4 Codificação por freqüência

Recentemente [24], foi proposto um novo método para transmissão de *qubits*. Ele utiliza bandas laterais originadas no sinal óptico em Alice, geradas através de um modulador alimentado por um sinal de RF utilizando baixa profundidade de modulação. Esse sinal é propagado até Bob e lá é modulado novamente pela mesma freqüência de RF. Alice e Bob possuem cada um, um modulador de fase conectados aos seus respectivos sinais de RF. Dependendo da diferença de fase imposta entre eles, interferência construtiva ou destrutiva ocorrerá nas bandas laterais, o que permite que esse sistema seja utilizado para QKD.

4.1 Princípio de operação

Alice possui uma fonte laser CW de freqüência ω_0 gerando pulsos coerentes fracos (WCP), um gerador de RF gerando um tom senoidal de freqüência Ω, um modulador óptico (amplitude ou fase) e um modulador de fase de RF (Radio-Freqüência). Bob também possui os moduladores de RF e óptico e um gerador de RF operando com a mesma freqüência Ω e com sincronismo de fase em relação ao gerador de Alice. Além disso, Bob possui dois SPADs com filtros ópticos para separar as bandas laterais e um fotodetector clássico para detectar o pico central que opera como o pulso intenso de referência para utilização do protocolo B92.

O bloco A que alimenta o modulador de RF de fase φ_1 gera uma seqüência aleatória de bits (levando-se em conta a escolha de bases no caso BB84) para a transmissão.O bloco B gera outra seqüência aleatória em Bob que alimenta o modulador φ_2 que irá realizar a escolha de bases de Bob (Figura 17).

Na saída do modulador de Alice teremos a portadora óptica centrada em ω_0 mais duas bandas laterais centradas em $\omega_0 \pm \Omega$ com fase φ_1. Esse sinal se propaga pela fibra óptica até Bob aonde é novamente modulado. Duas bandas laterais são então geradas em $\omega_0 \pm \Omega$ com fase φ_2. As bandas laterais que forem geradas em Bob a partir das bandas laterais geradas em Alice ($\omega_0 \pm 2\Omega$), ou seja os segundos harmônicos, são muito menores em intensidade, supondo uma profundidade de

modulação pequena, e não serão considerados adiante. As bandas $\omega_0 \pm \Omega$ geradas em Bob serão sobrepostas as bandas que foram geradas pela Alice. Dependendo da diferença de fase $\varphi_2 - \varphi_1$ ocorrerá interferência construtiva ou destrutiva das bandas laterais. Para que isso possa ocorrer é crucial que os geradores de RF de Alice e Bob estejam operando exatamente na mesma freqüência Ω e além disso, que os dois geradores estejam sempre em fase. Para isso é requerido a existência de um enlace de sincronismo entre os geradores de RF. Esse requerimento torna-se não trivial fora do laboratório, entretanto uma solução WDM foi proposta [25] para sobrepor essa dificuldade. A idéia foi utilizar um outro comprimento de onda na mesma fibra para a transmissão de um sinal de referência que será utilizado por Bob para sincronizar o seu gerador de RF com o de Alice. Essa solução ainda tem a vantagem de compensar efeitos de dispersão cromática que possam vir a prejudicar o sincronismo do sistema como um todo.

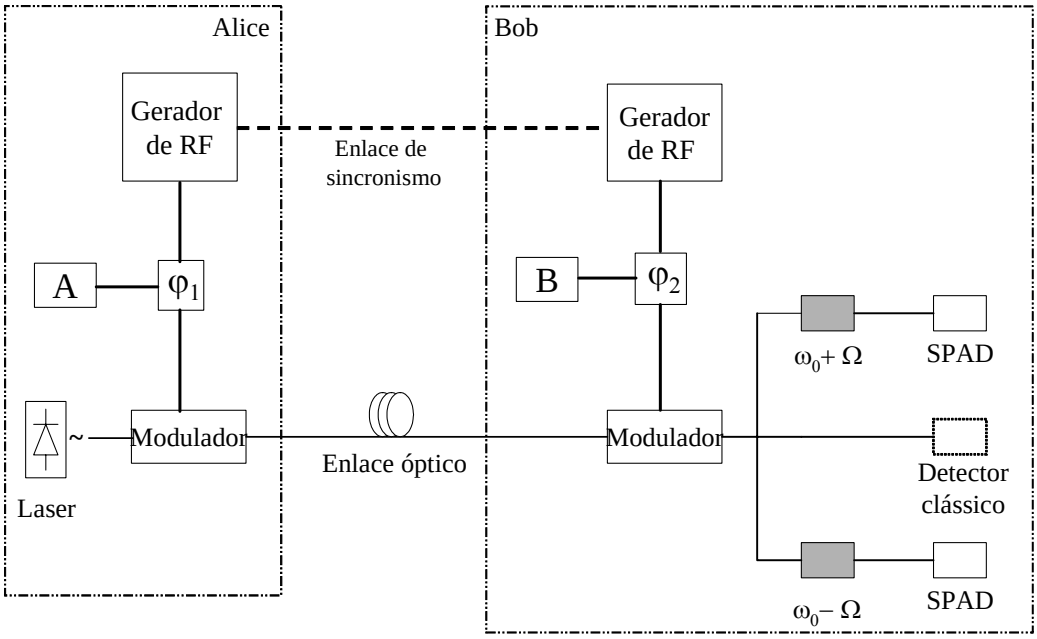


Figura 17: Esquema de transmissão de *qubits* utilizando codificação de freqüência. O enlace de sincronismo é fundamental para o funcionamento do sistema.

Como os moduladores podem ser de amplitude ou fase temos três opções para um sistema de codificação de fase: sistema PM-PM (modulação de fase em

ambos Alice e Bob), sistema AM-AM (modulação de amplitude em ambos Alice e Bob) e AM-PM (modulação de amplitude em Alice e de fase em Bob ou vice-versa). Será demonstrado que o sistema AM-AM pode se comportar exatamente como o sistema PM-PM, contrário ao que foi demonstrado em trabalhos anteriores [25] [26], ou seja que ele pode acomodar o protocolo B92. Será proposto então como solução para a utilização do BB84 um novo sistema (AM-PM).

