FUNDAMENTOS DE CRIPTOGRAFÍA CUÁNTICA

HERNÁN ORTIZ ROJAS

UNIVERSIDAD EAFIT
ESCUELA DE INGENIERÍA
DEPARTAMENTO DE INFORMÁTICA Y SISTEMAS
MEDELLÍN
2007

FUNDAMENTOS DE CRIPTOGRAFÍA CUÁNTICA

HERNÁN ORTIZ ROJAS

Trabajo de grado para optar por el
título de Ingeniero de Sistemas

Director
JUAN GUILLERMO LALINDE PULIDO
Ph. D. en Telecomunicaciones

UNIVERSIDAD EAFIT
ESCUELA DE INGENIERÍA
DEPARTAMENTO DE INFORMÁTICA Y SISTEMAS
MEDELLÍN
2007

A mis padres, Hernán y Nubia.

AGRADECIMIENTOS

A Juan Guillermo Lalinde le agradezco su guía, muy precisa y constante durante todo el proceso. Además le agradezco el tiempo que invirtió en el proyecto.

A mis profesores de matemáticas especiales: Andrés Sicard, Manuel Sierra y Hugo Guarín, les agradezco por introducirme a conceptos matemáticos indispensables para entender muchos conceptos relacionados con el tema.

Al profesor José Ignacio Marulanda, por hacer que me siguiera gustando la física.

Al físico Fred Alan Wolf por mostrarme otro camino para entender los fenómenos cuánticos, y animarme a investigar más sobre el tema.

A mis padres les agradezco por ser tan pacientes.

CONTENIDO

1 DESCRIPCIÓN DEL PROYECTO

1.1 PRESENTACIÓN

A pesar de que la criptografía tradicional permite en la actualidad mantener una comunicación segura entre dos partes, las propuestas algorítmicas de Shor en 1994, que usan las propiedades de un hipotético computador cuántico (que está en proceso de desarrollo), pondrían en peligro algunos sistemas criptográficos más usados, como el RSA.

La criptografía cuántica puede lograr comunicaciones seguras utilizando leyes de la naturaleza a escala cuántica, como el principio de incertidumbre de Heisenberg, la superposición cuántica y el enredo cuántico.

Esta monografía pretende abarcar de la manera más simplificada y directa posible los fundamentos de la criptografía cuántica, que es la única aplicación comercial existente hasta la fecha de la Teoría de la Información Cuántica, sirviendo como una introducción al tema, y una motivación para futuros estudios.

1.2 DEFINICIÓN DEL PROBLEMA

Se hace necesario facilitar a ingenieros, matemáticos y físicos, un acercamiento a la criptografía cuántica, con el fin de motivar la investigación académica y nuevos desarrollos en el área.

1.3 OBJETIVOS

1.3.1 Objetivo general

Documentar los conceptos básicos de la criptografía cuántica.

1.3.2 Objetivos específicos

- Describir los conceptos fundamentales de la criptografía tradicional, así como una visión histórica de la misma.

- Describir generalidades de la mecánica cuántica e ilustrar algunos conceptos de ésta que son importantes para el estudio de la criptografía cuántica.

- Introducir la computación cuántica y el efecto que ésta tendrá sobre la criptografía tradicional.

- Explorar la evolución de la criptografía cuántica, y los principales protocolos usados para generar claves cuánticas.

- Describir brevemente el panorama comercial de la criptografía cuántica hasta la fecha.

2 ¿QUÉ ES LA CRIPTOGRAFÍA?

Esta sección aborda el tema de la criptografía. La criptología incluye dos técnicas complementarias: la Criptografía y el criptoanálisis [Martorell 00].

El criptoanálisis, es el estudio de técnicas matemáticas para tratar de vulnerar técnicas criptográficas, y en general, servicios de seguridad de la información [Menezes, Oorshot y Vanstone 96].

La criptografía es: "... el estudio de técnicas matemáticas relacionadas con aspectos de la seguridad de la información tales como la confidencialidad, integridad de datos, autenticación de entidades, y autenticación de origen de los datos. La criptografía no es el único medio de proveer seguridad de la información, sino un conjunto de técnicas" [Menezes, Oorshot y Vanstone 96].

Otra definición, un poco más precisa, es "Rama inicial de las Matemáticas y en la actualidad también de la Informática y la Telemática, que hace uso de métodos y técnicas con el objeto principal de cifrar, y por tanto proteger, un mensaje o archivo por medio de un algoritmo, usando una o más claves" [Ramió 06].

Es importante mencionar que los esquemas de cifrado no son invulnerables. Por ejemplo, un espía, después de invertir un periodo de tiempo atacando el código, podría descifrar los datos. Este periodo de tiempo es importante porque la vida útil de la clave debe estar correlacionada con la vida útil de los datos que están siendo protegidos. En algunos casos un día es suficiente, mientras que en otros debería permanecer invulnerable de manera indefinida.

El ataque más simple que puede realizar un atacante para saber cuál clave se está usando en una comunicación, es hacer una búsqueda exhaustiva o de

“fuerza bruta” con diferentes claves hasta que alguna le funcione. El tamaño de la clave define el número de combinaciones que debe intentar, así que mientras ésta sea más grande, la tarea computacional es más compleja haciendo más seguro el esquema.

La criptografía se basa en ciertos tipos de funciones. Las más importantes son la función de una vía y la función de una vía con trampa. El término *función de una vía* se refiere a una función $y = f(x)$ en la que, dado x, es posible hacer la computación para hallar y; pero la inversa $x = f^{-1}(y)$, es decir, dado y encontrar x, es irrealizable computacionalmente. Así que es fácil hacer la computación directa, pero la inversa se complica.

El término “función de una vía con trampa” se refiere a una función $y = f(x)$ como la anterior, en la que es fácil hallar y dado x; pero se diferencia en que su inverso se puede obtener fácilmente con una información especial llamada *trampa*.

La existencia de las funciones de una vía y de una vía con trampa mencionadas anteriormente, no ha sido demostrada: “… No se sabe si estas funciones realmente son de una vía; sólo es una conjetura apoyada en investigaciones exhaustivas que hasta ahora han fallado en producir un algoritmo de inversión eficiente” [Goldrich 07]. Existen algunas funciones que aparentemente cumplen estas propiedades y se usan en la criptografía de clave pública. Más adelante se mencionará cómo, con el desarrollo de la computación cuántica, las funciones que aparentemente son “de una vía” pueden perder su utilidad en criptografía.

2.1 EVOLUCIÓN DE LA CRIPTOGRAFÍA

A continuación se hará un repaso muy breve a la historia de la criptografía. Para un estudio detallado del tema desde una perspectiva no-técnica se recomienda el libro *Codebreakers* [Kahn 96] y *The Code Book* [Singh 00]. Para un desarrollo técnico se recomiendan [Menezes, Oorshot y Vanstone 96] y [Ramió 06].

El uso de métodos para mantener secreta la información se ha registrado desde culturas antiguas. En la cultura egipcia los sacerdotes usaban jeroglíficos incomprensibles para el común de las personas. En la babilonia usaban la escritura cuneiforme (con caracteres que tenían forma de cuña o clavo) y en la cultura griega se inventaron un sistema en el que dependiendo del ancho de un bastón sobre el que se enrollaba un cinturón de cuero, podría leerse o no la información escondida.

En la Segunda Guerra Mundial la criptografía impulsó la creación de tecnología. Durante esta época, Alan Turing, en el Code and Cipher School de Inglaterra, desarrolló una aproximación estadística para descifrar el sistema de codificación alemán denominado Enigma. Con base en esta aproximación y las ideas de Max Newman, Tommy Flowers construyó el sistema COLOSSUS [Hodges;Sale], utilizado para descifrar el código Fish utilizado por los alemanes para comunicaciones estratégicas. Esto les permitió a los aliados una ventaja considerable en la guerra.

En el mundo moderno la criptografía no sólo es usada para el intercambio de mensajes secretos. Cada compra por medio de un sistema de comercio

electrónico, cada conversación por celular, cada retiro de dinero de un banco o transferencia electrónica necesita de un elemento clave: la confianza[1]. Para esto, la autenticación brinda una mayor seguridad frente a los medios físicos tradicionales: el uso de firmas digitales de acuerdo con la normatividad legal vigente permite tener certeza con respecto a la identidad del emisor. Las negociaciones por medio de comercio electrónico cada vez son más comunes, y mueven billones de dólares anuales [RSA]; hecho que no podría ser posible de no existir la criptografía y la autenticación. Otra aplicación de la criptografía que cada día adquiere más importancia es la creación de sistemas de gestión de derechos autor (DRM – Digital Rights Management) para proteger los contenidos digitales tales como audio y video [DRMWiki].

2.2 CRIPTOGRAFÍA DE CLAVE PRIVADA Y CLAVE PÚBLICA

Hasta la invención de la criptografía de clave pública en 1970`s, todos los sistemas criptográficos operaban en un principio diferente: el de la criptografía de clave privada. En un sistema de criptografía de clave privada, el emisor y el receptor deben tener la misma clave. El emisor la utiliza para cifrar[2] (*encriptar*) el

[1] Si bien la criptografía permite garantizar confidencialidad y no confianza, la confidencialidad es la base sobre la cual se construye la noción de confianza en el comercio electrónico.

[2] El verbo encriptar no existe en el español. Sin embargo, en la literatura de origen latinoamericano se utiliza este anglicismo. El verbo que existe en español es cifrar.

mensaje, y el receptor la usa para descifrar el mensaje cifrado. Por este motivo, los sistemas de criptografía de clave privada no garantizan autenticidad.

