5.
Contagem de fótons a 4.65 μm para criptografia quântica via canal atmosférico

Ao longo da última década, a caracterização e implementação bem sucedidas de sistemas de criptografia quântica, tanto via fibras ópticas quanto via propagação atmosférica, levou ao amadurecimento do que hoje chamamos de "comunicações quânticas". Grandes progressos têm sido feitos a cada ano que passa em diversas áreas, tais como a máxima distância em que se pode estabelecer uma chave secreta, como os efeitos do ruído de detecção podem ser minimizados e como os protocolos podem sofrer melhorias para melhor lidarem com diversos tipos de ataque.

Existe um assunto, entretanto, que é raramente discutido e até mesmo ignorado: a escolha do comprimento de onda dos fótons. É verdade que essa questão não faz sentido para sistemas que utilizam fibras ópticas, já que a janela em torno do comprimento de onda de 1550 nm corresponde à menor atenuação possível e, como já discutimos, há diversas tecnologias de detecção disponíveis, tais como o APD InGaAs. Para canais quânticos atmosféricos, os comprimentos de onda mais utilizados se encontram no visível ou no infravermelho próximo, tais como 780, 800, 850 ou mesmo 1550 nm (devido à abundante oferta de transmissores e detectores, graças ao mercado de fibras ópticas) [44,45,46]. Entretanto, não há nenhuma evidência concreta que essas sejam as melhores escolhas possíveis!

Sabemos que, diferentemente de guias de onda confinados, a atmosfera pode servir de canal para uma vasta faixa de freqüências, que vão desde as ondas de rádio até a luz ultravioleta. A princípio, um sistema de comunicações ópticas de espaço livre poderia empregar qualquer comprimento de onda que não corresponda à freqüência de absorção de um dos vários gases que compõem a atmosfera. Essas janelas de transmissão são perfeitamente bem conhecidas, como mostra a figura 39.

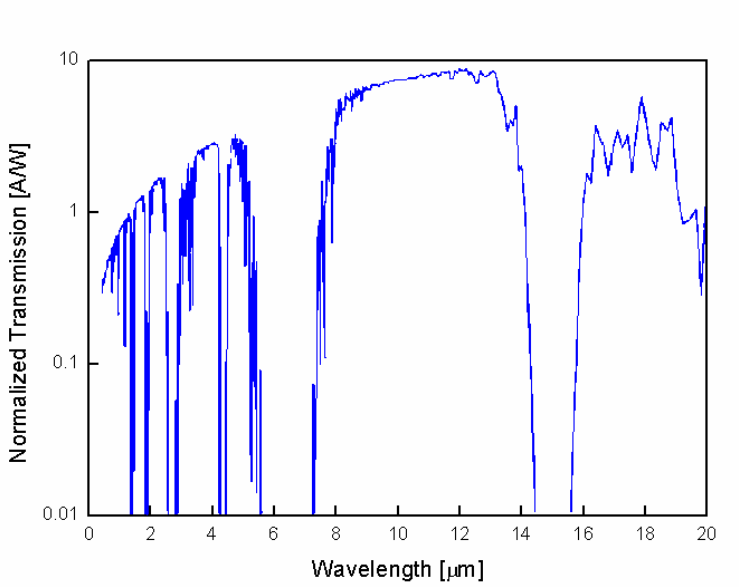

Figura 39. Curva típica de transmissão atmosférica sob condições climáticas limpas. A responsividade do detector é suposta constante. Figura obtida de [48].

Basta uma rápida olhada na figura 39 para constatar-se que o uso de um comprimento de onda no infravermelho mais distante poderia ser vantajoso; no caso de um sistema de criptografia quântica, menos perdas traduz-se como maior taxa de geração de chaves e maior distância máxima. De fato, algumas verificações experimentais recentes confirmaram que comprimentos de onda mais longos, nas faixas que chamamos de *infravermelho médio* (~3-13μm) e *infravermelho distante* (13-50μm), são menos suscetíveis à atenuação atmosférica e turbulência se comparadas às faixas no visível e infravermelho próximo, principalmente na presença de névoa ou neblina [47,48,49].

Além disso, devido aos recentes avanços na tecnologia de lasers de cascada quântica (QCL, *Quantum Cascade Laser*) [50], é possível gerar pulsos atenuados em praticamente qualquer comprimento de onda entre 3.5 e 67μm. Portanto, tanto o transmissor quanto o canal do sistema de comunicações quânticas poderiam perfeitamente ser adaptados para o uso de um maior comprimento de onda. Resta a pergunta: por que não explorar o infravermelho médio ou distante?

A resposta está na ausência de módulos contadores de fótons nesses comprimentos de onda. De fato, os dispositivos de estado sólido existentes para detecção de radiação no IV médio ou distante, geralmente detectores de mercúrio-cádmio-telúrio (HgCdTe) carecem de resolução temporal e sensibilidade requeridas para qualquer aplicação em comunicações quânticas. A única solução a esse

problema, da qual se tem conhecimento nos dias de hoje, é a conversão de freqüências em um meio não-linear, seguida de um APD. Observe que não estamos mais falando de uma opção, como no caso do experimento intra-cavidade para contagem de fótons a 1.55μm, mas da única forma possível dentro da tecnologia disponível.

Este capítulo tem como objetivo, portanto, apresentar as vantagens e desvantagens de um sistema de comunicações quânticas que utilize um QCL como transmissor, a atmosfera como canal e um sistema de detecção de dois estágios (conversão de freqüências seguida de um APD de silício[75]). A escolha do comprimento de onda a ser utilizado (4.65 μm) será justificada na seção 5.1, juntamente com uma discussão do problema de ruído térmico. A seção 5.2 fornece e discute os resultados experimentais enquanto a seção 5.3 determina, para o comprimento de onda escolhido, se o sistema proposto é ou não viável, levando-se em consideração os efeitos atmosféricos de espalhamento.

5.1.
Seleção do comprimento de onda

Apesar da existência de diversas janelas de transparência na atmosfera, nem todas podem ser utilizadas como o canal quântico de nosso sistema e, das que poderiam, nem todas se comportam de modo equivalente. Na verdade, o sistema de detecção restringe o número de faixas úteis, e não é difícil entender o porquê.

Em primeiro lugar, é preciso estabelecer *como* a conversão de freqüências será realizada. De acordo com o capítulo 3, é necessário escolher um cristal não-linear que seja capaz de fornecer acordo de fase entre os comprimentos de onda do sinal de entrada no infravermelho (que desejamos escolher), do feixe de bombeio (também a ser escolhido, dentre os disponíveis no mercado) e do sinal de soma de freqüências a ser detectado (que também deve ser escolhido!). A sub-seção a seguir mostra como isso pode ser feito.

---

[75] Observe que, no contexto atual, também faria sentido utilizar APDs de Germânio ou InGaAs. Retornaremos a esse assunto a seguir.

5.1.1.
Limites impostos pelo processo de detecção

Sabemos que o processo de soma de freqüências envolve 3 comprimentos de onda, que nessa discussão chamaremos de sinal de *entrada*, *bombeio* e *sinal de saída* (correspondendo, respectivamente, a ω_1, ω_2 e ω_3 do capítulo 3), além de um cristal não-linear. Além disso, desejamos utilizar um fotodiodo avalanche para realizar a detecção da luz convertida; conforme vimos na seção 2.4, as opções mais comuns são Si e InGaAs/InP, cada um sensível a faixas de comprimentos de onda de, respectivamente, 350-900 nm e 900-1700 nm.

Isso significa que precisamos encontrar cristais não-lineares que sejam transparentes não apenas no infravermelho médio/distante como também no visível e/ou infravermelho próximo. Não são poucos; a tabela 2 mostra alguns exemplos.

Cristal	Faixa de transparência [nm]
Ag_3AsS_3	600-13000
AgGaSe	710-18000
$AgGaS_2$	500-13000
CdSe	750-25000
GaSe	650-18000
$HgGa_2S_4$	500-13000
$LiIO_3$	300-6000
$LiNbO_3$	330-5500
Tl_3AsSe_3	1250-20000

Tabela 2. Alguns cristais não-lineares que podem ser utilizados para contagem de fótons no infravermelho médio/distante.

Além da transparência, o cristal não-linear a ser utilizado precisa ser capaz de fornecer casamento de fase birrefringente entre os comprimentos de onda desejados[76]. Observe que não há cristais não-lineares na tabela 2 que sejam transparentes a comprimentos de onda acima de 25 μm; isso acontece não porque

[76] A princípio, o casamento de fase poderia ser realizado com polarização periódica do cristal (*quasi-phasematching*), mas em geral esse é um processo muito caro e que precisa ser especialmente desenvolvido para cada tipo de material de modo a evitar imperfeições.

tais cristais não existem na natureza, mas porque os que existem não são transparentes a comprimentos de onda abaixo de 1700 nm. Portanto, aparentemente, 25 μm é um primeiro limite superior para o sinal de entrada.

Para o laser de bombeio, por outro lado, não há muitas opções. Assim como em qualquer processo de soma de freqüências, uma alta potência de bombeio é imprescindível para que a eficiência de conversão não seja baixa. Por essa razão, é necessário utilizar um laser semicondutor comercialmente disponível que possa gerar pelo menos 500 mW de potência[77]. Comprimentos de onda muito utilizados para bombeio são, por exemplo, 808, 980 e 1460 nm.

Quanto ao comprimento de onda de saída, é evidente que APDs de silício são sempre bem-vindos. Isso significa que, se possível, o sinal convertido deve ter, no máximo, comprimento de onda de 900 nm. Não precisamos nos preocupar com o valor mínimo pois, no limite inferior do infravermelho médio, teríamos no pior dos casos $3.5\,\mu\text{m} + 808\,\text{nm} \rightarrow 656\,\text{nm}$, um valor bem acima do mínimo.

Essas quatro condições, levadas em consideração simultaneamente, impõem limites à gama de comprimentos de onda que podem ser utilizadas para os fótons nos quais os qubits serão codificados. Entretanto, existe um outro fenômeno que estabelece limites ainda mais rigorosos: o ruído térmico.

5.1.2. Ruído térmico

Qualquer sistema de comunicações quânticas de espaço livre sofre de um tipo de ruído externo ao detector: o *ruído de fundo*. Esse ruído consiste em quaisquer fótons presentes na atmosfera que não possam ser distinguidos pelo detector dos fótons enviados pelo transmissor – isto é, de mesmo comprimento de onda e polarização (em alguns esquemas, também do tempo de chegada). No caso de sistemas operando no infravermelho médio/distante, esses fótons provêm, basicamente, da radiação de corpo negro emitida por todos os objetos em equilíbrio térmico com a temperatura ambiente (300 K). Chamamos esses fótons de *ruído térmico*.

[77] Supondo operação em regime contínuo (CW). Lasers semicondutores são preferíveis devido à praticidade e tamanho reduzido, mas uma configuração intra-cavidade também poderia ser vantajosa.

