Pontifícia Universidade Católica
do Rio de Janeiro

Thiago Ferreira da Silva

Elementos para comunicação quântica experimental utilizando fotodiodos avalanche

Tese de Doutorado

Tese apresentada ao Departamento de Engenharia Elétrica da PUC–Rio como requisito parcial para obtenção do título de Doutor em Engenharia Elétrica

Orientador: Prof. Guilherme Penello Temporão

Rio de Janeiro
dezembro de 2011

Pontifícia Universidade Católica
do Rio de Janeiro

Thiago Ferreira da Silva

Elementos para comunicação quântica experimental utilizando fotodiodos avalanche

Tese apresentada como requisito parcial para obtenção do título de Doutor pelo Programa de Pós–graduação em Engenharia Elétrica do Departamento de Engenharia Elétrica do Centro Técnico Científico da PUC–Rio. Aprovada pela Comissão Examinadora abaixo assinada.

Guilherme Penello Temporão
Orientador
Centro de Estudos em Telecomunicações /PUC–Rio

Prof. Jean Pierre von der Weid
Centro de Estudos em Telecomunicações /PUC–Rio

Prof. Giancarlo Vilela de Faria
Centro de Estudos em Telecomunicações /PUC–Rio

Prof^{a}. Patrícia Lustoza
Centro de Estudos em Telecomunicações /PUC–Rio

Prof. Rubens Viana
Universidade Federal do Ceará

Prof. Rogério Passy
MLS Wireless

Prof. José Eugenio Leal
Coordenador do Centro Técnico Científico — PUC–Rio

Rio de Janeiro, 19 de dezembro de 2011

Thiago Ferreira da Silva

Graduou-se em Engenharia de Telecomunicações pela Universidade Católica de Petrópolis, Petrópolis – RJ, em 2005. Obteve o título de Mestre em Engenharia Elétrica na sub-área Optoeletrônica & Instrumentação da linha de pesquisa em Eletromagnetismo Aplicado em 2008 pela Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro – RJ. Suas principais áreas de interesse envolvem detectores de fótons únicos, metrologia de fibras e de componentes ópticos e comunicações quânticas.

Ficha Catalográfica

Ferreira da Silva, Thiago

Elementos para comunicação quântica experimental utilizando fotodiodos avalanche / Thiago Ferreira da Silva; orientador: Guilherme Penello Temporão. — Rio de Janeiro : PUC–Rio, Departamento de Engenharia Elétrica, 2011.

v., 136 f: il. ; 29,7 cm

1. Tese (doutorado) - Pontifícia Universidade Católica do Rio de Janeiro, Departamento de Engenharia Elétrica.

Inclui referências bibliográficas.

1. Engenharia Elétrica – Tese. 2. Detectores de fótons únicos. 3. Fotodiodos avalanche. 4. Comunicação quântica. 5. Distribuição quântica de chaves. 6. Caracterização, modelagem e simulação de detectores. I. Temporão, Guilherme Penello. II. Pontifícia Universidade Católica do Rio de Janeiro. Departamento de Engenharia Elétrica. III. Título.

CDD: 621.3

Agradecimentos

Ao professor Temporão pela orientação;
Ao professor Jean Pierre pelo incentivo e ensinamentos;
À minha esposa Flavia pela paciência e apoio nestes anos, e ao meu filho Thales, pelo carinho;
À minha mãe Goreti, ao Ayres e à minha irmã Thaís, sempre comigo, mesmo que de longe;
Ao meu avô Ferreira, grande incentivador, em memória;
Ao amigo e companheiro de medições Guix pelas inúmeras discussões e caronas e aos camaradas do laboratório Andy, Chu, Djeisson e Gian pelo companheirismo;
À Amália pelo suporte e aos demais colegas do dia-a-dia;
Ao Douglas e ao Tito pela ajuda nas medições e ao Gustavo e ao Tarcísio pela programação dos FPGA's;
Ao CNPq pela bolsa nos primeiros seis meses do curso e à PUC-Rio pela bolsa de isenção.

Resumo

Ferreira da Silva, Thiago; Temporão, Guilherme Penello. **Elementos para comunicação quântica experimental utilizando fotodiodos avalanche**. Rio de Janeiro, 2011. 136p. Tese de Doutorado — Departamento de Engenharia Elétrica, Pontifícia Universidade Católica do Rio de Janeiro.

Detectores de fótons únicos baseados em fotodiodo avalanche (SPADs) são elementos essenciais em aplicações que requerem alta sensibilidade, como comunicações quânticas. É proposto um método para caracterização em tempo real da eficiência de detecção e das probabilidades de contagem de escuro e de pós-pulsos em SPADs através da análise da estatística de tempos entre detecções consecutivas utilizando instrumentação simples com o detector sob condições de operação. O método é então aplicado no monitoramento dos detectores utilizados em um sistema de distribuição quântica de chaves, motivado pela falha de segurança que imperfeições apresentadas pela tecnologia atual de detecção podem acarretar. Em especial, os ataques after-gate e *time-shif* são implementados e analisados. Uma simulação através do método de Monte-Carlo de um detector de fótons únicos composto por uma associação de diversos SPADs ativados serialmente e precedidos por uma chave óptica ativa é apresentada, visando otimizar a performance de detecção com tecnologia atual no tangente à freqüência de gatilho. É reportada ainda a interferência estável entre fótons provenientes de fontes laser atenuadas totalmente independentes, cuja visibilidade é monitorada ao longo do tempo para um enlace implementado sobre duas bobinas de 8,5 km com controle ativo de polarização, passo importante para a tecnologia de repetidores quânticos e para o protocolo para distribuição quântica de chaves independente do aparato de medição. Um medidor de estados de Bell é implementado, utilizando-se óptica linear, com a resposta do sistema verificada para diferentes combinações dos estados preparados em duas estações remotas conectadas à estação central de medição através do canal estabilizado.

Palavras–chave

Detectores de fótons únicos. Fotodiodos avalanche. Comunicação quântica. Distribuição quântica de chaves. Caracterização, modelagem e simulação de detectores.

Abstract

Ferreira da Silva, Thiago; Temporão, Guilherme Penello (Advisor). **Elements for quantum communication based on avalanche photodiodes**. Rio de Janeiro, 2011. 136p. PhD Thesis — Departamento de Engenharia Elétrica, Pontifícia Universidade Católica do Rio de Janeiro.

Single-photon detectors based on avalanche photodiodes (SPADs) are key elements in ultra-sensitive applications, such as quantum communication. This thesis presents a method for real-time characterization of the overall detection efficiency, afterpulse and dark count probabilities, based on the analysis of the statistics of times between consecutive detections with simple instrumentation under operational condition. The method is employed for monitoring the SPADs on a quantum key distribution system, to prevent security failures due to side-channel attacks caused by current technology loopholes. The after-gate and time-shift attacks are implemented and analyzed. A Monte-Carlo simulation of a serially-activated association of SPADs, preceeded by an active optical switch, is performed for enhancement of the gating frequency performance with detectors based on current technology. The stable interference between photons from two independent faint laser sources is also reported, with visibility stability monitored over time after an optical link composed by two polarization-controlled 8.5-km fiber spools, a key features for quantum repeater and the measurement device independent quantum key distribution protocols. A Bell states analyzer is implemented with linear optics, and its response is verified for different combination of polarization states received from the remote stations through the stabilized channels.

Keywords

Single-photon detectors. Avalanche photodiodes. Quantum communication. Quantum key distribution. Characterization, modeling and simulation of SPADs.

Sumário

Lista de figuras

Lista de tabelas

1
Introdução

Sistemas de comunicação quântica [1][2] utilizam detectores ópticos otimizados para a detecção de poucos fótons[3][4]. A tecnologia baseada em fotodiodo avalanche (SPADs, do inglês *single-photon avalanche photodiodes*) é amplamente difundida, devido à sua robustez, praticidade na utilização e características gerais, quando comparada com outros detectores, como tubos fotomultiplicadores ou nano-fios supercondutores. Devido à natureza estatística dos fótons e ao modo de operação dos SPADs, alguns efeitos devem ser quantificados para uma correta operação do sistema. No capítulo 2 é apresentado o desenvolvimento de uma técnica de caracterização em tempo real de detectores de fótons únicos sob condições reais de operação baseada na estatística dos tempos entre eventos consecutivos de detecção [5]. Um modelo analítico foi desenvolvido e, quando aplicado aos dados de medição, retorna alguns dos principais parâmetros de interesse do dispositivo. A eficiência de detecção, a probabilidade de contagens de escuro e a probabilidade de ocorrência de pós-pulsos são obtidos através do ajuste do modelo ao histograma dos tempos entre eventos consecutivos de detecção, com o dispositivo sob condição real de operação. A caracterização é executada em tempo real e não necessita intervenções no dispositivo, mas apenas acesso aos pulsos elétricos de saída. A viabilidade do método é demonstrada através da medição comparativa de três dispositivos comerciais operando em modo gatilhado, com validação dos resultados através de técnicas complementares, com boa concordância entre os resultados.

Comunicação segura e sigilosa é um desejo da civilização deste tempos imemoriais. O advento da chave criptográfica facilitou, de certa forma, a garantia da segurança durante o compartilhamento de informação, uma vez que o algoritmo de encriptação pôde ser amplamente divulgado. Apesar de comprovadamente segura, a cifra *one-time pad* depende da não reutilização da chave criptográfica, esta aleatoriamente gerada, que deve ser compartilhada pelas partes comunicantes. Visando solucionar o problema da troca de chaves, surgiu o protocolo de comunicação quântica conhecido como distribuição quântica de chaves (QKD, do inglês *quantum key distribution*) [6][7][2], cuja

segurança baseia-se nos princípios da física quântica [8][9]. Basicamente, a impossibilidade de replicação de um estado quântico desconhecido com precisão absoluta e a perturbação imposta a um sistema quântico durante uma medição garantem a identificação de um possível interceptador, revelado em uma etapa subseqüente de comunicação pelo aumento da taxa de erro. Implementações práticas de sistemas QKD, entretanto, podem ter a segurança comprometida por imperfeições apresentadas pelos equipamentos e dispositivos empregados [10]. Em especial, os chamados canais laterais (em inglês, *side-channels*) abertos pelos SPADs da estação de recepção possibilitam a manipulação externa do resultado de medição dos qubits através de diversas técnicas, como o envio de sinais ópticos para depletar a sensibilidade do detector – ou mesmo cegá-lo, o envio de pulsos para impor uma contagem em determinado SPAD ou da variação do tempo de chegada dos fótons dentro da janela de detecção, que causa um resultado tendencioso. Estas técnicas podem ou não ser combinadas com uma estratégia do tipo "interceptação-com-reenvio´´, causando pouco ou nenhum aumento da taxa de erro. No capítulo 3, é proposta a utilização do método de caracterização de SPADs, previamente apresentado, para o monitoramento em tempo real dos detectores em um sistema QKD [11][12]. Dois tipos particulares de ataque são experimentalmente simulados, os chamados "after-gate" [13] e "time-shift" [14], com aplicação do sistema de monitoramento para identificação da intervenção. O primeiro método de ataque é baseado no envio de pulsos ópticos fortes ao final da janela de detecção, codificados de acordo com o estado interceptado, forçando uma avalanche no detector correspondente àquele estado. A segunda estratégia explora o descasamento das curvas de eficiência dos detectores através da manipulação da posição temporal de incidência dos fótons em relação à janela de detecção, sem interceptação. Os sinais de intervenção deixados pelos ataques são quantificados, em especial a probabilidade de pós-pulsos, no primeiro caso, e a variação da eficiência de detecção e ocorrência de eventos temporalmente correlacionados, no segundo. Considerações acerca da eficácia do método de monitoramento contra outras estratégias de ataque baseadas na tecnologia atual são analisadas.

O capítulo 4 apresenta a simulação numérica da resposta de um detector de fótons únicos composto por diversos SPADs precedidos por uma chave óptica e sequencialmente acionados após cada evento de detecção. A redução do tempo morto do dispositivo é obtida através da ativação serial dos detectores. Para compensar a perda imposta pela chave, o dispositivo é resfriado, com compensação da tensão de excesso de polarização para aumento da eficiência de detecção com manutenção da taxa de contagens de escuro. As limitações

causadas pelo efeito de pós-pulsos em altas taxas de repetição são analisadas e discutidas. Os resultados indicam a possibilidade de extensão da freqüência de gatilho do detector através da técnica apresentada utilizando tecnologia atualmente disponível.

Sistemas de comunicação, de uma forma geral, estão sujeitos à atenuação do canal de propagação, que pode impor limitação severa em relação à distância do enlace ou à máxima taxa útil de transmissão. Diferente dos sistemas clássicos de comunicação óptica, em que estações repetidoras ou amplificadores são amplamente utilizados para recondicionamento ou amplificação do sinal, respectivamente, nos sistemas de comunicação quântica qualquer processo de amplificação é indesejado, sobretudo nas aplicações em criptografia. Como conseqüência, a extensão do alcance de um enlace não é uma tarefa trivial, mas pode ser obtida através dos protocolos de repetidores quânticos [15]. O repetidor quântico pode ser implementado baseado na interferência entre dois fótons emitidos por conjuntos atômicos remotamente localizados, e depende da indistinguibilidade entre os fótons, medidos com um analisador de estados de Bell em uma estação central, acessada via fibra óptica. No capítulo 5 é relatada a implementação experimental de um enlace composto por dois lances independentes de fibra óptica conectando duas estações remotas a uma estação central de medição. Os enlaces, de 8,5 km cada, são ativamente estabilizados através de controladores automáticos de polarização e a interferência entre fótons oriundos de fontes laser totalmente independentes é monitorada ao longo do tempo [16]. Além disso, acrescentando um analisador de estados de Bell, montado com óptica linear, é implementado o recentemente proposto sistema de distribuição de chaves com segurança independente do aparato de medição [17], uma solução alternativa para os *side-channels* abertos pelos SPADs. A resposta do sistema é analisada para diferentes combinações de estados de polarização enviados pelas duas estações remotas. Os resultados indicam a possibilidade de estabelecimento de protocolos de comunicação com codificação em polarização sobre fibra óptica, mesmo que baseados em interferência, bem como a viabilidade do protocolo MDI-QKD.

O capítulo 5 traz as conclusões referentes aos trabalhos desenvolvidos e expostos nesta tese.

2
Caracterização de detectores de fótons únicos pelo tempo entre detecções

Detectores de fótons únicos [3][4] são dispositivos amplamente utilizados em aplicações ultra-sensíveis, como astronomia[19], comunicações quânticas [1], reflectometria óptica no domínio do tempo com contagem de fótons [20][21], metrologia óptica com resolução superando os limites clássicos [22], sensoreamento remoto [23] e imageamento com fins biomédicos [24].

Em especial, os detectores de fótons únicos baseados em fotodiodo avalanche [25][26][27] destacam-se apresentando algumas vantagens sobre outras tecnologias, sendo mais eficientes e fáceis de manusear que os tradicionais tubos fotomultiplicadores (especialmente na região espectral do infravermelho) [28], e mais práticos que sistemas de conversão ascendente baseada em interação não-linear da luz em um cristal(em inglês *frequency up-conversion*) [29]. Outras tecnologias emergentes promissoras, como os nano-fios supercondutores de NbN [30][31], apresentam potencial para operação em altas taxas e com baixo *jitter* temporal, mas ainda apresentam baixa eficiência no infravermelho. Além disso, precisam operar em temperaturas criogênicas, o que torna inviável sua aplicação em campo. Os detectores SPADs desenvolveram-se nas últimas décadas, tanto para detecção de fótons na região visível do espectro eletromagnético, quanto no infra-vermelho. Neste último caso, um grande impulso se deve ao desenvolvimento das comunicações quânticas em comprimentos de onda compatíveis com os sistemas clássicos de transmissão sobre fibra óptica [1][2] (que apresentam baixa atenuação e abundância de equipamentos com baixo custo, devido à larga escala de produção), com destaque para os sistemas de distribuição quântica de chaves [2]. Diferentes fabricantes (Perkin-Elmer, idQuantique, MagiQ) oferecem detectores na forma de módulos contadores de fótons prontos para utilização, incluindo a estabilização térmica, o circuito de polarização elétrica e extinção de avalanche, o discriminador de eventos de detecção e, em alguns casos, um contador de pulsos integrado, com interface de comunicação. A configuração matricial de elementos sensíveis a fótons únicos também representa avanço significativo nesta área [32].

Para uma correta aplicação de SPADs em um sistema de medição,

algumas de suas características devem ser conhecidas. Ao longo dos últimos anos, várias técnicas foram desenvolvidas [33][34][35][36] para a caracterização de diversos parâmetros dos SPADs, em especial a eficiência de detecção, a probabilidade de contagens de escuro e a probabilidade de ocorrência de pós-pulsos [1]. Estes métodos apresentam como característica em comum o fato de utilizarem um arranjo especial para a caracterização de cada parâmetro individualmente. Métodos para caracterização da eficiência quântica baseados apenas nos valores médios de contagem no detector por intervalo de tempo quando submetido a uma fonte óptica com potência constante, geralmente superestimam este parâmetro, devido ao efeito de pós-pulsos, erroneamente assumidos como fótons incidentes [36]. Deste modo, quanto maior a freqüência de repetição, mais relevante será este desvio. Para evitar este desvio, pode-se realizar a medição com o detector operando em uma taxa de gatilho baixa ou, alternativamente, observar a distribuição temporal dos eventos de detecção. Em [36], a eficiência de detecção é corrigida eliminando os eventos ocorridos em intervalos de tempo curtos.

A probabilidade de ocorrência de uma contagem de escuro, devido a um portador de carga termicamente excitado ou tunelamento através da barreira de depleção, pode ser estimada com a entrada do detector bloqueada e aplicando-se um tempo morto suficientemente grande após cada evento de detecção. No caso de operação em modo gatilhado, pode-se reduzir a freqüência de gatilho para um valor baixo, como 10 kHz [114], e tomar a razão entre os valores médios de contagem pelo número de janelas abertas em um mesmo intervalo de tempo.

Sendo dependente do tempo de decaimento das armadilhas preenchidas no semicondutor durante uma avalanche, a contribuição nas contagens atribuída ao efeito de pós-pulsos pode ser obtida pelo método da janela dupla [34], que consiste em duas etapas. As armadilhas do semicondutor são inicialmente preenchidas com a incidência de um estímulo óptico durante uma janela curta inicial. Então, após um determinado tempo, uma segunda janela, longa, é aplicada ao detector até que uma detecção ocorra. O tempo decorrido entre a aplicação do pulso óptico e o primeiro evento de detecção dentro da segunda janela é medido e, o processo, repetido. Os resultados são agrupados em um histograma, que é então analisado através da função densidade de probabilidade cumulativa. Outro método [33] faz uso de um pulso inicial e abre uma janela de detecção com uma certa duração temporal após um determinado tempo de espera. Esta segunda janela é excursionada e dá origem a um histograma similar ao anterior, de onde a probabilidade de pós-pulsos é extraída.

[1] Tradução livre de *afterpulses*

Neste capítulo é proposto um método de caracterização de detectores de fótons únicos baseados em fotodiodos avalanche operando em modo Geiger através da análise da estatística de distribuição de tempos entre eventos consecutivos de detecção, como em [36]. O método proposto, entretanto, permite a caracterização de alguns dos principais parâmetros do SPAD simultaneamente e sob condições reais de operação em tempo real. A eficiência de detecção de fótons, a probabilidade de contagens de escuro e a probabilidade ocorrência de pós-pulsos podem ser quantificadas em tempo real por meio de instrumentação simples. Em complemento, o método também permite a caracterização do tempo morto do detector e, potencialmente, da largura da janela de gatilho, quando em modo gatilhado.

É apresentada uma breve descrição do princípio de funcionamento de um detector de fótons únicos por avalanche a definição dos parâmetros de interesse. Em seguida, o método de caracterização é apresentado, com a dedução do modelo analítico desenvolvido. Resultados experimentais da caracterização de três SPADs comerciais são mostrados e discutidos.

2.1 Dispositivos contadores de fótons

Fotodiodos avalanche (APD, do inglês *avalanche photodiode*) [38] apresentam uma região interna chamada camada de multiplicação. Portadores de carga transitando nesta região de campo elétrico intenso são capazes de arrancar outros portadores através do processo de ionização por impacto [39]. Este efeito opera em cascata e aumenta significativamente a fotocorrente, proporcionando alto ganho, de modo que o dispositivo apresenta grande sensibilidade [40]. Se um APD for reversamente polarizado ligeiramente acima da região de ruptura, sua operação torna-se não-linear e um único fóton pode ser capaz de desencadear uma avalanche, desde que sua energia seja maior que o *bandgap* do semicondutor. Assim, uma macro-corrente auto-sustentada da ordem de miliampère pode ser gerada [41]. A operação do dispositivo em modo Geiger é fundamental tanto para sua preservação, devido ao grande fluxo de corrente, quanto para sua reinicialização, pois durante uma avalanche, o detector fica temporariamente incapaz de novas detecções até ter a condição de polarização restaurada [26].

Os SPAD podem ser tipicamente classificados de acordo com o modo de operação como contínuo (*free-running*) ou gatilhado [25]. No primeiro, com exceção de um inevitável período de tempo morto, o detector se mantém continuamente apto a desencadear uma avalanche até a ocorrência de um evento de detecção. Logo que possível, a avalanche é extinta e a alta sensibilidade do dis-

positivo é re-estabelecida. Já no modo gatilhado, o detector torna-se sensível a poucos fótons apenas durante intervalos curtos de tempo – as chamadas janelas de detecção – de acordo com um sinal elétrico de gatilho (*trigger*), geralmente periódico. O fim da janela de detecção forçosamente desabilita o dispositivo.

Uma forma passiva de se extinguir o processo de avalanche (usualmente chamado *passive quenching*) utiliza um resistor de carga R_L (de alguns kΩ) em série com a fonte de polarização (V_{bias}) e com o APD [25], conforme mostrado na figura 2.1a. Quando a avalanche se inicia, o fotodiodo comporta-se como

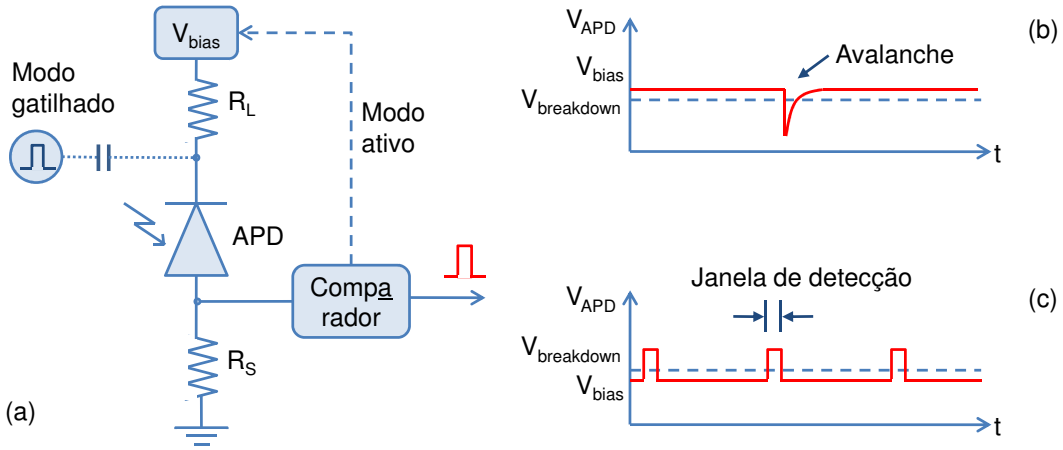

Figura 2.1: (a) Esquema simplificado de um SPAD operando em modo *free-running* com extinção passiva (*passive-quenching*). A seta tracejada indica realimentação do sinal de detecção para operação em modo ativo. A linha pontilhada mostra o acoplamento de um gerador de pulsos para operação em modo gatilhado. (b) Representação da tensão de polarização (V_{bias}) em relação à tensão de ruptura ($V_{breakdown}$) para operação em modo *free-running* e (c) gatilhado.

uma fonte de corrente com uma chave que se fecha. A avalanche pode ser monitorada pela queda de tensão no resistor em série R_S (de 50Ω, por exemplo) devido ao fluxo de corrente através deste. Um circuito discriminador deve ser utilizado e um pulso formatado (TTL ou NIM, por exemplo) é enviado para a saída do detector, indicando a ocorrência do evento de detecção. A corrente de avalanche gera também uma queda de tensão no resistor de carga R_L. A tensão de polarização sobre o fotodiodo, que originalmente era integral, reduz-se, de modo que a polarização deste elemento fica momentaneamente abaixo do limiar de ruptura, extinguindo-se a avalanche. Quando o fluxo de corrente cessa, a capacitância do fotodiodo recarrega-se e sua polarização retorna à condição inicial, acima do limiar de ruptura ($V_{breakdown}$), como indicado na figura 2.1b, tornando-se o dispositivo apto a detectar um novo fóton.

Este período morto (*deadtime*) entre a avalanche e o re-estabelecimento da condição de polarização próxima à ruptura pode ser minimizado através de

uma técnica ativa de extinção de avalanche. O sinal de saída é monitorado e, assim que discriminado – indicando o início de uma avalanche –, a tensão de polarização é ativamente reduzida. A seta tracejada na figura 2.1a representa o sinal de realimentação. O modo ativo é comumente empregado em dispositivos comerciais, pois possibilita maior taxa de contagem por reduzir os efeitos de pós-pulsos [25] [2]. Este modo de operação, chamado de *active-quenching*, é tipicamente, mas não exclusivamente [42], utilizado em SPADs de silício [25], estes compatíveis com a região espectral visível e início do infra-vermelho [43].

Para cada fóton incidente, o detector apresenta uma probabilidade não-unitária de completar o processo de acoplamento, absorção, geração de um par elétron-buraco e desencadeamento de uma avalanche, o que define o parâmetro eficiência de detecção [26]. Este representa a probabilidade de um fóton incidente gerar um evento de detecção observado como um pulso elétrico padrão.

Na realidade, mesmo portadores elétricos não originados por fótons podem desencadear uma avalanche. Este fenômeno é conhecido como contagem de escuro (*dark count*) e representa uma característica intrínseca aos SPADs. Este tipo de falsos eventos é causado por portadores termicamente promovidos da banda de valência para a banda de condução ou por cargas tunelando através da barreira de potencial (ou assistidas por um estado intermediário) [27]. As contagens de escuro de origem térmica podem ser reduzidas através do resfriamento do dispositivo [114]. Existem porém outras limitações para o resfriamento, como o aumento da constante de tempo das cargas armadilhadas causadoras de pós-pulsos [33] (como será discutido a seguir), de modo que os dispositivos são mantidos em uma temperatura ótima, cuja faixa depende, entre outros fatores, do material que os constitui. No caso de detectores baseados em InGaAs, este valor é ajustado em torno de -50^{o}C [44].

Para a detecção de fótons na região do infravermelho próximo, dois tipos principais de SPADs podem ser utilizados. Os detectores de germânio [45] foram inicialmente empregados para detecção em 1,3 μm, mas além de necessitarem ser operados sob temperatura criogênica (77 K) para redução do ruído, apresentam baixa eficiência em torno de 1,5 μm. Os SPADs baseados em InGaAs representam uma tecnologia madura e são facilmente encontrados para comercialização, adequando-se bem a sistemas de transmissão de fótons sobre fibra óptica [46][47]. Devido a seu maior ruído de escuro, quando comparados aos detectores de silício, os SPAD baseados em InGaAs, são geralmente operados em modo gatilhado [25][26][48][2]. Este modo de operação utiliza um

[2]Será visto no capítulo 4 que um artifício usualmente empregado para aumentar a taxa de gatilho de um SPAD consiste na minimização da corrente de avalanche através do dispositivo

gerador de pulsos de tensão acoplado ao circuito (linha pontilhada na figura 2.1a), que pode ser acionado por um oscilador interno ou um sinal externo. A tensão de polarização do fotodiodo é ajustada ligeiramente abaixo do limiar de ruptura. Quando o pulso elétrico é acionado, o APD fica momentaneamente acima da região de ruptura por um valor chamado tensão de excesso. Com o fim do pulso, a condição de polarização retorna ao estado inicial, como ilustrado na figura 2.1c. Durante esta janela temporal, um fóton pode ser detectado (ou uma contagem de escuro pode ser gerada), originando, à saída do SPAD, um pulso elétrico formatado. Além de permitir o sincronismo com outros elementos de um sistema, reduzindo o ruído, o modo gatilhado também permite o controle do tempo morto entre detecções através do ajuste da freqüência do gerador de pulsos. Este controle é especialmente importante quando a probabilidade de ocorrência do fenômeno dos pós-pulsos é relevante.

Este fenômeno pode ser compreendido da seguinte forma, quando uma avalanche ocorre, alguns portadores elétricos podem ficar presos em defeitos na estrutura do semicondutor. Estas armadilhas possuem um tempo médio de decaimento e, caso os portadores de carga sejam liberados durante o período subseqüente em que o dispositivo está apto a detectar um fóton, uma nova avalanche pode ser deflagrada. Como a probabilidade de decaimento é exponencial [48], existe uma maior probabilidade de ocorrência em intervalos de tempo mais próximos ao evento que originou a avalanche inicial. Se o tempo morto do detector for estendido além da constante de tempo, o efeito pode ser reduzido. Sendo o tempo de decaimento termicamente dependente, segundo a equação de Arrhenius [33], surge um compromisso entre a supressão das contagens de escuro termicamente geradas, as contagens de escuro devido a pós-pulsos e a taxa máxima de detecção do dispositivo.

Recentemente, progresso tem sido feito no sentido de estender a freqüência de operação de SPADs baseados em InGaAs. Basicamente, as técnicas desenvolvidas visam a redução do fenômeno de pós-pulso. Como o acúmulo de cargas é proporcional ao fluxo de corrente [41][40][27], deve-se evitar o preenchimento das armadilhas através de uma rápida supressão da avalanche. Um empecilho para tal se refere à resposta capacitiva do APD ao pulso de gatilho. O pulso elétrico é derivado pelo fotodiodo causando uma forte assinatura, presente em cada janela de detecção. Circuitos convencionais de polarização empregam um esquema de rejeição de modo comum composto por um circuito subtrator cujas entradas recebem os sinais de tensão oriundos do APD e de um capacitor equivalente, ambos submetidos ao sinal de gatilho [45][25]. Se uma janela de detecção for aberta e não houver evento de detecção, o sinal elétrico resultante fica abaixo do limiar do discriminador. No

caso oposto, em que uma avalanche ocorre, os sinais apresentam formas de onda diferentes, permitindo a discriminação do evento de contagem.

Duas técnicas principais podem ser empregadas para permitir a discriminação de avalanches de menor intensidade através da inibição da resposta transiente ao pulso elétrico. A técnica auto-diferencial permite um melhor casamento entre os sinais subtraídos por utilizar como referência uma réplica do pulso elétrico [49] ou óptico [50] gerado pelo APD em uma janela imediatamente anterior, devidamente atrasado. A supressão da avalanche assim que iniciada permite um menor acúmulo de cargas no detector. Outro método utiliza uma onda senoidal como gatilho e um filtro elétrico casado para mitigar a resposta transiente [51], visando o mesmo resultado final. Estes métodos, assim como técnicas híbridas [52] empregando características de ambos, permitem a extensão da freqüência de gatilhamento do dispositivo, com avanços significativos, especialmente em sistemas de distribuição quântica de chaves [53][54][55]. Além disso, a possibilidade de detecção de avalanches apresenta potencial para o desenvolvimento da capacidade de resolução do número de fótons em uma janela [56], estendendo a gama de aplicações dos SPADs.

2.2 Caracterização da janela temporal de detecção

Considerando módulos contadores de fótons baseados em APD operando em modo Geiger gatilhado, é necessária a caracterização de sua janela temporal de detecção. A largura efetiva da janela temporal dos SPADs foi calculada a partir da medição da curva de resposta temporal dos dispositivos. Para isso, foi utilizada uma fonte de fótons anunciados [3] [57] obtida através do processo de conversão paramétrica descendente espontânea (SPDC, do inglês *spontaneous parametric down-conversion*) de um fóton de bombeio em um par de fótons de menor energia. A energia e o momento do sistema devem ser conservados, de modo que os fótons gerados, chamados de *signal* e *idler*, apresentam forte correlação temporal, espectral e de polarização entre si. Detectando-se um fóton do par, tem-se um sinal elétrico indicativo da emissão do outro fóton em sua saída óptica, utilizado como fóton de prova.

No processo de SPDC, um fóton de bombeio é convertido em dois fótons de energia menor ao interagir com um cristal com não-linearidade de segunda ordem ($\chi^{(2)}$) não nula. Devido aos efeitos de *walk-off* apresentado em determinados cristais, é comum a utilização de estruturas do tipo *periodic poling* (PP). Isso significa que o índice de refração do cristal é modulado (de forma permanente) de modo que as três ondas (bombeio, *signal* e *idler*)

[3] Também chamada de fonte heráldica, do inglês *heralded single-photon source*

mantenham relação de fase entre si durante a propagação, tal que sinais gerados em diferentes pontos do cristal interfiram construtivamente, evitando seu cancelamento e contribuindo para a eficiência do processo. Obtém-se daí a condição conhecida como *quasi-phase matching*. O diagrama esquemático da fonte de fótons anunciados é mostrado na figura 2.2. O feixe de bombeio em

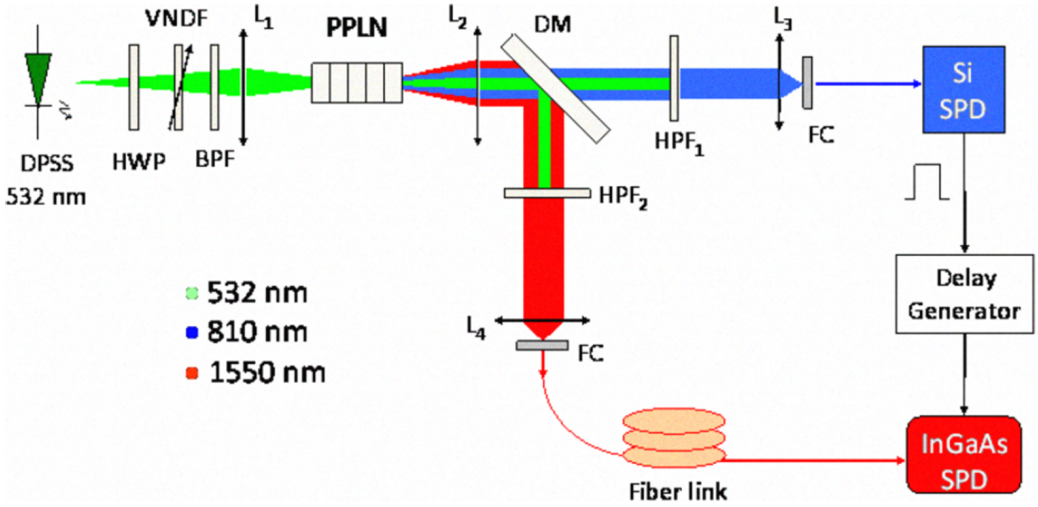

Figura 2.2: Fonte de fótons anunciados.

onda contínua (modo CW, do inglês *continuous wave*) de um laser Nd:YAG com comprimento de onda de 532 nm passa por uma lâmina de meia-onda (HWP, do inglês *half-wave plate*) para ajuste da polarização e é focalizado no cristal, do tipo PPLN (*periodicaly-poled Lithium Niobate*). Este, com 20 mm de comprimento, converte fótons de bombeio com uma determinada polarização em pares de fótons com comprimento de onda de 810 e 1550 nm com polarizações idênticas entre si e ortogonais ao bombeio. Um filtro do tipo vidro colorido (RG715) rejeita o comprimento de onda de bombeio e um espelho dicróico separa os fótons gerados, que são focalizados em fibras ópticas monomodo (para cada comprimento de onda) através de lentes asféricas. Os fótons em 810 nm são enviados para um detector de fótons únicos baseado em um APD de silício em modo *free-running*. Os pulsos elétricos de saída deste detector anunciam a existência do outro fóton do par, em 1550 nm, na saída óptica da fonte.

A caracterização da janela temporal de detecção dos SPADs foi feita através da varredura temporal relativa dos fótons anunciados, utilizando-se a configuração mostrada na figura 2.3.

Um gerador de atraso elétrico é utilizado para variar a relação temporal entre o sinal de gatilho e o fóton de prova, este atrasado por uma bobina de fibra óptica de alguns metros. Isto permite a variação do atraso elétrico do sinal de gatilho e a incidência dos fótons de prova em diferentes posições

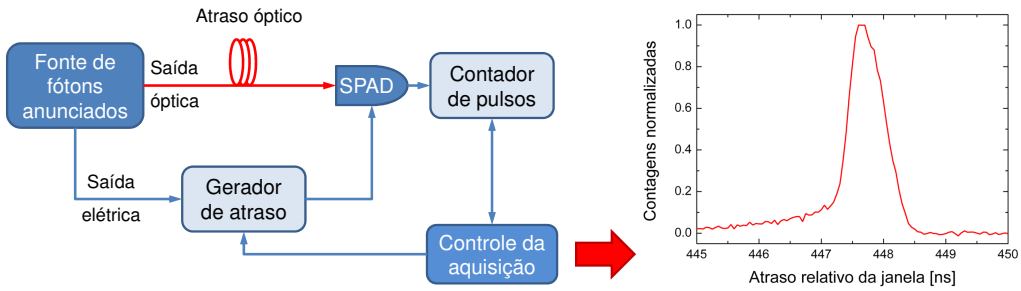

Figura 2.3: Caracterização da janela de detecção dos SPAD. O final da janela está localizado à esquerda da curva.

temporais da janela de detecção. Durante a varredura do sinal de gatilho, o número de contagens por intervalo de tempo, medido através de um contador de pulsos, é armazenado, resultando no mapeamento da janela de detecção do SPAD. A figura 2.3 mostra a medição de uma curva típica com a resposta do detector ao longo da janela de detecção (observe que o final da janela está à esquerda da figura, devido à sua varredura em relação aos fótons de prova). Pode-se observar que a largura da janela é menor que o valor nominal indicado pelo detector, neste caso 2,5 ns. O valor médio da linha base de ruído é calculado na região temporal anterior à janela, sendo removida da medição, que é então normalizada em relação ao valor máximo. O valor efetivo da largura da janela temporal é calculado através da razão entre a área da medida e a área correspondente a uma janela retangular com amplitude unitária, multiplicada pelo intervalo temporal de medição. Observar que o tempo de coerência entre os fótons de um par gerado por conversão paramétrica descendente neste tipo de arranjo é tipicamente menor que ps [58], tornando desnecessária a deconvolução em relação ao valor final.

A largura efetiva da janela varia para diferentes configurações de eficiência do detector. A alteração deste parâmetro é feita através de ajuste na tensão de polarização do APD e associada à indicação nominal no *display* do equipamento. A 2.4 mostra as curvas normalizadas da janela temporal de detecção de um dos detectores para diferentes valores de eficiência configurados (10%, 15% e 20%) com janela nominal de 2,5 ns (figura 2.4a) e a comparação entre as janelas de 2,5 e 5,0 ns com mesma eficiência nominal de 15%.

A tabela 2.1 abaixo mostra os resultados da caracterização da janela de detecção dos três SPADs, obtidos em diferentes configurações de eficiência de detecção e de largura nominal da janela.

Apesar de uma fonte heráldica ter sido utilizada, um pulso óptico curto, sincronizado com as janelas de detecção poderia ser utilizado. De forma semelhante, um gerador de atraso elétrico permitiria sua varredura em relação à janela. Um pulso óptico de 0,8 ns foi utilizado para verificação da medida

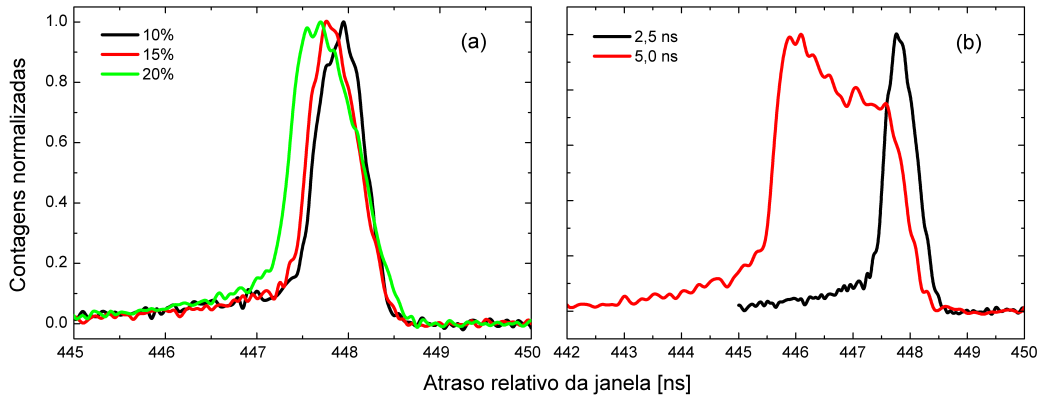

Figura 2.4: Comparação entre medições da janela do detector com diferentes (a) ajustes da eficiência nominal de detecção e (b) largura temporal nominal.

