimes \mathbb{1}_B\right]\right\} \tag{B.79}$$

$$= \mathrm{tr}_B\left\{\sigma^{AB}\left(X_A\otimes \mathbb{1}_B\right)\ \left[\left(\rho^A\right)^{-1}\otimes \mathbb{1}_B\right]\right\} \tag{B.80}$$

$$= \mathrm{tr}_B\left\{\sigma^{AB}\right\} X_A\left(\rho^A\right)^{-1} \tag{B.81}$$

$$= \sigma^A X_A\left(\rho^A\right)^{-1} \tag{B.82}$$

$$= \Delta_A\left(X_A\right), \tag{B.83}$$

finalizando a prova.

□

Apêndice C

Decomposição de Schmidt

A decomposição de Schmidt é uma ferramenta poderosa utilizada para descrever estados bipartidos puros.

Teorema C.1. *Seja $|\psi\rangle^{AB}$ um estado puro composto por dois sistemas bipartidos A e B no espaço de Hilbert $\mathcal{H}_A \otimes \mathcal{H}_B$. Então existem estados ortonormais $|\phi_i\rangle \in \mathcal{H}_A$ e $|\varepsilon_i\rangle \in \mathcal{H}_B$ tais que*

$$|\psi\rangle_{AB} = \sum_i^n \lambda_i |\phi_i\rangle |\varepsilon_i\rangle , \tag{C.1}$$

onde λ_i são números reais não nulos com $\sum_i^n \lambda_i^2 = 1$ e n a dimensão do espaço de $|\phi_i\rangle \in \mathcal{H}_A$, considerado dimensão menor ou igual a dimensão de $\mathcal{H}_B$.

Demonstração. Seja $|\psi\rangle_{AB} = \sum_{i,j}^{n_A,n_B} \alpha_{ij} |u_i\rangle_A |v_j\rangle_B$, com n_A e n_B a dimensão de $\mathcal{H}_A$ e $\mathcal{H}_B$ respectivamente. Aqui, os estados $|u_i\rangle_A$ formam uma base ortonormal do sistema A e $|v_j\rangle_B$ ortonormal do sistema B. Em adição, temos que $\rho^{AB} = |\psi\rangle_{AB} \langle\psi|$ é o operador densidade puro deste estado.

Sem perda de generalidade, podemos decompor um dos estados bipartidos, como por exemplo o $|u_i\rangle_A$, em uma base ortonormal $|u_i\rangle_A = \sum_k a_{ik} |\phi_k\rangle_A$ de interesse que possui dimensão $n = n_A$. Assim, temos $|\psi\rangle_{AB} = \sum_{j,k}^{n_B,n} (\sum_i^{n_A} \alpha_{ij} a_{ik}) |\phi_k\rangle_A |v_j\rangle_B$. A somatória entre parenteses da equação anterior é um número complexo de índices j e k que pode ser reescrito como $\lambda_k \beta_{kj}$, sendo λ_k um número real não nulo e que satisfaça a seguinte relação: $\sum_k \lambda_k^2 = 1$. Assim, o estado do sistema torna-se

$$|\psi\rangle_{AB} = \sum_k^n \sum_j^{n_B} \lambda_k \beta_{kj} |\phi_k\rangle_A |v_j\rangle_B = \sum_k^n \lambda_k |\phi_k\rangle_A |\varepsilon_k\rangle_B , \tag{C.2}$$

com $|\varepsilon_k\rangle_B = \sum_j^{n_B} \beta_{kj} |v_j\rangle_B$.

Resta agora verificar que $|\varepsilon_k\rangle_B$ é ortonormal. Para isso, supomos que a base $\{|\phi_i\rangle\}$ foi escolhida de forma a deixar $\rho^A = \mathrm{tr}_B\left\{\rho^{AB}\right\}$ diagonal, ou seja,

$$\rho^A = \sum_k^n \lambda_k^2 \left|\phi_k\right\rangle_A \left\langle\phi_k\right| . \tag{C.3}$$

Como ρ^A é um operador densidade, portanto com traço unitário, temos que $\sum_k^n \lambda_k^2 = 1$. Calculando diretamente o ρ^A da Eq. (C.2) encontramos,

$$\rho^A = \mathrm{tr}_B\left\{\rho^{AB}\right\} = \mathrm{tr}_B\left\{\sum_{k,l}^n \lambda_k\lambda_l \left|\phi_k\right\rangle_A \left\langle\phi_l\right| \otimes \left|\varepsilon_k\right\rangle_B \left\langle\varepsilon_l\right|\right\} . \tag{C.4}$$

Sabendo que $\mathrm{tr}_B\left\{\left|\varepsilon_k\right\rangle_B \left\langle\varepsilon_l\right|\right\} = \left\langle\varepsilon_l|\varepsilon_k\right\rangle_B$, o estado ρ^A é

$$\rho^A = \sum_{k,l}^n \lambda_k\lambda_l \left|\phi_i\right\rangle \left\langle\phi_j\right|^A \left\langle\varepsilon_l|\varepsilon_k\right\rangle_B . \tag{C.5}$$

Dessa forma, o operador ρ^A, Eq. (C.5), é diagonal somente se $\left\langle\varepsilon_l|\varepsilon_k\right\rangle_B = \delta_{ij}$. Assim, como $|\varepsilon_k\rangle = \sum_j^{n_B} \beta_{kj} \left|v_j\right\rangle_B$ temos que $\langle\varepsilon_l|\varepsilon_k\rangle = \sum_i^{n_B} \beta_{ki}\beta_{il}^\dagger$, pois os estados $|v_j\rangle$ são ortonormais. Portanto, temos que ρ^A é diagonal com autovalores λ_k^2 e os estados $\left|\varepsilon_k\right\rangle_B$ ortonormais se a matriz formada pelos elementos β_{ij} for uma transformação unitária do sistema B. Dessa forma asseguramos que $\sum_i^{n_B} \beta_{ki}\beta_{il}^\dagger = \delta_{lk}$.

□

Apêndice D

O protocolo de criptografia clássico RSA

O protocolo desenvolvido por Rivest, Samir e Adleman é um protocolo de chave pública, ou seja, Bob (o recebedor da mensagem secreta) divulga publicamente a chave necessária para criptografar a mensagem, mas somente ele consegue decriptá-la. Para que isso seja possível é necessário conhecer uma função matemática cuja a inversa só é possível para quem possui informações privilegiadas. Essa função é construindo através do cálculo modular e o protocolo pode ser implementado seguindo o algoritmo abaixo:

1. Bob escolhe secretamente dois números primos p e q. Quanto maiores esses valores maior o tempo necessário de processamento para descobri-los. Ilustrativamente escolheremos $p = 17$ e $q = 11$.

2. Bob agora calcula o número $N = pq$ e escolhe um novo número e. Aqui no nosso exemplo $N = 187$ e $e = 7$.

3. Bob divulga publicamente N e e. Estes números são necessários para encriptar a mensagem. Assim, qualquer um que queira enviar uma mensagem codificada para Bob, no caso Alice, utilizará esses dois números.

4. Primeiramente Alice deve mapear sua mensagem em um número M. Esta etapa pode ser feita considerando o sistema de dígitos binários ASCII. Em seguida ela converte o número binário em um número decimal. Alice vai enviar a letra X, por exemplo, que em ASCII é representada por 10111000. Este número binário é equivalente ao número 88 na base decimal. Portanto, $M = 88$.

5. Em seguida, Alice obtém um novo número C implementando uma operação matemática em seu número M de acordo com a fórmula

$$C = M^e \,(\mathrm{mod}\, N). \tag{D.1}$$

Aqui, N e e são os números divulgados por Bob. No nosso exemplo $C = 88^7 \,(\mathrm{mod}\, 187)$. Ou seja, Alice obtém $C = 11$.

6. Alice envia o valor de C para Bob. Perceba que por usar cálculo modular, Eva não pode inferir com certeza o valor da mensagem M. Sendo assim, Eva não consegue obter o teor da mensagem enviada para Bob.

7. Para Bob decodificar a mensagem C enviada por Alice, ele precisa obter um novo número d tal que

$$e \times d = 1 \,(\mathrm{mod}\,(p-1) \times (q-1)). \tag{D.2}$$

No nosso exemplo $(p-1)(q-1) = (16)(10) = 160$. Assim, $7 \times d = 1 \,(\mathrm{mod}\, 160)$, Bob obtém que $d = 23$.

