Ciencia e Ingeniería Neogranadina
ISSN: 0124-8170
revistaing@unimilitar.edu.co
Universidad Militar Nueva Granada
Colombia

Guillén, Edward Paul; Navarro Gasca, José Jaime
Sistema de distribución de claves mediante criptografía cuántica para evadir ataques del tipo "Man in the middle"
Ciencia e Ingeniería Neogranadina, vol. 16, núm. 2, agosto-diciembre, 2006, pp. 64-73
Universidad Militar Nueva Granada
Bogotá, Colombia

SISTEMA DE DISTRIBUCIÓN DE CLAVES MEDIANTE CRIPTOGRAFÍA CUÁNTICA PARA EVADIR ATAQUES DEL TIPO "MAN IN THE MIDDLE"

SYSTEM OF DISTRIBUTION OF KEYS BY MEANS OF QUANTUM CRYPTOGRAPHY TO EVADE ATTACKS OF TYPE "MAN IN THE MIDDLE".

Edward Paul Guillén [1]
José Jaime Navarro Gasca [2]

Fecha de Recepción: 31 de Agosto de 2006
Fecha de Aprobación: 22 de Octubre de 2006

RESUMEN: *Las nuevas técnicas criptográficas, como la criptografía cuántica, permiten diseñar sistemas de distribución cuánticos de claves con niveles de seguridad bastante altos. A lo largo de este documento se describirá como se comportan estos sistemas frente a ataques del tipo "Man in the middle" y que debilidades pueden llegar a presentar.*

PALABRAS CLAVES: *Criptografía Cuántica, Mecanismos cuánticos, Distribución de claves cuánticas, criptografía, seguridad en redes.*

ABSTRACT*: Nowadays, it is possible to design very secure systems for key distribution. According to quantum cryptography, which is based on the properties of quantum mechanics, quantum key distribution systems are the most secure way to exchange private keys. This document leads you towards the understanding of these systems.*

KEYWORDS*: Quantum cryptography, quantum mechanics, quantum key distribution, cryptography, network security.*

1 Universidad Militar "Nueva Granada" GISSIC – gissic@umng.edu.co
2 Universidad Militar "Nueva Granada" GISSIC – gissic@umng.edu.co

I. INTRODUCCIÓN

Desde los principios de la civilización humana, se ha buscado la forma de transmitir información confidencial de manera secreta. Desde entonces, la ciencia de la criptografía se ha venido utilizando especialmente para propósitos militares, diplomáticos, y gubernamentales en general. Tan solo hasta la proliferación de los computadores y de los sistemas de comunicaciones digitales, fue que surgió una gran demanda por el uso de las comunicaciones privadas y seguras. En los comienzos de la era digital eran pocos los que usaban la criptografía, pero el éxito de Internet y del comercio electrónico hizo posible que la mayoría de usuarios comenzaran a hacer uso de diferentes técnicas criptográficas.

La criptografía es el arte de cifrar y codificar la información, mientras que el criptoanálisis es el arte de romper ó descifrar dichos códigos. La criptología es la combinación de las dos.
El proceso por el cual se representa un mensaje de tal forma que éste no sea legible, se conoce como encripción. Este proceso se puede describir matemáticamente de la siguiente forma: una función Ek se encarga de transformar un texto plano legible a un texto cifrado ó encriptado. El parámetro k se conoce como clave. De esta manera, podemos decir que:

$Ek(P) = C$ (Encripción) y $Ek(C)^{-1} = P$ (Desencripción)

donde P es el texto plano y C es el texto cifrado.

Con el fin de utilizar este esquema de encripción, las dos partes involucradas en la comunicación deben poseer una clave común.

La transmisión de un mensaje secreto se realiza de la siguiente manera: el emisor selecciona una función de encripción y la aplica al texto plano que desea transmitir. Luego, el texto cifrado se envía hacia el receptor, quien a su vez conoce la misma clave que el emisor y de esta forma puede generar la función de encripción inversa para descifrar el mensaje.