Janela nominal [ns]	Eficiência nominal [%]	Janela efetiva [ns]		
		D_1	D_2	D_3
2,5	10	0,76	0,64	0,63
	15	0,77	0,77	0,81
	20	0,99	1,04	1,12
5	10	2,04	1,99	2,19
	15	2,24	2,24	2,26
	20	2,93	3,10	2,97

Tabela 2.1: Largura efetiva da janela temporal de detecção dos SPADs sob diferentes condições.

anterior. Foi feita a varredura de D_1, este operado com valores nominais de janela e eficiência de 2,5 ns e 10%, respectivamente. Considerando o pulso óptico como gaussiano, obteve-se valor compatível (0,76 ns), dentro da resolução apresentada, após sua deconvolução.

Para um laser atenuado, a probabilidade de se encontrarem n fótons em um intervalo de tempo, dado que haja μ fótons em média no mesmo intervalo, é dada pela distribuição de Poisson [60]

$$P(n,\mu) = e^{-\mu}\mu^n/n. \tag{2-1}$$

A potência óptica correspondente é dada pela energia quantizada de μ fótons no intervalo de tempo Δt do pulso ou da janela de detecção, ou seja,

$$P_{opt} = \mu h\nu/\Delta t\,, \tag{2-2}$$

onde ν é a freqüência óptica do sinal e h é a constante de Planck. Para valores muito pequenos de μ, a probabilidade de ocorrência de intervalos de tempo vazios (estados vácuo) passa a ser significativa. Por exemplo, para um número médio de 0,1 fótons por pulso óptico (ou janela de detecção), a probabilidade de não serem encontrados fótons é dada por $\mathrm{P}(0,0.1) = \mathrm{e}^{-0.1} = 90,48\%$. É

interessante notar que apenas 0,47% dos intervalos terão, estatisticamente, múltiplos fótons, enquanto que o complemento terá um único fóton [4]. Porém, se o valor de μ se elevar, a probabilidade de intervalos com pelo menos um fóton rapidamente satura em 100%, o que ocorre em torno de 450 pW para λ=1550 nm e Δt=2,5 ns.

2.3 Método e modelo para caracterização dos dispositivos

O método de caracterização proposto [5] é baseado na análise da distribuição estatística dos intervalos de tempo entre detecções consecutivas no SPAD [36], permitindo a extração simultânea e em tempo real de alguns parâmetros do dispositivo. Considerando detectores operando em modo Geiger gatilhado, assume-se que fora da duração temporal da janela de detecção não pode haver detecção de fótons, mesmo que o dispositivo seja submetido a uma fonte óptica no regime CW. Assim, o SPAD estará inativo na maior parte do tempo, uma vez que a freqüência típica de operação destes detectores é limitada em MHz e a duração típica de uma janela é da ordem de ns.

Neste caso, podemos definir os intervalos de tempo como múltiplos inteiros m do período de gatilho T. Dado que ocorreu um evento inicial de detecção, registra-se o tempo decorrido, em número de janelas gatilhadas [5] , até o próximo evento de detecção, não importando sua origem – se devido a um fóton incidente ou uma falsa contagem. O tempo entre este segundo evento e a próxima contagem é novamente medido e assim por diante até que se obtenha o número desejado de amostras. A figura 2.5 ilustra o princípio de aquisição dos tempos, com m=2 janelas abertas entre os dois primeiros eventos, m=4 janelas entre o segundo e o terceiro e m=M janelas entre a terceira e a quarta contagem.

A estatística de tempos entre detecções consecutivas é então representada na forma de um histograma que, após normalização, equivale à função distribuição de probabilidades do detector sob aquela condição de operação.

De acordo com a figura 2.5, a variável aleatória m assume o valor M caso ocorra, a partir do evento de referência, uma contagem na M-ésima janela aberta, precedida por M-1 janelas vazias, ou seja, sem registro de contagem.

[4] A distribuição estatística do número de fótons emitidos por uma fonte poissoniana é de fundamental importância em protocolos de distribuição quântica de chaves, como será discutido a partir do capítulo 3. A Eq.2-1 ilustra o compromisso entre a redução da probabilidade de emisão de pulsos contendo múltiplos fótons e pulsos de vácuo.

[5] No caso de detectores operando no modo *free-running*, eventos de detecção podem ocorrer em qualquer instante, a menos de um período morto imediatamente após uma contagem. De modo semelhante à aplicação das janelas de gatilho, o tempo morto do detector diminui sua taxa máxima de contagem, reduzindo, porém, a probabilidade de ruído ocasionado por pós-pulsos.

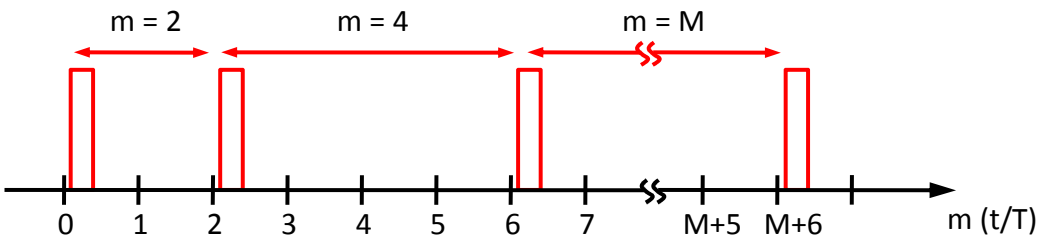

Figura 2.5: Aquisição dos tempos entre eventos consecutivos de detecção.

A probabilidade de ocorrer um determinado intervalo de tempo m pode então ser escrita em função da probabilidade de não ocorrência de contagem em todo o intervalo x ($P_{nc}(x)$), correspondendo aos *time-slots* variando de 1 a (m-1), de acordo com

$$P(m) = [1 - P_{nc}(m)] \prod_{x=1}^{m-1} P_{nc}(x)\,. \tag{2-3}$$

Um *time-slot* vazio significa que não houve detecção de fóton (P_{nf}), nem contagem de escuro (1-P_d) ou registro de pós-pulso (1-$P_a(x)$), este último dependente do tempo x decorrido deste o evento de referência, ou seja,

$$P_{nc}(x) = P_{nf}(1 - P_d)[1 - P_a(x)]\,. \tag{2-4}$$

A probabilidade de serem encontrados n fótons em um pulso laser atenuado com μ fótons em média é um processo estocástico dado pela distribuição de Poisson, mostrada na equação (2-1). Logo, a probabilidade de não ocorrência de detecção de um fóton em uma janela será dada por

$$P_{nf}(0, \mu\eta) = e^{-\mu\eta}\,, \tag{2-5}$$

onde foi incluída a eficiência de detecção η.

Assumindo uma constante de tempo predominante τ [35][33] para os portadores armadilhados no semicondutor, a probabilidade de ocorrência de um evento de pós-pulso dependerá do decaimento exponencial dado por

$$P_a(m) = P_0 e^{-mT/\tau}\,, \tag{2-6}$$

onde P_0 é uma amplitude proporcional ao número de armadilhas preenchidas.

Substituido a equação (2-4) em (2-3), obtém-se

$$\begin{aligned} P(m) \;\; = \;\; & \{1 - P_{nf}(1 - P_d)[1 - P_a(m)]\} \\ & [P_{nf}(1 - P_d)]^{m-1} \prod_{x=1}^{m-1} [1 - P_a(x)]\,, \end{aligned} \tag{2-7}$$

que pode ser reescrita incorporando as definições (2-5) e (2-6), resultando em

$$P(m) = \{1 - e^{-\mu\eta}(1 - P_d)[1 - P_0 e^{-mT/\tau}]\} \\ [e^{-\mu\eta}(1 - P_d)]^{m-1} \prod_{x=1}^{m-1} [1 - P_0 e^{-xT/\tau}] \,. \quad (2\text{-}8)$$

O produtório no fim da equação (2-8) reflete a dependência temporal da probabilidade de pós-pulso. Considera-se aqui que cada avalanche recarrega as armadilhas, restaurando a probabilidade inicial de pós-pulso P_a. Expandindo o produtório em uma série, chega-se a

$$\prod_{x=1}^{m-1} [1 - P_0 e^{-xT/\tau}] = 1 - \alpha + \beta \,, \quad (2\text{-}9)$$

onde α e β correspondem aos termos de primeira e segunda ordem em P_0, dados por

$$\alpha = \frac{P_0 e^{-\frac{T}{\tau}}}{e^{-T/\tau} - 1} (e^{-\frac{T}{\tau}(m-1)} - 1) \,. \quad (2\text{-}10)$$

$$\beta = \frac{P_0^2}{e^{-T/\tau} - 1} \quad \left\{ \frac{e^{-\frac{T}{\tau}(m+1)}(e^{-\frac{T}{\tau}(m-2)} - 1)}{e^{-T/\tau} - 1} \right. \\ \left. - \frac{e^{-3\frac{T}{\tau}}(e^{-2\frac{T}{\tau}(m-2)} - 1)}{e^{-2T/\tau} - 1} \right\} . \quad (2\text{-}11)$$

O termo de terceira ordem também foi obtido de forma analítica. Entretanto, sua influência sobre o resultado final foi analisada e considerada desprezível. A probabilidade total de ocorrência de pós-pulsos (P_T) é obtida através do somatório de $P_a(m)$ de 1 até ∞, resultando em

$$P_T = \sum_{m=1}^{\infty} P_a(m) = P_0 \frac{1}{e^{T/\tau} - 1} \,. \quad (2\text{-}12)$$

A equação resultante de (2-8) a (2-11) é ajustada ao histograma, normalizado de forma que a área sob a curva seja unitária. Na verdade, aplica-se o logaritmo na base 10 ao histograma normalizado e ao modelo antes do ajuste da curva, para obter-se melhor sensibilidade em relação aos pontos distantes da origem do eixo dos tempos, em se tratando de eventos predominantemente exponenciais. A figura 2.6 mostra um histograma de tempos típico e o ajuste do modelo a um SPAD comercial operando em modo gatilhado. O detalhe destacado na figura mostra os primeiros *bins*, que apresentam um comportamento peculiar, devido ao efeito de pós-pulsos. Uma discussão mais detalhada será feita adiante.

2.4

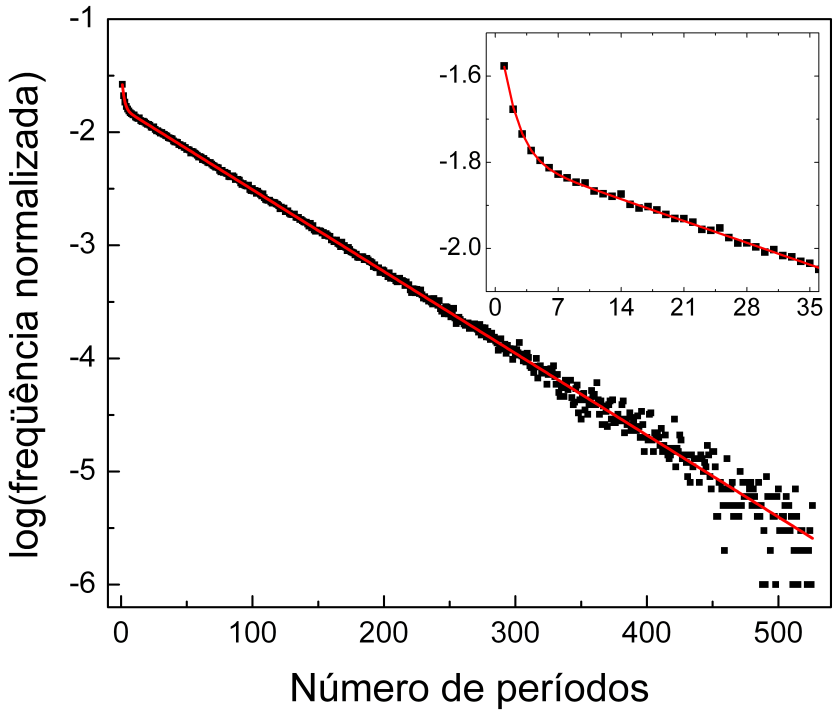

Figura 2.6: Aquisição dos tempo entre eventos consecutivos de detecção em um SPAD com o modelo desenvolvido ajustado. O detalhe da figura mostra uma ampliação da região inicial.

Arranjo experimental

O arranjo experimental para a caracterização dos SPADs através da medição e análise dos intervalos de tempo entre eventos de detecção é mostrado na figura 2.7. Os experimentos de caracterização dos SPADs foram realizados com um diodo laser (DL) operando em modo CW e emitindo na janela de telecomunicações, em 1550 nm. A saída fibrada do laser é conectada a um atenuador óptico variável (AOV), com o qual é possível ajustar o número médio de fótons por intervalo de tempo, auxiliado por um medidor de potência óptica. A saída do atenuador é então conectada ao SPAD sob caracterização, gatilhado por um sinal periódico fornecido por um gerador de pulsos. Ambos os sinais de detecção e de gatilho são amostrados por um conversor A/D de 100 MSamples/s conectado a um computador.

Três SPADs comerciais (D_1, D_2 e D_3) foram caracterizados. Para cada série de medição, foram ajustados os parâmetros internos do detector (eficiência e largura da janela de detecção) e as condições operacionais (freqüência de gatilho f e o número médio de fótons por janela μ). Os dados de cada série foram continuamente aquisitados e processados em tempo real através de um programa desenvolvido, que os agrupa em um histograma. Os parâmetros de

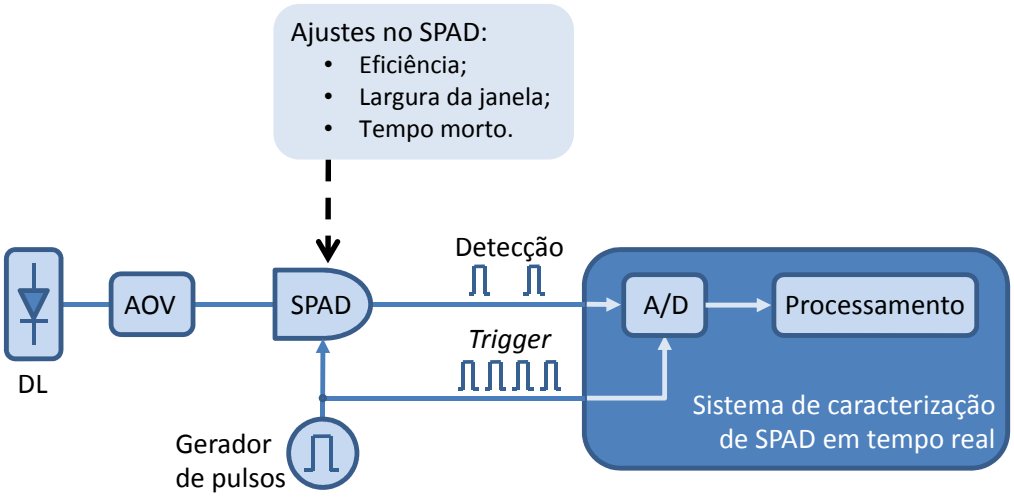

Figura 2.7: Arranjo experimental para aquisição dos intervalos entre detecções.

interesse do detector são obtidos através do ajuste do modelo apresentado aos dados de medição.

2.5 Resultados

Foram realizadas medidas de caracterização dos três SPADs variando-se a freqüência em 200, 400, 600, 800 e 1000 kHz e o número médio de 0,04, 0,08, 0,16 e 0,32 fótons por janela efetiva de detecção. Em todas as combinações foi utilizada a mesma largura da janela de detecção nominal em 5 ns com eficiência nominal de 15% e foram medidos 2×10^6 pontos para cada detector.

Na primeira série apresentada, o número médio de fótons μ foi fixado em 0,08 por janela efetiva, variando-se a freqüência de gatilho. O logaritmo dos histogramas normalizados das medidas de D_2 podem ser vistos na figura 2.8, agrupados por freqüência, sendo mostrados os pontos experimentais e a curva ajustada. O eixo das abscissas mostra o número de janelas consecutivas abertas entre detecções, valores múltiplos do período de repetição. Nos detalhes das figuras são mostrados os pontos iniciais, em escala ampliada, ficando evidente a presença de uma região inicial com maior inclinação. Este comportamento é atribuído à tendência de ocorrência de pós-pulsos logo após um evento de detecção, devido à sua dependência temporal, o que é indicado pelo aumento da contribuição da região de pós-pulsos com o aumento da freqüência de repetição. Isto se deve à redução do período de gatilho, que causa maior amostragem dos instantes de tempo em que as armadilhas apresentam maior probabilidade de emissão de carga.

A probabilidade de pós-pulsos obtida para os três detectores foi promediada para cada freqüência sobre a variação de μ, com os resultados apresentados

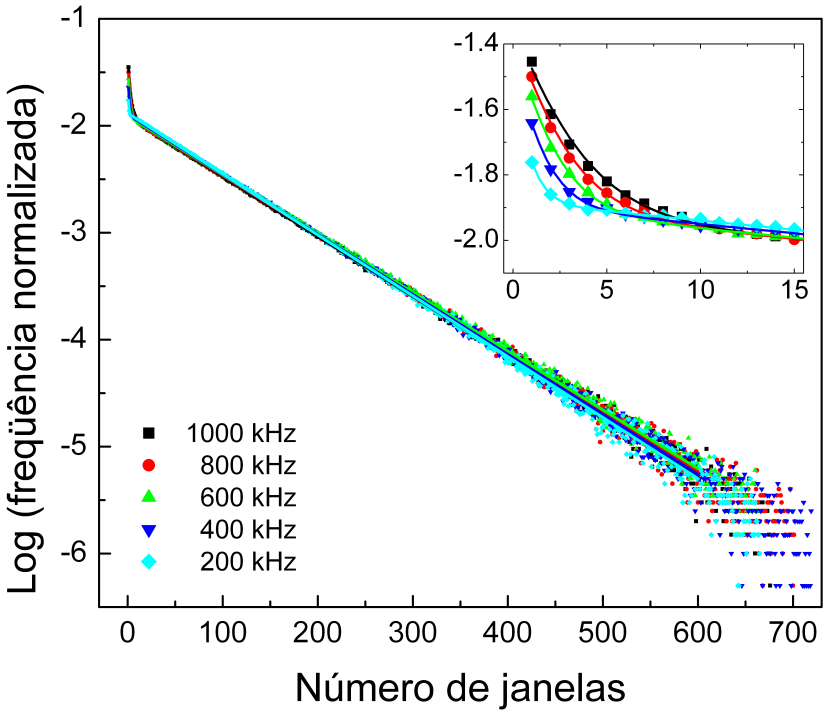

Figura 2.8: Histogramas de medições realizadas com μ fixo e diferentes valores de freqüência de gatilho com o modelo desenvolvido ajustado. O detalhe da figura mostra uma ampliação da região inicial.

na tabela 2.2.

Após o joelho da curva, segue uma região com inclinação mais suave (também exponencial, na escala linear), que corresponde aos eventos de detecção de fótons, que são independentes do tempo. A inclinação da curva (logarítmica) está diretamente relacionada ao produto $\mu\eta$ e praticamente não se altera com a freqüência de gatilho, quando observam-se as curvas superpostas em função do número de janelas. Cabe ressaltar que, caso os histogramas sejam representados em função do tempo, não haverá superposição das curvas, de forma que freqüências de gatilho maiores tornam os histogramas mais inclinados.

A segunda série de medição apresentada foi feita com a freqüência de janela fixa em 600 kHz e com μ variando. O comportamento geral dos histogramas resultantes, mostrados na figura 2.9, é similar ao das curvas da figura anterior.

Entretanto, com a variação do número médio de fótons por janela, a inclinação das curvas varia. Este comportamento é explicado pela própria definição de tempo entre eventos, pois para que um determinado intervalo ocorra, é necessário que não ocorra contagem em nenhuma janela aberta desde o evento de referência. Logo, esta probabilidade se reduz para intervalos de

Freqüência de gatilho [kHz]	Probabilidade de pós-pulsos [%]		
	D_1	D_2	D_3
200	0,56±0,03[1]	1,12±0,05	0,67±0,03
400	1,79±0,05	3,62± 0,08	2,10±0,03
600	3,28±0,08	6,47±0,08	3,81±0,08
800	4,83±0,22	9,98±0,31	5,72±0,15
1000	6,47±0,19	13,52±0,36	7,71±0,27

[1] Valores percentuais: média ± desvio-padrão.

Tabela 2.2: Probabilidade de pós-pulso (em %) em cada SPAD para diferentes freqüências de gatilho.

tempo maiores. O aumento de μ torna mais provável a ocorrência de dois eventos gerados pela detecção de fótons com intervalo de tempo mais curto, tornando mais abrupta a região de decaimento lento das curvas. No caso limite em que são detectados fótons em todas as janelas, o histograma se resumiria em um simples ponto.

Os valores finais para a eficiência de detecção e para a probabilidade de contagem de escuro dos SPAD foi calculada tomando a média de todas as séries, totalizando 20 valores para cada parâmetro. Estes resultados são mostrados na tabela 2.3. Os resultados obtidos foram validados através de

SPAD	η[%]	P_d ($\times 10^{-4}$)
D_1	15,10±0,15[1]	1,6±0,8
D_2	15,07±0,09	2,1±0,9
D_3	15,03±0,03	1,8±0,8

[1] Média ± desvio-padrão.

Tabela 2.3: Eficiência de detecção e probabilidade de contagem de escuro medidas para cada SPAD.

medições individuais especializadas, como mostrado a seguir.

2.5.1 Validação dos resultados

A probabilidade de ocorrência de contagens de escuro nos SPAD foi obtida individualmente, como forma de validação do método de caracterização desenvolvido. Os detectores foram gatilhados por um gerador de pulsos com taxa de repetição constante de 10 kHz. Cada pulso abre uma janela de detecção, cujo valor nominal é ajustado previamente. A taxa de gatilho do detector foi ajustada de forma a minimizar os efeitos de pós-pulsos no detector [35]. O período correspondente, de 100 μs, é muito maior que o tempo de decaimento das armadilhas, da ordem de poucos μs, permitindo seu escoamento entre duas janelas consecutivas de detecção. Foram monitoradas as freqüências de gatilho

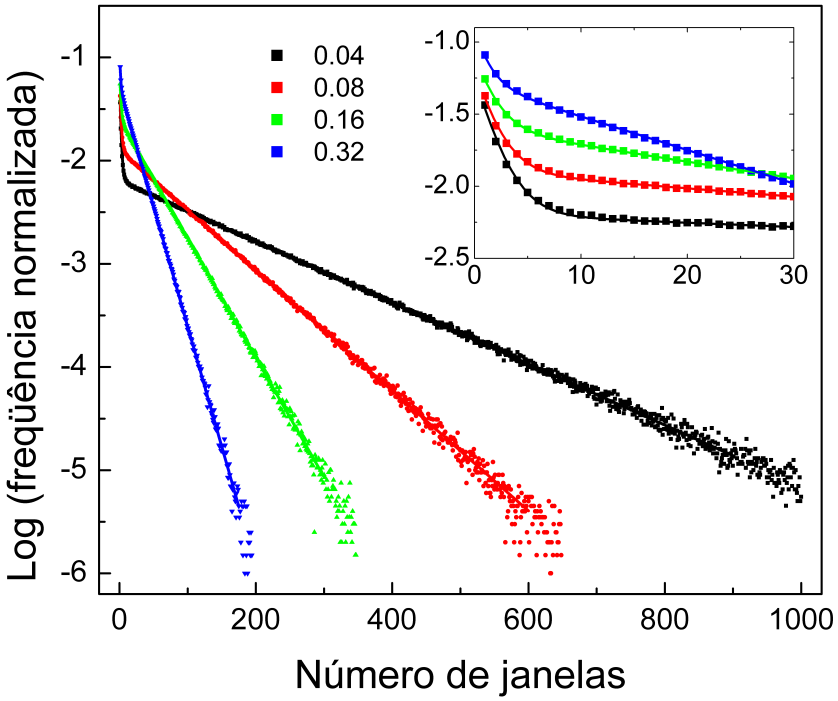

Figura 2.9: Histogramas de medições realizadas com freqüência de gatilho fixa em 600 kHz e diferentes valores de número médio de fótons μ com o modelo desenvolvido ajustado. O detalhe da figura mostra uma ampliação da região inicial.

e de contagem de eventos durante dez intervalos de 20 s para cada detector. A probabilidade de ocorrência de contagem de escuro por janela de detecção foi calculada para D_1, D_2 e D_3 como a razão entre os valores médios da taxa de contagens (C) e a freqüência de gatilho (G), resultando em $1,1 \times 10^{-4}$, $1,5 \times 10^{-4}$, e $1,2 \times 10^{-4}$, com desvio-padrão de $0,5 \times 10^{-4}$.

Os valores de eficiência de detecção foram verificados ajustando-se um valor conhecido para a potência óptica incidente de modo a obter determinado número médio de fótons por janela. A razão média das contagens medidas (C) em relação à freqüência de gatilho (G) foi calculada. Novamente foi escolhida uma taxa de repetição de gatilho de 10 kHz, para minimizar os efeitos de pós-pulsos. A partir da distribuição de Poisson, a eficiência de detecção pode ser escrita como

$$\eta = -\frac{1}{\mu} ln(1 - C/G + P_d)\,. \tag{2-13}$$

.

A verificação da probabilidade de pós-pulsos foi feita através de comparação com o método das áreas da FDP. É feito um ajuste linear ao decaimento lento do histograma normalizado – em escala logarítmica –, desprezando a região à esquerda do joelho da curva, correspondente aos pontos

iniciais associados aos eventos de pós-pulsos. Na figura 2.10 são mostradas as áreas separadas pela reta ajustada aos dados experimentais. A região hachu-

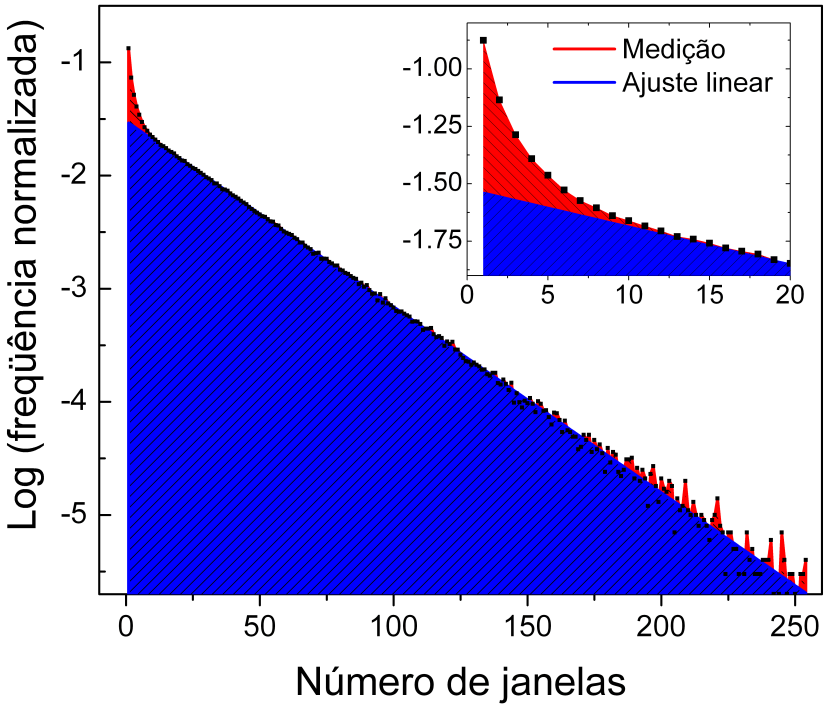

Figura 2.10: Extração da probabilidade de pós-pulsos pela área da FDP. Em vermelho, a região relacionada ao fenômeno. O detalhe da figura mostra uma ampliação da região inicial.

rada em vermelho apresenta a área correspondente à probabilidade unitária e é delimitada pelos pontos experimentais. A área azul é delimitada pela extrapolação da curva ajustada, e seu complemento representa a contribuição de pós-pulsos, cuja probabilidade é dada por este valor. A razão entre os valores calculados através do método da área e os resultados da caracterização pelo método proposto foi maior que 97,8%, indicando boa concordância do modelo desenvolvido.

2.5.2 Caracterização de SPADs em tempo real

Para atestar a eficácia do método proposto para caracterização de SPADs em tempo real, foram feitas 20 séries consecutivas de medição nas mesmas condições de operação, com o ajuste do modelo e extração dos parâmetros de interesse. O número de pontos destas séries foi variado e a estatística dos parâmetros foi obtida. A figura 2.11 mostra o fator de qualidade médio do ajuste do modelo (R^2) em função do número de amostras em cada série. O aumento no número de pontos amostrados resulta em um melhor casamento

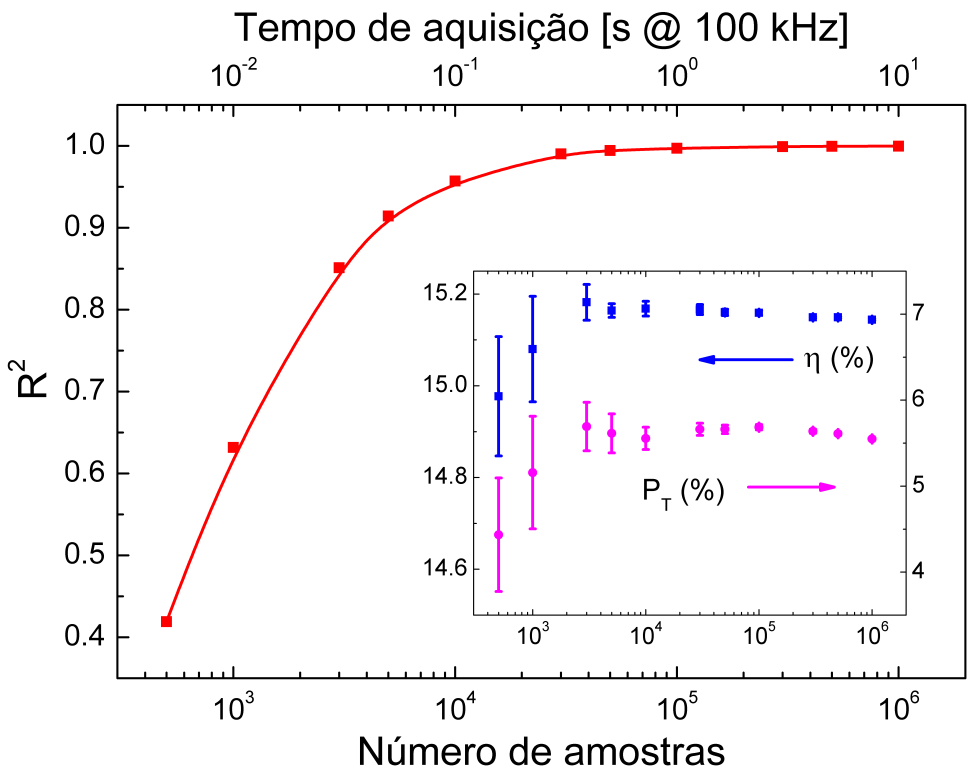

Figura 2.11: Qualidade do ajuste do modelo aos dados experimentais em função do número de pontos medidos (a linha é apenas uma referência visual). No detalhe, os valores médios dos parâmetros extraídos para eficiência de detecção (η) e probabilidade de pós-pulso (P_T).

entre o modelo e os dados medidos. Para séries com 3×10^5 pontos em cada curva, obteve-se um valor de R^2 melhor que 0,99, com este valor aumentando para 0,999 ao incrementar em uma ordem de grandeza o comprimento das série. O detalhe da figura mostra a evolução dos valores médios da eficiência de detecção e da probabilidade de pós-pulsos em função do tamanho das séries. Mesmo para 3×10^3 amostras, obtém-se um desvio-padrão experimental da média de 0,26% para a eficiência e de 5,0% para a probabilidade de pós-pulsos. O eixo horizontal superior indica o tempo de medição necessário para acumular determinado conjunto estatístico considerando uma taxa de detecção de 100 kHz.

Os resultados corroboram a aplicação do método para medição em tempo real. No próximo capítulo, será discutida uma aplicação do método de caracterização para o monitoramento dos SPAD de um sistema de distribuição quântica de chaves contra possíveis intervenções externas que poderiam comprometer a segurança da comunicação.

3
Monitoramento dos detectores de fótons únicos em sistemas de distribuição quântica de chaves

Dado que duas partes comunicantes – aqui chamados de Alice e Bob – possuem cópias idênticas de uma chave criptográfica, uma mensagem ininteligível para uma terceira parte não-autorizada (chamada de Eva [1]) – mas não para eles – pode ser gerada. O protocolo de criptografia de chave privada conhecido como *one-time pad*, ou cifra de Vernam [61], foi provado como seguro em 1949 [62], desde que a chave tenha sido aleatoriamente gerada e que seja utilizada apenas uma vez. Entretanto, é necessário que a chave seja previamente compartilhada por ambas as partes, o que pode representar um problema logístico. Uma solução para este problema foi apresentada em 1984, e ficou conhecida como criptografia quântica [6].

A assim chamada distribuição quântica de chaves (QKD, do inglês *quantum key distribution*)[6][7][2] permite o compartilhamento seguro de uma chave criptográfica entre duas partes comunicantes remotamente localizadas. Esta chave é formada por uma seqüência aleatória de bits e pode ser posteriormente utilizada na encriptação de uma mensagem a ser transmitida de forma sigilosa. Os portadores de informação enviados de Alice para Bob são estados quânticos gerados de acordo com o protocolo de comunicação. Sendo os fótons a escolha natural para comunicação à distância, pode-se escolher, em princípio, dentre diversos graus de liberdade destas partículas para a codificação dos qubits (acrônimo de *quantum bits*), como o estado de polarização ou a fase[2]. De forma geral, cada fóton é aleatoriamente preparado por Alice de acordo com um conjunto de bases em um determinado estado quântico, que é enviado através do canal óptico. Para cada qubit, Bob escolhe, também aleatoriamente, dentre diferentes bases de medição e registra um evento de contagem em um de seus detectores de fótons únicos, ao qual é associado um bit de comunicação.

Seguindo o pioneiro protocolo BB84 [6], são definidas duas bases canonicamente conjugadas de vetores ortogonais em um espaço de Hilbert bidimensional. No caso de codificação por polarização, podem ser escolhidos os estados

[1] O nome "Eva" é tradução de "Eve", que vem de um jogo fonético com a palavra inglesa *eavesdropper* (espião)

de polarização horizontal e vertical como os auto-vetores de uma base (base $\oplus$) e os estados diagonais -45^o e +45^o para compor a segunda (base $\otimes$). Em cada base, os estados são associados aos bits 0 e 1 – por exemplo, $|H\rangle \rightarrow 0$; $|V\rangle \rightarrow 1$; $|-45\rangle \rightarrow 0$; $|+45\rangle \rightarrow 1$, como ilustrado na figura 3.1. Cada qubit a ser

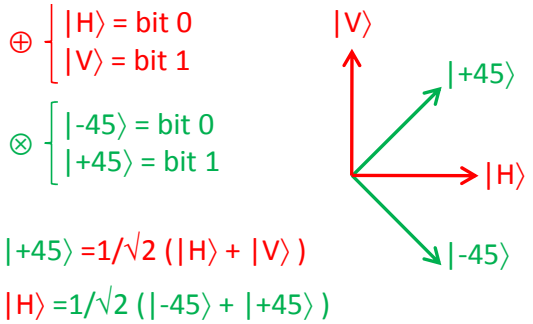

Figura 3.1: Representação das bases de codificação e da associação entre bits e estados quânticos para o protocolo BB84 com codificação em polarização.

enviado é codificado em um dos quatro estados de acordo com o bit e a base escolhidos por Alice (ambos aleatoriamente). Ao receber um fóton, Bob deve escolher, também aleatoriamente, a base de medição ($\oplus$ ou $\otimes$), por exemplo girando o estado de polarização de entrada em relação à base definida pelo seu aparato de medição. No caso de coincidência entre as bases de preparação e medição, o qubit recebido por Bob sempre será um auto-estado do operador que representa a medida e o resultado será determinístico. Caso contrário, o estado será colapsado em um dos vetores que compõem a base de medição e o resultado será aleatório. Como exemplo, caso o qubit $|H\rangle$ seja medido na base $\otimes$, o resultado terá a forma $1/\sqrt{2}(|-45\rangle + |+45\rangle)$, ou seja, terá 50% de probabilidade de ser observado como um bit 0 e 50% de probabilidade de ser observado como um bit 1.

A segurança incondicional atribuída à distribuição quântica de chaves baseia-se nos fundamentos da física quântica [2][10][8]. Qualquer tentativa realizada por uma parte não-autorizada de medição do estado quântico enviado de Alice para Bob o destruirá[2] (o estado será colapsado ao se projetar na base de medição de Eva), sem necessariamente revelar a informação contida. Além disso, diferente de bits clássicos (como pulsos elétricos), não é possível copiar um estado quântico desconhecido de forma determinística (teorema da não-clonagem [63],[64]). Intervenções externas ou tentativas de replicação dos qubits acarretam no aumento da taxa de erro do sistema (QBER, do inglês *qubit error-rate*) e podem revelar o ataque, como será visto adiante.

[2]Excetuando-se as medidas do tipo QND (do inglês *quantum non-demolition measurement*)[65]

Entretanto, apesar da comprovação teórica da segurança absoluta, mesmo assumindo que Eva possui acesso a qualquer tecnologia fisicamente realizável, certas características da tecnologia atual podem ser exploradas por um interceptador sem que este seja necessariamente revelado. A utilização destas imperfeições nos sistemas e dispositivos utilizados para QKD é chamada de *quantum hacking* [66], em alusão aos ataques clássicos em redes e sistemas de computadores convencionais. Um dos principais focos de ataques desta natureza é o detector de fótons únicos, especialmente os construídos através da amplamente difundida tecnologia baseada em fotodiodos avalanche[3]. Diversos esquemas foram propostos e implementados, inclusive ataques completos atuando em sistemas de distribuição quântica de chaves comerciais [66]. Para cada *loophole* encontrado uma série de contra-medidas é geralmente proposta. Entretanto, as alterações implementadas em um sistema ou dispositivo podem causar novas aberturas para outros ataques ou comprometer determinadas características, como a redução na eficiência de detecção ao se colocar um divisor óptico com um medidor de potência à entrada do SPAD na tentativa de identificar pulsos forte [67].

Este capítulo apresenta uma proposta de contra-medida para determinados ataques ao detector contador de fótons em sistemas de QKD. O sistema de caracterização em tempo real discutido no capítulo anterior é aplicado para monitorar os parâmetros de um SPAD durante sua utilização na distribuição de chaves. O método não-invasivo permite identificar a tentativa de manipulação do sistema através da assinatura deixada pelo interceptador nos detectores. Um sistema experimental foi montado e a eficácia da proposta foi testada contra o ataque *aftergate* [13] e contra o ataque *timeshift* [14], com resultados favoráveis à segurança da comunicação. Serão também discutidos os resultados obtidos contra uma variação do primeiro ataque, chamado *faint aftergate* [68], e apresentadas algumas considerações acerca da potencial aplicação do método de monitoramento em relação a outros protocolos de ataque.

3.1 Distribuição quântica de chaves e "quantum hacking"

Primeira aplicação direta da física quântica, a criptografia quântica tem origem no conceito abstrato de "dinheiro quântico", apresentado por Wiesner (e tardiamente publicado em [69]) aos autores do protocolo BB84, referindo-se a cédulas monetárias a prova de falsificação e envolvia a medição de um estado quântico superposto. Em 1984, C. Bennett e G. Brassard apresentaram uma aplicação prática deste conceito na forma do primeiro protocolo desta nova

[3]Recentemente ataques foram propostos contra detectores supercondutores [70]

tecnologia [6]. Paralelamente, em 1991, A. Ekert desenvolveu idéia semelhante, porém baseando-se em estados quânticos emaranhados. O protocolo E91 [7] utiliza uma fonte de pares de fótons emaranhados em algum grau de liberdade (como a polarização), que são enviados para as duas partes comunicantes. Após a medição de cada fóton em uma base aleatoriamente escolhida, é testada a violação da desigualdade de Bell como forma de verificação da segurança do processo. O primeiro sistema experimental, baseado no protocolo BB84, foi publicado em 1992 [71], com a transmissão de fótons codificados em polarização através de uma distância de 32 cm em laboratório. Hoje, além de sistemas experimentais implementados sobre centenas de quilômetros [46][47], versões comerciais são oferecidas por diferentes fabricantes (por exemplo, MagiQ ou idQuatique). Um marco da maturidade desta tecnologia ocorreu em 21 de outubro de 2007, quando um enlace criptográfico utilizando QKD foi estabelecido nas eleições suíças [72].

