UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA DA TELEINFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA DA TELEINFORMÁTICA

JOACIR SOARES DE ANDRADE

APLICAÇÕES DA FUNÇÃO W_q de LAMBERT-TSALLIS E DA DISENTROPIA EM DISTRIBUIÇÃO QUÂNTICA DE CHAVES

FORTALEZA
2023

JOACIR SOARES DE ANDRADE

APLICAÇÕES DA FUNÇÃO Wq de LAMBERT-TSALLIS E DA DISENTROPIA EM DISTRIBUIÇÃO QUÂNTICA DE CHAVES

Tese ou Dissertação apresentada ao Programa de Pós-Graduação em Engenharia da Teleinformática da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Doutor em **ENGENHARIA DA TELEINFORMÁTICA**. Área de concentração: Eletromagnetismo Aplicado.

Orientador: Prof. Dr. Rubens Viana Ramos

FORTALEZA
2023

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

A567a Andrade, Joacir Soares de.
Aplicações da função Wq Lambert-Tsallis e da disentropia em distribuição quântica de chaves / Joacir Soares de Andrade. – 2023.
66 f. : il. color.

Tese (doutorado) – Universidade Federal do Ceará, Centro de Tecnologia, Programa de Pós-Graduação em Engenharia de Teleinformática, Fortaleza, 2023.
Orientação: Prof. Dr. Rubens Viana Ramos.

1. distribuição quântica de chaves. 2. função wq de lambert-tsallis. 3. disentropia. 4. aleatoriedade. I. Título.
CDD 621.38

ATA DA SESSÃO DE DEFESA DE TESE DE DOUTORADO

UNIVERSIDADE FEDERAL DO CEARÁ

PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA DE TELEINFORMÁTICA

Como parte das exigências para concessão do grau de doutor, às 07:30 horas do dia 19 de Dezembro de 2023, realizou-se a sessão pública da defesa de tese de doutorado do aluno JOACIR SOARES DE ANDRADE. O trabalho tinha como título: "APLICAÇÕES DA FUNÇÃO Wq de LAMBERT-TSALLIS E DA DISENTROPIA EM DISTRIBUIÇÃO QUÂNTICA DE CHAVES".

Compunham a banca examinadora os professores(as) doutores(as) RUBENS VIANA RAMOS, orientador, JOAO BATISTA ROSA SILVA, CELSO JORGE VILLAS BOAS, DANIEL FELINTO PIRES BARBOSA e GUILHERME BARRETO XAVIER. O candidato expôs oralmente a tese, em seguida os membros da banca procederam à arguição, e a sessão foi finalizada com a APROVAÇÃO, por parte da banca examinadora, do trabalho sem ressalvas.

Foi lavrada a presente ata que é abaixo assinada pelos membros da referida banca:

gov.br Documento assinado digitalmente
RUBENS VIANA RAMOS
Data: 20/12/2023 07:14:08-0300
Verifique em https://validar.iti.gov.br

RUBENS VIANA RAMOS
UFC - Orientador

gov.br Documento assinado digitalmente
JOAO BATISTA ROSA SILVA
Data: 19/12/2023 19:20:33-0300
Verifique em https://validar.iti.gov.br

JOAO BATISTA ROSA SILVA
UFC - Examinador Interno

CELSO JORGE VILLAS BOAS
UFSCAR - Examinador Externo à Instituição

DANIEL FELINTO PIRES BARBOSA
UFPE - Examinador Externo à Instituição

GUILHERME BARRETO XAVIER
LIU - Examinador Externo à Instituição

Fortaleza, 19 de Dezembro de 2023

A Deus,

Aos meus pais Joaquim e Neuza.

A minha esposa Jacqueline.

As minhas filhas Dharana e Thamiris.

AGRADECIMENTOS

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001.

Ao prof. Dr. Rubens Viana Ramos, pela excelente orientação e incentivo à carreira de pesquisador.

A todos com quem tive excelente convivência durante o doutorado no ambiente do departamento de engenharia da Teleinformática, em especial aos professores Kleber Zuza e João Batista pelas amplas colaborações feitas ao trabalho. A professora Hilma Vasconcelos, aos funcionários Renato, Miraneide, Mauri, Edson, Phillipe, Oriel, Daniel, Tainá e Roberta. Aos colegas do curso, Leonardo, George, Claudomir, Sami, Jorge, Diego, Ianna, Aguiar, Jackson, Bruno, Tahim e Ítalo, que mesmo durante a pandemia mantivemos ciclos de estudos online. À Gisele e Ranara, companheiras de laboratório, dos grandiosos esforços na coleta de dados no LATIQ e na parceria em dois artigos. Aos doutores e ex-alunos do GIQ Franklin e Geovan, que de forma colaborativa me passaram informações sobre as boas práticas no laboratório que, juntamente a parceria do IFCE representado pelos professores Glendo, Fábio e Glaucionor, nos ajudaram com recursos materiais para as atividades no laboratório.

Ao amigo Gilvan, que durante o período inicial sem bolsa no programa de doutorado, ajudou-me financeiramente permitindo que o meu foco fosse apenas nos estudos e pesquisa. A minha cunhada Jeane Mary que muitas vezes me emprestou o carro para atravessar a cidade em direção ao campus do Pici, poupando-me 3 horas diárias desperdiçadas com deslocamento.

Aos meus irmãos, familiares e amigos que me incentivaram emocionalmente a retornar à universidade após 18 anos de afastamento, para dar continuidade ao aperfeiçoamento acadêmico.

“A consciência da ignorância e da dúvida, conduzida pelo método, nos farão chegar à verdade científica.”

Dary Alves Oliveira

RESUMO

A presente tese versa sobre distribuição quântica de chaves e está dividida em uma parte teórica e uma parte experimental. Na parte teórica, a função W_q de Lambert-Tsallis é utilizada para encontrar a fórmula analítica do comprimento de canal que maximiza a taxa de transmissão de bits seguros em uma rede óptica com sinais clássicos e quânticos trafegando na mesma fibra, em comprimentos de onda diferentes, e considerando o espalhamento Raman espontâneo. Em seguida W_q é utilizada para calcular a flutuação de portadores em um modulador de amplitude integrado em SiO_2 usado em QKD de variáveis contínuas, e no cálculo do parâmetro que modela um canal quântico estocástico de transmissividade com distribuição uniforme. Por fim, um novo protocolo de distribuição quântica de chaves chamado QKD baseado em disentropia, foi proposto. Este protocolo utiliza modulação de amplitude e detecta a presença de espionagem utilizando a disentropia. É o segundo protocolo de QKD que não utiliza a taxa de erro para detectar espionagem e é também o de mais simples implementação prática, embora possa não ser seguro contra ataques de espionagem que utilizem uma eficiente contagem de fótons. Na parte experimental, são apresentados os resultados experimentais de um detector de fótons controlado remotamente por luz.

Palavras-chave: distribuição quântica de chaves, função w_q de lambert-tsallis, disentropia, aleatoriedade.

ABSTRACT

This work is about quantum key distribution and it is divided in theoretical and experimental parts. In the theoretical part, the Lambert-Tsallis W_q function is used to find the analytical formula for the channel's length that maximizes the secure bit transmission rate in an optical network with classical and quantum signals in the same optical fiber, using different wavelengths, and taking into account the spontaneous Raman scattering. Following, W_q is used to calculate the fluctuation of carriers in a SiO_2 integrated amplitude modulator used in continuous variable QKD, as well in the calculation of the parameter that models a stochastic quantum channel with transmissivity with uniform distribution. At last, a new quantum key distribution protocol, named disentropy-based QKD, is proposed. This protocol uses only amplitude modulation and it detects the eavesdropping action by calculating the disentropy. It is the second QKD protocol that does not use quantum error rate to detect the eavesdropping and it is also the QKD protocol with the simplest implementation ever proposed. However, it may not be secure against eavesdropping techniques that employing efficient photon counting. In the experimental part, the experimental results of a remotely controlled single-photon detector is presented.

Keywords: quantum key distribution, lambert-tsallis w_q function, disentropy, randomness.

SUMÁRIO

INTRODUÇÃO

O surgimento de novas ferramentas matemáticas permite a obtenção de soluções analíticas para problemas cuja solução só era obtida por métodos numéricos. Uma dessas novas ferramentas matemáticas é a função W_q de Lambert-Tsallis. A função W_q é útil na solução de problemas nos quais as variáveis dependente e independente estão relacionadas por uma lei de potência. Assim, a função W_q de Lambert-Tsallis tem sido utilizada para encontrar soluções analíticas de problemas em física de semicondutores, eletrônica, óptica quântica, relatividade, dentre outras áreas. A função W_q também é utilizada na definição matemática da disentropia, que pode ser compreendida como uma medida de ordem ou de certeza, em outras palavras, pode-se dizer que a disentropia realiza o papel oposto ao da entropia. Contudo, matematicamente, essa relação não é dual visto que a entropia é descrita por uma função logarítmica que não responde com resultados reais a argumentos negativos, enquanto a disentropia é descrita pela função W_q que responde com valores reais a argumentos negativos desde que estejam dentro de um determinado intervalo. Devido a esse comportamento, a disentropia tem sido utilizada em problemas onde a entropia não pode ser utilizada, como por exemplo, na definição de uma medida de *quantumness*: a disentropia da função de Wigner. E na definição de uma medida de aleatoriedade: a disentropia da autocorrelação. Desta forma, a disentropia tem sido utilizada em problemas de mecânica estatística, astronomia, processamento de imagens, comunicação e computação quânticas, dentre outras áreas.

A presente tese está focada em aplicações da função W_q e da disentropia em distribuição quântica de chaves (QKD). De forma específica, a função W_q é utilizada na determinação analítica de parâmetros de canal em redes de QKD, e na modelagem de dispositivos optoeletrônicos (modulador de amplitude integrado em chip de SiO_2) utilizados em QKD. Além disso, a disentropia é utilizada no desenvolvimento de um novo protocolo de QKD que não usa a taxa de erro de bit para detectar a presença de espionagem no canal. Por fim, paralelo ao trabalho teórico, resultados experimentais de um detector de fótons controlado remotamente por luz também são apresentados. A descrição dos tópicos desta tese será apresentada abaixo.

No tópico 2 é feita uma revisão da função W_q de Lambert-Tsallis, bem como as soluções analíticas de dois circuitos são obtidas através do uso de W_q. O primeiro circuito é composto de uma fonte de tensão contínua, um resistor e um nanofio modelado pela equação de Mark-Helfrich. O segundo circuito é composto de uma fonte de tensão contínua, um resistor e um diodo modelado pela equação de Shockley.

O tópico 3 traz três aplicações da função W_q em distribuição quântica de chaves. Primeiramente, um rede quântica de acesso na configuração downstream e com sinais clássicos e quânticos na mesma fibra mas em comprimentos de onda diferentes, é considerada. Nesta, a função W_q é utilizada para determinar o comprimento de canal que maximiza a taxa de transmissão de bits seguros. Em seguida, considerando um modulador de amplitude integrado em chip de SiO_2 utilizado em distribuição quântica de chaves com variáveis contínuas, a função W_q é usada para calcular a flutuação de portadores em função da tensão aplicada no modulador. Por fim, a função W_q é utilizada para calcular o parâmetro que modela um canal estocástico com distribuição uniforme da transmissividade.

O tópico 4 apresenta o primeiro protocolo de distribuição quântica de chaves que não usa a taxa de erro para detecção de espionagem. O protocolo proposto, chamado de QKD baseado em disentropia, usa a aleatorieade da chave obtida por Bob (o receptor), medida pela disentropia, para inferir a presença de um(a) espião(ã) no canal. Adicionalmente, esse novo protocolo de QKD possui a implementação mais simples e barata dentre todos os protocolos já propostos.

No tópico 5, no intuito de facilitar o sincronismo entre Alice (transmissor) e Bob nas configurações de QKD sem comprometer a segurança do protocolo, são apresentados resultados experimentais de um detector de fótons baseado em fotodiodos de avalanche, que permite que Alice ative remotamente por luz os APDs de Bob.

Por fim, as conclusões e perspectivas de futuros trabalhos são mostradas no tópico 6. Em seguida as referências utilizadas na criação da tese bem como os anexos A e B, que apresenta em detalhes os principais cálculos do tópico 3 e os trabalhos decorrentes desta tese.

A FUNÇÃO W DE LAMBERT E W_Q DE LAMBERT-TSALLIS

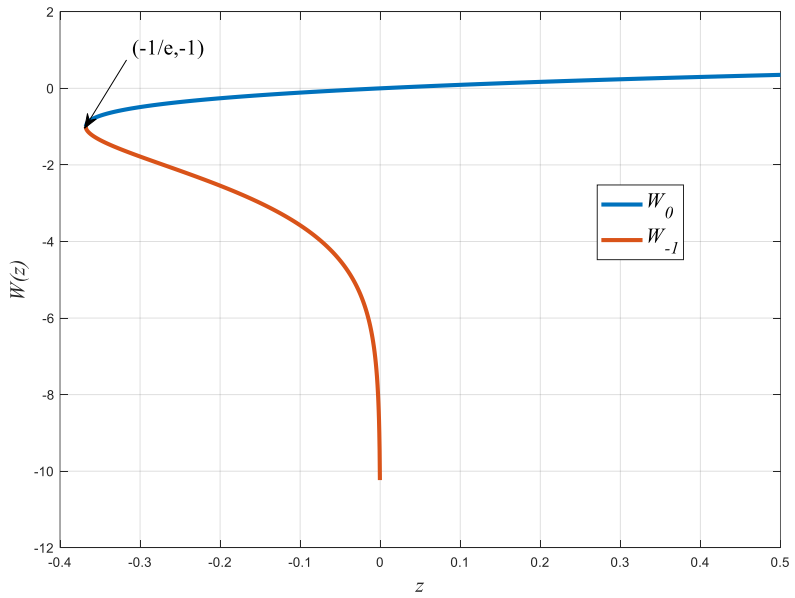
2.1 A Função W de Lambert

A função $W(z)$ definida para os complexos z, é uma função que resolve a seguinte equação

$$W(z)e^{W(z)} = z\,. \tag{2.1}$$

A $W(z)$ de Lambert pode usada para encontrar soluções analíticas em problemas de matemática, física e ciência da computação (1, 2). Existem infinitas soluções para $W(z)$ e estas são diferenciadas por um número inteiro que representam o ramo de W, ou seja, $W_t(z)$, t = 0, ±1, ±2, ±3... Dentre todas as soluções, as que possuem maior aplicabilidade na física e na engenharia são as que são reais. Elas ocorrem somente quando t = 0 e t =-1, $W_0(z)$ e $W_{-1}(z)$, e ocorrem apenas quando z é real. Os ramos $W_0(z)$ e $W_{-1}(z)$ são mostrados na Fig. 2.1.

Figura 2.1. $W(z)$ versus z.



Fonte: Elaborada pelo autor.

Como pode ser observado na Fig. 2.1, na faixa $-1/e \leq z \leq 0$ existem dois ramos reais de $W(z)$. O ramo satisfazendo $W(z) \geq -1$ é o ramo principal chamado $W_0(z)$ enquanto o ramo

satisfazendo $W(z) \leq -1$ é chamado de $W_{-1}(z)$. Para $z > 0$ só $W_0(z)$ é real e para $z < -1/e$ não há soluções reais. Portanto, $0 < W_{-1}(z) < -1$ para $-1/e \leq z < 0$, e $-1 < W_0(z) < +\infty$ para $-1/e \leq z < +\infty$. O ponto ($z_b = -1/e$, $W(z_b) = -1$) é chamado ponto de Branch. Ele é obtido calculando-se $dW/dz = \infty$. É também o ponto onde $W_{-1}(z) = W_0(z)$.

A utilização da função $W(z)$ na solução de problemas matemáticos requer que o referido problema seja escrito na forma da eq. (2.1). Alguns exemplos são mostrados abaixo (3)

I) Por definição, a solução de $ye^y = x$ é $y = W(x)$, ou seja

$$ye^y = x \rightarrow W\left(ye^y\right) = W\left(x\right) \rightarrow y = W\left(x\right). \tag{2.2}$$

II)

$$y\ln\left(y\right) = x \rightarrow y = e^{x/y} \rightarrow 1 = \frac{1}{y}e^{x/y} \rightarrow x = \frac{x}{y}e^{x/y} \rightarrow W\left(x\right) = W\left(\frac{x}{y}e^{x/y}\right)$$

$$\rightarrow W\left(x\right) = \frac{x}{y} \rightarrow y = \frac{x}{W\left(x\right)}. \tag{2.3}$$

III)

$$y\ln\left(y\right) = x \rightarrow x = \ln\left(y\right)e^{\ln(y)} \rightarrow W\left(x\right) = W\left[\ln\left(y\right)e^{\ln(y)}\right] \rightarrow W\left(x\right) = \ln\left(y\right) \rightarrow y = e^{W(x)} \tag{2.4}$$

IV)

$$\frac{\ln\left(y\right)}{y} = x \rightarrow \ln\left(y\right) = xy \rightarrow y = e^{xy} \rightarrow -xy = -xe^{xy} \rightarrow -xye^{-xy} = -x$$

$$\rightarrow W\left(-xye^{-xy}\right) = W\left(-x\right) \rightarrow -xy = W\left(-x\right) \rightarrow y = -\frac{W\left(-x\right)}{x}. \tag{2.5}$$

Uma generalização de $W(z)$ é obtida substituindo-se na eq. (2.1) a função exponencial pela função q-exponencial de Tsallis. Esta é definida como (4, 5)

$$e_q^z = \begin{cases} e^z & \text{se } q = 1 \\ \left[1+(1-q)z\right]^{1/(1-q)} & \text{se } q \neq 1 \ \& \ 1+(1-q)z > 0. \\ 0 & \text{se } q \neq 1 \ \& \ 1+(1-q)z \leq 0 \end{cases} \tag{2.6}$$

O parâmetro q, um número real, é chamado de parâmetro de não extensividade de Tsallis. A principal propriedade de e_q^x usada neste trabalho é a seguinte

$$\left(e_q^x\right)^\alpha = \left\{\left[1+(1-q)x\right]^{1/(1-q)}\right\}^\alpha = \left[1+(1-q)x\right]^{\alpha/(1-q)} = \left[1+\frac{(1-q)}{\alpha}\alpha x\right]^{\alpha/(1-q)} = e_{1-(1-q)/\alpha}^{\alpha x} \tag{2.7}$$

De (2.7) pode-se observar, por exemplo, que $e_q^x e_{2-q}^{-x} = 1$. A função inversa da q-exponencial é o logaritmo natural de Tsallis, definido como sendo

$$\ln_q(x) = \begin{cases} \ln(x) & x > 0 \ \& \ q = 1 \\ \dfrac{x^{(1-q)}-1}{1-q} & x > 0 \ \& \ q \neq 1 \\ \text{não definido} & x \leq 0 \end{cases}. \tag{2.8}$$