8. Agora basta Bob decriptar a mensagem através da fórmula

$$M = C^d \,(\mathrm{mod}\, N), \tag{D.3}$$

que recobra $M = 88$ para o nosso exemplo de $N = 187$ e $d = 23$.

9. Por fim, Bob converte M em números binários e lê a mensagem no sistema ASCII.

Utilizando o esquema de criptografia RSA é possível somente obter a mensagem conhecendo os números p e q. São esses números que permitem obter o valor de d que inverte a função modular

$$M = C^d (\mathrm{mod}\, N) = M^{e \times d} (\mathrm{mod}\, N). \tag{D.4}$$

Esse engenhoso protocolo é um dos protocolos mais utilizados nos dias atuais devido a sua facilidade de implementação.

Apêndice E

Análise de segurança sem a imposição do vínculo

No corpo principal da Tese apresentamos a análise de segurança dos protocolos BB84, Sec. 6.1, e GR10, Sec. 7.1, impondo um vínculo nos λ's para garantir que a representação baseada no emaranhamento reproduzisse as estatísticas corretas dos protocolos nas suas versões prepare-e-meça. Contudo, mesmo realizando os cálculos da segurança sem impor o vínculo dado pela Eq. (6.13), ainda obtemos que ele deve ser satisfeito como uma representação do melhor cenário para Eva. Em outras palavras, $\lambda_3 = \lambda_4$ é o cenário que permite a Eva extrair a maior quantidade de informação sobre a chave secreta. Nas seções seguintes provamos essa afirmação para os protocolos BB84 e GR10.

E.1 Fração da chave secreta para o BB84

A fração da chave secreta obtida na Sec. 6.1, descrita pela Eq. (6.32),

$$\begin{aligned} r &= \varepsilon_z \log \varepsilon_z + (1 - \varepsilon_x - \varepsilon_z/2) \log(2 - 2\varepsilon_x - \varepsilon_z) \\ &\quad + (\varepsilon_x - \varepsilon_z/2) \log(2\varepsilon_x - \varepsilon_z), \end{aligned}$$

foi obtida a partir da representação baseada em emaranhamento (6.1),

$$|\Psi\rangle_{ABE} = \sum_{j=1}^{4} \sqrt{\lambda_j} |\tilde{\Phi}_j\rangle_{AB} |\epsilon_j\rangle_E,$$

onde os estados compartilhados por Alice e Bob são as Eqs. (6.2)-(6.5),

$$\begin{aligned}
|\tilde{\Phi}_1\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \\
|\tilde{\Phi}_2\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \\
|\tilde{\Phi}_3\rangle &= |01\rangle, \\
|\tilde{\Phi}_4\rangle &= |10\rangle,
\end{aligned}$$

e os $|\epsilon_i\rangle$ são estados sob o controle de Eva. A partir do vínculo (6.13) ($\lambda_3 = \lambda_4 = \lambda$) obtivemos os seguintes valores para os λ's em função dos dados reais (taxas de erros na base x, ε_x, e na base z, ε_z),

$$\begin{aligned}
\lambda_1 &= 1 - \varepsilon_x - \varepsilon_z/2, \\
\lambda_2 &= \varepsilon_x - \varepsilon_z/2, \\
\lambda &= \varepsilon_z/2,
\end{aligned}$$

Eqs. (6.29)-(6.31).

Podemos escrever o operador densidade do estado (6.1) como

$$\tilde{\rho}^{ABE} = |\Psi\rangle_{ABE}\langle\Psi| \tag{E.1}$$

e, pelo postulado da medida, após Alice enviar o *qubit* $|a\rangle$ o estado final colapsa para

$$\tilde{\rho}_a^{ABE} = \frac{(|a\rangle_A\langle a| \otimes \mathbb{1}_{BE})\,\tilde{\rho}^{ABE}\,(|a\rangle_A\langle a| \otimes \mathbb{1}_{BE})^\dagger}{p_A(a)}, \tag{E.2}$$

com

$$p_A(a) = \mathrm{tr}\left\{(|a\rangle_A\langle a| \otimes \mathbb{1}_{BE})\,\tilde{\rho}^{ABE}\right\}, \tag{E.3}$$

a probabilidade de Alice enviar o estado $|a\rangle$. Entretanto, $p_A(a) = 1/2$ pois Alice tem total controle sobre o *qubit* que ela vai enviar e a intromissão de Eva não tem influência sobre a escolha de Alice. Este fato nos deu um vínculo a mais para determinarmos os valores dos λ's, como vimos na Sec. (6.1). No entanto, aqui, iremos prosseguir sem utilizar esse

resultado. Assim, quando Alice envia o *qubit* $|a\rangle = |0\rangle$, pela Eq. (E.3) temos

$$\begin{aligned} p_A(0) &= \frac{1}{2}(\lambda_1 + \lambda_2) + \lambda_3 \\ &= \frac{1}{2}(1 + \lambda_3 - \lambda_4), \end{aligned} \tag{E.4}$$

e quando Alice codifica o bit 1 (*qubit* $|a\rangle = |1\rangle$) a probabilidade é

$$\begin{aligned} p_A(1) &= \frac{1}{2}(\lambda_1 + \lambda_2) + \lambda_4 \\ &= \frac{1}{2}(1 - \lambda_3 + \lambda_4), \end{aligned} \tag{E.5}$$

onde usamos que os λ's são normalizados.

Calculando explicitamente a Eq. (E.2) usando as Eqs. (E.1) e (E.4) obtemos

$$\begin{aligned} \tilde{\rho}_0^{ABE} = \Big\{ & |00\rangle_{AB}\langle 00| \otimes \left[\lambda_1 |\epsilon_1\rangle_E\langle\epsilon_1| + \sqrt{\lambda_1\lambda_2}\left(|\epsilon_1\rangle_E\langle\epsilon_2| + |\epsilon_2\rangle_E\langle\epsilon_1|\right) + \lambda_2 |\epsilon_2\rangle_E\langle\epsilon_2|\right] \\ & + |00\rangle_{AB}\langle 01| \otimes \left[\sqrt{2\lambda_1\lambda_3}\,|\epsilon_1\rangle_E\langle\epsilon_3| + \sqrt{2\lambda_2\lambda_3}\,|\epsilon_2\rangle_E\langle\epsilon_3|\right] \\ & + |01\rangle_{AB}\langle 00| \otimes \left[\sqrt{2\lambda_1\lambda_3}\,|\epsilon_3\rangle_E\langle\epsilon_1| + \sqrt{2\lambda_2\lambda_3}\,|\epsilon_3\rangle_E\langle\epsilon_2|\right] \\ & + |01\rangle_{AB}\langle 01| \otimes \left[2\lambda_3 |\epsilon_3\rangle_E\langle\epsilon_3|\right] \Big\} \frac{1}{1 + \lambda_3 - \lambda_4}. \end{aligned} \tag{E.6}$$

Calculando também $\tilde{\rho}_0^E = \mathrm{tr}_{BE}\left\{\tilde{\rho}_0^{ABE}\right\}$ temos

$$\tilde{\rho}_0^E = \frac{\lambda_1 |\epsilon_1\rangle_E\langle\epsilon_1| + \sqrt{\lambda_1\lambda_2}\left(|\epsilon_1\rangle_E\langle\epsilon_2| + |\epsilon_2\rangle_E\langle\epsilon_1|\right) + \lambda_2 |\epsilon_2\rangle_E\langle\epsilon_2| + 2\lambda_3 |\epsilon_3\rangle_E\langle\epsilon_3|}{1 + \lambda_3 - \lambda_4}, \tag{E.7}$$

que possui os seguintes autovalores,

$$\left\{0, 0, \frac{\lambda_1 + \lambda_2}{1 + \lambda_3 - \lambda_4}, \frac{2\lambda_3}{1 + \lambda_3 - \lambda_4}\right\}. \tag{E.8}$$

Dessa forma, pela definição da entropia quântica dada pela Eq. (2.24),

$$S(\rho) = -\mathrm{tr}\left\{\rho \log(\rho)\right\},$$

obtemos

$$S(\tilde{\rho}_0^E) = h\left(\frac{2\lambda_3}{1 + \lambda_3 - \lambda_4}\right), \tag{E.9}$$

com $h(x)$ sendo a entropia binária.

