UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
CENTRO DE CIÊNCIAS E TECNOLOGIA
UNIDADE ACADÊMICA DE FÍSICA
COORDENAÇÃO DE PÓS-GRADUAÇÃO EM FÍSICA

DISSERTAÇÃO DE MESTRADO

Segurança dos Protocolos BB84 e B92 Sob Ataques Individuais

Naiara de Souza Barros

CAMPINA GRANDE
- Agosto 2016 -

UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
CENTRO DE CIÊNCIAS E TECNOLOGIA
UNIDADE ACADÊMICA DE FÍSICA
COORDENAÇÃO DE PÓS-GRADUAÇÃO EM FÍSICA

DISSERTAÇÃO DE MESTRADO

Segurança dos Protocolos BB84 e B92 Sob Ataques Individuais

Naiara de Souza Barros

Dissertação apresentada ao Programa de Pós-Graduação em Física da Universidade Federal de Campina Grande, como requisito parcial para obtenção do Grau de Mestre em Física.

Área de Concentração: Física da Matéria Condensada.
Orientador: Prof. Dr. Aercio F. de Lima

CAMPINA GRANDE
- Agosto 2016 -

Segurança dos Protocolos BB84 e B92 Sob Ataques Individuais

Naiara de Souza Barros

Aprovada em _____

Banca Examinadora

Prof. Dr. Aercio F. de Lima

Orientador

Prof. Dr. Rafael de Lima Rodrigues

Examinador Externo

Prof. Dr. Danieverton Moretti

Examinador Interno

"*O Senhor é o meu pastor: nada me faltará.*"
Salmos 23:1

Agradecimentos

Agradeço a Deus por ter me dado força para chegar até aqui. Agradeço à CAPES pelo financiamento do trabalho, à Unidade Acadêmica de Física e aos professores que contribuíram na construção do conhecimento necessário para a realização desse trabalho, ao professor Dr. Aercio F. Lima pela orientação deste trabalho e ao professor Dr. Danieverton Moretti por ceder o suporte necessário para o estudo. Agradeço aos amigos que ajudaram durante todo o mestrado: Hebertt Leandro, Stefane Judith. Agradeço a minha mãe Maria do Rosário, pelo apoio e incentivo aos estudos.

À minha família.

Lista de Figuras

Sumário

Resumo

Esta dissertação apresenta uma análise dos dois primeiros protocolos que foram propostos para uma troca de chave de forma segura. O primeiro protocolo foi implementado por Bennett e Brassard em 1984, atualmente conhecido como BB84, e o segundo protocolo foi implementado por Bennett em 1992, conhecido como B92. Após apresentarmos uma fundamentação teórica básica necessária para a compreensão desses protocolos, introduzimos e analisamos a segurança dos mesmos sobre um ataque individual em que um espião utiliza um procedimento de espionagem translúcida que interage com os protocolos de forma a obter mais informação sobre as mensagens secretas que estão sendo transmitidas pelos protocolos.

Palavras-chave: Bennett - Brassad - BB84 - B92 - Ataque individual - Espionagem translúcida.

Abstract

This paper presents an analysis of the first two protocols to be proposed for a secure key exchange. The first protocol was implemented by Bennett and Brassard in 1984, presently known as BB84 and the second protocol is implemented by Bennett in 1992, known as B92. After presenting a basic theoretical foundation necessary for an understanding of these protocols, we introduce and analyze the security of the same on an individual attack in which a eavesdropper uses a translucent eavesdropping procedure that interacts with the protocols in order to obtain more information about the secret messages they are being transmitted by the protocols.

Keywords: Bennett - Brassard - BB84 - B92 - Individual attack - Translucent eavesdropping.

Capítulo 1

Introdução

A criptografia quântica é uma técnica que permite que dois usuários legítimos de um canal, troquem informações secretas utilizando protocolos de distribuição quântica de chaves. Uma distribuição de chave segura permite que os dois usuários legítimos, produzam duas cópias idênticas de sequências de bits secretas e aleatórias, uma para cada usuário. Essa sequência aleatória aparentemente sem sentido para uma parte não autorizada é chamada de chave, que pode ser utilizada para encriptar mensagens entre os dois usuários. A segurança dessa mensagem criptografada, e de toda comunicação em geral, depende diretamente da segurança da distribuição dessa chave.

Na presença de um espião, os usuários legítimos devem entrar em acordo de qual protocolo utilizar para a distribuir a chave. Para essa escolha, dever ser levado em consideração a análise de qual protocolo é mais resistente a um espião que possue equipamentos computacionais ilimitado. Os primeiros protocolos introduzidos nesse campo, foram os protocolos BB84 [1], Ekert91 e B92 [2]. O BB84 e B92 são bastante similares, mas com um diferencial de que, o protocolo B92 utiliza apenas dois estados não-ortogonais e, em contra partida, o protocolo BB84 utiliza quatro estados, dois pares de estados ortogonais em que cada par utiliza um base conjugada. Apesar dessa diferença, os dois fazem o uso de princípios de segurança de forma similar. Já o protocolo Ekert91, utiliza estados emaranhados para garantir a sua segurança. E isso é um problema experimentalmente, pois, com a tecnologia atual, é difícil de implementar em canais ruidosos. Por esse motivo não o analisaremos nesse trabalho.

Este trabalho portanto, representa um esforço no sentido de clarear a compreensão de dois protocolos básicos, na qual se fundamenta a ideia da segurança na criptografia quântica.

Antes de analisarmos esses protocolos em ação, introduzimos nas seções seguintes fundamentações teóricas que são de grande utilidade para uma boa compreensão das análises dos protocolos.

Capítulo 2

Breve introdução à teoria da informação

Inicialmente, nessa breve introdução à teoria da informação, gostaria de definir o que é informação na teoria, mas não posso pois ela não é bem definida como no cotidiano onde a informação é a ação de informar ou de se informar. Isso se dá, pelo fato de que a teoria da informação é incapaz de nos dizer o que ela é. Ao longo dos estudos só somos capazes de ter uma percepção do que ela possa representar através do cálculo da entropia. E esse é um dos objetivos da teoria , medir a informação.

Os outros objetivos da teoria são: a transmissão de dados através de sistemas que permitem a correção de erros de modo que preservem os dados; a compressão de dados que possibilite uma transmissão curta e acelerada; e a criptografia que permite uma transmissão segura e sigilosa. De acordo com [3], essas três aplicações da teoria são fundamentais para a comunicação.

Agora, vamos iniciar os estudos a partir da entropia, que é o ponto inicial para o entendimento da teoria.

2.1 Entropia

A partir dos trabalhos de Boltzmann sobre a mecânica estatística, foi possível obter uma maior clareza sobre a entropia. Ele nos apresenta a entropia como a medida natural da desordem de um sistema físico. Mas, para a teoria da informação isso não é cabível, já que informação é o oposto de desordem. Quando pensamos em informação associamos a

conhecimenos ou fatos, por exemplo, um jornal só tem muitos expectadores se apresentar notícias novas, caso o jornal apresente várias vezes a mesma notícia já não terá tanta credibilidade, pois notícias que se repetem várias vezes tem pouca informação. Com isso em mente, podemos observar que, quanto mais novo for o fato ou o conhecimento mais informação iremos obter, pois fatos novos ou inesperados geram uma grande surpresa, e isso nos leva a presumir que a informação está ligada a ocorrência de evento. Shannon foi um dos precursores da teoria da informação, e em um dos seus trabalhos ele elucidou a medida da informação como sendo a entropia, H, e explanou-a da seguinte forma: Dada uma fonte com um espaço amostral X, que emite N símbolos com respectivas probabilidades $p_i\,(i = 1, 2, ..., N)$. A incerteza média sobre os valores da fonte X é medida por

$$H\left(X\right) = -\sum_{i=1}^{N} p_i \log_2 p_i, \tag{2.1}$$

que é a entropia de Shannon.

Por conveniência, utiliza-se o logaritmo na base 2, isso faz com que a unidade da medida da informação seja o bit, que é a abreviação de "dígito binário". O bit é a quantidade exata necessária para descrever o resultado da medida. Por exemplo, $N = 2^q$ símbolos equiprováveis, podem ser representados por $\log_2 N = \log_2 2^q = q$bits. Também poderiamos ter escolhido a representação na base 3 ou na base 4 definidos, respectivamente, por 'trit' e 'quad' unidades de informação. Mas, o bit é a unidade mais elementar e não pode ser fatiado para uma dimensão menor.

Já na mecânica quântica, os estados quânticos são descritos por operadores densidade ao invés de distribuições de probabilidades. Esses operadores densidade são hermitianos e positivos, que podem ser escritos na forma

$$\rho = \sum_{j} p_j \left|\psi_j\right\rangle \left\langle\psi_j\right|, \tag{2.2}$$

em que p_i é a probabilidade associada ao estado $\left|\psi_j\right\rangle$ e possuem o traço unitário, $tr\left(\rho\right) = 1$. Como a função traço independe da base escolhida, von Neumann definiu a entropia de

um estado quântico como

$$
\begin{aligned}
S(\rho) &= -tr(\rho \log \rho) \qquad (2.3)\\
&= -\sum_i \langle \psi_i | \rho \log \rho | \psi_i \rangle \\
&= -\sum_i \langle \psi_i | \left(\sum_j p_j |\psi_j\rangle \langle \psi_j| \right) \log \left(\sum_j p_j |\psi_j\rangle \langle \psi_j| \right) |\psi_i\rangle \\
&= -\sum_i \sum_j \langle \psi_i | p_j |\psi_j\rangle \langle \psi_j| \log \left(\sum_j p_j |\psi_j\rangle \langle \psi_j| \right) |\psi_i\rangle \\
&= -\sum_{i,j} p_j \underbrace{\langle \psi_i | \psi_j \rangle}_{\delta_i j} \log \left(\sum_j p_j \underbrace{\langle \psi_j | \psi_j \rangle}_{1} \underbrace{\langle \psi_j | \psi_i \rangle}_{\delta_i j} \right) \\
&= -\sum_i p_i \log p_i. \qquad (2.4)
\end{aligned}
$$

Comparando as duas entropias, vemos que são intrinsecamente análogas. A diferença entre elas é que, agora, a fonte é um sistema quântico caracterizado por um operador densidade ρ e não por uma distribuição de probabilidade. E, a entropia de von Neumann representa uma medida quântica de informação contida em um sistema ou estado quântico referente a uma fonte quântica, e a sua unidade de medida é o q-bit (ou qubit) que é o bit quântico de sistemas quânticos com dois níveis de energia.

Se um operador densidade ρ é positivo e possue um traço igual a 1, então ele tem uma decomposição espectral

$$\rho = \sum_i \lambda_i |\lambda_i\rangle \langle \lambda_i| , \qquad (2.5)$$

em que λ_i são os autovalores reais e não-negativos de ρ, e $|\lambda_i\rangle$ são os respectivos autoestados. Assim, a entropia de von Neumann toma a forma

$$S(\rho) = -\sum_i \lambda_i \log \lambda_i. \qquad (2.6)$$

A entropia de von Neumann é ordinariamente escrita na forma

$$S(\rho) = -k_B tr(\rho \ln \rho), \qquad (2.7)$$

em que k_B é a constante de Boltzmann e ln é o logaritmo natural. Essa expressão aparece naturalmente na mecânica estatística e difere da Eq. (2.3) por uma constante multiplicativa, mas não há diferença fundamental entre elas, apenas a unidade da entropia fornecida

é que muda entre ela.

Nesta seção apresentamos os problemas mais simples dos quais apenas eventos independentes como uma única fonte discreta X e um único estado quântico ρ são propostos, mas são poucos os problemas que utilizam apenas um evento e é por isso que a próxima seção será dedicada ao estudo da entropia na ocorrência de mais de um evento. A fim de simplificar os estudos, optaremos apenas para a ocorrência de dois eventos, tanto clássicos quanto quânticos.

2.2 Entropias relativa, conjunta e condicional

Como vimos anteriormente, a entropia está intrisicamente ligada a distribuição de probabilidade, e por isso, as entropias conjunta e condicional, estão ligadas as probabilidades conjunta e condicional, respectivamente. Já a entropia relativa é uma medida da distância entre duas distribuições de probabilidades de uma mesma fonte. Para fins didáticos, daremos início ao estudo introduzindo a definição de entropia conjunta.

Considere dois eventos $x \in X$ e $y \in Y$, em que X e Y são duas fontes. Um evento conjunto acontece quando há a ocorrência dos dois eventos x e y. E a probabilidade conjunta de observar dois eventos simultâneos é dada por

$$p(x,y) = p(x)p(y) = p(y)p(x) = p(y,x), \tag{2.8}$$

em que a distribuição conjunta é simétrica, e possui as seguintes propriedades

$$\begin{aligned} &\sum_{y\in Y} p(x,y) = p(x), \\ &\sum_{x\in X} p(x,y) = p(y), \\ &\sum_{y\in Y}\sum_{x\in X} p(x,y) = 1. \end{aligned} \tag{2.9}$$

Agora podemos definir a entropia conjunta, $H(X,Y)$, como

$$H(X,Y) = -\sum_{y\in Y}\sum_{x\in X} p(x,y)\log p(x,y), \tag{2.10}$$

que representa a informação média resultante dos eventos conjuntos que ocorrem a partir de duas fonte X e Y. E sua versão quântica tem a forma

$$S(A,B) = S(\rho_{AB}) = -tr\left(\rho_{AB}\log\rho_{AB}\right), \tag{2.11}$$

em que ρ_{AB} é o operador densidade do sistema composto (A, B). Sendo ρ_A e ρ_B os operadores densidade dos sistemas A e B, respectivamente, e que podem ser separados, $\rho_{AB} = \rho_A \otimes \rho_B$, de forma que possibilita escrever a entropia quântica conjunta como

$$S(\rho_{AB}) \;=\; -tr\left[(\rho_A \otimes \rho_B)\log(\rho_A \otimes \rho_B)\right].$$

Como é sabido que,

$$\log(\rho_A \otimes \rho_B) = \log(\rho_A) \otimes I_B + I_A \otimes \log\,(\rho_B),$$

logo,

$$\begin{aligned}
S(\rho_{AB}) &= -tr\left\{(\rho_A \otimes \rho_B)\left[\log(\rho_A) \otimes I_B + I_A \otimes \log\,(\rho_B)\right]\right\} \\
&= -tr\left[(\rho_A \log \rho_A) \otimes \rho_B + \rho_A \otimes (\rho_B \log \rho_B)\right] \\
&= -tr\left[(\rho_A \log \rho_A) \otimes \rho_B\right] - tr\left[\rho_A \otimes (\rho_B \log \rho_B)\right] \\
&= -\sum_{i,j} {}_A\langle\psi_i|\,{}_B\langle\psi_j|\,(\rho_A \log \rho_A \otimes \rho_B)\,|\psi_j\rangle_B\,|\psi_i\rangle_A \\
&\quad -\sum_{i,j} {}_A\langle\phi_i|\,{}_B\langle\phi_j|\,(\rho_A \otimes \rho_B \log \rho_B)\,|\phi_j\rangle_B\,|\phi_i\rangle_A \\
&= -\sum_{i} {}_A\langle\psi_i|\,\rho_A \log \rho_A\,|\psi_i\rangle_A \underbrace{\sum_{j} {}_B\langle\psi_j|\,\rho_B\,|\phi_j\rangle_B}_{1} \\
&\quad -\underbrace{\sum_{i} {}_A\langle\phi_i|\,\rho_A\,|\phi_i\rangle_A}_{1} \sum_{j} {}_B\langle\phi_j|\,\rho_B \log \rho_A\,|\phi_j\rangle_B \\
&= -tr_A(\rho_A \log \rho_A) - tr_B(\rho_B \log \rho_B) \\
&= S(\rho_A) + S(\rho_B). \qquad (2.12)
\end{aligned}$$

A Eq.(2.12) é a entropia de von Neumann conjunta de dois sistemas não correlacionados. Agora, iremos dirigir nosso estudo para a definição de probabilidade condicional, $p(b|a)$, que é a probabilidade que um evento b ocorra dado que o evento a tenha ocorrido. Pelo teorema de Bayes, a probabilidade condicional é calculada por

$$p(b|a) = \frac{p(a,b)}{p(a)}. \qquad (2.13)$$

E com isso, podemos escrever

$$p(a,b) = p(b|a)p(a) = p(a|b)p(b), \qquad (2.14)$$

que define a relação fundamental entre as probabilidades conjunta e condicional.

Se não há nenhuma relação entre os eventos a e b, ou seja, a e b são eventos independentes, a probabilidade de b conhecendo a não muda

$$p(b|a) = \frac{p(a,b)}{p(a)} = \frac{p(a)p(b)}{p(a)} = p(b), \tag{2.15}$$

do mesmo modo para a probabilidade de a conhecendo b não muda $p(a|b) = p(a)$. Caso contrário, se os eventos forem dependentes ou correlacionados, teremos $p(a,b) \neq p(a)p(b)$, e com isso as relações acima não serão satisfeitas.