Este desenvolvimento tecnológico beneficiou-se da vasta gama de componentes ópticos utilizados em sistemas clássicos de telecomunicações e, além disso, impulsionou o desenvolvimento de outras tecnologias correlatas, como as fontes de fótons únicos [73][74], geradores de números verdadeiramente aleatórios [75][76], sistemas de controle e estabilização de propriedades do canal óptico – como polarização [77][78][79] e fase [80], além do próprio detector de fótons únicos.

A codificação dos qubits pode ser feita em diferentes graus de liberdade de um fóton, como estado de polarização [6][81], posição temporal (*time-bin*) [82][83][84] ou fase relativa das bandas laterais de um pulso modulado [85][86][87]. A figura 3.2 apresenta um esquema prático genérico de distribuição quântica de chaves sobre fibra óptica com codificação em polarização. No protocolo BB84 [6] o estado quântico de cada qubit a ser enviado é esco-

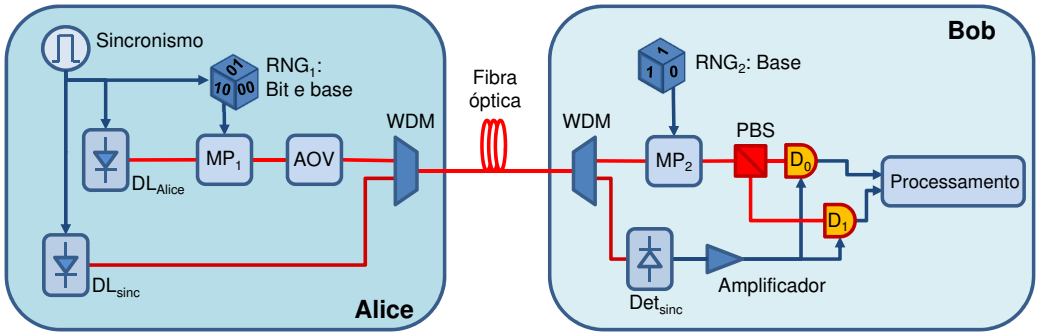

Figura 3.2: Exemplo de implementação prática de um sistema QKD baseado no protocolo BB84 com codificação em polarização.

lhido aleatoriamente dentre quatro possibilidade, de acordo com o bit e a base

aleatoriamente sorteados. Geradores verdadeiramente aleatórios, baseados em eventos quânticos podem (e devem) ser utilizados, em contra-ponto aos geradores pseudo-aleatórios, cujo valor futuro é determinável *a priori*, dado que se conheça o índice atual da máquina de estados. Um modulador eletro-óptico de polarização (MP_1) pode ser utilizado para girar o estado de polarização dos pulsos ópticos provenientes do laser DL_{Alice}. A potência óptica do sinal é ajustada através de um atenuador óptico variável (AOV) de modo que tenha, em média, em torno de 0,1 fóton por pulso. Segundo a distribuição de Poisson, este valor resulta em menos de 0,5% de pulsos contendo múltiplos fótons, às custas de 90,5% de pulsos de vácuo[4].

Em adição ao sinal quântico, Alice deve enviar um sinal de sincronismo para Bob, o que pode ser feito através da mesma fibra óptica utilizando a técnica de multiplexação óptica no domínio do comprimento de onda (WDM, do inglês *wavelength-domain multiplexing*). Um segundo laser é modulado em amplitude com o mesmo sinal de *trigger* utilizado para pulsar a fonte de fótons únicos. Ambos os comprimentos de onda são multiplexados e enviados para Bob através do canal óptico, que pode requerer algum tipo de estabilização, dependendo das características do sistema. Antes do aparato de medição, o comprimento de onda de sincronismo é demultiplexado, e o sinal elétrico recuperado por um foto-detector, é utilizado para gatilhar os SPADs com a janela casada com os pulsos atenuados.

Cada qubit recebido por Bob pode ser medido em uma das duas bases, também definida de forma aleatória. Por exemplo, uma lâmina de meia-onda pode ser utilizada para girar ou não o qubit em relação ao sistema de medição, composto por um divisor de feixe por polarização (PBS, do inglês *polarizing beamsplitter*) com um detector de fótons únicos em cada porta de saída. Para cada medição, há duas possibilidade de resultado, de acordo com o caminho tomado pelo fóton, e o acionamento de cada detector corresponde a um bit de informação. Caso a base de medição seja compatível com a de preparação, o resultado observado por Bob será determinístico. Caso contrário, haverá cinqüenta por cento de probabilidade de o fóton deixar o PBS por uma porta ou por outra, o que acarretará no acionamento aleatório de um dos detectores.

Após a etapa de transmissão dos qubits, é feita a reconciliação de bases entre Alice e Bob. Através de um canal público autenticado, chamado de canal clássico, Bob revela para Alice (e eventualmente também para Eva) a base escolhida em cada instante de detecção, sem revelar o resultado de cada medida. Os bits correspondentes aos casos de bases coincidentes são mantidos

[4]Na verdade, o valor médio de fótons por pulso pode ser elevado se utilizada a modificação *decoy states* [88][90]

e, os demais, descartados. A partir desta informação é calculada a taxa de erro de qubits (QBER) entre Alice e Bob. Se o valor estimado estiver acima de um determinado limiar (11% ou 15%, assumindo ataques coerentes [8] ou lineares [2], respectivamente)[5], o protocolo é interrompido. Por questão de segurança, assume-se que todo erro ocorrido durante uma transmissão é oriundo de uma possível intervenção da Eva. Se o limiar de segurança foi excedido, significa que uma quantidade crítica de informação pode ter sido interceptada e a chave está comprometida. Se a QBER estiver dentro do limite tolerável, é realizada a etapa de correção de erro, similar ao procedimento empregado nos sistemas convencionais de comunicação, em que, por exemplo, diferentes blocos de bits têm sua paridade testada. A última etapa é chamada de amplificação de privacidade, que visa reduzir a informação mútua média entre Alice/Bob e Eva, às custas do sacrifício de bits. Por exemplo, associando pares de bits através da operação ou-exclusivo, obtém-se um bit deterministicamente caso ambas as entradas da função sejam conhecidas. Se Eva possuir apenas um dos bits (mas Alice e Bob possuírem ambos), não terá terá nenhuma informação acerca do bit resultante, o que reduzirá seu conhecimento a respeito da seqüência final. Finalmente, de posse da chave criptográfica, a mensagem pode ser codificada utilizando o algoritmo *one-time pad* e transmitida de forma sigilosa, sendo então descartada.

O limite de segurança da QBER segura provado para sistemas baseados no protocolo BB84 é de 11% [8]. Nesta prova, assume-se que Eva tem acesso a qualquer tecnologia fisicamente realizável, como teleportação determinística de estado quântico [91][92] ou a realização de medida não-destrutiva do número de fótons (QND, do inglês *quantum non-demolition measurement*) [65], incluindo dispositivos sofisticados como memórias quânticas [93]. Como exemplo, as tecnologias citadas permitiriam a substituição do canal óptico entre Alice e Bob por um enlace mais curto (equivalente a um canal com menor atenuação para compensar alguma perda introduzida pela Eva), ou a verificação do número de fótons em um pulso óptico enviado por Alice, para realização do ataque de divisão do número de fótons (PNS, do inglês *photon-number splitting*) [94] ou para redução do ruído de seu detector implementando um relé quântico (do inglês *quantum relay*) [95][96]; ou armazenar um estado quântico em uma memória quântica [93] para posterior realização da etapa de medição. Outros protocolos podem possuir limites de QBER diferenciados, acima de 25% [97]. Entretanto, as provas de segurança em geral não levam em conta as imperfeições dos dispositivos e, em um cenário realista, os *side-channels* devem ser rigorosamentes avaliados, a fim de garantir a segurança do sistema [98].

[5]Na prática, considera-se uma QBER limite em torno de 10%.

Implementações práticas de sistemas com a atual tecnologia apresentam *loopholes* que podem ser explorados pela Eva para extração de informação causando pouco ou nenhum erro na QBER. Uma linha de pesquisa, chamada "quantum hacking", surgiu com o intuito de encontrar e sanar as falhas técnicas que possibilitem a intervenção incógnita de uma parte não autorizada [67]. Foi mostrada a vulnerabilidade de um sistema QKD a um ataque baseado na utilização de tecnologia atual por parte da Eva [99], com a a primeira implementação completa de um ataque sobre um sistema QKD publicada em 2011 [100], seguida por um ataque realizado sobre dois sistemas comercias de fabricantes diferentes com 100% de sucesso [66]. Estes resultados constituem marco nesta área e chamam a atenção para a necessidade de buscar falhas e soluções para que a tecnologia de distribuição quântica de chaves seja realmente incondicionalmente segura.

Alguns tipos de ataque, apesar de pouco sutis, permitem que Eva obtenha informação acerca da codificação dos qubits, mesmo que através da força bruta. O tipo conhecido como cavalo de Tróia [101], por exemplo, consiste na sondagem dos equipamentos utilizados por Alice e Bob para obter informação sobre a codificação utilizada para cada qubit. Este ataque é especialmente crítico quando realizado contra o sistema *plug & play* [102], em que Alice envia um pulso óptico para Bob que o codifica e reflete de volta para Alice, para a medição. Eva poderia enviar um pulso óptico forte contra-propagante para interrogar o equipamento de Bob e descobrir qual base foi utilizada na preparação do qubit. Uma solução direta para evitar o acoplamento da sonda é a utilização de um isolador óptico na saída da estação de transmissão.

Um ataque explorando a distribuição estatística poissoniana de fótons por intervalo de tempo das fontes ópticas comumente empregadas baseia-se na divisão do número de fótons (PNS) de um pulso não unitário. No caso de um laser atenuado, existe uma probabilidade não-nula de emissão de pulsos contendo múltiplos fótons. Isto pode permitir ao interceptador obter informação sem ser revelado [94]. Neste ataque, Eva retém *n-1* fótons do pulso contendo n partículas, enquanto que um fóton é recebido por Bob sem ter sido perturbado. Desta forma, ambos Eva e Bob recebem exemplares do estado quântico enviado por Alice. O interceptador pode medir os qubits ou, assumindo avanços tecnológicos, armazená-los em uma memória óptica para medição após a reconciliação de bases. A prevenção deste ataque usualmente é feita ajustando-se o atenuador para que a fonte emita pequenos valores médios de fótons por pulso; ou com uma fonte de estatística sub-poissoniana, como uma fonte heráldica [74]; ou através do uso da técnica de *decoy states* [90], que introduz pulsos contendo diferentes números médios de fótons intercalados com

os qubits tradicionais.

Certos ataques têm como alvo topologias específicas de sistemas de QKD. Por exemplo, Eva pode valer-se da imperfeição de outros componentes, como o espelho de Faraday empregado no sistema *plug & play*. Neste ataque, Eva envia pulsos de prova para Bob (que os prepara e reenvia) e os intercepta, enviando estados falsos para Alice. Porém, dado que o espelho de Faraday apresenta imperfeição, Eva pode inferir informação parcial da chave criptográfica devido ao fato de o espaço de Hilbert dos estados de codificação ser desdobrado em uma dimensão maior [103], ou seja, os qubits apresentam uma assinatura de polarização, além do estado codificado no tempo (*time-bin*). Este ataque, entretanto, eleva a QBER e sua eficácia depende do comprimento do enlace.

Uma classe particular de ataques tem como alvo *loopholes* nos detectores de fótons únicos, especialmente os baseados em fotodiodos avalanche. Um grupo destes ataques baseia-se no descasamento entre as curvas de eficiência (DEM, do inglês *detector efficiency mismatch*) dos dois SPADs utilizados por Bob no aparato de medição [104]. Eva intercepta e mede os qubits enviados por Alice com um aparato similar ao de Bob. De acordo com o resultado obtido, Eva forja um estado falso similar, chamado *faked-state* [67], e o envia para Bob de modo que incidam em uma posição temporal determinada da janela de detecção dos SPADs da estação receptora. Isto significa que, dependendo da posição temporal de incidência do fóton dentro das janelas descasadas, haverá maior ou menor probabilidade de detecção em um determinado SPAD. Deste modo, Eva pode inferir o resultado da medição realizada por Bob e obter informação parcial acerca da chave.

Esta característica pode ser explorada por Eva através da interceptação dos qubits e reenvio de um estado falso [104] ou mesmo sem interceptação, apenas manipulando a sincronização do sistema. Neste último caso, chamado *time-shift* [14][99], os fótons enviados por Alice são aleatoriamente atrasados ou adiantados opticamente dentre dois valores de tempo distintos, de modo a incidirem nos detectores de Bob em posições temporais em que há DEM favorável a Eva.

Outra forma de obter informação sobre o resultado da medição realizada por Bob sem interceptação explora o tempo morto dos SPADs operando em modo *free-running* [105]. São enviados pulsos fracos, preparados de forma que sejam detectados por um SPAD específico do aparato de medição. Se isto ocorrer antes da chegada do qubits enviado por Alice, este detector específico estará desabilitado e, se Bob registrar uma contagem, Eva saberá qual detector a clicou. Este esquema vale se o sistema QKD rejeitar contagens fora dos *time-slots* definidos pelo sincronismo.

Em outra família de ataques baseada no SPAD, Eva atua através da adulteração do ponto de operação do detector por meio de sinais ópticos externos. Os ataques do tipo *blinding* envolvem a manipulação direta remota e adulteração da resposta dos dispositivos, seja operando em modo passivo [106], ativo [107] e gatilhado [108]. Por meio de sinais ópticos fortes, Eva torna os detectores de Bob insensíveis a níveis baixos de radiação óptica e cegos para os qubits enviados por Alice. Nos ataques *tailored bright light* [66] e *thermal bliding* [108], isto se dá através da alteração do ponto de polarização elétrica dos detectores devido à operação em regime linear ou por aquecimento devido ao fluxo de corrente. Combinando com uma estratégia baseada em estados falsos, Eva prepara, de acordo com seu resultado da medição do qubit interceptado, um pulso óptico forte, que, incidindo no detector, força um evento de detecção na estação de Bob. Desta forma, a resposta do detector fica à mercê de Eva, que terá os mesmos resultados que Alice e Bob após a reconciliação de bases.

No ataque [107] operado contra detector em modo de operação *free-running* com luz forte, um laser CW é utilizado para forçar o fluxo de foto-corrente no SPAD. A queda de tensão sobre o resistor de polarização do APD depleta a tensão de polarização do dispositivo, reduzindo-a a um valor mais baixo que o limiar de ruptura. Quando isto ocorre, o detector fica insensível aos fótons incidentes e as contagens de escuro são suprimidas, resultando em contagem nula. O interceptador pode aplicar uma estratégia do tipo "intercepta-reenvia", medindo os fótons enviados por Alice e superpondo pulsos ópticos fortes ao sinal CW de "cegamento", de acordo com o resultado da medição. Este ataque causa uma contagem no detector de Bob com 100% de probabilidade, caso as bases concordem, ou não causa contagem, se as bases forem incompatíveis, suprimindo, inclusive, as contagens de escuro e os pós-pulsos.

O ataque *thermal blinding* é extensível também aos detectores com operação gatilhada e força o aquecimento do APD através da geração de fotocorrente com um sinal óptico externo (CW ou pulsado). O limiar de ruptura do fotodiodo pode variar 10 mV/K, como relatado no artigo, tornando o SPAD insensível a fótons únicos após determinado tempo de aquecimento. O controle do detector é feito de forma semelhante à relatada anteriormente, com interceptação dos qubits e reenvio de pulsos fortes. A contra-medida apresentada baseia-se no monitoramento dos parâmetros internos do APD, como corrente e temperatura.

Existe uma discussão a respeito do ponto de operação destes ataques [109][110][111] e se um ajuste criterioso do limiar de discriminação de avalanche e da resistência em série com o APD seriam suficientes para evitá-lo. Além

disso, é proposto em [110] o monitoramento da foto-corrente gerada pelo SPAD, proporcional à taxa de contagem no regime de poucos fótons. Outra contra-medida seria a utilização de um divisor desbalanceado e um detector de monitoramento à entrada do SPAD. Uma resposta definitiva à esta questão não foi publicada, mas argumenta-se que um detector sensível a poucos fótons poderia ser "cegado" pela Eva, enquanto que o limiar de um detector "clássico" não seria facilmente ajustado e este também seria passível de ataque, não sendo uma solução definitiva.

3.2 Time-shift attack

O descasamento das curvas de eficiência em função do tempo dos SPADs no aparato de detecção pode ser explorado para implementação do ataque *time-shift* em um sistema de QKD. O princípio explorado através deste método baseia-se em aumentar a probabilidade de detecção de um determinado estado quântico em um detector específico e reduzir sua probabilidade de detecção no outro detector, através da manipulação de seu tempo de chegada dentro das janelas de detecção. Assumindo uma estação receptora com dois detectores, para cada qubit, Eva pode impor um atraso óptico t_0 de modo que o fóton tenha alta probabilidade de detecção em um SPAD (η_{alta}) e baixa probabilidade de detecção no outro SPAD (η_{baixa}); ou um atraso t_1 para que ocorra o inverso. Esta técnica pode ser implementada com tecnologia disponível atualmente e não causa alteração da QBER, uma vez que não há interceptação dos fótons.

Um sistema de monitoramento dos detectores em tempo real é proposto para a verificação de uma possível intervenção externa durante a troca de chaves. Duas assinaturas deixadas pelo ataque *time-shift* passíveis de monitoramento são a variação da eficiência de detecção observada por Bob e a própria alteração imposta ao tempo de chegada dos fótons. O método baseia-se no mesmo princípio do sistema de caracterização de detectores apresentado na seção 2, em que é feita a análise da distribuição estatística dos tempos entre detecções consecutivas.

A quantidade de informação extraída pelo interceptador [14] depende da razão entre os dois valores de eficiência (r=η_{baixa}/η_{alta}) para um mesmo atraso temporal, e é dada pelo complemento da entropia de Shannon, calculada para a quantidade r/(r+1) – que é equivalente à probabilidade de Bob detectar o fóton no detector com menor eficiência, ou seja, a probabilidade de ocorrência do bit não esperado por Eva –, ou seja,

$$I(Eva:Bob) = 1 + \frac{r}{r+1} log_2 \left(\frac{r}{r+1}\right) + \left(1 - \frac{r}{r+1}\right) log_2 \left(1 - \frac{r}{r+1}\right). \tag{3-1}$$

A informação mútua média entre Eva e Bob, calculada conforme indicado, é mostrada na figura 3.3, em função dos valores de eficiência de detecção relativa dos dois detectores de Bob.

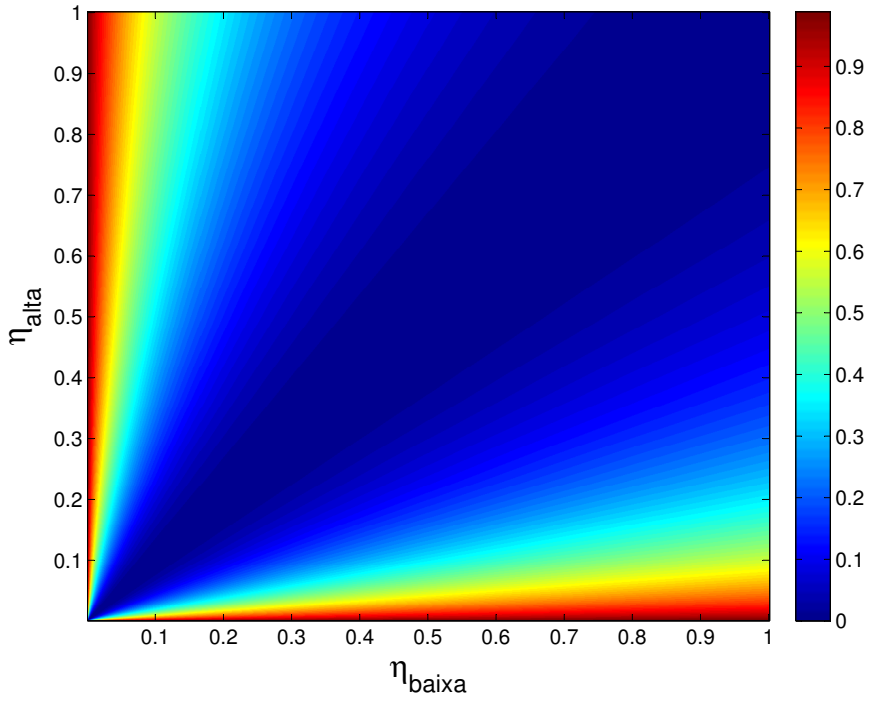

Figura 3.3: Informação mútua média entre Eva e Bob para os ataques baseados no descasamento de eficiência dos SPADs de recepção.

O limite superior para a taxa de transmissão segura de bits é dado pela entropia de Shannon da quantidade r/(r+1), que corresponde à informação mútua entre Alice e Bob dada a intervenção de Eva [14]. Se não houver descasamento de eficiências, a entropia é unitária. Caso haja descasamento, este valor indica a máxima taxa relativa de comunicação

Observa-se que o caso mais favorável para o ataque ocorre se, para um determinado atraso imposto pela Eva, o fóton é detectado com eficiência integral pelo SPAD de Bob (valor na prática com limite em torno de 15%) enquanto que, para outro valor de atraso, a eficiência é zero (assumindo comportamento complementar para o outro SPAD). Se não houver descasamento entre as curvas de eficiência, a informação mútua entre Eva e Bob será zero. A redução da eficiência de detecção aparente do SPAD sob ataque é intrínseca à operação do *time-shift*, e exploração de uma região menos eficiente da janela temporal do detector. Deste modo, o ataque deixa necessariamente uma assinatura. Como visto na seção 2, é possível extrair o produto η a partir do histograma de

tempos entre detecções de acordo com a inclinação da curva. Esta informação torna-se especialmente útil considerando que o ataque em questão não aumenta a QBER. Adiante serão feitas considerações sobre a possibilidade de compensação desta perda de eficiência.

No caso do monitoramento da adulteração dos intervalos de tempo, a resolução do histograma deve ser maior que o período de gatilho. Na verdade, a resolução da amostragem dos intervalos de tempo deve ser suficiente para que seja possível diferenciar os atrasos extras impostos aos fótons. Como Eva atua no sincronismo dos qubits através de uma linha de atraso bi-estável – impondo os tempos de chegada t_0 ou t_1 –, os intervalos de tempo possíveis entre detecções serão múltiplos do período de gatilho, mas com variação extra de acordo com o atraso ajustado durante os dois eventos que definem um intervalo de tempo, como ilustrado na figura 3.4. Se ambos os pulsos de detecção, de início e de

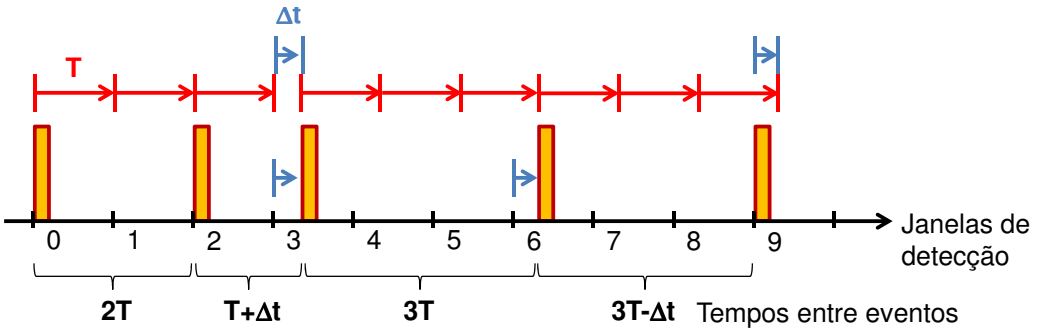

Figura 3.4: Representação esquemática dos tempos entre eventos durante o ataque *time-shift*. O atraso Δt é ativado aleatoriamente durante os *time-slots*, podendo ou não alterar o tempo de chegada do fóton. Os intervalos de tempo podem ser alongados ou encurtados com este valor, em relação aos valores múltiplos do período de gatilho.

término do intervalo, foram obtidos com atraso t_0 ou ambos com atraso t_1, o tempo correspondente será dado por M×T, ou seja, um múltiplo inteiro M do período de gatilho T. No caso em que o evento inicial foi gerado com atraso t_0 e, o evento final, com t_1, o intervalo de tempo correspondente será mais longo, e será dado por M×T+Δt (com $\Delta t = |t_1 - t_0|$). No caso inverso, em que o início ocorreu devido a um fóton adiantado e o evento final foi causado por um fóton atrasado, o intervalo será Δt mais curto que um múltiplo do período de gatilho. Como a escolha dos atrasos é aleatória, em metade dos casos ocorrerá um intervalo múltiplo do período de gatilho e a demais combinações apresentarão um quarto de probabilidade. O histograma de tempos entre eventos de detecção deverá apresentar picos triplos com espaçamento dado pelo atraso imposto pelo ataque. Além disso, a operação gatilhada síncrona do sistema de QKD resultará em um histograma discretizado de acordo com a freqüência de gatilho.

Existem maneiras de forçar o DEM durante o sincronismo de um sistema QKD, realizado antes da comunicação efetiva [112], dependendo de suas características. De qualquer modo, existe um compromisso entre a informação extraída por Eva e a assinatura por ela deixada. Ressalta-se aqui que este monitoramento é válido desde que o atraso induzido nos fótons seja maior que o *jitter* (resolução temporal) dos detectores.

3.2.1 Montagem experimental

Como prova de conceito, o ataque *time-shift* foi experimentalmente simulado conforme mostrado na figura 3.5. O sinal de sincronismo proveniente

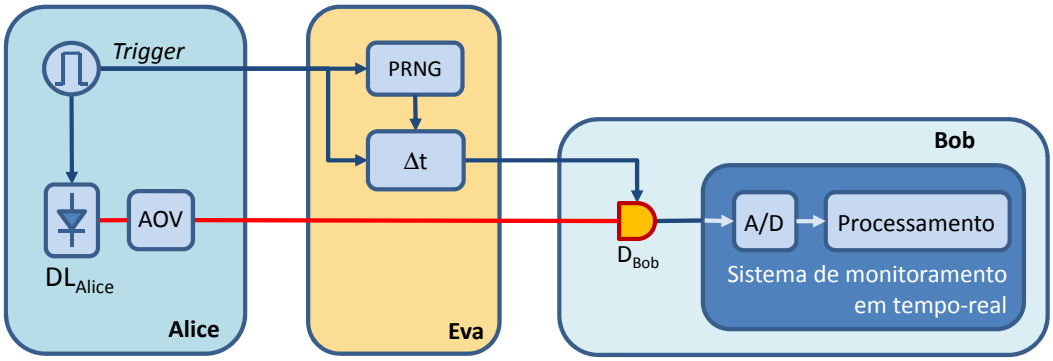

Figura 3.5: Diagrama da montagem experimental do ataque *time-shift* para monitoramento do detector.

de um gerador de pulsos é utilizado para pulsar o laser de Alice (DL_{Alice}). Os pulsos ópticos são atenuados e enviados para Bob. Diferentemente do ataque convencional, em que Eva altera o tempo de chegada dos fótons em relação à janela de detecção de Bob, optou-se por alterar o instante de gatilho do SPAD, sem prejuízo para a demonstração do monitoramento do detector. Um FPGA (*field-programmable gate-array*) foi utilizado para atrasar aleatoriamente cinqüenta por cento dos pulsos de sincronismo enviados para o SPAD, com um valor fixo de 60 ns, enquanto o tempo de chegada dos pulsos ópticos foi mantido fixo. Desta forma, é possível sincronizar o sistema para que os pulsos ópticos incidam em duas posições temporais distintas do detector, cuja janela de detecção foi ajustada em 100 ns. À saída elétrica do SPAD, foi conectado o sistema de monitoramento, composto por um cartão de aquisição de 100 MSamples/s e um computador para processamento dos dados.

O sincronismo do sistema foi verificado através da varredura dos pulsos ópticos em relação à janela de detecção. Esta varredura foi executada com o FPGA ajustado para alterar todos os pulsos de sincronismo com δ_0 e repetido com δ_1, conforme mostrado na figura 3.6. O pulso óptico também foi

varrido durante a alternância aleatória do sincronismo da janela do detector. A largura da janela de detecção foi escolhida como 100 ns devido à resolução

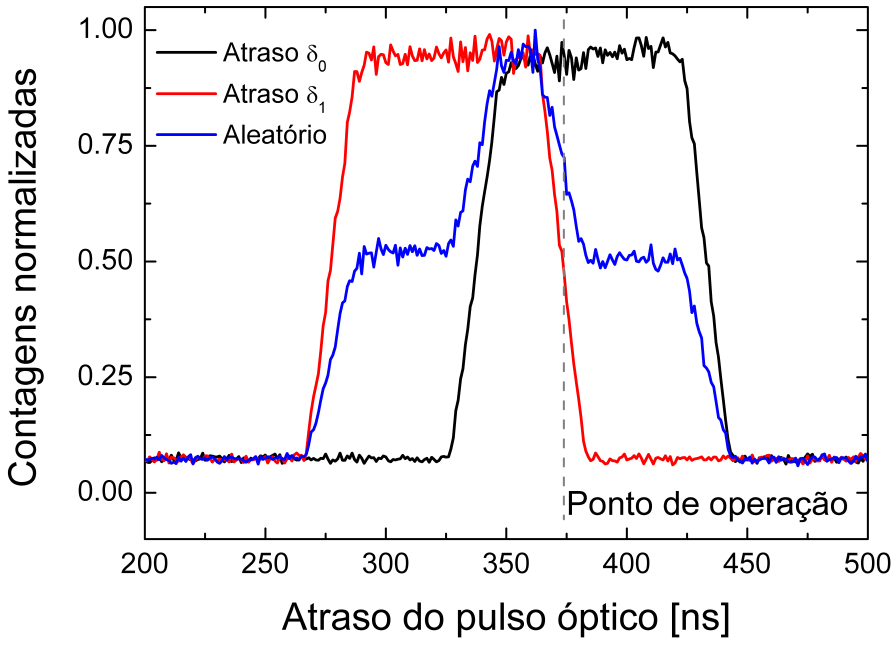

Figura 3.6: Varredura do gate com o pulso óptico para os casos em que o atraso óptico é fixo (com tempos δ_0 e δ_1) ou aleatório.

obtida para o gerador de atrasos aleatório, que apresentou *jitter* temporal de aproximadamente 20 ns. O ponto de operação do ataque escolhido está indicado pela linha tracejada na figura 3.6. Quando o atraso δ_0 é ajustado para o pulso óptico, a eficiência do detector equivale a seu valor máximo, uma vez que os fótons incidem no centro da janela (curva preta). Quando o atraso é alterado para δ_1, os fótons incidem no SPAD em uma posição temporal cuja eficiência equivale à metade do valor máximo (curva vermelha). As curvas vermelha e preta equivalem ao caso em que há descasamento de eficiência do detector. Nesta condição, o ataque permitiria a Eva obter 8,2% de informação. A curva azul mostra o valor efetivo obtido ao se efetuar a varredura do laser com atraso sendo chaveado entre os dois valores aleatoriamente. A eficiência média, neste caso, visualmente equivale a aproximadamente 75% do valor máximo. Os casos extremos do ataque correspondem à inexistência de descasamento entre os detectores (posição 356 ns), que corresponde ao caso ideal do ponto de vista da segurança; e ao total descasamento – por exemplo, a posição de 400 ns –, em que Eva pode inferir com alta probabilidade de acerto em qual detector houve a contagem, dado que um determinado atraso foi aplicado ao fóton.

O número de amostragens do A/D foi contado entre eventos de detecção consecutivos do SPAD e os dados foram agrupados na forma de um histo-

grama, equivalendo a uma base de tempo com resolução de 10 ns. Para fins comparativos, repetiu-se a medição para o caso em que os pulsos de gatilho sofrem atraso fixo. O histograma também foi gerado utilizando o período de gatilho como base de tempo.

3.2.2 Resultados

Conforme mencionado anteriormente, duas análises foram feitas a partir dos dados medidos. Inicialmente, os histogramas foram gerados com intervalo (bin) equivalente ao período de gatilho, neste caso 100 kHz (10 μs). A variação na inclinação dos histogramas – mostrados na figura 3.7, observada ao se comparar o caso com atraso aleatório com o caso de atraso fixo, corresponde a uma redução da eficiência global do detector. Como os fótons incidentes no

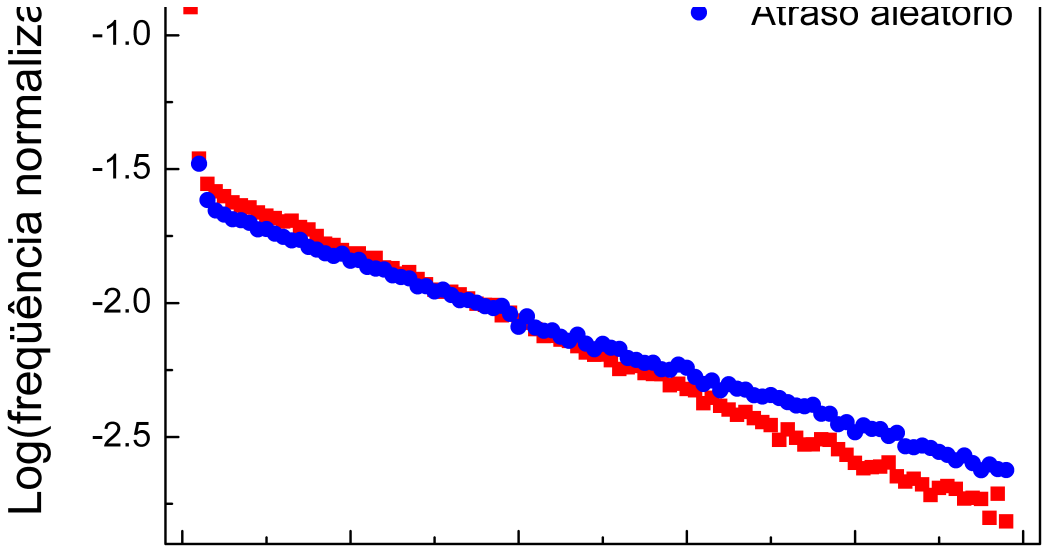

Figura 3.7: Histogramas dos tempos entre eventos no SPAD sob o ataque *time-shift* e com atraso relativo da janela de gatilho constante.

detector experimentam diferentes eficiências de detecção, o valor efetivo será menor que no caso de todos os fótons incidindo no centro da janela. Observando esta redução da eficiência ou, de forma equivalente, a redução do número médio de fótons recebido, Bob pode verificar a intervenção externa. Durante o ataque, a eficiência do SPAD observada por Bob foi reduzida de 15% para 11,8%. Do ponto de vista da Eva, diferentemente de outros ataques baseados no descasamento de eficiência [[67][68]], em que ocorre redução semelhante da eficiência aparente, a compensação deste efeito não é facilmente realizável no *time-shift* com a tecnologia atualmente disponível. Como não ocorre a interceptação e substituição dos fótons únicos por estados falsos cujo número de fótons pode ser ajustado, a alternativa baseia-se na substituição do canal

óptico entre Alice e Bob por um meio mais transparente ou a teleportação do estado.

Visualizando o histograma anterior com base de tempo de 10 ns, pode-se comparar os casos em que o SPAD está sujeito ao ataque com a resposta do dispositivo sob condições normais de operação (com atraso fixo entre os pulsos ópticos e as janelas de detecção), o que é visto na figura 3.8. Como a freqüência

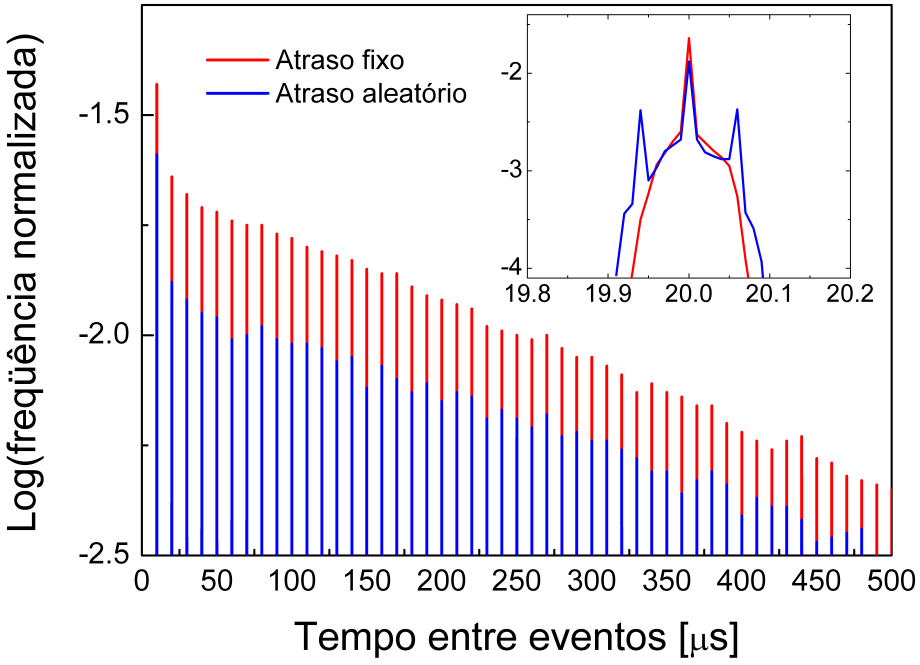

Figura 3.8: Histogramas de tempos entre eventos no SPAD sob o ataque *time-shift*. No detalhe é mostrado a ampliação de um bin, onde pode ser vista a assinatura do ataque, dada pelos três picos.

do sinal de gatilho aplicado ao detector foi ajustada em 100 kHz, os picos no histograma apresentam espaçamento de 10 μs entre si. Sob condição normal de operação, podem ser vistos picos únicos a cada período de gatilho, conforme mostrado no detalhe da figura, que amplia um dos picos (curva vermelha). Em contra-partida, quando sob ataque, o detector apresenta picos triplos, afastados por 60 ns entre si, devido ao atraso bi-estável aplicado por Eva. O alargamento temporal dos picos, em torno de 20 ns, deve-se ao *jitter* do FPGA utilizado para alternar o tempo relativo da janela de detecção em relação ao pulso óptico.

Um teste foi feito ajustando-se o ponto de operação do sistema em 356 ns (vide figura 3.6), gerando uma figura semelhante à anterior. Foi observada uma razão de 50% entre os picos laterais e o pico central do segundo bin do histograma preparado de acordo com a resolução do A/D, conforme previsto, sem alteração da eficiência aparente.

3.3 Aftergate attack

Conforme mencionado, a tecnologia atual utilizada em sistemas de QKD apresenta imperfeições que podem permitir o controle direto do detector de fótons únicos por uma terceira parte não autorizada. Combinada com uma estratégia do tipo *man-in-the-middle*, o interceptador força a operação dos detectores de Bob externamente. De acordo com seus próprios resultados de medição do qubit interceptado, Eva prepara um estado substituto e o envia para Bob. O resultado da medição deste estado é tendencioso e, monitorando a etapa posterior de reconciliação de bases, Eva pode inferir com alta probabilidade de acerto o bit compartilhando entre Alice e Bob.

No ataque *after-gate*, é explorado o regime de operação linear dos SPADs. Quando polarizado abaixo do limiar de ruptura, um APD apresenta resposta linear da fotocorrente em relação à potência óptica incidente. Este é o caso dos SPADs operados em modo gatilhado durante os longos intervalos entre a ativação das janelas de detecção. Se potência óptica suficiente incidir no detector nestes instantes, uma avalanche pode ser desencadeada.