Como podemos quantificar o efeito do ruído térmico em nosso sistema de detecção? Sabemos que o número médio de fótons de freqüência ω por modo em uma cavidade em equilíbrio térmico é dado por[78]:

$$\langle N(\omega)\rangle = \left[\exp\left(\frac{\hbar\omega}{kT}\right)-1\right]^{-1} \tag{5.1}$$

Onde k é a constante de Boltzmann e T a temperatura. Note que (5.1) descreve o número de fótons por modo espacial (**k**) e por freqüência (ω); podemos assumir que apenas um modo espacial é convertido em freqüência pelo processo não-linear, de forma que a *taxa média* de fótons térmicos por segundo chegando ao detector é dada por:

$$\langle n_{BG}\rangle = \int_{-\infty}^{\infty}\langle N(\omega)\rangle H(\omega)d\omega \tag{5.2}$$

Na expressão acima, $H(\omega)$ é a função de transferência normalizada dos componentes ópticos do estágio de detecção, que será em geral determinada pela banda passante do cristal não-linear e/ou de um filtro passa-banda utilizado especialmente com o propósito de diminuir o ruído de fundo. Se considerarmos que a função de transferência é centrada em ω_1 e tem largura espectral $\Delta\omega << \omega_1$, onde ω_1 é a freqüência do fóton a ser detectado, podemos reescrever a integral como:

$$\langle n_{BG}\rangle = \int_{-\Delta\omega/2}^{+\Delta\omega/2}\langle N(\omega)\rangle d\omega \approx \frac{\Delta\nu}{\exp(\hbar\omega_1/kT)-1} \tag{5.3}$$

onde $\Delta\nu = \Delta\omega/2\pi$. Observe, portanto, que o ruído é proporcional à aceitação espectral do dispositivo. Podemos agora definir o *número médio de fótons térmicos por pulso* como:

[78] Para uma interessante (e simples) demonstração da expressão 5.1, ver a seção 9.3 de [40].

$$\langle N_{BG} \rangle = \langle n_{BG} \rangle \Delta\tau = \frac{\Delta\nu \Delta\tau}{\exp(\hbar\omega_1 / kT) - 1} \tag{5.4}$$

Onde $\Delta\tau$ é a duração do pulso. Observe que a distribuição de probabilidade do número de fótons térmicos por pulso, assim como a distribuição do número de fótons por modo em uma cavidade em equilíbrio térmico, segue uma estatística de *Bose-Einstein* (ou *geométrica*), dada por:

$$p_{BG}(n) = \frac{\langle N_{BG} \rangle^n}{\left[\langle N_{BG} \rangle + 1\right]^{n+1}} \tag{5.5}$$

Dessa forma, a probabilidade de que, em um certo pulso, ocorra uma contagem de ruído, é dada pela probabilidade complementar de não haver nenhum ruído, isto é,

$$p_{noise} = 1 - (1 - p_{DC}) \sum_{j=1}^{\infty} p_{BG}(j)(1 - \eta_{\text{det}})^j \tag{5.6}$$

Onde p_{DC} é a probabilidade de contagens de escuro, que depende exclusivamente do APD sendo utilizado, e η_{det} é a eficiência global de detecção. A soma infinita representa eventos nos quais há múltiplos fótons de ruído chegando ao detector no mesmo intervalo de tempo, e podemos reescrevê-la como:

$$\sum_{j=1}^{\infty} p_{BG}(j)(1 - \eta_{\text{det}})^j = \frac{1}{\langle N_{BG} \rangle + 1} \sum_{j=1}^{\infty} \left[\frac{\langle N_{BG} \rangle (1 - \eta_{\text{det}})}{\langle N_{BG} \rangle + 1} \right]^j \tag{5.7}$$

É fácil perceber que (5.7) é a soma de uma progressão geométrica. Fazendo algumas contas e substituindo em (5.6), chegamos ao resultado:

$$p_{noise} = 1 - \frac{1 - p_{DC}}{\langle N_{BG} \rangle \eta_{\text{det}} + 1} \approx \langle N_{BG} \rangle \eta_{\text{det}} + p_{DC} \tag{5.8}$$

Onde a aproximação só é válida se $\langle N_{BG} \rangle$ for suficientemente pequena, o que em geral é verdade se pulsos curtos (da ordem de nanosegundos) forem utilizados. A importância relativa entre ruído de escuro e ruído térmico, logo, depende apenas da eficiência de detecção.

O gráfico da figura 40 mostra como o ruído térmico depende do comprimento de onda, supondo T = 300K e assumindo valores realistas de $\Delta\tau = 1\,\text{ns}$ e uma razão constante $\Delta\nu/\nu$ (isto é, um fator de qualidade constante) de 8000, que corresponde a um filtro de largura $\Delta\lambda = 0.1\,\text{nm}$ a 800 nm. A eficiência de detecção foi considerada constante e igual a 1 para todos os pontos da curva.

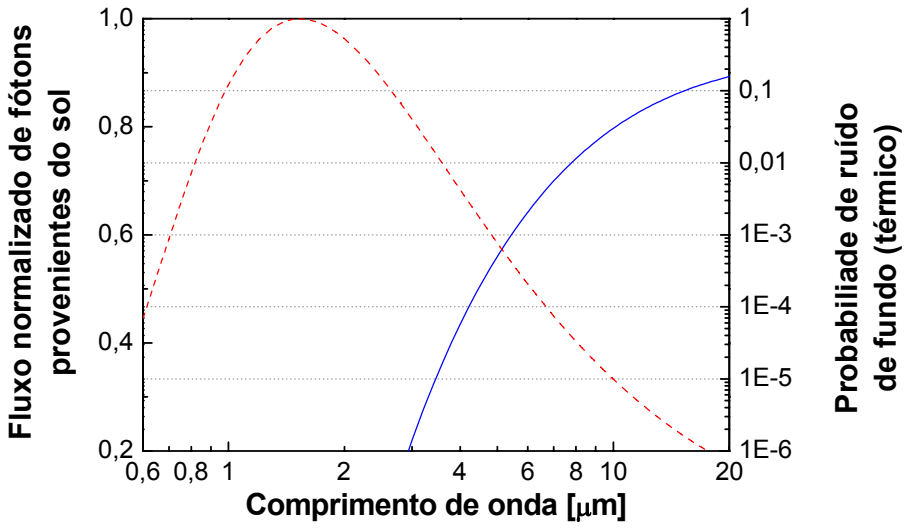

Figura 40. Linha sólida: probabilidade de ruído de fundo por pulso, em função do comprimento de onda. Linha tracejada: radiação solar normalizada, expressa em fótons por unidade de tempo por unidade de área por unidade de ângulo sólido.

Observe a curva cheia, cuja escala encontra-se no lado direito do gráfico. Para um comprimento de onda acima de 20 μm, a probabilidade de ruído (normalizada pela eficiência) é superior a ~15%, um valor extremamente alto. Essa simples observação nos leva a crer que sistemas de comunicações quânticas operando em comprimentos de onda no infravermelho distante não são viáveis.

Note, porém, que a curva decresce quase exponencialmente e que, a um comprimento de onda de 3 μm, o ruído já é 5 ordens de grandeza menor.

Observe ainda que a curva não pode ser extrapolada para o infravermelho próximo ou visível, já que a fonte de ruído predominante nesse caso é a luz do sol. Por essa razão, foi inserida no gráfico uma curva que mostra o fluxo normalizado de fótons provenientes do sol[79], dada por $\left(2/\lambda^2\right)\left(\exp\left[hc/\lambda kT\right]-1\right)^{-1}$. A escala nesse caso é linear, portanto não há diferença significativa entre os diferentes comprimentos de onda mostrados no gráfico com relação à radiação solar.

Aparentemente, a figura 40 nos informa que comprimentos de onda mais curtos são mais vantajosos! De fato, o visível e o infravermelho próximo não são afetados pela radiação de corpo negro a 300K, o que é sem dúvida uma vantagem, mas não podemos nos esquecer que o fator principal que nos levou a iniciar este estudo foi a maior *transmissão atmosférica*, que está diretamente relacionada, nesse caso, ao chamado *espalhamento Mie*.

5.1.3.
Condições atmosféricas e o espalhamento Mie

Existem três mecanismos básicos de espalhamento da luz na atmosfera, e todos eles podem ser definidos com relação a um *parâmetro de tamanho*, que pode ser definido como:

$$\alpha \equiv \frac{2\pi r}{\lambda} \tag{5.9}$$

Na definição acima, α é um parâmetro adimensional que relaciona o tamanho relativo de uma partícula presente na atmosfera, de raio médio *r*, e o comprimento de onda da luz incidente.

Quando $\alpha << 1$, isto é, quando a partícula é muito pequena quando comparada ao comprimento de onda, o mecanismo de espalhamento predominante é chamado de *espalhamento Rayleigh*, causado pelas moléculas dos gases existentes na atmosfera. Por ser fortemente dependente do comprimento de onda

($\sim\lambda^{-4}$), os menores comprimentos de onda sofrem muito mais espalhamento desse tipo. No caso da luz visível, o azul e o violeta são muito mais fortemente espalhados que o vermelho, podendo ser o mecanismo de atenuação predominante.

Se $\alpha >> 1$, temos o chamado *espalhamento geométrico*, que é independente do comprimento de onda da luz. Esse é o caso, por exemplo, da atenuação por chuvas, que afeta todos os comprimentos de onda da mesma forma. Com relação à luz visível, podemos observar espalhamento independente do comprimento de onda nas nuvens, que em dias de céu claro são brancas.

Porém, quando $\alpha \approx 1$ – isto é, quando o tamanho da partícula espalhadora é da mesma ordem de grandeza do comprimento de onda da luz – temos o chamado *espalhamento Mie*. Esse é o caso das névoas, neblinas e aerossóis, cujas partículas podem ter tamanhos variados dependendo das condições climáticas. Apesar de haver algumas fórmulas empíricas para o cálculo da atenuação causada por espalhamento Mie, elas não se aplicam igualmente em diferentes tipos de névoa, sendo necessário realizar um cálculo detalhado que leva em conta a distribuição estatística do tamanho das partículas espalhadoras.

Apenas como exemplo, um experimento realizado em uma encosta de montanha no Rio de Janeiro pelo mesmo grupo do qual faço parte[80] revelou que o espalhamento Mie depende fortemente do quão próximo o comprimento de onda se encontra com relação ao tamanho da gotícula de água presente na neblina. Ou seja, o estudo mostrou que, para $\alpha \cong 1$, a atenuação do enlace era muito menos pronunciada que para $\alpha > 1$. A figura 41 mostra alguns dados experimentais obtidos para diferentes níveis de visibilidade[81] do enlace, que dependia das condições climáticas [51].

---

[79] O pico de emissão de luz solar, próximo à janela de 1.55 μm, corresponde ao fluxo de fótons e não à intensidade, com a qual estamos mais habituados e cujo pico encontra-se no visível.

[80] Ver a descrição completa do experimento em [49].

[81] A visibilidade meteorológica é definida como a distância máxima na qual um objeto pode ser distinguido do ambiente de fundo pela visão humana (em geral, adota-se o comprimento de onda de 550 nm). Não confundir com a visibilidade interferométrica.

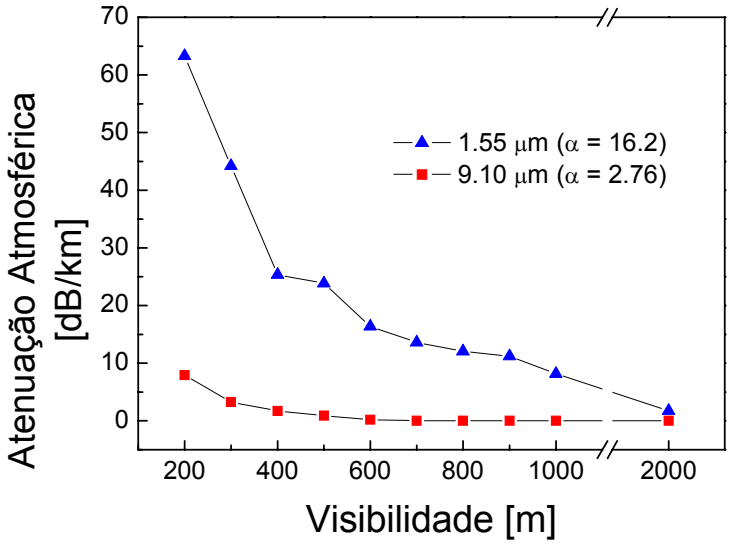

Figura 41. Dados experimentais de atenuação atmosférica para um enlace de visibilidade variável sob efeito de névoa "coastal upslope".

