UNIVERSIDADE FEDERAL DO CEARÁ

CENTRO DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA DE TELEINFORMÁTICA

PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA DE TELEINFORMÁTICA

FRANCISCO FRANKLIN SOUSA RIOS

CONTRIBUIÇÕES À ANÁLISE DE SEGURANÇA DE PROTOCOLOS DE CRIPTOGRAFIA QUÂNTICA

FORTALEZA

2018

FRANCISCO FRANKLIN SOUSA RIOS

CONTRIBUIÇÕES À ANÁLISE DE SEGURANÇA DE PROTOCOLOS DE CRIPTOGRAFIA QUÂNTICA

Tese apresentada ao Programa de Pós-Graduação em Engenharia de Teleinformática da Universidade Federal do Ceará, como parte dos requisitos para obtenção do título de Doutor em Engenharia de Teleinformática. Área de concentração: Eletromagnetismo Aplicado.

Orientador: Prof. Dr. Rubens Viana Ramos.

FORTALEZA

2018

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

R453c Rios, Francisco Franklin Sousa.
Contribuições à análise de segurança de protocolos de criptografia quântica / Francisco Franklin Sousa Rios. – 2018.
95 f. : il. color.

Tese (doutorado) – Universidade Federal do Ceará, Centro de Tecnologia, Programa de Pós-Graduação em Engenharia de Teleinformática, Fortaleza, 2018.
Orientação: Prof. Dr. Rubens Viana Ramos.

1. Compromisso Quântico de Informação. 2. Distribuição Quantum-caótica de Chaves. 3. Detecção Homódina. I. Título.

CDD 621.38

FRANCISCO FRANKLIN SOUSA RIOS

CONTRIBUIÇÕES À ANÁLISE DE SEGURANÇA DE PROTOCOLOS DE CRIPTOGRAFIA QUÂNTICA

Tese apresentada ao Programa de Pós-Graduação em Engenharia de Teleinformática da Universidade Federal do Ceará, como parte dos requisitos para obtenção do título de Doutor em Engenharia de Teleinformática. Área de concentração: Eletromagnetismo Aplicado.

Aprovada em: 29/ 06 / 2018.

BANCA EXAMINADORA

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

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

Prof. Dr. José Augusto Oliveira Huguenin
Universidade Federal Fluminense (UFF)

Prof. Dr. Sebastião José Nascimento de Pádua
Universidade Federal de Minas Gerais
(UFMG)

Prof. Dr. Fabio Alencar Mendonca
Instituto Federal de Educação, Ciência e
Tecnologia do Ceará (IFCE)

Aos meus pais, irmãs e namorada pelo incentivo e apoio. A meus amigos pelo companheirismo. Dedico.

AGRADECIMENTOS

Agradeço ao Prof. Dr. Rubens Viana Ramos pelos ensinamentos, amizade e apoio, me mostrando de forma concreta como se faz ciência.

Agradeço aos meus pais, José Waldery Rios e Maria Socorro Sousa Rios e irmãs, Perpétua Socorro Sousa Rios, Kênia Sousa Rios e Ana Luiza Sousa Rios, pelo amor, dedicação, incentivo, formação pessoal e educação.

Agradeço a Amanda Modesto de Oliveira pela cumplicidade em todos os momentos, carinho, compreensão e sobretudo pelo amor.

Agradeço à UFC e CAPES pelo apoio institucional e financeiro.

Agradeço aos professores, em especial ao Professor João Batista e a professora Hilma Vasconcelos, pela formação acadêmica e por contribuírem para o profissional que sou hoje.

Agradeço também a todos os colegas de laboratório Glaucionor, Ranara, Claudomir, Tahim, Samy, George, Fernando, Paulo Régis e Paulo Vinícius pelo companheirismo, a ajuda e pelos momentos de descontração. Em especial ao colega Geovan Guerra, que contribuiu nos experimentos de detecção homódina e na autoria de dois artigos decorrentes desta tese.

E a todos que de uma alguma forma, me ajudaram nesta conquista.

"Somente depois da última árvore derrubada, depois do último animal extinto, e quando perceber o último rio poluído, sem peixe, o homem verá que dinheiro não se come".

(Provérbio Indígena)

RESUMO

A presente tese pode ser dividida em três partes: I) Análise de segurança do protocolo quântico de compromisso de informação (QBC). II) Distribuição quantum-caótica de chaves (QCKD) com pulsos multifótons. III) Detecção homódina de estados coerentes atenuados. No que diz respeito à análise de segurança do protocolo de compromisso de informação, foi demonstrado que, levando em consideração a largura espectral dos pulsos ópticos e a dependência com a frequência de portas quânticas ópticas, o protocolo de QBC, ao contrário do que se pensava anteriormente, não é incondicionalmente inseguro. No que concerne à distribuição quantum-caótica de chaves, devido ao uso de estados coerentes com fases contínuas, a espiã faz um ataque usando tomografia quântica homódina. Neste caso, foi demonstrado que o transmissor pode usar estados coerentes com número médio de fótons bem maior que o valor tradicionalmente usado em protocolos de distribuição quântica de chaves – *Quantum key distribution*- (QKD) e o protocolo de QCKD ainda será seguro. Por fim, na parte da detecção homódina de fótons, foi realizado um experimento de detecção homódina de fótons no qual um sinal analógico modulante transportado por um estado coerente fortemente atenuado é recuperado por um receptor óptico baseado em fotodiodo PIN.

Palavras-chave: Compromisso Quântico de Informação. Distribuição Quantum-caótica de Chaves. Detecção Homódina.

ABSTRACT

This thesis can be divided in three parts: I) Security analysis of quantum bit commitment (QBC). II) Quantum-chaotic key distribution (QCKD) using multiphoton pulses. III) Homodyne detection of weak coherent states. In respect to the security analysis of quantum bit commitment, it was shown that if one takes into account the spectral width of the light pulses and the frequency dependence of optical quantum gates, the QBC, contrary to what was previously considered, is not unconditionally insecure. In what concerns the QCKD, the usage of coherent states with continuous phase forces the eavesdropper to use an attack based on quantum homodyne tomography. In this case, it was shown that the transmitter can use coherent states with mean photon number much larger than the value traditionally used in quantum key distribution QKD, and the QCKD will still be secure. At last, in the homodyne detection part, an experiment was realized showing the detection, by an optical receiver based on PIN photodiode, of an analog modulating signal carried by a strongly attenuated coherent state.

Keywords: Quantum Bit Commitment. Quantum-Chaotic Key Distribution. Homodyne Detection.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

APD	Fotodiodo de avalanche.
BC	Compromisso de informação.
BS	Divisor de feixes.
EPR	Einstein-Podolsky-Rosen
HOM	Hong-Ou-Mandel.
IMZ	Interferômetro de Mach-Zehnder.
PBS	Divisor de feixes dependente da polarização.
PIN	Fotodiodo *Positive-Intrinsic-Negative.*
QBC	Protocolos quânticos de compromisso da informação.
QCKD	Distribuição quantum-caótica de chaves.
QKD	Distribuição quântica de chaves.
SPD	Detector de fótons únicos.

SUMÁRIO

1 INTRODUÇÃO

Desde o início da era da informação quântica protocolos e sistemas de computação quânticos usando fótons únicos, fótons entrelaçados e estados coerentes têm sido propostos. Por exemplo, a interferência de fótons únicos é uma ferramenta crucial para a realização experimental de comunicação quântica, computação quântica e esquemas de metrologia quântica. O Teletransporte de um qubit óptico necessita de estados entrelaçados de dois fótons enquanto diversas configurações de protocolos de distribuição quântica de chaves – *quantum key distribution* - (QKD) usam estados coerentes atenuados. No entanto, em geral, suas descrições são baseadas em pulsos ópticos de frequência única. Normalmente, a interferência de um único fóton é analisada como se os fótons fossem produzidos por uma fonte óptica de uma única frequência, sua propagação em fibras ópticas estivesse livre de efeitos dispersivos e o comportamento dos dispositivos ópticos, como divisores de feixe, rotacionadores de polarização e moduladores de fase, não dependessem da frequência. Estas são, obviamente, simplificações da situação real. Uma fonte de frequência única violaria o princípio da incerteza de Heisenberg e, portanto, não existe. Além disso, os dispositivos ópticos são feitos de vidro e o índice de refração depende da frequência. Assim, divisores de feixes reais, rotacionadores de polarização e moduladores de fase são dispositivos dependentes da frequência. Desta forma, uma análise mais realista da segurança de protocolos de criptografia quântica em redes ópticas requer a consideração de campos contínuos na frequência, isto é, a largura espectral deve ser levada em consideração (SANTOS *et al.*, 1997). Nessa direção, a primeira parte da presente tese discute o uso de estados contínuos de um e dois fótons em algumas configurações ópticas típicas de protocolos de criptografia quântica e a segurança destes.

Devido ao grande tráfego de dados sigilosos pelas redes ópticas de comunicações, protocolos de segurança de dados são cruciais. Estes podem ser baseados na complexidade da solução de problemas matemáticos ou em sistemas físicos. Neste último caso, as duas tecnologias de segurança mais importantes são a criptografia caótica e a distribuição quântica de chaves. Recentemente o uso conjunto destas duas tecnologias, chamada de distribuição quantum-caótica de chaves (QCKD) (OLIVEIRA, DE; RAMOS, 2018), abriu a perspectiva para mudanças significativas nos protocolos quânticos. Nesta direção, a segunda parte desta tese mostra que a QCKD permite o uso de estados coerentes propagando no canal óptico com

número médio de fótons muito maior que 0,1, o valor tradicionalmente usado em sistemas de QKD.

Por fim, o grande desafio dos protocolos de criptografia quântica é a realização experimental dos mesmos. Um elemento crucial da realização experimental é a detecção de fótons. A detecção de fótons normalmente utiliza fotodiodos de avalanche (APDs). Eles requerem um resfriamento por causa do ruído de escuro[1], tempo de relaxação por causa da contagem de pós-pulso[2], alta voltagem de operação e são caros. Uma outra opção é a utilização de detecção homódina com fotodiodo PIN. As vantagens são o baixo preço, a baixa voltagem de operação, a inexistência de contagem de pós-pulso e o resfriamento é desnecessário. Nesta direção, a terceira parte desta tese apresenta um experimento de detecção homódina de estados coerentes fortemente atenuados, usando fotodiodos PIN.

Este trabalho está organizado da seguinte forma: no Capítulo 2 a teoria de estados contínuos de um e dois fótons, com foco na interferência, é revista. No Capítulo 3 é apresentada a análise de segurança de um protocolo de compromisso de informação levando em consideração a largura espectral dos pulsos ópticos utilizados. O Capítulo 4 discute a distribuição quantum-caótica de chaves usando pulsos multifótons. O Capítulo 5 mostra os resultados experimentais da detecção homódina de luz coerente fortemente atenuada. Por fim, as conclusões e perspectivas de trabalhos futuros são mostradas no Capítulo 6.

[1] O efeito de avalanche no detector não é causado somente pela absorção de fótons, outros mecanismos que geram pares elétron-buraco, na maior parte na maior parte dos casos, devido ao efeito térmico. Visto que esse ruído ocorre mesmo sem luz incidindo no detector, ele é chamado de ruído de escuro (*dark noise*) e, os pulsos elétricos gerados, de contagem de escuro (*dark counts*).

[2] Após a extinção de uma avalanche alguns elétrons ficam presos na região onde atua o campo elétrico e pode ocorrer uma nova avalanche causada por estes elétrons remanescentes. A esta detecção espúria que não é causada pela detecção de fótons damos o nome de detecção de pós-pulso.

2 INTERFERÊNCIA DE ESTADOS CONTÍNUOS DE UM E DOIS FÓTONS

2.1 Introdução

Neste capítulo é revisada a teoria de estados contínuos de um e dois fótons, bem como é considerado o efeito da largura espectral de fótons únicos em duas situações: interferência de um fóton único, interferência entre dois fótons únicos provenientes de diferentes fontes, a interferência de Hong-Ou-Mandel (HOM).

2.2 Estados Contínuos de Um e Dois Fótons

O estado contínuo do fóton único é dado por (SANTOS *et al.*, 1997)

$$\left|1_{\omega}\right\rangle = \int_0^{\infty} \sigma(\omega)\hat{a}^{+}(\omega)d\omega\left|0_{\omega}\right\rangle, \tag{1.1}$$

$$\int_0^{\infty} \left|\sigma(\omega)\right|^2 d\omega = 1. \tag{1.2}$$

Em (1.1) o estado $|0_{\omega}\rangle$ é o estado contínuo do vácuo e, consequentemente, $\hat{a}(\omega)\left|0_{\omega}\right\rangle = 0$, sendo que $\hat{a}(\omega)$ é o operador de aniquilação contínuo. Além disso, $|\sigma(\omega)|^2 d\omega$ dá a probabilidade da frequência do fóton pertencer ao intervalo $(\omega, \omega + d\omega)$. Para trabalhar com o fóton único contínuo em esquemas de comunicação quântica, primeiro faz-se sua discretização. Comecemos escrevendo $\sigma(\omega)$ na base das funções sinc[3] (a discretização usando as funções sinc facilita o cálculo das probabilidades importantes consideradas na taxa de erro e na análise de segurança) (RAMOS; SOUZA, 2001):

[3] O termo "sinc" é uma contração do nome da função em latim *sinus cardinalis* (seno cardinal), denotada por sinc(*x*) e às vezes como *Sa*(*x*). A função sinc normalizada é definida pela equação (1.4).

$$\sigma(\omega)=\sum_{k=-\infty}^{\infty}\sigma(k\omega_s)\,\mathrm{sinc}\left[(\omega-k\omega_s)/\omega_s\right], \tag{1.3}$$

$$\mathrm{sinc}(x)=\sin(\pi x)/\pi x. \tag{1.4}$$

Em (1.3) ω_s é o passo da discretização no domínio da frequência. Assim, $\sigma(k\omega_s)$ é o valor de $\sigma(\omega)$ em $\omega=k\omega_s$ e k é um número inteiro. Usando a ortogonalidade da função sinc,

$$\frac{1}{\omega_s}\int_{-\infty}^{\infty}\mathrm{sinc}\left[\frac{(\omega-k\omega_s)}{\omega_s}\right]\mathrm{sinc}\left[\frac{(\omega-m\omega_s)}{\omega_s}\right]d\omega=\delta_{km}, \tag{1.5}$$

e o fato de $\sigma(\omega)$ ser zero para frequências negativas, temos que

$$\int_0^{\infty}\left|\sigma(\omega)\right|^2 d\omega=\int_{-\infty}^{\infty}\left|\sigma(\omega)\right|^2 d\omega=\sum_{k=1}^{\infty}\left|\sigma(k\omega_s)\right|^2\omega_s=1. \tag{1.6}$$

A equação (1.6) mostra como representar discretamente o estado contínuo de fóton único:

$$\left|1_\omega\right\rangle=\sum_{k=1}^{\infty}\sigma(k\omega_s)\sqrt{\omega_s}\left|0\right\rangle_1\otimes\ldots\otimes\left|1\right\rangle_k\otimes\ldots \tag{1.7}$$

Segundo a equação (1.7), estado contínuo de fóton único pode ser aproximado por uma superposição do produto tensorial de osciladores discretos. Cada oscilador discreto trabalha em uma única frequência. Por exemplo, o estado $|0_1\rangle\otimes\ldots\otimes|1_k\rangle\otimes\ldots$ significa um fóton

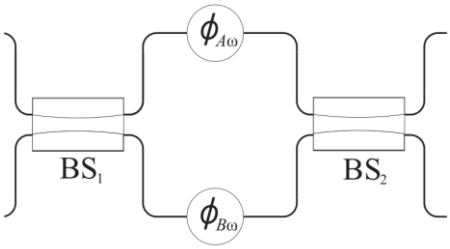
na frequência $k\omega_s$ e zero fótons nas outras frequências. O número de osciladores discretos é igual ao número de amostras de $\sigma(\omega)$ e a amplitude de probabilidade do *k*-ésimo termo na superposição é dada por $\sigma(k\omega_s)(\omega_s)^{1/2}$. Agora, se $\sigma(\omega)$ se anula para o $\omega > N\omega_s$, então, o número de osciladores é finito:

$$|1_\omega\rangle = \sum_{k=1}^{N} \sigma(k\omega_s)\sqrt{\omega_s}\,|\tilde{1}\rangle_k\,, \tag{1.8}$$

$$|\tilde{1}\rangle_k = |0\rangle_1 \otimes \ldots \otimes |1\rangle_k \otimes \ldots \otimes |0\rangle_N\,. \tag{1.9}$$

Para estudar a interferência de um único fóton, consideraremos o comportamento do estado quântico dado pela equação (1.8) num interferômetro de Mach-Zehnder (IMZ) cujos moduladores de fase dependem da frequência (para incluir a dependência de frequência dos divisores de feixe é apenas um exercício de álgebra).

Figura 1 - Interferômetro Mach-Zehnder com divisores de feixe balanceados sem perda e moduladores de fase dependentes da frequência ($\phi_{A\omega} \rightarrow \phi_A(\omega)$ e $\phi_{B\omega} \rightarrow \phi_B(\omega)$)



Fonte: Elaborada pelo autor.

O IMZ é composto por dois divisores de feixe sem perdas com transmitância $T = 1/2^{1/2}$ (e reflectância $R = i1/2^{1/2}$), e um modulador de fase em cada braço, $\phi_A(\omega)$ e $\phi_B(\omega)$. Esse interferômetro é útil nas configurações de protocolos de distribuição quântica de chaves. O estado de entrada é $|1_\omega\rangle|0_\omega\rangle$. O Esquema é mostrado na Figura 1.

Após algum desenvolvimento matemático obtém-se o seguinte estado quântico total na saída do interferômetro

$$\left|\psi_{\omega}\right\rangle = \sum_{k=1}^{N} \sigma\left(k\omega_s\right)\sqrt{\omega_s}\left|0\right\rangle_1\left|0\right\rangle_1 \otimes ... \otimes \left|\xi_{\omega}\right\rangle_k \otimes ... \otimes \left|0\right\rangle_N\left|0\right\rangle_N , \tag{1.10}$$

$$\left|\xi_{\omega}\right\rangle_k = ie^{i\Omega_k}\left\{\cos\left(\Delta_k\right)\left|1\right\rangle_k^a\left|0\right\rangle_k^b + \sin\left(\Delta_k\right)\left|0\right\rangle_k^a\left|1\right\rangle_k^b\right\}, \tag{1.11}$$

$$\Omega_k = \left[\phi_A\left(k\omega_s\right) + \phi_B\left(k\omega_s\right)\right]/2;\ \Delta_k = \left[\phi_A\left(k\omega_s\right) - \phi_B\left(k\omega_s\right)\right]/2. \tag{1.12}$$

Desta forma, as probabilidades do fóton emergir nas saídas *a* e *b* do interferômetro são dadas por

$$p_a = \sum_{k=1}^{N} \cos^2\left[\frac{\phi_A(k\omega_s) - \phi_B(k\omega_s)}{2}\right]\left|\sigma\left(k\omega_s\right)\right|^2 \omega_s , \tag{1.13}$$

$$p_b = \sum_{k=1}^{N} \sin^2\left[\frac{\phi_A(k\omega_s) - \phi_B(k\omega_s)}{2}\right]\left|\sigma\left(k\omega_s\right)\right|^2 \omega_s , \tag{1.14}$$

ou, retornando ao caso contínuo,

$$p_a = \int_0^{\infty} \cos^2\left[\frac{\phi_A(\omega) - \phi_B(\omega)}{2}\right]\left|\sigma\left(\omega\right)\right|^2 d\omega , \tag{1.15}$$

$$p_b = \int_0^{\infty} \sin^2\left[\frac{\phi_A(\omega) - \phi_B(\omega)}{2}\right]\left|\sigma\left(\omega\right)\right|^2 d\omega . \tag{1.16}$$

Observando as equações (1.15) e (1.16) verifica-se que a dependência da frequência pode aumentar a taxa de erro de um protocolo de QKD (este erro pode ser levado em

consideração através da visibilidade do interferômetro) ou pode ser utilizado para aumentar a segurança de um protocolo criptográfico quântico (GUERRA *et al.*, 2016).

Seja, agora, o experimento de HOM: a interferência entre dois pulsos contínuos de fótons únicos, provenientes de diferentes fontes, incidindo ao mesmo tempo em um divisor de feixes balanceado ao mesmo tempo e com a mesma polarização. O estado total na saída do divisor de feixes é

$$\begin{aligned} U_{BS}\left|1_{\omega}\right\rangle\left|1_{\omega}\right\rangle &= U_{BS}\left(\sum_{k=1}^{N}\sigma(k\omega_s)\sqrt{\omega_s}\left|\tilde{1}\right\rangle_k\right)\otimes\left(\sum_{l=1}^{N}\xi(l\omega_s)\sqrt{\omega_s}\left|\tilde{1}\right\rangle_l\right) \\ &= \sum_{k,l=1}^{N}\sigma(k\omega_s)\,\xi(l\omega_s)\,\omega_s U_{BS}\left|\tilde{1}\right\rangle_k\left|\tilde{1}\right\rangle_l. \end{aligned} \tag{1.17}$$

$$U_{BS}\left|\tilde{1}\right\rangle_k\left|\tilde{1}\right\rangle_l = \begin{cases} \left|0\right\rangle_1^a\left|0\right\rangle_1^b\otimes\ldots\otimes\left|\mu\right\rangle_k\otimes\ldots\otimes\left|\mu\right\rangle_l\otimes\ldots\otimes\left|0\right\rangle_N^a\left|0\right\rangle_N^b & \text{se } k\neq l, \quad (1.18) \\ \left|0\right\rangle_1^a\left|0\right\rangle_1^b\otimes\ldots\otimes\left|\lambda\right\rangle_k\otimes\ldots\otimes\left|0\right\rangle_N^a\left|0\right\rangle_N^b & \text{se } k=l, \quad (1.19) \end{cases}$$

$$\left|\mu\right\rangle_{r=k,l} = \cos\left(\theta(r\omega_s)\right)\left|1\right\rangle_r^a\left|0\right\rangle_r^b + i\sin\left(\theta(r\omega_s)\right)\left|0\right\rangle_r^a\left|1\right\rangle_r^b, \tag{1.20}$$

$$\left|\lambda\right\rangle_k = \sin\left(2\theta(k\omega_s)\right)\frac{\left|2\right\rangle_k^a\left|0\right\rangle_k^b + \left|0\right\rangle_k^a\left|2\right\rangle_k^b}{\sqrt{2}} + i\cos\left(2\theta(k\omega_s)\right)\left|1\right\rangle_k^a\left|1\right\rangle_k^b. \tag{1.21}$$

Na equação (1.17) $U_{BS}(\omega)$ é a operação unitária do divisor de feixes dependente da frequência.

$$U_{BS} = \begin{pmatrix} t & r \\ r' & t' \end{pmatrix} = \begin{pmatrix} \cos\left[\theta(\omega)\right] & i\text{sen}\left[\theta(\omega)\right] \\ i\text{sen}\left[\theta(\omega)\right] & \cos\left[\theta(\omega)\right] \end{pmatrix} \tag{1.22}$$

A transmitância (t) e reflectância (r) são, respectivamente, $\cos[\theta(\omega)]$ e $i\text{sen}[\theta(\omega)]$. Nas equações (1.18)-(1.21) a e b são os modos de saída do divisor de feixes. Usando as equações (1.17)-(1.21), obtém-se a probabilidade de coincidência, p_{coin},

$$p_{coin} = \sum_{\substack{k,l=1 \\ k\neq l}}^{N} \left|\sigma\left(k\omega_s\right)\xi\left(l\omega_s\right)\right|^2 \omega_s^2 \left[\begin{array}{l}\cos^2\left(\theta\left(k\omega_s\right)\right)\cos^2\left(\theta\left(l\omega_s\right)\right) \\ +\sin^2\left(\theta\left(k\omega_s\right)\right)\sin^2\left(\theta\left(l\omega_s\right)\right)\end{array}\right] + \sum_{k=1}^{N}\left|\sigma\left(k\omega_s\right)\xi\left(k\omega_s\right)\right|^2 \omega_s^2 \cos^2\left(2\theta\left(k\omega_s\right)\right). \quad (1.23)$$

Se o divisor de feixes não for dependente da frequência e for balanceado $\theta = \pi/4$, a equação (1.23) se reduz a

$$p_{coin} = \frac{1}{2} - \frac{1}{2}\sum_{k=1}^{N}\left|\sigma\left(k\omega_s\right)\xi\left(k\omega_s\right)\right|^2 \omega_s^2 , \quad (1.24)$$

ou, retornando ao caso contínuo,

$$p_{coin} = \frac{1}{2} - \frac{1}{2}\int\int_D \left|\sigma\left(\omega_1\right)\right|^2 \left|\xi\left(\omega_2\right)\right|^2 d\omega_1 d\omega_2 , \quad (1.25)$$

sendo $\left\{D = \left(\omega_1, \omega_2\right) \in R^2_{\geq 0} : \omega_1 = \omega_2\right\}$. Como se pode notar nas equações (1.24) e (1.25), a probabilidade de coincidência será zero somente quando as distribuições espectrais forem iguais $\sigma(\omega) = \xi(\omega) = \delta(\omega\text{-}\omega_0)$, isto é, ambos os fótons com a mesma frequência ω_0 (zero largura espectral). Isso ocorre porque, devido à distribuição espectral, não se pode garantir que ambos os fótons estejam na mesma frequência, mesmo que tenham as mesmas distribuições espectrais. Por outro lado, a probabilidade de coincidência é igual a 1/2 somente quando as distribuições espectrais dos fótons não têm sobreposição. No entanto, na prática, se a informação de frequência não puder ser obtida pelos detectores utilizados na experiência, isto é, se a largura de banda dos detectores for maior que a distribuição espectral dos fótons, os fótons com diferentes frequências tornam-se indistinguíveis e uma interferência de HOM perfeita pode ser conseguida.

3 COMPROMISSO QUÂNTICO DE INFORMAÇÃO USANDO ESTADOS CONTÍNUOS DE DOIS FÓTONS

3.1 Introdução

O protocolo de compromisso de informação (bit) - BC - exerce um papel de extrema importância na implementação de outros protocolos de segurança como o voto eletrônico, esquemas de identificação, entre outros.

Na busca de uma melhor compreensão desse protocolo, façamos o experimento mental em que duas entidades Alice e Bob, mutuamente desconfiadas e localmente distantes querem executar o protocolo, a seguir:

Alice escolhe secretamente o bit *b*. Neste momento, Bob quer ter certeza que Alice fez realmente uma escolha, mas Alice quer manter em segredo o valor de sua escolha até que decida revelá-lo. Para que Bob tenha certeza de que foi escolhido um bit, Alice envia para ele uma prova de sua escolha (um compromisso), e apenas com esta é impossível determinar o valor do bit *b*. Posteriormente, Alice revela *b* e Bob pode, finalmente, usando o compromisso recebido anteriormente, verificar a veracidade do que Alice havia dito (MENDONÇA, 2011).