Assumindo um sistema de distribuição quântica de chaves baseado no protocolo BB84 com codificação em polarização, Alice prepara aleatoriamente cada qubit em um dos quatro estados possíveis e o envia para Bob. Eva, que em princípio possui aparato de medição similar ao da estação receptora (como na figura 3.2, por exemplo), intercepta cada fóton e realiza a medição em uma base aleatoriamente escolhida. O interceptador prepara um pulso óptico com polarização idêntica ao seu resultado obtido e o envia para Bob. Este pulso possui potência óptica tal que, caso a base de medição escolhida por Bob seja compatível com seu estado de polarização, haverá probabilidade unitária de ocorrência de um evento de detecção no detector correspondente ao estado enviado. Por outro lado, caso as bases de preparação e de medição sejam incompatíveis, a projeção do estado de polarização do pulso óptico no PBS de Bob causará a divisão da potência óptica que, ficando 3 dB abaixo do limiar pré-estabelecido, não deflagará avalanche em nenhum dos dois SPADs. Por exemplo, se Bob escolhe realizar a medição na base $\oplus$ e Eva preparou um auto-estado do PBS, $|\mathrm{H}\rangle$ ou $|\mathrm{V}\rangle$, o detector correspondente à saída H ou V do PBS, respectivamente, será acionado, conforme ilustrado na figura 3.9a, uma vez que a perda será mínima. Caso Eva envie o estado $|+45\rangle$ ou $|\text{-}45\rangle$ e Bob escolha a base $\oplus$, a projeção do pulso óptico no PBS resultará na divisão em um pulso de potência menor em cada saída e não haverá evento de contagem (na figura 3.9b). Do ponto de vista do interceptador, um problema deste protocolo de ataque se refere ao fato de que, mesmo quando as bases

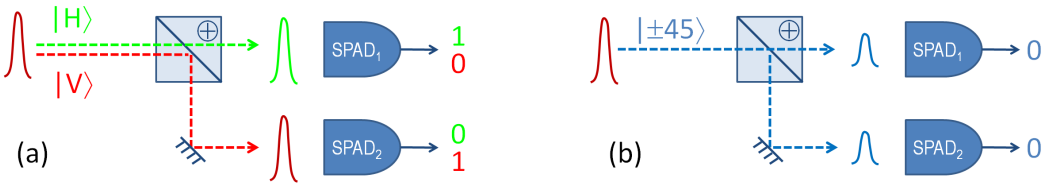

Figura 3.9: Projeção do pulso de ataque no PBS da estação receptora para bases de preparação e medição (a) coincidentes e (b) não coincidentes. No primero caso, haverá um evento de detecção no SPAD correspondente, enquanto que, no segundo, não haverá detecção.

de Eva e Bob são incompatíveis e não há evento de detecção, existe fluxo de cargas no detector, devido à geração de corrente elétrica em modo linear. Esta foto-corrente é suficiente para popular armadilhas no SPAD, responsáveis pelo efeito de pós-pulsos. Por este motivo, o ataque não é realizado antes da janela de detecção, pois haveria alta probabilidade de ocorrência de um pós-pulso. Para minimizar este efeito, Eva envia os pulsos fortes de modo que incidam nos detectores de Bob logo após o fechamento da janela de detecção (daí o nome do ataque). Mesmo tomando esta precaução, conforme indicado pelos autores proponentes do ataque [13], ainda haverá uma certa probabilidade de ocorrência de pós-pulsos devido à intervenção do interceptador.

3.3.1 Montagem experimental

Foi feita a simulação experimental da intervenção de um interceptador em um sistema QKD com codificação em polarização através do ataque *after-gate*, como mostrado na figura 3.10. A estação de Alice é composta por uma fonte

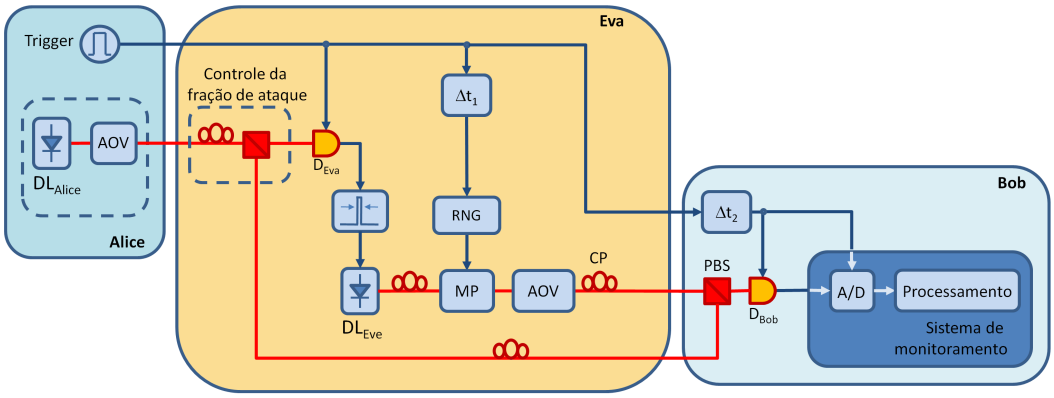

Figura 3.10: Montagem experimental do ataque *aftergate* sobre um sistema baseado no protocolo BB84 com codificação em polarização.

de fótons únicos, formada por um diodo laser CW (DL_{Alice}) em 1550 nm e um

atenuador óptico variável (AOV), e um gerador de pulsos para sincronismo do sistema. Para a demonstração, o estado de polarização enviado é fixo. O laser atenuado de Alice apresenta distribuição poissoniana do número de fótons por intervalo de tempo e é ajustado de modo que haja μ fótons em média por janela de detecção de Eva e Bob, como será visto adiante.

Eva pode escolher interceptar determinada fração dos fótons enviados através de um PBS precedido por um controlador de polarização. A fração não interceptada é encaminhada para Bob, como no caso sem ataque. O SPAD de Eva (SPAD_{Eva}) opera em modo gatilhado e é sincronizado com o sinal elétrico provido por Alice, possibilitando a detecção dos fótons interceptados dentro das janelas nominais de 5 ns. Cada evento de detecção no SPAD origina um pulso elétrico de 103.5 ns que é reformatado e modula diretamente um diodo laser para criação dos pulsos ópticos de ataque, com 1 ns de duração temporal, como mostrado na figura 3.11. A polarização de cada pulso é ajustada através de

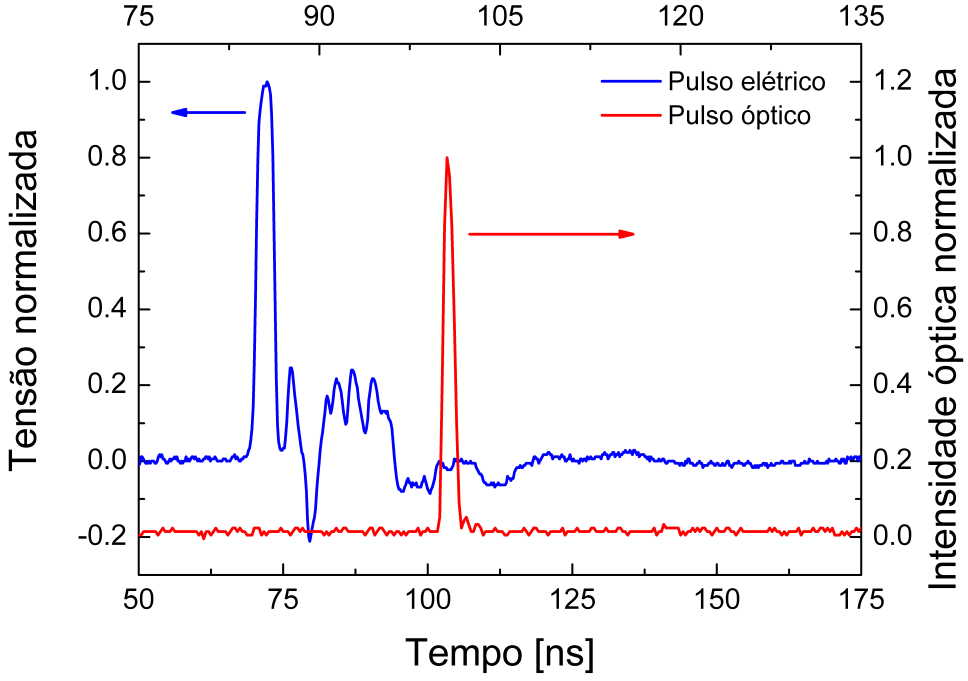

Figura 3.11: Pulso elétrico de modulação e pulso óptico forte gerado por Alice.

um modulador de polarização (MP) em $LiNbO_3$, atenuado através de um AOV e enviado para Bob. Como nesta montagem Alice não prepara o estado dos qubits, foi utilizada uma seqüência binária aleatória previamente gerada [76] para simular a escolha do estado de polarização feita por Eva. Em um sistema completo, esta escolha seria baseada nas detecções obtidas com um aparato similar ao de Bob na figura 3.2. Para cada pulso de sincronismo, um FPGA lê um bit de uma memória pré-armazenada com 2×10^5 bits aleatórios e realiza a

operação lógica "E", resultando na supressão da saída elétrica quando lido bit zero. Os pulsos elétricos lógicos têm sua amplitude devidamente formatada para atuar no MP. Caso o pulso elétrico de sincronismo seja suprimido pelo FPGA, a polarização do pulso óptico não é alterada. Caso contrário, a polarização do pulso é girada 90^o na esfera de Poincaré, correspondendo a um estado de polarização pertencente a uma base maximamente não-ortogonal ao caso inerte. O sinal de sincronismo é adequadamente atrasado para garantir a modulação da polarização dos pulsos ópticos gerados a partir dos eventos de contagem do SPAD_{Eva}, o que foi verificado com auxílio de um polarímetro.

A polarização dos pulsos ópticos de ataque é alinhada com o PBS na estação de Bob para o caso em que o MP não atua, garantindo a maximização do sinal óptico na porta conectada ao detector de Bob (SPAD_{Bob}). Quando o estado de polarização do pulso óptico é alternado, metade da potência óptica é enviada para cada porta de saída do PBS.

Os fótons não interceptados por Eva são combinados com os pulsos de ataque através da segunda porta de entrada do PBS de Bob [6]. A polarização é ajustada de modo a maximizar sua transmitância para o SPAD_{Bob}. Este detector é gatilhado pelo sinal de sincronismo, cujo atraso é casado com os pulsos de Eva, e abre janelas de detecção efetiva de 2,24 ns. Sua saída elétrica é conectada ao sistema de monitoramento, composto pelo conversor analógico-digital e pelo computador para processamento. O sinal de gatilho também é conectado ao A/D. O número de janelas abertas entre eventos consecutivos de contagem é contabilizado e os valores são acumulados na forma de um histograma, então analisado.

O ponto de operação do ataque foi ajustado incidindo-se o pulso óptico no SPAD em diferentes posições temporais em relação à janela de detecção. A potência foi variada em passos de 3 dB através de um AOV. A figura 3.12 mostra a variação da resposta da janela temporal do detector de acordo com a potência óptica. Observe que, como a janela foi atrasada em relação ao pulso óptico, seu final está localizada à esquerda, no gráfico. Ao aumentar a potência óptica, o final da janela do detector se estende. A partir de determinado valor, este alongamento varia de forma não-linear. O ponto de operação foi escolhido de modo que, variando-se a potência do pulso em 3 dB, o SPAD responda de forma binária. Isto significa que, com potência P_0, a probabilidade de contagem é 100% e, com potência P_0-3 dB, esta probabilidade é zero. Esta condição é alcançada com mínima potência P_0 para atenuação de 3 e 6 dB, correspondendo às curvas azul claro e azul escuro, respectivamente.

[6]Esta conexão é feita por praticidade, mas Eva poderia utilizar um acoplador 99:1, pois a perda no pulso forte pode ser compensada.

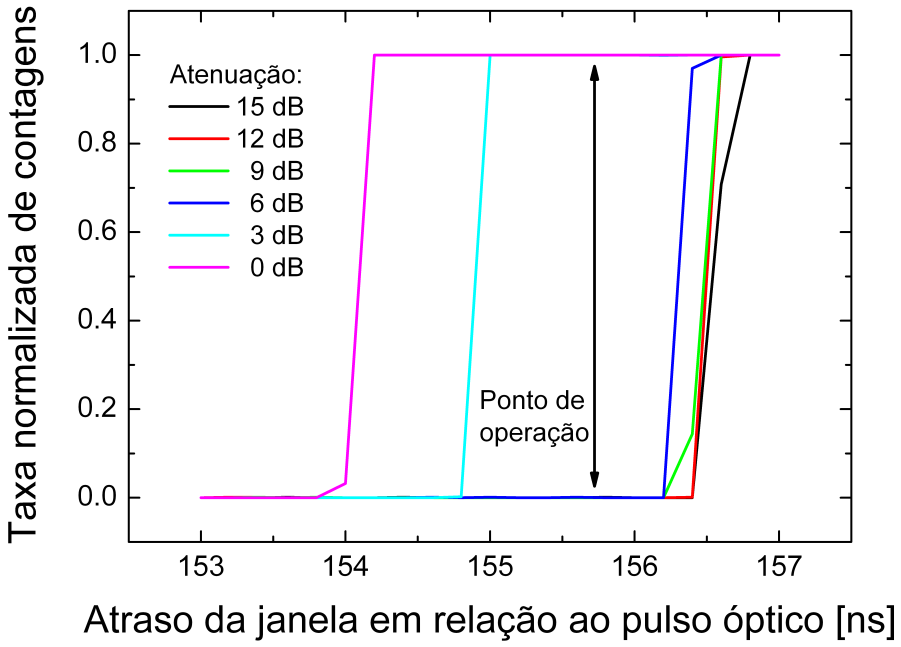

Figura 3.12: Varredura da janela de detecção em relação ao pulso óptico para diferente valores de potência. A seta mostra a posição temporal relativa referente ao ponto de operação para ataque *after-gate*.

3.3.2 Resultados

O SPAD foi monitorado durante o ataque *after-gate* em diferentes condições. Os histogramas de tempos entre detecções foram coletados variando-se a fração de ataque de modo que 100%, 50%, 10% e 1% dos fótons fosse interceptado, com o complemento seguindo diretamente para Bob. O atenuador de Alice foi ajustado para que sejam emitidos em média 0,4 fótons por janela efetiva de 2,2 ns (ajustada nos detectores de Eva e de Bob, ambos operando com eficiência de 15%). A freqüência de gatilho foi ajustada em 400 kHz. Duas sequências de medições foram realizadas, sem e com um tempo morto de 10 μs no SPAD de Bob. Os histogramas correspondentes podem ser vistos na figura 3.13, cada um composto por 2×10^5 pontos. A inclinação das curvas, idêntica para todo o grupo de medidas, indica que o número médio de fótons observado por Bob é mantido constante. Entretanto, o início do histograma, ressaltado no detalhes da figura, mostra um acréscimo nos eventos causados por pós-pulsos em função da fração de ataque. Mesmo com a imposição do tempo morto de 10 μs após cada detecção, observa-se um aumento significativo da probabilidade de pós-pulsos. O tempo morto pode ser visualizado no histograma através da ausência de eventos com espaçamento temporal menor que o valor imposto que, convertido em períodos de gatilho (2,5 μs), resulta em quatro bins vazios.

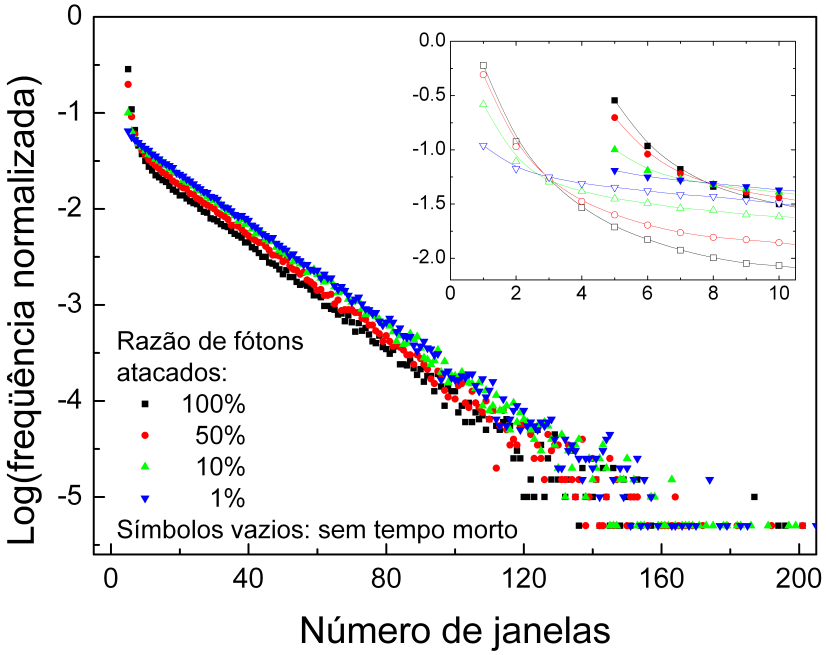

Figura 3.13: Histogramas dos tempos entre eventos com o detector submetido ao ataque *after-gate*, operado com diferentes frações de interceptação, com tempo morto de 10μs. No detalhe foi ampliado o início do histograma, comparado com o caso sem tempo morto.

Os resultados para a medição da probabilidade de pós-pulsos são mostrados na figura 3.14 para um conjunto de cinco repetições de cada medida. A probabilidade de afterpulses foi medida como desprezível, quando aplicado tempo morto (se não for aplicado, este valor corresponde a 1.79%). O acréscimo se deve à incidência de valor elevado de potência óptica fora da janela de detecção que, mesmo não sendo suficiente para desencadear uma avalanche, gera foto-corrente e preenche as armadilhas no semicondutor.

Os resultados indicam que o sistema de monitoramento é eficaz mesmo se uma pequena fração dos fótons for interceptada, devido à assinatura deixada na probabilidade de pós-pulsos, ainda que seja imposto tempo morto de 10 μs ao detector.

3.4 Ataque faint after-gate

Uma variação do ataque *after-gate* foi recentemente proposta, visando a redução da assinatura deixada no detector devido ao aumento da probabilidade de pós-pulsos. A variante atenuada, chamada *faint after-gate* (FAG), explora o comportamento supra-linear exibido por alguns SPADs [68]. Este efeito se

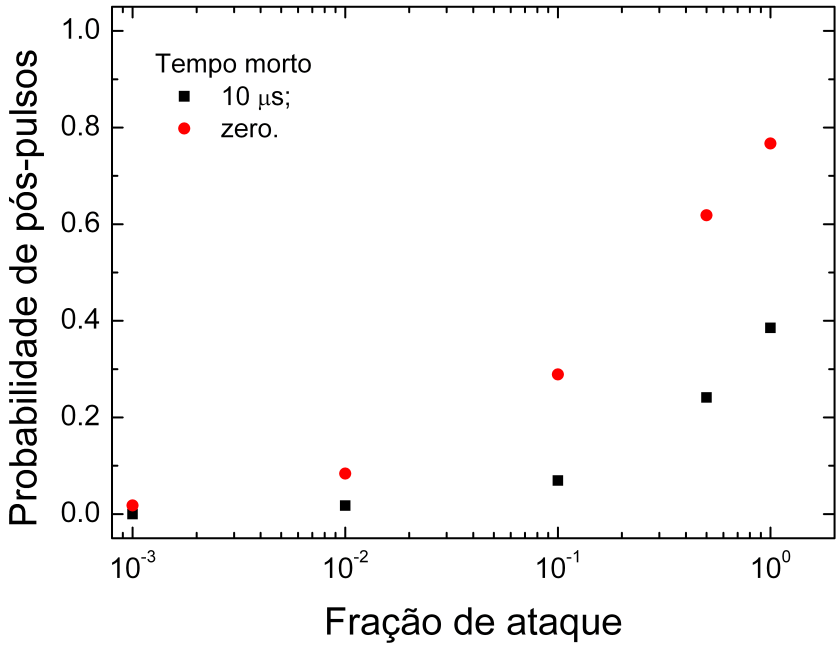

Figura 3.14: Probabilidade de pós-pulsos no detector sob o ataque *aftergate* para diferentes frações do número de fótons interceptados. Os resultados foram obtidos com 0 e 10 μs de tempo morto após detecções. O valor de referência, sem ataque, é mostrado como 0,1%.

refere à variação da curva de eficiência de um SPAD em função do número de fótons incidentes por intervalo de tempo. O protocolo de ataque é semelhante ao anteriormente descrito, de modo que Eva intercepta e mede os qubits enviados por Alice. Dependendo do resultado de sua medição, um determinado estado (de polarização, por exemplo) é preparado e enviado para Bob, em uma posição temporal localizada no fim da janela de detecção. Em contra-ponto ao ataque anteriormente descrito, este pulso óptico contém, em média, algumas dezenas de fótons (μ_0). Dependendo da escolha de base de Bob, haverá divisão da potência óptica, de forma semelhante à representada na figura 3.9. Caso as bases de preparação e de medição concordem, o número de fóton médio μ_0 será detectado com eficiência η_{alta}, enquanto que, caso as bases discordem, haverá divisão do número de fótons no PBS e $\mu_0/2$ fótons, em média, serão detectados com eficiência η_{baixa}. Semelhante ao caso *time-shift*, a razão entre os valores de eficiência de detecção em ambos os casos é utilizada para quantificar a quantidade de informação obtida pelo interceptador. No caso assintótico em que η_{alta} é unitária e η_{baixa} é zero, Eva terá acesso a 100% da informação, como no caso do ataque *after-gate*. Entretanto, a redução significativa do número de fótons enviados em cada pulso, especialmente nos casos em que há discordância entre as bases de preparação e de medição visa à redução da probabilidade de

pós-pulsos causados pelo ataque. Por outro lado, o interceptador deve atentar para a redução da eficiência média de detecção observada na recepção do sistema QKD. Cabe ressaltar também que, diferente do ataque *time-shift*, em que não há interceptação dos qubits e a QBER não se altera, o FAG introduz erro. Os estados falsos medidos por Bob com base diferente da utilizada por Eva em sua preparação possuem probabilidade não-nula de serem detectados, causando erro.

O ataque FAG foi experimentalmente simulado sobre a montagem mostrada na figura 3.10. As principais alterações referem-se à redução do número médio de fótons por pulso criado por Eva e à mudança do ponto temporal de operação. A janela do detector foi varrida em relação a um pulso óptico de 1 ns de largura temporal contendo 76 fótons em média, resultando no perfil mostrado na figura 3.15 (observe que o final da janela está mostrada à esquerda, devido à sua varredura em relação ao pulso óptico). Se o pulso for atenuado em

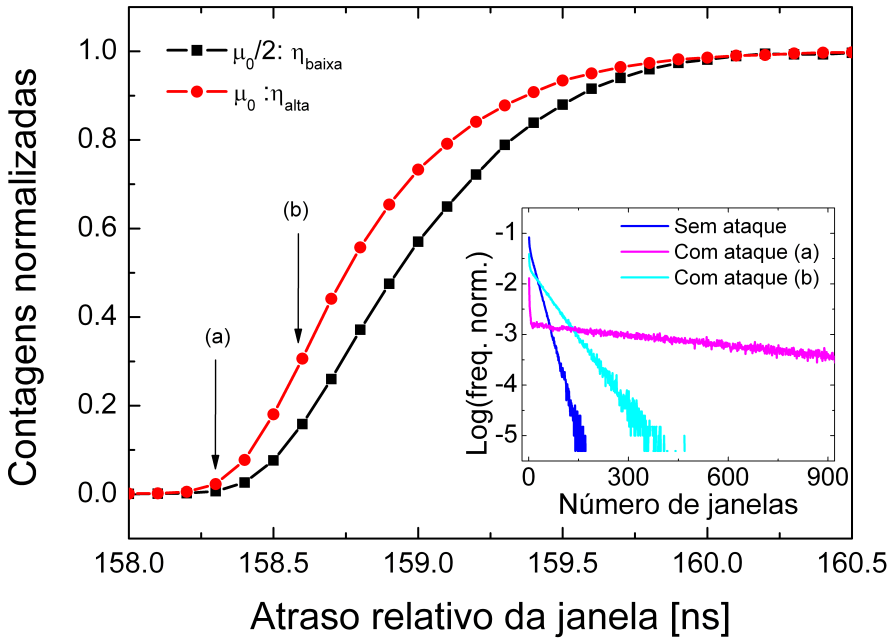

Figura 3.15: Varredura da janela de detecção do SPAD em relação a um laser pulsado com dois valores do número médio de fótons por pulso diferentes em 3dB. No detalhes são vistos os histogramas de tempos entre contagens medidos com o detector sob ataque (FAG) em duas posições diferentes de operação (a e b) e sem ataque.

3 dB, o perfil da janela varia, como mostrado na figura 3.15, deslocando a curva de eficiência de detecção. Foram escolhidos dois pontos de operação, identificados como (a) e (b) na figura. No primeiro, a razão entre as eficiências alta e baixa é máxima (4,3 vezes), correspondendo à situação em que há o maior

ganho de informação pelo interceptador. Entretanto, a eficiência relativa ao máximo da janela é reduzida para 0,0364 e 0,0084, com 76 e 38 fótons em média, respectivamente. No detalhe da figura, são mostrados os histogramas medidos com o detector sob o ataque FAG e sem ataque. A eficiência observada reduziu-se a 0,027 do valor original, o que é observado como uma menor inclinação da curva (mais horizontal). Eva poderia compensar esta redução tornando o enlace entre ela e Bob aproximadamente 16 dB mais transparente, se houver tal margem, ou poderia estar presente durante o estabelecimento da conexão, em que as perdas são estimadas, forjando uma perda maior para criar margem para compensação. Por exemplo, considerando um enlace entre Alice e Bob com 80 km, Eva poderia colocar sua estação de interceptação próxima à saída de Alice e seu laser na entrada de Bob, ou mesmo compensar a potência dos pulsos de forma que tenham a potência correta no fim da fibra. Em outras palavras, a redução dos *time-slots* vazios (sem fótons) poderia compensar a redução de eficiência. Entretanto, mesmo compensando a eficiência, o ataque ainda deixa marcas no SPAD. A probabilidade de pós-pulsos reduziu-se em 0,55 quando o ataque foi executado em relação à condição normal de operação, sem aplicação de tempo morto após detecções.

O ataque FAG foi operado em um segundo ponto, visando reduzir o efeito de diminuição da eficiência global (às custas de uma menor extração de informação pelo interceptador). A razão entre os valores de eficiência variando o número médio de fótons por pulso em 3 dB reduziu para 1,93, com menor perda da eficiência global, de 0,353. A probabilidade de pós-pulsos sob ataque reduziu em 0,745 em relação ao caso sem ataque, ainda detectável com o sistema de monitoramento.

A redução da probabilidade de pós-pulsos pode estar relacionada à menor tensão de excesso de polarização no final da janela, resultando em menor fluxo de cargas elétricas pelo detector e, consequentemente, menor população de armadilhas, em relação à incidência de fótons no meio da janela quando sob operação convencional. Em resumo, o método de monitoramento se mostrou eficaz contra o FAG em determinadas condições, através da verificação da redução da eficiência de detecção ou da probabilidade de pós-pulsos.

3.5 Discussão sobre a aplicação do sistema de monitoramento contra ataques do tipo blinding

Nesta seção é discutida a potencial aplicação do método de monitoramento contra ataques do tipo *blinding*, em que o detector é temporariamente desabilitado por meio de um sinal óptico externo. Nesta classe de ataques,

um sinal óptico, CW ou pulsado, é enviado pelo interceptador para "cegar" o detector, seja através de processo térmico ou elétrico. Eva utiliza um pulso forte para manipular a resposta dos detectores e impor o resultado obtido ao medir o qubit interceptado. O esquema de monitoramento proposto nas seções anteriores não requer intervenção interna no SPAD e pode acrescentar uma dificuldade extra do ponto de vista do interceptador. Além de Eva ter de recriar a estatística de detecção do SPAD durante o ataque, para evitar ser flagrada, há a possibilidade de Bob alterar intencionalmente algum parâmetro do detector aleatoriamente durante a comunicação, como o tempo morto ou a eficiência, com objetivo de verificar a ocorrência de eventos indesejados, ao custo de uma possível redução da taxa de comunicação.

Outro ataque recentemente proposto baseia-se na imposição de tempo-morto a um detector operando em modo *free-running* em um sistema síncrono [105], comum em implementações em espaço-livre [113]. Nestes sistemas geralmente são considerados apenas os eventos de detecção que ocorrerem durante os time-slots, definidos pelo sincronismo dos lasers pulsados utilizados. O interceptador envia um pulso óptico fraco, com 16 fótons em média, em um determinado estado (codificação em polarização, por exemplo) imediatamente antes do bit-slot. O detector correspondente àquele estado irá clicar, entrando no período de tempo morto. Este evento não é considerado pelo sistema e, caso o qubit enviado por Alice esteja preparado em uma base compatível com a medição, terá probabilidade unitária de ser detectado no SPAD correto. Deste modo, Eva obtém informação sobre a chave criptográfica sem realizar interceptação, preservando a QBER.

Como no caso do monitoramento do ataque *time-shift*, pode-se monitorar os eventos de contagem do SPAD em função do tempo. O monitoramento dos tempos entre detecções, considerando inclusive os eventos ocorridos fora dos time-slots, pode identificar o ataque. Mesmo se for adotada a estratégia de enviar pulsos em tempos aleatórios, simulando ruído de fundo, como proposto em [105], o monitoramento da eficiência de detecção e da probabilidade de contagem de escuro poderiam revelar o ataque.

A figura 3.16 mostra a medição tempo morto de um detector de silício operando em modo *free-running* realizada com um cartão de aquisição de 100 MS/s para uma fonte laser CW emitindo em 900 nm, cuja potência óptica foi variada de modo a obter diferentes taxas de contagem à saída do SPAD. O tempo morto medido foi de aproximadamente 40 ns, em concordância com a especificação do fabricante. O tempo de iluminação CW necessário para atingir a condição de supressão de contagens, aproximadamente 500 ns, é muito maior que a resolução de 10 ns do sistema de aquisição, permitindo o monitoramento

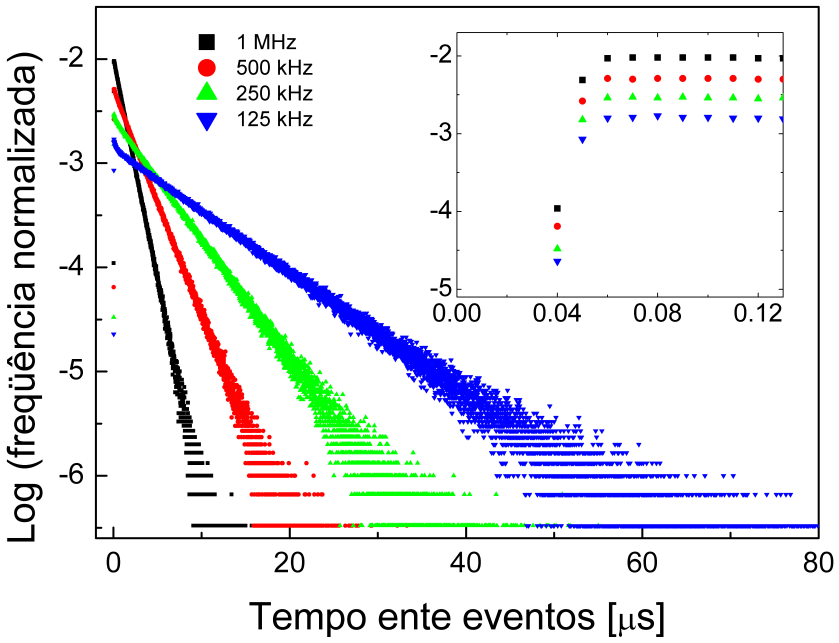

Figura 3.16: Varredura da janela de detecção do SPAD em relação a um laser pulsado com dois valores do número médio de fótons por pulso diferentes em 3dB. No detalhes são vistos os histogramas de tempos entre contagens medidos com o detector sob ataque (FAG) em duas posições diferentes de operação e sem ataque.

do detector.

4
Otimização dos parâmetros de um detector de fótons únicos baseado em fotodiodos avalanche sequencialmente acionado

A performance de SPADs baseados em InGaAs é severamente limitada pelo efeito de pós-pulsos. Mesmo quando operados em modo gatilhado, a degradação deste fenômeno pode ser significativa, dependendo da freqüência de gatilho utilizada. Como alternativa à redução da taxa de operação, pode-se impor um tempo morto após cada evento de detecção, com prejuízo da freqüência efetiva de operação. No capítulo 2 foram citadas algumas técnicas para redução dos pós-pulsos através de uma rápida cessação da corrente de avalanche. Estes métodos, porém, implicam na adoção de circuitos de polarização elétrica de grande complexidade e ajustes sensíveis.

Este capítulo apresenta a simulação de um dispositivo contador de fótons baseado na associação de diversos SPADs, estes assumidos como dispositivos comerciais padrão. Os detectores são sequencialmente acionados e gatilhados, o que impõe um tempo morto intrínseco devido ao ciclo de chaveamento. O objetivo principal desta configuração é a redução da probabilidade final de pós-pulso, que possibilite a elevação da freqüência de operação do dispositivo. Inicialmente, é feita a comparação de um SPAD único com o dispositivo sequencial. Em seguida, são analisadas as implicações no desempenho devido a uma chave óptica com parâmetros realistas. Para contornar as perdas impostas pela chave, os detectores são resfriados e a tensão de excesso de polarização é ajustada para aumentar a eficiência de detecção, o que também é considerado na análise.

4.1
Detector baseado em SPADs sequencialmente acionados

A otimização de determinado parâmetro de um SPAD é geralmente acompanhada pela deterioração de outra característica. A eficiência de detecção, por exemplo, é função da tensão de excesso de polarização, aumentando com este valor [27]. Entretanto, esta ação também acarreta no aumento da probabilidade de contagem de escuro. A redução da temperatura do detector, por outro lado, tem efeito inverso em relação às contagens de escuro, mas implica no

aumento da probabilidade de ocorrência de pós-pulsos.

Como mencionado anteriormente, um SPAD é basicamente composto por um APD reversamente polarizado e um circuito de extinção de avalanche, para operação em modo Geiger. Quando operado em modo gatilhado, o detector torna-se apto a detectar um único fóton durante o curto intervalo de duração temporal da janela, acionada por um sinal de gatilho. A eficiência de detecção depende de vários fatores, como a temperatura da junção e a tensão de excesso de polarização. Dado que um fóton é absorvido durante uma janela de detecção e um par de portadores elétricos é gerado na camada de depleção do SPAD, a probabilidade de ocorrência de uma avalanche depende do coeficiente de ionização da camada de multiplicação, onde há uma alta concentração de campo elétrico [41]. A tensão de excesso de polarização em relação ao limiar de ruptura não apenas aumenta a eficiência de detecção como causa um aumento linear da probabilidade de contagens de escuro. A partir de certo valor de tensão, entretanto, a probabilidade de tunelamento de portadores elétricos através da barreira de potencial se comporta de modo supra-linear [40].

A contribuição para as contagens de escuro de origem térmica pode ser reduzida através do resfriamento do APD, de acordo com a distribuição de Boltzmann. A fraca dependência da probabilidade de tunelamento de cargas impõe um limite à redução térmica de ruído. Além disso, a redução da temperatura do fotodiodo traz duas conseqüências. A primeira é a variação do limiar de ruptura do APD, à qual a tensão de excesso está relacionada. A segunda se refere ao aumento da constante de decaimento das armadilhas responsáveis pelo pós-pulsos. A probabilidade de ocorrência de um pós-pulso decai exponencialmente com o tempo de acordo com a constante de tempo dada pela equação de Arrhenius [33]

$$\tau = \frac{1}{T^2} e^{\frac{E_a}{kT}} , \tag{4-1}$$

sendo E_a a energia de ativação da armadilha dominante [J], T a temperatura da junção [K] e k a constante de Bolztmann [JK^{-1}].

Considerando um valor típico para a energia de ativação em torno de 0,1 eV [33] para um SPAD baseado em InGaAs, a constante de tempo aumenta por um fator 2,6 ao resfriar-se o detector de uma temperatura usual de -50^{o}C para -90^{o}C. Os módulos contadores de fótons comercialmente disponíveis são ajustados de modo a minimizar a probabilidade de contagem de escuro, enquanto a eficiência de detecção é mantida em um nível aceitável.

Devido ao baixo valor típico do ciclo de trabalho, o detector permanece inoperante e polarizado abaixo da tensão de ruptura a maior parte do tempo. Este modo de operação possibilita o escoamento das cargas armadilhadas pelo

semicondutor, reduzindo o efeito de pós-pulso. Entretanto, dependendo da freqüência de operação, o período de gatilho pode não ser suficientemente grande para mitigar este efeito. Como solução alternativa à aplicação de um tempo morto adicional, é proposta a construção de um detector de fótons únicos sequencialmente ativado, doravante chamado SASPD (do inglês *sequentialy-activated single-photon detector*).

O SASPD baseia-se em tecnologia atualmente disponível e compõe-se basicamente de uma série de SPADs operando em modo gatilhado. Os detectores são opticamente acessados através uma chave óptica rápida, como mostrado na figura 4.1, e sequencialmente acionados, de acordo com a ocorrência de eventos de detecção.

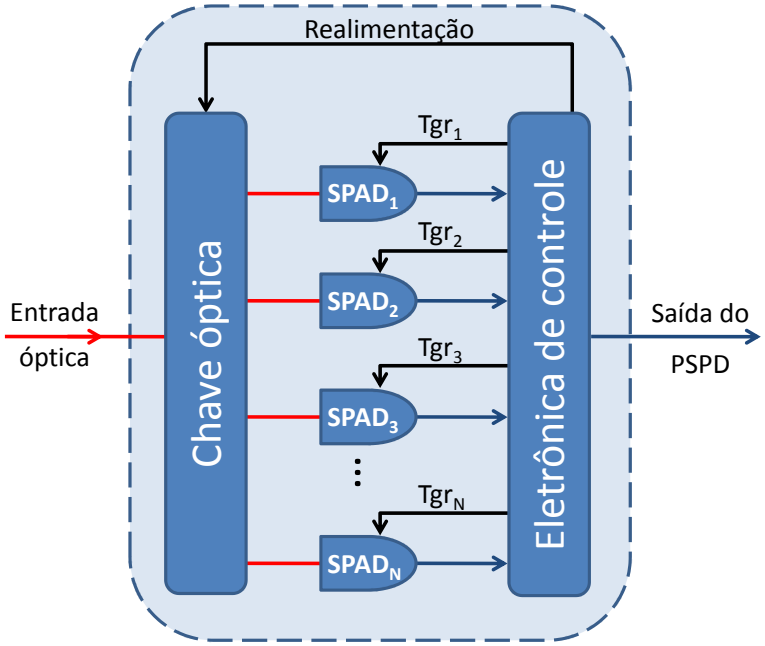

Figura 4.1: Diagrama esquemático do detector de fótons únicos paralelizado (SASPD) proposto.

Apenas um detector é gatilhado por vez, o que ocorre de forma síncrona (ou de acordo com um sinal de gatilho externo, dependendo da aplicação), mantendo-se os demais polarizados logo abaixo da tensão de ruptura. A polarização próxima a este limite inferior tem efeito benéfico para o decaimento das armadilhas, devido ao efeito Franz-Keldish [27]. Quando um evento de detecção ocorre, a chave óptica é acionada e comuta a conexão óptica da entrada para o próximo SPAD que passa a ser gatilhado. O acionamento sequencial garante que seja acionado o detector cuja última avalanche ocorreu há mais tempo. O tempo morto intrínseco proporcionado por esta estratégia estende o tempo disponível para o escoamento das armadilhas de cada SPAD

entre duas detecções consecutivas no mesmo elemento. O ciclo de operação mínimo do SASPD é dado por N detectores vezes o períodos de gatilho. Porém, devido à natureza estatística dos fótons e à eficiência não unitária dos SPADs, o valor médio de tempo entre acionamentos é estendido.

Chaves ópticas comerciais apresentam perda de inserção típica de 1 dB, com máxima taxa de comutação de 1 MHz. Analisando dados publicados em [114], verifica-se a possibilidade de compensação desta perda óptica através do resfriamento dos SPADs. Reduzindo-se a temperatura em 40 K, para 180 K, e corrigindo-se a tensão de excesso de polarização, um fator de acréscimo de 1,9 pode ser obtido para a eficiência de detecção, mantendo-se a probabilidade de contagem de escuro constante. Este fator permite o cascateamento de até três chaves ópticas, resultando em um arranjo de até oito detectores em paralelo. A contra-partida é a extensão da constante de tempo de armadilhamento e o conseqüente aumento da probabilidade de pós-pulsos. O ciclo de chaveamento estendido é utilizado para supressão deste efeito, e sua eficácia dependerá do número de detectores utilizados e da freqüência de operação.

4.2 Simulação de Monte-Carlo

Devido à complexidade do modelo de tempos entre detecções quando considerados diversos SPADs, com seus respectivos decaimentos exponenciais das armadilhas, a avaliação do SASPD proposto é feita através da simulação do dispositivo com o método de Monte-Carlo. A simulação numérica é feita janela a janela de detecção, considerando-se a probabilidade de existência e detecção de um fóton durante este período, a probabilidade de ocorrência de uma contagem de escuro e a probabilidade de pós-pulso, com cada detector mantendo o histórico de seu decaimento exponencial. O número de janelas de detecção ativadas entre duas detecções consecutivas do SASPD é registrado e um histograma similar ao apresentado no capítulo 2 é composto. Foi utilizado o gerador pseudo-aleatório Mersenne-Twister, cujo período de repetição é $(2^{19937}-1)/2$, para a geração de 1×10^6 eventos consecutivos.

