3 Sistemas reais

3.1 Transmissão e recepção

3.1.1 As fontes ópticas

Até aqui temos assumido sistemas ideais, isto é, fontes e detectores perfeitos. Mas como podemos gerar e detectar fótons unitários na prática? Já existem sistemas capazes de gerar fótons unitários, porém com uma eficiência muito baixa além de estarem muito distantes de serem práticos e transportáveis [3]. Para sistemas de criptografia quântica essas soluções ainda não são interessantes.

A saída mais utilizada até o momento é a aplicação de pulsos coerentes fracos (WCP). A idéia é utilizar um laser gerando pulsos a uma taxa constante. Na saída deste é colocado um atenuador calibrado de forma a diminuir a intensidade do laser, de forma que tenhamos uma média de uma fração de fóton por pulso. A distribuição de fótons na saída de um laser pode ser considerada poissoniana e é dada por: [18] (Figura 10).

$$P(n,\mu) = \frac{\mu^n e^{-\mu}}{n!}. \tag{3.1}$$

Essa expressão nos permite então calcular a probabilidade de se encontrar um número *n* de fótons por pulso, para um dado número μ médio de fótons para o mesmo pulso. Vamos supor que inicialmente queremos um número médio de fótons por pulso igual a um. Obtemos então P(0,1) = 0.368, isto é, em 36,8% dos pulsos não encontraremos nenhum fóton. Similarmente obtemos P(1,1) = 0.368, P(2,1) = 0,184 e P(3,1) = 0.061. Isto é para outros 36.8% dos pulsos encontraremos 1 fóton, enquanto para 18.4% teremos 2 fótons e 6.1% dos pulsos conterão 3 fótons. Finalmente 1.9% de todos os pulsos conterão 4 fótons ou mais.

O grande problema, como veremos nesse capítulo, é que pulsos contendo 2 fótons ou mais geram uma grande falha na segurança pela vulnerabilidade ao

ataque PNS (“divisão do número de fótons”). Nesse ataque Eva simplesmente rouba um dos fótons desses pulsos permitindo que o resto alcance Bob. Dessa maneira ela pode fazer o que quiser com o fóton adquirido por ela, sem alertar Alice e Bob de sua presença.

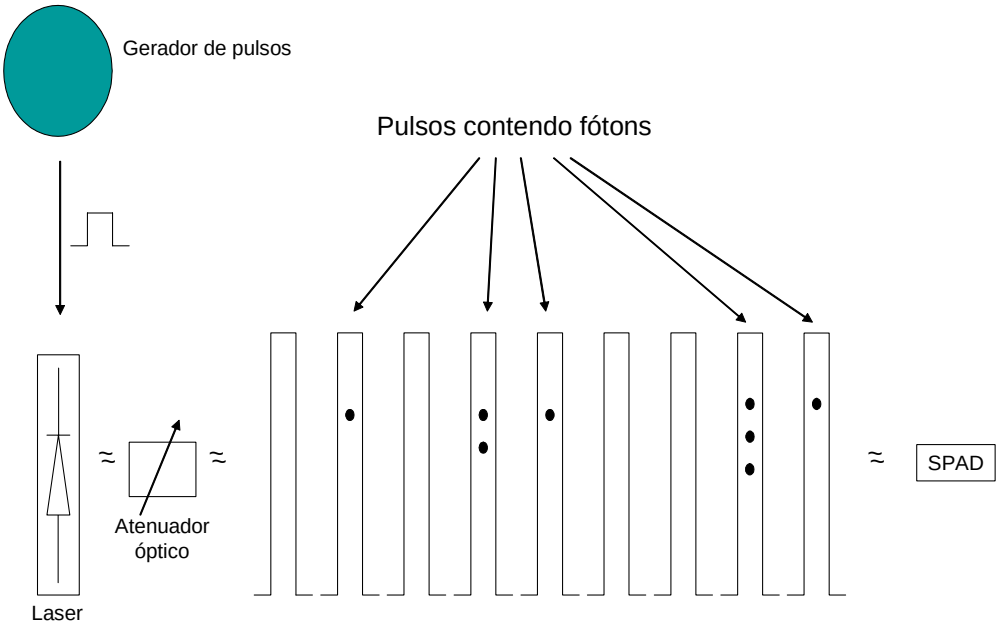

Figura 10: Situação esquemática da emissão de WCPs de um laser pulsado para μ = 1. Os pulsos contendo mais de um fóton são uma ameaça para a segurança do sistema.

O nosso problema agora é como evitar que uma grande parte dos pulsos contenha mais de um fóton. No nosso exemplo anterior vimos que 36.8% dos fótons não contém nenhum fóton, logo eles não serão úteis para o sistema. Dos pulsos restantes, 50% deles conterão um fóton, enquanto os outros 50% conterão dois fótons ou mais. Logo se o presente esquema for utilizado Eva poderá obter um ganho de informação sobre 50% dos fótons sem ser detectada! Essa situação é inaceitável.

Pode-se mostrar que a probabilidade de um WCP não vazio conter mais de um fóton é dada por: [3]

$$P(n>1 \mid n>0,\mu) = \frac{1-P(0,\mu)-P(1,\mu)}{1-P(0,\mu)} = \frac{1-e^{-\mu}(1+\mu)}{1-e^{-\mu}} \approx \frac{\mu}{2}. \qquad (3.2)$$

Como foi visto na caso anterior (μ = 1) a probabilidade de termos um WCP não vazio conter mais de um fóton é μ/2 = 1/2. Note que podemos reduzir o quanto quisermos essa probabilidade, para isso basta reduzirmos o valor de μ. A desvantagem é que reduziremos a taxa de transmissão, pois operando com um μ menor, teremos menos pulsos contendo fótons. O valor usualmente utilizado na prática é μ = 0.1. Isso nos dará P(0,0.1) = 0.905, ou seja, 90.5% dos pulsos não conterão nenhum fóton. Teremos P(1,0.1) = 0.0905 e P(2,0.1) = 0.00452. Com isso 9.05 % dos pulsos conterão 1 fóton e somente 0.45% dos pulsos conterão 2 fótons. Isso nos dará apenas aproximadamente 5% dos pulsos válidos (com fótons presentes) contendo 2 fótons ou mais, ou seja μ/2 = 0.1/2 = 0.05. Isso já nos dá um ganho de segurança pois agora somente 1 pulso em cada 20 pulsos válidos (ou 1 em 200 totais) será passível de sofrer um ataque PNS.

