"CONGRESO INTERNACIONAL DE INVESTIGACIÓN E INNOVACIÓN 2014"
Multidisciplinario
10 y 11 de abril de 2014, Cortazar, Guanajuato, México
ISBN: 978-607-95635

Sistema de criptografía cuántica de segunda generación (CV-QKD): Resultados preliminares de la implementación del algoritmo de un subsistema clásico para QKD via Internet.

Dr. Josue Aarón Lopez Leyva[1, 2*], Dr. Arturo Arvizu Mondragón [2], Dr. Francisco Javier Mendieta Jiménez [3].

[1]CETYS Universidad, Ensenada, B.C
[2] Division de Física Aplicada, CICESE, Ensenada, B.C.
[3] Agencia Espacial Mexicana (AEM), Distrito Federal
[*]*josue.lopez@cetys.mx*

Resumen

En el presente trabajo mostramos la implementación de un subsistema clásico, como parte de un sistema de criptografia cuántica de segunda generación (CV-QKD). Tal subsistema clásico consta del algortimo necesario para la encriptación de la información transmitída vía internet desde dos sitios remotos. Se obtuvieron algunos parámetros de desempeño del subsistema tales como: la longitud de la llave filtrada (*sifted key*), llave final, tiempo de ejecución del algoritmo de corección de errores y del compléto. Finalmente, se transmitió información segura (una imagen) utilizando tal algoritmo.

Abstract

ISBN: 978-607-95635

We present the implementation of a classical subsystem as part of a complete quantum cryptography system of second-generation (CV-QKD). Such classical subsystem consists of the necessary algorithm to encrypt the information transmitted via Internet using two remote sites. We obtained the performance of some parameters of the subsystem such as the length of the key filtered (sifted key), final key and duration of the execution of algorithm of error correction and overall QKD algorithm.

Palabras Clave: criptografía cuántica, algoritmo de corrección de errores, comunicación por sockets, codificación de fase.

ISBN: 978-607-95635

I. Introducción

En la actualidad existen diversos esquemas de seguridad (encriptación de información) que brindan una secrecía condicionada al poder de cómputo de las partes involucradas. De hecho, en los últimos años, se han presentado algunos casos de robo de información de manera cibernética; esto debido a que la criptográfia tradicional basa el nivel de seguridad en complejos algoritmos matemáticos, los cuales pueden ser relativamente fáciles de descifrar ya sea por equipos y sistemas comercializables o diseñados para tales propósitos. Sin embargo, en los últimos años se ha "manejado" otra manera de proveer ese requerimiento de seguridad, no basada en complejos algoritmos matemáticos, ni condicionado al poder de cómputo, sino más bien, basado en los principios y reglas de la naturaleza, es decir, de la mecánica cuántica. Estos sistemas proveen una alto nivel de seguridad incondicional a la información, además de tener la facilidad de poder detectar la presencia de un espía en el canal de comunicación usado (internet, fibra óptica, radio frecuencia, etc); a este tipo de sistema se denomina sistemas de Distribición de llave Cuántica (QKD, por sus siglas en inglés *Quantum Key Distribution*) (Elkouss, D., *et al*, 2013).

El objetivo de los sistemas QKD se puede entender bajo el escenario mostrado en la figura 1, donde un sistema A (Alice / servidor) desea enviar información segura por medio del Internet a un sistema B (Bob / cliente), no deseando que un sistema espía (Eva) adquiera la información que Alice envía a Bob.