Diante disso, já podemos introduzir a entropia condicional, que é definida por

$$H(X|Y) = -\sum_{x\in X}\sum_{y\in Y} p(x,y)\log p(x|y), \tag{2.16}$$

que é a informação média transmitida pela distribuição de probabilidade condicional, ou, de forma mais clara, é a informação que nós obtemos sobre a fonte X dado que a informação sobre a fonte Y é conhecida. A entropia condicional também pode ser escrita da seguinte forma

$$\begin{aligned}
H(X|Y) &= -\sum_{x\in X}\sum_{y\in Y} p(x,y)\log p(x|y) \\
&= -\sum_{x\in X}\sum_{y\in Y} p(x,y)\log \frac{p(x,y)}{p(y)} \\
&= -\sum_{x\in X}\sum_{y\in Y} p(x,y)\left[\log p(x,y) - \log p(y)\right] \\
&= -\sum_{x\in X}\sum_{y\in Y} p(x,y)\log p(x,y) + \sum_{x\in X}\sum_{y\in Y} p(x,y)\log p(y) \\
&= -\sum_{x\in X}\sum_{y\in Y} p(x,y)\log p(x,y) + \sum_{x\in X}\sum_{y\in Y} p(x)p(y)\log p(y) \\
&= -\sum_{x\in X}\sum_{y\in Y} p(x,y)\log p(x,y) + \sum_{y\in Y} p(y)\log p(y)\underbrace{\sum_{x\in X} p(x)}_{1} \\
&= -\sum_{x\in X}\sum_{y\in Y} p(x,y)\log p(x,y) + \sum_{y\in Y} p(y)\log p(y) \\
&= H(X,Y) - H(Y).
\end{aligned} \tag{2.17}$$

De forma similar, a entropia de von Neumann condicional é definida como

$$S(\rho_A|\rho_B) = S(\rho_{AB}) - S(\rho_B) \tag{2.18}$$

em que A e B são subsistemas de um sistema composto AB. Para um sistema não correlacionado, teremos

$$\begin{aligned} S(\rho_A|\rho_B) &= S(\rho_{AB}) - S(\rho_B) \\ &= S(\rho_A) + S(\rho_B) - S(\rho_B) \\ &= S(\rho_A). \end{aligned} \tag{2.19}$$

De forma análoga,

$$S(\rho_B|\rho_A) = S(\rho_B) \tag{2.20}$$

mostra que, a informação de um subsistema não é afetada pela informação do outro subsistema da qual é conhecida.

E por fim, e não menos importante, iremos definir a entropia relativa. Como foi visto anteriormente, as entropias estão intrisicamente ligadas às distribuições de probabilidade, mas a entropia relativa é diferente das outras entropias por ser considerada uma medida da distância entre duas distribuições de probabilidades, e ela também é conhecida como distância de Kullback-Leibler. Dada duas distribuições de probabilidade $p(x)$ e $q(x)$ em que x pertence a uma única fonte X, a entropia relativa é definida na forma

$$H\left(p(x)||q(x)\right) = \sum_{x\in X} p(x) \log \frac{p(x)}{q(x)}. \tag{2.21}$$

Apesar de ser considera uma distância, ela não é propriamente uma distância, pois não tem simetria $H\left(p(x)||q(x)\right) \neq H\left(q(x)||p(x)\right)$, e não satisfaz a desigualdade triângular, por isso não pode ser considerada um "distância métrica". E, também pode ser reescrita como

$$\begin{aligned} H\left(p(x)||q(x)\right) &= \sum_{x\in X} p(x) \log \frac{p(x)}{q(x)} \\ &= \sum_{x\in X} p(x) \left[\log p(x) - \log q(x)\right] \\ &= \sum_{x\in X} p(x) \log p(x) - \sum_{x\in X} p(x) \log q(x) \\ &= H(X) - \sum_{x\in X} p(x) \log q(x). \end{aligned} \tag{2.22}$$

Sua equivalente quântica é dada por

$$S\left(\rho||\sigma\right) = tr(\rho \log \rho) - tr(\rho \log \sigma), \tag{2.23}$$

em que ρ e σ são os operadores densidade de dois sistemas quânticos.

2.3 Informação mútua

Agora, para concluir a breve introdução a teoria da informação, iremos introduzir outro tipo de entropia que é a informação mútua. Dada duas fontes X e Y, a informação mútua mede a quantidade de informação em comum entre essas duas fontes, e ela pode ser calculada da seguinte forma

$$I(X;Y) = \sum_{x\in X}\sum_{y\in Y} p(x,y)\log\frac{p(x,y)}{p(x)p(y)}. \tag{2.24}$$

Em alguns livros a informação mútua também pode ser denotada por $H(X;Y)$ ou por $H(X:Y)$ e $I(X:Y)$, enfim, não há um consenso entre os autores enquanto a isso, porém, aqui iremos denotar a informação mútua como $I(X;Y)$. Observamos que, se as fontes forem independentes, teremos $p(x,y) = p(x)p(y)$, o que resultará em $\log 1 = 0$, isto é, a informação será nula para esse caso.

Além da Eq.(2.24), a informação mútua por ser escrita como

$$\begin{aligned} I(X;Y) &= \sum_{x\in X}\sum_{y\in Y} p(x,y)\left[\log p(x,y) - \log p(x) - \log p(y)\right] \\ &= \sum_{x\in X}\sum_{y\in Y} p(x,y)\log p(x,y) - \sum_{x\in X}\sum_{y\in Y} p(x,y)\log p(x) - \sum_{x\in X}\sum_{y\in Y} p(x,y)\log p(y) \\ &= \sum_{x\in X}\sum_{y\in Y} p(x,y)\log p(x,y) - \sum_{x\in X} p(x)\log p(x) - \sum_{y\in Y} p(y)\log p(y) \\ &= -H(X,Y) + H(X) + H(Y) \\ &= H(X) + H(Y) - H(X,Y). \end{aligned} \tag{2.25}$$

A partir da Eq(2.17), podemos escrever $H(X,Y) = H(Y) + H(X|Y)$, que, ao substituir na Eq. (2.25), obtemos

$$\begin{aligned} I(X;Y) &= H(X) + H(Y) - H(Y) - H(X|Y) \\ &= H(X) - H(X|Y). \end{aligned} \tag{2.26}$$

A Eq. (2.26) nos permite interpretar a informação mútua como a redução da incerteza em X que é obtido a partir do conhecimento de Y.

De forma similar podemos definir a informação mútua quântica como

$$S(\rho_A;\rho_B) = S(\rho_A) + S(\rho_B) - S(\rho_{AB}), \tag{2.27}$$

que também representa a medida da informação correlacionada entre os dois subsistemas A e B. E, se dois sistemas possuem informações correlacionadas, podemos dizer que seus estados quânticos estão emaranhados.

Capítulo 3

Medidas quânticas e POVM

Nesse capítulo iremos abordar um dos postulados fundamentais da mecânica quântica [4], que mostra como as medidas quânticas são descritas. Apresentaremos dois casos especias, as medidas projetivas ou medidas de von Neumann que também são conhecidas como medidas padrão, e as medidas POVM. Destinaremos um foco maior para as medidas POVM pelo motivo de que elas serão de grande utilidade para os capítulos seguintes.

3.1 Medidas quânticas

Uma definição geral para as medidas quânticas é fornecida pelo seguinte postulado da mecânica quântica [4]:

Postulado *As medidas quânticas são descritas por determinados operadores de medida* $\{M_m\}$*, em que o índice m se refere aos possíveis resultados da medida. Esses operadores atuam sobre o espaço de estados do sistema. Se o estado de um sistema quântico for* $|\psi\rangle$ *antes da medida, a probabilidade de um resultado m ocorrer é dado por:*

$$p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle , \tag{3.1}$$

e o estado do sistema após a medida será:

$$\frac{M_m |\psi\rangle}{\sqrt{\langle\psi| M_m^\dagger M_m |\psi\rangle}}. \tag{3.2}$$

Os operadores de medida satisfazem a relação de completude:

$$\sum_m M_m^\dagger M_m = I. \tag{3.3}$$

A Eq.(3.3), é naturalmente observada pelo fato de que a soma das probabilidades sobre todos os resultados m, deve ser igual a 1:

$$\begin{aligned}\sum_m p(m) &= \sum_m \langle\psi| M_m^\dagger M_m |\psi\rangle \\ &= \langle\psi| \left(\sum_m M_m^\dagger M_m\right) |\psi\rangle \\ &= \langle\psi| I |\psi\rangle = 1. \end{aligned} \tag{3.4}$$

Na mecânica quântica existe vários tipos de medidas, mas, como foi dito anteriormente, iremos apresentar nas seções seguintes apenas dois casos especiais, as medidas projetivas e as medidas POVM.

3.2 Medidas projetivas

Medida projetiva é tipo de medida mais utilizada na mecânica quântica e é de interesse básico em várias aplicações na computação e informação quântica [4]. Esta é a medição em que um observável A é medido em uma base ortonormal composta pelos autoestados do operador A.

A decomposição espectral de A é dada por

$$A = \sum_m m P_m, \tag{3.5}$$

em que P_m é o operador de projeção ou projetor sobre A com autovalor m. A probabilidade de se obter m a partir de um sistema no estado $|\psi\rangle$, é dada por

$$p(m) = \langle\psi| P_m |\psi\rangle . \tag{3.6}$$

Uma observação importante a ser destacada aqui é que chamaremos o 'autovalor' de resultado.

Já que cada resultado m tem uma probabilidade associada, então podemos obter o valor esperado de A:

$$\begin{aligned}\langle A\rangle &= \sum_m m p(m) \\ &= \sum_m m \langle\psi| P_m |\psi\rangle \\ &= \langle\psi| \sum_m m P_m |\psi\rangle = \langle\psi| A |\psi\rangle , \end{aligned} \tag{3.7}$$

que é um resultado bastante conhecido.

Com essas informações, podemos encontrar o estado final para um sistema puro. Por conseguinte, o estado $|\psi\rangle$ após a medição é modificado para $|\psi'\rangle$ dado por

$$|\psi'\rangle = \frac{P_m |\psi\rangle}{\sqrt{\langle\psi| P_m |\psi\rangle}}, \tag{3.8}$$

que ocorre com probabilidade $p(m)$ dada pela Eq. (3.6).

Uma propriedade importante das medidas projetivas é que, o número de resultados possíveis não excede a dimensão do espaço de Hilbert, e isso vem do fato de que cada autoestado tem apenas um resultado associado, por isso não pode conter mais resultados do que autoestados.

3.3 POVM

Como foi dito anteriormente, as medidas projetivas são as mais utilizadas na mecânica quântica, mas nem sempre é a melhor escolha. Existem situações em que é mais vantajoso utilizar um procedimento de medida mais geral que detecte resultados ao longo de conjuntos não-ortogonais.Uma medida que permite o uso de conjuntos não-ortogonais é conhecida como POVM (Positive Operator-Valued Measure). Ela é uma ferramenta essencial no processamento quântico de informações e principalmente na criptografia quântica. Um POVM é um conjunto de operadores Hermitianos, F_m, não-negativos

$$\langle\psi| F_m |\psi\rangle \geq 0, \tag{3.9}$$

para qualquer estado normalizado $|\psi\rangle$, de modo que satisfazem a condição de completude

$$\sum_m F_m = I, \tag{3.10}$$

em que o índice m indica as várias possibilidades de saída de uma implementação do POVM.

Os elementos do POVM não são operadores de projeção, então

$$F_m \neq |m\rangle \langle m|, \tag{3.11}$$

mas eles estão ligados de tal forma que podemos multiplicar o projetor, $|m\rangle \langle m|$, por um número correspondente não-negativo λ_m. Escolhendo adequadamente λ_m, podemos compor um POVM da seguinte forma

$$F_m = \lambda_m |m\rangle \langle m|, \tag{3.12}$$

Como o operador é não-negativo, então

$$\begin{aligned} \langle\psi| F_m |\psi\rangle &= \langle\psi| (\lambda_m |m\rangle \langle m|) |\psi\rangle \\ &= \langle\psi| \lambda_m |m\rangle \langle m|\psi\rangle \\ &= \lambda_m \langle\psi|m\rangle \langle m|\psi\rangle \\ &= \lambda_m |\langle m|\psi\rangle|^2 \geq 0. \end{aligned} \tag{3.13}$$

E a condição de completude será satisfeita se

$$\sum_m F_m = \sum_m \lambda_m |m\rangle \langle m| = I. \tag{3.14}$$

As restrições de λ_m seguem da Eq. (3.14). Como $\langle\psi| F_m |\psi\rangle = p(m)$ tem o significado de probabilidade, logo $p(m)$ não pode ser maior do que 1. Assumindo que $|m\rangle$ e $|\psi\rangle$ são normalizados, o produto interno $\langle m|\psi\rangle$ pode se tornar 1 quando $|m\rangle$ é colinear a $|\psi\rangle$. Portanto, o limite de λ_m é dado por:

$$0 \leq \lambda_m \leq 1. \tag{3.15}$$

O número de POVM possíveis é igual ao número de elementos do conjuntos $\{\lambda_m\}$ satisfazendo a Eq. (3.15). Quando $\lambda_m = 1$ recai a medida projetiva apresentada anteriormente. Para que nosso estudo sobre POVMs seja completado, devemos obter λ_m de forma explícita. Uma maneira de alcançar esse objetivo é analisar como o POVM se comporta ao tentar discriminar estados não-ortogonais sem ambiguidade. Essa aplicação tem um significado muito importante na criptografia quântica, como veremos na seção 4.2, ela está diretamente ligada a segurança do protocolo B92.

3.4 Discriminação de estados não-ortogonais

Para um espaço de Hilbert bidimensional, uma medida projetiva identifica corretamente dois estados ortogonais inseridos nesse espaço, já que a medida projetiva fornece dois resultados determinísticos. Para um problema em que seja necessário a obtenção de três resultados a medida projetiva irá falhar ao tentar gerar esses três resultados, pois uma medida projetiva não pode ultrapassar de dois resultado no espaço de Hilbert bidimensional. E para um problema em que é preciso distinguir estados não-ortogonais, o número de resultados pode ultrapassar a dimensionalidade do espaço de Hilbert [5].

Para os F_1, F_2 e $F_?$, de modo que

$$F_1 + F_2 + F_? = I, \tag{3.16}$$

com

$$p_1 = \langle\psi_1|F_1|\psi_1\rangle\,, \tag{3.17}$$

sendo a probabilidade de identificar o estado $|\psi_1\rangle$ com sucesso, e

$$q_1 = \langle\psi_1|F_?|\psi_1\rangle\,, \tag{3.18}$$

sendo a probabilidade de falhar na identificação do estado. De forma similar,

$$p_2 = \langle\psi_2|F_2|\psi_2\rangle\,, \tag{3.19}$$

é a probabilidade de sucesso e

$$q_2 = \langle\psi_2|F_?|\psi_2\rangle\,, \tag{3.20}$$

é a probabilidade de falhar na identificação do estado $|\psi_2\rangle$.
Para uma discriminação sem ambiguidade, devemos ter

$$\langle\psi_1|F_2|\psi_1\rangle = \langle\psi_2|F_1|\psi_2\rangle = 0. \tag{3.21}$$

Para determinar esses operadores explicitamente, vamos considerar que $A_k = U_k\sqrt{F_k}$ com $k = 1, 2, ?$, e U_k é um operador unitário. Logo,

$$F_k = A_k^\dagger A_k, \tag{3.22}$$

e a probabilidade pode ser expressa como

$$\left\langle\psi_i|A_k^\dagger A_k|\psi_i\right\rangle = \|A_k\psi_i\|^2 \geq 0. \tag{3.23}$$

Por causa da positividade da norma, a condição de discriminação sem ambiguidade é equivalente a

$$A_1\,|\psi_2\rangle = A_2\,|\psi_1\rangle = 0. \tag{3.24}$$

Introduzindo $\left|\psi_i^\perp\right\rangle$ como o vetor ortogonal a $|\psi_{i'}\rangle$, com $i \neq i'$, podemos escrever os operadores A_1 e A_2 na forma

$$A_1 = c_1\left|\bar{\psi}_1\right\rangle\left\langle\psi_1^\perp\right| \qquad \text{e} \qquad A_2 = c_2\left|\bar{\psi}_2\right\rangle\left\langle\psi_2^\perp\right|, \tag{3.25}$$

em que c_i é um coeficiente a ser determinado a partir da condição de otimização e $\left|\bar{\psi}_i\right\rangle$ é o estado normalizado pós-medida. Para uma perfeita distinguibilidade dos estados pós-medida, correspondendo a discriminação ideal, devemos ter

$$\left\langle\bar{\psi}_1|\bar{\psi}_2\right\rangle = 0, \tag{3.26}$$

para que eles possam ser representados por um par de vetores ortogonais.
Agora, podemos escrever os operadores na forma

$$F_1 = |c_1|^2 \left|\psi_1^{\perp}\right\rangle \left\langle\psi_1^{\perp}\right| \qquad \text{e} \qquad F_2 = |c_2|^2 \left|\psi_2^{\perp}\right\rangle \left\langle\psi_2^{\perp}\right|. \tag{3.27}$$

Inserindo essa expressões na Eqs.(3.17) e (3.19), obtemos

$$|c_1|^2 = \frac{p_1}{\left|\left\langle\psi_1|\psi_1^{\perp}\right\rangle\right|^2} \qquad \text{e} \qquad |c_2|^2 = \frac{p_2}{\left|\left\langle\psi_2|\psi_2^{\perp}\right\rangle\right|^2}. \tag{3.28}$$

Inserindo nas equações acima, o fato de que $|\langle\psi_1|\psi_2\rangle| = \cos\theta$ e $\left|\left\langle\psi_i|\psi_i^{\perp}\right\rangle\right| = \sin\theta$ para $i = 1, 2$, podemos escrever os operadores na forma

$$F_1 = \frac{p_1}{\sin^2\theta} \left|\psi_1^{\perp}\right\rangle \left\langle\psi_1^{\perp}\right| \qquad \text{e} \qquad F_2 = \frac{p_2}{\sin^2\theta} \left|\psi_2^{\perp}\right\rangle \left\langle\psi_2^{\perp}\right|. \tag{3.29}$$

