Universidad Autónoma de Baja California

Programa de Posgrado de Maestría y Doctorado en Ciencias e Ingeniería (MyDCI)

Facultad de Ciencias Químicas e Ingeniería.

Comunicaciones Ópticas Seguras con Criptografía Cuántica Homodina

Tesis que para obtener el grado de Doctor en Ciencias presenta

Edith García Cárdenas

Enero de 2014

Director de Tesis

Dr. Francisco Javier Mendieta Jimenez

Comité de Tesis

Dra. Rosa Martha López Gutiérrez

Dra. Adriana Nava Vega

Dr. Angel Gabriel Andrade Reátiga

Dr. Eduardo Álvarez Guzmán

Suplentes

Dr. Luis Enrique Palafox Maestre

Fecha de la defensa de tesis

21 de Enero de 2014

Universidad Autónoma de Baja California

FACULTAD DE CIENCIAS QUÍMICAS E INGENIERÍA

COORDINACIÓN DE POSGRADO E INVESTIGACIÓN

FOLIO No. 110

Tijuana, B. C., a 06 de enero de 2014

C. Edith García Cárdenas
Pasante de: Doctorado en Ciencias
Presente

El tema de trabajo y/o tesis para su examen profesional, en la Opción TESIS

Es propuesto, por el C. Dr. Francisco Javier Mendieta Jiménez

Quien será el responsable de la calidad de trabajo que usted presente, referido al tema Comunicaciones Ópticas Seguras con Criptografía Cuántica Homodina.

el cual deberá usted desarrollar, de acuerdo con el siguiente orden:

I.- MARCO TEORICO
II.- REALIZACION EXPERIMENTAL
III.- MEDICIONES Y ANÁLISIS DE RESULTADOS
IV.- CONCLUSIONES

UNIVERSIDAD AUTONOMA DE BAJA CALIFORNIA

FACULTAD DE CIENCIAS QUIMICAS E INGENIERIA

Q. Noemí Hernández Hernández
Sub-Director Secretario

Dr. Francisco Javier Mendieta Jiménez
Director de Tesis

Dr. Luis Enrique Palafox Maestre
Director

RESUMEN

En el presente trabajo se desarrolló el análisis teórico y la realización experimental, de un sistema de transmisión-recepción cuántico para aplicaciones en los sistemas de distribución de la llave criptográfica, para comunicaciones cuánticas seguras. Se implementó un receptor homodino de ocho puertos para ser utilizado en espacio libre en el rango de los 1550 nm para la detección de estados coherentes débiles que contienen información binaria. Se utilizó un esquema de modulación eficiente como la Modulación de Fase Binaria (BPSK por sus siglas en inglés), por lo que en el receptor se implementó un Lazo de Costas para la sincronización de la portadora. Se logró la recepción y análisis de señales cercanas al Límite cuántico estándar con potencias del orden de los femto watts, esto es en promedio un fotón por tiempo de bit y menores.

Se obtuvo la relación señal a ruido (SNR), la tasa de bits erróneos (BER), asi como un análisis de los resultados estadisticos de la información mutua entre transmisor (Alice) y receptor (Bob) con presencia de un espía (Eva); y de la distribución de cuasi probabilidad $\boldsymbol{Q}$ para los observables en fase y cuadratura que son medidos en forma simultánea. Los resultados muestran que es posible utilizar éste canal cuántico para comunicaciones cuánticas y para la distribución de llave criptográfica.

ABSTRACT

In this thesis we developed the thoretical analysis and the experimental realization of a transmission-reception system for applications in quantum key distribution systems for secure quantum communications. An 8-port homodyne receiver operating at 1550 nm, was implemented in free space technology for detection of weak coherent states that carry binary information. A suppressed-carrier modulation is used, therefore we implemented an optical Costas-loop-type carrier synchronizer. We were capable of receiving signals near the standard quantum limit (SQL) with weak coherent sates with a few femto watts power, this is one photon per bit average.

We performed measurements to obtain the bit error rate (BER), the signal to noise ratio (SNR), the mutual information between transmitter - receiver without and with the intervention of an evesdropper. We obtain the quasiprobability distribution Q function from the in-phase and quadrature observables that are simultaneously measured. The results show that the proposed setup is suitable for quantum communications and continuous variable quantum key distribution systems.

Dedicatoria

A mi esposo Eduardo Álvarez y a mi hija Mariana por todo lo que me brindan y me permiten darles.

私は大好きです

Agradecimientos

A mi esposo y a mi hija, por su amor, apoyo, paciencia y aguante que tuvieron conmigo para que yo lograra esta meta.

A mi Director de Tesis Dr. Francisco Javier Mendieta, por la oportunidad y confianza que me otorgó para trabajar en este proyecto.

A mi Comité de Tesis por sus valiosas aportaciones a este trabajo.

I would like to thank Doctor Philippe Gallion of the Ecole Nationale Supérieure des Télécommunications TELECOM ParisTech, for his valuable contributions to this work.

A la Facultad de Ciencias Químicas e Ingeniería por el apoyo que recibí para realizar mis estudios de doctorado y concluir esta tesis.

Al personal del Departamento de Electrónica y Telecomunicaciones (Investigadores, Técnicos y personal administrativo) de CICESE; y a los doctores Heriberto Márquez y David Salazar por sus amenas charlas, a los técnicos del Departamento de Óptica por el apoyo y confianza que me brindaron durante el trabajo experimental.

A mi madre, mis hermanas y sobrinos por su apoyo y palabras de aliento durante todos estos años.

A mi padre (q.e.p.d) por sus enseñanzas que me fueron muy útiles sobre todo durante mis incontables viajes manejando por carretera a Ensenada.

A mi hermano (q.e.p.d) por sus recuerdos y buenos momentos.

A mis amigos Norma Herrera Hernández, Ma. del Carmen Maya y Luis Alejandro Márquez, por su invualuable hospitalidad durante mis días de estancia en Ensenada. Gracias por su amistad y confianza.

A mi compañero de doctorado Josué A. López L. por el trabajo en equipo y a los compañeros del cubículo de estudiantes de doctorado por no cerrar la reja :)

A todos mis amigos (los que están cerca y los muy lejanos fisicamente) por sus consejos y ánimos que me dieron cuando más lo necesitaba.

A mis compañeros de trabajo de UABC por sus consejos, palabras de aliento y apoyo.

A mis alumnos, quienes también son mis grandes maestros.

A mis amigas Patricia Moreno, María Rocha, Juana Rodriguez y Norma O. Bravo, quienes en algun momento me apoyaron cuidando de mi querida hija mientras yo estaba en el trayecto de regreso a casa desde Ensenada o en alguna reunión de mi comité.

A Julieta Pacheco, por su valioso oportuno apoyo en la comunicación con mi director de tesis.

A mis maestros de paciencia, por que por la piedras que pusieron en el camino, me permitieron trabajar en mi práctica diaria para lograr un día sentir la Gran Compasión por todos los seres sintientes.

Al CONACYT por la beca otorgada para la realización de esta tesis.

Summary

A worldwide important aspect of communication networks is the security and confidentiality of information. Government communications, corporation information, and business transactions that are transmitted through the Internet demand the links to be trustworthy. The individuals need systems that provide assurance, that privacy is kept, and that the transmitted data will be received only by the individual or desired system. In order to achieve this, it has been developed a tool called cryptography.

At present, the security provided for the digital information is based on conventional encryption systems information. These systems consists of computational algorithms that are difficult to spy but are not unconditionally secure. One example of some implementations are RSA encryption code (Rivest, Shamir and Adleman, 1970) which is based on the factorization of two large prime numbers randomly chosen and kept in secrecy, however those numbers are about 10,200 digits and due to faster and better computing capacity of current computer equipment it is expected that the digits size will have to increase in order to keep the mesage decoding, difficult to achieve without the keys. As a result due to advances in computational capacity of espionage agents, in time these systems will turn vulnerable regardless of the complexity of the algorithm used.

Quantum cryptography can guarantee unconditional transmission security, for it is based not on a computational algorithm, but on the quantum properties of the photon. Quantum principles applied are based on the principle of "quantum demolition" which involves destruction of the state of the photon and the "no quantum cloning" which aserts that it is not possible to clone the state of a photon, which results in that any espionage activity modifies the transmission link properties for it alters the quantum state of the photon resulting in the detection of the tampering by the legitimate recipient message. The recipient can then ask the transmitter to stop sending information, before, there is enough data that the attacker can use to extract the encripted information.

Due to the urgency in ensuring the security of any transmitted information, major international efforts are being carried out in research and development of quantum cryptography communication systems, which aim to have a tool to confront the threats of future technolo-

gies interception and decryption of the information, which is looking to raise international standards of confidentiality and security of electronic communications and data exchange via public channels.

Information exchange in an unprotected channel between transmitter and receiver, who henceforth will be called Alice and Bob respectively, requires the generation and exchange of a cryptographic key, which Eve the spy (Evesdropper) will try to steal, in order to access the message. The security of the system therefore results from the inability of the spy, to duplicate the received signals or removing a significant portion of the data without producing a significant change in Bit Error Rate (BER) of the data received by the authentic recipient of the message (Bob). Thus the security is based on the physical characteristics of the physical signal received, *ie*, observing errors resulting from specific quantum states, such as the polarization or the phase of a photon for different conjugate bases, or such as the simultaneous measurement of the quadratures of the same quantum state.

The Quantum cryptography is therefore a growing research area for secure communications, which results from the confluence of two great achievements of the twentieth century science: The Information Theory and Quantum Physics. After decades of theoretical and experimental work, cryptographic Quantum Key Distribution has reached a stable status as a base for applied research and development.

In 1984 Bennett and Brassard proposed a protocol which they called the Quantum Key Distribution (QKD) BB84; the first experiments were carried out at wavelengths in the range of visible or near infrared, which is incompatible with current photonic communication networks. Recently there have been experimental demonstrations using wavelengths for telecommunications networks, based on photon polarization. However, these demonstrations have limited applications because of the reduced bandwidth of the used measurement systems. These systems used conventional photon detection devices operating in the optical communication band, nevertheless such devices have a very slow transfer rate for quantum key distribution. This is because that the avalanche photodiode (APD) used in the photon counters have a very low quantum efficiency in the near infrared, they suffer from a low response speed, besides a low operating temperature is required to reduce photon counting caused by dark current.

Coherent detection is the focus of this work; unlike photon counting techniques, it is based on the use of p.i.n photodetectors that are devices widely used in conventional high speed photonic communication networks. p.i.n devices have high quantum efficiency, fast response speed and low cost, and the advantage to work at room temperature. In the coherent detection technique, it is needed to measure In-phase (I) and Quadrature (Q) of the optical field; this kind of detection has been extensively studied because of its characteristics related to

the use of the complex amplitude modulations in the field optical, which allow the use of low numbers of photons or low value of the signal to noise ratio (SNR, signal to noise ratio) for a given BER (Bit Error Rate).

In a coherent detection scheme, a reference signal called Local Oscillator (LO) is used. The LO phase must be synchronized with the phase information of the optical carrier. This means that the signal reception is capable to deal with the complex amplitude of the optical field, furthermore an advantage of the coherent detection is that it is possible to achieve the standard quantum limit (SQL, Standard Quantum Limit) using a strong local oscillator (LO).

Throughout this work it is shown that it is possible to obtain viable results for a physical implementation of a quantum communications system proposing the following:

1. To analyze, design and implement a free-space quantum communications channel in Mexico, throug a homodyne receiver, for Quantum Key Distribution.
2. Verify that such quantum communications channel, provides the required conditions for its use in secure quantum communications.
3. To produce a transmission and reception of information, using weak coherent states, implying a femtowatt levels in bit power.
4. To verify that a homodyne receptor is capable to produce the quasiprobability funtion of a quantum state, without the need of using tomographic techniques.

Thesis proposal

To obtain a quantum channel implementation in México for a Quantum Key Distribution System, in order to have a foundation stone in the process to create a full quantum communication sistems. This implies that the current work will be concentrating in the first layer of the OSI 7 layer model.

The contribution of this work is the demonstration of the posibility of a direct measuremente of the quasiprobability function ($\boldsymbol{Q}$) through a two quadrature simultaneous measurement taking into account the quantum noise (vacuum noise); therefore there is no need of a traditional tomographic measurement; plus is possible to achieve this using a coherent modulation scheme with suppressed carrier.

With this work it is shown that:

1. The use of a homodyne scheme in order to detect femtowatt level signals, and weak coherent quantum states is feaseable.

2. We measure the two quadratures, simutaneously, even with the additional noise increase.
3. We use a 1 photon ber bit equivalent power, without the need of ultra short pulses containing hundreds of photons.
4. Balanced PIN photodetectors are used, allowing a better time-response of the system, and a seamles integration to modern optical communications networks
5. The achieved quantum channel, allows its use for Quantum Key Distribution implementations.

Experimental setup.

The experimental setup consists of a free space 8-port interferometer, where we use an external cavity laser tuned to a 1550.1 nm wavelength. This laser is used both as the carrier for the data, and the L.O. in order to operate in an stabilization free self-homodyne configuration, thus simplifying the automatic frequency control, leaving only the optical phase lock to be implemented. A pseudorandom data sequence at 350 Kbps is generated and used to drive the electro-optical phase modulator PM1 in order to get the optical BSPK modulation. In this set up, it is required to have well-defined polarization states that allow the detection of the conjugate variables at the BHD's. After setting the State of Polarization (SOP) of the modulated beam at a linear 45 degrees polarization, the beam is attenuated by 120 dB through a set of calibrated neutral density filters (ND-filters) in order to produce a quantum level signal, that is an optical beam power equivalent to 1 photon per bit duration; which in our case corresponds to a 45 fW signal power. This weak coherent signal is fed to the 8-port system. The local oscillator signal (with a 2mW power level) travels to a second phase modulator that will be used to control the relative local oscillator phase in a feedback loop (Costas loop) to maintain the 8-port interferometer in-phase lock. Then a $\lambda/4$ polarizer (QWP) is used to produce a circular polarization state. At the 8-port inputs, the local oscillator and the weak power modulated beams are combined through a non polarized beam splitter, then the combined signals emerging from the beam splitter are split in their vertical and horizontal components, using Polarized Beam Splitters in order to separate its quadratures, beating with a circularly polarized local oscillator, thus providing the $0^0$and 90^0 outputs in a stable setup. The vacuum noises enter in the system through the used and unusued ports of the PBSs. The vertical and horizontal optical fields impinge on the balanced homodyne photo detectors (BHD1 and BHD2) respectively (p.i.n photodetectors).

The electrical signals of the BHD's which correspond to the I and Q signals are simultaneously measured and they are post-processed. The I and Q signals will be used to generate the required error signals for the Costas Loop that will enable phase locking between the data signal and the local oscillator. For information-carrying signals, a precise phase lock between the signal and the L.O. is required. Since we are using an interferometric scheme we don't have a true optical Voltage Controlled Oscillator (VCO) to get such phase lock; however we implemented an "equivalent" optical VCO by means of the LO signal and an optical phase modulator driven by a signal obtained from processing the I, and Q signals. Therefore there is no need for a learning synchronizing sequence or residual carrier, which is of utmost importance in synchronous quantum communications and synchronous quantum cryptography. Our overall quantum efficiency is $\eta = 0.7$ due to optical losses and residual spatial mode mismatch between the signal and the L.O.

The received signals are statistically post-processed in order to show that this setup has the ability to discriminate the electric levels for the logical "1"s and "0"s, down to an average signal level of 0.25 photon per bit. We measure the quasiprobability Q function of the received field directly, we measure the uncertainty relationship for the quadratures I and Q measured and experimentally verify that it complies with the relationship for the simultaneous quadratures measurement of the optical field. The Bit Error Rate (BER) and the Mutual Information (I) between Alice and Bob (IAB) are finally obtained.

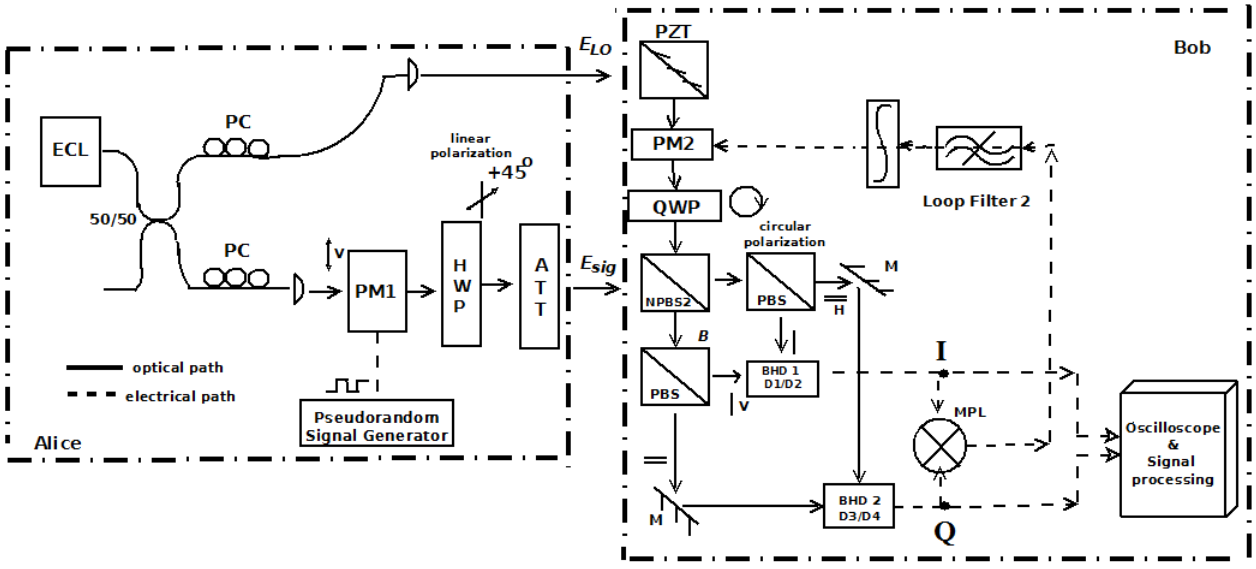
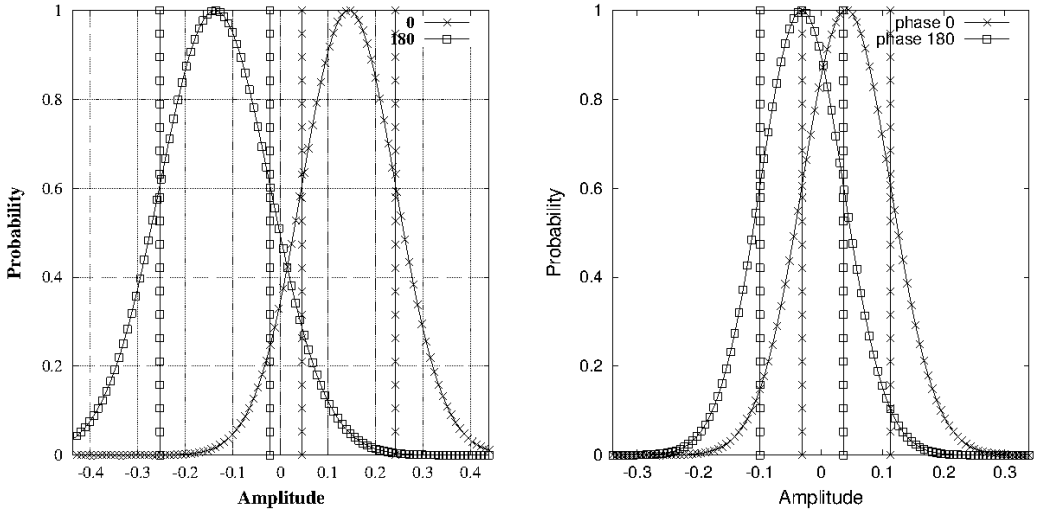


Figure 1.: 8 port homodyne receiver

Results

Fig. 2 shows the statistical distribution of the measured data for the voltage produced by the logical levels 1 and 0, received in the BHD, there is a small overlapping zone, allowing a clear discrimination between the two logical levels. However, in 2b(N = 0.25 average photons per bit duration), the overlapping between the symbols probability curves surpasses the first standard deviation, as a result we have an increase in the BER.



(a) N=1 **(b)** N=0.25

Figure 2.: Statistical distribution of themeasured data for N=1 and N=0.25 photon number.

Fig. 3 shows the measured quasiprobability distributions and the contour lines for the experimental data for the case of 1photon/bit. The raw data (a and c) and the reconstructed distribution with the mean and variance obtained from the raw data (b and d). In the case of the contour line graphs there is a slight asymmetry in one of the probability distributions; we attribute this to a slight unbalance in the input of the photo detectors, and/or due to the asymmetric modulation at the transmitter.

In 4a the theoretical and experimental BER results are compared, showing in general a good agreement, for our efficiency of 0.7. The Helstrom and standard quantum limits are also included for comparison. Based on the measured BER, it is possible to calculate the mutual information achievable between Alice and Bob. The mutual information is calculated

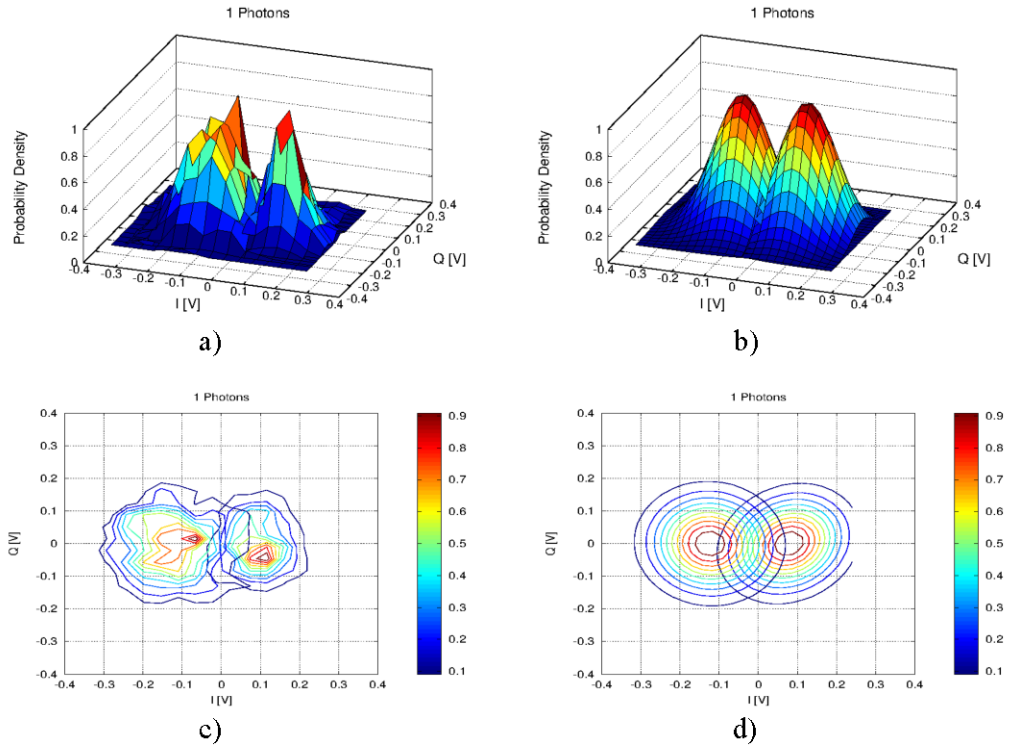


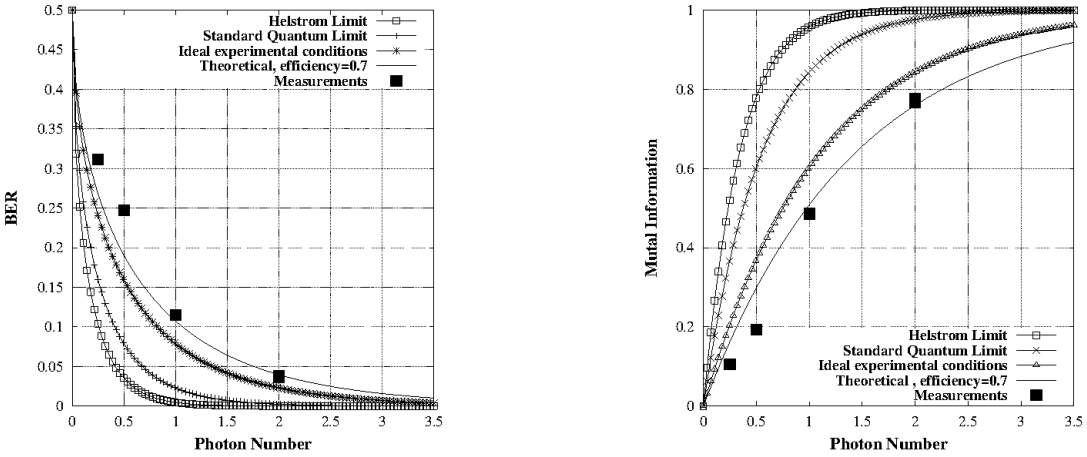
Figure 3.: Measured quasiprobability distributions and the contour lines for the experimental data for the case of 1 photon/bit, the raw data (a and c) and the reconstructed distribution with the mean and variance obtained from the raw data (b and d).

with the measured data. 4bshows the mutual information results as compared with the theoretical values for 0.7 efficiency.

Conclusions

According to results, this work has shown that the use of the homodyne scheme with weak coherent states, near the standard quantum limit allows an efficient implementation for detecting signals above the thermal noise of the electronic devices and photodetectors employed. This suggests that a system optimization process that reach efficiencies greater than 0.7, will provide optimum results for the transmission and reception process in a quantum channel.

It has been shown that this system allows the detection of the I and Q quadratures of the optical field simultaneously, even with the presence of additional noise (quantum noise) that is introduced through unused ports of the beam splitters. The results show that the presence of this noise does not reduce the ability to achieve the required signal to noise ratio (SNR), for the Bit Error Rate (BER) required for the system. Results show that noise an data



(a) N=1 **(b)** N=2

Figure 4.: Figure in the left shows the theoretical and experimental BER, the right figure shows the mutual information, both are calculated with the measured data.

maintain Gaussian distributions.

It has been also shown that it is possible to receive the energy of a single photon per bit (which is recommended for safety purposes a quantum cryptographic system), using a continuous laser source, using an attenuators array, to achieve a weak coherent signal power equivalent to 45 fW. The BPSK modulation format is used to test communication systems employing ultrashort pulses of large numbers of photons, for equivalent power per bit. This achievement demonstrates that it is possible to implement quantum homodyne detection, without the need of decoy signals to improve the channel safety, as in the case of cryptographic systems with hundreds of photons per pulse.

It has been shown that systems using P.I.N. balanced photodetectors are capable of receiving the transmitted data, and provides the possibility of working at higher data transmission rates. The photodetectors have a capacity of up to 10 MHz bandwidth, so this technology can increase the data bit rate in optical communication schemes for secure quantum cryptography systems. This technology has a high degree of development in the world of optical communications, and the integration with other components in semiconductor wafers can offer the ability to implement similar devices as the one implemented for free space links, that of course will increase the possibilities of optimization and efficiency improvements, required for optical communication systems in currently available commercial networks.

The results of the Bit Error Rate, signal to noise ratio and mutual information are close to those calculated theoretically and expected for the weak power of the received signal. The effect of the intrusion of a spy (Eve) on the link between Alice and Bob, was estimated in

order to calculate safety thresholds of Secure Key Rate transmission. From these results it has been shown that the quantum communication channel developed in free space, can be used for criptographic Quantum Key Distribution Systems (QKD), and this technology may be applied to the distribution encryption keys thorugh satellite links, in line of sight optical communications links, and quantum systems for optic fiber communications.

The system allows the direct measurement of the quantum quasiprobability Q function as the two fields quadratures are measured simultaneously. The direct measurement of the quasiprobability function is interesting as compared to the standard tomography: although the latter yields the Wigner distribution, it requires the sweeping of the L.O. phase. Our system yields the Q function directly which is of interest for information-carrying fields.

"We have a habit in articles published in scientific journals to make the work as finished as possible, to cover up all the tracks, to not worry about the blind alleys or describe how you had the wrong idea first, and so on. So there isn't any place to publish, in a dignified manner, what you actually did in order to get do the work"

- Richard Feynman.

Fragmento del discurso pronunciado durante su premiación como Premio Nobel de Física en 1966.

Índice general

Índice de figuras

Índice de tablas

Introducción

Un aspecto importante de las redes de comunicaciones en todo el mundo es la seguridad y confidencialidad de la información, los gobiernos, corporaciones, transacciones y negocios que se concretan vía internet, e individuos que necesitan sistemas que les proporcionen privacidad y certeza de que los datos que se transmiten serán recibidos sólo por la persona o sistema deseado. Para lograrlo el ser humano desde tiempos ancestrales ha desarrollado una herramienta llamada criptografía.

En la actualidad la seguridad de la información se basa en sistemas convencionales de encriptamiento de información que consisten en algoritmos computacionales que no son incondicionalmente seguros, tales como el código de encriptamiento RSA (Rivest, Shamir y Adleman,1970) ampliamente utilizado el cual consiste en la factorización del producto de dos números primos grandes elegidos aleatoriamente y mantenidos en secrecía, sin embargo esos números son del orden de 10,200 dígitos y se calcula que su tamaño aumente debido al incremento de la capacidad de cálculo de los equipos de cómputo actuales, de manera que dado a los avances en la capacidad computacional de los agentes de espionaje, estos sistemas son vulnerables independientemente de la complejidad del algoritmo utilizado [2, 3].

La criptografía cuántica es capaz de garantizar la seguridad incondicional por que está basada no en un algoritmo computacional si no en las propiedades cuánticas de un fotón. Los principios cuánticos en los que se basa la seguridad de la información que está contenida en la señal óptica (fotones) son la "demolición cuántica" la cual consiste en la destrucción del estado del fotón y en la "no clonación cuántica" la cual a su vez consiste en que no es posible clonar el estado de un fotón, lo que trae como consecuencia que cualquier actividad de espionaje altera el estado cuántico del fotón y es detectado por el receptor legítimo del mensaje [4, 5].

Siendo evidente la urgencia en la seguridad de cualquier tipo de informacion transmitida se están llevando a cabo grandes esfuerzos a nivel internacional en la investigación y desarrollo de la criptografía cuántica que tienen como objetivo contar con una herramienta que permita enfrentar las amenazas de futuras tecnologías de intercepción y desencripción de la información, con lo que se busca elevar los estándares internacionales de confidencialidad y seguridad

de las comunicaciones electrónicas e intercambio de datos vía canales públicos.