En la literatura, es común denominar a la parte que encripta y transmite los mensajes como Alice, y a la parte que recibe y decodifica como Bob (Ver Figura 1). Pero también existe Eve, un intruso que está pendiente de escuchar e interceptar la comunicación entre Alice y Bob.

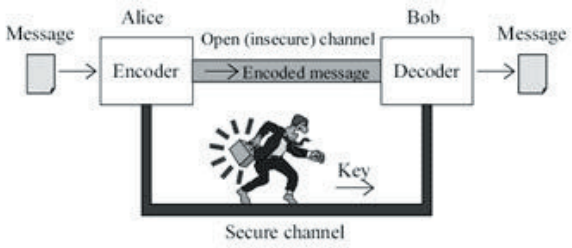

Figura 1: Esquema de un sistema de comunicación para distribución cuántica de claves. (Fuente: [11])

Mientras que en los inicios de la criptografía la seguridad de los métodos de encripción consistía en mantener en secreto el algoritmo de encripción que se estaba utilizando, hoy en día dicha seguridad recae sobre la privacidad de las claves. Es evidente que la seguridad se incrementa en la medida que aumenten el número de algoritmos posibles de encripción y la longitud de las claves (número de bits).
Existen dos tipos de criptosistemas, los que comparten las claves públicamente ó los que lo hacen secretamente.

En los criptosistemas asimétricos, Alice y Bob utilizan dos claves diferentes. Una clave pública que se utiliza en la encripción y otra privada para la desencripción. Estos criptosistemas también son conocidos como criptosistemas de clave pública.

Pero estos tipos de criptosistemas poseen un problema fundamental. En primer lugar, cualquier canal clásico privado se puede monitorear pasivamente, sin

que el transmisor o el receptor lo detecten.
Además, la física clásica permite medir todas las propiedades físicas de un objeto sin que se alteren dichas propiedades. Es por esto que la física clásica es vulnerable a cualquier tipo de interceptación.

Por otro lado, los algoritmos de encripción simétricos, aquellos que transmiten la clave con la cual se encripta o desencripta un mensaje, poseen la debilidad de que un intruso puede interceptar la comunicación para extraer la clave y posteriormente descifrar la información que esté circulando por el canal. En la criptografía clásica este problema se soluciona haciendo uso de los algoritmos de encripción asimétricos ó de clave pública. La seguridad de estos criptosistemas está basada en la complejidad matemática de factorizar productos de números primos muy grandes.
No obstante, se ha demostrado que un computador cuántico estaría en la capacidad de romper un criptosistema como estos en un tiempo muy reducido.
En conclusión, mientras usemos criptosistemas clásicos, no se podrá afirmar que la información está completamente protegida o segura.

A raíz de estos problemas surge una nueva alternativa para solucionar los problemas de distribución de claves de la criptografía clásica y es la distribución cuántica de claves ó QKD (Quantum Key Distribution, Distribución cuántica de claves).

II. ANÁLISIS DE LA PROBLEMÁTICA ACTUAL

La criptografía es el arte de convertir un mensaje a una forma ininteligible de tal manera que no cualquier persona sea capaz de interpretarlo. Para lograr esto es necesario hacer uso de algún algoritmo, también conocido como criptosistema, para que combine o mezcle el mensaje con alguna información adicional y de esta forma generar un criptograma, es decir un mensaje cifrado. La información adicional utilizada para alterar dicho mensaje se conoce como clave. Resulta evidente que para que un criptosistema sea lo suficientemente seguro, debe ser imposible descifrar un mensaje si no se conoce la clave. Por esta razón es que nos debemos concentrar en mantener la clave segura y evitar que ésta sea interceptada. Sin embargo, los actuales mecanismos clásicos de encripción aún presentan debilidades en este aspecto, pues en varias ocasiones muchos intrusos han conseguido obtener sus claves causando serios problemas a los sistemas de comunicación y a la información.

Un tipo de ataque clásico en criptografía se conoce como “Man-in-the-Middle Attack” el cual consiste básicamente en ubicar un dispositivo en el medio de una comunicación, y así éste puede recibir la información del transmisor para procesarla, interpretarla y finalmente reenviarla al receptor, sin que las partes lo detecten. Además este tipo de ataques es común gracias a que las claves se intercambian generalmente por redes públicas.