Uma outra solução é a utilização de pares de fótons gerados por "decaimento paramétrico" (*parametric downconversion)* a partir de um bombeio óptico em um cristal não-linear [3]. A idéia é que utilizemos um dos fótons do par para avisar ao sistema de que outro fóton foi criado e que está sendo enviado para Bob. Com isso pulsos com mais de um fóton são efetivamente eliminados (Figura 11).

O laser de bombeio produz pulsos ópticos muito intensos pois a conversão que ocorre no cristal não-linear é de muito baixa eficiência. Por essa razão esse esquema ainda não pode ser utilizado comercialmente gerando um desempenho pior do que os lasers gerando WCPs. O esquema utilizando pares de fótons pode vir a ser a melhor aproximação com a tecnologia atual para a "arma de fótons", isto é, uma fonte que manda um fóton e somente um quando ela for comandada.

Uma possibilidade ao se utilizar essas fontes é que podemos utilizar o protocolo EPR (com as devidas modificações no sistema), que fornece a vantagem adicional de se realizar o teste das inequalidades de Bell para a detecção de Eva.

Finalmente como é mostrado na figura 11, o computador de Alice comanda o sincronismo do sistema. Logo existe um enlace adicional, conectando Alice ao Bob. Na figura esse enlace é feito utilizando cabos elétricos, mas na prática ele pode ser um outro canal na mesma fibra óptica. Esse canal conectando os dois

computadores é o canal clássico e além de carregar informação quanto ao sincronismo do sistema, ele transportará a informação para a reconciliação.

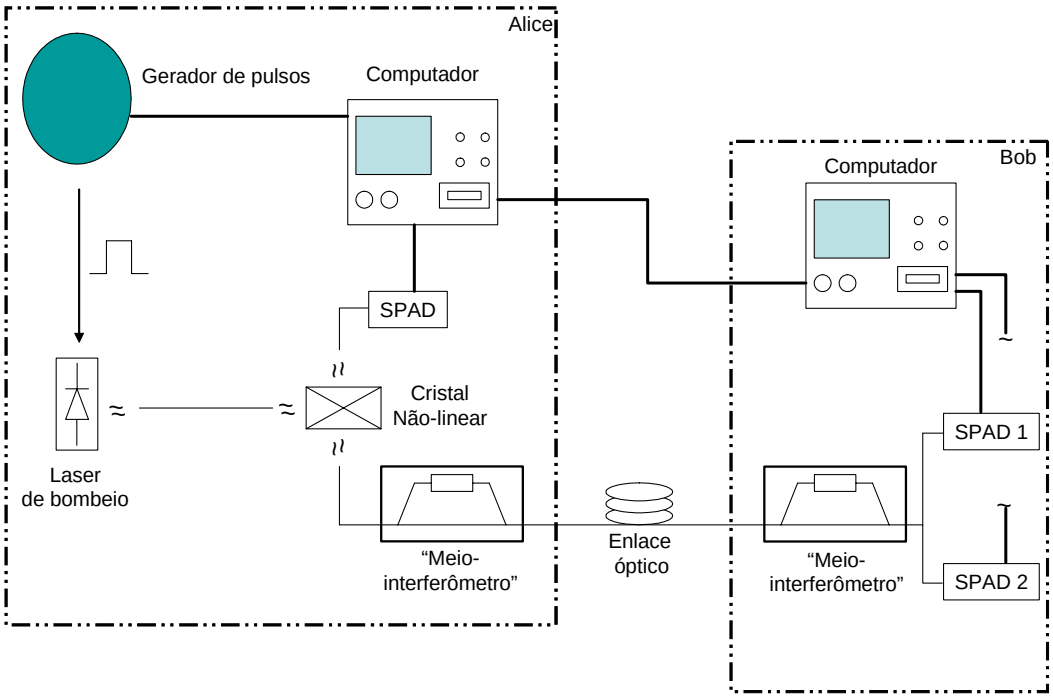

Figura 11: Esquema de transmissão de qubits utilizando um cristal não-linear para a geração de fótons. O SPAD pertencente à Alice serve para detectar quando um par foi gerado. O sinal dele é enviado a um computador que o processa e o envia a Bob para que ele saiba quais pulsos contém fótons. As linhas finas representam fibras ópticas enquanto as grossas, cabos elétricos. Foi utilizada a codificação de fase para essa representação, entretanto também poderia ser utilizada a por polarização.

3.2 Como detectar um fóton?

A primeira alternativa para a detecção de fótons unitários é a utilização de tubos foto-multiplicadores. No entanto eles não são muito práticos para a utilização fora do laboratório. Nos últimos anos o desenvolvimento de SPADs (fotodetectores avalanche para fótons unitários) para as janelas de transmissão em fibras ópticas (600-900nm e mais recentemente nas janelas de 1300 e 1550nm) vem abrindo muito esse campo [19].

3.2.1 Princípio de operação do APD

Independentemente do comprimento de onda de operação, a idéia é sempre a mesma. O que nos interessa nesses SPADs é o fato deles serem fotodetectores avalanche (APD). Os APDs não são nada mais do que um diodo p-i-n especificamente projetados para fornecer um ganho interno de corrente para cada fóton recebido, isto é, eles geram mais do que um portador elétron-buraco para cada fóton.

A estrutura dos APDs é formada por camadas p^+,i, p e n^+ (Figura 12). O campo elétrico intenso (aplicado reversamente) se distribui sobre as camadas i e p. Os fótons serão absorvidos na camada intrínseca, gerando pares elétron-buraco. Os portadores gerados atravessam a região intrínseca e chegam à região p onde se concentra a maior parte do campo elétrico. Eles então sofrem uma intensa aceleração e ganham energia suficiente para gerar outros pares elétron-buraco através de um fenômeno chamado de ionização de impacto. Como esses novos pares ainda estão sob a ação do campo elétrico intenso aplicado sob a região p, eles são fortemente acelerados e geram outros pares, e assim por diante. Esse fenômeno é chamado de efeito avalanche e é justamente esse efeito que permitirá que o APD seja utilizado para detectar fótons unitários.