Dado que o raio médio das partículas desse tipo específico de neblina é em torno de 4 μm, o parâmetro de tamanho para 1.55 μm é de 16.2, enquanto para 9.1 μm já se aproxima de 2.76. Observe a enorme diferença em situações de baixa visibilidade: a transmissão atmosférica no IV médio pode chegar a ser 6 ordens de grandeza superior ao IV próximo! Esses e muitos outros resultados mostram que o uso de comprimentos de onda mais longos pode ser extremamente vantajoso. Note, porém, que não existe diferença significativa de atenuação entre os comprimentos de onda utilizados para condições climáticas muito boas (visibilidade acima de 2000 metros).

Por essa razão, os gráficos das figuras 40 e 41 devem ser observados ao mesmo tempo, isto é: o uso de fótons no infravermelho médio pode ser extremamente vantajoso por um lado, o da atenuação, mas trazer desvantagens por outro, o do ruído. A escolha vai depender fortemente das condições climáticas do local onde se deseja instalar o enlace de espaço livre.

Para nossa montagem experimental, encontravam-se disponíveis dois QCLs, nos comprimentos de onda de 4.6 e 9.1 μm. Optamos pelo primeiro, em parte devido ao menor ruído térmico que seria obtido. A escolha será inteiramente justificada no decorrer da discussão dos resultados.

5.2.
Resultados experimentais

O trabalho experimental desse projeto começou com uma montagem extremamente simples e que foi sofrendo alterações ao longo do tempo a cada novo resultado. Essa seção não tem como objetivo descrever a história do experimento, mas apenas os resultados mais importantes obtidos em casa fase da montagem.

Inicialmente, fornecemos os resultados de medidas clássicas de eficiência de conversão, passando por uma caracterização do ruído no regime de contagem de fótons para, finalmente, podermos fazer uma estimativa da QBER que seria obtida pelo uso do dispositivo de detecção (em sua configuração final) em um sistema de comunicações quânticas.

Atente para o fato de que alguns parâmetros (por exemplo, a taxa de repetição do QCL) podem possuir valores distintos em diferentes etapas do experimento. Exceto seja dito o contrário, pressupõe-se que os componentes utilizados são os mesmos ao longo da descrição que se segue.

5.2.1.
Obtenção do sinal de soma de freqüências

A primeira montagem experimental para medida da eficiência de conversão está esquematizada na figura 42.

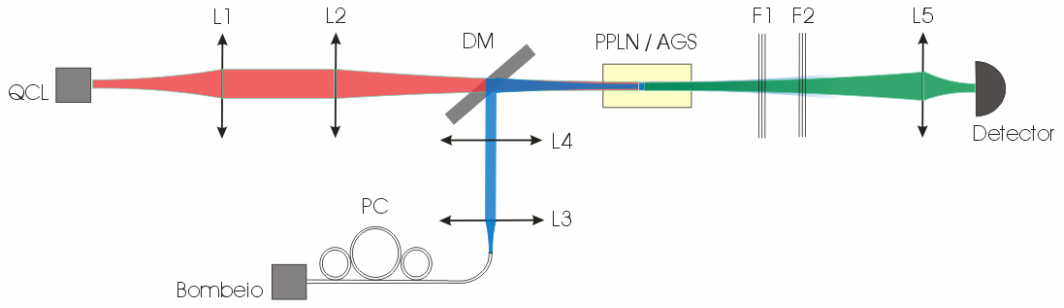

Figura 42. Montagem experimental para medida clássica de eficiência de conversão.

Nesta montagem, o *quantum cascade laser* (QCL), do fabricante Alpes Lasers, é configurado para produzir pulsos de luz a 4.65 μm de duração 100 ns e com uma taxa de repetição de 100 kHz. Com o auxílio de uma lente L_1, ele é

aproximadamente colimado[82] e feito passar através de duas fendas de mesma altura, que definem um eixo óptico ao longo do qual é posicionado posteriormente um cristal não-linear.

Convém ressaltar que nessa faixa espectral não há nenhum instrumento para visualização do feixe gerado pelo QCL, tais como câmeras ou cartões infravermelhos. Por isso, todo o processo de alinhamento é mais complicado, sendo necessário um detector com uma fenda (de diâmetro ajustável) diante de sua superfície sensível e montado em um estágio de translação *x*-*y*.

Quanto ao cristal não-linear, havia a disponibilidade de duas amostras: um cristal AGS ($AgGaS_2$, tiogalato de prata) e um PPLN (niobato de lítio periodicamente polarizado), que foram separadamente estudados. A tabela 3 compara os cristais segundo os parâmetros de interesse[83].

Cristal	Comprimento [mm]	d_{eff} [pm/V]	Casamento de fase
AGS	6	14,6	Tipo I
PPLN	10	16	QPM

Tabela 3. Comparação entre os cristais AGS e PPLN utilizados nas medidas.

Prosseguindo na descrição da montagem, o uso de um espelho dicróico de germânio (DM) permite a sobreposição do feixe proveniente do QCL com um feixe de bombeio a 980 nm com 320 mW de potência, do fabricante JDS, de forma que ambos sejam focalizados no interior do cristal não-linear. Dado que ambos os feixes devem satisfazer as condições de Boyd-Kleinman, que determinam um ponto de focalização e um parâmetro confocal para cada feixe, há necessidade de duas lentes para cada laser. Além disso, o máximo valor de potência de sinal convertido foi obtido apenas quando a lente L_3 foi montada sobre um estágio de translação que permitia livre posicionamento do feixe de bombeio.

[82] Devido ao astigmatismo do feixe e do fato de não haver lentes cilíndricas disponíveis (apropriadas para esse comprimento de onda), não foi possível colimá-lo perfeitamente.

[83] O coeficiente não-linear do cristal AGS foi obtido do software SNLO, mas na realidade não existe consenso sobre o valor do coeficiente d_{36} que o determina. Ver as refs. [52] e [53].

O controlador de polarização (PC) é utilizado para garantirmos que o estado de polarização da luz de bombeio, na entrada do cristal, é sempre vertical. Essa foi a direção escolhida como ordinária para os cristais AGS e PPLN, que realizam casamento de fase, respectivamente, birrefringente do tipo I (ooe) e *quasi-phasematching* (ooo). Portanto, o feixe a 4.65 μm também deve se manter com polarização vertical; a única diferença está no sinal convertido, que é polarizado horizontalmente no caso do AGS e verticalmente para o PPLN.

Os filtros F_1 e F_2 são, respectivamente, um filtro passa-baixa[84] com comprimento de onda de corte de 930 nm e um filtro passa-banda centrado em torno de 810 nm com 10 nm de largura espectral. Ambos servem ao objetivo comum de eliminar o feixe de bombeio. No caso específico do AGS, a montagem experimental contou ainda com um par de cubos polarizadores (PBS), cada um localizado entre as lentes L_3 e L_4 e entre os filtros e a lente L_5, de forma que o bombeio, de polarização vertical, também fosse fortemente reduzido ao passar por um polarizador na direção horizontal.

Finalmente, a lente L_5 é utilizada para focalizar o feixe de luz no detector de silício. Inicialmente, foi utilizado um detector clássico para as medidas de eficiência de conversão, que foram iniciadas com o cristal AGS, para o qual a montagem experimental é mais simples pois o cristal pode ser utilizado à temperatura ambiente. Constatou-se que, nesse caso, o cristal poderia ser mantido sobre um pedestal de posição fixa mas que possuísse a liberdade de girar em torno de seu eixo central, de forma que o ângulo de casamento de fase pudesse ser precisamente ajustado. Uma vez que os feixes estão sobrepostos, gira-se lentamente o cristal até a obtenção de sinal de soma de freqüências, indicado pelo detector.

Mas como saber se, de fato, o sinal obtido é resultado do processo não-linear? Afinal, não é possível enxergar o comprimento de onda de 809 nm a olho nu, diferentemente do que ocorre com a luz gerada no experimento de SFG intra-cavidade no qual o sinal gerado é vermelho[85]. Indiretamente, há várias formas,

[84] Os termos "passa-alta" e "passa-baixa", nessa tese, são sempre relacionados ao comprimento de onda e não à freqüência.

[85] Estamos falando de uma ordem de grandeza de nanowatts. É claro que, para feixes de bombeio a 809 nm de alta potência, podemos enxergá-los.

como por exemplo bloquear o feixe a 4.65 μm e verificar se o sinal desaparece, mas a rigor é preciso usar um analisador de espectro. A figura 43 mostra o resultado da medida.

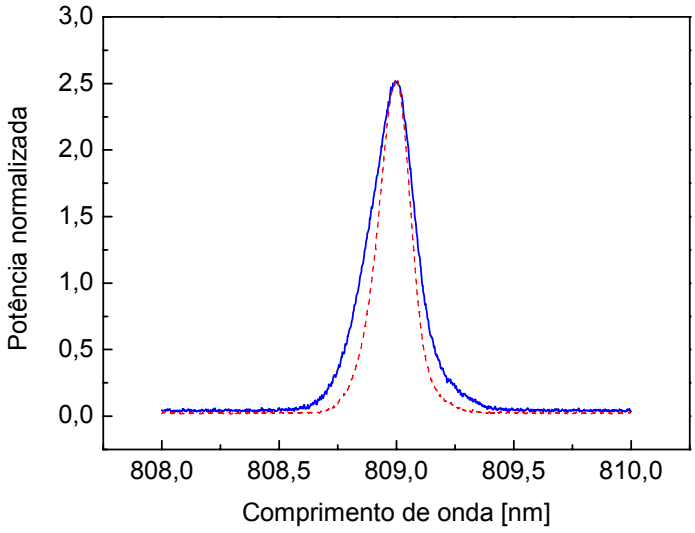

Figura 43. Espectro do sinal convertido usando o cristal AGS (linha cheia) e PPLN (linha tracejada). Observe que, em ambos os casos, ele é centrado em aprox. 809 nm.

O espectro do sinal não deixa dúvidas de que a potência observada corresponde ao comprimento de onda esperado. Observe que a largura à meia altura é bem inferior à largura do filtro passa-banda utilizado (10 nm), sugerindo que filtros mais estreitos podem ser utilizados para diminuição do ruído.

A montagem experimental com PPLN é praticamente idêntica, mas é necessário posicionar o cristal dentro de um forno cuja temperatura possa ser controlada. Verificou-se que havia casamento de fase em duas temperaturas distintas: 25 ºC e 93 ºC. Isso foi possível pois o cristal utilizado era dividido em diversas faixas (regiões), cada uma delas possuindo um período de polarização distinto, que variava de 21 a 22 μm com passos de 0.1 μm; portanto, cada temperatura encontrada corresponde a um período diferente. A figura 44 mostra como a eficiência de conversão varia com a temperatura, para o caso em que o período escolhido é de 22 μm.

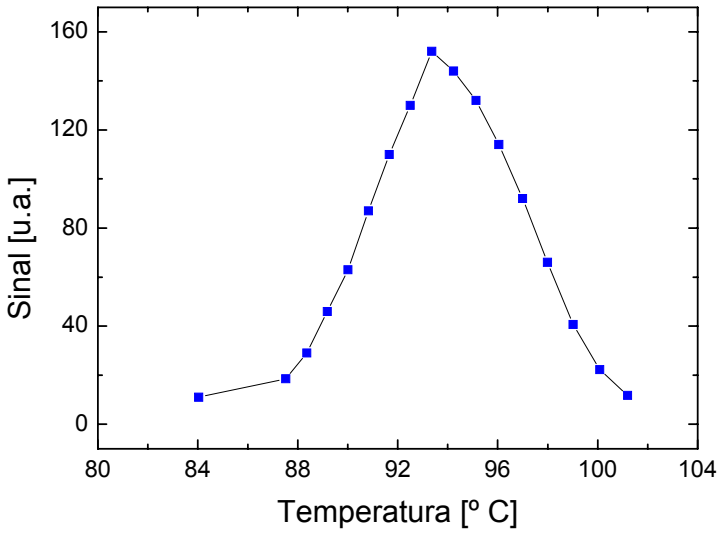

Figura 44. Variação do sinal de soma de freqüências com a temperatura do cristal PPLN, para um período de polarização de 22 μm.