Por outro lado, calculando explicitamente a Eq. (E.2) para $|a\rangle = |1\rangle$, obtemos usando as Eqs. (E.1) e (E.5) que

$$\begin{aligned}\tilde{\rho}_1^{ABE} = \Big\{ & |11\rangle_{AB}\langle 11| \otimes \left[\lambda_1 |\epsilon_1\rangle_E\langle\epsilon_1| - \sqrt{\lambda_1\lambda_2}\left(|\epsilon_1\rangle_E\langle\epsilon_2| + |\epsilon_2\rangle_E\langle\epsilon_1|\right) + \lambda_2 |\epsilon_2\rangle_E\langle\epsilon_2|\right] \\ & + |11\rangle_{AB}\langle 10| \otimes \left[\sqrt{2\lambda_1\lambda_4}\,|\epsilon_1\rangle_E\langle\epsilon_4| - \sqrt{2\lambda_2\lambda_4}\,|\epsilon_2\rangle_E\langle\epsilon_4|\right] \\ & + |10\rangle_{AB}\langle 11| \otimes \left[\sqrt{2\lambda_1\lambda_4}\,|\epsilon_4\rangle_E\langle\epsilon_1| - \sqrt{2\lambda_2\lambda_4}\,|\epsilon_4\rangle_E\langle\epsilon_2|\right] \\ & + |10\rangle_{AB}\langle 10| \otimes \left[2\lambda_4 |\epsilon_4\rangle_E\langle\epsilon_4|\right] \Big\} \frac{1}{1-\lambda_3+\lambda_4}.\end{aligned} \tag{E.10}$$

Analogamente à Eq. (E.7) temos

$$\tilde{\rho}_1^E = \mathrm{tr}_{BE}\left\{\tilde{\rho}_1^{ABE}\right\} \tag{E.11}$$

$$= \frac{\lambda_1 |\epsilon_1\rangle_E\langle\epsilon_1| - \sqrt{\lambda_1\lambda_2}\left(|\epsilon_1\rangle_E\langle\epsilon_2| + |\epsilon_2\rangle_E\langle\epsilon_1|\right) + \lambda_2 |\epsilon_2\rangle_E\langle\epsilon_2| + 2\lambda_4 |\epsilon_4\rangle_E\langle\epsilon_4|}{1-\lambda_3+\lambda_4}, \tag{E.12}$$

possui os seguintes autovalores,

$$\left\{0, 0, \frac{\lambda_1+\lambda_2}{1-\lambda_3+\lambda_4}, \frac{2\lambda_4}{1-\lambda_3+\lambda_4}\right\}. \tag{E.13}$$

Com isso

$$S(\tilde{\rho}_1^E) = h\left(\frac{2\lambda_4}{1-\lambda_3+\lambda_4}\right). \tag{E.14}$$

Por fim, a partir dos autovalores de $\rho^E = \mathrm{tr}_{AB}\left\{\rho^{ABE}\right\}$ encontramos que a entropia quântica de Eva é

$$S(\tilde{\rho}^E) = -\sum_{i=1}^{4} \lambda_i \log(\lambda_i). \tag{E.15}$$

Com esses resultados temos condições de escrever a quantidade de Holevo (2.105), cuja definição é

$$\chi(A:\tilde{\rho}^E) = S(\tilde{\rho}^E) - p_A(0)S(\tilde{\rho}_0^E) - p_A(1)S(\tilde{\rho}_1^E).$$

Substituindo as entropias quânticas dadas pelas Eqs. (E.15), (E.9) e (E.14), juntamente com as probabilidades de Alice codificar o bit 0 ou o bit 1, Eqs. (E.4) e (E.5) respectiva-

mente, encontramos

$$\chi(A:\tilde{\rho}^E) = -\sum_{i=1}^{4}\lambda_i\log(\lambda_i) - \frac{1}{2}\left[(1+\lambda_3-\lambda_4)h\left(\frac{2\lambda_3}{1+\lambda_3-\lambda_4}\right)+(1-\lambda_3+\lambda_4)h\left(\frac{2\lambda_4}{1-\lambda_3+\lambda_4}\right)\right]. \quad \text{(E.16)}$$

Sabendo que a probabilidade condicional de Bob obter o estado $|b\rangle$ dado que Alice obteve o estado $|a\rangle$ é

$$p_{B|A}(b|a) = \mathrm{tr}\left\{\left(|b\rangle_B\langle b|\otimes \mathbb{1}_{AE}\right)\tilde{\rho}_a^{ABE}\right\}, \quad \text{(E.17)}$$

encontramos

$$p_{B|A}(0|0) = \frac{1-(\lambda_3+\lambda_4)}{1+\lambda_3-\lambda_4}, \quad \text{(E.18)}$$

$$p_{B|A}(1|0) = \frac{2\lambda_3}{1+\lambda_3-\lambda_4}, \quad \text{(E.19)}$$

$$p_{B|A}(1|1) = \frac{1-(\lambda_3+\lambda_4)}{1-\lambda_3+\lambda_4}, \quad \text{(E.20)}$$

$$p_{B|A}(0|1) = \frac{2\lambda_4}{1-\lambda_3+\lambda_4}. \quad \text{(E.21)}$$

Aplicando a definição da entropia condicional $H(B|A) = \sum_a p_A(a)H(B|a)$, Eq. (2.4), onde

$$H(B|a) = -\sum_b p_{B|A}(b|a)\log\Big(p_{B|A}(b|a)\Big),$$

e usando as Eqs. (E.18-E.21) obtemos

$$H(B|0) = h\left(\frac{2\lambda_3}{1+\lambda_3-\lambda_4}\right), \quad \text{(E.22)}$$

$$H(B|1) = h\left(\frac{2\lambda_4}{1-\lambda_3+\lambda_4}\right). \quad \text{(E.23)}$$

Agora, como

$$p_B(b) = \sum_a p_A(a)p_{B|A}(b|a), \quad \text{(E.24)}$$

temos

$$P_B(0) = \frac{1}{2}(1-\lambda_3+\lambda_4), \tag{E.25}$$

$$P_B(1) = \frac{1}{2}(1+\lambda_3-\lambda_4), \tag{E.26}$$

onde utilizamos as Eqs. (E.4) e (E.5), as Eqs. (E.18-E.21) e a normalização dos λ's.

Pela definição da entropia de Shannon, $H(B) = -\sum_b p_B(b)\log(p_B(b))$, as Eqs. (E.25) e (E.26) resultam em

$$H(B) = h\left(\frac{1-\lambda_3+\lambda_4}{2}\right). \tag{E.27}$$

Com isso temos que a informação mútua, $I(A:B) = H(B) - H(B|A)$, Eq. (2.6), dada por

$$I(A:B) = h\left(\frac{1-\lambda_3+\lambda_4}{2}\right) - \frac{1}{2}\left[(1+\lambda_3-\lambda_4)h\left(\frac{2\lambda_3}{1+\lambda_3-\lambda_4}\right)+(1-\lambda_3+\lambda_4)h\left(\frac{2\lambda_4}{1-\lambda_3+\lambda_4}\right)\right]. \tag{E.28}$$

Substituindo as Eqs. (E.28) e (E.16) na fração da chave secreta, dada pelo limite de Devetak-Winter, Eq. (2.122), obtemos a taxa de segurança para o protocolo BB84,

$$r = h\left(\frac{1-\lambda_3+\lambda_4}{2}\right) + \sum_i^4 \lambda_i \log(\lambda_i). \tag{E.29}$$

Definindo a taxa de erro de Bob como usualmente fazemos, temos para a base z

$$\varepsilon_z = p_A(0)\, p_{B|A}(1|0) + p_A(1)\, p_{B|A}(0|1) = \lambda_3 + \lambda_4, \tag{E.30}$$

ao aplicarmos as Eqs. (E.4), (E.5), (E.18) e (E.21). No entanto, quando Alice e Bob, respectivamente, envia e recebe na base x, vamos obter as estatísticas diretamente a partir do operador densidade (E.1). Isto é feito considerando que

$$p_{A,B}(a,b) = \mathrm{tr}\left\{\left(|a\rangle_A\langle a| \otimes |b\rangle_B\langle b| \otimes \mathbb{1}_E\right)\tilde{\rho}^{ABE}\right\}, \tag{E.31}$$

com $|a\rangle$ e $|b\rangle$ sendo $|+\rangle$ ou $|-\rangle$ (estados que formam a base x). Deste modo, temos

$$\begin{aligned} p_{A,B}(+,-) &= \frac{1}{4}(2\lambda_2 + \lambda_3 + \lambda_4), \\ p_{A,B}(-,+) &= \frac{1}{4}(2\lambda_2 + \lambda_3 + \lambda_4), \end{aligned} \tag{E.32}$$

originando a taxa de erro da base x,

$$\varepsilon_x = p_{A,B}(+,-) + p_{A,B}(-,+) = \frac{1}{2}(2\lambda_2 + \lambda_3 + \lambda_4). \tag{E.33}$$