Dessa forma, F_1 e F_2 são operadores positivos semi-definido. Uma condição para que haja a existência de um POVM, é a positividade do operador inconclusivo, $F_?$,

$$F_? = I - F_1 - F_2. \tag{3.30}$$

E a condição de não negatividade do operador nos leva a condição,

$$q_1 q_2 \geq |\langle\psi_1|\psi_2\rangle|^2, \tag{3.31}$$

em que $q_1 = 1 - p_1$ e $q_2 = 1 - p_2$ são as probabilidades de falha para os correspondentes estados de entrada.
Seja

$$Q = \sum_i \eta_i q_i = \eta_1 q_1 + \eta_2 q_2, \tag{3.32}$$

a probabilidade total de falha, que para uma discriminação sem ambiguidade, ela deve ser mínima e, consequentemente, fornecer a probabilidade máxima de sucesso. Utilizando o limite mínimo da Eq.(3.31), obtemos que

$$q_1 q_2 = |\langle\psi_1|\psi_2\rangle|^2 = \cos^2\theta \tag{3.33}$$

$$q_2 = \frac{\cos^2\theta}{q_1}. \tag{3.34}$$

Inserindo na Eq.(3.32), produz

$$Q = \eta_1 q_1 + \eta_2 \frac{\cos^2\theta}{q_1}, \tag{3.35}$$

em que, agora, q_1 pode ser considerado como o parâmetro independente do problema. Otimizando Q com respeito a q_1, teremos

$$Q = \eta_1 q_1 + \eta_2 \frac{\cos^2\theta}{q_1} \approx 0, \tag{3.36}$$

por conseguinte

$$q_1^{POVM} = \sqrt{\frac{\eta_2}{\eta_1}}\cos\theta \qquad \text{e} \qquad q_2^{POVM} = \sqrt{\frac{\eta_1}{\eta_2}}\cos\theta. \tag{3.37}$$

Com isso, finalmente obtemos

$$Q^{POVM} = 2\sqrt{\eta_1\eta_2}\cos\theta, \tag{3.38}$$

que é a probabilidade de falha otimizada e é o mínimo teórico para a probabilidade de falha. Assim, a probabilidade de sucesso será máxima quando

$$P^{POVM} = 1 - Q^{POVM} = 1 - 2\sqrt{\eta_1\eta_2}\cos\theta. \tag{3.39}$$

Para o caso em que dois estados são equiprováveis e com $\theta = \pi/4$, teremos

$$Q^{POVM} = 2\sqrt{\frac{1}{2}\frac{1}{2}}\cos\frac{\pi}{4} = \frac{1}{\sqrt{2}} \approx 0,707, \tag{3.40}$$

que, de acordo com [6], ao tentar discriminar os estados utilizando medidas projetiva a probabilidade de falha minima será de $Q^{PROJ} = 0,75$, que é ligeiramente maior que a da medida POVM.

Como veremos na seção 4.2, a discriminação de estados não-ortogonais utilizando POVM desempenha um importante papel nas aplicações da criptografia quântica.

3.5 Medidas generalizadas

A medida mais geral em um sistema quântico consiste em aumentar os graus de liberdade do sistema e, em seguida, realizar uma medição nos estados desse sistema aumentado. Na mecânica quântica, os graus de liberdade são adicionados através de um sistema extra que é preparado para auxiliar o sistema que está sendo estudado, e esse

sistema extra é chamado de "ancila"[6]. Este "ancila"desempenha a mesma função que o sistema do ambiente de modo que o resultado das medições pode evoluir de tal maneira que leva os estados do sistema e do "ancila"a ficarem correlacionados.

Supondo que o "ancila"é preparado em um estado ρ_A e o sistema no estado ρ_S antes da medida, de modo que o estado conjunto dos sistemas possa ser escrito por

$$\rho \to \rho_S \otimes \rho_A. \tag{3.41}$$

Em seguida, o conjunto evolui sob alguma interação U, em que U é unitário, produzindo

$$\rho \to U\rho_S \otimes \rho_A U^\dagger. \tag{3.42}$$

Aplicando uma medida direta no "ancila"utilizando um conjunto de projetores parciais $\left\{I^S \otimes P_m^A\right\}$, teremos a estatística

$$p(m) \;=\; Tr\left\{\left(I^S \otimes P_m^A\right) U\left(\rho_S \otimes \rho_A\right) U^\dagger \left(I^S \otimes P_m^A\right)\right\}. \tag{3.43}$$

Assumindo que o "ancila"foi preparado no estado $|a\rangle$ e o sistema no estado ρ, teremos

$$\begin{aligned} p(m) &= tr\left\{\left(I^S \otimes P_m^A\right) U\left(\rho \otimes |a\rangle\langle a|\right) U^\dagger \left(I^S \otimes P_m^A\right)\right\} && (3.44)\\ &= tr\left\{P_m^A U |a\rangle \rho \langle a| U^\dagger P_m^A\right\} \\ &= tr\left\{K_m \rho K_m^\dagger\right\} \\ &= tr\left\{K_m^\dagger K_m \rho\right\} && (3.45)\\ &= tr\left\{E_m \rho\right\}. && (3.46) \end{aligned}$$

Os operados E_m são chamados de operadores de Kraus, que dependem da escolha de $|a\rangle$, do projetor P_m^A e da transformação unitária U, e devem satisfazer a propriedade

$$\sum_m E_m = \sum_m K_m^\dagger K_m = I. \tag{3.47}$$

De um modo geral, a transição do estado no processo de medição não é unitária, por isso, o processo de medida gera um novo estado que se transforma de acordo com o postulado da mecânica quântica.

Se o estado foi $|\psi_i\rangle$, ao obter o resultado m, o estado será

$$|\psi_i^m\rangle = \frac{K_m |\psi_i\rangle}{\sqrt{\langle\psi_i| K_m^\dagger K_m |\psi_i\rangle}}. \tag{3.48}$$

Portanto, o operador densidade correspondente ao resultado m será

$$\begin{aligned}
\rho_m &= \sum_i p(i|m) \left|\psi_i^m\right\rangle \left\langle\psi_i^m\right| \\
&= \sum_i \frac{p(m|i)p_i}{p(m)} \left(\frac{K_m \left|\psi_i\right\rangle}{\sqrt{\left\langle\psi_i\right| K_m^\dagger K_m \left|\psi_i\right\rangle}}\right) \left(\frac{\left\langle\psi_i\right| K_m^\dagger}{\sqrt{\left\langle\psi_i\right| K_m^\dagger K_m \left|\psi_i\right\rangle}}\right) \\
&= \sum_i \frac{p(m|i)p_i}{p(m)} \left(\frac{K_m \left|\psi_i\right\rangle \left\langle\psi_i\right| K_m^\dagger}{\left\langle\psi_i\right| K_m^\dagger K_m \left|\psi_i\right\rangle}\right). \qquad (3.49)
\end{aligned}$$

Sendo a probabilidade de obter o resultado m após realizar uma medida descrita por K_m no estado inicial $|\psi_i\rangle$

$$p(m|i) = tr\left(K_m^\dagger K_m \left|\psi_i\right\rangle \left\langle\psi_i\right|\right) = \left\langle\psi_i\right| K_m^\dagger K_m \left|\psi_i\right\rangle, \qquad (3.50)$$

resultará em

$$\begin{aligned}
\rho_m &= \sum_i \frac{p(m|i)p_i}{p(m)} \frac{K_m \left|\psi_i\right\rangle \left\langle\psi_i\right| K_m^\dagger}{p(m|i)} \\
&= \sum_i \frac{p_i}{p(m)} K_m \left|\psi_i\right\rangle \left\langle\psi_i\right| K_m^\dagger \\
&= \frac{K_m \left(\sum_i p_i \left|\psi_i\right\rangle \left\langle\psi_i\right|\right) K_m^\dagger}{p(m)} \\
&= \frac{K_m \rho K_m^\dagger}{tr\left(K_m^\dagger K_m \rho\right)}. \qquad (3.51)
\end{aligned}$$

As medidas generalizadas são muito importantes para a informação quântica porquanto a obtenção dos dados é conseguida através de um processo de medida, e a medida ideal é, geralmente, uma medida generalizada. A transformação unitária associada pode ser vista como o processamento da informação quântica. Implementar uma medida generalizada também permite que resultados inconclusivos realizem a discriminação de estados coerentes com baixo número de fótons, o que é impossível fazer utilizando uma medida padrão, essa discriminação é muito importante para muitas realizações de processamento de informação quântica.

3.6 POVM como uma medida generalizada

A medida POVM é vista como o melhor caso especial do formalismo das medidas generalizadas, pois fornece o meio mais simples de se estudar as estatísticas das medidas generalizdas. O POVM como uma medida generalizada também é muito importante na

teoria da informação quântica , uma vez que sua implementação permite obter o máximo de conhecimento sobre o estado de um sistema quântico de modo a minimizar a pertubação do estado do sistema.

Considerando que podemos escrever o operador K_m da seguinte forma [6]

$$K_m = U_m P_m, \tag{3.52}$$

em que U_m é uma transformação unitária, teremos a igualdade

$$\begin{aligned} K_m^\dagger K_m &= P_m U_m^\dagger U_m P_m \\ &= P_m P_m \\ &= P_m^2. \end{aligned} \tag{3.53}$$

Supondo que o dispositivo de medida não realiza a transformação unitária, podemos atribuir apenas

$$P_m = \sqrt{E_m}, \tag{3.54}$$

como resultado de um POVM. De forma mais clara, podemos comparar com o que foi feito na seção 3.3, lembrando que

$$F_m = \lambda_m \left|m\right\rangle \left\langle m\right|. \tag{3.55}$$

Como

$$F_m^\dagger = \lambda_m \left|m\right\rangle \left\langle m\right| = F_m, \tag{3.56}$$

então

$$\begin{aligned} F_m^\dagger F_m &= \lambda_m \left|m\right\rangle \left\langle m|m\right\rangle \left\langle m\right| \lambda_m \\ &= \lambda_m^2 \left|m\right\rangle \left\langle m\right| \\ &= \lambda_m F_m, \end{aligned} \tag{3.57}$$

ou seja,

$$\begin{aligned} F_m^\dagger F_m &= \frac{1}{\lambda_m} F_m^\dagger F_m \\ &= \left(\frac{F_m}{\sqrt{\lambda_m}}\right)^\dagger \left(\frac{F_m}{\sqrt{\lambda_m}}\right). \end{aligned} \tag{3.58}$$

Logo, o estado pós-medida será

$$|\psi_m\rangle = \frac{\left(F_m/\sqrt{\lambda_m}\right)|\psi\rangle}{\sqrt{\langle\psi|\left(F_m/\sqrt{\lambda_m}\right)^\dagger\left(F_m/\sqrt{\lambda_m}\right)|\psi\rangle}}. \tag{3.59}$$

E com isso, podemos denotar que

$$K_m = \frac{F_m}{\sqrt{\lambda_m}}, \tag{3.60}$$

de forma que a medida POVM assume um aspecto semelhante a que foi vista na seção anterior, em que

$$|\psi_m\rangle = \frac{K_m|\psi\rangle}{\sqrt{\langle\psi|K_m^\dagger K_m|\psi\rangle}}. \tag{3.61}$$

E, portanto,

$$P_m = \sqrt{E_m} = \sqrt{K_m^\dagger K_m} = \sqrt{\frac{F_m F_m}{\lambda_m}} = \sqrt{F_m}. \tag{3.62}$$

A Eq. (3.61) é bastante similar a Eq. (3.8), mas com um diferencial de que $K_m^\dagger K_m \neq K_m$, como é sugerido quando o operador é projetivo, e isso não acontece quando o operador é um POVM. Por isso a medida POVM é tratada como uma medida generalizada, pois ela se comporta como tal.

Neste capítulo mostramos uma pequena introdução sobre as medidas que serão utilizadas nos capítulos seguintes.

Capítulo 4

Trocas de chave e segurança na criptografia quântica

A criptografia é arte de tornar uma mensagem incompreensível para um espião (será chamado de Eva) na comunicação entre duas partes autorizadas, o emissor (será chamado de Alice) e o receptor (será chamado de Bob) [7]. Com a contribuição da mecânica quântica, aconteceu o surgimento da criptografia quântica. A criptografia quântica difere da criptografia convencional de modo que ela mantém os dados em segredo pelas propriedades da mecânica quântica. Uma notável aplicação da mecânica quântica na criptografia é a distribuição quântica de chaves [8], pois através dela é possível compartilhar chaves secretas de forma comprovadamente segura. A distribuição quântica de chaves permite adquirir uma sequência aleatória de bits, que é a chave, e é essa chave que permite com que Alice e Bob se comuniquem de forma segura.
Na criptografia quântica, Alice e Bob possuem dois canais de comunicação a disposição, um deles é o canal público ou canal clássico, que pode ser ouvido por qualquer pessoa, mas não pode ser modificado; e o outro é o canal quântico, no qual qualquer tentativa de espionagem nesse canal introduzirá erros na transmissão Fig.(4.1).

4.1 BB84

A origem da criptografia quântica pode ser atribuida a Wiesner que inicialmente teve seu trabalho rejeitado pela IEEE Transaction on Information Theory por não compreenderem a linguagem física na qual foi escrita, por isso, o trabalho original foi publicado

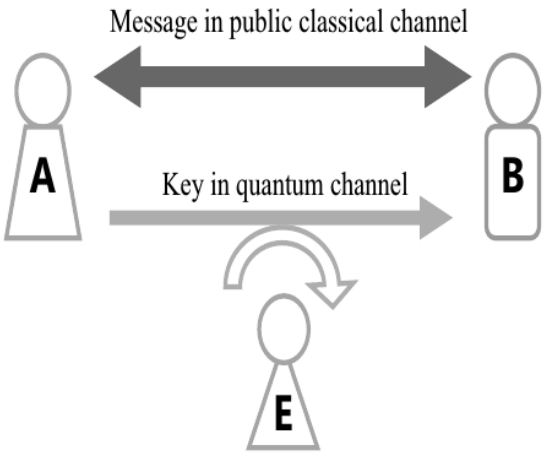

Figura 4.1: Esquema básico para troca de chaves.

uma década mais tarde por outra revista [9]. O trabalho de Wiesner sugere que estados quânticos poderiam ser armazenados por longos períodos de tempo de forma a serem utilizados como "dinheiro"à prova de falsificação, para isso seria necessário utilizar uma memória quântica de longo prazo, o que não era e ainda não é uma pratica viável. No entanto, Bennett e Brassard perceberam que ao invés de utilizar os estados quânticos para armazenar a informação eles poderiam ser utilizados para transmitir a informação. Logo, em 1984, eles publicaram o primeiro protocolo da criptografia quântica, que hoje é conhecido como BB84.

O protocolo BB84 utiliza dois estados puros $|u\rangle$ e $|v\rangle$, e mais dois estados ortogonais ao primeiro par $|\bar{u}\rangle$ e $|\bar{v}\rangle$, respectivamente. Escolhendos os vetores $|e_0\rangle$ e $|e_1\rangle$ como vetores de base no plano de $|u\rangle$ e $|v\rangle$, conforme é mostrado na Fig.4.2, os estados $|u\rangle$, $|v\rangle$, $|\bar{u}\rangle$ e $|\bar{v}\rangle$ podem ser descritos por uma forma geral que será bastante útil no capítulo 5.

A partir da Fig.4.2 , podemos escrever os estados na forma

$$|u\rangle = \cos\alpha\,|e_0\rangle + \sin\alpha\,|e_1\rangle\,, \tag{4.1}$$

$$|v\rangle = \sin\alpha\,|e_0\rangle + \cos\alpha\,|e_1\rangle\,, \tag{4.2}$$

$$|\bar{u}\rangle = -\sin\alpha\,|e_0\rangle + \cos\alpha\,|e_1\rangle\,, \tag{4.3}$$

$$|\bar{v}\rangle = \cos\alpha\,|e_0\rangle - \sin\alpha\,|e_1\rangle\,, \tag{4.4}$$

para um intervalo $0 < \alpha < \pi/4$, e para quaisquer par de vetores $|u\rangle$ e $|v\rangle$ com o produto

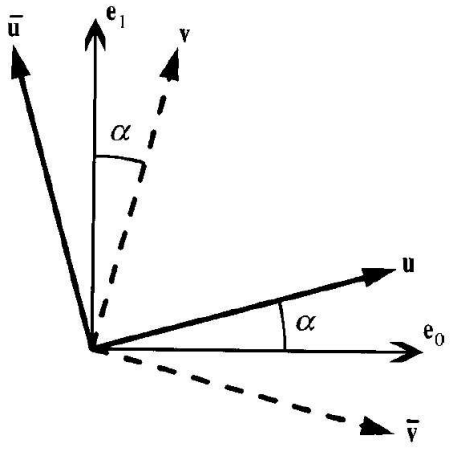

Figura 4.2: Estados quânticos utilizados no BB84

interno

$$\langle u|v\rangle = \sin 2\alpha. \tag{4.5}$$

Usualmente, o protocolo utiliza um sistema quântico composto por dois estados $|0\rangle$ e $|1\rangle$ que representam fótons linearmente polarizados em direções ortogonais em que devemos utilizar $2\alpha = \pi/4$, como veremos a seguir.