Um parâmetro dos APDs importante para nós (e existente em qualquer diodo) é a tensão de ruptura V_B. Essa tensão ocorre quando o campo elétrico reverso sob o diodo é intenso de tal forma que os portadores ganham tanta energia, que passam a gerar outros portadores através de colisões com átomos da rede que formam o semicondutor. Esse efeito é o mesmo que ocorre normalmente num APD que foi especificamente projetado para isso. No entanto sob um campo muito intenso a avalanche gera uma corrente elétrica que pode estar acima do valor máximo tolerado pelo dispositivo. Eventualmente essa corrente irá destruir a junção através de dissipação por efeito Joule se não houver limitação externa [20].

3.2.2 O APD como SPAD

Como foi mencionado anteriormente a propriedade dos APDs que os faz tão úteis para seu uso como SPAD é justamente o efeito de avalanche. Mas como

detectar um fóton que possui energia tão pequena (quase nula) utilizando um APD? Se ele for polarizado um pouco acima da tensão de ruptura, ele ficará numa situação de equilíbrio instável durante um período curto de tempo. Qualquer instabilidade (um portador gerado termicamente ou um fóton absorvido) causará uma avalanche, gerando um pulso de corrente macroscópico que pode ser detectado.

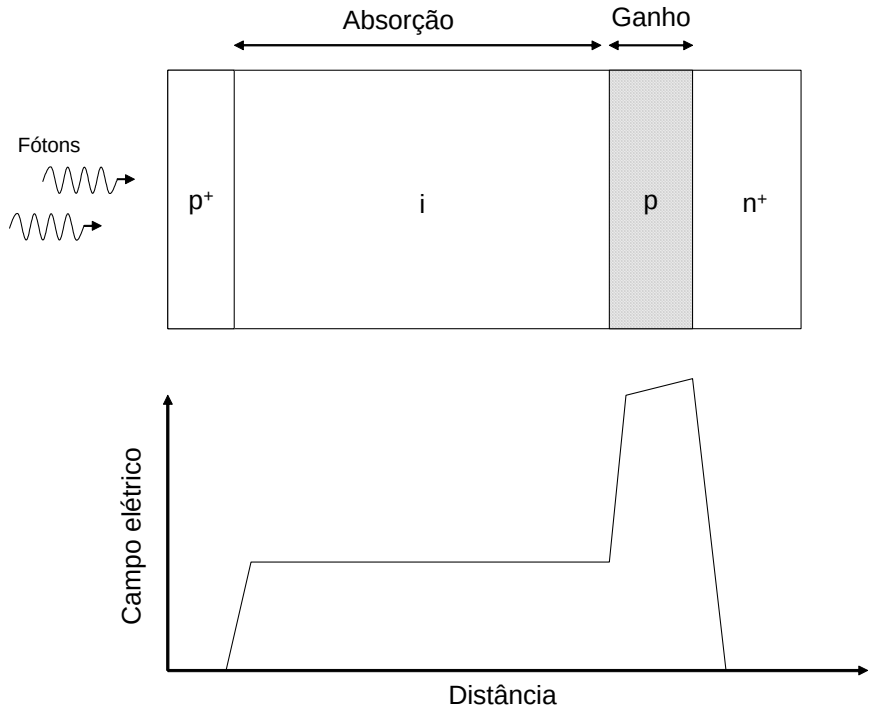

Figura 12: Esquema ilustrativo da estrutura de um APD indicando as regiões de ganho e absorção. Também encontra-se a distribuição do campo elétrico no dispositivo em função da distância.

Obviamente, se nada for feito para suprimir essa corrente o dispositivo irá ser destruído. Devemos utilizar um circuito para detectar e suprimir essa corrente. Existem três circuitos para fazer essa detecção: o circuito passivo, o circuito ativo e o circuito passivo gatilhado.

O circuito passivo é o mais simples de ser implementado (Figura 13a). O APD é colocado em série com um resistor de valor elevado da ordem de muitos kΩ (tipicamente 100 kΩ). A função desse resistor é diminuir a tensão aplicada no APD quando este entrar em avalanche. No terminal do APD, que deveria ser

conectado ao terra, inserimos um resistor de 50Ω de forma a obtermos um pulso de saída. A todo esse conjunto é aplicado reversamente a tensão de polarização reversa V_A.