Los esquemas de criptografía de clave privada clásicos se basan en dos operaciones fundamentales: La sustitución y la permutación. La sustitución establece una correspondencia entre los símbolos del alfabeto en el que está escrito el mensaje original y otro alfabeto (que puede ser el mismo). La clave determina cual de todas las sustituciones posibles va a ser utilizada. Por ejemplo, la palabra “computador”, con la clave a=>b, b=>c, c=>d…etc. produciría el mensaje: “dpnqvubeps”. La permutación consiste en alterar los símbolos de un mensaje cambiándoles el orden con una regla determinada, para que el criptograma contenga los mismos elementos del texto original, pero de una forma que resulta incomprensible si se desconoce dicha regla. Por ejemplo, la frase del filósofo griego Demócrito (sin signos de puntuación) “POR CONVENCION HAY COLOR DULZURA AMARGURA PERO EN REALIDAD HAY ATOMOS Y ESPACIO” en una tabla de diez columnas y ocho filas, se vería así:

P	O	R		C	O	N	V	E	N
C	I	O	N		H	A	Y		C
O	L	O	R		D	U	L	Z	U
R	A		A	M	A	R	G	U	R
A		P	E	R	O		E	N	
R	E	A	L	I	D	A	D		H
A	Y		A	T	O	M	O	S	
Y		E	S	P	A	C	I	O	

Figura 1: Representación de la frase de Demócrito en una tabla de 10x8

Al cambiar las filas con las columnas, el texto cifrado quedaría así: “PCORARAYOILA EY ROO PA E NRAELASC MRITPOHDAODOANAUR AMCVYLGEDOIE ZUN SONCUR H “

Un ejemplo de criptografía de clave privada es el criptosistema *one-time* pad. Éste es el único sistema criptográfico para el cual se ha demostrado que es irrompible y ha sido usado en trabajos de inteligencia y en enlaces de comunicación intergubernamental de alto nivel [Menezes, Oorshot y Vanstone 96]. En este sistema, dos partes tienen *pads* idénticos de claves cifradas, y cada vez que quieren comunicar un mensaje, cada parte usa la clave detallada en la página superior del *pad*, que ellos después rompen y destruyen. El siguiente mensaje se codifica usando la próxima clave de encriptación en el *pad* [Brown 00]. Ambas partes tienen que haberse encontrado, y haber generado anticipadamente una lista de claves. Las claves deben ser totalmente aleatorias y deben tener la misma longitud que el mensaje.

El gran problema de los sistemas de clave privada es la distribución de la clave. Para que sea segura, ambas partes tendrían que encontrarse físicamente, o usar un tercero en el que confíen plenamente (con mecanismos para evitar la traición, que es una característica muy factible en un ser humano), y por lo general esto aumentaría el costo. El trabajo de Diffie-Hellman en 1976 [Ramió 06] significó un paso gigantesco en el desarrollo de la criptografía al resolver el problema de intercambio de claves. Para esto utilizan un grupo multiplicativo con inverso y un generador *g* de manera que cada una de las partes involucradas genera un número aleatorio *a,* y comparten el resultado de g^a. Basándose en el número recibido y el número aleatorio generado, ambas partes generan la clave g^{ab} donde g^a es el valor recibido y *b* el valor generado. Su seguridad se debe a la dificultad de resolver el problema del logaritmo discreto [Menezes, Oorshot y Vanstone 96].

A finales de los 70s surgieron los criptosistemas de clave pública. El más importante es el RSA, inventado en 1978 por Ronald Rivest, Adi Shamir, y Leonard Adleman [RSA]. En estos sistemas, el emisor y el receptor usan claves distintas para *cifrar* y *descifrar* un mensaje. A diferencia de la criptografía de clave privada, donde se corre el riesgo al tener que compartir la única clave, la criptografía de clave pública funciona de la siguiente forma: cada receptor genera individualmente dos claves, una pública (que será compartida con cualquiera que desee enviarle un mensaje) y una privada, que se mantendrá en secreto. Si se cifra con la clave pública, se descifra con la clave privada y viceversa. De este modo, si un espía interceptara los datos que se estuvieran enviando firmados con la clave pública del receptor, no podría leerlo porque no tendría la clave privada del receptor garantizando confidencialidad. De la misma manera, si el emisor cifra los datos que va a enviar con su clave privada, se obtiene autenticidad porque el único que posee la clave privada es el emisor.

El sistema RSA, uno de los criptosistemas de clave pública más utilizado, se basa en la complejidad algorítmica de la factorización de enteros [Menezes, Oorshot y Vanstone 96], que con la tecnología actual tardaría años en ser vulnerado. Siendo un ejemplo de la función aparentemente de una vía con trampa, cuya definición se mencionó anteriormente.

3 GENERALIDADES DE LA MECÁNICA CUÁNTICA

“La teoría cuántica es, en el presente, el mejor modelo matemático para describir el mundo físico.” [Gruska 99].

La mecánica cuántica (o física cuántica) es un modelo para describir el comportamiento de las partículas subatómicas. Con ella se demuestra que la realidad a nivel microscópico se comporta muy diferente a lo que se experimenta a nivel macroscópico. La física clásica, en particular las leyes de la mecánica de Newton, permiten hacer experimentos que se verifican a escala macroscópica; por ejemplo, es posible seguir la trayectoria de una bala de cañón, o de una pelota de baloncesto; pero la física cuántica se ocupa de la mecánica a un nivel que no se puede capturar por los sentidos, como la polarización de un fotón, o el spin de un electrón. Los cambios significativos entre el nivel macroscópico y microscópico han sido objeto de estudio de muchos científicos que invierten sus vidas tratando de descubrir la llamada Gran Teoría Unificada, un grupo de leyes que logre unir la teoría de la relatividad y la mecánica cuántica en una sola.

“La mecánica cuántica es la descripción de movimiento e interacción de partículas en pequeñas escalas donde la naturaleza discreta del mundo físico adquiere importancia” [Wolfram 1]. Y además, constituye una base matemática lo suficientemente firme para desarrollar teorías físicas.

Los fenómenos que describe la física cuántica incluyen, entre otros, la superposición (los sistemas cuánticos pueden estar en diferentes estados a la vez), la dualidad onda-partícula (un estado cuántico evoluciona de acuerdo a una función de onda, al medirse, la función de onda colapsa), el enredo, y el principio de incertidumbre, que se tratarán en el próximo capítulo. Estos fenómenos no pueden ser descritos usando las leyes de la mecánica clásica, y por lo tanto,

necesitan un nuevo marco de trabajo con consideraciones diferentes. La interpretación Copenhagen “es un constructo filosófico que se formuló para brindar un marco de trabajo fundamental para el entendimiento de supuestos, limitaciones, y aplicabilidad de la teoría de la mecánica cuántica” [Wolfram 2]. “Fue establecida por el físico danés Niels Bohr a mediados de la década de 1920, y se convirtió durante muchos años en la visión estándar entre muchos físicos” [Brown 00].

Se basa en los siguientes dos principios:

1) Un sistema cuántico que no ha sido medido existe en un estado genuino de indeterminación. No tiene sentido decir (e incluso puede llevar a contradicciones) que está en un estado específico pero desconocido.

2) El acto de la medición fuerza a adoptar uno de los posibles valores clásicos, con una probabilidad que puede ser calculada del estado cuántico apropiado del sistema y su medición.

La interpretación Copenhagen no hace más fáciles de entender los fenómenos cuánticos, simplemente nos dice que no deberíamos esperar entenderlos de la forma que nos gustaría. Resuelve ciertas dificultades simplemente declarándolas fuera de los límites [Gruska 99].

La Interpretación de los Muchos Mundos, propuesta por el físico Hugh Everett en 1957, y cuyo mayor defensor es el físico David Deutsch (que se refiere a los muchos mundos como el multiverso) es otra manera de entender la mecánica cuántica. “Everett asume que, antes de una medición, todos los posibles resultados coexisten, y después de la medición, todos los posibles resultados de cada medición son preservados en una manera especial, a saber, que cada uno

lleva una existencia separada en su propio mundo o universo. Si una medida adicional en cualquiera de estos mundos lleva a la creación de nuevos mundos, estos son totalmente diferentes que todos los mundos que existían antes [Gruska 99]."

3.1 ACERCAMIENTO HISTÓRICO A LA MECÁNICA CUÁNTICA

A continuación se hará un recorrido histórico a las teorías posteriores a la relatividad de Einstein, para capturar así la esencia de la física cuántica. Si desea profundizar en este tema histórico, puede consultar [Cline 87].

En el año 1900, el físico Max Plank derivó ecuaciones correctas que describían la radiación de cuerpo negro, asumiendo que la materia puede absorber y emitir luz en porciones de $E = h\nu$. Esta idea fue controversial en su época, Plank no entendía por qué las ondas transportaban energía en cantidades discretas (llamadas cuantos). La teoría de Plank no fue tomada en serio hasta que Albert Einstein la llevó más allá en su tesis ganadora del Premio Nóbel sobre el efecto fotoeléctrico, en el que asume que la luz se comporta como partícula, que llamó fotones, y la relación entre la frecuencia de la luz (color) y la energía del fotón era $\nu = E / h$.

En 1913 el físico danés, también ganador del Nóbel, Niels Bohr, propuso que los electrones se mueven en órbita alrededor del núcleo del átomo, y que eso solo puede ocurrir en múltiplos enteros del número $\hbar = h / 2\pi$, así que los únicos valores permitidos del momento angular son $0, \hbar, 2\hbar ...$

En 1923, Louis deBroglie propuso la dualidad onda-partícula: planteó que si la luz (que hasta entonces había sido pensada como un proceso ondulatorio) algunas veces puede comportarse como partícula, entonces partículas como los electrones

tal vez pueden comportarse a veces como ondas. Combinó la ecuación de Plank $E = h\nu$ con la ecuación de Einstein $E = mc^2$ y propuso que cualquier cosa que oscila a una frecuencia ν sólo puede ocurrir en unidades discretas de masa $h\nu / c^2$.

En 1927, Werner Heisenberg descubrió uno de los principios y limitaciones fundamentales de la mecánica cuántica: el principio de incertidumbre de Heisenberg, que se trata en la sección 4.1 del próximo capítulo.

El físico austriaco Erwin Scrödinger se preguntaba si la superposición cuántica era un fenómeno específico de los objetos microscópicos o si también existía en los objetos macroscópicos y no podíamos observarla. De aquí surge su famoso experimento mental conocido como el Gato de Schrödinger, en el que dentro de una caja cerrada y opaca hay: un gato, una partícula radiactiva con un 50% de probabilidades de decaer en una hora, un detector que se activa si la partícula decae, una botella que contiene veneno letal para el gato, y sobre esta, un martillo. El objetivo del ejercicio es averiguar en qué estado está el gato (vivo o muerto) al cabo de una hora. Si la partícula decae (en un evento puramente aleatorio), el detector se activa y suelta el martillo, que cae rompiendo la botella, liberando el veneno, y matando al gato. Si la partícula no decae, el gato sigue vivo. Así que antes de mirar la caja, el gato está en una superposición de dos estados: vivo y muerto. Pero al mirar dentro de la caja, la superposición de estados colapsa en uno de los dos estados posibles. El valor del experimento, y la razón de su popularidad, es que logra plantear una situación que enlaza el mundo cuántico (partícula radiactiva) con el mundo macroscópico (el gato).