4.1.1 O protocolo

Alice e Bob devem previamente escolher quais estados ortogonais irão representar o bit 0 e o bit 1. De maneira que a implementação do protocolo BB84 seja facilmente compreendida, iremos apresentar sua implementação como um exemplo onde utilizaremos a seguinte notação

$$|0\rangle_D = \frac{1}{\sqrt{2}}\left(|0\rangle_R + |1\rangle_R\right), \tag{4.6}$$

$$|1\rangle_D = \frac{1}{\sqrt{2}}\left(|0\rangle_R - |1\rangle_R\right), \tag{4.7}$$

$$|0\rangle_R = \frac{1}{\sqrt{2}}\left(|0\rangle_D + |1\rangle_D\right), \tag{4.8}$$

$$|1\rangle_R = \frac{1}{\sqrt{2}}\left(|0\rangle_D - |1\rangle_D\right), \tag{4.9}$$

em que $|0\rangle_R$ e $|1\rangle_R$ representam a polarização horizontal e vertical do fóton na base retilínea, $|0\rangle_D$ e $|1\rangle_D$ representam a polarização 45° e 135° na base diagonal. As bases retilínea e diagonal são bases conjugadas em razão de que, um fóton preparado em um dos estados

da base retilínea irá se comportar de forma completamente aleatória quando medido na base diagonal, e o mesmo fato acontece caso contrário.

Com esses dados em mente, agora podemos analisar como o BB84 opera. Inicialmente, Alice deve escolher uma sequência aleatória de bits de modo a preparar cada fóton em um dos quatro estados citados acima e em seguida enviar para Bob através do canal quântico. Ao receber a sequência de bits, Bob deve escolher em qual base medir cada fóton e, em seguida, confirmar à Alice que recebeu e mediu os fótons.

Após a transmissão e detecção dos fótons, Alice e Bob revelam, através do canal clássico, apenas as bases utilizadas para enviar e medir, respectivamente. Em seguida, eles comparam cada base que foi utilizada por cada um de modo a considerar apenas os resultados nos quais ambos utilizaram a mesma base e descartar os casos em que utilizaram bases diferentes. Agora, Alice e Bob revelam uma pequena parte da sequência dos bits para comparar os resultados enviados com os resultados obtidos na medição. Na ausência de Eva, os resultados revelados por Alice devem coincidir com os resultados das medidas de Bob, e assim utilizar esses resultados como chave; mas, na presença de Eva, a probabilidade de que os resultados coincidam é quase nula. Para demonstrar esse fato, vamos supor que Alice, Bob e Eva utilizam para cada metade da sequência de bits a base retilínea e a base diagonal. Se Alice e Bob utilizarem a base retilínia, a probabilidade de Eva usar a mesma base é de 1/2. Agora, se Eva utilizar a base diagonal, a probabilidade de Bob medir corretamente o bit transmitido é de 1/2. Por exemplo, suponhamos que Alice tenha transmitido o bit 0 na base retilínea, $|0\rangle_R$, e Bob mediu na mesma base, mas Eva usou a base diagonal para medir o bit, o que levará o estado para um dos vetores da base diagonal,

$$|0\rangle_D = \frac{1}{\sqrt{2}}\left(|0\rangle_R + |1\rangle_R\right) \text{ ou } |1\rangle_D = \frac{1}{\sqrt{2}}\left(|0\rangle_R - |1\rangle_R\right).$$

Portanto, a probabilidade de Bob medir $|0\rangle_R$ é de

$$\begin{aligned} p(|0\rangle_R) &= |_R\langle 0|0\rangle_D|^2 = |_R\langle 0|1\rangle_D|^2 \\ p(|0\rangle_R) &= \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}. \end{aligned} \tag{4.10}$$

Para uma larga sequência de bits, a probabilidade de Bob medir os bits corretamente é de $(1/2)^N$, para cada N vezes que Eva utilizou a base errada [10].

Para uma melhor compreensão das etapas do protocolo, a Fig.4.3 [10] ilustra um exemplo de uma transmissão de chave quântica. Como vimos na Fig.4.3, a chave resultante entre

Sequência de bits de Alice	0	1	1	0	1	1	0	0	1	0	1	1
Bases escolhidas por Alice	D	R	D	R	R	R	R	R	D	D	R	D
Fótons enviados por Alice	$\|0\rangle_D$	$\|1\rangle_R$	$\|1\rangle_D$	$\|1\rangle_R$	$\|1\rangle_R$	$\|1\rangle_R$	$\|0\rangle_R$	$\|0\rangle_R$	$\|1\rangle_D$	$\|0\rangle_D$	$\|1\rangle_R$	$\|1\rangle_D$
Bases escolhidas por Bob	R	D	D	R	R	D	D	R	D	R	D	D
Bits recebido por Bob	1		1		1	0	0	0		1	1	1
Bob informa os bits detectados	R		D		R	D	D	R		R	D	D
Alice informa as bases corretas			OK		OK			OK				OK
Informação compartilhada			1		1			0				1
Bob revela alguns bits					1							
Confirmação de Alice					OK							
A chave resultante			1					0				1

Figura 4.3: Troca de chave feita por Alice e Bob na ausência de um espião

Alice e Bob é idêntica para ambos. Mas, esse é um caso especial onde não há ruído no canal ou a interferência de Eva. Quando o canal é ruidoso, ele introduz erros durante a transmissão dos bits e isso gera uma confusão na hora de reconciliar as bases, pois Alice e Bob não sabem se o erro produzido foi gerado por Eva ou pela imperfeiçao do canal. Com isso em mente, se faz necessário estimar uma quantidade de erro tolerável para o protocolo.

4.1.2 Estimativa de erro

Como o canal utilizado no protocolo é um canal binário, isto é, o canal transmite apenas dois valores possíveis 0 e 1, a taxa de erro Q desse canal é a probabilidade de que Alice envie 0 e Bob receba 1, ou, que Alice envie 1 e Bob receba 0. Na linguagem da teoria da computação, isso é chamado de probabilidade de cruzamento (crossover probability), e um canal com $Q > 0$ é considerado ruidoso.

Outro fato interessante a ser destacado é que, a probabilidade de cruzamento Q para o bit 1 é a mesma para o bit 0, por isso é dito que esse canal é binário simétrico. Por conseguinte, a incerteza de Bob sobre o valor do bit que ele recebe é dada pela função da entropia binária,

$$H(Q) = -Q\log(Q) - (1-Q)\log(1-Q). \tag{4.11}$$

A informação que ele obtém ao receber o bit é igual a

$$\begin{aligned} I(X;Y) &= H(X) - H(X|Y) \\ &= 1 + Q\log(Q) + (1-Q)\log(1-Q) \\ &= 1 - H(Q). \end{aligned} \tag{4.12}$$

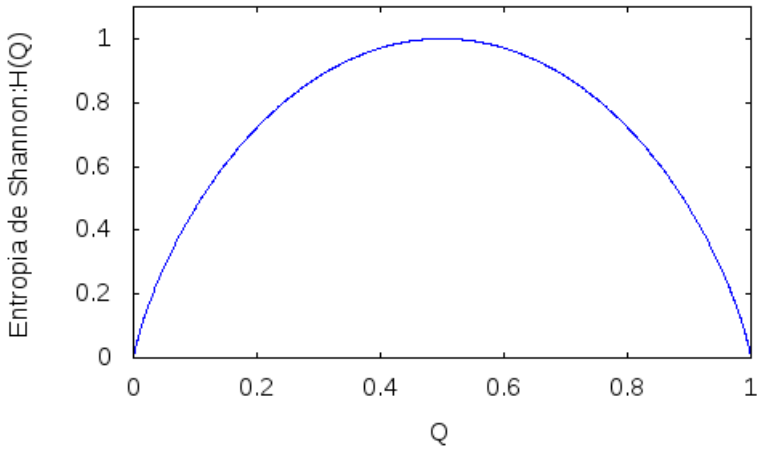

Figura 4.4: Figura mostrando a entropia binária de Shannon.

Isso quer dizer que para cada bit enviado por Alice, Bob recebe apenas $1 - H(Q)$ de informação.

A razão entre a informação recebida e enviada é chamada de capacidade do canal, C,

$$\begin{aligned} C &= \frac{bits\,recebidos}{bits\,enviados} \\ &= \frac{1 - H(Q)}{1} \\ &= 1 - H(Q), \end{aligned} \tag{4.13}$$

que estabele o limite superior teórico sobre a capacidade do canal.

Para estimar a taxa de erro Q, Alice e Bob escolhem aleatoriamente um certo número de bits transmitidos e os comparam públicamente. Caso a estimativa de erro seja superior ao estabelecido, o protocolo deve ser encerrado, pois pode ter vazado um excesso de informação para Eva. Caso contrário, em que a taxa de erro é aceitável, os bits são descartados e em seguida inicia-se a fase de reconciliação de informação.

4.1.3 Reconciliação de informação

Após a estimativa de erro, Alice e Bob devem eliminar esses erros encontrados em suas sequências, pois eles não sabem se foram gerados por Eva ou pelo canal. Mas, por medida de segurança, todo erro encontrado na comunicação é atribuído a Eva. Por conseguinte, é necessário a correção desses erros, e um dos passos para reduzí-los é através da reconciliação de informação, que também é chamada de correção de erro.

Com o intuito de diminuir a diferença entre as sequências de Alice e Bob, causadas pelos

erros, a reconciliação de informação implica em sacrificar alguns bits das sequências de forma a garantir a segurança da comunicação. E para isso, é necessário o mínimo de divulgação de informação possível através do canal público [11]. De acordo com o teorema da codificação de Shannon, o número mínimo de bits, r, que deve ser compartilhado publicamente para corrigir os erros da sequência de comprimento n é dado por

$$r = n\left[-Q\log Q-(1-Q)\log\left(1-Q\right)\right]. \tag{4.14}$$

A reconciliação de informação consiste em checar a paridade das sequências através da divulgação de alguns bits da mesma. Quando falamos em checar a paridade, na linguagem computacional, isso quer dizer que, a soma de todos os 0 e 1 de uma determinada sequência dever ser um número par ou ímpar. No processo de reconciliação, Alice e Bob dividem suas sequências em blocos do mesmo tamanho, que devem ser pequenos o suficiente de modo que seja estatísticamente improvável conter mais de um erro em cada bloco. Para cada bloco, eles comparam a paridade e mantém os blocos com paridades correspondentes, e para cada bloco com paridades diferentes, eles subdividem em blocos menores e comparam a paridade novamente. Esse procedimento é realizado até que os erros sejam encontrados e removidos. Por fim, Alice e Bob descartam o último bit de cada bloco e concluem com alto grau de confiança de que todos os erros foram removidos e que eles possuem, cada um, a mesma sequência de bits.

Esse procedimento corrige com eficiência os erros contidos nas sequências de Alice e Bob, mas não elimina as informações obtidas por Eva ao ouvir a divulgação das paridades dos blocos. Por isso, se faz necessário aplicar outro procedimento para aumentar a segurança e diminuir a informação que Eva tem sobre as sequências de Alice e Bob. Esse procedimento é conhecido como amplificação de privacidade e será discutida na seção seguinte.

4.1.4 Amplificação de privacidade

Após a reconciliação de informação, assumimos que Alice e Bob possuem em mãos sequências idênticas, mas Eva ainda pode ter informação sobre as sequências adquirida através da divulgação das paridades e pela medição correta dos bits. Para aumentar a segurança e consequentemente diminuir a informação obtida por Eva, se deve aplicar a técnica conhecida como amplificação de privacidade que foi inicialmente introduzida por [16] e tem o intuito de gerar uma sequência completamente aleatória e secreta da qual

Eva tenha o mínimo de informação possível.

De forma convencionalista [11], a espionagem de Eva sobre o canal quântico consiste em selecionar um função

$$e : \{0,1\}^N \rightarrow \{0,1\}^K , \tag{4.15}$$

cujo valor $e(x)$ lhe dá K bits de informação sobre x, assumindo que x é a sequência de bits de comprimento N que é comum a Alice e Bob. Na fase de amplificação de privacidade, Alice e Bob devem chegar a um acordo publicamente sobre uma função

$$g : \{0,1\}^N \rightarrow \{0,1\}^R , \tag{4.16}$$

para $R \leq N - K$, de forma que o conhecimento de e, $e(x)$ e g deixe Eva com uma pequena fração de um bit de informação sobre $g(x)$.

Para ilustrar um exemplo simples de amplificação de privacidade, vamos considerar que Alice e Bob compartilham apenas dois bits,

$$r_1 r_2 \in \{0,1\}^2 , \tag{4.17}$$

e estimam que Eva conheça apenas um bit e dos bits compartilhados, ou seja, $e = r_1$ ou $e = r_2$, em que a estimativa ocorre com uma probabilidade de $1 - Q$. Agora, eles podem escolher uma função XOR, que realiza uma soma de módulo 2 e é denotada pelo símbolo $\oplus$, logo

$$g\left(r_1 r_2\right) = r_1 \oplus r_2. \tag{4.18}$$

De um modo geral, para N bits, após a divulgação da função, Alice terá $[x_1 \oplus x_2 \oplus \cdots \oplus x_N]$ e Bob, ao efetuar a mesma operação, terá $[y_1 \oplus y_2 \oplus \cdots \oplus y_N]$. Como assumimos que após a reconciliação de informação eles possuem em mãos duas sequências iguais, então x_i deve ser igual a y_i, e consequentemente, as duas sequências continuam sendo iguais para cada um, exceto para Eva que, ao tentar realizar a mesma operação em seus bits adquiridos durante a espionagem, irá aumentar os erros dos seus bits e assim diminuir a sua informação.

Vale a pena notar que, se mesmo uma pequena diferença é deixada entre as sequências de Alice e Bob depois da reconciliação de informação, após a amplificação de privacidade as sequências finais serão quase completamente descorrelacionadas. Portanto, vimos que a reconciliação de informação seguida pela amplificação de privacidade, gera um sequência

livre de erros com alta probabilidade , enquanto reduz a informação de Eva essencialmente para zero, e assim, Alice e Bob chegam a uma chave criptográfica comprovadamente segura.

4.2 B92

Outro protocolo idealizado por Bennett é o B92, que é uma alternativa para o protocolo BB84. Em [2], Bennett mostrou que, em princípio, é possível a distribuição de uma chave usando apenas dois estados não-ortogonais de um sistema quântico, em vez de quatro, como é o caso do BB84. Esta afirmação é baseada no fato de que, na mecânica quântica, é possível distinguir dois estados não-ortogonais sem ambiguidade. Com efeito, a segurança desse protocolo basea-se na incapacidade de Eva de distinguir os estados sem ambiguidade e de não pertubá-los durante a espionagem.

Como o B92 utiliza apenas dois estados que não são ortogonais, $|u\rangle$ e $|v\rangle$, não há como Bob, e nem Eva, decodificar a mensagem enviada por Alice de forma determinística como no BB84. Contudo, por meio de uma medida generalizada, Bob pode obter resultados conclusivos e inconclusivos. Por exemplo, ao invés de obter apenas resultados binários como 0 ou 1, ele obterá um sistema ternário com resultados 0, 1 ou ?, em que ? representa os resultados inconclusivos. A medida generalizada ideal para esse propósito é um POVM que consiste em três operadores Hermitianos dados por [14]:

$$A_u = \frac{I - |v\rangle\langle v|}{1 + \langle u|v\rangle}, \tag{4.19}$$

$$A_v = \frac{I - |u\rangle\langle u|}{1 + \langle u|v\rangle}, \tag{4.20}$$

$$A_? = I - A_u - A_v, \tag{4.21}$$

em que $|u\rangle$ e $|v\rangle$ representam dois estados de polarização de fótons não ortogonais, de modo que $\langle u|v\rangle = \cos\theta$, como mostra Fig.4.5, e também são descritos pelas Eqs.(4.1) e (4.2). O operador $A_?$ representa os resultados inconclusivos obtidos por Bob. Esses operadores são apropriados para a realização do protocolo B92 pelo fato de que

$$\langle v|A_u|v\rangle = \frac{\langle v|v\rangle - \langle v|v\rangle\langle v|v\rangle}{1 + \langle u|v\rangle} = 0$$

e

$$\langle u|A_v|u\rangle = \frac{\langle u|u\rangle - \langle u|u\rangle\langle u|u\rangle}{1 + \langle u|v\rangle} = 0.$$

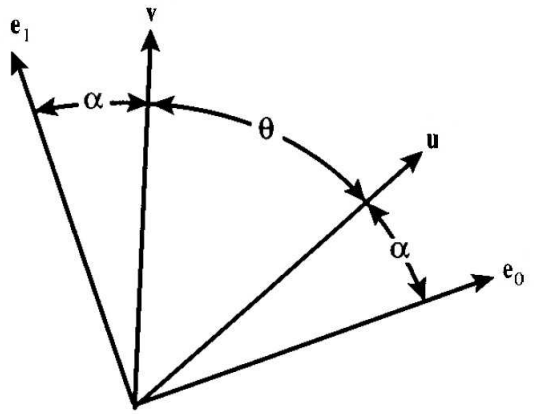

Figura 4.5: Estados quânticos utilizados no B92

Esses dois resultados nos diz que, um fóton com representação $|u\rangle$ tem um valor esperado diferente de zero apenas quando é medido pelos operadores A_u e $A_?$. O mesmo acontece quando um fóton, representado pelo estado $|v\rangle$, é medido pelos operadores A_v e $A_?$. Ou seja, Bob poderá concluir com segurança qual estado ele recebeu a partir do resultados das medições dos operadores A_u e A_v, e algumas vezes não poderá concluir nada a respeito dos estados recebidos a partir do resultado da medição do operador $A_?$, mas de nenhum modo ele errará na identificação dos estados. Com isso em mente, podemos descrever o protocolo.

