UNIVERSIDADE FEDERAL DO CEARÁ

CENTRO DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA DE TELEINFORMÁTICA

CURSO DE PÓS-GRADUAÇÃO EM ENGENHARIA DE TELEINFORMÁTICA

EMANOELA DE JESUS LOPES SOARES

GERADORES QUANTO-ÓPTICOS DE NÚMEROS ALEATÓRIOS

FORTALEZA

2013

EMANOELA DE JESUS LOPES SOARES

GERADORES QUANTO-ÓPTICOS DE NÚMEROS ALEATÓRIOS

Dissertação submetida à Coordenação do curso de Pós-graduação em Engenharia de Teleinformática da Universidade Federal do Ceará, como parte dos requisitos exigidos para obtenção do grau de Mestre em Engenharia de Teleinformática.

Orientador: Prof. Dr. Rubens Viana Ramos.

FORTALEZA

2013

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca de Pós-Graduação em Engenharia - BPGE

S653g Soares, Emanoela de Jesus Lopes.
Geradores quanto-ópticos de números aleatórios / Emanoela de Jesus Lopes Soares. – 2013.
53 f.: il. color. enc. ; 30 cm.

Dissertação (Mestrado) – Universidade Federal do Ceará, Centro de Tecnologia, Departamento de Engenharia de Teleinformática, Programa de Pós-Graduação em Engenharia de Teleinformática, Fortaleza, 2013.
Área de Concentração: Eletromagnetismo aplicado
Orientação: Prof. Dr. Rubens Viana Ramos

1. Teleinformática. 2. Dispositivos optoeletrônicos. 3. Detectores. I. Título.

CDD 621.38

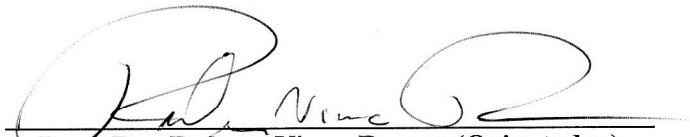
EMANOELA DE JESUS LOPES SOARES

GERADORES QUANTO-ÓPTICOS DE NÚMEROS ALEATÓRIOS

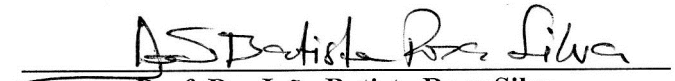
Dissertação submetida à Coordenação do Programa de Pós-Graduação em Engenharia de Teleinformática, da Universidade Federal do Ceará, como requisito parcial para a obtenção do grau de Mestre em Engenharia de Teleinformática.
Área de concentração: Eletromagnetismo Aplicado.

Aprovada em: 22/02/2013.

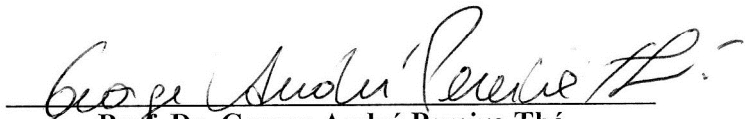
BANCA EXAMINADORA



Prof. Dr. Rubens Viana Ramos (Orientador)
Universidade Federal do Ceará - UFC



Prof. Dr. João Batista Rosa Silva
Universidade Federal do Ceará - UFC



Prof. Dr. George André Pereira Thé
Universidade Federal do Ceará – UFC

Prof. Dr. Fábio Alencar Mendonça
Instituto Federal de Educação, Ciência e Tecnologia do Ceará - IFCE

AGRADECIMENTOS

À FUNCAP pelo apoio financeiro com a manutenção da bolsa de auxílio.

Ao colega e orientador professor Rubens Viana Ramos do departamento de Engenharia de Teleinformática da Universidade Federal do Ceará pelo apoio, dedicação, zelo e paciência.

Aos professores que participaram das disciplinas de mestrado e aos da banca que completaram minha formação.

A Deus por sempre me guiar e iluminar meus passos.

Aos meus pais Antônia e Nonato, que com amor e carinho me educaram e sempre confiaram em meu potencial.

À minha família por me apoiar e incentivar em todos os momentos da minha vida.

Ao meu noivo Júlio por todo o apoio e compreensão nos momentos mais difíceis.

Aos colegas do GIQ: Keuliane, Daniel Barbosa, Daniela, David, Fábio, Fátima, Fernando, Hilma, João Batista, Luzeilton, Paulo Vinicius, Socorro, Paulo Regis, Geovan e Paulo Henrique pelo apoio, companheirismo e troca de conhecimentos.

RESUMO

Geradores quânticos de números aleatórios (GQNA) têm importantes aplicações em protocolos criptográficos, jogos e loterias, entre outros. Em contraste com geradores de números pseudoaleatórios baseados em software, a sequência de números gerada é verdadeiramente aleatória. A maioria dos GQNA encontrados na literatura é baseado em dispositivos optoeletrônicos, como fontes de fótons únicos e detectores de fótons. Nesta direção, a presente dissertação trata da teoria e experimento de GQNAs baseados em sistemas fotônicos, considerando geradores com variáveis discretas e contínuas. Em particular, três problemas foram considerados: 1) um novo modelo de GQNA de variável contínua utilizando a polarização da luz foi proposto. 2) a análise de desempenho de um GQNA usando apenas um detector de fótons, levando em consideração o afterpulsing e o tipo de estado quântico da luz utilizado, coerente ou térmico, foi realizada. 3) um GQNA com distribuição binomial foi construído.

Palavras chave: Geradores quânticos de números aleatórios, detectores de fótons únicos, estados coerente e térmico.

ABSTRACT

Quantum random number generators (QRNG) have important applications in cryptographic protocols, gaming and lotteries, among others. In contrast to pseudo-random number generators based on software, the sequence of random numbers generated is truly random. Most QRNG found in the literature are based on optoelectronic devices like single-photon sources and single-photon detectors. In this direction, the present dissertation deals with the theory and experiment QRNG based photonic systems, taking into account QRNG using discrete and continuous variables. In particular, three issues were considered: 1) a new model of continuous variable QRNG based on light polarization was proposed. 2) The performance of a QRNG employing only one single-photon detector, taking into account the afterpulsing and the quantum light state used, coherent or thermal, was realized. 3) A QRNG with binomial distribution was built.

Keywords: quantum random number generators, single photons detectors, coherent and thermal states.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS

APD Avalanche Photodiode – (Fotodiodo de Avalanche)

V_{APD} Tensão sobre o APD

V_B Tensão de ruptura do APD

N_{EP} Noise Equivalent Power - (Potência de ruído equivalente)

QKD Quantum Key Distribution – (Distribuição Quântica de Chaves)

TTL Transistor – Transistor Logic – (Lógica Transistor – Transistor)

RSA (Rivest, Shamir, Adelman) - Algoritmo de criptografia de dados

NIST National Institute of Standarts and tecnology

PIN Fotodiodo PIN - (Positive-Intrinsic-Negative)

GQNA Gerador quanto-óptico de números aleatórios

GNA Gerador de números aleatórios

GNPA Gerador de número pseudo-aleatório

BS Beam Splitter – (Divisor de feixes)

PBS Polarization Beam Splitter – (Divisor de feixes por polarização)

FPGA Field Programmable Gate Array

SPD Single Photon Detector – (Detector de fótons únicos)

DFI Detector de fótons isolados

SUMÁRIO

INTRODUÇÃO

Geradores de números aleatórios possuem diversas aplicações como, por exemplo, geradores de ruídos em testes de sistemas de comunicações, sorteios, jogos e protocolos de segurança de dados. Esta última, em particular, é fortemente sensível à qualidade do gerador de números aleatórios utilizados. Se a sequência numérica gerada não for realmente aleatória, é possível que a sequência gerada seja utilizada por um adversário para prever os próximos valores da sequência a serem gerados. Isto torna o sistema de segurança de dados vulnerável a ataques. Geradores pseudoaleatórios, implementados por software, são especialmente sensíveis a este tipo de ataque, pois os números da mesma são obtidos através de uma equação algébrica determinística.

Uma solução para este problema é o uso de geradores verdadeiramente aleatórios. Nesta categoria, os geradores baseados em propriedades quânticas, chamados geradores quânticos de números aleatórios (GQNAs), se apresentam como uma solução confiável e barata. Nesta direção, a presente dissertação descreve a teoria de detectores de fótons baseados em dispositivos fotônicos. São considerados geradores com variáveis discretas que utilizam detectores de fótons únicos e geradores com variáveis contínuas que utilizam fotodiodos PIN na detecção. Em particular, três problemas foram considerados: (1) A proposição de um novo GQNA de variável contínua baseado na polarização da luz. (2) A análise de desempenho de um GQNA que usa apenas um detector de fótons e opera com estados coerentes ou térmico. A análise leva em consideração a degradação provocada pelo afterpulsing no detector de fótons. (3) A construção de um GQNA com distribuição binomial.

Esta dissertação está estruturada da seguinte forma: no Capítulo 1 é feita uma revisão de fotodiodo de avalanche e detectores de fótons; no Capítulo 2 é feita uma revisão das propriedades que um bom gerador de números aleatórios deve apresentar; no Capítulo 3 é feita a descrição de alguns tipos de geradores de números aleatórios encontrados na literatura; no Capítulo 4 é apresentada a teoria de um GQNA com variável contínua que utiliza o ruído quântico presente na polarização da luz; no Capítulo 5 é apresentada a análise de desempenho (taxa de geração de números aleatórios) de um GQNA que usa apenas um detector de fótons; no Capítulo 6 são mostrados os resultados experimentais de um GQNA com distribuição binomial. Por fim, o Capítulo 7 traz as conclusões e perspectivas futuras.

1 FOTODIODO DE AVALANCHE E DETECTORES DE FÓTONS

A primeira classe de geradores quânticos de números aleatórios implementados em sistemas fotônicos utiliza alguma variável discreta como a localização ou o tempo de detecção de um fóton. Nestes casos, o principal equipamento é o detector de fótons e o principal elemento deste é o fotodiodo de avalanche.

Assim, o presente capítulo traz uma revisão de detectores de fótons e seu principal componente, o fotodiodo de avalanche.

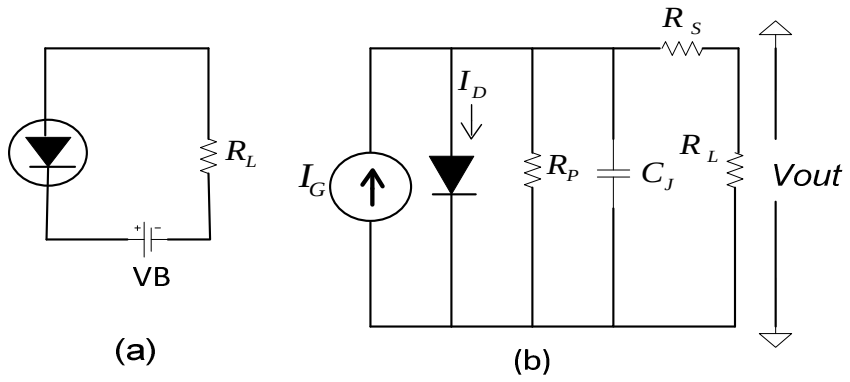
1.1 Fotodiodo de Avalanche

O fotodiodo é um dispositivo de junção p-n que quando polarizado com uma tensão reversa aumenta a sua corrente quando acontece absorção de fótons. A avalanche é uma corrente elétrica de magnitude crescente atravessando o fotodiodo e uma vez iniciada deve ser extinta para não danificar o componente.

O circuito elétrico de forma simplificada do detector de luz está mostrado na Fig. 1a. O circuito equivalente elétrico está esquematizado na Fig. 1b.

A polarização reversa causa fugas superficiais da junção p-n e isto pode ser representado por uma resistência equivalente R_p associada em paralelo com o diodo ideal. O valor dessa resistência depende da qualidade do semicondutor. Pelo projeto de uma junção p-n em cuja região de transição dos cristais são formadas cargas fixas de sinais contrários, fica fácil entender a existência de uma capacitância parasita de junção que influi na limitação da frequência de trabalho do fotodetector. Existe também uma resistência equivalente associada em série com o fotodiodo R_S. Por fim, R_L é a resistência de carga. Na Fig 1b, C_J é a capacitância parasita do fotodiodo, I_D é a corrente através do fotodiodo, V_{out} é o sinal de saída, e a corrente fotogerada é chamada de I_G [1].

Figura 1 - a) Circuito elétrico do detector b) Circuito do detector equivalente elétrico [1].

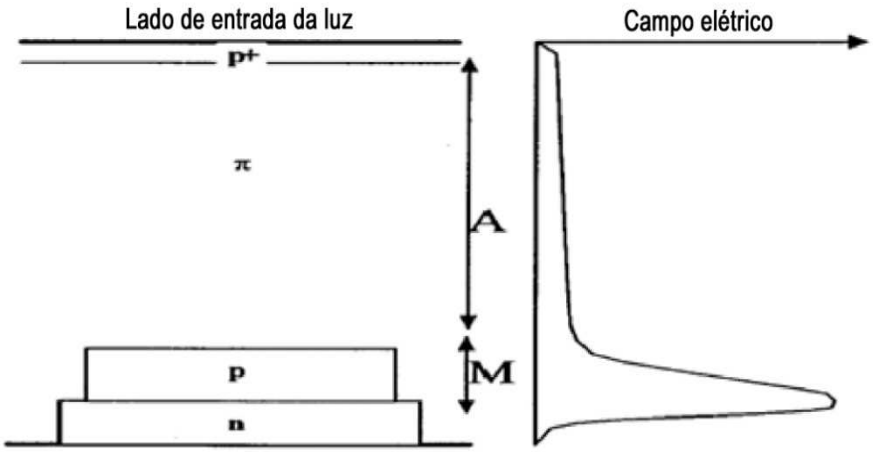


.