4.2 Sistema PM-PM

Será feito inicialmente o desenvolvimento do sistema PM-PM cuja análise será feita utilizando teoria clássica de propagação. O efeito no regime quântico é o mesmo se lembrarmos que a probabilidade de se encontrar um fóton em determinada condição é diretamente proporcional à intensidade clássica correspondente.

O campo elétrico na saída do laser pode ser escrito como:

$$E_0(t) = E_0 e^{j\omega_0 t} \tag{4.1}$$

onde E_0 é a amplitude do campo e ω_0 a freqüência óptica. Desse ponto em diante será suprimida a notação *(t)* para simplificar a visualização das equações. Ao passar pelo modulador de fase de Alice o campo E_A na saída deste é:

$$E_A = E_0 e^{j\omega_0 t} \cdot e^{j[m\cos(\Omega t + \varphi_1)]} \tag{4.2}$$

onde Ω é a freqüência de modulação do sinal de RF e φ_1 o valor de fase inferido por Alice no sinal de RF e m é a profundidade de modulação. Supondo que a profundidade de modulação é muito menor do que a unidade, a seguinte aproximação é válida:

$$e^{j(m\cos(\Omega t + \varphi_1))} \approx 1 + j(m\cos(\Omega t + \varphi_1)) \tag{4.3}$$

Essa aproximação foi feita baseando-se no fato de que $e^{j\theta} \approx 1 + j\theta$ para θ muito pequeno. Escrevendo agora (4.3) em termos de exponenciais obtemos:

$$E_A = E_0 e^{j\omega_0 t} \cdot \left\{ 1 + j\frac{m}{2}\left[e^{j(\Omega t + \varphi_1)} + e^{-j(\Omega t + \varphi_1)} \right] \right\} \tag{4.4}$$

Após um enlace de comprimento L obtemos o campo E_F na entrada do modulador de Bob:

$$E_F = E_0 \left\{ e^{j(\beta_0 L + \omega_0 t)} + j\frac{m}{2}\left[e^{j(\beta_+ L + (\omega_0 + \Omega)t + \varphi_1)} + e^{-j(-\beta_- L + (-\omega_0 + \Omega)t + \varphi_1)} \right] \right\} \tag{4.5}$$

aonde β_0, β_+ e β_- são as constantes de propagação para o pico central e bandas laterais superior e inferior, respectivamente. Desprezando a dispersão cromática, $\beta_\pm$ são dadas por:

$$\beta_\pm = \frac{n}{c}(\omega_0 \pm \Omega). \tag{4.6}$$

Após o modulador de fase de Bob o campo E_B será:

$$E_B = E_F \cdot e^{j[m\cos(\Omega t + \varphi_2)]}. \tag{4.7}$$

É utilizada a mesma (pequena) profundidade de modulação m que a utilizada por Alice. No entanto dessa vez é aplicado ao sinal de RF o desvio de fase φ_2 independentemente do valor utilizado por Alice. Utilizando a mesma aproximação para m pequeno se comparado à unidade:

$$E_B = E_F \cdot \left\{ 1 + j\frac{m}{2}\left[e^{j(\Omega t + \varphi_2)} + e^{-j(\Omega t + \varphi_2)} \right] \right\} \tag{4.8}$$

Realizando a multiplicação e desprezando os termos $e^{j\beta_0 L}$ pois como multiplicam todo o campo eles não contribuem para a informação de fase:

$$E_B = E_0 e^{j\omega_0 t} + E_0 j\frac{m}{2}\left\{ e^{j\left[\frac{n}{c}\Omega L + (\omega_0+\Omega)t+\varphi_1\right]} + e^{-j\left[\frac{n}{c}\Omega L + (-\omega_0+\Omega)t+\varphi_1\right]} \right\} +$$

$$+ E_0 j\frac{m}{2}\left\{ e^{j[(\omega_0+\Omega)t+\varphi_2]} + e^{-j[(-\omega_0+\Omega)t+\varphi_2]} \right\} - \frac{m^2}{4}(O^2)\ldots . \qquad (4.9)$$

Os termos cruzados na multiplicação que geram os termos de ordem superior e que são multiplicados por m^2 são desprezados, pois são muito pequenos (lembrando que m é muito menor do que um). Finalmente os termos $(n/c)\Omega L$ são então relativos a propagação da luz na fibra.

A equação (4.9) representa o campo após o modulador de Bob. Esse campo será agora filtrado antes de chegar aos SPADs. Supondo filtros ideais centrados em $\omega_0 \pm \Omega$ obtemos os campos E_{B+} e E_{B-} correspondentes aos dois filtros:

$$E_{B+} = E_0 j\frac{m}{2}\left\{ e^{j\left[\frac{n}{c}\Omega L + (\omega_0+\Omega)t+\varphi_1\right]} + e^{j[(\omega_0+\Omega)t+\varphi_2]} \right\}. \qquad (4.10)$$

$$E_{B-} = E_0 j\frac{m}{2}\left\{ e^{-j\left[\frac{n}{c}\Omega L + (-\omega_0+\Omega)t+\varphi_1\right]} + e^{-j[(-\omega_0+\Omega)t+\varphi_2]} \right\}. \qquad (4.11)$$

Nosso interesse agora é calcular a intensidade desses dois campos para sabermos qual será a probabilidade de encontrar o fóton nas duas bandas laterais. A intensidade é dada por:

$$I_{\pm} = E_{B\pm} E_{B\pm}^{*} \qquad (4.12)$$

onde * representa o complexo conjugado do campo. Para a banda lateral superior (campo E_{B+}) teremos:

$$I_+ = E_0{}^2\, j\frac{m}{2}\left\{ e^{j\left[\frac{n}{c}\Omega L+(\omega_0+\Omega)t+\varphi_1\right]} + e^{j[(\omega_0+\Omega)t+\varphi_2]} \right\}.$$

$$\cdot\left\{ -j\frac{m}{2}\left\{ e^{-j\left[\frac{n}{c}\Omega L+(\omega_0+\Omega)t+\varphi_1\right]} + e^{-j[(\omega_0+\Omega)t+\varphi_2]} \right\}\right\} \qquad (4.13)$$

$$I_+ = \frac{E_0{}^2 m^2}{4}\left[2 + e^{j\left(\frac{n}{c}\Omega L+\varphi_1-\varphi_2\right)} + e^{-j\left(\frac{n}{c}\Omega L+\varphi_1-\varphi_2\right)} \right] \qquad (4.14)$$

$$I_+ = \frac{E_0{}^2 m^2}{2}\left[1+\cos\left(\frac{n}{c}\Omega L+\varphi_1-\varphi_2\right)\right] \qquad (4.15)$$