4.2.1 O protocolo

Para iniciar o protocolo, Alice deve inicialmente escolher uma sequência aleatória para que seja enviada à Bob utilizando o estados $|u\rangle$ para codificar o bit 1 e o estado $|v\rangle$ para codificar o bit 0. Ao receber a sequência, Bob deve escolher aleatoriamente para cada estado recebido qual operador utilizar. Terminada a transmissão, Bob anuncia para Alice através do canal público em quais bits ele obteve um resultado conclusivo, mas sem informar qual operador utilizou para medí-los. Ao fazer isso, Alice e Bob descartam todos os outros dos quais Bob obteve resultados inconclusivos. Como no BB84, eles comparam o resultado de alguns bits para verificar se Eva interceptou a transmissão. Para isso, Bob anuncia publicamente qual operador utilizou para medir esses bits, se Eva não interferiu a transmissão, a medida de Bob deve corresponder ao estado enviado por Alice, ou seja, a medida A_u realizada por Bob deve corresponder ao estado $|u\rangle$ enviado por Alice e

o mesmo deve acontecer quando Bob realiza a medida A_v no estado $|v\rangle$ enviado por Alice. Caso aconteça um evento diferente, por exemplo, se Alice enviou um estado $|v\rangle$ e Bob obteve um resultado conclusivo ao medí-lo utilizando o operador A_u, ou se Alice ao enviar $|u\rangle$ e Bob tenha obtido um resultado conclusivo ao medir A_v, isso mostra que Eva interferiu na transmissão. Notemos que, essa descrição relata um procedimento realizado em equipamentos perfeitos, onde o canal quântico não pertuba os estados transmitidos, por isso devemos nos atentar para uma descrição onde os equipamentos não são ideais. Da mesma forma que no BB84, um canal quântico imperfeito pertuba os estados em trânsito mesmo na ausência de Eva, diante disso, tanto Bob quanto Eva encaram um problema de discriminação de estados não-ortogonais. A diferença entre eles é que, Bob está interessado em discriminar seus estados sem ambiguidade para que estejam de acordo com estados enviados por Alice, enquanto Eva está mais interessada em obter o máximo de informação possível em vez de obter informações deterministas em menos bits.

4.2.2 Exemplo de distribuição quântica de chave utilizando o B92

Ao gerar uma sequência de bits 0 e 1, Alice codifica-os em qubits, $|v\rangle = |0\rangle$ para o bit 0 e $|u\rangle = |+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ para o bit 1, com probabilidades *a priori* de 1/2. Após a codificação da sequência aleatória dos qubits, Alice envia a sequência para Bob, que utilizará a melhor estratégia de discriminação de estados. Utilizando a Eq. (3.38)

$$Q^{POVM} = 2\sqrt{\eta_1\eta_2}\cos\theta = 2\sqrt{\eta_1\eta_2}\,|\langle u|v\rangle|\,, \tag{4.22}$$

a probabilidade de sucesso de Bob será

$$P = 1 - Q^{POVM} = 1 - 2\sqrt{\frac{1}{2}\frac{1}{2}}\frac{1}{\sqrt{2}} = 1 - \frac{1}{\sqrt{2}} \approx 29,3\%. \tag{4.23}$$

Em seguida Bob anuncia publicamente para Alice em quais qubits ele obteve resultados conclusivos sem anunciar o resultado, e com isso, eles mantêm apenas esses qubits, dos quais a discriminação foi bem sucedida e descartam o restante de falhou. Na ausência de ruído e da espionagem de Eva, as duas sequências nas mãos de Alice e Bob devem ser idênticas. Mas caso Eva esteja espionando a transmissão, devemos incialmente analisar qual estratégia ela utilizou para monitorar a transmissão.

Supondo que Eva tenha interceptado um qubit, ao tentar discriminar o estado desse qubit

sem ambiguidade, ela falhará com uma probabilidade de

$$Q_E = 2\sqrt{\eta_1\eta_2}\cos\theta = 2\sqrt{\frac{1}{2}\frac{1}{2}}\frac{1}{\sqrt{2}} \approx 71\%. \tag{4.24}$$

Com uma probabilidade de falha tão alta Eva não tem ideia em qual estado o qubit foi preparado. E Bob, ao receber o qubit interceptado por Eva, tem a probabilidade de

$$\eta Q_E = \frac{1}{2\sqrt{2}} \approx 35,3\%, \tag{4.25}$$

de receber o bit errado. Esse erro pode ser facilmente detectado pela simples comparação pública de alguns bits, e caso o erro seja no alcance de 35%, o protocolo é encerrado.
Vimos que a discriminação sem ambiguidade não é a melhor estratégia para Eva utilizar, já que seu intuito é obter o máximo de informação possível produzindo o mínimo de erro nos resultados de Bob. Por isso se faz necessário analizar um caso que seja mais favorável para Eva.

4.2.3 Ataque opaco

Nessa estratégia de espionagem, Eva pode interceptar os fótons enviados por Alice, executar uma medição que maximize sua informação sobre os estados dos fótons e então preparar um novo estado baseado em seus resultados obtidos na medição para que, em seguida, enviá-lo a Bob. O procedimento ideal para esse caso é realizar uma medição de um operador Hermitiano do qual seus autovetores ortogonais sejam simetricamente relacionados, uma medição tipo von Neumann.
Eva ao utilizar a estratégia de espionagem opaca, ela realiza uma medida projetiva nos qubits interceptados para depois reenviá-los a Bob. Como no B92 utilizamos apenas os estados $|u\rangle$ e $|v\rangle$, Eva deverá preparar um qubit em um desses estados de acordo com resultado da sua medição sobre o qubit enviado por Alice. Eva não altera a taxa de resultados inconclusivos R, dada por

$$\begin{aligned} R &= \langle u|A_?|u\rangle = \langle v|A_?|v\rangle \\ &= |\langle u|v\rangle| \qquad (4.26) \\ &= \sin 2\alpha, \qquad (4.27) \end{aligned}$$

já que ela realiza medidas projetivas, e por isso, ela pode se disfarçar de Alice enviado os estados $|u\rangle$ e $|v\rangle$ com a mesma probabilidade. Mas ao fazer isso, ela altera a taxa de erro,

pois Eva não sabe em qual estado os bits foram codificados e isso fará com que ela falhe na identificação de alguns bits. Portanto, sua taxa de erro será

$$\begin{aligned} q &= \langle u|P_v|u\rangle = \langle v|P_u|v\rangle \\ q &= \sin^2\alpha, \end{aligned} \tag{4.28}$$

e o máximo de informação que ela pode obter sobre os bits interceptados é dada pela Eq. (4.12) [13],

$$I_{AE} = 1 + q\log q + (1-q)\log(1-q) \tag{4.29}$$

$$= 1 + \sin^2\alpha \log\left(\sin^2\alpha\right) + \cos^2\alpha \log\left(\cos^2\alpha\right). \tag{4.30}$$

Como Eva nem sempre acertará na identificação dos bits enviados por Alice, ela pode decidir interceptar apenas alguns bits com o propósito de diminur a taxa de erro de Bob de modo que ela não seja detectada. Supondo que Eva intercepte apenas uma fração de bits, η (não confundir η dessa seção com a probabilidade *a priori*, η_i, apresentada na seção 3.4). Sua informação sobre esses bits será

$$I_{AE} = \eta\left(1 + \sin^2\alpha \log\sin^2\alpha + \cos^2\alpha\log\cos^2\alpha\right). \tag{4.31}$$

Após Bob receber os bits enviados por Alice e os reenviados por Eva, ele continua com o protocolo aplicando o POVM em todos os bits recebido. Ao término de suas medições, ele anuncia publicamente para Alice quais foram os seus resultados inconclusivos, e ao fazer isso, eles estimarão a taxa de erro entre as duas sequências. Mas, como Eva interceptou uma fração deles, depois dos resultados inconclusivos serem descartados, a taxa de erro será

$$Q = \eta q = \eta\sin^2\alpha. \tag{4.32}$$

E a informação de Eva sobre os bits de Alice após os resultados inconclusivos serem descartados é

$$I_{AE} = \frac{Q}{\sin^2\alpha}\left(1 + \sin^2\alpha\log\sin^2\alpha + \cos^2\alpha\log\cos^2\alpha\right). \tag{4.33}$$

A taxa de erro entre Eva e Bob, é dada por

$$q_{EB} = \langle i|A_j|i\rangle, \qquad i \neq j, \tag{4.34}$$

que é a probabilidade de Bob obter o resultado j, sendo que Eva tenha enviado i. Mas, como Bob utiliza POVM, logo o resultado diferente de zero, será

$$q_{EB} = \langle i|A_?|i\rangle = \sin 2\alpha, \qquad i \in \{u, v\}\,. \tag{4.35}$$

E a informação entre Eva e Bob será de

$$I_{EB} = 1 + \sin 2\alpha \log(\sin 2\alpha) + (1 - \sin 2\alpha) \log(1 - \sin 2\alpha)\,. \tag{4.36}$$

Relacionando os dois resultados, iremos obter

$$\begin{aligned} I_{AB} &= 1 + \eta \sin^2\alpha \sin 2\alpha \log\left(\eta \sin^2\alpha \sin 2\alpha\right) \\ &\quad + \left(1 - \eta \sin^2\alpha \sin 2\alpha\right) \log\left(1 - \eta \sin^2\alpha \sin 2\alpha\right). \end{aligned} \tag{4.37}$$

Com uma taxa de erro de

$$q_{AB} = \eta \sin 2\alpha \sin^2\alpha \tag{4.38}$$

A relação entre $q_{AB} < q_{AE}$, mostra que ao relizar medidas tipo POVM, Bob reduz a sua própria taxa de erro e melhora sua eficiência ao identificar o estado quântico.
Vimos neste capítulo como atuam os protocolos BB84 e B92 em aplicações simples de espionagem. Tal conteúdo apresentado serve de base para uma melhor compreensão do capítulo seguinte, pois nele apresentaremos uma estratégia de espionagem em que Eva realiza ataques individuais que consiste em monitorar cada bit de informação individualmente.

Capítulo 5

Verificação da segurança dos protocolos sob ataques individuais

No capítulo anterior, foi apresentado como funciona os protocolos BB84 e B92 e como eles se comportam quando submetidos a uma estratégia de espionagem simples. Por isso, aqui apresentaremos uma estratégia de espionagem mais sofisticada onde Eva faz o uso de um sistema "ancila"para interagir unitariamente com os bits utilizados na transmissão entre Alice e Bob. Essa estratégia é conhecida como espionagem translucente, e na literatura o sistema "ancila"é comumente chamado de sonda, que daqui em diante será feito o mesmo. Para o caso mais simples no qual não há emaranhamento, Eva deixa os estados de interação prosseguir para Bob para que ela possa medi-los só após os processos de correção de erro e amplificação de privacidade. Mas a principal desvantagem dessa estratégia é que ao tenta obter informações sobre os bits enviados por Alice, Eva aumenta a superposição entre os estados enviados para Bob e consequentemente reduz sua informação sobre os bits de Bob. Para contornar essa situação a melhor estratégia a ser utilizada é a interação com emaranhamento, onde Eva utiliza a sua sonda para emaranhá-la com os bits enviados por Alice para que em seguinda sejam enviados à Bob. Essa estratégia é conhecida como espionagem translucente com emaranhamento [14], e será a estratégia estudada nesse capítulo.

5.1 O modelo da espionagem

Consideremos agora um ataque em que os bits preparados por Alice em um dos estados $|u\rangle$, $|v\rangle$, $|\bar{u}\rangle$, $|\bar{v}\rangle$ interagem com a sonda de Eva que inicialmente está preparada em um estado $|w\rangle$ [15]. O bit e a sonda se submetem a uma interação conjunta que evolui unitariamente da seguinte forma,

$$\begin{aligned} |e_m \otimes w\rangle &\rightarrow U\,|e_m \otimes w\rangle \\ &= \sum_n |e_n\rangle\,\langle e_n|U\,|e_m \otimes w\rangle \\ &= \sum_n |e_n\rangle \otimes |\Phi_{mn}\rangle\,, \end{aligned} \tag{5.1}$$

em que

$$|\Phi_{mn}\rangle \equiv \langle e_n|U|e_m \otimes w\rangle\,, \quad m,n = 0,1. \tag{5.2}$$

E consequentemente

$$\begin{aligned} \left\langle e_{m'} \otimes w|U^\dagger U|e_m \otimes w\right\rangle &= \langle e_{m'} \otimes w|\,U^\dagger \left(\sum_n |e_n\rangle\,\langle e_n|\right) U\,|e_m \otimes w\rangle \\ &= \sum_{n=0,1} \langle \Phi_{m'n}|\Phi_{mn}\rangle \\ &= \delta_{m'm}, \quad m',m = 0,1. \end{aligned} \tag{5.3}$$

A sonda e o fóton se tornam correlacionados seguindo a evolução determinada pelo operador U conhecido por Eva. Portanto, uma medição sobre a sonda pode revelar para Eva informação parcial, ou até mesmo informação completa sobre o fóton [15].
Como no BB84 e no B92 os estados são equiprováveis, de forma que eles sejam simétricos, Eva também pode considerar que o seu dispositivo possue a mesma simetria. Podemos associar essa simetria como uma reflexão R que troca $e_0 \leftrightarrow e_1$, e essa reflexão pode ser considerada dentro do espaço da sonda de tal forma que o operador U e o estado inical da sonda $|w\rangle$ são invariantes sobre R. Logo, a reflexão R pode trocar os estados $|\Phi_{00}\rangle$ com $|\Phi_{11}\rangle$, e $|\Phi_{01}\rangle$ com $|\Phi_{10}\rangle$, e consequentemente o produto interno obedecem às simetrias

$$\begin{aligned} \langle \Phi_{00}|\Phi_{01}\rangle &= \langle \Phi_{11}|\Phi_{10}\rangle\,, \\ \langle \Phi_{00}|\Phi_{10}\rangle &= \langle \Phi_{11}|\Phi_{01}\rangle\,, \\ \|\Phi_{00}\| = \|\Phi_{11}\| \;\text{ e }\; \|\Phi_{01}\| &= \|\Phi_{10}\|\,. \end{aligned} \tag{5.4}$$

Vamos agora escolher uma determinada base ortonormal $\{w_\beta\}$ no espaço da sonda. Se $|\Phi_{01}\rangle = \pm|\Phi_{10}\rangle$, escolhendo uma base $\{w_1, w_2\}$ no plano contendo $|\Phi_{01}\rangle$ e ortogonal ao espelho plano de reflexão R, podemos escever $|\Phi_{01}\rangle$, $|\Phi_{10}\rangle$, da forma

$$|\Phi_{01}\rangle = X_5\,|w_1\rangle + X_6\,|w_2\rangle\,, \tag{5.5}$$

$$|\Phi_{10}\rangle = X_6\,|w_1\rangle + X_5\,|w_2\rangle\,. \tag{5.6}$$

Notemos que $|w_1\rangle$ e $|w_2\rangle$ são trocados pela reflexão R, de modo que as projeções, $X_1 \equiv \langle\Phi_{00}|w_1\rangle = \langle\Phi_{11}|w_2\rangle$, e similarmente $X_2 \equiv \langle\Phi_{00}|w_2\rangle = \langle\Phi_{11}|w_1\rangle$. É necessário também, escolher mais dois vetores base $\{w_0, w_3\}$ de modo que sejam selecionados no plano definimos por $\left|\tilde{\Phi}_{00}\right\rangle$, $\left|\tilde{\Phi}_{11}\right\rangle$ de $|\Phi_{00}\rangle$ e $|\Phi_{11}\rangle$ ortogonais a $|w_1\rangle$ e $|w_2\rangle$. E $|w_0\rangle$ e $|w_3\rangle$ podem ser escolhidos simetricamente para obtermos

$$|\Phi_{00}\rangle = X_0\,|w_0\rangle + X_1\,|w_1\rangle + X_2\,|w_2\rangle + X_3\,|w_3\rangle\,, \tag{5.7}$$

$$|\Phi_{11}\rangle = X_3\,|w_0\rangle + X_2\,|w_1\rangle + X_1\,|w_2\rangle + X_0\,|w_3\rangle\,. \tag{5.8}$$

Assim escrevemos os quatros vetores de interesse $|\Phi_{mn}\rangle$ que estão contidos no espaço com quatro dimensões gerado por $\{|w_0\rangle\,, |w_1\rangle\,, |w_2\rangle\,, |w_3\rangle\}$.
Da Eq. (5.3) em conjunto com o que foi dito acima, exprimimos algumas restrições,

$$\|\Phi_{00}\|^2 + \|\Phi_{01}\|^2 = \|\Phi_{10}\|^2 + \|\Phi_{11}\|^2 \;=\; X_5^2 + X_6^2 + X_0^2 + X_3^2 + X_1^2 + X_2^2 = 1, \tag{5.9}$$

$$\langle\Phi_{10}|\Phi_{00}\rangle + \langle\Phi_{01}|\Phi_{00}\rangle \;=\; 2\,(X_1X_6 + X_2X_5) = 0. \tag{5.10}$$

Essas restrições podem ser satisfeitas por meio da seguinte parametrização

$$\begin{aligned} X_0 &= \sin\lambda\cos\mu, \qquad X_1 = \cos\lambda\cos\sigma\cos\phi, \\ X_2 &= \cos\lambda\cos\sigma\sin\phi, \qquad X_3 = \sin\lambda\sin\mu, \\ X_5 &= \cos\lambda\sin\sigma\cos\phi, \qquad X_6 = -\cos\lambda\sin\sigma\sin\phi. \end{aligned} \tag{5.11}$$

em que $\lambda, \mu, \sigma, \phi$, são quatro variáveis independentes.
A evolução descrita na Eq.(5.2) mostra que o fóton e a sonda estão em um estado quântico emaranhado, gerando uma relação entre as medida de Bob e Eva. Cada resultado observado por Bob é associado a um estado projetado ρ da sonda. Agora, Eva terá que determinar esse estado particular ρ, com probabilidade *a priori* p_i.
Vamos supor que Eva utilize um POVM para criar operadores E_m. O POVM quando

aplicado a um estado representado por uma matriz densidade ρ, produz cada resultado m com probabilidade

$$p(m|\rho) = tr(E_m \rho). \tag{5.12}$$

Após obter um resultado m, podemos calcular a probabilidade *a posteriori* através do teorema de Bayes,

$$q_{im} \equiv p(\rho|m) = \frac{p(m|\rho)p(\rho)}{p(m)}, \tag{5.13}$$

em que $p_m = p(m) = tr(E_m \sum p_i \rho^{(i)})$ é a probabilidade *a priori* do resultado m. Em vista disso, a entropia de Shannon do estado inicial da sonda é

$$H_0 = -\sum_i p_i \log p_i, \tag{5.14}$$

e a entropia de Shannon em relação ao valor *a posteriori* seguindo o resultado m é

$$H_m = -\sum_i q_{im} \log q_{im}, \tag{5.15}$$

e por conseguinte, o valor esperado do ganho de informação que Eva obtem a partir do POVM é expressado como

$$\begin{aligned} I &= \sum_m p_m (H_0 - H_m) \\ &= \sum_m p_m \left(-\sum_i p_i \log p_i + \sum_i q_{im} \log q_{im} \right). \end{aligned} \tag{5.16}$$

Os resultados dessa seção serão aplicados nos protocolos BB84 e B92. Em cada caso, os parâmetros $\lambda, \mu, \sigma, \phi$ serão relacionados com a taxa de erro ϵ de Bob, que para um ϵ fixo essas variáveis podem ser ajustadas de modo a minimizar a superposição entre os estados.