Pode-se dividir este protocolo em duas fases distintas:

a) A fase de compromisso, em que Alice envia uma evidencia de sua escolha;

b) A fase de revelação, em que a escolha é revelada de fato.

3.2 Protocolos Quânticos de Compromisso de Informação

Afim de se ter um melhor entendimento sobre os protocolos quânticos de compromisso da informação - QBC - é necessária uma breve revisão sobre o protocolo de QBC

baseado no protocolo de distribuição quântica de chaves BB84 e sobre a impossibilidade de segurança incondicional.

3.2.1 O Protocolo de Compromisso de Informação Baseado no Protocolo BB84

No esquema proposto por (MAYERS, 1997) o bit a ser comprometido é codificado na base linear $|0\rangle_+$, $|1\rangle_-$ ou na base diagonal $|0\rangle_\times$, $|1\rangle_\times$, sendo $|0\rangle_\times = \frac{1}{\sqrt{2}}\left(|0\rangle_+ + |1\rangle_+\right)$ e $|1\rangle_\times = \frac{1}{\sqrt{2}}\left(|0\rangle_+ - |1\rangle_+\right)$.

Na fase de compromisso do protocolo, uma sequência de bits aleatórios $w = w_1,w_2,...,w_n$ são gerados e codificados por Alice. Ela codifica cada bit w_i em um fóton segundo o protocolo BB84, usando a base linear $\theta = +$ para comprometer um bit 0 e a base diagonal $\theta = \times$ para se comprometer com o bit 1, em seguida ela envia para Bob a sequência w. Ao receber w Bob escolhe uma sequência de bases aleatórias $\theta^* = \theta_1^*, \theta_2^*, \ldots, \theta_n^* \in \{+,\times\}^n$ mede no registrador o valor de w_i usando a base θ_i^* e armazena o resultado w_i^* da medição.

Na segunda fase (fase de revelação) do protocolo, Alice anuncia a sequência binária w e Bob, por sua vez, pode determinar o bit b comparando as posições w_i e w_i^* em que $w_i \neq w_i^*$. Neste momento, Bob conhece cada uma das posições em que $\theta_i \neq \theta_i^*$, conhece também a base θ_i^* escolhida por ele. Observando as posições θ_i e θ_i^* Bob identifica o resultado como inconclusivo para as situações em que estas revelam valores diferentes para θ. Nesta situação tanto o bit $b = 0$ quanto o bit $b = 1$ correspondem a uma matriz de densidade maximamente mista e com isso Bob não obtém informação nenhuma sobre o valor de b.

Neste estudo os autores deixam clara a consideração de ambos os participantes serem honestos, bem como apontaram que Alice poderia utilizar uma estratégia para trapacear. Nesta estratégia Alice utilizaria um par de estados maximamente entrelaçados, ficaria com uma partícula do par e enviaria a outra para Bob e, por consequência do entrelaçamento, Alice

poderia modificar seus bits depois da fase de compromisso, ou seja ela poderia mudar de escolha sem que Bob percebesse.

3.2.2 A Impossibilidade de Segurança Incondicional

Diversos protocolos quânticos de compromisso de informação como os encontrados em (BRASSARD; CRÉPEAU, 1991; COLLINS, 1992; BRASSARD *et al.*, 1993; LO; ZHAO, 2008) tratam da comunicação em um só sentido, ou seja, de Alice para Bob (MENDONÇA, 2011). Conceitualmente, Alice envia dois sistemas quânticos um na fase de compromisso e outro na fase de revelação. Esquematicamente (LO; CHAU, 1997) e (MAYERS, 1997):

a) Alice escolhe um bit b que será comprometido com Bob. Logo se $b=0$, ela produz o estado

$$\left|0\right\rangle = \sum_i \alpha_i \left|e_i\right\rangle_A \otimes \left|\phi_i\right\rangle_B, \tag{2.1}$$

em que $\langle e_i|e_j\rangle = \delta_{ij}$ e os estados normalizados $|\phi_i\rangle_B$ não são necessariamente ortonormais. Analogamente, no caso de $b=1$ ela produz o estado

$$\left|1\right\rangle = \sum_j \beta_j \left|e'_j\right\rangle_A \otimes \left|\phi'_j\right\rangle_B, \tag{2.2}$$

em que $\left\langle e'_i \middle| e'_j \right\rangle = \delta_{ij}$, e os estados $\left|\phi'_i\right\rangle_B$ não são necessariamente ortonormais. Admite-se que Alice e Bob conheçam os estados $|0\rangle$ e $|1\rangle$ resultando que ambos conhecem os estados $\left|\phi_i\right\rangle_B$ e $\left|\phi'_i\right\rangle_B$.

b) Considerando que Alice seja honesta, Ela faz uma medição no primeiro registrador e determina o valor de i ou j, i se $b=0$, j se $b=1$.

c) Para evidenciar seu compromisso Alice envia o segundo registrador para Bob.

d) Na fase de revelação, os valores de b se i ou j são declarados por Alice. De posse desta informação, Bob faz medições no segundo registrador afim de verificar a veracidade da informação fornecida por Alice.

Deve haver correlação entre as informações cedidas por Alice e os resultados do experimento executado por Bob no registrador. Se realmente existirem as correlações esperadas Bob considera que Alice foi honesta, caso contrário, se não existirem as correlações esperadas, Bob considera que Alice trapaceou.

Para que Bob possa determinar o valor de *b* antes da fase de revelação, seu registrador deve conter informação suficiente sobre qual foi a escolha de Alice. A partir daí é possível se fazer uma análise de segurança a partir de duas hipóteses: uma ideal na qual o registrador não contém nenhuma informação sobre o valor de *b* (BENNETT; BRASSARD, 1984) e (ARDEHALI, 1995); e outra não ideal, na qual existe informação remanescente no registrador (BRASSARD; CRÉPEAU, 1990; BRASSARD *et al.*, 1993).

Para que Bob não tenha informação sobre o bit *b*, numa situação idealizada, as matrizes densidades que descrevem o segundo registrador devem ser iguais para os bits 0 e 1,

$$\mathrm{Tr_A}\left|0\right\rangle\left\langle 0\right| \equiv \rho_0^B = \rho_1^B \equiv Tr_A\left|1\right\rangle\left\langle 1\right|. \qquad (2.3)$$

Observando o Teorema da Decomposição de Schmidt (YANOFSKY, 2007), temos que se $\left|\psi\right\rangle$ é um vetor no espaço do produto tensorial $H_A \otimes H_B$ então existe uma base ortonormal $\left|\psi_i^A\right\rangle$ para H_A e uma base ortonormal $\left|\psi_i^B\right\rangle$ para H_B, além de números reais não negativos p_i, tal que

$$|\psi\rangle = \sum_i \sqrt{p_i}\,|\phi_i^A\rangle|\phi_i^B\rangle, \tag{2.4}$$

na qual $\sqrt{p_i}$ é chamado de coeficiente de Schmidit. A partir daí, pode-se escrever os estados representantes dos bits 0 e 1 como sendo:

$$|0\rangle = \sum_k \sqrt{\lambda_k}\,|\hat{e}_k\rangle_A \otimes |\hat{\phi}_k\rangle_B, \tag{2.5}$$

$$|1\rangle = \sum_k \sqrt{\lambda_k}\,|\hat{e}_k{}'\rangle_A \otimes |\hat{\phi}_k\rangle_B, \tag{2.6}$$

nos quais $\left(|\hat{e}_k\rangle_A, |\hat{e}'_k\rangle_A\right) \in H_A$ e $|\hat{\phi}_k\rangle_B \in H_B$ são bases ortonormais no espaço de Hilbert H_A e H_B. Portanto, é possível observar que para ambos estados os valores de λ_k e $|\hat{\phi}_k\rangle_B$ são iguais e a diferença está apenas no sistema possuído por Alice, $|\hat{e}_k\rangle_A$ ou $|\hat{e}'_k\rangle_A$. Além disso, existe uma transformação unitária U_A que permite o mapeamento de $|\hat{e}_k\rangle_A$ em $|\hat{e}'_k\rangle_A$,

$$U_A|\hat{e}_k\rangle_A = |\hat{e}'_k\rangle_A. \tag{2.7}$$

Assim, é possível observar, então, que $U_A\,|0\rangle = |1\rangle$, sendo aplicada localmente por Alice. Dito isto, Alice pode trapacear Bob não realizando o passo (b), no protocolo anteriormente citado, e no passo (d), decidir sobre o valor de b, mudando de $b=0$ para $b=1$ apenas aplicando U_A em seu sistema sem informar a Bob. Desta forma, segundo (LO; CHAU, 1997) e (MAYERS, 1997), o protocolo de QBC é incondicionalmente inseguro, ou seja, Alice sempre pode trapacear Bob sem correr risco de ser descoberta trapaceando.

3.3 Protocolo de QBC Levando em Considerção a Largura Espectral dos Pulsos Ópticos e a Dependência da Porta Quântica Óptica com a Frequência.

Foi demonstrado (LO; CHAU, 1997) que protocolos de QBC, sem qualquer restrição, não podem ser incondicionalmente seguros. Tentativas de produção de protocolos QBC incondicionalmente seguros com algumas restrições foram propostos (YUEN, 2003; MURTA *et al.*, 2013). Aqui, consideramos o protocolo de LC-QBC do ponto de vista prático, com o objetivo de mostrar que, pelo menos, em princípio, a estratégia de trapaça de Alice pode ser notada por Bob com uma probabilidade maior do que zero. As condições práticas consideradas são:

a) Os fótons entrelaçados têm uma distribuição espectral

b) As portas quânticas ópticas são dependentes da frequência.

O protocolo LC-QBC pode ser explicado simplificadamente da seguinte maneira: Alice e Bob concordam que os estados $|0_L\rangle = (|00\rangle+|11\rangle)2^{1/2}$ e $|1_L\rangle = (|01\rangle+|10\rangle)2^{1/2}$ representam, respectivamente, os bits lógicos ‘0’ e ‘1’. No estágio de compromisso, Alice, desonesta, prepara o estado $|0_L\rangle$ e envia o segundo qubit para Bob. Na fase de revelação, duas situações são possíveis:

a) Alice decide manter a opção ‘0’. Ela mede seu qubit usando a base $\{|0\rangle,|1\rangle\}$ e informa a Bob os valores do bit comprometido (‘0’) e o resultado de sua medição. Bob, por sua vez, mede seu qubit na mesma base e compara o resultado com aquele anunciado por Alice. Se os resultados das medições forem iguais, Bob acredita que Alice atuou honestamente.

b) Alice muda de ideia e decide revelar o valor ‘1’. Ela aplica a porta quântica NOT *X* em seu qubit e o mede. Alice informa a Bob os valores do bit comprometido (‘1’) e o resultado de sua medição. Bob, por sua vez, mede o qubit que ele mantem e compara o resultado com o anunciado por Alice. Se os resultados das medições forem diferentes, Bob acredita que Alice atuou com honestidade. Uma vez que Alice sempre pode mudar de ‘0’ para ‘1’ (aplicando a porta *X* em seu qubit) sem ser notada, ela sempre pode enganar Bob com zero probabilidade de ser descoberta.

Este cenário muda quando consideramos estados entrelaçados reais cujos fótons têm uma largura espectral diferente de zero. Consideremos que Alice e Bob executarão o protocolo LC-QBC usando o seguinte estado entrelaçado

$$\left|0_L\right\rangle = \int_0^\infty d\Omega\sigma(\Omega)\frac{\left|\omega_0+\Omega,\omega_0-\Omega\right\rangle_{HH}+\left|\omega_0+\Omega,\omega_0-\Omega\right\rangle_{VV}}{\sqrt{2}}. \tag{2.8}$$

A discretização do estado (2.8) usando (1.3)-(1.6) é

$$\left|0_L\right\rangle = \sum_{\substack{k,l=1\\k+l=M}}^{N}\sigma(k\omega_s,l\omega_s)\sqrt{\omega_s}\left[\frac{\left|\tilde{1}\right\rangle_k^H\left|\tilde{1}\right\rangle_l^H+\left|\tilde{1}\right\rangle_k^V\left|\tilde{1}\right\rangle_l^V}{\sqrt{2}}\right]. \tag{2.9}$$

$$M\omega_s = 2\omega_0. \tag{2.10}$$

De acordo com (2.9), com probabilidade $\left|\sigma(k\omega_s,l\omega_s)\right|^2\omega_s$ os fótons nas frequências $k\omega_s$ e $l\omega_s$ ($k\omega_s + l\omega_s = M\omega_s = 2\omega_0$) estão no estado entrelaçado $(|HH\rangle+|VV\rangle)/2^{1/2}$. A porta *X*, por sua vez, é um rotacionador de polarização dependente da frequência. É representado por $R[\theta(\omega)]$, sendo que $\theta(\omega_c) = \pi/2$ na frequência central ω_c. Quando Alice tenta trapaçear usando $R[\theta(\omega)]$, ela produz o estado quântico

$$R\left[\theta(\omega)\right]\left|0_L\right\rangle = \sum_{\substack{k,l=1\\k+l=M}}^{N}\sigma(k\omega_s,l\omega_s)\sqrt{\omega_s}\times\left[\begin{array}{l}\cos\left[\theta(k\omega_s)\right]\dfrac{\left(\left|\tilde{1}\right\rangle_k^H\left|\tilde{1}\right\rangle_l^H-\left|\tilde{1}\right\rangle_k^V\left|\tilde{1}\right\rangle_l^V\right)}{\sqrt{2}}\\+\sin\left[\theta(k\omega_s)\right]\dfrac{\left(\left|\tilde{1}\right\rangle_k^V\left|\tilde{1}\right\rangle_l^H+\left|\tilde{1}\right\rangle_k^H\left|\tilde{1}\right\rangle_l^V\right)}{\sqrt{2}}\end{array}\right]. \tag{2.11}$$

Um erro em Bob que denunciará a estratégia de trapaça de Alice, ocorrerá quando ela informar que escolheu o bit ‘1’ e Bob adquirir como resultado de sua medição o mesmo

resultado da medição de Alice. Usando o estado em (2.11) obtém-se a seguinte probabilidade de erro

$$PE = \sum_{\substack{k,l=1 \\ k+l=M}}^{N} \left|\sigma\left(k\omega_s, l\omega_s\right)\right|^2 \cos^2\left[\theta\left(k\omega_s\right)\right]\omega_s , \tag{2.12}$$

ou, retornando ao caso contínuo,

$$PE = \int_0^{\infty} d\Omega \left|\sigma\left(\Omega\right)\right|^2 \cos^2\left[\theta\left(\omega_0 + \Omega\right)\right]. \tag{2.13}$$

Em (2.13) assume-se que Alice e Bob mantiveram, respectivamente, os fótons com frequência central (ω_0+Ω) e (ω_0-Ω). Assim, uma vez que se leva em conta a distribuição espectral e a dependência da frequência de dispositivos ópticos, pode-se notar que a estratégia de Alice pode causar um erro em Bob, revelando sua trapaça.

4 DISTRUBUIÇÃO QUANTUM-CAÓTICA DE CHAVES COM PULSOS MULTIFÓTONS

4.1 Introdução

Recentemente foi apresentado na literatura um novo esquema de distribuição quântica de chaves chamado distribuição quantum-caótica de chaves (QCKD) (OLIVEIRA, DE; RAMOS, 2018). Não é objeto da presente tese a descrição detalhada do sistema de QCKD. Aqui, apresentamos uma propriedade interessante não verificada na citada referência. Basicamente, por usar estados coerentes com valores de fase que podem assumir qualquer valor no intervalo $[0,2\pi]$, um sistema de QCKD pode usar estados coerentes com número médio de fótons maior que 0,1, que é o valor tradicionalmente usado em sistemas de QKD.

Alguns sistemas de QKD seguem o modelo BB84, ou seja, Alice e Bob escolhem as bases aleatoriamente para geração e medição dos qubits. Posteriormente, em uma etapa chamada reconciliação de bases, eles divulgam publicamente as bases utilizadas e, apenas os bits obtidos quando Alice e Bob escolhem a mesma base são mantidos para formar a chave. Os demais bits são descartados. Para estes protocolos quanto maior o número de bases utilizadas mais seguro é o protocolo. Entretanto, uma vez que apenas os bits obtidos nos instantes em que eles escolheram as mesmas bases são mantidos, a taxa de transmissão de bits da chave decresce com o aumento do número de bases (BOURENNANE *et al.*, 2001).

O problema de aumentar a segurança aumentando o número de estados quânticos utilizados sem diminuir a taxa de transmissão de bits da chave pode ser contornado usando a QCKD. Para estes protocolos, embora a informação enviada seja discreta (bits ‘0’ e ‘1’), o conjunto de estados quânticos que trafegam no canal óptico é contínuo, o que leva ao aumento da segurança. Adicionalmente, como a QCKD não possui estágio de reconciliação de bases, a taxa de transmissão não diminui.

Uma vez que o número de estados quânticos utilizados aumenta e não há reconciliação de bases, é possível para Alice aumentar o número de fótons por pulso enviado para Bob sem que a segurança seja comprometida. Para isso, é necessário que o número de

fótons por pulso não ultrapasse o valor mínimo requerido para que uma espiã, chamada Eva, obtenha informação útil.

Se um protocolo QKD usa pulsos multifótons, a espiã, Eva, pode usar duas estratégias: Se ela tiver uma memória quântica, ela separa um fóton do pulso multifótons enviado por Alice e o mantém em sua memória. Após o estágio de reconciliação das bases, Eva pode medir o fóton na base correta, obtendo as informações corretas. Se Eva não tiver uma memória quântica, ela pode tentar obter o número máximo de fótons do pulso multifotônico (sem perturbar as estatísticas de detecção de Bob) e faz medições nesses fótons. Dos dados medidos, Eva infere o estado quântico enviado por Alice. Para o QCKD, ter uma memória quântica não é útil, já que não há estágio de reconciliação. Por isso, Eva precisa obter fótons e medi-los. Assim, a questão importante é: Qual o número máximo de fótons que Eva pode capturar para que, ainda assim, não seja possível que ela obtenha informações úteis da chave? Para responder a esta questão, utilizamos simulações numéricas de um protocolo QCKD usando o mapa logístico e sua implementação com o interferômetro Mach-Zehnder.

4.2 QCKD Multifóton com mapa logístico

O QCKD usando mapas logísticos sincronizados foi discutido em Damasceno *et al.*, 2018 . Sua dinâmica não linear é governada pelo conjunto de equações

$$z_{k+1} = \delta z_k \left(1 - z_k\right), \tag{3.1}$$

$$x_{n+1} = \lambda x_n \left(1 - x_n\right) + c\left[k - \lambda\left(1 - x_n - d\overline{z}_{k+1}\right)\right]\left(x_n - d\overline{z}_{k+1}\right), \tag{3.2}$$

$$y_{n+1} = \lambda y_n \left(1 - y_n\right) + c\left[k - \lambda\left(1 - y_n - d\overline{z}_{k+1}\right)\right]\left(y_n - d\overline{z}_{k+1}\right), \tag{3.3}$$

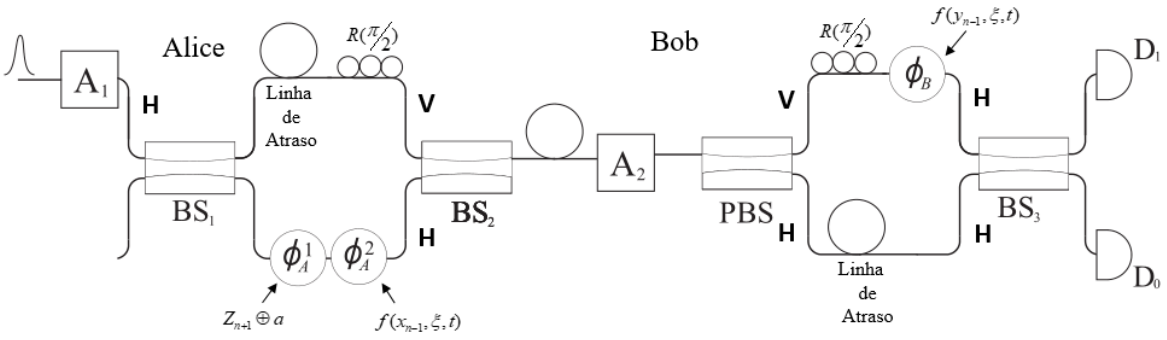
$$\overline{z}_{k+1} = 0 \text{ se } z_{k+1} < 0.5 \text{ e } 1 \text{ se } z_{k+1} \geq 0.5. \tag{3.4}$$

Como se pode notar em (3.1)-(3.4), o sistema Z aciona os sistemas X e Y com uma variável discreta, $\overline{z_n}$, que assume apenas dois valores, 0 e 1. A variável *d* em (3.2)-(3.3) ajusta o valor de $\overline{z_n}$. Uma vez que os sistemas caóticos X e Y são sincronizados, uma chave comum

pode ser estabelecida a partir de uma discretização das variáveis de saída. x_n (para Alice) e y_n (para Bob). Por exemplo, um valor de referência V_{ref} é escolhido. Se $x_n \geq V_{ref}$ ($y_n \geq V_{ref}$) um bit '1' armezanado por Alice (Bob), de outra forma um bit '0' é armazenado. Se $x_n = y_n$ os bits da chave de Alice e Bob serão os mesmos. Note que, desde que x_n e y_n assumam valores contínuos entre 0 and 1, uma codificação m-ária também é possível, implicando em uma taxa de transmissão mais alta. No entanto, não é nosso objetivo discutir essa questão aqui.

Para implementar um Sistema QCKD usando o mapa logístico e pulsos multifotônicos, a configuração óptica para QKD usando o interferômetro de Mach-Zehnder (IMZ) pode ser usada, como mostrado na Figura 2.

Figura 2 - Configuração óptica para distribuição de chaves quantum-caóticas usando pulsos multifótons com interferômetro Mach-Zehnder. A_1 e A_2 são atenuadores ópticos, D_1 e D_0 são detectores de fótons únicos, PBS é um divisor de feixe dependente da polarização e *H* e *V* representam os modos horizontal e vertical, respectivamente.



Fonte: Elaborada pelo autor.

O funcionamento do IMZ mostrado na Figura 2 tem sido amplamente discutido na literatura (GISIN *et al.*, 2002; LO; ZHAO, 2012) e não é nosso objetivo repeti-lo aqui. Os pontos principais relativos ao esquema na Figura 12 são:

a) O pulso de Alice no braço inferior do IMZ é modulado por fase ϕ_A^1 e ϕ_A^2, de acordo com os valores de $\overline{z_{k+1}} \oplus a$ e $f(x_{n-1},\xi,t)$: $\phi_A^1 = \pi(\overline{z_{n+1}} \oplus a)$ e $\phi_A^2 = \pi f(x_{n-1},\xi,t)$. Aqui, a função f é o mapa logístico $f_{n+1} = \xi f_m(1-f_m)$. O valor de entrada f_0 é x_{n-1} o valor de saída é f_t. Os parametros ξ e t são conhecidos apenas por Alice e Bob. Finalmente, a é a paridade do último dígito de f_t.

b) No lado de Bob, o pulso no braço superior do IMZ sofre uma mudança de fase dada por $\phi_B = f(y_{n-1},\xi,t)\pi$. Para Bob o valor de entrada é f_0 e y_{n-1} o valor de saída é f_t.

c) Por causa do código de polarização, ambos os pulsos chegam ao BS_3 ao mesmo tempo, com a mesma polarização e sofrem interferência. Dependendo da diferença de fases aplicada por Alice e por Bob, a luz será guiada para o detector de fótons únicos (SPD) D_0 ou D_1.

As probabilidades de detecção em D_0 e D_1 são dadas por

$$p_0 = \left(1-\exp\left(-\left|\alpha_B\right|^2 p_d\right)\right)\cos^2\left[\pi\left(\bar{z}_{k+1}\oplus a + f\left(x_{n-1},\xi,t\right) - f\left(y_{n-1},\xi,t\right)\right)/2\right], \quad (3.5)$$

$$p_1 = \left(1-\exp\left(-\left|\alpha_B\right|^2 p_d\right)\right)\sin^2\left[\pi\left(\bar{z}_{k+1}\oplus a + f\left(x_{n-1},\xi,t\right) - f\left(y_{n-1},\xi,t\right)\right)/2\right]. \quad (3.6)$$

Em (3.5)-(3.6), $|\alpha_B|^2$ é o número médio de fótons após o atenuador A_2 e p_d é a probabilidade de detecção de D_0 e D_1, desprezando o ruído. Para Bob, detecção em D_0 implica $\overline{z_{k+1}}\oplus a = 0$ enquanto a detecção em D_1 implica $\overline{z_{k+1}}\oplus a = 1$. Como pode ser visto em (3.5)-(3.6), as probabilidades de detecção dependem do sincronismo e o sincronismo depende das probabilidades de detecção.

A falta de sinais de sincronização causará a dessincronização dos mapas logísticos, resultando em uma alta taxa de erro. Para evitar isso, Alice e Bob devem atualizar os valores de x_n e y_n somente quando Bob tiver detecção. Isto implica que, quando Bob não tem detecção, ele informa a Alice e ela irá atualizar z_{k+1} e calcular um novo valor para f usando t+1, ao invés de t. Assim, todo pulso enviado por Alice terá um valor de fase diferente mesmo quando x_n não é atualizado. Bob vai fazer o mesmo até ter detecção.

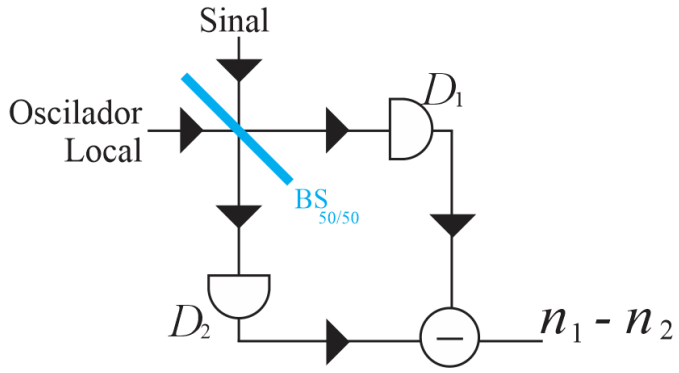
Agora, a questão importante é, se Alice envia um estado coerente para Bob com um número médio de fótons $|\alpha|^2$, qual é o máximo valor seguro para $|\alpha|^2$ se $[z_{k+1}\oplus a + f(x_{n-1},\xi,t)]\pi$ é uma fase contínua que varia no intervalo $[0,2\pi]$? Uma vez que Eva não sabe que base de medição usar, ela pode realizar uma tomografia homódina do estado que sai de Alice (RAFFAELLI *et al.*, 2018). Se a fidelidade da matriz de densidade reconstruída, F, é menor que 1, haverá um erro na fase estimada.