O APD é, normalmente, constituído por uma camada fortemente dopada “n”, uma camada levemente dopada “p”, uma camada de material intrínseco (“π”) e uma camada fortemente dopada “p+”. As camadas têm diferentes tipos e intensidades de dopagem, para modificar a distribuição do campo elétrico ao longo do fotodiodo.

Para entender melhor o funcionamento de um APD, considere a Fig. 2[2], na qual as regiões de absorção *A*, e multiplicação, *M*, são destacadas.

Figura 2 - Funcionamento do APD e o perfil do campo elétrico.



Na região *A* os fótons são absorvidos e pares elétron-lacuna são gerados. Devido ao campo elétrico existente na região *A*, os elétrons são levados para a região de multiplicação *M*. Nesta região a alta intensidade do campo elétrico acelera os elétrons que colidem com a rede cristalina e, através da ionização por impacto, podem arrancar outros elétrons. Uma vez que estão livres, estes elétrons podem, pelo mesmo processo, liberar outros elétrons formando um efeito em cascata. Com isso a corrente que flui pelo APD se torna facilmente detectável

mesmo quando apenas um fóton é absorvido pelo APD. A corrente que flui pelo APD é dada por:

$$I_S = MR_0(\lambda)P_S, \tag{1.1}$$

Em (1.1), P_S é a potência luminosa incidente, M é o ganho da região e R_0 é a responsividade dada por $R_0=q\eta/h\lambda$, sendo η a eficiência quântica, λ comprimento de onda, q é a carga do elétron e h constante de Planck. A responsividade é definida pela relação entre a fotocorrente gerada e a potência óptica incidente no fotodiodo. Na região de ganho linear, a fotocorrente gerada cresce linearmente com a potência de luz incidente. O aumento da fotocorrente por efeito de avalanche é descrita por um fator de multiplicação, M_0, que relaciona a fotocorrente multiplicada (I_{pm}) com a fotocorrente sem multiplicação (I_p):

$$M_0 = \frac{I_{pm}}{I_p} = \frac{1}{1-\left(\frac{V_D}{V_B}\right)^{\gamma}}, \tag{1.2}$$

Na equação (1.2), V_D é a tensão aplicada sobre o diodo, V_B é a tensão de ruptura e γé uma constante empírica que depende do material. A tensão de ruptura depende da dopagem dos cristais, da diferença de energia relativa à banda proibida e da temperatura. O valor da tensão de ruptura cresce com o aumento de temperatura, pois aumenta a probabilidade de colisões com a estrutura cristalina e o percurso no qual as partículas são aceleradas diminui de tamanho, logo eles não conseguem acumular energia cinética suficiente para causar uma ionização por impacto. Assim, uma maior tensão aplicada faz-se necessária.

No APD existem dois tipos de ruídos: o ruído *shot* e o ruído devido à formação da avalanche. O ruído shot depende da estatística poissoniana do número de elétrons que formam a corrente, pois o número de fótons incidentes em um fotodetector para um determinado intervalo de tempo é aleatório [3]. O ruído devido ao processo de formação de avalanche é modelado pelo fator de excesso de ruído F. O valor de F depende da dopagem, do ganho M_0 e do campo elétrico. O valor médio quadrático da corrente total de ruído do APD na ausência de luz é dado por [2]:

$$\langle i_n \rangle^2 = 2q\left(I_{DS} + I_{DB}M^2F\right)B, \tag{1.3}$$

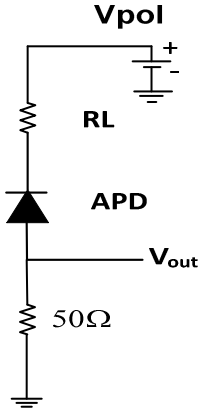
Em (1.3), I_{DS} é a componente de fuga superficial, I_{DB} é a corrente de fuga pelo interior do componente e B é a largura de banda do sistema. Na presença de luz o valor médio quadrático da corrente total de ruído é [2]:

$$\langle i_n \rangle^2 = 2q[I_{DS} + \left(I_{DB}M^2 + R_0(\lambda)M^2P_S\right)F]B. \tag{1.4}$$

1.1.1 Extinção Passiva, Ativa e Engatilhada

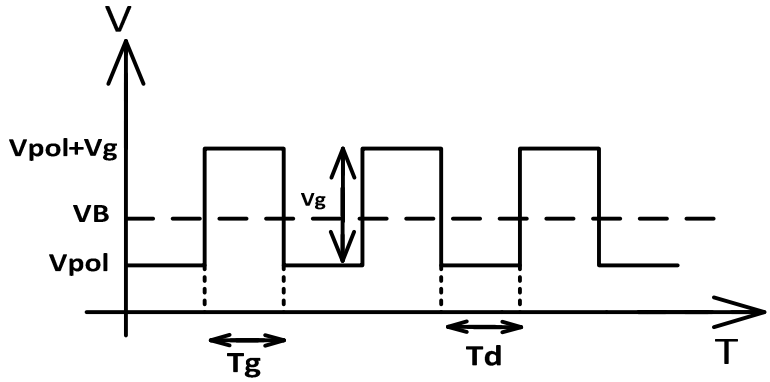
Uma vez iniciada a avalanche a mesma deve ser extinta para que o APD não se danifique devido ao alto valor de corrente que por ele circula. Há três tipos básicos de circuitos de extinção de avalanche utilizados em detectores de fótons: passiva, ativa e engatilhada. A Fig. 3 ilustra o circuito de extinção passiva em que a avalanche se extingue naturalmente através da queda de tensão em um resistor de valor elevado [4]. Como o resistor R_L possui valor elevado, a tensão sobre ele se eleva reduzindo a polarização sobre o APD, o que provoca a extinção da avalanche quando $V_{APD} \leq V_B$.

Figura 3 - Circuitos de polarização no modo passivo.



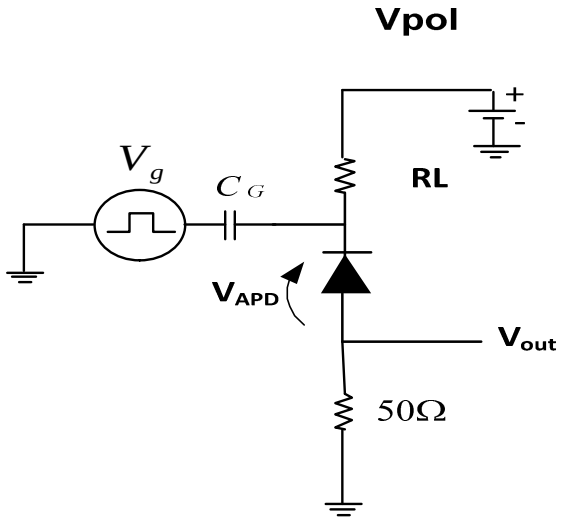
Para melhor compreensão do modo engatilhado é apresentado um trem de pulsos de gatilho na Fig. 4 que mostra a tensão V aplicada ao APD no modo de operação engatilhado. V_{pol} é a tensão de polarização DC aplicada abaixo da tensão de ruptura V_B, o pulso de gatilho tem amplitude V_g. A tensão V_{pol} é somada a V_g formando a tensão total sobre o APD (V_{APD}) com o objetivo de ultrapassar a tensão de ruptura. Quando V_{APD} excede V_B temos a tensão de excesso V_e dada por V_e=V_{APD}-V_B. Além disso, T_g é a duração do pulso de gatilho e T_d é o tempo de desuso entre os pulsos de gatilho.

Figura 4 - Modo de operação com trem de pulsos de gatilho.



No modo de extinção ativa, assim que uma avalanche se inicia, a tensão de saída é detectada por um circuito eletrônico que realimenta o circuito de polarização, fazendo com que a tensão de polarização do APD se reduza a um valor abaixo da tensão de ruptura. Após um período de tempo determinado, a polarização do fotodiodo retorna a seu valor inicial, próximo da tensão de avalanche. No modo engatilhado ou Geiger, o dispositivo tem um processo de avalanche restrito ao tempo de duração do pulso de gatilho. O circuito de extinção engatilhada é mostrado na Fig. 5 e C_G é um capacitor de acoplamento que une o pulso de gatilho ao circuito e tal que a reatância seja pequena na frequência da fonte de gatilho e impeça a fuga de corrente da fonte de polarização para o gerador de pulsos [4].

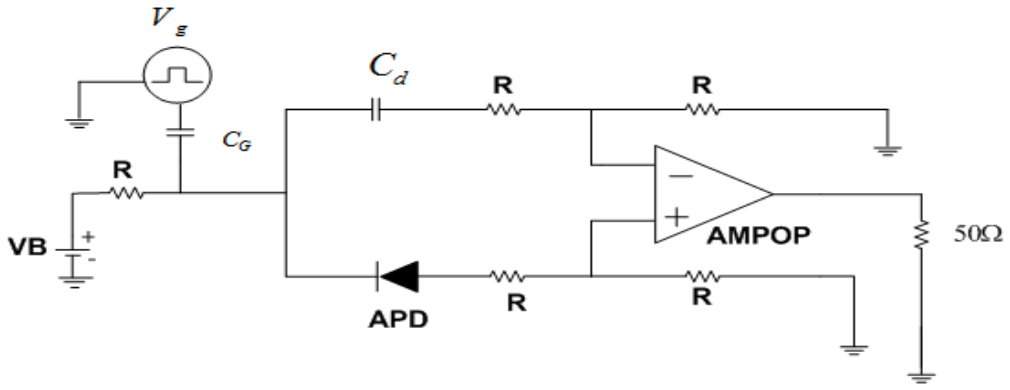
Figura 5 - Circuitos de polarização modo engatilhado.



1.1.2 Circuito Subtrator

Todo diodo semicondutor apresenta uma capacitância interna resultante da separação de cargas na barreira de potencial da camada de depleção formada na região de contato entre os semicondutores com diferentes dopagens. Quando o APD opera no modo Geiger, esta capacitância deriva os pulsos de gatilho, gerando um sinal espúrio nas transições de subida e de descida do pulso, que podem dificultar a detecção ou mesmo mascarar a contagem de fótons. Para amenizar este problema, se utiliza um circuito subtrator que compensa esta capacitância [4]. Neste caso, parte do pulso de gatilho segue para um capacitor com capacitância equivalente à do fotodiodo C_d, como na Fig. 6.

Figura 6 - Circuito de compensação de capacitância no modo Geiger.



Para o ajuste correto dos parâmetros do APD, deve-se levar em consideração a temperatura, a tensão do pulso de gatilho, a tensão de polarização, a taxa de repetição de gatilho e sua largura temporal. Todos estes parâmetros influenciam na probabilidade do fotodiodo gerar uma avalanche na presença e na ausência de fótons.

Uma característica importante do APD é a eficiência quântica η que se refere à probabilidade de um fóton ser internamente absorvido, gerar um par elétron-lacuna, e esses portadores desencadearem uma avalanche. Esse parâmetro é influenciado pela tensão de excesso, de modo que, aumentando esse valor, a eficiência também aumenta. Os elétrons que contribuem para a fotocorrente são provenientes de vários locais, alguns são gerados dentro da região de carga e logo são separados pelo campo elétrico resultante da barreira de potencial e da polarização reversa, outros são originários fora dessa região, mas dentro do percurso de difusão dos portadores. Aqueles portadores que estiveram fora do percurso de difusão desaparecem rapidamente e não contribuem para o aumento da fotocorrente. Em resumo, a

eficiência quântica relaciona o número de elétrons liberados por unidade de tempo com a quantidade de fótons que penetra no material por unidade de tempo.

O fotodiodo de avalanche deve ser resfriado devido à sua alta sensibilidade à geração térmica de pares elétron-lacuna. Os portadores (elétrons) gerados por excitação térmica contribuem para aumentar a taxa de avalanches ilegítimas, caracterizando assim o ruído de escuro. Outro efeito que contribui para avalanches espúrias é a ocorrência dos chamados *afterpulses*, ou pós-pulsos. Este efeito resulta de elétrons que ficaram presos em armadilhas durante o processo de avalanche e não conseguiram ser removidos pelo campo elétrico do dispositivo em tempo. Ao liberarem-se tardiamente, acabam desencadeando uma nova avalanche mesmo na ausência de fótons [5].

Os portadores presos possuem um tempo de vida finito τv, portanto pode-se evitar o afterpulsing fazendo-se o tempo entre os pulsos de gatilho T_d maior que τv. Assim, a máxima frequência de gatilho, f_g, na qual o afterpulsing é irrelevante é dada por [6]:

$$f_g = \frac{1}{(T_g + T_d)} < \frac{1}{\tau v}. \tag{1.5}$$

Portanto, para a redução do afterpulsing é necessário usar uma baixa frequência de pulsos de gatilho, de forma que os portadores aprisionados possam se libertar entre dois pulsos de gatilho. Logo, o afterpulsing limita a taxa de recebimento de fótons limitando, portanto, a velocidade de comunicação.

No processo de caracterização dos fotodiodos de avalanche, uma figura de mérito utilizada é o NEP, potência de ruído equivalente, e é definida como a potência radiante que produz uma relação sinal-corrente de escuro igual a 1. O NEP é calculado pela relação:

$$NEP = \frac{h\nu\sqrt{2R_d}}{\eta}, \tag{1.6}$$

Sendo R_d a taxa de contagem de escuro [5].