Assim,

$$e_q^{\ln_q(x)} = x \text{ para } x > 0 \tag{2.9}$$

$$\ln_q\left(e_q^x\right) = x \text{ para } 0 < e_q^x < \infty. \tag{2.10}$$

2.2 A Função W_q de Lambert-Tsallis

A função W_q de Lambert-Tsallis é a função que resolve a seguinte equação:

$$W_q(z)e_q^{W_q(z)} = z \tag{2.11}$$

As soluções de (2.11) são as funções W_q de Lambert-Tsallis introduzida em (3). Para q = 1 tem-

se $e_{q=1}^{z} = e^{z}$ e $W_{q\to 1}(z) = W(z)$. Usando a definição da função q-exponencial descrita em (2.6) em (2.11) pode-se encontrar uma expressão analítica de $W_q(z)$ para alguns valores especiais de q:

$$W_q^{(1-q)} + (1-q)W_q^{(2-q)} - z^{(1-q)} = 0. \tag{2.12}$$

No caso mais simples, $q = 2$, tem-se

$$W_2(z) = \frac{z}{z+1}, \tag{2.13}$$

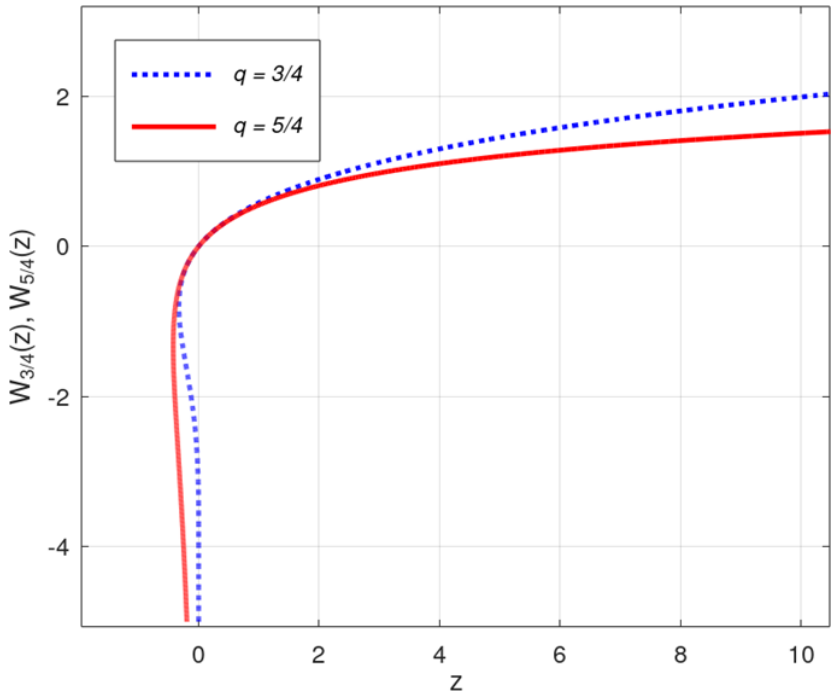
para $z \in (-1, +\infty)$.

Para $q = 3/2$ tem-se

$$W_{\frac{3}{2}}^{\pm}(z) = \frac{2(z+1) \pm 2\sqrt{2z+1}}{z} \tag{2.14}$$

A função $W_{3/2}^{+}(z)$ satisfaz a eq. (2.11) no intervalo $z \in$ [-1/2,∞), enquanto a função $W_{3/2}^{-}(z)$ satisfaz a eq. (2.11) no intervalo $z \in$ [-1/2,0). Pode-se mostrar que o ponto de ramificação da função W_q de Lambert-Tsallis é ($z_b = \exp_q(1/(q\text{-}2))/(q\text{-}2)$, $W_q(z_b) = 1/(q\text{-}2)$), para $q \neq 2$. Não há ponto de ramificação com z_b finito para $q = 2$. Assim, o ponto de ramificação para $q = 3/2$ possui $z_b = -½$. De forma geral, a solução no intervalo [z_b , 0) é $W_q^{-}(z)$ enquanto a solução no intervalo [z_b, ∞) é $W_q^{+}(z)$. As curvas de $W_q(z)$ versus z para $q = 3/4$ e $q = 5/4$ são mostradas na Fig. 2.2.

Figura 2.2. $W_q(z)$ versus z para q = 3/4 (linha pontilhada) e q = 5/4 (linha contínua).



Fonte: Elaborada pelo autor.

A utilização da função $W_q(z)$ na solução de problemas matemáticos requer que o referido problema seja escrito na forma da eq. (2.11). Alguns exemplos são mostrados abaixo (6).

I) $x^5 + Ax + B = 0$

Colocando x^5 em evidencia e subtraindo B em ambos os lados da igualdade, temos

$$x^5(1 + Ax^{-4}) = -B \qquad (2.15a)$$

Considerando a relação $1 + z = e_0^z$ e substituindo na eq. (2.15a), tem-se

$$x^5 e_0^{Ax^{-4}} = -B. \qquad (2.15b)$$

Elevando ambos os lados da eq. (2.15b) por -4/5, tem-se

$$\left[x^5 e_0^{Ax^{-4}}\right]^{\frac{-4}{5}} = (-B)^{\frac{-4}{5}}. \tag{2.15c}$$

utilizando a relação (2.7) em (2.15c) chega-se a

$$x^{-4} e^{\frac{\frac{-4}{5}Ax^{-4}}{1-\frac{(1-0)}{\frac{-4}{5}}}} = (-B)^{\frac{-4}{5}}. \tag{2.15d}$$

Multiplicando ambos os lados da eq. (2.15d) por $\frac{-4}{5}A$ resulta em

$$\frac{-4}{5}Ax^{-4} e_{\frac{9}{4}}^{\frac{-4}{5}Ax^{-4}} = \frac{-4}{5}A(-B)^{\frac{-4}{5}}. \tag{2.15e}$$

Portanto, usando-se a definição de $W_q(z)$ chega-se finalmente a

$$\frac{-4}{5}Ax^{-4} = W_{\frac{9}{4}}\left(\frac{-4}{5}AB^{\frac{-4}{5}}\right)$$

$$x^{-4} = \frac{-5}{4A}W_{\frac{9}{4}}\left(\frac{-4}{5}AB^{\frac{-4}{5}}\right)$$

Finalmente,

$$x = \left[\frac{-5}{4A}W_{\frac{9}{4}}\left(\frac{-4}{5}AB^{\frac{-4}{5}}\right)\right]^{-\frac{1}{4}}. \tag{2.15f}$$

II) $\frac{e^x + ae^{-x}}{2} = y$

Colocando e^x em evidência, tem-se

$$\frac{1}{2}e^{x}(1+ae^{-2x})=y \tag{2.16a}$$

Considerando a relação $1+x=e_0^x$ e substituindo na eq. (2.16a), obtêm-se

$$\frac{1}{2}e^{x}e_0^{ae^{-2x}}=y \tag{2.16b}$$

Elevando ambos os lados da eq. (2.16b) por -2, chega-se a

$$\left[\frac{1}{2}e^{x}e_0^{ae^{-2x}}\right]^{-2}=y^{-2} \tag{2.16c}$$

utilizando a eq. (2.7) em (2.16c) resulta em

$$4e^{-2x}e_{1-\frac{(1-0)}{-2}}^{-2ae^{-2x}}=y^{-2} \tag{2.16d}$$

Multiplicando ambos os lados da eq. (2.16d) por $\frac{-1}{2}a$, resulta em

$$-2ae^{-2x}e_{\frac{3}{2}}^{-2ae^{-2x}}=\frac{-a}{2}y^{-2}. \tag{2.16e}$$

Por fim, usando-se a definição de $W_q(z)$ chega-se finalmente a

$$-2ae^{-2x}=W_{\frac{3}{2}}\left(\frac{-a}{2}y^{-2}\right)\Longrightarrow x=\frac{-1}{2}ln\left[\frac{-1}{2a}W_{\frac{3}{2}}\left(\frac{-a}{2}y^{-2}\right)\right]. \tag{2.16f}$$

III) $x(1+x)^{\pi/2}=z$

$$x(e_0^x)^{\pi/2}=z \tag{2.17a}$$

$$x e^{\frac{\pi}{2} x}_{1-\frac{2}{\pi}} = z \tag{2.17b}$$

$$\frac{\pi}{2} x e^{\frac{\pi}{2} x}_{1-\frac{2}{\pi}} = \frac{\pi}{2} z \tag{2.17c}$$

$$\frac{\pi}{2} x = W_{1-\frac{2}{\pi}}\left(\frac{\pi}{2} z\right) \Longrightarrow x = \frac{2}{\pi} W_{1-\frac{2}{\pi}}\left(\frac{\pi}{2} z\right). \tag{2.17d}$$

A função $W_q(z)$ de Lambert-Tsallis pode ser numericamente calculada usando o método de Halley (3):

$$w_q(j+1) = w_q(j) - \frac{\left[w_q(j) e_q^{w_q(j)} - z\right]}{\left[e_q^{w_q(j)} + w_q(j) e^{q w_q(j)}_{2-\frac{1}{q}}\right] - \Delta} \tag{2.18}$$

$$\Delta = \frac{\left[w_q(j) e_q^{w_q(j)} - z\right]\left[2 e^{q w_q(j)}_{2-\frac{1}{q}} + \frac{w_q(j)}{q} e^{(2q-1) w_q(j)}_{\frac{3-2/q}{2-1/q}}\right]}{2\left[e_q^{w_q(j)} + w_q(j) e^{q w_q(j)}_{2-\frac{1}{q}}\right]} \tag{2.19}$$

O seguinte código escrito em MATLAB/OCTAVE encontra o valor de $W_q(z)$:

```
for n=1:1000
  A=(w.*Expq(w,q)-z);
  B=Expq(w,q)+w.*Expq(q*w,2-1/q);
  C=2*Expq(q.*w,2-1/q)+(w./q)*Expq((2*q-1).*w,(3-2/q)/(2-1/q));
  w = w – A./(B-(A.*C)/(2*B));
end
```

A convergência do método numérico acima depende de uma boa estimativa do valor inicial usado no primeiro passo. No algoritmo acima '*w*' é a estimativa inicial e '*Expq*(*z*,*q*)' é a função que implementa a eq. (2.6).

2.3 Entropia e Disentropia

A entropia é um conceito chave para a física e para a engenharia. Na engenharia ela é o ponto central da Teoria da Informação. Basicamente ela quantifica a incerteza associada a uma variável aleatória. Seja uma variável aleatória *X* que pode assumir os diferentes valores x_i, $i = \{1, \ldots, n\}$, com probabilidade p_i. A entropia de Shannon para essa distribuição de probabilidade discreta é dada por

$$H(X) = -\sum_i p_i \log_2 p_i \tag{2.20}$$

Se a variável assumir apenas dois valores distintos, $X = X_0$ e $X = X_1$, tem-se que $P(X = x_0) = p$ e $P(X = x_1) = 1 - p$. Nesta situação, a entropia de *X* fica da seguinte forma

$$H(X) = -p\log(p) - (1-p)\log(1-p) \tag{2.21}$$

A entropia é máxima quando os eventos são equiprováveis. No caso de (2.21), $p = (1\text{-}p) = 1/2$. Neste caso, a entropia $H(X)$ é igual a 1 bit. Por outro lado, a entropia é mínima quando a distribuição de probabilidade é uma função delta de Kronecker, isto é, uma das probabilidades vale '1' e todas as demais são nulas, o que implica que não há nenhuma incerteza no resultado do evento. Por fim, a entropia de Shannon pode ser generalizada pela entropia de Tsallis, dada por

$$S(X) = -\sum_i p_i^q \ln_q p_i \tag{2.22}$$

Usando a relação da eq. (2.8) em (2.11) pode-se encontrar uma relação entre $W_q(z)$ e $\ln_q(z)$, o que permite escrever a entropia de Tsallis dada em (2.22) em função de $W_q(z)$:

$$S(X) = -\sum_i \left[p_i^q W_q(p_i) +_q p_i^q \ln_q W_q(p_i) \right] \tag{2.23}$$

Em (2.23) a operação *q*-soma é dada por: $A +_q B = A + B + (1\text{-}q)AB$. O primeiro termo de (2.23) é chamado de disentropia (6):

$$D(X) = \sum_i p_i^q W_q(p_i) \tag{2.24}$$

A disentropia pode ser entendida como um conceito oposto ao da entropia. Assim, a disentropia mede o grau de certeza. A disentropia é máxima quando a distribuição de probabilidade é uma função delta de Kronecker e mínima quando a distribuição de probabilidade é uniforme. Embora a entropia e a disentropia aparentemente tenham papéis duais (se um problema pode ser resolvido maximizando (minimizando) a entropia, o mesmo problema pode ser resolvido minimizando (maximizando) a disentropia, existem problemas em que a disentropia pode ser utilizada e a entropia não pode. Isso acontece porque a disentropia usa a função W_q que aceita valores negativos em seu argumento se este for maior que o valor da abcissa do ponto de ramificação. Em particular, para $q = 2$, o argumento pode ser negativo no intervalo (0,-1).

2.4 Disentropia da Autocorrelação e Aleatoriedade

Um desses problemas onde a entropia não pode ser usada é a medida de aleatoriedade proposta em (7). Basicamente, a medida de aleatoriedade de um sinal $s(t)$ é a disentropia da autocorrelação do sinal ($R(\tau)$ para sinal contínuo e R_n para sinal discreto) com $q = 2$:

$$D_2 = \int_{-\infty}^{\infty} \frac{R^3(\tau)}{R(\tau)+1} d\tau \,, \tag{2.25}$$

$$D_2 = \sum_n \frac{R_n^3}{R_n+1} \tag{2.26}$$

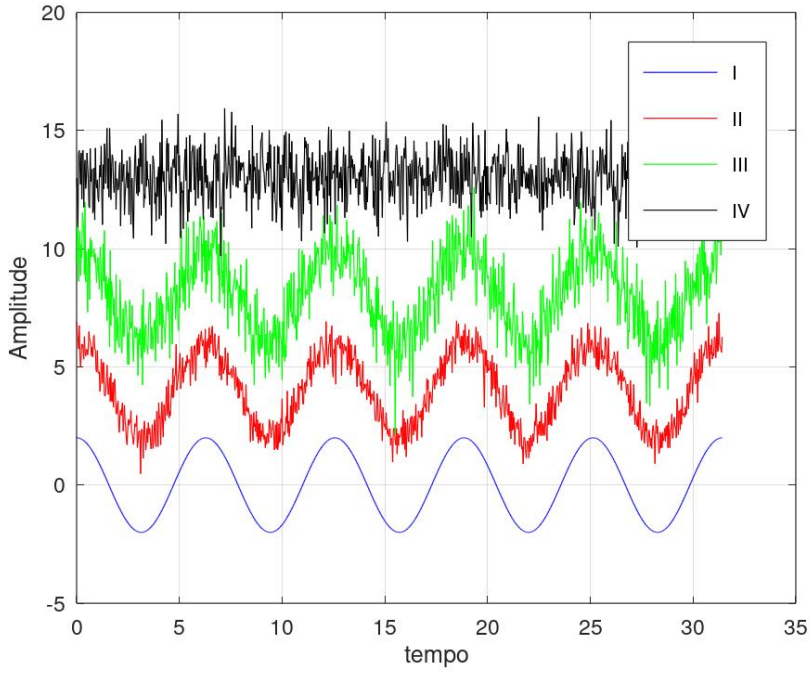
O valor de D_2 é mínimo (igual a 0.5) quando o sinal $s(t)$ for um ruído branco. Quanto maior o valor de $|D_2|$, menos aleatório é o sinal. A Fig. 2.4 mostra quatro sinais e a Tabela 2.1 mostra seus respectivos valores de aleatoriedade calculados com a disentropia da autocorrelação.

Tabela 2.1. Valores da aleatoriedade dos sinais mostrados na Fig. 2.3. $N(x,y)$ é um ruído Gaussiano de média x e variância y.

	$s(t)$	Aleatoriedade - $D_2(r(s(t)))$
I	**$2\cos(t)$**	**440.5509**
II	**$4 + 2\cos(t) + N(0,0.25)$**	**177.8085**
III	**$8 + 2\cos(t) + N(0,1)$**	**40.8840**
IV	**$13 + N(0,1)$**	**0.4945**

Fonte: Elaborada pelo autor.

Fig. 2.3. Sinais com diferentes níveis de ruído (Tabela 2.1) para o cálculo da aleatoriedade usando a disentropia da autocorrelação.



Fonte: Elaborada pelo autor.

A medida de aleatoriedade baseada na disentropia da autocorrelação já foi utilizada, por exemplo, para determinar a aleatoriedade do sinal emitido por um pulsar (8) e para descrever um protocolo de distribuição quântica de chaves no qual a ação de um espião pode ser inferida a partir da variação da aleatoriedade da chave obtida (9). Neste trabalho usou-se a disentropia da autocorrelação para calcular a aleatoriedade das chaves obtidas por Alice e Bob.

2.5 Aplicações de W_q em física de semicondutores e eletrônica

Em geral, obter as soluções analíticas da relação corrente-tensão, $I(V)$, de um circuito ou de nanoestruturas semicondutoras não é uma tarefa trivial. Para o circuito eletrônico simples composto por uma fonte de alimentação CC, um resistor e um diodo modelado pela equação de diodo de Shockley, a solução analítica para a corrente é baseada na função W de Lambert. Isso acontece porque no modelo de Shockley, a corrente que passa pelo diodo varia exponencialmente com a tensão nos terminais do diodo e a resistência em série no circuito não altera esse comportamento. O sucesso da função de Lambert na resolução de equações exatas ou aproximadas de circuitos pode ser medido pelo número de trabalhos encontrados na literatura (6-10). No entanto, em algumas situações, o dispositivo semicondutor possui uma relação não exponencial entre corrente e tensão, como a corrente limitada por carga espacial ("Space Charge Limited Current" - SCLC) em diodos, células solares e em algumas nanoestruturas (12-20, 24, 25). Nesses casos, a função Lambert não pode ser usada. Outra situação em que a função Lambert não é útil é quando um capacitor é colocado em série com um resistor e um diodo. Neste caso, a relação corrente-tensão também é não exponencial. Nessa direção, a presente tese traz a solução analítica para esses dois casos: 1) A SCLC versus tensão aplicada em um nanofio; 2) O circuito resistor-capacitor-diodo (RCD). Em ambos os casos as soluções analíticas dependem da função W_q de Lambert-Tsallis. Isso acontece porque em ambos os casos há uma dependência na forma de lei da potência entre a corrente do circuito e a tensão aplicada.

