4.
Elementos de QKD

Neste capítulo serão apresentados os principais elementos que compõem um sistema de distribuição quântica de chaves. Inicialmente será dissertado a respeito da geração dos qubits, tecendo-se comentários sobre as principais fontes capazes de gerar fótons no regime apropriado. Em seguida será abordado o detector de fótons únicos, suas características e modos de operação. Os principais esquemas de codificação serão apresentados, destacando-se o sistema de codificação em freqüência por dupla-modulação, assunto essencial para a implementação física do sistema que será apresentado, seguidos por considerações sobre o canal.

4.1.
Geração de qubits

Para que haja confidenciabilidade na distribuição quântica de chaves garantida pelas leis da mecânica quântica, deve-se, obviamente, operar o sistema em regime quântico. Isso significa que, de alguma forma, é necessário que se codifiquem e se transmitam fótons únicos, ou mesmo pulsos com uma distribuição estatística tal que não possuam, em sua maioria, mais de um fóton.

Atualmente, há três principais formas de se obter este tipo de fonte, sendo uma especializada e desenvolvida para tal, a própria fonte de fótons únicos, construída a partir de material semicondutor; a forma mais difundida e de menor custo, os pulsos ópticos coerentes fracos, obtidos com uma fonte laser altamente atenuada; e a conversão paramétrica descendente (PDC – *Parametric downconversion*), capaz de produzir fótons emaranhados, obtida com o bombeio óptico de um cristal não-linear.

4.1.1.
Fontes de fótons únicos com pontos quânticos

Fontes de fótons unitários sob demanda vêm sendo pesquisadas, podendo-se destacar as construídas a partir de pontos quânticos. Tais fontes constituem-se basicamente de um ponto quântico crescido no interior de uma estrutura semicondutora *bulk* e cercado por uma microcavidade óptica [6].

Após ser excitado por um pulso óptico curto, de poucos picossegundos, pares elétron-buraco são gerados. Se o sistema for excitado na freqüência de ressonância, a recombinação radiativa do par elétron buraco gerado dará origem a um fóton com comprimento de onda específico.

Com o crescimento de microcavidades dimensionadas e dispostas em torno dos pontos quânticos, é possível tornar a emissão direcional, permitindo o aumento do fator de acoplamento com dispositivos externos, como a fibra-óptica. Há relatos de fonte de fótons únicos com pontos quânticos com taxa de 76MHz, resfriados a temperaturas abaixo de 40K, com potencial para ultrapassar 10GHz [14].

Entretanto, o crescimento de pontos quânticos individuais de forma controlada continua sendo de difícil realização, além de tais fontes continuarem limitadas no que tange sua aplicação comercial, especialmente por sua baixa temperatura de operação, na ordem de poucas dezenas de Kelvin.

4.1.2.
Laser altamente atenuado

De fácil implementação e baixo custo, a utilização de pulsos ópticos coerentes fracos se mostra uma opção amplamente difundida para a geração de qubits nos atuais sistemas de criptografia quântica. Sua facilidade de implementação torna-a especialmente atraente, pois necessita apenas de uma fonte óptica coerente (laser) e um atenuador calibrado. A probabilidade de distribuição de fótons em um pulso óptico é um processo estocástico representado pela distribuição de Poisson [6]. A eq. 4.1 representa a probabilidade de se encontrar *n* fótons em um pulso contendo um número médio de μ fótons.

$$P(n,\mu) = \frac{\mu^n e^{-\mu}}{n!} \tag{4.1}$$

Na eq. 4.1, pode-se verificar que o aumento do número médio de fótons faz com que a probabilidade de se encontrar mais de um fóton por pulso também aumente, conforme pode ser observado na figura 2.

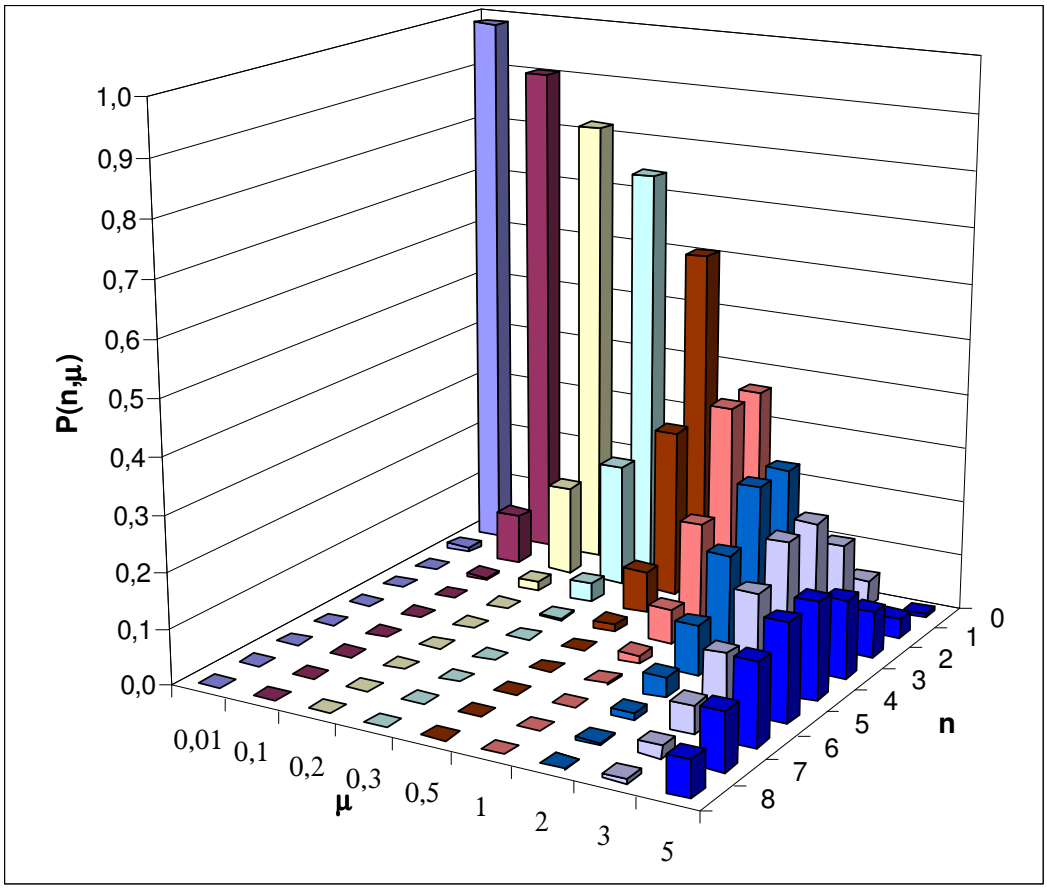

Figura 2: Probabilidade P(n,μ) de se encontrar *n* fótons em pulsos contendo μ fótons em média, conforme a distribuição de Poisson da eq. 4.1.