Resolvendo o sistema linear formado pelas Eqs. (E.30) e (E.33) mais o fato de que os λ's são normalizados,

$$\begin{aligned} \lambda_3 + \lambda_4 &= \varepsilon_z, \\ \frac{1}{2}(2\lambda_2 + \lambda_3 + \lambda_4) &= \varepsilon_x, \\ \sum_{i=1}^{4} \lambda_i &= 1, \end{aligned} \tag{E.34}$$

encontramos

$$\begin{aligned} \lambda_1 &= 1 - \frac{2\varepsilon_x + \varepsilon_z}{2}, \\ \lambda_2 &= \frac{2\varepsilon_x - \varepsilon_z}{2}, \\ \lambda_3 &= \varepsilon_z - \lambda_4. \end{aligned} \tag{E.35}$$

Analogamente como foi feito na análise de segurança do protocolo BB84 original, nós temos que os valores dos λ's são positivos e menores que um. Desta forma, para que λ_3 seja positivo na Eq. (E.35), λ_4 deve pertencer ao intervalo $[0, \varepsilon_z]$. Ou seja, $\lambda_4 = v\varepsilon_z$, com v pertencente ao intervalo $[0, 1]$. Disso resulta que

$$\begin{aligned} \lambda_1 &= 1 - \frac{2\varepsilon_x + \varepsilon_z}{2}, \\ \lambda_2 &= \frac{2\varepsilon_x - \varepsilon_z}{2}, \\ \lambda_3 &= \varepsilon_z(1 - v), \\ \lambda_4 &= \varepsilon_z v. \end{aligned} \tag{E.36}$$

Como nem todos os λ's foram definidos precisamente, já que não estamos usando o vínculo $p_A(a) = 1/2$, $(\lambda_3 = \lambda_4)$, vamos realizar uma minimização de r. Portanto, aplicando

os λ's, Eq. (E.36), na Eq. (E.29) encontramos

$$r = h\left(\frac{1}{2} - \frac{\varepsilon_z}{2}(1-2v)\right) + \theta\left(1 - \varepsilon_x - \frac{\varepsilon_z}{2}\right) + \theta\left(\varepsilon_x - \frac{\varepsilon_z}{2}\right) + \theta\left(\varepsilon_z v\right) + \theta\left(\varepsilon_z - \varepsilon_z v\right), \quad \text{(E.37)}$$

onde

$$\theta(x) = x\log(x). \quad \text{(E.38)}$$

Derivando, então, a taxa de segurança representada pela Eq. (E.37) em relação a v resulta em

$$\frac{\mathrm{d}r}{\mathrm{d}v} = \frac{\varepsilon_z}{\ln(2)}(\log(\varepsilon_z v) + \log(1+\varepsilon_z - 2\varepsilon_z v) - \log(\varepsilon_z - \varepsilon_z v) - \log(1-\varepsilon_z + 2\varepsilon_z v), \quad \text{(E.39)}$$

que é zero para $v = \frac{1}{2}$ e/ou $\varepsilon_z = 0$ (o limite de $\varepsilon_z \log(\varepsilon_z)$ é zero para $\varepsilon_z \to 0$). No entanto, derivando novamente a Eq. (E.39) em relação a v, se $\varepsilon_z = 0$ a derivada segunda é nula implicando que $\varepsilon_z = 0$ é um ponto de inflexão. Entretanto, para $v = 1/2$ a derivada segunda é $8(1-\varepsilon_z)\varepsilon_z/\ln(4)$, um número positivo, garantindo que temos um ponto de mínimo. Assim, substituindo os valores $v = 1/2$ na Eq. (E.36) obtemos

$$\begin{aligned} \lambda_1 &= 1 - \frac{2\varepsilon_x + \varepsilon_z}{2}, \\ \lambda_2 &= \frac{2\varepsilon_x - \varepsilon_z}{2}, \\ \lambda_3 &= \frac{\varepsilon_z}{2}, \\ \lambda_4 &= \frac{\varepsilon_z}{2}. \end{aligned} \quad \text{(E.40)}$$

Perceba que obtivemos o mesmo resultado da Sec. 6.1, ou seja, $\lambda_3 = \lambda_4$. Portanto ao aplicarmos o vínculo (6.13) desde o princípio não estamos facilitando a vida de Alice e Bob. Pelo contrário, ao aplicá-lo estamos considerando o melhor cenário para Eva.

E.2 Fração da chave secreta do protocolo GR10

Na Sec. 7.1 calculamos a fração da chave secreta $r = 1 - 2h(\varepsilon_x)$, Eq. (7.37), através da aplicação do vínculo das probabilidades $p_A(0) = p_A(1) = 1/2$. E esse vínculo originou que $\lambda_3 = \lambda_4 = \lambda$, Eq. (6.13). Aqui, não iremos aplicar esse vínculo e mostraremos que ele aparece naturalmente como pior cenário para Alice e Bob.

Iniciaremos nossa análise da mesma decomposição de Schmidt que nos levou a obter a

Eq. (7.37). Isto é, o estado compartilhado por Alice, Bob e Eva é a Eq. (7.6),

$$|\Psi\rangle_{ABE} = \sum_{j=1}^{4} \sqrt{\lambda_j} |\tilde{\Phi}_j\rangle_{AB} |\epsilon_j\rangle_E,$$

onde $|\tilde{\Phi}_i\rangle$ são as Eqs. (7.5), (7.7)-(7.9):

$$\begin{aligned} |\tilde{\Phi}_1\rangle &= \frac{1}{\sqrt{2}}(|{+}{+}\rangle + |{-}{-}\rangle), \\ |\tilde{\Phi}_2\rangle &= \frac{1}{\sqrt{2}}(|{+}{-}\rangle + |{-}{+}\rangle), \\ |\tilde{\Phi}_3\rangle &= |01\rangle\,, \\ |\tilde{\Phi}_4\rangle &= |10\rangle\,. \end{aligned} \tag{E.41}$$

Seguindo agora com o cálculo da informação mútua $I(A:B)$, Eq. (2.6), extraíremos as probabilidades a partir do operador densidade $|\Psi\rangle_{ABE}\langle\Psi|$, a Eq. (7.6). Aplicando as mesmas técnicas da seção anterior, encontramos

$$p_B(+) = p_B(-) = p_A(+) = p_A(-) = \frac{1}{2} \tag{E.42}$$

e que as probabilidades condicionais são (usando $\sum_{i=1}^{4} \lambda_i = 1$)

$$\begin{aligned} p_{B|A}(+|+) = p_{B|A}(-|-) &= \frac{1}{2}\left[1 + (\lambda_1 - \lambda_2)\right], \\ p_{B|A}(+|-) = p_{B|A}(-|+) &= \frac{1}{2}\left[1 - (\lambda_1 - \lambda_2)\right]. \end{aligned} \tag{E.43}$$

Usando a definição da entropia de Shannon, Eq. (2.1), e a Eq. (E.42), temos que a entropia clássica de Bob é

$$H(B) = h\left(\frac{1}{2}\right) = 1. \tag{E.44}$$

As Eqs. (E.43) e (E.42), quando aplicadas à definição da entropia condicional, Eq. (2.4), dá

$$H(B|A) = h\left[\frac{1}{2} - \frac{1}{2}(\lambda_1 - \lambda_2)\right]. \tag{E.45}$$

Por fim, juntando as Eqs. (E.44) e (E.45) na Eq. (2.6), obtemos a informação mútua entre Alice e Bob,

$$I(A:B) = 1 - h\left[\frac{1}{2} - \frac{1}{2}(\lambda_1 - \lambda_2)\right], \tag{E.46}$$

com $h(x) = -x\log x - (1-x)\log(1-x)$, Eq. (2.2).