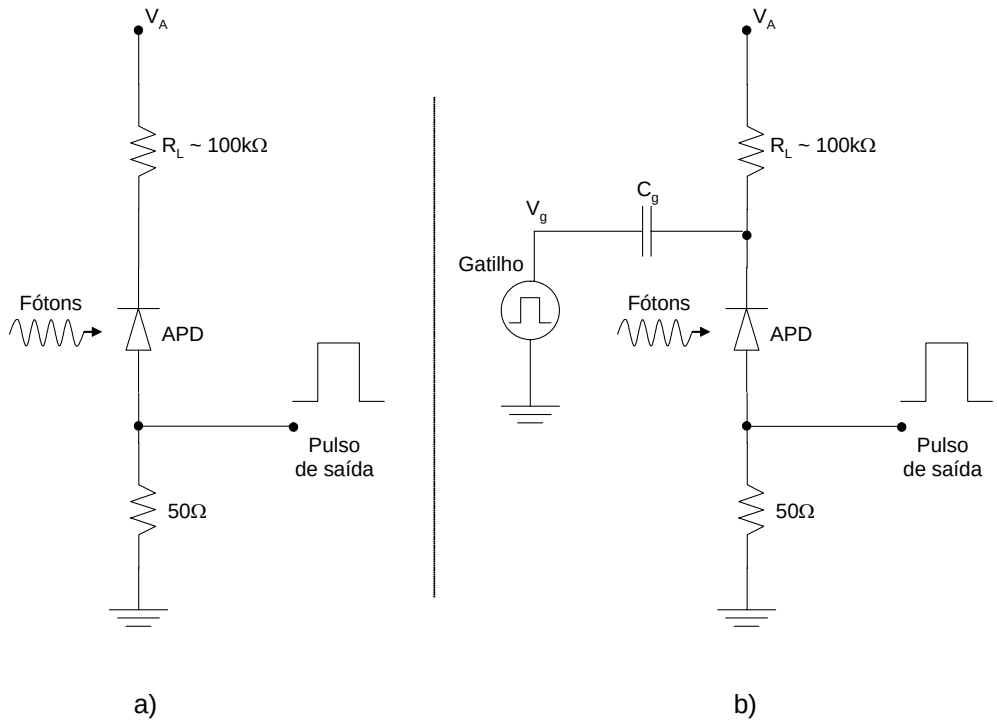

Figura 13: Á esquerda (a) está disposto o esquema passivo para detecção de pulsos gerados pelos APD. O esquema passivo gatilhado (b) é essencialmente o mesmo circuito com exceção dos pulsos (gatilhos) aplicados ao APD.

O princípio de funcionamento é o seguinte: V_A é elevado até um pouco acima do valor da tensão de ruptura V_B. Isso colocará o APD no limite de entrar em avalanche. A corrente que flui através dele é quase nula e conseqüentemente ele pode ser visto como um aberto no circuito. Dessa forma toda a tensão V_A é aplicada sobre o APD. Quando a avalanche disparar, uma corrente considerável fluirá através do APD e conseqüentemente pelo circuito, gerando um pulso de tensão sobre o resistor de 50Ω. Essa mesma corrente irá causar uma queda de tensão no resistor R_L, e conseqüentemente fará com que a tensão reversa aplicada ao APD diminua consideravelmente ficando abaixo de V_B. Nessa situação o APD encontra-se fora da região de equilíbrio instável, não ocorrendo outra avalanche e suprimindo a corrente. O APD voltará lentamente para a tensão V_A à medida que ele se recupera da avalanche, cujo tempo é característico de cada diodo.

Obviamente esse tempo de espera limita a taxa de operação do APD. Finalmente voltando à condição original ele está pronto para gerar outra avalanche.

Note que qualquer diodo p-i-n poderia ser utilizado para essa operação. Eles reagiriam exatamente da mesma forma. No entanto eles são muito ruidosos para a aplicação de detecção de fótons unitários devido justamente à falta do ganho interno que os APDs possuem.

A segunda opção é o modo ativo, situação em que possuímos uma eletrônica de alta velocidade e sensitividade que detecta quando o APD entra em avalanche e rapidamente diminui a tensão V_A abaixo do valor de V_B, para forçar o APD a se recuperar mais rápido, permitindo operações a taxas mais elevadas. O pulso gerado pela corrente de avalanche do APD é detectado por um comparador, que rapidamente chaveia a tensão V_A abaixo de V_B. Após um tempo controlado, o circuito eleva V_A para um valor $V_B + V_E$ onde V_E é o valor de tensão aplicado acima da tensão de ruptura sob o APD. A principal vantagem desse método é que ele proporciona transições rápidas entre o estado operacional do APD e o estado de relaxamento, efetivamente gerando taxas de operação mais elevadas. A desvantagem é que um circuito mais complexo é requerido.

Finalmente temos o sistema passivo gatilhado (Figura 13b). Nesse sistema (também chamado de operação no modo Geiger) a tensão V_A é mantida um pouco abaixo de V_B de forma que a probabilidade de que uma avalanche ocorra seja muito pequena. Um pulso quadrado (chamado de gatilho) de duração curta de amplitude V_g é aplicado fazendo com que a tensão reversa sob o APD seja $(V_A + V_g) > V_B$ durante o período de duração do gatilho (T_g). Isso faz com que o APD entre na região de ruptura durante T_g segundos. Se nesse momento ocorrer a absorção de um fóton ou a criação de um par elétron-buraco devido a uma emissão térmica, o APD entrará em processo de avalanche até o fim do gatilho, momento em que a tensão sob o APD passa a ser somente $V_A < V_B$, cessando a avalanche e recuperando o diodo ao seu estado normal. Se o período T_g for curto o suficiente o resistor R_L pode não ser necessário, pois o APD é retirado da região de ruptura antes que a corrente de avalanche alcance um nível que possa ser destrutivo para o dispositivo. O gatilho é mantido nessa posição (desativado) durante um tempo longo para que o APD se recupere e possa receber o próximo pulso. Na realidade para se obter um desempenho ótimo os parâmetros V_A, V_g e T_g precisam ser cuidadosamente escolhidos. Esse esquema apresenta um

desempenho muito superior ao esquema passivo. A desvantagem é que é necessário ter acesso a um gerador de pulsos com tempos de subida e descida rápidos (a ordem de grandeza de T_g para um desempenho satisfatório é da ordem de poucos ns). Outro problema é que o sistema inteiro precisa estar sincronizado, isto é, precisamos saber o tempo de chegada dos fótons para que o gatilho seja ativado.

3.2.3 Desempenho dos SPADs

Vimos acima como podemos operar os APDs para a detecção de fótons unitários. Iremos agora comentar sobre como seus parâmetros afetam a performance de um sistema de QKD.

Dependendo da região de operação em que queremos trabalhar nossa escolha do tipo de APD varia. Para comprimentos de onda mais baixos, na área de 500 - 1000 nm APDs de silício são os mais indicados. Eles ainda têm a vantagem de possuir uma eficiência quântica elevada e serem pouco ruidosos devido ao fato de já serem estudados há muitos anos [19] conseqüentemente sua estrutura já está bem otimizada. Nos comprimentos de onda mais elevados na região de 1300nm podemos utilizar APDs de germânio ou InGaAs. Finalmente na principal janela de operação de telecomunicações atualmente (1550nm) somos obrigados a utilizar InGaAs. O problema é que os APDs de Ge e InGaAs são muito inferiores em seu desempenho em relação aos de Si.