A equação (4.15) é a que representa a intensidade na banda lateral superior. Realizando o mesmo procedimento para a banda inferior:

$$I_- = E_0{}^2\, j\frac{m}{2}\left\{ e^{-j\left[\frac{n}{c}\Omega L+(-\omega_0+\Omega)t+\varphi_1\right]} + e^{-j[(-\omega_0+\Omega)t+\varphi_2]} \right\}.$$

$$\cdot\left\{ -j\frac{m}{2}\left\{ e^{j\left[\frac{n}{c}\Omega L+(-\omega_0+\Omega)t+\varphi_1\right]} + e^{j[(-\omega_0+\Omega)t+\varphi_2]} \right\}\right\} \qquad (4.16)$$

Seguindo os mesmos passos que no caso anterior obtemos a seguinte expressão para a intensidade da banda lateral inferior:

$$I_- = \frac{E_0{}^2 m^2}{2}\left[1+\cos\left(\frac{n}{c}\Omega L+\varphi_1-\varphi_2\right)\right] \qquad (4.17)$$

Podemos ver que as duas bandas laterais comportam-se da mesma maneira, visto que possuem exatamente a mesma expressão para as suas intensidades. Logo podemos concluir que a probabilidade do fóton ser encontrado será igual para as duas bandas. Observando (4.15) e (4.17) vemos que se a freqüência Ω do gerador

de RF for mantida fixa as intensidades das bandas dependem inteiramente da diferença de fases $\varphi_1 - \varphi_2$ imposta independentemente por Alice e Bob. Podemos observar que as bandas evoluem juntas com o cosseno ao quadrado da diferença de fase. Na figura 18, de caráter ilustrativo, é demonstrada uma simulação simples executada no software *MATLAB*. Foi calculado e disposto em um gráfico o espectro do sinal correspondente ao campo E_B para quatro valores de $\varphi_1 - \varphi_2$: 0, $\pi/2$, π e $3\pi/2$. Para a simulação foi considerado que o termo da propagação seja igual a zero apenas para simplificar a interpretação dos resultados. Na prática, dependendo da distância e da freqüência Ω iremos nos encontrar em algum ponto qualquer das equações (4.15) ou (4.17) e a diferença de fase continuará a determinar a intensidade das bandas laterais, fazendo com que apenas perca-se a referência inicial. A intensidade está disposta em escala linear. O espectro foi calculado para um sinal de baixa freqüência apenas com o propósito de conseguir executar a simulação em um tempo mais curto. No entanto a idéia é válida da mesma forma pois estamos operando no regime clássico, seja para uma portadora óptica ou um sinal de baixa freqüência. A portadora gerada (ω_0) é de 5 kHz com a freqüência de RF Ω de 500 Hz.

A partir do gráfico e pelas equações podemos observar que a intensidade das bandas laterais é máxima quando $\Delta\varphi = 0$ e mínima quando $\Delta\varphi = \pi$, com intensidades intermediárias em $\Delta\varphi = \pi/2$ e $\Delta\varphi = 3\pi/2$. Para o caso real em que o termo de propagação não é igual a zero teremos apenas valores diferentes de intensidade para essas diferenças de fase com o conjunto todo obedecendo sempre as equações (4.15) e (4.17).

No regime quântico teremos o seguinte: probabilidade máxima de encontrar o fóton em *uma* das bandas laterais (supondo pulsos contendo apenas um fóton) quando $\Delta\varphi = 0$, probabilidade intermediária para os casos em que $\Delta\varphi = \pi/2$ ou $\Delta\varphi = 3\pi/2$ e probabilidade mínima para $\Delta\varphi = \pi$. No caso ideal teremos probabilidade 1, 1/2 e 0 respectivamente. Como esse sistema pode ser utilizado para QKD? Se considerarmos o caso em que temos probabilidade 1 e 0 de detectar o fóton (o que irá depender da escolha das fases geradas por Alice e Bob) temos o caso de bases compatíveis. Para o caso de probabilidade ½, corresponde à situação de escolha de bases diferentes que devem ser descartados.

No entanto, para sistemas reais a situação não é tão simples assim. Devido a perdas no sistema e SPADs imperfeitos não podemos considerar o caso em que esperamos que o detector não dispare ($\Delta\varphi = \pi$). A tabela 3 indica todas as possibilidades para o sistema PM-PM.

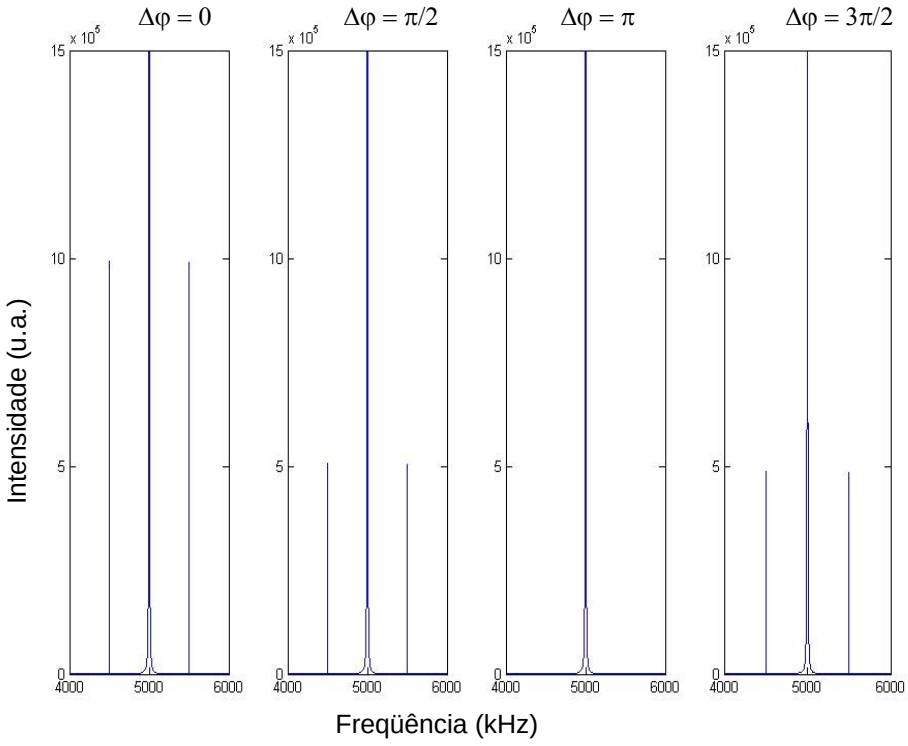


Figura 18: Espectro de freqüências gerado através de simulação no *MATLAB* para quatro valores de $\Delta\varphi$. O termo de propagação foi assumido como zero.