ISBN: 978-607-95635

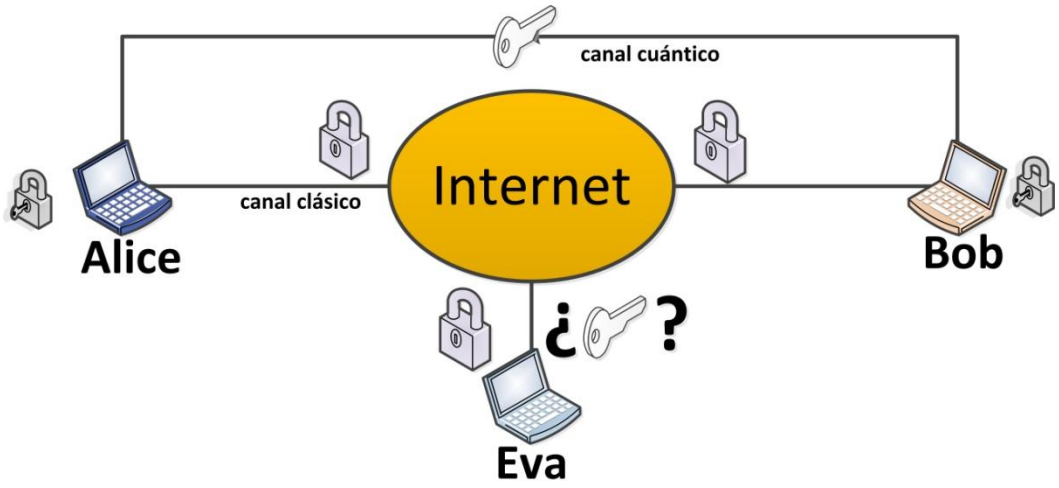


Figura 1. Esquema general de seguridad cuántica usando Internet.

Para tal propósito, Alice y Bob están formados por un subsistema clásico y otro cuántico, así como dos canales de comunicación de la misma naturaleza; un canal público (clásico) y otro privado (cuántico). En la actualidad, algunas compañías a nivel mundial comercializan sistemas QKD, entre las que se encuentran: IdQuantique (Suiza), Toshiba (Japón), SequereNet (Francia), MagiQ (E.U.A), Queensland Lab (Australia), entre otras. Cada una de ellas comercializando sistemas QKD de primera y/o segunda generación, DV-QKD (*Discrete Variable-Quantum Key Distribution*) y CV-QKD (*Continuous Variable-Quantum Key Distribution*), respectivamente. Sin embargo, estos equipos aun son de un elevado costo debido al estado del arte de la tecnología usada, lo cual hace restrictiva a la investigacion e innovación fuera de este círculo (Oesterling, *et al*, 2012). El presente artículo muestra el subsistema clásico de un sistema CV-QKD completo como parte del trabajo en equipo de CETYS Universidad y el Grupo de Comunicaciones Ópticas de CICESE. El subsistema clásico es el encargado del

ISBN: 978-607-95635

algoritmo de encriptamiento por medio del canal clásico, que en nuestro caso es Internet. Con respecto al subsistema cuántico, ya ha sido reportado por el mismo equipo de trabajo.

II. **Métodologia**

Básicamente se implementó el sistema CV-QKD completo mostrado en la figura 2, donde se desarrollaron los subsistemas clásico y cuántico de manera separada. Los detalles del subsistema cuántico ya han sido reportados (López, *et al* 2013). Así, el subsistema clásico consta de dos equipos de cómputo conectados a una red de comunicación (puede ser una Red de Área Local, Metropolitana y/o Mundial) como lo muestra la figura 3.