Dado o número médio μ, pode-se calcular a probabilidade de um pulso não conter fótons fazendo-se n=0, e comparar com a probabilidade de um pulso conter fótons, ou seja, P(n>0,μ)=1-P(n=0,μ), como pode ser visto na figura 3. As barras azuis representam a probabilidade de pulsos vazios, enquanto que a barras amarelo-claro representam a probabilidade de pulsos contendo fótons em qualquer quantidade, para diversos valores de μ.

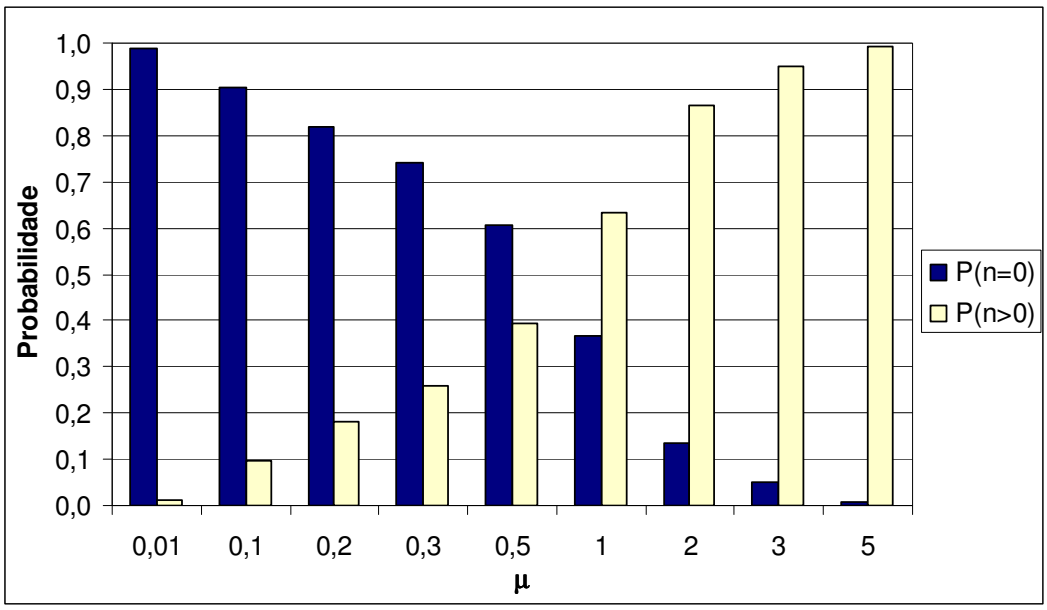

Figura 3: Probabilidade de pulsos vazios (barras azuis) e não-vazios (barras amarelo-claro) para diversos valores de μ.

Além disso, é de interesse calcular a probabilidade de um pulso cheio conter mais de um fóton. Isso pode ser obtido subtraindo-se da totalidade os pulsos contendo zero fóton e os pulsos contendo um fóton, e dividindo-se pela quantidade de pulsos não-vazios, ou seja, os pulsos vazios subtraídos da totalidade, como na eq. 4.2.

$$P(n>1 \mid n>0) = \frac{1 - P(0,\mu) - P(1,\mu)}{1 - P(0,\mu)} \tag{4.2}$$

Os resultados dessas distribuições em função de μ podem ser vistos na figura 4, em que as barras vermelhas representam a fração de pulsos cheios que contém apenas um fótons, enquanto que as barras verde-claro representam a fração complementar, ou seja, os pulsos cheios que contém mais de um fóton.

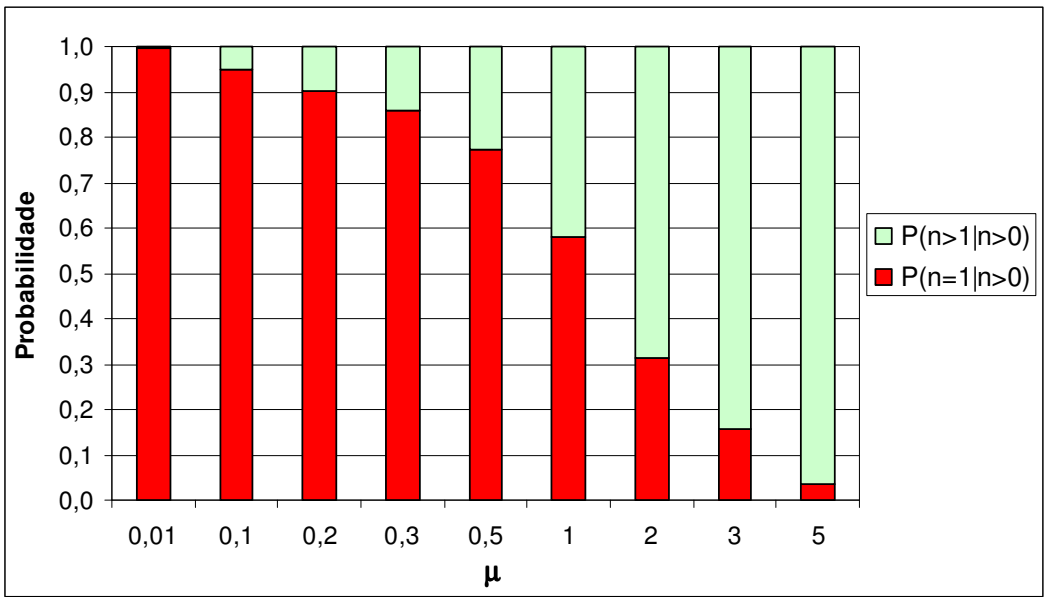

Figura 4: Probabilidade de pulsos não-vazios conterem apenas um (barras vermelhas) ou mais fótons (barras verde-claro).

Os pulsos ópticos devem ser atenuados de forma que se obtenha um compromisso entre reduzir o número de pulsos vazios e reduzir a quantidade de pulsos com múltiplos fótons. O número de fótons (em média) de cada pulso pode ser obtido a partir da medição da potência óptica (P_{opt}), dividindo-se este valor pela energia de um fóton na freqüência de operação, dada pela freqüência óptica (ν) multiplicada pela constante de Planck (h), e multiplicado-o pela janela de tempo de gatilho do pulso (Δt), como na eq. 4.3.

$$\mu = \frac{P_{opt}\,\Delta t}{h\upsilon} \tag{4.3}$$

Um número médio de fótons igual a 0,5 resulta em uma redução de aproximadamente 60% na taxa de transmissão da chave bruta (*raw key*, ou seja, a transmissão física, antes da reconciliação), pois mais da metade dos pulsos serão vazios, enquanto que, com μ=0,2, tem-se a probabilidade de que menos de 20% dos pulsos contenha fótons.

Entretanto, num dado sistema pode ser crucial que a probabilidade de o número de fótons não exceder a unidade seja baixa. Nos casos citados, apesar de haver mais pulsos cheios com μ igual a 0,5, mais de 20% deles não são

unitários, enquanto que este valor se reduz para menos de 10% no caso de 0,2 fótons por pulso.