Prosseguindo para a quantidade de Holevo, Eq. (2.105), a entropia quântica de Eva é obtida facilmente pois $\rho^E = \mathrm{tr}_{AB}\{|\Psi\rangle_{ABE}\langle\Psi|\}$ é diagonal. Portanto, pela definição de entropia quântica temos que

$$S(\rho^E) = -\sum_{i=1}^{4} \lambda_i \log(\lambda_i)\,. \tag{E.47}$$

A entropia quântica de Eva dado, que ela conheça a medida de Alice, é obtida pelo postulado da medida. Isto é,

$$\varrho_a^E = \mathrm{tr}_{AB}\left\{\frac{(|a\rangle_A\langle a|\otimes \mathbb{1}_{BE})\,|\Psi\rangle_{ABE}\langle\Psi|\,(|a\rangle_A\langle a|\otimes\mathbb{1}_{BE})}{\mathrm{tr}\{|\Psi\rangle_{ABE}\langle\Psi|\,(|a\rangle_A\langle a|\otimes\mathbb{1}_{BE})\}}\right\}.$$

Portanto

$$\begin{aligned}\varrho_+^E &= \sum_{j=1}^{4}\lambda_j\,|\epsilon_j\rangle_E\langle\epsilon_j| \\ &\quad +\sqrt{\lambda_1\lambda_3/2}\,(|\epsilon_1\rangle_E\langle\epsilon_3| + h.c.) + \sqrt{\lambda_1\lambda_4/2}\,(|\epsilon_1\rangle_E\langle\epsilon_4| + h.c.) \\ &\quad -\sqrt{\lambda_2\lambda_3/2}\,(|\epsilon_2\rangle_E\langle\epsilon_3| + h.c.) + \sqrt{\lambda_2\lambda_4/2}\,(|\epsilon_2\rangle_E\langle\epsilon_4| + h.c.)\,,\end{aligned} \tag{E.48}$$

$$\begin{aligned}\varrho_-^E &= \sum_{j=1}^{4}\lambda_j\,|\epsilon_j\rangle_E\langle\epsilon_j| \\ &\quad -\sqrt{\lambda_1\lambda_3/2}\,(|\epsilon_1\rangle_E\langle\epsilon_3| + h.c.) - \sqrt{\lambda_1\lambda_4/2}\,(|\epsilon_1\rangle_E\langle\epsilon_4| + h.c.) \\ &\quad +\sqrt{\lambda_2\lambda_3/2}\,(|\epsilon_2\rangle_E\langle\epsilon_3| + h.c.) - \sqrt{\lambda_2\lambda_4/2}\,(|\epsilon_2\rangle_E\langle\epsilon_4| + h.c.)\,,\end{aligned} \tag{E.49}$$

cujos autovalores são

$$\left\{0, 0, \frac{1}{2}\left[1 - \sqrt{(\lambda_1-\lambda_2)^2 + (\lambda_3-\lambda_4)^2}\right], \frac{1}{2}\left[1 + \sqrt{(\lambda_1-\lambda_2)^2 + (\lambda_3-\lambda_4)^2}\right]\right\}. \tag{E.50}$$

Com isso, aplicando a definição de entropia quântica, Eq. (2.24), encontramos

$$S(\varrho_+^E) = S(\varrho_-^E) = h\left[\frac{1}{2} - \frac{1}{2}\sqrt{(\lambda_1-\lambda_2)^2 + (\lambda_3-\lambda_4)^2}\right]. \tag{E.51}$$

Perceba que se tivéssemos $\lambda_3 = \lambda_4$, a Eq. (E.51) tornaria-se a entropia binária de $(1-\lambda_1+\lambda_2)/2$, o mesmo resultado de $S(\rho_+^E)$ e $S(\rho_-^E)$ da Sec. 7.1, como esperado.

Por fim, juntando as Eqs. (E.51) e (E.47) encontramos a quantidade de Holevo, Eq. (2.105),

$$\chi(A:\rho^E) = -\sum_{i=1}^{4}\lambda_i \log(\lambda_i) - h\left[\frac{1}{2} - \frac{1}{2}\sqrt{(\lambda_1-\lambda_2)^2+(\lambda_3-\lambda_4)^2}\right]. \tag{E.52}$$

Portanto, utilizando a informação mútua, Eq. (E.46), e a quantidade de Holevo, Eq. (E.52), na Eq. (2.122), obtemos

$$r = 1 - h\left[\frac{1}{2} - \frac{1}{2}(\lambda_1-\lambda_2)\right] + \sum_{i=1}^{4}\lambda_i \log(\lambda_i) + h\left[\frac{1}{2} - \frac{1}{2}\sqrt{(\lambda_1-\lambda_2)^2+(\lambda_3-\lambda_4)^2}\right]. \tag{E.53}$$

Com o auxílio das Eqs. (E.42) e (E.43), temos que as probabilidades conjuntas de Alice e Bob são

$$p_{A,B}(+,+) = p_{A,B}(-,-) = \frac{1}{4}(1+\lambda_1-\lambda_2), \tag{E.54}$$

$$p_{A,B}(+,-) = p_{A,B}(-,+) = \frac{1}{4}(1-\lambda_1+\lambda_2). \tag{E.55}$$

Portanto, a taxa de erro observada por Alice e Bob ao final da execução do protocolo é

$$\varepsilon_x = p_{A,B}(+,-) + p_{A,B}(-,+), \tag{E.56}$$

$$\varepsilon_x = \frac{1}{2}(1-\lambda_1+\lambda_2). \tag{E.57}$$

Resolvendo o seguinte conjunto de equações,

$$\begin{aligned} \varepsilon_x &= \frac{1}{2}(1-\lambda_1+\lambda_2), \\ 1 &= \lambda_1+\lambda_2+\lambda_3+\lambda_4, \end{aligned} \tag{E.58}$$

isto é, a Eq. (E.57) e a condição de normalização dos λ's, encontramos

$$\lambda_1 = 1 - \varepsilon_x - \frac{\lambda_3+\lambda_4}{2}, \tag{E.59}$$

$$\lambda_2 = \varepsilon_x - \frac{\lambda_3+\lambda_4}{2}. \tag{E.60}$$

Olhando atentamente para a Eq. (E.60), podemos dizer que $\lambda_3 + \lambda_4 \leq 2\varepsilon_x$, pois caso

contrário $\lambda_2 < 0$, o que não pode ocorrer. Portanto, nós temos que

$$\lambda_3 + \lambda_4 = 2b\varepsilon_x, \tag{E.61}$$

com b pertencente ao intervalo $[0, 1]$. Com isso, podemos escrever

$$\lambda_3 = 2b\varepsilon_x - \lambda_4. \tag{E.62}$$

E como $\lambda_3 \geq 0$, λ_4 deve ser menor ou igual que $2b\varepsilon_x$. Deste modo, temos que

$$\lambda_4 = v2b\varepsilon_x, \tag{E.63}$$

onde $v \in [0, 1]$. Escrevendo as Eqs. (E.59) - (E.63) em termos de v, b e ε_x temos

$$\begin{aligned}
\lambda_1 &= 1 - (1 + b)\varepsilon_x, && \text{(E.64)}\\
\lambda_2 &= (1 - b)\varepsilon_x, && \text{(E.65)}\\
\lambda_3 &= 2b(1 - v)\varepsilon_x, && \text{(E.66)}\\
\lambda_4 &= 2bv\varepsilon_x. && \text{(E.67)}
\end{aligned}$$

Substituindo as Eqs. (E.64)-(E.67) na Eq. (E.46) vemos que a informação mútua não depende de v e de b. Portanto, somente a quantidade de Holevo, Eq. (E.52), é uma função desses parâmetros. Consequentemente, devemos realizar uma maximização do χ para obtermos um limite inferior na taxa da chave secreta r.

No entanto, realizar a maximização desses dois parâmetros na Eq. (E.52) é muito difícil. Esse problema pode ser contornado se considerarmos o seguinte. A Eq. (E.52) pode ser dividida em dois grupos, a parte da entropia quântica de Eva composta por $\sum_{i=1}^{4} -\lambda_i \log(\lambda_i)$, que é positiva (veja teorema da Eq. (2.25)), e o negativo da entropia binária $h\left(\left[1 - \sqrt{(\lambda_1 - \lambda_2)^2 + (\lambda_3 - \lambda_4)^2}\right]/2\right)$. É o negativo dessa entropia binária que sempre diminui a quantidade de informação disponível à Eva, pois h é sempre positivo. Se considerarmos $h\left(\left[1 - \sqrt{(\lambda_1 - \lambda_2)^2 + (\lambda_3 - \lambda_4)^2}\right]/2\right) = 0$ na Eq. (E.52), estamos considerando a melhor situação possível para Eva. Ou seja, $\chi(A : \rho^e)_{max} = S(\rho^E)$ é o pior cenário possível para a segurança entre Alice e Bob. Sendo assim, considerando que a quantidade de Holevo é somente a entropia quântica de Eva,

$$\chi(A : \rho^e)_{max} = S(\rho^E) = \sum_{i=1}^{4} -\lambda_i \log(\lambda_i), \tag{E.68}$$

temos um limite inferior da fração da chave secreta.