Essa figura mostra que é muito mais "fácil" encontrar sinal de soma de freqüências no procedimento inicial de alinhamento para um PPLN do que para um AGS. Neste último, a dependência do ângulo de incidência é crítica (de poucos mrad), enquanto no primeiro, que é sempre mantido perpendicular ao eixo óptico, a dependência com a temperatura não é tão sensível.

Voltando à figura 43, vemos na linha tracejada o resultado da medida do espectro da luz convertida para ambas as temperaturas, que resultou em uma largura de linha mais estreita com relação ao AGS. Provavelmente, a diferença na largura vem do laser de bombeio, que pode ter variado de temperatura entre uma medida e outra (realizadas em um intervalo de algumas semanas). De fato, o que realmente limita a largura de linha do sinal convertido é o laser de bombeio, como veremos na seção 5.3.

5.2.2.
Medidas de eficiência e ruído no regime de contagem de fótons

Uma vez obtido o sinal de soma de freqüências, podemos prosseguir para as medidas de eficiência de conversão no regime de contagem de fótons[86]. A montagem experimental é idêntica à da figura 42, exceto pelo fato que o detector foi substituído por uma fibra monomodo a 830 nm conectada a um módulo de contagem de fótons. Além disso, o QCL foi reajustado para produzir pulsos de 20 ns com uma taxa de repetição de 750 kHz[87], gerando uma potência média de 1.57 mW, e posteriormente fortemente atenuado, por meio de 6 lâminas de vidro em série de ~ 1.5 mm de espessura cada, de atenuações previamente calibradas. A atenuação total medida foi de 54.8 dB, de forma que a taxa de fótons emitida por segundo é dada por:

$$n_{QCL} = \frac{P\lambda}{hc} = \frac{\left(1.57\times10^{-3}\right)\cdot\left(4.65\times10^{-6}\right)}{\left(6.62\times10^{-34}\right)\cdot\left(3\times10^{8}\right)} = 1.22\times10^{11}\,\text{Hz} \qquad (5.10)$$

A taxa acima foi a utilizada na configuração com cristal AGS. Para evitar que o dispositivo de contagem de fótons exiba efeitos de saturação, um par de lâminas de vidro extras, de menor espessura, foi utilizada na configuração com cristal PPLN, reduzindo a taxa (5.10) para 3.46×10^{10} Hz. A tabela 4 mostra os resultados obtidos.

	n_{QCL} [kHz]	n_{det} [kHz]	$\eta_{\text{det}} = \frac{n_{\text{det}}}{n_{QCL}}$	η_{opt}	η_q	$\eta_{SFG} = \frac{\eta_{\text{det}}}{\eta_{opt}\eta_q P_{pump}}$
AGS	$1.22\cdot10^{8}$	204	$1.7\cdot10^{-6}$	0.316	0.52	$1.9\cdot10^{-4}$ / W
PPLN	$3.46\cdot10^{7}$	125	$3.6\cdot10^{-6}$	0.137	0.52	$8.1\cdot10^{-4}$ / W

Tabela 4. Resultados das medidas de eficiência de conversão. No caso do PPLN, a eficiência de conversão é idêntica para as duas temperaturas de casamento de fase.

[86] As medidas também foram realizadas no regime "clássico" mas foram omitidas. Os mesmos resultados foram obtidos.

[87] 20 ns é o menor tempo possível de ser obtido com a eletrônica utilizada. A escolha de 750 kHz como taxa de repetição foi limitada pelo *duty cycle* do laser.

A coluna n_{det} mostra a taxa de pulsos obtida no contador de fótons quando há n_{QCL} fótons incidentes. O ruído em ambos os casos foi desprezado. A eficiência *global* η_{det}, definida como a razão entre essas duas taxas, indica a probabilidade que um fóton a 4.65 μm seja convertido e gere um pulso elétrico. Se esse valor for dividido pela transmissão dos componentes ópticos η_{opt} e pela eficiência do APD de silício η_q, obtemos a eficiência de conversão de freqüências, que na tabela 4 foi expressa em função da potência de bombeio, cujo valor é de 63 mW após perdas no espelho dicróico e em um filtro utilizado. Observe que, no caso do AGS, havia um filtro a menos na montagem experimental (e um PBS a mais), de forma que a transmissão dos componentes era superior.

É importante ressaltar que as condições de máxima eficiência obtidas para cada cristal não são as mesmas. De fato, devido ao comprimento distinto dos cristais e do tipo diferente de casamento de fase, a forma ideal de focalização dos feixes não é a mesma. Observe também que, no caso do PPLN, a eficiência depende sensivelmente da temperatura do forno no qual ele se encontra inserido (ver seção a seguir).

Como os valores de eficiência encontrados se relacionam aos valores teóricos esperados? No caso do PPLN, o casamento de fase é não-crítico, ou seja, não há *walk-off*, de forma que, na expressão (3.86), podemos escrever $h_{mm}(k,B) \approx 1$; no entanto, para o cristal AGS, de acordo com o software SNLO, o ângulo de walk-off é de 17.8 mrad, de forma que B = 1.36; dado que temos k = 4650/810 = 5.7, a figura 21 nos dá $h_{mm}(k,B) \cong 0.6$.

Usando a expressão (3.86), obtemos eficiências (para 1 W de bombeio) de $5.31 \cdot 10^{-4}$ e $2.41 \cdot 10^{-3}$ para AGS e PPLN, respectivamente. Comparando com os resultados da tabela 4, vemos que, no primeiro caso (AGS), há um fator 2.8 entre a eficiência teórica e a obtida na prática; no segundo caso (PPLN), o fator é 2.9. Embora 2.8 e 2.9 sejam valores bem próximos que aparentemente significam alguma coisa, note que eles podem ser explicados por motivos completamente distintos. No caso do AGS, o ângulo de casamento de fase ideal não correspondia a uma incidência perpendicular dos feixes, o que pode ter representado uma fonte de perdas; para o PPLN, o motivo principal está no fato do niobato de lítio não

ser muito transparente no comprimento de onda de 4.65 μm, como mostra a figura 45, extraída do banco de dados do software SNLO. De fato, vemos que esse comprimento de onda já se encontra no limite da faixa de transparência, com uma transmissão de ≈ 0.6.

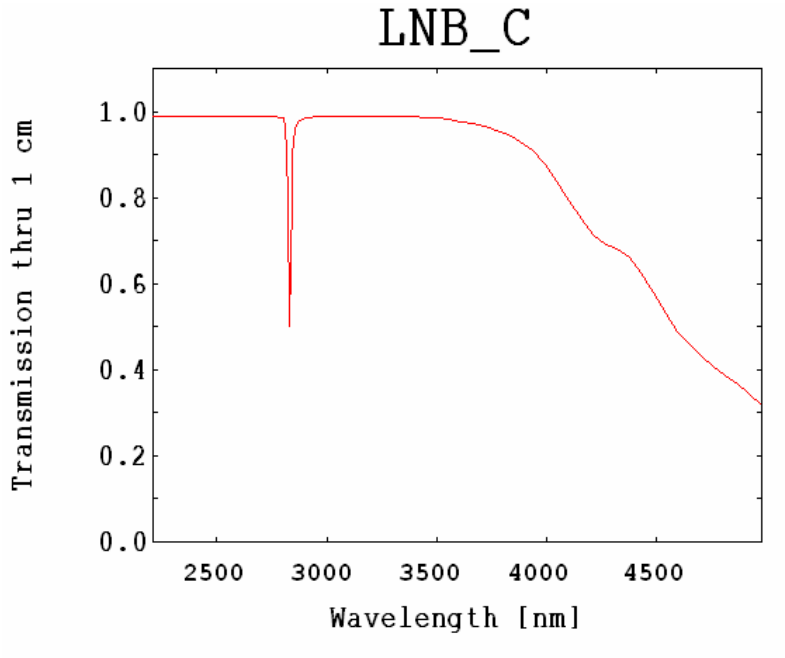

Figura 45. Transmissão da luz através de 1 cm de cristal de niobato de lítio, em função do comprimento de onda. Obtido do programa de simulação SNLO.

Segundo a teoria de Boyd-Kleinman, na presença de perdas não desprezíveis (como no presente caso), os feixes não devem ser focalizados no centro do cristal; é preferível focalizá-los em uma região mais próxima da interface de entrada, já que o sinal a ser convertido sofre menos perdas nessa região. Esse procedimento é equivalente a reduzir o comprimento efetivo do cristal, o que leva à redução da eficiência.

Uma vez caracterizada a eficiência, podemos avançar para as medidas de ruído. A taxa de escuro do detector EG&G foi medida desligando-se todas as fontes (QCL e bombeio) e isolando o detector ao máximo da luz ambiente residual, que está presente mesmo com a luz do laboratório apagada. O valor encontrado, 55 Hz, está próximo ao indicado pelo fabricante (< 50 Hz).

Já o ruído de fundo, caracterizado por fótons térmicos a 4.65 μm que são acidentalmente convertidos, deve ser medido com o laser de bombeio ligado. Foi curioso observar que, inicialmente, um nível extremamente alto de ruído foi encontrado pelo simples fato de que havia fótons de bombeio que se acoplavam ao

núcleo da fibra monomodo, atravessando todo o revestimento! Para evitar esse efeito foi necessário envolver todo o cabo com fita isolante.

Conforme foi dito anteriormente, o PPLN utilizado na medida apresentou casamento de fase para duas temperaturas distintas, 25 ºC e 93 ºC. A tabela 5 mostra os resultados da medida para ambas as temperaturas, além da medida para o AGS (sempre mantido a 25 ºC), comparando os resultados à teoria, dada pela expressão (5.3)[88].

	AGS	PPLN	
		25°C	93°C
$\langle n_{BG} \rangle_{\text{teoria}}$ [Hz]	7.7	16.8	118
$\langle n_{BG} \rangle_{\text{medido}}$ [Hz]	17.1	47.1	177

Tabela 5. Resultados da medida de ruído de fundo, após subtração das contagens de escuro (55 Hz).

Observe a grande diferença entre a taxas de ruído obtida, para as medidas com PPLN, quando se aumenta a temperatura de 25 para 93 ºC. Vimos na tabela 4 que a eficiência de conversão é independente da temperatura, portanto esse aumento não está relacionado a uma maior eficiência. A verdadeira explicação pode ser obtida através da figura 45, que mostra a baixa transparência do niobato de lítio no comprimento de onda que desejamos detectar. Isso significa que, da mesma forma que ele é capaz de absorver radiação, ele também é capaz de irradiar fótons nesse comprimento de onda; portanto, o ruído adicional vem da radiação de corpo negro do próprio PPLN, e obviamente ela não pode ser filtrada.

Note também que as taxas de ruído encontradas estão ligeiramente maiores que as previsões teóricas, o que pode representar que uma fonte de ruído extra esteja presente, como por exemplo fótons provenientes do laser de bombeio.

[88] O valor do ruído obtido nas configurações PPLN diferem do que foi publicado em [54]. A tabela fornecida nesta tese está correta; no entanto, o resultado final do artigo (sensibilidade de 1.24 pW) continua correta.

5.2.3.
Desempenho do detector

Na seção anterior, obtivemos 3 pares de resultados eficiência-ruído. De acordo com as tabelas 4 e 5, o cristal AGS exibiu a menor taxa de ruído térmico, mas ao mesmo tempo, a pior eficiência de conversão; enquanto isso, o cristal PPLN apresentou a maior eficiência e também a maior taxa de ruído. Como podemos comparar os detectores obtidos pelas diferentes configurações?