A escolha do tipo de APD varia conforme o comprimento de onda da região de operação. Os APDs de Ge e InGaAs são muito inferiores em seu desempenho em relação aos de Si, porém o comprimento de onda de operação para os APDs de Si corresponde à primeira

janela de transmissão das fibras ópticas cujo comprimento de onda é de 850nm. Nessa região a fibra óptica possui atenuação elevada de aproximadamente 2 dB/km, o que limita a distância entre emissor e receptor em sistemas de comunicações que utilizem luz de um fóton ou estados coerentes fortemente atenuados, como distribuição quântica de chaves. Na terceira janela óptica, em 1550 nm, a única opção é InGaAs. Nessa região a atenuação da fibra óptica é de apenas 0,25 dB/km [7].

1.2 Ruídos no APD e no Detector de fótons únicos

As contagens de escuro surgem a partir da geração de portadores nos fotodiodos por qualquer razão que não a absorção de fótons [8]. As contribuições para as contagens de escuro são: afterpulsing, portadores gerados termicamente e portadores gerados por processos de tunelamento. A geração de elétrons por excitação térmica aumenta a taxa de avalanches indesejáveis, o que pode causar erros em um sistema de comunicações que utilize detectores de fótons. Quanto maior a temperatura do fotodetector, menor é a força de ligação dos elétrons de valência nos átomos e, portanto, maior a probabilidade de um elétron ir para a banda de condução e causar uma avalanche [5]. A forma de diminuir a contagem de escuros é resfriar o APD. Isto evita a geração térmica de portadores de carga, mas não influencia nas avalanches causadas por tunelamento, uma vez que estas independem da temperatura.

Idealmente, o fotodetector responde a um fluxo de fótons gerando uma corrente elétrica proporcional. O dispositivo gera uma corrente cujo valor flutua em torno de sua média. Essas flutuações aleatórias são consequências dos ruídos. Algumas fontes de ruídos são inerentes ao processo de detecção do fóton [9]:

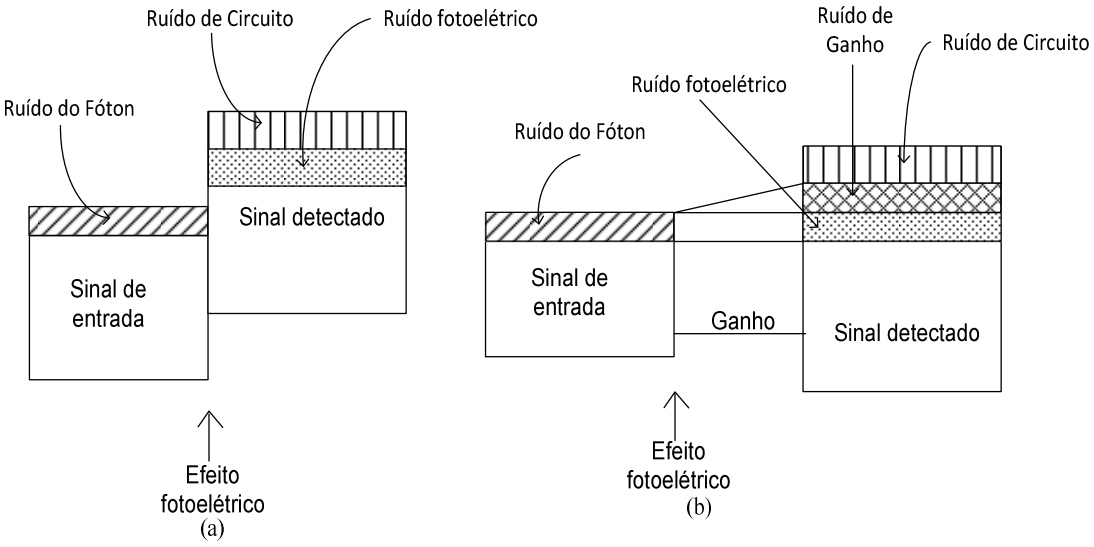
- Ruído do fóton: A principal fonte de ruído está associada ao número aleatório de fótons que chegam.
- Ruído foto-eletrônico: Considerando um detector com eficiência quântica menor que 1, um simples fóton gera um par elétron-lacuna com probabilidade η, porém existe a probabilidade de falha 1-η. Por causa dessa aleatoriedade do processo de geração dos portadores, uma fonte de ruído passa a existir.
- Ruído de ganho: O processo de amplificação que fornece ganho interno em fotodetectores como os APDs é aleatório. Cada fóton detectado gera um número

aleatório de portadores com um valor médio, mas com uma incerteza que é dependente da natureza do processo de amplificação.

- Ruído do circuito receptor: Ruído formado por vários componentes do circuito elétrico de um receptor óptico, como resistores e transistores.

A Fig. 7 ilustra as fontes de ruídos descritas acima:

Figura 7 - Sinal e fonte de ruído para (a) fotodetector sem ganho e (b) fotodetector com ganho [9].



2 PROPRIEDADES DE UM BOM GERADOR DE NÚMEROS ALEATÓRIOS

Mais apropriado que falar de números aleatórios é falar de sequências aleatórias. Para que uma sequência seja considerada aleatória ela deve ser testada por métodos estatísticos. Não há um limite de testes que possam ser aplicados, e a cada novo teste o grau de confiança no gerador aumenta. Os testes são divididos em duas classes: empíricos e teóricos [10].

Testes teóricos: Envolvem cálculos matemáticos para as propriedades estabelecidas pelo teste. São específicos para cada classe de geradores e se concentra na estrutura intrínseca de cada gerador para derivar características de comportamento da sequência de números, particularmente ao longo de todo um período. Indicam a qualidade de um gerador de acordo com algum critério matemático sem exigir geração de números.

Testes empíricos: Não se preocupam com a origem dos números apenas com os resultados, utilizam como base sequências geradas, verificando se suas propriedades são coerentes com o probabilisticamente esperado de uma distribuição aleatória.

Nenhuma bateria de testes garante qualidade de um gerador, mas quanto mais testes forem realizados com sucesso mais aumenta a confiança no gerador. O grau de certeza estatística depende do mecanismo de teste e do número de valores testados que compõem a sequência.

O processo de construção de geradores de números aleatórios deve obedecer às restrições de velocidade e cobertura do intervalo de geração. Um dos testes estatísticos mais básicos é o método Chi-quadrado que faz conexão com outros testes e permite comparar os valores obtidos através do gerador com os que seriam determinados pela curva real da função.

A ideia de sequência independente é que cada valor desta deveria ser obtido ao acaso, sem ter qualquer relação com seus antecessores ou os próximos na mesma sequência. Caso isso não seja possível, precisamos ao menos que a sequência se comporte de forma a parecer ter sido obtida ao acaso. A correlação entre números sucessivos deve ser pequena e se a mesma for significante, indica que há dependência entre os números sucessivos.

Cada teste efetuado em uma sequência indica que a mesma, aparentemente, apresenta ou não determinada característica esperada. O grau de certeza estatística depende do mecanismo de teste e do número de valores testados que compõem a sequência. Assim, nas seguintes seções são feitas revisões das propriedades de um bom gerador de números aleatórios.

2.1 Definições Formais

Esta seção descreve algumas das principais características importantes na geração de bits aleatórios. Os termos mais comuns utilizados para experimento com números aleatórios estão descritos a seguir:

- Aleatoriedade: Um número aleatório é aquele que pertence a uma série numérica e que não pode ser previsto a partir dos membros anteriores da série [10].

- Gerador de bits aleatórios: É um aparelho capaz de gerar uma sequência estatisticamente independente e não tendenciosa de dígitos binários (uns e zeros). Um gerador deste tipo é chamado criptograficamente de seguro se não houver algoritmo em tempo hábil de prever o próximo bit. O objetivo dos geradores de números aleatórios é realizar fisicamente o conceito matemático de variáveis aleatórias e sua construção deve ser baseada em uma sólida análise matemática de suas propriedades estruturais.

- GQNA: Significa gerador quântico de número aleatório e usa fontes não determinísticas (fontes de entropia) para a produção de aleatoriedade. A fonte de entropia consiste de algum efeito quântico ou variável quântica [11]. Este gerador produz sequências aleatórias imprevisíveis, por isso é chamado de verdadeiro GNA.

- GNPA: Significa gerador de número pseudoaleatório usa uma ou mais entradas e gera vários "pseudo" números aleatórios. Insumos para GNPAs são chamados de sementes que devem ser aleatórias e imprevisíveis. Assim, um GNPA deve obter suas sementes a partir das saídas de um GNA [11]. Um GNPA pode ser prontamente gerado no computador por meio de algoritmos deterministas com poucos parâmetros de entrada [12]. Este tipo de GNA é chamado de falso, pois as sequências formadas podem ser previsíveis. Tecnicamente falando, sendo o computador uma máquina de aritmética finita e discreta, é virtualmente impossível gerar números verdadeiramente aleatórios. Logo, o que se faz na prática é escolher um algoritmo determinístico que gere uma sequência de números de aparência aleatória, e cujo período desta seja grande o suficiente, essas sequências geradas por computador digital são chamadas pseudoaleatórias.

2.2 Aplicações de um Gerador de Números Aleatórios

Os geradores de números aleatórios são usados em várias aplicações como [13]:

- Simulação computacional: É a recriação de um fenômeno complexo. Números aleatórios são usados, por exemplo, para simular fenômenos naturais, na física nuclear, pesquisas de operações de pessoas como, por exemplo, a chegada de pessoas em intervalos aleatórios.

- Jogos de azar: A aleatoriedade é essencial para jogos de azar e vital para a indústria de jogos, incluindo jogos online.

- Protocolos de criptografia clássicos e quânticos: Criptografia é a ciência de escrever em códigos, que permite tornar incompreensível uma mensagem originalmente escrita com clareza, de forma que somente o destinatário a decifre e a compreenda. O objetivo principal da distribuição quântica de chaves é a geração de difíceis sequências para estabelecer uma comunicação segura entre dois usuários de um sistema de comunicações. Seu uso está em várias aplicações como: comércio eletrônico, comunicação pessoal, transmissão de dados por computador.

- Amostragem: Muitas vezes não é possível analisar todos os casos possíveis, mas uma amostra aleatória fornece a ideia do que seria o comportamento típico.

Comunicações seguras em redes dependem de tecnologias de criptografia que, por sua vez, requerem o uso de geradores aleatórios capazes de produzir essencialmente sequências de bits imprevisíveis. Uso mais comum em criptografia clássica:

- Chaves de sessão e mensagem para cifras simétricas;
- Sementes para rotinas que geram valores matemáticos (grandes números primos para RSA);
- Saltos para combinação com senhas;
- Valor para instâncias específicas de esquemas de assinatura digital [14].

2.3 Geradores Baseados em Processos Físicos

São geradores baseados na natureza probabilística de processos físicos intrinsecamente aleatórios, por exemplo, ruído térmico em resistores, emissão ou detecção de um fóton, dentre outros.

Um gerador deste tipo é realmente imprevisível e aleatório, mas seu resultado não pode ser diretamente utilizado, pois a distribuição nem sempre é uniforme, e fenômenos naturais podem produzir bits tendenciosos ou correlacionados.

Um dos maiores problemas é que um gerador físico está sujeito a desgaste e envelhecimento, especialmente quando é construído a partir de circuitos eletrônicos.

2.4 Recomendações

Para analisar corretamente uma sequência de números aleatórios com um teste é necessário ter cuidado sobre como esta deve esperar receber os valores a serem testados. A maior parte dos testes espera uma sequência de bits, não um valor inteiro, ou real entre zero e um. Possivelmente, esperam uma distribuição uniforme de bits, em algum formato especifico de arquivo. Os testes não devem ser executados em uma mesma sequência, mas em sequências distintas geradas pelo mesmo gerador, o que garante que são resultados independentes. Quanto ao tamanho da amostra, cada teste possui uma recomendação. E em relação ao critério de aprovação, este depende de um nível de significância. O nível recomendado pelo NIST é de 0,01% [11].

2.5 Qualidade de Números Aleatórios

Não existe uma bateria de testes ou mesmo um teste único capaz de provar, a partir de uma sequência de números, qualquer característica. Os testes são evidências estatísticas que indicam que a sequência parece se comportar de acordo com uma determinada propriedade, com certo grau de certeza [13].

Dentro de tanta incerteza e imprevisibilidade, e devido à importância de números aleatórios em tantos campos diferentes, é natural que haja uma busca prolongada por métodos capazes de testar e validar um gerador.

Os testes ajudam a detectar certos tipos de deficiências que o gerador pode ter. Isto é conseguido com uma amostra da sequência de saída e submetendo a vários testes

para avaliar se a sequência possui determinado atributo que a faz verdadeiramente aleatória. Há dois tipos de propriedades que podem ser testadas: as estáticas (tem a ver com valores, independente da ordem em que eles são gerados) e dinâmicas (que levam em conta padrões ou relações de ocorrência). Um teste que verificasse, em uma sequência, a quantidade de cada possível valor retornado, verificaria uma qualidade estática (mesmo número de ocorrências de cada elemento), enquanto que uma verificação de padrões de ocorrência estaria validando as propriedades dinâmicas [15].

2.6 Falhas em Testes Estatísticos

As falhas em testes estatísticos acontecem em duas categorias gerais:

- Proporcionais: ocorre quando um gerador falha em um teste com muita frequência.
- Uniformidade: quando um gerador falha de forma inconsistente. Algumas vezes ele pode ter resultados maravilhosos, e apresentar em outros momentos resultados péssimos [13].