Então, realizando a maximização para a Eq. (E.68) em relação aos parâmetro v e b, isto é, resolvendo o seguinte conjunto de equações,

$$\begin{cases} \dfrac{\mathrm{d}}{\mathrm{d}v}\displaystyle\sum_{i=1}^{4} -\lambda_i \log\left(\lambda_i\right) = 0, \\ \dfrac{\mathrm{d}}{\mathrm{d}b}\displaystyle\sum_{i=1}^{4} -\lambda_i \log\left(\lambda_i\right) = 0, \end{cases}$$

com λ_i dado pelas Eqs. (E.64)-(E.67) temos

$$b\left[\log\left(b(1-v)\varepsilon_x\right) - \log\left(bv\varepsilon_x\right)\right] = 0, \tag{E.69}$$

$$\log\left(\varepsilon_x - b\varepsilon_x\right) + \log\left(1-\varepsilon_x+b\varepsilon_x\right) - 2v\log\left(2bv\varepsilon_x\right) - 2(1-v)\log\left(2b(1-v)\varepsilon_x\right) = 0. \tag{E.70}$$

Note que consideramos $\varepsilon_x \neq 0$ nas expressões acima. A Eq. (E.69) é satisfeita se tivermos $v = 1/2$ ou $b = 0$. Considerando primeiro que $b \neq 0$ e $v = 1/2$, a Eq. (E.70) se reduz a

$$\log\left(\varepsilon_x - b\varepsilon_x\right) + \log\left(1 - (1+b)\varepsilon_x\right) - 2\log\left(b\varepsilon_x\right) = 0. \tag{E.71}$$

cuja solução é $b = 1 - \varepsilon_x$. Substituindo $b = 1 - \varepsilon_x$ e $v = 1/2$ nas Eqs. (E.64)-(E.67) encontramos

$$\lambda_1 = \left(1-\varepsilon_x\right)^2, \tag{E.72}$$

$$\lambda_2 = \varepsilon_x^2, \tag{E.73}$$

$$\lambda_3 = \left(1-\varepsilon_x\right)\varepsilon_x, \tag{E.74}$$

$$\lambda_4 = \left(1-\varepsilon_x\right)\varepsilon_x. \tag{E.75}$$

Se tivéssemos $b = 0$, teríamos $\lambda_3 = \lambda_4 = 0$ pelas Eqs. (E.65) e (E.66). Ou seja, em ambos os casos obteríamos o vínculo $\lambda_3 = \lambda_4$, Eq. (6.13).

Na Sec. E.3 provamos que a entropia quântica de Eva é menor para $b = 0$ do que para $b = 1-\varepsilon_x$ e $v = 1/2$. Portanto, o conjunto de Eqs. (E.72)-(E.75) formam o melhor cenário para Eva, de modo que estes valores devem ser considerados para o cálculo de r. Assim, substituindo as Eqs. (E.72)-(E.75) na Eq. (E.53) sem o termo $h\left(\left[1-\sqrt{(\lambda_1-\lambda_2)^2+(\lambda_3-\lambda_4)^2}\right]/2\right)$, pois o consideramos como sendo nulo, resulta que a taxa da chave secreta é

$$r = 1 - 3h\left(\varepsilon_x\right). \tag{E.76}$$

Na expressão acima $r > 0$ se $\varepsilon_x \lesssim 6.14\%$. Este resultado é menor que os 11% obtidos na Sec. 7.1, mas isso é devido a não aplicarmos o vínculo desde o princípio e desconsiderando o termo $h\left(\left[1-\sqrt{(\lambda_1-\lambda_2)^2+(\lambda_3-\lambda_4)^2}\right]/2\right)$ da expressão para r.

E.3 Qual o pior cenário dos para Alice e Bob?

Na seção E.2 temos os coeficientes representados pelas Eqs. (E.64)-(E.67),

$$\begin{aligned}\lambda_1 &= 1-(1+b)\varepsilon_x,\\ \lambda_2 &= (1-b)\varepsilon_x,\\ \lambda_3 &= 2b(1-v)\varepsilon_x,\\ \lambda_4 &= 2bv\varepsilon_x.\end{aligned}$$

E, considerando que o mínimo de segurança ocorra para $b = 0$, temos

$$\begin{aligned}\lambda_1 &= 1-\varepsilon_x,\\ \lambda_2 &= \varepsilon_x,\\ \lambda_3 &= 0,\\ \lambda_4 &= 0.\end{aligned}$$

Então, substituindo esses valores na entropia quântica de Eva, Eq. (E.47), resulta

$$s_1 = h\left(\varepsilon_x\right). \tag{E.77}$$

Em contrapartida, se temos $b = 1-\varepsilon_x$ e $v = 1/2$ obtemos as Eqs. (E.72)-(E.75),

$$\begin{aligned}\lambda_1 &= \left(1-\varepsilon_x\right)^2,\\ \lambda_2 &= \varepsilon_x^2,\\ \lambda_3 &= \left(1-\varepsilon_x\right)\varepsilon_x,\\ \lambda_4 &= \left(1-\varepsilon_x\right)\varepsilon_x.\end{aligned}$$

E, ao calcularmos a entropia quântica de Eva encontramos

$$s_2 = 2h\left(\varepsilon_x\right). \tag{E.78}$$

Nosso objetivo aqui é provar que $s_1 \leq s_2$, de modo que a escolha dos λ's como sendo as Eqs. (E.72)-(E.75) é o melhor cenário para Eva.

Subtraindo a Eq. (E.78) da Eq. (E.77) encontramos

$$s_2 - s_1 = h\left(\varepsilon_x\right). \tag{E.79}$$

que sempre é maior que zero se $\varepsilon_x > 0$. Logo, $s_2 > s_1$ e justificamos a escolha $b = 1 - \varepsilon_x$ e $v = 1/2$ como melhor cenário para Eva.

Apêndice F

O valor de p em uma base generalizada

A probabilidade de Bob obter um determinado estado teletransportado por Alice depende dos resultados das medidas de Bell generalizada obtidos por ela:

$$\begin{aligned}
|\Phi_1^n\rangle &= \frac{1}{\sqrt{1+n^2}}\left(|00\rangle + n\,|11\rangle\right), \\
|\Phi_2^n\rangle &= \frac{1}{\sqrt{1+n^2}}\left(n\,|00\rangle - |11\rangle\right), \\
|\Phi_3^n\rangle &= \frac{1}{\sqrt{1+n^2}}\left(|01\rangle + n\,|10\rangle\right), \\
|\Phi_4^n\rangle &= \frac{1}{\sqrt{1+n^2}}\left(n\,|01\rangle - |10\rangle\right),
\end{aligned} \tag{F.1}$$

com n o real variando de zero a um.