Sem dúvida, a configuração PPLN a 93 ºC não é desejável, pois basta diminuirmos a temperatura para 25 ºC e obtermos a mesma eficiência, porém um ruído bem inferior. Resta, pois, compararmos as duas restantes. Seguindo a idéia introduzida na seção 2.4.1.4, podemos calcular a *sensibilidade* dos dois detectores, que nesse contexto é dada por:

$$SNR_0 = \frac{hc}{\eta_{\det}\lambda}\langle n_{tot}\rangle \tag{5.11}$$

onde n_{tot} é a variável aleatória que descreve o ruído total, que podemos dividir em contagens de fundo (predominantemente ruído térmico) e contagens de escuro, que pressupomos descorrelacionadas de forma que:

$$\langle n_{tot}\rangle = \langle n_{dark}\rangle + \eta_{\det}\langle n_{BG}\rangle \tag{5.12}$$

Substituindo os valores em (5.11), obtemos, para as configurações com cristal AGS e PPLN (25 ºC), respectivamente, 180 pW e 124 pW de sensibilidade. Esse resultado mostra, portanto, que a configuração com PPLN é superior.

Observe, pois, que mesmo com uma eficiência global de 3.6×10^{-6} (ou seja, de cada 1 milhão de fótons enviados, apenas 3.6 em média são detectados), o dispositivo assim construído possui excelente sensibilidade, além de uma notável resolução temporal, obtida diretamente do APD de silício. A tabela 6 mostra uma comparação entre o detector assim obtido e outros detectores comercialmente disponíveis: um que funciona à temperatura ambiente (Vigo System PVI-5) e um outro, estado-da-arte, que é resfriado a nitrogênio líquido (Fermionics PV-650).

O tempo τ representa o tempo de resposta do dispositivo, que no caso do sistema upconversion é representado pela resolução temporal[89].

	τ [ns]	SNR_0 [pW]
Vigo System PVI-5	15	$1.63 \cdot 10^6$
Fermionics PV-650	20	223
PPLN @ 25°C + EG&G AQR-15FC	0.3	1.24

Tabela 6. Comparação entre a melhor configuração obtida e outros detectores comercialmente disponíveis.

É interessante observarmos que, mesmo usando uma potência de bombeio tão baixa (63 mW líquidos), a sensibilidade obtida é duas ordens de grandeza superior ao melhor detector em estado sólido para esse comprimento de onda. Uma pergunta que surge nesse momento: o que aconteceria se aumentássemos o bombeio (ou o comprimento do cristal)? A sensibilidade diminuiria ainda mais?

A resposta é negativa, como mostra a figura 46. Em primeiro lugar, é evidente que o aumento do bombeio implica no aumento da eficiência de conversão, e portanto da eficiência global. Observe no gráfico a existência de duas regiões de operação: para valores muito pequenos de eficiência, o ruído é dominado pelas contagens de escuro, que independem da eficiência de detecção. Assim, a curva cai com η_{det}^{-1} (uma reta no gráfico log-log).

Contudo, conforme a eficiência aumenta, os fótons oriundos de radiação térmica a 4.65 μm começam a ser convertidos e o ruído de fundo torna-se cada vez mais importante, até o momento em que é tão grande que o ruído de escuro pode ser desprezado. Nesse momento, podemos escrever:

$$SNR_0^{\min} \cong \frac{hc}{\eta_{\mathrm{det}}\lambda}\eta_{\mathrm{det}}\langle n_{BG}\rangle = \left(\frac{hc}{\lambda}\right)\frac{\Delta\nu}{\exp(hc/\lambda kT)-1} \tag{5.13}$$

[89] O tempo morto também poderia ser usado na comparação, que é de 50 ns para esse caso.

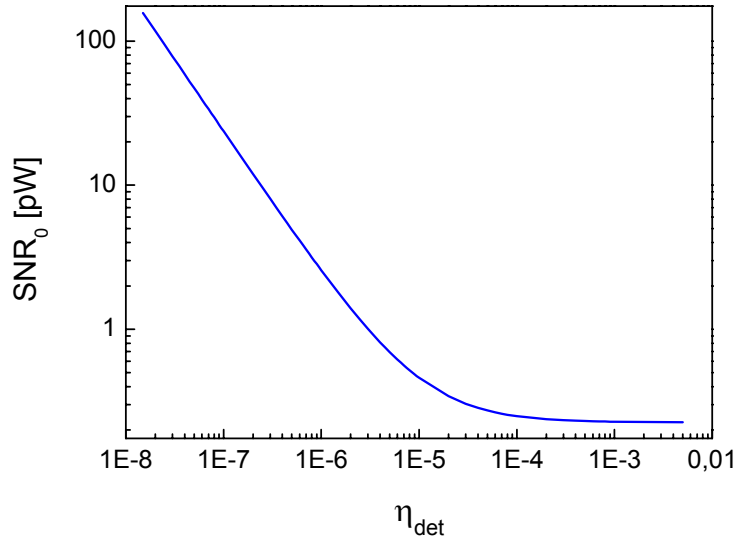

Figura 46. Variação teórica da sensibilidade com a eficiência global de detecção para a detecção via conversão de freqüências.

Onde a segunda igualdade foi obtida da expressão (5.3). Esse resultado mostra que a sensibilidade atinge um valor mínimo de saturação, correspondendo à região da direita do gráfico 46. Pela curva, vemos que esse valor não passa de algumas centenas de femtowatts.

Portanto, vemos que, se esse dispositivo for utilizado como um simples detector no infravermelho médio, ele pode apresentar várias vantagens sobre os existentes no mercado, como a elevada sensibilidade; entretanto, não podemos nos esquecer que trata-se de um sistema de detecção *monomodo*, o que pode ser um problema para algumas aplicações, como por exemplo em sistemas de comunicações de longa distância.

Dado que nosso objetivo principal é avaliar o detector proposto em um esquema de criptografia quântica, resta avaliarmos a QBER de um sistema construído usando detecção via soma de freqüências.

5.2.4. Montagem experimental para avaliação da QBER

No experimento anterior, avaliou-se o sistema de detecção via conversão de freqüências como uma ferramenta genérica, que a princípio poderia ser utilizado

em diversas áreas, como astronomia ou espectroscopia. Entretanto, resta avaliarmos sua aplicabilidade em sistemas de criptografia quântica, e a forma mais simples de fazê-lo consiste na caracterização das principais figuras de mérito que dependem da detecção. Conforme visto na seção 2.5.4, a QBER é o parâmetro mais utilizado para avaliação da segurança de um sistema de distribuição de chaves. A figura 47 mostra a montagem experimental utilizada para estimar a QBER de detecção no caso em que não há perdas no canal atmosférico.

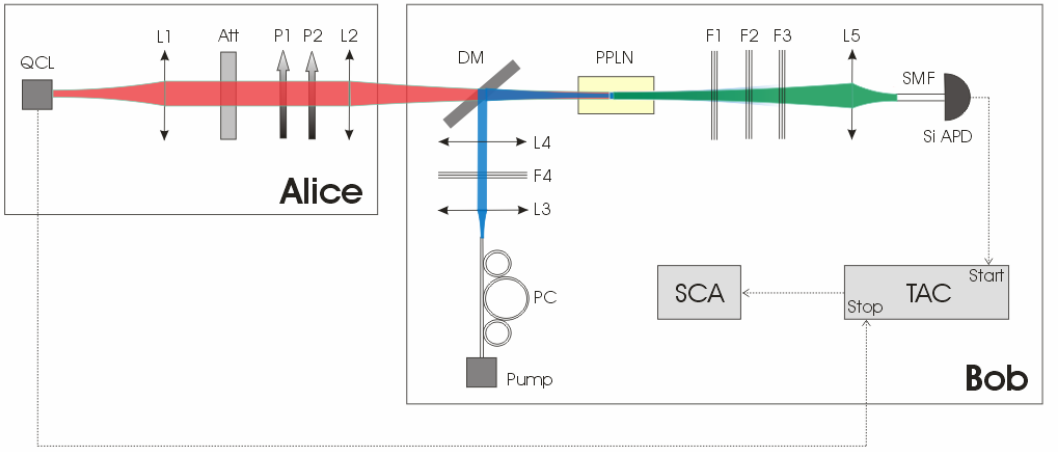

Figura 47. Montagem experimental para avaliação da QBER. As linhas pontilhadas representam conexões elétricas.

A primeira diferença importante entre essa montagem e a anterior (mostrada na fig. 42) está na possibilidade de alteração do estado de polarização dos fótons enviados por Alice ao longo de um grande círculo na esfera de Poincaré. Isso é possível devido à presença de dois polarizadores após o QCL, que conjuntamente simulam uma lâmina de meia-onda com perdas[90]. A figura 48 mostra o processo envolvido, no qual os estados inicial e final de polarização são representados por, respectivamente, $|\psi_i\rangle$ e $|\psi_o\rangle$. É fácil mostrar, usando a lei de Malus, que o coeficiente de transmissão do par de polarizadores é dado por:

$$\eta = \cos^2\alpha \cos^2(\theta - \alpha) \tag{5.14}$$

[90] Observe que, em sistemas de criptografia quântica, não há problema algum em haver perdas nos componentes ópticos de Alice, já que ela deve usar um atenuador de qualquer forma.

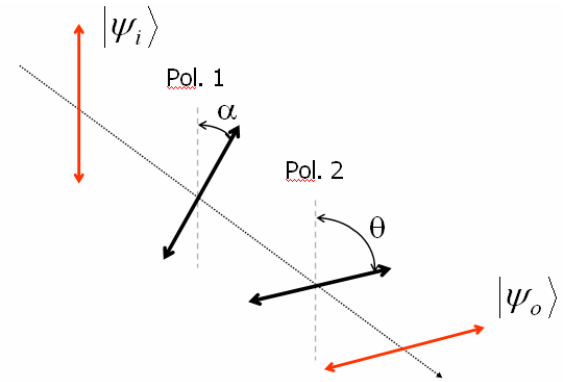

Figura 48. Rotação de polarização usando dois polarizadores.

A expressão (5.14) é importante pois ela nos diz como escolher o ângulo α para cada ângulo θ que desejamos rodar o estado de polarização de entrada, de forma a manter constante o coeficiente de transmissão η. É trivial perceber que (5.14) não possui solução para $\eta = 1$, mas ao mesmo tempo é intuitivo supor a existência de solução para $\eta = 0.25$, que é exatamente o valor máximo da transmissão quando desejamos girar um estado de polarização vertical para horizontal. Esse foi o valor utilizado na prática.

Assim como na medida de ruído, o QCL é configurado para gerar pulsos a uma taxa de repetição de 750 kHz; no entanto, como dissemos anteriormente, a menor duração de pulso atingível com a eletrônica disponível é de 20 ns – tempo demais para aplicações em comunicações quânticas, já que a taxa de ruído é proporcional à duração dos pulsos. Para obtermos uma menor duração, o seguinte truque foi utilizado: aplicar uma corrente de *bias* tal que, quando um pulso de corrente for aplicado, seu pico excede por muito pouco a corrente de limiar.

Para medir o pulso obtido, foi utilizado um conversor tempo-amplitude (TAC, *time-amplitude converter*) de forma a registrar o tempo de chegada dos fótons com relação ao tempo de emissão de um pulso elétrico no QCL. A figura 47 também mostra que as saídas do APD e do QCL foram conectadas, respectivamente, nas portas "start" e "stop" do TAC, de forma a gerar um histograma do tempo de chegada dos fótons[91]. Após alguns minutos, o formato do pulso de luz é reconstruído, como mostra a figura 49.

[91] Embora fosse mais lógico imaginar o contrário, isto é, usar os pulsos elétricos no QCL como "start" e a detecção como "stop", verificamos que o TAC se sobrecarregava devido ao grande número de eventos iniciados.