2.5.1 Corrente limitada por carga espacial (SCLC)

O mecanismo de transporte SCLC ocorre quando os contatos são capazes de injetar mais carga em um material do que a carga intrínseca. Este excesso de carga injetada controla o fluxo de corrente (12-22). O SCLC pode ocorrer em materiais livres de armadilhas (defeitos no semiconduitor) e materiais com armadilhas. No primeiro caso, para semicondutores, a relação I-V é dada pela lei de Mott-Gurney (23) .

$$J = \frac{9}{8}\varepsilon\mu\frac{V^2}{L^3}, \tag{2.27}$$

sendo ε a permissividade dielétrica do material, μ é a mobilidade do portador de carga, L é o comprimento do canal e V é a tensão aplicada. Por outro lado, a SCLC em nanofios com $L/R_d >> 1$, onde L e R_d são, respectivamente, o comprimento e o raio do nanofio, tem-se ($\zeta_0 \approx 1$) (24, 25)

$$J = \zeta_0 \left(\frac{R_d}{L} \right)^{-2} \varepsilon\mu \frac{V^2}{L^3}. \tag{2.28}$$

Deve-se notar que o transporte de carga em um semicondutor não é controlado por um único mecanismo. A mecânica SCLC ocorre em paralelo com o mecanismo Ôhmico ($J = ne\mu V/L$), por exemplo. No entanto, dependendo da tensão aplicada, um mecanismo de transporte pode ser o dominante. Portanto, neste trabalho estamos considerando apenas o SCLC como a mecânica de transporte de carga dominante.

Como se pode notar nas eqs. (2.27) e (2.28), ambos têm a mesma dependência da tensão aplicada e podem ser simplificados para $I = kV^2$, onde $I = JA$ (doravante A é a área efetiva que as cargas em movimento cruzam) e k é uma constante que leva em consideração os parâmetros geométricos e de propriedades do material. Se a estrutura semicondutora for colocada em um circuito elétrico com um resistor em série R e uma fonte de alimentação CC, a equação a ser resolvida para obter a relacao $I(V)$ é

$$I = k\left(V - RI\right)^2. \tag{2.29}$$

A eq. (2.29) pode ser facilmente resolvida usando métodos tradicionais. A corrente I é uma das raízes do polinômio $I^2 - (2V + (Rk^2)^1)I + V^2/R = 0$. Por outro lado, usando (2.11) e (2.6), a solução pode também ser escrita como $I = -[V/(2R)]W_0^{\pm}(-2Rk)$. Deve-se notar que $W_q(x) < 0$ quando $x < 0$. Como este resultado é trivial, não consideraremos mais detalhes sobre a SCLC livre de armadilhas.

Durante o crescimento dos nanofios, podem ser formadas armadilhas na superfície, que causam a depleção dos portadores e, portanto, as propriedades de transporte dos nanofios são afetadas por essas armadilhas. Neste caso, a densidade e a distribuição de energia das armadilhas são parâmetros importantes a serem considerados na modelagem da SCLC. Para

armadilhas que são distribuídas exponencialmente dentro do intervalo de banda de energia, a densidade da armadilha pode ser escrita como (12)

$$n_t(E) = \frac{N_t}{k_B T_c} \exp\left(-\frac{E}{k_B T_c}\right), \tag{2.30}$$

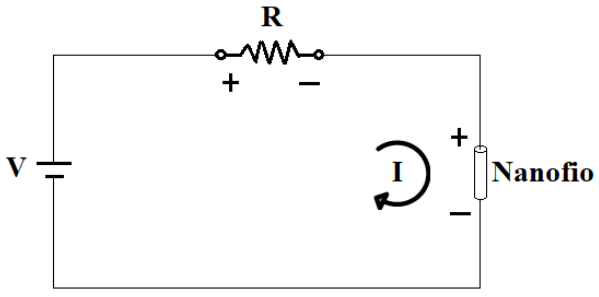
na qual E é a energia relativa medida a partir da parte inferior da banda de condução (considerando os buracos como portadores de carga), N_t é a densidade da armadilha, $E_t = k_B T_c$ é a constante característica da distribuição e T_c é a temperatura característica da armadilha. Neste caso, se apenas um tipo de portador de carga for considerado, μ é independente do campo e a concentração de portadores de carga livres é muito menor que a concentração de portadores de carga aprisionados (12), a relação *I-V* é dada pela equação de Mark-Helfrich (16)

$$J = q_e^{1-l} \mu N_{eff} \left(\frac{\varepsilon_r \varepsilon_0 l}{N_t (l+1)}\right)^l \left(\frac{2l+1}{l+1}\right)^{l+1} \frac{V^{l+1}}{L^{2l+1}}, \tag{2.31}$$

sendo q_e a carga elementar do elétron, $l = T_c/T$, T é a temperatura medida e N_{eff} é a densidade efetiva de estados do tipo portador de carga no semicondutor. Se o nanofio for colocado em um circuito elétrico com um resistor em série R e uma fonte de alimentação CC, como mostrado na fig. 2.4A, a equação a ser resolvida para obter a relação $I(V)$ é

$$I = A q_e^{1-l} \mu N_{eff} \left(\frac{\varepsilon_r \varepsilon_0 l}{N_t (l+1)}\right)^l \left(\frac{2l+1}{l+1}\right)^{l+1} \frac{(V - RI)^{l+1}}{L^{2l+1}}. \tag{2.32}$$

Figura 2.4A. Circuito elétrico formado por fonte de alimentação DC, resistor e nanofio



Fonte: Elaborada pelo autor.

A eq. (2.32) pode ser simplificada para

$$I = k(V - RI)^{l+1}. \tag{2.33}$$

Após algumas manipulações algébricas, a eq. (2.33) pode ser reescrita como

$$(l+1)\frac{RI}{V}e^{(l+1)\frac{RI}{V}}_{(l+2)/(l+1)} = k(l+1)RV^l \tag{2.34}$$

cuja solução é

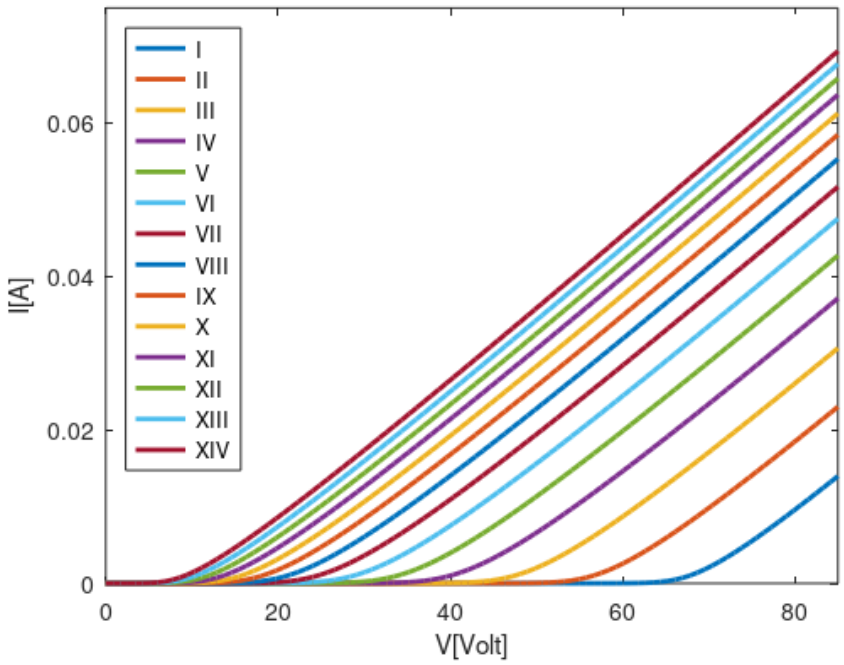
$$I = \frac{V}{R(l+1)}W_{(l+2)/(l+1)}\left(k(l+1)RV^l\right) \tag{2.35}$$

e, portanto, a solução de (2.32) é

$$I = \frac{V}{R(l+1)}W_{\frac{(l+2)}{(l+1)}}\left(\frac{Aq_e^{1-l}\mu N_{eff}}{L^{2l+1}}\left(\frac{\varepsilon_r\varepsilon_0 l}{N_t(l+1)}\right)^l\frac{(2l+1)^{l+1}}{(l+1)^l}RV^l\right) \tag{2.36}$$

A Fig. 2.4 mostra o gráfico da eq. (2.36) com os seguintes valores de parâmetros: $N_t = 2.4\times10^{17}\text{cm}^{-3}$, $T_c = 1670\text{K}$, $R = 1\text{k}\Omega$, $V \in \{0, 25\text{V}\}$, $L = 300\text{nm}$, $T \in \{100\text{-}300\text{K}\}$, $N_{eff} = 1.2\times10^{18}$. Quanto maior a temperatura, mais cedo aparece o joelho da curva.

Figura 2.4. *I* versus *V*. Na curva XIV $T = 300\text{K}$, enqunato que a curva I é para $T = 100\text{K}$.

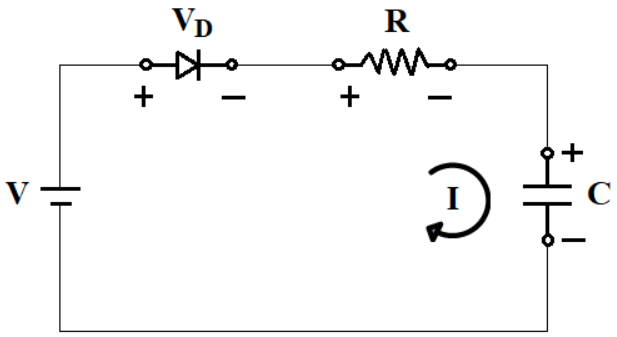


Fonte: Elaborada pelo autor.

2.5.2 O Circuito Resistor-Capacitor-Diodo

Nesta seção discutimos a relação $I(V)$ do circuito elétrico formado por uma fonte de alimentação CC, um diodo comum modelado pela equação de Shockley, um resistor e um capacitor, conforme mostrado na Fig. 2.5.

Figura 2.5. Circuito elétrico formado por fonte de alimentação DC, diodo, resistor e capacitor.



Fonte: Elaborada pelo autor.

A relação I-V da corrente do diodo é dada por

$$I = I_s\left[\exp\left(V_D/\eta V_T\right)-1\right], \tag{2.37}$$

na qual I_s é a corrente de saturação do diodo, V_D é a tensão entre os terminais do diodo, $V_T = k_BT/q_e$ é a tensão térmica e, por fim, η é o fator de idealidade do diodo ($1 < \eta < 2$ para diodos de silício). Aplicando a lei de Kirchhoff no circuito mostrado na Fig. 2.5 obtém-se

$$\left(\frac{Rk\left(I+I_s\right)+1}{Rk\left(I+I_s\right)}\right)\frac{dI}{dt}+\frac{I}{RC}=0, \tag{2.38}$$

uma vez que $dV/dt = 0$ (a fonte é CC). A solução da eq. (2.38) é

$$\frac{I^{b+1}}{\left(I+I_s\right)^b}=\frac{I_0^{b+1}}{\left(I_0+I_s\right)^b}e^{-\frac{t}{RC}}\ , \tag{2.39}$$

na qual $b = (RkI_s)^{-1}$ e $I_0 = I(t=0)$. Após algumas manipulações algébricas, a eq. (2.39) pode ser reescrita como

$$\frac{-bI}{(1+b)I_s}e^{\frac{-bI}{(1+b)I_s}}_{2+\frac{1}{b}} = \frac{-b}{(1+b)I_s}z^{\frac{1}{1+b}}I_s^{\frac{b}{1+b}}, \tag{2.40}$$

cuja solução é

$$I = -\frac{(1+b)I_s}{b}W_{2+\frac{1}{b}}\left[\frac{-b}{(1+b)I_s}z^{\frac{1}{1+b}}I_s^{\frac{b}{1+b}}\right] \tag{2.41a}$$

$$\text{com } z = I_0\left(1+I_s/I_0\right)^{-b}e^{-\frac{t}{RC}}. \tag{2.41b}$$

Assim, a solução de (2.39) é

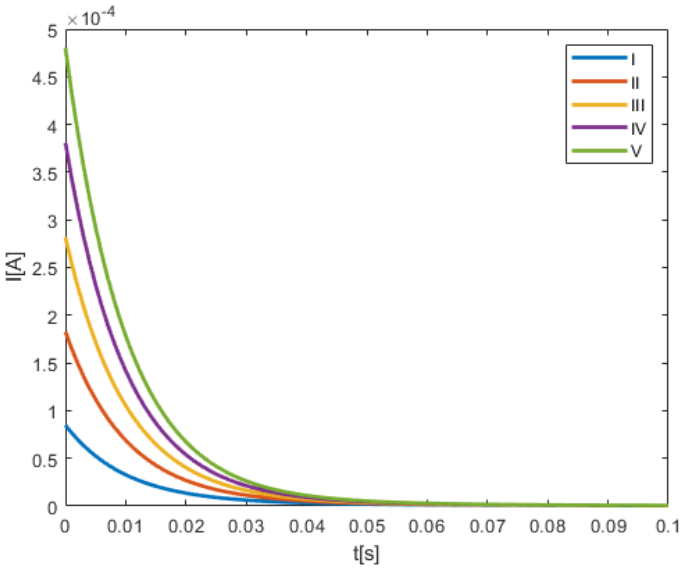
$$I = -\frac{(1+b)I_s}{b}W_{2+\frac{1}{b}}\left[\frac{-b}{(1+b)}I_s^{\frac{-1}{1+b}}\frac{I_0^{\frac{1}{1+b}}e^{-\frac{t}{(1+b)RC}}}{\left(1+I_s/I_0\right)^{\frac{b}{1+b}}}\right]. \tag{2.42}$$

Em $t = 0$, o capacitor não tem carga e o circuito pode ser visto como um circuito resistor-diodo, cuja corrente é dada por

$$I_0 = \frac{\eta V_T}{R}W\left(\frac{I_sR}{\eta V_T}e^{\frac{V+RI_s}{\eta V_T}}\right) - I_s. \tag{2.43}$$

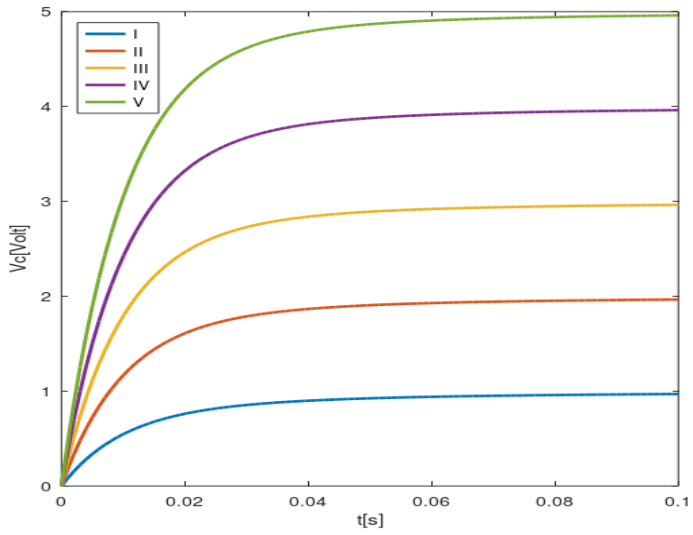
Portanto, as eqs. (2.42)-(2.43) fornecem a solução completa para a corrente no circuito RCD. Para mostrar os resultados fornecidos pelas eqs. (2.42)-(2.43), as Figs. 2.6 e 2.7 mostram, respectivamente, a corrente elétrica, I, e a tensão entre os terminais do capacitor, $V_c = V - RI - V_T\ln(I/I_s+1)$. Os valores dos parâmetros utilizados foram: $R = 10\text{k}\Omega$, $C = 1\mu\text{F}$, $I_s = 2.5\times10^{-7}$ A, $V_T = 0{,}026$V, $\mu = 1$ e $V = [1\text{V}, 2\text{V}, 3\text{V}, 4\text{V}, 5\text{V}]$. Usando esses valores, obtém-se $q = 2 + 1/b = 2 + 1/kRI_s = 2{,}0962$. Quanto maior for a tensão de alimentação, maior será o valor inicial da corrente e maior será o valor final de V_c.

Figura 2.6. Corrente elétrica no circuito mostrado na Fig. 2.5. Os valores da fonte de alimentação são: I – 1V, II – 2V, III – 3V, IV – 4V, V – 5V.



Fonte: Elaborada pelo autor.

Figura 2.7 – Tensão entre terminais do capacitor no circuito mostrado na Figura 2.5. Os valores de alimentação são: I – 1V, II – 2V, III – 3V, IV – 4V, V – 5V.



Fonte: Elaborada pelo autor.

As Figs. 2.6 e 2.7 mostram, respectivamente, a diminuição não exponencial da corrente e o aumento da tensão no capacitor.

APLICAÇÕES DA FUNÇÃO DE LAMBERT-TSALLIS EM QKD

3.1 Introdução

A tecnologia comercialmente disponível conhecida como Distribuição Quântica de Chaves (QKD) possibilita a transmissão segura de bits do remetente (Alice) para o destinatário (Bob) (26-30). A implementação de QKD em redes ópticas reais enfrenta desafios consideráveis que requerem superação. Dois desses desafios são: I) a coexistência de dados clássicos e quânticos na mesma rede óptica e II) a correta estimativa dos parâmetros necessários para o protocolo de QKD de variável contínua (CV-QKD).

No que diz respeito à coexistência de dados clássicos e quânticos que percorrem a mesma fibra óptica, o espalhamento Raman espontâneo surge como o principal ruído, limitando o comprimento máximo do canal. Por outro lado, a estimativa incorreta da transitividade do canal e do ruído excessivo no protocolo CV-QKD pode resultar em vulnerabilidades que facilitam atividades de espionagem. Essa estimativa inadequada de parâmetros pode ser causada por moduladores ópticos não ideais ou pela presença de um canal estocástico, onde a transmissividade é uma variável aleatória.

Este capítulo apresenta três aplicações da função W_q de Lambert-Tsallis em QKD. Inicialmente, é realizada uma análise do impacto do espalhamento Raman espontâneo em um protocolo QKD, calculando analiticamente o comprimento de fibra necessário para alcançar um nível específico de potência. Em seguida, utilizando a função W_q, é apresentada uma fórmula que permite calcular a porcentagem de flutuação da concentração de portadores livres em um modulador de amplitude integrado em SiO_2. Essa flutuação transforma a modulação Gaussiana em uma modulação não Gaussiana, resultando em uma estimativa incorreta da transitividade e do ruído excessivo em um protocolo CV-QKD com modulação Gaussiana. Portanto, é crucial determinar essa flutuação para implementar contramedidas eficazes (31).