Dado que a chave óptica comutou para um determinado detector – por exemplo $SPAD_1$ – as janelas de detecção são periodicamente acionadas, o que equivale ao teste probabilístico da ocorrência de um evento de detecção através da geração de um número aleatório para cada janela. A probabilidade de pós-pulso do detector ativo é considerada e reduz-se exponencialmente a cada novo teste, assim como a dos demais. A ocorrência de um evento de detecção, ou resultado positivo do teste de probabilidade, pára o contador de janelas, cujo valor é armazenado, e atribui a ele valor zero. A chave é comutada para o

próximo detector ($SPAD_2$), cuja origem da exponencial remonta ao seu último acionamento. A origem do decaimento das armadilhas do $SPAD_1$ é redefinida. A cada novo número aleatório gerado, o contador de tempo é incrementado, caso não ocorra resultado correspondente a um evento de detecção, ou seu valor é armazenado e a chave acionada, caso contrário. Este algoritmo é ilustrado na figura 4.2, onde os retângulos verticais representam eventos de detecção, os retângulos horizontais indicam o detector habilitado e as setas mostram a sequência de chaveamento. Em destaque são mostrados os número de janelas de detecção (estas correspondendo às marcações no eixo horizontal) acionadas entre detecções consecutivas. A probabilidade de detecção de um fóton ou de

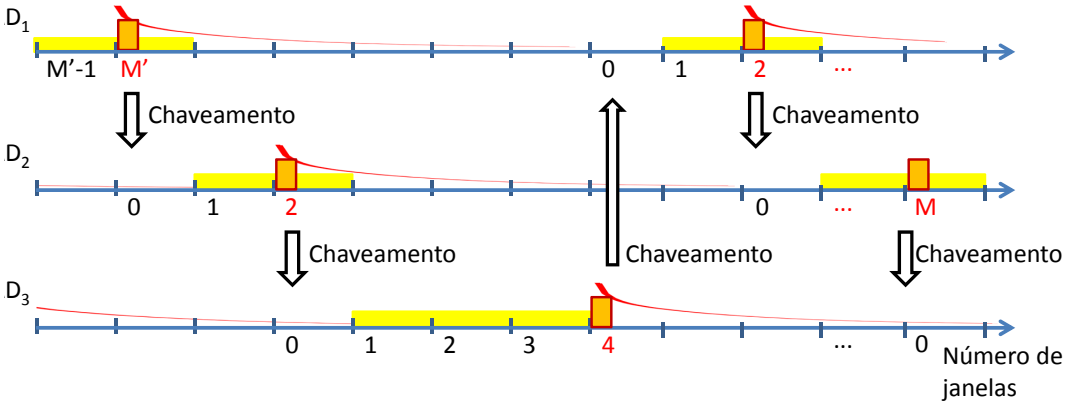

Figura 4.2: Representação esquemática da seqüência de chaveamento e aquisição para um SASPD composto por 3 SPADs. Curvas vermelhas indicam decaimento da probabilidade de pós-pulsos, retângulos laranja representam eventos de detecção, barras amarelas indicam o detector habilitado e as setas mostram a comutação da chave óptica.

ocorrência de uma contagem de escuro, dadas pelo complemento da equação (2-4) e por uma constante, respectivamente, são independentes da freqüência de gatilho, o mesmo não ocorrendo para a probabilidade de pós-pulso, dada pela equação (2-5).

A partir do histograma é extraída a probabilidade de ocorrência de pós-pulsos através do método das áreas, apresentado no capítulo 2. A figura 4.3a mostra o histograma gerado quando utilizados diferentes números de SPADs, operados com freqüência entre 0,5 e 10 MHz. O detalhe da figura destaca os intervalos curtos de tempo. Quando considerada uma chave óptica com parâmetros realistas, a eficiência de detecção é corrigida de acordo com a perda óptica, em função do número de detectores ou ramificações. Neste caso, os detectores foram resfriados a -90°C, com correção da tensão de excesso para manutenção da probabilidade de contagem de escuro em $1,5 \times 10^{-4}$ por janela nominal de 5 ns, resultando em aumento da constante de armadilhamento de 2,8 μs para

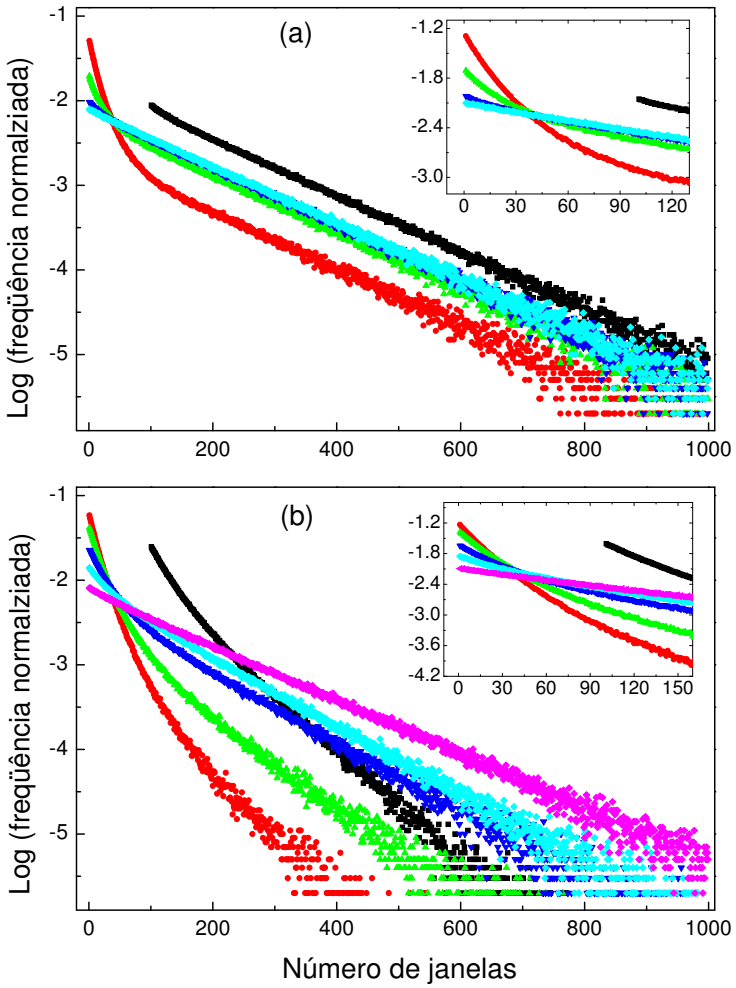

Figura 4.3: Histogramas da simulação do SASPD (a) temperatura normal e (b) resfriado, com chave óptica com perda.

6,9 μs. A eficiência de detecção é reduzida em 1 dB por chave óptica 1×2 cascateada, a partir do valor inicial de 28,5%, e os histogramas são mostrados na figura 4.3b.

4.3 Resultados

A probabilidade de pós-pulsos do SASPD foi calculada com o dispositivo operando em diferentes freqüências de gatilho. Estes valores são mostrados na figura 4.4 para detectores resfriados e com chave real.

Os valores de referência são representados por linhas tracejadas, que correspondem à probabilidade de pós-pulsos de um único SPAD operado em temperatura usual e com aplicação de tempo morto de 10 μs após cada evento de detecção. O eixo horizontal superior indica o valor efetivo da eficiência de detecção resultante da inserção de uma, duas ou três chaves ópticas cascateadas, dependendo do número de ramificações necessário. Observa-se

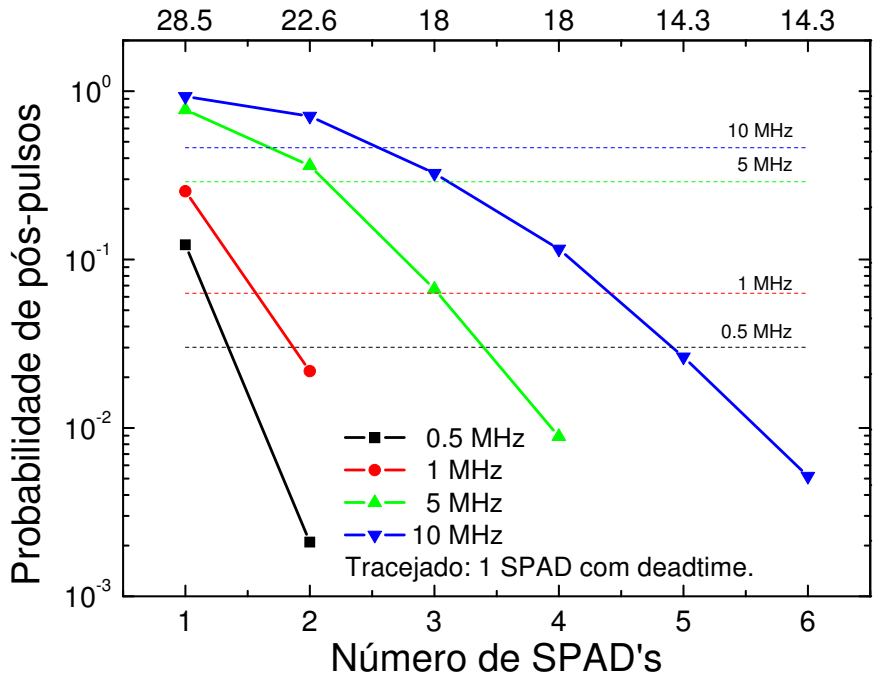

Figura 4.4: Probabilidade de pós-pulsos do SASPD resfriado, considerando uma chave óptica com parâmetros realistas. As curvas tracejadas representam o valor de referência de um único SPAD à temperatura padrão. Os símbolos abertos correspondem a 1 SPAD resfriado operando com tempo morto de 10 μs.

o decréscimo da probabilidade de pós-pulsos com o aumento do número de SPADs. Isto se deve ao aumento do tempo disponível para escoamento das cargas armadilhadas em cada SPAD proporcionado pelo ciclo de chaveamento.

O número de SPADs necessário para obter uma probabilidade de pós-pulsos menor que 1% é indicado na figura 4.5 para cada freqüência de gatilho dos dispositivos.

Mesmo com a extensão da constante de tempo por causa do resfriamento, o tempo morto intrínseco do SASPD garante, a partir de certo número de SPADs, a obtenção de baixa probabilidade de pós-pulso, mesmo em taxas elevadas de repetição. Considerando os detectores resfriados, foi obtida probabilidade de pós-pulso menor que 1% para freqüência de gatilho de 0,5, 1, 5 e 10 MHz a partir de 2, 3, 4 e 6 detectores concatenados, respectivamente. Um ganho de eficiência de 20% pode ser observado quando utilizados 4 detectores operando em 5 MHz, com probabilidade de pós-pulso menor que 1%. Estes resultados indicam a possibilidade de elevação da freqüência de operação de um detector de fótons únicos utilizando tecnologia atualmente disponível comercialmente sem aplicação de complexos esquemas de polarização elétrica e

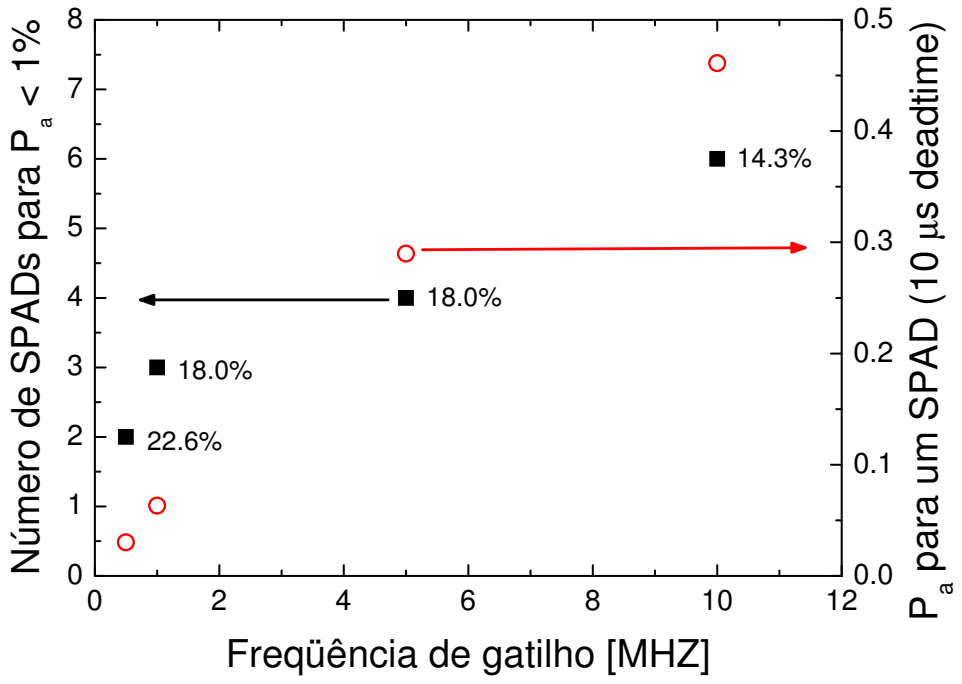

Figura 4.5: Número de SPADs associados no SASPD para obtenção de probabilidade de pós-pulsos menor que 1% em diferentes freqüências, considerando uma chave óptica com parâmetros realistas. Também é indicada a probabilidade de pós-pulso correspondente para apenas um SPAD operado a temperatura ambiente e com tempo morto de 10 μs após detecções.

extinção de avalanche.

5
Interferência estável entre lasers independentes para comunicação quântica segura

Sistemas de comunicações quânticas permitem a transferência de um estado quântico para um ponto remoto [1]. Além da distribuição quântica de chaves, outros protocolos incluem a teleportação de estado quântico [91][92] e a codificação densa [115][116]. No primeiro, é feita uma medida projetiva do estado quântico original com um fóton de um par emaranhado, através de uma medida de Bell. O resultado (uma dentro de quatro possibilidades) é enviado classicamente para o ponto remoto de transferência, onde o outro fóton do par sofre uma transformação unitária de acordo com a informação recebida. Os principais pontos deste protocolo se resumem ao fato de o estado quântico original não ser diretamente enviado, além de ser destruído no processo de medição, sem revelar informação suficiente para recriá-lo (o que obedece ao teorema da não-clonagem). Já a codificação densa permite o envio de dois bits de informação através um único fóton de um par emaranhado, utilizando também comunicação clássica auxiliar.

Qualquer sistema de comunicação, seja clássico ou quântico, está, em princípio, limitado pelas perdas do canal de propagação. Apesar de informação clássica poder ser amplificada ou recondicionada através de estações repetidoras, o mesmo não acontece para estados quânticos, devido ao teorema da não-clonagem. Uma solução é a utilização de repetidores quânticos. O protocolo BDCZ (Briegel, Dur, Cirac e Zoller) [117], propõe a utilização de memórias quânticas para armazenar fótons remotamente localizados e emaranhados entre si, para posterior utilização em teleportação. Além da memória quântica, outro recurso utilizado neste protocolo é a teleportação de emaranhamento (*entanglement swapping*)[118], em que dois fótons oriundos de dois pares emaranhados totalmente independentes são emaranhados entre si, através de uma medida projetiva dos outros dois fótons dos pares. O cascateamento destes nós, com etapas de purificação do estado final emaranhado [119][120], permite a obtenção de um par emaranhado cujos fótons localizam-se a uma distância maior que a originalmente factível através de propagação por um enlace direto de fibra óptica.

Para contornar as limitações impostas pela necessidade de utilização de memórias quânticas, foi proposto o protocolo DLCZ [121], que utiliza o emaranhamento de conjuntos atômicos (*atomic ensembles*) remotamente localizados, através de operações realizadas com óptica linear sobre os fótons emitidos por estes dispositivos. Entretanto, a necessidade de estabilização de fase dos canais quânticos constituem grande desafio tecnológico [122].

Um protocolo híbrido foi recentemente proposto [123][122], com a utilização de conjuntos atômicos e medidores de estado de Bell. Além de não utilizar memórias quânticas, o canal deve ser mais estável que o tempo de coerência dos fótons, valor muito menos crítico. Um ponto central deste protocolo se refere à medida projetiva em um analisador de estados de Bell (BSM, do inglês *Bell state measurement*) [118] realizada em pares de fótons, cada um emitido por um dos conjuntos atômicos, em uma configuração equivalente a um interferômetro de Hong-Ou-Mandel (HOM) [124]. O resultado da medida de Bell revela o estado emaranhado criado entre os dois conjuntos atômicos. A base desta medida depende do efeito de agrupamento (*photon bunching*), observado com a incidência de dois fótons indistinguíveis em um divisor de feixe (BS). Ambas as partículas emergem aleatoriamente na mesma porta de saída do BS. A indistinguibilidade dos fótons deve englobar diferentes graus de liberdade, como freqüência e tempo de coerência, incluindo o estado de polarização [125].

Interferência de um único fóton é conhecida há bastante tempo e constitui o princípio de QKD com codificação em *time-bins* [126]. Interferência entre dois fótons gerados por duas fontes fontes diferentes foi reportada utilizando-se SPDC de dois cristais bombeados pelo mesmo laser ou através de SPDC bombeada com um laser de freqüência dobrada combinada com amostra do mesmo laser na freqüência original [127]. Entretanto, interferência entre duas fontes totalmente independentes entre si requer o apagamento de qualquer informação que possa discriminar a origem dos fótons [125].

Outra aplicação do fenômeno de agrupamento de fótons foi recentemente proposta e visa resolver a vulnerabilidade imposta pelas imperfeições dos detectores de fótons únicos aos sistemas práticos de QKD. O assim chamado protocolo de distribuição quântica de chaves independente do dispositivo de medição (MDI-QKD, do inglês *measurement device independent QKD*) [17] permite que todo o sistema de medição seja controlado pelo interceptador, sem prejuízo para a segurança da comunicação. O principal recurso empregado é a medição de estados de Bell realizada sobre fótons indistinguíveis emitidos por fontes laser atenuadas independentes.

Considere inicialmente um sistema QKD baseado em pares de fótons

emaranhados (em polarização, por exemplo), como proposto em [83]. Uma estação central cria pares de fótons emaranhados em polarização, e envia um fóton para Alice e outro para Bob. Estes, similarmente ao caso do protocolo BB84, escolhem medir seus fótons em uma dentre duas bases, aleatoriamente escolhidas. seus resultados serão correlacionados quando as bases escolhidas forem compatíveis. A utilização de uma terceira base permite a redução da probabilidade de concordância entre as bases escolhidas e permite que a desigualdade de Bell seja testada [2]. Se a desigualdade de Bell for violada, significa que a fonte realmente emite estados emaranhados e não estados produto. Como ressaltado em [2], o fluxo de informação equivale à propagação em sentido reverso no tempo de Alice para a fonte de pares e então para Bob.

O protocolo MDI-QKD equivale ao protocolo baseado em pares de fótons emaranhados revertido no tempo [17]. Ao invés de os fótons de um par serem enviados a partir da estação central (Charlie) para Alice e Bob, estes enviam pulsos laser atenuados para a estação central, onde são medidos conjuntamente. Os resultados são pós-selecionados durante a reconciliação de bases, quando Charlie anuncia o resultado de suas medições e Alice e Bob compartilham as bases escolhidas por ambos para a preparação de cada pulso. A segurança é baseada no protocolo *decoy-states*, que permite estimar o ganho do canal e a QBER. Diferente de outros protocolos independentes dos dispositivos [128], o MDI-QKD em questão não necessita fechar o *loophole* de detecção, o que implicaria na utilização de detectores com alta eficiência de detecção e amplificação de qubit [129] ou medida quântica não destrutiva [65]. O uso de fontes laser atenuadas e o fato de não ser necessário um analisador de estados de Bell perfeito torna o protocolo MDI-QKD prático e realizável com tecnologia atual.

A primeira parte deste capítulo mostra a estabilização em polarização de dois canais quânticos, monitorada através dos efeito de agrupamento dos fótons emitidos por duas fontes independentes. Os resultados apresentados representam passo importante para a implementação prática do protocolo de repetidor quântico sobre fibra óptica com tecnologia atual. A segunda parte se refere à implementação de um sistema para MDI-QKD sobre os canais controlados com a realização de medidas de Bell na estação central remota.

5.1 Interferência em um divisor de feixe

Deseja-se obter a distribuição do número de fótons nos modos espaciais de saída $|\rangle_c$ e $|\rangle_d$ de um divisor de feixe (BS), em função dos estados incidindo em seus modos espaciais de entrada $|\rangle_a$ e $|\rangle_b$, identificados de acordo com a

figura 5.1.

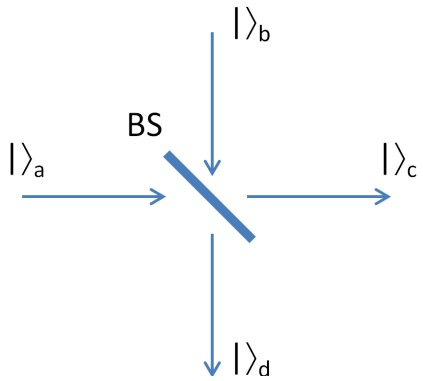

Figura 5.1: Modos espaciais de entrada ($|\rangle_a$ e $|\rangle_b$) e saída ($|\rangle_c$ e $|\rangle_d$) de um divisor de feixe (BS) com coeficientes de transmissão e reflexão t e r, respectivamente. Os valores de transmitância e reflectância obedecem à relação $|t|^2 + |r|^2 = 1$ e a fase relativa entre os modos de saída é $\pi/2$.

Sendo $\hat{x}^\dagger$ o operador criação atuando no modo $|\rangle_x$, a relação entre as entradas e saídas do BS pode ser descrita como

$$\begin{aligned} \hat{a}^\dagger &= t\hat{c}^\dagger + jr\hat{d}^\dagger \\ \hat{b}^\dagger &= jr\hat{c}^\dagger + t\hat{d}^\dagger \,, \end{aligned} \tag{5-1}$$

de forma que a diferença de fase entre as duas saída é $\pi/2$ e $|t|^2 + |r|^2 = 1$. [1]

A incidência de um fóton em uma porta de entrada do BS (com um estado vácuo na outra porta) pode ser tratada com a aplicação direta das eqs. 5-1:

$$\begin{aligned} |1,0\rangle_{a,b} &\rightarrow t|1,0\rangle_{c,d} + jr|0,1\rangle_{c,d} \\ |0,1\rangle_{a,b} &\rightarrow jr|1,0\rangle_{c,d} + t|0,1\rangle_{c,d} \,. \end{aligned} \tag{5-2}$$

Isto significa que o fóton emergirá aleatoriamente em um dos modos de saída do BS com probabilidade $|t|^2$ ou $|r|^2$.

A generalização do caso anterior, com estados de Fock com maior número de fótons, é obtida a partir da distribuição binomial dos fótons de entrada entre as saídas do BS, ou seja,

$$|M,0\rangle_{a,b} \rightarrow \sum_{m=0}^{M} j^m \sqrt{\frac{M!}{m!(M-m)!}} t^{M-m} r^m |M-m,m\rangle_{c,d}$$

[1] Aqui considerou-se r e t idênticos para ambos os modos de polarização horizontal e vertical, respectivamente paralelo (modo TM) e perpendicular (modo TE) ao plano de incidência no BS [60].

$$|0,N\rangle_{a,b} \rightarrow \sum_{n=0}^{N} j^n \sqrt{\frac{N!}{n!(N-n)!}} t^{N-n} r^n |n,N-n\rangle_{c,d}\,. \tag{5-3}$$

No caso da incidência de dois fótons indistinguíveis, um em cada modo de entrada, a saída será

$$|1,1\rangle_{a,b} \rightarrow (t^2-r^2)|1,1\rangle_{c,d} + jrt(|0,2\rangle_{c,d} + |2,0\rangle_{c,d})\,. \tag{5-4}$$

Isto resulta, no caso de um BS simétrico ($|t| = |r| = 1/\sqrt{2}$), no fenômeno de agrupamento de fótons (*photon bunching*), em que ambos os fótons ocupam o mesmo modo de saída, aleatoriamente. Este efeito não aparece no caso de dois fótons distinguíveis (ortogonalmente polarizados, por exemplo). Considerando os modos $|\rangle_{a'}$ e $|\rangle_{b'}$, ortogonais aos modos $|\rangle_a$ e $|\rangle_b$, considere a incidência simultânea de um fóton no modo $|\rangle_a$ e um fóton no modo $|\rangle_{b'}$. Aanálise semelhante à acima resultará em

$$\begin{aligned} |1,0,0,1\rangle_{a,a',b,b'} \rightarrow \quad & t^2|1,0,0,1\rangle_{c,c',d,d'} - r^2|0,1,1,0\rangle_{c,c',d,d'} \\ & + jrt(|1,1,0,0\rangle_{c,c',d,d'} + |0,0,1,1\rangle_{c,c',d,d'}) \end{aligned} \tag{5-5}$$

Desprezando o grau de liberdade extra e agrupando os modos $|\rangle_a$ e $|\rangle_{a'}$ e os modos $|\rangle_b$ e $|\rangle_{b'}$, tem-se

$$\begin{aligned} |saída\rangle_{c+c',d+d'}\langle saída|_{c+c',d+d'} = \quad & \frac{1}{1+r^2t^2}|1,1\rangle_{c+c',d+d'}\langle 1,1|_{c+c',d+d'} \\ & + \frac{r^2t^2}{1+r^2t^2}(|2,0\rangle_{c+c',d+d'}\langle 2,0|_{c+c',d+d'} \\ & + |0,2\rangle_{c+c',d+d'}\langle 0,2|_{c+c',d+d'}) \end{aligned} \tag{5-6}$$

ou seja, 50% de probabilidade de ser encontrado apenas um fóton em cada modo espacial de saída e 25% de probabilidade de ambos os fótons serem encontrados no mesmo modo, $|\rangle_c$ ou $|\rangle_d$ (com vácuo na outra porta), caso o BS seja simétrico.

No caso geral em que M fótons indistinguíveis incidem no modo $|\rangle_c$ e N fótons, no modo $|\rangle_d$, a distribuição à saída será [58] [2]

$$\begin{aligned} |M,N\rangle_{a,b} \rightarrow \quad & \sum_{m=0}^{M}\sum_{n=0}^{N} \frac{j^{m+n} * \sqrt{M!N!(M-m+n)!(N-n+m)!}}{(M-m)!m!(N-n)!n!} \\ & \times t^{M+N-m-n} r^{m+n} |M-m+n, N-n+m\rangle_{c,d} \end{aligned} \tag{5-7}$$

[2] A equação A.18 da referência citada foi modificada para que a diferença de fase entre as portas de saída do BS seja $\pi/2$, de acordo com [130]. Foi corrigido o expoente do termo de fase para m+n.

5.1.1 Estados coerentes

Considere agora um estado coerente, definido como uma superposição de estados de Fock [58][130], ou seja,

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \,. \tag{5-8}$$

A incidência de um estado deste tipo em um BS, tendo o vácuo no outro modo espacial de entrada, resulta em estados coerentes à saída do dispositivo. Isto pode ser mostrado reescrevendo-se o estado coerente como o operador deslocamento de Glauber aplicado sobre o vácuo e utilizando-se as eqs. 5-1, ou seja [130],

$$\begin{aligned}
|\alpha,0\rangle_{a,b} &= \hat{D}_a(\alpha)|0\rangle_a|0\rangle_b \\
|\alpha,0\rangle_{a,b} &\rightarrow e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}|0,0\rangle_{a,b} \\
|\alpha,0\rangle_{a,b} &\rightarrow e^{\hat{c}^\dagger + jr\hat{d}^\dagger - \alpha^* t\hat{c} + jr\hat{d}}|0,0\rangle_{c,d} \\
|\alpha,0\rangle_{a,b} &\rightarrow e^{\alpha t\hat{c}^\dagger - \alpha^* t\hat{c}} e^{jr\alpha\hat{d}^\dagger - (-jr\alpha^*\hat{d}}|0,0\rangle_{c,d} \\
|\alpha,0\rangle_{a,b} &\rightarrow |t\alpha, jr\alpha\rangle_{c,d} \\
|\alpha,0\rangle_{a,b} &\rightarrow e^{-\frac{|\alpha|^2}{2}} \sum_{m=0}^{\infty}\sum_{n=0}^{\infty} j^n \frac{\alpha^{m+n} t^m r^n}{\sqrt{m!n!}} |m,n\rangle_{c,d}
\end{aligned} \tag{5-9}$$

E, de forma análoga,

$$\begin{aligned}
|0,\alpha\rangle_{a,b} &\rightarrow |jr\alpha, t\alpha\rangle_{c,d} \\
|0,\alpha\rangle_{a,b} &\rightarrow e^{-\frac{|\alpha|^2}{2}} \sum_{m=0}^{\infty}\sum_{n=0}^{\infty} j^m \frac{\alpha^{m+n} t^n r^m}{\sqrt{m!n!}} |m,n\rangle_{c,d}
\end{aligned} \tag{5-10}$$

Considerando dois estados de Fock como entrada, análise semelhante resultará em

$$\begin{aligned}
|\alpha_1,\alpha_2\rangle_{a,b} &= \hat{D}_a(\alpha_1)\hat{D}_b(\alpha_2)|0\rangle_a|0\rangle_b \\
|\alpha_1,\alpha_2\rangle_{a,b} &\rightarrow |t\alpha_1 + jr\alpha_2, jr\alpha_1 + t\alpha_2\rangle_{c,d}
\end{aligned} \tag{5-11}$$

que, ao expandir, resulta em uma série na forma

$$|\alpha_1,\alpha_2\rangle_{a,b} \rightarrow e^{-\frac{|\alpha_1|^2+|\alpha_2|^2}{2}} \sum_{m=0}^{\infty}\sum_{n=0}^{\infty} \frac{(t\alpha_1 + jr\alpha_2)^m (jr\alpha_1 + t\alpha_2)^n}{\sqrt{m!n!}} |m,n\rangle_{c,d}$$

$$|saída\rangle_{c,d} = A_1|0,0\rangle_{c,d} + A_2|1,0\rangle_{c,d} + A_3|0,1\rangle_{c,d} + A_4|1,1\rangle_{c,d} + ... \tag{5-12}$$

A probabilidade de ocorrência de um determinado número de fótons nas saídas do BS é dada pelo quadrado do módulo da amplitude de probabilidade

correspondente, como, por exemplo, $P(|1,0\rangle_{c,d}\langle 1,0|_{c,d}) = |A_2|^2$.

Tratamento semelhante é dispensado ao caso de dois estados coerentes distinguíveis (em freqüência, por exemplo) como entrada, ou seja,

$$|\alpha_1, 0, 0, \alpha_2\rangle_{a,a',b,b'} \rightarrow |t\alpha_1, jr\alpha_2, jr\alpha_1, t\alpha_2\rangle_{c,c',d,d'} \,. \tag{5-13}$$

Que, expandido, torna-se

$$\begin{aligned} |saída\rangle_{c,d} = A_1|0,0,0,0\rangle_{c,c',d,d'} + A_2|1,0,0,0\rangle_{c,c',d,d'} + A_3|0,1,0,0\rangle_{c,c',d,d'} + \\ A_4|1,1,0,0\rangle_{c,c',d,d'} + A_5|2,0,0,0\rangle_{c,c',d,d'} + A_6|0,2,0,0\rangle_{c,c',d,d'} + \\ A_7|0,0,1,0\rangle_{c,c',d,d'} + A_8|0,0,0,1\rangle_{c,c',d,d'} + ... \end{aligned} \tag{5-14}$$

Neste caso, as amplitudes de probabilidade dos modos espaciais ortogonais não podem ser agrupadas diretamentem ou seja, a probabilidade de ocorrência de um determinado número de fótons nas saídas do BS (desprezando-se o grau e liberdade extra) é dada pela soma dos módulos quadráticos das amplitudes de probabilidade correspondentes. Por exemplo, a probabilidade de ocorrência de dois fótons no mesmo modo temporal da saída "c" do BS com vácuo na saída "d", considerando ambos os modos $|\rangle_c$ e $|\rangle_{c'}$, será $P(|2,0\rangle_{c+c',d+d'}\langle 2,0|_{c+c',d+d'}) = |A_4|^2 + |A_5|^2 + |A_6|^2$, de acordo com a eq. 5-14.

O fenômeno de interferência pode ser observado através de um par de detectores de fótons únicos, colocado nas saídas do BS e gatilhado de forma a observar o mesmo modo temporal em ambos os braços. Isto significa que, dado que dois fótons deixam o divisor ao mesmo tempo por portas distintas, os detectores serão gatilhados no instante de incidência dos fótons em cada um. Um maior número de eventos coincidentes é esperado quando os fótons são distinguíveis, em relação ao caso em que há indistinguibilidade. A visibilidade da interferência pode ser quantificada através da equação [131]

$$V = \frac{C_{dist} - C_{ind}}{C_{dist}} \,, \tag{5-15}$$

sendo C_{dist} e C_{ind} a taxa de contagens coincidentes observada com os fótons distinguíveis e indistinguíveis, respectivamente. O máximo valor deste parâmetro para fontes poissonianas é 0,5, correspondendo ao caso de máximo contraste, obtido quando os fótons apresentam a mesma freqüência, mesma polarização e são observados no mesmo modo temporal. Este valor diverge do caso de dois fótons únicos, emitidos por fontes sub-poissonianas, cujo valor de visibilidade máxima tende à unidade [58]. A visibilidade da interferência também depende da intensidade relativa (R) dos dois lasers incidentes, de acordo com [131]

$$V(R) = \frac{2R}{(R+1)^2}\,, \tag{5-16}$$

sendo R=min$\{I_1,I_2\}$/max$\{I_1,I_2\}$.

Caso dois lasers com estados de polarização distintos sejam utilizados, a visibilidade dependerá da projeção dos estados de polarização. Considerando dois SOPs com ângulo relativo θ e mesma intensidade, a fração da intensidade do laser 2 (I_2) paralela ao laser 1 (I_1), será $I_2\cos^2\theta$, enquanto que $I_2\mathrm{sen}^2\theta$ – ortogonal a I_1– contribuirá com o aumento das contagens coincidentes. A visibilidade pode ser reescrita considerando a intensidade relativa como função da polarização de acordo com

$$V(\theta) = \frac{2\frac{cos^2\theta}{1+sen^2\theta}}{\left(1+\frac{cos^2\theta}{1+sen^2\theta}\right)^2}\,. \tag{5-17}$$

Considere aqui fontes ópticas CW, de forma que pode incidir luz nos detectores em qualquer instante de tempo. A abertura da janela de detecção em cada detector possibilitará um disparo de contagem, caso haja um fóton no período de tempo correspondente e de acordo com sua eficiência de detecção. O fenômeno de agrupamento, que pode ocorrer dentro do comprimento de coerências dos fótons das fontes – caso indistinguíveis – pode ser observado através do registro de contagens coincidentes entre os dois detectores. A taxa de contagens coincidentes é mínima quando os modos temporais dos detectores estão casados, o que significa que ambas as janelas de detecção são acionadas em intervalos de tempo correlacionados. Em outras palavras, as janelas são abertas de forma que o tempo de vôo de um par de fótons a partir do BS seja equivalente para os dois braços onde se localizam os detectores de fótons únicos. Caso os fótons se agrupem, um dos detectores não registrará contagem e, conseqüentemente, não haverá coincidência de cliques. Caso uma das janelas seja atrasada em relação à outra, um dos detectores poderá ou não detectar fótons, porém de forma descorrelacionada com o outro dispositivo. Nesta situação, é esperada a mínima taxa de coincidências, já que o efeito de agrupamento não é percebido pelo sistema de medição [3]. Varrendo-se o atraso relativo entre os detectores e tomando o número de coincidências em intervalos regulares de aquisição, espera-se um gráfico com a forma de um vale ("Hong-Ou-Mandel dip"), cuja região de mínimo corresponde à situação de casamento do atraso. A largura e a forma deste vale originam-se da convolução das janelas de detecção com a função de onda temporal dos fótons. Desta forma, quanto maior a coerência dos lasers utilizados, mais largo o vale é esperado, pois

[3]Os sistemas de medição tradicionais, usualmente composto por fotodiodos avalanche, não é capaz de resolver o número de fótons no mesmo modo espacial incidentes durante uma mesma janela de medição.

maior atraso é necessário para exceder o tempo de coerência dos fótons. O efeito discriminatório da janela de detecção deve também ser considerado pois sua largura deve ser tal que não possibilite a distinção da fonte de onde se originaram os fótons. Estabelece-se, portanto, um compromisso entre estes diversos fatores.

5.2 Protocolo para distribuição quântica de chaves independente dos detectores e a medida de Bell

Recentemente, foi proposto um protocolo para distribuição quântica de chaves independente das imperfeições dos detectores de fótons únicos. O protocolo não só se propõe a eliminar o *loop-hole* de detecção, como também os *side-channels* abertos pelos SPADs, permitindo, inclusive, que os detectores estejam sob o controle de Eva.

O esquema MDI-QKD [17] baseia-se em uma medida conjunta de dois pulsos ópticos enviados pelas partes que desejam compartilhar a chave criptográfica. Alice e Bob possuem estações compostas por um laser pulsado atenuado e ambos enviam pulsos ópticos contendo um número médio de fótons baixo, da ordem de 1 fóton por pulso [4], codificados em um determinado estado de polarização aleatoriamente escolhido, para uma estação central, chamado Charlie, como ilustrado na figura 5.2.

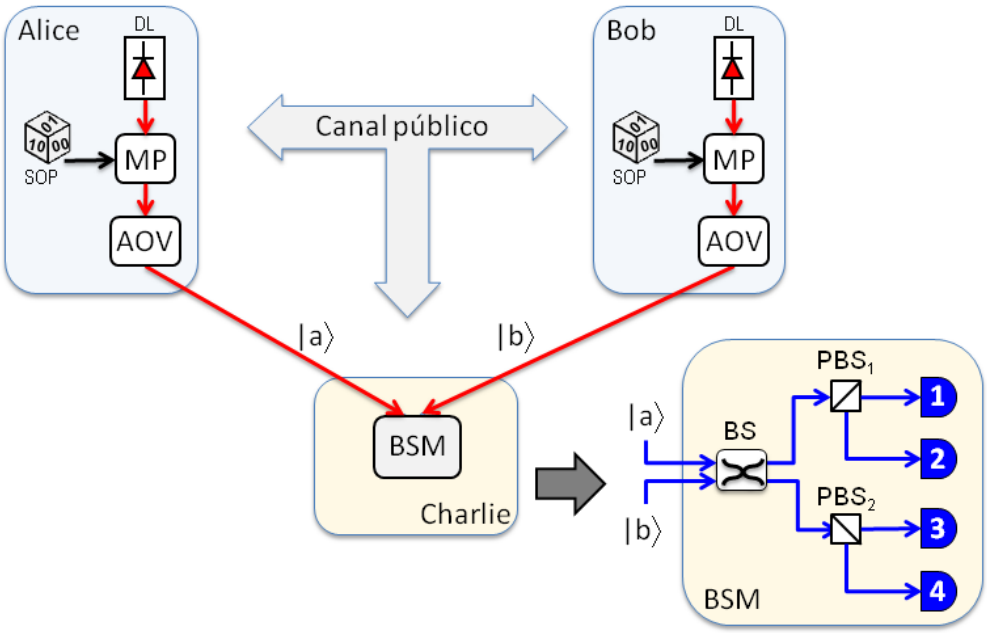

Figura 5.2: Diagrama esquemático do sistema de distribuição de chaves independente dos detectores.

[4]Valores da ordem de 1 fóton por pulso são possíveis graças ao protocolo *decoy states* [88][89]

Duas bases maximamente conjugadas são definidas ($\oplus$ e $\otimes$), cada uma formada por dois estados de polarização ortogonais, como no protocolo BB84 ($\oplus \rightarrow |\mathrm{H}\rangle$ e $|\mathrm{V}\rangle$; $\otimes \rightarrow |{+45}\rangle$ e $|{-45}\rangle$). A preparação dos fótons enviados por Alice e Bob pode ser feita através de um modulador de polarização (MP), escolhendo aleatoriamente dentre as quatro possibilidades. Na estação central, é feita uma medida interferométrica conjunta dos dois pulsos através de um analisador de estado de Bell, cuja resposta está contida em um conjunto de quatro possibilidades. Na etapa de reconciliação de bases, Charlie anuncia publicamente o resultado de suas medidas de Bell, seguido pelo anúncio de Alice e de Bob de suas bases de preparação. Sabendo então os instantes em que ambas as bases de preparação coincidiram e os resultados da medida de Bell, Alice e Bob podem calcular a taxa de erro e a taxa segura de geração da chave. Os detalhes do protocolo em função do resultado anunciado por Charlie serão descritos após a introdução do analisador de estados de Bell na próxima seção. O protocolo MDI-QKD faz uso de *decoy states* para potencialmente alcançar distância antes somente possíveis em sistemas baseados em fontes de pares de fótons emaranhados [18]. Isto é possível pois a estatística de eventos causados por pulsos contendo múltiplos fótons podem ser isolados dos eventos devidos a pulso com um fóton apenas, como será visto mais adiante.