Pela tabela 3 podemos notar que é possível a aplicação do protocolo B92 pelo sistema PM-PM utilizando as possibilidades ou da parte esquerda da tabela ou da direita. Identificando as linhas na cor cinza na tabela (cujas diferenças de fase são sempre de 0 ou π) vemos que em todos os instantes em que Alice e Bob escolhem o mesmo estado, eles obtém 1 nos SPADs (no caso de somente um fóton no pulso ele tem 50% de probabilidade de escolher qualquer uma das bandas), e no caso que eles escolham valores tais que a diferença destes seja π eles não detectarão nenhum fóton no detector (a menos da contagem de escuro).

Como no sistema original utilizando B92 [12], Bob recordará todos os instantes em que seu SPAD disparou. Ele então avisará Alice quando isso ocorreu,

PM-PM									
Bit	Alice	Bob	$\omega 0 + \Omega$	$\omega 0 - \Omega$	Bit	Alice	Bob	$\omega 0 + \Omega$	$\omega 0 - \Omega$
0	0	0	1	1	0	$\pi/2$	0	?	?
	0	$\pi/2$	?	?		$\pi/2$	$\pi/2$	1	1
	0	π	**	**		$\pi/2$	π	?	?
	0	$3\pi/2$	?	?		$\pi/2$	$3\pi/2$	**	**
1	π	0	**	**	1	$3\pi/2$	0	?	?
	π	$\pi/2$	?	?		$3\pi/2$	$\pi/2$	**	**
	π	π	1	1		$3\pi/2$	π	?	?
	π	$3\pi/2$	?	?		$3\pi/2$	$3\pi/2$	1	1

Tabela 3: Gama de possibilidades para o sistema PM-PM fazendo o termo de propagação igual a zero. “1” representa probabilidade máxima de o fóton estar nas bandas laterais, “?” indica dúvida, ou seja, probabilidade de 50%, e “**” indica probabilidade mínima. As linhas na cor cinza indicam a utilização do B92.

e os dois automaticamente sabem qual valor o outro inferiu. Em todos os outros casos os valores serão descartados. Obviamente que erros serão introduzidos pela contagem de escuro dos detectores e por eventuais erros de transmissão. Eles serão corrigidos durante o processo de correção de erros dentro da reconciliação. Como já foi mencionado, para que a informação que um eventual espião possa ter adquirido seja reduzida a zero, é necessário que a *QBER* do sistema não seja maior do que 15% (assumindo ataques individuais).

É importante lembrarmos que o B92 como está apresentado aqui é potencialmente inseguro. Eva pode interceptar todos os fótons e bloquear todos aqueles em que ela obtiver uma medida inconclusiva. Para os instantes em que ela conseguir uma contagem válida, basta que ela envie a Bob o mesmo fóton que ela mediu, pois nestes instantes ela tem certeza de que mediu o fóton corretamente. Esse sistema já está apto a incorporar o esquema do pulso intenso de referência. Não foi mencionado ainda mas a profundidade de modulação *m* é utilizada de forma a termos μ fótons por pulso nas bandas laterais. Como *m* é tipicamente muito menor do que a unidade o pico central é clássico, podendo então ser utilizado como referência. Nessa situação Eva não pode bloquear o pulso de referência pois Bob irá descartar todos os instantes de tempo em que não haja a presença deste pulso. Caso Eva opte por interceptar os fótons mesmo assim, a taxa de erro do sistema aumentará, pois ao acionar o seu modulador, Bob poderá fazer com que um fóton do pico central vá para uma das bandas laterais gerando erros.

Finalmente existe uma alternativa para a proteção do B92 sem a utilização do pulso intenso de referência [6] [12]. Sem a presença de Eva existe uma proporção bem definida do número de “1s” recebidos. Caso Eva comece a interceptar fótons essa proporção é modificada e ela pode ser detectada. No entanto se as perdas no sistema forem elevadas essa proporção também é modificada acusando a existência de uma Eva que simplesmente não está ali. Por essa razão a utilização do pulso de referência como segurança para o protocolo B92 é mais interessante.

Não podemos aplicar a versão clássica do BB84 nesse caso, pois não podemos contar com a detecção da ausência de fótons. Caso as bandas se comportassem de forma complementar (isto é, uma estando no máximo enquanto a outra está no mínimo) poderíamos utilizar o BB84 (Alice escolhe 4 valores entre duas bases, tipicamente 0, $\pi/2$, π e $3\pi/2$, enquanto Bob utiliza dois valores para selecionar as bases, 0 e $\pi/2$). Esse é o caso do sistema AM-PM que será demonstrado na seção 4.4.

4.3 Sistema AM-AM

Os resultados anteriores são idênticos ao que foi obtido em [24] e [27]. O mesmo grupo posteriormente propôs um outro esquema utilizando dois moduladores MZ (*Mach-Zender*) de amplitude. Eles propuseram que o novo sistema pode operar com BB84 clássico, isto é, as bandas comportam-se de forma complementar. Nesta seção será mostrado que na verdade o sistema AM-AM utilizando moduladores MZ sem *chirp* comporta-se exatamente como o PM-PM e que somos obrigados a utilizar B92 ou uma versão modificada do BB84, caso optemos pelo AM-AM. Será comentado e demonstrado mais adiante que se utilizarmos moduladores que adicionem *chirp* ao sinal óptico o sistema pode suportar o BB84 clássico. Será utilizada a mesma notação matemática que aplicada no desenvolvimento do esquema PM-PM e em [25]-[26] para permitir que o leitor possa comparar os diferentes formatos de modulação

Será então suposto um modulador MZ em Alice. Ela possui o mesmo equipamento descrito na seção anterior (figura 17) com exceção do modulador que agora é de amplitude. A luz proveniente do laser é modulada com freqüência

Ω sendo que a informação a ser transmitida é sobreposta a esse sinal de RF utilizando desvios de fase φ_1. Além disto, o modulador é polarizado com uma tensão DC sobreposta ao sinal de RF que irá gerar um desvio de fase Ψ_1 em um dos braços do MZ. (Figura 19).