Mesmo geradores bons eventualmente falham. A partir de certo percentual de falhas a confiabilidade é prejudicada. As informações seguintes são uma lista de possíveis explicações para detalhar porque um conjunto de dados falhou em um teste estatístico [11]:

a) Um teste estatístico incorretamente programado.

b) Um teste estatístico (imaturo) subdesenvolvido: Há ocasiões em que tanto a teoria da probabilidade ou a complexidade não está suficientemente desenvolvida ou compreendida para facilitar uma análise rigorosa de um teste estatístico.

c) Uma implementação inadequada de um gerador de números aleatórios: Pode ser que um GNA na parte hardware ou software falhe devido a um defeito no projeto ou a um erro de implementação de codificação.

d) Opções incorretas para parâmetros de entrada: Considerações devem ser feitas muitas vezes em relação à entrada de experimentação numérica. Parâmetros, a saber: comprimento da sequência, tamanho da amostra, tamanho do bloco e modelo.

2.7 Confiabilidade de um Gerador

Os requisitos para avaliação de um algoritmo quanto a seu uso em criptografia se dividem em duas categorias: os requisitos estatísticos: (sequência passa nos testes estatísticos) e a resistência a ataques: (mesmo sendo conhecido o algoritmo usado e os valores ou parte das variáveis de estado do gerador, não deve ser possível reconstituir a sequência). Caso haja uma fonte de entropia em uso, mesmo com toda a entrada conhecida, não deve ser possível adivinhar o próximo valor. Um bom gerador deve passar nos testes para uniformidade e independência da sequência produzida e o tempo deve ser otimizado para garantir a eficiência do gerador [16].

2.8 Testes de Geração de Números Aleatórios

O NIST é um pacote estatístico composto de 15 testes que foram desenvolvidos para testar a aleatoriedade das sequências binárias produzidas por hardware ou software. Abaixo está representada uma tabela com o nome dos 15 testes e o parâmetro e avaliação de cada um.

Tabela 1 - Resumo do pacote estatístico NIST.

Teste	Parâmetro detectado
Frequência (Monobit)	Zeros e uns igualmente
Frequência de um bloco	Zeros e uns igualmente
Teste de Corrida	Oscilação de zeros igualmente rápida ou lenta
Maior Corrida de uns dentro de um bloco	Oscilação de zeros igualmente rápida ou lenta
Posto da matriz binária	Desvio de distribuição de posto esperado
Espectral da transformada discreta de Fourier	Padrões repetitivos
Casamento de padrão sem superposição	Ocorrências irregulares de um modelo pré-especificado
Casamento de padrão com superposição	Ocorrências irregulares de um modelo pré-especificado
Estatística universal de Maurer	Incompressibilidade da sequência
Complexidade Linear	Registrador de deslocamento de realimentação linear
Serial	Não-uniformidade na distribuição conjunta para sequências de comprimento *m.*

Continua

Tabela 1 - Resumo do pacote estatístico NIST

Teste	Parâmetro detectado
Entropia aproximada	Não-uniformidade na distribuição conjunta para sequências de comprimento *m*
Somas cumulativas	Muitos zeros e uns igualmente em fase precoce ou tardia da sequência
Excursões aleatórias	Desvio da distribuição do número de visitas de um passeio aleatório para um determinado estado
Variantes de excursão aleatória	Desvio da distribuição do número de visitas (em muitos passeios aleatórios) para um determinado estado

Fonte: [11].

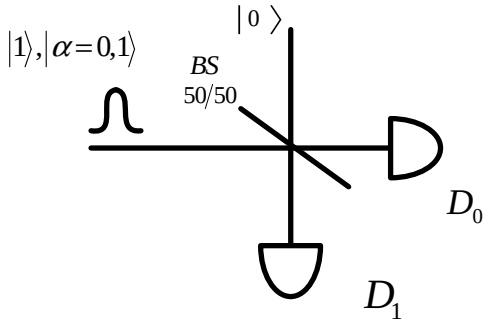
3 MODELOS DE GERADORES QUANTO-ÓPTICOS DE NÚMEROS ALEATÓRIOS

Nesta seção são descritos modelos de geradores quanto-ópticos de números aleatórios e é discutida a influência dos parâmetros dos detectores na sequência aleatória gerada. Os geradores quanto-ópticos de números aleatórios podem ser construídos com variável aleatória discreta ou contínua. No caso da variável aleatória discreta, normalmente o processo de medição do sistema quântico resulta em dois valores possíveis; um destes valores representa o bit lógico ‘0’ e o outro valor o bit lógico ‘1’. No caso variável contínua, os possíveis resultados da medição formam uma faixa contínua de valores. Esta faixa é dividida em trechos menores e o valor do bit ou sequência binária obtida depende de qual trecho o resultado da medição se situa.

3.1 Geradores Quanto-Ópticos de Números Aleatórios Com Variável Discreta

O GQNA mais simples é o mostrado na Fig. 8 [17].

Figura 8 - GQNA utilizando como entrada o estado número $|1\rangle$ ou um estado coerente com baixo número médio de fótons.



Na Fig. 8 um divisor de feixes balanceado (reflectância igual à transmitância) é utilizado. Em cada porta de saída do divisor de feixes um detector de fótons é colocado. Quando um fóton incide no divisor (ideal), ele tem 50% de chance de ser refletido (e detectado em D_1, o que representa o bit ‘1’), e 50% de chance de ser transmitido (e detectado em D_0, o que representa o bit ‘0’). Quando o estado na entrada do divisor é $|1\rangle|0\rangle$ tem-se na saída do divisor $U_B|1\rangle|0\rangle=(|1\rangle|0\rangle+|0\rangle|1\rangle)/2^{1/2}$, sendo U_B a operação unitária que caracteriza o divisor de feixes balanceado. Neste caso, as probabilidades de detecção em D_0 e D_1 são, respectivamente, dadas por:

$$p_0^{|1\rangle} = [1-(1-\eta_0/2)(1-p_{D0})], \tag{3.1}$$

$$p_1^{|1\rangle} = [1-(1-\eta_1/2)(1-p_{D1})], \tag{3.2}$$

Nas equações (3.1)-(3.2), η_0 e η_1 são, respectivamente, as eficiências quânticas dos detectores D_0 e D_1, enquanto que P_{D0} e P_{D1} são, respectivamente, as probabilidades de contagem de escuro, dos detectores D_0 e D_1. A probabilidade de geração de um bit aleatório, por pulso óptico emitido, é dada por:

$$P_B^{|1\rangle} = p_0^{|1\rangle}(1-p_1^{|1\rangle}) + (1-p_0^{|1\rangle})p_1^{|1\rangle}. \tag{3.3}$$

Por outro lado, se o estado total na entrada do divisor for o estado coerente $|\alpha\rangle|0\rangle$, o estado na saída será $U_B|\alpha\rangle|0\rangle = |\alpha/2^{1/2}\rangle|i\alpha/2^{1/2}\rangle$ e as probabilidades de detecção em D_0 e D_1 são, respectivamente:

$$p_0^{|\alpha\rangle} = 1-e^{-\eta_0\frac{|\alpha|^2}{2}}(1-p_{D0}) \tag{3.4}$$

$$p_1^{|\alpha\rangle} = 1-e^{-\eta_1\frac{|\alpha|^2}{2}}(1-p_{D1}). \tag{3.5}$$

Neste caso, a probabilidade de geração de um bit aleatório é dada por:

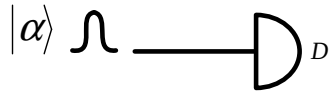
$$P_B^{|\alpha\rangle} = p_0^{|\alpha\rangle}(1-p_1^{|\alpha\rangle}) + (1-p_0^{|\alpha\rangle})p_1^{|\alpha\rangle}. \tag{3.6}$$

Toda vez que não houver detecção ou houver detecção nos dois detectores, o resultado é descartado. Desta forma, nos sistemas reais a taxa de geração de bits aleatórios é sempre inferior à taxa de chegada dos pulsos ópticos. Ausência de detecções pode ocorrer devido à baixa eficiência (< 1) dos detectores, absorção de fótons pelo divisor de feixes ou ausência de fótons no pulso quando o estado coerente for utilizado. Por outro lado, detecções simultâneas em D_0 e D_1 podem ocorrer devido às contagens de escuro ou quando houver mais de um fóton por pulso, o que pode ocorrer quando o estado coerente é utilizado. Se as fontes de estados número e coerente operam com a mesma taxa de geração de pulsos luminosos, então $P_B^{|1\rangle} > P_B^{|\alpha\rangle}$. Além disso, para que a sequência de bits obtida não seja polarizada, ou seja,

para que $p_0 = p_1$, os detectores devem ser iguais (mesmos valores de eficiência quântica e de probabilidades de contagem de escuro e de afterpulsing) e o divisor de feixes deve ser realmente balanceado. Como na prática isto não ocorre, deve-se processar a sequência binária obtida para que a mesma se torne despolarizada.

Uma forma de evitar a polarização da sequência binária obtida e o pós-processamento para correção desta, consiste em construir um GQNA que utilize apenas um detector de fótons, como mostrado na Fig. 9.

Figura 9 - GQNA com detecção de estado coerente.



Basicamente, no esquema da Fig. 9 há apenas uma fonte que gera estados coerentes e um detector de fótons. Quando um estado coerente com número médio de fótons $|\alpha|^2$ incide em um detector de fótons de limiar, a probabilidade de haver uma avalanche (desconsiderando as contagens pós-pulsos) é dada por:

$$p = 1 - e^{-\eta|\alpha|^2}\left(1 - p_D\right). \tag{3.7}$$

Neste caso, há três possibilidades de obter uma sequência binária aleatória. Na primeira, a variável aleatória utilizada é a ocorrência ou não de uma avalanche [18]. Para cada pulso óptico incidente no detector *D*, se ocorrer uma avalanche o bit 1 é obtido, caso contrário, o bit 0 é obtido. Para que a sequência gerada fique despolarizada, o número médio de fótons do pulso incidente é aumentado até que $p = 0{,}5$, ou seja,

$$|\alpha|^2 = \frac{1}{\eta}\ln\left(\frac{0{,}5}{1 - p_D}\right). \tag{3.8}$$

Nesta configuração, a taxa de produção de bits aleatórios é igual à taxa de geração dos pulsos ópticos, ou seja, para cada pulso óptico enviado ao detector um bit aleatório é obtido. Na prática ocorre que, sendo o número médio de fótons mais elevado, a corrente produzida na avalanche será maior o que aumenta a probabilidade de uma contagem pós-pulso. Esta claramente polariza a sequência binária através do aumento da quantidade de bits

‘1’. Para evitar este efeito a taxa de geração de pulsos ópticos deve ser reduzida, o que também diminuirá a taxa de geração de bits aleatórios, ou deve-se utilizar um circuito eletrônico que cesse a avalanche muito rapidamente, o que não é uma tarefa muito simples.

A segunda possibilidade para o esquema da Fig. 9 é utilizar o estado coerente com número médio de fótons 0,1 e usar o intervalo de tempo τ entre duas detecções (número de pulsos de gatilho) como variável aleatória [19] [20]. A distribuição de probabilidade de τ assume valores maiores para tempo mais curtos e valores menores para tempos mais longos. Desta forma, é possível encontrar um valor de tempo de referência τ_{ref} tal que $\tau \leq \tau_{ref}$ implica em bit 0, caso contrário bit 1. Neste caso, a taxa média de geração de bits aleatórios é $1/\tau_{ref}$.

A terceira possibilidade consiste em também utilizar o estado coerente com número médio de fótons 0,1 e contar a paridade dos pulsos de gatilho quando houver detecção. Se uma detecção ocorrer em um pulso de gatilho par, um bit ‘0’ é registrado, caso contrário o bit ‘1’ é obtido [21].

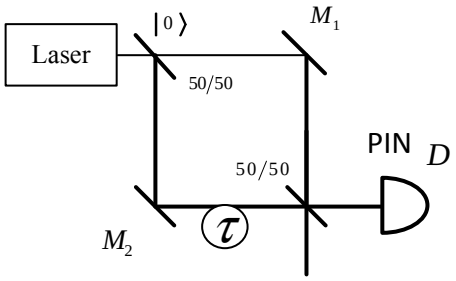
Embora estes dois últimos esquemas utilizando apenas um detector apresentem um menor custo e menor polarização da sequência binária produzida, os mesmos problemas de velocidade de operação devido à baixa eficiência e à probabilidade de contagem pós-pulso dos detectores de fótons permanecem.

3.2 Geradores Quanto-Ópticos de Números Aleatórios Com Variável Contínua

Os GQNAs com variável discreta têm como principal desvantagem o fato da velocidade de operação (número de bits aleatórios gerados por segundo) ser fortemente dependente do desempenho dos detectores de fótons. Com a atual tecnologia de desenvolvimento de fotodiodos de avalanche e de fontes de fótons únicos, a máxima velocidade de GQNAs com detectores de fótons é de poucas dezenas de Mbits/s.

Para um GQNA atingir a velocidade de Gbits/s, faz-se o uso de uma variável quântica contínua. O primeiro GQNA com variável contínua é mostrado na Fig. 10 [22].

Figura 10 - GQNA com variável contínua.



A fonte de ruído utilizada é o ruído de fase devido às emissões espontâneas no laser semicondutor. O interferômetro de Mach-Zenhder transforma este ruído de fase em ruído de amplitude. Na Fig. 10, o tempo de atraso τ deve ser maior que o tempo de coerência da fonte de luz. Neste caso, a fase relativa entre o campo gerado pelo laser e a versão dele atrasada de τ vai variar aleatoriamente. Desta forma, a quantidade de luz entregue ao detector óptico baseado em fotodiodos PIN também vai variar aleatoriamente.