Finalmente, devido a flutuações ambientais ou atividades de espionagem, a transmissividade do canal pode tornar-se uma variável aleatória seguindo uma distribuição de probabilidade específica, geralmente caracterizada por um parâmetro. Considerando que a transmissividade T segue uma distribuição uniforme no intervalo $[\lambda T_0, T_0]$, com $0 < \lambda < 1$ (32), apresentamos uma fórmula para determinar o valor do parâmetro λ. Em certo sentido, esse parâmetro mensura o impacto do ruído no canal ou de atividades de espionagem na comunicação do canal.

3.2 Impacto do SRS em QKD em Redes Ópticas Passivas

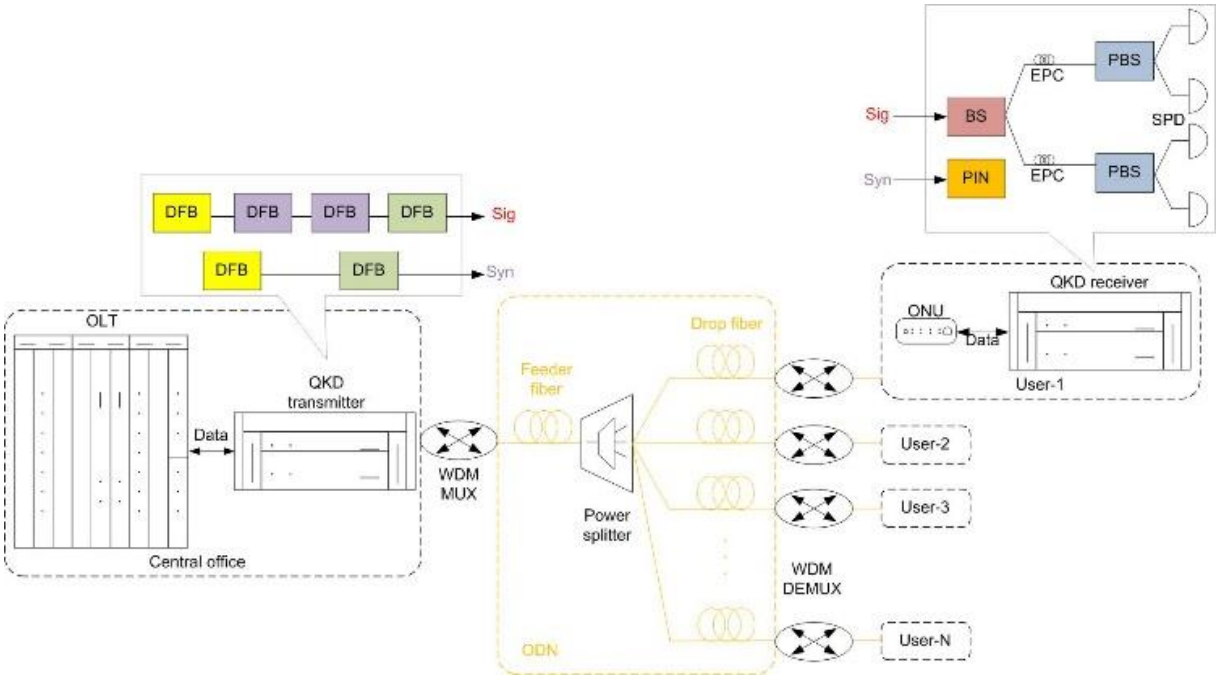
Para ser amplamente adotada, uma configuração óptica de Distribuição Quântica de Chaves (QKD) precisa ser flexível, reconfigurável e escalável. Essas características podem ser alcançadas ao realizar QKD em redes ópticas já instaladas, integrando dados quânticos e clássicos na mesma fibra óptica. No entanto, devido à substancial diferença de potência óptica utilizada pelos protocolos de comunicação quântica e clássica, a coexistência de sinais de dados quânticos e clássicos na mesma fibra óptica pode prejudicar o protocolo quântico.

A presença de amplificadores ópticos na rede óptica impede a realização do QKD na janela de 1550 nm devido ao intenso ruído de emissão espontânea amplificada nessa parte do espectro. Em tal situação, o protocolo de QKD poderia ser implementado em 1310 nm. No entanto, devido à elevada perda de fibra nesse comprimento de onda, a distância entre o transmissor e o receptor é severamente limitada. Para alcançar distâncias maiores, é necessário executar o protocolo de QKD em 1550 nm e os dados clássicos em 1310 nm.

A colocação de dados quânticos e clássicos na janela de 1550 nm é possível se uma fibra multinúcleos for utilizada, embora essas fibras ainda sejam dispendiosas e apresentem diafonia entre diferentes núcleos, que deve ser considerada. Outra opção é o uso de redes ópticas passivas (PON), onde amplificadores ópticos não são empregados. Em todos esses casos, o crosstalk linear proveniente de (de)multiplexadores e filtros ópticos imperfeitos, juntamente com vários efeitos não lineares, como mistura de quatro ondas (FWM) e os espalhamentos de Brillouin, Rayleigh e Raman, dificultam a integração eficiente de dados quânticos e clássicos (33-35).

Embora seja possível evitar o espalhamento FWM, Brillouin e Rayleigh alocando o canal quântico de forma espectralmente distante dos canais de dados clássicos, o espalhamento Raman apresenta uma grande mudança espectral e, portanto, pode não ser completamente evitado. Assim, o desafio mais significativo na coexistência de dados quânticos e clássicos na mesma fibra óptica é a geração de falsas contagens causadas pelo espalhamento Raman espontâneo (33, 36-38). O SRS aumenta a taxa de erro quântico (QBER), reduzindo a taxa de chave segura. Portanto, um design cuidadoso de redes ópticas que suportem serviços quânticos e clássicos deve abordar a geração do SRS. Neste contexto, consideramos a rede óptica passiva (PON), conforme discutido em (33, 37, 38), cujo esquema é mostrado na Figura 3.1.

Figura 3.1. QKD em rede óptica passiva na configuração downstream.



Fonte: Elaborada pelo autor.

Na comunicação clássica, o sinal downstream do terminal de linha óptica (OLT) no escritório central é enviado a todos os usuários por um divisor de feixes, e o sinal upstream de apenas uma unidade de rede óptica (ONU) colocada no nó do usuário é transmitido para OLT em cada intervalo de tempo (39). No caso de uma rede de acesso quântico (QAN) usando a estrutura PON, pode-se ter duas configurações: 1) Downstream, em que o receptor QKD é colocado nos nós dos usuários (40) e 2) upstream, em que o transmissor QKD é colocado nos nós dos usuários (37). Como a configuração downstream tem menos ruído SRS do que a configuração upstream e a taxa de geração segura não depende do número de usuários, nesta tese consideraremos apenas a configuração downstream. Consideramos a configuração $1 \times N$: Uma OLT com transmissor QKD e N ONU's cada uma com seu receptor QKD. Entre a OLT e a ONU estão a fibra alimentadora, com comprimento L_F, um divisor de potência passivo $1 \times N$ (alimentador único) e as fibras drop com comprimento $L_D << L_F$. Assim como em (33), consideramos que os fótons de ruído SRS são gerados principalmente pelo sinal OLT. Além disso, consideramos duas situações: I) os dados clássicos são transmitidos em 1310 nm. II) os dados clássicos são transmitidos em 1480 nm. Em ambos os casos os dados quânticos são

transmitidos em 1550 nm. O sinal OLT gera fótons de ruído SRS tanto na fibra alimentadora (S_F) quanto na fibra drop (S_D). Os valores de S_F e S_D são dados por (36).

$$S_F = \left\{ P\beta \Big/ \left[N\left(\alpha_q - \alpha_c\right) \right] \right\} \left(e^{-\alpha_c L_F} - e^{-\alpha_q L_F} \right) e^{-\alpha_q L_D}, \tag{3.1}$$

$$S_D = \left\{ P\beta \Big/ \left[N\left(\alpha_q - \alpha_c\right) \right] \right\} \left(e^{-\alpha_c L_D} - e^{-\alpha_q L_D} \right) e^{-\alpha_c L_F}, \tag{3.2}$$

nas quais P é a potência de lançamento do sinal OLT, N é a taxa de divisão do divisor de potência, β é o coeficiente SRS, α_c (α_q) é a perda de fibra no comprimento de onda dos dados clássicos (quânticos). Consideramos o protocolo BB84 QKD com dois estados isca (41). A taxa de chave segura do protocolo QKD é limitada inferiormente por

$$R = q\left\{ Q_1 \left[1 - H_2\left(e_1\right) \right] - f_{ec} Q_\mu H_2\left(e_\mu\right) \right\}, \tag{3.3}$$

sendo q = ½ para o protocolo BB84, f_{ec} é a eficiência da correção de erros, $H_2(x) = -x\log_2(x)-(1-x)\log_2(1-x)$, Q_μ e e_μ são o ganho geral e QBER do estado do sinal, enquanto Q_1 e e_1 são o ganho e QBER dos estados de um fóton do sinal. Assumindo o estado do sinal QKD com número médio de fótons μ e dois estados iscas com números médios de fótons ν ($< \mu$) e 0, a eq. (3.3) é calculado usando (35, 36)

$$Q_{\mu(\nu)} = 1 - \left(1 - Y_0\right) \exp\left(-\mu(\nu) \eta_B e^{-\alpha_q L - 10\log_{10}(N)} \right), \tag{3.4}$$

$$e_{\mu(\nu)} = e_d + \left[\left(1/2 - e_d\right) Y_0 \right] \Big/ Q_{\mu(\nu)}, \tag{3.5}$$

$$Q_1 = \frac{\mu^2 e^{-\mu}}{\mu\nu - \nu^2} \left(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0 \right), \tag{3.6}$$

$$e_1 = \left(e_\nu Q_\nu e^\nu - 0.5 Y_0 \right) \Big/ \left(Y_1 \nu \right), \tag{3.7}$$

$$Y_1 = \frac{\mu}{\mu\nu - \nu^2} \left(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0 \right), \tag{3.8}$$

$$Y_0 = 2p_{dark} + p_R\left(L\right). \tag{3.9}$$

Em (3.4)-(3.5) o comprimento do canal é igual a L e η_b é a eficiência quântica do detector de fóton único do receptor. e_d representa os erros de desalinhamento, visibilidade não unitária do interferômetro e modulação imperfeita, p_{dark} é a taxa de contagem de escuro dos detectores de fótons únicos e $p_R(L)$ é probabilidade de haver uma detecção causada por fótons gerados pelo SRS na fibra óptica e dada por (38)

$$p_R(L) = \left\{\left[S_F(L) + S_D(L)\right]\Delta f\,\Delta t\eta_B\right\}\Big/(hf). \tag{3.10}$$

Em (3.10) h é a constante de Planck, f é a frequência óptica do sinal quântico, Δf é a largura de banda de recepção do canal quântico e Δt é o intervalo de tempo efetivo em que o detector esta apto a ter uma deteção (largura dos pulsos de gatilho do detector de fótons).

A partir de um valor para p_R, utiliza-se (3.10) para obter o valor de $S_F + S_D$. O valor de $S_F + S_D$, por sua vez, é utilizado em (3.1) + (3.2). Por fim, o comprimento do canal, $L = L_D + L_F$, é obtido usando a função W_q de Lambert-Tsallis para inverter (3.1) + (3.2). O resultado é ($\alpha_q < \alpha_c$) (ver Apêndice A)

$$L = \frac{1}{\alpha_q - \alpha_c}\ln\left(\frac{\alpha_q}{\alpha_q - \alpha_c} W_{1-\frac{\alpha_q}{\alpha_c-\alpha_q}}\left[\frac{\alpha_q - \alpha_c}{\alpha_q}(-z)^{\frac{\alpha_c-\alpha_q}{\alpha_q}}\right]\right) \tag{3.11}$$

$$z = \frac{N\left(S_F + S_D\right)\left(\alpha_q - \alpha_c\right)}{P\beta} = \frac{Nhfp_R\left(\alpha_q - \alpha_c\right)}{\Delta f\,\Delta t\eta_B P\beta}. \tag{3.12}$$

Usando o ponto de ramificação de W_q na eq. (3.11) pode-se encontrar a seguinte relação entre P, N e p_R:

$$\frac{Np_R}{P} \geq \frac{\Delta f\,\Delta t\eta_B\beta}{hf}\frac{\left[1-\left(\alpha_q/\alpha_c\right)\right]}{\left(\alpha_c - \alpha_q\right)}\left(\frac{\alpha_q}{\alpha_c}\right)^{\frac{\alpha_q}{\alpha_c-\alpha_q}}. \tag{3.13}$$

Em outras palavras, se a eq. (3.13) não for satisfeita, não será possível encontrar um valor para L. De acordo com (3.3)-(3.8), R é máximo quando Y_0 é mínimo (quanto menor o ruído, maior a taxa de transmissão). O valor mínimo de Y_0 é alcançado quando p_R é mínimo e, conforme (3.13), o valor mínimo de p_R é

$$p_R^{\min} = \frac{P\Delta f\,\Delta t\eta_B\beta}{Nhf}\frac{\left[1-\left(\alpha_q/\alpha_c\right)\right]}{\left(\alpha_c - \alpha_q\right)}\left(\frac{\alpha_q}{\alpha_c}\right)^{\frac{\alpha_q}{\alpha_c-\alpha_q}}. \tag{3.14}$$

Portanto, substituindo (3.14) em (3.11)-(3.12), o valor ótimo de L é

$$L^{opt} = \frac{1}{\alpha_q - \alpha_c} \ln\left(\frac{\alpha_q}{\alpha_q - \alpha_c} W_{1-\frac{\alpha_q}{\alpha_c - \alpha_q}} \left[\frac{\alpha_q - \alpha_c}{\alpha_c} \left[1 - \frac{\alpha_q}{\alpha_c} \right]^{\frac{\alpha_c - \alpha_q}{\alpha_q}} \right] \right). \tag{3.15}$$

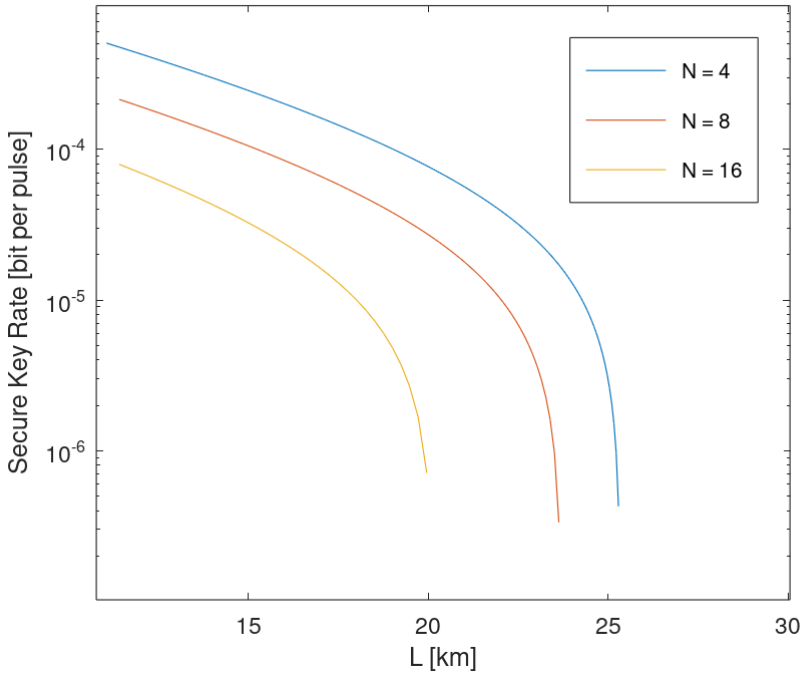
Por exemplo, usando α_c = 0.38 dB/km e α_q = 0.35 dB/km, tem-se L_{opt} = 11.90 km enquanto para α_c = 0.48 dB/km e α_q = 0.35 dB/km tem-se L_{opt} = 10.55 km. Como se pode notar, quanto menor o valor de α_c maior é o valor de L_{opt}. Isso acontece porque será necessário mais comprimento de fibra para atenuar o sinal clássico (o que diminui o SRS) ao nível aceitável.

Em nossa primeira simulação usamos α_c = 0.48 dB/km (1310 nm), α_q = 0.35 dB/km (1550nm) (26), η_B = 0.15, P = 0.5 mW, N = {4, 8, 16}, hf é a energia do fóton em 1550 nm, $p_{dark} = 2\times10^{-7}$, Δt = 1 ns, Δf = 100 GHz, f_{ec} = 1.2, μ = 0.4, v = 0.1, e_d = 0.02 e $\beta = 7\times10^{-9}\text{nm}^{-1}$. As perdas de inserção dos divisores de potência são 6.2 dB, 9.2 dB e 12.7 dB para 1 × 4, 1 × 8, 1 × 16, respectivamente. Não estamos considerando o efeito de *afterpulsing* nos detectores, na Fig. 3.2 podem-se ver as curvas da taxa de chave segura versus o comprimento do canal obtido em (3.11)-(3.12).

Para um determinado valor de p_R, o comprimento da fibra diminui e a perda de inserção do divisor de potência aumenta quando N aumenta. Portanto, a taxa R é maior para o valor de N que minimiza $[\alpha_q L(N)+10\log_{10}(N)]$. Para ter alta taxa de chave segura são necessários enlaces curtos (mais fótons do sinal quântico chegarão ao detector), porém, neste caso o SRS aumenta (os sinais clássicos são menos atenuados) o que aumenta o QBER diminuindo a taxa de chave segura.