5.2 Espionagem no BB84

Vamos denotar $(i; j)$ como o evento em que Alice transmite o estado $|i\rangle$, que, seguindo a evolução conjunta U de $|i\rangle$ com a sonda de Eva, Bob observa o resultado $|j\rangle$ ao executar uma medida projetiva, em que $i, j \in \{u, \bar{u}, v, \bar{v}\}$, e esse evento ocorre com uma probabilidade

$$\begin{aligned} P_{i.j} &\equiv Prob(j|i; \{j, \bar{j}\}) = \mathrm{tr}(|j\rangle \langle j| \rho^{(i)}) \\ &= \left\langle i \otimes w | U^\dagger | j \right\rangle \langle j | U | i \otimes w \rangle \\ &= \langle \psi_{i,j} | \psi_{i,j} \rangle = \left\| \psi_{i,j} \right\|^2, \quad \text{em que } |\psi_{i,j}\rangle \equiv \langle j|U|i \otimes w\rangle . \end{aligned} \tag{5.17}$$

Também podemos escrever equações explícitas para a Eq.(5.17) utilizando a Eq.(5.2) das seguintes formas:

$$\begin{aligned}
|\psi_{u,v}\rangle &= \langle v|U|u\otimes w\rangle \\
&= (\sin\alpha\,\langle e_0| + \cos\alpha\,\langle e_1|)\,U\,(\cos\alpha\,|e_0\otimes w\rangle + \sin\alpha\,|e_1\otimes w\rangle) \\
&= \sin\alpha\cos\alpha\,\langle e_0|U|e_0\otimes w\rangle + \sin^2\alpha\,\langle e_0|U|e_1\otimes w\rangle + \cos^2\alpha\,\langle e_1|U|e_0\otimes w\rangle \\
&\quad + \sin\alpha\cos\alpha\,\langle e_1|U|e_1\otimes w\rangle \\
|\psi_{u,v}\rangle &= \cos^2\alpha\,|\Phi_{01}\rangle + \sin^2\alpha\,|\Phi_{10}\rangle + \sin\alpha\cos\alpha\,(|\Phi_{00}\rangle + |\Phi_{11}\rangle)\,, \qquad (5.18) \\
|\psi_{u,u}\rangle &= \cos^2\alpha\,|\Phi_{00}\rangle + \sin^2\alpha\,|\Phi_{11}\rangle + \sin\alpha\cos\alpha\,(|\Phi_{10}\rangle + |\Phi_{01}\rangle)\,, \qquad (5.19) \\
|\psi_{u,\bar{v}}\rangle &= \cos^2\alpha\,|\Phi_{00}\rangle - \sin^2\alpha\,|\Phi_{11}\rangle + \sin\alpha\cos\alpha\,(|\Phi_{10}\rangle - |\Phi_{01}\rangle)\,, \qquad (5.20) \\
|\psi_{u,\bar{u}}\rangle &= \cos^2\alpha\,|\Phi_{01}\rangle - \sin^2\alpha\,|\Phi_{10}\rangle + \sin\alpha\cos\alpha\,(|\Phi_{11}\rangle + |\Phi_{00}\rangle)\,, \qquad (5.21) \\
|\psi_{v,\bar{u}}\rangle &= \cos^2\alpha\,|\Phi_{11}\rangle - \sin^2\alpha\,|\Phi_{00}\rangle + \sin\alpha\cos\alpha\,(|\Phi_{01}\rangle - |\Phi_{10}\rangle)\,, \qquad (5.22) \\
|\psi_{\bar{u},u}\rangle &= \cos^2\alpha\,|\Phi_{10}\rangle - \sin^2\alpha\,|\Phi_{01}\rangle + \sin\alpha\cos\alpha\,(|\Phi_{11}\rangle + |\Phi_{00}\rangle)\,, \qquad (5.23) \\
|\psi_{\bar{u},\bar{u}}\rangle &= \cos^2\alpha\,|\Phi_{11}\rangle + \sin^2\alpha\,|\Phi_{00}\rangle - \sin\alpha\cos\alpha\,(|\Phi_{10}\rangle + |\Phi_{01}\rangle)\,. \qquad (5.24)
\end{aligned}$$

Utilizando as simetrias das Eqs.(5.4) e (5.9), obtemos os seguintes produtos internos,

$$\begin{aligned}
\|\psi_{u,v}\|^2 &= \langle\psi_{u,v}|\psi_{u,v}\rangle \\
&= \left[\cos^2\alpha\,\langle\Phi_{01}| + \sin^2\alpha\,\langle\Phi_{10}| + \sin\alpha\cos\alpha\,(\langle\Phi_{00}| + \langle\Phi_{11}|)\right] \\
&\quad \left[\cos^2\alpha\,|\Phi_{01}\rangle + \sin^2\alpha\,|\Phi_{10}\rangle + \sin\alpha\cos\alpha\,(|\Phi_{00}\rangle + |\Phi_{11}\rangle)\right] \\
&= \left(\cos^4\alpha + \sin^4\alpha\right)\|\Phi_{01}\|^2 + \frac{\sin^2 2\alpha}{2}\left(\|\Phi_{00}\|^2 + \langle\Phi_{00}|\Phi_{11}\rangle + \langle\Phi_{10}|\Phi_{01}\rangle\right) \\
&\quad + \sin 2\alpha\,(\langle\Phi_{00}| + \langle\Phi_{11}|)\left[|\Phi_{01}\rangle + (|\Phi_{10}\rangle + |\Phi_{01}\rangle)\sin^2\alpha\right] \\
&= \|\Phi_{01}\|^2 + \frac{\sin^2 2\alpha}{2}\left(\|\Phi_{00}\|^2 - \|\Phi_{01}\|^2 + \langle\Phi_{00}|\Phi_{11}\rangle + \langle\Phi_{10}|\Phi_{01}\rangle\right) \\
&\quad + \sin 2\alpha\,\langle\Phi_{11}|\,(|\Phi_{10}\rangle + |\Phi_{01}\rangle) \\
&= \frac{1}{2}\left[(1-d) + (d+a)\sin^2 2\alpha + c\sin 2\alpha\right], \qquad (5.25) \\
\|\psi_{u,u}\|^2 &= \frac{1}{2}\left[(1+d) + (a-d)\sin^2 2\alpha + c\sin 2\alpha\right], \qquad (5.26) \\
\|\psi_{u,\bar{v}}\|^2 &= \frac{1}{2}\left[(1+d) - (d+a)\sin^2 2\alpha - c\sin 2\alpha\right], \qquad (5.27) \\
\|\psi_{u,\bar{u}}\|^2 &= \frac{1}{2}\left[(1-d) + (d-a)\sin^2 2\alpha - c\sin 2\alpha\right], \qquad (5.28) \\
\|\psi_{\bar{u},u}\|^2 &= \frac{1}{2}\left[(1-d) + (d-a)\sin^2 2\alpha + c\sin 2\alpha\right], \qquad (5.29) \\
\|\psi_{\bar{u},\bar{u}}\|^2 &= \frac{1}{2}\left[(1+d) + (a-d)\sin^2 2\alpha - c\sin 2\alpha\right], \qquad (5.30)
\end{aligned}$$

em que a, b, c e d, são definidos na forma

$$\begin{aligned} a &\equiv \Phi_{00}\Phi_{11} + \Phi_{01}\Phi_{10} = 2\left(X_0X_3 + X_1X_2 + X_5X_6\right) \\ &= \sin^2\lambda \sin 2\mu + \cos^2\lambda \cos 2\sigma \sin 2\phi, \qquad (5.31) \\ b &\equiv \Phi_{00}\Phi_{11} - \Phi_{01}\Phi_{10} = 2\left(X_0X_3 + X_1X_2 - X_5X_6\right) \\ &= \sin^2\lambda \sin 2\mu + \cos^2\lambda \sin 2\phi, \qquad (5.32) \\ c &\equiv 2\Phi_{00}\left(\Phi_{01} \pm \Phi_{10}\right) = 2\Phi_{11}\left(\Phi_{10} \pm \Phi_{01}\right) = 2\left(X_1 \pm X_2\right)\left(X_5 \pm X_6\right) \\ &= \cos^2\lambda \sin 2\sigma \sin 2\phi, \qquad (5.33) \\ d &\equiv \Phi_{00}^2 - \Phi_{01}^2 = X_0^2 + X_1^2 + X_2^2 + X_3^2 - X_5^2 - X_6^2 \\ &= \sin^2\lambda + \cos^2\lambda \sin 2\sigma. \qquad (5.34) \end{aligned}$$

E finalmente,

$$\begin{aligned} \langle\psi_{u,\bar{v}}|\psi_{v,\bar{u}}\rangle &= \frac{1}{2}\left[(a+b) - (1+b)\sin^2 2\alpha + c\sin 2\alpha\right], \qquad (5.35) \\ \langle\psi_{u,u}|\psi_{\bar{u},\bar{u}}\rangle &= \frac{1}{2}\left[(a+b) + (d-a)\sin^2 2\alpha\right]. \qquad (5.36) \end{aligned}$$

Assumindo que Eva é capaz de preservar o estado $|\psi_{i,j}\rangle$ até o momento em que Alice e Bob conferem publicamente as bases dos seus fótons, ela deve agora distinguir apenas entre dois estados associados à base anunciada, isto é, distinguir entre $|\psi_{u,u}\rangle$ e $|\psi_{\bar{u},\bar{u}}\rangle$, ou entre $|\psi_{v,v}\rangle$ e $|\psi_{\bar{v},\bar{v}}\rangle$. Como conhecemos os estados $|\psi_{i,j}\rangle$, podemos calcular a taxa de erro ϵ. Uma vez que as escolhas de Alice e Bob são aleatórias e simétricas, a taxa de erro é dada por

$$\begin{aligned} \epsilon &= \frac{P_{u,\bar{u}} + P_{\bar{u},u} + P_{v,\bar{v}} + P_{\bar{v},v}}{P_{u,\bar{u}} + P_{\bar{u},u} + P_{v,\bar{v}} + P_{\bar{v},v} + P_{u,u} + P_{\bar{u},\bar{u}} + P_{v,v} + P_{\bar{v},\bar{v}}}, \qquad (5.37) \\ &= \frac{\|\psi_{u,\bar{u}}\|^2 + \|\psi_{\bar{u},u}\|^2}{\|\psi_{u,\bar{u}}\|^2 + \|\psi_{\bar{u},u}\|^2 + \|\psi_{u,u}\|^2 + \|\psi_{\bar{u},\bar{u}}\|^2} \qquad (5.38) \\ &= \frac{(1-d) + (d-a)\sin^2 2\alpha}{(1-d) + (d-a)\sin^2 2\alpha + (1+d) + (a-d)\sin^2 2\alpha} \\ &= \frac{1}{2}\left[1 - \frac{1}{2}(d+a)\right]. \qquad (5.39) \end{aligned}$$

A intenção de Eva é obter o máximo de informação possível sobre os fótons de Bob, e para isso ela deve minimizar a superposição, S entre os estados que ela deve distinguir ,

$$S = \frac{\langle\psi_{u,u}|\psi_{\bar{u},\bar{u}}\rangle}{\|\psi_{u,u}\|\,\|\psi_{\bar{u},\bar{u}}\|} = \frac{\langle\psi_{v,v}|\psi_{\bar{v},\bar{v}}\rangle}{\|\psi_{v,v}\|\,\|\psi_{\bar{v},\bar{v}}\|} \tag{5.40}$$

$$= \frac{\frac{1}{2}(a+b)+\frac{1}{2}(d-a)\sin^2 2\alpha}{\sqrt{\frac{1}{2}\left[(1+d)+(a-d)\sin^2 2\alpha+c\sin 2\alpha\right]}\sqrt{\frac{1}{2}\left[(1+d)+(a-d)\sin^2 2\alpha-c\sin 2\alpha\right]}}$$

$$= \frac{b+\frac{1}{2}(a+d)}{\sqrt{\left[1+\frac{1}{2}(a+d)\right]^2-\frac{1}{2}c^2}}$$

$$= \frac{1-2\epsilon+b}{\sqrt{\left[2-2\epsilon\right]^2-\frac{1}{2}c^2}}. \tag{5.41}$$

E, as condições mínimização para um ϵ constante são,

$$\lambda=\mu=0, \qquad \cos\sigma=1, \qquad -1<\sin 2\phi\leq 1, \tag{5.42}$$

consequentemente,

$$a=b=\sin 2\alpha, \qquad c=0, \qquad d=1, \tag{5.43}$$

que substituindo na Eq.(5.40), obtemos

$$\epsilon=\frac{1}{4}(1-\sin 2\phi). \tag{5.44}$$

Portanto, o mínimo condicional de S é

$$S_{min}=\frac{1-2\epsilon+\sin 2\alpha}{2(1-\epsilon)}=3-\frac{2}{1-\epsilon} \tag{5.45}$$

A Eq.(5.45) reforça o que foi dito anteriormente, que, Eva não consegue espionar sem introduzir erros, e para que ela tenha o total conhecimento da transmissão a taxa de erro deve ser $\epsilon=\frac{1}{3}$, que fornece, $S=0$.

5.3 Espionagem no B92

Assumiremos aqui que Bob escolhe o método mais simples em vez de um mais eficiente, isto é, ele escolhe um tipo von Neumann em vez de um POVM, embora o número de resultados inconclusivos são reduzidos com um POVM. A operação do B92 na sua variante de von Neumann é a seguinte: um fóton transmitido por Alice em um dos estados $|u\rangle$ e $|v\rangle$, é medido por Bob em uma das bases ortonormais $\{u,\bar{u}\}$, $\{v,\bar{v}\}$. A

medição de Bob no estado $|\bar{v}\rangle$ exclui o estado de entrada $|v\rangle$, e isso indica com segurança o estado $|u\rangle$, e portanto, o seu valor 1; e a medição no estado $|u\rangle$ indica $|v\rangle$,e portanto, o valor do bit 0. E os resultados das medições nos estados $|v\rangle$ e $|u\rangle$, que são consistentes com as entradas $|v\rangle$ e $|u\rangle$, são descartados como inconclusivos. Com isso em mente, podemos agora descrever a taxa de erro como

$$\begin{aligned}\epsilon &= \frac{P_{u,\bar{u}} + P_{v,\bar{v}}}{P_{u,\bar{v}} + P_{u,\bar{u}} + P_{v,\bar{u}} + P_{v,\bar{v}}} \\ &= \frac{P_{u,\bar{u}}}{P_{u,\bar{v}} + P_{u,\bar{u}}} \\ &= \frac{\|\psi_{u,\bar{u}}\|^2}{\|\psi_{u,\bar{v}}\|^2 + \|\psi_{u,\bar{u}}\|^2}. \end{aligned} \tag{5.46}$$

Utilizando as Eqs (5.27) e (5.28), obtemos

$$\begin{aligned}\epsilon &= \frac{\|\psi_{u,\bar{u}}\|^2}{\|\psi_{u,\bar{v}}\|^2 + \|\psi_{u,\bar{u}}\|^2} = \frac{1}{2}\left[\frac{(1-d) + (d-a)\sin^2 2\alpha - c\sin 2\alpha}{1 - a\sin^2 2\alpha - c\sin 2\alpha}\right] \\ &= \frac{1}{2}\left(1 - \frac{d\cos^2 2\alpha}{1 - a\sin^2 2\alpha - c\sin 2\alpha}\right). \end{aligned} \tag{5.47}$$

Agora, Eva terá que distinguir os estados $|\psi_{u,\bar{v}}\rangle$ e $|\psi_{v,\bar{u}}\rangle$, pois os outros resultados aparecem como erros ou inconclusivos. Logo, nesse caso, S é escrito na forma

$$S = \frac{\langle\psi_{u,\bar{v}}|\psi_{v,\bar{u}}\rangle}{\|\psi_{u,\bar{v}}\|\,\|\psi_{v,\bar{u}}\|} = \frac{\langle\psi_{u,\bar{v}}|\psi_{v,\bar{u}}\rangle}{\|\psi_{u,\bar{v}}\|^2}, \tag{5.48}$$

que, utilizando as Eqs. (5.20), (5.22) e (5.27) podemos reescrevê-la na forma

$$S = \frac{\langle\psi_{u,\bar{v}}|\psi_{v,\bar{u}}\rangle}{\|\psi_{u,\bar{v}}\|^2} = \frac{(a+b) - (1+b)\sin^2 2\alpha + c\sin 2\alpha}{(1+d) - (a+d)\sin^2 2\alpha - c\sin 2\alpha}. \tag{5.49}$$

Na seção seguinte apresentaremos uma implementação dessa espionagem com uma solução específica para os parâmetros $\{\lambda, \mu, \sigma, \phi\}$, utilizando uma variável auxiliar γ pelas relações

$$\lambda = \mu = 0, \qquad \sin 2\phi = \frac{\sin\gamma}{\sin\delta}, \qquad \cos 2\sigma = \frac{\cos\delta}{\cos\gamma}, \qquad \text{com} - \delta \leq \gamma \leq \delta, \tag{5.50}$$

em que

$$\sin\delta \equiv \frac{\sin 2\alpha}{\sqrt{1+\sin^2 2\alpha}}, \qquad \cos\delta \equiv \frac{1}{\sqrt{1+\sin^2 2\alpha}}, \qquad \text{com} \qquad 0 < \delta < \frac{\pi}{4}, \tag{5.51}$$

e os ângulos ϕ e σ são escolhidos de forma que $\cos 2\phi \geq 0$ e $\sin 2\sigma \geq 0$. E a interação toma a forma

$$|u \otimes w\rangle \to U\,|u \otimes w\rangle = x\,|u \otimes w_u\rangle + y\,|v \otimes w_v\rangle\,, \tag{5.52}$$

$$|v \otimes w\rangle \to U\,|v \otimes w\rangle = y\,|u \otimes w_u\rangle + x\,|v \otimes w_v\rangle \tag{5.53}$$

em que

$$|w_u\rangle \equiv \cos\gamma\,|w_1\rangle + \sin\gamma\,|w_2\rangle\,, \tag{5.54}$$

$$|w_v\rangle \equiv \sin\gamma\,|w_1\rangle + \cos\gamma\,|w_2\rangle\,. \tag{5.55}$$

E que também mudaremos a notação de $|w\rangle$ para $|e\rangle$.