Ficamos então numa posição conflitante, pois o comprimento de onda de operação para os APDs de Si corresponde à primeira janela de transmissão das fibras ópticas (~ 850nm). Essa região possui atenuação relativamente elevada (~ 2dB/km) o que limita a distância máxima de transmissão. Se nossa intenção é ir para a segunda janela (1300nm) onde a atenuação é menor (0.5dB/km) não podemos utilizar detectores de Si pois esses APDs não respondem a esse comprimento de onda (Figura 14), então ficamos obrigados a optar por APDs de Ge ou InGaAs. Finalmente na terceira janela (1550nm) nossa única opção é InGaAs. Nessa região a atenuação é de apenas 0.25dB/km podendo aumentar a distância máxima do sistema consideravelmente. Infelizmente o ganho geral de performance que podemos obter em relação ao Si não é de um para um devido ao

elevado ruído dos detectores de InGaAs. Mas de qualquer forma as distâncias obtidas pelo uso de InGaAs ainda são maiores do que utilizando Si. APDs de silício são utilizados em duas situações: em sistemas de FSO (transmissão óptica no espaço livre) onde podemos operar em torno de 780nm, e a outra em redes locais onde a distância de transmissão não ultrapassa 10km [21]. Nessas situações é vantajoso utilizar detectores de Si devido ao seu baixo ruído, oferecendo performance superior ao InGaAs.

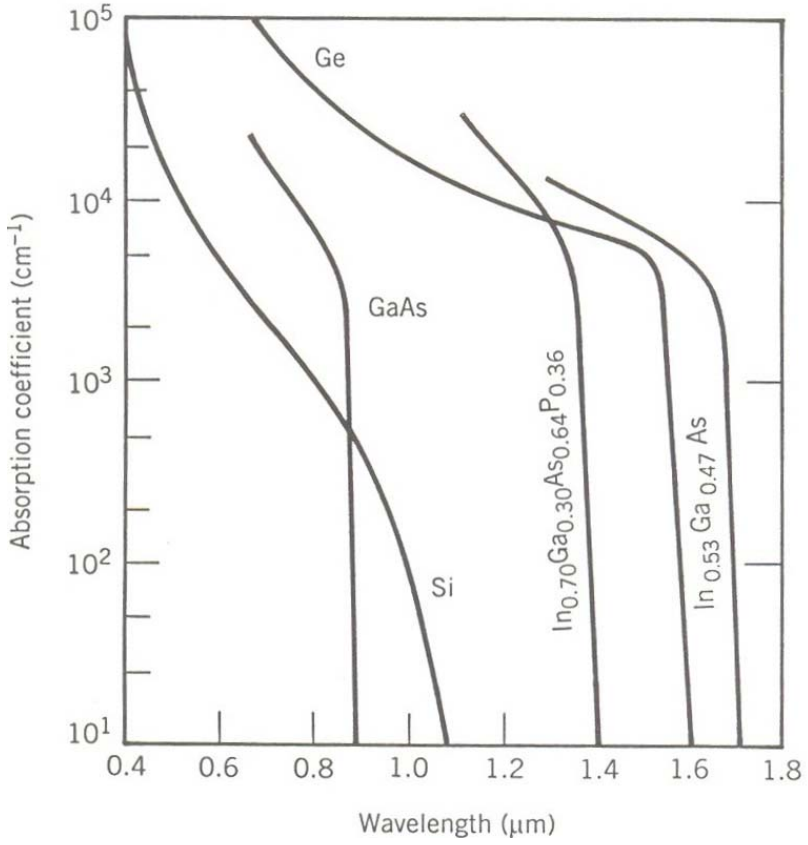

Figura 14: Gráfico dos coeficientes de absorção para diversas ligas semicondutoras em função do comprimento de onda. Retirado de [15].

Para poder ser eficaz em um sistema de QKD um APD deve possuir:

- Eficiência quântica elevada – para maximizar a probabilidade de um fóton ser absorvido e gerar um par elétron – buraco.
- Baixa contagem de escuro – dada pela probabilidade de uma corrente de avalanche ser gerada na ausência de um fóton. Será discutido mais em detalhes abaixo.

- Baixo *jitter* de tempo – o tempo de chegada de um fóton, sua absorção sucedida, a geração da corrente de avalanche e sua efetiva detecção são estatisticamente distribuídas ao redor de um valor médio. Essa incerteza é chamada de *jitter* de tempo, e apesar de não ser crítico existem limites nesse valor [22].

Dentro da eficiência quântica, estão incluídos parâmetros intrínsecos ao material, bem como o acoplamento óptico entre a fibra e o APD. Através de variações em parâmetros como a tensão V_A, podemos obter um aumento na eficiência quântica, pagando o preço de um aumento no ruído [19].

A contagem de escuro, que é dada por contagens detectadas na ausência de luz, tem sua origem em duas fontes. A primeira é gerada por portadores térmicos, ou seja, portadores gerados pela excitação térmica. Claramente então, a contagem de escuro é um parâmetro dependente da temperatura. A segunda fonte são os chamados *afterpulses* que são gerados a partir de armadilhas (defeitos presentes na rede). Quando ocorre uma avalanche, portadores ficam presos nessas armadilhas e se soltam aos poucos sob a ação do campo elétrico atuante. Se o APD voltar a ficar dentro da região de ruptura seja qual for o método de operação utilizado, os portadores eventualmente ainda presos em armadilhas poderão gerar avalanches que podem gerar contagens falsas. Os *afterpulses* são o principal limitador da taxa de operação dos APDs, além de atuarem como um limite inferior da temperatura de operação dos dispositivos. Se olharmos somente as contagens de escuro geradas por portadores térmicos, poderíamos ingenuamente acreditar que quanto menor a temperatura, menor as contagens de escuro. Isso seria verdadeiro se as contagens de escuro dependessem somente das emissões térmicas. No entanto se abaixarmos muito a temperatura os *afterpulses* passam a ser dominantes e sua probabilidade de causarem uma avalanche aumenta à medida que o APD é resfriado. A taxa máxima de operação de um APD no modo passivo gatilhado é da ordem de 1 MHz. O ponto ótimo de operação para InGaAs é em torno de -58^0C [19] permitindo o uso de refrigeradores *Peltier*, muito mais práticos do que soluções como nitrogênio líquido. Uma grande desvantagem do InGaAs em relação ao Ge na região de 1300nm é que ele requer resfriamento através de nitrogênio líquido para operar no ponto ótimo.