Em implementações experimentais, é comum o relato da utilização de 0,1 ou 0,2 fótons por pulso em média. Cabe ressaltar que a escolha adequada deste valor, que otimizará o compartilhamento da chave após a destilação, depende de fatores como o protocolo utilizado, a perda óptica do canal e a tecnologia considerada para Eva [6].

4.1.3. Conversão paramétrica descendente

Determinados materiais dielétricos, quando submetidos a campos eletromagnéticos intensos, exibem efeitos ópticos não-lineares, devido à variação da orientação de seus dipólos.

Ao se incidir um fóton de bombeio em um cristal não-linear que possua o tensor susceptibilidade de segunda ordem $\chi^{(2)}$ não-nulo, ou seja, que não tenha sua estrutura centro-simétrica, poderá ocorrer a conversão paramétrica descendente, que corresponde à criação espontânea de fótons com a interação inelástica do campo de bombeio com o material.

A interação deste fóton de bombeio com o meio, quando na condição de casamento de fase, dá origem a um par de fótons cujo emaranhamento pode ser observado com a devida separação temporal e espacial. Como a energia deve ser conservada, a soma das freqüências dos dois fótons gerados na direção dos eixos do cristal deve igualar-se à freqüência do fóton de bombeio, o mesmo valendo para os vetores de onda.

Dependendo do tipo de casamento de fase, obtém-se PDC do tipo I ou do tipo II, sendo que, no primeiro, os fótons são criados com polarizações paralelas, enquanto que, no segundo, os fótons emergem com polarizações ortogonais em relação à orientação dos eixos do cristal.

Pode-se obter também as chamadas fontes *heralded*, em que um dos fótons é detectado e o sinal elétrico é utilizado para anunciar a presença do outro [13]. Este esquema pode solucionar o problema causado pela emissão espontânea de fótons pelo cristal, tornando possível conhecer os momentos em que há fótons sendo emitidos.

4.2.
Detecção de qubits - SPAD

Para se efetuar uma transmissão quântica, é necessário ser capaz de detectar um fóton único. Para tal, é comum a utilização dos chamados *detectores de fótons únicos por avalanche* (SPAD – *Single-photon avalanche photodetector*) e um detector de fótons únicos. Tal dispositivo é obtido ao se resfriar um fotodiodo de avalanche (APD – *Avalanche photo-diode*) reversamente polarizado a uma determinada temperatura, em combinação com algum tipo de circuito de extinção de avalanche. Detectores de InGaAs/InP devem ser utilizados, caso se deseje explorar a janela de transmissão no comprimento de onda de 1550nm que, por corresponder ao mínimo de atenuação das fibras ópticas, entre outros motivos, propiciou o desenvolvimento de boa parte dos dispositivos ópticos para telecomunicações. Outros métodos são alvos de pesquisas, como o baseado em supercondutores, que apresenta *jitter* reduzido (~7 vezes menor), porém opera à temperatura de 2,9K [42].

4.2.1.
Extinção passiva, ativa e gatilhada

O APD deve ser reversamente polarizado próximo à tensão de avalanche, de forma que a incidência de um fóton possa criar um par elétron-buraco que desencadeará o processo de avalanche por ionização de impacto. O elétron primário é acelerado pelo campo elétrico e pode ter energia suficiente para criar outros pares secundários e sustentar uma corrente de avalanche em regime permanente. Para que outro fóton possa ser detectado (e o dispositivo ser preservado), a corrente deve ser extinta de alguma forma. Há três tipos básicos de circuitos de extinção de avalanche geralmente utilizados em detectores de fótons únicos.

Mais básico deles, o sistema de extinção passiva, como o próprio nome diz, deixa que a avalanche naturalmente se extinga através da queda de tensão em um resistor de valor elevado, como na fig. 5a. A corrente elétrica foto-gerada flui pelo resistor de 50Ω, gerando uma queda de tensão em cima deste. Como o resistor de carga R_L apresenta valor elevado (50-500 kΩ) [6], maior que a resistência interna do fotodiodo, a tensão sobre ele se eleva, reduzindo a polarização do APD e, conseqüentemente, extinguindo a avalanche. O tempo de

recuperação do diodo é dado por R_L e por sua resistência e capacitância interna [15], limitando a taxa de contagem a poucos MHz [6].

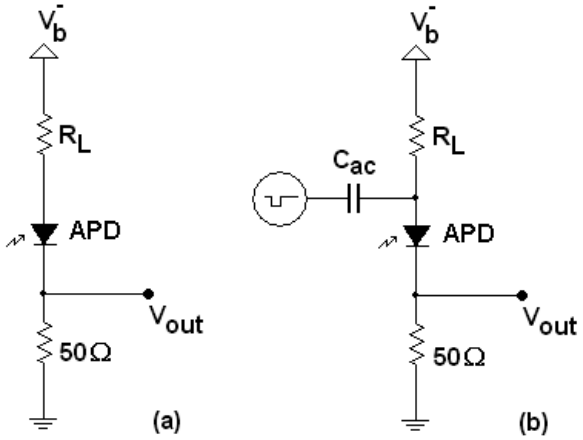

Figura 5: Circuitos de polarização do SPAD no modo passivo (a) e no modo gatilhado (b).

Já no modo de extinção ativa, assim que uma avalanche se inicia, a tensão de saída é detectada por um circuito eletrônico que realimenta o circuito de polarização, fazendo com que a tensão de polarização do APD seja reduzida a um valor abaixo da tensão de ruptura. Após um período de tempo determinado, a polarização do fotodiodo retorna a seu valor inicial, próximo da tensão de avalanche [15]. Apesar de eletronicamente mais complexo que o modo passivo, este tipo de extinção possibilita um aumento na taxa de contagem devido à redução do tempo morto entre duas possíveis avalanches, podendo alcançar poucas dezenas de MHz [6].

Finalmente, no modo Geiger, ou modo pulsado, o dispositivo tem a possibilidade de iniciar um processo de avalanche restringida a apenas os instantes do pulso elétrico de gatilho. O APD é polarizado abaixo da tensão de avalanche e são introduzidos no circuito pulsos periódicos e curtos de tensão, como na figura 5b. Nesses instantes de tempo, o pulso, de poucos nanosegundos de duração, eleva a tensão do dispositivo ao limiar de avalanche, ficando este apto a detectar a incidência de um fóton. Com o fim do pulso de gatilho, o fotodiodo volta à condição de baixa polarização até que chegue o próximo pulso elétrico. Neste caso, o resistor de carga R_L pode ter valor menor, o suficiente apenas para que a corrente do pulso de gatilho não flua para a fonte

de polarização V_b. Essa técnica, além de prover certa resolução temporal, reduz o ruído do detector [15].