ISBN: 978-607-95635

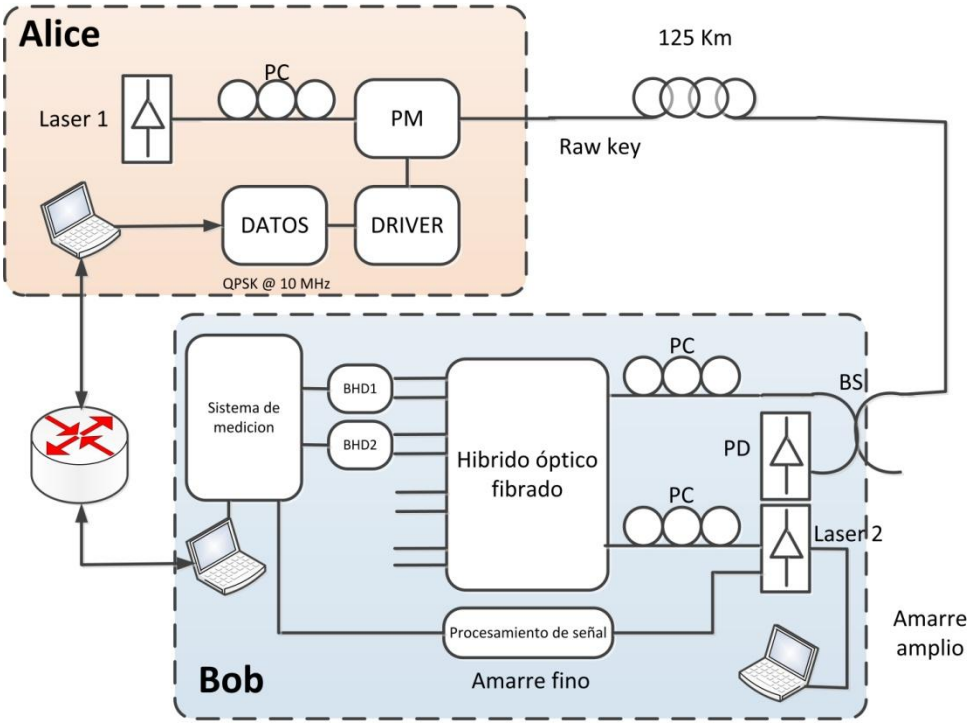
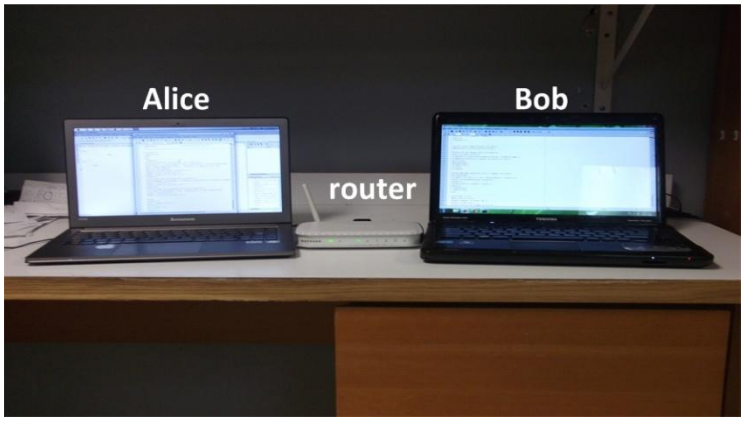


Figura 2. Sistema QKD completo. PM: modulador de fase, BS: separador de haz, PD: fotodetector, PC: controlador de polarización, BHD: detector homodino balanceado.



ISBN: 978-607-95635

Figura3. Subsistema clásico. Alice: sistema transmisor, Bob: sistema receptor, y el router inalámbrico que provee la red de comunicación.

Básicamente, se implementó el algoritmo QKD en los sistemas computacionales correspondientes a Alice y Bob. En este caso, se eligió el algoritmo para sistemas QKD con variables continuas, denominado CV-QKD (Oesterling, *et al*, 2012). El algoritmo consta de cuatro etapas. **La primera etapa** es la transmisión de la cadena de fotones con formato de modulación QPSK (QPSK, *Quadrature Phase Shift Keying*) sobre el canal cuántico de Alice hacia Bob para obtener la *llave cruda* o "*raw key*", además, Alice mantiene una base de datos de la codificación usada para futuras operaciones; esta acción la lleva a cabo el sub-sistema cuántico y no se detalla en este trabajo. **En la segunda etapa**, Bob envía a Alice por medio del canal clásico (Internet) la base que eligió para la medición; en nuestro caso las bases se refieren al componénte en fase y cuadratura usádo en la modulación. El esquema de modulación QPSK consta de cuadro símbolos, los cuales son representados de manera binaria como 00, 01, 11, 10, donde el primer bit denota la base usada ("0" y "1" lógicos usan la base en fase y cuadratura, respectivamente) y el segundo bit el desfase ("0" y "1" lógicos un desfase de cero y noventa grados con referencia a la base, respectivamente). Alice recibe esa información y determina cuales fueron las coincidencias de bases entre ambos sistemas, y comunica a Bob las incorrectas, de manera que ambas partes eliminan las no-coincidencias, obteniendo así la llave filtrada, "*sifted key*". En este punto, la longitud de la *sifted key* debe de ser aproximadamente la mitad que la *raw key,* sino es así, la comunicación se cancela y se genera una nueva *raw key* debido a la posibilidad de un espía. Es posible que existan errores en los datos de la *sifted key* medidos por Bob, lo cuales pudieron ser ocasionados por el desempeño normal del sistema de transmisión, o bien, por un sistema ***espía.*** Por lo que Bob debe determinar los errores en los datos medidos denominado QBER (*Quantum Bit Error Rate*) y compararlos con el QBER teórico y/o el usado para la