Medidas recentes [23] mostram que no modo passivo de operação os detectores de Ge possuem em média três ordens de grandeza, menor probabilidade

de disparar uma contagem falsa do que os de InGaAs. De fato os APDs de InGaAs apresentam uma probabilidade tão elevada de disparar uma contagem falsa sob modo passivo que seu uso é proibitivo para QKD nesse modo. Em modo passivo gatilhado a situação se inverte. O Ge é um pouco pior do que o InGaAs que por sua vez possui duas ordens de grandeza em média menor probabilidade de disparar uma contagem falsa do que o Ge sob modo passivo.

Um comentário final sob o desempenho dos SPADs: Atualmente eles são o maior limitador dos sistemas de QKD. Com eficiências quânticas da ordem de 10% para o InGaAs operando como SPAD (nos melhores casos) esses dispositivos limitam a taxa de transmissão bem como a distância máxima de transmissão. O limite da distância será discutido mais profundamente na seção sobre possíveis ataques que Eva pode realizar. A razão de um valor tão baixo para a eficiência quântica, é que os APDs de InGaAs não foram projetados para uso como SPAD, contrário aos dispositivos de Si, que possuem eficiências quânticas em torno de 60%. Já até existem dispositivos comerciais para contar fótons baseados em APDs de Si [19], infelizmente seu uso em QKD em fibras esbarra no problema da janela de transmissão. Daqui em diante assumiremos detectores de InGaAs operando sob modo passivo gatilhado.

3.3 QBER

No fim das contas o que nos interessa em um sistema de QKD é a taxa de bits que irão formar a chave secreta (R_{dist}), ou seja, os bits "úteis" depois de todo o processo de reconciliação e a distância máxima de transmissão. O valor R_{dist} não é fácil de ser estimado pois ele depende da estratégia de ataque que Eva pode tomar. Mas de qualquer forma é importante conhecer o valor de QBER do sistema (o análogo para *qubits* da clássica BER) pois, como sabemos, se Eva optar por interceptar todos os *qubits* num sistema operando com BB84, medi-los e reenviá-los ela criará uma taxa de erro de 25%. Obviamente então, qualquer sistema de QKD que se preze tem que apresentar uma QBER consideravelmente abaixo desse valor na ausência de Eva.

Um fato que já deve estar ficando claro, é que as taxas oferecidas por um sistema de QKD estão muito aquém dos valores de gigabits/s oferecidos pelos

modernos sistemas de comunicações ópticas. O primeiro teto encontra-se no detector que não consegue responder a nada muito maior do que 1 MHz. Se isto já não bastasse, metade dos *qubits* são descartados (tanto no BB84 como no B92) para garantir a segurança do sistema. Há ainda baixíssimas eficiências quânticas, bem como perdas ao longo da fibra. E para terminar esse cenário , em média somente um cada dez pulsos contêm fótons. O resultado final é que os sistemas operam com R_{dist} da ordem de poucos kilobits.

Como a BER, a QBER é definida como a razão de *qubits* errados pelo número total de *qubits* enviados podendo ser expressa em termos de taxas [3]:

$$QBER = \frac{N_{errado}}{N_{certo} + N_{errado}} = \frac{R_{erro}}{R_{sift} + R_{erro}} \approx \frac{R_{erro}}{R_{sift}} . \tag{3.3}$$

A taxa R_{sift} (*sifted rate)* corresponde aos *qubits* medidos por Alice e Bob utilizando a mesma base. Essa taxa é metade da taxa bruta (R_{raw}) que corresponde a todos os *qubits* recebidos por Bob. Já a taxa bruta é essencialmente o produto da freqüência de geração de pulsos no laser f_{rep} (que é a mesma freqüência que será utilizada para gatilhar o detector), pelo número médio de fótons por pulso μ, pela probabilidade t_{link} de um fóton chegar a Bob e finalmente pela probabilidade η do fóton ser detectado. Temos então:

$$R_{sift} = \frac{1}{2} R_{raw} = \frac{1}{2} f_{rep} t_{link} \mu\eta . \tag{3.4}$$

Existem três contribuições possíveis para a taxa de erro R_{erro}. A primeira é devida à fótons que são desviados para o detector errado devido a uma interferência imperfeita, por exemplo. Essa taxa, chamada de R_{opt} é dada pelo produto da *sifted rate* pela probabilidade p_{opt} de um fóton ir para o detector errado:

$$R_{opt} = R_{sift} p_{opt} = \frac{1}{2} f_{rep} t_{link} \mu\eta \cdot p_{opt} . \tag{3.5}$$

A segunda contribuição é dada pelas contagens de escuro geradas pelo detector. Somente contagens de escuro geradas durante a janela de tempo curta em que a chegada de um fóton é esperada são considerados:

$$R_{\text{det}} = \frac{1}{2}\frac{1}{2} f_{rep} p_{dark} n \,. \tag{3.6}$$

R_{det} é a taxa de bits errados, devido às contagens de escuro, p_{dark} é a probabilidade de obtermos uma contagem de escuro por janela de tempo por detector e n o número de detectores. Os dois fatores 1/2 são devido ao fato de que uma contagem de escuro tem 50% de probabilidade de ocorrer quando Alice e Bob escolherem bases diferentes (sendo eliminado durante a reconciliação) e 50% de probabilidade de ocorrer no detector correto.

A contribuição final, chamada de R_{acc} não será considerada aqui, visto que só se aplica a sistemas utilizando partículas emaranhadas. Ela ocorre quando pares diferentes em estados diferentes chegam juntos na mesma janela de tempo.