Es por esto que surge la gran necesidad de crear un mecanismo de encripción que no sea vulnerable a esta forma de ataques y es en este escenario donde tiene protagonismo la criptografía cuántica.

III. INGENIERÍA DEL PROYECTO

La distribución cuántica de claves, QKD (Quantum Key Distribution), es una tecnología que se propuso como solución a los problemas de distribución de claves en los criptosistemas clásicos. Basado en las leyes de la mecánica cuántica, la QKD permite que las partes involucradas en una comunicación puedan intercambiar las claves de forma segura, las cuales de hecho se pueden utilizar en la criptografía clásica.
Debido a que la criptografía cuántica está fundamentada en la mecánica cuántica, obedece a las siguientes propiedades:

- No se pueden hacer medidas sin perturbar el sistema. (A menos que el estado sea compatible con la medición).

- No se puede determinar simultáneamente y con un alto grado de precisión la posición y el momento de la partícula.

- No se puede medir la polarización del fotón en la base vertical/horizontal y en la base diagonal simultáneamente.

- No se puede duplicar un estado cuántico desconocido.

La primera regla puede ser interpretada como un punto de vista negativo de la mecánica cuántica comparada con la mecánica clásica. Sin embargo al ver el lado positivo debido a nuevos hitos en las concepciones de la información, permite pasar de una etapa de inconvenientes, a las aplicaciones potencialmente útiles, desprendiéndose el teorema de la no clonación: La copia perfecta en el mundo cuántico es imposible. El hecho de que los estados cuánticos, también conocidos como información cuántica, no pueden ser copiados es uno de los atributos específicos de esta nueva clase de información tan diferente y por tanto tan atractiva, haciendo a la criptografía cuántica potencialmente segura. [10]

La idea principal de la distribución cuántica de claves consiste en explotar el hecho de que un estado cuántico no se puede copiar y que no es posible realizar una medición sin tener que alterar dicho estado cuántico. Es posible establecer un canal de comunicaciones seguro si la información clásica se transmite codificada en estados cuánticos únicos. Esto no quiere decir que se va a evitar que un espía (Eve) extraiga información valiosa del canal, sino que será posible detectarlo inmediatamente. En un canal de transmisión ideal, sin pérdidas y sin ruido, es posible detectar intrusos mediante el análisis del ruido introducido a los estados transmitidos. En canales reales, la situación es un poco más complicada pero sin embargo también es posible detectar la presencia de intrusos o de alteraciones en la comunicación.

A. El Qubit

En la teoría de la información clásica la unidad básica de la información es un bit binario y éste sólo puede ser 0 ó 1. En la teoría de la información cuántica la unidad básica de la información es el bit cuántico ó qubit, y estos pueden existir en dos posibles estados: uno único (0 ó 1) ó como la superposición de los dos estados anteriores. Sin embargo, la mayor diferencia entre un bit clásico y un qubit es que múltiples qubits pueden experimentar un entrelazamiento cuántico, también denominado 'entanglement'. Además, un qubit es un fotón que se puede polarizar ya sea linealmente (Horizontal o Vertical) o circularmente (Derecha o Izquierda). Sin embargo, en los laboratorios es más común trabajar con polarización lineal ya que esta última es más fácil de detectar. Asimismo, es más frecuente trabajar con fotones gracias a que estos son capaces de cubrir recorridos de grandes distancias y además pueden viajar a través del espacio libre o por fibra óptica. Cabe aclarar que los canales de comunicación que se emplean para la distribución cuántica de claves, no son cuánticos. Lo que es cuántico es la información que dicho canal está transportando. [3]