4.2.2. Circuito subtrator

Todo diodo semicondutor apresenta uma capacitância interna resultante da separação de cargas na barreira de potencial da camada de depleção formada na região de contato entre os semicondutores com diferentes dopagens [16]. Quando um SPAD opera no modo Geiger, esta capacitância, geralmente em torno de 1pF deriva os pulsos de gatilho, gerando um sinal espúrio nas transições de subida e de descida do pulso, que podem dificultar a detecção ou mesmo mascarar a contagem de fótons.

Para contornar este problema, usualmente se utiliza um circuito subtrator que compensa esta capacitância [15,17,18]. O pulso de gatilho é entregue ao circuito através de uma capacitância de acoplamento (C_{ac}) e dividido, sendo que parte dele chega ao fotodiodo APD, tornando-o propício a deflagrar uma avalanche caso receba um fóton, e parte segue para um estube, capacitor ou diodo com capacitância equivalente ao do fotodiodo (C_d), como na figura 6. As duas tensões são então subtraídas pelo amplificador operacional (AO), cancelando-se os componente iguais, ou seja, os espúrios da derivada. Obtém-se, assim, à saída do SPAD, o pulso de avalanche “limpo”.

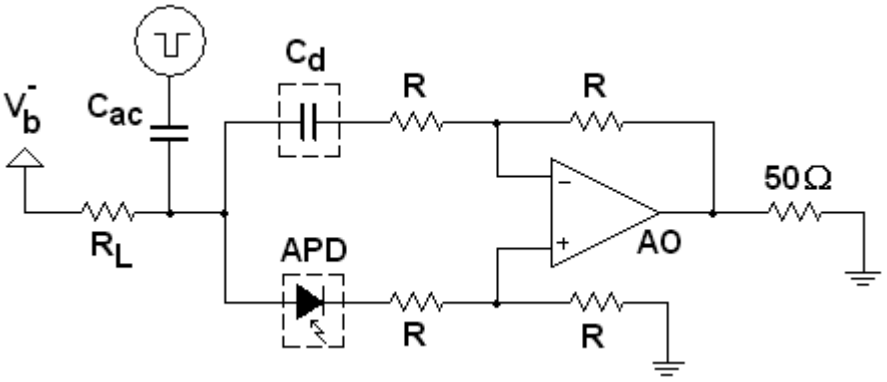

Figura 6: Circuito de compensação de capacitância para operação do SPAD no modo Geiger.

Apesar de as taxas de transmissão de qubits serem baixas, se comparadas às de comunicações ópticas clássicas, de poucos MHz, contra dezenas de GHz, o pulso de gatilho deve ser quadrado. Isso significa que o tempo de subida será da ordem de nanosegundo, resultando em uma freqüência máxima do sinal na ordem dos GHz. Deve-se, portanto, tomar as devidas precauções no tocante ao circuito em questão. As trilhas devem ser consideradas como guias de onda e ter sua impedância e comprimento devidamente calculados, assim como os cabos que o conectam ao fotodiodo, já que este deve ser resfriado e, possivelmente, não terá sua montagem diretamente na placa. Pode ser interessante providenciar o casamento de impedâncias na conexão entre a linha de transmissão e os terminais do APD, com um capacitor e um resistor de 50Ω no lado da tensão de polarização e um resistor idêntico no outro terminal. Os componentes devem ser próprios para alta freqüência, como os de montagem em superfície (SMD – *Surface-mounted devices*), incluindo o amplificador operacional.

Atenção especial deve ser dispensada ao acoplamento da fonte de polarização e da fonte de pulsos ao circuito. O capacitor de acoplamento (C_{ac}) deve ter capacitância tal que impeça a fuga de corrente da fonte de polarização para a fonte de pulsos, assim como o resistor R_L deve impedir que os pulsos desviem-se do fotodiodo, indo para fonte de polarização. Este resistor pode ser convenientemente substituído por um indutor, que atuará como elemento de baixa impedância para o sinal contínuo e de alta impedância para o sinal alternado.

4.2.3. Características relevantes

Deve-se atentar para o ajuste correto dos parâmetros do SPAD, de acordo com as características do sistema implementado, ressaltando-se a temperatura, a tensão de excesso do pulso de gatilho, a tensão de polarização, a taxa de repetição de gatilho e sua largura temporal.

Característica fundamental dos fotodiodos utilizados em detectores de fótons únicos, a eficiência quântica (η) se refere ao acoplamento da luz no dispositivo e à probabilidade de um fóton ser internamente absorvido, gerando um par elétron-buraco, associada à probabilidade desses portadores desencadearem uma avalanche [15]. Esse parâmetro é fortemente influenciado

pela tensão de polarização do APD e pela tensão de excesso, no caso gatilhado, de modo que, aumento esse valor, a eficiência também aumenta, assim como o ruído [18].

Seja qual for o modo de operação escolhido, o fotodiodo de avalanche deve ser resfriado, devido à sua alta sensibilidade à geração térmica. Os portadores térmicos podem vir a desencadear o processo de avalanche e, conseqüentemente, acusar uma contagem errônea pela ausência de fótons, caracterizando o ruído de escuro. Entretanto, faz-se necessário um compromisso entre ruído de escuro e temperatura, pois, ao reduzir-se esta, aumenta a possibilidade de ocorrência dos assim chamados *afterpulses*, ou pós-pulsos.

Estes pós-pulsos resultam de pares elétron-buraco que ficaram presos durante o processo de avalanche e não conseguiram ser removidos pelo campo elétrico do dispositivo em tempo. Ao liberarem-se tardiamente, acabam desencadeando uma avalanche em momento inoportuno. O modo de operação Geiger suaviza este problema, crítico no modo de extinção passivo, pois, com o fim do pulso de gatilho, a tensão de polarização cai a um valor que impossibilita uma nova avalanche até a chegada de um novo pulso elétrico. Este efeito limita o intervalo entre os pulsos – tempo morto – e, conseqüentemente, a taxa de transmissão de qubits, já que influencia fortemente na contagem de escuro [17,18].

Como figura de mérito para comparações entre detectores de fótons únicos, pode-se utilizar a potência de ruído equivalente (NEP – *Noise equivalent power*) em [$WHz^{-1/2}$], dada pela eq. 4.4, definida como a potência óptica necessária para que seja medida uma relação sinal-ruído unitária [6], onde a variável R representa a taxa de contagens de escuro.

$$NEP = \frac{h\upsilon}{\eta}\sqrt{2R} \tag{4.4}$$

Entretanto, tal parâmetro não se mostra prático, pois não faz muito sentido falar de banda passante de um fóton. Na prática, pode-se utilizar a relação entre o sinal e o ruído de escuro (SNR_0), dada pela eq. 4.5.

$$SNR_0 = \frac{h\upsilon R}{\eta} \tag{4.5}$$

Quando devidamente resfriados e com o nível de tensão de gatilho adequado, tipicamente em 4V para tensão de avalanche de 41,5V, tais detectores apresentam contagem de escuro típica entre $0,2–2\times10^{-4}$ contagens por janela de 5ns [17]. Os detectores de InGaAs/InP apresentam eficiência quântica entre 8 e 13%, valor baixo se comparado com os detectores de silício. Na figura 7 vê-se uma curva típica que ilustra a relação entre temperatura e NEP para um fotodiodo daquele tipo operando nas condições citadas acima [17]. Observa-se que a temperatura ótima se encontra próxima de -60ºC, resultando em uma potência de equivalente de ruído da ordem de $2,5\times10^{-16}W/Hz^{½}$.