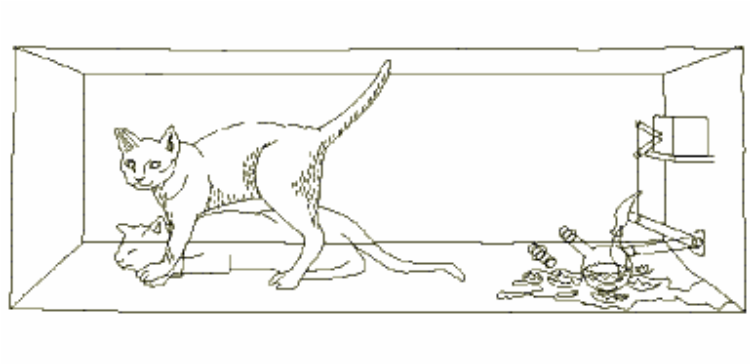


Figura 2: El gato de Schrödinger

En 1926, Scrödinger derivó su famosa ecuación de onda[3] $\psi(x,t)$, que describe la evolución de un sistema cuántico cuando no está siendo observado, y que es:

$$i\hbar\frac{\partial\psi}{\partial t} = -\frac{\hbar^2}{2m}\frac{\partial^2\psi}{\partial x^2} + V\psi$$

"La ecuación de Schrödinger juega un rol lógicamente análogo a la segunda ley de Newton: dadas las condiciones iniciales adecuadas [típicamente $\psi(x,0)$], la ecuación de Schrödinger determina $\psi(x,t)$ para todo el tiempo futuro, así como, en la mecánica clásica, la ley de Newton determina $x(t)$ para todo el tiempo futuro." [Griffiths 04].

[3] El funcionamiento de la ecuación de onda de Schrödinger está por fuera del alcance de esta monografía. Para un estudio profundo del tema, refiérase a [Griffiths 04].

4 CONCEPTOS DE FÍSICA CUÁNTICA USADOS EN CRIPTOGRAFÍA

A continuación se presentarán con más detalle algunos de los conceptos mencionados en el capítulo anterior, y se mencionará la importancia de estos en la criptografía cuántica.

4.1 PRINCIPIO DE INCERTIDUMBRE DE HEISENBERG

En 1927, Werner Heisenberg descubrió un principio fundamental de la mecánica cuántica que lleva su nombre: el principio de incertidumbre de Heisenberg. Dice que ciertos pares de propiedades físicas están relacionados de tal forma que cuando se obtiene información sobre una de ellas, disminuye la información que se puede obtener sobre la otra. Este es el caso de la posición de las partículas y el momentum: cuando se mide la posición con exactitud, esto hace que la medición del momentum tenga menos certeza, y viceversa.

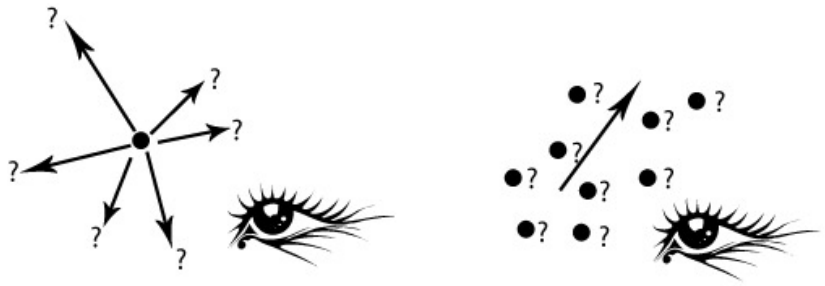


Figura 3: Principio de Incertidumbre de Heisenberg

En el caso específico de la criptografía cuántica, en el que es necesario medir la polarización de los fotones, la elección sobre qué dirección medir afecta todas las

medidas que se realizarán después. A continuación se presenta un ejemplo descrito por Salvatore Vittorio en el artículo *Quantum Cryptography: Privacy Through Uncertainty*, publicado en 2002 [CSA], y que sirve para aclarar el papel del principio de incertidumbre de Heisenberg en la criptografía cuántica: "Si se mide la polarización de un fotón[4] que pasa por medio de un filtro orientado verticalmente, el fotón emerge como verticalmente polarizado a pesar de su dirección inicial de polarización. Si se pone un segundo filtro orientado a un ángulo θ de la vertical, hay cierta probabilidad de que el fotón pasará también por el segundo filtro, y esta probabilidad depende del ángulo θ. Mientras θ incrementa, la probabilidad de que el fotón pase también por el segundo filtro decrementa hasta que llega a 0 en $\theta = 90$ grados (en el caso en que el segundo filtro es horizontal). Cuando θ = 45 grados, la probabilidad de que el fotón pase por el segundo filtro es exactamente ½. Este es el mismo resultado que se obtiene con una secuencia de fotones aleatoriamente polarizados afectados en el segundo filtro, así que se dice que el primer filtro vuelve aleatorias las mediciones del segundo."

En otras palabras, si utilizamos fotones con dos polarizaciones diferentes que formen un ángulo de 90º entre si y al filtrar los fotones se utilizan los filtros adecuados, es decir bien orientados, el fotón pasará si coincide con la polarización del filtro y no pasará si su polarización es ortogonal a la del filtro. Estos eventos son determinísticos y por lo tanto se puede utilizar una polarización para representar el 1 y la otra para representar el 0. Si el filtro que se utiliza no es

[4] La polarización de los fotones se tratará en la sección 4.3

adecuado, es decir no está bien orientado, no sólo el paso del fotón deja de ser determinístico sino que adicionalmente altera la polaridad del mismo.

4.2 ENREDO CUÁNTICO, PARADOJA EPR, Y DESIGUALDAD DE BELL

Albert Einstein creía que la teoría de la física cuántica estaba incompleta, ya que no le permitía obtener predicciones certeras de los resultados de las mediciones. A él no le parecía correcto tener que recurrir a probabilidades, creía que había una pieza faltante y necesitaba algo más profundo, más detallado, unas *variables escondidas que* describían el comportamiento de las partículas, y que al hallarse, permitirían construir una teoría fundamental de la naturaleza. El problema era principalmente el enredo cuántico (cuyos efectos fueron descritos por Einstein como “fantasmagóricas acciones a distancia”). Un par de partículas están enredadas cuando, al crearse juntas, o al haber interactuado en algún momento, mantienen una especie de “conexión” o correlación, de tal forma que al saber el estado de una partícula *inmediatamente* se sabe el estado de la otra. Esto permite que incluso a distancias inmensas, dicho par de partículas interactúe sin limitarse a la velocidad de la luz. La teoría especial de la relatividad dice que ninguna interacción mediada por partículas materiales puede transmitirse más rápido que la velocidad de la luz, lo cual podría explicar por qué este fenómeno era tan inconcebible para Albert Einstein.

Así que en 1935, junto a sus jóvenes ayudantes Boris Poldoski y Nathan Rosen, Einstein propuso un experimento mental que imaginaba mediciones simultáneas de momentum y posición en pares correlacionados de partículas, y lo llamaron “La Paradoja EPR”. Como ya se mencionó, el principio de incertidumbre de Heisenberg dice que sólo es posible conocer el momentum o la posición de una

partícula, pero no ambos. La paradoja entonces plantea que si dos partículas están enredadas, por ejemplo A y B, se podría medir la posición de la partícula A, con lo que también se sabría la posición de la partícula B. Y si al mismo tiempo se mide el momentum en B, entonces también se sabría el momentum en A, y se tendría información completa sobre la partícula, incumpliendo con el principio de incertidumbre de Heisenberg, y creando así la paradoja. Pero "Bohr y sus seguidores argumentaron en contra que las dos partículas formaban un sistema cuántico inseparable, y que al discutir las circunstancias de una, no se podrían ignorar las mediciones realizadas a la otra" [Brown 00].

En 1954, John Bell publicó unas expresiones matemáticas conocidas como la Desigualdad de Bell, a las que el físico Henry Stapp calificó como: "el descubrimiento más profundo de la ciencia" [Williams y Clearwater 98]. La desigualdad de Bell establece un límite en la cantidad de correlación esperada entre dos partículas que interactuaron tomando como punto de partida tres supuestos: i) Lo lógica es válida. ii) Existen variables ocultas y iii) las variables ocultas son locales [Harrison 99]. Este límite ha sido violado en múltiples experimentos[5] luego alguno de los supuestos es falso. Dados los supuestos con los que se construyó la desigualdad, esto "… implica que no hay teorías de variables escondidas locales para la mecánica cuántica. ¡La realidad en verdad es fantasmagórica! [...] El hecho de que dos partículas se separen físicamente no

[5] En 1982, el experimento de Aspect, Dalibard y Roger, violó la desigualdad de Bell usando un sistema de dos fotones correlacionados. En febrero de 1995, Pan, Bouwmeester, Daniell, Weinfurter, y Zeilinger, reportaron una observación de no-localidad cuántica en un experimento de tres fotones, y hasta la fecha se han realizado experimentos de enredo cuántico de hasta cuatro fotones.

implica que sus estados dejen de estar correlacionados. La correlación EPR es una interacción latente que entra en juego cuando se hacen las mediciones. O abandonamos nuestra noción de localidad o abandonamos nuestra noción de correlaciones probabilísticas. En términos de los ángulos de los polarizadores, la desigualdad de Bell puede expresarse como:

$$\frac{1}{2}\sin^2(\theta_2-\theta_1)+\frac{1}{2}\sin^2(\theta_3-\theta_2)-\frac{1}{2}\sin^2(\theta_3-\theta_1)\geq 0$$

Si la realidad es local, esta desigualdad siempre debería ser cierta sin importar los ángulos en los que se configuran los polarizadores. Por lo tanto, la superficie generada por la fórmula debería ser siempre mayor o igual a cero. Si cualquier valor es menor que cero, esto muestra que la física es no-local" [Williams y Clearwater 98].

En la siguiente figura se puede observar cómo, con diferentes configuraciones, se obtienen resultados negativos para la desigualdad, demostrando teóricamente los valores para los cuales se produce una violación a la desigualdad de Bell.