B. Protocolos de QKD

BB84: En la criptografía cuántica, los codificadores son quienes definen como se representa la información clásica mediante estados cuánticos. Una forma para codificar información clásica por medio de fotones polarizados, consiste en representar un '0' lógico como un fotón polarizado horizontalmente (I->>) , y un '1' lógico como un fotón polarizado verticalmente (I->>). Este esquema de codificación por polarización lineal sería suficiente para poder transmitir datos entre Alice y Bob, pero no para ofrecer un canal de comunicaciones seguro. El hecho de codificar información en una sola base (rectilínea) hace que sea más fácil la detección de la información. [13]

El protocolo BB84, llamado así en honor a los apellidos de sus desarrolladores Charles Bennett - Guilles Brassard y al año en que lo presentaron (1984), ex-

tiende un poco el anterior esquema de codificación haciendo uso de una segunda base para así generar más formas de polarización. Esta base, conocida como base diagonal, permite representar un '0' lógico como un fotón polarizado diagonalmente hacia la derecha (45°) y un '1' lógico como un fotón polarizado diagonalmente hacia la izquierda (135°). Entonces tenemos que: un '0' lógico se podrá representar mediante polarización horizontal ó diagonal derecha, y un '1' lógico se representará con fotones polarizados verticalmente o diagonal izquierda.
El funcionamiento del protocolo se puede explicar por medio de los siguientes tres pasos:

1. Cada vez que Alice quiera enviarle un bit a Bob, ella debe seleccionar una de las dos bases (lineal ó diagonal), que en realidad son filtros de polarización, con el fin de enviar el fotón correspondiente y así polarizarlo en una de las 4 posibles formas de polarización (0°-45°-90°-135°).
2. Bob, de igual manera tendrá que seleccionar una de las dos bases para realizar el filtrado del fotón que va a recibir. Además, Bob debe registrar cual fue la secuencia de las bases utilizadas para la recepción, ya que estas son necesarias en el momento de verificar los patrones de Alice con respecto a los de Bob.
3. Después de terminada la transmisión de la información, Bob deberá enviarle a Alice (por un canal público que soporte métodos de autenticación) el registro de las bases utilizadas durante el proceso de recepción, para que ella lo compare con el registro de bases utilizado en el proceso de transmisión y así poder saber con certeza que medidas tuvieron en común Alice y Bob. Es importante aclarar que en ningún momento Bob revelará el resultado de su medición, tan solo le dirá a Alice cual fue la forma y el orden con la que midió las polarizaciones de los fotones recibidos. Una vez realizada la comparación, Alice le comunicará a Bob cuales fueron los fotones que se codificaron y se decodificaron con la misma base, y estos serán los que conformarán la clave secreta.
En este protocolo el canal cuántico se utiliza únicamente para el intercambio de las claves privadas, mientras que el resto de información se transmite por el canal público.
Una vez Alice y Bob han acordado la clave, ellos pueden comenzar a transferirse información de manera segura. La propiedad de poder intercambiar una clave de manera absolutamente segura antes de intercambiar cualquier otro tipo de información, da origen a lo que en criptografía cuántica se conoce como sistema seguro One-Time Code-Pad.
Suponiendo que Alice y Bob ya poseen la misma clave para comunicarse de forma segura, veamos como sería un proceso básico de encripción/desencripción:

Encripción		
	Clave:	011101
		XOR
	Texto de Alice:	101010
	Texto cifrado:	110111
Desencripción		
	Texto cifrado:	110111
		XOR
	Clave:	011101
	Texto de Bob:	101010

Nótese que ni Alice ni Bob deciden cual es la clave que se va a utilizar durante la transferencia de la información. De hecho, la ventaja de este protocolo es que la clave se genera aleatoriamente según los filtros polarizantes que utilicen ambas partes.
Sin embargo, la verdadera dificultad que presenta este protocolo radica en mantener estable la polarización de los fotones en transmisiones a larga distancia. Pues ocurre que en enlaces de muy larga distancia es probable que el ruido que se suma al canal, altere las polarizaciones de los fotones.

B92: Este protocolo lo propuso Charles Bennett en 1992. A diferencia del protocolo BB84, éste protocolo transmite fotones individuales polarizados en dos sistemas no ortogonales de referencia incompatibles, uno lineal (horizontal-vertical) y otro diagonal (izquierda o derecha).