Basicamente, o campo elétrico produzido pelo laser é descrito pela equação:

$$E(t) = E_0 \exp\left[i\left(\omega t + \theta(t)\right)\right], \tag{3.9}$$

Sendo E_0 a amplitude (considerada constante), ω é a frequência angular e $\theta(t)$ representa a flutuação de fase da luz emitida pelo laser. Após a passagem pelo interferômetro de Mach-Zehnder com diferença de fase entre os braços de $2k\pi+\pi/2$ (k inteiro), a corrente que flui no fotodiodo é definida por:

$$i(t) \propto P\text{sen}\left[\theta(t)-\theta(t+\tau)\right] \propto P\left[\theta(t)-\theta(t+\tau)\right] \equiv P\Delta\theta(t), \tag{3.10}$$

Sendo P a potência óptica emitida pelo laser. Adicionalmente, $\Delta\theta(t)$ pode ser considerado pequeno o suficiente tal que a senóide possa ser aproximada pelo seu argumento.

Como em qualquer gerador de números aleatórios baseado em sistemas físicos, junto ao ruído quântico há um ruído clássico na fase. Os ruídos clássicos dominantes neste caso são a flutuação na ocupação de estados nas bandas de valência e de condução [23] e o ruído $1/f$ [24]. Estes dois ruídos clássicos são independentes da potência luminosa emitida pelo laser, enquanto que o ruído quântico varia inversamente com a potência. Desta forma, a

variação da flutuação da fase é dada por $\langle \Delta\theta(t)^2 \rangle = Q/P + C$, sendo que o primeiro representa a contribuição quântica ao ruído e o segundo termo representa a contribuição clássica. A detecção deste sinal óptico por um fotodiodo resulta na geração de uma tensão proporcional à corrente dada em (3.10), o que resulta em uma flutuação desta tensão da forma:

$$\left\langle V^2(t) \right\rangle = GP^2 \left\langle \Delta\theta^2(t) \right\rangle = GQP + GCP^2 + N. \tag{3.11}$$

Na equação (3.11), G é o ganho do sistema de detecção e N é o ruído adicionado pelo próprio detector. Por fim, define-se como figura de mérito a relação sinal-ruído (sendo aqui o ruído quântico é considerado o sinal) que pode ser obtida experimentalmente por:

$$SNR = \frac{GQP}{GCP^2 + N}. \tag{3.12}$$

Desta forma, pode-se encontrar experimentalmente a potência óptica que maximiza a relação sinal-ruído, este é o ponto de operação ótimo do GQNA.

Como o sinal de tensão obtido no detector é aleatório, ele é diretamente utilizado para a geração dos bits aleatórios. Cada valor de tensão medido é transformado em uma sequência binária de oito bits.

Por fim, há outras implementações de GQNA que não são discutidas nesta dissertação, como o GQNA utilizando o estado vácuo e detecção homódina [25], a descorrelação da distribuição do número de fótons de dois pulsos consecutivos emitidos por um laser [26] e a amplificação óptica do vácuo [27].

4 TEORIA DE UM GERADOR QUÂNTICO DE NÚMEROS ALEATÓRIOS DE VARIÁVEL CONTÍNUA UTILIZANDO POLARIZAÇÃO DA LUZ

O primeiro ponto a ser levado em consideração quando da proposição de um modelo de GQNA é a escolha do ruído quântico a ser utilizado. Neste capítulo, é apresentada a teoria de um modelo inédito de GQNA de variável contínua baseado na polarização da luz.

4.1 Teoria de um gerador quântico de números aleatórios de variável contínua utilizando polarização da luz

Classicamente, o estado de polarização da luz é totalmente caracterizado pelo vetor de Stokes $[S_0, S_1, S_2, S_3]^T$ sendo que,

$$S_0 = |\alpha_1|^2 + |\alpha_2|^2, \tag{4.1}$$

$$S_1 = |\alpha_1|^2 - |\alpha_2|^2, \tag{4.2}$$

$$S_2 = \left(\alpha_1^* \alpha_2 + \alpha_1 \alpha_2^*\right), \tag{4.3}$$

$$S_3 = -i\left(\alpha_1^* \alpha_2 - \alpha_1 \alpha_2^*\right). \tag{4.4}$$

Nas equações (4.1)-(4.4), α_1 e α_2 são, respectivamente, as amplitudes das componentes *x* e *y* do vetor campo elétrico. O parâmetro S_0 mede a intensidade do feixe e S_1, S_2 e S_3 caracterizam a polarização. De forma semelhante, os operadores quânticos de Stokes são definidos como sendo [28], [29]:

$$\hat{S}_0 = \hat{a}_1^\dagger \hat{a}_1 + \hat{a}_2^\dagger \hat{a}_2, \tag{4.5}$$

$$\hat{S}_1 = \hat{a}_1^\dagger \hat{a}_1 - \hat{a}_2^\dagger \hat{a}_2, \tag{4.6}$$

$$\hat{S}_2 = \hat{a}_1^\dagger \hat{a}_2 + \hat{a}_2^\dagger \hat{a}_1, \tag{4.7}$$

$$\hat{S}_3 = -i\left(\hat{a}_1^\dagger \hat{a}_2 - \hat{a}_2^\dagger \hat{a}_1\right) \tag{4.8}$$

$$\left[\hat{a}_i, \hat{a}_j^\dagger\right] = 1, \ i, j = 1, 2. \tag{4.9}$$

Nas equações (4.5)-(4.9) $\hat{a}_1^{\dagger}(\hat{a}_1)$ e $\hat{a}_2^{\dagger}(\hat{a}_2)$ são, respectivamente, os operadores de criação (aniquilação) das componentes *x* e *y*. Pode-se mostrar que para o estado coerente $|\alpha_1,\alpha_2\rangle$, os valores médios dos parâmetros de Stokes são aqueles mostrados nas equações (4.1)-(4.4) $\langle\alpha_1,\alpha_2|\hat{S}_i|\alpha_1,\alpha_2\rangle = S_i$, i=0,1,2,3. Entretanto, os parâmetros quânticos exibem flutuações que são expressas por suas variâncias [28], [29].

$$V_i \equiv \left\langle \left(\Delta\hat{S}_i\right)^2 \right\rangle = \left\langle \hat{S}_i^2 \right\rangle - \left\langle \hat{S}_i \right\rangle^2, \quad i = 0,1,2,3\,, \tag{4.10}$$

$$\left\langle \hat{S}_i^x \right\rangle = \langle \alpha_1\alpha_2 | \hat{S}_i^x | \alpha_1\alpha_2 \rangle, \quad x = 1,2. \tag{4.11}$$

Os valores médios e as variâncias dos parâmetros quânticos de Stokes de um estado coerente $|\alpha,\beta\rangle$ ($|\alpha\rangle$ representa a luz polarizada na direção *x* e $|\beta\rangle$ a luz polarizada na direção *y*) são dados por:

$$|\alpha,\beta\rangle = \sum_{n=0}^{\infty} e^{-\frac{|\alpha|^2}{2}} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \otimes \sum_{k=0}^{\infty} e^{-\frac{|\beta|^2}{2}} \frac{\beta^k}{\sqrt{k!}} |k\rangle \tag{4.12}$$

$$\left\langle \hat{S}_1 \right\rangle = |\alpha|^2 - |\beta|^2, \qquad \left\langle \hat{S}_1^2 \right\rangle = \left(|\alpha|^2 - |\beta|^2\right)^2 + |\alpha|^2 + |\beta|^2, \qquad V_1 = |\alpha|^2 + |\beta|^2 \tag{4.13}$$

$$\left\langle \hat{S}_2 \right\rangle = \alpha^*\beta + \alpha\beta^*, \qquad \left\langle \hat{S}_2^2 \right\rangle = \left(\alpha^*\beta\right)^2 + \left(\alpha\beta^*\right)^2 + |\alpha|^2 + |\beta|^2 + 2|\alpha|^2|\beta|^2, \quad V_2 = |\alpha|^2 + |\beta|^2 \tag{4.14}$$

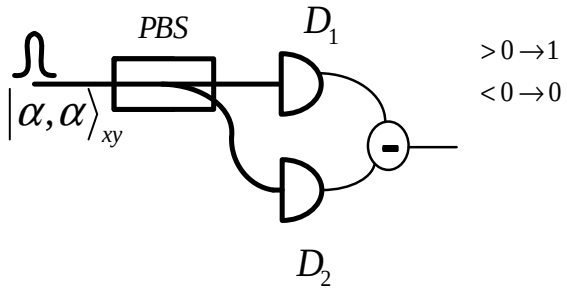
$$\left\langle \hat{S}_3 \right\rangle = i\left(\alpha^*\beta - \alpha\beta^*\right), \left\langle \hat{S}_3^2 \right\rangle = -\left(\alpha^*\beta\right)^2 - \left(\alpha\beta^*\right)^2 + |\alpha|^2 + |\beta|^2 + 2|\alpha|^2|\beta|^2, \; V_3 = |\alpha|^2 + |\beta|^2 \tag{4.15}$$

De (4.13)-(4.15), pode-se observar que a variância dos parâmetros de Stokes é tanto maior quanto maior for a potência óptica total. Portanto, qualquer parâmetro de Stokes pode ser usado como variável aleatória de um GQNA. Medições sucessivas de um destes parâmetros resultarão em uma sequência aleatória de valores cuja variância é proporcional à potência óptica do feixe medido.

O esquema óptico do GQNA inédito baseado na medição do parâmetro de Stokes S_2 é apresentado na Fig. 11. Um pulso de luz polarizado linearmente em $\pi/4$ passa por um divisor de feixes por polarização e a luz emitida em cada saída é detectada por um receptor óptico. A diferença dos sinais obtidos pelos fotodetectores é usada como variável aleatória.

Há duas possibilidades de formação da sequência binária: 1) Se a diferença das potências medidas em D_1 e D_2 for positiva, o bit ‘1’ é obtido, caso contrário o bit ‘0’ é obtido. 2) Como no caso do GQNA da Fig. 10, pode-se usar um conversor analógico-digital para obter uma sequência binária para cada valor da diferença de sinal.

Figura 11 - Gerador utilizando estado coerente e um PBS.



As vantagens deste GQNA são a simplicidade e a velocidade de operação, pois os detectores são baseados em fotodiodos PIN comuns e não em detectores de fótons com APDs. As desvantagens são, como em outros casos, a necessidade dos detectores D_1 e D_2 terem as mesmas características e a não idealidade do divisor de feixes por polarização. Além disso, deve-se levar em consideração o ruído introduzido pelos detectores D_1 e D_2.

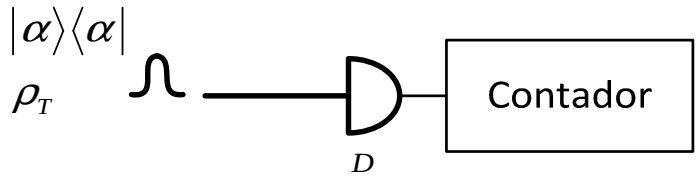
5 GERADOR QUÂNTICO DE NÚMEROS ALEATÓRIOS COM DISTRIBUIÇÃO BINOMIAL

Este capítulo discute a teoria da implementação de um GQNA com distribuição binomial, o uso do mesmo como GQNA binário e o desempenho de acordo com a fonte luminosa que utiliza estado coerente ou estado térmico.

5.1 Gerador quântico de números aleatórios com distribuição Binomial

O esquema óptico do GQNA com distribuição binomial, GQNA-BIN, é apresentado na Fig. 12

Figura 12 - Gerador quântico de números aleatórios com distribuição binomial, utilizando somente uma fonte luminosa de estado coerente ou térmico, um detector de fótons únicos e um contador de eventos.



O GQNA-BIN da Fig. 12 trabalha da seguinte forma: pulsos fracos de luz (emitidos por um laser – estado coerente - ou por um led – estado térmico) são detectados por um detector de fótons únicos e um contador de eventos registra o número de contagens (avalanches) obtidas em um intervalo fixo de tempo τ. Neste intervalo, existem N pulsos de gatilho no detector de fótons únicos, portanto, a distribuição do número de contagens segue a distribuição binomial, sendo a probabilidade da haver n detecções em N pulsos dada por $P(n)=\{N!/[n!(N-n)!]\}P^n(1-P)^{N-n}$ na qual P é a probabilidade de haver uma avalanche quando da chegada de um pulso óptico.