El intercambio de información en un canal no protegido entre Transmisor y Receptor, a quien se denominará de ahora en adelante Alice y Bob respectivamente, requiere de la generación e intercambio de una clave criptográfica, la cual tratará de obtener el espía Eve (*Evesdropper*) para tener acceso al mensaje. La seguridad entonces resulta de la imposibilidad para el espía de duplicar las señales recibidas o de extraer una parte significativa sin marcar su intervención por una modificación importante de la Tasa de Transmisión de Errores de Bit (BER, *Bit Error Rate*) de las señales recibidas por el destinatario legítimo del mensaje. Por lo tanto la seguridad se basa en las características físicas de la señal recibida, es decir, en los errores resultantes de observaciones incompatibles de un mismo estado cuántico, tales como la polarización o la fase de un fotón sobre bases conjugadas diferentes, o como la medición simultánea de las dos cuadraturas de un mismo estado cuántico.

La criptografía cuántica es por lo tanto, un área de investigación en expansión para las comunicaciones seguras, basada en la confluencia de dos grandes logros de la ciencia en el siglo XX : La Teoría de la Información y la Física Cuántica, y tras décadas de trabajo teórico y experimental sobre la distribución cuántica de la llave criptográfica, se ha creado una base estable para actividades de investigación aplicada y desarrollo, y actualmente en el mundo se registran procesos avanzados en sus diversos aspectos con pruebas de campo realizadas tanto para sistemas de transmisión óptica con fibra [4] así como en el espacio libre [6] e incluso sistemas criptográficos ópticos entre satélites[7]. Dicho avance se ha desarrollado principalmente para sistemas de comunicaciones punto a punto, ya que la amplificación de señales a niveles cuánticos constituye un problema aun sin resolver, sin embargo, ya se han reportado algunos experimentos en redes fotónicas basados en la Multicanalización por División de Longitud de Onda (WDM por sus siglas en inglés) [8], lo que presenta un escenario favorable para el futuro de esta tecnología aplicada a redes de alta velocidad.

En 1984 Bennet y Brassard propusieron un protocolo al que denominaron BB84 para la Distribución Cuántica de la Clave criptográfica (QKD, Quantum Key Distribution), en donde los primeros experimentos fueron llevados a cabo en longitudes de onda en el rango del visible o en cercano infrarrojo, lo cual es incompatible con las redes de fotónicas actuales; más recientemente se han realizado demostraciones en las longitudes de onda de las telecomunicaciones, basadas en la polarización de fotones[9]. Sin embargo, estas demostraciones tienen aplicaciones limitadas debido al ancho de banda reducido de los sistemas de medición con detección de fotones convencionales que operan en la banda de las comunicaciones ópticas, lo que da como resultado una tasa de transmisión muy lenta de distribución de la clave cuántica. Esto es debido a que los fotodiodos de avalancha (APD, *Avalanche Photo Diode*) utilizados en los

contadores de fotones presentan una muy baja eficiencia cuántica en el infrarrojo cercano y una baja velocidad de respuesta al estar necesariamente operados en modo "compuerteado" (modo Gieger),además de que es necesaria una baja temperatura de operación para reducir el conteo de fotones provocados por la corriente de oscuridad.

La detección coherente que es el tema central de este trabajo, a diferencia de la técnica de conteo de fotones, está basada en el uso de fotodetectores p.i.n. convencionales que son utlizados ampliamente en comunicaciones fotónicas, los cuales presentan alta eficiencia cuántica, rápida velocidad de respuesta y bajo costo, además de trabajar a temperatura ambiente. En la técnica de detección coherente es necesario realizar mediciones de las componentes en fase (I) y en cuadratura (Q) del campo óptico, este tipo de detección ha sido ampliamente estudiando dadas sus características relacionadas con utilización de modulaciones en la amplitud compleja del campo óptico, lo cual permiten el uso de bajos números de fotones, o un bajo valor de la relación señal a ruido (SNR, *signal to noise ratio*) para un BER dado.

En un esquema de detección coherente se utiliza una señal de referencia llamada Oscilador Local (OL) cuya fase debe estar sincronizada con la fase de la portadora óptica de la información, lo cual implica que la recepción presente sensibilidad a la amplitud compleja del campo óptico, sin embargo una ventaja de la detección coherente es que es posible alcanzar el Límite Cuántico Estándar (SQL, *Standard Quantum Limit*) utilizando una señal intensa como OL.

Los formatos de modulación eficientes utilizados en detección coherente, producen una señal óptica con portadora suprimida, lo que hace necesario utilizar técnicas elaboradas de sincronización de fase, ya que los esquemas tradicionales de rastreo de portadora tales como el amarre de fase (PLL, Phase Loop Lock) no son aplicables en este caso, ya que no hay nada a que encadenarse[10]. Por lo que para efectuar la sincronización a partir de la señal de información misma (con portadora suprimida para economizar potencia) han sido propuestos varios enfoques heredados de la teoría de la detección y estimación estadística. Sus límites fundamentales en la detección y estimación óptica de parámetros han sido estudiados para canales ópticos clásicos en presencia de ruido de amplitud y de ruido de fase, este último causado por la anchura completa a media altura (FWHM, Full Width at Half-Maximum) en el espectro de láseres de semiconductor[11]. La aplicación de los resultados de la estimación por máxima similitud de una señal en presencia de ruido conduce a estructuras complicadas dificilmente implementables de manera práctica, por lo que se prefieren esquemas simplificados, resultando en estructuras que se conocen como Lazo de encadenamiento de fase óptico para portadoras piloto, o el Lazo de Costas para modulaciones para portadora suprimida [12]. Estas últimas están basadas en la medición de ambas cuadraturas del campo óptico recibido,

por ejemplo en la recepción de señales QPSK y aún en BPSK, en donde una cuadratura sirve para detección de datos y la otra para encadenamiento de fase[13].

Justificación e impacto

Con base a lo expuesto anteriormente se identifican los siguientes problemas fundamentales asociados a los enlaces de comunicaciones seguros empleando critpografia cuántica.

1.- Un problema es que una implementación basada en conteo de fotones, que es la propuesta original para un sistema de criptografía cuántica, no es viable para ser utilizado en conjunto con un sistema de comunicaciones actuales de alta velocidad por que requieren tecnologia adicional de alto costo (como los sistemas de enfriamiento) y velocidad de operación alcanza apenas el orden de los MHz, además de presentar baja eficiencia cuántica, por lo que una solución es el uso de tecnologías como la detección coherente en donde se utilizan dispositivos con alta eficiencia cuántica que pueden alcanzar velocidades de transmisión más altas.

3.- Algunos de los sistemas que están siendo estudiados hasta el momento se basan en sistemas de transmisión que utilizan láseres que miten pulsos formados por cientos de fotones, lo cual compromete la seguridad de la llave criptográfica al no transmitir un solo fotón por bit, y como consecuencia se ven en la necesidad de emplear técnicas más complejas como la modulación en fase en conjunto con la modulación en amplitud. En este trabajo en el receptor inciden pulsos que contienen un solo fotón por bit en promedio y se logra recuperar la información que contiene la trama de bits transmitida.

4.- El área de investigación de la criptografía cuántica es un tema emergente con gran potencial económico, ya que está siendo requerido por las compañías que ofrecen servicio de seguridad de la información en enlaces de comunicaciones en el estado de Baja California y a nivel mundial.

Por lo tanto el poder desarrollar un sistema de comunicación para implementar criptografia cuántica en comunicaciones ópticas es un área de oportunidad para las instituciones de investigación superior en la región. Además de que el contar con una tecnología nacional que refuerce la seguridad en los enlaces de comunicaciones da la oportunidad a México de contar con el potencial de independencia tecnológica en esta área, además de impactar en la seguridad de la información sensible en diversos campos de la economía, seguridad nacional y sociedad.

Objetivos

Análisis, diseño e implementación del un canal de comunicación cuántica en espacio libre, con receptor homodino en México para aplicaciones a la distribución de la llave criptográfica cuántica.

Asegurar que el canal criptográfico cumple con las características asociadas a los requerimientos de la criptografia para seguridad

Realizar el proceso de transmisión-recepción de información con estados débiles coherentes, esto implica la recepción de señales del orden de los femtowatts.

Determinar la viabilidad del uso de un receptor homodino para la reconstrucción de la función de distribución de cuasiprobabilidad de un estado cuántico sin utilizar técnicas de tomografía.

Propuesta del trabajo de tesis

Realizar una implementación en México de un canal cuántico para aplicación a un sistema de distribución de la llave criptográfica cuántica, ya que el contar con éste, se da el primer paso para el desarrollo de un sistema completo de comunicaciones cuánticas, por lo que se aborda exclusivamente la capa física (de acuerdo al modelo de referencia OSI).

La contribución de este trabajo de tesis es a cabo la medición directa de la función de cuasiprobabilidad ($\boldsymbol{Q}$) cuántica midiendo las dos cuadraturas del campo óptico en forma simultánea, es decir, no es necesario realizar una medición tomográfica tradicional, tomando en cuenta el efecto del ruido de vacío debido a la medición simultánea de las cuadraturas.

A lo largo de éste trabajo se se ve que:

1. Es posible el uso de un esquema homodino para detectar señales de muy bajo nivel de potencia y estados coherentes débiles muy cerca del límite cuántico estándar.
2. Es posible medir las dos cuadraturas en forma simultánea, aunque esto imponga un ruido adicional en el sistema (ruido de vacío).
3. Es posible emplear la potencia equivalente de 1 fotón por bit sin requerir uso de pulsos ultracortos que contienen cientos de fotones.
4. Es posible el uso de fotodetectores balanceados tipo p.i.n. que ofrezcan mejor velocidad de respuesta e integración a redes de comunicaciones ópticas modernas.
5. El canal de comunicaciones cuántico desarrollado podrá ser utilizado para sistemas de distribución cúantica de la llave criptográfica (QKD).

Organización del documento

En el Capítulo 1 se proporcionan los principios básicos de criptografía, de óptica cuántica y el funcionamiento del lazo de Costas, que utlizados en forma conjunta permiten la posibilidad de impementar un canal cuántico para criptografía cuántica que brinda la seguridad incondicional para la información transmitida.

En el Capítulo 2 se muestra los resultados de la caracterización del octapuerto homodino, su análisis teórico para estados coherentes débiles y se describe el montaje experimental.

En el Capítulo 3 se muestran y analizan los resultados experimentales obtenidos de la medición de las cuadraturas del campo óptico en forma simultánea para energías de un fotón por bit y menores.

Finalmente en el Capítulo 4 se presentan las conclusiones y trabajo a futuro.

1. Marco Teórico

1.1. Seguridad de la información en una red de comunicaciones.

Como se ha mencionado, la temática de la seguridad en el intercambio de información es un tema indispensable para el desarrollo de la actividad comercial y política en el mundo.

Se dice que un sistema es seguro si se logran reducir sus vulnerabilidades, y de acuerdo a la Organización Internacional para Estandarización (ISO, por sus siglas en inglés) y al Insitutto Nacional de Estándares (NIST), "se considera vulnerabilidad a cualquier flaqueza que pueda ser aprovechada para violar un sistema o la información que éste contiene" [14, 15] por lo que se tiene que estudiar el sistema para detectar los puntos débiles por los que pueda llevarse acabo una posible violación a la seguridad, es decir, detectar las amenazas; y si ésta última es en forma intencional se considera un ataque.

De acuerdo a estadisticas de la NIST el 65 % de los ataques son considerados internos, es decir, que provienen de personas que pertenecen o han pertenecido a la organización, mientras que del restante 35 % el 20 % es debido a desastres naturales y el 15 % se atribuye a "*Hackers*" y "*Crackers*" (es importante describir de manera clara las acciones que toman ambos grupos, por un lado los *"Hackers"* se identifican con el grupo de personas interesadas en comprender el funcionamiento de sistemas, identificar sus debilidades, y explotar funcionalidades no documentadas que ofrezcan la flexibiliad adecuada, para mejorar y recomendar correcciones en sistemas; mientras que el *"Cracker"* tiene como objetivo explotar las vulnerabilidades de los sistemas, sin comunicarlo a otros que podrían corregir la vulnerabilidad, con el fin de obtener algún tipo de ganancia ilícita). En ocasiones los Crakers dirigen sus ataques vía algoritmos computacionales, o directamente sobre el medio físico[16].

Aún cuando se han generado recomendaciones por parte de la ITU-R para la implementación de los sistemas de telecomunicaciones en red (ITU-R X.800), la cuantificación de la seguridad del sistema queda en función de los criterios que el usuario emplee para considerar segura su información durante un tiempo determinado, es decir, hasta que se logre romper el código

con el que encriptó su información. Los atacantes del sistema suelen emplear técnicas que buscan aplicar el menor esfuerzo posible por vulnerar la seguridad del sistema, incluyendo para ello, acciones de ingeniería social (es decir un análisis de los usos y costumbres de los usuarios, y su candidez), robo directo de las llaves de encriptación, o modificación explícita de los programas, para ganar acceso al sistema mediante puertas traseras o *backdoors*. En los sistemas de transmisión de información, para dotar el enlace con algún tipo de seguridad, se ha empleado la criptografía como un esquema básico para ofrecer seguridad en el intercambio de información privada, si bien existen métodos sofisticados que ofrecen protección de información, ninguno de ellos basados en algoritmo computacional ofrece seguridad incondicional.

1.2. Criptografía.

La palabra criptografía proviene del griego κρύπτω *(krypto*, oculto), y de γράφω *(graphos*, escribir), lo que significa "escritura oculta". Es considerada una ciencia, la cual permite cifrar (encripción) y descifrar (desencripción) información para el intercambio de mensajes, que deberán ser leídos solo por la persona a quien va dirigida y es quien tiene la clave para descifrar el mensaje [17, 18]. La importancia de la secrecía de cierta información y el cifrado de ésta se remonta desde tiempos antiguos. Se sabe que los egipcios hace 4,500 años utilizaron jeroglíficos no de uso común para ocultar información durante las guerras (caso conocido es la máquina *enigma*, empleada por el ejército alemán, cuyo sistema fué muy dificil de romper para los ejércitos aliados). Desde entonces los métodos criptográficos han evolucionado en complejidad y han tenido un papel decisivo en la historia; por ejemplo, en México en los inicios del siglo XX, se utlizó el método de sustitución simple como herramienta criptográfica durante las campañas militares del General Porfirio Díaz, método que utilizaba incluso para su correspondencia personal [19] , este método consiste en sustituir una letra del alfabeto utilizado por otra letra del mismo alfabeto.

En 1917, Gilbert S. Vernam propuso un sistema de encriptamiento el cual se conoce como Cifrado Vernam o "*One-time Pad*" (OTP), que se basa en el uso de una llave criptográfica por una sola ocasión. El texto del transmisor se combina con una serie de bits generados en forma pseudoaleatoria (los cuales forman la llave criptográfica) por medio de una operación XOR para generar un texto cifrado. [20] El texto y la llave son de la misma longitud en bits. Este tipo de cifrado aún se utiliza con frecuencia en Internet.

La era de la criptografia moderna se considera que inicia con C. Shannon, quien publicó en 1949 el artículo "*Communication Theory of Secrecy Systems*" en el Journal Técnico de los

Laboratorios Bell [21], que en conjunto con "*A Mathematical Theory of Communications*" (1948) inicaron con el establecimiento de las bases teóricas para la criptografia. A partir de ese momento para el proceso de encriptamiento, al mensaje se le aplica una técnica basada en algoritmos computacionales para que parezca totalmente ininteligible a cualquier receptor que no cuente con la clave de descifrado. Sin embargo, en el trayecto hacia el sistema receptor el mensaje puede ser interceptado y puede aplicarsele una técnica complementaria, es decir criptoanálisis, con el fin de recuperar el mensaje.

Por lo tanto los sistemas de seguridad actuales se basan en sistemas convencionales de encriptamiento de información que consisten en algoritmos computacionales que no son incondicionalmente seguros, tales como el código de encriptamiento RSA (Rivest, Shamir y Adleman,1970) ampliamente utilizado[3]. Otro esquema que emplea criptografía para transmitir información, es el sistema PGP, desarrollado por Philip R. "Phil" Zimmermann, Jr.

Una de las principales debilidades de éstos esquemas es el que es necesario distribuir la llave criptográfica, requerida para recuperar el mensaje, ya que si la llave es interceptada por un atacante, el atacante puede tener la capacidad de robar la información transmitida.

La criptografía cuántica es capaz de garantizar la seguridad incondicional por que está basada no en un algoritmo computacional sino en las propiedades cuánticas de del fotón que contiene la llave criptográfica[4, 5].

1.3. Sistemas de distribución de la llave criptográfica.

Uno de los principales problemas en la criptografía es la distribución de la llave criptográfica de forma segura entre los usuarios correspondientes. En 1976 Martin Hellman y Whitfield Diffie en la Universidad de Stanford inventaron un método para transferir la llave criptográfica en forma segura por medios digitales, el método de intercambio es conocido ahora como "Método Diffie-Hellman" el cual consiste en la distribución de una "llave pública" y una "llave privada" [22].

1.3.1. Criptografía con llave pública (criptografía asimétrica):

En esta forma de criptografía el usuario tiene un par de llaves criptográficas, una pública y una privada. La llave privada se mantiene en secreto, mientras que la llave pública se distribuye. existe una relación matemática entre las ambas, pero la llave privada no puede derivarse de la llave pública. Un mensaje encriptado con la llave pública puede desencriptarse solo con la llave

Figura 1.1.: En la figura de la izquierda Alice y Bob intercambian información utilizando un sistema de criptografia clásica sin darse cuenta de que están siendo espiados por Eva. A la derecha Alice y Bob utilizan una distribución de la llave criptográfica en el dominio cuántico y pueden darse cuenta cuando son espiados.

privada correspondiente. La seguridad de esta llave reside en la complejidad computacional para lograr la factorización de dos múmeros primos, y es seguro sólo por el tiempo en el cual se calcula que el esquema de seguridad no será roto, aunque esta predicción debe tomarse con precuaciones, por ejemplo, en 1977 Rivest estimó que la factorización de números de 125 dígitos requerirían 40 cuatrillones de años, sin embargo en 1994 fué factorizado un número de 129 dígitos [23]. Los sistemas criptográficos actuales consideran prudente usar claves de 512 dígitos, aunque los expertos sugieren números 1024 dígitos, sin embargo en el año 2012 la empresa DigiCert's [24] utilizó una llave de 2048 bits para certificar una llave como segura.

Los sistemas electrónicos y el incremento en la capacidad de cómputo de los sistemas, indican que cada vez es más dificil ofrecer una seguridad incondicional cuando se emplean los esquemas tradicionales criptográficos, de ahí que surja la importancia de contar con un sistema de comunicación que permita la transmisión de llaves criptográficas con mínima o nula posibilidad de intercepción del mensaje.

En un sistema criptográfico clásico, el transmisor, que de ahora en adelante lo llamaremos Alice, y el receptor al cual llamaremos Bob, intercambian información que contiene la llave que puede desencriptar el mensaje enviado. Las características de la señal física que lleva la información, ya sea óptica o eléctrica permiten el espionaje sin cambiar el estado de los bits de información que continúa su trayectoria hacia Bob, ya que cada bit contiene miles o millones de electrones o fotones, por lo que si se extrae un porcentaje pequeño del total, ni Alice ni Bob se darán cuenta de lo sucedido ya que el efecto en el BER no será perceptible.

1.3.2. Criptografía cuántica

Una propuesta para resolver el problema de seguridad condicional de la criptografía clásica, es la criptografia cuántica, que se basa en el uso del estado cuántico de un solo fotón para la distribución de la llave criptográfica, lo que permite que se puedan distinguir en caso de espionaje ya que está basada en los siguientes teoremas:

- Es imposible medir los estados de un sistema cuántico sin perturbarlo. Un sistema cuántico es un conjunto de caracteristicas físicas, las cuales por su naturaleza no es posible medir una característica o variable sin afectar simultáneamente el estado de las demás variables, como consecuencia el estado cuántico del sistema cambia.
- Es imposible medir simultáneamente un solo fotón con dos bases conjugadas. Entenderemos como bases conjugadas como dos caracteristicas específicas de un sistema cuántico que por su naturaleza se consideran ortogonales entre sí, por ejemplo, estado de polarización, estado de fase y spín.
- Es imposible copiar un fotón sin destruirlo de acuerdo al teorema de "no clonación", este teorema propuesto por establece Wotters y Zurek [25]establece que en un proceso de medición de un estado cuántico se pierde parte de la información de un sistema al perturbar el estado cuántico, por lo cual no es posible reproducirlo de manera idéntica al original.

Con base a esos teoremas, en 1984 Charles Bennet y Gilles Brassard propusieron el primer sistema criptográfico conocído hoy como el protocolo BB84, el cual permite una distribución segura de la llave criptográfica (QKD, Quantum Key Distribution) [4, 26]. En este protocolo, Alice elige una serie de bases que representan los bits a transmitir, en forma aleatoria, la combinación de los bits y las bases forman la llave criptográfica utilizando bits individuales, es decir que representan el estado cuántico del fotón, éstos son los llamados bits cuánticos o qbits, que se explicarán mas adelante en este capítulo. Como se muestra en la figura Figura 1.2 para su implementación se determinan dos bases con dos estados posibles en cada base; si se utiliza por ejemplo, el estado de polarización de la luz para representar un estado, se podría tener entonces la base 1 (B1) con dos estados de polarización: polarización vertical (V) y polarizacion horizontal (H), que servirán para representar el 1 y el 0 lógico, mientras que la base 2 (B2) los estados de polarización serán lineales a $+45^0$y -135^0 que representarán a su vez el 1 y 0 lógicos. Alice elige aleatoriamente entre una base y otra para el envío de los 1s y 0s por el canal cuántico. En el receptor cada vez que Bob recibe un bit tiene que elegir aleatoriamente entre una de las dos bases y procede a medir. En la Figura 1.2 se muestra un ejemplo de la transmisión y recepción de los bits de la llave empleando el protocolo BB84.

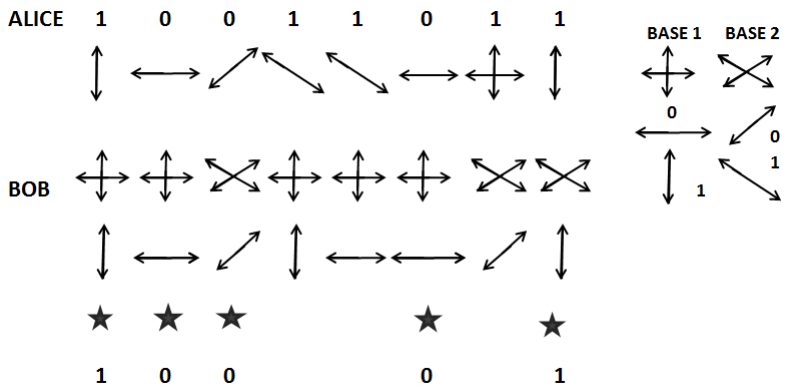


Figura 1.2.: Ejemplo del protocolo BB84 para la transmisión de la llave criptográfica entre Alice y Bob. La estrella indica que coincidieron las bases que ambos eligieron.

Una vez que se ha transmitido la llave criptográfica es necesario llevar a cabo los procesos de reconciliación de la llave y corrección de errores para finalmente llegar a la destilación de la misma que desencriptará el mensaje [27].

En la figura Figura 1.3 se muestra el modelo de capas de un sistema de distribución cuántica de la llave propuesto por Joguet et al[28]. Como se puede apreciar el primer nivel está en el dominio fotónico y es en donde se ubica en el nivel (o capa) cuántica, el resto del sistema se encuentra en el dominio clásico; es lo que se llama una red híbrida; este tipo de redes son por lo pronto, la solución para los sistemas de comunicaciones que buscan la seguridad en la transmisión de datos dado que los enlaces cuánticos están limitados por distancias hasta de 100 Km. En paralelo, otros grupos de investigación están desarrollando sistemas QKD, por ejemplo en Bienfang *et. al.* se muestran resultados de un sistema QKD en espacio libre, mientras que en Peev *et. al.* los enlaces del sistema son fibrados [29, 30]. Se han tenido buenos avances en el desarrollo de sistemas QKD en donde por ejemplo el proyecto Tokio es el más avanzado y se espera que el desarrollo de repetidores cuánticos permitirá distancias mucho mayores a los que se han alcanzado actualmente [31, 32, 33].El primer paso es por lo tanto, asegurar que el óptimo funcionamiento del canal cuántico, es decir, un canal de comunicación que es capaz de transmitir información a niveles cuánticos, que precisamente es el tema de éste trabajo doctoral, para posteriormente estar en condiciones de aplicar el resto de un protocolo criptográfico.

De acuerdo al modelo de Joguet, el primer nivel es en donde se lleva a cabo el intercambio de la llave en bruto (*raw key*), está en el dominio óptico y es un enlace punto a punto. El resto

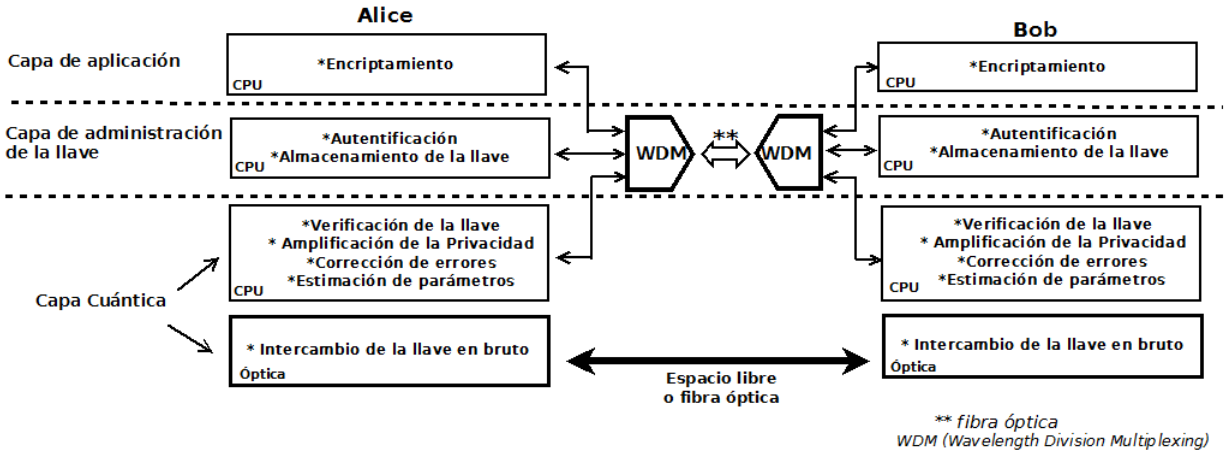


Figura 1.3.: Modelo de capas de un sistema de distribución cuántica de la llave criptográfica propuesto por Jouguet et al.

del intercambio de información se realiza vía *software* en canales públicos. De este modo, Alice y Bob utilizan el canal cuántico para el envío de la información óptica cuántica (los bits) y utilizan canales públicos para el resto del protocolo, así como para el envío del mensaje encriptado.

Las primeras propuestas para canal cuántico, como las utilizadas en el BB84, se basan en sistemas trasmisores con fuentes de un solo fotón mientras que el receptor se requieren de igual forma detectores de un solo fotón[34, 35, 36] . Las desventajas de esta tecnología es que las fuentes de un solo fotón son sistemas sofisticados y con alto costo, mientras que los sistemas en el receptor están basados en receptores APD en modo "compuerteado" los cuales presentan alta corriente de oscuridad, baja eficiencia (aproximadamente 20 %), requieren sistemas de enfriamiento, trabajan a velocidades bajas (del orden de los MHz) [37]. Esta caracteristica implica que no son compatibles con los sistemas de comunicaciones de alta velocidad actuales. Las ventajas son que no requieren de una señal extra de referencia, y la decisión para determinar si llegó un 1 o un 0 es inmediata, a estos sistemas se les conoce como Sistemas de Distribución de la llave criptografica de Variables Discretas (DV-QKD, Discrete Variables - QKD).

Dadas las desventajas para una implementación práctica de las DV-QKD, en la última década se han propuesto técnicas de QKD que aprovechan el estudio previo, conocimiento y desarrollo de tecnologías como láseres de pulsos cortos y esquemas de detección coherente,[38, 39, 40], las cuales tienen como ventajas el uso de fotoreceptores del tipo p.i.n., los cuales presentan mejor eficiencia cuántica, no requieren bajas temperaturas para su operación como en el caso de los receptores APD, son capaces de trabajar a velocidades del orden de los GHz y se puede trabajar con una señal cerca de Límite cuántico estándar (SQL, por sus siglas en

inglés, que se describirá mas adelante), por lo que el ruido dominante es el ruido cuántico. La desventaja es que requieren de una señal de referencia externa y es necesario un proceso de post detección para decidir si se recibió un 1 ó 0 lógico[41]. Esta técnica es la denominada Distribución Cuántica de la Llave con variables continuas (CV-QKD ó Continous Variable-Quantum Key Distribution, por sus siglas en inglés).

En las propuestas de CV-QKD en lugar de utilizar fuentes de un solo fotón, hacen uso de fuentes láser fuertemente atenuadas con potencias de salida equivalentes a la de cientos de fotones o menores, como por ejemplo en Grosshans 2003 [42, 43], sin embargo la transmisión de más de un solo fotón corre el riesgo de ser interceptada por un espía y que éste pueda recuperar la información a partir de unos cuantos fotones; por lo anterior tomando en cuenta la necesidad de seguridad se prefiere que la llave sea encriptada en fotones únicos. En un intento por mejorar la seguridad utilizando fuentes atenuadas se ha propuesto utilizar estados cuánticos como señuelos (*decoy states*), pero esto añade complejidad a su implementación por que se basa en la transmisión de pulsos de diferente amplitud y fase utilizando un atenuador óptico variable para que el número de fotones del estado coherente transmitido sea diferente en cada símbolo [44, 45, 46]. En la tabla Tabla 1.1 se muestran algunos ejemplos del estado del arte de la implementación de los sistemas QKD en laboratorios de primer nivel en el mundo.

La propuesta de esta tesis doctoral, se basa en la recepción de estados coherentes débiles, procedentes de pulsos láser fuertemente atenuados con la potencia equivalente a la de un sólo foton con CV-QKD, mientras que en la recepción la implementación se basa en esquema interferométrico con detección coherente, lo que nos permite el uso de fotodetectores tipo p.i.n y las ventajas que éstos ofrecen comparados con los APD. En un sistema de detección coherente Alice codifica los bits de la llave criptográfica en las cuadraturas del campo eléctrico (amplitud y fase) de los estados coherentes que envía, mientras que Bob mide el valor de las cuadraturas utilizando un detector homodino con alta sensibilidad y bajo ruido electrónico dado que se reciben potencias ópticas del orden de los femtowatts. Este detector está basado en un octapuerto homodino el cual se describe en la Sección 1.6.

1.4. Conceptos de Teoría de la Información.

En 1948 Claude Shannon publicó "La Teoría Matemática de las Comunicaciones" [21, 47], en la que describió cómo se puede medir la información proporcionada por una fuente de datos, ya sea transmisión telefónica, radio, enlace entre computadoras, enlace satelital, etc. También demostró que es posible medir la capacidad de un canal empleado en el proceso de

Tabla 1.1.: Estado del arte en la implementación de los sistemas de distribución de la llave criptográfica cuántica.