5.2.1
Analisador de estados de Bell

Considere os estados de Bell, que definem um par de estados maximamente emaranhados na base computacional (considerando estados de polarização, por exemplo)

$$\begin{aligned}
|\phi^+\rangle &\rightarrow \frac{1}{\sqrt{2}}(|H\rangle_a|H\rangle_b + |V\rangle_a|V\rangle_b) \\
|\phi^-\rangle &\rightarrow \frac{1}{\sqrt{2}}(|H\rangle_a|H\rangle_b - |V\rangle_a|V\rangle_b) \\
|\psi^+\rangle &\rightarrow \frac{1}{\sqrt{2}}(|H\rangle_a|V\rangle_b + |V\rangle_a|H\rangle_b) \\
|\psi^-\rangle &\rightarrow \frac{1}{\sqrt{2}}(|H\rangle_a|V\rangle_b - |V\rangle_a|H\rangle_b)\,, \qquad \text{(5-18)}
\end{aligned}$$

onde $|\mathrm{H}\rangle_x$ e $|\mathrm{V}\rangle_x$ representam um estado de Fock $|1\rangle$ com polarização horizontal ou vertical, respectivamente, nos modos espaciais $|\rangle_a$ ou $|\rangle_b$.

Um analisador de estados de Bell (BSA, do inglês *Bell states analyzer*) corresponde a um dispositivo capaz de discriminar os estados mostrados na eq. 5-18. Utilizando-se óptica linear, é possível construir um BSA com resolução para dois estados de Bell, enquanto que os demais não retornam resultado

determinado. O BSA mostrado na figura 5.2.1 é composto por um BS seguido por dois PBS, em cujos modos de saída são colocados detectores de fótons únicos.

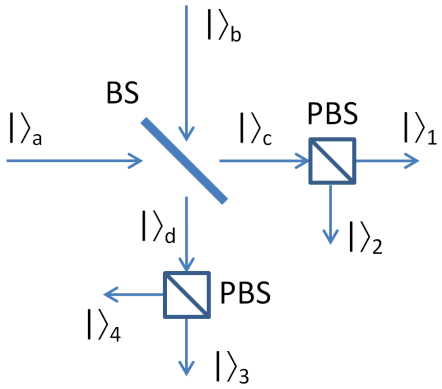

Figura 5.3: Analisador de estados de Bell. Em cada modo espacial de saída, $|\rangle_1$ a $|\rangle_4$, *écolocadoumdetectordefótonsúnicos.Amediçãodeestados*$|\psi^+\rangle$ e $|\psi^-\rangle$ é observada na forma de contagens coincidentes entre determinados pares de detectores. Os demais estados não podem ser discriminados nesta configuração.

A transformação imposta pelo BS é dada pela eq. 5-1. Considerando que cada estados horizontalmente polarizados são transmitidos pelo PBS e estados verticais são refletidos, a transformação realizada pode ser escrita como

$$\begin{aligned} \hat{c}^\dagger &= cos(\theta)\hat{1}^\dagger + jsen(\theta)\hat{2}^\dagger \\ \hat{d}^\dagger &= cos(\theta)\hat{3}^\dagger + jsen(\theta)\hat{4}^\dagger \,, \end{aligned} \tag{5-19}$$

em que θ corresponde ao ângulo entre o estado de polarização de entrada e a base determinada pelos PBS (base $\oplus$), ou seja, o estado de entrada pode ser descrito como $|\theta\rangle = cos(\theta)|H\rangle + sen(\theta)|V\rangle$. Combinando as equações 5-1 e 5-19, obtém-se a relação entre os modos de entrada e saída do BSA

$$\begin{aligned} \hat{a}^\dagger &\rightarrow tcos(\theta)\hat{1}^\dagger + jsen(\theta)\hat{2}^\dagger + jrcos(\theta)\hat{3}^\dagger - rsen(\theta)\hat{4}^\dagger \\ \hat{b}^\dagger &\rightarrow jrcos(\theta)\hat{1}^\dagger - rsen(\theta)\hat{2}^\dagger + tcos(\theta)\hat{3}^\dagger + jtsen(\theta)\hat{4}^\dagger \end{aligned} \tag{5-20}$$

.

5.2.2 Estados de Fock

Considere agora dois estados de Fock com um fóton apenas cada, incidindo nos modos de entrada do BSA. Os estados de polarização destes fótons é descrito por seu ângulo em relação aos PBS, θ e φ, relacionados aos

modos $|\rangle_a$ e $|\rangle_b$, respectivamente. Isto significa que, dependendo destes ângulos, os estados de polarização serão uma superposição dos estados horizontal e vertical, ou seja, $|\theta\rangle_a = cos\theta|H\rangle_a + sen\theta|V\rangle_a$ e $|\varphi\rangle_b = cos\varphi|H\rangle_b + sen\varphi|V\rangle_b$.

Assumindo fótons distinguíveis em determinado grau de liberdade – como freqüência ou tempo, por exemplo –, definem-se dois modos de entrada para cada modo espacial, ou seja, $|\theta,0\rangle_{a,b}|0,\varphi\rangle_{a',b'}$. A aplicação das transformações da eq. 5-20, leva ao seguinte resultado, em função dos modos de saída, observados na forma de detecções coincidentes entre dois detectores, ou como fótons recebido por um mesmo detector

$$
\begin{aligned}
|\theta,0,0,\varphi\rangle_{a,a',b,b'} \rightarrow \\
& jrtcos(\theta)cos(\varphi)|1,1,0,0,0,0,0,0\rangle_{1,1',2,2',3,3',4,4'} \\
& -rtcos(\theta)sen(\varphi)|1,0,0,1,0,0,0,0\rangle_{1,1',2,2',3,3',4,4'} \\
& +t^2cos(\theta)cos(\varphi)|1,0,0,0,0,1,0,0\rangle_{1,1',2,2',3,3',4,4'} \\
& +jt^2cos(\theta)sen(\varphi)|1,0,0,0,0,0,0,1\rangle_{1,1',2,2',3,3',4,4'} \\
& -rtsen(\theta)cos(\varphi)|0,1,1,0,0,0,0,0\rangle_{1,1',2,2',3,3',4,4'} \\
& -jrtsen(\theta)sen(\varphi)|0,0,1,1,0,0,0,0\rangle_{1,1',2,2',3,3',4,4'} \\
& +jt^2sen(\theta)cos(\varphi)|0,0,1,0,0,1,0,0\rangle_{1,1',2,2',3,3',4,4'} \\
& -t^2sen(\theta)sen(\varphi)|0,0,1,0,0,0,0,1\rangle_{1,1',2,2',3,3',4,4'} \\
& -r^2cos(\theta)cos(\varphi)|0,1,0,0,1,0,0,0\rangle_{1,1',2,2',3,3',4,4'} \\
& -jr^2cos(\theta)sen(\varphi)|0,0,0,1,1,0,0,0\rangle_{1,1',2,2',3,3',4,4'} \\
& +jrtcos(\theta)cos(\varphi)|0,0,0,0,1,1,0,0\rangle_{1,1',2,2',3,3',4,4'} \\
& -rtcos(\theta)sen(\varphi)|0,0,0,0,1,0,0,1\rangle_{1,1',2,2',3,3',4,4'} \\
& -jr^2sen(\theta)cos(\varphi)|0,1,0,0,0,0,1,0\rangle_{1,1',2,2',3,3',4,4'} \\
& +r^2sen(\theta)sen(\varphi)|0,0,0,1,0,0,1,0\rangle_{1,1',2,2',3,3',4,4'} \\
& -rtsen(\theta)cos(\varphi)|0,0,0,0,0,1,1,0\rangle_{1,1',2,2',3,3',4,4'} \\
& -jrtsen(\theta)sen(\varphi)|0,0,0,0,0,0,1,1\rangle_{1,1',2,2',3,3',4,4'}
\end{aligned}
\tag{5-21}
$$

No caso de fótons indistinguíveis, pode-se agrupar os modos $|\rangle_1$ e $|\rangle_{1'}$, $|\rangle_2$ e $|\rangle_{2'}$,etc. Isto resulta em

$$
\begin{aligned}
|\theta,\varphi\rangle_{a,b} \rightarrow \\
& jrtcos(\theta)cos(\varphi)|D_1\rangle - jrtsen(\theta)sen(\varphi)|D_2\rangle \\
& +jrtcos(\theta)cos(\varphi)|D_3\rangle - jrtsen(\theta)sen(\varphi)|D_4\rangle \\
& -rtsen(\theta+\varphi)|C_{1,2}\rangle + (t^2-r^2)cos^2(\theta)cos^2(\varphi)|C_{13}\rangle \\
& +j(t^2cos(\theta)sen(\varphi) - r^2sen(\theta)cos(\varphi))|C_{14}\rangle
\end{aligned}
$$

$$+j(t^2 sen(\theta)cos(\varphi) - r^2 cos(\theta)sen(\varphi))|C_{23}\rangle$$
$$+(r^2 - t^2)sen^2(\theta)sen^2(\varphi)|C_{24}\rangle - rtsen(\theta+\varphi)|C_{34}\rangle\,, \quad (5\text{-}22)$$

com $|C_{xy}\rangle$ representando coincidência entre os detectores x e y (vide figura 5.2) e $|D_z\rangle$ representando contagem no detector z. Estes estados estão associados à localização dos fótons nos modos espaciais correspondentes aos quatro detectores e podem ser definidos como

$$\begin{aligned}
|D_1\rangle &= |2,0,0,0\rangle \\
|D_2\rangle &= |0,2,0,0\rangle \\
|D_3\rangle &= |0,0,2,0\rangle \\
|D_4\rangle &= |0,0,0,2\rangle \\
|C_{12}\rangle &= |1,1,0,0\rangle \\
|C_{13}\rangle &= |1,0,1,0\rangle \\
|C_{14}\rangle &= |1,0,0,1\rangle \\
|C_{23}\rangle &= |0,1,1,0\rangle \\
|C_{24}\rangle &= |0,1,0,1\rangle \\
|C_{34}\rangle &= |0,0,1,1\rangle\,. \qquad (5\text{-}23)
\end{aligned}$$

Ressalta-se que, em alguns casos, indistinguibilidade não faz sentido, como para $|0,\pi/2\rangle_{a,b}$, ou seja, um fóton polarizado horizontalmente e outro verticalmente, intrinsecamente distinguíveis.

5.2.3 Estados de Bell

Os resultados da análise da resposta do BSA para cada estado de Bell (eqs. 5-18) são obtidos através das eqs. 5-22, fazendo-se $|H,H\rangle_{a,b}$=$|\theta=0,\varphi=0\rangle$, $|H,V\rangle_{a,b}$=$|\theta=0,\varphi=\pi/2\rangle$, $|V,H\rangle_{a,b}$=$|\theta=\pi/2,\varphi=0\rangle$ e $|V,V\rangle_{a,b}$=$|\theta=\pi/2,\varphi=\pi/2\rangle$, e resultam em

$$\begin{aligned}
|\phi^+\rangle_{a,b} &\rightarrow \frac{1}{2}(|D_1\rangle - |D_2\rangle + |D_3\rangle - |D_4\rangle) \\
|\phi^-\rangle_{a,b} &\rightarrow \frac{1}{2}(|D_1\rangle + |D_2\rangle + |D_3\rangle + |D_4\rangle) \\
|\psi^+\rangle_{a,b} &\rightarrow \frac{1}{\sqrt{2}}(|C_{12}\rangle + |C_{34}\rangle) \\
|\psi^-\rangle_{a,b} &\rightarrow \frac{1}{\sqrt{2}}(|C_{14}\rangle - |C_{23}\rangle)\,, \qquad (5\text{-}24)
\end{aligned}$$

As fases representadas pelos sinais positivos e negativos não são men-

suráveis[5]. Estes resultados indicam que os estados $|\psi^+\rangle$ e $|\psi^-\rangle$ são identificáveis de forma determinística através de eventos coincidentes entre pares de detectores. Já os estados $|\phi^+\rangle$ e $|\phi^-\rangle$ não podem ser distinguidos de eventos simples de detecção. De forma análoga, pode-se discriminar os estados $|\phi^+\rangle$ e $|\phi^-\rangle$ acrescentando uma lâmina de meia-onda antes de uma porta de entrada do analisador, à custa da impossibilidade de detecção dos outros dois estados. Pode-se, ainda, com outra configuração, discriminar três estados de Bell, cada um com probabilidade individual não unitária e probabilidade global de sucesso menor ou igual a meio [132] [133]. Alternativas para a implementação de analisadores de estados de Bell completos envolvem elementos ópticos não-lineares ou hiper-emaranhamento [124].

5.2.4 De volta ao protocolo

Voltando ao caso do protocolo MDI-QKD, cabe lembrar que Alice e Bob enviam um estado de polarização aleatoriamente escolhido e que Charlie realiza a medição destes pulsos com um BSA. Na etapa de reconciliação de bases apenas os casos em que há concordância de bases entre Alice e Bob serão considerados. Para dois fótons não-emaranhados e independentes, porém indistinguíveis, incidentes no medidor de estados de Bell, obtém-se, através das eqs. 5-22, os resultados para a base retilínea ($\oplus$)

$$\begin{aligned}
|H,H\rangle_{Alice,Bob} &\rightarrow \frac{1}{\sqrt{2}}(|D_1\rangle + |D_3\rangle) \\
|V,V\rangle_{Alice,Bob} &\rightarrow \frac{1}{\sqrt{2}}(|D_2\rangle + |D_4\rangle) \\
|H,V\rangle_{Alice,Bob} &\rightarrow \frac{1}{2}(-|C_{12}\rangle - |C_{34}\rangle + j|C_{14}\rangle - j|C_{23}\rangle) \\
&\equiv \frac{1}{\sqrt{2}}(|\psi^+\rangle - j|\psi^-\rangle) \\
|V,H\rangle_{Alice,Bob} &\rightarrow \frac{1}{2}(-|C_{12}\rangle - |C_{34}\rangle - j|C_{14}\rangle + j|C_{23}\rangle) \\
&\equiv \frac{1}{\sqrt{2}}(|\psi^+\rangle + j|\psi^-\rangle)
\end{aligned} \tag{5-25}$$

De forma semelhante, a preparação de ambos os estados na base diagonal ($\otimes$) resultará em

$$|+45,+45\rangle_{Alice,Bob} \rightarrow \frac{1}{2\sqrt{2}}(j|D_1\rangle - j|D_2\rangle + j|D_3\rangle - j|D_4\rangle)$$

[5]Isso ocorre pois as medidas sempre são realizadas na base canônica dos modos espaciais.

$$
\begin{aligned}
& & & +\frac{1}{2}(-|C_{12}\rangle - |C_{34}\rangle) \\
& & \equiv & \frac{1}{\sqrt{2}}(j|\phi^+\rangle - |\psi^+\rangle) \\
|-45,-45\rangle_{Alice,Bob} & \rightarrow & \frac{1}{2\sqrt{2}}(j|D_1\rangle - j|D_2\rangle + j|D_3\rangle - j|D_4\rangle) \\
& & & +\frac{1}{2}(|C_{12}\rangle + |C_{34}\rangle) \\
& & \equiv & \frac{1}{\sqrt{2}}(j|\phi^+\rangle + |\psi^+\rangle) \\
|+45,-45\rangle_{Alice,Bob} & \rightarrow & \frac{1}{2\sqrt{2}}(|D_1\rangle + |D_2\rangle + |D_3\rangle + |D_4\rangle) \\
& & & -\frac{1}{2}(|C_{14}\rangle - |C_{23}\rangle) \\
& & \equiv & \frac{1}{\sqrt{2}}(|\phi^-\rangle - |\psi^-\rangle) \\
|-45,+45\rangle_{Alice,Bob} & \rightarrow & \frac{1}{2\sqrt{2}}(|D_1\rangle + |D_2\rangle + |D_3\rangle + |D_4\rangle) \\
& & & +\frac{1}{2}(|C_{14}\rangle - |C_{23}\rangle) \\
& & \equiv & \frac{1}{\sqrt{2}}(|\phi^-\rangle + |\psi^-\rangle)\,.
\end{aligned}
$$

Após Charlie realizar as medições e Alice e Bob concordarem em relação às bases utilizadas na preparação, os casos em que ambos utilizaram a base $\oplus$ são efetivamente utilizados para o compartilhamento da chave. Se Alice e Bob prepararem estados idênticos nesta base, não haverá contagens coincidentes no aparato de Charlie. Logo estes eventos não contribuem para a formação da chave.

Porém, se os estados preparados forem ortogonais nesta base, o resultado do analisador de estados de Bell será equivalente a $|\psi^+\rangle$ ou $|\psi^-\rangle$, aleatoriamente. Assim, Alice e Bob sabem o SOP de sua contra-parte, bastando que um deles inverta seu bit para compartilharem o mesmo valor. A ocorrência de erros corresponde a um evento coincidente equivalente a $|\psi^+\rangle$ ou $|\psi^-\rangle$ quando os estados quânticos preparados são idênticos, na base $\oplus$. Caso os estados preparados sejam ortogonais, um resultado inconclusivo no analisador de estados de Bell resultará em redução da taxa de bits, não contribuindo para a taxa de erro.

Os casos em que a base $\otimes$ é utilizada por ambas as partes gera um resultado $|\psi^+\rangle$ quando os estados são iguais, ou $|\psi^-\rangle$ quando os estados são diferentes. Na verdade, nota-se nas equações 5-25 a possibilidade de ocorrência dos estados $|\phi^+\rangle$ ou $|\phi^-\rangle$, porém estes não são observados na forma de coincidências e são descartados. Os resultados na base $\otimes$ são utilizado para

estimar o ganho e a QBER do canal através de *decoy-states* e para verificar a quantidade de amplificação de privacidade necessária nas etapas subsequëntes através da análise da estatística dos eventos causados por um fóton apenas de Alice e um de Bob.

5.2.5 Estados coerentes

Devido à natureza poissoniana das fontes ópticas, além da probabilidade de emissão de um fóton simultaneamente por Alice e por Bob com probabilidade P_1=P(1)P(1), deve-se considerar a emissão de dois fótons por Alice e vácuo por Bob e o inverso, vácuo por Alice e dois fótons por Bob, o que ocorre com probabilidade P_2=P(2)P(0)=P(0)P(2), no caso de potências iguais. É possível mostrar, através da distribuição de Poisson – ver eq. 2-1, que

$$\begin{aligned} P_1 &= P(1)P(1) = (\mu e^{-\mu})(\mu e^{-\mu}) = \mu^2 e^{-2\mu} \\ P_2 &= P(0)P(2) = P(2)P(0) = (e^{-\mu})\left(\frac{e^{\mu 2}{}^{-\mu}}{2}\right) \\ P_2 &= 2P_1 \end{aligned} \tag{5-26}$$

.

Esta consideração acrescenta um fundo de ruído às medições de coincidências, pois multiplos fótons emitidos pela mesma fonte serão distribuídos binomialmente entre as saídas do BS do BSA. A probabilidade condicional de ocorrência de contagem coincidente entre um determinado par de detectores dado que um evento coincidente ocorreu é mostrada na tabela 5.1.

Alice	Bob	$\|C_{12}\rangle$	$\|C_{13}\rangle$	$\|C_{14}\rangle$	$\|C_{23}\rangle$	$\|C_{24}\rangle$	$\|C_{34}\rangle$
$\|$H$\rangle$	$\|$H$\rangle$	0	1	0	0	0	0
$\|$V$\rangle$	$\|$V$\rangle$	0	0	0	0	1	0
$\|$H$\rangle$	$\|$V$\rangle$	1/6	1/6	1/6	1/6	1/6	1/6
$\|$V$\rangle$	$\|$H$\rangle$	1/6	1/6	1/6	1/6	1/6	1/6
$\|+45\rangle$	$\|+45\rangle$	3/10	1/10	1/10	1/10	1/10	3/10
$\|$-45$\rangle$	$\|$-45$\rangle$	3/10	1/10	1/10	1/10	1/10	3/10
$\|+45\rangle$	$\|$-45$\rangle$	1/10	1/10	3/10	3/10	1/10	1/10
$\|$-45$\rangle$	$\|+45\rangle$	1/10	1/10	3/10	3/10	1/10	1/10

Tabela 5.1: Probabilidade condicional de coincidências dada a ocorrêcnia de um evento coincidente no analisador de estados de Bell para ocaso de duas fontes poissonianas indistinguíveis.

Entretanto, ressalta-se aqui que estes resultados não invalidam as análises apresentadas até o momento, o que é previsto em [17]. Nota-se que no caso

$|\mathrm{H}\rangle_a|\mathrm{H}\rangle_b$, apenas coincidências entre os detectores 1 e 3 ocorrem. Estas devem-se aos casos em que dois fótons incidem na mesma porta do BSA, o que ocorre com probabilidade três vezes menor que o caso de um fóton em cada porta sofrendo agrupamento (ver apêndice). Situação semelhante acontece no caso $|\mathrm{V}\rangle_a|\mathrm{V}\rangle_b$, porém em relação ao par 2 e 4. Estes eventos coincidentes são descartados em todas as ocasiões e não alteram o funcionamento do protocolo.

Quando os estados são preparados como $|+45\rangle_a|+45\rangle_b$ ou $|\text{-}45\rangle_a|\text{-}45\rangle_b$, a probabilidade de agrupamento também é três vezes maior que a probabilidade de não agrupamento (ver apêndice). Porém a proporção de eventos coincidentes é 5/3 maior que a probabilidade de contagens únicas. Os eventos coincidentes ocorrem , em sua maioria, no mesmo braço do analisador como mostrado na tabela 5.1. Quando estados diagonais diferentes são medidos, a probabilidade de agrupamento no BS é 0,5. Porém, devido à pós-seleção realizada pelos PBS, a probabilidade de coincidências também é 5/3. Curiosamente, o efeito observado equivale a um anti-agrupamento, com detecções entre SPADs localizados em braços diferentes do analisador (como indicado na tabela 5.1). Os fótons idênticos incidentes na mesma porta do aparato causam um fundo de ruído, com distribuição de probabilidades de coincidência uniforme entre os detectores, o que reduz a fração de coincidências correspondentes aos estados $|\psi_+\rangle$ e $|\psi_-\rangle$. Como mencionado no parágrafo anterior, os resultados $|C_{13}\rangle$ e $|C_{24}\rangle$ são descartados. Com a utilização de *decoy-states*, é possível extrair informações acerca da contribuição de 1 fóton emitido por Alice e 1 fóton emitido por Bob, informação esta utilizada para estimar o ganho do canal, a QBER e a taxa de bits.

Uma peculiaridade do protocolo MDI-QKD se refere ao fato de que, na base retilínea, se Alice e Bob enviaram estados ortogonais, caso Charlie não meça $|\psi^+\rangle$ ou $|\psi^-\rangle$ não haverá geração de erro, pois as demais possibilidades ($|\phi^+\rangle$ e $|\phi^-\rangle$) não resultam em resultado favorável para Charlie, ou seja, estes eventos são automaticamente descartados. Isto significa que haverá apenas redução da taxa de geração da chave segura, mas não haverá aumento da QBER. Outro ponto favorável, se refere à robustez da base retilínea aos pulsos contendo múltiplos fótons, pois dão origem a eventos do tipo $|D_{13}\rangle$ ou $|D_{24}\rangle$, descartados por Charlie. Assim, novamente a natureza poissoniana das fontes não interfere no bom funcionamento do protocolo.

No caso distinguível, a proporções de coincidências na base $\otimes$ torna-se equiprovável, com 1/3 de probabilidade para todas as combinações de estados. A razão de contraste do número de coincidências, entretanto, varia, sendo 0,5 para o par de detectores 1 e 3 no caso $|\mathrm{H}\rangle|\mathrm{H}\rangle$ (ver apêndice).

Como será visto adiante, é de especial interesse observar a razão entre

as contagens coincidentes considerando apenas os pares $|C_{12}\rangle$, $|C_{13}\rangle$ e $|C_{14}\rangle$, devido à montagem experimental realizada [6]. Dos resultados anteriores, extrai-se a tabela 5.2.

Alice	Bob	$\|C_{12}\rangle$	$\|C_{13}\rangle$	$\|C_{14}\rangle$
$\|H\rangle$	$\|H\rangle$	0	1	0
$\|V\rangle$	$\|V\rangle$	0	0	0
$\|H\rangle$	$\|V\rangle$	1/3	1/3	1/3
$\|V\rangle$	$\|H\rangle$	1/3	1/3	1/3
$\|+45\rangle$	$\|+45\rangle$	3/5	1/5	1/5
$\|-45\rangle$	$\|-45\rangle$	3/5	1/5	1/5
$\|+45\rangle$	$\|-45\rangle$	1/5	1/5	3/5
$\|-45\rangle$	$\|+45\rangle$	1/5	1/5	3/5

Tabela 5.2: Probabilidade condicional de coincidências dada a ocorrêcnia de um evento no detector 1 do BSA para ocaso de duas fontes poissonianas indistinguíveis.

Ainda observa-se maior ocorrência de resultados $|\psi_+\rangle$ e $|\psi_-\rangle$ quando os estados, preparados na base $\otimes$, são iguais ou diferentes, respectivamente, enquanto que apenas $|C_{13}\rangle$ ocorre quando ambos os SOP são horizontais. Isto significa que esta sub-tabela é representativa da resposta do BSA e do protocolo MDI-QKD. Estes valores serão experimentalmente verificados na próxima seção.

5.3 Montagem experimental

Para observação da interferência entre fótons de fontes independentes, foram utilizados dois lasers sintonizáveis de cavidade externa operando em modo CW, com largura de linha média de 800 kHz e 5 MHz, passando por atenuadores ópticos variáveis (AOV), como mostrado na figura 5.4. Após propagação por duas fibras independentes, cada uma com 8,5 km de comprimento, os sinais são combinados em um BS 2×2, também em fibra. Em cada saída do BS é colocado um SPAD operando em modo gatilhado. O detector $SPAD_1$ utiliza base de tempo interna e gatilha com freqüência de 100 kHz. Para cada evento de detecção, é gerado um pulso elétrico que, após passar por um gerador de atraso (Δt) gatilha o detector $SPAD_2$. Um trecho de alguns metros de fibra óptica (delay) garante que o sinal de gatilho chegue ao $SPAD_2$ antes do tempo de propagação dos fótons após o BS.

O comprimento de onda dos lasers foi ajustado para o canal DWDM número 39, centrado em 1546,12 nm. As freqüências ópticas foram ajustadas

[6] A verificação do BSA construído nesta tese e do protocolo MDI-QKD implementado é feita através do monitoramento das coincidências entre o detector 1 e os demais.

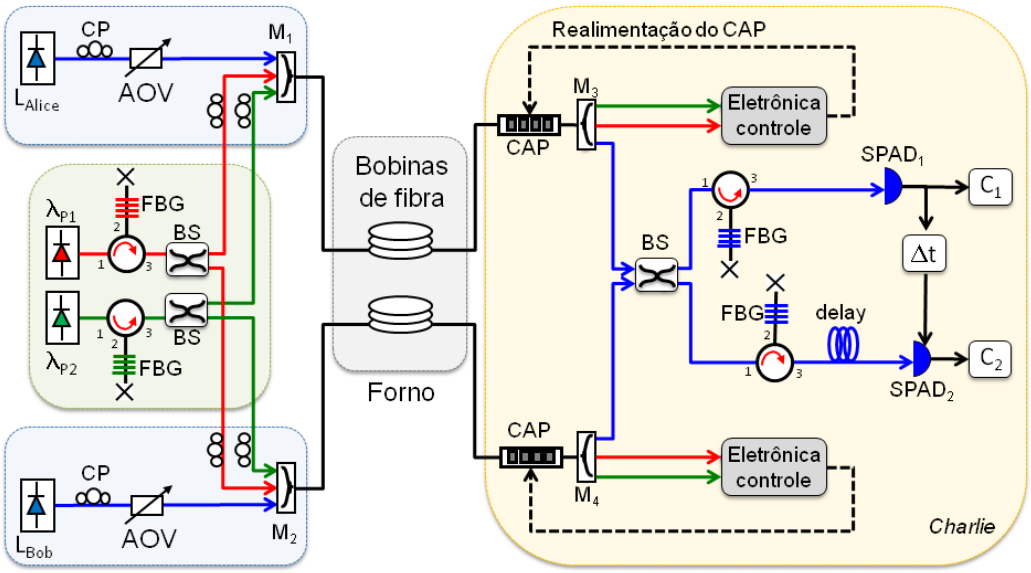

Figura 5.4: Montagem experimental para observação de interferência estável entre fontes independentes através de fibra óptica estabilizada em polarização.

para se obter a máxima superposição entre as linhas laser, monitoradas através de uma amostra de cada fonte extraída com um divisor óptico e recombinadas em um analisador de espectro elétrico. Para evitar os efeitos de uma deriva lenta permanente de uma das fontes laser, o comprimento de onda de um deles foi sistematicamente corrigido através de um ajuste fino (passo mínimo de 400 kHz) de acordo com o tom de batimento observado, mantendo este sinal abaixo de 10 MHz. Ressalta-se aqui que esta correção não impõe limitação em um sistema real de comunicação, já que as estações poderiam travar a freqüência óptica em linhas de absorção de HCN, que apresenta comprimento de onda próximo ao utilizado [7].

Para a estabilização das bobinas de fibra óptica em relação à polarização utilizam-se dois lasers CW do tipo DFB (λ_{P1} e λ_{P2}) operando em canais DWDM vizinhos ao canal quântico (canais 40 e 38, centrados em 1545,35 nm e 1546,92 nm, respectivamente). Para simplificar a montagem, estes lasers foram compartilhados por ambas as estações, sem comprometer, todavia, a verossimilhança do sistema em relação ao um enlace real. Os laser de controle de polarização foram divididos para os dois braços do sistema (Alice/Charlie e Bob/Charlie). A emissão espontânea amplificada (ASE, do inglês *amplified spontaneous emission*) dos lasers foi filtrada com redes de Bragg (FBG) em reflexão, centradas nos comprimentos de onda destes e conectadas a circuladores ópticos. Os canais de controle foram agregados ao canal quântico em cada braço do sistema através de multiplexadores WDM (M_1 e M_2).

[7] De fato, é possível observar interferência mesmo que haja uma pequena diferença entre os comprimentos de onda envolvidos.

Após transmissão pelas bobinas de fibra óptica, os sinais de controle são demultiplexados e detectados, gerando um sinal de realimentação que atua em um controlador automático de polarização colocado no final do enlace, dentro da estação de Charlie. Os sinais de controle dos dois braços do sistema são independentes e fazem com que os controladores estabilizem os respectivos canais quânticos, desfazendo as transformações do estado de polarização devido à variação aleatória de birrefringência sofridas pelas fibras ao longo do tempo. Para acelerar este processo degradativo e atestar a eficácia do controle, as bobinas de fibra foram submetidas a um forno durante as medições. Uma medida polarimétrica dos lasers com comprimento de onda ajustado para o canal quântico, controlados após propagação pelas fibras, pode ser vista na figura 5.5. Um conjunto de filtros foi utilizado em cada saída do BS para

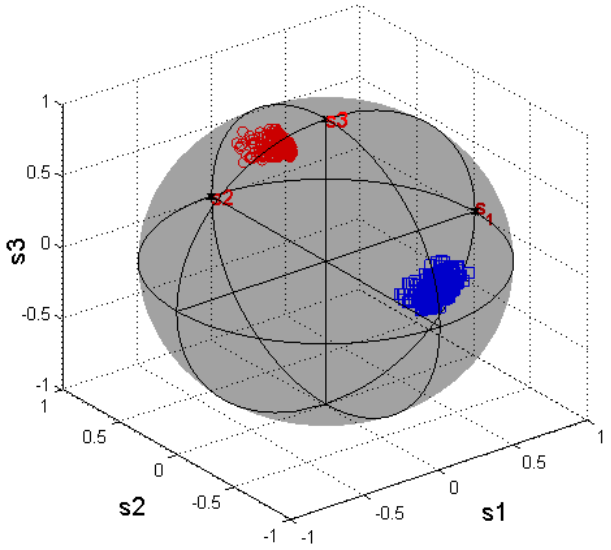

Figura 5.5: Observação durante 0,2 s do estado de polarização dos lasers em um polarímetro após propagação através do canal quântico estabilizado.

minimizar possíveis efeitos não-lineares gerados na fibra pelo sinais de controle, estes em torno de -1 dBm, como espalhamento Raman espontâneo. Uma rede de Bragg centrada no canal quântico foi utilizada em modo reflexivo em conjunto com um circulador óptico em cada porta de saída do BS.

O segundo grupo de medidas foi realizado com auxílio de um analisador de estados de Bell. Este aparato foi montado conectando-se um PBS em cada saída do BS, precedidos por um controlador de polarização (tipo "orelhas de Mickey") e com um detector de fótons únicos em uma das quatro portas de saída, totalizando quatro SPADs. O detector rotulado como "1" é operado com base de tempo interna e utilizado para engatilhar os demais, numerados de 2

a 4, conforme a figura 5.6. A razão de coincidências entre os detectores, $|C_{12}\rangle$,

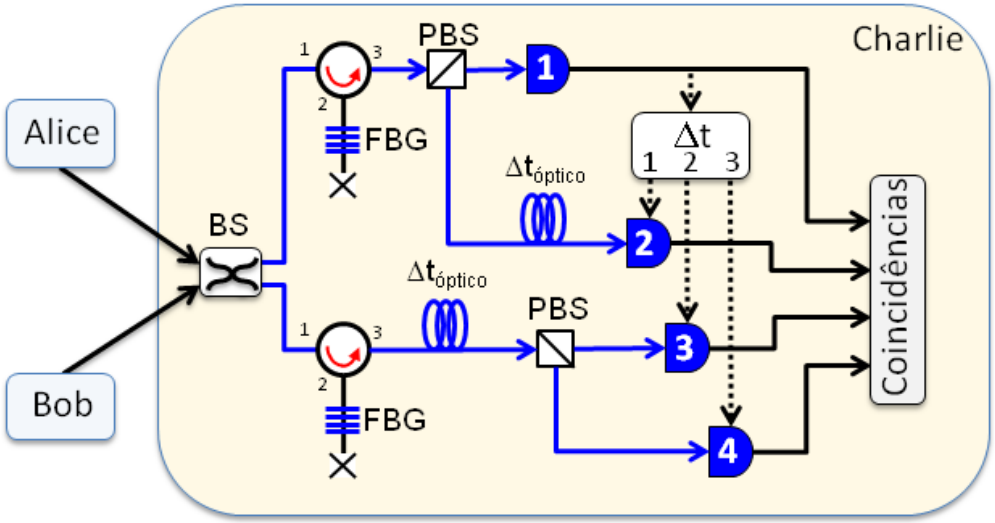

Figura 5.6: Medidor de estados de Bell implmentado na estação intermediária.

$|C_{13}\rangle$ e $|C_{14}\rangle$, são lidas, bem como a taxa de contagens dos detector "1", $|D_1\rangle$.

Um modulador de amplitude foi utilizado de forma auxiliar em um dos lasers para mapear o atraso temporal relativo entre os detectores. Um pulso óptico foi gerado e o atraso do sinal de modulação, também utilizado para engatilhar os detectores foi variado para obtenção da condição de casamento temporal. Após esta medida, o modulador foi retirado. Um polarímetro foi utilizado de forma auxiliar para ajuste do sistema de controle de polarização e para ajuste dos estados de polarização enviados por Alice e Bob e monitoramento do canal quântico.

Um sistema automatizado de aquisição de dados foi confeccionado para leitura dos contadores de pulsos acoplados aos SPADs e atuação no gerador de atraso.

5.4 Resultados

Os lasers foram ajustados como indistinguíveis em polarização e freqüência e variou-se o atraso relativo entre as janelas de detecção dos dois SPADs mostrados na figura 5.4. O vale de coincidências foi observado e convertido em uma curva de visibilidade em função do atraso, como mostrado na figura 5.7a. A visibilidade foi calculada utilizando a equação 5-15, tomando como referência (taxa de coincidências com fótons distinguíveis) o valor com atraso de 160 ns em relação ao ponto de mínimo. A visibilidade máxima é calculada como 48,7%, ocorrendo no ponto convencionado como atraso zero. A largura do pico de visibilidade à meia-altura é de 94,5 ns, que corresponde a

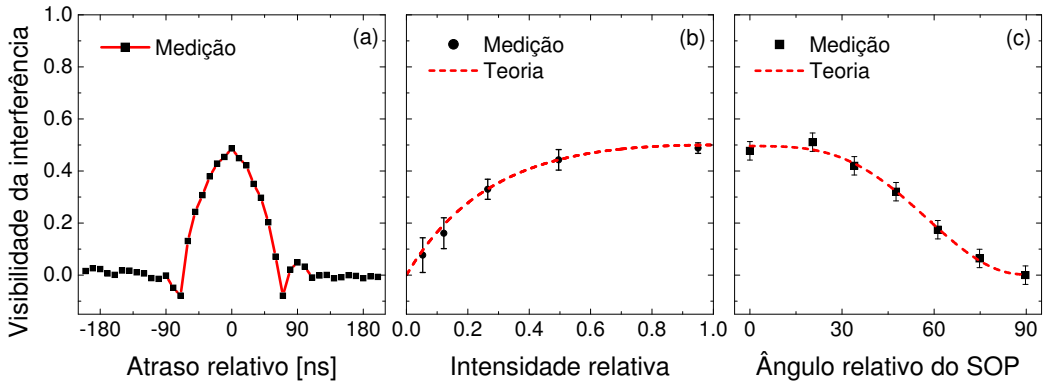

Figura 5.7: Variação da visibilidade de interferência em função (a) do atraso relativo das janelas de detecção, (b) do ângulo relativo dos estados de polarização e (c) das intensidade relativa dos lasers independentes. A linha na figura (a) é apenas uma referência visual.

uma largura de linha de 3.4 MHz (considerando uma distribuição gaussiana). Alargando-se a linha espectral de uma das fontes ópticas através de modulação em freqüência com uma onda triangular, observou-se o estreitamento do pico de visibilidade, porém com a posição temporal de máximo mantida. esta posição temporal se mantém mesmo com o deslocamento da freqüência relativa entre os dois lasers em algumas dezenas de MHz [59][134].

A intensidade relativa das fontes laser incidindo no BS foi variada. A curva obtida é mostrada na figura 5.7b, com o ajuste teórico da equação 5-16. Observa-se a redução da visibilidade com o desbalanceamento da intensidades.

A variação da razão de coincidências foi observada também ao se variar o ângulo relativo entre os estados de polarização dos lasers. A curva de visibilidade medida é mostrada na figura 5.7c, com ajuste da equação 5-17. O valor mínimo é observado quando os estados de polarização dos lasers estão ortogonais, enquanto que as polarizações paralelas entre si geram o maior contraste.

A taxa de contagens coincidentes entre os detectores nas portas de saída do BS foi medida com os lasers independentes transmitidos sobre as duas bobinas de fibra com os controles de polarização ligados. Os lasers foram feitos indistinguíveis em polarização e freqüência e a taxa de coincidências foi medida com as janelas de detecção casadas e com atraso de 1 μs – tempo muito maior que a coerência dos fótons –, como mostrado na figura 5.8.

A visibilidade média, obtida ao longo de 42 minutos de medição com o forno ativo, foi calculada considerando os casos distinguível e indistinguível, resultando em 47,8%. Ao se desligar o controle de polarização, a variação aleatória da birrefringência das fibras com a temperatura fez com que a taxa

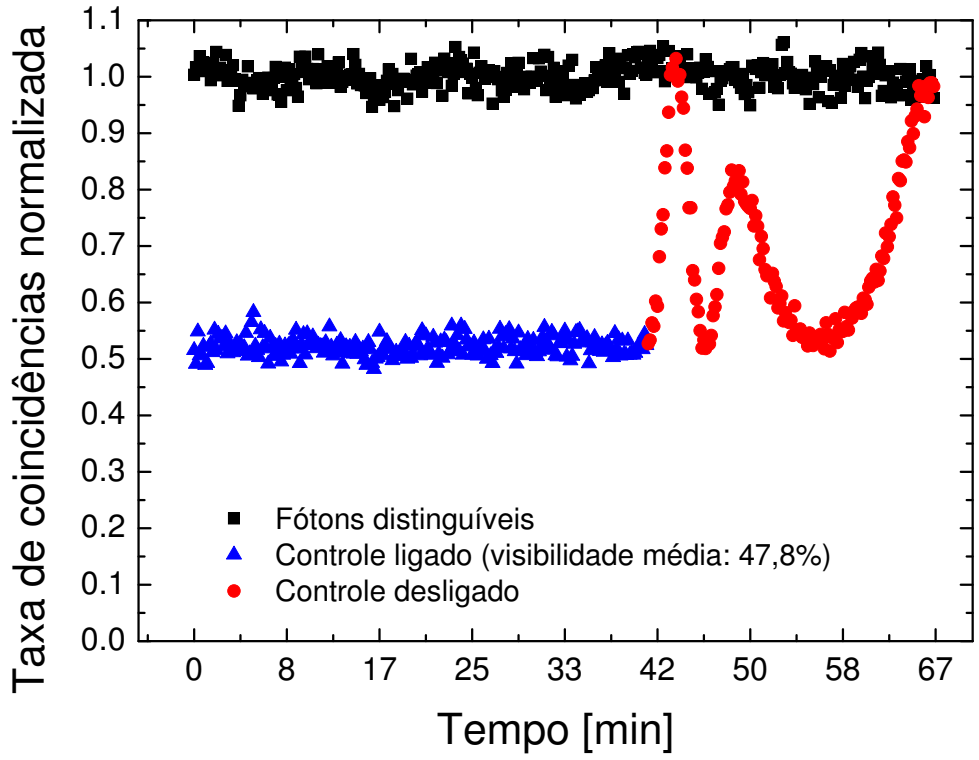

Figura 5.8: Taxa normalizada de contagens medida com o controle ligado (triângulos) e deslligado (círculos). Os fótons foram feitos distinguíveis em ambos os casos descasando-se o atraso relativo das janelas de detecção (quadrados pretos).

de coincidências oscilasse aleatoriamente entre os valores mínimo e máximo, (0,5 e 1, respectivamente, considerando valores normalizados) devido à variação do ângulo relativo entre os SOP dos lasers.