ISBN: 978-607-95635

calibración del enlace de comunicación; si el QBER de los datos medidos fue mayor que el QBER teórico (considerando un margen de error), se considera que existe un espía en el canal y se aborta la transmisión, generando una nueva *raw key.* **La tercera etapa** consiste en corregir los errores presentes en la *sifted key* por medio de un algoritmo de corrección de errores, tal etapa se denomina "***reconciliación"***. En este caso, se decidió analizar la paridad de bloques de distintas longitudes hasta determinar la posición de los bits erróneos y proceder a su corrección. Hasta este momento, se puede considerar que la llave obtenida después de la reconciliación es segura, sin embargo, aun existe un método para mejorar la seguridad, denominado "***amplificación de seguridad"***, siendo esta **la cuarta etapa**. Aquí, se elige una función particular de la amplia familia de funciones de Hash usadas en la criptografía convencional o clásica; con anterioridad Alice y Bob deben de poseer en su base de datos aquellas funciones de Hash que podrían ser usadas (usualmente funciones de compresión), de manera que, al comunicarse por el canal clásico, determinen cual usarán para obtener ***la llave final***. (Trappe, et al, 2002). En nuestro caso se programó la función mostrada en las ecuaciones (1 y 2), donde los datos obtenidos después de la reconciliación con una longitud L son divididos en dos bloques m_1 y m_2, para ser operados por medio de una lógica XOR, obteniendo así la llave final k, con la cual será encriptada la información.

$$m_1 = [m_{11}, m_{12}, m_{13}, \ldots, m_{1(L/2-1)}]$$
$$m_2 = [m_{21}, m_{22}, m_{23}, \ldots, m_{2L}] \quad (1)$$

$$k = [(m_{11} \oplus m_{21}), (m_{12} \oplus m_{22}), (m_{13} \oplus m_{23}), \ldots, (m_{1(L/2-1)} \oplus m_{2L})] \quad (2)$$

ISBN: 978-607-95635

Si bien la llave final es altamente segura, también la longitud de ella es mucho menor a la "*raw key*" debido a los procesos ya mencionados (Mink, et al, 2009). La figura 3 muestra el algoritmo implementado en Matlab 2011a usando la comunicación por internet vía ***sockets***.