En primer lugar, Alice comienza a transmitirle a Bob una secuencia de fotones. Después de que Alicia haya transmitido todos los fotones a Bob, se procede a evaluar de que forma realizó la detección Bob y a mirar en donde hay coincidencias con respecto a Alice.

Primero que todo, Alice y Bob generan, independientemente, unas secuencias totalmente aleatorias mediante cualquier proceso no determinístico, y estas pasan a ser sus claves primarias. Una vez cada uno ha generado su propia clave, Alice comienza a transmitir una secuencia de fotones polarizados hacia Bob. Los fotones que transmite Alice se polarizarán verticalmente (90°, para representar un '0' lógico) ó diagonalmente (45°-Diagonal derecha, para representar un '1' lógico). Una vez Alice le ha enviado su clave primaria a Bob, representada mediante fotones polarizados en 45° ó 90°, él debe comenzar a realizar el proceso de detección. Para esto, Bob también utiliza dos tipos de filtros polarizantes pero con la diferencia de que estos filtros representarán un '0' lógico cuando el filtro se encuentre polarizado en 135° (Diagonal izquierda), y un '1' lógico cuando el filtro se encuentre polarizado horizontalmente (0°). [2]

Cada vez que Bob reciba un fotón de Alicia, él seleccionará una polarización de acuerdo con su clave primaria y llevará un registro del resultado de observar si dicho fotón pasó o no a través del polarizador elegido, así como el tipo de polarizador que utilizó en cada caso.

Si Bob utiliza en la detección un filtro que se encuentre en la misma base que el fotón transmitido por Alice, dicho fotón no podrá pasar a través de éste. Esto se debe a que el fotón transmitido por Alice y el filtro utilizado por Bob estarán formando siempre un ángulo de 90°, lo cual quiere decir que son siempre perpendiculares.

Por ejemplo: Si Alice transmite un fotón polarizado linealmente, es decir verticalmente, y Bob emplea un filtro polarizado en la misma base lineal (o sea horizontalmente), el fotón no podrá pasar por el filtro dado que entre ellos se forma un ángulo de 90º. Igual ocurre cuando Alice transmite con polarización diagonal (derecha) y Bob recibe con polarización diagonal (izquierda).

Pero por otro lado, si Bob utiliza en la detección un filtro polarizante que se encuentre en la base contraria a la que utilice Alice en la transmisión, el fotón siempre formará un ángulo de 45° con respecto al filtro polarizante de Bob. En este caso, la incertidumbre cuántica hará que los fotones que lleguen al detector de Bob se comporten como si el 50% de ellos estuvieran polarizados paralelamente al filtro polarizante (es decir que lo atraviesan), mientras que el otro 50% se comportará como si estuvieran polarizados perpendicularmente al polarizador (es decir, que no lo atraviesan). Por lo tanto, y de acuerdo con la tabla 1, cada vez que Bob registre el paso de un fotón sabe con certeza que él y Alice tienen el mismo valor de bit de clave primaria.

Una vez finalizada la transmisión de todos los fotones, Bob le enviará a Alice una copia de sus mediciones (coincidencias y fallos) a través de un canal público. Sin embargo, Bob nunca le dirá cuales fueron las polarizaciones que él empleo para obtener cada bit.

Finalmente, Alice y Bob almacenarán únicamente la secuencia de bits formada por los resultados afirmativos de Bob, y ésta será la clave privada que ellos utilizarán como clave de sesión. En promedio, el 25% de los bits transmitidos son los que llegan con éxito lo cual quiere decir que el 75% de bits de la secuencia original se pierden. Este el precio que tiene que pagar la criptografía cuántica, se pierde en eficiencia pero se gana en seguridad.

Sistemas de QKD por codificación de fase: La idea de codificar bits de información mediante el ajustamiento de la fase de los fotones, la propuso inicialmente Bennett. Sin embargo, el primero en desarrollar este sistema fue Paul Townsend en 1993. Este sistema se basa en el protocolo BB84 ya que hace uso de 4 valores posibles de fases. En este caso, el análisis de los estados cuánticos se realiza por medio de interferómetros En la Figura 2 se muestra la versión en fibra

óptica del interferómetro de Mach-Zehnder. Este interferómetro junto con una fuente y un detector de fotones, se puede utilizar como un sistema de distribución cuántica de claves.