AUTOR	TECNOLOGÍA/ PROTOCOLO	CACARTERÍSTICAS DEL ENLACE	FIBRA / ESPACIO LIBRE	COMENTARIOS	Journal/AÑO DE PUBLICACIÓN
Jouguet et al.	CVQKD	*17.7Km, pulsos @1550nm, *tasa de repetición =500KHz, *Tiempo del pulso=100nseg, *Modulación de amplitud y fase	Fibrado.		Optics express 2012
Pomerico et al	Pair of photons	Frecuencia= 4MHz	Fibrado.		Optics express 2012
Stuki, Legré, Robordy, Zbiden, Gisin et al.	BB84 and SARG04 pulsos débiles	Enlace punto a punto, * Raw key 4-5 minutos	*1 par de fibras QKD, *Bit rate= 10Gbps, *Enlace más largo=17.1Km, * Pérdidas = -4.6dB	Protocolo SARG04 más eficiente para largas distancias. Require sistema de enfriamiento a -40°C	New Journal on Physics 2011
Sasaki, Legré, Robordy, et al. Tokyo QKD project.	6 sistemas diferentes QKD integrados. Red dorsal cuántica (*Quantum Back Bone*) BB84,SARG04 y DPS-QKD.	*Enlace mas largo=90Km, * pérdidas =27dB, *pulsos@1550nm. * Tasa de repetición=1.25Gbps, *Duración del pulso=100ps.	*Fibrado, *λ=1550.92nm, *Long onda enlace cuántico=1549.32nm *WDM	El nivel de seguridad depende de la clase de números aleatorios y el método de destilación de la llave.	Optics Express 2011
Scarani, Acín, Robordy and Gisin.	SARG04	*Pulsos débiles, *Utiliza dos estados no ortogonales.			Phys. Rev. Lett. 2004
Weier		*Pulsos atenuados, *Basado en el estado de polarización de los fotones.	*Espacio libre, *d=4Km, *QBER=3.5%		Fortsch.Phy 2006
Elboukhari et al. (a Survey)	Protocolo COW (*Coherent One-Way protocol*). Gisin 2004.	La llave se obtiene a partir de la medición del tiempo de arribo de los fotones.			Int. Journal of computer science 2010
Qing Xu et al.	Conteo de fotones	Distancia = 11 Km, *Qbit rate = 4Mbps, * λ=1550nm	Fibrado		Journal of Lightwave Tech. 2009

la comunicación a partir del conocimiento de su ancho de banda y la relación señal a ruido de la señal que contiene los datos. Ésta teoría fué posteriormente la base para el desarrollo de los métodos de corrección de errores, compresión de señales, supresión de ruidos y redundancia para el mejoramiento de las comunicaciones. En 1949, Shannon publica la "Teoría de las comunicaciones de sistemas secretos" [48], en la que propuso técnicas matemáticas para analizar los sistemas de criptografía, y muestra que es válido tratar a un sistema criptográfico como un sistema no criptográfico ruidoso, por lo que era posible utilizar las técnicas empleadas en la teoría de 1948.

Los estudios y teoría derivada de los documentos de Shannon son ahora la base de lo que comprende actualmente la Teoría de la Información, cuyos elementos básicos son la fuente de la información (y sus diferentes tipos), la capacidad de canal de transmisión, el mensaje que son los datos que viajan por un canal, el código empleado para representar el mensaje, y la información. Ahora bien, la información que contiene un mensaje se puede medir cuantitativamente a partir de la entropía (H), la cual mide la incertidumbre del mensaje, también se puede considerar como la cantidad de información promedio que contienen los símbolos usados [22, 49], y se expresa con la Ecuación 1.1 la cual representa la entropía conjunta

$$H\left(X,Y\right)=-\Sigma_{x,y}\ p\left(x,y\right)\ log\left[p\left(x,y\right)\right] \tag{1.1}$$

en donde (X)y (Y) son variables aleatorias independientes que tienen asociada una distribución de probabilidad $p\left(x\right)$y $p\left(y\right)$ respectivamente. La entropía conjunta proporciona una medida de la información total que contiene el sistema X,Y. El análisis de Shannon fué descrito en principio para sistemas discretos, pero posteriormente se generalizó para sistemas con variables continuas.

Una medida derivada del conocimiento de la entropía del sistema es la Información Mutua(I)(ver Ecuación 1.2), que es la información relativa a una variable apartir del conocimiento de la segunda variable.

$$I\left(X,Y\right)=H\left(X\right)-H\left(X/Y\right) \tag{1.2}$$

En un sistema criptográfico, el concepto de Información mutua nos proporciona una medida de la información que hay entre el Alice y Bob I_{AB}, es decir en nuestro caso $I(X,Y)=I_{AB}$,

la cual se puede reescribir como la Ecuación 1.3 que toma en cuenta la probabilidad de error P_e calculada a partir de los datos recibidos.

$$I_{AB} = 1 + P_e(I)\ log_2 P_e(I) + (1 - P_e(I))\ log_2(1 - P_e(I)) \tag{1.3}$$

en donde P_e es para una variable aleatoria binaria es

$$P_e = Q\ \left(\sqrt{\frac{2E_b}{N_0}}\right) \tag{1.4}$$

Q es la función de error complementaria, $E_b$es la energía de bit y N_0es la energía de ruido

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp\left(-\frac{u^2}{2}\right)\ du \tag{1.5}$$

El máximo valor de la Información mutua nos da la medida de la cantidad de información que puede ser transmitida en un canal, es decir la Capacidad de canal C, que se representa con la Ecuación 1.6[1].

$$C = Blog_2\left(1 + \frac{S}{N}\right) \tag{1.6}$$

en donde B es el ancho de banda de la señal medido en Hertz, S es la potencia promedio de la señal y N es la potencia promedio del ruido. La relación $\frac{S}{N}$ es la denominada Relación señal a ruido (SNR, por sus siglas en inglés), el log_2 es debido al uso de un canal binario, la capacidad de canal es medida en número de símbolos/segundo.

Para Bob, las pérdidas que puede observar debido a la prescencia de un espía (Eve) son equivalentes a las que provoca el ruido, ya que representan pérdidas de la información que le envió Alice, por lo que se puede considerar el impacto de Eve como ruido en exceso en el sistema. Es posible tratar de calcular la Información mutua entre Bob y Eva (I_{BE}), la cual debe cumplir con la condición $I_{AB} > I_{BE}$ para considerar que el sistema ofrece seguridad incondicional haciendo uso de la Ecuación 1.7[42]

$$I_{BE} = \frac{1}{2}\, log_2 \left[(\eta\, G)^2 \,(V + \chi) \left(\frac{1}{V} + \chi \right) \right] \tag{1.7}$$

en donde η es la eficiencia total del receptor (Bob) que en nuestro experimento es igual a 0.7 (70 %) tomando en cuenta las pérdidas por acoplamiento y la eficiencia cuántica de los fotoreceptores, es un pa'rametro importante por que es un parámetro asociado con la figura de ruido del sistema, a mayor eficiencia mejor figura de ruido. La variable G es la eficiencia total del canal la cual se considera igual a 1 en este caso para considerar sólamente el impacto de la intromisión de Eva con el ruido en exceso, V es la varianza del estado cuántico en el transmisor el cual toma en cuenta el ruido cuántico y la varianza de Alice (el estado cuántico preparado en el transmisor) y χ es el ruido equivalente medido en la entrada del receptor el cual se calcula con la Ecuación 1.8

$$\chi = \frac{1 - \eta\, G}{\eta\, G} + \varepsilon \tag{1.8}$$

ε representa el ruido por imperfecciones fuera del sistema de Bob y es este ruido el que puede ser controlado por Eva. Para determinar si el sistema ofrece seguridad incondicional es necesario calcular la Tasa de la llave criptográfica segura por pulso que está representada por la Ecuación 1.9, en donde $\beta \leq 1$es la eficiencia de la reconciliación de la llave, que en los sistemas QKD tienen valores tipicos de 0.9 y 0.898 [50], por debajo de esos parámetros se considera que la distribución de la llave no es segura.

$$\Delta I = \beta I_{AB} - I_{BE} \tag{1.9}$$

1.5. Conceptos de Óptica Cuántica

Una vez expuestas las caractarísticas del tratamiento estadístico y los requerimientos que exige la Teoría de la Información, para poder ofrecer un enlace seguro, es importante relacionar la información con los conceptos correspondientes de la óptica cuántica.

1.5.1. Bit clásico y Bit cuántico

El concepto con el que se puede representar información es el bit clásico, el cual puede tomar el valor de 1 ó 0 sin estados intermedios, en donde en el receptor se tiene una probabilidad (p) de recepción de dichos estados de p(1) y p(0) respectivamente, en donde p(0) + p(1) = 1. En un sistema cuántico la información se representa con el Bit Cuántico también conocido como qubit, el cual está formado por una superposición de estados cuánticos, es decir, puede ser 1 y 0 en forma simultánea. [51, 52] y se representan como $|1\rangle$y $|0\rangle$, es decir, un estado cuántico de dos dimensiones se pueden representar con la Ecuación 1.10

$$|qubit\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle \tag{1.10}$$

en donde

$$|\alpha_0|^2 + |\alpha_1|^2 = 1 \tag{1.11}$$

Una vez que el qubit es observado se decide cuál es su valor, que puede ser "cero" con la amplitud de probabilidad de $|\alpha_0|^2$ o el valor de "uno" con la amplitud de probabilidad de $|\alpha_1|^2$. Ahora bien, lo que se observa finalmente es un valor promedio para el estado cuántico medido, es decir su densidad de probabilidad ψ , donde $|\psi\rangle = \sum \alpha_i |\psi_i\rangle$, éste es denominado "el observable".

Los observables en una medición cuántica los cuales llamaremos A y B obedecen al principio de incertidumbre de Heisenberg, el cual establece que no se puede determinar simultáneamente y con presición un par de variables como la posición x y momento p de un objeto. Si se tiene mayor precisión en la posición, menos presición se tendrá en el momento y viceversa, esta relación se expresa con la Ecuación 1.12. Tomando como fundamento este principio en nuestro sistema se pueden representar la relación de incertidumbre de nuestros observables de acuerdo a la Ecuación 1.13[53]

$$\Delta x \Delta p \geq \frac{\hbar}{2} \tag{1.12}$$

$$\left\langle (\Delta A)^2 \right\rangle \left\langle (\Delta B)^2 \right\rangle \geqslant \frac{1}{4} \left\| \langle [A, B] \rangle \right\|^2 \tag{1.13}$$

en donde

$$\Delta A = A - \langle A \rangle \tag{1.14}$$

en donde A es el valor medido y $\langle A \rangle$ es el valor promedio del observable y $\hbar$ es la constante de Planck normalizada, es decir la constante de Planck (h) expresada en radianes, y $h = 6.6261 \times 10^{-34} Js$

1.5.2. Función de Distribución de Wigners y Función *Q.*

Dado que en la mecánica cuántica no se pueden observar directamente los estados cuánticos, se hace uso de una herramienta que permite predecir la estadística de las observaciones en una medición cuántica, esta es la Distribución de Probabilidad de Wigner, la cual cuantifica la probabilidad de encontrar el valor de las cuadraturas (q y p), representadas como estados cuánticos $|x + ip\rangle$, en un espacio de fase de una medición simultánea [54, 55]. Como veremos más adelante, en este trabajo las cuadraturas q y p representarán a nuestros observables I (In- phase) y Q (quadrature) respectivamente en el octapuerto y se podrá obtener una representación gráfica del comportamiento estadistico de los observables. La distribución $W(q, p)$ representa la analogía mas cercana entre un sistema cuántico y la distribución de probabilidad en un sistema clásico y se puede considerar que se comporta como una distribución de probabilidad conjunta. Las distribuciones de Wigner para el estado de vacío y un estado coherente se representan con la Ecuación 1.15 y la Ecuación 1.16, en donde $(q^2 - q_0^2)$ y $(p^2 - p_0^2)$ representan el estado coherente desplazado de su estado de vacío $(-q_0^2 - p_0^2)$ y gráficamente con la Figura 1.4 y Figura 1.5 respectivamente [54, 56, 57].

$$W_0(q, p) = \frac{1}{\pi} e^{(-q_0^2 - p_0^2)} \tag{1.15}$$

$$W(q, p) = \frac{1}{\pi} e^{(-(q^2 - q_0^2) - (p^2 - p_0^2))} \tag{1.16}$$

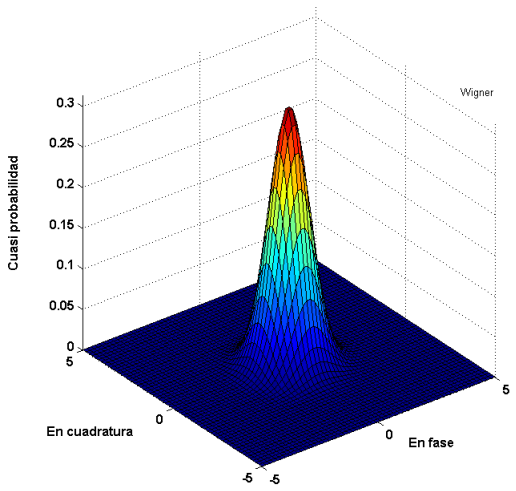


Figura 1.4.: Representación gráfica de la función de distribución de Wigner para un estado coherente de vacío.

Sin embargo, la función de Wigner puede dar resultados negativos, por lo que se utiliza un procedimiento matemático para suavizar la función de Wigner convolucionándola con una distribución Gaussiana similar a la que presenta un estado de vacío, el resultado es conocido como la función Q o función de quasi-probabilidad de Husimi [54], la cual es positiva y es normalizada a la unidad. La función Q puede ser vista como densidades de probabilidad y es representada con la Ecuación 1.17, Figura 1.6.

$$Q(q,p) = \frac{1}{2\pi} e^{\left[-\frac{1}{2}(q-q_0)^2 - \frac{1}{2}(p-p_0)^2\right]} \tag{1.17}$$

1.6. Sistema de comunicación óptica segura con esquema homodino y fotodetectores balanceados.

Los sistemas de recepción coherente para sistemas de comunicaciones eficientes con portadora suprimida han sido ampliamente estudiados [13] y han sido evidentes las ventajas que ofrecen con respecto a los sistemas de detección directa. Los primeros presentan una mayor sensitividad, permitiendo alcanzar el límite cuántico estándar en la medición de la señal, cosa que no es posible lograr en los sistemas de detección directa; además en las redes de

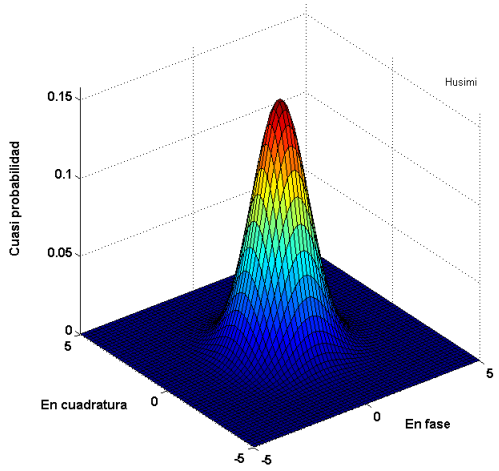


Figura 1.5.: Representación gráfica de la función de distribución $\boldsymbol{Q}$ para un estado coherente

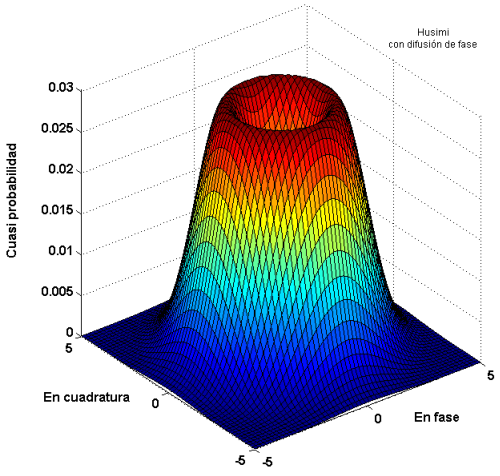


Figura 1.6.: Representación gráfica de la función $\boldsymbol{Q}$ para un estado coherente con fase difundida.

datos de alta velocidad se ha comprobado que los sistemas de detección coherente reducen la latencia en los enlaces y reducen el uso de sistemas de compensación por dispersión en los enlaces fibrados [13, 58]. En este trabajo se implementó un sistema de transmisión y detección coherente BPSK autohomodinado.

En un sistema homodino la señal de datos y el oscilador local deben estar encadenados en fase para la detección de la señal que contiene los datos, como se observa en la Figura 1.6, la función $\boldsymbol{Q}$ es útil para respresentar estados con fase difundida.

En la Figura 1.7 se muestra el principio de un sistema homodino óptico general que tiene la capacidad de medir una sola de las cuadraturas de la señal de salida. La señal que contiene los datos E_S (Ecuación 1.18) se mezcla con una señal que proviene de un oscilador local E_{OL} (Ecuación 1.19) por medio de un divisor de haz 50/50 en donde la potencia óptica se representa con la Ecuación 1.20, la señal del oscilador local tiene un potencia mucho mayor comparado con la de datos ($P_{OL} \gg P_s$).

$$E_s = \sqrt{P_s}\, e^{j(\omega_0 t)}\, e^{(\omega_C t+\theta)} \tag{1.18}$$

$$E_{OL} = \sqrt{P_{OL}}\, e^{j\omega_0 t} \tag{1.19}$$

$$P(t) = \frac{1}{2}\,|E_s + E_{OL}|^2 \tag{1.20}$$

En las ecuaciones anteriores la frecuencia angular de la señal óptica está representada por ω_0 mientras que ω_C es la frecuencia angular de la señal portadora de los datos. Las unidades del campo eléctrico están en V/m, mientras que las unidades de la potencia están en Watts.

En éste esquema de cuatro puertos, los dos haces que emergen del divisor de haz inciden en un par de fotodetectores balanceados (BHD por sus siglas en inglés) en donde la diferencia de corrientes generadas en cada uno de ellos será amplificada y será nuestro observable. En éste sistema es posible medir una de las dos cuadraturas del campo óptico, si se requieren medir las dos cuatraturas se tiene que realizar de forma conmutada [17].

En cada una de las salidas del divisor de haz el campo eléctrico se representa con la Ecuación 1.21 y Ecuación 1.22.

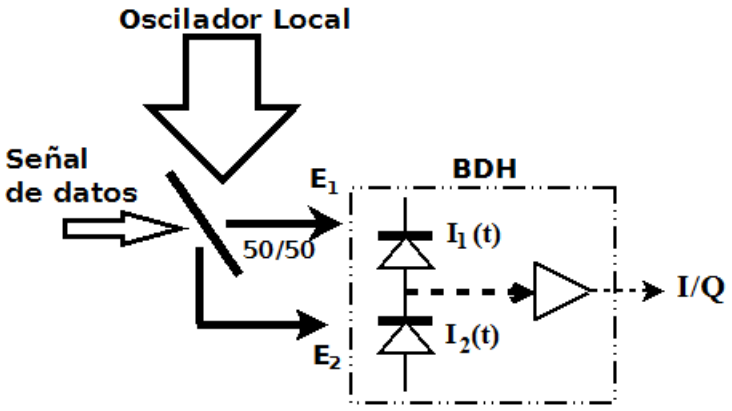


Figura 1.7.: Receptor de cuatro puertos para la detección de las cuadraturas I y Q en forma conmutada.

$$E_1 = \frac{1}{\sqrt{2}}\left(E_S + E_{OL}\right) \tag{1.21}$$

$$E_2 = \frac{1}{\sqrt{2}}\left(E_S - E_{OL}\right) \tag{1.22}$$

la potencia óptica asociada al campo eléctrico de la señales ópticas es dada por la Ecuación 1.23

$$P(t) = \frac{1}{2}\ |E_{OL} + E_S|^2 \tag{1.23}$$

mientras que la fotocorriente generada por la incidencia de un haz óptico en un fotodetector se expresa de acuerdo a la Ecuación 1.24, en donde $\Re$ representa la responsividad del fotodetector en A/W.

$$I = \Re\, P_{incidente} \tag{1.24}$$

por lo tanto las corrientes generadas en cada uno de los fotoreceptores son

$$I_1(t) = \frac{1}{2}\,\Re\left(P_s + P_{OL} + 2\sqrt{P_s P_{OL}}\,\cos(\omega_c t + \theta) + n_{q1}\right) \tag{1.25}$$

$$I_2(t) = \frac{1}{2}\Re\left(P_s + P_{OL} - 2\sqrt{P_s P_{OL}}\cos(\omega_c t + \theta) + n_{q2}\right) \tag{1.26}$$

en donde P_s es la potencia de la señal de datos, P_{OL} es la potencia del OL, ω_c es la frecuencia angular del oscilador local, θ fase de la señal modulada y la del oscilador local y n_q es el ruido cuántico del fotoreceptor. Éste ruido se debe a la naturaleza aleatoria de la incidencia de los fotones en el fotodetector, que es caracterizada por una distribución de probabilidad de Poisson. Por lo tanto la corriente de salida de uno de los fotoreceptores balanceados es la resta de $I_1(t)$ y $I_2(t)$ como está expresado en la Ecuación 1.27

$$I_{BHD} = I_1 - I_2 = 2\,\Re\sqrt{P_s P_{OL}}\cos(\omega_c t + \Delta\theta) \tag{1.27}$$

Para poder medir ambas cuadraturas en forma simultánea se propone un esquema de 8 puertos como el que se muestra en la Figura 1.8. El efecto de ruido de vacío se refleja como un incremento de la varianza del valor promedio de los observables (ver figura Figura 1.9) en el caso de un receptor homodino de 8 puertos como el que se muestra en laFigura 1.8, las expresiones que representan las corrientes de salida de los fotodetectores BHD1 y BHD2 Ecuación 1.28 y Ecuación 1.29

$$I_{BHD_1} = I_1 - I_2 = 2\,\Re\sqrt{P_s\,P_{OL}}\,\cos(\omega_c t + \Delta\theta) \tag{1.28}$$

$$I_{BHD_2} = I_1 - I_2 = 2\,\Re\sqrt{P_s\,P_{OL}}\,\sin(\omega_c t + \Delta\theta) \tag{1.29}$$

cuando los dos brazos están balanceados, el término de DC se elimina al restarse las corrientes. Se han reportado esquemas experimentales que utilizan una implementación similar y llegan a obtener ambas cuadraturas pero en forma conmutada, es decir, no es simultáneamente [17].

A partir de la obtención de las corrientes de salida de los fotodetectores, es posible observar las señales con un osciloscopio, los voltajes esperados se describen con la Ecuación 1.30 y Ecuación 1.31.

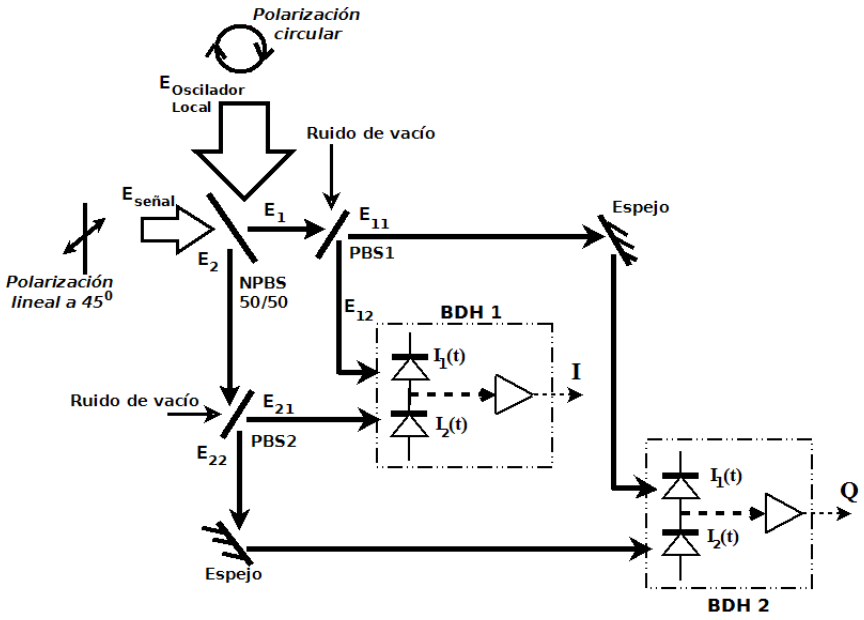


Figura 1.8.: Señales de entrada al octapuerto y salidas de los divisores de haz polarizado y no polarizado.

$$V_I(mV) = F_R\, G_{BHD} \left(\frac{\sqrt{P_s P_{OL}}}{2} \right) \cos\theta \tag{1.30}$$

$$V_Q(mV) = F_R\, G_{BHD} \left(\frac{\sqrt{P_s P_{OL}}}{2} \right) \sin\theta \tag{1.31}$$

en donde G_{BHD} es la ganancia del BHD, F_R es el factor de respuesta del BHD el cual en nuestro experimento tiene un valor de 0.66 V/mW @ 1550nm,

De acuerdo a la Figura 1.8 las señales de entrada al octapuerto, son las señales provenientes del oscilador local E_{OL} con un estado de polarización circular, y la señal débil coherente que contiene los datos de la llave criptográfica E_S con estado de polarización lineal a 45^0 , se mezclan en el divisor de haz no polarizado (NPBS, *Non Polarizer Beam Splitter*). El ajuste de los estados de polarización de las señales es de suma importancia para obtener las dos cuadraturas del campo óptico de igual amplitud y el desfase correcto entre ellas. Las señales de entrada se representan con la Ecuación 1.32 y Ecuación 1.33 [59, 60].

$$E_{OL} = |E_{OL}|\ e^{j\theta_{OL}} \begin{bmatrix} \cos\varepsilon \\ \sin\varepsilon\ e^{j\frac{\pi}{2}} \end{bmatrix} \tag{1.32}$$

$$E_S = |E_S|\ e^{j\theta_S} \begin{bmatrix} \cos\beta \\ \cos\beta \end{bmatrix} \tag{1.33}$$

en donde θ_{OL}representa la fase del OL y $\theta_{Señal}$ corresponde a la fase de la señal de datos, ε y β representan los ángulos entre las componentes de campo eléctrico del OL, que en éste caso ambas son iguales a 45^0. Es la diferencia de fase $\Delta\theta = \theta_{OL} - \theta_{Señal}$ la que proporciona la señal que representa el error de fase entre ambas señales y que servirá para el sistema de retroalimentación y corrección de fase.

Al emerger del NPBS 50/50, tomando en cuenta los estados de polarización de las señales y de acuerdo a la Ecuación 1.21y Ecuación 1.22, se tiene en cada salida

$$E_1 = \frac{1}{\sqrt{2}} \left[|E_{OL}|\, e^{j\theta_{OL}} \begin{bmatrix} \cos\varepsilon \\ \sin\varepsilon\ e^{j\frac{\pi}{2}} \end{bmatrix} + |E_S|\, e^{i\theta_S} \begin{bmatrix} \cos\beta \\ \sin\beta \end{bmatrix} \right] \tag{1.34}$$

y

$$E_2 = \frac{1}{\sqrt{2}} \left[|E_{OL}|\, e^{j\theta_{OL}} \begin{bmatrix} \cos\varepsilon \\ \sin\varepsilon\ e^{j\frac{\pi}{2}} \end{bmatrix} - |E_S|\, e^{i\theta_S} \begin{bmatrix} \cos\beta \\ \sin\beta \end{bmatrix} \right] \tag{1.35}$$

Cada una de éstas dos señales E_1 y E_2, inciden en un divisor de haz polarizado 50/50 (NPBS, Non polarized beam splitter), como se observa en la Figura 1.8 para separarlas en sus componentes horizontal y vertical a cada una de ellas. A la salida de PBS1 se tienen E_{11} y E_{12} que son las componentes vertical y horizontal respectivamente del campo eléctrico de E_1 y de forma similar a la salida de PBS2 se tienen las señales E_{21} y E_{22}, de acuerdo a las ecuaciones siguientes

$$E_1 = E_{11} + E_{12} \tag{1.36}$$

$$E_2 = E_{21} + E_{22} \tag{1.37}$$

$$Salidas\ PBS1 \rightarrow E_{11} + E_{12} + E_{RV} \tag{1.38}$$

$$E_{11} = \frac{1}{\sqrt{2}} \left[|E_{OL}|\ e^{j\theta_{OL}t} \left[\ \sin\varepsilon\ e^{i\frac{\pi}{2}}\ \right] + |E_S|\, e^{j\theta_S} \left[\ \sin\beta\ \right] \right] \tag{1.39}$$

$$E_{12} = \frac{1}{\sqrt{2}} \left[|E_{OL}|\ e^{j\theta_{OL}} \left[\ \cos\varepsilon\ \right] + |E_S|\, e^{j\theta_S t} \left[\ \cos\beta\ \right] \right] \tag{1.40}$$

$$Salidas\ PBS2 \rightarrow E_{21} + E_{22} \tag{1.41}$$

$$E_{21} = \frac{1}{\sqrt{2}} \left[|E_{OL}|\, e^{j\theta_{OL}t} \left[\ \cos\varepsilon\ \right] - |E_{Señal}|\, e^{i\theta_{señal}} \left[\ \cos\beta\ \right] \right] \tag{1.42}$$

$$E_{22} = \frac{1}{\sqrt{2}} \left[|E_{OL}|\, e^{j\theta_{OL}} \left[\ \sin\varepsilon\ e^{j\frac{\pi}{2}}\ \right] - |E_{Señal}|\, e^{i\theta_{señal}} \left[\ \sin\beta\ \right] \right] \tag{1.43}$$

Por lo tanto, en el BHD1 inciden las componentes vertical del campo eléctrico (E_{11}y E_{22}), y en BHD2 las componentes horizontales (E_{12}y E_{21}). Sin embargo, en el proceso de separación de las componentes del campo eléctrico en sus estados de polarización, se introduce el ruido de vacío por los puertos no utilizados y como consecuencia se tiene una varianza mayor en los observables como se representa en la Figura 1.9 [61]. Las corrientes de salida de los BHDs serán afectadas por esas variaciones causadas por el ruido, tomando esto en cuenta y de acuerdo a la Ecuación 1.39, Ecuación 1.40, Ecuación 1.42 y Ecuación 1.43, se obtiene la Ecuación 1.44

$$I_{BHD1} = \frac{\Re}{2}\left[|E_{11} + E_{RV}|^2 + [E_{22} + E_{RV}]^2\right] \tag{1.44}$$

$$\begin{aligned} I_{BHD1} = \ & \frac{\Re}{2}\left[\left[|E_{OL}|\, e^{j\theta_{OL}t}\left[\ \sin\varepsilon\ e^{i\frac{\pi}{2}}\ \right] + |E_S|\, e^{j\theta_S}\left[\ \sin\beta\ \right] + E_{RV}\right]^2 + \right. \\ & \left.\left[|E_{OL}|\, e^{j\theta_{OL}}\left[\ \sin\varepsilon\ e^{j\frac{\pi}{2}}\ \right] - |E_S|\, e^{i\theta_S}\left[\ \sin\beta\ \right] + E_{RV}\right]^2\right] \end{aligned} \tag{1.45}$$

$$I_{BHD2} = \frac{\Re}{2}\left[|E_{12} + E_{RV}|^2 + [E_{21} + E_{RV}]^2\right] \tag{1.46}$$

$$\begin{aligned} I_{BHD2} = \ & \frac{\Re}{2}\left[\left[|E_{OL}|\, e^{j\theta_{OL}}\left[\ \cos\varepsilon\ \right] + |E_S|\, e^{j\theta_S t}\left[\ \cos\beta\ \right] + E_{RV}\right]^2 - \right. \\ & \left.\left[|E_{OL}|\, e^{j\theta_{OL}t}\left[\ \cos\varepsilon\ \right] - |E_S|\, e^{i\theta_S}\left[\ \cos\beta\ \right] + E_{RV}\right]^2\right] \end{aligned} \tag{1.47}$$

en el resultado obtenido, después del desarrollo de la Ecuación 1.45 y Ecuación 1.47 finalmente se toman en cuenta los términos en donde aparece E_{OL}, ya que es el término que proporciona la potencia suficiente para que la señal sea detectada, los términos en los que sólo aparece E_S tienen una contribución mínima en la potencia de la señal resultante. Se puede considerar que la corriente en los fotodetectores entonces depende en mayor medida y es proporcional a E_{OL} y las variaciones del campo eléctrico ocasionadas por el ruido de vacío.

$$I_{BHD1} \propto \frac{\Re}{2}\left[E_{OL}(E_{señal} + \triangle I + \triangle I_{RV})\ \cos[\theta_{OL} - \theta_{señal} - \theta_{modul}]\right] \tag{1.48}$$

$$I_{BHD2} \propto \frac{\Re}{2}\left[E_{OL}(E_{señal} + \triangle Q + \triangle Q_{RV})\ \sin[\theta_{OL} - \theta_{señal} - \theta_{modul}]\right] \tag{1.49}$$

Con la información de la corriente y potencia promedio de los observables, es posible calcular el número de fotones que contiene el estado coherente débil utilizando la Ecuación 1.50, en donde N es el número de fotones, P es la potencia del haz óptico, T es el intervalo de tiempo de observación, es decir el tiempo de bit, h es la constante de Planck (6.62559×10^{-34} J) y ν es la frecuencia de la señal óptica [13].