As simulações numéricas mostram que um erro de 0,05 rad no valor da fase do estado coerente enviado por Alice provoca um erro de cerca de 13% nos bits da chave,

indicando a presença de Eva. A fidelidade entre dois estados coerentes com o mesmo número médio de fótons (consideramos que Eva conhece o número médio de fótons usado por Alice), $\langle n \rangle$, é dada por $F = e^{\{-2\langle n \rangle [1-\cos(\Delta)]\}}$, onde Δ é a diferença entre os ângulos dos dois estados coerentes considerados. Usando $\Delta = 0{,}05$ rad, a fidelidade é $F \approx 0{,}95$ quando $\langle n \rangle = 20$. Portanto, daqui em diante, consideramos $F = 0{,}95$ como o valor máximo para a fidelidade permitida para Eva.

A nova questão é: quantos estados coerentes com número médio de fótons $|\beta|^2$ são necessários para estimar o valor da fase com um erro de 0,05 rad? Vamos supor que Eva usa o esquema homódino mostrado em Figura 3 .

Figura 3 - Esquema Homódino usando divisor de feixe balanceado e contadores de fótons (D_1 e D_2).



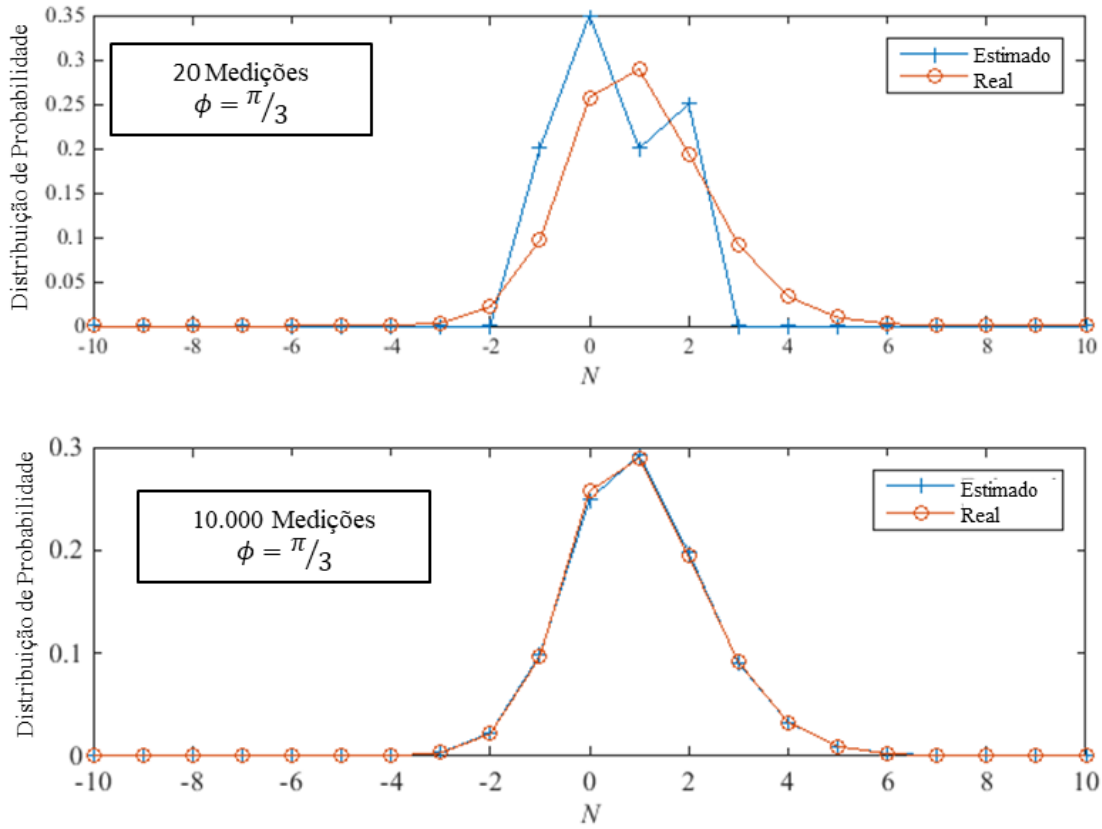
Fonte: O autor

Na Figura 3, D_1 e D_2 são contadores de fótons. Eva divide o estado coerente enviado por Alice em r cópias com número médio de fótons $|\beta|^2$, $r = |\alpha|^2/|\beta|^2$, portanto, o estado no modo sinal é $||\beta|e^{i\phi}\rangle$ onde ϕ é a fase total escolhida por Alice. O oscilador local usado por Eva é o estado coerente $||\beta|\rangle$ (com fase igual a 0 rad). A distribuição de probabilidade da diferença do número de fótons medidos por D_1 (n_1) e D_2 (n_2), $N = n_1 - n_2$, é dada pela distribuição de Skellam

$$P_N = e^{-2|\beta|^2} \left|\tan(\phi)\right|^N I_{|N|}\left(2|\beta|^2 \left|\sin(2\phi)\right|\right). \qquad (3.7)$$

Em (3.7), $I_{|N|}$ é a função de Bessel modificada do primeiro tipo. Assim, se Eva mede a variável N um número r de vezes, ela pode obter uma estimativa para P_N e, usando esta estimativa e a equação (3.7), ela obtém uma estimativa para ϕ. Como se pode notar, Eva não pode usar $|\beta|^2$ muito próximo de zero pois neste caso o ângulo ϕ perde sua importância (para $\beta = 0$, $P_0 = 1$ para qualquer valor de ϕ). Uma boa estimativa de P_N requer um valor grande para r. Sendo bem conservador, assume-se que Eva usa $|\beta|^2 = 1$. Dado que Alice usa $|\alpha|^2 = 20$, Eva terá somente $r = 20$ copias para obter sua estimativa da distribuição P_N. Na Figura 4 tem-se a distribuição real de P_N da equação (3.7) e uma estimativa da distribuição de N para $r = 20$ (superior) e $r = 10.000$ (inferior), para $|\beta| = 1$ e $\phi = \pi/3$.

Figura 4 – Distribuições real e estimada, nas simulações numéricas, para P_N usando $|\beta| = 1$ e $\phi = \pi/3$.



Como se pode ver na Figura 4, 20 medições não fornecerão dados suficientes para uma boa estimativa de P_N. Assim, daqui em diante, assumimos que Alice usará $|\alpha|^2 = 20$. Os valores de ϕ estimados usando $min_{\phi}\Sigma_n\left(P_N(\phi) - \widehat{P_N}\right)^2$ com as distribuições estimadas mostradas na Figura 4 acima são ϕ_{est} = 0.845801322478620 para 20 medições e ϕ_{est} = 1.04059954682362 para 10 mil medições ($\pi/3$ = 1.04719755119660).

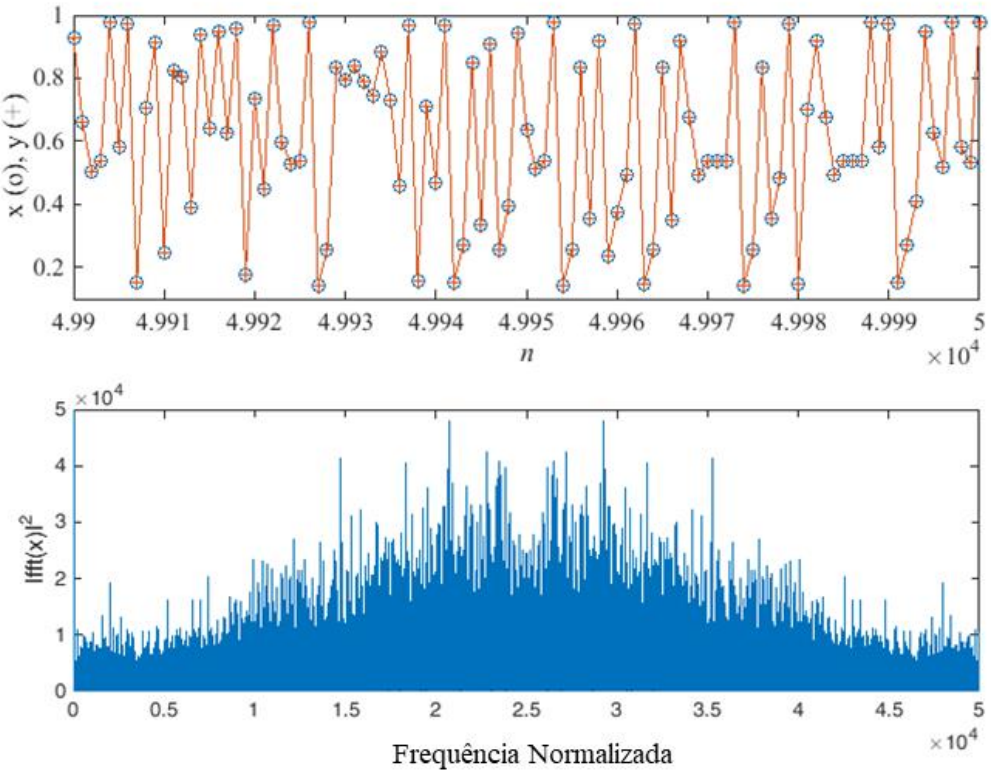
Por outro lado, para garantir que Bob terá detecção de fótons únicos, deve-se ter

$$\left|\alpha_B\right|^2 = \left|\alpha\right|^2 10^{\frac{-(\sigma L + A_2)}{10}} = 0.1, \qquad (3.8)$$

na qual σ = 0,27 dB/km é o coeficiente de perdas da fibra óptica e L é o comprimento do enlace óptico entre Alice e Bob. O comprimento máximo do enlace é obtido quando A_2 = 0. Neste caso, tem-se L_{max} = 85 km.

A Figura 5 mostra uma simulação da sincronização entre os sistemas não lineares de Alice e Bob para os seguintes valores de parâmetros: p_d = 0,15, L = 85 km, $|\alpha|^2$ = 20, σ = 0,27 dB/km, δ = 4, λ = 3,9, k = 0,2, c = 0,5, d = 0,5. Os valores iniciais das variáveis dinâmicas são $x(1)$ = 0,7, $y(1)$ = 0,7, $z(1)$ = 0,2. Para o mapa logístico f usou-se ξ = 3,97 e t = 1000.

Figura 5 - Sincronização dos sistemas caóticos X (o) e Y (+). Somente os últimos 100 valores de uma simulação de 50.000 são mostrados. A parte de baixo é a transformada rápida de Fourier da saída x_n.



Na Figura 5 o gráfico superior mostra a sincronização entre as chaves geradas pelos mapas logísticos de Alice (cruz vermelha) e Bob (circulo azul).

O gráfico da parte inferior por sua vez mostra a transformada de fourier da série de dados formada pelo mapa logístico de Alice (Bob). O fato de os picos nos valores de frequência não estarem isolados, ou seja, o fato de exisistir continuidade no espectro de frequência revela o carater caotico da série.

5 DETECÇÃO ÓPTICA

5.1 Introdução

Os sistemas de transmissão por fibras ópticas em geral empregam a modulação direta da intensidade do sinal óptico, normalmente gerado por lasers semicondutores, e a detecção direta através de fotodiodos PIN ou avalanche.

O fotodiodo PIN do inglês *Positive-Intrinsic-Negative* é um fotodetector no qual a espessura da camada de depleção pode ser modificada para geração de grande fotocorrente. Se a espessura da camada de depleção for maior, a área da superfície na qual a luz está sendo detectada também aumenta. Portanto, a eficiência de conversão de um fotodiodo aumenta e, consequentemente, a fotocorrente que ele irá gerar (ROCHA; CARNEIRO, 1989)

O fotodiodo Avalanche é um fotodetector no qual são gerados mais pares de elétron-buraco devido à ionização por impacto. É semelhante ao fotodiodo PIN onde pares elétron-buraco são gerados devido à absorção de fótons, mas além disto o fotodiodo de avalanche usa o princípio de ionização por impacto para aumentar a magnitude da fotocorrente, devido ao campo eletrico a que é submetido (SALEH; TEICH, 1991).

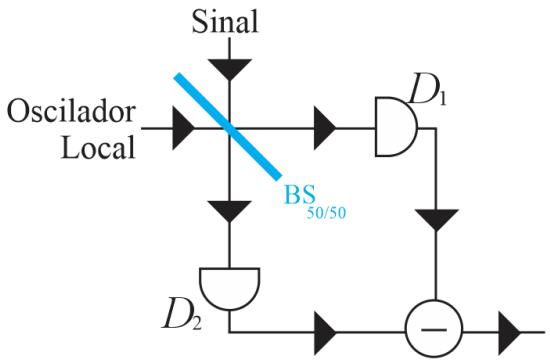
A variação da potência da luz se transforma em variação de corrente que flui pelo fotodiodo. Entretanto, a partir de 1980, verificou-se um esforço crescente na pesquisa de sistemas de comunicação óptica que carregam a informação na fase. Estes sistemas são chamados de sistemas coerentes.

Na detecção coerente utiliza-se uma técnica caracterizada pelo uso de um outro feixe de luz, usado como referência, chamado de oscilador local. Quando o oscilador local possui a mesma frequência do sinal a ser medido, o método de detecção é denominado detecção homódina. Caso contrário, o procedimento é denominado detecção heteródina (LEONHARDT *et al.*, 1996).

5.2 Detecção Heteródina

O diagrama esquemático mostrado na Figura 6 representa a detecção heteródina. O sinal óptico recebido e o sinal laser local são combinados em um divisor de feixe $BS_{50/50}$ (*Beam Splitter* que transmite 50% do sinal e reflete 50% do mesmo). As saídas do BS estão conectadas a entrada de dois fotodetectores distintos (D_1 e D_2).

Figura 6 – Diagrama da detecção Heteródina (Homódina). Combinação do Sinal e do sinal do Oscilador Local.



Fonte: Elaborada pelo autor.

A fotocorrente é dada por (4.1):

$$i_{ph} = R_0 P_i = R_e \left\langle e_i^2 \right\rangle, \tag{4.1}$$

em que P_i é a potência óptica total de entrada e a constante R_e inclui a responsividade e as constantes necessárias para converter de watts para $(V/m)^2$.

A responsividade do fotodiodo é denominada R_0 e é obtida a partir das propriedades intrínsecas do fotodiodo e varia com o comprimento de onda. Sua unidade é Amperes por Watt *(A/W)* e é dada pela equação (4.2);

$$R_0 = \frac{q\eta}{hf} \ , \tag{4.2}$$

onde η é a eficiência quântica, h é a constante de Planck, f é a frequência do sinal óptico, q é a carga do elétron.

Contribuições à análise de segurança de protocolos de criptografia quântica

Sabendo que a soma de duas ondas eletromagnéticas deve ser representada em termos da soma das amplitudes de intensidades de seus campos. Assumindo, ainda, que os dois campos na entrada do $BS_{50/50}$ têm a mesma polarização, o campo elétrico na entrada é a soma do campo elétrico da portadora modulada, e_1, com o campo elétrico do laser local, e_0; Neste caso, a fotocorrente é dada por:

$$i_{ph} = R_e \left\langle e_i^2 \right\rangle = R_e \left\langle \left(e_1 + e_0\right)^2 \right\rangle = R_e \left\langle \left(e_1^2 + 2e_1e_0 + e_0^2\right) \right\rangle, \tag{4.3}$$

em que

$$e_1 = E_1 \left[1 + mf\left(t\right)\right] \cos\left(\omega_1 t\right) \tag{4.4}$$

e

$$e_0 = E_0 \cos\left(\omega_0 t\right) \tag{4.5}$$

Observa-se que e_1 tem sua amplitude modulada. Efetuando a substituição das equações (4.4) e (4.5) na equação (4.3) obtem-se uma equação que determina a fotocorrente no fotodiodo, a partir da expansão do produto dos termos do cosseno e desprezando os termos de alta frequência,

$$i_{ph} = R_e \left\{ \frac{1}{2} E_1^2 \left[1 + mf(t) \right]^2 + \frac{1}{2} E_1^2 + E_0 E_1 \left[1 + mf(t) \right] \cos(\omega_1 - \omega_0) t \right\}. \quad (4.6)$$

É esperado, na detecção heteródina que $E_0 >> E_1$, então:

$$i_{ph} = R_e \left\{ \frac{1}{2} E_0^2 + E_0 E_1 \left[1 + mf(t) \right] \cos(\omega_1 - \omega_0) t \right\}. \quad (4.7)$$

A corrente é formada a partir da soma de um termo de corrente contínua *dc* com um termo de frequência intermediária (ω_1 - ω_0). Este último, por sua vez, é passível de amplificação, bem como de recuperação em uma demodulação; o envelope $f(t)$ detectado produz uma voltagem na saída que pode ser escrita na forma:

$$v = AR_e E_0 E_1 mf(t). \quad (4.8)$$

A constante A depende do circuito eletrônico de detecção. Em termos de potência óptica, tem-se:

$$i \sim R_0 \left[P_0 P_1 \right]^{\frac{1}{2}} mf(t). \quad (4.9)$$

A proporcionalidade entre a amplitude do sinal no receptor e a raiz quadrada da potência dos campos ópticos de sinal e oscilador local é indicada pela equação (4.9). Por isso, o campo do oscilador local deve ser forte quando o campo do sinal é fraco.

5.3 Detecção Homódina

Em medições homódinas as ondas são derivadas da mesma fonte laser. Esta técnica de medição apresenta sensibilidade à fase no sentido de que a potência do sinal heteródino é dependente da fase relativa do sinal, bem como do oscilador local.

Uma adaptação de grande utilidade é a detecção homódina balanceada, técnica que consiste na colocação de dois fotodiodos após um $BS_{50/50}$, pois, com a utilização desta técnica, a soma e a diferença das fotocorrentes são obtidas eletronicamente (JONES, 1988).

A detecção homódina é um caso particular da detecção heteródina em que a frequência do oscilador local é igual a frequência óptica da portadora resultando numa frequência intermediária é igual a zero (YEH, 1990).

Para a realização de detecção homódina utiliza-se um laser intenso como oscilador local. O sinal a ser medido é combinado com o oscilador local. Utilizando um controlador de polarização garante-se que detector meça a interferência entre estes dois feixes tornando-o sensível à diferença de fase entre eles. Já o BS é escolhido de modo que o oscilador local tenha uma potência maior que o sinal (ORTEGA, 2015).

Como, na detecção homódina, a frequência do oscilador local é a mesma frequência do sinal. Para este tipo de detecção, ambas as ondas são virtualmente derivadas da mesma fonte laser. Esta técnica é sensível à fase pois a potência do sinal heteródino depende da fase relativa do sinal e do oscilador local e pode até desaparecer totalmente. Sendo assim uma adaptação útil é a detecção homódina balanceada, nesta dois fotodiodos são posicionados após um $BS_{50/50}$, e a soma e diferença das fotocorrentes são obtidas eletronicamente (YEH, 1990).

Em aplicações não-clássicas, a detecção homódina balanceada revelou-se apropriada para a medição direta de quadraturas de campos elétricos de modos eletromagnéticos. Proposta inicialmente por Yuen e Chan (1983) a detecção homódina balanceada utilizada para detectar estados comprimidos do campo eletromagnético e em seguida para estudos como a caracterização completa de estados quânticos via tomografia quântica (HANSEN *et al.*, 2001).

Segundo Yuen e Chan (1983) o ruído quântico nas detecções heteródina e homódina é normalmente analisado pressupondo a saída do fotodetector poissoniana, condicionada pelo sinal de entrada. Supõe-se que este ruído quântico surge a partir do ruído do oscilador local. Contudo, em uma análise completamente quântica, observa-se que ela realmente surge a partir da flutuação quântica do sinal. Diante disto, é possivél utilizar detecção homódina para sondar a pequena flutuação de uma única quadratura em estados coerentes de dois fótons, também chamados de estados comprimidos. Leonhardt e Paul (1994) propuseram

um esquema experimental, no qual, é possivél evitar a deterioração das medições de detecção homódinas ocasionadas por detectores não ideais.

Afim de se determinar o conteúdo espectral dos estados quânticos de luz, as técnicas homódinas representam a classe mais importante de medidas quânticas disponíveis, quando se trata do regime de variáveis contínuas (YUEN; SHAPIRO, 1980; SHAPIRO, 1985). Através da detecção homódina espectral são realizadas, geralmente, as detecções de modos espectrais.

Nestes casos, um campo de laser espectralmente estreito constitui o oscilador local, e a fotocorrente detectada passa por uma análise de Fourier, onde, a partir do seu espectro de potência é obtida toda a informação acessível sobre o estado quântico. Esta técnica tem sido largamente empregada em observações de compressão de ruído quântico, bem como, reconstrução de espaço de fase de um estado quântico comprimido e emaranhamento do tipo EPR (Einstein-Podolsky-Rosen) em modos espectrais (BREITENBACH *et al.*, 1997).

Apesar do exposto, a detecção homódina não produz uma medição completa do estado quântico da luz que comtemple os dois modos de banda lateral que contribuem para o ruído quântico. Uma técnica de medição alternativa foi proposta por Barbosa *et al.*, (2013) chamada de detecção de ressonância e consiste numa técnica auto-homódina que emprega, antes da medição de intensidade, uma cavidade óptica para manipular os modos espectrais.

Hirano *et al.*, (2003) propõem o uso da detecção homódina balanceada no cumprimento do protocolo BB84 utilizando codificação de fase. A detecção balanceada é uma técnica em que a radiação é dividida por um elemento óptico em dois feixes de potências ópticas iguais, estes, por sua vez, são detectados por dois fotodiodos distintos. Porém na detecção homódina tem-se a vantagem de poder realizar o processo com apenas um fotodetector.

A detecção homódina não é apenas uma ferramenta ideal para medir as estatísticas de fótons, ela também pode ser aplicada na reconstrução da matriz de densidade completa, ou seja do estado quântico, de um modo de luz. Na matriz de densidade encontra-se a máxima informação possível permitida pelos próprios princípios da mecânica quântica (LEONHARDT *et al.*, 1996).

5.4 Construção do Interferômetro de Mach–Zehnder

Nesta seção os resultados experimentais obtidos, a partir da construção de um interferômetro de Mach-Zehnder com a utilização de fibra óptica, são apresentados e discutidos.

Os equipamentos utilizados na construção do Interferômetro em questão estão elencados a seguir:

a) Um laser da **THORLABS** (*Multi Channel Fiber Coupled Laser Source*),

b) Um gerador de sinais da **AGILENT** (N9310A RF *Signal Generator* 9 KHz – 3 GHz),

c) Um osciloscópio da **ROHDE & SCHWARZ** (RTM 1052 *Oscilloscope* – 500 MHz – 5 GSa/s),

d) Um analisador de espectro da **ROHDE & SCHWARZ** (FSV *Signal Analyzer* – 10 Hz a 3,6 GHz),

e) Dois moduladores de fase da **JDS *Uniphase***,

f) DoisTrês divisores de feixes (*Beam Spliter* – BS) 50/50,

g) Um circulador,

h) Uma fibra com atenuação de 20 dB,

i) Um conector com atenuação de 15 dB ,

j) Um atenuador variável digital (*Digital Variable Attenuator* – VOA) de até 60 dB da **OZ** *OPTICS*,

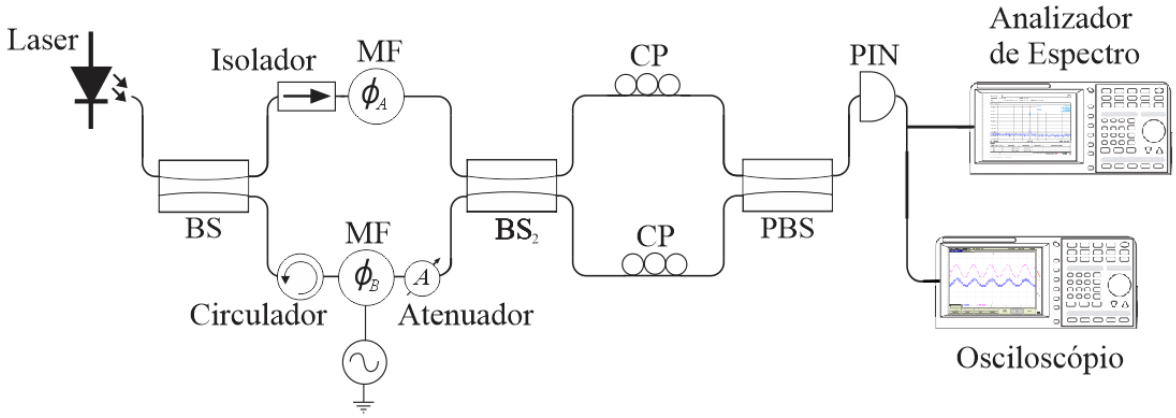
k) Dois controladores de polarização (CP),

l) Um divisor de feixe por polarização (*Polarization Beam Splitter* – PBS) e

m) Um fotodetector PIN.

Na primeira etapa do experimento uma configuração simplificada do interferômetro foi executada, nesta foram utilizados apenas o laser, dois BS, dois moduladores de fase e o sinal modulante alimentando apenas o modulador de fase B, conforme ilustrado na Figura 7.

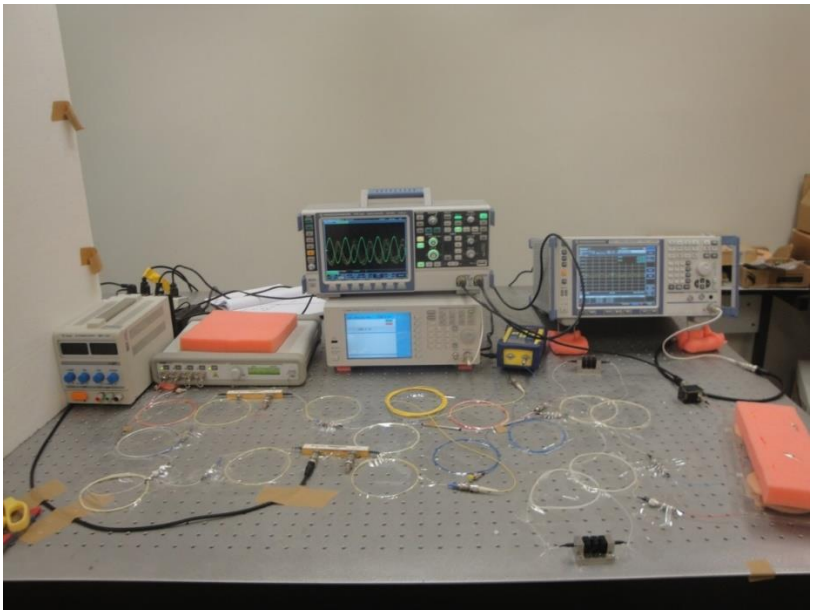
Figura 7 - Diagrama esquemático do Interferômetro de Mach – Zehnder - experimento executado em laboratório.



Fonte: Elaborada pelo autor.

A configuração física do experimento em funcionamento no local em que foi realizado - mesa óptica do Laboratório de Informação Quântica (LATIQ) - pode ser observada na Figura 8. Nesta é possivél observar a detecção do sinal na forma de uma senóide no osciloscópio, senóide esta resultante da interferência entre o sinal modulante e o sinal do oscilador local.