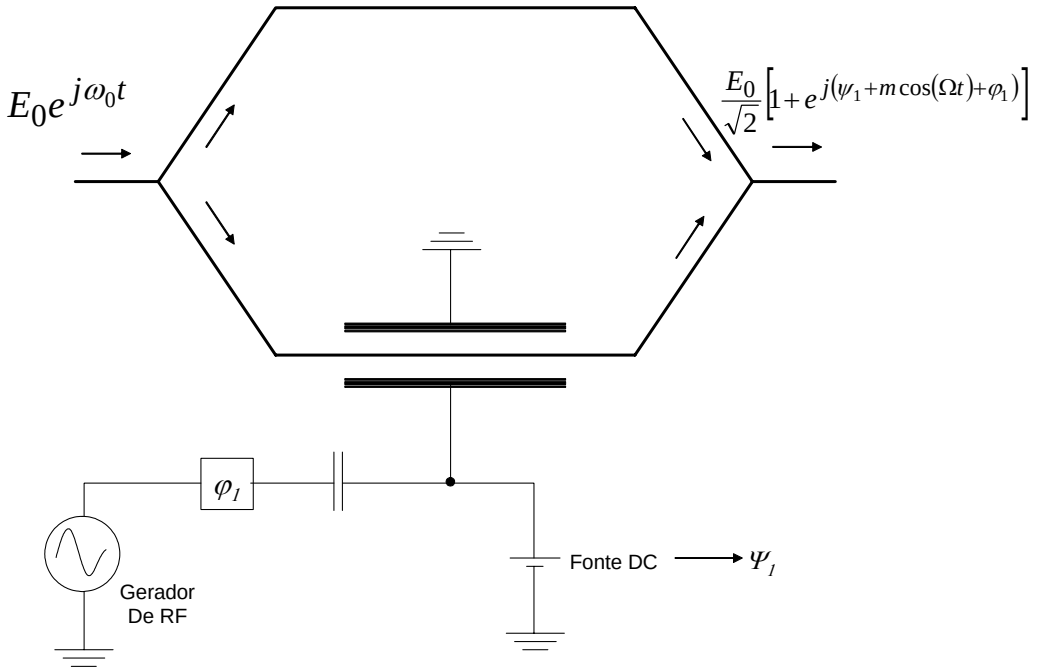


Figura 19: Diagrama de um modulador MZ com os sinais ópticos de entrada e saída. O MZ utiliza um gerador de RF conectado em série com o defasador de fase de RF para o sinal modulante. Este sinal é sobreposto a um nível de tensão DC que irá gerar o desvio de fase Ψ_1 em um dos braços do modulador.

Novamente o campo saindo do modulador de Alice é dado por (4.1). Após o modulador temos a seguinte expressão para o campo E_A:

$$E_A = \frac{E_0}{2}\left[1+e^{j(\psi_1+m\cos(\Omega t+\varphi_1))}\right].e^{j\omega_0 t} \qquad (4.18)$$

Foi novamente suprimida a notação *(t)* para tornar mais fácil a leitura. Ψ_1 é a representação para o desvio de fase induzido em um dos braços do modulador para uma tensão de polarização (*bias*) aplicada. Apesar de utilizar a mesma letra, a profundidade de modulação *m* não tem exatamente o mesmo significado em relação ao *m* do PM-PM. Enquanto aqui *m* é adimensional e está relacionado a amplitude da modulação, no sistema anterior *m* tem dimensão de radianos e está relacionado à fase. Será utilizada a mesma letra pois o conceito é o mesmo, inclusive o requisito de que *m* deve ser muito menor do que a unidade. Realizando a mesma aproximação que no sistema PM-PM para o caso em que *m* é muito menor do que um:

$$E_A = \frac{E_0}{2}\left[1 + e^{j\Psi_1}\left(1 + jm\cos(\Omega t + \varphi_1)\right)\right]\cdot e^{j\omega_0 t} =$$

$$= \frac{E_0}{2}\left\{1 + e^{j\Psi_1}\left[1 + j\frac{m}{2}\left(e^{j(\Omega t+\varphi_1)} + e^{-j(\Omega t+\varphi_1)}\right)\right]\right\}\cdot e^{j\omega_0 t} \qquad (4.19)$$

Será tomado um caminho diferente agora do que foi utilizado no sistema anterior. Iremos inicialmente calcular a intensidade do sinal na saída do modulador de Alice:

$$I_A = E_A E_A^{\,*} = \frac{E_0^{\,2}}{4}\left\{1 + e^{j\Psi_1}\left[1 + j\frac{m}{2}\left(e^{j(\Omega t+\varphi_1)} + e^{-j(\Omega t+\varphi_1)}\right)\right]\right\}\cdot$$

$$\cdot\left\{1 + e^{-j\Psi_1}\left[1 - j\frac{m}{2}\left(e^{j(\Omega t+\varphi_1)} + e^{-j(\Omega t+\varphi_1)}\right)\right]\right\} \qquad (4.20)$$

Fazendo a multiplicação, agrupando os termos, reescrevendo as exponenciais em termos de senos e cossenos, e desprezando os termos em m^2:

$$I_A = \frac{E_0^{\,2}}{2}\left[1 + \cos\Psi_1 - m\cdot sen\Psi_1\cos(\Omega t + \varphi_1)\right] \qquad (4.21)$$

A partir de (4.21) obtemos o que já era de se esperar para um modulador MZ. Dependendo do valor de Ψ_1 ($\pi/2$ ou $3\pi/2$) obtemos modulação máxima, isto é, as bandas laterais estão com máxima intensidade. Se Ψ_1 for 0 apenas a

portadora óptica não modulada deixará o modulador, enquanto que se $\Psi_1 = \pi$ nenhuma luz sairá do modulador.