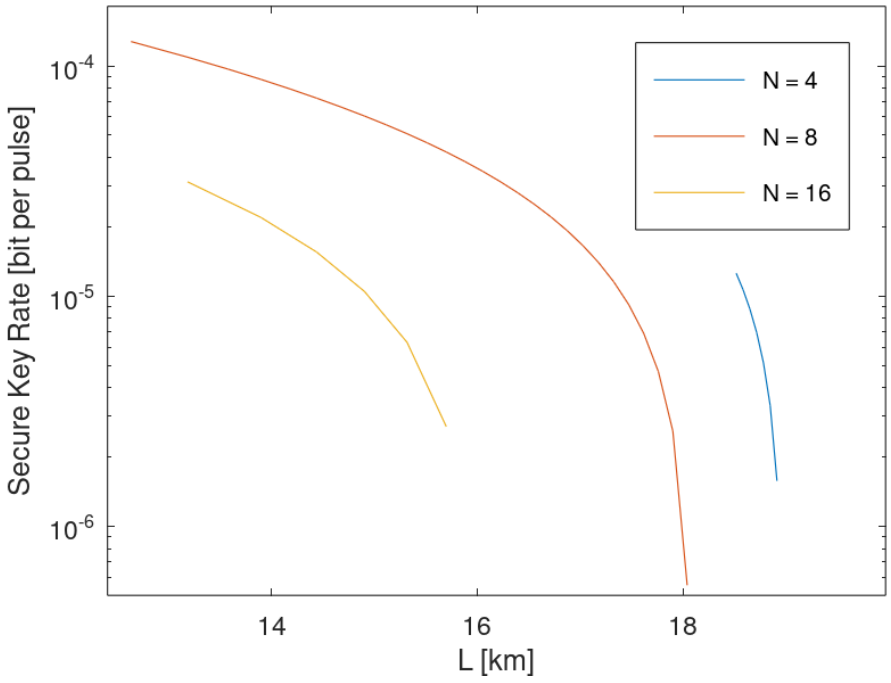
Em nossa segunda simulação foi utilizado α_c = 0,38 dB/km (1480 nm) e os demais parâmetros assumiram os mesmos valores utilizados na primeira simulação. Os gráficos da taxa de bits da chave segura versus comprimento do canal são mostrados na Fig. 3.3. Utilizar o canal clássico em 1480 nm resulta em um valor maior de p_R que deveria ser compensado pelas perdas no divisor de potência. Isto explica o pior comportamento mostrado na Fig. 3.3 para N = 4 e distâncias inferiores a aproximadamente 18 km. Por outro lado, para L > ~19 km, a atenuação da fibra do sinal clássico é forte o suficiente para diminuir o valor do SRS a um nível onde uma chave pode ser estabelecida para N = 4.

Figura 3.2. R versus L. α_c = 0,48 dB/km (1310 nm), α_q = 0,35 dB/km (1550nm)



Fonte: Elaborada pelo autor

Figura 3.3. R versus L. α_c = 0.38 dB/km (1480 nm), α_q = 0.35 dB/km (1550nm)



Fonte: Elaborada pelo autor

3.3 Uso de W_q na Análise de um Modulador de Amplitude de SiO_2 em Chip

Um dispositivo crucial em distribuição quântica de chaves de variável contínua (CV-QKD) é o modulador de amplitude em Alice. Quando um modulador em chip de SiO_2 é utilizado, flutuações na densidade de portadores livres podem resultar em uma modulação não gaussiana que, por sua vez, causará uma determinação errada dos parâmetros do canal (transmissividade e ruído de excesso total). Segundo o modelo descrito em (31), o valor da quadratura do sinal modulado, x_{0A}, é dado por (λ = 1550 nm)

$$x_{0A}^2 = 2x_{10}^2\left\{1-\sin\left[\frac{2\pi}{\lambda}L\left(-8.8\cdot10^{-22}r-8.5\cdot10^{-18}r^{0.8}\right)\right]\right\}, \tag{3.16}$$

$$\text{com}\quad r=\frac{\varepsilon_0\varepsilon_r}{et_{ox}t}V_D\left(1+\delta_{Ne}\right), \tag{3.17}$$

onde ε_0 é a constante dielétrica no vácuo, ε_r é a permissividade relativa do dióxido de silício, t_{ox} é a espessura da estrutura da camada fina de SiO_2 no modulador de amplitude baseado em um interferômetro Mach-Zehnder, t é a espessura efetiva da camada de carga em ambos os lados da estrutura de crista de camada fina de SiO_2 no modulador, e é a carga do elétron, L é o comprimento do guia de onda óptico da estrutura de capacitor semicondutor de óxido metálico (MOS), V_D é a tensão aplicada, x_{10} é a quadratura da metade do sinal antes da modulação e δ_{Ne} (=δ_{Nh}) é a porcentagem da flutuação da concentração de portadoras livres.

Para corrigir a determinação incorreta dos parâmetros do canal quântico, algumas estratégias podem ser utilizadas, como as descritas em (31). Um passo importante para a implementação de uma estratégia de defesa é a determinação de $\delta_{Ne} \times V_D$. Usando a função W_q de Lambert-Tsallis , depois de alguma álgebra pode-se encontrar que (ver Apêndice A)

$$\delta_{Ne}=\frac{et_{ox}t}{\varepsilon_0\varepsilon_r V_D}\left\{\frac{4B}{A}W_{-3}\left[\frac{A}{4B}\left(\frac{z}{B}\right)^{\frac{1}{4}}\right]\right\}^5-1, \tag{3.18}$$

Com

$$z=\arcsin\left(1-\frac{x_{0A}^2}{2x_{10}^2}\right), \tag{3.19}$$

sendo $A = -8.8\times10^{-22}(2\pi/\lambda)L$, $B = -8.5\times10^{-18}(2\pi/\lambda)L$. Assim, após a medição de x_{0A}, pode-se utilizar (3.18)-(3.19) para determinar o valor da flutuação δ_{Ne}. Assim, as eqs. (3.18)-(3.19) podem ser usadas para implementar a estratégia de defesa dinâmica discutida em (31).

3.4 Utilização de W_q na Determinação do Parâmetro do Canal Estocástico

Conforme discutido na seção 3.3, a estimativa da transmissividade do canal é uma etapa importante no CV-QKD. Depois que Alice e Bob trocaram sinais quânticos, eles compartilham os vetores correlacionados $X_A = \{x_{A1}, x_{A2},\ldots,x_{AN}\}$ e $X_B = \{x_{B1}, x_{B2},\ldots,x_{BN}\}$. A transmissividade do canal pode ser estimada por (32)

$$\hat{T} = \frac{\left[E\left(X_A X_B\right)\right]^2}{\eta\left[E\left(X_A^2\right)\right]^2} = \left[E\left(\sqrt{T}\right)\right]^2 \tag{3.20}$$

na qual η é a eficiência de detecção e $E(z)$ é o valor esperado de z. Porém, devido a flutuações ambientais ou ações de espionagem, a transmissividade do canal pode se tornar uma variável aleatória obedecendo a uma determinada distribuição de probabilidade. Quando a transmissividade T é um número aleatório uniformemente distribuído entre λT_0 e T_0 ($T_0 = 10^{-\alpha L}$ onde α é o coeficiente de perda da fibra e L é o comprimento do canal), com $0 \le \lambda \le 1$, tem-se o valor teórico (32)

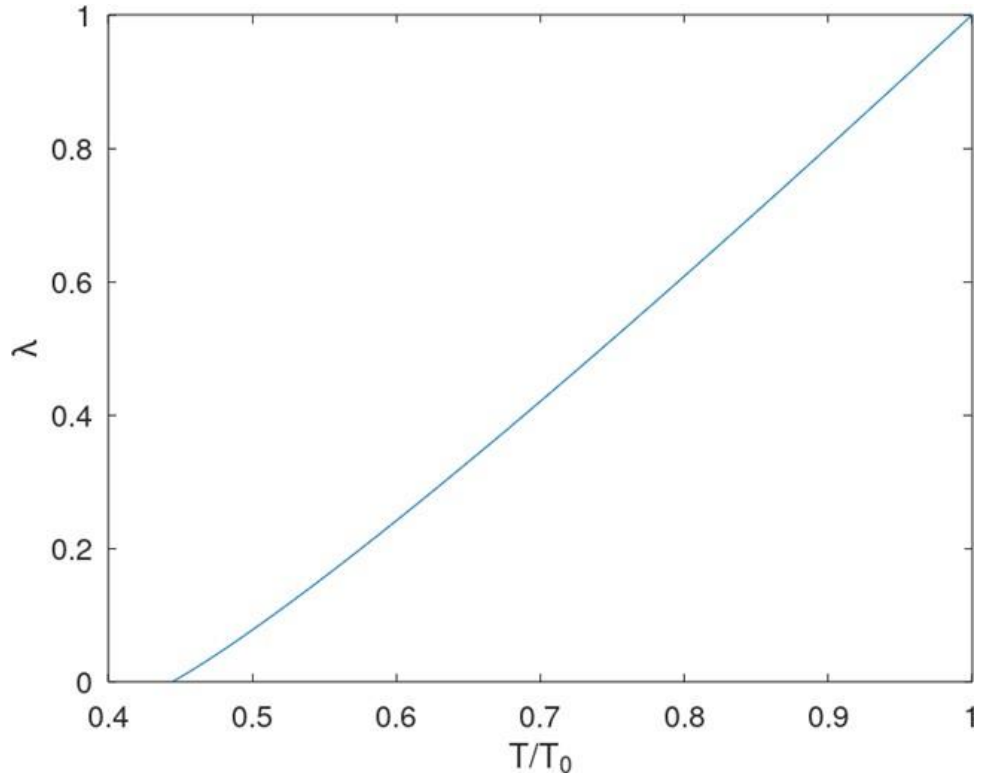
$$T = \left[\frac{2\left(1-\lambda^{3/2}\right)}{3\left(1-\lambda\right)}\right]^2 T_0 . \tag{3.21}$$

Portanto, a transmissividade do canal é parametrizada pela variável λ. Pode-se notar em (3.21) que $\lambda = 0$ implica $T/T_0 = 4/9$. Para obter o valor de λ quando T é medido, pode-se usar (ver Apêndice A):

$$\lambda = \left[3\sqrt{\frac{T}{T_0}}W_{-1}\left(-\frac{1}{3}\sqrt{\frac{T_0}{T}}\sqrt{1-\frac{2}{3}\sqrt{\frac{T_0}{T}}}\right)\right]^2 , \tag{3.22}$$

A curva λ versus T/T_0 é mostrada na Fig. 3.4. Pode-se notar que, como esperado, quando o valor estimado para T é tal que $T/T_0 < 4/9$, eq. (3.22) retornará valores imaginários (que não são mostrados na Fig. 3.4).

Figura 3.4 – λ versus T/T_0 (eq. (3.22)).



Fonte: Elaborado pelo autor.

DETECÇÃO DE ESPIONAGEM SEM USAR TAXA DE ERRO: A DISTRIBUIÇÃO QUÂNTICA DE CHAVES BASEADA NA DISENTROPIA

4.1 Introdução

A distribuição quântica de chaves experimentou enormes avanços desde a sua concepção no início dos anos 80. Desde canais de poucos centímetros de comprimento até centenas de quilômetros de canais de fibra óptica e comunicações via satélite que cobrem distâncias de milhares de quilômetros (43-44). Hoje em dia existem vários protocolos QKD diferentes, como BB84 (45), B92 (46), DPS-QKD (differential phase-shift) (47), COW-QKD (coherent one-way) (48), Twin-Field QKD (49), *mode-pairing* QKD (50) , MDI-QKD (measurement device independent) (51), QKD com estados iscas (41), QKD de duas camadas (53), QKD quântico-caótico (54), QKD de variável contínua (55), entre outros.

A implementação desses protocolos exigiu o desenvolvimento de novos dispositivos ópticos e optoeletrônicos, como novas fontes de fótons únicos e de dois fótons, no lado do transmissor (56, 57), e novos detectores de fótons únicos usando fotodiodos de avalanche e supercondutores, no lado do receptor (56-59). Outras fronteiras tecnológicas também estão sendo atacadas pela comunidade de QKD, como a integração em chips de silício de moduladores ópticos, fontes ópticas e detectores de fótons (60).

Além de exigir o desenvolvimento de novos dispositivos ópticos, a maioria das configurações de QKD são dependentes de fase e polarização. Portanto, suas implementações requerem um esquema ativo de controle de polarização (61, 62) e interferometria muito estável. Além disso, embora o protocolo CV-QKD possa ser implementado com dispositivos ópticos e optoeletrônicos atuais, sua implementação com oscilador local requer uma tarefa complexa de pós-processamento (63, 64).

Apesar dos avanços muito significativos realizados nas últimas duas décadas, todas as implementações de protocolos QKD sofrem de baixas taxas de transmissão de bits seguros, implementações complexas e custos elevados. Idealmente, um protocolo QKD deve fornecer segurança perfeita, fácil implementação, pós-processamento de baixa complexidade e baixo custo. A maioria desses requisitos pode ser alcançada com um protocolo QKD baseado apenas em modulação de amplitude. No entanto, até agora, tal protocolo de QKD não foi proposto, uma vez que nenhuma prova de segurança foi fornecida. O problema é que para tal tipo de protocolo de QKD os erros introduzidos por um espião seriam mascarados pelas inevitáveis perdas na fibra óptica. Nessa direção, o presente trabalho propõe o primeiro protocolo de QKD

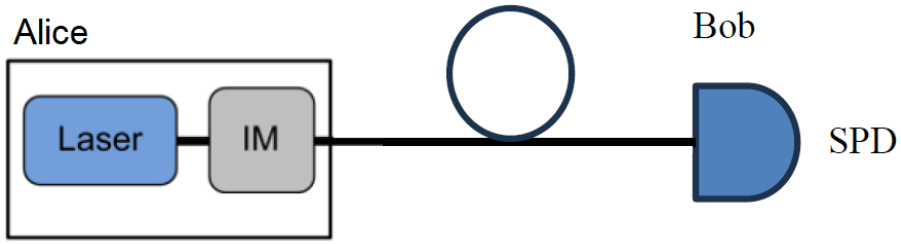
cuja segurança não é baseada na taxa de erro e, portanto, permite a construção de um protocolo de QKD utilizando apenas modulação de amplitude.

Neste capítulo, apresentamos um novo protocolo de distribuição quântica de chaves que possui a configuração óptica mais simples entre todos os protocolos de QKD já propostos, portanto, é um protocolo de baixo custo e fácil implementação. Além disso, este novo protocolo QKD é baseado em modulação de amplitude e detecta a ação de espionagem verificando a aleatoriedade da chave obtida por Bob. Assim, a estimativa da taxa de erro para detecção de espionagem não é necessária.

4.2 Metodologia e Resultados Obtidos

A ferramenta matemática crucial para o protocolo proposto está baseada na disentropia vista no capítulo 2, ou seja, a medida de aleatoriedade de um sinal ou sequência numérica é a disentropia de sua autocorrelação, dada pela eq. (2.25) para o caso contínuo e pela eq. (2.26) para o caso discreto. O protocolo de QKD aqui proposto é semelhante ao protocolo COW (48). A informação do bit é codificada na posição do pulso dentro de um intervalo de tempo. Porém, o interferômetro utilizado no protocolo COW para detecção de espionagem não é necessário, o que torna sua implementação mais fácil. A configuração óptica necessária para implementação do protocolo de QKD baseado em disentropia é mostrada na Fig. 4.1.

Figura 4.1. Configuração do protocolo QKD baseado em disentropia. IM – modulador de intensidade e SPD – detector de fóton único.



Fonte: Elaborada pelo autor.

Como pode ser visto na Fig. 4.1, a configuração óptica é extremamente simples e fácil de implementar. O modulador de intensidade externo em Alice pode ser opcional, pois o protocolo aqui proposto também funcionará corretamente se for usada modulação direta do laser (o que pode ser feito quando o comprimento do canal é tal que a dispersão pode ser desprezada). Como

também pode ser observado na Fig. 4.1, não há necessidade de controle de polarização ou de manutenção da estabilidade de interferômetros, permitindo uma implementação fácil, rápida e de baixo custo. Para o *k*-ésimo intervalo de tempo, os bits lógicos são codificados da seguinte forma

$$|0_k\rangle = |\alpha\rangle_k|0\rangle_k \tag{4.1}$$

$$|1_k\rangle = |0\rangle_k|\alpha\rangle_k \tag{4.2}$$

Os valores de α são escolhidos aleatoriamente entre os valores $\{\alpha_1, \alpha_2\}$. O protocolo é descrito a seguir: Inicialmente, Alice e Bob concordam em usar os seguintes conjuntos de estados coerentes: S_1 $\{|\alpha_1\rangle$ (bit '0'), $|\alpha_2\rangle$ (bit '1')$\}$ e S_2 $\{|\alpha_2\rangle$ (bit '0'), $|\alpha_1\rangle$ (bit '1')$\}$, com $|\alpha_1|^2 > |\alpha_2|^2$. Esta codificação está resumida na Tabela 4.1.

Tabela 4.1. Bits codificados por estados coerentes

	Bit ‘0’	Bit ‘1’
S_1	$\|\alpha_1\rangle$	$\|\alpha_2\rangle$
S_2	$\|\alpha_2\rangle$	$\|\alpha_1\rangle$

Fonte: Elaborada pelo autor.

As etapas do protocolo são:

1) Para cada pulso de luz que envia para Bob, Alice escolhe aleatoriamente o conjunto (S_1 ou S_2) e os valores do bit (posição do pulso dentro do intervalo de tempo) que serão utilizados.
2) Para cada pulso de luz recebido de Alice, Bob mede sua posição dentro de cada intervalo de tempo.
3) Ao final do protocolo, Alice informa publicamente a Bob qual conjunto (S_1 ou S_2) foi utilizado para cada intervalo de tempo.

Usando a disentropia da autocorrelação dada pela eq. (2.26), Bob calcula a aleatoriedade das duas chaves K_1 ($D_2(K_1)$) e K_2 ($D_2(K_2)$) obtidas, respectivamente, utilizando apenas os bits

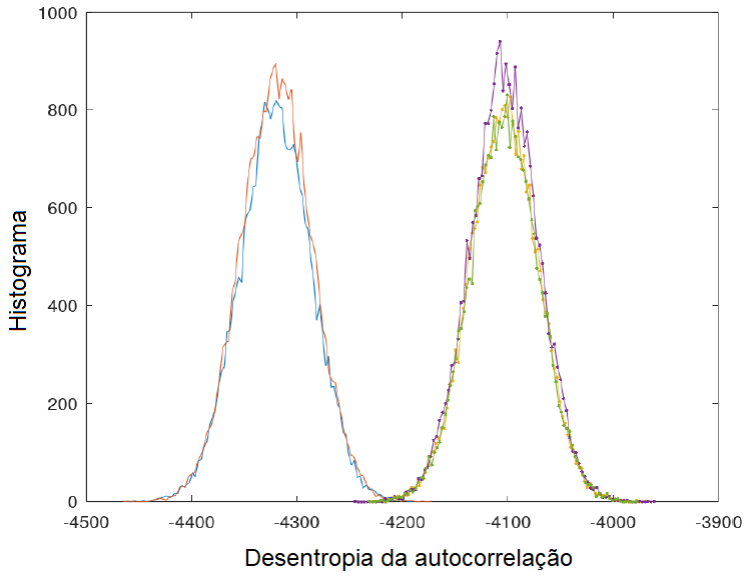
medidos quando os conjuntos S_1 (K_1) e S_2 (K_2) foram utilizados. Como $|\alpha_1|^2 > |\alpha_2|^2$, para a chave K_1 tem-se mais bits ‘0’ do que bits ‘1’ e o oposto ocorre para K_2. Assim, as chaves K_1 e K_2 são enviesadas e sua aleatoriedade (disentropia) não será máxima (mínima). Para K_1 tem-se $p_0 = 1-(1-p_d)exp(-\eta t|\alpha_1|^2)$ e $p_1 = 1-(1-p_d)exp(-\eta t|\alpha_2|^2)$ enquanto para K_2 tem-se $p_0 = 1-(1-p_d)exp(-\eta t|\alpha_2|^2)$ e $p_1 = 1-(1-p_d)exp(-\eta t|\alpha_1|^2)$, onde t é a transmissividade do canal e p_0 e p_1 são, respectivamente, as probabilidades de um bit '0' e um bit '1' serem detectados. A chave final obtida sem considerar os conjuntos S_1 e S_2, por sua vez, é nao enviezada.