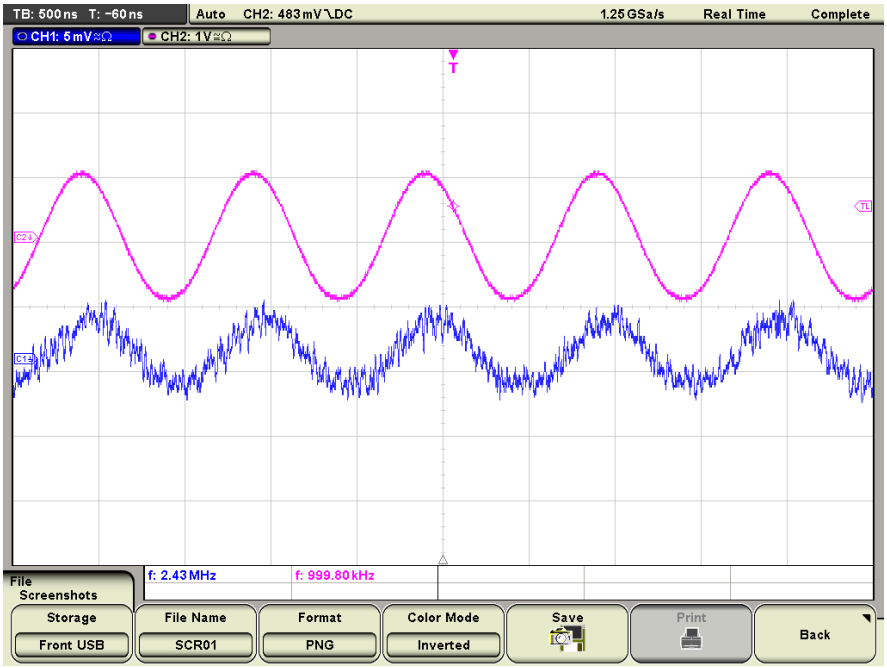
Figura 8 - Circuito físico montado no laboratório - Interferômetro de *Mach – Zehnder*.



Fonte: Elaborada pelo autor.

Na Figura 9 a tela (*printscreen*) do analisador de espectro é mostrada. É possível observar nesta a detecção do sinal após a interferência. A frequência emitida pelo gerador de sinais é de 1 MHz, a mesma encontrda na senóide. É possível localizar este valor na figura observando o valor de f = 999,80 kHz (na cor rosa) na parte inferior da tela.

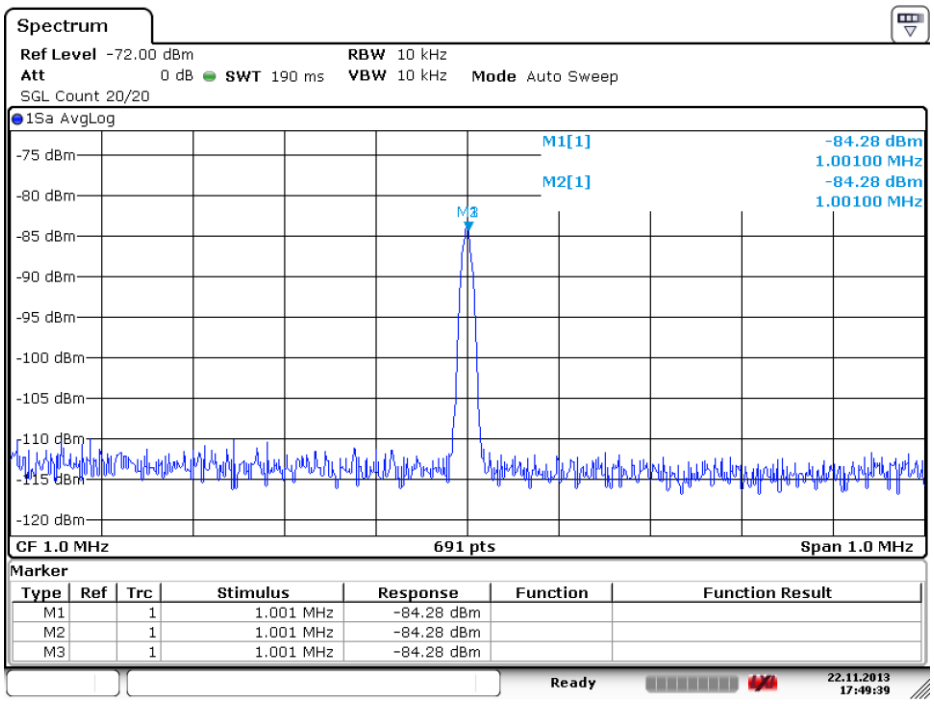
Figura 9 - Sinal senoidal resultante do experimento visto no Osciloscópio.



Fonte: Elaborada pelo autor.

Ao observar o resultado mostrado na tela do analisador de espectro (Figura 10), mais uma vez é possível distinguir o sinal emitido pelo gerador, depois de ocorrida a interferência. Nesta tela é possível localizar este valor observando a frequência dos tres marcadores sobrepostos (M1 = 1000,1 MHz, M2 = 1000,1 MHz e M3 = 1000,1 MHz) localizados no pico do sinal e com seus respectivos valores especificados na tabela na parte inferior da própria tela.

Figura 10 - Sinal visto no Analisador de Espectro com atenuação de 35 dB.



Fonte: Elaborada pelo autor.

5.5 EXPERIMENTO DE DETECÇÃO DE ESTADOS COERENTES FORTEMENTE ATENUADOS COM MEDIÇÃO HOMÓDINA

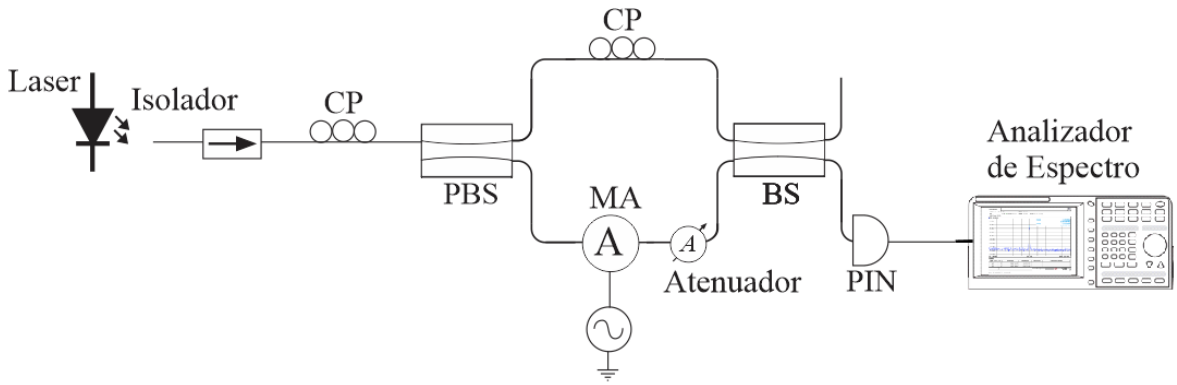
O experimento de detecção de estados coerentes fortemente atenuados utilizando a técnica de detecção homódina é, de fato, um experimento no qual se mede a interferência. Neste, como veremos a seguir, o sinal óptico portador da informação é atenuado fortemente antes de chegar ao divisor de feixe em que ocorre a interferência.

É possível observar o esquema ópitico, representante do experimento no diagramana da Figura 11, bem como a fotografia real do experimento (Figura 12). O controlador de polarização (CP) e o divisor de feixes por polarização (PBS) na entrada do detector (PIN), trabalhando em conjunto, funcionam como um divisor de feixes com reflexividade ajustável, ou seja é possível, através de ajustes, administrar a intensidade do sinal óptico em cada saida do divisor de feixe.

Durante o experimento, ajustou-se o diodo laser de maneira que este operasse bem acima da corrente de limiar. O gerador de sinal, por sua vez, foi configurado para que o sinal modulante apresentasse amplitude de 2,238,8 mV e as frequências de 1,0; 1,2; 1,3 e 1,5 GHz.

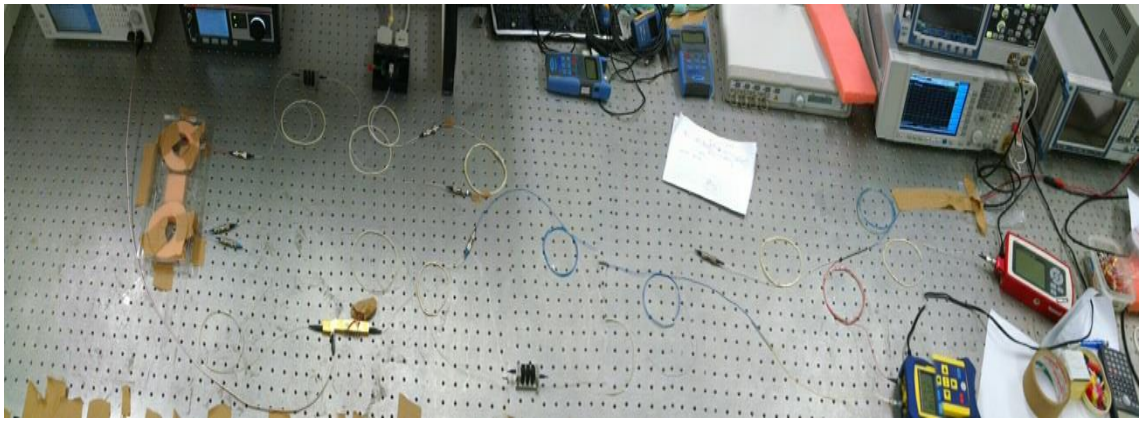
A potência óptica foi medida na entrada e saida do PBS, na entrada apresentou um valor de 5,9±0,3 mW; Na saída, a partir da configuração realizada no conjunto CP-PBS, aferiu-se uma distribuição na qual aproximadamente 90% do sinal 5,35 mW foi conduzido a um dos braços (braço do oscilador local) e aproximadamente 6% do sinal 346,9 μW ao outro braço (braço do sinal). Portanto, sem atenuação, a potência média que se observa na entrada do BS pelo braço do circuito com 6% da potência total é de aproximadamente 1,642 μW e pelo outro braço, com 90% da potência é de aproximadamente 4,123 mW. Existe ainda uma perda de potência que pode ser observada e esta se deve aos moduladores.

Figura 11 - Circuito Óptico fortemente atenuado.



Fonte: Elaborada pelo autor.

Figura 12 - Circuito Óptico de fortemente atenuado - Mesa Óptica.



Fonte: Elaborada pelo autor.

No braço do sinal foi utilizado um sistema para atenuação composto por uma fibra óptica com atenuação fixa no valor de 20 dB e um atenuador variável que pode ser configurado com valores que vão de 1 a 60 dB, dito isto, a atenuação no experimento poderia alcançar um valor máximo de atenuação de 80 dB, proporcionando atenuação suficiente para se atingir um regime de fóton único.

Para efetuar o cálculo da atenuação é necessária utilização de alguns parâmetros, são estes:

a) comprimento de onda λ = 1550 nm.

b) constante de Planck h = 6,626·10^{-34} Js.

c) velocidade da luz c = 3·10^{8} m/s.

d) a potência medida na entrada do divisor de feixes na ausência de atenuação, P_{med} = 1,642 μW.

e) o fluxo médio de fótons desejados n = 0,1.

Para o cálculo da atenuação temos as seguintes expressões:

$$nf = \frac{P_{med}10^{-0.1\alpha[dB]}\lambda}{hc} \Rightarrow \alpha = -10\ \log_{10}\left(\frac{nfhc}{P_{medido}\lambda}\right), \tag{4.10}$$

em que *f* é a frequência do sinal modulante e α é a atenuação desejada.

A partir da equação (4.10) pode-se obter os valores necessários de frequência e atenuação para se obter um regime que considerado de fóton único, ou seja que apresentem, como resultado o valor de $n = 0{,}1$ fótons.

A Tabela 1 apresenta estes valores considerando dois valores distintos de potência na entrada do BS. São eles: 1,642 µW e 1,542 µW.

Tabela 1 - Atenuação para fótons.

Frequência (GHz)	1,642 µW	1,542 µW
	Atenuação α (dB)	
1	51,0733	50,8004
1,2	50,2815	50,0086
1,3	49,9339	49,6610
1,5	49,3124	49,0395

Fonte: Elaborada pelo autor.

5.6 Resultados das Medições

Os resultados das medições são apresentados na Tabela 2. Estes, decorrem de sucessivas medições nas quais os valores de atenuação óptica foram sistematicamente alterados de maneira crescente a fim de descrever o comportamento do sinal medido pelo analizador de espectro a medida que o valor de atenuação aumentava.

Ainda na Tabela 2 é possível observar a potência elétrica medida pelo analisador de espectro em função da variação dos valores de atenuação, e o respectivo número médio de fótons para essa potência. O valor da potência no analisador de espectro na ausência de potência ópitca, ou seja, quando o laser está desligado (LD = OFF) é apresentado como valor de referência para a situação em que o único sinal que se observa é o ruído de fundo.

Com o propósito de ilustrar os diferentes resultados nas medições experimentais da Figura 13 bem como da Figura 14 apresentam a captura de tela do analisador de espectro na

situação de ausência do sinal óptico (quando o laser está desligado) e na situação em que o sinal modulante está configurado segundo as seguintes especificações:

a) Frequência de 1,3 GHz alimentando o modulador de amplitude e

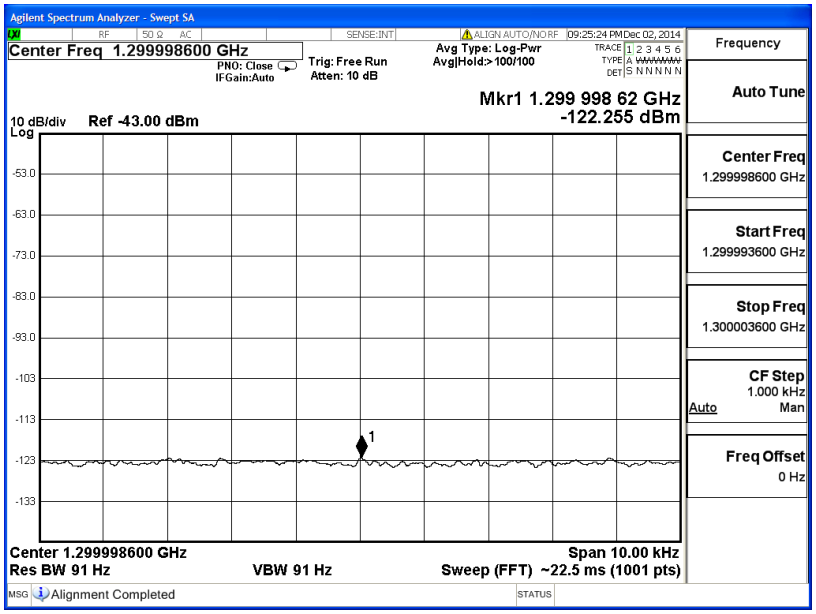
b) Atenuação óptica de 50 dB no braço do sinal (n ~ 0,1).

Tabela 2 - Resultados das medições.

FREQUÊNCIA		1.0 GHz			1.2 GHz			1.3 GHz			1.5 GHz		
LD	dB	dBm	NÚMERO DE FÓTONS		dBm	NÚMERO DE FÓTONS		dBm	NÚMERO DE FÓTONS		dBm	NÚMERO DE FÓTONS	
			1,642 µW	1,542 µW		1,642 µW	1,542 µW		1,642 µW	1,542 µW		1,642 µW	1,542 µW
ON	21	-95.030	101.7026	95.5088	-94.471	84.7522	79.5907	-90.334	78.2328	73.4683	-89.566	67.8018	63.6725
ON	25	-99.027	40.4885	38.0227	-98.560	33.7405	31.6856	-93.819	31.1450	29.2483	-93.247	26.9924	25.3485
ON	30	-102.608	12.8036	12.0238	-104.117	10.6697	10.0199	-97.083	9.8489	9.2491	-99.544	8.5357	8.0159
ON	35	-107.529	4.0489	3.8023	-108.378	3.3740	3.1686	-101.511	3.1145	2.9248	-104.769	2.6992	2.5348
ON	40	-111.626	1.2804	1.2024	-113.115	1.0670	1.0020	-107.350	0.9849	0.9249	-107.377	0.8536	0.8016
ON	45	-116.263	0.4049	0.3802	-116.690	0.3374	0.3169	-111.867	0.3115	0.2925	-111.442	0.2699	0.2535
ON	46	-116.977	0.3216	0.3020	-117.032	0.2680	0.2517	-113.485	0.2474	0.2323	-112.559	0.2144	0.2014
ON	47	-118.427	0.2555	0.2399	-118.049	0.2129	0.1999	-114.339	0.1965	0.1845	-113.790	0.1703	0.1599
ON	48	-118.818	0.2029	0.1906	-119.272	0.1691	0.1588	-114.885	0.1561	0.1466	-114.385	0.1353	0.1270
ON	49	-119.636	0.1612	0.1514	-120.190	0.1343	0.1261	-115.468	0.1240	0.1164	-114.873	0.1075	0.1009
ON	50	-119.985	0.1280	0.1202	-120.627	0.1067	0.1002	-116.461	0.0985	0.0925	-116.561	0.0854	0.0802
ON	51	-120.637	0.1017	0.0955	-120.918	0.0848	0.0796	-116.869	0.0782	0.0735	-117.045	0.0678	0.0637
ON	52	-120.892	0.0808	0.0759	-121.177	0.0673	0.0632	-117.398	0.0621	0.0584	-117.779	0.0539	0.0506
ON	53	-121.015	0.0642	0.0603	-121.626	0.0535	0.0502	-118.200	0.0494	0.0464	-117.840	0.0428	0.0402
ON	54	-121.694	0.0510	0.0479	-122.334	0.0425	0.0399	-119.394	0.0392	0.0368	-118.659	0.0340	0.0319
ON	55	-122.255	0.0405	0.0380	-122.549	0.0337	0.0317	-120.240	0.0311	0.0292	-120.126	0.0270	0.0253
ON	60	-122.826	0.0128	0.0120	-123.435	0.0107	0.0100	-122.292	0.0098	0.0092	-121.225	0.0085	0.0080
OFF	X	-123.530	0	0	-123.317	0	0	-122.758	0	0	-121.800	0	0

Fonte: Elaborada pelo autor.

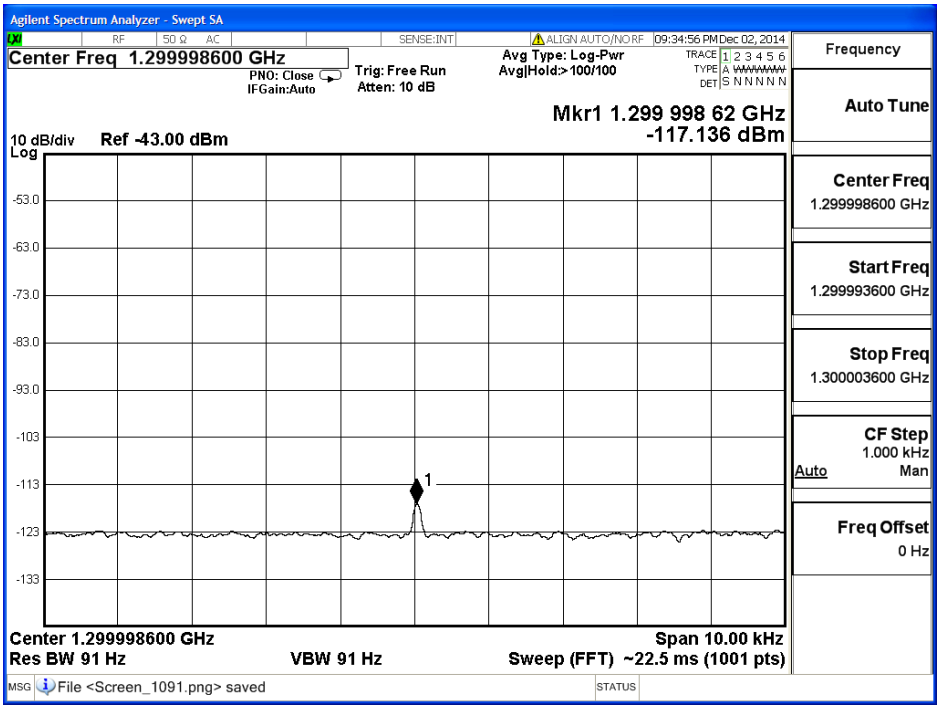
Figura 13 - Tela do analisador de espectro com o laser desligado.



Fonte: Elaborada pelo autor.

Na Figura 13 o número 1 , que pode ser localizado no meio da tela, representa o marcador que localiza, no gráfico, a frequência de 1,3GHz que neste caso, por não estar recebendo o sinal óptico, não difere das outras frequências.

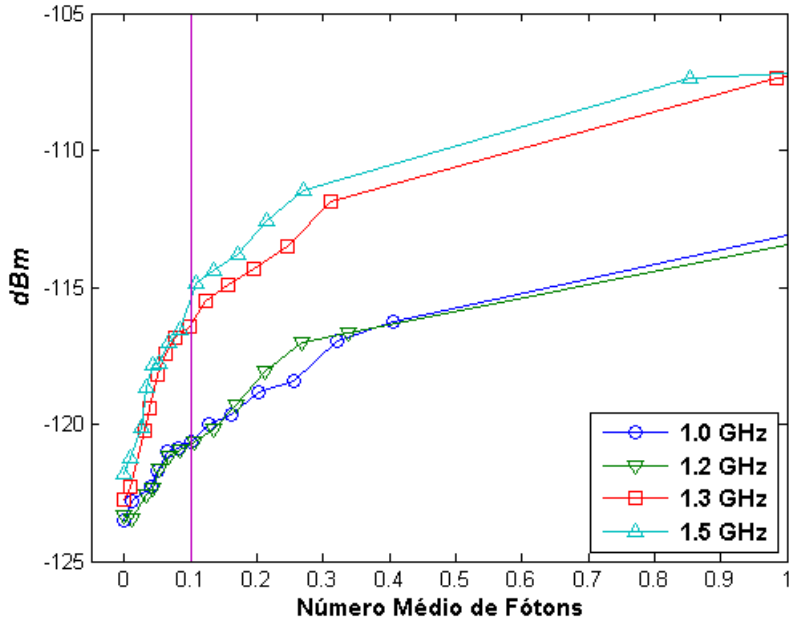
Figura 14 - Tela do analisador de espectro quando um sinal modulante de 1,3 GHz é utilizado. Atenuação 50 dB e número médio de Fótons 0,0985.



Fonte: Elaborada pelo autor.

A Figura 14, por sua vez, mostra a frequência localizada no marcador 1 (1,3 GHz) em destaque por estar recebendo o sinal óptico. A partir dos resultados obtidos nos experimentos utilizando o valor de potência medida, para as quatro frequências consideradas, é possível calcular o número médio de fótons. No caso da Figura 14 potência óptica medida indica um número médio de fotons de aproximadamente 0,0985.

Figura 15 - Número Médio de Fótons versus Potência.



Fonte: Elaborada pelo autor.

De posse dos valores obtidos através das medições foi construído o gráfico (Figura 15) que, fornece artificios para compararmos como os valores de potência variam em função do número médio de fótons.

6 CONCLUSÕES E PERSPECTIVAS DE TRABALHOS FUTUROS

6.1 CONCLUSÕES

A presente tese pode ser dividia em três partes: I) Protocolo quântico de compromisso de informação. II) Distribuição quantum-caótica de chaves com pulsos multifótons. III) Detecção homódina de estados coerentes fortemente atemnuados. As conclusões referentes a cada uma dessas partes são as seguintes:

6.1.1 Protocolo quântico de compromisso de informação

Foi demonstrado que, considerando uma situação física mais realista, ou seja, que os fótons possuem distribuição espectral e que as portas quânticas ópticas variam com a frequência, ao contrário do que fora demonstrado na literatura, o protocolo quântico de compromisso de informação proposto por Lo-Chau e Mayers não é incondicionalmente inseguro. Em outras palavras, há uma probabilidade maior que zero que Alice seja pega trapaceando.

6.1.2 Distribuição quantum-caótica de chaves com pulsos multifótons

Uma vez que o protocolo QCKD usas estados coerentes com valores contínuos de fase, Alice pode usar estados coerentes com um número médio de fótons muito maior que 0,1, o valor tradicionalmente usado em configurações de QKD. Isso é possível porque, sem saber quais bases de medição usar, Eva ataca realizando uma tomografia homódina. Assim, é suficiente para manter a segurança que Alice use um estado coerente com o número médio de fótons menor do que o valor necessário para Eva obter uma boa estimativa do estado enviado por ela.

É importante notar que o protocolo QCKD usado requer que Alice e Bob compartilhem antecipadamente os mesmos dados de seus sistemas não lineares (parâmetros e valores iniciais). Essa é a autenticação necessária para evitar o ataque conhecido como *man-in-the-midle*. Entretanto, pode-se argumentar que, como Alice e Bob compartilham os mesmos

parâmetros e valores iniciais, seus sistemas não lineares estarão sempre sincronizados e a comunicação quântica entre eles não será necessária. Isto é uma meia verdade. Sem a comunicação quântica, sua dinâmica dos sistemas não lineares será determinística. A detecção de fótons únicos em Bob introduz um parâmetro aleatório nos sistemas não lineares, tornando sua dinâmica além de não linear, estocástica. Além disso, também é possível trocar o sistema não linear *Z* por um verdadeiro gerador de bit aleatório, aumentando ainda mais a imprevisibilidade dos sistemas não lineares usados por Alice e Bob.

6.1.3 Detecção homódina de fótons.

O experimento de realizado detecção homódina de fótons realizado mostrou que o sinal analógico transportado por um estado coerente fortemente atenuado pode ser recuperado por um receptor óptico baseado em PIN, a vantagem deste dispositivo é além de seu custo inferior, o seu fácil manuseio e a possibilidade de realizar a detecção sem a necessidade de elevadas voltagens nem resfriamento.

Na detecção homódina a necessidade de um oscilador local em fase com a portadora de sinal á a desvantagem desta técnica, desvantagem esta também encontrada sistemas de detecção coerente.

6.2 Perspectivas de Trabalhos Futuros

Como perspectivas de trabalhos futuros pode-se citar:

a) A análise de segurança de outros protocolos de criptografia quântica levando em consideração a largura espectral dos fótons e a dependência com a frequencia das portas quânticas envolvidas.

b) Analisar a segurança do protocolo de QCKD considerando outros tipos de ataque, como o ataque por máquina de clonagem.

c) Aperfeiçoar o experimento de medição homódina de fótons e utilizá-lo na caracterização de fontes de estados quânticos e na realização experimental de protocolos de QKD.

7 REFERÊNCIAS

ARDEHALI, M. A perfectly secure quantum bit commitment protocol. **Los Alamos preprint archive quant-ph/9505019**, 1995.

BARBOSA, F. A. S.; COELHO, A. S.; CASSEMIRO, K. N.; *et al.* Beyond spectral homodyne detection: Complete quantum measurement of spectral modes of light. **Physical Review Letters**, v. 111, n. 20, p. 200402, 2013.