A QBER pode ser expressa da seguinte forma:

$$QBER = \frac{R_{opt} + R_{\text{det}}}{R_{sift}} = p_{opt} + \frac{p_{dark} n}{t_{link} \eta 2\mu} = QBER_{opt} + QBER_{\text{det}} \,. \tag{3.7}$$

Olhando as duas contribuições que nos restaram e analisando-as, pode-se afirmar que $QBER_{opt}$ é independente da taxa de transmissão, dependendo somente do contraste das franjas de interferência (se o sistema utilizado for codificação de fase) ou do contraste de polarização. Efetivamente esse parâmetro é uma medida da qualidade óptica do sistema. Manter a sua estabilidade (não permitir que a polarização flutue com o tempo, por exemplo) é um parâmetro crucial para determinar a qualidade do sistema de QKD. Em sistemas de polarização é relativamente simples manter um contraste de 100:1, o que equivale a ,uma $QBER_{opt}$ de 1%, no entanto é necessário mantê-la estável ao longo do tempo, um problema não trivial em sistemas baseados em fibras ópticas. Em sistemas de codificação por fase, $QBER_{opt}$ e a visibilidade das franjas V estão relacionados por [3]:

$$QBER_{opt} = \frac{1-V}{2} \tag{3.8}$$

Por exemplo, para uma visibilidade de 98% temos uma $QBER_{opt}$ de 1%. Novamente é necessário que V fique estável ao longo do tempo. Uma possível solução para esse problema é o sistema "*Plug and Play*" apresentado no capítulo anterior.

A segunda contribuição, $QBER_{det}$, aumenta com a distância, dado que a contagem de escuro se mantém constante e a taxa de bits decresce com a distância (t_{link}, a probabilidade de um fóton chegar a Bob decai à medida que a distância de transmissão aumenta). A quantidade $QBER_{det}$ fica então dependente da taxa de contagem de escuro para uma mesma distância. Como $QBER_{opt}$ é essencialmente independente do comprimento do enlace, o ruído do detector é o que limita a distância de transmissão de um sistema de QKD. Por essa razão, à medida que a demanda aumentar, novos detectores de InGaAs mais eficientes devem vir a ser desenvolvidos, permitindo um grande avanço na performance dos sistemas de QKD.

3.4 Ataques

O problema de se tratar matematicamente os ataques realizados por Eva, de uma forma geral é extremamente complicado. Normalmente algumas premissas são tomadas para se realizar a análise. É rapidamente entendido que se os sistemas físicos utilizados são desprovidos de falhas, o sistema é absolutamente seguro, dado que ele é baseado nas leis da mecânica quântica, que foi e vem sendo testada extensivamente até o presente momento e ainda não apresentou falhas.

Para o caso de sistemas reais, que possuem falhas, a situação não é tão simples e a prova de segurança é extremamente complexa. A idéia desta seção é apenas fornecer ao leitor uma breve noção do estudo dos possíveis ataques a sistemas de QKD.

Apesar de poder parecer absurdo, em alguns casos será assumido que Eva tem acesso à tecnologia ainda inexistente, sendo na verdade somente limitada

pelas leis da mecânica quântica. Existem dois tipos principais de ataques, os incoerentes ou individuais e os coerentes.

Os ataques incoerentes podem ser realizados com a tecnologia atual, isto é Eva utiliza os mesmos equipamentos que Alice e Bob. Para os ataques coerentes e PNS é necessário que Eva tenha acesso a um computador quântico e memória quântica.

3.4.1 Ataques incoerentes

São os ataques mais simples e a idéia é que Eva intercepte os fótons individualmente, meça-os numa base escolhida aleatoriamente entre as duas preparadas por Alice e retransmita os fótons para Bob de acordo com o resultado obtido por ela (Figura 5). Nesse caso mais simples e assumindo BB84, ela obtém 0.5 bit de informação para cada bit na *sifted key* e infere uma QBER de 25% [3]. Pulsos contendo mais de um fóton não estão incluídos nessa primeira análise. Na realidade para uma QBER próxima de 25% conseguimos detectar a presença de Eva, mas será possível tornar a chave segura utilizando os procedimentos clássicos de correção de erro e amplificação da privacidade? A resposta é não. Para que isso seja possível a QBER na verdade tem que ser menor do que aproximadamente 15% [3]. Caso isso não ocorra, eles sabem que Eva está presente mas não podem utilizar a chave pois não conseguirão torná-la segura. Nesse caso eles possuem três opções em teoria: tentam uma nova transmissão (em princípio eles não sabem se a QBER elevada é devido a Eva ou alguma perda no sistema devido a efeitos adversos), tentam outro canal ou recorrem a algoritmos quânticos para amplificação da privacidade e correção de erro, requerendo um computador quântico, indisponível num futuro próximo.

Uma falha de segurança grave corresponde à existência de pulsos contendo multi-fótons abrindo caminho para ataques PNS. Nesse tipo de ataque Eva mede todos os pulsos que Alice envia pelo canal quântico. Todos os pulsos que contêm um fóton são bloqueados por Eva. Para os pulsos contendo dois fótons ou mais ela guarda um para si enquanto envia o outro para Bob sem nenhuma perturbação. Note que Bob não tem como saber quantos fótons o pulso continha na saída de Alice. É verdade que Bob pode notar uma diminuição na taxa R_{raw} de *qubits* que

ele recebe, afinal todos os bits que contêm 1 fóton (em geral a maioria) está sendo bloqueada por Eva. Para evitar isso, ela tem que substituir o canal que a liga a Bob por um mais transparente, ou seja, com menos perdas. Felizmente para nós Eva está com um grande problema nas mãos. Como diminuir as perdas do canal se as atuais fibras ópticas já estão próximas do limite mínimo para atenuação dada pelo espalhamento Rayleigh? A primeira saída seria Eva utilizar um canal mais curto, só que é bem possível que Alice e Bob já estejam utilizando o canal mais curto possível. A outra saída é teleportação, pois com isso as perdas do canal passariam a zero (assumindo teleportação perfeita), já que o *qubit* seria transportado através de um canal clássico. Assumindo então que Eva conseguiu a façanha de adquirir um canal mais transparente, Bob não irá detectar a sua presença. Assumindo BB84 e caso ela tenha acesso a um meio de guardar os *qubits* indefinidamente (salvar os *qubits* em uma memória quântica ou utilizar um *loop* de fibra sem perdas), ela pode simplesmente esperar a reconciliação de bases para assim realizar as medidas em seus *qubits* de forma determinística (Figura 15).