Um GQNA binário pode ser obtido, por exemplo, fazendo a seguinte codificação: se o número de contagens obtido é par, o bit gerado é o ‘0’, caso contrário o bit ‘1’ é gerado. Portanto, a probabilidade deste GQNA produzir o bit 0, P_0, é dada por:

$$P_0 = \sum_{n=0,2,4}^{N} \binom{N}{n} P^n \left(1-P\right)^{N-n}, \tag{5.1}$$

Dado um valor de *P* (diferente de 0 e 1) é sempre possível encontrar um valor de *N* tal que P_0 seja arbitrariamente próximo de 0,5. Entretanto, quanto menor este valor de *N*, menor o tempo de contagem e mais rápido é o GQNA. Logo, o desempenho de um GQNA mostrado na Fig. 12 depende do valor de *N* que, por sua vez, depende do valor de *P* e este último depende das propriedades do detector de fótons únicos e da fonte de luz utilizados. Para um detector de fótons únicos com eficiência quântica η, probabilidade de contagem de escuro p_d e afterpulsing modelada pela probabilidade p_a e τ o tempo de decaimento para a probabilidade de afterpulsing cair de *1/e* (ver apêndice B), a probabilidade de uma avalanche ser disparada durante um pulso de gatilho é dada por [30][31]:

$$P^2 - [p_a(1-p_D)e^{\tau} + p_D + (1-e^{\tau})]P + p_D(1-e^{\tau}) = 0, \tag{5.2}$$

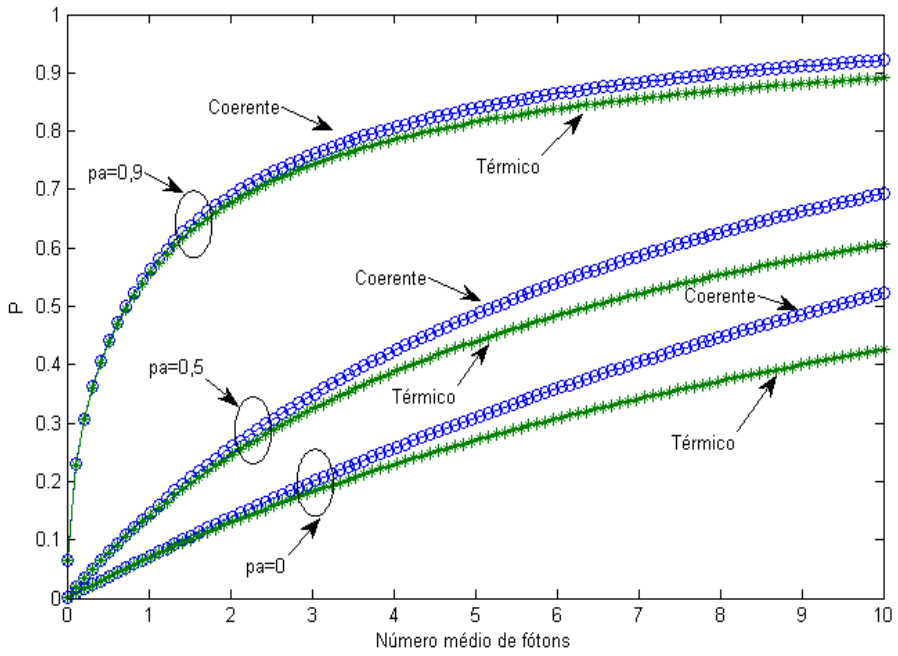
Na qual $p_D \equiv p_D^c$ para a fonte coerente e $p_D \equiv p_D^t$ para a fonte térmica, sendo:

$$p_D = 1 - e^{-\eta\mu}(1-p_d) \equiv p_D^c, \tag{5.3}$$

$$p_D = 1 - \frac{1}{1+\eta\mu_t}(1-p_d) \equiv p_D^t. \tag{5.4}$$

Além disso, em (5.3) e (5.4), μ e μ_t são, respectivamente, o número médio de fótons dos estados coerente e térmico usados. Pode-se facilmente verificar que para $p_a = 0$ (ausência de afterpulsing), a solução da Eq. (5.2) é P_D , como esperado. Por outro lado, se $p_a = 1$, então $P = 1$. Usando as equações (5.2)-(5.4) para um detector de fótons únicos com η = 0,074, $p_d = 2{,}9 \cdot 10^{-5}$, $p_a = \{0{,}9;\ 0{,}5;\ 0\}$ e $\tau = 2{,}34$, a Fig. 13 mostra o valor de *P* na Eq. (5.2) para diferentes números médios de fótons, considerando o uso de ambos os estados coerente e térmico.

Figura 13 - *P* versus número médio de fótons.



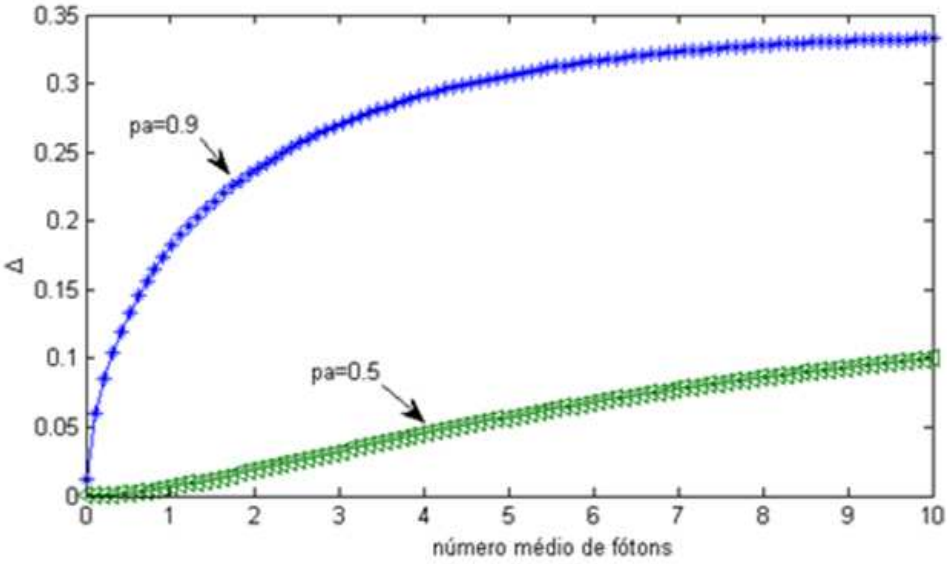
Na Fig. 13 podemos ver, como esperado, que quanto maior a probabilidade de afterpulsing maior o valor de *P*. Além disso, a probabilidade de avalanche quando o estado coerente é usado, chamada P_c , é maior que a probabilidade de avalanche quando o estado térmico é usado, chamada de P_t. Isto acontece porque para o mesmo número médio de fótons, a componente do vácuo para o estado coerente é menor que a componente do vácuo para o estado térmico.

Na Fig. 13 também pode ser visto que o afterpulsing tem o efeito de amplificação na probabilidade de disparar uma avalanche, $Pc,t(p_a > 0) > Pc,t\ (p_a = 0)$. Esta amplificação é maior para o estado térmico que para o estado coerente. A fim de ver isto, a Fig. 14 mostra o valor da diferença entre os ganhos dos estados térmicos e coerentes, Δ, para dois diferentes valores de p_a, versus o número médio de fótons, sendo Δ dado por:

$$\Delta = \frac{P_t}{P_D^t} - \frac{P_c}{P_D^c}. \tag{5.5}$$

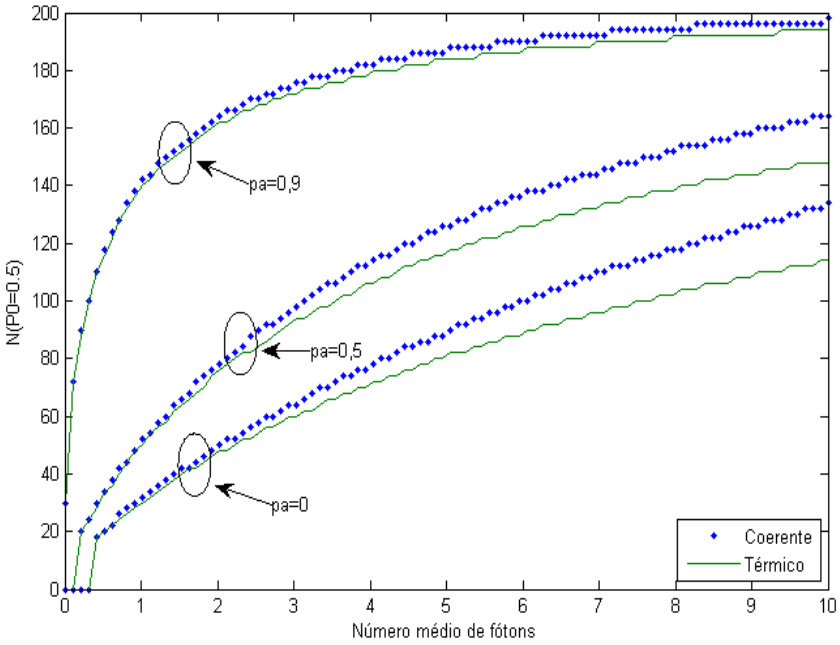
Sendo P_D^t a probabilidade do estado térmico sem afterpulsing e P_D^c a probabilidade do estado coerente sem afterpulsing.

Figura 14 - Δ versus número médio de fótons.



A Fig. 14 mostra que o desempenho do GQNA depende da probabilidade de afterpulsing e do estado quântico utilizado. Para observar melhor este fato, a Fig. 15 mostra o mínimo valor de N na Eq. (5.1) tal que P_0 =0,5 +10^{-5}, versus o número médio de fótons, para três valores de p_a (0,9; 0,5; 0), e considerando ambos os estados, térmico e coerente.

Figura 15 - N versus número médio de fótons para p_a = 0, 0,5 e 0,9.



Enquanto um aumento de p_a leva ao aumento de P na Eq. (5.2), isto também leva ao aumento do valor de N. Quanto maior for o valor de N, menor a taxa de geração de bits aleatórios do GQNA mostrado da Fig. 12 e, portanto, o menor desempenho deste GQNA. Essa é uma particularidade da Eq. (5.1). Se P=1, então P_0=0 se N é ímpar e P_0=1 se N é par. Portanto, em contraste com GQNA tradicional mostrado na Fig. 8, o aumento de P diminui a velocidade do GQNA. Pela mesma razão N aumenta quando o número médio de fótons cresce.

As maiores vantagens deste GQNA são a simplicidade e baixo custo, enquanto que a principal desvantagem é a baixa velocidade. De fato, tem-se apenas um bit aleatório por N pulsos de gatilho.

É importante observar que a variável quântica utilizada no GQNA da Fig. 12 é a amplitude da componente do vácuo e, portanto, ele não funciona como se uma fonte verdadeira de fótons únicos fosse utilizada (uma vez que nesta a componente do vácuo não existe). A amplitude da componente do vácuo é essencial para a aleatoriedade, pois o GQNA não seria aleatório se sempre houvesse detecção. O mesmo ocorre se a luz coerente ou térmica utilizada tiver um número médio de fótons elevados, pois neste caso a amplitude da componente do vácuo seria próxima de zero. Outro questionamento que pode surgir é por que não utilizar uma fonte com número médio de fótons tal que $P_{c,t}$ = 0,5 e usar N = 1? Para um detector de fótons únicos sem ruído (p_d = 0) e com eficiência quântica η = 0,1, por exemplo, aquele número médio de fótons seria aproximadamente 6.9. Com este valor, a probabilidade de pulsos com muitos fótons aumenta bastante. Isto leva ao aumento do afterpulsing, pois a corrente que flui no APD durante uma avalanche cresce com o número de fótons absorvidos, e o afterpulsing cresce com o aumento do valor da corrente de avalanche.

Por fim, poderíamos obter um bit aleatório por pulso de gatilho se houvesse uma fonte luminosa que produzisse o estado quântico $(|0\rangle+|1\rangle)/2^{1/2}$, ou seja, uma superposição do estado vácuo e do estado número de um fóton. Como esta fonte ainda não existe, a aproximação da mesma com estados coerentes e térmicos leva a uma piora do desempenho, ou seja, a um número maior de pulsos de gatilho para se obter um único bit aleatório.

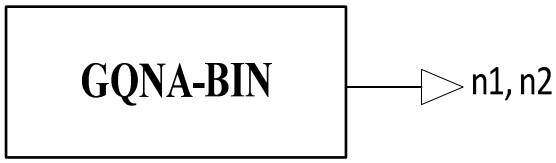
5.2 Aplicações do GQNA com distribuição binomial

A principal utilização do GQNA-BIN não é como GQNA binário, uma vez que a eficiência (taxa de bits aleatórios/número de pulsos de gatilho) tende a ser baixa. Entretanto,

existem aplicações clássicas e quânticas nas quais uma variável aleatória binomial é requerida. Em particular, protocolos de distribuição quântica de chaves com variáveis contínuas requerem modulações com variáveis aleatórias gaussianas ou não gaussianas [32], [33],[34]. Nestes casos, estados coerentes da forma $|x+ip\rangle$ são utilizados, sendo que x e p seguem uma distribuição que pode ser Gaussiana ou não, dependendo do protocolo.

A proposição a ser feita aqui é que o GQNA-BIN seja utilizado para a escolha aleatória dos valores de x e p dos estados coerentes $|x+ip\rangle$. O valor médio e a variância da distribuição binomial são, respectivamente, dadas por NP e $NP(1-P)$. Portanto, o número de pulsos de gatilho e as características da fonte luminosa e do detector de fótons controlam a distribuição binomial obtida pelo GQNA da Fig. 12. Entretanto, a variável aleatória produzida pelo GQNA-BIN é um número inteiro, enquanto que os valores de x e p podem ser reais. Há, portanto, a necessidade de uma codificação ou mapeamento do resultado produzido pelo GQNA-BIN e o estado coerente a ser produzido. Sejam K e W valores da variável aleatória obtida pelo GQNA-BIN. Pode-se, por exemplo, assumir que $x=(K-NP)/S$ e $p=(W-NP)/S$, sendo S um valor escolhido para controlar a faixa de valores de x e p. A codificação está descrita na Fig. 16 A subtração da média é importante para que valores positivos e negativos de x e p sejam igualmente prováveis.

Figura 16. Resultado do mapeamento do GQNA-BIN.