BENNETT, C. H.; BRASSARD, G. Quantum Cryprography: Public Key distribution and coin tossing. Int. Conf. on Computers, Systems & Signal Processing. **Anais...** . p.175–179, 1984.

BOURENNANE, M.; KARLSSON, A.; BJÖRK, G. Quantum key distribution using multilevel encoding. **Physical Review A**, v. 64, n. 1, p. 012306, 2001.

BRASSARD, G.; CRÉPEAU, C. Quantum Bit Commitment and Coin Tossing Protocols. Proceedings of the 10th Annual International Cryptology Conference on Advances in Cryptology. **Anais...** . p.49–61, 1991.

BRASSARD, G.; CREPEAU, C.; JOZSA, R.; LANGLOIS, D. A quantum bit commitment scheme provably unbreakable by both parties. Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science. **Anais...** . p.362–371, 1993.

BREITENBACH, G.; SCHILLER, S.; MLYNEK, J. Measurement of the quantum states of squeezed light. **Nature1**, v. 387, p. 471–475, 1997.

COLLINS, G. P. Quantum cryptography defies eavesdropping. **Physics Today**, v. 45, n. 11, p. 21–23, 1992.

DAMASCENO, R. L. C.; OLIVEIRA, G. L. DE; RAMOS, R. V. **Quantum-chaotic key distribution with synchronized logistic maps**. Relatório interno. Universidade Federal do Ceará. Fortaleza, 2018.

GISIN, N.; RIBORDY, G.; TITTEL, W.; ZBINDEN, H. Quantum cryptography. **Reviews of Modern Physics**, v. 74, n. 1, p. 145–195, 2002.

GUERRA, A. G. DE A. H. **Comunicação Quântica Segura Direta E Polarização Quântica Usando Estados Contínuos Da Luz**. 2017. 89 f. Universidade Federal do Ceará. 2017.

GUERRA, A. G. DE A. H.; RIOS, F. F. S.; RAMOS, R. V. Quantum secure direct communication of digital and analog signals using continuum coherent states. **Quantum Information Processing**, v. 15, n. 11, p. 4747–4758, 2016.

HANSEN, H.; AICHELE, T.; HETTICH, C.; *et al.* Ultrasensitive pulsed, balanced homodyne detector: application to time-domain quantum measurements. **Optics Letters**, v. 26, n. 21, p. 1714, 2001.

HIRANO, T.; YAMANAKA, H.; ASHIKAGA, M.; KONISHI, T.; NAMIKI, R. Quantum cryptography using pulsed homodyne detection. **Physical Review A**, v. 68, n. 4, p. 042331,

2003.

JONES, W. . Introduction to Optical Fiber Communication Systems. Workshop-June. **Anais...** . v. 17, p.1–20, 1988.

LEONHARDT, U.; MUNROE, M.; KISS, T.; RICHTER, T.; RAYMER, M. . Sampling of photon statistics and density matrix using homodyne detection. **Optics Communications**, v. 127, n. 1–3, p. 144–160, 1996.

LEONHARDT, U.; PAUL, H. High-accuracy optical homodyne detection with low-efficiency detectors: “Preamplification” from antisqueezing. **Physical Review Letters**, v. 72, n. 26, p. 4086–4089, 1994.

LO, H.-K.; CHAU, H. F. Is Quantum Bit Commitment Really Possible? **Physical Review Letters**, v. 78, n. 17, p. 3410–3413, 1997.

LO, H.-K.; ZHAO, Y. Quantum Cryptography. **Scientific American**, v. 267, n. 4, p. 50–57, 2008.

LO, H.-K.; ZHAO, Y. Quantum cryptography. **Computational Complexity**. p.2453–2477, 2012.

MAYERS, D. Unconditionally secure quantum bit commitment is impossible. **Physical Review Letters**, v. 78, n. 17, p. 3414–3417, 1997.

MENDONÇA, F. A. **Protocolos e Detectores de Fótons para Cominicações Quânticas**. 2011. Universidade Federal do Ceará. 2011.

MURTA, G.; CUNHA, M. T.; CABELLO, A. Quantum nonlocality allows for ever-lasting unconditionally secure bit commitment. **measurements**, v. 16, p. 1, 2013.

OLIVEIRA, G. L. DE; RAMOS, R. V. Quantum-chaotic cryptography. **Quantum Information Processing**, v. 17, n. 3, p. 40, 2018.

ORTEGA, L. P. Compressão de ruído quântico em um interferômetro Sagnac em fibra com laser pulsado em 1, 55 microns. , 2015.

RAFFAELLI, F.; FERRANTI, G.; MAHLER, D. H.; *et al.* A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers. **Quantum Science and Technology**, v. 3, n. 2, p. 025003, 2018.

RAMOS, R. V.; SOUZA, R. F. Simulations of continuum coherent states and its use in quantum cryptographic systems. **Journal of Modern Optics**, v. 48, n. 6, p. 989–1003, 2001.

ROCHA, M. DE L.; CARNEIRO, F. R. Sistemas de Comunicações Opticas Coerentes (Tutorial). Disponível em: <https://goo.gl/CeJVqQ>. Acesso em: 30/4/2018.

SALEH, B. E. A.; TEICH, M. C. Eletro-Optocs. **Fundamentals of photonics**, 1991.

SANTOS, D. J.; LOUDON, R.; FRAILE-PELÁEZ, F. J. Continuum states and fields in quantum optics. **American Journal of Physics**, v. 65, n. 2, p. 126–132, 1997.

SHAPIRO, J. Quantum noise and excess noise in optical homodyne and heterodyne receivers. **IEEE Journal of Quantum Electronics**, v. 21, n. 3, p. 237–250, 1985.

YANOFSKY, N. S. **An Introduction to Quantum Computing**. Oxford University Press, 2007.

YEH, C. Introduction to Optical Fiber Communication Systems. **Handbook of Fiber Optics**. p.213, 1990.

YUEN, H. P. How to Build Unconditionally Secure Quantum Bit Commitment Protocols. **arXiv**, v. quant-ph, 2003.

YUEN, H. P.; CHAN, V. W. S. Noise in homodyne and heterodyne detection. **Optics Letters**, v. 8, n. 3, p. 177, 1983.

YUEN, H. P.; SHAPIRO, J. H. Optical Communication with Two-Photon Coherent States — Part III: Quantum Measurements Realizable with Photoemissive Detectors. **IEEE Transactions on Information Theory**, v. 26, n. 1, p. 78–92, 1980.

ANEXO A – 1º ARTIGO DECORRENTE DA TESE

Quantum Inf Process (2016) 15:4747–4758
DOI 10.1007/s11128-016-1410-0

Quantum secure direct communication of digital and analog signals using continuum coherent states

Antônio Geovan de Araújo Holanda Guerra[1] ·

Received: 18 February 2016 / Accepted: 28 July 2016 / Published online: 11 August 2016

Abstract In this work, we present optical schemes for secure direct quantum communication of digital and analog signals using continuum coherent states and frequency-dependent phase modulation. The main advantages of the proposed schemes are that they do not use entangled states and they can be implemented with today technology. The theory of quantum interference of continuum coherent state is described, and the optical setups for secure direct communication are presented and their securities are discussed.

Keywords Quantum communication · Coherent states · Thermal states

1 Introduction

Quantum key distribution (QKD) is a well studied quantum protocol [1–4] that has achieved a commercial status. An intrinsic property of QKD protocols is the fact that the final key is a random sequence of bits not controlled by any of the legitimate participants, Alice and Bob. This happens because, in the QKD protocols rules, at least one of them makes (binary) random modulations in the optical signal or random choice of

✉ Rubens Viana Ramos
rubens.viana@pq.cnpq.br

Antônio Geovan de Araújo Holanda Guerra
geovanguerra@gmail.com

Francisco Franklin Sousa Rios
frfranklin.rios@gmail.com

the basis of measurement. An alternative is the quantum secure direct communication (QSDC) [5–9]. In such protocols, the communication is deterministic, in the sense that, under noiseless condition, the sender controls the information received by the receiver. Hence, the QSDC is useful for secure transmission of any kind of message, including a cryptographic key. From the best of our knowledge, with exception of the protocol proposed in [10], all the other QSDC protocols found in the literature (up to the present moment) require at least a quantum resource not currently available with today technology. In this direction, the present work describes optical setups using only common linear optical devices, APD-based single-photon detectors and coherent and thermal light sources, for running QSDC protocol of digital and analog signals. A crucial point in the security of the proposed schemes is the spectral distribution of the continuum coherent states. Using a frequency-dependent phase modulation, Alice can hide the phase modulation applied by Bob, making the proposed schemes highly secure. At last, the scheme for QSDC of analog signals uses in the detection a PIN-based optical receiver, what makes its implementation easier and cheaper.

This work is outlined as follows: In Sect. 2, the continuum coherent states are reviewed and their quantum interference is described. In Sect. 3, the optical setups for QSDC of digital signals are presented and their securities are discussed. In Sect. 4, the optical setup for QSDC of analog signals is presented and, at last, the conclusions are drawn in Sect. 5.

2 Continuum coherent state

Before describing the optical setups, let us start by describing the continuum coherent state. It is defined as [11]

$$|\alpha_\omega\rangle = \exp\left[\int \left[\alpha\left(\omega\right) a^\dagger\left(\omega\right) - \alpha^*\left(\omega\right) a\left(\omega\right)\right] \mathrm{d}\omega\right] |0_\omega\rangle \tag{1}$$

$$\langle n\rangle = \int_0^\infty |\alpha\left(\omega\right)|^2 \,\mathrm{d}\omega. \tag{2}$$

In (2), $\langle n\rangle$ is the mean photon number of the state $|\alpha_\omega\rangle$, where $\alpha(\omega)$ is the complex amplitude of the field. Now, let us write $\alpha(\omega)$ in the basis of sinc functions:

$$\alpha\left(\omega\right) = \sum_{k=-\infty}^{\infty} \alpha\left(k\omega_s\right) \mathrm{sinc}\left[\left(\omega - k\omega_s\right)/\omega_s\right] \tag{3}$$

$$\mathrm{sinc}(x) = \sin\left(\pi x\right)/\pi x. \tag{4}$$

In (3), ω_s is the step size in the frequency domain. Using the orthogonality of the sinc function,

$$\frac{1}{\omega_s}\int_{-\infty}^{\infty} \mathrm{sinc}\left[\frac{\left(\omega - k\omega_s\right)}{\omega_s}\right] \mathrm{sinc}\left[\frac{\left(\omega - m\omega_s\right)}{\omega_s}\right] \mathrm{d}\omega = \delta_{km}, \tag{5}$$

and the fact that $\alpha(\omega)$ is zero for negative frequencies, one has that

$$\langle n\rangle = \int_0^{\infty} |\alpha\,(\omega)|^2\,\mathrm{d}\omega = \int_{-\infty}^{\infty} |\alpha\,(\omega)|^2\,\mathrm{d}\omega = \sum_{k=1}^{\infty} |\alpha\,(k\omega_s)|^2\,\omega_s. \tag{6}$$

Equation (6) shows us how to make discrete the continuum coherent state: The continuum coherent state can be approximated by a tensor product of single-frequency coherent states [12]. If $\alpha(\omega)$ vanishes for $\omega > N\omega_s$, then one has just a finite number of modes and, hence,

$$|\alpha_\omega\rangle = \prod_{k=1}^{N} \left|\alpha\,(k\omega_s)\,\sqrt{\omega_s}\right\rangle. \tag{7}$$

As it can be noted in (7), the number of discrete oscillators is equal to the number of samples taken from the field's envelope. This the reason for which we chose the sinc functions for decomposition. Each discrete oscillator is in a (single-frequency) coherent state, and the amplitude of the k-th oscillator is equal to the product of the k-th sample of $\alpha(\omega)$ and the square root of ω_s.

Now, let us consider a Mach-Zehnder interferometer (MZI) in which the phase modulators are frequency-dependent. The MZI is composed by two lossless beam-splitters having transmittance $T = 1/2^{1/2}$ (and reflectance $R = i1/2^{1/2}$) and one phase modulator in each arm, $\phi_A(\omega)$ and $\phi_B(\omega)$. Having as input the state $|\alpha_\omega\rangle|0_\omega\rangle$, the total state at the output is

$$|\psi\rangle = \prod_{k=1}^{N} \left|\alpha\,(k\omega_s)\,\sqrt{\omega_s}e^{i\Omega_k}\cos\left(\Delta_k\right)\right\rangle \left|\alpha\,(k\omega_s)\,\sqrt{\omega_s}e^{i\Omega_k}\sin\left(\Delta_k\right)\right\rangle \tag{8}$$

$$\Omega_k = [\phi_A\,(k\omega_s) + \phi_B\,(k\omega_s)]/2; \quad \Delta_k = [\phi_A\,(k\omega_s) - \phi_B\,(k\omega_s)]/2. \tag{9}$$

Hence, the mean photon numbers at the interferometer's outputs are

$$\langle n_1\rangle = \sum_{k=1}^{N} |\alpha\,(k\omega_s)|^2 \cos^2\left(\frac{\phi_A\,(k\omega_s) - \phi_B\,(k\omega_s)}{2}\right)\omega_s \tag{10}$$

$$\langle n_2\rangle = \sum_{k=1}^{N} |\alpha\,(k\omega_s)|^2 \sin^2\left(\frac{\phi_A\,(k\omega_s) - \phi_B\,(k\omega_s)}{2}\right)\omega_s \tag{11}$$

or, returning to the continuous case,

$$\langle n_1\rangle = \int_0^{\infty} \cos^2\left[\frac{\phi_A\,(\omega) - \phi_B\,(\omega)}{2}\right]|\alpha\,(\omega)|^2\,\mathrm{d}\omega \tag{12}$$

$$\langle n_2\rangle = \int_0^{\infty} \sin^2\left[\frac{\phi_A\,(\omega) - \phi_B\,(\omega)}{2}\right]|\alpha\,(\omega)|^2\,\mathrm{d}\omega. \tag{13}$$

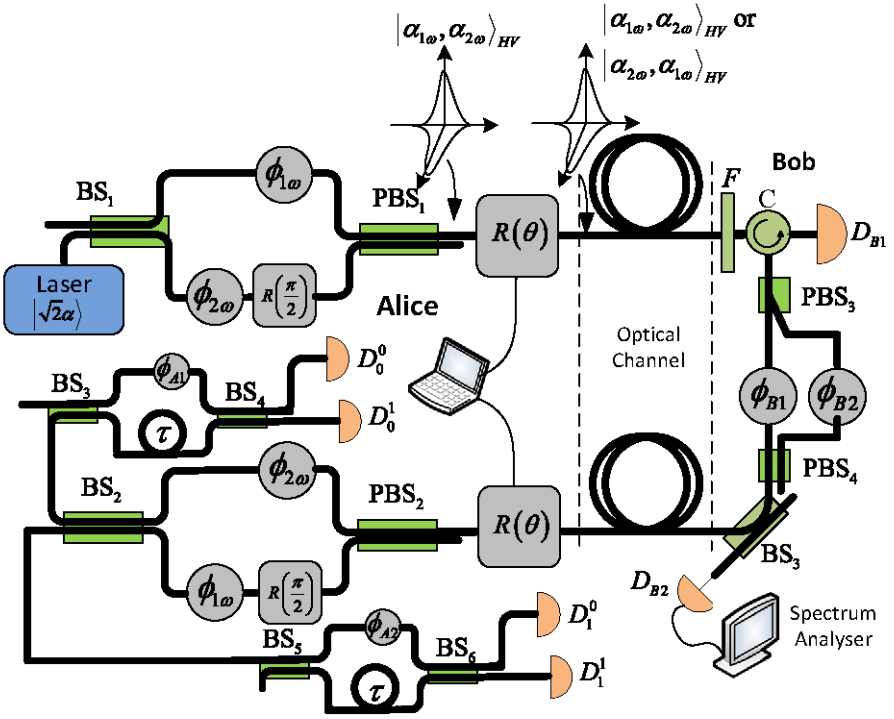


Fig. 1 Optical setup I for QSDC of digital data

3 Quantum secure direct communication of digital signals

A straightforward application of the interference of continuum coherent states is to increase the security of some quantum communication setups. Here, we are going to use continuum coherent states in optical setups for QSDC. The first setup is shown in Fig. 1.

The setup in Fig. 1 works as follows: Initially, using the beam splitter BS_1, the dispersive elements $\phi_{1\omega}$ and $\phi_{2\omega}$ ($\phi_{1\omega}$ and $\phi_{2\omega}$ introduce a different phase modulation in each spectral component of the optical signal), the $\pi/2$-polarization rotator and the polarizing beam splitter PBS_1, Alice produces the two-mode state $|\alpha_{1\omega}, \alpha_{2\omega}\rangle_{\mathrm{HV}}$ (H and V stand for horizontal and vertical polarization modes). After, using $R(\theta)$, Alice randomly rotates its polarization by 0 or $\pi/2$. Thus, the quantum state launched in the optical link is $\rho_A = 0.5|\alpha_{1\omega}, \alpha_{2\omega}\rangle_{HV}\langle\alpha_{1\omega}, \alpha_{2\omega}| + 0.5|\alpha_{2\omega}, \alpha_{1\omega}\rangle_{HV}\langle\alpha_{2\omega}, \alpha_{1\omega}|$. When this state reaches Bob's place, each polarization mode is phase modulated, now by a frequency independent phase modulator. Hence, the quantum state leaving Bob is

$$\begin{aligned}\rho_B = {} & 0.5\left|\alpha_{1\omega}e^{i\phi_{B1}}, \alpha_{2\omega}e^{i\phi_{B2}}\right\rangle_{HV}\left\langle\alpha_{1\omega}e^{i\phi_{B1}}, \alpha_{2\omega}e^{i\phi_{B2}}\right| \\ & + 0.5\left|\alpha_{2\omega}e^{i\phi_{B1}}, \alpha_{1\omega}e^{i\phi_{B2}}\right\rangle_{HV}\left\langle\alpha_{2\omega}e^{i\phi_{B1}}, \alpha_{1\omega}e^{i\phi_{B2}}\right|. \end{aligned} \tag{14}$$

Bob chooses randomly one of the values $\{0, \pi, \pi/2, 3\pi/2\}$ for ϕ_{B1} and ϕ_{B2}, however, if he wants to transmit the bit 0 (1), he does $\phi_{B1} - \phi_{B2} = 0(\pi)$. The state in (14) is sent back to Alice. Alice, by her turn, applies a polarization rotation of 0 or $\pi/2$, in such way that, the pulse that passed through the dispersive element $\phi_{1\omega}(\phi_{2\omega})$ in the transmission, it will pass now by the dispersive element $\phi_{2\omega}(\phi_{1\omega})$. Additionally, a $\pi/2$ polarization rotation is applied in one of the pulses. In this way, the two pulses will arrive at BS_2 at the same time, with the same polarization and phase difference equal to $\phi_{B1}-\phi_{B2}$. If $\phi_{B1}-\phi_{B2} = 0$, and the light is sent to the upper interferometer composed by $BS_3 - \phi_{A1} - BS_4$ and detected in D_0^0 or D_0^1, which implies the detection of a bit '0'. On the other hand, if $\phi_{B1} - \phi_{B2} = \pi$, the light is sent to the lower interferometer composed by $BS_5 - \phi_{A2} - BS_6$ and detected in D_1^0 or D_1^1,which implies the detection of a bit '1'. Alice chooses randomly one of the values $\{0, \pi/2\}$ for ϕ_{A1} and ϕ_{A2}.

The security of this scheme is based on two conditions: (1) The secrets known only by Alice: the mean photon number of the continuum coherent state used, the values of $\phi_{1\omega}$ and $\phi_{2\omega}$ and which states are in the horizontal and vertical polarizations. (2) The differential quadrature phase-shift quantum key distribution that runs in parallel. For the eavesdropper, Eve, to get any information about Bob's modulations, she can try to make interference between the optical pulses leaving Bob's place, however, without knowing $\phi_{1\omega}$and$\phi_{2\omega}$, she will not be able to get any useful information since she will be limited by (12) and (13). In other words, using a beam splitter to make the interference of the pulses coming from Bob (first Eve has to rotate by $\pi/2$ the polarization of one of them), Eve will obtain the following mean photon numbers at her beam splitter's outputs

$$\langle n_1 \rangle = \int_0^\infty \cos^2 \left[\frac{(\phi_{1\omega}(\omega) - \phi_{2\omega}(\omega)) + (\phi_{B1} - \phi_{B2})}{2} \right] |\alpha(\omega)|^2 \, \mathrm{d}\omega \quad (15)$$

$$\langle n_2 \rangle = \int_0^\infty \sin^2 \left[\frac{(\phi_{1\omega}(\omega) - \phi_{2\omega}(\omega)) + (\phi_{B1} - \phi_{B2})}{2} \right] |\alpha(\omega)|^2 \, \mathrm{d}\omega. \quad (16)$$

Hence, the mean photon numbers depend on $\phi_{1\omega}$ and $\phi_{2\omega}$ that are not known by Eve. The worst case for Eve occurs when $\phi_{1\omega}$ and $\phi_{2\omega}$ are chosen in such way that

$$\int_0^\infty \cos\left[\phi_{1\omega}(\omega) - \phi_{2\omega}(\omega)\right] |\alpha(\omega)|^2 \, d\omega = 0. \quad (17)$$

Eve can try to find out the values of the functions $\phi_{1\omega}$ and $\phi_{2\omega}$. In order to prevent this attack, the mean photon number of the pulses must be low. If $\phi_{1\omega}$ and $\phi_{2\omega}$ were functions with low autocorrelation (like a random process), a mean photon number equal to 0.1 photons per frequency would be a good choice since Eve would have to find out the value of each frequency independently. However, in practice, the functions $\phi_{1\omega}$ and $\phi_{2\omega}$ produced by a dispersive optical element tend to be smooth and well behaved. In this case, a more conservative choice of less than one photon per pulse (i.e., considering all frequencies) in average would make the system more secure. In the extreme case of $\phi_{1\omega}$ being constant (frequency independent), the traditional case of 0.1 photons per pulse is recovered.

Another possibility for Eve to get information about Bob's modulations is to send optical pulses to Bob and analyze them after Bob's modulations. In order to avoid this attack, Bob uses three countermeasures: (1) He has a filter F that forces Eve to use the wavelength that Bob's detectors "see". (2) He uses the circulator C and the detector D_{B1} in order to make his setup unidirectional. (3) He uses a single-photon detector, D_{B2}, plugged to an electrical spectrum analyzer (ESA) and checks the electrical power in a fixed frequency band. This electrical power will depend on the photon number distribution of the quantum light state (and, hence, on the mean photon number) used by Alice [10,13,14]. Without knowing the correct value of the mean photon number or to send pulses out of the correct time, slots will result in a different value for the measured electrical power. At the end of the communication, Bob informs to Alice the electrical power measured and Alice checks if that value is in accordance with the mean photon number used. This avoids, for example, the usage of strong optical pulses that would make Eve's task of getting ϕ_{B1} and ϕ_{B2} values easier.

In a practical point of view, Alice will accept a value measured by Bob inside of a range around the expected value. In this case, Eve does not need to know the exact value of the mean photon number used by Alice; a good approximation may be enough. In this direction, let us consider the following situation: Eve breaks the optical link between Alice and Bob. She uses a beam splitter (with reflectivity value equal to the loss in the link between Alice and Bob) at Alice's output. In one output, Eve uses the same measurement setup as Bob (a single-photon detector plugged to a spectral analyzer) to get an estimation α_{est} of the mean photon number used by Alice. After this, she prepares and sends to Bob the quantum state $|\alpha_{est}, \alpha_{est}\rangle_{HV}$. At Bob's output, Eve gets the state $|\alpha_{est}\exp(i\phi_{B1}), \alpha_{est}\exp(i\phi_{B2})\rangle_{\mathrm{HV}}$. Since $\phi_{B1} - \phi_{B2} = 0$ or π (the cases where $\phi_{B1} - \phi_{B2}$ is equal to $\pi/2$ or $3\pi/2$ are discussed latter), Eve can use a simple beam splitter to make their interference and to obtain the bit value sent by Bob. Now, according to that result, Eve modulates the non-detected part of the pulse sent by Alice and she sends it back to Alice by a lossless fiber. There are two problems in this attack. Firstly, Eve will need many pulses sent by Alice in order to get a good estimation of the mean photon number used [13]. While she is still measuring, she will have to send pulses to Bob with a guessed mean photon number (the lack of light arriving in Bob will result in an electrical power equal to the background noise). Secondly, as it can be note in Fig. 1, there is a differential quadrature phase-shift quantum key distribution running in parallel.

Even when Eve can determine the bit of the QSDC protocol sent by Bob ($\phi_{B1} - \phi_{B2}$), she cannot determine the values of ϕ_{B1} and ϕ_{B2} separately, and hence, she will introduce errors in the QKD protocol, what will be noted by Alice after the classical communication between Bob and her, when Bob reveals the bases used. One must note that the situations where $\phi_{B1} - \phi_{B2}$ is equal to $\pi/2$ or $3\pi/2$ are decoy states. At the end of the protocol, Bob informs to Alice in which time slots he used a decoy state and the corresponding bit is discarded.

The optical setup of the differential quadrature QKD protocol embedded in the optical setup of the QSDC protocol is composed by ϕ_{B1} and ϕ_{B2} in Bob and the upper ($\mathrm{BS}_3 - \phi_{A1} - \mathrm{BS}_4$) and lower ($\mathrm{BS}_5 - \phi_{A2} - \mathrm{BS}_6$) interferometers in Alice. Its rules and security are well described in [14,15]. The error rate in the key obtained in this QKD protocol is used to infer the presence of Eve, although other applications for

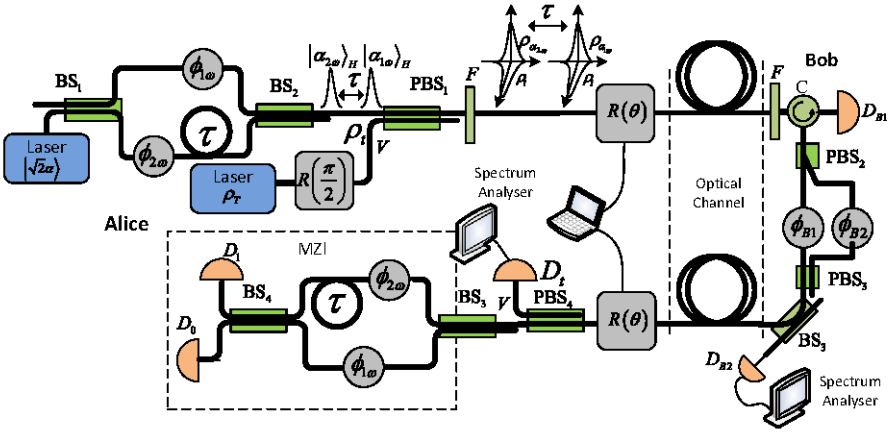


Fig. 2 Optical setup II for QSDC of digital messages

this key could also be realized. At last, one should note that after the interference in BS_2 the phase of the output pulse is $\phi_{B1} + \phi_{B2}$. Hence, the phase difference between two-consecutive pulses (n-th and $(n+1)$-th) in the QKD setup is $[\phi_{B1}(n) + \phi_{B2}(n)] - [\phi_{B1}(n+1) + \phi_{B2}(n+1)]$. Depending on the value of $\phi_{B1}(n) - \phi_{B2}(n)$ and $\phi_{B1}(n+1) - \phi_{B2}(n+1)$, the QKD setup uses $(BS_3 - \phi_{A1} - BS_4)$ or $(BS_5 - \phi_{A2} - BS_6)$.