O desenvolvimento acima é relevante para demonstrar que um modulador MZ comporta-se como um modulador de amplitude genérico (como não poderia deixar de ser). Este fato será utilizado para mostrar que a equação de saída do campo óptico para o MZ é idêntica a de um modulador de amplitude genérico, e que será conseqüentemente utilizada para o cálculo das intensidades das bandas laterais.

Como queremos modulação máxima, para maximizar a probabilidade de que um fóton seja efetivamente modulado (se projete para uma das bandas laterais), suporemos por exemplo $\Psi_1 = 3\pi/2$, dessa forma podemos deduzir que a partir de (4.21):

$$E_A = \frac{E_0}{\sqrt{2}}\sqrt{1+m\cdot\cos(\Omega t+\phi_1)}\cdot e^{j\omega_0 t} \tag{4.22}$$

Na realidade essa é a equação geral para qualquer modulador em amplitude, como queríamos mostrar. O resultado final para as intensidades utilizando $\Psi_1 = \pi/2$ será análogo. Novamente será utilizada a aproximação para *m* no qual:

$$\frac{E_0}{\sqrt{2}}\sqrt{1+m\cdot\cos(\Omega t+\phi_1)}\cdot e^{j\omega_0 t} \approx \frac{E_0}{\sqrt{2}}e^{j\omega_0 t}\left(1+\frac{m}{2}\cos(\Omega t+\phi_1)\right) \tag{4.23}$$

Reescrevendo (4.23) em termos de exponenciais:

$$E_A = \frac{E_0}{\sqrt{2}}e^{j\omega_0 t}\left\{1+\frac{m}{4}\left[e^{j(\Omega t+\varphi_1)}+e^{-j(\Omega t+\varphi_1)}\right]\right\} \tag{4.24}$$

Esse é o sinal na saída de Alice. Propagando-o através de uma fibra de comprimento *L* obtemos o sinal E_F na entrada do modulador de Bob:

$$E_F = \frac{E_0}{\sqrt{2}}\left\{e^{j(\beta_0 L+\omega_0 t)}+\right.$$

$$+\frac{m}{4}\left[e^{j(\beta_+ L+(\omega_0+\Omega)t+\varphi_1)}+e^{-j(-\beta_- L+(-\omega_0+\Omega)t+\varphi_1)}\right]\Bigg\} \tag{4.25}$$

Novamente estamos desprezando a dispersão cromática. O sinal na saída de Bob com ele empregando $\Psi_2 = 3\pi/2$ será:

$$E_B=\frac{E_F}{\sqrt{2}}\left\{1+\frac{m}{4}\left[e^{j(\Omega t+\varphi_2)}+e^{-j(\Omega t+\varphi_2)}\right]\right\} \tag{4.26}$$

Multiplicando e desprezando os termos $e^{j\beta_0 L}$ teremos que:

$$E_B=\frac{E_0}{2}\left\{e^{j\omega_0 t}+\frac{m}{4}\left\{e^{j\left[\frac{n}{c}\Omega L+(\omega_0+\Omega)t+\varphi_1\right]}+e^{-j\left[\frac{n}{c}\Omega L+(-\omega_0+\Omega)t+\varphi_1\right]}\right\}+\right.$$

$$\left.+\frac{m}{4}\left\{e^{j[(\omega_0+\Omega)t+\varphi_2]}+e^{-j[(-\omega_0+\Omega)t+\varphi_2]}\right\}+\frac{m^2}{16}(O^2)...\right\} \tag{4.27}$$

Novamente os termos de ordem superior são desprezados. (4.27) é o campo na entrada dos filtros levando aos SPADs. Seguindo o mesmo procedimento do caso PM-PM será calculada agora a intensidade para as duas bandas laterais.

$$I_+=\frac{{E_0}^2}{4}\left\{\frac{m}{4}\left[e^{j\left(\frac{n}{c}\Omega L+(\omega_0+\Omega)t+\varphi_1\right)}+e^{j((\omega_0+\Omega)t+\varphi_2)}\right]\right\}\cdot$$

$$\cdot\left\{\frac{m}{4}\left[e^{-j\left(\frac{n}{c}\Omega L+(\omega_0+\Omega)t+\varphi_1\right)}+e^{-j((\omega_0+\Omega)t+\varphi_2)}\right]\right\} \tag{4.28}$$

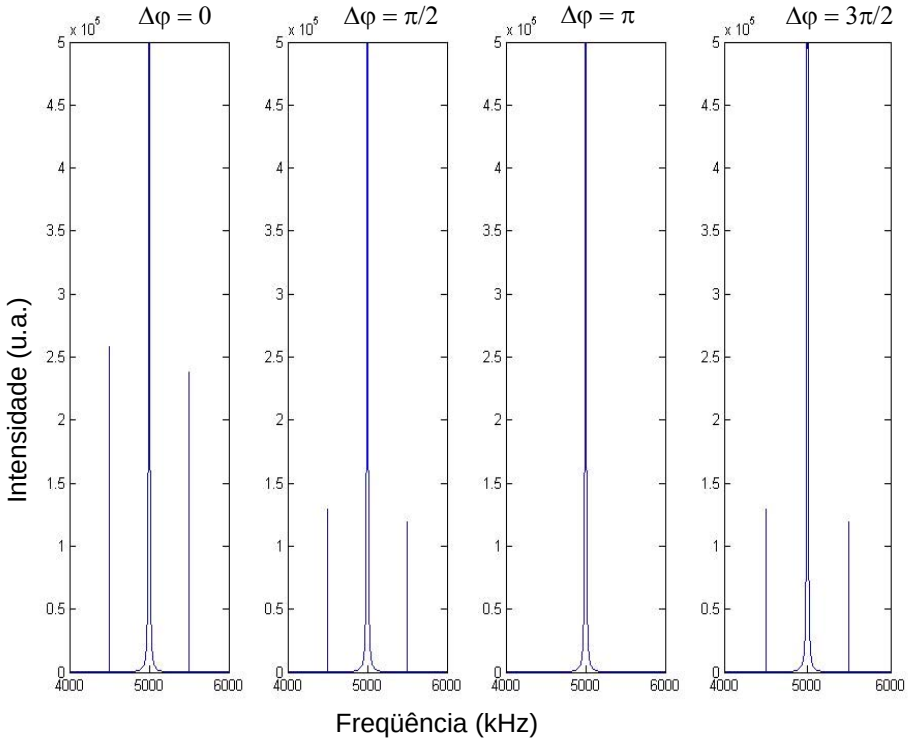
Multiplicando e reescrevendo as exponenciais como um cosseno:

$$I_+=\frac{{E_0}^2 m^2}{32}\left[1+\cos\left(\frac{n}{c}\Omega L+\phi_1-\phi_2\right)\right] \tag{4.29}$$