O desvio do valor de visibilidade em relação ao valor máximo pode ter origem no desbalanceamento do BS, tendo sido observado também no caso sem fibras e sem controle de polarização. Estes resultados mostram a possibilidade de implementação prática de protocolos de comunicação quântica dependentes da polarização sobre fibra óptica, operando de forma estável.

Inserindo o analisador de estados de Bell após o BS, foram registradas as razões de coincidências entre o detector 1 e os demais ($|C_{12}\rangle$, $|C_{13}\rangle$ e $|C_{14}\rangle$) para diferentes combinações dos estados de polarização enviados por Alice e Bob, considerando os casos em que as bases de preparação coincidem. A tabela 5.3 mostra os resultados das proporções entre as coincidências medidas, nos casos em que o atraso relativo das janelas de detecção estão casados (colunas "Ind") e descasados (colunas "Dist").

A primeira coluna indica o estado de polarização enviado por Alice, enquanto que a primeira linha indica o estado preparado por Bob. Observa-se que no caso $|\mathrm{H}\rangle|\mathrm{H}\rangle$, existe maior probabilidade de ocorrerem eventos

	$\|H\rangle$		$\|V\rangle$		$\|+45\rangle$		$\|-45\rangle$		
$\|H\rangle$	0.023	0.014	0.345	0.333	–	–	–	–	C_{12}
	0.941	0.964	0.341	0.350	–	–	–	–	C_{13}
	0.036	0.022	0.314	0.317	–	–	–	–	C_{14}
$\|V\rangle$	0.357	0.340	0.476	0.509	–	–	–	–	C_{12}
	0.319	0.340	0.000	0.000	–	–	–	–	C_{13}
	0.324	0.321	0.524	0.491	–	–	–	–	C_{14}
$\|+45\rangle$	–	–	–	–	0.585	0.356	0.209	0.343	C_{12}
	–	–	–	–	0.207	0.300	0.207	0.315	C_{13}
	–	–	–	–	0.207	0.333	0.584	0.338	C_{14}
$\|-45\rangle$	–	–	–	–	0.210	0.333	0.595	0.318	C_{12}
	–	–	–	–	0.204	0.333	0.195	0.337	C_{13}
	–	–	–	–	0.586	0.333	0.210	0.356	C_{14}
	Ind	**Dist**	**Ind**	**Dist**	**Ind**	**Dist**	**Ind**	**Dist**	

Tabela 5.3: Resultados dos analisador de estados de Bell para as diferentes combinações dos estados de polarização dos lasers atenuados independentes.

coincidentes entre os detectores 1 e 3. Este valor tende à unidade, a menos de desalinhamento dos componentes, e independe da distinguibilidade dos fótons. Observando, entretanto, a razão de coincidências absoluta, ou seja, o número de coincidências $|C_{13}\rangle$ em relação ao número de contagens $|D_1\rangle$ para ambos os casos, distinguível e indistinguível, tem-se 48,4% de visibilidade.

Quando Alice e Bob enviam estados de polarização diferentes, mas na mesma base $\oplus$, tem-se coincidências equiprováveis em ambos os casos. Para $|V\rangle|V\rangle$, observa-se uma redução severa do número de eventos de gatilho, $|D_1\rangle$, devido ao fato de o detector 1 estar conectado à porta V do PBS. Das coincidências observadas, causadas por desalinhamento ou contagens de escuro, metade ocorreu em cada detector.

Quando os SOPs são combinados na base $\otimes$, tem-se 48,5%, 47,7%, 47,4% e 45,4% de visibilidades nos casos $|+45\rangle|+45\rangle$, $|+45\rangle|-45\rangle$, $|-45\rangle|-45\rangle$ e $|-45\rangle|+45\rangle$, respectivamente, considerando o casamento e descasamento dos atrasos das janelas. A distribuição de coincidências observada tende a 60%, 20% e 20% para $|C_{12}\rangle$, $|C_{13}\rangle$ e $|C_{14}\rangle$, respectivamente, nos casos $|+45\rangle|+45\rangle$ e $|-45\rangle|-45\rangle$ e se aproxima de 20%, 20% e 40% nos casos $|+45\rangle|-45\rangle$ e $|-45\rangle|+45\rangle$. Ao fazeren-se os fótons indistinguíveis, observa-se uma distribuição equiprovável de contagens coincidentes em todos os casos da base diagonal.

Os valores apresentados na tabela anterior são representados de forma gráfica na figura 5.9, separados de acordo com a base escolhida, para os casos distinguível e indistinguível.

A medida foi repetida ajustando-se 0,1 fótons por janela de detecção antes das bobinas de fibra. A distribuição de coincidências entre os pares de

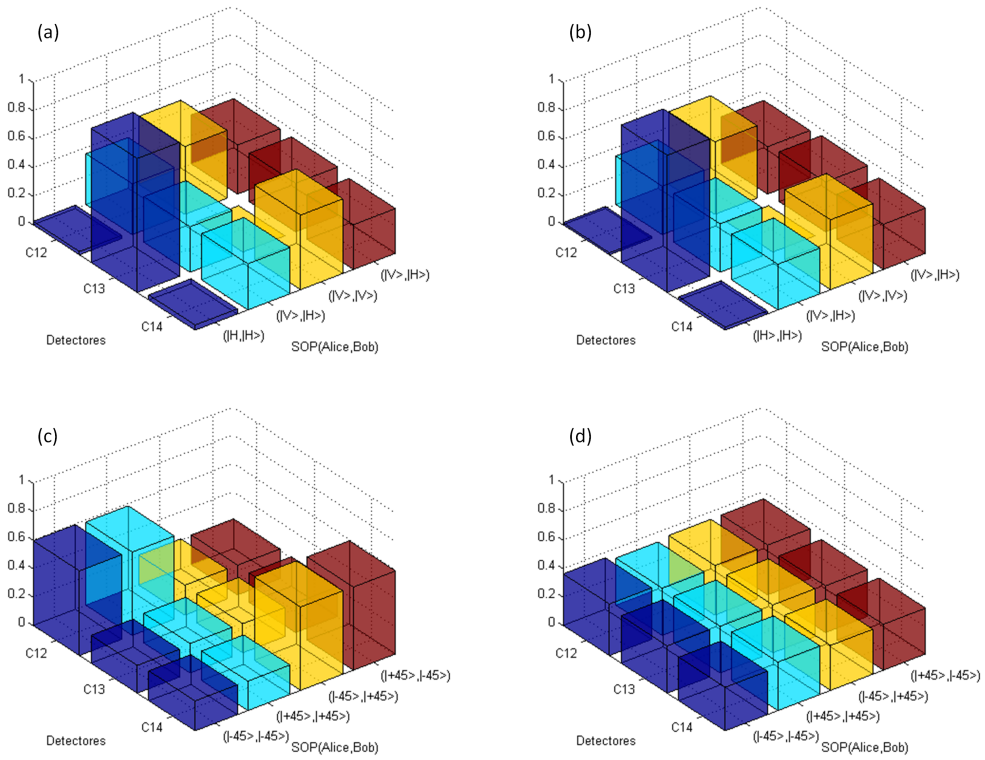

Figura 5.9: Proporção de eventos coincidentes para diferentes combinações dos estados de polarização, considerando apenas $|C_{12}\rangle$, $|C_{13}\rangle$ e $|C_{14}\rangle$.

detectores $|C_{12}\rangle$, $|C_{13}\rangle$ e $|C_{14}\rangle$ para o caso indistinguível foi, respectivamente, 0,08, 0,91 e 0,01 para os estados $|\mathrm{H}\rangle|\mathrm{H}\rangle$, 0,20, 0,23 e 0,57 para os estados $|\text{-}45\rangle|\text{-}45\rangle$ e 0,59, 0,22 e 0,19 para os estados $|\text{-}45\rangle|{+}45\rangle$.

Os resultados apresentados atestam a viabilidade de utilização de controle ativo de polarização para o estabelecimento de sistemas de comunicação quântica dependentes da polarização, como o protocolo de repetidor quântico baseado em óptica linear e o protocolo MDI-QKD. Além disso, mostra-se a viabilidade da construção de um BSA para MDI-QKD baseado em óptica linear e totalmente implementado em fibra óptica.

6
Conclusões

A pesquisa e desenvolvimento dos sistemas de distribuição quântica de chaves nas últimas décadas ajudaram a impulsionar outras tecnologias, em especial os detectores de fótons únicos com operação na janela espectral de telecomunicações (em torno de 1550 nm). Além disso, o caminho para outros sistemas de comunicações quânticas foi pavimentado, incluindo a teleportação quântica, com desenvolvimento de protocolos de repetidor quântico que possibilitam a extensão da distância de um enlace. Esta tese apresentou estudo acerca de elementos essenciais em sistemas de comunicação quântica, baseando-se em considerações práticas e atendo-se à tecnologia atualmente disponível. Em especial, o detector de fótons únicos baseado em fotodiodo avalanche desempenhou papel principal nos estudos desenvolvidos, tendo sido abordados aspectos de caracterização do dispositivos e aplicação, incluindo um estudo sobre sua vulnerabilidade em sistemas tradicionais de distribuição de chaves e aplicação em sistemas robustos a ataques ao detector.

No capítulo 2 foi apresentado método para caracterização de SPADs em tempo real através de instrumentação simples. Analisando o histograma de intervalos de tempo entre eventos consecutivos de detecção, é possível extrair simultaneamente a eficiência de detecção, a probabilidade de contagem de escuro e a probabilidade de pós-pulso através do ajuste de um modelo analítico aos dados medidos. Os resultados de caracterização de diferentes dispositivos comerciais atestam a eficácia do método.

Como extensão do trabalho apresentado, pode-se investigar a aplicação do método desenvolvido para a caraterização também do tempo morto de detectores operando em modo *free-running* e da janela de detecção de SPADs operando em modo gatilhado. Ambas as medidas podem ser realizadas utilizado-se *hardware* com alta-resolução de amostragem e luz CW, através da análise dos intervalos de tempo entre medições consecutivas. Um contador de intervalos de tempo foi utilizado para a medição do tempo morto de dois SPADs de silício através de uma configuração tipo *auto-start-stop*, semelhante ao método relatado, com boa concordância entre os resultados, quando comparados a uma medida realizada com um osciloscópio rápido. Os resultados

preliminares para a caracterização da janela de detecção de SPADs operando em modo gatilhado são promissores e podem representam uma forma simples de caracterização deste parâmetro sem a utilização de laser pulsado, fonte heráldica ou gerador de atraso.

No capítulo 3 foi mostrada a aplicação do sistema de caracterização no monitoramento dos SPADs de um sistema QKD durante sua operação, com objetivo de verificar uma possível intervenção por parte de um interceptador. O método se mostrou aplicável contra dois esquemas de ataque, o *after-gate* e o *time-shift*, sem a necessidade de modificações no detector. O primeiro caso foi demonstrado através da implementação de um sistema simplificado de QKD com codificação em polarização. O detector foi monitorado durante o ataque e sua resposta foi comparada com o caso sob operação normal. Verificou-se a elevação da probabilidade de pós-pulsos mesmo se aplicado tempo morto extra no detector ou se apenas uma pequena fração dos fótons for interceptada. Contra o segundo ataque, verificou-se experimentalmente a alteração da eficiência de detecção do SPAD sob intervenção, o que precisaria ser compensado pelo interceptador. Mesmo sendo em princípio possível, sob certas circunstâncias, uma assinatura temporal é deixada nos eventos de detecção, que resultam em picos extras no histograma de tempos, quando observado com resolução suficiente. No caso da versão atenuada do por pulsos fortes (*faint after-gate*), observou-se experimentalmente resultado favorável sob certas condições. Também foi discutida a eficácia do monitoramento contra outros protocolos de ataque, em especial os que desabilitam os SPADs por meio de sinal óptico externo. O sistema de monitoramento é potencialmente aplicável ao caso em que o tempo morto de um detector é ativado externamente por meio de um pulso óptico fraco para que não detecte o qubit. A proposta é monitorar os intervalos de tempo de modo similar ao caso *time-shift*. Apesar de não poder afirmar categoricamente sobre a eficácia, foi proposta a alteração aleatória de algum parâmetro do detector como forma de monitorar uma intervenção e assegurar um grau extra de proteção ao sistema para prevenção dos casos em que o interceptador assume total controle dos detectores.

Ainda não está claro se é possível construir um detector cuja resposta não possa ser adulterada. O recente desenvolvimento da linha de pesquisa denominada *quantum-hacking* apontou diversas "portas de entrada" para execução de um ataque sobre um sistema em princípio absolutamente seguro. As recentes propostas de ataque contra elementos de um sistema QKD prático, bem como as propostas de contra-medidas, indicam a maturidade desta tecnologia. O trabalho desenvolvido não esgota as possibilidades e pode ser estendido através da implementação experimental de outros ataques para

avaliação quantitativa da proteção propiciada em um cenário com tecnologia atual.

A simulação apresentada no capítulo 4 mostra a possibilidade de extensão da freqüência de operação de um detector de fótons únicos através da ativação serial de um grupo de SPADs. Este método é proposto como solução alternativa aos complexos esquemas de polarização elétrica e extinção de avalanche existentes e baseia-se em tecnologia atualmente disponível. A atenuação imposta pela chave óptica utilizada para comutar entre os detectores é compensada pelo resfriamento dos SPADs e correção da tensão de excesso de polarização, com possibilidade de ganho de eficiência global.

A implementação prática do detector paralelizado seria interessante e possibilitaria a verificação detalhada de sua performance e limitações. Para isso seria necessário o acesso ao controle de temperatura dos dispositivos e a construção do circuito lógico, este facilmente concebível através de FPGA.

O capítulo 5 apresentou a implementação de um enlace conectando duas estações remotas a uma estação central através de fibra óptica estabilizada em polarização. A interferência estável entre fótons oriundos de fontes laser atenuadas totalmente independentes foi demonstrada, o que constitui passo importante para a implementação do protocolo de repetidor quântico. Além disso, a tecnologia de estabilização do canal quântico é imediatamente aplicável a sistemas de QKD baseados em polarização e mesmo em *time-bins*, baseados em interferômetros.

A recente preocupação com a segurança prática de sistemas de QKD motivou a busca por um protocolo intrinsecamente robusto contra os *loopholes* apresentados. O protocolo MDI-QKD, proposto no final de 2011, propõe um sistema cujos SPADs da estação central podem inclusive ser controlados pelo interceptador, sem prejuízo para a segurança da distribuição da chave criptográfica entre as duas partes remotas. Além da interferência remota de fótons oriundos de fontes laser atenuadas independentes, o protocolo requer uma medida conjunta destes fótons em um analisador de estados de Bell, também construído nesta tese. Os resultados de transmissão e medição dos estados quânticos nas diferentes bases de preparação do protocolo, obtidos sobre os canais estabilizados de 8,5 km cada, mostram a correta implementação do analisador de estados de Bell e a efetiva estabilização do canal, indicando a viabilidade da implementação prática do protocolo.

A implementação de um sistema completo, com a troca efetiva de chave e operando em modo pulsado, será uma continuação do trabalho realizado. Ressalta-se aqui que ainda não há relatos, verificados até o momento, de implementação prática deste protocolo, tendo os autores do protocolo realizado

apenas a verificação da interferência entre dois lasers, em uma medida sem enlace de fibra [1].

[1]O protocolo MDI-QKD foi originalmente divulgado no repositório de acesso livre arxiv.org mantido pela Cornell University Library em 07/09/2011 e posteriormente publicado no periódico Physical Review Letters em 30/03/2012. Em 03/04/2012 foi divulgado no Arxiv um artigo[135] relatando a implementação de uma versão do referido sistema, porém com codificação em time-bin. No momento da impressão da versão final desta tese, estamos trabalhando na versão pulsada do sistema MDI-QKD com codificação em polarização e estabilização dos canais, com previsão de publicação.

Referências Bibliográficas

[1] N. Gisin and R. Thew (2007), *Quantum communication*, Nat. Photon. 1, pp. 165-171.

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden (2002), *Quantum criptography*, Rev. Mod. Phys. 74, pp. 145-195.

[3] R. H. Hadfield (2009), *Single-photon detectors for optical quantum information applications*, Nature Photon. 3, pp. 696-705.

[4] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov 2011 *Invited Review Article: Single-photon sources and detectors* , Rev. Sci. Instrum. 82, pp. 071101.

[5] T. Ferreira da Silva, G. B. Xavier, and J. P. von der Weid (2011), *Real-time characterization of gated-mode single-photon detectors*, IEEE J. Quantum Electron. 47 (9), pp. 1251-1256.

[6] C. Bennett, Brassard (1984), *Quantum cryptography: public key distribution and coin tossing*, International Conference on Computers, Systems / Signal Processing, Proc. of, Bangalore, India, December 10-12.

[7] A. K. Ekert (1991) *Quantum cryptography based on Bell's theorem*, Phys. Rev. Lett. 67, pp. 661–663.

[8] P. W. Shor and J. Preskill (2000) *Simple Proof of Security of the BB84 Quantum Key Distribution Protocol*, Phys. Rev. Lett. 85 (2), pp. 441-444.

[9] H.-K. Lo and H. F. Chau (1999) *Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances*, Science 283 (5410), pp. 2050-2056.

[10] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev (2009) *The security of practical quantum key distribution*, Rev. Mod. Phys 81 (3), pp. 1301–1350.

[11] T. Ferreira da Silva, G. B. Xavier, G. P. Temporão, and J. P. von der Weid (2011), *Monitoring single-photon detectors against eavesdropping in*

quantum cryptography systems, QCRYPT 2011: First Annual Conference on Quantum Cryptography, September 12-16, 2011, Zurich, Switzerland.

[12] T. Ferreira da Silva, G. B. Xavier, G. P. Temporão, and J. P. von der Weid (2012), *Real-time monitoring of single-photon detectors against eavesdropping in quantum key distribution systems*, *Submetido para Optics Express em 2012.*.

[13] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov and G. Leuchs (2011), *After-gate attack on a quantum cryptosystem*, New J. Phys. 13, pp. 013043.

[14] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma (2007) *Time-shift attack in practical quantum cryptosystems*, Quant. Inf. Comp. 7, pp. 073.

[15] N. Sangouard, C. Simon, H. Riedmatten, and N. Gisin (2011) *Quantum repeaters based on atomic ensembles and linear optics*, Rev. Mod. Phys. 83, pp. 33-80.

[16] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. P. Temporão, and J. P. von der Weid (2012), *Polarization-stable long-distance interference of independent photons for quantum communications*, Quantum Information and Measurement, 19-21 March 2012, Berlin, Germany.

[17] H.-K. Lo, M. Curty, and B. Qi (2011) *Measurement device independent quantum key distribution*, arXiv:1109.1473v1 [quant-ph] 7 Sep 2011.

[18] H.-K. Lo, M. Curty, and B. Qi (2012) *Measurement device independent quantum key distribution*, Phys. Rev. Lett. 108, pp. 130503.

[19] N. S. Nightingale (1991), *A new silicon avalanche photodiode photon counting detector module for astronomy*, Exp. Astron. 1, pp. 407422.

[20] B. F. Levine, C. G. Bethea, and J, Campbell (1985), *1.52 μm room temperature photon counting optical time domain reflectometer*, Electron. Lett. 21 (5), pp. 194-196.

[21] A. L. Lacaita, P. A. Francese. S. D. Cova, and G. Ripamonti (1993) *Single-photon optical-time-domain reflectometer at 1.3 m with 5 cm resolution and high sensitivity*, Opt. Lett. 18 (13), pp. 1110-1112.

[22] M. W. Mitchell, J. S. Lundeen, and A. M. Steinberg (2004) *Super-resolving phase measurements with a multiphoton entangled state*, Nature 429, pp. 161-164.

[23] G. Ripamonti and A. Lacaita (1993) *Single-photon semiconductor photodiodes for distributed optical fiber sensors: state of the art and perspectives*, Proc. SPIE ,vol. 1797, pp. 38-49.

[24] A. F. Abouraddy, M. B. Nasr, B. E. A. Saleh, A. V. Sergienko, and M. C. Teich (2002) *Quantum-optical coherence tomography with dispersion cancellation*, Phys. Rev. A, vol. 65, pp. 053817.

[25] S. Cova, M. Ghioni, A. Lacaita, C. Samori, and F. Zappa (1996), *Avalanche photodiodes and quenching circuits for single-photon detection*, Appl. Opt. 35 (12), pp. 1956-1976.

[26] A. Karlsson, M. Bourennane, G. Ribordy, H. Zbeinden, J. Brendel, J. Rarity, and P. Tapster (1999) *A single-photon counter for long-haul telecom*, IEEE Circuits Devices Mag. 15 (6), pp. 34-40.

[27] S. Cova, M. Ghioni, A. Lotito, I. Reich, and F. Zappa, "Evolution and prospects for single-photon avalanche diodes and quenching circuits," J. Mod. Opt. **51**, 1267–1288 (2004).

[28] H. Kume, K. Koyama, K. Nakatsugawa, S. Suzuki, and D. Fatlowitz (1988) *Ultrafast microchannel plate photomultipliers*, Appl. Opt. 27 (6) 6, pp. 1170.

[29] G. Temporão, S. Tanzilli, H. Zbinden, N. Gisin, T. Aellen, M. Giovannini, and J. Faist (2006), *Mid-infrared single-photon counting*, Opt. Lett. 31 (8), pp. 1094-1096.

[30] G. N. Gol'tsman, O. Okunev, G. Chulkova, A. Lipatov, A. Semenov, K. Smirnov, B. Voronov, A. Dzardanov, C. Williams, and Roman Sobolewski (2001) *Picosecond superconducting single-photon optical detector* , App. Phys. Lett. 79 (6), pp. 705-707.

[31] A. Korneev, P. Kouminov, V. Matvienko, G. Chulkova, K. Smirnov, B. Voronov, G. N. Gol'tsman, M. Currie, W. Lo, K. Wilsher, J. Zhang, W. Slysz, A. Pearlman, A. Verevkin, and R. Sobolewski (2004) "Sensitivity and gigahertz counting performance of NbN superconducting single-photon detectors," Appl. Phys. Lett **84** (26), 5338 (1998).

[32] F. Zappa, A. Gulinatti, P. Maccagnani, S. Tisa, and S. Cova (2005) *SPADA: single-photon avalanche diode arrays*, IEEE Photon. Technol. Lett. 17 (3), pp. 657-659.

[33] K. E. Jensen, P. I. Hopman, E. K. Duerr, E. A. Dauler, J. P. Donnelly, S. H. Groves, L. J. Mahoney, K. A. McIntosh, K. M. Molvar, A. Napoleone, D. C.

Oakley, S. Verghese, C. J. Vineis, and R. D. Younger (2006), *Afterpulsing in Geiger-mode avalanche photodiodes for 1.06 μm wavelength*, Appl. Phys. Lett. 88 (13), pp. 133503.

[34] S. Cova, A. Lacaita, and G. Ripamonti (1991), *Trapping phenomena in avalanche photodiodes on nanosecond scale*, IEEE Electron Dev. Lett. 12 (12), pp. 685-687.

[35] J. Zhang, R. Thew, J.-D. Gautier, N. Gisin, and H. Zbinden (2009) *Comprehensive Characterization of InGaAs-InP Avalanche Photodiodes at 1550 nm With an Active Quenching ASIC*, IEEE J. Quantum Electron. 45 (7), pp. 792-799.

[36] A. Yoshizawa, R. Kaji, and H. Tsuchida (2002), *Quantum efficiency evaluation method for gated-mode single-photon detector*, Electron. Lett. 38 (23), pp. 1468-1469.

[37] G. Ribordy, J.-D. Gaultier, H. Zbinden, and N. Gisin, "Performance of InGaAs/InP avalanche photodiodes as gated-mode photon counters," Appl. Opt. **37**, 2272–2277 (1998).

[38] J. C. Campbell (2007) Recent advances in telecommunications avalanche photodiodes, J. Lightwave Technol. 25 (1), pp. 109-121.

[39] P. Antognetti, and W. G. Oldham (1975), *The role of ionization coefficient in the operation of avalanche diodes above breakdown*, J. Electron. Materials 4 (1), pp. 77-90.

[40] W. G. Oldham, R. R. Samuelson, and P. Antognetti, "Triggering phenomena in avalanche diodes," IEEE Trans. Electron Devices **19**, 1056–1060 (1972).

[41] R. J. McIntyre (1973) *On the avalanche initiation probability of avalanche photodiodes above the breakdown voltage*,' IEEE Trans. Electron Devices 20, pp. 637–641.

[42] R. T. Thew, D. Stucki, J.-D. Gautier, H. Zbinden, and A. Rochas (2007) *Free-running InGaAs/InP avalanche photodiode with active quenching for single photon counting at telecom wavelengths*,Appl. Phys. Lett. 91, pp. 201114 (2007).

[43] H. Dautet, P. Deschamps, B. Dion, A. D. MacGregor, D. MacSween, R. J. McIntyre, C. Trottier, and P. P. Webb (1993) *Photon counting techniques with silicon avalanche photodiodes*, App. Opt. 32 (21), pp. 3894-3900.

[44] N. Namekata, Y. Makino, and S. Inoue (2002) *Single-photon detector for long-distance fiber-optic quantum key distribution*, Opt. Lett. 27 (11), pp. 954-956.

[45] A. Lacaita, P. A. Francese, F. Zappa, and S. Cova (1994) *Single-photon detection beyond 1 μm: performance of commercially available germanium photodiodes*, App. Opt. 33 (30), pp. 6902-6918.

[46] C. Gobby, Z. L. Yuan, and A. J. Shields (2004), *Quantum key distribution over 122 km of standard telecom fiber*, Appl. Phys. Lett. 84, pp. 3762.

[47] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten (2009), *High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres*, New J. Phys. 11, pp. 075003.

[48] D. Stucki, G. Ribordy, A. Stefanov, H. Zbinden, J. G. Rarity, and T. Wall (2001), *Photon counting for quantum key distribution with Peltier cooled InGaAs/InP APD's*, J. Mod. Opt. 48 (13), pp. 1967-1981.

[49] Z. L. Yuan, B. E. Kardynal, A. W. Sharpe, and A. J. Shields (2007), *High speed single photon detection in the near infrared*, Appl. Phys. Lett. 91 (4), pp. 041114.

[50] Y. Jian, E. Wu, G. Wu, and H. Zeng (2010), *Optically self-balanced InGaAs-InP avalanche photodiode for infrared single-photon detection*, IEEE Photon. Technol. Lett. 22 (3), pp. 173-175.

[51] N. Namekata, S. Sasamori, and S. Inoue (2006), *800 MHz single-photon detection at 1550-nm using an InGaAs/InP avalanche photodiode operated with a sine wave gating*, Opt. Express 14 (21), pp. 10043-10049.

[52] J. Zhang, R. Thew, C. Barreiro, and H. Zbinden (2009), *Practical fast gate rate InGaAs/InP single-photon avalanche photodiodes*, Appl. Phys. Lett. 95, pp. 091103.

[53] Z. L. Yuan, A. R. Dixon, J. F. Dynes, A. W. Sharpe, and A. J. Shields (2008), *Gigahertz quantum key distribution with InGaAs avalanche photodiodes*, Appl. Phys. Lett. 92, pp. 201104.

[54] A. R. Dixon, J. F. Dynes, Z. L. Yuan, A. W. Sharpe, A. J. Bennett, and A. J. Shields (2009), *Ultrashort dead time of photon-counting InGaAs avalanche photodiodes*, Appl. Phys. Lett., vol. 94, pp. 231113.

[55] N. Namekata, H. Takesue, T. Honjo, Y. Tokura, and S. Inoue (2011), *High-rate quantum key distribution over 100 km using ultra-low-noise, 2-GHz sinusoidally gated InGaAs/InP avalanche photodiodes*, Opt. Express 19 (11), pp. 10632-10639.

[56] B. E. Kardynal, Z. L. Yuan, and A. J. Shields (2008), *An avalanche-photodiode-based photon-number-resolving detector*, Nat. Photon., vol. 2, pp. 425-428.

[57] T. Ferreira da Silva, G. B. Xavier, T. R. Pinheiro, and J. P. von der Weid (2009), *A heralded single-photon source for quantum communications compatible with long-distance optical fibers*, 2009 SBMO/IEEE MTT-S International, pp. 718-720, 3-6 Nov. 2009.

[58] Z.-Y. J. Ou (2007), *Multi-photon quantum interference*, New York: Springer Science+Business Media.

[59] T. Legero, T. Wilk, A. Kuhn, and G. Rempe (2003), *Time-resolved two-photon quantum interference*, App. phys. B 77, pp. 797-803.

[60] B. E. A. Saleh and M. C. Teich (1991), *Fundamentals of photonics*, New York: John Wiley & Sons.

[61] G. Vernam (1926) *Cipher printing telegraph systems for secret wire and radio telegraphic communications*, J. Am. Inst. Electr. Eng. 45, pp. 109-115.

[62] C. E. Shannon (1949) *Communication theory of secrecy systems*, Bell Syst. Tech. J. 28, pp. 656-715.

[63] W. K. Wootters and W. H. Zurek (1982), *A single quantum cannot be cloned*, Nature 299, pp. 802-803.

[64] V. Scarani, S. Iblisdir, N. Gisin, and A. Acín (2005), *Quantum cloning*, Rev. Mod. Phys. 77, pp. 1225-1256.

[65] P. Grangier, J. A. Levenson, and J.-P. Poizat (1998) Quantum non-demolition measurements in optics, Nature 396, pp. 537-542.

[66] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov (2010) *Hacking commercial quantum cryptography systems by tailored bright illumination*, Nat. Photon. 4, pp. 686-689.

[67] V. Makarov and D. R. Hjelme (2005) *Faked states attack on quantum cryptosystems*, J. Mod. Opt. 52, 691-705.

[68] L. Lydersen, N. Jain, C. Wittmann, O. Maroy, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs (2011) *Superlinear threshold detectors in quantum cryptography*, Phys. Rev. A 84 032320.

[69] S. Wiesner (1983), *Conjugate coding*, ACM SIGACT News 15 (1), pp. 78-88.

[70] L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, and V. Makarov (2011) *Controlling a superconducting nanowire single-photon detector using tailored bright illumination*, Pre-print em arXiv:1106.2396v3 [quant-ph].

[71] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin (1992), *Experimental quantum cryptography*, J. Cryptology 5 (1), pp. 3-28.

[72] E. Messmer, Network World (11 out 2007) *Quantum cryptography to secure ballots in Swiss election* http:////www.networkworld.com//news//2007//101007-quantum-cryptography-secure-ballots.html, acessado em 31/08/2011.

[73] Z. Yuan, B. E. Kardynal, R. M. Stevenson, A. J. Shields, C. J. Lobo, K. Cooper, N. S. Beattie, D. A. Ritchie, and M. Pepper (2002) Electrically driven single-photon source, Science 295, pp. 102-105.

[74] S. Fasel, O. Alibart, S. Tanzilli, P. Baldi, A. Beveratos, N. Gisin, and H. Zbinden (2004) *High-quality asynchronous heralded single-photon source at telecom wavelength* , New. J. Phys. 6, pp. 163.

[75] J. G. Rarity, P. C. M. Owens, and P. R. Tapster (1994) *Quantum Random-number Generation and Key Sharing*, J. Mod. Opt. 41 (12), pp. 2435-2444.

[76] G.B. Xavier, T. Ferreira da Silva, G. Vilela de Faria, G.P. Temporao, and J.P. von der Weid (2009) *Practical random number generation protocol for entanglement-based quantum key distribution*, Quantum Inf. Comput., 9 (7 & 8), pp. 0683–0692.

[77] G. B. Xavier, G. Vilela de Faria, G. Temporão and J. P. von der Weid (2008) Full polarization control for fiber optical quantum communication systems using polarization encoding, Opt. Express 16, pp. 1867-1873.

[78] G. B. Xavier, G. Vilela de Faria, T. Ferreira da Silva, G. P. Temporão and J. P. von der Weid (2010) *Two-way quantum communication in a single optical fiber with active polarization compensation*, Quantum Communication and Quantum Networking, Springer Berlin Heidelberg, vol. 36, pp. 125–131.

[79] G. B. Xavier, G. Vilela de Faria, T. Ferreira da Silva, G. P. Temporão, and J. P. von der Weid (2011) *Active polarization control for quantum communication in long-distance optical fibers with shared telecom traffic*, Microwave and Optical Technol. Lett. 53 (11), pp. 2661–2665.

[80] G. B. Xavier, and J. P. von der Weid (2011) *Stable single-photon interference in a 1 km fiber-optic Mach-Zehnder interferometer with continuous phase adjustment* Opt. Lett. 36, pp. 1764-1766.

[81] G. B. Xavier, N. Walenta, G. Vilela de Faria, G. P. Temporão, N. Gisin, H. Zbinden, and J. P. von der Weid (2009) *Experimental polarization encoded quantum key distribution over optical fibres with real-time continuous birefringence compensation*,New J. Phys. 11, pp. 045015.

[82] C. H. Bennett (1992) *Quantum cryptography using any two nonorthogonal states*, Phys. Rev. Lett. 68, pp. 3121–3124.

[83] A. K. Ekert, J. G. Rarity, P. R. Tapster, and G. M. Palma (1992) *Practical quantum cryptography based on two-photon interferometry*, Phys. Rev. Lett 69 (9), pp. 1293-1295

[84] G. Ribordy, J. Brendel, J.-D. Gautier, N. Gisin, and H. Zbinden (2000) Long-distance entanglement-based quantum key distribution , Phys. Rev. A 63, pp. 012309.

[85] J. M. Mérolla, Y. Mazurenko, J. P. Goedgebuer, and W. T. Rhodes (1999) *Single-photon interference in sideband of phase-modulated light for quantum cryptography*, Phys. Rev. Lett. 82, pp. 1656-1659.

[86] G. B. Xavier and J. P. von der Weid (2005) *Modulation schemes for frequency coded quantum key distribution*, Elect. Lett. 41 (10), pp. 607-608.

[87] T. Ferreira da Silva and J. P. von der Weid (2009) *Optical transmission of frequency-coded quantum bits with WDM synchronization*, J. Microwaves Optoelectron. Electromag. Appl. 8 (1), pp. 163S-178S.

[88] W.-Y. Hwang (2003) *Quantum Key Distribution with High Loss: Toward Global Secure Communication*, Phys. Rev. Lett. 91, pp. 057901.

[89] H.-K. Lo, X. Ma, and K. Chen (2005) *Decoy State Quantum Key Distribution*, Phys. Rev. Lett. 94, pp. 230504.

[90] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian (2006) *Experimental quantum key distribution with decoy states*, Phys. Rev. Lett. 96, pp. 070502.

[91] G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters (1993) *Teleporting an unknown quantum state via dual classic and Einstein-Podolsky-Rosen channels*, Phys. Rev. Lett. 70, 1895-1899.

[92] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger (1997) *Experimental quantum teleportation*, Nature 390, pp. 575–579.

[93] K. F. Reim, P. Michelberger, K. C. Lee, J. Nunn, N. K. Langford, and I. A. Walmsley (2011) Single-Photon-Level Quantum Memory at Room Temperature , Phys. Rev. Lett 107, pp. 053603.

[94] Felix S, Gisin N, Stefanov A and Zbinden H 2001, *Faint laser quantum key distribution: eavesdropping exploiting multiphoton pulses*, J. Mod. Phys. 48 (13), pp. 2009-2021.

[95] B. C. Jacobs, T. B. Pittman, and J. D. Franson (2002) Quantum relays and noise suppression using linear optics, Phys. Rev. A 66, pp. 052307.

[96] H. Riedmatten, I. Marcikic, W. Tittel, H. Zbinden, D. Collins, and N. Gisin (2004) Long Distance Quantum Teleportation in a Quantum Relay Configuration , Phys. Rev. Lett. 92, pp. 047904.

[97] H. F. Chau (2002) *Practical scheme to share a secret key through a quantum channel with a 27.6% bit error rate*, Phys. Rev. A 66, pp. 060302(R).

[98] C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma (2009) *Security proof of quantum key distribution with detection efficiency mismatch*, Quantum Inf. Comput. 9, pp. 131-165.

[99] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo (2008) *Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems*, Phys. Rev. A 78, pp. 042333.

[100] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov (2011) *Full-field implementation of a perfect eavesdropper on a quantum cryptography system*, Nat. Commun. 2, pp. 349.

[101] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy (2006) Trojan-horse attacks on quantum-key-distribution systems, Phys. Rev. A 73, pp. 022320.

[102] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin (1997) *"Plug and play" systems for quantum cryptography* , App. Phy. Lett. 70, pp. 793-795.

[103] S.-H. Sun, M.-S. Jiang, and L.-M. Liang (2011) *Passive Faraday-mirror attack in a practical two-way quantum-key-distribution system*, Phys. Rev. A 83, 062331.

[104] V. Makarov, A. Anisimov, and J. Skaar (2006) *Effects of detector efficiency mismatch on security of quantum cryptosystems*, Phys. Rev. A 74, pp. 022313.

[105] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter (2011) *Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors*, New J. Phys. 13, pp. 073024.

[106] V. Makarov (2009) *Controlling passively quenched single photon detectors by bright light*, New J. Phys. 11, pp. 065003.

[107] S. Sauge, L. Lydersen, A. Anisimov, J. Skaar, and V. Makarov (2011) *Controlling an actively-quenched single photon detector with bright light*, Optics Express19 (23), pp. 23590-23600.

[108] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar and V. Makarov (2010) *Thermal blinding of gated detectors in quantum cryptography*, Optics Express, Vol. 18 Issue 26, pp. 27938–27954.

[109] Z. L. Yuan, J. F. Dynes, and A. J. Shields (2010) *Avoiding the blinding attack in QKD*, Nat. Photonics 4, pp. 800-801.

[110] Z. L. Yuan, J. F. Dynes, and A. J. Shields (2011) *Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography*, Appl. Phys. Lett. 98, pp. 231104.

[111] L. Lydersen, V. Makarov, and J. Skaar (2011) *Comment on "Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography" [Appl. Phys. Lett. 98, 231104 (2011)]*, Appl. Phys. Lett. 99, pp. 196101.

[112] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs (2011) Device Calibration Impacts Security of Quantum Key Distribution Phys. Rev. Lett. 107, pp. 110501.

[113] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter (2007) *Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km*, Phys. Rev. Lett. 98, pp. 010504.

[114] G. Ribordy, J.-D. Gaultier, H. Zbinden, and N. Gisin, "Performance of InGaAs/InP avalanche photodiodes as gated-mode photon counters," Appl. Opt. **37**, 2272–2277 (1998).

[115] C. H. Bennett, and S. J. Wiesner (1992) *Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states*, Phys. Rev. Lett. 69 (20), pp. 2881–2884.

[116] K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger (1996) *Dense Coding in Experimental Quantum Communication*, Phys. Rev. Lett. 76 (25), pp. 4656–4659.

[117] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller (1998) *Quantum repeaters: the role of imperfect local operations in quantum communication*, Phys. Rev. Lett. 81 (26), pp. 5932–5935.

[118] D. Bouwmeester, A. Ekert, and A. Zeilinger (xx), *The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation, Quantum Computation*, Berlin: Springer.

[119] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller (1999) *Quantum repeaters based on entanglement purification*, Phys. Rev. A 59 (1), pp. 169–181.