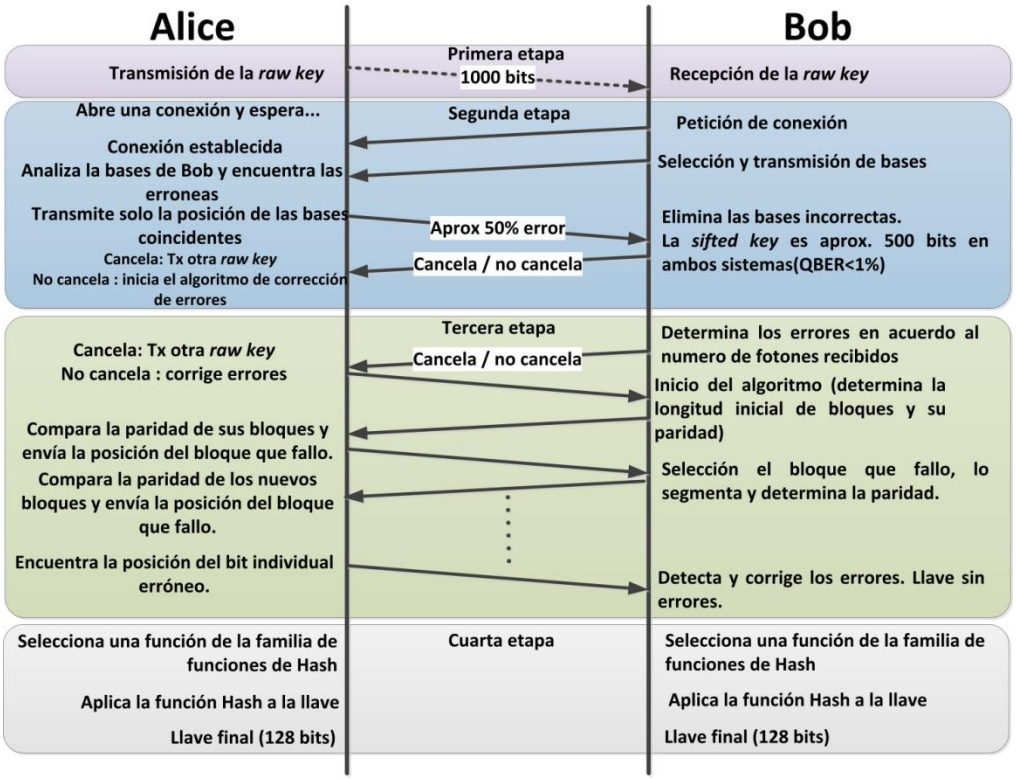
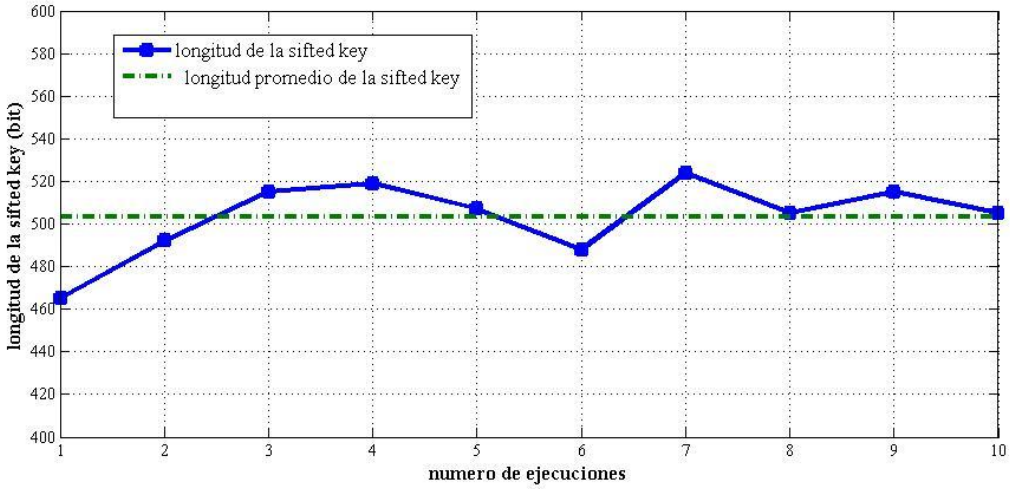


Figura 4. Algoritmo CV-QKD implementado usando *sockets* en Matlab.

ISBN: 978-607-95635

III. Resultados

Entre las mediciones que se realizaron con el algoritmo mencionado fue, la determinacion de la longitud de la *raw key.* El software se programó para se enviaran 1000 bit (o fotones en el canal cuántico), así que, la *sifted key* debería de ser aproximadamente la mitad de la longitud de la *raw key* en condiciones ideales; de esta manera se obtuvo la figura 5, con una longitud promedio de 505 bits, cumpliendo la condición para continuar con el algotirmo CV-QKD. La velocidad de transmisión de la *raw key* está limitada básicamente por el sub-sistema cuántico, donde el limitante lo estipula el manejador (driver) del modulador de fase, el modulador de fase y el sistema generador de datos binario. Mientras más longitud tenga la *raw key,* será posible obtener una llave final de mayor longitud. Usualmente los sistemas comerciales trabajan con una llave final de 128 bits, aunque recientemente se ha reportado un sistema CV-QKD que produce una *raw key* de 1 Mbps (Dixon, *et al*, 2010).