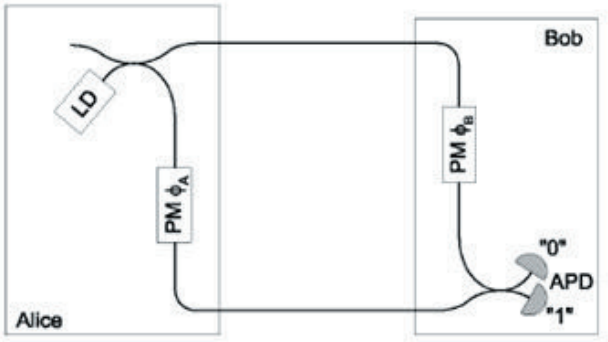

Figura 2: Interferómetro de Mach-Zehnder.

En este esquema, Alice y Bob utilizan interferómetros de Mach-Zehnder desbalanceados, ya que un brazo es más largo que el otro. Los dos interferómetros se conectan en serie por medio de una fibra óptica (Ver Figura 3), y cada uno de los interferómetros contiene un modulador de fase en el brazo más corto.

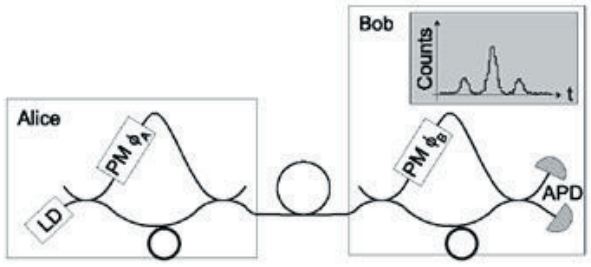

Figura 3: Sistema de QKD por interferómetros. [LD: Laser diode, PM: Phase modulator, APD: avalanche photodiode]

Veamos como sería el funcionamiento: En este sistema es posible aplicar cuatro valores de corrimientos de fase. En primera instancia, Alice debe seleccionar que valor de corrimiento de fase desea aplicar al fotón, entre (0, π/2, π, 3 π/2), para codificar un bit clásico. Por otro lado, Bob también debe seleccionar que valor de corrimiento de fase desea aplicar (entre 0 y π/2) al fotón que está recibiendo y además asocia el puerto de salida "0" (APD-superior) a bits con valor lógico igual a 0 y el puerto de salida "1" (APD inferior) a bits con valor lógico igual a 1. Cuando la diferencia en fase entre las fases aplicadas por Alice y por Bob a cada fotón sea igual a 0 ó π, quiere decir que Alice y Bob está utilizando bases de medición compatibles y por lo tanto se obtendrán resultados válidos. En este caso, Alice podrá inferir, a partir del corrimiento de fase que ella le aplicó al fotón, cual va a ser el puerto de salida de éste (en el lado de Bob) y cual fue el valor de bit registrado por Bob para dicho fotón. De igual manera, Bob estará en la capacidad de deducir el valor de corrimiento de fase aplicado por Alice, si él conoce por cual puerto sale el fotón. Pero cuando la diferencia en fase es igual a π/2 ó 3π/2, se concluye que Alice y Bob están utilizando bases de medición incompatibles y en este caso el fotón seleccionará aleatoriamente por que puerto salir.

Una vez Alice termina de enviar toda la información a Bob, ellos proceden a comparar los resultados haciendo uso de un canal público.

De igual manera que en el protocolo BB84, los bits que lográ detectar Bob serían los que conforman la clave privada para Alice y para Bob.

Finalmente, es importante mencionar que para que no se generen errores durante la transmisión de los fotones se debe garantizar que las longitudes de cada uno de los brazos de los interferómetros debe ser la misma del uno con respecto al otro.