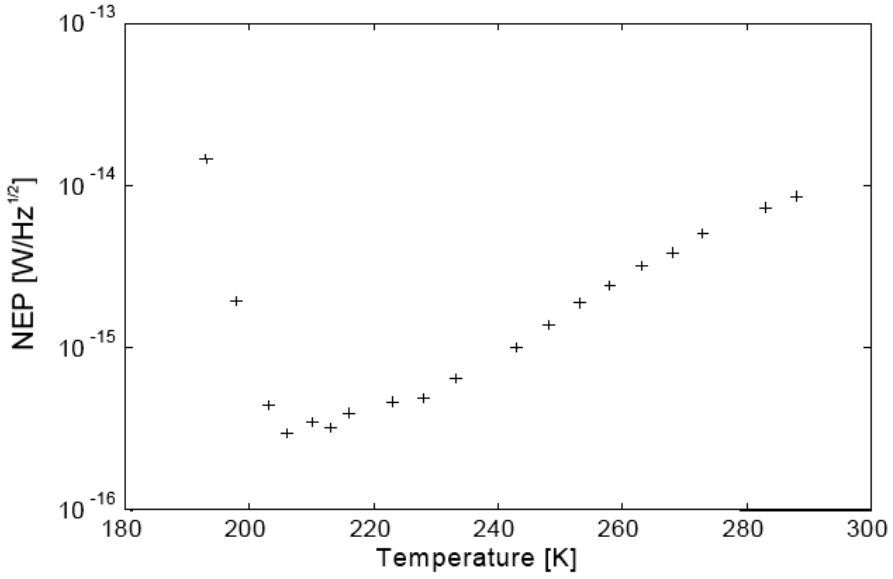

Figura 7: Potência efetiva de ruído (NEP) em função da temperatura para um fotodiodo de InGaAs/InP operando em modo Geiger [17].

A eficiência quântica dos detectores de silício é elevada apenas em comprimentos de onda abaixo de 1,1μm, podendo exceder 70%, enquanto apresentam responsividade desprezível no comprimento de onda de 1550nm, sendo utilizados especialmente em enlaces em espaço livre [6] ou em enlaces curtos, até 10km, na primeira janela de telecomunicações (980nm) [19].

Há propostas de implementação do sistema em 1550nm e utilização de detectores de silício na recepção, através da conversão de comprimento de onda para valores menores por meio do bombeio de guias de onda do tipo PPLN (*Periodically poled* $LiNbO_3$). Com uma alta potência de bombeio, obtém-se uma eficiência geral em torno de 40%, além da possibilidade de se operar o detector em modo passivo, que possibilita a elevação da taxa de transmissão [25,26].

Finalmente, os detectores de germânio apresentam uma grande restrição prática, pois precisam ser resfriados a temperaturas tão baixas quanto 77K para que tenham boa performance [17].

4.3. Tipos de codificação

Serão vistos nessa seção os três principais tipos de codificação de qubits. Enquanto a codificação de fótons por polarização suporta apenas protocolos como o BB84 ou SARG04 (a menos que se consiga transmitir junto ao sinal quântico um pulso de referência a este vinculado, de forma que Eva não seja capaz de recriá-lo sem introduzir erros no sistema.), a codificação por fase ou por freqüência possibilita também a implementação do protocolo B92.

4.3.1. Codificação por polarização

Basicamente, no sistema de codificação por polarização, Alice possui uma fonte de fótons seguida por uma célula de Pockels (CP_1) (ou outro elemento capaz de variar a polarização da luz de forma controlada, como um piezoelétrico), como na figura 8 [9].

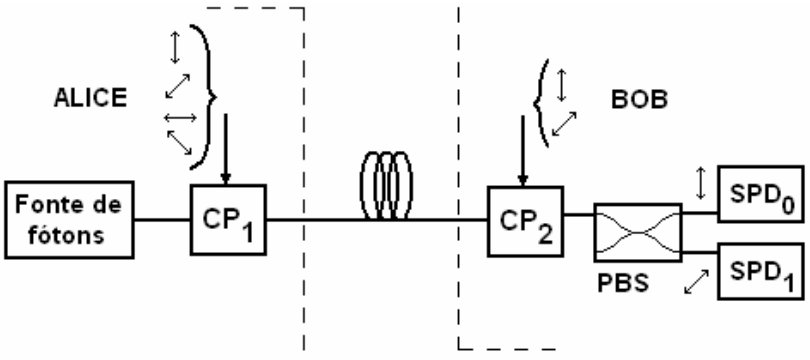

Figura 8: Configuração do sistema de codificação por polarização em que Alice e Bob escolhem suas bases aleatoriamente utilizando, por exemplo, uma célula de Pockels [9]. Dependendo da medição, o fóton emergirá de uma das saídas do divisor de feixes por polarização (PBS), atingindo um dos detectores de fótons únicos (SPD), o que acusará o bit de informação.

Para cada bit randômico a ser transmitido, a polarização é escolhida aleatoriamente dentre quatro possibilidades (protocolo BB84) agrupadas em duas bases não ortogonais, como polarização horizontal e vertical representando os bits 1 e 0, respectivamente, em uma base ⊕, e polarização na base diagonal ⊗ com os ângulos de -45º e +45º, também representando os bits 1 e 0.

Na recepção, os pulsos passam por outra célula de Pockels (CP_2), através da qual Bob escolherá, aleatoriamente, dentre uma das duas bases ⊕ ou ⊗. Em seguida, é colocado um divisor de feixe óptico por polarização (PBS – *Polarization beam-splitter*).

Caso a base de medição de Bob coincida com a de preparação do qubit por Alice, o fóton incidente no PBS emergirá por uma porta específica deste, de acordo com o estado codificado, atingindo um determinado detector de fótons isolados (SPD – *Single photon detector*). Neste caso, se Alice codificou o qubit com polarização vertical, o fóton emergirá da porta conectada ao SPD_0, que acusará uma contagem. Caso a polarização tenha sido horizontal, o fóton sairá pela outra porta dos PBS e atingirá o SPD_1. A preparação e medição do qubits na mesma base diagonal terão resultados semelhante, acusando contagem no SPD_0 ou no SPD_1 para os estados +45º e -45º, respectivamente.