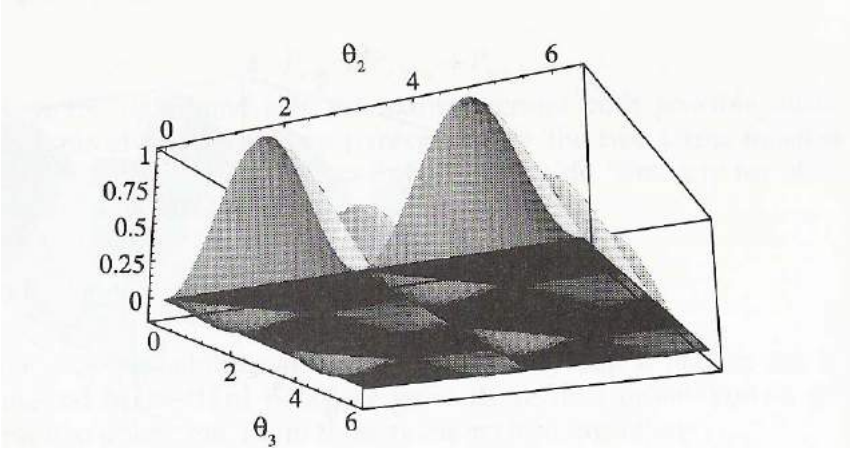


Figura 4: La desigualdad de Bell se viola con ciertas configuraciones de los polarizadores [Williams y Clearwater 98].

El enredo cuántico es la base del protocolo EPR para criptografía cuántica, y también de la construcción de repetidores cuánticos, que se mencionarán en el próximo capítulo.

4.3 POLARIZACIÓN DE UN FOTÓN

Los fotones parecen ser el mejor medio para transportar información cuántica en grandes distancias [Brukner 02]. Son partículas sin masa, que se mueven a la velocidad de la luz, y que no tienen carga eléctrica. Además se producen y se detectan fácilmente, y la transmisión por fibra óptica de los fotones con una longitud de onda específica es lo suficientemente confiable como para aplicaciones prácticas.

”Los fotones son ’ondas electromagnéticas transversales’. Esto significa que los campos eléctrico y magnético son perpendiculares a la dirección en la que se propagan. Además, los campos eléctrico y magnético son perpendiculares entre ellos. Entonces, en el sistema de coordenadas tridimensional de ejes x, y y z, si un fotón se propaga en la dirección z, los campos eléctrico y magnético oscilan en los planos xz y yz respectivamente.” [Williams y Clearwater 98]

Una de las propiedades de los fotones de las que se vale la criptografía cuántica para codificar un bit es la polarización, que se refiere al plano en el que oscila el campo eléctrico mientras el fotón se propaga. En la polarización lineal, el campo eléctrico del fotón se mantiene en el mismo plano, en cambio en la polarización circular, la luz del campo eléctrico rota a cierta frecuencia mientras el fotón se

propaga. La criptografía cuántica puede implementarse con cualquiera de estos dos casos, o con una combinación de ellos.

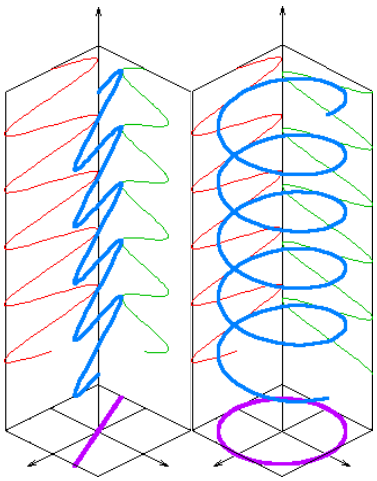


Figura 5: Polarización lineal y circular de un fotón

Los fotones atraviesan un polarizador, y así se obtienen diferentes polarizaciones que representan estados cuánticos, y a partir de ahí se puede hacer una correlación a bits. El funcionamiento del polarizador se explica con más detalle en el siguiente capítulo, para el protocolo BB84.

4.4 QUBITS

La computación cuántica opera con qubits, que para efectos prácticos en criptografía pueden pensarse como estados de polarización de un fotón. La correlación es la siguiente:

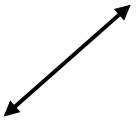
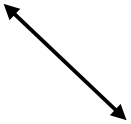
	Polarización rectilínea	Polarización diagonal
Estado $\|0\rangle$ Fotón polarizado en 0° o 45°		
Estado $\|1\rangle$ Fotón polarizado en 90° o 135°		

Figura 6: Estados de polarización de un fotón

El término qubit fue acuñado por Benjamín Schumacher a principios de los 90s y de acuerdo con la notación de Dirac, el estado $|\phi\rangle$ se pronuncia "ket ϕ". Matemáticamente, "un qubit (bit cuántico) es un estado cuántico $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ donde $\alpha, \beta \in \mathbb{C}$ y $|\alpha|^2 + |\beta|^2 = 1$"[Gruska 99]. Al hacer la medición del qubit, se obtiene $|0\rangle$ con probabilidad $|\alpha|^2$ y $|1\rangle$ con probabilidad $|\beta|^2$. Los factores α y β se llaman amplitudes de probabilidad, y son importantes para la criptografía cuántica porque con ellos se crean todos los ángulos de polarización diferentes a

45 grados (que se crea con la suma de $|0\rangle + |1\rangle$[6], luz polarizada a medio camino entre el horizontal y el vertical).

En la teoría de la información cuántica, un qubit $|\phi\rangle$ puede estar en los dos estados básicos computacionales $|0\rangle$ y $|1\rangle$, que usualmente se toman como los valores de bits clásicos 0 y 1. Pero además, puede estar en un estado de superposición, es decir en $|0\rangle$ y $|1\rangle$ al mismo tiempo, hasta que es medido y colapsa en uno de ellos.

Se denominan Estados Puros aquellos estados de los que se puede obtener el máximo conocimiento, no pudiéndose obtener un conocimiento total debido al principio de incertidumbre de Heisenberg mencionado anteriormente. Los Estados Mixtos son entonces aquellos estados de los que se puede obtener muy poco conocimiento.

4.5 TEOREMA DE NO-CLONACIÓN

El teorema de no-clonación, cuya prueba (realizada por William Wooters y Wojciech Zurek) fue publicada en la revista Nature en 1982, significó un avance fundamental para el desarrollo tanto de la teoría de información cuántica como de la criptografía cuántica. Si fuera posible para un espía copiar los estados cuánticos

---

[6] En sentido estricto, debe ser $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ para garantizar que la probabilidad $|\alpha|^2$ y $|\beta|^2$ sean válidas.

mientras viajan del emisor al receptor, la criptografía cuántica no tendría sentido. A continuación se explica matemáticamente el teorema de no-clonación, como se encuentra en el libro Quantum Computation and Quantum Information [Nielsen y Chuang 00], página 532:

> **Teorema**: Se tiene una máquina cuántica con dos ranuras etiquetadas A y B. La ranura A, ranura de datos, inicia en un estado cuántico desconocido pero puro, $|\psi\rangle$. Este es el estado que se copia en la ranura B, o ranura objetivo. Se asume que la ranura objetivo inicia en algún estado puro, $|s\rangle$. Entonces el estado inicial de la máquina copiadora es $|\psi\rangle \otimes |s\rangle$. Alguna evolución unitaria[7] U efectúa ahora el procedimiento de copia, idealmente,
>
> $$|\psi\rangle \otimes |s\rangle \xrightarrow{U} \left(|\psi\rangle \otimes |s\rangle\right) = |\psi\rangle \otimes |\psi\rangle$$
>
> Si se supone que este procedimiento de copia funciona para dos estados particulares puros $|\psi\rangle$, y $|\varphi\rangle$ entonces se tiene:
>
> $$U\left(|\psi\rangle \otimes |s\rangle\right) = |\psi\rangle \otimes |\psi\rangle$$
> $$U\left(|\varphi\rangle \otimes |s\rangle\right) = |\varphi\rangle \otimes |\varphi\rangle$$

---

[7] La evolución de un sistema cuántico se describe por la ecuación lineal de Schrödinger, cuyo tratamiento está por fuera del alcance de esta monografía. Para entender cómo funciona esta ecuación, podrá encontrar información detallada en [Griffiths 04].

Tomando el producto interno de estas dos ecuaciones da como resultado

$$\langle\psi|\varphi\rangle = \left(\langle\psi|\varphi\rangle\right)^2$$

Pero $x = x^2$ sólo tiene dos soluciones, $x = 0$ y $x = 1$, entonces, ó $|\psi\rangle = |\varphi\rangle$ ó $|\psi\rangle$ y $|\varphi\rangle$ son ortogonales. Es decir que el dispositivo de clonación sólo puede clonar estados ortogonales, y por eso la clonación cuántica general es imposible.

Ya que es posible copiar estados ortogonales, al desarrollar un protocolo criptográfico es importante que el emisor tenga en cuenta que los estados cuánticos que prepara para enviar deben ser no-ortogonales. En otras palabras, se deben tener en cuenta las mismas consideraciones que se tiene en la criptografía clásica para evitar claves débiles. Las excepciones, como el protocolo EPR donde se requieren estados ortogonales, deben demostrar que no son vulnerables a estos procesos de copia.

5 COMPUTACIÓN CUÁNTICA

Los computadores clásicos son sistemas físicos y esto tiene implicaciones de espacio, tiempo y energía. Cada vez se incrementa la demanda por computadores más rápidos, pero para que esto suceda es necesario controlar el calor que se genera en los procesos computacionales, reducir el tamaño de los componentes y hacer que estén más cerca entre ellos (porque las señales dentro del computador no pueden viajar más rápido que la velocidad de la luz). “Mientras los dispositivos de computación siguen miniaturizándose, se acerca rápidamente al nivel microscópico, en el que dominan las leyes del mundo cuántico [...] Alrededor del año 2020, la computación se llevaría a cabo en el nivel atómico” [Gruska 99].

Con la llegada de la teoría cuántica y algunas de sus propiedades, como superposición y enredo cuántico (que se mencionarán en el siguiente capítulo), se predijo que los computadores cuánticos, definidos como “un tipo de computador que explota las interacciones de la mecánica cuántica” [Gershenfeld y Chuang 98], podrían desarrollar ciertas tareas computacionales exponencialmente más rápido que cualquier computador convencional. Dichas predicciones van de la mano con los desarrollos de algoritmos cuánticos, que desde una base teórica, aprovechan las características de la teoría cuántica. “Factorizar un número de 400 dígitos –una hazaña numérica necesaria para romper algunos códigos de seguridad– le tomaría billones de años incluso al supercomputador más rápido. Pero un computador cuántico podría completar la tarea en más o menos un año” [Gershenfeld y Chuang 98].