C. Resultados

Respuesta de los criptosistemas clásicos y cuánticos frente a ataques del tipo "Man in the middle": Es necesario aclarar que existen dos tipos de ataques de "Man in the middle". Uno es pasivo (extracción de información mediante interceptación) y el otro es activo (Extracción de información mediante suplantación).

En los laboratorios se ha comprobado que los protocolos de QKD no son vulnerables frente a ataques del

tipo “Man in the middle - pasivos”.
Por otro lado, dentro de la comunidad de la criptografía cuántica, muchas veces se cae en el error de pensar que como Eve está limitada por las ya conocidas propiedades de la mecánica cuántica, ella no puede hacer nada, y no se prevé que ella puede llegar a tener a su disposición tecnología y procesos matemáticos más avanzados que cualquier sistema actual.

Como resultado, se ha demostrado que ningún sistema de QKD puede resistir un ataque del tipo Man in the middle – activo.

Para que ocurra el ataque, el atacante (Eve) debe actuar de igual forma que si lo fuese a hacer sobre un criptosistema clásico. El objetivo es que Eve suplante a Bob cuando este hablando con Alice, y suplante a Alice cuando esté hablando con Bob. Para lograr esto basta con cortar la fibra óptica y establecer dos sesiones diferentes con cada uno de ellos.

Implementaciones actuales y futuros desarrollos:
-Actualmente, la BBN Technologies de los Estados Unidos está construyendo múltiples enlaces de QKD para consolidar lo que sería una red cuántica de QKD. Así, si un enlace fallara ya sea porque lo estén interceptando frecuentemente o porque este presentando niveles de ruido muy altos, se procedería a hacer uso de otro enlace QKD en la red. La idea es que si algunos de los enlaces de la red cuántica no están ocupados, estos se podrán utilizar no sólo para el envío de claves sino también para transportar mensajes de los usuarios encriptados.
-En el DARPA se están llevando a cabo investigaciones que apuntan a la creación de repetidores cuánticos. De conseguir crear tales repetidores, los problemas de distancia quedarían solucionados.
-En la actualidad ya es posible encontrar equipos de QKD y generadores de números cuánticos aleatorios. Entre las marcas que se pueden encontrar en el mercado están: id Quantique y magiqtech.

Debilidades en los sistemas de QKD:
-Una de las debilidades de estos sistemas radica en el tipo de medio de transmisión que se utilice para el transporte de las claves. Generalmente el medio de transmisión utilizado es la fibra óptica. Sin embargo, la fibra óptica presenta altos niveles de pérdidas (la fibra óptica no es perfectamente circular) por lo que los fotones que viajan a través de ella difícilmente podrán recorrer largas distancias (mayores a 100 km).
-El dicho de que la seguridad es tan fuerte como su eslabón más débil, aplica en estos sistemas. Hemos visto, durante el estudio de los sistemas de QKD, que estos se basan en dos tipos de canales: uno cuántico y uno clásico. Esto se puede ver como una debilidad ya que finalmente lo que se ha ganado en seguridad dentro del canal cuántico, se pierde en el momento en que se transfiere información tan delicada por un medio de un canal no muy seguro como lo es el canal clásico.

IV. CONCLUSIONES

-Una de las limitaciones que actualmente poseen los sistemas de QKD es la distancia. Se ha conseguido realizar transmisiones de claves cuánticas hasta una distancia de aproximadamente 100 km [10], lo cual todavía sigue siendo muy bajo. Cualquier sistema de distribución de claves actual debería estar en la capacidad de poder transmitir dichas claves entre dos puntos cualesquiera sin que la distancia fuera un problema.
Esas limitaciones de distancia se deben básicamente a que los medios de transmisión impiden que por ejemplo la polarización de un fotón, permanezca perfecta durante trayectos muy largos. Además, a esto se le puede agregar el ruido propio que añade cada medio de transmisión. Pero la razón más importante por la cual la distancia se vuelve una limitante es porque para poder transmitir información a través de un enlace de fibra óptica resulta estrictamente necesario utilizar repetidores que amplifiquen y retransmitan las señales, lo cual resulta imposible en los sis-

temas de QKD. Evidentemente, dicha manipulación alteraría la información cuántica que transportan los fotones.