De modo geral, Alice quer teletransportar um dos dois estados que codificam os bits 0 e 1, $|v_0\rangle$ ou $|v_1\rangle$. De modo geral, estes estados são definidos em relação a base z como

$$\begin{aligned}
|v_0\rangle &= \cos\left(\frac{\theta}{2}\right)|0\rangle + \mathrm{e}^{\mathrm{i}\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle, \\
|v_1\rangle &= \sin\left(\frac{\theta}{2}\right)|0\rangle - \mathrm{e}^{\mathrm{i}\phi}\cos\left(\frac{\theta}{2}\right)|1\rangle,
\end{aligned} \tag{F.2}$$

com θ o ângulo azimutal e ϕ o ângulo polar na esfera de Bloch [34]. Para que Alice teletransporte seu estado a Bob, ele envia um *qubit* do canal $|\Phi_1^n\rangle$, Eq. (F.1), com o $n = n_1$ ou $n = n_2$. Alice escolhe aleatoriamente um dos *qubits* que quer teletransportar e faz sua

medida de Bell generalizada escolhendo $k = n_1$ ou $k = n_2$. Assim, se Alice quer teleportar o estado $|v_0\rangle$, o estado inicial compartilhado por Alice e Bob, antes de Alice aplicar a medida de Bell generalizada será

$$\varrho_{0_{\theta\phi}}^{AB} = |v_0\rangle_A\langle v_0| \otimes |\Phi_1^n\rangle_{AB}\langle\Phi_1^n| \,. \tag{F.3}$$

E se ela quer teleportar $|v_1\rangle$ o estado será

$$\varrho_{1_{\theta\phi}}^{AB} = |v_1\rangle_A\langle v_1| \otimes |\Phi_1^n\rangle_{AB}\langle\Phi_1^n| \,. \tag{F.4}$$

Dependendo de qual estado de Bell generalizado Alice obtém na sua medida, $|\Phi_1^k\rangle$, $|\Phi_2^k\rangle$, $|\Phi_3^k\rangle$ ou $|\Phi_4^k\rangle$, Bob aplica a transformação unitária correspondente em seu *qubit* como visto na Sec. 3.2. As fórmulas para encontrar as probabilidades de Alice e Bob dependendo das transformações aplicadas seguem abaixo:

$$\begin{aligned}
p_{B|A}(b|\Phi_1^k a) &= \mathrm{tr}\left\{\varrho_{a_{\theta\phi}}^{AB}\left(|\Phi_1^k\rangle_A\langle\Phi_1^k| \otimes |b\rangle_B\langle b|\right)\right\}, \\
p_{B|A}(b|\Phi_2^k a) &= \mathrm{tr}\left\{(\mathbb{1}_A \otimes \sigma_{zB})\,\varrho_{a_{\theta\phi}}^{AB}\,(\mathbb{1}_A \otimes \sigma_{zB})\left(|\Phi_2^k\rangle_A\langle\Phi_2^k| \otimes |b\rangle_B\langle b|\right)\right\}, \\
p_{B|A}(b|\Phi_3^k a) &= \mathrm{tr}\left\{(\mathbb{1}_A \otimes \sigma_{xB})\,\varrho_{a_{\theta\phi}}^{AB}\,(\mathbb{1}_A \otimes \sigma_{xB})\left(|\Phi_3^k\rangle_A\langle\Phi_3^k| \otimes |b\rangle_B\langle b|\right)\right\}, \\
p_{B|A}(b|\Phi_4^k a) &= \mathrm{tr}\left\{[\mathbb{1}_A \otimes (\sigma_z\sigma_x)_B]\,\varrho_{a_{\theta\phi}}^{AB}\,[\mathbb{1}_A \otimes (\sigma_x\sigma_z)_B]\left(|\Phi_4^k\rangle_A\langle\Phi_4^k| \otimes |b\rangle_B\langle b|\right)\right\}.
\end{aligned} \tag{F.5}$$

Sendo assim, utilizando a Eq. (F.5), a probabilidade de Bob obter $|v_0\rangle$ dado que Alice teletransportou este mesmo estado e mediu o estado de Bell $|\Phi_j^k\rangle$ é

$$\begin{aligned}
p_{B|A}(v_0|\Phi_1^k v_0) &= \frac{[1 + kn + (1 - kn)\cos(\theta)]^2}{4(1 + k^2)(1 + n^2)}, \\
p_{B|A}(v_0|\Phi_2^k v_0) &= \frac{[k + n + (k - n)\cos(\theta)]^2}{4(1 + k^2)(1 + n^2)}, \\
p_{B|A}(v_0|\Phi_3^k v_0) &= \frac{[k + n - (k - n)\cos(\theta)]^2}{4(1 + k^2)(1 + n^2)}, \\
p_{B|A}(v_0|\Phi_4^k v_0) &= \frac{[1 + kn - (1 - kn)\cos(\theta)]^2}{4(1 + k^2)(1 + n^2)}.
\end{aligned} \tag{F.6}$$

Perceba que as probabilidades (F.6) dependem de k, n e somente de θ. De fato, o n é devido a escolha do canal que foi feita a transmissão e k é o valor escolhido por Alice para aplicar a medida de Bell. A informação nova que temos aqui é a independência das probabilidades em relação ao ângulo ϕ. Ou seja, ao escolhermos uma base com $\theta = \theta_1$

e $\phi = 0$, qualquer outra base que possui o ângulo $\theta = \theta_1$ e $\phi \neq 0$ possuirá as mesmas probabilidades.

Alice, pelo protocolo, tem 50% de chance de escolher se ela vai teleportar o *qubit* $|v_0\rangle$ ou o $|v_1\rangle$. Ou seja, $p_A(v_0) = p_A(v_1) = 1/2$. Portanto, a probabilidade total de Bob ver $|v_0\rangle$ se Alice teletransportou $|v_0\rangle$ é

$$p_{A,B}(v_0, v_0) = p_A(v_0) \sum_i^4 p_{B|A}(v_0|\Phi_i^k v_0) = \frac{1}{2} \sum_i^4 p_{B|A}(v_0|\Phi_i^k v_0). \tag{F.7}$$

Substituindo $p_{B|A}(v_0|\Phi_i^k v_0)$ dado pela Eq. (F.6) obtemos

$$p_{A,B}(v_0, v_0)\Big|_{k,n} = \frac{(1+kn)^2 + (k+n)^2 + [(1-kn)^2 + (k-n)^2]\cos^2(\theta)}{4(1+k^2)(1+n^2)}, \tag{F.8}$$

cujo valor depende do canal escolhido por Bob, n, e da base que Alice utilizou em sua medida, k.

Usando a Eq. (F.5) com Alice ainda teletransportando $|v_0\rangle$, a probabilidade de Bob obter $|v_1\rangle$, isto é, medir um valor diferente do enviado por Alice é

$$\begin{aligned} p_{B|A}(v_1|\Phi_1^k v_0) = p_{B|A}(v_1|\Phi_4^k v_0) &= \frac{(1-kn)^2 \sin^2(\theta)}{4(1+k^2)(1+n^2)}, \\ p_{B|A}(v_1|\Phi_2^k v_0) = p_{B|A}(v_1|\Phi_3^k v_0) &= \frac{(k-n)^2 \sin^2(\theta)}{4(1+k^2)(1+n^2)}. \end{aligned} \tag{F.9}$$

Dessa forma, a probabilidade total de Bob divergir do *qubit* de Alice é

$$p_{A,B}(v_1, v_0)\Big|_{k,n} = \frac{[(1-kn)^2 + (k-n)^2]\sin^2(\theta)}{4(1+k^2)(1+n^2)}. \tag{F.10}$$

Realizando os mesmos cálculos com Alice teletransportando $|v_1\rangle$ encontramos que a probabilidade $p_{A,B}(v_1, v_1)|_{k,n}$ é a mesma que a probabilidade de Alice teletransportar $|v_0\rangle$ e Bob obter $|v_0\rangle$, Eq. (F.8), e que a probabilidade $p_{A,B}(v_0, v_1)|_{k,n} = p_{A,B}(v_1, v_0)|_{k,n}$, Eq. (F.10).

Nas Secs. 7.2 e 7.2.1 nós consideramos três diferentes *ensembles* para os estados da base x. São eles, p, p_M e p_{P_1}, respectivamente as Eqs. (7.54), (7.89) e (7.91). Nesta seção, encontraremos essas probabilidades para uma base generalizada.

A escolha de Bob e Alice para os valores de n e k é aleatória, assim como o *qubit* que Alice quer teleportar. Assim sendo, cada um destes eventos tem probabilidade de 50% de ocorrer.