Dos de los algoritmos cuánticos más estudiados son: el algoritmo para encontrar orden y el algoritmo para factorizar. Ambos se basan en el procedimiento de estimación de fase, que a su vez se basa en la Transformada de Fourier Cuántica[8]. El problema de factorización resulta ser equivalente al problema de encontrar orden, ya que un algoritmo rápido para encontrar orden puede convertirse en un algoritmo rápido para factorizar [Nielsen y Chuang 00].

El algoritmo para factorizar fue propuesto en 1994 por Peter Shor en los laboratorios Bell de AT&T, y mostró cómo un computador cuántico puede calcular los factores y divisores de números muy grandes en un tiempo muy corto. Este algoritmo tuvo dos consecuencias importantes: probó que el RSA –qué, como se mencionó en el Capítulo I, se basa en la complejidad algorítmica de la factorización de enteros muy grandes–, sería vulnerable en el momento en que se construyera el primer computador cuántico; y comprobó el paralelismo cuántico, que según el físico David Deutsch (acreditado como "el padre de la computación cuántica" [Wired 07]), demostraba la realidad de los universos paralelos y su infinito potencial para el procesamiento de información. "Para Deutsch, la única respuesta coherente a la pregunta ¿dónde se lleva a cabo la factorización? es que diferentes partes del cálculo se llevan a cabo en diferentes universos" [Brown 00].

Aunque la mayoría de los avances en el área hayan sido a nivel teórico, el algoritmo de Shor alertó a organizaciones de seguridad y agencias de inteligencia para que se tomaran en serio el desarrollo de sistemas de criptografía cuántica,

[8] Para más información sobre estos algoritmos y procedimientos, refiérase a [Nielsen y Chuang 00].

fue rápidamente reconocido como la *killer app* de la computación cuántica, e incrementó la investigación en el área.

En la actualidad, para considerarse una nueva tecnología (sin entrar a las dificultades físicas de elección de los mejores materiales para un sistema cuántico), la computación cuántica aún se enfrenta a grandes dificultades como: adecuadas correcciones de error, que necesitan un aumento considerable de qubits en el sistema (de 100 a 200 qubits lógicos, y 1000 o más qubits físicos, según David Deutsch [Wired 07]); mejoras en la medición para evitar perder información en los valores de los qubits; un entendimiento más profundo de los mecanismos involucrados en el enredo cuántico, y una adecuada gestión para la interacción con el ambiente.

En general, el objetivo de la computación cuántica de utilizar mecanismos naturales para realizar operaciones con datos va más allá de un procesamiento más rápido, o un dispositivo más pequeño. Para los investigadores esto puede hacer parte de un entendimiento más profundo sobre la realidad. “Estamos *hackeando* el universo” dice el investigador del MIT Seth Lloyd, quién realizó el primer diseño factible de un computador cuántico. “No podríamos construir computadores cuánticos si el universo no fuera cuántico y no computara. Pero podemos hacerlo, porque el universo guarda y procesa información a nivel cuántico. O sea que, en sí mismo, el universo es un gran computador cuántico” [Lloyd 07].

6 CRIPTOGRAFÍA CUÁNTICA

Antes de iniciar este capítulo es importante hacer énfasis en la dualidad conceptual que existe entre los investigadores del fenómeno cuántico. Debido a que las propiedades de la física cuántica mencionadas en el capítulo II, físicos como David Deutsch creen que la única forma de entender completamente la naturaleza es aceptar la existencia de un número ilimitado de universos paralelos. Otros físicos no creen esta idea, y prefieren trabajar sobre el Espacio de Hilbert, un espacio matemático abstracto que contiene todos los posibles estados cuánticos[9]. Sin embargo, el tratamiento de estas abstracciones está fuera del alcance de esta monografía, y no se incluirá en la explicación de los protocolos de la criptografía cuántica.

A continuación se presentará un recorrido general a los desarrollos en este campo. Si desea profundizar en los temas, puede consultar los libros: [Chuang y Nielsen 00], [Brown 00], [Williams y Clearwater 98] y [Gruska 99]. También en la bibliografía podrá encontrar más referencias al tema.

6.1 LOS EXPERIMENTOS MENTALES

Las raíces de la criptografía cuántica inician en la Universidad de Columbia, a finales de 1960, con la idea de Stephen Wiesner para construir billetes que fueran imposibles de falsificar, y con la propuesta de enviar a través de un canal cuántico dos mensajes clásicos, para que el receptor sólo pudiera extraer uno de ellos;

[9] Mayor información sobre los espacios de hilbert en [Wolfram 3].

aunque quiso publicar un *paper* en 1970, sus ideas eran tan extrañas para la época que no lo tomaron en serio hasta 1983, y su publicación inspiró a otros autores a desarrollar teorías sobre el tema.

En el mundo de la criptografía cuántica es bien conocida la anécdota en la que Gilles Brassard, experto en criptografía de la Universidad de Montreal, y Charles Bennett de IBM, se conocieron nadando por casualidad en el mar de Puerto Rico, y empezaron a hablar sobre esas ideas "locas" de Wiesner. Ambos siguieron encontrándose, compartiendo nuevas ideas y considerando sus implicaciones, hasta concluir que no era necesario usar mecánica cuántica para almacenar información sino para, usando las propiedades de los fotones, transmitir información. Una de sus ideas más fuertes era la aplicación de la mecánica cuántica a la criptografía de clave pública, y para esto desarrollaron el protocolo BB84 (Brassard-Bennett-1984), para implementar un sistema de distribución de clave cuántica. Dicho protocolo se explicará posteriormente.

En 1990 Artur Ekert de la universidad de Oxford propuso un sistema de criptografía muy relacionado con el famoso experimento EPR propuesto en 1935 por Einstein, Podolsky y Rosen, usando las propiedades del enredo cuántico, que podría definirse como un estado donde dos objetos pueden tratarse como uno incluso cuando están separados físicamente, lo que significa que un cambio en uno instantáneamente afecta al otro [Dornan 04].

6.2 DE LA TEORÍA A LA PRÁCTICA

Fue hasta 1989 que las ideas de Brassard y Bennett (que en un principio, incluso para ellos, eran consideradas como ciencia ficción, o experimentos mentales) tuvieron su primera aplicación práctica en un canal de 30 centímetros, a través de un prototipo desarrollado por el centro de investigaciones de IBM. Cinco años

después (1994), Paul Towersend y Christophe Marand de los laboratorios de investigación de Telecom en Inglaterra usaron una modificación del protocolo BB84 para demostrar la primera distribución real de claves cuánticas a amplio rango, 30 kilómetros, pero distribuidos en la misma habitación. Luego, en 1997, un equipo de la Universidad de Geneva fue el primero en demostrar un sistema en el que el emisor y el receptor estaban *realmente* separados, a una distancia de 23 kms. La señal se transmitió por medio de un cable de fibra óptica extendido bajo el lago Geneva, junto con una técnica muy óptima para cancelación de ruido o errores. Dos años después (1999), Richard Hughes y su equipo del departamento de física en el Laboratorio Nacional Alamos aumentaron el rango de esta distribución de claves cuánticas a 48 kilómetros [Brown 00]. El más reciente experimento, realizado en marzo de 2007 por el mismo laboratorio, logró aumentar la distancia a 148.7 kilómetros [Nikbin 06].

Todos los anteriores sistemas están limitados a un espacio geográfico pequeño. No se podría construir una red global para distribuir claves cuánticas basándose en dichos sistemas, ya que en el momento en que el dispositivo (repetidor) que restaura las señales debilitadas entre en contacto con la señal, la modifica y corrompe los datos. Así que los repetidores tradicionales no funcionarían en este tipo de redes. Para solucionar este problema los investigadores han encontrado tres alternativas: una es que se establezcan diferentes claves, configuradas en cada estación del repetidor, de tal forma que el emisor y el receptor vayan estableciendo claves cuánticas distintas mientras recorren la distancia. El problema es que esto estimularía la imaginación de espías que podrían vulnerar la estación del repetidor, e interceptar el momento en que se traduce clásicamente la información de un código de encriptación a otro, así que no valdría la pena esforzarse mucho por este lado [Brown 00].

La segunda alternativa es transmitir fotones por el aire o el espacio en vez de usar cables de fibra óptica. Muchos experimentos de este tipo han sido en las

montañas, donde la altitud reduce al mínimo la turbulencia atmosférica. En el año 2002, en el laboratorio Nacional de Los Alamos, se estableció un enlace de 10 kilómetros por el aire. El mismo año, QinetiQ en Farnborough, y la Universidad Ludwing Maximilian de Munich, establecieron un enlace de 23 kilómetros entre dos cimas de los Alpes meridionales. Se decía que con los telescopios mayores, filtros adecuados y recubrimientos antirreflectantes era posible llegar a una red satelital en órbita terrestre que permitiera una cobertura mundial [Stix 05]. En 2007, un equipo europeo de físicos hizo una distribución de clave cuántica segura entre dos de las Islas Canarias. La transmisión fue hecha por el aire, entre telescopios separados a 144 kilómetros [Savage 07].

La tercera alternativa es la construcción de repetidores cuánticos, que se basaría en la construcción de circuitos cuánticos lógicos, una especie de computador cuántico elemental que explotaría los efectos no locales de las partículas enredadas. En 2004, un equipo del Instituto de Física Experimental de Viena dirigido por Anton Zeilinger informó que habían extendido bajo el Danubio por un conducto del alcantarillado un cable de fibra óptica con un fotón enredado en cada extremo. La conexión entre ambos fotones *teleportó* la información de un tercer fotón al otro lado del Danubio a 600 metros de distancia. Pero para que la idea de los repetidores sea válida a gran escala (a nivel global), se necesitaría construir unas memorias cuánticas que almacenen los qubits sin corromperlos antes de enviarlos al enlace siguiente, y la construcción de estos dispositivos, hasta la fecha, aún está en su infancia [Stix 05].