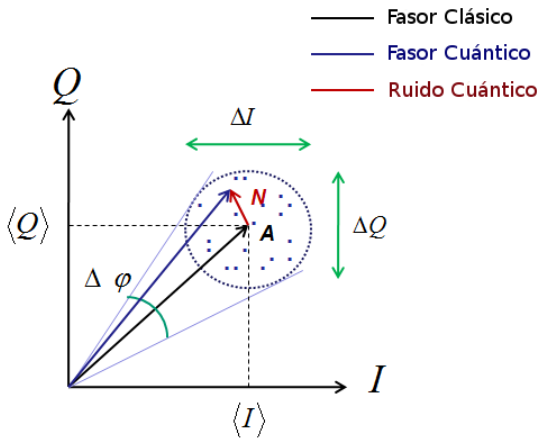


Figura 1.9.: Incremento de la varianza de la amplitud y fase en los observables como efecto del ruido.

$$N = \frac{PT}{h\nu} \tag{1.50}$$

En los observables (valor promedio) de ambas cuadraturas I y Q, existe un término en el dominio clásico (primer término de Ecuación 1.51 y Ecuación 1.52)y otro en el dominio cuántico (segundo término de las ecuaciones mencionadas) que son descritas a través del "operador de número de fotones" $\widehat{N}$ de la señal débil coherente, por lo que los observables se pueden describir como

$$I = \left\langle \widehat{N}_{In-phase} \right\rangle + \left\langle \Delta\widehat{N}_{In-Phase} \right\rangle \tag{1.51}$$

$$Q = \left\langle \widehat{N}_{Quadrature} \right\rangle + \left\langle \Delta\widehat{N}_{Quadrature} \right\rangle \tag{1.52}$$

en donde $\left\langle \widehat{N} \right\rangle$y $\left\langle \Delta\widehat{N} \right\rangle$son el número de fotones promedio y las fluctuaciones promedio del número de fotones respectivamente [62].

En este sistema con esquema de modulación BPSK con estados débiles coherentes la Relación Señal a Ruido SNR (signal to Noise Ratio) se define como la potencia normalizada de la señal, dividida por la varianza estándar de la misma (ver Ecuación 1.53), la cual es función

del número de fotones que inciden en el fotoreceptor, al igual que la tasa de bits erróneos (BER, Bit Error rate) de la forma

$$SNR = \frac{\left\langle \widehat{N_I} \right\rangle^2}{\left\langle \widehat{N_I^2} \right\rangle} = 2N \tag{1.53}$$

y el BER

$$BER = \frac{1}{2}\, erfc\left(\sqrt{N}\right) \tag{1.54}$$

en donde N es promedio del número de fotones por bit y erfc es la función de error complementaria [62, 63]. En este esquema de detección de las cuadraturas en forma simultánea el valor de la SNR resulta la mitad del valor que se obtiene en un esquema de cuadraturas conmutadas [17] , por el ruido adicional (ruido de vacío) que también afecta al BER. La densidad de probabilidad para las dos cuadraturas de acuerdo a Ecuación 1.4 se puede calcular con Ecuación 1.55 y Ecuación 1.56, para posteriormente representarlas en forma gráfica como en la Figura 1.10

$$P_e(I) = \frac{1}{\sqrt{2\pi}}\, \exp\left(-\frac{1}{2}\left(\left\langle \widehat{N_I} \right\rangle + \triangle \widehat{N_I}\right)^2\right) \tag{1.55}$$

$$P_e(Q) = \frac{1}{\sqrt{2\pi}}\, \exp\left(-\frac{1}{2}\left(\left\langle \widehat{N_Q} \right\rangle + \triangle \widehat{N_Q}\right)^2\right) \tag{1.56}$$

Considerando que el ruido que presenta la señal es del tipo blanco gaussiano y aditivo, es posible identificar el valor medio de un "1" ó "0" lógicos del bit correspondiente y el ruido como asociado con la varianza de la señal, de tal modo que podemos calcular la potencia de ruido promedio asociada a la transmisión, lo que nos remite a la definición de energía de bit a ruido y como consecuencia con la tasa de error de bit. Por lo tanto si se calcula la varianza podemos determinar la SNR y el BER de los observables I y Q que se medirán.

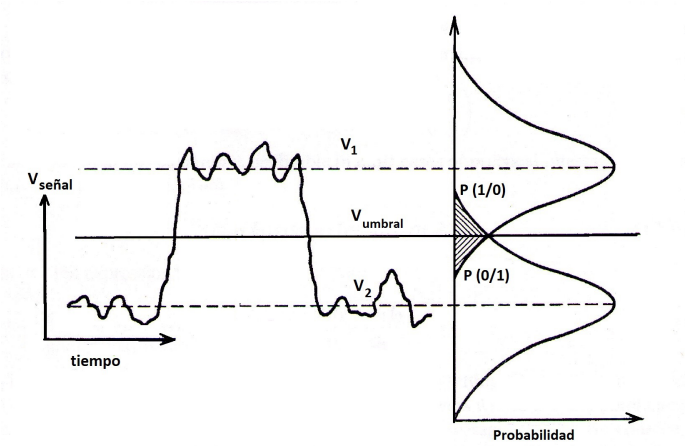


Figura 1.10.: Densidad de probabilidad de la señal detectada que contiene los datos (I). (*Figura basada en [1]*)

1.7. Sistemas de estabilización del receptor homodino

El uso de un Lazo de Costas es ampliamente utilizado para sistemas de comunicaciones que hacen uso de esquemas de modulación eficientes con portadora suprimida, tal como BPSK y otras constelaciones de mayor orden [64, 65], ya que permite la detección de la componente en fase (I) y la componente en cuadratura (Q) de la señal de entrada y como consecuencia tener la posibilidad de hacer cálculos de estimación del error fase o frecuencia.

Durante el desarrollo de la presente investigación, se inicia la implementación de Lazo de Costas autohomodino, con el fin de contar con un control de la fluctuación lenta del cambio de fase entre la señal modulada y la señal con la información; así como una fluctuación rápida de la fase, que puede presentarse en un enlace en espacio libre, debido a la turbulencia en la trayectoria del haz; de manera independiente. Los resultados obtenidos presentan las variaciones correspondientes a la evolución rápida de fase y los tiempos de amarre logrados.

En consecuencia, es relevante comentar los conceptos generales del Lazo de Costas implementado.

En particular para el caso en estudio, el Lazo de Costas se emplea fundamentalmente para la recuperación de portadora, aunque en el caso particular se emplean componentes en estado autohomodinado, lo cual reduce la complejidad que puede derivarse del sistema, cuando se emplean enlaces ópicos.

El primer problema que se presenta en los sistemas de comunicaciones ópticas con esquemas de detección homodina, resulta de la frecuencia detectada que puede presentarse cuando se trabaja con dos lásers con distintas frecuencias; ya que una diferencia de unas décimas de nanómetro, se ve reflejada en diferencias frecuenciales del orden de los GHz.

1.7.1. Descripción del Lazo de Costas en estado Estable

En este caso la señal de información y la del oscilador local están en el dominio óptico, la detección de fase se lleva a cabo en los fotodetectores balanceados, en los cuales ocurre un "batimiento" entre las dos señales ópticas de entrada con una función de transferencia no lineal, produciendo una señal a la frecuencia intermedia en la salida, ahora en el dominio eléctrico, del detector. Como hemos comentado anteriormente, diferencias en longitud de onda relativamente pequeñas, pueden llevar a diferencias frecuenciales grandes. Dado que la prueba de concepto en marcha pretende determinar la eficacia de la implementación del lazo para el control de la fase en el enlace de comunicaciones ópticas, se realiza el enlace con un oscilador local que surge del mismo haz láser, y que debido al trayecto óptico empleado

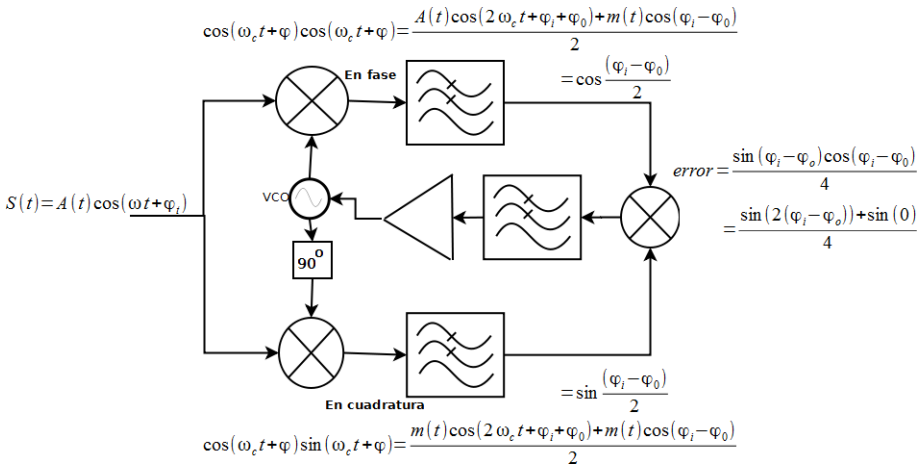


Figura 1.11.: Diagrama general de un Lazo de Costas, donde M representa el Mezclador como detector de fase, LPF es un filtro paso bajas, A es la ganancia del Lazo, Mm es un multiplicador en banda base, VCO es un oscilador controlado por voltaje,

para transmitir el haz hasta el detector, puede sufrir de variaciones de fase, producto de inestabilidades en el aire (tubulencia) del trayecto. Ésta evolución es relativamente rápida, por lo cual la evolución lenta de la envolvente puede analizarse posteriormente, y resulta de mayor interés identificar el funcionamiento del sistema de control de retroalimentación del lazo, para la envolvente rápida, la cual involucra el uso de un modulador electroóptico en el oscilador local del detector, para efectuar la retroalimentación sobre la fase del oscilador local.

El Lazo de Costas divide la señal de entrada en sus componente en I y Q, tal como se muestra en la Figura 1.11, en el caso que nos ocupa, la salida correspondiente del detector de Fase I y del detector de fase ,Q corresponden a las salidas de los fotodetectores balanceados, que reciben la incidencia del haz cuántico, modulado, (en nuestro caso por una señal BPSK), y la incidencia del haz correspondiente al oscilador local en su componente cosenoidal o senoidal (de ahí la importancia del octapuerto, y el control de polarización en el sistema). La señal entonces interactúa con el oscilador local (en su componente correspondiente cosenoidal o senoidal) a través del Detector de Fase, que en el diagrama aparece como un elemento de multiplicación [66, 67].

Si proponemos que la señal de entrada cuente con la representación matemática:

$$V_S(t) = A_{Señal}\,\cos(\omega_{Señal}\,t + \phi_{Señal}) \tag{1.57}$$

y el oscilador local con la representación matemática:

$$V_{OL}(t) = A_{OL}\,\cos(\omega_{OL}\,t + \phi_{OL}) \tag{1.58}$$

Dichas señales se multiplican con el objetivo de tener como resultado una señal que contiene la información de la diferencia de fase entre I y Q de magnitud proporcional a esa diferencia, es decir $I = \frac{1}{2}A_S A_{OL} Sen(\phi_s - \phi_{OL})$ y $Q = \frac{1}{2}A_S A_{OL} Cos(\phi_s - \phi_{OL})$

Entonces el resultado de la multiplicación de ambas señales (Ecuación 1.57 y Ecuación 1.58) puede expresarse matemáticamente como:

$$\begin{aligned} V_{Mult} &= A_S\,A_{OL}\,\cos(\omega_S\,t + \phi_S)\,\cos(\omega_{OL} + \phi_{OL}) \\ &= A_S\,A_{OL}\,\{\cos((\omega_S - \omega_{OL})\,t + (\phi_S - \phi_{OL})) \\ &\quad + \cos((\omega_S + \omega_{OL})\,t + (\phi_S + \phi_{OL}))\} \end{aligned} \tag{1.59}$$

Dado que para el presente análisis, podemos asegurar que ω_S y ω_{OL} son iguales (receptor homodino), mientras que la suma, nos genera una componente del doble de la frecuencia portadora; en el caso de los dispositivos ópticos, no es posible generar la señal eléctrica correspondiente al doble de la frecuencia de la portadora; por lo que el fotodetector funciona simultáneamente como detector de fase y filtro paso baja, por lo que la señal esperada a la salida del fotodetector (voltaje resultante de la multiplicación portadora×señal V_{Mult}) resultaría en la Ecuación 1.60, que representa el error de fase que servirá para corregir el desfase de las señales del oscilador local y la de datos para lograr su amarre.

$$V_{Mult} = \frac{1}{4}A_S\,A_{OL} Sen(\phi_S - \phi_{OL}) \tag{1.60}$$

Adicionalmente, si la diferencia de fases entre la señal de entrada al sistema y la retroalimentada son iguales, la salida del multiplicador será máxima.

1.7.2. Diseño del sistema de retroalimentación

Se requiere partir de la expresión de la varianza de la señal de error de fase $\sigma^2_{e\omega}$ (ver Ecuación 1.61) del Lazo de Costas para optimizarla y calcular la constante de tiempo τ_1 los cuales son necesarios para diseñar el filtro del lazo (ver Figura 1.11).

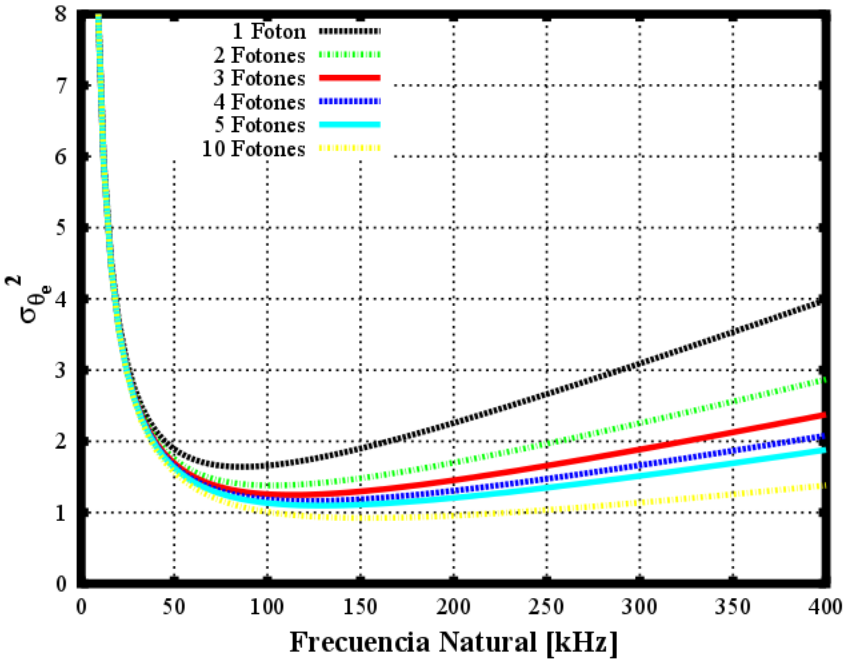


Figura 1.12.: Varianza del error de fase (σ_e^2) vs frecuencia natural del sistema.

$$\sigma_e^2 = \frac{\Delta\nu}{\sqrt{2}f_n} + \frac{3\pi T_p f_n}{2\sqrt{2}N_s} \tag{1.61}$$

en donde $\Delta\nu$ representa el ancho de banda de la señal moduladora, f_n es la frecuencia natural del lazo, T_p es el periodo de bit de la señal moduladora y N_s es el número de fotones. El primer término de la Ecuación 1.61 representa el ruido de fase y el segundo término el ruido cuántico. El comportamiento de σ_e^2 con la variación de la frecuencia natural del sistema para varios números de fotones se muestra en la figura .

De acuerdo a las consideraciones mencionadas en[68] se calcula la frecuencia natural óptica del lazo de la configuración mostrada a continuación y con la siguiente ecuación

$$f_n = \sqrt{\frac{2\Delta\nu N_s}{3\pi T_p}} \tag{1.62}$$

La ganancia de lazo K_L se calcula a partir de la ganancia del fotodetector K_{Det} y la ganancia del Vco del lazo K_{VCO-M}, en donde

$$K_{Det} = \Re_{Det} \sqrt{P_{señal}\, P_{OL}}\ \sin(\phi)\, G_{BHD} \tag{1.63}$$

La responsividad del fotodetector ($\Re$) es de 0.66 V/mW, la potencia de la señal que contiene la señal de datos es $P_{señal} = 45\ fW$, la potencia del oscilador local $P_{OL} = 2\ mW$, $\phi = 180^0$ es el ángulo de defasamiento, la ganancia del foto detector G_{BHD} es de 3×10^4.

Con el valor de la frecuencia natural y la ganancia de lazo es posible calcular las constantes de tiempo τ_1 y τ_1 a partir de Ecuación 1.64 y Ecuación 1.65.

$$\tau_1 = \frac{K_L}{(2\pi f_n)^2} \tag{1.64}$$

$$\tau_2 = \frac{2\zeta}{f_n} \tag{1.65}$$

Con los valores de τ y considerando que el amplificador operacional (OPAMP) tiene una ganancia alta, se propone un valor para el capacitor C para después calcular las resistencias del filtro R_1 y R_2 utilizando las expresiones Ecuación 1.66 y Ecuación 1.67.

$$\tau_1 = R_1 C \tag{1.66}$$

$$\tau_2 = R_2 C \tag{1.67}$$

Los resultados de la implementación del lazo se exponen en el capítulo que trata sobre la caracterización del octapuerto.

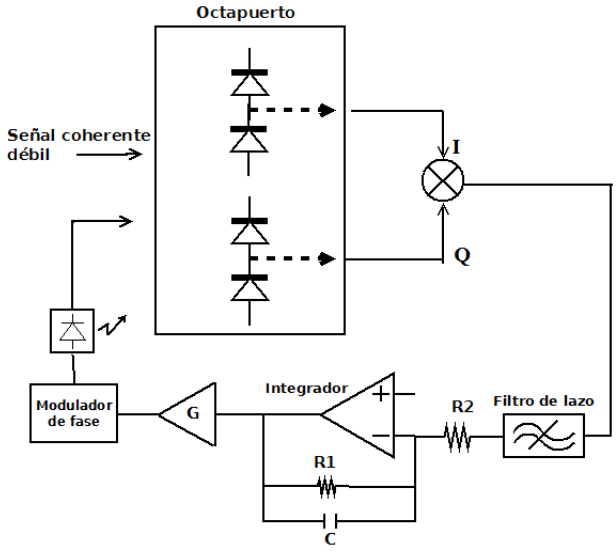


Figura 1.13.: Componentes del lazo de Costas. OL=Oscilador local, G=Ganancia del amplificador,

2. Realización Experimental

2.1. Introducción

A continuación se describirá el esquema experimental del sistema de comunicación óptica coherente para criptografía cuántica, en donde el sistema transmisor es el equipo que tendría Alice y el receptor corresponde a Bob. En primer lugar se describirá el proceso de caracterización de sistema de fotodetección para determinar si es adecuado para la recepción de señales débiles del orden de decenas de femtowatts y con esto asegurar que es posible efectuar mediciones cerca del límite cuántico estándar. Posteriormente se describirá el montaje del octapuerto y el sistema autohomodinado, que sirve como plataforma para asegurar el funcionamiento y recuperación de datos, haciendo énfasis en las variables de medición y las restricciones que nos impone la infraestructura disponible.

2.2. Transmisor y Receptor cuántico

El sistema transmisor cuenta con una estructura simple, para un desarrollo de prueba de concepto, está integrado por un transmisor de señales digitales pseudoaleatorias que proporciona la señal que entra a un modulador electroóptico cuya salida está modulada en un esquema de BPSK, el cual puede migrarse con facilidad a esquemas de alto orden M-PSK, mediante una selección juciosa de los niveles de señal alimentados al modulador, y en un momento dado, la selección de componentes adicionales, la implementación de modulaciones M-QAM, que ofrezcan la posiblidad de explorar los protocolos de critpografía de variables continuas con estados de señuelos (*decoy states*). Una vez que la señal está modulada ésta incide en un polarizador lineal a 45^0, esto nos permite obtener las dos componentes ortogonales del campo eléctrico E_x y E_y del E_{Total}. Posteriormente la señal es atenuada aproximadamente 120 dB para lograr un estado coherente débil, generando el elemento cuántico que contiene la información a transmitir, que en este caso es el estado de fase.

El receptor cuántico, se basa en un montaje de los componentes con la configuración de un octapuerto, además de una la señal de referencia OL, posteriormente la separación de las

componentes del estado de polarización de la señal que es resultado de la mezcla de la señal coherente débil y el OL, y finalmente los fotodetectores balanceados para E_x y E_y. Como ya se vió en el capítulo anterior en la implementación del octapuerto se tienen dos puertos no utilizados, los cuales son fuente de ruido de vacío, que se debe tomar en cuenta en el proceso de análisis de la señal detectada.

En este trabajo es de suma importancia ser capaces de medir las señales de salida de los fotodetectores y visualizarlos por medio de un osciloscopio para la captura de los datos. Una vez que se tenga ésa información se realizan las estadisticas para obtener la tasa de error de bit, relación señal a ruido y la información mutua principalmente, que son parámetros fundamentales de un sistema de comunicaciones los cuales a su vez nos permiten determinar si el canal cuántico es viable para su utilización en criptografía o comunicaciones cuánticas.

2.3. Caracterización del octapuerto.

Para asegurar que el octapuerto está trabajando en las condiciones óptimas se caracterizaron diferentes parámetros tal como el ruido cuántico, ruido electrónico, corriente de oscuridad de los fotodetectores, atenuación de la señal modulada, estados de polarización de la luz y calibración del sistema receptor para verificar que se logró recibir un estado coherente débil de 1 fotón por bit o menor. En particular el ruido electrónico nos proporciona imformación de la potencia que debe entregar el oscilador local para asegurar que en el proceso de fotodetección el ruido preponderante se deba fundamentalmente al ruido cuántico, mejorando la eficiencia del sistema.

Para la caracterización del montaje experimental y de los fotodetectores Balanceados BHD, se utilizó un osciloscopio, analizador de espectros, Analizador de polarización en espacio libre, Fotoreceptor de potencias ópticas del orden de femto watts y fotoreceptor de un sólo fotón *Single Photon Detector* (SPD). A continuación se describirá el proceso de caracterización y los resultados.

2.3.1. Medición del ruido electrónico.

El ruido electrónico se midió apagando los fotodetectores dejando conectadas sus salidas al osciloscopio para observar el ruido electrónico que genera el sistema. El resultado se muestra en la Figura 2.1, en donde se tiene un valor promedio aproximado de -102 dBm. En la Figura 2.3 se observa que el ruido electrónico tiene niveles por debajo del ruido cuántico. Al observar los efectos de las fuentes de ruido, se identificó una componente frecuencial dentro

del ancho de banda de los fotodetectores, coincidente con ruido proveniente de la línea de alimentación, por estas razones para reducir éstas interferencias no deseadas, se emplearon ferritas en las conexiones que van de las fuentes de alimentación hacia la circuitería electrónica analógica implementada.

2.3.2. Medición del ruido por corriente de oscuridad.

Para la medición del ruido generado por la corriente de oscuridad, los fotodetectores balanceados se ajustaron con una ganancia de 1×10^2, se bloqueó la entrada de la señal del OL, de datos y de cualquier tipo de luz ambiental a los fotodetectores. La señal de salida de los fotodetectores se observó con un analizador de espectros para analizar su respuesta en un rango de frecuencias, que mostró una respuesta plana en el intervalo 0.1-1 MHz, con un valor de potencia promedio de -85 dBm, como se muestra en la Figura 2.1. Se realizó la medición de los voltajes de salida de los fotodetectores en el dominio del tiempo para diferentes valores de potencia de OL, los resultados se muestran en la Figura 2.2.

2.3.3. Medición del ruido cuántico.

Un ruido inevitable en los sistemas optoelectrónicos es el ruido de disparo o Ruido *Shot*, generado por fenómenos asociados a la característica discreta de la generación de carga eléctrica en los fotodetectores. Una técnica para medir éste ruido consiste en bloquear la señal de datos que incide en el separador de haz de la entrada del octapuerto, dejando en la otra entrada del separador la señal del OL, se mide el ruido total a la salida del receptor y a éste último se le resta el ruido electrónico [69]. Para poder medir el ruido de disparo, es necesario que el OL tenga un valor considerable comparado con la señal de datos, de este modo su valor quedará por encima del ruido electrónico y poder medirlo; se consideró adecuado un voltaje del oscilador local de 2mW puesto que la señal de datos tendría una potencia del orden de los femtowatts. Utilizando el analizador de espectros, se midió el ruido de disparo para los diferentes valores de ganancia que tienen los fotodetectores, es decir, para 1×10^3,3×10^3, 1×10^4, y 3×10^4 V/V, en un intervalo de 0 a 1 MHz de frecuencia. Los resultados se muestran en la Figura 2.3.

Los resultados de la Figura 2.1 nos muestran que el ruido generado por el oscilador local está por encima de los ruidos de oscuridad y el electrónico, lo que permite la correcta detección de la señal que contiene los datos, estas condiciones nos aseguran que es posible trabajar cercanamente al límite del fotodetector (*shot noise limited* detector). Se observa en la gráfica

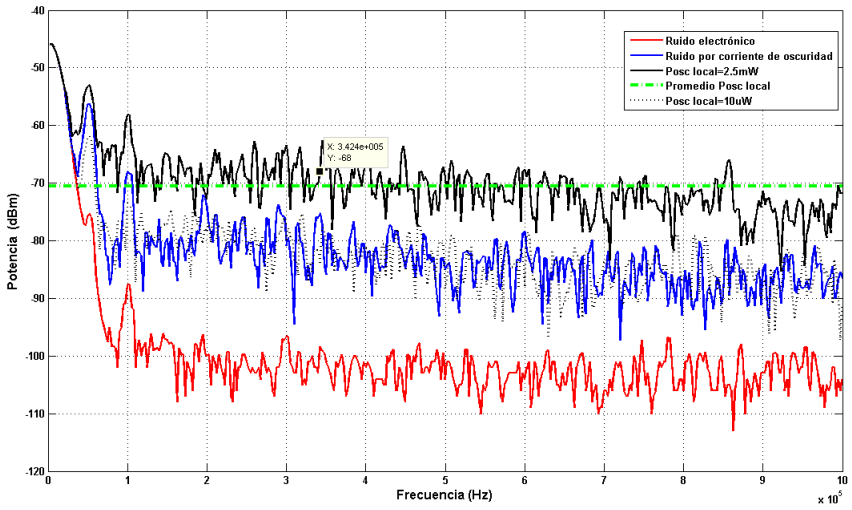


Figura 2.1.: Espectro en frecuencia de: la señal del oscilador local para potencias de 2.5 mW y 10 microWatts, ruido electrónico, ruido ocasionado por y la corriente de oscuridad, con una ganancia en los fotodetectores de 1000.

Figura 2.2 que el shot noise tiene una dependencia lineal con la potencia del OL al cumplir con la forma $y = ax + b$.