Para o primeiro caso, onde todos os eventos são considerados, a probabilidade de Alice e Bob terem os mesmos *qubits*, $\tilde{p}$, é a seguinte,

$$\begin{aligned}\tilde{p} =& p_A(n_1)p_B(n_1)p_{A,B}(v_0,v_0)\Big|_{\substack{k=n_1\\n=n_1}} + p_A(n_1)p_B(n_2)p_{A,B}(v_0,v_0)\Big|_{\substack{k=n_1\\n=n_2}} \\ &+ p_A(n_2)p_B(n_1)p_{A,B}(v_0,v_0)\Big|_{\substack{k=n_2\\n=n_1}} + p_A(n_2)p_B(n_2)p_{A,B}(v_0,v_0)\Big|_{\substack{k=n_2\\n=n_2}},\end{aligned} \tag{F.11}$$

onde $p_A(n_i)$ e $p_B(n_i)$ são as probabilidades de eles escolherem n_i. Como n e k são escolhidos aleatoriamente temos que $p_A(n_i) = p_B(n_j) = 1/2$. Com isso e a Eq. (F.8) encontramos que

$$\tilde{p} = \frac{1}{2} - \frac{1}{4}\left(1 - \frac{(n_1+n_2)^2(1+n_1n_2)^2}{\left(1+n_1^2\right)^2\left(1+n_2^2\right)^2}\right)\sin^2(\theta). \tag{F.12}$$

A segunda combinação, $\tilde{p}_{P_1}$, considera somente os caso em que Alice escolheu $k = n_1$ ou n_2 para a medida e Bob sempre enviou o canal $n = n_1$:

$$\begin{aligned}\tilde{p}_{P_1} =& p_A(n_1)p_{A,B}(v_0,v_0)\Big|_{\substack{k=n_1\\n=n_1}} + p_A(n_2)p_{A,B}(v_0,v_0)\Big|_{\substack{k=n_2\\n=n_1}}, \\ =& \frac{1}{2}\left(p_{A,B}(v_0,v_0)\Big|_{\substack{k=n_1\\n=n_1}} + p_{A,B}(v_0,v_0)\Big|_{\substack{k=n_2\\n=n_1}}\right).\end{aligned} \tag{F.13}$$

Substituindo $p_{A,B}(v_0,v_0)$ dado pela Eq. (F.8) encontramos

$$\tilde{p}_{P_1} = \frac{1}{2} - \frac{1}{4}\left(1 - \frac{2n_1(n_1+n_2)(1+n_1n_2)}{\left(1+n_1^2\right)^2\left(1+n_2^2\right)^2}\right)\sin^2(\theta). \tag{F.14}$$

O último *ensemble* é aquele para o qual consideramos somente os casos em que a condição de *matching* é satisfeita, ou seja, os caso em que Alice e Bob utilizam o mesmo valor para n e k:

$$\tilde{p}_M = \frac{1}{\mathcal{N}}\left(p_{A,B}(v_0,v_0)\Big|_{\substack{k=n_1\\n=n_1}} + p_{A,B}(v_0,v_0)\Big|_{\substack{k=n_2\\n=n_2}}\right), \tag{F.15}$$

onde

$$\begin{aligned}\mathcal{N} =& 2\left(p_{A,B}(v_0,v_0)\Big|_{\substack{k=n_1\\n=n_1}} + p_{A,B}(v_0,v_0)\Big|_{\substack{k=n_2\\n=n_2}}\right. \\ &\left. + p_{A,B}(v_0,v_1)\Big|_{\substack{k=n_1\\n=n_1}} + p_{A,B}(v_0,v_1)\Big|_{\substack{k=n_2\\n=n_2}}\right).\end{aligned} \tag{F.16}$$

A Eq. (F.16) é multiplicada por 2 devido a termos $p_{A,B}(v_1, v_1) = p_{A,B}(v_0, v_1)$ e $p_{A,B}(v_0, v_1) = p_{A,B}(v_1, v_0)$ inclusas na normalização. Aplicando as Eqs. (F.8) e (F.10) nas Eqs. (F.16) e (F.15) encontramos que a probabilidade nos eventos com *matching* é

$$\tilde{p}_M = \frac{1}{2} - \frac{1}{4}\left(1 - \frac{2n_1^2}{(1+n_1^2)^2} - \frac{2n_2^2}{(1+n_2^2)^2}\right)\sin^2(\theta), \tag{F.17}$$

que também é simétrica pela troca de $n_1 \leftrightarrow n_2$.

Referências Bibliográficas

[1] S. Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* (First Anchor Books Edition, New York, 2000).

[2] R. Rivest, A. Shamir, and L. Adleman, MIT Laboratory for Computer Science, Technical Report, MIT/LCS/TR-212, 1979.

[3] P. Shor, SIAM Journal of Computing **26**, 1484 (1997).

[4] C. H. Bennett, and G. Brassard, Quantum cryptography: public key distribution and coin tossing, in: Proceedings of the IEEE International Conference on Computers Systems and Signal Processing, Bangalore, India, 1984, p. 175.

[5] B. Scheneier, *Applied Cryptography: Protocolos, Algorithms, and Source Code in C* (John Wiley & Sons, 2015).

[6] S. Levy, *Crypto: How the Code Rebels Beat the Government–Saving Privacy in the Digital Age* (Penguin Publishing Group, 2001).

[7] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[8] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[9] Ch. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).

[10] http://www.idquantique.com.

[11] http://www.magiqtech.com.

[12] https://www.quintessencelabs.com.

[13] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[14] W. K. Wootters, and W. H. Zurek, Nature (London) **299**, 802 (1982).

[15] D. Dieks, Phys. Lett. **92A**, 271 (1982).

[16] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W.K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[17] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).

[18] G. Gordon, and G. Rigolin, Opt. Commun. **283**, 184 (2010).

[19] W.-Li Li, C.-Feng Li, and G.-C. Guo, Phys. Rev. A **61**, 034301 (2000).

[20] P. Agrawal, and A. K. Pati, Phys. Lett. A **305**, 12 (2002).

[21] G. Gordon, and G. Rigolin, Phys. Rev. A **73**, 042309 (2006).

[22] G. Gordon, and G. Rigolin, Phys. Rev. A **73**, 062316 (2006).

[23] G. Gordon, and G. Rigolin, Eur. Phys. J. D **45**, 347 (2007).

[24] G. Rigolin, J. Phys. B: At. Mol. Opt. Phys. **42**, 235504 (2009).

[25] R. Fortes, and G. Rigolin, Ann. Phys. (N.Y.) **336**, 517 (2013).

[26] R. Fortes, and G. Rigolin, Phys. Rev. A **92**, 012338 (2015).

[27] R. Fortes, and G. Rigolin, Phys. Rev. A **93**, 062330 (2016).

[28] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[29] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

[30] L. Goldenberg, and L. Vaidman, Phys. Rev. Lett. **75**, 1239 (1995).

[31] M. Koashi, and N. Imoto, Phys. Rev. Lett. **79**, 2383 (1997).

[32] C. Shukla, A. Banerjee, A. Pathak, and R. Srikanth, Int. J. Quantum. Inform. **6**, 1640021 (2016).

[33] M. M. Wilde, *Quantum Information Theory* (Cambridge University Press, New York, 2013).

[34] M. A. Nielsen, and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2010).

[35] M. A. Nielsen, and D. Petz, Quantum Inf. Comput. **5**, 507 (2005).

[36] A. S. Holevo, Probl. Inf. Transm. **9**, 177 (1973).

[37] T. M. Cover, and J. A. Thomas, *Elements of Information Theory* (Wiley and Sons, New York, 1991).

[38] C.E. Shannon, Bell Syst. Tech J. **27**, 379; 623 (1948).

[39] I. Devetak, and A. Winter, Proc. R. Soc. London, Ser. A **461**, 207 (2005).

[40] J. von Neumann,*Mathematical Foundations of Quantum Mechanics* (Princeton University Press, Princeton, 1996).

[41] P. W. Shor, and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[42] H.-K. Lo, Quantum Inf. Comput. **1**, 81 (2001).

[43] L. P. Hughston, R. Jozsa, and W. K. Wootters, Phys. Lett. A **183**, 14 (1993).

[44] B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. **95**, 080501 (2005).

[45] R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005).

[46] R. Renner, Nat. Phys. **3**, 645 (2007).

[47] R. Renner, and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).

[48] C.H. Bennett, G. Brassard, S. Bredibart, and S. Wiesner, IBM Tech. Discl. Bull. **26**, 4363 (1984).

[49] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).

[50] H. Bechmann-Pasquinucci, and N. Gisin, Phys. Rev. A **59**, 4238 (1999).

[51] E. Prugovečki, *Quantum Mechanics in Hilbert Space*, Pure and applied mathematics: a series of monographs and textbooks (Academic Press, 1971).

[52] J. Bae, and A. Acín, Phys. Rev. A **75**, 012334 (2007).

[53] D. Lima, and G. Rigolin, Quantum Inf. Process. **19**, 201 (2020).

[54] S. Boyd, and L. Vanderberghe, *Convex Optimization* (Cambridge University Press, 2004).

[55] E. L. Lima, *Curso de Análise*, Projeto Euclides (IMPA, 1989).