A segurança baseia-se no fato de que os estados coerentes $|\alpha_1\rangle$ e $|\alpha_2\rangle$ são não ortogonais e, portanto, não podem ser distinguidos de forma não ambígua. Caso o espião altere os valores de $|\alpha_1|^2$ e $|\alpha_2|^2$, as probabilidades de detecção em Bob mudarão, o que alterará o valor da disentropia calculada por Bob, denunciando o ataque.

Um ataque de divisor de feixe é possível se o espião puder compensar a perda introduzida pelo divisor de feixe inserido no canal, porém o espião não pode enviar pulsos fortes para garantir a detecção em Bob conforme descrito em (48), pois isso também alterará as probabilidades de detecção e o valor da disentropia calculado por Bob, denunciando o ataque. Assim, a quantidade de informações que o espião pode obter limita a distância segura entre Alice e Bob, como também ocorre no protocolo COW, porém o espião não pode garantir que um valor de bit que obtido durante um ataque também será obtido por Bob e usado na chave.

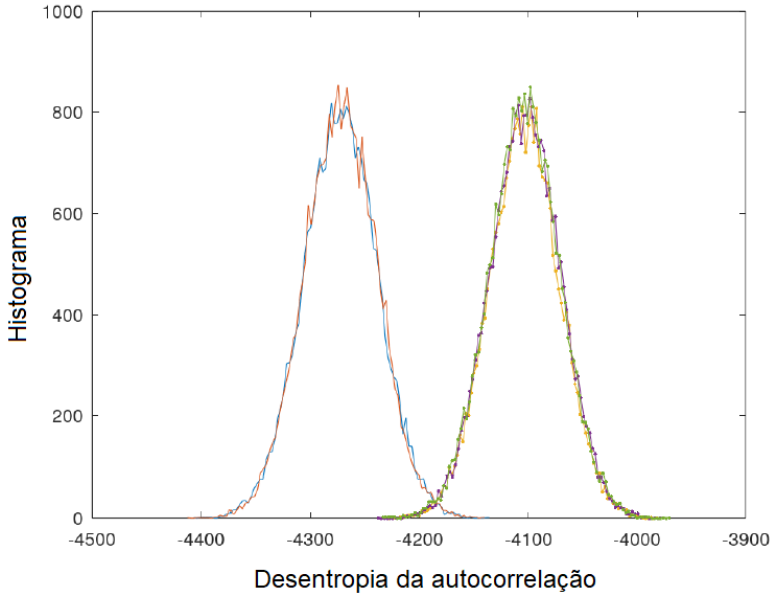
O estado quântico visto pelo espião é $\rho = 1/2|\alpha_1\rangle\langle\alpha_1| + 1/2|\alpha_2\rangle\langle\alpha_2|$. Assim, vamos supor que o valor considerado pelo espião seja $|\alpha_m|^2 = (|\alpha_1|^2+|\alpha_2|^2)/2$. Usando $|\alpha_1|^2 = 0{,}75$, $|\alpha_2|^2 = 0{,}5$ e $|\alpha_m|^2 = 0{,}625$, pode-se ver na Fig. 2 ($\eta = 0{,}4$, $p_d = 10^{-5}$, $t = 10^{-0{,}25}$) e na Fig. 3 ($\eta = 0{,}8$, $p_d = 10^{-5}$, $t = 10^{-0{,}25}$) os histogramas dos valores da disentropia calculada por Bob após várias execuções do protocolo, com (curva direita) e sem (curva esquerda) espionagem.

Figura 4.2. Histograma da disentropia da autocorrelação calculada por Bob com (direita) e sem espião (esquerda) ($\eta = 0{,}4$, $p_d = 10^{-5}$, $t = 10^{-0{,}25}$)



Fonte: Elaborada pelo autor.

Figura 4.3. Histograma da disentropia da autocorrelação calculada por Bob com (direita) e sem espião (esquerda) ($\eta = 0{,}8$, $p_d = 10^{-5}$, $t = 10^{-0{,}25}$ (10 km)).



Fonte: Elaborada pelo autor.

Como pode-se ver nas Figs. 4.2 e 4.3, um valor de limiar para a disentropia pode ser estabelecido e usado para decidir se a chave final deve ser descartada e o protocolo reiniciado ou não. Para as simulações mostradas nas Figs. 4.2 e 4.3, utilizamos um procedimento semelhante ao usado em (30) para redimensionar os valores de disentropia, basicamente, as sequências de bits obtidas por Bob foram somadas a um sinal determinístico (uma função senoidal) antes do cálculo da disentropia.

Embora apenas a versão com dois estados coerentes tenha sido apresentada, a extensão do protocol usando quatro, seis ou mais estados coerentes é direta. Quanto maior o número de estados, mais difícil será o trabalho da espiã. Por exemplo, vamos assumir que Alice e Bob concordem com os seguintes conjuntos : S_1 {$|\alpha_1\rangle$ (bit '0'), $|\alpha_2\rangle$ (bit '1')}, S_2 {$|\alpha_2\rangle$ (bit '0'), $|\alpha_1\rangle$ (bit '1')}, S_3 {$|\alpha_3\rangle$ (bit '0'), $|\alpha_4\rangle$ (bit '1')}, S_4 {$|\alpha_4\rangle$ (bit '0'), $|\alpha_3\rangle$ (bit '1')}, com $|\alpha_1|^2 > |\alpha_2|^2$ e $|\alpha_3|^2 > |\alpha_4|^2$. Esta codificação está resumida na Tabela 4.4.

Tabela 4.2. Bits codificados por estados coerentes com dois pares de conjuntos.

	Bit ‘0’	Bit ‘1’
S_1	$\|\alpha_1\rangle$	$\|\alpha_2\rangle$
S_2	$\|\alpha_2\rangle$	$\|\alpha_1\rangle$
S_3	$\|\alpha_3\rangle$	$\|\alpha_4\rangle$
S_4	$\|\alpha_4\rangle$	$\|\alpha_3\rangle$

Fonte: Elaborada pelo autor.

As etapas do protocolo são:

1) Para cada pulso de luz que envia para Bob, Alice escolhe aleatoriamente o conjunto (S_1, S_2, S_3 ou S_4) e o valor do bit (posição do pulso dentro do intervalo de tempo) que serão utilizados.

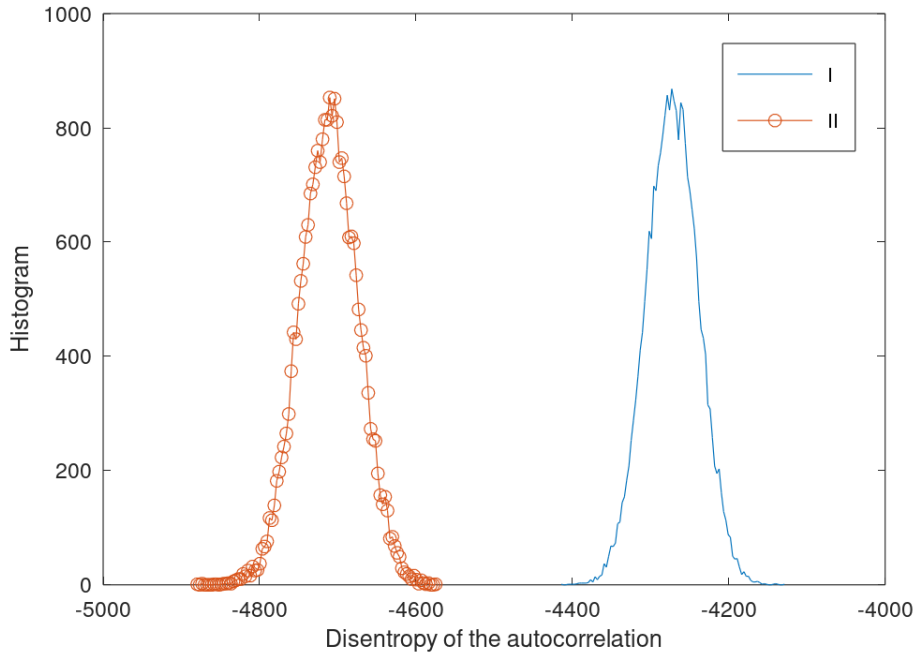
2) Para cada pulso de luz recebido de Alice, Bob mede sua posição dentro de cada intervalo de tempo.

3) Ao final do protocolo, Alice informa publicamente a Bob qual conjunto (S_1, S_2, S_3 ou S_4) foi utilizado para cada intervalo de tempo.

4) Bob forma a chave K_i usando apenas os bit obtidos quando o conjunto S_i foi utilizado e calcula a disentropia $D_2(K_i)$. Pode-se notar que haverá um limiar diferente da disentropia para inferir a presenca da espiã em cada conjunto e a ação da espiã não poderá violá-lo em nenhum dos dois casos.

Por exemplo, consideremos a situação em que $|\alpha_1|^2 = 0{,}75$, $|\alpha_2|^2 = 0{,}5$, $|\alpha_3|^2 = 0.85$, $|\alpha_4|^2 = 0{,}4$. As disentropias calculadas por Bob estão mostradas na Fig. 4.4.

Figura 4.4. Histograma da disentropia da autocorrelação calculada por Bob quando dois pares de conjuntos sao utilizados ($\eta = 0{,}8$, $p_d = 10^{-5}$, $t = 10^{-0{,}25}$ (10 km)). Linha - S_1 e S_2 , Bolas - S_3 e S_4.



Fonte: Elaborada pelo autor.

Como mostrado na Fig. 4.4, não ha superposição entre as curvas esperadas portanto, não há como a(o) espiã(o) conseguir satisfazer os dois resultados ao mesmo tempo.

Por fim, para evitar que Eva obtenha informações completas dos valores dos bits durante um ataque, Alice e Bob podem usar uma camada extra de criptografia, uma criptografia caótica na qual a separação entre os intervalos de tempo varia de acordo com um sistema caótico cujos parâmetros são conhecidos apenas por Alice e Bob (neste caso, os valores dos parâmetros pertencem à chave inicial utilizada para autenticação). Sem saber quando um intervalo de tempo começa e termina, o espião não saberá se um bit ‘0’ ou ‘1’ foi detectado.

DETECTOR DE FÓTONS CONTROLADO REMOTAMENTE POR LUZ

5.1 Introdução

Todos os detectores de fótons únicos (Single-photon detectors - SPD) relatados na literatura se deparam com dois problemas:

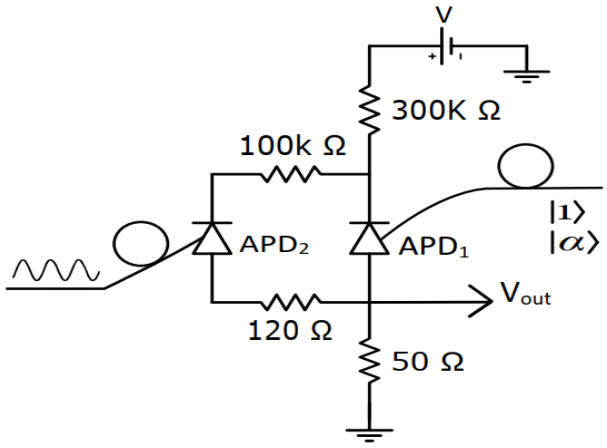
I) Aumentar a eficiência quântica e diminuir as probabilidades de contagem escura e de pós-contagem, e diminuir efeitos de borda devido ao chaveamento do APD com pulsos de gatilho.
II) Evitar ataques de cavalos de Tróia em distribuição quântica de chave (66).

Há uma terceira preocupação que abordamos neste capítulo, o sincronismo entre Alice e Bob. Focandos em diminuir falsas detecções devido à contagem de escuro, os APDs de Bob devem ser ligados apenas quando o pulso de luz enviado por Alice chegar em Bob. Consequentemente, um sincronismo entre Alice e Bob deve ser estabelecido. Nesta direção, o presente capítulo mostra como construir um SPD que facilite o sincronismo entre Alice e Bob, de forma que Alice ative remotamente os APDs de Bob sem comprometer a segurança do protocolo de QKD.

5.2. Chaveamento óptico do SPD

O esquema proposto para o chaveamento remoto do SPD está na Fig. 5.1 e, como se pode ver, o APD 1 funciona em modo Geiger para detectar o fóton de sinal, enquanto o APD 2, trabalhando no modo linear, é responsável por desativar ou ativar o APD 1. Quando APD 2 for iluminado (escurecido), sua condutividade aumenta (diminui), e isso força a tensão sobre os terminais do APD 1 a permanecer abaixo (acima) da tensão de ruptura e, dessa forma, uma avalanche não pode (pode) ocorrer. Assim, os sinais de chaveamento são pulsos ópticos na configuração da Fig. 5.1. Para mostrar o comportamento do SPD, a saída do circuito na Fig. 5.1 foi conectada a um analisador de espectro e a energia elétrica na banda 10MHz-30MHz foi medida conforme (70).

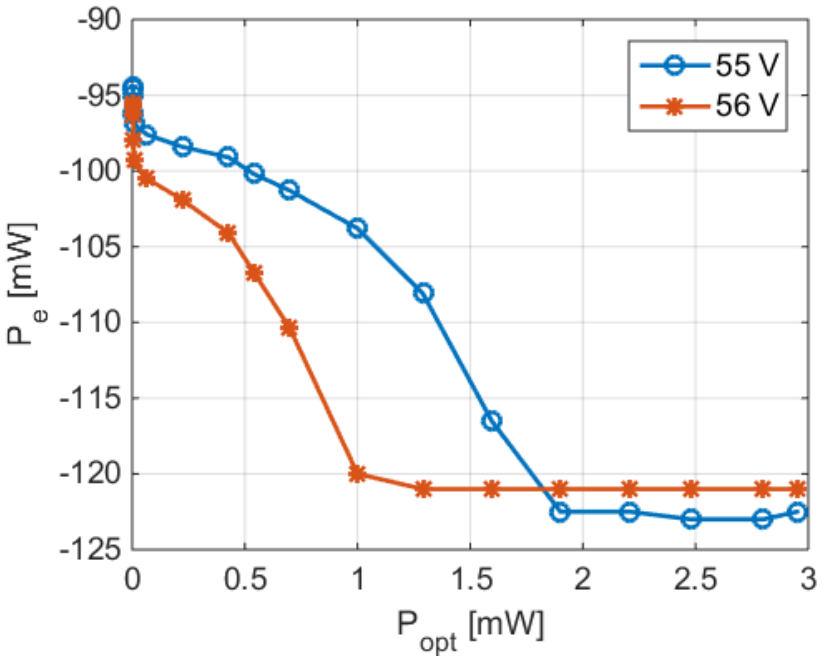
Figura 5.1. Circuito para chaveamento remoto do detector de fótons usando APDs



Fonte: Elaborada pelo autor.

Dois valores de tensão foram utilizados: 55V e 56V (tensão de ruptura do APD é de 51V). O APD 2 foi iluminado por um Laser CW com potência óptica variando no intervalo [0, 2.9] mW. Por fim, os dois APDs foram operados à temperatura ambiente (22 °C).

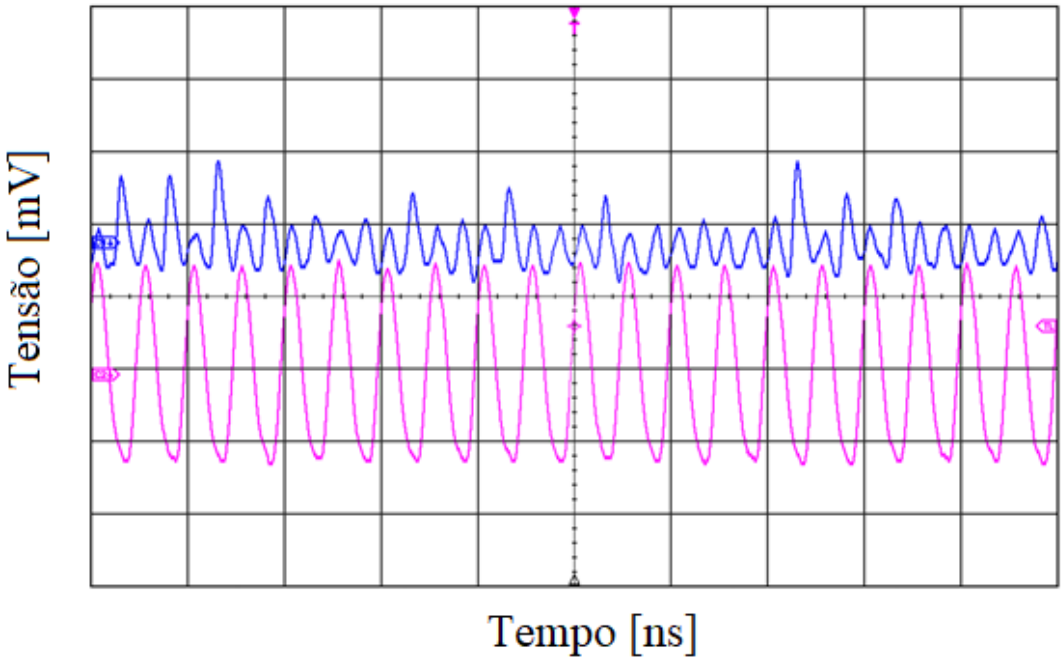
Figura 5.2. Potência elétrica (P_e) medida na banda [10MHz -30MHz] versus a potência óptica (P_{opt}) do laser CW que ilumina o APD 2.



Fonte: Elaborada pelo autor.

Como se pode ver na Fig. 5.2, para uma tensão no APD de 55V (56V), uma potência óptica de 1mW (2mW) inibe completamente as avalanches (o ruído de fundo é de -120dBm). Já na Fig. 5.3, se vê o sinal de saída (V_{out} na Fig. 5.1) quando o laser que ilumina APD 2 é modulado por uma onda senoidal de 200 MHz (10ns por divisão na Fig 5.3). Os picos mais altos (traço azul) são avalanches que podem ocorrer apenas quando o sinal de modulação é baixo (traço rosa).

Figura 5.3. Avalanches ocorrendo apenas durante a parte baixa do sinal de modulação.