The second setup for QSDC of digital messages is shown in Fig. 2. Comparing with the first setup shown in Fig. 1, it has the security improved by the use of thermal states. A detailed discussion about security of two-layer quantum protocols using coherent and thermal states can be found in [16]. The setup in Fig. 2 works as follows: Alice produces two optical pulses, separated in time by τ. The first pulse is in the state $(\rho_1 \otimes \rho_T)_{HV}$, while the second one is in the state $(\rho_2 \otimes \rho_T)_{HV}$ where $\rho_1 = |\alpha_{1\omega}\ \alpha_{1\omega}|$, $\rho_2 = |\alpha_{2\omega}\ \alpha_{2\omega}|$, and ρ_T is the density matrix of the thermal state, $\rho_T = \sum_n \left[\mu_T^n / (1+\mu_T)^{1+n}\right] |n\ n|$ where μ_T is the mean photon number. After Alice's first polarization rotator $R(\theta)$, the first pulse launched in the channel is $1/2\,(\rho_1 \otimes \rho_T)_{HV} + 1/2\,(\rho_T \otimes \rho_1)_{HV}$, while the second pulse is in the state $1/2\,(\rho_2 \otimes \rho_T)_{HV} + 1/2\,(\rho_T \otimes \rho_2)_{HV}$. However, Alice acts in such way that, if ρ_1 is in the horizontal (vertical) mode ρ_2 is in the vertical (horizontal) mode. When the pulses arrive at Bob, they are phase modulated (one may note that the thermal states are not affected by Bob's phase modulation) and sent back to Alice. Alice, by her turn, applies a polarization rotation in such way that the thermal state always emerge in the vertical output of PBS_4. On the other hand, the horizontal pulses are sent to an interferometer with a delay of τ in one of the arms. At its output, there will be interference between the pulses that took the short-long and long-short paths in Alice's interferometers. The phase difference between the pulses that will suffer interference is equal to $\phi_{B1} - \phi_{B2}$. Once again, if $\phi_{B1} - \phi_{B2=}0(\pi)$, a detection occurs in $D_0(D_1)$ and a bit 0 (1) is recorded.

As discussed in [14], the security of this scheme is based on the secrets known only by Alice: the mean photon number used for the coherent and thermal states, the values of $\phi_{1\omega}$ and $\phi_{2\omega}$ and which states are in the horizontal and vertical polarizations.

For Eve to get any information about Bob's modulation, she has to make interference between the optical pulses leaving Bob's place; however, she does not know in which polarization mode the coherent states are and which are the values of $\phi_{1\omega}$ and $\phi_{2\omega}$, and hence, she will not be able to get any useful information. As it happened in the first scheme, another possibility for Eve is to send optical pulses to Bob and analyze them after Bob's modulations. As before, Bob uses the filter F, the circulator C together with detector D_{B1} and a single-photon detector, D_{B2}, plugged to an ESA. The electrical power measured by the ESA will depend on the mean photon numbers chosen by Alice for the coherent and thermal states. Without knowing the exact value of those mean photon number or sending pulses out of the correct time, slots will result in a different value for the measured electrical power. At the end of the communication, Bob informs to Alice the electrical power measured and Alice checks if that value is in accordance with the mean photon numbers used.

Since Alice uses low mean photon number pulses, sometimes, she will not have any detection in D_0 and D_1. In these cases, Alice informs to Bob the time slots in which she did not have any detection, and they run the protocol again until the complete information is transmitted from Bob to Alice.

Although not shown in Fig. 2, the differential quadrature phase-shift QKD can be easily included in this setup by placing the upper and lower interferometers of Fig. 1 in Alice.

4 Quantum secure direct communication of analog signals

Single-photon detectors based on APDs are expensive, they have to be cooled in order to decrease the dark current that can flag a false photo-detection, they have problems to operate at high transmission rates due to the after pulsing and they have low quantum efficiency at 1550 nm optical window. Hence, quantum communication setups using PIN-based optical receivers are highly desired, since PIN photodiodes are cheaper, faster and they do not need to be cooled. Continuous and discrete variable QKD setups using PIN-based optical receivers have been reported, however, all of these protocols are based on the measurements of the quadratures and, hence, they use two PIN detectors. On the opposite direction, the optical scheme for QSDC of analog data here proposed uses only one PIN detector, as shown in Fig. 3. Since the information to be transmitted is an analog signal, the light sources are CW.

The QSDC protocol can be understood as follows: The coherent state emitted by Alice's CW coherent source is split by the unsymmetrical beam splitter BS_1 into the signal (ρsig - with mean photon number lower than 1) and local (ρ_{LO} - with high mean photon number) components. The signal and local coherent states pass through the same dispersive optical devices and they get frequency-dependent phase modulation. Furthermore, ρ_{LO} is delayed in order to compensate the time needed to the signal pulse sent to Bob to return to Alice's apparatus. Once in Bob, the light beams are phase modulated by an analog signal. Once again, the thermal state is not affected by Bob's phase modulator. At Alice's apparatus input, the same polarization rotation must be applied in order to assure the thermal state in the vertical polarization and the signal

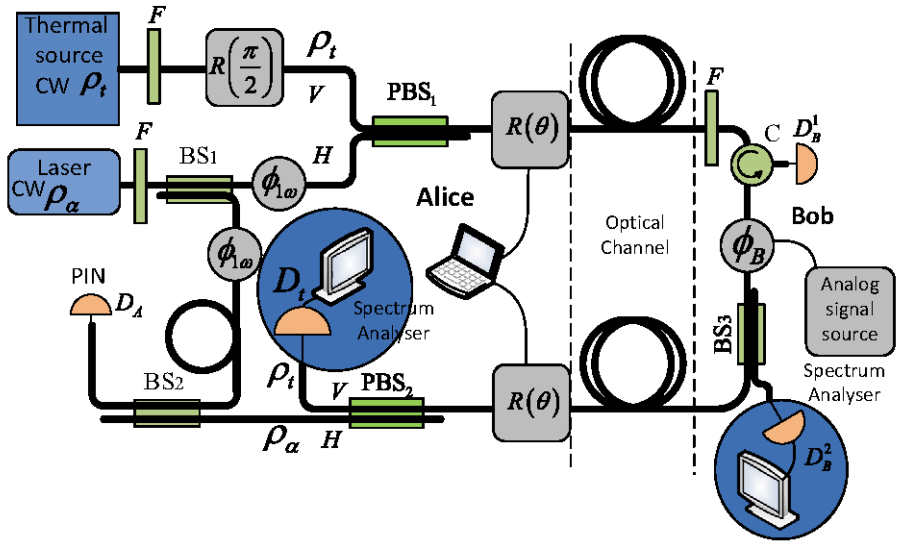


Fig. 3 Optical scheme for QSDC of analog messages

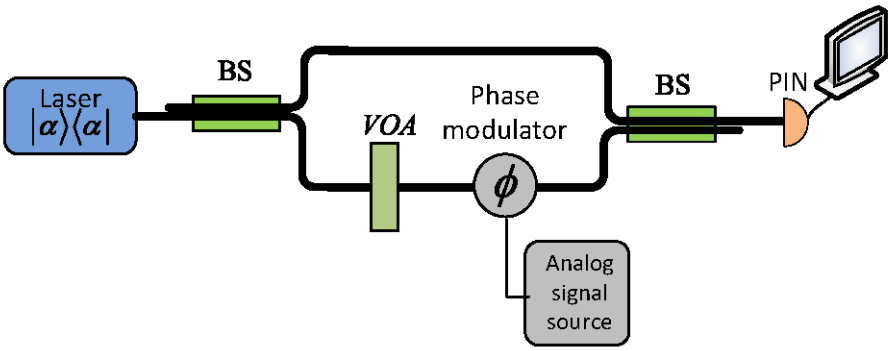


Fig. 4 Optical scheme for detection of modulated weak coherent state using PIN photodiode. *VOA*: variable optical attenuator, *BS* balanced beam splitter

(coherent state) in the horizontal polarization. The former is sent to the state analyzer (single-photon detector and ESA), while the second is sent directly to a PIN-based optical receiver. As happened in the other proposed schemes, the security is based on the secrets known only by Alice: the mean photon numbers of the coherent and thermal states, the polarization codification and the value of $\phi_{1\omega}$. Without knowing $\phi_{1\omega}$ and where the coherent state is, Eve cannot get any useful information. Bob's analog signal appears in the PIN photocurrent.

In order to show that the analog signal carried by a weak coherent state can be recovered by a PIN-based optical receiver, we implemented a Mach-Zehnder interferometer (MZI) with a phase modulator in one of the arms and a PIN detector plugged at one of the MZI outputs. The scheme is shown in Fig. 4.

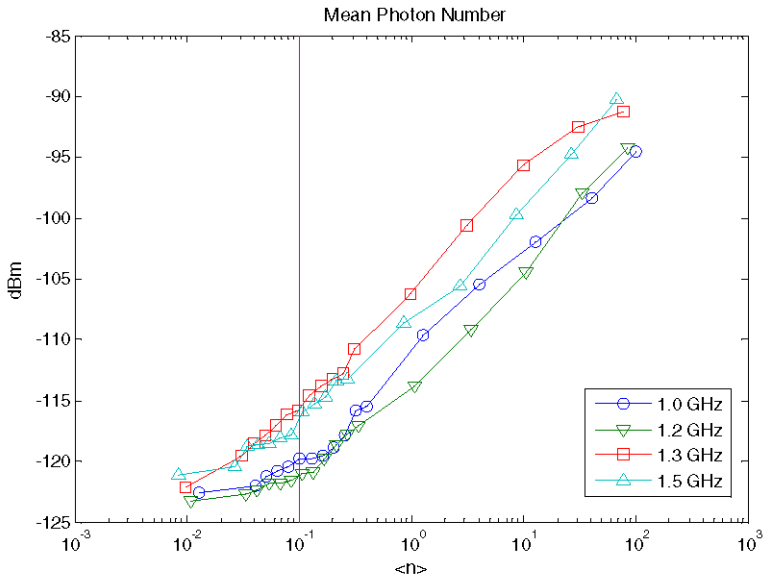


Fig. 5 Electrical power measured with the spectrum analyzer versus mean photon number of the attenuated coherent state

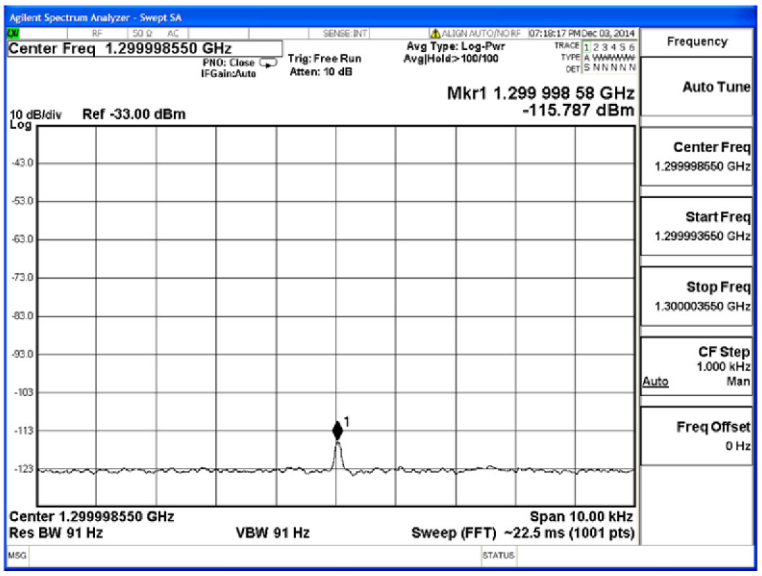


Fig. 6 Measurement of the 1.3 GHz modulating signal carried in an optical signal with mean photon number $\sim 0.1/\text{ns}$

The analog signal source used was a sinusoidal signal produced by a signal generator. The electrical power of the signal measured in the spectrum analyzer versus mean photon number of the attenuated coherent state can be seen in Fig. 5. Four different frequencies were used: 1, 1.2, 1.3 and 1.5 GHz.

Figure 6, by its turn, shows the screen of the spectrum analyzer when the signal generator is working at 1.3 GHz and the mean (flux) photon number of the attenuated coherent state is $\sim 0.1/\text{ns}$.

5 Conclusions

In conclusion, the present work showed three schemes for QSDC feasible with current technology. The security of the schemes is guaranteed by the use of a secret frequency-dependent phase modulation applied only by Alice, the use of thermal states and an embedded QKD protocol running in parallel. There a number of security issues that should be taken into account. For example, beam splitter, intercept-resend and photon number splitting attack are not useful in the schemes with thermal states just because the eavesdroper (Eve) does not know where the coherent state is and she cannot discriminate unambiguously between coherent and thermal states. The trojan horse attack where Eve sends pulses to Bob does not work because Eve does not know which quantum state to send to Bob in order to do not alter his measurement in the spectrum analyzer. At the same time, Eve cannot estimate the mean photon number and the spectrum distribution of the pulses sent by Alice since, once more, she does not know where the coherent state is. At last, Eve's attack will cause errors in the QSCD and QKD protocols what makes her detection easier.

Acknowledgments This work was supported by the Brazilian agencies CAPES and CNPq via Grant no. 303514/2008-6. Also, this work was performed as part of the Brazilian National Institute of Science and Technology for Quantum Information.

References

1. Bennett, C. H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India 175 (1984)
2. Ekert, A.K.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. **67**(6), 661 (1991)
3. Namekata, N., Fuji, G., Inoue, S., Honjo, T., Takesue, H.: Differential phase shift quantum key distribution using single-photon detectors based on a sinusoidally gated InGaAs/InP avalanche photodiode. Appl. Phys. Lett. **91**, 011112 (2007)
4. Lo, H.-K., Zhao, Y.: Quantum cryptography. In: Meyers, R.A. (ed.) Computational Complexity, pp. 2453–2477. Springer, New York (2012)
5. Liu, Z., Chen, H., Liu, W., Xu, J., Wang, D., Li, Z.: Quantum secure direct communication with optimal quantum superdense coding by using general four-qubit states. Quant. Inf. Process. **12**(1), 587 (2013)
6. Chang, Y., Xu, C.-X., Zhang, S.-B., Yan, L.-L.: Quantum secure direct communication and authentication protocol with single photons. Chin. Sci. Bull. **58**(36), 4571 (2013)
7. Wang, C., Hao, L., Song, S.Y., Long, G.L.: Quantum direct communication based on quantum search algorithm. Int. J. Quant. Inf. **8**(3), 443 (2010)
8. Long, G.L., Liu, X.S.: Theoretically efficient high-capacity quantum-key-distribution scheme. Phys. Rev. A **65**, 032302 (2002)
9. Deng, F.-G., Long, G.-L., Liu, X.-S.: Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys. Rev. A **68**, 042317 (2003)
10. Mendonca, F.A., de Brito, D.B., Ramos, R.V.: An optical scheme for quantum multi-service network. Quant. Inf. Comp. **12**(7&8), 620 (2012)
11. Santos, D.J., Loudon, R., Fraile-Peláez, F.J.: Continuum states and fields in quantum optics. Am. J. Phys. **65**, 126 (1997)

12. Ramos, R.V., Souza, R.F.: Simulations of continuum coherent states and its use in quantum cryptographic systems. J. Mod. Opt. **48**(6), 989 (2001)
13. Cavalcanti, M.D.S., Mendonça, F.A., Ramos, R.V.: Spectral method for characterization of avalanche photodiode working as single-photon detector. Opt. Lett. **36**(17), 3446 (2011)
14. Inoue, K., Iwai, Y.: Differential-quadrature-phase-shift quantum key distribution. Phys. Rev. A **79**, 022319 (2009)
15. Kawakami, S., Sasaki, T., Koashi, M.: Security of differential quadrature phase shift quantum key distribution, xxx.lanl.gov 1512.08129v2 (2015). http://arxiv.org/pdf/1512.08129v2.pdf
16. Pinheiro, P.V.P., Ramos, R.V.: Two-layer quantum key distribution. Quant. Inf. Process. **14**(6), 2111 (2015)

ANEXO B - 2º ARTIGO DECORRENTE DA TESE

QUANTUM COMMUNICATION WITH CONTINUUM SINGLE-PHOTON, TWO-PHOTON AND COHERENT STATES

F. FRANKLIN S. RIOS[a]
Department of Teleinformatic Engineering, Federal University of Ceará - DETI/UFC, C.P. 6007 Campus do Pici Fortaleza, Ceará - 60455-970, Brazil.

A. GEOVAN DE A. H. GUERRA[b]
Quantum Information Group, Lab. of Quantum Information Technology, C.P. 6007 Campus do Pici Fortaleza, Ceará - 60455-970, Brazil.

Received August 16, 2016
Revised September 28, 2017

In this work, we analyze the behavior of continuum single-photon, two-photon and coherent states in some quantum communication schemes. In particular, we consider the single-photon in a Mach-Zenhder interferometer, the Hong-Ou-Mandel interference, the quantum bit commitment protocol and a new protocol for secure transmission of sampled analog signals. Furthermore, it is shown an equation for estimating the spectral distri-

Keywords: Continuum light states, Two-photon interference and Quantum bit commitment
Communicated by: I Cirac & G Milburn

1 Introduction

Since the beginning of the quantum information era several quantum tasks using single-photon, entangled two-photon and coherent states have been proposed. For example, the single-photon interference is a crucial tool for experimental realization of quantum communication, quantum computation and quantum metrology schemes. Teleportation requires two-photon entangled states while several quantum key distribution setups use weak coherent states. However, in general, their descriptions are based on single-frequency optical pulses. Usually, the single-photon interference is analyzed as if the photons were produced by a single-frequency optical source, their propagation in optical fibers was free of dispersive effects and the behavior of the optical devices, like beam splitters, polarization rotators and phase modulators, were not frequency-dependent. These are, obviously, simplifications of

[a]frfranklin.rios@gmail.com
[b]geovanguerra@gmail.com
[c]rubens.viana@pq.cnpq.br

the real situation. A single-frequency source would violate the Heisenberg uncertainty principle and, hence, it does not exist. Moreover, optical devices are made of glass and the refractive index is frequency dependent. For example, the photon propagation in dispersive optical fibers results in an additional phase term of the type ($\beta L + 1/2\beta_2\omega^2 L - 1/6\beta_3\omega^3 L$) [1] where β is the constant of propagation, β_2 is the group velocity dispersion (GVD), β_3 is the third order dispersion (usually considered when $\beta_2 \sim 0$) and L is the fiber's length propagated. Furthermore, real beam splitters, polarization rotators and phase modulators are frequency-dependent devices. Hence, a more realistic analysis of quantum communication schemes requires the consideration of continuum fields [2]. In this direction, the present work discusses the use of continuum optical fields in some quantum optical setups and quantum communication protocols. In particular, the spectral distribution of single-photons produced by a heralded single-photon source using four-wave mixing in optical fibers is analyzed and an optical setup for secure transmission of sampled analog states is presented, as well we discuss the security of quantum bit commitment when continuum entangled two-photon states are used. This work is outlined as follows: In Section 2 the discretization of the continuum single-photon state is reviewed. Following, the single-photon interference, the two-photon interference (HOM experiment) and the single-photon propagation in a birefringent channel are discussed. In Section 3 the discussion of the spectral width of the single-photons produced by four-wave mixing in optical fibers is presented. In Section 4 the security of quantum bit commitment protocol using continuum two-photon entangled states is considered. In Section 5, an optical setup for secure transmission of sampled analog signals is described and the conclusions are drawn in Section 6.

2 Quantum communication with continuum single-photon state

In this section, we consider the effect of the spectral width of single-photons in three situations: single-photon interference, interference between two single-photons coming from different sources (Hong-Ou-Mandel experiment) and single-photon propagation in a birefringent channel. The single-photon continuum state is given by [2]

$$|1_\omega\rangle = \int_0^\infty \sigma(\omega)\hat{a}^+(\omega)d\omega\,|0_\omega\rangle \tag{1}$$

$$\int_0^\infty |\sigma(\omega)|^2\,d\omega = 1 \tag{2}$$

The state $|0_\omega\rangle$ is the continuum vacuum state and, hence, $\hat{a}(\omega)\,|0_\omega\rangle = 0$, where $\hat{a}(\omega)$ is the continuum annihilation operator. Furthermore, $|\sigma(\omega)|^2$ gives the probability of the frequency of the photon to belong to the interval $(\omega, \omega + d\omega)$. In order to work with the continuum single-photon in quantum communication schemes, we firstly make its discretization. Let us start by writing $\sigma(\omega)$ in the basis of sinc functions (the discretization using the sinc functions makes easier the calculation of the important probabilities considered in the error rate and security analysis) [3]:

$$\sigma(\omega) = \sum_{k=-\infty}^{\infty} \sigma(k\omega_s)\mathrm{sinc}[(\omega - k\omega_s)/\omega_s] \tag{3}$$

$$\mathrm{sinc}(x) = \sin(\pi x)/\pi x \tag{4}$$

In (3) ω_s is the step of discretization in the frequency domain. Thus, $\sigma(k\omega_s)$ is the value of $\sigma(\omega)$ in $\omega = k\omega_s$ where k is an integer number. Using the orthogonality of the sinc function,

$$\frac{1}{\omega_s}\int_{-\infty}^{\infty} \operatorname{sinc}\left[\frac{(\omega - k\omega_s)}{\omega_s}\right] \operatorname{sinc}\left[\frac{(\omega - m\omega_s)}{\omega_s}\right] d\omega = \delta_{km} \tag{5}$$

and the fact that $\sigma(\omega)$ zero for negative frequencies, one has that

$$\int_0^{\infty} |\sigma(\omega)|^2 \, d\omega = \int_{-\infty}^{\infty} |\sigma(\omega)|^2 \, d\omega = \sum_{k=1}^{\infty} |\sigma(k\omega_s)|^2 \, \omega_s = 1 \tag{6}$$

Equation (6) shows us how to make discrete the continuum single-photon state:

$$|1_\omega\rangle = \sum_{k=1}^{\infty} \sigma(k\omega_s)\sqrt{\omega_s}\, |0\rangle_1 \otimes \cdots \otimes |1\rangle_k \otimes \cdots \tag{7}$$

According to (7), the continuum single-photon state can be approximated by a superposition of the tensor product of discrete oscillators. Each discrete oscillator works in a single-frequency. For example, the state $|0\rangle_1 \otimes \cdots \otimes |1\rangle_k \otimes \cdots$ means one photon in the frequency $k\omega_s$ and zero photons in the other frequencies. The number of discrete oscillators is equal to the number of samples of $\sigma(\omega)$ and the amplitude of probability of k-th term in the superposition is given by $\sigma(k\omega_s)(\omega_s)^{1/2}$. Now, if $\sigma(\omega)$ vanishes for $\omega > N\omega_s$, then one has just a finite number of oscillators:

$$|1_\omega\rangle = \sum_{k=1}^{N} \sigma(k\omega_s)\sqrt{\omega_s}\, |\tilde{1}\rangle_k \tag{8}$$

$$|\tilde{1}\rangle_k = |0\rangle_1 \otimes \cdots \otimes |1\rangle_k \otimes \cdots \otimes |0\rangle_N \tag{9}$$

Now, in order to study the single-photon interference, we will consider the behavior of the quantum state given in (8) in a Mach-Zehnder interferometer (MZI) whose phase modulators are frequency-dependent (to include the frequency dependence of the beam splitters is just an algebra exercise). The MZI is composed by two lossless beam-splitters having transmittance $T = 1/2^{1/2}$(and reflectance $R = i1/2^{1/2}$), and one phase modulator in each arm, $\phi_A(\omega)$ and $\phi_B(\omega)$. Such interferometer is useful in quantum key distribution (QKD) setups. The input state is $|\, 1_\omega\rangle \, |\, 0_\omega\rangle$. The scheme is shown in Fig.1.

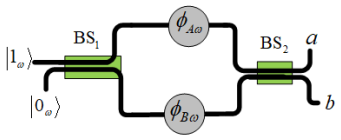


Fig. 1. Mach-Zehnder interferometer with lossless balanced beam splitters and frequency-dependent phase modulators ($\phi_{A\omega} \rightarrow \phi_A(\omega)$,$\phi_{B\omega} \rightarrow \phi_B(\omega)$).

After some algebra one gets the following total quantum state at the interferometer output

$$|\psi_\omega\rangle = \sum_{k=1}^{N} \sigma\left(k\omega_s\right)\sqrt{\omega_s}|0\rangle_1|0\rangle_1 \otimes ... \otimes |\xi_\omega\rangle_k \otimes ... \otimes |0\rangle_N|0\rangle_N \tag{10}$$

$$|\xi_\omega\rangle_k = ie^{i\Omega_k}\left\{\cos\left(\Delta_k\right)|1\rangle_k^a|0\rangle_k^b + \sin\left(\Delta_k\right)|0\rangle_k^a|1\rangle_k^b\right\} \tag{11}$$

$$\Omega_k = \left[\phi_A\left(k\omega_s\right) + \phi_B\left(k\omega_s\right)\right]/2;\ \Delta_k = \left[\phi_A\left(k\omega_s\right) - \phi_B\left(k\omega_s\right)\right]/2. \tag{12}$$

Hence, the probabilities of the photon to emerge at the outputs a and b of the interferometer are given by

$$p_a = \sum_{k=1}^{N} \cos^2\left[\frac{\phi_A(k\omega_s)-\phi_B(k\omega_s)}{2}\right]\left|\sigma\left(k\omega_s\right)\right|^2\omega_s \tag{13}$$

$$p_b = \sum_{k=1}^{N} \sin^2\left[\frac{\phi_A(k\omega_s)-\phi_B(k\omega_s)}{2}\right]\left|\sigma\left(k\omega_s\right)\right|^2\omega_s \tag{14}$$

or, returning to the continuous case,

$$p_a = \int_0^\infty \cos^2\left[\frac{\phi_A(\omega)-\phi_B(\omega)}{2}\right]\left|\sigma\left(\omega\right)\right|^2 d\omega \tag{15}$$

$$p_b = \int_0^\infty \sin^2\left[\frac{\phi_A(\omega)-\phi_B(\omega)}{2}\right]\left|\sigma\left(\omega\right)\right|^2 d\omega. \tag{16}$$

Observing (15)-(16) one sees that the frequency-dependence can increase the error rate of a QKD protocol (this error can be taken into account through the visibility of the interferometer) or it can be designedly used to increase the security of a quantum cryptographic protocol.