A Fig. 16 trabalha da seguinte forma: são escolhidos dois valores aleatoriamente da distribuição binomial e estes valores são utilizados para realizar a codificação de x e p.

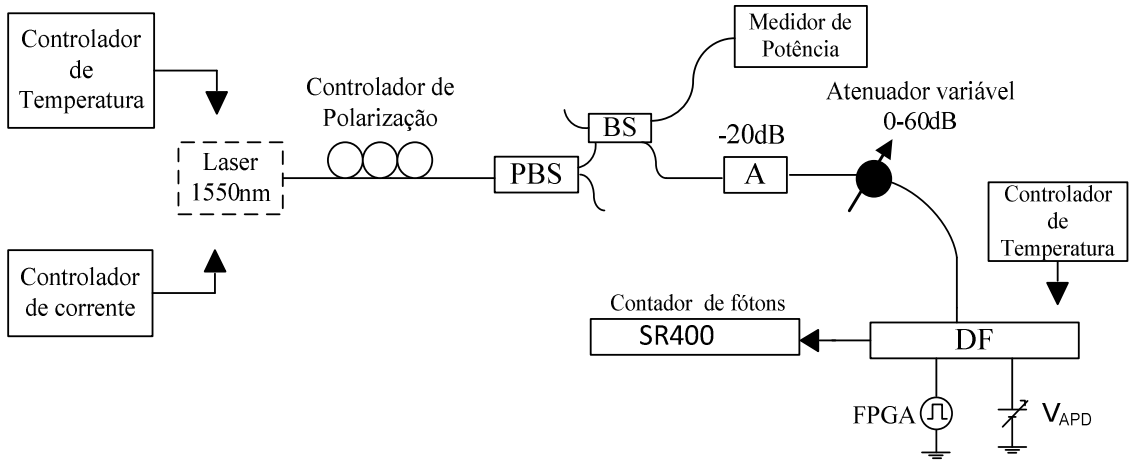
6 IMPLEMENTAÇÃO EXPERIMENTAL DO GQNA COM DISTRIBUIÇÃO BINOMIAL

Neste capítulo são apresentados os resultados experimentais da construção de um GQNA com distribuição binomial. Foram utilizados um detector de fótons e um laser semicondutor operando bem acima do limiar, para gerar estados coerentes, e bem abaixo do limiar, para gerar estados térmicos.

6.1 Experimento do Gerador Quanto-óptico de Números Aleatórios com Distribuição Binomial

O GQNA-BIN implementado é o mostrado na Fig. 12 e o esquema óptico experimental do mesmo é apresentado na Fig. 17.

Figura 17 - Esquema óptico do GQNA-BIN.



O experimento da Fig. 17 consiste na contagem do número de detecções, em um intervalo fixo de tempo, quando o detector de fótons é iluminado pela luz fortemente atenuada gerada por um diodo laser semicondutor CW, com corrente de limiar de 15,5 mA, operando com as correntes de 3 mA (estado térmico) e 37,2 mA (estado coerente). Os parâmetros mais relevantes para o ajuste experimental são: o valor da atenuação, corrente do laser, tensão sobre o APD e a frequência de gatilho do laser. A atenuação é aplicada para diminuir a intensidade do laser de forma que tenhamos o número médio de fótons pequeno por janela de gatilho. A frequência do sinal de gatilho do APD utilizada foi baixa o suficiente para que o afterpulsing pudesse ser desconsiderado.

O aparato experimental completo foi montado de tal forma que a luz emitida pelo laser fosse atenuada diferentemente nos dois valores de correntes utilizados a fim de que o número médio de fótons incidentes fosse o mesmo para as duas correntes.

O laser utilizado é o CQF915/408-19330 da JDSU, o medidor de potência é o PM100D da Thorlabs, o controlador de temperatura utilizado no detector de fótons é ITC4005 da Thorlabs, a placa FPGA Virtex-6 ML605 foi utilizada como gerador de sinal de gatilho, o contador de fótons é o SR400 da Stanford Research e, por fim, o detector de fótons foi construído com o fotodiodo de InGaAs/InP PGA-400 da Princeton Lightwave.

No esquema da Fig. 17, a luz emitida pelo laser CW na janela de 1550 nm, passa inicialmente por um atenuador composto por um controlador de polarização e um divisor de feixes por polarização (PBS). Uma das saídas do PBS é conectada a um acoplador óptico (BS). Uma das saídas do BS é conectada ao medidor de potência para monitoramento e a outra segue pela atenuação fixa de -20 dB para em seguida passar pelo atenuador óptico digital variável (0-60 dB da OZ Optic). Por fim, o sinal óptico chega ao detector de fótons, cujo sinal de saída é conectado ao detector de eventos SR400. A frequência do pulso de gatilho utilizada foi 62,5kHz, a tensão total sobre o APD foi de 71,2 V o que resultou em uma tensão de excesso de 1,8 V. A temperatura de operação do fotodiodo foi em torno de -40,65°C. O tempo de integração foi de 50ms, resultando em N = 3125 pulsos de gatilho por valor aleatório obtido. O número médio de fótons por duração de pulso de gatilho, t_g, é :

$$\langle n \rangle = \frac{t_g . P_{opt}}{hc/\lambda}. \qquad (6.1)$$

No experimento foram utilizados λ = 1550,75 nm, t_g = 10 ns, e P_{opt} = -80 dBm (além disso, h = 6,626·10-34 m^2kg/s e c = $3 \cdot 10^8$ m/s), portanto, o número médio de fótons é aproximadamente 0,78. Por fim, a eficiência quântica e a probabilidade de contagem de escuros do detector são, respectivamente, η = 0,095 e p_d = 0,1 (ver Fig. 19).

As curvas da frequência relativa do número de contagens, para o GQNA-BIN usando estados coerente e térmico, são mostradas na Fig. 18. Cada curva possui 70.000 pontos e os valores médios e variâncias são $\langle n \rangle$ = 507.3 e Δn^2 = 417.7298 para o estado térmico, e $\langle n \rangle$ = 515.6384 e Δn^2 = 439.5654 para o estado coerente. Com estes valores têm-se que as probabilidades de detecção por pulso são de ~0,159 para o estado térmico e ~0,165 para o estado coerente. A curva da frequência relativa do número de contagens de escuro, para

o GQNA-BIN é mostrada na Fig. 19. A curva possui 20.000 pontos e o valor médio das contagens é $\langle n \rangle$ =330.76.

Figura 18 - Frequência relativa do número de contagens para o GQNA-BIN usando estados térmico e coerente.

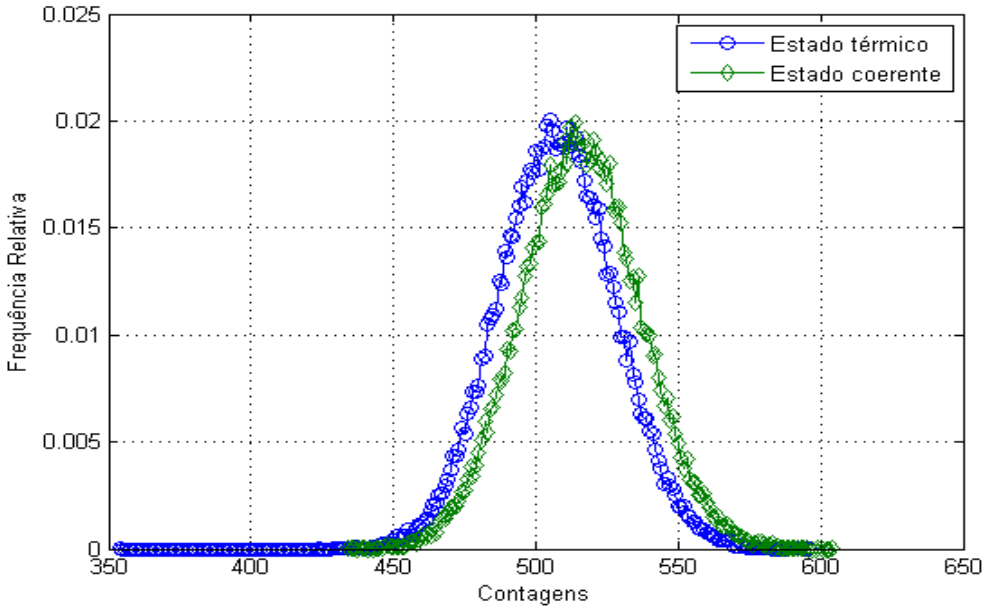
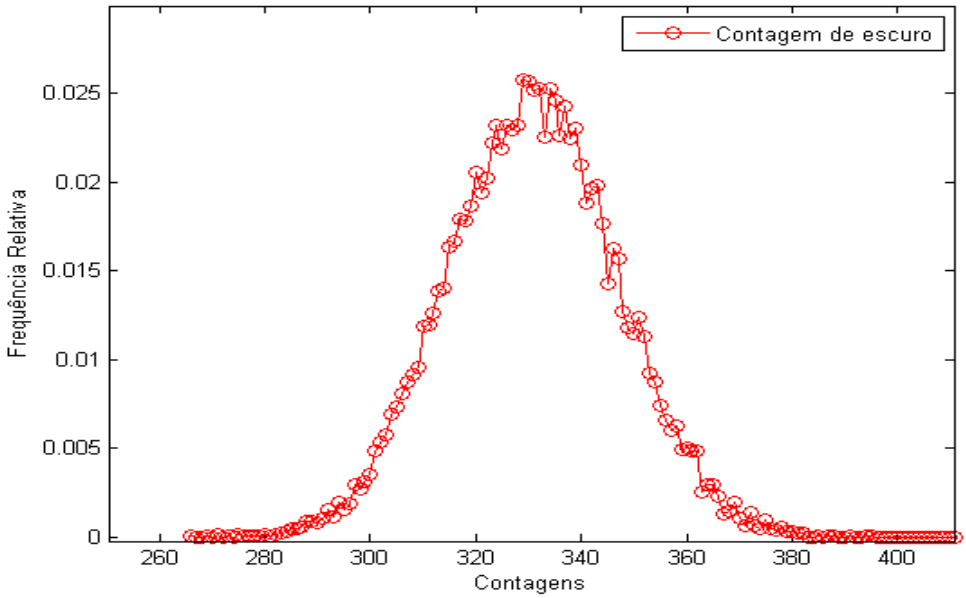


Figura 19 - Frequência relativa do número de contagens de escuro para o GQNA-BIN.



7 CONCLUSÕES E PERSPECTIVAS

7.1 Conclusões

Esta dissertação teve como principais objetivos o estudo teórico de geradores quanto-ópticos de números aleatórios e a realização experimental de um GQNA com distribuição binomial. Como contribuições do trabalho podem-se citar:

1. A proposição de um GQNA de variável contínua baseado na polarização da luz.
2. A análise teórica do desempenho de um GQNA binário construído a partir de um GQNA binomial, levando em consideração o afterpulsing e o tipo de estado quântico da luz utilizado, coerente ou térmico.
3. A construção de um GQNA binomial utilizando um detector de fótons, um laser fortemente atenuado e um contador de eventos.

Do trabalho realizado pode-se concluir que:

1. O GQNA de variável contínua baseado na medição de um dos parâmetros de Stokes possui como vantagens a implementação simples e potencial para ser rápido o suficiente para trabalhar na faixa de gigabits/s. Semelhantemente ao que ocorre com outros GQNA de variáveis contínuas, deve haver o cuidado na construção dos detectores de tal forma que o ruído introduzido pelo circuito eletrônico dos detectores não seja mais potente que o ruído quântico que se deseja observar.
2. Para a análise teórica do GQNA binário construído a partir do GQNA-BIN, pode-se observar que: 1) o afterpulsing degrada o desempenho do gerador. 2) para os mesmos valores de afterpulsing e número médio de fótons, o gerador utilizando estado térmico é levemente mais rápido que o gerador utilizando estado coerente.
3. O GQNA-BIN é de fácil implementação e apresentou resultados coerentes com a teoria e pode ser utilizado em protocolos de distribuição quântica de chaves com variáveis contínuas.

7.2 Perspectivas de Trabalhos Futuros

Como perspectivas de trabalhos futuros decorrentes dos resultados da presente dissertação, podem-se citar:

1. Construir o GQNA de variável contínua baseado em polarização da luz.
2. Construir versões mais compactas do GQNA com distribuição binomial para utilizá-lo em sistemas de distribuição quântica de chaves com variável contínua.

APÊNDICES

APÊNDICE A - Teoria Quântica da Detecção Óptica

A.1 Estados Quânticos

Nesta seção serão apresentados modelos da mecânica quântica da luz para a compreensão dos resultados experimentais. Na mecânica quântica os resultados dos experimentos não são únicos, várias possibilidades de saída ocorrem com algumas probabilidades. Logo, um simples número é insuficiente para descrever as possíveis saídas de um determinado experimento. Na teoria quântica, os campos são representados por operadores quânticos. Estes operadores estão presentes nas soluções dos osciladores harmônicos quânticos e também utilizados na representação do campo elétrico, já que este se trata de um campo oscilante.