5.4 Implementação no B92

Para um estado de polarização $|\psi\rangle$ arbitrário, dado por

$$|\psi\rangle = \alpha\,|u\rangle + \beta\,|v\rangle\,, \tag{5.56}$$

em que α e β são constantes reais, e os valores esperados dos operadores POVMs dados pelas Eqs. (4.19) - (4.21), se tornam

$$\langle\psi|A_u|\psi\rangle = \alpha^2\,(1-\cos\theta)\,, \tag{5.57}$$

$$\langle\psi|A_v|\psi\rangle = \beta^2\,(1-\cos\theta)\,, \tag{5.58}$$

$$\langle\psi|A_?|\psi\rangle = (\alpha+\beta)^2\cos\theta. \tag{5.59}$$

A implementação estudada nesse trabalho esta representada na Fig.5.1 [16]. O circuito

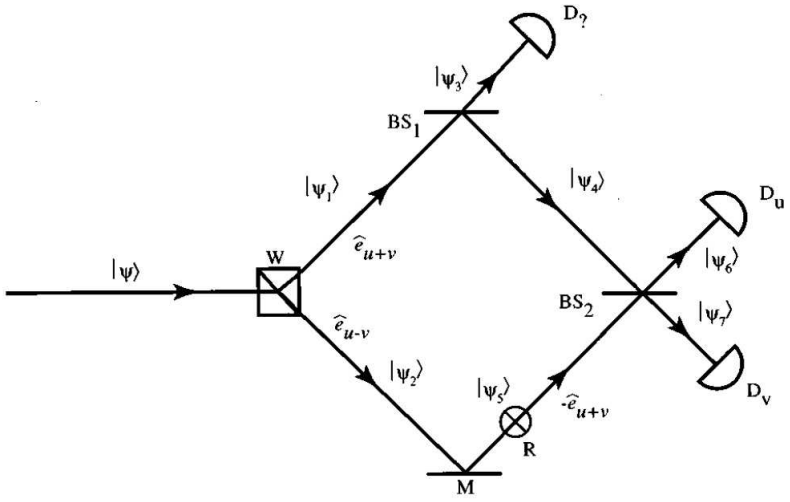

Figura 5.1: Circuito que implementa um POVM na transmissão de dois estados quânticos não-ortogonais

apresentado é um sistema óptico. As linhas retas com setas representam os possíveis caminhos que os fótons podem seguir através do circuito. O caminho marcado por $|\psi\rangle$ é

a entrada do fóton represenado pela Eq.(5.56). D_u, D_v, $D_?$ são detectores de fótons que representam as medidas dos operadores A_u, A_v, $A_?$, respectivamente, que aqui tratamos como ideais. W é um prisma de Wollaston, que está alinhado de modo que um fóton incidente com vetor de polarização $\mathbf{e}_{u+v}$ tomará o caminho pelo estado $|\psi_1\rangle$ e $\mathbf{e}_{u+v}$ e não o caminho pelo vetor de polarização $\mathbf{e}_{u-v}$ e $|\psi_2\rangle$, em que $\mathbf{e}_{u+v}$ denota um vetor unidade de polarização correspondente ao estado $|u+v\rangle = |u\rangle + |v\rangle$ e é perpendicular ao vetor unidade de polarização $\mathbf{e}_{u+v}$ correspondente ao estado de polarização $|u-v\rangle = |u\rangle - |v\rangle$. Os estados $|u+v\rangle$ e $|u-v\rangle$ são ortogonais e possuem

$$\langle u+v|u-v\rangle = 0, \qquad \mathbf{e}_{u+v}\cdot\mathbf{e}_{u-v} = 0. \tag{5.60}$$

O circuito também apresenta dois beam splitters denotados por BS_1 e BS_2, e o BS_2 é um beam splitter 50-50 para que um fóton possa entrar em qualquer entrada. No circuito também é apresentado um espelho, M, e um rotador de polarização $\pi/2$, R, que transforma um fóton com vetor de polarização $\mathbf{e}_{u-v}$ em um vetor de polarização $-\mathbf{e}_{u+v}$. Para descrevermos a dinâmica do circuito, devemos escrever as expressões para os estados $|\psi_i\rangle$ dos fótons $i = 1, 2, ..., 7$. Os estados são

$$\begin{aligned}
|\psi_1\rangle &= \frac{\langle\psi|e_{u+v}\rangle}{\|e_{u+v}\|}|e_{u+v}\rangle \\
&= (\alpha\langle u| + \beta\langle v|)\left(\frac{|u+v\rangle}{\|u+v\|}\right)|e_{u+v}\rangle \\
&= \frac{\alpha(\langle u|u\rangle + \langle u|v\rangle) + \beta(\langle v|u\rangle) + \langle v|v\rangle}{\sqrt{\langle u+v|v+u\rangle}}|e_{u+v}\rangle \\
&= (\alpha+\beta)\frac{1+\cos\theta}{\sqrt{2(1+\cos\theta)}}|e_{u+v}\rangle \\
|\psi_1\rangle &= 2^{-1/2}(\alpha+\beta)(1+\cos\theta)^{1/2}|e_{u+v}\rangle, \qquad (5.61)\\
|\psi_2\rangle &= 2^{-1/2}(\alpha-\beta)(1+\cos\theta)^{1/2}|e_{u-v}\rangle. \qquad (5.62)
\end{aligned}$$

Dado que iremos tratar de detectores ideais, logo, devemos ter

$$\langle\psi|A_?|\psi\rangle = \langle\psi_3|\psi_3\rangle, \tag{5.63}$$

$$\langle\psi|A_u|\psi\rangle = \langle\psi_6|\psi_6\rangle, \tag{5.64}$$

$$\langle\psi|A_v|\psi\rangle = \langle\psi_7|\psi_7\rangle, \tag{5.65}$$

em que cada medida associada aos detectores equivale à probabilidade dos estados dos fótons incidentes nos detectores. E a partir disso, obtemos

$$\begin{aligned} \langle\psi_3|\psi_3\rangle &= \langle\psi|A_?|\psi\rangle \\ &= (\alpha+\beta)^2\cos\theta. \end{aligned} \tag{5.66}$$

Logo,

$$|\psi_3\rangle = (\alpha+\beta)^2(\cos\theta)^{1/2}|e_{u+v}\rangle\,. \tag{5.67}$$

Para escrevermos a expressão para o estado $|\psi_4\rangle$, devemos analisar a dinâmica do BS_1. Como o estado $|\psi_1\rangle$, ao passar pelo BS_1, transmite $|\psi_3\rangle$ para o detector $D_?$, logo, devemos ter

$$\begin{aligned} T_1 &= \frac{\langle\psi_3|\psi_3\rangle}{\langle\psi_1|\psi_1\rangle} = \frac{(\alpha+\beta)^2\cos\theta}{2^{-1/2}(\alpha+\beta)(1+\cos\theta)^{1/2}} \\ &= 1-\tan^2\frac{\theta}{2}, \end{aligned} \tag{5.68}$$

como $T_1 = 1 - R_1$, logo

$$R_1 = \tan^2\frac{\theta}{2}. \tag{5.69}$$

Com isso, devemos ter

$$\begin{aligned} R_1 &= \frac{\langle\psi_4|\psi_4\rangle}{\langle\psi_1|\psi_1\rangle} \\ \langle\psi_4|\psi_4\rangle &= R_1\langle\psi_1|\psi_1\rangle \\ &= \tan^2\left(\frac{\theta}{2}\right)\frac{(\alpha+\beta)^2}{2}(1+\cos\theta) \\ &= \frac{(\alpha+\beta)^2}{2}(1-\cos\theta)\,, \end{aligned} \tag{5.70}$$

e

$$|\psi_4\rangle = i2^{-1/2}(\alpha+\beta)(1-\cos\theta)^{1/2}|e_{u+v}\rangle\,, \tag{5.71}$$

já que o estado $|\psi_4\rangle$ é o resultado da reflexão do estado $|\psi_1\rangle$ no BS_1, e $i = \exp\left(i\frac{\pi}{2}\right)$ é o fator de fase.

Agora, para o estado $|\psi_5\rangle$, devemos analisar o rotador de polarização R, que converte a polarização da direção $\mathbf{e}_{u-v}$ para $-\mathbf{e}_{u+v}$, de modo que

$$|\psi_5\rangle = -2^{-1/2}(\alpha-\beta)(1-\cos\theta)|e_{u+v}\rangle\,. \tag{5.72}$$

Seguindo a mesma linha de pensamento adotada no BS_1 para o BS_2, mas com o diferencial de que o BS_2 é 50-50, isto é,

$$R_2 = T_2 = \frac{1}{2}. \tag{5.73}$$

Com isso em mente e analisando a Fig.(5.1), verificamos que

$$|\psi_6\rangle = \sqrt{T_2}\,|\psi_5\rangle + i\sqrt{R_2}\,|\psi_4\rangle = -\alpha\,(1-\cos\theta)^{1/2}\,|e_{u+v}\rangle\,, \tag{5.74}$$

$$|\psi_7\rangle = \sqrt{T_2}\,|\psi_4\rangle + i\sqrt{R_2}\,|\psi_5\rangle = i\beta\,(1-\cos\theta)^{1/2}\,|e_{u+v}\rangle\,. \tag{5.75}$$

Para conservar a probabilidade, devemos analisar se

$$\langle\psi_3|\psi_3\rangle + \langle\psi_6|\psi_6\rangle + \langle\psi_7|\psi_7\rangle = \langle\psi|\psi\rangle\,, \tag{5.76}$$

$$(\alpha+\beta)^2\cos\theta + \alpha^2\,(1-\cos\theta) + \beta^2\,(1-\cos\theta) = (\alpha\,\langle u|\,\beta\,\langle v|)\,(\alpha\,|u\rangle + \beta\,|v\rangle)$$

$$\alpha^2 + \beta^2 + 2\alpha\beta\cos\theta = \alpha^2 + \beta^2 + 2\alpha\beta\cos\theta, \tag{5.77}$$

e isso mostra que o circuito satisfaz as estatísticas.

5.4.1 Espionagem

Aqui denotaremos o estado inicial da sonda de Eva como $|e\rangle$, que ao interagir com os estados $|u\rangle$ e $|v\rangle$, gera

$$|\phi_1\rangle = |u\rangle \otimes |e\rangle\,, \tag{5.78}$$

$$|\phi_2\rangle = |v\rangle \otimes |e\rangle\,, \tag{5.79}$$

que, após sua espionagem, gera

$$\left|\phi_1^{'}\right\rangle = a\,|u\otimes e_u\rangle + b\,|v\otimes e_v\rangle\,, \tag{5.80}$$

$$\left|\phi_2^{'}\right\rangle = b\,|u\otimes e_u\rangle + a\,|v\otimes e_v\rangle\,, \tag{5.81}$$

em que a e b são constantes reais. Os estados da sonda foram escolhidos de forma a serem orientados simetricamente em relação a base $\{|e_0, |e_1\rangle\rangle\}$, como mostra a Fig. (5.2).

Escrevendo os estados na forma, Eqs. (5.55) e (5.56),

$$|e_u\rangle = \cos\gamma\,|e_0\rangle + \sin\gamma\,|e_1\rangle\,, \tag{5.82}$$

$$|e_v\rangle = \sin\gamma\,|e_0\rangle + \cos\gamma\,|e_1\rangle\,, \tag{5.83}$$

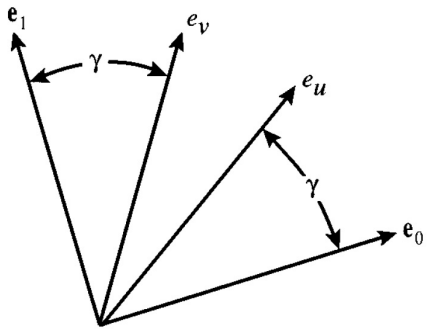

Figura 5.2: Relação entre os vetores base da sonda de Eva e dos estados transmitidos

com $\langle e_u|e_v\rangle = \sin 2\gamma$, as seguintes normalizações devem ser assumidas,

$$\|\phi_1\|^2 = \|\phi_2\|^2 = \|\phi_1'\|^2 = \|\phi_2'\|^2 = 1 \qquad \text{e} \tag{5.84}$$

$$\langle e_u|e_u\rangle = \langle e_v|e_v\rangle = 1. \tag{5.85}$$

Como a correlação entre os estados de Eva e os fótons é determinada por uma operação unitária, a unitariedade exige que

$$\begin{aligned} (\langle\phi_1| + \langle\phi_2|)(|\phi_1\rangle + |\phi_2\rangle) &= (\langle\phi_1'| + \langle\phi_2'|)(|\phi_1'\rangle + |\phi_2'\rangle) \\ \langle\phi_1|\phi_2\rangle + \langle\phi_2|\phi_1\rangle &= \langle\phi_1'|\phi_2'\rangle + \langle\phi_2'|\phi_1'\rangle . \end{aligned}$$

Dizendo que $Re\langle\phi_1|\phi_2\rangle = Re\langle\phi_1'|\phi_2'\rangle$, obtemos

$$\sin 2\alpha = 2ab + \left(a^2 + b^2\right)\sin 2\alpha \sin^2 2\gamma. \tag{5.86}$$

Lembrando que,

$$\langle\phi_1'|\phi_1'\rangle = 1 = a^2 + b^2 + 2ab\sin 2\alpha \sin^2 2\gamma, \tag{5.87}$$

a unitariedade será restrigida apenas aos valores dos parâmetros de emaranhamento a, b e γ da sonda de Eva para um ângulo específico α.