ISBN: 978-607-95635

Figura 5. Medición de la longitud de la *sifted key.*

Ademas, se determinó tiempos de ejecución de los algoritmos de corrección de errores y completo, debido a que, es importante conocer estos tiempos para modificar el *hardware* y *software* con el fin de incrementar la tasa de transmición de la llave final.. La figura 6 muestra el tiempo de ejecución de tales algoritmos.

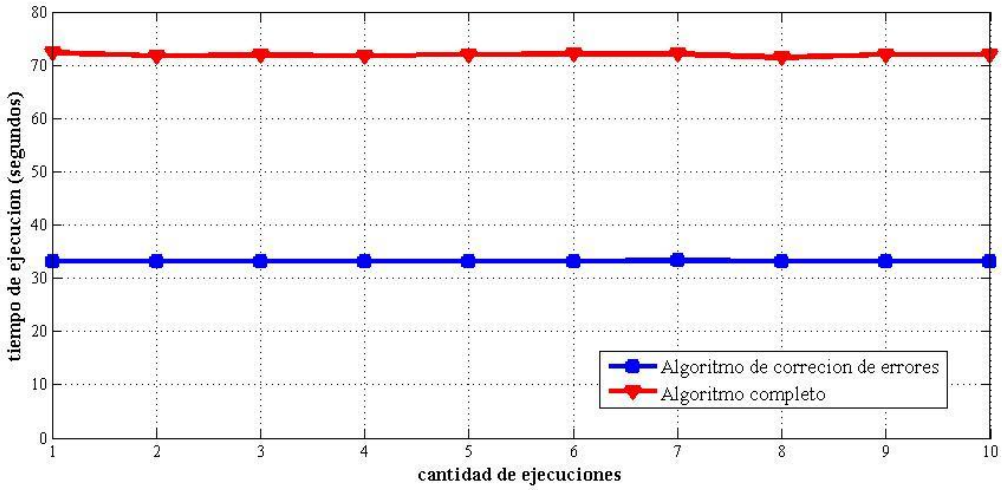


Figura 6. Tiempos de ejecución del algoritmo de corrección de errores y completo.

Por medio de programación, se añadieron los errores obtenidos prácticamente del subsistema cuántico (1.5 errores promedio de cada 10 bits utilizando un fotón por pulso) (Lopez, J.A., *et al*, 2012), debido a que, por el momento, el subsistema clásico y cuántico no están interconectados.

ISBN: 978-607-95635

Finalmente, se obtuvo una llave final de 128 bits, de manera que se encriptó una imagen de 128 pixeles solo para comprobar el algortimo completo en un ambiente real. La figura 7 muestra el diagrama de transmisión de encriptación y desencriptacion de la imagen elegida (la leta Q).

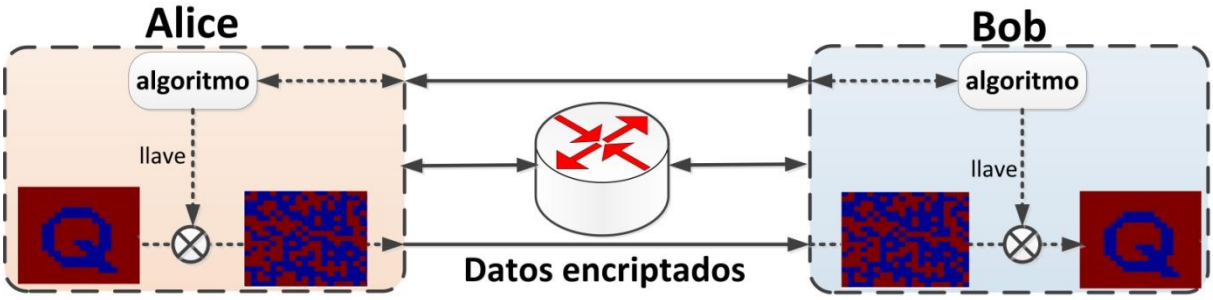


Figura 7. Esquema general de encriptación con la imagen seleccionada.