Now, let us consider the HOM experiment, the interference between two continuum single-photon pulses, coming from different single-photon sources, impinging in a beam splitter at the same time and with the same polarization. The total state at the beam splitter's output is

$$\left[U_{BS}|1_\omega\rangle|1_\omega\rangle = U_{BS}\left(\sum_{k=1}^{N}\sigma\left(k\omega_s\right)\sqrt{\omega_s}|\tilde{1}\rangle_k\right)\otimes\left(\sum_{l=1}^{N}\xi\left(l\omega_s\right)\sqrt{\omega_s}|\tilde{1}\rangle_l\right) = \sum_{k,l=1}^{N}\sigma\left(k\omega_s\right)\xi\left(l\omega_s\right)\omega_s U_{BS}|\tilde{1}\rangle_k|\tilde{1}\rangle_l\right. \tag{17}$$

In (17) $U_{BS}(\omega)$ is the unitary operation of the frequency-dependent beam splitter. Its transmittance and reflectance are, respectively, $\cos(\theta(\omega))$ and $i\sin(\theta(\omega))$. Thus,

$$U_{BS}|\tilde{1}\rangle_k|\tilde{1}\rangle_l = \begin{cases} |0\rangle_1^a|0\rangle_1^b \otimes ... \otimes |\mu\rangle_k \otimes ... \otimes |\mu\rangle_l \otimes ... \otimes |0\rangle_N^a|0\rangle_N^b & \text{if } k \neq l \\ |0\rangle_1^a|0\rangle_1^b \otimes ... \otimes |\lambda\rangle_k \otimes ... \otimes |0\rangle_N^a|0\rangle_N^b & \text{if } k = l \end{cases} \tag{18}$$

$$|\mu\rangle_{r=k,l} = \cos\left(\theta\left(r\omega_s\right)\right)|1\rangle_r^a|0\rangle_r^b + i\sin\left(\theta\left(r\omega_s\right)\right)|0\rangle_r^a|1\rangle_r^b \tag{19}$$

$$|\lambda\rangle_k = \sin\left(2\theta\left(k\omega_s\right)\right)\frac{|2\rangle_k^a|0\rangle_k^b + |0\rangle_k^a|2\rangle_k^b}{\sqrt{2}} + i\cos\left(2\theta\left(k\omega_s\right)\right)|1\rangle_k^a|1\rangle_k^b \tag{20}$$

In (18)-(20) a and b are the beam splitter's output modes. Using (17)-(20), one gets the coincidence probability

$$p_{coin} = \sum_{\substack{k,l=1 \\ k\neq l}}^{N} |\sigma\left(k\omega_s\right)\xi\left(l\omega_s\right)|^2\omega_s^2\left[\cos^2\left(\theta\left(k\omega_s\right)\right)\cos^2\left(\theta\left(l\omega_s\right)\right) + \sin^2\left(\theta\left(k\omega_s\right)\right)\sin^2\left(\theta\left(l\omega_s\right)\right)\right]$$
$$+\sum_{k=1}^{N}|\sigma\left(k\omega_s\right)\xi\left(k\omega_s\right)|^2\omega_s^2\cos^2\left(2\theta\left(k\omega_s\right)\right) \tag{21}$$

If the beam splitter is not frequency-dependent and balanced ($\theta = \pi/4$) (21) reduces to

$$p_{coin} = \frac{1}{2} - \frac{1}{2}\sum_{k=1}^{N}|\sigma\left(k\omega_s\right)\xi\left(k\omega_s\right)|^2\omega_s^2 \tag{22}$$

or, returning to the continuous case,

$$p_{coin} = \frac{1}{2} - \frac{1}{2}\int\int_D |\sigma\left(\omega_1\right)|^2|\xi\left(\omega_2\right)|^2 d\omega_1 d\omega_2 \tag{23}$$

where $D = \{(\omega_1,\omega_2) \in \mathrm{R}^2{}_{\geq 0} : \omega_1 = \omega_2\}$. As one may note in (22)-(23), the coincidence probability will be zero only when the spectral distributions are $\sigma(\omega) = \xi(\omega) = \delta(\omega\text{-}\omega_0)$, that is, both photons having the same single-frequency ω_0 (and zero spectral width). This happens because, due to the spectral distribution, one cannot guarantee that both photons will be in the same frequency, even if they have the same spectral distributions. On the other hand, the coincidence probability is equal to 1/2 only when the spectral distributions of the photons do not have any overlap. However, in practice, if frequency information cannot be gained by the detectors used in the experiment, that is, if the detectors' bandwidth is wider than photons spectral distribution, then photons with different frequencies become indistinguishable and a perfect Hong-Ou-Mandel interference can be achieved.

At last, we consider the continuum single-photon light propagating in a frequency-dependent phase-damping channel as discussed in [4, 5]. Initially, at the channel's input, the quantum state is

$$|\psi\rangle = |1_\omega\rangle \otimes (a|H\rangle + b|V\rangle) = \sum_{k=1}^{N}\sigma\left(k\omega_s\right)\sqrt{\omega_s}|\tilde{1}\rangle_k \otimes (a|H\rangle + b|V\rangle) \tag{24}$$

Therefore, for the initial state frequency and polarization are not entangled. The channel's propagation effect is modeled by the unitary operator $U(\omega) = \lambda_H(\omega)|H\rangle\langle H| + \lambda_V(\omega)|V\rangle\langle V|$ (*H*

and V mean, respectively, horizontal and vertical modes, the eigenvalues depend on the frequency while the eigenstates are constant). Hence, the state at channel's output is

$$|\psi_{out}\rangle = \sum_{k=1}^{N} \sigma(k\omega_s)\sqrt{\omega_s}|\tilde{1}\rangle_k U(a|H\rangle + b|V\rangle) = \sum_{k=1}^{N} \sigma(k\omega_s)\sqrt{\omega_s}|\tilde{1}\rangle_k (a\lambda_H(k\omega_s)|H\rangle + b\lambda_V(k\omega_s)|V\rangle) \quad (25)$$

$$\rho = |\psi_{out}\rangle\langle\psi_{out}| = \sum_{k,l=1}^{N} \sigma(k\omega_s)\sigma^*(l\omega_s)\omega_s|\tilde{1}\rangle_k{}_l\langle\tilde{1}| \otimes \begin{pmatrix} |a|^2 \lambda_H(k\omega_s)(\lambda_H(l\omega_s))^* |H\rangle\langle H| \\ +|b|^2 \lambda_V(k\omega_s)(\lambda_V(l\omega_s))^* |V\rangle\langle V| \\ +ab^* \lambda_H(k\omega_s)(\lambda_V(l\omega_s))^* |H\rangle\langle V| \\ +a^* b(\lambda_H(l\omega_s))^* \lambda_V(k\omega_s)|V\rangle\langle H| \end{pmatrix} \quad (26)$$

In order to get only the polarization information, the frequency variable is traced out in (26). Using $Tr_\omega(|\tilde{1}\rangle_k{}_l\langle\tilde{1}|) = {}_l\langle\tilde{1} \mid \tilde{1}\rangle_k = \delta_{kl}$ and (6) one gets for the final output state

$$\rho = \begin{bmatrix} |a|^2 & ab^* \sum_{k=1}^{N} |\sigma(k\omega_s)|^2 \omega_s \lambda_H(k\omega_s)(\lambda_V(k\omega_s))^* \\ a^* b \sum_{k=1}^{N} |\sigma(k\omega_s)|^2 \omega_s (\lambda_H(k\omega_s))^* \lambda_V(k\omega_s) & |b|^2 \end{bmatrix} \quad (27)$$

For this birefringent channel, one has eigenvalues of the form

$$\lambda_{H,V}(k\omega_s) = e^{i\left(\frac{n_{H,V} k\omega_s L}{c}\right)}, \quad (28)$$

where $n_{H,V}$ are the refractive index in the orthogonal directions, c is the light velocity and L is the channel's length. The fidelity between the input and output state is given by

$$F = \langle\psi|\rho|\psi\rangle = |a|^4 + |b|^4 + 2|a|^2|b|^2 \sum_{k=1}^{N} |\sigma(k\omega_s)|^2 \omega_s \cos\left(\frac{n_H - n_V}{c} k\omega_s L\right) \quad (29)$$

or, returning to the continuous case,

$$F = |a|^4 + |b|^4 + 2|a|^2|b|^2 \int_0^\infty |\sigma(\omega)|^2 \cos\left(\frac{n_H - n_V}{c}\omega L\right) d\omega. \quad (30)$$

As expected, if the medium is not birefringent, $n_H = n_V$, then $F = 1$. In order to gain some physical insight, let us consider the simple case of a rectangular spectrum with width $\Delta\omega$ and centered in the frequency ω_0: $\sigma(\omega) = \sigma_0$in the interval $[\omega_0$ - $\Delta\omega/2$, $\omega_0 + \Delta\omega/2]$ and zero otherwise. In this case, the fidelity is simply given by

$$F = |a|^4 + |b|^4 + 2|a|^2|b|^2 \frac{2c}{(n_H - n_V)L} \sin\left(\frac{(n_H - n_V)L}{c}\frac{\Delta\omega}{2}\right) \cos\left(\frac{(n_H - n_V)L}{c}\omega_0\right). \quad (31)$$

One may note that, if $|\psi\rangle = (|H\rangle + |V\rangle)/2^{1/2}$, then F =1/2 when $L = 2c\pi/[(n_H - n_V)\Delta\omega]$. As expected, the shorter the spectral width the longer the photon can travel. In Fig. 2 one can see the variation of F versus L for an input state with a Gaussian spectrum having ω_0= $8.3.10^{14}$ [rad/s] (λ = 1550 nm) and $\Delta\omega = 1.33.10^{10}$ [rad/s]. The other parameters values are $n_H = 1.46$, $n_V = 1.465$.

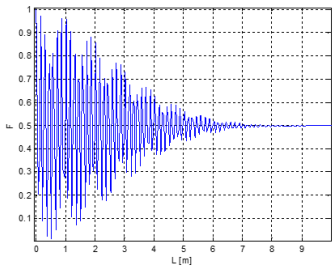


Fig. 2. Fidelity given by Eq. (31) versus channel's length L. Input state $(|H\rangle + |V\rangle)/2^{1/2}$ and Gaussian spectrum.

As one can notice in Fig. 2 the birefringence is very harmful for quantum states that are superposition of $|H\rangle$ and $|V\rangle$. On the other hand, since the channel considered is a phase damping channel, the input states $|H\rangle$ and $|V\rangle$ do not suffer any kind of perturbation ($F = 1$).

3 Spectral distribution of a single-photon produced by a four-wave mixing-based two-photon Source

The two-photon states are mostly produced by parametric down conversion and spontaneous or stimulated four-wave mixing in optical fibers. Thus, the frequencies of the created photons have to obey the energy conservation law. For the four-wave mixing, for example, two photons from the pump beam (ω_p) are annihilated while two new photons, named signal (ω_{sig}) and idler (ω_{id}), are created. The relation $2\omega_p$=ω_{sig}+ω_{id} must be obeyed. For this case, the signal and idler annihilation ($\hat{a}_s, \hat{a}_i$) and creator $\left(\hat{a}_s^\dagger, \hat{a}_i^\dagger\right)$ operators are governed by the following coupled differential equations [1, 6]

$$\frac{d\hat{a}_s}{dz} = i\left(\delta/2\right)\hat{a}_s + 2i\gamma A_p^2 \hat{a}_i^\dagger \tag{32}$$

$$\frac{d\hat{a}_i}{dz} = i\left(\delta/2\right)\hat{a}_i + 2i\gamma A_p^2 \hat{a}_s^\dagger. \tag{33}$$

In (32)-(33), z is the spatial coordinate, γ is the fiber nonlinearity coefficient, A_p^2 is the pump power and δ is the phase mismatch given by

$$\delta = \beta\left(\omega_{sig}\right) + \beta\left(\omega_{id}\right) - 2\beta\left(\omega_p\right) + 2\gamma A_p^2. \tag{34}$$

The equations (32)-(33) do not take into account the spontaneous Raman scattering (SRS) [7]. In practice, the SRS is reduced by choosing ω_{sig}- ω_i far from $2\pi\cdot$13THz [8] or cooling the fiber in order to decrease the phonon population [9]. The solutions of (32)-(33) are [1, 6]

$$\hat{a}_s\left(z\right) = k_1 \hat{a}_s\left(0\right) + k_2 \hat{a}_i^\dagger\left(0\right) \tag{35}$$

$$\hat{a}_i(z) = k_1 \hat{a}_i(0) + k_2 \hat{a}_s^{\dagger}(0) \tag{36}$$

$$k_1 = \cosh(gz) + (i\delta/2g)\sinh(gz) \tag{37}$$

$$k_2 = i(\gamma/g) A_p^2 \sinh(gz) \tag{38}$$

$$g = \sqrt{\gamma^2 A_p^4 - \delta^2/4}. \tag{39}$$

The two-photon source, in practice, can produce multiphoton pulses. Hence, the quantum state produced is of the form $|\psi\rangle = \sum_n c_n |n,n\rangle$, having equal individual states $\rho = \sum_n |c_n|^2 |n\rangle\langle n|$. The photon number distribution of the signal and idler modes are equal to [10]

$$p_n = \frac{2}{(\Delta k_+ + 1)} \left[\frac{(\Delta k_+ - 1)}{(\Delta k_+ + 1)}\right]^n \tag{40}$$

$$\Delta k_+ = \left(|k_1|^2 + |k_2|^2\right) = \cosh^2(gz) + \left[\frac{\delta^2}{4g^2} + \frac{\gamma^2}{g^2} A_p^4\right] \sinh^2(gz). \tag{41}$$

Considering that the idler mode is detected by an ideal photon counter, the single-photon state at the signal mode (conditioned to single-photon detection in the idler mode and for a monochromatic pump field) is given by $\prod_a^b$

$$|1_\omega\rangle = \sum_{k=1}^{N} \sigma(k\omega_s) \sqrt{\omega_s} |\tilde{1}\rangle_k = \sum_{k=1}^{N} \left[\frac{p_1(k\omega_s) \prod_{\substack{l=1 \\ l\neq k}}^{N} p_0(l\omega_s)}{\sum_{k=1}^{N} p_1(k\omega_s) \prod_{\substack{l=1 \\ l\neq k}}^{N} p_0(l\omega_s)}\right]^{1/2} |\tilde{1}\rangle_k \tag{42}$$

$$N\omega_s = \omega_p - \omega_s \tag{43}$$

where, according to (40),

$$p_0(k\omega_s) = \frac{2}{(\Delta k_+ + 1)} \tag{44}$$

$$p_1(k\omega_s) = \frac{2}{(\Delta k_+ + 1)} \left[\frac{(\Delta k_+ - 1)}{(\Delta k_+ + 1)}\right]. \tag{45}$$

Furthermore, the phase mismatch is

$$\delta = \beta(k\omega_s) + \beta([2(N+1) - k]\omega_s) - 2\beta((N+1)\omega_s) + 2\gamma A_p^2. \tag{46}$$

According to (41)-(46), δ plays a crucial role in the spectral width of the single-photon state produced by a heralded single-photon source using four-wave mixing in optical fiber. Without knowing the formula of $\beta(\omega)$ is not possible to go beyond, however, one can clearly see that the optical power of the pump beam is important not only to keep small the amount of multiphoton pulses ($\gamma A_p^2 L_f << 1$), but it also has implications on the spectral width of the generated single-photon pulses: The variation of A_p^2 makes a variation in Δk_+ that, by its turn, changes p_0 and p_1 in (42).

4 Quantum bit commitment using continuum two-photon states

Now, let us consider the implications of continuum states in the quantum bit commitment (QBC) protocol. It has been shown that QBC protocols without any restriction cannot be unconditionally secure [11]. Attempts of producing unconditional QBC protocols with some restrictions have been proposed [12, 13]. Here, we consider the Lo-Chau's QBC protocol (LC-QBC) from a practical point of view, aiming to show that, at least in principle, Alice's cheating strategy may be noticed by Bob with a probability larger than zero. The practical conditions considered are: the entangled photons have a spectral distribution and the quantum gates are frequency-dependent. The LC-QBC protocol can be explained in the following way: Alice and Bob agree that the states $|0_L\rangle = (|00\rangle+|11\rangle)/2^{1/2}$ and $|1_L\rangle = (|01\rangle+|10\rangle)/2^{1/2}$ represent, respectively, the logical bits '0' and '1'. In the commitment stage, Alice prepares the state $|0_L\rangle$ and she sends the second qubit to Bob. In the unveil stage two situations are possible: 1) Alice decides to keep the choice '0'. She measures her qubit using the $\{|0\rangle,|1\rangle\}$ basis and informs to Bob the values of the bit committed ('0') and the result of her measurement. Bob, by his turn, measures his qubit in the same basis and compares the result with that one announced by Alice. If the results of the measurements are the same, Bob thinks that Alice acted honestly. 2) Alice changes her mind and decides to unveil the value '1'. She applies the NOT gate X and realizes a measurement in her qubit. Alice informs to Bob the values of the bit committed ('1') and the result of her measurement. Bob, by his turn, measures his qubit and compares the result with that one announced by Alice. If the measurement results are different, Bob thinks that Alice acted honestly. Since Alice can always change from '0' to '1' (by applying the X gate in her qubit) without being noticed, she can always cheat Bob with zero probability of being caught cheating. This scenario changes when we consider real entangled states whose photons have non-zero spectral width. Let us consider that Alice and Bob will run the LC-QBC protocol using the following entangled state

$$|0_L\rangle = \int_0^\infty d\Omega\sigma\left(\Omega\right)\frac{|\omega_0+\Omega,\omega_0-\Omega\rangle_{HH}+|\omega_0+\Omega,\omega_0-\Omega\rangle_{VV}}{\sqrt{2}}. \tag{47}$$

The discretization of the state (47) using (3)-6 is

$$|0_L\rangle = \sum_{\substack{k,l=1\\k+l=M}}^{N} \sigma\left(k\omega_s,l\omega_s\right)\sqrt{\omega_s}\left[\frac{|\tilde{1}\rangle_k^H|\tilde{1}\rangle_l^H+|\tilde{1}\rangle_k^V|\tilde{1}\rangle_l^V}{\sqrt{2}}\right]. \tag{48}$$

$$M\omega_s = 2\omega_0. \tag{49}$$

According to (48), with probability $|\sigma(k\omega_s,l\omega_s)|^2\omega_s$ the photons in the frequencies $k\omega_s$ and $l\omega_s$ ($k\omega_s + l\omega_s = M\omega_s = 2\omega_0$) are in the entangled state $(|HH\rangle+|VV\rangle)/2^{1/2}$. The NOT gate, by its turn, is a frequency-dependent polarization rotator. It is represented by $R[\theta(\omega)]$, where $\theta(\omega_c) = \pi/2$ in the central frequency ω_c. When Alice tries to cheat applying $R[\theta(\omega)]$, she produces the quantum state

$$R\left[\theta\left(\omega\right)\right]\left|0_L\right\rangle = \sum_{\substack{k,l=1 \\ k+l=M}}^{N} \sigma\left(k\omega_s, l\omega_s\right)\sqrt{\omega_s} \times \left[\begin{array}{l} \cos\left[\theta\left(k\omega_s\right)\right]\frac{\left(\left|\tilde{1}\right\rangle_k^H\left|\tilde{1}\right\rangle_l^H - \left|\tilde{1}\right\rangle_k^V\left|\tilde{1}\right\rangle_l^V\right)}{\sqrt{2}} \\ +\sin\left[\theta\left(k\omega_s\right)\right]\frac{\left(\left|\tilde{1}\right\rangle_k^V\left|\tilde{1}\right\rangle_l^H + \left|\tilde{1}\right\rangle_k^H\left|\tilde{1}\right\rangle_l^V\right)}{\sqrt{2}} \end{array}\right]. \quad (50)$$

An error in Bob denouncing Alice's cheating strategy will occur when Alice informs that she chose bit '1' and Bob gets in his measurement the same result as Alice got in her measurement. Using the state in (50) one gets the following error probability

$$PE = \sum_{\substack{k,l=1 \\ k+l=M}}^{N} \left|\sigma\left(k\omega_s, l\omega_s\right)\right|^2 \cos^2\left[\theta\left(k\omega_s\right)\right]\omega_s \quad (51)$$

or, returning to the continuum case,

$$PE = \int_0^\infty d\Omega \left|\sigma\left(\Omega\right)\right|^2 \cos^2\left[\theta\left(\omega_0+\Omega\right)\right]. \quad (52)$$

In (52) it is assumed that Alice (Bob) kept the photon with central frequency ω_0+Ω (ω_0-Ω). Hence, once one takes into account the spectral distribution and the frequency dependence of optical devices, one may note that Alice's strategy may cause an error in Bob, revealing her cheating strategy.

5 Quantum communication using continuum coherent states

Optical schemes for quantum secure direct communication using continuum coherent states have been proposed in [14]. In this section, we describe an optical setup for secure transmission of sampled analog signals using continuum coherent states. However, before describing the optical setup proposed, let us start by describing the continuum coherent state used. It is defined as [2]

$$\left|\alpha_\omega\right\rangle = \exp\left[\int\left[\alpha\left(\omega\right)a^\dagger\left(\omega\right) - \alpha^*\left(\omega\right)a\left(\omega\right)\right]d\omega\right]\left|0_\omega\right\rangle \quad (53)$$

$$\left\langle n\right\rangle = \int_0^\infty \left|\alpha\left(\omega\right)\right|^2 d\omega. \quad (54)$$

In (54) $\left\langle n\right\rangle$ is the mean photon number of the state $\left|\alpha_\omega\right\rangle$, where $\alpha(\omega)$ is the complex amplitude of the field. Now, using (3)-(6) in the discretization of (53) one gets

$$\left|\alpha_\omega\right\rangle = \prod_{k=1}^{N}\left|\alpha\left(k\omega_s\right)\sqrt{\omega_s}\right\rangle. \quad (55)$$

$$\left\langle n\right\rangle = \int_0^\infty \left|\alpha\left(\omega\right)\right|^2 d\omega = \int_{-\infty}^\infty \left|\alpha\left(\omega\right)\right|^2 d\omega = \sum_{k=1}^{N}\left|\alpha\left(k\omega_s\right)\right|^2\omega_s. \quad (56)$$

In (55)-(56) it is considered that $\alpha(\omega)$ vanishes for $\omega > N\omega_s$. Equation (55) shows that the continuum coherent state can be approximated by a tensor product of single-frequency discrete oscillators in coherent states [3]. Due to the decomposition in sinc functions, the number of discrete oscillators is equal to the number of samples taken from the field's envelope. Each discrete oscillator is in a (single-frequency) coherent state and the amplitude of the k-th oscillator is equal to the product of the k-th sample of $\alpha(\omega)$ and the square root of ω_s.

In a Mach-Zehnder interferometer with frequency-dependent phase modulators, the mean photon numbers at the interferometer's outputs are [14]

$$\langle n_1 \rangle = \sum_{k=1}^{N} |\alpha(k\omega_s)|^2 \cos^2\left(\frac{\phi_A(k\omega_s) - \phi_B(k\omega_s)}{2}\right)\omega_s \tag{57}$$

$$\langle n_2 \rangle = \sum_{k=1}^{N} |\alpha(k\omega_s)|^2 \sin^2\left(\frac{\phi_A(k\omega_s) - \phi_B(k\omega_s)}{2}\right)\omega_s \tag{58}$$

or, returning to the continuous case,

$$\langle n_1 \rangle = \int_0^{\infty} \cos^2\left[\frac{\phi_A(\omega) - \phi_B(\omega)}{2}\right] |\alpha(\omega)|^2 \, d\omega \tag{59}$$

$$\langle n_2 \rangle = \int_0^{\infty} \sin^2\left[\frac{\phi_A(\omega) - \phi_B(\omega)}{2}\right] |\alpha(\omega)|^2 \, d\omega. \tag{60}$$

The optical setup that implements the secure transmission of sampled analog signals scheme is shown in Fig. 3.

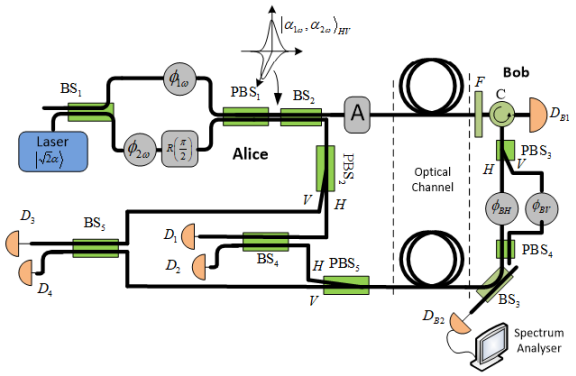


Fig. 3. Optical setup for secure transmission of sampled analog signals. BS – beam splitter, PBS – polarizing beam splitter, C – optical circulator, R – polarization rotator, F – optical filter, D – detector, A – optical attenuator, ϕ - phase modulator and ϕ_ω - frequency-dependent phase modulator.