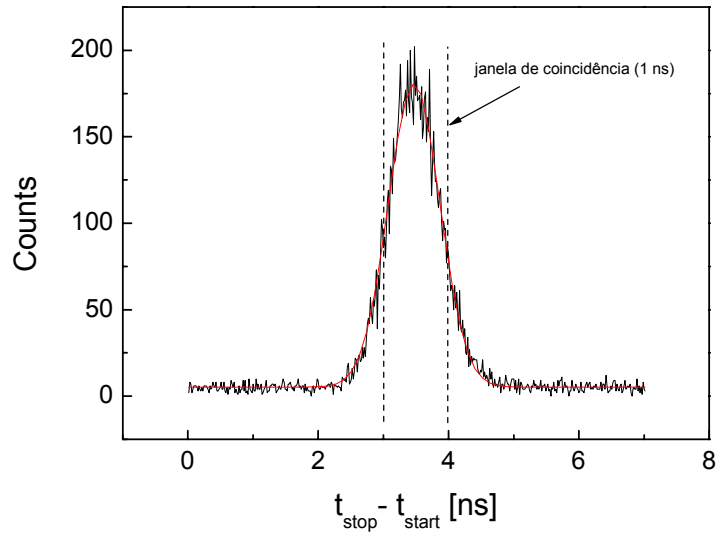

Figura 49. Histograma do tempo de chegada dos fótons (t_{start}) com relação ao tempo de emissão dos pulsos elétricos no QCL (t_{stop}) após vários segundos.

A figura mostra claramente que os pulsos de luz gerados pelo QCL, quando eletricamente polarizado próximo ao limiar, possuem uma largura à meia altura de aproximadamente 1 ns, já levando-se em conta a resolução temporal do APD (cerca de 300 ps). Isso sugere que podemos usar uma janela de coincidência, de 1 ns de duração, e selecionar como "válidos" quaisquer pulsos produzidos nesse intervalo, usando um analisador de canal único (SCA, *single channel analyzer)*. Esse procedimento é chamado de *pós-seleção*.

É importante ressaltar que as perdas totais foram calibradas de forma que, na saída do segundo polarizador (P2), cada pulso continha, em média, 0.8 fótons. Dado que são gerados 750 mil pulsos por segundo, isso corresponde a pouco mais de 2 fótons por segundo na detecção, e é por essa razão que são necessários vários segundos para a obtenção da figura 49.

Para medirmos a QBER, a polarização dos fótons enviados por Alice é variada (ângulo θ da figura 48) e, para cada passo, o número de eventos de contagem no SCA é gravado um certo número de vezes para um tempo de integração fixo de 100 s cada. Esse número de eventos é, então, plotado contra o ângulo θ e uma função cosseno é ajustada aos pontos experimentais, como mostra a figura 50. Note que o cristal não-linear já atua como um polarizador na

recepção, sempre com eixo de transmissão na direção de casamento de fase (no caso, polarização vertical).

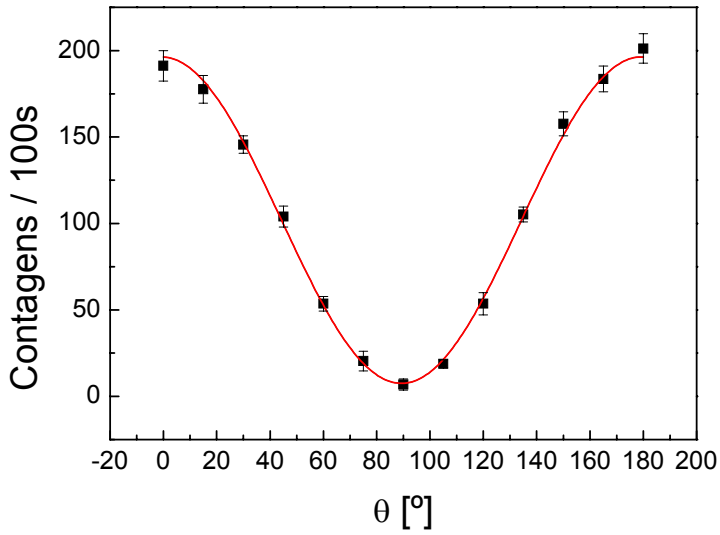

Figura 50. Curva de visibilidade para detecção de fótons únicos a 4.65 μm na base horizontal-vertical para μ = 0.8.

Dado que a visibilidade, obtida pela função cosseno (linha cheia no gráfico), é de 92.6%, podemos concluir que:

$$QBER = \frac{1-V}{2} = 3.7\% \tag{5.15}$$

Como esse valor se compara às previsões teóricas? Usando as expressões (2.43), (5.4) e (5.8), substituindo os valores obtidos na tabela 4, e adicionando 20% de perdas no processo de pós-seleção, também obtemos *QBER* = 3.7%, confirmando a validade do resultado experimental. Essa seria, portanto, a QBER mínima atingível se o detector desenvolvido fosse diretamente utilizado em um sistema de criptografia quântica, supondo ausência de perdas no espaço livre. Isso não é nem um pouco razoável!

Embora esse resultado sirva como uma prova de princípio, a utilidade do detector na prática é inviável. A seção a seguir discute como esse princípio poderia ser aplicado a um sistema realista.

5.3.
Estudo de viabilidade para criptografia quântica

Os resultados experimentais confirmam que um sistema de distribuição quântica de chaves operando em um comprimento de onda no infravermelho médio pode ser seguro, dado que foi obtida uma QBER experimental de 3.7% mesmo com uma probabilidade de detecção extremamente baixa. Nesse momento, é necessário discutirmos quais são os requerimentos técnicos para que um sistema real possa ser implementado.

5.3.1.
Construindo Alice e Bob

Como implementar Alice e Bob na prática? Embora possa haver mais de uma opção para comprimentos de onda mais tradicionais, sistemas operando no infravermelho médio sofrem de sérias restrições com relação à disponibilidade de componentes ópticos. Talvez a restrição mais séria seja a ausência de separadores de feixe polarizadores (PBS), que são amplamente utilizados em sistemas de criptografia quântica, sobretudo na recepção[92]. Além disso, não há componentes que sejam capazes de alterar ativamente a polarização. Essas duas limitações devem ser levadas em consideração nas propostas de configuração para Alice e Bob. Começando pelas damas, a montagem de Alice pode ser vista na fig. 51.

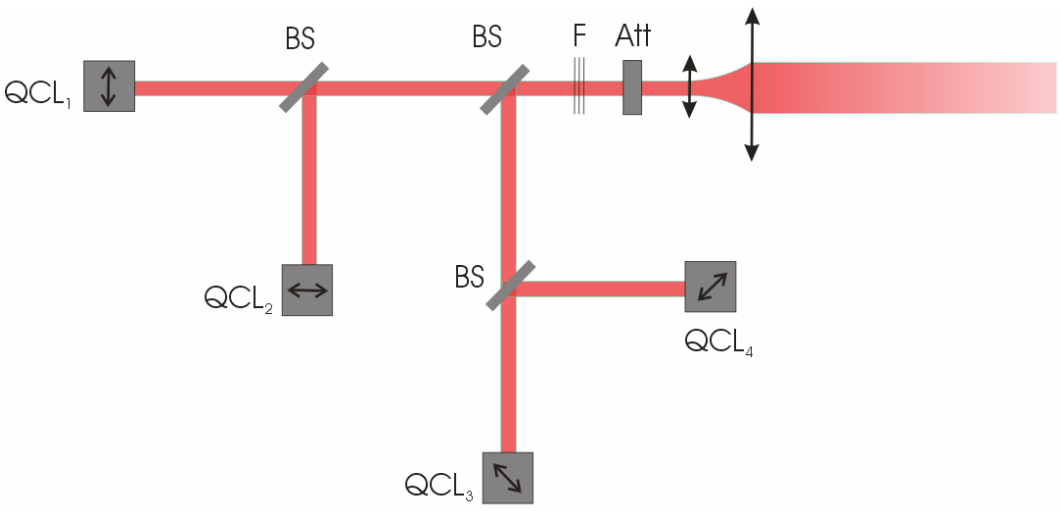

Figura 51. Implementação prática do sistema de transmissão (Alice).

[92] Essa informação data de Agosto de 2006.

Na montagem proposta para Alice, quatro QCLs, cada um gerando luz polarizada em um dos quatro estados de polarização do protocolo BB84, são conectados por meios de separadores de feixe 50/50. A escolha do estado de polarização poderia ser feita, por exemplo, partindo-se de lasers verticalmente polarizados e usando-se dois polarizadores de teflon, da mesma forma que foi realizada a montagem experimental na seção 5.2 (nesse caso os polarizadores estariam fixos). Observe que o atenuador é colocado apenas na saída, já que há um fator 1/4 de transmissão devido a duas incidências em separadores de feixe. Adicionalmente, um filtro interferencial é inserido em série com o atenuador, de forma que seja impossível sabermos a proveniência de um dado fóton através de uma medida de espectro. Em seguida, um telescópio se encarrega de alargar o feixe para que os efeitos de difração na atmosfera sejam minimizados.

No escritório de Bob, a ausência de um PBS complica um pouco a situação. Existem pelo menos duas alternativas; começamos pela mais realista, isto é, pela qual há certeza de que funcionaria, ilustrada na figura 52. Observe a semelhança à configuração de Alice.

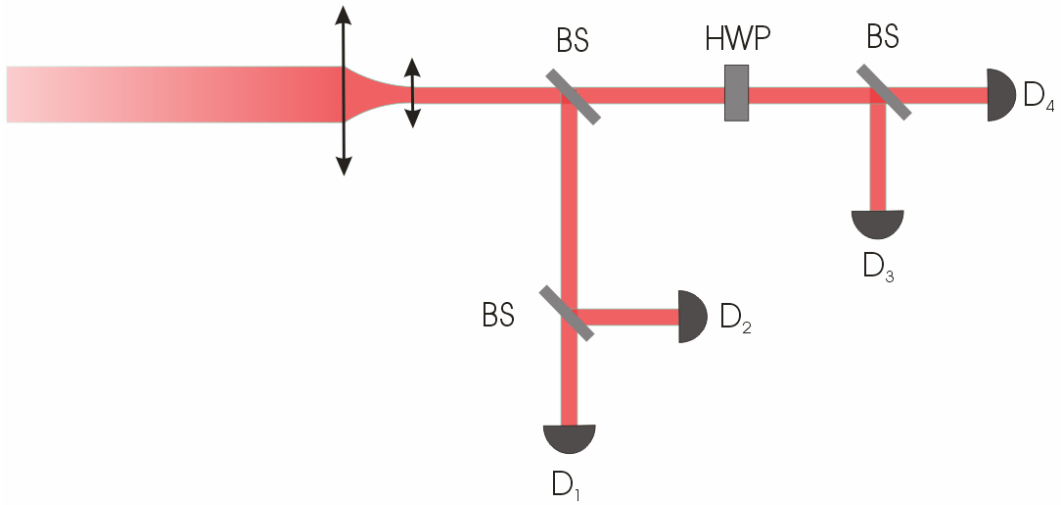

Figura 52. Implementação prática do sistema de recepção (Bob): primeira opção. Os detectores D_i incluem o processo de soma de freqüências.

O primeiro separador de feixe implementa uma escolha passiva de base, mas observe que, agora, as perdas introduzidas pelos três deles são prejudiciais ao sistema: há uma probabilidade de apenas 1/4 que um fóton atinja o detector "correto", contra uma probabilidade de 1/2 se houvesse disponibilidade de PBSs nesse comprimento de onda. Observe ainda que a orientação dos cristais não-

lineares, em cada par de detectores, deve ser de forma que atuem como polarizadores ortogonais entre si. Os feixes de bombeio, por conseguinte, também deverão ser ortogonalmente polarizados.