Contudo, se a base de medição divergir da base de preparação, ou seja, se as bases forem incompatíveis, haverá probabilidades iguais de o fóton emergir de qualquer uma das portas do PBS, resultando em uma contagem aleatória de bit 0 ou bit 1.

Cabe ressaltar a importância de haver apenas um fóton em cada pulso, pois, caso contrário, Eva poderia medir um fóton em cada base, e retransmitir para Bob, ou medir um dos fótons enquanto o outro segue para Bob (PNS).

4.3.2. Codificação por fase

Pode-se utilizar a fase como parâmetro alternativo à polarização para codificação dos fótons, sendo este mais atrativo para a transmissão por canal cabeado.

O sistema é configurado de maneira similar a um interferômetro de Mach-Zehnder, com um modulador de fase em cada braço, como na figura 9a. Na verdade, sendo difícil manter a relação de fase entre os braços por percursos longos, é mais prático colapsar o sistema em dois interferômetros (figura 9b), apesar da perda de metade da potência [9].

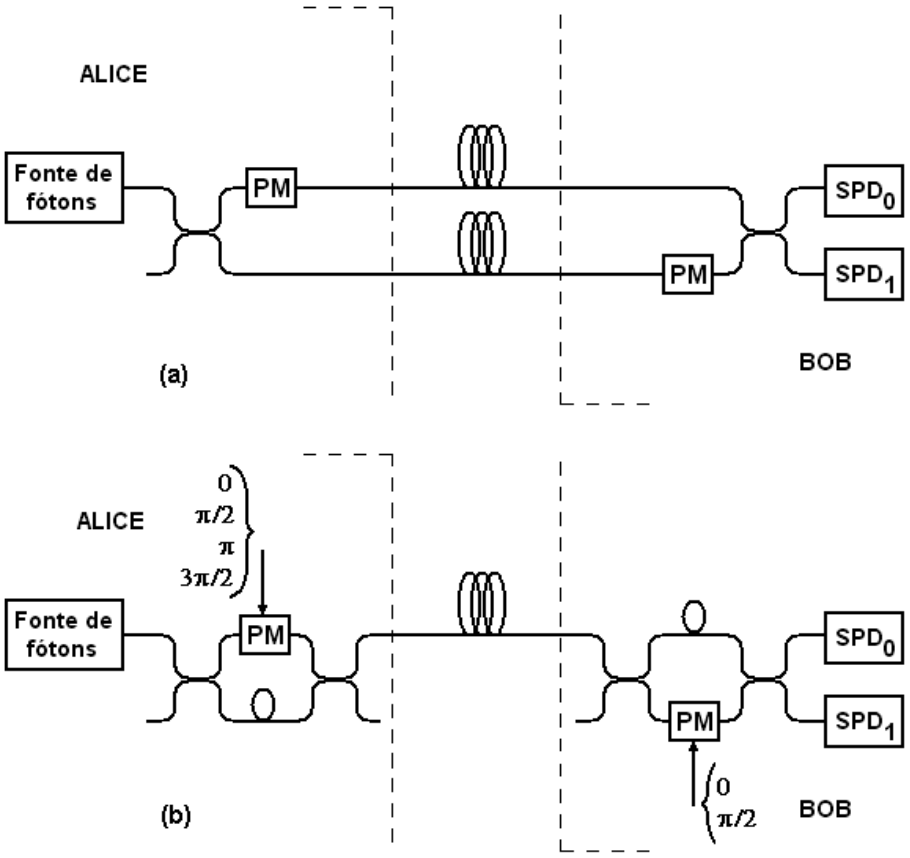

Figura 9: Configuração do sistema de codificação por fase com interferômetro de Mach-Zehnder inteiro (a) e colapsado em dois (b) [9]. A escolha das bases é feita através dos moduladores de fase (PM). Dependendo da combinação, o fóton atingirá um dos dois detectores de fótons únicos (SPD), acusando o bit.

Para implementação do protocolo BB84, Alice pode gerar quatro fases em duas bases: 0 e π (base 1) ou $\pi/2$ e $3\pi/2$ (base 2). Acionando um modulador de fase (PM), Alice prepara seus qubits codificando aleatoriamente os pulsos ópticos provenientes de sua fonte.

Escolhendo entre duas fases, uma de cada base, Bob efetua a mudança de fase dos fótons, obtendo medições nas bases $\oplus$ ou $\otimes$. Os detectores de Bob acusarão corretamente os bits 0 ou 1 em SPD_0 ou SPD_1, respectivamente, devido ao divisor (ou seja, o fóton emergirá por uma das portas de acordo com sua fase), caso tenha escolhido base compatível com a preparação. Caso a base escolhida por Bob esteja errada, o fóton ativa um dos detectores aleatoriamente.

Os fótons poderão seguir quatro caminhos entre Alice e Bob, de acordo com os caminhos ópticos dos braços dos interferômetros. Os caminhos longo-

longo e curto-curto devem ser desprezados, pois não apresentam interferência, ao contrário dos caminhos longo-curto e curto-longo.

Na versão B92 deste sistema, Alice escolhe, assim como Bob, aleatoriamente entre duas fases, uma em cada base. Além disso, utiliza-se apenas um detector na recepção. Caso a diferença entre a fase de Bob em relação à de Alice seja 0, a interferência será construtiva, resultando em uma contagem no SPD. Caso a defasagem seja igual a π, não haverá contagem, pois a interferência será destrutiva.

4.3.3. Codificação por freqüência

A codificação por freqüência comporta ambos os protocolos B92 e BB84 ou mesmo SARG04, dependendo de sua implementação [8]. Este tipo de sistema baseia-se na dupla modulação de um pulso óptico e na conseqüente interferência entre as bandas laterais e a portadora. Os tipos de modulação determinarão o protocolo a ser seguido, ou seja, no caso AM-AM ou PM-PM, o protocolo será B92, enquanto que, no caso AM-PM ou PM-AM, poderá ser BB84, B92, SARG04, entre outros.

Como pode ser visto na figura 10, a técnica utiliza dois moduladores ópticos, um localizado em Alice e outro em Bob. Após o correto ajuste da fase de referência (o sinal óptico de Alice deve chegar ao modulador de Bob no mesmo instante que o sinal elétrico dele), Alice escolhe aleatoriamente a fase ϕ_1 de seu sinal de rádio-freqüência, enquanto Bob escolhe, também aleatoriamente, a fase ϕ_2 de sua RF, ambos os sinais com freqüência *f*.

Como conseqüência da primeira modulação, o bit será codificado em ambas as bandas laterais de acordo com sua diferença de fase em relação à portadora óptica. A segunda modulação aplicará uma nova fase às bandas laterais, resultando em interferências construtivas ou destrutivas, ou seja, a diferença de fase resultante está relacionada à escolha adequada ou não da base de medição do qubit em relação à sua preparação.