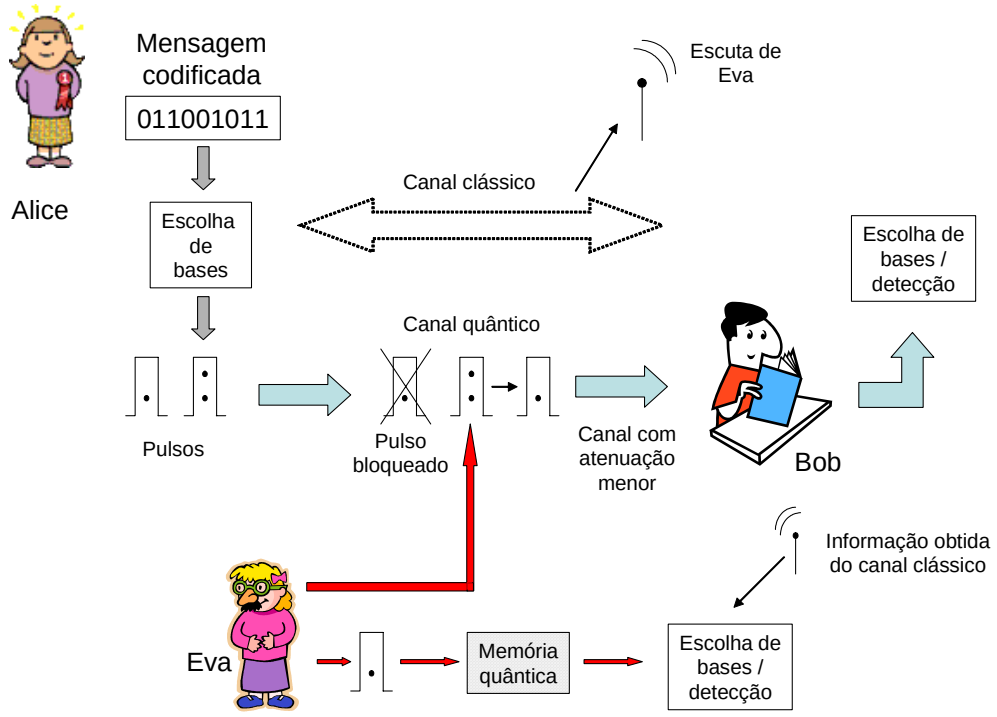

Figura 15: Ataque PNS realizado por Eva em um sistema de QKD. O sistema pode ser codificado por fase ou polarização.

Devido aos ataques PNS, é muito importante para a segurança dos sistemas de QKD que o valor médio μ de fótons por pulso seja menor do que 1 (ao se utilizar fontes poissonianas). Quanto menor for μ, mais pulsos Eva será obrigada a bloquear e conseqüentemente, mais difícil será mascarar a sua presença.

3.4.2 Ataques coerentes

Esse tipo de ataque é subdividido em dois tipos: ataques conjuntos (*joint attacks*), em que Eva mede e processa vários *qubits* de forma coerente simultaneamente; nos ataques coletivos (Figura 16) (*collective attacks*), Eva acopla sondas (*probes*) em *qubits* individuais como nos ataques incoerentes, mas processa todas essas sondas de forma simultânea como nos ataques coerentes.

Para ambos os ataques coerentes o procedimento é usualmente o mesmo: Eva espera que o processo de reconciliação termine para medir as sondas cuidadosamente armazenadas em uma memória quântica. Os ataques coerentes também introduzem erros no sistema. No entanto, o limite de *QBER* para que ainda seja possível realizar correção de erro e amplificação da privacidade clássicos cai para 11% [3].

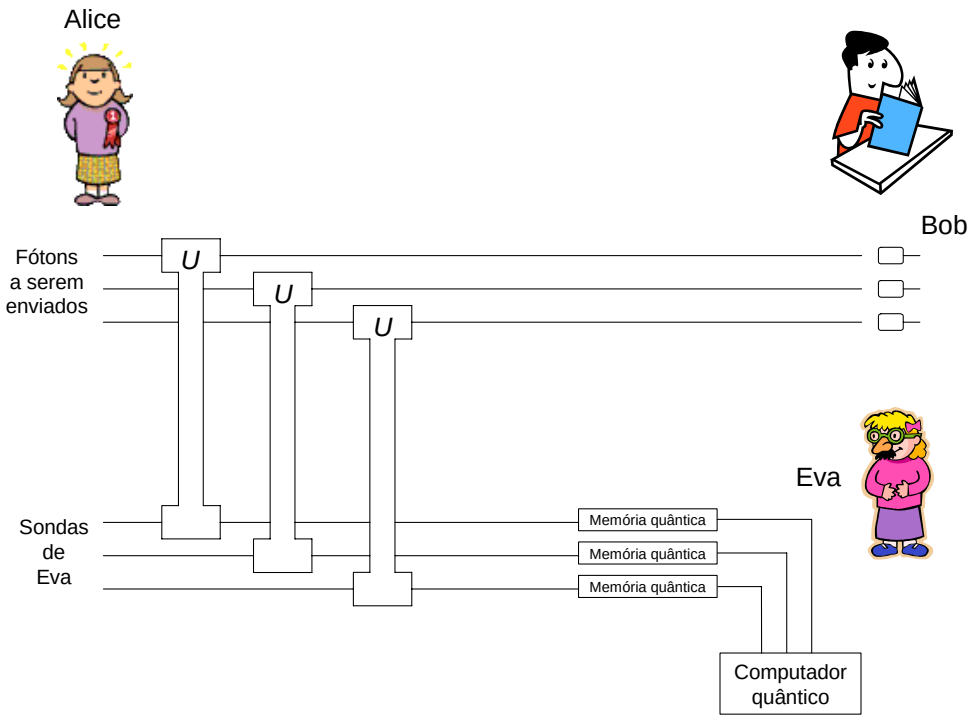

Figura 16: Esquema de ataque coletivo praticado por Eva. No ataque conjunto Eva utiliza uma sonda de dimensão *n* aonde *n* é o número de *qubits* transmitido e processa todas as sondas simultaneamente num computador quântico após a reconciliação de bases.