IV. **Conclusiones**

En el presente trabajo se han mostrado los resultados preliminares de un subsistema clásico de un sistema completo CV-QKD o de segunda generación implementado con comunicación via *sockets* en la plataforma de Matlab, donde finalmente se transfirió información (una imagen) por medio del protocolo TCP/IP Aunque el presente sistema fue funcional, es importante analizar los resultados de los tiempos de ejecucion de los algoritmos, especialmente el del algoritmo de corrección de errores, ya que éste consume casi el 50% del tiempo del algoritmo completo, esto debido a la gran cantidad de intercambio de información (longitud del bloque para determinar la paridad, la paridad de cada bloque, bloque incorrecto) entre Alice y Bob. Tal hecho ocasiona que el sistema sea lento, por lo que se propone la implementación del algoritmo usando arreglos de

ISBN: 978-607-95635

compuertas programables (FPGA) para mayor velocidad. Además, es importante mencionar que las funciones típicas de Hash usadas en dispositivos comerciales, hacen uso de operaciones binarias de alto nivel con el propósito de añadir dificultad de encontrar funciones que colisiones a los mismos valores. Actualmente existen algoritmos de corrección de errores mas sofisticados usados en sistemas QKD, tal como el CASCADE, asi como técnicas para aumentar la privacidad basada en las matrices de Toeplitz, además de funciones de Hash mas complejas (SHA-512 o 256) (Jouguet, P., *et. al,* 2013). Sin embargo, el propósito de este trabajo era clarificar los aspectos generales, y proceder a las mejoras pertinentes del estado del arte actual.

Agradecimientos

Deseamos extender nuestro agradecimiento a CONACYT por apoyar el proyecto de investigación actual del Grupo de Comunicaciones Ópticas en CICESE y a todo el apoyo de personal administrativo de CETYS Universidad, así como a los estudiantes de licenciatura Elías Bautista Martínez y Johana Paulina Ibarra García por su apoyo.

V. **Bibliografia**

Dixon, A. R., Yuan, Z. L., Dynes, J. F., Sharpe, A. W., y A. J. Shields. (2010). Continuous operation of high bit rate quantum key distribution. Appl. Phys. Lett. 96, 161102 (2010); http://dx.doi.org/10.1063/1.3385293

ISBN: 978-607-95635

Elkouss, D., Martinez-Mateo, J., Ciurana, A., Martin, V.(abril, 2013). Secure optical networks based on quantum key distribution and weakly trusted repeaters. IEEE/OSA Journal of Optical Communications and Networking. 5(4). 316-328.

López, J.A., Arvizu, A., García, E., Mendieta, F.J., Álvarez, E., Gallion, P. (octubre, 2012). Detection of phase-diffused weak-coherent-states using an optical Costas loop. Optical Engineering. 51(10). 1-8

López, Josue A., Arvizu Arturo, Jose Roberto. J. Roberto, Miguel V., Antonio F. S. ,J. Santos, F.J. Mendieta, R. Muraoka , E. García. (2013.) 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. IEEE Summer Topicals. Waikoloa Hawaii, USA (Conferencia)

Mink, Alan., Frankel, Sheila., Periner, Ray. (2009). Quantum Key Distribution (QKD) and Commodity Security Protocols: Introduction and Integration. Internacional Journal of Network Security and its Applications (IJNSA), Vol.1, No.2, pp 101-112.

Oesterling, L., Hayford, D., Friend, G. (2012). Comparison of commercial and next generation quantum key distribution: Technologies for secure communication of information. IEEE Conference on Technologies for Homeland Security (HST), pp 156-161.

Trappe, Wade., Washington, Lawrence C. (2002) Introduction to Cryptography with Coding Theory. Pearson Prentice Hall.

ISBN: 978-607-95635

Jouguet, P., Sebastien K-J, Leverrier, A., Grangier, P., Diamanti, E. (2013). Experimental demonstration of long-distance continuous-variable quantum key distribution. Nature Photonics, 7. 378-381.