6.3 DISTRIBUCIÓN DE CLAVES CUÁNTICAS (QKD)

En este contexto sería más apropiado decir Generación de Claves Cuánticas que Distribución de Claves Cuánticas, ya que el proceso ocurre entre el emisor y el receptor conjuntamente y ninguno de ellos puede predeterminar la clave que se

generará al completar el protocolo. Sin embargo se hablará de Distribución de Claves Cuánticas porque es el nombre más común en el área de la criptografía.

En el proceso de generación de clave cuántica se deben cumplir las siguientes condiciones:

1) Ningún intruso puede obtener la clave transmitida.

2) Cualquier intento de intromisión para obtener la clave transmitida puede ser detectado con alta probabilidad.

3) Los usuarios pueden estar seguros de que están compartiendo la misma clave [Gruska 99].

A continuación se analiza detalladamente el protocolo BB84, y luego se mencionan los protocolos B92, y EPR.

6.3.1 El protocolo BB84

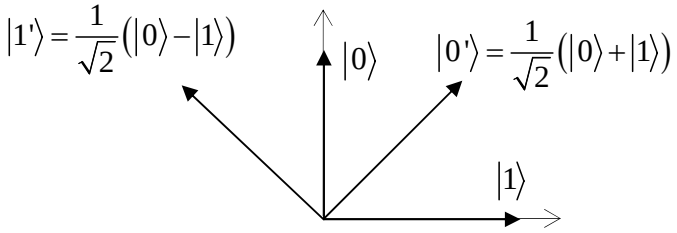


Figura 7: Gráfica para representar la polarización de fotones en el protocolo BB84

El esquema propuesto en 1984 por Brassard y Bennett implica el envío de fotones preparados en diferentes estados de polarización. Usando un filtro de polarización, se selecciona el ángulo de polarización con respecto a la horizontal. También se puede usar un método más sofisticado, en el que se usa un aparato conocido como *Pockels cell* que hace posible que el campo eléctrico del fotón oscile en el plano deseado. Como se vio anteriormente, se pueden elegir cuatro ángulos en particular: 0, 45, 90, y 135 grados, (↔ ↗ ↕ ↖). Los fotones polarizados en ángulos de 0 y 45 representan el valor binario 0, y los fotones polarizados en ángulos de 90 y 135 representan el valor binario 1; una vez hecha esta correspondencia, una secuencia de bits puede ser convertida en una secuencia de fotones polarizados.

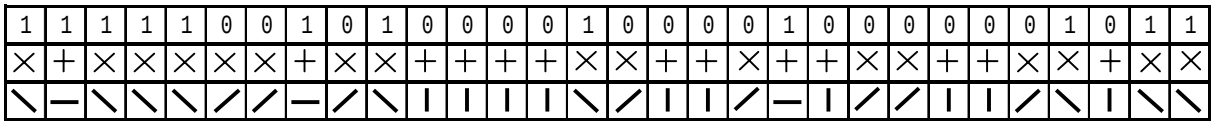


Figura 8: Alicia codifica bits como fotones polarizados. La primera fila indica la secuencia de bits. La segunda indica la orientación usada por el filtro. La tercera indica el resultado de la polarización.

Para explicar cómo se intercambia una clave secreta, y usando la notación convencional en criptografía, se llamará al emisor Alicia, al receptor Bob, y al espía, Eva. Primero, Alicia genera una secuencia de fotones cuyas polarizaciones elige aleatoriamente de una de las cuatro anteriores. Cuando Bob recibe los fotones, decide aleatoriamente si medir las polarizaciones a lo largo de las direcciones rectilíneas (horizontal/vertical) o a lo largo de las diagonales. Esto se puede hacer usando un cristal de calcita o carbonato de calcio ($CaCO_3$), que tiene la propiedad de birrefringencia, esto significa que los electrones en el cristal no

son afectados por la misma fuerza en cada dirección. De esta forma, un fotón que pasa por el cristal sentirá una fuerza electromagnética diferente dependiendo de la orientación de su campo eléctrico relativa al eje de polarización del cristal. Es decir, los fotones que llegan se separan en dos caminos de acuerdo a su estado de polarización.

Intuitivamente, es posible que Bob discrimine con certeza sólo entre estados perpendiculares (es decir, ortogonales) y sólo si tiene su aparato de medición orientado correctamente. Si Alicia envía un flujo de fotones polarizados sólo diagonalmente, y Bob configura su receptor para distinguir polarizaciones rectilíneas, cada fotón tendría un 50% de probabilidad de tomar la ruta horizontal y un 50% de probabilidad de tomar la ruta vertical. El camino para cualquier fotón en particular sería completamente aleatorio y no permite determinar si Alicia envío un 1 o un 0. Lo mismo ocurriría en el caso inverso, cuando Alicia utiliza polarización rectilínea y Bob polarización diagonal. Pero si la polarización utilizada por Alicia y Bob es la misma, entonces podría distinguir las dos polarizaciones con 100% de exactitud, asumiendo que tiene un detector y cristal perfectos. De esta forma Bob podría extraer un bit de información por cada fotón [Brown 00].

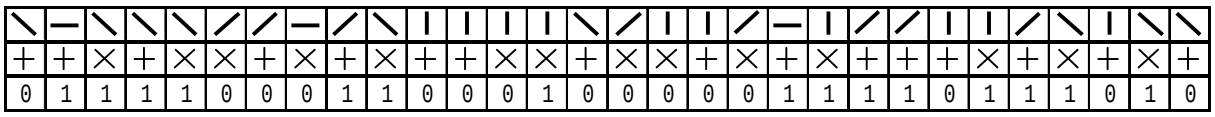


Figura 9: Bob decodifica fotones polarizados como bits. La primera fila indica la secuencia de fotones recibida. La segunda fila indica la configuración del cristal de calcita de Bob. La tercera fila indica el resultado de la medición.

Este comportamiento se explica por el principio de incertidumbre de Heisenberg explicado en el Capítulo III. Si se hace un tipo incorrecto de medición en una partícula, se modifica su estado cuántico, haciendo que sea imposible recuperar la

información. Cuando Alicia envía dos fotones, el primero polarizado verticalmente y el segundo horizontalmente, si Bob tiene su cristal orientado para detectar polarizaciones rectilíneas, verá un fotón irse por el primer camino, y el otro por el segundo camino. Pero si Bob tuviera su cristal configurado para detectar polarizaciones diagonales, aunque ve dos fotones, no hay forma de encontrar el estado original. Más aún, los dos fotones que ve Bob pueden tomar el mismo camino aunque los fotones originales tenían diferente polarización. El principio de incertidumbre se encarga de que el mismo acto de medición perturbe el estado del sistema que Bob está tratando de medir.

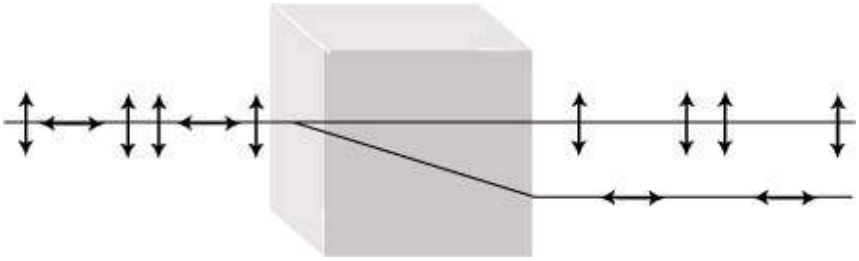


Figura 10: Cristal de Calcita que separa fotones de diferente polarización

En el protocolo BB84, Alicia y Bob eligen entre polarizaciones rectilíneas y diagonales de manera aleatoria. Una vez Alicia ha enviado su secuencia inicial de fotones por un canal cuántico (“un medio de transmisión que aísla el estado cuántico de las interacciones con el ambiente”, [Gruska 99]), para probar la seguridad del canal, Bob le comunica a Alicia por medio de un canal público qué tipo de polarización usó para un subgrupo de dicha secuencia; si rectilíneo o diagonal. Luego Alicia le comunica a Bob qué tipo de polarización usó. Para los casos en los que usaron el mismo tipo de polarizaciones, Alicia le dice a Bob el valor de los bits que debió haber medido, y la verificación debe asegurar que los

bits de Bob concuerdan al 100% con los de Alicia. Y luego este subgrupo de bits de prueba se desecha; es decir, no serán parte de la clave.

Esta aproximación no garantiza la detección de un intruso, pero si se diseña adecuadamente el procedimiento se puede obtener un alto nivel de certeza. “Mientras más bits se prueben, es más probable que se detecte algún espía potencial. De hecho, para cada bit probado por Alicia y Bob, la probabilidad de que esta prueba revele la presencia de un espía que está presente es ¼. Entonces, si se prueban *N* bits, la probabilidad de detectar un espía que esté presente es $1-\left(\frac{3}{4}\right)^N$ ” [Williams y Clearwater 98].

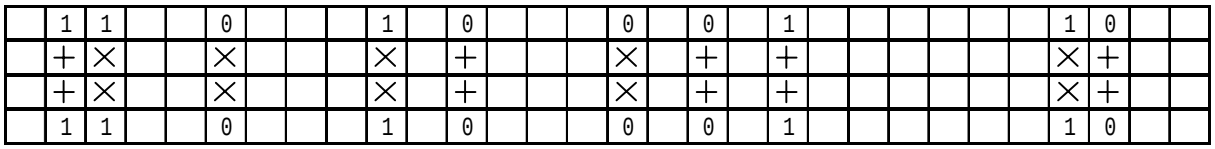


Figura 11: Alicia y Bob comparan un subgrupo de bits para probar, y verificar la presencia de un espía. En todos los bits se usó la misma orientación para polarizar y medir, y el valor del bit es igual, mostrando que no hay un espía presente.

Una vez se sabe que el canal es seguro, Alicia y Bob comparten entre sí la orientación de polarización que usaron para cada uno de los bits que no fueron desechados, pero no se dicen el resultado de la medición. Aquellos bits para los que usaron la misma orientación de polarización constituyen la clave para cifrar los mensajes.