Fonte: Elaborada pelo autor.

Como é mostrado nas Figs. 5.2 e 5.3, o SPD apresentado na Fig. 5.1 pode ser acionado pela luz, portanto, pode ser acionado remotamente se uma fibra óptica longa for colocada entre a fonte do laser e o APD 2. Dependendo do comprimento da fibra óptica, um amplificador óptico pode ser necessário. Para caracterizar o APD usado (C30617BQC-07-FC da Perking Elmer) em nosso novo esquema, usamos as equações (47):

$$P^2 - [p_a(1 - P_D)e^{\tau} + P_D + (1 - e^{\tau})]P + P_D(1 - e^{\tau}) = 0 \quad (5.1)$$

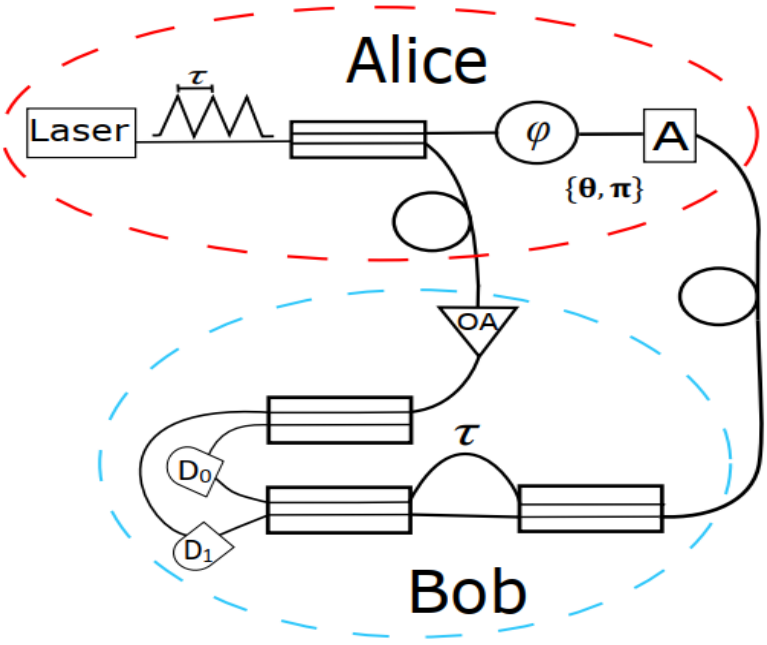
$$P_D = 1 - e^{-\eta\mu}(1 - p_d) \quad (5.2)$$

Em (5.1) e (5.2) p_d é a probabilidade de contagem de escuro, η é a eficiência quântica, μ é o número médio de fótons do pulso e a detecção de contagem pós-pulso é caracterizada pelas variáveis p_a e τ, onde $p_a\, e^{[-(k-1)]}$ é a probabilidade de contagem de pós-pulso devido a uma avalanche que ocorreu k janelas de gatilho antes e, τ é a largura da janela temporal. Finalmente, P é a razão entre o número medido de avalanches em um segundo dividido pelo número de vales do sinal de onda senoidal por segundo. Usando um sinal senoidal de 280MHz e trabalhando em temperatura ambiente, os resultados são de $\eta \sim 2{,}1\%$, $p_d \sim 0{,}23\%$, $pa \sim 9\%$ e $\tau \sim 0{,}04$. Os valores experimentais obtidos são consistentes com um SPD que não foi projetado para ser um detector de fóton único (71).

5.2. Distribuição quântica de chaves usando SPDs com chaveamento óptico

A configuração óptica de um protocolo QKD por mudança de fase diferencial (DPS-QKD) (14) empregando SPDs acionados remotamente é mostrada na Fig. 5.4.

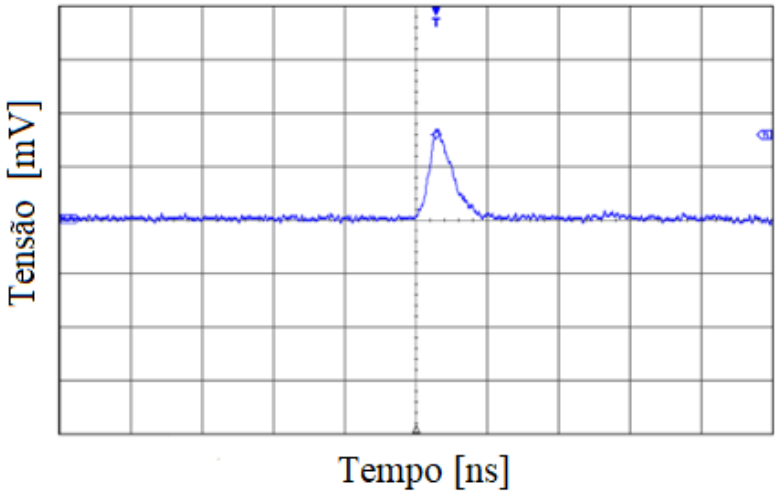
Figura 5.4. Configuração óptica para DPS-QKD empregando detectores de fótons únicos remotamente acionados. OA - Amplificador óptico, A - atenuador óptico. D_0 e D_1 são detectores de fóton único do tipo mostrado na Fig. 5.1.



Fonte: Elaborada pelo autor.

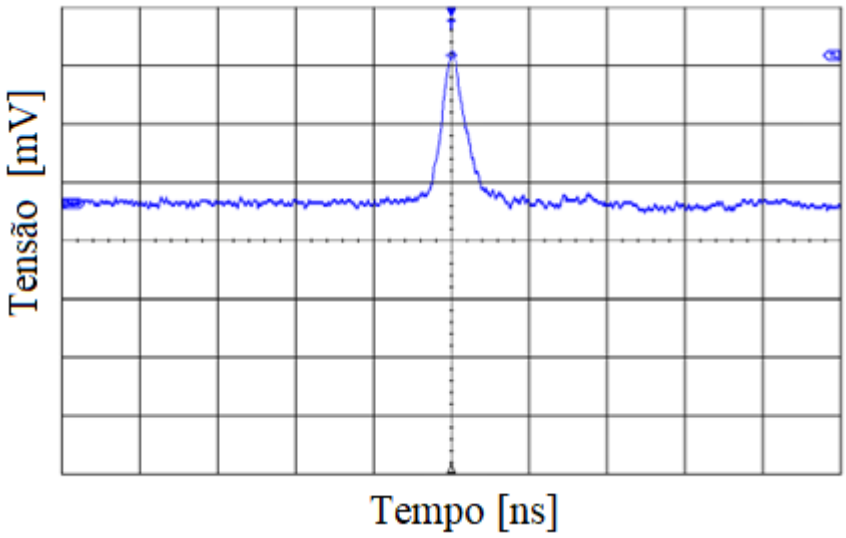
Na Fig. 5.4, um divisor de feixe 50/50 divide os pulsos ópticos produzidos por Alice. Os pulsos na primeira saída do divisor de feixe de Alice são enviados diretamente a Bob através de um canal óptico. Em Bob, esses pulsos ópticos são amplificados (OA) e divididos por outro divisor de feixe para acionar os dois SPDs de Bob. Os pulsos ópticos na segunda saída do divisor de feixe de Alice são modulados em fase (0 ou π rad), atenuados no nível de fóton único (estados coerentes com número médio de fótons igual a 0.1) e enviados através do canal quântico óptico ao interferômetro de Bob. Um detalhe importante de se observar é que, uma avalanche no APD 1 não pode ser iniciada iluminando o APD 2; ou seja, o APD 1 pode ser bloqueado, mas não controlado remotamente. Embora o espião, Eve, não possa forçar a detecção em Bob apenas alterando os pulsos ópticos de gatilho, ela pode tentar evitar detecções em Bob colocando pulsos ópticos extras nos intervalos de tempo em que se espera que a detecção ocorra. Todavia, como os pulsos ópticos de gatilho são pulsos clássicos com muitos fótons, é mais fácil para Bob monitorar esses pulsos para verificar se o espaçamento temporal entre pulsos ópticos de gatiho consecutivos é sempre o mesmo. Por fim, pode-se notar que o circuito na Fig. 5.1 pode ser facilmente transformado em um SPD de extinção ativa se o sinal de saída for amplificado e usado para alimentar um laser que ilumina o APD 2. Pode-se ver na Fig. 5.5 (5ns por divisão / 200mV por divisão) uma avalanche amplificada extinta passivamente, enquanto a Fig. 5.6 mostra uma avalanche amplificada ativamente extinta.

Figura 5.5. Sinal de avalanche extinto passivamente. O pico tem aproximadamente 380mV.



Fonte: Elaborada pelo autor.

Figura 5.6. O sinal de avalanche se é extinto ativamente. O pico tem aproximadamente 220mV.



Fonte: Elaborada pelo autor.

Conforme observado na Fig. 5.6 (5ns por divisão / 100mV por divisão), a extinção ativa limita a quantidade de corrente que flui através do APD (o sinal de avalanche tem menor amplitude), diminuindo a quantidade de portadores presos na região ativa, o que diminui a probabilidade de contagem pós-pulso.

CONCLUSÕES E PERSPECTIVAS DE TRABALHOS FUTUROS

6.1 Conclusões

A presente tese forneceu, de forma inédita, os seguintes resultados:

1. A solução analítica da relação *I* versus *V* de um circuito composto por uma fonte de tensão contínua, um resistor e um dispositivo que obedece à lei de Mark-Helfrich, como um nanofio: **Equação (2.36)**.

2. A solução analítica da relação *I* versus *V* de um circuito composto por uma fonte de tensão contínua, um resistor, um capacitor e um diodo: **Equações (2.42)-(2.43)**.

3. A solução analítica para o valor mínimo da probabilidade de uma detecção ser causada por fótons provenientes do espalhamento Raman espontâneo, quando canais clássicos e quânticos são integrados na mesma fibra óptica na configuração downstream: **Equação (3.14).**

4. A solução analítica para o comprimento do canal óptico que maximiza a taxa de transferência de bits seguros quando canais clássicos e quânticos são integrados na mesma fibra óptica na configuração downstream: **Equação (3.15).**

5. Uma fórmula analítica para a determinação da percentagem de flutuação de portadores em um modulador integrado em chip de SiO_2 utilizado em QKD de variáveis contínuas: **Equações (3.18)-(3.19)**.

6. Uma fórmula analítica para a determinação do parâmetro que modula um canal quântico estocástico de QKD de variáveis contínuas: **Eq. (3.22)**

7. Um novo protocolo de QKD baseado em modulação de amplitude, que apresenta a configuração mais simples e barata dentre todas as propostas até o momento existentes, e que realiza a detecção de espionagem sem utilizar a taxa de erro. Entretanto, a segurança contra ataques que utilizem uma eficiente contagem de fótons não está garantida.

8. Resultados experimentais de um detector de fótons controlado remotamente por luz.

Portanto, pode-se concluir que

1. Em ambos os casos considerados na tese, as soluções analíticas obtidas estão de acordo com o comportamento físico esperado, mostrando que a função W_q é uma ferramenta matemática útil para fornecer soluções analíticas de equações de circuitos que possuam uma relação do tipo lei de potência entre corrente e tensão.

2. Poucos resultados em distribuição quântica de chaves são analíticos. Nesta direção, os resultados analíticos obtidos com a função de Lambert-Tsallis facilitam o entendimento da importância de alguns dos vários parâmetros envolvidos em um protocolo de QKD. Em particular, no caso estudado nesta tese, pode-se perceber na equação (3.15) a importância dos coeficientes de atenuação da fibra óptica e, portanto, da escolha correta dos comprimentos de onda utilizados para os canais clássico e quântico. Além disso, modelos mais completos para os dispositivos utilizados na realização de protocolos de QKD, como fontes, detectores e moduladores, permitem encontrar vulnerabilidades e contramedidas que as anulem. Portanto, a função de Lambert-Tsallis também é uma ferramenta matemática importante para o engenheiro quântico que, por exemplo, deseja determinar o comprimento que maximiza a taxa de transmissão de uma rede de acesso quântico.

3. O protocolo de QKD proposto nesta tese é, ao mesmo tempo, o um dos primeiros da história a detectar a presença de espionagem sem utilizar, de nenhuma forma, a taxa de erro. O que mostra o poder da disentropia. É também o mais simples dentre todos os protocolos de QKD já propostos pois, baseado apenas em modulação de amplitude, sua implementação prática não requer controle de polarização nem estabilização de interferômetros, sendo possível sua implementação apenas com um laser semicondutor, um atenuador e um detector de fótons. Entretanto, sua segurança contra uma espiã muito poderosa que efetue uma eficiente contagem de fótons não está garantida.

4. A demonstração experimental de um detector de fótons únicos remotamente acionado por luz abre novas possibilidade de implementação de protocolo de QKD, com Alice mais ativa e Bob mais passivo.

6.2 Perspectivas de Trabalhos Futuros

Como perspectivas de trabalhos futuros podem ser citados:

1. Desenvolver no LATIQ um gerador quântico de números aleatórios e usar a disentropia da autocorrelação e testes do NIST para verificar a qualidade das sequências aleatórias geradas.
2. Usar a disentropia da autocorrelação na detecção de espionagem em outros protocolos de QKD não considerados nesta tese.
3. Realizar a análise de segurança do protocolo de QKD proposto contra uma espiã que efetue uma eficiente contagem de fótons.
4. Melhorar a eficiência quântica do detector remotamente controlado para utilizá-lo em um sistema real de distribuição quântica de chaves.
5. Implementar o protocolo de QKD aqui proposto em laboratório.

REFERÊNCIAS

1 Corless, R. M.; Gonnet, G. H.; Hare, D. E. G.; Jeffrey, D. J.; Knuth, D. E. *On the Lambert W function*, Advances in Computational Mathematics, 5, 329 – 359, 1996.

2 Valluri, S. R.; Jeffrey, D. J.; Corless, R. M. *Some applications of the Lambert W function to Physics*, Canadian Journal of Physics, 78, 9, 823-831. 2000.

3 Silva, G. B da. *A função Wq de Lambert-Tsallis e suas aplicações*. 52p. Tese (Doutorado em Engenharia da Teleinformática) – Programa de Pós-graduação em Engenharia da Teleinformática. Universidade Federal do Ceará, Fortaleza, 2021.

4 Curado, E. M. F.; Tsallis, C. *Generalized statistical mechanics: connection with thermodynamics*, J. Phys. A: Math. Gen. 24, L69, 1991. doi: 10.1088/0305-4470/24/2/004

5 Tsallis, C. *Possible generalization of Boltzmann-Gibbs statistics*, J. Stat. Phys. 52, 479, 1988.

6 Silva, I. K. A. da. *Aplicações da função de Lambert-Tsallis em Contadores de Fótons*. 29p. (Mestrado em Engenharia da Teleinformática) – Instituto federal de Educação, Ciência e Tecnologia do Ceará IFCE, Fortaleza, 2023.

7 Ramos, R. V. *Estimation of the randomness of continuous and discrete signals using the disentropy of the autocorrelation*, SN Comput. Sci., 2, 254. 2021. doi.org/10.1007/s42979-021-00666-w

8 Almeida, F. J. L. de; Ramos, R. V. *Disentropy in astronomy*, Eur. Phys. J. Plus, 138, 20, 2023. doi.org/10.1140/epjp/s13360-022-03640-4

9 Castro, G. S.; Ramos, R. V. *Enhancing eavesdropping detection in quantum key distribution using disentropy measure of randomness*, Quant. Inf. Process., 21, 79, 2022. doi.org/10.1007/s11128-022-03422-y

10 Mendes, F.V.; Lima, C.; Ramos, R. V. *Applications of the Lambert–Tsallis Wq function in quantum photonic Gaussian boson sampling*. Quantum Inf Process 21, 215, 2022. doi.org/10.1007/s11128-022-03559-w

11 Andrade, J. S. de; Nobrega, K. Z.; Ramos, R. V. *Analytical solution of the current-voltage characteristics of circuits with power-law dependence of the current on the applied voltage using the Wq de Lambert-Tsallis function*, IEEE Trans. Circuits Syst. II Express Briefs. 2021. doi.org/10.1109/TCSII.2021.3110407

12 Rafiq, M. A. *Carrier transport mechanisms in semiconductor nanostructures and devices*, Journal of Semiconductors, Vol. 39, No. 6, 061002-1/13, 2018.

13 Xu, Wei; Chin, Alan; Ye, Laura; Ning, C. Z.; Yu, Hongbin. *Charge transport and trap characterization in individual GaSb nanowires*, J. Appl. Phys. 111, 104515-1/4, 2012. doi.org/10.1063/1.4720080

14 Rafiq, M. A.; Tsuchiya, Y.; Mizuta, H.; Oda, S.; Uno, Shigeyasu; Durrani, Z. A. K.; Milne,

W. I.; *Charge injection and trapping in silicon nanocrystals*, Appl. Phys. Lett. 87, 182101-1/3, 2005. doi.org/10.1063/1.2119431

15 Schricker, April D.; Davidson III, Forrest M.; Wiacek, Robert J.; Korgel, Brian A. *Space charge limited currents and trap concentrations in GaAs nanowires*, Nanotechnology 17. 2681–2688, 2006. doi:10.1088/0957-4484/17/10/040

16 Mark, P.; Helfrich, W. *Space-Charge-Limited Currents in Organic Crystals*. Journal of Applied Physics. 33, 1962, doi:10.1063/1.1728487

17 Dacuña, J.; Salleo, A. *Modeling Space-Charge Limited Currents in Organic Semiconductors: Extracting Trap Density and Mobility*, Phys. Rev. B 84, 195209/1-9, 2011.

18 Marinov, O.; Deen, M. J.; Datars, R. *Compact modeling of charge carrier mobility in organic thin-film transistors*, J. Appl. Phys. 106, 064501/1-13, 2009. doi.org/10.1063/1.3212539

19 Röhr, Jason A. et al. *On the correct interpretation of the low voltage regime in intrinsic single-carrier devices*, J. Phys.: Condens. Matter, 29, 205901/1-9, 2017.

20 Franz, Schauer. *Space-charge-limited currents for organic solar cells optimisation*, Solar Energy Materials & Solar Cells, 87, 235–250, 2005.

21 Kao, K. C.; Hwang, W. *Electrical Transport in Solids: With Particular Reference to Organic Semiconductors*. International series in the science of the solid state: Elsevier Science & Technology Books, A34, 174-175, 1981.

22 Lampert, M. A.; Mark, P. *Current injection in solids*. Science, 170: 966, 1970.

23 Mott, N. F.; Gurney, R. *W. Electronic processes in ionic crystals*. New York: Dover Publications, 2 ed., 275p, 1964.

24 Talin, A. A.; Léonard, F.; Katzenmeyer, A. M. et al. *Transport characterization in nanowires using an electrical nanoprobe*, Semicond. Sci. Technol., 25, 24015, 2010.