Para maximizar a informação sobre os estados dos fótons, Eva utilizará medições tipo von Neumann. A fim de simplificar e tornar a compreensão mais clara, iremos inserir os índices α, β e ϵ, que representam respectivamente, a transmissão de Alice, a recepção de Bob e a pertubação de Eva. Portanto, o estado $|\epsilon\alpha\rangle$ é o estado pertubado que Eva transmite a Bob depois de medir ϵ quando Alice transmite α. O efeito da medição pode ser representado por

$$P_0 = I \otimes |e_0\rangle\langle e_0| \qquad \text{e} \qquad P_1 = I \otimes |e_1\rangle\langle e_1| . \tag{5.88}$$

A amplitude de probabilidade de Eva medir 0 quando Alice envia 0, $|00\rangle$ é medida a partir da projeção Eq.(5.89)

$$\begin{aligned} P_0 |\phi_1'\rangle &= |00\rangle \otimes |e_0\rangle \\ P_0 |\phi_1'\rangle &= (I \otimes |e_0\rangle \langle e_0|) (a |u \otimes e_u\rangle + b |v \otimes e_v\rangle) \\ &= a \langle e_0|e_u\rangle |u\rangle \otimes |e_0\rangle + b \langle e_0|e_v\rangle |v\rangle \otimes |e_0\rangle \\ &= a \cos\gamma |u\rangle |e_0\rangle + b \sin\gamma |v\rangle |e_0\rangle , \end{aligned} \tag{5.89}$$

comparando com Eq.(5.90), obtemos

$$|00\rangle = a \cos\gamma |u\rangle + b \sin\gamma |v\rangle . \tag{5.90}$$

De forma similar, a amplitude de probabilidade de Eva medir 1 quando Alice envia 0, $|10\rangle$ é determinada por

$$\begin{aligned} P_1 |\phi_1'\rangle &= |10\rangle \otimes |e_1\rangle \\ &= a \sin\gamma |u\rangle |e_1\rangle + b \cos\gamma |v\rangle |e_1\rangle , \end{aligned} \tag{5.91}$$

com,

$$|10\rangle = a \sin\gamma |u\rangle + b \cos\gamma |v\rangle . \tag{5.92}$$

A amplitude de probabilidade de Eva medir 0 quando Alice envia 1, $|01\rangle$ é determinada por

$$\begin{aligned} P_0 |\phi_2'\rangle &= |01\rangle \otimes |e_0\rangle \\ &= b \cos\gamma |u\rangle |e_0\rangle + a \sin\gamma |v\rangle |e_0\rangle , \end{aligned} \tag{5.93}$$

com,

$$|01\rangle = b \cos\gamma |u\rangle + a \sin\gamma |v\rangle . \tag{5.94}$$

E a amplitude de probabilidade de Eva medir 1 quando Alice envia 1, $|11\rangle$ é determinada por

$$\begin{aligned} P_1 |\phi_2'\rangle &= |11\rangle \otimes |e_0\rangle \\ &= b \sin\gamma |u\rangle |e_0\rangle + a \cos\gamma |v\rangle |e_0\rangle , \end{aligned} \tag{5.95}$$

com,

$$|11\rangle = b\sin\gamma\,|u\rangle + a\cos\gamma\,|v\rangle\,. \tag{5.96}$$

As Eqs. (5.91), (5.93), (5.95) e (5.97) sãos os quatro estados perturbados resultantes da perturbação de Eva na transmissão entre Alice e Bob. Já que calculamos as amplitudes de probabilidade, podemos agora calcular a probabilidade de Eva detectar ϵ e Bob detectar β quando Alice envia α, tal probabilidade é descrita por

$$p\,(\alpha,\epsilon,\beta) = \langle\epsilon\alpha|A_\beta|\epsilon\alpha\rangle\,, \tag{5.97}$$

que, para cada caso, obtemos

$$\begin{aligned}
p\,(0,0,0) &= \langle 00|A_0|00\rangle = a^2\,(1-\sin 2\alpha)\cos^2\gamma, && (5.98)\\
p\,(0,0,1) &= \langle 00|A_1|00\rangle = b^2\,(1-\sin 2\alpha)\sin^2\gamma, && (5.99)\\
p\,(0,0,?) &= \langle 00|A_?|00\rangle = (a\cos\gamma + b\sin\gamma)^2\sin 2\alpha, && (5.100)\\
p\,(0,1,0) &= \langle 10|A_0|10\rangle = a^2\,(1-\sin 2\alpha)\sin^2\gamma, && (5.101)\\
p\,(0,1,1) &= \langle 10|A_1|10\rangle = b^2\,(1-\sin 2\alpha)\cos^2\gamma, && (5.102)\\
p\,(0,1,?) &= \langle 10|A_?|10\rangle = (a\sin\gamma + b\cos\gamma)^2\sin 2\alpha, && (5.103)\\
p\,(1,0,0) &= \langle 01|A_0|01\rangle = b^2\,(1-\sin 2\alpha)\cos^2\gamma, && (5.104)\\
p\,(1,0,1) &= \langle 01|A_1|01\rangle = a^2\,(1-\sin 2\alpha)\sin^2\gamma, && (5.105)\\
p\,(1,0,?) &= \langle 01|A_?|01\rangle = (a\sin\gamma + b\cos\gamma)^2\sin 2\alpha, && (5.106)\\
p\,(1,1,0) &= \langle 11|A_0|11\rangle = b^2\,(1-\sin 2\alpha)\sin^2\gamma, && (5.107)\\
p\,(1,1,1) &= \langle 11|A_1|11\rangle = a^2\,(1-\sin 2\alpha)\cos^2\gamma, && (5.108)\\
p\,(1,1,?) &= \langle 11|A_?|11\rangle = (b\sin\gamma + a\cos\gamma)^2\sin 2\alpha. && (5.109)
\end{aligned}$$

Conhecendo as probabilidades dos estados perturbados, podemos agora, obter as expressões das taxas de erro de todos os canais entre Alice e Bob. A taxa de erro de Bob antes de descartar os resultados inconclusivos, q, é

$$\begin{aligned}
q &= \sum_{\epsilon=0,1} p\,(0,\epsilon,1) = \sum_{\epsilon=0,1} p\,(1,\epsilon,0)\\
&= b^2\,(1-\sin 2\alpha)\,. && (5.110)
\end{aligned}$$

E taxa dos resultados inconclusivos de Bob, r, é dada por

$$\begin{aligned}
r &= \sum_{\epsilon=0,1} p\,(0,\epsilon,?) = \sum_{\epsilon=0,1} p\,(1,\epsilon,?)\\
&= \left(a^2+b^2+2ab\sin 2\gamma\right)\sin 2\alpha. && (5.111)
\end{aligned}$$

Logo, a taxa de erro no canal de Alice e Bob, Q, é obtida por

$$Q = \frac{q}{1-r} = \frac{b^2}{a^2+b^2}. \tag{5.112}$$

De forma similar, a taxa de erro no canal de Alice e Eva depois que os resultados inconclusivos foram descartados, é dada por,

$$Q_{AE} = \frac{q_{AE}}{1-r}, \tag{5.113}$$

em que

$$q_{AE} = \sum_{\beta=0,1} p\left(0,1,\beta\right) = \left(a^2 \sin^2\gamma + b^2\cos^2\gamma\right)\left(1-\sin 2\alpha\right), \tag{5.114}$$

é a taxa de erro do canal entre Alice e Eva. Logo,

$$Q_{AE} = \left(1 - \frac{b^2}{a^2+b^2}\right)\sin^2\gamma + \frac{b^2}{a^2+b^2}\cos^2\gamma = (1-Q)\sin^2\gamma + Q\cos^2\gamma. \tag{5.115}$$

Agora, a taxa de erro do canal entre Eva e Bob é

$$q_{BE} = \sum_{\alpha=0,1} p\left(\alpha,0,1\right) = \left(b^2+a^2\right)\left(1-\sin 2\gamma\right). \tag{5.116}$$

Portanto, a taxa de erro do canal entre Eva e Bob após os resultados inconclusivos tenham sido descartados é

$$Q_{BE} = \frac{q_{BE}}{1-r} = \sin^2\gamma. \tag{5.117}$$

Agora, podemos parametrizar as taxas de erro nos canais de Alice e Eva, Q_{AE}, e de Eva e Bob, Q_{BE}, em termos da taxa de erro Q e do ângulo θ entre os dois estados de polarização dos fótons não-ortogonais, da seguinte forma

$$Q_{AE}\left(Q,\theta\right) = \frac{1}{2} - \left(\frac{1}{2} - Q\right)\left[1 - F\left(Q,\theta\right)^2\right]^{1/2}, \tag{5.118}$$

e

$$Q_{BE}\left(Q,\theta\right) = \frac{1}{2} - \frac{1}{2}\left[1 - F\left(Q,\theta\right)^2\right]^{1/2}, \tag{5.119}$$

em que

$$F\left(Q,\theta\right) = \frac{2\left[Q\left(1-Q\right)\right]^{1/2}\sec\theta - 1}{2\left[Q\left(1-Q\right)\right]^{1/2}\cos\theta - 1}. \tag{5.120}$$

Sem os resultados inconclusivos, o canal entre Alice e Bob opera como um canal binário, portanto, a informação mútua é

$$I_{AB} = 1 + Q \log Q + (1 - Q) \log (1 - Q). \tag{5.121}$$

Desde que os canais entre Alice e Eva, e Eva e Bob também sejam simetricamente binários, a suas respestivas informação mútua são

$$I_{AE} = 1 + Q_{AE} \log Q_{AE} + (1 - Q_{AE}) \log (1 - Q_{AE}), \tag{5.122}$$

e

$$I_{BE} = 1 + Q_{BE} \log Q_{BE} + (1 - Q_{BE}) \log (1 - Q_{BE}), \tag{5.123}$$

em que Q_{AE} e Q_{BE} são dados por Eqs (5.120) e (5.121), respectivamente. Assim, a informação mútua em cada canal é também expressa em termos do ângulo entre os estados não-ortogonais e a taxa de erro do canal entre Alice e Bob, com nenhuma dependência explícita aos parâmetros desconhecidos de Eva. A Fig(5.3), mostra que existe uma escolha ótima que possibilita maximizar a informação mútua, que Eva pode adquirir com relação a informação compartilhada entre Alice e Bob (I_{AB}) (linha superior à esquerda). Assim o valor máximo, para a informação mútua no canal Eva-Bob é obtido para uma escolha adequada da base sonda, conhecida como base de Breit, correspondendo a $\alpha = \pi/8$ ou equivalentemente $\theta = \pi/4$. Também apresentamos um gráfico comparando a Informação compartilhada entre Eva e Alice Fig(5.4). No ataque estudado aqui, a melhor estratégia de Eva é adquirir informação minimizando o dano provocado nos portadores de informação. Diferentemente do ataque opaco, que utiliza uma medição projetiva, na estratégia translucente o POVM é utilizado. Nesse caso uma transformação unitária é realizada fazendo os portadores de informação interagir com a sonda de Eva. Eva pode decidir só utilizar a sonda após Alice e Bob completarem seu protocolo (amplificação de privacidade). Esse parece ser a melhor estratégia de Eva.

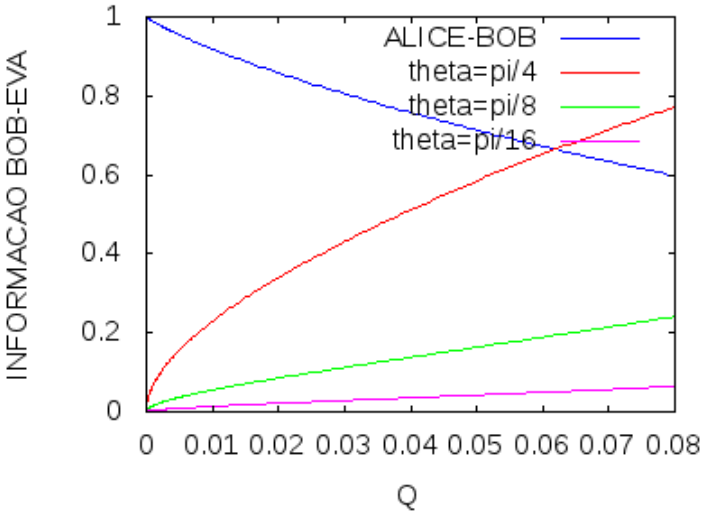

Figura 5.3: A figura mostra a informação mútua entre Eva e Bob, para diversos valores de θ.

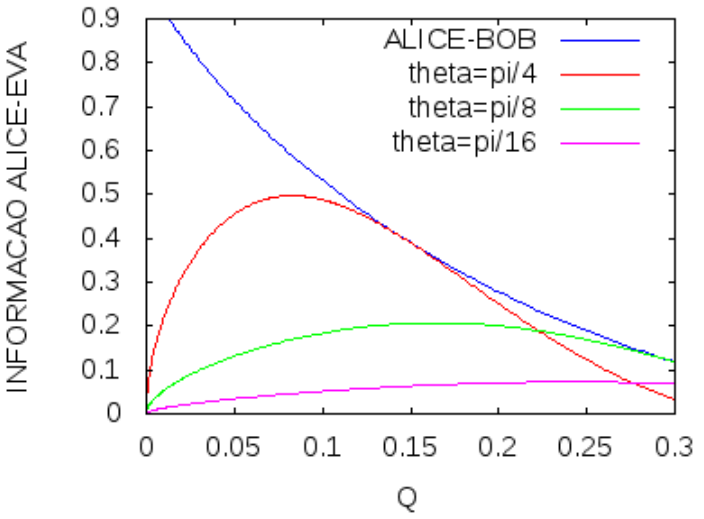

Figura 5.4: A figura mostra a informação mútua entre Alice e Eva, para diversos valores de θ.

Capítulo 6

Conclusão e perspectiva

Neste trabalho analisamos dois protocolos básicos para troca de chaves, que foram os primeiros protocolos propostos pela criptografia quântica, o BB84 e B92. Após apresentá-los, verificamos sua segurança sob um ataque individual que consiste em atacar cada um fóton por vez. Com o auxílio do circuito apresentado na Fig.(5.1), que implementa a medição através de um POVM ótico, analisamos um ataque conhecido como translúcido com emaranhamento. Apresentamos, seguindo a literatura, as expressões algébricas para as taxas de erro e para as informações mútua em termos da taxa de erro no canal entre Alice e Bob e o ângulo formado entre os dois estados de polarização não-ortogonais. Realçamos na última secção que, ao escrevermos a informação mútua explicitamente em termos da taxa de erro, verificamos que as informações sobre os estados não dependem dos parâmetros da sonda de Eva, o que a impede de manipulá-los para obter mais informação sobre os estados de polarização. Como perspectiva para complementar essa investigação, seria desenvolver em detalhe um estudo para explicitar o tipo de interação unitária (o Hamiltoniano) que possibilitaria a evolução unitária dos estados sonda -$\mathbf{e_u}(\mathbf{e_v})$- acoplados com os portadores de informação escolhidos por Alice- $\mathbf{u}(\mathbf{v})$.

Referências Bibliográficas

[1] C. H. Bennett and G. Brassard Proc.Quantum cryptography: public key distribution and coin tossing. IEEE Conf. on Computers, Systems and Signal Processing, Bangalore India, p. 175, 1984.

[2] C. H. Bennett. Quantum cryptography using any two nonorthogonal states. Physical Review Letters, 68, p.3121, 1992.

[3] E. Desurvire. Classical and Quantum Information Theory. Cambridge University Press, 2009.

[4] M. A. Nielsen e I. L. Chuang. Quantum Computation and Quantum Information. Cambridge University Press, Cambridge, 2000.

[5] J.A. Bergou, U. Herzog and M. Hillery. Discrimination of quantum states. Lect. Notes Phys., 649, p.417, 2004.

[6] M. Fayngold and V. Fayngold. Quantum Mechanics and Quantum Information. Addison-Wesley Publishing Company, revised edition edition, 2013.

[7] V. Scarani, S. Iblisdir, N. Gisin and A. Acín. Quantum cloning. Reviews of Modern Physucs, 77, p.1225, 2005.

[8] S. Lin, Q. Wen, F. Gao, and F. Zhu. Eavesdropping on secure deterministic communication with qubits through photon-number-splitting attacks. Physical Review A, 79, p.054303, 2009.

[9] V. Makarov. Quantum cryptography and quantum cryptanalysis. NTNU Norwegian University of Science and Technology, Trondheim, 2007.

[10] G. Rigolin and A. A. Rieznik. Introdução à criptografia quântica. Rev. Bras. Ensino Fis. 27, p.517, 2005.

[11] G. Brassard and L. Salvail. Secret-Key Reconciliation by Public Discussion. Eurocrypt, 93, p. 410, 1994.

[12] C. H. Bennett, G. Brassard and J. Rober. Privacy amplification by public discussion. SIAM J. Comput., 17, p. 210, 1988.

[13] M. Zou and G. Zhang. Information investigation for B92 protocol in quantum cryptography. Quantum Optics and Applications in Computing and Communications II, 5631, p.181, 2005.

[14] A. K. Ekert, B. Huttner, G. M. Palma and A. Peres. Eavesdropping on quantum-cryptographical systems. Physical Review A, 50, p.1047, 1994.

[15] B. A. Slutsky, R. Rao, P. Sun, and Y. Fainman. Security of quantum cryptography against individual attacks. Physical Review A, 57, p.2383, 1998.

[16] H. E. Brandt, J. M. Myers and S. J. Lomonaco Jr. Aspects of entangled translucent eavesdropping in quantum cryptography. Physical Review A, 56, p.4456, 1997.

[17] J.A. Bergou and M. Hillery. Introductio to the theory of quantum information processing. Ed. Springer, 2013.

[18] N. Lütkenhaus, M. Dusek and M. Hendrych. Quantum cryptography. Physical Review, 115, p.485, 1959.

[19] A. Furusawa and P. Loock. Quantum teleportation and entanglement. Addison-Wesley Publishing Company, revised edition edition, 2011.

[20] D. Bruβ and G. Leuchs. Lectures on quantum information. Progress in Optics, 49, p.381, 2006. e-print archive: quant-ph/0601207v3.

[21] J. A. Jones and D. Jaksch. Quantum information, computation and communication. Cambridge University Press, Cambridge 2012.

[22] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer. Generalized privacy amplification. IEEE Transactions on information theory, 41, 1995.

[23] J. Maziero. Understanding von Neumann's entropy. Rev. Bras. Ensino Fis., 37, p.1314, 2015. e-print archive: quant-ph/1502.04489v2.

[24] A. M. Abbas, A. Goneid and S. El-Kassas. Privacy amplification in quantum cryptography BB84 using combined univarsal-truly random hashing. International Journal of Information (IJINS), 3, p.98, 2014.

[25] Y. Watanabe. Privacy amplification for quantum key distribution. J. Phys. A: Math. Theor., 40, p.99, 2007.

[26] B. Huttner, N, Imoto, N. Gisin and T. Mor. Qauntum cryptography with coherent states. Physical Review A, 51, p.1863, 1995.

[27] C. A. Fuchs and A. Peres. Quantum-state disturbance versus information gain: Uncertainty relations for quantum information. Physical Review A, 53, p.2038, 1995.

[28] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden. Quantum cryptography. Reviews of Modern Physucs, 74, p.145, 2002.

[29] V. Scarani, H. B. Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus and M. Peev. The security of practical quantum key distribution. Reviews of Modern Physucs, 81, p.1301, 2009.