2.3.4. Medición de los estados de polarización.

Como ya se explicó anteriormente es necesario que la señal de datos y la señal del OL que entran al octapuerto tengan un estado de polarización bien definido para poder medir las cuadraturas del campo óptico, para ello se realizaron mediciones de los estados de polarización en los siguientes lugares: a) a la entrada del modulador de fase para asegurar que se tuviera un estado de polarización lineal vertical, b) antes del conjunto de filtros de atenuación de la señal para verificar que tuviéramos una polarización lineal con una inclinación a 45^0 en la señal que contiene los datos y que entrará al octapuerto, c) en la entrada del octapuerto para verificar que la señal del OL tuviera un estado de polarización circular y finalmente en d) a la salida del divisor de haz que está a la entrada del octapuerto (NPBS). Los parámetros de Stokes medidos en diferentes puntos del octapuerto se observan en la Figura 2.4, con dichos parámetros proporcionan información de la intensidad y estado de polarización del haz óptico, su descripción se presenta en el Apéndice C

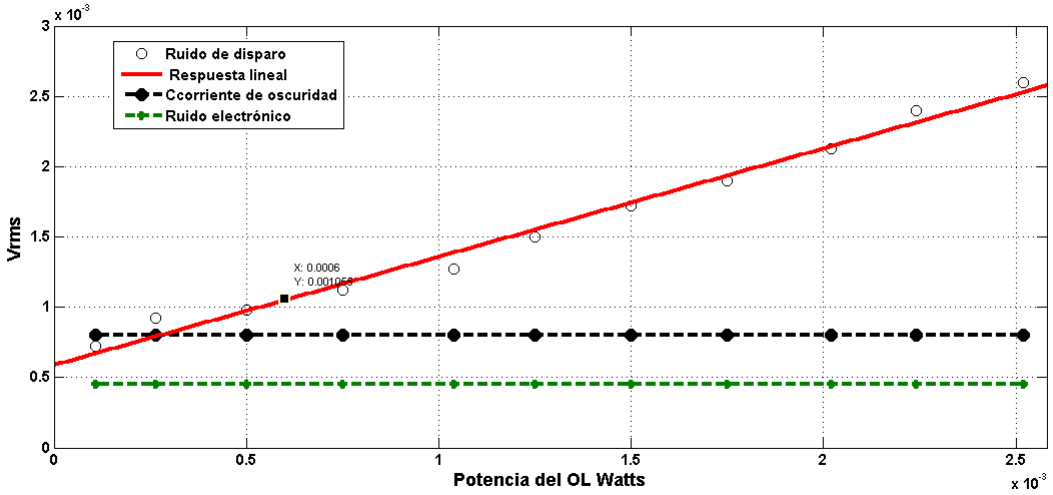


Figura 2.2.: Gráfica en donde se muestra el valor del ruido de diparo, el voltaje producido por la corriente de oscuridad y la relación lineal entre el ruido electronico y la potencia del oscilador local

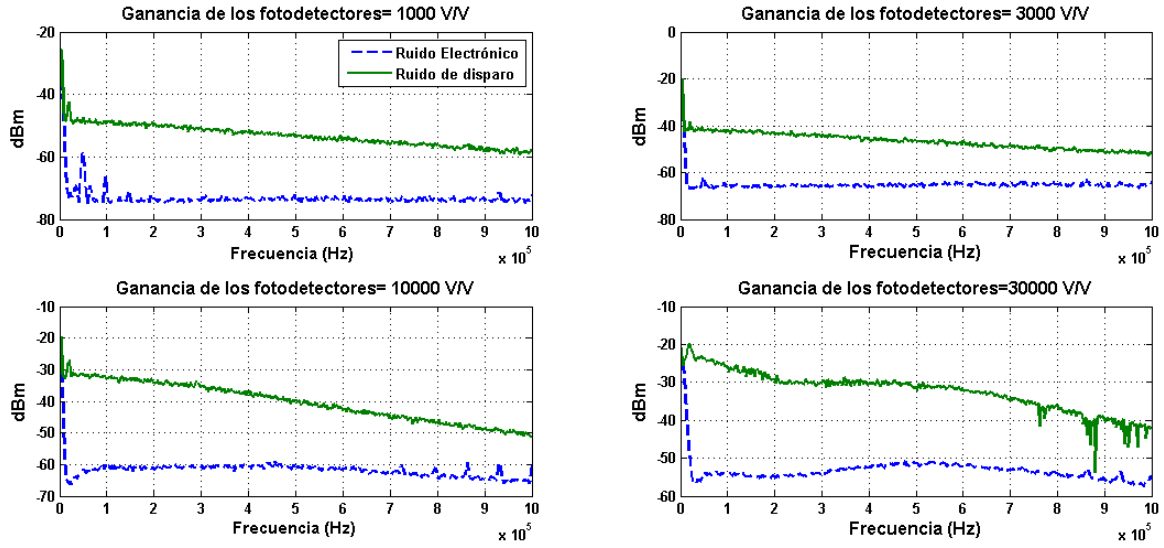


Figura 2.3.: Espectro de potencia de los ruidos electrónicos y de disparo para ganancias de los fotodetectores de 1000, 3000, 10000 y 30000 V/V

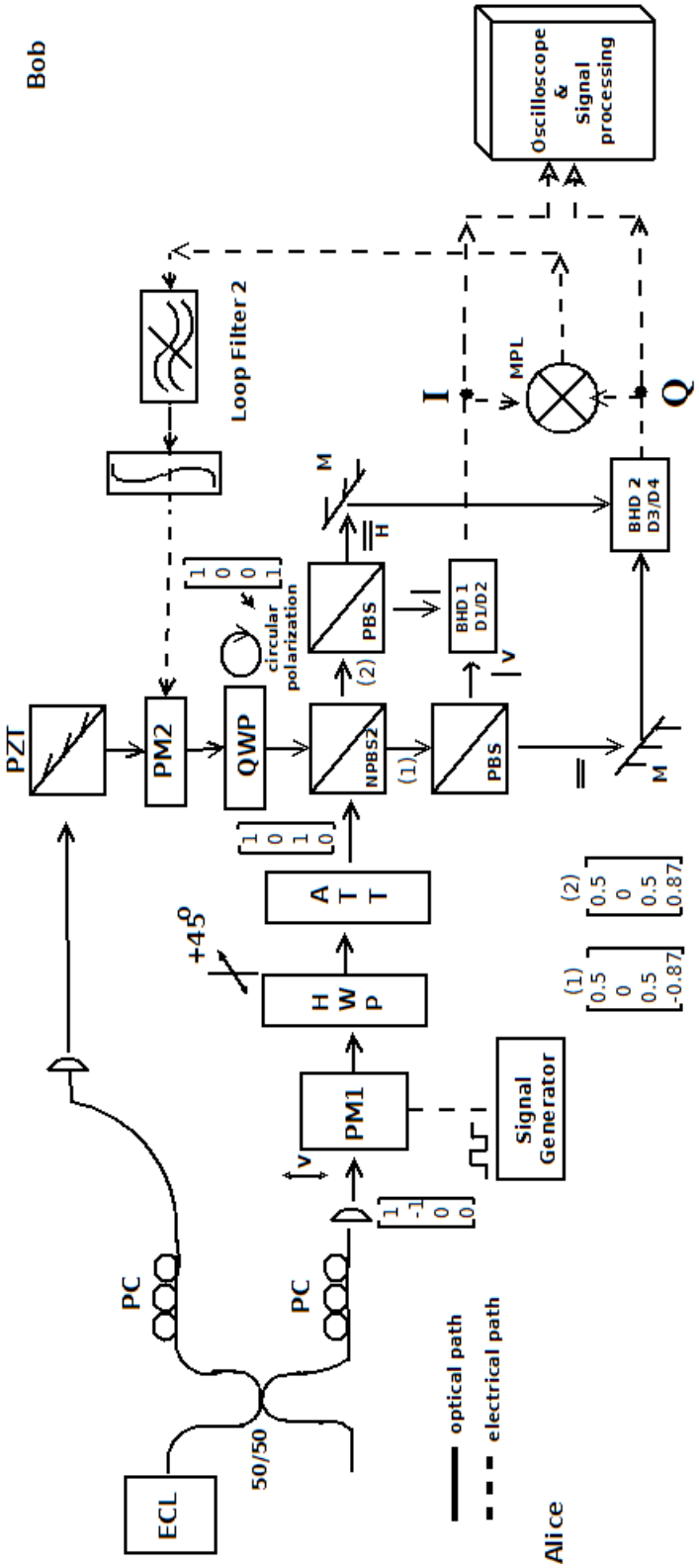


Figura 2.4.: Estados de polarización medidos en puntos importantes del octapuerto para asegurar su correcto funcionamiento. ECL: External Cavity Laser, PM: Phase Modulator, PC: Polarization Controller, NPBS: Non Polarized Beam Splitter, PBS: Polarized Beam Splitter, HWP: Half Wave Plate, QWP: Quarter Wave Plate, ND: Neutral Density Filter BHD: Balanced Homodyne Detector, PZT= Piezoelectric, MPL: Multiplier, M:Mirror, ATT: attenuator..

2.3.5. Medición del número de fotones por bit a la entrada del octapuerto con el detector de un solo fotón y con el fotodetector de femtowatts.

Para asegurar que se estaba trabajando con una potencia de la señal de datos de un fotón por bit promedio, se utilizaron un Detector de un solo fotón (SPD, *Single Photon Detector*) y un fotodetector de señales ópticas del orden de los femtowatts. La Figura 2.5 muestra ambos medidores dentro del montaje experimental del octapuerto.

a) **Detector de un solo fotón**. El principio de funcionamiento del detector utilizado se basa en un fotodetector de Avalancha (APD, *Avalanche Photo Detector*) en el modo Geiger [70]. El APD está polarizado con un voltaje inverso y se le aplica un voltaje (en un pulso) que lo lleva a un punto en el que permite la conducción de corriente por un periodo de tiempo. Lo anterior permite tener una ventana temporal en la que son detectados los fotones que incidan en ese momento para dar inicio a la avalancha. Es necesario introducir en el menú de inicio del SPD los parámetros que permiten calcular el número de conteos reales C_{real} para que éste funcione adecuadamente con las condiciones del experimento, tales como la ventana de tiempo en la que el detector estará disponible para la fotodetección y la frecuencia de la señal con la que se va a trabajar. Para determinar el conteo real que proporciona el SPD se utiliza la Ecuación 2.1.

$$C_{real} = \frac{(C - DC - AF)}{DE} \tag{2.1}$$

Donde C_{real} es el número de eventos registrados finales (número de fotones incidentes) después de considerar los siguientes parámetros: C es el conteo de eventos que proporciona el SPD en la pantalla de salida, DC (*Dark Current Count*) es el conteo por la corriente de oscuridad el cual tiene un valor de 0.5, AF (*After Pulse Count*) son los conteos que se registran aún cuando el pulso a medir ya terminó, el cual registra un valor de 121, y DE (*Detector Eficiency*) es la eficiencia del fotodetector que en este caso es de 0.2, es decir 20 %. Es necesario realizar varias pruebas para calibrar el SPD para verificar que se tiene un resultado de conteo lo más cercano posible a las predicciones basadas en el cálculo de la potencia de la señal de acuerdo al número de fotones, el cual se puede realizar con la Ecuación 1.50. Es posible visualizar los eventos del conteo en un osciloscopio, un ejemplo de ello se muestra en la Figura 2.6.

b) **Detector de femtowatts**. Se utilizó un fotodetector muy sensible, es decir que sea capaz de detectar señales del orden de los femtowatts, para ajustar la potencia de entrada

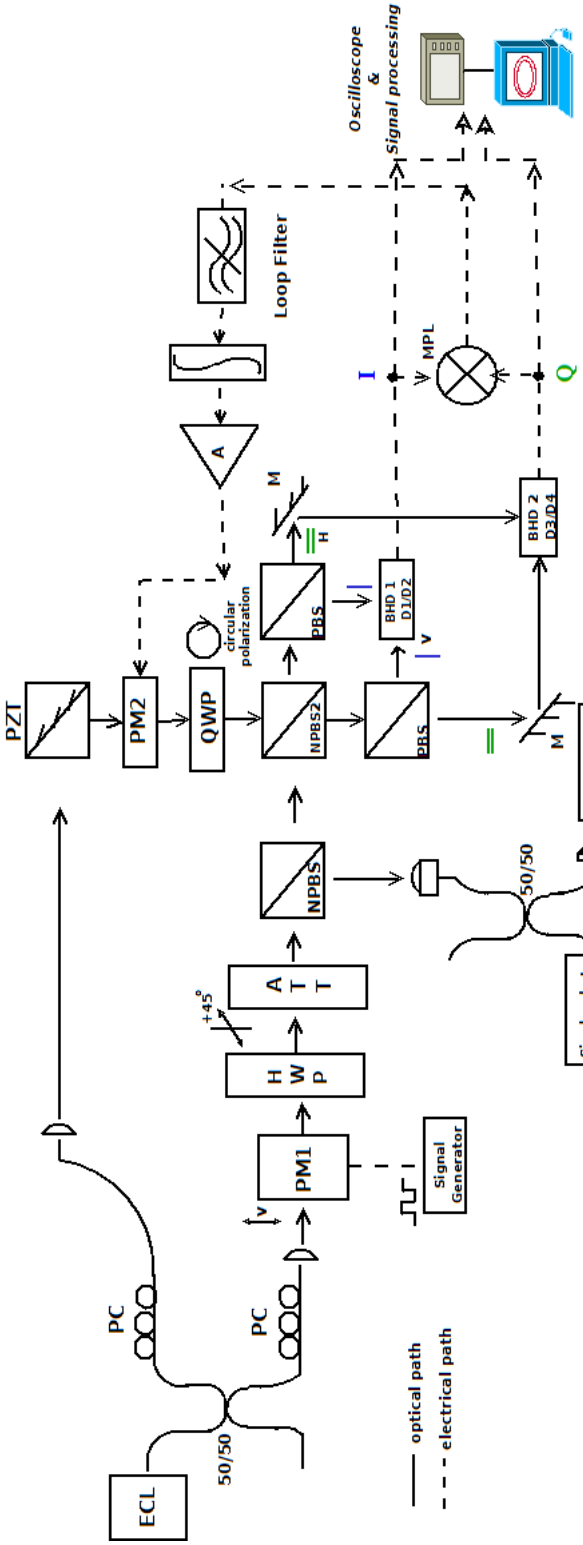


Figura 2.5.: Detector de un solo fotón y fotodetector de femtowatts para la calibración del número de fotones que inciden a la entrada del octapuerto. ECL: External Cavity Laser, PM: Phase Modulator, PC: Polarization Controller, NPBS: Non Polarized Beam Splitter, PBS: Polarized Beam Splitter, HWP: Half Wave Plate, QWP: Quarter Wave Plate, ND: Neutral Density Filter BHD: Balanced Homodyne Detector, PZT= Piezoelectric, MPL: Multiplier, M:Mirror, ATT: attenuator.

Figura 2.6.: Salida del contador de fotones. Se observan los conteos en una ventana de tiempo.

al octapuerto a una potencia equivalente a un fotón por bit promedio a una frecuencia de modulación de los datos de 350 KHz, lo que arroja un resultado de una potencia de 45 fW. La potencia mínima que se puede detectar con este dispositivo es de 10 fW, mientras que la potencia de saturación con una onda continua es de 0.25 nW@1600nm.

2.4. Realización Experimental.

El sistema experimental que se muestra en la Figura 2.7, consiste en un interferómetro en espacio libre de 8 puertos en el cual se utiliza un láser de cavidad externa sintonizado a una longitud de onda de 1550 nm. La señal proveniente del láser es utilizada tanto para la señal que contiene los datos, como para la señal de referencia (oscilador local) de modo que el sistema opera en una configuración auto homodina.

Se genera una secuencia de datos pseudo aleatoria a 350 Kbps como entrada del modulador de fase electroóptico (PM1 en la figura) con el fin de generar una señal con modulación BPSK (Binary Shift Keying). En este sistema es escencial que los estados de polarización estén siempre bien definidos y sin variaciones para asegurar la detección correcta de las variables conjugadas en los fotodetectores (BHDs). A la entrada del modulador de fase la señal debe tener un estado de polarización lineal vertical para minimizar la modulación residual en amplitud como lo refiere el manual del modulador.

Después de ajustar el estado de polarización del haz modulado a una polarización lineal a 45 grados, éste es atenuado 120 dB por medio de un set de filtros de densidad neutral (ND-filters) para producir un estado coherente débil (WCS, weak coherent states). El haz

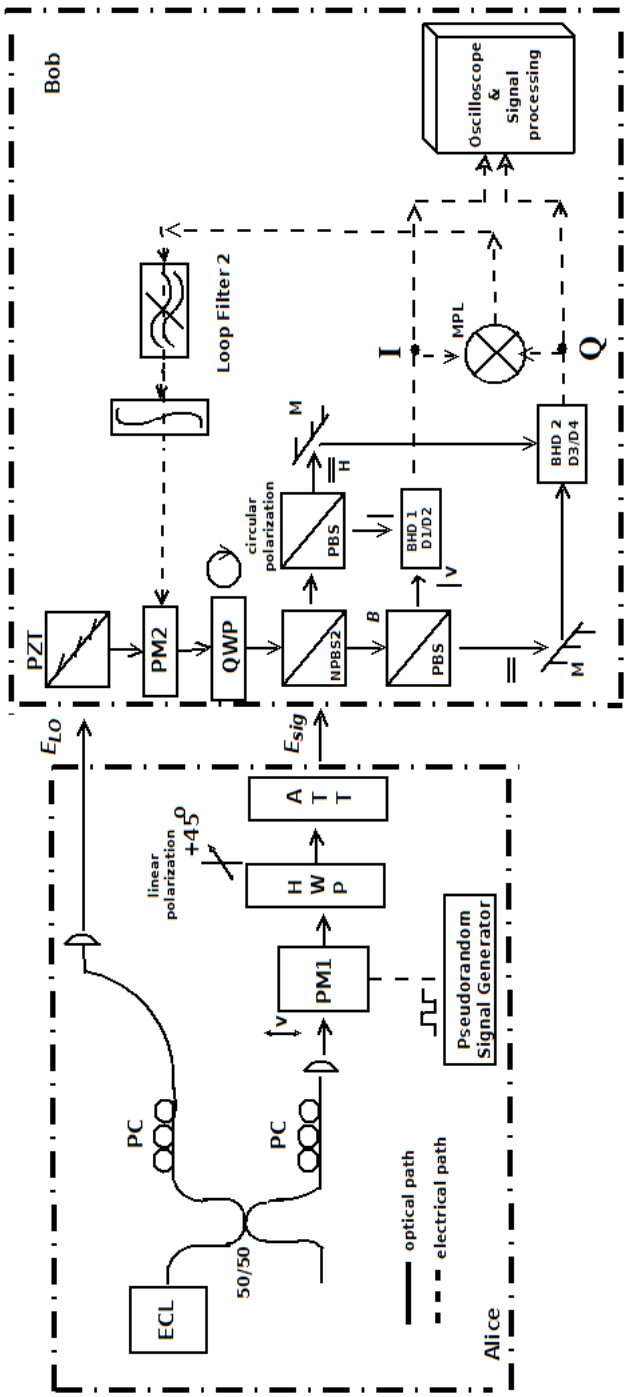


Figura 2.7.: Montaje experimental del octapuerto homodino que incluye el sistema de retroalimentación basado en un lazo de Costas con modulación en fase binaria para estados coherentes débiles en espacio libre y fotodetección balanceada. ECL: External Cavity Laser, PM: Phase Modulator, PC: Polarization Controller, NPBS: Non Polarized Beam Splitter, PBS: Polarized Beam Splitter, HWP: Half Wave Plate, QWP: Quarter Wave Plate, ND: Neutral Density Filter BHD: Balanced Homodyne Detector, PZT= Piezoelectric, MPL: Multiplier, M:Mirror, ATT: attenuator.

atenuado tiene una potencia equivalente a un fotón por bit en promedio, que para la frecuencia de modulación de 350 KHz, dicha potencia equivale a 45 fW. La señal en estado coherente débil es introducida al octapuerto.

La señal del oscilador local (LO por sus siglas en inglés) que tiene una potencia de 2 mW, viaja a través de un segundo modulador de fase, el cual servirá para el control de fase relativa en un lazo de retroalimentación (Lazo de Costas), de este modo se logra mantener el amarre de fase en el sistema interferométrico del octapuerto. A continuación la señal es introducida a un polarizador de $\lambda/4$ para producir un estado de polarización circular.

Las señales del oscilador local y el estado coherente débil se combinan en el divisor de haz no polarizado (NPBS) 50/50 que está a la entrada del octapuerto, posteriormente, cada una de las señales que emergen del divisor son separadas en sus componentes vertical y horizontal. Las componentes verticales inciden en el fotodetector 1 (BHD1) y las componentes horizontales en el fotodetector 2 (BHD2). En estos últimos NPBS es en donde el ruido de vacío se introduce en el sistema a través de los puertos que no son utilizados. Las señales eléctricas de los fotodetectores que corresponden a las señales en fase (I) y en cuadratura (Q) son medidas en forma simultánea, estas señales representan las señales eléctricas en banda base empleadas originalmente para modular la portadora y usadas en el receptor para realizar el análisis estadístico para calcular el BER, SNR y la Información Mutua entre Alice y Bob, éstos parámetros son la base para determinar la viabilidad del enlace cuántico (el procesamiento inicial de los datos recibidos está descrito en el apéndice D). Las señales I y Q también son utilizadas para el lazo de retroalimentación para lograr el amarre de fase entre las señales de datos y oscilador local.

Dado que estamos utilizando un esquema interferométrico, no se cuenta un oscilador controlado por voltaje (VCO) para lograr el amarre de fase, sin embargo se implementó el equivalente a un VCO por medio de la señal de LO y el modulador de fase 2. Por lo tanto, no se tiene la necesidad de un sistema de sincronización con secuencia de aprendizaje o de una portadora residual para recuperar los datos, ésto último es de suma importancia en los sistemas de comunicaciones cuánticas y sistemas de criptografia cuánticas síncronas.

Se realizó un cálculo de los Voltajes de salida V_Iy V_Q de acuerdo a la Ecuación 1.30 y Ecuación 1.31 para ciertos valores de potencias de OL y de la Señal de datos, posteriormente se ajustaron los mismos valores de potencia de ambas señales y se midieron los voltajes en el osciloscopio. De acuerdo a los resultados se estima que la eficiencia cuántica lograda en el sistema es de 0.73 debido a las pérdidas ópticas y a las pérdidas por desacoplamiento espacial entre las señales del OL y la de datos.

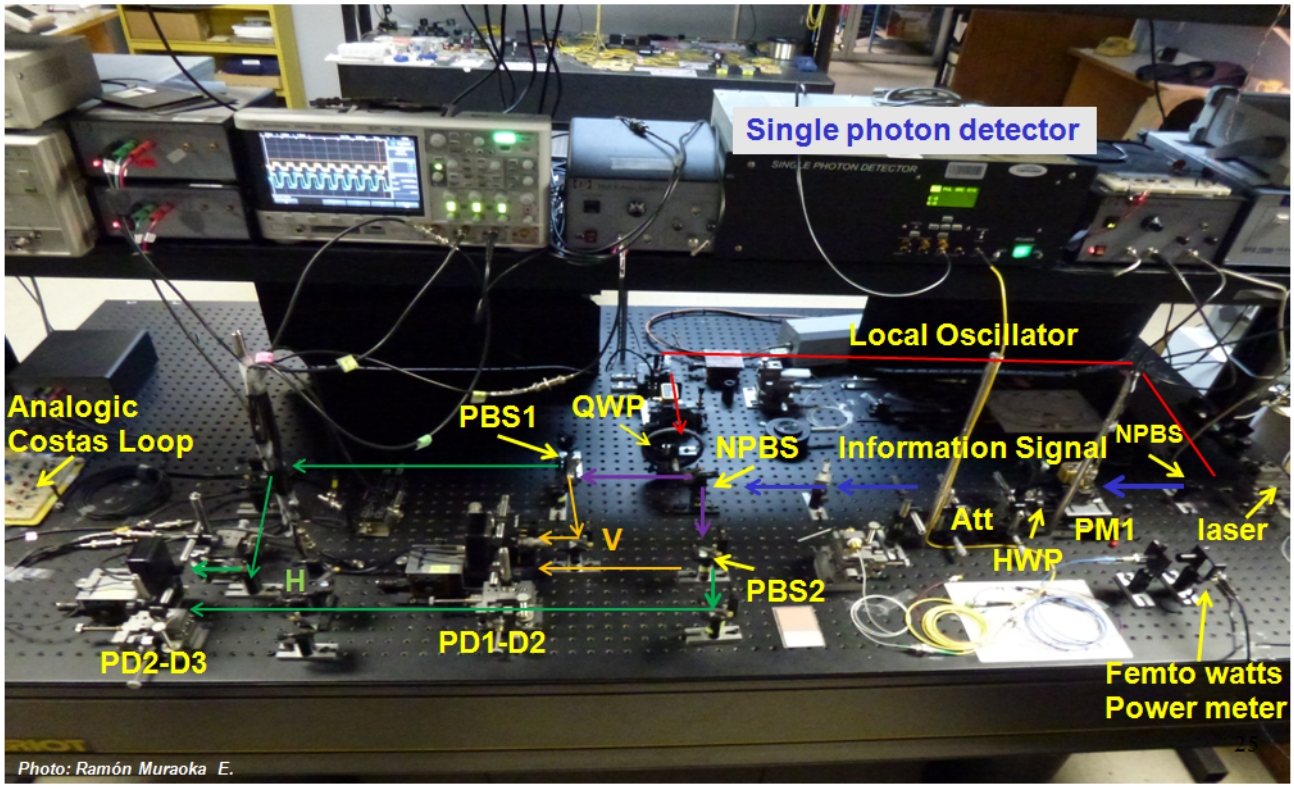


Figura 2.8.: Fotografia del montaje experimental del octapuerto homomodino para la tedección de estados coherentes débiles.

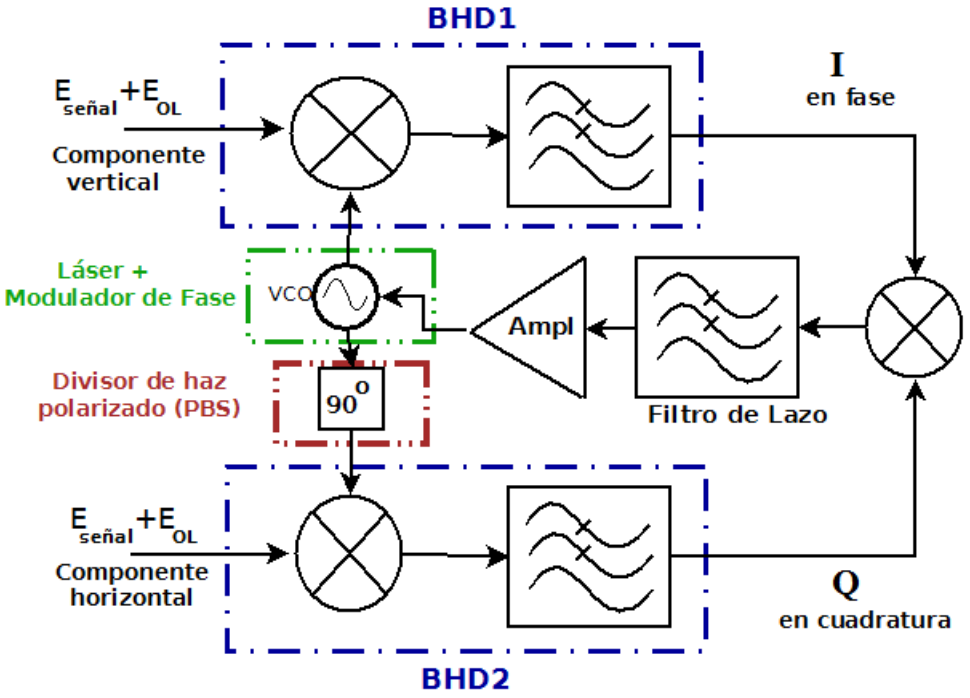


Figura 2.9.: Esquema de un Lazo de Costas general y los dispositivos equivalentes en el experimento.

2.5. Lazo de Costas para el receptor cuántico

Una vez que se cuenta con el sistema de detección caracterízado, y que se cuenta con los elementos para realizar la modulación del sistema, es necesario asegurar la estabilidad y encadenamiento de fase del oscilador local y los datos recibidos, para generar el homodinado necesario en el sistema de detección. Por éstas razones será necesario generar un esquema de estabilización para el receptor homodino.

2.5.1. Diseño del sistema de estabilización del receptor homodino.

Durante el desarrollo de la presente investigación, se implementó el lazo de Costas auto homodinado, con el fin de contar con un control de la fluctuación lenta del cambio de fase entre la señal modulada y la señal con la información; así como una evolución rápida de la fase, que puede presentarse en un enlace en espacio libre, debido a la turbulencia en la trayectoria del haz. Los resultados obtenidos presentan las variaciones correspondientes a la evolución rápida de fase y los tiempos de amarre logrados. Con base en el modelo general de un Lazo de Costas (ver Figura 2.9) primero se identificaron los dispositivos que realizan las diferentes funciones de los elementos del Lazo.

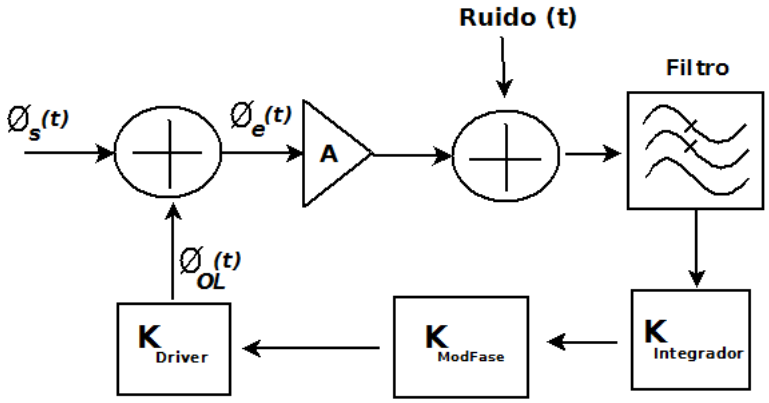


Figura 2.10.: Modelo del Lazo de Costas a pequeña señal.

De acuerdo al modelo de pequeña señal del Lazo de Costas [71, 68] que se muestra en la Figura 2.10, a las ecuaciones de la sección 1.7.2. y a las caracteristicas de los componentes (cuyos parámetros son proporcionados en los manuales correspondientes por los fabricantes), se realizaron los cálculos para el diseño del lazo para 1, 2, 3, 4 y 5 fotones. Los resultados de los cálculos de los filtros se muestran en el apéndice C.