In Fig. 3, $\phi_{1\omega}$ and $\phi_{2\omega}$ (ϕ_{BH} and ϕ_{BV}) are (not) frequency-dependent phase-modulators while A is an optical attenuator. The filter F avoids a spy (Eve) to use optical signals in a frequency range not seen by Bob's detectors. The circulator C and detector D_{B1} makes the setup one-directional. Light detected in D_{B1} implies the existence of an attack. At last, the set BS_3-D_{B2}-Spectrum analyzer works as a watch-dog avoiding Eve to send strong signals to Bob aiming to read them at the output [15, 16]. As it can be noted, the optical scheme in Fig. 3 uses the frequency-dependent phase modulation, only known by Alice, to hide Bob's phase-modulation. Since the pulse sent by Alice has low mean photon number, Eve cannot determine the functions $\phi_{1\omega}$ and $\phi_{2\omega}$. Considering the beam splitters obey the relation

$$U_{BS}|\xi,\lambda\rangle = \left|\frac{\xi+\lambda}{\sqrt{2}}, \frac{-\xi+\lambda}{\sqrt{2}}\right\rangle, \tag{61}$$

the equations that explain the functioning of the setup in Fig. 3 are the following: The quantum states at PBS_2's and at the channel's inputs are, respectively,

$$\left|\alpha_1 e^{i\phi_1(\omega)}, \alpha_1 e^{i\phi_2(\omega)}\right\rangle_{HV} \tag{62}$$

$$\left|\alpha_2 e^{i\phi_1(\omega)}, \alpha_2 e^{i\phi_2(\omega)}\right\rangle_{HV} \tag{63}$$

$$\alpha_2 = \alpha_1 10^{-\frac{\epsilon[dB]}{10}}. \tag{64}$$

In (64), ϵ (in dB) is the loss of the attenuator A. The total state at Bob' output is

$$\left|\alpha_3 e^{i[\phi_1(\omega)+\phi_{BH}]}, \alpha_3 e^{i[\phi_2(\omega)+\phi_{BV}]}\right\rangle_{HV} \tag{65}$$

$$\alpha_3 = t_B \alpha_2. \tag{66}$$

In (66) t_B is the transmissivity of BS_3. Returning to Alice, the quantum states at beam splitters BS_4 and BS_5 inputs are

$$\left|\alpha_1 e^{i\phi_1(\omega)}, \alpha_3 e^{i[\phi_1(\omega)+\phi_{BH}]}\right\rangle \tag{67}$$

$$\left|\alpha_1 e^{i\phi_2(\omega)}, \alpha_3 e^{i[\phi_2(\omega)+\phi_{BV}]}\right\rangle. \tag{68}$$

Now, using (61), the states at beam splitters BS_4 and BS_5 outputs are

$$\left|\frac{\alpha_1 e^{i\phi_1(\omega)} + \alpha_3 e^{i[\phi_1(\omega)+\phi_{BH}]}}{\sqrt{2}}, \frac{-\alpha_1 e^{i\phi_1(\omega)} + \alpha_3 e^{i[\phi_1(\omega)+\phi_{BH}]}}{\sqrt{2}}\right\rangle_{12} \tag{69}$$

$$\left|\frac{\alpha_1 e^{i\phi_2(\omega)} + \alpha_3 e^{i[\phi_2(\omega)+\phi_{BV}]}}{\sqrt{2}}, \frac{-\alpha_1 e^{i\phi_2(\omega)} + \alpha_3 e^{i[\phi_2(\omega)+\phi_{BV}]}}{\sqrt{2}}\right\rangle_{34}. \tag{70}$$

Hence, the photocurrents in D_1, D_2, D_3 and $D_4$are, respectively,

$$I_{1,2} = R\left[\frac{\alpha_1^2+\alpha_3^2}{2} \pm \alpha_1\alpha_3\cos(\phi_{BH})\right] \tag{71}$$

$$I_{3,4} = R\left[\frac{\alpha_1^2 + \alpha_3^2}{2} \pm \alpha_1\alpha_3 \cos\left(\phi_{BV}\right)\right]. \tag{72}$$

In (71)-(72) R is the responsivity of the detectors. Now, making $I = (I_1\text{-}I_2) + (I_3\text{-}I_4)$ one has

$$I = 2R\alpha_1\alpha_3\left[\cos\left(\phi_{BH}\right) + \cos\left(\phi_{BV}\right)\right]. \tag{73}$$

Here we will assume a sampled analog modulating signal, hence, $\phi_{BH} = mS_H(kT)$ and $\phi_{BV} = mS_V(kT)$, where m ($<<1$) is the modulation index, k is an integer number and T is the time step, equal to the time separation between consecutive optical pulses generated by the laser. Obviously, in order to satisfy the Nyquist theorem, the maximal frequency components of S_H and S_V are lower or equal to $1/(2\,T)$. For a small value of m one has $\cos(\phi_{BH}) \sim 1+\phi_{BH} = 1 + mS_H(kT)$ and, similarly, $\cos(\phi_{BV}) \sim 1 + mS_V\,(kT)$. Substituting these expressions in (73) one finally gets

$$I \approx 2R\alpha_1\alpha_3\left\{2 + m\left[S_H\,(kT) + S_V\,(kT)\right]\right\}. \tag{74}$$

Thus, according to (74), using a low-pass filter, Alice can recover the signal $S(t) = \mathrm{S}_H(t) + S_V(t)$ sent, in a secure way, by Bob.

One may note that, the best that Eve can do is to use a beam splitter with reflectivity equal to the loss between Alice and Bob and to change the fiber between Alice and Bob by a lossless fiber. At Bob's output, Eve uses the same apparatus of Alice. Thus, Eve would get

$$I \approx 2R\alpha_2\alpha_3\left\{2 + m\left[S_H\,(kT) + S_V\,(kT)\right]\right\}. \tag{75}$$

Since $\alpha_2 << \alpha_1$, the signal obtained by Eve would be very weak and not detectable. Furthermore, due to (59)-(60), Eve would not have enough information to reconstruct $\phi_{1\omega}$ and $\phi_{2\omega}$ and to resend the correct state to Alice. At last, the security of the scheme in Fig. 3 can be even improved by the usage of thermal states [14, 16].

6 Conclusions

The present work showed that considering the spectral distribution of single-photons, two-photon entangled states and coherent states is an important issue in the analysis of quantum error rate and security of quantum communication protocols. In fact, a quantum protocol can be considered unconditionally secure or insecure only if all conditions required by physical laws are taken into account in the security analysis, this includes, obviously, the non-zero spectral distribution of the optical pulses and frequency dependence of optical devices. In this direction, the present work provided

(i) Analytical equations for single-photon interference when the phase modulators are frequency-dependents, and two-photon interference (HOM experiment) when the two single-photons at the beam splitters' inputs have different spectral distributions.

(ii) An equation for estimating the spectral distribution of single-photons, produced by a source based on four-wave mixing in optical fibers, versus the optical power of the pump beam.

(iii) A formula for the probability of Alice being caught cheating in a quantum bit commitment protocol realized with entangled photons, when real conditions are considered.
(iv) An optical setup for secure transmission of a sampled analog signal. The spectral width and the frequency-dependence of the phase-modulators were used to provide the security of the system.

Acknowledgements

This work was supported by the Brazilian agencies CAPES and CNPq via Grant no. 307062/2014-7. Also, this work was performed as part of the Brazilian National Institute of Science and Technology for Quantum Information.

References

[1] G. P. Agrawal (2007). *Nonlinear fiber optics*. Academic press.

[2] D. J. Santos, R. Loudon, and F. J. Fraile-Peláez (1997). Continuum states and fields in quantum optics. *American Journal of Physics*, Vol. 65(2), pp. 126–132.

[3] R. V. Ramos and R. F. Souza (2001). Simulations of continuum coherent states and its use in quantum cryptographic systems. *Journal of Modern Optics*, Vol. 48(6), pp. 989–1003.

[4] A. J. Berglund (2000). Quantum coherence and control in one-and two-photon optical systems. *arXiv preprint quant-ph/0010001*.

[5] Y.-X. Gong, Y.-S. Zhang, Y.-L. Dong, X.-L. Niu, Y.-F. Huang, and G.-C. Guo (2008). Dependence of the decoherence of polarization states in phase-damping channels on the frequency spectrum envelope of photons. *Physical Review A*, Vol. 78(4), pp. 042103.

[6] G. Agrawal. *Applications of nonlinear fiber optics*. Academic press, 2007.

[7] Q. Lin, F. Yaman, and G. P. Agrawal (2006). Photon-pair generation by four-wave mixing in optical fibers. *Optics letters*, Vol. 31(9), pp. 1286–1288.

[8] X. Li, J. Chen, P. Voss, J. Sharping, and P. Kumar (2004). All-fiber photon-pair source for quantum communications: Improved generation of correlated photons. *Optics express*, Vol. 12(16), pp. 3737–3744.

[9] H. Takesue and K. Inoue (2005). 1.5-μm band quantum-correlated photon pair generation in dispersion-shifted fiber: suppression of noise photons by cooling fiber. *Optics express*, Vol 13(20), pp. 7832–7839.

[10] D. B. de Brito and R. V. Ramos (2010). Analysis of heralded single-photon source using four-wave mixing in optical fibers via wigner function and its use in quantum key distribution. *IEEE Journal of Quantum Electronics*, Vol. 46(5), pp. 721–727, 2010.

[11] H.-K. Lo and H. F. Chau (1997). Is quantum bit commitment really possible? *Physical Review Letters*, Vol. 78(17) pp. 3410.

[12] H. P. Yuen (2003). How to build unconditionally secure quantum bit commitment protocols. *arXiv preprint quant-ph/0305144*.

[13] G. Murta, M. T. Cunha, and A. Cabellov(2013). Quantum nonlocality as the route for ever-lasting unconditionally secure bit commitment. *measurements*, pp. 16:17.

[14] A. G. d. A. H. Guerra, F. F. S. Rios, and R. V. Ramos (2016). Quantum secure direct communication of digital and analog signals using continuum coherent states. *Quantum Information Processing*, Vol. 15(11), pp. 4747–4758.

[15] P. V. P. Pinheiro and R. V. Ramos (2015). Two-layer quantum key distribution. *Quantum Information Processing*, Vol. 14(6), pp. 2111–2124.

[16] F. A. Mendonça, D. B. De Brito, and R. V. Ramos (2012). An optical scheme for quantum multi-service network. *Quantum Info. Comput.*, Vol. 12(7-8), pp. 620–629.

ANEXO B - 3º ARTIGO DECORRENTE DA TESE

Multiphoton Pulses and Homodyne Tomography Attack in Quantum-Chaotic Key Distribution

R. L. C. Damasceno, F. F. S. Rios and R. V. Ramos

ranaralouise@gmail.com frfranklin.rios@gmail.com rubens.ramos@ufc.br

Lab. of Quantum Information Technology, Department of Teleinformatic Engineering – Federal University of Ceara - DETI/UFC, C.P. 6007 – Campus do Pici - 60455-970 Fortaleza-Ce, Brazil.

The quantum-chaotic key distribution (QCKD) in optical networks was introduced in a recent paper. In that work, several differences between QKD and QCKD were pointed out. In this direction, the present work shows that, for a eavesdropper that uses a quantum homodyne attack, the mean photon number used by Alice in the QCKD protocol can be much larger than 0.1 without compromising its security.

1. Introduction

For quantum key distribution using discrete states, the larger the number of bases used the more secure is the protocol. However, since Alice and Bob keep only the information obtained in those time slots in which they chose the same bases, the key transmission rate decreases when the number of bases increases [1]. The problem of increasing the security by increasing the number of quantum states used without decreasing the transmission rate can be overcome by using quantum-chaotic key distribution (QCKD) [2,3]. In this case, although the information sent is discrete (bits '0' and '1'), the set of quantum states that travel in the channel is continuous, which increases the security. Furthermore, QCKD does not require the bases reconciliation procedure hence, the key transmission rate does not decrease.

If the number of different quantum states used to carry information increases, a question immediately arises: Can the amount of photons per quantum state be increased without weakening or destroying the security? If a QKD protocol uses multiphoton pulses, the eavesdropper, Eve, can use two strategies: If she has a quantum memory, she can obtain some photons from the multiphoton pulse sent by Alice and keep them in her quantum memory. After the bases reconciliation stage, Eve can measure the photon in the correct basis getting the correct information. If Eve does not have a quantum memory, she can try to get the maximal number of photons from the multiphoton pulse (without disturbing Bob's detection statistics) and she makes measurements on those photons. From the measured data, Eve infers the quantum state sent by Alice. For QCKD, to have a quantum memory is not useful, since there is no reconciliation stage. Hence, Eve has to get photons and measure them in order to infer the state sent by Alice. Thus, the important question is: how many photons can Eve get and still be unable to obtain useful information of the key? In order to answer this question, we use numerical simulations of a QCKD protocol using the logistic map and its implementation with the Mach-Zehnder interferometer. Furthermore, we assume that Eve uses a homodyne tomography attack.

2. Multiphoton QCKD with Logistic Map

Basically, in chaotic cryptography, the transmitter (Alice) and reciever (Bob) have nonlinear systems with the same parameters values. These information shared by Alice and Bob in advance serve as authentication. Differently of what was done in [2], here the nonlinear systems used are nonlinear

difference equations running in computers. The QCKD using synchronized logistic maps has been discussed in [3]. Its nonlinear dynamic is governed by the set of equations

$$z_{k+1} = \delta z_k (1 - z_k) \tag{1}$$

$$x_{n+1} = \lambda x_n (1 - x_n) + c\left[k - \lambda(1 - x_n - d\overline{z}_{k+1})\right](x_n - d\overline{z}_{k+1}) \tag{2}$$

$$y_{n+1} = \lambda y_n (1 - y_n) + c\left[k - \lambda(1 - y_n - d\overline{z}_{k+1})\right](y_n - d\overline{z}_{k+1}) \tag{3}$$

$$\overline{z}_{k+1} = 0 \text{ if } z_{k+1} < 0.5 \text{ and } 1 \text{ if } z_{k+1} \geq 0.5. \tag{4}$$

As one can note in (1)-(4), the Z system drives the X and Y systems with a discrete variable, $\overline{z_n}$, that assumes only two values, 0 and 1. The variable d in (2)-(3) controls the strength of $\overline{z_n}$. Once the chaotic systems X and Y are synchronized, a common key can be established from a discretization of the output variables x_n (for Alice) and y_n (for Bob). For example, a reference value V_{ref} is chosen. If $x_n \geq V_{ref}$ ($y_n \geq V_{ref}$) a bit '1' is recorded by Alice (Bob), otherwise a bit '0' is recorded. If $x_n = y_n$ the bits of Alice and Bob's key will be the same. Note that, since x_n and y_n assume continuous values between 0 and 1, an m-ary codification is also possible, implying a higher transmission rate. However, it is not our goal to discuss this issue here.

In order to implement a QCKD system using the logistic map and multiphoton pulses, the optical setup for QKD using the Mach-Zehnder interferometer (MZI) can be used, as shown in Fig. 1.

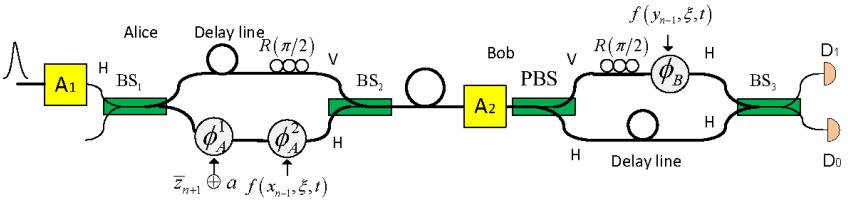


Fig. 1 – Optical setup for quantum-chaotic key distribution using multiphoton pulses with Mach-Zehnder interferometer. A_1 and A_2 are optical attenuators, D_1 and D_0 are single-photon detectors, PBS is a polarizing beam splitter and H and V stand for horizontal and vertical modes.

The functioning of the MZI shown in Fig. 1 has been widely discussed in the literature [4,5] and it is not our goal to repeat it here. The main points concerning the scheme in Fig. 1 are:

1. Alice's pulse in the lower arm is phase modulated by ϕ_A^1 and ϕ_A^2, according to the values of $\overline{z_{k+1}} \oplus a$ and $f(x_{n-1},\xi,t)$: $\phi_A^1 = \pi(\overline{z_{n+1}} \oplus a)$ and $\phi_A^2 = \pi f(x_{n-1},\xi,t)$. Here, the function f is the logist map $f_{m+1} = \xi f_m(1-f_m)$. The input value f_0 is x_{n-1} and the output value is f_t. The parameters ξ and t are only known by Alice and Bob. At last, a is the parity of the i-th digit of f_t.
2. At Bob's side, the pulse in the upper arm suffers a phase shift given by $\phi_B = f(y_{n-1},\xi,t)\pi$. For Bob, the input value f_0 is y_{n-1} and the output value is f_t.
3. Because of the polarization code, both pulses arrive at BS_3 at the same time, with the same polarization and an interference will take place. Depending on the difference of the phases applied by Alice and by Bob, the light pulse will be guided to the single-photon detector (SPD) D_0 or D_1. The probabilities of detection in D_0 and D_1 are given by

$$p_0 = \left(1 - \exp\left(-\left|\alpha_B\right|^2 p_d\right)\right)\cos^2\left[\pi\left(\overline{z}_{k+1} \oplus a + f\left(x_{n-1},\xi,t\right) - f\left(y_{n-1},\xi,t\right)\right)/2\right] \quad (5)$$

$$p_1 = \left(1 - \exp\left(-\left|\alpha_B\right|^2 p_d\right)\right)\sin^2\left[\pi\left(\overline{z}_{k+1} \oplus a + f\left(x_{n-1},\xi,t\right) - f\left(y_{n-1},\xi,t\right)\right)/2\right]. \quad (6)$$

In (5)-(6), $|\alpha_B|^2$ is the mean photon number after the attenuator A_2 and p_d is the probability of detection of D_0 and D_1, here considered noiseless. For Bob, detection in D_0 implies $\overline{z_{k+1}} \oplus a = 0$ while detection in D_1 implies $\overline{z_{k+1}} \oplus a = 1$. As can be seen in (5)-(6), the probabilities of detection depend on the synchronism and the synchronism depends on the probabilities of detection.

The lack of synchronization signals will cause the desynchronization of the logistic maps, resulting in a high error rate. In order to avoid this, Alice and Bob should update the values of x_n and y_n only when Bob has detection. This implies that, when Bob has no detection he informs Alice and she will update z_{k+1} and calculating a new value for f using t+1, instead of t. Hence, every pulse sent by Alice will have a different phase value even when x_n is not updated. Bob will do the same until he has detection.

Now, the important question is, if Alice sends a coherent state to Bob with mean photon number $|\alpha|^2$, what is the maximal secure value of $|\alpha|^2$ if $[z_{k+1} \oplus a + f(x_{n-1},\xi,t)]\pi$ is a continuous phase ranging in the interval $[0,2\pi]$? Since Eve does not know which basis of measurement to use, we assume that she can realize a homodyne tomography of the state leaving Alice [6]. If the fidelity of the reconstructed density matrix, F, is lower than 1, there will be an error in the estimated phase. Numerical simulations show that an error of 0.05 rad in the value of the phase of the coherent state sent by Alice causes an error of around 13% in the bits of the key, indicating Eve's presence. The fidelity between two coherent states with the same mean photon number (we consider Eve knows the mean photon number used by Alice), $\langle n \rangle$, is given by $F = \exp\{-2\langle n \rangle[1-\cos(\Delta)]\}$, where Δ is the difference between the angles of the two considered coherent states. Using $\Delta = 0.05$ rad, the fidelity is $F \approx 0.95$ when $\langle n \rangle = 20$. Hence, hereafter we consider $F = 0.95$ as the maximal value for the fidelity allowed for Eve. Now, the new question is: how many coherent states with mean photon number $|\beta|^2$ are necessary in order to have a good estimation of the phase? Let us assume that Eve uses the homodyne scheme shown in Fig. 2.

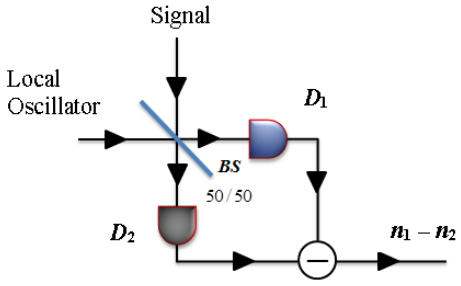


Fig. 2 – Homodyne scheme using balanced beam splitter and photon counters (D_1 and D_2).

In Fig. 2, D_1 and D_2 are photon counters. Eve divides the coherent state sent by Alice in r copies having mean photon number $|\beta|^2$, $r = |\alpha|^2/|\beta|^2$, hence, the signal state is $||\beta|e^{i\phi}\rangle$ where ϕ is the total phase chosen by Alice. The local oscillator used by Eve is the coherent state $||\beta|\rangle$ (with phase equal to 0 rad). The probability distribution of the difference of the number of photons measured by D_1 (n_1) and D_2 (n_2), $N = n_1$-n_2, is given by the Skellam distribution

$$P_N = e^{-2|\beta|^2} \left|\tan(\phi)\right|^N I_{|N|}\left(2|\beta|^2 \left|\sin(2\phi)\right|\right). \tag{7}$$

In (7), $I_{|N|}$ is the modified Bessel function of the first kind. Thus, if Eve measures the variable N a number r of times, she can have an estimation for P_N and, using this estimation and (7), she gets an estimation for ϕ. As one can note, Eve cannot use $|\beta|^2$ very close to zero since in this case the angle ϕ loses its importance (for $\beta = 0$, $P_0 = 1$ for any value of ϕ). A good estimation of P_N will require a large value for r. Let us be very conservative assuming that Eve uses $|\beta|^2 = 1$. Assuming also that Alice uses $|\alpha|^2 = 20$, Eve would have only $r = 20$ copies to make her estimation of P_N. Using a numerical simulation, one can see in Fig. 3 the real (Eq. 7) and estimated distributions of N for $r = 20$ (upper) and $r = 10{,}000$ (lower) for $|\beta| = 1$ and $\phi = \pi/3$.

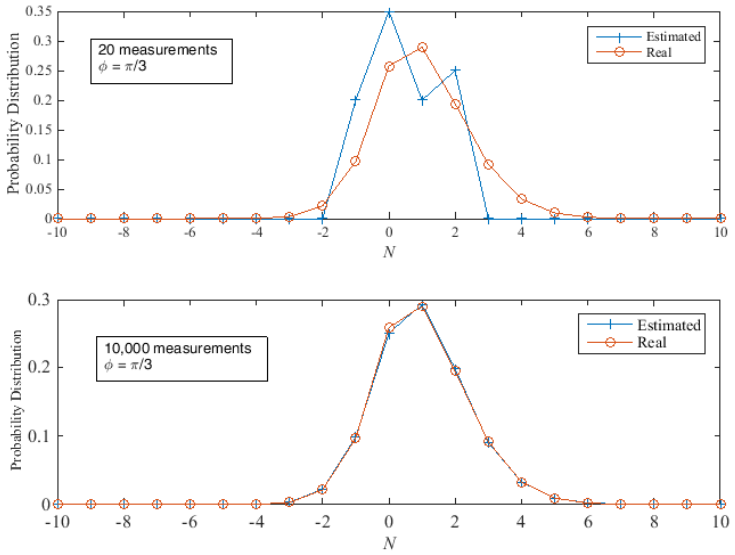


Fig. 3 – Real and estimated distributions for N having $|\beta| = 1$ and $\phi = \pi/3$.

As one can see in Fig. 3, 20 measurements will not provide enough data for a good estimation of P_N. The phase estimation obtained by $min_\phi \Sigma_N \left[P_N(\phi) - \widetilde{P_N}\right]^2$, where $\widetilde{P_N}$ is the estimation of P_N shown in Fig. 3, are $\tilde{\phi} = 0.845801322478620$ rad for 20 measurements and $\tilde{\phi} = 1.04059954682362$ rad for 10,000 measurements ($\phi = \pi/3 = 1.04719755119660$). Hence, hereafter we assume that Alice will use $|\alpha|^2 = 20$.

On the other hand, in order to guarantee that Bob will have single-photon detection, one should have

$$|\alpha_B|^2 = |\alpha|^2 10^{\frac{-(\sigma L + A_0)}{10}} = 0.1, \tag{8}$$

where $\sigma = 0.27$ dB/km is the fiber's loss coefficient and L is the fiber length between Alice and Bob. The maximal fiber length that obeys (8) is achieved when $A_2 = 0$. In this case one has $L_{max} = 85$ km.

Figure 4 shows a simulation of the synchronization between Alice and Bob's nonlinear systems for the follwoing parameters values: $p_d = 0.15$, $L = 85$ km, $|\alpha|^2 = 20$, $\sigma = 0.27$ dB/km, $\delta = 4$, $\lambda = 3.9$, $k = 0.2$, $c = 0.5$, $d = 0.5$, while the initial values of the dynamic variables are $x(1) = 0.7$, $y(1) = 0.7$, $z(1) = 0.2$. For the logistic map f we used $\xi = 3.97$ and $t = 1000$. The lower part of Fig. 4 is the fast Fourier transform of x_n. Its continuous behavior reinforces the random character of x_n.

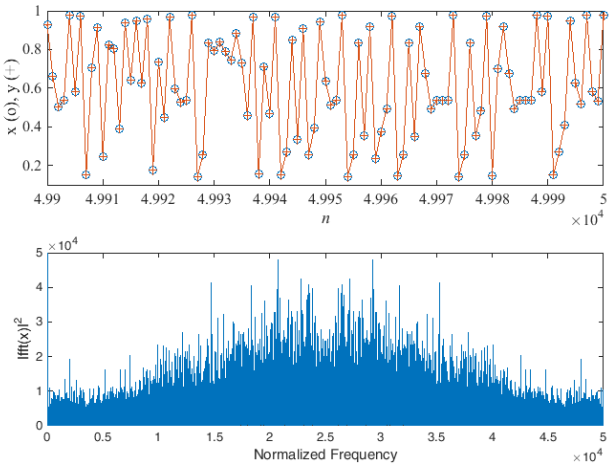


Fig. 4 – Synchronization of the chaotic systems X (o) and Y (+). Only the last 100 values from a simulation with 50,000 runs are shown. The bottom part is the Fourier transform of the output x_n.

3. Conclusions

The present work showed that, since QCKD uses coherent states with continuous phase and there is no bases reconciliation stage, Alice can use coherent states with a mean photon number much larger than 0.1, the value traditionally used in QKD setups. This is possible because, without knowing which bases of measurement to use, Eve attacks using a homodyne tomography so, its enough for Alice to use a coherent state with the mean photon number lower that the value necessary for Eve getting a good estimation of the state sent by her.

The QCKD requires that Alice and Bob share in advance the same data of their nonlinear systems (parameters and initial values). However, in this case, one may wonder that since Alice and Bob share the same parameters and initial values, their nonlinear systems will be always synchronized and the quantum communication between them will not be necessary. This is true, nevertheless, without the quantum communication their dynamic will be deterministic, what can weaken the criptographic scheme used. The single-photon detection at Bob introduces a random noise in the nonlinear systems making their dynamic nonlinear and stochastic (but still synchronized). Furthermore, it is also possible to change the nonlinear system Z by a true random bit generator, increasing more the unpredictability of the nonlinear systems used by Alice and Bob.

At last, one may note that, if Eve measures the correct value for $\phi = \phi_A^1 + \phi_A^2$, she can use a brute force attack, choosing values for ξ and t, in order to determine the value of $x_{n\text{-}1}$, what implies in the knowledge of the bit of the key. Hence, 'classical' pulses must be avoided by Alice.

Acknowledgements

This work was supported by the Brazilian agencies CAPES and CNPq via Grant no. 307062/2014-7. Also, this work was performed as part of the Brazilian National Institute of Science and Technology for Quantum Information. The authors gratefully acknowledge many helpful discussions with Jonas Söderholm of Federal University of Ceara.

References

[1] Bourennane, M., Karlsson, A ., and Björk, G .: Quantum key distribution using multilevel encoding, Phys. Rev. A, 64, 012306/1-5, 2001.

[2] de Oliveira, G. L., and Ramos, R. V.: Quantum-chaotic cryptography, Quant. Inf. Process., 17, 40, 2018. https://doi.org/10.1007/s11128-017-1765-x

[3] Damasceno, R. L. C., de Oliveira, G. L., and Ramos, R. V.: Quantum-chaotic key distribution with synchronized logistic maps, Internal Report, Federal University of Ceara, 2018.

[4] Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H.: Quantum cryptography, Rev. Mod. Phys., 74, 145-195, 2002.

[5] Lo, H.-K., and Zhao, Y.: Quantum cryptography, Computational Complexity, 2453, 2012.

[6] Raffaelli, F., Ferranti, G., Mahler, D. H., Sibson, P., Kennard, J. E., Santamato, A., Sinclair, G., Bonneau, D., Thompson M. G., and Matthews, J. C. F., A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers, Quantum Sci. Technol., 3, 025003, 2018.