Entretanto, o maior obstáculo à construção de um sistema prático de criptografia quântica está, como vimos, na baixa eficiência de conversão de freqüências obtida em laboratório, que é fruto de uma modesta potência de bombeio. De forma a possibilitar uma eficiência de conversão razoável sem que haja necessidade de lasers de bombeio extremamente potentes, cada um dos quatro detectores D_i da figura 52 poderia ser implementado com uma configuração semelhante à cavidade em "L" da figura 32, que foi realizada experimentalmente em outro contexto. Considerando que o mesmo tipo de cristal (niobato de lítio) foi usado, temos plena convicção de que, com um laser de bombeio de 809 nm a 5 W, é possível obter uma potência de bombeio intra-cavidade de 25 W (ver a figura 35, cap. 4). A única diferença estaria no revestimento anti-reflexivo utilizado nos espelhos esféricos e, principalmente, no material do espelho dicróico, que poderia agora utilizar um material transparente ao infravermelho médio (por exemplo, CaF_2).

Nessa configuração, o processo de conversão de freqüências seria alterado para:

$$4.65\,\mu\text{m} + 1.064\,\mu\text{m} \xrightarrow{SFG} 870\,\text{nm} \qquad (5.16)$$

Observe que o comprimento de onda foi alterado de 809 para 870 nm, o que não é problemático pois continua dentro da faixa de detecção do APD de silício e, mais importante ainda, pode ser distinguido do feixe de bombeio!

Uma outra possibilidade, que fica aqui apenas como sugestão devido à sua difícil implementação, consiste na utilização de apenas um separador de feixes e de dois detectores; no entanto, cada detector seria formado por uma cavidade em "L" contendo dois cristais não-lineares em série ortogonalmente orientados[93], como mostra a figura 53.

[93] A idéia de usar dois cristais em série foi originalmente sugerida, com implementação em guias de onda, por [55].

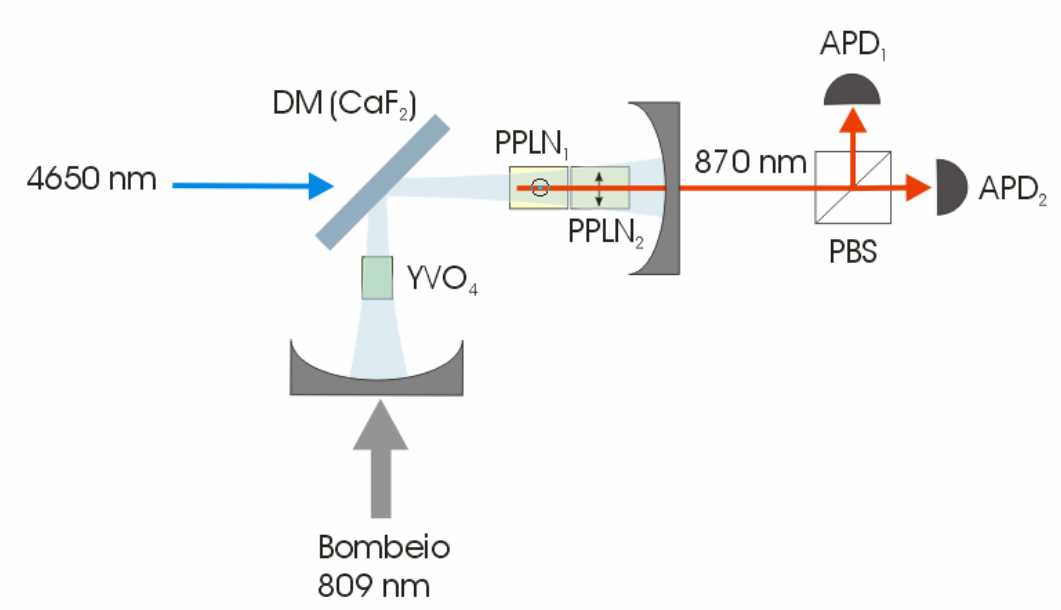

Figura 53. Configuração alternativa para o sistema de detecção de Bob.

O processo envolvido na configuração da figura 53 é equivalente ao apresentado na seção 4.2, com a diferença que há dois cristais não-lineares. Para entendermos o efeito causado por esse arranjo, considere que o PPLN 1 proporciona casamento de fase para a polarização vertical e o PPLN 2 para a horizontal; o feixe de bombeio deve estar polarizado linearmente a ±45º, de forma que a potência útil em cada cristal seja metade da potência de bombeio[94].

Vamos agora supor que o estado de polarização de entrada é genérico, de forma que possa ser escrito como:

$$\begin{aligned} |\psi_i\rangle &= |\lambda_1\rangle \otimes \left(\alpha|H\rangle + \beta|V\rangle\right) \\ &= \alpha|\lambda_1\rangle \otimes |H\rangle + \beta|\lambda_1\rangle \otimes |V\rangle \end{aligned} \tag{5.17}$$

O estado do fóton após o cristal PPLN 1 será dado por:

$$T_1|\psi_i\rangle = \alpha|\lambda_1\rangle \otimes |H\rangle + \beta|\lambda_3\rangle \otimes |V\rangle \tag{5.18}$$

[94] Alternativamente, o bombeio pode estar polarizado verticalmente (como na seção 4.2) mas os cristais não-lineares estarem orientados a ±45º.

Ou seja, apenas a componente vertical sofre conversão de freqüências, enquanto a horizontal não sofre alteração. Após o segundo cristal, obtemos finalmente o estado:

$$\begin{aligned} T_2T_1|\psi_i\rangle &= \alpha|\lambda_3\rangle \otimes |H\rangle + \beta|\lambda_3\rangle \otimes |V\rangle \\ &= |\lambda_3\rangle \otimes (\alpha|H\rangle + \beta|V\rangle) \end{aligned} \tag{5.19}$$

Onde ocorre exatamente o contrário. Dado que todos os feixes envolvidos são ordinários, não existe nenhum efeito de *walk-off*. Observe, portanto, que o estado de polarização é conservado no processo, e agora um PBS (comercialmente disponível no comprimento de onda gerado) pode ser utilizado para separar as duas componentes. Essa proposta é pouco realista pois ela pressupõe uma alta eficiência de conversão, para que ambos os processos (nos dois cristais) ocorram simultaneamente com alta probabilidade.

Em qualquer uma das duas configurações, é preciso que o estágio de filtragem também seja aprimorado com relação à montagem experimental de prova de princípio. De acordo com (5.4), a única forma de manter a contagem de ruído de fundo a menor possível é minimizar os termos $\Delta\nu$ e $\Delta\tau$. Considerando os valores realistas de largura de linha, para 4.65 e 1.06 μm de, respectivamente, 1.5 nm e 0.1 nm, o espectro dos fótons convertidos satisfará:

$$\begin{aligned} \Delta\lambda_3 &< \left(\frac{\lambda_3}{\lambda_1}\right)^2 \Delta\lambda_1 + \left(\frac{\lambda_2}{\lambda_1}\right)^2 \Delta\lambda_2 \\ &= \left(\frac{870}{4650}\right)^2 1.5 + \left(\frac{870}{1064}\right)^2 0.1 \cong 0.1\text{nm} \end{aligned} \tag{5.20}$$

Que é um valor inferior aos 0.35 nm utilizados no experimento. Quanto a $\Delta\tau$, não vemos nenhuma forma simples de diminui-lo abaixo de 1 ns; assim sendo, podemos prosseguir para a discussão de performance do sistema.

5.3.2.
Desempenho e limites no canal atmosférico

Podemos agora estimar o desempenho do sistema proposto. Supondo, portanto, que é gerada uma potência intra-cavidade de 25 W, um filtro interferencial de 0.1 nm de largura com 80% de transmissão e deixando os demais parâmetros sem alteração, a eficiência de conversão é aumentada de um fator 1250, fazendo com que a eficiência global seja dada por $\eta_{\text{det}} = 4.5 \times 10^{-3}$, um valor muito mais razoável.

Ao mesmo tempo, se Alice usar uma taxa de repetição de, digamos, 100 MHz, a taxa de bits "bruta" (antes do processo de *sifting*) em Bob, supondo a primeira configuração sugerida, seria dada por:

$$\begin{aligned} R_{raw} &= (1/4) f \mu \eta_{atm} \eta_{cpl} \eta_{\text{det}} \\ &= \left(\mu \eta_{atm} \eta_{cpl}\right) \cdot 112.5\,\text{kHz} \end{aligned} \tag{5.21}$$

Onde escrevemos $\eta_{link} \equiv \eta_{cpl}\eta_{atm}$ para podermos diferenciar as perdas intrínsecas à propagação atmosférica das perdas de acoplamento no receptor (que incluem as perdas por difração). O termo entre parênteses é função das condições atmosféricas e possui um limite mínimo, como veremos adiante.

É claro que qualquer aumento em eficiência implica em igual aumento do ruído térmico. O fator 1250 é grande o suficiente para que torne-se muito maior que o ruído de contagens de escuro e que o ruído de fluorescência que verificamos no capítulo 4, de forma que ambos podem ser desprezados. Nesse caso[95], a QBER de detecção é dada por:

$$\begin{aligned} QBER &\cong \left\{ 2 + \frac{\mu \eta_{cpl} \eta_{atm}}{\Delta\tau \Delta\nu} \left[\exp\left(\frac{hc}{\lambda_1 kT} \right) - 1 \right] \right\}^{-1} \\ &= \frac{1}{2 + 700 \cdot \mu \eta_{cpl} \eta_{atm}} \end{aligned} \tag{5.22}$$

[95] A expressão (5.22) é válida desde que o ruído térmico seja dominante; portanto, independe do valor absoluto da taxa de ruído e do valor da eficiência.

Dado que, na prática, a QBER não pode tomar valores acima de 10%[96], concluímos de (5.22) que:

$$\mu\eta_{cpl}\eta_{atm} > 10^{-2} \tag{5.23}$$

Aparentemente, a restrição é muito severa: não podemos ter mais de 20 dB de perdas no enlace. Note que esse limite não pode ser diminuído com o aumento da eficiência de conversão; de fato, ele é conseqüência da radiação de corpo negro, que só poderia ser amenizada se houvesse a possibilidade de diminuirmos a duração do pulso, a largura de linha do filtro de recepção ou – em uma situação altamente hipotética – a temperatura ambiente[97].

As duas outras figuras de mérito utilizadas para caracterização da performance de um sistema de criptografia quântica – a taxa de bits e a máxima distância – podem ser calculadas se as perdas atmosféricas no comprimento de onda selecionado forem conhecidas. Embora seja evidente que o produto $\mu\eta_{cpl}\eta_{atm}$ seja função das condições atmosféricas, não é nem um pouco óbvia a dependência desse produto com relação ao *tipo* de clima.

Mas como caracterizamos um clima? Como vimos na seção 5.1.3, o mecanismo de atenuação mais importante no infravermelho médio é o espalhamento Mie, cujo efeito é determinado pelo parâmetro de tamanho $\alpha = 2\pi r/\lambda$. Desta forma, quando nos referimos ao "tipo" de clima, estamos simplesmente falando da distribuição estatística do tamanho das partículas em suspensão na atmosfera. Se as condições atmosféricas forem perfeitas – ou seja, ausência de partículas de neblina, nevoeiro ou fumaça – a atenuação é muito baixa e (5.23) é facilmente satisfeito, muito embora um sistema de comunicações quânticas operando em um comprimento de onda mais curto (IV próximo, por exemplo) seja bem mais vantajoso nessas condições pelo ganho de simplicidade e eficiência de detecção.

---

[96] Teoricamente, de acordo com (2.49), a QBER poderia atingir 12%, mas o valor de 10% é mais usual em discussões práticas.

[97] Levando-se em consideração o problema do aquecimento global, do qual tanto se fala nos dias de hoje, isso seria realmente formidável!