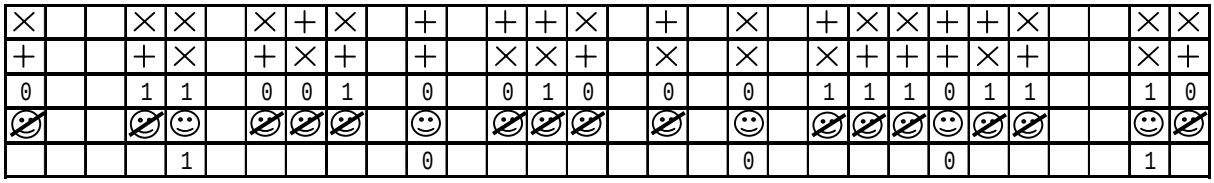
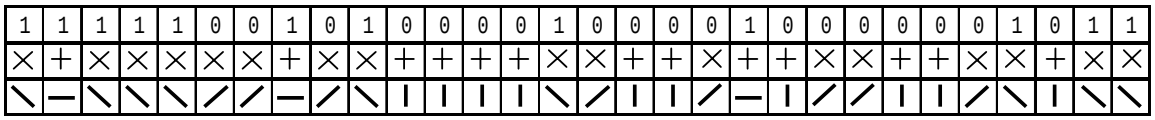


Figura 12: Clave generada. Los casos en que la orientación del polarizador es igual a la orientación del cristal, se representan por ☺, y esto significa que el bit se tomó como parte de la clave.

¿Qué ocurre con este protocolo si Eva se las arreglara para medir las polarizaciones de los fotones mientras están en camino desde donde Alicia hasta donde Bob? En este caso, para que Eva pueda medir los fotones interceptados, debe haber escogido una orientación de polarización. Si Eva quisiera tener certeza de no ser detectada, necesitaría correr la suerte de escoger para cada bit transmitido la misma orientación de polarización que Alicia, lo cual, si el tamaño de la clave es lo suficientemente largo, sería prácticamente imposible. Si Eva elige la orientación incorrecta, modificará la polarización del fotón y su presencia podrá ser detectada en la fase de prueba. A continuación se ilustra paso a paso el protocolo BB84 en el caso de la presencia de Eva.

1) Codificación de los bits de Alicia a estados de polarización:



2) Intercepción y medición de Eva (en los casos en que la configuración de sus polarizaciones no es igual a la de Alicia, Eva modifica irreparablemente el estado original):

↘	—	↘	↘	↘	↗	↗	—	↗	↘	|	|	|	|	↘	↗	|	|	↗	—	|	↗	↗	|	|	↗	↘	|	↘	↘
+	+	×	+	×	+	+	×	×	+	+	+	×	+	+	×	+	×	+	×	×	×	+	×	×	+	×	+	×	+
0	1	1	1	1	0	0	1	0	0	0	0	1	0	0	0	0	0	1	1	1	0	1	1	0	0	1	0	1	0

3) Bob, aún sin estar consciente de la presencia de Eva, realiza sus mediciones:

|	—	↘	—	↘	|	|	↘	↗	|	|	|	↘	|	|	↗	|	↗	—	↘	↘	↗	—	↘	↗	|	↘	|	↘	|
+	+	×	+	×	×	+	×	+	×	+	+	×	×	+	×	×	+	×	+	×	+	+	+	×	+	×	+	×	+
0	1	1	1	1	1	0	1	1	1	0	0	1	0	0	0	0	0	1	1	1	1	1	0	0	0	1	0	1	0

4) Pero en la fase de prueba, Alicia y Bob detectan la presencia de Eva. En este caso, la inconsistencia se detecta solo en un bit (en la tercera columna de la prueba), y deciden desechar toda la secuencia de fotones para empezar de nuevo el procedimiento.

		1		1	0				1	0	0				0				1				0				0		
		×		×	×				×	+	+				×				+				+				+		
		×		×	×				×	+	+				×				+				+				+		
		1		1	1				1	0	0				0				1				0				0		

En la descripción de este esquema, Bennett y Brassard discutieron dos tipos diferentes de canales de comunicación que serían requeridos entre Alicia y Bob. Uno es el canal cuántico, mencionado anteriormente, que transporta los fotones polarizados (qubits), y el otro es un canal convencional clásico (o canal público), como un cable telefónico, que transportaría todas las conversaciones en las que Alicia y Bob discuten las mediciones que han hecho y los datos que quieren comparar. Estas conversaciones pueden ser públicas, porque ninguna de esa información revelará los contenidos de los qubits intercambiados a lo largo del canal cuántico, aparte de los qubits sacrificados que se usan para comprobar la integridad del canal cuántico [Brown 00].

6.3.2 El protocolo B92

El protocolo B92 es llamado el “protocolo mínimo” para generación de claves cuánticas [Gruska 99]. Fue publicado por Bennett en 1992, y es muy usado experimentalmente debido a su simplicidad.

Este protocolo es muy similar al BB84, pero en este, Alicia sólo usa dos direcciones no-ortogonales entre sí para polarizar su secuencia de fotones aleatoriamente: 90° que corresponde a $|0\rangle$ y 135° que corresponde a $|1'\rangle$. Cuando los fotones son recibidos por Bob, él hace la medición orientando su cristal aleatoriamente en 0° que corresponde a $|1\rangle$ y 45° que corresponde a $|0'\rangle$.

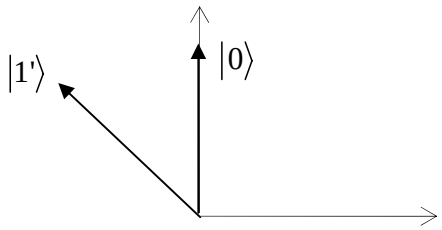
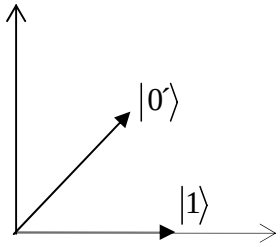


Figura 13: a) Gráfica para representar la polarización de fotones que usa Alicia en el protocolo B92.



b) Gráfica para representar la orientación del cristal que usa Bob para las mediciones en el protocolo B92

La idea en la que se basa el protocolo es que si Alicia envía un fotón con una polarización cualquiera y ese fotón cruza el filtro para detección, entonces se puede afirmar que el filtro de detección y el filtro de envío no son ortogonales entre

sí. Si Alicia había polarizado el fotón en $|0\rangle$, y Bob lo mide utilizando un filtro polarizado en dirección $|0'\rangle$, el fotón tiene ½ de probabilidad de pasar por el cristal. Lo mismo ocurre si Alicia polariza el fotón en $|1'\rangle$ y Bob realiza la medición en $|1\rangle$. Por otro lado, si Alicia polarizó el fotón en $|0\rangle$ y Bob lo mide en $|1'\rangle$, o si Alicia polarizó el fotón en $|1'\rangle$ y Bob lo mide en $|0'\rangle$, estos fotones no pasarán por el cristal y por lo tanto, no serán registrados por Bob.

En la siguiente tabla, se puede observar un resumen de lo anterior:

Codificación de Alicia	Medición de Bob	Resultado de la medición	Probabilidad
$\|0\rangle$	$\|0'\rangle$	Pasa / No pasa	1/2
$\|0\rangle$	$\|1\rangle$	No pasa	1
$\|1'\rangle$	$\|0'\rangle$	No pasa	1
$\|1'\rangle$	$\|1\rangle$	Pasa / No pasa	1/2

Al finalizar la secuencia, Bob le dice a Alicia las posiciones de los fotones que pasaron por el cristal (pero no el valor de las mediciones), y la correlación de estas con los bits será la clave que usarán para cifrar los mensajes.

A continuación se muestra un ejemplo de clave generada por el protocolo B92. En la primera fila está la secuencia de bits generada por Alicia. En la segunda fila está la polarización de dichos bits. En la tercera fila está la orientación del cristal de Bob con el que realiza la medición. En la cuarta fila están los fotones que pasan por el cristal. Y en la quinta fila está la correlación de los fotones a la secuencia de bits que conforma la clave. Por efectos de facilitar la visualización del protocolo, se asume que todos los fotones que tenían la probabilidad ½ de pasar, lo hicieron.

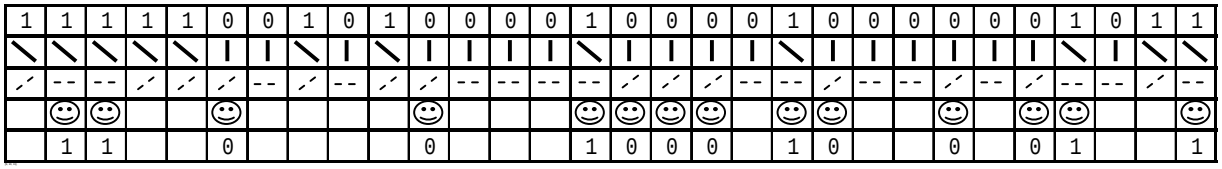


Figura 14: Generación de clave con el protocolo B92.

Mientras que en el protocolo BB84 se desechaba ½ de los bits, en éste se desechan ¾ (la mitad por las orientaciones, y la mitad de los que quedan, por la probabilidad del 50% de que pasen), así que la clave estará formada por ¼ de los bits transmitidos, por lo que se requiere enviar muchos más fotones en este protocolo que en el BB84 para lograr una clave de la misma longitud.

6.3.3 El Protocolo EPR

También es llamado el protocolo E91 (ya que fue propuesto por Ekert en 1991), este protocolo involucra las propiedades del enredo cuántico en la generación de la clave. Es importante resaltar que en este protocolo no existen estados de polarización predefinidos, es decir, Alicia no envía estados de polarización como en los protocolos anteriores; los estados de polarización se generan en el momento de la medición.

Para generar la clave, Alicia y Bob comparten varios pares enredados de fotones. Estos estados se conocen como pares EPR (la paradoja EPR se trató en el capítulo III) y se pueden obtener de varias formas. Una es que Alicia prepare los pares y envíe las mitades a Bob, o al contrario. Otra opción es que entre a participar un tercero que prepare los pares y envíe las mitades correspondientes a Alicia y Bob. La última opción es que Alicia y Bob se hayan encontrado (incluso hace mucho tiempo) y hayan compartido los pares enredados guardándolos hasta el presente [Nielsen y Chuang 00].

Antes de generar la clave, Alicia y Bob prueban un conjunto aleatorio de pares con el fin de comprobar que están enredados y que son lo suficientemente puros. Esta prueba es posible gracias al teorema de la desigualdad de Bell, explicado en el Capítulo III. Los pares que no pasan esta prueba son desechados porque podrían haber sido modificados por un espía o haber adquirido cierto ruido en el canal.