Ganancia del integrador (K_i)= 0.3 @ 350 KHz

Ganancia del driver del modulador de fase (K_{Driver})= 40V/V

Ganancia del Modulador de fase ($K_{Modfase}$)=9.67×10^{-3} rad/Volt

Frecuencia moduladora ($f_{moduladora}$)=350 KHz

Ganancia del VCO-PM (K_{VCO-PM})=$K_i\ K_{Driver}\ K_{ModFase}\ f_{moduladora}$

$K_{Detector} = \frac{1}{2}(1000)(0.84)\, F_R\, G_{BHD} \sqrt{P_{OL} P_{señal}}$ V/rad

$K_{Lazo} = (K_{VCO-PM})(K_{Detector})$

T_p (Periodo de la señal de datos $f = 350\ KHz$)= 10 μseg

$\triangle\nu_1$= 350KHz ,

ζ (Factor de amortiguamiento) = $\frac{1}{\sqrt{2}}$

N (número de fotones)

Dado que la frecuencia natural del sistema es dependiente del número de fotones (N), es necesario calcular e implementar un filtro de lazo para cada N diferente, y elegir el que se necesita por medio de un interruptor. Se midió el retardo de la señal de retroalimentación que fué de aproximandamente de $0.6 \times 10^{-6} s$, tiempo que de acuerdo a los resultados es necesario reducir para que la señal de corrección de error llegue a tiempo y se efectúe el amarre de fases. La optimización de este parámetro está fuera de los alcances de este trabajo y forma parte de

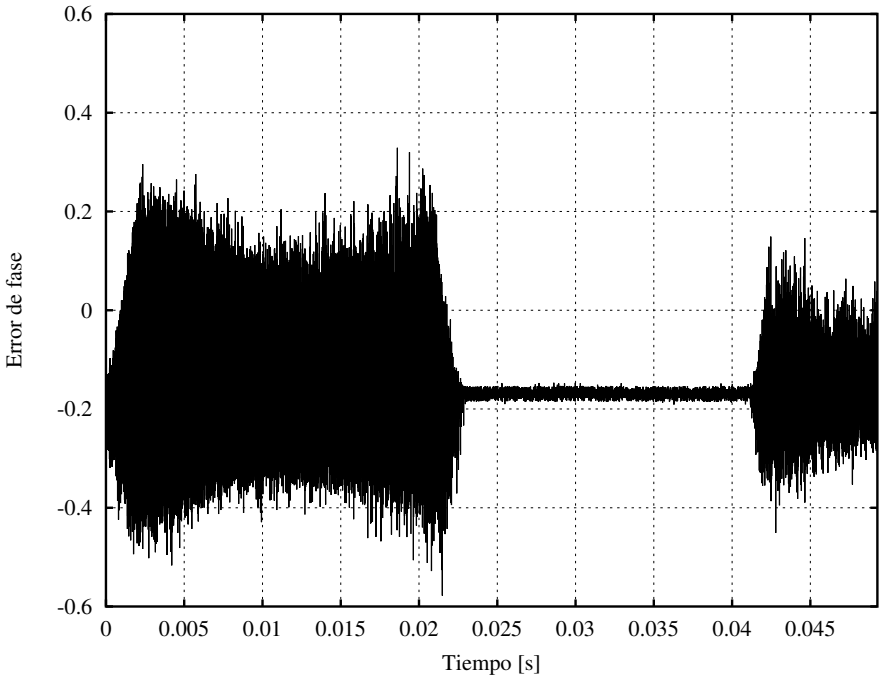


Figura 2.11.: Salida del integrador del lazo de Costas en donde se muestran periodos de no amarre-amarre-no amarre de fase.

la siguiente etapa del proyecto en la cual el Lazo de Costas tiene una implementación digital basada en Arreglos de compuertas lógicas programables (*Field-Programmable Gate Arrays*, FPGA's por sus siglas en inglés).

La Figura 2.11 muestra la salida del integrador del lazo, en donde se observan los intervalos de tiempo de no amarre con V_{salida} que tienen valores de máximo 0.2 mV hasta -4 mV, mientras que los intervalos de amarre de fase van desde los -0.18 mV hasta los -0.16 mV. El tiempo de amarre del lazo es aproximadamente de 20ms, lo cual no permitía la estabilización de las señales de salida de forma adecuada.

Se han reportado sistemas de en donde se implementa el amarre de fase entre señales de muy bajas potencias, por ejemplo, en Liao et al. [72] se logró un amarre de fase entre una señal de $2pW$ y la señal de referencia (OL) de $200\mu W$, el cual duró 1.5 minutos, lo que nos indica la necesidad de mejorar el tiempo de amarre, aún con las señales tan débiles que se utilizan en el sistema.

2.6. Experimentos desarrollados

Una vez caracterizados los componentes del sistema, se diseñaron e implementaron una serie de experimentos con el fin de asegurar que el canal de comunicaciones y el sistema de detección cumplen con los requerimientos que exige un enlace de comunicaciones cuántico para criptografia cuántica. En un enlace de este tipo el ruido cuántico tiene valores cercanos a la potencia de la señal que contiene la información, esta condición implica que se observan relaciones señal a ruido cercanas a 1, que a su vez implican un enlace en un canal sumamente ruidoso, lo anterior impone condiciones de tasas de error de bit del orden de valores que oscilan entre los 0.1 y hasta 0.5 y bajo estas condiciones es importante cotejar que la información que ha transmitido Alice y ha recibido Bob se mantengan dentro de ciertos niveles, los cuales se miden a través del parámetro de información mutua. Si un sistema para comunicaciones con criptografia cuántica cumple con estas condiciones, es posible asegurar experimentalmente su viabilidad para implementarlo fisicamente. Si bien podemos determinar tanto la tasa de bits erróneos como la información mutua entre Transmisor y Receptor partir de la SNR, experimentalmente se extrae esta información de los observables que en nuestro caso corresponden a las señales en fase y cuadratura (I y Q) que contiene el fotón recibido.

Para ello, se han elegido analizar los siguientes parámetros y condiciones para 5,4,3,2, y 1 fotón por bit promedio medidos:

1.- Análisis de los valores detectados en los fotodetectores balanceados I y Q.

2.- Determinación de la estadística de los voltajes de salida en la señales I y Q en un esquema de post-procesamiento, empleando un programa automatizado en Matlab para el análisis de valores media, desviación estándar y varianza simultánea

3.- Determinación de la tasa de error de bit mediante un programa en Matlab.

4.- Determinación de la Información mutua Alice-Bob a partir de las señales I y Q, y cálculo de la Información mutua entre Eva y Bob, en caso de que hubiera un espía. Mediciones de 10, 5, 4, 3, 2 y 1 fotón.

5.- Medicion de los periodos de estabilidad del lazo de costas empleando un esquema analógico para retroalimentación.

Los resultados y análisis se muestran en el siguiente capítulo.

3. Mediciones y análisis de resultados

3.1. Introducción

Tras desarrollar la propuesta experimental e implementar el sistema de comunicación óptico por criptografía cuántica, es necesario analizar los resultados experimentales de distintos aspectos del sistema. Como primer paso se identifican las características de la señal eléctrica recibida en los fotodetectores balanceados, con el fin de determinar el ancho de banda eléctrico, que se puede esperar en las señales I y Q recibidas.

La ventaja de contar con el esquema óptico del octapuerto, es que permite mantener estabilidad en el estado de polarización de las señales transmitidas en espacio libre, de modo tal que los divisores de haz polarizados nos permiten emular el efecto de defasamiento entre las componentes de campo eléctrico de las señales requerido para el oscilador local en un esquema de detección homodina por Lazo de Costas.

3.2. Señal coherente débil detectada.

En el sistema de fotodetectores balanceados, como se describe en la sección Sección 2.3 en la página 40 la dificultad de la medición en bajo número de fotones y el uso del octapuerto, se genera por la presencia de ruido cuántico. Dada la densidad de potencia para el caso de bajo número de fotones y la potencia óptica del ruido que es muy cercano al nivel de potencia de la señal (recordemos que la relación señal a ruido en el caso de 1 fotón por bit es de 2 como lo implica la Ecuación 1.53 en la página 31), el nivel de ruido puede parecer excesivo, e incluso, resultar difícil de determinar si la señal se recibe de manera correcta a simple vista. Ésto puede observarse en la Figura 3.1. En ella se observa el comportamiento eléctrico de la salida de los fotodetectores balanceados, correspondientes a: en la parte superior la señal I (1), en la región media la señal Q (2) y en la parte inferior de la imagen, la señal eléctrica correspondiente a los datos (3) que presenta un defasamiento determinado por los circuitos eléctricos empleados para la modulación de la señal a transmitir, y que es empleada para controlar el modulador electroóptico del sistema transmisor.

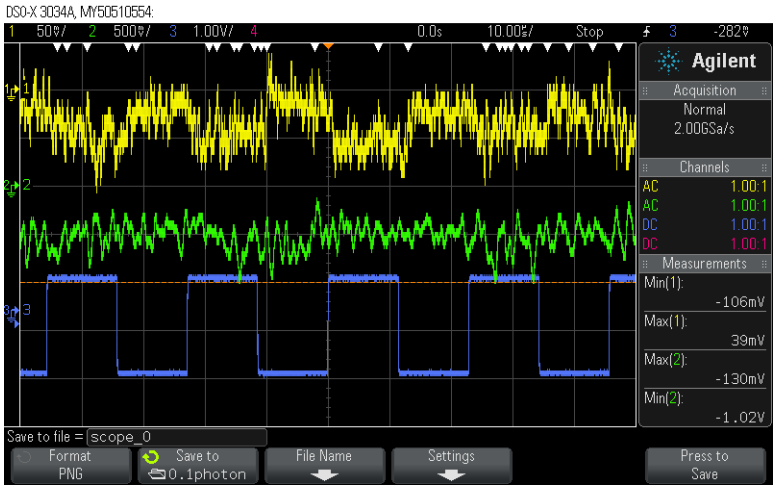


Figura 3.1.: Señales I y Q en el dominio del tiempo, para 1 foton por bit promedio. La gráfica en color amarillo es la señal en fase (I), en color verde se tiene la señal en cuadratura (Q) y en color azul se tiene la señal transmitida que es la salida del generador de señales.

A simple vista, puede apreciarse las variaciones eléctricas, en un momento en que la señal se encuentra en la fase adecuada, tal que la señal eléctrica en el brazo Q no contiene información de datos, y en cambio, contiene únicamente una señal eléctrica generada por el ruido, que predomina en el fotodetector balanceado Q. En el caso de la señal eléctrica correspondiente al brazo en fase, es posible apreciar que la relación señal a ruido generada en el detector balanceado, se encuentra dentro del comportamiento esperado para una relación señal a ruido de 2. No es posible observar con absoluta certeza el comportamiento de los datos recibidos; sin embargo la evolución eléctrica del ruido, "sugiere" que es posible determinar la posible presencia de la señal de datos, enmascarada por el ruido cuántico. Éstos resultados se analizan posteriormente para identificar el comportamiento estadístico de los valores en nivel 1 o en nivel 0.

3.3. Determinación de la varianza de las señales coherentes débiles detectadas.

Como hemos mencionado, para identificar el BER, así como para determinar el valor óptimo para identificar la presencia de un dato "1" o de un dato "0", es necesario realizar un análisis estadístico del comportamiento de los valores de voltaje asociados a ambos datos. Para realizar éste análisis, se emplea una comparación de los datos modulados (señal original de datos), con los datos recibidos (señal modulada), y una vez ajustados los parámetros de fase correspondiente, para hacer coincidir los datos de nivel 1 o nivel 0, se procede a separar los

voltajes detectados durante el periodo de los datos. De esta manera es posible analizar para una larga serie de bits, el comportamiento estadístico de voltajes para los niveles de 1 y de 0. Se realizaron también experimentos en los cuales se contaba únicamente con una serie de datos en nivel 1 solamente o serie de datos en nivel 0, para realizar la comparación entre éstos datos estadísticos, y los datos estadísticos de los niveles extraídos por comparación con los datos orginales, y los resultados obtenidos fueron consistentes entre sí.

Una muestra del análisis estadístico se observa en la Figura 3.2. En la figura puede apreciarse una estadística ajustada a la curva gaussiana, partiendo de los valores promedio y de desviación estándar de cada uno de los datos. En el caso de los datos cuya fase coincide con 0 grados (marcados con x en la gráfica), se puede observar un comportamiento estadístico congruente con lo esperado. La desviación estándar se encuentra muy cercana al margen que separa los datos 1 y los datos 0. La separación indica que la relación señal a ruido en estos resultados es ligeramente superior a 2, lo cual puede deberse a una potencia promedio ligeramente superior a 1 fotón por bit, sin llegar a ser mucho mayor. Los datos correspondientes la fase de 180 grados, se muestran con símbolos cuadrados en la gráfica, su distribución presenta una desviación estándar ligeramente mayor, que puede estar asociada con algunos ajustes de voltaje para la alimentación del modulador electroóptico del transmisor (en ocasiones éste se encontraba desbalanceado). Aún con los detalles asociados a la implementación del sistema, es evidente que la estadística nos muestra niveles de voltaje promedios, que nos permiten reconocer los niveles 1 y 0 para la señal BPSK transmitida, y contenida completamente en el brazo en fase (I).

Con el objetivo de realizar un análisis para determinar si las observaciones resultan válidas, se realizaron distintos experimentos, con niveles de potencia óptica mayores y menores a 1 fotón por bit. Probablemente el caso más relevante, sea el caso de una potencia promedio de 0.25 fotón por bit. Nuevamente se ha realizado una comparación de niveles de potencia para niveles de 1, 0 y para patrones de ceros y unos, y para la transmisión de datos pseudoaleatorios. El análisis estadístico de los voltajes medidos, arroja una variación estadística como la mostrada en la Figura 3.3. Como se puede apreciar, el ruido cuántico se mantiene constante, por lo que cualquier incremento que se presentara en la varianza(ruido) sugiere la presencia de un espía; por otro lado, los niveles de la media para los datos 1 y 0, disminuyen de valor esto quiere decir que se está controlando la cantidad de fotones en el sistema, es decir, la potencia equivalente a un solo foton por bit promedio o menos, tal como es requerido en un sistema de criptografía cuántica.

La curva corresponde a una situación donde los valores de las varianzas de los datos 1 y 0, coinciden con los voltajes promedio de los datos. Es decir que estadísticamente la probabilidad

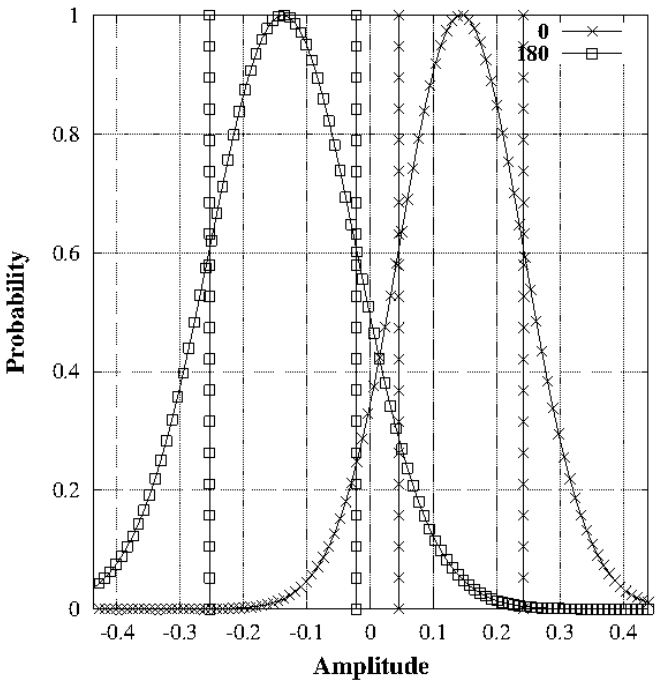


Figura 3.2.: Histogramas para los niveles lógicos del 1's y 0's de los datos recibidos (I), para N=1 fotón por bit promedio.

de detectar los niveles 1 y 0 llegan al límite es decir, ya no se puede discernir correctamente entre los niveles lógicos, es decir se llega al límite de Shannon, en donde la energía de bit es igual a la energía de ruido y el BER se incrementará considerablemente.

En la Figura 3.4 pueden observarse los análisis de la función conjunta de probabilidad (función $\boldsymbol{Q}$) obtenidos de los datos para I y Q. En estas representaciones se observan de manera simultánea el comportamiento estadistico de la señal en fase y cuadratura que nos permiten determinar con presición la estadistica de los datos, en la columna del lado izquierdo (figuras a) y c)) se observan los datos sin procesamiento obtenidos de la detección en el lazo de Costas y puede observarse claramente cómo la representación de los dos simbolos derivados de la modulación BPSK son discernibles, mientras que en la columna derecha (figuras b) y d)) se observan los resultados del post procesamiento y de igual forma describe el punto en el cual puede identificarse el umbral de desición. En el renglón superior se observan los histogramas correspondientes de la densidad de probabilidad, mientras que en el renglón inferior (figuras c) y d)) se observa una representación de curvas de nivel de las probabilidades asociadas a los simbolos correspondientes al 1 y 0.

En la figura a), se puede apreciar la distribución del muestreo de una señal de 1 fotón por bit, para 1200 muestras, es decir el equivalente de 400 muestras para los tres bit detectados en una lectura del osciloscopio, para una señal pseudoaleatoria, con predominancia de datos

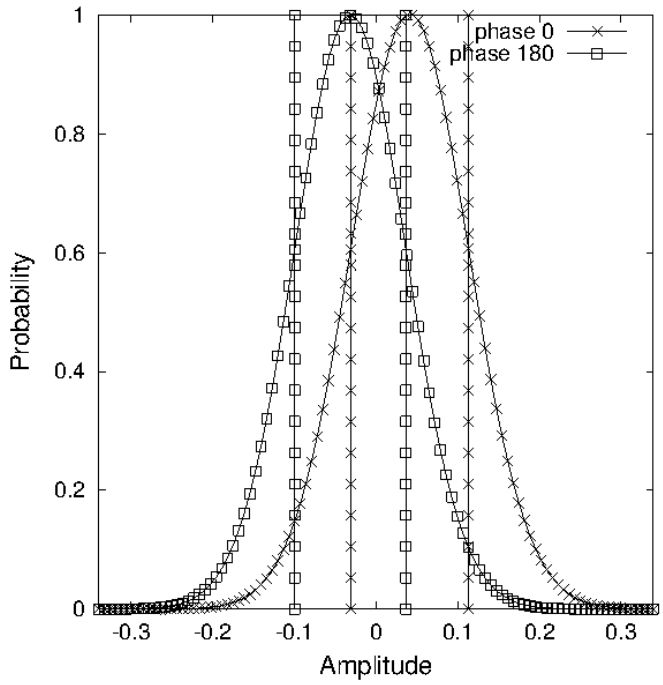


Figura 3.3.: Histogramas para los niveles lógicos del 1's y 0's de los datos recibidos (I), para N=0.25 fotones por bit promedio.

0. En ella se puede apreciar para un valor de paroximadamente -0.1 V para el canal I y de 0.05 para el canal Q. Para el caso de los datos en "1", se observan niveles de voltaje de 0.1 V para el canal I y de -0.5 V para el canal Q. La figura c) muestra las curvas de contorno asociado a histogramas de los datos "1" y "0". A partir del análisis de los histogramas, se determina el valor promedio, la varianza y la desviación estándar. Una vez analizados los datos estadísticamente se pueden observar las curvas estadísticas para los valores asociados en las figuras b) y d). A partir de estos resultados puede observarse que en una densidad de probabilidad de 0.4 se da el traslape de símbolos, ésto solamente se puede presentar en condiciones en donde la relación señal a ruido es cercana a 1 y estamos muy cercanos al límite cuántico estándar. Lo anterior indica que en un proceso de recuperación de bits el umbral de desición tradicional puede ser aplicado coincidiendo los criterios de detección de señales en sistemas de comunicaciones en ambiente ruidoso con las codidiciones que nos arroja un enlace cuántico.

Partiendo del conocimiento de que el ruido cuántico se mantiene constante, al reducir la potencia de los simbolos se tendrá asociado un corrimiento del valor de la media, y dado que la varianza no cambia su posición deberá recorrerse proporcionalmente al que se ha recorrido la media. En este caso se redujo la potencia de la señal al equivalente a 0.25 fotones por bit promedio, y se observa que el límite inferior de la varianza de la distribución de probabilidad

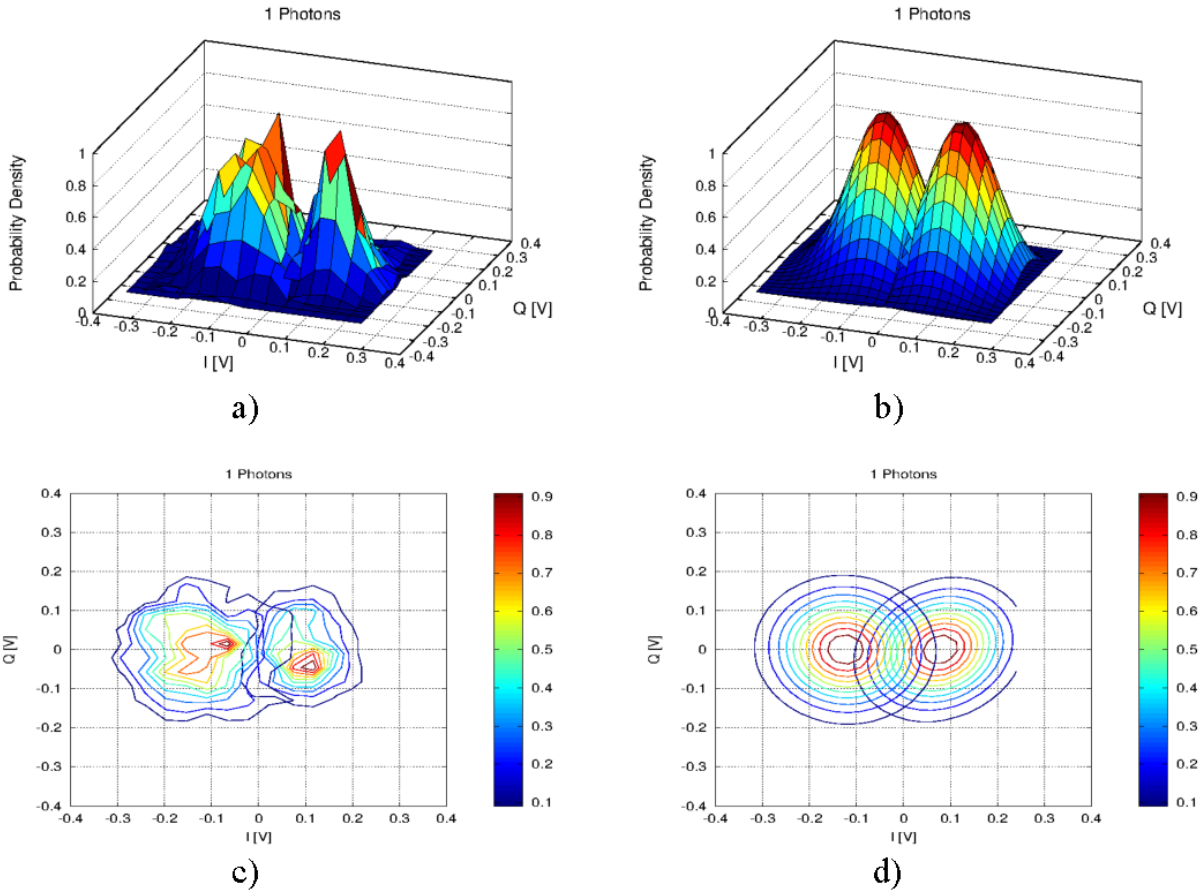


Figura 3.4.: Resultados para 1 fotón por bit. a) Distribución de probabilidad de la función Q utilizando los datos antes del procesamiento (originales), b) Distribución de probabilidad reconstruida a partir del cálculo de la media y la varianza obtenida de los datos originales, c) Líneas de contorno obtenidas utilizando los datos originales, d) Líneas de contorno obtenidas a partir de la distribución de probabilidad reconstruida.

del simbolo 1, coincide con el pico máximo de la distribución de probabilidad del simbolo 0, esto se observa en la figura 3.5 d) en el punto I=0.04, Q=0. Esto nos sugiere que para potencias equivalentes a 0.25 fotones la probabilidad de error ya es muy alta.

En la Figura 3.5 puede observarse los análisis obtenidos de los datos para I y Q. En la figura a), se puede apreciar la distribución del muestreo de una señal de 0.25 fotones por bit, para 1200 muestras, es decir el equivalente de 400 muestras para los tres bit detectados en una lectura del osciloscopio, para una señal pseudoaleatoria, con predominancia de datos "0". En ella se puede apreciar para un valor de aproximadamente -0.1 V para el canal I y de -0.21 para el canal Q. La figura c), muestra las curvas de contorno asociado a histogramas de los datos 1 y 0. A partir del análisis de los histogramas, se determina el valor promedio, la varianza y la desviación estándar. Las curvas gaussianas asociadas a la media, varianza y promedio, muestran la dificultad asociada a determinar con precisión los datos 1 y 0, bajo estas condiciones.

3.4. Determinación de la Tasa de Error de Bit

A partir de los valores medio y de desviación estándar de los datos, es posible obtener la relación señal a ruido, y en consecuencia encontrar la tasa de error de bit del sistema. De los resultados teóricos, es posible calcular los niveles de BER como lo muestra la Figura 3.6, al comparar los resultados teóricos con las mediciones experimentales se observa que las mediciones se acercan al comportamiento teórico esperado. Tal como se esperaba el error del sistema tiende a incrementarse al reducir la potencia de la señal transmitida.

Los resultados muestran congruencia entre las mediciones estadísticas y un conteo comparativo dato por dato de los resultados recibidos, contra los transmitidos. Para el cual se desarrolló un programa en MATLAB, cuya estructura identificaba los valores de "1" o "0" en función del promedio del voltaje durante un periodo de bit, y un comparador; y después verificaba bits erróneos al comparar éste resultado contra los datos originales.

3.5. Determinación de la Información mutua

Como se vió en la sección 1.4, la información mutua es una medida de la cantidad de información que recibe Bob de Alice, si la información mutua tiene un valor de 1 quiere decir que Bob tiene la certeza de que recibió todos los bits correctamente y valores por debajo de éste indica que hay un grado de incertidumbre en la detección. En el caso de la intromisión

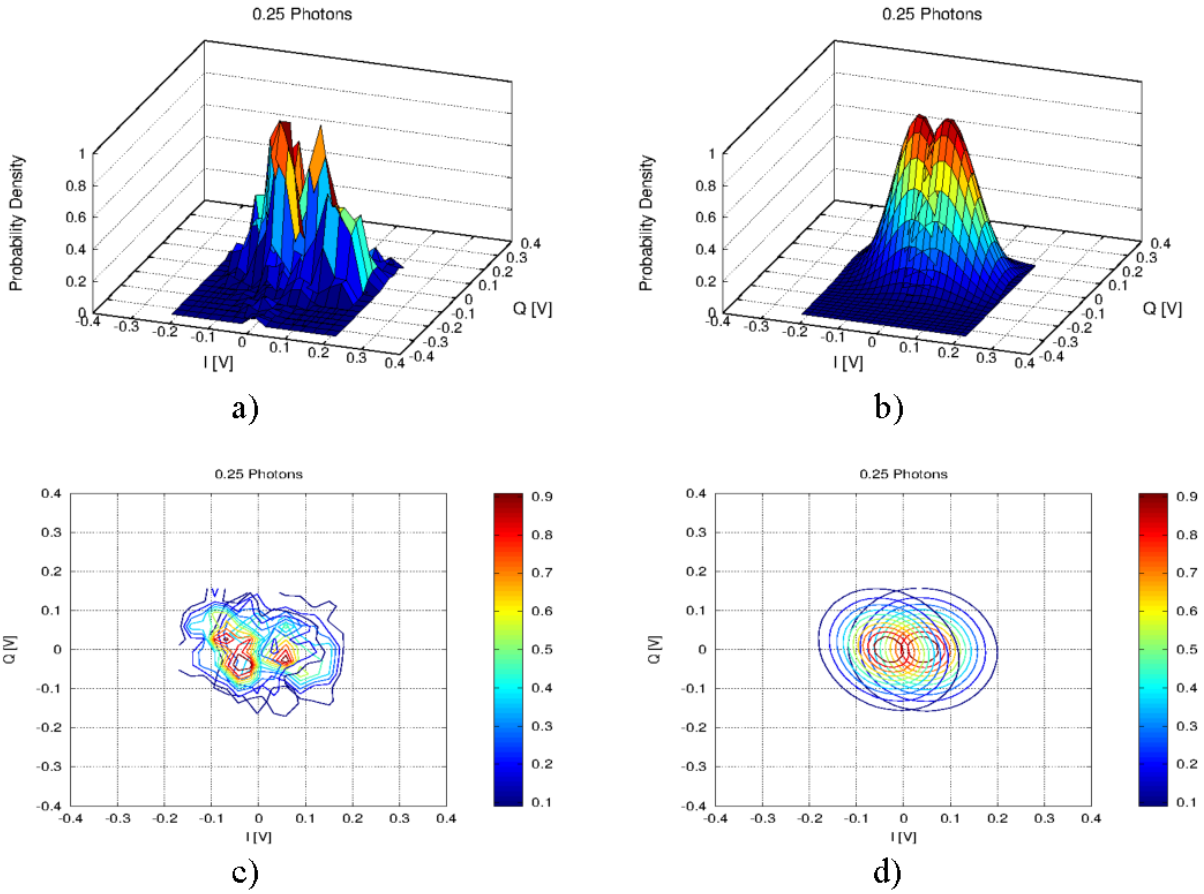


Figura 3.5.: Resultados para 0.25 fotones por bit. a) Distribución de probabilidad de la función Q utilizando los datos antes del procesamiento (originales), b) Distribución de probabilidad reconstruida a partir del cálculo de la media y la varianza obtenida de los datos originales, c) Líneas de contorno obtenidas utilizando los datos originales, d) Líneas de contorno obtenidas a partir de la distribución de probabilidad reconstruida.

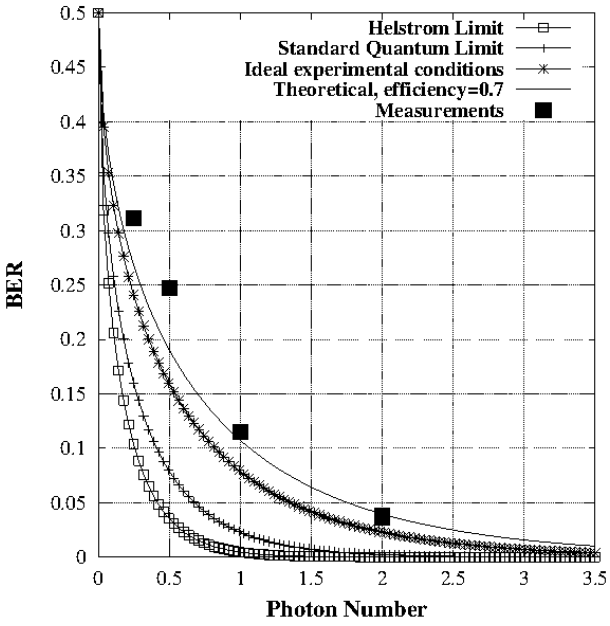


Figura 3.6.: Tasa de bits erróneos para diferente número de fotones: a) Límite de Helstrom, b) Límite cuántico estándar, c) Condiciones experimentales ideales, d) condiciones teóricas con eficiencia η=0.7 y e) datos medidos.

de Eva con un ataque con divisor de haz (colocado en su trayectoria), se tendrán puertos no utilizados lo cual incrementa aun más el ruido cuántico, lo que resulta en una disminución de la información mutua; en ese momento es cuando se realiza la toma de desición para detener la transmisión de datos. Si podemos identificar si el sistema cumple con los valores esperados de información mutua teórico, consideramos que es un sistema viable para su implementación en un sistema de comunicaciones fotónicas actuales. Dada al importancia de este parámetro, éste se calcula mediante un procesamiento de datos se realiza fuera de línea empleando datos experimentales, realizando una comparación entonces, contra los valores medidos y los valores teóricos.