-Por otro lado, es supremamente difícil la generación de un único fotón debido a la distribución estadística de Poisson de la energía proveniente de fuentes lumínicas. Sería ideal poder hacerlo ya que así se evitaría cualquier intento de duplicación o extracción de un fotón en un ataque del tipo Man in the middle. Pero el problema está en que un impulso puede contener varios fotones a la vez, lo cual le permitiría a Eve extraer alguno de ellos y dejar pasar los otros, sinque sea detectada. [10].

-También es necesario tener en cuenta que la QC es una técnica bastante nueva, que se encuentra en etapa de desarrollo y que muy posiblemente avanzará en cuanto a las dificultades que ella aún presenta. Por esto, el alcance de este proyecto se va a ver limitado temporalmente, mientras los investigadores propongan otra nueva técnica ó un nuevo protocolo que sea capaza de solventar las anteriores dificultades.

REFERENCIAS

[1] ELLIOT, C. PEARSON, D. TROXEL, G. Quantum Cryptography in Practice. BBN Technologies. 2002.12.p

[2] LOMONACO, S. J. A Quick Glance at Quantum Cryptography. University of Maryland Baltimore County. 1998.54.p

[3] BOHM, H. R. A compact source for polarization entangled photon pairs. Vienna University of Technology. 2003.68.p

[4] MAKAROV, V. HJELME, D. R. Faked states attack on quantum cryptosystems. Norwegian University of Science and Technology. 2005.15.p

[5] REDMOND, W. Is the future of cryptography in qubits?. GIAC Security Essentials Certification. 2002.12.p

[6] VAKHITOV, A. MAKAROV, V. HJELME, D. R. Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography. Norwegian University of Science and Technology. 2001.16.p

[7] MULLINS J. Making Unbreakable Code. IEEE Spectrum. 2002.6.p

[8] SCHILLER, C. No Single Killer App for PKI. GSEC. 2002.28.p

[9] WOOD, D. PKI, The What, The Why, and The How. GSEC – SANS Institute. 2002.18.p

[10] GISIN, N. RIBORDY, G. TITTEL, W. ZBINDEN, H. Quantum Cryptography. Group of Applied Physics - University of Geneva. 2002.51.p

[11] ELLIOT, C. Quantum Cryptography. IEEE Security and Privacy. 2004.5.p

[12] KLISTNER, T. Quantum Cryptography: Is your data safe even when somebody looks?. GSEC. 2001.13.p

[13] BRYLEVSKI, A. Quantum Key Distribution: Real Time Compensation of Interferometer Phase Drift. NTNU Department of Physical Electronics. 2003.45.p

[14] PATERSON, K. G. PIPER, F. AND SCHACKT, R. Why Quantum Cryptography?. University of London. 2005.5.p

[15] JAIN, R. RADHAKRISHNAN, J. SEN, P. Prior entanglement, message compression and privacy in quantum communication. Proceedings of the Twentieth Annual IEEE Conference on Computational Complexity (CCC'05). 2005.12.p

[16] AUBURN, B. R. Quantum Encryption – A Means to perfect security?. SANS Institute. 2003.14.p

[17] GOMEZ, J. P. NAVARRO, J. J. QUINTERO, R. Crip-

tografía Cuántica. Universidad Militar Nueva Granada. 2005.11.p

[18] CASTAÑEDA, M. G. DE-GEUS. J. E. Introducción a la física moderna. Universidad Nacional de Colombia. 1993.421.p

[19] RITTER, T. Learning about Criptography [en línea]. 2 de Septiembre de 2003 [Citado en 22/02/2006]. Disponible en Internet :< http://www.ciphersbyritter.com/LEARNING.HTM >.

[20] ANSHEL, M. Computer Security and Criptography [en línea]. [Citado en 22/02/2006]. Disponible en Internet : < http://www-cs.engr.ccny.cuny.edu/~csmma/#scintro >.