Una vez tienen el conjunto de pares que usarán para generar la clave, tanto Alicia como Bob realizan mediciones independientes escogiendo aleatoriamente sus orientaciones. Luego se comunican por un canal público y comparan las orientaciones que usaron. En los casos en los que las orientaciones son diferentes, se desechan esos fotones, quedando así formada la clave por aquellos fotones para los que Alicia y Bob escogieron la misma orientación de medición. Como ya habían comprobado que los fotones estaban enredados, pueden estar seguros de que la información de los fotones medidos con la misma orientación es igual. Sólo queda hacer la correlación a bits y cifrar sus mensajes.

Respecto a la seguridad del protocolo, un espía no puede obtener información mientras los fotones están viajando por el canal cuántico, porque los fotones no llevan información codificada, están en un estado indeterminado. Además, si Eva realiza una medición, se perturba el enredo cuántico y al hacer la prueba, Alicia y Bob descartarían este par.

El protocolo EPR fue adaptado en 1992 por Bennett, Brassard y Mermin en un protocolo llamado BBM92, que para la generación de clave combina el enredo cuántico y el protocolo B92, que como se vio anteriormente, consiste en la medición aleatoria de fotones en dos bases no-ortogonales [Waks, Zeevi, y Yamamoto 02].

7 LA CRIPTOGRAFÍA CUÁNTICA COMERCIAL

A diferencia de la computación cuántica, que aún se enfrenta con grandes problemas (mencionados en el capítulo II), la criptografía cuántica en la actualidad ya ofrece productos comerciales. Esto debido a que no es necesario un computador cuántico para generar una clave cuántica. Desde el año 2002, las compañías Id Quantique, de Ginebra, y MagiQ Technologies, de Nueva York, han ofrecido al público productos comerciales que envían una clave de criptografía cuántica a más de los 30 centímetros recorridos en el experimento original de Bennett [Stix 2005]. Id Quantique, que se describe a sí misma como: "Líder en el desarrollo de soluciones avanzadas de cifrado basadas en la criptografía clásica y cuántica", ofrece las soluciones Cerberis (que combina el cifrado a alta velocidad basado en el estándar AES, con la seguridad de una Distribución de Clave Cuántica), Vectis (un hardware para cifrado de enlaces punto a punto en redes de fibra óptica que también usa AES y Distribución de Clave Cuántica), Clavis (un sistema para investigación y desarrollo de aplicaciones de Distribución de Clave Cuántica), y Quantis (un generador cuántico de números aleatorios *reales* que se puede conectar al puerto USB) [IdQuantique].

Figura 15: Sistema de criptografía cuántica de ID Quantique

La compañía MagiQ Technologies, creada en 2002, describe su actividad como: “Soluciones de información cuántica para el mundo real” [MagiQ], y ofrece MagiQ QPN, un sistema de Distribución de Clave Cuántica y criptografía digital convencional que promete: i) regeneración en tiempo real de claves criptográficas, ii) distribución de clave segura “irrompible” entre partes, y iii) cifrado y descifrado de datos.

La compañía SmartQuantum, creada en Octubre de 1994 y con sedes en Francia y Estados Unidos, promete “asegurar datos en movimiento” [SmartQuantum], y ofrece el “SQBox Defender”, que también combina Distribución de Clave Cuántica y criptografía digital.

Es importante mencionar que los costos de estos sistemas aún son bastante elevados, y los mercados de estas compañías se centran principalmente en el sector militar y gubernamental, o en algunas empresas que requieren seguridad extrema. Además hasta la fecha operan con fibra óptica y a distancias limitadas.

8 CONCLUSIONES

Los protocolos de criptografía cuántica tratados en esta monografía (BB84, B91 y E91), se abordaron de acuerdo a las siguientes preguntas:

1) *¿Cómo se transmite la información?* Esto incluye desde la codificación de bits a polarización de fotones y viceversa, hasta la forma en que se configuraría cada orientación de polarización de los filtros, teniendo en cuenta las propiedades de la mecánica cuántica.

2) *¿Qué pasa cuando hay un tercero que quiere leer la información?* En este caso se estudió el comportamiento del sistema cuando se involucra un espía, analizando cómo dicho espía perturba el mismo sistema con su medición, y cómo se puede detectar por medio de una verificación entre las partes.

Estos protocolos de criptografía cuántica se podrían clasificar de la siguiente forma:

	Por enredo cuántico	Por canal cuántico
Varias Polarizaciones	E91	BB84
Dos Polarizaciones	BBM92	B92

Es importante resaltar que la criptografía cuántica es, hasta la fecha, la única aplicación comercial de la rama de la Información Cuántica, y que empresas como MagiQ Technologies y Id Quantique, aunque estén aún en plena etapa experimental, han alcanzado la madurez necesaria para abrir un nuevo mercado.

Ahora falta que la criptografía cuántica sobrepase las limitaciones de distancia entre las partes, y que, ya sea por cables o satélites, logren un cubrimiento a nivel mundial, para así convertirse en un estándar en comunicaciones seguras. Y mientras esto ocurre, estaremos esperando la llegada del primer computador cuántico, que al hacer vulnerables algunos de los sistemas criptográficos actuales, nos obligaría a usar la criptografía cuántica como un estándar para comunicaciones seguras, sin importar el costo.

BIBLIOGRAFÍA

[Brown 00] Julian Brown. “Minds, Machines, and the Multiverse”. Simon & Schuster, NY; 2000. 396 páginas. ISBN: 0684814811

[Brukner 02] Caslav Brukner. “Quantum Entanglement: Information-theoretical Foundations, Bell’s Theorems and Quantum Communication Complexity”, Institut für Experimentalphysik der Universität Wien, 2002. 168 páginas.

[Cline 87] Barbara Lovett Cline. “Men Who Made a New Physics: Physicists and the Quantum Theory”. University Of Chicago Press. Estados Unidos, 1987. 288 páginas. ISBN: 0226110273.

[CSA] CSA’s Quantum Cryptography: http://www.csa.com/discoveryguides/crypt/overview.php

[Dornan 04] Andy Dornan. “Quantum Cryptography: Security through uncertainty”. Network Magazine. 2004. Página 61 y 62.

[DRMWiki] Digital Rights Management: http://en.wikipedia.org/wiki/Digital_rights_management

[Gershenfeld y Chuang 98] Neil Gershenfeld e Isaac L. Chuang. “Quantum Computing with Molecules”. Scientific American, 1998. http://www.media.mit.edu/physics/publications/papers/98.06.sciam/0698gershenfeld.html

[Goldrich 07] Oded Goldrich. “Foundations of Cryptography”. Cambridge University Press; 2007. 392 páginas. ISBN: 0521035368.

[Griffiths 04] David J. Griffiths. “Introduction to Quantum Mechanics (2nd Edition)”. Benjamin Cummings; 2nd edition; 2004. 480 páginas. ISBN: 0131118927.

[Gruska 99] Jozef Gruska. “Quantum Computing”. Mc Grawl-Hill, UK, 1999. 439 páginas. ISBN: 0077095030

[Harrison 99] Bell’s Theorem: http://www.upscale.utoronto.ca/GeneralInterest/Harrison/BellsTheorem/BellsTheorem.html

[Hodges] Historia de Alan Turing: http://www.turing.org.uk/turing/scrapbook/electronic.html

[IdQuantique] Id Quantique: “A quantum leap for Cryptography” http://www.idquantique.com

[Kahn 96] David Kahn. “Codebreakers”. Scribner; Rev Sub edition; 1996. 1200 páginas. ISBN: 0684831309.

[Lloyd 07] Seth Lloyd. “Programming the Universe: A Quantum Computer Scientist Takes on the Cosmos”. Vintage. Estados Unidos, 2007. 256 páginas. ISBN: 1400033861.

[MagiQ] MagicQ: http://www.magiqtech.com

[Martorell 00] Manuel Pons Martorell. “Criptología”. http://www.criptored.upm.es/descarga/criptologia.zip

[Menezes, Oorschot y Vanstone 97] A. Menezes, P. van Oorschot, S. Vanstone. “Handbook of Applied Cryptography”. CRC Press, Canada; 1997. 816 páginas. ISBN: 0849385237.

[Nielsen y Chuang 00] Michael A. Nielsen, Isaac L. Chuang. “Quantum Computation and Quantum Information”. Cambridge University Press, EEUU; 2000. 675 páginas. ISBN: 0521635039.

[Nikbin 06] Darius Nikbin. “Quantum encryption sets long-distance record”. PhysicsWeb, 2006. http://physicsweb.org/articles/news/10/10/2

[Ramió 06] Jorge Ramió. “Libro Electrónico de Seguridad Informática y Criptografía”. http://www.criptored.upm.es/guiateoria/gt_m001a.htm

[RSA] RSA: http://www.rsa.com/

[Sale] Historia del dispositivo COLOSSUS: http://www.codesandciphers.org.uk/lorenz/colossus.htm

[Savage 07] Neil Savage. “New Record for Quantum Cryptography”. MIT’s Technology Review, 2007. http://www.technologyreview.com/Infotech/18838/?a=f

[Singh 00] Simon Singh. “The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography”. Anchor; 2000. 432 páginas. ISBN: 0385495323.

[SmartQuantum] SmartQuantum: http://www.smartquantum.com/

[Stix 05] Gary Stix. “Criptografía cuántica comercial”. Investigación y Ciencia. 2005. Páginas: 55–59.

[Waks, Zeevi, y Yamamoto 02] Edo Waks, Assaf Zeevi, y Yoshihisa Yamamoto. “Security of quantum key distribution with entangled photons against individual attacks”. Physical Review, 2002. http://www.optics.rochester.edu/~stroud/cqi/stanford/3_Yamamoto.pdf

[Williams y Clearwater 98] Colin P. Williams y Scout H. Clearwater. “Explorations in Quantum Computing”. Springer-Verlag, New York; 1998. 307 páginas. ISBN: 038794768X

[Wired 07] The father of quantum computing: David Deutsch http://www.wired.com/science/discoveries/news/2007/02/72734

[Wolfram 1] Wolfram - Quantum Mechanics definition: http://scienceworld.wolfram.com/physics/QuantumMechanics.html

[Wolfram 2] Wolfram – Copenhagen Interpretation definition: http://scienceworld.wolfram.com/physics/CopenhagenInterpretation.html

[Wolfram 3] Wolfram – Hilbert Space definition: http://mathworld.wolfram.com/HilbertSpace.html