Como se observa en la figura Figura 3.7 se observa la comparación de los valores de información mutua para cinco casos: a) Límite de Helstrom, el cual se deriva de una teoría estadística propuesta por C.W Helstrom en la década de os 60s, que calcula la mínima probabilidad de error alcanzable teóricamente para una detección cuántica en condiciones ideales lo que permite llegar al límite cúantico estándar. En el caso de señales binarias propone dos hipótesis para el resultado llamadas H_0 y H_1 [53], que corresponden a las hipótesis de que el bit transmitido fue 0 y 1 respectivamente, el siguiente caso es el b) Límite cuántico estándar, en donde el límite es el nivel del ruido cuántico, c) Condiciones experimentales ideales, en este caso se considera el ruido cuántico y ruido electrónico, pero no se toman en cuenta las pérdidas por acoplamiento del haz entre los diferentes dispositivos a través de los cuales viaja la se-

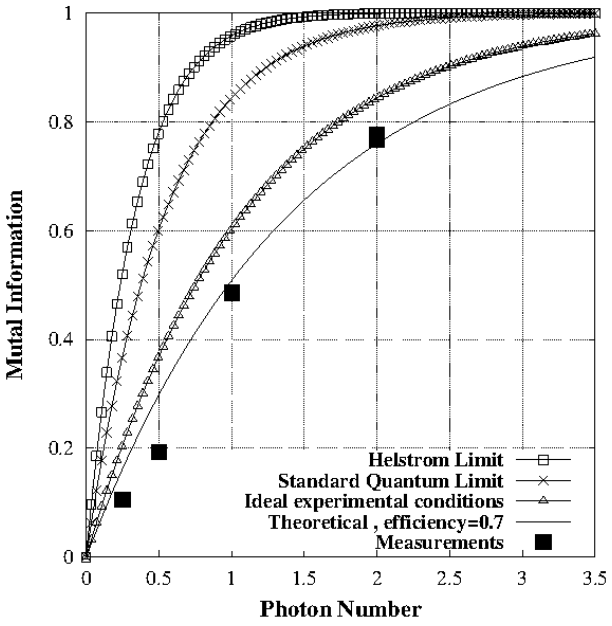


Figura 3.7.: Información Mutua para diferente número de fotones: a) Límite de Helstrom, b) Límite cuántico estándar, c) Condiciones experimentales ideales, d) condiciones teóricas con eficiencia η=0.7 y e) datos medidos.

ñal óptica, el caso d) Condiciones teóricas con eficiencia de 0.7, contempla las pérdidas por acoplamiento y atenuación de la señal óptica en la trayectoria (ver Apéndice B) y finalmente el caso e) Datos medidos, es la información mutua calculada de los datos experimentales. El error relativo porcentual en el caso de 1 fotón por bit comparando los casos d) y e) es de 4.48 %, mientras que para 2 fotones por bit el error es de 2.19 %, los cuales se consideran adecuados considerando el bajo nivel de potencia al trabajar al niveles cuánticos.

Otras mediciones realizadas, nos permiten identificar la comparación entre la relación señal a ruido teórica, de un sistema ideal (eficiencia cuántica unitaria), contra las mediciones de nuestro sistema (eficiencia cuántica de 0.7). Como se muestra en la Figura 3.8, para las condiciones de 1 fotón por bit, el análisis de los datos muestra una relación señal a ruido de 7.8 dB para el caso de 5 fotones por bit, un valor cercano a los 5 dB, en el caso de los 4 fotones por bit. En el caso de 2 fotones por bit, el resultado nos ofrece un valor cercano a 4 dB, mientras que en 1 foton por bit, los resultados muestran una relación señal a ruido ligeramente mayor a 1 dB. los resultados para 0.5 y 0.25 fotones por bit, se incluyen para remarcar que las mediciones y experimentos desarrollados, presentan el comportamiento esperado, considerando la diferencia de la eficiencia cuántica entre el caso teórico ideal y los resultados experimentales.

En la Figura 3.9 se muestra la máxima capacidad que es posible alcanzar para nuestro sistema

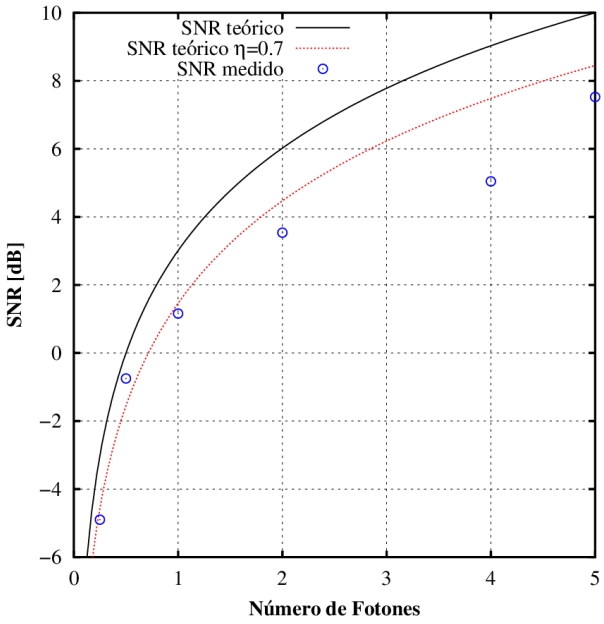


Figura 3.8.: Relación señal a ruido (SNR) vs Número de fotones (N)

BPSK al emplear un canal cuántico. se muestran y comparan resultados para una capacidad de canal ideal, teórico con eficiencia de 0.7 y de los datos obtenidos en las mediciones. Si bien el sistema se ha empleado para una transmisión de 350 kbps los resultados sugieren que es posible alcanzar una capacidad de canal de 750Kbps y mejorando la eficiencia estaríamos cercanos a 1Mbps.

Una vez identificados los valores actuales alcanzables por el sistema, es importante identificar las limitaciones que se pueden presentar. Uno de los elementos que son de particular interés es el correspondiente al desviación estándar, asociado al factor $1/e$ de la distribucion gaussiana. Los resultados experimentales para el caso de ambas cuadraturas, se aprecian en la Figura 3.10, y puede apreciarse que los resultados se mantienen congruentes con lo ya presentado. Éstos datos están relacionados con la varianza y la relación de incertidumbre.

A partir de los resultados experimentales, se obtiene la gráfica que representa la relación de incertidumbre en la Figura 3.11. Se sugiere la posiblidad que una diferencia en la ganancia de los fotodetectores balanceados, genera una diferencia entre los resultados de la varianza de I y de Q, aunque también ésta diferencia podría deberse a un trayecto óptico más largo en el brazo I del sistema.

Todos los resultados anteriores, nos proporcionan parámetros para determinar la información mutua, que finalmente nos determinan la capacidad de Alice y Bob de intercambiar la información de manera adecuada, con los valores de confiabilidad que nos permite el sistema de comunicaciones cuánticas, con la baja relación señal a ruido.

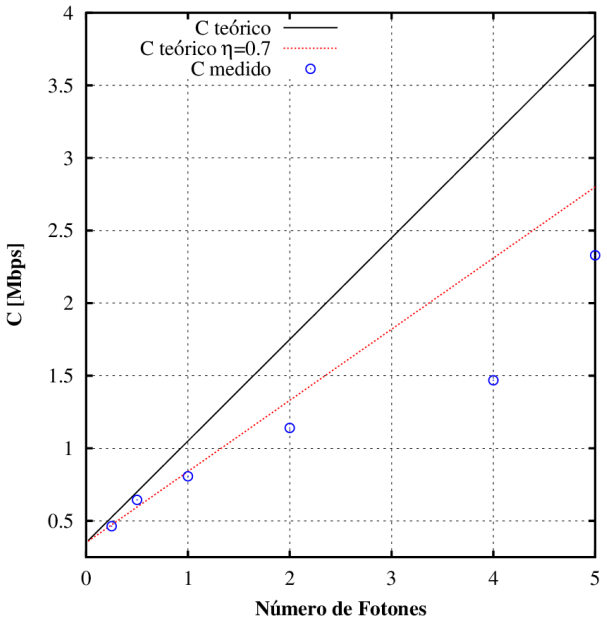


Figura 3.9.: Capacidad de canal (C) vs Número de fotones (N)

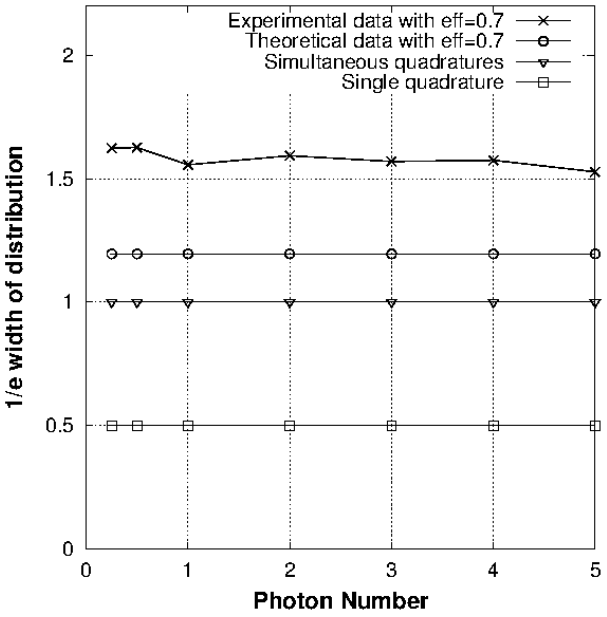


Figura 3.10.: Ancho de 1/e de la distribución en función del número de fotones para a) medición con una sóla cuadratura, b) cuadraturas simultáneas, c) resultados teóricos para nuestro experimento con eficiencia η=0.7 y d) resultados experimentales con eficiencia η=0.7

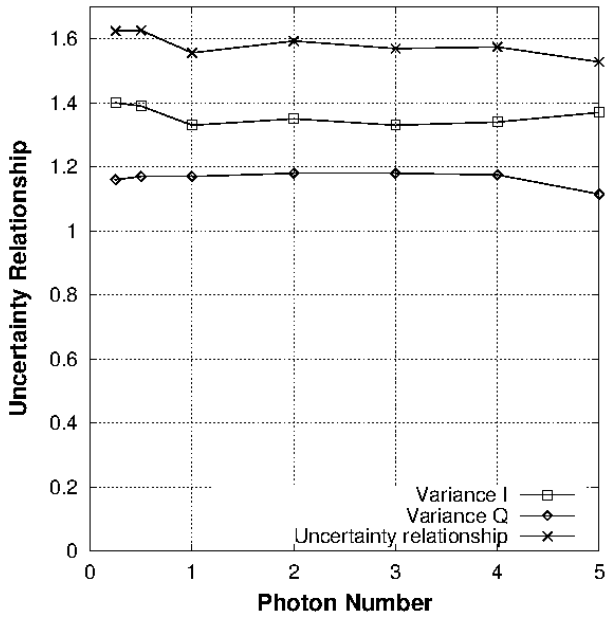


Figura 3.11.: Relación de incertidumbre para las cuadraturas I y Q en función del número de fotones.

La Figura 3.12 surge del análisis presentado en la sección 1.4, y nos permite identificar los efectos sobre la Información mutua de Alice y Bob, del ruido que provoca un ataque al enlace por medio de Eva. Como se puede observar, conforme el ruido de Eva se incrementa, la información mutua de Alice y Bob I_{AB} decae, lo que permite identificar inmediatamente si existe la intervención de un espía. La varianza en el transmisor de un sistema de variables continuas, en el que Alice imprime cierta incertidumbre en el proceso (la Varianza proporcionada por Alice V_A= 0), cuenta con mejor desempeño de Información mutua, ya que el ruido que puede interceptar Eva en el sistema generará una degradación más pronunciada, ofreciendo la capacidad de detectar intrusiones del sistema.

Desde la perspectiva de la información mutua que existe entre Bob y Eva (mostrada en la Figura 3.13), es claro que para que la información que Eva extrae del sistema presente sea parecida a la que recibe Bob (y por consiguiente, para que le ofrezca a Eva la posibilidad de extraer la información transmitida por Alice), se requiere de niveles de ruido mayores a 0.5, para que con las varianzas de Alice, el sistema de Eva, cuente con la capacidad de robo de información.

De los resultados obtenidos, podemos también extrapolar las condiciones en que el intercambio de la llave criptográfica cuenta con un nivel seguro de intercambio de información, identificado por las condiciones en las que la diferencia entre la Información mutua Alice-Bob (I_{AB}) y la Información mutua entre Eva y Bob (I_{EB}). Cuando el sistema muestra que la

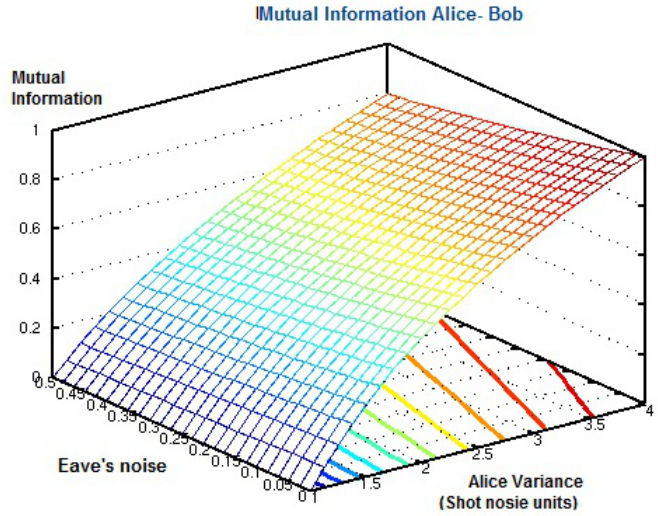


Figura 3.12.: Efecto del ruido causado por Eva en la Información mutua entre Alice y Bob

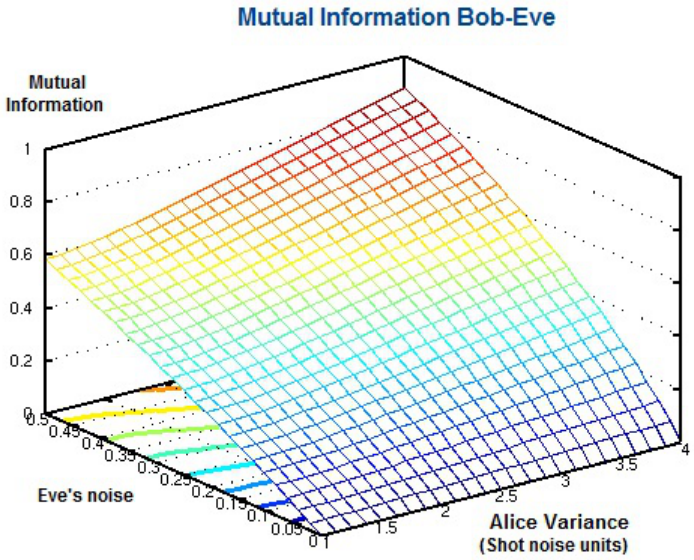


Figura 3.13.: Información mutua entre Bob y Eva.

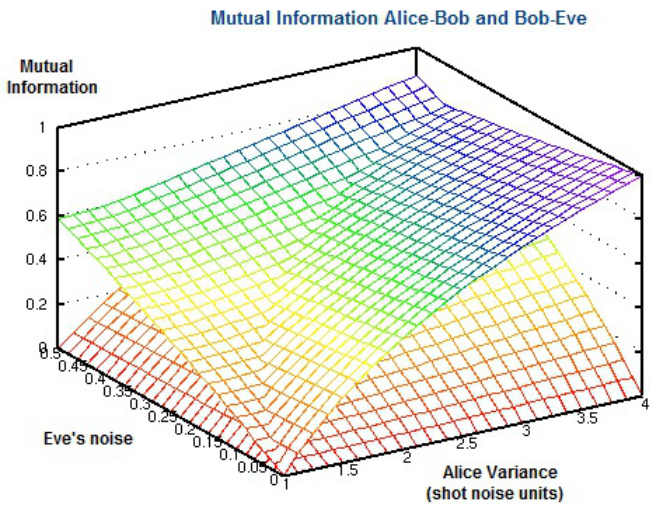


Figura 3.14.: Información mutua Alice-Bob y Bob-Eva

diferencia es positiva (ver Ecuación 1.9), implica que la información que es capaz de extraer Eva, no presenta condiciones que le permitan recuperar o extraer información valiosa con cierto nivel de certidumbre (Figura 3.15). A mayores inveles de incertidumbbre en la varianza del sistema por parte de Alice, el margen de zona segura, resulta menor, ya que Bob debe lidiar con las condiciones de incertidumbre de Alice y las que Eva inyectan al sistema. Éstos resultados, permiten predecir que para el sistema desarrollado, siendo que la varianza se encuentra cercano al valor de 2, el sistema presenta condiciones que permiten ofrecer seguridad, de acuerdo con los parámetros teóricos especificados en los análisis.

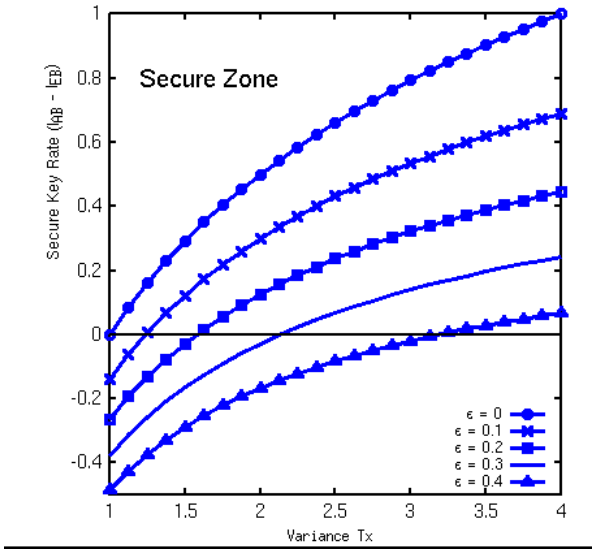


Figura 3.15.: Zona de seguridad para la distribución de la llave criptográfica.

4. Conclusiones

4.1. Introducción

Al inicio del presente trabajo, se propuso como elementos de tesis a comprobar cinco puntos, asociados con dificultades y propuestas que técnicamente no habían sido abordadas hasta la fecha, los resultados resultan satisfactorios, y es importante retomarlos, para remarcar los alcances, virtudes y limitaciones del trabajo.

4.2. Contribución y resultados obtenidos

En este trabajo se ha desarrollado un sistema de recepción homodina de 8 puertos, en espacio libre, de alta sensitividad, para la detección de señales coherentes débiles.

La primera contribución de este trabajo es la medición directa de la función de cuasiprobabilidad ($\boldsymbol{Q}$) cuántica midiendo las dos cuadraturas del campo óptico en forma simultánea, es decir, no es necesario realizar una medición tomográfica tradicional. Se logró dicha medición aun con el ruido de vacío adicional debido a la medición simultánea de las cuadraturas.

La segunda contribución es que se demostró que no es necesario contar con una señal de referencia adicional o señal portadora, aun trabajando a niveles cuánticos. El utilizar un esquema de portadora suprimida representa un ahorro de energía en un sistema de comunicaciones.

Adicionalmente se ha demostrado que el uso del esquema homodino, con estados coherentes débiles, cercanos al Límite Cuántico Estándar, permite la implementación eficiente de detección de las señales, por encima del ruido térmico y electrónico de los fotodetectores empleados. Ésto sugiere que un proceso de optimización del sistema, para alcanzar eficiencias mayores a 0.7, permitirá obtener resultados óptimos para el proceso de transmisión y recepción en un canal cuántico.

Otro resultado es que se observa que el sistema permite la detección de las dos cuadraturas I y Q, del campo óptico en forma simultánea, aún con la presencia del ruido adicional (ruido

cuántico) que se introduce por los puertos no utilizados en los divisores de haz polarizados. Los resultados demuestran que la presencia de éste ruido no reduce la capacidad de alcanzar la relación señal a ruido necesaria, para obtener la Tasa de Error de Bit requerido para el sistema, y los resultados estadísticos mantienen su distribución gaussiana, una vez que se han eliminado los ruidos electrónicos del sistema.

En el caso de la recepción se ha comprobado que es posible la recepción de la energía de un solo fotón por bit promedio (que es lo recomendable para fines de seguridad en un sistema de criptografía cuántica), empleando una fuente láser contínua, mediante un arreglo de atenuadores, para alcanzar la potencia equivalente a 45 fW de la señal coherente débil en un formato de modulación BPSK, comparado con otros sistemas de comunicaciones, que emplean pulsos ultracortos de gran número de fotones, para obtener la potencia equivalente por bit. Éste logro demuestra que, sí es posible la implementación de detecciones cuánticas homodinas, sin la necesidad de utilizar señales como señuelo para mejorar la seguridad, como en el caso de los sistemas criptográficos con centenas de fotones por pulso.

Con el uso de sistemas de fotodetectores balanceados, desarrollados con la tecnología empleada típicamente en sistemas de comunicaciones ópticas tradicionales, el sistema es capaz de recibir los datos débiles coherentes transmitidos, y ofrece la posibilidad de trabajar a mayores velocidades de transmisión en los esquemas de comunicaciones ópticas seguras con criptografía cuántica, lo cual ya ha sido reconocido en publicaciones cientificas que citan resultados parciales de este trabajo [73].

Los resultados de la Tasa de Bits erróneos, Relación señal a ruido y la Información mutua muestran valores muy cercanos a los calculados teóricamente y esperados dada la potencia tan débil de la señal recibida. Se estimó el efecto de la intromisión de un espía (Eva) en el enlace entre Alice y Bob para calcular los umbrales de seguridad en la Tasa de transmisión de la llave segura (*secure key rate*). A partir de éstos resultados se ha demostrado que el canal de comunicaciones cuántico desarrollado en espacio libre, puede ser utilizado para sistemas de Distribución cúantica de la llave criptográfica (QKD), y ésta tecnología puede ser aplicable a la distribución de llave criptográfica satelital, a enlaces de comunicaciones ópticas en línea de visibilidad directa y a sistemas de comunicaciones cuánticas por fibra óptica.

4.3. Otros resultados relevantes

Una ventaja observada en la implementación del sistema mediante este esquema, es que se emplean fotodetectores p.i.n que no requieren de sistemas de enfriamiento que suelen emplearse en otros esquemas para tratar de limitar el efecto del ruido térmico, y limitar las

contribuciones de ruido al ruido cuántico. El sistema con el esquema de fotodetectores balanceados presenta alta eficiencia cuántica (aprox. 90 %) y mediante una selección cuidadosa de componentes, es capaz de operar a las tasas de transmisión de las redes de comunicaciones actuales, lo que lo hace compatible con sistemas de Multicanalización por división de Longitud de Onda, y acercando el futuro de las comunicaciones ópticas seguras a las redes de comunicaciones actuales.

Se implementó un sistema de Lazo de Costas para el encadenamiento de fase de las señales de datos y la del oscilador local, lo que permite el uso de señales de datos con portadora suprimida que son económicas en potencia de portadora. El sistema basado en un procesamiento eléctrico de la señal recibida, mediante circuitería analógica, como prueba de concepto para la estabilidad del sistema lograron periodos cortos de estabilidad del lazo de costas, por lo que no se alcanzó una estabilidad de amarre de fase del oscilador local y de la señal suficiente para una visualización estable a largo plazo en el tiempo. Lo anterior se atribuye al retraso de la señal de corrección de error en la circuitería analógica, los resultados preliminares observados sugieren que la implementación del sistema de Lazo de Costas, se realice empleando técnicas de procesamiento digital de señales, en sistemas empotrados que ofrezcan al sistema tiempos de retraso más cortos.

Éste esquema experimental alcanzó una eficiencia de 0.7, cuyo valor se considera aceptable para su aplicación en esquemas de transmisión-recepción de señales por medio de canal cuántico, y de acuerdo a otros esquemas QKD experimentales desarrollados en otras partes del mundo. Es posible optimizar aún más el esquema y probablemente alcanzar una eficiencia cuántica de 0.8, mediante un trabajo más minucioso en el proceso de implementación del sistema.

Algunos experimentos preliminares, sugieren que es posible utilizar este esquema experimental como canal cuántico en un sistema criptográfico, tanto en espacio libre como en sistemas fibrados.

Un conjunto de publicaciones y presentaciones en congreso se pueden ver en el Apéndice A, y otras publicaciones están en proceso de desarrollo.

4.4. Trabajo a futuro

El proceso de un desarrollo tecnlógico y cientifico nunca concluye de manera definitiva, sin embargo, a través de los avances, en ocasiones modestos, es posible acercarse cada vez más a un sistema con capacidad de explotación técnica y tecnológica. El presente trabajo sugiere

algunas líneas de trabajo futuro para el esquema implementado, que permitirían mejorar los detalles observados durante el desarrollo de la tesis, consistentes en:

Mejorar el balance de la señal incidente en ambos fotodetectores, así como optimizar las trayectorias ópticas que recorren los haces hacia los fotodetectores balanceados, de tal manera que sea posible determinar con precisión si algunas diferencias en cuanto a la detección óptica de las señales en los brazos I y Q, se deben a la trayectoria óptica, o a una diferencia de los componentes fotodetectores; en cuyo caso sería deseable la implementación de los fotodetectores en un solo sistema integrado, para contar con un mejor control y mayor similitud en el comportamiento electrónico de los dispositivos empleados para éste trabajo.

La implementación del Lazo de Costas digital permitirá una estabilización de lazo de mucho mayor duración que con lo logrado en forma analógica, ya que los tiempos de retardo que se pueden presentar en el sistema, dependen en gran medida de la programación del dispositivo, la optimización de trayectorias eléctricas de los algoritmos, y la flexibilidad del diseño. El grupo de colaboración del Cuerpo Académico Sistemas Empotrados Aplicados a Comunicaciones Fotónica Instrumentación y Control (SEACFIC) de la Universidad Autónoma de Baja California, ha tenido avances en la caracterización y resultados preliminares del la implementación del Lazo de Costas basado en FPGAs, lo que ha brindado un panorama favorable para la continuación en el desarrollo del proyecto [74].

Se identificó una fuente de ruido de baja frecuencia, al parecer relacionada con la linea de alimentación de los sistemas, por ésta razón será conveniente implementar un filtro de baja frecuencia para controlar la evolución lenta de la componente espectral que se vizualiza en el momento en que se logra el procesamiento de los datos fuera de línea. Se estima que esta frecuencia es de aproximadamente 60 Hz.

Una vez optimizado el montaje experimental, es necesario introducir la presencia de un espía (Eva) para la caraterización del sistema, antes y después de la presencia del atacante. De la misma manera, se requere efectuar una estricta caracterización del sistema de detección y las perturbaciones generadas sin Eva y después con Eva para medir, comparar resultados y cuanfitificar el impacto en ambos escenarios.

Es necesario migrar a una modulación QPSK, para generar las condiciones adecuadas para producir la impementación del protocolo de comunicación requerido.

A. Productividad

A.1. Artículos publicados

Edith García, Francisco J. Mendieta, Josué A. Lopez, Eduardo Alvarez, Arturo Arvizu and Philippe Gallion. *Phase-Locked Homodyne Measurement of Quasiprobability Q Function and Detection of Information-Carrying Weak-Coherent-States*. Microwave and Optical Technology Letters. Vol. 55, No.10, October 2013. pp. 2431-2437.

Lopez, Josué, **Garcia Edith**, Arturo Arvizu, Mendieta Francisco and Gallion Phillipe. *Mutual Information in weak-coherent-state using a homodyne optical Costas Loop with different phase errors*. Microwave and Optical Technology Letters, Vol.55. Issue 4, April 2013.

Josué A. Lopez, Arturo Arvizu, **Edith García**, Francisco J. Mendieta, Eduardo Alvarez and Philippe Gallion. *Detection of phase-diffused weakcoherent- states using an optical Costas loop*. Optical Engineering 51(10), 105002 (October 2012).

A.2. Congresos presentados

Eduardo Álvarez Guzmán, **Edith García Cárdenas**, José L. González Vázquez1, José L. Del Río1, Josué A. López Leyva, Francisco J. Mendieta Jiménez, Jorge E. Loya Hernández y Arturo Arvizu Mondragón. *Quantum Key Distribution Detection System using FPGA's: Preliminary results*. Mexican Optics and Photonics Meeting 2013. September. Ensenada, B.C.

E. García, , J.A. López, , E. Álvarez, F. J.Mendieta and A. Arvizu. *Scenario analysis for performance evaluation of free space quantum and classical communication channels*. Conference 8842-13. SPIE 2013 Optics + Photonics, San Diego, California, USA. August 2013.

J.A. López, A. Arvizu, J. Roberto, Miguel V., Antonio F. S. ,J. Santos, F.J. Mendieta, R. Muraoka and **E. García**. *Preliminary Results of the First Optical Quantum Communication in Mexico: 2 photons/bit at 5 Mbps using 62 and 125 Km in a Commercial Optical Network*. TuD4.3 IEEE Summer Tropicals, Hawaii July 2013.

E. García, F. J.Mendieta , J.A. López, y E. Álvarez. *Protocolos para la distribución de la llave criptográfica utilizados criptografía cuántica.* Congreso Regional de Óptica (CREO) 2012. Ensenada, B.C. Septiembre del 2012.

Josué Aarón López Leyva, Arturo Arvizu, Francisco Javier Mendieta y **Edith García**. *Diseño e implementación de un lazo de Costas opto – electrónico optimo para la detección de estados coherentes débiles.* SOMIXXVII Congreso de Instrumentación Culiacán, Sinaloa, México 29-31 de octubre, 2012.

E. García, J.A. López, F.J. Mendieta, A. Arvizu. *Quantum Security in Homodyne Reception Using Weak Coherent States.* 22nd General Congress of the International Commission for Optics (ICO-22). Puebla 2011.

Edith García C., Francisco Javier Mendieta J., Josué A. López L. y Arturo Arvizu M. *Comunicaciones seguras con criptografia cuántica.* Segundo Congreso Internacional "La Investigación en el Posgrado". Aguascalientes 2011.

Josué A. López L., Arturo Arvizu M., **Edith García C**., Francisco Javier Mendieta J. *Comunicaciones Cuánticas Con Aplicaciones Satelitales.*Segundo Congreso Internacional "La Investigación en el Posgrado". Aguascalientes 2011.

J. A. López, **E. García**, F. J. Mendieta, A. Arvizu and Phillipe Gallion. *Simultaneous Quadrature Detection of Suppressed-Carrier Weak-Coherent-States using a Homodyne Optical Costas Loop Receiver.* Proc. SPIE 8163, Quantum Communications and Quantum Imaging IX, 81630E . San Diego, CA. 2011.

J.A. Lopez, **E. Garcia**, F. J. Mendieta, P. Gallion , A. Arvizu. *Quasiprobabilities in Simultaneous Quadrature Detection in Quantum Cryptography and Communications.*Workshop Theory and Realisation of Practical Quantum Key Distribution 2010. Waterloo, Canada. June 2010.

F. J. Mendieta, P. Gallion, P. Bellot, **E. Garcia**, J.A. López and A. Arvizu. A Holistic Approach to Security in Quantum Key Distribution Systems. Workshop Theory and Realisation of Practical Quantum Key Distribution 2010. Waterloo, Canada. June 2010.