25 Talin, A. A.; Léonard, F.; Katzenmeyer, A. M. et al. *Unusually strong space charge-limited current in thin wires*, Phys Rev Lett, 101, 76802, 2008.

26 Lo, H.-K.; Curty, Curty, M.; Tamaki, K. *Secure quantum key distribution*, Nature Photonics, 18, 595-604, 2014.

27 Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N. J.; Dušek, M.; Lütkenhaus, N.; Peev, M. *The security of practical quantum key distribution*, Rev. Mod. Phys. 81, 1301–1350, 2009.

28 Inoue, K. *Differential phase-shift quantum key distribution systems*, IEEE Sel. Top. in Quant. Elec., 21, 3, 6600207, 2015.

29 Li, Y.-P.; Chen, W.; Wang, F.-X.; Yin, Z.-Q.; Zhang, L.; Liu, H.; Wang, S.; He, D.-Y.; Zhou, Z.; Guo, G.-C.; Han, Z.-F. *Experimental realization of a reference-frame independent decoy BB84 quantum key distribution based on Sagnac interferometer*, Optics Letters, 44, 18, 4523-4526, 2019.

30 Silva, J. R. da; Ramos, R. V. *Applications of the Lambert–Tsallis Function in X-Ray Free Electron Laser*, IEEE Transactions on Plasma Science, 50, 10, 3578-3582, 2022. doi: 10.1109/TPS.2022.3205545

31 Li, L.; Huang, P.; Wang, T.; Zeng, G. *Practical security of a chip-based continuous-variable quantum-key-distribution system*, Phys. Rev. A, 103, 032611/1-10, 2021.

32 Zheng, Y.; Liu, W.; Cao, Z.; Peng, J. *Monitoring scheme against local oscillator attacks for practical continuous-variable quantum-key- distribution systems in complex communication environments*, Phys. Rev. A, 101, 022319/1-10, 2020.

33 Aleksic, S.; Hipp, F.; Winkler, D.; Poppe, A.; Schrenk, B.; Franzl, G. *Perspectives and limitations of QKD integration in metropolitan area networks*, Opt. Express, Vol. 23, No. 8, 10359-10373, 2015, doi:10.1364/OE.23.010359

34 Bahrami, Arash; Lord, Andrew; Spiller, Timothy. *Quantum key distribution integration with optical dense wavelength division multiplexing: a review*, IET Quantum Commun., Vol. 1, no. 1, 9-15, 2020. doi: 10.1049/iet-qtc.2019.0005

35 Vorontsova, I.; Goncharov, R.; Tarabrina, A.; Kiselev, Fedor; Egorov, V. *Theoretical analysis of quantum key distribution systems when integrated with a DWDM optical transport network*, arXiv:2209.15507, 2022.

36 Patel, K. A.; Dynes, J. F.; Choi, I.; Sharpe, A.W.; Dixon, A. R.; Yuan, Z. L. Penty, R.V.; Shields, A. J. *Coexistence of High-Bit-Rate Quantum Key Distribution and Data on Optical Fiber*, Phys. Rev. X, 2, 041010/1-8, 2012.

37 Fröhlich, B.; Dynes, J. F.; Lucarini, M.; Sharpe, A. W.; Tam, S.; W. Yuan, -B.; Z.; Shields, A. J. *Quantum secured gigabit optical access networks*, Scientific Reports, 5, 18121/1-7, 2015. doi: 10.1038/srep18121.

38 Cai, C.; Sun, Y.; Ji, Y. *Intercore spontaneous Raman scattering impact on quantum key distribution in multicore fiber*, New J. Phys., 22, 083020/1-13, 2020. doi.org/10.1088/1367-2630/aba023

39 Wang, Bi-Xiao; Tang, Shi-Biao; Mao, Yingqiu; Xu, Wenhua; Cheng, Ming; Zhang, Jun; Chen, Teng-Yun; Pan, Jian-Wei. *Practical quantum access network over a 10 Gbit/s Ethernet passive optical network*, Optics Express, 29, 23, 38582/1-9, 2021. doi.org/10.1364/OE.442785.

40 Townsend, P. D. *Quantum cryptography on multiuser optical fiber networks*, Nature 385, 47–49, 1997.

41 Ma, X.; Qi, B.; Zhao, Y.; Lo, H.-K. *Practical decoy state for quantum key distribution*, Phys. Rev. A, 72, 012326/1-15, 2005. doi: 10.1103/PhysRevA.72.012326.

42 Damasceno, R.L.C.; Andrade, J. S.; Ramos, R.V. *Applications of the Lambert–Tsallis Wq function in QKD*, J. Opt. Soc. Am. B, 40, 9, 2280-2286, 2023,.

43 Liu, H. et al. *Field test of twin-field quantum key distribution through sending-or-not-sending over 428 km*, Phys. Rev. Lett., 126, 250502, 2021.

44 Liao, S. K.; Cai, W. Q.; Liu, W. Y. et al. *Satellite-to-ground quantum key distribution, Nature*, 549, 43, 2017.

45 Bennett, C. H.; Brassard, G. *Quantum Cryptography: Public Key Distribution and Coin Tossing*. in Proc. IEEE International Conference on Computers, Systems and Signal Processing. IEEE Press, New York, pp. 175–179, 1984. doi: 10.1016/j.tcs.2011.08.039

46 Bennet, C. H. *Quantum cryptography using any two non-orthogonal states*, Phys. Rev. Lett., 68, 3121, 1992.

47 Inoue, K.; Waks, E.; Yamamoto, Y. *Differential-phase-shift quantum key distribution using coherent light*, Phys. Rev. A, 68, 2, 022317, 2003.

48 Stucki, D.; Brunner, N.; Gisin, N.; Scarani, V.; Zbinden, H. *Fast and simple one-way quantum key distribution*. Appl. Phys. Lett., 87, 19, 194108, 2005.

49 Li, B.-H.; Xie, Y.-M.; Li, Z.; Weng, C.-X.; Li, C.-L.; Yin, H.-L.; Chen, Z.-B. *Long-distance twin-field quantum key distribution with entangled sources*, Opt. Lett., 46, 22, 5529, 2021.

50 Zeng, P.; Zhou, H.; Wu, W.; Ma, X., *Mode-pairing quantum key distribution*, Nat. Comm, 13, 3903, 2022.

51 Lo, H.-K.; Curty, M.; Qi, B. *Measurement-device-independent quantum key distribution*, Phys. Rev. Lett., 108, 130503, 2012.

52 Pinheiro, P. V. P.; Ramos, R. V. *Two-layer quantum key distribution*, Quantum Inf Process, 14, 2111, 2015.

53 de Oliveira, G. L.; Ramos, R.V.; *Quantum-chaotic cryptography*, Quantum Inf Process 17, 40, 2018.

54 Garay-Palmett, at al. *Fiber-based photon-pair generation: tutorial*, J. Opt. Soc. of Am., 40, 3, 469 (2023).

55 Thomas, S. E. at al. *Bright polarized single-photon source based on a linear dipole*, Phys. Rev. Lett., 126, 233601 (2021).

56 Raupach, S. M. F. at al., *Detection rate dependence of the inherent detection efficiency in single-photon detectors based on avalanche diodes*, Phys. Rev. A, 105, 042615 (2022).

57 Fukuda, D.; Fujii, G.; Numata, T.; Amemiya, K.; Yoshizawa, A.; Tsuchida, H.; Fujino, H.; et al., *Titanium superconducting photon-number-resolving detector*. IEEE Trans. Appl. Supercond. 21, 3, 241, 2011.

58 Li, L.; Wang, T.; Li, X.; Huang, P.; Guo, Y.; Lu, L.; Zhou, L.; Zeng, G. *Continuous-variable quantum key distribution with on-chip light sources*, Photon. Research, 11, 4, 504, 2023.

59 Xavier, G. B.; de Faria, G. V.; Temporão, G. P.; von der Weid, J. P., *Full polarization control for fiber optical quantum communication systems using polarization encoding*, Opt. Express, 16, 3, 1873, 2008.

60 Peranić, M.; Clark, M.; Wang, R.; et al. *A study of polarization compensation for quantum networks*, EPJ Quant. Technol., 10, 30, 2023.

61 Pereira, D.; Pinto, A. N.; Silva, N. A. *Polarization diverse true heterodyne receiver architecture for continuous variable quantum key distribution*, J. of Lightwave Tech., 41, 2, 432, 2023.

62 Zhang, H.; Liu, P.; Guo, Y.; Zhang, L.; Huang, D. *Blind modulation format identification using the DBSCAN algorithm for continuous-variable quantum key distribution*, J. Opt. Soc. of Am., 36, 3, B51, 2019.

63 da Silva, G.B.; Ramos, R.V. *The Lambert–Tsallis Wq function*, Physica A, 525, 164, 2019.

64 Ramos, R.V. *Disentropy of the Wigner function*, J. Opt. Soc. of Am. B, 36, 8, 2244, 2019.

65 Trenyi, R.; Curty, M. *Zero-error attack against coherent-one-way quantum key distribution*, New J. Phys., 23, 093005, 2021.

66 S. Sajeed; C. Minshull; N. Jain; V. Makarov. *Invisible Trojan-horse attack*, Scientific Reports, 7, 8403/1-7, 2017.

67 Yuan, Z. L.; Dixon, A. R.; Dynes, J. F.; Sharpe, A. W.; Shields, A. J. *Gigahertz quantum key distribution with InGaAs avalanche photodiodes*, Appl. Phys. Lett. 92, 20, 201104, 2008.

68 Chen, J.; Wu, G.; Xu, L.; Gu, X.; Wu, E.; Zeng, H. *Stable quantum key distribution with active polarization control based on time-division multiplexing*, N. J. Phys., 11, 6, 065004, 2009.

69 Scarani, V. et al., *The security of practical quantum key distribution*, Rev. Mod. Phys. 81, 1301–1350, 2009.

70 Santabaia, M. D. C.; Mendonça, F. A.; Ramos, R. V. *Spectral method for characterization of avalanche photodiode working as single-photon detector*, Opt. Lett., 36, 17, 3446, 2011.

71 Castro, Giselle Silva; Andrade, Joacir Soares de; Damasceno, Ranara Louise Campo; Silva, Joao Batista Rosa; Ramos, Rubens Viana. *Remotely Gated InGaAs Single-Photon Detector at 1550 nm*, IEEE PHOTONICS TECHNOLOGY LETTERS, v. 1, p. 1-1, 2019.

ANEXO A – RESULTADOS DAS APLICAÇÕES LAMBERT-TSALLIS EM QKD NO TÓPICO 3

Usando (3.1)-(3.2) e (3.10), obtém-se facilmente

$$p_R = \frac{\Delta f \Delta t \eta_B P \beta}{Nhf\left(\alpha_q - \alpha_c\right)}\left(e^{-\alpha_c L} - e^{-\alpha_q L}\right) . \tag{A.1}$$

Para inverter a eq. (A.1), pode-se seguir os seguintes passos:

$$e^{-\alpha_c L} - e^{-\alpha_q L} = z, \;\; z = \frac{Nhf\left(\alpha_q - \alpha_c\right) p_R}{\Delta f \Delta t \eta_B P \beta} \Rightarrow \tag{A.2}$$

$$e^{-\alpha_q L}\left(1 - e^{\left(\alpha_q - \alpha_c\right)L}\right) = -z \Rightarrow \tag{A.3}$$

$$e^{-\alpha_q L} e_0^{-e^{\left(\alpha_q - \alpha_c\right)L}} = -z \Rightarrow \tag{A.4}$$

$$\left[e^{-\alpha_q L} e_0^{-e^{\left(\alpha_q - \alpha_c\right)L}}\right]^{-\frac{\left(\alpha_q - \alpha_c\right)}{\alpha_q}} = \left(-z\right)^{-\frac{\left(\alpha_q - \alpha_c\right)}{\alpha_q}} \Rightarrow \tag{A.5}$$

$$e^{\left(\alpha_q - \alpha_c\right)L} e^{\frac{\frac{\left(\alpha_q - \alpha_c\right)}{\alpha_q} e^{\left(\alpha_q - \alpha_c\right)L}}{1 + \frac{\alpha_q}{\left(\alpha_q - \alpha_c\right)}}} = \left(-z\right)^{-\frac{\left(\alpha_q - \alpha_c\right)}{\alpha_q}} \Rightarrow \tag{A.6}$$

$$\frac{\left(\alpha_q-\alpha_c\right)}{\alpha_q}e^{\left(\alpha_q-\alpha_c\right)L}e^{\frac{\left(\alpha_q-\alpha_c\right)}{\alpha_q}e^{\left(\alpha_q-\alpha_c\right)L}}{}^{1+\frac{\alpha_q}{\left(\alpha_q-\alpha_c\right)}} = \frac{\left(\alpha_q-\alpha_c\right)}{\alpha_q}\left(-z\right)^{-\frac{\left(\alpha_q-\alpha_c\right)}{\alpha_q}} \Rightarrow \tag{A.7}$$

$$\frac{\left(\alpha_q-\alpha_c\right)}{\alpha_q}e^{\left(\alpha_q-\alpha_c\right)L} = W_{1+\frac{\alpha_q}{\left(\alpha_q-\alpha_c\right)}}\left(\frac{\left(\alpha_q-\alpha_c\right)}{\alpha_q}\left(-z\right)^{-\frac{\left(\alpha_q-\alpha_c\right)}{\alpha_q}}\right) \Rightarrow \tag{A.8}$$

$$L = \frac{1}{\alpha_q-\alpha_c}\ln\left\{\frac{\alpha_q}{\alpha_q-\alpha_c}W_{1+\frac{\alpha_q}{\left(\alpha_q-\alpha_c\right)}}\left(\frac{\left(\alpha_q-\alpha_c\right)}{\alpha_q}\left(-z\right)^{-\frac{\left(\alpha_q-\alpha_c\right)}{\alpha_q}}\right)\right\}. \tag{A.9}$$

Para obter (3.18) - (3.19) de (3.16) - (3.17), pode-se seguir os seguintes passos: (A = -8.8·10^{-22} ($2\pi/\lambda$)L, B = -8.5·10^{-18}($2\pi/\lambda$)L e r é dada pela eq.. (3.17))

$$Ar + Br^{0.8} = arc\sin\left(1-\frac{x_{0A}^2}{2x_{10}^2}\right) = z \Rightarrow \tag{A.10}$$

$$r^{0.8}\left(1+\frac{A}{B}r^{0.2}\right) = \frac{z}{B} \Rightarrow r^{0.8}e_0^{\frac{A}{B}r^{0.2}} = \frac{z}{B} \Rightarrow \tag{A.11}$$

$$\left(r^{0.8}e_0^{\frac{A}{B}r^{0.2}}\right)^{\frac{0.2}{0.8}} = \left(\frac{z}{B}\right)^{\frac{0.2}{0.8}} \Rightarrow r^{0.2}e_{-3}^{\frac{A}{4B}r^{0.2}} = \left(\frac{z}{B}\right)^{\frac{1}{4}} \Rightarrow \tag{A.12}$$

$$\frac{A}{4B}r^{0.2}e_{-3}^{\frac{A}{4B}r^{0.2}} = \frac{A}{4B}\left(\frac{z}{B}\right)^{\frac{1}{4}} \Rightarrow \frac{A}{4B}r^{0.2} = W_{-3}\left(\frac{A}{4B}\left(\frac{z}{B}\right)^{\frac{1}{4}}\right) \Rightarrow \tag{A.13}$$

$$r = \left[\frac{4B}{A} W_{-3}\left(\frac{A}{4B}\left(\frac{z}{B} \right)^{\frac{1}{4}} \right) \right]^5 . \tag{A.14}$$

Por fim, eq. (3.22) pode ser obtido da seguinte maneira : ($\tau = (T/T_0)^{1/2}$)

$$\frac{1-\lambda^{3/2}}{1-\lambda} = \frac{3}{2}\tau \Rightarrow \frac{3}{2}\tau\lambda - \lambda^{3/2} = \frac{3}{2}\tau - 1 \Rightarrow \tag{A.15}$$

$$\lambda\left(1 - \frac{2}{3\tau}\lambda^{1/2}\right) = 1 - \frac{2}{3\tau} \Rightarrow \lambda e_0^{-\frac{2}{3\tau}\lambda^{1/2}} = 1 - \frac{2}{3\tau} \Rightarrow \tag{A.16}$$

$$\sqrt{\lambda e_0^{-\frac{2}{3\tau}\lambda^{1/2}}} = \sqrt{1 - \frac{2}{3\tau}} \Rightarrow \lambda^{1/2} e_{-1}^{-\frac{1}{3\tau}\lambda^{1/2}} = \sqrt{1 - \frac{2}{3\tau}} \Rightarrow \tag{A.17}$$

$$-\frac{1}{3\tau}\lambda^{1/2} e_{-1}^{-\frac{1}{3\tau}\lambda^{1/2}} = -\frac{1}{3\tau}\sqrt{1 - \frac{2}{3\tau}} \Rightarrow \tag{A.18}$$

$$-\frac{1}{3\tau}\lambda^{1/2} = W_{-1}\left(-\frac{1}{3\tau}\sqrt{1 - \frac{2}{3\tau}} \right) \Rightarrow \tag{A.19}$$

$$\lambda = 9\frac{T}{T_0} W_{-1}^2\left(-\frac{1}{3}\sqrt{\frac{T_0}{T}}\sqrt{1 - \frac{2}{3}\sqrt{\frac{T_0}{T}}} \right) . \tag{A.20}$$

ANEXO B - LISTA DE ARTIGOS PUBLICADOS E SUBMETIDOS

1. G. S. Castro, **J. S. de Andrade**, R. L. C. Damasceno, J. B. Rosa Silva and R. V. Ramos, "Remotely Gated InGaAs Single-Photon Detector at 1550 nm", *IEEE Photonics Technology Letters*, vol. 32, no. 2, pp. 129-131, (2020) doi: 10.1109/LPT.2019.2960773.

2. **J. S. de Andrade**, K. Z. Nobrega and R. V. Ramos, "Analytical solution of the current-voltage characteristics of circuits with power-law dependence of the current on the applied voltage using the Lambert-Tsallis Wq function", *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 69, no. 3, pp. 769-773, (2022) doi: 10.1109/TCSII.2021.3110407.

3. R. L. C. Damasceno, **J. S. de Andrade**, and R. V. Ramos, "Applications of the Lambert–Tsallis Wq function in QKD", J. Opt. Soc. Am. B 40, 2280-2286 (2023)

4. **J. S. de Andrade**, K. Z. Nobrega, J. B. R. Silva, and R. V. Ramos, Eavesdropping detection without using error rate: The disentropy-based quantum key distribution, 2023. (submitted)