[120] J.-W. Pan, C. Simon, C. Brukner, and A. Zeilinger (2001) *Entanglement purification for quantum communication*, Nature 410, pp. 1067-1070.

[121] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller (2001) *Long-distance quantum communication with atomic ensembles and linear optics*, Nature 414, 413–418.

[122] Z.-S. Yuan, Y.-A. Chen, B. Zhao, S. Chen., J. Schmiedmayer, and J.-W. Pan (2008) *Experimental demonstration of a BDCZ quantum repeater node*, Nature 454 (28), pp. 1098–1101.

[123] Z.-B. Chen, B. Zhao, Y.-A. Chen, J. Schmiedmayer, and J.-W. Pan (2007) *Fault-tolerant quantum repeater with atomic ensembles and linear optics*, Phys. Rev. A 76,pp. 022329.

[124] J.-W. Pan, Z.-B. Chen, C.-Y. Lu, H. Weinfurter, A. Zeilinger, and M. Zukowski (2011) *Multi-photon entanglement and interferometry*, Pre-print in arXiv:0805.2853v2.

[125] H. Paul (1986) *Interference between independent photons*, Rev. Mod. Phys. 58 (1), pp. 209-231.

[126] P. D. Townsend, J. G. Rarity and P. R. Tapster (1993) *Single photon interference in 10 km long optical fibre interferometer*, Elect. Lett. 29 (7), pp. 634-635.

[127] R. Kaltenbaek, B. Blauensteiner, M. Zukowski, M. Aspelmeyer, and A. Zeilinger (2006) *Experimental interference of independent photons*, Phys. Rev. Lett. 96, pp. 240502.

[128] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani (2007) *Proposal for Implementing Device-Independent Quantum Key Distribution Based on a Heralded Qubit Amplifier*, Phys. Rev. Lett. 98, pp. 230501.

[129] N. Gisin, S. Pironio, and N. Sangouard (2010) *Proposal for Implementing Device-Independent Quantum Key Distribution Based on a Heralded Qubit Amplifier*, Phys. Rev. Lett. 105,pp. 070501.

[130] C. C. Gerry, and P. L. Knight(2005), *Introductory quantum optics*, New York: Cambridge Univeristy Press.

[131] J. G. Rarity, P. R. Tapster, and R. Loudon (2005) *Non-classical interference between independent sources* J. Opt. B: Quantum Semiclass. Opt. 7, pp. S171-S175.

[132] J. Calsamiglia, and N. Lütkenhaus (2001) *Maximum efficiency of a linear-optical Bell-state analyzer*, App. Phys. B 72, pp. 67–71.

[133] J. A. W. van Houwelingen, N. Brunner, A. Beveratos, H. Zbinden, and N. Gisin (2006) *Quantum Teleportation with a Three-Bell-State Analyzer*, Phys. Rev. Lett. 96, pp. 130502.

[134] D. Vitorei, T. Ferreira da Silva, G. P. Temporão, and J. P. von der Weid (2012) *Tailoring two-photon interference from independent sources*, *Aceito para* 11th Intl. Conference on Quantum Communication, Measurement and Computing (QCMC), Vienna, Autria, 30th July - 3rd August 2012.

[135] A. Rubenok, J .A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel (2012) *Proof-of-principle field test of quantum key distribution immune to detector attacks*, arXiv:1204.0738v1, 3 Apr 2012.

Apêndice

Analisador de estados de Bell: fonte poissoniana

Neste apêndice será considerado o caso em que os estados quânticos de entrada no analisador de estados de Bell, mostrado na figura 5.2.1, são emitidos por duas fontes poissonianas. Novamente, cada fóton pode ser codificado em duas bases, $\oplus$ e $\otimes$, formadas por estados de polarização ortogonais. Como visto, a probabilidade de ocorrência de dois fótons no mesmo modo espacial de entrada do analisador é metade da probabilidade de ocorrência de um fóton em cada porta de entrada. Serão consideradas as probabilidade P_1=P(1)P(1) de incidência de um fóton enviado por Alice e um fóton enviado por Bob; P_2=P(2)P(0), referente à dois fóton enviados por Alice; e P_2=P(0)P(2) referente à probabilidade de dois fótons serem enviados por Bob, somando à unidade (P_1+2P_2=1). Os modos temporais serão identificados com um índice sobrescrito. Serão calculadas as probabilidades de ocorrência e não-ocorrência do efeito de agrupamento de fótons após o BS (*photon bunching*), referenciadas como *B* e *NB*, respectivamente. A fração de eventos correspondendo a coincidências entre detectores, ou existência de fótons simultaneamente em mais de um modo espacial, será calculada e representada por C, com a probabilidade de não ocorrência de coincidência representada por NC. Finalmente, será calculada a probabilidade condicional de eventos coincidentes entre determinado par de detectores, dada a ocorrência de uma coincidência. A probabilidade relativa de coincidências será renormalizada considerando apenas os casos utilizados nas medições realizadas nesta tese, em que foram observadas coincidências de eventos entre os pares de SPADs 1 e 2; 1 e 3; e 1 e 4.

I. $|\mathrm{H}\rangle_{\mathbf{Alice}}$, $|\mathrm{H}\rangle_{\mathbf{Bob}} \Rightarrow$ **caso indistinguível**

$$P_1|H^1\rangle_a|H^1\rangle_b\langle H^1|_a\langle H^1|_b + P_2|H^2\rangle_a|H^2\rangle_a\langle H^2|_a\langle H^2|_a \\ +P_2|H^3\rangle_b|H^3\rangle_b\langle H^3|_b\langle H^3|_b$$

Observando após o BS, a probabilidade de agrupamento dos fótons no mesmo modo espacial $|\rangle_c$ ou $|\rangle_d$ ou de separação dos fótons (B e NB, respectivamente)

será B=3/4 e NB=1/4. Considerando agora os eventos de detecção:

$$\begin{aligned} BELL_{|H\rangle|H\rangle ind} &\rightarrow \frac{1}{\sqrt{2}}\left(|D_1\rangle + |D_3\rangle\right) \text{ com } P_1 \\ &\rightarrow \frac{1}{2}\left(|D_1\rangle - |D_3\rangle + j|C_{13}\rangle + j|C_{13}\rangle\right) \text{ com } P_2 \\ &\rightarrow \frac{1}{2}\left(-|D_1\rangle + |D_3\rangle + j|C_{13}\rangle + j|C_{13}\rangle\right) \text{ com } P_2 \end{aligned}$$

A probabilidade de ocorrência (C) e de não ocorrência (NC) de um evento coincidente é obtida a partir do resultado acima, e pode ser quantificada como C=1/4 e NC=3/4.

Após normalização, a probabilidade condicional de ocorrência de determinada coincidência dado que houve um evento coincidente pode ser escrita como:

C_{12}=0; C_{13}=1; C_{14}=0; C_{23}=0; C_{24}=0; C_{34}=0.

Considerando agora apenas as coincidências observáveis quando o detector 1 opera como trigger para os demais, temos a probabilidade de ocorrência de determinado resultado, após normalização:

C_{12}=0; C_{13}=1; C_{14}=0.

II. $|H\rangle_{\mathbf{Alice}}$, $|H\rangle_{\mathbf{Bob}} \Rightarrow$ **caso distinguível**

$$\begin{aligned} P_1|H^1\rangle_a|H^2\rangle_b\langle H^1|_a\langle H^2|_b + P_2|H^3\rangle_a|H^3\rangle_a\langle H^3|_a\langle H^3|_a \\ +P_2|H^4\rangle_b|H^4\rangle_b\langle H^4|_b\langle H^4|_b \end{aligned}$$

Observando após o BS, a probabilidade de agrupamento dos fótons no mesmo modo espacial $|\rangle_c$ ou $|\rangle_d$ ou de separação dos fótons (B e NB, respectivamente) será B=1/2; NB=1/2. Considerando agora os eventos de detecção:

$$\begin{aligned} BELL_{|H\rangle|H\rangle dist} &\rightarrow \frac{1}{2}\left(j|D_1\rangle + j|D_2\rangle + |C_{13}\rangle - |C_{13}\rangle\right) \text{ com } P_1 \\ &\rightarrow \frac{1}{2}\left(|D_1\rangle - |D_3\rangle + j|C_{13}\rangle + j|C_{13}\rangle\right) \text{ com } P_2 \\ &\rightarrow \frac{1}{2}\left(-|D_1\rangle + |D_3\rangle + j|C_{13}\rangle + j|C_{13}\rangle\right) \text{ com } P_2 \end{aligned}$$

A probabilidade de ocorrência (C) e de não ocorrência (NC) de um evento coincidente é obtida a partir do resultado acima, e pode ser quantificada como C=1/2 e NC=1/2.

Após normalização, a probabilidade condicional de ocorrência de determinada coincidência dado que houve um evento coincidente pode ser escrita como:

C_{12}=0; C_{13}=1; C_{14}=0; C_{23}=0; C_{24}=0; C_{34}=0.

Considerando agora apenas as coincidências observáveis quando o detector 1 opera como trigger para os demais, temos a probabilidade de ocorrência de determinado resultado, após normalização:
C_{12}=0; C_{13}=1; C_{14}=0.

III. $|V\rangle_{\mathbf{Alice}}$, $|V\rangle_{\mathbf{Bob}} \Rightarrow$ **caso indistinguível**

$$P_1|V^1\rangle_a|V^1\rangle_b\langle V^1|_a\langle V^1|_b + P_2|V^2\rangle_a|V^2\rangle_a\langle V^2|_a\langle V^2|_a \\ +P_2|V^3\rangle_b|V^3\rangle_b\langle V^3|_b\langle V^3|_b$$

Observando após o BS, a probabilidade de agrupamento dos fótons no mesmo modo espacial $|\rangle_c$ ou $|\rangle_d$ ou de separação dos fótons (B e NB, respectivamente) será B=3/4 e NB=1/4.
Considerando agora os eventos de detecção:

$$\begin{aligned} BELL_{|V\rangle|V\rangle ind} &\rightarrow \frac{1}{\sqrt{2}}\left(|D_2\rangle + |D_4\rangle\right) \text{ com } P_1 \\ &\rightarrow \frac{1}{2}\left(-|D_2\rangle + |D_4\rangle - j|C_{24}\rangle - j|C_{24}\rangle\right) \text{ com } P_2 \\ &\rightarrow \frac{1}{2}\left(|D_2\rangle - |D_4\rangle - j|C_{24}\rangle - j|C_{24}\rangle\right) \text{ com } P_2 \end{aligned}$$

A probabilidade de ocorrência (C) e de não ocorrência (NC) de um evento coincidente é obtida a partir do resultado acima, e pode ser quantificada como C=1/4 e NC=3/4.
Após normalização, a probabilidade condicional de ocorrência de determinada coincidência dado que houve um evento coincidente pode ser escrita como:
C_{12}=0; C_{13}=0; C_{14}=0; C_{23}=0; C_{24}=1; C_{34}=0
Considerando agora apenas as coincidências observáveis quando o detector 1 opera como trigger para os demais, temos a probabilidade de ocorrência de determinado resultado, após normalização:
C_{12}=0; C_{13}=0; C_{14}=0.

IV. $|V\rangle_{\mathbf{Alice}}$, $|V\rangle_{\mathbf{Bob}} \Rightarrow$ **caso distinguível**

$$P_1|V^1\rangle_a|V^2\rangle_b\langle V^1|_a\langle V^2|_b + P_2|V^3\rangle_a|V^3\rangle_a\langle V^3|_a\langle V^3|_a \\ +P_2|V^4\rangle_b|V^4\rangle_b\langle V^4|_b\langle V^4|_b$$

Observando após o BS, a probabilidade de agrupamento dos fótons no mesmo

modo espacial $|\rangle_c$ ou $|\rangle_d$ ou de separação dos fótons (B e NB, respectivamente) será B=1/2 e NB=1/2.

Considerando agora os eventos de detecção:

$$\begin{aligned} BELL_{|V\rangle|V\rangle dist} &\rightarrow \frac{1}{2}\left(-j|D_2\rangle - j|D_4\rangle - |C_{24}\rangle + |C_{24}\rangle\right) \text{ com } P_1 \\ &\rightarrow \frac{1}{2}\left(-|D_2\rangle + |D_4\rangle - j|C_{24}\rangle - j|C_{24}\rangle\right) \text{ com } P_2 \\ &\rightarrow \frac{1}{2}\left(+|D_2\rangle - |D_4\rangle - j|C_{24}\rangle - j|C_{24}\rangle\right) \text{ com } P_2 \end{aligned}$$

A probabilidade de ocorrência (C) e de não ocorrência (NC) de um evento coincidente é obtida a partir do resultado acima, e pode ser quantificada como C=1/2 e NC=1/2.

Após normalização, a probabilidade condicional de ocorrência de determinada coincidência dado que houve um evento coincidente pode ser escrita como:

C_{12}=0; C_{13}=0; C_{14}=0; C_{23}=0; C_{24}=1; C_{34}=0.

Considerando agora apenas as coincidências observáveis quando o detector 1 opera como trigger para os demais, temos a probabilidade de ocorrência de determinado resultado, após normalização:

C_{12}=0; C_{13}=0; C_{14}=0.

V. $|H\rangle_{\mathbf{Alice}}$, $|V\rangle_{\mathbf{Bob}}$ ⇒ **indistinguibilidade não faz sentido aqui**

$$\begin{aligned} P_1|H^1\rangle_a|V^2\rangle_b\langle H^1|_a\langle V^2|_b + P_2|H^3\rangle_a|H^3\rangle_a\langle H^3|_a\langle H^3|_a \\ +P_2|V^4\rangle_b|V^4\rangle_b\langle V^4|_b\langle V^4|_b \end{aligned}$$

Observando após o BS, a probabilidade de agrupamento dos fótons no mesmo modo espacial $|\rangle_c$ ou $|\rangle_d$ ou de separação dos fótons (B e NB, respectivamente) será B=1/2 e NB=1/2.

Considerando agora os eventos de detecção:

$$\begin{aligned} BELL_{|H\rangle|V\rangle} &\rightarrow \frac{1}{2}\left(-|C_{12}\rangle - |C_{34}\rangle + j|C_{14}\rangle - j|C_{23}\rangle\right) \text{ com } P_1 \\ &\rightarrow \frac{1}{2}\left(|D_1\rangle - |D_3\rangle + j|C_{13}\rangle + j|C_{13}\rangle\right) \text{ com } P_2 \\ &\rightarrow \frac{1}{2}\left(+|D_2\rangle - |D_4\rangle - j|C_{24}\rangle - j|C_{24}\rangle\right) \text{ com } P_2 \end{aligned}$$

A probabilidade de ocorrência (C) e de não ocorrência (NC) de um evento coincidente é obtida a partir do resultado acima, e pode ser quantificada como C=3/4 e NC=1/4.

Após normalização, a probabilidade condicional de ocorrência de determinada coincidência dado que houve um evento coincidente pode ser escrita como:
C_{12}=1/6; C_{13}=1/6; C_{14}=1/6; C_{23}=1/6; C_{24}=1/6; C_{34}=1/6.
Considerando agora apenas as coincidências observáveis quando o detector 1 opera como trigger para os demais, temos a probabilidade de ocorrência de determinado resultado, após normalização:
C_{12}=1/3; C_{13}=1/3; C_{14}=1/3.

VI. $|V\rangle_{\mathbf{Alice}}$, $|H\rangle_{\mathbf{Bob}}$ ⇒ **indistinguibilidade não faz sentido aqui**

$$P_1|V^1\rangle_a|H^2\rangle_b\langle V^1|_a\langle H^2|_b + P_2|V^3\rangle_a|V^3\rangle_a\langle V^3|_a\langle V^3|_a \\ +P_2|H^4\rangle_b|H^4\rangle_b\langle H^4|_b\langle H^4|_b$$

Observando após o BS, a probabilidade de agrupamento dos fótons no mesmo modo espacial $|\rangle_c$ ou $|\rangle_d$ ou de separação dos fótons (B e NB, respectivamente) será B=1/2 e NB=1/2. Considerando agora os eventos de detecção:

$$\begin{aligned} BELL_{|V\rangle|H\rangle} &\rightarrow \frac{1}{2}\left(-|C_{12}\rangle - |C_{34}\rangle + j|C_{14}\rangle - j|C_{23}\rangle\right) \text{ com } P_1 \\ &\rightarrow \frac{1}{2}\left(-|D_2\rangle + |D_4\rangle - j|C_{24}\rangle - j|C_{24}\rangle\right) \text{ com } P_2 \\ &\rightarrow \frac{1}{2}\left(-|D_1\rangle + |D_3\rangle + j|C_{13}\rangle + j|C_{13}\rangle\right) \text{ com } P_2 \end{aligned}$$

O restante da análise é idêntica ao item anterior.

VII. $|{+}45\rangle_{\mathbf{Alice}}$, $|{+}45\rangle_{\mathbf{Bob}}$ ⇒ **caso indistinguível**

$$P_1|+45^1\rangle_a|+45^1\rangle_b\langle+45^1|_a\langle+45^1|_b + P_2|+45^2\rangle_a|+45^2\rangle_a\langle+45^2|_a\langle+45^2|_a \\ +P_2|+45^3\rangle_b|+45^3\rangle_b\langle+45^3|_b\langle+45^3|_b$$

Observando após o BS, a probabilidade de agrupamento dos fótons no mesmo modo espacial $|\rangle_c$ ou $|\rangle_d$ ou de separação dos fótons (B e NB, respectivamente) será B=3/4 e NB=1/4. Considerando agora os eventos de detecção:

$$\begin{aligned} BELL_{|+45\rangle|+45\rangle ind} &\rightarrow \frac{1}{2\sqrt{2}}\{j|D_1\rangle + j|D_3\rangle - j|D_2\rangle - j|D_4\rangle \\ &\quad -|C_{12}\rangle - |C_{12}\rangle - |C_{34}\rangle - |C_{34}\rangle\} \text{ com } P_1 \\ &\rightarrow \frac{1}{4}\{|D_1\rangle - |D_3\rangle - |D_2\rangle + |D_4\rangle \\ &\quad +j|C_{12}\rangle - j|C_{34}\rangle + j|C_{12}\rangle - j|C_{34}\rangle \end{aligned}$$

$$
\begin{aligned}
& +j|C_{13}\rangle - j|C_{24}\rangle + j|C_{13}\rangle - j|C_{24}\rangle \\
& -|C_{14}\rangle - |C_{23}\rangle - |C_{23}\rangle - |C_{14}\rangle\} \text{ com } P_2 \\
\rightarrow\ & \frac{1}{4}\{-|D_1\rangle + |D_3\rangle + |D_2\rangle - |D_4\rangle \\
& -j|C_{12}\rangle + j|C_{34}\rangle - j|C_{12}\rangle + j|C_{34}\rangle \\
& +j|C_{13}\rangle - j|C_{24}\rangle + j|C_{13}\rangle - j|C_{24}\rangle \\
& -|C_{14}\rangle - |C_{23}\rangle - |C_{23}\rangle - |C_{14}\rangle\} \text{ com } P_2
\end{aligned}
$$

A probabilidade de ocorrência (C) e de não ocorrência (NC) de um evento coincidente é obtida a partir do resultado acima, e pode ser quantificada como C=5/8 e NC=3/8. Após normalização, a probabilidade condicional de ocorrência de determinada coincidência dado que houve um evento coincidente pode ser escrita como:
C_{12}=3/10; C_{13}=1/10; C_{14}=1/10; C_{23}=1/10; C_{24}=1/10; C_{34}=3/10.
Considerando agora apenas as coincidências observáveis quando o detector 1 opera como trigger para os demais, temos a probabilidade de ocorrência de determinado resultado, após normalização:
C_{12}=3/5; C_{13}=1/5; C_{14}=1/5.

VIII. $|+45\rangle_{\mathbf{Alice}}$, $|+45\rangle_{\mathbf{Bob}} \Rightarrow$ **caso distinguível**

$$
\begin{aligned}
P_1|+45^1\rangle_a|+45^2\rangle_b\langle+45^1|_a\langle+45^2|_b + P_2|+45^3\rangle_a|+45^3\rangle_a\langle+45^3|_a\langle+45^3|_a \\
+P_2|+45^4\rangle_b|+45^4\rangle_b\langle+45^4|_b\langle+45^4|_b
\end{aligned}
$$

Observando após o BS, a probabilidade de agrupamento dos fótons no mesmo modo espacial $|\rangle_c$ ou $|\rangle_d$ ou de separação dos fótons (B e NB, respectivamente) será B=1/2 e NB=1/2. Considerando agora os eventos de detecção:

$$
\begin{aligned}
BELL_{|+45\rangle|+45\rangle dist} \rightarrow\ & \frac{1}{4}\{j|D_1\rangle + j|D_3\rangle - j|D_2\rangle - j|D_4\rangle \\
& -|C_{12}\rangle - |C_{12}\rangle - |C_{34}\rangle - |C_{34}\rangle \\
& +|C_{13}\rangle + |C_{24}\rangle - |C_{13}\rangle - |C_{24}\rangle \\
& +j|C_{14}\rangle + j|C_{23}\rangle - j|C_{23}\rangle - j|C_{14}\rangle\} \text{ com } P_1 \\
\rightarrow\ & 14\{|D_1\rangle - |D_3\rangle - |D_2\rangle + |D_4\rangle \\
& +j|C_{12}\rangle - j|C_{34}\rangle + j|C_{12}\rangle - j|C_{34}\rangle \\
& +j|C_{13}\rangle - j|C_{24}\rangle + j|C_{13}\rangle - j|C_{24}\rangle \\
& -|C_{14}\rangle - |C_{23}\rangle - |C_{23}\rangle - |C_{14}\rangle\} \text{ com } P_2 \\
\rightarrow\ & \frac{1}{4}\{-|D_1\rangle + |D_3\rangle + |D_2\rangle - |D_4\rangle
\end{aligned}
$$

$$-j|C_{12}\rangle + j|C_{34}\rangle - j|C_{12}\rangle + j|C_{34}\rangle$$
$$+j|C_{13}\rangle - j|C_{24}\rangle + j|C_{13}\rangle - j|C_{24}\rangle$$
$$-|C_{14}\rangle - |C_{23}\rangle - |C_{23}\rangle - |C_{14}\rangle\} \text{ com } P_2$$

A probabilidade de ocorrência (C) e de não ocorrência (NC) de um evento coincidente é obtida a partir do resultado acima, e pode ser quantificada como C=6/8 e NC=2/8.

Após normalização, a probabilidade condicional de ocorrência de determinada coincidência dado que houve um evento coincidente pode ser escrita como:

C_{12}=1/6; C_{13}=1/6; C_{14}=1/6; C_{23}=1/6; C_{24}=1/6; C_{34}=1/6.

Considerando agora apenas as coincidências observáveis quando o detector 1 opera como trigger para os demais, temos a probabilidade de ocorrência de determinado resultado, após normalização:

C_{12}=1/3; C_{13}=1/3; C_{14}=1/3.

IX. $|\text{-}45\rangle_{\mathbf{Alice}}$, $|\text{-}45\rangle_{\mathbf{Bob}} \Rightarrow$ **caso indistinguível**

$$P_1|-45^1\rangle_a|-45^1\rangle_b\langle-45^1|_a\langle-45^1|_b + P_2|-45^2\rangle_a|-45^2\rangle_a\langle-45^2|_a\langle-45^2|_a$$
$$+P_2|-45^3\rangle_b|-45^3\rangle_b\langle-45^3|_b\langle-45^3|_b$$

Observando após o BS, a probabilidade de agrupamento dos fótons no mesmo modo espacial $|\rangle_c$ ou $|\rangle_d$ ou de separação dos fótons (B e NB, respectivamente) será B=3/4 e NB=1/4. Considerando agora os eventos de detecção:

$$\begin{aligned} BELL_{|-45\rangle|-45\rangle ind} \rightarrow\ & \frac{1}{2\sqrt{2}}\{j|D_1\rangle + j|D_3\rangle - j|D_2\rangle - j|D_4\rangle \\ & +|C_{12}\rangle + |C_{12}\rangle + |C_{34}\rangle + |C_{34}\rangle\} \text{ com } P_1 \\ \rightarrow\ & \frac{1}{4}\{|D_1\rangle - |D_3\rangle - |D_2\rangle + |D_4\rangle \\ & -j|C_{12}\rangle + j|C_{34}\rangle - j|C_{12}\rangle + j|C_{34}\rangle \\ & +j|C_{13}\rangle - j|C_{24}\rangle + j|C_{13}\rangle - j|C_{24}\rangle \\ & +|C_{14}\rangle + |C_{23}\rangle + |C_{23}\rangle + |C_{14}\rangle\} \text{ com } P_2 \\ \rightarrow\ & \frac{1}{4}\{-|D_1\rangle + |D_3\rangle + |D_2\rangle - |D_4\rangle \\ & +j|C_{12}\rangle - j|C_{34}\rangle + j|C_{12}\rangle - j|C_{34}\rangle \\ & +j|C_{13}\rangle - j|C_{24}\rangle + j|C_{13}\rangle - j|C_{24}\rangle \\ & +|C_{14}\rangle + |C_{23}\rangle + |C_{23}\rangle + |C_{14}\rangle\} \text{ com } P_2 \end{aligned}$$

A probabilidade de ocorrência (C) e de não ocorrência (NC) de um evento

coincidente é obtida a partir do resultado acima, e pode ser quantificada como C=5/8 e NC=3/8. Após normalização, a probabilidade condicional de ocorrência de determinada coincidência dado que houve um evento coincidente pode ser escrita como:
C_{12}=3/10; C_{13}=1/10; C_{14}=1/10; C_{23}=1/10; C_{24}=1/10; C_{34}=3/10.
Considerando agora apenas as coincidências observáveis quando o detector 1 opera como trigger para os demais, temos a probabilidade de ocorrência de determinado resultado, após normalização:
C_{12}=3/5; C_{13}=1/5; C_{14}=1/5.

X. $|+45\rangle_{\mathbf{Alice}}$, $|+45\rangle_{\mathbf{Bob}}$ ⇒ **caso distinguível**

$$P_1|-45^1\rangle_a|-45^2\rangle_b\langle -45^1|_a\langle -45^2|_b + P_2|-45^3\rangle_a|-45^3\rangle_a\langle -45^3|_a\langle -45^3|_a + P_2|-45^4\rangle_b|-45^4\rangle_b\langle -45^4|_b\langle -45^4|_b$$

Observando após o BS, a probabilidade de agrupamento dos fótons no mesmo modo espacial $|\rangle_c$ ou $|\rangle_d$ ou de separação dos fótons (B e NB, respectivamente) será B=1/2 e NB=1/2. Considerando agora os eventos de detecção:

$$\begin{aligned}
BELL_{|-45\rangle|-45\rangle dist} \rightarrow\ & \frac{1}{4}\{j|D_1\rangle + j|D_3\rangle - j|D_2\rangle - j|D_4\rangle \\
& +|C_{12}\rangle + |C_{12}\rangle + |C_{34}\rangle + |C_{34}\rangle \\
& +|C_{13}\rangle + |C_{24}\rangle - |C_{13}\rangle - |C_{24}\rangle \\
& -j|C_{14}\rangle + j|C_{23}\rangle + j|C_{23}\rangle - j|C_{14}\rangle\} \text{ com } P_1 \\
\rightarrow\ & 14\{|D_1\rangle - |D_3\rangle - |D_2\rangle + |D_4\rangle \\
& -j|C_{12}\rangle + j|C_{34}\rangle - j|C_{12}\rangle + j|C_{34}\rangle \\
& +j|C_{13}\rangle - j|C_{24}\rangle + j|C_{13}\rangle - j|C_{24}\rangle \\
& +|C_{14}\rangle + |C_{23}\rangle + |C_{23}\rangle + |C_{14}\rangle\} \text{ com } P_2 \\
\rightarrow\ & \frac{1}{4}\{-|D_1\rangle + |D_3\rangle + |D_2\rangle - |D_4\rangle \\
& +j|C_{12}\rangle - j|C_{34}\rangle + j|C_{12}\rangle - j|C_{34}\rangle \\
& +j|C_{13}\rangle - j|C_{24}\rangle + j|C_{13}\rangle - j|C_{24}\rangle \\
& +|C_{14}\rangle + |C_{23}\rangle + |C_{23}\rangle + |C_{14}\rangle\} \text{ com } P_2
\end{aligned}$$

A probabilidade de ocorrência (C) e de não ocorrência (NC) de um evento coincidente é obtida a partir do resultado acima, e pode ser quantificada como C=6/8 e NC=2/8.
Após normalização, a probabilidade condicional de ocorrência de determinada

coincidência dado que houve um evento coincidente pode ser escrita como:
C_{12}=1/6; C_{13}=1/6; C_{14}=1/6; C_{23}=1/6; C_{24}=1/6; C_{34}=1/6.
Considerando agora apenas as coincidências observáveis quando o detector 1 opera como trigger para os demais, temos a probabilidade de ocorrência de determinado resultado, após normalização:
C_{12}=1/3; C_{13}=1/3; C_{14}=1/3.

XI. $|+45\rangle_{\mathbf{Alice}}$, $|\text{-}45\rangle_{\mathbf{Bob}} \Rightarrow$ **caso indistinguível**

$$P_1|+45^1\rangle_a|-45^1\rangle_b\langle+45^1|_a\langle-45^1|_b + P_2|+45^2\rangle_a|+45^2\rangle_a\langle+45^2|_a\langle+45^2|_a \\ +P_2|-45^3\rangle_b|-45^3\rangle_b\langle-45^3|_b\langle-45^3|_b$$

Observando após o BS, a probabilidade de agrupamento dos fótons no mesmo modo espacial $|\rangle_c$ ou $|\rangle_d$ ou de separação dos fótons (B e NB, respectivamente) será B=1/2 e NB=1/2. Considerando agora os eventos de detecção:

$$\begin{aligned} BELL_{|+45\rangle|-45\rangle ind} \;\rightarrow\; & \frac{1}{2\sqrt{2}}\{j|D_1\rangle + j|D_2\rangle + j|D_3\rangle + j|D_4\rangle \\ & -j|C_{14}\rangle + j|C_{24}\rangle + j|C_{32}\rangle - j|C_{41}\rangle\} \text{ com } P_1 \\ \rightarrow\; & \frac{1}{4}\{+|D_1\rangle - |D_2\rangle + j|C_{12}\rangle + j|C_{21}\rangle \\ & -|D_3\rangle + |D_4\rangle - j|C_{34}\rangle - j|C_{43}\rangle \\ & +j|C_{13}\rangle - j|C_{24}\rangle - |C_{14}\rangle - |C_{24}\rangle \\ & +j|C_{31}\rangle - j|C_{42}\rangle - |C_{32}\rangle - |C_{41}\rangle\} \text{ com } P_2 \\ \rightarrow\; & \frac{1}{4}\{-|D_1\rangle + |D_2\rangle + j|C_{12}\rangle + j|C_{21}\rangle \\ & +|D_3\rangle - |D_4\rangle - j|C_{34}\rangle - j|C_{43}\rangle \\ & +j|C_{13}\rangle - j|C_{24}\rangle + |C_{14}\rangle + |C_{23}\rangle \\ & +j|C_{31}\rangle - j|C_{42}\rangle + |C_{32}\rangle + |C_{41}\rangle\} \text{ com } P_2 \end{aligned}$$

A probabilidade de ocorrência (C) e de não ocorrência (NC) de um evento coincidente é obtida a partir do resultado acima, e pode ser quantificada como C=5/8 e NC=3/8.
Após normalização, a probabilidade condicional de ocorrência de determinada coincidência dado que houve um evento coincidente pode ser escrita como:
C_{12}=1/10; C_{13}=1/10; C_{14}=3/10; C_{23}=3/10; C_{24}=1/10; C_{34}=1/10.
Considerando agora apenas as coincidências observáveis quando o detector 1 opera como trigger para os demais, temos a probabilidade de ocorrência de determinado resultado, após normalização:

C_{12}=1/5; C_{13}=1/5; C_{14}=3/5.

XII. $|+45\rangle_{\mathbf{Alice}}$, $|\text{-}45\rangle_{\mathbf{Bob}}$ ⇒ **caso distinguível**

$$P_1|+45^1\rangle_a|-45^2\rangle_b\langle+45^1|_a\langle-45^2|_b + P_2|+45^3\rangle_a|+45^3\rangle_a\langle+45^3|_a\langle+45^3|_a + P_2|-45^4\rangle_b|-45^4\rangle_b\langle-45^4|_b\langle-45^4|_b$$

Observando após o BS, a probabilidade de agrupamento dos fótons no mesmo modo espacial $|\rangle_c$ ou $|\rangle_d$ ou de separação dos fótons (B e NB, respectivamente) será B=1/2 e NB=1/2.

Considerando agora os eventos de detecção:

$$\begin{aligned}
BELL_{|+45\rangle|-45\rangle dist} \rightarrow\ & \frac{1}{4}\{j|D_1\rangle + j|D_2\rangle + |C_{12}\rangle - C_{21} \\
& + j|D_3\rangle + j|D_4\rangle + |C_{34}\rangle - C_{43} \\
& + |C_{13}\rangle + |C_{24}\rangle - j|C_{14}\rangle + j|C_{24}\rangle \\
& - C_{31} - C_{42} + jC_{32} - jC_{41}\} \text{ com } P_1 \\
\rightarrow\ & \frac{1}{4}\{+|D_1\rangle - |D_2\rangle + j|C_{12}\rangle + jC_{21} \\
& - |D_3\rangle + |D_4\rangle - j|C_{34}\rangle - jC_{43} \\
& + j|C_{13}\rangle - j|C_{24}\rangle - |C_{14}\rangle - |C_{32}\rangle \\
& + jC_{31} - jC_{42} - C_{32} - C_{41}\} \text{ com } P_2 \\
\rightarrow\ & \frac{1}{4}\{-|D_1\rangle + |D_2\rangle + j|C_{12}\rangle + j|C_{21}\rangle \\
& + |D_3\rangle - |D_4\rangle - j|C_{34}\rangle - j|C_{43}\rangle \\
& + j|C_{13}\rangle - j|C_{24}\rangle + |C_{14}\rangle + |C_{23}\rangle \\
& + j|C_{31}\rangle - j|C_{42}\rangle + |C_{32}\rangle + |C_{41}\rangle\} \text{ com } P_2
\end{aligned}$$

A probabilidade de ocorrência (C) e de não ocorrência (NC) de um evento coincidente é obtida a partir do resultado acima, e pode ser quantificada como C=3/4 e NC=1/4.

Após normalização, a probabilidade condicional de ocorrência de determinada coincidência dado que houve um evento coincidente pode ser escrita como:

C_{12}=1/6; C_{13}=1/6; C_{14}=1/6; C_{23}=1/6; C_{24}=1/6; C_{34}=1/6.

Considerando agora apenas as coincidências observáveis quando o detector 1 opera como trigger para os demais, temos a probabilidade de ocorrência de determinado resultado, após normalização:

C_{12}=1/3; C_{13}=1/3; C_{14}=1/3.

XIII. $|\text{-}45\rangle_{\mathbf{Alice}}$, $|{+}45\rangle_{\mathbf{Bob}} \Rightarrow$ **caso indistinguível**

$$P_1|-45^1\rangle_a|+45^1\rangle_b\langle-45^1|_a\langle+45^1|_b + P_2|-45^2\rangle_a|-45^2\rangle_a\langle-45^2|_a\langle-45^2|_a \\ +P_2|+45^3\rangle_b|+45^3\rangle_b\langle+45^3|_b\langle+45^3|_b$$

Observando após o BS, a probabilidade de agrupamento dos fótons no mesmo modo espacial $|\rangle_c$ ou $|\rangle_d$ ou de separação dos fótons (B e NB, respectivamente) será B=1/2 e NB=1/2. Considerando agora os eventos de detecção:

$$\begin{aligned} BELL_{|-45\rangle|+45\rangle ind} \;\rightarrow\; & \frac{1}{2\sqrt{2}}\{j|D_1\rangle + j|D_2\rangle + j|D_3\rangle + j|D_4\rangle \\ & +j|C_{14}\rangle - j|C_{24}\rangle - jC_{32} + jC_{41}\} \text{ com } P_1 \\ \rightarrow\; & \frac{1}{4}\{+|D_1\rangle - |D_2\rangle - j|C_{12}\rangle - jC_{21} \\ & -|D_3\rangle + |D_4\rangle + j|C_{34}\rangle + jC_{43} \\ & +j|C_{13}\rangle - j|C_{24}\rangle + |C_{14}\rangle - |C_{23}\rangle \\ & +jC_{31} - jC_{42} + C_{32} + C_{41}\} \text{ com } P_2 \\ \rightarrow\; & \frac{1}{4}\{-|D_1\rangle + |D_2\rangle - j|C_{12}\rangle - j|C_{21}\rangle \\ & +|D_3\rangle - |D_4\rangle + j|C_{34}\rangle + j|C_{43}\rangle \\ & +j|C_{13}\rangle - j|C_{24}\rangle - |C_{14}\rangle - |C_{23}\rangle \\ & +j|C_{31}\rangle - j|C_{42}\rangle - |C_{32}\rangle - |C_{41}\rangle\} \text{ com } P_2 \end{aligned}$$

A probabilidade de ocorrência (C) e de não ocorrência (NC) de um evento coincidente é obtida a partir do resultado acima, e pode ser quantificada como C=5P/8 e NC=3P/8.

Após normalização, a probabilidade condicional de ocorrência de determinada coincidência dado que houve um evento coincidente pode ser escrita como:
C_{12}=1/10; C_{13}=1/10; C_{14}=3/10; C_{23}=3/10; C_{24}=1/10; C_{34}=1/10.

Considerando agora apenas as coincidências observáveis quando o detector 1 opera como trigger para os demais, temos a probabilidade de ocorrência de determinado resultado, após normalização:
C_{12}=1/5; C_{13}=1/5; C_{14}=3/5.

XIV. $|{+}45\rangle_{\mathbf{Alice}}$, $|\text{-}45\rangle_{\mathbf{Bob}} \Rightarrow$ **caso distinguível**

$$P_1|+45^1\rangle_a|-45^2\rangle_b\langle+45^1|_a\langle-45^2|_b + P_2|+45^3\rangle_a|+45^3\rangle_a\langle+45^3|_a\langle+45^3|_a \\ +P_2|-45^4\rangle_b|-45^4\rangle_b\langle-45^4|_b\langle-45^4|_b$$

Observando após o BS, a probabilidade de agrupamento dos fótons no mesmo modo espacial $|\rangle_c$ ou $|\rangle_d$ ou de separação dos fótons (B e NB, respectivamente) será B=1/2 e NB=1/2.

Considerando agora os eventos de detecção:

$$\begin{aligned}
BELL_{|+45\rangle|-45\rangle dist} \rightarrow\ & \frac{1}{4}\{j|D_1\rangle + j|D_2\rangle + |C_{12}\rangle - C_{21} \\
& + j|D_3\rangle + j|D_4\rangle + |C_{34}\rangle - C_{43} \\
& + |C_{13}\rangle + |C_{24}\rangle - j|C_{14}\rangle + j|C_{24}\rangle \\
& - C_{31} - C_{42} + jC_{32} - jC_{41}\} \text{ com } P_1 \\
\rightarrow\ & \frac{1}{4}\{+|D_1\rangle - |D_2\rangle + j|C_{12}\rangle + jC_{21} \\
& - |D_3\rangle + |D_4\rangle - j|C_{34}\rangle - jC_{43} \\
& + j|C_{13}\rangle - j|C_{24}\rangle - |C_{14}\rangle - |C_{24}\rangle \\
& + jC_{31} - jC_{42} - C_{32} - C_{41}\} \text{ com } P_2 \\
\rightarrow\ & \frac{1}{4}\{-|D_1\rangle + |D_2\rangle + j|C_{12}\rangle + j|C_{21}\rangle \\
& + |D_3\rangle - |D_4\rangle - j|C_{34}\rangle - j|C_{43}\rangle \\
& + j|C_{13}\rangle - j|C_{24}\rangle + |C_{14}\rangle + |C_{23}\rangle \\
& + j|C_{31}\rangle - j|C_{42}\rangle + |C_{32}\rangle + |C_{41}\rangle\} \text{ com } P_2
\end{aligned}$$

A probabilidade de ocorrência (C) e de não ocorrência (NC) de um evento coincidente é obtida a partir do resultado acima, e pode ser quantificada como C=3/4 e NC=1/4.

Após normalização, a probabilidade condicional de ocorrência de determinada coincidência dado que houve um evento coincidente pode ser escrita como:
C_{12}=1/6; C_{13}=1/6; C_{14}=1/6; C_{23}=1/6; C_{24}=1/6; C_{34}=1/6.

Considerando agora apenas as coincidências observáveis quando o detector 1 opera como trigger para os demais, temos a probabilidade de ocorrência de determinado resultado, após normalização:
C_{12}=1/3; C_{13}=1/3; C_{14}=1/3.