Yudith González, Josué López, Arturo Arvizu, Francisco Mendieta, Joel Santos, **Edith García**, Roberto Conte. *Herramienta para Evaluación del Presupuesto de Potencia Óptica en enlaces de Comunicaciones Clásicas y Cuánticas en Espacio libre.* ROC&C Acapulco 2012.

B. Caracterización de las pérdidas del híbrido de 90^0

Un elemento característico requerido para la determinación de pérdidas y eficiencia en el sistema detector homodino, es el octapuerto. En el presente caso se midieron y analizaron las pérdidas generadas sobre la potencia transmitida en los puertos del híbrido de 90 (véase la Fig. B.1). Éste módulo consiste en un divisor de haz 50/50 y dos divisores de haz polarizados.

Cada trayectoria puede tiene diferente longitud y por lo tanto diferentes pérdidas, y en este caso se realizaron ajustes para que la potencia de los haces recibidos en ambos fotodetectores tuvieran el mismo nivel. En la figura Fig. B.1 se observan las trayectorias de la señal de datos (color verde) y la del oscilador local (color naranja) en donde la letra T indica la trayectoria de la señal transmitida y R la de la señal reflejada. Las cantidades representan la fracción de la señal que incide con respecto al total. El punto inicial es en donde la señal óptica proveniente del láser es dividida en dos trayectorias, un a de éstas sirve para obtener la señal de referencia y la otra para ser modulada por la señal de datos y atenuada hasta logar el estado coherente débil (primer separador de haz en el extremo izquierdo de la figura 2.5).

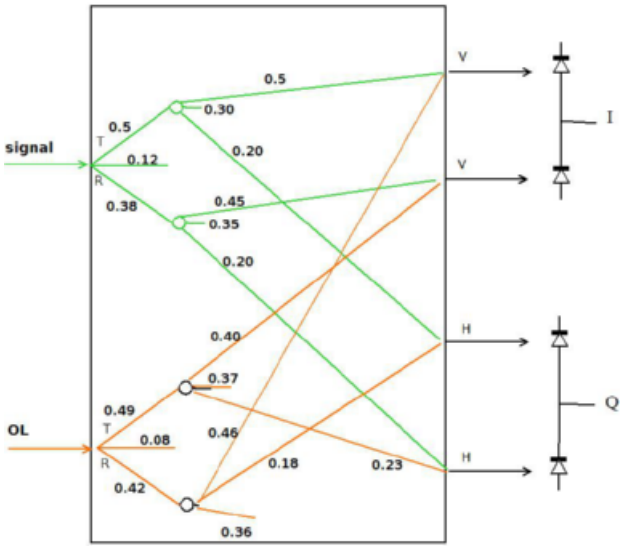


Figure B.1.: Medición inicial de los niveles de potencia en la trayectoria óptica del haz de oscilador local y señal de datos.

C. Parámetros de Stokes

Los parámetros de Stokes son una representación matemática en forma de vector, del estado de polarización de la luz. Si consideramos que las componentes del campo eléctrico de una onda electromagnética son $E_x(z,t) = E\ \cos(kz - \omega t)\ \hat{i}$ y $\qquad E_y(z,t) = E\ \cos(kz - \omega t + \varepsilon)\ \hat{j}$. En donde k es conocido como el número de propagación, z es la dirección en la que viaja la onda,ω es la frecuencia angular de la onda y ε es la diferencia de fase entre las componentes del campo eléctrico $E_x(z,t)$ el vector de Stokes es

$$S = \begin{bmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \end{bmatrix}$$

Los elementos del vector están definidos por

$S_0 = \langle E_{0x}^2 \rangle + \langle E_{0y}^2 \rangle$

$S_1 = \langle E_{0x}^2 \rangle - \langle E_{0y}^2 \rangle$

$S_2 = \langle 2\ E_{0x}\ E_{0y}\ \cos\varepsilon \rangle$

$S_3 = \langle 2\ E_{0x}\ E_{0y}\ \sin\varepsilon \rangle$

S_0es la irradiancia óptica del haz, mientras que los valores de $S_{1,}S_2$y S_3definen el estado de polarización de la luz, y $\varepsilon = \varepsilon_y - \varepsilon_x$ es la diferencia de fase entre las dos componentes del campo eléctrico. [59]

D. Tabla de cálculo de filtros optimizados para Lazo de Costas

Los resultados calculados del filtro optimizado para bajo número de fotones y frecuencias de tasa de transmisión, se incluyen a continuación como una referencia de valores esperados en función de las características del sistema. Éste resultado nos indica que si se requieren sistemas adaptables a distintas tasas de transmision, resultará más adecuado contar con un sistema empotrado, que ofrezca mayor flexibilidad que el sistema analógico.

Tabla D.1.: Tabla con las constantes de tiempo del lazo de retroalimentación, resistores y capacitores exigidos por el sistema, para su optimización en el caso de detección cuántica homodina. N es el número de fotones de la señal de datos.

Caso y Filtro	ω_{n-opt}	τ_1	τ_2	R_1	R_2	C
Caso 1 N=0.1						
Lazo PM	91.52 Krad/s	13.13 µseg	15.45 µseg	1.2 KΩ	1.5 KΩ	10 nF
Lazo PZT	2.89 Krad/s	13.81 µseg	0.488 mseg	1.2 KΩ	4.7 KΩ	10 nF
Caso 2 N=0.2						
Lazo PM	0.129 Mrad/s	9.32 µseg	0.345 mseg	1 KΩ	1 KΩ	10 nF
Lazo PZT	4.093 Mrad/s	9.324 µseg	0.3454 mseg	1 KΩ	33 KΩ	10 nF
Caso 3 N=1						
Lazo PM	289.44 Krad/s	4.155 µseg	4.88 µseg	3.9 KΩ	4.7 KΩ	1 nF
Lazo PZT	9.15 Krad/s	4.169 µseg	154.5 µseg	3.9 KΩ	150 KΩ	1 nF
Caso 4 N=10						
Lazo PM	2.894 Mrad/s	91.52 µseg	28.94 mseg	1.2 KΩ	1.5 MΩ	1 nF
Lazo PZT	91.59 Krad/s	1.318 µseg	48.86 µseg	1.5 KΩ	4.7 KΩ	1 nF

E. Postprocesamiento de datos y estadísticos

La captura de los valores de salida de corriente en los fotodetectores balanceados, nos permite realizar un análisis fuera de línea, que nos ofrecen información adicional al respecto del comportamiento de la señal. Particularmente a partir de los datos recibidos, es posible obtener variaciones estadísticas de los niveles de ruido cuántico.

A continuación se muestran los pasos efectuados para llevar a cabo el postprocesamiento de los observables (señales I y Q) que se realizaron con un programa en MATLAB.

1.-El primer paso es corregir el corrimiento en tiempo que hay entre la señal transmitida y la señal medida. En la Figura E.1 , lado izquierdo se observan las señales sin la corrección de corrimiento, las señales de la derecha ya tienen dicha corrección.

2.- Se aplicó un filtro a la señal de datos para tratar de reducir el ruido de la señal de datos para estar en condiciones de analizar la estadistica. En la Figura E.1, la señal en color azul es la señal sin filtrar y en colo rojo se muestra la señal filtrada.

3.- Con mediciones que se obtuvieron con ristras de datos en niveles de sólo "1" y sólo "0" lógicos se determinó el nivel de voltaje correspondiente los dos niveles, ésto sirvió para comparar ésos niveles pero ahora con una señal de "1" y "0" alternados, o con señales pseudoaleatorias.

4.- Con los niveles de "1" y "0" definidos, se calcula el valor promedio y la varianza de la señal. Con éste resultado se calcula la SNR.

5.- Con los resultados del paso 4, se analiza la ristra de datos completa para compararla con la señal transmitida, y de esta forma obtener el BER.

Se aplicó el proceso de filtrado a la señal transmitida solo para fines de comparación.

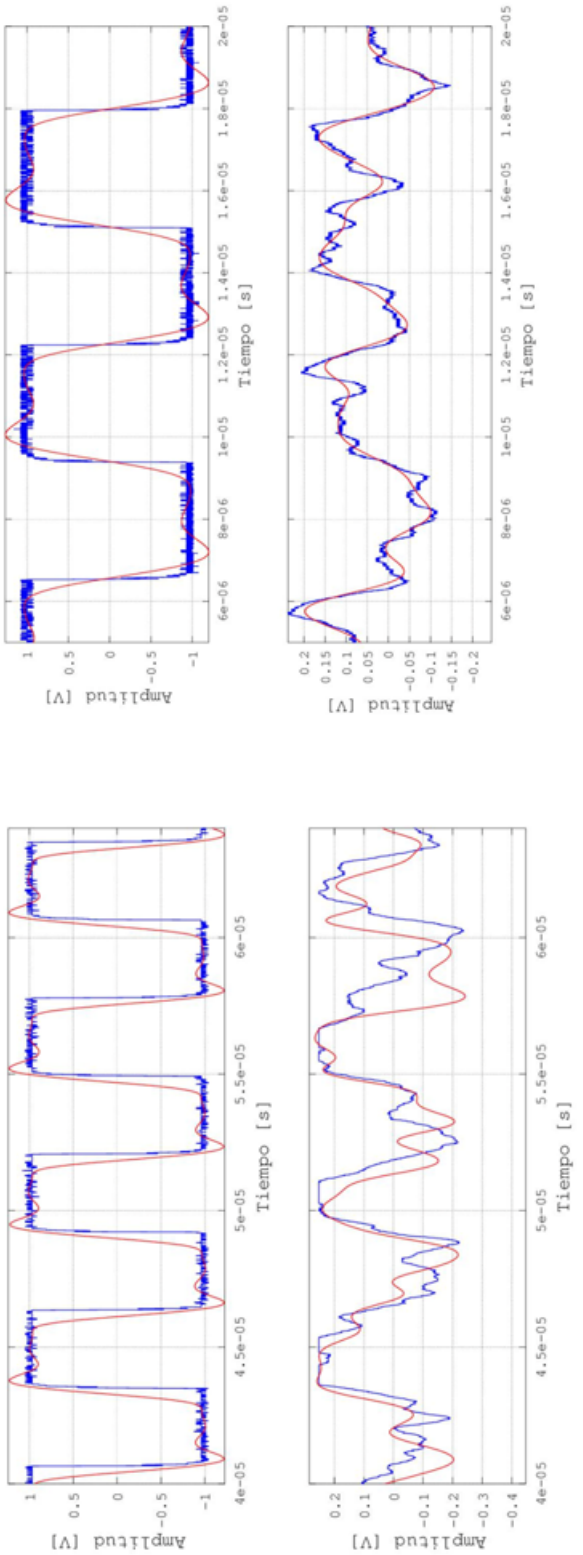


Figura E.1.: Post procesamiento de la señal medida para 4 fotones (caso de la izquierda) y 0.5 fotones por bit. Las señales de la parte superior corresponden a la señal transmitida, las de la parte inferior son las de la señal de datos (I)

Acrónimos

Acrónimos empleados en el presente documento:

ASK: amplitude shift keying / *modulación por corrimiento de amplitud*

APD: avalanche photodiode / *fotodiodo de avalancha*

BB84: Bennett-Brassard 1984

BER: bit error rate / *tasa de bits erróneos*

BHD: balanced homodyne detection / *detección homodina balanceada*

BPSK: binary phase shift keying / *modulación por corrimiento de fase binaria*

BS: beam splitter / *divisor de haz*

CW: continuous wave / *onda continua*

FC: fiber coupler / *acoplador de fibra*

FPGA: field-programmable gate arrays / *arreglo de compuertas lógicas programables*

FWHM: full width at half maximum /*anchura completa a media altura*

OL: local oscillator / *oscilador local*

p.i.n.: p-intrinsic-n photodiode / *fotodiodo p-intrínseco-n*

PLL: phase locked loop / *lazo de amarre o encadenamiento de fase*

PSK: phase shift keying / *modulación por corrimiento de fase*

QC: quantum cryptography / *criptografía cuántica*

QKD: quantum key distribution / *distribución cuántica de la llave*

QPSK: quaternary phase shift keying / *modulación por corrimiento de fase cuaternaria*

RSA: Rivest Shamir Adelman

SNR: signal to noise ratio / *relación señal a ruido*

SPD: single photon detector / *detector de un solo fotón*

SQL: Standard quantum limit / *límite cuántico estándar*

VCO: voltaje controlled oscillator / *oscilador controlado por voltaje*

WCS: weak coherent states / *estados coherentes débiles*

WDM: wavelength division multiplexing / *multicanalización por división de longitud de onda*

Bibliografía

[1] B. Sklar, *Digital Communications*. New Jersey: Prentice Hall, 1988.

[2] P. Stavroulakis and M. Stamp, *Handbook of Information and Communication Security*. Springer-Verlag, 2010.

[3] R. Michel, "Quantum crypt. enhancenment of agt communications security using quantum cryptography," *"ENST,/ EEC/QC.12.01.WP3.A."*, jan 2005.

[4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, pp. 145–195, Mar 2002. http://link.aps.org/doi/10.1103/RevModPhys.74.145.

[5] R. J. Hughes, D. M. Alde, P. Dyer, G. G. Luther, G. L. Morgan, and M. Schauer, "Quantum cryptography," *Contemporary Physics*, vol. 36, no. 3, pp. 149–163, 1995. http://www.tandfonline.com/doi/abs/10.1080/00107519508222149.

[6] M. Toyoshima, Y. Takayama, W. Klaus, H. Kunimori, M. Fujiwara, and M. Sasaki, "Free-space quantum cryptography with quantum and telecom communication channels," *Acta Astronautica*, vol. 63, no. 1-4, pp. 179 – 184, 2008. Touching Humanity - Space for Improving Quality of Life. Selected Proceedings of the 58th International Astronautical Federation Congress, Hyderabad, India, 24-28 September 2007.

[7] P. Villoresi, F. Tamburini, M. Aspelmeyer, T. Jennewein, R. Ursin, C. Pernechele, G. Bianco, A. Zeilinger, and C. Barbieri, "Space-to-ground quantum communication using an optical ground station: a feasibility study," pp. 113–120, 2004. + http://dx.doi.org/10.1117/12.564296.

[8] R. J. Runser, T. Chapuran, P. Toliver, N. A. Peters, M. S. Goodman, J. T. Kosloski, N. Nweke, S. R. McNown, R. J. Hughes, D. Rosenberg, C. G. Peterson, K. P. McCabe, J. E. Nordholt, K. Tyagi, P. A. Hiskett, and N. Dallmann, "Progress toward quantum communications networks: opportunities and challenges," pp. 64760I–64760I–15, 2007. + http://dx.doi.org/10.1117/12.708669.

[9] K. Inoue, "Quantum key distribution technologies," *Selected Topics in Quantum Electronics, IEEE Journal of*, vol. 12, no. 4, pp. 888–896, 2006.

[10] G. M. Floyd, *Phaselock Techniques*. Wiley and Sons Ltd, 2005.

[11] C. Georghiades and D. L. Snyder, "A proposed receiver structure for optical communication systems that employ heterodyne detection and a semiconductor laser as a local oscillator," *Communications, IEEE Transactions on*, vol. 33, no. 4, pp. 382–384, 1985.

[12] I. Djordjevic, M. Stefanovic, S. Ilic, and G. Djorjevic, "An example of a hybrid system: Coherent optical system with costas loop in receiver-system for transmission in base band," *Journal of Lightwave Technology*, vol. 16, pp. 177–183, Feb. 1998.

[13] K. Leonid, S. Benedetto, and A. Willner, *Optical Fiber Communications Systems*. Artech House, 1996.

[14] B. Chris and C. Hunt, *Mastering Netwok Security*. Network Press, Sybex, 2nd ed., 2003.

[15] I. T. Force, "Request for comments: 4949." http://tools.ietf.org/html/rfc4949.

[16] NIST, *Telcommunications Security Guidelines for Telecommunications Management Network*. Series 800-13. NIST Special Publication Computer Security. US Department of Commerce, 2011.

[17] Q. Xu, *Optical Homodyne Detection and Applications in Quantum cryptography*. PhD thesis, ENST - Telecom ParisTech., 2009.

[18] G. SEKAR, *Cryptanalysis and Design of Symmetric Cryptographic Algorithms*. PhD thesis, Katholieke Universiteit Leuven. Belgium, 2011.

[19] J. de J Angel and G. Morales-Luna, "Algunos sistemas criptográficos durante la presidencia de porfirio díaz," *Departamento de Computación*, 2007.

[20] S. J. Lomonaco, *Coding Theory and Cryptography*, ch. A Talk on Quantum Cryptography or How Alice Outwits Eve. Springer, 2000.

[21] C. Shannon, *The Matematical Theory of Communication*. University of Illinois Press, 1975.

[22] D. G. Luenberger, *Information Science*. Princeton University Press, 2006.

[23] A. Shamir and E. Tromer, "On the cost of factoring rsa-1024," *RSA CryptoBytes*, vol. 6, pp. 10–19, 2003.

[24] Digicert, "Digicert home page.," June 2009. http://www.digicert.com.

[25] W.K.Wooters and W. Zurek, "A single quantum can not be cloned," *Nature*, pp. 802–803, October 1982.

[26] P. Bellot and D. Minh-Dung, "BB84 implementation and computer reality," in *International Conference on Computing and Communication Technologies, 2009. RIVF '09.*, 2009.

[27] G. V. Assche, *Quantum Cryptography and Secret-Key Distillation*. Cambridge University Press, 2006.

[28] P. Jouguet and et al, "Field test of classical symmetric encryption with continuous variables quantum key distribution," *Optics Express*, vol. 20, June 2012.

[29] M. Peev and et al, "The SECOQC quantum key distribution network in vienna," *Journal of Optical Communications and Networking*, vol. 11.

[30] J. Bienfang, A. Gross, A. Mink, B. Hershman, A. Nakassis, X. Tang, R. Lu, D. H. Su, C. W. Clark, and C. J. Williams, "Quantum key distribution with 1.25 gbps clock synchronization," *Optics Express*, vol. 12.

[31] M. Lamonica, ""a hybrid system could secure transmissions over hundreds of kilometers"," july 2013. http://spectrum.ieee.org/computing/networks/longdistance-quantum-cryptography.

[32] M. Sasaki and et al., "Field test of quantum key distribution in the tokyo qkd network," *Opt. Express*, vol. 19, pp. 100387–10409, 2011.

[33] L. Salvail, M. Peev, E. Diamanti, R. Alleaume, and T. L. Norbert Lütkenhaus, "Security of trusted repeater quantum key distribution networks," *Journal of Optical Communications and Networking*, vol. 5.

[34] M. Ardehali, H. F. Chau, and H.-K. Lo, "Efficient quantum key distribution," *Phys. Rev A*, vol. 68, pp. 133–165, 2003.

[35] F. G. Deng, G. L. Long, and X.-S. Liu, "A two-step quantum direct communication protocol using einstein-podolsky-rosen pair block," *Journal of Cryptology*, vol. 18, 2005.

[36] P. Grangier, "Experiments with single photons," *Séminaire Poincaré*, vol. 2, july 2005.

[37] S. Cova, M. Ghioni, A. Lacaita, C. Samori, , and F. Zappa, "Absolute efficiency and time-response measurement of single-photon detectors," *Applied optics*, vol. 35, no. 12, 1996.

[38] A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, "No-switching quantum key distribution using broadband modulated coherent light," *Phys. Rev. Lett.*, vol. 95, p. 180503, Oct 2005. http://link.aps.org/doi/10.1103/PhysRevLett.95.180503.

[39] M. Legre, H. Zbinden, and N. Gisin, "Implementation of continuous variable quantum cryptography in optical fibres using a go-return configuration," *Quantum Info. Comput.*, vol. 6, pp. 326–335, July 2006. http://dl.acm.org/citation.cfm?id=2012086.2012088.

[40] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.*, vol. 88, p. 057902, Jan 2002. http://link.aps.org/doi/10.1103/PhysRevLett.88.057902.

[41] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, pp. 1301–1350, Sep 2009. http://link.aps.org/doi/10.1103/RevModPhys.81.1301.

[42] F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. Cerf, and P. Grangier, "Quantum key distribution using gaussian-modulated coherent states," *Nature*, vol. 421, pp. "238–241", jan 2003.

[43] P. Chan, I. Lucio, X. Mo, and W. Tittel, "Quantum key distribution," *Femtosecond-Scale Optics*, 2011.

[44] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," *Phys. Rev. Lett.*, vol. 92, p. 057901, Feb 2004. http://link.aps.org/doi/10.1103/PhysRevLett.92.057901.

[45] C. Marcos, "Sistemas cuanticos de distribucion de clave basadas en pulsos de luz coherente atenuados," *Optica Pura y Aplicada*, vol. 43, no. 1, pp. 17–22, 2010.

[46] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Phys. Rev. Lett.*, vol. 91, p. 057901, Aug 2003. http://link.aps.org/doi/10.1103/PhysRevLett.91.057901.

[47] G. Jaeger, *Quantum Information*. Springer, 2004.

[48] C. Shannon, "Communication theory of secrecy systems," 1949. http://netlab.cs.ucla.edu/wiki/files/shannon1949.pdf.

[49] M. Ueli and S. Wolf, "The intrinsic conditional mutual information and perfect secrecy," 1997.

[50] Y. Chi, B. Qi, W. Zhu, L. Qian, H.-K. Lo, S.-H. Youn, A. I. Lvovsky, and L. Tian, "A balanced homodyne detector for high-rate gaussian-modulated coherent-state quantum key distribution.," *New Journal of Physics*, vol. 13, 2011.

[51] B. Schumacher, "Quantum mechanics: The physics of the microscope world. parts i and ii," 2009. Published by The Teaching Company, 2009. USA.

[52] R. Feynman, *Lectures on Physics. Vol.III Quantum Mechanics.* Pearson/Addison-Wesley,, 2006.

[53] P. Gallion, F. J. Mendieta, and S. Jiang, *Noise in optical communications and cryptography*, vol. 52. E. Wolf (Editor), Elsevier, Hungary, 2009.

[54] L. Ulf, *Measuring the quantum state of light.* Cambridge University Press, 1997.

[55] M. A. Parker, *Physics of Optoelectronics.* CRC Press, 2005.

[56] J. C. Petrucelli, *Generalized Wigner Functions.* PhD thesis, A disertation submitted to the University of Rochester., 2010.

[57] D. Petz, *A Brief Introduction to the Wigner Distribution.* www.scarpaz.com, 2003.

[58] R. Saunders, "When does coherent vs direct detection make sense for 40g/100g network deployments?," *Lightwave Magazine*, 9 2010. http://www.lightwaveonline.com/blogs/lightwave-guest-blog/2010/09/when-does-coherent-vs-direct-detection-make-sense-for-40g100g-network-deployments.html.

[59] E. Hecht, *Optics.* Addison Wesley, Pearson Education Inc., 2002.

[60] E. Collet, *Polarized light:fundamentals and applications.* Michigan, USA: Marcel Dekker, 1993.

[61] E. Desurvire, "Three-dimensional quantum vacuum-noise signal beamsplitter model for nonideal linear optical amplifiers," *Optical Fiber Technology*, vol. 5.

[62] E. García, F. Mendieta, J. López, E. Alvarez, A. Arvizu, and P. Gallion, "Phase-locked homodyne measurement of quasiprobability q function and detection of information-carrying weak-coherent states," *Microwave and Optical technology Letters*, vol. 55, no. 10.

[63] J. Lopez, A. Arvizu, E. García, F. Mendieta, and P. Gallion, "Detection of phase diffused weak coherent-states using an optical costas loop," *Opt Eng*, vol. 51, 2012.

[64] I. Djordjevic, "Optical homodyne psk receivers with a costas loop for high-speed long-haul communications," *Journal of Optical Communications*, vol. 23, no. 4, p. 154.

[65] L. Kazovsky, "Balanced phase-locked loops for optical homodyne receivers," *IEEE Journal of Lightwave Technology*, vol. LT-4, no. 2, pp. 185–195, 1986.

[66] G. Kalivas, *Digital Radio Systems Design.* Wiley and Sons Ltd, 2009.

[67] R. E. Best, *Phase-Locked Loops. Design, Simulation and Applications.* Mc. Graw Hill, 4th ed., 1999.

[68] Q. Xu, A. Mondragon, P. Gallion, and F. Mendieta, "Homodyne in-phase and quadrature detection of weak coherent states with carrier phase tracking," *Selected Topics in Quantum Electronics, IEEE Journal of*, vol. 15, no. 6, pp. 1581–1590, 2009.

[69] Y. Chi, *High Speed Homodyne Detector for Gaussian-Modulated Coherent-State Quantum Key Distribution*. PhD thesis, University of Toronto, 2009.

[70] R. Brown, R. Jones, J. Rarity, and K. Ridley, "Characterization of silicon avalanche photodiodes for photon correlation measurements," *Applied Optics*, vol. 26, june 1987.

[71] M. Simon and W. Lindsey, "Optimum performance of suppressed carrier receivers with costas loop tracking," *IEEE Trans. on Comm*, vol. COM-25, pp. 215–227, 1977.

[72] A. Liao, W.-T. Ni, and J.-T. Shy, "Pico-watt and femtto-watt weak-light phase-locking," *International Journal of Modern Physics*, vol. 7.

[73] S. Olivares, S. Cialdi, F. Castelli, and M. Paris, "Homodyne detection as a near-optimum receiver for phase-shift-keyed binary communication in the presence of phase diffusion," *Physical Review A*, vol. 87, 2013.

[74] E. Alvarez, E. Garcia, J. Gonzalez, J. D. Rio, J. L. Leyva, F. Mendieta, J. Loya, and A. Arvizu, "Quantum key distribution detection system using fpgas: Preliminary results," in *Mexican Optics and Photonics Meeting 2013. Ensenada, Mexico*, 2013.

Glosario

ANCHO DE BANDA Rango de frecuencias en las que se concentra la mayor parte de la potencia de una señal

BPSK Modulación por corrimiento de fase binario. Técnica en la que la información a transmitir modula la fase de una señal senoidal. En este caso se tienen dos estados posibles que permiten transmitir un sólo bit en cada uno de ellos.

BRA-KETS Notación estándar para representar estados cuánticos. En la expresión $\langle\varphi \mid \psi\rangle$, $\langle\varphi$
es el bra y $\psi\rangle$ es el ket y puede interpretarse como la amplitud de probabilidad de que un estado ψ colapse al estado φ.

CRACKER Individuo con conocimientos técnicos avanzads y con propósitos maliciosos y criminales.

DETECCIÓN COHERENTE Es una técnica de detección que se basa en la mezcla de no lineal de la señal a detectar (la que contiene información) con una señal generada por un oscilador local en el receptor.

FUNCION DE DISTRIBUCIÓN DE WIGNER Es una representación de la distribución de cuasiprobabilidad marginal de las dos cuadraturas de un estado cuántico en particular, en un espacio fasorial. Para ello, se obtiene una serie de mediciones de una de las cuadraturas (observables) para obtener lo distribución marginal, la cual se representa en un plano de un sistema de coordenadas x-y.

FUNCION DE ERROR (*erf*) Es una función matemática que muestra la probabilidad de que el error de una medición de valor X, se encuentre comprendido en el intervalo $-X$ y $+X$.

FUNCION DE HUSIMI Es una distribución de cuasiprobabilidad utilizada en mecánica cuántica para representar la distribución en el espacio de fase de un estado cuántico, en

escencia es equivalente a la Función de distribución de Wigner pero convolucionada con una función gaussiana que representa al ruido de vacío.

FUNCIÓN DE DIDTRIBUCIÓN DE WIGNER Es una representación de la distribución de cuasiprobabilidad marginal de las dos cuadraturas de un estado cuántico, en particular en un espacio fasorial. Para ello, se obtiene una serie de mediciones de una de las cuadraturas (observables) para obtener lo distribución marginal, la cual se representa en un plano de un sistema de coordenadas x-y.

HACKER Se refiere a una persona que gusta de entender, modificar y explirar sistemas de programación, particularmente sistemas de cómputo y redes.

LIMITE CUÁNTICO ESTÁNDAR (SQL, *Standard Quantum Limit*) Nivel de ruido cuántico mínimo que se puede obtener sin utilizar estados comprimidos de la luz. El ruido cuántico es una restricción en las mediciones a muy bajo número de fotones.

MODELO OSI. (OSI, *Open System Interconnection*) El modelo de interconexión de sistemas abiertos fue creado por la Organización Internacional para la Estandarización (ISO) en 1980. Es un marco de referencia para la definición de arquitecturas en la interconexión de los sistemas de comunicaciones. El modelo consta de 7 niveles o capas: Física, Enlace de datos, Red, Transporte, Sesión, Presentación y Aplicación. En este trabajo de tesis se está trabajando únicamente en la primera capa, la física.

MULTICANALIZACIÓN POR DIVISIÓN DE LONGITUD DE ONDA. (WDM, Wavelength Division Multiplexing). Es la tecnología que consiste en multicanalizar varios canales ópticos cada uno con una diferente longitud de onda en una misma fibra óptica.

QBITS Un bit es la unidad de información en los sistemas de información el cual tiene valores únicos y definidos de 1 y 0. Un Qbit es un 1 y un 0 al mismo tiempo, es decir es una superposición de estados, que al momento de medirlo colapsarán a un 1 ó 0.

QPSK Modulación por corrimiento de fase cuaternario. Técnica en la que la información a transmitir modula la fase de una señal senoidal. En este caso se tienen cuatro estados posibles que permiten transmitir dos bits en cada uno de ellos.

RECONCILIACIÓN DE LA LLAVE CRIPTOGRÁFICA Proceso en el cual Alice y Bob comparten por medio de un canal público la informació9n de las bases utilizadas en la secuencia de bits de la llave enviados. Los bits correspondientes en las anticoincidencias serán desechados.

RELACIÓN SEÑAL A RUIDO (SNR, *Signal to Noise Ratio*) Es una medida de comparación entre los niveles de potencia de la señal de información y la del ruido, comúnmente expresada en decibeles.

RELACIÓN SEÑAL A RUIDO (SNR,*Signal To Noise Ratio*) Es una medida de comparación entre los niveles de potencia de la señal de información y la del ruido, comúnmente expresada en decibeles.

RUIDO DE DISPARO (Ruido *Shot*) es el ruido que tiene su origen en la naturaleza corpuscular de la luz. Si el número de fotones que inciden en el receptor es reducido se pueden observar fluctuaciones importantes en la estadistica de arribo, la distribución que presentan es de tipo Poissoniana.

RUIDO DE VACÍO este ruido está relacionado con con las fluctuaciones en el punto cero del campo eléctrico de un estado de vacío. Este ruido es considerado para no violar la relación de incertudumbre de Heisenmberg.

TASA DE BITS ERRONEOS (BER, *Bit Error Rate*) Es el número de bits que se reciben en forma errónea, con respecto al total de bits que se enviaron durante un periodo de tiempo definido.