O filtro então separa a portadora óptica das bandas laterais, enviando estas para o multiplexador em comprimento de onda que as separará e as enviará aos detectores. A acusação de contagem se dará de acordo com a posição espectral dos fótons em uma ou outra banda lateral.

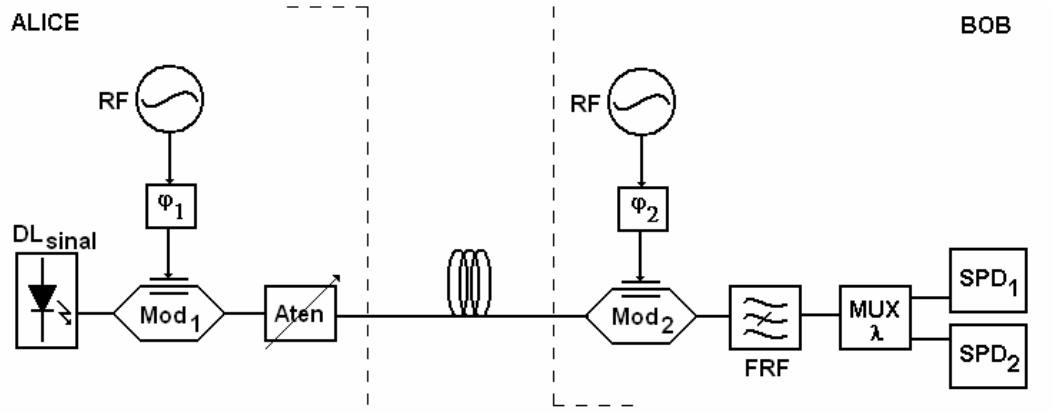

Figura 10: Sistema de distribuição quântica de chaves por codificação em freqüência. Caso o protocolo utilizado seja B92, Bob deve substituir o multiplexador (MUX) e o filtro rejeita-faixa (FRF) por um filtro passa faixa centrado em uma das bandas laterais e precisará de apenas um dos detectores de fótons únicos (SPD).

4.3.3.1. AM-AM ou PM-PM

A técnica utiliza dois moduladores de fase ou dois moduladores de amplitude [7], um localizado em Alice e outro em Bob. Alice escolhe aleatoriamente a fase Φ_1 dentre 0 ou π, representando bits 0 e 1, respectivamente, para seu sinal de rádio-freqüência que modulará o sinal óptico proveniente de um laser pulsado, que será atenuado. Na recepção, Bob também escolherá sua fase Φ_2 aleatoriamente dentre 0 ou π.

A relação entre as fases escolhidas gerará interferência, de forma que a intensidade das bandas laterais será máxima quando $|\Phi_1-\Phi_2|=0$ e mínima quando $|\Phi_1-\Phi_2|=\pi$, resultando em uma possibilidade de medição ou não, respectivamente.

O filtro passa-faixa tem seu pico de transmissão centralizado em uma das bandas laterais de transmissão, ou seja, em $\omega_0 \pm \Omega$ (ω_0 sendo a freqüência óptica). O sinal filtrado é então enviado ao detector de fótons únicos.

Assim, quando houver bandas laterais, significa que Bob escolheu a base de medição correta e, de acordo com esta base, saberá qual bit foi recebido. Caso não haja bandas laterais, a diferença de fase terá sido π e não haverá como determinar se houve decodificação na base errada ou se o fóton não foi recebido, devendo este instante ser descartado no passo posterior do protocolo,

quando as bases são publicamente comparadas. Cabe ressaltar que ambas as bandas laterais se comportam de maneira semelhante simultaneamente. A tabela 3 mostra as combinações de fase possíveis para o caso em que se utiliza o protocolo B92.

Alice		**Bob**		
Bit	Φ_1	Φ_2	$\Delta\Phi$	**Bit**
0	0	0	0	0
	0	π	π	Não
1	π	0	π	Não
	π	π	0	1

Tabela 3: Combinações de fases para o esquema de codificação por freqüência com protocolo B92.

Este esquema de codificação preenche o requisito de segurança do protocolo em questão, pois envia-se pulsos de referência junto com os qubits. Estes pulsos são a própria portadora óptica, que terá número de fótons superior ao das bandas laterais onde está codificada a informação. Caso Eva bloqueie um qubit, bloqueará também este pulso, revelando-se para Bob. Caso tente enviar apenas o pulso, retendo as bandas laterais, não obterá informação, pois Alice e Bob descartarão este qubit posteriormente.

4.3.3.2. AM-PM ou PM-AM

O caso AM-PM (ou PM-AM) se assemelha ao anterior. Todavia, sua compatibilidade com o protocolo BB84 (SARG04) o torna especialmente atraente para a distribuição quântica de chaves.

Este esquema possibilita que o qubit seja encontrado de forma complementar em apenas uma das bandas laterais do pulso modulado, caso a base de medição seja compatível, ou apresente ambigüidade, caso a base seja erroneamente escolhida.

Assim, pode-se demonstrar que, se ambos os moduladores receberem o mesmo sinal de RF e tiverem as fases e profundidades de modulação devidamente ajustadas, além do correto ajuste da tensão de polarização do modulador AM, as bandas laterais comportar-se-ão de forma complementar. Isso se deve ao fato de a modulação AM gerar um par de bandas laterais igualmente espaçadas em relação à portadora óptica de uma distância espectral igual à do sinal de RF modulante e com fases idênticas, enquanto que a modulação PM gera bandas de forma semelhante, porém com fases opostas.

Logo, é possível obter uma situação ótima em que uma das bandas laterais se extingue enquanto a outra é mantida. De acordo com a escolha das fases de Alice e de Bob, o qubit poderá estar codificado na banda lateral inferior ou na banda lateral superior, representando os bits 0 e 1, ou com probabilidades idênticas de ser encontrado em uma das bandas laterais.

Como na figura 10, Alice deve escolher a fase do sinal de RF que modulará sua fonte laser. Porém, agora, além da escolha aleatória do bit a ser enviado, deverá ser escolhida, também de forma randômica, uma base de codificação, ou seja, a base 0 e π ou a base $\pi/2$ e $3\pi/2$. Os pulsos modulados preparados por Alice são adequadamente atenuados, para que se adeqüem ao regime quântico, e transmitidos para Bob.

Na recepção, Bob deverá escolher aleatoriamente dentre dois valores fixos de fase, um de cada base, como, por exemplo, 0 e $\pi/2$, para cada qubit. A diferença entre as fases escolhidas pelas partes comunicantes determinará a freqüência onde estará localizado o qubit, conforme a tabela 4. Caso a diferença de fase seja igual a zero ou π, Bob terá escolhido a base adequada e poderá medir o qubit na banda lateral inferior ou superior, respectivamente. Se a base escolhida não for compatível com a de preparação do qubit, a diferença de fase será $\pi/2$ e Bob encontrará o qubit em uma das bandas laterais aleatoriamente, com probabilidades semelhantes.