Refazendo o mesmo cálculo para a banda lateral inferior obtém-se:

$$I_{-} = \frac{{E_0}^2 m^2}{32}\left[1+\cos\left(\frac{n}{c}\Omega L+\phi_1-\phi_2\right)\right] \tag{4.30}$$

Vemos então que a menos de uma constante as duas equações acima são idênticas a (4.15) e (4.17), expressões para a intensidade das bandas laterais para o sistema AM-AM. Mesmo que utilizemos $\Psi_2 = \pi/2$ gerando $\Psi_1 - \Psi_2 = \pi$ como sugerido em [25], as intensidades continuarão idênticas a (4.29) e (4.30). Novamente foi realizada uma simulação no *MATLAB* sob as mesmas condições da realizada para o PM-PM (Figura 20). Apesar da pequena diferença observada, observamos que os espectros são essencialmente os mesmos, provando que os



dois sistemas comportam-se da mesma forma.

Figura 20: Espectros do sinal na saída do modulador de Bob.

Como as bandas laterais do sistema AM-AM comportam-se da mesma forma que no PM-PM, esse sistema deve operar nas mesmas condições, ou seja, trabalhando no protocolo B92.

Nos trabalhos [25] e [26] os autores propuseram que o sistema AM-AM pode na verdade operar com BB84, isto é, as bandas laterais comportam-se complementarmente. Como acabamos de demonstrar isso é impossível pelo menos com o uso de moduladores MZ sem *chirp* (*zero-chirp*).

Como foi proposto em [25] é possível utilizar o sistema AM-AM, bem como o PM-PM com uma versão modificada do BB84. Essa idéia foi proposta com o intuito de utilizar o sistema AM-AM com somente um SPAD centrado em uma das bandas laterais ao invés de dois. Note que mesmo em um sistema que opere com as bandas laterais evoluindo complementarmente, a utilização de somente um SPAD destrói essa propriedade e a habilidade de utilizar o BB84 clássico. Isso é o equivalente às duas bandas comportarem-se juntas como no PM-PM, com a desvantagem de cortarmos pela metade a probabilidade de detectar um fóton. Nessa versão Alice utilizaria os quatro valores usuais, no entanto, Bob utilizaria os mesmos quatro valores ao invés dos dois usuais. Dessa forma as duas bases seriam varridas e essa nova gama de possibilidades é ilustrada em toda a tabela 3. Esse protocolo apesar de funcionar com o mesmo princípio do BB84 clássico apresenta uma séria desvantagem, dado que a taxa de bits cai pela metade, pois agora só 25% das escolhas de bases estarão corretas contra 50% do BB84 clássico.

4.4 Sistema AM-PM

Finalmente, propomos um novo sistema, utilizando uma combinação de moduladores de fase e amplitude. Essa combinação irá fazer com que as intensidades das bandas laterais comportem-se complementarmente.

Será suposto que Alice possui um modulador de amplitude enquanto Bob ficará com o modulador de fase. No entanto o desempenho do sistema será idêntico se a combinação utilizada for ao contrário.

Como Alice utiliza um modulador de amplitude, aproveitaremos o equacionamento anterior. A diferença é que como as profundidades de modulação não são exatamente as mesmas para os dois moduladores escreveremos m_1 para o

modulador de Alice e m_2 para o de Bob. No entanto as mesmas aproximações serão feitas para m_1 e m_2. O campo na saída de Bob e antes dos filtros será:

$$E_B = E_0\left\{e^{j\omega_0 t} + \frac{m_1}{4}\left\{e^{j\left[\frac{n}{c}\Omega L+(\omega_0+\Omega)t+\varphi_1\right]} + e^{-j\left[\frac{n}{c}\Omega L+(-\omega_0+\Omega)t+\varphi_1\right]}\right\}+\right.$$

$$\left. + j\frac{m_2}{4}\left\{e^{j[(\omega_0+\Omega)t+\varphi_2]} + e^{-j[(-\omega_0+\Omega)t+\varphi_2]}\right\} + j\frac{m_1 m_2}{8}(O^2)...\right\}. \qquad (4.31)$$

O processo para o cálculo das intensidades das bandas laterais é exatamente o mesmo dos dois sistemas demonstrados acima. Com isso em mente obtemos:

$$I_+ = \frac{{E_0}^2}{8}\left[\frac{{m_1}^2}{4} + {m_2}^2 - m_1 m_2 \cdot \sin\left(-\frac{n}{c}\Omega L - \phi_1 + \phi_2\right)\right]. \qquad (4.32)$$

$$I_- = \frac{{E_0}^2}{8}\left[\frac{{m_1}^2}{4} + {m_2}^2 + m_1 m_2 \cdot \sin\left(-\frac{n}{c}\Omega L - \phi_1 + \phi_2\right)\right]. \qquad (4.33)$$

Nesse caso fica fácil de perceber que as bandas evoluem complementarmente, devido aos sinais trocados antes do termo senoidal. Podemos montar agora uma tabela com os resultados possíveis para esse sistema:

AM-PM				
Bit	Alice	Bob	$\omega 0 + \Omega$	$\omega 0 - \Omega$
0	0	0	1	**
	0	$\pi/2$	?	?
1	π	0	**	1
	π	$\pi/2$	?	?
Bit	Alice	Bob	$\omega 0 + \Omega$	$\omega 0 - \Omega$
0	$\pi/2$	0	?	?
	$\pi/2$	$\pi/2$	1	**
1	$3\pi/2$	0	?	?
	$3\pi/2$	$\pi/2$	**	1

Tabela 4: Resultados possíveis para o sistema AM-PM, novamente fazendo com que o termo de propagação seja igual a zero. As quatro linhas superiores correspondem à base "A" enquanto as inferiores à "B". A mesma notação da tabela anterior é utilizada.