A.2 Estados Fock

â e â † são os operadores de aniquilação e criação para fótons, respectivamente. Estes operadores obedecem a seguinte regra de comutação:

$$[\hat{a}, \hat{a}^{\dagger}] = 1 \qquad \text{(A.1)}$$

O operador número utilizado para definir o número de fótons no campo é dado por:

$$\hat{n} = \hat{a}^{\dagger}\hat{a} \qquad \text{(A.2)}$$

Os estados de Fock ou estados número são autoestados do operador número:

$$\hat{n}\left|n\right\rangle = n\left|n\right\rangle \qquad \text{(A.3)}$$

Onde os autovalores n=0,1,2,... A ação dos operadores: criação e aniquilação sobre o estado número fornecem os seguintes resultados:

$$a^{\dagger}\left|n\right\rangle = \sqrt{n+1}\left|n+1\right\rangle \qquad \text{(A.4)}$$

$$\hat{a}\left|n\right\rangle = \sqrt{n}\left|n-1\right\rangle \qquad \text{(A.5)}$$

Esses resultados mostram o porquê dos nomes criação e aniquilação, uma vez que o operador criação em um estado $\left|n\right\rangle$ gera um estado de ordem superior $\left|n+1\right\rangle$, o contrário ocorre quando se aplica o operador aniquilação gerando um estado de ordem inferior $\left|n-1\right\rangle$.

A.3 Estados Coerentes

Outro estado apropriado para o estudo dos campos ópticos é o estado coerente que é conhecido como o autovetor do operador destruição dado pela relação:

$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle \tag{A.6}$$

Outra maneira de definir o estado coerente é utilizar o operador deslocamento que é um gerador de estado coerente aplicado ao estado vácuo $|0\rangle$:

$$|\alpha\rangle = \hat{D}(\alpha)|0\rangle \tag{A.7}$$

Onde o operador deslocamento é definido como:

$$\hat{D}(\alpha) = \exp(\alpha\hat{a}^{\dagger} - \alpha^{*}\hat{a}) \tag{A.8}$$

Listamos abaixo algumas propriedades dos estados coerentes:

- A probabilidade de se encontrar n fótons no estado coerente $|\alpha\rangle$, é dada por:

$$p_n = \left|\langle n|\alpha\rangle\right|^2 = \frac{\exp^{-|\alpha|^2}|\alpha|^{2n}}{n!} \tag{A.9}$$

- O valor do número médio de fótons é dado por:

$$\langle n\rangle = \langle\alpha|\hat{n}|\alpha\rangle = |\alpha|^2 \tag{A.10}$$

- A variância:

$$(\Delta n)^2 = \langle n^2\rangle - \langle n\rangle^2 = |\alpha|^2 \tag{A.11}$$

A.4 Estado Térmico

O estado térmico é um estado de mistura da radiação eletromagnética que é produzido por uma fonte luminosa incoerente com distribuição de probabilidade do número de fótons da luz térmica dada por:

$$P_n = \frac{\langle n\rangle^n}{\left(1+\langle n\rangle\right)^{n+1}} \tag{A.12}$$

Onde $\langle n\rangle$ é o número médio de fótons [35].

APÊNDICE B - Cálculo da Probabilidade de Ocorrência de Avalanche na Presença de Afterpulsing.

Para um detector de fótons com extinção engatilhada, a probabilidade de haver uma detecção na *n*-ésima janela de gatilho é dada por [31]:

$$p_1 = p_D \tag{B.1.a}$$

$$p_2 = p_D + (1-p_D)\,p_1 p_a \tag{B.1.b}$$

$$p_3 = p_D + (1-p_D)\,p_2 p_a + (1-p_D)(1-p_2)\,p_1 p_a e^{-\tau} \tag{B.1.c}$$

$$p_4 = p_D + (1-p_D)\,p_3 p_a + (1-p_D)(1-p_3)\,p_2 p_a e^{-\tau} + (1-p_D)(1-p_3)(1-p_2)\,p_1 p_a e^{-2\tau} \tag{B.1.d}$$

$$\vdots$$

$$p_n = p_D + (1-p_D)\,p_a\left[\sum_{k=1}^{n-1} p_k e^{-(n-1-k)\tau}\prod_{j=k+1}^{n-1}(1-p_j)\right] \tag{B.1.e}$$

$$p_D = 1-e^{\eta\mu}(1-p_d) \tag{B.1.f}$$

em que μ é o número médio de fótons da luz coerente incidente, η a eficiência quântica do APD, p_d a probabilidade haver uma contagem de escuro e $p_a e^{-(k-1)\tau}$ é a probabilidade de haver uma contagem *afterpulse* devido à uma avalanche que ocorreu há *k* janelas de gatilho atrás. No regime estacionário tem-se $p_n=p_{n+1}=P$. Usando esta condição em (B.1e) chega-se a:

$$P^2 - \left[p_a(1-p_D)e^{\tau} + p_D + (1-e^{\tau})\right]P + p_D(1-e^{\tau}) = 0. \tag{B.2}$$

REFERÊNCIAS

[1] RIBEIRO, José Antônio Justino, **Comunicações ópticas**, 4. ed. Érica, 2010.

[2] Perkin-Elmer Optoelectronics Technical Staff, Avalanche Photodiodes: A User's Guide, Perkin-Elmer Optoelectronics, 2004. Disponível em: < http://www.perkinelmer.com/CMSResources/Images/446538APP_AvalanchePhotodiodesUsersGuide.pdf>. Acesso em: 20 março. 2012.

[3] CAVALCANTI, Maria Daniela Santibaia. **Caracterização de fotodiodos de Avalanche operando no modo Geiger usando análise espectral**. 2011 Dissertação (Mestrado em Engenharia de Teleinformática) – Centro de Tecnologia, Universidade Federal do Ceará, Fortaleza, 2011.

[4] SILVA, Thiago Ferreira. **Transmissão óptica de bits quânticos codificados em frequência com sincronismo por WDM**. 2008 Dissertação (Mestrado em Engenharia Elétrica) – Centro de Tecnologia, Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2008.

[5] THÉ, George André Pereira. **Teoria e implementação de detectores de fótons isolados para comunicações quânticas em redes ópticas**, 2006 Dissertação (Mestrado em Engenharia de Teleinformática) - Centro de Tecnologia, Universidade Federal do Ceará, Fortaleza, 2006.

[6] NAMEKATA, Naoto, **Single-photon generation and detection for quantum key distribution at 1550 nm**. 2007 Tese (Doutorado em Ciência Quântica) - Centro de Ciência e Tecnologia, Nihon University, 2007.

[7] STUCKI, D. *et al*. Photon Counting for quantum key distribution with Peltier Cooled InGaAs/InP APDs. **Journal of Modern Optics**. v. 48, n.13, p. 1967-1981, 2001. Disponível em:< http://arxiv.org/pdf/quant-ph/0106007.pdf>. Acesso em 24 junho. 2012.

[8] RIBORDY, G. *et al*. Performance of InGaAs/InP avalanche photodiodes as gated-mode photon counters, **Applied Optics**, v. 37, n.12, p. 2272-2277, 1998. Disponível em: < http://www.opticsinfobase.org/view_article.cfm>. Acesso em 10 julho. 2012.

[9] SALEH, Bahaa E. A. e TEICH, Malvin Carl, **Fundamentals of photonics**, 2. ed.: Wiley Interscience,1991.

[10] KNUTH, Donald Ervin, **The art of computer programming**, 2 ed: Adisson Wesley, vol 2, 1981.

[11] Natl. Inst. Stand. Technol. Spec. Publ. 800-22rev1a, 131 pages (April 2010). Disponível em: <csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf>. Acesso em 10 setembro. 2011.

[12] NIEDERREITER, Harald, **Random number generation and quasi-Monte Carlo methods,** Society for Industrial and Applied Mathematics**,** 1992**.**

[13] KENNY, C. **Random Number Generators: An Evaluation and Comparison of Random.org and Some Commonly Used Generators.** April 2005. Trinity College Dublin. Disponível em: <http://www.random.org/analysis/Analysis2005.pdf>. Acesso em: 5 abril . 2012.

[14] KELSEY, J, *et al*. **Yarrow-160**: Notes on the Design and Analysis of the Yarrow Cryptographic Pseudorandom Number Generator. Sixth Annual Workshop on Selected Areas in Cryptography, Springer Verlag, August 1999. Disponível em: <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.35.9959>. Acesso em: 10 março. 2012.

[15] GENTLE, James E. **Random Number Generation and Monte Carlo Methods**, 2 ed., Springer, 2005.

[16] L'ECUYER, P. Uniform random number generation, **Annals of Operations Research**, v. 53, p. 77-120, 1994. Disponível em: < http://www.springerlink.com/content/q126444k3w32t031/fulltext.pdf>. Acesso em: 15 julho. 2012.

[17] ID Quantique with paper, Random Number Generation using quantum physics versão 3.0, Abril 2010. Disponível em: <http://www.idquantique.com/images/stories/PDF/quantis-random-generator/quantis-whitepaper.pdf>. Acesso em: 15 novembro. 2012.

[18] WEI, W. *et al.* Quantum random number generator based on the photon number decision of weak laser pulses, **quant-ph**, 2008. Disponível em: < http://arxiv.org/pdf/0811.0082.pdf >. Acesso em: 16 novembro. 2012.

[19] WAYNE, M. *et al*. Photon arrival time quantum random number generation, **Journal of Modern Optics**, p. 1-7, 2009. Disponível em:< http://research.physics.illinois.edu/QI/Photonics/papers/wayneJMO.pdf>. Acesso em: 15 outubro. 2012.

[20] WAYNE, M. *et al*. Low-bias high-speed quantum random number generator via shaped optical pulses, **Optics Express**, v. 18, nº 8, p. 9351-9357, 2010. Disponível em:< http://www.opticsinfobase.org/oe/abstract.cfm?uri=oe-18-9-9351 >. Acesso em: 15 outubro. 2012.

[21] DYNES, J. *et al*. A high speed, postprocessing free, quantum random number generator, **Applied Physics Letters**, nº 93, p. 031109/1-3, 2008. Disponível em: < http://arxiv.org/pdf/0807.4111v1.pdf>. Acesso em: 08 outubro. 2012.

[22] XU, F. *et al*. Ultrafast quantum random number generation based on quantum phase fluctuations, **Quantum Physics**, v. 20, nº 11, p. 12366-12377, 2012. Disponível em:< http://arxiv.org/pdf/1109.0643.pdf>. Acesso em: 01 setembro. 2012.

[23] VAHALA, K. *et al*. Occupation fluctuation noise: A fundamental source of linewidth broadening in semiconductor lasers, **Applied Physics Letters**, v. 43, p. 140-142, 1983. Disponível em:< http://authors.library.caltech.edu/5835/1/VAHapl83c.pdf >. Acesso em: 04 setembro 2012.

[24] KIKUCHI, K. *et al*. Dependence of semiconductor laser linewidth on measurement time: evidence of predominance of 1/*f* noise, **Electronics Letters**, v.21, n° 22, p. 1011-1012, 1985. Disponível em: <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=4251544&contentType=Journals+%26+Magazines&sortType%3Dasc_p_Sequence%26filter%3DAND%28p_IS_Number%3A4251538%29>. Acesso em: 04 setembro. 2012.

[25] SYMUL, T. *et al*. Real time demonstration of high bitrate quantum random number generation with coherent laser light, **Appied Physics Letters**, v. 98, p.1-4, 2011. Disponível em: < http://arxiv.org/pdf/1107.4438.pdf>. Acesso em: 10 outubro. 2012.

[26] WEY,W. *et al.* Bias-free true random-number generator. **Optics Letters.** v. 34, n.12, p. 1876-1878, 2009. Disponível em: <http://arxiv.org/pdf/0905.0779v2.pdf>. Acesso em: 10 outubro. 2012.

[27] JOFRE, M. *et al.* True random numbers from amplified quantum vacuum, **Optic Express**, v.19, n.21, p.20665-20672. Disponível em: <http://arxiv.org/pdf/1110.0599.pdf>. Acesso em: 10 outubro. 2012.

[28] BORELLI, L. F. M. *et al*. Quantum key distribution using polarized coherent states, 2006. Disponível em: < http://cdsweb.cern.ch/record/722634/files/0403076.pdf>. Acesso em 10 agosto. 2012.

[29] LUIS, A. Degree of polarization in quantum optics, **Physical review**. A 66, 013806, 2002. Disponível em: < http://pra.aps.org/pdf/PRA/v66/i1/e013806>. Acesso em: 2 agosto. 2012.

[30] CAVALCANTI, M.D.S. *et al*. Spectral method for characterization of avalanche photodiode working as single-photon detector, **Optical Letters**, v. 36, n. 17, p. 3446-3448, 2011. Disponível em: < http://www.opticsinfobase.org/ol/abstract.cfm?uri=ol-36-17-3446>. Acesso em: 12 agosto. 2012.

[31] MENDONÇA, Fábio Alencar. **Protocolos e Detectores de Fótons para Comunicações Quânticas.** Tese (Doutorado em Engenharia de Teleinformática) - Centro de Tecnologia, Universidade Federal do Ceará, Fortaleza, 2011.

[32] LEVERRIER. A. *et al*. Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation, **Physical Review A**, v. 83, 042312/1-15, 2011. Disponível em: < http://arxiv.org/pdf/1101.3008v2.pdf >. Acesso em: 15 de novembro. 2012.

[33] LEVERRIER. A. *et al*. Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation, **Physical Review Letters**, v. 102, 180504/1-4, 2009. Disponível em: < http://arxiv.org/pdf/0812.4246v1.pdf >. Acesso em: 15 novembro 2012.

[34] JOUGUET, Paul, *et al*. Long-distance continuous-variable quantum key distribution with a Gaussian modulation, **Physical Review A**, v. 84, 062317/1-7, 2011. Disponível em: < http://arxiv.org/pdf/1110.0100v2.pdf >. Acesso em: 10 de novembro. 2012.

[35] WALLS, Daniel Frank. e MILBURN, Gerard. J., **Quantum Optics**. Springer, 1994.