Como na figura 10, para que Bob efetue uma medida que lhe informe a posição espectral do qubit decodificado, é necessário que a portadora óptica seja filtrada, pois não carrega informação e contribuiria com ruído. As bandas laterais devem, então, ser espectralmente separadas pelo multiplexador de comprimento de onda e detectadas independentemente por dois detectores de fótons únicos. Como no caso anterior, pode-se aproveitar a portadora extraída como pulso de referência e tornar o sistema mais robusto contra certos tipos de ataques.

Alice			Bob				
Base	**Bit**	Φ_1	Φ_2	$\Delta\Phi$	$P(\|\Omega-\omega_0\rangle)$	$P(\|\Omega+\omega_0\rangle)$	**Bit**
α	0	0	0	0	0	1	1
		0	$\pi/2$	$\pi/2$	0,5	0,5	0 ou 1
	1	π	0	π	1	0	0
		π	$\pi/2$	$\pi/2$	0,5	0,5	0 ou 1
β	0	$\pi/2$	0	$\pi/2$	0,5	0,5	0 ou 1
		$\pi/2$	$\pi/2$	0	0	1	1
	1	$3\pi/2$	0	$\pi/2$	0,5	0,5	0 ou 1
		$3\pi/2$	$\pi/2$	π	1	0	0

Tabela 4: Combinações de fase para o esquema de codificação por freqüência com protocolo BB84. Após a decodificação, os qubits podem assumir os estados referentes às bandas laterais $|\Omega\pm\omega_0\rangle$ com probabilidade (P) igual a 0, 0,5 ou 1.

4.4. Considerações sobre o canal

Devido a variações da birrefringência da fibra, ocasionadas por imperfeições de simetria no momento da fabricação ou por condições ambientais diversas (carga de vento e temperatura), o canal está sujeito à dispersão dos modos de polarização. Isso significa que há troca aleatória de energia entre os dois modos de polarização do campo óptico, ou seja, além de o modo propagante no eixo rápido se afastar do modo propagante no eixo lento (dispersão), a polarização flutuará.

Assim, caso se deseje utilizar a codificação por polarização em sistemas ópticos guiados, faz-se necessária a utilização de fibras mantenedoras de polarização com alta birrefringência – fibras *hi-bi*, ou a utilização de compensação ativa de polarização.

O primeiro caso pode inviabilizar um projeto, dado o alto custo envolvido, além da maior atenuação deste tipo de fibra em relação às fibras convencionais atuais.

A segunda opção possibilita a utilização da malha óptica já implementada, composta em sua maioria por fibras padrão ou DS. Sistemas de compensação

ativa de polarização vêm sendo desenvolvidos [20], prometendo avanços significativos para os sistemas quânticos deste tipo.

Entretanto, a QKD com codificação por polarização é atrativa para comunicações ópticas em espaço-livre, já que esta característica é conservada pelo meio.

4.5. QBER sistêmica

Na realidade, qualquer que seja o sistema de distribuição quântica de chaves implementado, haverá sempre uma determinada taxa de erros de qubits, independente da presença de Eva. Esta QBER sistêmica é dada pela razão entre o número de bits errados compartilhados por Alice e Bob e o número total de bits da *sifted key*, esta, metade da *raw key*, no caso do protocolo BB84. A eq. 4.6 representa a taxa de qubits da *sifted key*, expressa em função da taxa de repetição (f_{rep}) dos pulsos, ou qubits, do número médio de fótons por pulso (μ), da probabilidade de um fóton chegar ao detector (P_a) e da probabilidade de o fóton ser detectado (η), segundo [6].

$$R_{sifted} = \frac{1}{2} R_{raw} = \frac{1}{2} f_{rep} \mu P_a \eta \tag{4.6}$$

A taxa de bits errados na QBER pode ser decomposta em duas contribuições, no caso de QKD com partículas simples. Os erros introduzidos por dispositivos ópticos utilizados na decodificação (R_{disp}) podem ser expressos pela taxa da *sifted key* multiplicada pela soma das probabilidades de o fóton seguir para o detector errado (P_{disp}) e de ser detectado um fóton proveniente do ruído de fundo do sistema, como na eq. 4.7. Fisicamente, estes erros são causados por interferência imperfeita, desalinhamento de polarização ou desbalanceamento de interferômetros.

$$R_{disp} = R_{sifted} \left(P_{disp} + P_{fundo} \right) \tag{4.7}$$

Já os erros originários dos detectores (R_{det}) devem-se a contagens de escuro (portadores térmicos) na janela de tempo em que o dispositivo estaria apto a receber um fóton. Esta taxa de erro pode ser descrita pela eq. 4.8,

considerando que os *afterpulses* (pós-pulsos ocasionados pelo armadilhamento de pares elétron-buraco) foram minimizados. A probabilidade de contagem de escuro nos dois detectores por janela de gatilho, assumidas como iguais, é dada por P_{esc}.

$$R_{\det} = \frac{1}{2} f_{rep} P_{esc} \tag{4.8}$$

A QBER do sistema sem a interferência do espião pode ser escrita como na eq. 4.9.

$$QBER = \frac{\frac{2R_{sifted}\left(P_{disp} + P_{fundo}\right)}{f_{rep}} + P_{esc}}{\mu P_a \eta} \tag{4.9}$$

Assim, a QBER total possui duas contribuições, uma devida ao ruído de escuro do detector ($QBER_{det}$) e outra devida à probabilidade de um fóton seguir para o detector errado e ao ruído de fundo do sistema ($QBER_{disp}$). Esta última, é dada, no caso do sistema de codificação por freqüência, especialmente pelo desvio de fase dos moduladores QPSK e pelo interferômetro de Mach-Zehnder utilizado na separação das bandas laterais do sinal

A partir das contagens finais do sistema, obtém-se a visibilidade, dada classicamente pela eq. 4.10, considerando-se as contagens máxima e mínima, ou seja, com o sistema operando com decodificação correta dos qubits (no caso específico de codificação por freqüência, a diferença de fases sendo igual a zero ou π).

$$V = \frac{Contagem_{máx} - Contagem_{mín}}{Contagem_{máx} + Contagem_{mín}} \tag{4.10}$$

A QBER total do sistema sem a presença do espião será dada pela eq. 4.11, estando relacionada à visibilidade calculada.

$$QBER = \frac{1-V}{2} \tag{4.11}$$

Entretanto, subtraindo-se o ruído dos detectores das contagens, tem-se novo valor de visibilidade, resultando em uma QBER devida apenas aos dispositivos do sistema (eq. 4.12), enquanto que o restante, em relação à QBER total, corresponderá aos detectores (eq. 4.13).

$$QBER_{disp} = \frac{1 - \frac{Contagem_{máx} - Contagem_{mín}}{Contagem_{máx} + Contagem_{mín} - 2\,ruído}}{2} \tag{4.12}$$

$$QBER_{\det} = QBER - QBER_{disp} \tag{4.13}$$