O protocolo BB84 clássico pode ser prontamente aplicado. Alice pode escolher entre duas bases e Bob utiliza dois valores (0 e $\pi/2$) para a sua medida. Durante a reconciliação, Bob avisa Alice quais valores ele utilizou para suas medidas e Alice em resposta o avisa quais bits ele deve guardar. Note que em nenhum momento Bob revela publicamente qual SPAD disparou. Alice sabe essa informação a partir dos valores revelados publicamente por Bob e dos valores que ela utilizou em seu modulador de RF φ_1.

Refazendo a mesma simulação no *MATLAB* do espectro do campo na saída de Bob, obtemos para os mesmos quatro valores do desvio de fase $\Delta\varphi$ a figura 21:

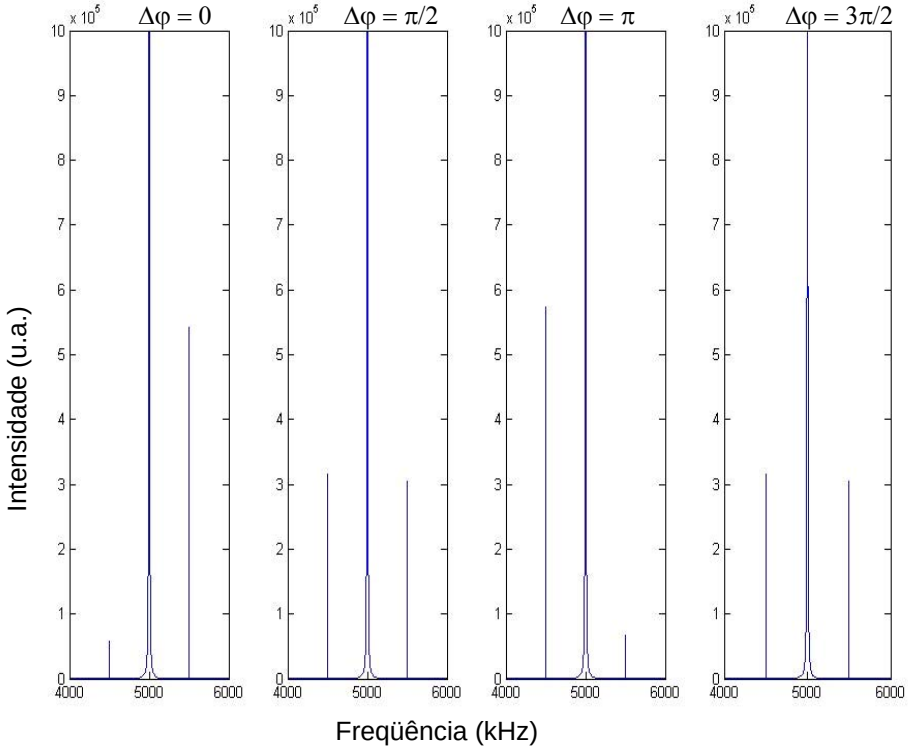


Figura 21: Espectro do sistema AM-PM para os mesmos quatro valores de $\Delta\varphi$.

Finalmente possuímos um sistema no qual podemos utilizar BB84 clássico devido ao comportamento complementar das bandas. Nos casos em que $\Delta\varphi = \pi/2$ ou $\Delta\varphi = 3\pi/2$ as intensidades encontram-se igualmente distribuídas entre as duas bandas, o fóton terá 50% de probabilidade de encontrar-se em qualquer uma delas. Logo esses valores serão descartados. Para os outros dois casos de $\Delta\varphi$ temos a certeza de qual *qubit* foi enviado pois nesse caso temos uma

situação mutuamente exclusiva em um sistema ideal: *ou* o fóton se encontrará em uma banda *ou* ele não chegou. Por um sistema ideal queremos dizer máxima visibilidade de interferência e detectores perfeitos, mas como sabemos que na prática isto é impossível, ocorrerão erros no sistema que serão corrigidos durante o processo de reconciliação.

4.5 Considerações finais sobre a codificação por freqüência

Esse método possui algumas vantagens sobre os outros dois apresentados. Ele também é insensível à polarização, como o método de codificação de fase, contanto que moduladores insensíveis à polarização sejam utilizados. Como o sistema na realidade é baseado em freqüências de RF (da ordem de GHz) ele é consideravelmente mais simples de ser estabilizado se comparado com a codificação de fase pois a estabilização dos "meios-interferômetros" não é muito trivial. Esse sistema é então uma alternativa ao problema da estabilização como o "*Plug and Play"* [3].

A principal desvantagem, e possível complicação, é a necessidade de um enlace de sincronismo de forma a garantir que os geradores de RF de Alice e Bob estejam operando na mesma freqüência Ω e em fase. Como as intensidades das bandas laterais dependem de desvios de fase (φ_1 e φ_2) aplicados sobre a portadora de RF Ω qualquer variação na fase dessa portadora corresponderá a um imprevisível desvio de fase gerado por Alice e Bob que causará erros (por exemplo, o fóton sendo desviado para a banda errada). Por esse motivo é crucial que os dois geradores de RF operem sempre em sincronismo, sob a penalidade de aumentar $QBER_{opt}$.

Como foi mencionado, para a operação do sistema não é estritamente necessária a utilização de dois SPADs. Podemos utilizar somente um posicionado em uma das bandas laterais. Pode ser visto que o protocolo B92 pode ser aplicado imediatamente da mesma maneira do que no caso com dois SPADs [24]. A desvantagem é que nossa probabilidade de detectar fótons cairá pela metade, visto que o fóton tem probabilidade 1/2 de encontrar-se em qualquer uma das bandas. É o preço a se pagar pela utilização de um sistema menos dispendioso. Também é possível a utilização da versão modificada do BB84 [25]. Note que a utilização de

somente um SPAD no sistema AM-PM corresponde à mesma situação dos sistemas AM-AM ou PM-PM , ou seja, as bandas laterais comportam-se juntas.