A performance relativa de um sistema no infravermelho médio será máxima, portanto, sob condições atmosféricas nas quais o espalhamento Mie é muito pequeno para o comprimento de onda selecionado mas, ao mesmo tempo, grande para os demais comprimentos de onda mais usuais (curtos). Em termos do parâmetro de tamanho, desejamos que α seja pequeno a 4.65 μm e próximo da unidade a (por exemplo) 780 nm. Um bom exemplo que satisfaz essas condições é um tipo de névoa chamada de *névoa de radiação* (*radiation fog*), muito comum em regiões próximas a lagos. Por exemplo, na região da cidade de Neuchâtel, na Suíça, um dos tipos mais comuns de névoa de radiação possui gotículas de água de raio médio da ordem de 2 μm [56]; comparando os comprimentos de onda citados acima, temos:

$$\alpha_{4.65\,\mu\text{m}} = \frac{4\pi}{4.65} = 2.79$$
$$\alpha_{780\,\text{nm}} = \frac{4\pi}{0.78} = 16.1 \qquad (5.24)$$

Observe que esses valores são extremamente próximos dos parâmetros de tamanho presentes no experimento de C. Colvero *et al* descrito na seção 5.1.3; de acordo com a figura 41, os parâmetros são 2.76 e 16.2! Devido à falta de dados experimentais no comprimento de onda que selecionamos, procedemos da seguinte forma: dado que os parâmetros de tamanho são praticamente idênticos aos de uma realização experimental, tomamos emprestados os valores da figura 41 para avaliação do sistema a 4.65 μm sob névoa de radiação com partículas de raio médio 2 μm. Nessa analogia, portanto, substituimos 9.1 por 4.65 μm e 1.55 μm por 780 nm.

Fica claro, da observação da figura 41, que o sistema proposto a 4.65 μm seria útil sob condições climáticas de visibilidade até, pelo menos, 2 km. Além disso, a diferença em atenuação aumenta com a distância do enlace; por exemplo, se um certo enlace possuir 10 km de comprimento, a presença de névoa com 600 m de visibilidade implicaria em uma atenuação de 164 dB a 780 nm e apenas 1.9 dB a 4.65 μm – um ganho de transmissão de 16 ordens de grandeza!

No entanto, em comunicações de longa distância, o efeito de turbulência atmosférica é sempre mais pronunciado, e os efeitos de distorção de frente de

onda tornam-se mais preocupantes, especialmente se o sistema de detecção for monomodo, que é o caso. Isso significa que o fator de acoplamento η_{cpl} pode se tornar pequeno demais, tal que (5.23) não seja satisfeita. Portanto, o sistema de detecção desenvolvido não pode ser aplicado a enlaces de longa distância.

De forma a compararmos os dois sistemas, vamos também supor que o sistema a 780 nm também utiliza detecção monomodo – isto é, um APD de silício conectado a uma fibra óptica. Esse método é muitas vezes utilizado quando se deseja eliminar o ruído de fundo, como por exemplo luz solar refletida na direção do detector. Dado que estamos comparando um sistema hipotético a um real, vamos supor que *todo* o ruído de fundo é bloqueado pelo sistema de filtragem a 780 nm, de forma que todas as contagens indesejadas venham do ruído de escuro, que assumimos ser de 100 Hz. Adicionalmente, supomos que a eficiência de detecção global do sistema a 780 nm é de 70% e que o fator de acoplamento η_{cpl} é de 0.2 para ambos os sistemas, um valor realista para um enlace de 1.5 km. A tabela 7 fornece os resultados para uma condição de visibilidade de 300 m e uma taxa de repetição f = 10 MHz para Alice, que envia pulsos com $\mu = 1$.

	η_{atm}	$\eta_{cpl}\eta_{\mathrm{det}}$	p_{photon}	p_{noise}	R_{raw}	$QBER$
4.6 μm	3.22×10^{-1}	9×10^{-4}	2.9×10^{-4}	6.8×10^{-6}	2.9 kHz	2.24%
780 nm	2.31×10^{-7}	1.4×10^{-1}	3.2×10^{-8}	1.0×10^{-7}	0.32 Hz	43.1%

Tabela 7. Comparação entre dois sistemas de criptografia quântica de espaço livre operando a 4.65 μm e 780 nm através de 1.5 km de névoa de radiação, com partículas de raio ~ 2 μm em média e visibilidade de 300 m.

Observe que, sob essas condições, o sistema a 780 nm não é capaz de estabelecer uma chave secreta, enquanto o sistema a 4.65 μm é pouco afetado. O produto $\mu\eta_{cpl}\eta_{atm}$, nesse caso, vale 6.44×10^{-2}.

É importante ressaltar que, no exemplo da tabela 7, toda e qualquer influência da luz solar espalhada foi ignorada, o que pode ser muito difícil de ser obtido, tanto no infravermelho médio como no próximo, mesmo utilizando-se detectores monomodo [57]. A seção a seguir trata desse problema.

5.3.3.
O efeito da luz solar: uma discussão qualitativa

Em dias de neblina muito forte, muitas vezes temos que parar e olhar com calma para sabermos a posição exata do sol, pois temos a impressão de que a luz chega a nossos olhos por todas as direções. Esse é exatamente o efeito do espalhamento Mie sobre a luz solar, e não é difícil imaginar de que forma um sistema de comunicações pode ser prejudicado por esse efeito.

De acordo com a figura 40, o fluxo de fótons solares (medido em fótons por unidade de tempo por unidade de área por unidade de ângulo sólido) não depende muito do comprimento de onda na faixa que estamos considerando, isto é, entre 600 nm e 10 μm; a única diferença entre os diferentes comprimentos de onda da luz solar, portanto, está no espalhamento que sofrem ao incidirem sobre o volume atmosférico que contém o enlace. A figura 54 ilustra o problema. Suponha que tanto Alice como Bob utilizam telescópios de mesmo diâmetro (D_0), que a propagação dos qubits se dá ao longo do eixo horizontal e que o ângulo de elevação do sol é representado por θ.

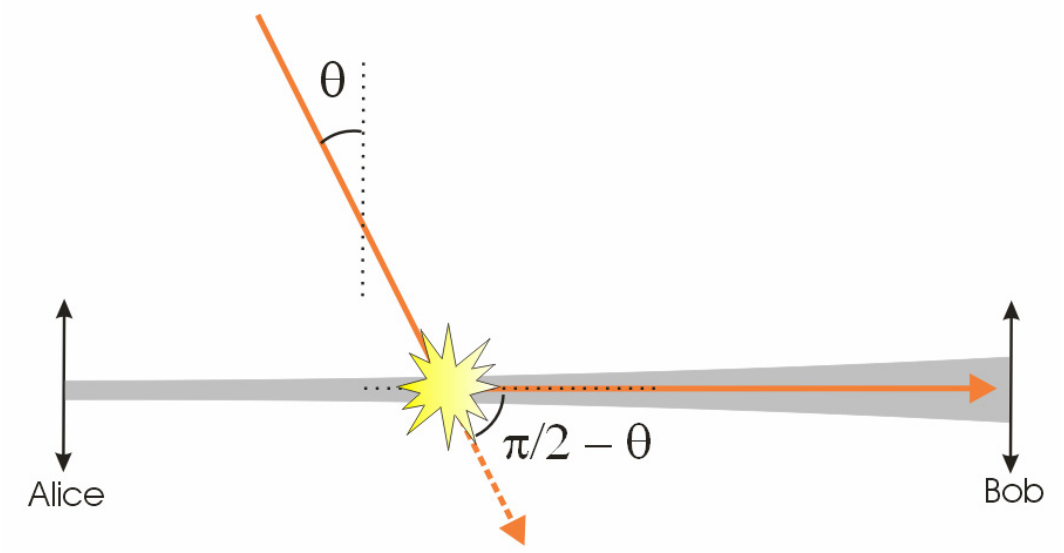

Figura 54. Modelagem dos efeitos da radiação solar sobre um sistema de comunicações quânticas de espaço livre.

Observe a presença de duas condições para que o fóton representado pela seta inclinada seja acoplado ao modo de propagação do sinal e conseqüentemente possa gerar uma contagem de ruído: (1) um evento de espalhamento deve ocorrer e (2) dado que um espalhamento ocorreu, o desvio de ângulo do raio solar deve

ser de aproximadamente $\pi/2-\theta$. Essas duas condições dependem de propriedades chamadas de, respectivamente, *probabilidade de espalhamento* e *distribuição angular de espalhamento*.

Conforme vimos na seção anterior, a probabilidade de espalhamento é dada pela relação existente entre o comprimento de onda usado, o tamanho das partículas e, principalmente, a concentração delas. Quanto menor a visibilidade meteorológica, maior a concentração de partículas e, portanto, maior a probabilidade que um evento de espalhamento ocorra. Essa dependência pode ser claramente visualizada na figura 41.

A distribuição angular de espalhamento depende apenas do parâmetro de tamanho, e pode ser caracterizada pela chamada *Função de Fase de Mie*, representada por $\Phi(\pi/2-\theta)$. Essa função tem uma interpretação probabilística imediata, já que sua integral ao longo de todos os ângulos de espalhamento é 1. Dado que, em geral, o cálculo dessa função é extremamente complexo, usamos um programa de computador chamado MiePlot. A figura abaixo mostra as funções de fase para os comprimentos de onda 780 nm e 4.65 μm, supondo o mesmo tipo de névoa no qual os parâmetros de tamanho são dados por, respectivamente, 2.79 e 16.1.

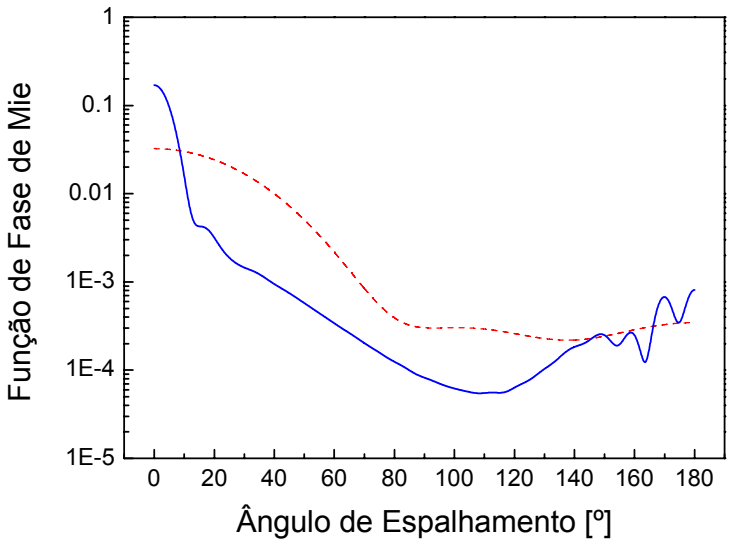

Figura 55. Função de fase de Mie para névoa de radiação com raio médio de 2 μm (10% de desvio padrão, distribuição log-normal) para os comprimentos de onda relevantes. Na simulação, considerou-se luz despolarizada.

Observe que, para os fótons solares a 780 nm, o espalhamento é muito mais pronunciado na mesma direção do raio de origem, enquanto para os fótons a 4.65 μm, o espalhamento se dá de forma muito mais homogênea. Esse comportamento já nos dá uma pista importante na avaliação do impacto da luz solar: os dois efeitos, probabilidade de espalhamento e distribuição angular, atuam em direções contrárias. Enquanto o primeiro favorece os comprimentos de onda mais longos, já que a atenuação é mais branda, o segundo favorece os comprimentos de onda mais curtos, pois a probabilidade que o desvio angular se dê na direção de Bob é muito menor (supondo que o sol não está próximo ao horizonte de Alice).

Portanto, podemos intuitivamente concluir que os efeitos da luz solar sobre o desempenho de sistemas de comunicações quânticas é extremamente dependente das condições atmosféricas e da posição relativa do sol com relação ao enlace, de forma que é muito difícil afirmarmos, a priori, qual comprimento de onda é mais ou menos susceptível a essa influência. Uma resposta definitiva a respeito do assunto necessitaria de uma análise rigorosa da situação, que leve em consideração o múltiplo espalhamento da luz solar ao longo da direção de propagação do sinal; próximos trabalhos futuros abordarão esse assunto.